

Security, Alerting, Monitoring and More with the Elastic Stack



x-pack

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 - Cluster Pulse Development Trial 7 days ago to a few seconds ago refreshed every 1m Dashboards

QUERY
Filtered | Node events | Index events | Routing events

FILTERING

CLUSTER SUMMARY
Name: elasticsearch Status: green Nodes: 4 Indices: 3 Shards: 14 Data: 25.43 MB CPU: 14% Memory: 407.66 MB / 3.87 GB Up time: 15.4 m Version: 1.4.5

TIME LINE
View | Zoom Out | Node events (8) Index events (24) Routing events (70) count per 1h | (102 hits)

CLUSTER EVENTS 0 to 100 of 102 available for paging

@timestamp	_type	event	message
2016-02-07T15:28:07.616-07:00	routing_event	shard_started	[topbeat-2016.02.07] started on [n3][192.168.1.108:9303]
2016-02-07T15:28:07.438-07:00	routing_event	shard_started	[topbeat-2016.02.07] started on [n3][192.168.1.108:9303]
2016-02-07T15:28:07.062-07:00	routing_event	shard_started	[topbeat-2016.02.07] started on [n3][192.168.1.108:9303]
2016-02-07T15:28:07.062-07:00	routing_event	shard_relocating	[topbeat-2016.02.07] relocating to [n3][192.168.1.108:9303] from [n0]...
2016-02-07T15:28:06.854-07:00	routing_event	shard_relocating	[topbeat-2016.02.07] relocating to [n3][192.168.1.108:9303] from [n1]...
2016-02-07T15:28:06.854-07:00	routing_event	shard_relocating	[topbeat-2016.02.07] relocating to [n3][192.168.1.108:9303] from [n2]...
2016-02-07T15:28:02.398-07:00	node_event	node_joined	[n3][192.168.1.108:9303] joined
2016-02-07T15:27:58.467-07:00	routing_event	shard_started	[topbeat-2016.02.07] started on [n2][192.168.1.108:9302]
2016-02-07T15:27:58.027-07:00	routing_event	shard_started	[topbeat-2016.02.07] started on [n2][192.168.1.108:9302]
2016-02-07T15:27:58.003-07:00	routing_event	shard_started	[topbeat-2016.02.07] started on [n2][192.168.1.108:9302]
2016-02-07T15:27:58.003-07:00	routing_event	shard_relocating	[topbeat-2016.02.07] relocating to [n2][192.168.1.108:9302] from [n0]...
2016-02-07T15:27:58.003-07:00	routing_event	shard_started	[topbeat-2016.02.07] started on [n2][192.168.1.108:9302]

EVENT TYPES

Term	Count	Action
routing_event	70	Q
index_event	24	Q
node_event	8	Q

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

QUERY

Pinned n1

FILTERING

OS CPU



JVM HEAP USAGE (%)



LOAD (1M)



- OS
- OS EXTENDED
- JVM MEMORY
- JVM GC YOUNG
- JVM GC OLD
- INDICES SEARCH REQUESTS QUERY
- INDICES SEARCH REQUESTS FETCH

