配置基于EVT的身份服务引擎被动ID代理

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

需要新协议

- 使用MS-EVEN6的优势
  - 高可用性
  - 可扩展性
  - 扩展测试设置架构
  - 历史事件查询
  - 减少处理开销

配置

- 连接图
- 配置
  - 为PassiveID代理配置ISE
  - 了解PassiveID代理配置文件

验证

- 验证ISE上的PassiveID服务
- 验证Windows Server上的代理服务
- Windows AD域中的必需设置 — 组策略对象(GPO)

简介

本文档介绍在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代理的优势，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，该解决方案还使用Cisco FirePower管理中心。

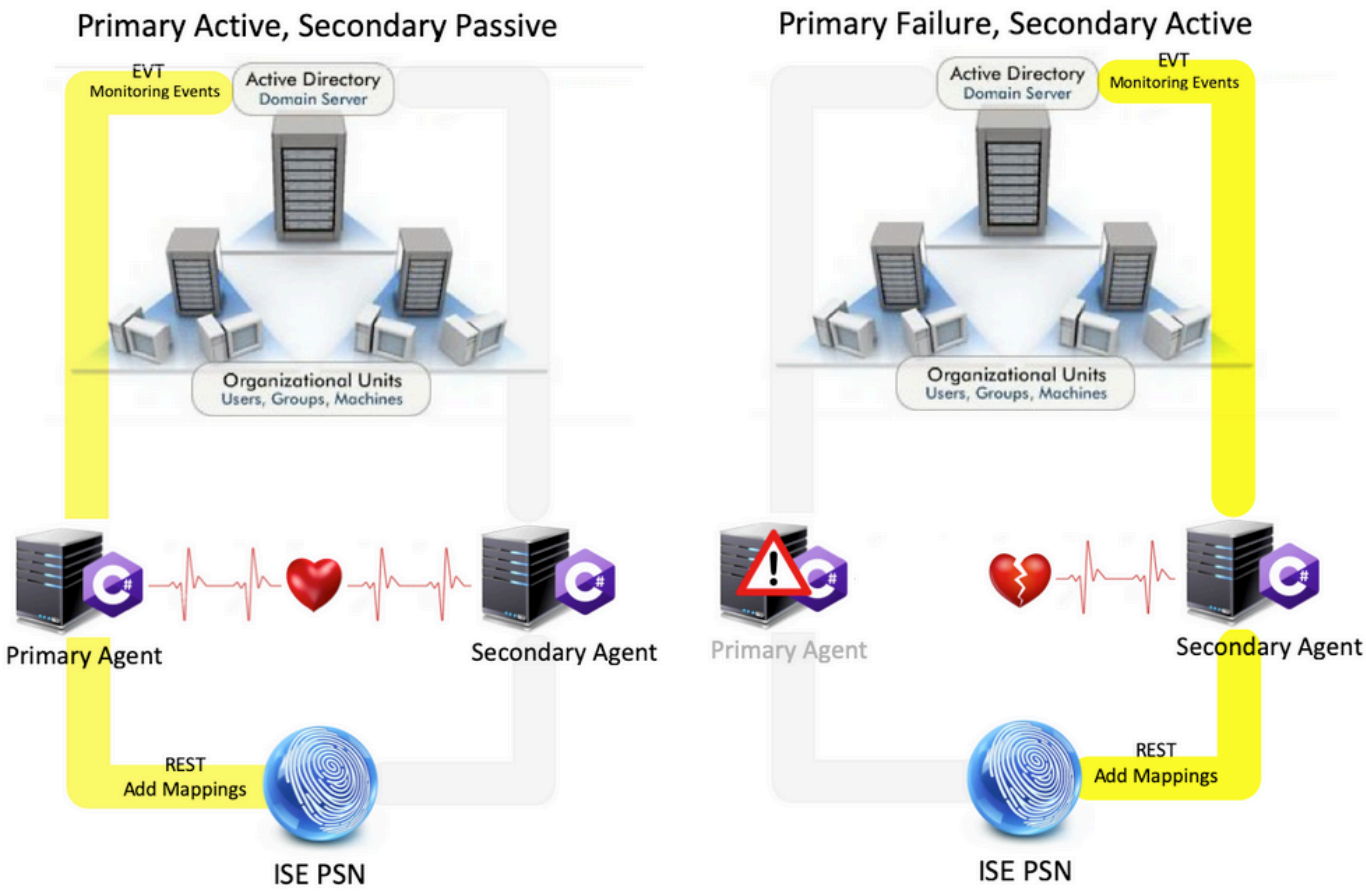
需要新协议

ISE的被动身份（被动ID）功能驱动许多重要使用案例，包括基于身份的防火墙、EasyConnect等。此功能取决于监控登录Active Directory域控制器并获取其用户名和IP地址的用户的能力。用于监控域控制器的当前主协议是WMI。但是，它难以配置/无法配置，会对客户端和服务器造成性能影响，有时在大规模部署中查看登录事件时会有极高的延迟。通过深入研究和备用方式轮询被动身份服务所需的信息，我们决定采用替代协议 — 称为事件处理API(EVT)，该协议在处理此使用案例时更有效。它有时也称为MS-EVEN6，也称为事件远程协议，它是基于RPC的有线基础协议。

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，将错过登录事件，基于身份的防火墙等功能将在此期间丢失数据。这是在此版本之前使用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。

