Configurar o Agente de ID Passivo do Identity Services Engine baseado em EVT

Contents

Introduction

Este documento descreve o novo ISE Passive Identity Connector (ISE-PIC) Agent que foi introduzido na versão 3.0 do ISE, suas vantagens e a configuração deste agente no ISE. O ISE Passive Identity Agent tornou-se parte integrante da solução Identity Firewall usando também o Cisco FirePower Management Center.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração do Cisco Identity Services
- Protocolos MS-RPC, WMI
- Administração do Ative Diretory

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Identity Services Engine versão 3.0 e superior
- Microsoft Windows Server 2016 Standard

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

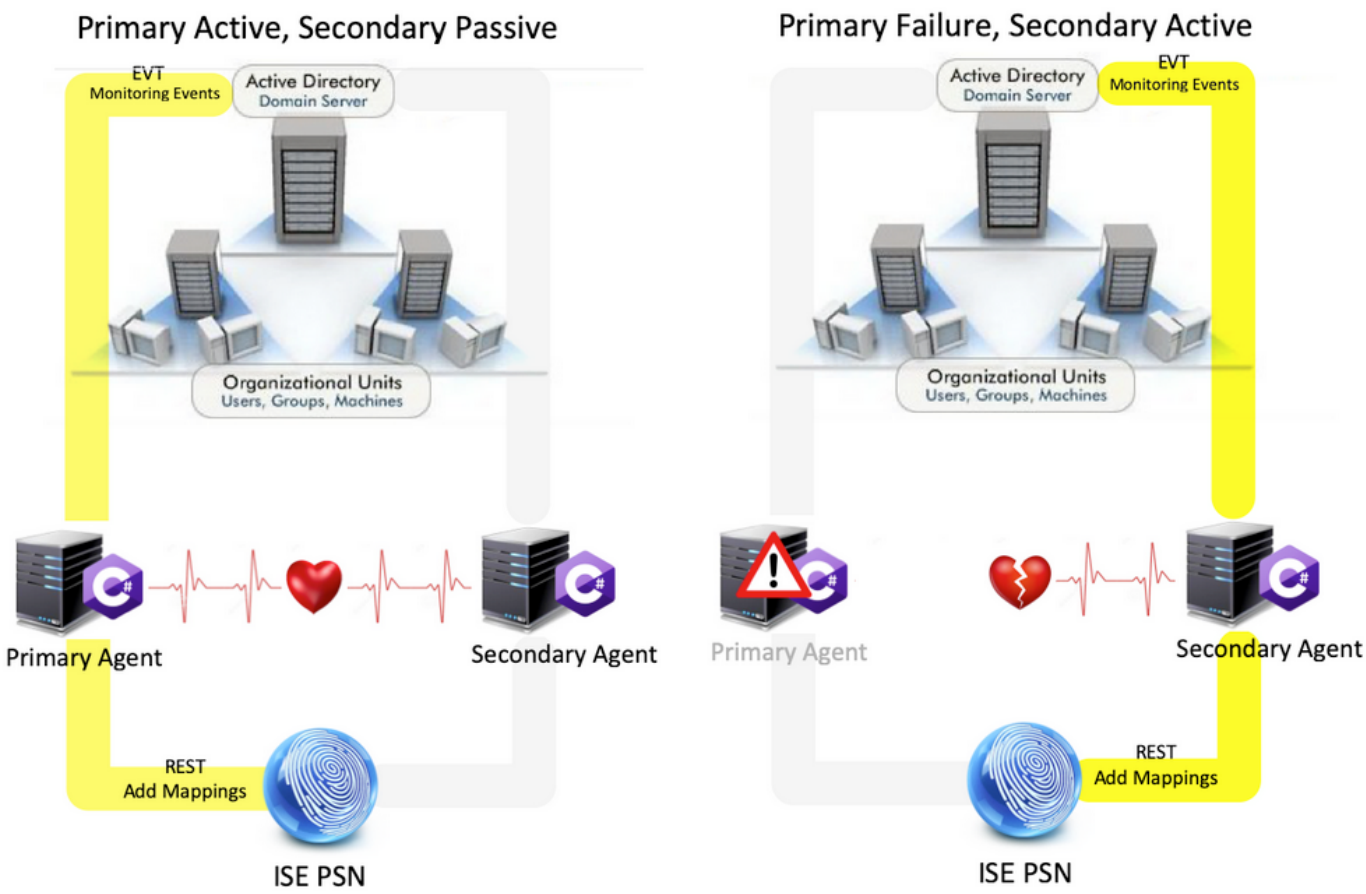
Necessidade de um novo protocolo

O recurso Identidade Passiva (ID Passivo) do ISE gera vários casos de uso importantes, incluindo Firewall Baseado em Identidade, EasyConnect, etc. Esse recurso depende da capacidade de monitorar usuários que fazem login nos Controladores de Domínio do Ative Diretory e aprendem seu nome de usuário e endereços IP. O protocolo principal atual que usamos para monitorar os Controladores de Domínio é WMI. No entanto, é difícil/invasivo configurar, tem um impacto no desempenho de clientes e servidores e, às vezes, tem uma latência extremamente grande para ver eventos de login em implantações escaladas. Depois de uma pesquisa completa e de maneiras alternativas de pesquisar as informações necessárias para os Passive Identity Services, foi decidido um protocolo alternativo, conhecido como EVT ou Eventing API, que é mais eficiente no tratamento desse caso de uso. Às vezes é conhecido como **MS-EVEN6**, também conhecido como Eventing Remote Protocol, que é o protocolo baseado em RPC na rede.

Vantagens com o uso do MS-EVEN6

Alta Disponibilidade

O agente original não tinha opção de Alta Disponibilidade e, se fosse necessário fazer a manutenção no servidor onde o agente estava em execução ou com uma falha, os eventos de logon seriam perdidos e recursos como o Firewall baseado em identidade veriam uma perda de dados durante esse período. Essa é uma das principais preocupações com o uso do ISE PIC Agent antes desta versão. O ISE usa a porta UDP 9095 para trocar heartbeats entre os agentes.