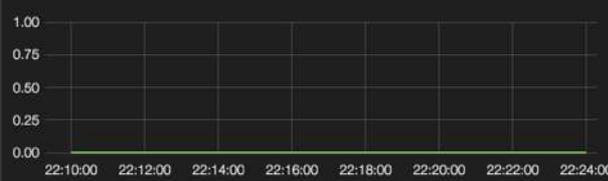
INDICES INDEXING RATE



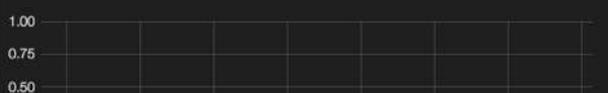
INDICES TOTAL INDEXING TIME



INDICES INDEXING THROTTLING TIME



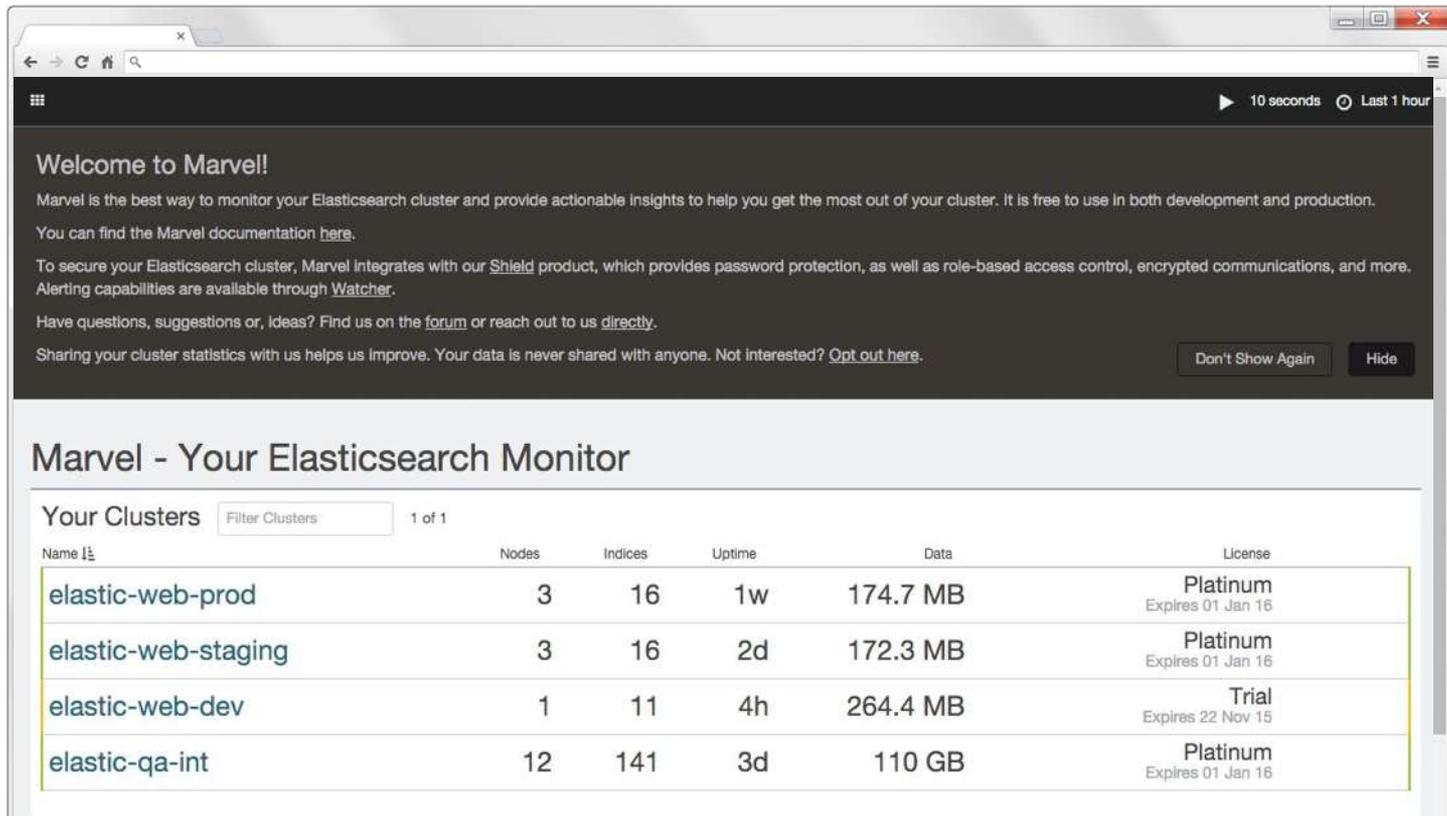
INDICES DELETE RATE



Monitoring for Elasticsearch 2.x

Yes, we like to rename things :)

Multi-Cluster Support



Welcome to Marvel!

Marvel is the best way to monitor your Elasticsearch cluster and provide actionable insights to help you get the most out of your cluster. It is free to use in both development and production.

