Security, Alerting, Monitoring and More with the Elastic Stack

Monitoring

All the Things

Tanguy Leroux @tlrx

Tim Sullivan @timsullivanyeah

Logging and monitoring are at the heart of making sure your solutions are up and running to your expectations.

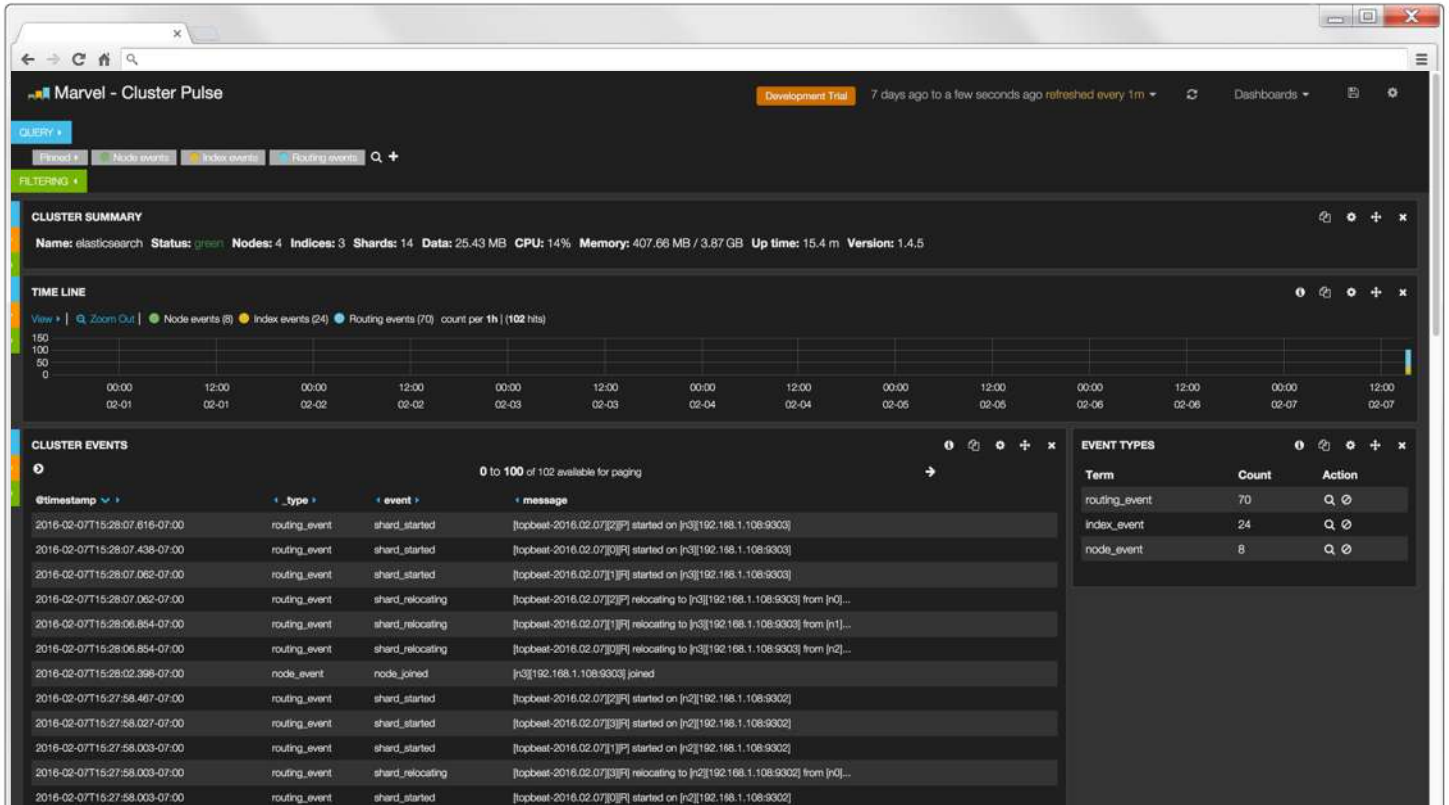
- David Messina

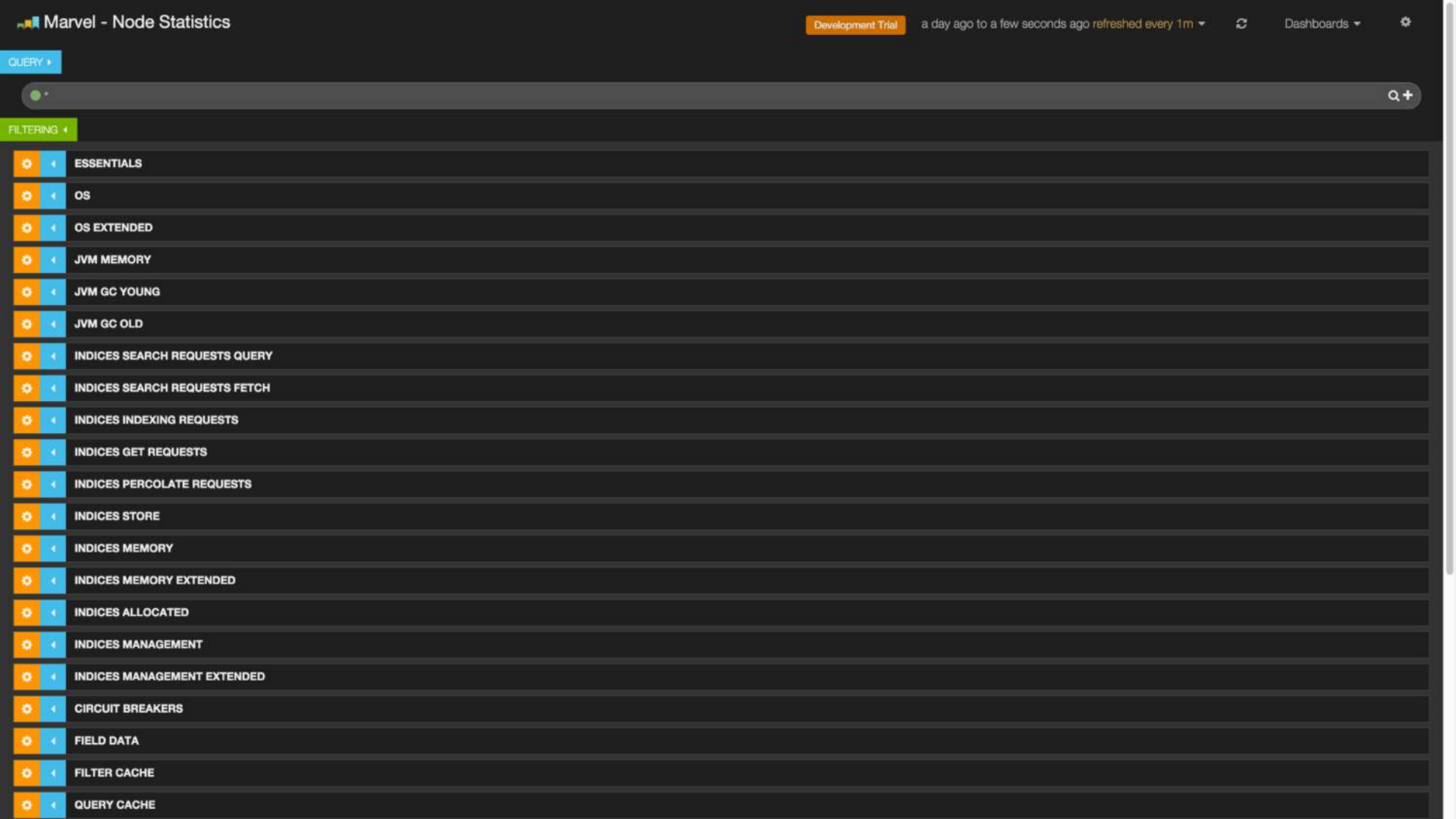
VP, Enterprise Marketing at Docker’s VP of Enterprise Marketing