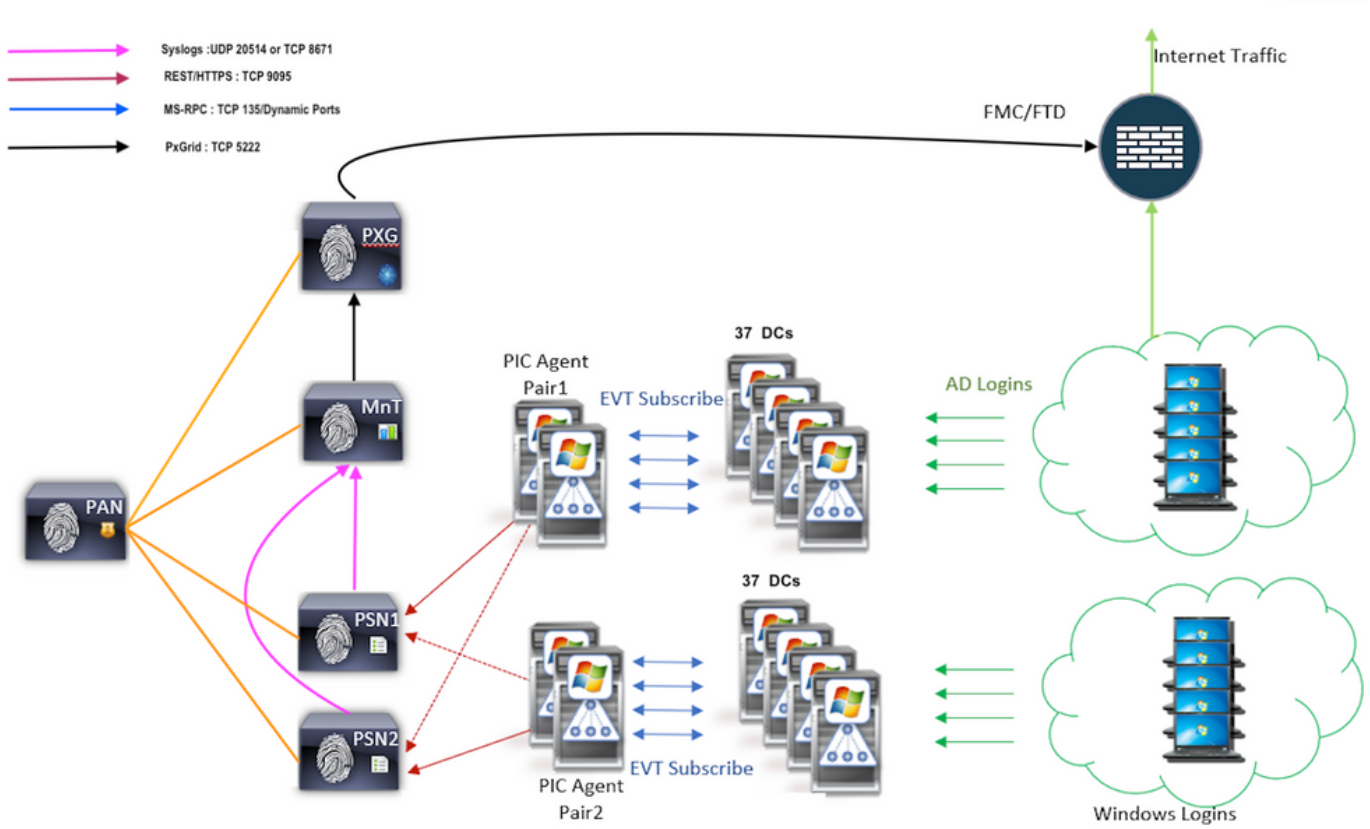


Escalabilidade

O novo agente oferece melhor suporte com números de escala maiores para um número suportado de controladores de domínio e o número de eventos que ele pode lidar. Aqui estão os números de escala que foram testados:

- Número máximo de controladores de domínio monitorados (com 2 pares de agentes): 74
- Número máximo de mapeamentos/eventos testados: 292.000 (3.950 eventos por DC)
- TPS máximo testado: 500

