

LT Auditor+ Syslog Server

Table of Contents

Overview
Data Flow
Installation
Minimum Requirements3
Installation Steps3
Configuring LT Auditor+ Syslog Server5
Connection5
Processor Settings5
Messages6
Use rules to log messages to new event log6
Rules
Add New Device
Add Device Default Setting8
Add Operations Settings12
Configuring LT Auditor+ to alert and log events created in the rules event log
(SyslogAuditing)16
Appendix A19
Parsing key value pairs19
Parsing JSON messages
Appendix B21
Regular Expressions (RegEx)21
Useful RegEx commands21



Overview

The LT Auditor+ Syslog Server application can receive syslog messages from multiple network devices, filter these messages in real time, and transpose or map filtered messages to formats that allow for enhanced querying and reporting. LT Auditor+ Syslog Server's powerful filtering technology can be configured to collect information that is relevant to meet regulatory compliance requirements, assist with trouble shooting and fulfill data log retention policies. Filtered data can be processed with LT Auditor+ to provide real-time notification for any critical events and provide enhanced reporting.

Centralized collection of syslog messages from devices like routers, switches, firewalls, Wireless Access Points (WAP), VPNs etc., generate a tremendous volume of data, much of which is useless and redundant. LT Auditor+ Syslog Server can ingest and process extremely large volumes of data and filter this data down to critical actionable information.

Data Flow

The schema below outlines the data flow with LT Auditor+ for Syslog Serve



Installation

LT Auditor+ Syslog Server can be installed on any of the following Windows operating systems:

- Windows 10
- Windows Server 2012R2, 2016, 2019

Minimum Requirements

- .NET v 4.0
- Minimum 1GB of RAM
- 500MB of free disk space
- x64 Windows operating system

Installation Steps

To install the LT Auditor+ Syslog Server follow the instructions below:

1. Run Setup_LTASyslogServer_x64.exe to bring up the welcome screen



2. Click Next to bring up Customer Information portal.

LT Auditor+ Syslog Server - InstallShield Wizard
Customer Information Please enter your information.
User Name: Blue Lance
Organization: Blue Lance
Install this application for:
 Anyone who uses this computer (all users) Only for me (Amazon)
InstallShield
< Back Next > Cancel

3. Enter information and click Next to bring window to select destination folder. If you wish to change the default click the Change button. Click Next to proceed with the installation.

岁 LT Auditor+ Syslog Server - InstallShield Wiz	zard X
Destination Folder Click Next to install to this folder.	と
Install LT Auditor + Syslog Server to: C:\Program Files\Blue Lance, Inc\LT Auditor +\Syslog Server\	Change
InstallShield	
< Back Next >	Cancel

- 4. On completion of the installation the following folder structure is created on the destination folder
 - Syslog Server\Bin contains all executable files
 - Syslog Server\Config contains the file LTAuditorSyslogReceiver.json used to define the Syslog Server setting
 - Syslog Server\Config\SyslogRules contains all the rule files LT Auditor+ Syslog Server will use. Rule files can be shared

A new service called LT Auditor+ Syslog Server is installed



Configuring LT Auditor+ Syslog Server

To launch the application, click Start \rightarrow All Programs \rightarrow Blue Lance, Inc \rightarrow Syslog Server to bring up the LT Auditor+ Syslog Server Config Application as shown below:

e U	FAuditor+ Syslog Server Config Application	_ _ ×
Settings Rules Connection © UDP Port O TCP 514 Messages	Processor settings Threads 3 1002	vverts per thread
Message offset 9 Target event log LTALog Target event log source LTALog Evolutie logion for messages containing specific text	Log all messages with Event Id # 3456 Contains audt_protocol Ref. accol	Log messages with custom Event Ids based on content EventID 4344 44
Use as delimiter to exclude multiple texts	sshd	4345
		Delete
Use rules to log messages to new event log Rules event log Rules event log source SyslogAudting SyslogAudting V Log me	Log debug messages Interval to log data received/m 30	ecorded stats (minutes)
		Save

Connection

This section defines how LT Auditor+ Syslog Server receives syslog messages. The default protocol used is UDP on port 514. To receive messages using the TCP protocol change the Connection type to select the TCP option and port. The default TCP port is 1468

Note: Ensure that firewall settings allow for traffic to the LT Auditor+ Syslog Server from all Syslog devices on the defined protocol and port.

Processor Settings

This section specifies resources used to process messages received. Increase the *Threads* count if the application receives a very high volume of messages.

Note: Use asynchronous process is not used at this time.



Messages

This section defines where all received messages are logged. LT Auditor+ Syslog Server stores messages to Windows event logs.

