EVT 기반 ID 서비스 엔진 수동 ID 에이전트 구성

목차

소개

이 문서에서는 ISE 3.0 버전에서 도입된 새로운 ISE ISE PIC(Passive Identity Connector) 에이전트, 그 장점 및 ISE에서 이 에이전트의 구성에 대해 설명합니다.ISE Passive Identity Agent는 Cisco FirePower Management Center를 사용하는 ID 방화벽 솔루션의 핵심적인 부분이 되었습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Identity Services 관리
- MS-RPC, WMI 프로토콜
- Active Directory 관리

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine 버전 3.0 이상
- Microsoft Windows Server 2016 Standard

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

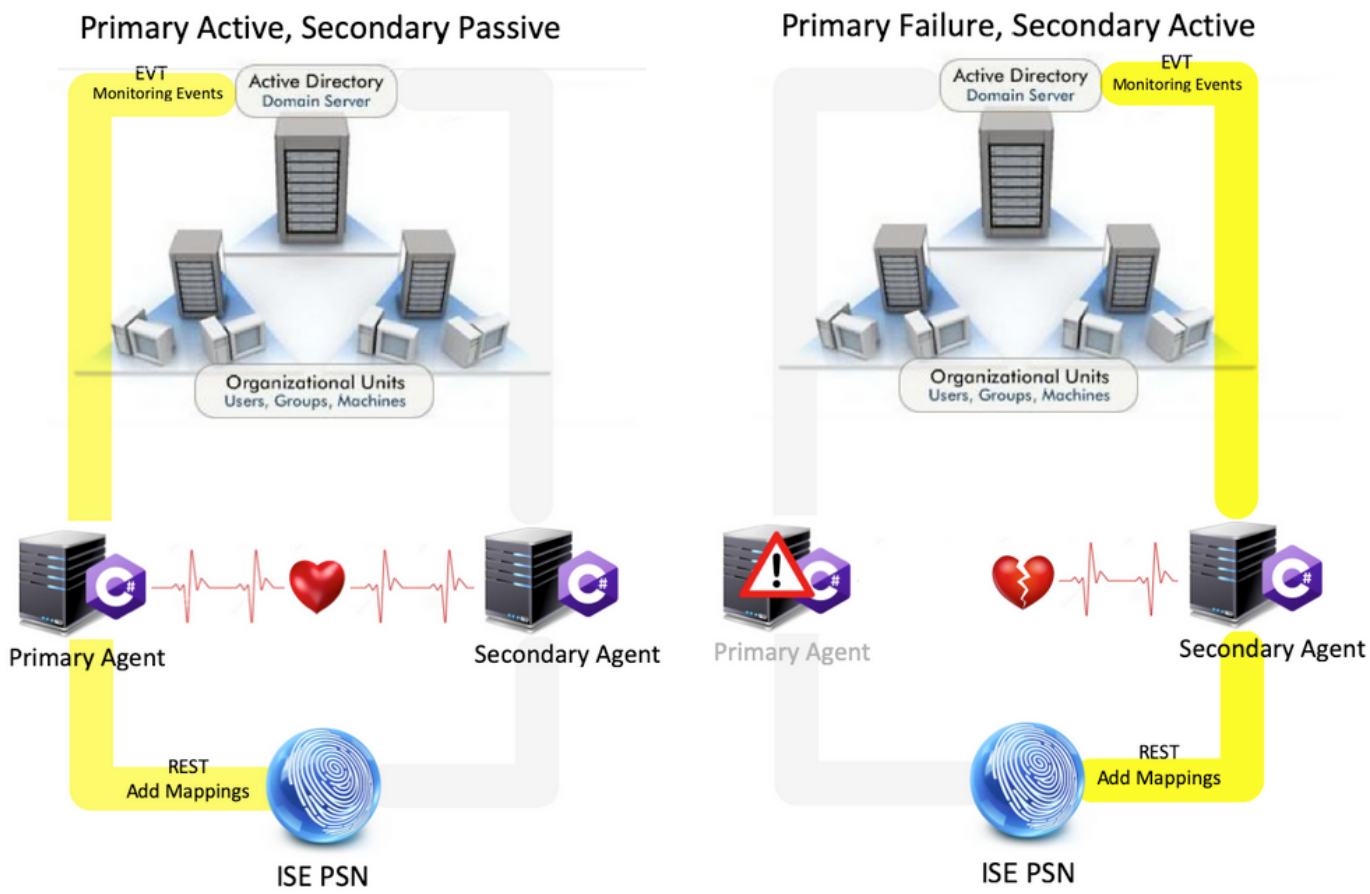
새로운 프로토콜의 필요성

ISE의 패시브 ID(Passive ID) 기능은 ID 기반 방화벽, EasyConnect 등을 비롯한 여러 중요한 사용 사례를 구동합니다.이 기능은 Active Directory 도메인 컨트롤러에 로그인하고 사용자 이름과 IP 주소를 학습하는 사용자를 모니터링하는 기능에 따라 달라집니다.도메인 컨트롤러를 모니터링하는 데 사용하는 현재 주 프로토콜은 WMI입니다.그러나 구성이 어렵고, 간섭이 심하며, 클라이언트와 서버 모두에 성능에 영향을 미치며, 대규모 구축에서 로그온 이벤트를 볼 때 지연 시간이 매우 큰 경우도 있습니다.Passive Identity Services에 필요한 정보를 폴링하기 위한 철저한 조사와 대체 방법, EVT 또는 Eventing API라고 하는 대체 프로토콜, 이 활용 사례를 처리하는 데 더 효율적인 방법이 결정되었습니다.MS-**EVEN6**라고도 하며, Eventing Remote Protocol이라고도 합니다. 이는 기본 RPC 기반 on-the-wire 프로토콜입니다.

MS-EVEN6 사용의 장점

고가용성

원래 에이전트에는 고가용성 옵션이 없으며 에이전트가 실행 중이거나 가동 중지된 서버에서 유지보수를 수행해야 하는 경우 로그온 이벤트가 누락되고 ID 기반 방화벽 같은 기능을 사용하면 이 기간 동안 데이터가 손실됩니다.이 릴리스에 앞서 ISE PIC 에이전트를 사용하는 데 있어 가장 큰 문제 중 하나입니다.ISE는 UDP Port 9095를 사용하여 에이전트 간 하트비트를 교환합니다.

