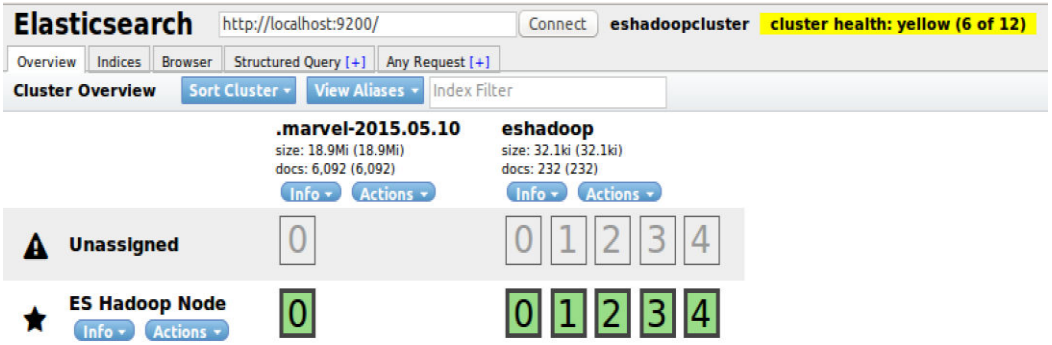
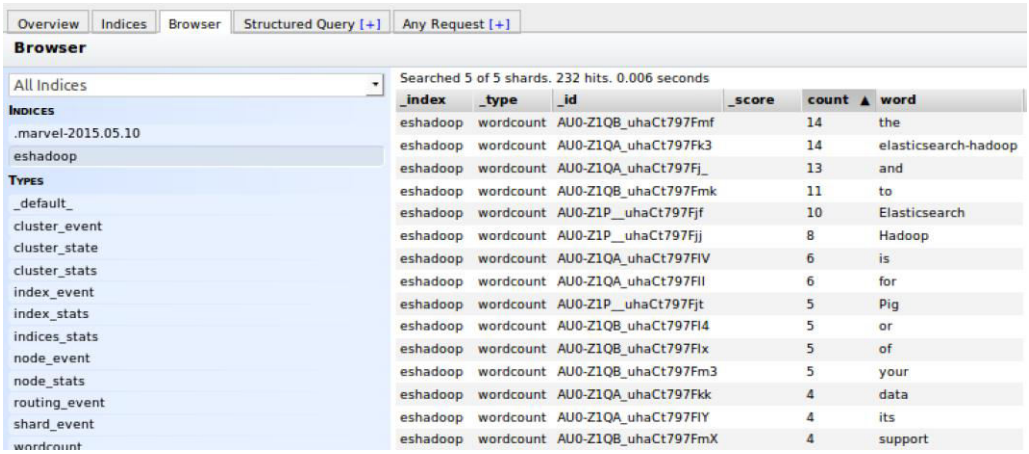
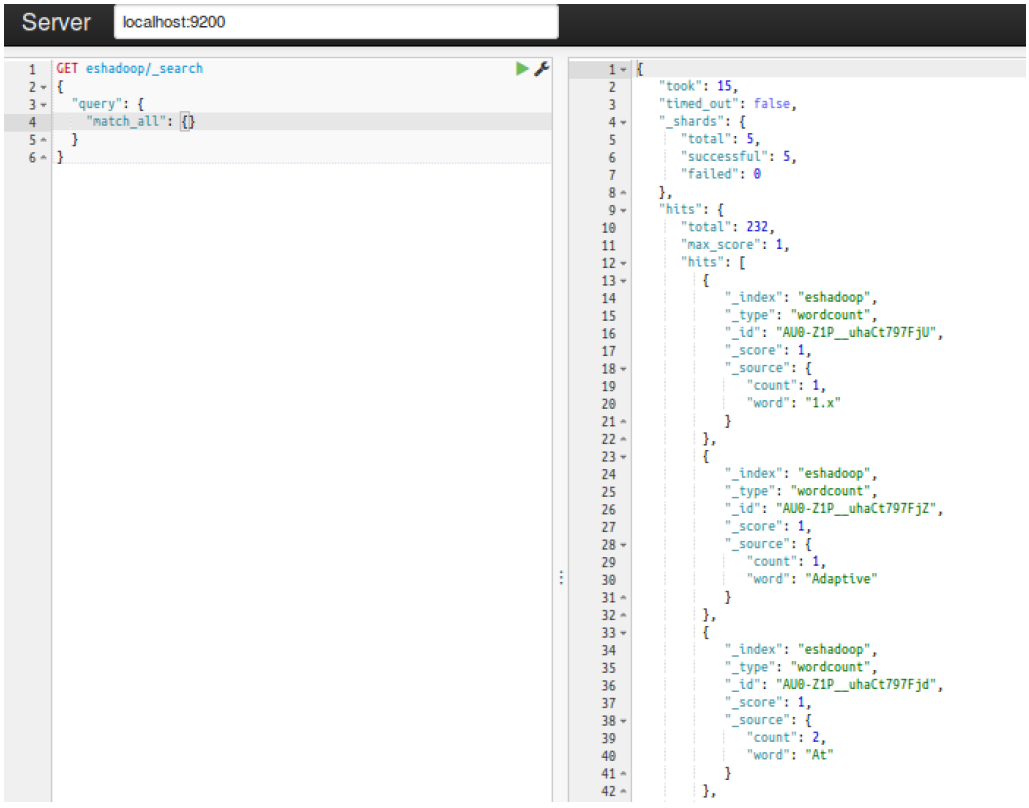
Chapter 1

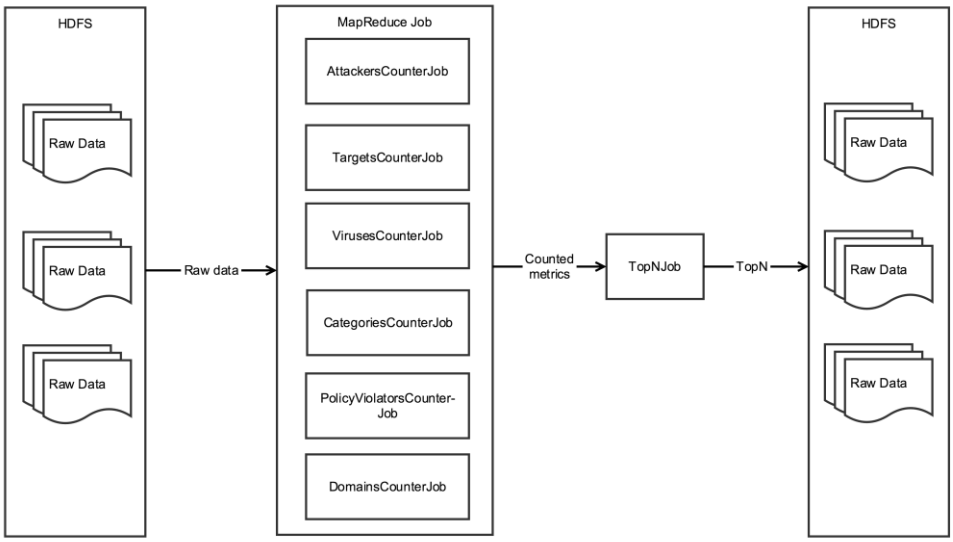

Elasticsearch
http://localhost:9200/
Connect
eshadoopcluster
cluster health: yellow (6 of 12)
Overview
Indices
Browser
Structured Query [+]
Any Request [+]
Cluster Overview
Sort Cluster
View Aliases
Index Filter
.marvel-2015.05.10
size: 18.9Mi (18.9Mi)
docs: 6,092 (6,092)
Info
Actions
eshadoop
size: 32.1ki (32.1ki)
docs: 232 (232)
Info
Actions
Unassigned
0
0 1 2 3 4
ES Hadoop Node
Info
Actions
0
0 1 2 3 4

