在ISE上配置外部系統日誌伺服器

目錄

箇小

必要條件

屬求

聚用元件

訂景資訊

訂最直端目誌記錄目標(UDP Syslog)

範別

配置直話記錄類別下的遠端目標

瞭解類別

核驗和払障排除

簡介

本文檔介紹如何在ISE上配置外部系統日誌伺服器。

必要條件

需求

思科建議您瞭解以下主題:

- 身份服務引擎(ISE)。
- 系統日誌伺服器

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 身分辨識服務引擎(ISE) 3.3版。
- Kiwi Syslog伺服器v1.2.1.4

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。

背景資訊

來自ISE的系統日誌消息由日誌收集器收集和儲存。這些日誌收集器被分配給監控節點,以便

MnT在本地儲存所收集的日誌。

要收集外部日誌,需要配置外部系統日誌伺服器,這些伺服器稱為目標。日誌分為各種預定義的類 別。

您可以透過編輯與其目標、嚴重性級別相關的類別來自定義日誌記錄輸出。

組態

您可以使用Web介面建立要將系統日誌消息傳送到其中的遠端系統日誌伺服器目標。日誌消息根據 syslog協定標準傳送到遠端syslog伺服器目標(請參閱RFC-3164)。

配置遠端日誌記錄目標(UDP Syslog)



在思科ISE GUI中,點選選單圖示(__________)並選擇管理>系統>記錄>遠端記錄目標>點選增加。



注意:此配置示例基於名為「配置遠端日誌記錄目標」的螢幕快照。

- 名稱為Remote_Kiwi_Syslog,您可以在此輸入遠端Syslog伺服器的名稱,此名稱用於說明目 的。
- 目標型別為UDP Syslog,在此配置示例中,使用的是UDP Syslog;但您可以從目標型別下拉 選單配置更多選項:

UDP Syslog:用於透過UDP傳送Syslog消息,適用於輕量級和快速日誌記錄。

TCP系統日誌:用於透過TCP傳送系統日誌消息,它透過錯誤檢查和重傳功能提供可靠性。

安全系統日誌:是指使用TLS加密透過TCP傳送的系統日誌消息,確保資料完整性和機密性。

- Status為Enabled,您必須從Statusdrop下拉選單中選擇Enableders。
- 摘要,您可以選擇性地輸入新目標的簡短摘要。
- 主機/IP地址,此處輸入儲存日誌的目標伺服器的IP地址或主機名。思科ISE支援IPv4和IPv6格



注意:必須說明的是,如果要配置帶FQDN的系統日誌伺服器,則必須設定DNS快取以避免 對效能產生影響。如果沒有DNS快取,ISE會在每次必須將系統日誌資料包傳送到配置了 FQDN的遠端日誌記錄目標時查詢DNS伺服器。這會對ISE效能產生嚴重影響。

在部署的所有PSN中使用service cache enable命令可解決此問題:

範例

ise/admin(config)# service cache enable hosts ttl 180

• 埠為514,在此配置示例中,Kiwi Syslog伺服器偵聽埠514,這是UDP syslog消息的預設埠。 但是,使用者可以將此埠號 更改為1到65535之間的任意值。請確保您的所需埠未被任何防火牆阻止。

• Facility Code as LOCAL6,您可以從下拉選單中選擇必須用於日誌記錄的Syslog裝置代碼。有效選項為Local0到Local7。

• Maximum Length為1024,您可以在此處輸入遠端日誌目標消息的最大長度。 最大長度設定為1024,預設情況下為ISE 3.3版本,值為200到1024位元組。



注意:為避免將截斷的消息傳送到遠端日誌記錄目標,您可以將「最大長度」修改為「8192」。

• Include Alarms For this Target,為了使其簡單,在此配置示例中,未選中Include Alarms For this Target;但是,當您選中此覈取方塊時,也會將警報消息傳送到遠端伺服器。

• Compliance to RFC 3164已選中,當您選中此覈取方塊時,即使使用了反斜線(\),傳送到遠端伺服器的系統日誌消息中的 分隔符(,; { } \ \ \)也不會被轉義。

