

# Een passieve ID-agent voor EVT-gebaseerde Identity Services Engine

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Noodzaak van een nieuw protocol](#)

[Voordelen van het gebruik van MS-EVEN6](#)

[Hoge beschikbaarheid](#)

[schaalbaarheid](#)

[Schaal testarchitectuur](#)

[Historische gebeurtenissen Query](#)

[Minder verwerking overhead](#)

[Configureren](#)

[Connectiviteitsdiagram](#)

[Configuraties](#)

[ISE configureren voor PassiveID Agent](#)

[Configuratie-bestand van Passive ID Agent begrijpen](#)

[Verifiëren](#)

[Controleer passieve ID-services op ISE](#)

[Controleer de Agent-services op Windows-server](#)

## Inleiding

Dit document beschrijft de nieuwe ISE Passive Identity Connector (ISE-PIC) Agent die is geïntroduceerd in de ISE 3.0 versie, de voordelen en de configuratie van deze agent op ISE. ISE Passive Identity Connector is een integraal onderdeel geworden van de oplossing voor Identity Firewall met behulp van Cisco FirePower Management Center.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco-identiteitsbeheer
- MS-RPC-, WMI-protocollen
- Active Directory-beheer

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine versie 3.0 en hoger
- Microsoft Windows Server 2016 - standaard

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Noodzaak van een nieuw protocol

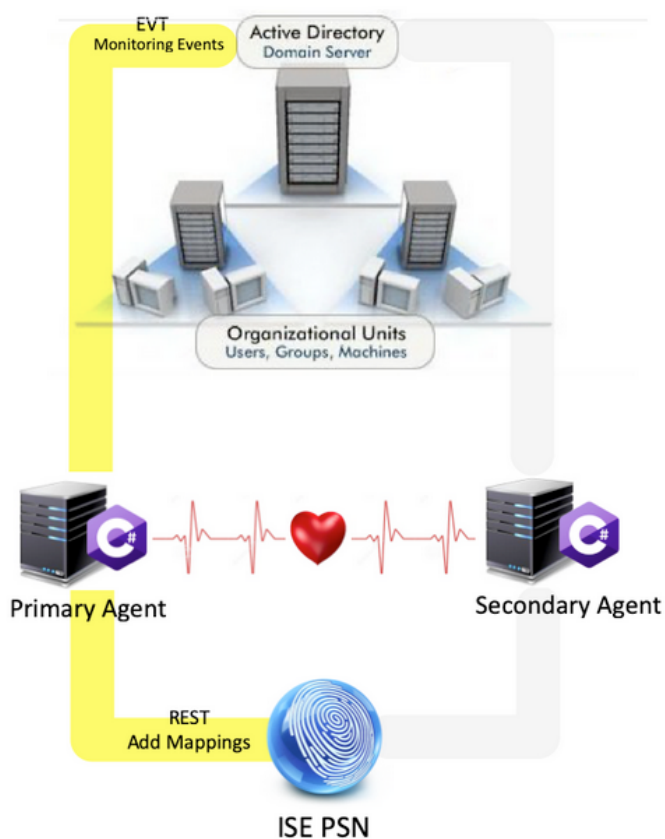
Met de optie Passive Identity (Passive ID) van ISE wordt een aantal belangrijke gebruikgevallen ondersteund, zoals een op identiteit gebaseerde firewall, EasyConnect, enz. Deze optie hangt af van de mogelijkheid om gebruikers te controleren die loggen in Active Directory Domain Controllers en hun gebruikersnaam en IP-adressen te leren. Het huidige hoofdprotocol dat we gebruiken om de Domain Controllers te controleren is WMI. Het is echter moeilijk/invasief om aan te passen, heeft een prestatiegerelateerde impact op zowel klanten als servers en soms is de vertraging extreem groot bij het zien van openings van een aanmelding gebeurtenissen in geschaalde implementaties. Na grondig onderzoek en alternatieve manieren om de informatie te krijgen die nodig is voor Passive Identity Services, werd besloten een alternatief protocol - gekend als de EVT of Eventing API, dat efficiënter is in de behandeling van deze use zaak. Het wordt soms **MS-EVEN6** genoemd, ook wel bekend als "**Eventing Remote Protocol**", dat het onderliggende RPC-gebaseerde protocol op de draad is.