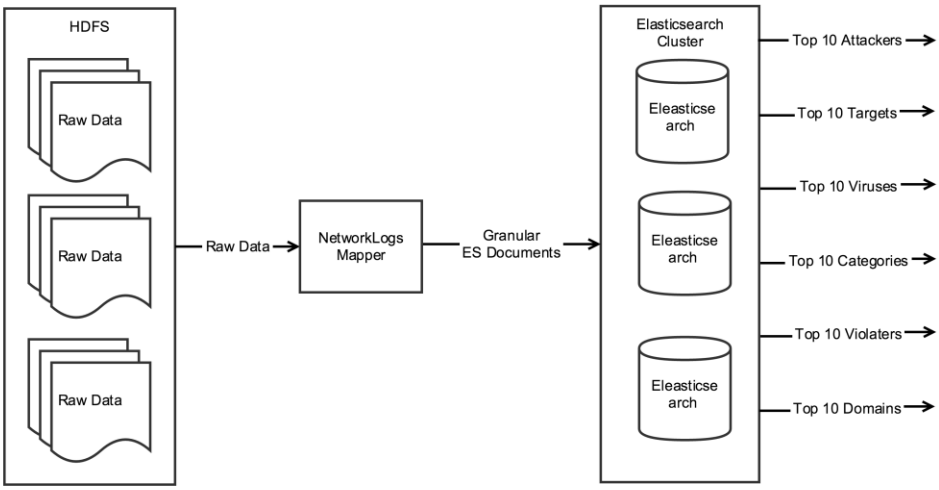

Overview
Indices
Browser
Structured Query [+]
Any Request [+]
Browser
All Indices
INDICES
.marvel-2015.05.10
eshadoop
TYPES
default
cluster_event
cluster_state
cluster_stats
index_event
index_stats
indices_stats
node_event
node_stats
routing_event
shard_event
wordcount
Searched 5 of 5 shards. 232 hits. 0.006 seconds
_index _type _id _score count ▲ word
eshadoop wordcount AU0-Z1QB_uhaCt797Fmf 14 the
eshadoop wordcount AU0-Z1QA_uhaCt797Fk3 14 elasticsearch-hadoop
eshadoop wordcount AU0-Z1QA_uhaCt797Fj_ 13 and
eshadoop wordcount AU0-Z1QB_uhaCt797Fmk 11 to
eshadoop wordcount AU0-Z1P__uhaCt797Fjf 10 Elasticsearch
eshadoop wordcount AU0-Z1P__uhaCt797Fjj 8 Hadoop
eshadoop wordcount AU0-Z1QA_uhaCt797FlV 6 is
eshadoop wordcount AU0-Z1QA_uhaCt797FlI 6 for
eshadoop wordcount AU0-Z1P__uhaCt797Fjt 5 Pig
eshadoop wordcount AU0-Z1QB_uhaCt797Fl4 5 or
eshadoop wordcount AU0-Z1QB_uhaCt797Flx 5 of
eshadoop wordcount AU0-Z1QB_uhaCt797Fm3 5 your
eshadoop wordcount AU0-Z1QA_uhaCt797Fkk 4 data
eshadoop wordcount AU0-Z1QA_uhaCt797FlY 4 its
eshadoop wordcount AU0-Z1QB_uhaCt797FmX 4 support

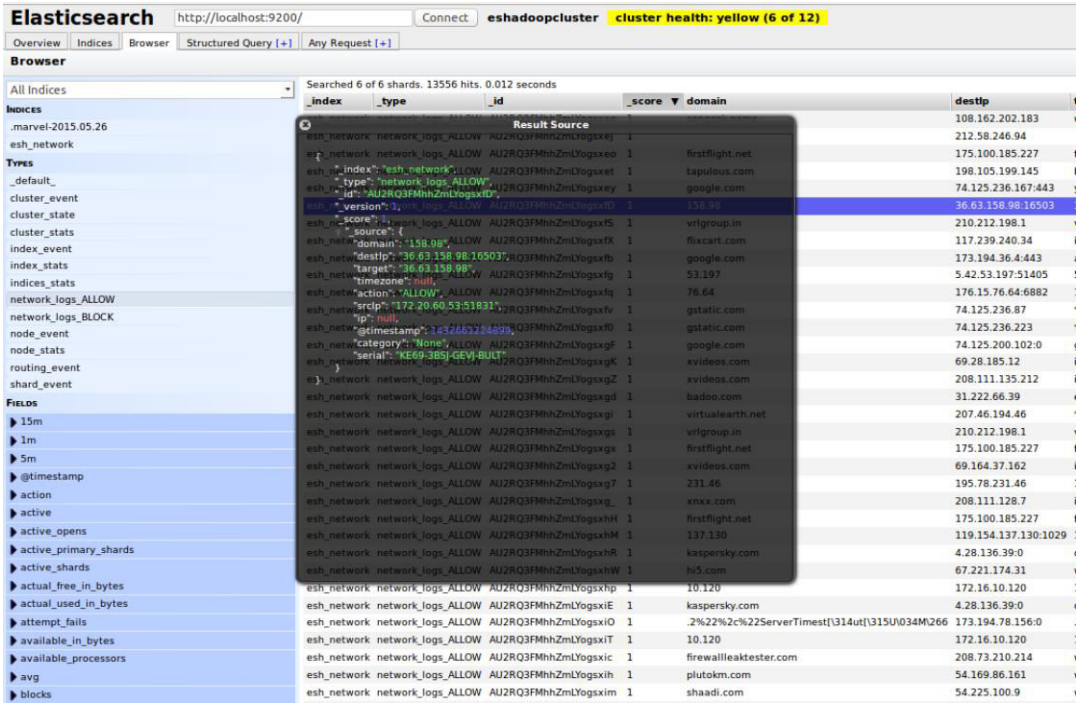

CLUSTER SUMMARY
Name: eshadoopcluster Status: yellow Nodes: 1 Indices: 2 Shards: 6 Data: 19.52 MB CPU: 2% Memory: 98.00 MB / 1015.69 MB Up time: 6.9 m Version: 1.5.1
DOCUMENT COUNT
SEARCH REQUEST RATE
INDEXING REQUEST RATE
NODES
1 of 1 nodes / 0 selected / Last 10m
Full / Compact
nodes
OS CPU (%)
Load (1m)
JVM Mem (%)
Disk Free Space
IOps
ES Hadoop Node
10.0.2.15:9300
22.0
0.2
9.0
29.7 GB
2.9
INDICES
2 of 2 indices / 0 selected / Last 10m
Full / Compact
indices
Documents
Index Rate
Search Rate
Merge Rate
Field Data
eshadoop
232.0
0.0
0.0
0.0
0.0
.marvel-2015.05.10
6.2 K
0.5
1.5
0.0
164.4 KB


Server
localhost:9200
GET eshadoop/_search
{
"query": {
"match_all": {}
}
}
{
"took": 15,
"timed_out": false,
"_shards": {
"total": 5,
"successful": 5,
"failed": 0
},
"hits": {
"total": 232,
"max_score": 1,
"hits": [
{
"_index": "eshadoop",
"_type": "wordcount",
"_id": "AU0-Z1P__uhaCt797FjU",
"_score": 1,
"_source": {
"count": 1,
"word": "1.x"
}
},
{
"_index": "eshadoop",
"_type": "wordcount",
"_id": "AU0-Z1P__uhaCt797FjZ",
"_score": 1,
"_source": {
"count": 1,
"word": "Adaptive"
}
},
{
"_index": "eshadoop",
"_type": "wordcount",
"_id": "AU0-Z1P__uhaCt797Fjd",
"_score": 1,
"_source": {
"count": 2,
"word": "At"
}
},

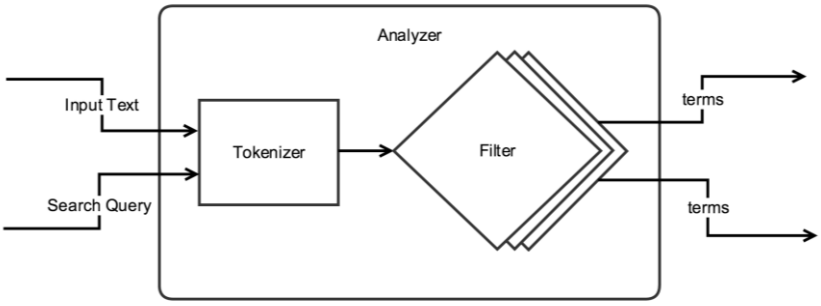
Chapter 2


HDFS
Raw Data
Raw Data
Raw Data
Raw data
MapReduce Job
AttackersCounterJob
TargetsCounterJob
VirusesCounterJob
CategoriesCounterJob
PolicyViolatorsCounter-Job
DomainsCounterJob
Counted metrics
TopNJob
TopN
HDFS
Raw Data
Raw Data
Raw Data

