Configurar ISE 2.2 PIC com o fornecedor do diretório ativo WMI

Índice

Introdução

Este documento descreve como configurar e pesquisar defeitos o desenvolvimento passivo do conector da identidade do Identity Services Engine (ISE PIC) com o fornecedor de Windows Management Instrumentation do diretório ativo (AD WMI). O ISE PIC é uma versão de pouco peso ISE que se centre sobre características passivas ID.

O ISE PIC é uma única solução ID para todo o portfólio do Cisco Security que usa a identidade passiva somente. Significa que a autorização ou as políticas não podem ser configuradas em ISE

PIC. Apoia fornecedores diferentes (agentes, WMI, Syslog, API) e pode ser integrado através do RESTO API. Tem capacidades para perguntar valores-limite (é o usuário entrado? É o valor-limite ainda conectado?)

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Motor do serviço da identidade de Cisco
- Microsoft ative directory
- Microsoft WMI

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 2.2.0.470 passiva do conector da identidade do motor do serviço da identidade de Cisco
- Pacote de serviços 1 de Microsoft Windows 7
- R2 do Microsoft Windows server 2012

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

A quantidade máxima de Nós no desenvolvimento ISE PIC é 2. Este exemplo mostra como configurar o desenvolvimento ISE PIC para a Alta disponibilidade, SO2 que as máquinas virtuais (VM) são usadas. Em um desenvolvimento ISE PIC, os Nós podem ter papéis: Preliminar e secundário. Neste somente um nó pode ser preliminar em um momento e os papéis podem somente ser mudados manualmente com o GUI. Em caso da falha principal todas as características ainda são executado em secundário à exceção do UI. Somente a promoção manual a preliminar permite o UI.

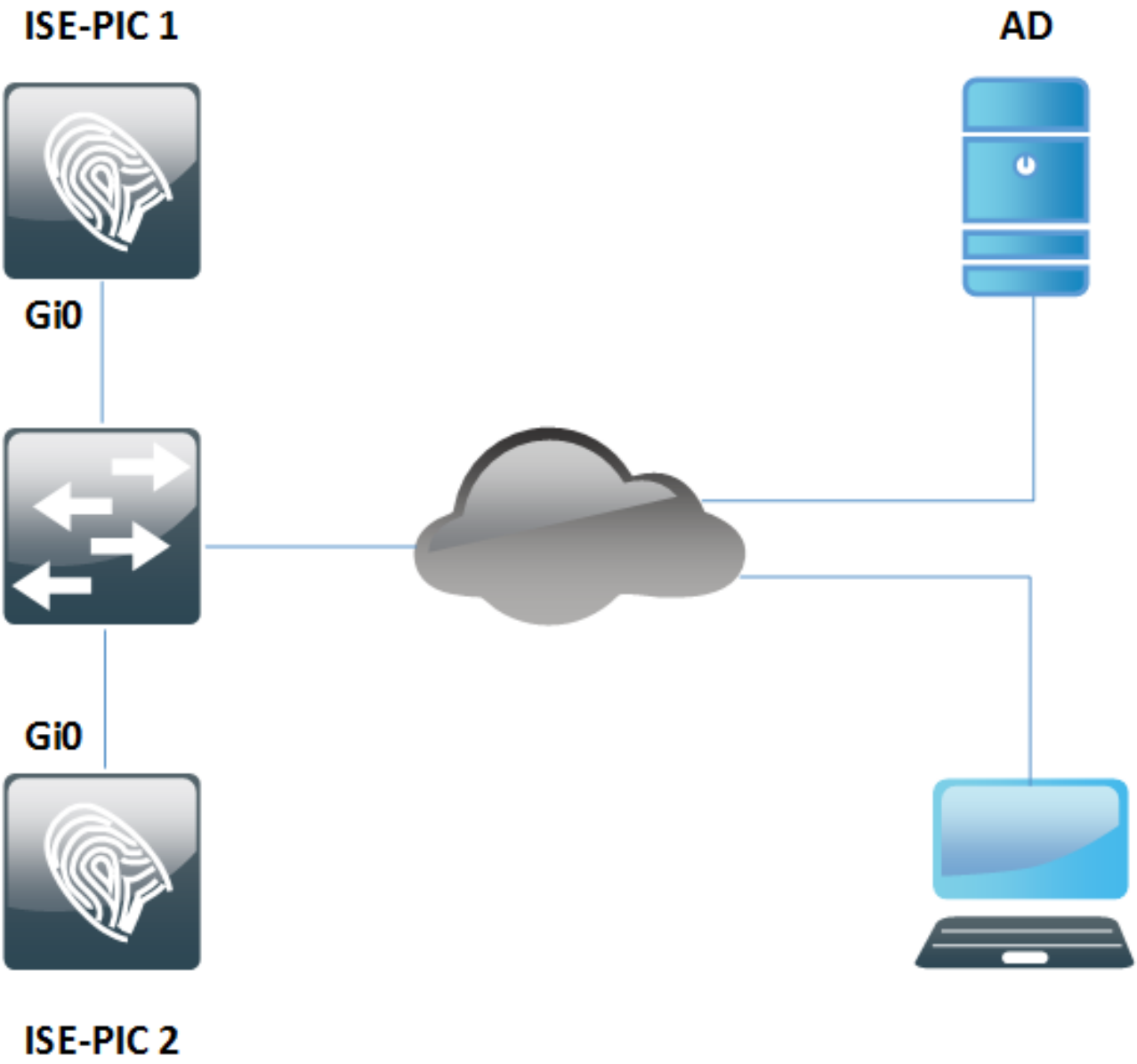
Este exemplo mostra como configurar o fornecedor WMI para o diretório ativo. WMI consiste em um grupo de Ramais ao modelo do driver do Windows que fornece uma relação do sistema operacional através de que proveu componentes fornecem a informação e a notificação. WMI é a aplicação de Microsoft dos padrões modelo com base na Web do gerenciamento corporativo (WBEM) e da informação comum (CIM) do grupo de trabalho distribuído do Gerenciamento (DMTF).

Nota: Mais informação sobre WMI pode ser encontrada no local de Microsoft do oficial:

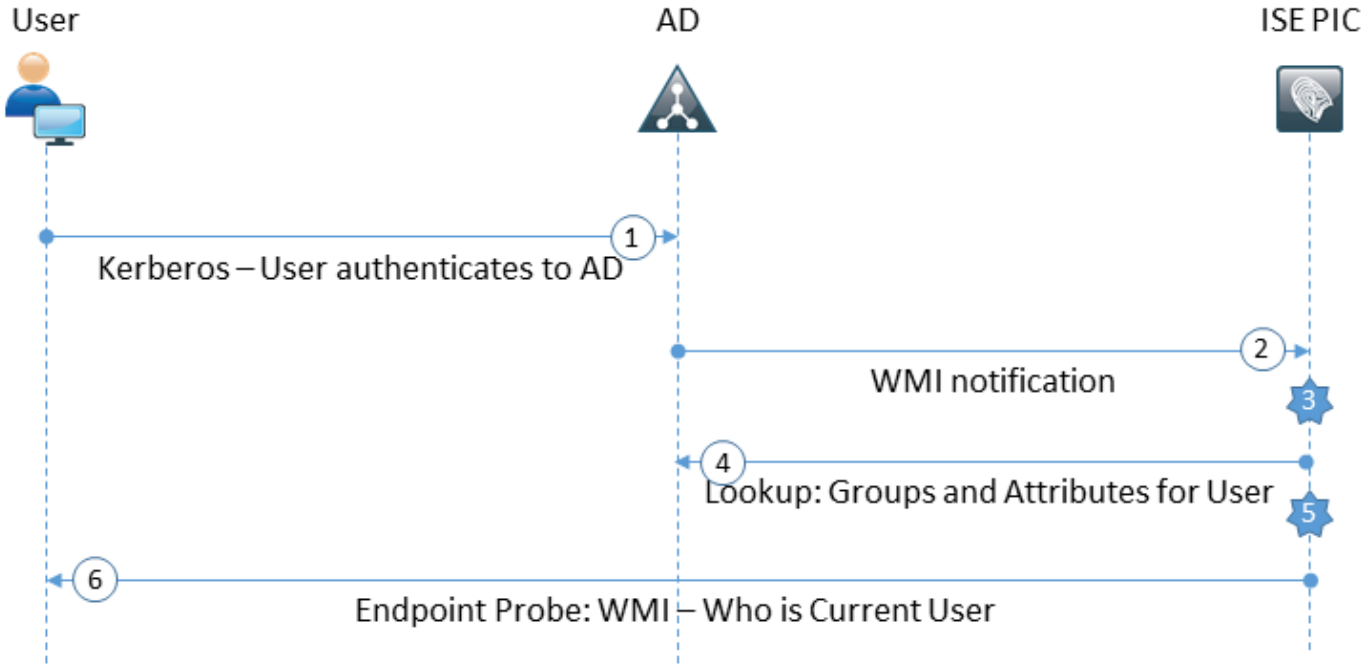
Sobre WMI

Diagrama de Rede

A informação no documento usa a instalação de rede mostrada na imagem:



Fluxo de trabalho



1. Entre ao PC e obtenha autenticado no AD.

2. WMI notifica ISE PIC sobre esta autenticação.

3. O ISE adiciona username obrigatório: IP_Address a seu diretório da sessão.

4. O ISE recupera os grupos e os atributos de usuário do AD.

5. O ISE salvar esta informação em seu diretório da sessão.

6. Cada 4 (não configuráveis) ISE PIC das corridas horas da ponta de prova do valor-limite: Primeiramente tenta WMI ao valor-limite.Se WMI falha então o ISE PIC executa ISEExec. Pergunta o valor-limite para o usuário e permite WMI pela próxima vez.Igualmente o ISE PIC recupera o MAC address do valor-limite e do tipo do OS.

   Em ISE PIC é possível permitir somente/pontas de prova valor-limite do desabilitação. O nó principal pergunta todos os valores-limite, nó secundário é para a Alta disponibilidade somente.

