Configuración del Agente de ID pasiva de Identity Services Engine basado en EVT

Contenido

Introducción

Este documento describe el nuevo ISE Passive Identity Connector (ISE-PIC) Agent introducido en la versión de ISE 3.0, sus ventajas y la configuración de este agente en ISE. ISE Passive Identity Agent se ha convertido en una parte integral de la solución de firewall de identidad gracias a Cisco FirePower Management Center.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administración de Cisco Identity Services
- MS-RPC, protocolos WMI
- Administración de Active Directory

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Identity Services Engine versión 3.0 y posterior
- Estándar de Microsoft Windows Server 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

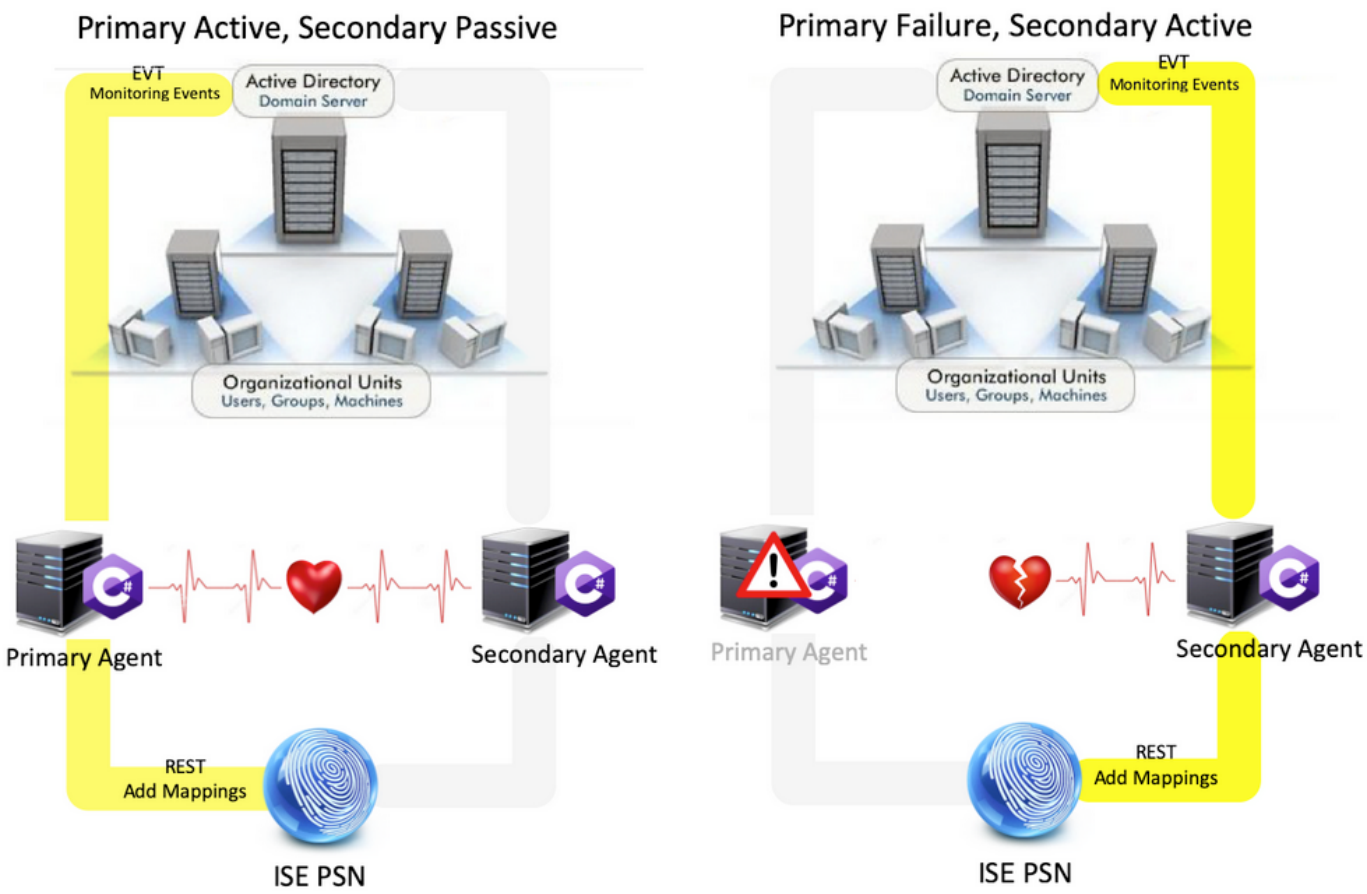
Necesidad de un nuevo protocolo

La función de identidad pasiva (ID pasiva) de ISE impulsa varios casos prácticos importantes, incluidos el firewall basado en identidad, EasyConnect, etc. Esta función depende de la capacidad de supervisar a los usuarios que inician sesión en los controladores de dominio de Active Directory y de aprender su nombre de usuario y sus direcciones IP. El protocolo principal actual que utilizamos para monitorear los controladores de dominio es WMI. Sin embargo, la configuración es difícil/invasiva, tiene un impacto en el rendimiento tanto en los clientes como en los servidores, y a veces tiene una latencia extremadamente alta al ver los eventos de inicio de sesión en implementaciones a escala. Tras una investigación exhaustiva y otras formas de sondear la información requerida para los Servicios de identidad pasiva, se decidió un protocolo alternativo, conocido como EVT o API de evasión, que es más eficiente en el manejo de este caso práctico. A veces se denomina **MS-EVEN6**, también conocido como Eventing Remote Protocol, que es el protocolo RPC subyacente basado en el cable.

Ventajas con el uso de MS-EVEN6

Alta disponibilidad

El agente original no tenía la opción High Availability y, si es necesario realizar el mantenimiento en el servidor en el que el agente se estaba ejecutando o se había producido una interrupción, se perderían los eventos de inicio de sesión y características como Firewall basado en identidad verían una pérdida de datos durante este período. Esta es una de las principales preocupaciones con el uso de ISE PIC Agent antes de esta versión. ISE utiliza UDP Port 9095 para intercambiar latidos entre los agentes.

