

ISE 2.2 PIC configureren met actieve Directory WMI-providers

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Werkstroom](#)

[Configureren](#)

[ISE PIC-implementatie configureren](#)

[Stap 1 \(optioneel\). Installeer betrouwbare certificaten.](#)

[Stap 2 \(optioneel\). Installeer systeemcertificaten.](#)

[Stap 3. Voeg secundair knooppunt aan de implementatie toe.](#)

[Active Directory Providers configureren](#)

[Stap 1. Sluit ISE PIC aan op het domein.](#)

[Stap 2. Tune permissies op AD.](#)

[Stap 3. Voeg passieve ID-agents toe.](#)

[Verifiëren](#)

[Plaatsing](#)

[Installatiepagina](#)

[Dashboard-pagina](#)

[Subscriber](#)

[Systeemoverzicht](#)

[Leveranciers en sessies](#)

[startpagina](#)

[Live Sessies](#)

[Problemen oplossen](#)

[Plaatsing](#)

[Vaak: secundair knooppunt is niet bereikbaar](#)

[Actieve map en WMI](#)

[Vaak: ISE PIC schrijft "Kan uitvoerbaar niet uitvoeren op](#)

Inleiding

Dit document beschrijft hoe u de AAD-provider kunt configureren en problemen oplossen bij het gebruik van Identity Services Engine Passive Identity Connector (ISE PIC) en actieve Directory Windows Management Instrumentation. ISE PIC is een lichtgewicht ISE versie die zich op passieve ID-functies richt.

ISE PIC is één enkele ID-oplossing voor alle Cisco security portfolio die alleen passieve identiteit

gebruikt. Dit betekent dat autorisatie of beleid niet kan worden ingesteld op ISE PIC. Het ondersteunt verschillende providers (Agents, WMI, Syslog en API) en kan worden geïntegreerd via REST API. Het heeft mogelijkheden om eindpunten te vragen (is Gebruiker ingelogd? Is het eindpunt nog verbonden?)

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- Cisco Identity Services Engine
- Microsoft Active Directory
- Microsoft WMI

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine Passive Identity Connector versie 2.2.0.470
- Microsoft Windows 7 Service Pack 1
- Microsoft Windows Server 2012r2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

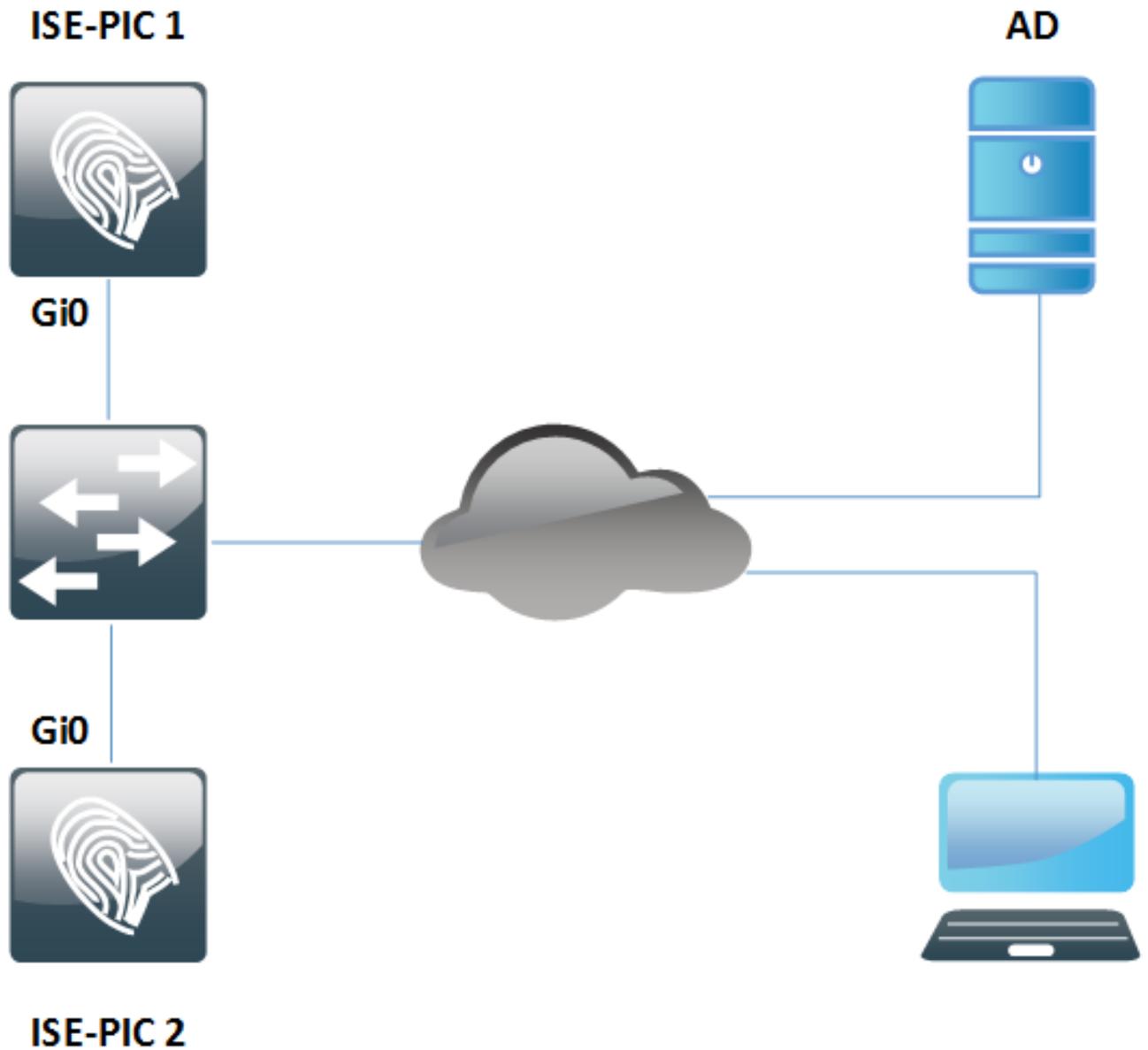
De maximale hoeveelheid knooppunten in ISE PIC-implementatie is 2. Dit voorbeeld toont hoe de ISE PIC-implementatie voor hoge beschikbaarheid te configureren, zodat er 2 virtuele machines (VMs) worden gebruikt. In een ISE PIC plaatsing, kunnen de knopen rollen hebben: Primair en secundair. In dit enige knooppunt kan tegelijkertijd Primair zijn en de rollen kunnen alleen handmatig door GUI worden gewijzigd. In het geval van primaire mislukking lopen alle functies nog op Secundair behalve UI. Alleen handmatige promotie naar Primair maakt de UI mogelijk.