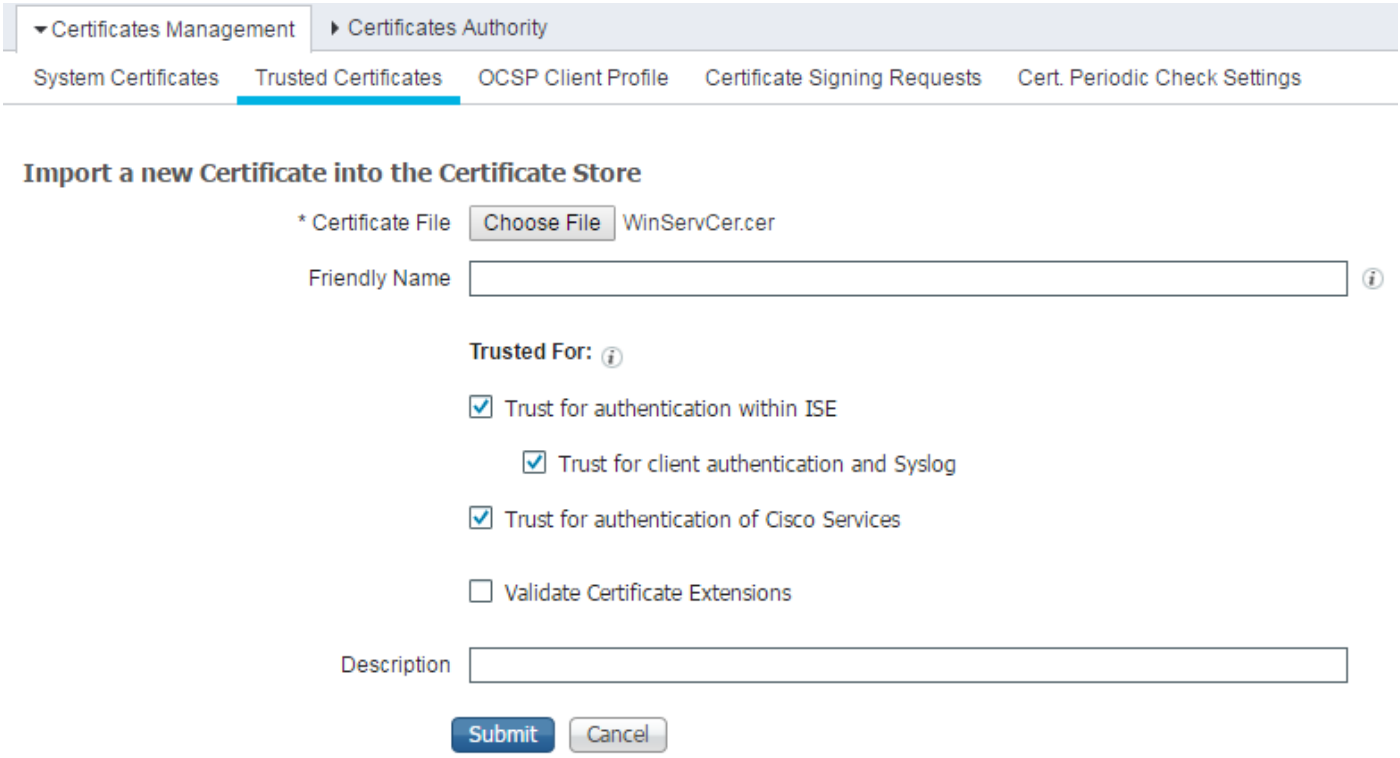
Configurar

Configurar o desenvolvimento ISE PIC

Etapa 1 (opcional). Instale certificados confiáveis.

A corrente completa dos Certificados de seu Certificate Authority (CA) deve ser instalada à loja confiada ISE. Entre a ISE PIC GUI e navegue aos **Certificados > ao Gerenciamento > aos certificados confiáveis de Certificados**. Clique a **importação** e selecione seu certificado de CA de seu PC.

Segundo as indicações da imagem, o clique **submete-se** para salvar mudanças. Repita esta etapa para todos os Certificados da corrente. Repita etapas no nó secundário também.

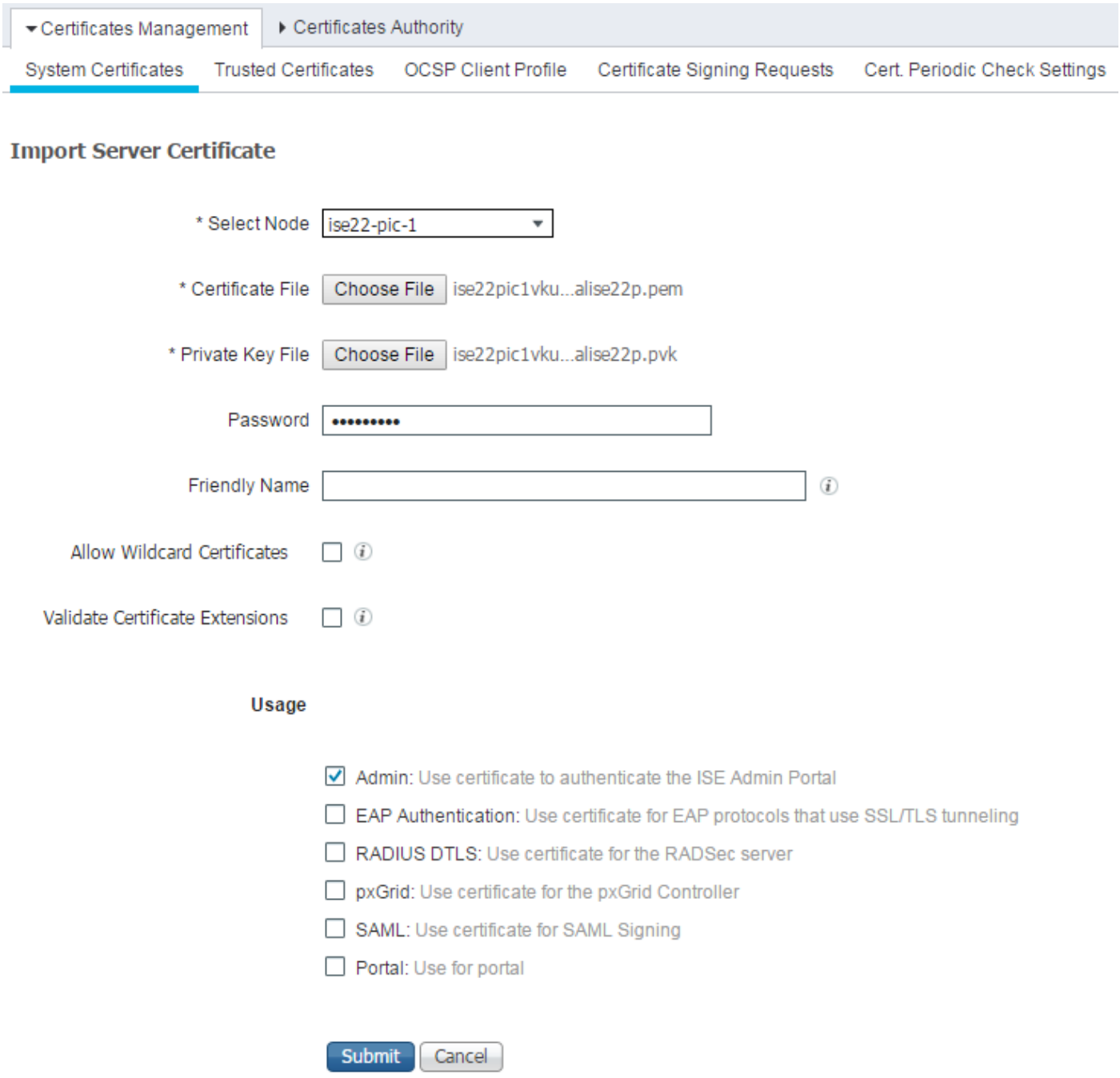


Etapa 2 (opcional). Instale Certificados do sistema.

Certificados da **opção 1.** já gerados por CA junto com a chave privada.

Navegue aos **Certificados dos Certificados > do Gerenciamento > do sistema de Certificados** e clique a **importação**. Selecione o **arquivo certificado** e o **arquivo-chave privado**, entra no campo de *senha* se a chave privada é cifrada.

Segundo as indicações das **opções de uso da** verificação da imagem:



Nota: Desde que o ISE PIC é baseado no código ISE e pode facilmente ser ISE FULL-caracterizado convertido com licenças apropriadas, todas as opções de uso estão disponíveis. Os papéis tais como a **autenticação de EAP**, o **RAIO DTL**, o **SAML** e o **portal** não são usados por ISE PIC.

O clique **submete-se** para instalar o certificado. Repita este procedimento em um nó secundário também.

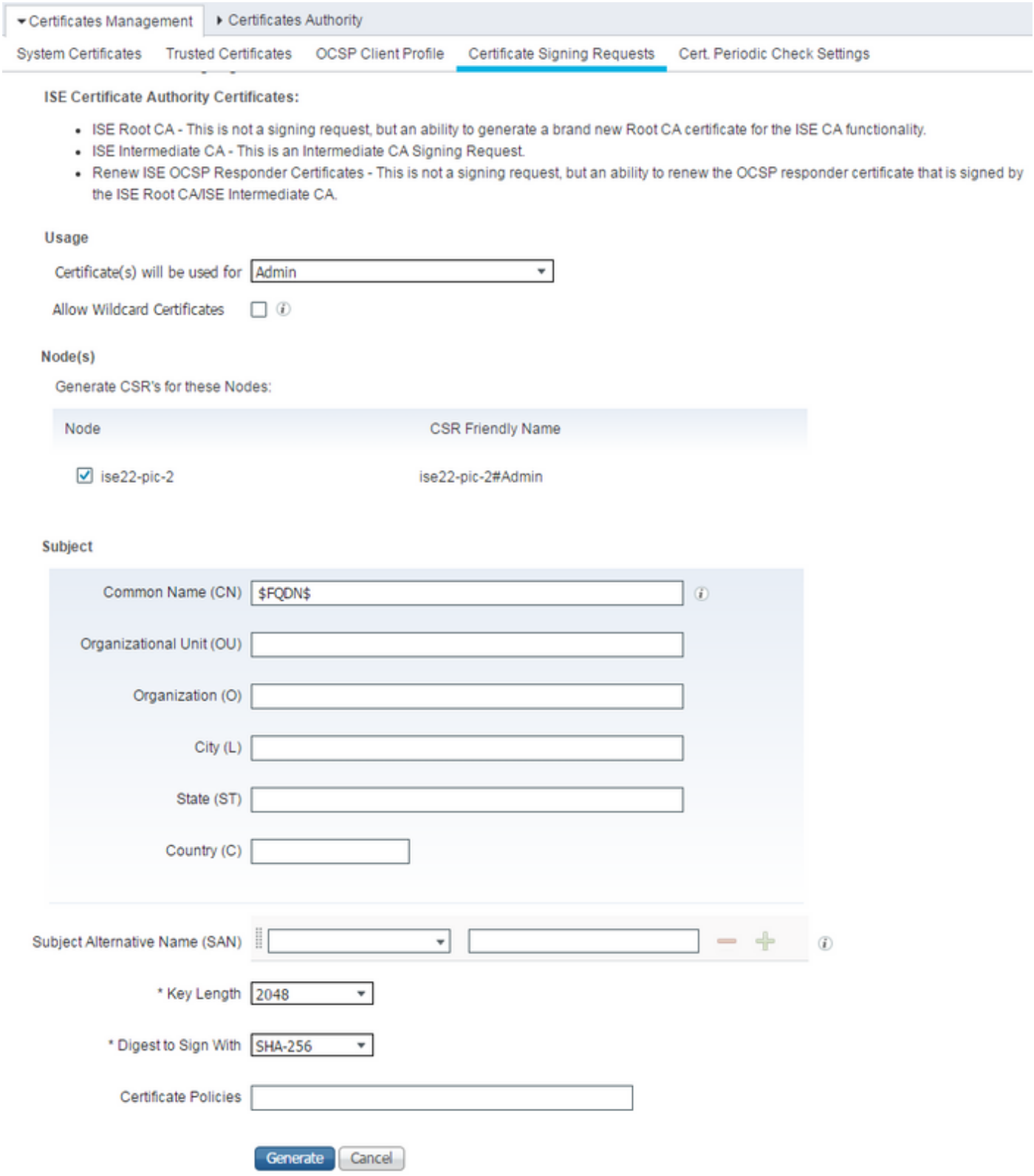
Nota: Todos os serviços no nó ISE PIC reiniciam depois que importação do certificado de servidor.