You can find the Marvel documentation [here](#).

To secure your Elasticsearch cluster, Marvel integrates with our [Shield](#) product, which provides password protection, as well as role-based access control, encrypted communications, and more. Alerting capabilities are available through [Watcher](#).

Have questions, suggestions or, ideas? Find us on the [forum](#) or reach out to us [directly](#).

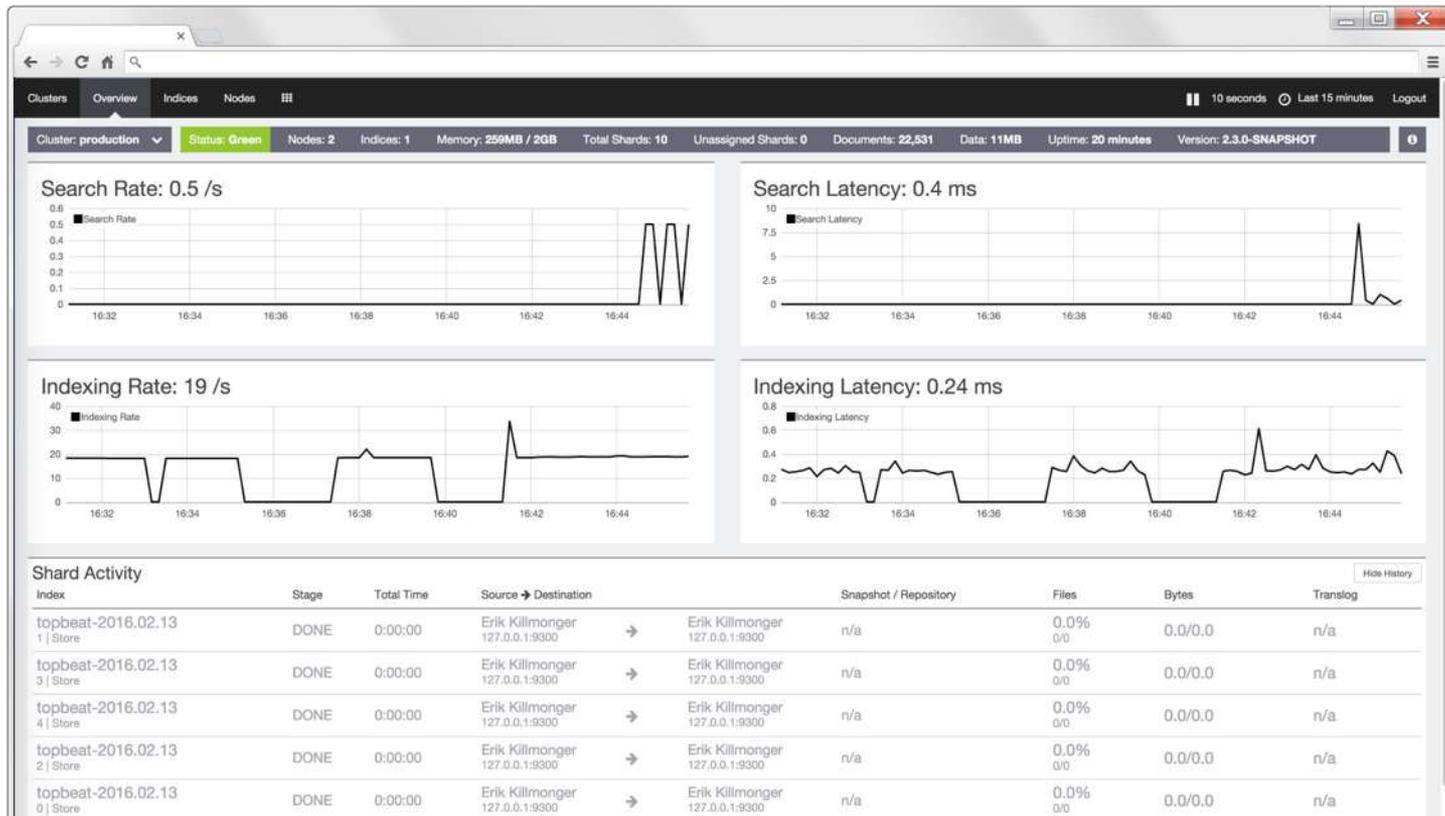
Sharing your cluster statistics with us helps us improve. Your data is never shared with anyone. Not interested? [Opt out here](#).