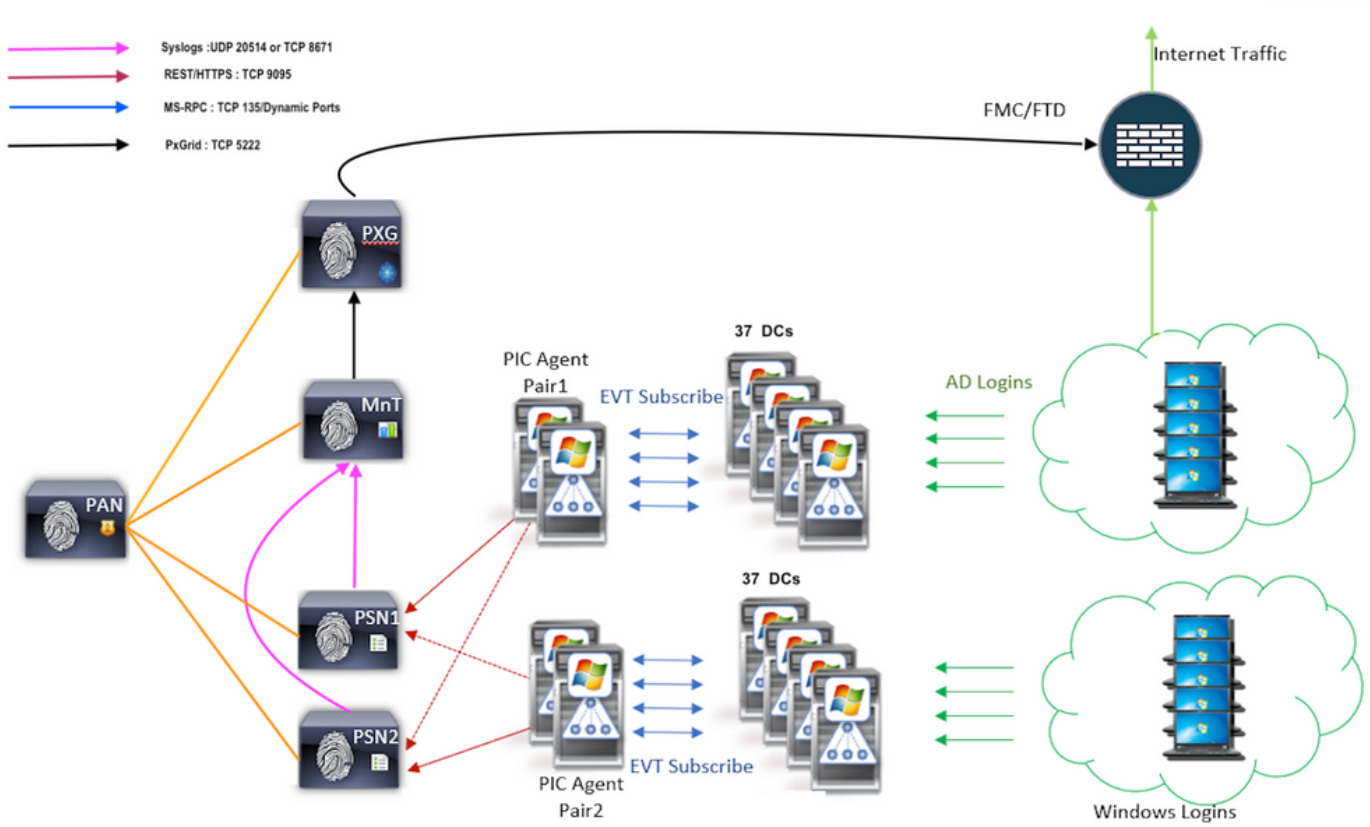


확장성

새 에이전트는 지원되는 도메인 컨트롤러 수와 처리할 수 있는 이벤트 수에 대한 확장 번호를 늘려 더 나은 지원을 제공합니다.테스트한 스케일 번호는 다음과 같습니다.

- 모니터링되는 최대 도메인 컨트롤러 수(에이전트 2쌍 포함):74
- 테스트된 최대 매핑/이벤트 수:292,000(DC당 3,950개의 이벤트)
- 테스트한 최대 TPS:500