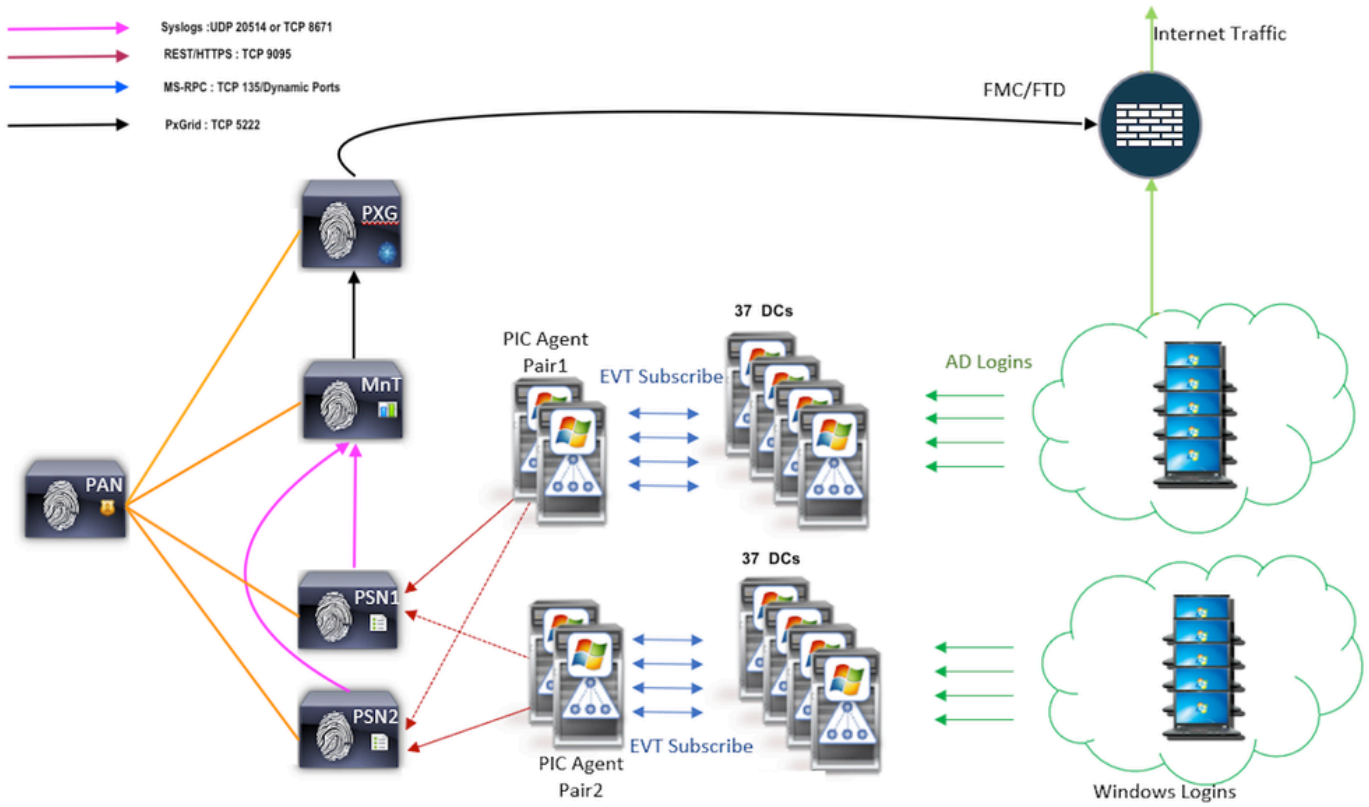


可扩展性

新代理通过增加支持数量的域控制器数量及其可以处理的事件数量来提供更好的支持。以下是测试过的规模数字：

- 监控的域控制器的最大数量（有2对代理）：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

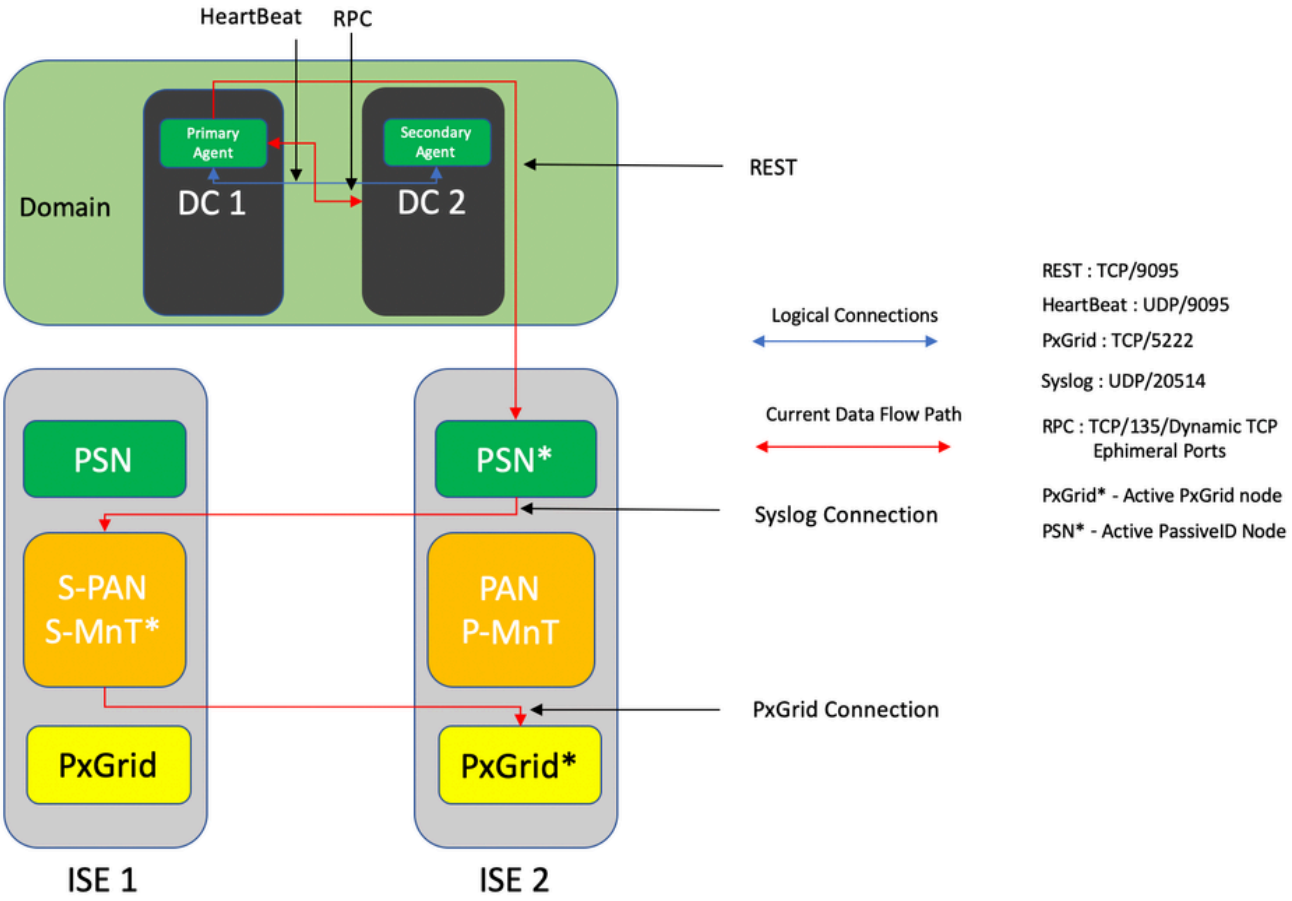
如果发生故障切换，或者对PIC-Agent执行服务重启以确保没有数据丢失，将再次查询过去在配置时间内生成的事件，并将其发送到PSN节点。默认情况下，ISE会查询从服务开始起价值60秒的过去事件，以弥补服务丢失期间的任何数据丢失。