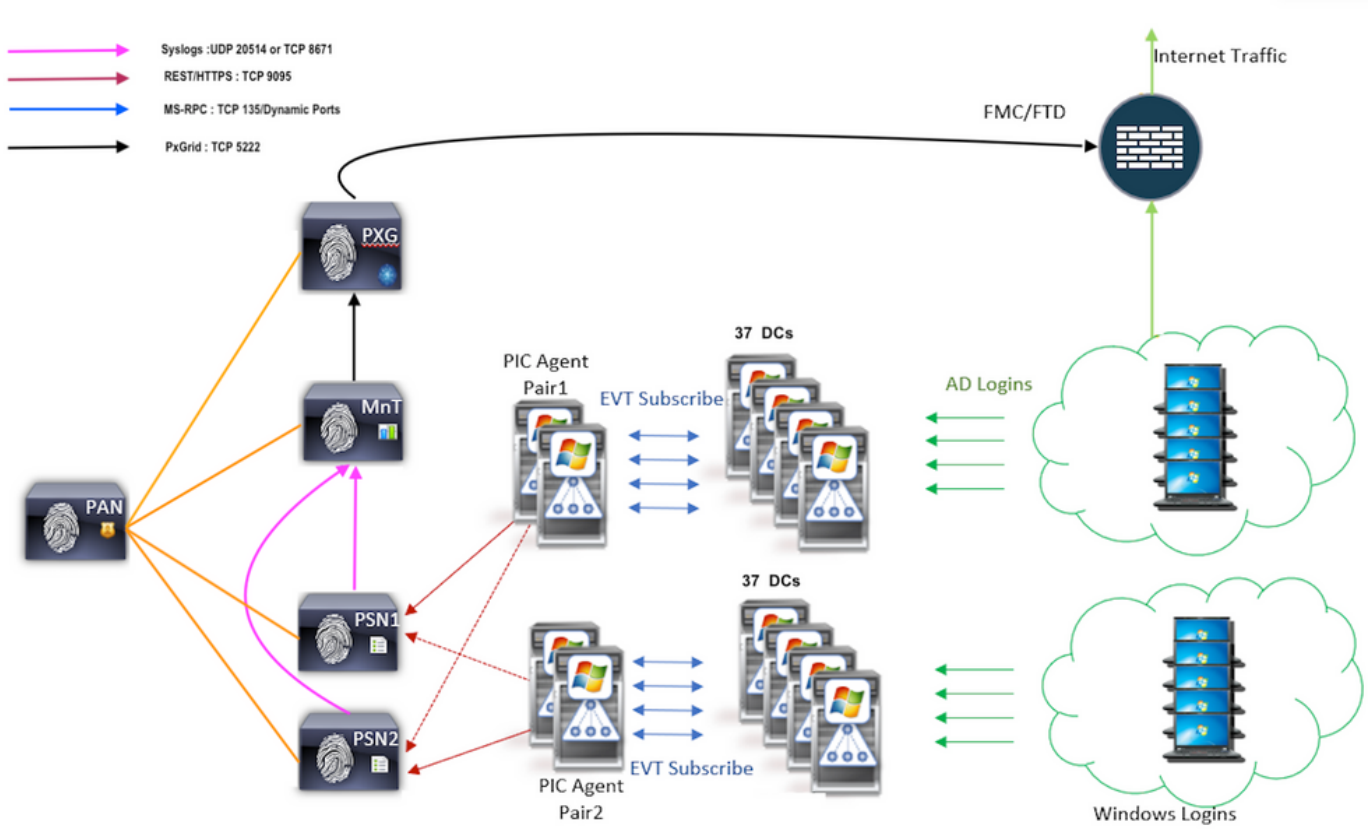


Escalabilidad

El nuevo agente proporciona mejor soporte con mayores números de escala para un número admitido de controladores de dominio y el número de eventos que puede manejar. Estos son los números de escala que se probaron :

- Número máximo de controladores de dominio supervisados (con 2 pares de agentes): 74
- Número máximo de asignaciones/eventos probados: 292 000 (3950 eventos por DC)
- Prueba máxima de TPS: 500