Arquitetura de configuração do Scale Test



Consulta de eventos históricos

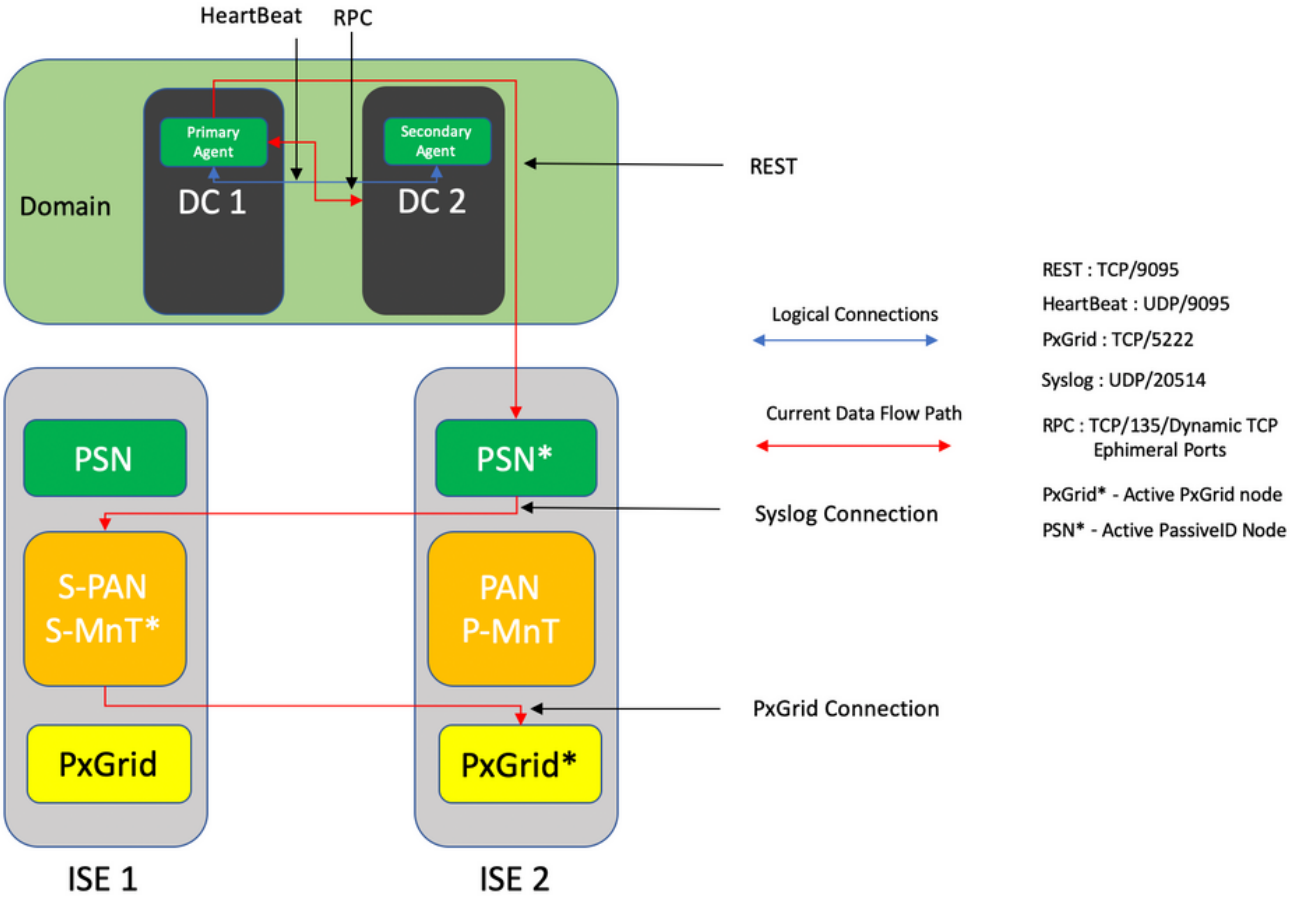
Em caso de failover ou em caso de reinicialização do serviço, o agente PIC é feito para garantir que nenhum dado seja perdido, os eventos gerados para o período de tempo anterior são consultados e enviados novamente aos nós PSN. Por padrão, o valor de 60 segundos de eventos passados desde o início do serviço é consultado pelo ISE para negar qualquer perda de dados durante a perda do serviço.

Menos sobrecarga de processamento

Ao contrário da WMI que é intensa da CPU em grande escala ou carga pesada, a EVT não consome muitos recursos como a WMI. Os testes de escala mostraram um desempenho muito melhor das consultas com o uso de EVT.

