Configuración del Agente de ID pasiva de Identity Services Engine basado en EVT

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Necesidad de un nuevo protocolo Ventajas con el uso de MS-EVEN6 Alta disponibilidad **Escalabilidad** Ampliación de la arquitectura de configuración de pruebas Consulta de eventos históricos Menos gastos generales de procesamiento Configurar Diagrama de conectividad Configuraciones Configuración de ISE para Agente PassiveID Comprender el archivo de configuración del agente de PasivoID Verificación Verificar los servicios de PasivoID en ISE Verificar servicios de agente en Windows Server

Introducción

Este documento describe el nuevo ISE Passive Identity Connector (ISE-PIC) Agent introducido en la versión de ISE 3.0, sus ventajas y la configuración de este agente en ISE. ISE Passive Identity Agent se ha convertido en una parte integral de la solución de firewall de identidad gracias a Cisco FirePower Management Center.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administración de Cisco Identity Services
- MS-RPC, protocolos WMI
- Administración de Active Directory

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Identity Services Engine versión 3.0 y posterior
- Estándar de Microsoft Windows Server 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Necesidad de un nuevo protocolo

La función de identidad pasiva (ID pasiva) de ISE impulsa varios casos prácticos importantes, incluidos el firewall basado en identidad, EasyConnect, etc. Esta función depende de la capacidad de supervisar a los usuarios que inician sesión en los controladores de dominio de Active Directory y de aprender su nombre de usuario y sus direcciones IP. El protocolo principal actual que utilizamos para monitorear los controladores de dominio es WMI. Sin embargo, la configuración es difícil/invasiva, tiene un impacto en el rendimiento tanto en los clientes como en los servidores, y a veces tiene una latencia extremadamente alta al ver los eventos de inicio de sesión en implementaciones a escala. Tras una investigación exhaustiva y otras formas de sondear la información requerida para los Servicios de identidad pasiva, se decidió un protocolo alternativo, conocido como EVT o API de evasión, que es más eficiente en el manejo de este caso práctico. A veces se denomina **MS-EVEN6**, también conocido como Eventing Remote Protocol, que es el protocolo RPC subyacente basado en el cable.

Ventajas con el uso de MS-EVEN6

Alta disponibilidad

El agente original no tenía la opción High Availability y, si es necesario realizar el mantenimiento en el servidor en el que el agente se estaba ejecutando o se había producido una interrupción, se perderían los eventos de inicio de sesión y características como Firewall basado en identidad verían una pérdida de datos durante este período. Esta es una de las principales preocupaciones con el uso de ISE PIC Agent antes de esta versión. ISE utiliza UDP Port 9095 para intercambiar latidos entre los agentes.



Escalabilidad

El nuevo agente proporciona mejor soporte con mayores números de escala para un número admitido de controladores de dominio y el número de eventos que puede manejar. Estos son los números de escala que se probaron :

- Número máximo de controladores de dominio supervisados (con 2 pares de agentes): 74
- Número máximo de asignaciones/eventos probados: 292 000 (3950 eventos por DC)
- Prueba máxima de TPS: 500

Ampliación de la arquitectura de configuración de pruebas



Consulta de eventos históricos

En caso de conmutación por fallas o en caso de que se realice un reinicio del servicio para el agente de PIC, para asegurarse de que no se pierda ningún dato, se consultan los eventos que se generan durante el tiempo dado pasado y se envían nuevamente a los nodos PSN. De forma predeterminada, el ISE consulta el valor de 60 segundos de los eventos pasados desde el inicio del servicio para anular cualquier pérdida de datos durante la pérdida del servicio.

Menos gastos generales de procesamiento

A diferencia de WMI, que es una CPU intensa en gran escala o carga pesada, EVT no consume tantos recursos como WMI. Las pruebas de escala mostraron un rendimiento muy mejorado de las consultas con el uso de EVT.

Configurar

Diagrama de conectividad



Configuraciones

Configuración de ISE para Agente PassiveID

Para configurar los servicios PassiveID, uno debe tener los Servicios de identidad pasiva habilitados en al menos un nodo de servicio de políticas (PSN). Se puede utilizar un máximo de dos nodos para Passive Identity Services que funciona en modo de funcionamiento Activo/En espera. ISE también se debe unir a un dominio de Active Directory y sólo los controladores de dominio presentes en ese dominio pueden ser supervisados por agentes configurados en ISE. Para unirse a ISE a un dominio de Active Directory, refiérase a la <u>Guía de Integración de Active Directory</u>.