Marvel - Your Elasticsearch Monitor

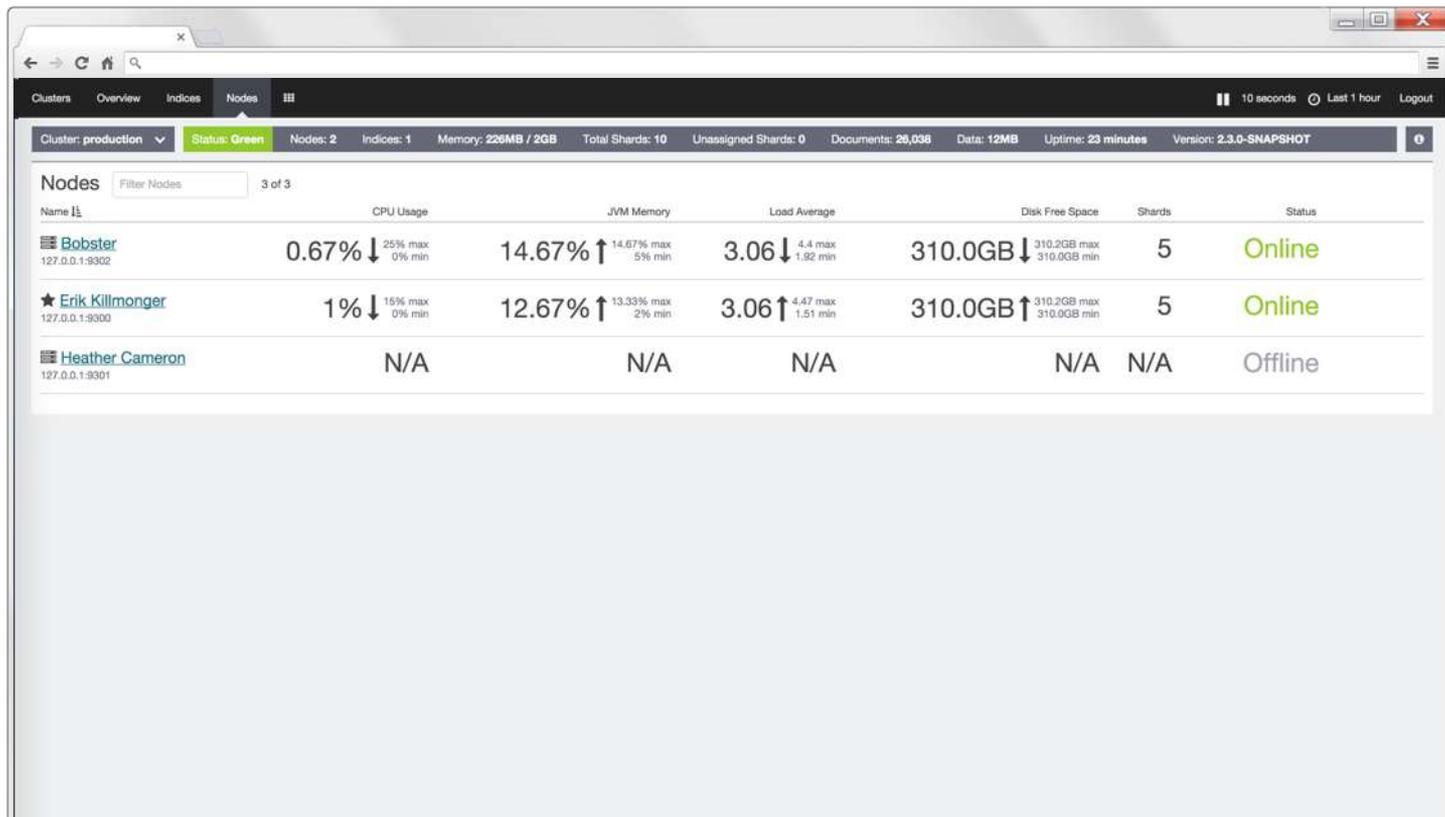
Your Clusters 1 of 1

Name	Nodes	Indices	Uptime	Data	License
elastic-web-prod	3	16	1w	174.7 MB	Platinum Expires 01 Jan 16
elastic-web-staging	3	16	2d	172.3 MB	Platinum Expires 01 Jan 16
elastic-web-dev	1	11	4h	264.4 MB	Trial Expires 22 Nov 15
elastic-qa-int	12	141	3d	110 GB	Platinum Expires 01 Jan 16

Cluster Overview at a Glance



Node Listing



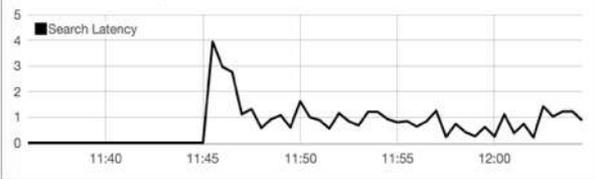
The screenshot displays the 'Nodes' tab in the Elasticsearch management interface. At the top, a navigation bar shows 'Clusters', 'Overview', 'Indices', and 'Nodes'. Below this, a summary bar indicates the cluster is 'production' with a 'Status: Green', 2 nodes, 1 index, 226MB memory, 10 total shards, 0 unassigned shards, 26,038 documents, 12MB data, 23 minutes uptime, and version 2.3.0-SNAPSHOT. The main content area is titled 'Nodes' and shows a table of 3 nodes. The table columns are Name, CPU Usage, JVM Memory, Load Average, Disk Free Space, Shards, and Status. The nodes listed are Bobster (Online), Erik Killmonger (Online), and Heather Cameron (Offline).

