在ISE上配置外部系统日志服务器

目录

箇小

先决条件

要求

使用的组件

打量信息

配置远程日志记录目标(UDP系统日志))

示例

在Logging Categories下配置远程目标

了解类別

检验和故障排除

简介

本文档介绍如何在ISE上配置外部系统日志服务器。

先决条件

要求

Cisco 建议您了解以下主题:

- 身份服务引擎(ISE)。
- 系统日志服务器

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 身份服务引擎(ISE) 3.3版本。
- Kiwi Syslog Server v1.2.1.4

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

ISE中的系统日志消息由日志收集器收集和存储。这些日志收集器被分配给监控节点,因此MnT在

本地存储收集的日志。

要收集外部日志,您需要配置外部系统日志服务器,这些服务器称为目标。日志可分为各种预定义 类别。

您可以通过编辑与其目标、严重性级别等相关的类别来自定义日志记录输出。

配置

可以使用Web界面创建系统日志消息发送到的远程系统日志服务器目标。日志消息根据系统日志协 议标准发送到远程系统日志服务器目标(请参阅RFC-3164)。

配置远程日志记录目标(UDP Syslog)



在思科ISE GUI中,点击Menuicon(

)并选择Administration>System>Logging>Remote Logging Targets >点击Add。



注意:此配置示例基于名为"配置远程日志记录目标"的屏幕快照。

- 名称为Remote_Kiwi_Syslog,您可以在此处输入远程Syslog服务器的名称,此名称用于说明目的。
- 目标类型为UDP Syslog,在此配置示例中,使用了UDP Syslog;但是,您可以从Target Type下拉列表配置更多选项:

UDP系统日志:用于通过UDP发送系统日志消息,适用于轻量级和快速日志记录。

TCP系统日志:用于通过TCP发送系统日志消息,通过错误检查和重传功能提供可靠性。

安全系统日志:是指通过TCP和TLS加密发送的系统日志消息,确保数据完整性和机密性。

- 状态为已启用,必须从状态下拉列表中选择已启用。
- 说明,(可选)您可以输入新目标的简要说明。
- Host / IP Address,在这里输入存储日志的目标服务器的IP地址或主机名。Cisco ISE支持

IPv4和IPv6格式的日志记录。



注意:必须指出的是,如果要使用FQDN配置系统日志服务器,则必须设置DNS缓存以避免 对性能产生影响。如果没有DNS缓存,每次必须将系统日志数据包发送到配置了FQDN的远 程日志记录目标时,ISE都会查询DNS服务器。这会对ISE性能产生严重影响。

在部署的所有PSN中使用service cache enable命令可克服此问题:

示例

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

• 端口作为514,在此配置示例中,Kiwi Syslog服务器在侦听端口514,该端口是UDP syslog消息的默认端口。但是,用户可以将此端口号更改为1到65535之间的任何值。请确保所需的端口未被任何防火墙阻止。

• Facility Code 作为LOCAL6,您可以从下拉列表中选择必须用于日志记录的Syslog设备代码。有效选项为Local0到 Local7。

• Maximum Length为1024,您可以在此处输入远程日志目标消息的最大长度。默认情况下,最大长度设置为1024 ISE 3.3版本,值介于200到1024字节之间。



注意:为避免将截断的消息发送到远程日志记录目标,您可以将Maximum Length修改为8192。

• Include Alarms For This Target(为了使其简单),在此配置示例中,未选中Include Alarms For this Target;但是,选中此复选框时,也会将警报消息发送到远程服务器。

• Compliance to RFC 3164已选中,当您选中此复选框时,即使使用反斜线(\),也不会转义发送到远程服务器的系统日志消息中的定界符(,; { } \ \ \)。

