The Elastic Stack

Log management and analysis

Klaus Kämpf
Product Owner
kkaempf@suse.com

About this presentation

- What is log analysis ?
- Why do I need it ?
- The Elastic stack
- Practical example
- Alternatives

About me

- SUSE veteran
- Open source veteran

  (Google knows it all)
- Father, Maker, Hacker
- Agilist
- Currently: Product Owner for SUSE Container platform offering

Log Analysis

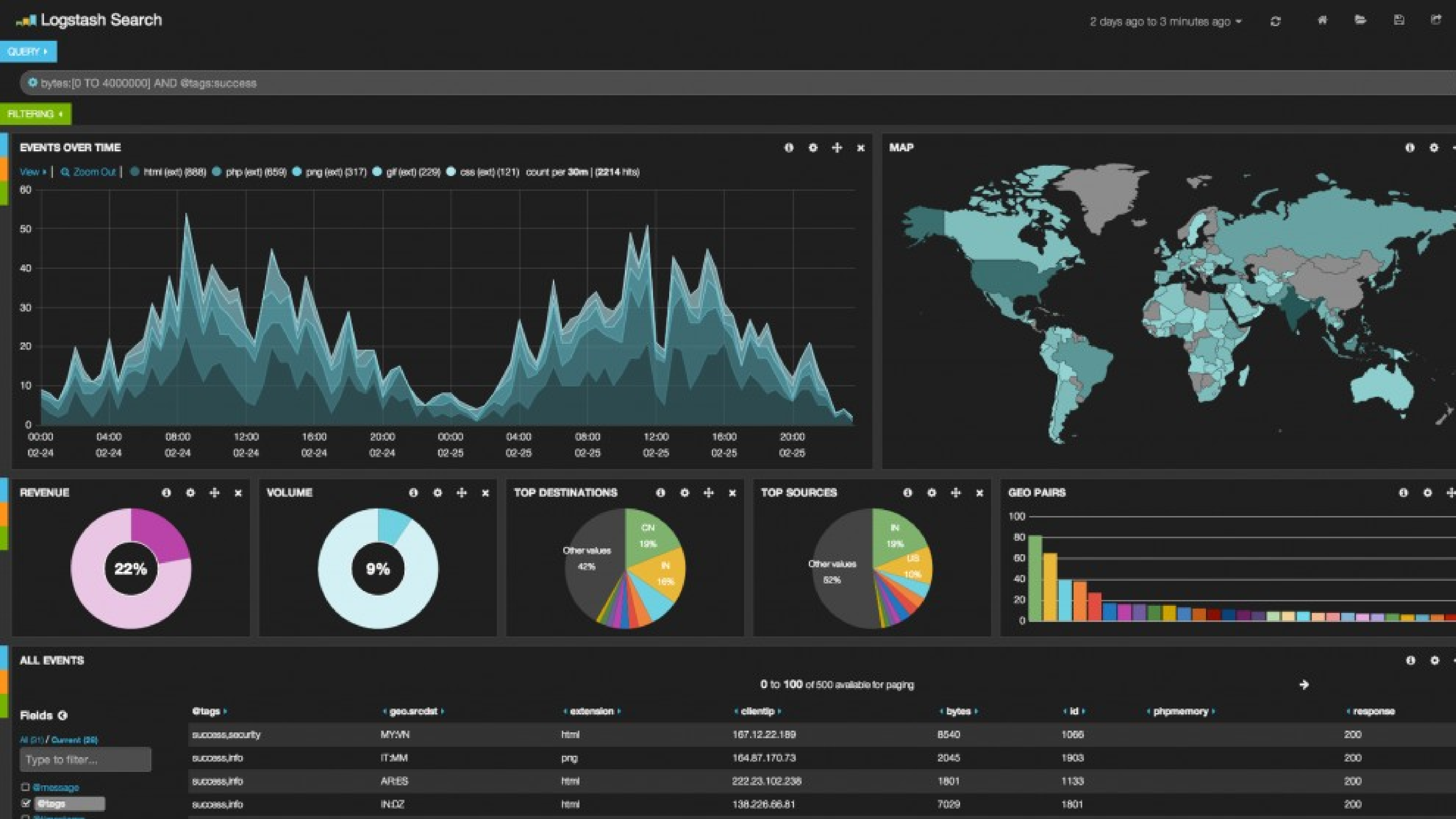
```
127.0.0.1 - - [05/Oct/2016:15:30:18 +0200] "GET /cgi-bin/translate_key.cgi?scout_shared_key=7a6a63848194
10.160.4.230 - - [05/Oct/2016:15:30:18 +0200] "POST /satconfig/cgi-mod-perl/accept_status_log.cgi HTTP/1.
127.0.0.1 - - [05/Oct/2016:15:30:39 +0200] "GET /cgi-bin/translate_key.cgi?scout_shared_key=7a6a63848194
10.160.4.230 - - [05/Oct/2016:15:30:39 +0200] "POST /tsdb HTTP/1.1" 200 82 "-" "libwww-perl/5.816"
10.160.4.230 - - [05/Oct/2016:15:30:39 +0200] "POST /cgi-bin/eventHandler.cgi HTTP/1.1" 200 82
127.0.0.1 - - [05/Oct/2016:15:30:40 +0200] "GET /cgi-bin/translate_key.cgi?scout_shared_key=7a6a63848194
10.160.4.230 - - [05/Oct/2016:15:30:40 +0200] "GET /satconfig/cgi-mod-perl/fetch_commands.cgi?cluster_id=
10.160.4.230 - - [05/Oct/2016:15:30:41 +0200] "GET /satconfig/cgi-mod-perl/fetch_commands.cgi?cluster_id=
10.160.4.230 - - [05/Oct/2016:15:30:50 +0200] "POST /tsdb HTTP/1.1" 200 164 "-" "libwww-perl/5.816"
10.160.4.230 - - [05/Oct/2016:15:30:50 +0200] "POST /cgi-bin/eventHandler.cgi HTTP/1.1" 200 164
10.162.166.1 - - [05/Oct/2016:15:30:58 +0200] "POST /XMLRPC HTTP/1.1" 200 163
