

Configurar ISE 2.2 PIC com o fornecedor do diretório ativo WMI

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Fluxo de trabalho](#)

[Configurar](#)

[Configurar o desenvolvimento ISE PIC](#)

[Etapa 1 \(opcional\). Instale certificados confiáveis.](#)

[Etapa 2 \(opcional\). Instale Certificados do sistema.](#)

[Etapa 3. Adicionar o nó secundário ao desenvolvimento.](#)

[Configurar fornecedores do diretório ativo](#)

[Etapa 1. Junte-se a ISE PIC ao domínio.](#)

[Etapa 2. Adicionar agentes de PassiveID.](#)

[Verificar](#)

[Desenvolvimento](#)

[Página do desenvolvimento](#)

[Página do painel](#)

[Assinantes](#)

[Sumário do sistema](#)

[Fornecedores e sessões](#)

[Home Page](#)

[Sessões vivas](#)

[Troubleshooting](#)

[Desenvolvimento](#)

[Problema comum: o nó secundário não é reacheable](#)

[Diretório ativo e WMI](#)

[Problema comum: O ISE PIC joga “incapaz de executar executável em ...” erro](#)

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 active 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

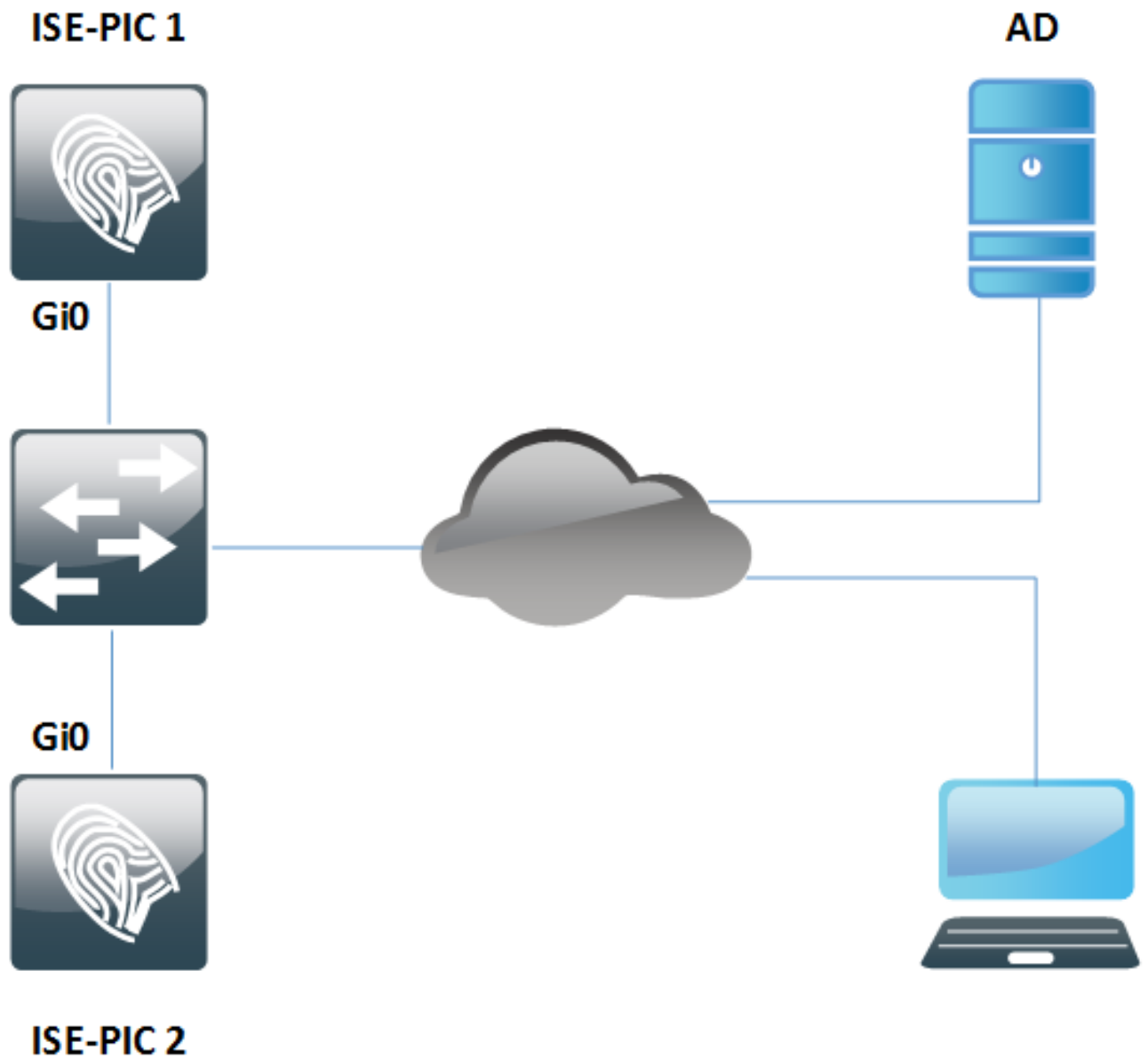
A quantidade máxima de Nós no desenvolvimento ISE PIC é 2. Este exemplo mostra como configurar o desenvolvimento ISE PIC para a Alta disponibilidade, SO2 que as máquinas virtuais (VM) são usadas. Em um desenvolvimento ISE PIC, os Nós podem ter papéis: Preliminar e secundário. Neste somente um nó pode 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).