Ampliación de la arquitectura de configuración de pruebas



Consulta de eventos históricos

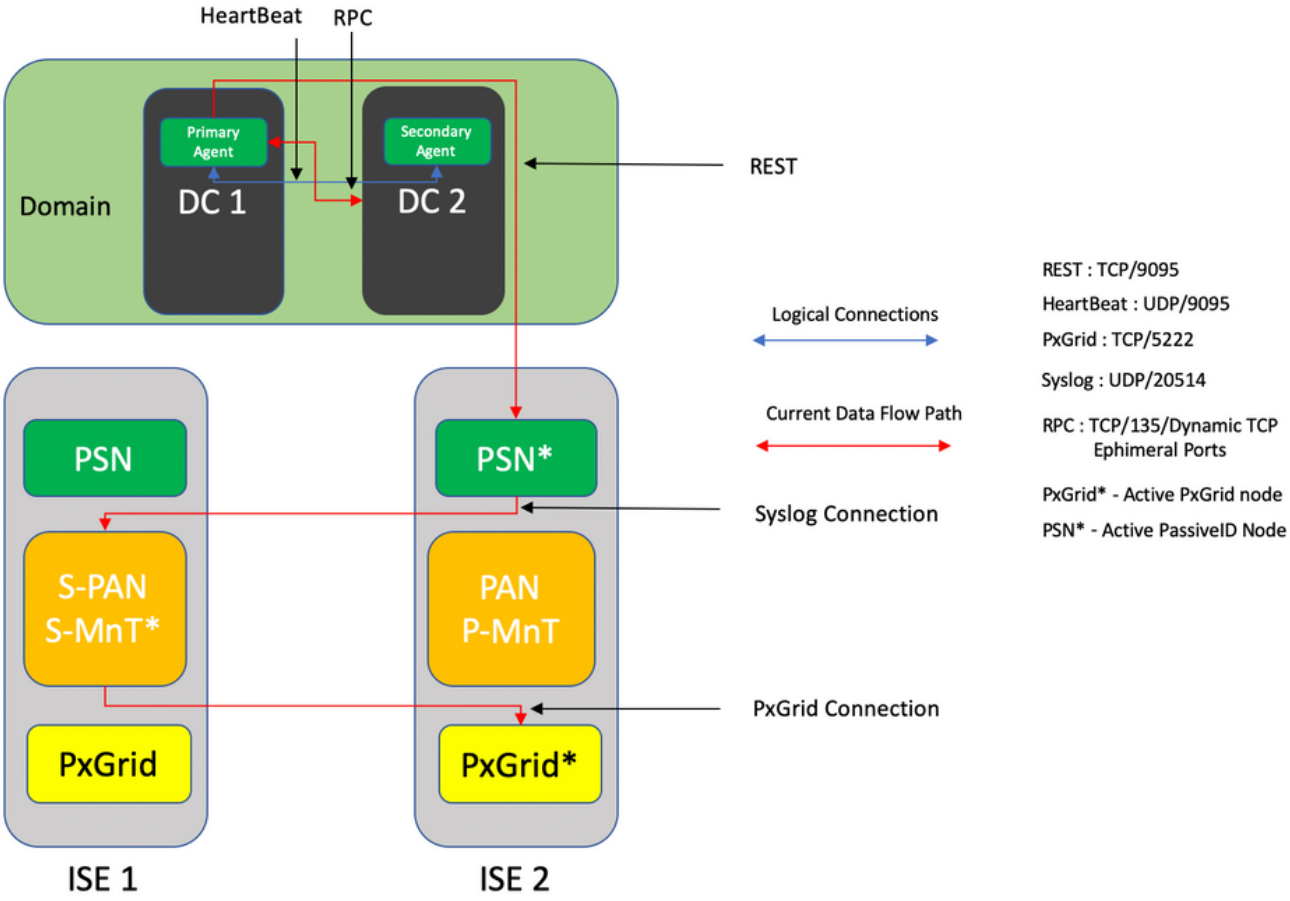
En caso de conmutación por fallas o en caso de que se realice un reinicio del servicio para el agente de PIC, para asegurarse de que no se pierda ningún dato, se consultan los eventos que se generan durante el tiempo dado pasado y se envían nuevamente a los nodos PSN. De forma predeterminada, el ISE consulta el valor de 60 segundos de los eventos pasados desde el inicio del servicio para anular cualquier pérdida de datos durante la pérdida del servicio.

Menos gastos generales de procesamiento

A diferencia de WMI, que es una CPU intensa en gran escala o carga pesada, EVT no consume tantos recursos como WMI. Las pruebas de escala mostraron un rendimiento muy mejorado de las consultas con el uso de EVT.