- 1. *Message offset* Specifies if input message should be trimmed. This option is set if there are symbols or characters that need to be removed at the start of the message text before logging the message.
- 2. *Target event log* Windows Event Log name used to log messages received. Logname specified here will get created.
- 3. *Target event log source* required for creating the target Windows Event Log
- 4. Exclude logging for messages containing specific text Used to exclude logging messages that contain certain text. Multiple text strings can be entered delimited with the 'l' symbol. For example entering 'read transfer multiple! write_transfer_max_size' will exclude any message received that contain these two text messages.
- 5. Log messages with Event Id # Logs messages received with Event Id specified in this box.
- 6. Log messages with custom Event Ids based on content Create custom Event Ids to log messages based on content.

Use rules to log messages to different event log

This section activates rules that can be applied to incoming messages in order to log them to a different event log. Rules can transpose incoming messages to a specific taxonomy that allows other applications to easily process and report on this information.

For example, a message like '<30>2020-01-02T12:34:17-05:00 BLCLUSTER1(id1) sshd[35000]: Accepted publickey for ORG\bjones from 156.18.2.249 port 50302 ssh2: RSA SHA256:5RHXgD7Z+xRtSfpcED45VpivoKLouUw5XsRN2nfApJw' Can be split into multiple fields and logged to an event log in key value pairs such as:

Operation=Login User=ORG\Jones Node=156.18.2.249 Server=BLCLUSTER1

Transformation into key value pairs makes it easy for another application to process this information and report on this activity.

If the rules event log name is SyslogAuditing, these transformed events can be processed by LT Auditor+ to create alerts and reports.

Log messages to target event log – Selecting this option will log messages both in the rules event log as well as the target event log defined in the Messages section.



Log debug messages – Selecting this option will log debug messages in the Application Event Log. Debug information will include a listing of the configuration files read. Statistical information such as the number of events received / minute is logged based on the setting in *Interval to log data received/recorded stats (minutes).*

Rules

The Rules tab is where rules are defined to create key value pairs of the message to enable alerting and reporting in LT Auditor+.

Dite			U.	Auditor	+ sysiog se	eiver coning Ap	plicatio	on			Ľ	
Devices						Default Settings						
Device Name Isilon	Source IP	Category Isilon	JSON No	EventId 36000		Field Name	E	P	K	Key	JSON Token	Custom
Operations		Add		Edit	Delete	Operation						
Name	EventId	Search1	Search	2	Enabled	Heid Name	E	۲	N	ney	JSUN Token	Custom

Click on Rules tab to display the following window:

Most syslog message formats can be broken out in four primary components:

<Date & Time of event> <Host that generated event> <Process> <Message>

The data that needs to be parsed is in the Message component and the first three components can be described as the header part. Parsing of this syslog message will depend on the type of device sending messages and an analysis and understanding of the syslog message is required prior to creating parsing rules.

In the Rules window shown above, the upper half of the screen is used to break down a syslog message received into these four parts, namely Date & Time, Host, Process and Message. This is referred to as the Device Default Settings. The bottom part of the screen above is used to break down the Message part component into unique operations that can be used for alerting and reporting. This section is referred to as the Operations Settings.



Add New Device

Prior to adding a new device for creating rules, first get the device to send messages to the LT Auditor+ Syslog Server. Viewing the target event log will confirm that messages are being received.

Note: If messages from multiple devices are being received, use the option '*Log messages with custom Event Ids based on content*' to only log data based on the IP address of the new device. Once this has been configured, clear the target event log and generate new syslog messages from the device. The target event log will now be populated with new messages from this new device, providing a data set that can be used to create new rules.

Adding a new device will require two sets of actions

- 1. Add the Device default setting
- 2. Add Operations settings for alerting/notification and reporting in LT Auditor+

Add Device Default Setting

Click Add under Devices grid in the previous illustration to bring up the following screen:

		Add new Device	e	– – ×
Name of device	Device IP addre	155	Operation category	Default EventId
Message to parse				Get Data
Message action Offset Parsed Message	Delimiter	O Convert to JSON		Parse Message
Date and Time	Position V	Position V	Name Position V	Message
				OK Cancel

Name of Device – Name of the device model that will be sending syslog messages

Device IP Address – IP Addresses of all devices of the same model that will be sending messages to the LT Auditor+ Syslog Server. Multiple IP Addresses can be entered separated with a comma e.g. 10.3.45.5,128.4.5.8,....

Operation Category – This field defines the category for all operations that will be created to enable parsing of messages from this device. This is absolutely required for reporting in LT Auditor+.



Default Event Id – This will be the default Event Id used by LT Auditor+ Syslog Server to log data to the SyslogAuditing event log.

