Configure External Syslog Server on ISE

Contents

Introduction
<u>Prerequisites</u>
<u>Requirements</u>
Components Used
Background Information
Configuration
ConfiguringRemote Logging Target (UDP Syslog)
Example
Configuring Remote Target under Logging Categories
Understanding Categories
Verifying and Troubleshooting

Introduction

This document describes how to configure External Syslog Server on ISE.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Services Engine (ISE).
- Syslog Servers

Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine (ISE) 3.3 version.
- Kiwi Syslog Server v1.2.1.4

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Syslog messages from ISE are collected and stored by log collectors. These log collectors are assigned to Monitoring nodes so MnT storages the collected logs locally.

To collect logs externally, you configure external syslog servers, which are called targets. Logs are classified into various predefined categories.

You can customize logging output by editing the categories with respect to their targets, severity level, and so on.

Configuration

You can use the web interface to create remote syslog server targets to which system log messages are sent. Log messages are sent to the remote syslog server targets in accordance with the syslog protocol standard (see RFC-3164).

Configuring Remote Logging Target (UDP Syslog)



In the Cisco ISE GUI, click theMenuicon (

) and choose Administration>System>Logging>Remote Logging Targets > Click Add.



Note: This configuration example is based on screenshot named: Configuring Remote Logging Target.

- Name as Remote_Kiwi_Syslog, here you can enter the name of the Remote Syslog server, this is used for descriptive purposes.
- **Target Type** as **UDP Syslog**, in this configuration example, **UDP Syslog** is being used; however, you can configure more options from **Target Type** drop-down list:

UDP Syslog: Used for sending syslog messages over UDP, suitable for lightweight and fast logging.

TCP Syslog: Used for sending syslog messages over TCP, which provides reliability with error checking and retransmission capabilities.

Secure Syslog: it refers to syslog messages being sent over TCP with TLS encryption, ensuring data integrity and confidentiality.

- Status as Enabled, you must choose Enabled from the Status drop-down list.
- **Description**, optionally you can enter a brief description of the new target.

• Host / IP Address, here you enter the IP address or hostname of the destination server that store the logs.Cisco ISE supports IPv4 and IPv6 formats for logging.



Note: It is essential to mention that if you are going to configure a syslog server with FQDN, you must set up DNS caching to avoid impact on the performance. Without DNS caching, ISE queries DNS server each time a syslog packet has to be sent to the remote logging target configured with FQDN. This have a severe impact on ISE performance.

Use theservice cache enablecommand in all the PSN of the deployment to overcome this:

Example

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

• **Port** as **514**, in this configuration example, the Kiwi Syslog Server is listening in port **514** which is the default port for UDP syslog messages. However, users can change this port number to any value between 1 and 65535.Make sure your desired port is not being blocked by any Firewall.

- Facility Code as LOCAL6, you can choose the syslog facility code that must be used for logging, from the drop-down list. Valid options are Local0 through Local7.
- Maximum Length as 1024, here you can enter the maximum length of the remote log target messages. Maximum length is set to 1024 by default ISE 3.3 version, values are from 200 through 1024 bytes.



Note: To avoid sending truncated messages to your Remote logging Target, you can modify the Maximum Length as 8192.

- Include Alarms For this Target, to keep it simple, in this configuration example, Include Alarms For this Target is not checked; however, when you check this check box, alarm messages are sent to the remote server as well.
- Comply to RFC 3164 is checked, when you check this check box, the delimiters (, ; { } \\) in the syslog messages sent to the remote servers are not escaped even if a backslash (\) is used.
- Once configuration is finished, click on **Save**.
- Once you save, system is going to display this warning: You have chosen to create an unsecure (TCP/UDP) connection to the server. Are you sure you want to proceed?, click on Yes.

	dentity Services I	Engine					Q	۵	?	Q					
PI	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Check	s Backup & Restore	Admin Access	Settings				
5	Dashboard	Log Settings				Remote_Kiwi_Syslog									
ц <mark>в</mark>	Context Visibility	Remote Logging	Targets	Loggi	ng Target										
×	Operations	Message Catalog	3	* Nan	ne	Remote_Kiv	vi_Syslog	Target Type	UDP SysLog						
•	Policy	Collection Filters		Descr	intion	Remote Logo	ing Target	Status							
20	Administration			* Hoo	/ ID Addross	10	, ing tangot								
កា	Work Centers			HUS	I / IF Address		_								
				- Port		514		(Valid Range	(0 65535)						
(?)	Interactive Help			Facilit	y Code	LOCAL6									
				* Max	imum Length	1024		(Valid Range	200 to 8192)						
				Incluc	le Alarms For this T	arget 📃									
												Save			set

Configuring Remote Target

Configuring Remote Target under Logging Categories

Cisco ISE sends auditable events to the syslog target. Once you configured your Remote logging Target, you then need to map the **Remote Logging Target** to the intended categories to forward the auditable events.