Configurar

Diagrama de conectividad

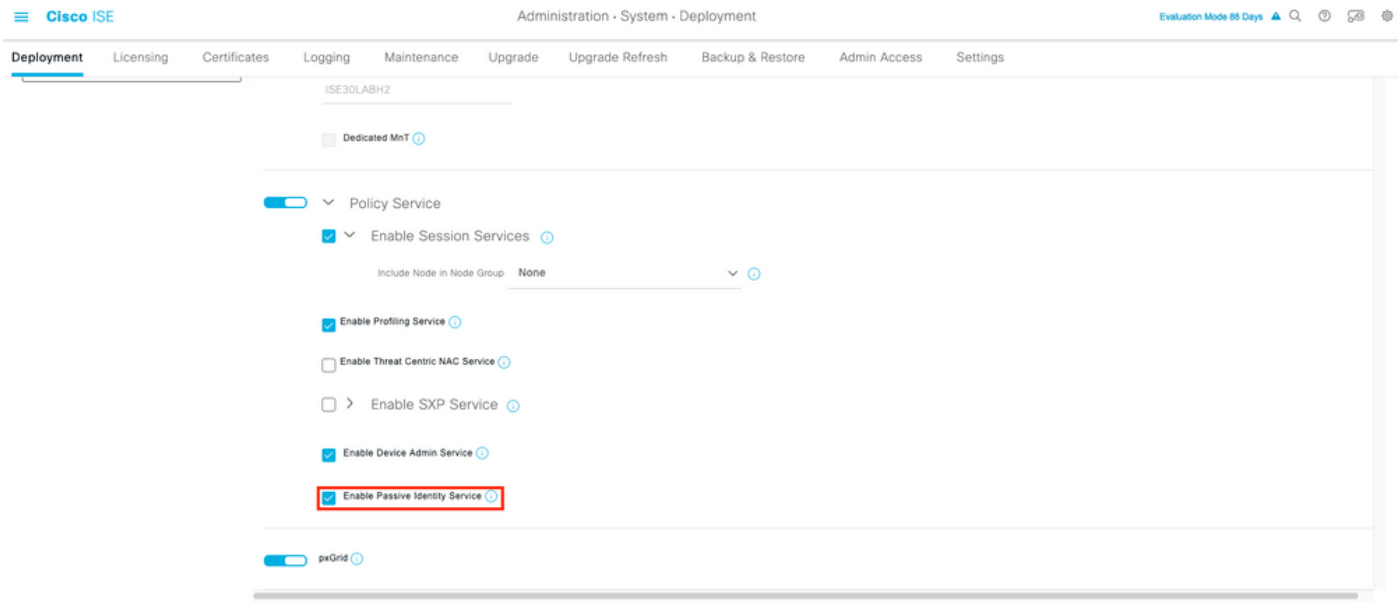


Configuraciones

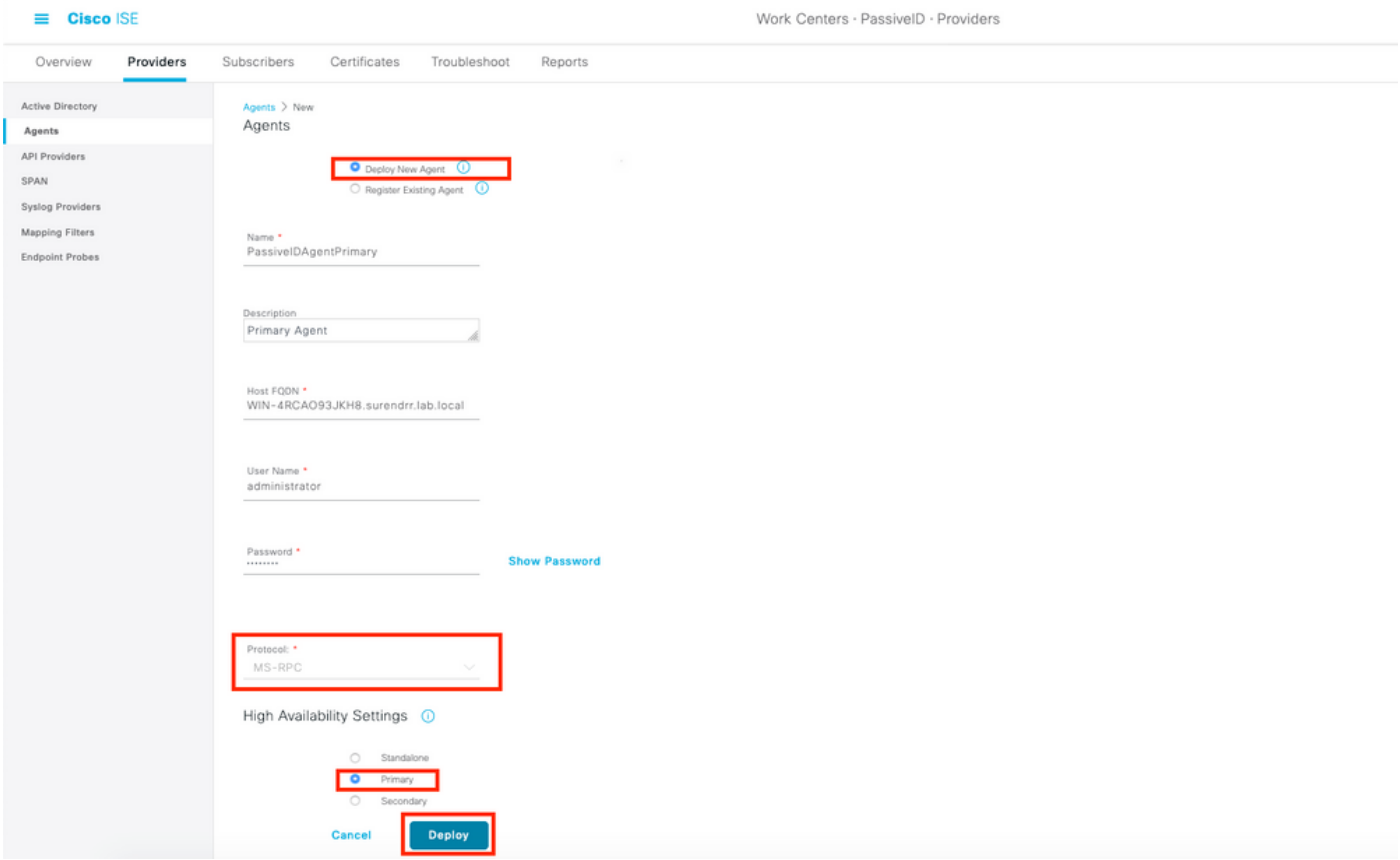
Configuración de ISE para Agente PassiveID

Para configurar los servicios PassiveID, uno debe tener los Servicios de identidad pasiva habilitados en al menos un nodo de servicio de políticas (PSN). Se puede utilizar un máximo de dos nodos para Passive Identity Services que funciona en modo de funcionamiento Activo/En espera. ISE también se debe unir a un dominio de Active Directory y sólo los controladores de dominio presentes en ese dominio pueden ser supervisados por agentes configurados en ISE. Para unirse a ISE a un dominio de Active Directory, refiérase a la Guía de Integración de Active Directory.

Vaya a **Administration > System > Deployment > [Choose a PSN] > Edit** para habilitar Passive Identity Services como se muestra aquí :



Navegue hasta **Centros de trabajo > ID pasivo > Proveedores > Agentes > Agregar** para implementar un nuevo agente como se muestra aquí :

