配置基於EVT的身份服務引擎被動ID代理

目錄

簡介 必要條件 需求 採用元件 需要新協定 使用MS-EVEN6的優勢 高可用性 可擴充性 擴展測試設定架構 歷史事件查詢 減少處理開銷 設定 連線圖 組態 為PassiveID代理配置ISE 瞭解被動ID代理配置檔案 驗證 驗證ISE上的PassiveID服務 驗證Windows伺服器上的代理服務

簡介

本文檔介紹在ISE 3.0版本中引入的新ISE被動身份聯結器(ISE-PIC)代理、其優勢以及此代理在 ISE上的配置。ISE被動身份代理也已成為使用Cisco FirePower Management Center的身份防火牆 解決方案的組成部分。

必要條件

需求

思科建議您瞭解以下主題:

- 思科身份服務管理
- MS-RPC、WMI協定
- Active Directory管理

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- •思科身份服務引擎3.0及更高版本
- Microsoft Windows Server 2016標準版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

需要新協定

ISE的被動身份(被動ID)功能驅動許多重要的使用案例,包括基於身份的防火牆、EasyConnect等 。此功能取決於監控使用者登入Active Directory域控制器並學習其使用者名稱和IP地址的能力。當 前用於監視域控制器的主要協定是WMI。但是,配置是困難/侵入性的,對客戶端和伺服器都有效能 影響,而且在規模化部署中檢視登入事件時有時具有非常大的延遲。經過深入的研究和替代方法以 輪詢被動身份服務所需的資訊後,決定採用另一種協定(稱為EVT或Eventing API),以便更高效 地處理此使用案例。它有時也稱為**MS-EVEN6**,也稱為Eventing Remote Protocol,它是基於 RPC的底層協定。

使用MS-EVEN6的優勢

高可用性

原始代理沒有高可用性選項,如果需要在該代理正在運行的伺服器上進行維護或發生中斷,會錯過 登入事件,基於身份的防火牆等功能會在此期間丟失資料。這是在此版本之前使用ISE PIC代理的主 要問題之一。ISE使用UDP埠9095在代理之間交換心跳。



可擴充性

新代理通過增加支援數量的域控制器以及它可以處理的事件數量來提供更好的支援。以下是測試過 的刻度數:

- •受監控的域控制器的最大數量(2對Agent):74
- 測試的最大對映/事件數: 292,000(每個資料中心3950個事件)
- 測試的最大TPS:500

擴展測試設定架構



歷史事件查詢

在故障轉移或對PIC-Agent執行服務重啟的情況下,為確保資料不會丟失,將查詢過去給定時間內 生成的事件,並再次傳送到PSN節點。預設情況下,ISE會查詢從服務開始起價值60秒的過去事件 ,以彌補服務丟失期間的任何資料丟失。

減少處理開銷

與大規模或重負載下CPU密集的WMI不同,EVT不像WMI那樣消耗那麼多資源。Scale測試表明使 用EVT查詢的效能有了很大提高。

設定

連線圖



組態

為PassiveID代理配置ISE

要配置PassiveID服務,必須至少在一個策略服務節點(PSN)上啟用被動身份服務。最多兩個節點可 用於被動身份服務,該服務以主用/備用模式運行。ISE還必須加入到Active Directory域,並且只有 該域中存在的域控制器才能由ISE上配置的代理進行監控。若要將ISE加入Active Directory域,請參 閱<u>Active Directory整合指南。</u>

導航到**Administration > System > Deployment > [Choose a PSN] > Edit以啟**用Passive Identity Services,如下所示:

≡ Cisco 🗄	SE				Admi	nistration · System ·	Deployment			Evaluation Mode 88 Days	A Q	0	70 (
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Upgrade Refresh	Backup & Restore	Admin Access	Settings				
			ISE30LA	BH2									
			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	rvice 🕕								
			\Box >	Enable SXP Ser	vice 🕕								
			Enabl	le Device Admin Service	0								
			C Enabl	le Passive Identity Servic	* 🕡								
			pxGrid ()										

導航到**工作中心(Work Centers)>被動ID(PassiveID)>提供程式(Providers)>代理(Agents)>新增 (Add)**,以部署新代理,如下所示:

≡ Cisco	ISE	Work Centers · PassiveID · Providers
Overview	Providers	Subscribers Certificates Troubleshoot Reports
Active Directory		Agents > New
Agents		Agents
API Providers		
SPAN		
Syslog Providers		
Mapping Filters		Name *
Endpoint Probes		PassiveIDAgentPrimary
		Description
		Primary Agent
		Host FOON *
		WIN-4RCA093JKH8,surendrr.lab.local
		User Name * administrator
		Pasword * Show Password
		Protocol: * MS-RPC V
		High Availability Settings
		O Standalove
		O Primary
		Secondary
		Cancel Deploy

