配置基於EVT的身份服務引擎被動ID代理

目錄

簡介

本文檔介紹在ISE 3.0版本中引入的新ISE被動身份聯結器(ISE-PIC)代理、其優勢以及此代理在ISE上的配置。ISE被動身份代理也已成為使用Cisco FirePower Management Center的身份防火牆解決方案的組成部分。

必要條件

需求

思科建議您瞭解以下主題：

- 思科身份服務管理
- MS-RPC、WMI協定
- Active Directory管理

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身份服務引擎3.0及更高版本
- Microsoft Windows Server 2016標準版

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

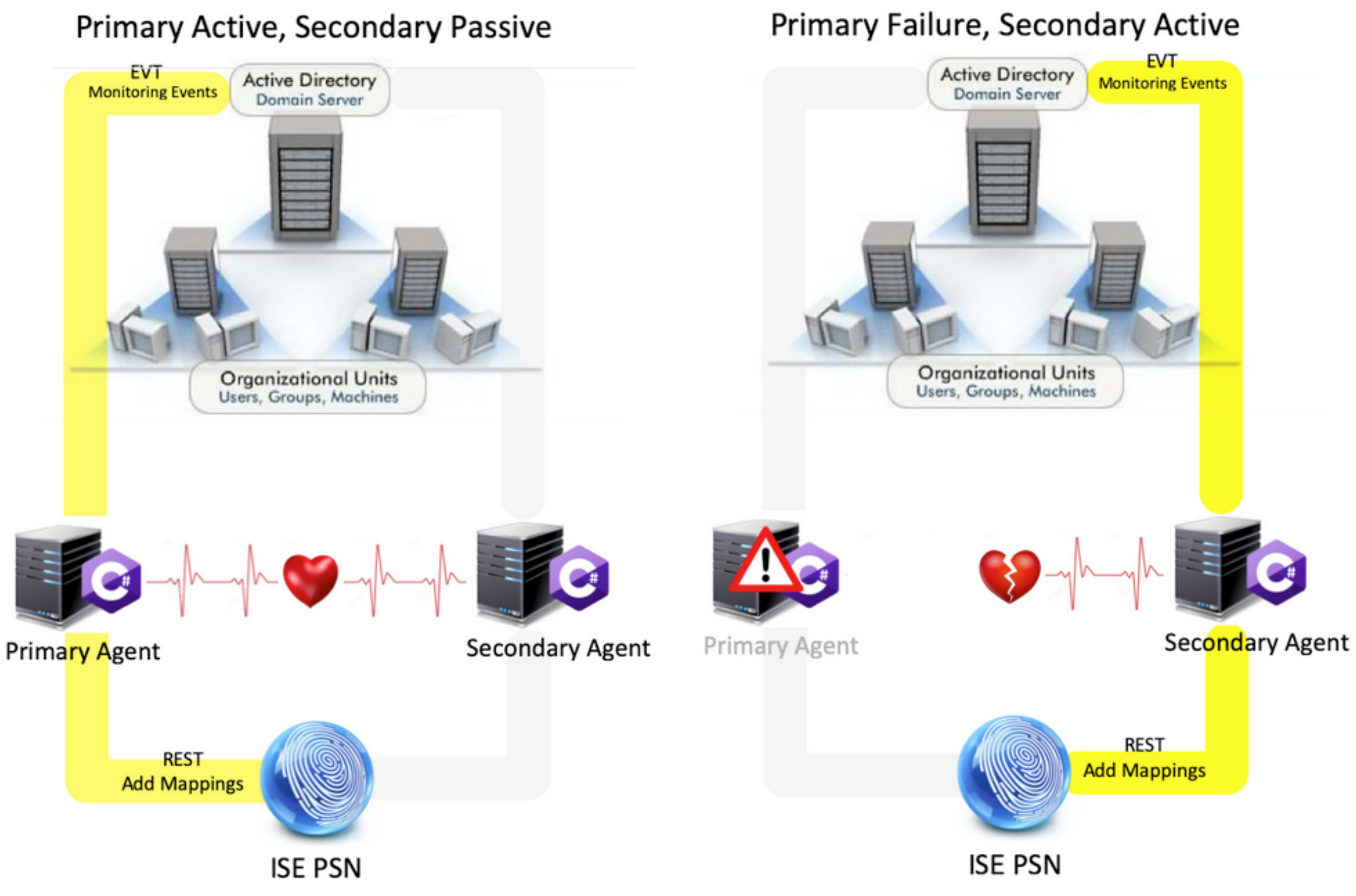
需要新協定

ISE的被動身份（被動ID）功能驅動許多重要的使用案例，包括基於身份的防火牆、EasyConnect等。此功能取決於監控使用者登入Active Directory域控制器並學習其使用者名稱和IP地址的能力。當前用於監視域控制器的主要協定是WMI。但是，配置是困難/侵入性的，對客戶端和伺服器都有效能影響，而且在規模化部署中檢視登入事件時有時具有非常大的延遲。經過深入的研究和替代方法以輪詢被動身份服務所需的資訊後，決定採用另一種協定（稱為EVT或Eventing API），以便更高效地處理此使用案例。它有時也稱為**MS-EVEN6**，也稱為Eventing Remote Protocol，它是基於RPC的底層協定。

使用MS-EVEN6的優勢

高可用性

原始代理沒有高可用性選項，如果需要在該代理正在運行的伺服器上進行維護或發生中斷，會錯過登入事件，基於身份的防火牆等功能會在此期間丟失資料。這是在此版本之前使用ISE PIC代理的主要問題之一。ISE使用UDP埠9095在代理之間交換心跳。