Dit voorbeeld toont hoe te om de Leverancier van WMI voor Actieve Map te vormen. WMI bestaat uit een reeks uitbreidingen van het Windows-driver-model dat een besturingssysteeminterface biedt waardoor met instrumenten ondersteunde onderdelen informatie en kennisgeving leveren. WMI is de implementatie door Microsoft van de normen van het Web-Based Enterprise Management (WBEM) en Common Information Model (CIM) van de Distributed Management Task Force (DMTF).

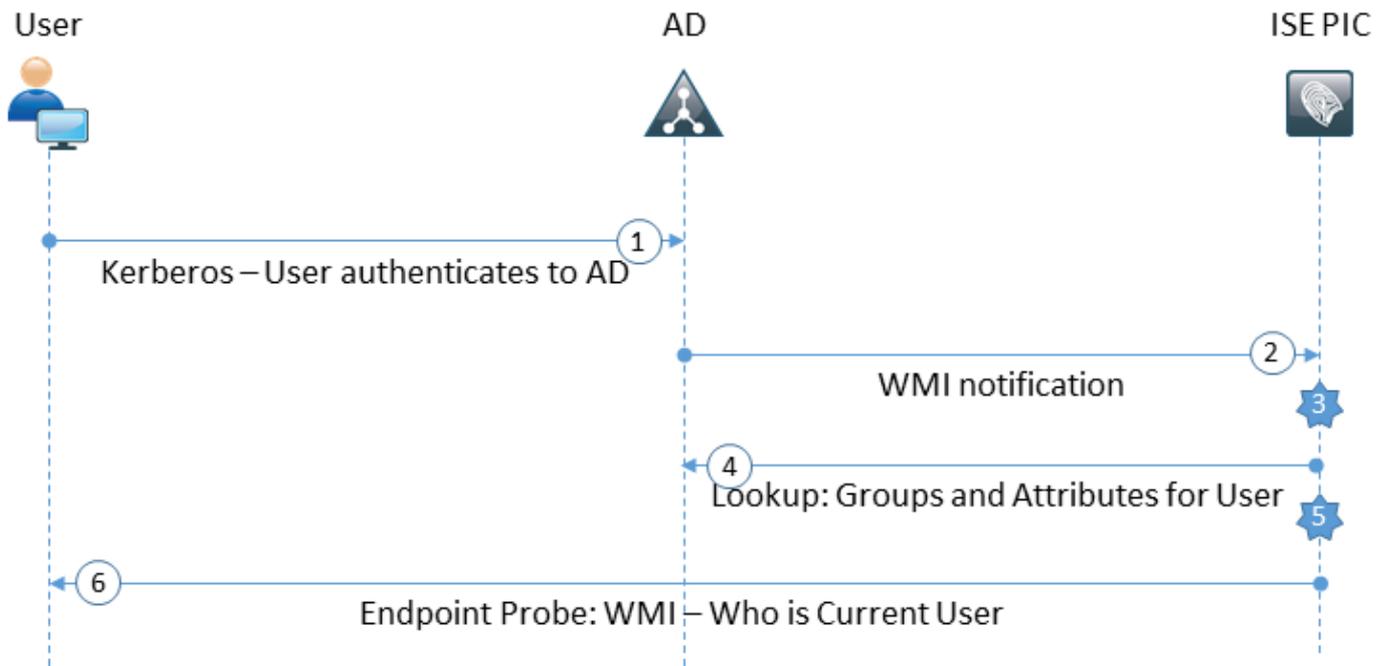
Opmerking: Meer informatie over WMI is te vinden op de officiële Microsoft-website: [Over WMI](#)

Netwerkdigram

De informatie in het document gebruikt de netwerkinstellingen die in de afbeelding worden weergegeven:



Werkstroom



1. Meld u aan bij PC en krijgt u authenticatie op AD.
 2. WMI informeert ISE PIC over deze authenticatie.
 3. ISE voegt bindende naam toe: IP_Address aan zijn Session Directory.
 4. ISE haalt gebruikersgroepen en -kenmerken terug uit AD.
 5. ISE slaat deze informatie op in de sessie van ISE.
 6. Om de 4 uur (niet aanpasbaar) draait ISE PIC Endpoint Probe:
Eerst probeert het WMI naar het Endpoint. Als de WMI niet lukt, voert ISE PIC ISEExec uit. Het stelt vragen bij het Endpoint voor de gebruiker en stelt WMI voor de volgende keer in. ISE PIC haalt ook het MAC-adres van het Endpoint en het OS-type op.
- Op ISE PIC is het alleen mogelijk om endpointtests in/uit te schakelen. Primaire knooppunt vraagt alle endpoints, secundair knooppunt is alleen voor hoge beschikbaarheid.