减少处理开销

与WMI不同，EVT在大规模或重负载下会占用大量CPU，EVT不会像WMI那样占用太多资源。规模测试表明，使用EVT后，查询性能得到了显着提高。

配置

连接图

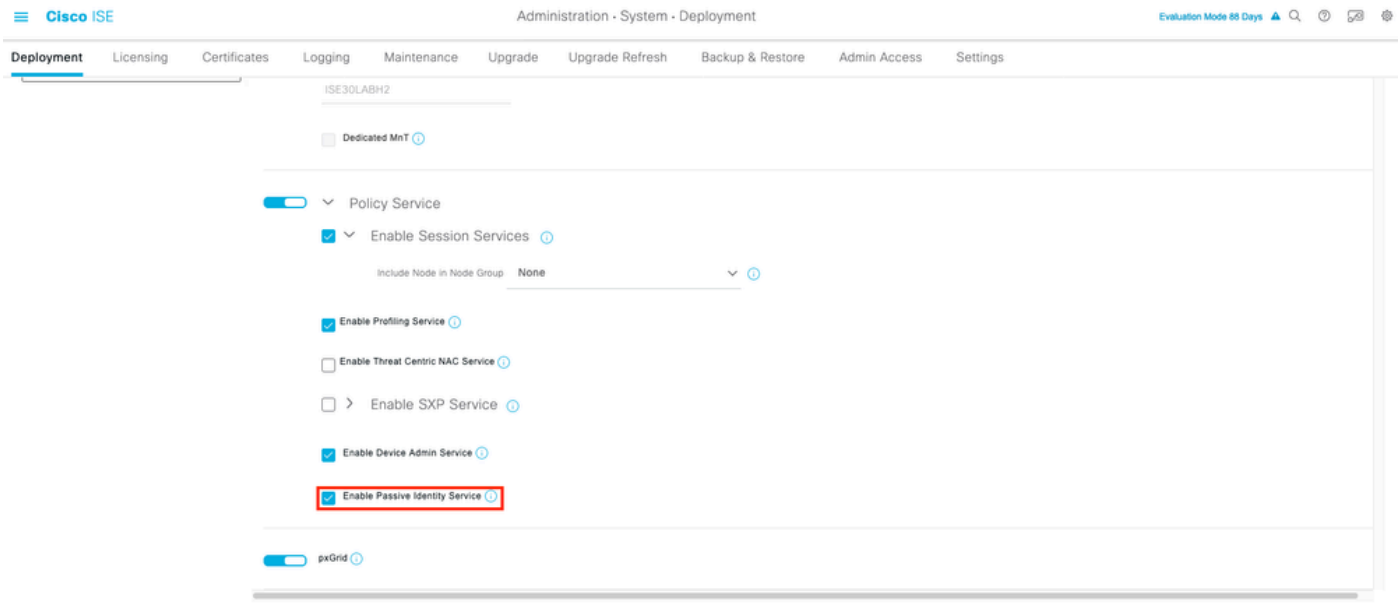


配置

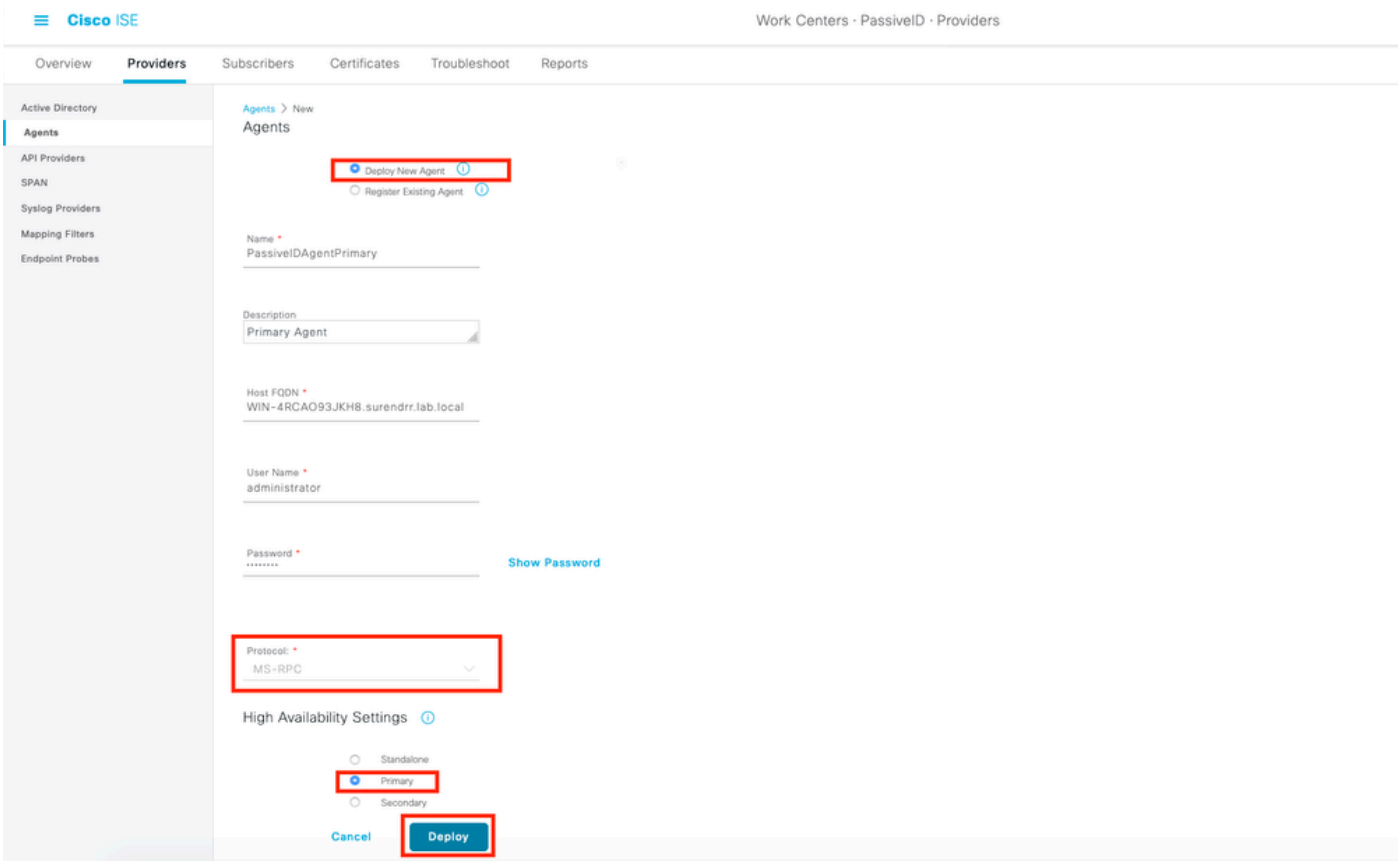
为PassiveID代理配置ISE

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被动身份服务，该服务在主用/备用操作模式下运行。