配置基于EVT的身份服务引擎被动ID代理

目录

简介

本文档介绍ISE 3.0版本中引入的新身份服务引擎(ISE)被动身份连接器(ISE-PIC)代理。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科身份服务管理
- MS-RPC、WMI协议
- Active Directory管理

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎3.0版及更高版本
- Microsoft Windows Server 2016标准版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文还介绍了ISE-PIC代理的优点以及此代理在ISE上的配置。ISE被动身份代理已成为身份防火墙解决方案不可或缺的一部分，该解决方案也使用Cisco FirePower管理中心。

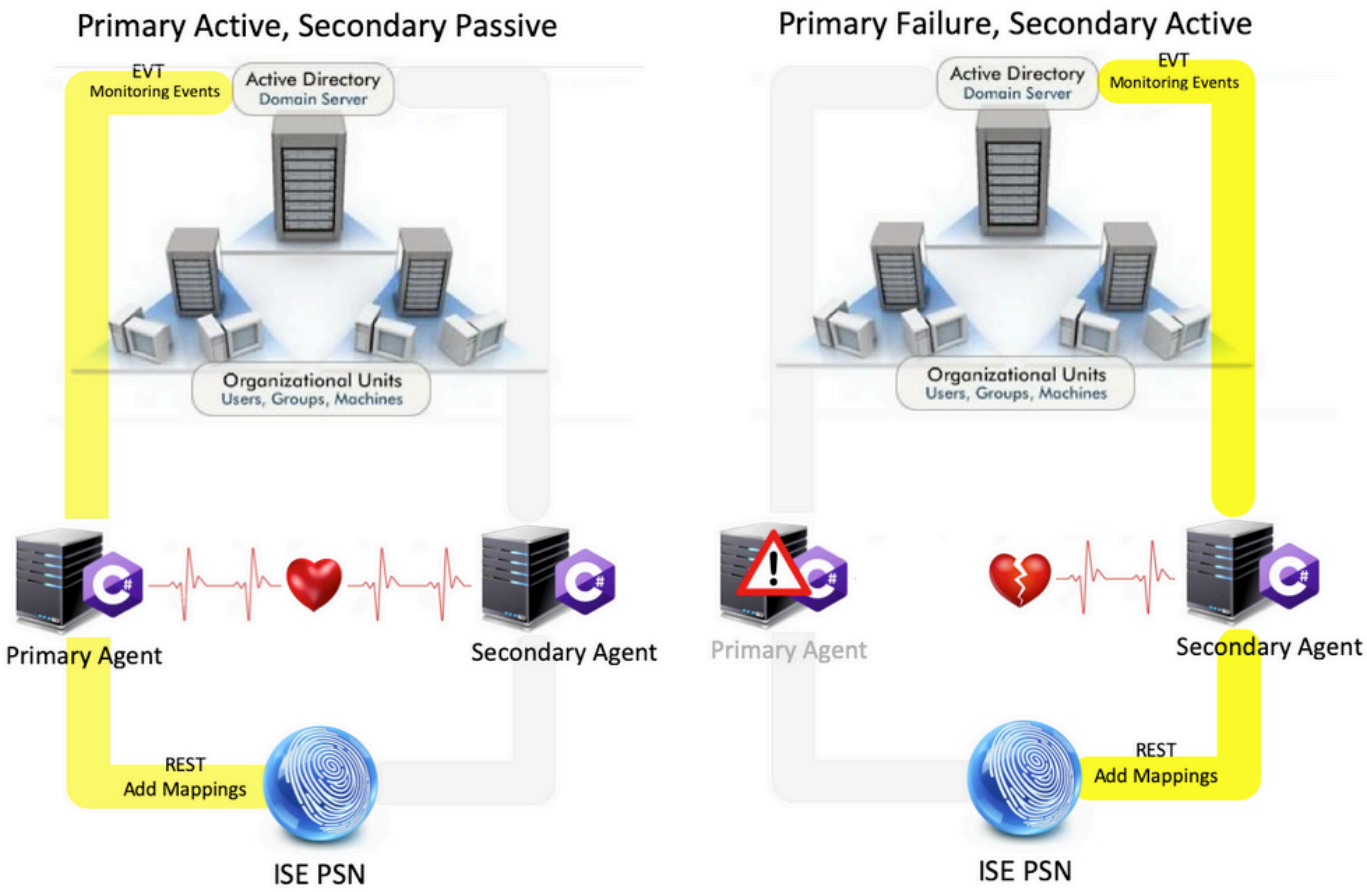
需要新协议

ISE的被动身份（被动ID）功能推动了许多重要的使用案例，包括基于身份的防火墙、EasyConnect等。此功能取决于能否监控登录Active Directory域控制器并了解其用户名和IP地址的用户。用于监控域控制器的当前主协议是WMI。但是，它很难/无法进行配置，会对客户端和服务器的性能造成影响，有时在扩展部署中查看登录事件时会有极长的延迟。在深入研究和选择备用方式轮询被动身份服务所需的信息后，我们决定采用一种备用协议-称为事件API (EVT)，它可更有效地处理此使用案例。它有时也称为MS-EVEN6，也称为事件远程协议，是基于RPC的底层在线协议。

使用MS-EVEN6的优势

高可用性

原始代理没有高可用性(HA)选项，如果需要在运行代理的服务器上进行维护或发生中断，登录事件将会丢失，基于身份的防火墙等功能在此期间将发生数据丢失。这是此版本之前使用ISE PIC代理的主要问题之一。从此版本开始，座席可以在高可用性模式下工作。ISE使用UDP端口9095在代理之间交换心跳以确保高可用性。可以配置多个HA代理对以监控不同的域控制器。