Configureren

ISE PIC-implementatie configureren

Stap 1 (optioneel). Installeer betrouwbare certificaten.

De volledige keten van certificaten van uw certificaatinstelling (CA) moet in een ISE-betrouwbare winkel worden geïnstalleerd. Meld u aan bij ISE PIC GUI en navigeer naar **Certificaten > Certificaten Management > Trusted Certificates**. Klik op **Importeren** en selecteer het certificaat van uw computer.

Zoals in de afbeelding wordt weergegeven, klikt u op **Inzenden** om wijzigingen op te slaan. Herhaal deze stap voor alle certificaten van de keten. Herhaal ook stappen op het secundaire knooppunt.

The screenshot shows a web interface for managing certificates. 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), 'OCSP Client Profile', 'Certificate Signing Requests', and 'Cert. Periodic Check Settings'. The main heading is 'Import a new Certificate into the Certificate Store'. The form includes a field for '* Certificate File' with a 'Choose File' button and the filename 'WinServCer.cer'. Below that is a 'Friendly Name' text input field with an information icon. The 'Trusted For:' section has 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). At the bottom, there is a 'Description' text input field and two buttons: 'Submit' and 'Cancel'.

Stap 2 (optioneel). Installeer systeemcertificaten.

Optie 1. Certificaten die reeds door CA zijn gegenereerd samen met een privé-toets.

Navigeer in op **certificaten > Certificaten Management > Systeemcertificaten** en klik op **Importeren**. Selecteer **certificaatbestand** en **privé-sleutelbestand**, voer het veld *Wachtwoord* in als de particuliere sleutel is versleuteld.

Zoals wordt aangegeven in de opties voor de controle van de afbeelding:

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

Opmerking: Aangezien ISE PIC is gebaseerd op ISE-code en gemakkelijk met de juiste licenties kan worden geconverteerd naar volledig opgetuigde ISE-licenties, zijn alle gebruiksopties beschikbaar. Rollen zoals **EAP-verificatie**, **RADIUS DTLS**, **SAML** en **Portal** worden niet door ISE PIC gebruikt.

Klik op **Indienen** om certificaat te installeren. Herhaal deze procedure ook voor een secundair knooppunt.

Opmerking: Alle services op het ISE PIC-knooppunt worden opnieuw gestart na de invoer van servercertificaat.

Optie 2. Genereert certificaataanvraag (CSR), teken dit met CA en verbind op ISE.

navigeren naar **Certificaten > Beheer van certificaten > pagina voor aanvragen voor certificaatsignalering** en klik op **CSR (certificaatsignaalaanvraag genereren)**.

Selecteer het knooppunt en gebruik en voer indien nodig de andere velden in:

▼ 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)

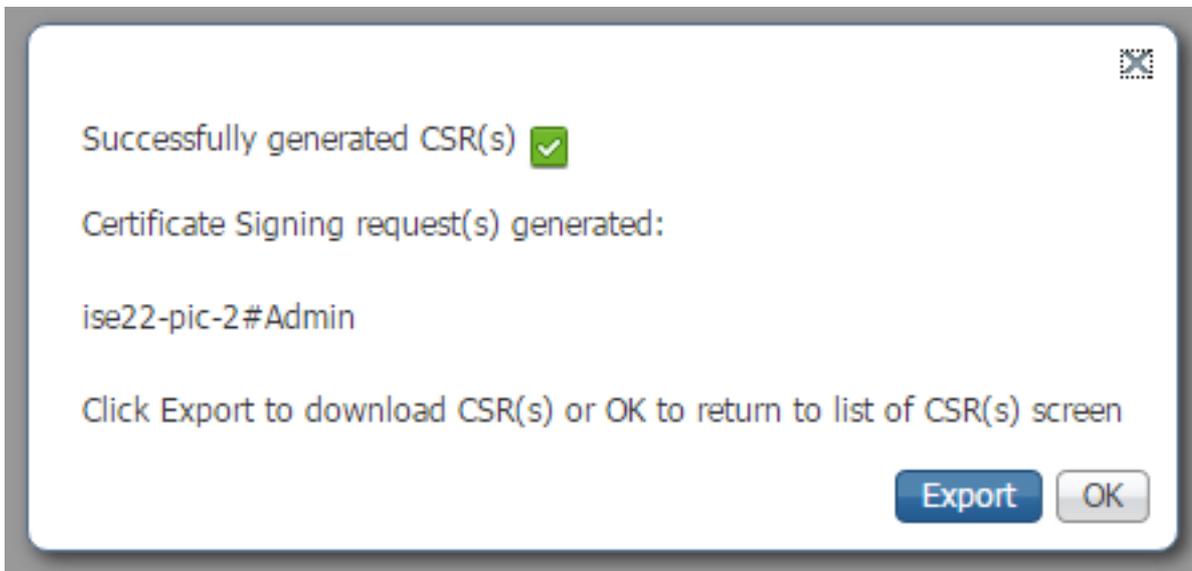
Subject Alternative Name (SAN) - + ⓘ

* Key Length

* Digest to Sign With

Certificate Policies

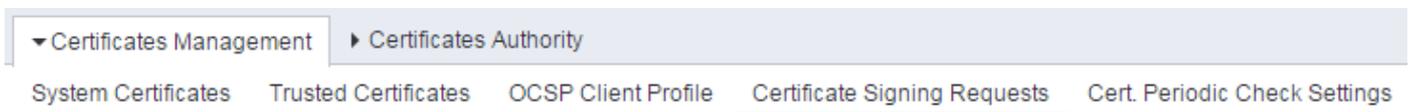
Klik op **Generate**. Er verschijnt een nieuw venster met een optie om CSR te exporteren:



Klik op **Exporteren**, sla het gegenereerde *.pem-bestand op en teken het met CA. Nadat CSR is ondertekend, kunt u terugkeren naar **Certificaten > Certificaten Management > pagina Aanvragen voor certificaatsignalering selecteren** en op **Bind Certificaat** klikken:

<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

Selecteer het certificaat dat met uw CA is ondertekend en klik op **Indienen** om wijzigingen toe te passen:



Bind CA Signed Certificate

* Certificate File certnew.cer

Friendly Name

Validate Certificate Extensions

Usage

Admin: Use certificate to authenticate the ISE Admin Portal

Alle services in het opnieuw opstarten van het ISE PIC-knooppunt nadat u op **Inzenden** klikt om certificaat te installeren.

