

使用Active Directory WMI提供程式配置ISE 2.2 PIC

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[網路圖表](#)

[工作流程](#)

[設定](#)

[配置ISE PIC部署](#)

[第1步 \(可選\)。安裝受信任的證書。](#)

[第2步 \(可選\)。安裝系統證書。](#)

[步驟3.將輔助節點新增到部署中。](#)

[配置Active Directory提供程式](#)

[步驟1.將ISE PIC加入域。](#)

[步驟2.調整AD許可權。](#)

[步驟3.新增PassiveID代理。](#)

[驗證](#)

[部署](#)

[部署頁面](#)

[儀表板頁](#)

[訂閱者](#)

[系統摘要](#)

[提供商和會話](#)

[首頁](#)

[即時會話](#)

[疑難排解](#)

[部署](#)

[常見問題：輔助節點無法訪問](#)

[Active Directory和WMI](#)

[常見問題：ISE PIC拋出「無法在上運行執行檔](#)

簡介

本文檔介紹如何使用Active Directory Windows Management Instrumentation(AD WMI)提供程式配置身份服務引擎被動身份連結器(ISE PIC)部署並對其進行故障排除。ISE PIC是關注被動ID功能的輕量ISE版本。

ISE PIC是僅使用被動身份的所有思科安全產品組合的單ID解決方案。這意味著無法在ISE PIC上配置授權或策略。它支援不同的提供程式 (代理、WMI、系統日誌、API) , 並可通過REST API進行

整合。它具有查詢端點的功能(使用者是否登入？終端是否仍然連線？)

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- 思科身分識別服務引擎
- Microsoft Active Directory
- Microsoft WMI

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎被動身分識別連結器版本2.2.0.470
- Microsoft Windows 7 Service Pack 1
- Microsoft Windows Server 2012 r2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

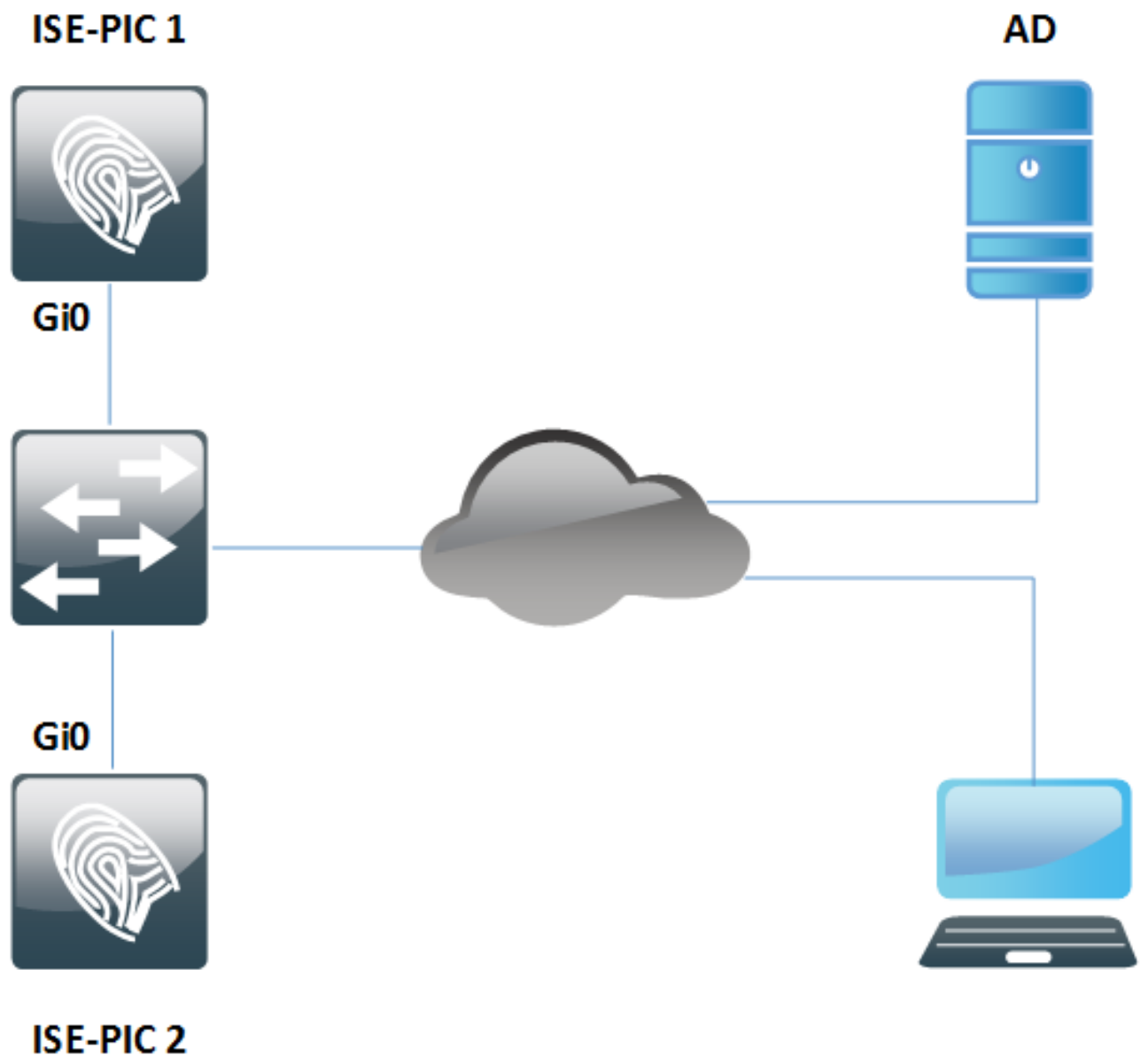
ISE PIC部署中的最大節點數量為2。此示例說明如何配置ISE PIC部署以實現高可用性，從而使用2個虛擬機器(VM)。在ISE PIC部署中，節點可以具有以下角色：主要和輔助。在此模式下，一次只能有一個節點為主節點，並且只能通過GUI手動更改角色。如果主裝置發生故障，除UI外，所有功能仍會在輔助裝置上運行。只有手動提升為主使用者才能啟用使用者介面。

