

The Zenoss Enablement Series:

How to Search and Display Logs with Kibana (v4.5+)

Document Version 500 – p2

Zenoss, Inc.

www.zenoss.com

Copyright © 2016-2017 Zenoss, Inc. 11305 Four Points Drive, Bldg. 1 - Suite 300, Austin, Texas 78726, U.S.A. All rights reserved.

Zenoss and the Zenoss logo are trademarks or registered trademarks of Zenoss, Inc. in the United States and other countries. All other trademarks, logos, and service marks are the property of Zenoss or other third parties. Use of these marks is prohibited without the express written consent of Zenoss, Inc. or the third-party owner.

Cisco, Cisco UCS, Cisco Unified Computing System, Cisco Catalyst, and Cisco Nexus are trademarks or registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

Flash is a registered trademark of Adobe Systems Incorporated.

Oracle, the Oracle logo, Java, and MySQL are registered trademarks of the Oracle Corporation and/or its affiliates. Linux is a registered trademark of Linus Torvalds.

SNMP Informant is a trademark of Garth K. Williams (Informant Systems, Inc.). Sybase is a registered trademark of Sybase, Inc.

Tomcat is a trademark of the Apache Software Foundation.

vSphere is a trademark of VMware, Inc. in the United States and/or other jurisdictions.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries. All other companies and products mentioned are

trademarks and property of their respective owners.

Table of Contents

Applies To	
Kibana and Control Center	
Log File Entries	2
Accessing Kibana Log File Entries Action Icons	
Searching Logs with Kibana Kibana Search Syntax	4
Kibana Time Range Search Filter	4
Performing a Kibana Log Search	5
Customizing the Search Results Fields	6
Saving and Recalling Searches	
Kibana Search Examples	9
-	

Applies To

The procedure outlined in this document applies to Zenosss 5.x with Control Center 1.2.x + and Kibana 4.5+.

Kibana and Control Center

Log files are an important part of the Control Center data. Control Center uses *Logstash* from Elastic (<u>https://www.elastic.co/products/logstash</u>) to monitor service daemon log files. It parses them and forwards them to *Elasticsearch*.

A browser-based user interface called *Kibana* enables you to display and search Elasticsearch databases, including the log files that Control Center monitors. For additional information about Kibana, see <u>https://www.elastic.co/products/kibana</u>.

Accessing Kibana

To access the Kibana interface:

- 1. Login to the Control Center UI.
- 2. Click the Logs tab to launch Kibana.

Control Center	Applications	Resource Pools	Hosts	Logs	Backup / Restore	👤 zenoss 💌 0	2	Logout	About
Logs									

The *Kibana* pane displays, where by default, Kibana retrieves the most recent log file entries. The entries display in the main pane together with a graph of results.