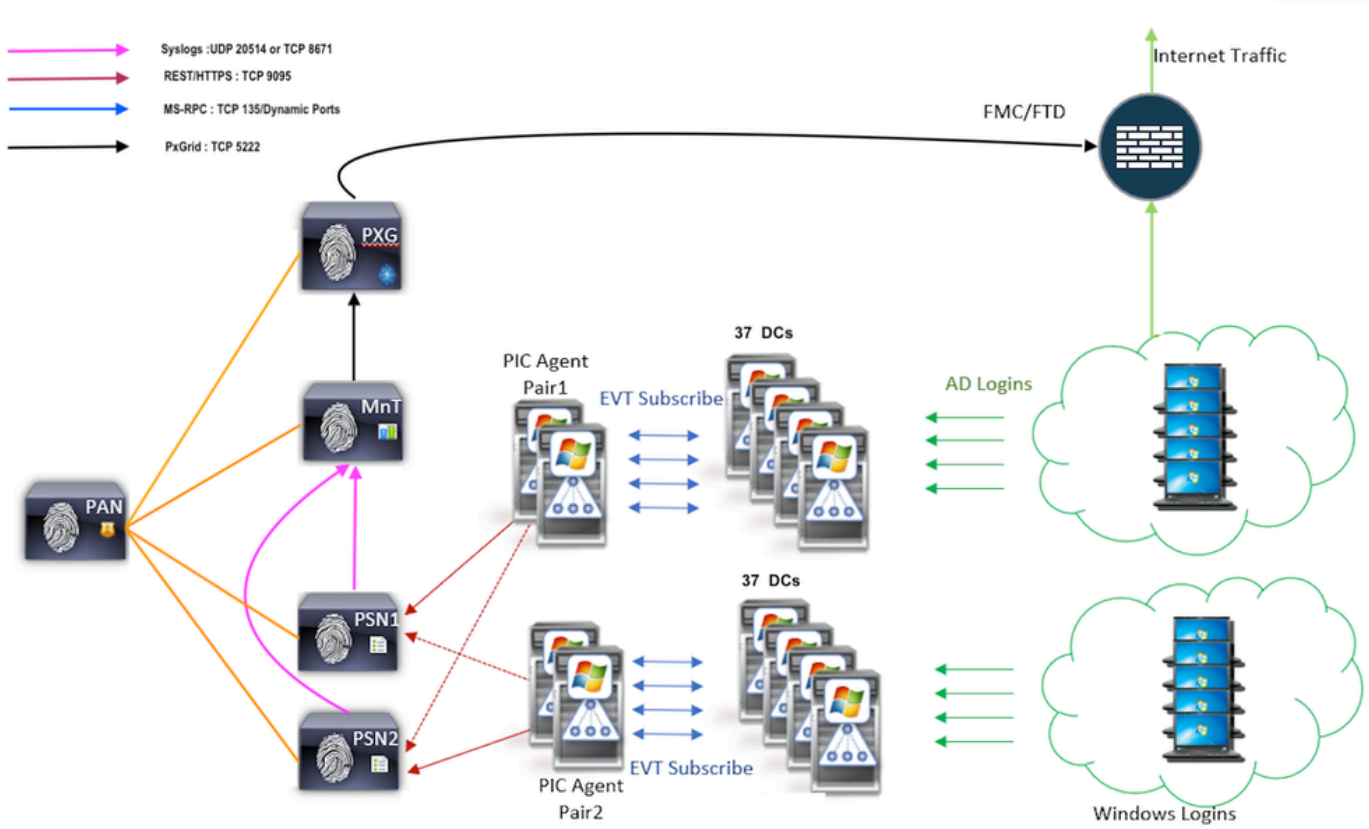


可扩展性

新代理通过增加扩展数量为支持的域控制器数量以及它可以处理的事件数量提供更好的支持。以下是测试的标准编号：

- 监控的域控制器的最大数量（2对Agent）：74
- 测试的最大映射/事件数：292,000（每个DC 3950个事件）
- 测试的最大TPS：500

扩展测试设置架构



历史事件查询

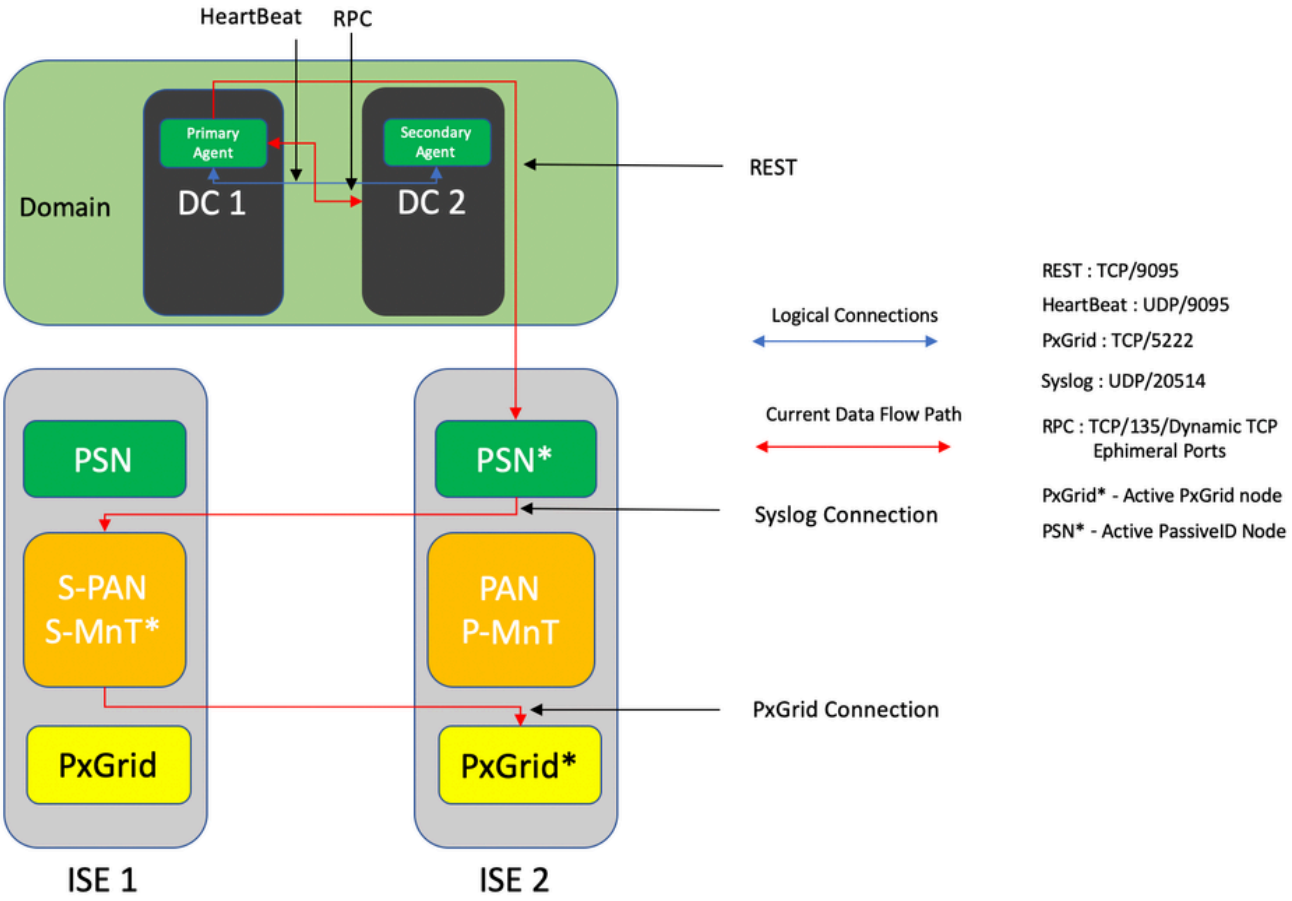
在故障切换的情况下，或在为PIC-Agent执行服务重新启动的情况下，为确保不丢失数据，将查询过去在配置的时间内生成的事件，并再次发送到PSN节点。默认情况下，ISE会查询从服务启动时算起的60秒过去事件，以抵消服务丢失期间的任何数据丢失。