The logging targets can then be mapped to each of these logging categories. Event logs from these log categories are generated only from PSN nodes and can be configured to send the relevant logs to the Remote Syslog server depending on the services that are enabled on those nodes:

- AAA Audit
- AAA Diagnostics
- Accounting
- External MDM
- Passive ID
- Posture and Client Provisioning Audit
- Posture and Client Provisioning Diagnostics
- Profiler

Event logs from these log categories are generated from all nodes in the deployment and can be configured to send the relevant logs to the Remote Syslog server:

- Administrative and Operational Audit
- System Diagnostics
- System Statistics

In this configuration example, you are going to configure Remote Target under four Logging Categories, these 3 to send authentication traffic logs: **Passed Authentications**, **Failed Attempts** and **Radius**

Accounting, and this category for ISE Administrator logging traffic:



Note: This configuration example is based on screenshot named: Configuring Remote Logging Target

In the Cisco ISE GUI, click theMenuicon (



) and choose Administration>System>Logging>Logging Categories, and click on the required category (Passed Authentications, Failed Attempts and Radius Accounting).

Step 1-Log Severity Level: An event message is associated with a severity level, which allows an administrator to filter the messages and prioritize it. Select the log severity level as required. For some logging categories, this value is set by default, and you cannot edit it. For some logging categories, you can choose one of the these severity levels from a drop-down list:

- **FATAL**: Emergency level. This level means that you cannot use Cisco ISE and you must immediately take the necessary action.
- ERROR: This level indicates a critical error condition.
- **WARN**: This level indicates a normal but significant condition. This is the default level set for many logging categories.
- INFO: This level indicates an informational message.
- **DEBUG**: This level indicates a diagnostic bug message.

Step 2- Local Logging: This checkbox enables the local log generation. Meaning, that the logs generated by the PSNs are saved on the specific PSN generating the log as well. We recommend to keep the default configuration

Step 3- Targets: This area allows you to choose the targets for a logging category by transferring the targets between the Available and the Selected areas using the left and right arrow icons.

TheAvailablearea contains the existing logging targets, both local (predefined) and external (user-defined).

The**Selected**area, which is initially empty, then displays the targets that have been chosen for the category.

Step 4- Repeat from step 1 to step 3 to add Remote Target under **Failed Attempts and Radius Accounting** categories.

	dentity Services	Engine				Adm	inistration /	' System				Q	۵
ĮI	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings		
≣ ।ड % ●	Dashboard Context Visibility Operations Policy	Log Settings Remote Logging Logging Categor Message Catalog Collection Filters	ries g s	Logging Categ Logging C Name Log Severi	ories List > F Category Pa: ty Level IN	Passed Authentications ssed Authentications IFO							
2 0	Administration Work Centers			Local Logg Targets	(L ing d	.og level can not be cha ailable:	nged.) Selec	:ted:					
?	Interactive Help							ogCollector rofilerRadiusProbe emote_Kiwi_Syslog				Save	

Mapping Remote Targets to intended Categories

Step 5- Verify that your Remote Target is under the required categories. You must be able to see the remote target you just added.

In this screenshot, you can see the remote target **Remote_Kiwi_Syslog** mapped to the required categories.

