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 gebruiksgevallen 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.



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 identiteitsservices 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:

≡ Cisco IS	SE				Evaluation Mode 88 Days	Q	0	2						
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Upgrade Refresh	Backup & Restore	Admin Access	Settings					
			ISE30LA	8H2										
			Dedic	ated MnT 🕠										
		-	⊃ ~ Pol	licy Service Enable Session										
				Include Node in Node Group None 🗸 🛈										
			C Enable	e Profiling Service 🕕										
			Enable	e Threat Centric NAC Se	rvice 🕕									
			\Box >	Enable SXP Ser	vice 🕕									
			Enabl	e Device Admin Service	0									
			Enabl	e Passive Identity Servic	* 🛈									
		_	pxGrid 🕕											

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

≡ Cisco	ISE	Work Centers · PassiveID · Providers
Overview	Providers	Subscribers Certificates Troubleshoot Reports
Active Directory		Agents > New
Agents		Agents
API Providers		
SPAN		Depoy term Agent
Syslog Providers		
Mapping Filters		Name *
Endpoint Probes		PassiveIDAgentPrimary
		Description
		Primary Agent
		Host FQON *
		WIN-4RCA093JKH8.surendrr.tab.local
		User Name *
		administrator
		Desenant 1
		Show Password
		Protocol. *
		MS-RPC V
		High Availability Settings 0
		Secondary
		Canada Dantas
		Carler Depty

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.

Overview Providers Subscribers Certificates Troubleshoot Reports Active Directory Image: Certificates Image: Certificates Image: Certificates Image: Certificates Apents Image: Certificates Image: Certificates Image: Certificates Image: Certificates Apiters Image: Certificates Image: Certificates Image: Certificates Image: Certificates Systeg Providers Image: Certificates Image: Certificates Image: Certificates Image: Certificates Systeg Providers Image: Certificates Image: Certificates Image: Certificates Image: Certificates Systeg Providers Image: Certificates Image: Certificates Image: Certificates Image: Certificates Systeg Providers Image: Certificates Image: Certificates Image: Certificates Image: Certificates Systeg Providers Image: Certificates Image: Certificates Image: Certificates Image: Certificates Bescription Image: Certificates Image: Certificates Image: Certificates Image: Certificates Hoat FQDN * Image: Certificates Image: Certificates Image: Certificates Image: Certificates	
Active Directory Agents Agents Parviders Parviders PassiveIDAgeSecondary PassiveIDAgeSecondary Bitters Endpoint Probes Bescription Secondary Agent Hast FQDN * WIN-4RCAO93JKH8.surendrr.lab.local	
Agents Register Existing Agent API Providers SPAN Systog Providers Mapping Filters Endpoint Probes Description Secondary Agent	
API Providers SPAN Syslog Providers BassiveIDAgeSecondary Syslog Providers BassiveIDAgeSecondary Bescription Endpoint Probes Bescription Host FQDN * WIN-4RCAO93JKH8.surendrr.lab.local	
SPAN Name * PassiveIDAgeSecondary Syslog Providers Mapping Fitters Endpoint Probes Description Secondary Agent Host FQDN * WIN-4RCAO93JKH8.surendrr.lab.local	
Syslog Providers Mapping Filters Endpoint Probes Host FQDN * WIN-4RCAO93JKH8.surendrr.lab.local	
Mapping Filters Endpoint Probes Description Secondary Agent Host FQDN * WIN-4RCAO93JKH8.surendrr.lab.local	
Endpoint Probes Description Secondary Agent Host FQDN * WIN-4RCAO93JKH8.surendrr.lab.local	
Host FQDN * WIN-4RCAO93JKH8.surendrr.lab.local	
Host FQDN * WIN-4RCAO93JKH8.surendrr.lab.local	
Host FQDN * WIN-4RCAO93JKH8.surendrr.lab.local	
WIN-4RCAO93JKH8.surendrr.lab.local	
User Name *	
administrator	
Password *	
Show Password	
Protocol: *	
MS-RPC V	
High Availability Settings 0	
O Standalana	
O Primary	
 Secondary 	
Primary Agents	
PassiveIDAgentPrimary	
Cancel Deploy	

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.