## Voordelen van het gebruik van MS-EVEN6

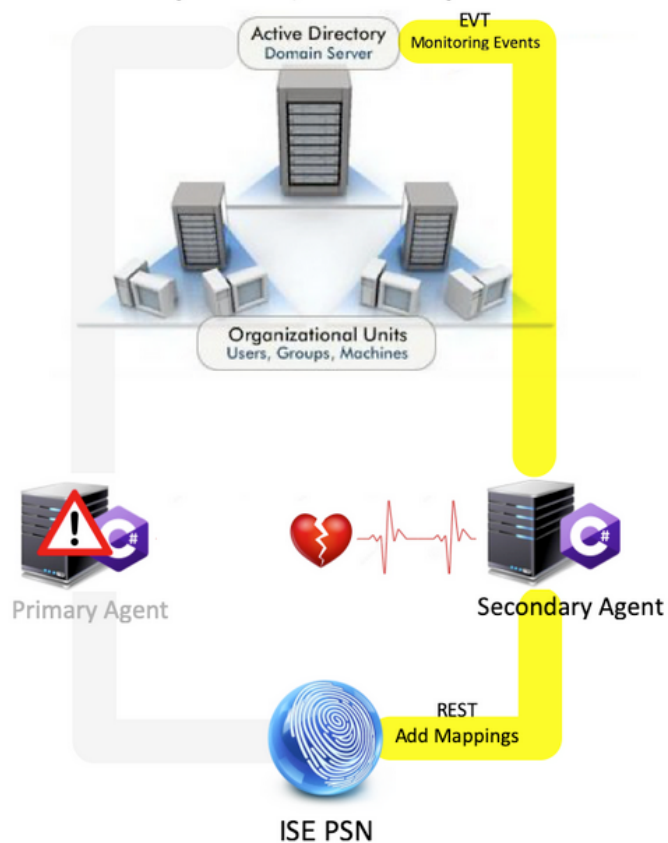
### Hoge beschikbaarheid

De oorspronkelijke agent had geen optie voor hoge beschikbaarheid en als het nodig is om onderhoud uit te voeren op de server waar de agent actief was of een storing had, zouden openingsgebeurtenissen gemist worden en functies zoals Identity-Based Firewall zouden een verlies van gegevens tijdens deze periode zien. Dit is een van de belangrijkste zorgen met het gebruik van ISE PIC Agent vóór deze release. ISE gebruikt UDP Port 9095 om hartslagen tussen de agents uit te wisselen.

## Primary Active, Secondary Passive



## Primary Failure, Secondary Active

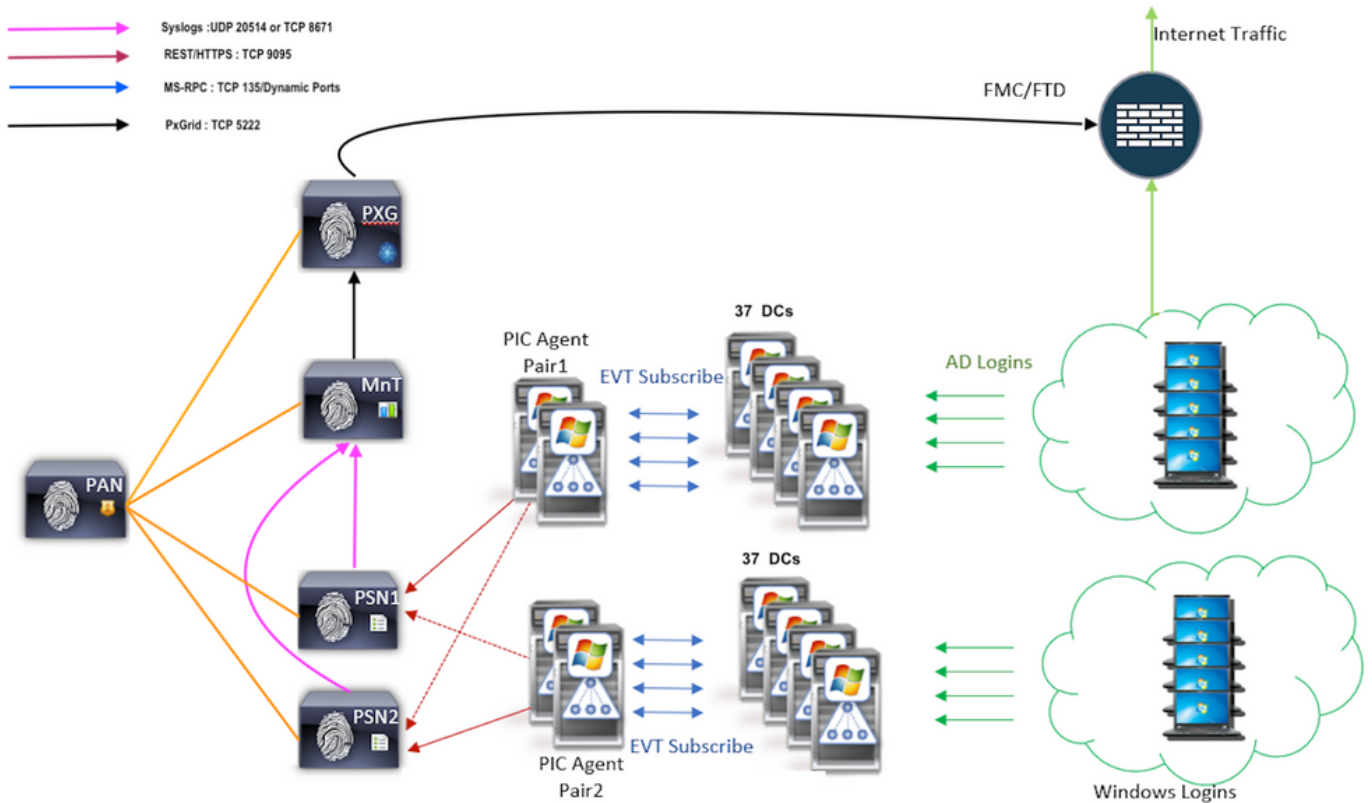


## schaalbaarheid

De nieuwe agent biedt betere ondersteuning met verhoogde schaalgetallen voor een ondersteund aantal domeincontrollers en het aantal gebeurtenissen dat deze kunnen verwerken. Hier zijn de schaalnummers die getest werden:

- Maximum aantal gecontroleerde domeincontrollers (met 2 paren agents): 74
- Maximum aantal geteste Mappings/gebeurtenissen: 292.000 (3.950 gebeurtenissen per DC)
- Maximale geteste TPS: 500