테스트 설정 아키텍처 확장



기록 이벤트 쿼리

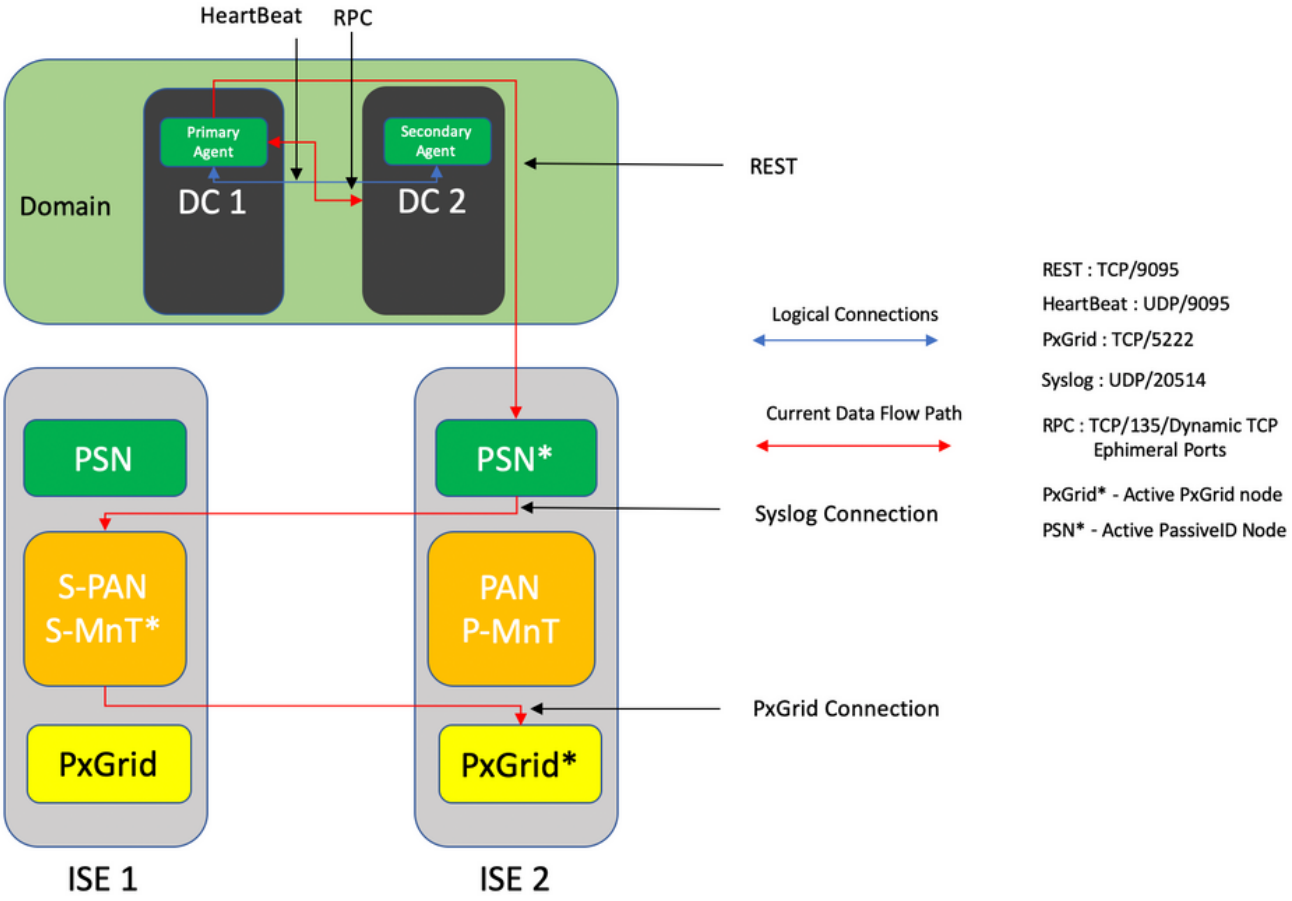
장애 조치의 경우 또는 PIC-Agent에 대해 서비스를 다시 시작하는 경우 데이터가 손실되지 않도록 지정된 시간 동안 생성된 이벤트를 쿼리하여 PSN 노드로 다시 보냅니다.기본적으로 서비스 시작 시점부터 60초 분량의 과거 이벤트가 ISE에 의해 쿼리되어 서비스 손실 중 데이터 손실을 방지합니다.

처리 오버헤드 감소

대규모 또는 과부하 상태에서 CPU가 집중된 WMI와 달리 EVT는 WMI와 같은 많은 리소스를 사용하지 않습니다.규모 테스트에서는 EVT를 사용하여 쿼리의 성능이 크게 향상되었습니다.