10.162.166.1 - - [05/Oct/2016:15:30:58 +0200] "POST /XMLRPC HTTP/1.1" 200 731
10.160.4.230 - - [05/Oct/2016:15:31:00 +0200] "POST /cobbler_api HTTP/1.1" 200 144 "-" "Java/1.7.0"
10.160.4.230 - - [05/Oct/2016:15:31:00 +0200] "POST /cobbler_api HTTP/1.1" 200 129 "-" "Java/1.7.0"
10.160.4.230 - - [05/Oct/2016:15:31:00 +0200] "POST /tsdb HTTP/1.1" 200 111 "-" "libwww-perl/5.816"
10.160.4.230 - - [05/Oct/2016:15:31:00 +0200] "POST /cgi-bin/eventHandler.cgi HTTP/1.1" 200 111
10.160.4.230 - - [05/Oct/2016:15:31:05 +0200] "POST /tsdb HTTP/1.1" 200 87 "-" "libwww-perl/5.816"
10.160.4.230 - - [05/Oct/2016:15:31:05 +0200] "POST /cgi-bin/eventHandler.cgi HTTP/1.1" 200 87
127.0.0.1 - - [05/Oct/2016:15:31:18 +0200] "GET /cgi-bin/translate_key.cgi?scout_shared_key=7a6a63848194
10.160.4.230 - - [05/Oct/2016:15:31:18 +0200] "POST /satconfig/cgi-mod-perl/accept_status_log.cgi HTTP/1.
10.160.4.230 - - [05/Oct/2016:15:31:41 +0200] "GET /satconfig/cgi-mod-perl/fetch_commands.cgi?cluster_id=
10.160.4.230 - - [05/Oct/2016:15:32:00 +0200] "POST /cobbler_api HTTP/1.1" 200 144 "-" "Java/1.7.0"
10.160.4.230 - - [05/Oct/2016:15:32:00 +0200] "POST /cobbler_api HTTP/1.1" 200 129 "-" "Java/1.7.0"
127.0.0.1 - - [05/Oct/2016:15:32:18 +0200] "GET /cgi-bin/translate_key.cgi?scout_shared_key=7a6a63848194
10.160.4.230 - - [05/Oct/2016:15:32:18 +0200] "POST /satconfig/cgi-mod-perl/accept_status_log.cgi HTTP/1.
10.162.166.1 - - [05/Oct/2016:15:32:26 +0200] "POST /XMLRPC HTTP/1.1" 200 163
10.162.166.1 - - [05/Oct/2016:15:32:27 +0200] "POST /XMLRPC HTTP/1.1" 200 731
```