A opção 2. gerencie a solicitação de assinatura de certificado (CSR), assina-a com CA e liga-a no ISE.

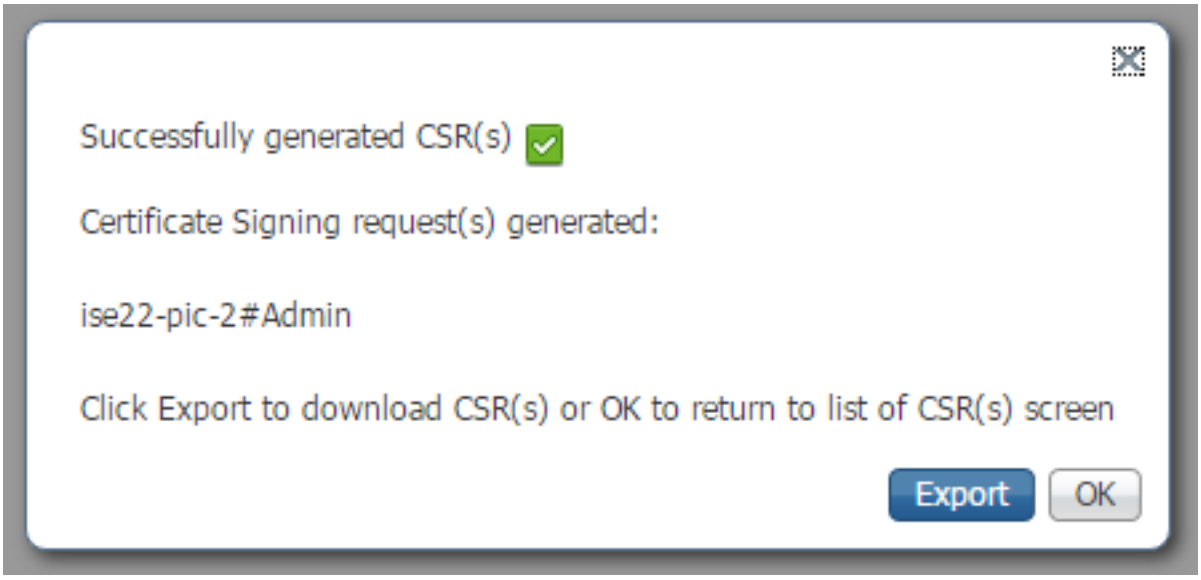
Navegue à página dos **Certificados > do Gerenciamento > das solicitações de assinatura de**

certificado de Certificados e o clique **gerencie as solicitações de assinatura de certificado (CSR)**.

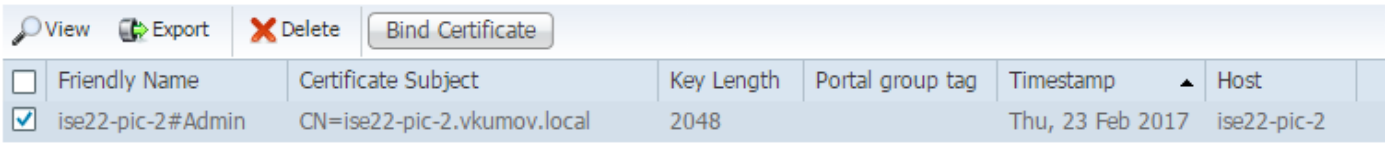
Selecione o nó e o uso, entra nos outros campos se for necessário:



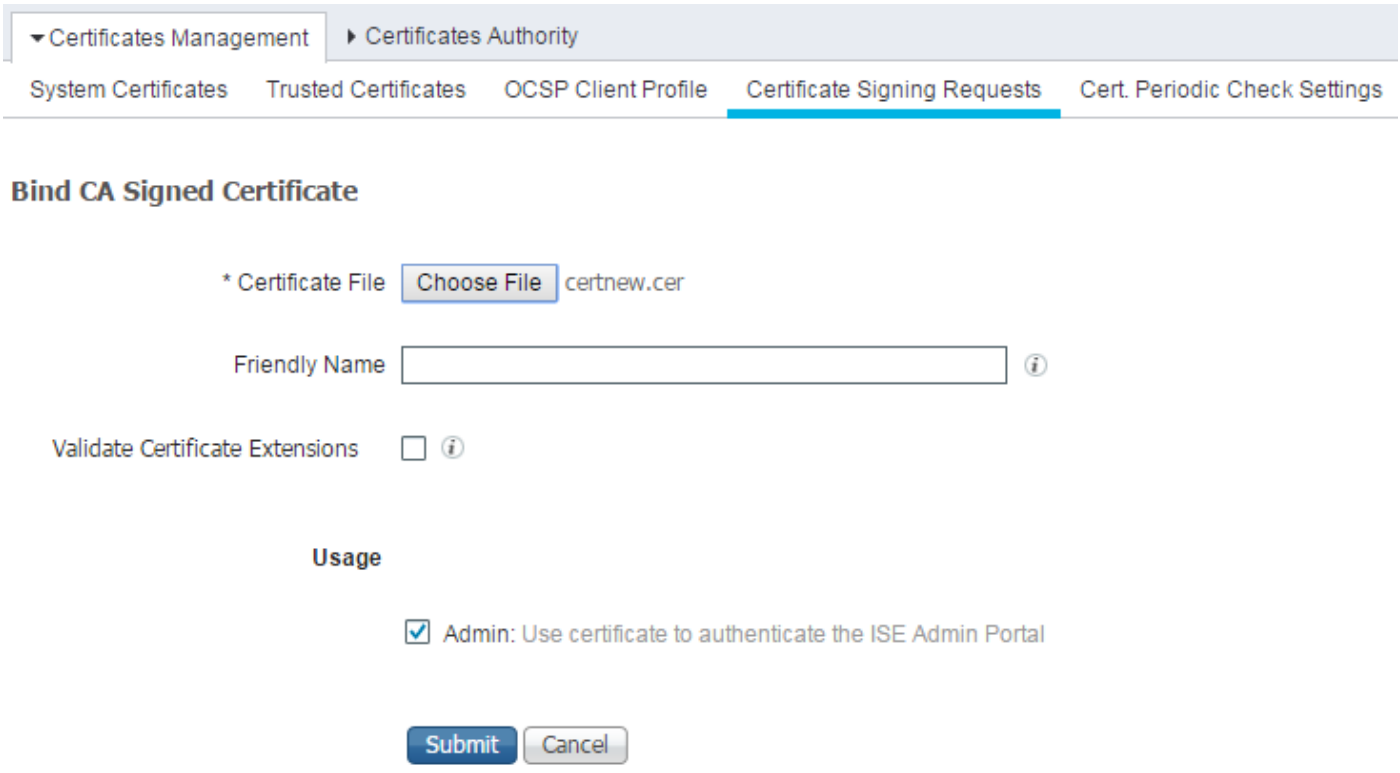
O clique **gerencie.** A nova janela estala acima com uma opção **para exportar o** CSR gerado:



Clique a **exportação,** salvar o arquivo gerado ***.pem** e assine-o com CA. Uma vez que o CSR é assinado navega de volta à página dos **Certificados > do Gerenciamento > das solicitações de assinatura de certificado de Certificados**, seleciona seu CSR e clique o **certificado do ligamento**:



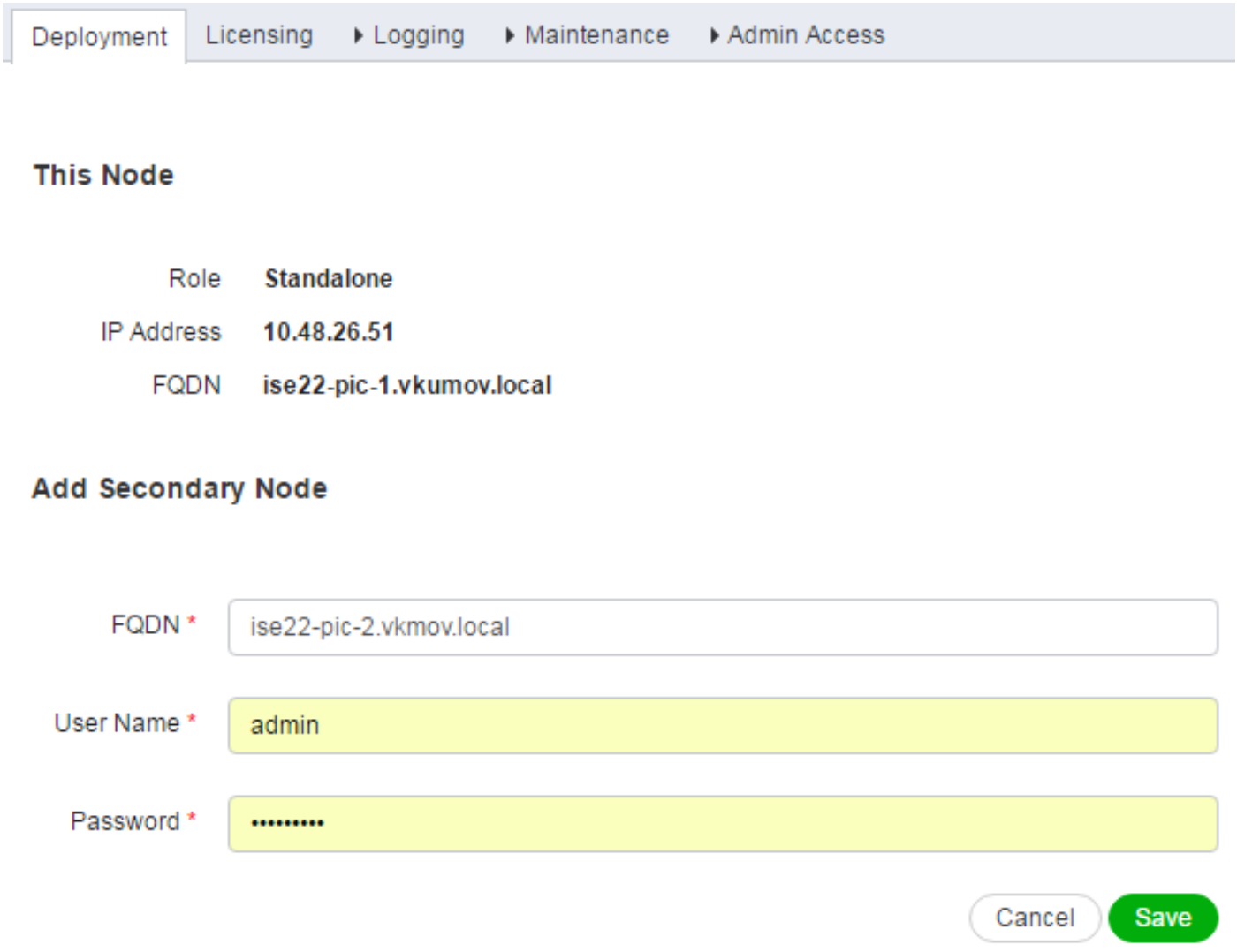
Selecione o certificado que foi assinado com seu CA e o clique **se submete** para aplicar mudanças:



Todos os serviços no reinício do nó ISE PIC depois que você clique **se submete** para instalar o certificado.

