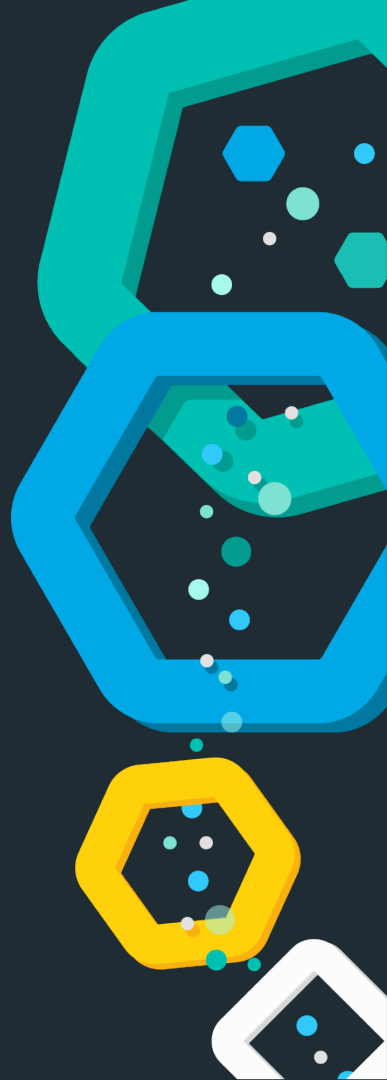
elastic

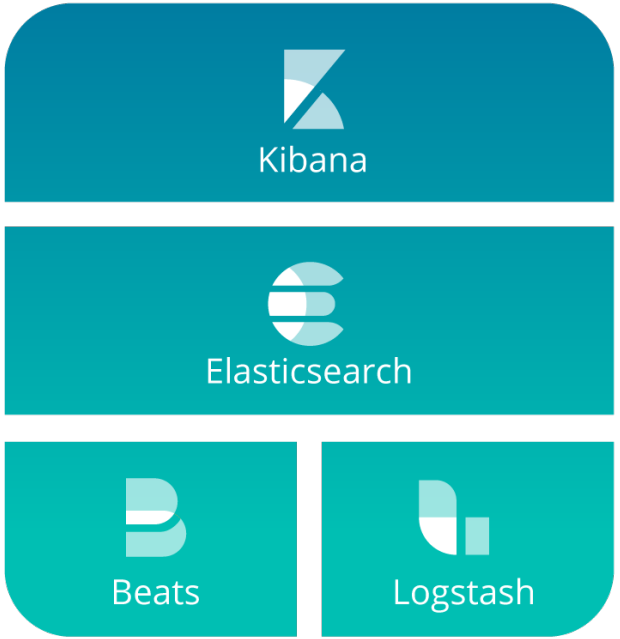
PRODUCT OVERVIEW

Elastic Stack, X-Pack, and Elastic Cloud



Elastic Stack

100% open source



elastic

X-Pack

Single install
Extensions for the Elastic Stack
Subscription pricing

Security

Alerting

Monitoring

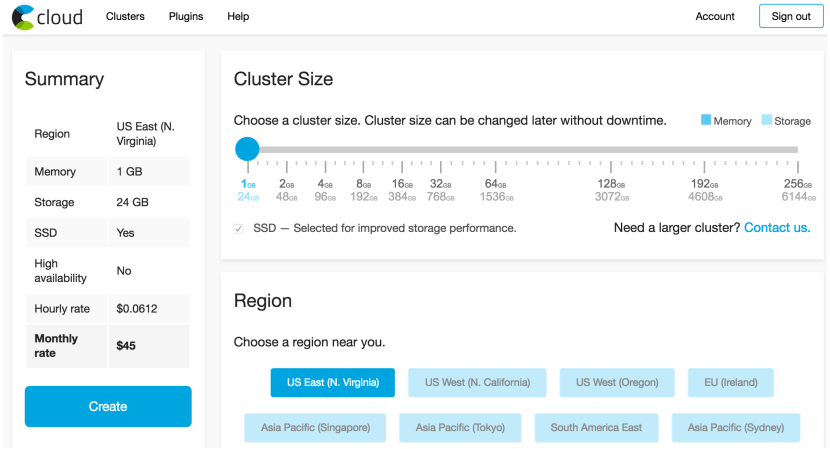
Reporting

Graph

Machine Learning

Elastic Cloud

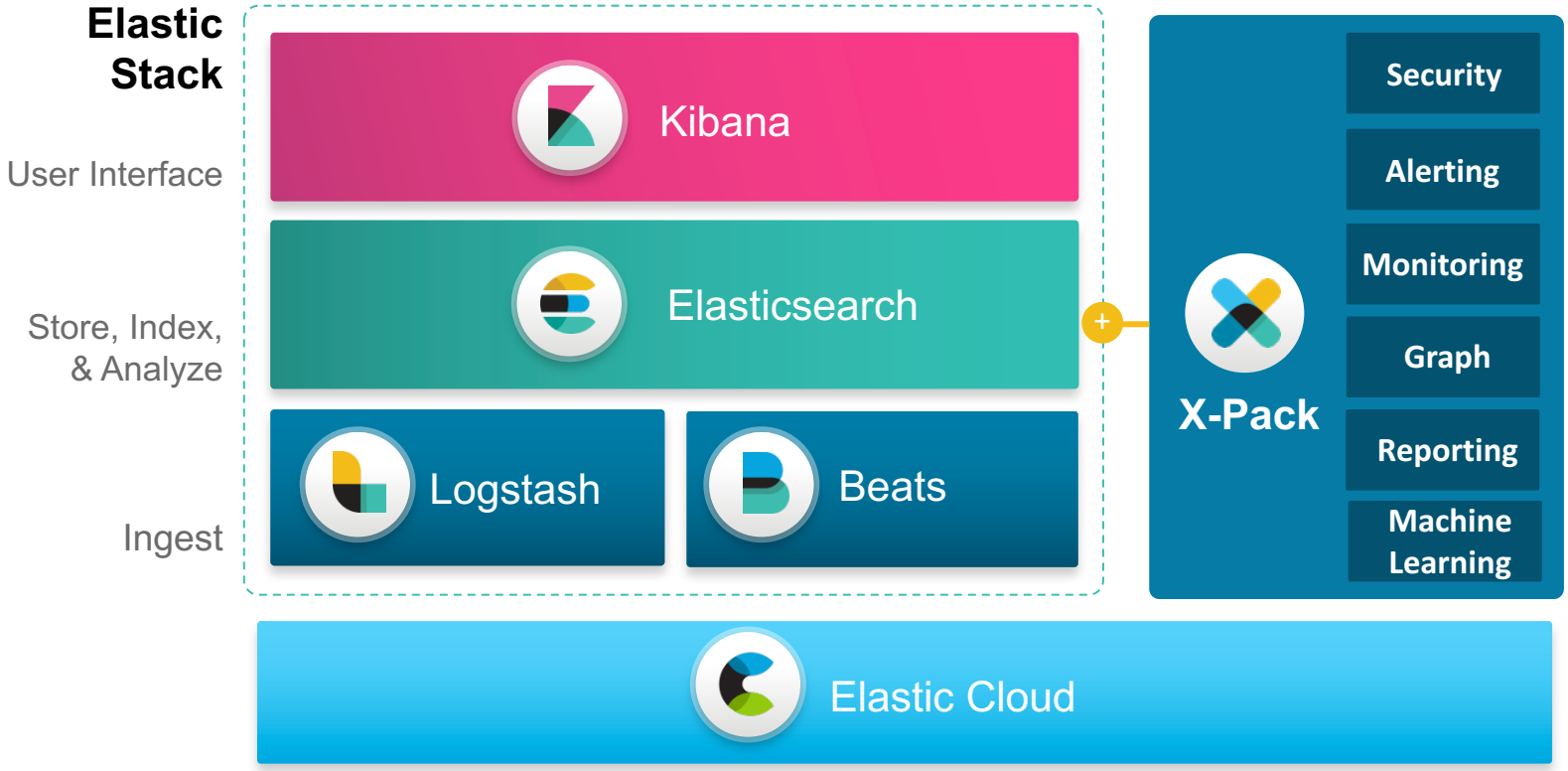
Hosted Elasticsearch & Kibana
Includes X-Pack features
Starts at $45/mo



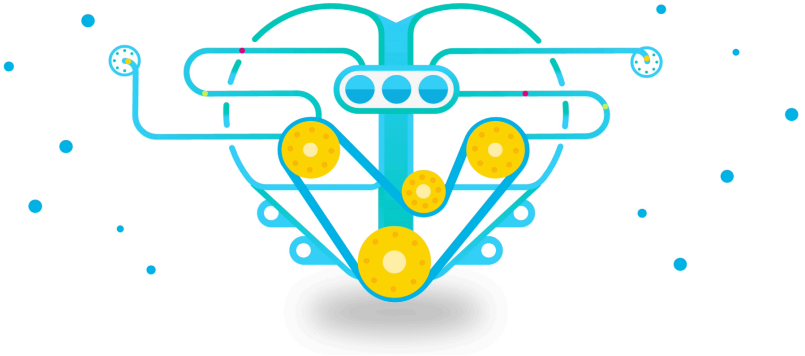
Available in AWS today
Available in Google Cloud Platform (soon)
Available as a private cloud/on-premise solution
(Elastic Cloud Enterprise)

elastic

Elastic: Product Portfolio



elastic



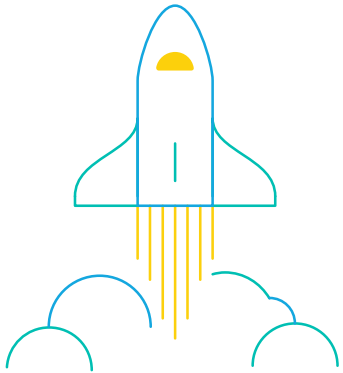
Elasticsearch

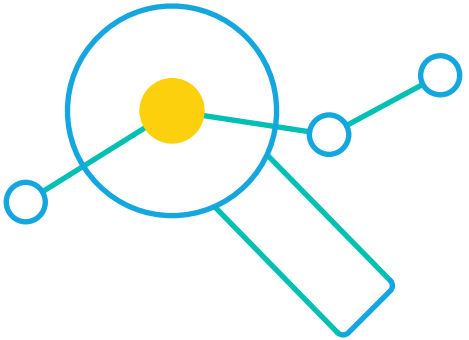
Heart of the Elastic Stack

Distributed, Scalable	**High-availability**	**Multi-tenancy**
Developer Friendly	**Real-time, Full-text Search**	**Aggregations**

Elasticsearch is…

An open source, distributed, scalable, highly available, document-oriented, RESTful, full text search engine with real-time search and analytics capabilities

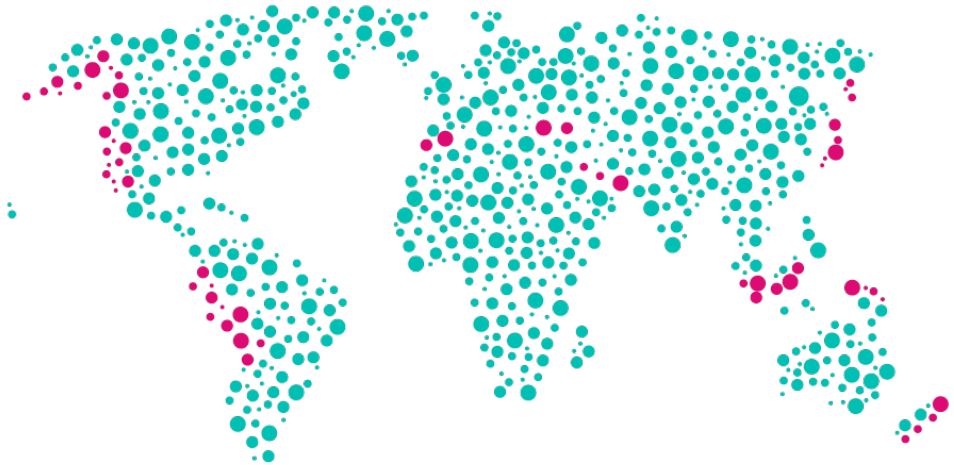





elastic

Kibana

Window into the Elastic Stack



Visualize and analyze	**Geospatial**	**Customize and Share Reports**
Graph Exploration	**UX to secure and manage the Elastic Stack**	**Build Custom Apps**

elastic

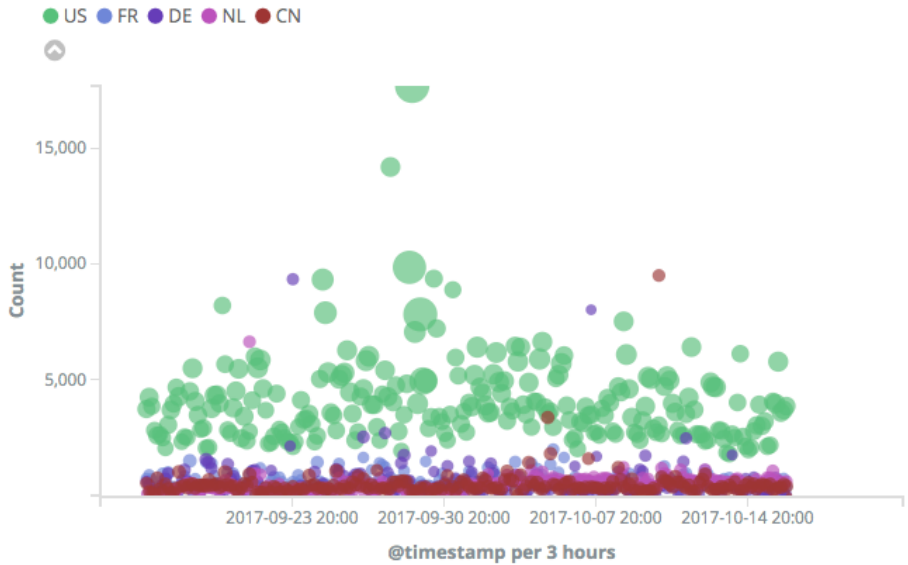
Apache - Total Visitors

2,317,838

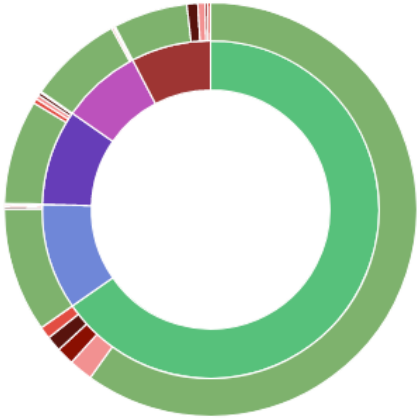
Apache - Unique Visitors

29,740

Apache - Bytes and Count



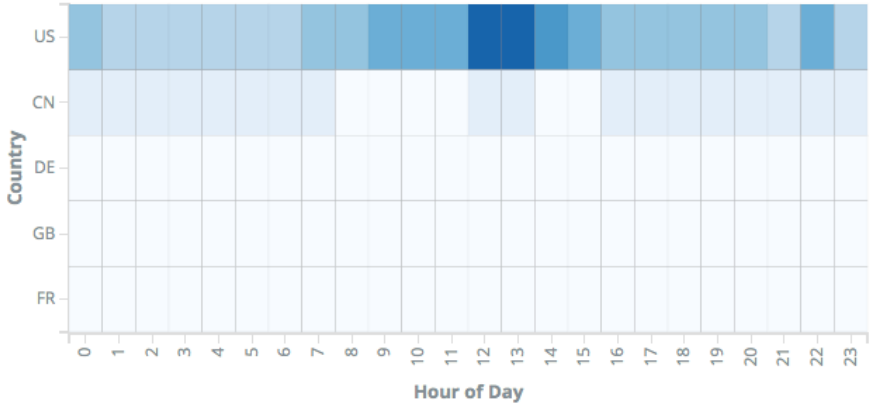
Apache - Country and Status



Apache - Unique Visitor...