Stap 3. Voeg secundair knooppunt aan de implementatie toe.

ISE PIC staat toe om 2 knopen in een plaatsing voor Hoge beschikbaarheid te hebben. Er is geen tweerichtingsvertrouwen nodig voor certificaten (in vergelijking met de gebruikelijke ISE-inzet). Als u een secundair knooppunt aan de implementatie wilt toevoegen, navigeer dan naar de **implementatiepagina** op uw primaire ISE PIC-knooppunt, zoals in de afbeelding:

The screenshot shows a navigation bar with the following tabs: Deployment (selected), Licensing, Logging, Maintenance, and Admin Access.

This Node

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

Add Secondary Node

FQDN *

User Name *

Password *

Voer FQDN-naam (Full Qualified Domain Name) van het secundaire knooppunt in, beheerder geloofsbrieven van dat knooppunt en klik op **Save**. Indien het primaire ISE PIC-knooppunt niet in staat is om het beheercertificaat van het tweede knooppunt te controleren, vraagt het om bevestiging voordat het dat certificaat in een vertrouwde winkel installeert.

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

Klik in dat geval op **Importeren op Certificaat en ga** verder om het knooppunt aan te sluiten bij de implementatie. U moet weten dat het knooppunt is toegevoegd. Alle diensten op de secundaire knooppunten restart.



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

Binnen 10-20 minuten moeten knooppunten gesynchroniseerd worden en de status van het knooppunt moet veranderen van **In uitvoering** aan **Verbonden**:

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

Active Directory Providers configureren

ISE PIC gebruikt Windows Management Instrumentation (WMI) om informatie over sessies te verzamelen bij AD en werkt als een Pub/Subcommunicatie, wat betekent:

- ISE PIC abonneert op bepaalde gebeurtenissen
- WMI waarschuwt ISE PIC wanneer deze gebeurtenissen zich voordoen: 4768 (verlening van Kerberos-vergunningen) en 4770 (vernieuwing van Kerberos-textielproducten) Vermeldingen in sessiemap verlopen (schoonmaken)

Stap 1. Sluit ISE PIC aan op het domein.

Als u zich aan ISE PIC bij het domein wilt aansluiten, navigeer dan naar **providers > Active Directory** en klik op **Add**:

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

Connection

* Join Point Name ⓘ

* Active Directory Domain ⓘ

Submit Cancel

Vul de velden **Point Name** en **Active Directory Domain** in en klik op **Inzenden** om wijzigingen op te slaan. **Join Point Name** is een naam die alleen in ISE PIC wordt gebruikt. **Active Directory Domain** is de naam van het domein waar ISE PIC moet worden aangesloten en het moet kunnen worden opgelost met DNS server die op ISE PIC is geconfigureerd.

Na het maken van punt ISE van het Samenvoegen zou u moeten vragen of u knooppunten aan het domein wilt aansluiten. Klik op **Ja**. Er verschijnt een venster waarin u inloggegevens kunt opgeven om zich bij het domein aan te sluiten:

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

Vul de velden **Domain Administrator** en **Wachtwoord** in en klik op **OK**.

Ook al wordt het veld **Domain Administrator** genoemd, het is niet nodig om beheerdergebruiker te gebruiken om **zich bij ISE PIC aan het domein aan te sluiten**. Deze gebruiker moet voldoende rechten hebben om computerrekeningen in het domein te maken en te verwijderen, of de wachtwoorden te wijzigen voor eerder gemaakte computerrekeningen. De actieve toegang van de folder die vereist is voor het uitvoeren van verschillende bewerkingen kan in dit [document](#) gevonden worden.