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Active Directory域，请参阅Active Directory集成指南。

导航到Administration > System > Deployment > [Choose a PSN] > Edit以启用被动身份服务，如下所示：



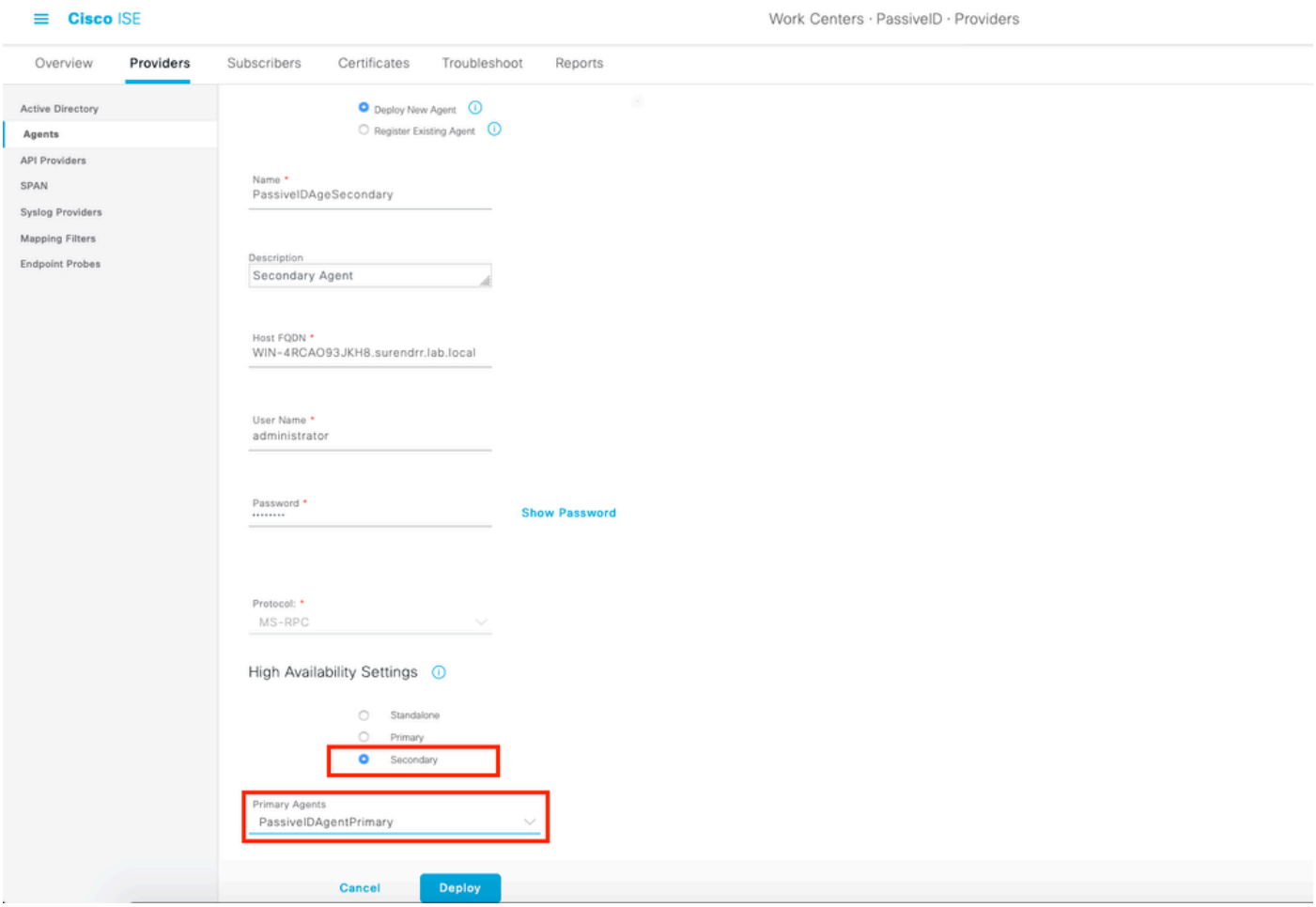
导航到工作中心(Work Centers)>被动ID(PassiveID)>提供商(Providers)>代理(Agents)>添加(Add)，以部署新代理，如下所示：



