

Using Kibana4 to read logs at Wikimedia

Wikimedia Tech Talk, 2016-11-14



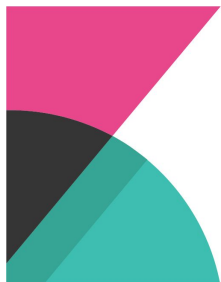
Elasticsearch

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.



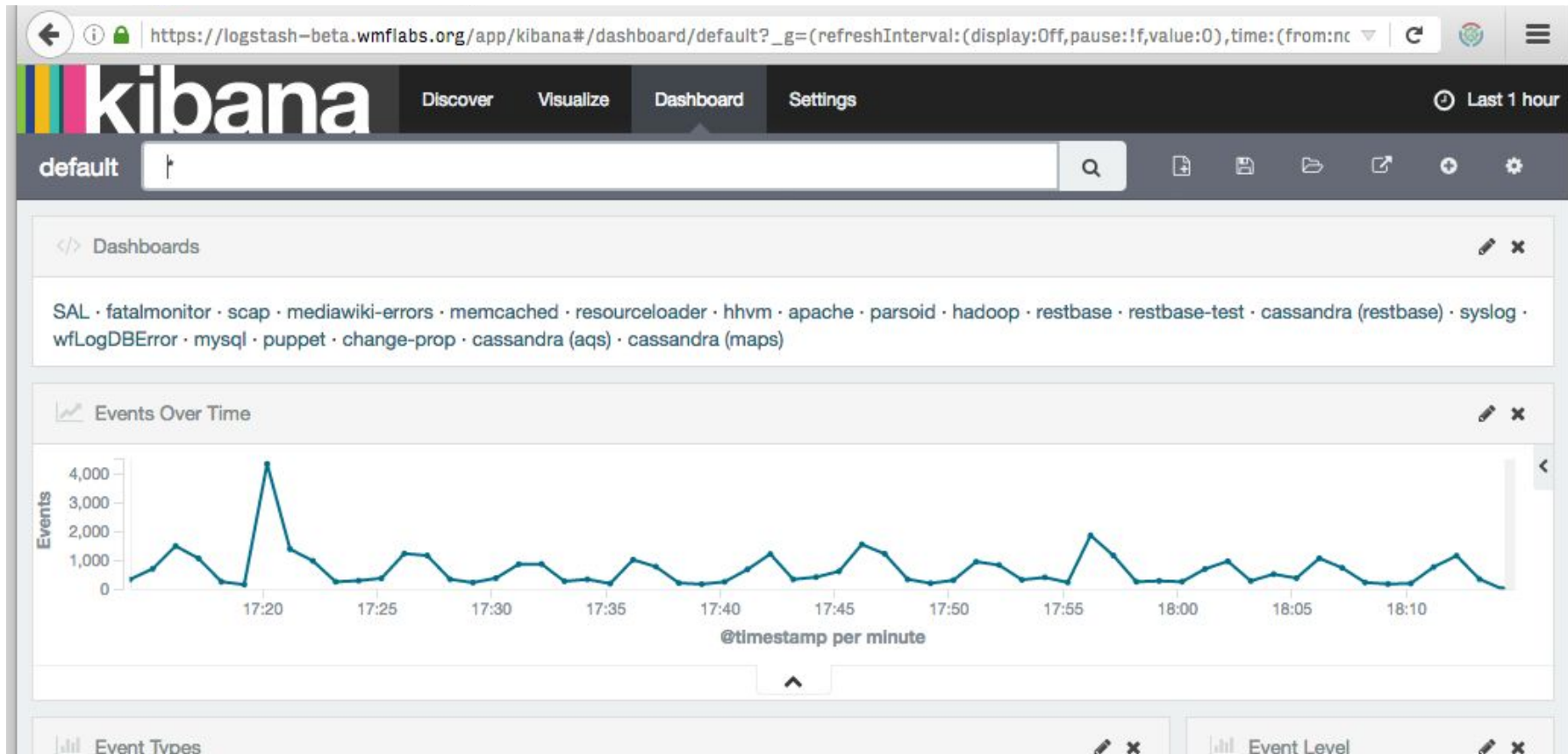
Kibana

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

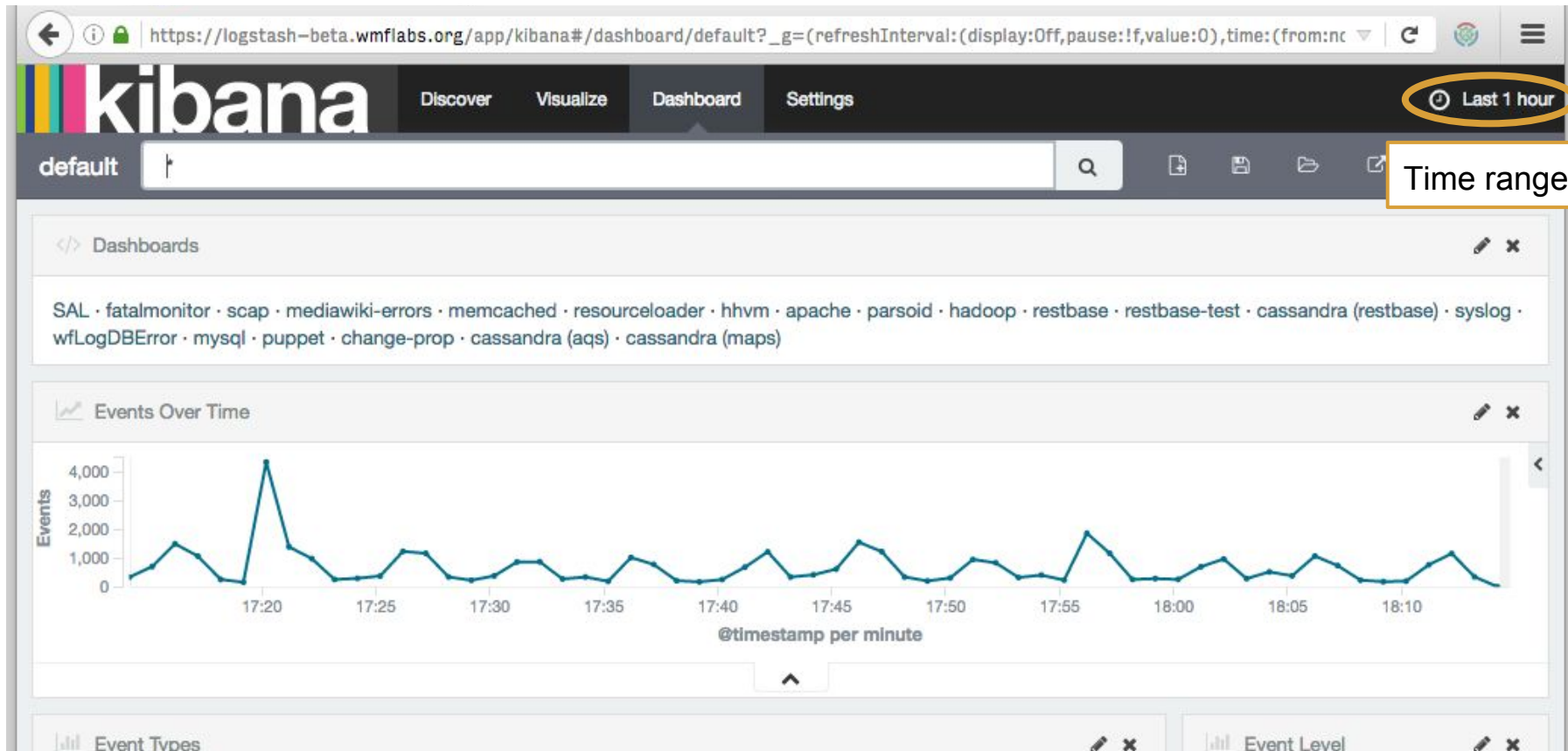


Kibana4 Dashboards

The screenshot displays the Kibana4 web interface. At the top, the browser address bar shows the URL: `https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:nc`. The Kibana logo is on the left, and navigation tabs for 'Discover', 'Visualize', 'Dashboard', and 'Settings' are in the center. On the right, there is a 'Last 1 hour' filter. Below the navigation bar, a search bar contains the text 'default', which is circled in orange. A callout box with an orange border points to this search bar, containing the text 'Dashboard name'. Below the search bar, a list of dashboard items is shown, including 'SAL', 'fatalmonitor', 'scap', 'mediawiki-errors', 'memcached', 'resourceloader', 'hhvm', 'apache', 'parsoid', 'hadoop', 'restbase', 'restbase-test', 'cassandra (restbase)', 'syslog', 'wfLogDBError', 'mysql', 'puppet', 'change-prop', 'cassandra (aqs)', and 'cassandra (maps)'. The main visualization area shows a line chart titled 'Events Over Time' with a y-axis labeled 'Events' ranging from 0 to 4,000 and an x-axis labeled '@timestamp per minute' with time markers from 17:20 to 18:10. The chart shows a significant spike in events around 17:20. Below the chart, there are tabs for 'Event Types' and 'Event Level'.

Dashboard name

Kibana4 Dashboards



Kibana4 Dashboards

The screenshot shows the Kibana4 web interface. The browser address bar displays the URL: `https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:nc`. The Kibana logo is visible on the left, and navigation tabs for "Discover", "Visualize", "Dashboard", and "Settings" are in the center. On the right, there are controls for "Auto-refresh" and "Last 1 hour", with the latter being circled in green. Below the navigation bar, a "Quick" menu is open, showing a grid of time range options. At the bottom, a search bar contains the text "default" and a list of dashboard names is displayed.

