elastic{on} 2017

x-pack

What x-citing in x-pack?

Monitoring	Chris Earle	@pickypg
Security	Jay Modi	@jaymode2001
Reporting	Brandon Kobel	@kobelb
Alerting	Alexander Reelsen	@spinscale
	Shaunak Kashyap	@shaunak
Graph	Mark Harwood	@elasticmark

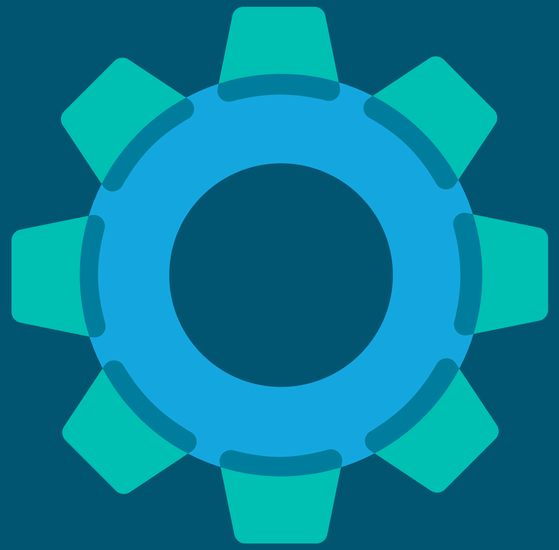
Agenda

x-pack

All the news

1. Management & Monitoring
2. Security
3. Reporting
4. Alerting
5. Graph

x-pack



Management & Monitoring

Thank You, the Management

x-pack

- Foundation (5.0)
- Elastic Stack Integration (5.0 for Elasticsearch integration)
  - It’s not just for Kibana anymore!
- User Management (5.0+)
- Role Management (5.0+)
- Search Profiler (5.1)
  - Free with Basic license!

More Synergy to Come

x-pack

- More Management Puns and Buzzwords
- Deeper Elastic Stack Integration
  - Elasticsearch management (e.g., putting a UI on top of complicated APIs)
  - Logstash management (e.g., shared configurations stored in Elasticsearch)
  - Beats management
  - Monitoring integration
  - Kibana APIs

Did he say Monitoring?

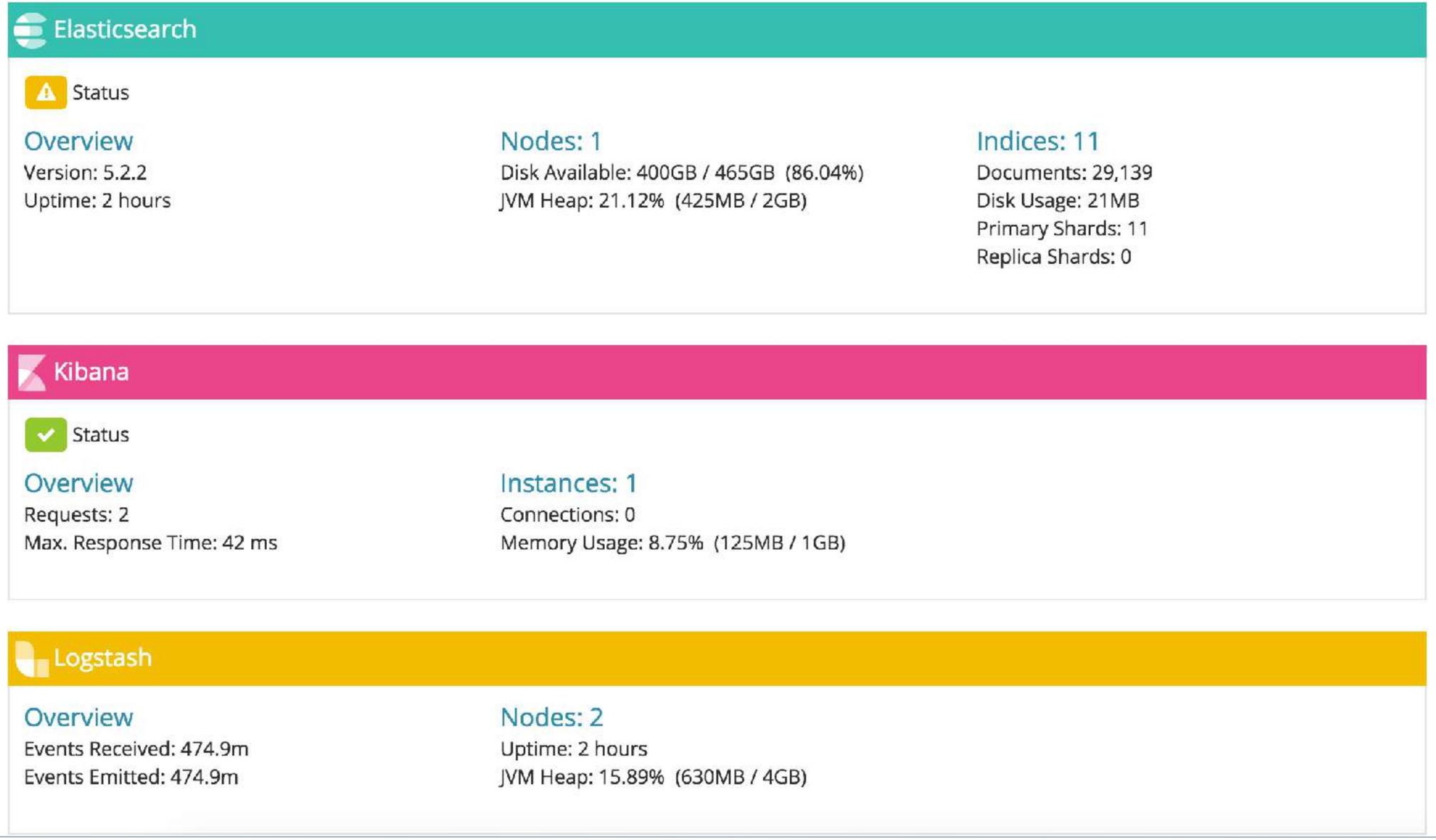
That sounds like a good segue

Monitoring: Reloaded

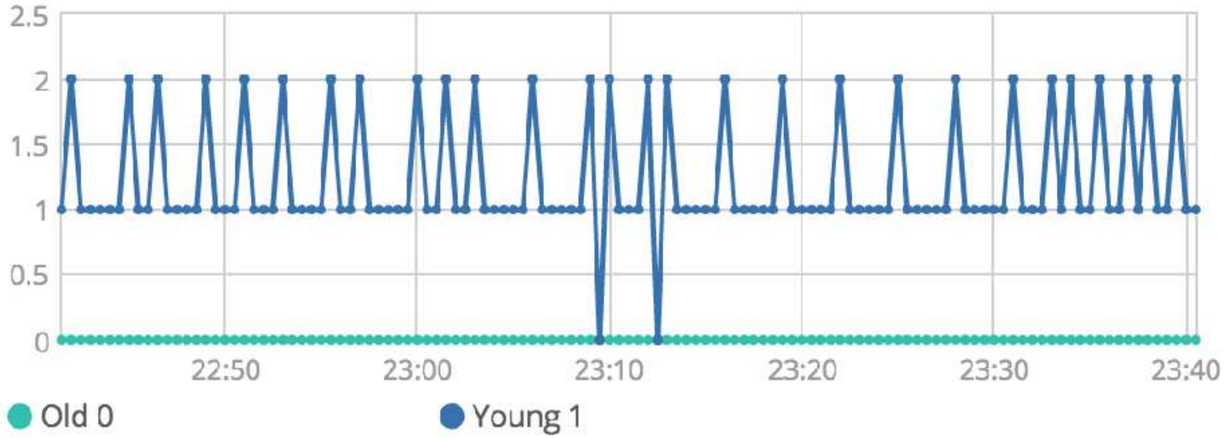
x-pack

- Kibana Monitoring (5.0)
- Multiple Series per chart for simplified comparisons (5.0)
- Improved HTTP Exporter using Low-level REST Client (5.0)
- Advanced Node and Index views (5.1)
- Logstash Monitoring (5.2)
- Cgroup (Container) metric display for Elasticsearch (5.2)

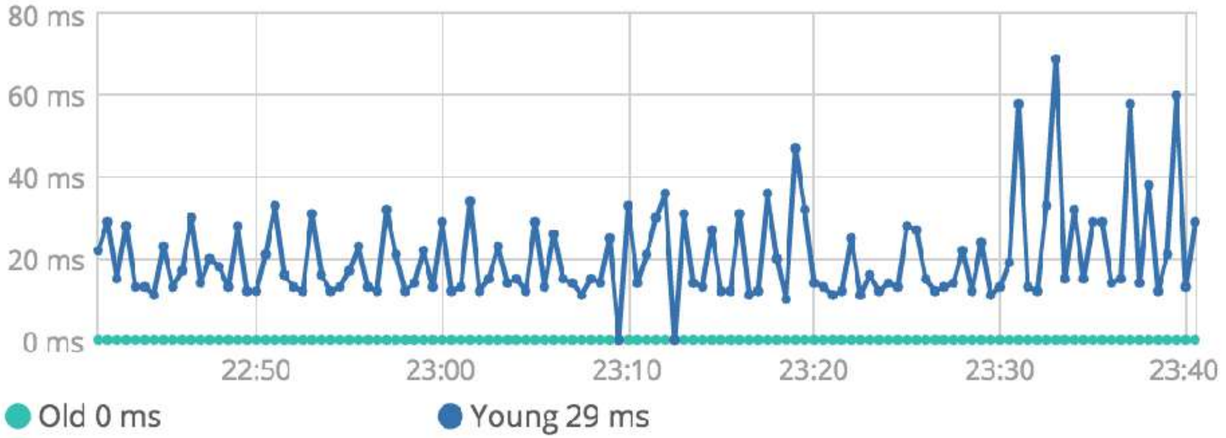
x-pack


Elasticsearch
Status
Overview
Version: 5.2.2
Uptime: 2 hours
Nodes: 1
Disk Available: 400GB / 465GB (86.04%)
JVM Heap: 21.12% (425MB / 2GB)
Indices: 11
Documents: 29,139
Disk Usage: 21MB
Primary Shards: 11
Replica Shards: 0
Kibana
Status
Overview
Requests: 2
Max. Response Time: 42 ms
Instances: 1
Connections: 0
Memory Usage: 8.75% (125MB / 1GB)
Logstash
Overview
Events Received: 474.9m
Events Emitted: 474.9m
Nodes: 2
Uptime: 2 hours
JVM Heap: 15.89% (630MB / 4GB)