此示例說明如何為Active Directory配置WMI提供程式。WMI包含一組對Windows驅動程式模型的擴展，這些擴展提供一個作業系統介面，通過這個介面被檢測的元件提供資訊和通知。WMI是Microsoft從分散式管理任務組(DMTF)實施的基於Web的企業管理(WBEM)和通用資訊模型(CIM)標準。

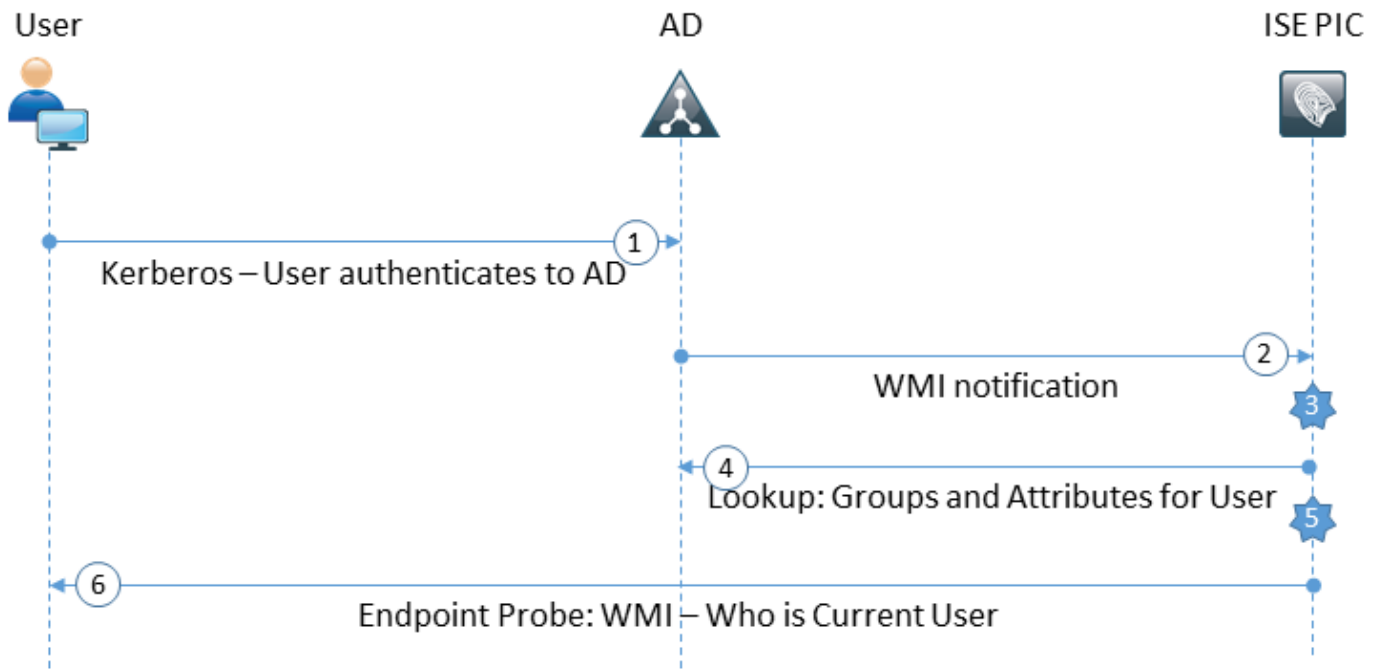
附註：有關WMI的詳細資訊可以在官方Microsoft站點上找到：[關於WMI](#)

