

EVT-basierter Identity Services Engine-passiver ID-Agent konfigurieren

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Bedarf an einem neuen Protokoll](#)

[Vorteile durch den Einsatz von MS-EVEN6](#)

[Hohe Verfügbarkeit](#)

[Skalierbarkeit](#)

[Architektur für Scale-Test-Setup](#)

[Abfrage von Verlaufereignissen](#)

[Weniger Verarbeitungsaufwand](#)

[Konfiguration](#)

[Verbindungsdiagramm](#)

[Konfigurationen](#)

[Konfigurieren der ISE für den PassiveID-Agenten](#)

[PassiveID Agent-Konfigurationsdatei verstehen](#)

[Überprüfung](#)

[Überprüfen Sie die PassiveID-Services auf der ISE.](#)

[Überprüfen Sie die Agent-Dienste auf Windows Server.](#)

Einführung

Dieses Dokument beschreibt den neuen ISE Passive Identity Connector (ISE-PIC) Agent, der in der ISE 3.0-Version eingeführt wurde, seine Vorteile und die Konfiguration dieses Agenten auf der ISE. Der ISE Passive Identity Agent ist dank Cisco FirePower Management Center auch ein integraler Bestandteil der Identity Firewall-Lösung geworden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Identity Services Administration
- MS-RPC, WMI-Protokolle
- Active Directory-Verwaltung

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Identity Services Engine ab Version 3.0
- Microsoft Windows Server 2016-Standard

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Bedarf an einem neuen Protokoll

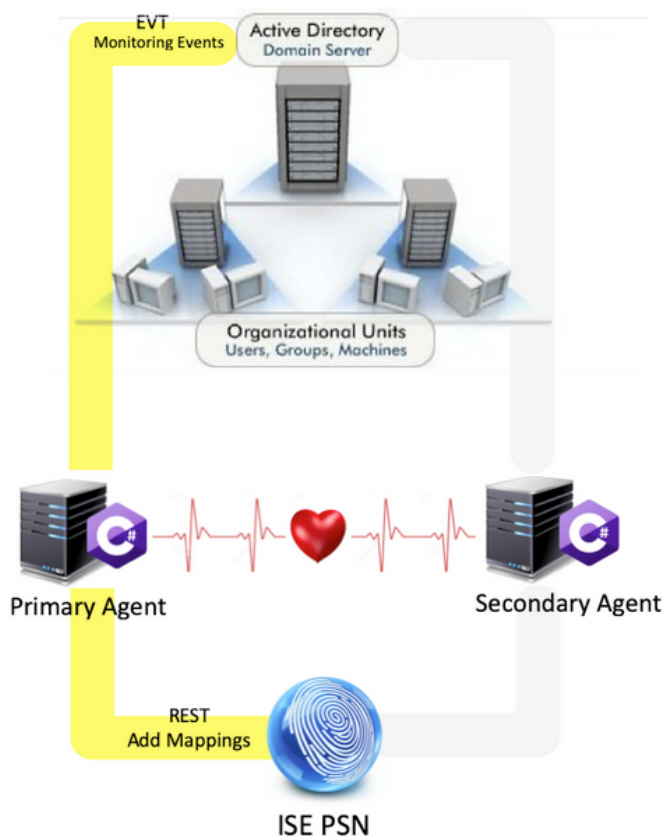
Die Passive Identity-Funktion (Passive Identity, passive ID) der ISE unterstützt eine Reihe wichtiger Anwendungsfälle, darunter die identitätsbasierte Firewall, EasyConnect usw. Diese Funktion hängt von der Fähigkeit ab, Benutzer zu überwachen, die sich bei Active Directory Domain Controllern anmelden und deren Benutzernamen und IP-Adressen ermitteln. Das aktuelle Hauptprotokoll, das wir zur Überwachung der Domänencontroller verwenden, ist WMI. Die Konfiguration ist jedoch schwierig/invasiv, sie hat Auswirkungen auf die Leistung von Clients und Servern und manchmal eine extrem hohe Latenz bei der Anzeige von Anmeldeereignissen in skalierten Bereitstellungen. Nach gründlicher Recherche und alternativen Möglichkeiten, die für passive Identitätsdienste erforderlichen Informationen abzurufen, wurde ein alternatives Protokoll - das EVT- oder Eventing-API genannt wird, entschieden, das bei der Behandlung dieses Anwendungsfalls effizienter ist. Es wird manchmal auch als **MS-EVEN6** bezeichnet, auch bekannt als Eventing Remote Protocol, das das zugrunde liegende RPC-basierte, drahtgebundene Protokoll ist.