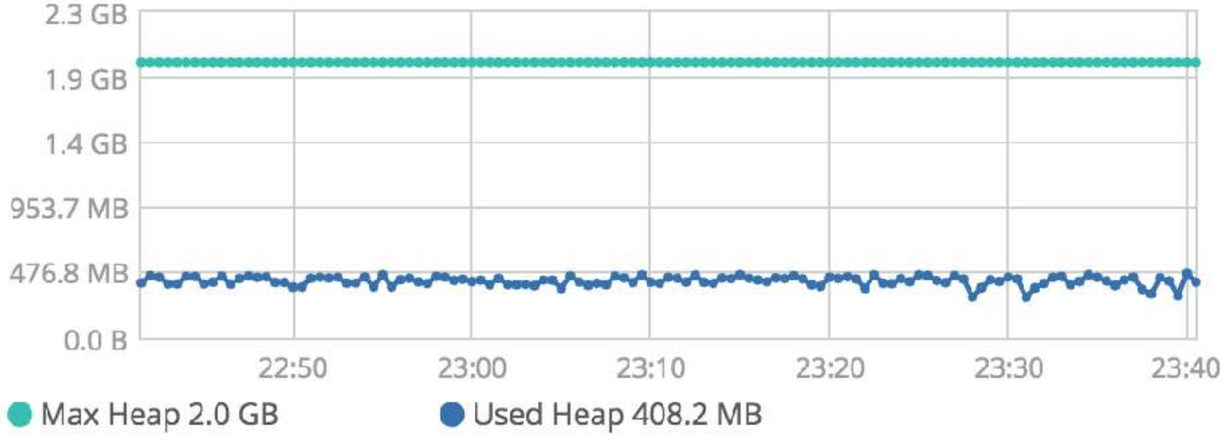
GC Count



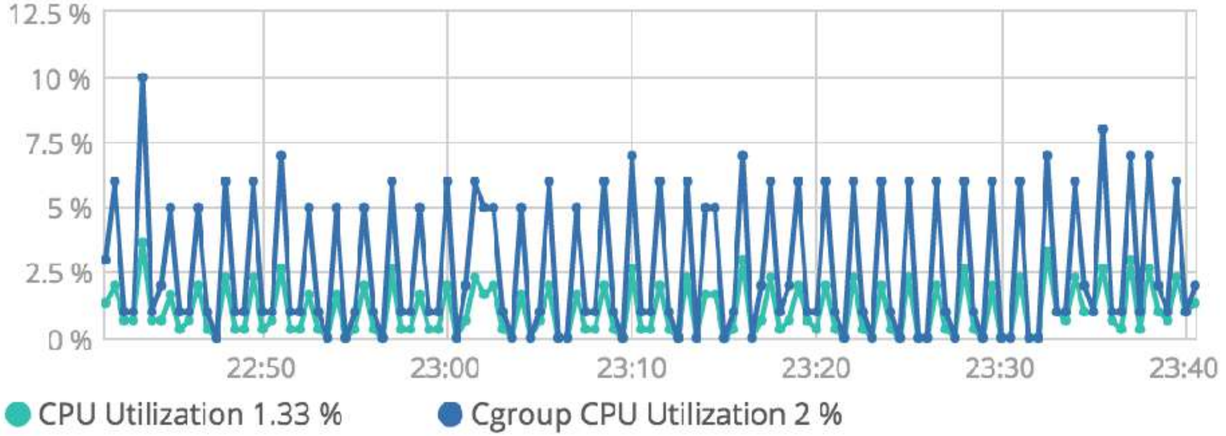
GC Duration (ms)



JVM Heap (GB)



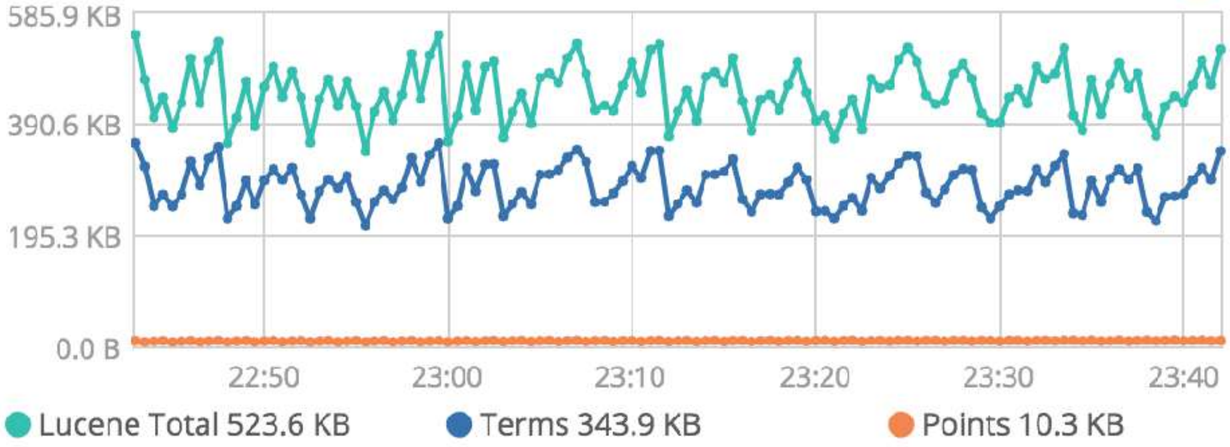
CPU Utilization (%)



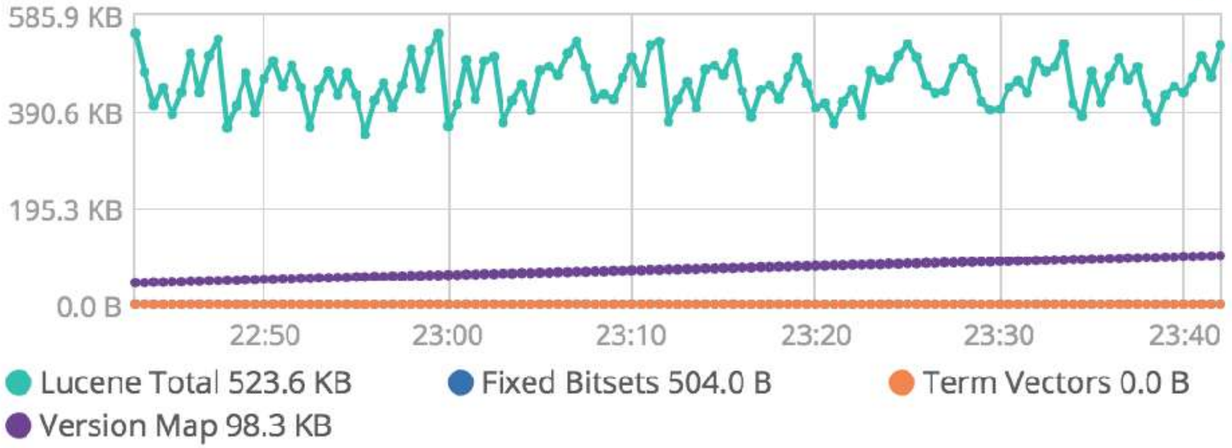
x-pack

Index Memory - Lucene 1 (KB)

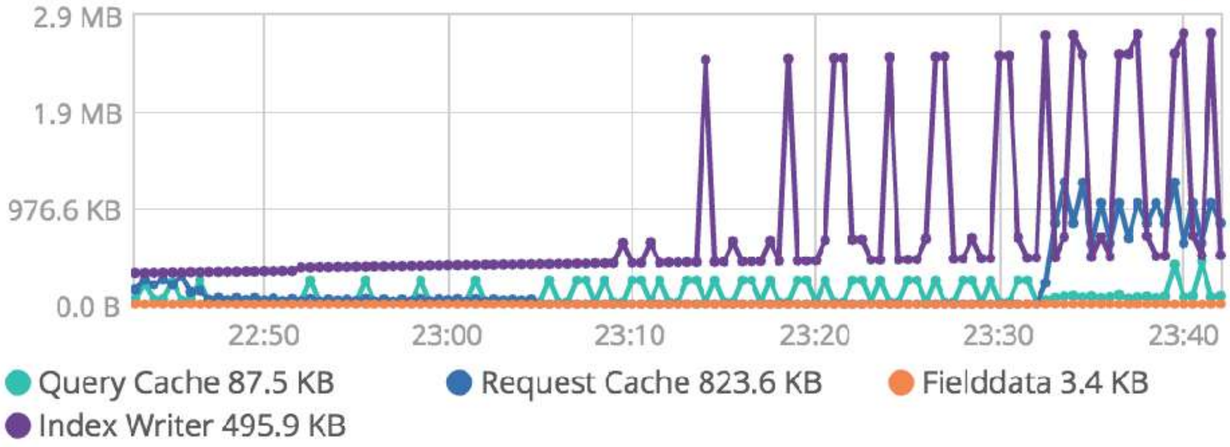
Index Memory - Lucene 2 (KB)



Index Memory - Lucene 3 (KB)



Index Memory - Elasticsearch (KB)



Wait for Applause to Stop

You were applauding, right?

Monitoring: Revolution(s)

x-pack

- Cluster Alerts
  - Proactive, automatic notifications of problems via Watcher
- Logstash Pipeline Viewer
  - Find bottlenecks in your Logstash nodes and plugins
- Machine Learning integration
- Beats integration

Clusters

10 seconds

Last

test-cluster

Your Trial license will expire on April 6, 2017.