網路圖表

檔案中的資訊使用圖中所示的網路設定：



工作流程



1. 登入到PC並在AD上通過身份驗證。
2. WMI通知ISE PIC有關此身份驗證。
3. ISE將繫結Username:IP_Address新增到其會話目錄。
4. ISE從AD檢索使用者組和屬性。
5. ISE將此資訊儲存到其會話目錄中。
6. 每4小時 (不可配置) ISE PIC運行終端探測：
 - 首先，它嘗試通過WMI訪問終結點。如果WMI失敗，則ISE PIC運行ISExec。它將查詢使用者的終結點並啟用下一次的WMI。此外，ISE PIC會檢索終端和作業系統型別的MAC地址。

在ISE PIC中，僅可以啟用/禁用終端探測。主節點查詢所有端點，輔助節點僅用於高可用性。

設定

配置ISE PIC部署

第1步 (可選)。安裝受信任的證書。

應將證書頒發機構(CA)的完整證書鏈安裝到ISE受信任儲存。登入到ISE PIC GUI並導航到**證書>證書管理>受信任證書**。按一下**Import**，然後從您的PC中選擇您的CA證書。

如圖所示，按一下**Submit**以儲存變更。對鏈結的所有憑證重複此步驟。在輔助節點上重複步驟。

Import a new Certificate into the Certificate Store

* Certificate File WinServCer.cer

Friendly Name



Trusted For:

Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

第2步 (可選)。 安裝系統證書。

選項1:CA已連同私鑰一起產生的憑證。

導覽至**Certificates > Certificates Management > System Certificates**，然後按一下**Import**。選擇**Certificate File**和**Private Key File**，如果私鑰已加密，請輸入**Password**欄位。

如下圖所示，勾選「Usage」選項：

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

附註：由於ISE PIC基於ISE代碼，可以輕鬆轉換為具有相應許可證的全功能ISE，因此所有使用選項均可用。ISE PIC不使用**EAP身份驗證**、**RADIUS DTLS**、**SAML**和**門戶**等角色。

按一下**Submit**安裝證書。在輔助節點上也重複此過程。

附註：ISE PIC節點上的所有服務在伺服器證書匯入後重新啟動。

選項2.生成證書簽名請求(CSR)，使用CA對其進行簽名並在ISE上繫結。

導覽至**Certificates > Certificates Management > Certificate Signing Requests**頁面，然後按一下**Generate Certificate Signing Requests(CSR)**。

選擇節點和使用情況，如果需要，輸入其他欄位：

▼ 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)

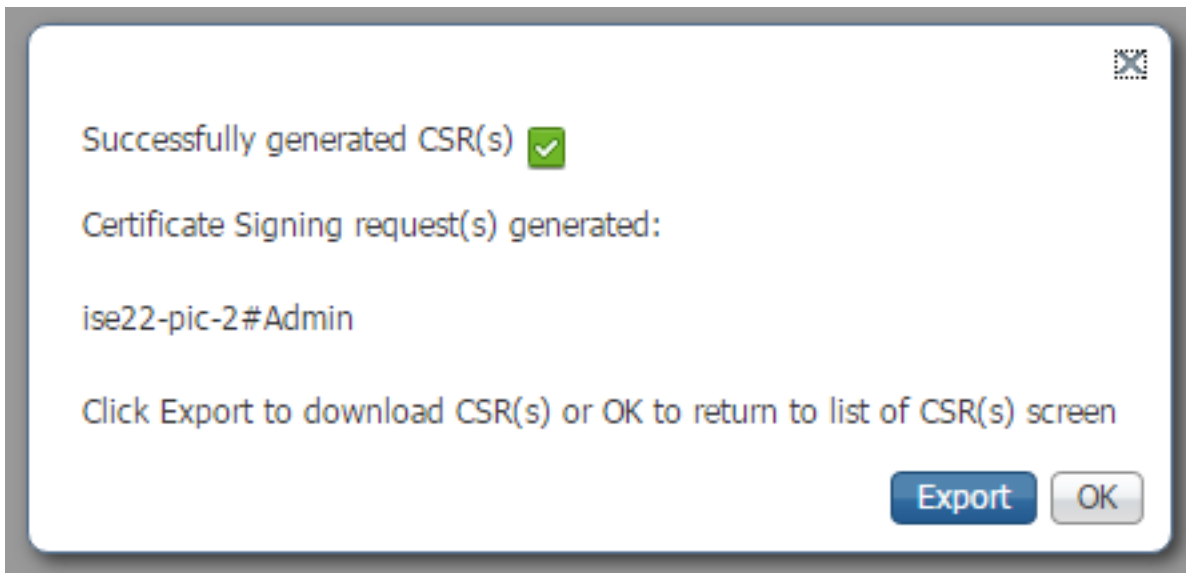
Subject Alternative Name (SAN) - + ⓘ

* Key Length

* Digest to Sign With

Certificate Policies

按一下「Generate」。系統隨即會彈出新視窗，並顯示Export generated CSR:



按一下「**Export**」，儲存產生的*.pem檔案，然後使用CA對其進行簽名。簽署CSR後，導覽回憑證 >憑證管理>憑證簽署請求頁面，選擇您的CSR，然後按一下**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