	dentity Services E	Ingine									(Administration /	/ System	
Щ	Bookmarks	Deployment	Licensing C	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup	& Restore	Admin Access	Settings		
52	Dashboard	Los Catilana												
	Context Visibility	Remote Logging T	largets	Logo	ing Cat	egories								
		Logging Categorie												
~	Operations	Message Catalog												
0	Policy	Collection Filters			Parent Catego	TV.	Ca	tegory	т	Targets		Severity	Local Log	
	Administration				AAA Audit				-	LogCollector			INFO	enable
	Work Centers			6						LogCollector.Pro	ofilerRadiusProbe.Rem	note Kiwi Syslog	INFO	enable
										LogCollector.Pro	ofilerRadiusProbe.Rem	note Kiwi Syslog	INFO	enable
	Interactive Help				AAA Diagnosti	cs.				LogCollector		/ - /	WARN	enable
													WARN	enable
													WARN	enable
								entity Stores Diagnostics					WARN	enable
													WARN	enable
										LogCollector			WARN	enable
										LogCollector			INFO	enable
										LogCollector			INFO	enable
				0						LogCollector			INFO	enable
				0						LogCollector			WARN	enable
				0	ACI Binding					LogCollector			INFO	enable
				0	Accounting					LogCollector			INFO	enable
				0					1	LogCollector,Pro	ofilerRadiusProbe,Rem	note_Kiwi_Syslog	INFO	enable
				0						LogCollector			INFO	enable
				0	Administrative	and Operational Audit			l Audit	LogCollector,Rei	mote_Kiwi_Syslog		INFO	enable
				0	External MDM					LogCollector			INFO	enable
				0	PassiveID					LogCollector			INFO	enable
				0	Posture and Cl	ient Provisioning Audi	t Po		g Audit I	ProfilerRadiusPr	obe,LogCollector		INFO	enable
				0	Posture and Cl	ient Provisioning Diag	nostics Po		g Diagno I	LogCollector			WARN	enable
				0	Profiler				I	LogCollector			INFO	enable
				0	System Diagno	stics			1	LogCollector			WARN	enable
				0									WARN	enable
				0									WARN	enable
				0					1	LogCollector			INFO	enable
				0					I	LogCollector			INFO	enable
				0	System Statisti	cs			1	LogCollector			INFO	enable

Verifying Categories

Understanding Categories

A message is generated when an event occurs. There are different types of event messages generated from multiple facilities such as the kernel, mail, user level, and so on.

These errors are categorized within the Message Catalog and these events also are organized hierarchically into categories.

These categories have Parent Categories containing one or some categories.

Parent Category	Category
AAA Audit	AAA Audit
	Failed Attempts
	Passed Authentication
AAA Diagnostics	AAA Diagnostics
	Administrator Authentication and Authorization

	Authentication Flow Diagnostics Identity Store Diagnostics Policy Diagnostics Radius Diagnostics Guest
Accounting	Accounting Radius Accounting
Administrative and Operational Audit	Administrative and Operational Audit
Posture and Client Provisioning Audit	Posture and Client Provisioning Audit
Posture and Client Provisioning Diagnostics	Posture and Client Provisioning Diagnostics
Profiler	Profiler
System Diagnostics	System Diagnostics Distributed Management Internal Operations Diagnostics
System Statistics	System Statistics

In this screenshot you can see that **Guest** is a Message Class and categorized as a **Guest Category**. This Guest Category has a Parent Category called **AAA Diagnostics**.

$\equiv \frac{\mathrm{diade}}{\mathrm{cisco}}$ Identity Services	Engine							Administration / System		
J Bookmarks	Deployment Licensing	Certifica	tes Logging	Maintenance	Upgrade	Health Checks	Backup & Restore Ad	min Access Settings		
Dashboard Context Visibility Operations Policy	Log Settings Renote Lopping Targets Logging Categories Massage Catalog Collection Filters	M	essage C	atalog						
Administration		Ca	itegory Name			Message Class	Message Code	Message Text	Message Description	Severity
		91	an)							
- Work Centers		G	iest			Guest	86001	Guest user has entered the guest portal login page	Guest user has entered the guest portal login page	INFO
		Gu	est			Guest	86002	Sponso Guest user has entered the guest portal login page	Sponsor has suspended a guest user account	INFO
② Interactive Help		Gu	iest			Guest	86003	Sponsor has enabled a guest user account	Sponsor has enabled a guest user account	INFO
		Gu	est			Guest	86004	Guest user has changed the password	Guest user has changed the password	INFO
		Gu	est			Guest	86005	Guest user has accepted the Use Policy	Guest user has accepted the use policy	INFO
		Gu	iest			Guest	86006	Guest user account is created	Guest user account is created	INFO
		Gu	iest			Guest	86007	Guest user account is updated	Guest user account is updated	INFO
		Gu	iest			Guest	86008	Guest user account is deleted	Guest user account is deleted	INFO
		Gu	est			Guest	86009	Guest user is not found	Guest user record is not found in the database	INFO
		Gu	est			Guest	86010	Guest user authentication failed	Guest user authentication failed. Please check your password and account permis.	INFO
		Gu	iest			Guest	86011	Guest user is not enabled	Guest user authentication failed. User is not enabled. Please contact your system	. INFO
		Gu	iest			Guest	86012	User declined Access-Use Policy	Guest User must accept Access-Use policy before network access is granted	INFO
		Gu	iest			Guest	86013	Portal not found	Portal is not found in the database. Please contact your system administrator	INFO
		Gu	iest			Guest	86014	User is suspended	User authentication failed. User account is suspended	INFO
		Gu	est			Guest	86015	Invalid Password Change	Invalid password change. Use correct password based on the password policy	INFO
		Gs	est			Guest	86016	Guest Timeout Exceeded	Timeout from server has exceeded the threshold. Please contact your system adm.	. INFO