City	Count of Unique Clients
Beijing	569
Ashburn	397
Redmond	383
Chicago	379
London	248
Los Angeles	232

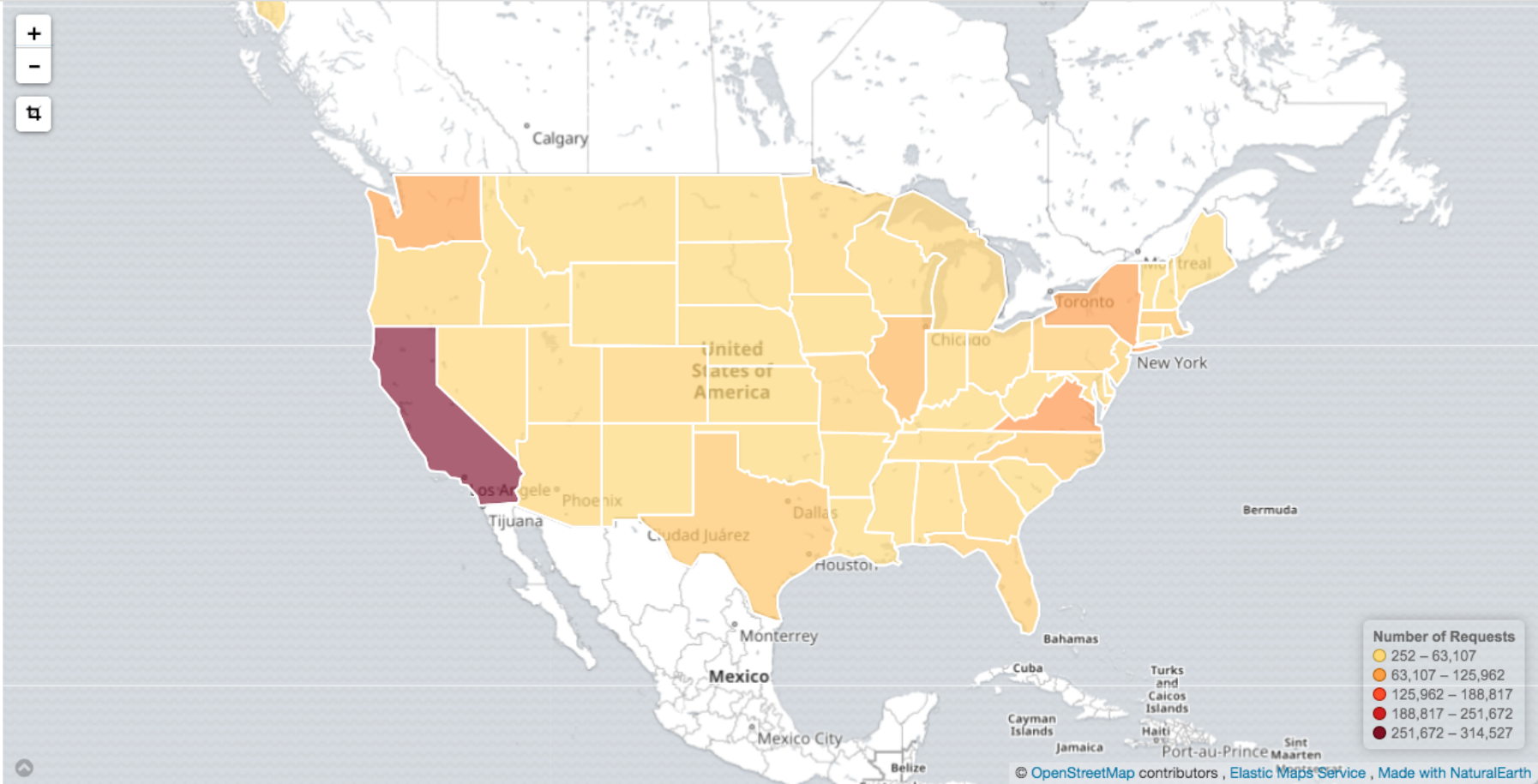
Apache - Country traffic by hour



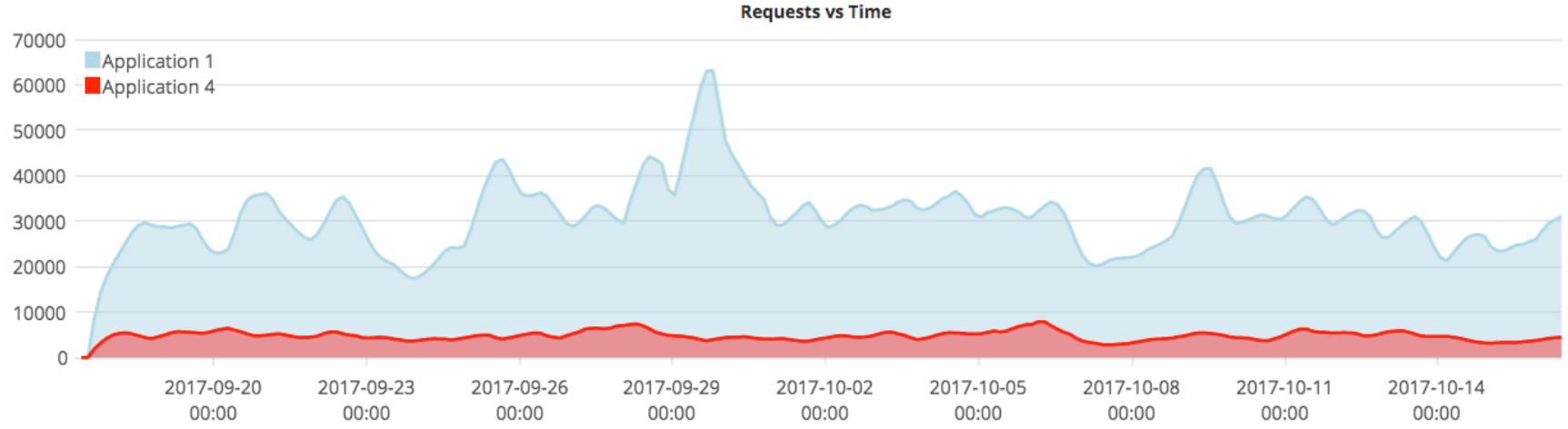
Apache - Top OS small

apache2.access.geoip.country_iso_code:US Uses lucene query syntax

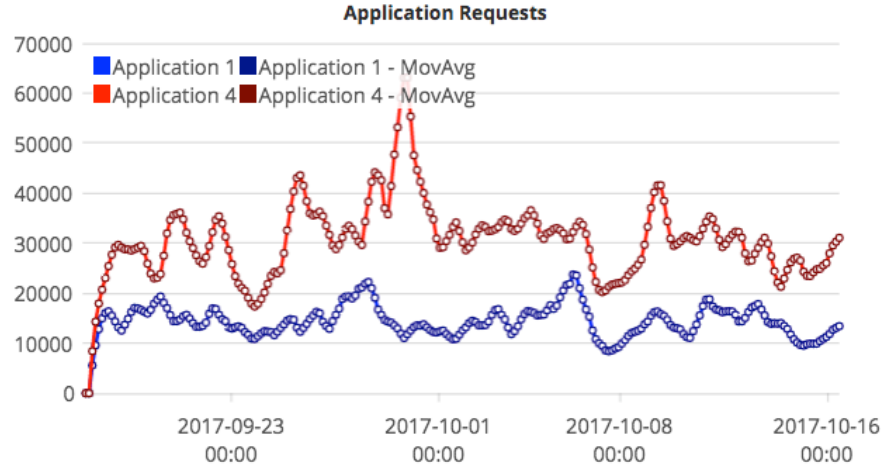
apache2.access.geoip.country_iso_code: "US" Add a filter + Actions



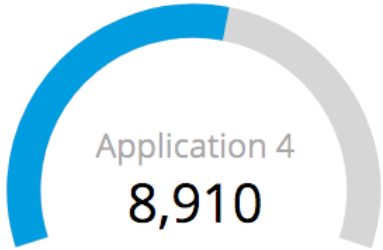
TS - Req v Time



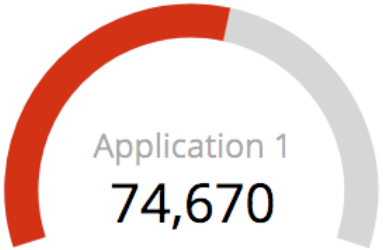
TS - App Requests

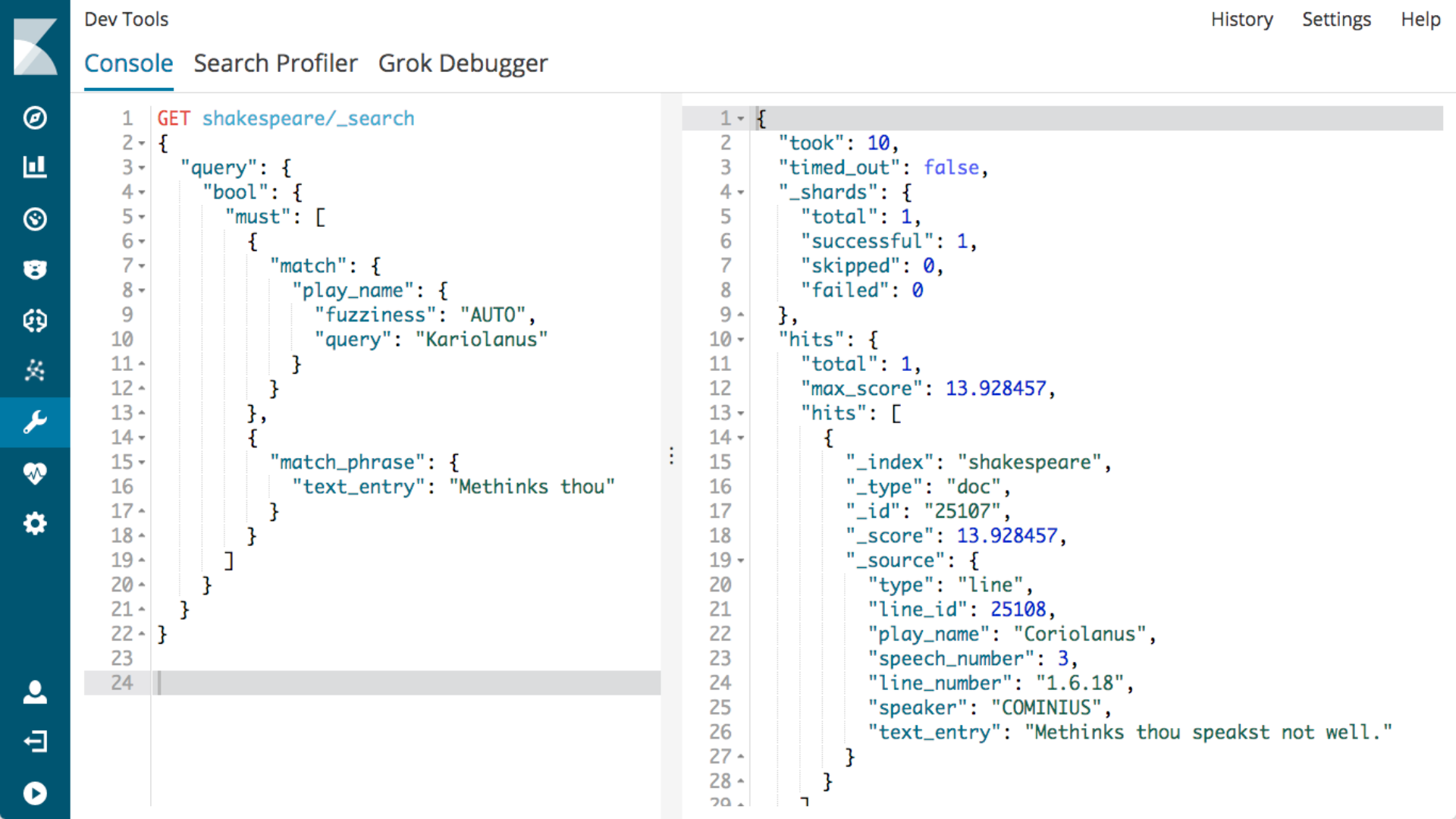


TS - App4



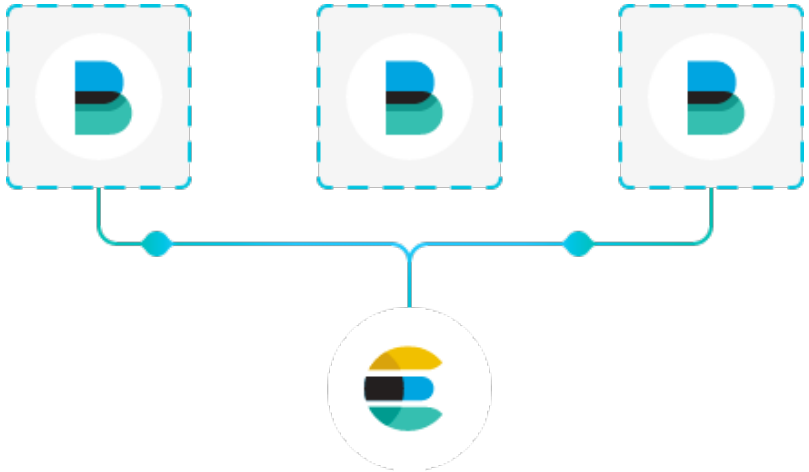
TS - App1



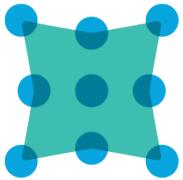

Dev Tools
History
Settings
Help
Console
Search Profiler
Grok Debugger
GET shakespeare/_search
{
"query": {
"bool": {
"must": [
{
"match": {
"play_name": {
"fuzziness": "AUTO",
"query": "Kariolanus"
}
}
},
{
"match_phrase": {
"text_entry": "Methinks thou"
}
}
]
}
}
}
{
"took": 10,
"timed_out": false,
"_shards": {
"total": 1,
"successful": 1,
"skipped": 0,
"failed": 0
},
"hits": {
"total": 1,
"max_score": 13.928457,
"hits": [
{
"_index": "shakespeare",
"_type": "doc",
"_id": "25107",
"_score": 13.928457,
"_source": {
"type": "line",
"line_id": 25108,
"play_name": "Coriolanus",
"speech_number": 3,
"line_number": "1.6.18",
"speaker": "COMINIUS",
"text_entry": "Methinks thou speakst not well."
}
}

Beats

Window into the Elastic Stack



Ship data from the source	**Ship and centralize in Elasticsearch**	**Ship to Logstash for transformation and parsing**
Ship to Elastic Cloud	**Libbeat: API framework to build custom beats**	**30+ community Beats**



PACKETBEAT
Network Data

METRICBEAT
Metrics

WINGLOGBEAT
Window Events

FILEBEAT
Log Files

HEARTBEAT
Uptime Monitoring

More than 30 community Beats and growing …

Apachebeat, dockbeat, httpbeat, mysqlbeat, nginxbeat, redis beats, twitterbeat, and more

beat.hostname:"orion.company.co"

Uses lucene query syntax

Add a filter +

System Navigation [Metricbeat System]

System Overview | Host Overview | Containers overview

CPU Usage Gauge [Metricbeat Syste...

