IMAGEN de la configuración ISE 2.2 con el proveedor del Active Directory WMI

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Antecedentes
Diagrama de la red
Flujo de trabajo
Configurar
Despliegue de la IMAGEN de la configuración ISE
Paso 1 (opcional). Instale los certificados confiables.
Paso 2 (opcional). Instale los Certificados del sistema.
Paso 3. Agregue el nodo secundario al despliegue.
Configure los proveedores del Active Directory
Paso 1. Únase a la IMAGEN ISE al dominio.
Paso 2. Agregue los agentes de PassiveID.
Verificación
Despliegue
Página del despliegue
Página del panel
Suscriptores
Resumen del sistema
Proveedores y sesiones
Home Page
Sesiones vivas
Troubleshooting
Despliegue
Problema frecuente: el nodo secundario no es reacheable
Active Directory y WMI
Problema frecuente: La IMAGEN ISE lanza “incapaz de ejecutar ejecutable en …” error

Introducción

Este documento describe cómo configurar y resolver problemas el despliegue pasivo del conector de la identidad del Identity Services Engine (IMAGEN ISE) con el proveedor de Windows Management Instrumentation del Active Directory (AD WMI). La IMAGEN ISE es una versión ligera ISE que se centra en las características pasivas ID.

La IMAGEN ISE es una sola solución ID para toda la cartera del Cisco Security que utilice la identidad pasiva solamente. Significa que la autorización o las directivas no se puede configurar

en la IMAGEN ISE. Apoya a diversos proveedores (agentes, WMI, Syslog, API) y puede ser integrado vía el RESTO API. ¿Tiene capacidades de preguntar los puntos finales (es el usuario abierto una sesión? Es el punto final todavía conectado?)

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

- Motor del servicio de la identidad de Cisco
- Microsoft Active Directory
- Microsoft WMI

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 2.2.0.470 pasiva del conector de la identidad del motor del servicio de la identidad de Cisco
- Service Pack 1 de Microsoft Windows 7
- R2 del Microsoft Windows server 2012

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

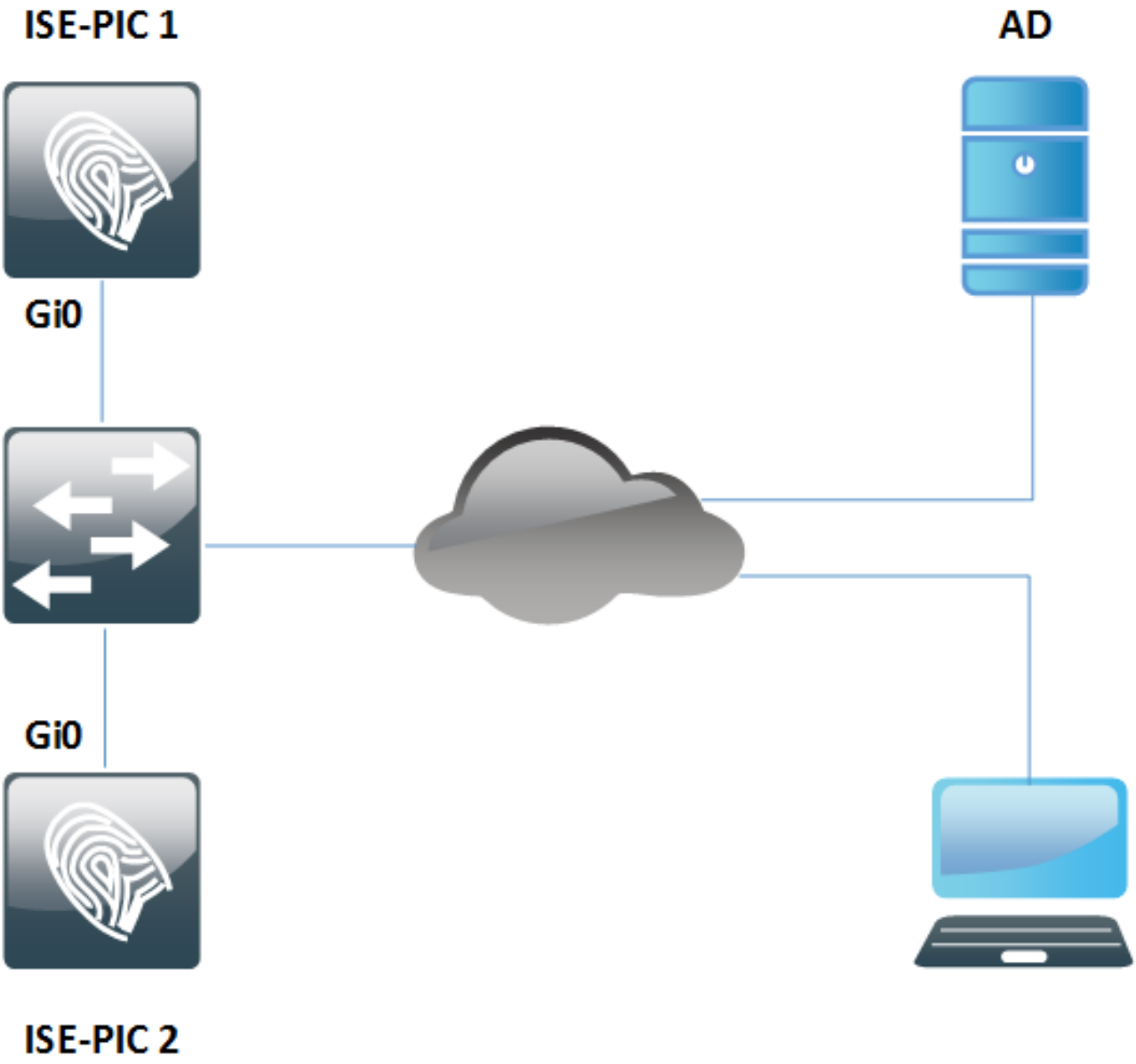
La cantidad máxima de Nodos en el despliegue de la IMAGEN ISE es 2. Este ejemplo muestra cómo configurar el despliegue de la IMAGEN ISE para la Alta disponibilidad, so2 que se utilizan las máquinas virtuales (VM). En un despliegue de la IMAGEN ISE, los Nodos pueden tener papeles: primario y secundario. En este solamente un nodo puede ser el en un momento primario y los papeles se pueden cambiar solamente manualmente con el GUI. En caso de la falla primaria todas las características todavía se ejecutan en secundario a excepción del UI. Solamente la promoción manual a primario habilita el UI.

Este ejemplo muestra cómo configurar el proveedor WMI para el Active Directory. WMI consiste en un conjunto de las Extensiones al modelo del driver de Windows que proporciona una interfaz del sistema operativo a través de la cual equipó los componentes proporcionen la información y la notificación. WMI es la implementación de Microsoft de los estándares modelo basados en web de la administración de empresas (WBEM) y de la información común (CIM) del grupo de trabajo distribuido de la Administración (DMTF).

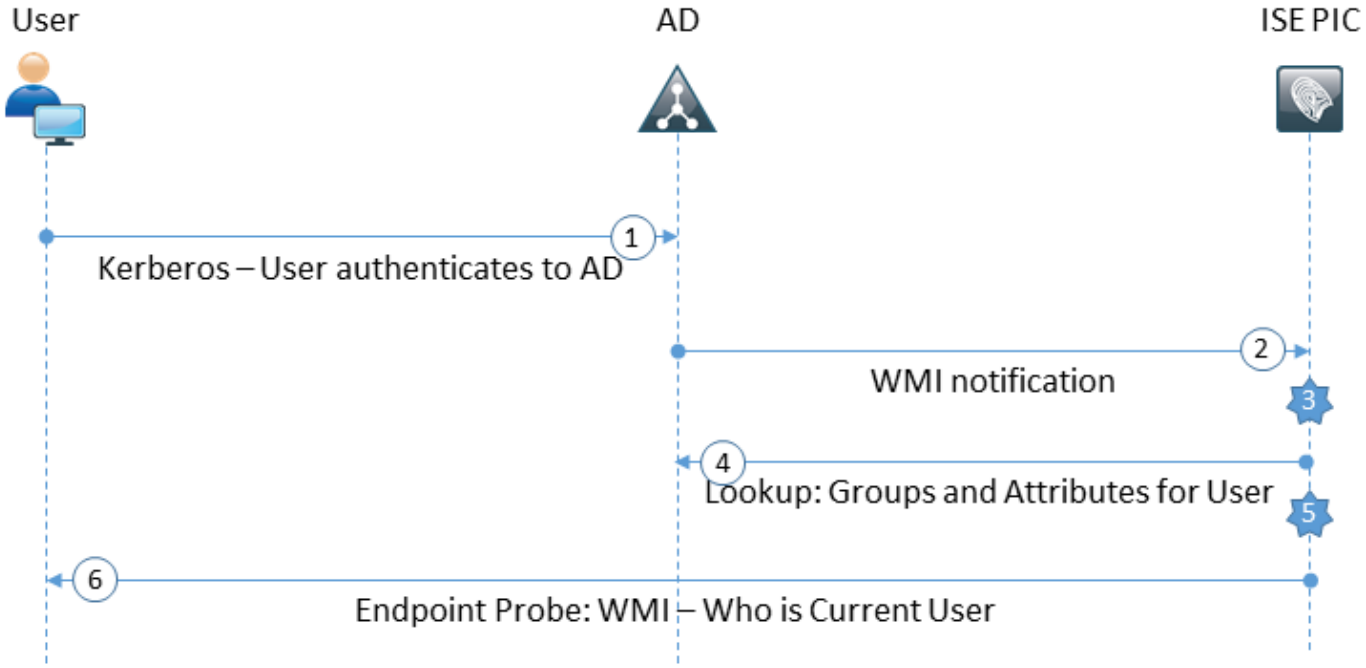
Nota: Más información sobre WMI se puede encontrar en el sitio de Microsoft del funcionario: Sobre WMI

Diagrama de la red

La información en el documento utiliza la configuración de la red mostrada en la imagen:



Flujo de trabajo



1. Inicie sesión al PC y consiga autenticado en el AD.

2. WMI notifica la IMAGEN ISE sobre esta autenticación.

3. El ISE agrega el nombre de usuario obligatorio: IP_Address a su directorio de la sesión.

4. El ISE extrae los grupos y los atributos de usuario del AD.

5. El ISE guarda esta información en su directorio de la sesión.

6. Cada 4 horas (no configurables) ISE de la IMAGEN de los funcionamientos de sonda del punto final:
   Primero intenta WMI al punto final.Si WMI falla entonces la IMAGEN ISE ejecuta ISEExec. Pregunta el punto final para el usuario y el permiso WMI por la vez próxima.También la IMAGEN ISE extrae la dirección MAC del punto final y del tipo OS.

   En la IMAGEN ISE es posible habilitar solamente/las sondas del punto final de la neutralización. El Nodo primario pregunta todos los puntos finales, nodo secundario está para la Alta disponibilidad solamente.

