The Zenoss Enablement Series:

How to Search and Display Logs with Kibana

Document Version 500 - p1

Zenoss, Inc.

www.zenoss.com

Table of Contents

Applies To

The procedure outlined in this document applies to Zenosss 5.x Control Center.

Kibana and Control Center

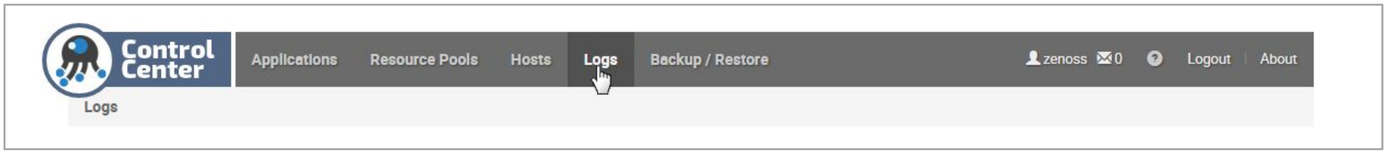
Log files are an important part of the Control Center data. Control Center uses *Logstash* from Elastic (https://www.elastic.co/products/logstash) to monitor service daemon log files. It parses them and forwards them to *Elasticsearch*.

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.

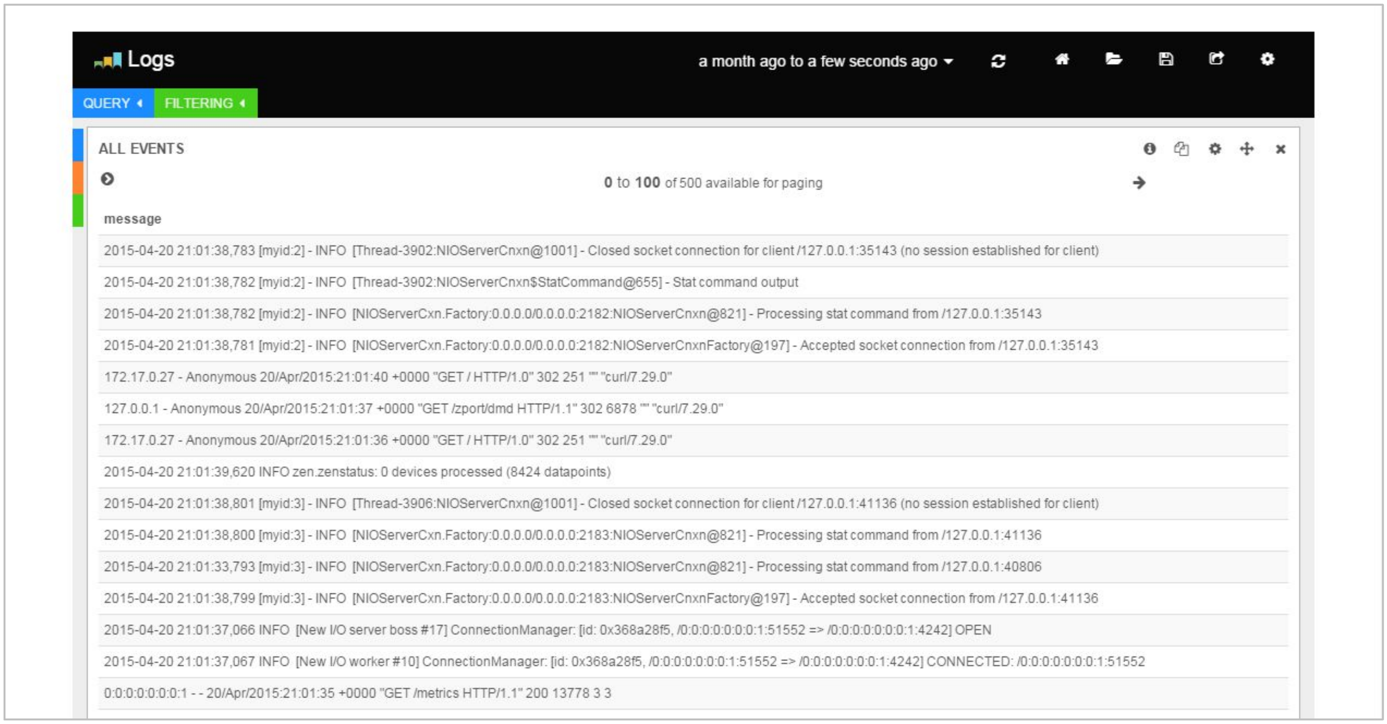
Accessing Kibana

To access the Kibana interface:

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



The *Logs* pane displays, where by default, Kibana retrieves the 500 most recent log file entries and displays them in table form, 100 per page.