CPU Usage
17.39%

Memory Usage Gauge [Metricbeat S...

Memory Usage
79.2%

Load Gauge [Metricbeat System]

5m Load
2.4

Inbound Traffic [Metricbeat System]

Inbound Traffic
5.3KB/s
Total Transfered 5.9MB

Outbound Traffic [Metricbeat System]

Outbound Traffic
776.2B/s
Total Transfered 2.8MB

Packetloss [Metricbeat System]

In Packetloss
0
Out Packetloss 2

Swap usage [Metricbeat System]

Swap usage
91.9%

Memory usage vs total

Memory usage
12.7GB
Total Memory 16.0GB

Number of processes [Metricbeat Sy...

Processes
25

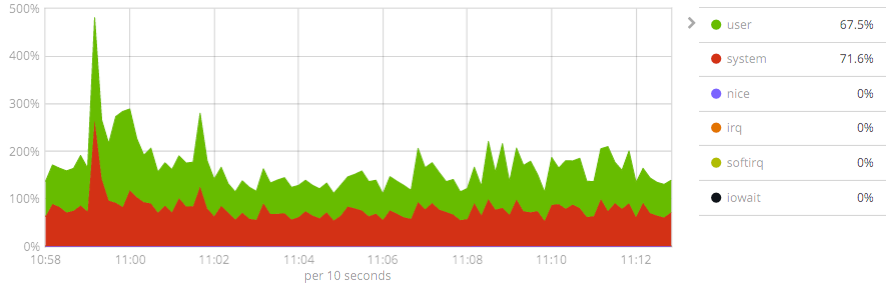
Disk used [Metricbeat System]

Disk used
39.44%

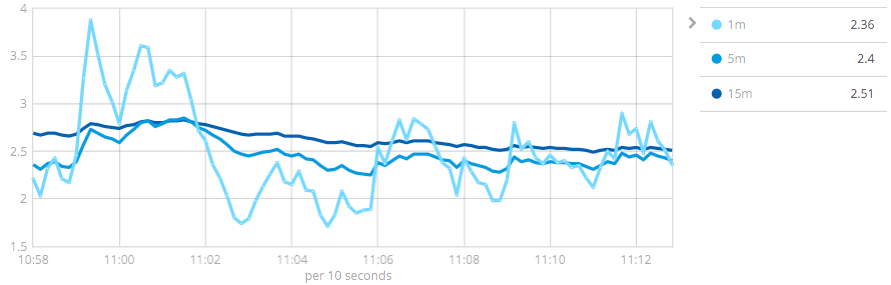
Disk Usage [Metricbeat System]

/Volumes/MobileBackups	100%
/	34.2%
/Volumes/Clone	25.9%
/Volumes/TimeMachine	25.4%
/net	0%
/home	0%

CPU Usage [Metricbeat System]

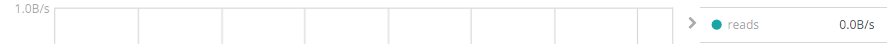


System Load [Metricbeat System]

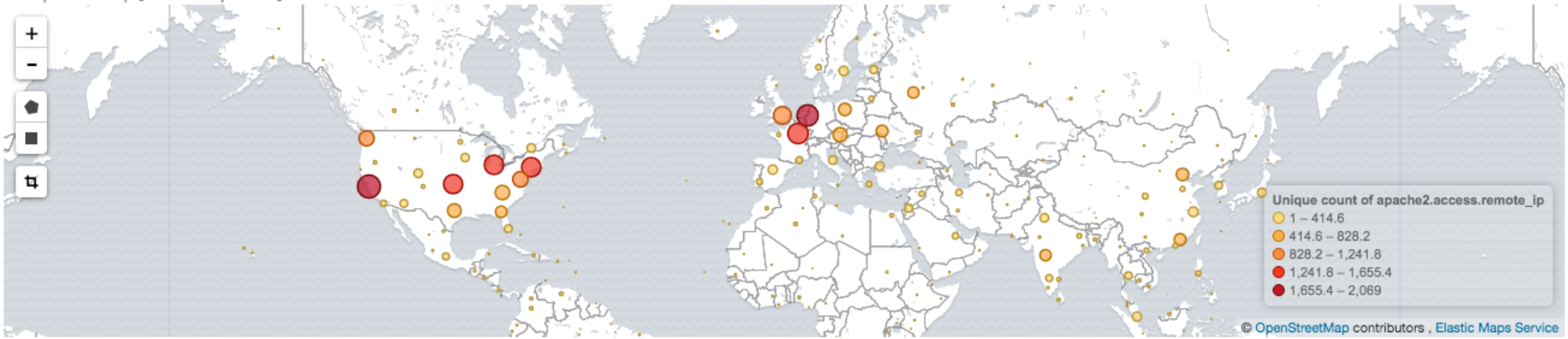


Memory Usage [Metricbeat System]

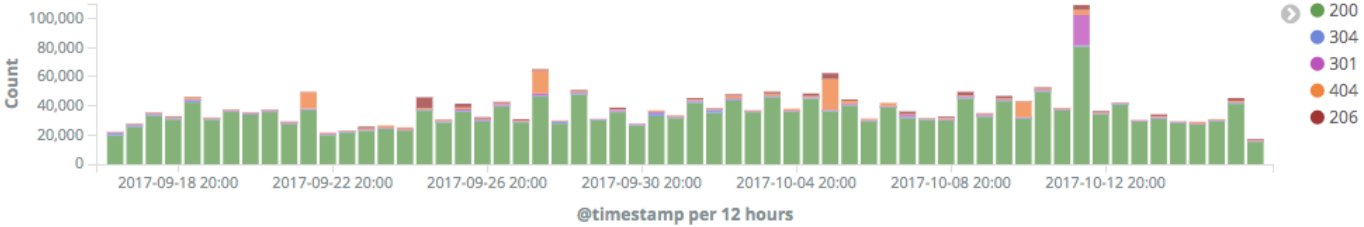
Disk IO (Bytes) [Metricbeat System]



Unique IPs map [Filebeat Apache2]

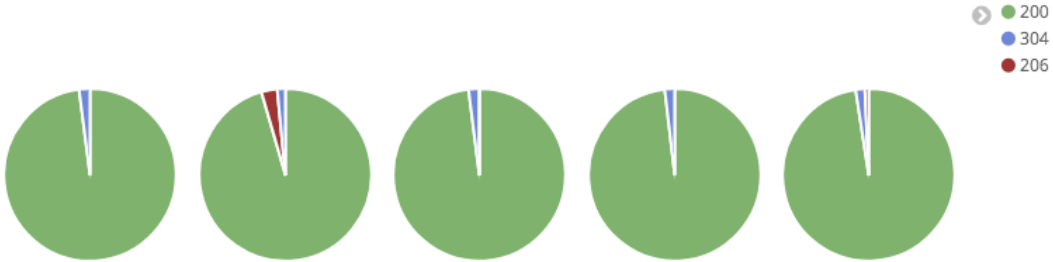


Response codes over time [Filebeat Apache2]

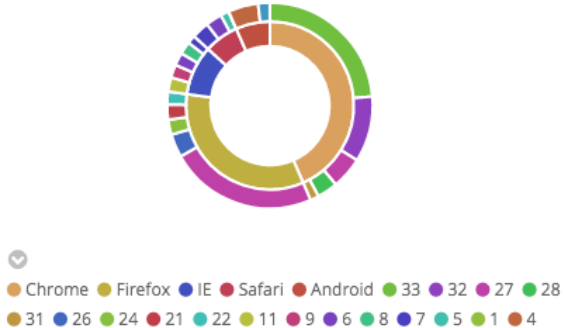


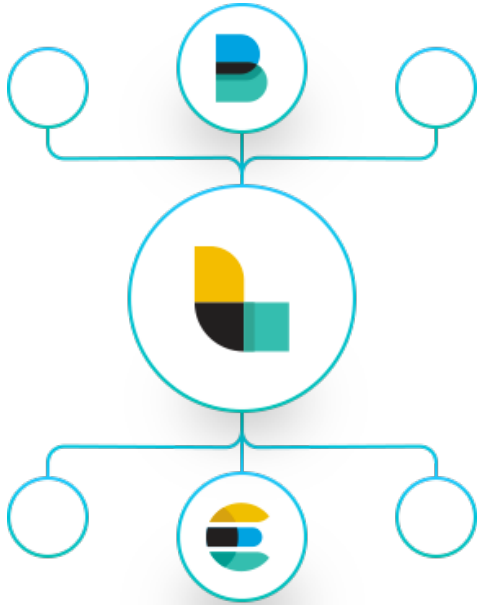
Operating systems breakd...

Top URLs by response code [Filebeat Apache2]



Browsers breakdown [Filebeat Apache2]