减少处理开销

与WMI不同，EVT在大规模或重负载下会占用CPU资源，WMI不会消耗太多资源。扩展测试表明，使用EVT后，查询性能得到了很大的提高。

配置

连接图

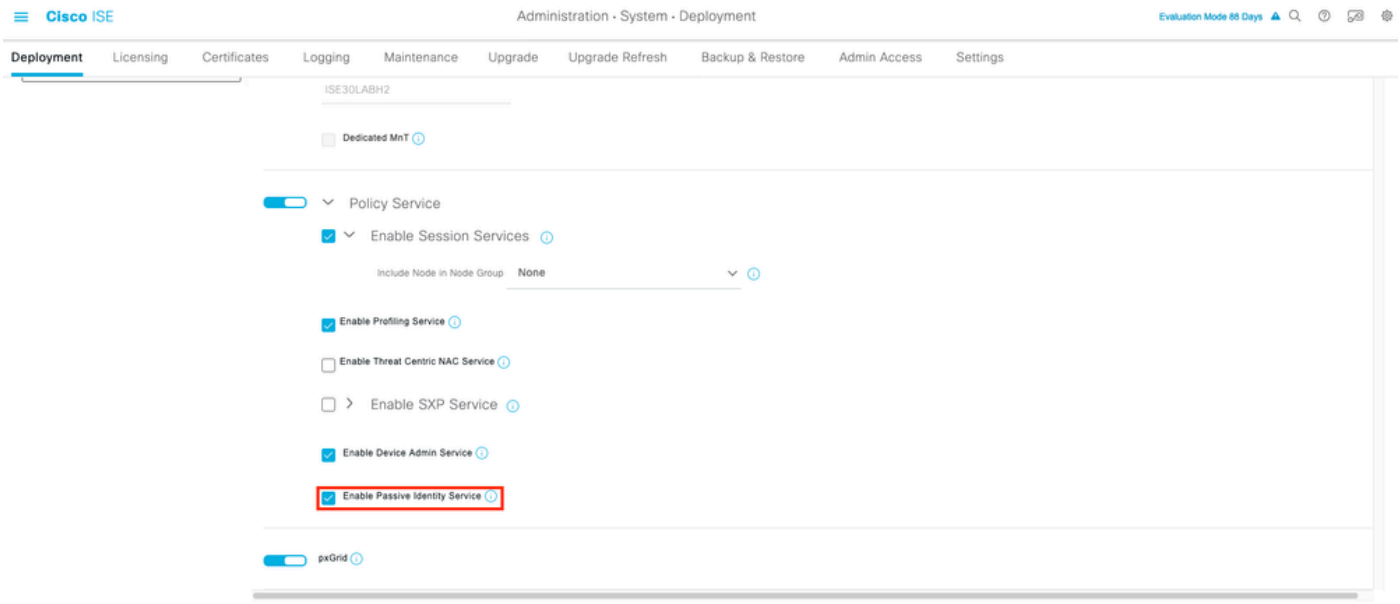


配置

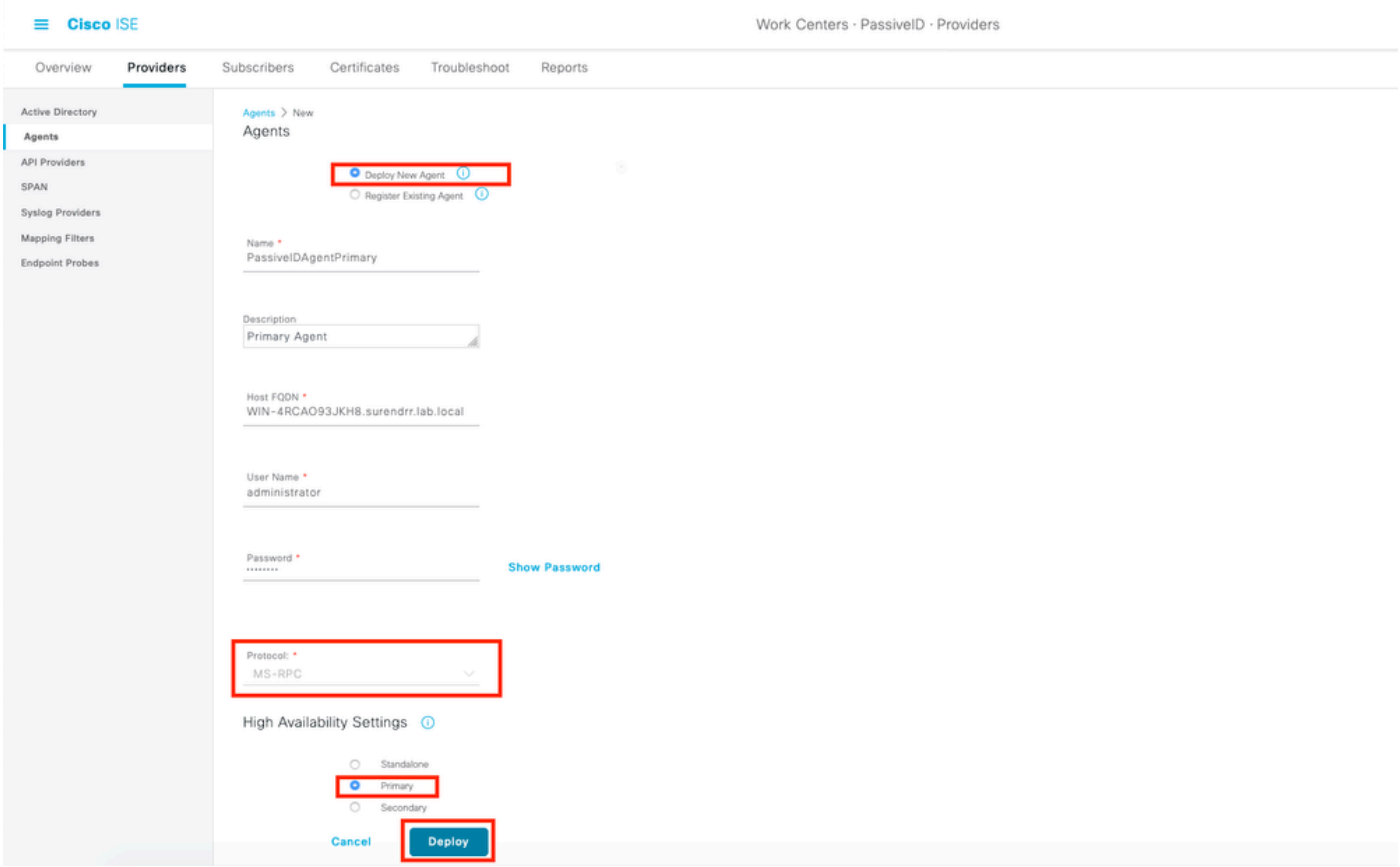
为PassiveID代理配置ISE

要配置PassiveID服务，必须在至少一个策略服务节点(PSN)上启用被动身份服务。最多两个节点可用于在主用/备用操作模式下运行的被动身份服务。ISE还必须加入到Active Directory域，并且只有该域中存在的域控制器可以由ISE上配置的代理监控。要将ISE加入到Active Directory域，请参阅Active Directory集成指南。