Verifying and Troubleshooting

Taking a TCP Dump against the Remote Logging Target is the fastest troubleshooting and verifying step to confirm whether or not log events are being sent.

Capture must be taken from the PSN that authenticates user because PSN is going to generate log messages and these messages are going to be sent to the Remote Target



In the Cisco ISE GUI, click theMenuicon () and choose **Operations**> **Troubleshoot**>**TCP Dump**> Click on **Add**.

- You must filter traffic, add ip host <remote_target_IP_addres> filter field.
- You must take capture from PSN handling authentications.

≡	dentity Services	Engine			Operations / Troubleshoot	
щ	Bookmarks	Diagnostic Tools Download Lo	gs Debug Wizard			
	Dashboard	General Tools ~	TCP Dump > New			
	Operations	RADIUS Authentication Troubl Execute Network Device Com	Add TCP Dump Add TCP Dump packet for monitoring on a n	stwork interface and troubleshoot problems on the network as they appear.		
	Policy	Evaluate Configuration validat Posture Troubleshooting	Host Name* SSPT33A			
a. fi	Administration Work Centers	EndPoint Debug				
		Session Trace Tests	Network Interface* GigabitEthernet 0 [Up, Running] V			
	Interactive Help	TrustSec Tools >	Filter			
			E.g: ip host 10.77.122.123 and not 10.177.122.119			
			File Name Remote Syslog Server Test			
			Repository			
			File Size 10Mb			
			Limit to 1 File(s)			
			Time Limit 5			
			Minute(s)			
						Save Save and Run

TCP Dump

In this screenshot, you can see how ISE is sending Syslog messages for ISE Administrator logging traffic.