Configurar

Diagrama de conectividade

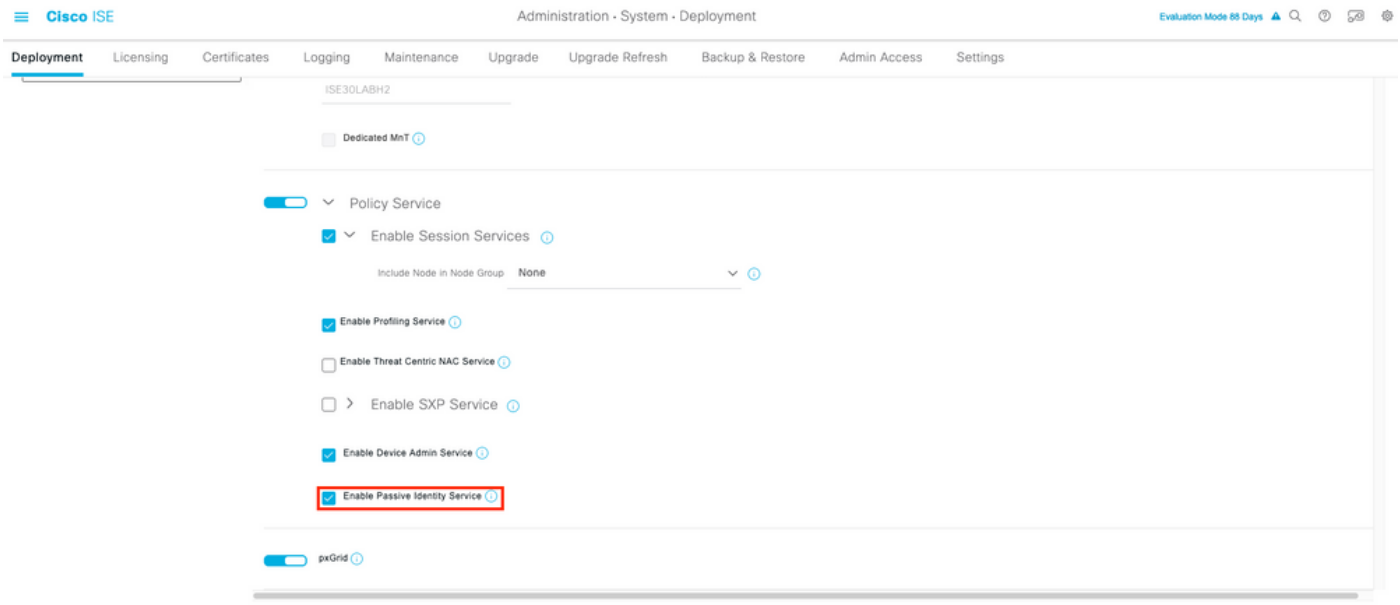


Configurações

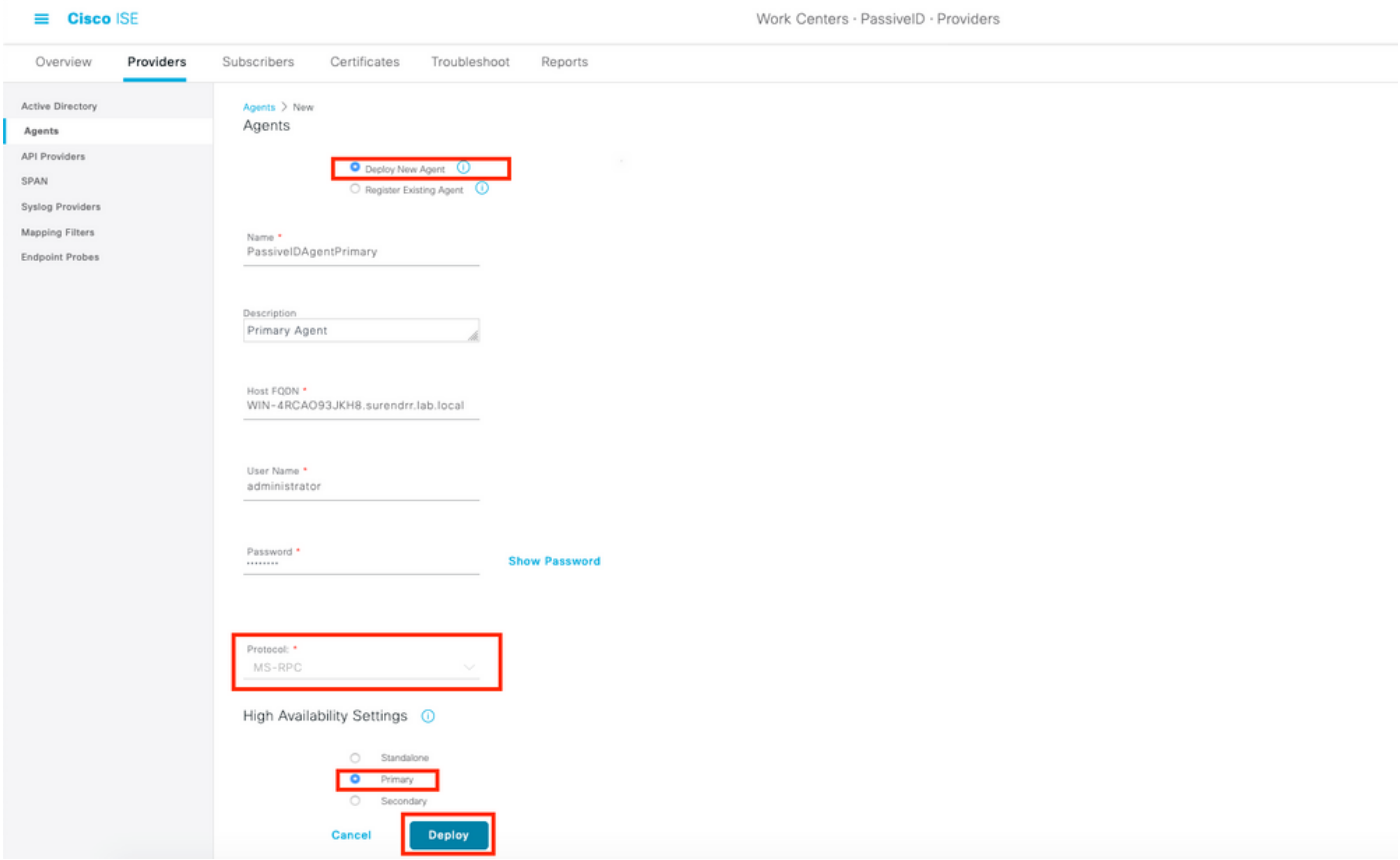
Configurar o ISE para o PassiveID Agent

Para configurar os serviços PassiveID, é necessário ter os Passive Identity Services ativados em pelo menos um Policy Service Node (PSN). Um máximo de dois nós pode ser usado para Passive Identity Services que funciona no modo de operação Ativo/Standby. O ISE também deve ser associado a um domínio do Ative Diretory e somente os controladores de domínio presentes nesse domínio podem ser monitorados por Agentes configurados no ISE. Para ingressar no ISE em um domínio do Ative Diretory, consulte o Guia de Integração do Ative Diretory.

Navegue até **Administration > System > Deployment > [Choose a PSN] > Edit** para habilitar o Passive Identity Services conforme mostrado aqui:



Navegue até **Centros de trabalho > IDsPassivos > Provedores > Agentes > Adicionar** para implantar um novo agente como mostrado aqui:

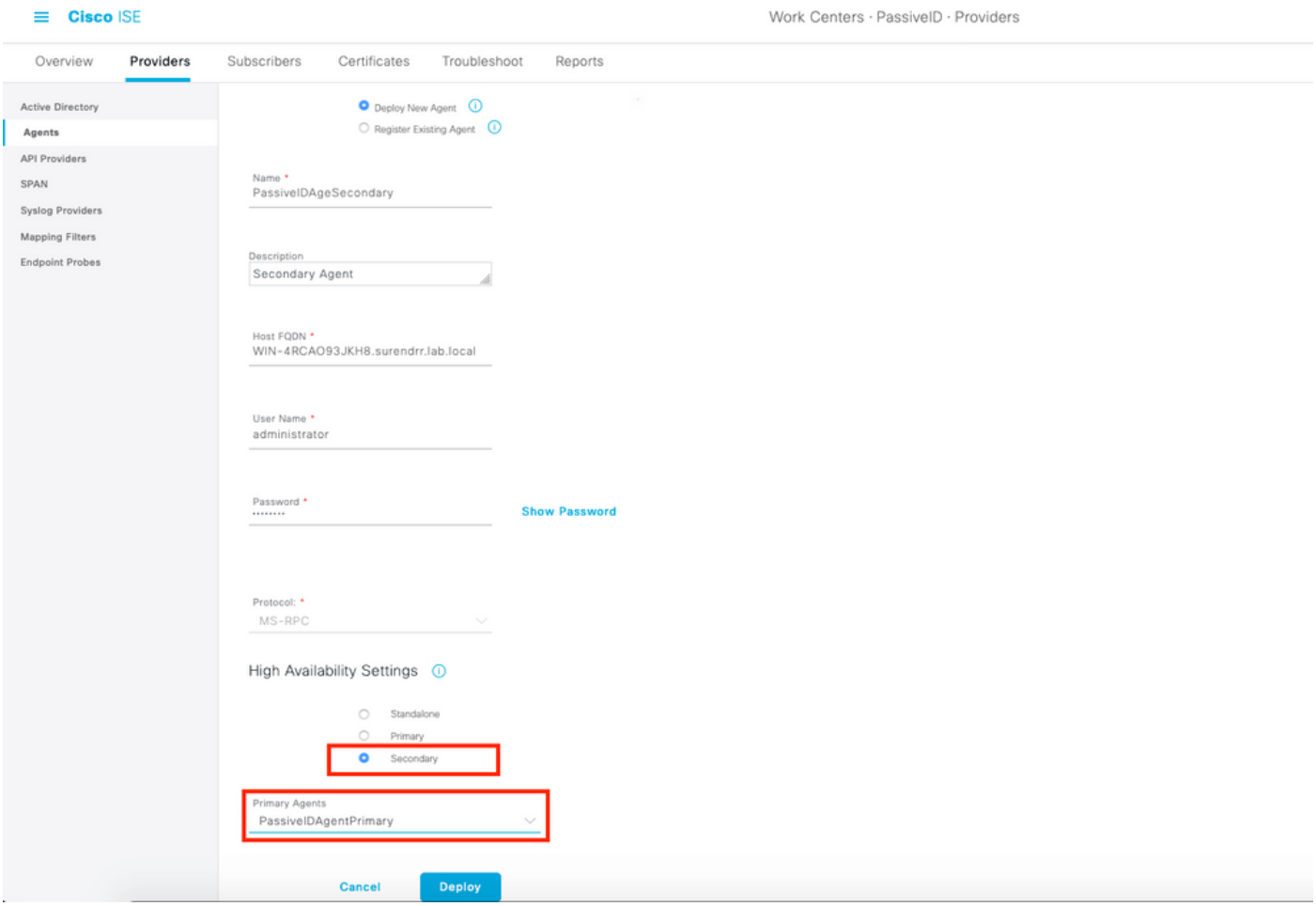


Note: 1. Se o agente estiver planejado para ser instalado pelo ISE no controlador de domínio, a conta usada aqui deve ter privilégios suficientes para instalar um programa e executá-lo no servidor mencionado no campo FQDN do host. O FQDN do host aqui pode ser o de um servidor membro em vez de um controlador de domínio.

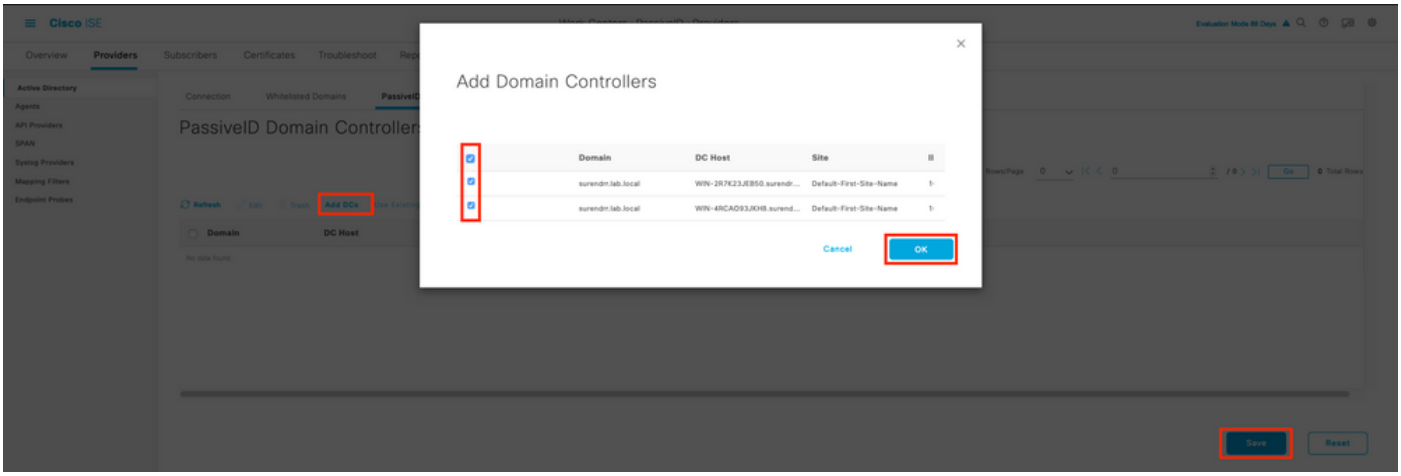
2. Se um agente já estiver instalado manualmente ou em uma implantação anterior do ISE, com MSRPC, as permissões e configurações necessárias no Ative Diretory ou no Windows serão menores em comparação com o WMI, o outro protocolo (e o único disponível antes do 3.0) usado pelos agentes PIC. A conta de usuário usada nesse caso

pode ser uma conta de domínio regular que faz parte do **grupo de Leitores de log de eventos.** Escolha **Registrar Agente Existente** e use esses detalhes de conta para registrar o agente que é manualmente instalado nos controladores de domínio.

