Bartłomiej Marcinkowski

ELK story

(Elastic Stack example use)

Intro

Modern ELASTIC STACK:

ELASTICSEARCH + LOGSTASH / BEATS + KIBANA

Elasticsearch

Open-source, broadly-distributable, readily-scalable, enterprise-grade search engine.

- partitioning documents across shards (containers)
- multi-node cluster
- balancing shards across nodes
- replication
- routing across nodes
- API

Logstash

Open source, server-side data processing pipeline. It’s main purpose is to collect, parse and transform logs.

- various inputs/outputs
- lots of plugins (data sources/codecs/filters)
- parse / transform data on the fly

Kibana

Open-source tool used to Explore, Visualize, Discover Data. A Picture is worth a thousand log lines.

- GUI for ElasticSearch data (Discover)
- histograms,line graphs,pie charts (Visualize)
- GEO data
- group data into dashboards

What is it for?

```
2017-06-14 21:46:19 ERROR: COMMAND_FAILED
```

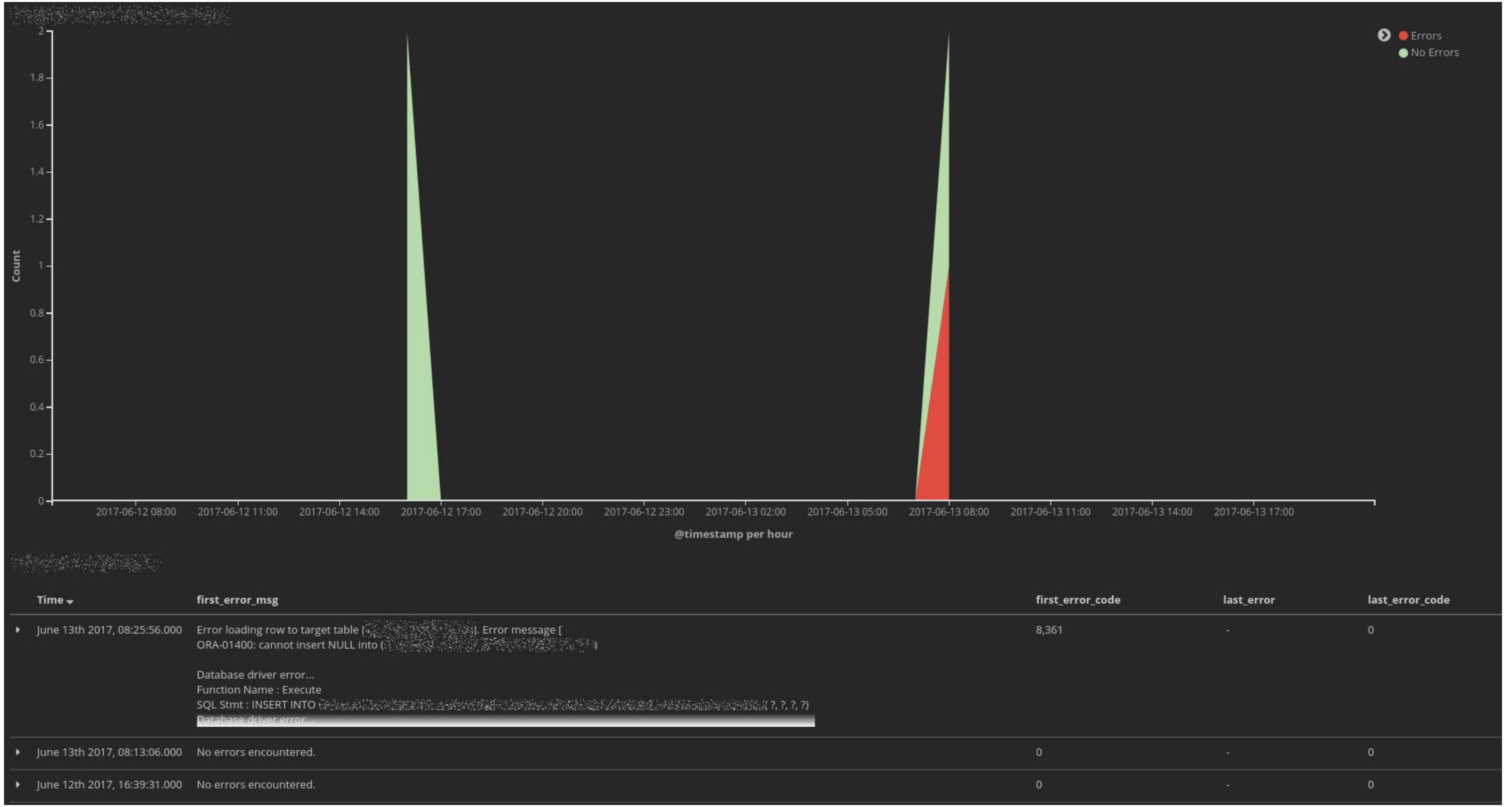
@timestamp	2017-06-14 21:46:19
msg_type	ERROR
@message	COMMAND_FAILED

What is it for?

```
2017-06-14 22:42:14 WARNING: INVALID_SERVICE: cockpit
```

@timestamp	2017-06-14 22:42:14
msg_type	WARNING
@message	INVALID_SERVICE
submessage	cockpit

What is it for?



[redacted]

Time ▾	first_error_msg	first_error_code	last_error	last_error_code
June 13th 2017, 08:25:56.000	Error loading row to target table [[redacted]]. Error message [ORA-01400: cannot insert NULL into ([redacted]) Database driver error... Function Name : Execute SQL Stmt : INSERT INTO [redacted](?, ?, ?, ?) Database driver error...	8,361	-	0
June 13th 2017, 08:13:06.000	No errors encountered.	0	-	0
June 12th 2017, 16:39:31.000	No errors encountered.	0	-	0

Logstash - Input plugins (shipper)

- file

```
input {
  file {
    add_field => { ”application” => "YOUR_APP" }
    type => "LOG_TYPE"
    path => "/full/path/to/logfile(s)"
  }
}
```

^ note: codec is plain (default)

Logstash - Input plugins (shipper)

- tcp

```
input {
  tcp {
    add_field => { “application” => “YOUR_APP" }
    port => 4000
    codec => "json"
  }
}
```

Logstash - Input plugins (shipper)