## Schaal testarchitectuur



## Historische gebeurtenissen Query

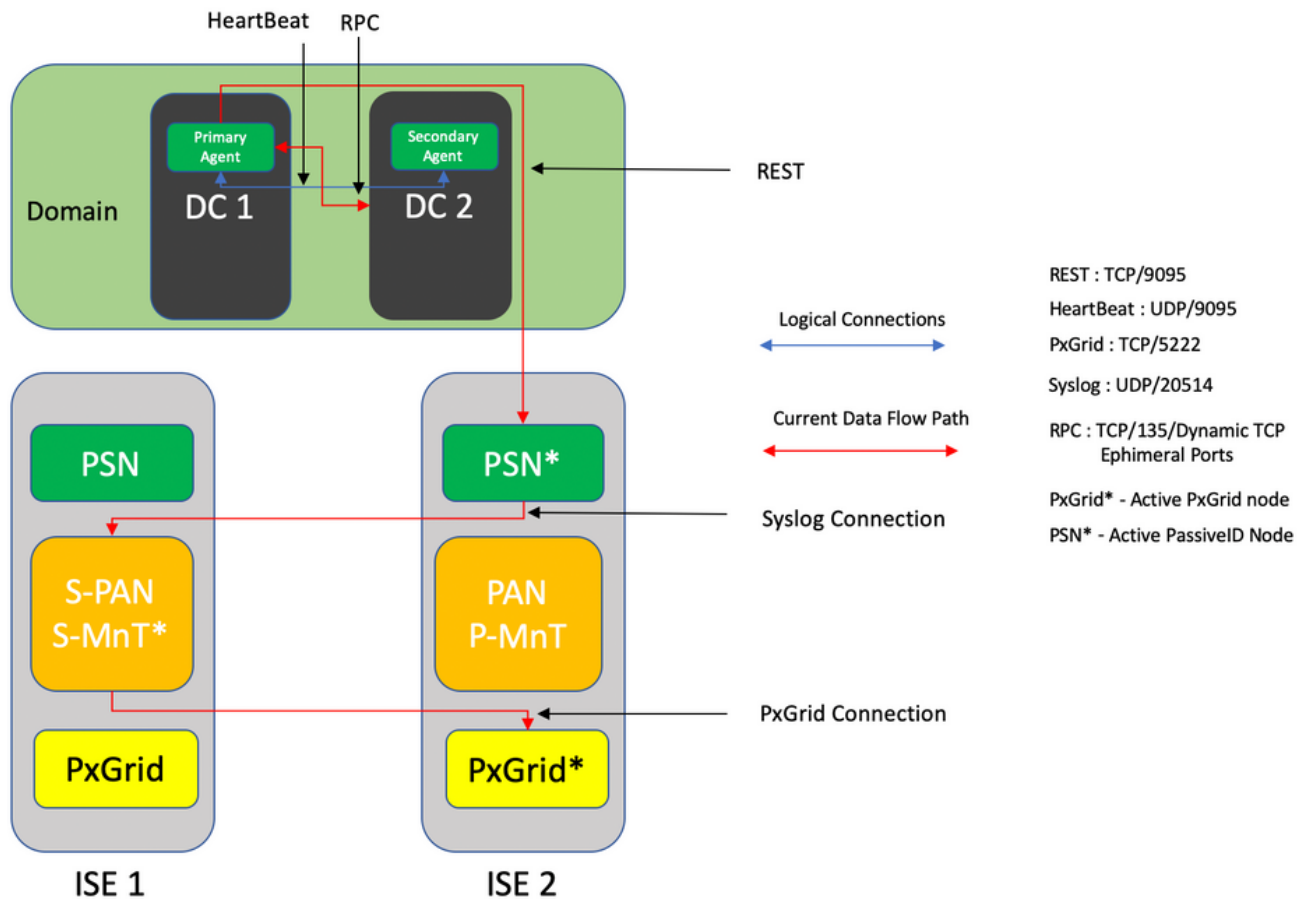
In het geval van failover of in het geval van een service start wordt uitgevoerd voor de PIC-agent, om er zeker van te zijn dat er geen gegevens verloren gaan, worden gebeurtenissen die voor de voorbije gegeven hoeveelheid tijd gegenereerd en opnieuw naar de PSN-knooppunten verzonden. Standaard wordt 60 seconden van gebeurtenissen uit het verleden vanaf het begin van de service door de ISE gevraagd om enig verlies aan gegevens tijdens het serviceverlies te negeren.

## Minder verwerking overhead

Anders dan WMI, dat CPU-intensief is bij grote schaal of zware belasting, verbruikt EVT niet zoveel middelen als WMI. Uit de schaaltests bleek dat de vragen met het gebruik van EVT veel beter werden beantwoord.