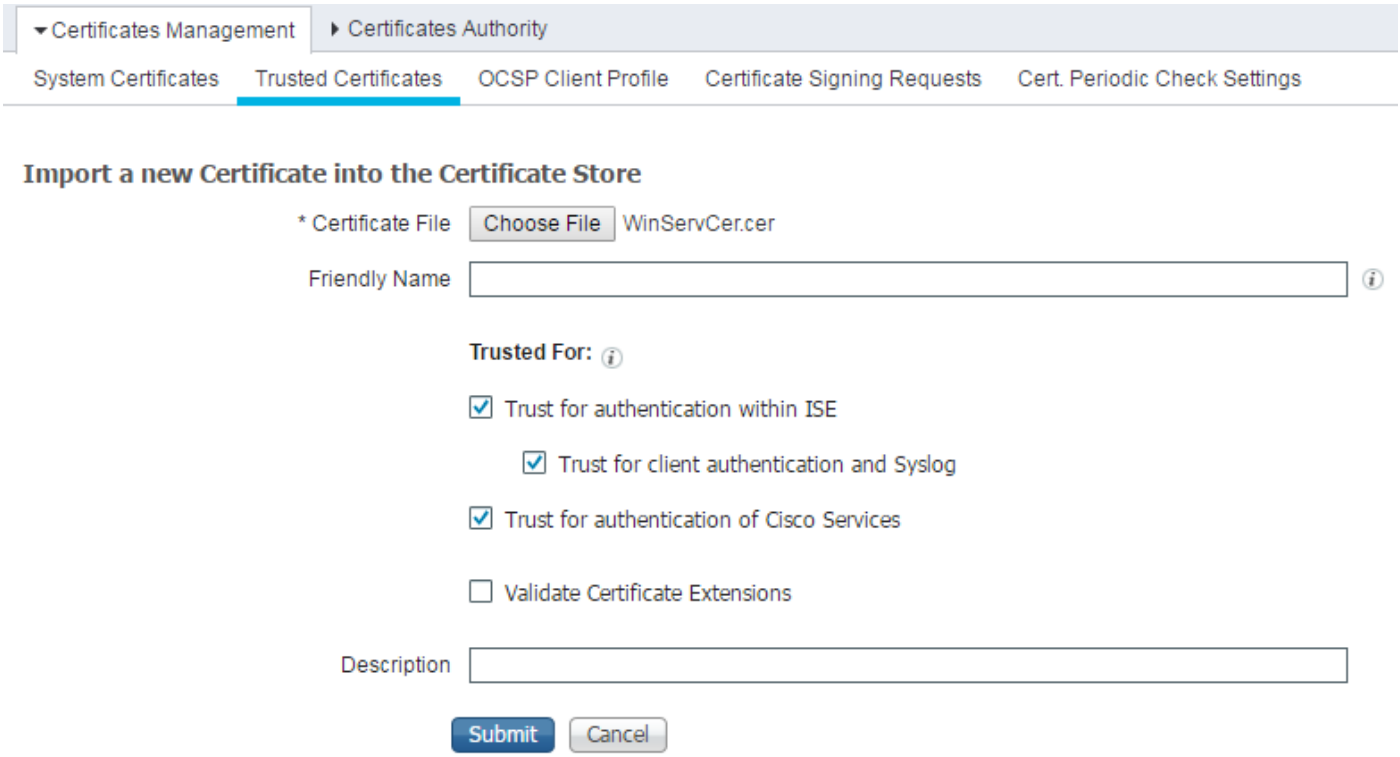
Configurar

Despliegue de la IMAGEN de la configuración ISE

Paso 1 (opcional). Instale los certificados confiables.

El encadenamiento lleno de los Certificados de su Certificate Authority (CA) se debe instalar al almacén confiado en ISE. Inicie sesión a la IMAGEN GUI ISE y navegue a los **Certificados > a la Administración > a los certificados confiables de Certificados**. Haga clic la **importación** y seleccione su certificado de CA de su PC.

Tal y como se muestra en de la imagen, el tecleo **somete** para salvar los cambios. Relance este paso para todos los Certificados del encadenamiento. Relance los pasos en el nodo secundario también.

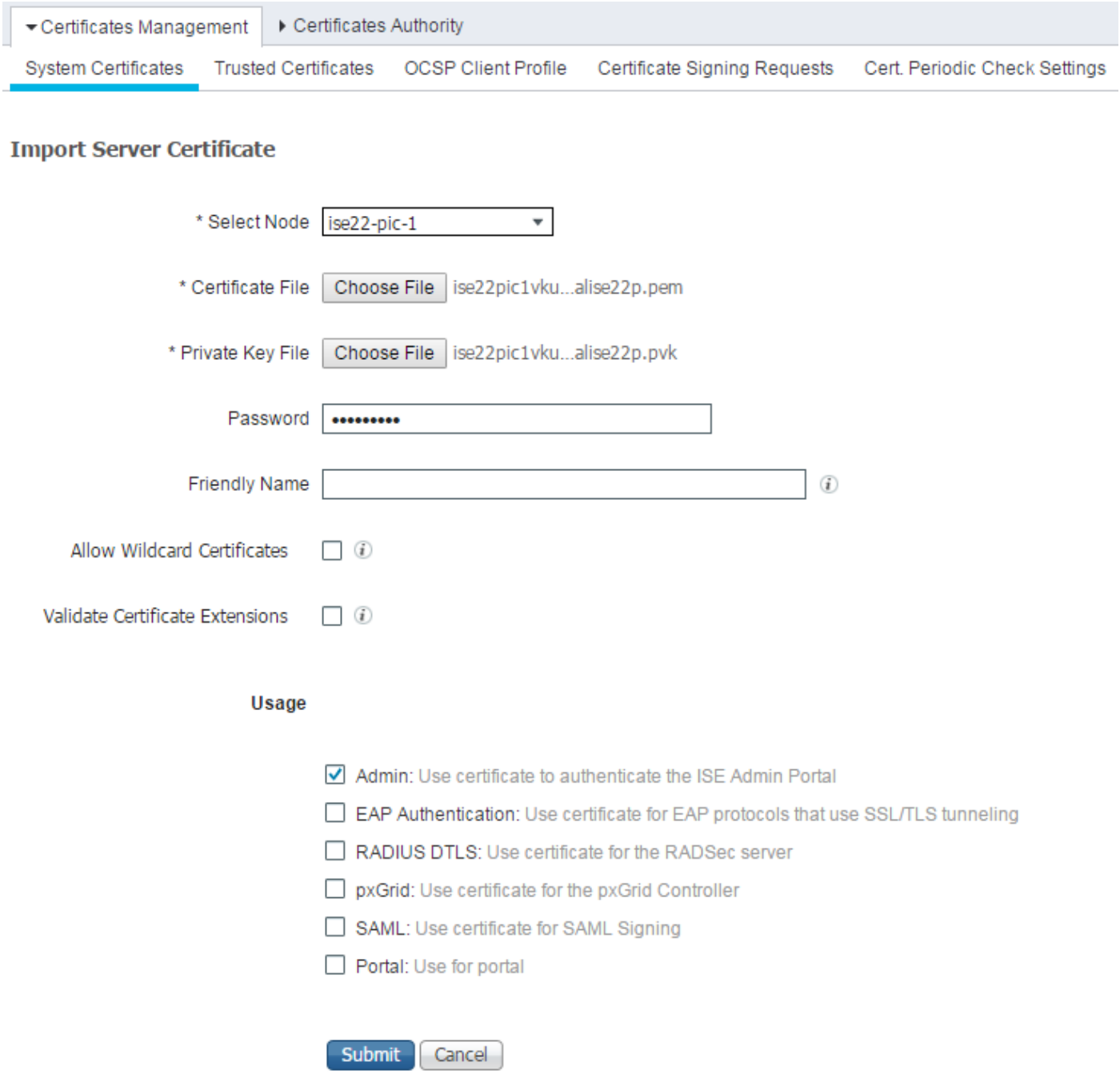


Paso 2 (opcional). Instale los Certificados del sistema.

La opción 1. certifica generado ya por CA junto con la clave privada.

Navegue a los **Certificados de los Certificados > de la Administración > del sistema de Certificados** y haga clic la **importación**. Seleccione el **archivo de certificado** y el **archivo de clave privado**, ingresa el campo de *contraseña* si se cifra la clave privada.

Tal y como se muestra en de las **opciones de uso del** control de la imagen:



Nota: Puesto que la IMAGEN ISE se basa en el código ISE y se puede convertir fácilmente al ISE completamente equipado con las licencias apropiadas, todas las opciones de uso están disponibles. Los papeles tales como **autenticación EAP**, **RADIUS DTL**, **SAML** y **portal** no son utilizados por la IMAGEN ISE.

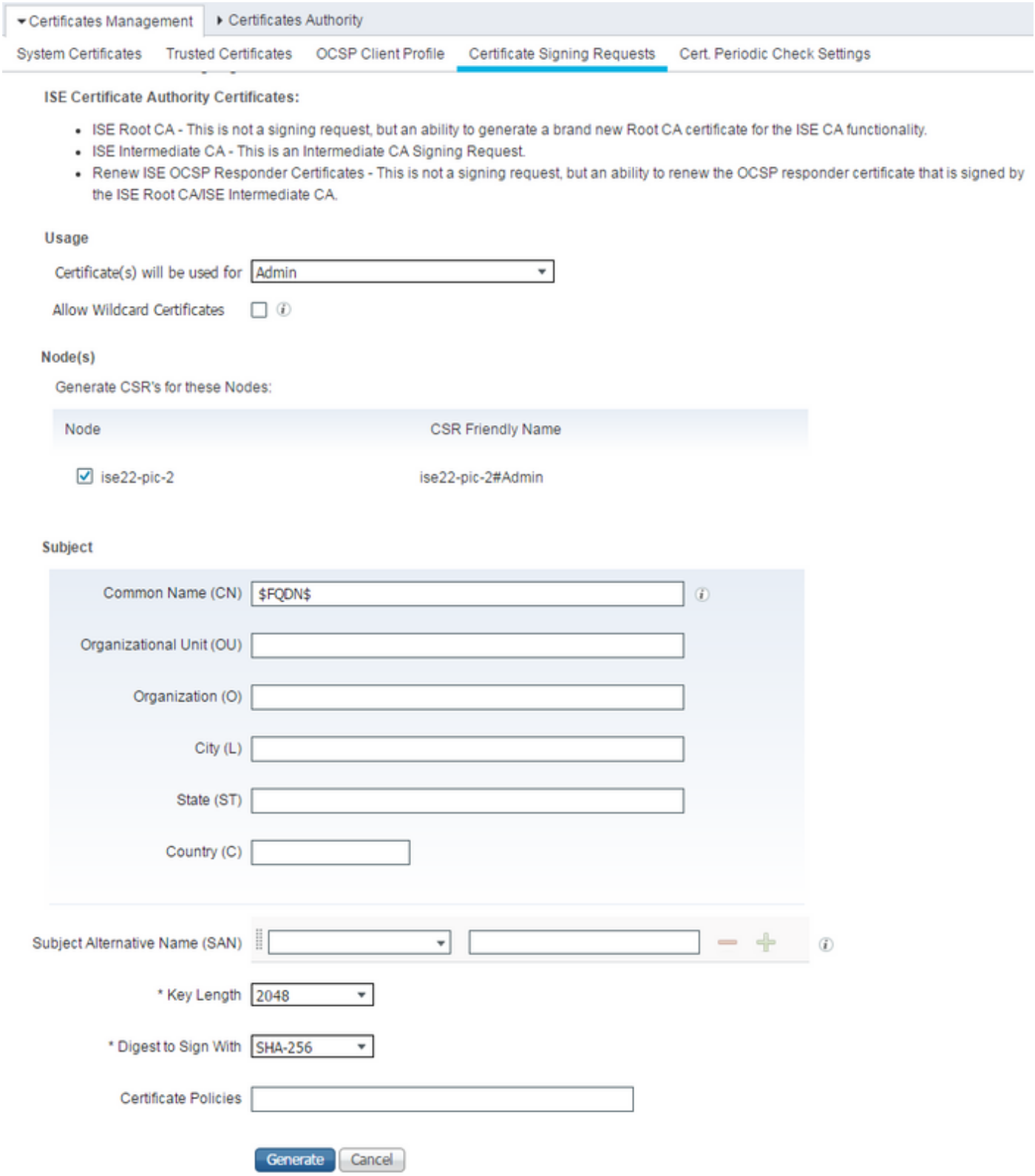
El tecleo **somete** para instalar el certificado. Relance este procedimiento en un nodo secundario también.

