Using Kibana4 to read logs at Wikimedia

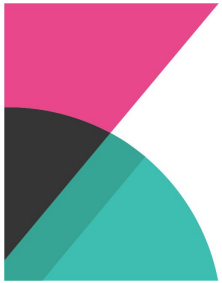
Wikimedia Tech Talk, 2016-11-14

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.



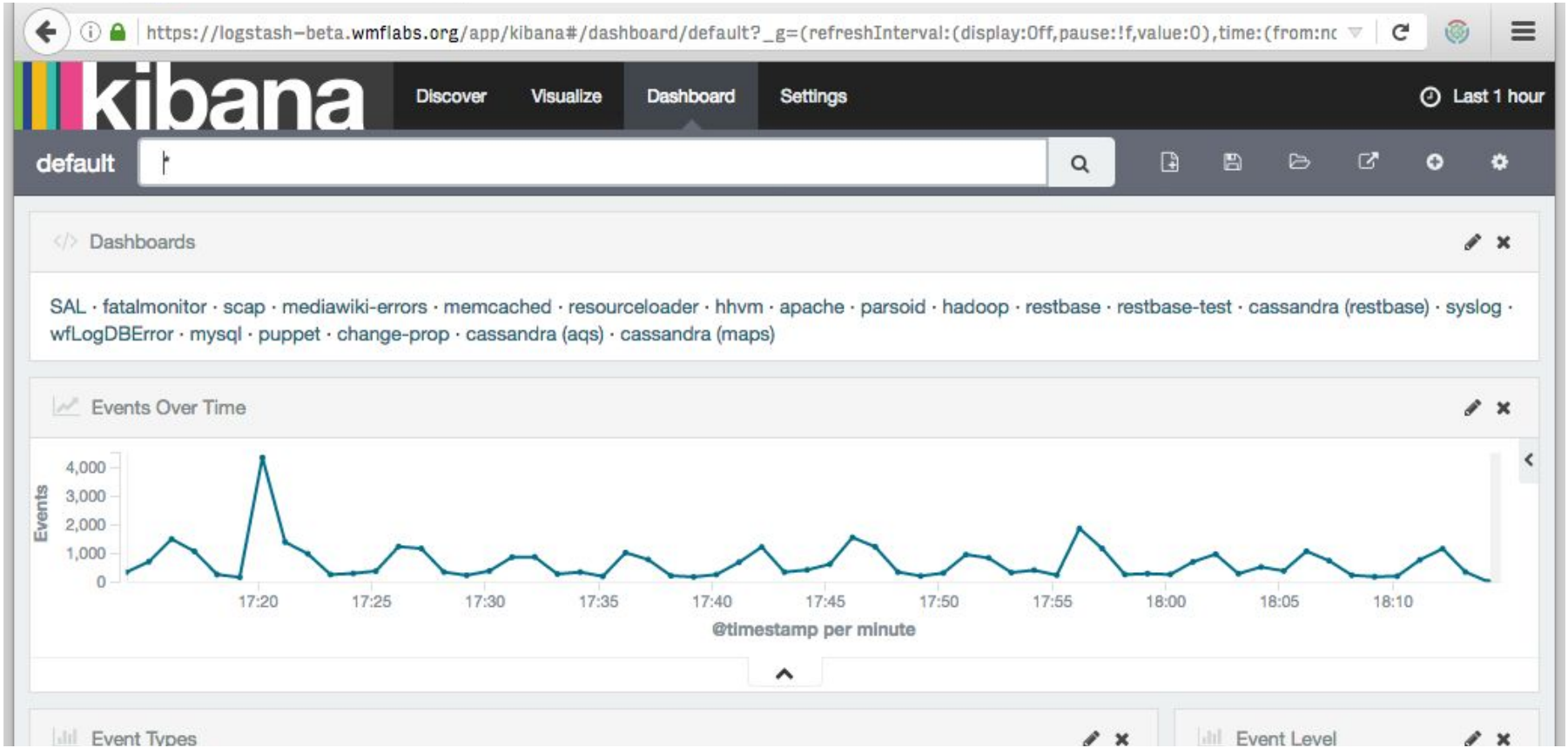
Kibana

Browser based analytics and search dashboard for Elasticsearch.

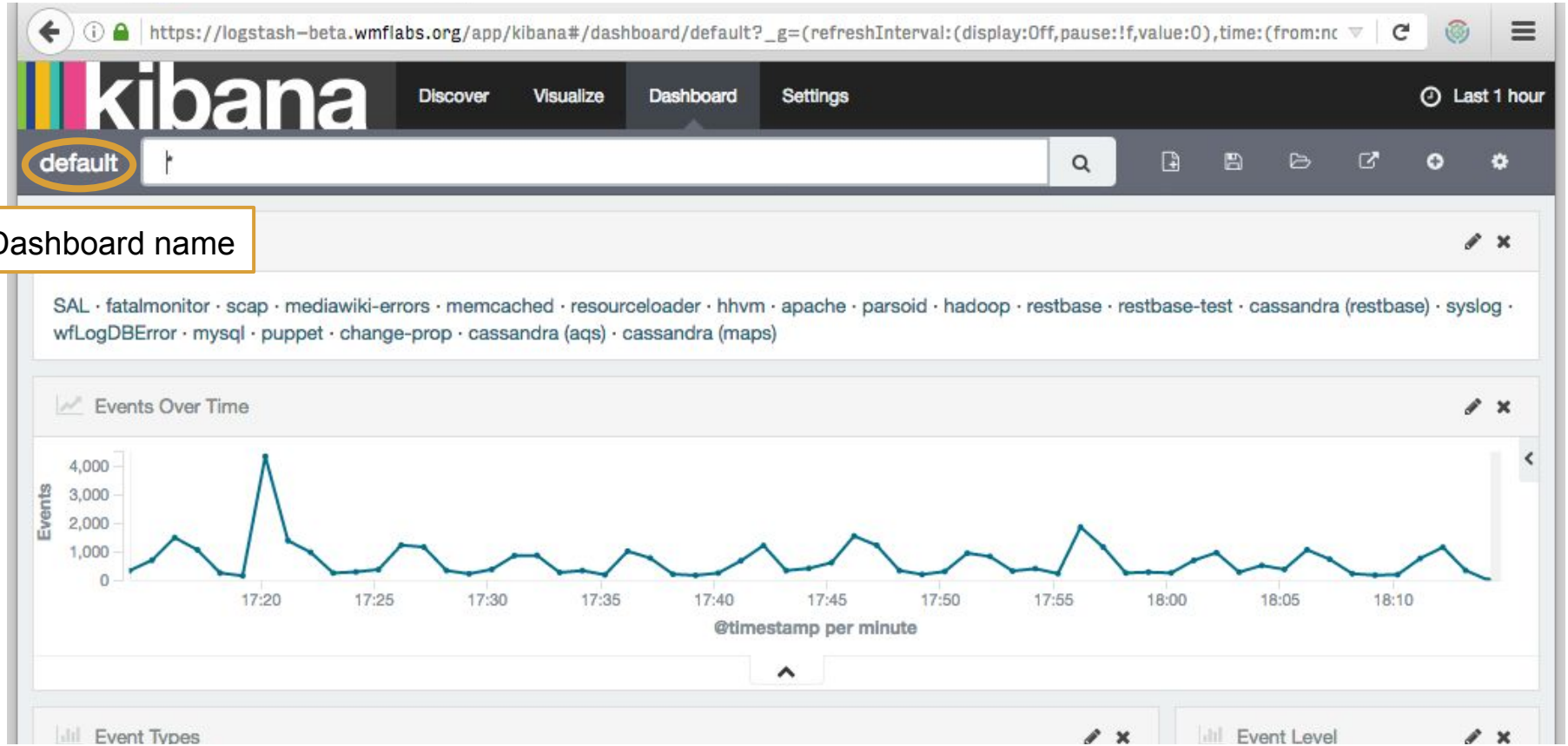
Kibana at Wikimedia

- 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.