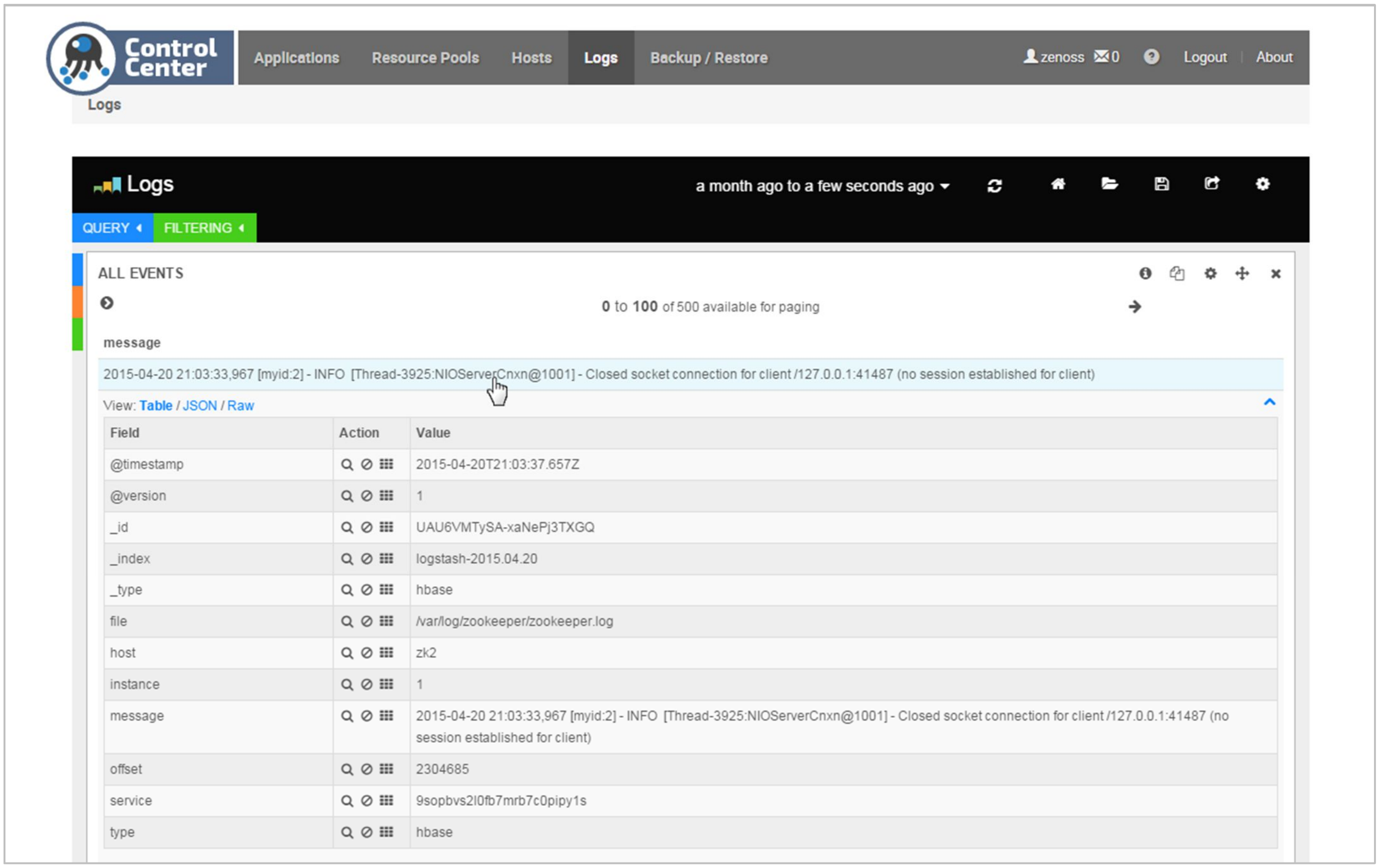
0 to 100 of 500 available for paging

```
message
2015-04-20 21:01:38,783 [myid:2] - INFO  [Thread-3902:NIOServerCnxn@1001] - Closed socket connection for client /127.0.0.1:35143 (no session established for client)
2015-04-20 21:01:38,782 [myid:2] - INFO  [Thread-3902:NIOServerCnxn$StatCommand@655] - Stat command output
2015-04-20 21:01:38,782 [myid:2] - INFO  [NIOServerCxn.Factory:0.0.0.0/0.0.0.0:2182:NIOServerCnxn@821] - Processing stat command from /127.0.0.1:35143
2015-04-20 21:01:38,781 [myid:2] - INFO  [NIOServerCxn.Factory:0.0.0.0/0.0.0.0:2182:NIOServerCnxnFactory@197] - Accepted socket connection from /127.0.0.1:35143
172.17.0.27 - Anonymous 20/Apr/2015:21:01:40 +0000 "GET / HTTP/1.0" 302 251 "" "curl/7.29.0"
127.0.0.1 - Anonymous 20/Apr/2015:21:01:37 +0000 "GET /zport/dmd HTTP/1.1" 302 6878 "" "curl/7.29.0"
172.17.0.27 - Anonymous 20/Apr/2015:21:01:36 +0000 "GET / HTTP/1.0" 302 251 "" "curl/7.29.0"
2015-04-20 21:01:39,620 INFO zen.zenstatus: 0 devices processed (8424 datapoints)