Get Data – Click this button to pull up events logged from the device. The screen below displays events from a NAS appliance.

e	LT Auditor+ Syslog Server Config Application
Settinas Rules	🤪 Search Events 💶 🗖 🗙
Name of device	Search
NAS Device	
Message to parse	Events 20>2020-01-02T12:34:17-05:00 BLCLUSTER-2 shd[35000]: Accepted publickey for COPO\\banner from 192.15.2.246 port 50302 sh2: RSA SHA2 230>2020-01-02T12:51:50-05:00 BLCLUSTER-2 audit protocol[72714]: 51-92-1-1112011120baa0137 15 98 370/FSW81TEISLCCFSSEILEIS167
	<30>2020-01-02T12:39:45-05:00 BLCLUSTER-2 sshd/92157]: Failed password for invalid user abcdef from 192.15.2.246 port 51842 ssh2
	<30>2019-12-18T20:38:43-06:00 BLCLUSTER-1 audit_protocol[2203]: GFoster1000004[System]1]192.168.114.1ISMBIOPENISUCCESS]1048705[DIRK]
	<30>2019-12-18T20:07:34-06:00 BLCLUSTER-1 audt_protocol[2203]; JSmith 1000004 System 1 192.168.114.1 SMB OPEN SUCCESS 1442207 FILE C
Message action	<30>2019-12-18T20:17:51-06:00 BLCLUSTER-1 audit_protocol[2203]: TPeter[1000004 System]1 192.168.114.1 SMB DELETE SUCCESS DIR 4297263
Offset	<30>2019-12-18T20:11:58-06:00 BLCLUSTER-1 audit_protocol[2203]: HFox1000004/System]1[192.168.114.1 SMB OPEN SUCCESS 1048704 FILE OF
Damed Massage	<30>2020-01-02T12:30:30-05:00 BLCLUSTER-2 audit_protocol[20190]: KLoweryI1006030[Data]2]137.15.245.192[SMB]READ[SUCCESS]FILE]4690341
Falseu Message	<30>2019-12-18T20:10:10-06:00 BLCLUSTER-1 audit_protocol[2203]: DSam[1000004 System]1 192.168.114.1ISMB DELETE SUCCESS FILE 4297197
	<3052019-12-18120:06:49-06:00 BLCUUSTER-1 audit_protocol[2203]: PJoInh[System1]192.168.114.1IS/MBOPENIS/0CCESSI1048/05/DIRCREATED
r	<3052019-12-18120:11:58-06:00 BLCLUSTER-1 audit_protocol[2203]; FSam(System)1192:168:114.1IS/MBIRENAMEIS/UCCESSIFILE429/265259/fs/ 200-2019.1219720.1624 (AGO D) CLUETE 1 audit_protocol[2203]; FSam(System)1192:168:114.1IS/MBIRENAMEIS/UCCESSIFILE429/265259/fs/
	S0/2019 12/1612010, 624/06.00 BLCLD31EPH-1 adult_protocol[22/03]. UCH81000004[93ytem](1192,166,114,1[596]051_3ECUF11190CCE35]RLE 202019.12/1612019.53.06:00 BLCLD31EPH-1 adult_protocol[22/03]. UCH8100004[93ytem](1192,166,114,1[596]DEF1.54][05104
	C002019-101000 (2000) C00000 (2000) C00000000 (2000) C000000 (2000) C000000000000000000000000000000000
	colored and the second seco
Date and Time	<30>2020-01-02T12-51:50-05:00 BLCLUSTER-2 audit_protocol[74714]; S-1-22-1-11112[11112[Data]2[137,15.98.37]NFS]WRITEISUCCESSIFILEI5167(
	<30>2020-01-02T12:30:30-05:00 BLCLUSTER-2 audt_protocol[20190]: KLowery1006030 Data 2 137.15.245.192 SMB READ SUCCESS FILE 469034;
	<30>2019-12-18T20:06:49-06:00 BLCLUSTER-1 audt_protocol[2203]: PJohn/System 11192.168.114.1 SMBIOPEN SUCCESS 1048705 DIRICREATED
	<30>2019-12-18T20:07:34-06:00 BLCLUSTER-1 audit_protocol[2203]; JSmith 1000004 System 1 192.168.114.1 SMB OPEN SUCCESS 1442207 FILE C
	430-2019-12-18T20-11-58-06-00 BLCL LISTER-1 audit. orotocol/22031: HEox1000004/System11192-168-114_IISMB/0PEN/SL/CCESS1048704/EI/EI/EPC *
·	Add Edt Delete

As discussed earlier, the parsing process starts with identifying the header and message components. Select one event and double click to show the message text:

		Add new Device			- 🗆 X
Name of device NAS Device	Device IP address 172.31.13.156		Operation category Isilon	Default 36000	EventId
Message to parse					
<30>2019-12-18T20:38:43-06:00 BLCLU: OPENEDI4297263254I/ifs/MyData/Test	STER-1 audit_protocol[2203]: GFost	ter 1000004 System 1 192.1	68.114.1 SMB OPEN SUCCESS 1	048705 DIR	Get Data
Message action Offset Parsed Message	r O	Convert to JSON			Parse Message
Date and Time	Host Name	Process Na	ame	Message	
Position v		Position V	Position V		Position V
				ОК	Cancel

From the text displayed we see a set of characters <30> followed by date and time, hostname, process name and start of the message text with GFoster...