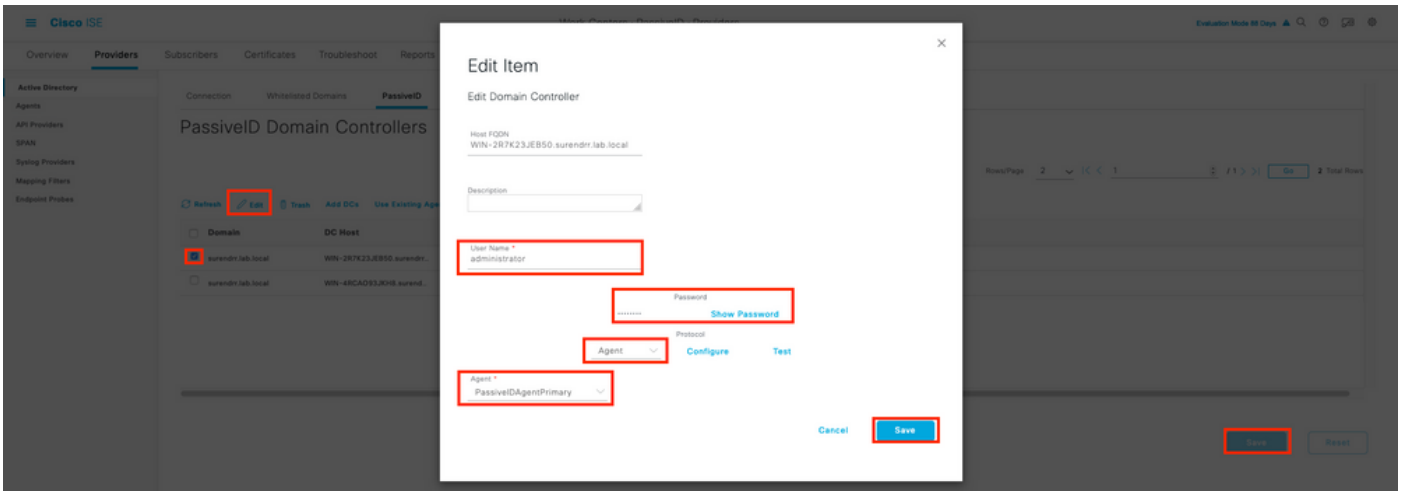
Após uma implantação bem-sucedida, configure outro agente em um servidor diferente e adicione-o como um agente secundário e, em seguida, seu peer principal, como mostrado nesta imagem.



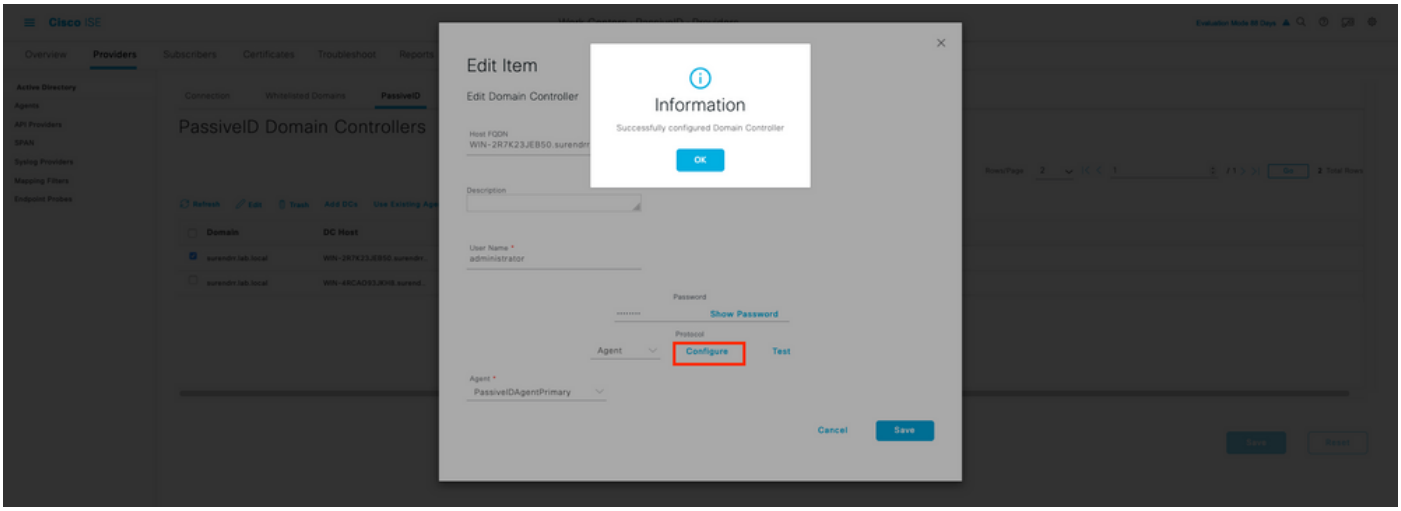
Para monitorar os controladores de domínio usando os agentes, navegue para **Centros de trabalho > IDsPassivos > Provedores > Ative Diretory > [Clique no ponto de união] > IDsPassivos**. Clique em **Adicionar DCs** e escolha os controladores de domínio dos quais os eventos/mapeamento de IP do usuário são recuperados, clique em **OK** e, em seguida, clique em **Salvar** para salvar as alterações, como mostrado nesta imagem.

