EVTベースのIdentity Services Engineパッシブ IDエージェントの設定

内容

概要

このドキュメントでは、ISE 3.0バージョンで導入された新しいISEパッシブIDコネクタ(ISE-PIC)エージェント、その利点、およびISEでのエージェントの設定について説明します。ISEパッシブIDエージェントは、Cisco FirePower Management Centerを使用するアイデンティティファイアウォールソリューションの不可欠な要素となっています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Administration
- MS-RPC、WMIプロトコル
- Active Directory管理

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engineバージョン3.0以降
- Microsoft Windows Server 2016 Standard

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

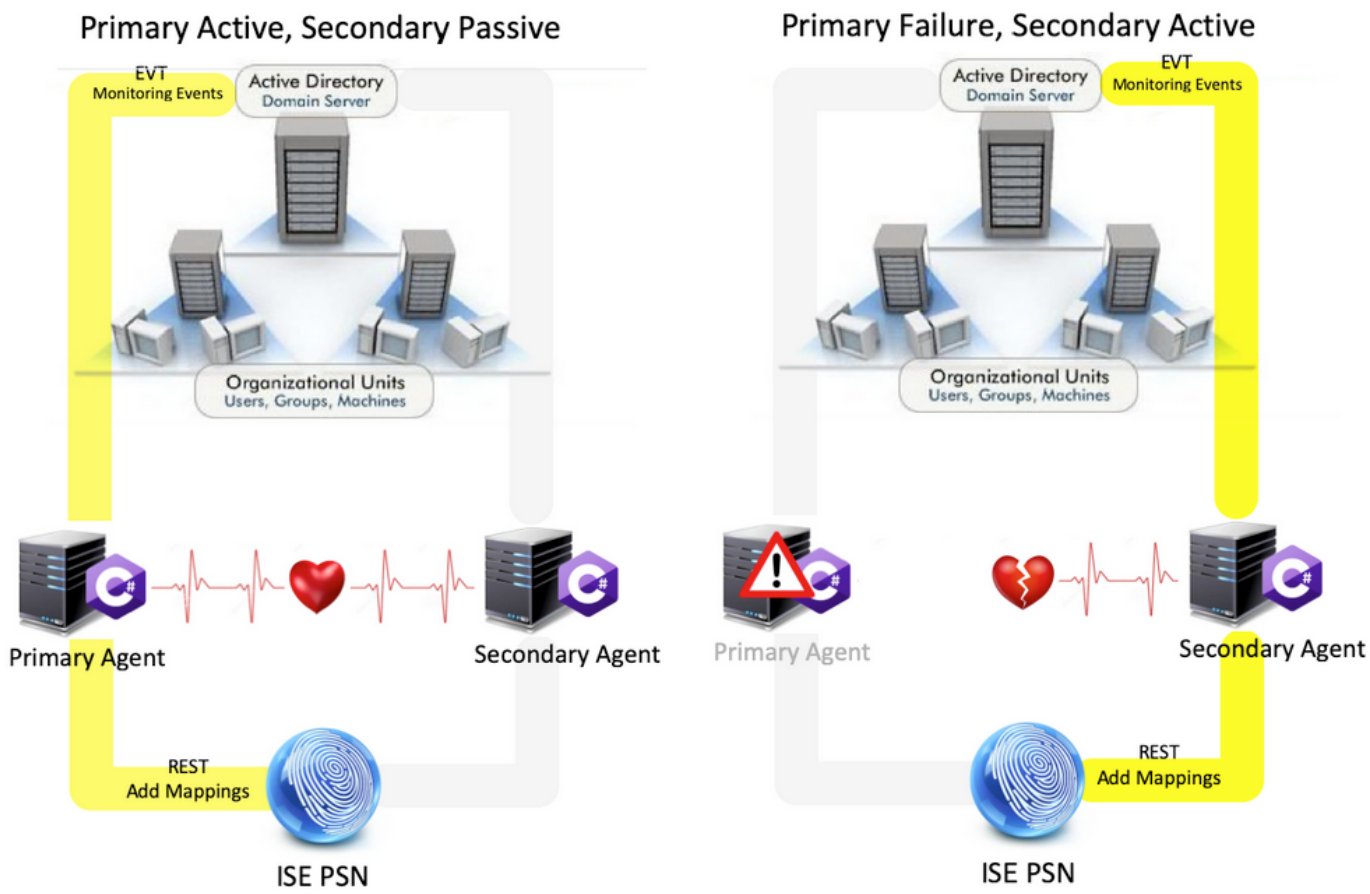
新しいプロトコルの必要性

ISEのパッシブID（パッシブID）機能は、IDベースのファイアウォール、EasyConnectなど、多くの重要な使用例を促進します。この機能は、Active Directoryドメインコントローラにログインし、ユーザ名とIPアドレスを学習するユーザを監視する機能によって異なります。ドメインコントローラの監視に使用する現在のメインプロトコルはWMIです。ただし、設定は困難/侵襲的であり、クライアントとサーバの両方でパフォーマンスに影響を与えます。また、規模の大きい展開でログオンイベントを確認する際に非常に大きな遅延が発生する場合もあります。Passive Identity Servicesに必要な情報をポーリングするための徹底的な調査と代替方法の後、EVTまたはEventing APIと呼ばれる代替プロトコルが決定されました。これは、この使用例の処理により効率的です。これは、**MS-EVEN6**とも呼ばれ、Eventing Remote Protocol(EVP)とも呼ばれます。これは、RPCベースのThe Wireプロトコルの基盤です。

MS-EVEN6の使用による利点

ハイ アベイラビリティ

元のエージェントには高可用性オプションがなく、エージェントが実行されているサーバまたは停止しているサーバでメンテナンスを行う必要がある場合は、ログオンイベントが失われ、IDベースのファイアウォールなどの機能では、この間データが失われます。これは、このリリースより前のISE PIC Agentの使用に関する主な懸念事項の1つです。ISEはUDPポート9095を使用して、エージェント間でハートビートを交換します。