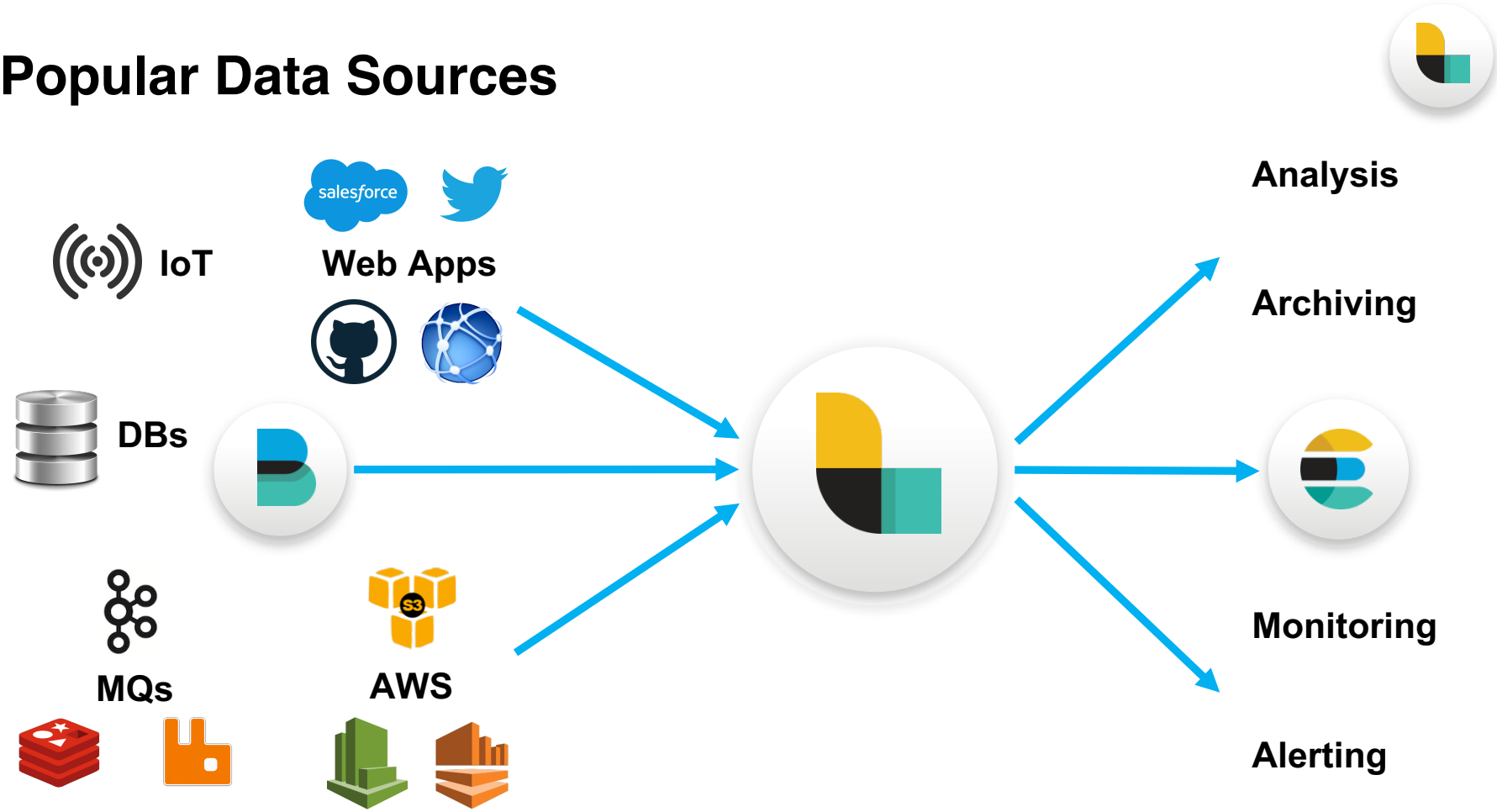


Logstash

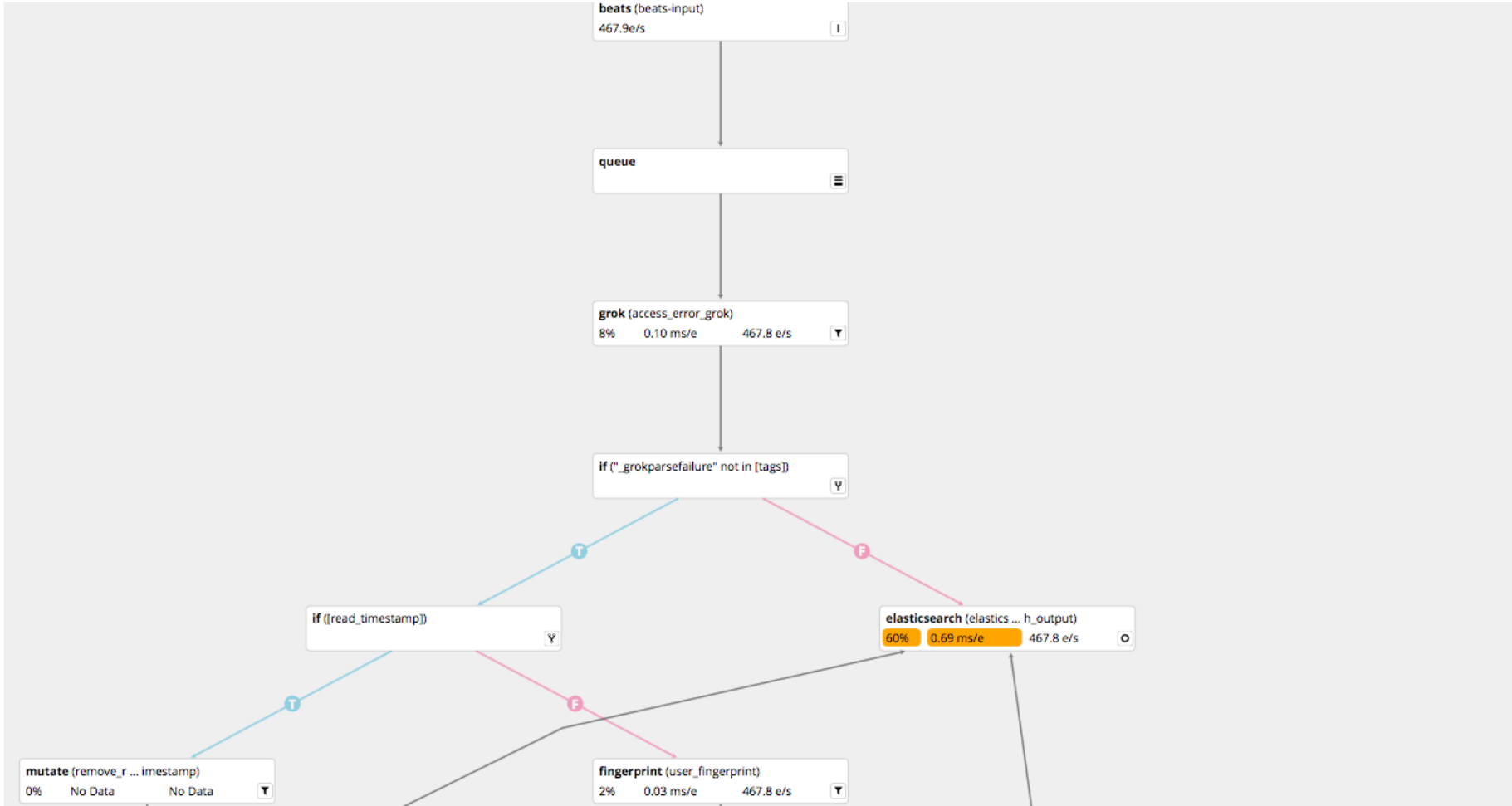
Data processing pipeline

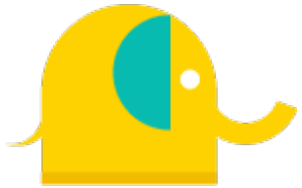
Ingest data of all shapes, sizes, and sources	**Parse and dynamically transform data**	**Transport data to any output**
Secure and encrypt data inputs	**Build your own pipeline**	**More than 200+ plugins**

Popular Data Sources



Version e456ab

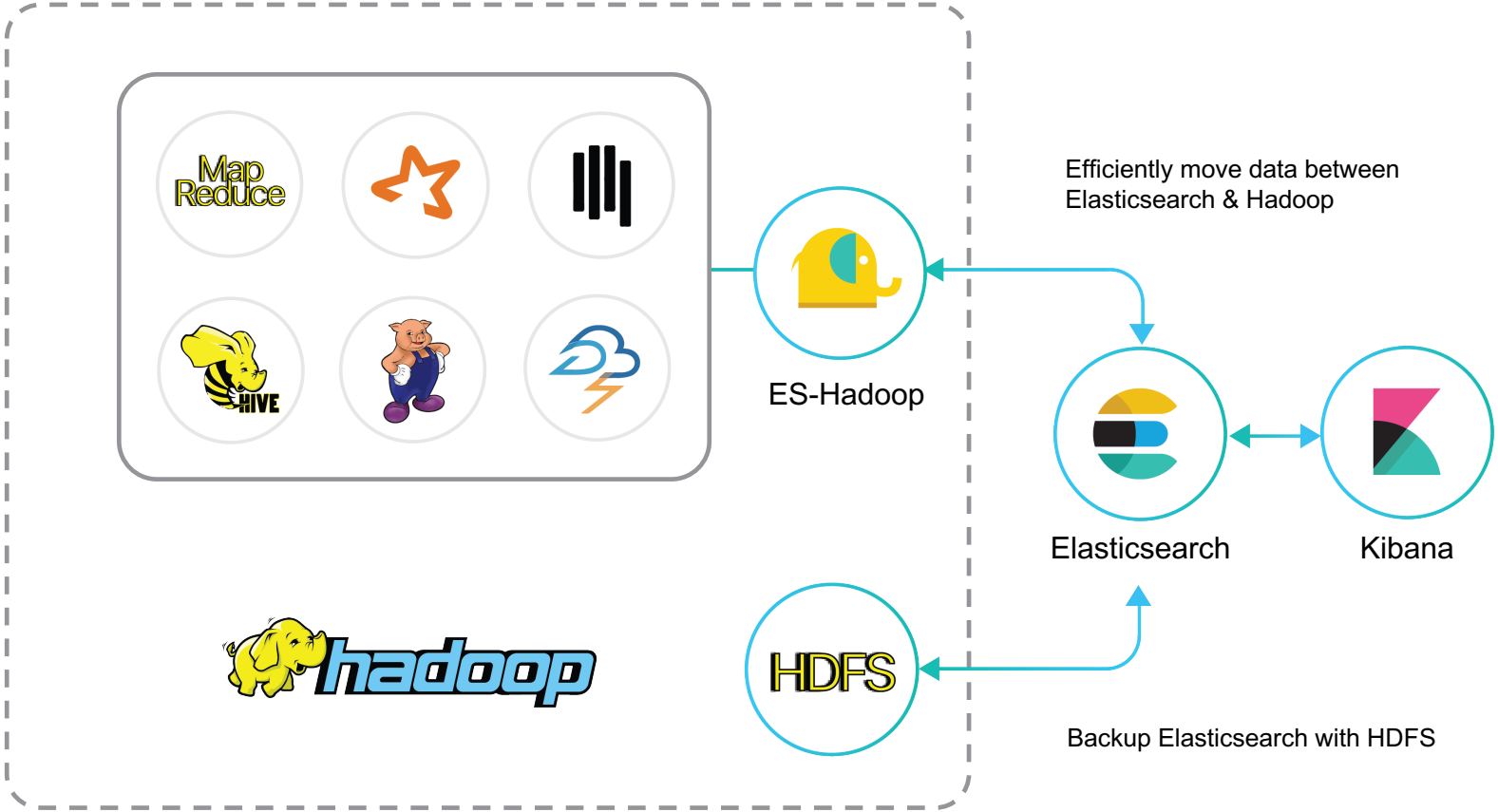




ES-Hadoop

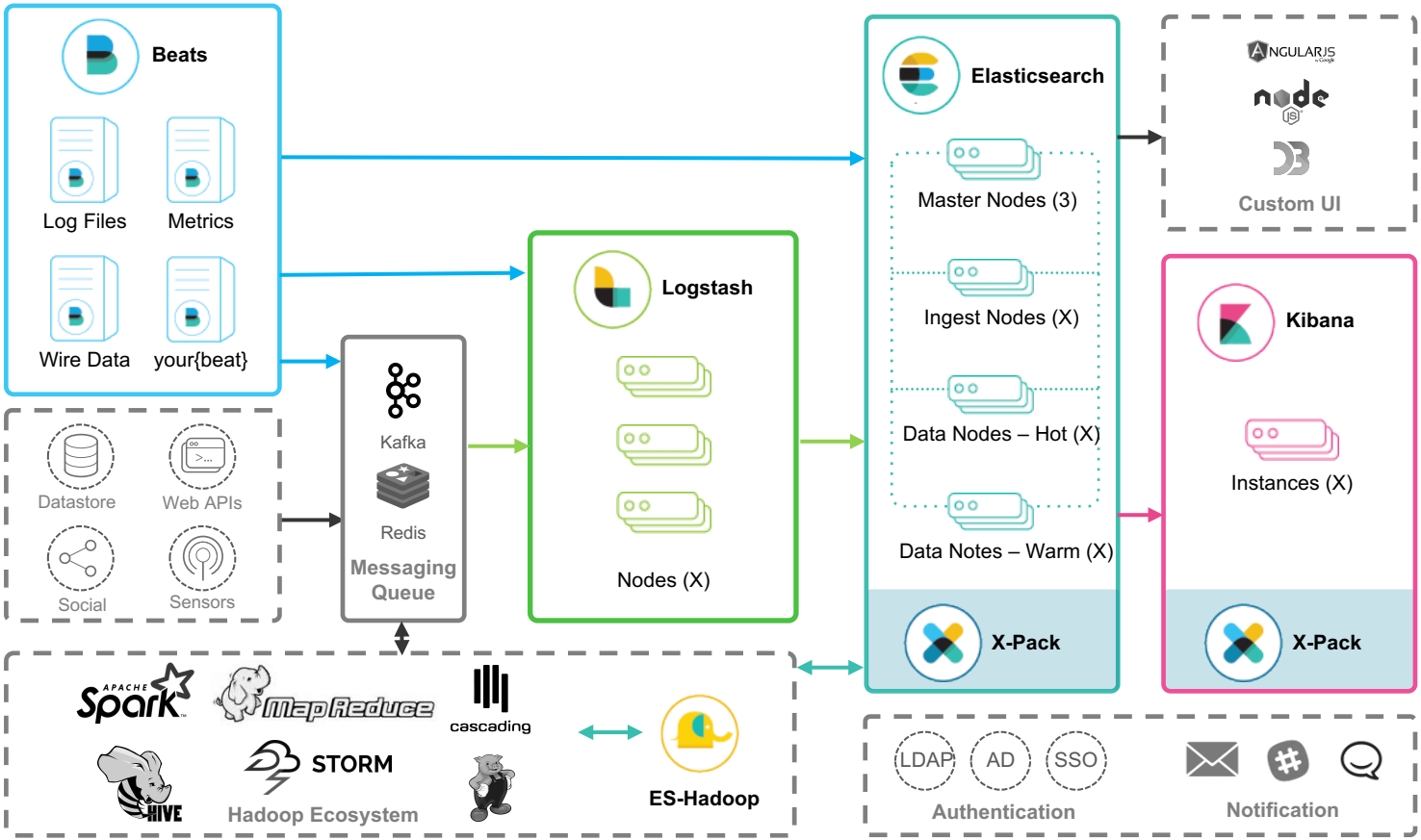
Elasticsearch for Hadoop

Two-way connector	**Index Hadoop data in Elasticsearch**	**Enable real-time search capabilities**
Visualize HDFS data in Kibana	**Snapshot and restore with HDFS**	**Support for Spark, Storm MapReduce, and more**


Map Reduce
HIVE
hadoop
ES-Hadoop
HDFS
Efficiently move data between Elasticsearch & Hadoop
Elasticsearch
Kibana
Backup Elasticsearch with HDFS

elastic

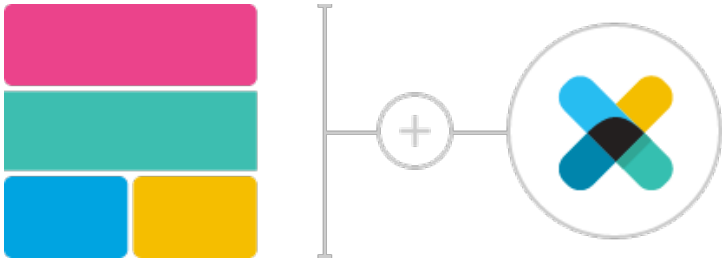
System Architecture



elastic

X-Pack

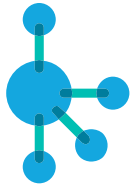
Extensions for the Elastic Stack



Security

Alerting

Monitoring



Graph

Reporting

Machine Learning

X-Pack

Security

AUTHENTICATION

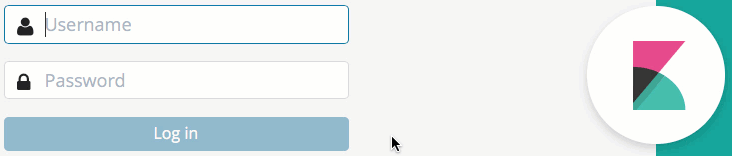
- Username and password
- Integrate with authentication systems
- Create a custom realm to authenticate users

