BLUE LANCE

LT Auditor+ Syslog Server

Table of Contents

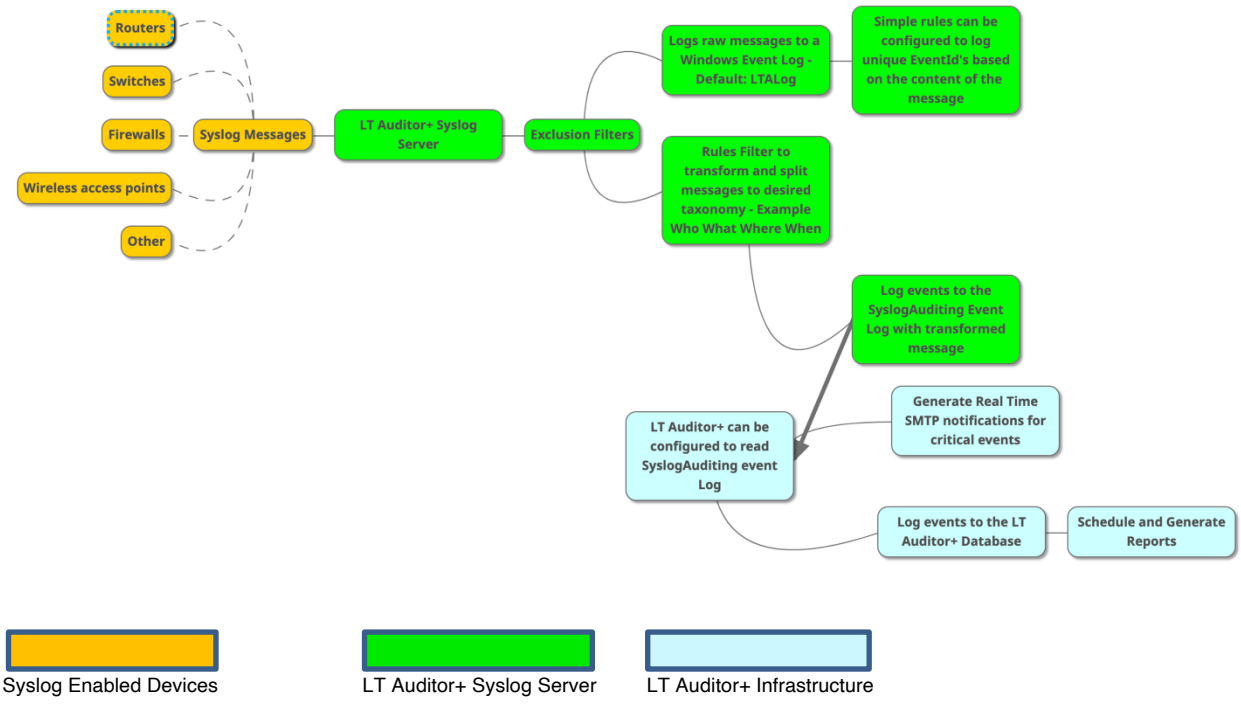
Overview

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

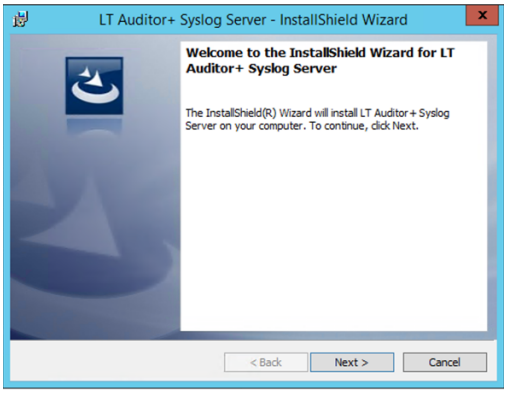
Minimum Requirements

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

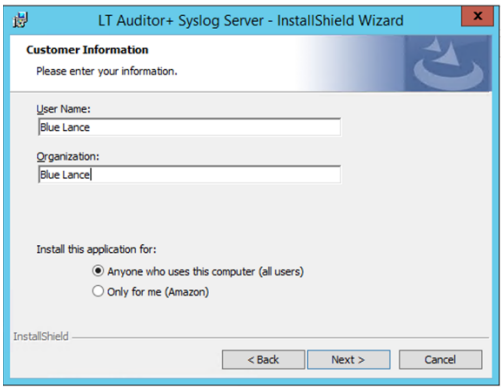
Installation Steps

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

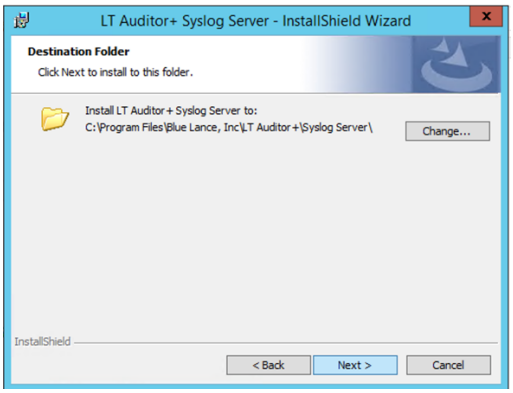
1. Run Setup_LTASyslogServer_x64.exe to bring up the welcome screen



2. Click Next to bring up Customer Information portal.



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.