完成配置后,单击Save。

•

•

保存后,系统将显示以下警告:您已选择创建与服务器的不安全(TCP/UDP)连接。是否确定要继续?,请单击Yes。

	diada Identity Services	Engine				Adn			Q	۵	?	Q			
щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
20 	Dashboard	Log Settings	Targets			> Remote_Kiwi_Syslog									
*	Operations	Logging Categor Message Catalo	ries g	Loggi	ng Target	Pemote Ki	wi Svelog	Target Type	UDP Svel og						
0	Policy Administration	Collection Filters		Desc	iption	Remote Log	ging Target	Status	Z Enabled V						
	Work Centers			* Hos	t / IP Address	10.1	-								
?	Interactive Help			* Port	y Code	514 LOCAL6		(Valid Range 1	to 65535)						
				* Max	imum Length	1024		(Valid Range 2	200 to 8192)						
				Inclue	le Alarms For this	Target 🗌									
												Save	J	Re	

配置远程目标

在Logging Categories下配置远程目标

思科ISE将可审核事件发送到系统日志目标。配置远程日志记录目标后,您需要将远程日志记录目标映射到所需的类别以转发可审核 的事件。

然后,日志记录目标可以映射到这些日志记录类别中的每一项。 这些日志类别中的事件日志只能从PSN节点生成,并且可以根据这些 节点上启用的服务,配置为将相关日志发送到远程系统日志服务器:

AAA审核

•

记账

•

• 外部MDM

.

被动ID

•

状态和客户端调配审核

• 状态和客户端调配诊断

• 分析器

这些日志类别中的事件日志是从部署中的所有节点生成的,可以配置为将相关日志发送到远程系统日志服务器:

行政和业务审计

•

•

•

系统诊断

系统统计信息

在此配置示例中,您将在四个日志记录类别下配置远程目标,这三个类别将发送身份验证流量日志:Passed Authentications、Failed Attempts和Radius Accounting,以及该类别用于ISE管理员日志记录流量:



注意:此配置示例基于名为"配置远程日志记录目标"的屏幕快照

在思科ISE GUI中,点击Menuicon(



)并选择Administration>System>Logging>Logging Categories,然后点击所需类别(Passed Authentications、Failed Attempts和 Radius Accounting)。

第1步-日志严重性级别:事件消息与严重性级别相关联,允许管理员过滤消息并设置其优先级。 根据需要选择日志严重性级别。 对 于某些日志记录类别,该值默认设置,您无法编辑它。对于某些日志记录类别,您可以从下拉列表中选择以下严重性级别之一:

FATAL:紧急级别。此级别表示您不能使用思科ISE,您必须立即采取必要的操作。

ERROR:此级别指示严重错误情况。

٠

٠

٠

.

WARN:此级别指示正常但重要的情况。这是为许多日志记录类别设置的默认级别。

INFO:此级别表示参考消息。

DEBUG:此级别指示诊断漏洞消息。

第2步-本地日志记录:此复选框启用本地日志生成。这意味着PSN生成的日志也保存在生成日志的特定PSN上。我们建议保留默认配 置

第3步-目标:此区域允许您选择日志记录类别的目标,方法是使用左箭头和右箭头图标在Availableand和Selectedareas之间传输目标。 Availablearea包含现有的日志记录目标,本地(预定义)和外部(用户定义)。

Selectedarea最初为空,然后显示为类别选定的目标。

第4步-重复第1步到第3步,在Failed Attempts and Radius Accounting类别下添加远程目标。

	dentity Services	Engine				Adm	inistration /	' System				Q	۵
ĮĮ	Bookmarks	Deployment	Licensing	Certificates Lo	ogging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings		
	Dashboard Context Visibility Operations Policy	Log Settings Remote Logging (Logging Categor Message Catalor Collection Filters	Targets ries g	Logging Categorie Logging Cat Name Log Severity I	es List > egory Pa Level	Passed Authentications assed Authentications NFO							
-	Work Centers			Local Logging Targets	(I 9 Av	Log level can not be cha	nged.) Selec	cted:					
?	Interactive Help						 > 	ogCollector rofilerRadiusProbe emote_Klwi_Syslog					
												Save	