Problem statement

- Many deamons
- Large stacks
- Distributed
- Huge amounts of data
- Hard to read

Problem statement (2)

- Central logging
- Safe, Tamper-resistant
- Dependency, Causality
- One-offs vs. Trends
- Text vs. Graphic



bytes:[0 TO 4000000] AND @tags:success

0 to 100 of 500 available for paging

@tags	geo.srcdst	extension	clientip	bytes	id	phpmemory	response
success,security	MY:VN	html	167.12.22.189	8540	1066		200
success,info	IT:MM	png	164.87.170.73	2045	1903		200
success,info	AR:ES	html	222.23.102.238	1801	1133		200
success,info	IN:DZ	html	138.226.66.81	7029	1801		200

The Elastic stack

(formerly: ELK stack)

Elasticsearch

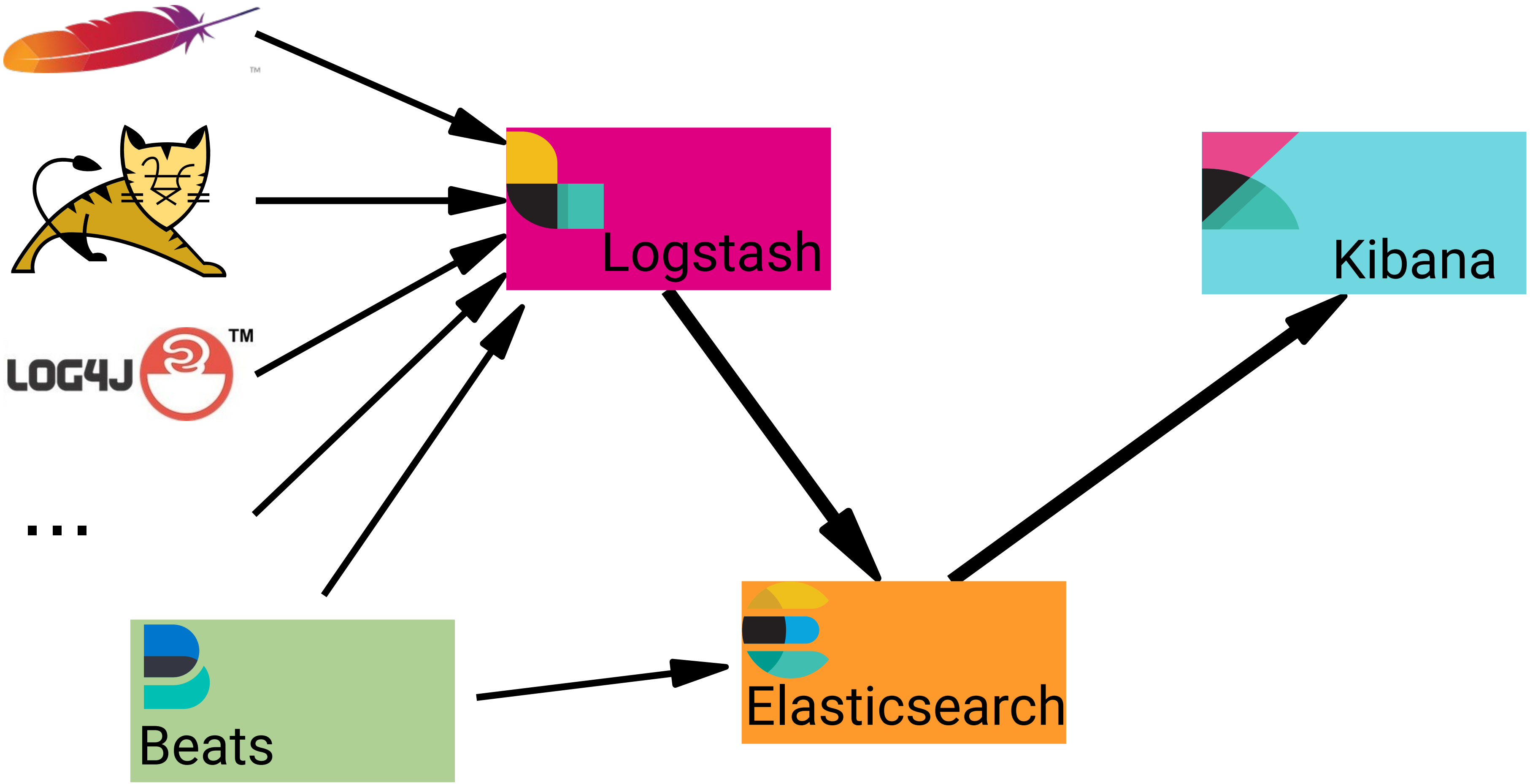
Logstash

Kibana

Database

Log server / parser

UI



Logstash

Kibana

...

Beats

Elasticsearch

Apache Logos: The Apache Software Foundation - http://svn.apache.org/viewvc/jakarta/site/xdocs/images/logos/tomcat.eps, Apache License 2.0, https://commons.wikimedia.org/w/index.php?curid=11302180

Beats

Beats

- Formerly ‘logstash-forwarder’
- Unobtrusive (log) file forwarder
  - ‘tail -f | tee’
- Written in Go, fast
- Simple configuration

Beats

- Filebeat
- Metricbeat
- Packetbeat
- Heartbeat
- Auditbeat
- Winlogbeat
- Functionbeat

Example: Apache + Filebeat

```
# /usr/filebeat/filebeat.yml
filebeat:
  prospectors:
    -
      paths:
        - /var/log/apache2/access_log
      encoding: utf-8
      input_type: log
      document_type: access_log
    ...
output:
  logstash:
    hosts: ["logstash.mgr.suse.de:5045"]
```