Browser address bar: `https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:nc`

Navigation tabs: Discover, Visualize, **Dashboard**, Settings

Auto-refresh: [Refresh icon] Auto-refresh [On/Off]

Last 1 hour: [Refresh icon] Last 1 hour

Quick menu options:

Quick	Today	Yesterday	Last 15 minutes	Last 30 days
Relative	This week	Day before yesterday	Last 30 minutes	Last 60 days
Absolute	This month	This day last week	Last 1 hour	Last 90 days
	This year	Previous week	Last 4 hours	Last 6 months
	The day so far	Previous month	Last 12 hours	Last 1 year
	Week to date	Previous year	Last 24 hours	Last 2 years
	Month to date		Last 7 days	Last 5 years
	Year to date			

Search bar: default [Search icon]

Dashboard list: </> Dashboards [Edit icon] [Close icon]

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

Kibana4 Dashboards

The screenshot shows the Kibana4 dashboard interface. At the top, the URL is `https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:nc`. The navigation bar includes "Discover", "Visualize", "Dashboard", and "Settings". The "default" dashboard is selected, and a search bar contains the query `Elasticsearch "query string query"`. Below the search bar, a list of log sources is shown: `SAL · fatalmonitor · scan · mediawiki_errors · memcached · resourceloader · bhym · apache · parseid · hadoop · restbase · restbase-test · cassandra (restbase) · syslog · wfLog`. A text box explains: "Search terms are OR'ed by default. Use 'AND' to combine terms." Below this, the "Events Over Time" visualization is shown as a line graph. The y-axis is labeled "Events" and ranges from 0 to 4,000. The x-axis is labeled "@timestamp per minute" and shows time from 17:20 to 18:10. The graph shows a significant spike in events around 17:20, reaching approximately 4,000 events per minute, followed by a period of lower activity with several smaller peaks.