Nota: Todos los servicios en el nodo de la IMAGEN ISE recomienzan después de que importación del certificado de servidor.

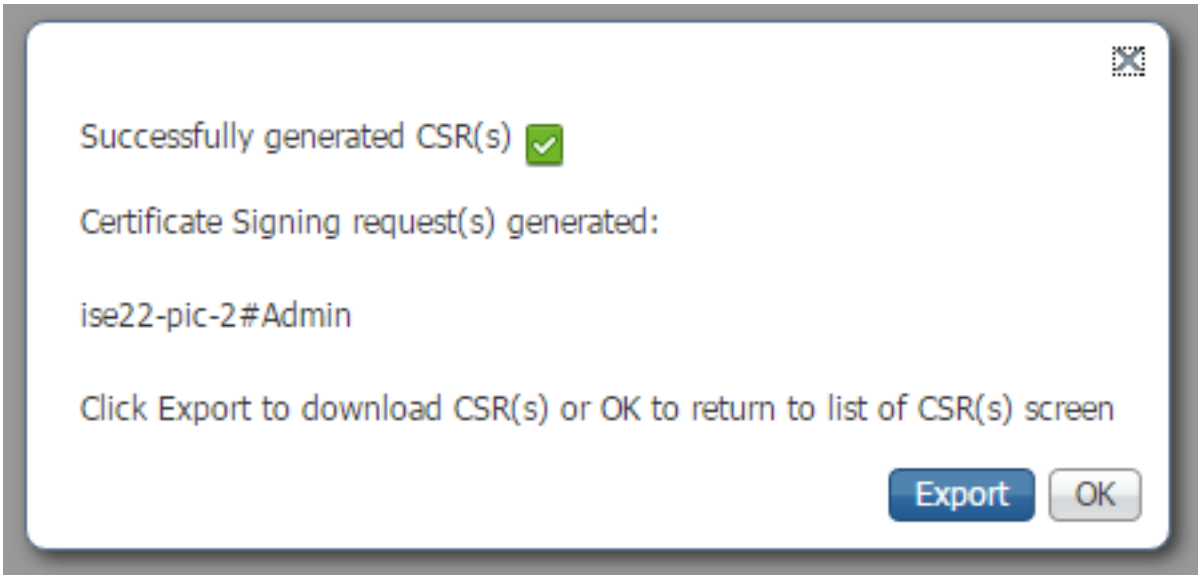
La opción 2. genera el pedido de firma de certificado (CSR), lo firma con CA y ata en el ISE.

Navegue a la página de los **Certificados > de la Administración > de los pedidos de firma de certificado de Certificados** y el tecleo **genera los pedidos de firma de certificado (CSR)**.

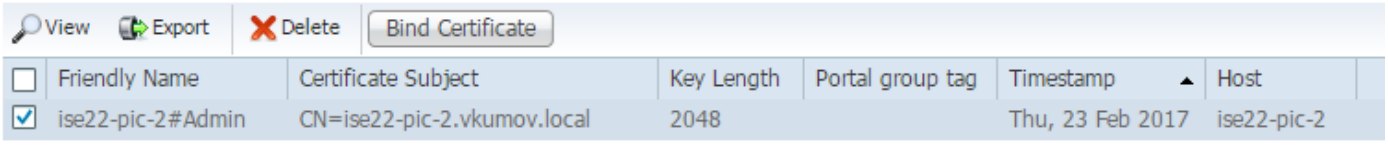
Seleccione el nodo y el uso, ingresa los otros campos si procede:



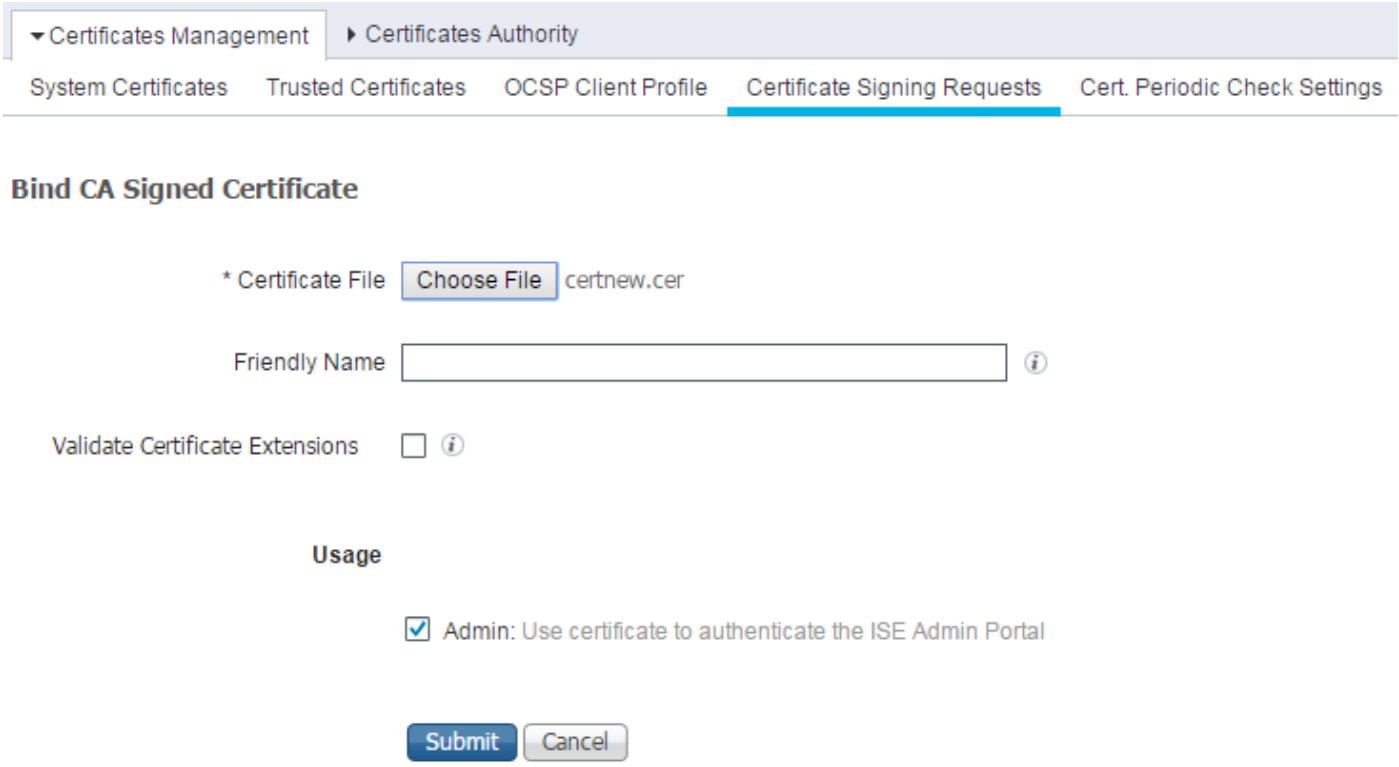
El tecleo **genera.** La nueva ventana surge con una opción **para exportar el** CSR generado:



Haga clic la **exportación,** salve el archivo generado ***.pem** y fírmelo con CA. Una vez que se firma el CSR navega de nuevo a la página de los **Certificados > de la Administración > de los pedidos de firma de certificado de Certificados**, selecciona su CSR y haga clic el **certificado del lazo**:



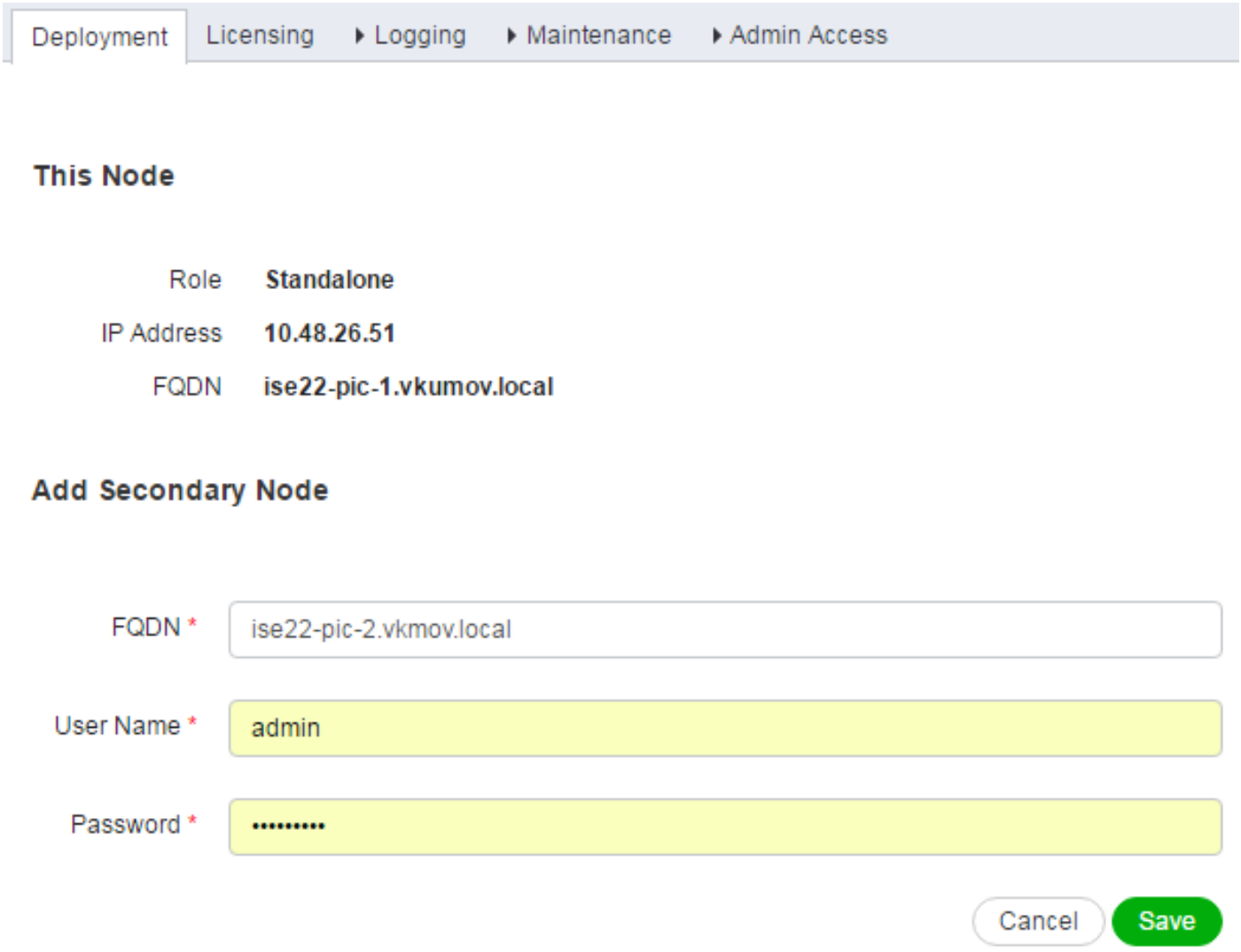
Seleccione el certificado que fue firmado con su CA y el tecleo **somete** para aplicar los cambios:



Todos los servicios en el reinicio del nodo de la IMAGEN ISE después de que usted tecleo **someta** para instalar el certificado.

