The Zenoss Enablement Series:

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

Document Version 500 – p2

Zenoss, Inc.

www.zenoss.com

Table of Contents

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

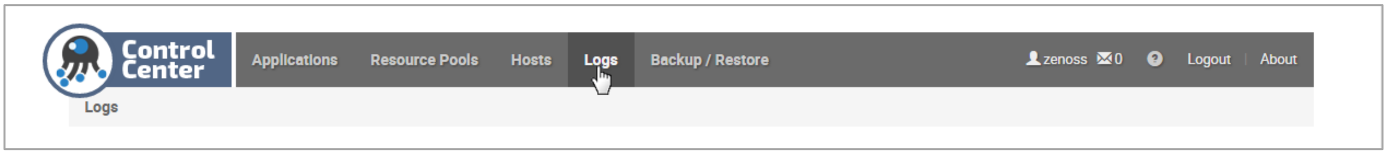
Log files are an important part of the Control Center data. Control Center uses *Logstash* from Elastic (https://www.elastic.co/products/logstash) to monitor service daemon log files. It parses them and forwards them to *Elasticsearch*.

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 https://www.elastic.co/products/kibana.

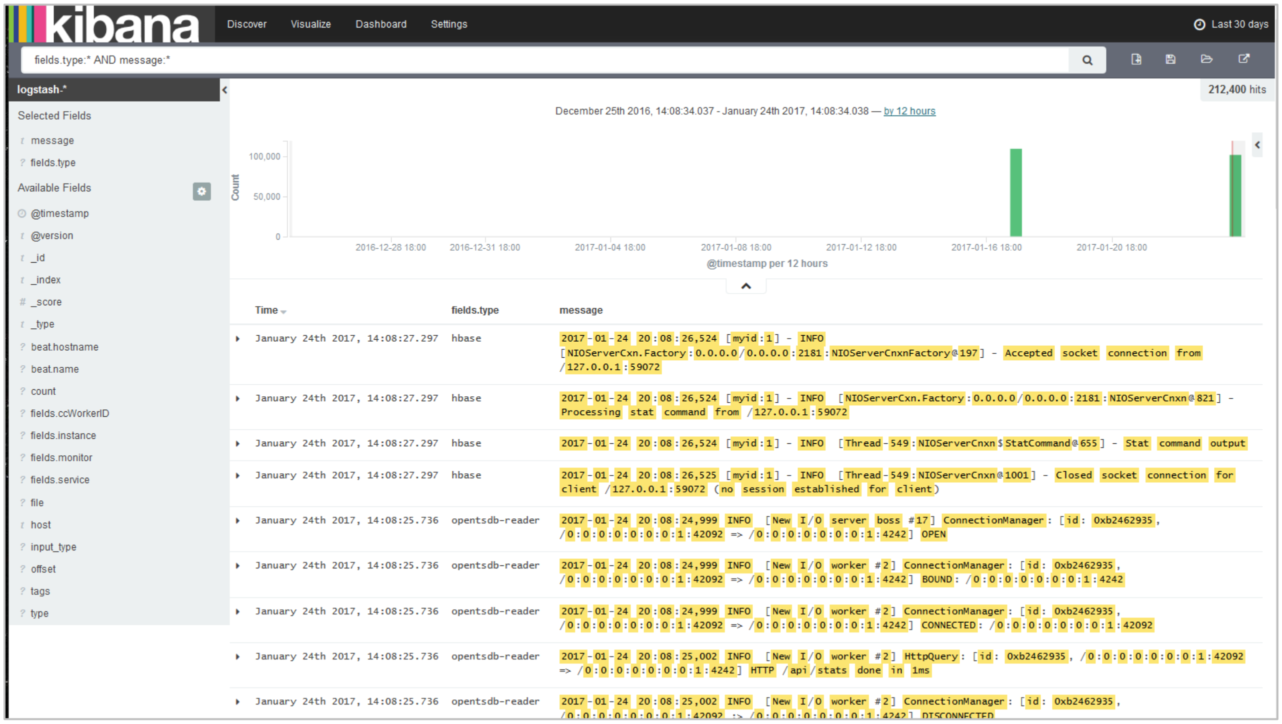
Accessing Kibana

To access the Kibana interface:

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

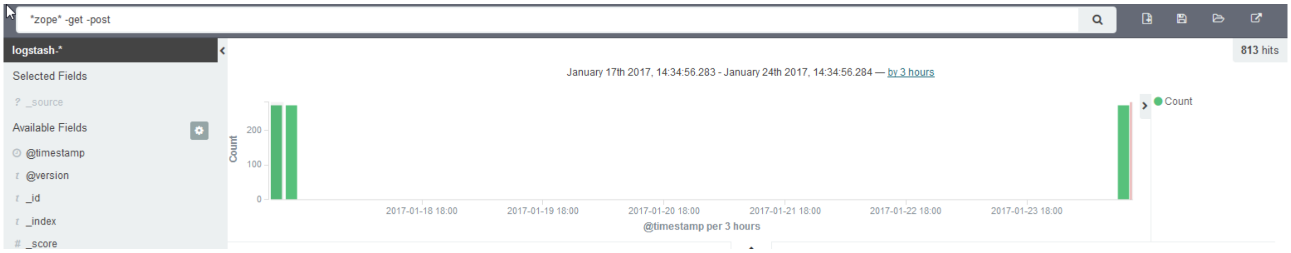


The *Kibana* pane displays, where by default, Kibana retrieves the most recent log file entries. The entries display in the main pane together with a graph of results.



Time	fields.type	message
January 24th 2017, 14:08:27.297	hbase	2017-01-24 20:08:26,524 [myid:1] - INFO [NIOServerCxn.Factory:0.0.0.0/0.0.0.0:2181:NIOServerCnxnFactory@197] - Accepted socket connection from /127.0.0.1:59072
January 24th 2017, 14:08:27.297	hbase	2017-01-24 20:08:26,524 [myid:1] - INFO [NIOServerCxn.Factory:0.0.0.0/0.0.0.0:2181:NIOServerCnxn@821] - Processing stat command from /127.0.0.1:59072
January 24th 2017, 14:08:27.297	hbase	2017-01-24 20:08:26,524 [myid:1] - INFO [Thread-549:NIOServerCnxn$StatCommand@655] - Stat command output
January 24th 2017, 14:08:27.297	hbase	2017-01-24 20:08:26,525 [myid:1] - INFO [Thread-549:NIOServerCnxn@1001] - Closed socket connection for client /127.0.0.1:59072 (no session established for client)
January 24th 2017, 14:08:25.736	opentsdb-reader	2017-01-24 20:08:24,999 INFO [New I/O server boss #17] ConnectionManager: [id: 0xb2462935, /0:0:0:0:0:0:0:1:42092 => /0:0:0:0:0:0:0:1:4242] OPEN
January 24th 2017, 14:08:25.736	opentsdb-reader	2017-01-24 20:08:24,999 INFO [New I/O worker #2] ConnectionManager: [id: 0xb2462935, /0:0:0:0:0:0:0:1:42092 => /0:0:0:0:0:0:0:1:4242] BOUND: /0:0:0:0:0:0:0:1:4242
January 24th 2017, 14:08:25.736	opentsdb-reader	2017-01-24 20:08:24,999 INFO [New I/O worker #2] ConnectionManager: [id: 0xb2462935, /0:0:0:0:0:0:0:1:42092 => /0:0:0:0:0:0:0:1:4242] CONNECTED: /0:0:0:0:0:0:0:1:42092
January 24th 2017, 14:08:25.736	opentsdb-reader	2017-01-24 20:08:25,002 INFO [New I/O worker #2] HttpQuery: [id: 0xb2462935, /0:0:0:0:0:0:0:1:42092 => /0:0:0:0:0:0:0:1:4242] HTTP /api/stats done in 1ms
January 24th 2017, 14:08:25.736	opentsdb-reader	2017-01-24 20:08:25,002 INFO [New I/O worker #2] ConnectionManager: [id: 0xb2462935, /0:0:0:0:0:0:0:1:42092 => /0:0:0:0:0:0:0:1:4242] DISCONNECTED

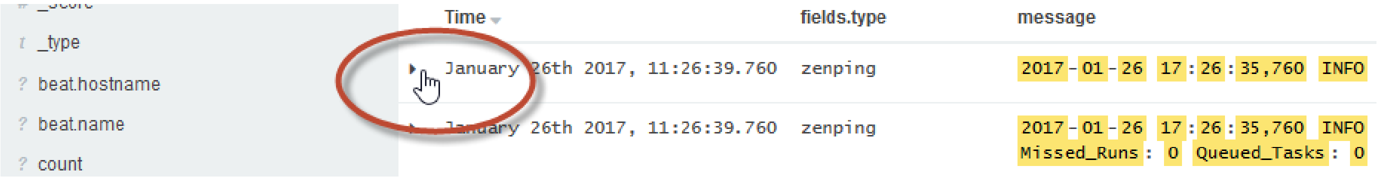
The search results graph displays in the top of the Kibana pane:



Log File Entries

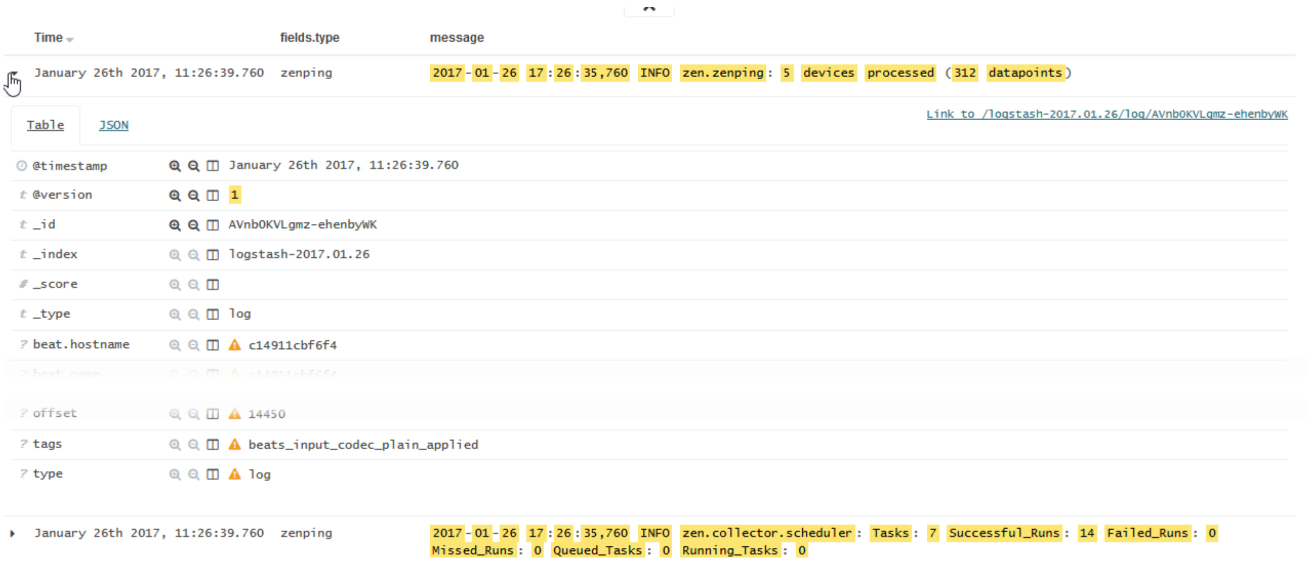
Logstash parses each log file entry into fields and adds fields about the source and type of the entry. Note that different message *types* contain different *fields*.

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



Time	fields.type	message
January 26th 2017, 11:26:39.760	zenping	2017-01-26 17:26:35,760 INFO
January 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
January 26th 2017, 11:26:39.760	zenping	2017-01-26 17:26:35,760 INFO zen.zenping: 5 devices processed (312 datapoints)

Table JSON

Link to /logstash-2017.01.26/log/AVnbOKVLgmz-ehenbyWK

@timestamp	January 26th 2017, 11:26:39.760
@version	1
_id	AVnbOKVLgmz-ehenbyWK
_index	logstash-2017.01.26
_score	
_type	log
beat.hostname	⚠ c14911cbf6f4
beat.name	⚠ c14911cbf6f4
offset	⚠ 14450
tags	⚠ beats_input_codec_plain_applied
type	⚠ log

January 26th 2017, 11:26:39.760	zenping	2017-01-26 17:26:35,760 INFO zen.collector.scheduler: Tasks: 7 Successful_Runs: 14 Failed_Runs: 0 Missed_Runs: 0 Queued_Tasks: 0 Running_Tasks: 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:

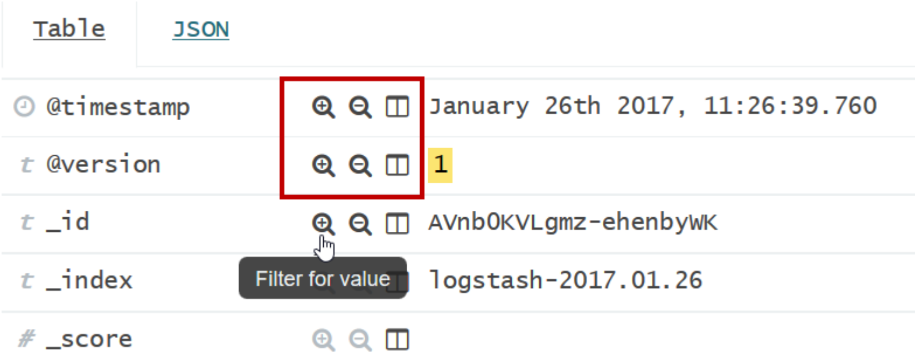


Table JSON

@timestamp	January 26th 2017, 11:26:39.760
@version	1
_id	AVnbOKVLgmz-ehenbyWK
_index	logstash-2017.01.26
_score	

The icons specify particular actions:

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

⊖ **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)

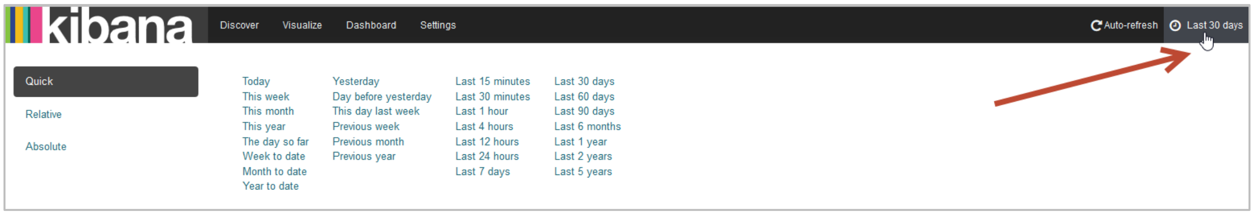
  `–` (minus; cannot include)

- Parenthesis can be used for grouping.

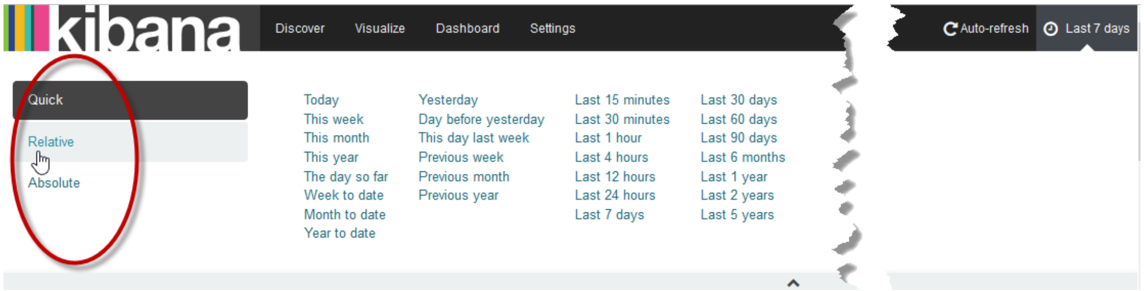
Kibana Time Range Search Filter

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:



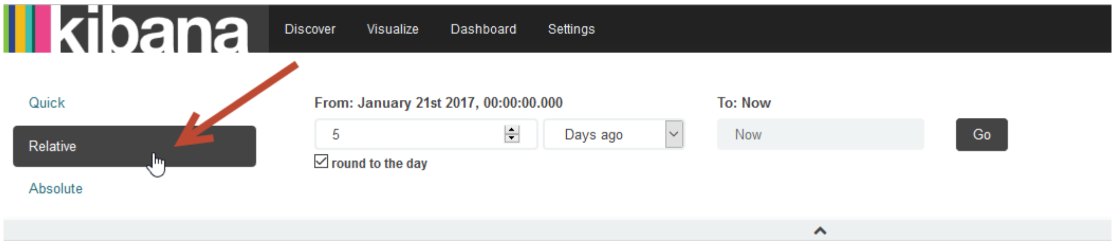
The main pane displays Quick options (default) in the center of the pane and options on the left side to set additional time range selections.



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.