将远程目标映射到目标类别

第5步-验证远程目标是否位于所需的类别下。您必须能够看到刚刚添加的远程目标。

在此屏幕截图中,您可以看到远程目标Remote_Kiwi_Syslog映射到所需的类别。

	alialia Identity Services E	Engine									(Administration /	System	
Щ	Bookmarks	Deployment	Licensing C	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup	& Restore	Admin Access	Settings		
	Dashboard Context Visibility Operations	Log Settings Remote Logging Ta Logging Categories Message Catalog Collection Filters	irgots	Logg Ø Edit	gging Categories									
	Policy				Parent Categor	γ	Ca	ategory	т	argets			Severity	Local Log
20	Administration			0	AAA Audit					LogCollector			INFO	enable
ก็เ	Work Centers			0						LogCollector,Pro	ofilerRadiusProbe,Ren	note_Kiwi_Syslog	INFO	enable
				0					L	LogCollector,Pro	ofilerRadiusProbe,Ren	note_Kiwi_Syslog	INFO	enable
	Interactive Help			0	AAA Diagnosti	:5				LogCollector			WARN	enable
				0									WARN	enable
				0									WARN	enable
				0									WARN	enable
				0									WARN	enable
				0						LogCollector			WARN	enable
				0						LogCollector			INFO	enable
				0						LogCollector			INFO	enable
				0						LogCollector			INFO	enable
				0						LogCollector			WARN	enable
				0	ACI Binding					LogCollector			INFO	enable
				0	Accounting					LogCollector			INFO	enable
				0					L	LogCollector,Pro	ofilerRadiusProbe,Ren	note_Kiwi_Syslog	INFO	enable
				0						LogCollector			INFO	enable
				0	Administrative	and Operational Audi	t Ad	dministrative and Operational	Audit L	LogCollector,Rei	mote_Kiwi_Syslog		INFO	enable
				0	External MDM					LogCollector			INFO	enable
				0	PassiveID					LogCollector			INFO	enable
				0	Posture and Cli	ent Provisioning Aud			Audit F	ProfilerRadiusPr	obe,LogCollector		INFO	enable
				0	Posture and Cli	ient Provisioning Diag	nostics Po			LogCollector			WARN	enable
				0	Profiler					LogCollector			INFO	enable
				0	System Diagno	stics				LogCollector			WARN	enable
				0									WARN	enable
				0									WARN	enable
				0						LogCollector			INFO	enable
				0						LogCollector			INFO	enable
				0	System Statisti	cs				LogCollector			INFO	enable

检验类别

了解类别

事件发生时生成消息。从多个工具(如内核、邮件、用户级别等)生成的事件消息有不同类型的生成。

这些错误在消息目录中进行分类,这些事件也按层次进行分类。

这些类别的Parent Categories包含一个或多个类别。

父类别	分类
AAA审核	AAA审核
	失败的尝试
	通过身份验证
AAA诊断	AAA诊断
	管理员身份验证和授权

	身份验证流诊断
	身份库诊断
	策略诊断
	Radius诊断
	访客
记账	记账
	RADIUS 记帐
行政和业务审计	行政和业务审计
状态和客户端调配审核	状态和客户端调配审核
状态和客户端调配诊断	状态和客户端调配诊断
分析器	分析器
系统诊断	系统诊断
	分布式管理
	内部运行诊断
系统统计信息	系统统计信息