default

Elasticsearch "[query string query](#)"

SAL · fatalmonitor · scan · mediawiki_errors · memcached · resourceloader · bhym · apache · parseid · hadoop · restbase · restbase-test · cassandra (restbase) · syslog · wfLog

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

Events Over Time

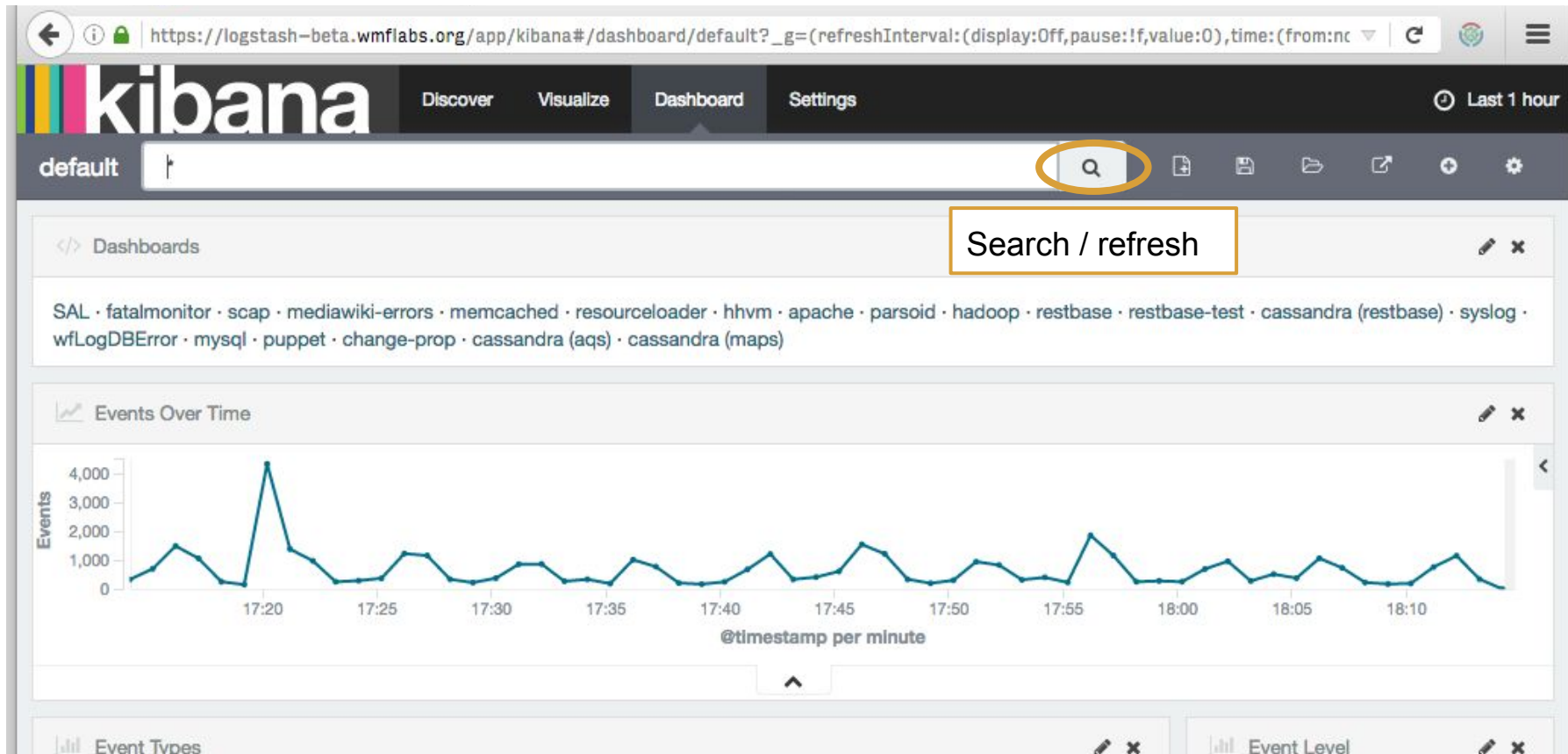
Events

@timestamp per minute

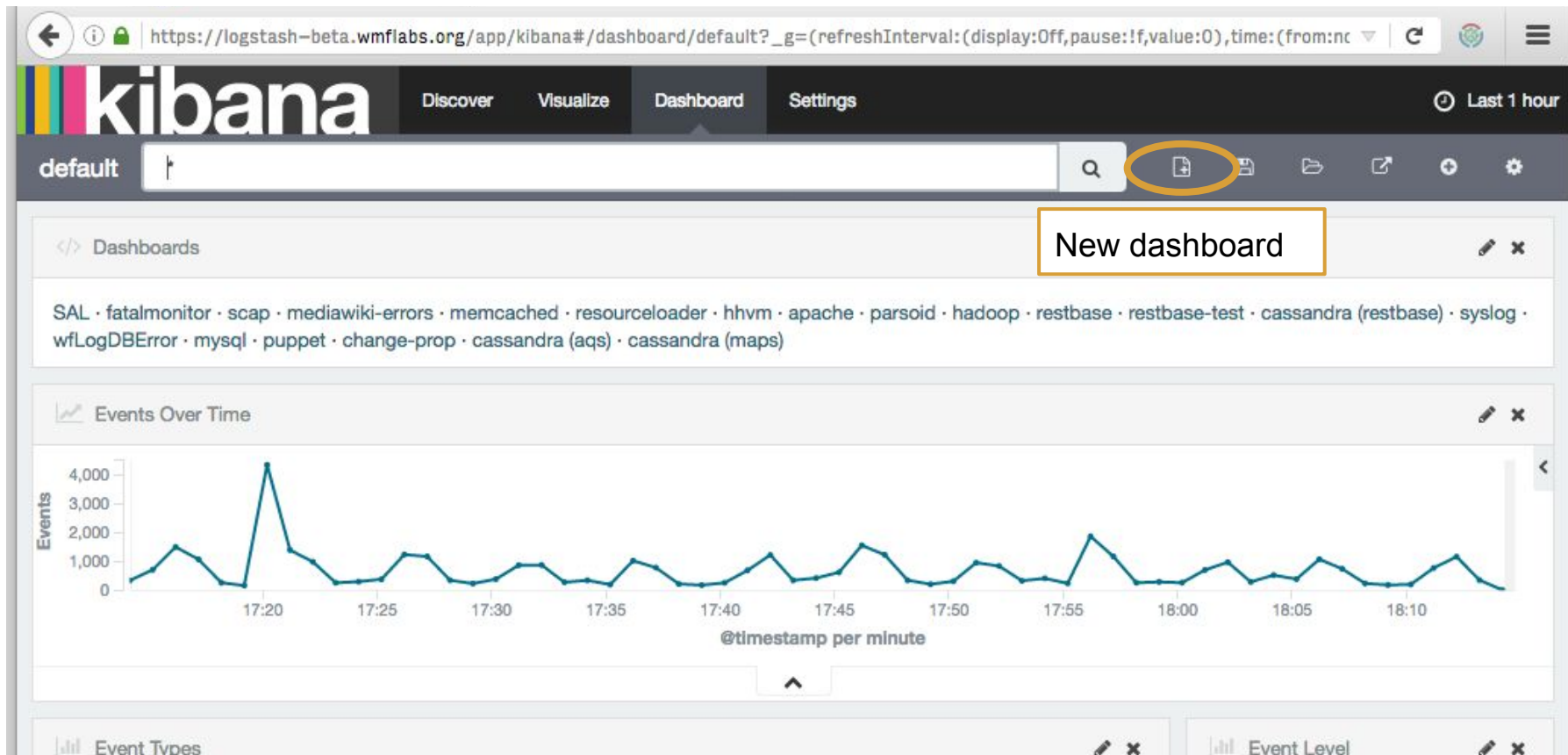
Event Types

Event Level

Kibana4 Dashboards



Kibana4 Dashboards



Kibana4 Dashboards

default

Save dashboard

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.

Events Over Time

Events

@timestamp per minute

Timestamp	Events
17:20	400
17:21	1500
17:22	1000
17:23	200
17:24	4000
17:25	1200
17:26	400
17:27	1000
17:28	1200
17:29	400
17:30	400
17:31	900
17:32	900
17:33	400
17:34	400
17:35	1000
17:36	800
17:37	400
17:38	400
17:39	1200
17:40	400
17:41	400
17:42	400
17:43	1500
17:44	1200
17:45	1500
17:46	400
17:47	400
17:48	400
17:49	400
17:50	1000

Kibana4 Dashboards

The screenshot displays the Kibana4 dashboard interface. At the top, the browser address bar shows the URL: `https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:nc`. The Kibana logo is on the left, and navigation tabs for 'Discover', 'Visualize', 'Dashboard', and 'Settings' are in the center. A search bar contains the text 'default'. On the right, there are icons for saving, loading, and other actions. A yellow circle highlights the 'Load dashboard' icon (a folder with an arrow). Below this, a button labeled 'Load dashboard' is highlighted with a yellow box. The main content area shows a list of dashboards: 'SAL · fatalmonitor · scap · mediawiki-errors · memcached · resourceloader · hhvm · apache · parsoid · hadoop · restbase · restbase-test · cassandra (restbase) · syslog · wfLogDBError · mysql · puppet · change-prop · cassandra (aqs) · cassandra (maps)'. Below the