Vaya a Administration > System > Deployment > [Choose a PSN] > Edit para habilitar Passive Identity Services como se muestra aquí :

≡ Cisco I	SE				Admir	nistration - System -	Deployment			Evaluation Mode 88 Days	9	9 5	3 (
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Upgrade Refresh	Backup & Restore	Admin Access	Settings				
			ISE30LA	8H2									
			Dedic	ated MnT 🕕									
		-	🗖 🗸 Po	licy Service									
				Enable Session	Services 🕕)							
				Include Node in Node	Group None		× 0						
			Enable	e Profiling Service 🕕									
			Enable	e Threat Centric NAC Se	vice 🕕								
			\Box >	Enable SXP Ser	rice 🕕								
			C Enabl	e Device Admin Service	0								
			Enable	e Passive Identity Servic	• 🕖								
		_	pxGrid 🕡										

Navegue hasta **Centros de trabajo > ID pasivo > Proveedores > Agentes > Agregar** para implementar un nuevo agente como se muestra aquí :

■ Cisco ISE	Work Centers · PassiveID · Providers
Overview Providers	Subscribers Certificates Troubleshoot Reports
Active Directory	Agents > New
Agents	Agents
API Providers	C Deploy New Agent
SPAN	C Register Existing Agent
Syslog Providers	
Mapping Filters	Name * PassiveIDAgentPrimary
Endpoint Probes	
	Description Primary Agent
	· · · ////////////////////////////////
	Hols + GON + MCAO93JKH8, surendrr.lab.local
	The Alignet
	o der Kallen administrator
	Personni *
	Show Password
	Protocol: *
	MS-RPC V
	nigh Avenavnity Settings 🕖
	O Standalone
	O Primary
	O Secondary
	Cancel Deploy

Nota: 1. Si ISE tiene previsto instalar el agente en el controlador de dominio, la cuenta utilizada aquí debe tener privilegios suficientes para instalar un programa y ejecutarlo en el servidor mencionado en el campo FQDN del host. El FQDN de host aquí puede ser el de un servidor miembro en lugar de un controlador de dominio.

2. Si un agente ya se ha instalado manualmente o desde una implementación anterior de ISE, con MSRPC, los permisos y configuraciones necesarios en el lado de Active Directory o Windows son menos comparados con WMI, el otro protocolo (y el único disponible antes de 3.0) utilizado por los agentes PIC. La cuenta de usuario utilizada en este

caso puede ser una cuenta de dominio regular que forma parte del **grupo de lectores de registros de eventos. Elija Registrar agente existente** y utilice estos detalles de cuenta para registrar el agente que se instala manualmente en los controladores de dominio.

Después de una implementación exitosa, configure otro agente en un servidor diferente y agréguelo como un agente secundario y luego su peer primario como se muestra en esta imagen.

■ Cisco ISE		Work Centers · PassiveID · Providers
Overview Providers	Subscribers Certificates Troubleshoot	t Reports
Active Directory Agents	Deploy New Agent O Register Existing Agent	
API Providers SPAN Syslog Providers Mapping Filters Endpoint Probes	Name • PassiveIDAgeSecondary Description	
	Secondary Agent	
	User Name * administrator	
	Password *	Show Password
	Protocol: • MS-RPC \lor	
	High Availability Settings Standatone Primary Secondary	
	Primary Agents PassiveIDAgentPrimary Cancel Deploy	<u>×</u>

Para monitorear los controladores de dominio usando los agentes, navegue hasta **Centros de trabajo > ID pasivo > Proveedores > Active Directory > [Haga clic en el punto de unión] > ID pasivo**. Haga clic en **Agregar DC** y elija los controladores de dominio desde los cuales se recuperan los eventos/asignaciones de IP de usuario y haga clic en **Aceptar** y luego haga clic en **Guardar** para guardar los cambios, como se muestra en esta imagen.