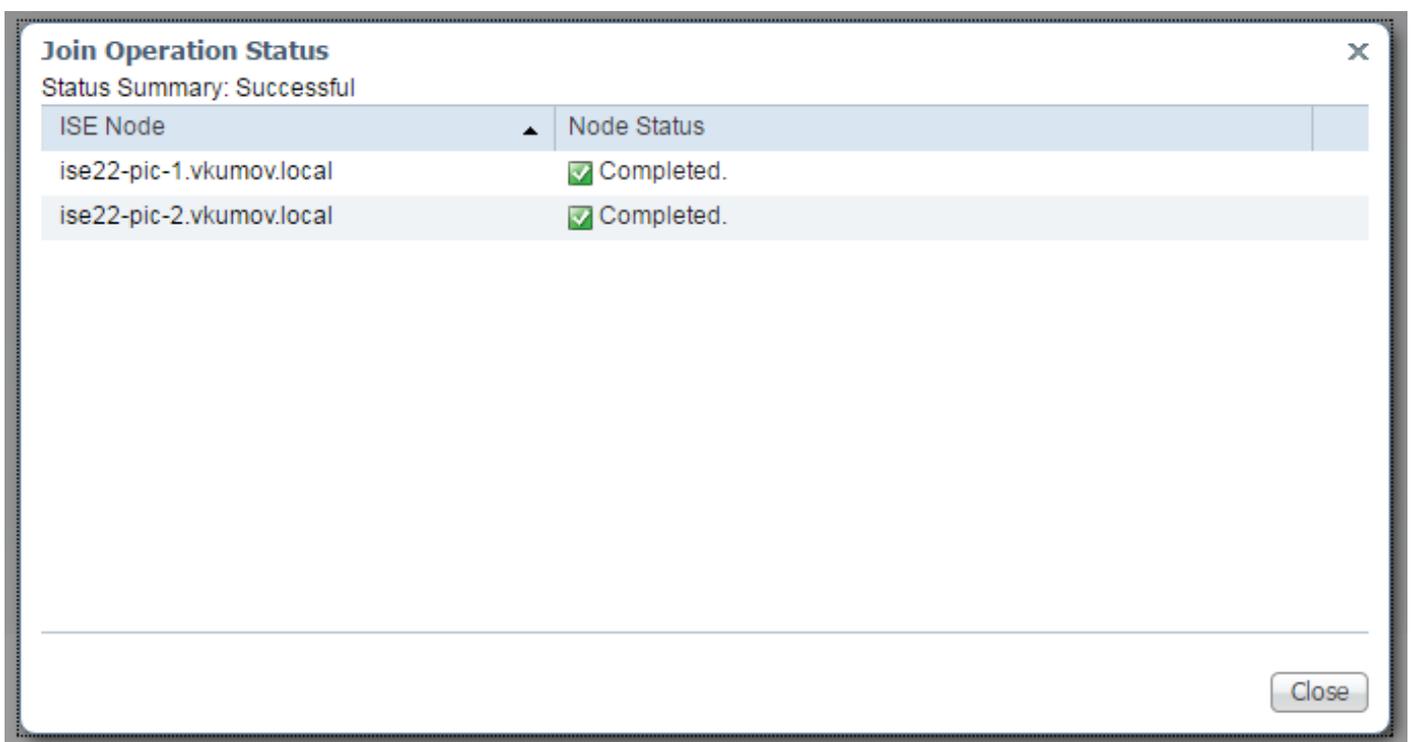
Er is echter vereist dat u Domain Administrator-referenties gebruikt tijdens het aansluiten, als u WMI wilt gebruiken. **De WMI-optie in configuratie** vereist:

- Wijzigingen in het register
- Toestemmingen om DCOM te gebruiken

- Vergunningen voor gebruik van WMI op afstand
- Toegang tot het lezen van het Security Event Log van de AD Domain Control
- Windows Firewall moet verkeer van/naar ISE PIC mogelijk maken (er wordt corresponderend Windows-firewallbeleid gemaakt tijdens **WMI in configuratie**)

Opmerking: **Store Credentials** is altijd ingeschakeld op ISE PIC omdat dit vereist is voor Endpoint Probes en WMI-configuratie. ISE slaat ze op, versleuteld intern.

Zoals in de afbeelding wordt getoond, toont ISE PIC het resultaat van de bewerking in een nieuw venster:



Stap 2. Tune permissies op AD.

Controleer en stel rechten voor de gebruiker in op AD per document: [Identity Services Engine Passive Identity Connector \(ISE-PIC\) installatie- en beheerdershandleiding:](#)

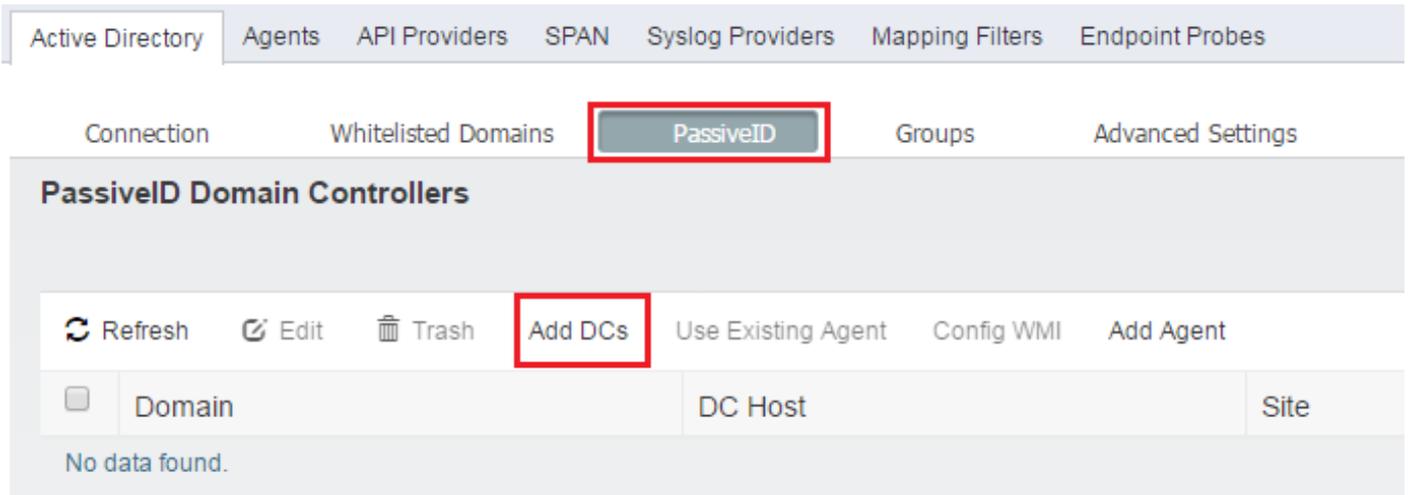
Instellen van toegangsrechten als AD-gebruiker in de Admin-groep van het domein

Voor Windows 2008 R2, Windows 2012 en Windows 2012 R2 heeft de Domain Admin-groep standaard niet volledige controle over bepaalde registratiesleutels in het Windows-besturingssysteem. De beheerder van de actieve map moet de volledige controle van de actieve gebruiker van de map op de volgende registratiesleutel geven

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

Stap 3. Voeg passieve ID-agents toe.