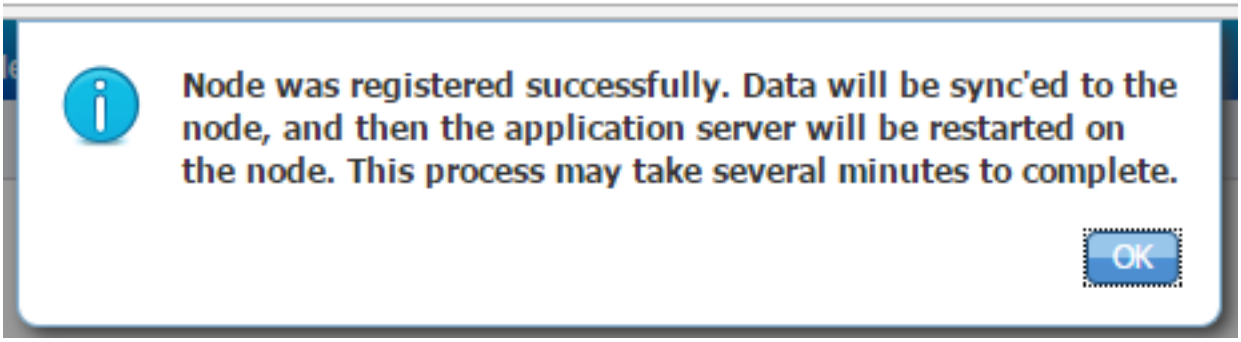
Paso 3. Agregue el nodo secundario al despliegue.

La IMAGEN ISE permite tener 2 Nodos en un despliegue para la Alta disponibilidad. No requiere para tener una confianza bidireccional de los Certificados (que comparan al despliegue usual ISE). Para agregar un nodo secundario al despliegue, navegue a la **página de la administración > del despliegue** en su nodo primario de la IMAGEN ISE, tal y como se muestra en de la imagen:

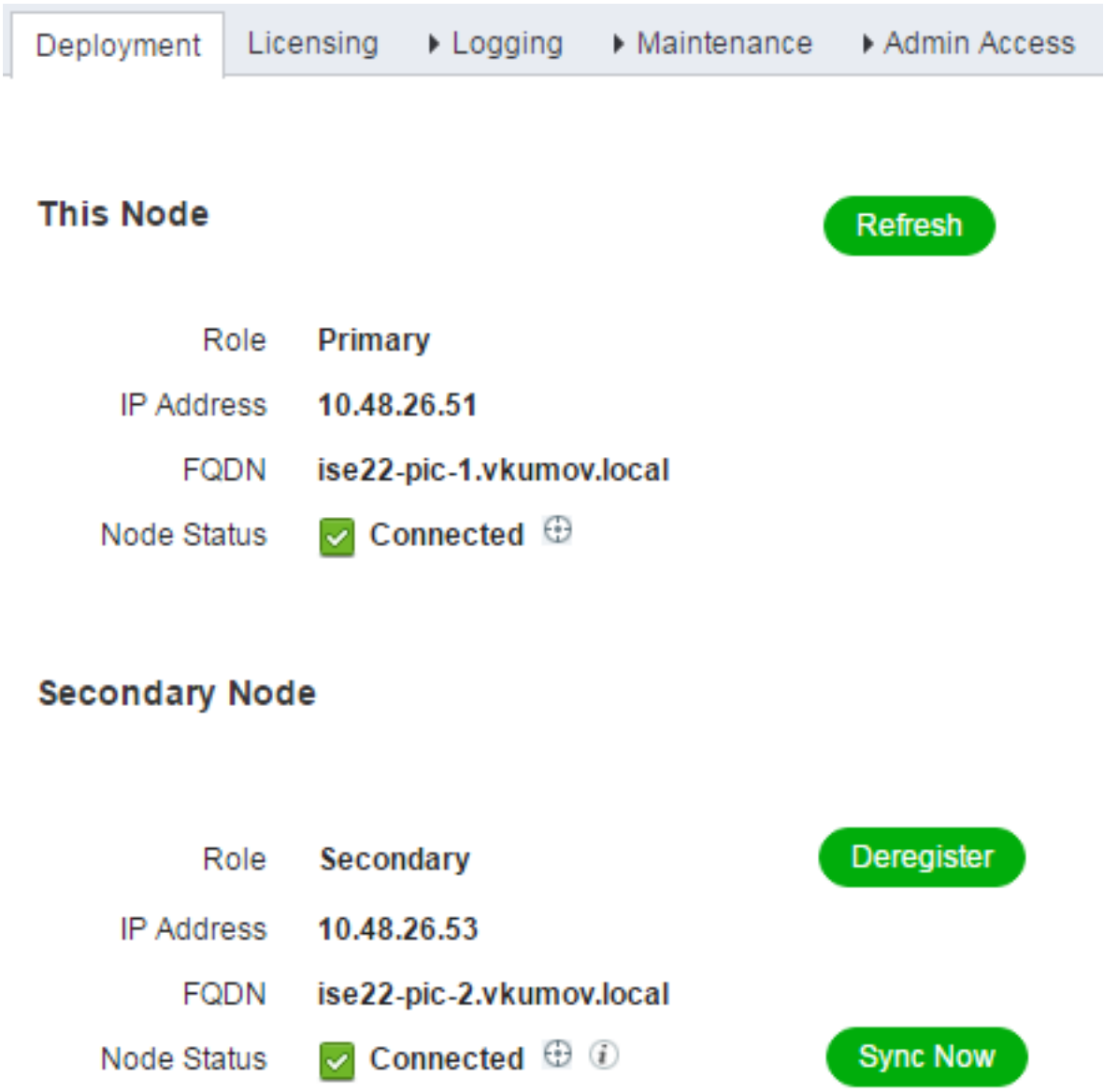


Ingrese el Nombre de dominio totalmente calificado (FQDN) (FQDN) del nodo secundario, las credenciales del administrador de esa **salvaguardia del** nodo y del tecleo. En caso de que el nodo primario de la IMAGEN ISE no pueda verificar el certificado admin del segundo nodo pide la confirmación antes de que instale que certificado en el almacén de confianza.

En tal tecleo del caso **Import Certificate (Importar certificado) y proceda** para unirse al nodo al despliegue. Usted debe conseguir una notificación que el nodo esté agregado con éxito. Todos los servicios en los reinicios secundarios del nodo.



Dentro de 10-20 Nodos de los minutos debe ser sincronizado y el estatus del nodo debe cambiar de **en curso** a conectado:



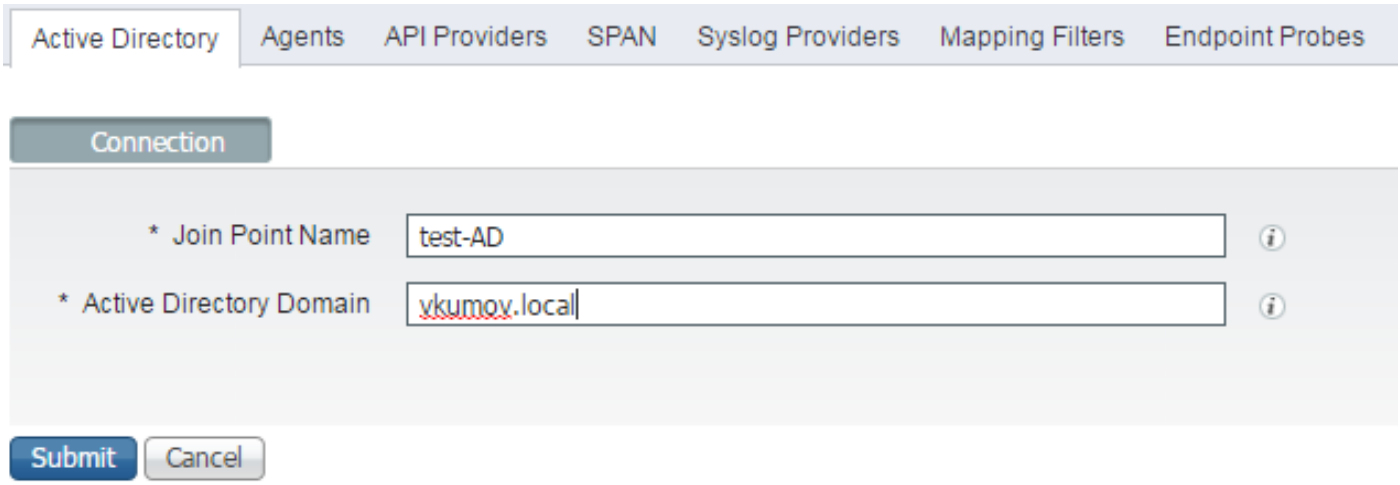
Proveedores del Active Directory de la configuración

La IMAGEN ISE utiliza Windows Management Instrumentation (WMI) para recoger la información sobre las sesiones del AD y los actos como un communitation del Pub/del submarino, que significa:

- La IMAGEN ISE inscribe a ciertos eventos
- WMI alerta la IMAGEN ISE cuando ocurren esos eventos: 4768 (el Kerberos marca la concesión) y 4770 (el Kerberos marca la renovación)Las entradas en el directorio de la sesión expiran (la purgación)

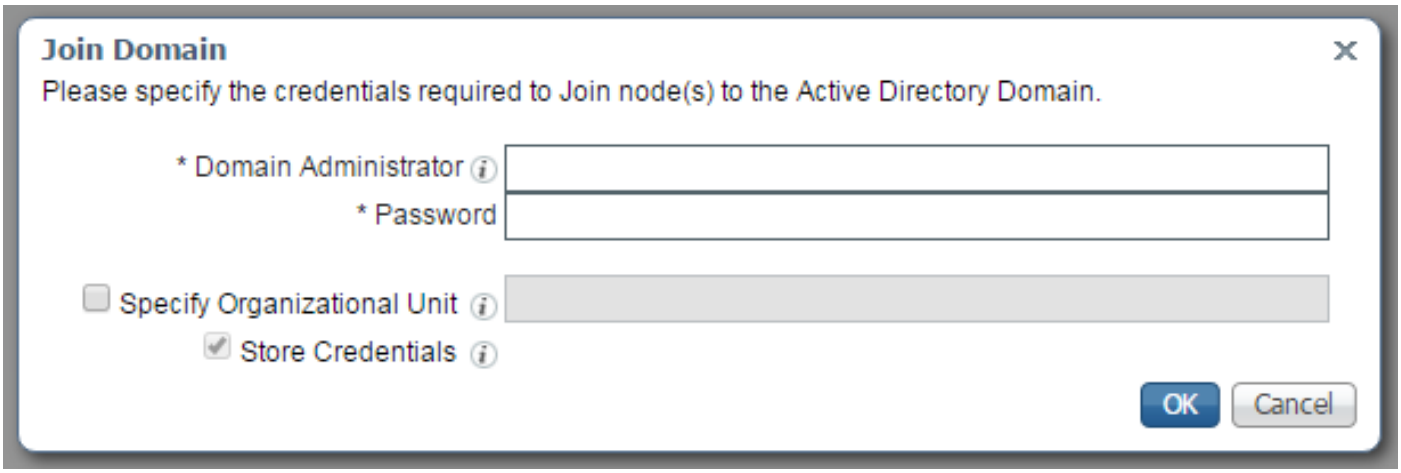
Paso 1. Únase a la IMAGEN ISE al dominio.

Para unirse a la IMAGEN ISE al dominio, navegar a los **proveedores > al Active Directory** y al tecleo **agregue**:



El terraplén **se une al nombre de la punta** y los campos y el tecleo del **dominio de Active Directory someten** para salvar los cambios. **Únase al nombre de la punta** es un nombre que se utiliza en la IMAGEN ISE solamente. **El dominio de Active Directory** es el nombre del dominio donde la IMAGEN ISE debe ser unida a y debe ser resolvable con el servidor DNS configurado en la IMAGEN ISE.