## Configureren

### Connectiviteitsdiagram

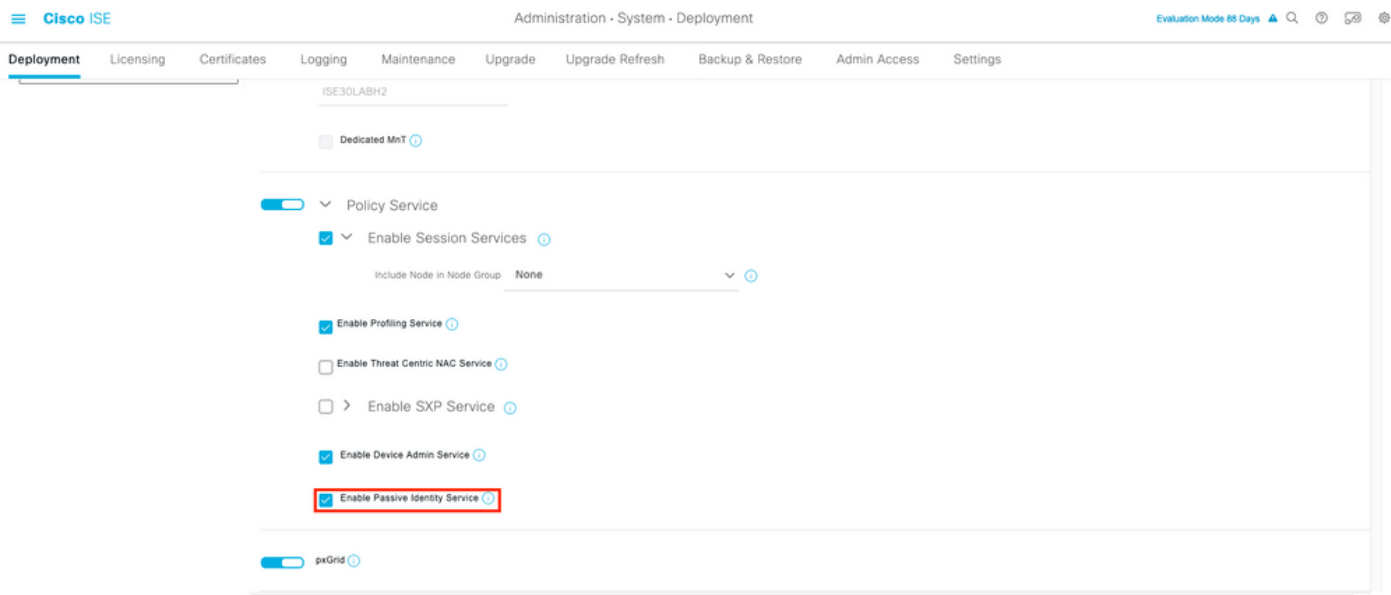


## Configuraties

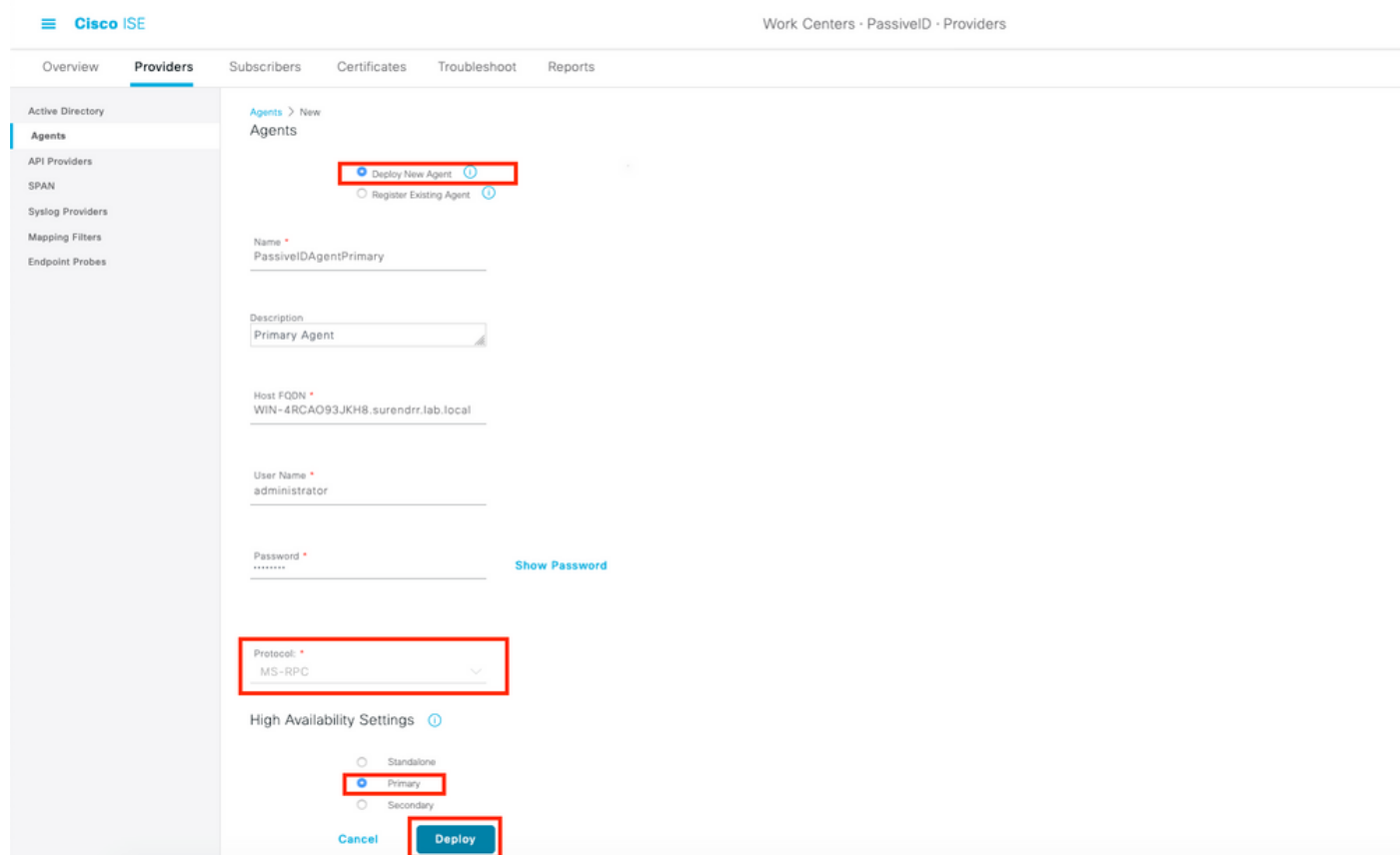
### ISE configureren voor PassiveID Agent

Om de PassiveID-services te kunnen configureren hebt u de Passive Identity Services ingeschakeld op minimaal één Policy Service Node (PSN). Er kunnen maximaal twee knooppunten worden gebruikt voor passieve identiteitservices die in actieve/standby modus werken. ISE moet ook worden aangesloten bij een Active Directory-domein en alleen de domeincontrollers die in dat domein aanwezig zijn, kunnen worden gecontroleerd door agents die op ISE zijn geconfigureerd. Raadpleeg de [integratiegids](#) van de [actieve map](#) om zich bij ISE aan te sluiten op een [domein](#) van de actieve map.