The goal is to identify the four components and to do so we set the following parameters:

Offset – This is used to remove characters at the beginning of the message. For this message set the offset to 4 to remove <30>

Delimiter – Select the delimiter to parse the components. For this device the delimiter appears to be the space character.

Convert to JSON – If the device was sending messages in JSON format set this parameter to JSON.

Parse Message – Click this button to parse the message to display the following window:

9	A	dd new Device	_ D X
Name of device NAS Device	Device IP address 172.31.13.156	Operation category Isilon	Default EventId 36000
Message to parse			
<30>2019-12-18T20:38:43-06:00 BLC OPENEDI4297263254I/ifs/MyData/Te	LUSTER-1 audit_protocol[2203]: GFoster[10 st	000004 System 1 192.168.114.1 SMB OPEN SUCC	CESS 1048705 DIR
Message action Offset 4	niter O Co	nvert to JSON	Parse Message
2019-12-18T20:38:43-06:00 BI	.CLUSTER-1 audit_prot	tocol[2203]: GFoster11000004lSystem	m11192
Date and Time	- Host Name	Process Name	Message
✓ 0 Position	V 1 Posi	tion v 2 Position	V 3 Position V
			OK Cancel

For the example above there is a clear demarcation for the four components. Check component boxes below and drag the text resembling each component to the appropriate box as shown:

•	Add new Device		_ 🗆 X
Name of device NAS Device	Device IP address 172.31.13.156	Operation category Isilon	Default EventId
Message to parse			
<30>2019-12-18T20:38:43-06:00 BLCLUSTER-1 OPENED 4297263254 /ifs/MyData/Test	audt_protocol[2203]: GFoster1000004 System11192	.168.114.1 SMB OPEN SUCCESS 1048705 E	DIRI A Get Data
Message action			
Offset 4	O Convert to JSON		Parse Message
Parsed Message			
2019-12-18T20:38:43-06:00 BLCLUSTEF	k-1 audit_protocol(2203):	GFoster11000004(System111192	ר
Date and Time	ost Name	Messac	
O Position	1 Position v 2	Position V 3	Position V
			OK Cancel



Component Box	Unchecked	Checked
Date and Time	Time computed when	Selects parsed position to
	message was received	determine time
Host Name	Uses IP address of device	Selects parsed position for
		Hostname; Can use Custom
		in dropdown for custom
		value
Process Name	No value is recorded	Selects parsed position for
		Hostname; Can use a
		Custom value in dropdown
		for custom value
Message	**	Selects parsed position for
		start of Message text. This
		box must be checked

** Leaving unchecked can cause unpredictable results.

In this example the rule is based on the position of the component in the text. If date and time is not clearly identified or is split across multiple text messages such as 'January 10 2020 14:20:34', then leave the Date & Time component box unchecked. LT Auditor+ for Syslog Server will use the time message as received for the date stamp.

Other options available are displayed if the component dropdown is clicked as shown:

User	Node
☑ 0	Position V 4
Object2	Position KeyValuePair JSONToken Custom
Value2	Apply Regular Expression (RegEx)

Position - Rule is based on position of the component as shown above

KeyValuePair – If component is a key value pair, LT Auditor+ Syslog Server can process this separately. This is typically seen when setting up Operations discussed later in the document. For example: if a device transmits a message with component user=mHarry, the username can be derived using KeyValuePair. We want reports to display mHarry and not user=mHarry. Select the KeyValuePair option and enter user= and the system will retrieve mHarry from the text.

JSONToken – If the device is sending messages in JSON format, make sure to click *'Convert to JSON'* and use JSONToken

Custom – In certain situations there may be a need to insert a custom message to identify a component. Custom messages entered here can be reported on.



Apply Regular Expression (RegEx) – In situations where extra processing is required on the component after retrieval from Position or KeyValuePair or JSONToken a RegEx expression entered here can be applied to derive the desired result. The following are examples:

- If component has quotes or brackets like "Admin" or (Admin) apply RegEx expression [^0-9a-zA-Z]+ to strip out unwanted characters to get Admin
- If component has extra characters like 20.4.5.6:8000 apply RegEx expression :(.*) to get 20.4.5.6

Note – RegEx expressions are a very popular method used to convert text messages to desired content and there is a lot of documentation available to display examples to meet any particular requirement.

Click OK to save the Default Device Setting.