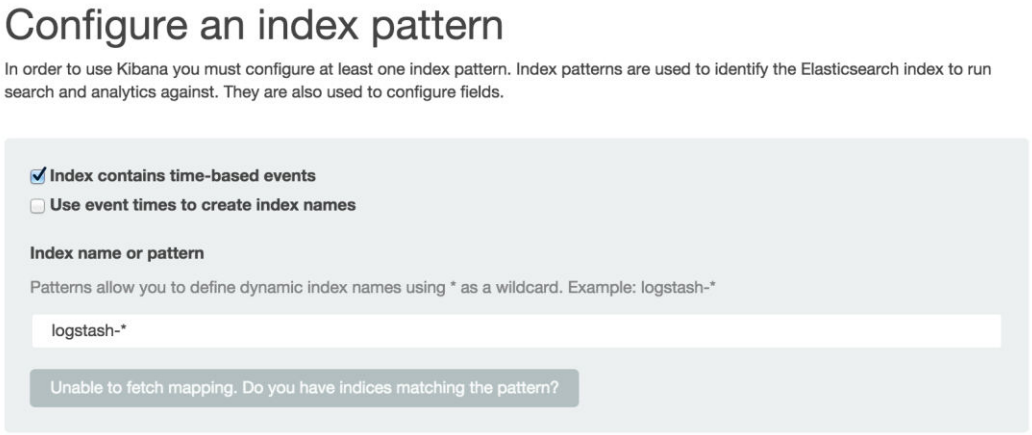

HDFS
Raw Data
Raw Data
Raw Data
Raw Data
NetworkLogs Mapper
Granular ES Documents
Elasticsearch Cluster
Eleasticse arch
Eleasticse arch
Eleasticse arch
Top 10 Attackers
Top 10 Targets
Top 10 Viruses
Top 10 Categories
Top 10 Violaters
Top 10 Domains

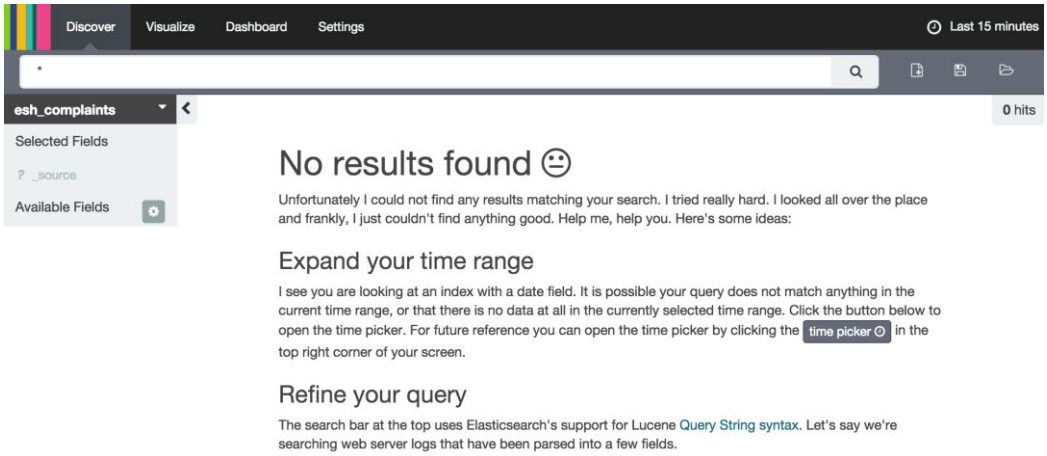

Elasticsearch
http://localhost:9200/
Connect
eshadoopcluster
cluster health: yellow (6 of 12)
Overview
Indices
Browser
Structured Query [+]
Any Request [+]
Browser
All Indices
Searched 6 of 6 shards. 13556 hits. 0.012 seconds
_index
_type
_id
_score
domain
destIp
Result Source
Indices
.marvel-2015.05.26
esh_network
Types
default
cluster_event
cluster_state
cluster_stats
index_event
index_stats
indices_stats
network_logs_ALLOW
network_logs_BLOCK
node_event
node_stats
routing_event
shard_event
Fields
15m
1m
5m
@timestamp
action
active
active_opens
active_primary_shards
active_shards
actual_free_in_bytes
actual_used_in_bytes
attempt_fails
available_in_bytes
available_processors
avg
blocks

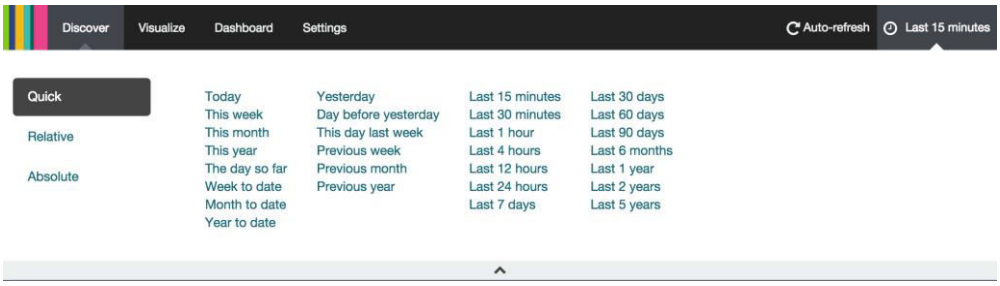
Chapter 3

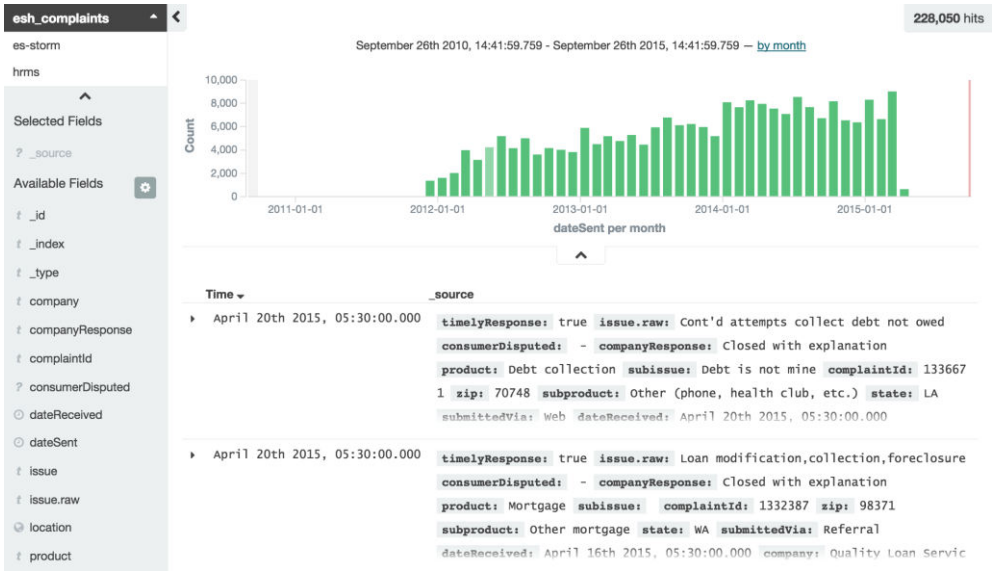

Analyzer
Input Text
Search Query
Tokenizer
Filter
terms
terms

Chapter 4


Configure an index pattern
In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.
Index contains time-based events
Use event times to create index names
Index name or pattern
Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*
logstash-*
Unable to fetch mapping. Do you have indices matching the pattern?