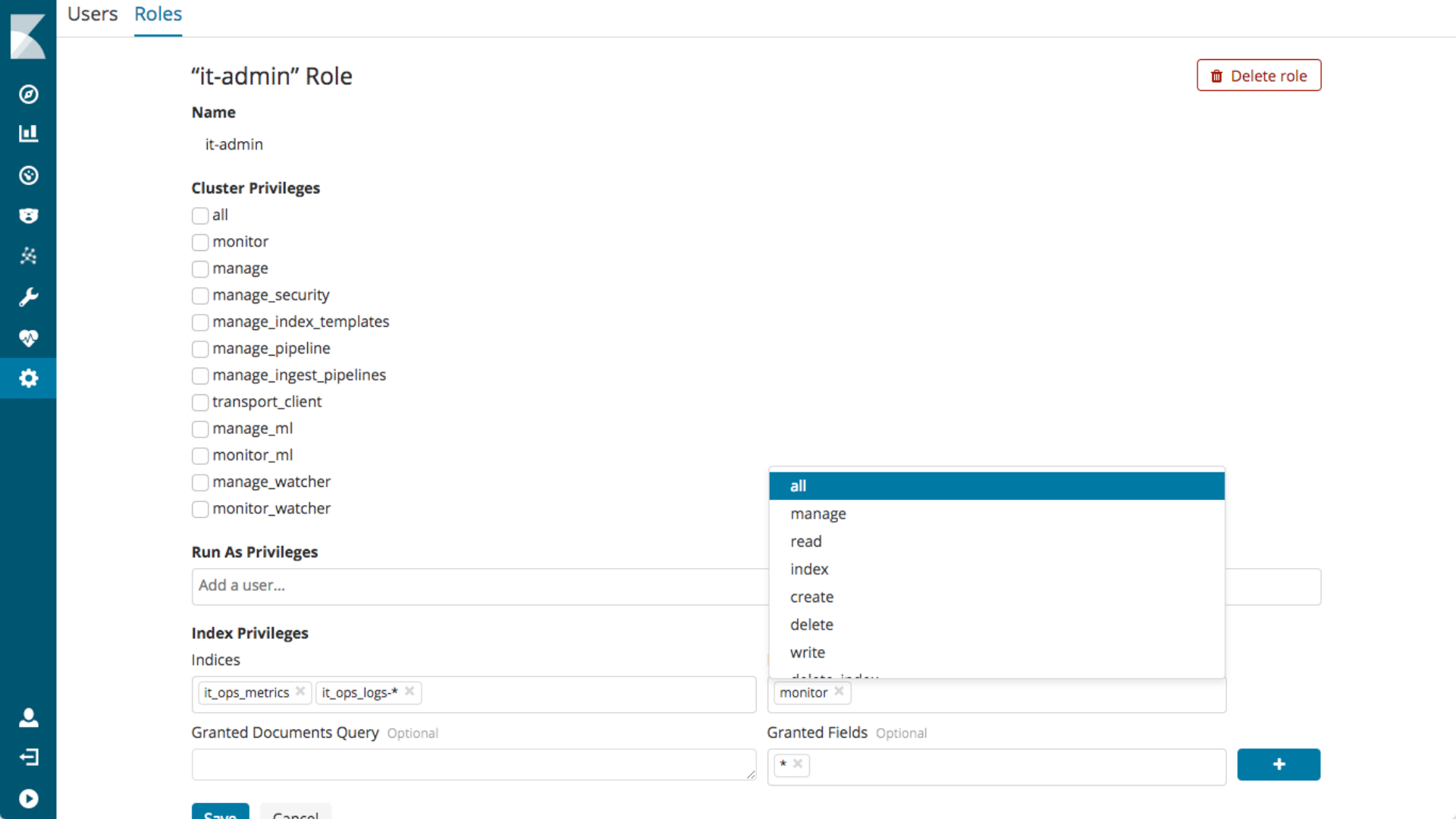
AUTHORITIZATION

- Manage users and roles
- Assign permissions and privileges

ADDITIONAL CONTROLS

- SSL/TLS encryption
- IP filtering
- Field and document level security
- Audit logging


Username
Password
Log in


Users
Roles
"it-admin" Role
Delete role
Name
it-admin
Cluster Privileges
all
monitor
manage
manage_security
manage_index_templates
manage_pipeline
manage_ingest_pipelines
transport_client
manage_ml
monitor_ml
manage_watcher
monitor_watcher
all
manage
read
index
create
delete
write
Run As Privileges
Add a user...
Index Privileges
Indices
it_ops_metrics
it_ops_logs-*
monitor
Granted Documents Query Optional
Granted Fields Optional
*
+
Save
Cancel

X-Pack

Alerting

SETUP ALERTS

- Create Watches to detect changes in your data
- Trigger automatic notifications
- Setup nested alerts
- Store and track alert history

NOTIFY AND INTEGRATE

- Email
- Slack
- Pagerduty
- Hipchat or JIRA
- Other monitoring systems

Status Edit

Host CPU Watcher

Send out an alert when specific conditions are met. This will run once every 5 minutes.

Name

Host CPU Watcher

Select an Index

metricbeat-* ×

Broad searches can be done by adding * to your query

Select a time field

@timestamp

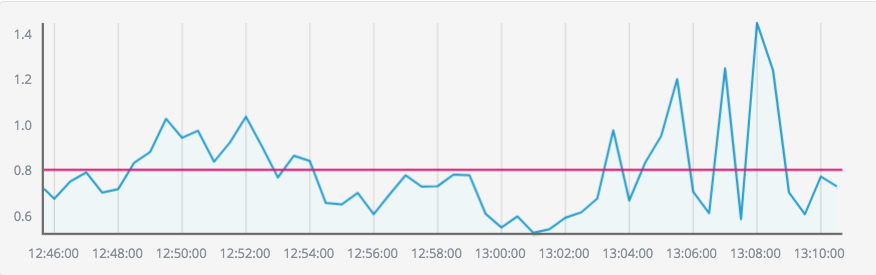
Run this watch every

5 minutes

Matching the following condition

WHEN average() OF system.cpu.user.pct GROUPED OVER top 5 'beat.hostname' IS ABOVE 0.8 FOR THE LAST 5 minutes

beat.hostname (1 of 3): orion.company.co



X-Pack

Monitoring

MONITOR CLUSTER HEALTH

- Prebuilt Kibana dashboards to monitor the performance of the Elastic Stack
- Get vital statistics at various levels -- cluster, node, and indices

OPTIMIZE CLUSTER PERFORMANCE

- Multicluster support to compare health and performance of multiple clusters
- Analyze historical or real-time data for root cause analyses
- Utilize analyses to proactively optimize and improve cluster performance
- Configure data retention policy

Nodes: **3** Indices: **24** Memory: **3GB / 5GB** Total Shards: **56** Unassigned Shards: **0** Documents: **3,665,331** Data: **3GB** Health: Green

Indices

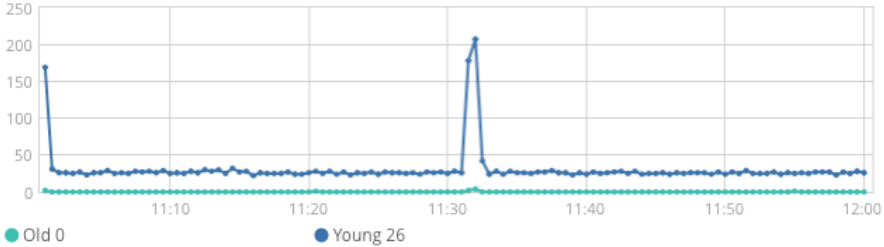
Filter Indices

3 of 3 Show system indices

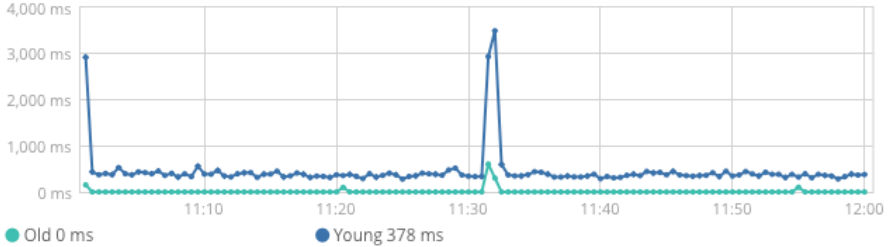
Name	Status	Document Count	Data	Index Rate	Search Rate	Unassigned Shards
elasticlogs-2017.10.12	Green	2m	1.3 GB	372.73 /s	0 /s	0
filebeat-6.0.0-rc1-2017.10.10	Green	994.7k	545.9 MB	0 /s	0 /s	0
filebeat-6.0.0-rc1-2017.10.11	Green	5.4k	2.1 MB	0 /s	0 /s	0

10.141.15.207:19471 JVM Heap: **17%** Free Disk Space: **101.1 GB** Documents: **3.6m** Data: **1.3 GB** Indices: **24** Shards: **28** Type: **Node** Health: Online

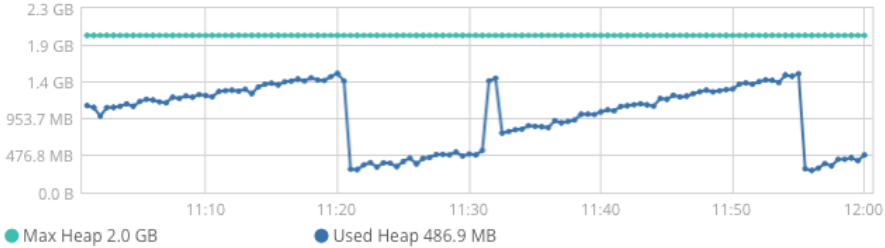
GC Count



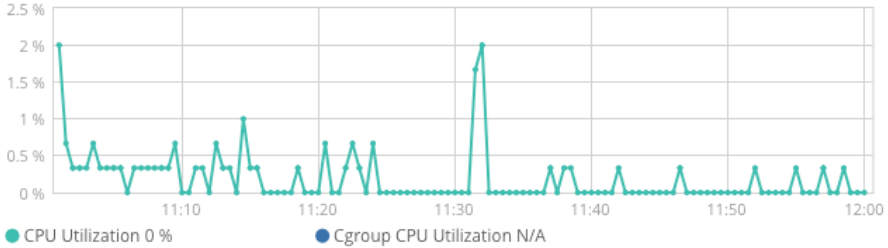
GC Duration (ms)



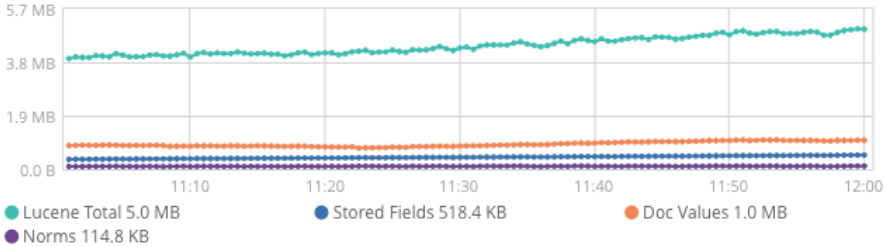
JVM Heap (GB)



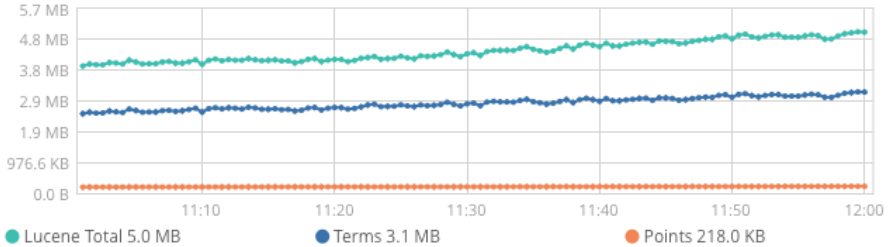
CPU Utilization (%)



Index Memory - Lucene 1 (MB)



Index Memory - Lucene 2 (MB)



X-Pack

Reporting

AUTOMATE SCHEDULING

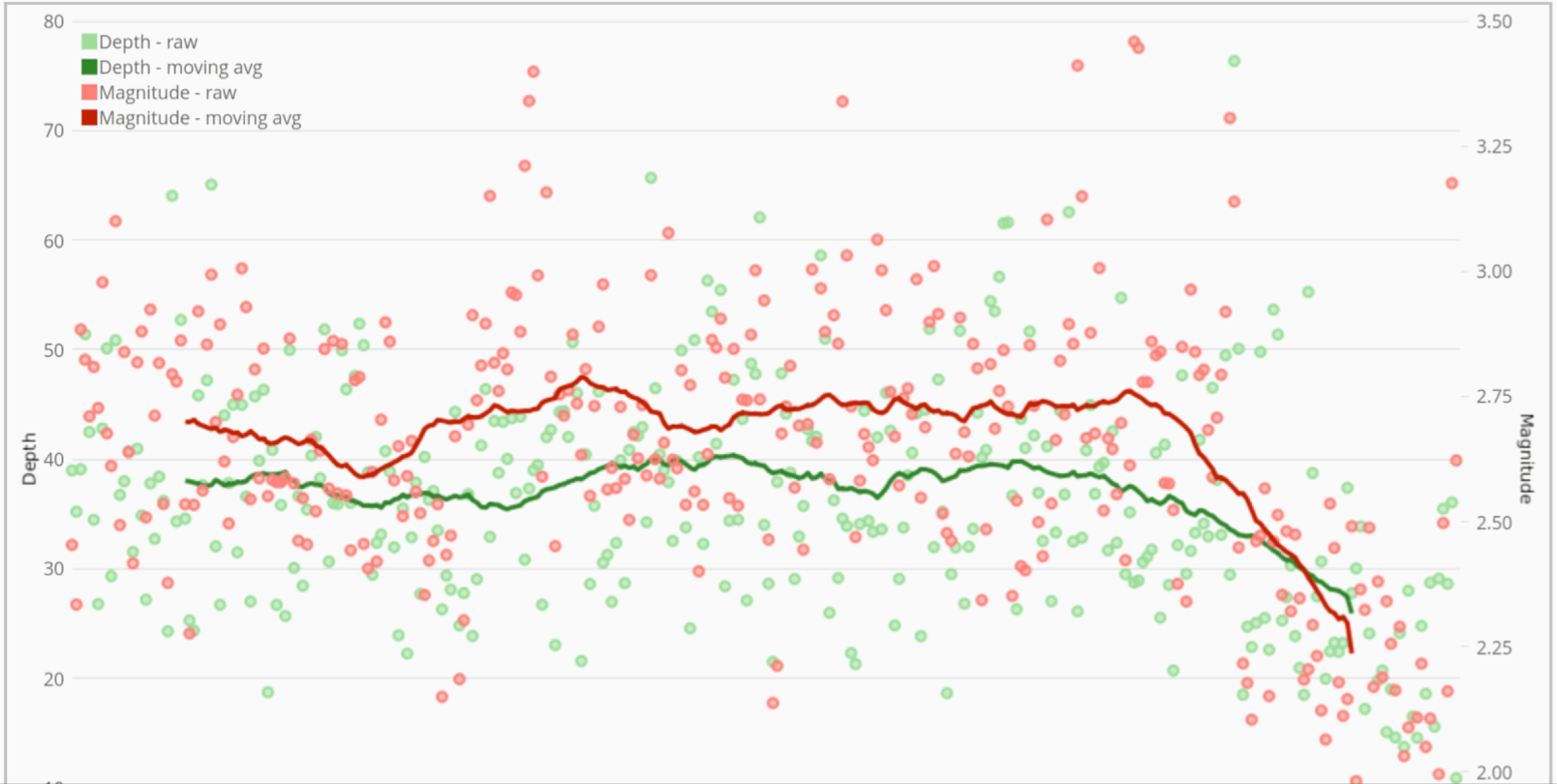
- Email recurring status updates daily, weekly, monthly, etc.
- Combine reporting with X-Pack alerting capabilities to trigger conditional reports

SHARE AND COLLABORATE

- Export any Kibana visualization or dashboard
- Print-optimized and PDF formatted
- Download and share past reports
- Export search results to CSV format.