2015-04-20 21:01:38,801 [myid:3] - INFO  [Thread-3906:NIOServerCnxn@1001] - Closed socket connection for client /127.0.0.1:41136 (no session established for client)
2015-04-20 21:01:38,800 [myid:3] - INFO  [NIOServerCxn.Factory:0.0.0.0/0.0.0.0:2183:NIOServerCnxn@821] - Processing stat command from /127.0.0.1:41136
2015-04-20 21:01:33,793 [myid:3] - INFO  [NIOServerCxn.Factory:0.0.0.0/0.0.0.0:2183:NIOServerCnxn@821] - Processing stat command from /127.0.0.1:40806
2015-04-20 21:01:38,799 [myid:3] - INFO  [NIOServerCxn.Factory:0.0.0.0/0.0.0.0:2183:NIOServerCnxnFactory@197] - Accepted socket connection from /127.0.0.1:41136
2015-04-20 21:01:37,066 INFO  [New I/O server boss #17] ConnectionManager: [id: 0x368a28f5, /0:0:0:0:0:0:0:1:51552 => /0:0:0:0:0:0:0:1:4242] OPEN
2015-04-20 21:01:37,067 INFO  [New I/O worker #10] ConnectionManager: [id: 0x368a28f5, /0:0:0:0:0:0:0:1:51552 => /0:0:0:0:0:0:0:1:4242] CONNECTED: /0:0:0:0:0:0:0:1:51552
0:0:0:0:0:0:0:1 - - 20/Apr/2015:21:01:35 +0000 "GET /metrics HTTP/1.1" 200 13778 3 3
```