Elasticsearch

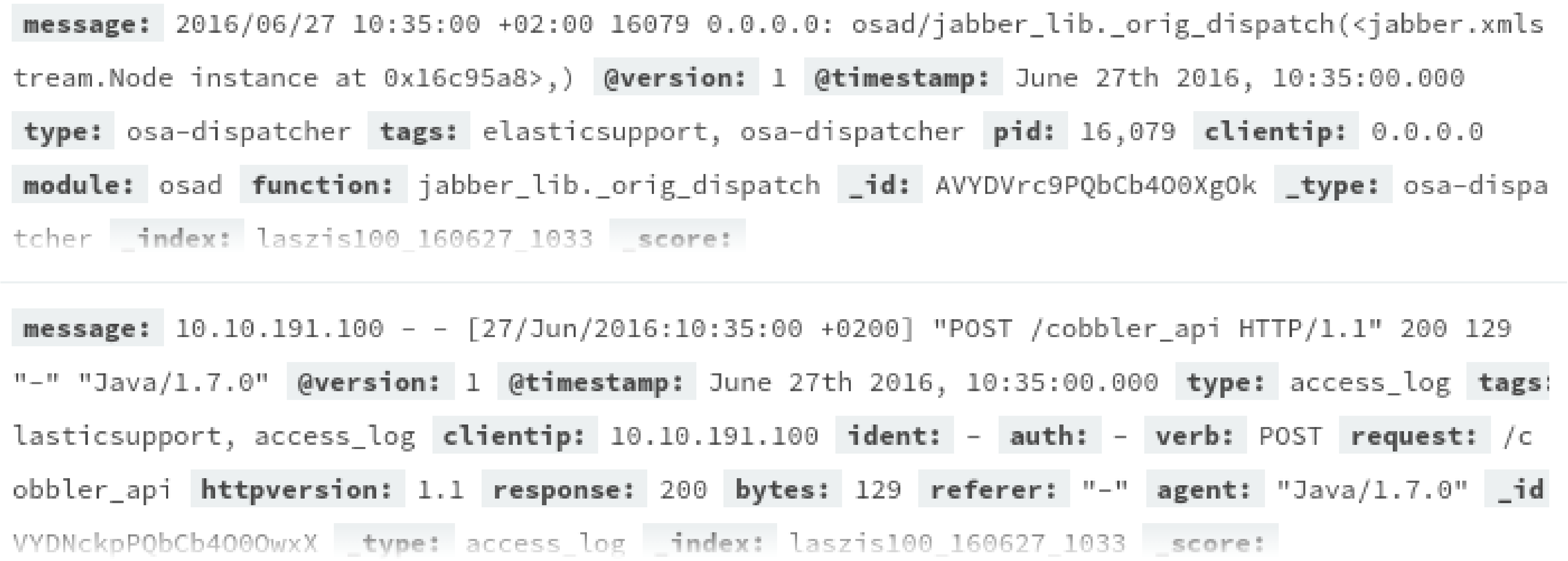
Elasticsearch

- Fulltext database (Apache Lucene)
- Key-Value pairs
- Scalable

Terminology

- Index: Database
- Mapping: Schema
- Document: Record
- Field: key-value pair

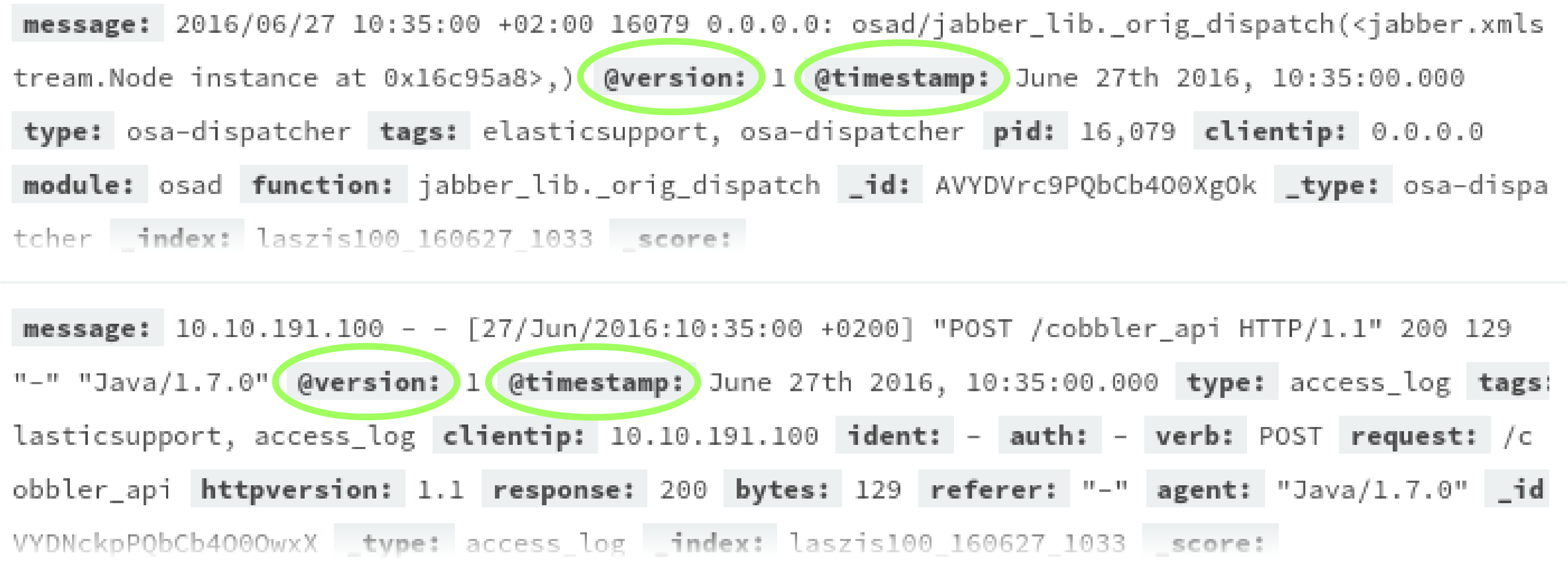
Elasticsearch – raw data



```
message: 2016/06/27 10:35:00 +02:00 16079 0.0.0.0: osad/jabber_lib._orig_dispatch(<jabber.xmls
tream.Node instance at 0x16c95a8>,) @version: 1 @timestamp: June 27th 2016, 10:35:00.000
type: osa-dispatcher tags: elasticsupport, osa-dispatcher pid: 16,079 clientip: 0.0.0.0
module: osad function: jabber_lib._orig_dispatch _id: AVYDVrc9PQbCb4O0XgOk _type: osa-dispa
tcher _index: laszis100_160627_1033 _score:
```

```
message: 10.10.191.100 - - [27/Jun/2016:10:35:00 +0200] "POST /cobbler_api HTTP/1.1" 200 129
"-" "Java/1.7.0" @version: 1 @timestamp: June 27th 2016, 10:35:00.000 type: access_log tags:
lasticsupport, access_log clientip: 10.10.191.100 ident: - auth: - verb: POST request: /c
obbler_api httpversion: 1.1 response: 200 bytes: 129 referer: "-" agent: "Java/1.7.0" _id
VYDNckpPQbCb4O0OwxX _type: access_log _index: laszis100_160627_1033 _score:
```