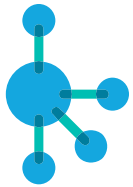
Earthquake Summary — Fri, Jan 1, 2016 12:00 AM to Tue, Nov 15, 2016 6:42 AM

Earthquakes - depth v mag



```
"@timestamp",depth,mag,location,message
"June 11th 2016, 03:55:17.140","7.59","1.46","44.3883, -110.9933","2016/06/11 03:55:17.14,44.3883,-110.9933,7.59,1.46,ML,15,124,14,0.12,WY,"
"June 11th 2016, 03:50:19.480","10.67","1.39","33.4712, -116.476","2016/06/11 03:50:19.48,33.4712,-116.4760,10.67,1.39,ML,84,,,0.17,CI,37381431"
"June 11th 2016, 03:49:12.000","3.04","1.05","38.8247, -122.8028","2016/06/11 03:49:12.00,38.8247,-122.8028,3.04,1.05,Md,23,55,1,0.02,NC,72649791"
"June 11th 2016, 03:38:12.690","8.95","1.66","41.9007, -119.647","2016/06/11 03:38:12.69,41.9007,-119.6470,8.95,1.66,ML,10,216,13,0.11,NN,547552"
"June 11th 2016, 03:18:10.050","7.69","1.05","41.8539, -119.6714","2016/06/11 03:18:10.05,41.8539,-119.6714,7.69,1.05,ML,9,223,15,0.11,NN,547585"
"June 11th 2016, 03:08:45.170","9.77","1.48","33.475, -116.4438","2016/06/11 03:08:45.17,33.4750,-116.4438,9.77,1.48,ML,94,,,0.16,CI,37381319"
"June 11th 2016, 03:07:45.430","8.74","1.87","33.4708, -116.4455","2016/06/11 03:07:45.43,33.4708,-116.4455,8.74,1.87,ML,103,,,0.21,CI,37381311"
"June 11th 2016, 03:04:43.910","9.91","2.22","33.4807, -116.4157","2016/06/11 03:04:43.91,33.4807,-116.4157,9.91,2.22,ML,148,,,0.16,CI,37381287"
"June 11th 2016, 02:43:34.780","579.26","4.8","-18.0502, -178.3982","2016/06/11 02:43:34.78,-18.0502,-178.3982,579.26,4.80,Mb,,74,3,0.80,us,201606112008"
"June 11th 2016, 01:59:43.550","7.58","1.03","33.482, -116.414","2016/06/11 01:59:43.55,33.4820,-116.4140,7.58,1.03,ML,50,,,0.21,CI,37381055"
"June 11th 2016, 01:40:30.950","10.81","3.04","33.4598, -116.4883","2016/06/11 01:40:30.95,33.4598,-116.4883,10.81,3.04,ML,220,,,0.18,CI,37380967"
"June 11th 2016, 01:39:52.720","10.09","1.78","33.4553, -116.4637","2016/06/11 01:39:52.72,33.4553,-116.4637,10.09,1.78,ML,93,,,0.20,CI,37380959"
"June 11th 2016, 01:38:47.980","7.26","1.8","36.082, -89.7815","2016/06/11 01:38:47.98,36.0820,-89.7815,7.26,1.80,Md,24,78,8,0.14,NM,"
"June 11th 2016, 01:36:36.260","2.51","1.01","37.2795, -121.657","2016/06/11 01:36:36.26,37.2795,-121.6570,2.51,1.01,Md,16,85,7,0.05,NC,72649711"
"June 11th 2016, 01:26:37.520","8.38","1.05","34.036, -117.0975","2016/06/11 01:26:37.52,34.0360,-117.0975,8.38,1.05,ML,34,,,0.12,CI,37380911"
"June 11th 2016, 01:22:23.340","12.27","1.28","33.484, -116.4567","2016/06/11 01:22:23.34,33.4840,-116.4567,12.27,1.28,ML,65,,,0.22,CI,37380887"
"June 11th 2016, 01:17:18.500","7.26","3.5","36.4887, -98.7261","2016/06/11 01:17:18.50,36.4887,-98.7261,7.26,3.50,ML,,49,,0.51,tul,201606112006"
"June 11th 2016, 01:16:19.820","9.57","1.02","33.4783, -116.4055","2016/06/11 01:16:19.82,33.4783,-116.4055,9.57,1.02,ML,44,,,0.16,CI,37380879"
"June 11th 2016, 01:05:24.970","1.8","1.01","38.8388, -122.7983","2016/06/11 01:05:24.97,38.8388,-122.7983,1.80,1.01,Md,7,154,1,0.05,NC,72649696"
"June 11th 2016, 01:05:16.950",10,4,"-0.5957, 29.4435","2016/06/11 01:05:16.95,-0.5957,29.4435,10.00,4.00,Mb,,113,1,0.90,us,201606112005"
"June 11th 2016, 00:58:16.410","92.4","4.1","2.4287, 128.0806","2016/06/11 00:58:16.41,2.4287,128.0806,92.40,4.10,Mb,,117,2,0.80,us,201606112004"
"June 11th 2016, 00:43:19.470","6.75","1.22","41.8917, -112.7938","2016/06/11 00:43:19.47,41.8917,-112.7938,6.75,1.22,Mc,11,207,13,0.10,UU,"
"June 11th 2016, 00:41:37.800","3.5","1.7","48.157, -116.36","2016/06/11 00:41:37.80,48.1570,-116.3600,3.50,1.70,ML,12,143,58,0.16,MB,"
"June 11th 2016, 00:39:48.600","2.12","1.3","33.1815, -115.6133","2016/06/11 00:39:48.60,33.1815,-115.6133,2.12,1.30,ML,13,,,0.12,CI,37380799"
"June 11th 2016, 00:36:30.140","475.27","4.2","-24.1258, 179.1065","2016/06/11 00:36:30.14,-24.1258,179.1065,475.27,4.20,Mb,,92,6,0.92,us,201606112003"
"June 11th 2016, 00:27:57.750","9.19","2.11","33.4788, -116.4152","2016/06/11 00:27:57.75,33.4788,-116.4152,9.19,2.11,ML,124,,,0.17,CI,37380735"
"June 11th 2016, 00:27:29.270","77.69","4.6","4.0462, 126.4564","2016/06/11 00:27:29.27,4.0462,126.4564,77.69,4.60,Mb,,93,3,0.64,us,201606112002"
"June 11th 2016, 00:24:01.310","521.14","4.5","-23.663, -179.7763","2016/06/11 00:24:01.31,-23.6630,-179.7763,521.14,4.50,Mb,,121,6,0.84,us,201606112001"
"June 11th 2016, 00:22:21.380","5.97","1.3","36.2727, -89.5548","2016/06/11 00:22:21.38,36.2727,-89.5548,5.97,1.30,Md,12,109,4,0.02,NM,"
"June 11th 2016, 00:20:47.110","3.44","1.66","38.8237, -122.8022","2016/06/11 00:20:47.11,38.8237,-122.8022,3.44,1.66,Md,79,53,1,0.06,NC,72649671"
"June 11th 2016, 00:05:36.440","-0.85","1.55","38.7853, -122.7652","2016/06/11 00:05:36.44,38.7853,-122.7652,-0.85,1.55,Md,46,65,2,0.10,NC,72649651"
"June 11th 2016, 00:00:49.870","3.42","1.85","38.824, -122.8018","2016/06/11 00:00:49.87,38.8240,-122.8018,3.42,1.85,Md,79,42,1,0.06,NC,72649611"
"June 11th 2016, 23:59:40.500","2.4",1,"38.8235, -122.8007","2016/06/10 23:59:40.50,38.8235,-122.8007,2.40,1.00,Md,12,123,1,0.02,NC,72649621"
"June 10th 2016, 23:57:55.220","2.94","3.31","38.8253, -122.7983","2016/06/10 23:57:55.22,38.8253,-122.7983,2.94,3.31,ML,86,31,1,0.06,NC,72649606"
"June 10th 2016, 23:54:38.540","77.86","4.5","13.0767, 144.3792","2016/06/10 23:54:38.54,13.0767,144.3792,77.86,4.50,Mb,,153,1,0.91,us,201606102086"
"June 10th 2016, 23:51:03.860","11.51","1.07","33.4797, -116.4697","2016/06/10 23:51:03.86,33.4797,-116.4697,11.51,1.07,ML,62,,,0.26,CI,37380623"
"June 10th 2016, 23:49:09.460","10.29","1.15","33.4665, -116.4137","2016/06/10 23:49:09.46,33.4665,-116.4137,10.29,1.15,ML,62,,,0.13,CI,37380607"
"June 10th 2016, 23:46:11.710","9.38","1.78","33.4618, -116.4237","2016/06/10 23:46:11.71,33.4618,-116.4237,9.38,1.78,ML,97,,,0.22,CI,37380559"
"June 10th 2016, 23:42:58.090","11.08","2.95","33.4592, -116.4247","2016/06/10 23:42:58.09,33.4592,-116.4247,11.08,2.95,ML,152,,,0.16,CI,37380543"
"June 10th 2016, 23:38:22.140","7.34","1.36","35.7717, -121.097","2016/06/10 23:38:22.14,35.7717,-121.0970,7.34,1.36,Md,33,66,5,0.09,NC,72649586"
"June 10th 2016, 23:34:28.740","-0.86","1.75","39.0873, -122.6283","2016/06/10 23:34:28.74,39.0873,-122.6283,-0.86,1.75,Md,22,71,13,0.12,NC,72649581"
"June 10th 2016, 23:31:00.000","9.94","1.49","33.4545, -116.4628","2016/06/10 23:31:00.00,33.4545,-116.4628,9.94,1.49,ML,76,,,0.22,CI,37380527"
"June 10th 2016, 23:19:56.550","341.09",4,"-31.0368, -179.8159","2016/06/10 23:19:56.55,-31.0368,-179.8159,341.09,4.00,Mb,,124,2,0.96,us,201606102084"
"June 10th 2016, 23:12:42.480","70.17","4.2","-5.5807, 146.4612","2016/06/10 23:12:42.48,-5.5807,146.4612,70.17,4.20,Mb,,128,4,0.61,us,201606102083"
"June 10th 2016, 23:11:18.920","118.54","4.6","37.563, 71.8189","2016/06/10 23:11:18.92,37.5630,71.8189,118.54,4.60,Mw,,65,0,1.00,us,201606102082"
"June 10th 2016, 23:11:00.520","12.75","1.09","33.4752, -116.5057","2016/06/10 23:11:00.52,33.4752,-116.5057,12.75,1.09,ML,59,,,0.20,CI,37380479"
"June 10th 2016, 23:03:28.410","10.24",1,"33.4718, -116.4125","2016/06/10 23:03:28.41,33.4718,-116.4125,10.24,1.00,ML,53,,,0.12,CI,37380471"
"June 10th 2016, 23:03:20.690","11.73","1.48","35.6165, -118.2395","2016/06/10 23:03:20.69,35.6165,-118.2395,11.73,1.48,ML,32,,,0.13,CI,37380463"
"June 10th 2016, 23:01:19.470","12.03","1.9","35.6152, -118.2405","2016/06/10 23:01:19.47,35.6152,-118.2405,12.03,1.90,ML,56,,,0.13,CI,37380455"
"June 10th 2016, 22:47:08.990","3.83","1.76","36.9413, -122.2048","2016/06/10 22:47:08.99,36.9413,-122.2048,3.83,1.76,Md,18,235,14,0.07,NC,72649551"
"June 10th 2016, 22:44:26.220","2.34","1.19","38.8273, -122.8532","2016/06/10 22:44:26.22,38.8273,-122.8532,2.34,1.19,Md,22,61,0,0.02,NC,72649531"
"June 10th 2016, 22:44:09.560","11.65","1.7","33.4705, -116.4458","2016/06/10 22:44:09.56,33.4705,-116.4458,11.65,1.70,ML,93,,,0.22,CI,37380415"
"June 10th 2016, 22:43:23.710","13.42","1.06","33.4718, -116.4308","2016/06/10 22:43:23.71,33.4718,-116.4308,13.42,1.06,ML,53,,,0.20,CI,37380407"
"June 10th 2016, 22:42:59.490","34.89","4.4","36.1248, 143.359","2016/06/10 22:42:59.49,36.1248,143.3590,34.89,4.40,Mb,,131,3,0.70,us,201606102081"
"June 10th 2016, 22:40:15.970","9.93","1.77","33.4723, -116.4803","2016/06/10 22:40:15.97,33.4723,-116.4803,9.93,1.77,ML,94,,,0.21,CI,37380399"
"June 10th 2016, 22:31:27.440","2.74","1.75","35.1362, -116.5507","2016/06/10 22:31:27.44,35.1362,-116.5507,2.74,1.75,ML,36,,,0.18,CI,37380391"
"June 10th 2016, 22:30:41.270",10,"4.7","-37.1629, -95.3267","2016/06/10 22:30:41.27,-37.1629,-95.3267,10.00,4.70,Mb,,75,17,0.62,us,201606102080"
"June 10th 2016, 22:17:42.730","10.01","1.01","33.4847, -116.4938","2016/06/10 22:17:42.73,33.4847,-116.4938,10.01,1.01,ML,60,,,0.23,CI,37380359"
"June 10th 2016, 22:07:23.170","4.7","1.61","34.702, -116.2407","2016/06/10 22:07:23.17,34.7020,-116.2407,4.70,1.61,ML,19,,,0.09,CI,37380335"
"June 10th 2016, 21:51:27.400","14.41","4.2","24.2918, 125.1914","2016/06/10 21:51:27.40,24.2918,125.1914,14.41,4.20,Mb,,120,2,0.73,us,201606102079"
"June 10th 2016, 21:36:11.820","12.34","1.01","33.476, -116.461","2016/06/10 21:36:11.82,33.4760,-116.4610,12.34,1.01,ML,50,,,0.12,CI,37380207"
```