選擇與您的CA簽名的證書，然後按一下**Submit**以應用更改：

▼ 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

按一下**Submit**安裝證書後，ISE PIC節點上的所有服務都會重新啟動。

步驟3.將輔助節點新增到部署中。

ISE PIC允許在部署中具有2個節點以實現高可用性。它不需要具有雙向證書信任（與常規ISE部署

相比)。要將輔助節點新增到部署，請在主ISE PIC節點上導航到**管理>部署**頁面，如下圖所示：

The screenshot shows the 'Deployment' page in the ISE management interface. At the top, there is a navigation bar with tabs for 'Deployment', 'Licensing', 'Logging', 'Maintenance', and 'Admin Access'. Below this, the 'This Node' section displays the current node's configuration: Role is 'Standalone', IP Address is '10.48.26.51', and FQDN is 'ise22-pic-1.vkumov.local'. The 'Add Secondary Node' section contains three input fields: 'FQDN *' with the value 'ise22-pic-2.vkumov.local', 'User Name *' with the value 'admin', and 'Password *' with masked characters '.....'. At the bottom right of the form are two buttons: 'Cancel' and 'Save'.

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

Add Secondary Node

FQDN * ise22-pic-2.vkumov.local

User Name * admin

Password *

Cancel Save

輸入輔助節點的完全限定域名(FQDN)以及該節點的管理員憑據，然後按一下**儲存**。如果主ISE PIC節點無法驗證第二個節點的管理員證書，它會在受信任儲存中安裝證書之前要求確認。

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

在這種情況下，按一下**Import Certificate and Proceed**將節點加入部署。您應該會收到已成功新增節點的通知。輔助節點上的所有服務都會重新啟動。



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

OK



應在10-20分鐘內同步節點，且節點的狀態應從 **進行中** 成長至 **已連線**：

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

配置Active Directory提供程式

ISE PIC使用Windows Management Instrumentation(WMI)從AD收集有關會話的資訊，並像Pub/Sub通訊一樣工作，這意味著：

- ISE PIC訂閱某些事件
- 發生以下事件時WMI會向ISE PIC發出警報：4768 (Kerberos票證授予) 和4770 (Kerberos票證續訂) 會話目錄中的條目過期 (清除)

步驟1.將ISE PIC加入域。

若要將ISE PIC加入域，請導航到**Providers > Active Directory**並按一下**Add**：

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

填充**加入點名稱**和**Active Directory域**欄位，然後按一下**Submit**以儲存更改。**連線點名稱**是僅在ISE PIC中使用的名稱。**Active Directory域**是應加入ISE PIC的域的名稱，它應該能夠通過ISE PIC上配置的DNS伺服器進行解析。

建立加入點後，ISE PIC應詢問您是否希望將節點加入域。按一下**Yes (是)**。應彈出一個視窗，以便您提供加入域的憑據：

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

填充**域管理員**和**密碼**欄位，然後按一下**確定**。

即使該欄位名為**域管理員**，也無需使用管理員使用者將ISE PIC加入域。此使用者應具有足夠的許可權，可以在域中建立和刪除電腦帳戶，或者更改以前建立的電腦帳戶的密碼。執行各種操作所需的Active Directory帳戶許可權可以在本文檔中找到。

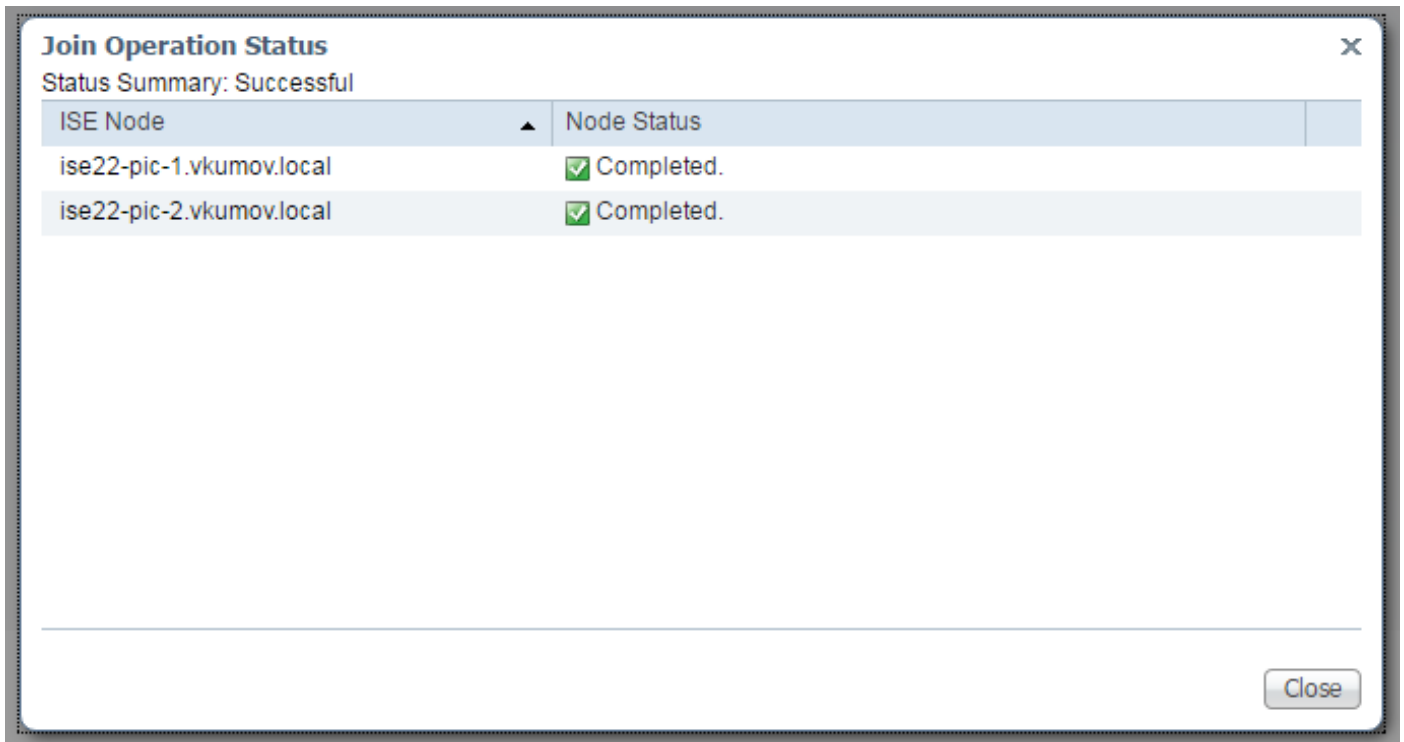
但是，如果您想要使用WMI，則需要在加入期間使用域管理員憑據。**Config WMI**選項要求：