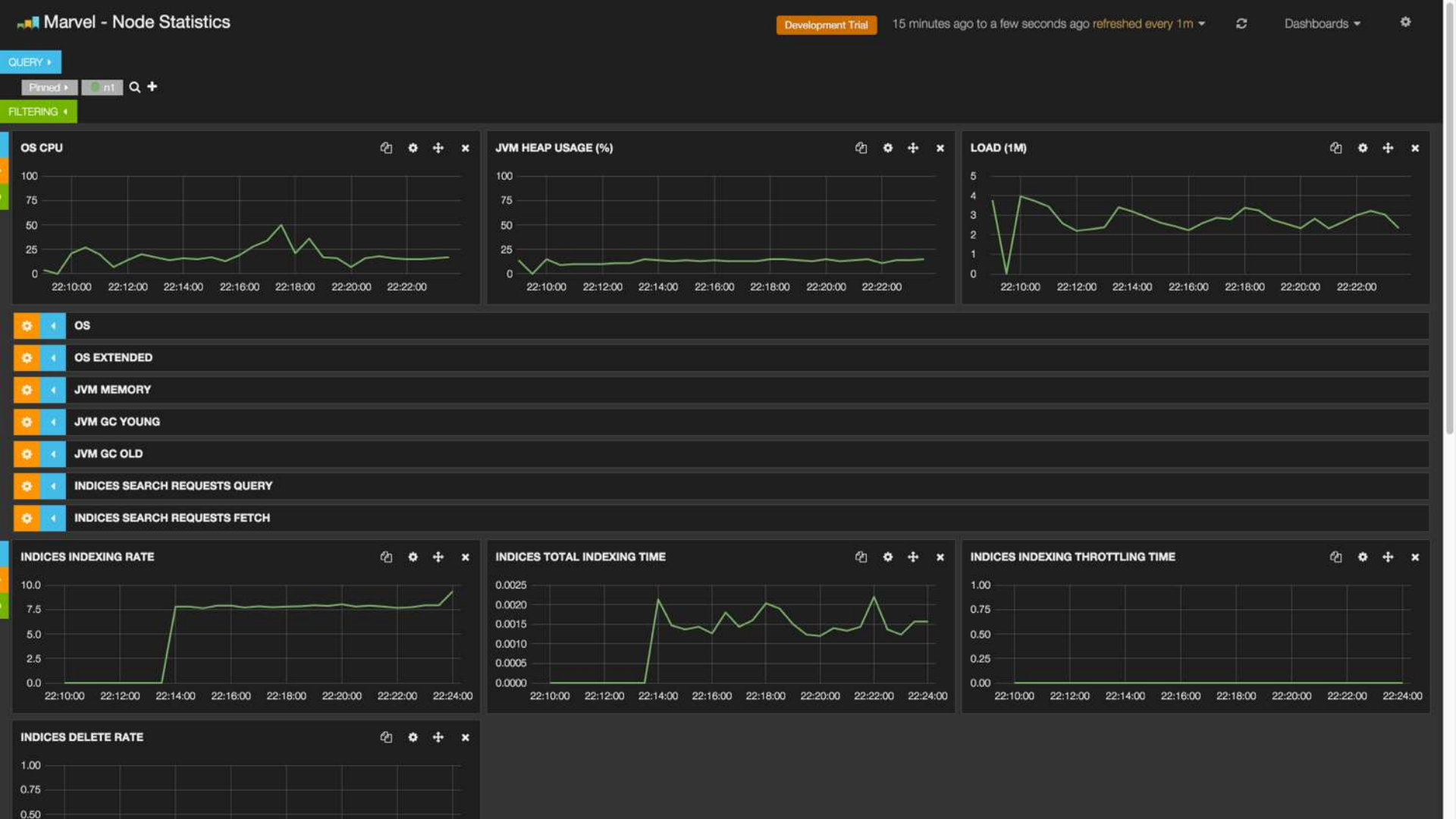
And then Marvel 1.0 Arrived

First commercial plugin of Elastic!