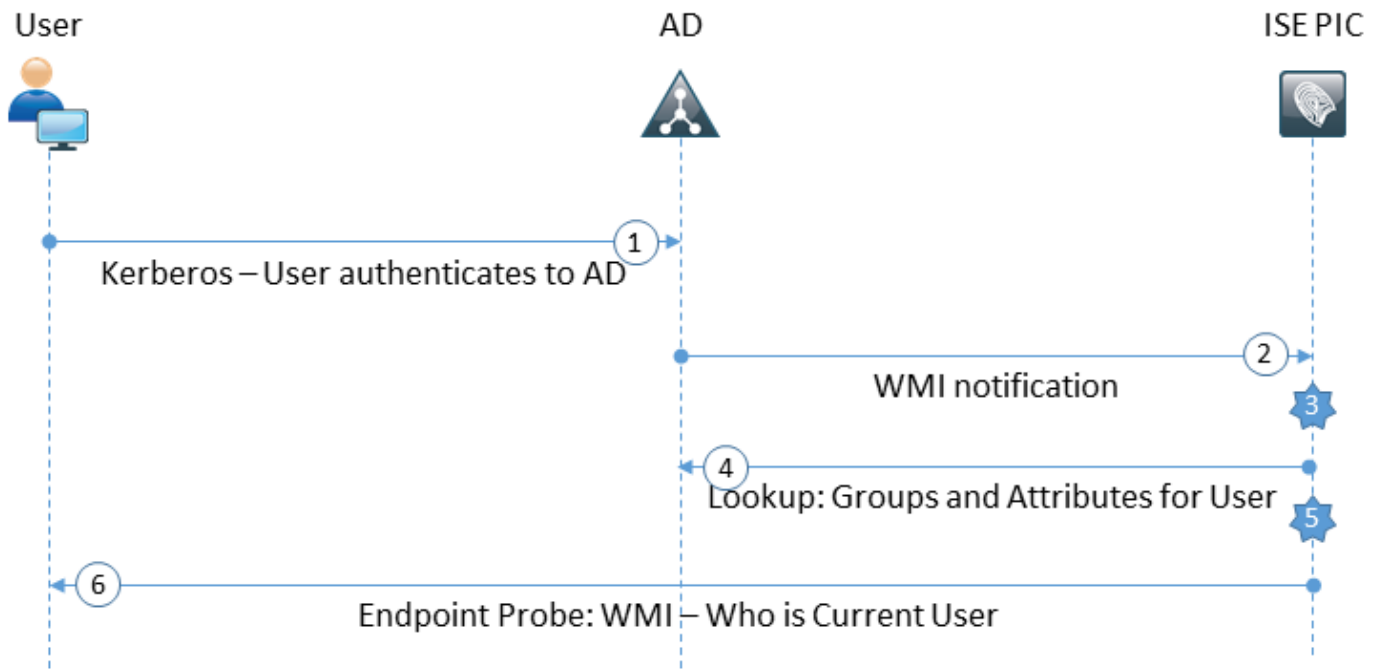
Nota: Mais informação sobre WMI pode ser encontrada no local de Microsoft do oficial:

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.