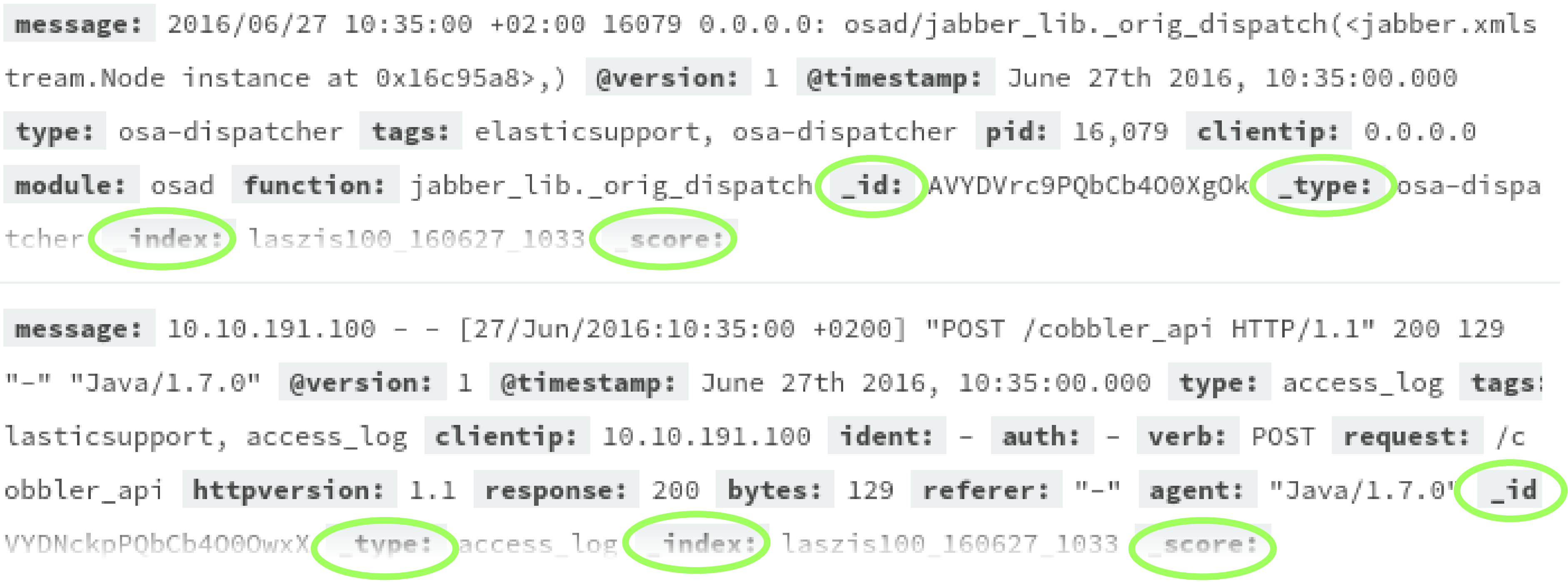
Elasticsearch – Kibana fields



```
message: 2016/06/27 10:35:00 +02:00 16079 0.0.0.0: osad/jabber_lib._orig_dispatch(<jabber.xmls
tream.Node instance at 0x16c95a8>,) @version: 1 @timestamp: June 27th 2016, 10:35:00.000
type: osa-dispatcher tags: elasticsupport, osa-dispatcher pid: 16,079 clientip: 0.0.0.0
module: osad function: jabber_lib._orig_dispatch _id: AVYDVrc9PQbCb4O0XgOk _type: osa-dispa
tcher _index: laszis100_160627_1033 _score:
```

```
message: 10.10.191.100 - - [27/Jun/2016:10:35:00 +0200] "POST /cobbler_api HTTP/1.1" 200 129
"-" "Java/1.7.0" @version: 1 @timestamp: June 27th 2016, 10:35:00.000 type: access_log tags:
lasticsupport, access_log clientip: 10.10.191.100 ident: - auth: - verb: POST request: /c
obbler_api httpversion: 1.1 response: 200 bytes: 129 referer: "-" agent: "Java/1.7.0" _id
VYDNckpPQbCb4O0OwxX _type: access_log _index: laszis100_160627_1033 _score:
```