Log File Entries

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

To display the fields within a message, click on the **message row**. For example:



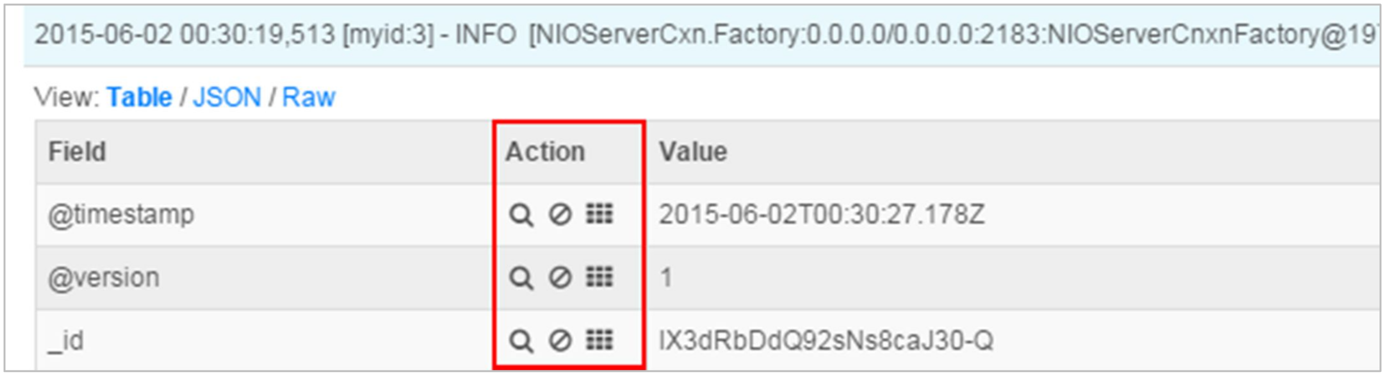
2015-04-20 21:03:33,967 [myid:2] - INFO [Thread-3925:NIOServerCnxn@1001] - Closed socket connection for client /127.0.0.1:41487 (no session established for client)

View: Table / JSON / Raw

Field	Action	Value
@timestamp	🔍 ⊘ ▦	2015-04-20T21:03:37.657Z
@version	🔍 ⊘ ▦	1
_id	🔍 ⊘ ▦	UAU6VMTySA-xaNePj3TXGQ
_index	🔍 ⊘ ▦	logstash-2015.04.20
_type	🔍 ⊘ ▦	hbase
file	🔍 ⊘ ▦	/var/log/zookeeper/zookeeper.log
host	🔍 ⊘ ▦	zk2
instance	🔍 ⊘ ▦	1
message	🔍 ⊘ ▦	2015-04-20 21:03:33,967 [myid:2] - INFO [Thread-3925:NIOServerCnxn@1001] - Closed socket connection for client /127.0.0.1:41487 (no session established for client)
offset	🔍 ⊘ ▦	2304685
service	🔍 ⊘ ▦	9sopbvs2l0fb7mrb7c0pipy1s
type	🔍 ⊘ ▦	hbase

Action Icons

The field details include three action icons:



2015-06-02 00:30:19,513 [myid:3] - INFO [NIOServerCxn.Factory:0.0.0.0/0.0.0.0:2183:NIOServerCnxnFactory@19

View: Table / JSON / Raw

Field	Action	Value
@timestamp	🔍 ⊘ ▦	2015-06-02T00:30:27.178Z
@version	🔍 ⊘ ▦	1
_id	🔍 ⊘ ▦	IX3dRbDdQ92sNs8caJ30-Q

The icons specify particular actions:

🔍 Add a filter to match the selected field and value.

⊘ Add a filter to **not** match (exclude messages with) the selected field and value.

▦ 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)

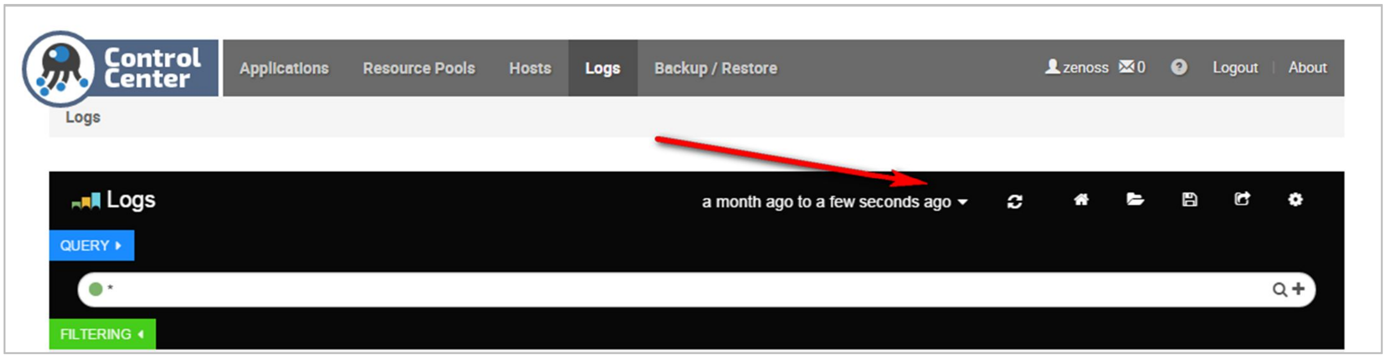
  − (minus; cannot include)

- Parenthesis can be used for grouping.

