EVTベースのIdentity Services Engineパッシブ IDエージェントの設定

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 新しいプロトコルの必要性 MS-EVEN6の使用による利点 ハイ アベイラビリティ 拡張性 <u>スケールテストセットアップアーキテクチャ</u> 履歴イベントクエリ 処理オーバーヘッドの削減 設定 接続図 設定 <u>PassiveID AgentのISEの</u>設定 PassiveIDエージェント設定ファイルについて 確認 ISEでのPassiveIDサービスの確認 Windows Serverでのエージェントサービスの確認

概要

このドキュメントでは、ISE 3.0バージョンで導入された新しいISEパッシブIDコネクタ(ISE-PIC)エージェント、その利点、およびISEでのエージェントの設定について説明します。ISEパッ シブIDエージェントは、Cisco FirePower Management Centerを使用するアイデンティティファ イアウォールソリューションの不可欠な要素となっています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Administration
- MS-RPC、WMIプロトコル
- Active Directory管理

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engineバージョン3.0以降
- Microsoft Windows Server 2016 Standard

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

新しいプロトコルの必要性

ISEのパッシブID(パッシブID)機能は、IDベースのファイアウォール、EasyConnectなど、多く の重要な使用例を促進します。この機能は、Active Directoryドメインコントローラにログインし 、ユーザ名とIPアドレスを学習するユーザを監視する機能によって異なります。ドメインコント ローラの監視に使用する現在のメインプロトコルはWMIです。ただし、設定は困難/侵襲的であり 、クライアントとサーバの両方でパフォーマンスに影響を与えます。また、規模の大きい展開で ログオンイベントを確認する際に非常に大きな遅延が発生する場合もあります。Passive Identity Servicesに必要な情報をポーリングするための徹底的な調査と代替方法の後、EVTまたは Eventing APIと呼ばれる代替プロトコルが決定されました。これは、この使用例の処理により効 率的です。これは、MS-EVEN6とも呼ばれ、Eventing Remote Protocol(EVP)とも呼ばれます。こ れは、RPCベースのThe Wireプロトコルの基盤です。

MS-EVEN6の使用による利点

ハイ アベイラビリティ

元のエージェントには高可用性オプションがなく、エージェントが実行されているサーバまたは 停止しているサーバでメンテナンスを行う必要がある場合は、ログオンイベントが失われ、IDベ ースのファイアウォールなどの機能では、この間データが失われます。これは、このリリースよ り前のISE PIC Agentの使用に関する主な懸念事項の1つです。ISEはUDPポート9095を使用して 、エージェント間でハートビートを交換します。



拡張性

新しいエージェントは、サポートされる数のドメインコントローラと処理できるイベントの数に 対して、より多くのスケール数をサポートします。テストされたスケール番号を次に示します (図1を参照)。

- •モニタされるドメインコントローラの最大数(エージェントの2ペアあり):74
- テストされたマッピング/イベントの最大数:292,000(DCあたり3950イベント)
- テストされる最大TPS:500

スケールテストセットアップアーキテクチャ



履歴イベントクエリ

フェールオーバーの場合、またはPIC-Agentに対してサービスの再起動が実行された場合、デー タが失われないように、過去の一定時間に生成されたイベントが照会され、PSNノードに再送信 されます。デフォルトでは、サービスの開始時から60秒に相当する過去のイベントがISEによっ て照会され、サービスの損失中にデータの損失が相殺されます。

処理オーバーヘッドの削減

大規模または高負荷でCPU負荷が高いWMIとは異なり、EVTはWMIほど多くのリソースを消費し ません。スケールテストでは、EVTを使用したクエリのパフォーマンスが大幅に向上しました。

設定

接続図



設定

PassiveID AgentのISEの設定

PassiveIDサービスを設定するには、1つ以上のポリシーサービスノード(PSN)でPassive Identity Servicesが有効になっている必要があります。アクティブ/スタンバイモードで動作するパッシブ IDサービスには、最大2つのノードを使用できます。ISEはActive Directoryドメインに参加する必 要があり、そのドメインに存在するドメインコントローラだけがISEで設定されたエージェント によってモニタできます。ISEをActive Directoryドメインに参加させるには、『<u>Active Directory</u> <u>Integration Guide</u>』を参照してください。