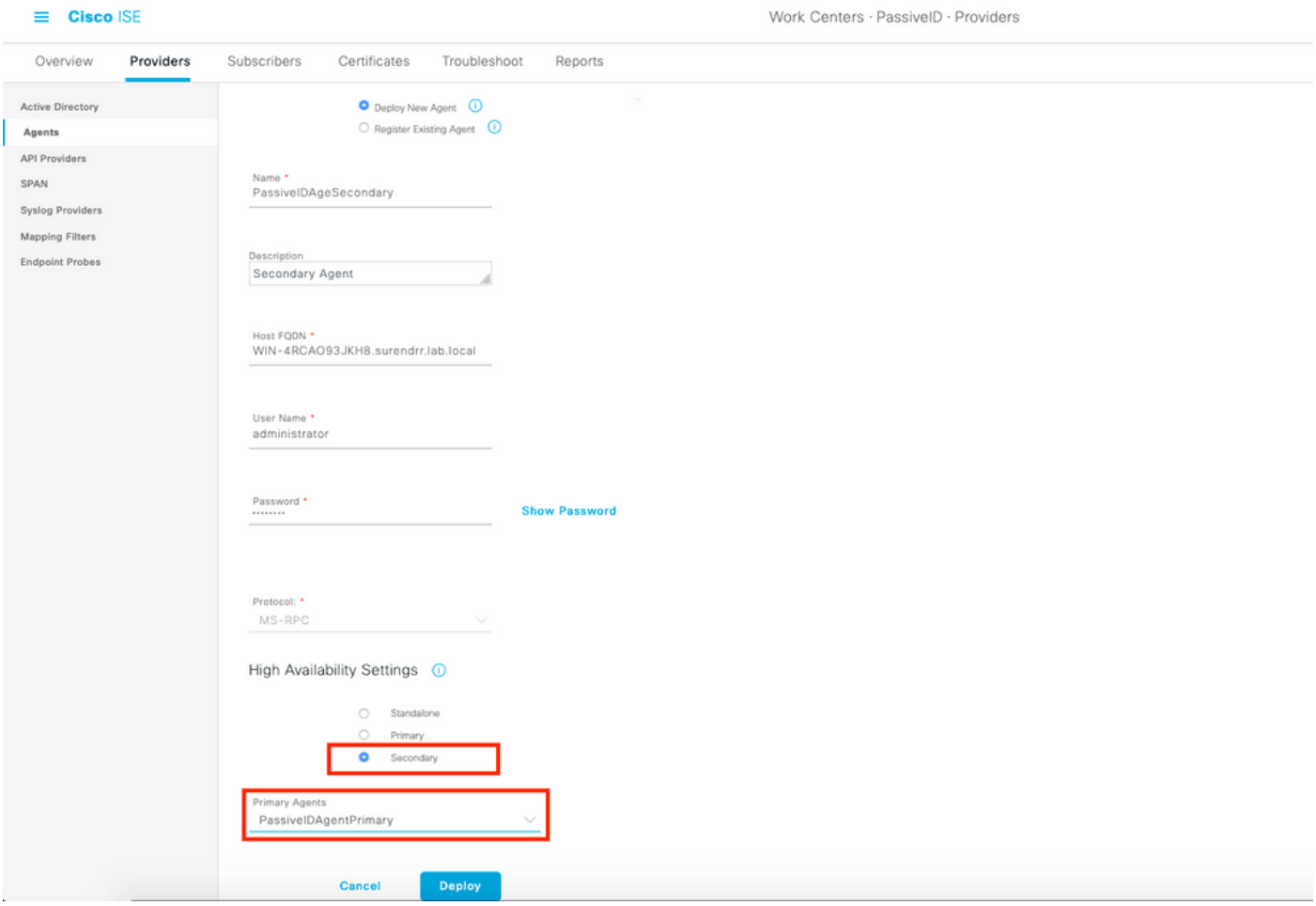


Nota: 1. Si ISE tiene previsto instalar el agente en el controlador de dominio, la cuenta utilizada aquí debe tener privilegios suficientes para instalar un programa y ejecutarlo en el servidor mencionado en el campo FQDN del host. El FQDN de host aquí puede ser el de un servidor miembro en lugar de un controlador de dominio.

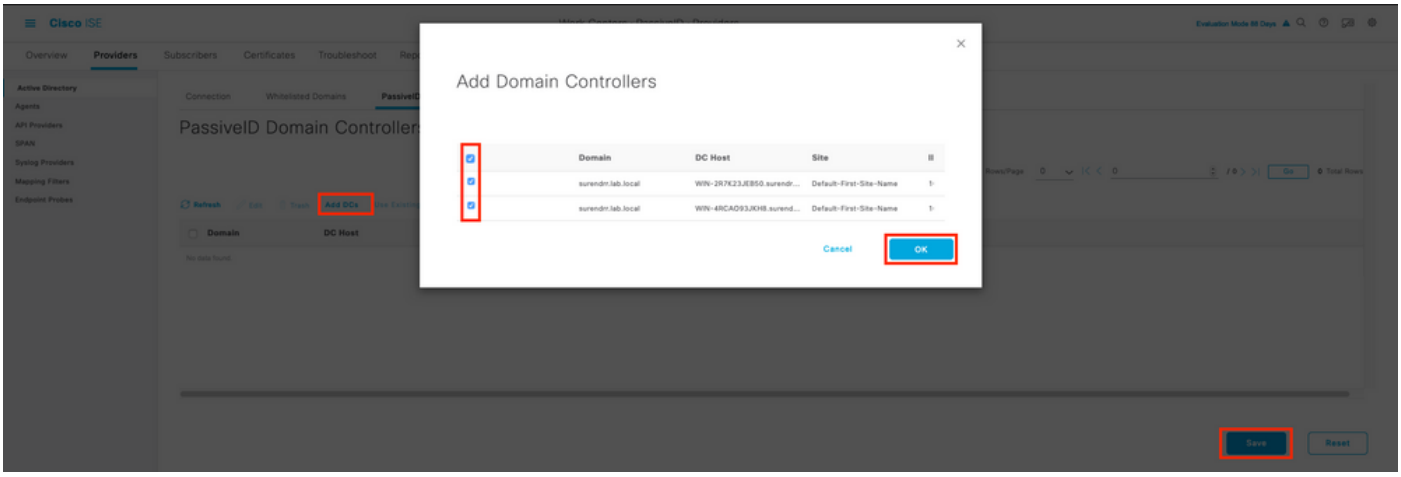
2. Si un agente ya se ha instalado manualmente o desde una implementación anterior de ISE, con MSRPC, los permisos y configuraciones necesarios en el lado de Active Directory o Windows son menos comparados con WMI, el otro protocolo (y el único disponible antes de 3.0) utilizado por los agentes PIC. La cuenta de usuario utilizada en este

caso puede ser una cuenta de dominio regular que forma parte del **grupo de lectores de registros de eventos. Elija Registrar agente existente** y utilice estos detalles de cuenta para registrar el agente que se instala manualmente en los controladores de dominio.