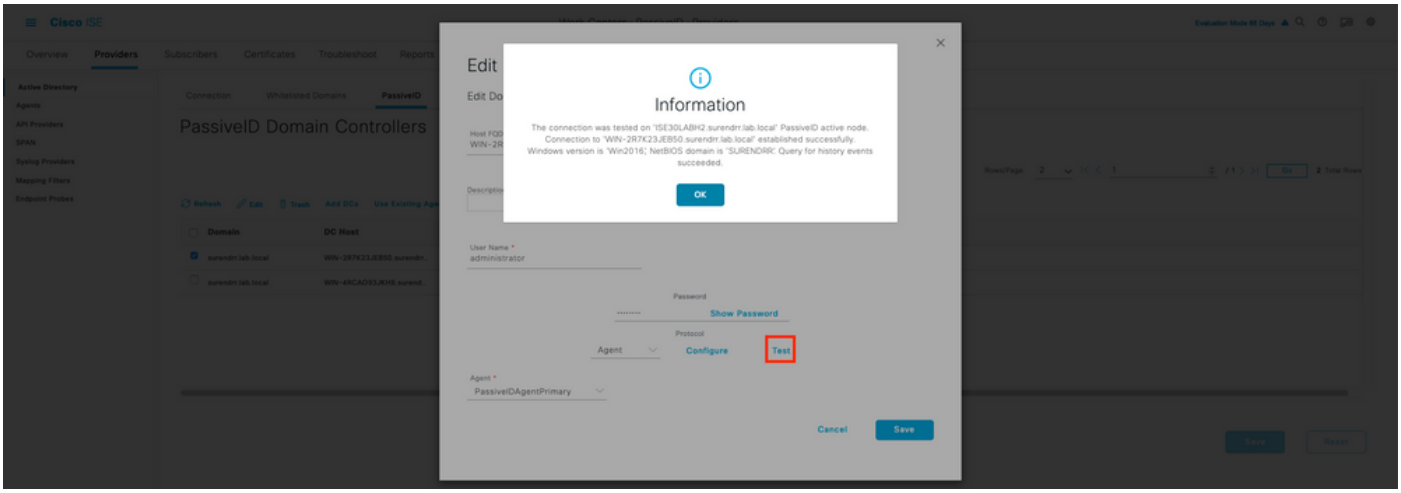


Para especificar os Agentes que devem ser usados para recuperar os eventos de, Navegue até **Centros de Trabalho > IDs** Passivos **> Provedores > Ative Diretory > [Clique no Ponto de união] > IDsPassivos.** Escolha os controladores de domínio e clique em **Editar**. Digite o *Nome de usuário* e a *Senha.* Escolha **Agente** e, em seguida, **Salvar** a caixa de diálogo. Clique em **Save** na guia PassiveID para concluir a configuração.



Você pode verificar se a configuração está corretamente aplicada com a ajuda dos botões **Configurar** e **Testar**, como mostrado nas imagens aqui:





Entender o arquivo de configuração do agente PassiveID

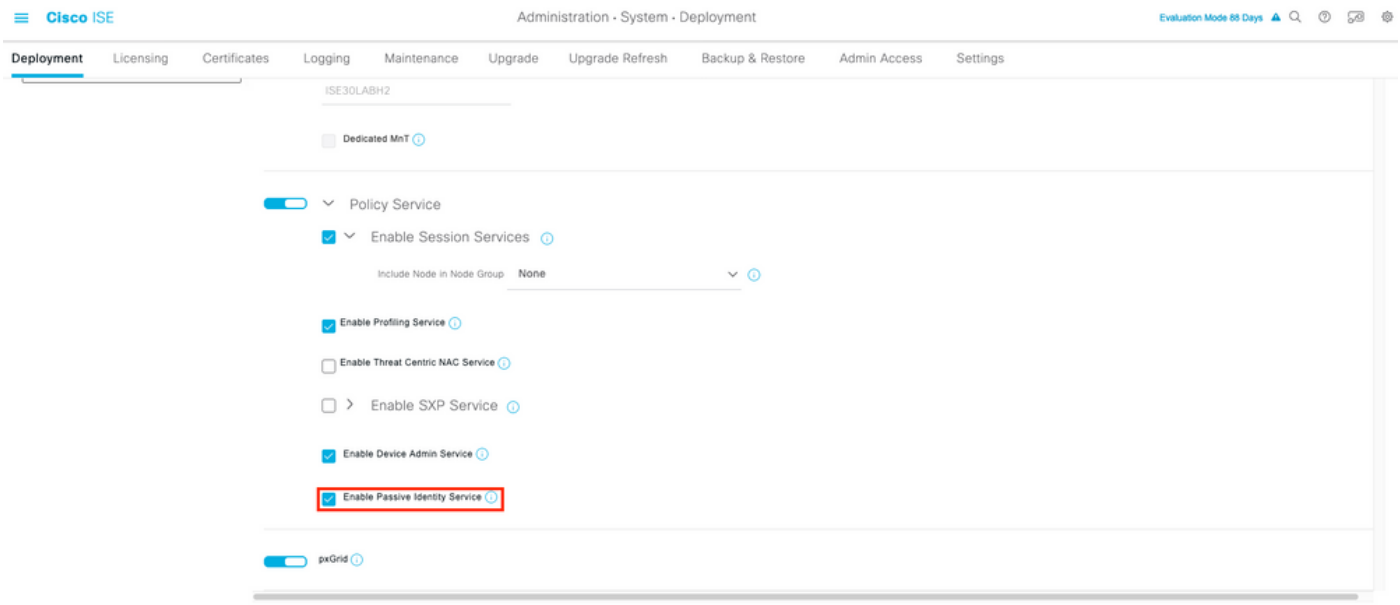
O arquivo de configuração do PassiveID Agent está localizado em **C:\Program Files**

(x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config . O arquivo de configuração tem conteúdo mostrado aqui:

Verificar

Verifique os serviços PassiveID no ISE

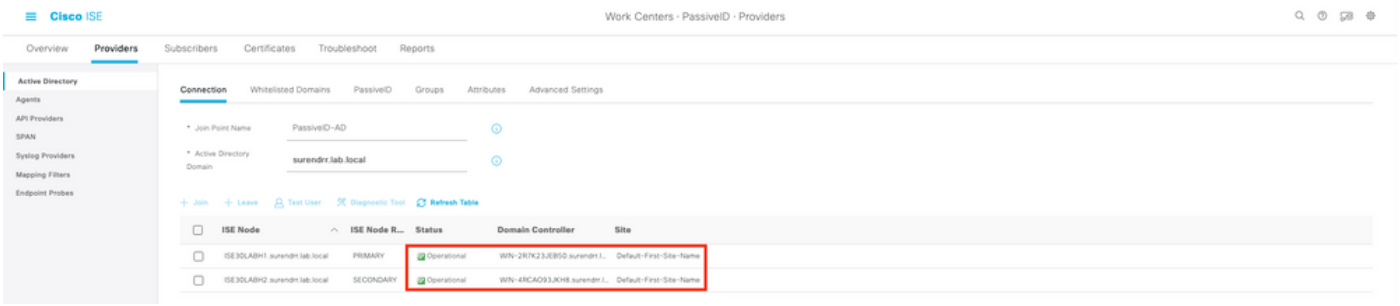
1. Verifique se o serviço PassiveID está ativado na GUI e também está marcado como sendo executado do comando **show application status ise** na CLI do ISE.