- 登錄檔更改
- 使用DCOM的許可權
- 遠端使用WMI的許可權
- 有權讀取AD域控制器的安全事件日誌

- Windows防火牆必須允許來自/發往ISE PIC的流量(在配置WMI期間將建立相應的Windows防火牆策略)

附註：由於端點探測和WMI配置需要儲存憑據，因此始終在ISE PIC上啟用儲存憑據。ISE在內部對其進行加密儲存。

如圖所示，ISE PIC在新視窗中顯示操作結果：



步驟2.調整AD許可權。

根據文檔檢查並調整使用者對AD的許可權：[身份服務引擎被動身份連結器\(ISE-PIC\)安裝和管理員指南](#)：

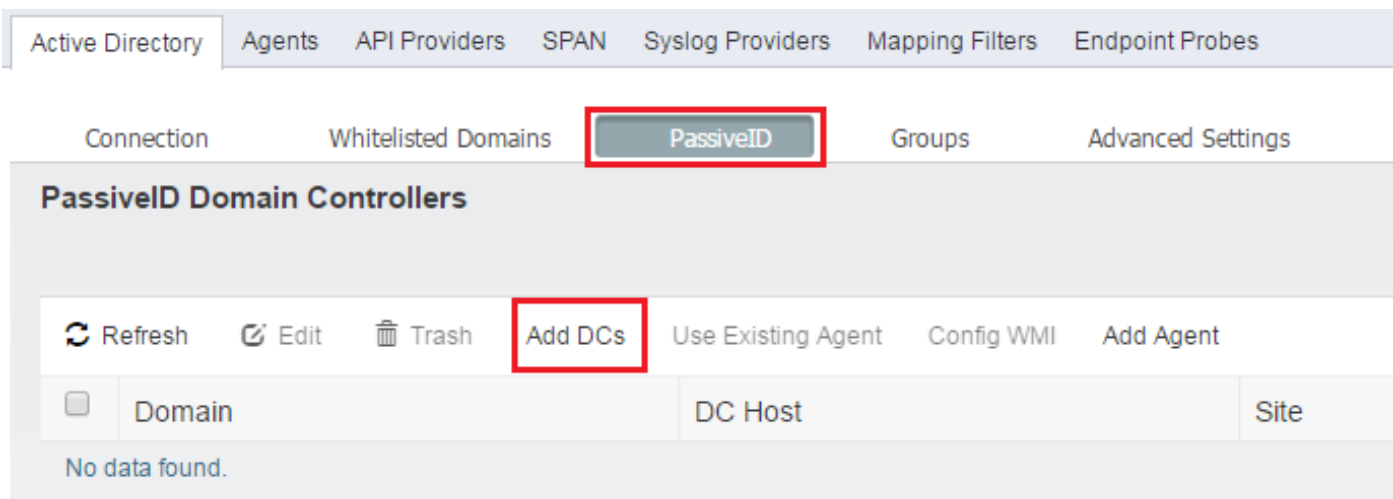
在域管理組中的AD使用者時設定許可權

對於Windows 2008 R2、Windows 2012和Windows 2012 R2，預設情況下，域管理組對Windows作業系統中的某些登錄檔項沒有完全控制。Active Directory管理員必須向Active Directory使用者授予對下列登錄檔項的完全控制許可權