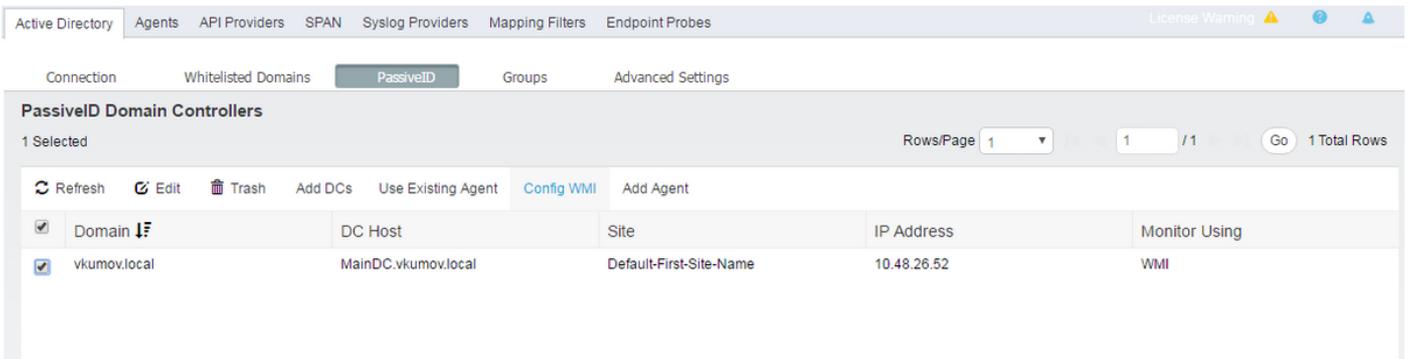
navigeer in het AD-domein naar het tabblad PassiveID en klik op **Add DC's** zoals in de afbeelding:



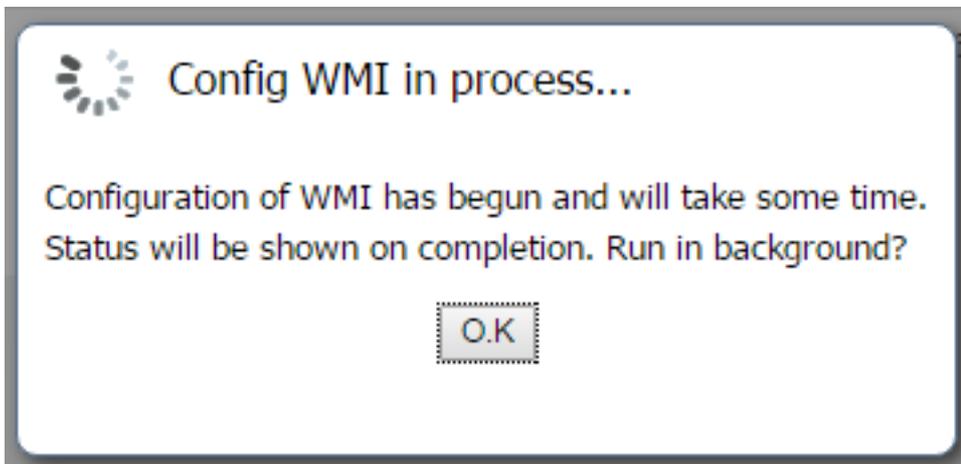
Er verschijnt een nieuw venster en ISE laadt een lijst met alle beschikbare domeincontrollers. Selecteer DC's waarin u WMI wilt configureren en klik op **OK** om wijzigingen op te slaan, zoals in de afbeelding:



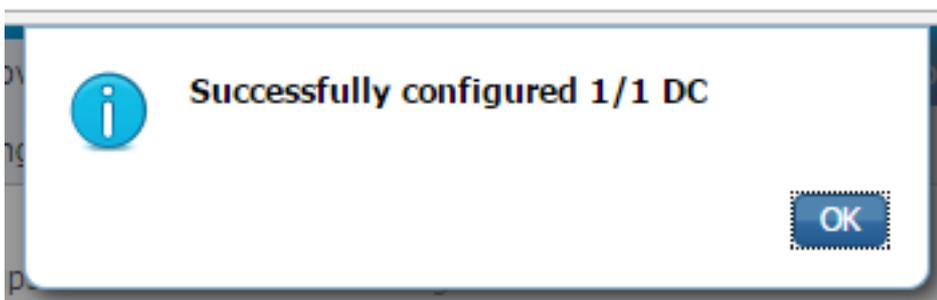
Geselecteerde DC's worden toegevoegd aan de lijst van **PassiveID Domain Controllers**. Selecteer uw DC's en klik op de knop **Config WMI**:



ISE PIC toont een bericht dat het configuratieproces in gang is:



Na een paar minuten toont het u een bericht dat WMI met succes is ingesteld op geselecteerde DC's:



Verifiëren

Plaatsing

De status van de inzet kan op een paar manieren worden gecontroleerd:

Installatiepagina

Navigeer aan **Beheerder > Pagina van de Plaatsing** kan de huidige staat van de plaatsing worden gecontroleerd:

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.
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.

Van deze pagina kan het secundaire knooppunt indien nodig worden gedereguleerd. Handmatige synchronisatie kan worden gestart en **Sync Status** kan worden gecontroleerd.

Dashboard-pagina

Op een hoofdpagina van ISE PIC is er een dashlet genaamd **Subscriber**. Met dit veld kunt u de huidige status van uw ISE PIC-knooppunten controleren, zoals in de afbeelding:

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

ISE PIC maakt 2 abonnees voor elk knooppunt - **beheer** en **beheer**. Al deze knooppunten zouden in **Online** status moeten zijn, wat betekent dat knooppunten bereikbaar en operationeel zijn.

