

Configurare ISE 2.2 PIC con il provider WMI Active Directory

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Flusso di lavoro](#)

[Configurazione](#)

[Configurazione dell'installazione di ISE PIC](#)

[Passaggio 1 \(facoltativo\). Installa certificati attendibili.](#)

[Passaggio 2 \(facoltativo\). Installa certificati di sistema.](#)

[Passaggio 3. Aggiungere il nodo secondario alla distribuzione.](#)

[Configura provider Active Directory](#)

[Passaggio 1. Entra nel dominio ISE PIC.](#)

[Passaggio 2. Ottimizzare le autorizzazioni in AD.](#)

[Passaggio 3. Aggiungere gli agenti PassiveID.](#)

[Verifica](#)

[Implementazione](#)

[Pagina Distribuzione](#)

[Pagina Dashboard](#)

[Sottoscrittori](#)

[Riepilogo del sistema](#)

[Provider e sessioni](#)

[Home page](#)

[Sessioni Live](#)

[Risoluzione dei problemi](#)

[Implementazione](#)

[Problema comune: nodo secondario non raggiungibile](#)

[Active Directory e WMI](#)

[Problema comune: ISE PIC visualizza il messaggio "Unable to run executable on](#)

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi alla distribuzione di Identity Services Engine Passive Identity Connector (ISE PIC) con il provider WMI Active Directory. ISE PIC è una versione leggera di ISE che si concentra sulle funzionalità dell'ID passivo.

ISE PIC è una soluzione a ID singolo per tutte le soluzioni Cisco Security Portfolio che utilizza solo

identità passiva. Ciò significa che l'autorizzazione o le policy non possono essere configurate su ISE PIC. Supporta diversi provider (Agents, WMI, Syslog, API) e può essere integrato tramite l'API REST. Può eseguire query sugli endpoint. L'utente ha eseguito l'accesso? L'endpoint è ancora connesso?)

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il numero massimo di nodi nella distribuzione ISE PIC è 2. Nell'esempio viene mostrato come configurare la distribuzione ISE PIC per l'alta disponibilità, in modo da utilizzare 2 macchine virtuali (VM). In un'implementazione ISE PIC, i nodi possono avere i seguenti ruoli: Primario e secondario. In questo caso, solo un nodo può essere primario alla volta e i ruoli possono essere modificati solo manualmente tramite GUI. In caso di errore primario, tutte le funzionalità vengono ancora eseguite su Secondario ad eccezione di UI. Solo la promozione manuale a principale consente di attivare l'interfaccia utente.

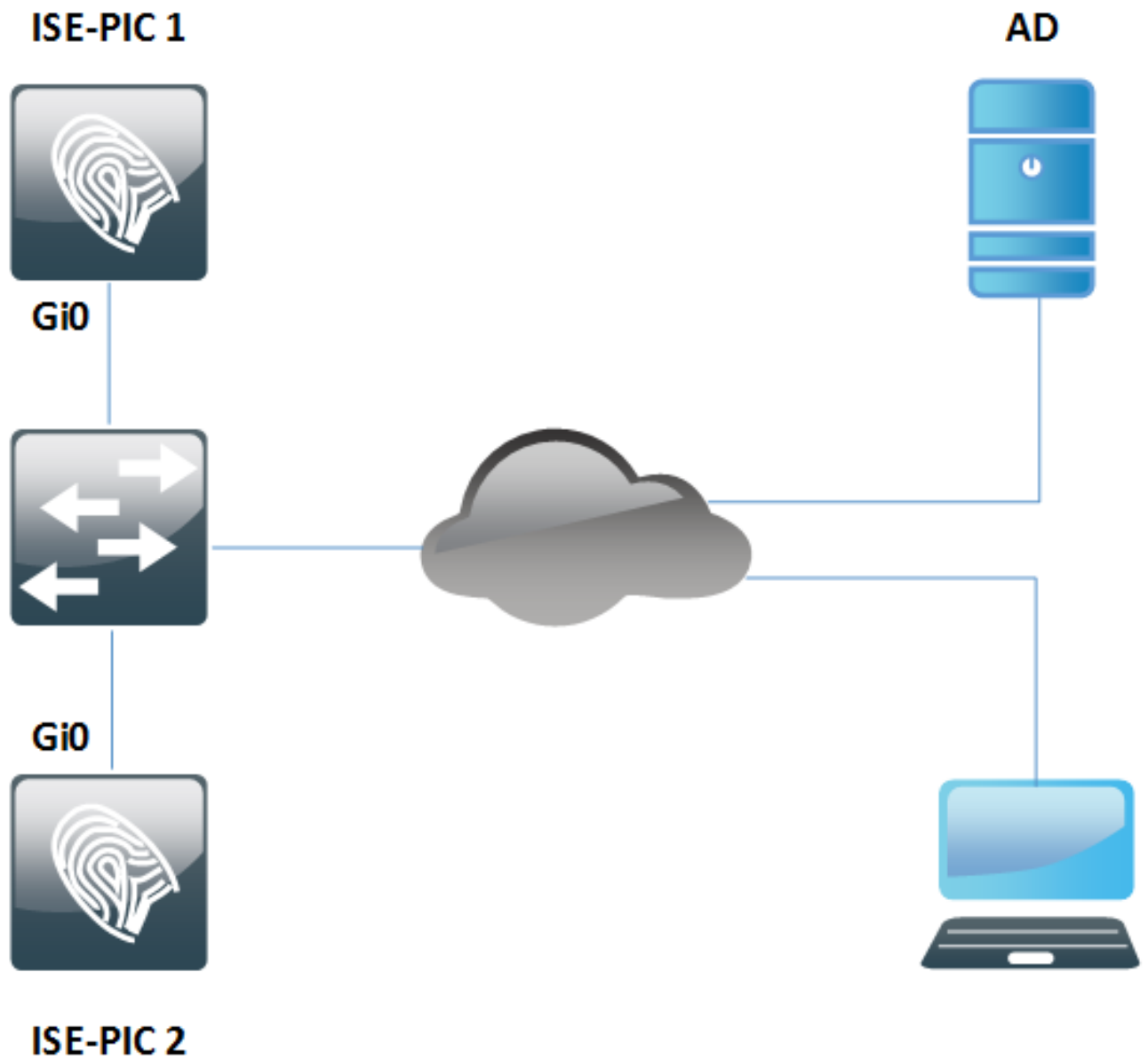
In questo esempio viene illustrato come configurare il provider WMI per Active Directory. WMI è costituito da un insieme di estensioni del modello di driver di Windows che fornisce un'interfaccia del sistema operativo tramite la quale i componenti instrumentati forniscono informazioni e notifiche. WMI è l'implementazione Microsoft degli standard WBEM (Web-Based Enterprise Management) e CIM (Common Information Model) della Distributed Management Task Force (DMTF).