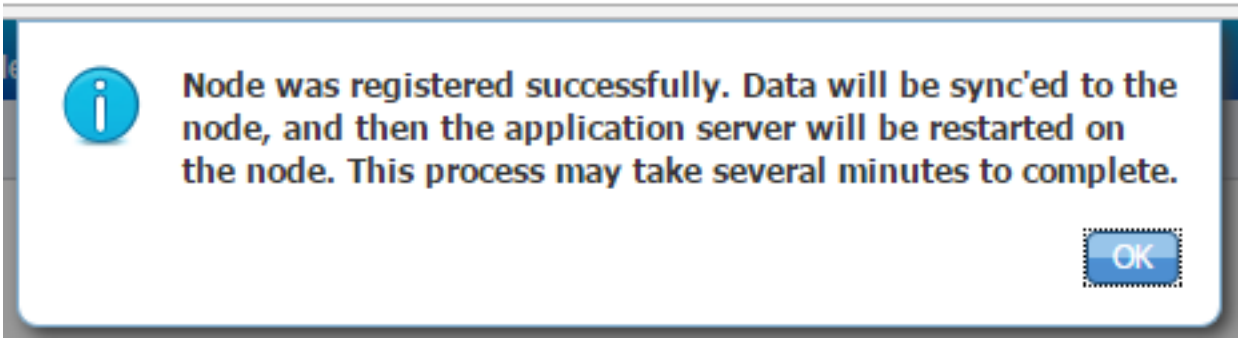
Etapa 3. Adicionar o nó secundário ao desenvolvimento.

O ISE PIC reserva ter 2 Nós em um desenvolvimento para a Alta disponibilidade. Não exige para ter uma confiança em dois sentidos dos Certificados (que comparam ao desenvolvimento usual ISE). A fim adicionar um nó secundário ao desenvolvimento, navegue à **página da administração > do desenvolvimento em** seu nó preliminar ISE PIC, segundo as indicações da imagem:

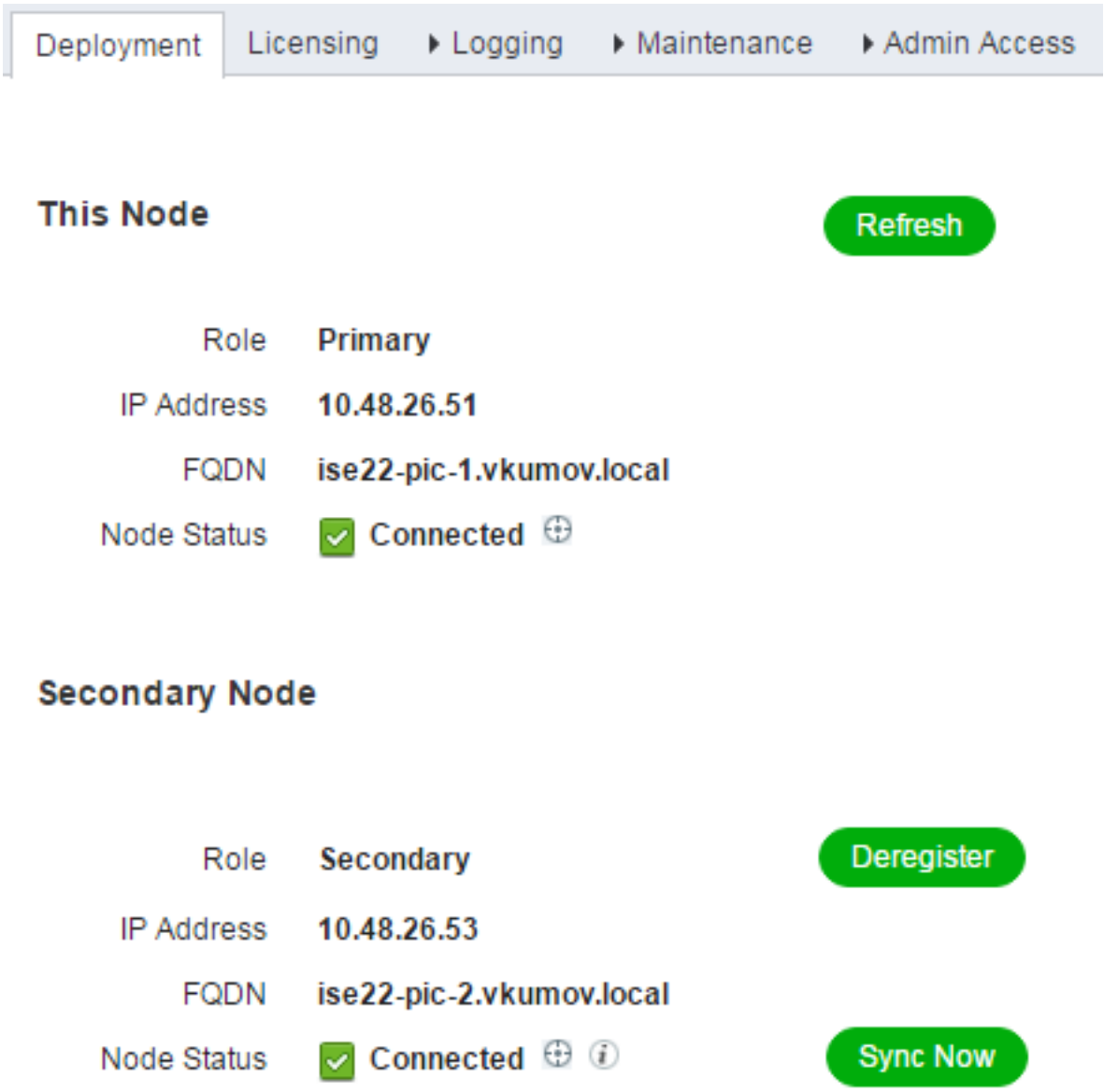


Incorpore o nome de domínio totalmente qualificado (FQDN) do nó secundário, credenciais do administrador dessa **salvaguarda do** nó e do clique. Caso que o nó preliminar ISE PIC não pode verificar o certificado admin do segundo nó pede a confirmação antes que instale que certificado na loja confiada.

Em tal **certificado de importação do** clique do caso **e continue** a fim juntar-se ao nó ao desenvolvimento. Você deve obter uma notificação que o nó está adicionado com sucesso. Todos os serviços nos reinícios secundários do nó.



Dentro de 10-20 Nós dos minutos deve ser sincronizado e o estado do nó deve mudar de **em andamento** ao conectado:



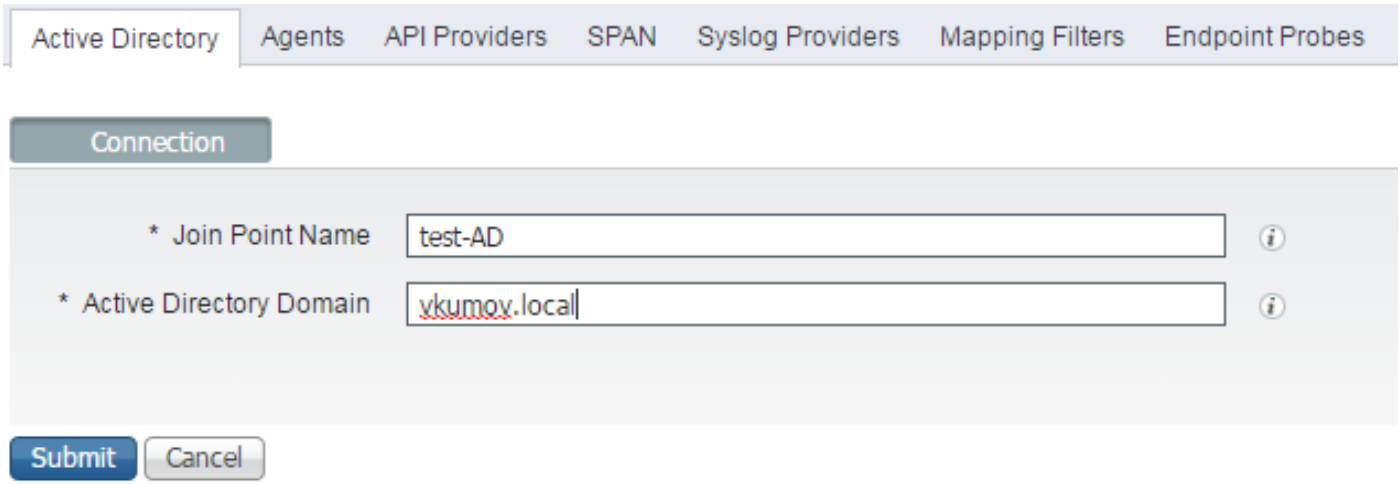
Configurar fornecedores do diretório ativo

O ISE PIC usa Windows Management Instrumentation (WMI) para recolher a informação sobre sessões do AD e atos como um communitation do bar/sub, que signifique:

- O ISE PIC subscreve a determinados eventos
- WMI alerta ISE PIC quando aqueles eventos ocorrem: 4768 (o Kerberos Ticket a concessão) e 4770 (o Kerberos Ticket a renovação)As entradas no diretório da sessão expiram (a remoção)

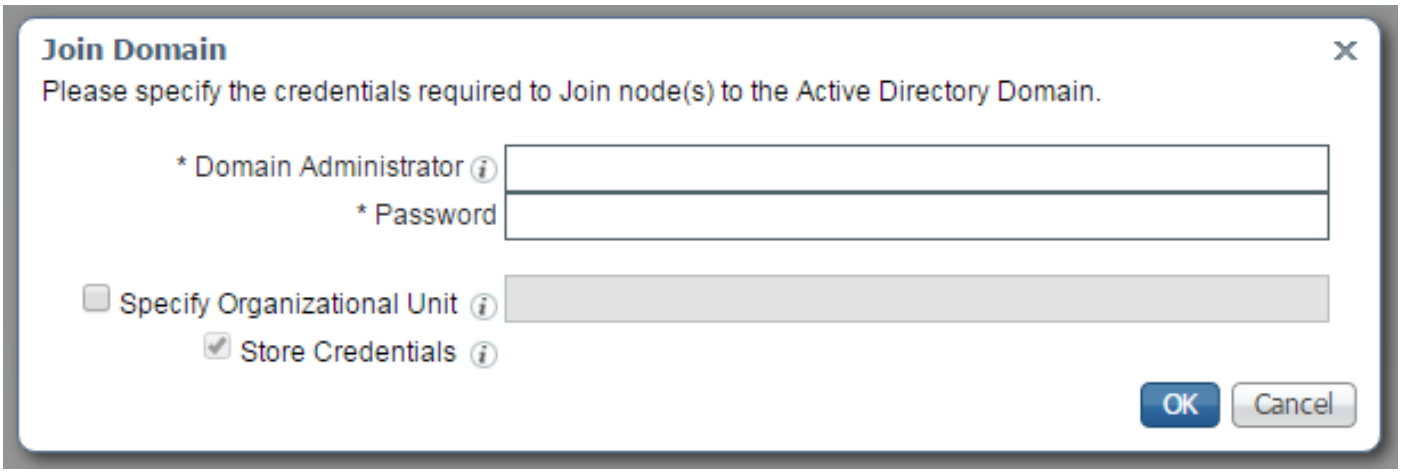
Etapa 1. Junte-se a ISE PIC ao domínio.