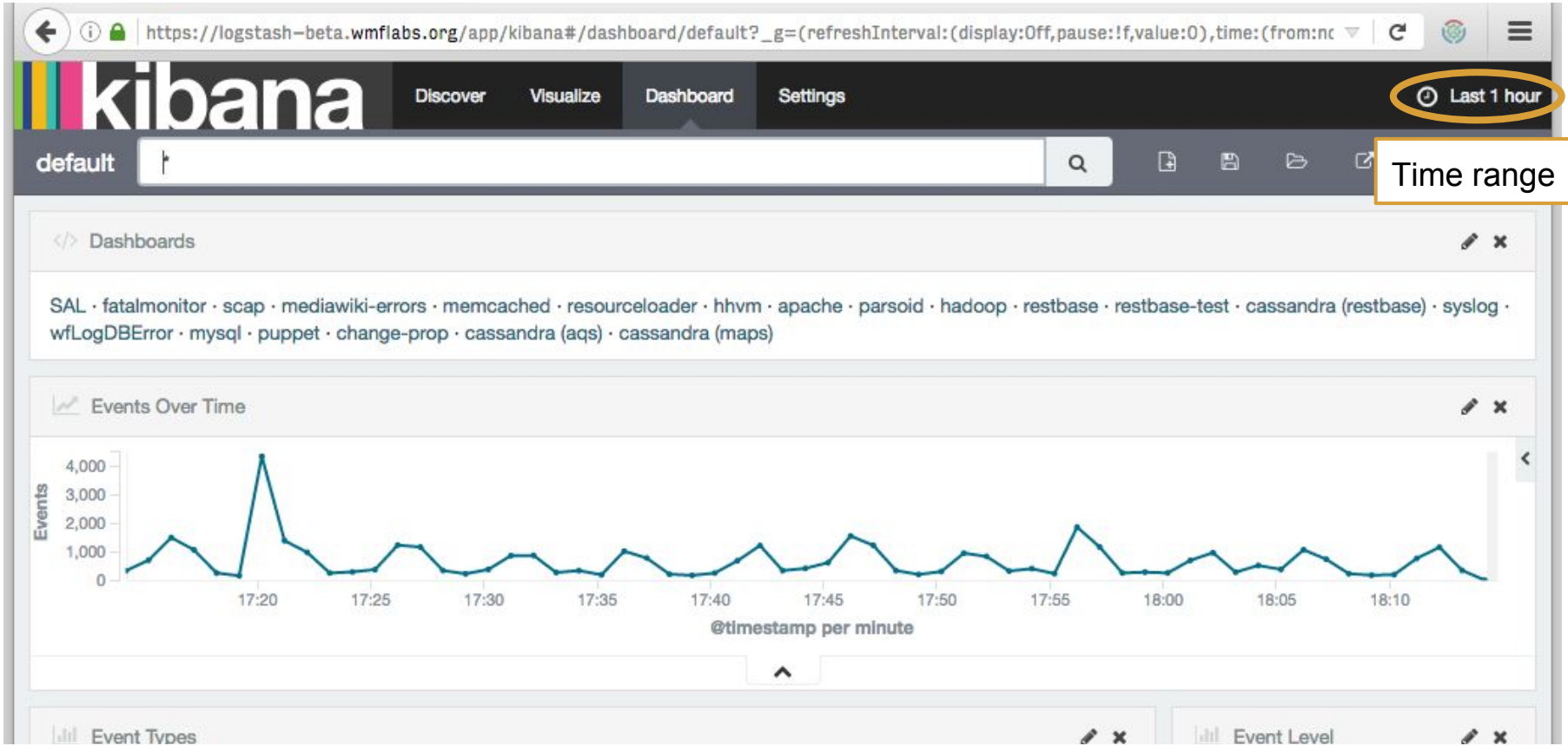
Kibana4 Dashboards



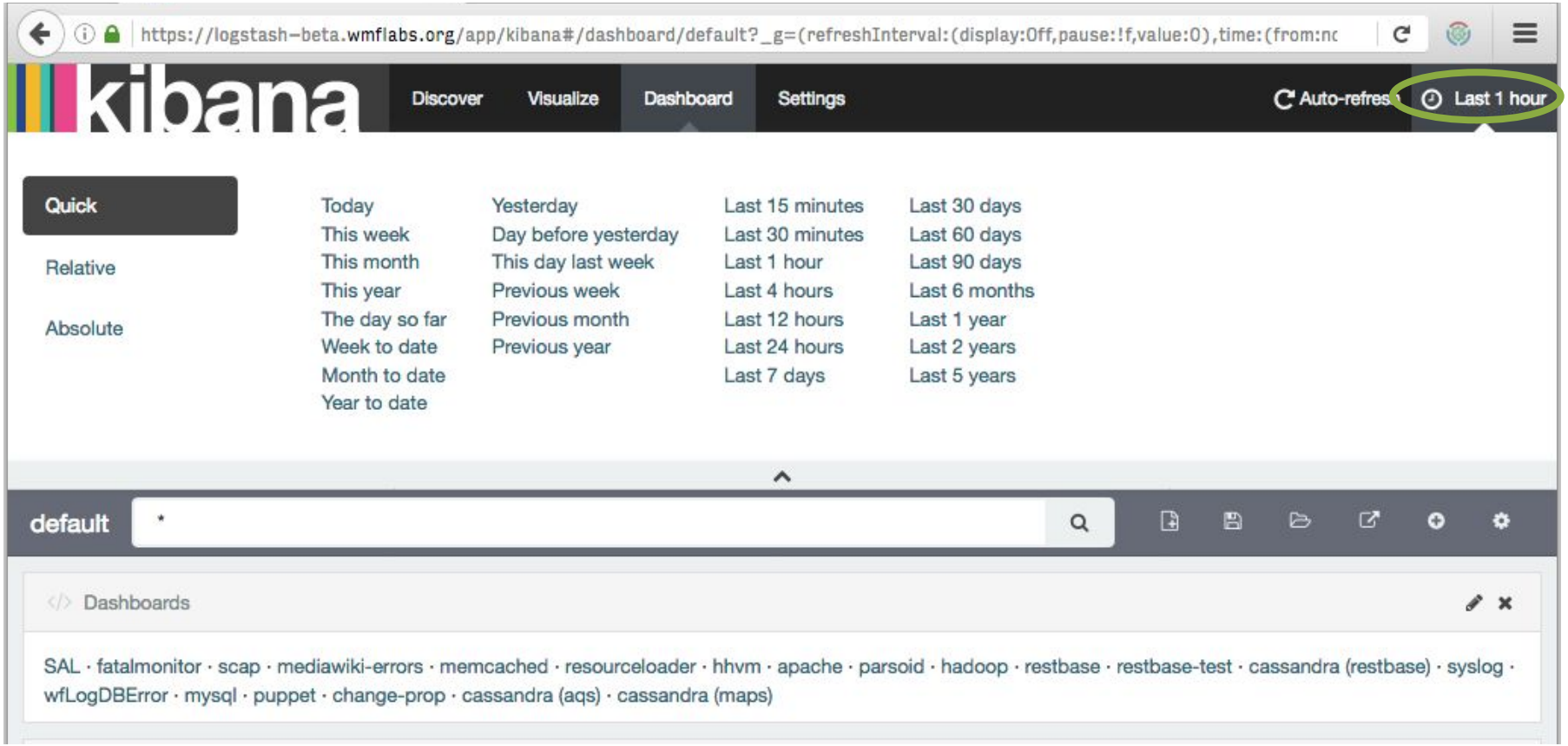
Kibana4 Dashboards



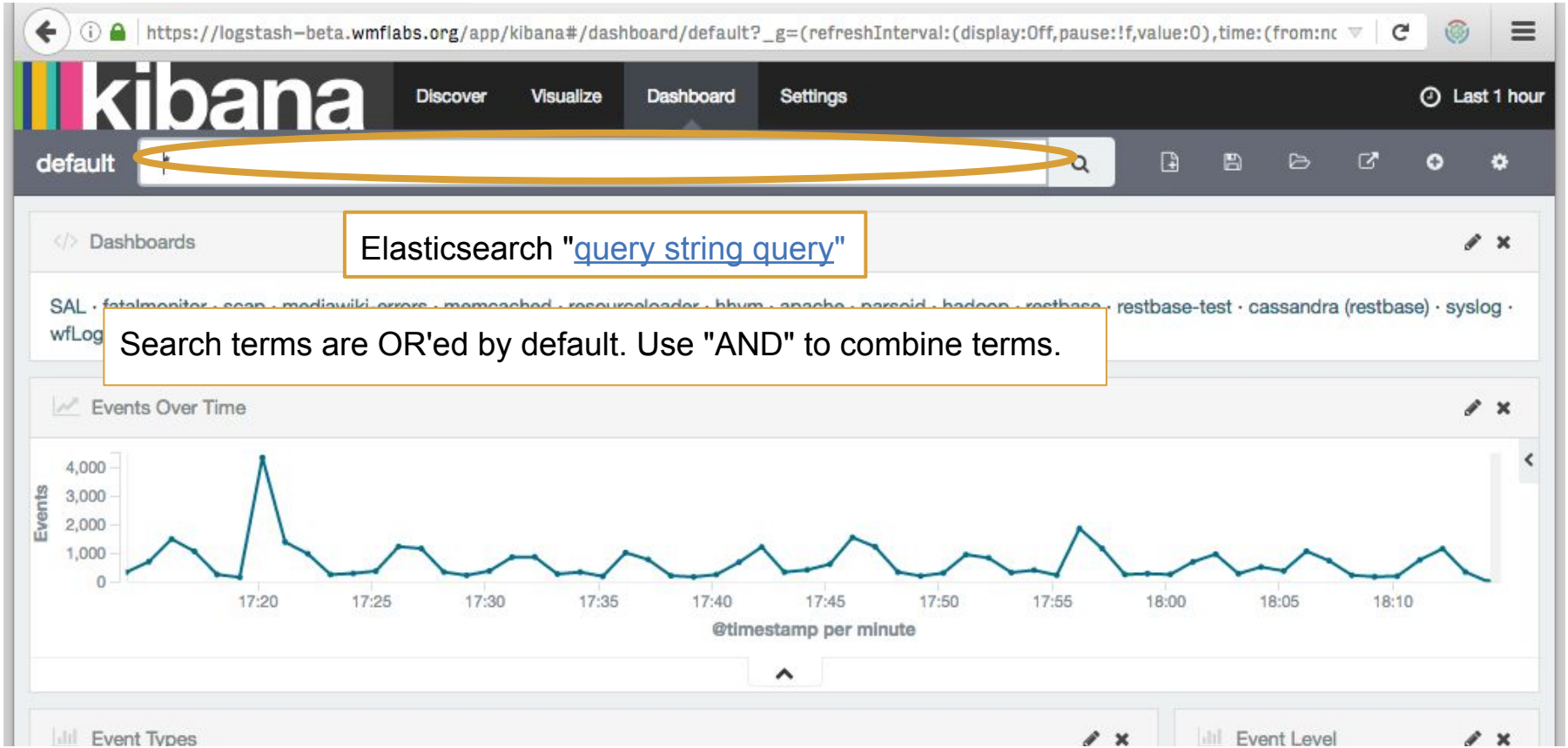
Kibana4 Dashboards



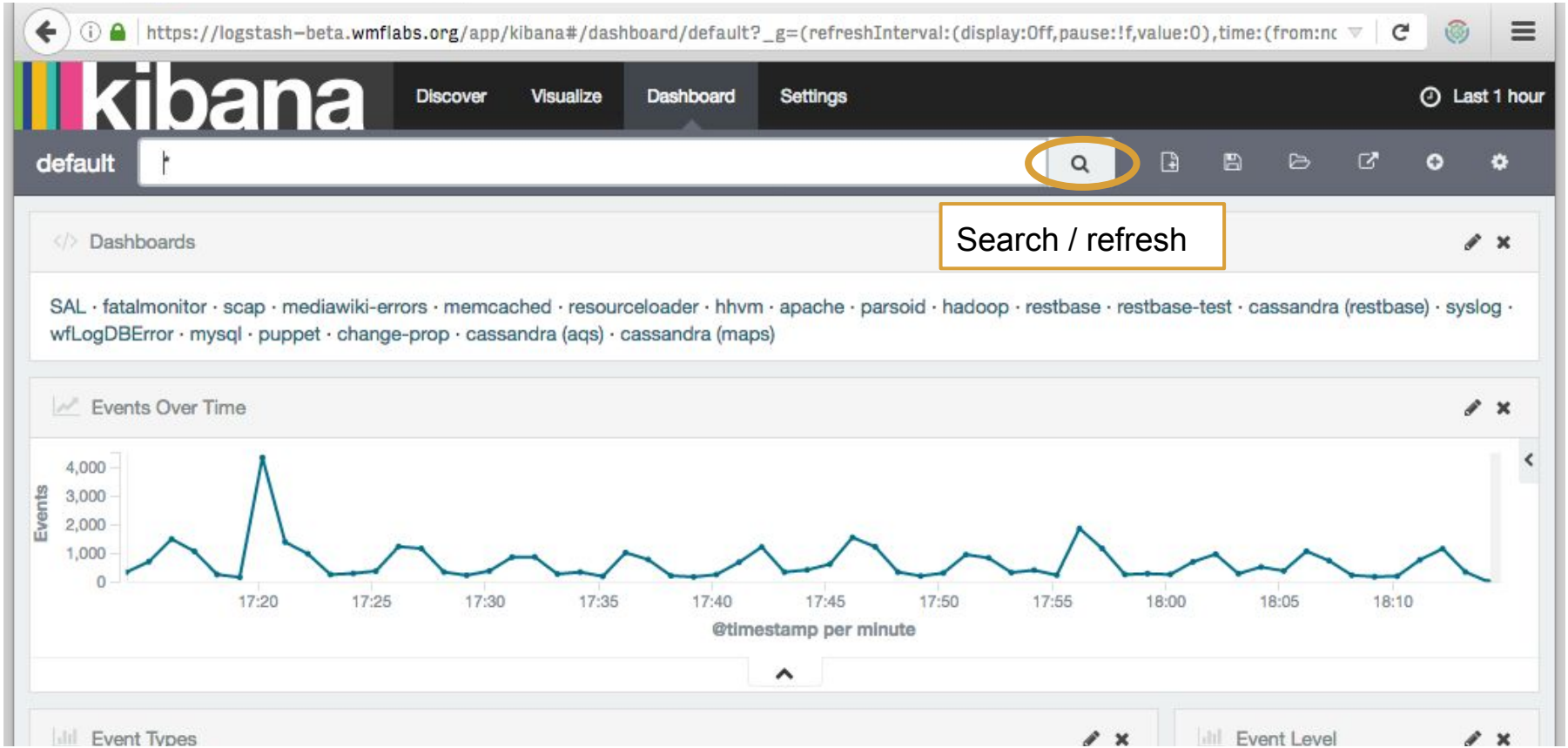
Kibana4 Dashboards



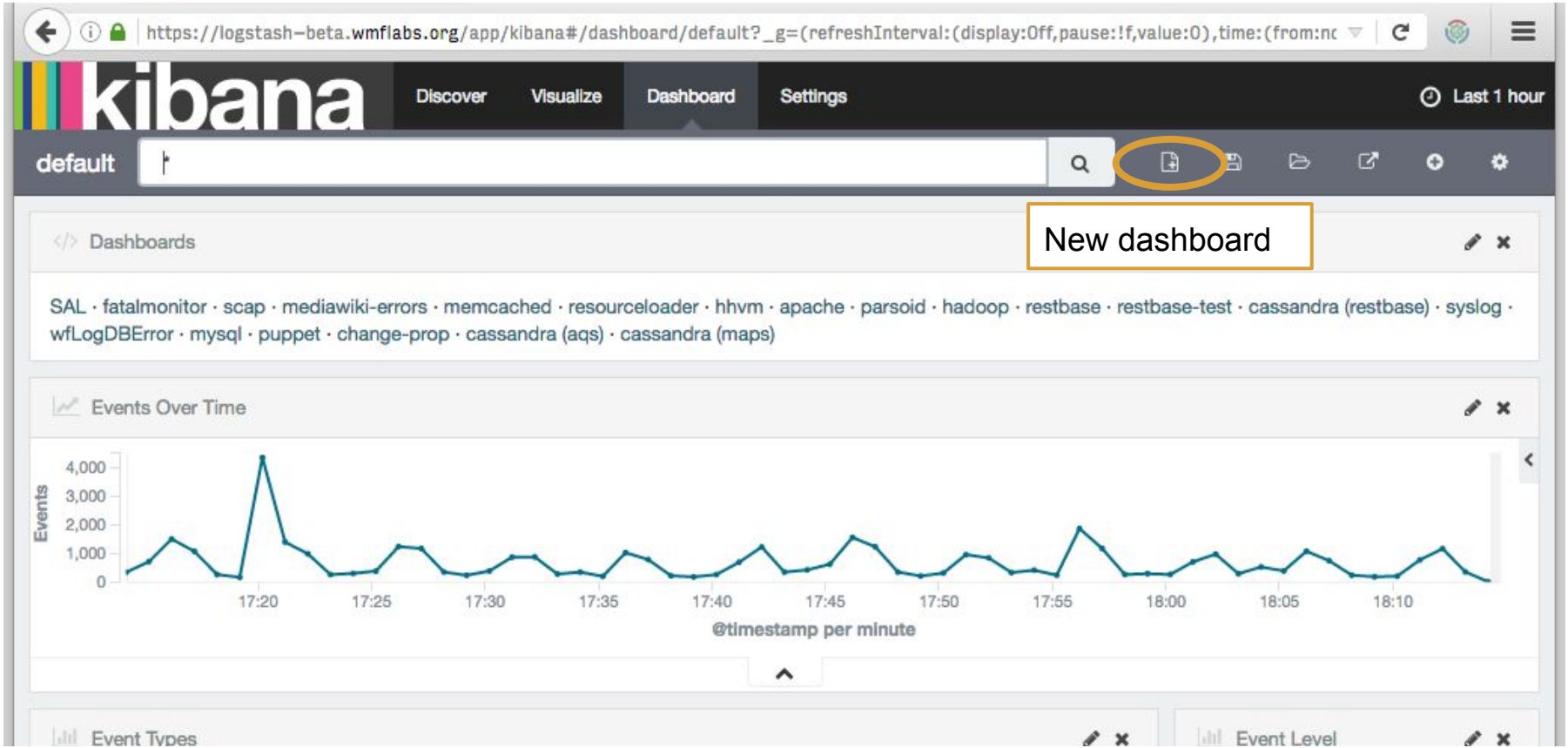