- jdbc

```
input {
  jdbc {
    add_field => { "application" => "YOUR_APP"  }
    jdbc_driver_library => "/path/to/ojdbc7.jar"
    jdbc_driver_class => "Java::oracle.jdbc.driver.OracleDriver"
    jdbc_connection_string => “jdbc:oracle:thin:@host:port/service"
    jdbc_user => "user"
    jdbc_password => "pass"
    record_last_run => true
    last_run_metadata_path => "/path/to/metdata/file"
    schedule => "* * * * *"
    use_column_value => true
    tracking_column => log_date
    statement => "select * from (select * from SOMEVIEW order by LOG_ID ASC) where
LOG_DATE > :sql_last_value"
  }
```

Logstash - Input plugins (shipper)

- jdbc (timestamp fix)

```
filter {
        date {
              match => ["some_timestamp_col”,"ISO8601"]
              target => "@timestamp"
         }
}
```

Logstash - Input plugins (processor)

- redis

```
redis {
    host => "some_fqdn1"
    data_type => "list"
    key => "logstash"
    codec => json
    threads => 3
    add_field => { "redis_host" => "myhostname1" }
  }
[...]
```

Logstash - filter / grok

```
filter {
  if [type] == "syslog" {
    grok {
      match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_hostname} %{DATA:syslog_program}(?:\[%{POSINT:syslog_pid}\])?: %{GREEDYDATA:syslog_message}" }
      add_field => [ "received_at", "%{@timestamp}" ]
      add_field => [ "received_from", "%{host}" ]
    }
}
```

Logstash - filter / mutate

```
filter {
 if !("" in [application] and "" != [application]) {
    mutate {
      add_field => {
        logstash_error => "#missing 'application' field"
      }
    }
  }
}
```

Logstash - output / elasticsearch

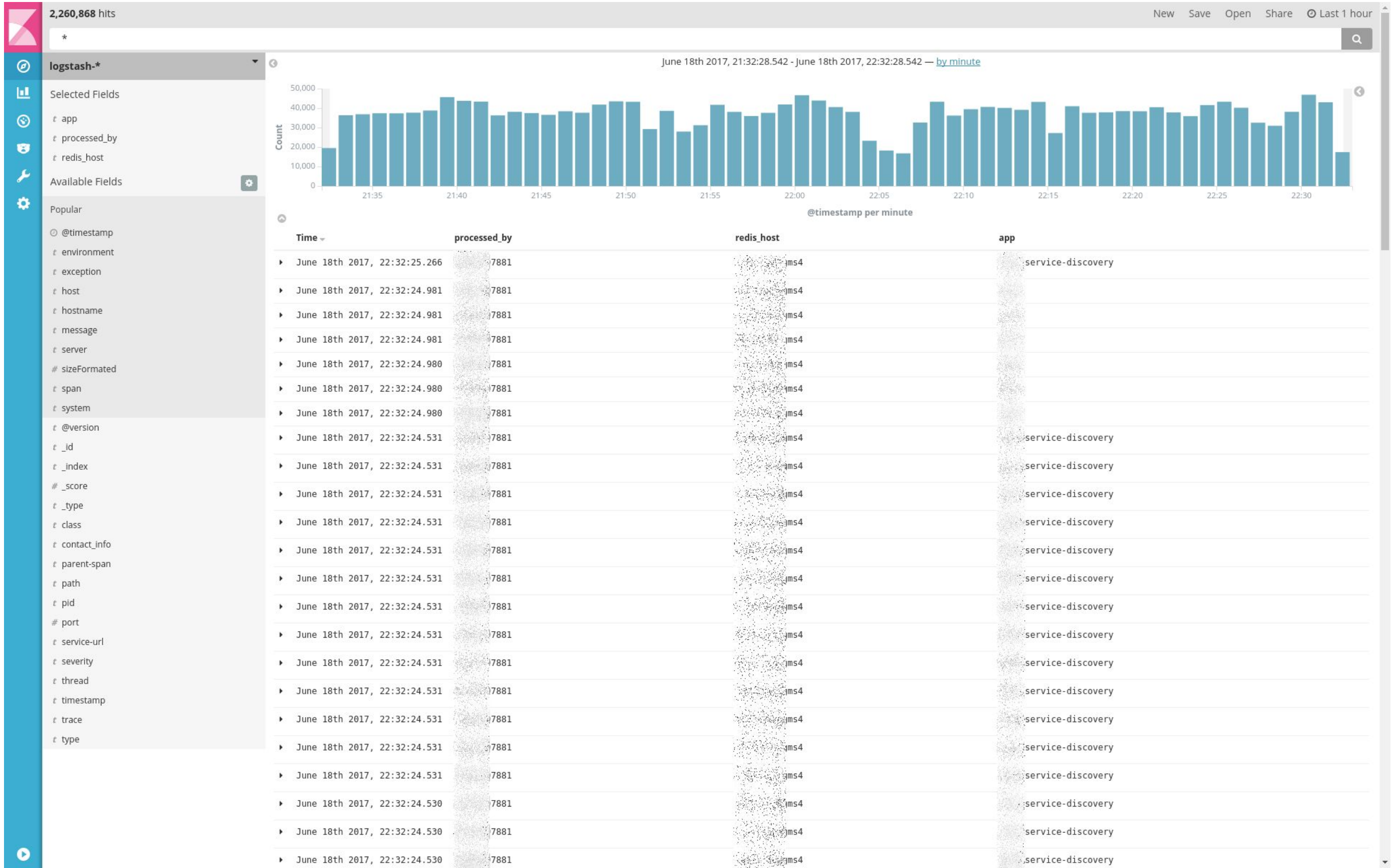
```
output {
  if [logstash_error] or ("_grokparsefailure" in [tags]) {
    elasticsearch {
      hosts => ["host1",”host2”]
      index => "logstasherror-%{+YYYY.MM.dd}"
      codec => "json"
    }
  } else {
    elasticsearch {
      hosts => ["host1",”host2”]
      codec => "json"
    }
  }
}
```

* Note:default index is **logstash-%{+YYYY.MM.dd}**

Logstash - output / email

```
output {
  if [logtype] == "Error" and [system]=="VeryImportant" {
        email {
                  address => "mailhost.fqdn"
                  body => "some text with %{[varables]}"
                  subject => "%{[logtype]} - Scarry message"
                  to => "admin@omg.site"
                  from => "elk@omg.site"
         }
    }
}
```