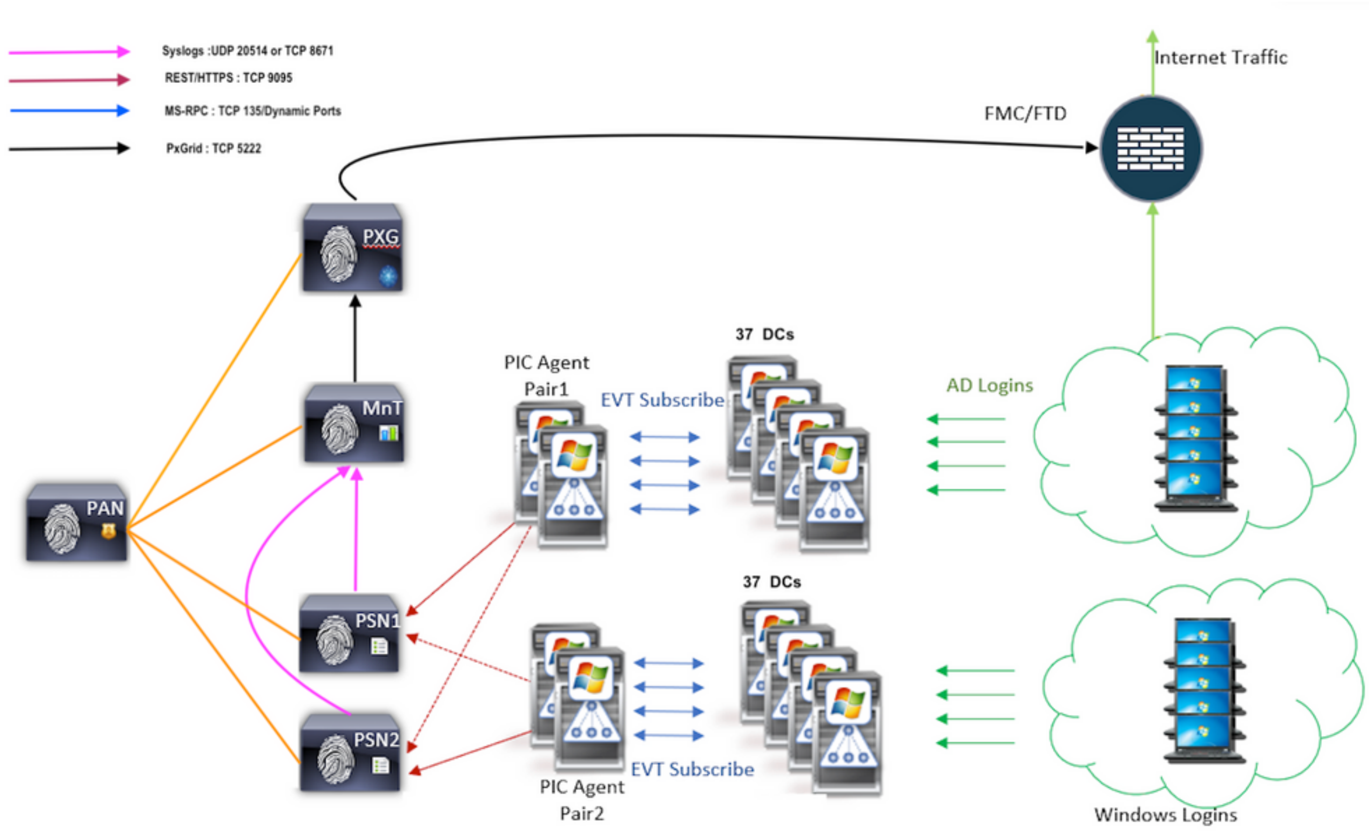


可擴充性

新代理通過增加支援數量的域控制器以及它可以處理的事件數量來提供更好的支援。以下是測試過的刻度數：

- 受監控的域控制器的最大數量（2對Agent）：74
- 測試的最大對映/事件數：292,000（每個資料中心3950個事件）
- 測試的最大TPS:500

擴展測試設定架構



歷史事件查詢

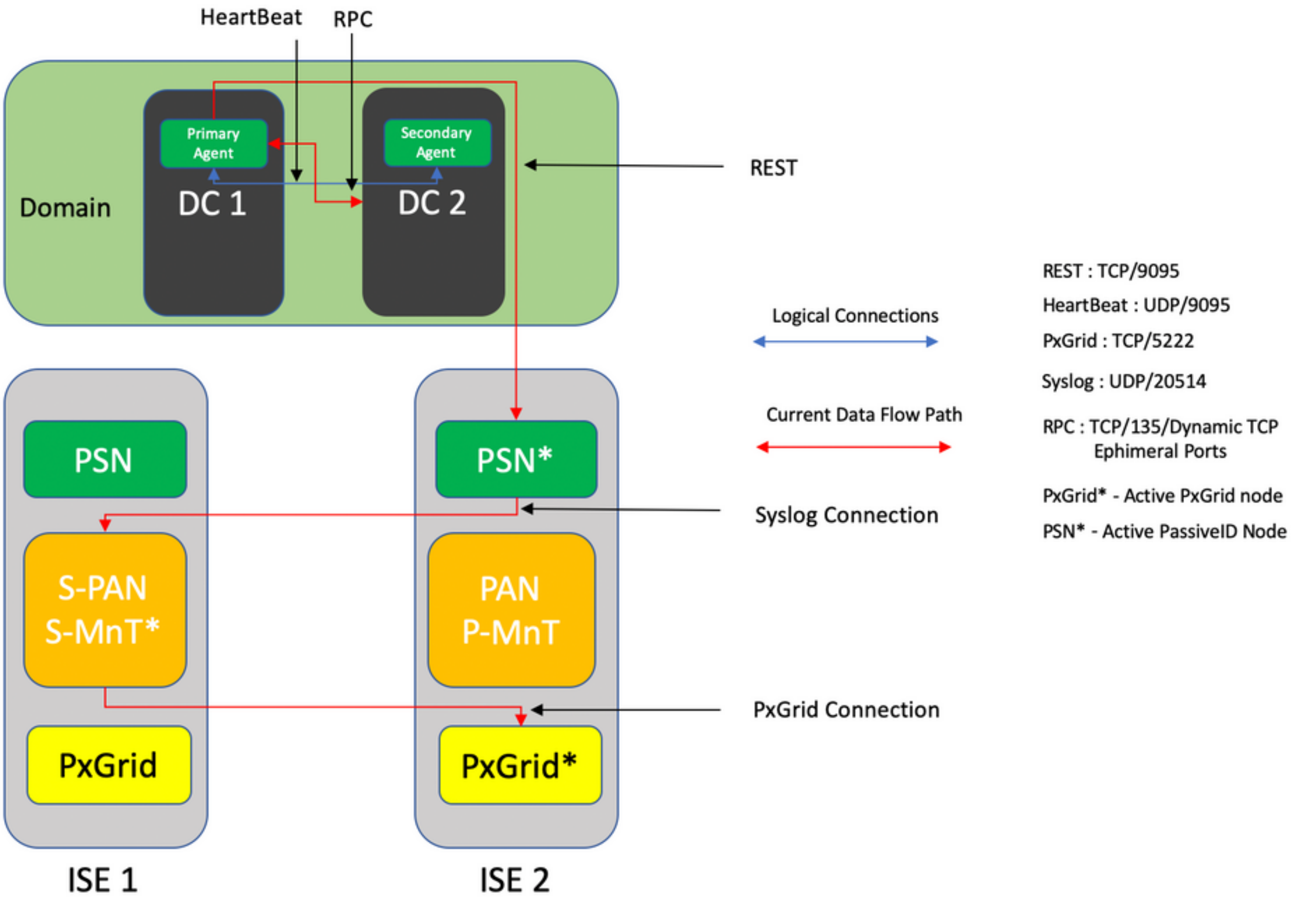
在故障轉移或對PIC-Agent執行服務重啟的情況下，為確保資料不會丟失，將查詢過去給定時間內生成的事件，並再次傳送到PSN節點。預設情況下，ISE會查詢從服務開始起價值60秒的過去事件，以彌補服務丟失期間的任何資料丟失。