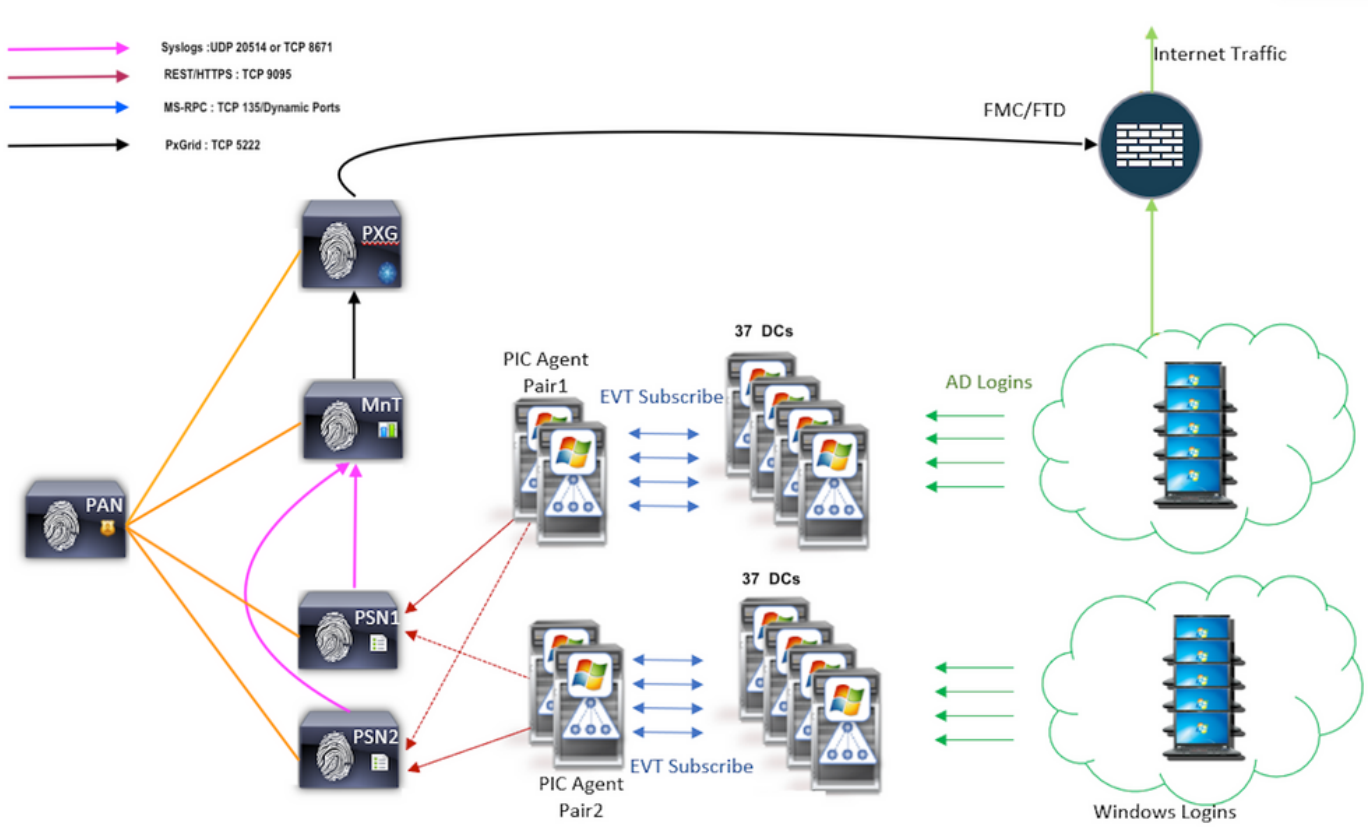


拡張性

新しいエージェントは、サポートされる数のドメインコントローラと処理できるイベントの数に対して、より多くのスケール数をサポートします。テストされたスケール番号を次に示します（図1を参照）。

- モニタされるドメインコントローラの最大数（エージェントの2ペアあり）:74
- テストされたマッピング/イベントの最大数：292,000（DCあたり3950イベント）
- テストされる最大TPS:500