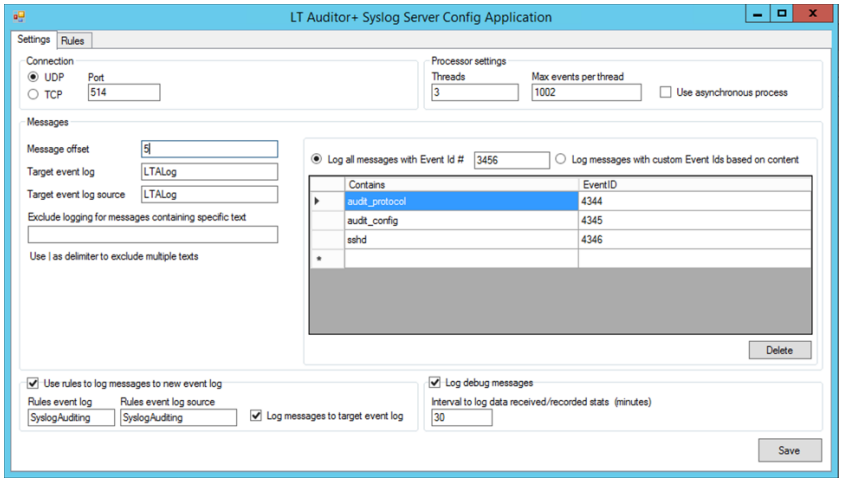
4. On completion of the installation the following folder structure is created on the destination folder

   - 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 → All Programs → Blue Lance, Inc → Syslog Server to bring up the LT Auditor+ Syslog Server Config Application as shown below:



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 'I' symbol. For example entering 'read transfer multiplel 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.

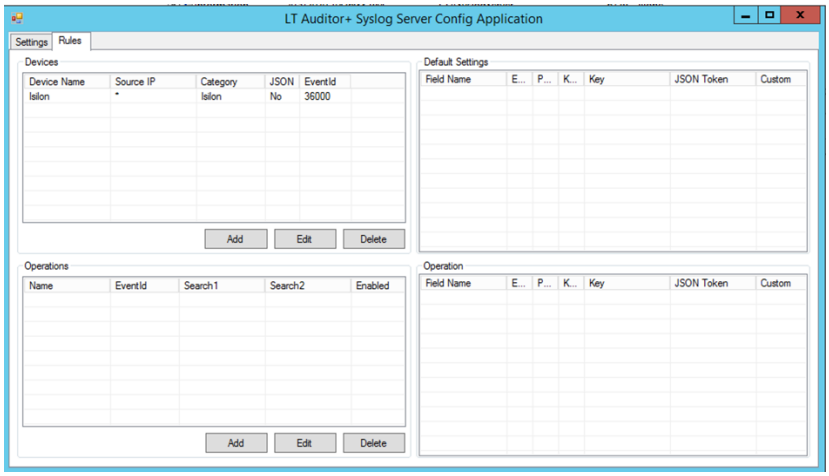
Log messages to target event log – Selecting this option will log messages both in the rules event log as well as the target event log defined in the Messages section.

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+.

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.

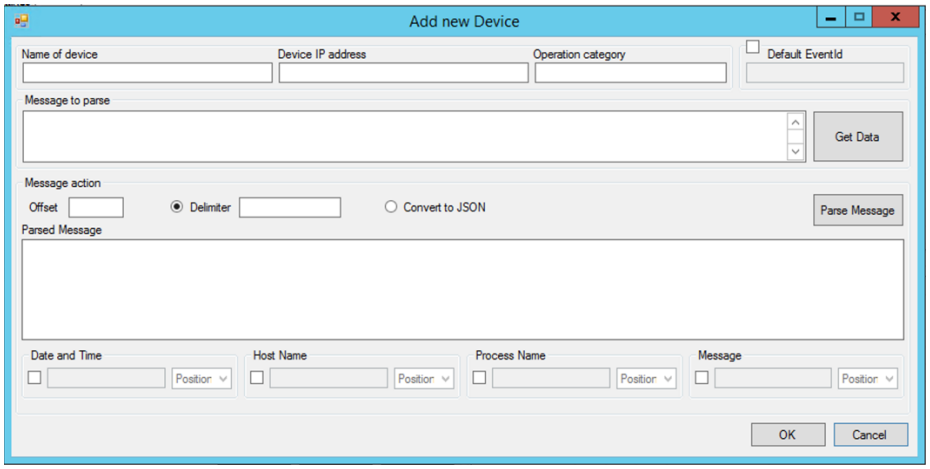
Note: If messages from multiple devices are being received, use the option '*Log messages with custom Event Ids based on content'* to only log data based on the IP address of the new device. Once this has been configured, clear the target event log and generate new syslog messages from the device. The 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:



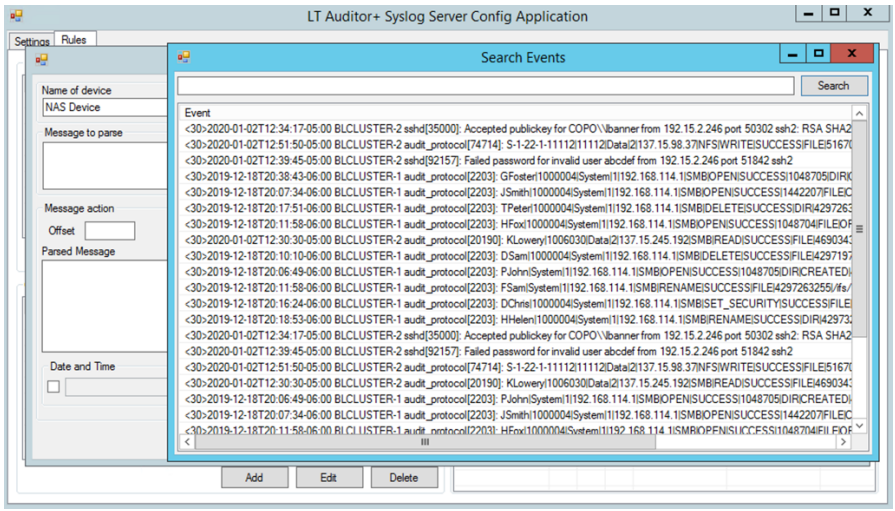
Name of Device – Name of the device model that will be sending syslog messages

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,….

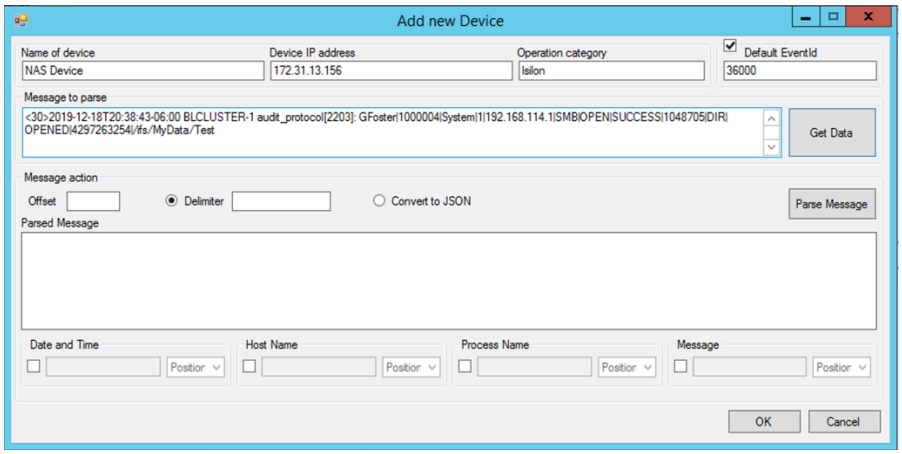
Operation Category – This field defines the category for all operations that will be created to enable parsing of messages from this device. This is absolutely required for reporting in LT Auditor+.

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.



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:



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…

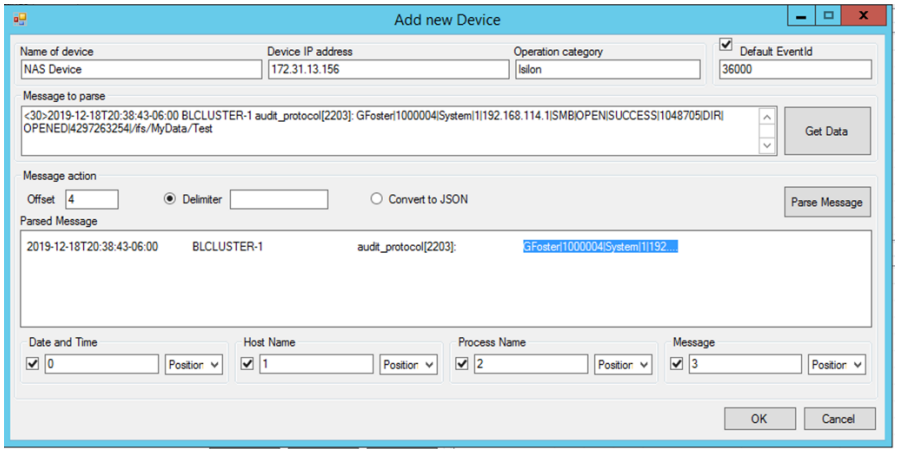
The goal is to identify the four components and to do so we set the following parameters:

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

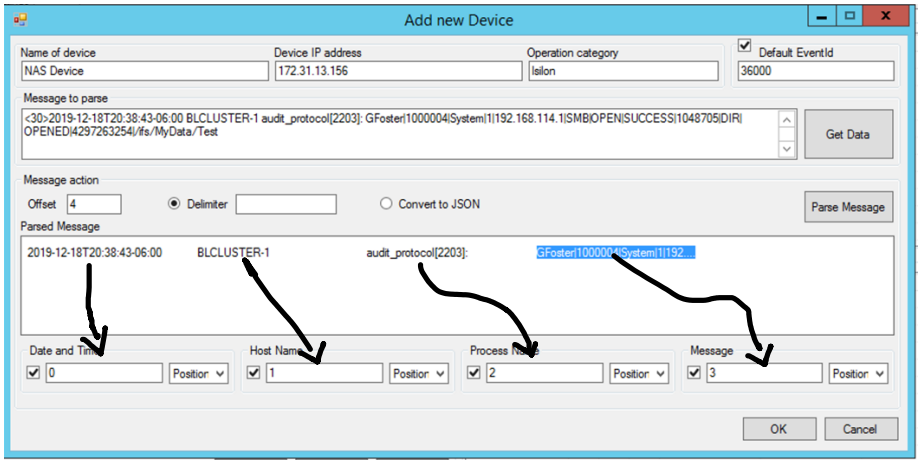
Delimiter – Select the delimiter to parse the components. For this device the delimiter appears to be the space character.

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:



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:

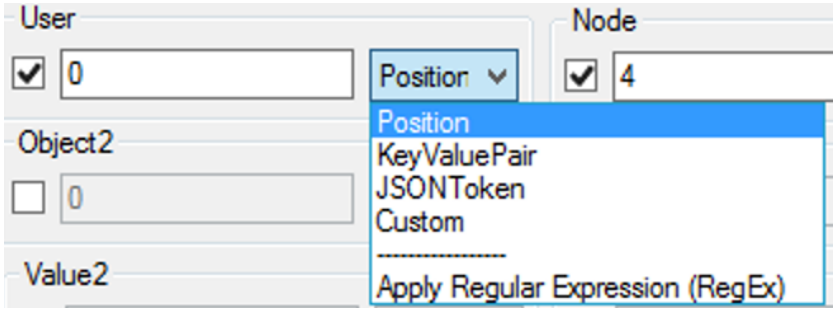


Component Box	Unchecked	Checked
Date and Time	Time computed when message was received	Selects parsed position to determine time
Host Name	Uses IP address of device	Selects parsed position for Hostname; Can use Custom in dropdown for custom value
Process Name	No value is recorded	Selects parsed position 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:



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:

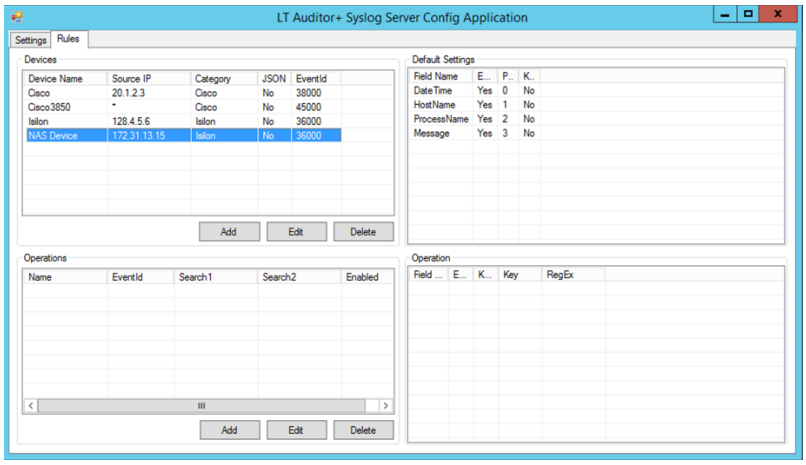
- If component has quotes or brackets like “Admin” or (Admin) apply RegEx expression [^0-9a-zA-Z]+ to strip out unwanted characters to get Admin
- If component has extra characters like 20.4.5.6:8000 apply RegEx expression :(.*) to get 20.4.5.6

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.