減少處理開銷

與大規模或重負載下CPU密集的WMI不同，EVT不像WMI那樣消耗那麼多資源。Scale測試表明使用EVT查詢的效能有了很大提高。

設定

連線圖

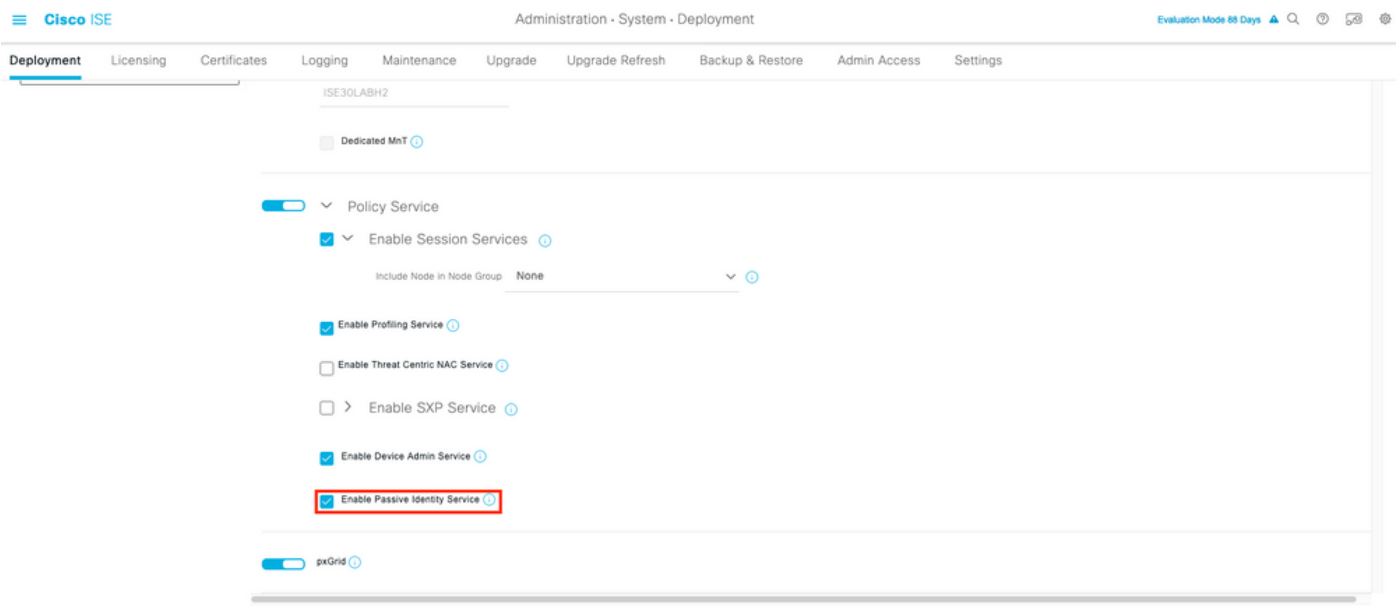


組態

為PassiveID代理配置ISE

要配置PassiveID服務，必須至少在一個策略服務節點(PSN)上啟用被動身份服務。最多兩個節點可用於被動身份服務，該服務以主用/備用模式運行。ISE還必須加入到Active Directory域，並且只有該域中存在的域控制器才能由ISE上配置的代理進行監控。若要將ISE加入Active Directory域，請參閱Active Directory整合指南。

導航到**Administration > System > Deployment > [Choose a PSN] > Edit以啟**用Passive Identity Services，如下所示：



ISE30LABH2

☐ Dedicated MnT

Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

☐ Enable Threat Centric NAC Service

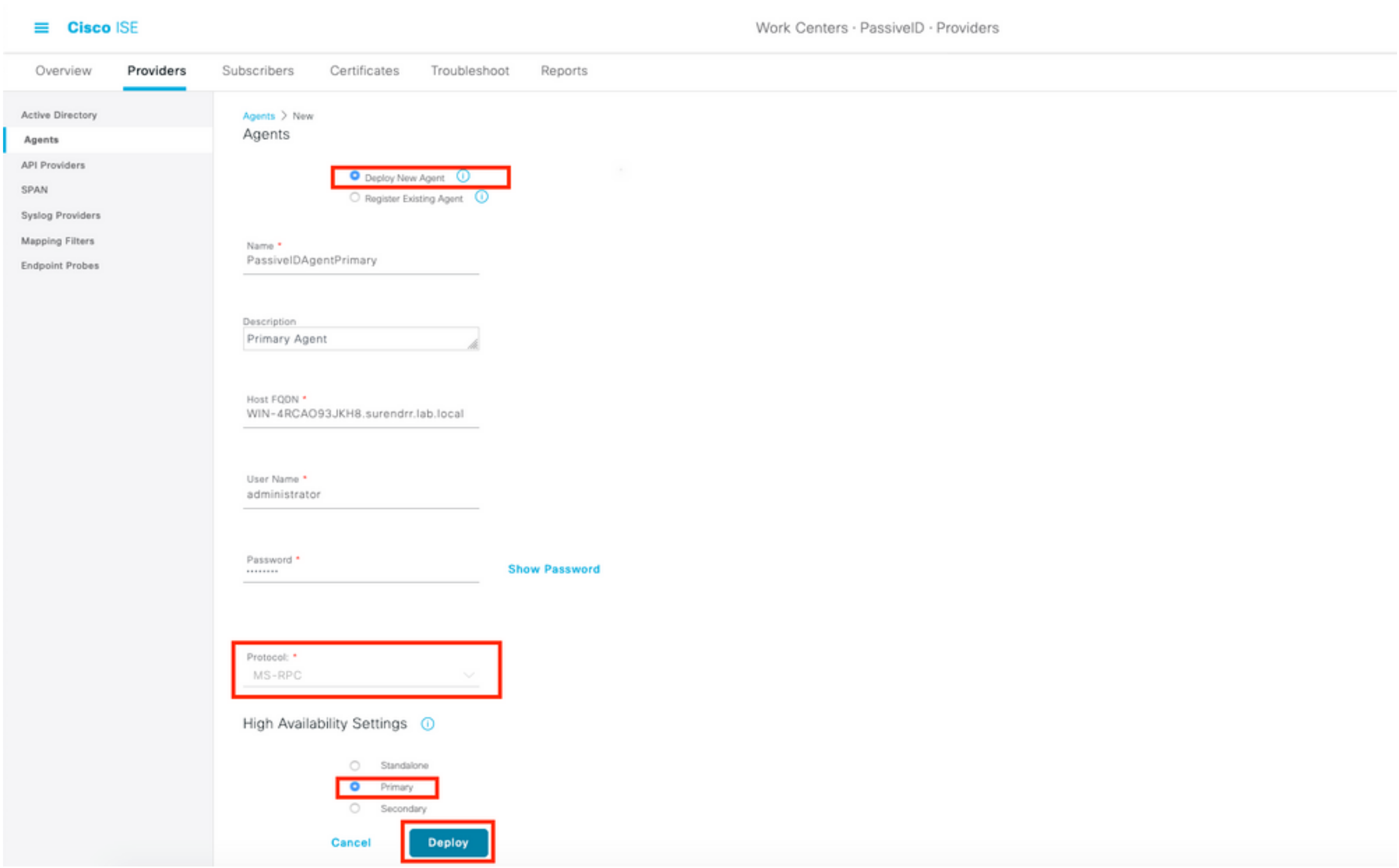
☐ Enable SXP Service

☑ Enable Device Admin Service

☑ Enable Passive Identity Service

pxGrid

導航到**工作中心(Work Centers)>被動ID(PassiveID)>提供程式(Providers)>代理(Agents)>新增(Add)**，以部署新代理，如下所示：