导航到管理>系统>部署> [选择PSN] >编辑，以启用被动Identity Services，如下所示：



导航到工作中心(Work Centers) >被动ID (PassiveID) >提供程序(Providers) >代理(Agents) >添加(Add)以部署新代理，如下所示：

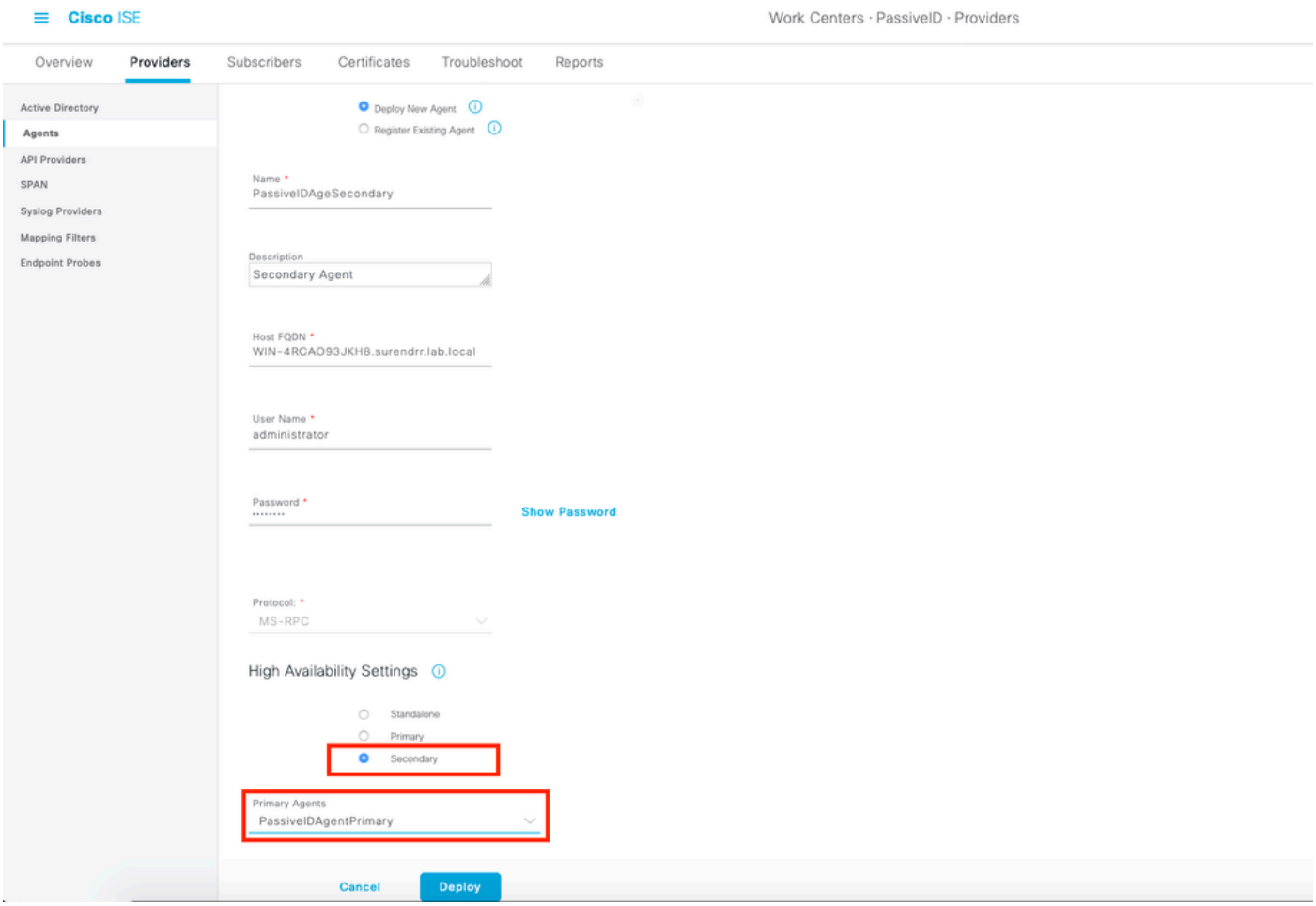


注：1.如果代理要由ISE安装在域控制器上，则此处使用的帐户必须具有足够的特权来安装程序，并在主机完全限定域名(FQDN)字段中提及的服务器上运行该程序。此处的主机FQDN可以是成员服务器而非域控制器的FQDN。