Navigeren in op **Beheer > Systeem > Plaatsing > [Kies een PSN] > Bewerken** om passieve Identity Services zoals hier getoond wordt in te schakelen:



Navigatie in naar **werkcentra > PassiveID > Leveranciers > Middelen > Toevoegen** om een nieuwe Agent in te stellen zoals hier wordt getoond:

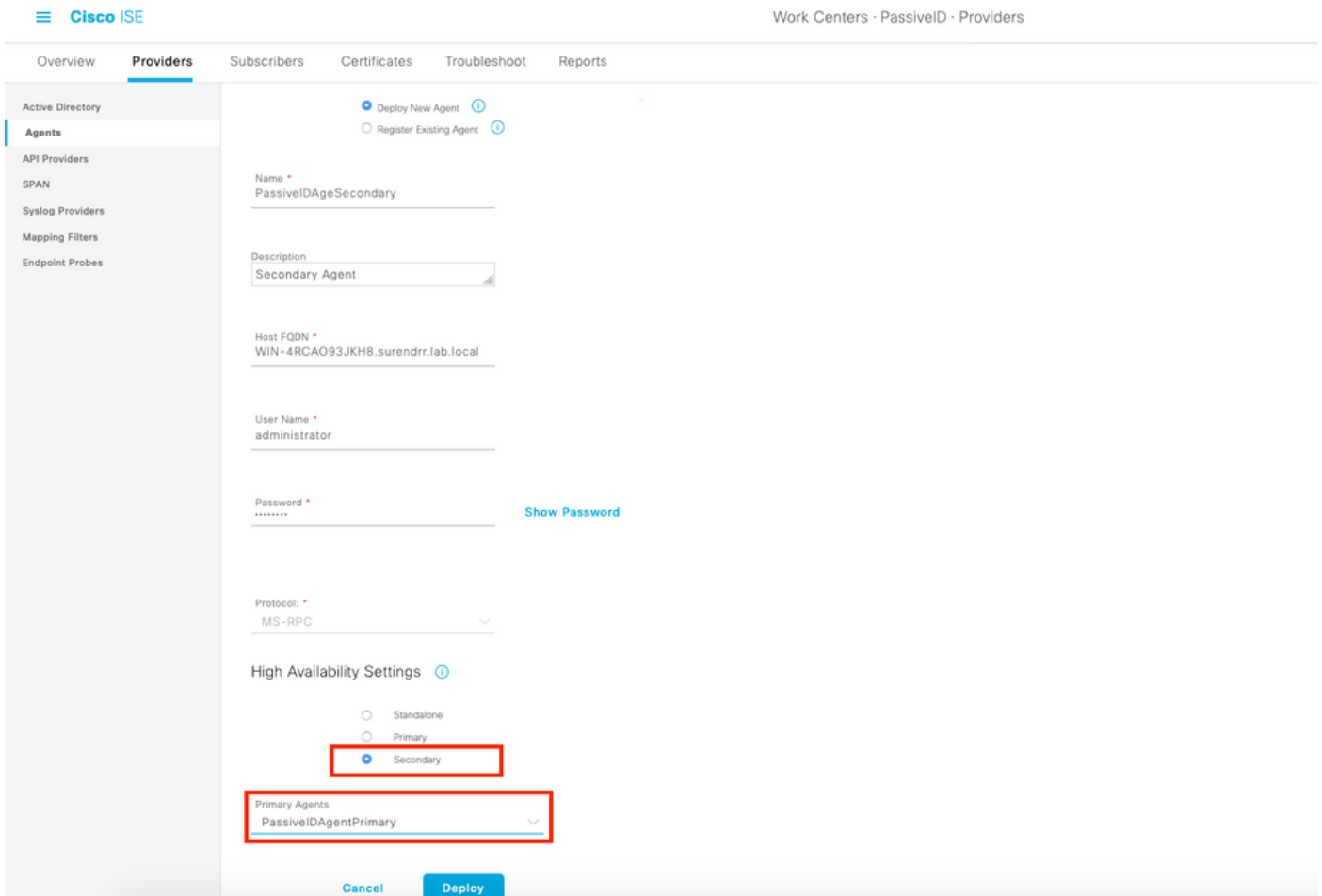


**Opmerking:** 1. Als de agent volgens plan door ISE op de Domain Controller zal worden geïnstalleerd, moet de hier gebruikte account voldoende rechten hebben om een programma te installeren en op de server uit te voeren die in het Host FQDN-veld wordt vermeld. Host FQDN hier kan dat van een aangesloten server zijn in plaats van een domeincontroller.

