

The Zenoss Enablement Series:

How to Search and Display Logs with Kibana

Document Version 500 - p1

Zenoss, Inc.

www.zenoss.com

Copyright © 2016 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

| Kibana and Control Center 1 Accessing Kibana 1 Log File Entries 2 Action Icons 3 Searching Logs with Kibana 4 Kibana Search Syntax 4 |
|--|
| Accessing Kibana |
| Log File Entries |
| Action Icons |
| Searching Logs with Kibana |
| |
| Kibana Time Range Search Filter4 |
| Performing a Kibana Log Search |
| Customizing the Search Results Fields |
| Kibana Search Examples |

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 (<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 | 9 | Logout | About |
|---------------------|--------------|----------------|-------|------|------------------|--------------|---|--------|-------|
| Logs | | | | | | | | | |

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.

| | a month ago to a few seconds ago 👻 | S | * | Þ | Ð | C | ٥ | | | | |
|---|--|-------------|----------------|---|----------|---|-----|--|--|--|--|
| | | | | | | | | | | | |
| ALL EVENTS | | | | C | 1 | ¢ | + × | | | | |
| 0 | 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 | establishe | ed 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 [NIOSer | verCxn.Factory:0.0.0.0/0.0.0.0:2182:NIOServerCnxn@821] - Processing stat command from /127. | 0.0.1:351 | 43 | | | | | | | | |
| 2015-04-20 21:01:38,781 [myid:2] - INFO [NIOSer | 5-04-20 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 +00 | 00 "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 d | evices 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 | establishe | ed for client) | | | | | | | | |
| 2015-04-20 21:01:38,800 [myid:3] - INFO [NIOSer | verCxn.Factory:0.0.0.0/0.0.0.0:2183:NIOServerCnxn@821] - Processing stat command from /127. | 0.0.1:411: | 36 | | | | | | | | |
| 2015-04-20 21:01:33,793 [myid:3] - INFO [NIOSer | verCxn.Factory:0.0.0.0/0.0.0.0:2183:NIOServerCnxn@821] - Processing stat command from /127. | 0.0.1:4080 | 06 | | | | | | | | |
| 2015-04-20 21:01:38,799 [myid:3] - INFO [NIOSer | verCxn.Factory:0.0.0.0/0.0.0.0:2183:NIOServerCnxnFactory@197] - Accepted socket connection 1 | irom /127./ | 0.0.1:41136 | | | | | | | | |
| 2015-04-20 21:01:37,066 INFO [New I/O server be | oss #17] ConnectionManager: [id: 0x368a28f5, /0:0:0:0:0:0:0:0:1:51552 => /0:0:0:0:0:0:0:0:1:4242] OF | 'EN | | | | | | | | | |
| | | | | | | | | | | | |

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:

| Center | Applications Res | ource Pools H | osts Logs | Backup / Restore | | Zenoss ! | ×0 🔮 | Logout | A |
|--------------------------|--------------------------|---|--------------------------------------|--|-----------------------|-------------------|----------------|-----------|---|
| .ogs | | | | | | | | | |
| | | | | | | | | | |
| Logs | | | | a month ago to a few secon | ds ago 👻 😂 | A | L B | C | • |
| | | | | | | | | | |
| PILTERING 4 | | | | | | | | | |
| ALL EVENTS | | | | | | | 0 | ආ \$ | ÷ |
| 0 | | | 0 te | 0 100 of 500 available for paging | | | > | | |
| message | | | | | | | | | |
| 2015-04-20 21:03:33,967 | [myid:2] - INFO [Thread- | 3925:NIOServerCnxr | n@1001] - Close | d socket connection for client /127.0.0.1:4148 | 7 (no session establi | shed for client) | | | |
| View: Table / JSON / Raw | | | | | | | | | |
| Field | Action | Value | | | | | | | |
| @timestamp | 0 ⊘ Ⅲ | 2015-04-20T21:03 | 3:37.657Z | | | | | | |
| @version | 0 ⊘ Ⅲ | 1 | | | | | | | |
| _id | 0 ⊘ Ⅲ | UAU6VMTySA-xat | NePj3TXGQ | | | | | | |
| _index | 0 ⊘ Ⅲ | logstash-2015.04.2 | 20 | | | | | | |
| _type | 0 ⊘ Ⅲ | hbase | | | | | | | |
| file | 0 ⊘ Ⅲ | /var/log/zookeeper | r/zookeeper.log | | | | | | |
| host | Q Ø Ⅲ | zk2 | | | | | | | |
| instance | Q Ø Ⅲ | 1 | | | | | | | |
| message | Q Ø III | 2015-04-20 21:03: session establishe | :33,967 [myid:2] - ed for client) | INFO [Thread-3925:NIOServerCnxn@1001] | - Closed socket con | nection for clier | nt /127.0.0.1: | 41487 (no | |
| | | | | | | | | | |
| offset | 0 ⊘ Ⅲ | 2304685 | | | | | | | |