Top Cluster Alerts

This cluster is running with multiple versions of Logstash. Versions: [5.2.1, 5.2.2].
March 7, 2017 10:18:01 PM

Always Actionable

Elasticsearch cluster status is yellow. Allocate missing replica shards.
March 7, 2017 10:18:01 PM

Last Checked

View all alerts

Elasticsearch

Health

Overview
Version: 6.0.0-alpha1
Uptime: 25 minutes

Nodes: 1
Disk Available: 401GB / 465GB (86.34%)
JVM Heap: 18.01% (363MB / 2GB)

Indices: 11
Documents: 16,836
Disk Usage: 15MB
Primary Shards: 11
Replica Shards: 0

Kibana

Health

Overview
Requests: 3
Max. Response Time: 115 ms

Instances: 1
Connections: 0
Memory Usage: 4.87% (70MB / 1GB)

x-pack

Security

elastic

elastic on 2017

Certificate Generation Utility (5.0)

x-pack

Simple CLI tool with a specific purpose

```
$ cat instances.yml
instances:
  - name: "node1"
    ip:
      - "192.0.2.1"
    dns:
      - "node1.mydomain.com"
  - name: "node2"
    ip:
      - "192.0.2.2"
      - "198.51.100.1"
  - name: "node4"
    dns:
      - "node4.mydomain.com"
      - "node4.internal"
  - name: "CN=node5,OU=IT,DC=mydomain,DC=com"
    filename: "node5"
$ bin/x-pack/certgen -in instances.yml -out certificate-bundle.zip
```

Certificate Generation Utility

```
$ unzip certificate-bundle.zip
$ tree
.
├── ca
│   ├── ca.crt
│   └── ca.key
├── certificate-bundle.zip
├── node1
│   ├── node1.crt
│   └── node1.key
├── node2
│   ├── node2.crt
│   └── node2.key
├── node4
│   ├── node4.crt
│   └── node4.key
└── node5
    ├── node5.crt
    └── node5.key
```

Consistent TLS Configuration

Setting pattern consistent across the stack

```
xpack.ssl.key:                      "/home/es/config/x-pack/node01.key"
xpack.ssl.certificate:              "/home/es/config/x-pack/node01.crt"
xpack.ssl.certificate_authorities: [ "/home/es/config/x-pack/ca.crt" ]
```

Consistent responses (5.1)

Without X-Pack:

```
$ curl -u elastic localhost:9200/_cat/indices
$
```

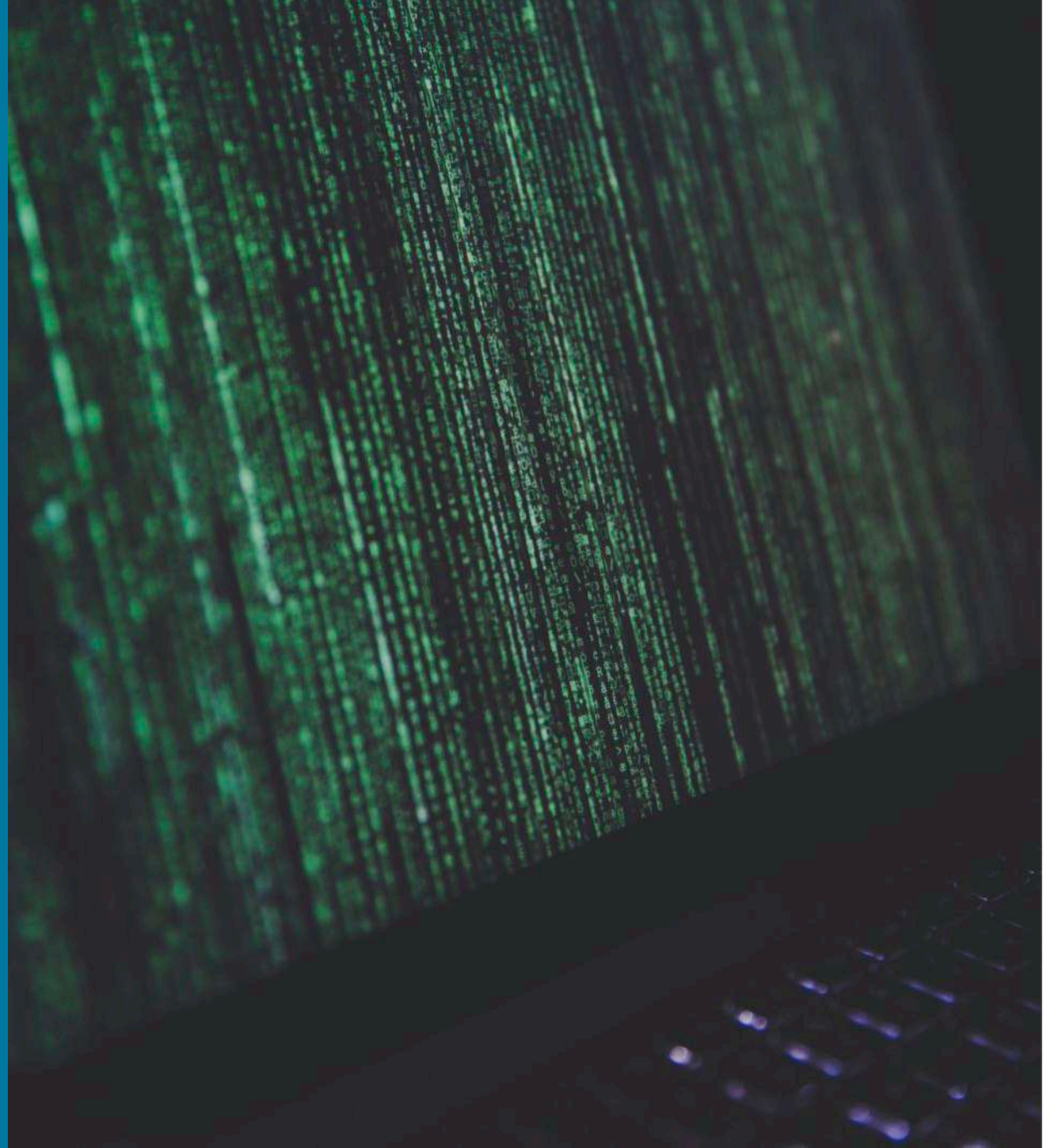
X-Pack 5.0:

```
$ curl -u elastic localhost:9200/_cat/indices
{"error":{"root_cause":[{"type":"index_not_found_exception","reason":"no such
index","index_uuid":"_na_","index":"_all"}],"type":"index_not_found_exception","reason":"no such
index","index_uuid":"_na_","index":"_all"},"status":404}
$
```

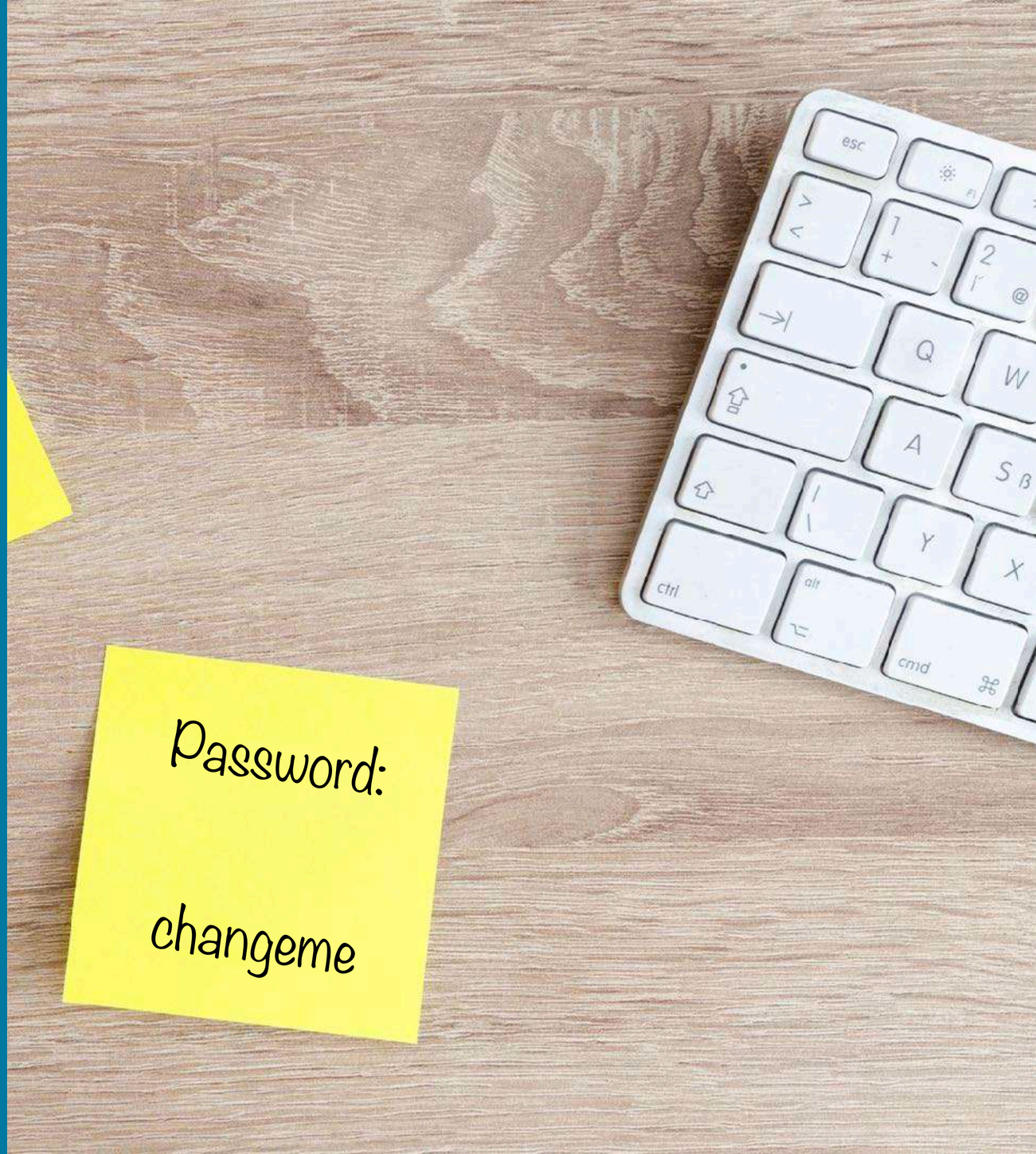
X-Pack 5.1+:

```
$ curl -u elastic localhost:9200/_cat/indices
$
```