Cluster Pulse



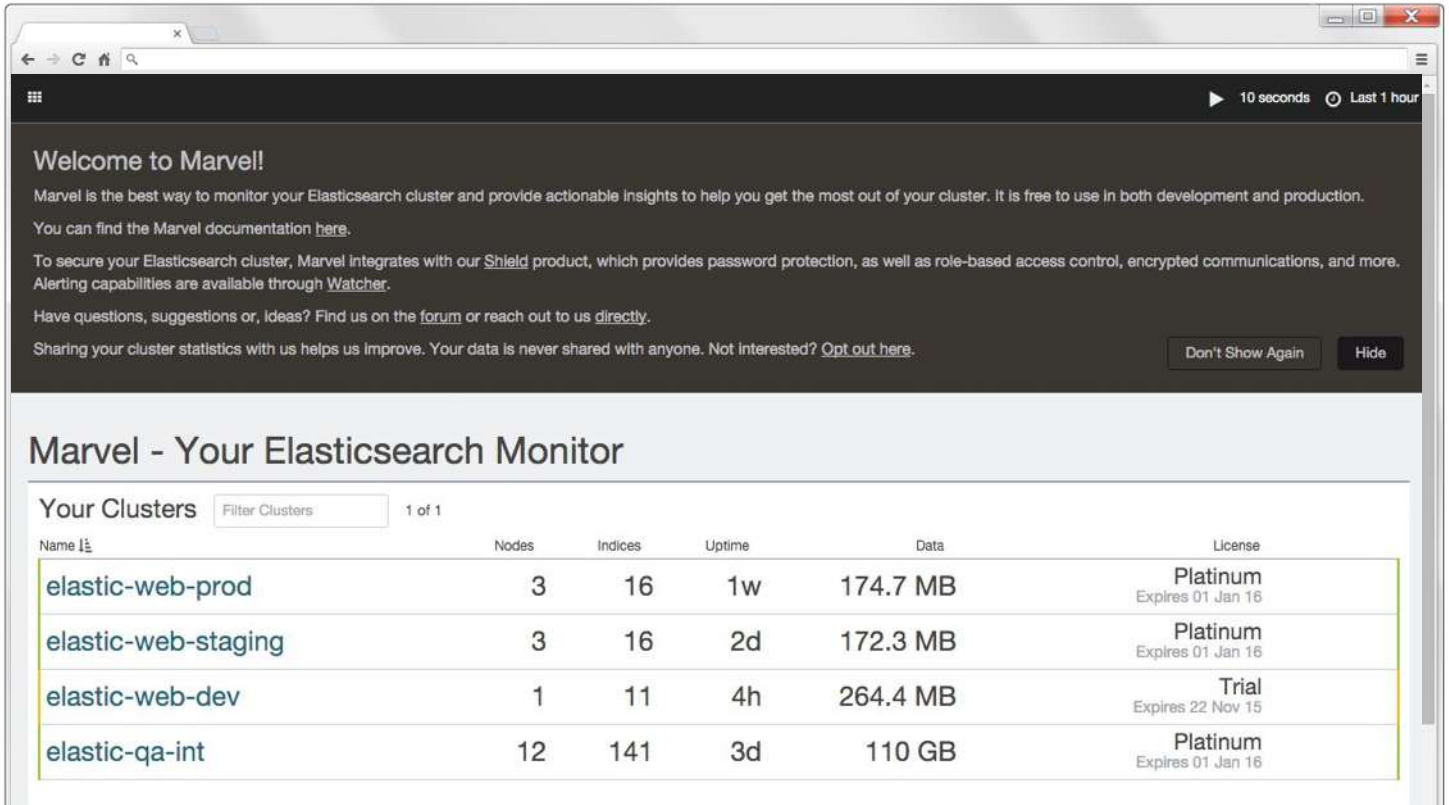

Marvel - Node Statistics
Development Trial
a day ago to a few seconds ago refreshed every 1m
Dashboards
QUERY
*
FILTERING
ESSENTIALS
OS
OS EXTENDED
JVM MEMORY
JVM GC YOUNG
JVM GC OLD
INDICES SEARCH REQUESTS QUERY
INDICES SEARCH REQUESTS FETCH
INDICES INDEXING REQUESTS
INDICES GET REQUESTS
INDICES PERCOLATE REQUESTS
INDICES STORE
INDICES MEMORY
INDICES MEMORY EXTENDED
INDICES ALLOCATED
INDICES MANAGEMENT
INDICES MANAGEMENT EXTENDED
CIRCUIT BREAKERS
FIELD DATA
FILTER CACHE
QUERY CACHE


Marvel - Node Statistics
Development Trial
15 minutes ago to a few seconds ago refreshed every 1m
Dashboards
QUERY
Pinned
n1
FILTERING
OS CPU
100
75
50
25
0
22:10:00
22:12:00
22:14:00
22:16:00
22:18:00
22:20:00
22:22:00
JVM HEAP USAGE (%)
100
75
50
25
0
22:10:00
22:12:00
22:14:00
22:16:00
22:18:00
22:20:00
22:22:00
LOAD (1M)
5
4
3
2
1
0
22:10:00
22:12:00
22:14:00
22:16:00
22:18:00
22:20:00
22:22:00
OS
OS EXTENDED
JVM MEMORY
JVM GC YOUNG
JVM GC OLD
INDICES SEARCH REQUESTS QUERY
INDICES SEARCH REQUESTS FETCH
INDICES INDEXING RATE
10.0
7.5
5.0
2.5
0.0
22:10:00
22:12:00
22:14:00
22:16:00
22:18:00
22:20:00
22:22:00
22:24:00
INDICES TOTAL INDEXING TIME
0.0025
0.0020
0.0015
0.0010
0.0005
0.0000
22:10:00
22:12:00
22:14:00
22:16:00
22:18:00
22:20:00
22:22:00
22:24:00
INDICES INDEXING THROTTLING TIME
1.00
0.75
0.50
0.25
0.00
22:10:00
22:12:00
22:14:00
22:16:00
22:18:00
22:20:00
22:22:00
22:24:00
INDICES DELETE RATE
1.00
0.75
0.50

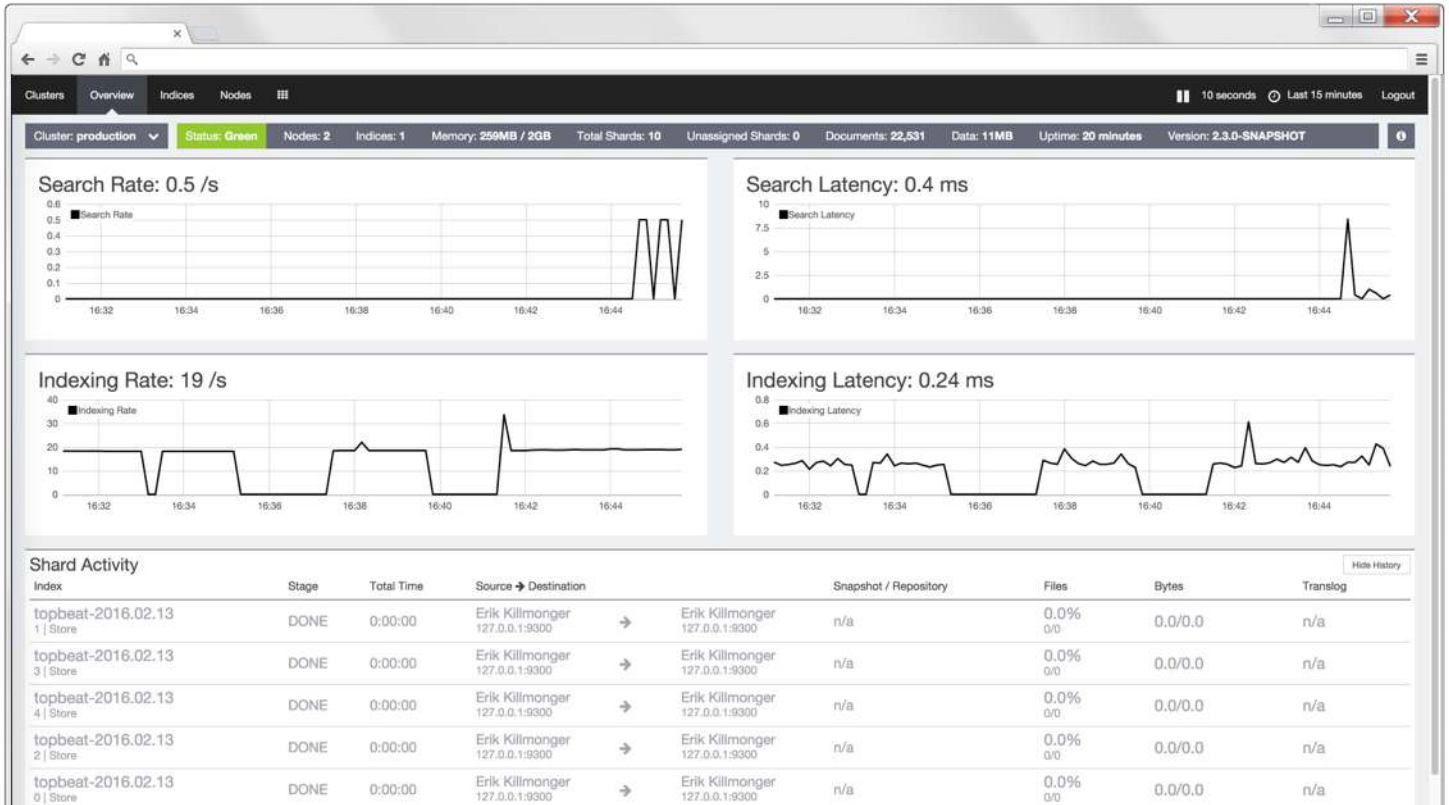
Monitoring for Elasticsearch 2.x

Yes, we like to rename things :)