Discover
Visualize
Dashboard
Settings
Last 15 minutes
esh_complaints
0 hits
Selected Fields
? _source
Available Fields
No results found
Unfortunately I could not find any results matching your search. I tried really hard. I looked all over the place and frankly, I just couldn't find anything good. Help me, help you. Here's some ideas:
Expand your time range
I see you are looking at an index with a date field. It is possible your query does not match anything in the current time range, or that there is no data at all in the currently selected time range. Click the button below to open the time picker. For future reference you can open the time picker by clicking the time picker in the top right corner of your screen.
Refine your query
The search bar at the top uses Elasticsearch's support for Lucene Query String syntax. Let's say we're searching web server logs that have been parsed into a few fields.

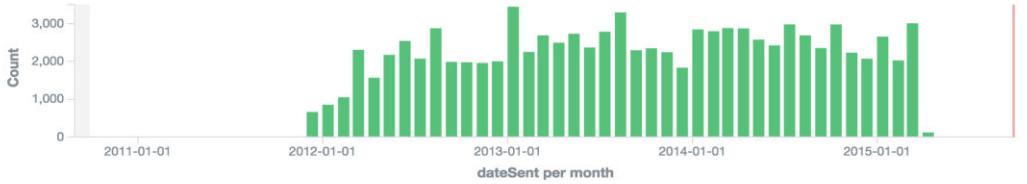

Discover
Visualize
Dashboard
Settings
Auto-refresh
Last 15 minutes
Quick
Relative
Absolute
Today
This week
This month
This year
The day so far
Week to date
Month to date
Year to date
Yesterday
Day before yesterday
This day last week
Previous week
Previous month
Previous year
Last 15 minutes
Last 30 minutes
Last 1 hour
Last 4 hours
Last 12 hours
Last 24 hours
Last 7 days
Last 30 days
Last 60 days
Last 90 days
Last 6 months
Last 1 year
Last 2 years
Last 5 years



April 20th 2015, 05:30:00.000 1332387 Mortgage Loan modification,collection,foreclosure

Table JSON Link to /esh_complaints/complaints/AU89Hib6E2xLOyMazTAO

t _id	AU89Hib6E2xLOyMazTAO
t _index	esh_complaints
t _type	complaints
t company	Quality Loan Service Corporation
t companyResponse	Closed with explanation
t complaintId	1332387
? consumerDisputed	-
dateReceived	April 16th 2015, 05:30:00.000
dateSent	April 20th 2015, 05:30:00.000
t issue	Loan modification,collection,foreclosure
t issue.raw	Loan modification,collection,foreclosure
location	47.196272, -122.31577
t product	Mortgage



Time	complaintId	product	issue
April 20th 2015, 05:30:00.000	1332387	Mortgage	Loan modification,collection,foreclosure
April 20th 2015, 05:30:00.000	1336622	Mortgage	Loan servicing, payments, escrow account
April 20th 2015, 05:30:00.000	1324585	Consumer loan	Managing the loan or lease

Table JSON

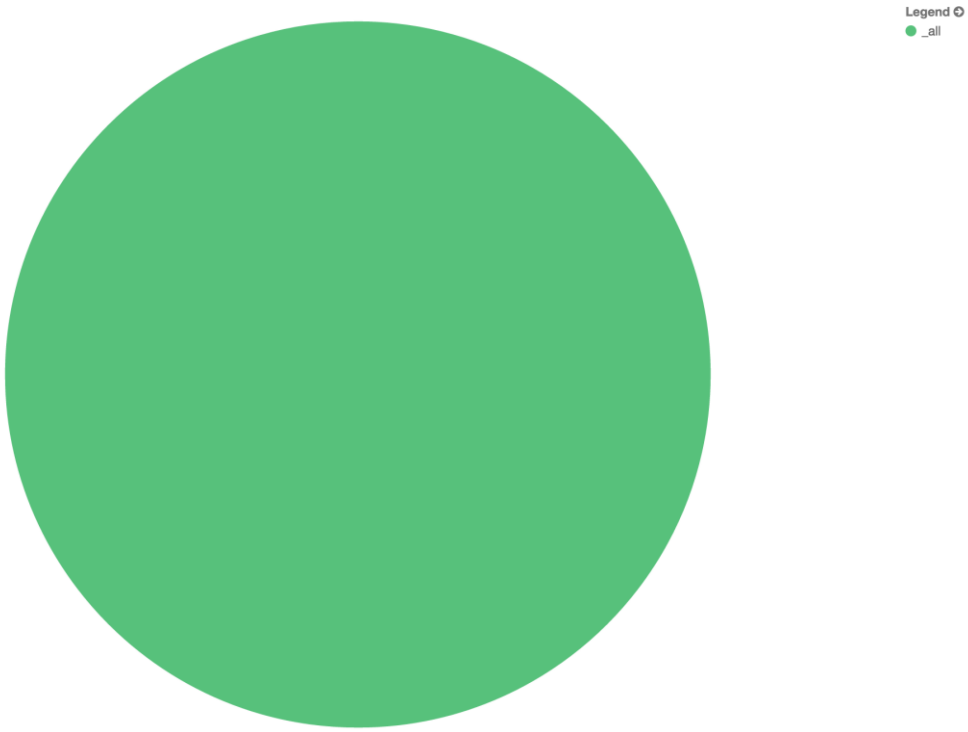
Link to /esh_complaints/complaints/AU89G1uLE2xL0yMayzIF

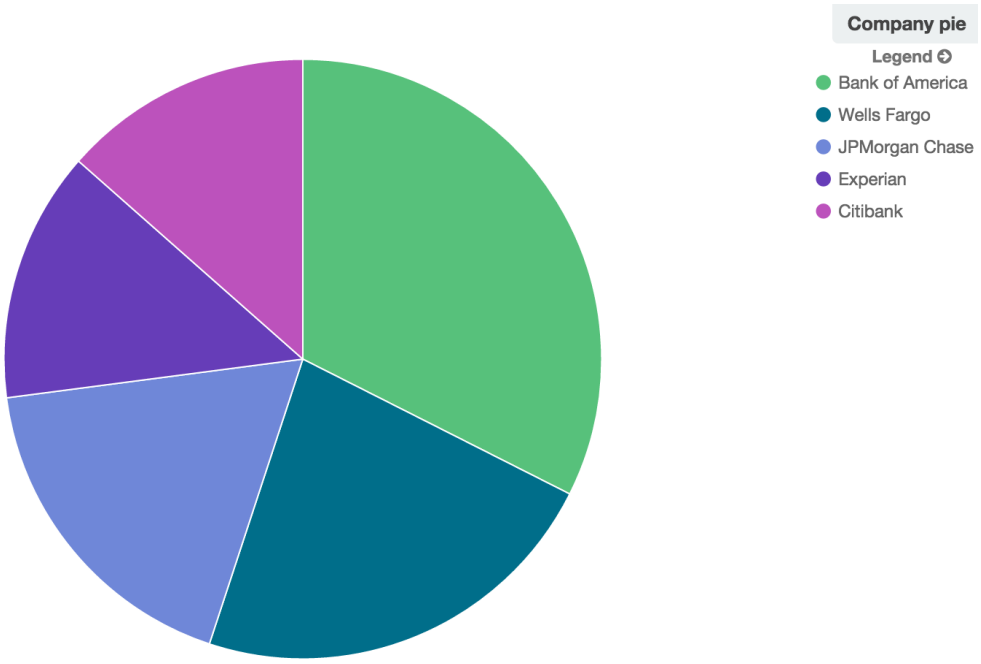
t _id	AU89G1uLE2xL0yMayzIF
t _index	esh_complaints

Create a new visualization

Step 1

Area chart	Great for stacked timelines in which the total of all series is more important than comparing any two or more series. Less useful for assessing the relative change of unrelated data points as changes in a series lower down the stack will have a difficult to gauge effect on the series above it.
Data table	The data table provides a detailed breakdown, in tabular format, of the results of a composed aggregation. Tip, a data table is available from many other charts by clicking grey bar at the bottom of the chart.
Line chart	Often the best chart for high density time series. Great for comparing one series to another. Be careful with sparse sets as the connection between points can be misleading.
Markdown widget	Useful for displaying explanations or instructions for dashboards.
Metric	One big number for all of your one big number needs. Perfect for show a count of hits, or the exact average a numeric field.
Pie chart	Pie charts are ideal for displaying the parts of some whole. For example, sales percentages by department.Pro Tip: Pie charts are best used sparingly, and with no more than 7 slices per pie.
Tile map	Your source for geographic maps. Requires an elasticsearch geo_point field. More specifically, a field that is mapped as type:geo_point with latitude and longitude coordinates.
Vertical bar chart	The goto chart for oh-so-many needs. Great for time and non-time data. Stacked or grouped, exact numbers or percentages. If you are not sure which chart your need, you could do worse than to start here.