Kibana4 Dashboards



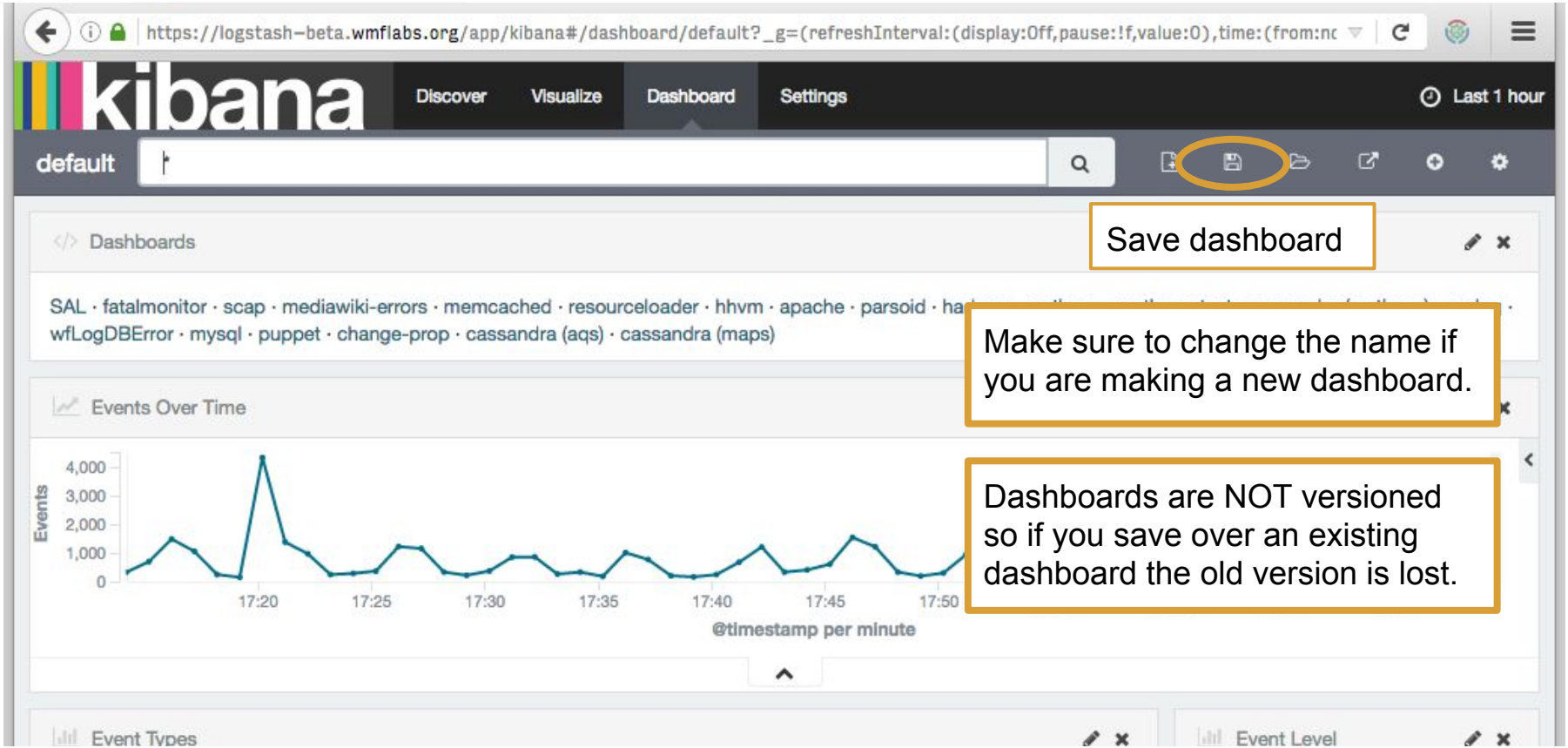
Kibana4 Dashboards



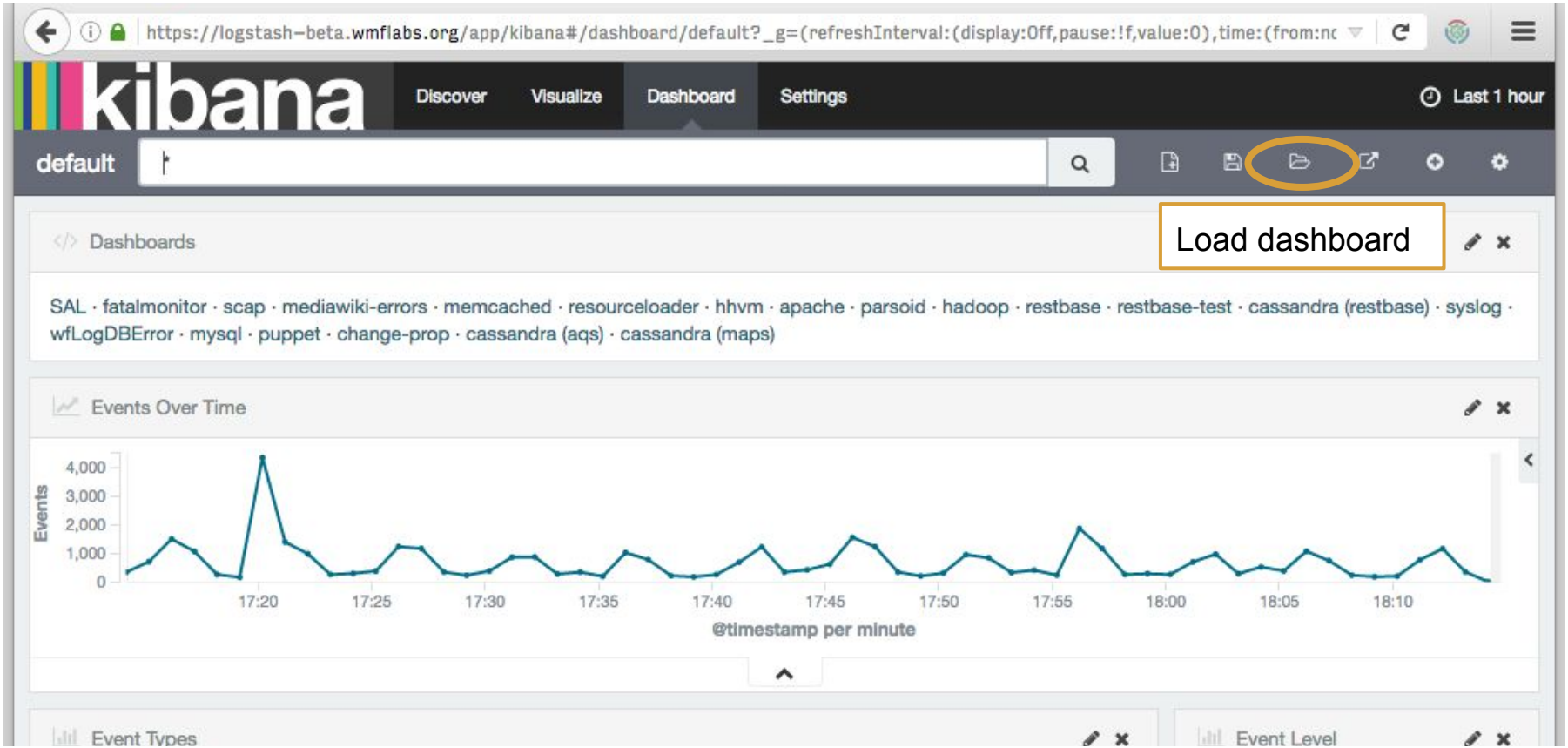
Kibana4 Dashboards



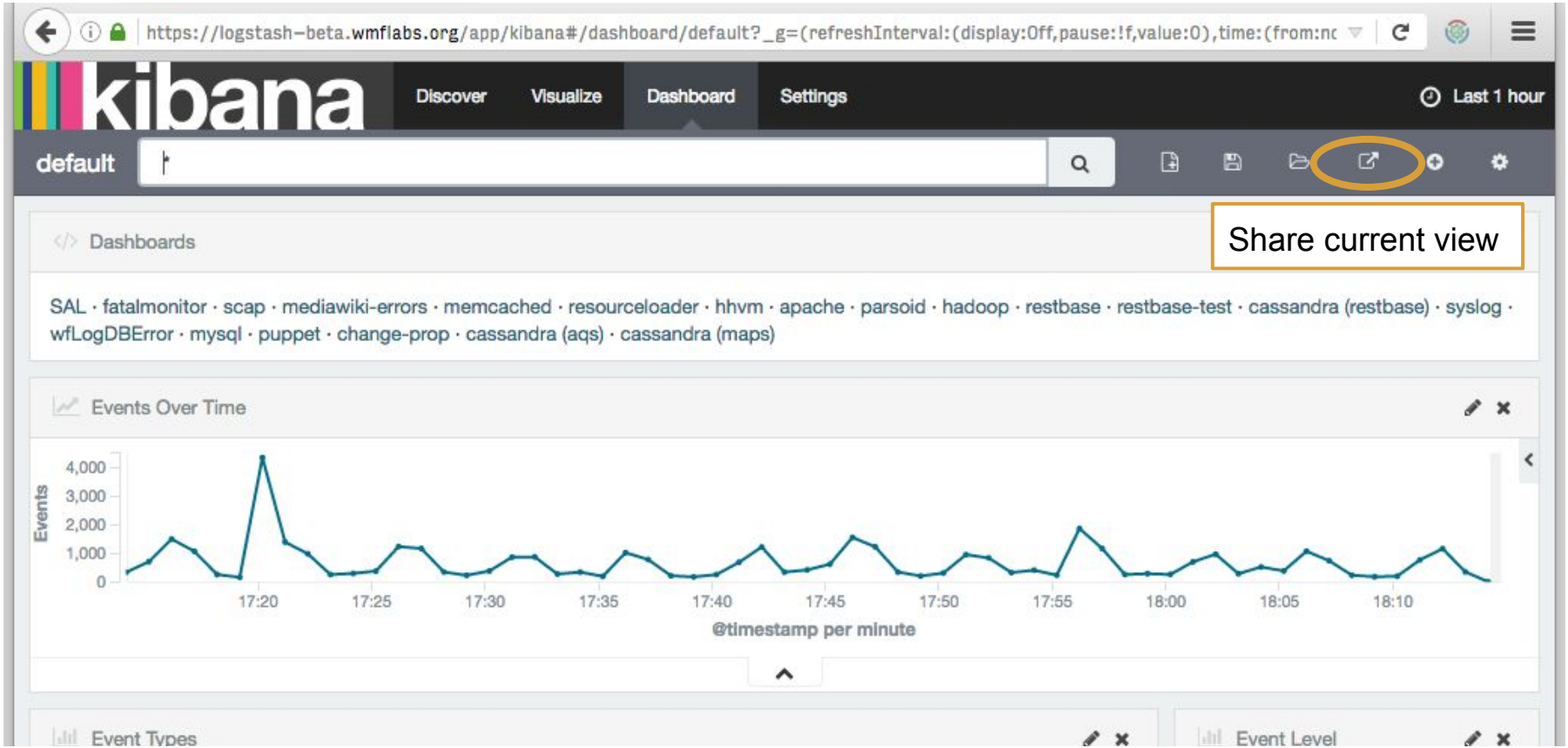
Kibana4 Dashboards



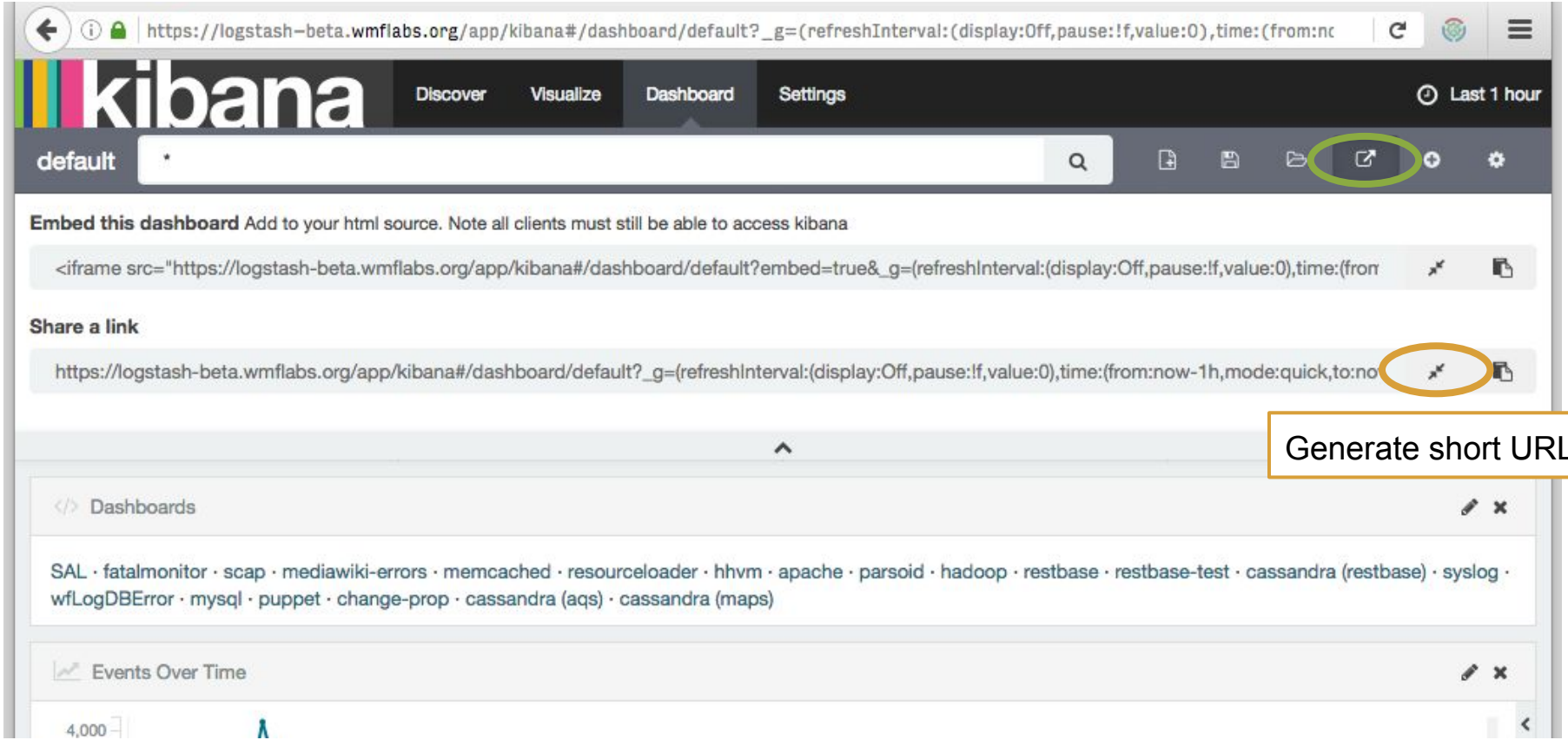
Kibana4 Dashboards



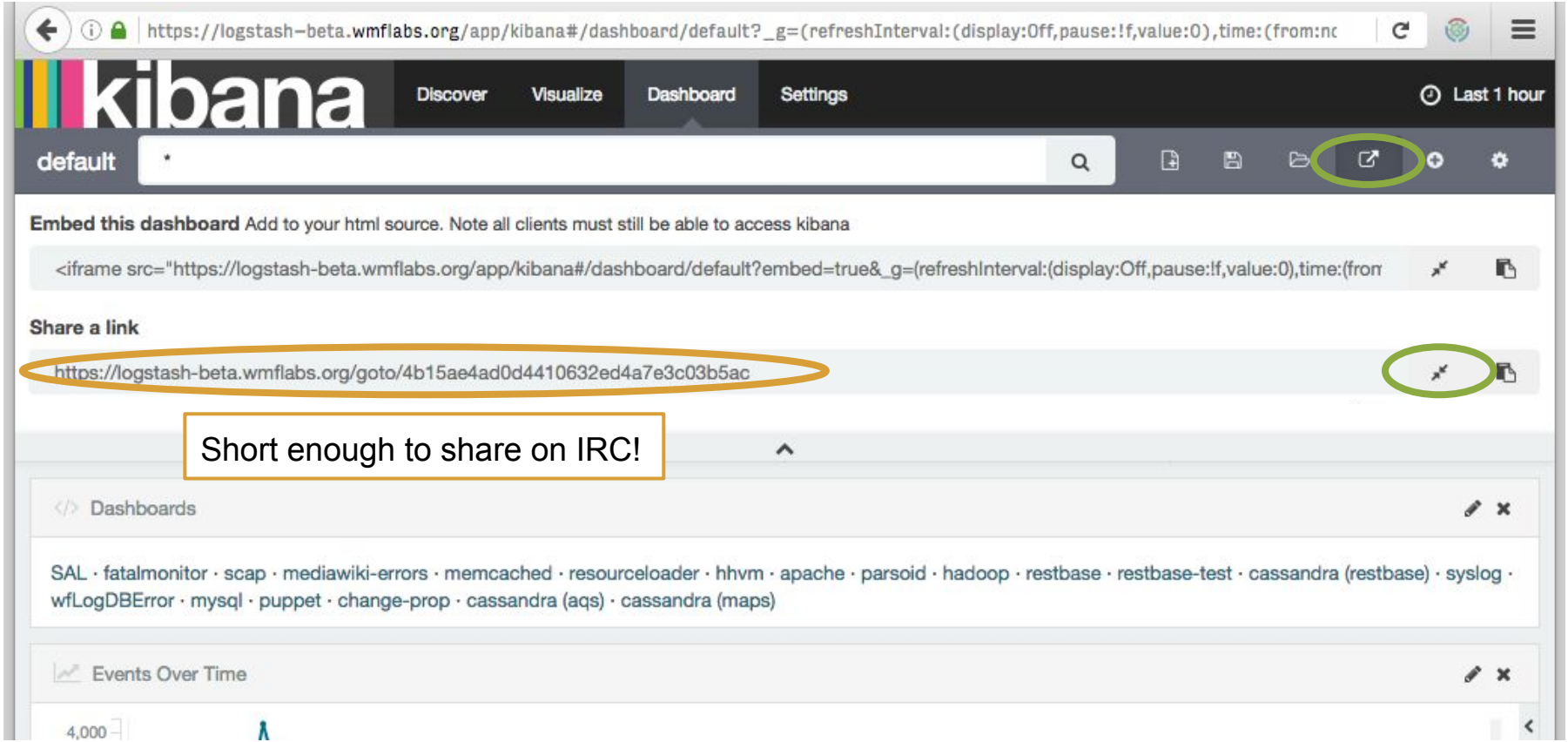