Kibana - Discover



2,260,868 hits

*

logstash-*

June 18th 2017, 21:32:28.542 - June 18th 2017, 22:32:28.542 — by minute

Selected Fields

- app
- processed_by
- redis_host

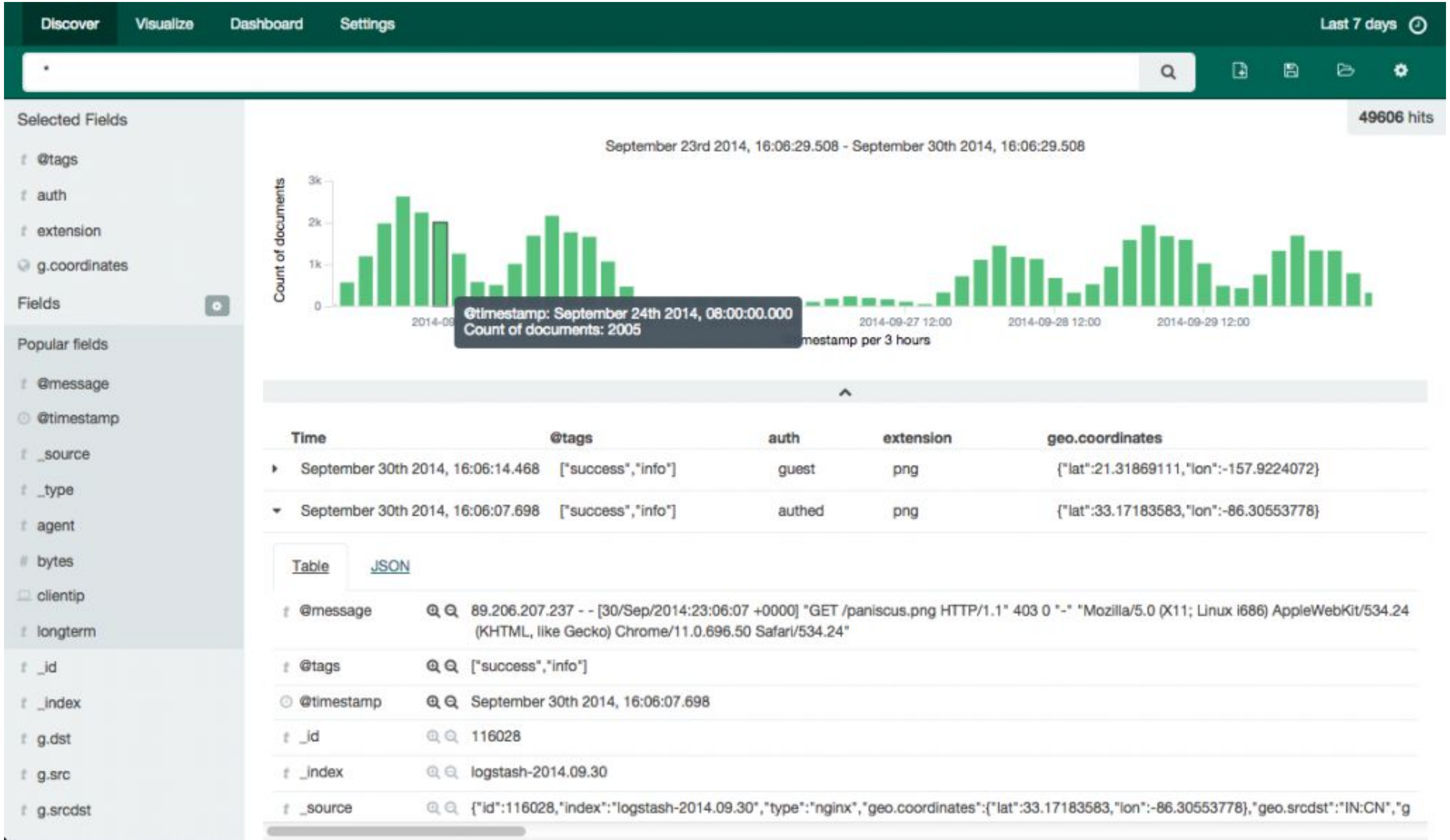
Available Fields

Popular

- @timestamp
- environment
- exception
- host
- hostname
- message
- server
- sizeFormated
- span
- system
- @version
- _id
- _index
- _score
- _type
- class
- contact_info
- parent-span
- path
- pid
- port
- service-url
- severity
- thread
- timestamp
- trace
- type

Time	processed_by	redis_host	app
June 18th 2017, 22:32:25.266	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.981	[redacted]7881	[redacted]ms4	[redacted]
June 18th 2017, 22:32:24.981	[redacted]7881	[redacted]ms4	[redacted]
June 18th 2017, 22:32:24.981	[redacted]7881	[redacted]ms4	[redacted]
June 18th 2017, 22:32:24.980	[redacted]7881	[redacted]ms4	[redacted]
June 18th 2017, 22:32:24.980	[redacted]7881	[redacted]ms4	[redacted]
June 18th 2017, 22:32:24.980	[redacted]7881	[redacted]ms4	[redacted]
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.531	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.530	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.530	[redacted]7881	[redacted]ms4	[redacted]service-discovery
June 18th 2017, 22:32:24.530	[redacted]7881	[redacted]ms4	[redacted]service-discovery