Add Operations Settings

To add Operations, click on the newly added device in the Device box as shown below:

8			LT	Auditor	+ Syslog Se	rver Config	Appli	cati	on			Ŀ	- 0	x
Settings Rules														
Devices						Default Setti	ngs							
Device Name	Source IP	Category	JSON	EventId		Field Name	E	P	K					
Cisco	20.1.2.3	Cisco	No	38000		DateTime	Yes	0	No					
Cisco 3850	•	Cisco	No	45000		HostName	Yes	1	No					
Isilon	128.4.5.6	Isilon	No	36000		ProcessNan	ne Yes	2	No					
NAS Device	172.31.13.15	Isilon	No	36000		Message	Yes	3	No					
		Add		Edit	Delete									_
Operations						Operation								
Name	EventId	Search1	Search	h2	Enabled	Field E.	K	Ke	у	RegEx				
														_
<		ш			>									_
		Add		Edit	Delete									
								-						

Click Add in the Operations box to bring up the Add new Operation window:

• -			Add new Operat	on			- 🗆 X
Name of device NAS Device	Device IP Address 172.31.13.15	Operation category Isilon	Convert to JSON				✓ Enable
Operation name	Event Id	Search to identify opera	ation	Addi	tional search to	identify operation	
Message to parse	36001						
Delimiter: Parsed message	Parse N	lessage					Get Data
User	Position V	Node	Domai	1	Position 1	Object1	Position V
Object2		Class1	Class2		POSIDOI +	Value1	POSIDON V
	Position V		Position V		Position V		Position V
Value2	Position V	UDF1	UDF2 Position ∨ □		Position V	UDF3	Position V
	Position V						
						ОК	Cancel

Click *Get Data* and select an event for which an Operation is to be created. In the example shown below a message denoting successful deletion of a file has been selected.

22		Add new	Operation		L	- 🗆 X
Name of device NAS Device	Device IP Address 172.31.13.15	Operation category Isilon Convert t	o JSON			Enable
Operation name	Event Id	Search to identify operation		Additional search t	o identify operation	
Delete File	36001	DELETEISUCCESSIFILEI				
Message to parse						
<30>2019-12-18T20:10 4297197477//ifs/MyDa Delimiter:	0:10-06:00 BLCLUSTEF sta/Test/New Text Doc	R-1 audit_protocol[2203]: DSam 1000004 Syst ument (2).bd	tem 1 192.168.114.1 SMB E	ELETEISUCCESSIF	ile)	Get Data
Parsed message						
DSam (User)	1000004	System	1		192.168.114.1 (Node)	~
SMB	DELETE	SUCCESS	FILE		4297197477	
He /MuDists /Test /New	w Text					~
User		Node	Domain		Object1	
	Position V	✓ 4 Position ∨		Position V	✓ 10	Position V
Object2		Class1	Class2		Value1	
	Position V	Position V		Position V		Position V
Value2		UDF1	UDF2		UDF3	
	Position V	Position V		Position V		Position V
UDF4						
	Position V					
					ОК	Cancel

Operation name – Describes the operation being created. In this example it is Delete File

Event Id – Operation Event Id. This number is automatically incremented from Default Id defined for the device but can be modified.

Search to identity operation – This box must contain a value that identifies the operation. In the example we look for the text DELETEISUCCESSIFILE in the message to denote a delete file operation



Additional search to identify operation – If there is an additional text string in the message to provide extra proof for the operation enter the text here. For our example we do not require this.

Delimiter – Delimiter to parse the Message component. In this example you can see that the message component is delimited with the 'l' symbol.

Parse Message – Click button to parse message.

Drag and drop parsed text strings to the appropriate component boxes. In the example above: User, Node and Object1 boxes have been used. These denote the user, node and filename.

Click OK to save. Verification of components selected can be viewed by clicking the Device name and the Operation as shown below:



Verification that this rule is working can be obtained by reviewing the target event log and the rules event log as shown below:

Target Event Log

8	Event Propert	ies - Event 34	56, LTALog	x
General Details <30>2020-04-07T 192.168.114.1JSME Log Name:	20:10:10-06:00 BLCLUSTER-1 a SIDELETEISUCCESSIFILEI429719	udit_protocol[22 97477 /ifs/MyData	3]: DSam 1000004 System 1 /Test/New Text Document (2).txt	
Source:	LTALog	Logged:	4/8/2020 7:54:39 AM	•
Event ID:	3456	Task Category:	None	
Level:	Information	Keywords:	Classic	
User:	N/A	Computer:	WIN-H8EG9QHMFC9.blcorp.com	
OpCode:				
More Information:	Event Log Online Help			
Сору				Close

Rules Event Log (SyslogAuditing)

SyslogAuditing	Number of events: 4			
Level	Date and Time	Source	Event ID	Task Cat
Information		SyslogAuditing		
 Information 	4/8/2020 7:53:15 AM	SyslogAuditing	36001	(1)
Information	4/7/2020 8:29:21 PM	SyslogAuditing	45002	(1)
(i) Information	4/7/2020 3:30:06 PM	SyslogAuditing	45002	(1)
				>
C	1			~
Event 30001, Sys	logAdditing			
General Deta	ils			
SysLog Data Operation Generated Host Nam Process N Message I Category: Source: RuleID: User: Node Add Object1:	257 Description: NAS Device-Delete File Time: 4/(2/2020-2:10:10:AM audit_protocol(2203); tetails: DSam(1)(00004[5yetam](1):92.168.114.1]SMB[DELETE[SL islon Detect File 999 DSam (2):48:141 /fdx/MyData/Test/New Test Document (2).bt	JCCESS]FILEJ42971974771/rft;/MyData/Text/New Text Document (2).t	st	_

Observe that the Rule event log has correctly parsed the message into the key value pairs User: DSam, Node: 192.168.114.1, Object1: /ifs/MyData/Test/New Text Document(2).txt.