スケールテストセットアップアーキテクチャ



履歴イベントクエリ

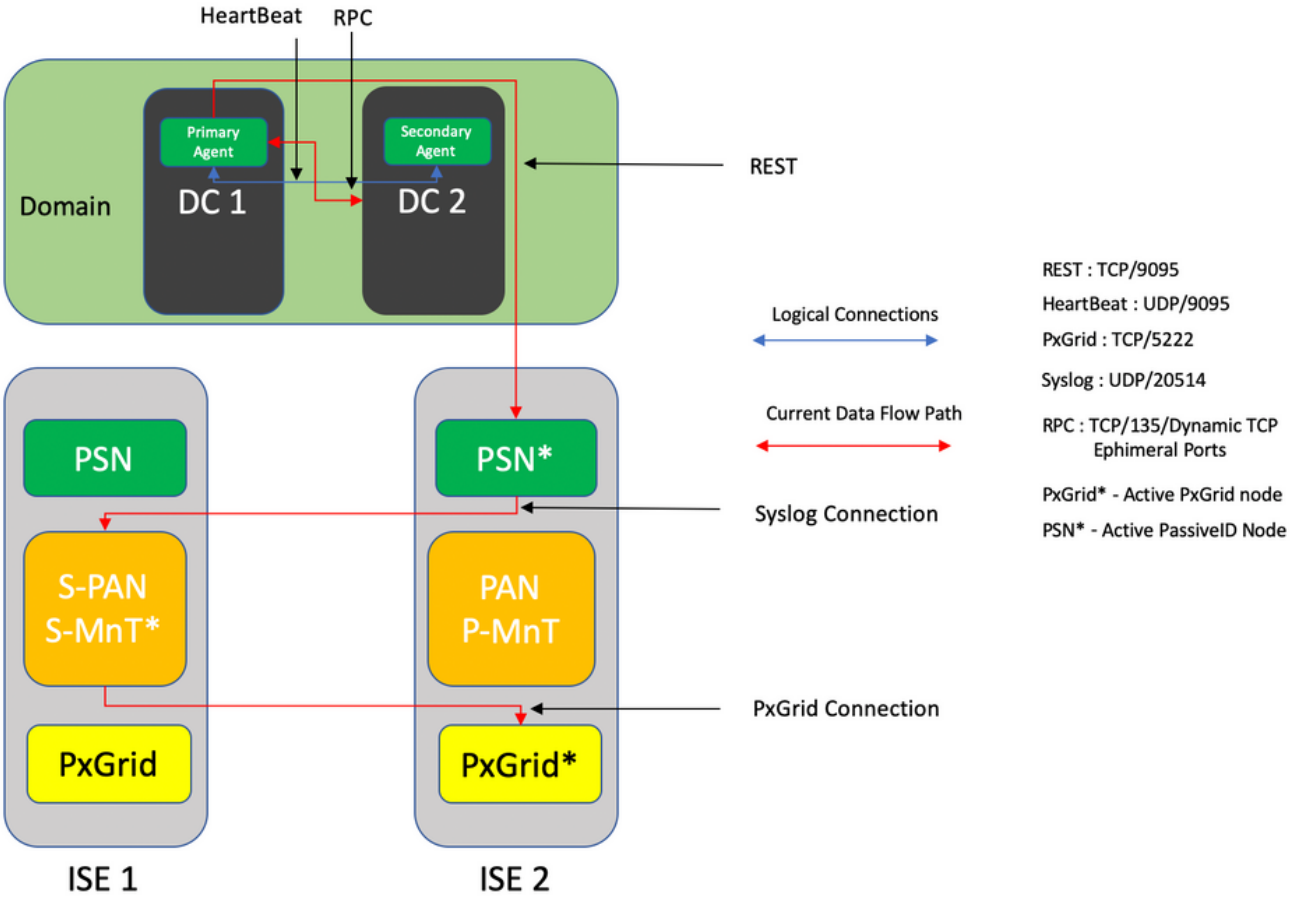
フェールオーバーの場合、またはPIC-Agentに対してサービスの再起動が実行された場合、データが失われないように、過去の一定時間に生成されたイベントが照会され、PSNノードに再送信されます。デフォルトでは、サービスの開始時から60秒に相当する過去のイベントがISEによって照会され、サービスの損失中にデータの損失が相殺されます。

処理オーバーヘッドの削減

大規模または高負荷でCPU負荷が高いWMIとは異なり、EVTはWMIほど多くのリソースを消費しません。スケールテストでは、EVTを使用したクエリのパフォーマンスが大幅に向上しました。