Nota: Ulteriori informazioni su WMI sono disponibili sul sito ufficiale di Microsoft: [Informazioni](#)

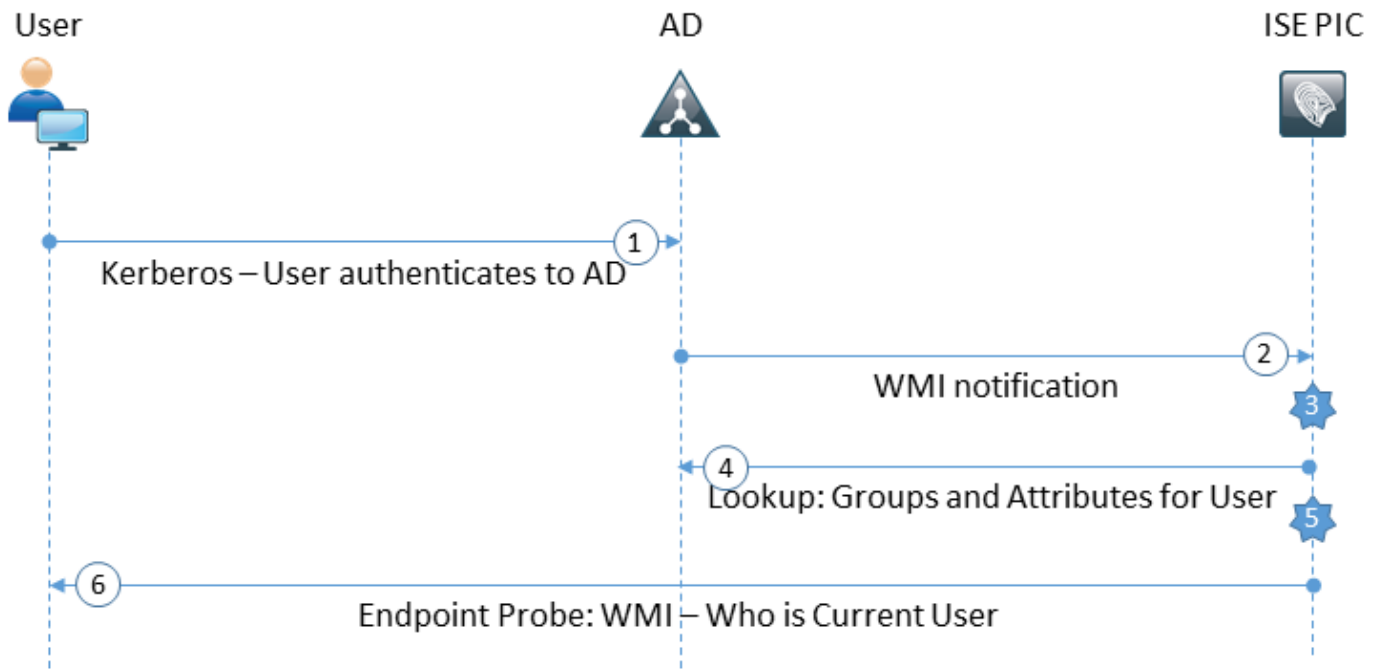
[su WMI](#)

Esempio di rete

Le informazioni contenute nel documento utilizzano le impostazioni di rete mostrate nell'immagine:



Flusso di lavoro



1. Accedere al PC e autenticarsi in Active Directory.
 2. WMI notifica ad ISE PIC questa autenticazione.
 3. ISE aggiunge il binding Username:IP_Address alla propria directory di sessione.
 4. ISE recupera i gruppi e gli attributi dell'utente da AD.
 5. ISE salva queste informazioni nella sua directory di sessione.
 6. Ogni 4 ore (non configurabile) ISE PIC esegue Endpoint Probe:
 Innanzitutto tenta di raggiungere l'endpoint tramite WMI. Se WMI non riesce, ISE PIC esegue ISEExec. Esegue una query sull'endpoint per l'utente e abilita WMI per la prossima volta. Anche ISE PIC recupera l'indirizzo MAC dell'endpoint e il tipo di sistema operativo.
- Con ISE PIC, è possibile solo abilitare/disabilitare le sonde per endpoint. Il nodo primario esegue una query su tutti gli endpoint. Il nodo secondario è solo per la disponibilità elevata.