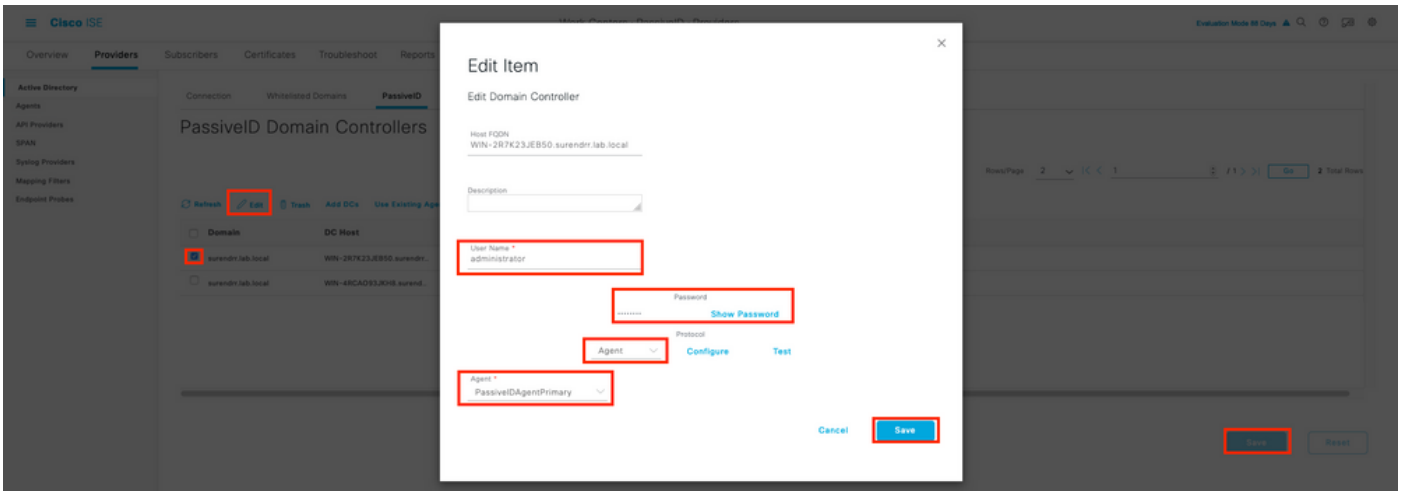
Después de una implementación exitosa, configure otro agente en un servidor diferente y agréguelo como un agente secundario y luego su peer primario como se muestra en esta imagen.



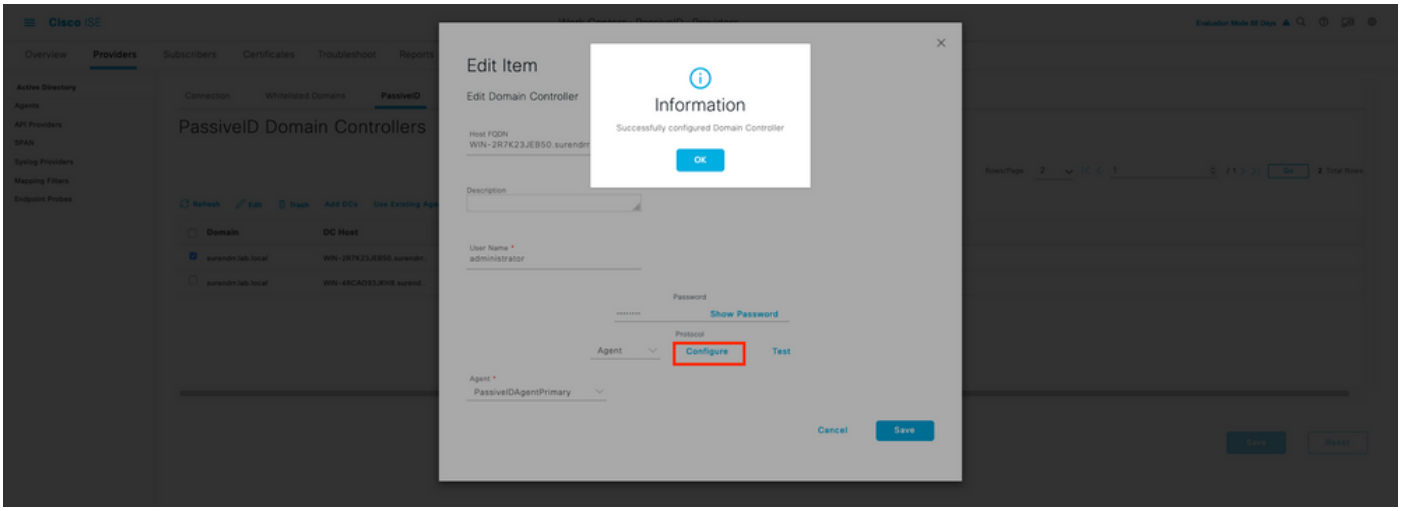
Para monitorear los controladores de dominio usando los agentes, navegue hasta **Centros de trabajo > ID pasivo > Proveedores > Active Directory > [Haga clic en el punto de unión] > ID pasivo**. Haga clic en **Agregar DC** y elija los controladores de dominio desde los cuales se recuperan los eventos/asignaciones de IP de usuario y haga clic en **Aceptar** y luego haga clic en **Guardar** para guardar los cambios, como se muestra en esta imagen.