TLS only for node to node transport



Goodbye Default Passwords

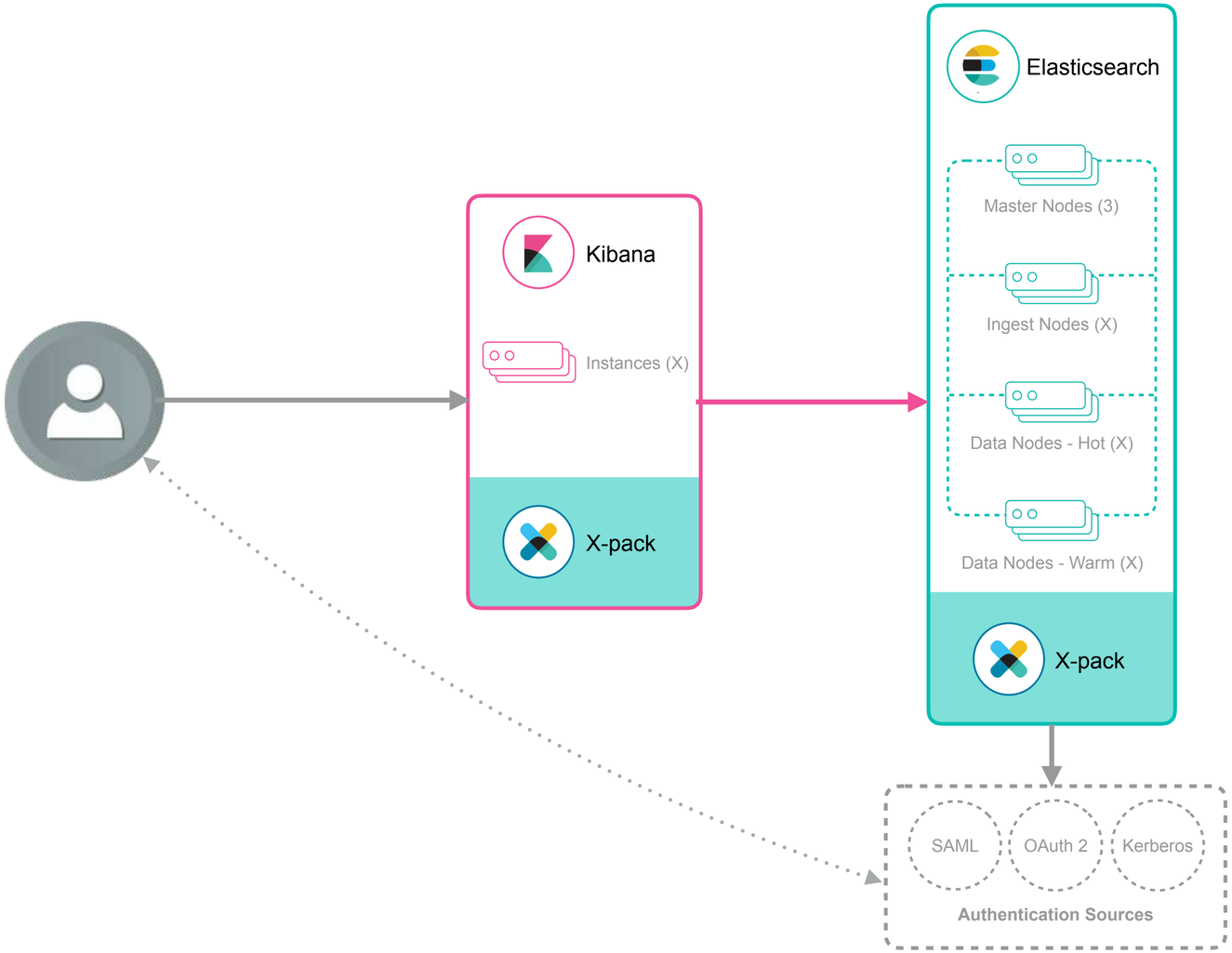


Passwords removed from configuration files

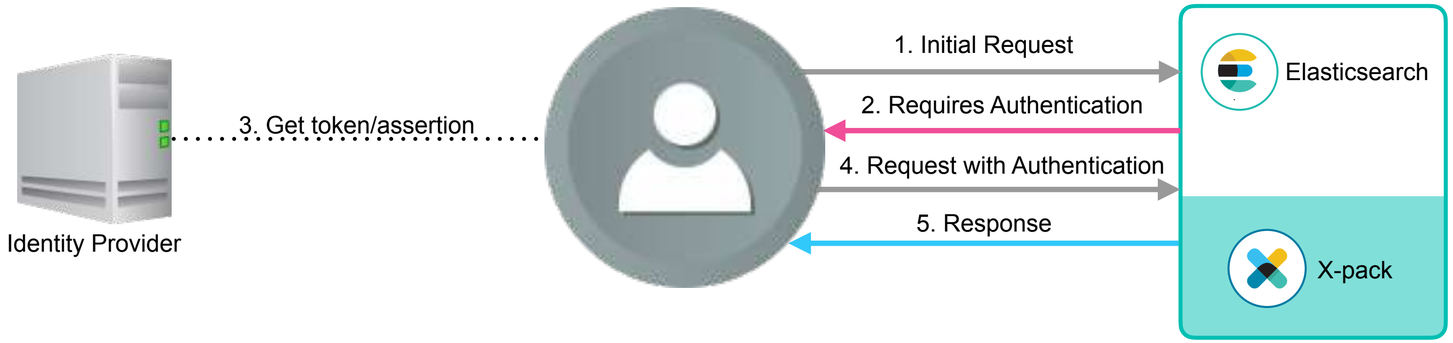
```
xpack:
  security:
    ssl:
      key: '/etc/elasticsearch/config/x-pack/node1.key'
      key_passphrase: 'my super secret password is changeme!'
      certificate: '/etc/elasticsearch/config/x-pack/node1.crt'
    transport:
      ssl:
        enabled: true
```

Single Sign On

x-pack



Generalized Single Sign On Flow



x-pack

Reporting

elastic

elastic on 2017

Google

Gmail

More

COMPOSE

Inbox
Starred
Important
Sent Mail
Drafts (2)
Personal

Brandon

Make a call

Also try our mobile apps for Android and iOS

Primary

Your Primary tab is empty.

Personal messages and message

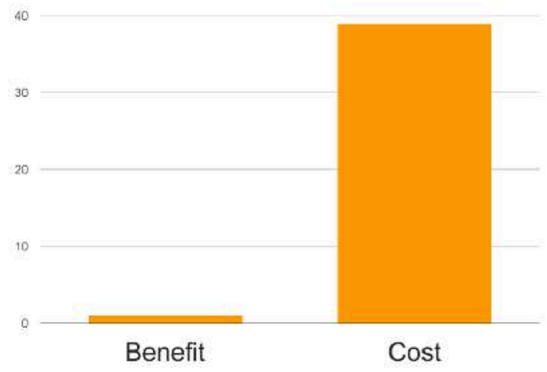
To add or remove tabs click inbox

0.47 GB (3%) of 15 GB used
Manage

Control Library Cost/Benefit

boss@company.com

Control Library Cost/Benefit



Send

Saved

Google

Gmail

More

1–1 of 1

COMPOSE

Inbox (1)
Starred
Important
Sent Mail
Drafts (2)
Personal

Brandon

Make a call

Also try our mobile apps for Android and iOS

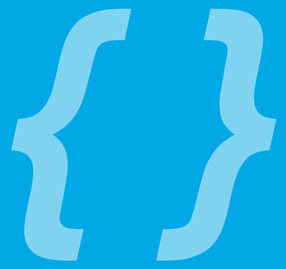
Primary | Social | Promotions

VP of Engineering	Invitation: Control Toolkit Alternatives @ Mon Feb 19, 2(	Feb 22

0.47 GB (3%) of 15 GB used
Manage

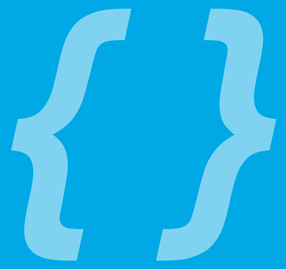
Terms - Privacy

Last account activity: 20 hours ago
Details



When numbers in tabular form are taboo and words will not do the work well, as is often the case, there is one answer left: Draw a picture.

Darrell Huff

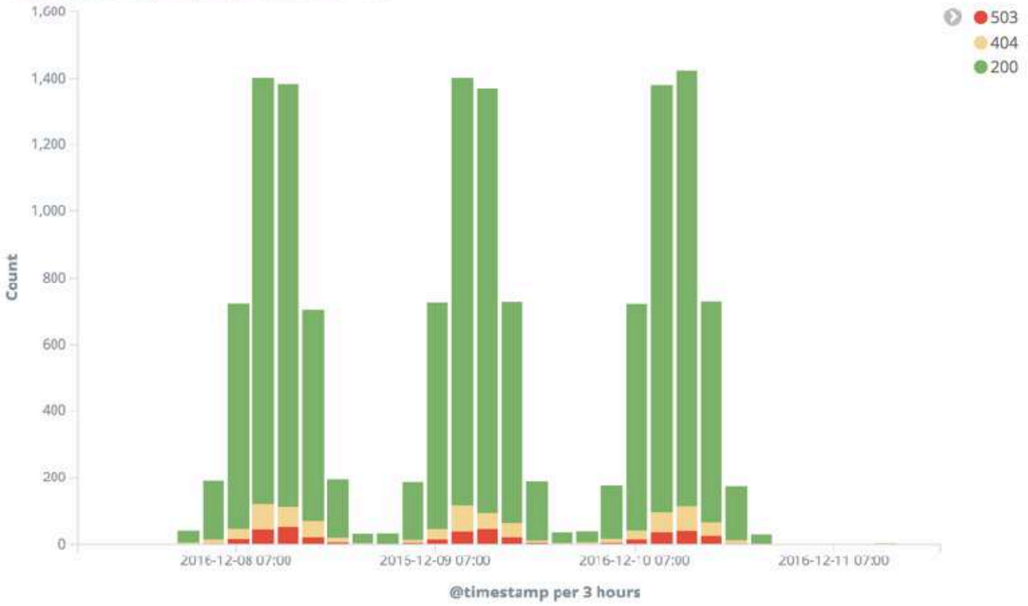


When numbers in tabular form are taboo and words will not do the work well, as is often the case, there is one answer left: Draw a picture.