kibana	3 '	Discover	Visualize Dashboard S	ettings		O Last 30 days
fields.type:* AND message:*						
logstash-*	<					212,400 hits
Selected Fields					December 25th 2016, 14:08:3	34.037 - January 24th 2017, 14:08:34.038 — <u>by 12 hours</u>
t message						
? fields.type		100,000				
Available Fields	•	50.000				
 @timestamp 	_	0 00,000				
t @version		0				
t_id			2016-12-28 18:00	2016-12-31 18:00	2017-01-04 18:00	2017-01-08 18:00 2017-01-12 18:00 2017-01-16 18:00 2017-01-20 18:00 @timestamp per 12 hours
t _index						
# _score		Time	_	fields.type	message	
t_type						
? beat.hostname		 Janua 	ary 24th 2017, 14:08:27.297	hbase		26,524 [myid:1] - INFO :0.0.0.0/0.0.0.0:2181:NIOServerCnxnFactory@197] - Accepted socket connection from
? beat.name					/127.0.0.1:59072	
? count		 Janua 	ary 24th 2017, 14:08:27.297	hbase	2017 - 01 - 24 20 : 08 : 2	26,524 [myid:1] - INFO [NIOServerCxn.Factory:0.0.0.0/0.0.0.0:2181:NIOServerCnxn@821] -
? fields.ccWorkerID					Processing stat comm	nand from /127.0.0.1:59072
? fields.instance		 Janua 	ary 24th 2017, 14:08:27.297	hbase	2017 - 01 - 24 20 : 08 : 2	26,524 [myid:1] - INFO [Thread-549:NIOServerCnxn\$StatCommand@655] - Stat command output
? fields.monitor		 Janua 	ary 24th 2017, 14:08:27.297	bbasa	2017-01-24 20:08:2	26,525 [myid:1] - INFO [Thread-549:NIOServerCnxn@1001] - Closed socket connection for
? fields.service		• Janua	a y 2401 2017, 14.00.27.257	IIDase		0072 (no session established for client)
? file		Janua	ary 24th 2017, 14:08:25.736	opentsdb-reader	2017-01-24 20:08:2	24,999 INFO [New I/O server boss #17] ConnectionManager: [id: 0xb2462935,
t host			- ,			:42092 => /0:0:0:0:0:0:0:1:4242] OPEN
? input_type ? offset		Janua	ary 24th 2017, 14:08:25.736	opentsdb-reader	2017 - 01 - 24 20 : 08 : 2	24,999 INFO [New I/O worker #2] ConnectionManager: [id: 0xb2462935,
? tags			- ,			:42092 => /0:0:0:0:0:0:0:1:4242] BOUND: /0:0:0:0:0:0:0:1:4242
? type		 Janua 	ary 24th 2017, 14:08:25.736	opentsdb-reader		24,999 INFO [New I/O worker ≠2] ConnectionManager: [id: 0xb2462935, :42092 → /0:0:0:0:0:0:0:0:1:4242] CONNECTED: /0:0:0:0:0:0:0:0:1:42092
					/0.0.0.0.0.0.01	
		 Janua 	ary 24th 2017, 14:08:25.736	opentsdb-reader		55,002 INFO [New I/O worker #2] HttpQuery: [id: 0xb2462935, /0:0:0:0:0:0:0:0:1:42092 :1:4242] HTTP /api/stats done in 1ms
		 Janua 	ary 24th 2017, 14:08:25.736	opentsdb-reader		25,002 INF0 [New I/O worker #2] ConnectionManager: [id: 0xb2462935,

The search results graph displays in the top of the Kibana pane:

zope -get -post	٩		a d	ď
logstash.*				813 hits
Selected Fields	January 17th 2017, 14:34:56.283 - January 24th 2017, 14:34:56.284 — <u>by 3 hours</u>			
? _source	10 C	> ● Cou	unt	
Available Fields	± 200 -			
 @timestamp 	5 ₁₀₀			
t @version				
ℓ_id	0			
t _index	@imestamp per 3 hours			
# _score				

Log File Entries

Logstash parses each log file entry into fields and adds fields about the source and type of the entry. Note that different message *types* contain different *fields*.

To display the fields and data within a message, click on the message chevron. For example:

#_30010	Time 🗸	fields.type	message
t _type ? beat.hostname	January 26th 2017, 11:26:39.760	zenping	2017-01-26 17:26:35,760 INFO
? beat.name ? count	landary 26th 2017, 11:26:39.760	zenping	2017 - 01 - 26 17:26:35,760 INFO Missed_Runs: 0 Queued_Tasks: 0

The message details display:

Time 🗸	fields.type	message	<u> </u>		
January 26th 201	7, 11:26:39.760 zenping	2017 - 01 - 26 17 : 26 : 35,	760 INFO zen.zenping:	5 devices processed (312 datapoints)
Table JSON				Link	<pre>x to /logstash-2017.01.26/log/AVnb0KVLgmz-ehenbyWK</pre>
<pre>② @timestamp</pre>	🍳 🍳 🔲 January 26th 2017, 11:26	:39.760			
t @version	Q Q 🔲 1				
t_id	Q Q □ AVnb0KVLgmz-ehenbyWK				
t _index	@ @ □ logstash-2017.01.26				
#_score	@ @ □				
t_type	@ @ 🔲 log				
<pre>? beat.hostname</pre>	@ 🔍 🔟 🔺 c14911cbf6f4				
7 offset	@ @ []] 🛕 14450				
? tags	@ @ 🔲 🛕 beats_input_codec_pla	in_applied			
? type	🔍 🔍 🔟 🔺 log				
 January 26th 201 	7, 11:26:39.760 zenping	2017 - 01 - 26 17 : 26 : 35, Missed_Runs : 0 Queued_			Successful_Runs: 14 Failed_Runs: 0

Action Icons

The message details pane includes three action icons for each entry, with mouse-over (mouse hover) descriptions and grayed-out unavailable actions:

<u>Table</u> <u>J</u>	SON
② @timestamp	🗨 🗨 🔲 January 26th 2017, 11:26:39.760
t @version	QQ 🛛 <mark>1</mark>
t_id	👲 🖸 🔲 AVnb0KVLgmz-ehenbyWK
t _index	Filter for value logstash-2017.01.26
# _score	\oplus \bigcirc \square

The icons specify particular actions:

G Filter for value - Add a filter to match the selected field and value

Q Filter out value - Add a filter to not match (exclude messages with) the selected field and value.