配置完成後,按一下Save。

•

٠

儲存後,系統將顯示以下警告:您已選擇建立到伺服器的不安全(TCP/UDP)連線。是否確實要繼續?,請按一下Yes。

	diale Identity Services E	Engine				Adr			Q	۵	?	¢			
щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
	Dashboard	Log Settings				> Remote_Kiwi_Syslog									
망	Context Visibility	Remote Logging	a Targets	Loggin	g Target										
×	Operations	Message Catalo	ines ig												
Ð	Policy	Collection Filter	s	* Name		Remote_Ki	iwi_Syslog	Target Type	UDP SysLog						
20	Administration			Descrip	ition	Remote Log	iging Target	Status	Z Enabled 🗸						
កា	Work Centers			* Host	/ IP Address	10.:									
				* Port		514		(Valid Range 1	to 65535)						
?	Interactive Help			Facility	Code	LOCAL6									
				* Maxin	num Length	1024		(Valid Range 2	200 to 8192)						
				Include	Alarms For this	Target 🗌									
				Comply	to RFC 3164	0									
												Save			

設定遠端目標

配置日誌記錄類別下的遠端目標

思科ISE將可審計事件傳送到系統日誌目標。配置遠端日誌記錄目標後,您需要將遠<mark>端日誌記錄目標</mark>對映到所需的類別以轉發可審計 的事件。

然後,日誌記錄目標可以對映到這些日誌記錄類別中的每一種。 這些日誌類別中的事件日誌僅從PSN節點生成,可以配置為將相關日 誌傳送到遠端系統日誌伺服器,具體取決於這些節點上啟用的服務:

AAA稽核

•

•

計量

•

•

外部MDM

•

被動Id

•

狀態和客戶端調配稽核

• 狀態與使用者端布建診斷

• 效能評測器

這些日誌類別中的事件日誌從部署中的所有節點生成,可以配置為將相關日誌傳送到遠端系統日誌伺服器:

行政和業務審計

•

•

•

系統診斷

系統統計資料

在此配置示例中,您將在四個日誌記錄類別下配置遠端目標,這三個Logging Categories用於傳送身份驗證流量日誌:**Passed** Authentications、Failed Attempts和Radius Accounting,此類別用於ISE管理員日誌記錄流量:



注意:此配置示例基於名為「配置遠端日誌記錄目標」的螢幕快照

在思科ISE GUI中,點選選單圖示(



)並選擇Administration>System>Logging>Logging Categories,然後點選所需類別(Passed Authentications、Failed Attempts和 Radius Accounting)。

步驟1-日誌嚴重性級別:事件消息與嚴重性級別相關聯,允許管理員過濾消息並排定其優先順序。根據需要選擇日誌嚴重性級別。 對於某些日誌記錄類別,預設情況下會設定此值,您無法對其進行編輯。對於某些日誌記錄類別,您可以從下拉選單中選擇以下嚴 重性級別之一:

嚴重:緊急程度。此級別意味著您不能使用Cisco ISE,您必須立即採取必要的操作。

錯誤:此層次表示嚴重錯誤情況。

•

•

•

٠

WARN:此級別指示正常但重要的情況。這是為許多記錄類別設定的預設級別。

INFO:此級別表示參考消息。

DEBUG:此級別指示診斷錯誤消息。

•

第2步-本地日誌記錄:此覈取方塊用於啟用本地日誌生成。這意味著PSN生成的日誌也儲存在生成日誌的特定PSN上。我們建議保留 預設配置

步驟3 -目標:此區域允許您選擇日誌記錄類別的目標,方法是使用左箭頭和右箭頭圖示在Availabledarea和Selectedarea之間傳輸目標 。

Availablearea包含現有的日誌記錄目標,既包括本地目標(預定義),也包括外部目標(使用者定義)。

Selectedarea (最初為空白)接著會顯示已為該類別選擇的目標。

第4步-重複第1步到第3步,在嘗試失敗和Radius記帳類別下增加遠端目標。

	dentity Services	Engine			Administration / System											
μ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrad	e Health Checks	Backup & Restore	Admin Access	Settings					
	Dashboard	Log Settings	Targate			Passed Authentications										
喝	Context Visibility	Logging Categor	ries	Logging	ing Category											
×	Operations	Message Catalo	9	Name	Pa	essed Authentications										
U	Policy	Collection Filters	s	Log Sever	ity Level IN	NFO										
20	Administration				(1	Log level can not be cha	inged.)									
តា	Work Centers			Local Log	ging											
				Targets	A	vailable:	S	Selected:								
0	Interactive Heln							LogCollector								
0								ProfilerRadiusProbe								
								Kelilote_Kiwi_Oyslog								
												Save				