Kibana4 Dashboards



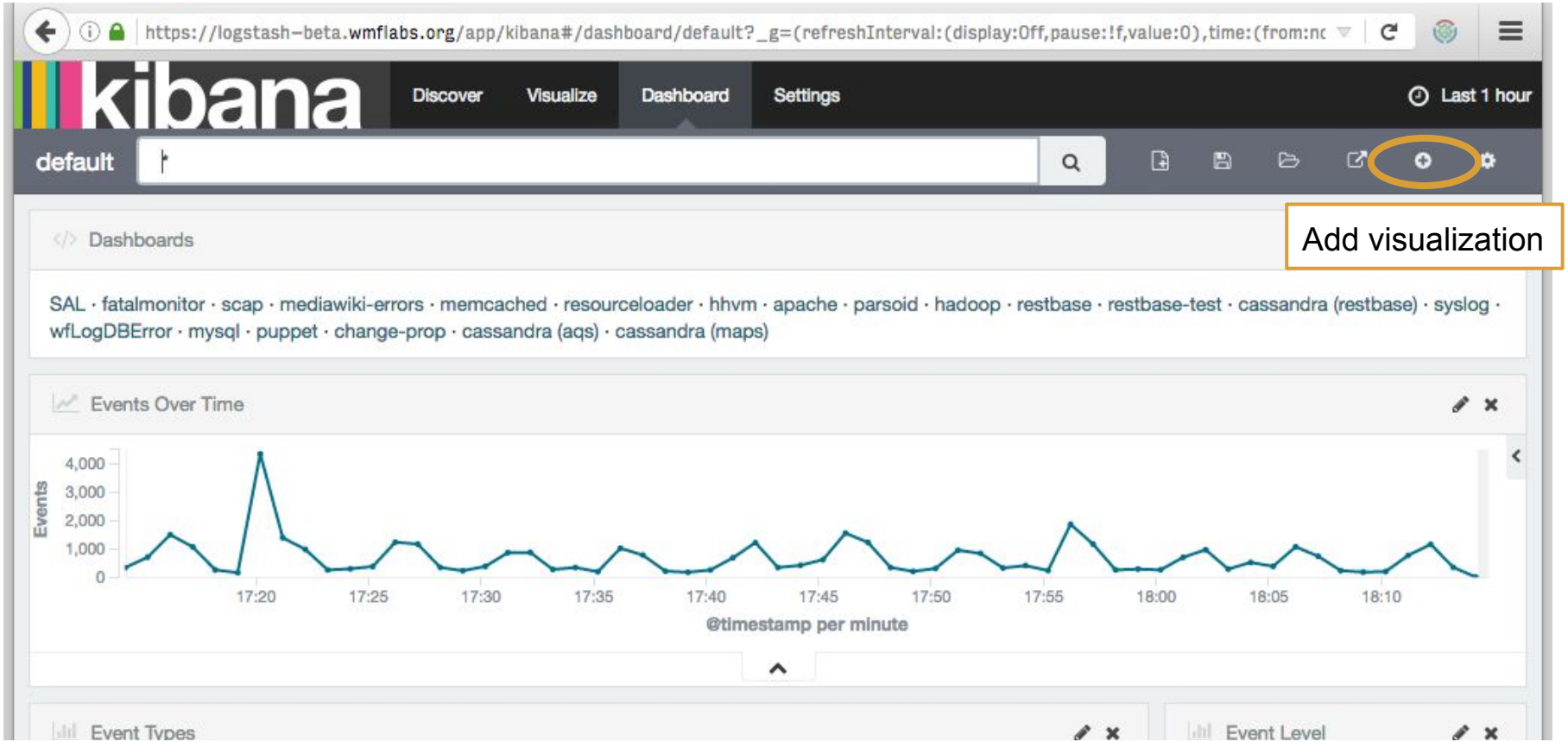
Kibana4 Dashboards



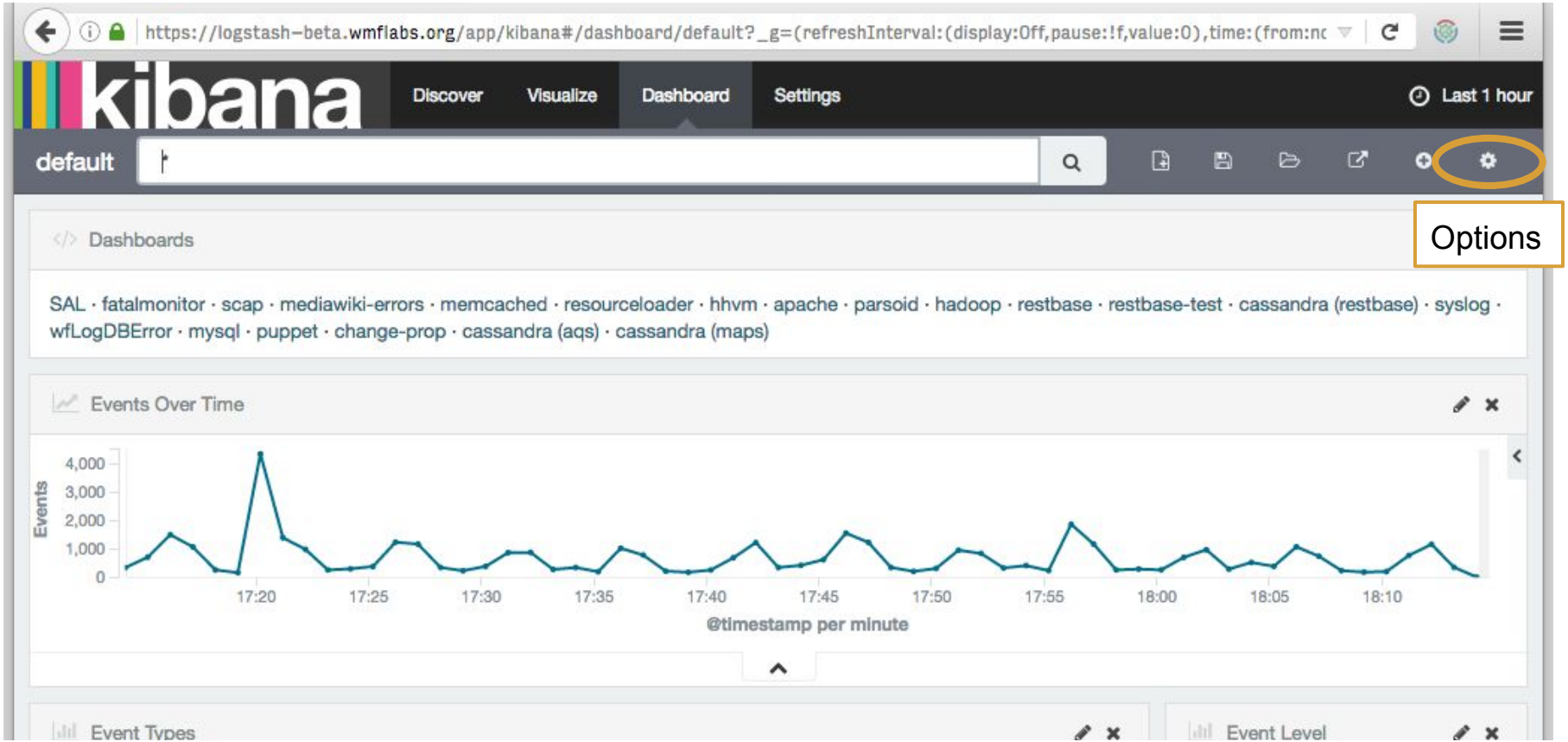
Kibana4 Dashboards



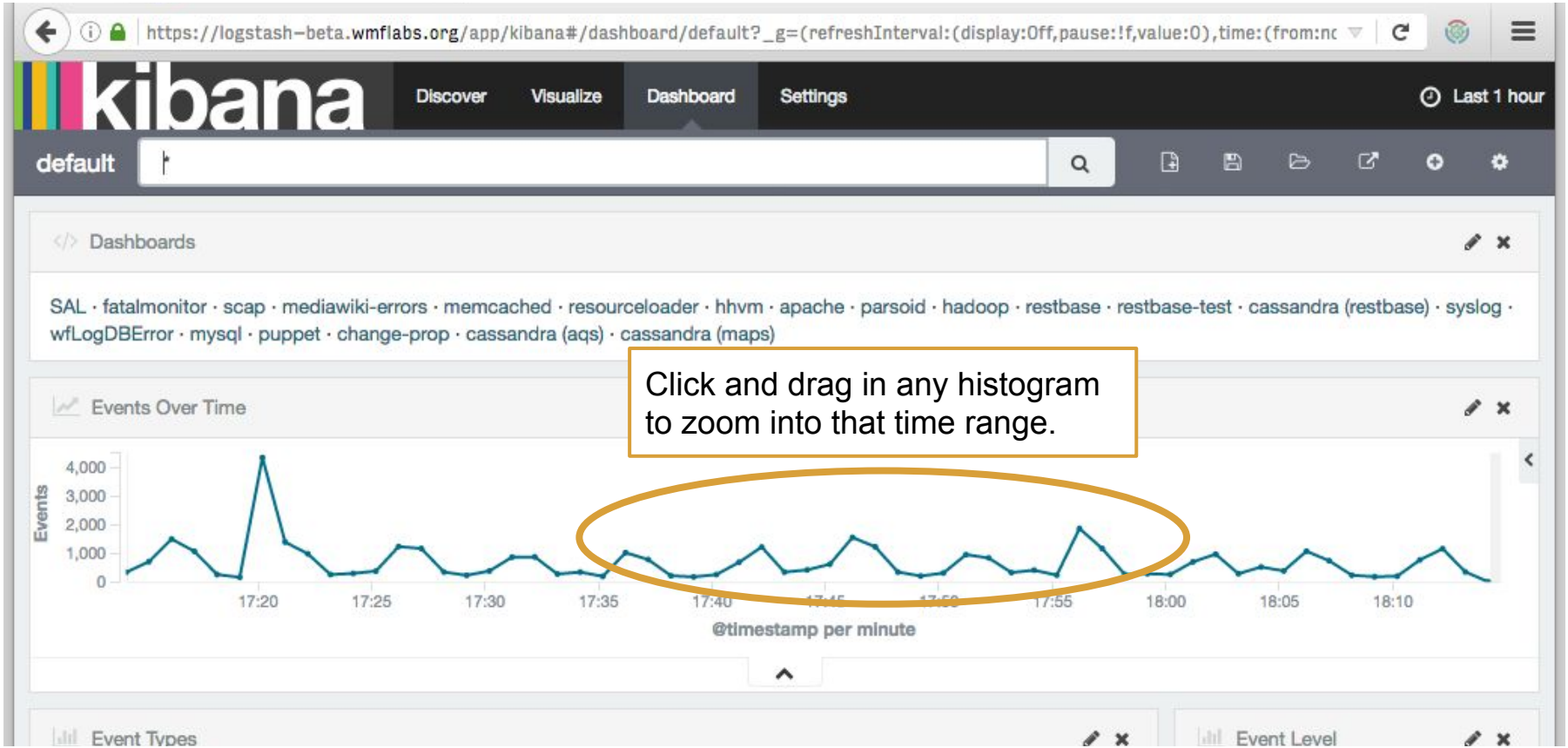
Kibana4 Dashboards



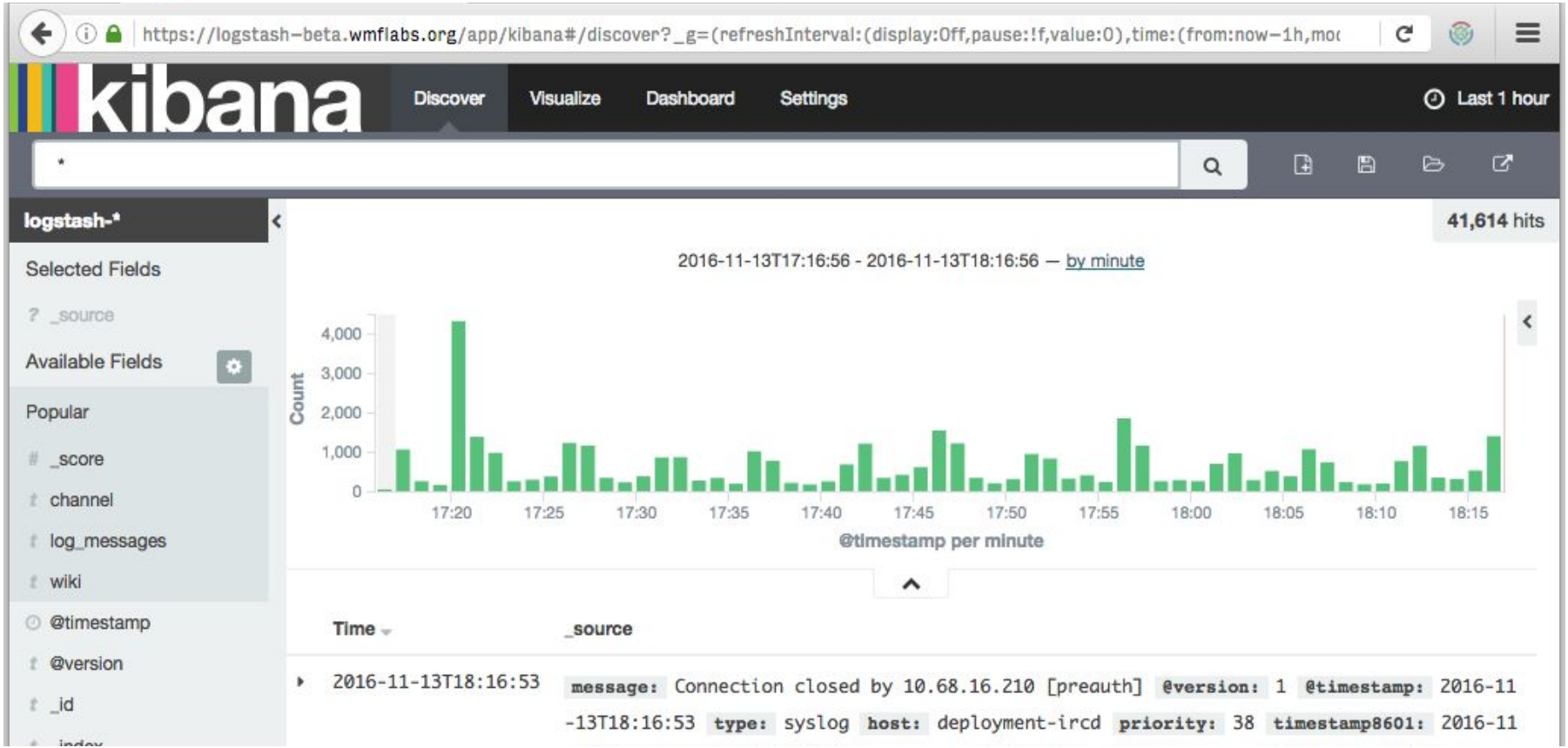
Kibana4 Dashboards