E Cisco ISE				ork Cantors, DecelualD	- Dres ideas				Evaluation Mode 18 Days 🛦 Q. 🕐 💭 🖓 🤁
Overview Providers		Troubleshoot Rep					×		
Active Directory		ted Domains PassivelD	Add Domain	Controllers					
API Providers SPAN	PassiveID Don	nain Controller:	_						
Syslog Providers			ø	Domain	DC Host	Site		Rows/Page 0 🗸 K C 0	5 /0 > > Go 0 Total Rows
Mapping Filters			8	surendm.lab.local	WIN-2R7K23JE850.surendr	Default-First-Site-Name	Þ.		
Endpoint Probes	2 Refresh / Edit 10	and Add DCs Day Existing	8	surendm.lab.local	WIN-4RCA093JKH8.surend	Default-First-Site-Name	Þ		
	Domain	DC Host							
						Cancel	ок		
							_		
									Save

Para especificar los agentes que se deben utilizar para recuperar los eventos, vaya a **Centros de trabajo > ID pasivo > Proveedores > Active Directory > [Haga clic en el punto de unión] > ID pasivo.** Elija los controladores de dominio y haga clic en **Editar**. Introduzca el *nombre de usuario* y la *contraseña*. Elija **Agente** y, a continuación, **Guardar** el cuadro de diálogo. Haga clic en **Guardar** en la ficha PassiveID para completar la configuración.

E Cisco ISE		Winds Procedures - Barrelands - Barrelanders
Overview Providers		Edit Item
Active Directory Agents	Connection Whitelisted Domains PassiveID	Edit Domain Controller
API Providers SPAN Syslog Providers	PassiveID Domain Controllers	Hose FOON WNN-2877K23JEB50.surendrf.lab.tocal
Mapping Fitters Endpoint Probes	🔿 Refresh 🥒 Est. 🐧 Tauch - Add DCa - Una Enlating Age	Description
	Domain DC Host	That Value 4
	surendrr.lab.local WIN-2R7K23JEB50.surendrr.	administrator
	surendr: lab local WHY-4ECA0933098 served.	Passerd Agent Configure Test Agent PassiveIDAgemPrimary Configure Test Cartei Seven

Se puede verificar si la configuración se aplica correctamente con la ayuda de los botones **Configurar** y **Prueba**, como se muestra en las imágenes aquí:

		Ulark Parton - Doolard B - Deviden	Evaluation Mode & Days 🔺 🔍 🗇 🔂 🕀
Overview Providers	Subscribers Certificates Troubleshoot Reports	Edit Item	
Active Directory	Conception URBANISted Domains Description	Edit Demain Constaller	
		Information	
		Heet FQDN Successfully configured Domain Controller WIN-2R7K23JEB50.surender	
		0x 10 0 10 0 10 0 10 0 10 0 10 0 10 0 1	
	🛛 Refeats 🖉 Edit 🔘 Track Add DCa Una Existing Age	Description	
	Domain DC Host		
		User Name * administrator	
	surender lab local WIN-4RCA093.80% surend.		
		Show Password	
		Agent V Configure Test	
		Apert *	
		PassiveiDAgentPrimary V	
		Cancel	
E Cisco ISE			Evaluation Mode Mil Days 🔺 Q. 🕐 🕼 🖨
Cisco ISE	Subscribers Certificates Troubleshoot Reports		Evaluation Much III Days 🛦 Q. 💿 🕅 🔍
Cisco ISE Overview Providers Asthe Directory	Subscribers Certificates Troubleshoot Reports	Edit	Environdente Market Million als Caper 🛦 🔍 💿 🎵 🖶
Cisco ISE Overview Providers Astree Dresstery Agents	Subscribers Certificates Troubleshoot Reports Cernection Whitefaled Domains PasswerD	Edit () Edit () Edit Do Information	
Cisco ISE Overview Providers Active Directory Agents Arth produces Bank	Subscribers Certificates Troubleshoot Reports Certificates Domains Passeet0 PassiveID Domain Controllers	Edit Edit Do Information The connection to VMP-20723LR50 usered has local" assisted as stabilitied successfully.	mandra Mala 10 may 2 Q C [2 0
Cisco ISE Overview Providers Artina Deseting Approximations BRAN Syncip Providers	Subscribers Certificates Troubleshoot Reports Certificates Domains Passeet0 PassiveID Domain Controllers	Edit Edit Do Information WN-28 Window senson is Win-2002 Stability surendim Jab local" PassivelD active node. Connection is Win-2002 Stability surendim Jab local" assivelD active node. Connection is Win-2002 Stability Build State and a stability surendim Jab local" assivelD active node.	Endeder Main H Payr & Q C [3] 0
Cisco ISE Overview Providers Artina Deastery Apress Art Providers BrAN Typing Providers Displain Previs	Subscribers Certificates Troubleshoot Reports Cernection Whitefaled Domains Passeet0 PassiveID Domain Controllers	Edit Edit Do Information WW-270 Www.270 The connection was trasted on 1952/04/04/05 average tablished accessfully Wordswas version in WW-2072/32/85/04 average tablished accessfully Wordswas version in WW-2072/32/85/04/04 average tablished accessfully wordswas version in WW-2072/32/85/04/04/04 average tablished accessfully wordswas version in WW-2072/32/85/04/04/04 average tablished accessfully wordswas version in WW-2072/32/85/04/04/04/04/04/04/04/04/04/04/04/04/04/	Endeden Mole III Days & Q. () () () () () () () () () () () () ()
Claco ISE Overview Providers Artina Deseting Artina Deseting Artina Deseting Artina Deseting Artina Deseting Artina Deseting Deseting Providers Designer Providers	Subscribers Certificates Troubleshoot Reports Cernection Whitefaled Domains Passeet0 PassiveID Domain Controllers	Edit Edit Do Information WH-2P2 WH-2P2 Connection to WH-2P7C32.4EH0 Aurendri Ale Iocal PasswelD active rods. Connection to WH-2P7C32.4EH0 Aurendri Ale Iocal PasswelD active rods. Succeeded.	2 Markadam Malak Hil Days & Q. O Di G
Cisco ISE Overview Providers Artina Desekry Artina Desekry Artina Desekry Artina Desekry Bana Typing Providers Designer Providers Designer Providers	Subscribers Certificates Troubleshoot Reports Cernection Whitefaled Domains Passeet0 PassiveID Domain Controllers Blakesh af an State Act Dis Use Scalary Age Domain DC Heat Control Report DC Heat	Edit Edit Di Information Wei-270 Wei-270 Descrete Descrete Line Home *	Evaluation Motols HE (bays 🛋 🔍 🕐 💭 🗭 🗭
Clace SE Overview Providers Artic Denselse Artic Denselse Artic Providers Arti	Subscribers Certificates Troubleshoot Reports Connaction Whiteshoet Domain Controllers PassiveID Domain Controllers	Edit Edit Di Information Image: Comparison of Comparison	Endeden Mole HE Pays ▲ Q. O 52 ●
Creaner SE Oreaner Antre Oreactury Antre Oreac	Subscribers Cersificates Troubleshoot Reports Connection Whitestoted Domain Controllers PassiveID Domain Controllers	Edit	Endeder Mols Hil Pays & Q O Di G
Ciaco ISE Overnere Poyders Arthe Breastray Arthe Powders Marine M	Subscribers Cersticates Troubleshoot Reports Connection WhiteInited Domains PassiveD PassiveID Domain Controllers Referst @ Ean @ Tauk Add DCs Dee Exercise Age Demain DD Heat sevender Lab head With-387/23.3.8595 sevender sevender Lab head With-387/23.3.8595 sevender	Edit Edit D Information Within Wit	Califordin Mole Hill Pary & C. O. D. D. O.
Ciaco ISE Overview Poyders Arthe Bioastrey Arthe Poidons DATA Poidons Data Poidons Po	Subscribers Certificates Troubleshoot Reports Connection Whiteleted Domain Controllers PassiveID Domain Controllers © Balank & Call © truck Act DCs One Ceating Age © Domain DC Heat © avender Lab Issue White-1075/23.21583 avender. © sevender lab Issue White-1075/23.21583 avender.	Edit Edit Diformation More real More re	2 (1)) 6 2 100 fam
Ciaco ISE Donniew Posiders Antre General Antre G	Subscribers Certificates Troubleshoot Reports Connection Whitelevel Domain Controllers Passivel D Domain Controllers Passive D Domain Controllers Passive D Domain OC Heat Passeder tab heat Whitelevel 2000 Barreader sevender tab heat Whitelevel 2000 Barreader	Ecite Ender Ender Erection Ender	
Ciaco (SE Overview Possideur Antre Greeken Antre Greeken Marging Provideur Angeling Provideur Angeli	Subscribers Certificates Troubleshoot Reports Connection Whitestand Domains Passwell PassiveID Domain Controllers Passwell ID Domain Controllers Passwell Ibb Ioal 900-207023.0250 auronatic Suswell Ibb Ioal 900-207023.0250 auronatic	Edit Edit Difference Binor	
Cinco (SE Antor General Antor Gene	Subscribers Certificates Troubleshoot Reports	Edit Edit Difference Witten	

Comprender el archivo de configuración del agente de PasivoID

El archivo de configuración de PassiveID Agent se encuentra en C:\Program Files

(x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config. Aquí se muestra el contenido del archivo de configuración:

Verificación

Verificar los servicios de PasivoID en ISE

1. Verifique si el servicio PassiveID está habilitado en la GUI y también está marcado ejecutando el comando **show application status ise** en la CLI del ISE.