Multi-Cluster Support



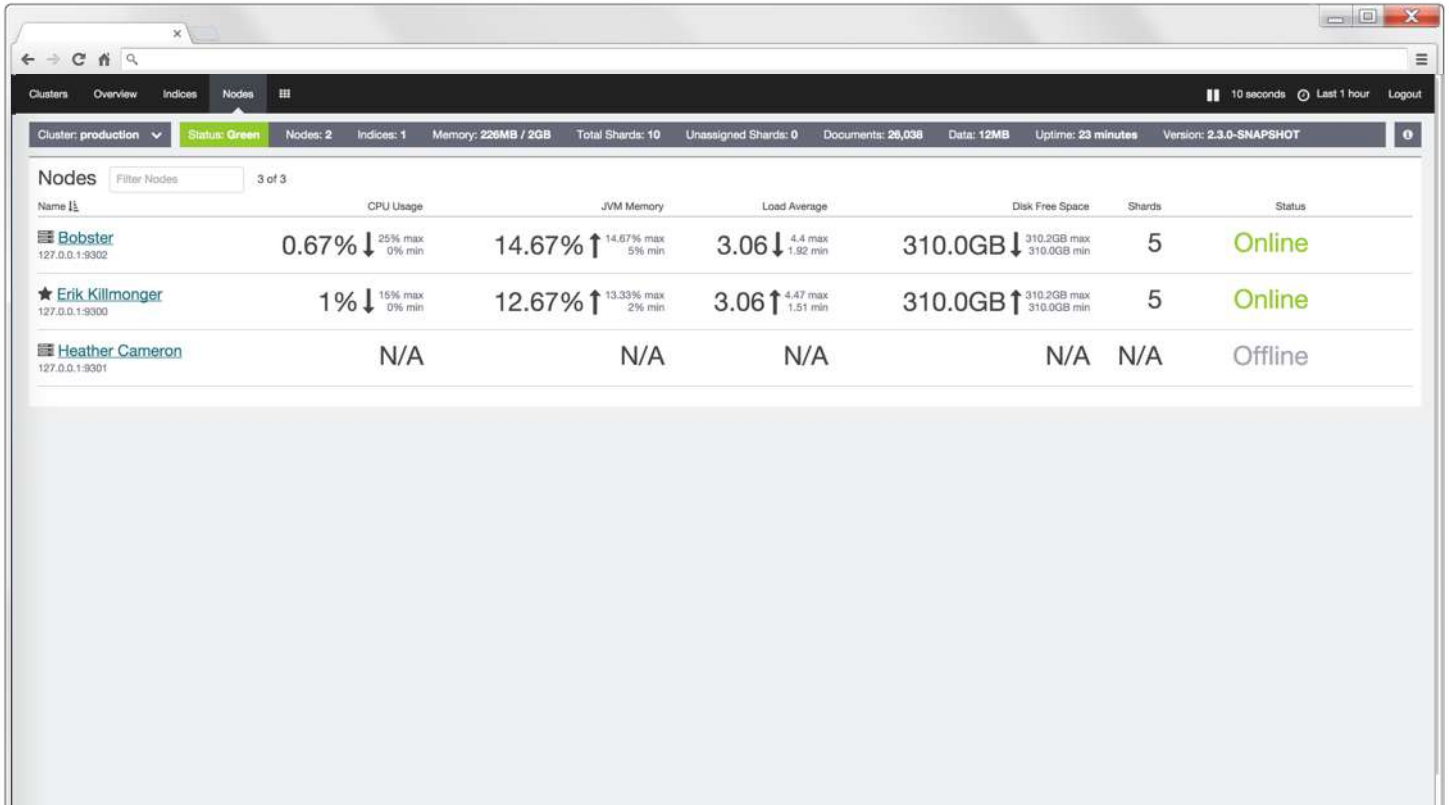
Cluster Overview at a Glance



elastic on

elastic

Node Listing



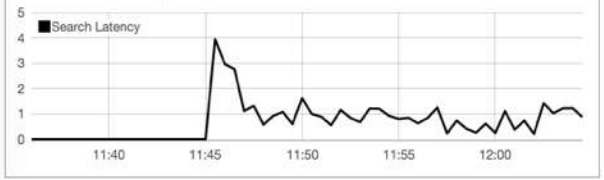
Clusters | Overview | Indices | Nodes | 10 seconds | Last 30 minutes

Cluster: **elasticsearch** | Status: **Green** | Nodes: **2** | Indices: **6** | Memory: **171MB / 2GB** | Total Shards: **20** | Unassigned Shards: **0** | Documents: **25,707** | Data: **12MB** | Uptime: **20 minutes** | Version: **2.3.0-SNAPSHOT**

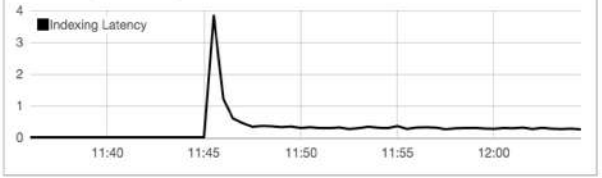
★ Azazel

127.0.0.1:9300 Documents: 25.7k Data: 6.3MB Free Disk Space: 310.2GB Indices: 6 Total Shards: 10 Type: Master Node Status: Online