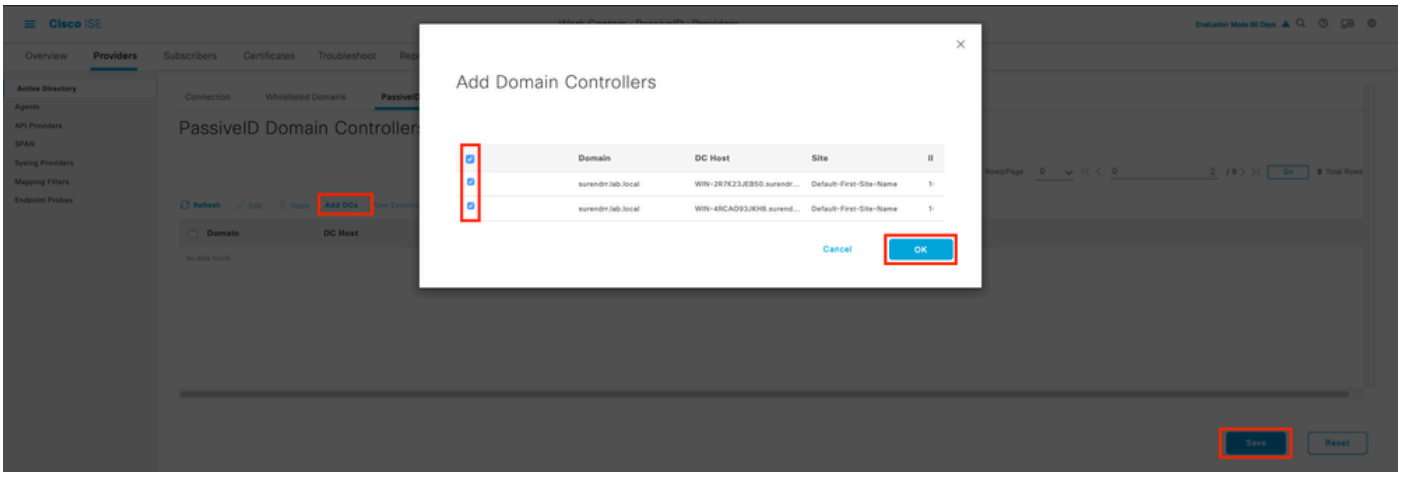
注意：1.如果代理由ISE安装在域控制器上，此处使用的帐户必须具有足够的特权来安装程序，并在主机完全限定域名(FQDN)字段中提到的服务器上运行该程序。此处的主机FQDN可以是成员服务器（而不是域控制器）的FQDN。

2.如果代理已手动安装，或者从以前的ISE部署通过MSRPC安装，则Active Directory或Windows端所需的权限和配置与WMI相比，PIC代理使用的另一个协议（以及3.0之前唯一可用的协议）更少。在这种情况下，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Register Existing Agent，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。

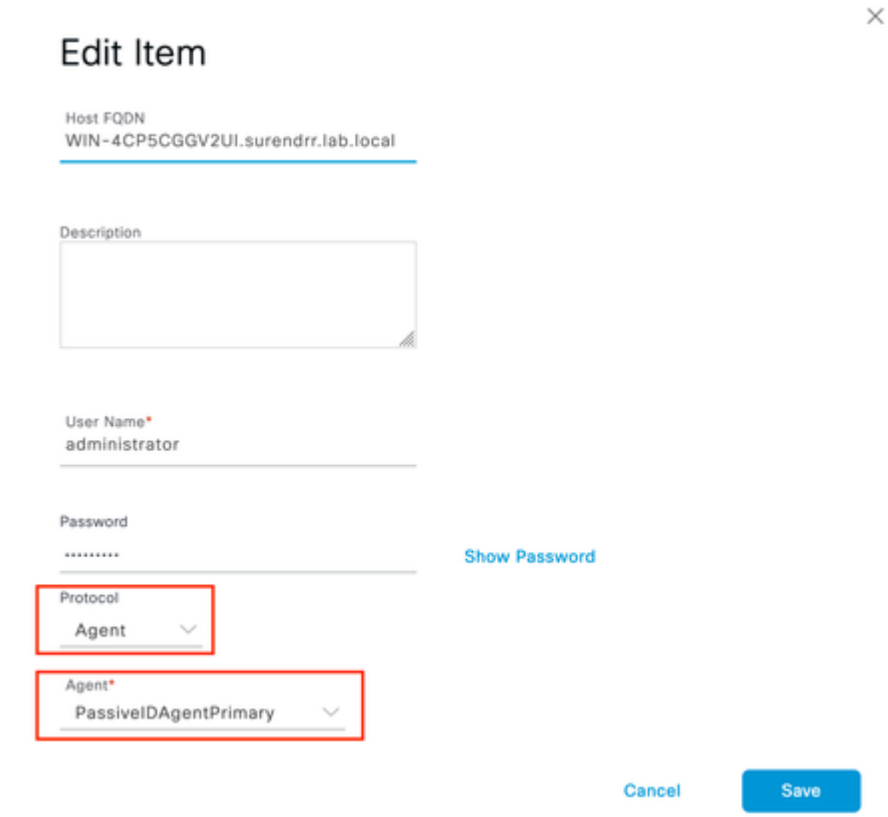
成功部署后，在其他服务器上配置另一个代理，并将其添加为辅助代理，然后添加其主要对等体，如此图所示。



要监控使用代理的域控制器，请导航到工作中心(Work Centers)> PassiveID >提供程序(Providers)> Active Directory > [点击加入点(Join Point)] > PassiveID。单击Add DC并选择域控制器（从中检索用户 — IP映射/事件），单击OK，然后单击Save以保存更改，如本图所示。



要指定可用于从中检索事件的代理，请导航到Work Centers > PassiveID > Providers > Active Directory > [Click on the Join Point] > PassiveID。选择域控制器，然后单击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。



监控域控制器

注意：本节中提供了配置和测试选项，一直到版本3.0 Patch 4为止。

了解PassiveID代理配置文件

PassiveID Agent配置文件位于C:\Program Files(x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config。配置文件包含如下所示的内容：