設定

接続図

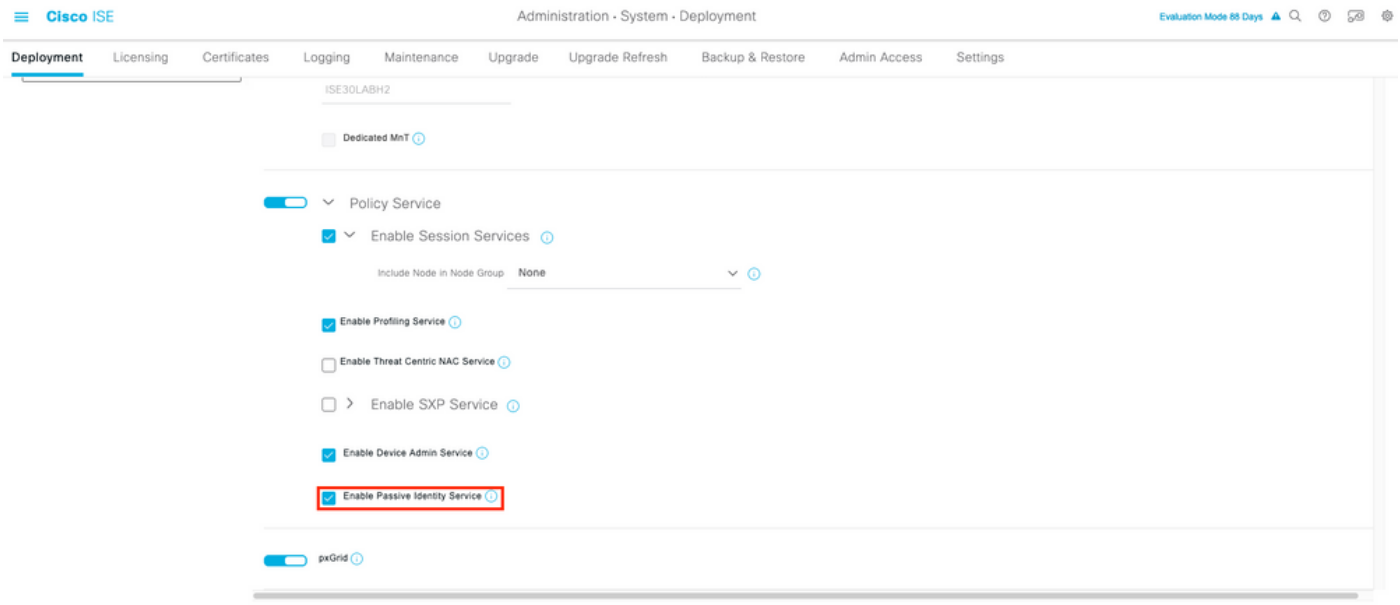


設定

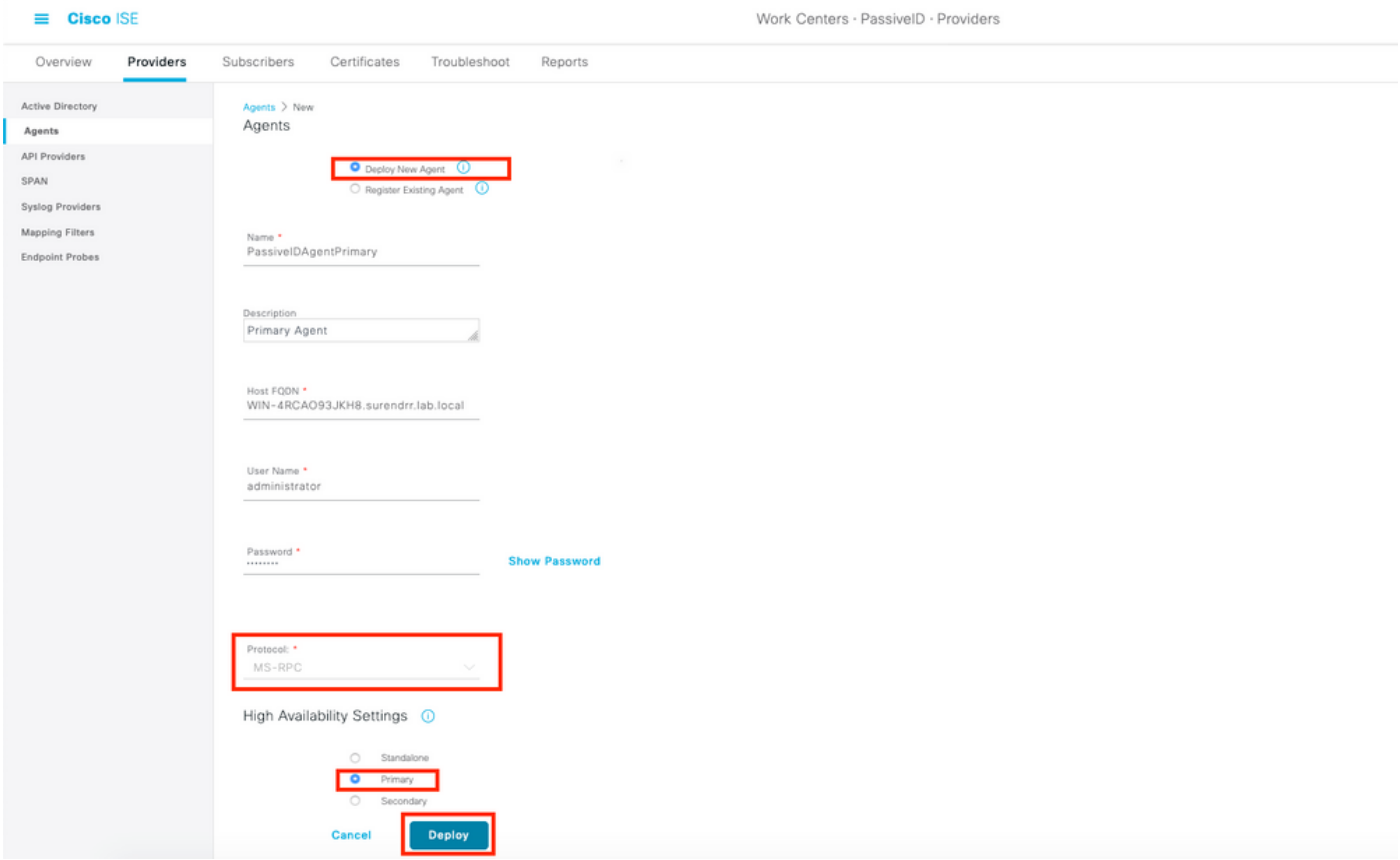
PassiveID AgentのISEの設定

PassiveIDサービスを設定するには、1つ以上のポリシーサービスノード(PSN)でPassive Identity Servicesが有効になっている必要があります。アクティブ/スタンバイモードで動作するパッシブIDサービスには、最大2つのノードを使用できます。ISEはActive Directoryドメインに参加する必要があり、そのドメインに存在するドメインコントローラだけがISEで設定されたエージェントによってモニタできます。ISEをActive Directoryドメインに参加させるには、『Active Directory Integration Guide』を参照してください。

[Administration] > [System] > [Deployment] > [Choose a PSN] > [Edit]に移動し、次のように Passive Identity Servicesを有効にします（図2を参照）。



[Work Centers] > [PassiveID] > [Providers] > [Agents] > [Add]に移動して、次のように新しいエージェントを展開します（図を参照）。