Configurazione

Configurazione dell'installazione di ISE PIC

Passaggio 1 (facoltativo). Installa certificati attendibili.

È necessario installare la catena completa di certificati dell'Autorità di certificazione (CA) nell'archivio attendibile ISE. Effettuare il login alla GUI ISE PIC e selezionare **Certificati > Gestione certificati > Certificati attendibili**. Fare clic su **Importa** e selezionare il certificato della CA dal PC.

Come mostrato nell'immagine, fare clic su **Submit** (Invia) per salvare le modifiche. Ripetere questo

passaggio per tutti i certificati della catena. Ripetere i passaggi anche sul nodo secondario.

The screenshot shows the 'Certificates Authority' section of the Cisco ISE interface. The 'Trusted Certificates' tab is selected. The form is titled 'Import a new Certificate into the Certificate Store'. It includes a 'Certificate File' field with a 'Choose File' button and the filename 'WinServCer.cer'. Below this is a 'Friendly Name' text input field. The 'Trusted For' section contains 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'.

Passaggio 2 (facoltativo). Installa certificati di sistema.

Opzione 1. Certificati già generati da CA insieme alla chiave privata.

Passare a **Certificati > Gestione certificati > Certificati di sistema** e fare clic su **Importa**.

Selezionare **File certificato** e **File chiave privata**, immettere il campo *Password* se la chiave privata è crittografata.

Come mostrato nell'immagine, controllare le opzioni di **utilizzo**:

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: Poiché ISE PIC è basato su codice ISE e può essere facilmente convertito in ISE completo di tutte le funzionalità con le licenze appropriate, sono disponibili tutte le opzioni di utilizzo. **ISE PIC non utilizza** ruoli quali **Autenticazione EAP, RADIUS DTLS, SAML e Portal**.

Fare clic su **Invia** per installare il certificato. Ripetere questa procedura anche su un nodo secondario.

Nota: Tutti i servizi sul nodo ISE PIC vengono riavviati dopo l'importazione del certificato del server.

Opzione 2. Generare la richiesta di firma del certificato (CSR), firmarla con CA e associarsi all'ISE.

Passare alla pagina **Certificati > Gestione certificati > Richieste di firma del certificato** e fare clic su **Genera richieste di firma del certificato (CSR)**.

Selezionare il nodo e l'utilizzo, immettere gli altri campi, se necessario:

▼ 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)

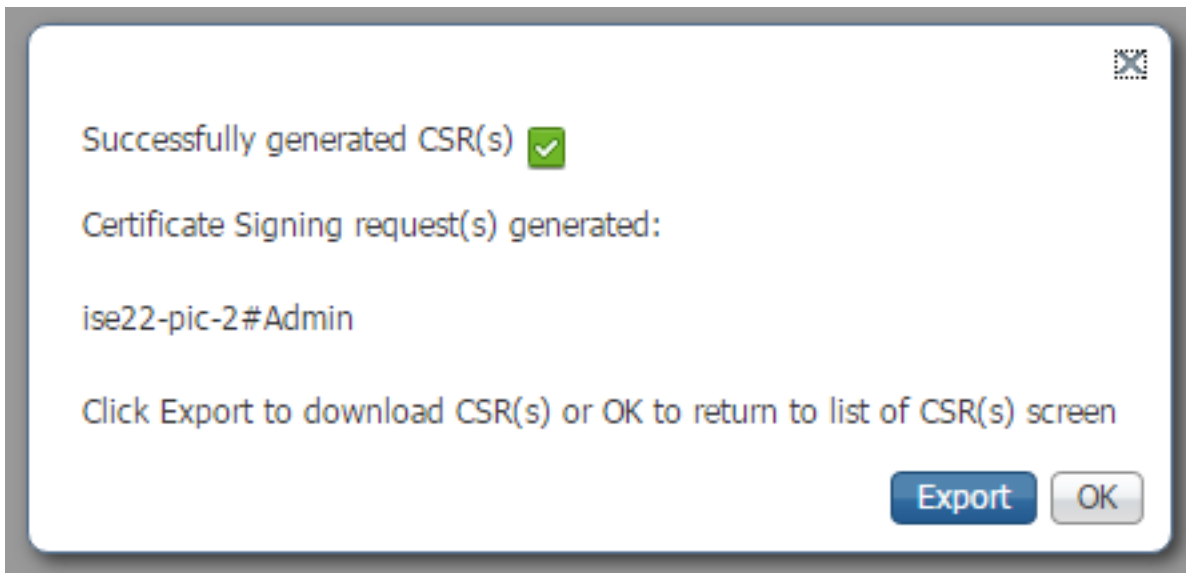
Subject Alternative Name (SAN) - + ⓘ

* Key Length

* Digest to Sign With

Certificate Policies

Fare clic su **Genera**. Viene visualizzata una nuova finestra con l'opzione **Esporta CSR** generato:



Fare clic su **Esporta**, salvare il file *.pem generato e firmarlo con CA. Dopo aver firmato CSR, tornare alla pagina **Certificati > Gestione certificati > Richieste di firma del certificato**, selezionare il CSR e fare clic su **Associa certificato**:

| | | | Bind Certificate | | |
|---|-----------------------------|------------|----------------------------------|------------------|-------------|
| <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 |

Selezionare il certificato firmato con la CA e fare clic su **Invia** per applicare le modifiche:

▼ Certificates Management ► Certificates Authority

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

Bind CA Signed Certificate

* Certificate File certnew.cer

Friendly Name ⓘ

Validate Certificate Extensions ⓘ

Usage

Admin: Use certificate to authenticate the ISE Admin Portal

Tutti i servizi sul nodo ISE PIC vengono riavviati dopo aver fatto clic su **Submit (Invia)** per installare il certificato.