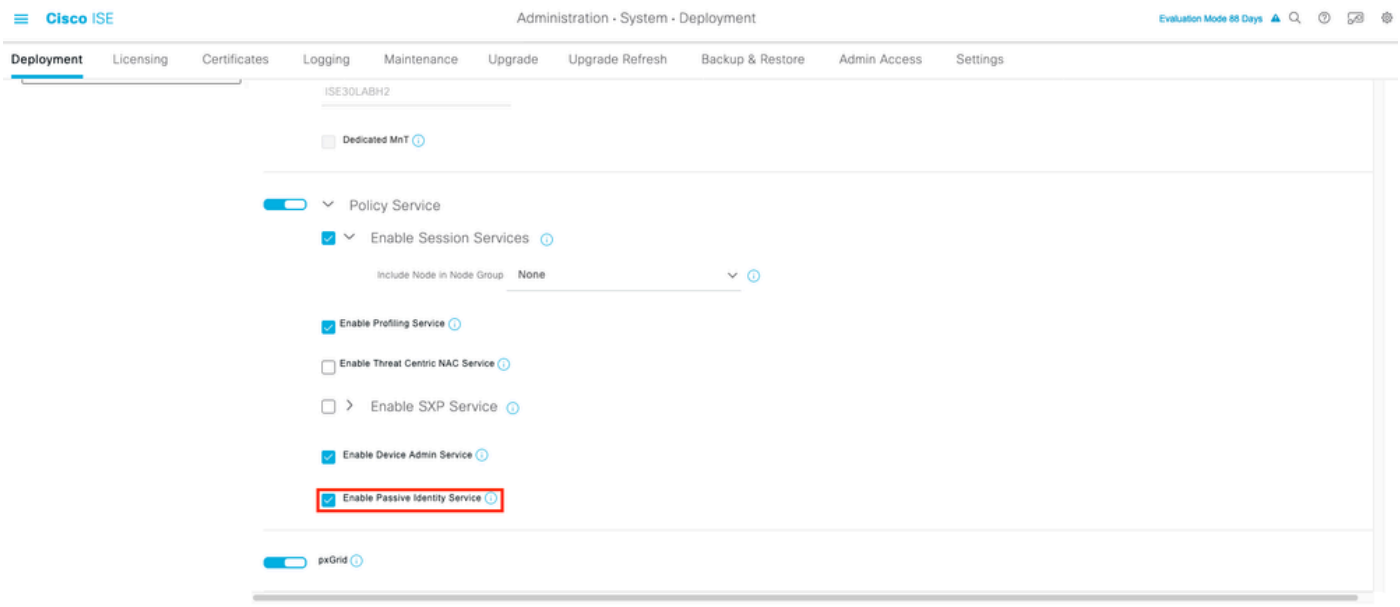
```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
<configSections>
<section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler， log4net"/>
</configSections>
<log4net>
<root>
<level value="DEBUG" /> <! — 日志记录级别：OFF、FATAL、ERROR、WARN、INFO、DEBUG、ALL —>
<! — 该设置为其运行所在的服务器上的PassiveID Agent收集的日志的日志级别。-- >
<appender-ref ref="RollingFileAppender" />
</root>
<appender name="RollingFileAppender" type="log4net.Appender.RollingFileAppender">
<file value="CiscoISEPICAgent.log" /> <! — 请勿修改此 — >
<appendToFile value="true" />
<rollingStyle value="Size" />
<maxSizeRollBackups value="5" /> <! — 此数字设置回滚之前生成的日志文件的最大数量 — >
<maximumFileSize value="10MB" /> <! — 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 value="%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"/> <! — 此数字定义代理等待心跳的最长时间（以毫秒为单位），超过此持续时间后，另一个代理被降级 — >
<add key="showHeartbeats" value="false" /> <! — 将该值更改为"true"可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。除非思科TAC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的介质类型。请勿更改此值 — >
<add key="maxHistorySeconds" value="60" /> <! — 定义服务重新启动时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"，查看接收并发送到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，对于故障转移，与主动PassiveID PSN节点通信时可能发生的错误数将计入 — >
<add key="nodeFailoverMaxErrors" value="5" /> <! — 定义在故障切换到备用PassiveID PSN节点之前，在指定节点FailoverTimeSpan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服务是否在GUI上启用，并且在ISE的CLI上使用show application status ise命令标记为正在运行。



<#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

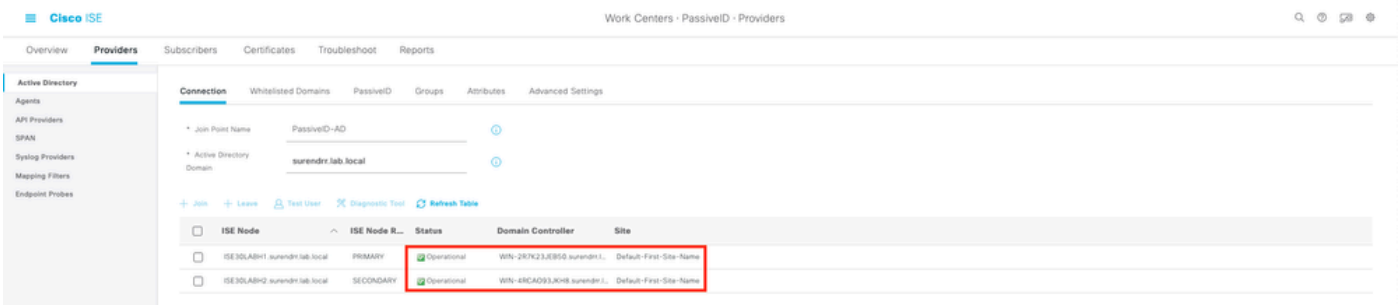
PassiveID Endpoint Service running

18281

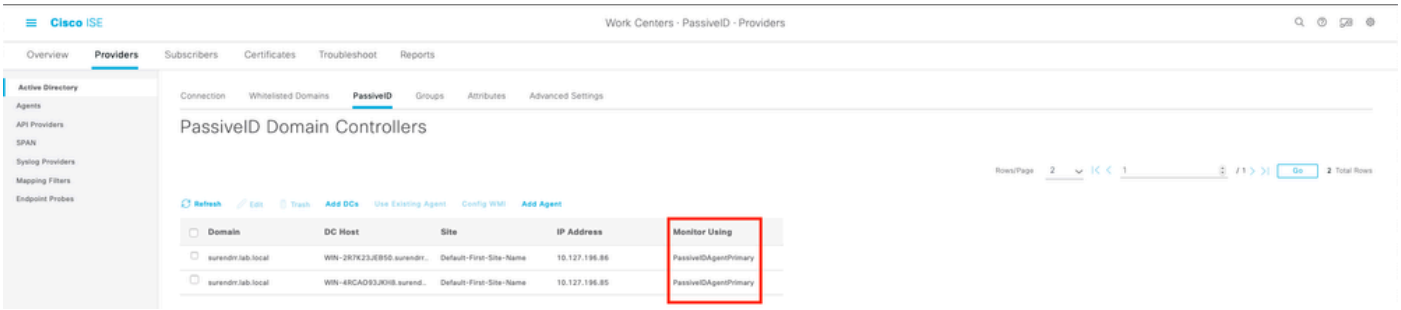
PassiveID SPAN Service running