Agents

● Deploy New Agent

○ Register Existing Agent

Name * PassiveIDAgentPrimary

Description Primary Agent

Host FQDN * WIN-4RCAO93JKH8.surendrr.lab.local

User Name * administrator

Password * ••••••••

Show Password

Protocol: * MS-RPC

High Availability Settings

○ Standalone

● Primary

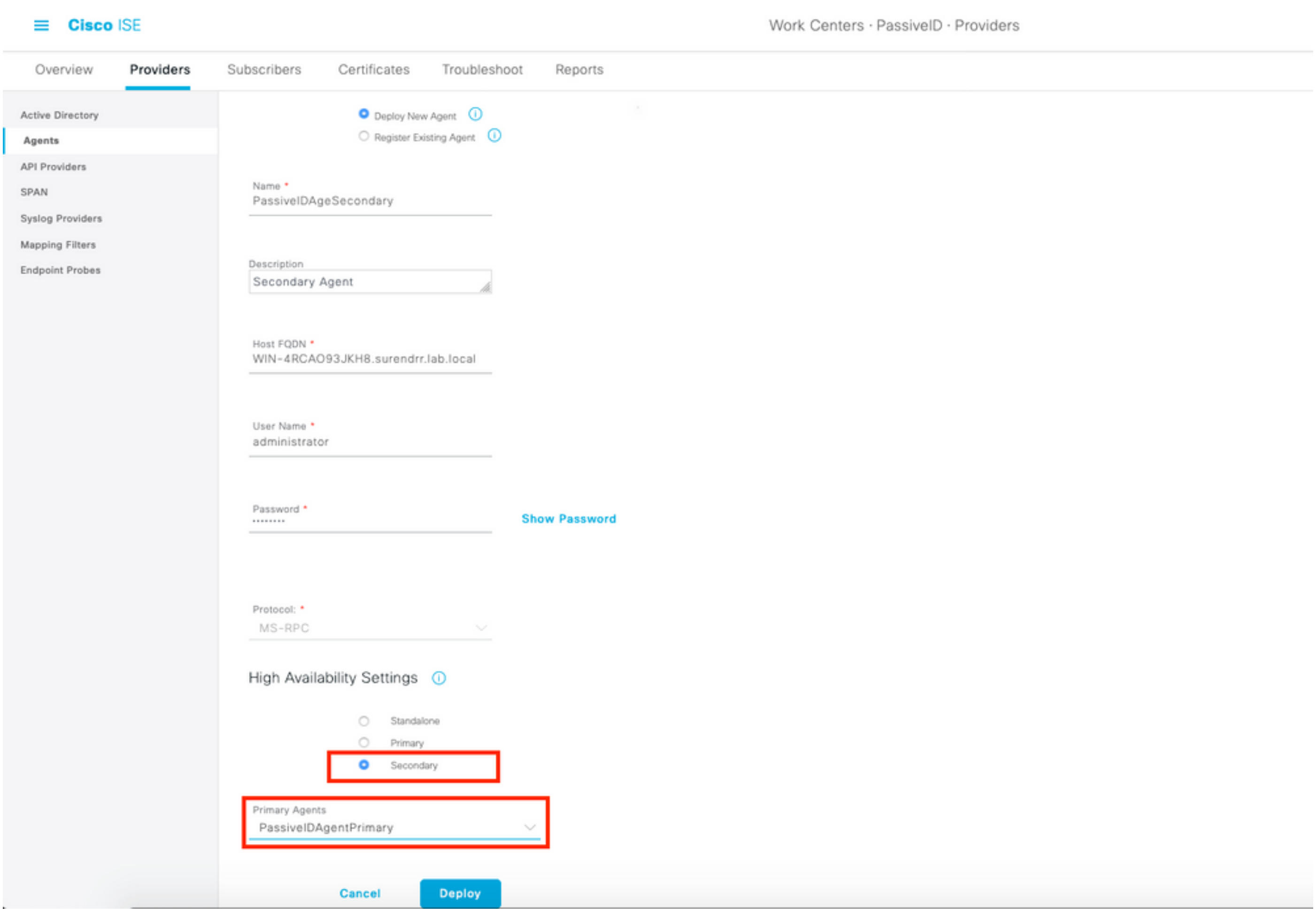
○ Secondary

Cancel Deploy

附註：1.如果代理計畫由ISE安裝在域控制器上，此處使用的帳戶必須具有足夠的特權，以便安裝程式並在主機FQDN欄位中提到的伺服器上運行該程式。這裡的主機FQDN可以是成員伺服器而不是域控制器的FQDN。

2.如果代理已手動安裝或從ISE的先前部署使用MSRPC安裝，則Active Directory或Windows端所需的許可權和配置與WMI相比，PIC代理使用的其他協定（以及3.0之前唯一可用的協定）較少。在此情況下使用的使用者帳戶可以是常規域帳戶，該帳戶是事件日誌讀**者器組的一部分。選擇註冊現有代理**，然後使用這些帳戶詳細資訊註冊在域控制器上手動安裝的代理。