Elasticsearch – internal fields



```
message: 2016/06/27 10:35:00 +02:00 16079 0.0.0.0: osad/jabber_lib._orig_dispatch(<jabber.xmls
tream.Node instance at 0x16c95a8>,) @version: 1 @timestamp: June 27th 2016, 10:35:00.000
type: osa-dispatcher tags: elasticsupport, osa-dispatcher pid: 16,079 clientip: 0.0.0.0
module: osad function: jabber_lib._orig_dispatch _id: AVYDVrc9PQbCb4O0XgOk _type: osa-dispa
tcher _index: laszis100_160627_1033 _score:
```

```
message: 10.10.191.100 - - [27/Jun/2016:10:35:00 +0200] "POST /cobbler_api HTTP/1.1" 200 129
"-" "Java/1.7.0" @version: 1 @timestamp: June 27th 2016, 10:35:00.000 type: access_log tags:
lasticsupport, access_log clientip: 10.10.191.100 ident: - auth: - verb: POST request: /c
obbler_api httpversion: 1.1 response: 200 bytes: 129 referer: "-" agent: "Java/1.7.0" _id
VYDNckpPQbCb4O0OwxX _type: access_log _index: laszis100_160627_1033 _score:
```

Logstash

Logstash - Overview

- Logserver
- Scalable
- Time-based events
- JRuby

- Input: Text or JSON
- Filter: Parse and manipulate
- Output: Elasticsearch or other

Logstash - input.conf

```
input {
  stdin {}
}
```

Logstash - input.conf

```
input {
  tcp {
    port => 9000
    type => "access_log"
  }
  tcp {
    port => 9001
    type => "error_log"
    tags => ["tag1", "tag2"]
...
```

Logstash Grok Patterns

Logstash - filter.conf

```
# osa-dispatcher
# 2015/06/12 11:39:04 +02:00 14117 0.0.0.0: osad/jabber_lib.main('ERROR',...)
filter {
  if ([type] == "osa-dispatcher") {
    grok {
      match => {
       "message" => "\d\d\d\d\/\d\d\/\d\d\s\d\d:\d\d:\d\d\s[+-]\d\d:\d\d:timestamp ...”
      }
    }
  }
}
```

Logstash - filter.pattern

```
# osa-dispatcher
# 2015/06/12 11:39:04 +02:00 14117 0.0.0.0: osad/jabber_lib.main('ERROR',...)

TIMESTAMP \d\d\d\d\/\d\d\/\d\d\s\d\d:\d\d:\d\d\s[+-]\d\d:\d\d
PID [\d]+
FUNCTION [\w_\.]+
ARGS \([^\)]+\)
```

Logstash - filter.conf

```
filter {
  if ([type] == "osa-dispatcher") {
    grok {
      match => {
       "message" => "%{TIMESTAMP:timestamp} %{PID:pid:int} %{IPV4:clientip}: ...”
      }
    }
  }
}
```

Logstash - output.conf

```
output {
  stdout { codec => rubydebug }
}
```

Logstash - output.conf

```
output {
  elasticsearch {
    hosts => [“localhost:9200”]
  }
}
```

Logstash - Start

```
# ls
filter.conf  input.conf  osa-
dispatcher.pattern  output.conf
rhn_web_api.pattern


# logstash -f ./\*.conf --auto-reload
```

Kibana

Kibana - Overview

- Web based visualization frontend for Elasticsearch
- Time-based events
- Comfortable query interface
- Dashboard management

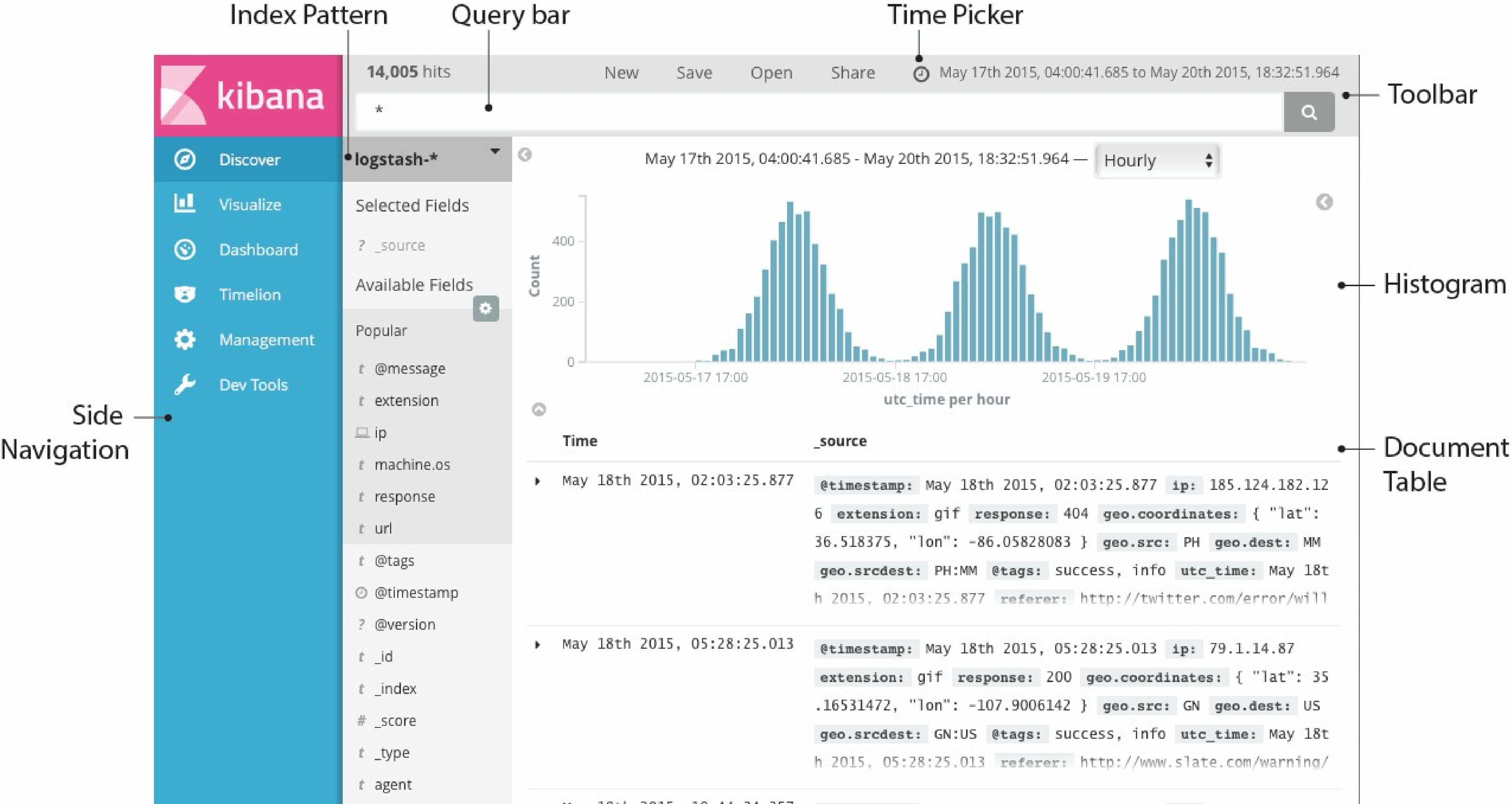
- Settings
- Discover
- Visualize
- Dashboard