구성

연결 다이어그램

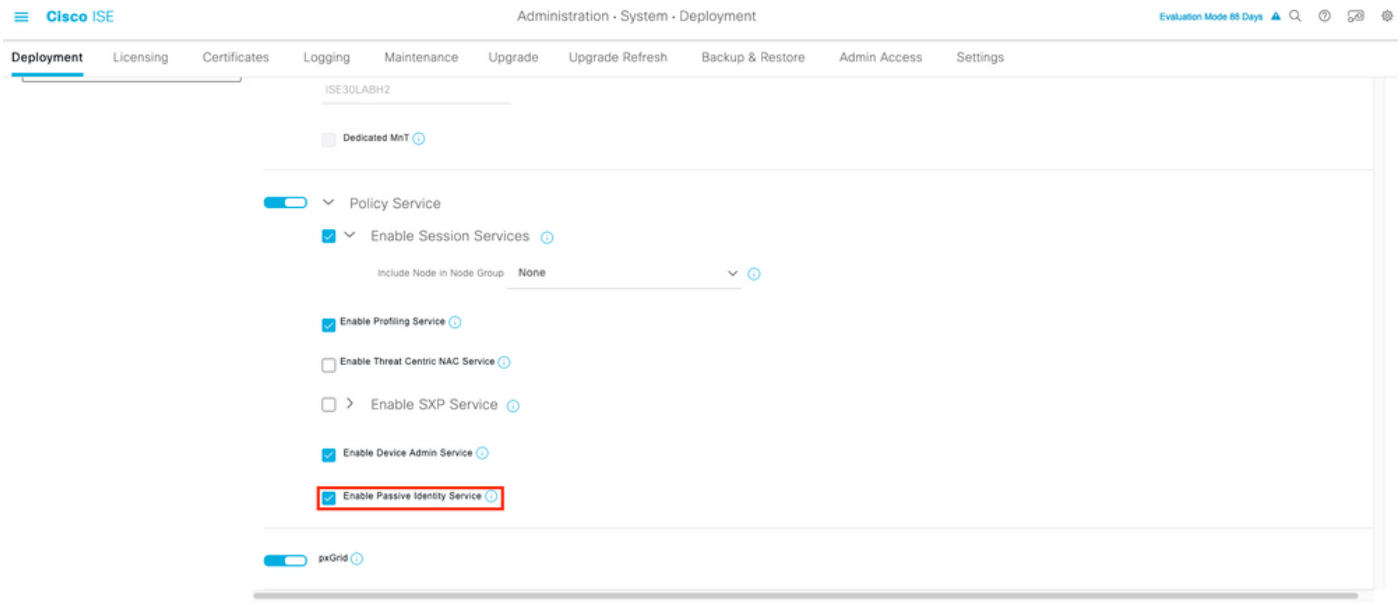


구성

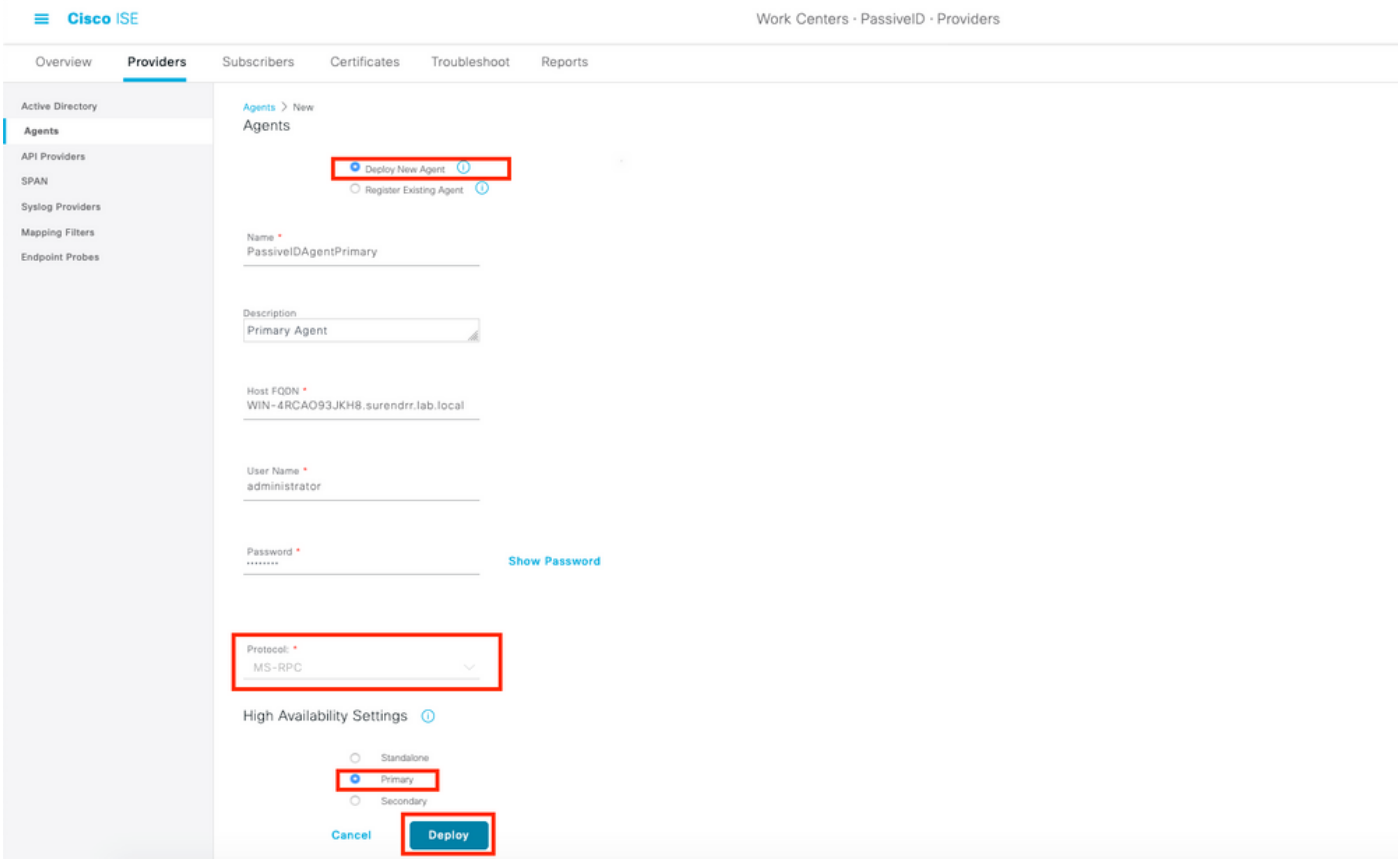
PassiveID 에이전트에 대한 ISE 구성

PassiveID 서비스를 구성하려면 하나 이상의 PSN(Policy Service Node)에서 Passive Identity Services를 활성화해야 합니다.액티브/스탠바이 작업 모드에서 작동하는 패시브 ID 서비스에 최대 2개의 노드를 사용할 수 있습니다.또한 ISE는 Active Directory 도메인에 가입되어야 하며 해당 도메인에 있는 도메인 컨트롤러만 ISE에 구성된 에이전트에 의해 모니터링할 수 있습니다.ISE를 Active Directory 도메인에 가입시키려면 Active Directory 통합 가이드를 참조하십시오.

Administration(관리) > **System(시스템) > Deployment(구축) > [Choose a PSN](PSN 선택) > Edit(편집)로 이동하여** 여기에 표시된 대로 Passive Identity Services(수동 ID 서비스)를 활성화합니다.



Work Centers(작업 **센터) > PassiveID > Providers(제공자) > Agents(상담원) > Add(추가)**로 이동하여 여기에 표시된 대로 새 에이전트를 구축합니다.