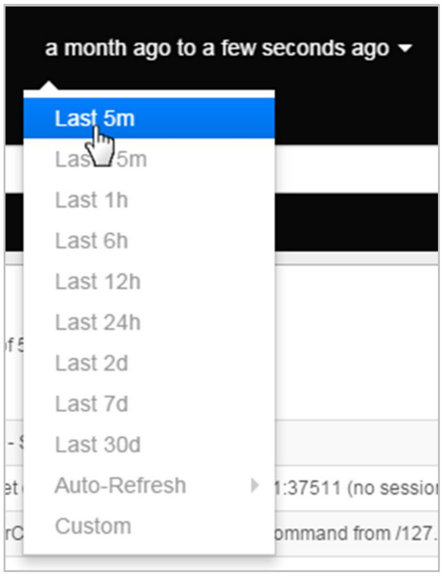
Kibana Time Range Search Filter

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

1. Click the current time range (with down chevron) located in the top of the **Logs** pane:



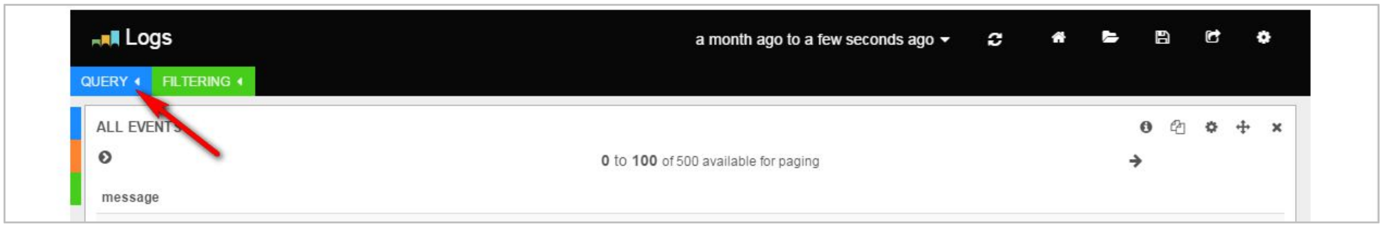
The drop down menu displays additional time range selections.



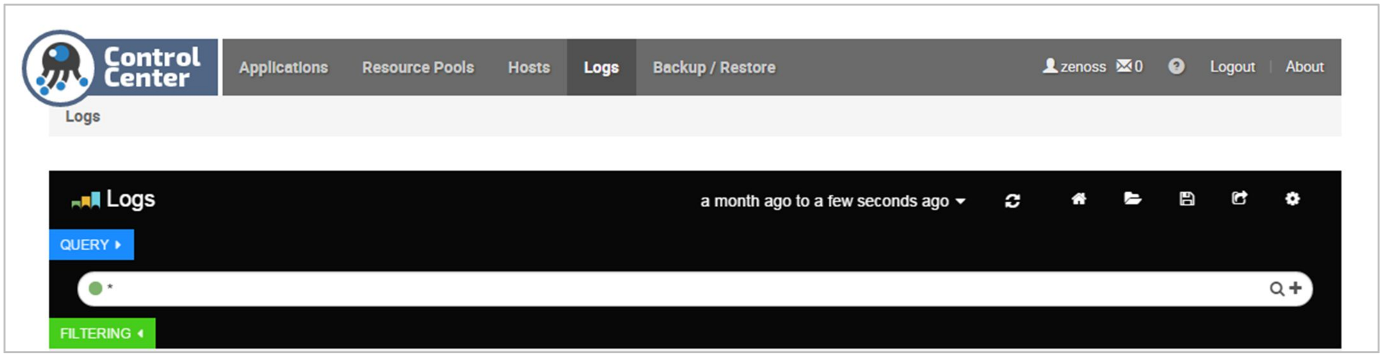
2. Select the appropriate option to save and close the drop down menu.