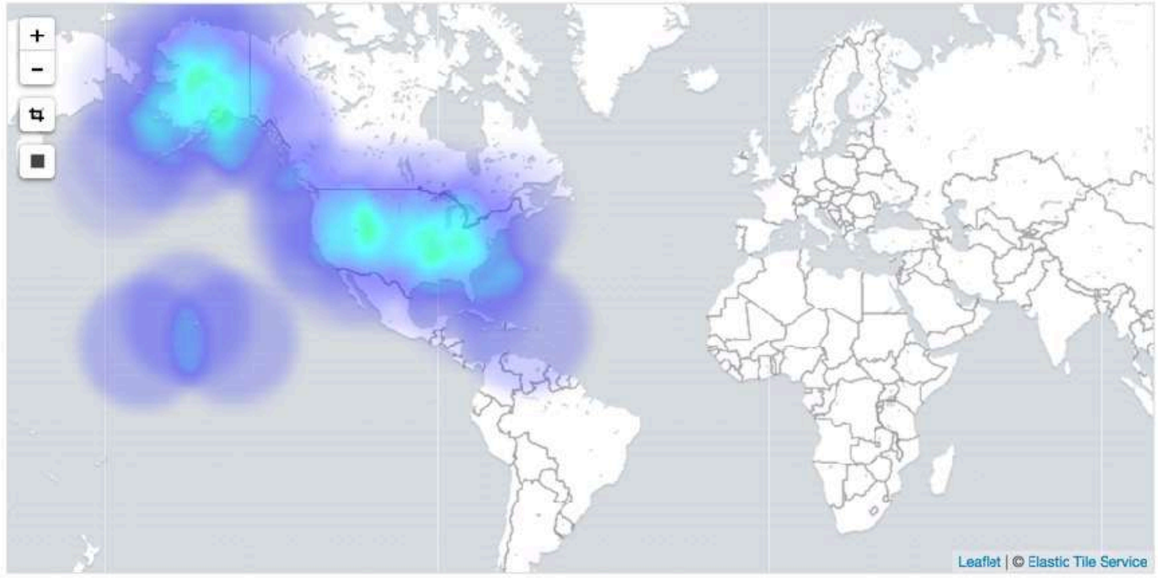
Darrell Huff ***"How to Lie with Statistics"***

Discover
Visualize
Dashboard
Timelion
Graph
Dev Tools
Monitoring
Management

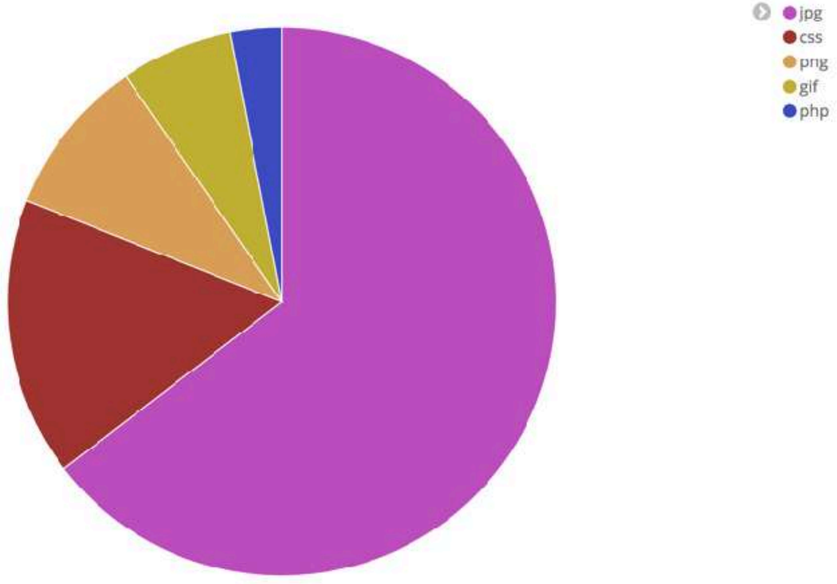
Request Count by Response Codes Over Time