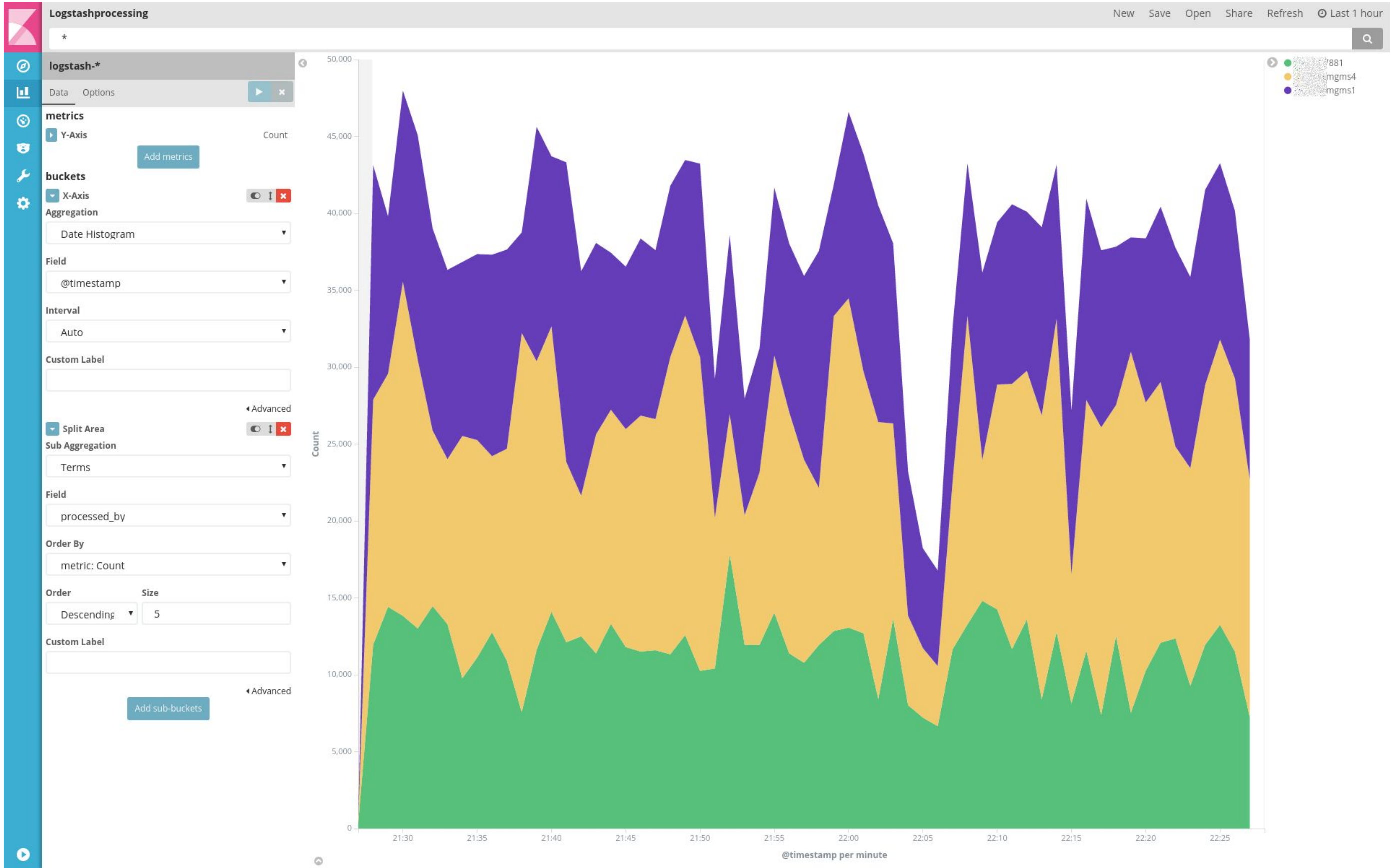
Kibana - Discover



Time	@tags	auth	extension	geo.coordinates
September 30th 2014, 16:06:14.468	["success","info"]	guest	png	{"lat":21.31869111,"lon":-157.9224072}
September 30th 2014, 16:06:07.698	["success","info"]	authed	png	{"lat":33.17183583,"lon":-86.30553778}

@message	89.206.207.237 - - [30/Sep/2014:23:06:07 +0000] "GET /paniscus.png HTTP/1.1" 403 0 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24"
@tags	["success","info"]
@timestamp	September 30th 2014, 16:06:07.698
_id	116028
_index	logstash-2014.09.30
_source	{"id":116028,"index":"logstash-2014.09.30","type":"nginx","geo.coordinates":{"lat":33.17183583,"lon":-86.30553778},"geo.srcdst":"IN:CN","g

Kibana - Visualize



Logstashprocessing

New Save Open Share Refresh Last 1 hour

*

logstash-*

Data Options

metrics

Y-Axis Count

Add metrics

buckets

X-Axis

Aggregation: Date Histogram

Field: @timestamp

Interval: Auto

Custom Label:

Advanced

Split Area

Sub Aggregation: Terms

Field: processed_by

Order By: metric: Count

Order: Descending

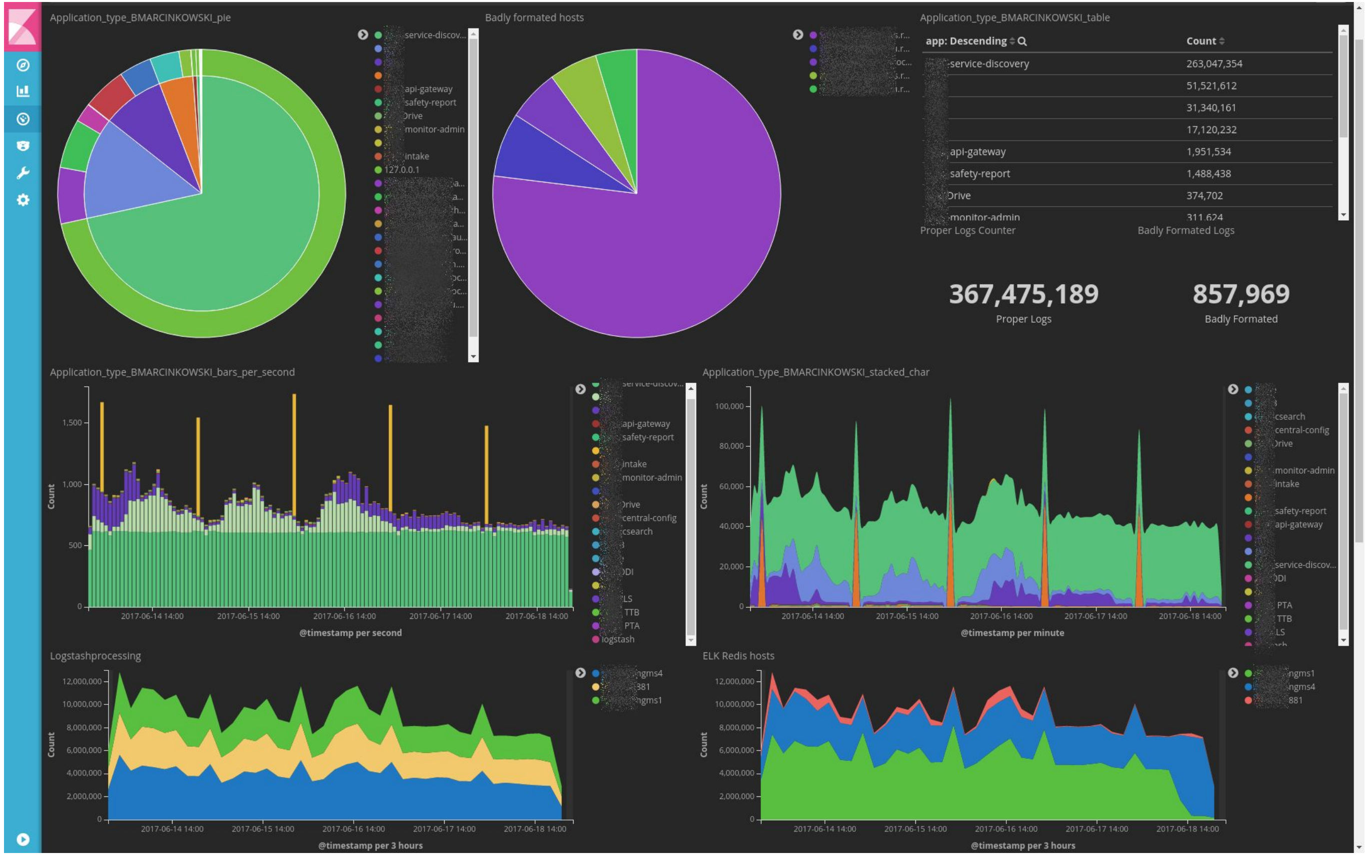
Size: 5

Custom Label:

Advanced

Add sub-buckets

Kibana - Dashboard



Application_type_BMARCINKOWSKI_table

app: Descending	Count
[redacted]-service-discovery	263,047,354
[redacted]	51,521,612
[redacted]	31,340,161
[redacted]	17,120,232
[redacted] api-gateway	1,951,534
[redacted] safety-report	1,488,438
[redacted]Drive	374,702
[redacted]-monitor-admin	311,624