The screenshot shows a web interface for certificate management. At the top, there is a navigation bar with 'Certificates Management' and 'Certificates Authority'. Below this, there are several tabs: 'System Certificates', 'Trusted Certificates' (which is highlighted with a blue underline), 'OCSP Client Profile', 'Certificate Signing Requests', and 'Cert. Periodic Check Settings'. The main heading is 'Import a new Certificate into the Certificate Store'. Below the heading, there is a form with the following elements: a label '* Certificate File' followed by a 'Choose File' button and the filename 'WinServCer.cer'; a 'Friendly Name' text input field with an information icon; a 'Trusted For:' section with an information icon and four checkboxes: 'Trust for authentication within ISE' (checked), 'Trust for client authentication and Syslog' (checked), 'Trust for authentication of Cisco Services' (checked), and 'Validate Certificate Extensions' (unchecked); and a 'Description' text input field. At the bottom of the form are two buttons: 'Submit' and 'Cancel'.

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:

Import Server Certificate

* Select Node

* Certificate File ise22pic1vku...alise22p.pem

* Private Key File ise22pic1vku...alise22p.pvk

Password

Friendly Name ⓘ

Allow Wildcard Certificates ⓘ

Validate Certificate Extensions ⓘ

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- SAML: Use certificate for SAML Signing
- Portal: Use for portal

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:

▼ Certificates Management ▸ Certificates Authority

System Certificates Trusted Certificates OCSP Client Profile **Certificate Signing Requests** Cert. Periodic Check Settings

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for

Allow Wildcard Certificates ⓘ

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ise22-pic-2	ise22-pic-2#Admin

Subject

Common Name (CN) ⓘ

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

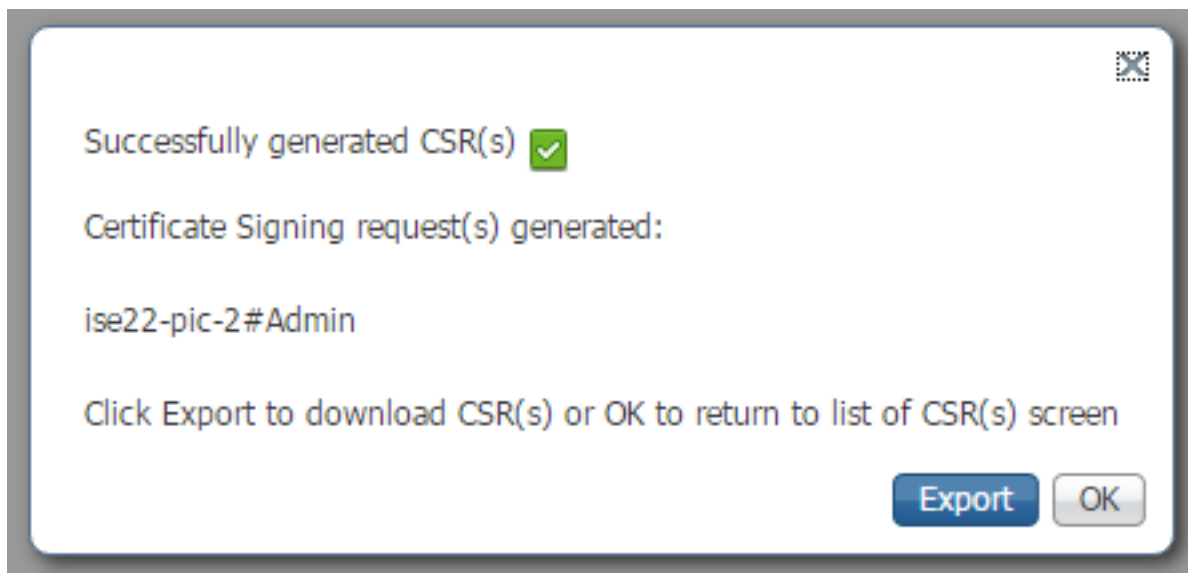
Subject Alternative Name (SAN) - + ⓘ

* Key Length

* Digest to Sign With

Certificate Policies

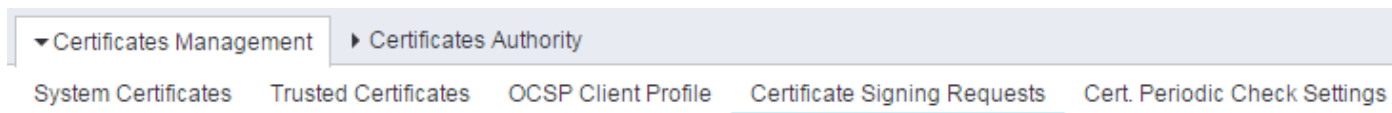
O clique **gerencie**. A nova janela estala acima com uma opção **para exportar o CSR gerado**:



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**:

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input checked="" type="checkbox"/>	ise22-pic-2#Admin	CN=ise22-pic-2.vkumov.local	2048		Thu, 23 Feb 2017	ise22-pic-2

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



Bind CA Signed Certificate

* Certificate File certnew.cer

Friendly Name ⓘ

Validate Certificate Extensions ⓘ

Usage

Admin: Use certificate to authenticate the ISE Admin Portal

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:

The screenshot shows the administration interface of an ISE PIC node. At the top, there is a navigation bar with tabs: 'Deployment' (selected), 'Licensing', 'Logging', 'Maintenance', and 'Admin Access'. Below this, the 'This Node' section displays the following information:

Role	Standalone
IP Address	10.48.26.51
FQDN	ise22-pic-1.vkumov.local

Below the 'This Node' section is the 'Add Secondary Node' section, which contains three input fields:

- FQDN *: ise22-pic-2.vkumov.local
- User Name *: admin
- Password *:

At the bottom right of the 'Add Secondary Node' section, there are two buttons: 'Cancel' and 'Save'.

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.

Certificate Warning



The node you are trying to register uses a self-signed certificate which is not trusted.
Are you sure you want to trust this certificate and proceed with registration?

If you are unsure, please click 'Cancel Registration' and manually setup trust under 'Certificate Management' before registering the node.

Serial Number : 58 AE E4 EF 00 00 00 00 62 E0 F9 86 17 5A 34 91
Issued to : CN=ise22-pic-2.vkumov.local
Issued by : CN=ise22-pic-2.vkumov.local
Issued On : Thu Feb 23 14:34:39 CET 2017
Expires On : Sat Feb 23 14:34:39 CET 2019
Signature Algorithm : SHA256withRSA
SHA-256 Fingerprint : 2D 4C 9A 7D FF 72 C7 93 73 C4 FB F0 58 E0 59 2F 24 40 F0 F8 77 50 D4 52 E6 3D
EF 56 CA 5F 4E 15
SHA-1 Fingerprint : 11 AB F0 8F 0C 89 50 FE 06 AC 2F AD 81 03 1D 52 D2 17 AB 61
MD5 Fingerprint : DD 27 87 FA 5D 18 E9 5C 71 BD 6A 5A 47 10 95 66

Additional Warnings

Import Certificate and Proceed

Cancel Registration

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.



Node was registered successfully. Data will be sync'ed to the node, and then the application server will be restarted on the node. This process may take several minutes to complete.

OK



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

This Node

Refresh

Role	Primary
IP Address	10.48.26.51
FQDN	ise22-pic-1.vkumov.local
Node Status	<input checked="" type="checkbox"/> Connected 

Secondary Node

Role	Secondary
IP Address	10.48.26.53
FQDN	ise22-pic-2.vkumov.local
Node Status	<input checked="" type="checkbox"/> Connected  

Deregister

Sync Now

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 communication 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**:

Active Directory Agents API Providers SPAN Syslog Providers Mapping Filters Endpoint Probes

Connection

* Join Point Name ⓘ

* Active Directory Domain ⓘ

Submit Cancel

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:

Join Domain ⓘ

Please specify the credentials required to Join node(s) to the Active Directory Domain.

* Domain Administrator ⓘ

* Password

Specify Organizational Unit ⓘ

Store Credentials ⓘ

OK Cancel

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](#).