成功部署後，將另一個代理配置到其他伺服器上，並將其新增為輔助代理，然後新增其主要對等體，如下圖所示。



● Deploy New Agent
○ Register Existing Agent

Name *
PassiveIDAgeSecondary

Description
Secondary Agent

Host FQDN *
WIN-4RCAO93JKH8.surendrr.lab.local

User Name *
administrator

Password *
••••••••

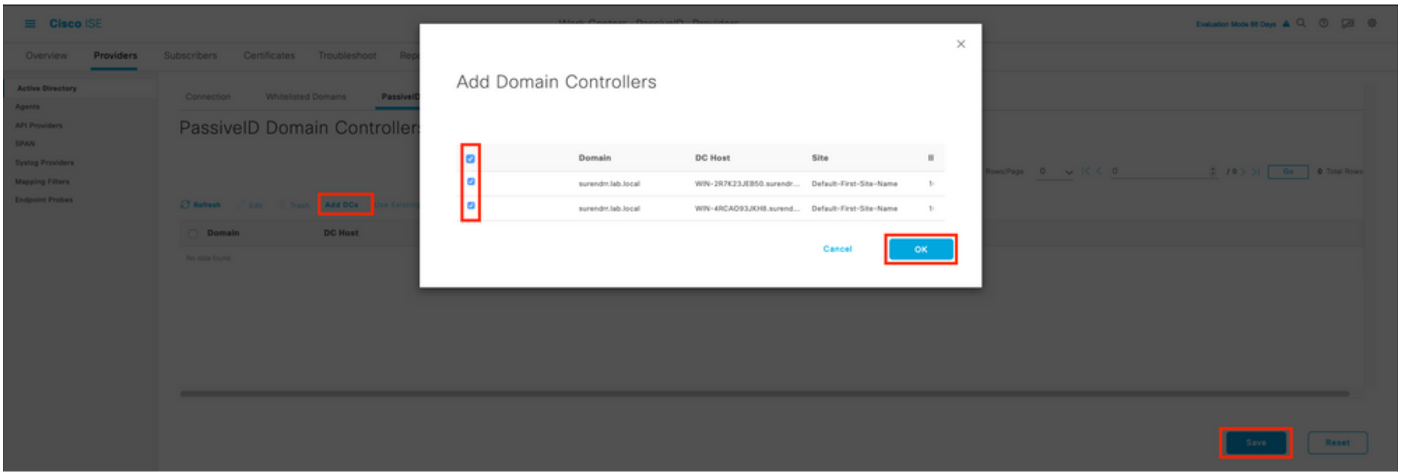
Protocol: *
MS-RPC

High Availability Settings

○ Standalone
○ Primary
● Secondary

Primary Agents
PassiveIDAgentPrimary

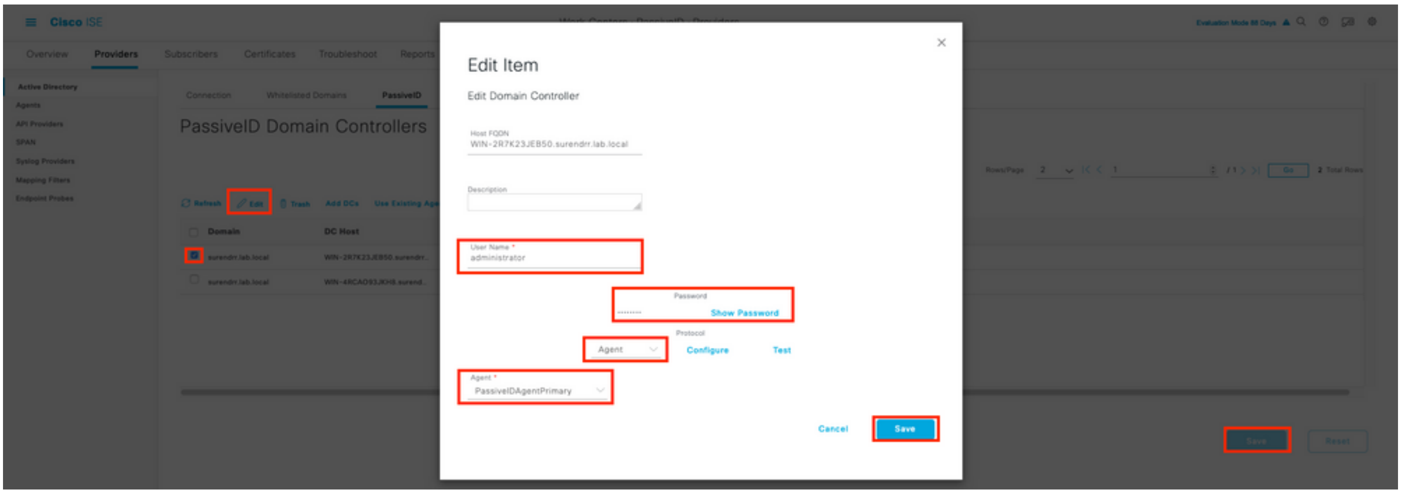
若要使用代理監視域控制器，請導航到**工作中心>被動ID >提供程式> Active Directory > [按一下加入點] > PassiveID**。按一下「**Add DCs**」，然後選擇從中檢索使用者 — IP對映/事件的域控制器，然後按一下「**OK**」，再按一下「**Save**」以儲存變更，如下圖所示。



Add Domain Controllers

☑	Domain	DC Host	Site
☑	surendrr.lab.local	WIN-2R7K23JE850.surendr...	Default-First-Site-Name
☑	surendrr.lab.local	WIN-4RCAO93JKH8.surend...	Default-First-Site-Name

若要指定應用於從中檢索事件的代理，請導航到**Work Centers > PassiveID > Providers > Active Directory > [按一下加入點] > PassiveID。選擇域控制器並按一下Edit**。輸入*User Name*和*Password*。選擇**Agent**，然後選擇**Save**對話方塊。在PassiveID頁籤上按一下**Save**以完成配置。