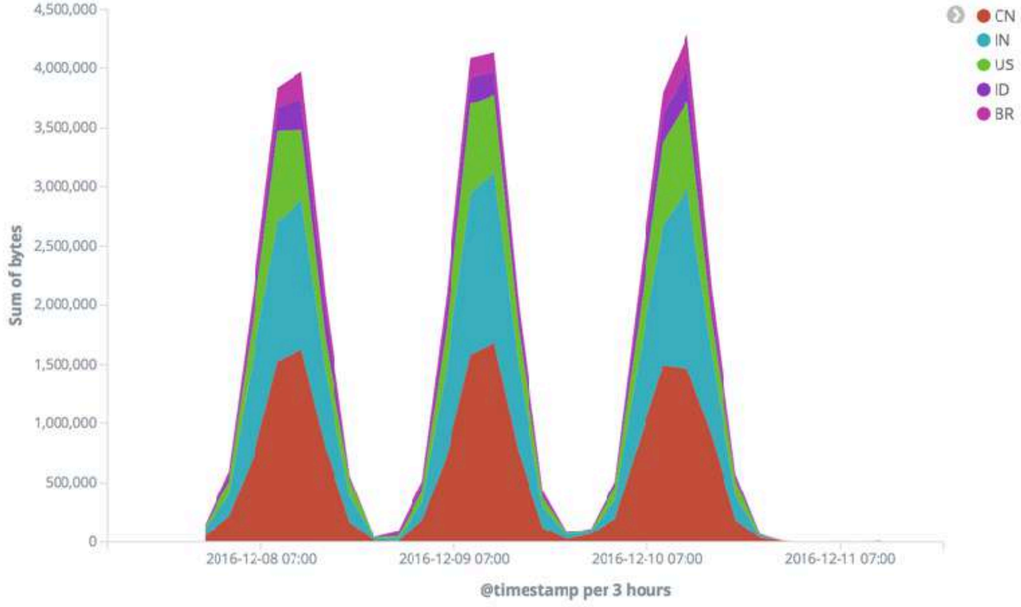
Requests by Geographic Source



Bandwidth by Resource Extension

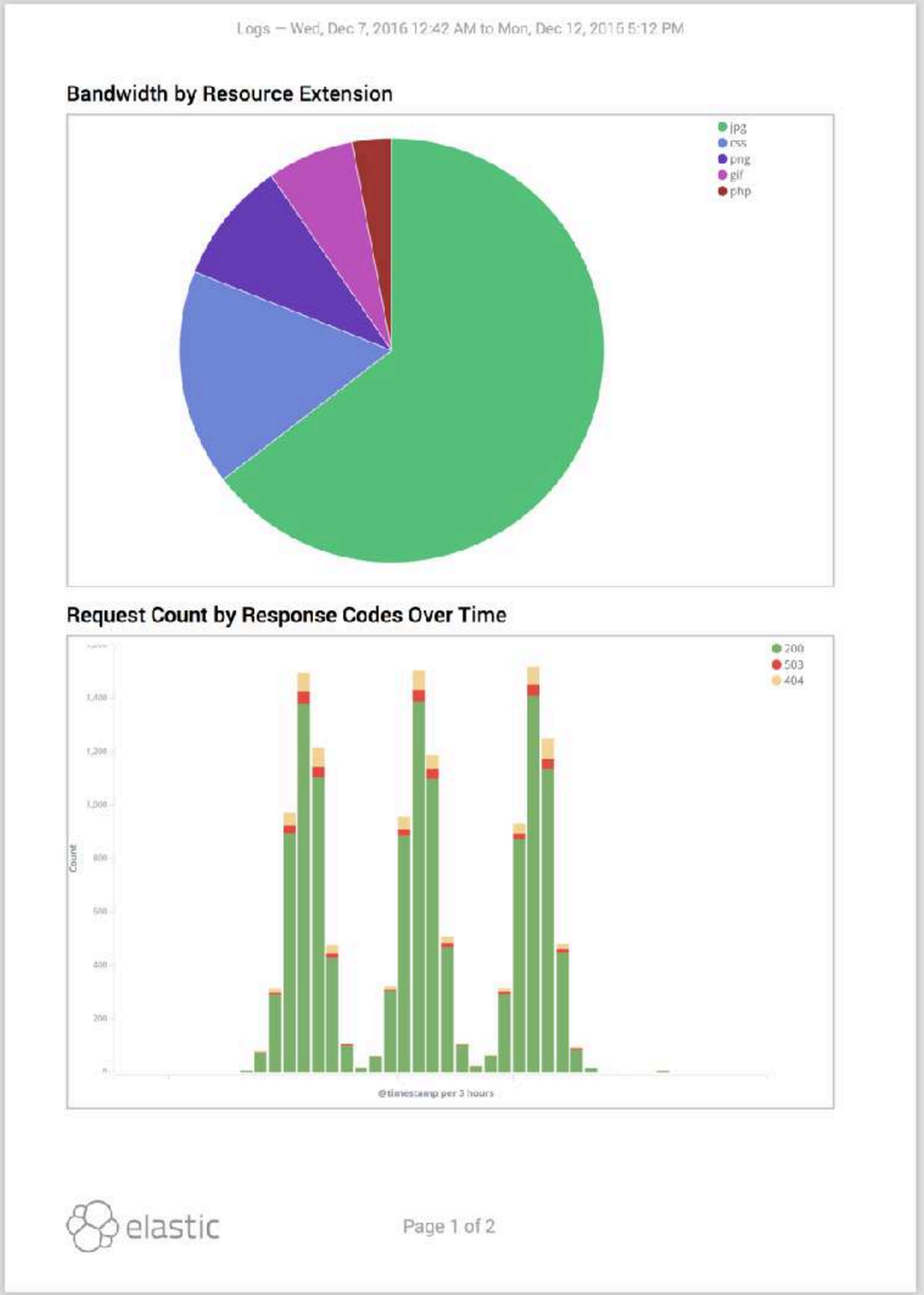


Bandwidth by Geographic Source Over Time

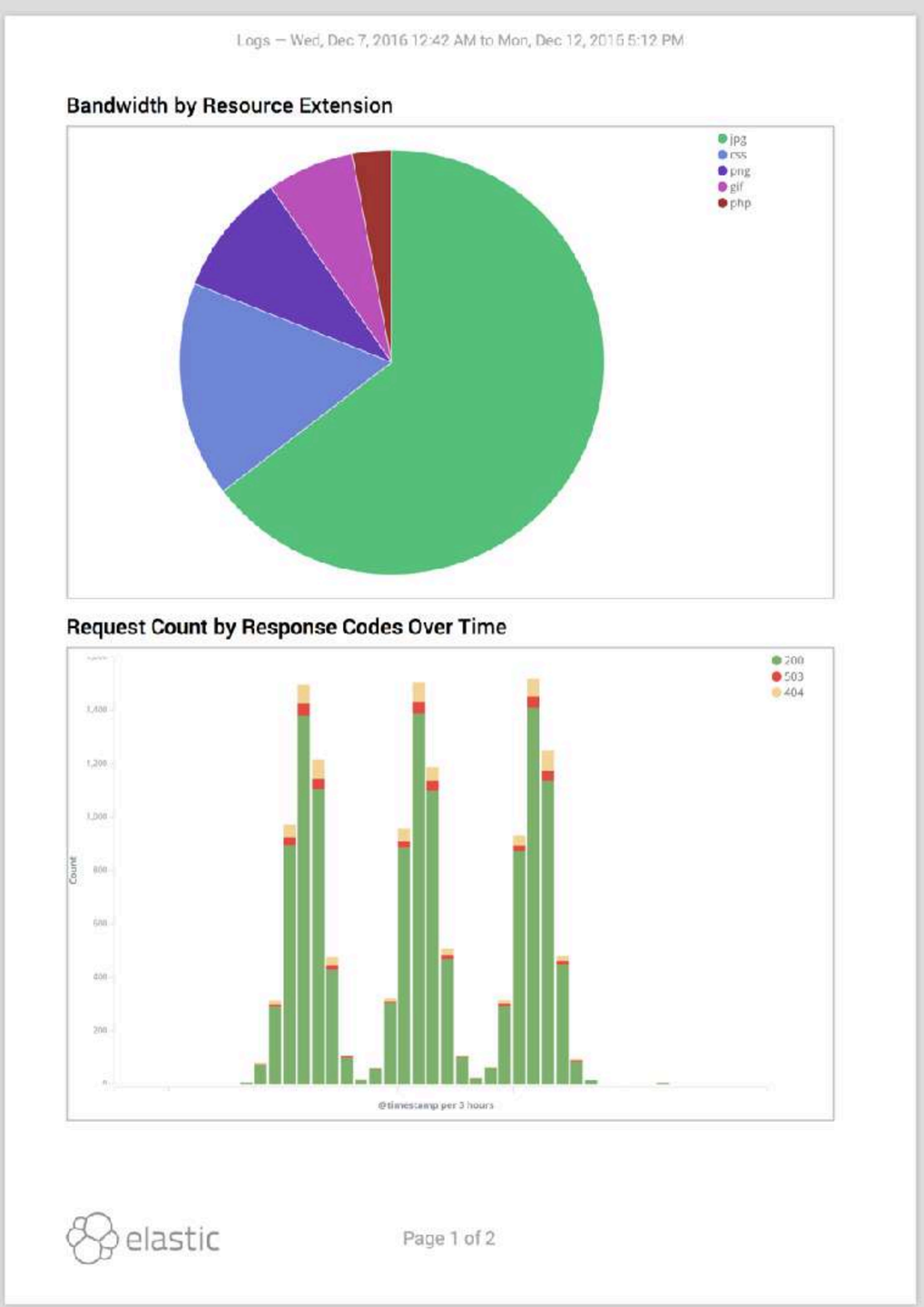


elastic
Logout
Collapse

Downloadable PDF



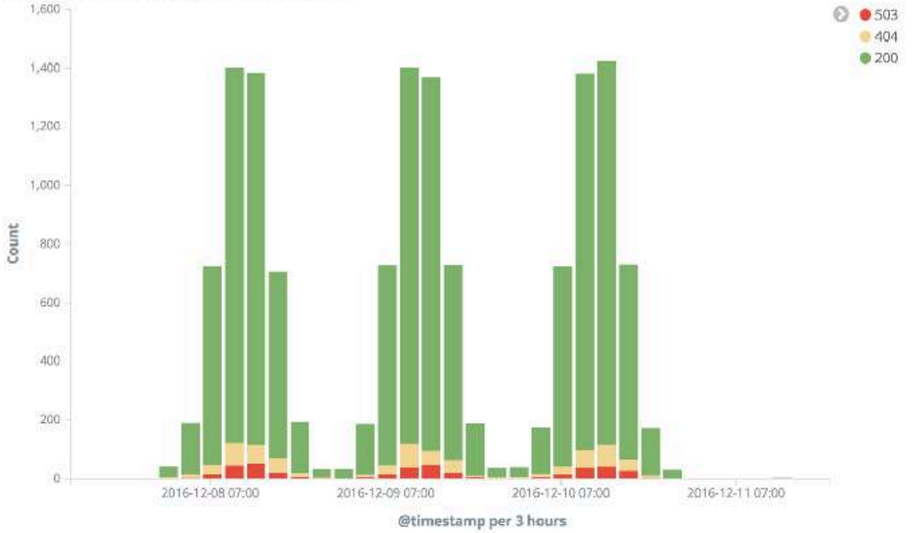
Utilizes Existing Infrastructure



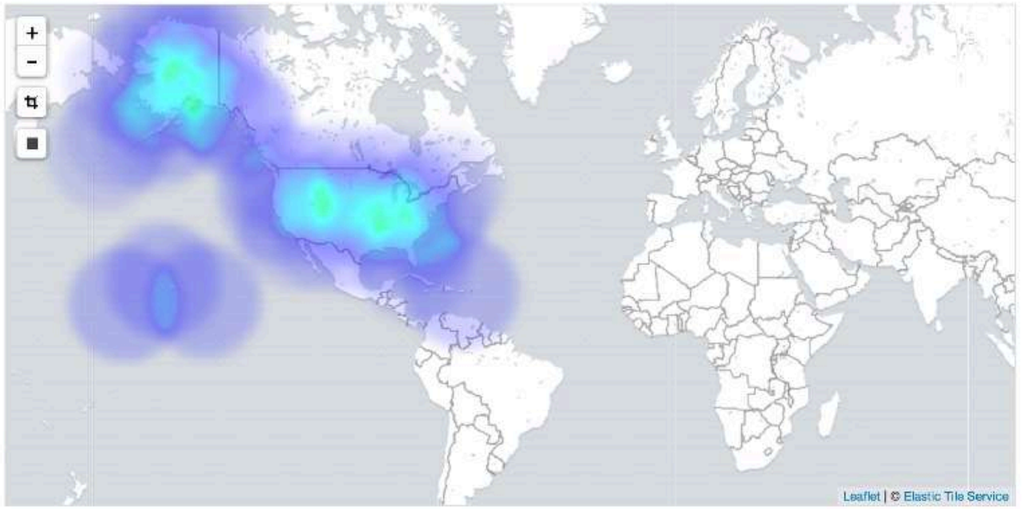
What’s Next?

More Layout Options

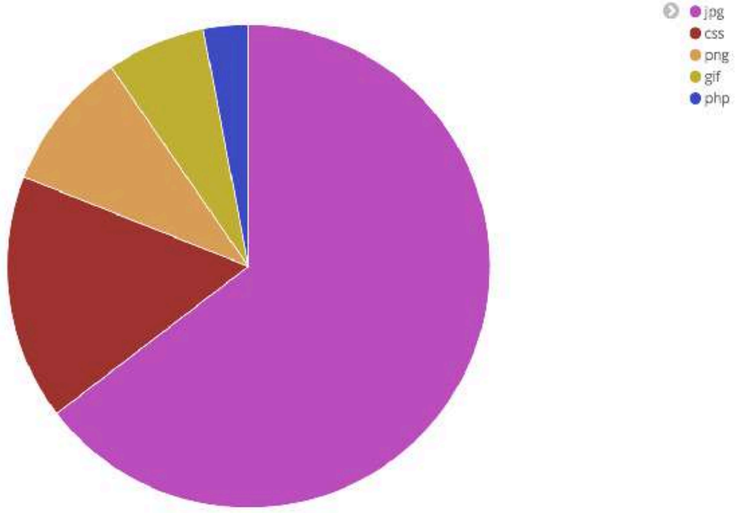
Request Count by Response Codes Over Time



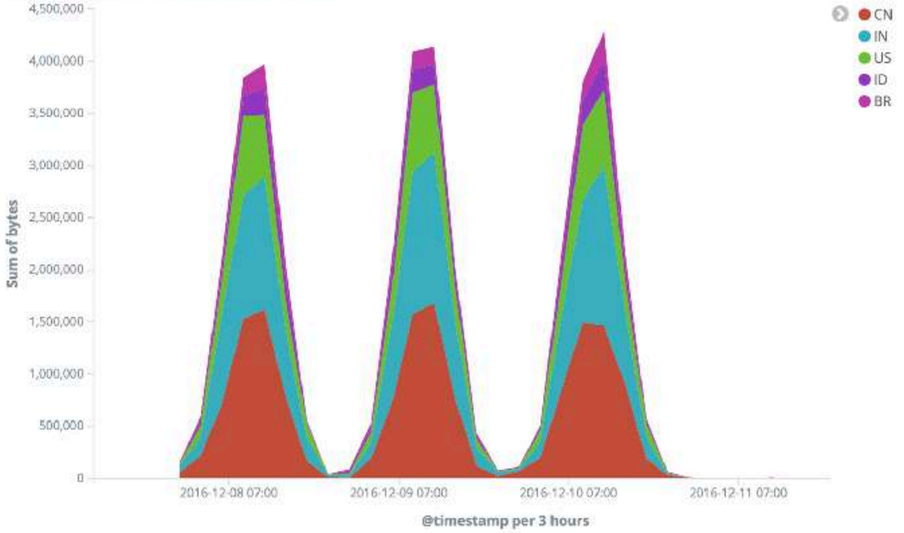
Requests by Geographic Source



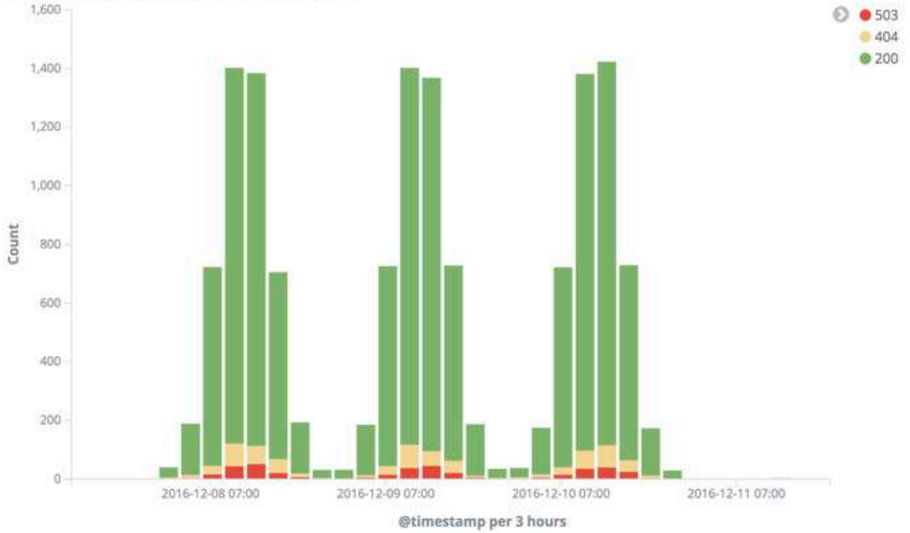
Bandwidth by Resource Extension



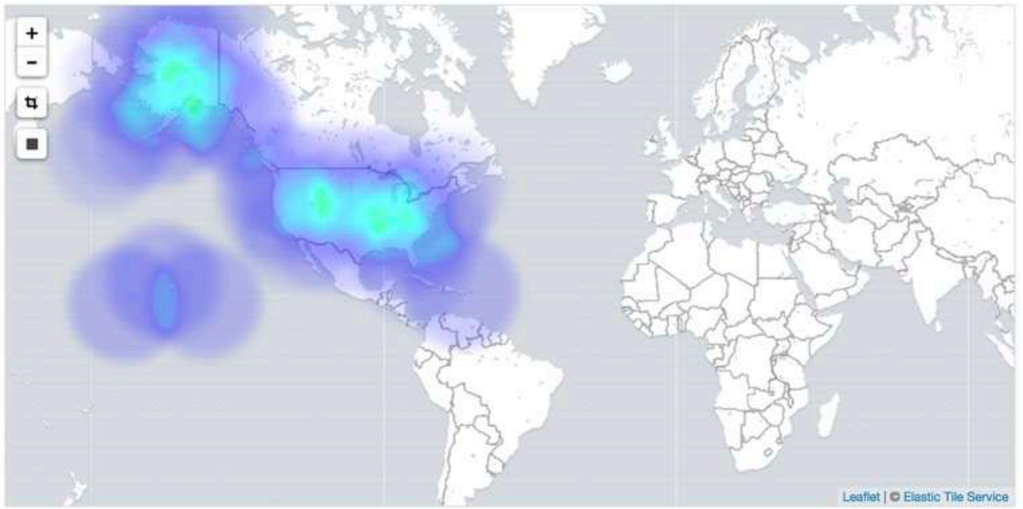
Bandwidth by Geographic Source Over Time