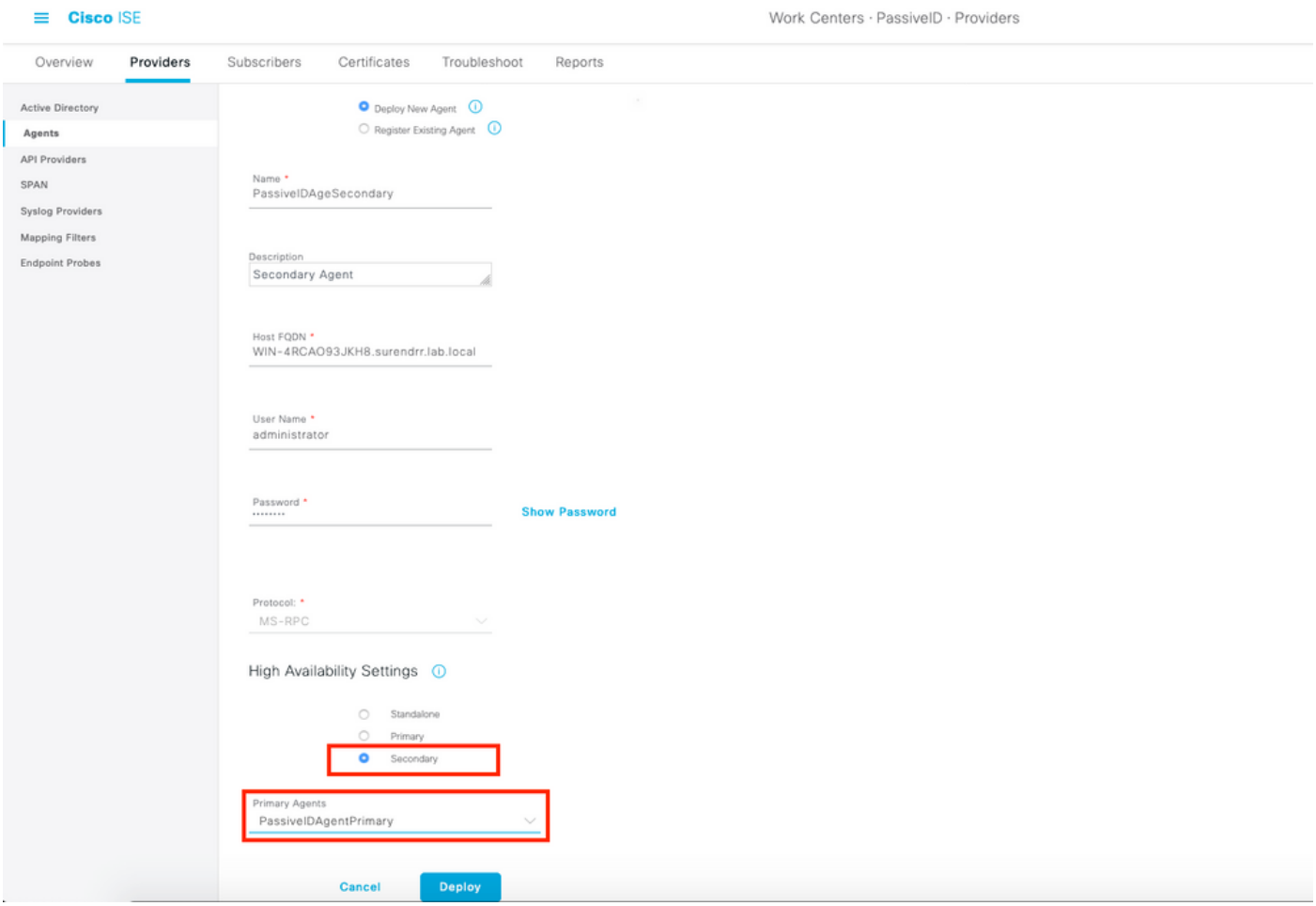


참고:1. 에이전트가 도메인 컨트롤러에 ISE에 의해 설치되도록 계획되어 있는 경우, 여기에서 사용된 계정은 프로그램을 설치하고 Host FQDN 필드에 언급된 서버에서 실행할 수 있는 충분한 권한을 가지고 있어야 합니다.여기서 호스트 FQDN은 도메인 컨트롤러 대신 구성원 서버의 FQDN일 수 있습니다.

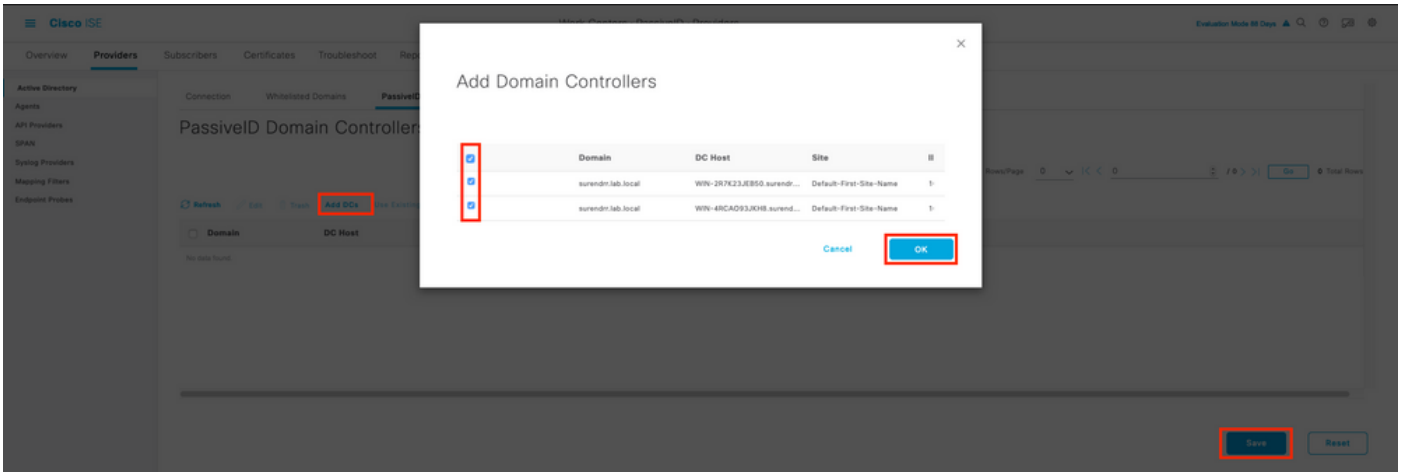
2. 에이전트가 이미 수동으로 설치되었거나 MSRPC를 사용하여 ISE의 이전 배포에서 설치된 경우 Active Directory 또는 Windows 측에서 필요한 권한 및 구성이 WMI에 비해 적으며 PIC 에이전트가 사용하는 다른 프로토콜(및 3.0 이전 버전만 사용 가능)이 사용됩니다.이 경우에 사용되는 사용자 계정은 **이벤트 로그 판독기 그룹**의 일부인 일반 도메인 계정일 수 있

습니다.Register **Existing Agent(기존 에이전트 등록)**를 선택하고 이러한 계정 세부 정보를 사용하여 도메인 컨트롤러에 수동으로 설치된 에이전트를 등록합니다.

성공적으로 구축한 후 다른 서버에서 다른 에이전트를 구성하고 이 이미지에 표시된 대로 보조 에이전트로 추가한 다음 기본 피어로 추가합니다.