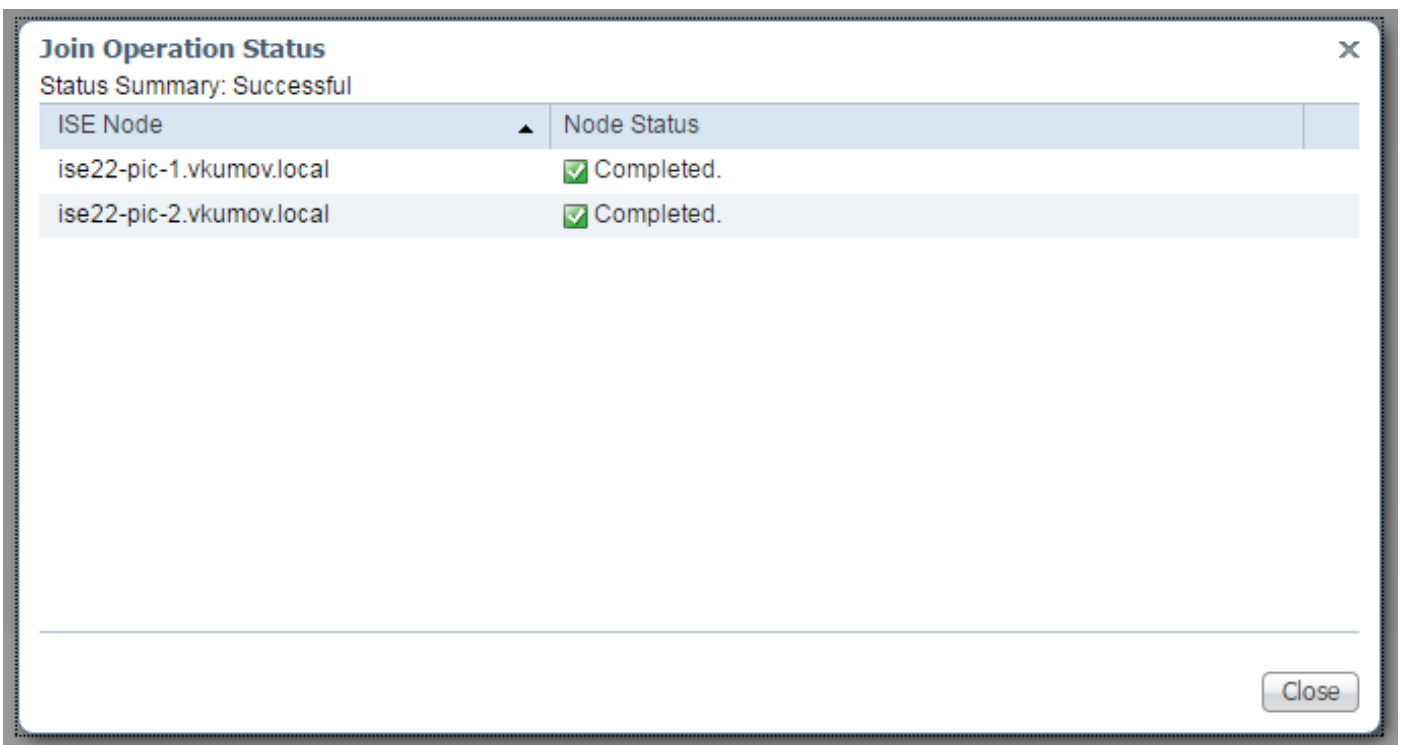
Contudo é administrador de domínio que do uso do requiredto as credenciais durante se juntam se você gostaria de usar WMI. A opção da **configuração WMI** exige:

- 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:

Active Directory Agents API Providers SPAN Syslog Providers Mapping Filters Endpoint Probes

Connection Whitelisted Domains **PassiveID** Groups Advanced Settings

PassiveID Domain Controllers

Refresh Edit Trash **Add DCs** Use Existing Agent Config WMI Add Agent

<input type="checkbox"/>	Domain	DC Host	Site
No data found.			

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:

Add Domain Controllers ✕

1 Selected

<input type="checkbox"/>	Domain	DC Host	Site	IP Address
<input checked="" type="checkbox"/>	vkumov.local	MainDC.vkumov.local	Default-First-Site-Name	10.48.26.52
<input type="checkbox"/>	vkumov.local	maindc.vkumov.local		139.156.158.9

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

Active Directory Agents API Providers SPAN Syslog Providers Mapping Filters Endpoint Probes License Warning