Legend
_all


Company pie
Legend
Bank of America
Wells Fargo
JPMorgan Chase
Experian
Citibank

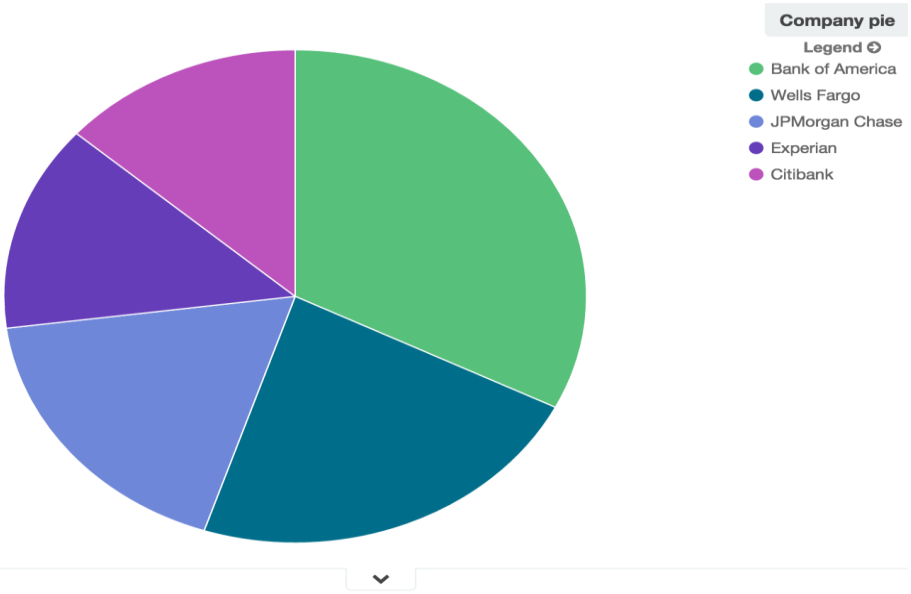
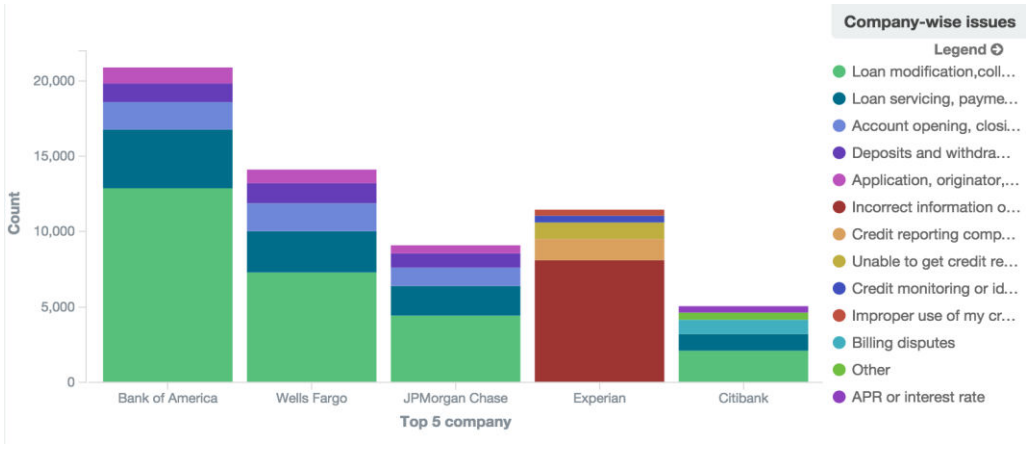
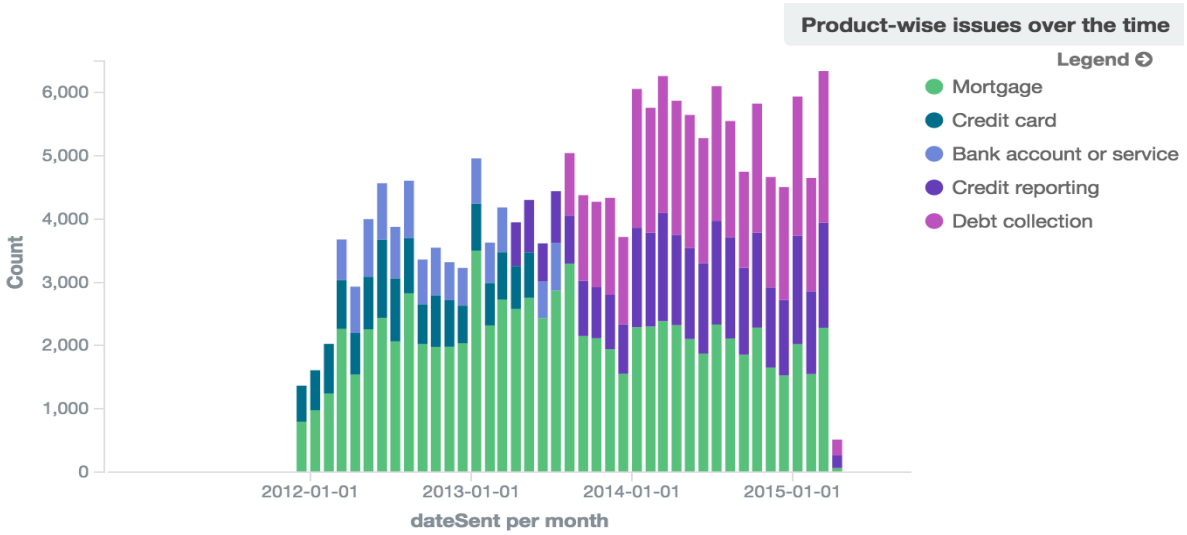
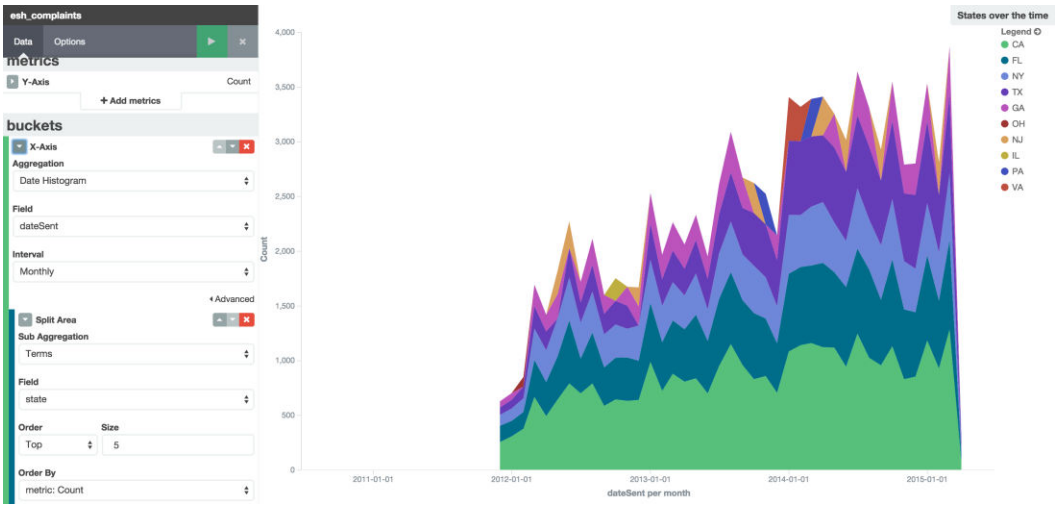