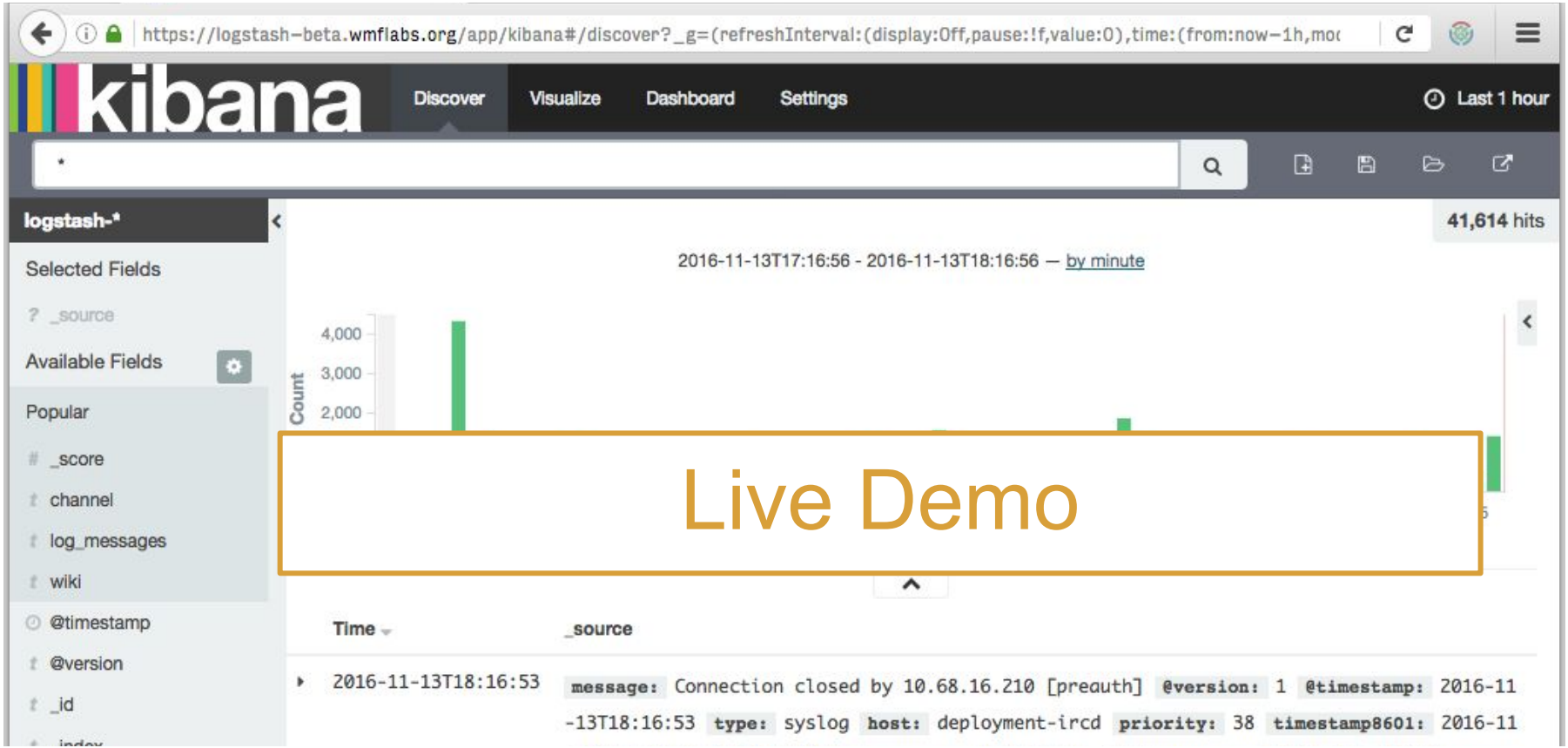
Kibana4 Dashboards



Kibana4 Discover



Kibana4 Discover



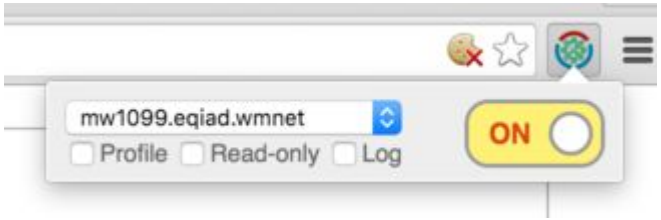
X-Wikimedia-Debug header

- 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

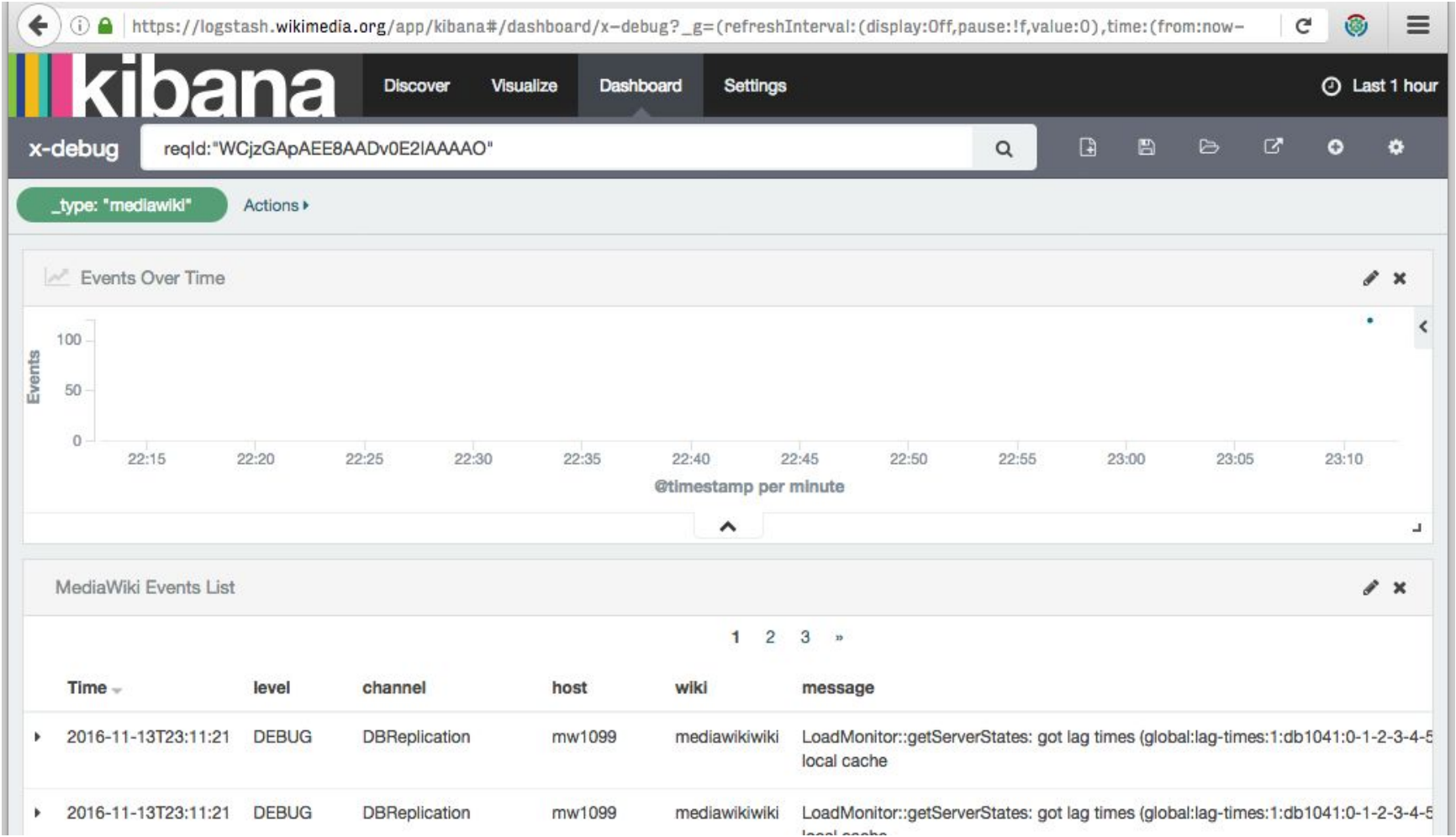
Read more at https://wikitech.wikimedia.org/wiki/X-Wikimedia-Debug

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.


https://logstash.wikimedia.org/app/kibana#/dashboard/x-debug?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-
kibana
Discover
Visualize
Dashboard
Settings
Last 1 hour
x-debug
reqId:"WCjzGApAEE8AADv0E2IAAAAO"
_type: "mediawiki"
Actions
Events Over Time
Events
100
50
0
22:15
22:20
22:25
22:30
22:35
22:40
22:45
22:50
22:55
23:00
23:05
23:10
@timestamp per minute
MediaWiki Events List
1 2 3 »
Time
level
channel
host
wiki
message
2016-11-13T23:11:21 DEBUG DBReplication mw1099 mediawikiwiki LoadMonitor::getServerStates: got lag times (global:lag-times:1:db1041:0-1-2-3-4-5
local cache
2016-11-13T23:11:21 DEBUG DBReplication mw1099 mediawikiwiki LoadMonitor::getServerStates: got lag times (global:lag-times:1:db1041:0-1-2-3-4-5

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.