Performing a Kibana Log Search

1. To begin a Kibana search, click the QUERY ◂ button in the top left of the **Logs** pane:


Logs
a month ago to a few seconds ago ▾
QUERY ◂
FILTERING ◂
ALL EVENTS
0 to 100 of 500 available for paging
message

The query search field displays:

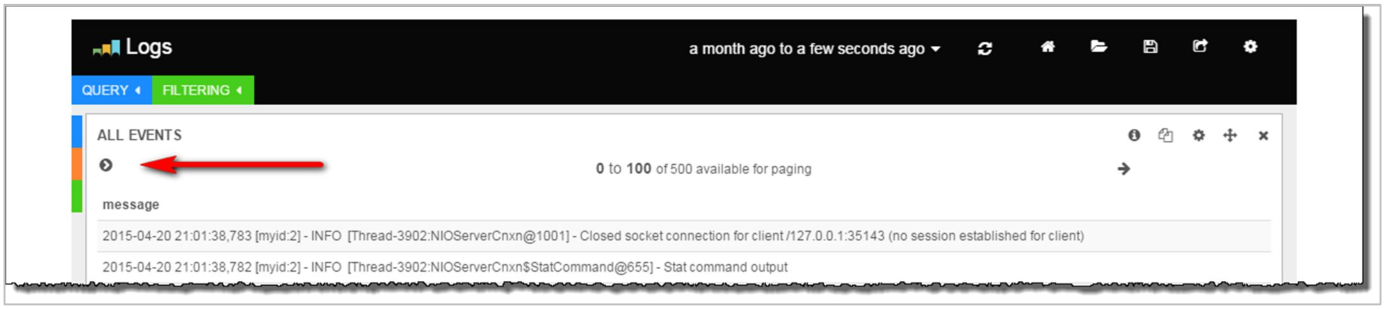


2. Enter the search string
3. Click **Enter** (or the magnifying glass icon 🔍) to begin the search and display the results.

Customizing the Search Results Fields

You can customize which fields display in the search results messages. To change which fields are visible:

1. Click the field list icon ❯ to open the **Field** list.



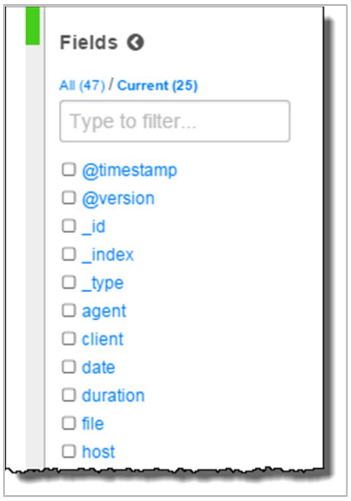
ALL EVENTS

0 to 100 of 500 available for paging

message

```
2015-04-20 21:01:38,783 [myid:2] - INFO  [Thread-3902:NIOServerCnxn@1001] - Closed socket connection for client /127.0.0.1:35143 (no session established for client)
2015-04-20 21:01:38,782 [myid:2] - INFO  [Thread-3902:NIOServerCnxn$StatCommand@655] - Stat command output
```

The **Fields** list:



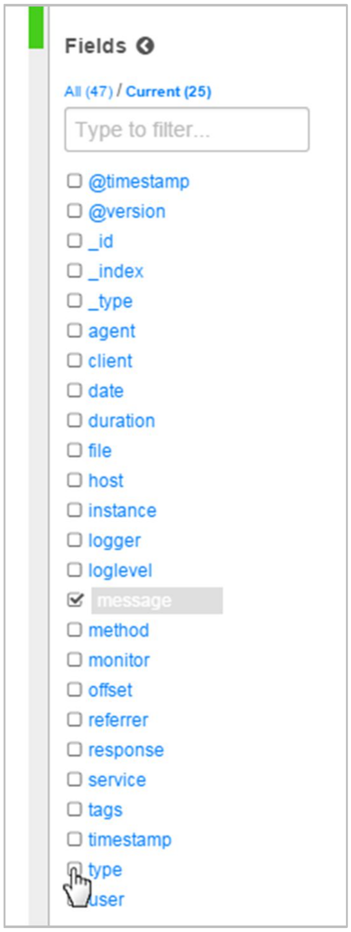
Fields

All (47) / Current (25)

Type to filter...