list is a visualization titled 'Events Over Time', which is a line chart showing the number of events per minute from 17:20 to 18:10. The y-axis is labeled 'Events' and ranges from 0 to 4,000. The x-axis is labeled '@timestamp per minute' and shows time intervals. The chart shows a significant spike in events around 17:20, reaching over 4,000. Other smaller spikes occur around 17:45 and 17:55. Below the chart, there are tabs for 'Event Types' and 'Event Level'.

default

Discover Visualize Dashboard Settings

Last 1 hour

Load dashboard

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

Events Over Time

Events

@timestamp per minute

Event Types

Event Level

Kibana4 Dashboards

The screenshot displays the Kibana4 dashboard interface. At the top, the browser address bar shows the URL: `https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:nc`. The Kibana logo is on the left, and navigation tabs for 'Discover', 'Visualize', 'Dashboard', and 'Settings' are in the center. A search bar contains the text 'default'. On the right, there are icons for file operations and a 'Share current view' icon, which is circled in yellow. Below the navigation bar, a 'Dashboards' section lists various dashboards: SAL, fatalmonitor, scap, mediawiki-errors, memcached, resourceloader, hhvm, apache, parsoid, hadoop, restbase, restbase-test, cassandra (restbase), syslog, wfLogDBError, mysql, puppet, change-prop, cassandra (aqs), and cassandra (maps). The main area features a line chart titled 'Events Over Time' showing event counts per minute from 17:20 to 18:10. The y-axis is labeled 'Events' and ranges from 0 to 4,000. The x-axis is labeled '@timestamp per minute'. A prominent peak is visible at 17:20, reaching approximately 4,200 events. Other smaller peaks occur around 17:45 and 17:55. Below the chart, there are tabs for 'Event Types' and 'Event Level'.