Toggle column in table - Toggle the selected field display in the table.

Searching Logs with Kibana

Kibana Search Syntax

Kibana enables you to search the various fields within the logs. You can specify various criteria to refine the search results, including the timeframe for the search. The basic Kibana query syntax includes the following:

- String
- field:string
- field:"multi-word string"
- field:/regular-expression/

Notes:

- An asterisk (*) in the query string matches any set of characters, including the empty string
- A question mark (?) matches any single character
- Supported Boolean operators include:
 - AND

OR

NOT

- + (plus; must include)
- (minus; cannot include)
- Parenthesis can be used for grouping.

Kibana Time Range Search Filter

To specify or update the Kibana built-in time range filter:

1. The current time range displays in the top right of the Logs pane. Click the **current time range** to display the available time range filters:

kibana	Discover Visualiz	e Dashboard Settin	ngs		C Auto-refresh O Last 30 days
Quick	Today This week	Yesterday Day before yesterday	Last 15 minutes Last 30 minutes	Last 30 days Last 60 days	
Relative	This week This month This year	This day last week Previous week	Last 1 hour Last 4 hours	Last 60 days Last 90 days Last 6 months	
Absolute	The day so far Week to date Month to date Year to date	Previous month Previous year	Last 12 hours Last 24 hours Last 7 days	Last 1 year Last 2 years Last 5 years	

The main pane displays Quick options (default) in the center of the pane and options on the left side to set additional time range selections.

kibana	Discover Visualize	Dashboard Settir	ngs		C Auto-refresh 🧿 Last 7 days
Quick Relative M Absolute	Today This week This month This year The day so far Week to date Month to date Year to date	Yesterday Day before yesterday This day last week Previous week Previous month Previous year	Last 15 minutes Last 30 minutes Last 1 hour Last 4 hours Last 12 hours Last 24 hours Last 24 hours Last 7 days	Last 30 days Last 60 days Last 90 days Last 6 months Last 1 year Last 2 years Last 5 years	

- 2. Select a Range for the log filter:
 - a. A **Quick** (default) predefined range.
 - b. Select the appropriate option to apply it and trigger an auto-refresh.

OR

a. Specify a custom defined time range.Select **Relative** or **Absolute**, to display the specifications pane.

kibana	Discover Visualize	Dashboard Settings		
Quick Relative Absolute	From: January 21 5 I round to the day	st 2017, 00:00:00.000	To: Now Now	Go

b. Enter the time range definition to filter the log, and click Go.

kibar	Discover Visualize Dashboard Settings	
Quick	From: January 21st 2017, 00:00:00.000 To: Now	
Relative	5 Days ago V Now	Go
Absolute	✓ round to the day	10
	A	

3. Click the current time range in the upper right, or the chevron in the center of the pane to close the options pane.

Performing a Kibana Log Search

1. To begin a Kibana search, enter a search string in the top field of the Logs pane:

	kibana	Discover	Visualize	Dashboard	Settings	
	fields.type:* AND message:*					Q
le	ogstash-* 🧎 🕻 🗸					
S	elected Fields				December 27th 2016, 12:36:26.952 - January 26th 2017, 12:36:26.952 — <u>by 12 hours</u>	

Q

- 2. Click Enter (or the magnifying glass icon Q) to begin the search and display the results
- 3. To begin a new search, click **New Search** to clear the previous search begin:

Dashboard	Settings					🕘 La	ast 30 days
			Q		8		
			7	New Searc	h	:	2,050 hits
		December 25th 2016, 14:20:33.154 - January 24th 2017, 14:20:33.155 — <u>by 12 hours</u>					
							<