Passaggio 3. Aggiungere il nodo secondario alla distribuzione.

ISE PIC prevede 2 nodi in un'implementazione per l'alta disponibilità. Non è necessario avere un trust bidirezionale tra certificati (rispetto alla normale distribuzione ISE). Per aggiungere un nodo secondario alla distribuzione, passare alla **pagina Amministrazione > Distribuzione** sul nodo principale ISE PIC, come mostrato nell'immagine:

Deployment | Licensing | Logging | Maintenance | 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 *

Immettere il nome di dominio completo (FQDN) del nodo secondario, le credenziali di amministratore del nodo e fare clic su **Salva**. Nel caso in cui il nodo primario ISE PIC non sia in grado di verificare il certificato di amministratore del secondo nodo, richiede la conferma prima di installare il certificato nell'archivio attendibile.

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

In questo caso, fare clic su **Importa certificato e procedere** per aggiungere il nodo alla distribuzione. È consigliabile ricevere una notifica che avvisa che il nodo è stato aggiunto correttamente. Tutti i servizi nel nodo secondario vengono riavviati.



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



Entro 10-20 minuti i nodi devono essere sincronizzati e lo stato del nodo deve essere modificato da **In corso** a **Connesso**:

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

Configura provider Active Directory

ISE PIC utilizza Strumentazione gestione Windows (WMI) per raccogliere informazioni sulle sessioni da AD e opera come una community Pub/Sub, il che significa:

- ISE PIC partecipa a determinati eventi
- WMI avvisa ISE PIC quando si verificano tali eventi: 4768 (concessione ticket Kerberos) e 4770 (rinnovo ticket Kerberos)Le voci nella directory di sessione scadono (Elimina)

Passaggio 1. Entra nel dominio ISE PIC.

Per aggiungere ISE PIC al dominio, selezionare **Provider > Active Directory**, quindi fare clic su **Add** (Aggiungi):

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

Connection

* Join Point Name test-AD

* Active Directory Domain vkumov.local

Submit Cancel

Compilare i campi **Nome punto di join** e **Dominio Active Directory** e fare clic su **Invia** per salvare le modifiche. **Nome punto di join** è un nome utilizzato solo in ISE PIC. **Dominio Active Directory** è il nome del dominio a cui deve essere aggiunto ISE PIC e deve essere risolvibile con il server DNS configurato su ISE PIC.

Dopo la creazione di Join Point ISE PIC dovrebbe chiedere se si desidera aggiungere nodi al dominio. Fare clic su **Sì**. Viene visualizzata una finestra che consente di fornire le credenziali per l'aggiunta al dominio:

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

Compilare i campi **Domain Administrator** e **Password** e fare clic su **OK**.

Anche se il campo è denominato **Domain Administrator**, non è necessario utilizzare l'utente amministratore per **aggiungere** l'ISE PIC al dominio. L'utente deve disporre di privilegi sufficienti per creare e rimuovere account computer nel dominio o per modificare le password per account computer creati in precedenza. In questo [documento](#) sono disponibili le autorizzazioni per account di Active Directory necessarie per eseguire diverse operazioni.