[Administration] > [System] > [Deployment] > [Choose a PSN] > [Edit]に移動し、次のように Passive Identity Servicesを有効にします(図2を参照)。

≡ Cisco I	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	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 Serv	rice 🕕								
			Enabl	e Device Admin Service	0								
			Z Enabl	e Passive Identity Servic	• 🕕								
		_	pxGrid 🕡										

[Work Centers] > [**PassivelD] > [Providers] > [Agents] > [Add]に移動し**て、次のように新しいエー ジェントを展開します(図を参照)。

E Cisco ISE	Work Centers · PassiveID · Providers
Overview Providers	Subscribers Certificates Troubleshoot Reports
Active Directory Agents	Agents > New Agents
API Providers SPAN Syslog Providers	Dupplay New Agent O Register Existing Agent
Mapping Filters Endpoint Probes	Name * PassiveIDAgentPrimary
	Description Primary Agent
	Host FQON * WIN-4RCAO93JKH8.surendrr.lab.local
	Usar Name * administrator
	Password Show Password
	Protocol: * MS-RPC \checkmark
	High Availability Settings 🕕
	Standalone Primary Secondary Cancel Deploy

注:1.エージェントがドメインコントローラにISEによってインストールされる予定の場合 、ここで使用するアカウントには、プログラムをインストールし、[ホストのFQDN(ホス トのFQDN)]フィールドに示されているサーバで実行するのに十分な権限が必要です。こ こでホストFQDNは、ドメインコントローラではなくメンバサーバのホストFQDNにするこ とができます。

2.エージェントがMSRPCを使用してISEから以前に手動またはインストールされてい る場合、Active DirectoryまたはWindows側で必要な権限と設定は、PICエージェントが使用 する他のプロトコル(および3.0より前に使用可能な唯一のプロトコル)とのWMIよりも少 少少少少少数)。この場合に使用するユーザーアカウントは、イベントログリーダーグルー プの一部である通常のドメインアカウントである可能性があります。[既存のエージェント の登録]を選択し、これらのアカウントの詳細を使用して、ドメインコントローラに手動で インストールされたエージェントを登録します。

導入が正常に完了したら、別のサーバに別のエージェントを設定し、セカンダリエージェントと して追加してから、次の図に示すようにプライマリピアを追加します。

■ Cisco ISE		Work Centers · PassiveID · Providers
Overview Provider	rs 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 Acent	
	Secondary Agent	
	Host FQDN *	
	User Name *	
	administrator	
	Password *	
	Show Password	
	Protocol: *	
	MS-RPC \checkmark	
	High Availability Settings ()	
	Standalone Rrimpy	
	Secondary	
	- coordary	
	Primary Agents	
	PassiveIDAgentPrimary ~	
	Cascel Deploy	
	Cancel Depidy	

エージェントを使用してドメインコントローラを監視するには、[Work Centers] > [PassiveID] > [Providers] > [Active Directory] > [Click on the Join Point] > [PassiveID]に移動します。次の図に示 すように、[Add DCs]をクリックし、ユーザIPマッピング/イベントの取得元のドメインコントロ ーラを選択し、[OK]をクリックし、[Save]をクリックして変更を保存します。

E Cisco ISE			Hade Contace - Decelorit	h - Dravidara				Evaluation Mode M Days 🛦 Q, 🕐 💬 💭
Overview Providers		Rept				×		
Active Directory	Connection Whitelisted Domains P	Add Domain	Controllers					
API Providers	PassiveID Domain Contro	ller:						
SPAN Syslog Providers		•	Domain	DC Host	Site		Remarkan 0 w IC C 0	5 (0)) Gall & Intel Bowy
Mapping Filters		8	surendm.lab.local	WIN-287K23JE850.surendr	Default-First-Site-Name	Þ		
Endpoint Probes	C Refresh / Eds C Truck Add DDs Une	Calendary 🖸	surendrr.lab.local	WIN-4RCA093JKH8.surend	Default-First-Site-Name	1		
	Domain DC Host							
					Gancel	ок		
		_				_		
								Save