A fim juntar-se a ISE PIC ao domínio, para navegar aos **fornecedores > ao diretório ativo** e ao clique **adicionar**:



A suficiência **junta-se ao nome do ponto** e os campos e o clique do **domínio do diretório ativo submetem-se** para salvar mudanças. **Junte-se ao nome do ponto** é um nome que seja usado em ISE PIC somente. **O domínio do diretório ativo** é o nome do domínio onde o ISE PIC deve ser juntado e deve ser solucionável com o servidor DNS configurado em ISE PIC.

Depois que a criação do ponto ISE PIC Join deve lhe perguntar se você gostaria de se juntar a Nós ao domínio. Clique em Sim. Um indicador deve estalar acima para que você forneça credenciais para juntar-se ao domínio:



Encha campos do **administrador de domínio** e de **senha** e clique a **APROVAÇÃO.**

Mesmo que o campo seja chamado **administrador de domínio** não é necessário usar o usuário do administrador **para juntar-se a** ISE PIC ao domínio. Este usuário deve ter privilégios suficientes criar e remover contas de máquina no domínio, ou altere as senhas para contas de máquina previamente criadas. As permissões da conta de diretório ativo exigidas executando várias operações podem ser encontradas neste documento.

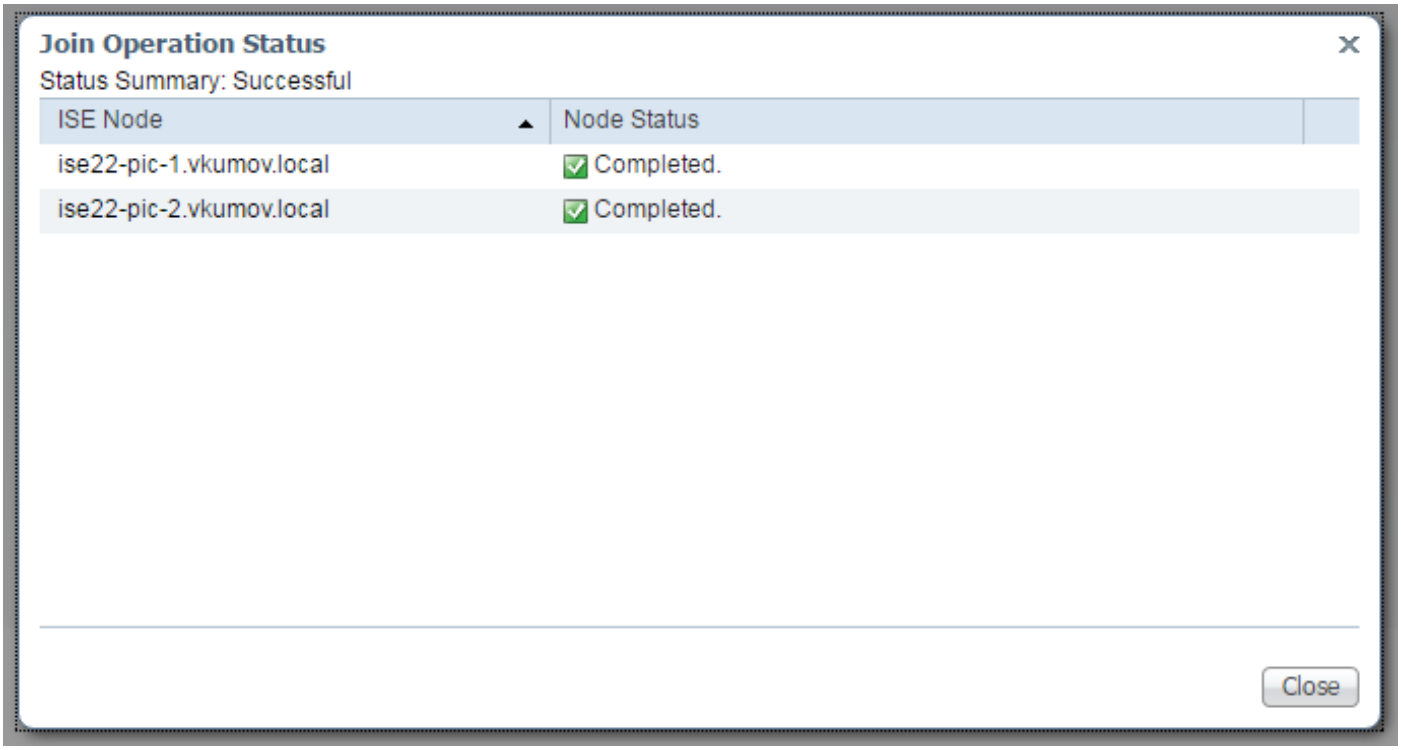
Contudo é administrador de domínio que do uso do requiredto as credenciais durante se juntam se você gostaria de usar WMI. A opção da **configuração WMI** exige:

- Mudanças de registro
- Permissões usar o DCOM

- Permissões usar remotamente WMI
- Alcance para ler o log de evento de segurança do domínio Controlle AD
- O Windows Firewall deve permitir o tráfego desde/até ISE PIC (as políticas correspondentes do Windows Firewall serão criadas durante a **configuração WMI**)

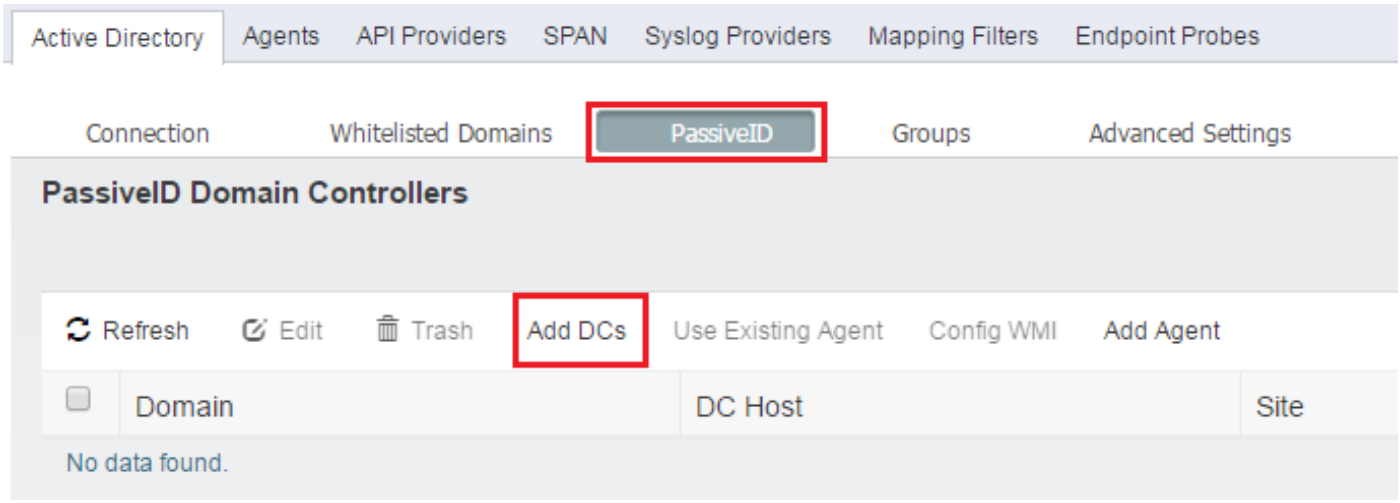
  Nota: As credenciais da loja são sejam permitidas sempre em ISE PIC desde que se exige para pontas de prova do valor-limite e configuração WMI. O ISE armazena-os cifrou internamente.

Segundo as indicações da imagem, o ISE PIC mostra o resultado da operação em uma nova janela:



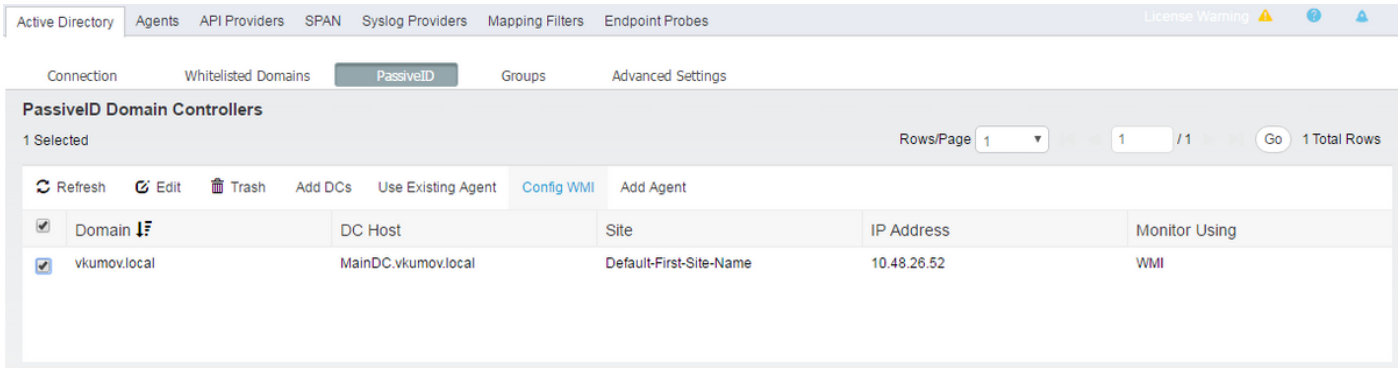
Etapa 2. Adicionar agentes de PassiveID.