Connection Whitelisted Domains **PassiveID** Groups Advanced Settings

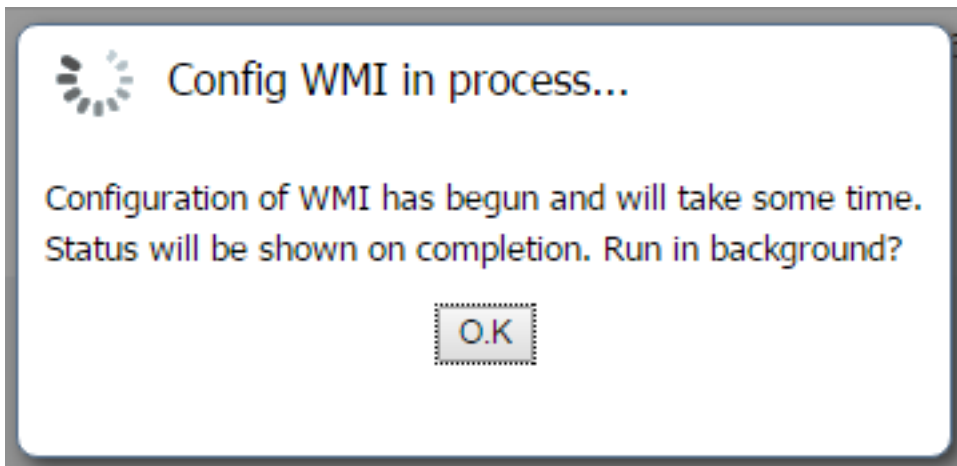
PassiveID Domain Controllers

1 Selected Rows/Page 1 / 1 Go 1 Total Rows

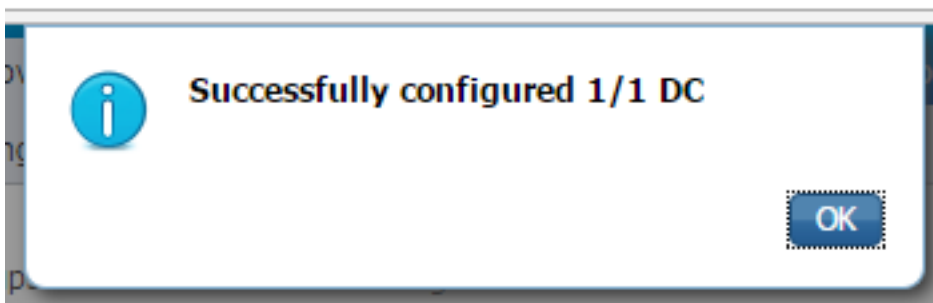
Refresh Edit Trash Add DCs Use Existing Agent **Config WMI** Add Agent

<input checked="" type="checkbox"/>	Domain	DC Host	Site	IP Address	Monitor Using
<input checked="" type="checkbox"/>	vkumov.local	MainDC.vkumov.local	Default-First-Site-Name	10.48.26.52	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:

This Node

Refresh

Role Primary
IP Address 10.48.26.51
FQDN ise22-pic-1.vkumov.local
Node Status Connected 

Secondary Node

Role Secondary
IP Address 10.48.26.53
FQDN ise22-pic-2.vkumov.local
Node Status Connected 

Deregister

Deployment Status

Registered : Thu Feb 23 2017 15:57:27 GMT+0100 (Central European Standard Time)

Sync Status : 0 messages to be synced.

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:

SUBSCRIBERS 🔄		
Name	Status	Description
<input type="text" value="Name"/>	<input type="text" value="Status"/>	<input type="text" value="Description"/>
ise-admin-ise22-pic-1	Online	
ise-admin-ise22-pic-2	Online	
ise-mnt-ise22-pic-1	Online	
ise-mnt-ise22-pic-2	Online	