イベントの取得に使用するエージェントを指定するには、[Work Centers] > [PassiveID] > [Providers] > [Active Directory] > [Click on the Join Point] > [PassiveID]に移動します。ドメインコ ントローラを選択し、[Edit]をクリ**ックします**。ユーザ名とパスワードを入力します。[Agent]を選 択し、[Save the dialog box]を選択します。[PassiveID]タブの[Save]をクリックして、設定を完了 します。

E Cisco ISE		Minde Chanteger, Barris halfe i Borge 🛦 Q. 💿 💭
Overview Providers		Edit Item
Active Directory Agents	Connection Whitelisted Domains PassivelD	Edit Domain Controller
API Providers SPAN Syslog Providers	PassiveID Domain Controllers	Host FOON WIN-287X23JEB50 surendiri.lab.local
Mapping Filters Endpoint Probes	🗇 Refresh 🥖 Kata 🖏 Tasah 🛛 Add DCa — Una Taisting Ag	
	Domain DC Host	User Name *
	surendrr.lab.local WIN-2R7K23JE850.surendrr.	administrator
	wurdentrüch forei WRT-ERCADISZROR zurweit.	Persond Agent Share Password Agent Configure Test PassvelDAgentPrimary C Cancel Eve

次の図に示すように、[Configure]ボタンと[Test]ボタンを使用して、設定が正しく適用されている かどうかを確認できます。

E Cisco ISE			Evaluation Mode M Days 🛦 Q, 🕥 💯 🕸
Overview Providers Active Overview Active Overview Add Previders Data Byting Previders Magning Fitters Endquale Proteix	Subscribers Certificates Troubleshoot Reports Correction WhiteRead Domains PassiveID PassiveID Domain Controllers	Edit Item Edit Domain Controller Hear room Write-287X23JCB50.surener Write-287X23JCB50.surener Description	
	Demake DC Hest Demake DC Hest wrederlak bood with 4504032008 bareade. wrederlak bood with 4504032008 baread.	Due Name * administrator Passend Show Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passeord Test Apent Passeord Test Apent Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passeord Passe	
		PassivelDAgentPrimary V Cancel Sare	Int
		Weigh Provident Basel will a Provident	Evaluation Mode M Days 🔺 Q. 🕐 💢 🕀
Desrview Providers Active Diseases Active Diseases Active Diseases SPAN Spring Providers Disponet Proves	Subscribers Cernificates Troubleshoot Reports Connection Whatsles Dumains PassiveD PassiveID Domain Controllers I Infram. I Gen I Taulo Act CCs Vie Control Ace Demain DC Hose DC Hose White Jak Seal White J30(23.0005 acender. www.inframedia.based White J30(23.0005 acender.	Edit Edit Bar Da Wei 200 Barretro Barre	
		Cancel Save	

PassiveIDエージェント設定ファイルについて

PassiveID Agent構成ファイルはC:\Program Files (x86)\Cisco\Cisco ISE PassiveID

Agent\PICAgent.exe.configにあります。設定ファイルには、次の内容が含まれています(図2を参照)。

確認

ISEでのPassiveIDサービスの確認

1. GUIでPassiveIDサービスが有効になっていること、およびISEのCLIで**show application status** iseコマンドを使用して実行中とマークされていることを確認します。

≡ Cisco 🗄	SE				Admi	nistration - System -	Deployment			Evaluation Mode 88 Days	Q (9 29	6
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Upgrade Refresh	Backup & Restore	Admin Access	Settings				
			ISE30L/	ABH2									
			Dedic	ated MnT 🕡									
		-		licy Service	Sonicos								
				Include Node in Node	Group None		× 0						
			C Enabi	e Profiling Service 🕕									
			Enabl	e Threat Centric NAC Se	rvice (i)								
			\Box >	Enable SXP Ser	vice 🕕								
			Enab	le Device Admin Service	0								
			🔽 Enab	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. ISE Active Directoryプロバイダーが[Work Centers] > [PassiveID] > [Providers] > [Active Directory] > [Connection]でドメインコントローラに接続されているかどうかを確認します。