Vorteile durch den Einsatz von MS-EVEN6

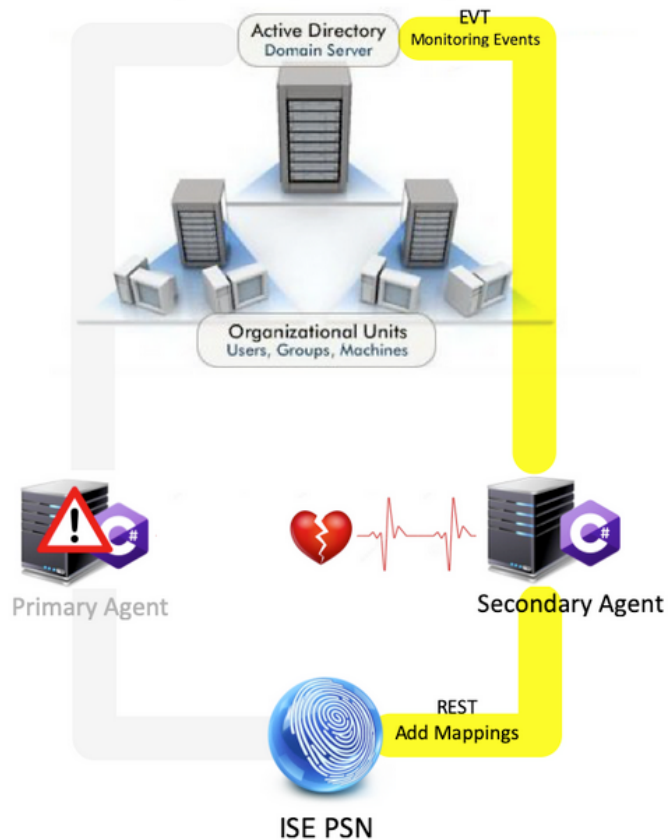
Hohe Verfügbarkeit

Der ursprüngliche Agent verfügte über keine High Availability-Option. Wenn Wartungsarbeiten auf dem Server durchgeführt werden müssen, auf dem der Agent ausgeführt wurde oder bei einem Ausfall aufgetreten war, würden Anmeldeereignisse verpasst und Funktionen wie die identitätsbasierte Firewall würden in diesem Zeitraum einen Datenverlust erleiden. Dies ist eines der Hauptprobleme bei der Verwendung von ISE PIC Agent vor dieser Version. Die ISE verwendet den UDP-Port 9095, um Heartbeats zwischen den Agenten auszutauschen.

Primary Active, Secondary Passive



Primary Failure, Secondary Active

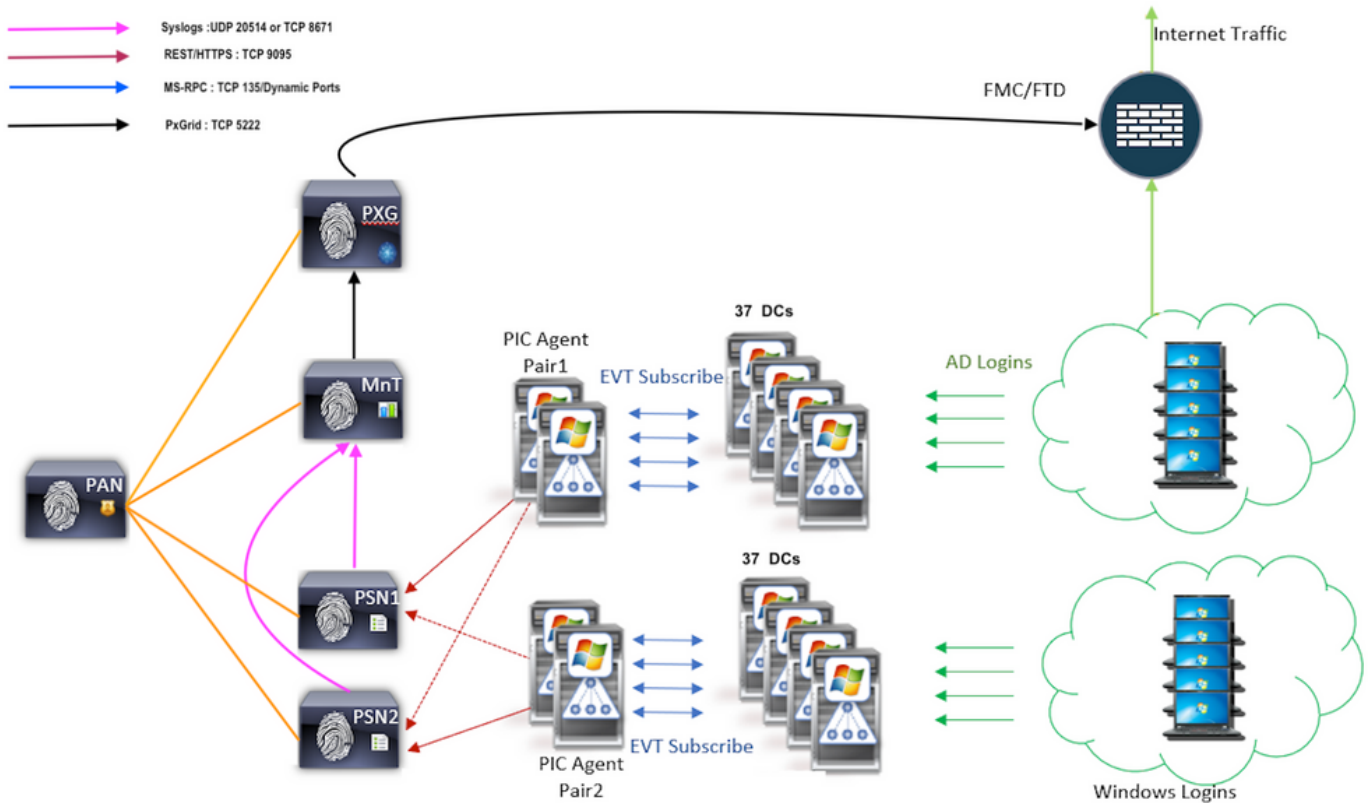


Skalierbarkeit

Der neue Agent bietet bessere Unterstützung durch höhere Skalierungszahlen für eine unterstützte Anzahl von Domain-Controllern und die Anzahl der Ereignisse, die er verarbeiten kann. Die getesteten Skalierungszahlen sind wie folgt:

- Maximale Anzahl der überwachten Domänen-Controller (mit zwei Agentenpaaren): 74
- Maximale Anzahl getesteter Zuordnungen/Ereignisse: 292.000 (3.950 Ereignisse pro Rechenzentrum)
- Maximale getestete TPS: 500