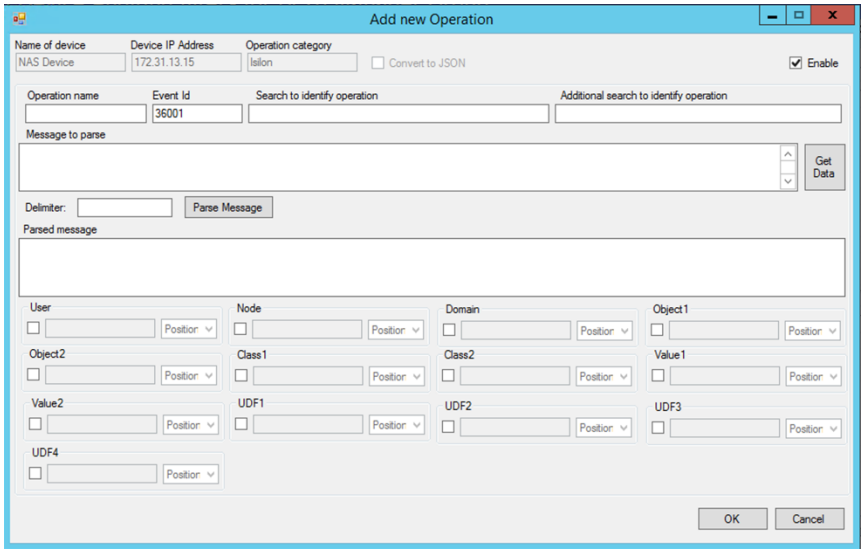
Click OK to save the Default Device Setting.

Add Operations Settings

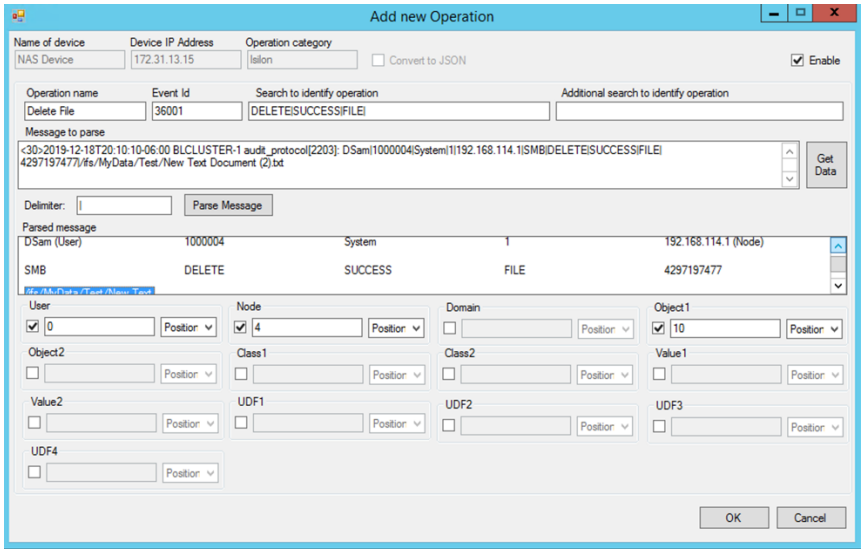
To add Operations, click on the newly added device in the Device box as shown below:



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



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.



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 DELETE|SUCCESS|FILE in the message to denote a delete file operation

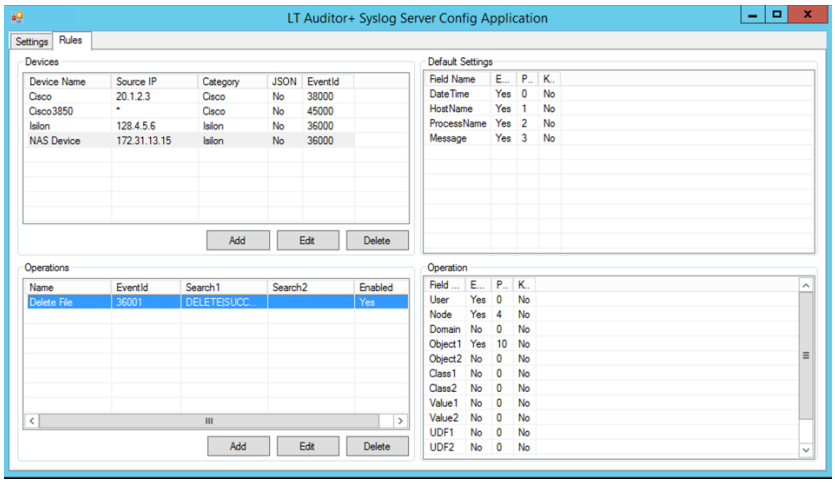
Additional search to identify operation – If there is an additional text string in the message to provide extra proof for the operation enter the text here. For our example we do not require this.