default

Discover Visualize Dashboard Settings

Last 1 hour

Share current view

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

Events Over Time

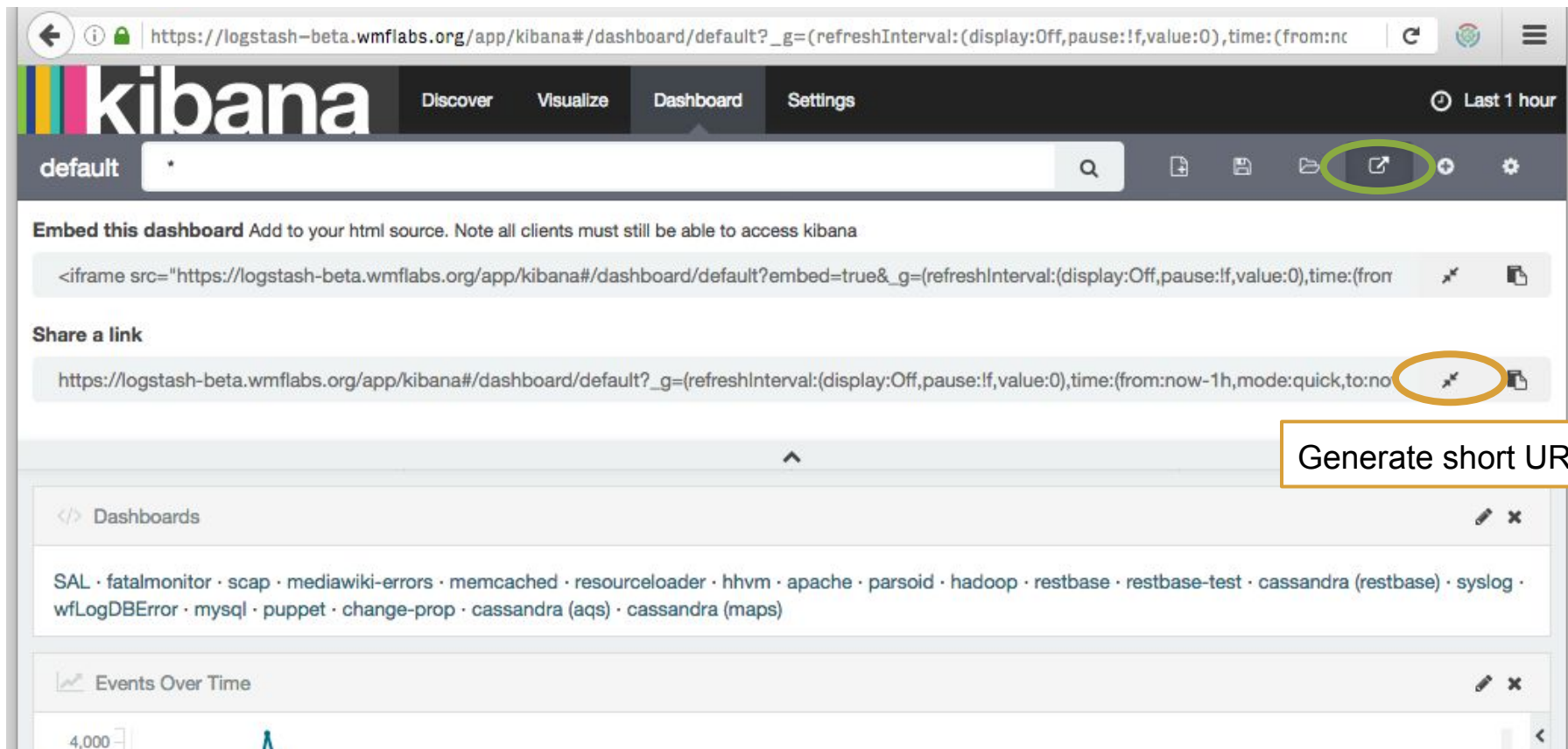
Events

@timestamp per minute

Event Types

Event Level

Kibana4 Dashboards



The screenshot shows the Kibana4 dashboard interface. At the top, there is a navigation bar with the Kibana logo and tabs for Discover, Visualize, Dashboard, and Settings. The current view is the 'default' dashboard. Below the navigation bar, there is a search bar and a toolbar with icons for save, share, and settings. The share icon is circled in green. Below the toolbar, there is a section for embedding the dashboard, followed by a section for sharing a link. The share link is circled in orange, and a callout box points to it with the text 'Generate short URL'. Below the share link, there is a list of dashboards and an 'Events Over Time' chart.