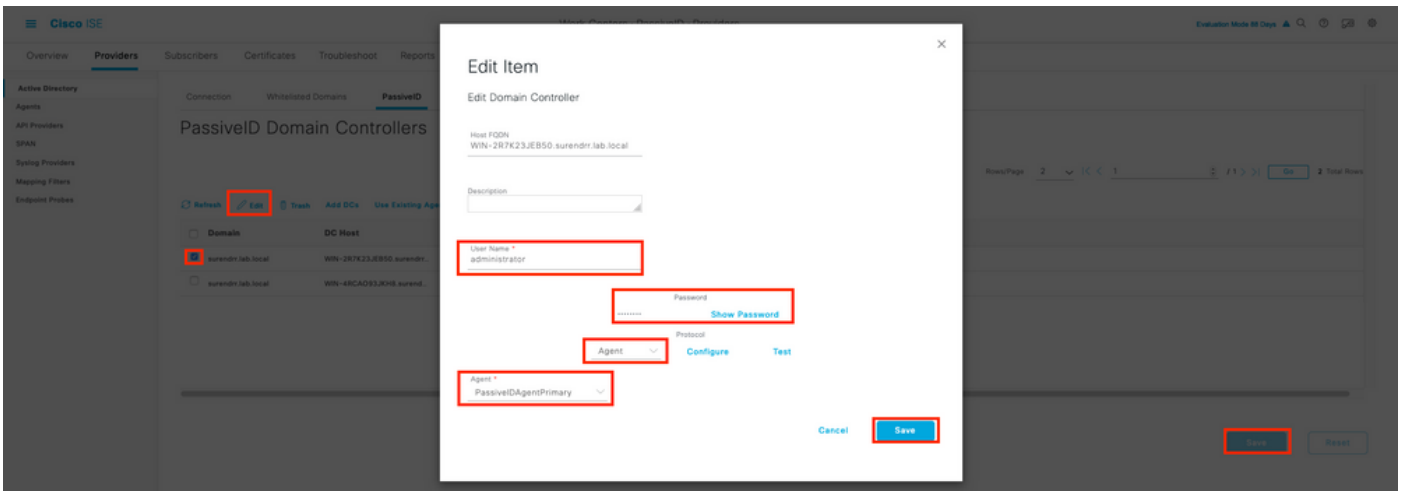


에이전트를 사용하여 도메인 컨트롤러를 모니터링하려면 **Work Centers(작업 센터) > PassiveID > Providers(제공자) > Active Directory > [Click on the Join Point] > PassiveID로 이동합니다**.Add DCs(**DC 추가)**를 클릭하고 User-IP Mapping/events(사용자-IP 매핑/이벤트)가 검색되는 도메인 컨트롤러를 선택한 다음 **OK(확인)를** 클릭한 다음 **Save(저장)를** 클릭하여 이 이미지에 표시된 대로 변경 사항을 저장합니다.

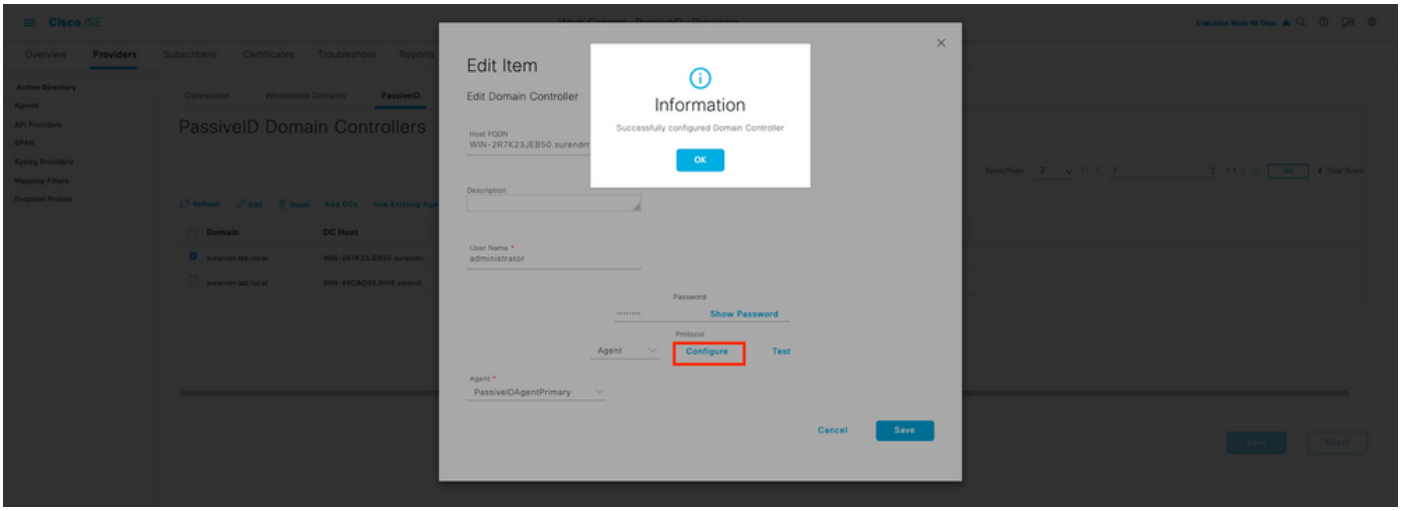


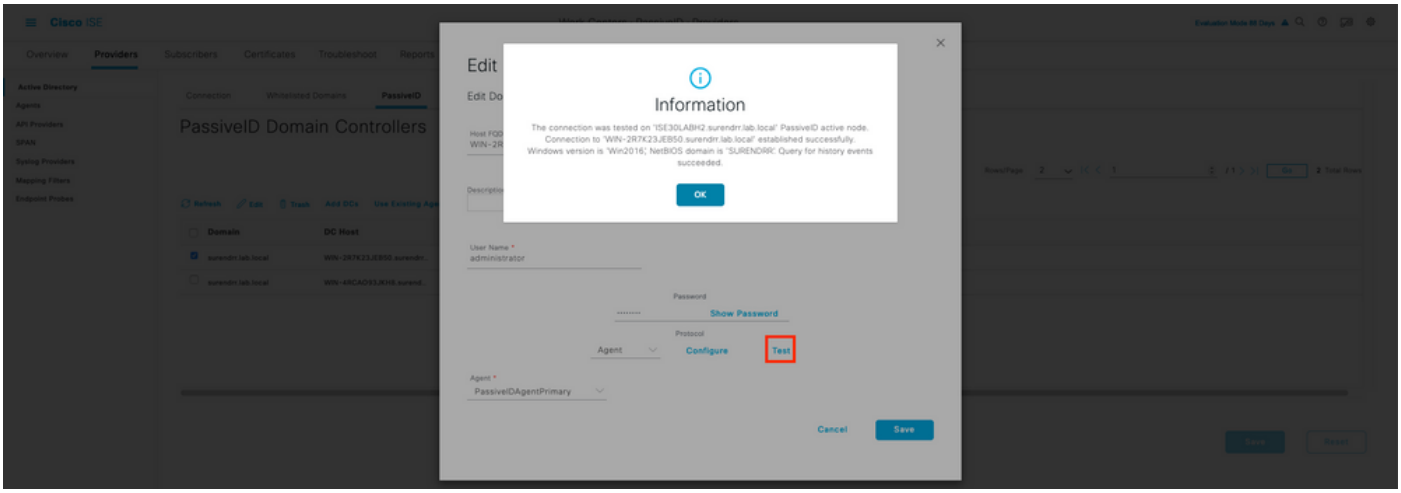
이벤트를 검색하는 데 사용할 에이전트를 지정하려면 Work Centers(작업 센터) > PassiveID >