Edit Item

Edit Domain Controller

Host FQDN: WIN-2R7K23JEB50.surendrr.lab.local

Description

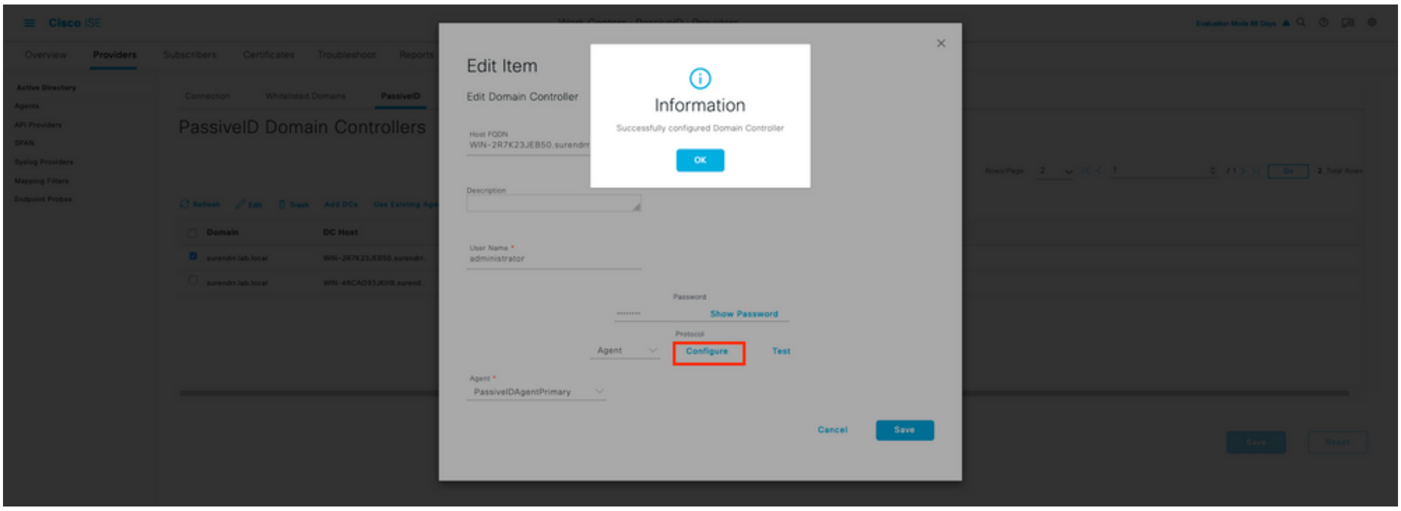
User Name *: administrator

Password: ········· Show Password

Protocol: Agent — Configure — Test

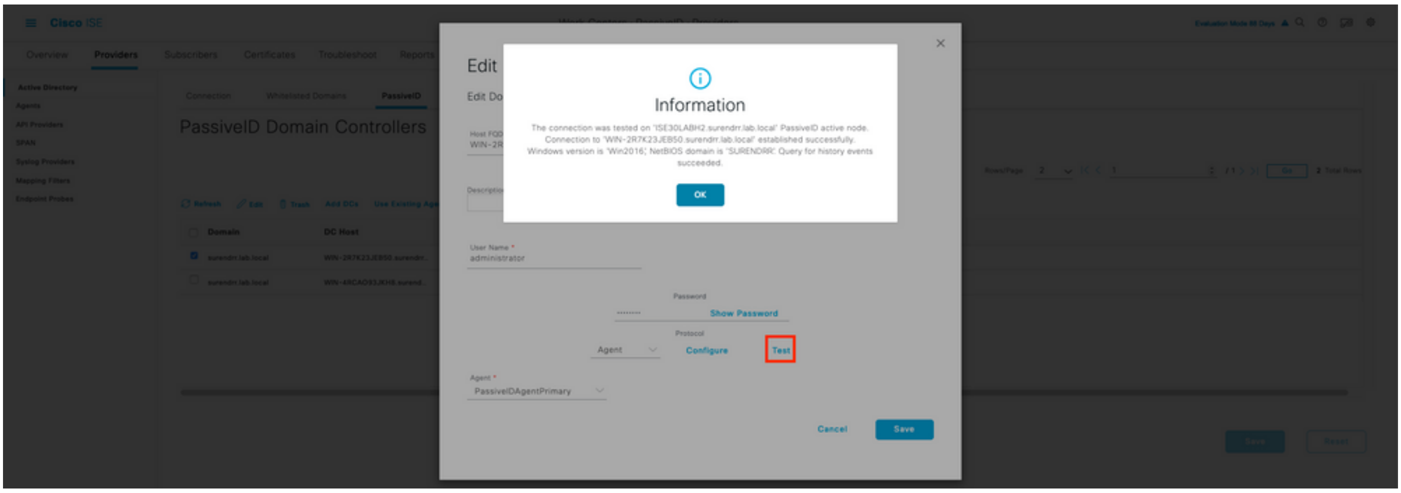
Agent *: PassiveIDAgentPrimary

您可以使用Configure和Test按鈕來檢查是否正確應用了配置，如下圖所示：



Information

Successfully configured Domain Controller



Information

The connection was tested on 'ISE30LABH2.surendrr.lab.local' PassiveID active node. Connection to 'WIN-2R7K23JEB50.surendrr.lab.local' established successfully. Windows version is 'Win2016', NetBIOS domain is 'SURENDRR'. Query for history events succeeded.

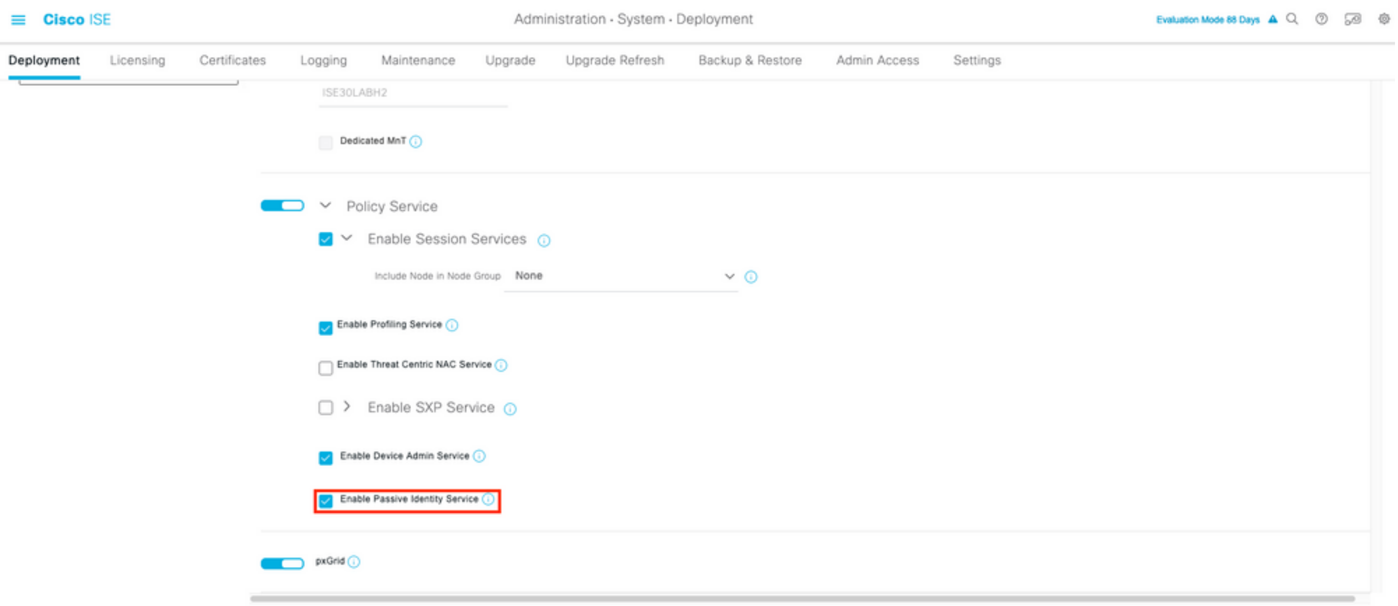
瞭解被動ID代理配置檔案

PassiveID Agent配置檔案位於**C:\Program Files(x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config**。此配置檔案的內容如下所示：

驗證

驗證ISE上的PassiveID服務

1.驗證PassiveID服務是否在GUI上啟用，並且在ISE的CLI上通過**show application status ise**命令標籤為正在運行。



ISE30LABH2

□ Dedicated MnT

Policy Service

☑ Enable Session Services

Include Node in Node Group: None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

□ Enable SXP Service

☑ Enable Device Admin Service

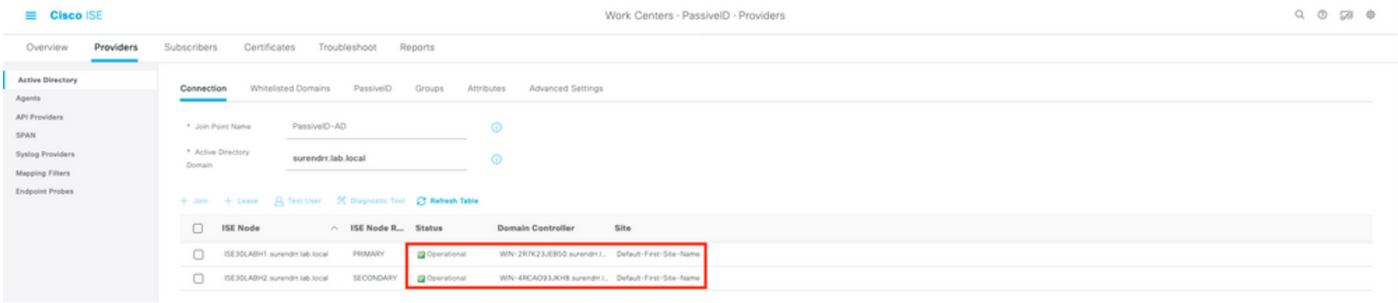
☑ Enable Passive Identity Service

pxGrid

```
ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 129052
Database Server running 108 PROCESSES
Application Server running 9830
Profiler Database running 5127
ISE Indexing Engine running 13361
AD Connector running 20609
M&T Session Database running 4915
M&T Log Processor running 10041
Certificate Authority Service running 15493
EST Service running 41658
SXP Engine Service disabled
Docker Daemon running 815
TC-NAC Service disabled
pxGrid Infrastructure Service disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager disabled
pxGrid Controller disabled
PassiveID WMI Service running 15951
PassiveID Syslog Service running 16531
PassiveID API Service running 17093
PassiveID Agent Service running 17830
PassiveID Endpoint Service running 18281
PassiveID SPAN Service running 20253
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 1472
ISE API Gateway Database Service running 4026
ISE API Gateway Service running 7661
Segmentation Policy Service disabled
REST Auth Service disabled
SSE Connector disabled
```