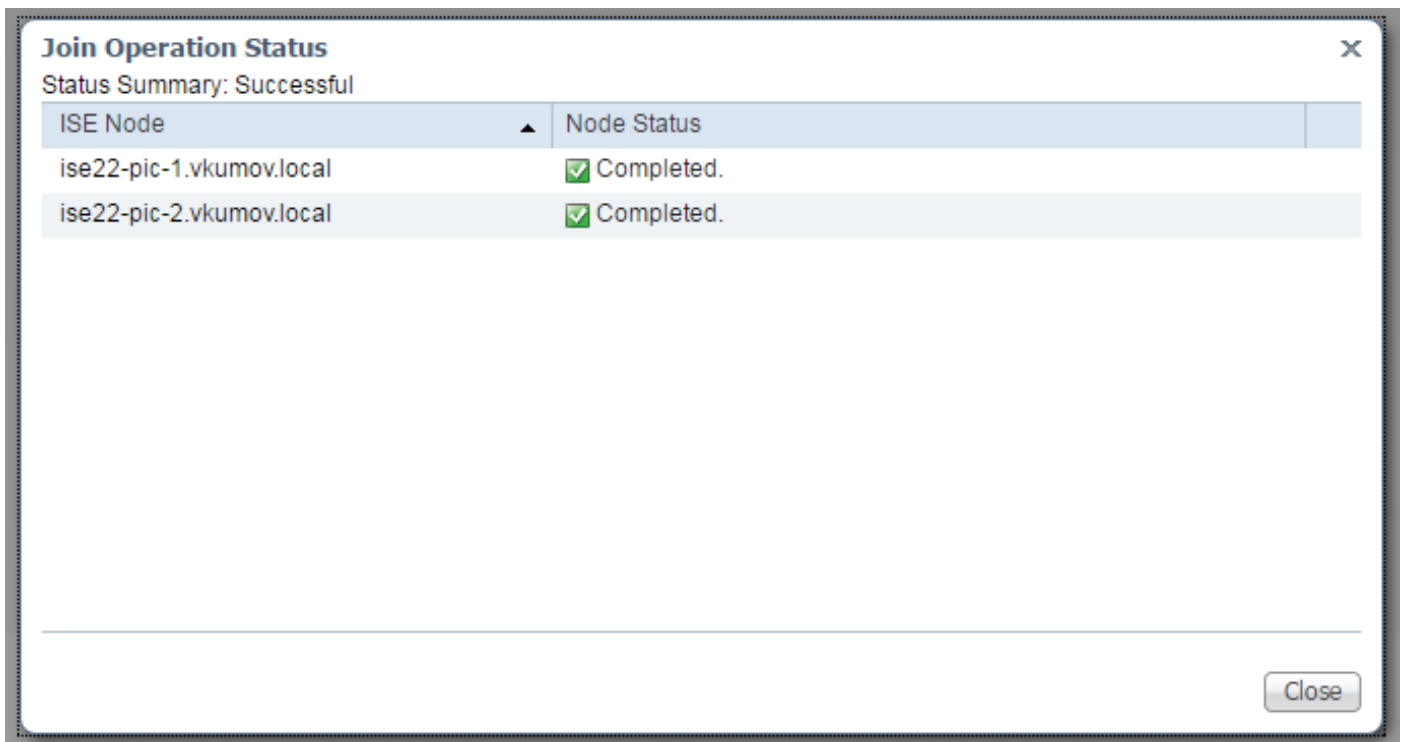
È tuttavia necessario utilizzare le credenziali di Domain Administrator durante l'aggiunta se si desidera utilizzare WMI. L'opzione **Config WMI** richiede:

- Modifiche del Registro di sistema
- Autorizzazioni per l'utilizzo di DCOM

- Autorizzazioni per l'utilizzo remoto di WMI
- Accesso per la lettura del registro eventi sicurezza del controller di dominio Active Directory
- Windows Firewall deve consentire il traffico da/verso ISE PIC (i criteri di Windows Firewall corrispondenti verranno creati durante **Config WMI**)

Nota: Store Credentials è sempre abilitato su ISE PIC poiché è richiesto per le sonde per endpoint e la configurazione WMI. ISE le memorizza internamente,

Come mostrato nell'immagine, ISE PIC mostra il risultato dell'operazione in una nuova finestra:



Passaggio 2. Ottimizzare le autorizzazioni in AD.

Verificare e ottimizzare le autorizzazioni per l'utente in Active Directory per il documento: [Guida all'installazione e amministrazione di Identity Services Engine Passive Identity Connector \(ISE-PIC\)](#):

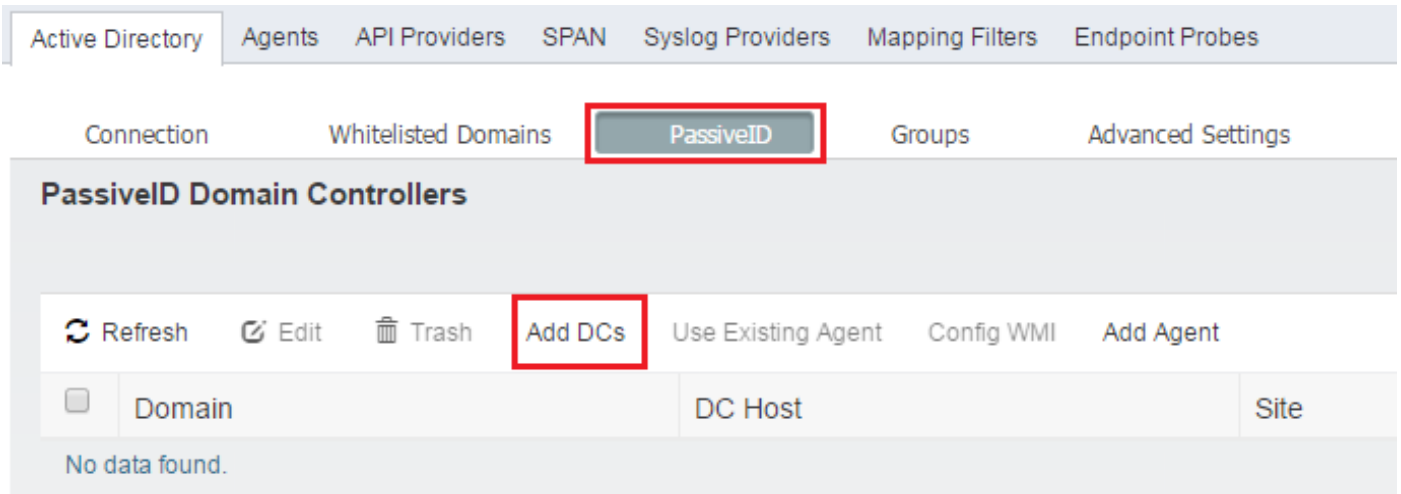
Imposta autorizzazioni per l'utente AD nel gruppo Domain Admin

Per impostazione predefinita, in Windows 2008 R2, Windows 2012 e Windows 2012 R2 il gruppo Domain Admin non dispone del controllo completo su determinate chiavi del Registro di sistema nel sistema operativo Windows. L'amministratore di Active Directory deve concedere all'utente di Active Directory autorizzazioni di controllo completo per la chiave del Registro di sistema seguente

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

Passaggio 3. Aggiungere gli agenti PassivID.