Action Icons

The field details include three action icons:

| 2015-06-02 00:30:19,513 [myid:3] - INFO [NIOServerCxn.Factory:0.0.0.0/0.0.0.2183:NIOServerCnxnFactory@1 | | | | | | | | | | | |
|---|--------------------------|--------------------------|--|--|--|--|--|--|--|--|--|
| View: Table / JSON / Raw | View: Table / JSON / Raw | | | | | | | | | | |
| Field | Action | Value | | | | | | | | | |
| @timestamp | Q Ø Ⅲ | 2015-06-02T00:30:27.178Z | | | | | | | | | |
| @version | Q Ø Ⅲ | 1 | | | | | | | | | |
| _id | Q Ø Ⅲ | IX3dRbDdQ92sNs8caJ30-Q | | | | | | | | | |

The icons specify particular actions:

- **Q** 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:

| Control Center | Applications | Resource Pools | Hosts | Logs | Backup / Restore | | L zenoss | ₩0 | 9 | Logout | About |
|--------------------|--------------|----------------|-------|------|--|---|----------|----|---|--------|------------|
| Logs | | | | | | | | | | | |
| International Logs | | | | | a month ago to a few seconds ago $ullet$ | C | ñ | | 1 | Ľ | ۰ |
| QUERY > | | | | | | | | | | | |
| | | | | | | | | | | | Q + |

The drop down menu displays additional time range selections.

| | a month ago to a | fews | seconds ago 👻 |
|-----|------------------|------|---------------------|
| | Last 5m | | |
| | Las 5m | | |
| ١. | Last 1h | | |
| | Last 6h | | |
| | Last 12h | | |
| | Last 24h | | |
| 15 | Last 2d | | |
| | Last 7d | | |
| - 5 | Last 30d | | |
| et | Auto-Refresh | Þ | 1:37511 (no sessio) |
| rC | Custom | | ommand from /127. |
| | | | |

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:

| In Logs | a month ago to a few seconds ago 👻 | 2 | ñ | L. | 6 | C | ٥ |
|------------|--------------------------------------|---|---|----|----------|---|-----|
| | | | | | | | |
| ALL EVENTS | | | | | 0 4 | ٥ | + × |
| 0 | 0 to 100 of 500 available for paging | | | ÷ | → | | |
| message | | | | | | | |

The query search field displays:

| Control Center | Applications | Resource Pools | Hosts | Logs | Backup / Restore | | <u>↓</u> zenoss | ⊠0 | 9 | Logout | About |
|-------------------|--------------|----------------|-------|------|---|---|-----------------|----|---|--------|-------|
| Logs | | | | | | | | | | | |
| | | | | | a month ago to a few seconds ago \checkmark | 3 | * | ł | 1 | Ŀ | • |
| • | | | | | | | | | | | Q + |
| | | | | | | | | | | | |

- 2. Enter the search string
- 3. Click **Enter** (or the magnifying glass icon **Q**) 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:

Search & Display Logs with Kabana

Q

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



The Fields list:

| | Fields O |
|-----|-------------------------|
| | 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 |
| |
| □ tags |
| timestamp |
| ft type |
| Luser |

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 | 0 0 → | ත | ¢ | ÷ | × |
|---|----------|--------|--------|-------|----|
| message 🕨 | | type | | | ٦ |
| I0428 22:20:05.770558 00044 stats.go:129] INTERNAL totalIncoming: 545346 6.5/s:1m 6.6/s:5m 6.6/s:15m | п | netric | shippe | er | |
| 2015-04-28 22:20:04,866 INFO zen.Syslog: No matching parser: " | z | ensys | slog | | |
| 2015-04-28 22:20:06,795 [myid:3] - INFO [NIOServerCxn.Factory:0.0.0.0/0.0.0.2183:NIOServerCnxnFactory@197] - Accepted socket connection from /127.0 | h | base | | | |
| 2015-04-28 22:20:06,473 INFO zen.zenmailtx: 0 devices processed (33477 datapoints) | z | enma | iltx | | |
| 172.17.42.1 - Anonymous 28/Apr/2015:22:20:05 +0000 "GET / HTTP/1.0" 302 251 "" "curl/7.29.0" | z | ope_ | acces | s_log | gs |
| 127.0.0.1 - Anonymous 28/Apr/2015:22:20:02 +0000 "GET /zport/dmd HTTP/1.1" 302 6888 *** "curl/7.29.0" | z | ope_ | acces | s_log | gs |
| 172.17.0.87 - Anonymous 28/Apr/2015:22:20:02 +0000 "GET / HTTP/1.0" 302 251 "" "curl/7.29.0" | z | ope_ | acces | s_log | gs |
| 127.0.0.1 - Anonymous 28/Apr/2015:22:20:04 +0000 "GET /zport/dmd HTTP/1.1" 302 6878 "" "curl/7.29.0" | z | ope_ | acces | s_log | gs |

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 <i>zenperfsnmp</i> , only some services specify a log level. The query will work even in the absence of a log level. |