將遠端目標對映到目標類別

第5步-驗證您的遠端目標是否在所需類別下。您必須能夠看到您剛剛增加的遠端目標。

在此螢幕截圖中,您可以看到對映到所需類別的遠端目標Remote_Kiwi_Syslog。

	diala Identity Services E	Engine										Administration /	System	
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & R	estore A	dmin Access	Settings		
	Dashboard Context Visibility	Log Settings Remote Logging Logging Categor	Targets	Logg	ogging Categories									
~ 0	Policy	Message Catalog Collection Filters	9											
3.	Administration				Parent Catego	ry .	Ca	itegory	Target	ts			Severity	Local Log
	Wark Capitara			0	AAA Audit				LogCi	ollector			INFO	enable
	work centers			0					LogCi	ollector,Profiler	RadiusProbe,Rem	ote_Kiwi_Syslog	INFO	enable
				0					LogCi	ollector,Profiler	RadiusProbe,Rem	ote_Kiwi_Syslog	INFO	enable
	Interactive Help			0	AAA Diagnosti	cs			LogCi	ollector			WARN	enable
				0									WARN	enable
				0									WARN	enable
				0									WARN	enable
				0									WARN	enable
				0					LogC	ollector			WARN	enable
				0					LogCi	ollector			INFO	enable
				0					LogCi	ollector			INFO	enable
				0					LogCi	ollector			INFO	enable
				0					LogCi	ollector			WARN	enable
				0	ACI Binding				LogCi	ollector			INFO	enable
				0	Accounting				LogCi	ollector			INFO	enable
				0					LogCo	ollector,Profiler	RadiusProbe,Rem	ote_Kiwi_Syslog	INFO	enable
				0					LogC	ollector			INFO	enable
				0	Administrative	and Operational Audit			Audit LogCi	ollector,Remote	e_Kiwi_Syslog		INFO	enable
				0	External MDM				LogC	ollector			INFO	enable
				0	PassiveID				LogC	ollector			INFO	enable
				0	Posture and Cl	ient Provisioning Audi			Audit Profile	erRadiusProbe,	LogCollector		INFO	enable
				0	Posture and Cl	ient Provisioning Diag	nostics Po		Diagno LogCe	ollector			WARN	enable
				0	Profiler				LogC	ollector			INFO	enable
				0	System Diagno	stics			LogCi	ollector			WARN	enable
				0									WARN	enable
				0									WARN	enable
				0					LogC	ollector			INFO	enable
				0					LogCi	ollector			INFO	enable
				0	System Statisti	ics			LogC	ollector			INFO	enable

驗證類別

瞭解類別

當事件發生時,會產生訊息。從多個工具(如核心、郵件、使用者級別等)生成了不同型別的事件消息。

這些錯誤在報文目錄中進行了分類,並且這些事件也按層次進行了分類。

這些類別具有包含一個或多個類別的父類別。

父類別	類別
AAA稽核	AAA稽核
	失敗的嘗試
	透過驗證
AAA診斷	AAA診斷
	管理員驗證與授權

	驗證流程診斷
	辨識存放區診斷
	原則診斷
	Radius診斷
	訪客
計量	計量
	RADIUS 計量
行政和業務審計	行政和業務審計
狀態和客戶端調配稽核 	狀態和客戶端調配稽核
狀態與使用者端布建診斷 	狀態與使用者端布建診斷
效能評測器	效能評測器
系統診斷	系統診斷
	分散式管理
	內部作業診斷
系統統計資料	系統統計資料