Last refreshed: 2017-02-24 09:31:58

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

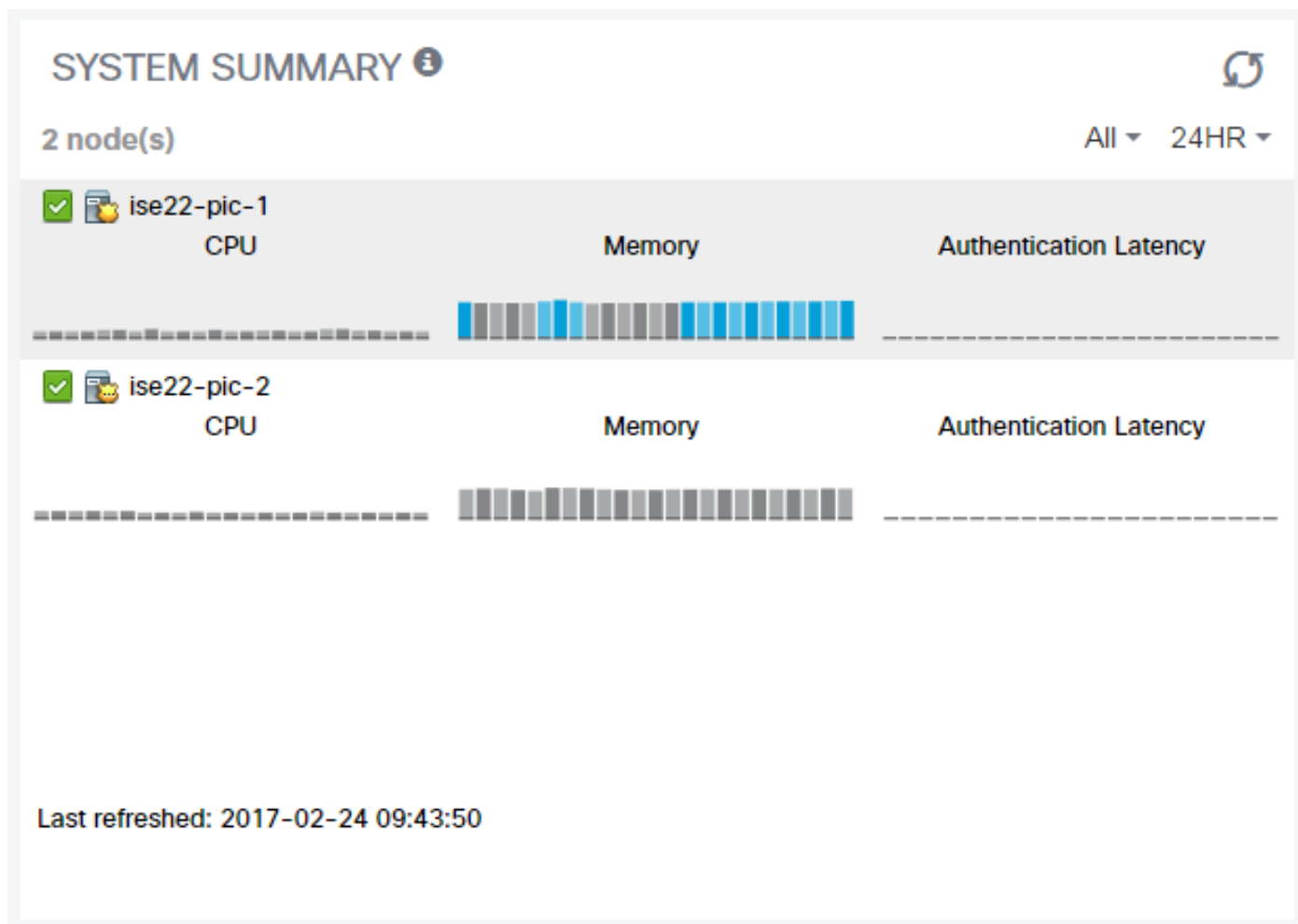
Os **assinantes** paginam são uma versão estendida do dashlet dos assinantes do Home Page de ISE PIC. Esta página mostra todo o pxGrid relativo, porém o estado de Nós ISE PIC pode ser verificado aqui também:

Cisco ISE Passive Identity Connector							
Clients							
Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log	
<input type="checkbox"/> ▶ ise-mnt-ise22-pic-2		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate	View	
<input type="checkbox"/> ▶ ise-mnt-ise22-pic-1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate	View	
<input type="checkbox"/> ▼ ise-admin-ise22-pic-1		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate	View	
Capability Detail							
						1 - 8 of 8 Show 25 per page	
Capability Name	Capability Version	Messaging Role	Message Filter				
<input type="radio"/> GridControllerAdminService	1.0	Sub					
<input type="radio"/> AdaptiveNetworkControl	1.0	Pub					
<input type="radio"/> Core	1.0	Sub					
<input type="radio"/> EndpointProfileMetaData	1.0	Pub					
<input type="radio"/> EndpointProtectionService	1.0	Pub					
<input type="radio"/> IdentityGroup	1.0	Pub					
<input type="radio"/> SessionDirectory	1.0	Pub					
<input type="checkbox"/> ▶ ise-admin-ise22-pic-2		Capabilities(3 Pub, 1 Sub)	Online	Administrator	Certificate	View	

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 nenhuma 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**:

PASSIVE IDENTITY METRICS



PROVIDERS ?

Status	Name	Domain	Type	IP/Host	Agent
<input checked="" type="checkbox"/>	MainDC.vkumov.lo...	vkumov.local	DC	MainDC.vkumov.lo...	WMI

Sessões vivas

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

Initiated	Updated	Account S...	Action	Endpoint ID	Identity	IP Address	Server	Session Source	Provider	User Dom...	User NetBI...	AD User Resolved Id...
Feb 24, 2017 09:16:45:721 AM	Feb 24, 2017 09:16:45:721 AM	0 s	Show Actions	10.48.26.51	Administrator	10.48.26.51	ise22-pic-2	PassiveID	WMIEndPoint	vkumov/local	VKUMOV	Administrator@vkumov...