X-Pack



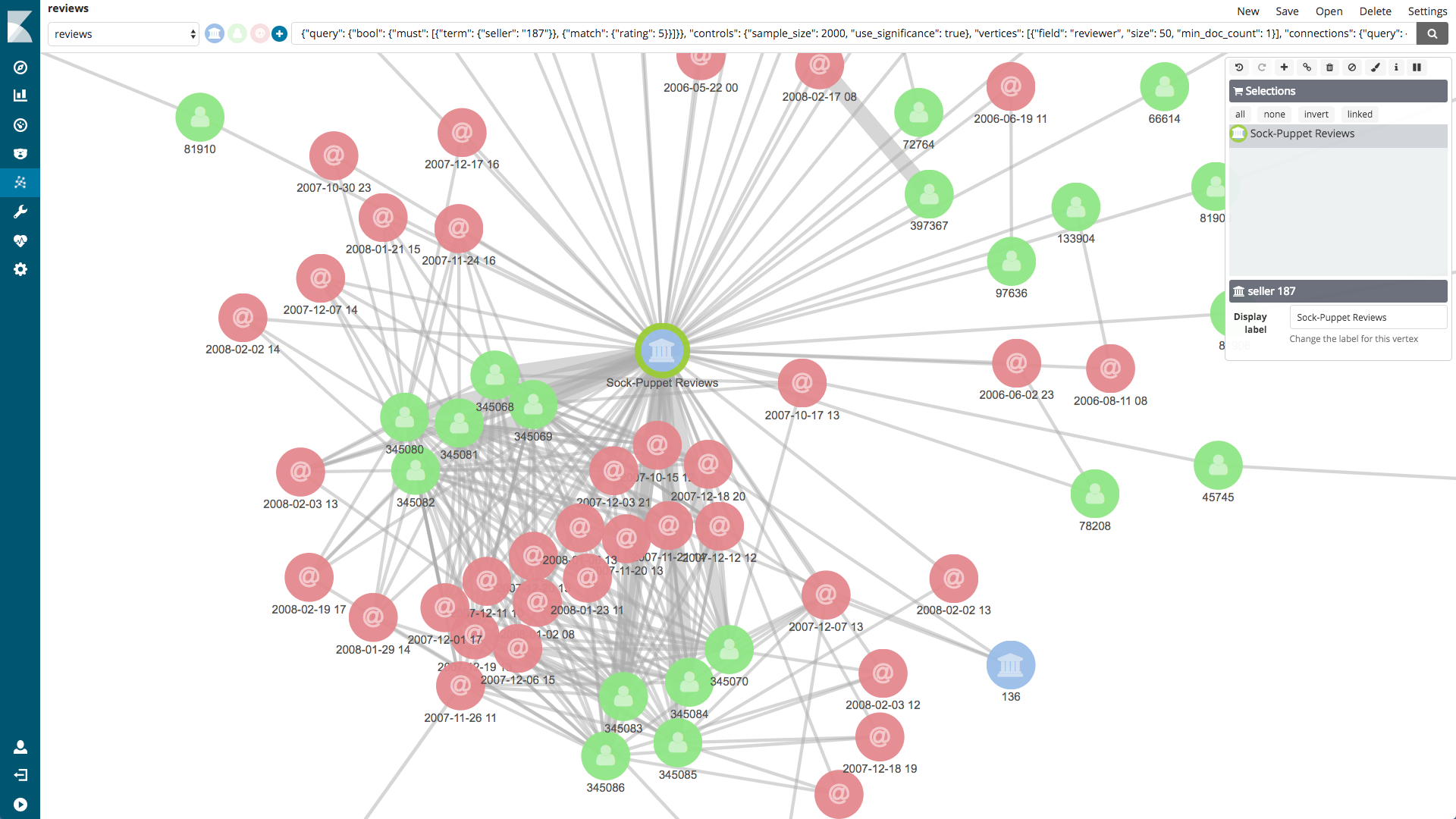
Graph

A NEW WAY TO EXPLORE DATA

- Uses relevance capabilities of Elasticsearch
- Discover linkages and connections
- Leverage API and UI-drive tool

EXTEND TO NEW USE CASES

- Fraud discovery
- Recommendations
- Cyber security
- Behavioral analyses


reviews
New
Save
Open
Delete
Settings
reviews
{"query": {"bool": {"must": [{"term": {"seller": "187"}}, {"match": {"rating": 5}}]}}, "controls": {"sample_size": 2000, "use_significance": true}, "vertices": [{"field": "reviewer", "size": 50, "min_doc_count": 1}], "connections": {"query":
Selections
all
none
invert
linked
Sock-Puppet Reviews
seller 187
Display label
Sock-Puppet Reviews
Change the label for this vertex
Sock-Puppet Reviews
81910
2007-10-30 23
2007-12-17 16
2008-01-21 15
2007-11-24 16
2007-12-07 14
2008-02-02 14
2006-05-22 00
2008-02-17 08
72764
2006-06-19 11
66614
397367
133904
8190
97636
2006-06-02 23
2006-08-11 08
2007-10-17 13
45745
78208
345068
345069
345080
345081
345082
2008-02-03 13
2007-12-03 21
2007-12-18 20
2008-02-19 17
2008-01-29 14
2007-12-01 17
2008-01-23 11
2007-12-06 15
2007-11-26 11
2007-12-07 13
2008-02-02 13
345070
345084
345083
345085
345086
136
2008-02-03 12
2007-12-18 19

X-Pack

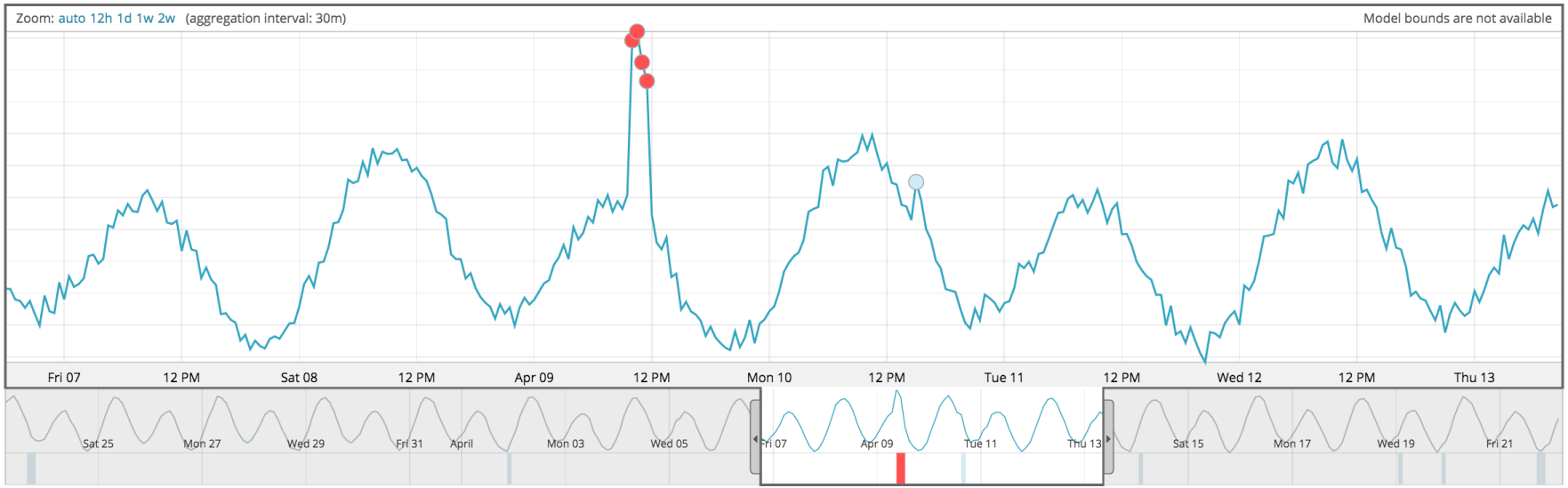
Machine Learning

UNSUPERVISED MACHINE LEARNING

- Automatically detect anomalies
- Advanced correlation and categorization
- Identify root cause(s)
- Expose early warning signs

ENABLE NEW USE CASES

- Analyze time series data
- Expand security, IT Ops, fraud, finance, and many more use cases
- Available as beta in the 5.4 release



Anomalies

Severity threshold: warning **Interval:** Auto

time	max severity	detector	found for	influenced by	actual	typical	description	job ID
April 9th 2017, 10:00	92	mean(response) (mm-job-3)	server_3	host: server_3 service: app_5	2.42113	2.31031	Unusually high	mm-job-3

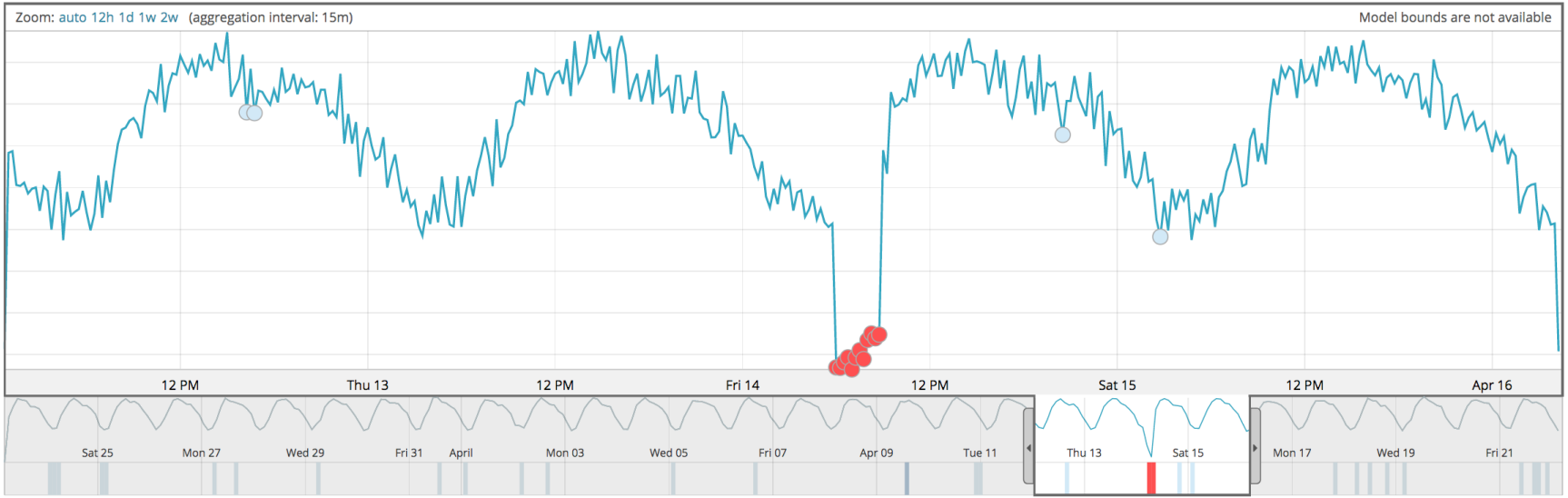
Description:
critical anomaly in mean(response) (mm-job-3) found for host server_3

Details on highest severity anomaly:

host:	server_3
time:	April 9th 2017, 10:15:00 to April 9th 2017, 10:30:00
function:	mean
fieldName:	response
actual:	2.42113
typical:	2.31031
job ID:	mm-job-3
probability:	5.59379e-13

Influenced by:

host	server_3
service	app_5



Anomalies

Severity threshold: warning **Interval:** Auto

time	max severity	detector	found for	influenced by	actual	typical	description	job ID
April 14th 2017	98	sum(total) (mm-job-4)	app_1	service: app_1	938905	1705380	2x lower	mm-job-4

Description:
critical anomaly in sum(total) (mm-job-4) found for service app_1

Details on highest severity anomaly:

service:	app_1
time:	April 14th 2017, 06:00:00 to April 14th 2017, 06:15:00
function:	sum
fieldName:	total
actual:	938905
typical:	1705380
job ID:	mm-job-4
probability:	4.84657e-20

Influenced by:

service	app_1

April 15th 2017	< 1	sum(total) (mm-job-4)	app_1	service: app_1	1564560	1789200	1.1x lower	mm-job-4
April 12th 2017	< 1	sum(total) (mm-job-4)	app_1	service: app_1	2156840	2353140	1.1x lower	mm-job-4

Chart interval: 1h Use full server* data

New job from index pattern server*

Job settings

Fields

event rate	Count
accept	Mean
deny	Mean
response	Mean
total	Sum

Sparse data

Split Data

host.keyword

Key Fields (Influencers)

- host.keyword
- service.keyword

Bucket span

30m Estimate bucket span

Job Details

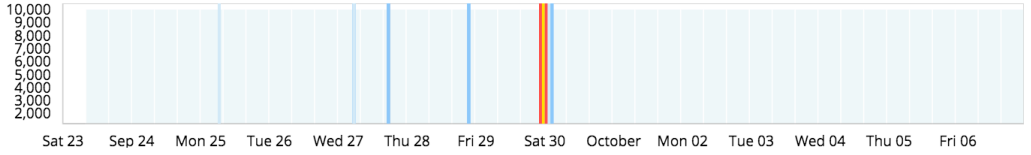
Job multimetric-1 created

Reset View Results

Continue job in real-time

Results

Document count



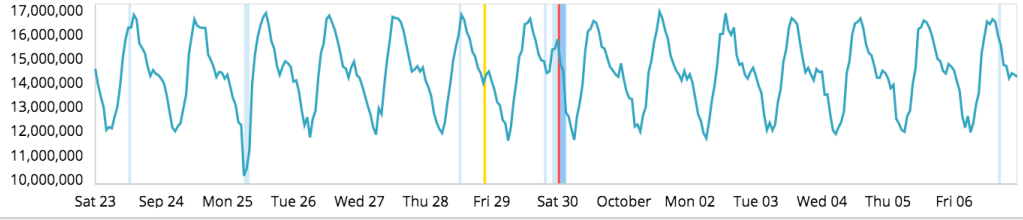
Data split by host.keyword

server_3

server_2

server_1

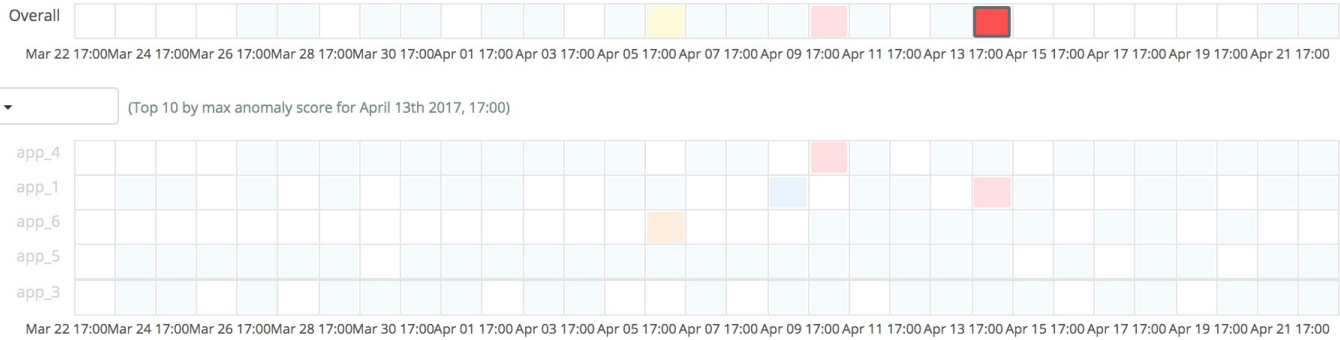
Sum total



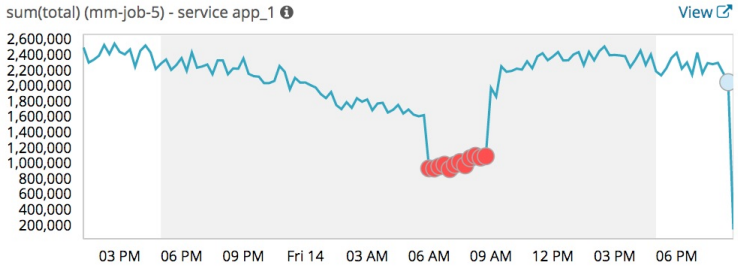
Top Influencers

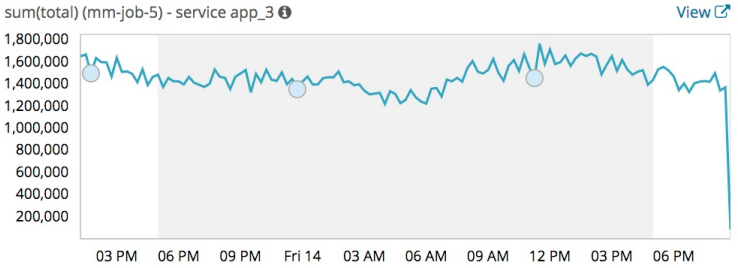
service		
app_4	99	1518
app_1	98	1024
app_6	57	203
app_0	5	11
app_5	2	5
app_2	< 1	2
app_3	< 1	1