Proper Logs Counter

367,475,189

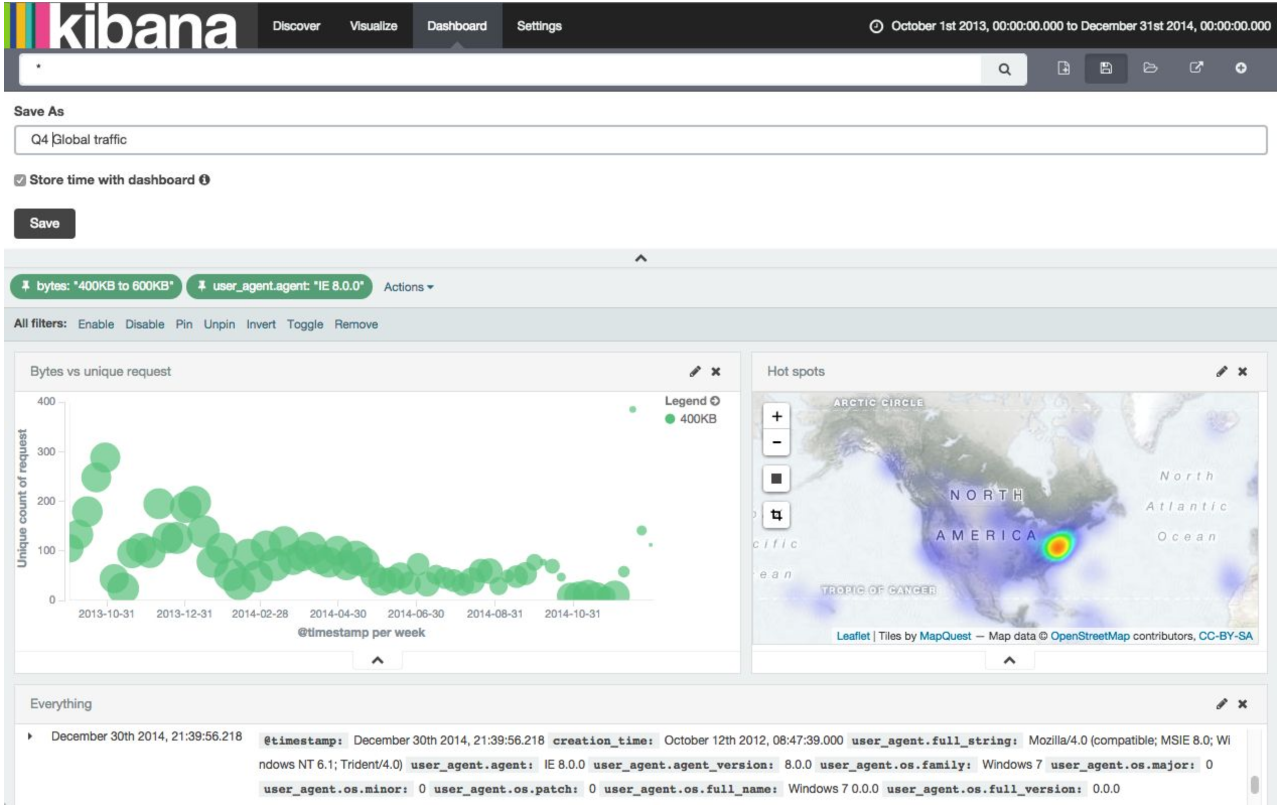
Proper Logs

Badly Formated Logs

857,969

Badly Formated

Kibana - Dashboard



October 1st 2013, 00:00:00.000 to December 31st 2014, 00:00:00.000

*

Save As

Q4 Global traffic

☑ Store time with dashboard

Save

bytes: "400KB to 600KB" user_agent.agent: "IE 8.0.0" Actions

All filters: Enable Disable Pin Unpin Invert Toggle Remove

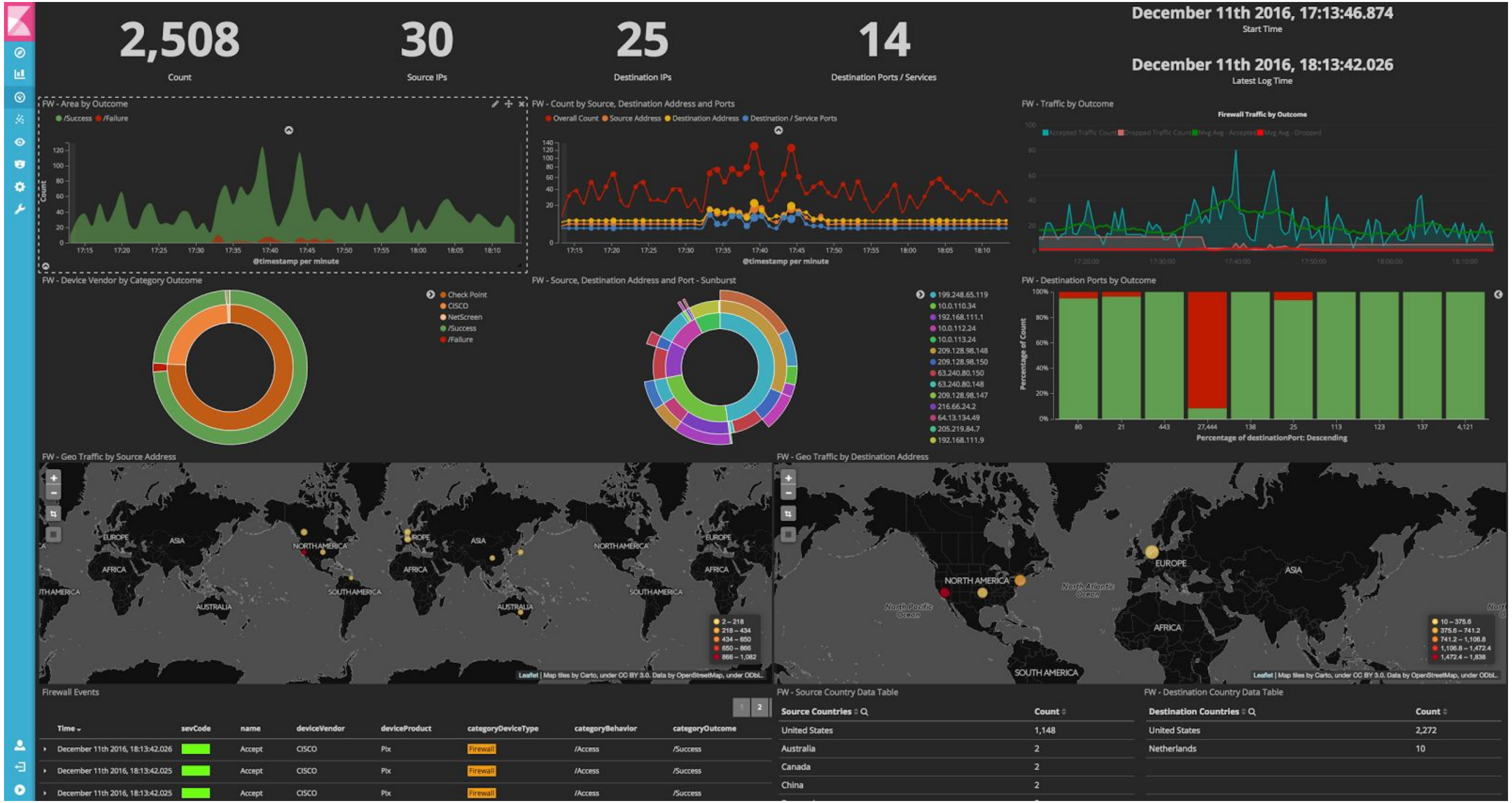
Bytes vs unique request

Hot spots

Everything

December 30th 2014, 21:39:56.218 @timestamp: December 30th 2014, 21:39:56.218 creation_time: October 12th 2012, 08:47:39.000 user_agent.full_string: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0) user_agent.agent: IE 8.0.0 user_agent.agent_version: 8.0.0 user_agent.os.family: Windows 7 user_agent.os.major: 0 user_agent.os.minor: 0 user_agent.os.patch: 0 user_agent.os.full_name: Windows 7 0.0.0 user_agent.os.full_version: 0.0.0

Kibana - Dashboard



2,508
Count

30
Source IPs

25
Destination IPs

14
Destination Ports / Services

December 11th 2016, 17:13:46.874
Start Time

December 11th 2016, 18:13:42.026
Latest Log Time

Firewall Events

Time	sevCode	name	deviceVendor	deviceProduct	categoryDeviceType	categoryBehavior	categoryOutcome
December 11th 2016, 18:13:42.026	🟩	Accept	CISCO	Pix	Firewall	/Access	/Success
December 11th 2016, 18:13:42.025	🟩	Accept	CISCO	Pix	Firewall	/Access	/Success
December 11th 2016, 18:13:42.025	🟩	Accept	CISCO	Pix	Firewall	/Access	/Success