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

```
<iframe src="https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?embed=true&_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-1h,mode:quick,to:now))" />
```

Share a link

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

Generate short URL

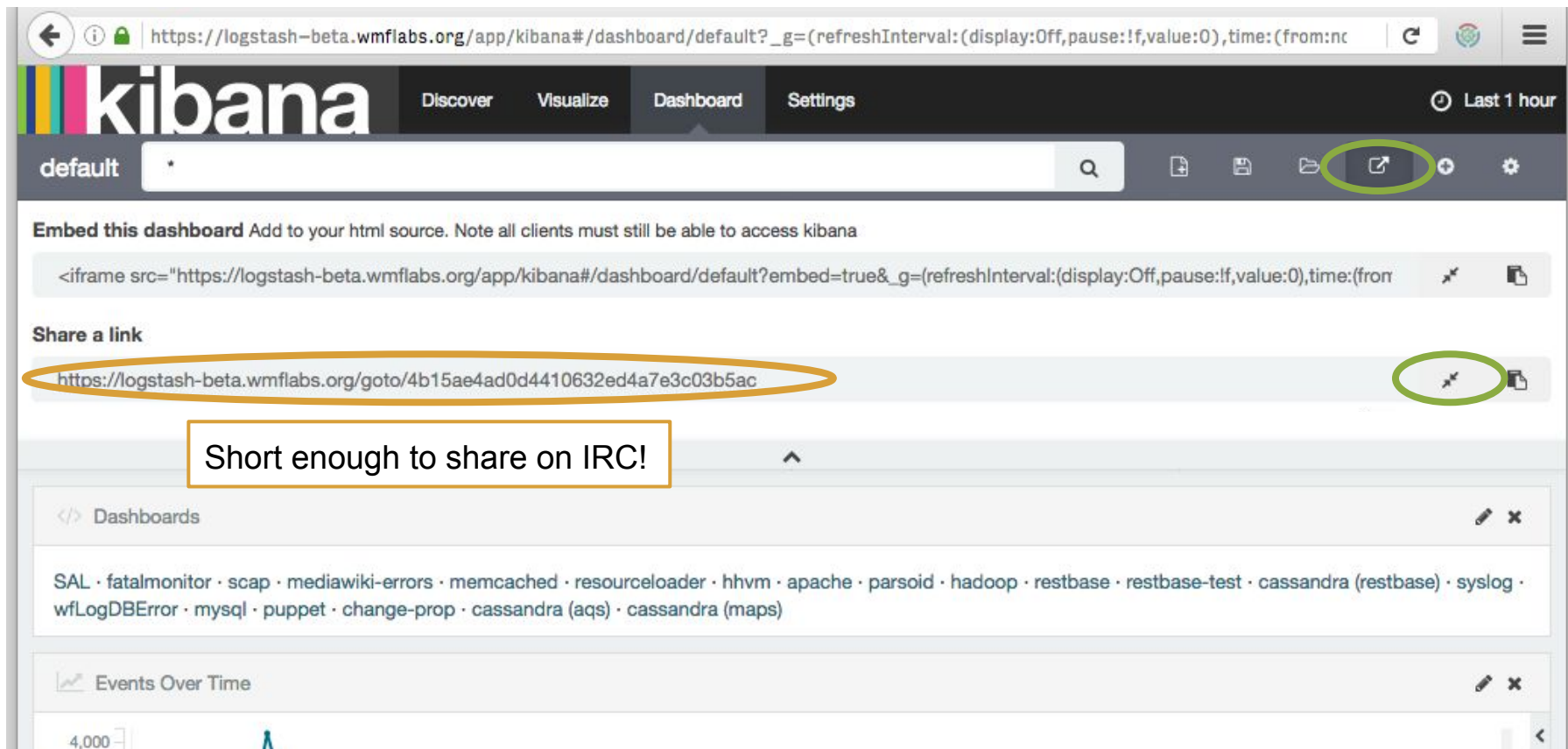
</> Dashboards

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

Events Over Time

4,000

Kibana4 Dashboards



The screenshot shows the Kibana4 dashboard interface. At the top, the URL is `https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:nc`. The navigation bar includes "Discover", "Visualize", "Dashboard", and "Settings". The "default" dashboard is selected, and the time range is set to "Last 1 hour".

Below the navigation bar, there are icons for "Embed", "Save", "Share", "Refresh", and "Settings". The "Share" icon (a square with an arrow) is circled in green. Below this, the "Embed this dashboard" section provides an `<iframe src="https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?embed=true&_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from` snippet. The "Share a link" section shows a URL: `https://logstash-beta.wmflabs.org/goto/4b15ae4ad0d4410632ed4a7e3c03b5ac`, which is circled in orange. A green circle highlights the share icon next to this link. A text box with an orange border contains the text "Short enough to share on IRC!".

At the bottom, the dashboard content is visible, including a "Dashboards" section with a list of dashboards: SAL, fatalmonitor, scap, mediawiki-errors, memcached, resourceloader, hvm, apache, parsoid, hadoop, restbase, restbase-test, cassandra (restbase), syslog, wfLogDBError, mysql, puppet, change-prop, cassandra (aqs), and cassandra (maps). Below this is an "Events Over Time" section with a line graph and a y-axis value of 4,000.

Kibana4 Dashboards

The screenshot displays the Kibana4 dashboard interface. At the top, the browser address bar shows the URL: `https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:nc`. The Kibana logo is on the left, and navigation tabs for 'Discover', 'Visualize', 'Dashboard', and 'Settings' are in the center. A 'Last 1 hour' filter is on the right. Below the navigation bar is a search bar with the text 'default' and a search icon. To the right of the search bar is a toolbar with icons for home, save, share, and a circled 'Add visualization' button. Below the toolbar is a 'Dashboards' section with a list of dashboard names: 'SAL · fatalmonitor · scap · mediawiki-errors · memcached · resourceloader · hhvm · apache · parsoid · hadoop · restbase · restbase-test · cassandra (restbase) · syslog · wfLogDBError · mysql · puppet · change-prop · cassandra (aqs) · cassandra (maps)'. Below this is an 'Events Over Time' visualization, a line chart showing event counts per minute. The y-axis is labeled 'Events' and ranges from 0 to 4,000. The x-axis is labeled '@timestamp per minute' and shows time from 17:20 to 18:10. A significant peak is visible at approximately 17:20, reaching over 4,000 events. Below the chart is an 'Event Types' section with a bar chart and an 'Event Level' section with a bar chart.