• •																							SPT33A_GigabitEthernet 5.pcap
1		R	0				6		2	(⇒		$\overline{\mathbf{A}}$					Đ,	Q	Q			
		anlau	Gitor I	- 90 1-	-				•			_		_	_						_		
	лу-а с	apriay LTime	HHEET	~++ >			10	011500					Dest	inatio			6	rotoco	-		ath		
NO.		2024	-07-2	5 10.	29:37	. 2354	S 41 1∣	0urce 0.20	1.23	1.67			10-5	201	m 231.90		S	vsloc		Leui	ցւո ֏Բ	15	mmu Inclais.NOTTCF: 1ul 25 11:29:37 SSPT336 CTSF Administrative and Operational Audit 0000000000 1 0 2024-07-25 11:29:37.234 -05:00 0000012031
ſ	2	202-	-07-2	5 10.	29.37	0565	04 1	a 2a	1 23	1 67			10.1	201	231.90		5	velo	9		47	13 1	Locale NATIFE: Jul 25 11:25:04 SSPT34 CISE Administrative and Operational Audit 0000000001 10 2024-07-25 11:25:07:254 -05:00 0000012001
	3	2024	-07-2	5 10:	30:00	. 5592	93 1	0.20	1.23	1.67			10.5	201.3	231.90		s	vslo	9		35	15 1	ICAL6.NOTICE: Jul 25 11:30:00 SSPT33A CISE Administrative and Operational Audit 00000000021 1 0 2024-07-25 11:30:00 SSB - 05:00 000001293
	4	2024	-07-2	5 10:	31:12	.7964	73 1	0.20	1.23	1.67			10.3	201.	231.90		s	vslo			47	13 1	LOCAL6.NOTICE: Jul 25 11:31:12 SSPT33A CISE Administrative and Operational Audit 0000000033 1 0 2024-07-25 11:31:12.796 -05:00 0000012895
	5	2024	-07-2	5 10:	32:01	.2177	80 1	0.20	1.23	1.90			10.2	201.	231.95		в	ROWSE	ER		24	13 H	Host Announcement DESKTOP-J6CKUCC, Workstation, Server, SQL Server, NT Workstation
i –	6	2024	-07-2	5 10:	32:10	. 3835	30 1	0.20	1.23	1.67			10.2	201.3	231.90		s	yslog	9		52	10 L	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000024 1 0 2024-07-25 11:32:10.382 -05:00 0000012896
		2024	-07-2	5 10:	32:10	. 3836	68 1	0.20	1.23	1.67			10.2	201.3	231.90		s	yslog	9		51	.9 L	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE Administrative and Operational Audit 000000025 1 0 2024-07-25 11:32:10.383 -05:00 0000012897
	8	2024	-07-2	5 10:	32:10	.3837	60 1	0.20	1.23	1.67			10.2	201.3	231.90		s	yslog	9		51	.6 L	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000026 1 0 2024-07-25 11:32:10.383 -05:00 0000012898
		2024	-07-2	5 10:	32:10	. 3838	07 1	0.20	1.23	1.67			10.2	201.3	231.90		S	yslog	9		51	.6 L	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000027 1 0 2024-07-25 11:32:10.383 -05:00 0000012899
	10	2024	-07-2	5 10:	32:10	.3838	78 1	0.20	1.23	1.67			10.2	201.3	231.90		s	yslog	9		52	18 L	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000028 1 0 2024-07-25 11:32:10.383 -05:00 0000012900
		2024	-07-2	5 10:	32:10	. 3839	45 1	0.20	1.23	1.67			10.2	201.3	231.90		s	yslog	9		51	17 L	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000029 1 0 2024-07-25 11:32:10.383 -05:00 0000012901
L	12	2024	-07-2	5 10:	32:10	.3840	53 1	0.20	1.23	1.67			10.2	201.3	231.90		S	yslog	9		50	15 L	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000030 1 0 2024-07-25 11:32:10.383 -05:00 0000012902
_	_	_	_	_		_	_	_	_		_	_	_	_		_	_		_	_	_	_	
> En	ame 1	. 385	, hyte	5 0D	wire	(3080	hite	s). 3	185	hytes	can	ture	ч (з	080	hits)								
> Et	herne	t II.	Srci	VMwa	re a5	:46:1	2 (06	1:50:	:56:	a5:46	:12)	. Dst	t: VI	Mwan	e a5:e	5:86	(00:	:50:5	6:a5	:e5:8	6)		
> In	terne	t Pro	tocol	Vers	ion 4	. Src	: 10.	.201.	.231	.67.	Dst:	10.3	201.3	231.	90								
> Us	er Da	tagra	m Pro	tocol	, Src	Port	: 327	724.	Dst	Port	: 51	4											
~ t	trunc	ated	Syslo	a mes	sage:	LOCA	L6.N0	DTICE	E: J	ul 25	11:	29:3	7 SSI	ртзз	A CISE	_Admi	inist	trati	ve_a	nd_0p	erati	.ona	al_Audit 000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersio
	1011	0	= Fac	ilit	y: L0	CAL6 ·	- res	erve	d fo	or loo	alı	use ([22]										
		.101	= Lev	el: I	NOTIC	E – n	ormal	but	sig	nific	ant	cond	itic	on (5									
~	Messa	ige [trunca	ted]	: Jul	25 1	L:29:	37 S	SPT	33A CI	ISE_/	\dmin	nistr	ativ	e_and_	Oper	atio	nal_/	Audit	000	00000	20 1	1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, AdminInter
	Sy	slog	times	tamp	(RFC3	3164):	Jul	25 1	11:2	9:37													
	Sy	slog	hostn	ame:	SSPT3	B3A																	
	Sy	slog	proce	ss id	I: CIS	δE																	
	Sy	slog	messa	ge id	[tru	Incate	d]: _	_Adm:	inis	trati	ve_a	nd_0	pera	tion	al_Aud	it 00	00000	86626	910	2024	-07-2	25 1	11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, AdminInterface=GUI, AdminI

Syslog traffic