Architektur für Scale-Test-Setup



Abfrage von Verlaufereignissen

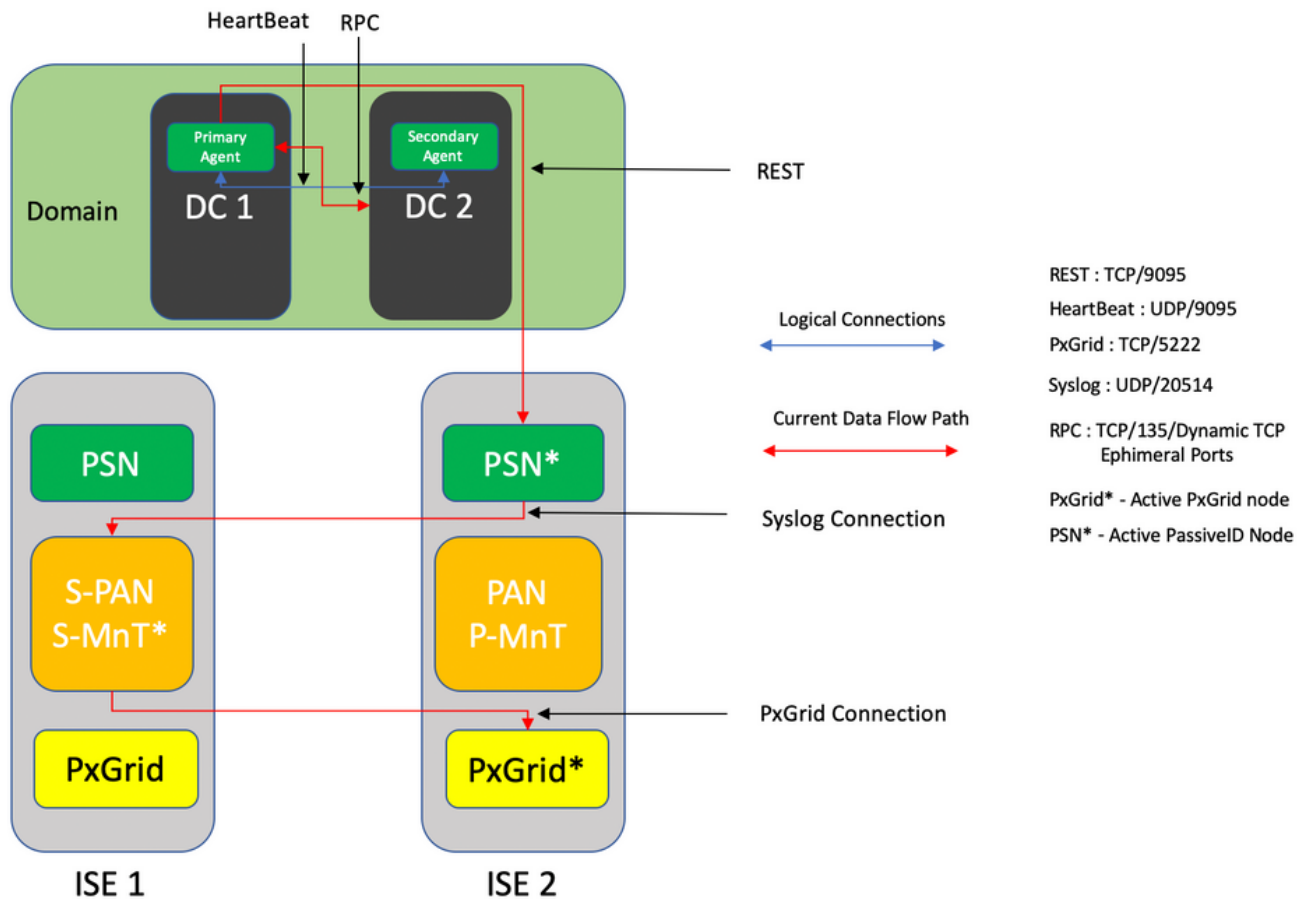
Im Falle eines Failovers oder eines Service-Neustarts für den PIC-Agent werden Ereignisse abgefragt und an die PSN-Knoten erneut gesendet, um sicherzustellen, dass keine Daten verloren gehen. In der Standardeinstellung werden von der ISE zurückliegende Ereignisse, die 60 Sekunden nach Servicestart zurückliegen, abgefragt, um Datenverluste während des Serviceverlusts auszugleichen.

Weniger Verarbeitungsaufwand

Im Gegensatz zu WMI, das CPU-intensiv unter großem Umfang oder hoher Auslastung ist, verbraucht EVT nicht so viele Ressourcen wie WMI. Die Skalentests zeigten eine deutlich verbesserte Leistung der Anfragen bei Verwendung von EVT.