E Cisco ISE	Work Centers - PassiveID - Providers	
Overview Providers	Subscribers Certificates Troubleshoot Reports	
Active Directory Agents	Connection Whitelated Domains PassiveID Groups Attributes Advanced Settings	
API Providers SPAN	* Juin Point Name PassivaD-AD ()	
Syslog Providers Mapping Filters	* Active Directory surendrr/lab.local	
Endpoint Probes	+ John + Leave 🚊 Test User 🗶 Disposeds Test 🧭 Referent Table	
	ISE Node ISE Node R. Status Domain Controller Site	
	C SESCLADIT suveroficial toxis PRIMARY BODING White Sections With 2017(2),2006 surrants. Default Prist-Sec Tame	
	C SESSLAR 2 avends tab total SECONDARY 2 Constraint With-4ECA033.004 avenues. University of the Second	

3.必要なドメインコントローラがAgentによって監視されているかどうかを確認しま**す。[Work** Centers] > [PassiveID] > [Providers] > [Active Directory] > [PassiveID]。

E Cisco ISE				Work C	Centers · PassiveID · Providers		Q @
Overview Providers	Subscribers Certificates	Troubleshoot Report	3				
Active Directory	Connection Whitelisted	Domains PassiveID Gro	ups Attributes Ad	Ivanced Settings			
PI Providers PAN	PassiveID Dor	nain Controllers					
Syslog Providers						Rows/Page 2 🗸 🗟 1	0 /1>> 00 4
Mapping Pitters Endpoint Probes	2 Refresh / Eds. 0 1	ash 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	PassivetDAgentPrimary		
	surendm.lab.local	WIN-4RCA093.RH8.surend.	Default-First-Site-Name	10.127.196.85	PassiveIDAgentPrimary		

4.監視対象のドメインコントローラのステータスがアップ状態であるかどうかを確認します。つ まり、[Work Centers] > [PassiveID] > [Overview] > [Dashboard]のダッシュボードで緑色にマーク されます。

≡ Cisco	ISE					Work C	enters · P	assiveID - Overview			0.050
Overview	Providers	Subscribers Cert	tificates Troubleshoot	Reports							
Introduction Dashboard		Main									
Uve Sessions		Session ()	• 💿	Providers () 2	Agents 2			Subscribers ③ 10			Ø
		PROVIDERS 0			ø	SUBSCRIBER	s 💿		0	ACTIVE SESSIONS	0
		Status Name	87/33/2009. avrendet lab local REA0933018 avrendet lab local	Agent Agent PasalvelOAgentPrimary PasalvelOAgentPrimary	Domain Domain surrendri Jab. Ioca surrendri Jab. Ioca	Name Name Ne-admin-,, Ne-admin-,, Ne-bridge,, Ne-bridg	Status Status Online Online Online Online Online Online Online	Description 		No deta available.	

5. Windowsログオンがドメインコントローラに登録されている場合に入力されるライブセッショ ンを確認しま**す。[Work Centers] > [PassivelD] > [Overview] > [Live Sessions]を選択します**。

≡ Cisco	ISE					Work Centers · Pa	ssiveID - Overviev	v						Q,	0 5	i 0
Overview	Providers	Subscribers Certificates	Troubleshoot Reports													
Introduction Dashboard											Re	hush lever s	Show Latest 20 rec	With ords ↓ La	in ist 24 ho	urs v
		🖉 Refresh 🖞 Export To 🗸													7 Filter N	
		Initiated	Updated	Session Sta	Provider	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture St	Security G	Server	Auth M.	. Auth	entica
		×				~	Endpoint ID	Identity		 Endpoint Profile 	Posture Statu	Security Grou	Server	Auth Met	h Auth	enticat
		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 20	20 18:01:03 GMT+0530 (India Stand	tand Time)										Reco	ards Shov	wn: 1

Windows Serverでのエージェントサービスの確認

1. PICエージェントがインストールされているサーバでISEPICAgentサービスを確認します。

j⊠ Task Manager File Options View				-		×
Processes Performance Users	Details	Services				
Name	PID	Description	Status	Grou	p	^
SEPICAgent	9392	Cisco ISE PassivelD 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			
🖓 VaultSvc	724	Credential Manager	Running			
🔍 UI0Detect		Interactive Services Detection	Stopped			
🔍 UevAgentService		User Experience Virtualization Service	Stopped			
🔍 TrustedInstaller		Windows Modules Installer	Stopped			
CarlieringEngineService		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 | Several Open Services