Na página do domínio AD navegue à aba de PassiveID e o clique **adiciona DC**, segundo as indicações da imagem:

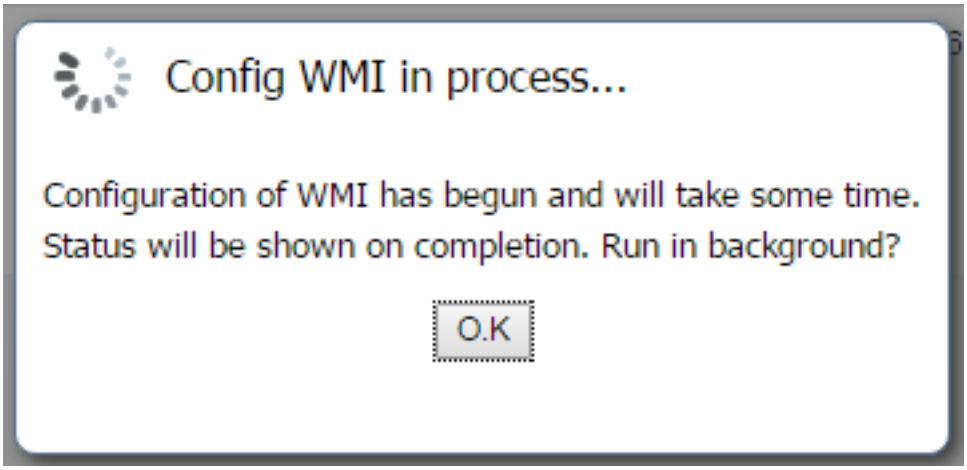


Uma nova janela estala acima e o ISE carrega uma lista de todos os controladores de domínio disponíveis. Selecione os DC onde você gostaria de configurar WMI e clicar a **APROVAÇÃO** para salvar mudanças, segundo as indicações da imagem:

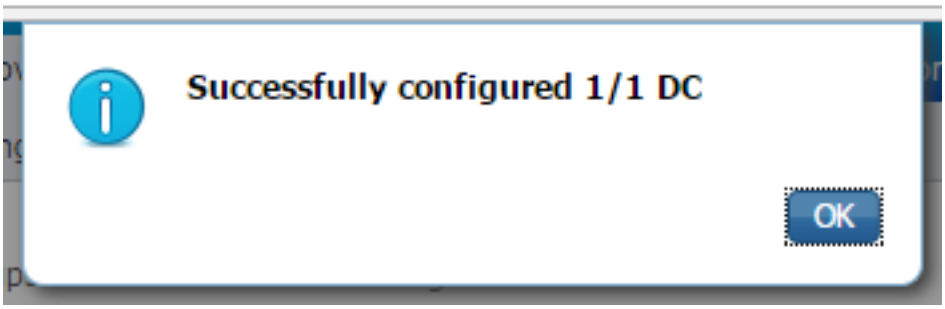
Os DC selecionados são adicionados à lista de **controladores de domínio de PassiveID.** Selecione seus DC e clique o botão da **configuração WMI**:



O ISE PIC mostra a uma mensagem que o processo de configuração é em andamento:



Depois que o par de minutos ele lhe mostra uma mensagem que WMI está configurado com sucesso em DC selecionados:



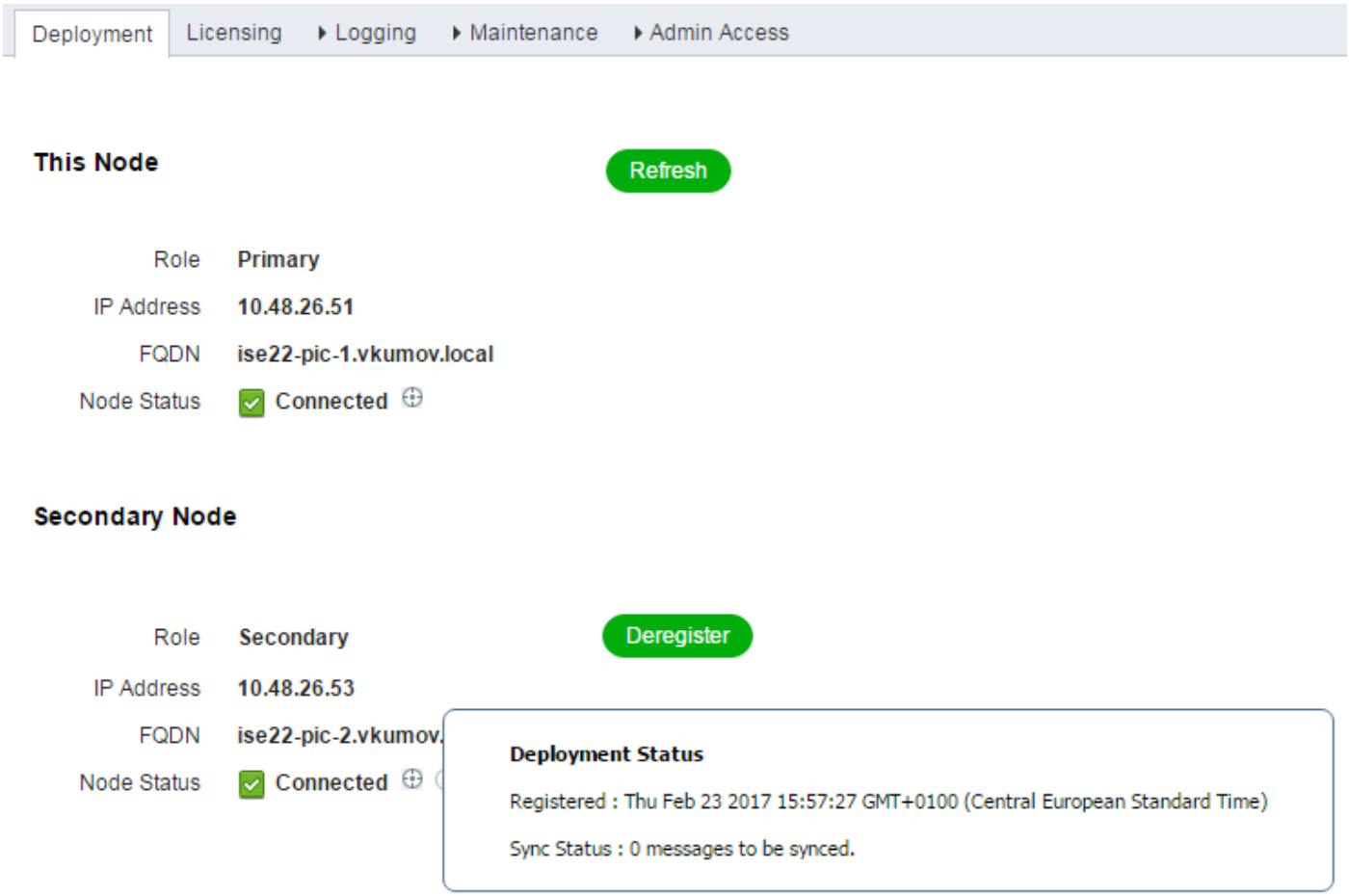
Verificar

Desenvolvimento

O estado do desenvolvimento pode ser verificado dentro algumas das maneiras:

Página do desenvolvimento

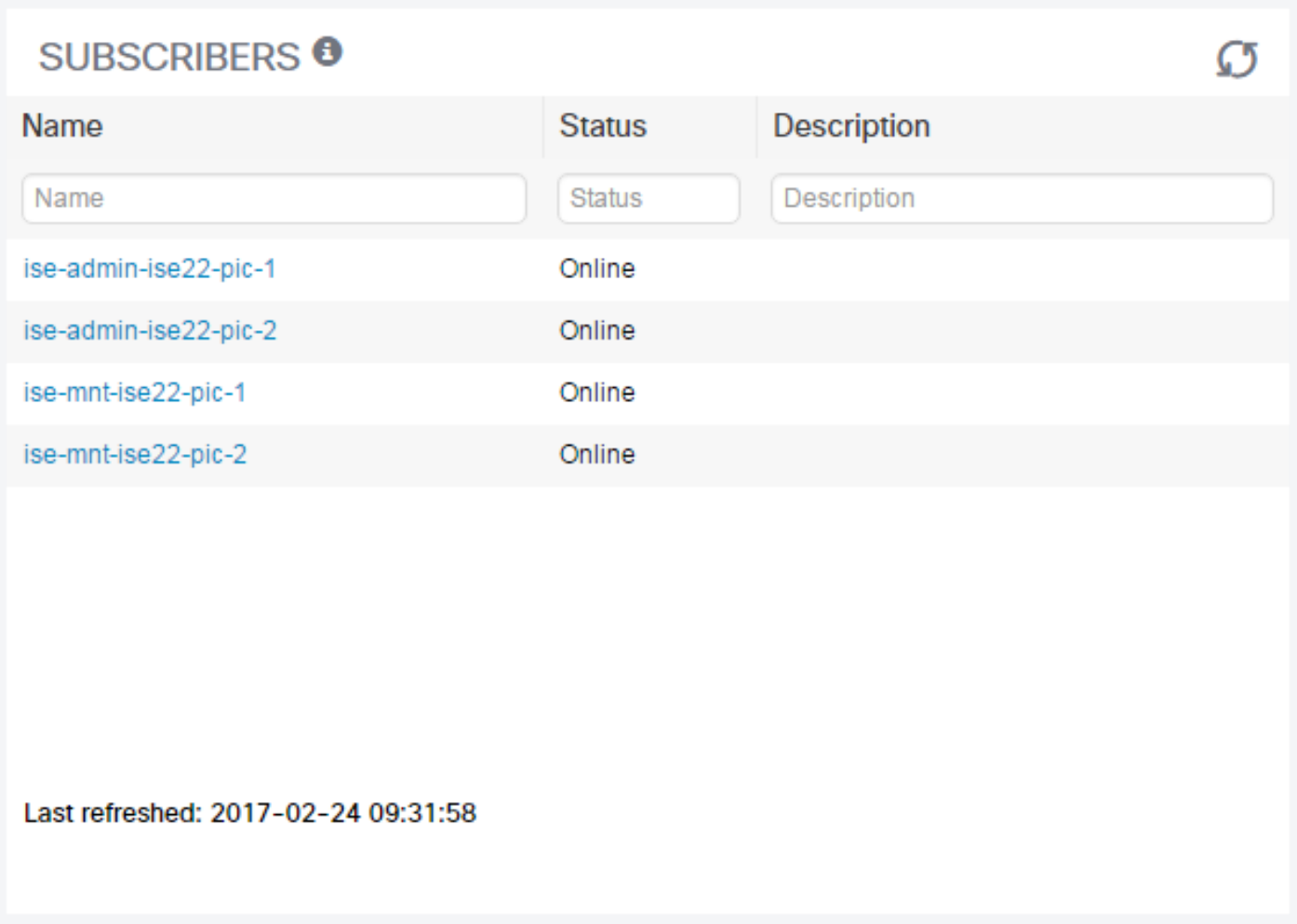
Navegue à **página que da administração > do desenvolvimento o** estado atual do desenvolvimento pode ser verificado:



Desta página o nó secundário pode de registro desfeito/cancelado se necessário. A sincronização manual pode ser começada e o **status de sincronização** pode ser verificado.