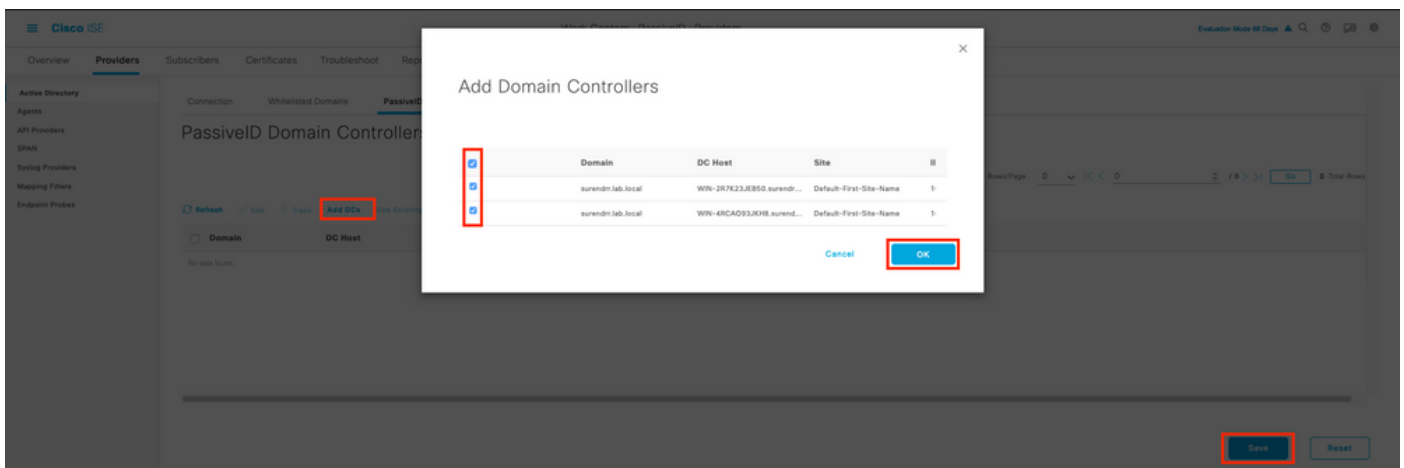
2. Als een agent reeds handmatig of vanaf een vorige plaatsing vanuit de ISE, met MSRPC, is de permissie en de configuraties die aan de kant Actieve Map of Windows zijde nodig zijn minder geïnstalleerd dan WMI, het andere protocol (en de enige beschikbare vóór

3.0) dat door PIC agenten gebruikt wordt. De gebruikersaccount die in dit geval wordt gebruikt, kan een reguliere domeinaccount zijn die deel uitmaakt van de **groep Event Log Reader**. Kies **Bestaande Agent registreren** en gebruik deze accountgegevens om de agent te registreren die handmatig op de domeincontrollers is geïnstalleerd.

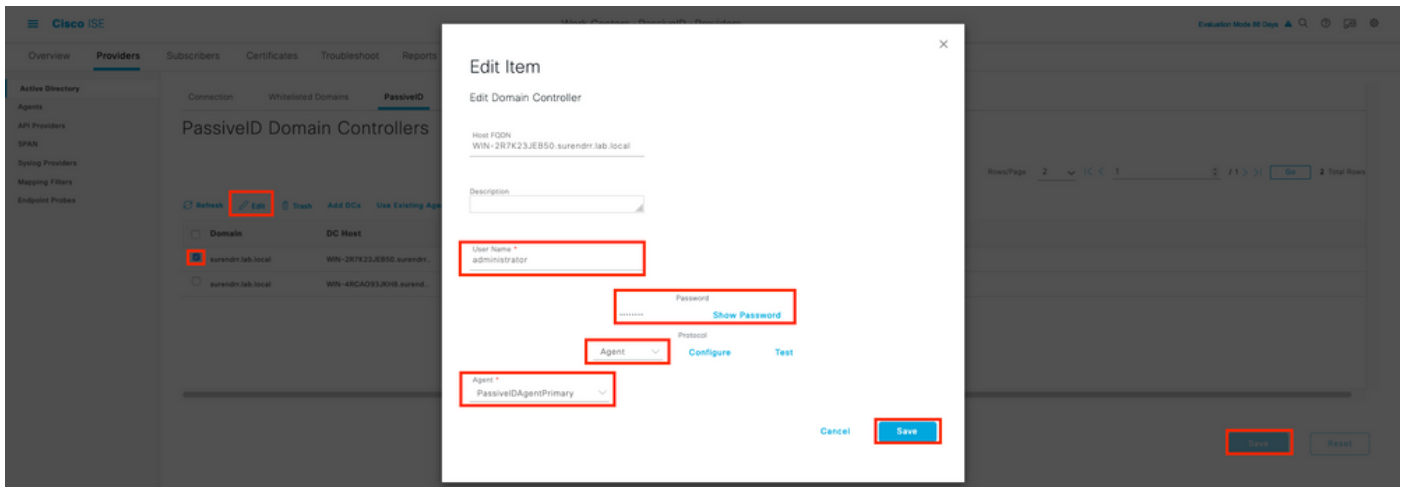
Na een succesvolle plaatsing, moet u een andere agent op een andere server vormen en toevoegen als secundaire agent en dan zijn primaire peer zoals getoond in dit beeld.