Konfiguration

Verbindungsdiagramm

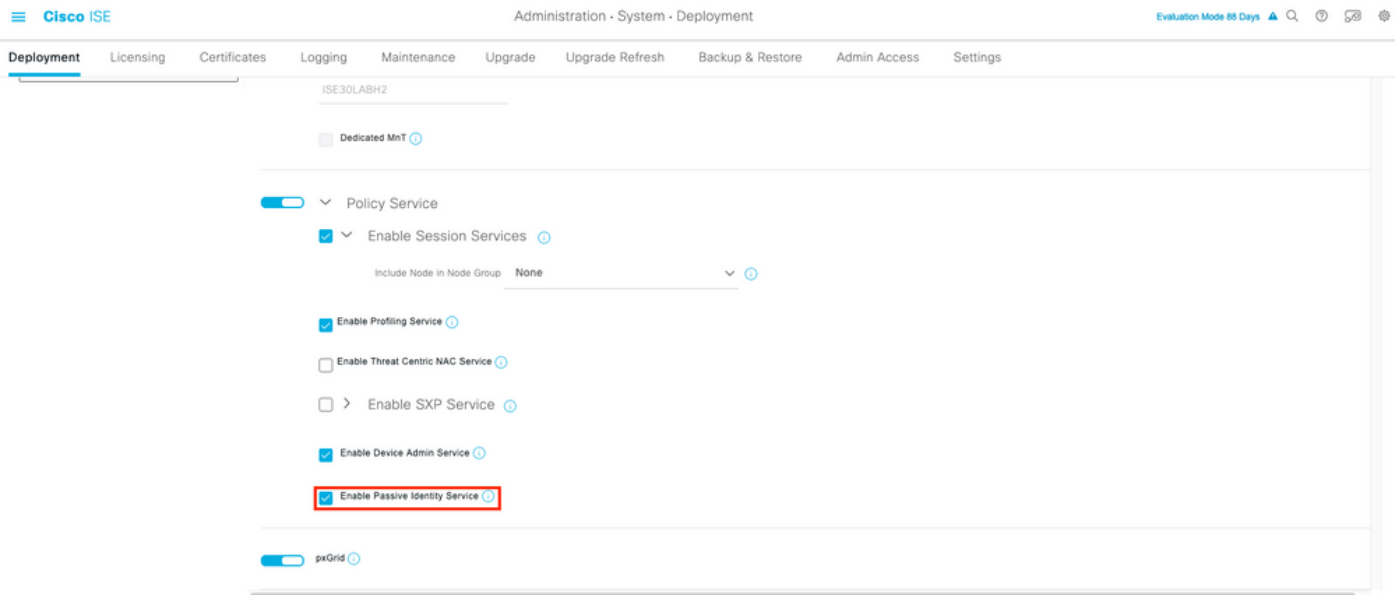


Konfigurationen

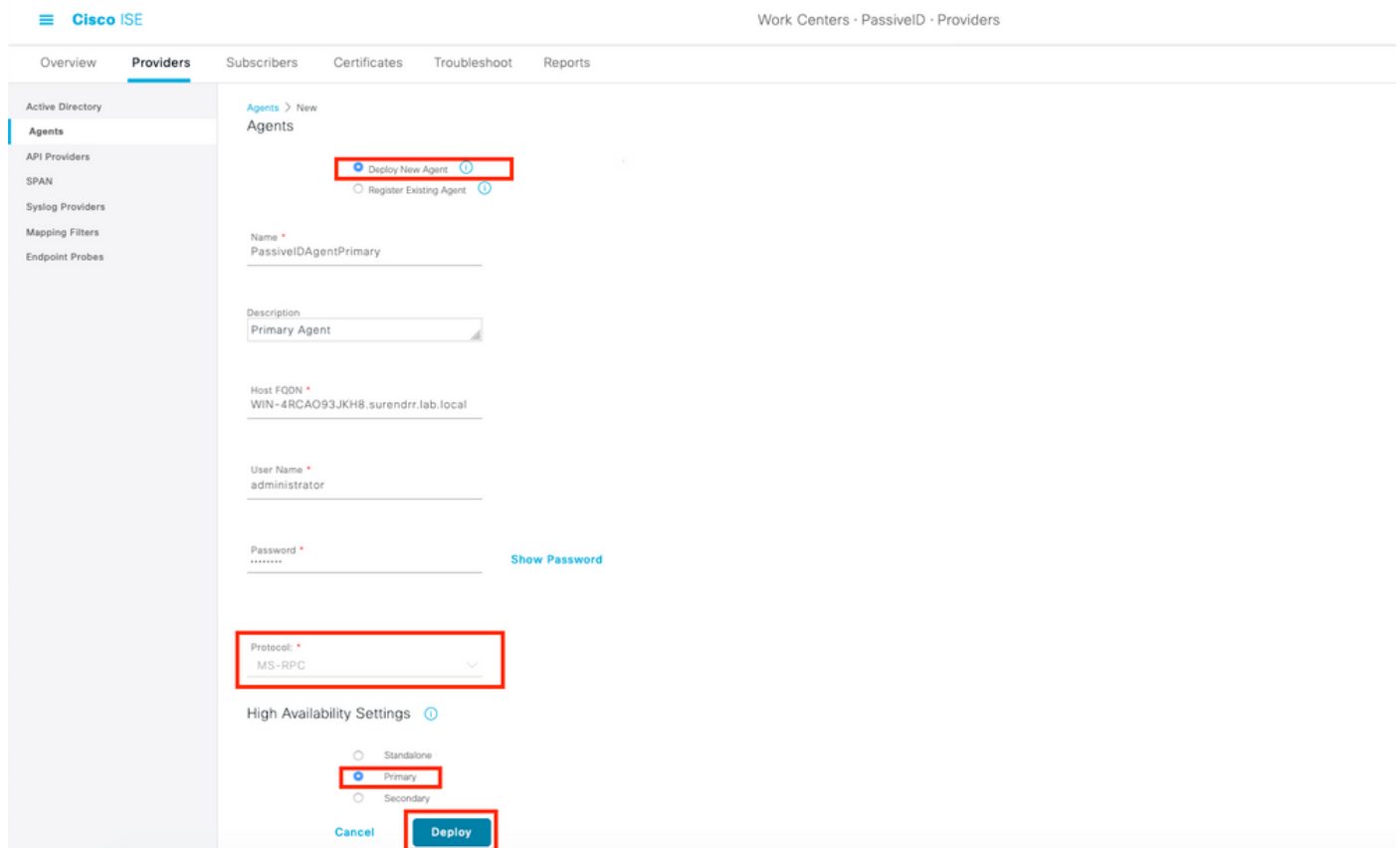
Konfigurieren der ISE für den PassiveID-Agenten

Um PassiveID-Dienste zu konfigurieren, müssen die Passive Identity Services auf mindestens einem Policy Service Node (PSN) aktiviert sein. Maximal zwei Knoten können für passive Identitätsdienste verwendet werden, die im Aktiv/Standby-Betriebsmodus funktionieren. Die ISE muss auch einer Active Directory-Domäne hinzugefügt werden, und nur die in dieser Domäne vorhandenen Domänen-Controller können von Agents überwacht werden, die auf der ISE konfiguriert sind. Informationen zum Beitritt zur ISE zu einer Active Directory-Domäne finden Sie im [Active Directory Integration Guide](#).