Página do painel

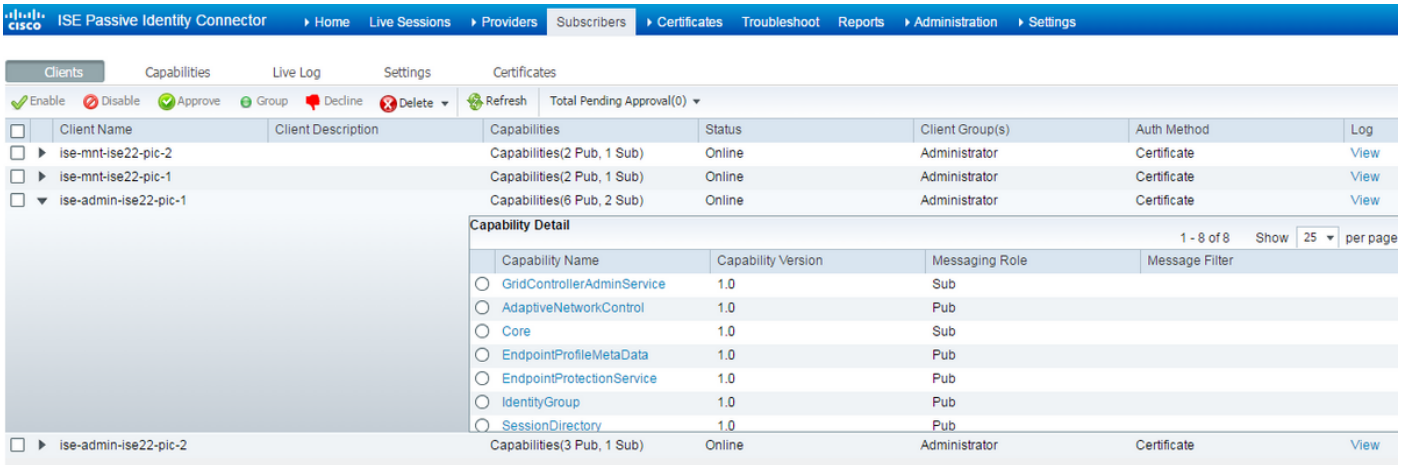
Em uma página principal ISE PIC há um dashlet chamado **Assinantes**. Com este dashlet você pode verificar o status atual de seus Nós ISE PIC, segundo as indicações da imagem:



O ISE PIC cria 2 assinantes para cada nó - **admin** e **MNT.** Todo devem estar no **status on-line** que significa que os Nós são reacheable e operacionais.

Assinantes

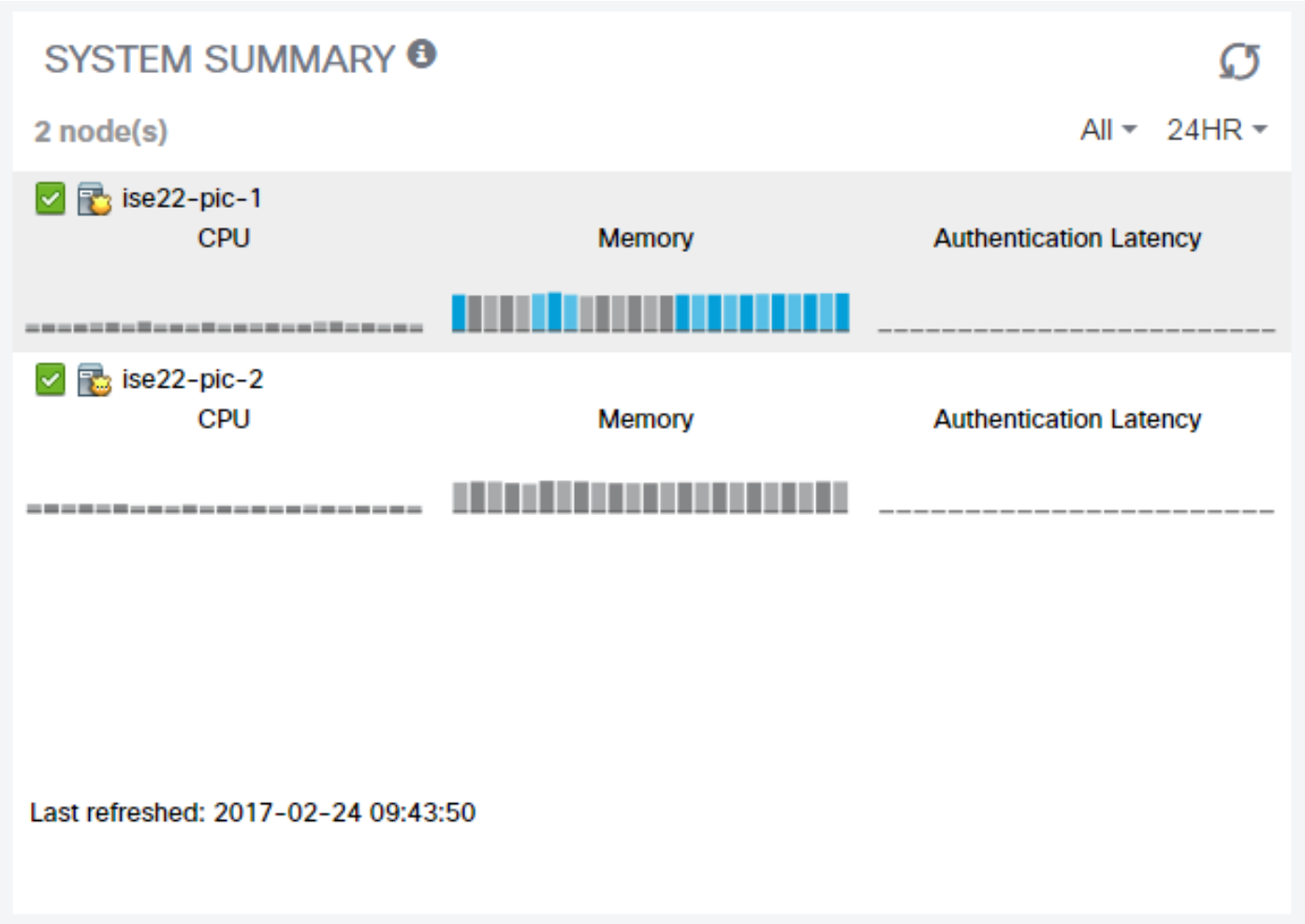
Os assinantes paginam são uma versão estendida do dashlet dos assinantes do Home Page de ISE PIC. Esta página mostra todo o pxGrid relativo, porém o estado de Nós ISE PIC pode ser verificado aqui também:



Sumário do sistema

O ISE PIC reserva monitorar também o sumário da saúde dos Nós. Este dashlet pode ser

encontrado em casa **> painel > adicional**:

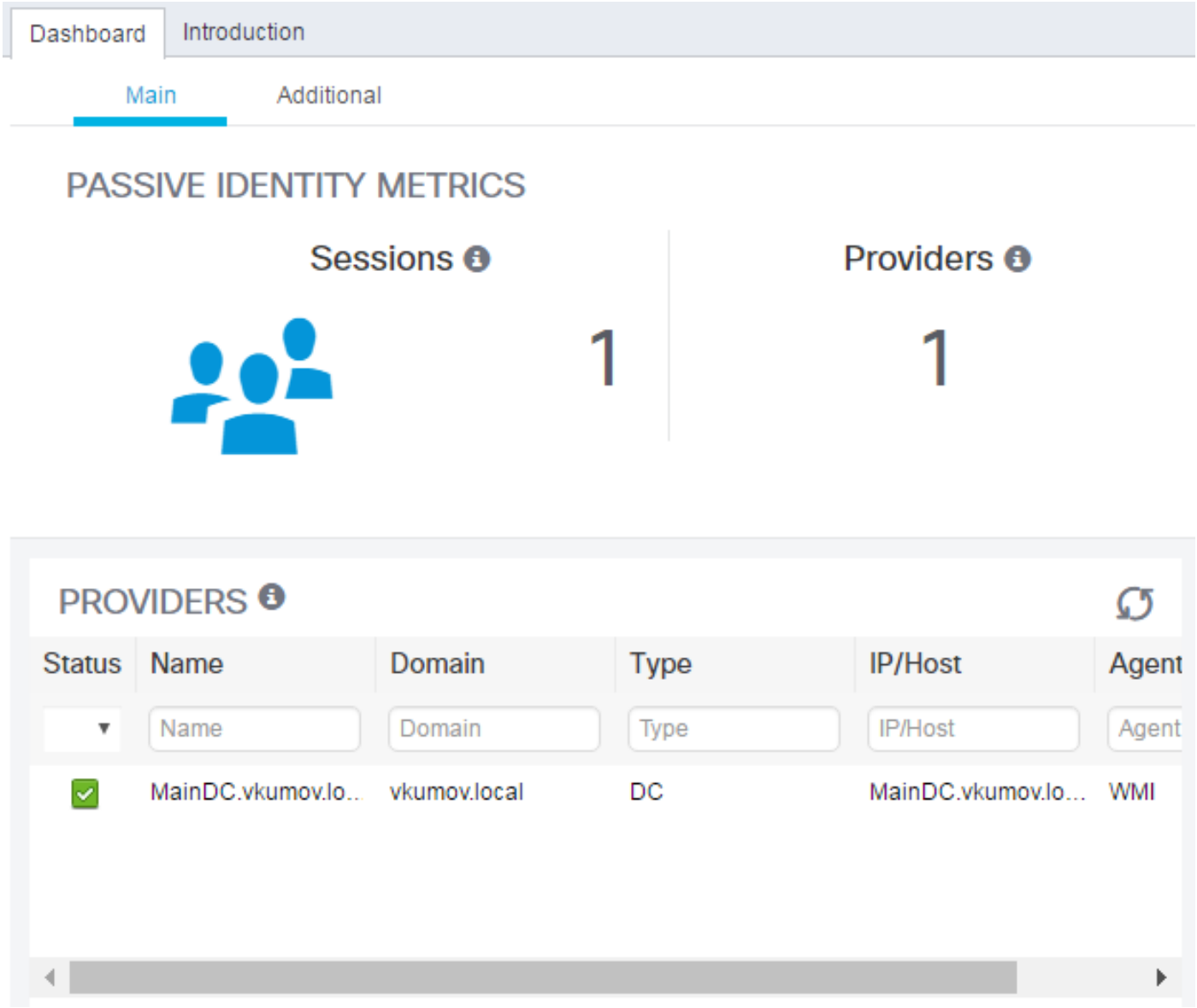


A latência da autenticação é sempre 0ms desde que o ISE PIC não executa nenhumas autenticações/autorizações.