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

步驟3.新增PassiveID代理。

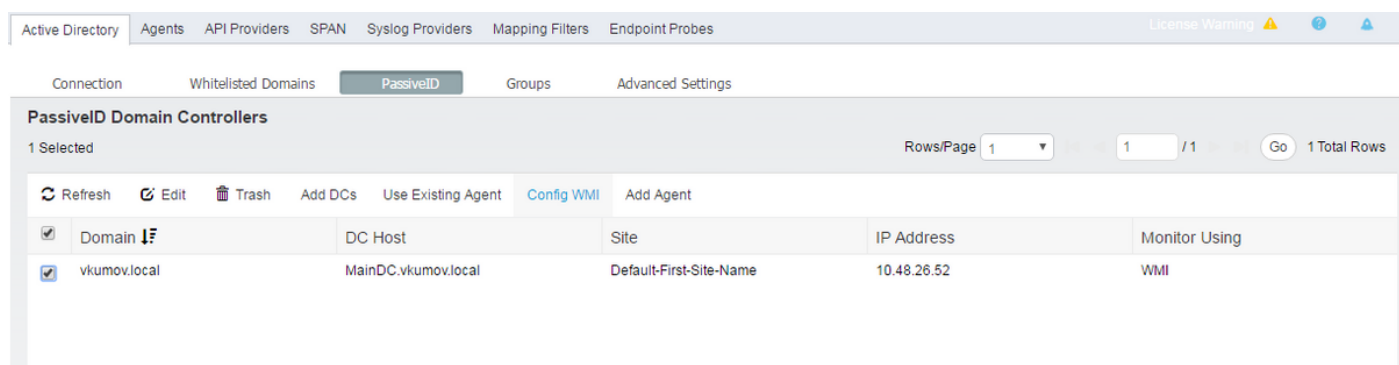
在AD域頁面上，導航到PassiveID頁籤，然後點選Add DC，如下圖所示：



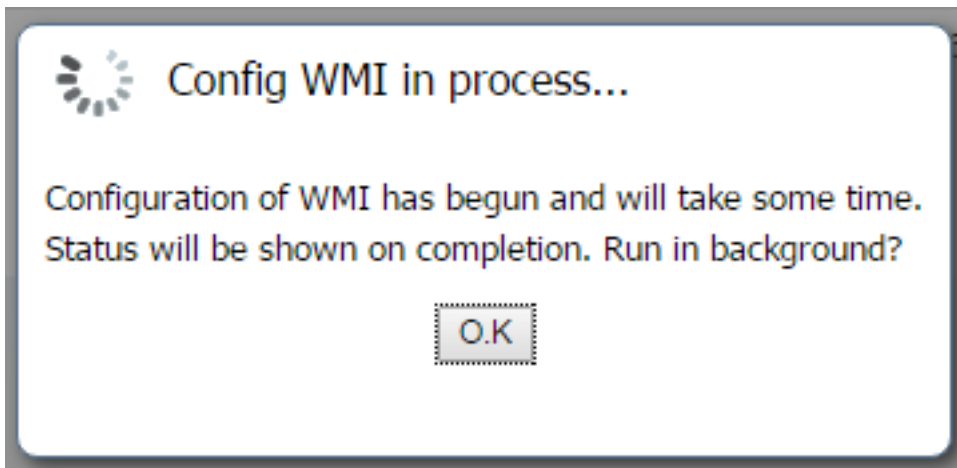
系統彈出一個新視窗，ISE載入所有可用域控制器的清單。選擇要配置WMI的DC，然後按一下OK以儲存更改，如下圖所示：



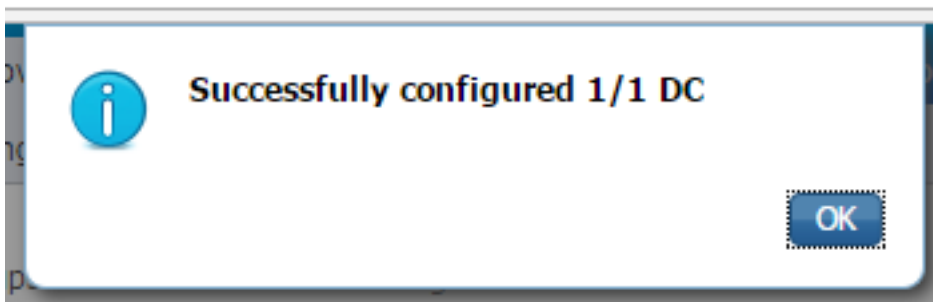
選定的DC將新增到PassiveID域控制器的清單中。選擇您的DC，然後按一下Config WMI 按鈕：



ISE PIC顯示一條消息，說明配置過程正在進行：



幾分鐘後，它向您顯示一條消息，表明已在選定的DC上成功配置WMI:



驗證

部署


可以通過幾種方法檢查部署狀態：

部署頁面


導航到**管理>部署**頁，可以檢查部署的當前狀態：

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.