```
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
```

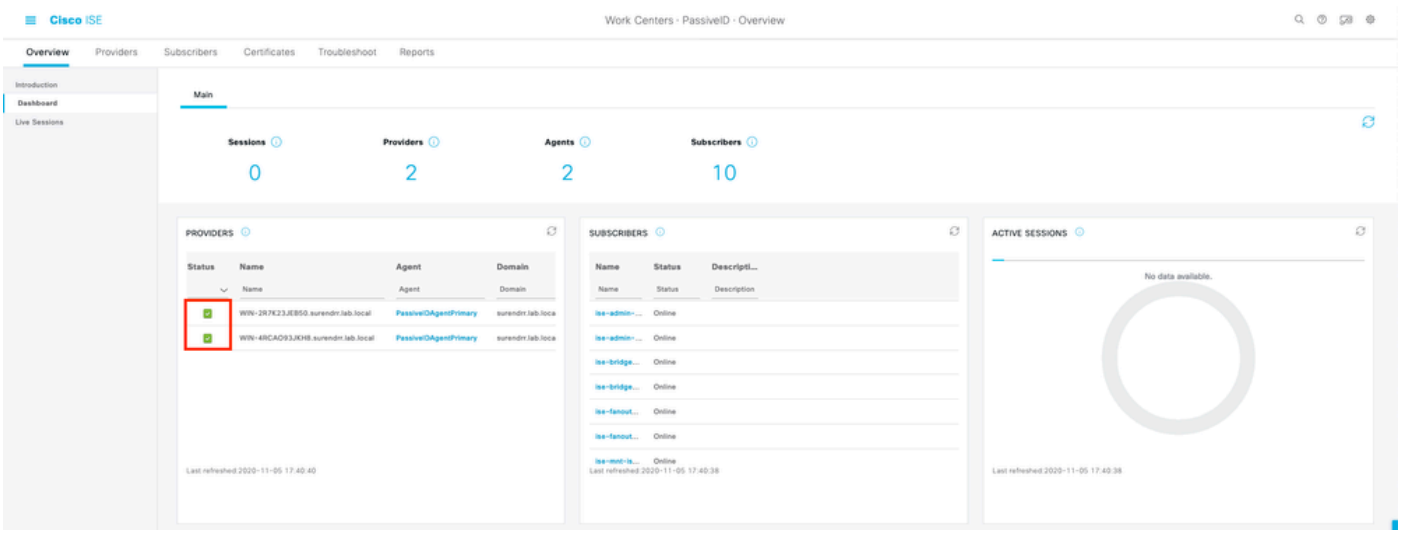
2.验证ISE Active Directory提供程序是否已连接到位于Work Centers > PassiveID > Providers > Active Directory > Connection的域控制器。



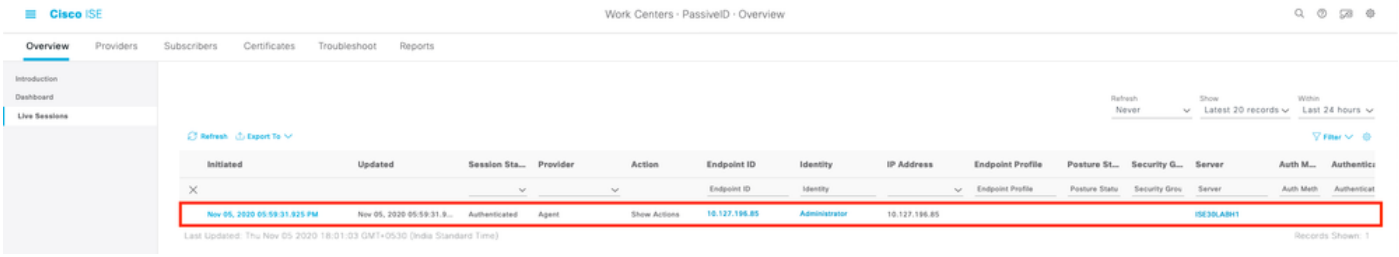
3.验证所需域控制器是否由Agent at Work Centers > PassiveID > Providers > Active Directory > PassiveID监控。



4.验证受监控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。

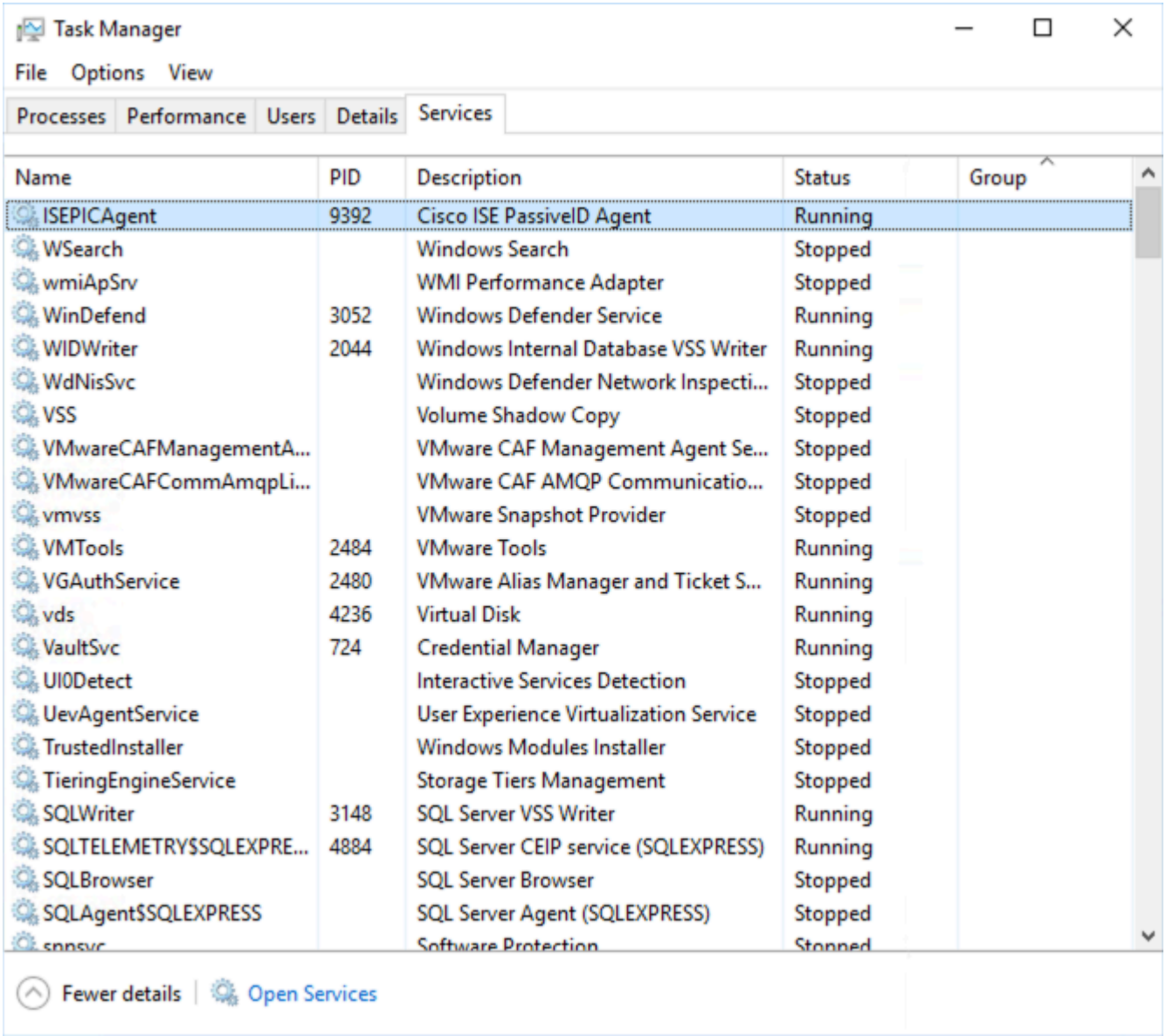


5.验证在域控制器上注册Windows登录时是否在Work Centers > PassiveID > Overview > Live Sessions中填充实时会话。



验证Windows Server上的代理服务

1.验证安装了PIC Agent的服务器上的ISEPICAgent服务。