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

Parse Message – Click button to parse message.

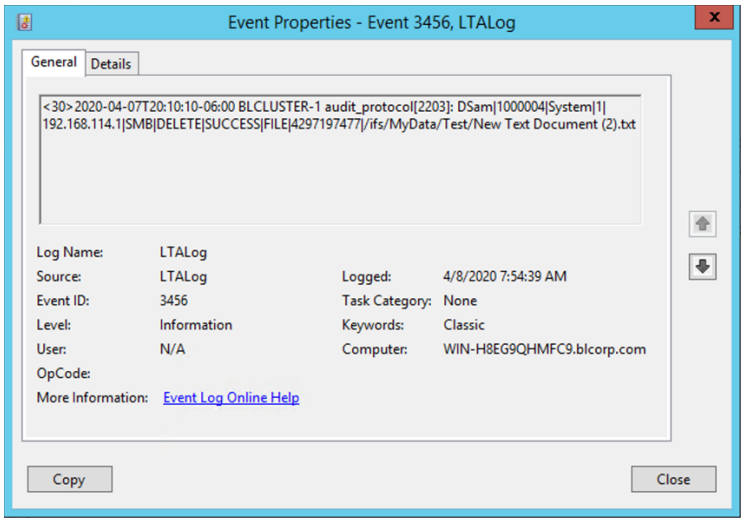
Drag and drop parsed text strings to the appropriate component boxes. In the example above: User, Node and Object1 boxes have been used. These denote the user, node and filename.

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

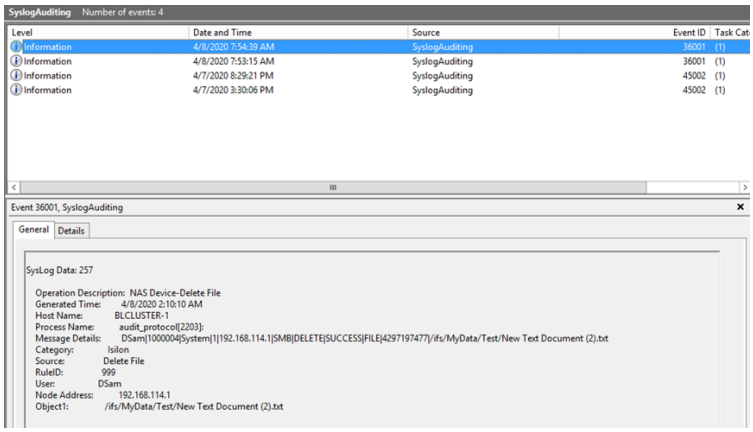


Verification that this rule is working can be obtained by reviewing the target event log and the rules event log as shown below:

Target Event Log



Rules Event Log (SyslogAuditing)



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.

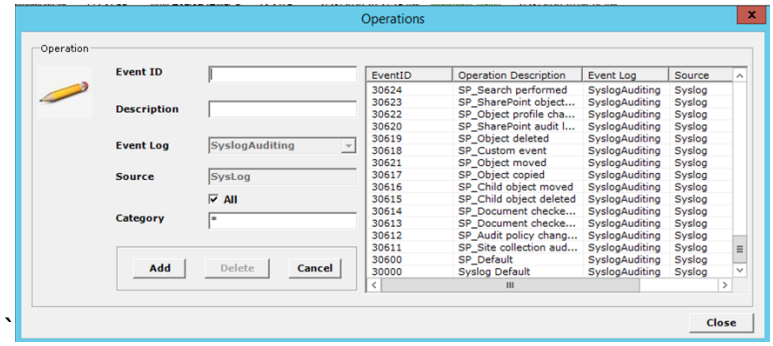
Configuring LT Auditor+ to alert and log events

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

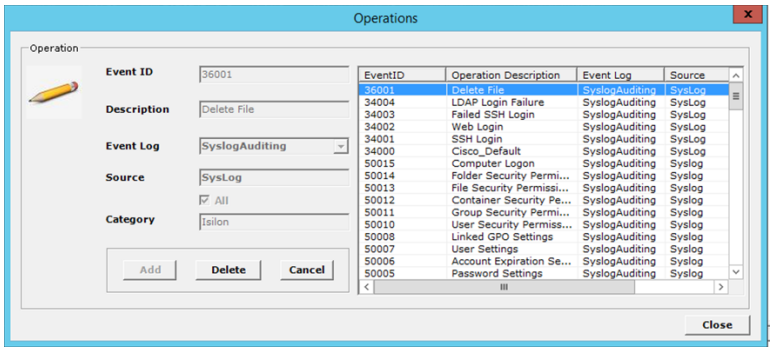
1. Create operations in LT Auditor+ to match operations created in LT Auditor+ Syslog Server
2. Create LT Auditor+ filters to capture and log the data. Alerting can be setup at this stage.
3. Create report queries to report on the data. Reports can be scheduled at this stage.