如果需要，可從此頁面取消註冊輔助節點。可以啟動手動同步並**檢查同步狀態**。

儀表板頁

在ISE PIC首頁面上，有一個名為**Subscribers**的Dashlet。通過此dashlet，您可以檢查ISE PIC節點的當前狀態，如下圖所示：

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為每個節點建立2個訂戶 — admin和mnt。所有節點都應處於Online 狀態，這意味著節點可訪問且運行正常。

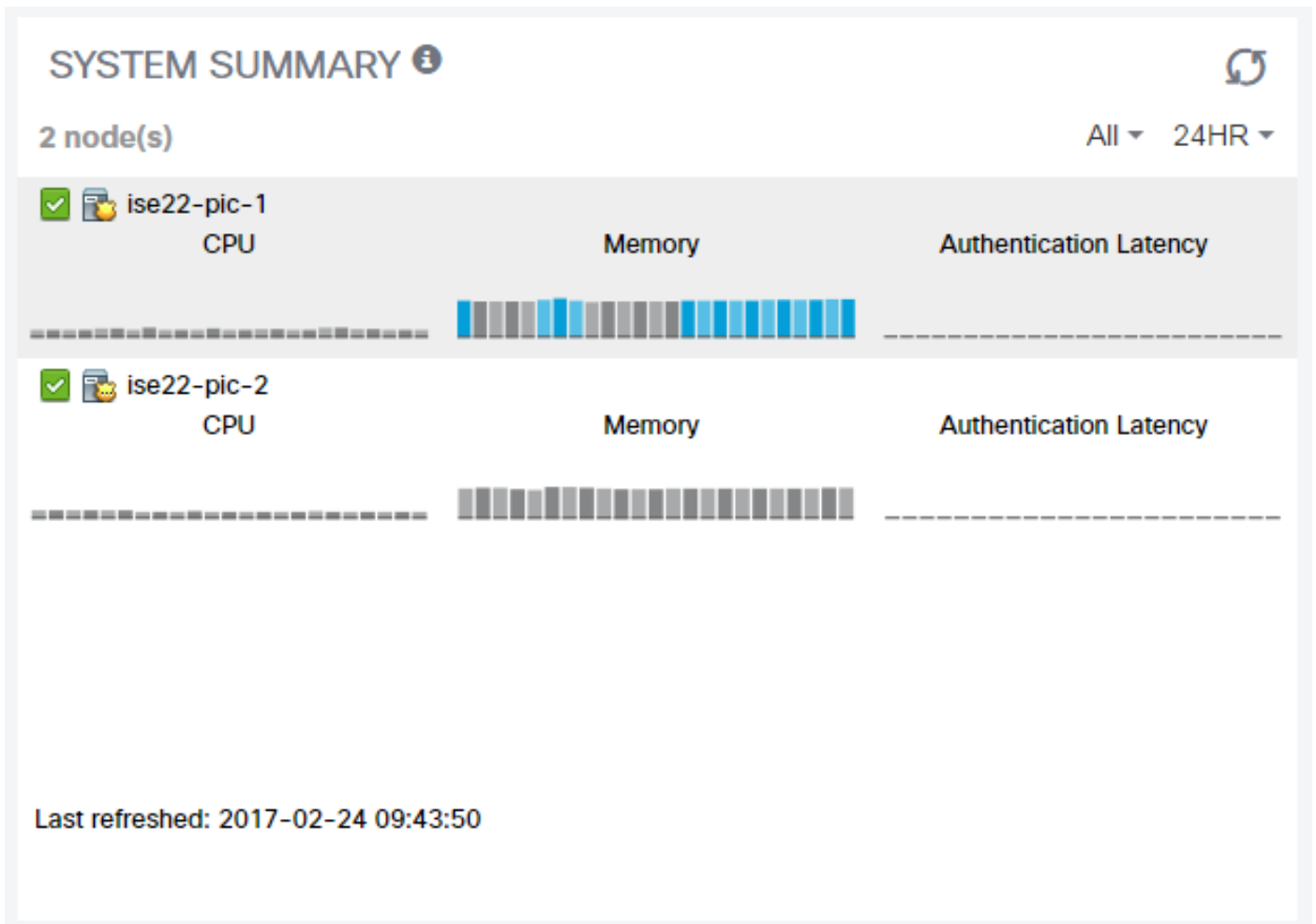
訂閱者

訂閱者頁面是來自ISE PIC首頁的訂戶dashlet的擴展版本。此頁顯示所有與pxGrid相關的內容，但也可在此處檢查ISE PIC節點的狀態：

Cisco ISE Passive Identity Connector						
Clients						
<input type="checkbox"/>	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
<input type="checkbox"/>	ise-mnt-ise22-pic-2		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
<input type="checkbox"/>	ise-mnt-ise22-pic-1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
<input type="checkbox"/>	ise-admin-ise22-pic-1		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate
Capability Detail						
			1 - 8 of 8 Show 25 per page			
<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

系統摘要

ISE PIC還允許監控節點的運行狀況摘要。此Dashlet位於Home > Dashboard > Additional:



身份驗證延遲始終為0ms，因為ISE PIC不執行任何身份驗證/授權。

提供商和會話

首頁

導航到Home > Dashboard頁時，可以檢查提供程式狀態、其找到的會話的數量和數量：

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

即時會話

有關所有找到的使用者會話的詳細資訊，請參閱即時會話頁面：

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...