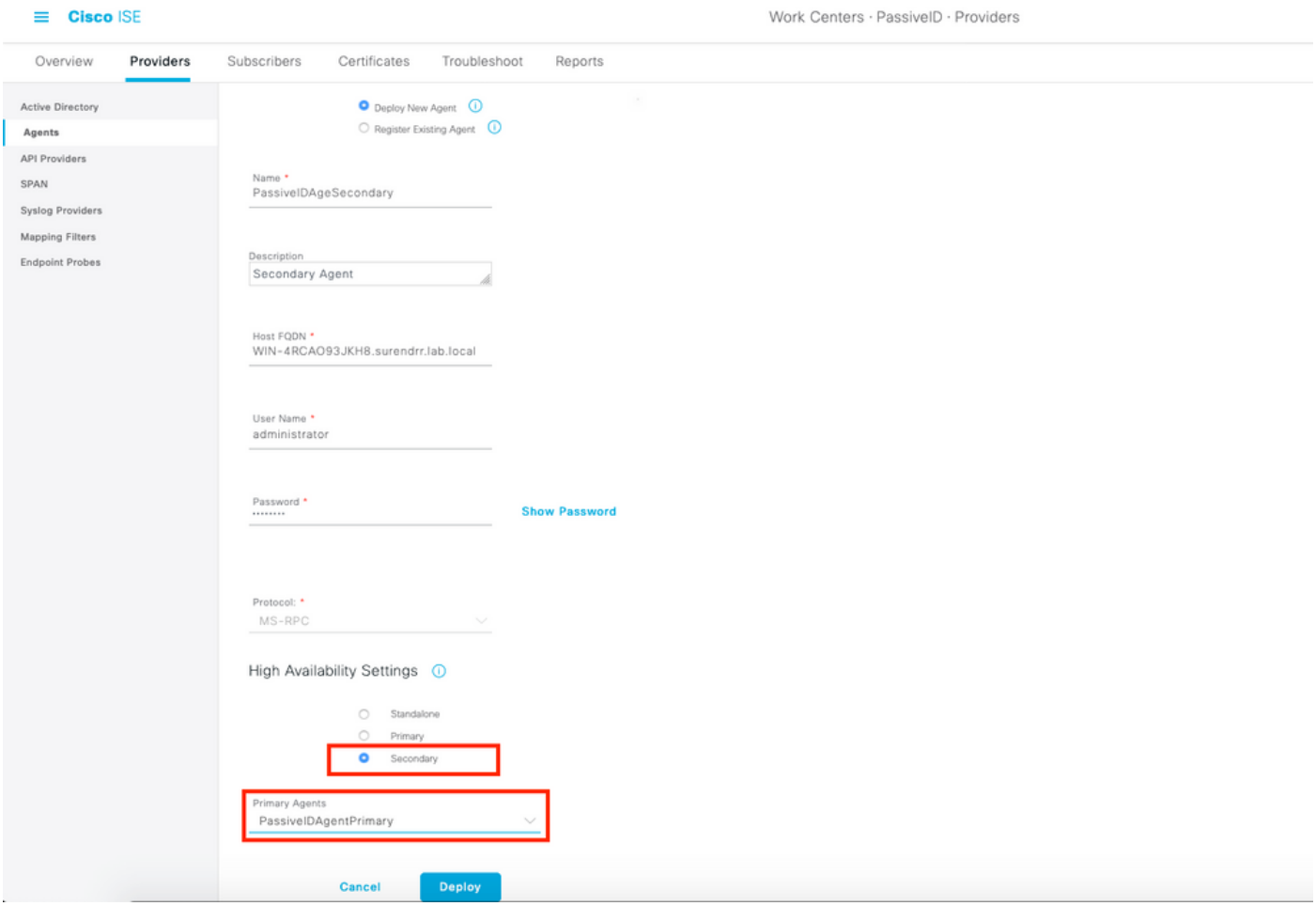


注：1.エージェントがドメインコントローラにISEによってインストールされる予定の場合、ここで使用するアカウントには、プログラムをインストールし、[ホストのFQDN（ホストのFQDN）]フィールドに示されているサーバで実行するのに十分な権限が必要です。ここでホストFQDNは、ドメインコントローラではなくメンバサーバのホストFQDNにすることができます。

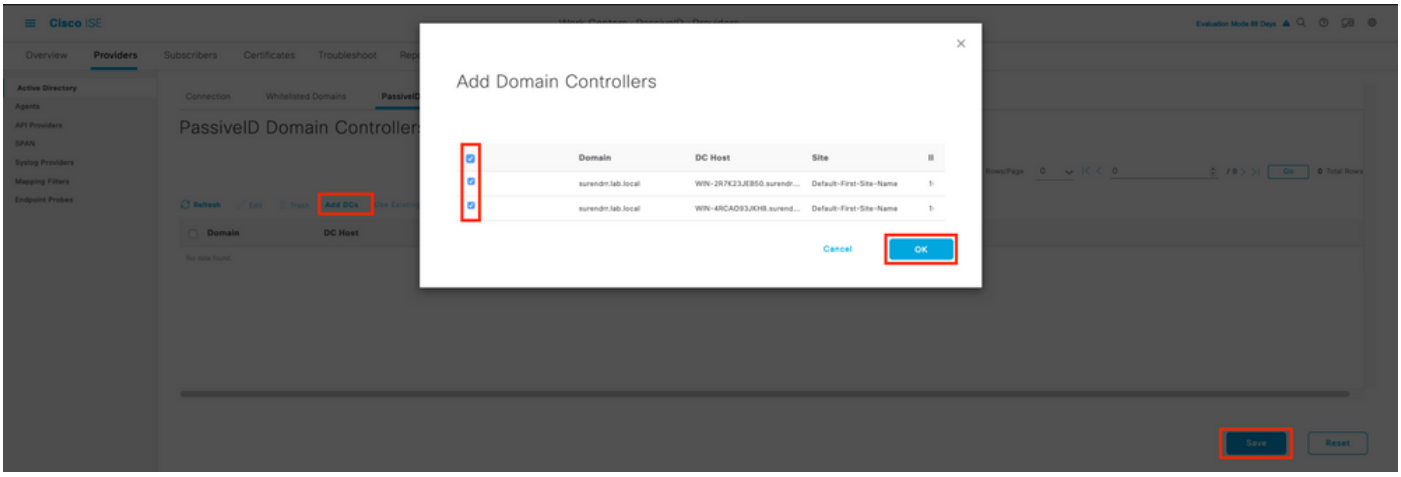
2.エージェントがMSRPCを使用してISEから以前に手動またはインストールされている場合、Active DirectoryまたはWindows側で必要な権限と設定は、PICエージェントが使用する他のプロトコル（および3.0より前に使用可能な唯一のプロトコル）とのWMIよりも少

少少少少少数)。この場合に使用するユーザーアカウントは、イベントログリーダーグループの一部である通常のドメインアカウント**である可能性があります。**[既存の**エージェントの登録]を選択**し、これらのアカウントの詳細を使用して、ドメインコントローラに手動でインストールされたエージェントを登録します。