2.驗證ISE Active Directory提供程式是否已在**Work Centers > PassiveID > Providers > Active**

Directory > Connection連線到域控制器。

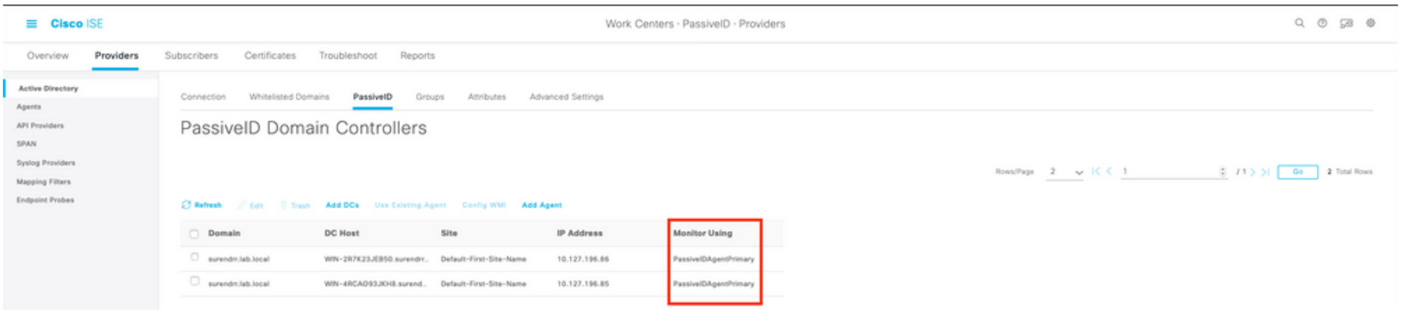


* Join Point Name: PassiveID-AD

* Active Directory Domain: surendrr.lab.local

☐	ISE Node	ISE Node R...	Status	Domain Controller	Site
☐	ISE30LABH1.surendrr.lab.local	PRIMARY	☑ Operational	WIN-2R7K23JEB50.surendrr.l...	Default-First-Site-Name
☐	ISE30LABH2.surendrr.lab.local	SECONDARY	☑ Operational	WIN-4RCAO93JKH8.surendrr.l...	Default-First-Site-Name

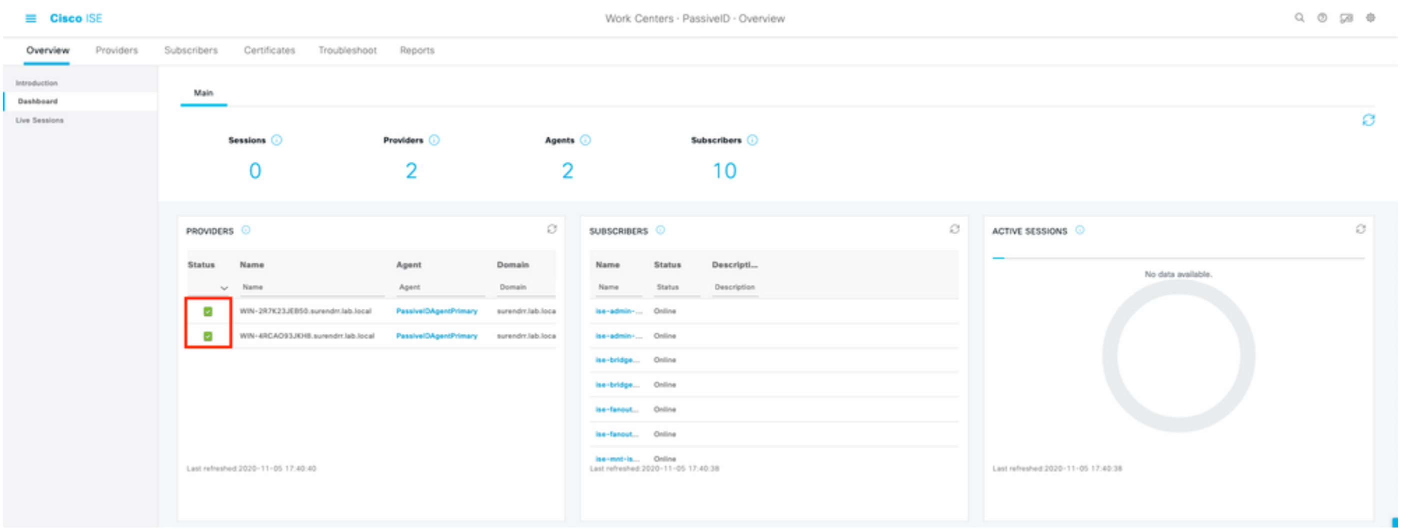
3.驗證Agent at Work Centers > PassiveID > Providers > Active Directory > PassiveID是否正在監視所需的域控制器。



PassiveID Domain Controllers

☐	Domain	DC Host	Site	IP Address	Monitor Using
☐	surendrr.lab.local	WIN-2R7K23JEB50.surendrr...	Default-First-Site-Name	10.127.196.86	PassiveIDAgentPrimary
☐	surendrr.lab.local	WIN-4RCAO93JKH8.surend...	Default-First-Site-Name	10.127.196.85	PassiveIDAgentPrimary

4.驗證受監控域控制器的狀態是否為up(即控制面板上Work Centers > PassiveID > Overview > Dashboard處標籤為綠色)。



Sessions: 0 | Providers: 2 | Agents: 2 | Subscribers: 10

PROVIDERS

Status	Name	Agent	Domain
☑	WIN-2R7K23JEB50.surendrr.lab.local	PassiveIDAgentPrimary	surendrr.lab.loca
☑	WIN-4RCAO93JKH8.surendrr.lab.local	PassiveIDAgentPrimary	surendrr.lab.loca

Last refreshed:2020-11-05 17:40:40

SUBSCRIBERS

Name	Status	Descripti...
ise-admin-...	Online	
ise-admin-...	Online	
ise-bridge...	Online	
ise-bridge...	Online	
ise-fanout...	Online	
ise-fanout...	Online	
ise-mnt-is...	Online	

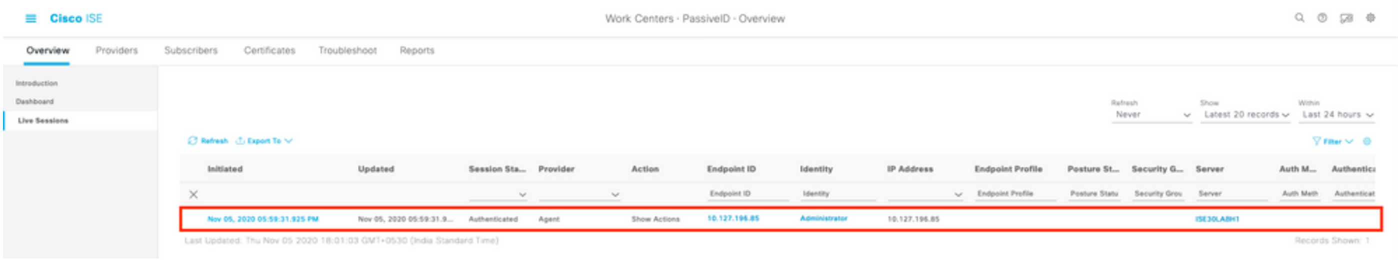
Last refreshed:2020-11-05 17:40:38

ACTIVE SESSIONS

No data available.