包含以下資訊：

- 提供程式 — 用於標識此會話的提供程式
- 啟動和更新 — 啟動和相應地更新會話的時間戳
- IP地址 — 終端的地址
- 操作 — ISE可以執行的操作（例如，檢查終端狀態，或者如果ISE PIC與pxGrid整合，則傳送請求以清除會話）

疑難排解

部署

若要解決部署和複製問題，請檢視以下日誌檔案：

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

若要啟用調試，請導航到**管理>記錄>調試日誌配置**：

[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

這些調試將寫入**replication.log**檔案。以下是正常複製過程的示例：

```
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]
```

來自ise-psc.log的消息：

```
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
```

常見問題：輔助節點無法訪問

如果輔助節點無法訪問，則將顯示在**管理>部署**頁面：

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 **✘ 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包含以下消息：

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

以下訊息說明無法到達的專案，例如節點沒有回應ping:

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

要採取的操作：檢查全域性節點的FQDN是否可解析，檢查節點之間的基本網路連線。

如果應用程式在輔助節點上未處於運行狀態，或節點之間存在防火牆，則**ise-psc.log**可能會顯示以下消息：

```
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

```

要執行的操作：檢查輔助節點上的應用狀態，如果允許節點間的所有連線，則檢查網路連線。

Active Directory和WMI

要對Active Directory WMI進行故障排除，請查詢這些檔案：

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

而且可以在Administration > Logging > Debug Log Configuration中啟用有用的調試：

The screenshot shows the 'Debug Log Configuration' page for the node 'ise22-pic-2.vkumov.local'. The page has a navigation bar with 'Deployment', 'Licensing', 'Logging', 'Maintenance', and 'Admin Access'. Below the navigation bar are 'Local Log Settings', 'Debug Log Configuration', and 'Download Logs'. The main content area shows a table of components and their log levels. The 'PassiveID' component is highlighted with a red box, showing its log level is set to 'DEBUG'.

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

和：

The screenshot shows the 'Active Directory' component with its log level set to 'DEBUG'. The description is 'Active Directory client internal messages'.

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

以下是啟用調試的從passive-wmi.log獲取的新會話的示例：

```

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, 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, 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\Administrator
\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:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
, Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current
events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity
Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.dc-host =
MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-pic-2 , Identity
Mapping.event-ip-address = 10.48.26.52 ,
2017-02-24 11:36:22,589 DEBUG [Thread-11][] com.cisco.idc.dc-probe- Received login event.
Identity Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0,
76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0,
69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2,
0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1,
1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
```

```

{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12", "2", ":", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t:1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
, Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current
events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = :1 , Identity
Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.event-user-name = Administrator ,
Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-
pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,

```

從passive-endpoint.log進行端點檢查的示例（在這種情況下，無法從ISE訪問端點）：

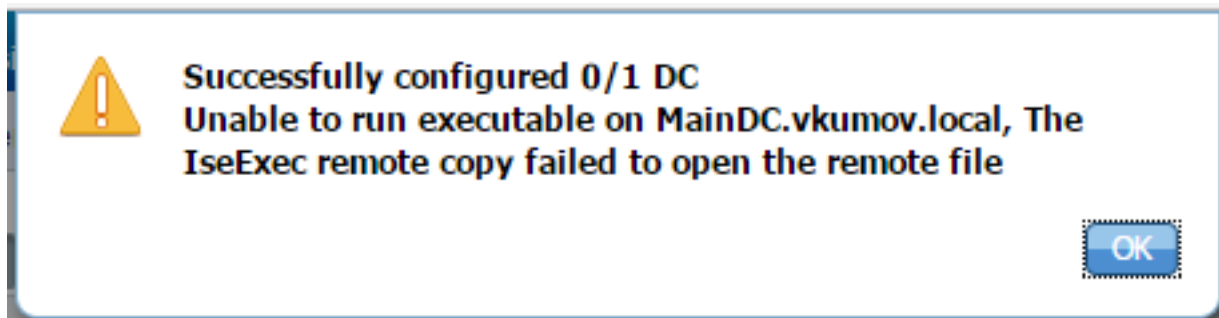
```

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

```

常見問題：ISE PIC拋出「無法在<DC名稱>上運行執行檔.....」 錯誤

如果用於將ISE PIC加入域的使用者沒有足夠的許可權，ISE PIC會在WMI配置過程中引發錯誤：



可以在ad_agent.log檔案中找到適當的調試 (Active Directory日誌級別應設定為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
```

要執行的操作：使用域管理員憑據將ISE PIC節點重新加入域，或將用於加入操作的使用者新增到AD中的域管理員組。