Name	CPU Usage	JVM Memory	Load Average	Disk Free Space	Shards	Status
 Bobster 127.0.0.1:9302	0.67% ↓ 25% max 0% min	14.67% ↑ 14.67% max 5% min	3.06 ↓ 4.4 max 1.92 min	310.0GB ↓ 310.2GB max 310.0GB min	5	Online
 Erik Killmonger 127.0.0.1:9303	1% ↓ 15% max 0% min	12.67% ↑ 13.33% max 2% min	3.06 ↑ 4.47 max 1.51 min	310.0GB ↑ 310.2GB max 310.0GB min	5	Online
 Heather Cameron 127.0.0.1:9301	N/A	N/A	N/A	N/A	N/A	Offline

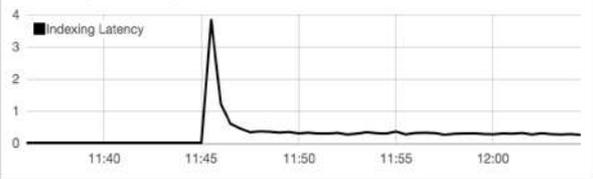
★ Azazel

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**

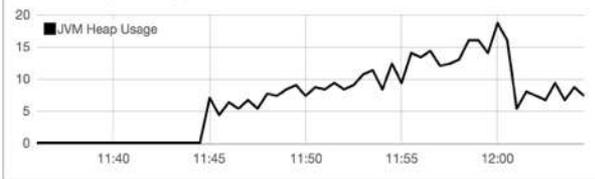
Search Latency: 0.88 ms



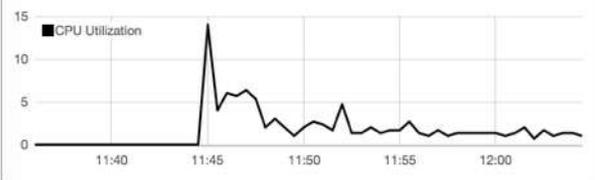
Indexing Latency: 0.25 ms



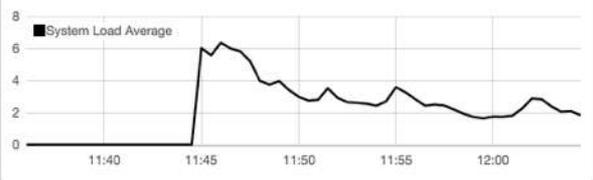
JVM Heap Usage: 7.33 %