Last refreshed:2020-11-05 17:40:38

5.驗證在**工作中心>被動ID >概述>即時會話**的域控制器上註冊Windows登入時填充的即時會話。



Refresh: Never | Show: Latest 20 records | Within: Last 24 hours

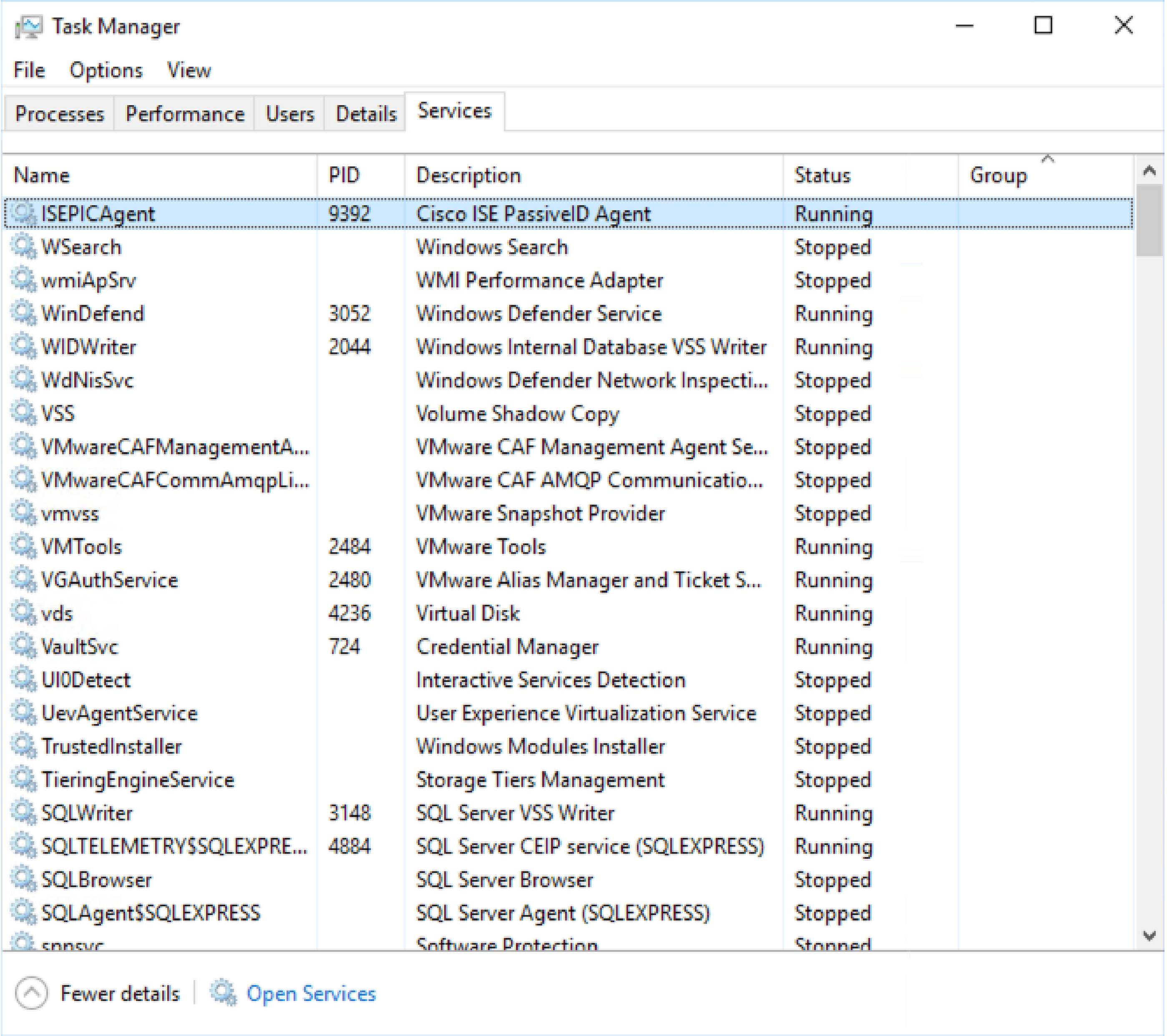
Initiated	Updated	Session Sta...	Provider	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture St...	Security G...	Server	Auth M...	Authentica
Nov 05, 2020 05:59:31.925 PM	Nov 05, 2020 05:59:31.9...	Authenticated	Agent	Show Actions	10.127.196.85	Administrator	10.127.196.85				ISE30LABH1		

Last Updated: Thu Nov 05 2020 18:01:03 GMT+0530 (India Standard Time)

Records Shown: 1

驗證Windows伺服器上的代理服務

1.驗證安裝了PIC Agent的伺服器上的ISEPICAgent服務。



Name	PID	Description	Status	Group
ISEPICAgent	9392	Cisco ISE PassiveID Agent	Running	
WSearch		Windows Search	Stopped	
wmiApSrv		WMI Performance Adapter	Stopped	
WinDefend	3052	Windows Defender Service	Running	
WIDWriter	2044	Windows Internal Database VSS Writer	Running	
WdNisSvc		Windows Defender Network Inspecti...	Stopped	
VSS		Volume Shadow Copy	Stopped	
VMwareCAFManagementA...		VMware CAF Management Agent Se...	Stopped	
VMwareCAFCommAmqpLi...		VMware CAF AMQP Communicatio...	Stopped	
vmvss		VMware Snapshot Provider	Stopped	
VMTools	2484	VMware Tools	Running	
VGAuthService	2480	VMware Alias Manager and Ticket S...	Running	
vds	4236	Virtual Disk	Running	
VaultSvc	724	Credential Manager	Running	
UI0Detect		Interactive Services Detection	Stopped	
UevAgentService		User Experience Virtualization Service	Stopped	
TrustedInstaller		Windows Modules Installer	Stopped	
TieringEngineService		Storage Tiers Management	Stopped	
SQLWriter	3148	SQL Server VSS Writer	Running	
SQLTELEMETRY$SQLEXPRE...	4884	SQL Server CEIP service (SQLEXPRESS)	Running	
SQLBrowser		SQL Server Browser	Stopped	
SQLAgent$SQLEXPRESS		SQL Server Agent (SQLEXPRESS)	Stopped	
sppsvc		Software Protection	Stopped	