在此螢幕截圖中,可以看到Guest是消息類並分類為Guest類別。 此訪客類別有一個稱為AAA Diagnostics的父類別。

≡	dentity Services	Engine								(Administration / System			
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings			
ः हा *	Dashboard Context Visibility Operations	Log Settings Remote Logging Logging Categor Message Catalog	Targets ries	Mess	age Ca	atalog								
0	Policy	Collection Filters		Export Category	/ Name			Message Class	Message Code	Message Text		Message Description	Severity	
(2)	Administration			gues										
កា	Work Centers			Guest				Guest	86001	Guest user ha	s entered the guest portal login page	Guest user has entered the guest portal login page	INFO	
				Guest				Guest	86002	Sponso Guest	t user has entered the guest portal login page	Sponsor has suspended a guest user account	INFO	
?	Interactive Help			Guest				Guest	86003	Sponsor has e	nabled a guest user account	Sponsor has enabled a guest user account	INFO	
				Guest				Guest	86004	Guest user ha	s changed the password	Guest user has changed the password	INFO	
				Guest				Guest	86005	Guest user ha	s accepted the Use Policy	Guest user has accepted the use policy	INFO	
				Guest				Guest	86006	Guest user ac	count is created	Guest user account is created	INFO	
				Guest				Guest	86007	Guest user ac	count is updated	Guest user account is updated	INFO	
				Guest				Guest	86008	Guest user ac	count is deleted	Guest user account is deleted	INFO	
				Guest				Guest	86009	Guest user is	not found	Guest user record is not found in the database	INFO	
				Guest				Guest	86010	Guest user au	thentication failed	Guest user authentication failed. Please check your password and account permis	INFO	
				Guest				Guest	86011	Guest user is	not enabled	Guest user authentication failed. User is not enabled. Please contact your system	INFO	
				Guest				Guest	86012	User declined	Access-Use Policy	Guest User must accept Access-Use policy before network access is granted	INFO	
				Guest				Guest	86013	Portal not four	d	Portal is not found in the database. Please contact your system administrator	INFO	
				Guest				Guest	86014	User is susper	nded	User authentication failed. User account is suspended	INFO	
				Guest				Guest	86015	Invalid Passwo	ord Change	Invalid password change. Use correct password based on the password policy	INFO	
				Quest				Quarte	96016	Quest Timonu	Eveneded	Timoout from conversion are exceeded the threshold. Disease contact your system ode	INFO	

訊息目錄

檢驗和故障排除

對遠端日誌記錄目標執行TCP轉儲是確認是否傳送日誌事件的最快的故障排除和驗證步驟。

捕獲必須來自對使用者進行身份驗證的PSN,因為PSN將生成日誌消息,並且這些消息將傳送到遠端目標



在思科ISE GUI中,點選選單圖示(

),然後選擇操作>故障排除>TCP轉儲>點選增加。

- 您必須過濾流量,請增加ip host <remote_target_IP_addres> filter欄位。
- 您必須從PSN獲取處理身份驗證的捕獲。

≡	dentity Services	Engine	Operations / Troubleshoot	
Щ	Bookmarks	Diagnostic Tools Download Lo	gs Debug Wizard	
	Dashboard	General Tools 🗸 🗸	TOP Dump X New	
망 (~~	Context Visibility	RADIUS Authentication Troubl Execute Network Device Com	Add TCP Dump	
	Policy	Evaluate Configuration Validat Posture Troubleshooting	Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.	
\$ 0	Administration	Agentiess Posture Troublesho	SSPT33A	
កា	Work Centers	EndPoint Debug TCP Dump	Network Instringer	
		Session Trace Tests	GigabitEthernet 0 [Up, Running] 🗸 🔘	
?	Interactive Help	TrustSec Tools	Filter	
			fe host 10.20	
			E gip host 10.77.122.123 and not 10.177.122.119	
			File Name Remote Syslog Server Test	
			Repository 0	
			File Size 0 10 0	
			1 File(a)	
			Tins Lint 0	
			Minute(s)	
			Promiscuous Mode	
			Cancel Save and Run	