Providers(패시브 ID) > Active Directory > [Click on the Join Point] > PassiveID로 이동합니다.도메인 컨트롤러를 선택하고 **Edit**(수정)를 클릭합니다.*사용자 이름* 및 *비밀번호*를 *입력합니다.*Agent(**에이전트**)를 선택한 다음 **Save**(저장)를 선택합니다.PassiveID 탭에서 Save를 클릭하여 컨피그레이션을 완료합니다.



구성 및 테스트 버튼의 도움을 받아 컨피그레이션이 올바르게 적용되었는지 확인하려면 여기 이미지에 표시된 대로 다음을 수행하십시오.





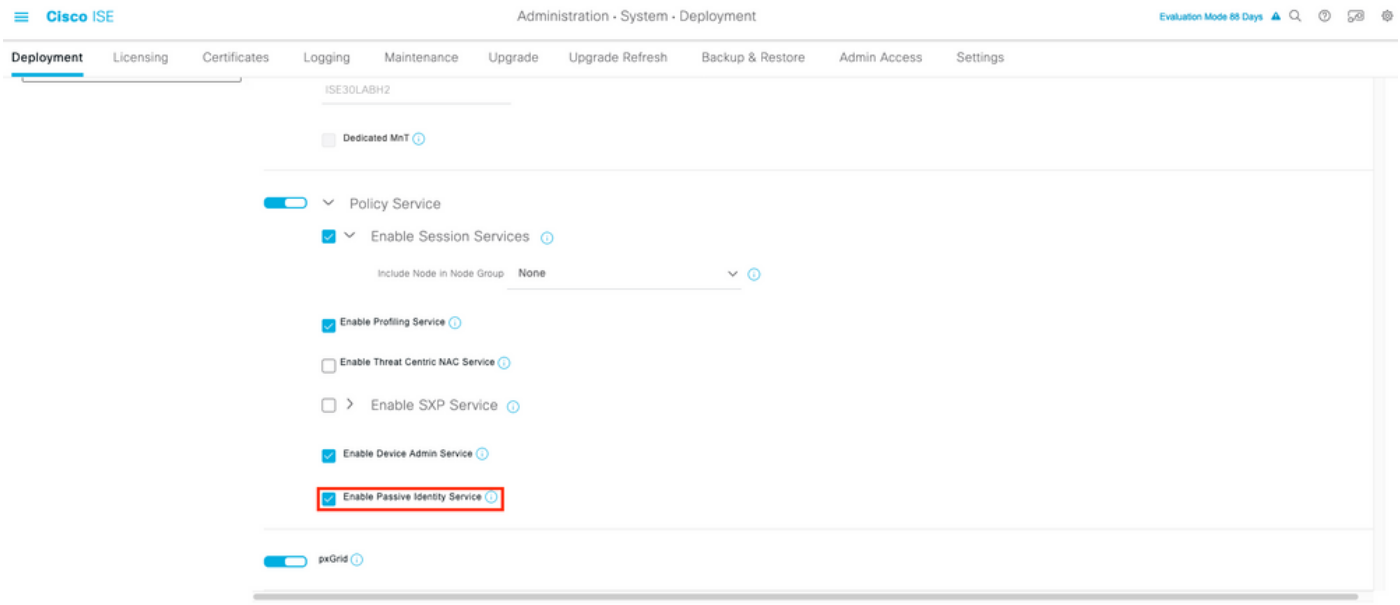
PassiveID 에이전트 구성 파일 이해

PassiveID Agent 구성 파일은 C:\Program Files **(x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config에 있습니다.**컨피그레이션 파일에는 다음과 같은 내용이 있습니다.

다음을 확인합니다.

ISE에서 PassiveID 서비스 확인

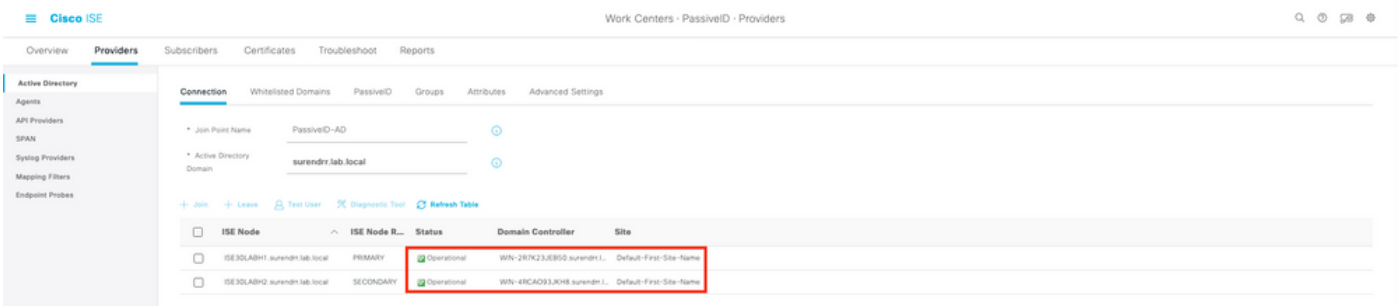
1. GUI에서 PassiveID 서비스가 활성화되고 ISE의 CLI에서 **show application status** 명령에서 실행으로 표시되는지 확인합니다.