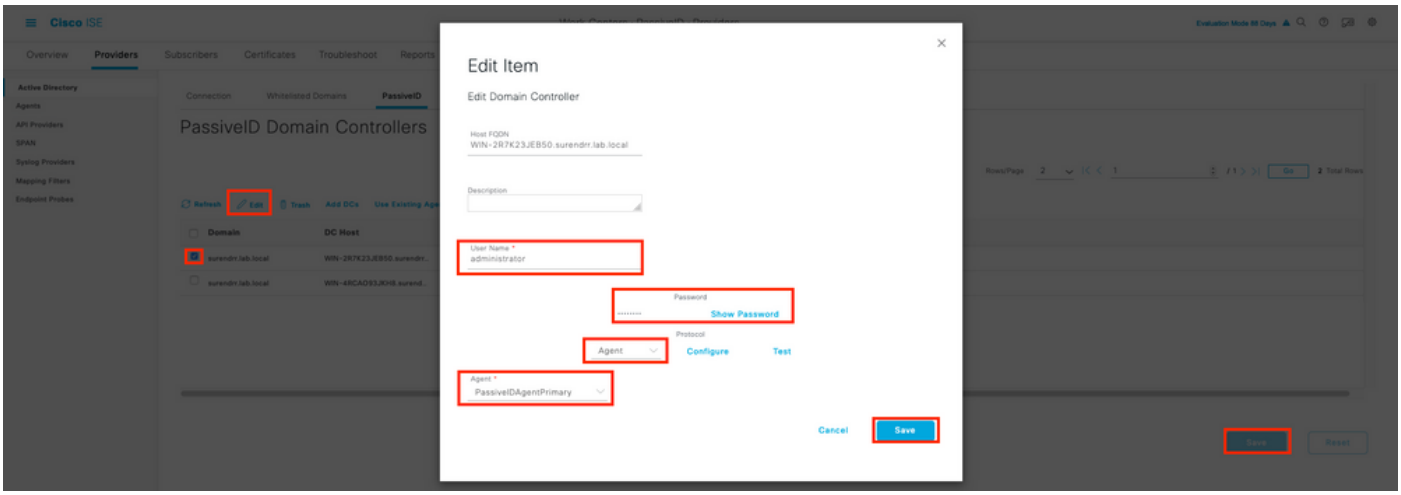
導入が正常に完了したら、別のサーバに別のエージェントを設定し、セカンダリエージェントとして追加してから、次の図に示すようにプライマリピアを追加します。



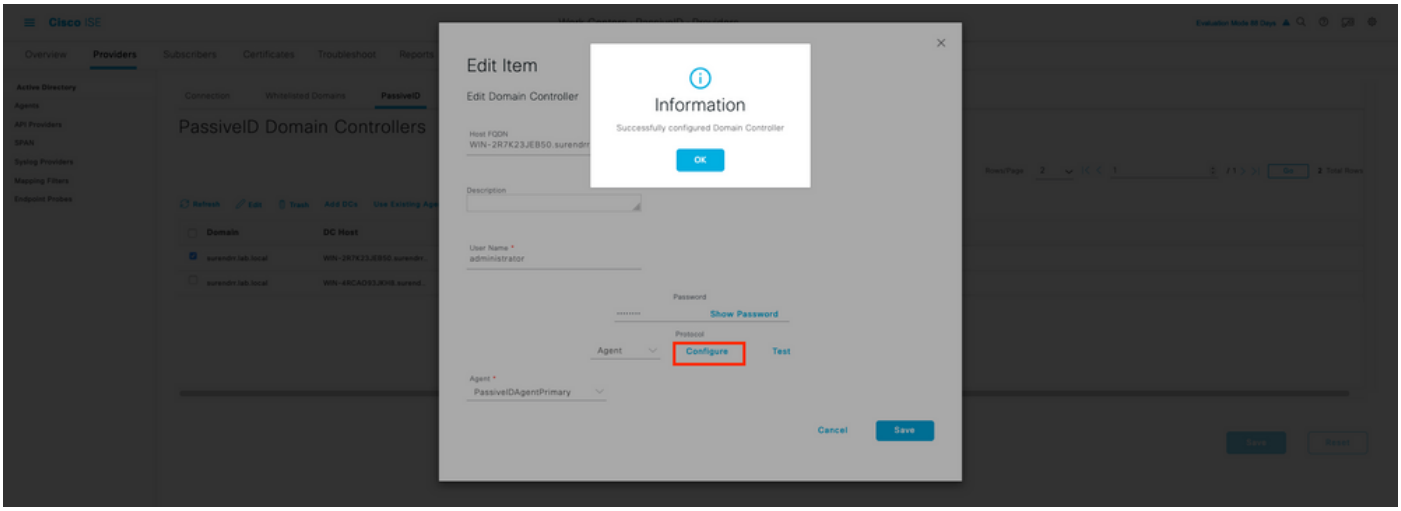
エージェントを使用してドメインコントローラを監視するには、**[Work Centers] > [PassiveID] > [Providers] > [Active Directory] > [Click on the Join Point] > [PassiveID]に移動します。**次の図に示すように、[Add DCs]をクリックし、ユーザIPマッピング/イベントの取得元のドメインコントローラを選択し、[OK]をクリックし、[Save]をクリックして変更を保存します。