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



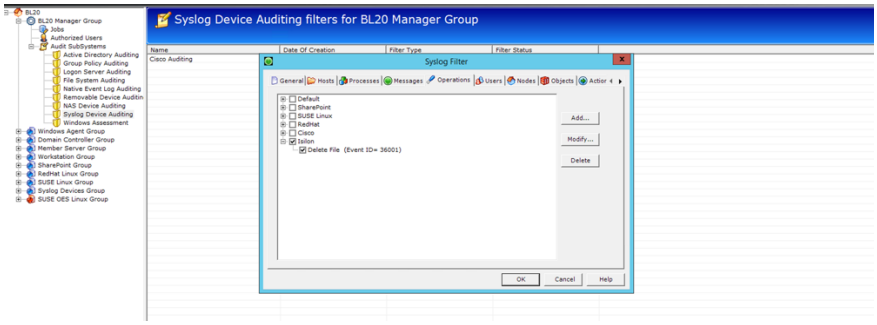
For our example enter information as shown in the screen above.



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

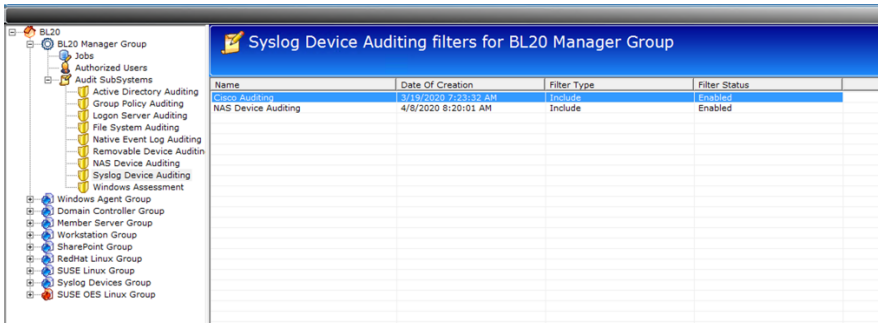
Create filters in LT Auditor+

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



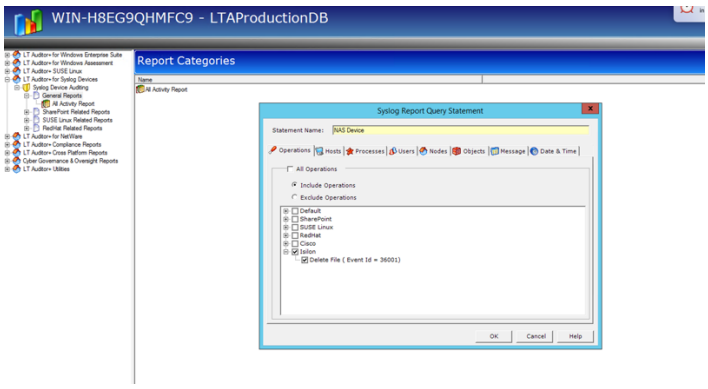
Alerting can be setup similar to any other event captured in LT Auditor+. Please refer to the LT Auditor+ Configuration guide for instructions on setting up alerts.

Click Ok to create the filter as shown below.

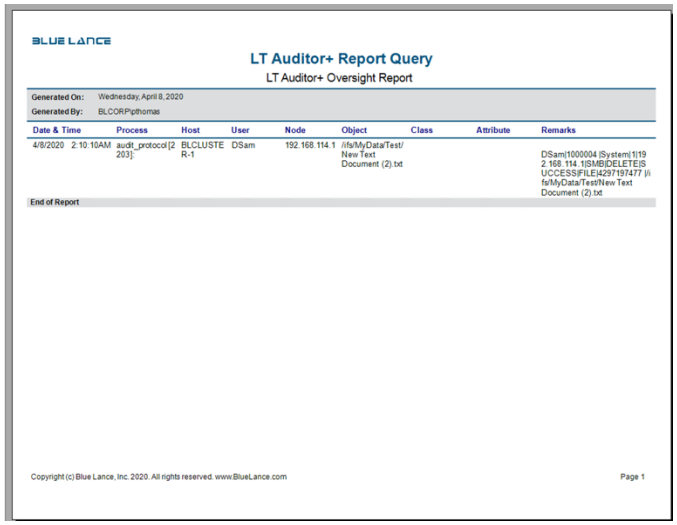


Create report queries in LT Auditor+

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.