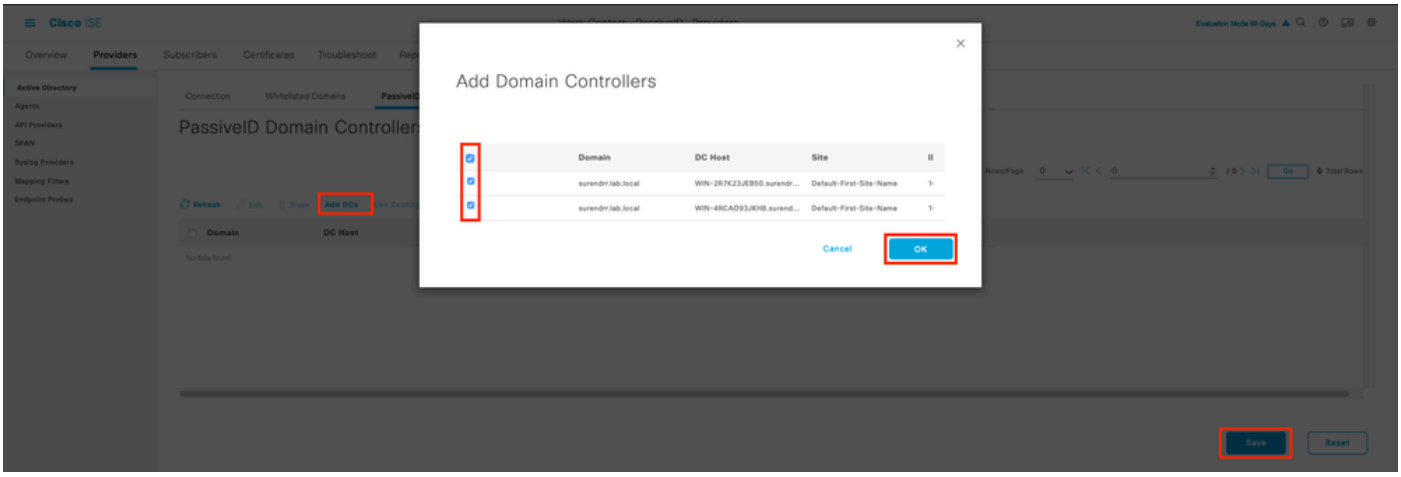
2. 如果已经手动安装代理，或以前部署的ISE使用MSRPC安装代理，则Active Directory或Windows端所需的权限和配置与WMI相比更少，而PIC代理使用的另一个协议（以及3.0之前