Configuring LT Auditor+ to alert and log events

The following steps outline how to configure LT Auditor+ to create alerts and log events captured in with LT Auditor+ Syslog Server:

- 1. Create operations in LT Auditor+ to match operations created in LT Auditor+ Syslog Server
- 2. Create LT Auditor+ filters to capture and log the data. Alerting can be setup at this stage.
- 3. Create report queries to report on the data. Reports can be scheduled at this stage.

Create operations in LT Auditor+

1. Launch LT Auditor+ Management Console and click Options->Syslog Rule->Master Settings -> Operations to bring up the Operations Window

-	Event ID	1	EventID	Operation Description	Event Log	Source	
			30624	SP_Search performed	SyslogAuditing	Syslog	
	Description		30623	SP_SharePoint object	SyslogAuditing	Syslog	
	Description		30622	SP_Object profile cha	SyslogAuditing	Syslog	
			30620	SP_SharePoint audit I	SyslogAuditing	Syslog	
	Free Aller	Court and a standard and	30619	SP_Object deleted	SyslogAuditing	Syslog	
	Event Log	SysiogAuditing	30618	SP_Custom event	SyslogAuditing	Syslog	
			30621	SP_Object moved	SyslogAuditing	Syslog	
	Source	SysLog	30617	SP_Object copied	SyslogAuditing	Syslog	
			30616	SP_Child object moved	SyslogAuditing	Syslog	
			30615	SP_Child object deleted	SyslogAuditing	Syslog	
	Catanan		- 30614	SP_Document checke	SyslogAuditing	Syslog	
	Category	*	30613	SP_Document checke	SyslogAuditing	Syslog	
			30612	SP_Audit policy chang	SyslogAuditing	Syslog	
			30611	SP_Site collection aud	SyslogAuditing	Syslog	
		Contract Contract	30600	SP_Default	SyslogAuditing	Syslog	
	Add	Delete Cancel	30000	Syslog Default	SyslogAuditing	Syslog	
			<	III			2

For our example enter information as shown in the screen above.

Event ID	36001	EventID	Operation Description	Event Log	Source	-
	1	26001	Delete Sile	Suclea Auditina	Suchee	-
		34004	LDAR Login Failure	SyslogAuditing	Systog	18
Description	Delete File	34003	Eniled SSH Login	SyslogAuditing	Systog	
	1	34003	Web Login	SyslogAuditing	SysLog	
		34002	SEH Login	SyslogAuditing	SysLog	
Event Log	SyslogAuditing -	24000	Cisco Default	SyslogAuditing	Systog	
	,	54000	Cisco_Deladic	SyslogAuditing	SysLog	
-	a	50015	Computer Logon	SyslogAuditing	Syslog	
Source	SysLog	50014	File Converte Dermine	SyslogAuditing	Syslog	
	E au	50013	File Security Permissi	SyslogAuditing	Syslog	
	I⊻ All	50012	Container Security Pe	SyslogAuditing	Syslog	
Category	Isilon	50011	Group Security Permi	SyslogAuditing	Syslog	
	131011	50010	User Security Permiss	SyslogAuditing	Syslog	
		50008	Linked GPO Settings	SysiogAuditing	Syslog	
		50007	User Settings	SyslogAuditing	Syslog	
bba	Delete Cancel	50006	Account Expiration Se	SyslogAuditing	Syslog	
nuu	Derete	50005	Password Settings	SyslogAuditing	Syslog	1
	Event ID Description Event Log Source Category	Event ID 36001 Description Delete File Event Log SyslogAuditing Source SysLog IZ All Category Tailon Add Delete Cancel	Event ID 36001 EventID Description Delete File 34004 24003 34004 34002 Event Log SyslogAuditing v Source Syslog 50014 F7 All 50013 50011 Category Isilon 50011 Add Delete Cancel	Event ID 36001 EventID Operation Description Description Delete File 34004 LDAP Login Failure Source SystogAuditing * 34003 Failed SSH Login Source Systog Source Source	Event ID 36001 EventID Operation Description Event Log Description Delete File SyslogAudring 34004 LDAP Login Failure SyslogAudring 34003 Failed SSH Login SyslogAudring 34003 Failed SSH Login SyslogAudring 24004 Web Login SyslogAudring SyslogAudring SyslogAudring 35001 Compare Login SyslogAudring SyslogAudring SyslogAudring Source SysLog Source SyslogAudring SyslogAudring SyslogAudring F7 <ali< td=""> Source SyslogAudring SyslogAudring SyslogAudring SyslogAudring Source SyslogAudring Source SyslogAudring SyslogAudring SyslogAudring Source SyslogAudring Source SyslogAudring SyslogAudring SyslogAudring Source SyslogAudring SyslogAudring SyslogAudring SyslogAudring Source SyslogAudring SyslogAudring SyslogAudring SyslogAudring Source SyslogAudring <</ali<>	Event ID 36001 EventID Operation Description Event Log Source 34001 Delete File 34004 LDAP Login Failure SyslogAuditing Syslog 34002 Failed SSH Login SyslogAuditing <

Note: Ensure that you enter Event ID, Description and Category exactly as they were setup in LT Auditor+ Syslog Server.