TCP傾印

在此螢幕截圖中,您可以看到ISE如何為ISE管理員日誌記錄流量傳送系統日誌消息。

•••																SSPT33A_GigabitEthernet 5.pcap
📕 🔳 ,	<u>í</u>		1 🔀	6	् 🖕	-	2	ি	<u> </u>	-		Ð,	Q	Q	•••	
Apply a dis	splay filter ·	<\$\$/>														
No. - 1 3 4 5 6 7 8 9 10 11 - 12	Time 2024-07-22 2024-07-22 2024-07-22 2024-07-22 2024-07-22 2024-07-22 2024-07-22 2024-07-22 2024-07-22 2024-07-22 2024-07-22 2024-07-25	i 10:29: i 10:29: i 10:32: i 10:32:	37, 23544 49, 05529 0, 55929 12, 79647 81, 21778 10, 38353 10, 38356 10, 38376 10, 38387 10, 38394 10, 38405	Source 1 10.2 4 10.2 3 10.2 9 10.2 8 10.2 8 10.2 8 10.2 8 10.2 10.2 8 10.2	20 01.231. 01.231. 01.231. 01.231. 01.231. 01.231. 01.231. 01.231. 01.231. 01.231. 01.231. 01.231. 01.231.	57 57 57 90 57 57 57 57 57 57 57	I	Desti 10.2 10.2 10.2 10.2 10.2 10.2 10.2 10.2	nation (01.23 (01.23) (01.23) (01.23) (01.23) (01.23) (01.23) (01.23) (01.23) (01.23) (01.23)	1.90 1.90 1.90 1.95 1.90 1.90 1.90 1.90 1.90 1.90		Protoc Syslo Syslo Syslo Syslo Syslo Syslo Syslo Syslo Syslo	ol 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	Leng	th 385 423 385 423 520 519 516 516 528 517 505	<pre>Info DCGALE.NUTICE: JUL 25 11:29:37 SSFT33A CISE_dministrative_and_Operational_Audit 000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012091 DCGALE.NUTICE: JUL 25 11:29:40 SSFT33A CISE_dministrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:29:00.05 -05:00 0000012093 DCGALE.NUTICE: JUL 25 11:31:05 SSFT33A CISE_dministrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:31:02.766 -05:00 0000012093 DCGALE.NUTICE: JUL 25 11:32:10 SSFT33A CISE_dministrative_and_Operational_Audit 0000000023 1 0 2024-07-25 11:32:02.058 -05:00 0000012093 DCGALE.NUTICE: JUL 25 11:32:10 SSFT33A CISE_dministrative_and_Operational_Audit 0000000025 1 0 2024-07-25 11:32:03.28 -05:00 0000012093 DCGALE.NUTICE: JUL 25 11:32:10 SSFT33A CISE_dministrative_and_Operational_Audit 0000000005 1 0 2024-07-25 11:32:03.38 -05:00 0000012093 DCGALE.NUTICE: JUL 25 11:32:10 SSFT33A CISE_dministrative_and_Operational_Audit 000000000000000000000000000000000000</pre>
<pre>> Frame 1: > Ethernet</pre>	: 385 bytes t II, Src:	s on wir VMware_	e (3080 a5:46:12	bits), (00:5	385 by 0:56:a5:	es ca 46:12	ptured), Ds1	d (30 t: V№	980 bi Mare_	ts) a5:e5:	:86 (0	0:50:5	56:a5	:e5:86		
> Internet	t Protocol	Version	4, Src:	10.20	1.231.6	, Dst	: 10.2 14	201.2	231.90							
v dser bat (trunca 1011 ····· v Messa Sys Sys Sys	ated]Syslog 0 = Fac .101 = Lev ge [trunca slog times' slog hostna slog proces	ility: I el: NOT ted]: Ju tamp (RF ame: SSP ss id: C ge id [t	e: LOCAL OCAL6 - ICE - nor IL 25 11: C3164): T33A ISE runcated	6.NOTI reserv mal bu 29:37 Jul 25]: _Ad	, Dst Fo CE: Jul ved for it signi SSPT33A 11:29: ministra	25 11 local ficant CISE_ 37	:29:37 use (cond Admin	7 SSF (22) litio histr	PT33A n (5) ative_ tional	CISE_/	Admini perat	ional_	ive_a Audit 0 1 0	nd_0pe : 0000 2024-	eratio 000020	nal_Audit 000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersio 0 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, AdminInter 5 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, AdminInterface=GUI, Admini

系統日誌流量

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。