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

Component Name	Log Level	Description
<input type="radio"/> portal-web-action	INFO	Base Portal debug messages
<input type="radio"/> posture	INFO	Posture debug messages
<input type="radio"/> previewportal	INFO	Preview Portal debug messages
<input type="radio"/> profiler	INFO	profiler debug messages
<input type="radio"/> provisioning	INFO	Client Provisioning client debug messages
<input type="radio"/> prrt-JNI	INFO	prrt policy decision request processing layer related messages
<input type="radio"/> pxgrid	INFO	pxGrid messages
<input type="radio"/> Replication-Deployment	DEBUG	Logger related to Deployment Registration,Deregistration,Sync and ...
<input type="radio"/> Replication-JGroup	WARN	Logger related to JGroup Node State
<input type="radio"/> ReplicationTracker	INFO	PSC replication related debug messages
<input type="radio"/> report	INFO	Debug reports on M&T nodes
<input type="radio"/> RuleEngine-Attributes	INFO	Additional rule evaluation attributes in audit logging at DEBUG
<input type="radio"/> 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.persistence.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.persistence.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.persistence.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.persistence.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.persistence.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.persistence.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.persistence.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.persistence.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**:

Deployment Licensing ▶ Logging ▶ Maintenance ▶ Admin Access

This Node Refresh

Role	Primary
IP Address	10.48.26.51
FQDN	ise22-pic-1.vkumov.local
Node Status	✔ Connected ⊕

Secondary Node Deregister

Role	Secondary
IP Address	10.48.26.53
FQDN	ise22-pic-2.vkumov.local
Node Status	✘ Disconnected ⊕

Deployment Status
Registered : Thu Feb 23 2017 15:57:27 GMT+0100 (Central European Standard Time)
Sync Status : Node not reachable
since : Fri Feb 24 2017 10:27:36 GMT+0100 (Central European Standard Time)

ise-psc.log contém esta mensagem:

```
2017-02-24 10:43:21,587 INFO [admin-http-pool1155][[]  
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 secundário 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:**

The screenshot shows the Cisco ISE configuration interface. At the top, there are tabs for 'Deployment', 'Licensing', 'Logging', 'Maintenance', and 'Admin Access'. Below these, there are sub-tabs for 'Local Log Settings', 'Debug Log Configuration', and 'Download Logs'. The 'Debug Log Configuration' tab is currently selected and highlighted in blue.

Node List > ise22-pic-2.vkumov.local Debug Level Configuration

Component Name	Log Level	Description
org-apache-cxf	WARN	CXF messages
org-apache-digester	WARN	XML processing apache internal messages
PanFailover	INFO	Pap Failover related messages
PassiveID	DEBUG	PassiveID events and messages
policy-engine	INFO	Policy Engine 2.0 related messages
portal	INFO	Portal (Guest, Hotspot, BYOD, CP) debug messages

E:

Active Directory	DEBUG	Active Directory client internal messages
------------------	-------	---

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, 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, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0,
69, 0, 0, 0, 1, 2, 0, 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", ":", "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, 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, 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", ":", "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, 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, 24, 0,
69, 0, 0, 0, 1, 2, 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, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1,
1, 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", ":", "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 `unreachable` 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, 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, 24, 0,
69, 0, 0, 0, 1, 2, 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, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1,
1, 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", ":", "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, 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", ":", "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
{
```

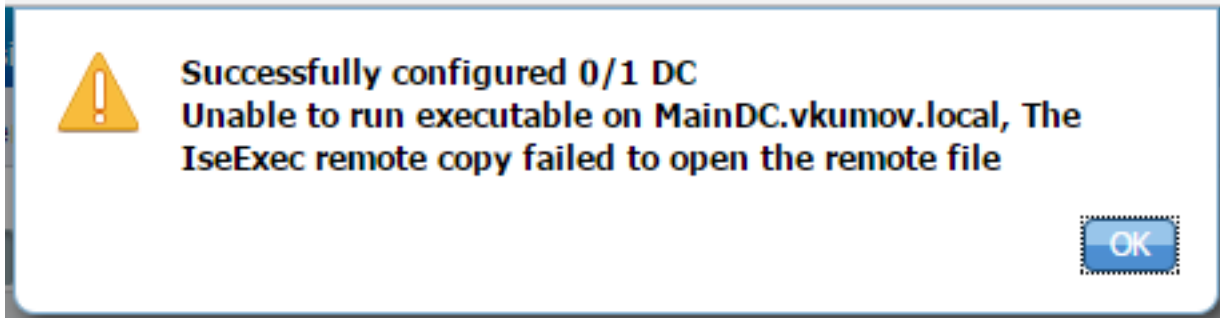
```

SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 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, 24, 0,
69, 0, 0, 0, 1, 2, 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, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1,
1, 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", ":", "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.