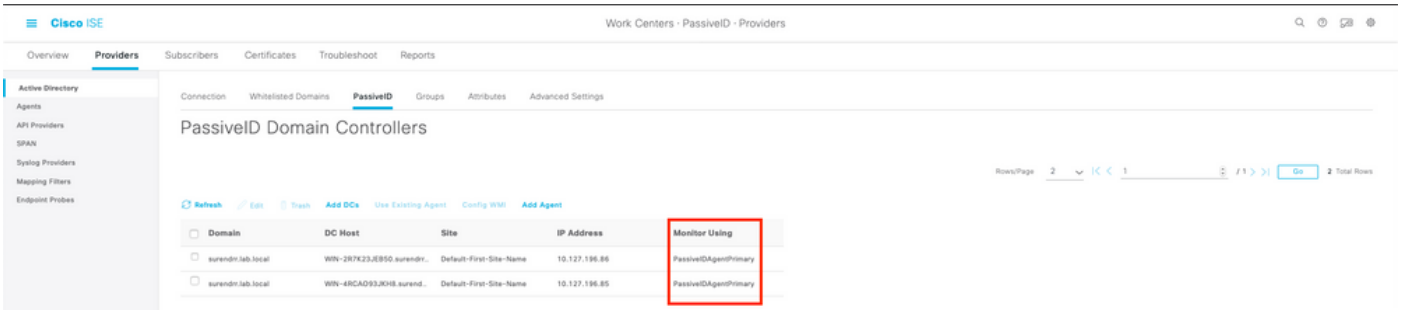

```
ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 129052
Database Server running 108 PROCESSES
Application Server running 9830
Profiler Database running 5127
ISE Indexing Engine running 13361
AD Connector running 20609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

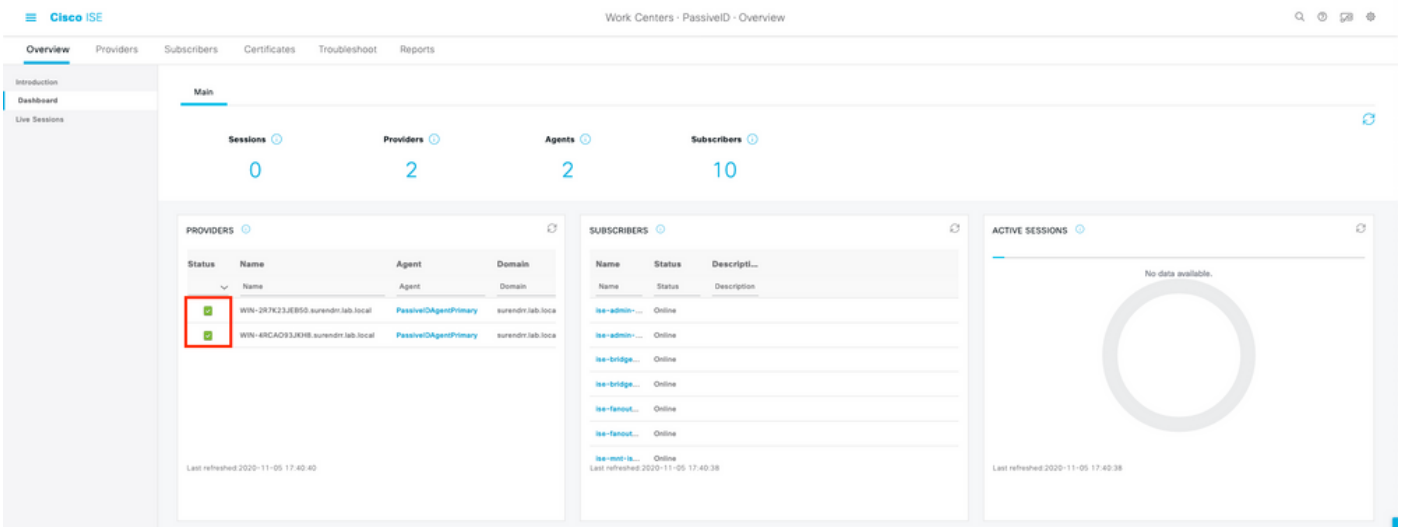
2. Verifique se o provedor do ISE Ative Diretory está conectado aos controladores de domínio em **Centros de Trabalho > IDs** Passivos **> Provedores > Ative Diretory > Conexão**.



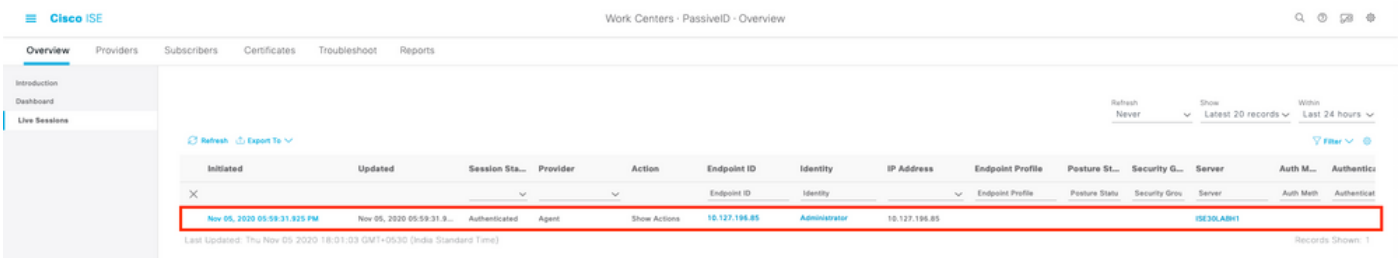
3. Verifique se os controladores de domínio necessários estão sendo monitorados pelo **Agent em Centros de Trabalho > PassiveID > Providers > Ative Diretory > PassiveID**.



4. Verifique se o status dos controladores de domínio sendo monitorados está ativo, ou seja, marcado em verde no painel em **Centros de trabalho > ID** passivo **> Visão geral > Painel**.



5. Verifique se as sessões ao vivo estão sendo preenchidas quando um login do Windows está registrado no controlador de domínio em **Centros de Trabalho > PassiveID > Visão geral > Sessões ao vivo**.



Verificar serviços do agente no Windows Server

1. Verifique o serviço ISEPICAgent no servidor onde o agente PIC está instalado.