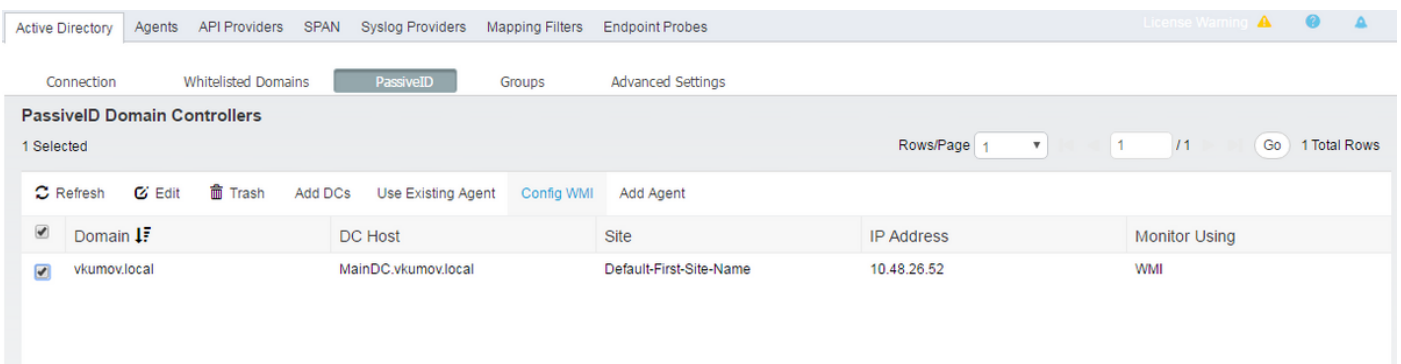
Nella pagina Dominio Active Directory passare alla scheda ID passivo e fare clic su **Aggiungi controller di dominio**, come mostrato nell'immagine:



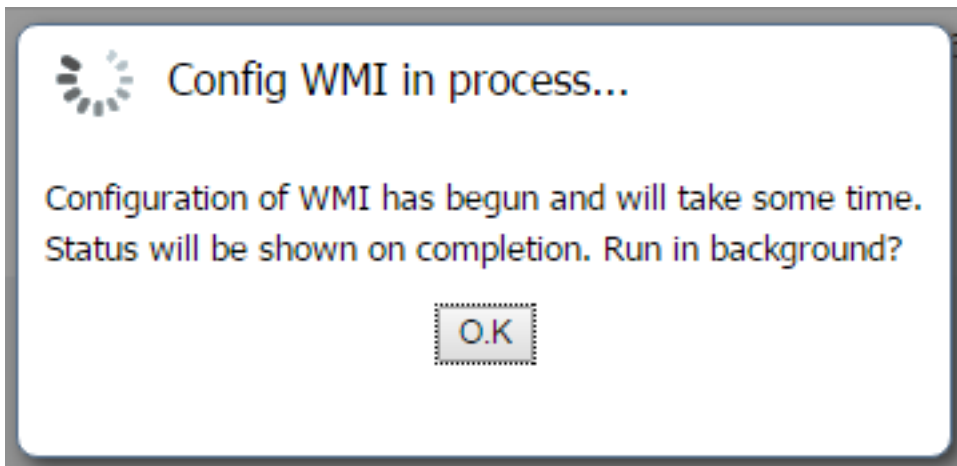
Viene visualizzata una nuova finestra e ISE carica un elenco di tutti i controller di dominio disponibili. Selezionare i controller di dominio in cui configurare WMI e fare clic su **OK** per salvare le modifiche, come mostrato nell'immagine:



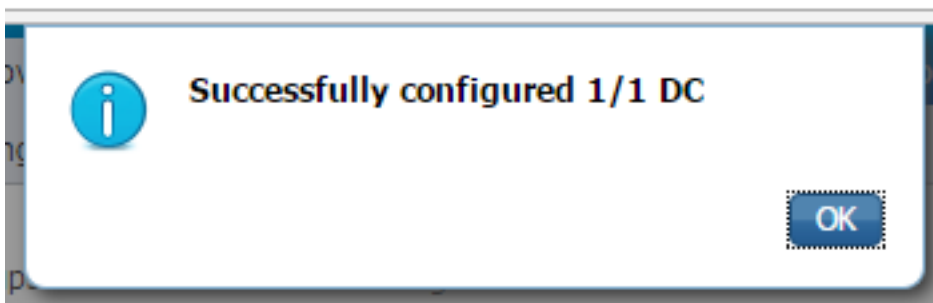
I controller di dominio selezionati vengono aggiunti all'elenco dei **controller di dominio con ID passivo**. **Selezionare i controller di dominio e fare clic sul pulsante Configura WMI:**



ISE PIC visualizza un messaggio indicante che è in corso un processo di configurazione:



Dopo alcuni minuti viene visualizzato un messaggio che indica che WMI è stato configurato correttamente nei controller di dominio selezionati:



Verifica

Implementazione


È possibile controllare lo stato della distribuzione in diversi modi:

Pagina Distribuzione


Passare alla **pagina Amministrazione > Distribuzione**. È possibile controllare lo stato corrente della distribuzione:

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.

Da questa pagina è possibile annullare la registrazione del nodo secondario, se necessario. È possibile avviare la sincronizzazione manuale e controllare lo stato della sincronizzazione.