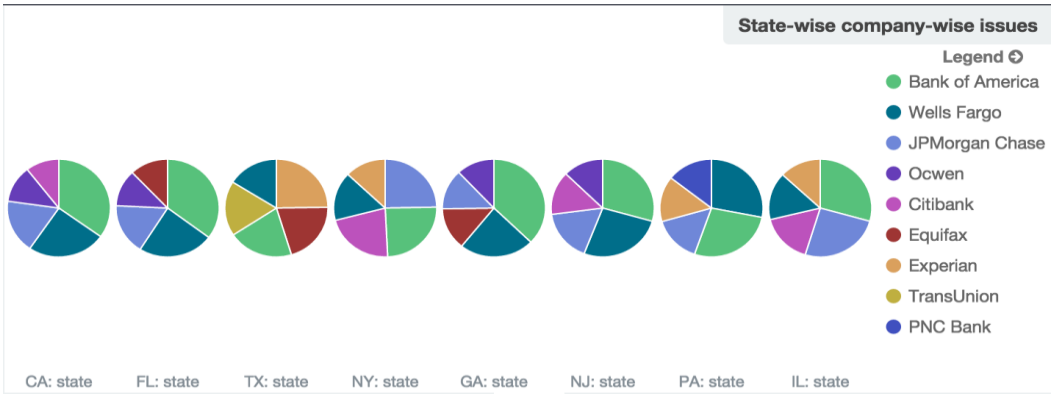
Table | Request | Response | Statistics

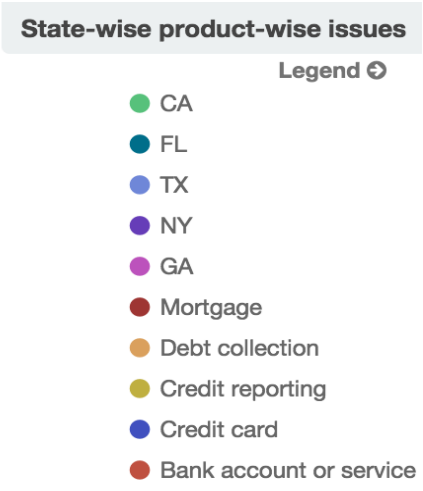
Top 5 company	Count
Bank of America	27,574
Wells Fargo	19,249
JPMorgan Chase	15,201
Experian	11,523
Citibank	11,491

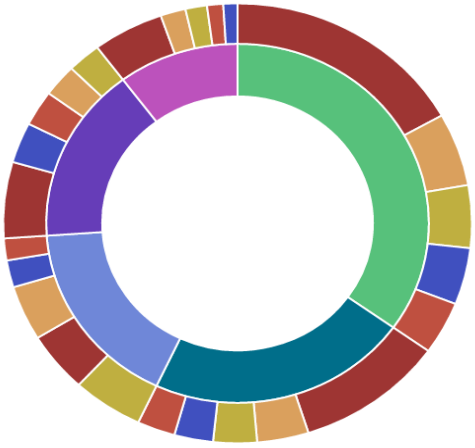



Product-wise issues over the time
Legend
Mortgage
Credit card
Bank account or service
Credit reporting
Debt collection
Count
6,000
5,000
4,000
3,000
2,000
1,000
0
2012-01-01
2013-01-01
2014-01-01
2015-01-01
dateSent per month

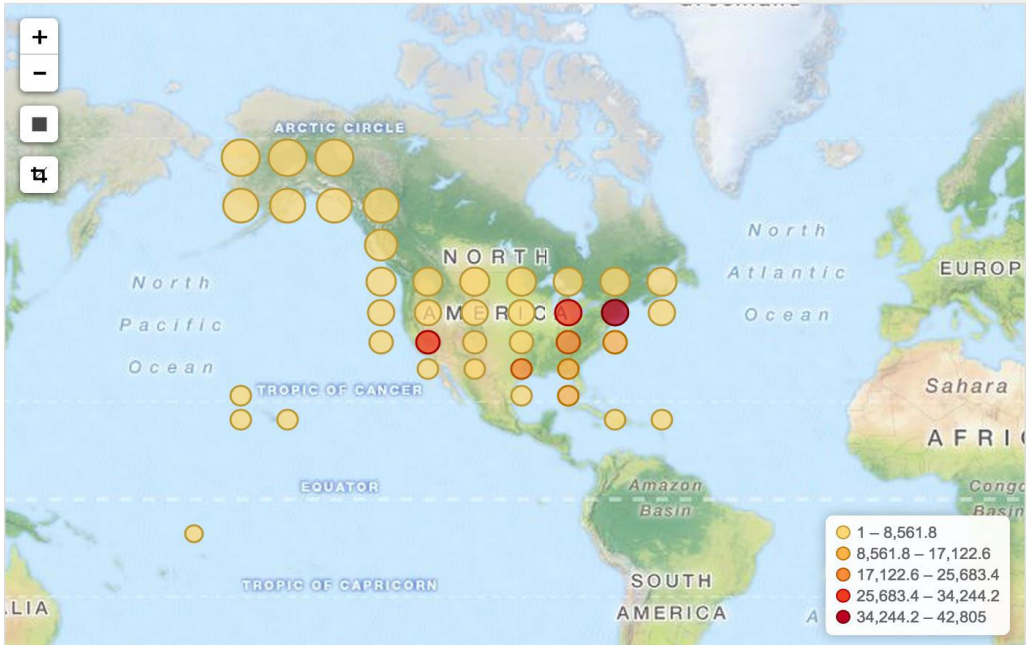

esh_complaints
Data
Options
metrics
Y-Axis
Count
+ Add metrics
buckets
X-Axis
Aggregation
Date Histogram
Field
dateSent
Interval
Monthly
Advanced
Split Area
Sub Aggregation
Terms
Field
state
Order
Top
Size
5
Order By
metric: Count
States over the time
Legend
CA
FL
NY
TX
GA
OH
NJ
IL
PA
VA
Count
4,000
3,500
3,000
2,500
2,000
1,500
1,000
500
0
2011-01-01
2012-01-01
2013-01-01
2014-01-01
2015-01-01
dateSent per month


State-wise company-wise issues
Legend
Bank of America
Wells Fargo
JPMorgan Chase
Ocwen
Citibank
Equifax
Experian
TransUnion
PNC Bank
CA: state
FL: state
TX: state
NY: state
GA: state
NJ: state
PA: state
IL: state


State-wise product-wise issues
Legend
CA
FL
TX
NY
GA
Mortgage
Debt collection
Credit reporting
Credit card
Bank account or service