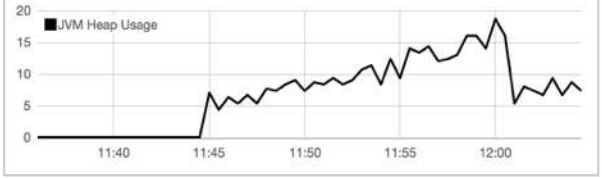
Search Latency: 0.88 ms



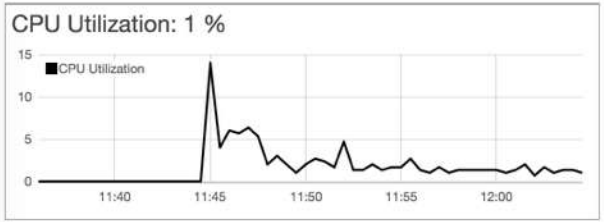
Indexing Latency: 0.25 ms



JVM Heap Usage: 7.33 %



CPU Utilization: 1 %



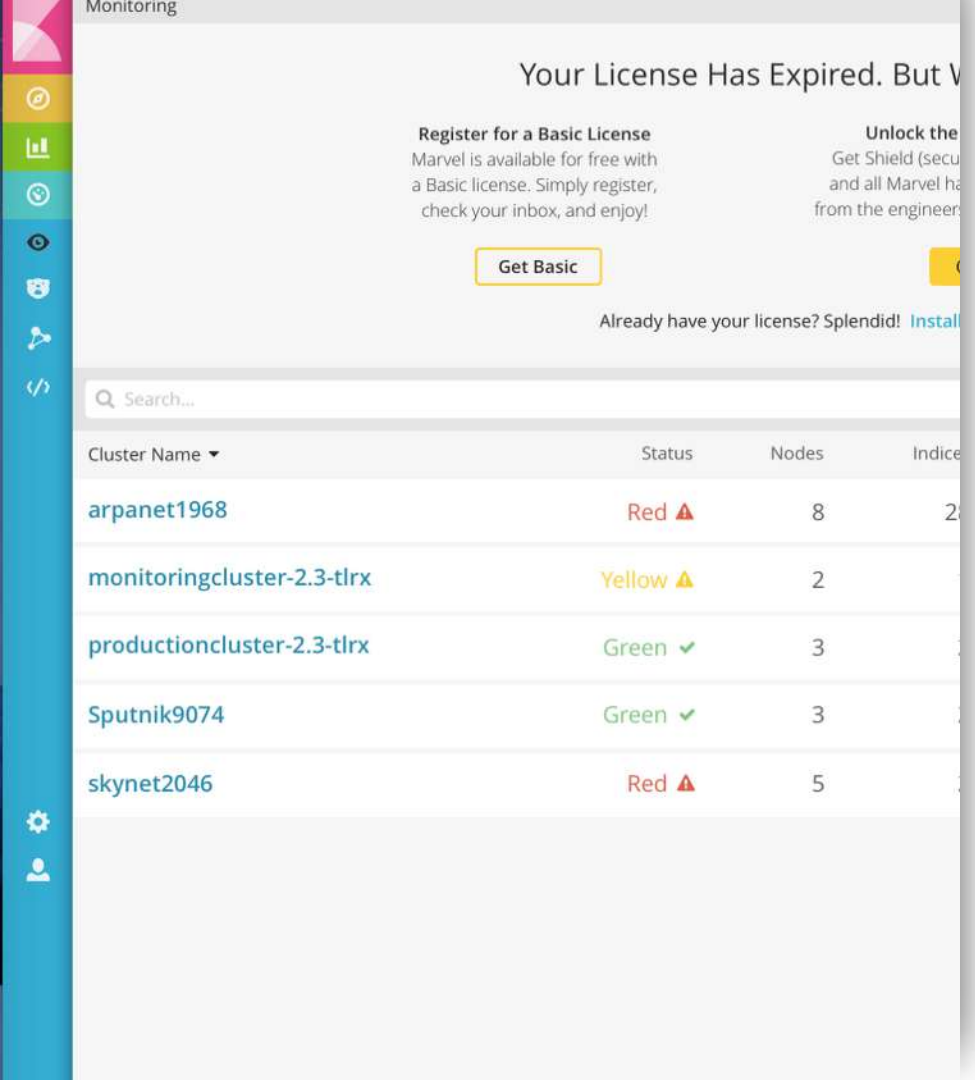
System Load Average: 1.82

Segment Count: 40.33

Shard Legend Primary Replica Relocating Initializing

Indices

.kibana 0 | .marvel-es-1-2016.02.11 0 | .marvel-es-1-2016.02.12 0 | .marvel-es-1-2016.02.13 0 | .marvel-es-data-1 0 | topbeat-2016.02.13 0 1 2 3 4



Kibana 5

New design

Issues

Cross-Stack Monitoring

elastic

elastic on

Monitoring Elasticsearch

Spotlight Theater @ 4:40pm

Security

Don’t Hack Me Bro!

Jay Modi @jaymode2001

Security for the Elastic Stack

Simply Secure Elasticsearch

- Username/password protection

Advanced Security When Needed

- LDAP, Active Directory, and PKI integration
- Role-based access control
- Field and document level security
- Encrypted communication
- Auditing

Adding Users (now)

Command Line Utility

```
$ bin/shield/esusers useradd jaymode -r admin
Enter new password:
Retype new password:
```