- ☐ @timestamp
- ☐ @version
- ☐ _id
- ☐ _index
- ☐ _type
- ☐ agent
- ☐ client
- ☐ date
- ☐ duration
- ☐ file
- ☐ host

2. Select a field to include in the display, for example *type*:



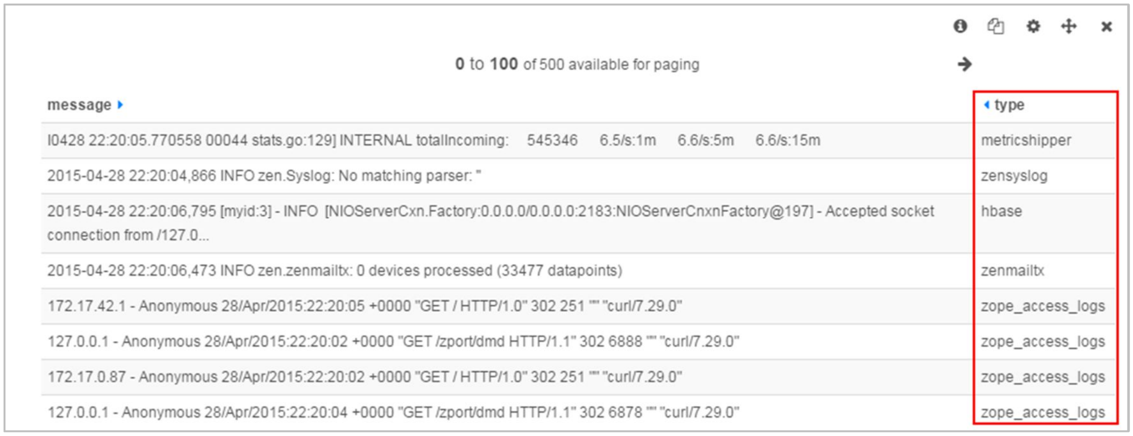
Fields

All (47) / Current (25)

Type to filter...

- □ @timestamp
- □ @version
- □ _id
- □ _index
- □ _type
- □ agent
- □ client
- □ date
- □ duration
- □ file
- □ host
- □ instance
- □ logger
- □ loglevel
- ☑ message
- □ method
- □ monitor
- □ offset
- □ referrer
- □ response
- □ service
- □ tags
- □ timestamp
- □ type
- □ user

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



0 to **100** of 500 available for paging

message ▸	◂ type
I0428 22:20:05.770558 00044 stats.go:129] INTERNAL totalIncoming: 545346 6.5/s:1m 6.6/s:5m 6.6/s:15m	metricshipper
2015-04-28 22:20:04,866 INFO zen.Syslog: No matching parser: ''	zensyslog
2015-04-28 22:20:06,795 [myid:3] - INFO [NIOServerCxn.Factory:0.0.0.0/0.0.0.0:2183:NIOServerCnxnFactory@197] - Accepted socket connection from /127.0...	hbase
2015-04-28 22:20:06,473 INFO zen.zenmailtx: 0 devices processed (33477 datapoints)	zenmailtx
172.17.42.1 - Anonymous 28/Apr/2015:22:20:05 +0000 "GET / HTTP/1.0" 302 251 "" "curl/7.29.0"	zope_access_logs
127.0.0.1 - Anonymous 28/Apr/2015:22:20:02 +0000 "GET /zport/dmd HTTP/1.1" 302 6888 "" "curl/7.29.0"	zope_access_logs
172.17.0.87 - Anonymous 28/Apr/2015:22:20:02 +0000 "GET / HTTP/1.0" 302 251 "" "curl/7.29.0"	zope_access_logs
127.0.0.1 - Anonymous 28/Apr/2015:22:20:04 +0000 "GET /zport/dmd HTTP/1.1" 302 6878 "" "curl/7.29.0"	zope_access_logs

Kibana Search Examples

To effectively use the Kibana search engine, it is important to use appropriate search strings that return the information of interest. 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.