Después de que la creación de la IMAGEN de la punta ISE Join deba preguntarle si usted quisiera unirse a los Nodos al dominio. Haga clic en Sí Una ventana debe surgir para que usted proporcione las credenciales para unirse al dominio:



Llene los campos del **administrador de dominio** y de **contraseña** y haga clic la **AUTORIZACIÓN.**

Aunque el campo se llama **administrador de dominio** no es necesario utilizar al usuario administrador **para unirse a la** IMAGEN ISE al dominio. Este usuario debe tener privilegios suficientes de crear y de quitar las cuentas de equipo en el dominio, o altere las contraseñas para las cuentas de equipo previamente creadas. Los permisos de la cuenta de directorio activa requeridos para realizar las diversas operaciones se pueden encontrar en este documento.

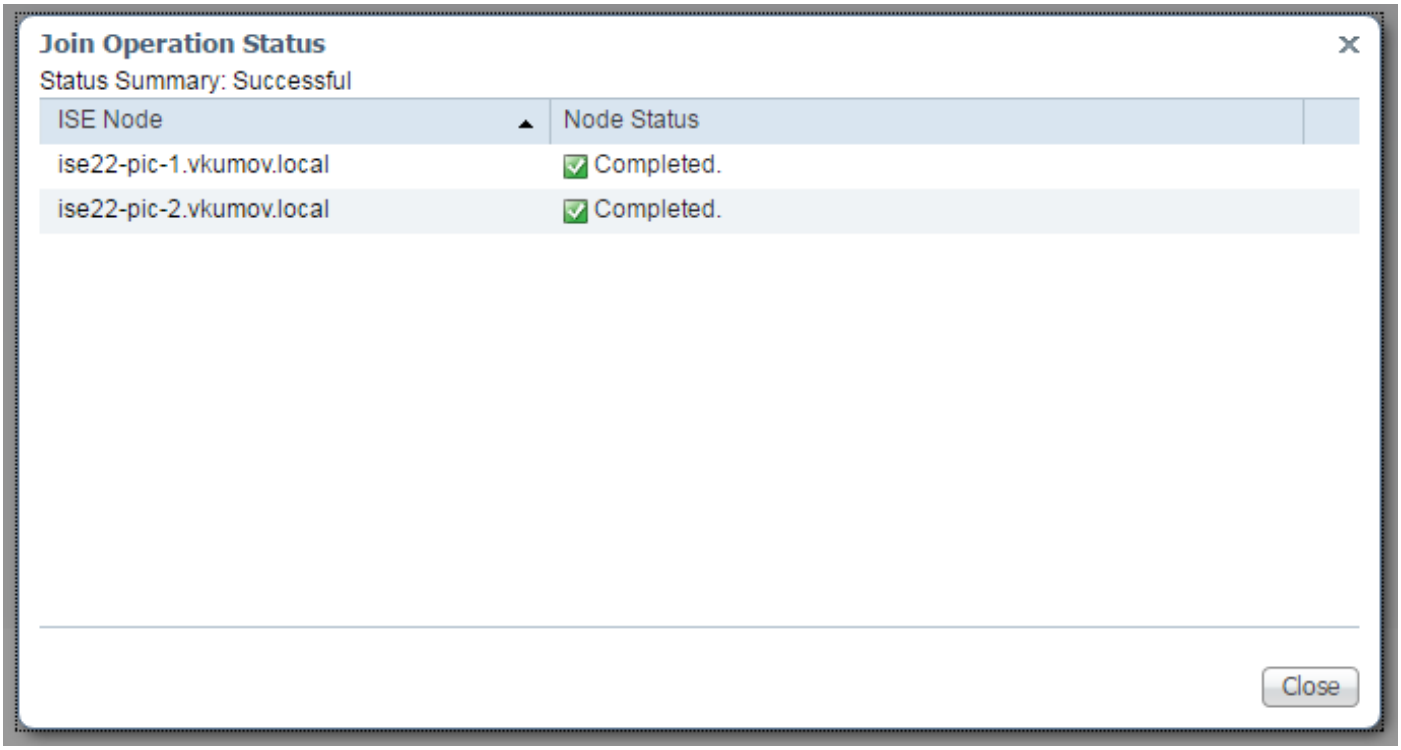
Sin embargo es administrador de dominio del uso del requiredto que las credenciales durante se unen a si usted quisiera utilizar WMI. La opción de los **Config WMI** requiere:

- Cambios de registro
- Permisos para utilizar el DCOM

- Permisos para utilizar WMI remotamente
- Acceso para leer el registro de evento de seguridad del dominio Controlle AD
- Firewall de Windows debe permitir el tráfico desde/hasta la IMAGEN ISE (la correspondencia firewall de Windows las directivas será creada durante los **Config WMI**)

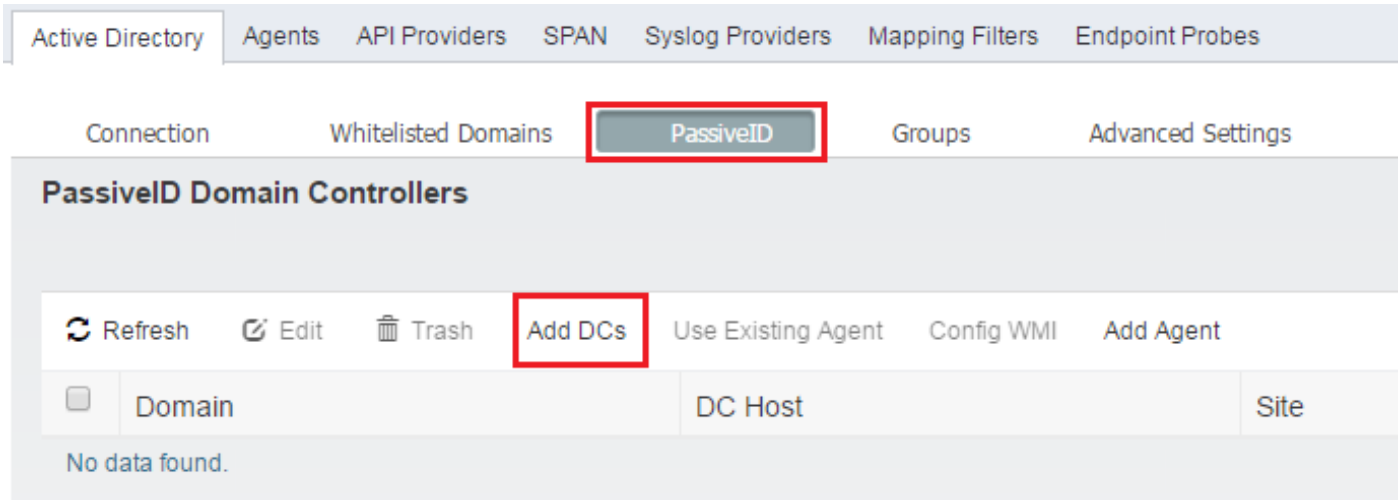
  Nota: Las credenciales del almacén son se habiliten siempre en la IMAGEN ISE puesto que se requiere para las sondas del punto final y la configuración WMI. El ISE las salva cifró internamente.

Tal y como se muestra en de la imagen, la IMAGEN ISE muestra el resultado de la operación en una nueva ventana:



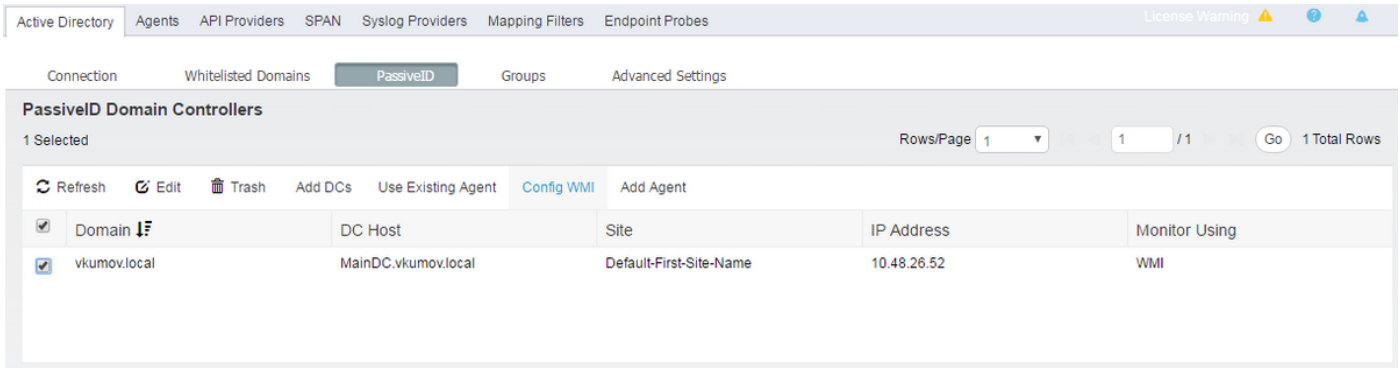
Paso 2. Agregue los agentes de PassiveID.

En la página del dominio AD navegue a la lengueta de PassiveID y el tecleo **agrega DCS**, tal y como se muestra en de la imagen:

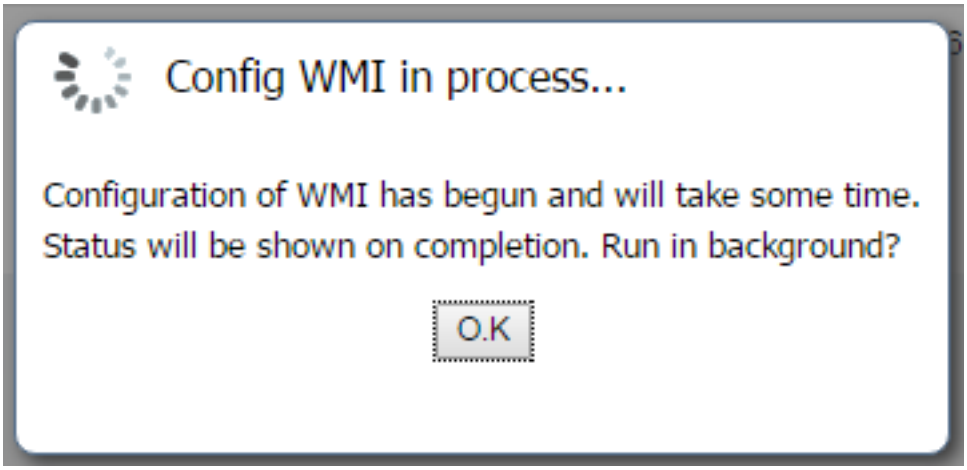


Una nueva ventana surge y el ISE carga una lista de todos los controladores de dominio disponibles. Seleccione DCS donde usted quisiera configurar WMI y hacer clic la **AUTORIZACIÓN** para salvar los cambios, tal y como se muestra en de la imagen:

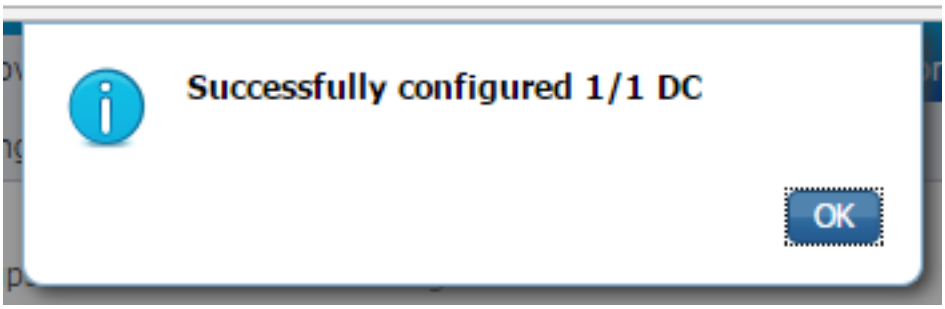
DCS seleccionado se agrega a la lista de **controladores de dominio de PassiveID.** Seleccione su DCS y haga clic el botón de los **Config WMI**:



La IMAGEN ISE muestra a mensaje que el proceso de configuración está en curso:



Después de que el par de los minutos él le muestre un mensaje que WMI está configurado con éxito en DCS seleccionado:



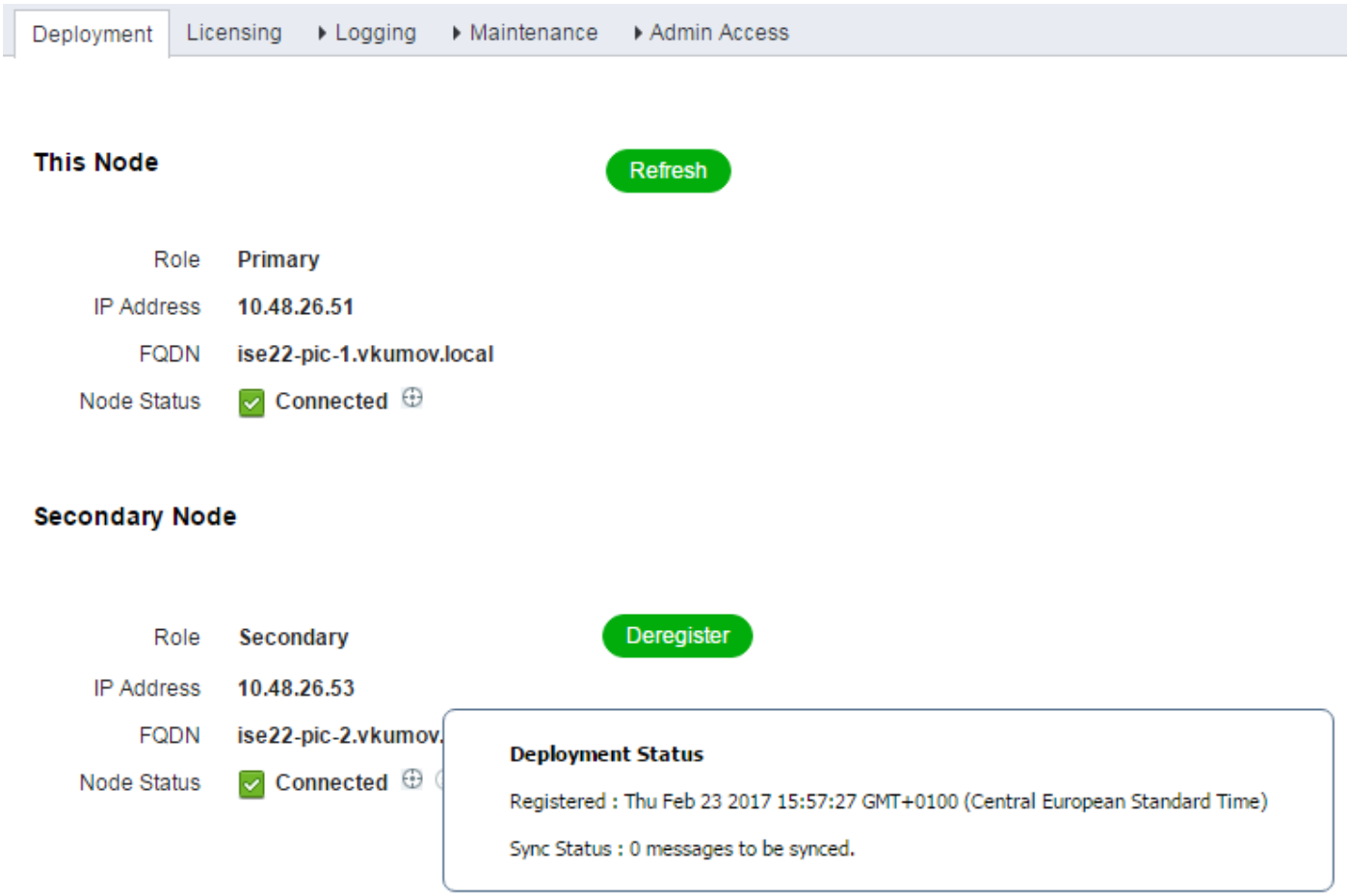
Verificación

Despliegue

El estatus del despliegue se puede llegar algunas de las maneras:

Página del despliegue

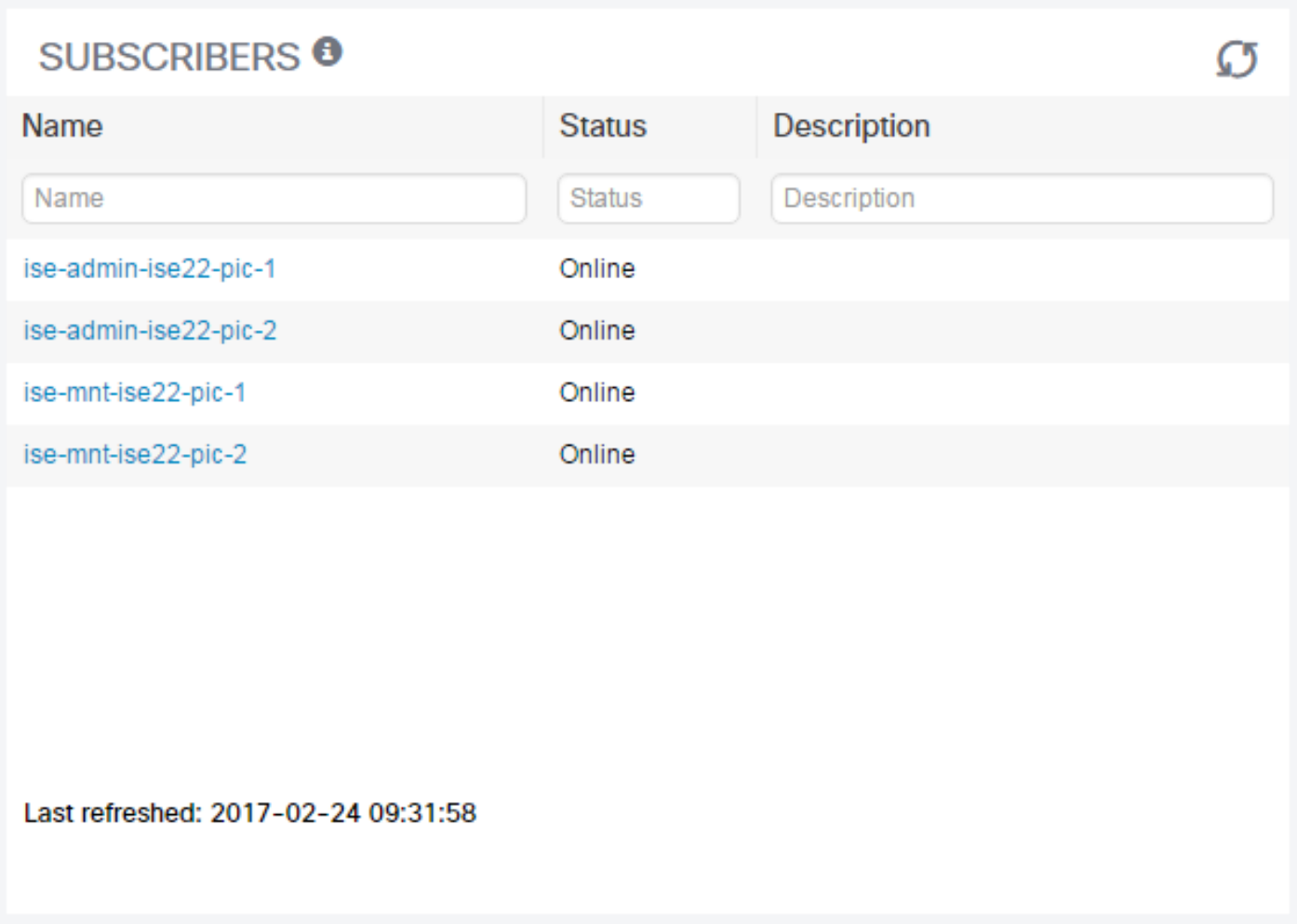
Navegue a la **página de la administración > del despliegue que el** estado actual del despliegue puede ser marcado:



De esta página el nodo secundario puede de desregistrado si es necesario. La sincronización manual puede ser comenzada y el **estado de sincronización** puede ser marcado.

Página del panel

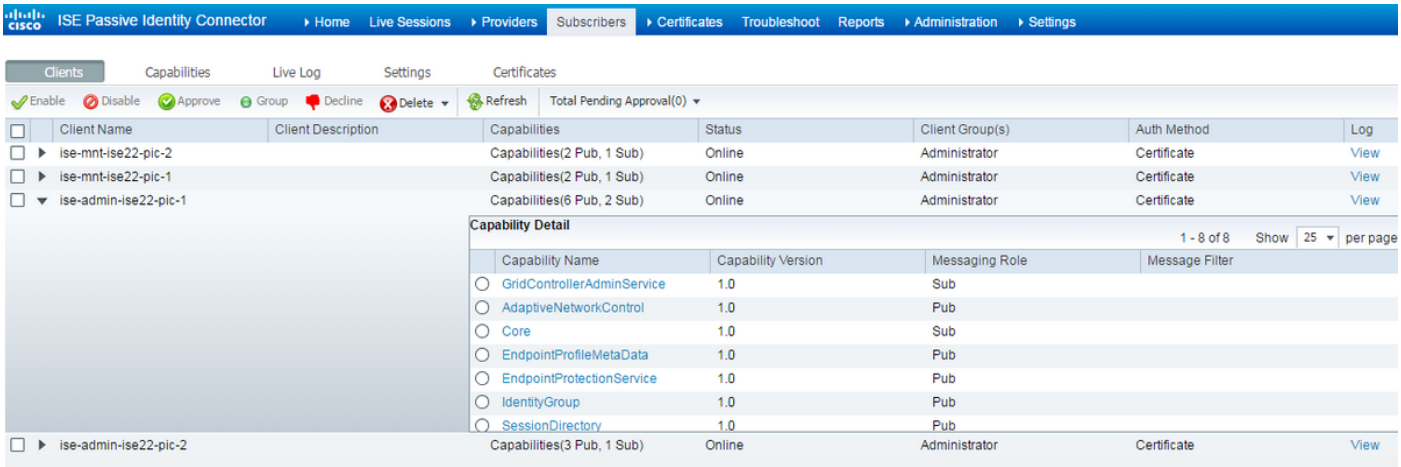
En una página principal de la IMAGEN ISE hay un dashlet llamado **Subscribers**. Con este dashlet usted puede marcar el estado actual de sus Nodos de la IMAGEN ISE, tal y como se muestra en de la imagen:



La IMAGEN ISE crea a 2 suscriptores para cada nodo - **admin** y **MNT.** Todos deben estar en el **estado en línea** que significa que los Nodos son reacheable y operativos.