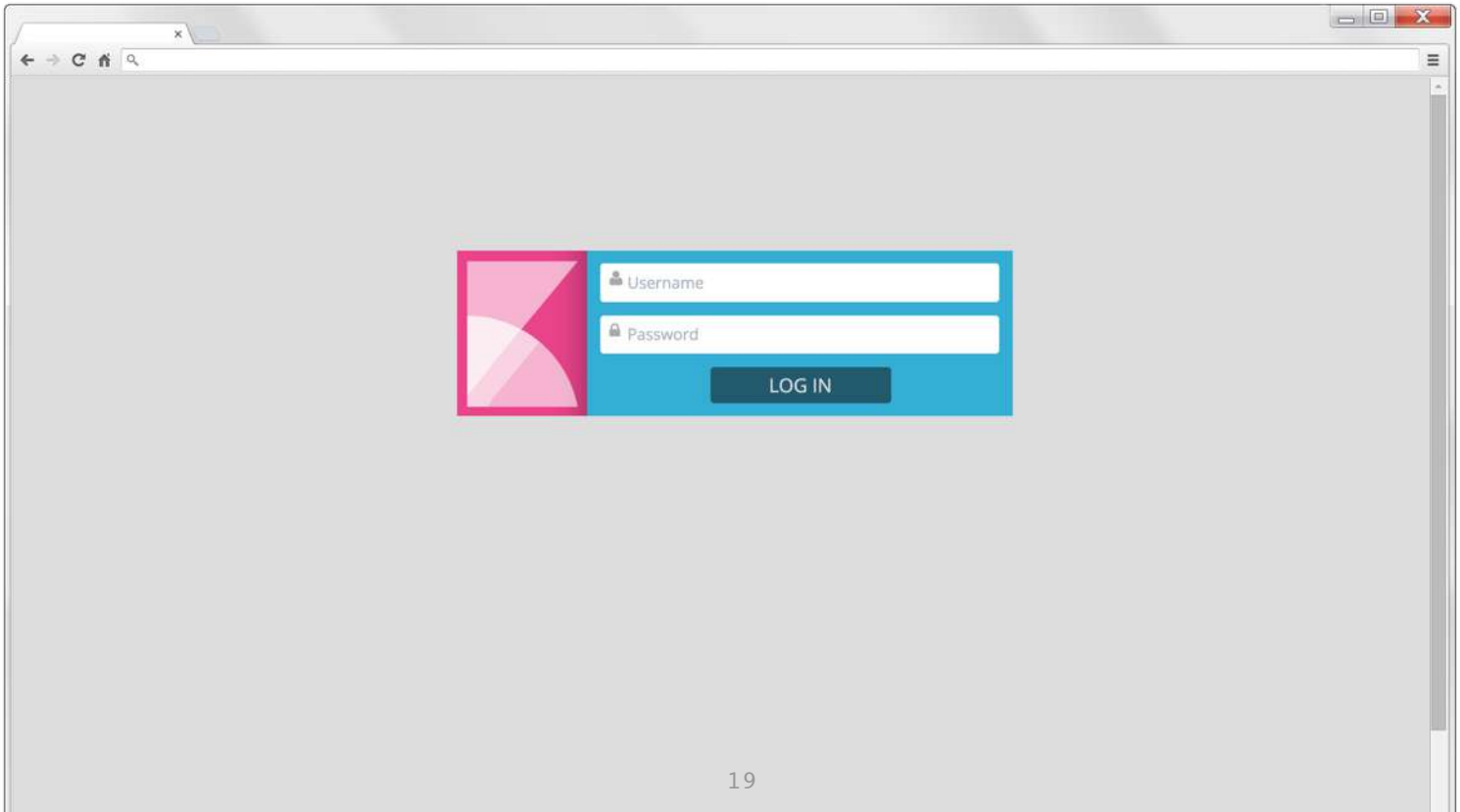
Security APIs

User and Role management

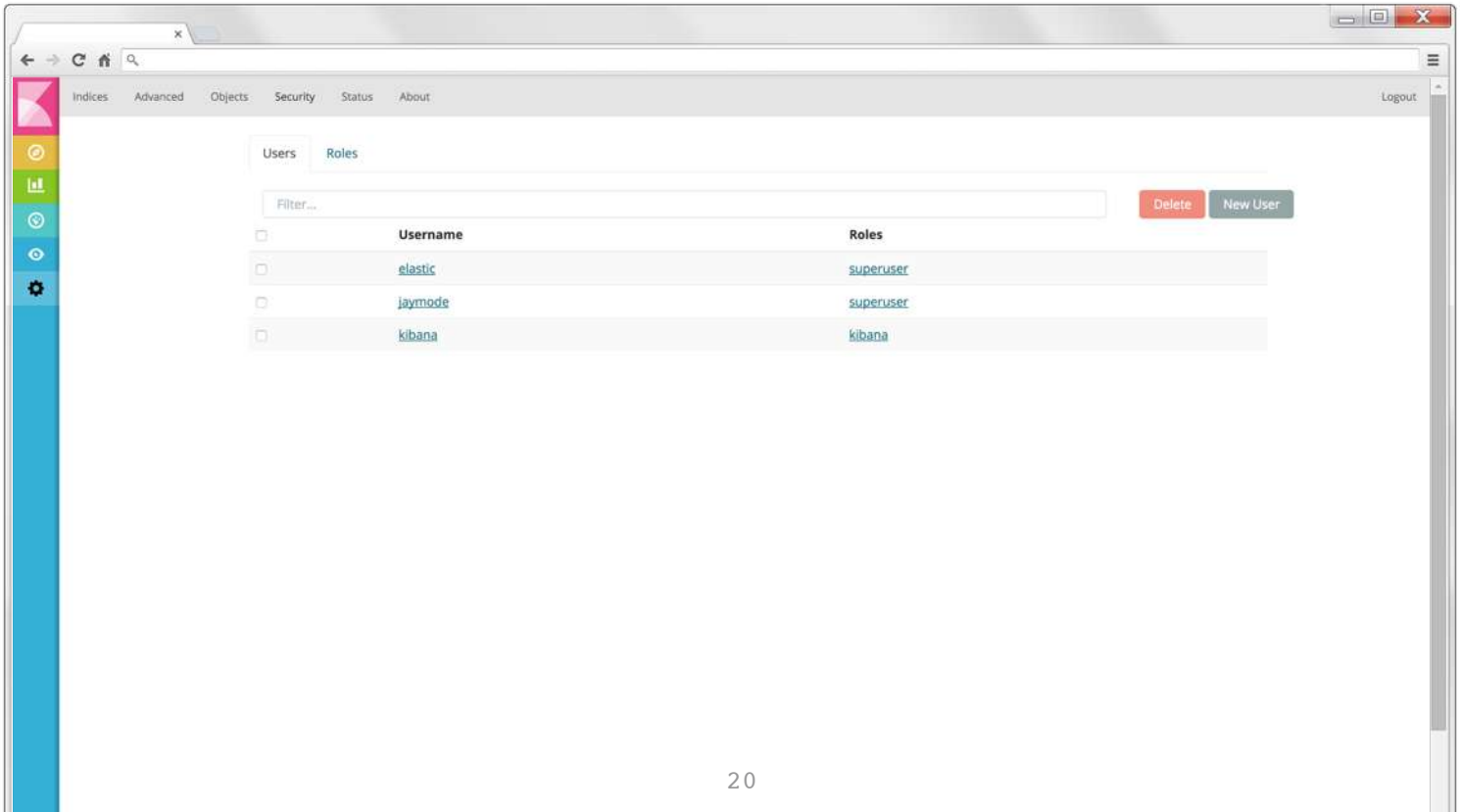
```
curl –XPUT localhost:9200/_shield/user/jaymode –d  ‘
{
    "roles" : ["engineering", "security"],
    "password" : "changeme"
}’

curl –XPUT localhost:9200/_shield/role/security –d  ‘
{
    "cluster": ["all"],
    "indices": [
        {
          "names": ".shield_audit_log-*",
          "privileges": ["all"]
        }
     ]
}’
```

Kibana Sessions and Login Screen



User and Roles UI



Security Configuration API & UI

Kibana Security

Built In Users

elastic on

Securing Elasticsearch

Spotlight Theater @ 2:40pm

Alerting

Watch This!

Alexander Reelsen @spinscale

Notify me on chat, if we have over 1000 orders per hour

- The Startup CEO

Trigger an alert, when the same IP accesses all services in a certain interval

- Your Admin

Email me when the product is back in stock!

- Desperate Online Shopper

5% traffic increase in the last 5 minutes.
Ping folks on chat!

- Your Loadbalancer

5% traffic increase in the last 5 minutes at 2am.
Pager time!

- Not your SO

Can you predict the additional system resources for the next two weeks?

- Every system architect ever

A Watch consists of…

- Trigger
- Input
- Condition
- Actions
- Metadata
- Transformation

PUT /_watcher/watch/cluster_health

```
{









}
```

PUT /_watcher/watch/cluster_health

```
{
  "trigger" : {
    "schedule" : { "interval" : "10s" }
  }









}
```

PUT /_watcher/watch/cluster_health

```
{
  "trigger" : {
    "schedule" : { "interval" : "10s" }
  },
  "input" : {
    "http" : {
      "request" : { "url" : "http://localhost:9200/_cluster/health" }
    }
  }









}
```

PUT /_watcher/watch/cluster_health

```
{
  "trigger" : {
    "schedule" : { "interval" : "10s" }
  },
  "input" : {
    "http" : {
      "request" : { "url" : "http://localhost:9200/_cluster/health" }
    }
  },
  "condition" : {
    "compare" : { "ctx.payload.status" : { "eq" : "red" } }
  }









}
```

PUT /_watcher/watch/cluster_health

```
{
  "trigger" : {
    "schedule" : { "interval" : "10s" }
  },
  "input" : {
    "http" : {
      "request" : { "url" : "http://localhost:9200/_cluster/health" }
    }
  },
  "condition" : {
    "compare" : { "ctx.payload.status" : { "eq" : "red" } }
  },
  "actions" : {
    "send_email" : {
      "email" : {
        "to" : "admin@example.org",
        "subject" : "Cluster Status Warning",
        "body" : "Cluster status is RED"
      }
    }
  }
}
```