附註:1.如果代理計畫由ISE安裝在域控制器上,此處使用的帳戶必須具有足夠的特權,以便 安裝程式並在主機FQDN欄位中提到的伺服器上運行該程式。這裡的主機FQDN可以是成員伺 服器而不是域控制器的FQDN。

2.如果代理已手動安裝或從ISE的先前部署使用MSRPC安裝,則Active Directory或 Windows端所需的許可權和配置與WMI相比,PIC代理使用的其他協定(以及3.0之前唯一可 用的協定)較少。在此情況下使用的使用者帳戶可以是常規域帳戶,該帳戶是事件日誌讀**者器** 組的一部分。選擇註冊現有代理,然後使用這些帳戶詳細資訊註冊在域控制器上手動安裝的代 理。

成功部署後,將另一個代理配置到其他伺服器上,並將其新增為輔助代理,然後新增其主要對等體 ,如下圖所示。

≡ Cisco IS	Work Centers · PassiveID · Providers
Overview	Providers Subscribers Certificates Troubleshoot Reports
Active Directory	Deploy New Agent
Agents	Register Existing Agent
API Providers	
SPAN	Name * PassiveIDAgeSecondary
Syslog Providers	
Mapping Filters	
Endpoint Probes	Description Secondary Agent
	Host FUDW WIN- ARCA093JKH8.surendrr.lab.local
	User Name * administrator
	Password * Show Password
	MS-RPC V
	High Availability Settings 0
	Sundakne
	Primary Agents
	PassiveIDAgentPrimary V
	Cancel Deploy

若要使用代理監視域控制器,請導航到**工作中心>被動ID >提供程式> Active Directory > [按一下加入點] > PassiveID**。按一下「Add DCs」,然後選擇從中檢索使用者 — IP對映/事件的域控制器 ,然後按一下「OK」,再按一下「Save」以儲存變更,如下圖所示。

E Cisco ISE	_	Mindy Constant - Darah	alD-Dravidara			1	Evaluation Mode M Days 🛦 🔍 🕐 528 🚳
Overview Providers	Subscribers Certificates Troubleshoot Rep.				×		
Active Directory Agents API Providers	Connection Whitelated Domains PassivelD PassiveID Domain Controller:	Add Domain Controllers					
SPAN Syslog Providers		2 Domain	DC Host	Site		and an an M. C. C.	A (A) N To A Test Inc.
Mapping Fitters		surendm.lab.local	WIN-2R7K23JE850.surendr	Default-First-Site-Name	5		
	S Refresh / Eds. C Track Add DDs Use Existing	surendm.lab.local	WIN-4RCA093JKH8.surend.	Default-First-Site-Name	1-		
	Demain DC Heat			Cancel	×		
							Save

若要指定應用於從中檢索事件的代理,請導航到Work Centers > PassiveID > Providers > Active Directory > [按一下加入點] > PassiveID。選擇域控制器並按一下Edit。輸入*User Name*和 *Password*。選擇Agent,然後選擇Save對話方塊。在PassiveID頁籤上按一下Save以完成配置。

E Cisco ISE		High Postage Bool alb. Booldage	Evaluation Mode Mil Days 🛦 🔍 🕥 🔂 🚭
Overview Providers		Edit Item	
Active Directory Agents	Connection Whitelisted Domains PassiveID	Edit Domain Controller	
API Providers SPAN System Providers	PassiveID Domain Controllers	Heit FORN WIN-2R7X23JEB50.surendir.lab.local	
Mapping Filters Endpoint Probes	🖉 Refresh 🖉 Kata 🛛 Trash - Add DCa - Usa Existing Age	Beaufiges 2 w 15 5 1	2 Total Rows
	Domain DC Host		
	surender.lab.local WIN-287K23./E850 surender.	Over Neme * administrator	
	waveder tab head WHI-48CA0932018 surved.	Pessor Sdow Passed Agent ~ Pristod Configure Test Agent * PassiveDAgentPrimary ~ Cancel Bree	

您可以使用Configure和Test按鈕來檢查是否正確應用了配置,如下圖所示:

E Cisco ISE			Searce - Deschalb - Drei Glass		Evaluation Mode M Days 🔺 Q. 🗇 💭			
Overview Providers	Troubleshoot Reports	Edit Item	0	^				
Active Directory Agents	d Domains PassiveID	Edit Domain Controller	Information					
API Providers SPAN Systeg Providers Mapping Filters	ain Controllers	Host FQDN WIN-2R7K23JE850.surender	Successfully configured Domain Controller					
Endpoint Probes	Add DCs Use Existing Age	Description						
	DC Host							
	WN-2R7K23.E850.surendre.	User Name * administrator						
	WN-4RCAD93.00% surved	Agent * PassiveIDAgentPrimary	Passed Bow Passed AgentConfigure Test 					
				Cancel Save				