的唯一协议）则更少。本例中使用的用户帐户可以是属于事件日志读取器组的常规域帐户。选择注册现有代理，然后使用这些帐户详细信息注册在域控制器上手动安装的代理。

成功部署后，在其他服务器上配置另一个代理，并将其添加为辅助代理，然后添加其主要对等体，如下图所示。

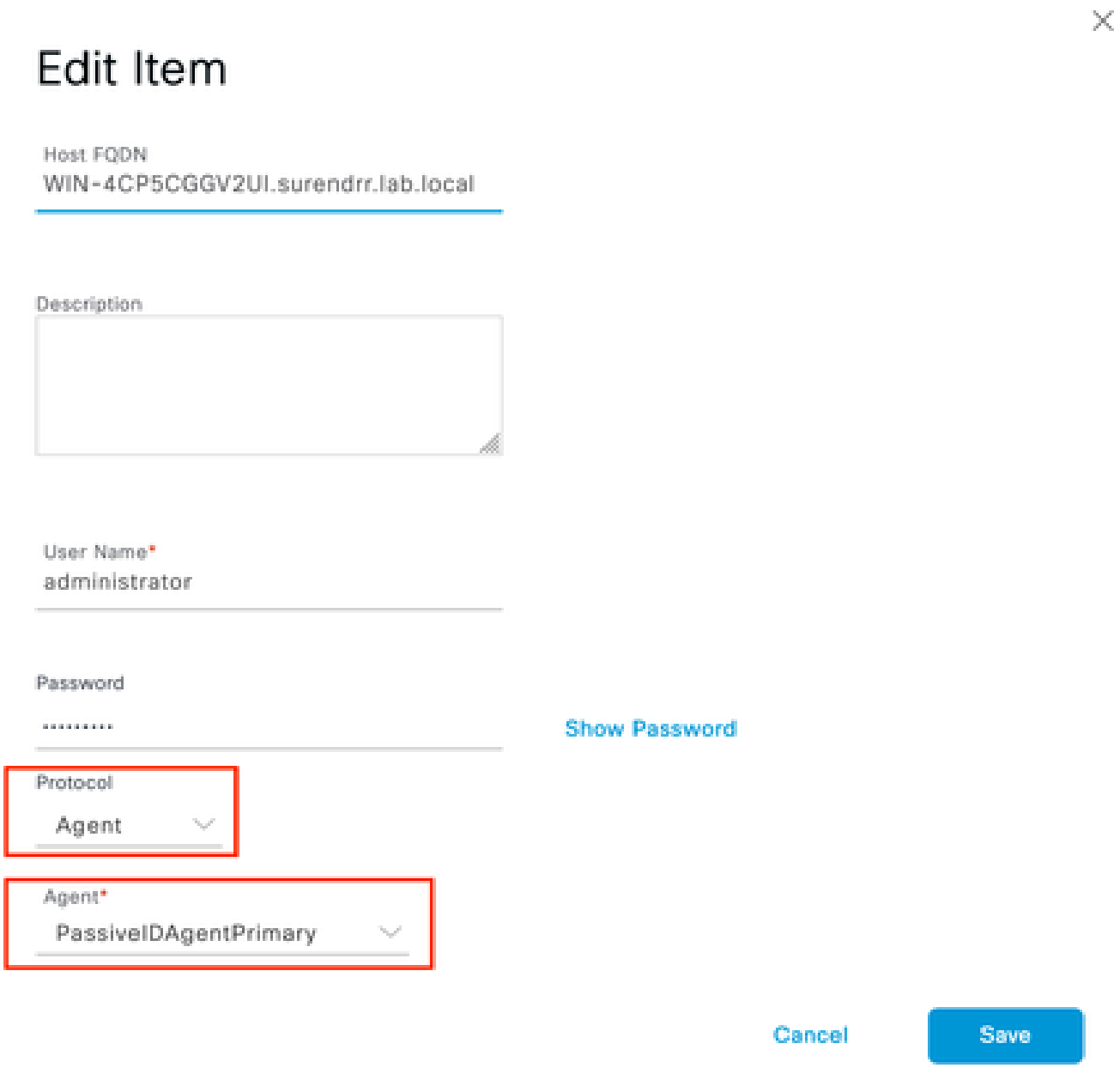


要监控使用代理的域控制器，请导航到工作中心> PassiveID >提供程序> Active Directory > [单击加入点] > PassiveID。点击添加DC，选择从中检索用户-IP映射/事件的域控制器，点击确定，然后点击保存以保存更改，如此图中所示。



要指定可用于从中检索事件的代理，请导航到工作中心(Work Centers) > PassiveID >提供程序

(Providers) > Active Directory > [点击加入点] > PassiveID。选择域控制器并单击Edit。输入用户名和密码。选择Agent，然后选择Save对话框。单击PassiveID选项卡上的Save以完成配置。



注意：在3.0版补丁4之前的版本中，本节提供配置和测试选项。

了解PassiveID代理配置文件

PassiveID代理配置文件位于C:\Program Files (x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config。配置文件的内容如下所示：

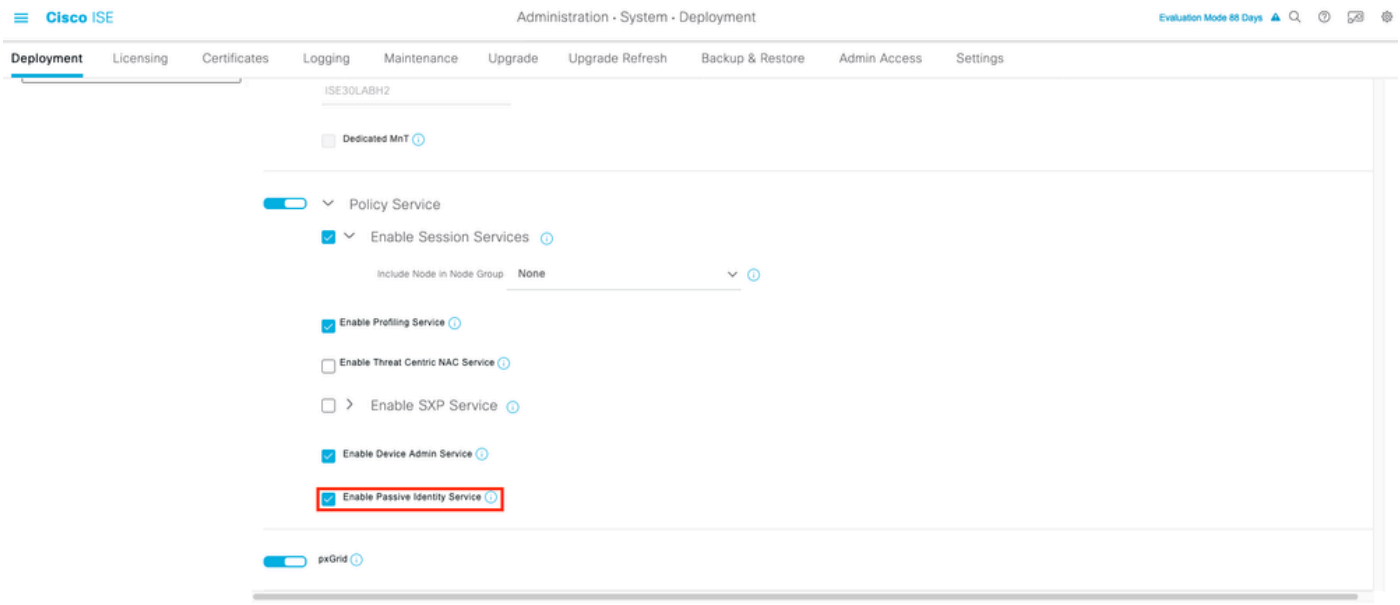
< ? xml version="1.0" encoding="utf-8" ? >
<configuration>
<configSects>
<section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler， log4net"/>

```
</configSections>
<log4net>
<root>
<level value="DEBUG" /> <！—日志记录级别：关闭、致命、错误、警告、信息、调试、全部—>
<！—该设置为其运行所在的服务器上的PassiveID Agent收集的日志的日志级别。-- >
<appender-ref ref ref="RollingFileAppender" />
</root>
<appender name="RollingFileAppender" type="log4net.Appender.RollingFileAppender">
<file value="CiscoISEPICAgent.log" /> <！—请勿修改此文件—>
<appendToFile value="true" />
<rollingStyle value="Size" />
<maxSizeRollBackups value="5" /> <！—此数字设置滚动更新之前生成的日志文件的最大数量—>
<maximumFileSize value="10MB" /> <！—用于设置生成的每个日志文件的最大大小—>
<staticLogFileName value="true" />
<layout type="log4net.Layout.PatternLayout">
<conversionPattern值="%date %level - %message%newline" />
</layout>
</appender>
</log4net>
<startup>
<supportedRuntime version="v4.0"/>
<supportedRuntime version="v2.0.50727"/>
</startup>
<appSettings>
<add key="heartbeatFrequency" value="400" /> <！—此数字定义在ISE上成对配置的主代理和辅助代理之间运行的心跳频率（以毫秒为单位）—>
<add key="heartbeatThreshold" value="1000"/> <！—该值定义代理在标记另一个代理之后等待检测信号的最长时间（以毫秒为单位）—>
<add key="showHeartbeats" value="false" /> <！—将值更改为“true”以在日志文件中查看心跳消息—>
<add key="maxRestThreads" value="200" /> <！—定义可生成以向ISE发送事件的REST线程的最大数量。除非得到思科TAC的建议，否则请勿更改此值。—>
<add key="mappingTransport" value="rest" /> <！—定义用于将映射发送到ISE的介质的类型。请勿更改此值—>
<add key="maxHistorySeconds" value="60" /> <！—定义在服务重新启动的情况下需要检索历史事件的持续时间（以秒为单位）—>
<add key="restTimeout" value="5000" /> <！—定义对ISE的REST调用的超时值—>
<add key="showTPS" value="false" /> <！—将此值更改为“true”，以查看收到并发送到ISE的事件的TPS —>
<add key="showPOSTS" value="false" /> <！—将此值更改为“true”以打印发送到ISE的事件—>
<add key="nodeFailoverTimeSpan" value="5000" /> <！—定义阈值的条件（以毫秒为单位），在该阈值内，与活动PassiveID PSN节点通信时可能发生的错误数将计入故障转移范围—>
<add key="nodeFailoverMaxErrors" value="5" /> <！—定义在故障切换到备用PassiveID PSN节点之前，在指定nodeFailoverTimeSpan内容许的最大错误数—>
</appSettings>
</configuration>
```

