Using Kibana4 to read logs at Wikimedia

Wikimedia Tech Talk, 2016-11-14
Elasticsearch
Document oriented full text search engine built on top of Apache Lucene.

Logstash
Pipeline processing system that connects "inputs" to "outputs" with optional "filters" in between.

Kibana
Browser based analytics and search dashboard for Elasticsearch.

Elasticsearch, Logstash, and Kibana are trademarks of Elasticsearch BV, registered in the U.S. and in other countries.
Kibana at Wikimedia

- WMF Beta cluster: https://logstash-beta.wmflabs.org/
- WMF production: https://logstash.wikimedia.org/
  - Requires a signed NDA because of access to potentially sensitive data.
Kibana4 Dashboards
Kibana4 Dashboards

Dashboard name

Events Over Time

Event Types
Kibana4 Dashboards

Elasticsearch "query string query"

Search terms are OR'ed by default. Use "AND" to combine terms.
Kibana4 Dashboards

Search / refresh
Kibana4 Dashboards

New dashboard
Kibana4 Dashboards

Make sure to change the name if you are making a new dashboard.

Dashboards are NOT versioned so if you save over an existing dashboard the old version is lost.
Kibana4 Dashboards

Load dashboard
Kibana4 Dashboards

Share current view
Kibana4 Dashboards

Embed this dashboard Add to your html source. Note all clients must still be able to access kibana

```html
<iframe src="https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?_g=(refreshInterval:(display:Off,pause:If,value:0),time:(from:\n
Share a link

https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?_g=(refreshInterval:(display:Off,pause:If,value:0),time:(from:now-1h,mode:quick,to:now)

Generate short URL

Dashboards

SAL · fatalmonitor · scap · mediawiki-errors · memcached · resourceloader · hhvm · apache · parsoid · hadoop · restbase · restbase-test · cassandra (restbase) · syslog · wflLogDBError · mysql · puppet · change-prop · cassandra (aqs) · cassandra (maps)

Events Over Time

4,000
Kibana4 Dashboards

Short enough to share on IRC!
Kibana4 Dashboards

Add visualization
Kibana4 Dashboards

Options
Kibana4 Dashboards

Click and drag in any histogram to zoom into that time range.
Kibana4 Discover
Kibana4 Discover

Live Demo
X-Wikimedia-Debug header

- Handle request on a specific backend server
- Never return results from Varnish cache
- Enable verbose logging
- Record code profiling data for performance analysis
- Enable read-only mode to simulate a locked database

Read more at https://wikitech.wikimedia.org/wiki/X-Wikimedia-Debug
Using X-Wikimedia-Debug

$ curl -H 'X-Wikimedia-Debug: backend=mw1099.eqiad.wmnet; log'
https://meta.wikimedia.org/wiki/Main_Page

Firefox and Chrome browser extensions are available to make using X-Wikimedia-Debug easy.
**MediaWiki Events List**

<table>
<thead>
<tr>
<th>Time</th>
<th>Level</th>
<th>Channel</th>
<th>Host</th>
<th>Wiki</th>
<th>Message</th>
</tr>
</thead>
</table>
Credits

- Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries.
- Kibana is a trademark of Elasticsearch BV, registered in the U.S. and in other countries.
- Logstash is a trademark of Elasticsearch BV, registered in the U.S. and in other countries.
- Elasticsearch, Kibana, and Logstash logos retrieved 13 November 2016 from https://www.elastic.co/products and used for purposes of identification.