≡ Cisco IS	SE				Admir	nistration · System ·	Deployment			Evaluation Mode 88 Days	A Q	0	,7
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Upgrade Refresh	Backup & Restore	Admin Access	Settings				
			ISE30LA	ABH2									
			Dedic	cated MnT 🕡									
		-	🗆 🗸 Po	licy Service									
			~	Enable Session	Services 🕕								
				Include Node in Node	Group None		× 0						
			Enable	e Profiling Service 🕕									
			Enable	e Threat Centric NAC Se	rvice 🕕								
			\Box >	Enable SXP Ser	vice 🕕								
			Enable	le Device Admin Service	0								
			Enable	le Passive Identity Servi	* 🛈								
		-	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. Verifique si el proveedor de ISE Active Directory está conectado a los controladores de dominio en **Centros de trabajo > ID pasivo > Proveedores > Active Directory > Conexión**.

E Cisco ISE	Work Centers - PassiveID - Providers	
Overview Providers	Subscribers Certificates Troubleshoot Reports	
Active Directory Agents	Connection Whitelisted Domains PassiveID Groups Attributes Advanced Settings	
API Providers SPAN	* Join Point Name PassiveID-AD 0	
Syslog Providers Mapping Filters	* Active Directory Domain surrendry lab local	
Endpoint Probes	+ Join + Leave 🔗 Treat Uner 🛠 Diagnostic Text 🔿 Referent Table	
	isE Node A isE Node R Status Demain Controller Site	
	🖸 ISEQUARIT surrentisk local PRIMARY 🖉 Operational With-201433/BSG surrenti. Ordust Friti Star-Nerve	
	🗈 ISESIARD avendrate boot SECONDATY 📴 Oversions INV-4EX-0033,014 svender L. Defaul Prict Star-Name	

3. Verifique si los controladores de dominio requeridos están siendo monitoreados por el **Agente** en los Centros de Trabajo > PasivoID > Proveedores > Active Directory > PasivoID.

E Cisco ISE				Work Ce	anters · PassiveID · Providers		0.05
Overview Providers	Subscribers Certificates	Troubleshoot Report	15				
Active Directory Agents	Connection Whitelisted	Domains PassivelD Gro	oups Attributes Ad	vanced Settings			
API Providers	PassiveID Dor	nain Controllers					
Syslog Providers						Rows/Page 2 🗸 K < 1	3 /1>> Go 2 To
Mapping Filters Endpoint Probes	S Refresh / Eds 0 1	ush Add DCs Use Existing A	gent Config WMI Add	Agent			
	Domain	DC Host	Site	IP Address	Monitor Using		
	 surendm.teb.local 	WN-2R7K23JE850.surendry.	Default-First-Site-Name	10.127.196.86	PassivetDAgentPrimary		
	 surendm.lab.local 	WIN-4RCA093JICH8.surend.	Default-First-Site-Name	10.127.196.85	PassiveIDAgentPrimary		

4. Verifique si el estado de los controladores de dominio que se monitorean está activo, es decir, marcado en verde en el panel en **Centros de trabajo > ID pasivo > Descripción general > Panel**.

E Cisco ISE			Wo	k Centers · PassiveID · Overview			0.0 58 0
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. Verifique que las sesiones en directo se completen cuando se registra un inicio de sesión de Windows en el controlador de dominio en **Centros de trabajo > ID pasivo > Descripción general > Sesiones en directo**.

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		
		Last Updated: Thu Nov 05 2020	18:01:03 GMT+0530 (India Stand	lard Time)										Record	ds Shown: 1

Verificar servicios de agente en Windows Server

1. Verifique el servicio ISEPICAgent en el servidor donde está instalado el agente PIC.

₫짚 Task Manager				-		×
File Options View						
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			
🔍 VGAuthService	2480	VMware Alias Manager and Ticket S	Running			
🔍 vds	4236	Virtual Disk	Running			
CaultSvc	724	Credential Manager	Running			
🔍 UI0Detect		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\$SQLEXPRE	4884	SQL Server CEIP service (SQLEXPRESS)	Running			
SQLBrowser		SQL Server Browser	Stopped			
SQLAgent\$SQLEXPRESS		SQL Server Agent (SQLEXPRESS)	Stopped			
C. spnsvc		Software Protection	Stonned			~

Fewer details | 🎇 Open Services