Recap

2.0: Hipchat action

```
"actions" : {
  "notify-hipchat" : {
    "hipchat" : {
      "account" : "integration-account",
      "message" : {
        "body" : "@{{ctx.metadata.userOnDuty}} Encountered
{{ctx.payload.hits.total}} errors in the last 5 minutes
(facepalm)",
        "format" : "text",
        "color"  : "red",
        "notify" : true
      }
    }
  }
}
```

2.0: Slack action

```
"actions" : {
  "notify-slack" : {
    "slack" : {
      "message" : {
        "from" : "watcher",
        "to" : [ "#admins", "#errors" ] ,
        "text" : "Monitoring incident",
        "attachments" : [ {
          "text" : "@{{ctx.metadata.userOnDuty}} Encountered
{{ctx.payload.hits.total}} errors in the last 5 minutes
(facepalm)",
          "title" : "text",
          "color"  : "danger" ] }
...
```

2.0: Activate/Deactivate REST API

```
PUT /_watcher/watch/<watch_id>/_activate

PUT /_watcher/watch/<watch_id>/_deactivate
```

2.0: Array Compare

```
"condition": {
  "array_compare": {
    "ctx.payload.aggregations.top_tweeters.buckets" : {
      "path": "doc_count",
      "gte": {
        "value": 25,
        "quantifier": "some"
      }
    }
  }
}
```

2.1: Chained inputs

```
"input" : {
   "chain": {
     "inputs": [
       {
         "first": { "simple" : { "path" : "/_search" } }
       },
       {
         "second": { "http" : { "request" : { … } } }
       }
     ]
   }
 }
 ...
}
```

2.1: Chained inputs

```
"input"
   "chain"
     "inputs"

          "first"


          "second"


   }
  }
  ...
}
```

{{ctx.payload.first.path}}

{{ctx.payload.second.hits.total}}

2.3: PagerDuty action

```
"actions" : {
  "notify-pagerduty" : {
    "pagerduty" : {
      "message" : {
        "description" : "Main system down, please check!
Happened at {{ctx.execution_time}}",
        "client" : "/foo/bar/{{ctx.watch_id}}",
        "attach_payload" : true,
        "context" : [ {
          "type" : "response",
          "href" : "http://www.test.de/foo" }
        ]
...
```

2.3: External email attachments

```
"actions" : {
  "email_admin" : {
    "email" : {
      "to" : "ceo@example.org",
      "attachments" : {
        "my_id" : {
          "http" : {
            "request" : {
              "url" : "http://example.org/daily-report.pdf"
            }
          }
        }
      }
    }
...
```

What's next?

Curator

Watcher UI

Actions

elastic on

BoF: Alerting & Notifications

Share Your Watcher Stories

Friday, Lunch area @ 11:00am

Reporting

Kibana For Your Inbox

Joe Fleming @w33ble

I need this information.
Can you send me a report?

- Every Manager Ever


kibana
Discover
Visualize
Dashboard
Settings
Last 4 hours
Traffic Info
Byte Counts
5,686.446
Average bytes
5,491.218
50th percentile of bytes
19,783,147
Sum of bytes
Hits by Extension
jpg
css
gif
png
php
Count
utc_time per 5 minutes
Geo Distribution
Siberia
ASIA
EUROPE
Gobi
Sahara
Arabian Peninsula
AFRICA
Indian Ocean
Indonesia
AUSTRALIA
SOUTH AMERICA
Header Distribution