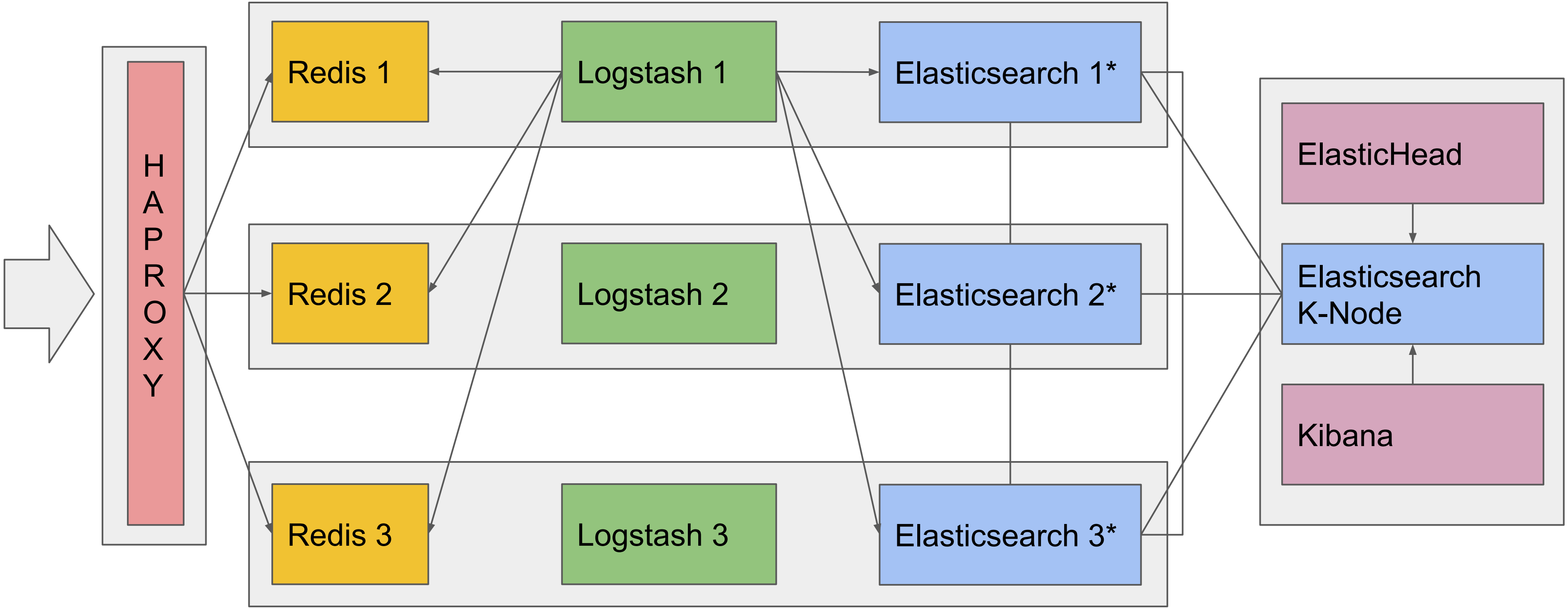
FW - Source Country Data Table

Source Countries	Count
United States	1,148
Australia	2
Canada	2
China	2

FW - Destination Country Data Table

Destination Countries	Count
United States	2,272
Netherlands	10

Elastic Stack example - DEV environment



* Data nodes: 8vCPU, 32GB RAM, 320GB storage

Tips and Tricks - Elasticsearch config

- Long and big queries: queue_size
- Seperate clusters for applications / message types (Tribe node)
- Define your shards need (speed vs safety)

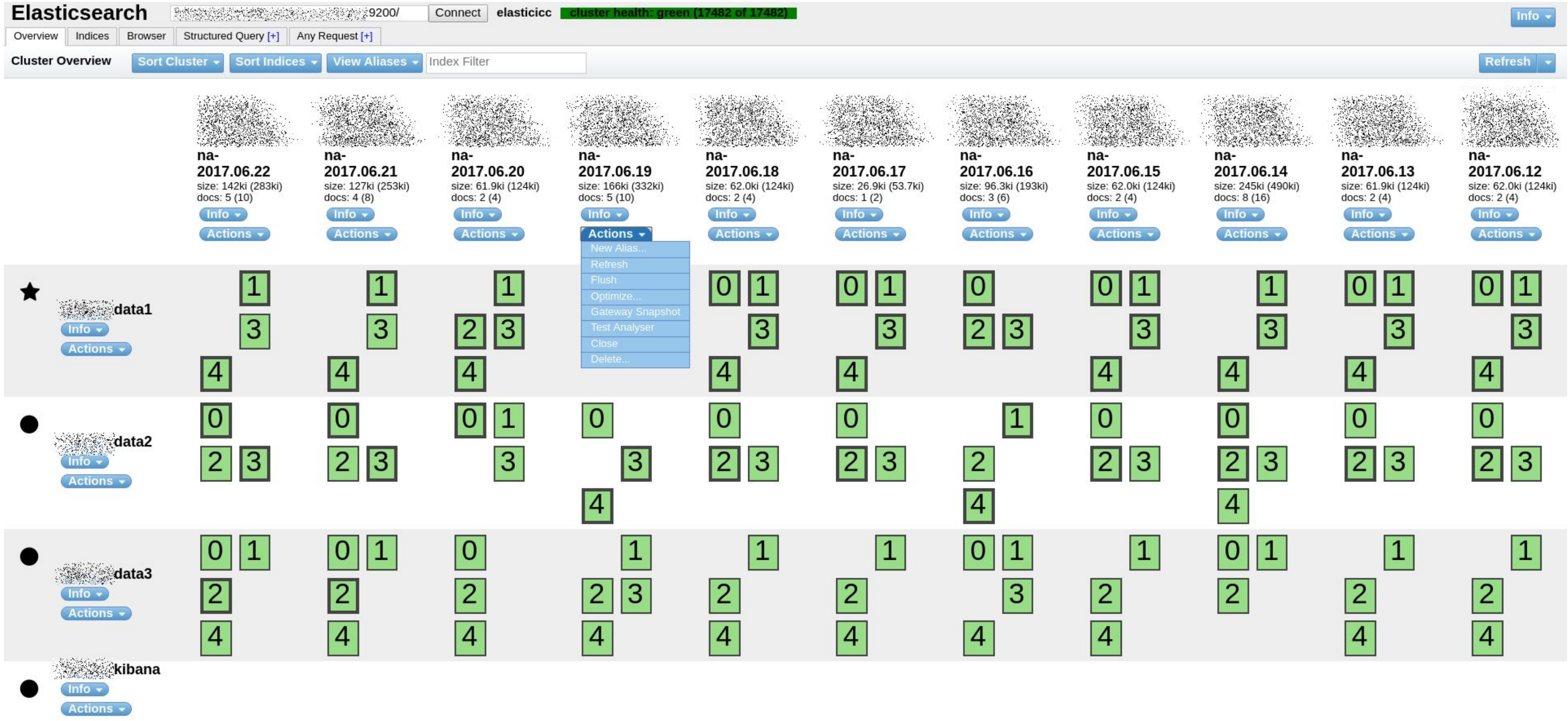
Tips and Tricks - Logstash

- Multi outputs (system logs / application logs)
- Separate Index for applications
- Text output for debug purposes
- Works as shipper
- Localhost tcp access for applications
- Hub for databases logs