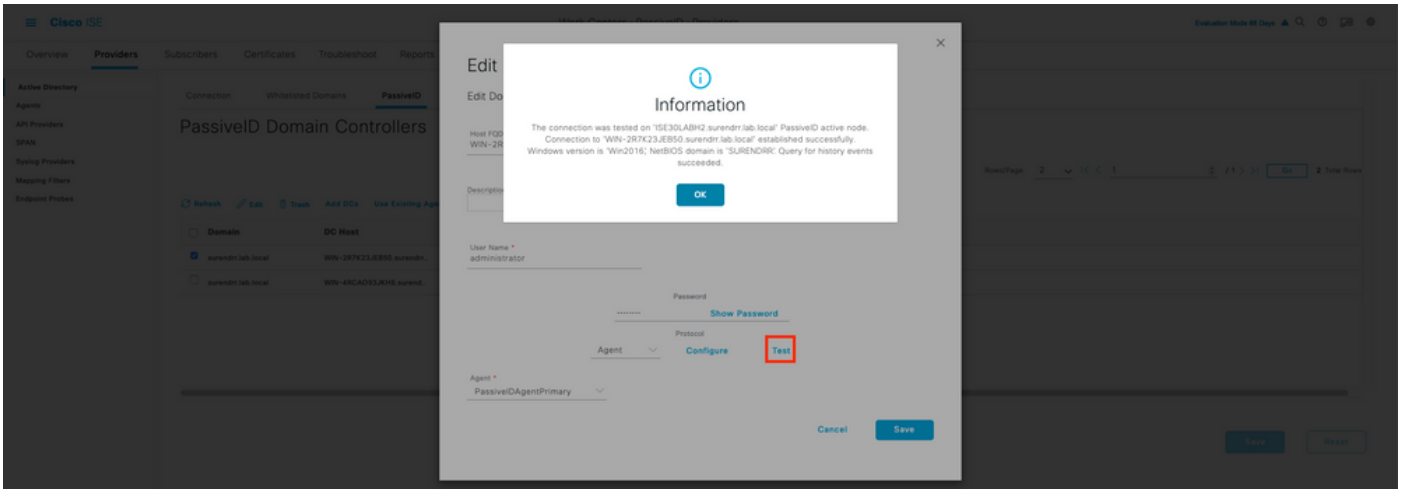


イベントの取得に使用するエージェントを指定するには、[Work Centers] > [PassiveID] > [Providers] > [Active Directory] > [Click on the Join Point] > [PassiveID]に移動します。ドメインコントローラを選択し、[Edit]をクリックします。ユーザ名とパスワードを入力します。[Agent]を選択し、[Save the dialog box]を選択します。[PassiveID]タブの[Save]をクリックして、設定を完了します。



次の図に示すように、[Configure]ボタンと[Test]ボタンを使用して、設定が正しく適用されているかどうかを確認できます。





PassiveIDエージェント設定ファイルについて

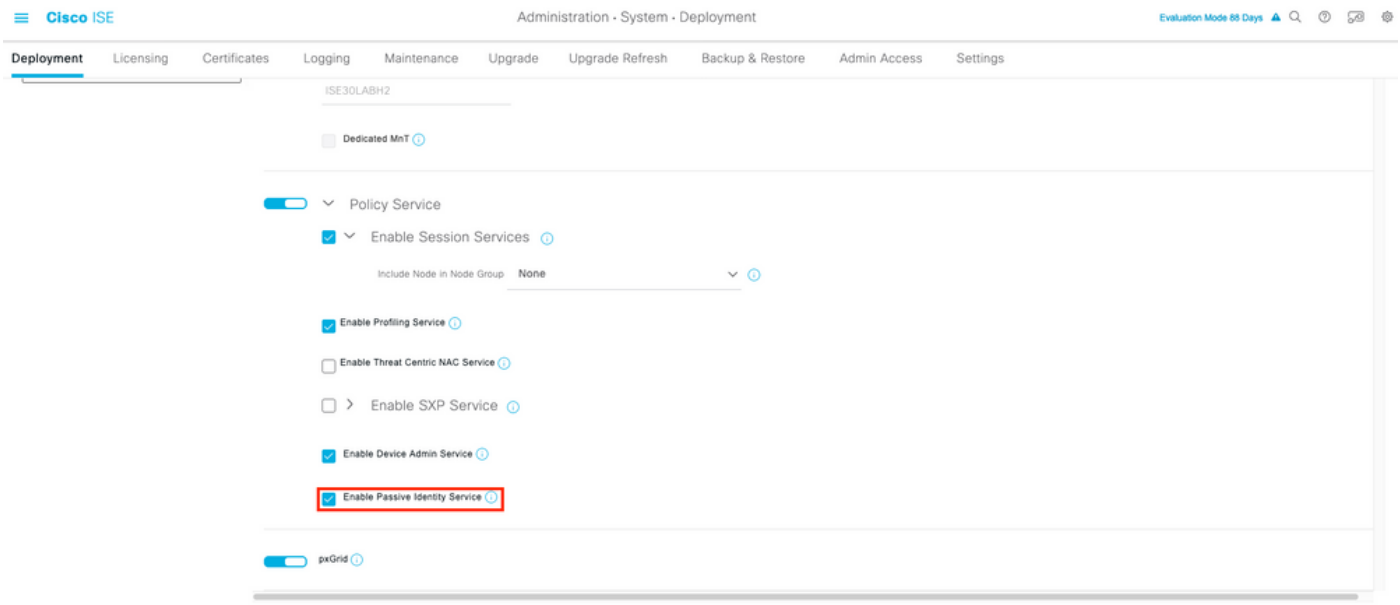
PassiveID Agent構成ファイルはC:\Program Files (x86)\Cisco\Cisco ISE PassiveID

Agent\PICAgent.exe.configにあります。設定ファイルには、次の内容が含まれています（図2を参照）。

確認

ISEでのPassiveIDサービスの確認

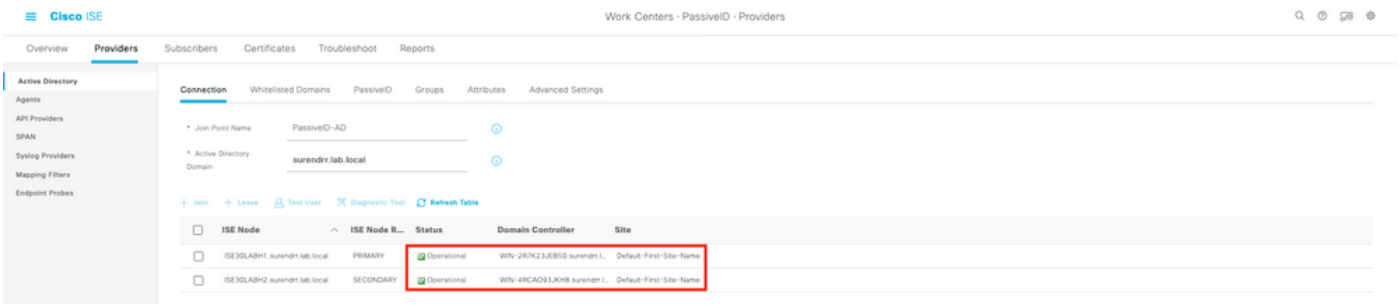
1. GUIでPassiveIDサービスが有効になっていること、およびISEのCLIでshow application status iseコマンドを使用して実行中とマークされていることを確認します。