在此屏幕截图中,您可以看到访客是消息类并分类为访客类别。 此访客类别有一个称为AAA诊断的父类别。

Ξ	ender Identity Services F	Engine								(Administration / System			ļ
ļ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings			
Ξ:	Dashboard	Log Settings		Mess	ane Ca	atalog								
12	Context Visibility	Logging Categor	ries	11000	uge or	itulog								
*	Operations	Message Catalog												
- 0	Policy	Collection Filters							N 0			Name Baradadar		
	o Administration			Category	/ Name			Message Class	Message Code	Message lext		Message Description	Seventy	
ភា	Work Centers			99969				<u> </u>						
				Guest				Guest	86001	Guest user hat	s entered the guest portal login page	Guess user has entered the guest portal login page		
(?	Interactive Help			Guest				Guest	86003	Sponsor has e	user has entered the guest portal login page	Sponsor has enabled a quest user account	INFO	
				Guest				Guest	86004	Guest user has	s changed the password	Guest user has changed the password	INFO	
				Guest				Guest	86005	Guest user has	s accepted the Use Policy	Guest user has accepted the use policy	INFO	
				Guest				Guest	86006	Guest user act	count is created	Guest user account is created	INFO	
				Guest				Guest	86007	Guest user act	count is updated	Guest user account is updated	INFO	
				Guest				Guest	86008	Guest user act	count is deleted	Guest user account is deleted	INFO	
				Guest				Guest	86009	Guest user is r	not found	Guest user record is not found in the database	INFO	
				Guest				Guest	86010	Guest user aut	thentication failed	Guest user authentication failed. Please check your password and account permis	. INFO	
				Guest				Guest	86011	Guest user is r	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	nd	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	Change	Invalid password change. Use correct password based on the password policy	INFO	
										The second se		the thread of the second	and the second se	

邮件目录

检验和故障排除

对远程日志记录目标执行TCP转储是确认是否发送日志事件的最快故障排除和验证步骤。

捕获必须来自对用户进行身份验证的PSN,因为PSN将生成日志消息,这些消息将发送到远程目标



在思科ISE GUI中,点击Menuicon (

)并选择Operations> Troubleshoot> TCP Dump>点击Add。

- 您必须过滤流量,添加ip host <remote_target_IP_addres> filter字段。
- 您必须从PSN处理身份验证中获取捕获。

≡	alialia Identity Services	Engine	Operations / Troubleshoot
Щ	Bookmarks	Diagnostic Tools Download Lo	ogs Debug Wizard
55	Dashboard		
명	Context Visibility	General Tools ~	10 ² bung / New
X	Operations	Execute Network Device Com	Add TCP Dump
	Policy	Evaluate Configuration Validat	Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.
		Posture Troubleshooting Agentiess Posture Troublesho	fiet Starsa
#0	Administration	- EndPoint Debug	
-fil	Work Centers	TCP Dump	Network Inserface
		Session Trace Tests	GigabilEthernet 0 (Up, Running) 🗸 🕐
?	Interactive Help	TrustSec Tools	
			Eg: is host 10.77.122.123 and not
			Finitume Section Server Test
			Repository
			File State
			Mb
			File(s)
			Time Linit
			5
			Promiscuous Mode
			Cancel Save and Run