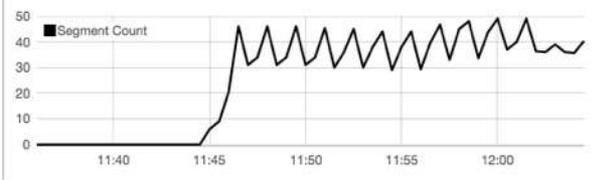
CPU Utilization: 1 %



System Load Average: 1.82

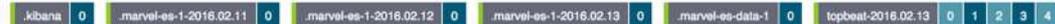


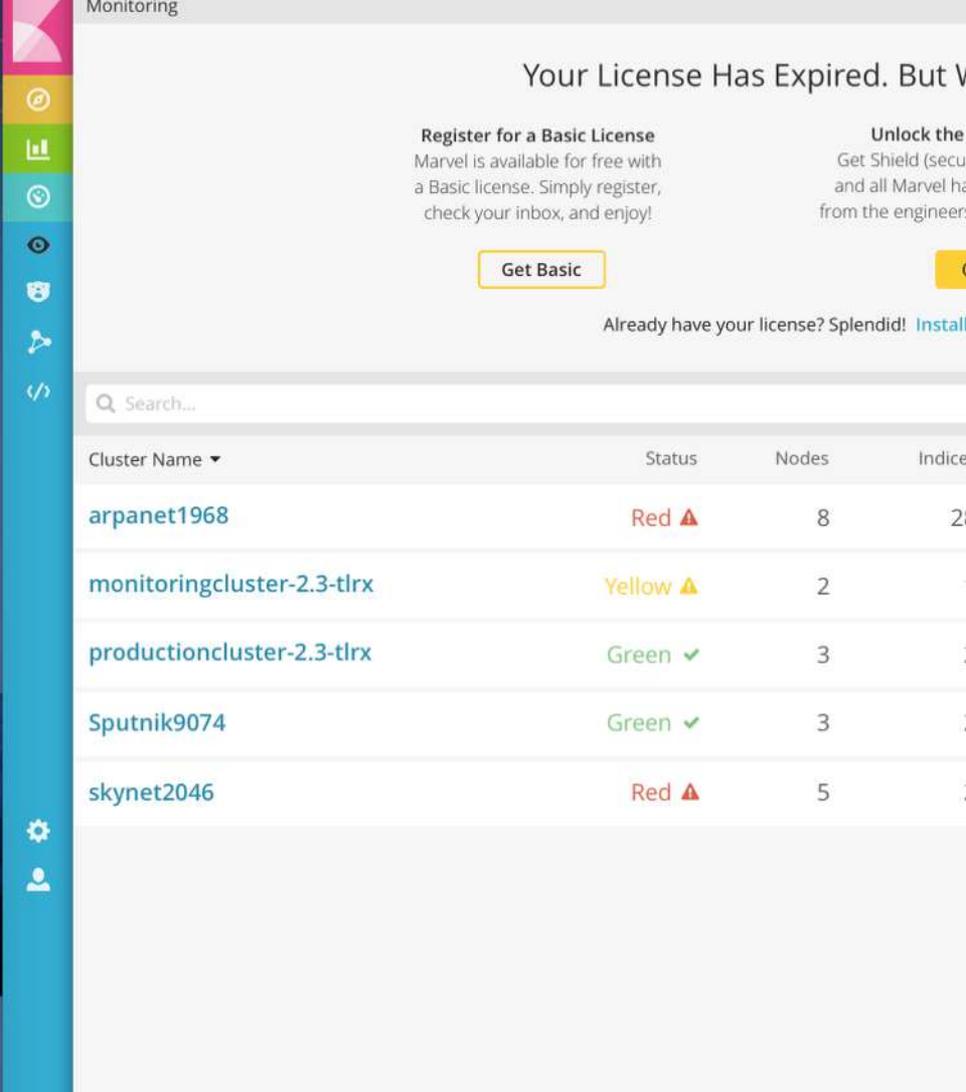
Segment Count: 40.33



Shard Legend ■ Primary ■ Replica ■ Relocating ■ Initializing

Indices





Kibana 5

New design

Issues

Cross-Stack Monitoring



Monitoring Elasticsearch

Spotlight Theater @ 4:40pm



x-pack

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:
```

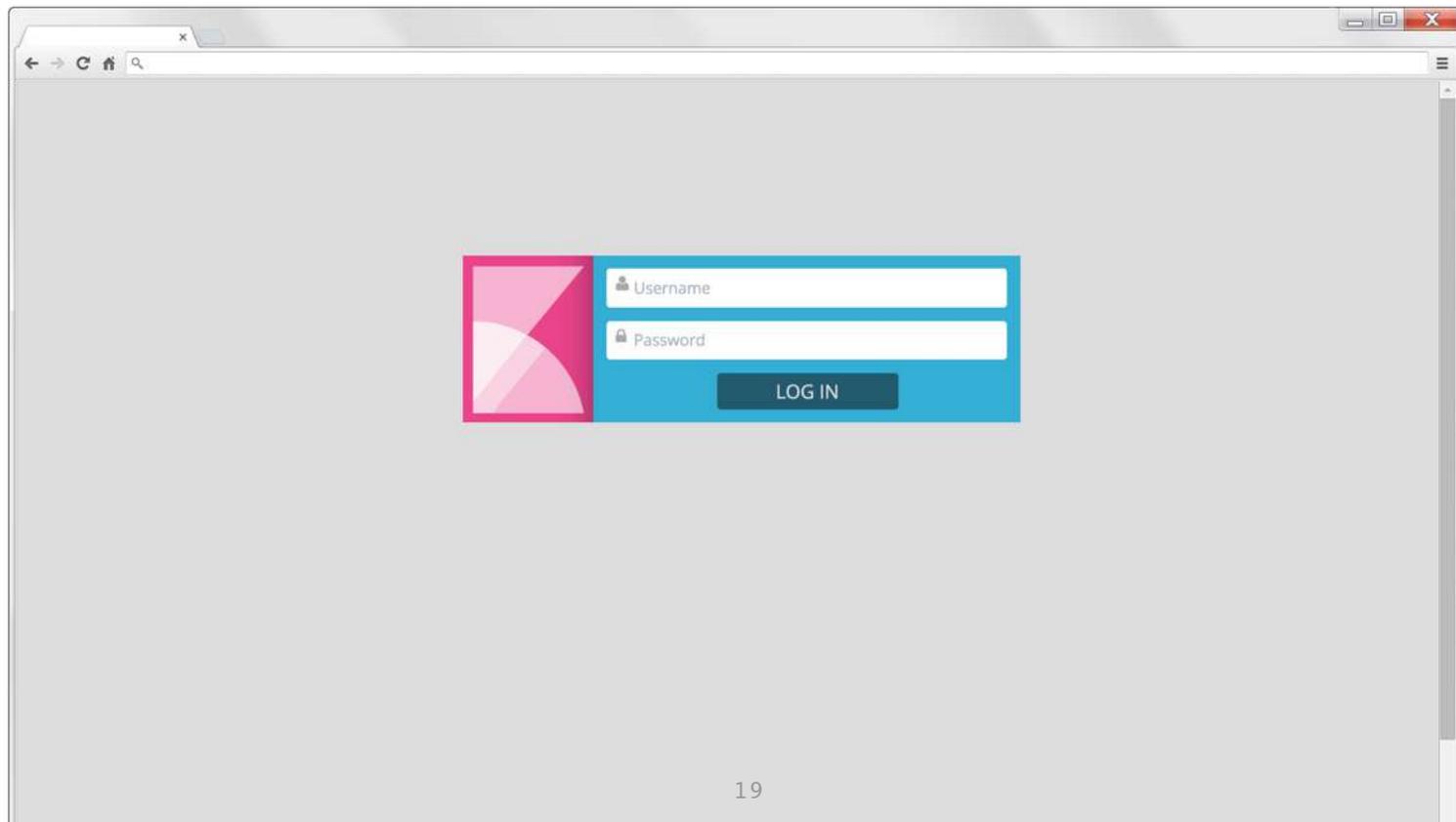
Security APIs

User and Role management

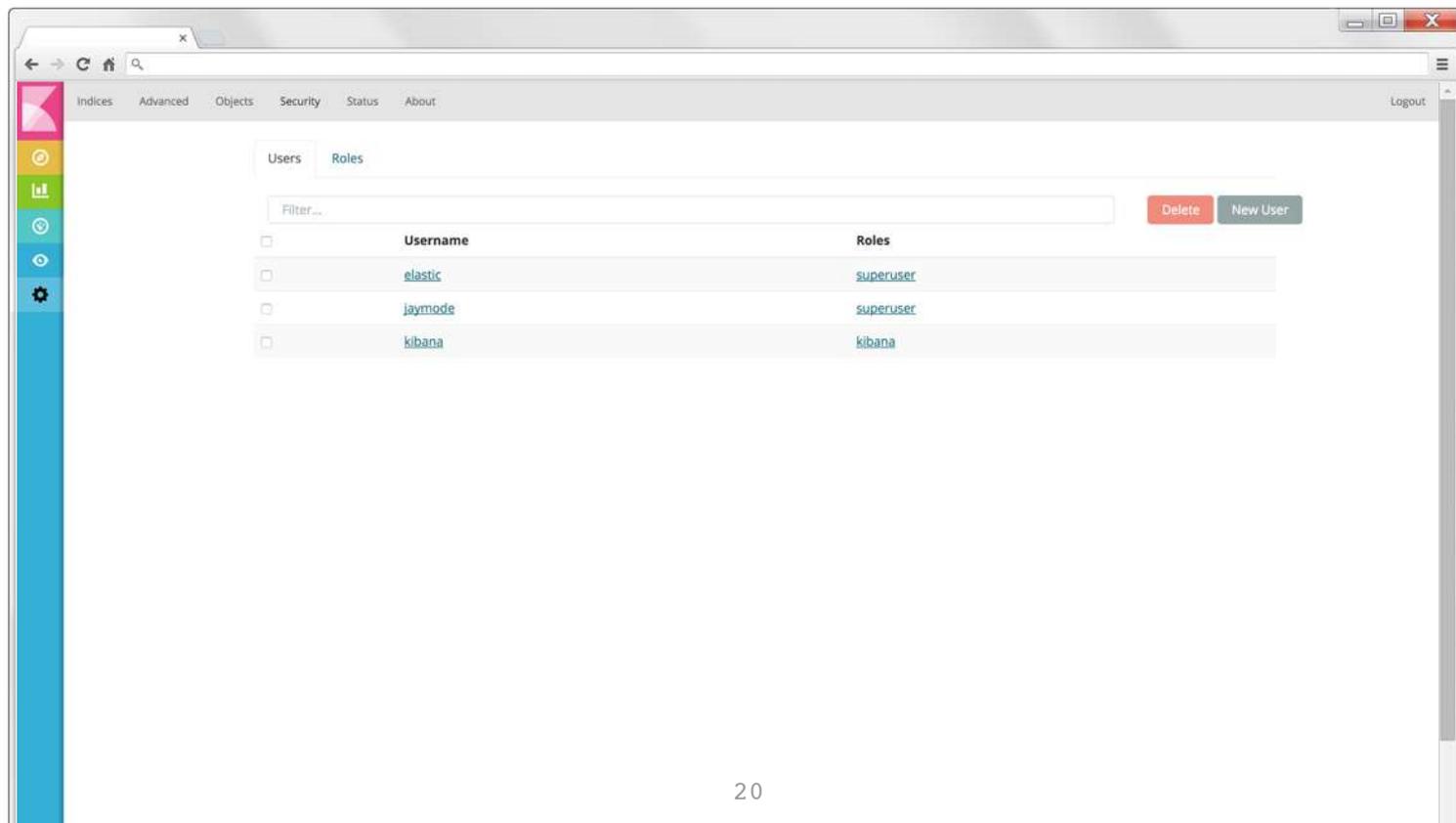
```
curl -XPUT localhost:9200/_shield/user/jaymode -d '{
  "roles" : ["engineering", "security"],
  "password" : "changeme"
}'