Kibana - Settings

- Select index pattern
  - wildcards possbile
- Time based ?
  - Time-field name

Loads mapping

- field names
- field types
- analyzed ?



Index Pattern

Query bar

Time Picker

Toolbar

Histogram

Document Table

Side Navigation

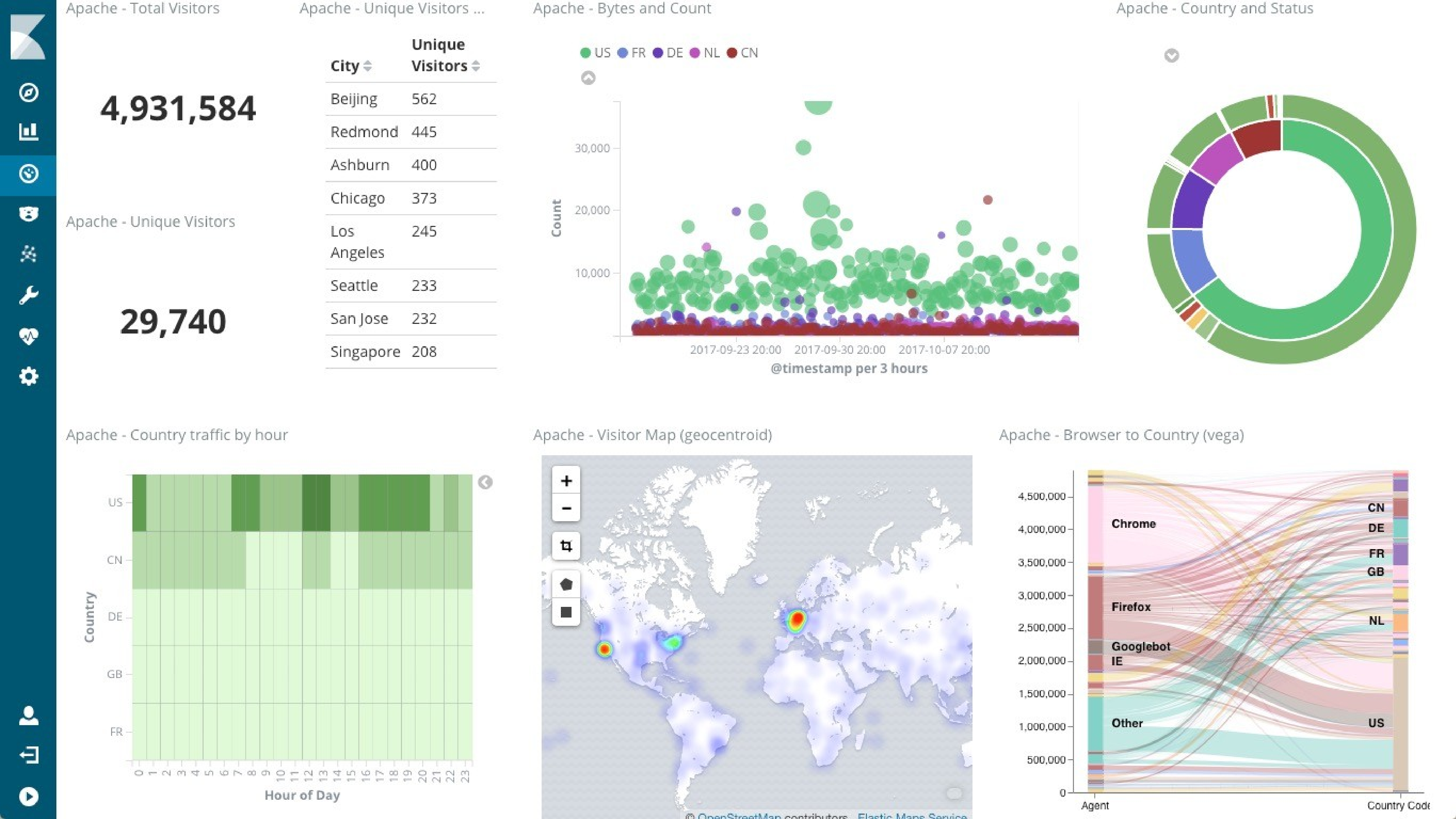
```
May 18th 2015, 02:03:25.877   @timestamp: May 18th 2015, 02:03:25.877 ip: 185.124.182.12
                              6 extension: gif response: 404 geo.coordinates: { "lat":
                              36.518375, "lon": -86.05828083 } geo.src: PH geo.dest: MM
                              geo.srcdest: PH:MM @tags: success, info utc_time: May 18t
                              h 2015, 02:03:25.877 referer: http://twitter.com/error/will

May 18th 2015, 05:28:25.013   @timestamp: May 18th 2015, 05:28:25.013 ip: 79.1.14.87
                              extension: gif response: 200 geo.coordinates: { "lat": 35
                              .16531472, "lon": -107.9006142 } geo.src: GN geo.dest: US
                              geo.srcdest: GN:US @tags: success, info utc_time: May 18t
                              h 2015, 05:28:25.013 referer: http://www.slate.com/warning/
```