Create filters in LT Auditor+

Create a filter for this event in the Management Console as shown:

BL20 BL20 Manager Group Jobs Authorized Users Audit SubSystems N	🍯 Syslog Device Au	Date Of Creation	20 Manager Group	Filter Status		
Ante Ducker Anter Anter States Anter Ducker Anter Pre States Anter	ines Audéring	Central Denter Denter	Systog Fiter	Users Nodes (1) OC	X Add Modry Delete Cancel Heb	

Alerting can be setup similar to any other event captured in LT Auditor+. Please refer to the LT Auditor+ Configuration guide for instructions on setting up alerts.

Click Ok to create the filter as shown below.

e Auditing filters for B	L20 Manager Gr	oup	
Date Of Creation	Filter Type	Filter Status	
3/19/2020 7:23:32 AM	Include	Enabled	
4/8/2020 8:20:01 AM	Include	Enabled	
	20 Auditing filters for B	22 Auditing filters for BL20 Manager Gr	Auditing filters for BL20 Manager Group Dete of Creation Filter Type Filter Status Dete of Creation Filter Type Filter Status database Filter Status database Filter Status database Filter Status database Filter Status

Create report queries in LT Auditor+

Create a query to report on this event in the LT Auditor+ Reporting Console as shown below in the Reporting Arm LT Auditor+ for Syslog Server.



Generate a report to view the activity.

					Auditor+ O	versight Report	t t		
Generated On: Generated By:	Wednesd	ay, April 8, 202 othomas	20						
Date & Time	Pro	cess	Host	User	Node	Object	Class	Attribute	Remarks
4/8/2020 2:10	:10AM aud 203	t_protocol (2 j:	BLCLUSTE R-1	DSam	192.168.114.1	/ifs/MyData/Test/ New Text Document (2).txt			DSam 1000004 System 1 19 2.168.114.1 SMB DELETE S UCCESS FILE 4297197477 fs/MyData/Test/New Text Document (2).bd

The report shows how the message has been transformed to units like Host, User, Node and Object which allow easier querying and easy to understand reports.

Appendix A

Examples of other methods of parsing syslog messages.

Parsing key value pairs

<188>2024: *Apr 7 16:25:30.969: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: administrator] [Source: 14.25.31.178] [localport: 22] [Reason: Login Authentication Failed] at 16:25:30 UTC Tue Apr 7 2020

In the message above one can use the KeyValuePair option to retrieve the user and node as shown below:

8			Edit - Log	in Failed			_ 🗆 🗙
lame of device Cisco 3850	Device IP Address 20.4.5.6	Operation category Cisco	Convert to	JSON			✓ Enable
Operation name	Event Id	Search to identify	y operation		Additional search t	o identify operation	
Login Failed	45003	Login failed					
Message to parse							
Delimiter:] Parsed message	Parse 1	Message					
User		Node		Domain		Object1	
user:	KeyValı 🗸	Source:	KeyValt 🗸	0	Position V	0	Position V
Object2		Class1		Class2		Value1	
0	Position V	0	Position V	0	Position V	0	Position V
Value2		UDF1		UDF2		UDF3	
0	Position V	0	Position V	0	Position V	0	Position V
UDF4							
0	Position V						
							Canad

The option requires the key name to be entered in the component box as well the right delimiter. In this example we use the key names 'user: ' and 'Source: ' and since the value ends with the character ']', this symbol is used as the Delimiter.

Alternatively, one could use the space delimiter and apply a RegEx expression to remove the symbol ']' as shown below:

		Edit - Login	
me of device sco3850	20.4.5.6	Operation category Disco Convert to JSON	✓ Enat
Operation name	Event Id	Search to identify operation Additional search to identify operation	
Login	45001	Login Success SEC_LOGIN-5-LOGIN_SUCCESS	
Message to parse			
Delmiter:	Parse M	eesooo	Ge ↓ Dat
		Regular Expression (RegEx)	
Jser Z	Autor	Not Regular Expression (RegEx)	
Jser Ziluser:	Apply F 🗸	Not Regular Expression (RegEx) Cbject 1 Cbject 1 Cbject 1 Cbject 1 Cbject 1 Cbject 1	Position
Jser 2 user: Dbject2	Apply F V	Not Regular Expression (RegEx) Copect 1	Position
Jser v user: Dbject2 0	Apply F V	Not Regular Expression (RegEx) X Image: Comparison to apply 0 0 0 Image: Comparison to apply 0 0 0 0 Image: Comparison to apply Image: Comparison to apply 0	Position Position
Joer 2 user: 2bject2 0 /alue2	Apply F v Position v	Nod Regular Expression (RegEx) X Object 1 V RegEx expression to apply 0 0 0 V V V V 0 0 0 V Test RegEx expression V 0 0 0 0 VD VD VDF3 0 0 0 0 0	Position
Jser 2 user: bject2 0 Value2 0	Apply F v Position v Position v	Regular Expression (RegEx) X Object 1 0 Image: Comparison of a poly 0	Position Position Position
User User: Object2 0 Value2 0 UDF4	Postion v	Not Regular Expression (RegEx) X PegEx expression to apply 0 0 With State 2014 Value 1 0 Test RegEx expression UD Test Save 00se	Position Position