From: January 21st 2017, 00:00:00.000

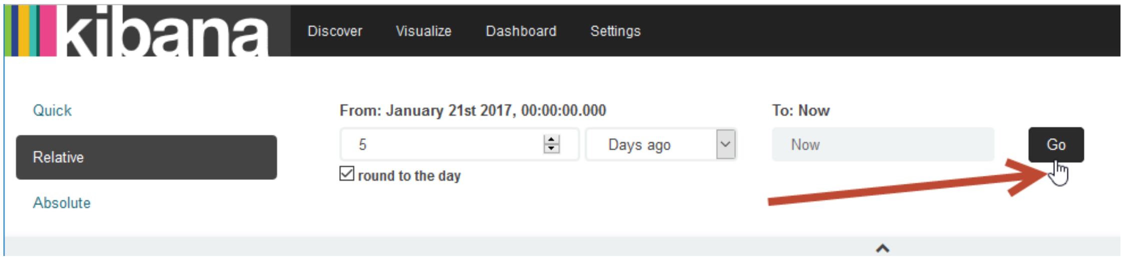
5 Days ago

☑ round to the day

To: Now

Now

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



From: January 21st 2017, 00:00:00.000

5 Days ago

☑ round to the day

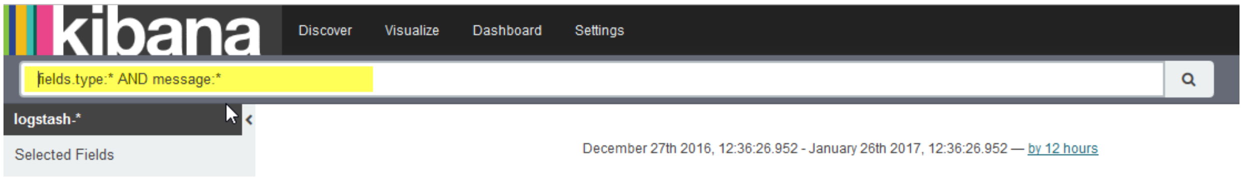
To: Now

Now

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:



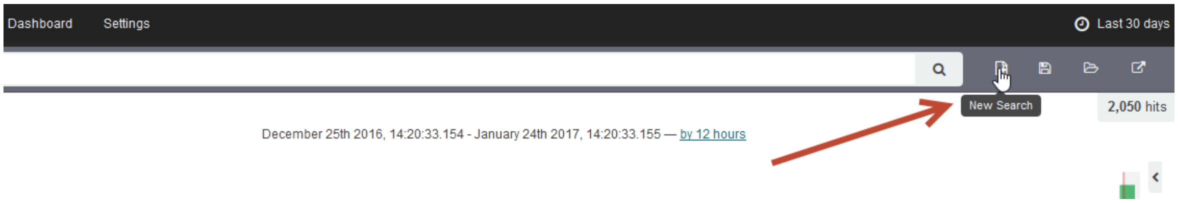
fields.type:* AND message:*

logstash-*

December 27th 2016, 12:36:26.952 - January 26th 2017, 12:36:26.952 — by 12 hours

2. Click **Enter** (or the magnifying glass icon 🔍) to begin the search and display the results

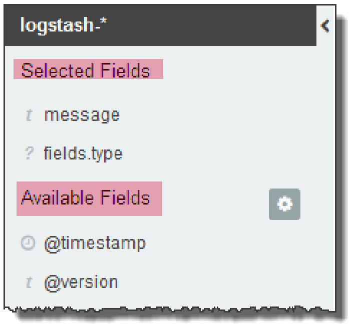
3. To begin a new search, click **New Search** to clear the previous search begin:



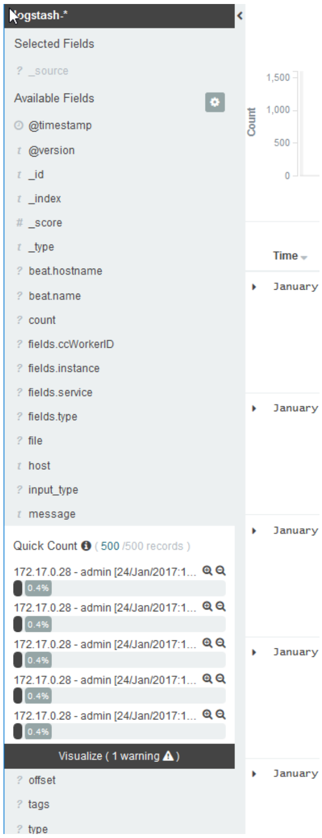
December 25th 2016, 14:20:33.154 - January 24th 2017, 14:20:33.155 — by 12 hours

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):