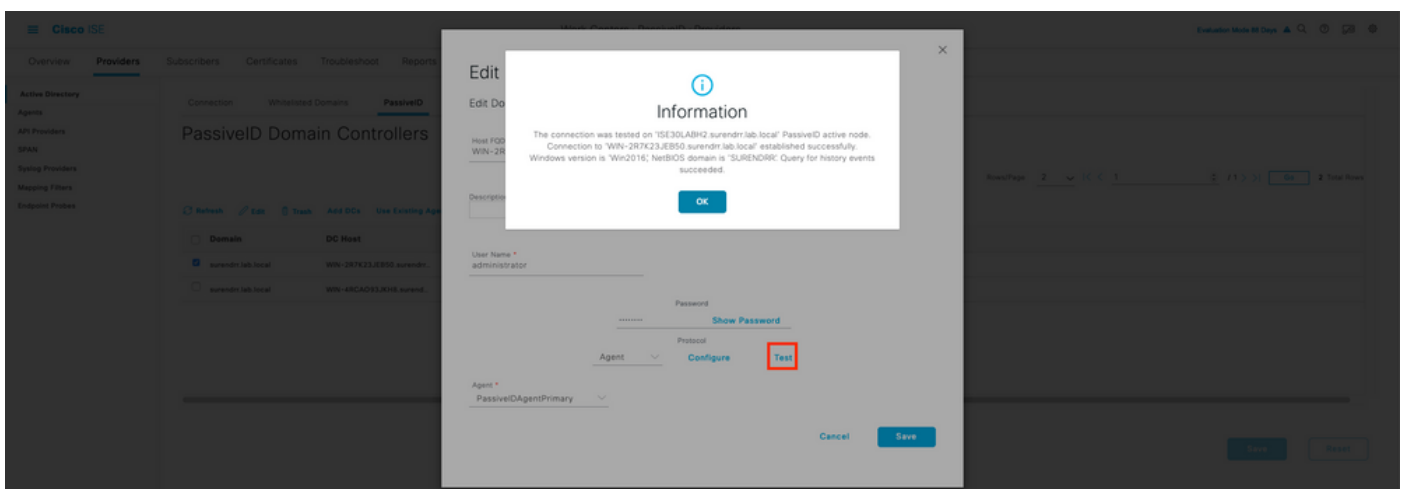
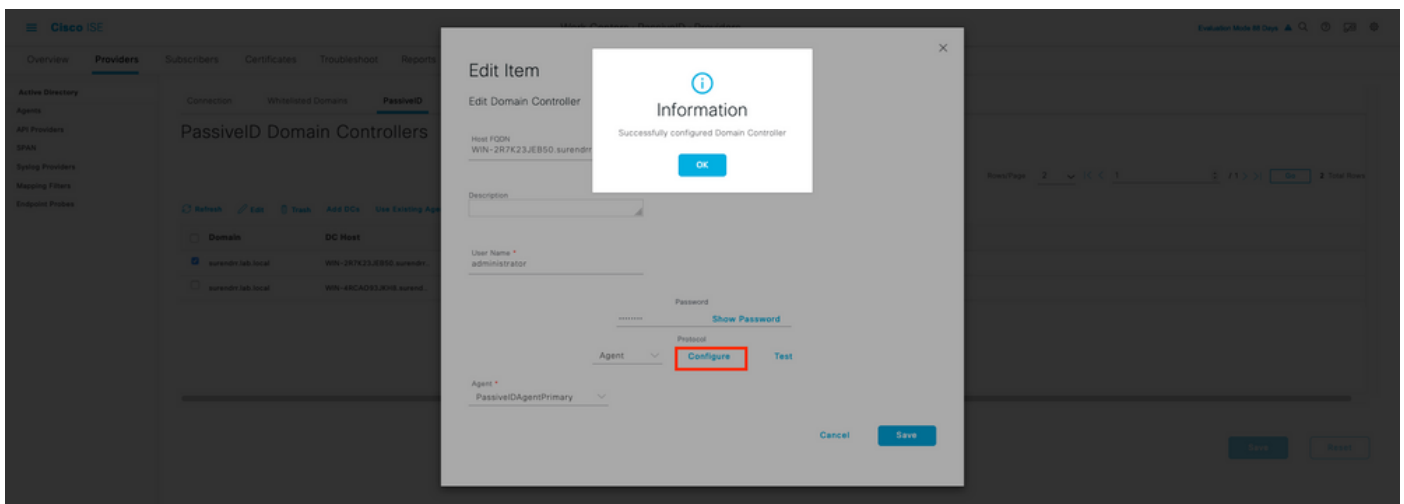
Om de domeincontrollers met de agents te bewaken, navigeer naar **werkcentra > PassiveID > Providers > Actieve map > [Klik op het punt om te voegen] > Passive ID**. Klik op **Add DC's** en kies de domeincontrollers waarvan de User-IP mapping/events worden opgehaald en klik op **OK** en klik vervolgens op **Save** om de wijzigingen op te slaan, zoals in deze afbeelding wordt getoond.



Om de agenten te specificeren die zouden moeten worden gebruikt om de gebeurtenissen van te herstellen, navigeer naar **Werkcentra > PassiveID > Providers > Actieve Map > [Klik op het Punt van de Samenvoegen] > PassiveID**. Kies de domeincontrollers en klik op **Bewerken**. Voer de *gebruikersnaam* en het *wachtwoord in*. Klik op **Agent** en **Sla** het dialoogvenster **op**. Klik op **Opslaan** op het tabblad PassiveID om de configuratie te voltooien.