Kibana - Discover

- No results found ?
  - Expand your time range
- Explore fields
  - Include/Exclude
- Create query
- Save search
- Visualize !

Kibana - Visualize

- Create new
  - Select visualization type
- New/Saved search
- Graph-specific parameters



Apache - Total Visitors

4,931,584

Apache - Unique Visitors

29,740

Apache - Unique Visitors ...

City	Unique Visitors
Beijing	562
Redmond	445
Ashburn	400
Chicago	373
Los Angeles	245
Seattle	233
San Jose	232
Singapore	208

Apache - Bytes and Count

Apache - Country and Status

Apache - Country traffic by hour

Apache - Visitor Map (geocentroid)

Apache - Browser to Country (vega)

Kibana - Dashboard

- Visualize Elasticsearch fields
- Collection of visualization tiles
- Table, Graph, Map, …
- Can be saved/shared

Help !

Help !

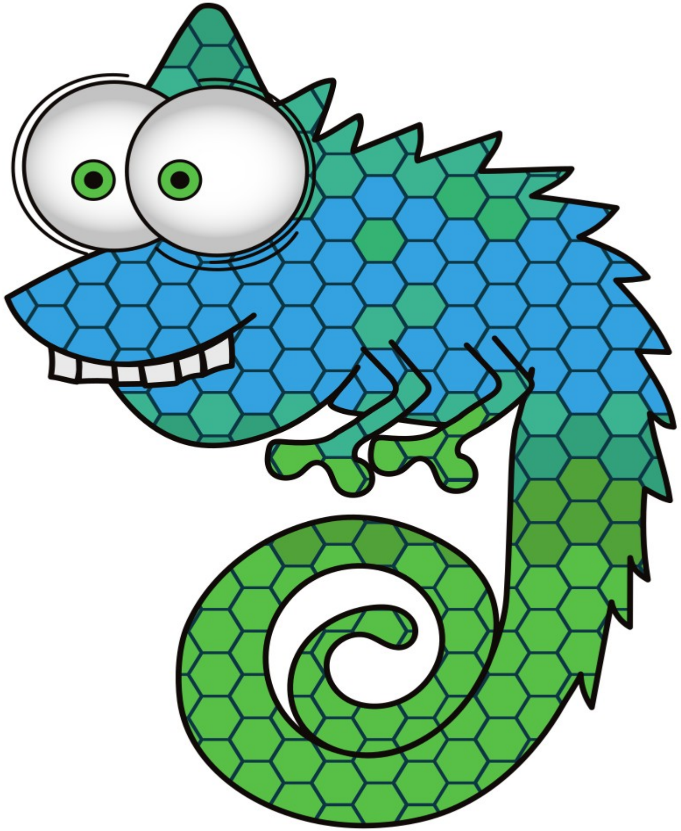
- https://github.com/elastic is **very** active
- Packaging is complex
- Java, JRuby, Go, JavaScript … oh my !

`security:logging` on build.opensuse.org

Other resources

- https://github.com/SUSE/log-analysis
- Dockerfiles
- Salt states
- Grok patterns

Contributions welcome !



Join Us at www.opensuse.org

License

General Disclaimer

This document is not to be construed as a promise by any participating organisation to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. openSUSE makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for openSUSE products remains at the sole discretion of openSUSE. Further, openSUSE reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All openSUSE marks referenced in this presentation are trademarks or registered trademarks of SUSE LLC, in the United States and other countries. All third-party trademarks are the property of their respective owners.

Credits

Template
Richard Brown
rbrown@opensuse.org

Design & Inspiration
openSUSE Design Team
http://opensuse.github.io/branding-guidelines/