Navigieren Sie zu **Administration > System > Deployment > [Wählen Sie ein PSN] > Edit**, um passive Identitätsdienste zu aktivieren, wie hier gezeigt:



Navigieren Sie zu **Work Center > PassiveID > Providers > Agents > Add** to deploy a new Agent, wie hier gezeigt:



Hinweis: Das hier verwendete Konto muss über ausreichend Berechtigungen verfügen, um ein Programm zu installieren und auf dem im Feld Host FQDN (Host FQDN) genannten Server auszuführen. Der Host-FQDN hier kann der eines Mitglieds-Servers sein, nicht der eines Domänencontrollers. Wenn ein Agent bereits manuell oder aus einer früheren Bereitstellung von der ISE installiert wurde, wählen Sie **Bestehenden Agenten registrieren aus**.

Konfigurieren Sie nach einer erfolgreichen Bereitstellung einen anderen Agenten auf einem anderen Server, und fügen Sie ihn als sekundären Agent und dann als dessen primären Peer

hinzu, wie in diesem Image gezeigt.

Cisco ISE Work Centers · PassiveID · Providers

Overview **Providers** Subscribers Certificates Troubleshoot Reports

Active Directory

Agents

API Providers

SPAN

Syslog Providers

Mapping Filters

Endpoint Probes

Deploy New Agent 1

Register Existing Agent 1

Name *
PassiveIDAgeSecondary

Description
Secondary Agent

Host FQDN *
WIN-4RCAO93JKH8.surendrr.lab.local

User Name *
administrator

Password *
..... Show Password

Protocol *
MS-RPC

High Availability Settings 1

Standalone

Primary

Secondary

Primary Agents
PassiveIDAgentPrimary

Cancel Deploy

Um die Domänencontroller mithilfe der Agenten zu überwachen, navigieren Sie zu **Work Centers > PassiveID > Providers > Active Directory > [Click on the Join Point] > PassiveID**. Klicken Sie auf **Add DCs**, wählen Sie die Domänencontroller aus, von denen die Benutzer-IP-Zuordnung/Ereignisse abgerufen werden, und klicken Sie auf **OK** und klicken Sie dann auf **Save**, um die Änderungen zu speichern, wie in diesem Bild gezeigt.