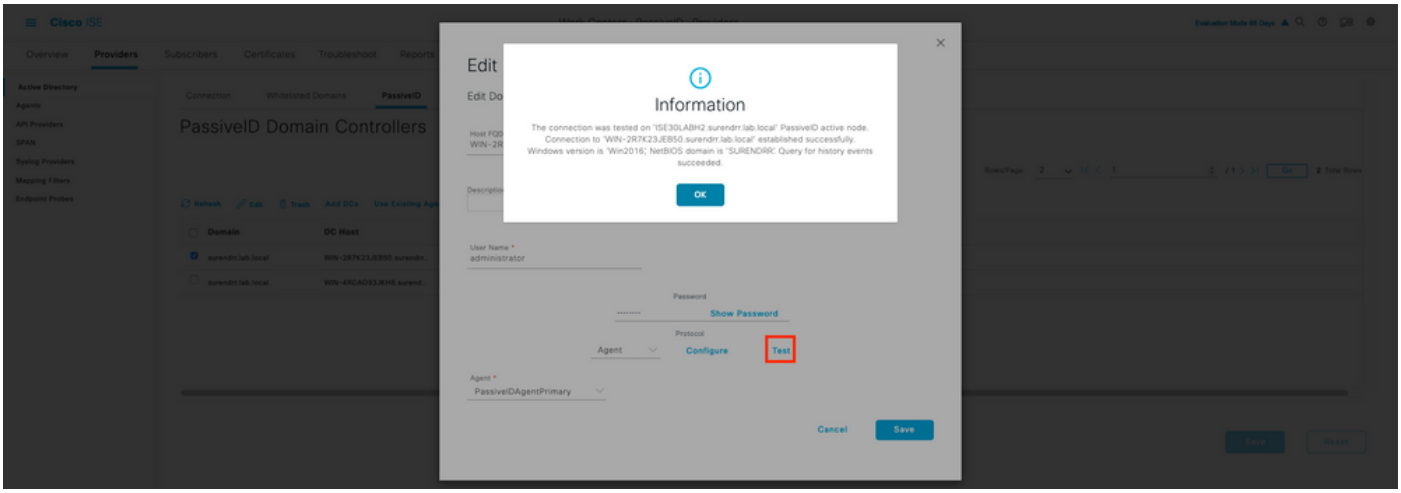


Para especificar los agentes que se deben utilizar para recuperar los eventos, vaya a **Centros de trabajo > ID pasivo > Proveedores > Active Directory > [Haga clic en el punto de unión] > ID pasivo.** Elija los controladores de dominio y haga clic en **Editar**. Introduzca el *nombre de usuario* y la *contraseña*. Elija **Agente** y, a continuación, **Guardar** el cuadro de diálogo. Haga clic en **Guardar** en la ficha PassiveID para completar la configuración.



Se puede verificar si la configuración se aplica correctamente con la ayuda de los botones **Configurar** y **Prueba**, como se muestra en las imágenes aquí:





Comprender el archivo de configuración del agente de PasivoID

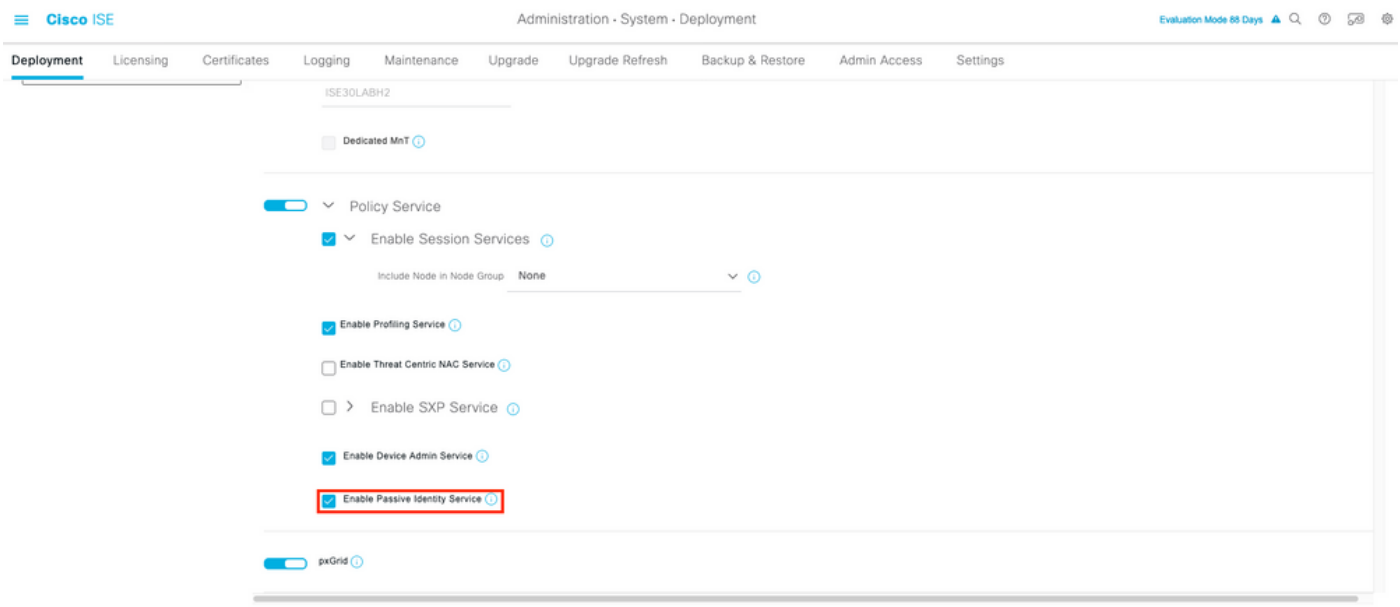
El archivo de configuración de PassiveID Agent se encuentra en **C:\Program Files**

(x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config. Aquí se muestra el contenido del archivo de configuración:

Verificación

Verificar los servicios de PasivoID en ISE

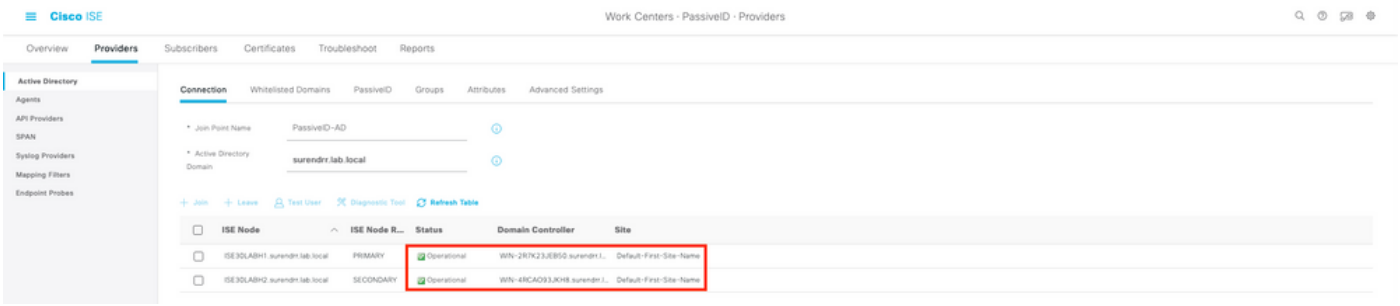
1. Verifique si el servicio PassiveID está habilitado en la GUI y también está marcado ejecutando el comando **show application status ise** en la CLI del ISE.