default

Discover Visualize Dashboard Settings

Last 1 hour

default

+

</> Dashboards

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

Events Over Time

Events

@timestamp per minute

Event Types

Event Level

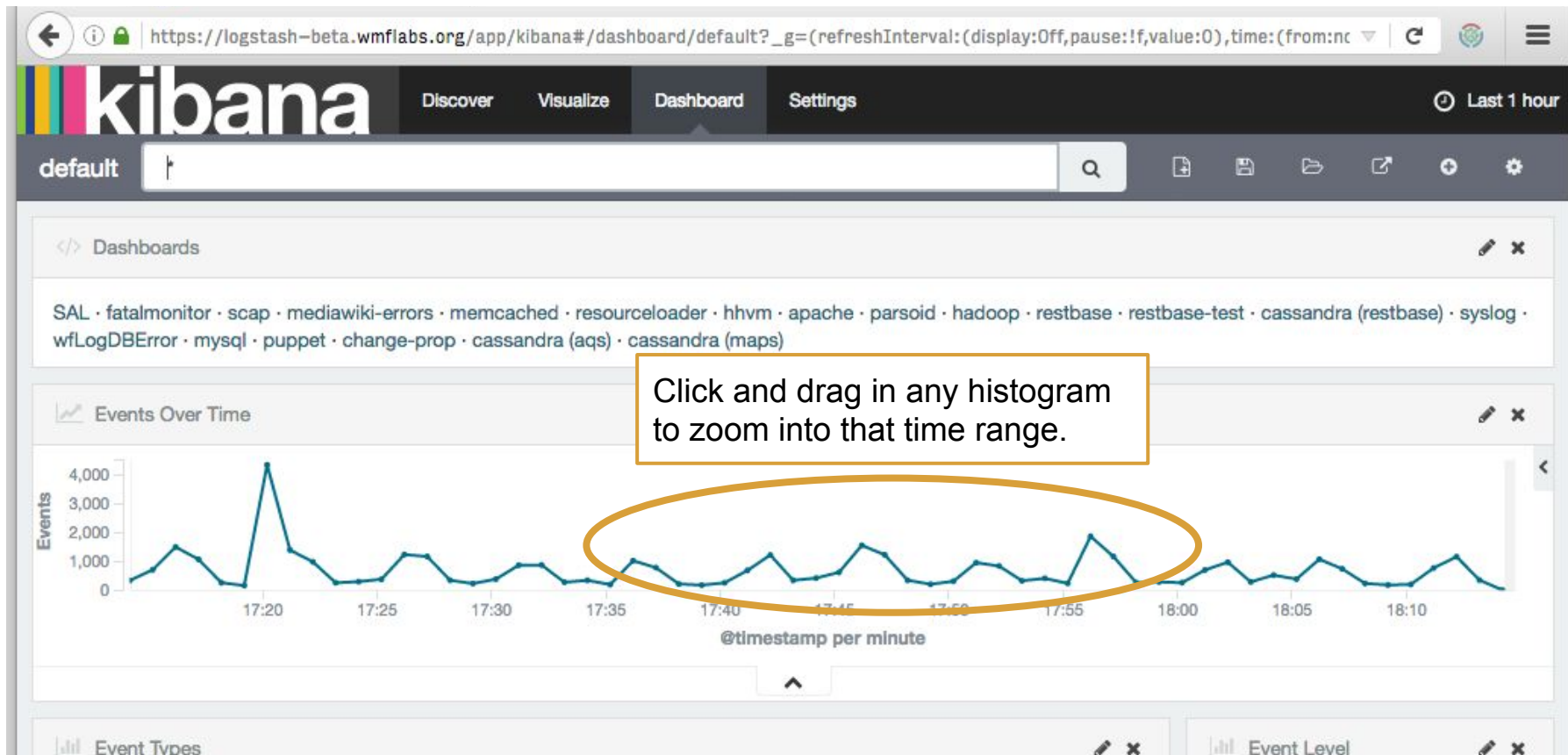
Add visualization

Kibana4 Dashboards

The screenshot displays the Kibana4 dashboard interface. At the top, the URL is `https://logstash-beta.wmflabs.org/app/kibana#/dashboard/default?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:nc`. The navigation bar includes the Kibana logo, tabs for "Discover", "Visualize", "Dashboard", and "Settings", and a "Last 1 hour" time filter. A search bar contains the text "default". To the right of the search bar are icons for home, save, share, and a settings gear icon, which is circled in orange. Below the search bar, a "Dashboards" section lists various dashboards: "SAL · fatalmonitor · scap · mediawiki-errors · memcached · resourceloader · hhvm · apache · parsoid · hadoop · restbase · restbase-test · cassandra (restbase) · syslog · wfLogDBError · mysql · puppet · change-prop · cassandra (aqs) · cassandra (maps)". The main visualization is a line chart titled "Events Over Time" showing the number of events per minute from 17:20 to 18:10. The y-axis is labeled "Events" and ranges from 0 to 4,000. The x-axis is labeled "@timestamp per minute" and shows time intervals. The chart shows a significant spike in events around 17:20, reaching approximately 4,000. Other smaller spikes occur around 17:45 and 17:55. Below the chart, there are sections for "Event Types" and "Event Level", both with edit and close icons.