Pagina Dashboard

Sulla pagina principale di ISE PIC è presente una dashlet chiamata **Subscribers**. Con questa dashlet è possibile controllare lo stato attuale dei nodi ISE PIC, come mostrato nell'immagine:

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 crea 2 iscritti per ciascun nodo - **admin** e **mnt**. Tutti devono essere in stato **Online** il che significa che i nodi sono raggiungibili e operativi.

Sottoscrittori

Subscribers page è una versione estesa della dashlet Subscribers dalla Home page di ISE PIC. Questa pagina mostra tutte le informazioni relative a pxGrid, tuttavia lo stato dei nodi ISE PIC può essere controllato anche qui:

ISE Passive Identity Connector | Home | Live Sessions | Providers | **Subscribers** | Certificates | Troubleshoot | Reports | Administration | Settings

Clients | Capabilities | Live Log | Settings | Certificates

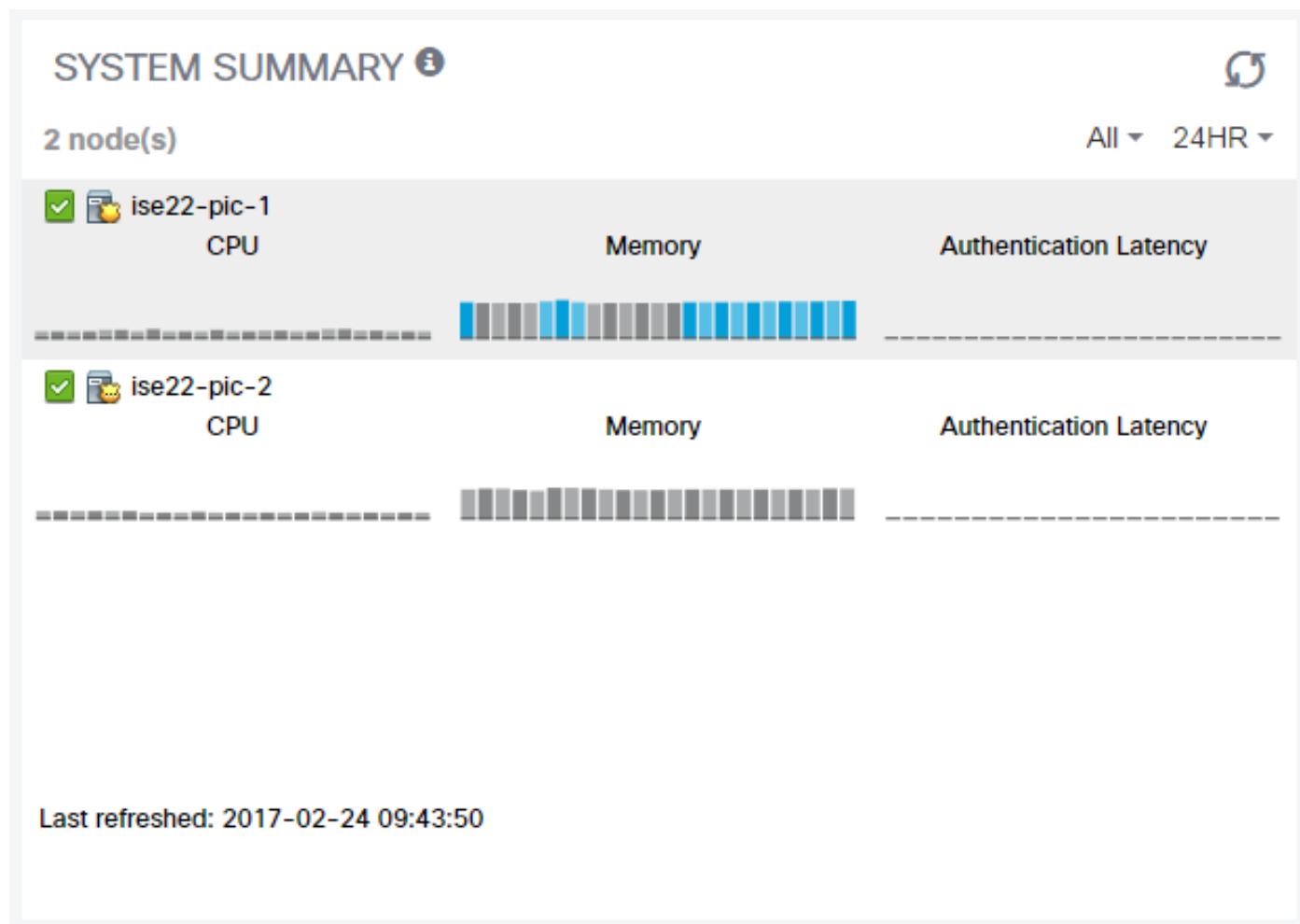
Enable
 Disable
 Approve
 Group
 Decline
 Delete
 Refresh
 Total Pending Approval(0)

| 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 |

Riepilogo del sistema

ISE PIC consente anche di monitorare il riepilogo dello stato dei nodi. Questa dashlet è disponibile

in Home > Dashboard > Ulteriori informazioni:



La latenza di autenticazione è sempre di 0 ms in quanto ISE PIC non esegue alcuna autenticazione/autorizzazione.