E Cisco ISE			Nork Contare Developed	h - Dresidere				Evaluation Mode M Days 🔺 Q, 🕐 🗔 🖓
Overview Providers						×		
Active Directory Agents API Providers	Connection Whitelisted Domains Passivell Passivell Domain Controller	Add Domain	Controllers					
SPAN Systog Providers Mapping Filters		0 0	Domain surendm.lab.local	DC Host WN-287K23JE850.surendr	Site Default-First-Site-Name	н.	Roms/Page 0 v < < 0	7.0 > > 00 0 Total Rows
Endpoint Probes	C Referent (2 time) track Add DDs (10 times	0	surendm.lab.local	WIN-4RCA093JKH8.surrend	Default-First-Site-Name	1		
	Domain DC Host				Cancel	ox		
								Save Reset

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.

E Cisco ISE		Work Processor P
Overview Providers		Edit Item
Active Directory Agents	Connection Whitelisted Domains PassiveID	Edit Domain Controller
API Providers SPAN Syslog Providers	PassivelD Domain Controllers	Host FODN WIN-287X23JEB50 surender.lab.local
Mapping Filters Endpoint Probes	🖉 Refresh 🥖 Karr 🕆 Yosh 🛛 Add DCe — Use Existing A	Description
	Domain DC Host	the line t
	surendrr.lab.local WIN-2R7K23,/EB50.surendrr.	Unit hereit a damarate stater
	serender laki Sociel WRV-dRCA053.0018 avende.	Passord See Passord Agent V Passord Agent Configure Test Passord Canfigure Test Cancel Even Cancel Even