Customizing the Search Results Fields

You can customize which fields display in the search results messages. The left pane displays both currently **Selected Fields** (applied) and **Available Fields** (not yet applied):

logstash-*	<
Selected Fields	
t message	
? fields.type	
Available Fields	
② @timestamp	
t @version	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	

The pane includes a list of pre-define fields. These fields can be optionally applied to the Log display table:

ogstash-*	<
Selected Fields	
? _source	1,500 -
Available Fields	
<ul> <li>@timestamp</li> </ul>	1,000 -
t @version	500 -
₹_id	0
₹_index	
# _score	
≀_type	Time 🚽
? beat.hostname	
? beat.name	<ul> <li>January</li> </ul>
? count	
? fields.ccWorkerID	
? fields.instance	
? fields.service	January
? fields.type	<ul> <li>January</li> </ul>
? file	
t host	
? input_type	
t message	January
Quick Count () ( 500 /500 records )	<ul> <li>January</li> </ul>
172.17.0.28 - admin [24/Jan/2017:1 Q Q	
172.17.0.28 - admin [24/Jan/2017:1 QQ	
0.4%	
172.17.0.28 - admin [24/Jan/2017:1 Q Q	January
172.17.0.28 - admin [24/Jan/2017:1 Q Q	
172.17.0.28 - admin (24/Jan/2017:1 QQ	
Visualize ( 1 warning 🗚 )	
? offset	<ul> <li>January</li> </ul>
? tags	
? type	

To change which fields (columns) are visible within the Log display table:

1. Consult the left pane to discover the currently **Selected Fields** (applied) and **Available Fields** (not yet applied):

logstash-*	<
Selected Fields	
t message	
? fields.type	
Available Fields	
② @timestamp	
t @version	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	

2. To add a field (column) to include in the log display table, mouse-over (mouse hover) the field to display add. Click add:

logstash-*	<
Selected Fields	
t message	
? fields.type	
Available Fields	
② @timestamp	
t @version	
t_id	
t _index	adt
# _score	

3. To verify the new field displays, look at the Log message table. The new column, named _*index* in this example, now shows within the list:

			^	
	Time 🗸	fields.type	message * 🗙 « »	_index
×	January 26th 2017, 12:36:17.693	zauth_access_logs	127.0.0.1 - Anonymous [26/Jan/2017:18:36:17] +0000] "GET /zport/dmd HTTP/1.1" 302 2954 "" "curl/7.29.0"	logstash- 2017.01.26
×	January 26th 2017, 12:36:14.693	zauth_access_logs	127.0.0.1 - Anonymous [26/Jan/2017:18:36:12 +0000] "GET /zport/dmd HTTP/1.1" 302 2954 "" "curl/7.29.0"	logstash- 2017.01.26
•	January 26th 2017, 12:36:14.355	centralquery	ERROR [2017-01-26 18:36:09,054] com.sun.jersey.spi.co	logscash-

4. To remove a currently displayed field (column) from the log display table, mouse-over (mouse hover) the field to display *remove*. Click **remove**:



Saving and Recalling Searches

The Kibana engine enables both saving searches and recalling searches for reuse.

Save Current Search

2.

To save the current search:

1. Click Save Search.

Dashboard Settings	O Last 30 days
December 25lh 2016, 14:20:33.154 - January 24lh 2017, 1	14:20:33.155 — <u>by 12 hours</u>
Enter a descriptive name for the search and click S	Save.
	_
Save Search	
My new seardh	
Save	

Recall a Saved Search

To recall a saved search for reuse:

1. Click Load Saved Search.

2. Find and click the name of the saved search.

audit.log	Q	ß	B	Þ	ß
Saved Search Filter		m		aved se	arches
My new search					

Kibana displays a searching message and then displays the completed search.

Kibana Search Examples

Effective use of the Kibana search engine requires use of appropriate search strings that return the required information. The following are examples of useful search strings.

Search Expression	Returns
audit.log	messages from the audit log
audit.log – "user=unknown"	messages from the audit log involving known users
event.log	event.log entries. Note : The event.log file is where Zope logs non-HTTP related messages.
Z2.log	Z2.log entries Note : The Z2.log contains HTTP messages.
zenperfsnmp- INFO	messages from the zenperfsnmp service omitting INFO level messages. Note: Although any service name can be used in place of <i>zenperfsnmp</i> , only some services specify a log level. The query will work even in the absence of a log level.