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



Securing Elasticsearch

Spotlight Theater @ 2:40pm



x-pack

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



BoF: Alerting & Notifications

Share Your Watcher Stories

Friday, Lunch area @ 11:00am



x-pack

Reporting

Kibana For Your Inbox

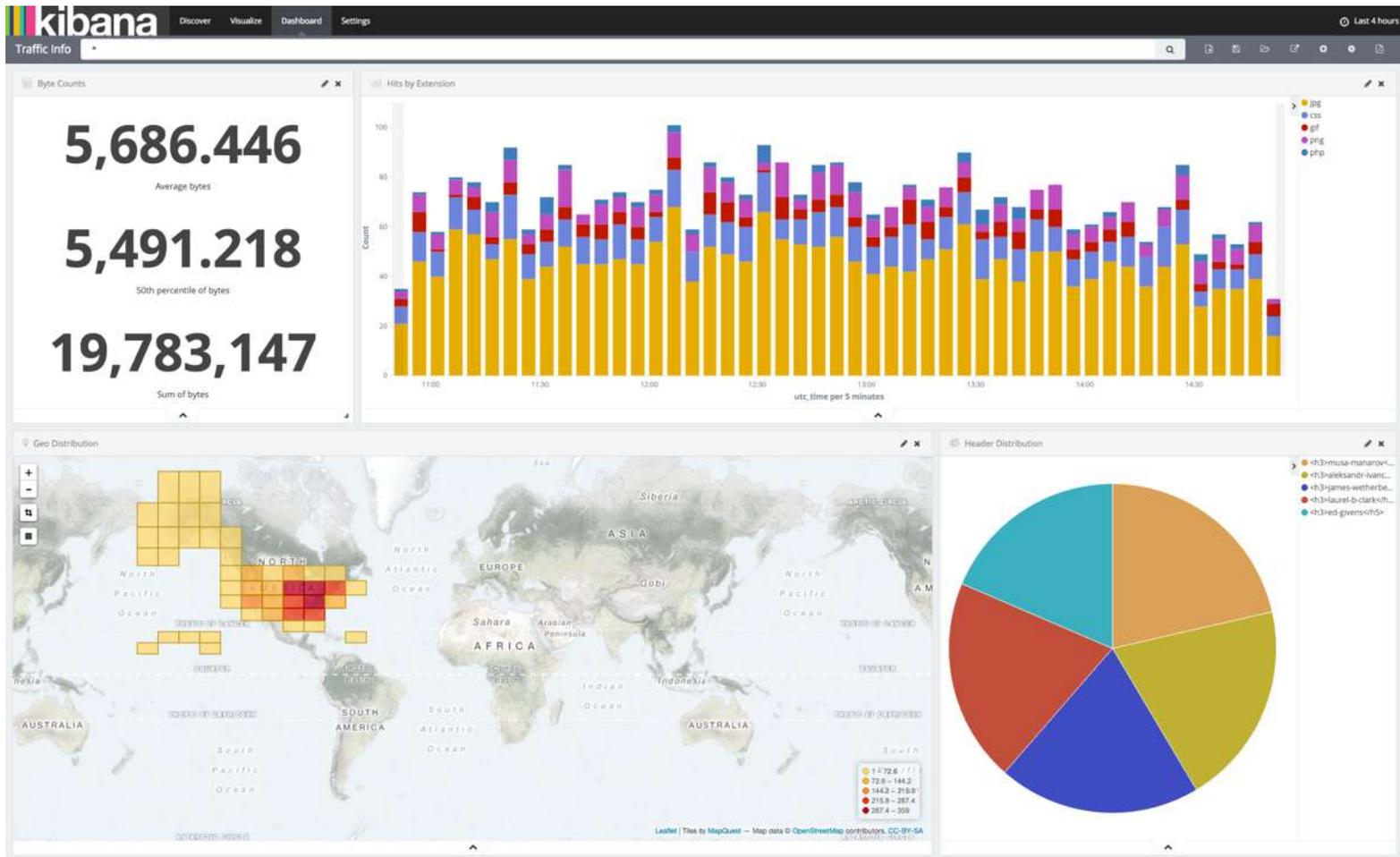
Joe Fleming

@w33ble



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

- Every Manager Ever



Byte Counts

5,678.296

Average bytes

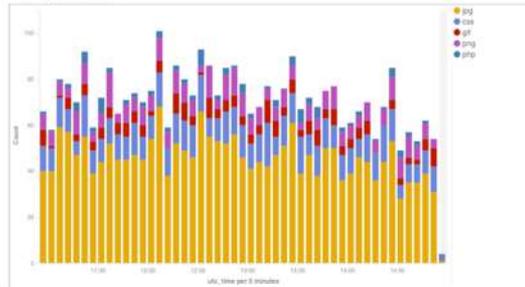
5,459.354

300th percentile of bytes