E Cisco ISE	Hindy Paratase - Read and - Aver idea	Evaluator Mode III Days 🔺 Q. 🕐 😥 🗢
Overview Providers	Edit	
Active Directory Agents	Passwith Edit Do Information	
API Providers SPAN Syslog Providers Mapping Filters	Tollers The connection was tested on "5(30)(ABH2 surendratab.local" PassiveD active node. Connection to WW-2017(22)(ABH2 surendratab.local" PassiveD active node. Connection to WW-2017(2)(ABH2 surendratab.local" PassiveD active node. Windows version is "Win2016; hetB03 domains is "SURB/RORC Query for hasary events paceeded.	
	Des Tranting Age	
	User Name * administrator	
	Different.	
	Agent * PassiveIDAgentPrimary · PassiveIDAgentPrimary · Configure Test Agent * PassiveIDAgentPrimary · Configure Test Configure Test	

瞭解被動ID代理配置檔案

PassiveID Agent配置檔案位於C:\Program Files(x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config。此配置檔案的內容如下所示:



驗證ISE上的PassiveID服務

1.驗證PassiveID服務是否在GUI上啟用,並且在ISE的CLI上通過**show application status ise**命令標 籤為正在運行。

≡ Cisco I	ISE				Admi	nistration - System -	Deployment			Evaluation Mode 88 Days 🔺	Q (0)	50 (
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Upgrade Refresh	Backup & Restore	Admin Access	Settings			
			ISE30L4	ABH2								
			Dedic	cated MnT 🕕								
		-	□ ~ Po	licy Service Enable Session	Services 🧃)						
				Include Node in Node	Group None		~ 0					
			Enabl	e Profiling Service 🕕								
			Enabl	e Threat Centric NAC Se	rvice 🕕							
			\Box >	Enable SXP Ser	vice 🕕							
			🔽 Enab	le Device Admin Service	0							
			Menab	le Passive Identity Servi	ie 🕕							
		-	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.驗證ISE Active Directory提供程式是否已在Work Centers > PassiveID > Providers > Active

Directory > Connection連線到域控制器。

Cisco ISE	Work Centers - PassiveID - Providers	
Overview Providers	Subscribers Certificates Troubleshoot Reports	
Active Directory Agents	Connection Whitelated Domains PassivetD Groups Attributes Advanced Settings	
API Providers SPAN Syslog Providers Macoine Filters	* Join Puint Name Pass/veD-AD O * Adive Divestry Domain surendr: lab.local O	
Endpoint Probes	+ Jain + Leave A Test User X Disputsion Table ISE Node ^ ISE Node R Status Domain Controller Site	
	0 6530LABH: svendstablooit PRMARY IIII Operational WM-2020230550 svendst.l. Cellsoft-Franchise-Name 0 6530LABH2 svendstablooit SECONDARY IIIII Operational WM-4ECA033048 svendst.l. Cellsoft-Franchise-Name	

3.驗證Agent at Work Centers > PassiveID > Providers > Active Directory > PassiveID是否正在監 視所需的域控制器。



4.驗證受監控域控制器的狀態是否為up(即控制面板上Work Centers > PassiveID > Overview > Dashboard處標籤為綠色)。

E Cisco ISE		Work Centers - PassiveID - Overview	Q (0) 58 4	þ
Overview Providers St	ubscribers Certificates Troubleshoot Reports			
Introduction Dashbaard Live Sessions	Main Sessions ③ Providers ③ 0 2	Agents ③ Subscribers ③ 2 10	e	;
	PROVIDERS O Status Name Agent Work-307231,0000 avender Lab. Soci Passive/Dagent/many Work-4054,0033,0000 avender Lab. Soci Passive/Dagent/many	SUBSCHIRRS Subschirters Summer Status Summer Stat	C ACTIVE SESSIONS O CONTRACTOR SOLUCION CONTRA	

5.驗證在工作中心>被動ID >概述>即時會話的域控制器上註冊Windows登入時填充的即時會話。

E Cisco ISE				Work Centers · Pa	ssiveID - Overview						9) [2
Overview Providers	Subscribers Certificates Tro	ubleshoot Reports										
Introduction Dashboard Live Researce									Refresh Never	Show Latest 20 reco	Within rds 🗸 Last :	24 hours 🗸
	🖉 Refresh 👍 Export To 🗸										V	litter 🗸 💿
	Initiated	Updated	Session Sta Provider	Action	Endpoint ID	Identity	IP Address Endpoint	Profile Posture !	it Security G	Server	Auth M	Authentica
	×		×	~	Endpoint ID	Identity	v Endpoint	rofile Posture S	latu 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	and Time)								Record	s Shown: 1

驗證Windows伺服器上的代理服務

1.驗證安裝了PIC Agent的伺服器上的ISEPICAgent服務。

rife Options view						
Processes Performance Use	s 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			
🔅 VMwareCAFCommAmqpLi		VMware CAF AMQP Communicatio	Stopped			
wmvss		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			
🔍 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			
Snnsvc		Software Protection	Stonned			~

🔿 Fewer details | 🍓 Open Services