Geography-wise issues

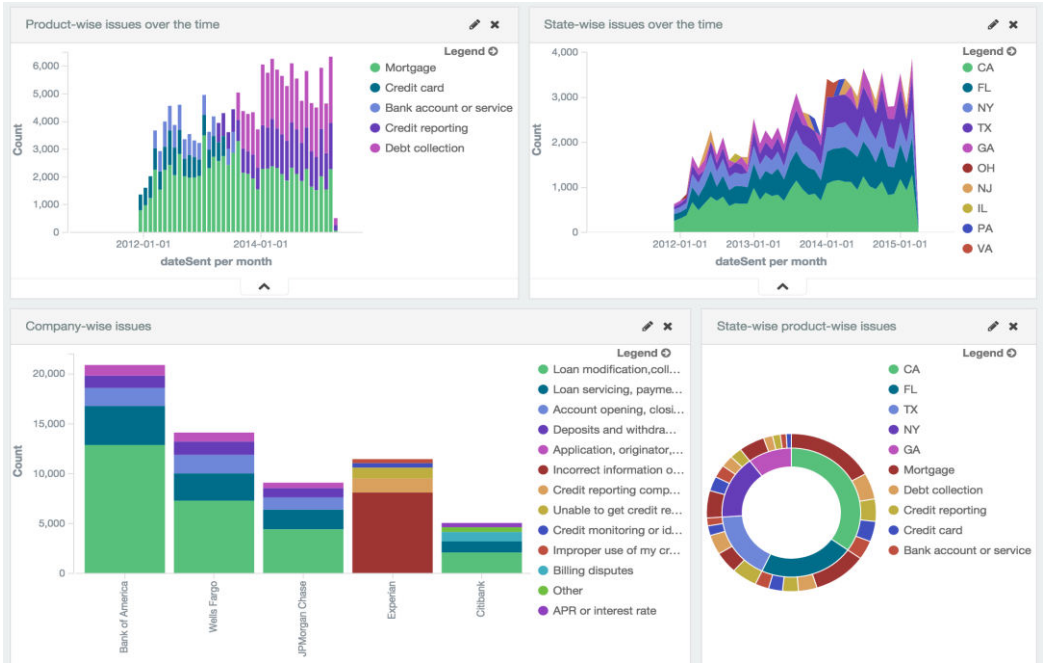


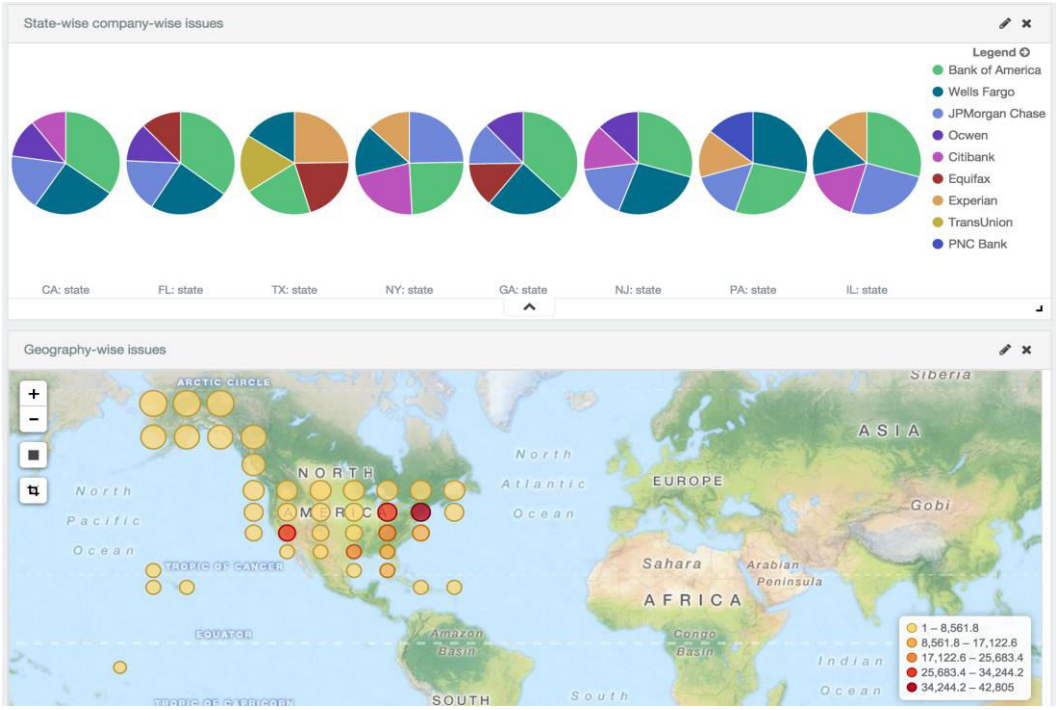
Visualizations | Searches

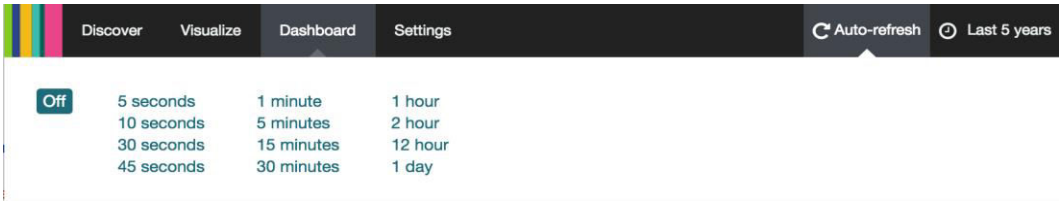
manage visualizations

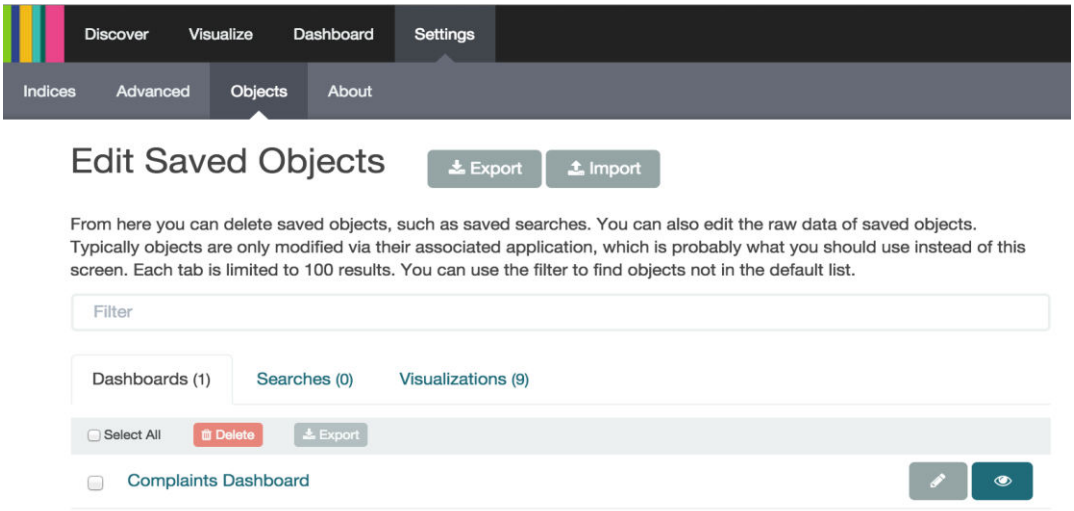
prod — 2 visualizations

- Product-wise issues over the time
- State-wise product-wise issues

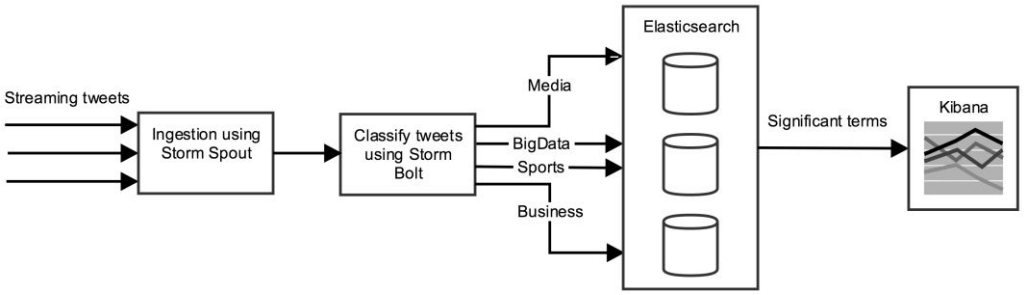

Product-wise issues over the time
Count
6,000
5,000
4,000
3,000
2,000
1,000
0
2012-01-01
2014-01-01
dateSent per month
Legend
Mortgage
Credit card
Bank account or service
Credit reporting
Debt collection
State-wise issues over the time
Count
4,000
3,000
2,000
1,000
0
2012-01-01
2013-01-01
2014-01-01
2015-01-01
dateSent per month
Legend
CA
FL
NY
TX
GA
OH
NJ
IL
PA
VA
Company-wise issues
Count
20,000
15,000
10,000
5,000
0
Bank of America
Wells Fargo
JPMorgan Chase
Experian
Citibank
Legend
Loan modification,coll...
Loan servicing, payme...
Account opening, closi...
Deposits and withdra...
Application, originator,...
Incorrect information o...
Credit reporting comp...
Unable to get credit re...
Credit monitoring or id...
Improper use of my cr...
Billing disputes
Other
APR or interest rate
State-wise product-wise issues
Legend
CA
FL
TX
NY
GA
Mortgage
Debt collection
Credit reporting
Credit card
Bank account or service