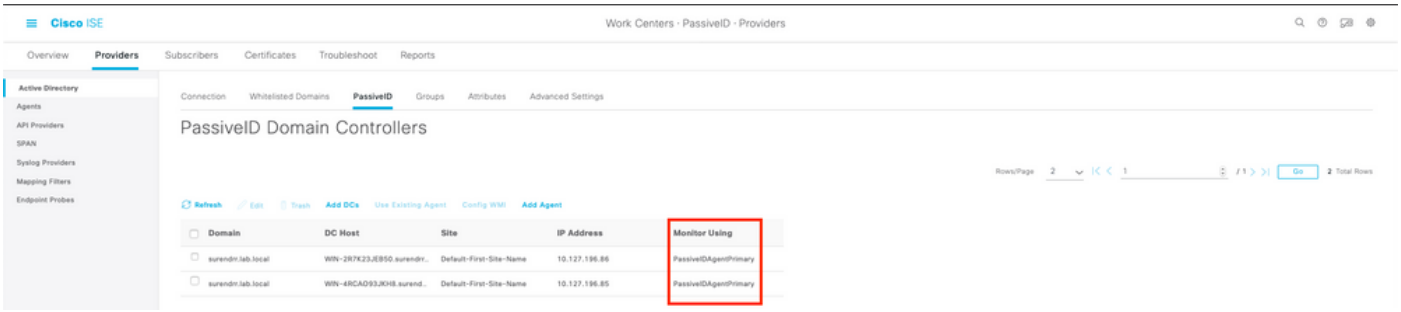

```
ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 129052
Database Server running 108 PROCESSES
Application Server running 9830
Profiler Database running 5127
ISE Indexing Engine running 13361
AD Connector running 20609
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
```

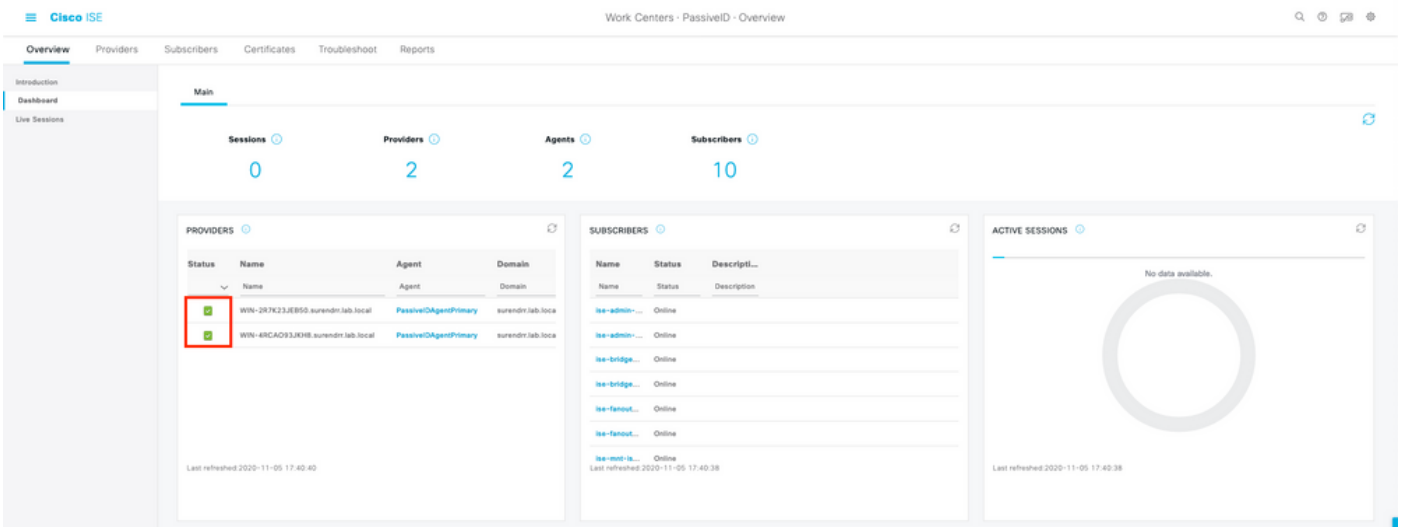
2. Verifique si el proveedor de ISE Active Directory está conectado a los controladores de dominio en **Centros de trabajo > ID pasivo > Proveedores > Active Directory > Conexión**.



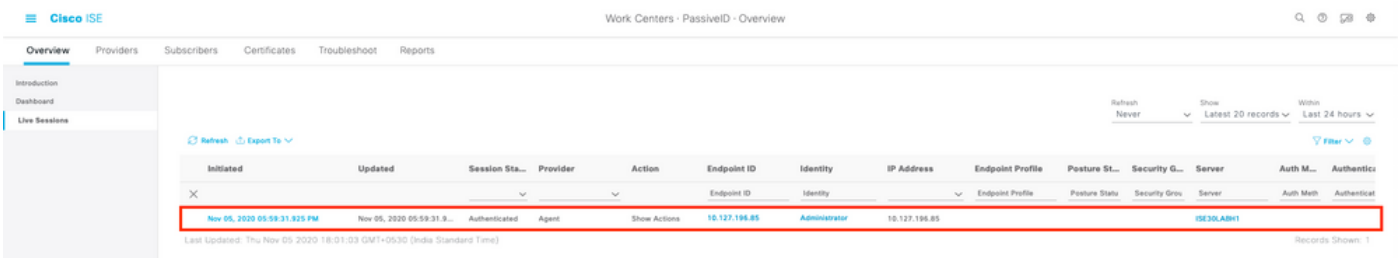
3. Verifique si los controladores de dominio requeridos están siendo monitoreados por el **Agente en los Centros de Trabajo > PasivoID > Proveedores > Active Directory > PasivoID**.



4. Verifique si el estado de los controladores de dominio que se monitorean está activo, es decir, marcado en verde en el panel en **Centros de trabajo > ID pasivo > Descripción general > Panel**.



5. Verifique que las sesiones en directo se completen cuando se registra un inicio de sesión de Windows en el controlador de dominio en **Centros de trabajo > ID pasivo > Descripción general > Sesiones en directo**.



Verificar servicios de agente en Windows Server

1. Verifique el servicio ISEPICAgent en el servidor donde está instalado el agente PIC.