Suscriptores

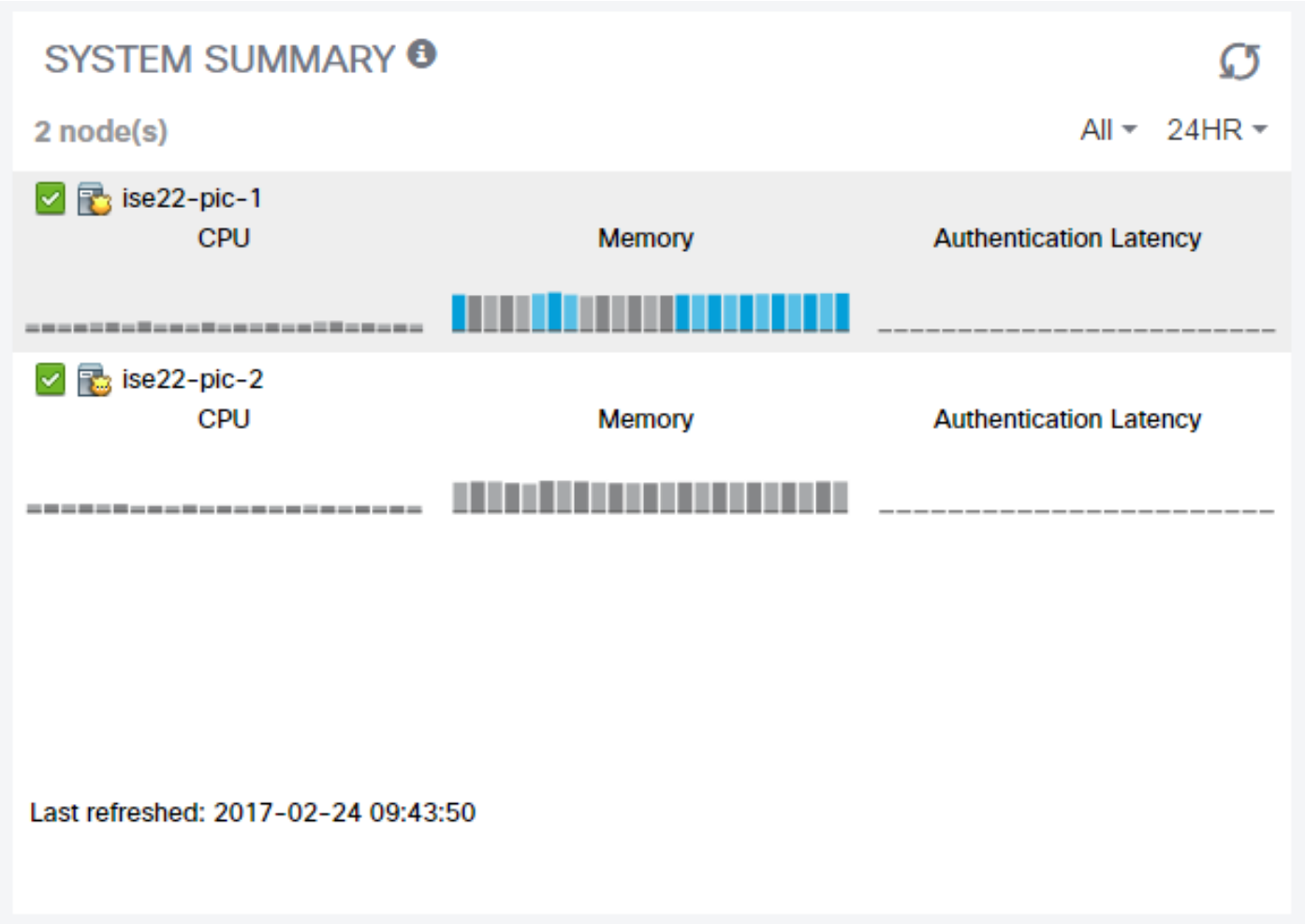
Los suscriptores paginan son una versión extendida del dashlet de los suscriptores del Home Page de la IMAGEN ISE. Esta página muestra todo el pxGrid relacionado, no obstante el estatus de los Nodos de la IMAGEN ISE se puede marcar aquí también:



Resumen del sistema

La IMAGEN ISE permite monitorear el resumen de la salud de los Nodos también. Este dashlet se

puede encontrar en casa **> panel > adicional**:

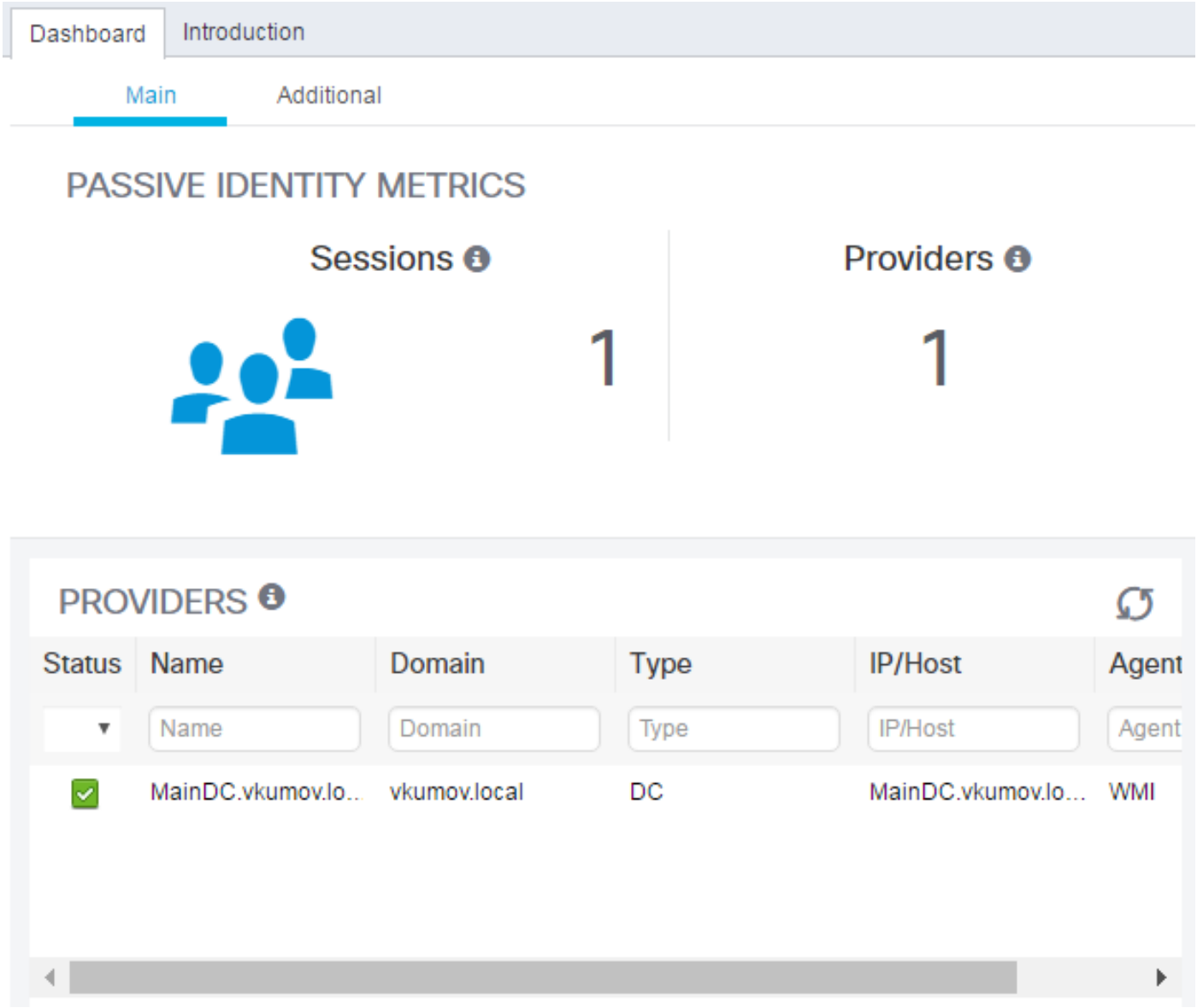


El tiempo de espera de la autenticación es siempre 0ms puesto que la IMAGEN ISE no realiza ningunas autenticaciones/autorizaciones.

Proveedores y sesiones

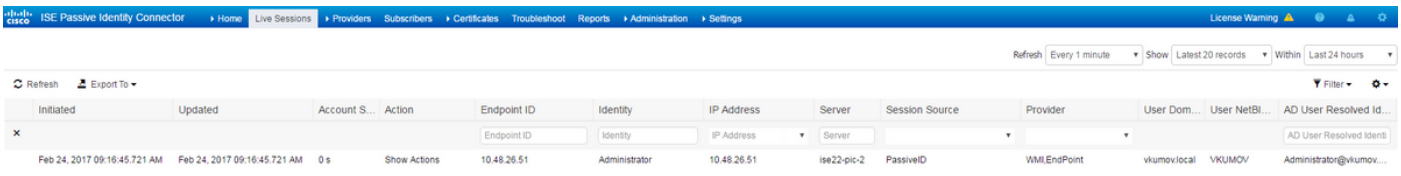
Home Page

Los estatuses de los proveedores, su cantidad y la cantidad de sesiones encontradas pueden ser marcados mientras que usted navega **para dirigirse > página del panel**:



Sesiones vivas

La información detallada sobre toda encontró que las sesiones de usuarios pueden ser encontrados en la página de las **sesiones Live**:



Contiene la información tal como:

- Proveedor - qué proveedores fueron utilizados para identificar esta sesión
- Iniciado y puesto al día - grupos fecha/hora en que la sesión se inicia y se pone al día por consiguiente
- Dirección IP - el direccionamiento del punto final

- La acción - las acciones que el ISE puede realizar (por ejemplo, estatus del punto final del control, o si la IMAGEN ISE se integra con el pxGrid después envía una petición de borrar la sesión)

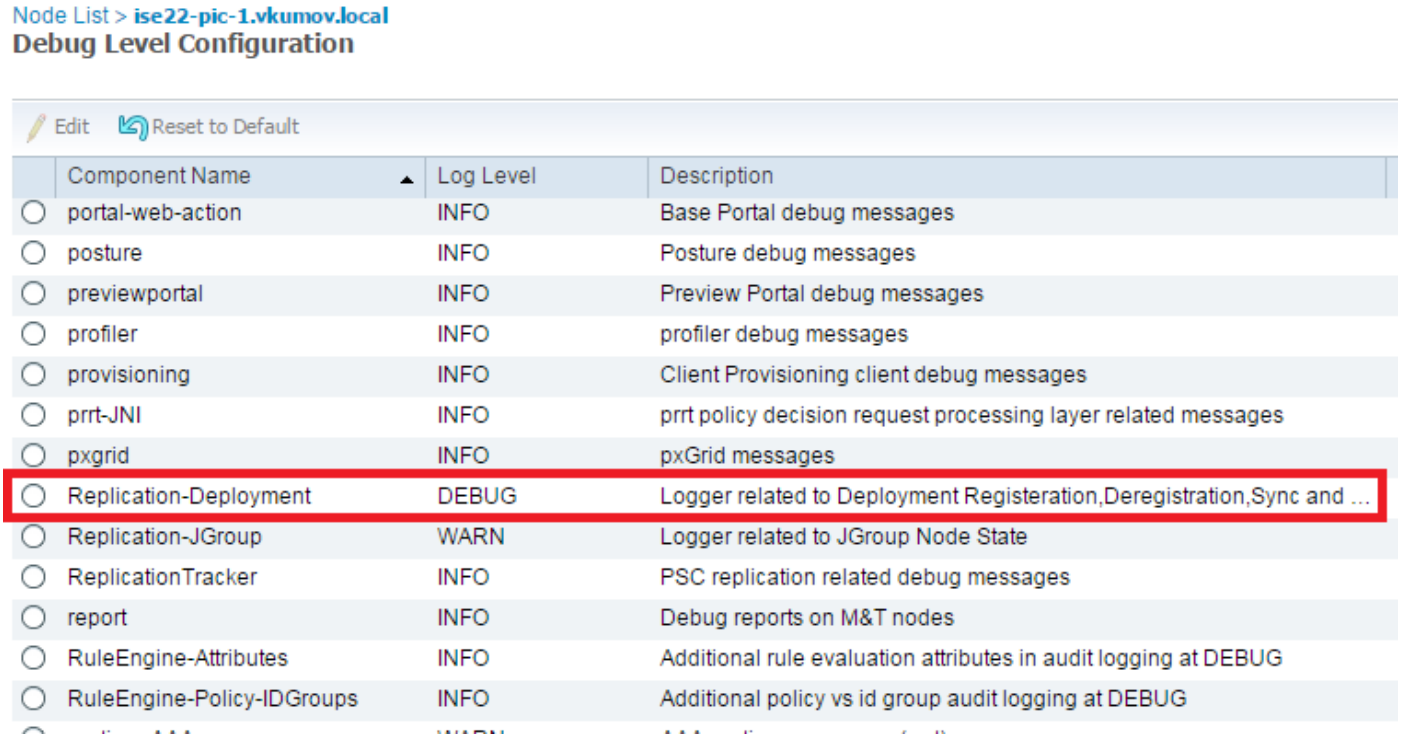
Troubleshooting

Despliegue

Para resolver problemas los problemas del despliegue y del repliaction, mire en esos archivos del registro:

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

Para habilitar los debugs, navegue a la **administración > a la configuración del registro del registro > del debug**:



Estos debugs se escriben al archivo de **replication.log**. Aquí está un ejemplo de un proceso de replicación 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 mensaje de **ise-psc.log**:

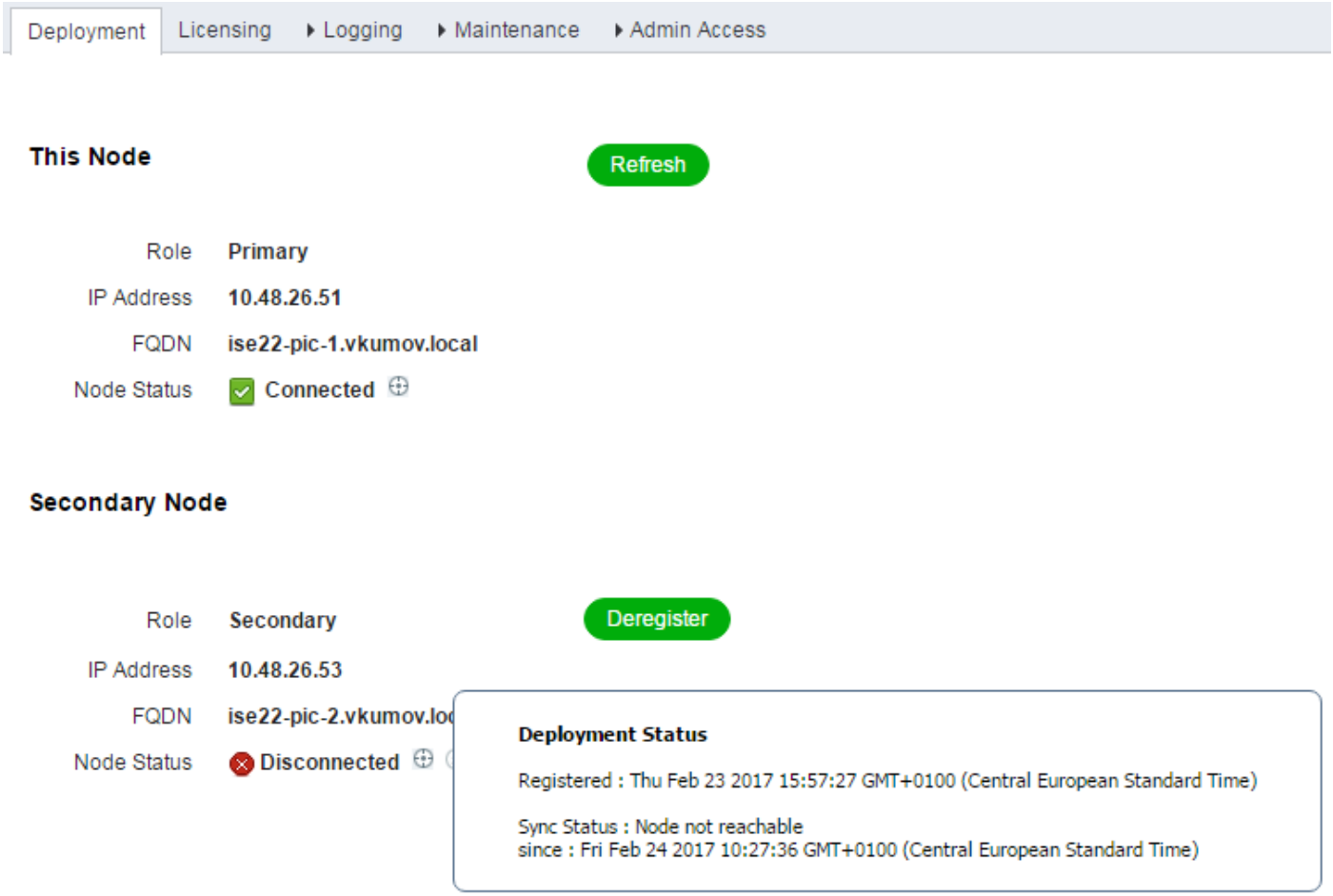
2017-02-24 10:11:06,893 INFO [pool-215-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -::::- Calling the publisher job from
clusterstate processor
2017-02-24 10:11:06,893 DEBUG [pool-214-thread-1][]

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]
```

Problema frecuente: el nodo secundario no es reacheable

Si el nodo secundario llega a ser unreacheable sería visualizado en la **página de la administración > del despliegue**:



ise-psc.log contiene el este mensaje:

```
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
```

Este mensaje explica cuál no es reacheable, por ejemplo el nodo no responde para hacer ping:

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

Acciones a tomar: marque si FQDN del nodo socandary es resolvable, conectividad de red básica del control entre los Nodos.

En caso de que las aplicaciones no estén en el estado de ejecución en el nodo secundario o hay un Firewall entre los Nodos, **ise-psc.log** puede mostrar esos mensajes:

```
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
```

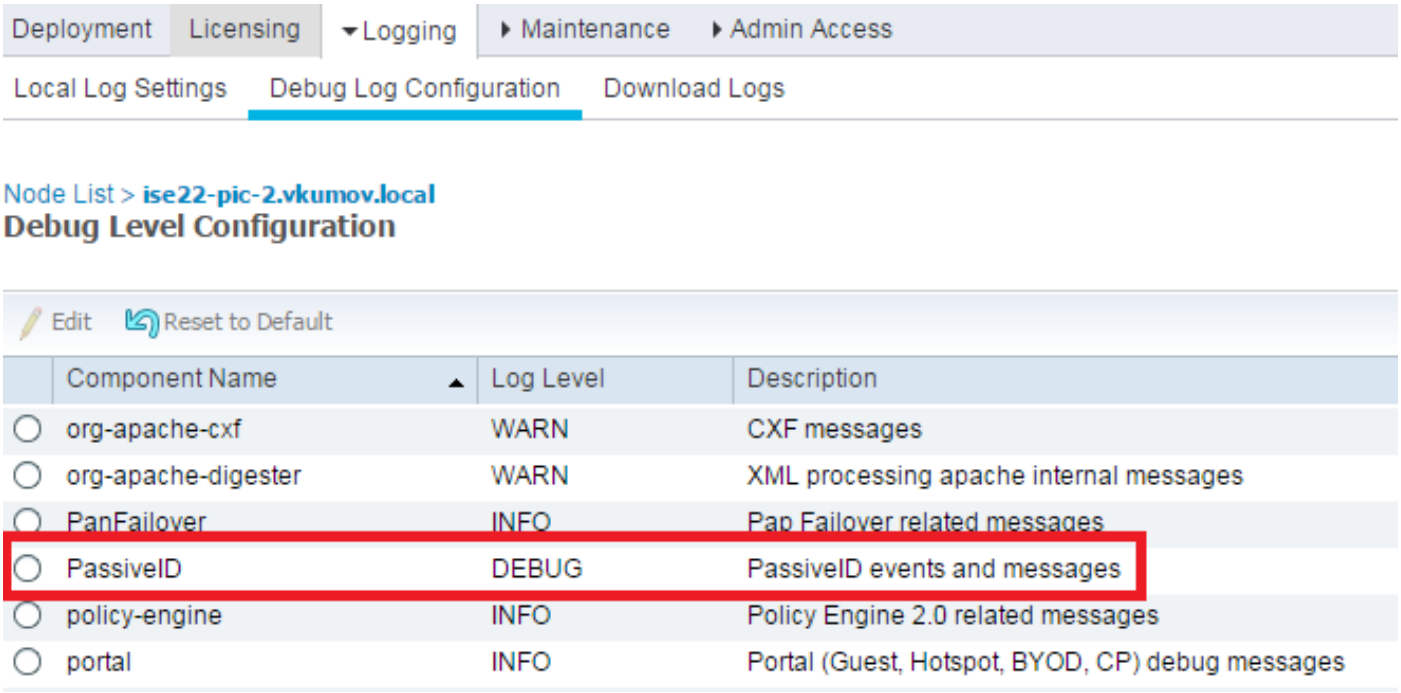
Acciones a tomar: marque el estatus de la aplicación en el nodo secundario, conectividad de red del control si todas las conexiones se permiten entre los Nodos.

Active Directory y WMI

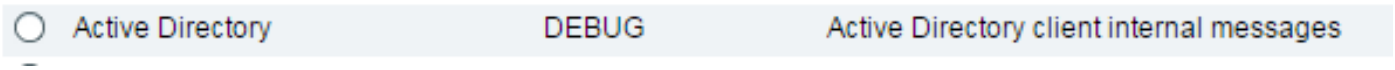
Para resolver problemas el Active Directory WMI mire en esos archivos:

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

Y los debugs útiles pueden habilitado en la **administración > la configuración del registro del registro > del debug**:



Y:



Aquí está un ejemplo de una nueva sesión docta de **passive-wmi.log** con los debugs habilitados:

```
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 ,

Ejemplo del control del punto final de **passive-endpoint.log** (en este caso el punto final era unreacheable del 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 =

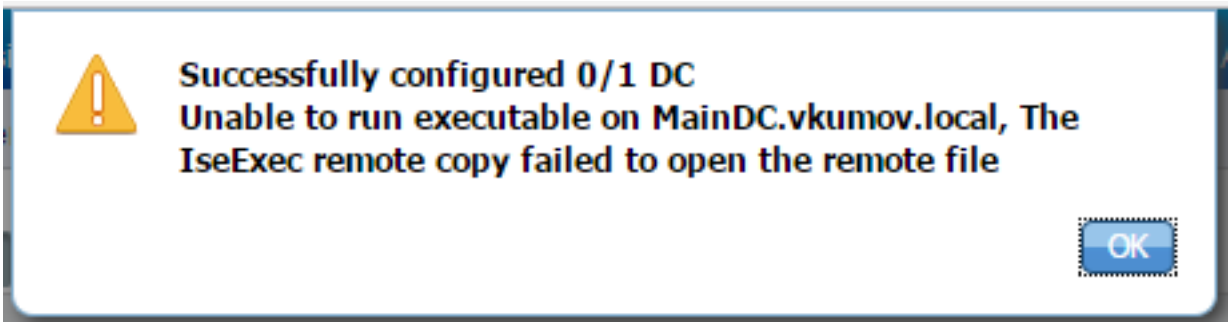
instance of __**InstanceCreationEvent**
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0,
76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0,
69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 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 ,

Problema frecuente: Tiros de la IMAGEN ISE "incapaces de ejecutar ejecutable en el name> <DC…" error

Si el usuario que se utiliza para unirse a la IMAGEN ISE al dominio no tiene bastantes permisos, la IMAGEN ISE lanza un error durante la configuración WMI:



Los debugs apropiados se pueden encontrar en el archivo de **ad_agent.log** (el nivel del registro del Active Directory se debe fijar PARA HACER EL DEBUG DE):

```
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
```

Acciones a tomar: Re-únase a los Nodos de la IMAGEN ISE al dominio con las credenciales del administrador de dominio o agregue al usuario para quien se utiliza se unen a la operación al grupo de *Admins del dominio* en el AD.