Provider e sessioni

Home page

Gli stati dei provider, la loro quantità e la quantità di sessioni trovate possono essere controllati mentre si passa alla **pagina Home > Dashboard**:

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 |

Sessioni Live

Informazioni dettagliate su tutte le sessioni degli utenti trovate sono disponibili nella pagina **Live Sessions**:

| 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... |

Contiene informazioni quali:

- Provider - Provider utilizzati per identificare la sessione
- Avviata e aggiornata - timestamp dell'avvio e dell'aggiornamento della sessione
- Indirizzo IP - Indirizzo dell'endpoint
- Azione: azioni che ISE può eseguire (ad esempio, controllare lo stato dell'endpoint o se ISE

PIC è integrato con pxGrid, inviare una richiesta di cancellazione della sessione)

Risoluzione dei problemi

Implementazione

Per risolvere i problemi relativi alla distribuzione e alla replica, esaminare i seguenti file di registro:

- replica.log
- distribuzione.log
- ise-psc.log

Per abilitare i debug, selezionare **Amministrazione > Registrazione > Configurazione log di debug**:

[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 |

Questi debug vengono scritti nel file **replication.log**. Di seguito è riportato un esempio di un normale processo di replica:

```
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]
```

Messaggio da 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:
SYNC_COMPLETED
```

Problema comune: nodo secondario non raggiungibile

Se il nodo secondario diventa irraggiungibile, viene visualizzato nella **pagina Amministrazione > Distribuzione**:

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 contiene il seguente messaggio:

```
2017-02-24 10:43:21,587 INFO [admin-http-pool155][]
admin.restui.features.deployment.DeploymentIDCUIApi -:::- Replication status for node ise22-
pic-2 = NODE NOT REACHABLE
```

Questo messaggio spiega ciò che non è raggiungibile, ad esempio il nodo non risponde al ping:

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

Azioni da intraprendere: verificare se l'FQDN del nodo secondario è risolvibile, controllare la connettività di rete di base tra i nodi.

Se le applicazioni non sono in esecuzione sul nodo secondario o è presente un firewall tra i nodi, **ise-psc.log** può visualizzare i messaggi seguenti:

```
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

```

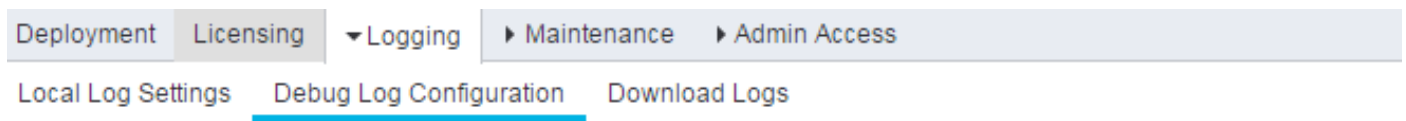
Azioni da eseguire: verificare lo stato dell'applicazione nel nodo secondario, controllare la connettività di rete se tutte le connessioni sono consentite tra i nodi.

Active Directory e WMI

Per risolvere i problemi relativi all'analisi di tali file da parte di WMI di Active Directory:

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

I debug utili possono essere abilitati selezionando **Amministrazione > Registrazione > Configurazione log di debug:**



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

| 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 |

E:

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

Di seguito è riportato un esempio di una nuova sessione appresa da **passive-wmi.log** con debug abilitati:

```
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, 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:\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, 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.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:\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::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
```

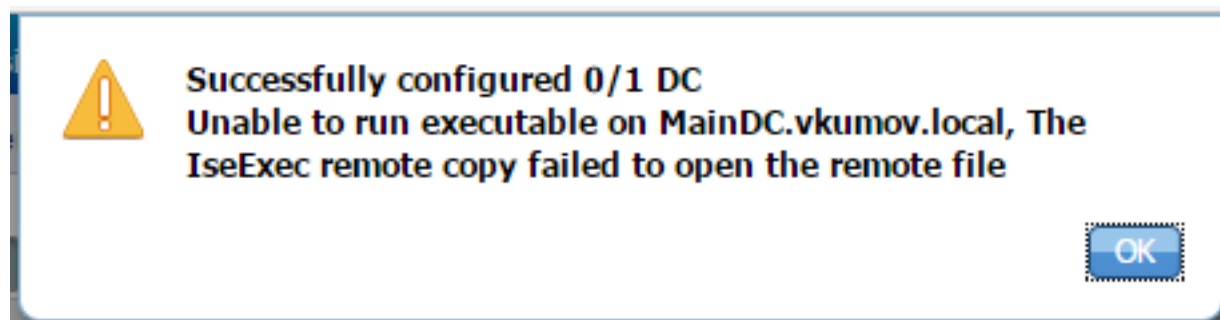
Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.event-user-name = Administrator ,
Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-
pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,

Esempio di controllo endpoint da **passive-endpoint.log** (in questo caso l'endpoint non è raggiungibile da 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
```

Problema comune: ISE PIC visualizza "Impossibile eseguire l'eseguibile su <nome controller di dominio>..." errore

Se l'utente utilizzato per aggiungere ISE PIC al dominio non dispone di autorizzazioni sufficienti, ISE PIC genera un errore durante la configurazione WMI:



I debug appropriati sono disponibili nel file **ad_agent.log** (il livello di log di Active Directory deve essere impostato su DEBUG):

```
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
```

Azioni da eseguire: aggiungere nuovamente i nodi ISE PIC al dominio con le credenziali di amministratore di dominio o aggiungere l'utente utilizzato per l'operazione di aggiunta al gruppo

Domain Admins in Active Directory.