验证

验证ISE上的PassiveID服务

1. 验证PassiveID服务是否已在GUI上启用，并是否已在ISE的CLI上标记为running(使用show application status ise命令)。



<#root>

```
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

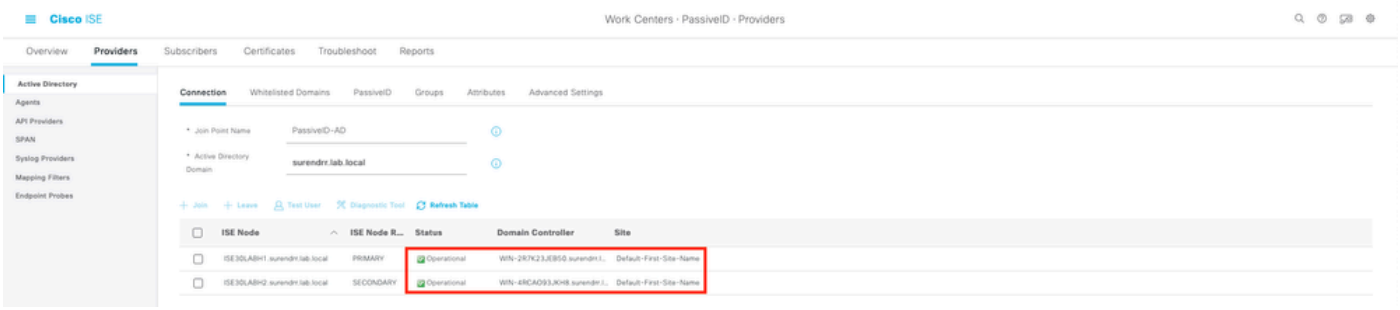
PassiveID Syslog Service running

16531

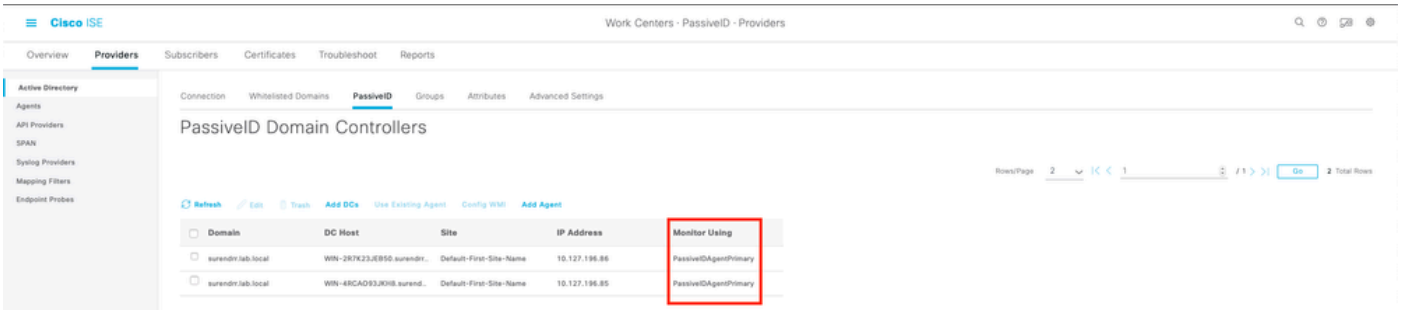
PassiveID API Service running