Subscriber

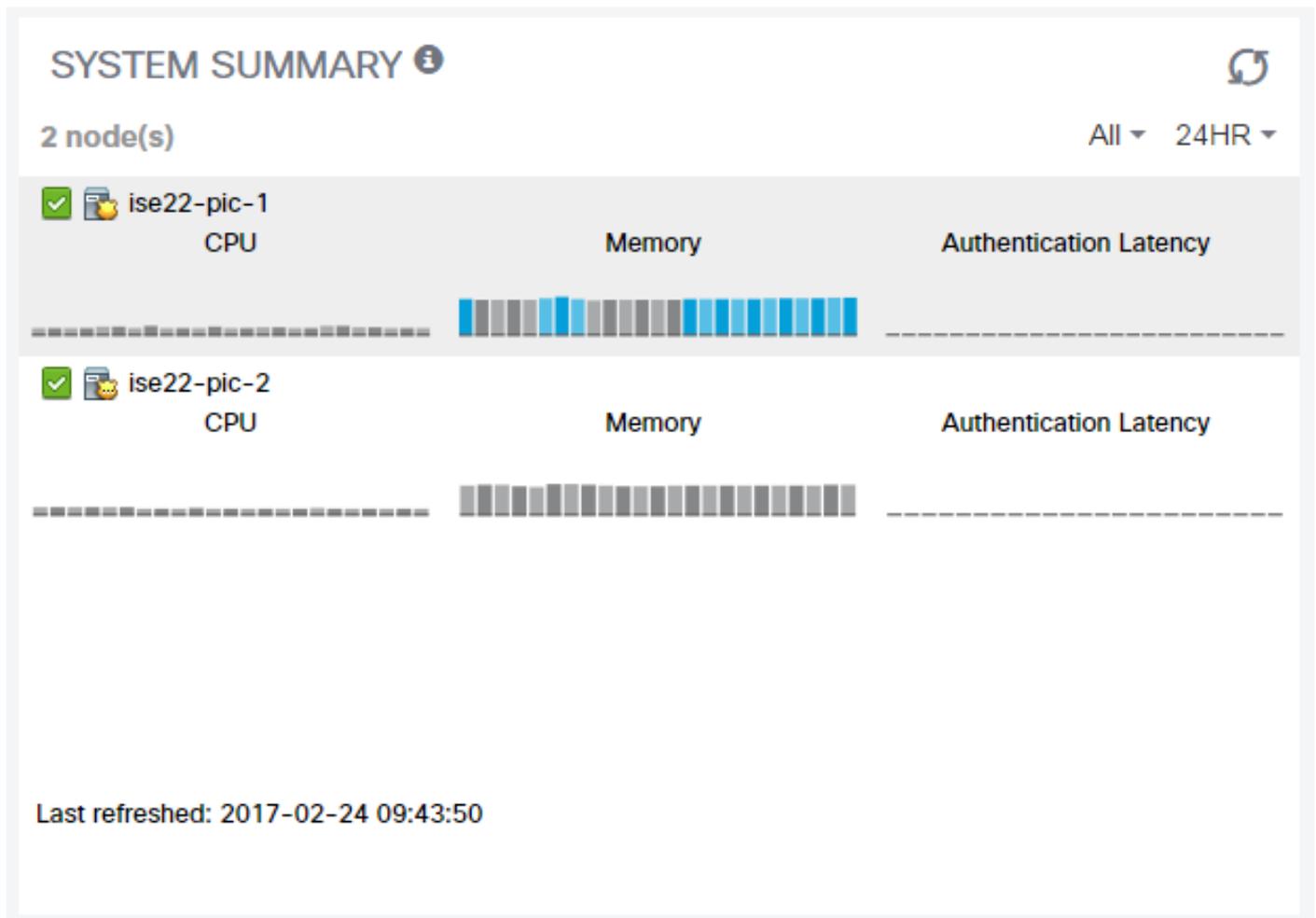
Subscriber-pagina is een uitgebreide versie van de abonnees die vanaf de startpagina van ISE PIC wordt geleverd. Deze pagina toont alle pxGrid-gerelateerde, maar de status van ISE PIC-knooppunten kan hier ook worden gecontroleerd:

Cisco ISE Passive Identity Connector							
Home Live Sessions Providers Subscribers Certificates Troubleshoot Reports Administration Settings							
Clients Capabilities Live Log Settings Certificates							
<input type="checkbox"/> Enable <input type="checkbox"/> Disable <input type="checkbox"/> Approve <input type="checkbox"/> Group <input type="checkbox"/> Decline <input type="checkbox"/> Delete <input type="checkbox"/> Refresh Total Pending Approval(0)							
<input type="checkbox"/>	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							
<input type="radio"/>	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

Systemoverzicht

Met ISE PIC kan ook de gezondheidssamenvatting van de knooppunten worden gevolgd. Dit

venster is te vinden in Home > Dashboard > Extra:



De Latentie van de Verificatie is altijd 0ms, aangezien ISE PIC geen authenticaties/vergunningen uitvoert.

Leveranciers en sessies

startpagina

De status van providers, hun hoeveelheid en de hoeveelheid gevonden sessies kunnen worden gecontroleerd terwijl u naar **startpunt > Dashboard** navigeert:

PASSIVE IDENTITY METRICS

Sessions ⓘ



1

Providers ⓘ

1

PROVIDERS ⓘ



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

Live Sessies

Gedetailleerde informatie over alle gevonden gebruikerssessies is te vinden op de pagina **Live Sessies**:

Initiated	Updated	Account S...	Action	Endpoint ID	Identity	IP Address	Server	Session Source	Provider	User Dom...	User NetBl...	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...