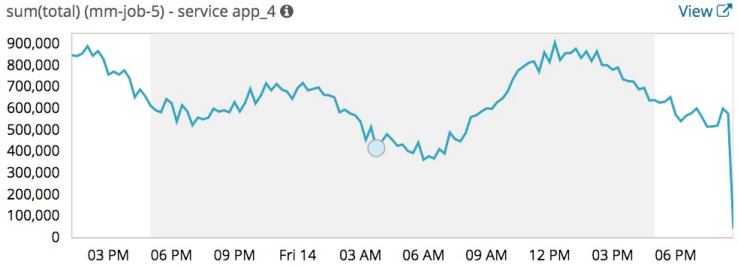
Anomaly timeline

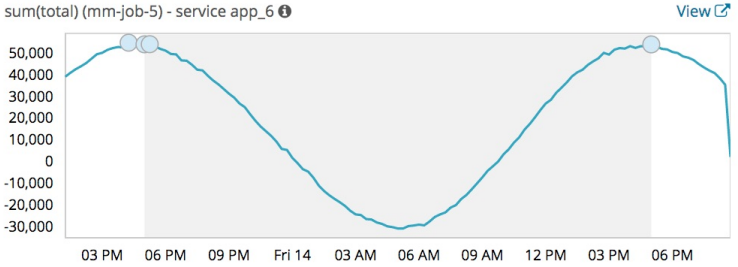


Anomalies



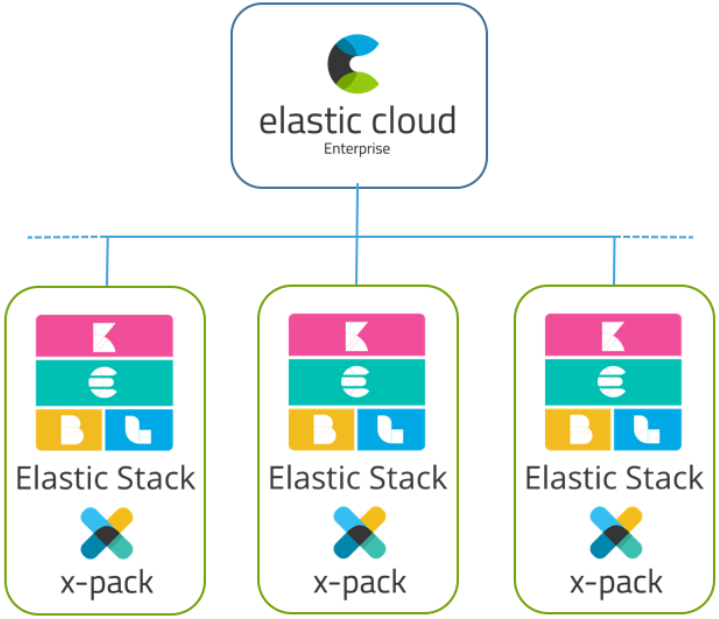




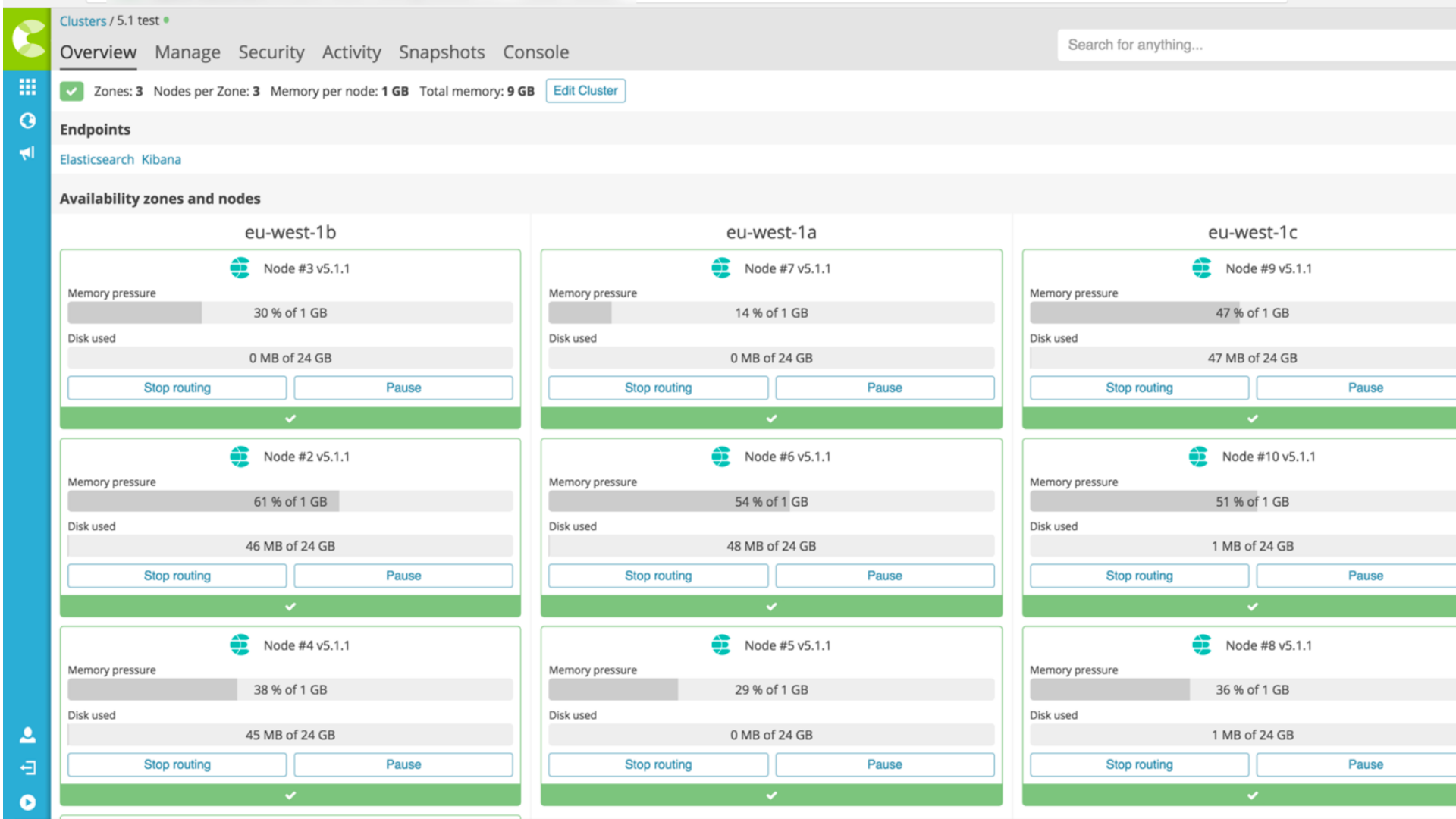


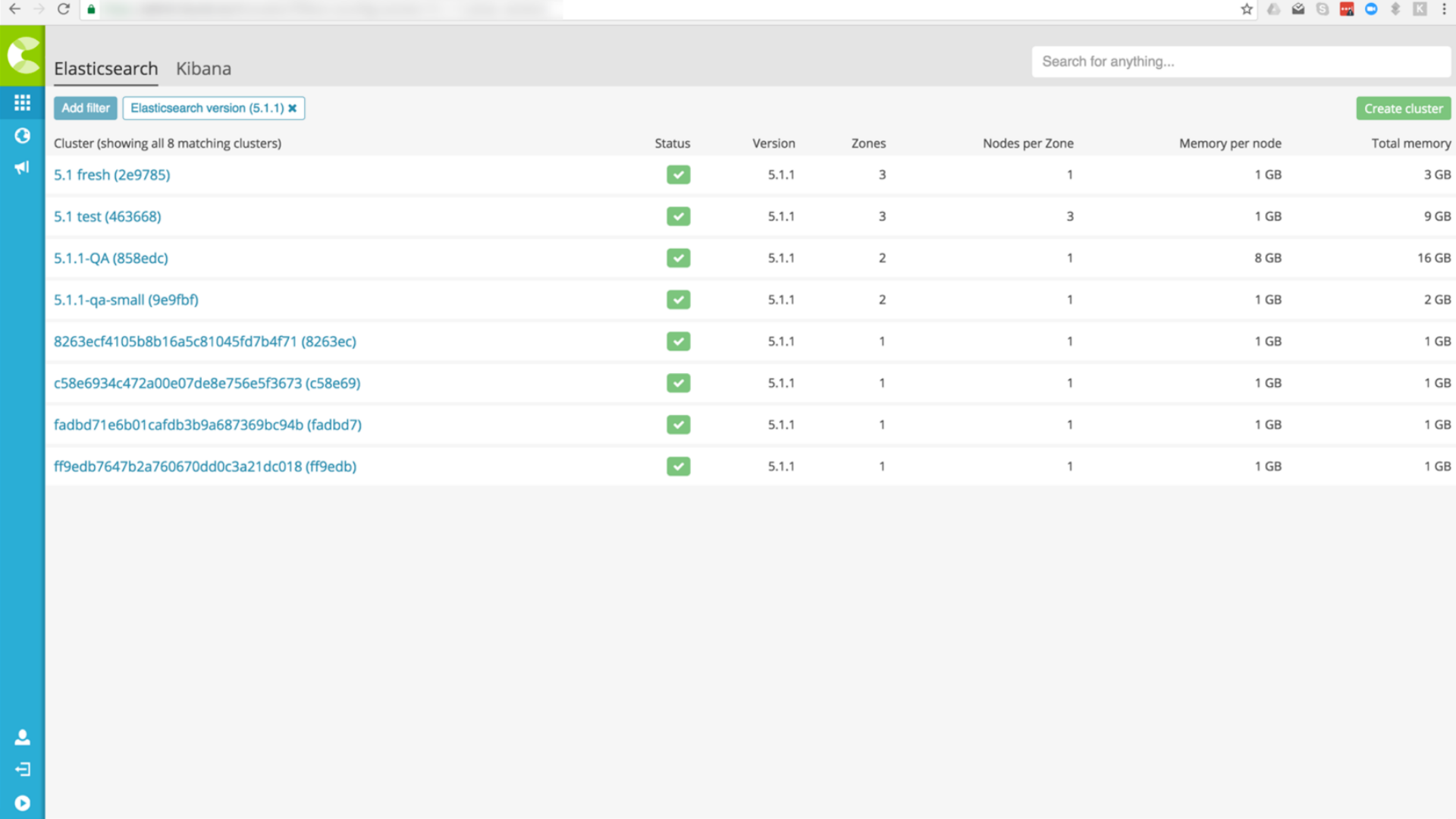
Elastic Cloud Enterprise

Provision and manage multiple Elastic Stack environments; Expose logging as a service to your entire organization



elastic


Clusters / 5.1 test
Overview
Manage
Security
Activity
Snapshots
Console
Search for anything...
Zones: 3 Nodes per Zone: 3 Memory per node: 1 GB Total memory: 9 GB
Edit Cluster
Endpoints
Elasticsearch Kibana
Availability zones and nodes
eu-west-1b
eu-west-1a
eu-west-1c
Node #3 v5.1.1
Memory pressure
30 % of 1 GB
Disk used
0 MB of 24 GB
Stop routing
Pause
Node #7 v5.1.1
Memory pressure
14 % of 1 GB
Disk used
0 MB of 24 GB
Stop routing
Pause
Node #9 v5.1.1
Memory pressure
47 % of 1 GB
Disk used
47 MB of 24 GB
Stop routing
Pause
Node #2 v5.1.1
Memory pressure
61 % of 1 GB
Disk used
46 MB of 24 GB
Stop routing
Pause
Node #6 v5.1.1
Memory pressure
54 % of 1 GB
Disk used
48 MB of 24 GB
Stop routing
Pause
Node #10 v5.1.1
Memory pressure
51 % of 1 GB
Disk used
1 MB of 24 GB
Stop routing
Pause
Node #4 v5.1.1
Memory pressure
38 % of 1 GB
Disk used
45 MB of 24 GB
Stop routing
Pause
Node #5 v5.1.1
Memory pressure
29 % of 1 GB
Disk used
0 MB of 24 GB
Stop routing
Pause
Node #8 v5.1.1
Memory pressure
36 % of 1 GB
Disk used
1 MB of 24 GB
Stop routing
Pause


Elasticsearch
Kibana
Search for anything...
Add filter
Elasticsearch version (5.1.1) ✖
Create cluster
Cluster (showing all 8 matching clusters)
Status
Version
Zones
Nodes per Zone
Memory per node
Total memory
5.1 fresh (2e9785)
5.1.1
3
1
1 GB
3 GB
5.1 test (463668)
5.1.1
3
3
1 GB
9 GB
5.1.1-QA (858edc)
5.1.1
2
1
8 GB
16 GB
5.1.1-qa-small (9e9fbf)
5.1.1
2
1
1 GB
2 GB
8263ecf4105b8b16a5c81045fd7b4f71 (8263ec)
5.1.1
1
1
1 GB
1 GB
c58e6934c472a00e07de8e756e5f3673 (c58e69)
5.1.1
1
1
1 GB
1 GB
fadbd71e6b01cafdb3b9a687369bc94b (fadbd7)
5.1.1
1
1
1 GB
1 GB
ff9edb7647b2a760670dd0c3a21dc018 (ff9edb)
5.1.1
1
1
1 GB
1 GB

Available capacity

Zone	elasticsearch	elasticsearch_data	elasticsearch_master_only	kibana	non_ssd	
eu-west-1a	333.38 GB	293.81 GB	43.63 GB	43.63 GB	43.63 GB	289.75
eu-west-1b	541 GB	508.25 GB	33.5 GB	33.5 GB	33.5 GB	507.5
eu-west-1c	343.13 GB	290.13 GB	89.63 GB	89.63 GB	89.63 GB	253.5

eu-west-1a

Allocator	Status	Available capacity	Node distribution
[redacted]	✓	234 GB	
[redacted]	✓	27 GB	
[redacted]	✓	23.25 GB	
[redacted]	✓	19 GB	
[redacted]	✓	9.25 GB	
[redacted]	✓	4.5 GB	
[redacted]	✓	3.19 GB	
[redacted]	✓	3.19 GB	
[redacted]	✓	2 GB	
[redacted]	✓	1.56 GB	
[redacted]	✓	1.25 GB	
[redacted]	✓	1.13 GB	
[redacted]	✓	1 GB	
[redacted]	✓	512 MB	

THANK YOU

@elastic

www.elastic.co