The RegEx expression '[^0-9a-zA-Z]+' removes all non-alphanumeric characters. For more information on RegEx commands review Appendix B.

Parsing JSON messages

If incoming messages are in JSON format they may look like the following text

02-21-2020 15:00:25 Local7.Debug 156.9.4.25 2020-03-21 15:00:25,747 eDirectory : INFO {"Source" : "eDirectory#NMAS","Observer" : {"Account" : {"Domain" : "BLTEST_TREE","Name" : "CN=bltest,OU=Resources,O=Houston","Id" : "0"},"Entity" : {"SysAddr" : "156.9.5.131","SysName" : "torldap2.corp.toronto.ca","SvcName" : "nmas"}},"Initiator" : {"Account" : {"Name" : "CN=bluser,OU=Staff,O=Houston"},"Entity" : {"SysAddr" : "156.9.5.131:50681"}},"Target" : {"Data" : {"ClassName" : "User","Name" : "CN=bluser,OU=Staff,O=Houston","SubTarget" : "CN=torldap2,OU=Resources,O=Toronto","Version" : "2"},"Account" : {"Domain" : "BLTEST-TREE"}},"Action" : {"Event" : {"Id" : "0.0.2.0","Name" : "CREATE_SESSION","CorrelationID" : "nmas#-1453326157#","SubEvent" : "DSE_NMAS_LOG_FINISH_LOGIN_STATUS"},"Time" : {"Offset" : 1582315225},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}

In the LT Auditor+ Syslog Server check the option *Convert to JSON* and click the *Parse Message* button to get JSON tokens with values of the message as shown below:

•9	Add new De	vice	– – X	
Name of device XDAS Message to parse [02:21:2020 15:00:25 Local Z Debug	Device IP address 	Operation category XDAS	Default EventId	
""ODmercon#NMAS" "Observe": ["Account": ["Domain": "BLTEST_TREE": "Name": "ON-blact OU-Fleetources() -Houston"; "Id": "O"), "Entry": Get Data "GysAdd": "156.9.5.131"; "SysName": Toridap2.corp.toronto.cs,", "SvcName": "Immas")), "Initiator": ["Account": ["Name": " Get Data Message action				
Source=Directory#NMAS Observer.Account. Domain=BL Observer Account. Mame=CN= Observer. Entity. SysAddr=156.9 Target. Data. ClassName=User Target. Data. Name=CN=bluser Target. Data. SubTarget=CN=tor Target. Data. Version=2 Target. Account. Domain=BLTE Action. Event. Id=0.0.2.0 V				
Date and Time Ht	st Name Pro	Cess Name Position ✓	Message Positior OK Cancel	

Drag and drop the required components to both Device Default Setting and Operation Settings windows and make sure to select the option JSONToken to process the message. Additional RegEx expressions can be applied for further processing.

Appendix B

Regular Expressions (RegEx)

Regular Expressions is a well-known methodology used to process and format textual strings. LT Auditor+ Syslog Server provides the option to apply RegEx expressions on components to clear out unwanted characters in the desired value.

Example:

Some devices send the IP Address with the port number such as 10.4.7.8:4000. The port number will keep changing and it is better to remove it. To do so we could apply the expression :(*.) which will remove all characters including and after the ':' symbol.

Useful RegEx commands

Purpose	RegEx Expression	Example
Remove non alphanumeric	[^0-9a-zA-Z]+	(Admin) ==> Admin
characters		
Remove non-alphanumeric	[^0-9a-zA-Z]+	(10.4.5.6) ==> 10.4.5.6
characters and keep one		Note the non-alphanumeric
non-alphanumeric		character '.' has been
character		retained.
Remove port numbers	:(.*)	10.2.5.77:4000 ==>
from IP Address		10.2.5.77
Remove n number of	^.{n} – where n is a	Dom\Bluser ==> use ^{4}
characters at the beginning	number	==> Bluser – where first 4
		characters are removed
Combine expressions	(^.{2})I(\)(.*))	This removes the first two
using the 'l' symbol and		characters and then
ensure both expressions		removes all text after the
are enclosed with		first occurrence of the
parenthesis		symbol ')'.
		5(10.5.6.8) ==> 10.5.6.8