Tips and Tricks - security

- Apache / NGINX as proxy (Kibana frontend password)
- Enable SSL
- Firewall Elasticsearch cluster input
- Logstash “keys” - drop “unsigned” messages

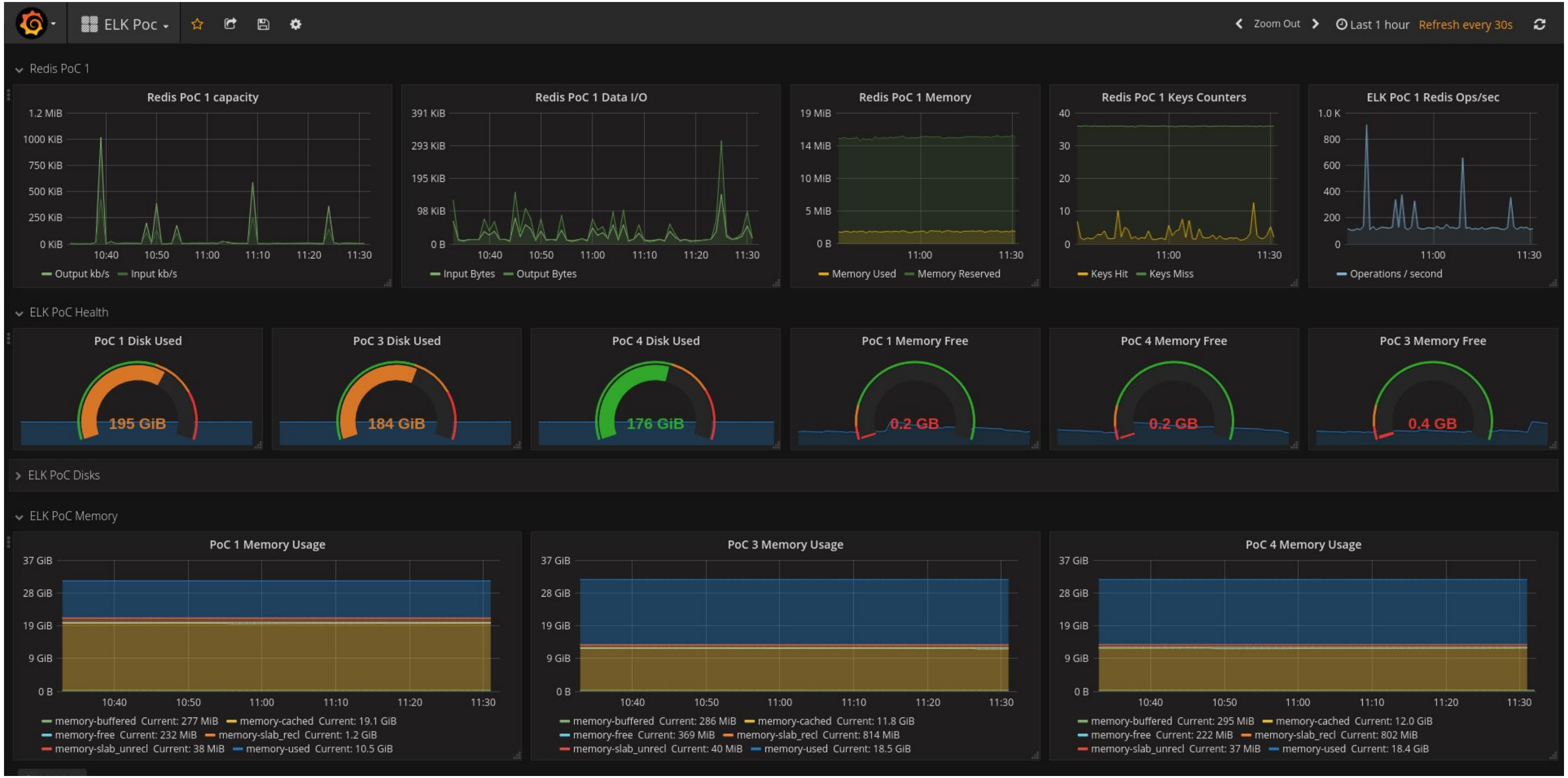
Tips and Tricks - ElasticHead



[redacted]9200/ elasticicc cluster health: green (17482 of 17482)

	[redacted]na-2017.06.22 size: 142ki (283ki) docs: 5 (10)	[redacted]na-2017.06.21 size: 127ki (253ki) docs: 4 (8)	[redacted]na-2017.06.20 size: 61.9ki (124ki) docs: 2 (4)	[redacted]na-2017.06.19 size: 166ki (332ki) docs: 5 (10)	[redacted]na-2017.06.18 size: 62.0ki (124ki) docs: 2 (4)	[redacted]na-2017.06.17 size: 26.9ki (53.7ki) docs: 1 (2)	[redacted]na-2017.06.16 size: 96.3ki (193ki) docs: 3 (6)	[redacted]na-2017.06.15 size: 62.0ki (124ki) docs: 2 (4)	[redacted]na-2017.06.14 size: 245ki (490ki) docs: 8 (16)	[redacted]na-2017.06.13 size: 61.9ki (124ki) docs: 2 (4)	[redacted]na-2017.06.12 size: 62.0ki (124ki) docs: 2 (4)
★ [redacted]data1	1 3 4	1 3 4	1 2 3 4		0 1 3 4	0 1 3 4	0 2 3	0 1 3 4	1 3 4	0 1 3 4	0 1 3 4
● [redacted]data2	0 2 3	0 2 3	0 1 3	0 3 4	0 2 3	0 2 3	1 2 4	0 2 3	0 2 3 4	0 2 3	0 2 3
● [redacted]data3	0 1 2 4	0 1 2 4	0 2 4	1 2 3 4	1 2 4	1 2 4	0 1 3 4	1 2 4	0 1 2	1 2 4	1 2 4
● [redacted]kibana											

Tips and Tricks - monitoring



X-Pack

- Shield
- Alerting
- Monitoring
- Machine Learning
- Graph
- Reporting

Links

- https://www.elastic.co/
- http://grokconstructor.appspot.com/do/match
- Kibana 5 Introduction: https://www.youtube.com/watch?v=mMhnGjp8oOI
- Twitter analysis with Elastic Stack: https://www.youtube.com/watch?v=YVPpDt_pEME

?