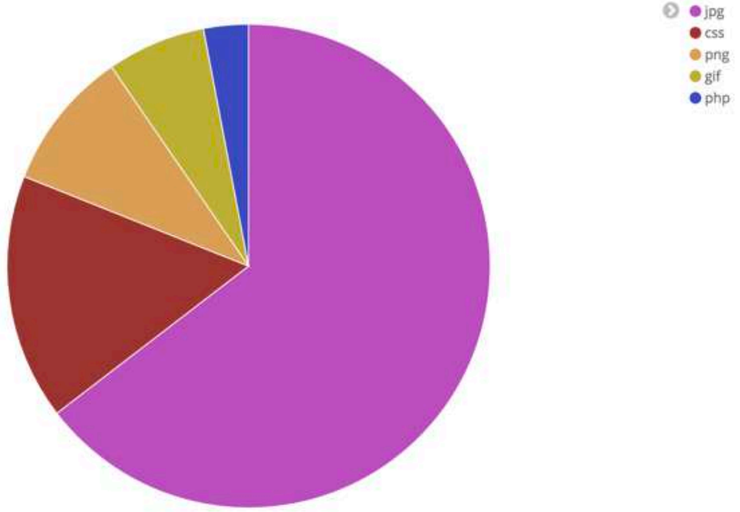
Request Count by Response Codes Over Time



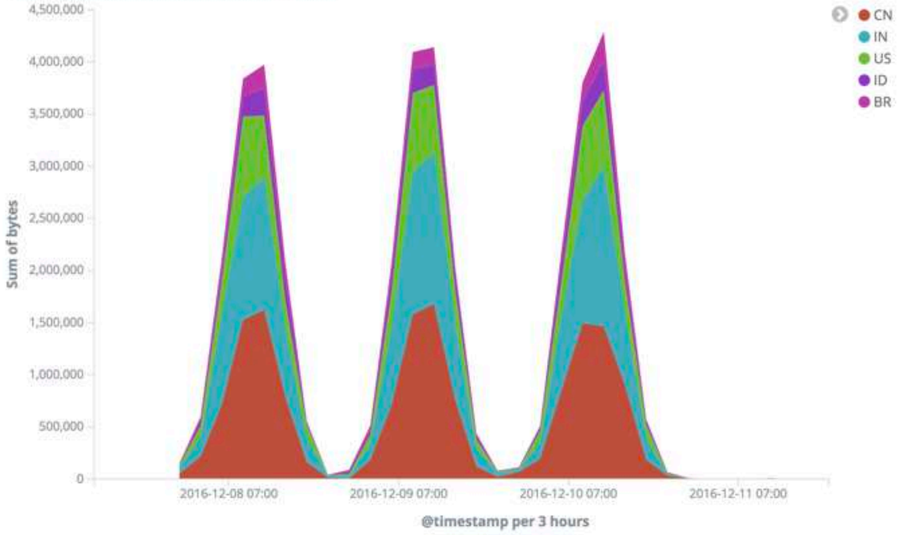
Requests by Geographic Source



Bandwidth by Resource Extension



Bandwidth by Geographic Source Over Time

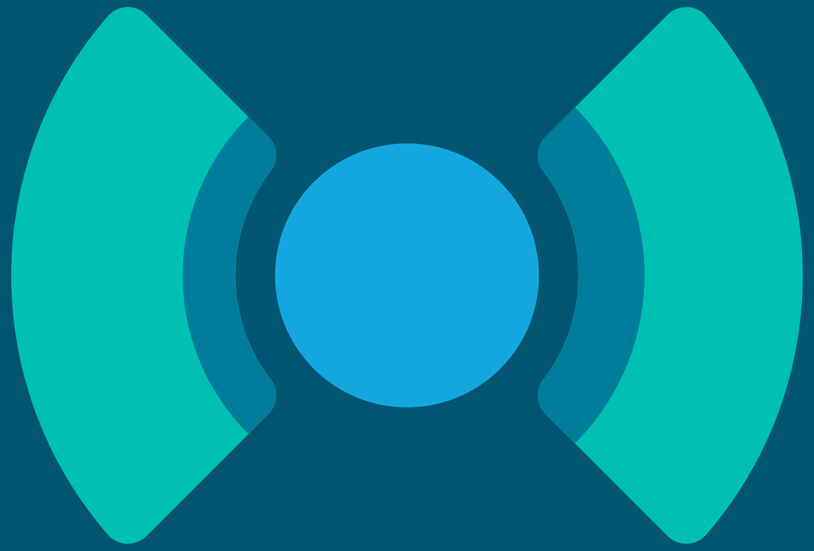


ACME

Additional Output Formats

EXPORT TO CSV

x-pack



Alerting

elastic

elastic on 2017

Alerting: **Past**, present & future

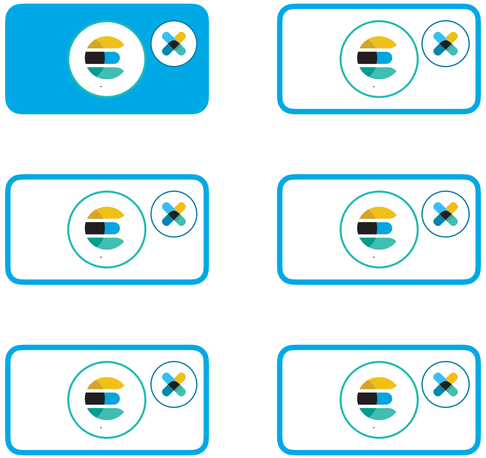
x-pack

- Versioned watch history templates
- Conditions per action
- JIRA action
- Email action: Reporting integration (backported to 2.4)
- Index action: Specify document id (5.3)

Alerting: Past, **present** & future

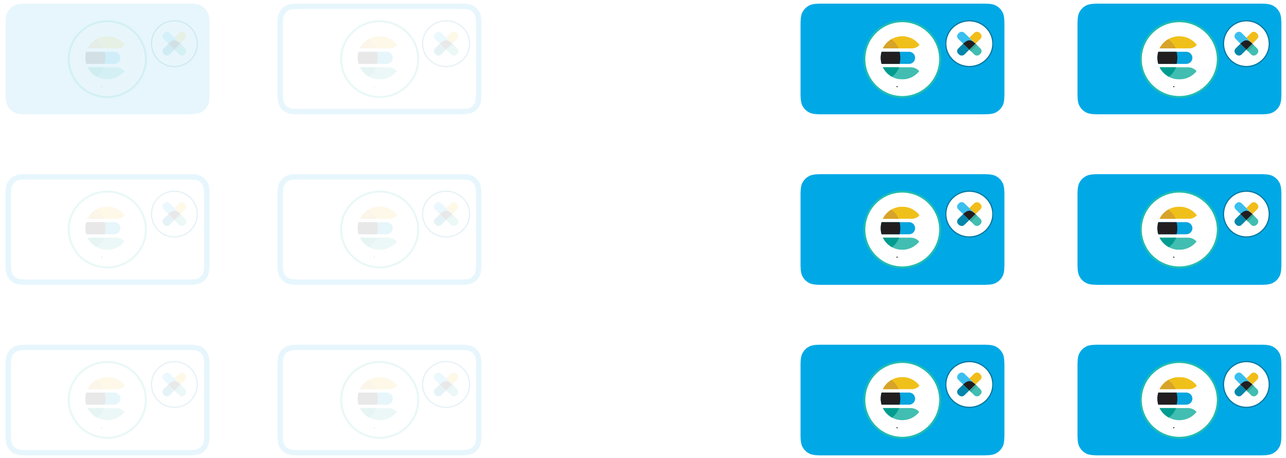
x-pack

- Watch execution happens on master node



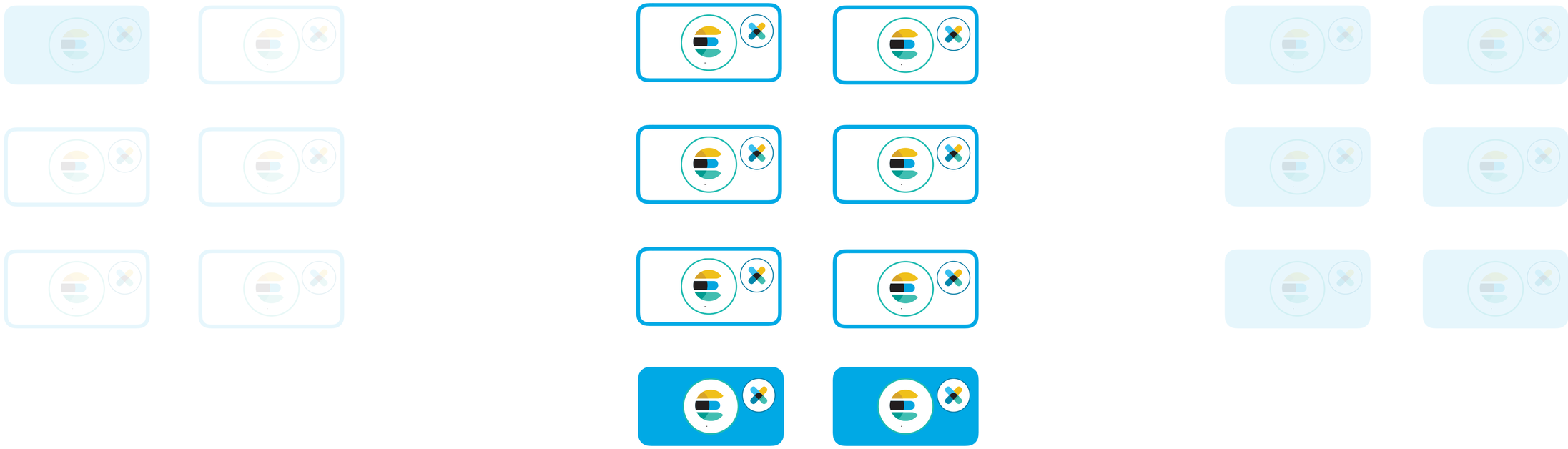
Alerting: Past, **present** & future

- Watch execution should happen on all nodes



Alerting: Past, **present** & future

- Watch execution should happen on all nodes



Alerting: Distributed watch execution

x-pack

- Move execution to data nodes, where the `.watches` shards are
- No single point of failure
- Master node does not do any workload
- Add replicas on the fly to scale out execution
- Shard Allocation Filtering allows for dedicated watcher nodes
- Fully backwards-compatible on API level