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

		Mark Cantors - David all - Droiders	Evaluation Mode M Days 🔺 🔍 🗇 💭 🕀
Overview Providers	Subscribers Certificates Troubleshoot Reports	Edit Item	
Active Directory	Connection Whitelated Domains PassivelD	Edit Domain Controller	
	PassivelD Domain Controllers	Information Successfully configured Domain Controller	
		Hear FOOM WIN-2R7K23JEB50 surendrr	
	🖓 Refresh 🖉 Eds 🔘 Track Add DC+ Use Existing Age		
		User Name *	
	surrendy: Jab. Jocal WN-387X23JE850 surendy:	administrator	
	surender/ab.local WIN-4RCA093,0048.surend.	Passerd	
		Pressool	
		Agent Configure Test	
	_	Agent * PassiveIDAgentPrimary V	
		Cancel Save	
Cisco ISE		No. 6	Contraction Mode MI Days 🔺 Q. 🕐 🗊 🛛
Cisco ISE Overview Providers	Subscribers Certificates Troubleshoot Reports	Edit	Evaluation March 10 Days 🛦 🔍 💿 💭 🗭
Cisco ISE Overview Providers Active Directory Active Directory	Subscribers Certificates Troubleshoot Reports Connaction Whitelete Domain PestietD	Edit (i) East Do Information	towarden Mala II (say & Q, (b) (2))
Cisco ISE Overview Providers Active Directory Agents Althrenders	Subscribers Certificates Troubleshoot Reports Connection Whiteleted Domans PasswerD PassiveID Domain Controllers	Edit Edit Do Information The connection was treated on "ECIOUADHIQ surrent" Allo local" PassiveID active rode.	Konstation Made III Days & Q. O (20)
Cisco ISE Overview Providers Active Diversity Agents Ant Providers Strat Systep Troubles	Subscribers Certificates Troubleshoot Reports Cennection Whitelated Demans PassiveD PassiveID Domain Controllers	Edit Edit Do Information WN-29 WN-2972123280 Aurora Surveyor lab local established successfully Wrdews version is Win2016; IselfIOS dumain is SUBINDEP: Overy for history events Exceeded.	Contradic Mala II Days & Q. (0) [27] (0)
Cisco ISE Overview Providers Active Devisitive Active Devisitive Active A	Subscribers Certificates Troubleshoot Reports Cennection Whitelated Demains PastwerD PassiveID Domain Controllers	Edit Edit Do Information WN-7872 Testing burder to burd Passing active roads. Convection & Win/2015; Natrido Jackard Survey rais board active roads. Convection & Win/2015; Natrido Jackard Survey rais board active roads. Successful Windows version is "Win/2015; Natrido Jackard Survey rais board active roads. Successful	Example Main H Days & Q. (0) [22] (0)
Cisco ISE Overvice Povders Arche Dosstny Arche Annaine Sana Bying Provides Engano Provides	Subscribers Certificates Troubleshoot Reports Connection Whiteleted Domains PastwerD PassiveID Domain Controllers	Edit Edit Do Information WN-787 WN-787 WN-287 Categories Support State Passing State P	2 (1)) <u>(1)</u> 2 (2) (2)
Cisco ISE Overvice Postders Arthe Destay Arthe Destay Arthe Destay Mage Provides Despand Provides	Subscribers Certificates Troubleshoot Reports Connection Whiteleted Domains PastwerD PassiveID Domain Controllers Connection Certificates Controllers Connection Certificates Controllers Connection Certificates Controllers Connection Certificates Controllers Controllers Certificates Controllers C	Edit Edit De Ministra Ministra Descriptor Descriptor Descriptor	Example Main H Tapp & Q, ∅ (20 (20 (20 (20 (20 (20 (20 (20 (20 (20
Cisco ISE Overview Powders Arthue Directione Arthue Directione Arthue Directione Magning Frankets Directione Directione	Subscribers Certificates Troubleshoot Reports Connection Whitefalled Damains Pastwerd PassiveID Domain Controllers Connection	Edit Edit Di Information Ministry Decentors Understand * Statistical document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Windpaty (KetRid) document (b) Call / Resolved active node. Convection is Call / Resolved active node. Convecti	Constant Male III Tapp ▲ Q. (0) [20] (0)
Cisco ISE Overview Powders Artine Directions Artine Directions Artine Directions Magning Providers Directions Directions	Subscribers Certificates Troubleshoot Reports Cernection Whitefalled Demains Pastwerd PassiveID Domain Controllers	Edit Edit Information Ministration Ministratio	Constant Male III Tapp ▲ Q. (0) [20] (0) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
Cisco ISE Overview Postders Antre Dessure Agens Agens Maryon Antre San Overview San Overview San Overview San	Subscribers Certificates Troubleshoot Reports Cernection Whitefaled Demans Passwerd PassiveID Domain Controllers Refer Cart State Act State Des Exercise App Demant Do Heat Do Heat Demant With SINTER 2008 Bareador With Act State 2008 Bareador With Act Act Act Bareador With Act Act Act Bareador With Act Act Bareador Wi	Edit	Constant Hall IN TABLE & Q. (0) [20] (0) 2. (1) > () (0) 2. hold have
Circo ISE Derrich Payders Arter Ar	Subscribers Certificates Troubleshoot Reports Cernection Whitefaled Domains Passweld PassiveID Domain Controllers Balands 2 East 5 tasks Act Dis Use fronting Age Demain DC Heat Domain DC Heat Demain D	Edit Edit Di Difformation Window version is "Windows version is "USD (ULU) Summarized local" PassiveD active rode. Conceptor Decorer D	Constant Markel M Tage & Q. (0) [20] (0)
Circo SE Donnon Anto Boestry Anto Boestry Anto Boestry Man Anto Boestry Ban Ban Ban Ban Ban Ban Ban Ban Ban Ban	Subscribers Certificates Toubleshoot Reports Connection Whitelebel Domain Controllers PassiveID Domain Controllers Connection Controllers Controllers Controllers Controllers Controllers Contro	Edit En De Winnard W Winnard W Winnard Winnard W Winnard W Winnard Winnard Winnard Winnard W Winnard W	Constant Made II (Japp & Q. () () () () ()
Circo ISE Denrice Poyders Artes Descruy Artes Descruy Arte	Subscribers Certificates Troubleshoot Reports Connection Whitelevel Domain Controllers PassiveID Domain Controllers © Britesh 2 Ser © Task Add Dis Use Excelling Age © Domain Dis Host Use Excelling Age © Domain Dis Host Use Excelling Age © Domain Dis Host Use Excelling Age	Edit Encode Image: Construction of the state of th	
Circo ISE Denrice Poyders Artes Denstry Artes Denstry Martin Martin Martin Martin Circo ISE Artes Denstry Circo ISE	Subscribers Certificates Troubleshoot Reports Connection Whitestored Domain Controllers PassiveID Domain Controllers PassiveID Domain Controllers PassiveII Domain OC Heat Subscribe Ide Idea Wei-20722328388 aurente Wei-2072338988 aurente		Control Mail III Days & Q Image: The second secon