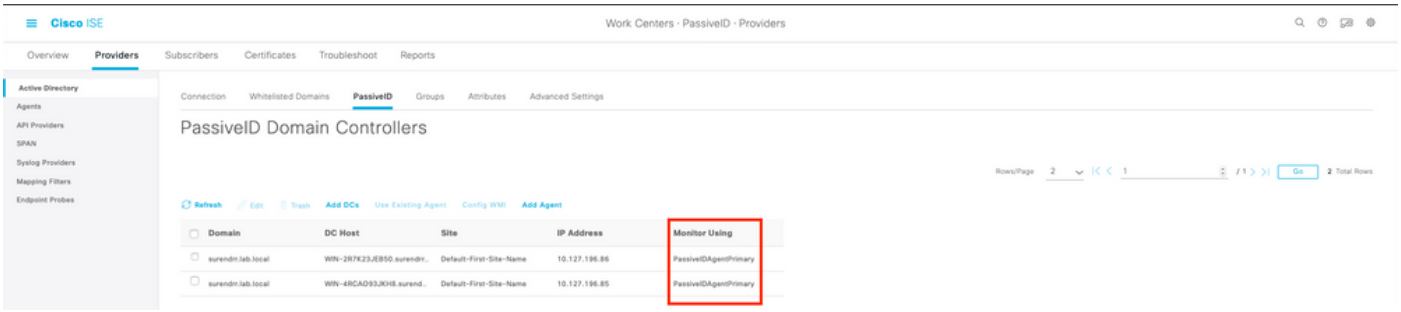

```
ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 129052
Database Server running 108 PROCESSES
Application Server running 9830
Profiler Database running 5127
ISE Indexing Engine running 13361
AD Connector running 20609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

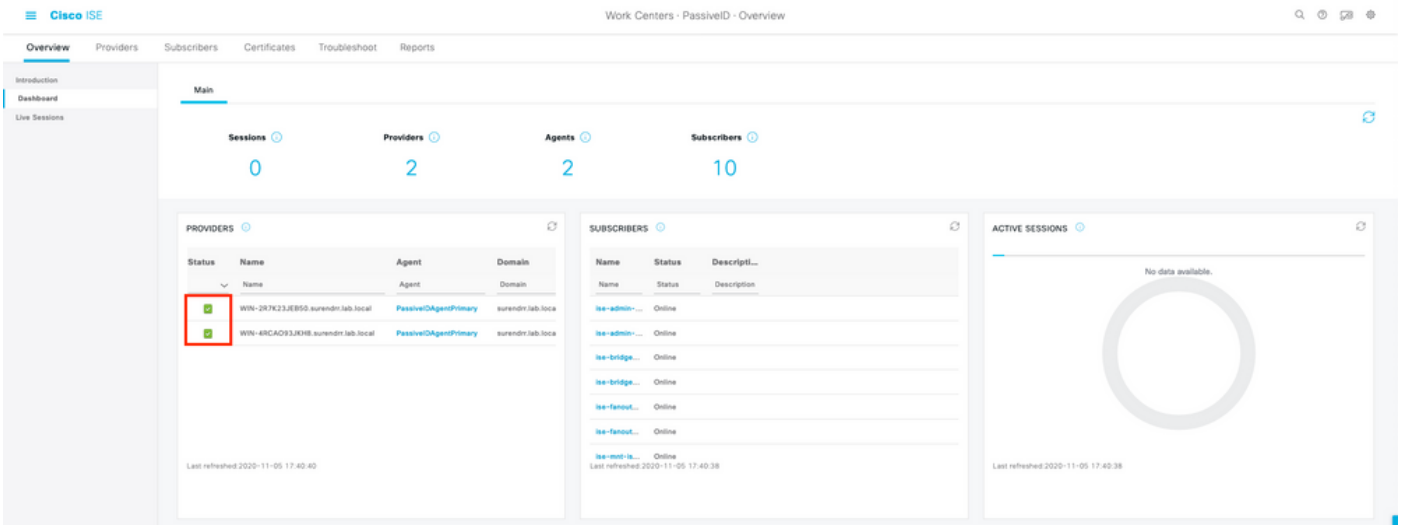
2. ISE Active Directory 공급자가 **작업 센터 > PassiveID > Providers > Active Directory > Connection**에서 도메인 컨트롤러**에** 연결되어 있는지 **확인합니다**.



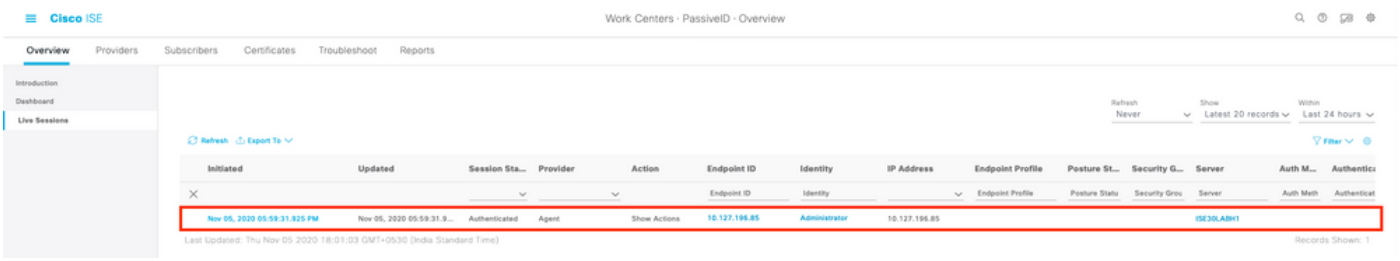
3. 필요한 도메인 컨트롤러가 작업 **센터 > PassiveID > Providers > Active Directory > PassiveID**의 **에이전트에서 모니터링되고 있는지 확인합니다**.



4. 모니터링 중인 도메인 컨트롤러의 상태가 **Work Centers(작업 센터) > PassiveID > Overview(개요) > Dashboard(대시보드)**의 대시보드에서 녹색으로 표시된 **상태인지 확인합니다**.



5. Windows 로그온이 **Work Centers(작업 센터) > PassiveID > Overview(개요) > Live Sessions(라이브 세션)**에서 도메인 컨트롤러에 등록될 때 채워지는 라이브 세션**을 확인합니다**.



Windows 서버에서 에이전트 서비스 확인

1. PIC 에이전트가 설치된 서버에서 ISEPICAgent 서비스를 확인합니다.