TCP转储

在此屏幕截图中,您可以看到ISE如何为ISE管理员日志记录流量发送系统日志消息。

•	• •																								SSPT33A_GigabitEthernet 5.pcap	
4	[🗖		6)			×	6		R 1	(⇒	2	6	• 1	- €				Ð, (e,	Q				
	Apply :	ı dist	lay filte	< <	3\$/>																					
		1 2 2 3 4 2 5 2 5 2 5 2 5 2 5 2 5 2 5 2 5 2 5 2	ime 024-07 024-07 024-07 024-07 024-07 024-07 024-07 024-07 024-07 024-07 024-07 024-07	7-25 7-25 7-25 7-25 7-25 7-25 7-25 7-25	10:2 10:3 10:3 10:3 10:3 10:3 10:3 10:3 10:3	29:37 29:49 10:00 11:12 22:01 22:10 22:10 22:10 22:10 22:10 22:10 22:10	.2354 .0565 .5592 .7964 .2177 .3835 .3836 .3837 .3838 .3838 .3838 .3839 .3840	S 41 1 94 1 93 1 73 1 80 1 30 1 68 1 66 1 97 1 78 1 45 1 55 1	Gource (0.20) (0.20) (0.20) (0.20) (0.20) (0.20) (0.20) (0.20) (0.20) (0.20) (0.20) (0.20) (0.20) (0.20) (0.20)	11.23 11.23 11.23 11.23 11.23 11.23 11.23 11.23 11.23 11.23 11.23 11.23 11.23 11.23	1.67 1.67 1.67 1.67 1.67 1.67 1.67 1.67			Des 10. 10. 10. 10. 10. 10. 10. 10. 10.	tinat 201 201 201 201 201 201 201 201 201 201	tion .231. .231. .231. .231. .231. .231. .231. .231. .231. .231. .231.	.90 .90 .90 .90 .95 .90 .90 .90 .90 .90 .90		Pro Sys Sys Sys Sys Sys Sys Sys Sys Sys Sys	tocol alog alog alog wyser alog alog alog alog alog alog alog alog	 	Lengt	h 385 423 385 423 243 520 519 516 516 528 517 505	Info LOCALI LOCALI LOCALI Host J LOCALI LOCALI LOCALI LOCALI LOCALI LOCALI	6.NOTICE: Jul 25 11:29:37 SSPT33A CISE_Administrative_and_Operational_Audit 000000020 1 0 2024-07-25 11:29:37.234 -05:00 00000 6.NOTICE: Jul 25 11:29:40 SSPT33A CISE_Administrative_and_Operational_Audit 0000000201 1 0 2024-07-25 11:29:40,066 -05:00 00000 6.NOTICE: Jul 25 11:31:00 SSPT33A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:32:10:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:32:10:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000022 1 0 2024-07-25 11:32:10:303 -05:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:32:10:303 -05:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:32:10:303 -05:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:32:10:303 -05:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:32:10:303 -05:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:32:10:303 -05:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:32:10:303 -05:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000022 1 0 2024-07-25 11:32:10:303 -05:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000025 1 0 2024-07-25 11:32:10:303 -05:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000025 1 0 2024-07-25 11:32:10:303 -05:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000030 1 0 2024-07-25 11:32:10:303 -05:00 0000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000003 1 0 2024-07-25 11:32:10:303 -05:00 00000 6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_A	912891 912892 912893 912895 912895 912896 912897 912898 912899 912900 912900 912902
~ ~ ~ ~ ~	Frame Ether Inter User [tru 10 V Me	1: net Data ncal 1 0 ssag Sys Sys	385 by II, Si Protor gram 1 ed]Sys = 101 = e [tru .og tin .og hos	vtes rc: \ Proto slog Faci Leve ncat mesta stnar	on w /Mwar /ersi ocol, mess (lity (l: N ed]: amp (me: S s id:	vire re_a5 ion 4 Src age: LO OTIC Jul (RFC3 SSPT3 : CIS	(3080 :46:1 , Src Port LOCA CAL6 - E - no 25 12 :164): 3A :E	bit 2 (0 : 10 : 32 L6.N - res ormal L:29: Jul	s), 201 .201 724, 0TIC serve 1 but :37 S .25	385 :56:: Dst E: Ju ed fo t sig SSPT3 11:2	oytes a5:46 .67, Port ul 25 or loo mific 3A CI 9:37	cap :12) Dst: : 51 11: :alt (SE_/	ture , Ds 10. 4 29:3 Jse (cond Admir	d (3 t: V 201. 7 SS (22) diti nist	1080 Mwa 231 SPT3 on rat:	bits re_a5 .90 33A CI (5) ive_a	s) 5:e5: ISE_A	86 () Idmin perat	00:5 istr	0:56: ative	a5:e	5:86) _Oper) 00020	al_Auc 1 0 2	dit 0000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, Config 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, Admin	Versio

系统日志流量

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。