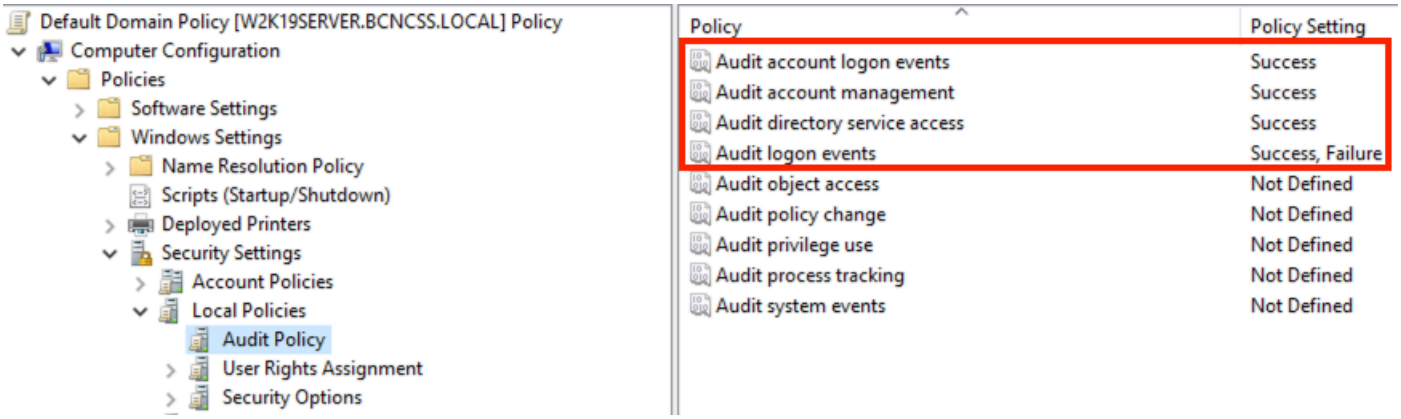
Windows AD域中的必需设置 — 组策略对象(GPO)

1.为使ISE PIC代理能够读取用户登录和注销事件条目，使用的帐户可以是服务帐户（没有密码过期

），也可以是常规域帐户和事件日志读取器组的成员

2. — 在“域策略”中，确认以下设置已设置为：

默认域策略（或客户用于其域计算机的策略）> Windows设置>安全设置>本地策略>审核策略并启用以下条目：



某些客户依赖高级审计策略配置，而不是使用传统本地策略

.

如果出现这种情况，请设置Advanced 审核策略:在Group Policy Management Editor中。展开Computer Configuration →导航到Policies →导航到Windows Settings →导航到Security Settings →导航到Advanced Audit Policy Configuration →导航到Audit Policies。设置以下审计策略：

帐户管理

·审核计算机帐户管理：成功

·审核通讯组管理：成功

·审核安全组管理：成功

·审核用户帐户管理：成功

DS访问

·审核目录服务访问：成功

登录/注销

·审核注销：成功

用户登录后即可立即看到ISE PIC中的会话条目。

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）。