Byte Counts

5,678.296

Average bytes

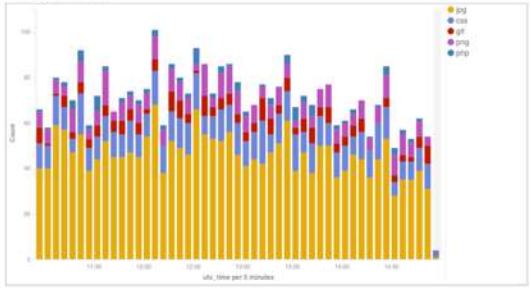
5,459.354

50th percentile of bytes

19,663,940

Sum of bytes

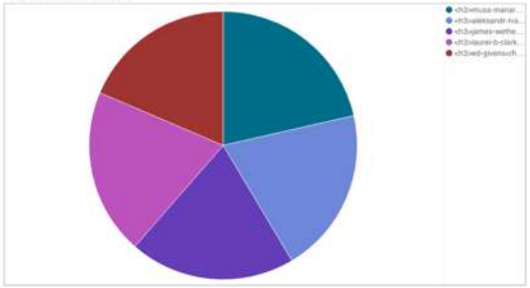
Hits by Extension



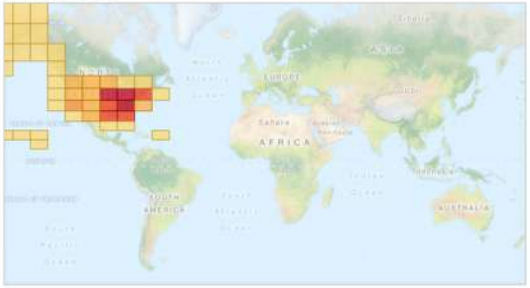
elastic

Page 1 of 2

Header Distribution



Geo Distribution

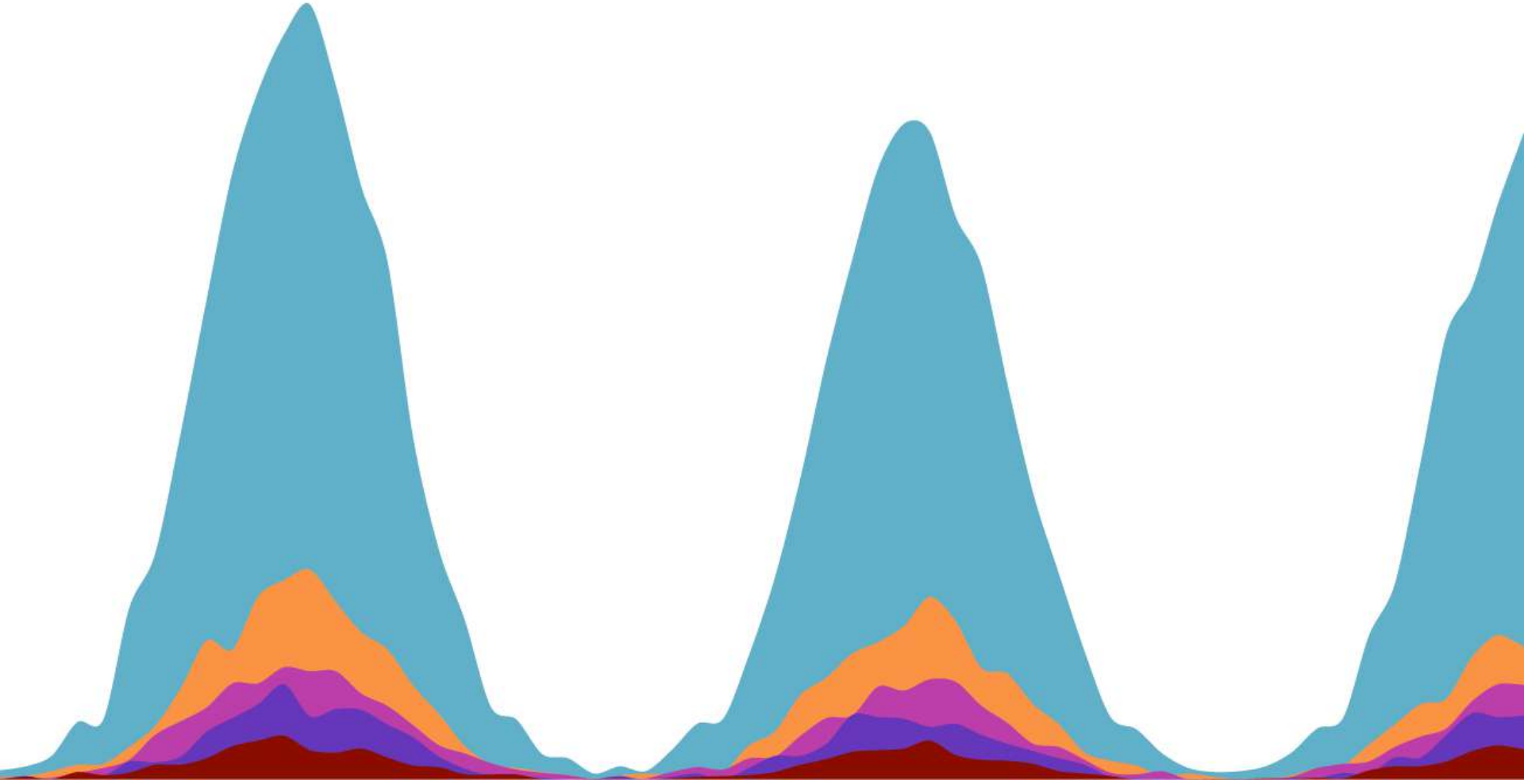


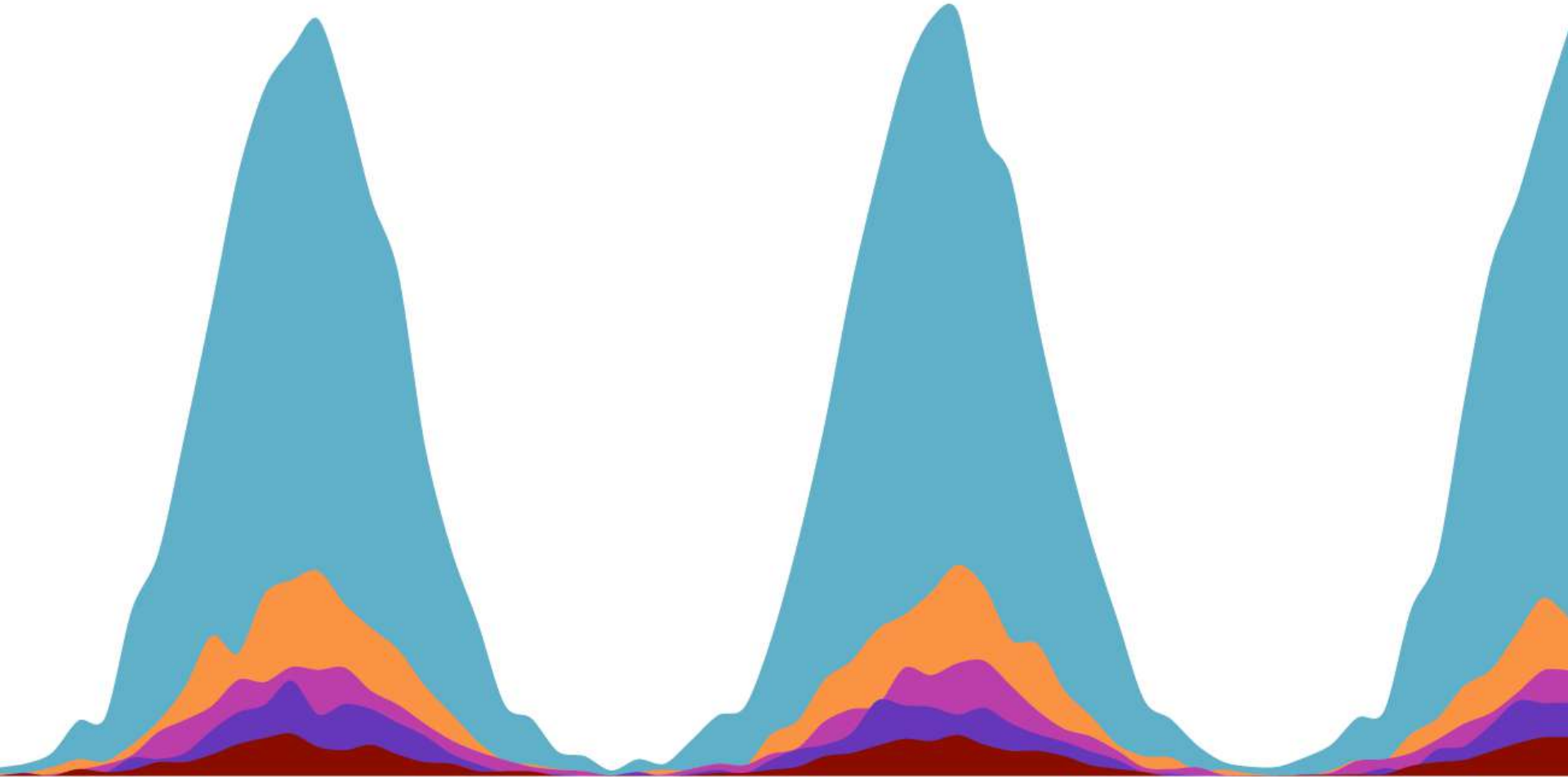
elastic

Page 2 of 2

Network’s down.
Meeting’s over.

- No Manager Ever





Delivery with Alerting

```
"actions" : {
  "email_admin" : {
    "email" : {
      "to" : "ceo@example.org",
      "attachments" : {
        "my_id" : {
          "http" : {
            "request" : {
              "url" : "http://example.org/daily-report.pdf"
            }
          }
        }
      }
    }
...
```

5.0 Alpha 1

Distributed Rendering

Administrative Control

Historical Archive

elastic on

From Dashboard to PDF

Generate Reports with the Elastic Stack

Spotlight Theater @ 3:40pm


ASK ME ANYTHING
ASK ME ANYTHING
elastic
SEARCH
ASK ME

Securing Elasticsearch
Spotlight Theater: 2:40pm

From Dashboard to PDF
Spotlight Theater: 3:40pm

Monitoring Elasticsearch
Spotlight Theater: 4:40pm

BoF: Alerting & Notifications
Lunch Area: Friday at 11:00am