Cisco ISE Evaluation Mode 90 Days

Overview **Providers** Subscribers Certificates Troubleshoot Reports

Active Directory

Agents

API Providers

SPAN

Syslog Providers

Mapping Filters

Endpoint Probes

PassiveID Domain Controller

Network Lab Host Add DCs

Domain DC Host

No data found

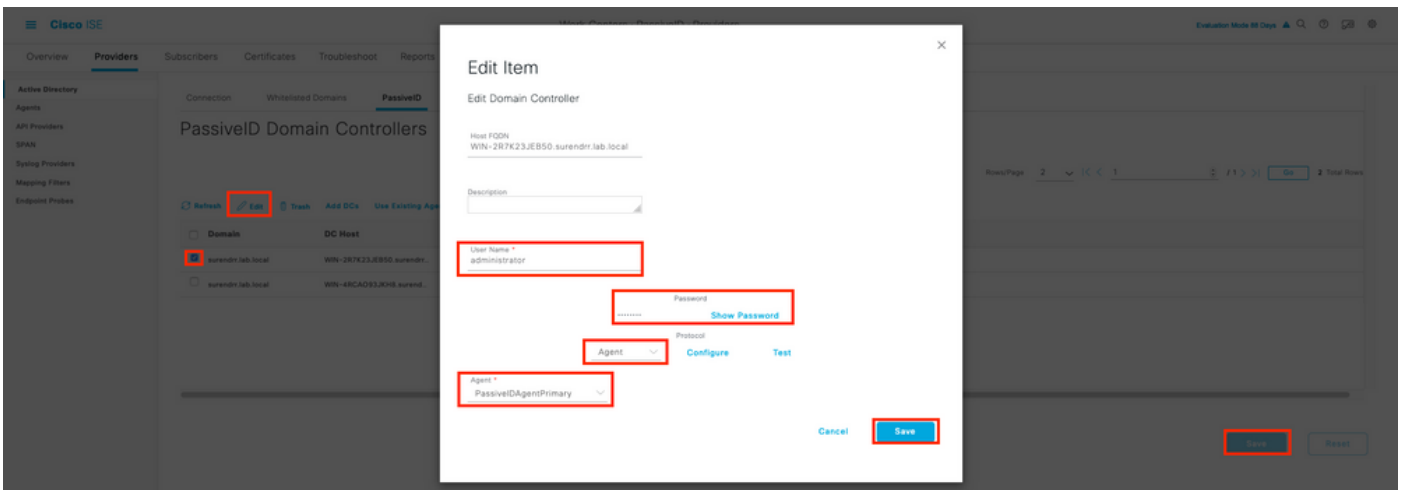
Save Reset

Add Domain Controllers

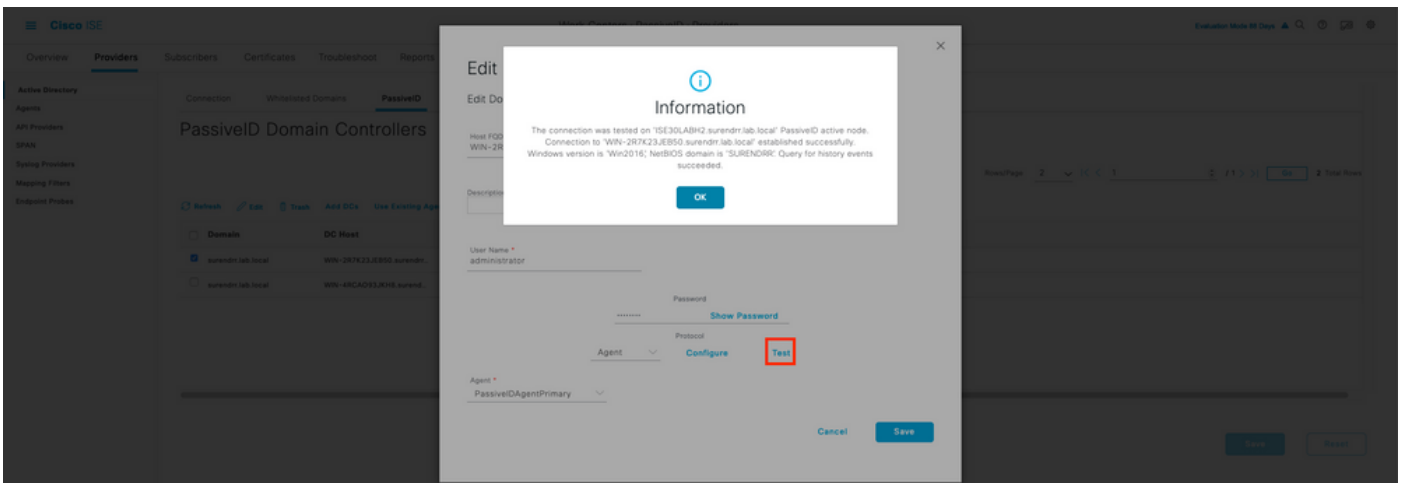
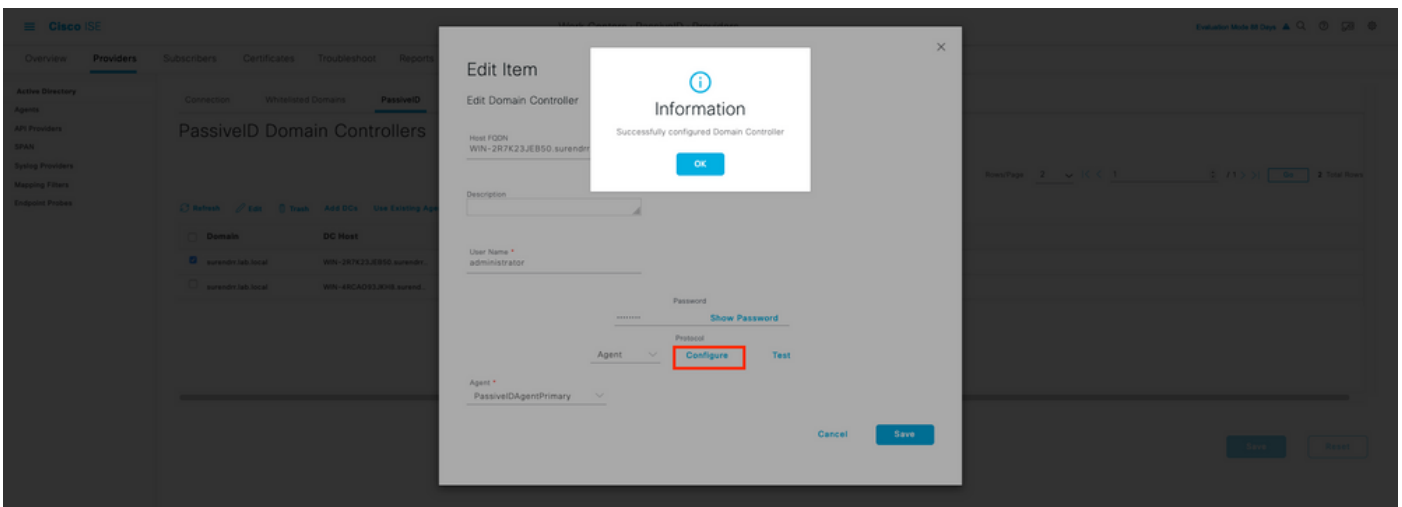
Domain	DC Host	Site	
surendrr.lab.local	WIN-2R7K23JEB50.surendr...	Default-First-Site-Name	1
surendrr.lab.local	WIN-4RCAO93JKH8.surendr...	Default-First-Site-Name	1

Cancel OK

Um die Agenten anzugeben, von denen die Ereignisse abgerufen werden sollen, navigieren Sie zu **Work Centers > PassiveID > Providers > Active Directory > [Klicken Sie auf Join Point] > PassiveID**. Wählen Sie die Domänencontroller aus, und klicken Sie auf **Bearbeiten**. Geben Sie den *Benutzernamen* und das *Kennwort* ein. Wählen Sie **Agent** und dann **Speichern** des Dialogfelds. Klicken Sie auf der Registerkarte PassiveID auf **Speichern**, um die Konfiguration abzuschließen.



Mithilfe der Schaltflächen **Konfigurieren** und **Test** können Sie überprüfen, ob die Konfiguration korrekt angewendet wurde, wie in den folgenden Bildern gezeigt:



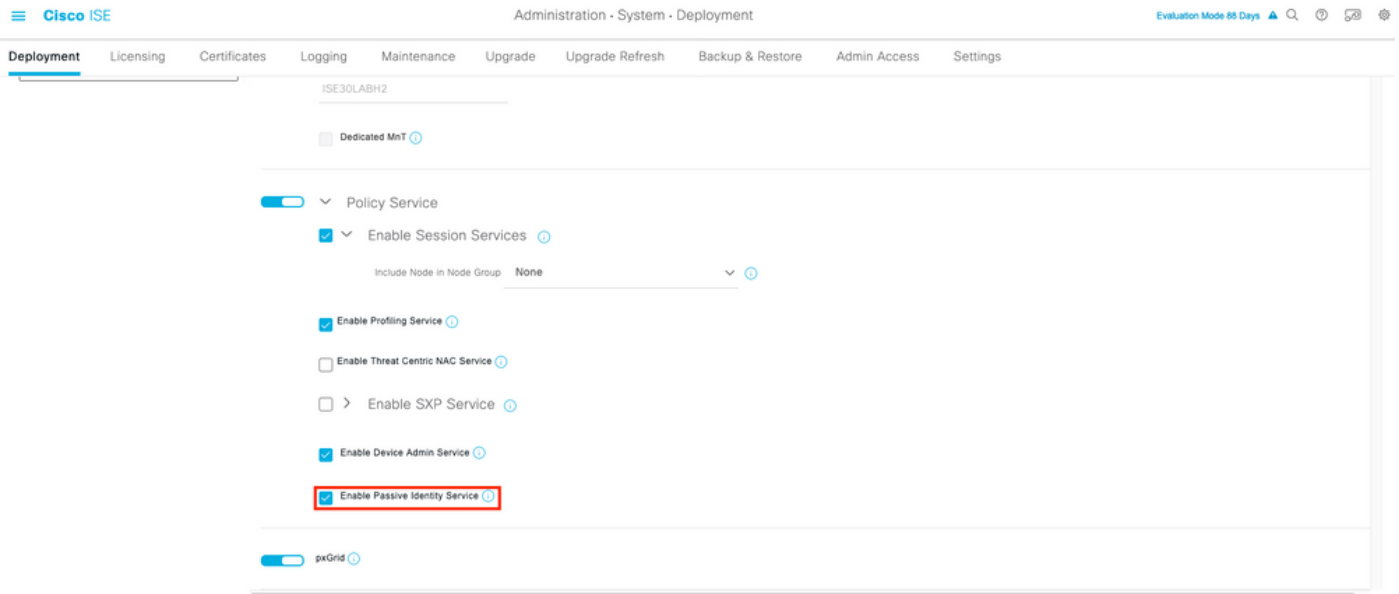
PassiveID Agent-Konfigurationsdatei verstehen

Die Konfigurationsdatei für den PassiveID Agent finden Sie unter **C:\Program Files (x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config**. Die Konfigurationsdatei enthält den Inhalt, der hier angezeigt wird:

Überprüfung

Überprüfen Sie die PassiveID-Services auf der ISE.

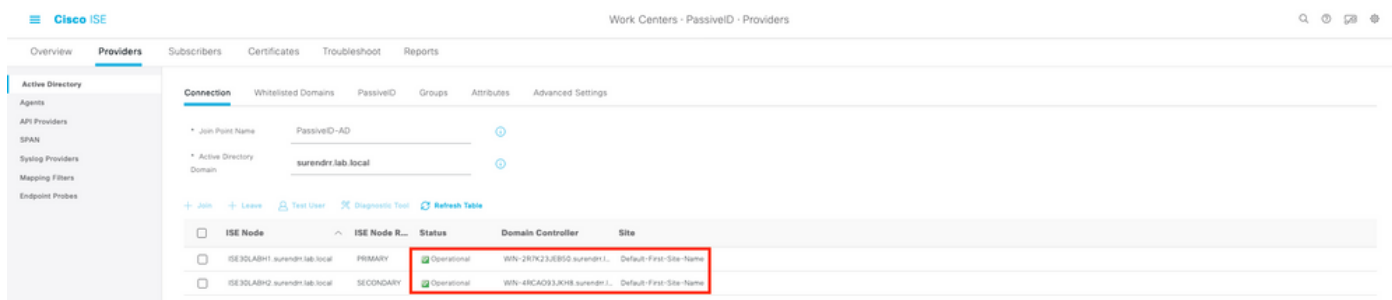
1. Überprüfen Sie, ob der PassiveID-Dienst auf der GUI aktiviert ist und außerdem mit dem Befehl `show application status ise` (Anwendungsstatus anzeigen) in der CLI der ISE markiert ist.