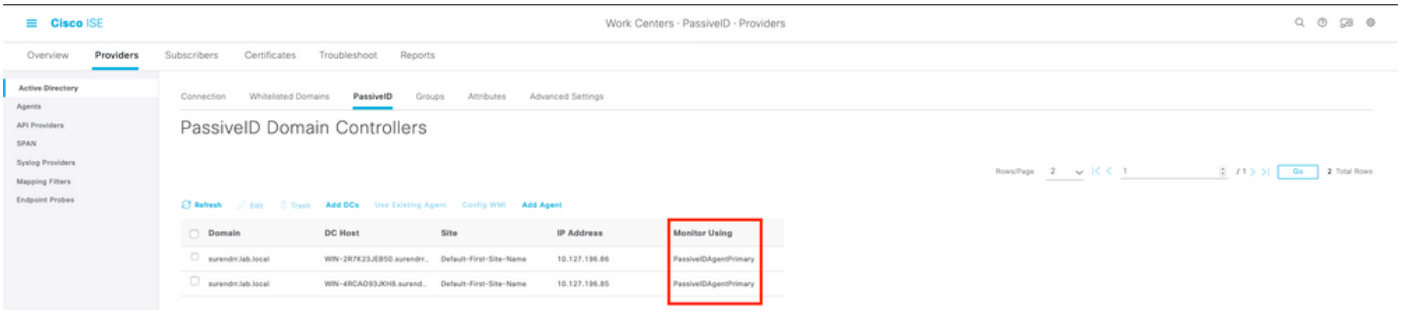

```
ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 129052
Database Server running 108 PROCESSES
Application Server running 9830
Profiler Database running 5127
ISE Indexing Engine running 13361
AD Connector running 20609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

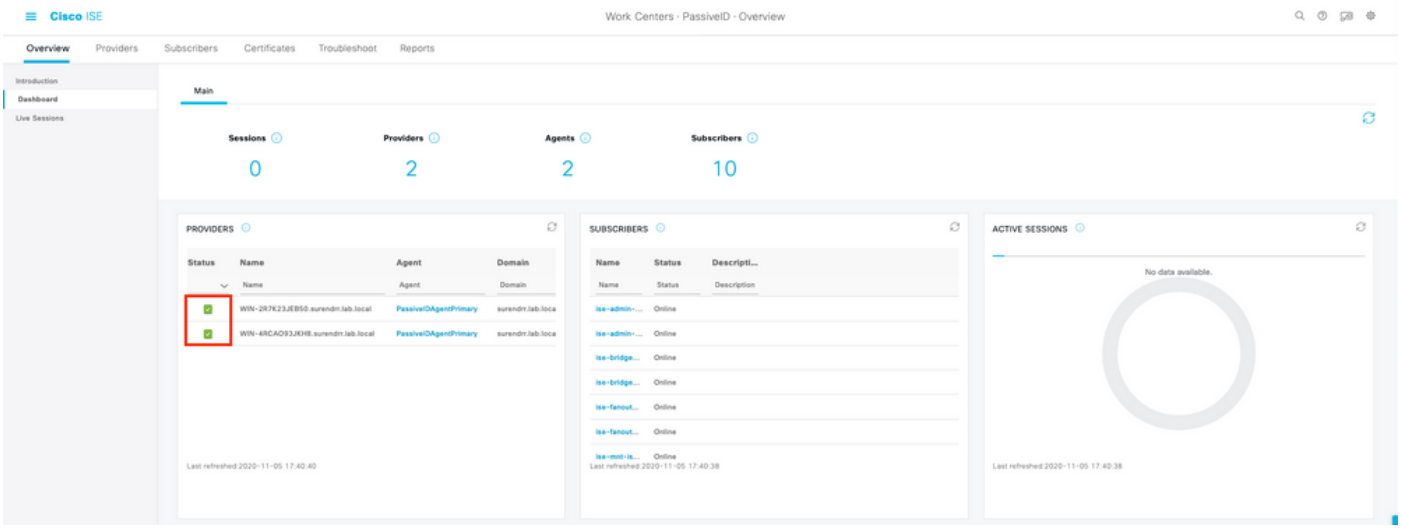
2. ISE Active Directoryプロバイダーが[Work Centers] > [PassiveID] > [Providers] > [Active Directory] > [Connection]でドメインコントローラに接続されているかどうかを確認します。



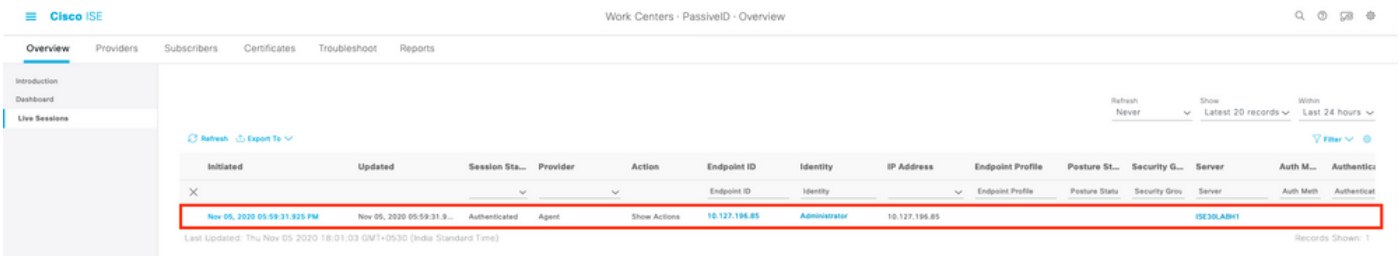
3.必要なドメインコントローラがAgentによって監視されているかどうかを確認します。[Work Centers] > [PassiveID] > [Providers] > [Active Directory] > [PassiveID]。



4.監視対象のドメインコントローラのステータスがアップ状態であるかどうかを確認します。つまり、[Work Centers] > [PassiveID] > [Overview] > [Dashboard]のダッシュボードで緑色にマークされます。



5. Windowsログオンがドメインコントローラに登録されている場合に入力されるライブセッションを確認します。[Work Centers] > [PassiveID] > [Overview] > [Live Sessions]を選択します。



Windows Serverでのエージェントサービスの確認

1. PICエージェントがインストールされているサーバでISEPICAgentサービスを確認します。