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**.

≡ Cisco IS	SE		Administration - System - Deployment									ର ଡ	50	4
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Upgrade Refresh	Backup & Restore	Admin Access	Settings					
			ISE30LA	BH2										
			Dedic	ated MnT 🕡										
		-	🗖 🗸 Po	licy Service										
			~	Z Y Enable Session Services ()										
				Include Node in Node	Group None		× 0							
			C Enable	e Profiling Service 🕕										
			Enable	e Threat Centric NAC Se	rvice 🕕									
			\Box >	Enable SXP Ser	vice 🕕									
			Enable	le Device Admin Service	0									
			Enabl	le Passive Identity Servi	ce 🕕									
		-	pxGrid 🕢											

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 > PassiveID > Providers > Active Directory > Connection.

E Cisco ISE	Work Centers - PassiveID - Providers	
Overview Providers	Subscribers Centificates Troubleshoot Reports	
Active Directory Agents	Connection Whitelated Domains PassiveID Groups Attributes Advanced Settings	
API Providers SPAN	• Join Point Name PassivaD-AD ()	
Syslog Providers Mapping Filters	* Active Directory surrendri Aab Jocal .	
Endpoint Probes	+ John + Leave 🚊 Test Uner 🗶 Disposeds Test 🕃 Referent Table	
	ISE Node ^ ISE Node R_ Status Domain Controller Site	
	SESSLAHL.uvendrika.local PRMARY @Oversional WIN-28/N23/E9/G avendrit Overal-First: Sta-Name	
	St320ABQ zvendnikt local SECONDAVY 20pertional WhiteRCA033.008 zvendnil. Cvfaul-Final-Star-Name	

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

			Work C	Centers · PassiveID · Provi
Subscribers Certificates	Troubleshoot Report	3		
Connection Whitelisted	Domains PassivelD Gro	ups Attributes Ad	vanced Settings	
PassiveID Dor	main Controllers			
() Refresh / Lot () 1	tesh Add DCs Use Existing A	gent Config WMI Add	Agent	
Domain	DC Host	Site	IP Address	Monitor Using
 surendm.lab.local 	WIN-2R7K23JE850.surendry.	Default-First-Site-Name	10.127.196.86	PassiveIDAgentPrimary
	Subscribers Certificates Connecton Whitelated PassiveID Dor Cannecton Connecton Datasa Connecton Domain Domain Surende Jab Iscal	Subscribers Certificates Troubleshoot Report Connection WhiteInited Domains PassiveID Ore PassiveID Domain Controllers Dataset CER Task Act DCs Una Cathling A Domain DC Host parendrabalticat WH-207X22X850 surrentr.	Subscribers Certificates Troubleshoot Reports Connection Whitelated Domain PassiveID Groups Attributes Ad PassiveID Domain Controllers C Releash C Eat C Starts Add DCs Use Existing Agent Config WMI Add Domain DC Host Site Domain DC Host Site	Subscribers Certificates Troubleshoot Reports Connection Whitelated Domains PassiveID Groups Attributes Advanced Settings PassiveID Domain Controllers Baheah Cell Texas Add DCe Use Existing Agent Centig With: Add Agent Domain DC Host Site IP Address Bornain DC Host Site IP Address serendrizablisti WHY-2874224590 avender, Detail-Frist-Site-Name 10.137.156.56