Het bevat informatie als:

- Provider - welke providers werden gebruikt om deze sessie te identificeren
- Initiële en bijgewerkte tijdstempels wanneer de sessie wordt gestart en dienovereenkomstig wordt bijgewerkt
- IP-Address - het adres van het Endpoint

- Actie - acties die ISE kan uitvoeren (bijvoorbeeld de status van het eindpunt controleren, of als ISE PIC met pxGrid is geïntegreerd, stuur dan een verzoek naar duidelijke sessie)

Problemen oplossen

Plaatsing

Om implementaties en replek van de oplossing problemen op te lossen, kijk in die logbestanden:

- replicatie.log
- plaatsing.log
- ise-psc.log

Om de knoppen in te schakelen, navigeer naar **Beheer > Vastlegging > Logconfiguratie van het defect:**

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

Deze exemplaren worden geschreven aan **replicatie.log** bestand. Hier is een voorbeeld van een normaal replicatieproces:

```
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]
```

Een bericht van ise-psc.log:

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

Vaak: secundair knooppunt is niet bereikbaar

Als het secundaire knooppunt onbereikbaar wordt, wordt het weergegeven op de **pagina Administratie > Plaatsing**:

Deployment Licensing ▶ Logging ▶ Maintenance ▶ Admin Access

This Node

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

Refresh

Secondary Node

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

Deregister

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 bevat dit bericht :

```
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
```

Dit bericht legt uit wat niet bereikbaar is, bijvoorbeeld het knooppunt reageert niet op ping:

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

Te nemen maatregelen: Controleer of FQDN van het knooppunt van het ziekenhuis oplosbaar is, controleer de basisnetwerkverbinding tussen knooppunten.

Als de toepassingen niet in staat zijn om actief te zijn op secundaire knooppunten of er een firewall tussen knooppunten is, kan **ise-psc.log** deze berichten laten zien:

```
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

```

Handelingen die moeten worden ondernomen: controleer de toepassingsstatus op het secundaire knooppunt, controleer de netwerkconnectiviteit als alle verbindingen tussen knooppunten zijn toegestaan.

Actieve map en WMI

Om de actieve WMI-versie van de map op te lossen moet u deze bestanden bekijken:

- passief-wmi.log
- passief-eindpunt.log
- ise-psc.log
- ad_agent.log

En de bruikbare uiteinden kunnen worden ingeschakeld bij **Beheer > Vastlegging > Logconfiguratie van het bug-logbestand:**

Deployment Licensing Logging Maintenance Admin Access

Local Log Settings **Debug Log Configuration** Download Logs

Node List > ise22-pic-2.vkumov.local

Debug Level Configuration

Edit Reset to Default

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

En:

<input type="radio"/> Active Directory	DEBUG	Active Directory client internal messages
--	-------	---

Hier is een voorbeeld van een nieuwe geleerde sessie van **passief-wmi.log** met gebruik van

debugs:

```
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, 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, 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", ":", "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, 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, 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:\t\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\t\tkrbtgt
\n\tService ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t\t:
\n\tClient Port:\t\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t\t0x40810010
\n\tResult Code:\t\t\t0x0
\n\tTicket Encryption Type:\t\t0x12
\n\tPre-Authentication Type:\t\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, 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:\t\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\t\tkrbtgt
\n\tService ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t\t:1
\n\tClient Port:\t\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t\t0x40810010
\n\tResult Code:\t\t\t0x0
\n\tTicket Encryption Type:\t\t0x12
\n\tPre-Authentication Type:\t\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";
};
```

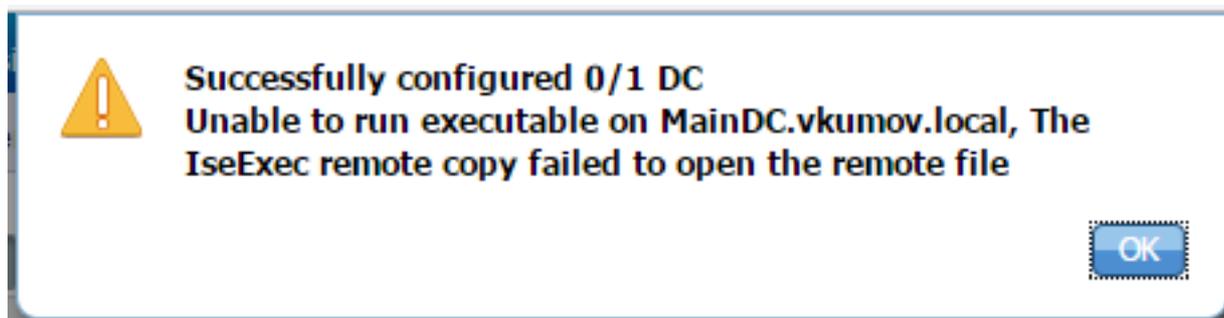
, Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.event-user-name = Administrator , Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,

Voorbeeld van eindpuntcontrole van **passief-eindpunt.log** (in dit geval was het eindpunt onbereikbaar via ISE):

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

Vaak: ISE PIC gooit "Kan uitvoerbaar op <DC naam> niet starten.." fout

Als een gebruiker die wordt gebruikt om zich aan ISE PIC aan het domein aan te sluiten niet genoeg rechten heeft, gooit ISE PIC een fout tijdens de configuratie van WMI:



U vindt de juiste **debugs** in het bestand **ad_agent.log** (het logniveau van de actieve map moet op DEBUG worden ingesteld):

```
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
```

Handelingen die moeten worden ondernomen: Sluit me weer aan op ISE PIC-knooppunten bij het

domein met Domain Administrator-referenties, of voeg de gebruiker toe die wordt gebruikt om mee te werken aan de *Domain Admins*-groep in de AD.