Alerting: Past, present & **future**

x-pack

- Structure of a single watch is too static
- The order of execution is simple
  - **`input -> condition -> actions`**
- What if you wanted:
  - **`input -> condition -> input -> input -> if -> email -> else -> logging`**
- Keep state between watch executions
- Making the core execution async

Alerting: One last thing...

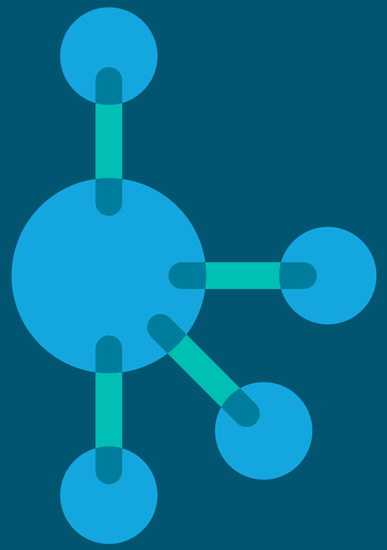
x-pack

DEMO

elastic

elastic on 2017

x-pack



Graph

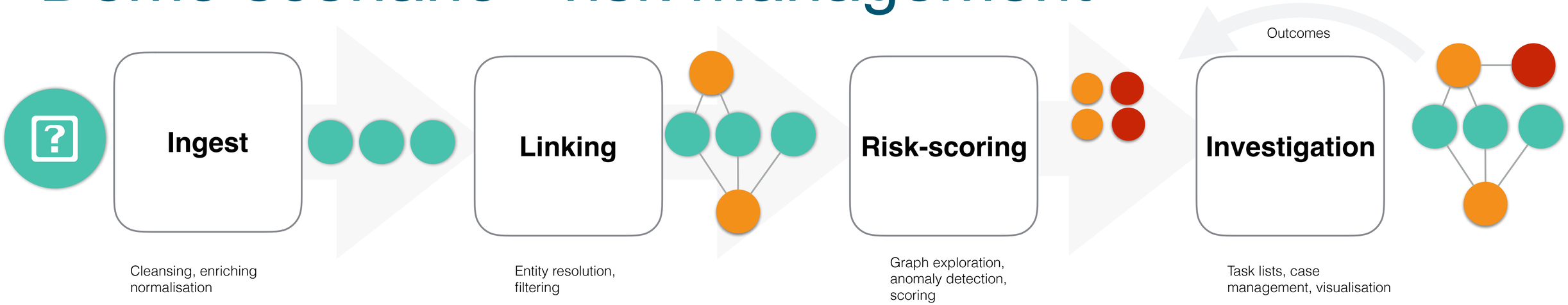
New Graph UI features

x-pack

- Explore across multiple indices
- Simplified field configuration
- Saveable/shareable workspaces
- Deep linking into Graph
- Deep linking out of Graph

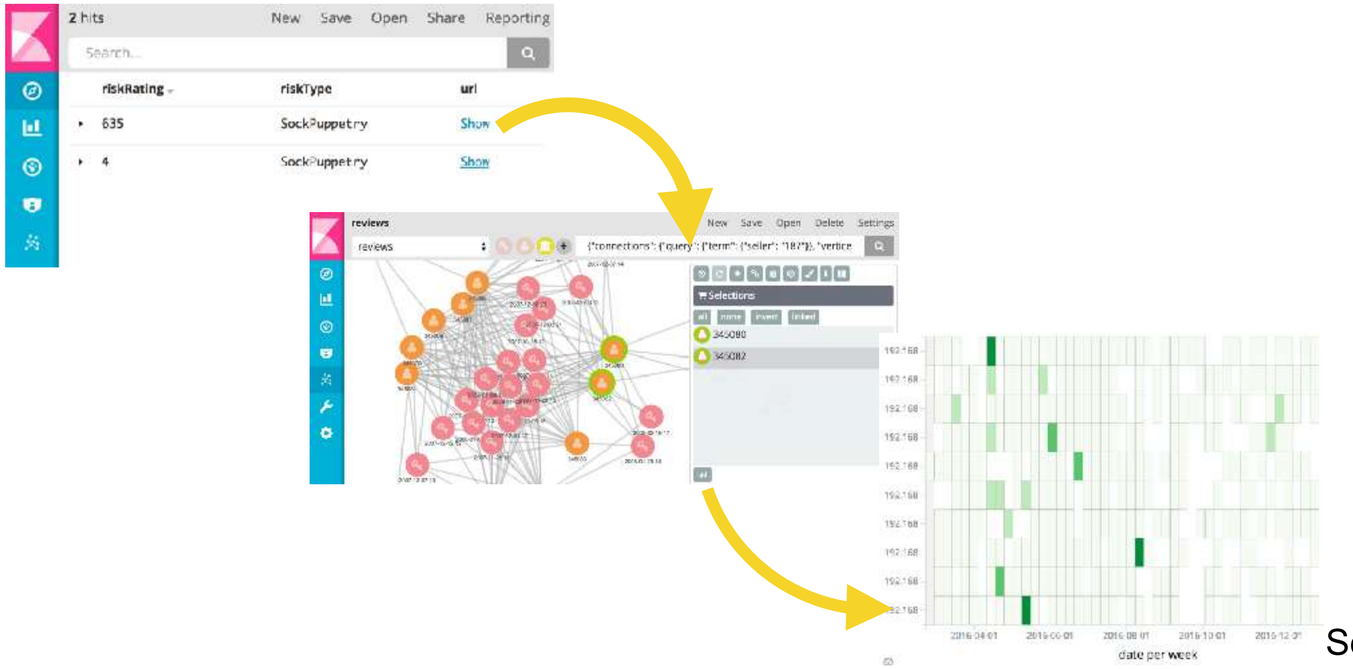
Demo scenario - risk management

x-pack



Responding to risk alerts

x-pack



See example: http://bit.ly/es_fraud

x-pack

DEMO

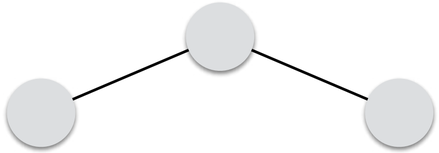
elastic

elastic on 2017

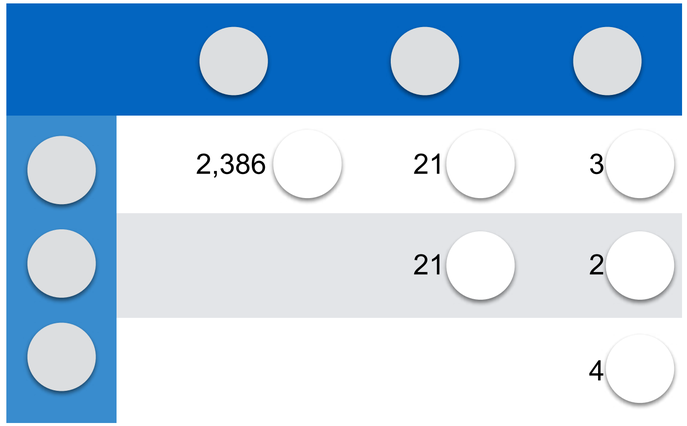
x-pack

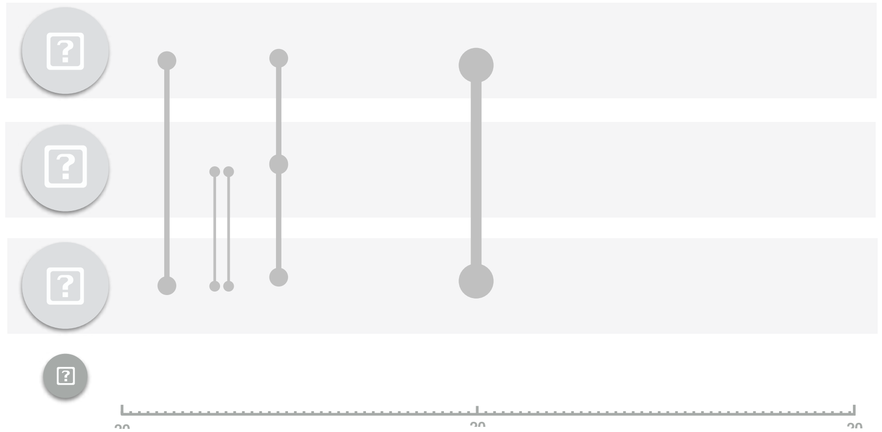
Graph futures

More details behind connections, more perspectives



adjacency_matrix aggregation





with nested aggregations…

= graphs over time visualizations

Other Talks You Should See

x-pack

- BoF: Alerting Use-Cases, today, 1:15
- BoF: Effectively Using Monitoring, today, 3:15
- X-Pack Enablement Security Workshop, Thursday, 9:00
- Getting Your Data Graph Ready, Thursday, 12:45
- The Usual Suspects: Automatic Alerts to Monitor your Cluster, Thursday, 1:45

More Questions?

Visit us at the AMA

www.elastic.co

Please attribute Elastic with a link to elastic.co

Except where otherwise noted, this work is licensed under
http://creativecommons.org/licenses/by-nd/4.0/

Creative Commons and the double C in a circle are
registered trademarks of Creative Commons in the United States and other countries.
Third party marks and brands are the property of their respective holders.