U kunt controleren of de configuratie correct is toegepast met behulp van de knoppen **Configureren** en **Test**, zoals in de afbeeldingen hier wordt weergegeven:



## Configuratie-bestand van Passive ID Agent begrijpen

Het configuratiebestand van PassiveID Agent is te vinden op **C:\Program Files (x86)\Cisco\Cisco**

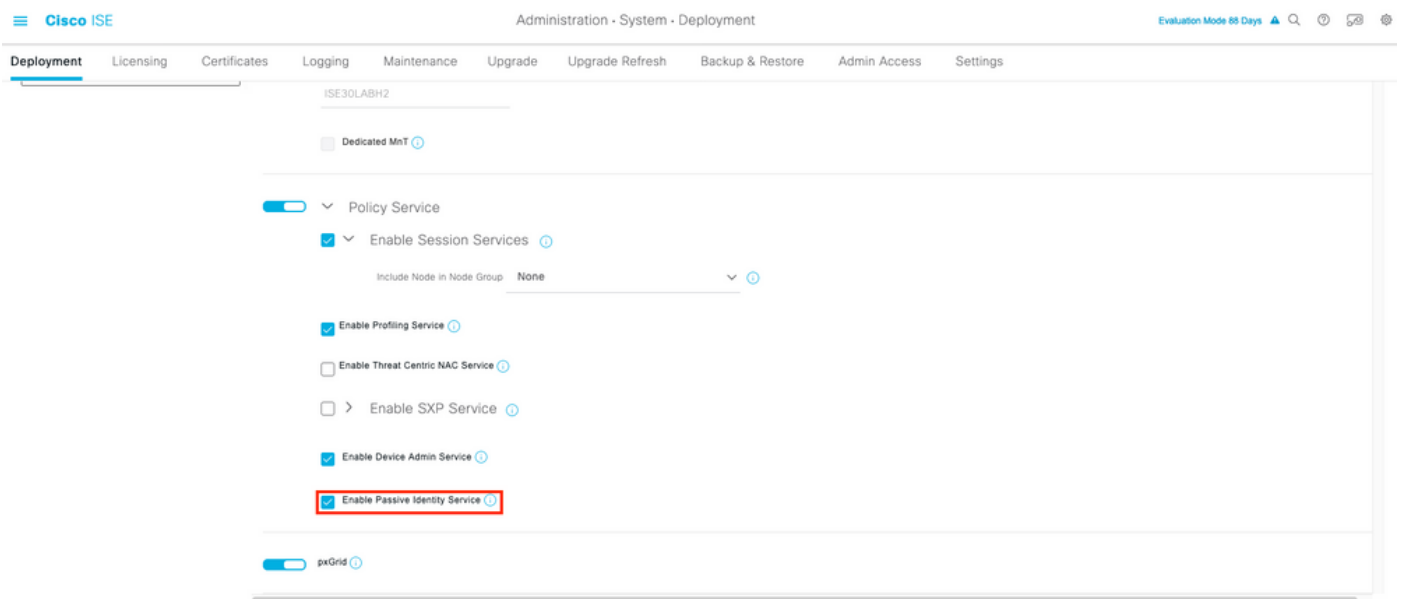


ISE PassiveID Agent\PICAgent.exe.. Het configuratiebestand heeft content die hier wordt getoond:

## Verifiëren

### Controleer passieve ID-services op ISE

1. Controleer of de PassiveID-service op de GUI is ingeschakeld en ook wordt aangeduid hoe de toepassingsstatus van de opdracht op de CLI van de ISE wordt weergegeven.



```
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. Controleer of ISE Active Directory provider is verbonden met de domeincontrollers bij **Workcenters > PassivID > Providers > Active Directory > Connection.**

ISE Node	ISE Node R...	Status	Domain Controller	Site
<input type="checkbox"/>	ISE3LABH1 surendr.lab.local	Operational	WIN-287K23JEB50 surendr.l...	Default-First-Site-Name
<input type="checkbox"/>	ISE3LABH2 surendr.lab.local	Operational	WIN-48CA093JKH8 surendr.l...	Default-First-Site-Name

3. Controleer of de vereiste domeincontrollers door de agent worden gecontroleerd op het werk > **PassivID > Providers > Active Directory > PassivID.**

Domain	DC Host	Site	IP Address	Monitor Using	
<input type="checkbox"/>	surendr.lab.local	WIN-287K23JEB50 surendr...	Default-First-Site-Name	10.127.196.85	PassiveIDAgentPrimary
<input type="checkbox"/>	surendr.lab.local	WIN-48CA093JKH8.surend...	Default-First-Site-Name	10.127.196.85	PassiveIDAgentPrimary

4. Controleer of de status van de te bewaken domeincontrollers hoger is, d.w.z. dat deze op het dashboard zijn aangegeven op **de werkstations > PassivID > Overzicht > Dashboard.**

Status	Name	Agent	Domain
<input type="checkbox"/>	WIN-287K23JEB50 surendr.lab.local	PassiveIDAgentPrimary	surendr.lab.local
<input type="checkbox"/>	WIN-48CA093JKH8.surendr.lab.local	PassiveIDAgentPrimary	surendr.lab.local

5. Controleer of er live sessies worden ingevuld wanneer een aanmelding van een Windows-verbinding is geregistreerd op de domeincontroller in **Workcenters > PassivID > Overzicht > Live Sessies.**

Cisco ISE Work Centers - PassiveID - Overview

Overview Providers Subscribers Certificates Troubleshoot Reports

Refresh Never Show Latest 20 records Within Last 24 hours

Refresh Export To 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 PM	Nov 05, 2020 05:59:31 S...	Authenticated	Agent	Show Actions	10.127.194.85	Administrator	10.127.194.85	Endpoint Profile	Posture Status	Security Gro...	ISE30LAB1	Auth Meth	Authentic

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

## Controleer de Agent-services op Windows-server

1. Controleer de ISEPICAgent service op de server waar PIC Agent is geïnstalleerd.

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