```
 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
```

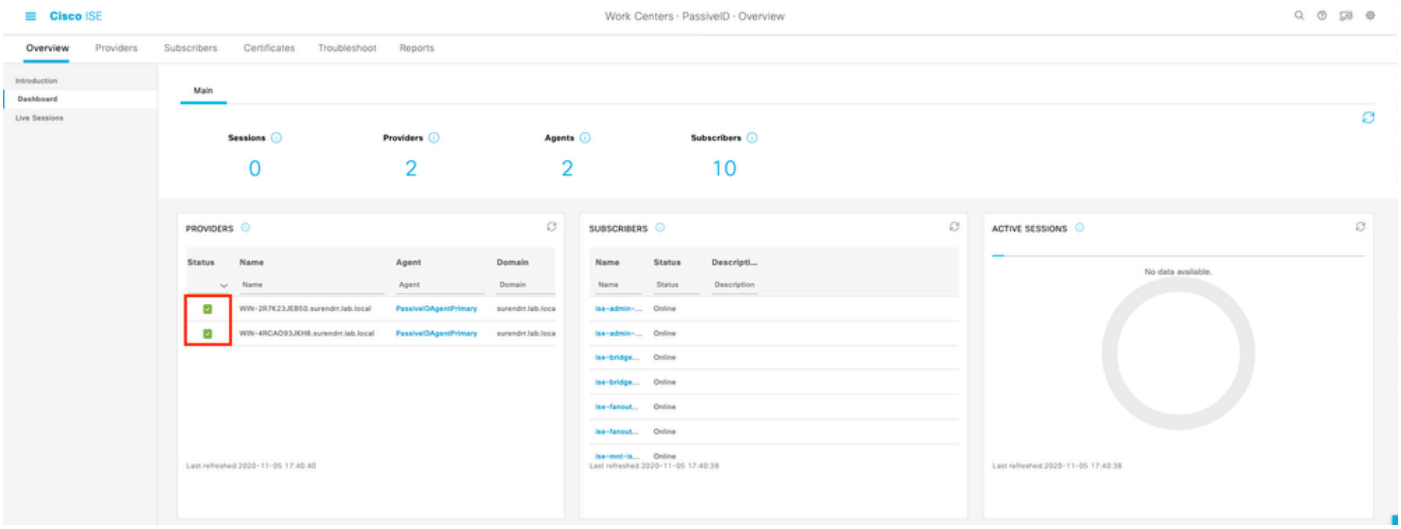
2. 在Work Centers > PassiveID > Providers > Active Directory > Connection下验证ISE Active Directory提供程序是否已连接到域控制器。



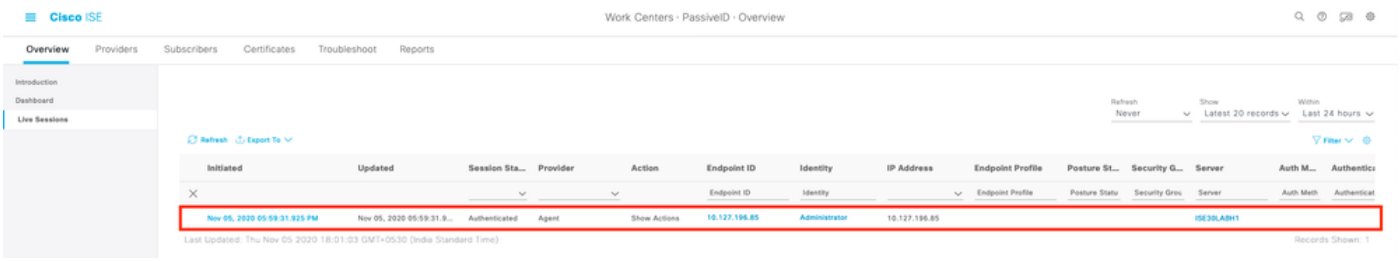
3. 验证Agent at Work Centers > PassiveID > Providers > Active Directory > PassiveID是否监视所需的域控制器。



4. 验证受监控的域控制器的状态是否为up。例如，在Work Centers > PassiveID > Overview > Dashboard的控制面板上标记为绿色。

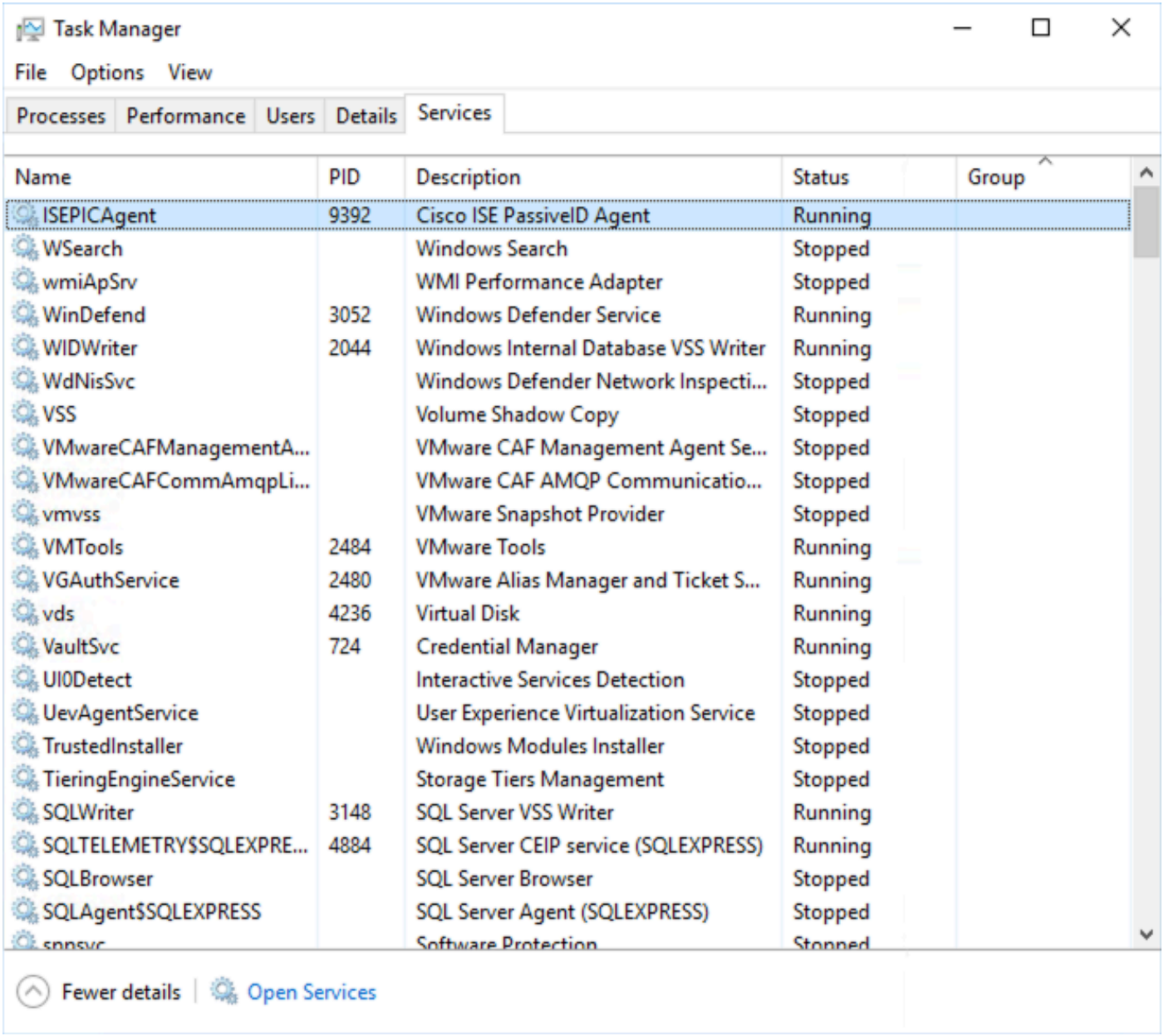


5. 验证当在Work Centers > PassiveID > Overview > Live Sessions的域控制器上注册Windows登录时是否填充了实时会话。



验证Windows服务器上的代理服务

1. 验证安装了PIC Agent的服务器上的ISEPICAgent服务。


Task Manager
File Options View
Processes Performance Users Details Services
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
Fewer details
Open Services

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。