Options

Kibana4 Dashboards



Kibana4 Discover

Browser address bar: [https://logstash-beta.wmflabs.org/app/kibana#/discover?_g=\(refreshInterval:\(display:Off,pause:!f,value:0\),time:\(from:now-1h,mor](https://logstash-beta.wmflabs.org/app/kibana#/discover?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-1h,mor)

kibana Discover Visualize Dashboard Settings Last 1 hour

logstash-* 41,614 hits

2016-11-13T17:16:56 - 2016-11-13T18:16:56 — by minute

Time	Count
17:16:56	1000
17:17:56	200
17:18:56	400
17:19:56	4200
17:20:56	1300
17:21:56	1000
17:22:56	300
17:23:56	400
17:24:56	1200
17:25:56	1100
17:26:56	400
17:27:56	400
17:28:56	800
17:29:56	800
17:30:56	300
17:31:56	400
17:32:56	1000
17:33:56	600
17:34:56	300
17:35:56	400
17:36:56	200
17:37:56	400
17:38:56	600
17:39:56	1200
17:40:56	400
17:41:56	600
17:42:56	1500
17:43:56	1200
17:44:56	400
17:45:56	1500
17:46:56	1200
17:47:56	400
17:48:56	600
17:49:56	900
17:50:56	800
17:51:56	400
17:52:56	600
17:53:56	1800
17:54:56	1200
17:55:56	400
17:56:56	600
17:57:56	400
17:58:56	600
17:59:56	400
18:00:56	600
18:01:56	400
18:02:56	800
18:03:56	1000
18:04:56	400
18:05:56	600
18:06:56	400
18:07:56	1000
18:08:56	600
18:09:56	400
18:10:56	400
18:11:56	600
18:12:56	1100
18:13:56	400
18:14:56	600
18:15:56	1400

Selected Fields: ? _source

Available Fields: [Settings]

Popular:

- # _score
- ↑ channel
- ↑ log_messages
- ↑ wiki

Time: @timestamp

@version

↑ _id

↑ index

Time	_source
2016-11-13T18:16:53	<code>message: Connection closed by 10.68.16.210 [preauth] @version: 1 @timestamp: 2016-11-13T18:16:53 type: syslog host: deployment-ircd priority: 38 timestamp@601: 2016-11</code>

Kibana4 Discover

The screenshot displays the Kibana Discover interface. At the top, the browser address bar shows the URL: `https://logstash-beta.wmflabs.org/app/kibana#/discover?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-1h,mor`. The Kibana logo is on the left, and navigation tabs for 'Discover', 'Visualize', 'Dashboard', and 'Settings' are in the center. A search bar is on the right, and a refresh icon is labeled 'Last 1 hour'. Below the navigation, a search bar contains a single asterisk. On the left, a sidebar for 'logstash-*' lists 'Selected Fields' (including `? _source`) and 'Available Fields' (including `# _score`, `↑ channel`, `↑ log_messages`, `↑ wiki`, `○ @timestamp`, `↑ @version`, `↑ _id`, and `↑ index`). The main area shows a bar chart for the time range '2016-11-13T17:16:56 - 2016-11-13T18:16:56' with a 'by minute' aggregation. The y-axis is labeled 'Count' and ranges from 0 to 4,000. A large orange box with the text 'Live Demo' is overlaid on the chart. Below the chart, a table shows a log entry:

Time	_source
2016-11-13T18:16:53	<code>message: Connection closed by 10.68.16.210 [preauth] @version: 1 @timestamp: 2016-11-13T18:16:53 type: syslog host: deployment-ircd priority: 38 timestamp@601: 2016-11</code>

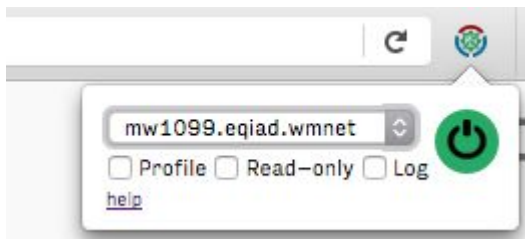
X-Wikimedia-Debug header

- 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.

x-debug

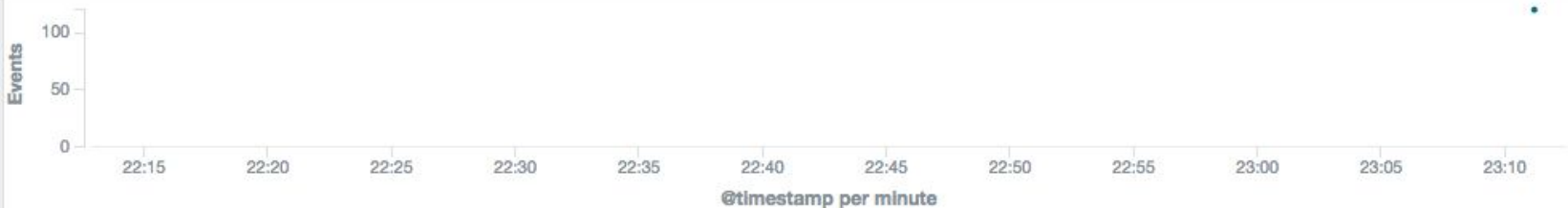
reqId:"WCjzGApAEE8AADv0E2IAAAAO"



_type: "mediawiki"

Actions ▶

Events Over Time



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 local cache

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.

Copyright © 2016, [Bryan Davis](#) and the [Wikimedia Foundation](#).

This work is licensed under a [Creative Commons Attribution-Share Alike 4.0 International](#) license.