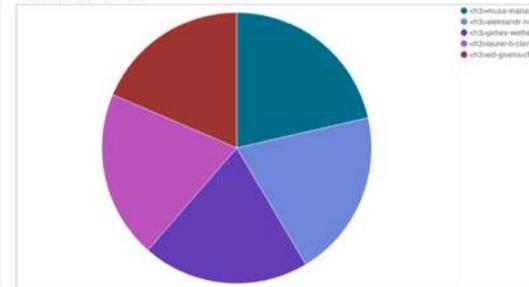
19,663,940

Sum of bytes

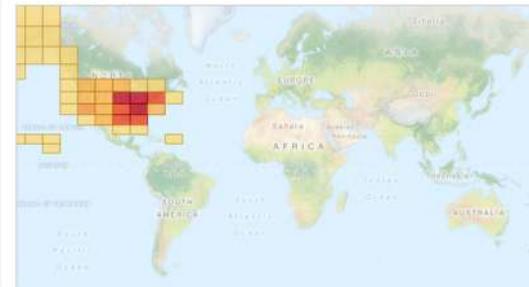
Hits by Extension



Header Distribution



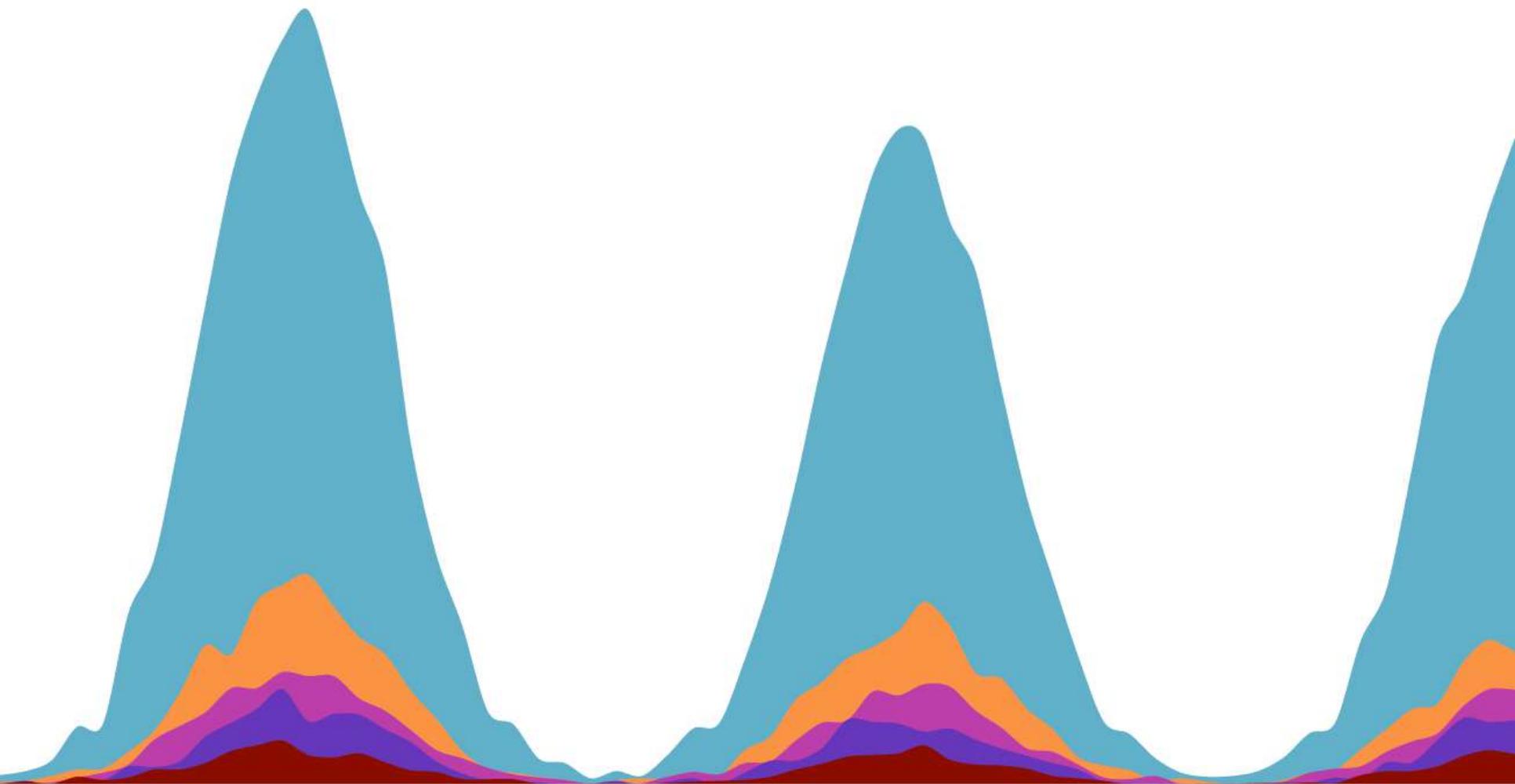
Geo Distribution

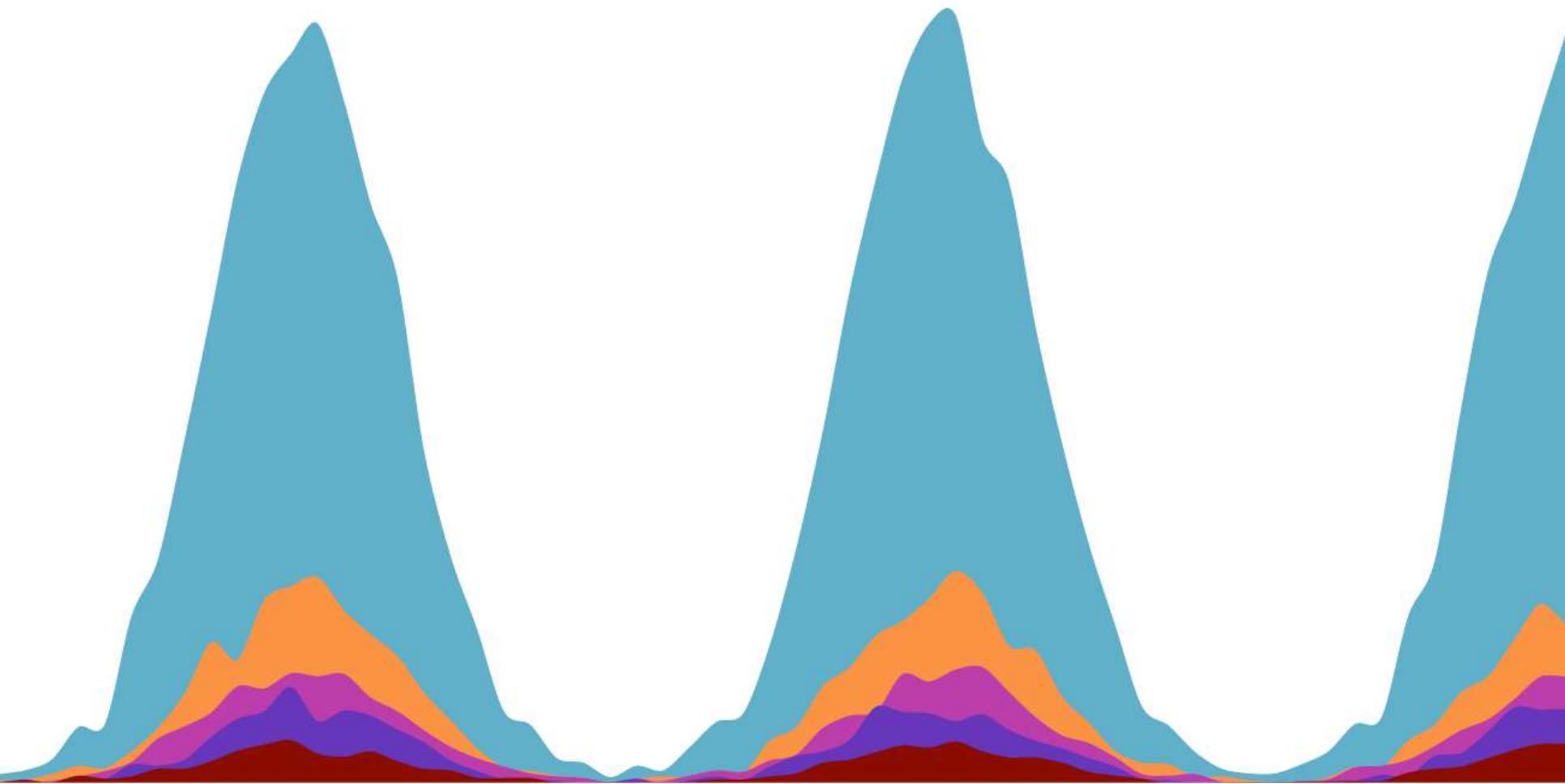




**Network's down.
Meeting's over.**

- 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



From Dashboard to PDF

Generate Reports with the Elastic Stack

Spotlight Theater @ 3:40pm

ASK ME ANYTHING

ASK ME ANYTHING

elastic

SEARCH

ASK ME ANYTHING

ASK ME ANYTHING

ASK ME ANYTHING



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