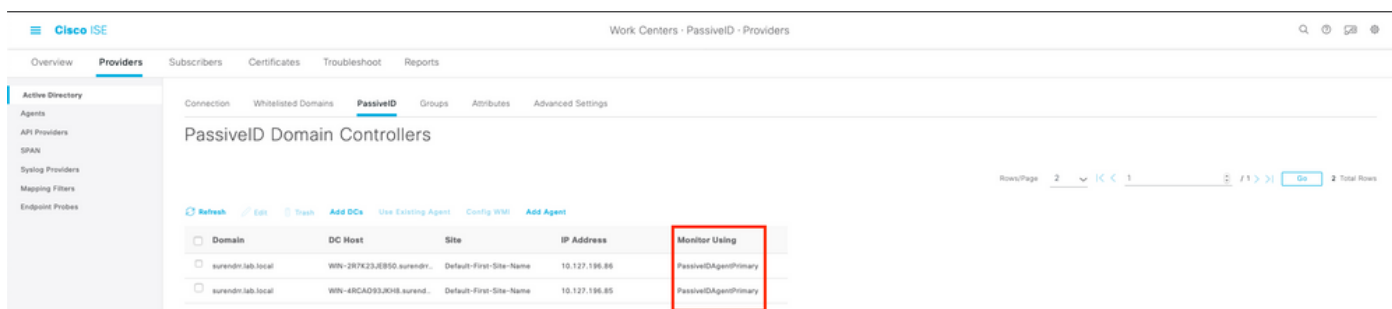
```
ISE PROCESS NAME STATE PROCESS ID
-----
Database Listener running 129052
Database Server running 108 PROCESSES
Application Server running 9830
Profiler Database running 5127
ISE Indexing Engine running 13361
AD Connector running 20609
M&T Session Database running 4915
M&T Log Processor running 10041
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

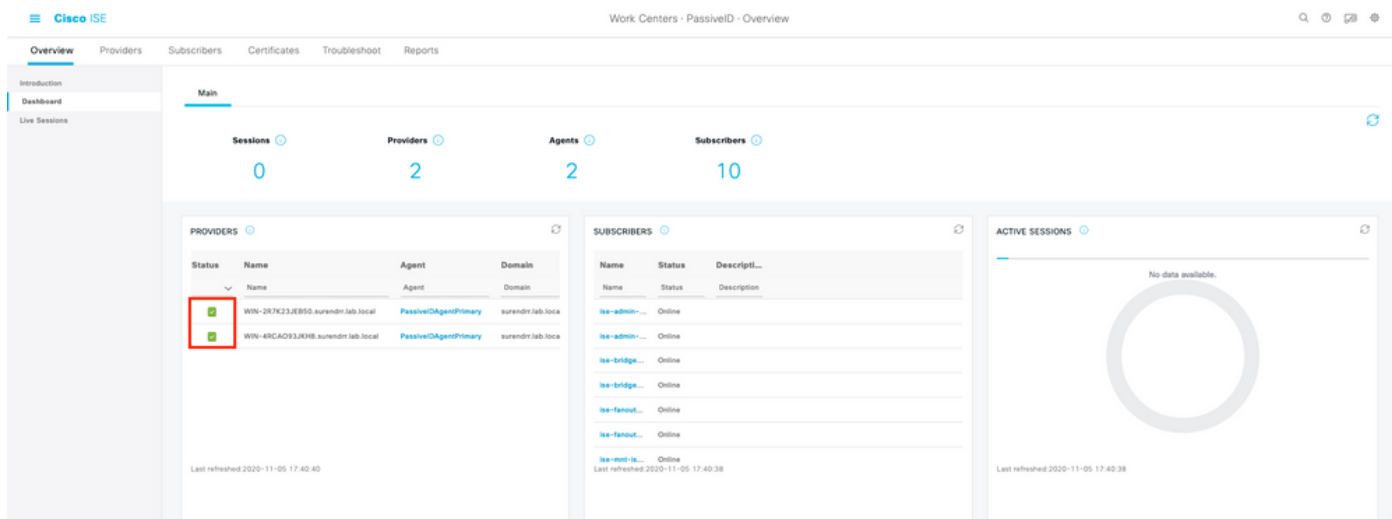
2. Überprüfen Sie, ob der ISE Active Directory-Provider mit den Domänen-Controllern in **Work Centers > PassiveID > Providers > Active Directory > Connection** verbunden ist.



3. Überprüfen Sie, ob die erforderlichen Domänen-Controller vom Agent in **Work Centers > PassiveID > Providers > Active Directory > PassiveID** überwacht werden.



4. Überprüfen Sie, ob der Status der zu überwachenden Domänencontroller aktiv ist, d. h. auf dem Dashboard in **Work Centers > PassiveID > Overview > Dashboard** grün markiert ist.



5. Überprüfen Sie, ob Live-Sitzungen aufgefüllt werden, wenn eine Windows-Anmeldung beim Domänencontroller in **Work Centers > PassiveID > Overview > Live Sessions** registriert ist.

Cisco ISE Work Centers - PassiveID - Overview

Overview Providers Subscribers Certificates Troubleshoot Reports

Introduction Dashboard Live Sessions

Refresh Never Show Latest 20 records Within Last 24 hours Filter

Initiated	Updated	Session Sta...	Provider	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture St...	Security G...	Server	Auth M...	Authentic
Nov 05, 2020 05:59:31.925 PM	Nov 05, 2020 05:59:31.9...	Authenticated	Agent	Show Actions	10.127.194.85	Administrator	10.127.194.85	Endpoint Profile	Posture Status	Security Gro...	ISE30LAB11	Auth Meth	Authentic

Last Updated: Thu Nov 05 2020 18:01:03 GMT+05:30 (India Standard Time) Records Shown: 1

Überprüfen Sie die Agent-Dienste auf Windows Server.

1. Überprüfen Sie den ISEPICAgent-Dienst auf dem Server, auf dem PIC Agent installiert ist.

Task Manager

File Options View

Processes Performance Users Details Services

Name	PID	Description	Status	Group
ISEPICAgent	9392	Cisco ISE PassiveID Agent	Running	
WSearch		Windows Search	Stopped	
wmiApSrv		WMI Performance Adapter	Stopped	
WinDefend	3052	Windows Defender Service	Running	
WIDWriter	2044	Windows Internal Database VSS Writer	Running	
WdNisSvc		Windows Defender Network Inspecti...	Stopped	
VSS		Volume Shadow Copy	Stopped	
VMwareCAFManagementA...		VMware CAF Management Agent Se...	Stopped	
VMwareCAFCommAmqpLi...		VMware CAF AMQP Communicatio...	Stopped	
vmvss		VMware Snapshot Provider	Stopped	
VMTools	2484	VMware Tools	Running	
VGAuthService	2480	VMware Alias Manager and Ticket S...	Running	
vds	4236	Virtual Disk	Running	
VaultSvc	724	Credential Manager	Running	
UIODetect		Interactive Services Detection	Stopped	
UevAgentService		User Experience Virtualization Service	Stopped	
TrustedInstaller		Windows Modules Installer	Stopped	
TieringEngineService		Storage Tiers Management	Stopped	
SQLWriter	3148	SQL Server VSS Writer	Running	
SQLTELEMETRY\$SQLEXPRESS	4884	SQL Server CEIP service (SQLEXPRESS)	Running	
SQLBrowser		SQL Server Browser	Stopped	
SQLAgent\$SQLEXPRESS		SQL Server Agent (SQLEXPRESS)	Stopped	
snpsvc		Software Protection	Stopped	

Fewer details | Open Services