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

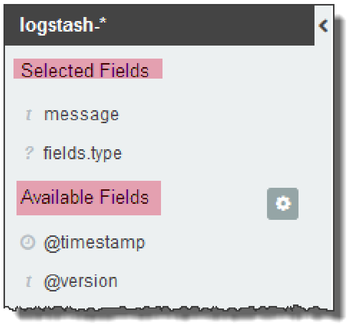


(500 /500 records)

```
172.17.0.28 - admin [24/Jan/2017:1...
0.4%
172.17.0.28 - admin [24/Jan/2017:1...
0.4%
172.17.0.28 - admin [24/Jan/2017:1...
0.4%
172.17.0.28 - admin [24/Jan/2017:1...
0.4%
172.17.0.28 - admin [24/Jan/2017:1...
0.4%
```

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

message

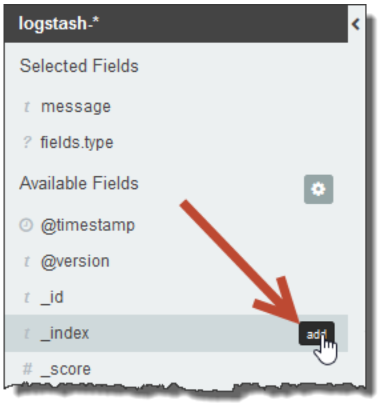
fields.type

Available Fields

@timestamp

@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

message

fields.type

Available Fields

@timestamp

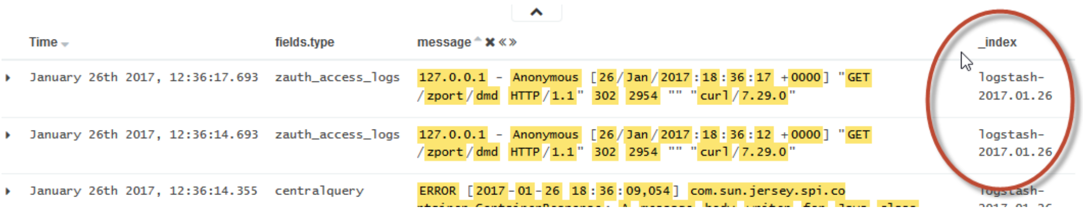
@version

_id

_index

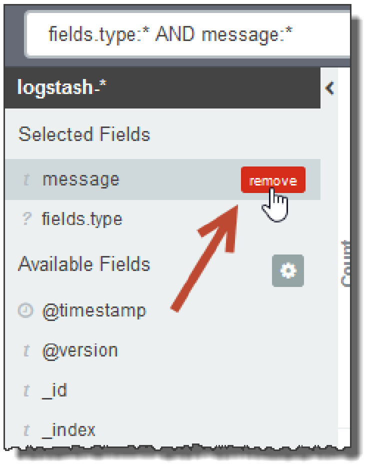
_score

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	logstash-

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



fields.type:* AND message:*

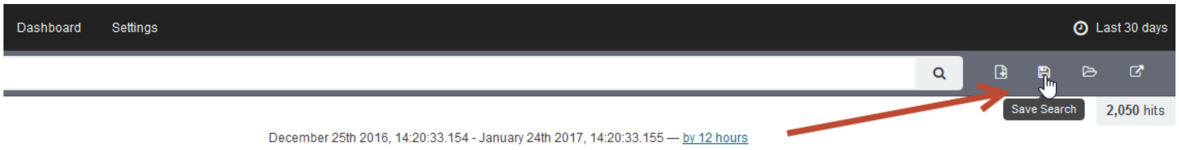
Saving and Recalling Searches

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

Save Current Search

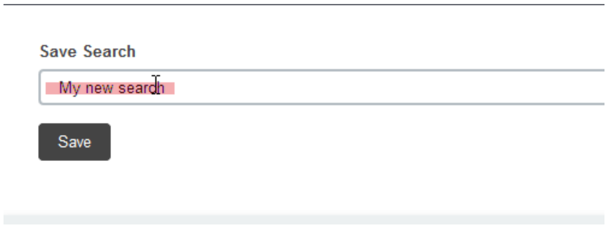
To save the current search:

1. Click **Save Search.**



December 25th 2016, 14:20:33.154 - January 24th 2017, 14:20:33.155 — by 12 hours

2. Enter a descriptive name for the search and click **Save.**



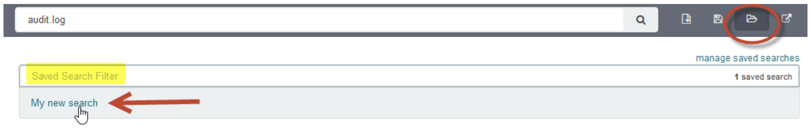
My new search

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

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 *zenperfsnmp,* only some services specify a log level. The query will work even in the absence of a log level.