BLUE LANCE

LT Auditor+ Report Query

LT Auditor+ Oversight Report

Generated On: Wednesday, April 8, 2020
Generated By: BLCORP\pthomas

Date & Time	Process	Host	User	Node	Object	Class	Attribute	Remarks
4/8/2020 2:10:10AM	audit_protocol[203]:	BLCLUSTER-1	DSam	192.168.114.1	/ifs/MyData/Test/New Text Document (2).txt			DSam\1000004 \System\1\192.168.114.1\SMB\DELETE\SUCCESS\FILE\4297197477 /ifs/MyData/Test/New Text Document (2).txt

End of Report

Copyright (c) Blue Lance, Inc. 2020. All rights reserved. www.BlueLance.com

Page 1

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.

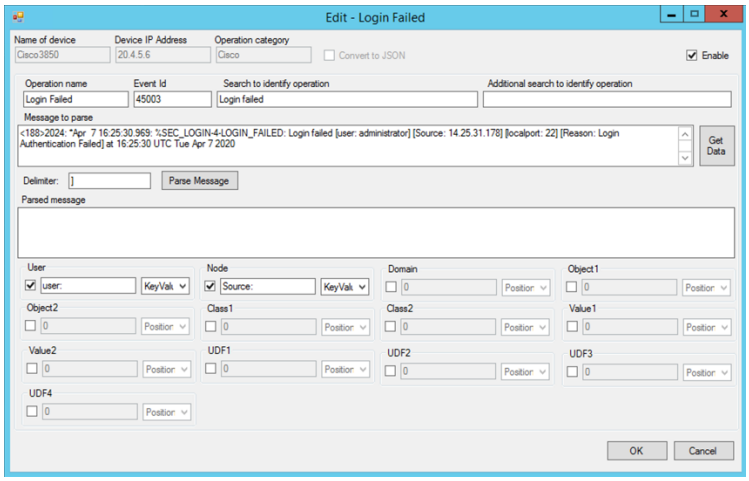
Appendix A

Examples of other methods of parsing syslog messages.

Parsing key value pairs

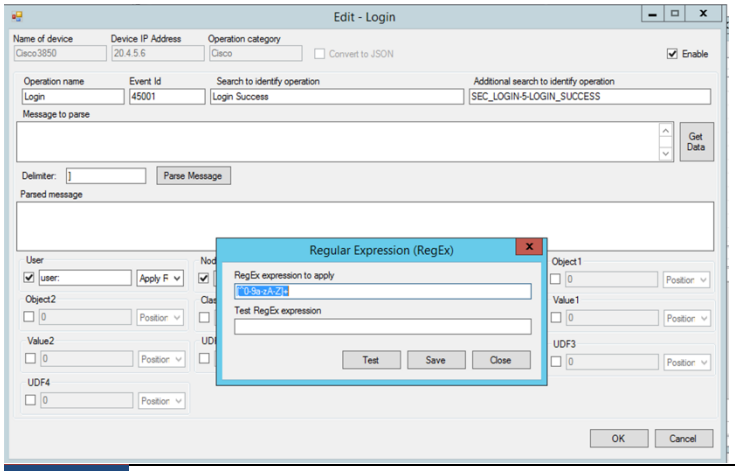
<188>2024: *Apr 7 16:25:30.969: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: administrator] [Source: 14.25.31.178] [localport: 22] [Reason: Login Authentication Failed] at 16:25:30 UTC Tue Apr 7 2020

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



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:



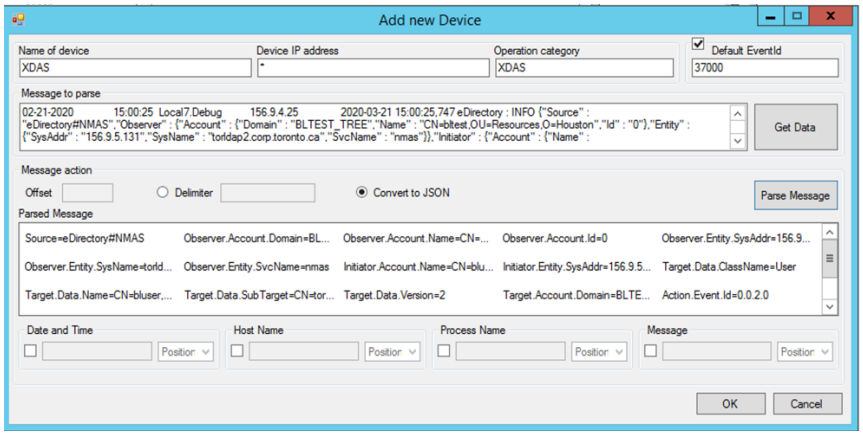
The RegEx expression '[^0-9a-zA-Z]+' removes all non-alphanumeric characters. For more information on RegEx commands review Appendix B.

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:



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