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 > PassiveID > Overzicht > Dashboard**.

E Cisco ISE			Wo	k Centers · PassiveID · Overview			0.0500
Overview Providers	Subscribers Certificates Troubleshoot	Reports					
Uve Sessions	Sessions 📀 Pro	oviders 💿 2	Agents 💿 2	Subscribers 📀			Ø
	PROVIDERS	Anant Domain	Ø SUBSCR	IBERS O	Ø	ACTIVE SESSIONS	0
	Varie	Agent Domain PassiveiDAgentPrimary surendrr.lat	Name Noca Ne-adr	Status Description Status Okine		No data mediable.	
			ise-brid ise-brid ise-fant	0 0 0 0 0 0 0 0 0 0			
	Last refreshed 2020-11-05 17:40.40		Last refre	-Ia Oxime hest 2020-11-05 17:40:38		Last refeated 2020-11-05 17.42.38	

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

Cisco ISE						Work Centers · Pa	ssiveID - Overview	·						9, 0) 58 ¢
Overview Pr	roviders	Subscribers Certificates	Troubleshoot Reports												
Introduction Dashboard Uve Sessions											Re	hush lever v	Show Latest 20 record	Within ds 🗸 Last	24 hours 🗸
		🖉 Refresh 👍 Export To 🗸												V	Filter 🗸 🕤
		Initiated	Updated	Session Sta	Provider	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture St	Security G	Server	Auth M	Authentica
		×				~	Endpoint ID	Identity		 Endpoint Profile 	Posture Statu	Security Grou	Server	Auth Meth	Authenticat
		Nov 05, 2020 05:59:31.925 PM	Nov 05, 2020 05:59:31.9	Authenticated	Agent	Show Actions	10.127.196.85	Administrator	10.127.196.85				ISE30LABH1		
East Updand. The Nev 6 2020 18:01:03 GMT-0530 (India Standard Tree)											Record	ds Shown: 1			

Controleer de Agent-services op Windows-server

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

Task Manager				-		×
Processes Performance Users	Details	Services				
Name	PID	Description	Status	Gro	up ^	^
SEPICAgent	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			
KMwareCAFCommAmqpLi		VMware CAF AMQP Communicatio	Stopped			
🔍 vmvss		VMware Snapshot Provider	Stopped			
🔍 VMTools	2484	VMware Tools	Running			
Service VGAuthService	2480	VMware Alias Manager and Ticket S	Running			
🔍 vds	4236	Virtual Disk	Running			
SaultSvc	724	Credential Manager	Running			
🔍 UI0Detect		Interactive Services Detection	Stopped			
🔍 UevAgentService		User Experience Virtualization Service	Stopped			
Carl TrustedInstaller		Windows Modules Installer	Stopped			
TieringEngineService		Storage Tiers Management	Stopped			
SQLWriter	3148	SQL Server VSS Writer	Running			
SQLTELEMETRY\$SQLEXPRE	4884	SQL Server CEIP service (SQLEXPRESS)	Running			
SQLBrowser		SQL Server Browser	Stopped			
SQLAgent\$SQLEXPRESS		SQL Server Agent (SQLEXPRESS)	Stopped			
C snnsvc		Software Protection	Stopped			~

🔿 Fewer details | 🍓 Open Services