Fornecedores e sessões

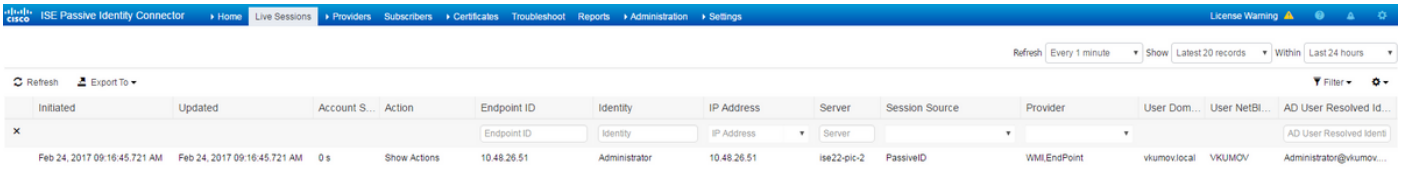
Home Page

Os estados dos fornecedores, sua quantidade e uma quantidade de sessões encontradas podem ser verificados quando você navegar **para dirigir > página do painel**:



Sessões vivas

A informação detalhada sobre toda encontrou que sessões de usuários podem ser encontrados na página das **sessões Live**:



Contém tal informação como:

- Fornecedor - que fornecedores foram usados para identificar esta sessão
- Iniciado e actualizado - timestamps em que a sessão é iniciada e atualizada em conformidade
- Endereço IP de Um ou Mais Servidores Cisco ICM NT - o endereço do valor-limite
- A ação - as ações que o ISE pode executar (por exemplo, estado do valor-limite da

verificação, ou se o ISE O PIC é integrado com pxGrid a seguir envia um pedido cancelar a sessão)

Troubleshooting

Desenvolvimento

Para pesquisar defeitos edições do desenvolvimento e do repliaction, olhe naqueles arquivos de registro:

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

A fim permitir debuga, navegam à **administração > registrando > debugam a configuração do log**:

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

Estes debugam são escritos ao arquivo de **replication.log**. Está aqui um exemplo de um processo de replicação 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]

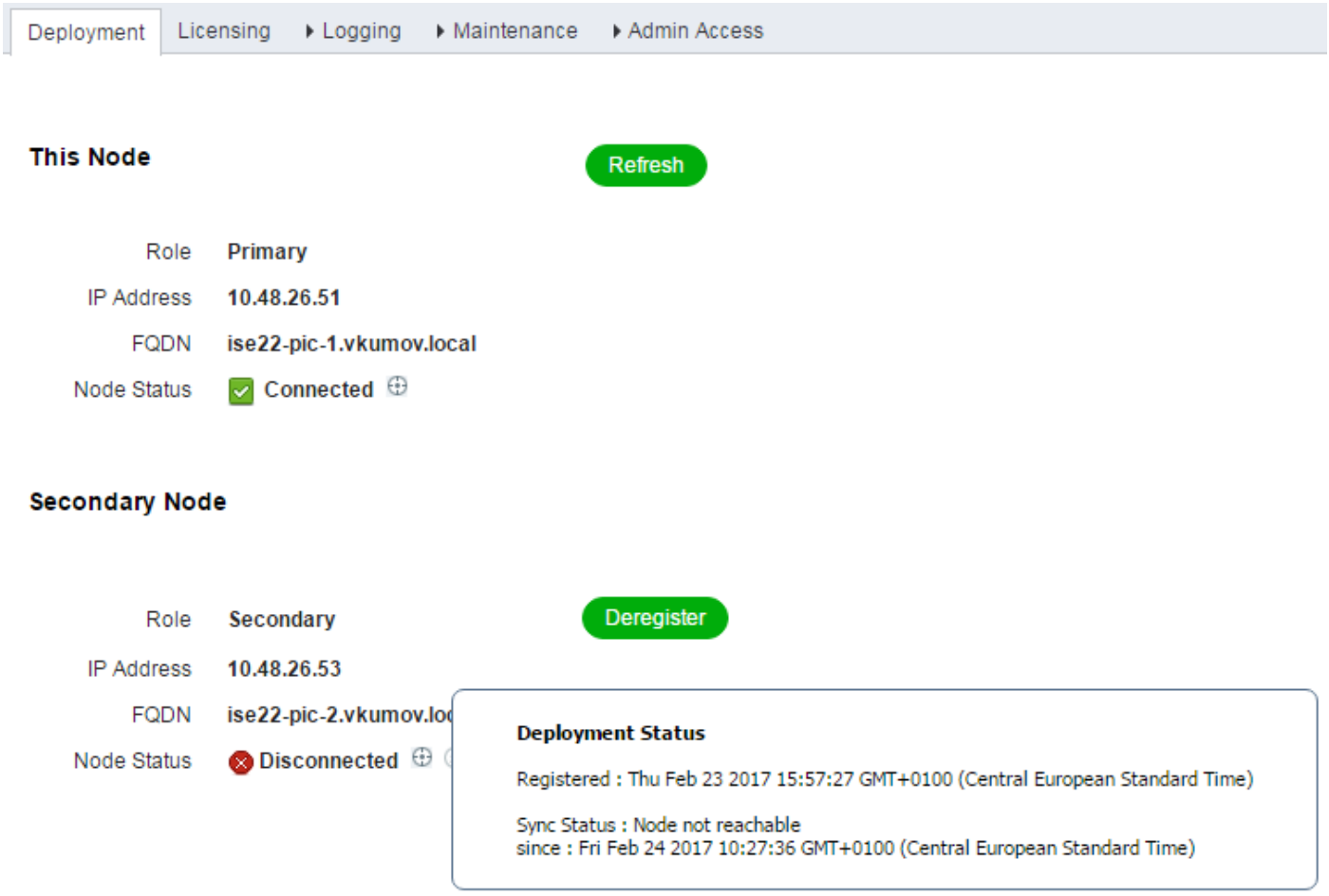
Uma mensagem de **ise-psc.log**:

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 comum: o nó secundário não é reacheable

Se o nó secundário se torna unreacheable estaria indicado na **página da administração > do desenvolvimento**:



ise-psc.log contém esta mensagem:

```
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
```

Esta mensagem explica o que não é reacheable, por exemplo o nó não responde para sibilar:

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

Ações a tomar: verifique se FQDN do nó socandary for solucionável, verifique a conectividade de rede básica entre Nós.

Caso que os aplicativos não estão no estado de execução no nó secundário ou há um Firewall entre Nós, **ise-psc.log** pode mostrar aquelas mensagens:

```
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
```

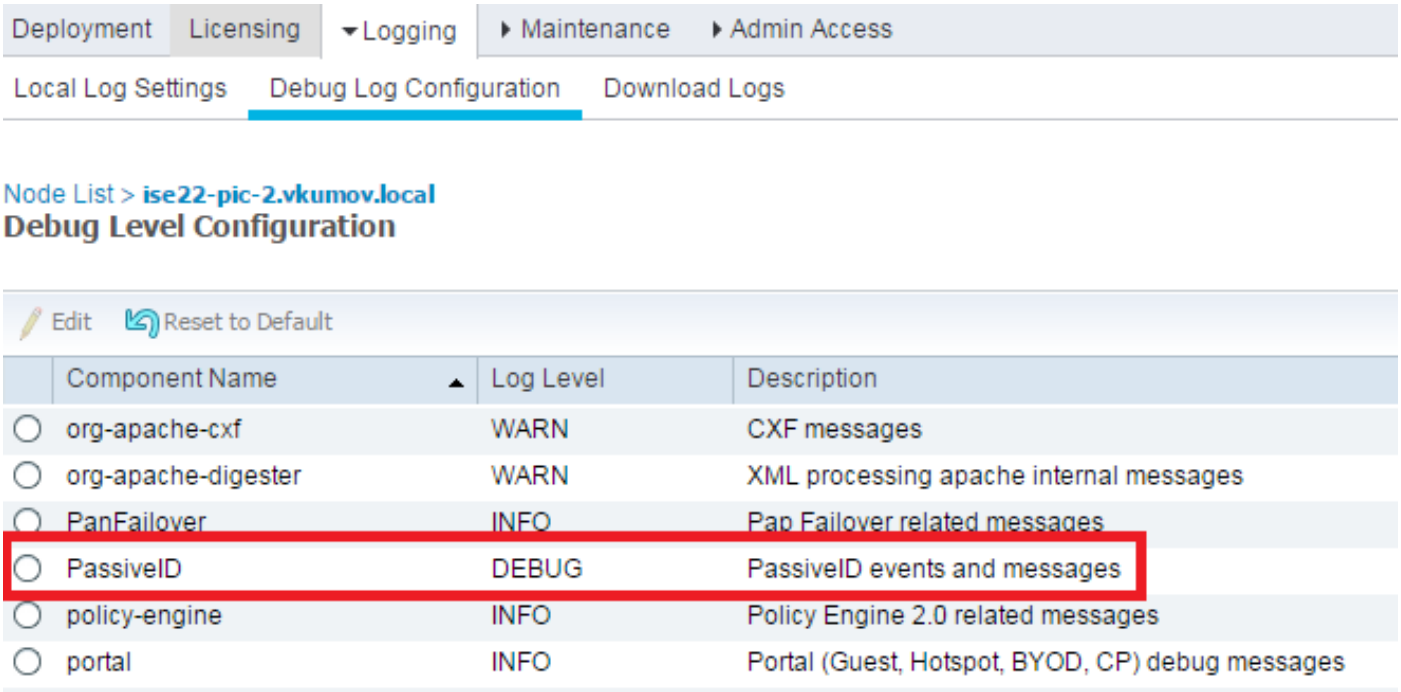
Ações a tomar: verifique o estado do aplicativo no nó secundário, verifique a conectividade de rede se todas as conexões são permitidas entre Nós.

Diretório ativo e WMI

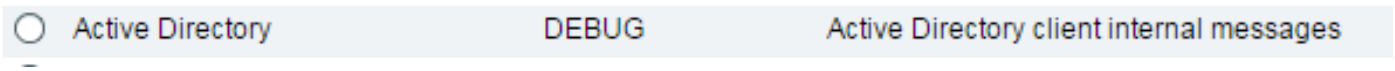
Para pesquisar defeitos o diretório ativo WMI olhe naqueles arquivos:

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

E o útil debuga pode permitido na **administração > registrando > para debugar a configuração do log**:



E:



Está aqui um exemplo de uma sessão instruída nova de **passive-wmi.log** com debuga permitido:

```
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 ,
```

Exemplo da verificação do valor-limite de passive-endpoint.log (neste caso o valor-limite era unreacheable do 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
{
```

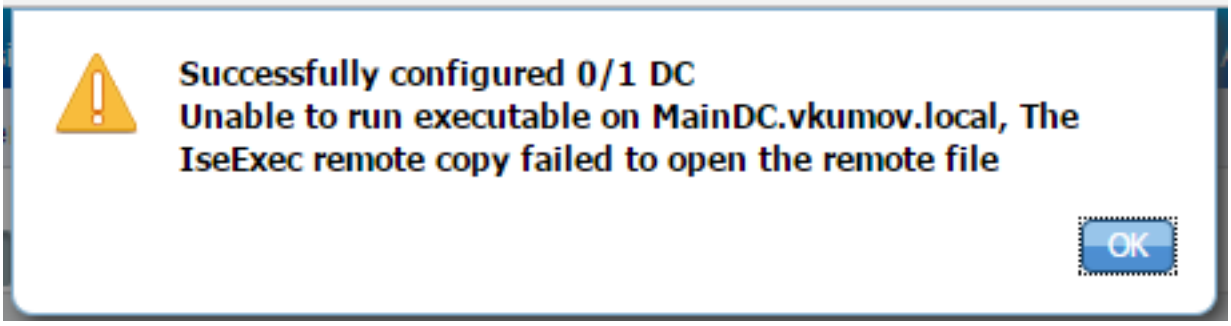
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0,
76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0,
69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2,
0, 0, 0, 0, 0, 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 comum: Lances ISE PIC “incapazes de executar executável no name> <DC…” erro

Se o usuário que está usado para se juntar a ISE PIC ao domínio não tem bastante permissões, o ISE PIC joga um erro durante a configuração WMI:



Apropriado debuga pode ser encontrado no arquivo de **ad_agent.log** (o nível do log do diretório ativo deve ser ajustado PARA DEBUGAR):

```
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
```

Ações a tomar: Re-junte-se a Nós ISE PIC ao domínio com credenciais do administrador de domínio ou adicionar-se o usuário que é usado para se juntam à operação ao grupo de *Admins do domínio no* AD.