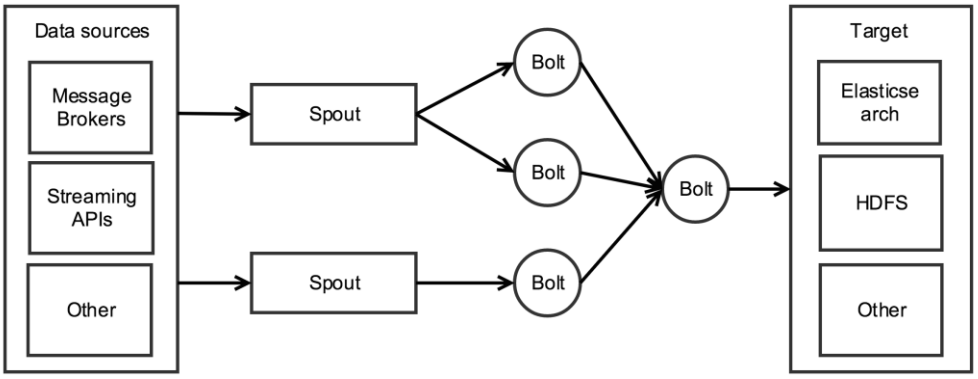

State-wise company-wise issues
Legend
Bank of America
Wells Fargo
JPMorgan Chase
Ocwen
Citibank
Equifax
Experian
TransUnion
PNC Bank
CA: state
FL: state
TX: state
NY: state
GA: state
NJ: state
PA: state
IL: state
Geography-wise issues
ARCTIC CIRCLE
NORTH
AMERICA
North
Pacific
Ocean
North
Atlantic
Ocean
EUROPE
ASIA
Siberia
Gobi
Sahara
Arabian
Peninsula
AFRICA
TROPIC OF CANCER
EQUATOR
Amazon
Basin
Congo
Basin
Indian
Ocean
SOUTH
South
1 – 8,561.8
8,561.8 – 17,122.6
17,122.6 – 25,683.4
25,683.4 – 34,244.2
34,244.2 – 42,805

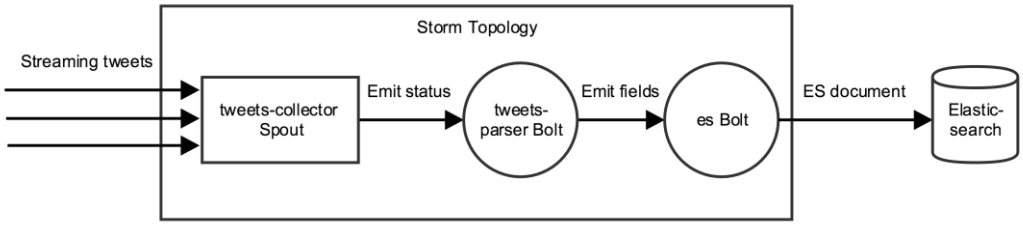

Discover
Visualize
Dashboard
Settings
Auto-refresh
Last 5 years
Off
5 seconds
10 seconds
30 seconds
45 seconds
1 minute
5 minutes
15 minutes
30 minutes
1 hour
2 hour
12 hour
1 day

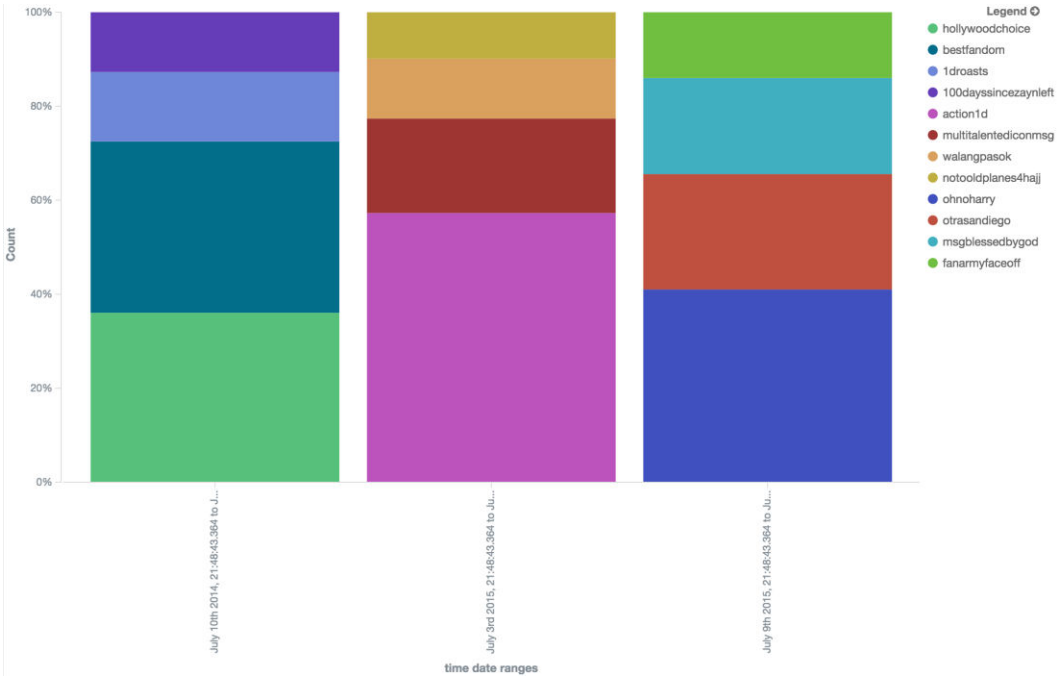

Discover
Visualize
Dashboard
Settings
Indices
Advanced
Objects
About
Edit Saved Objects
Export
Import
From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects.
Typically objects are only modified via their associated application, which is probably what you should use instead of this
screen. Each tab is limited to 100 results. You can use the filter to find objects not in the default list.
Filter
Dashboards (1)
Searches (0)
Visualizations (9)
Select All
Delete
Export
Complaints Dashboard

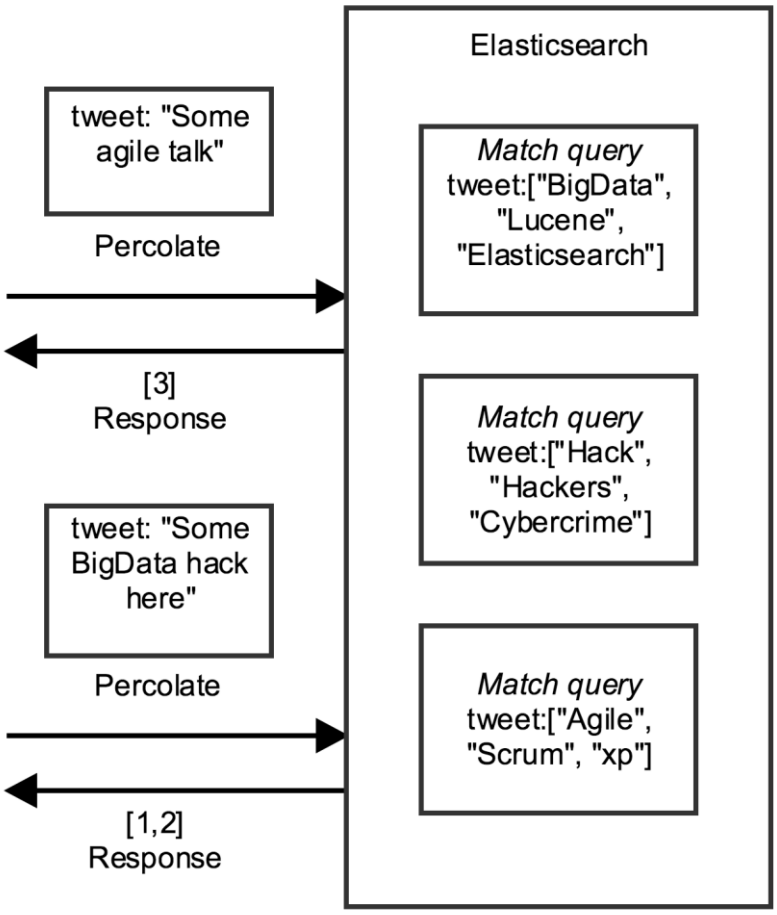
Chapter 5


Streaming tweets
Ingestion using Storm Spout
Classify tweets using Storm Bolt
Media
BigData
Sports
Business
Elasticsearch
Significant terms
Kibana

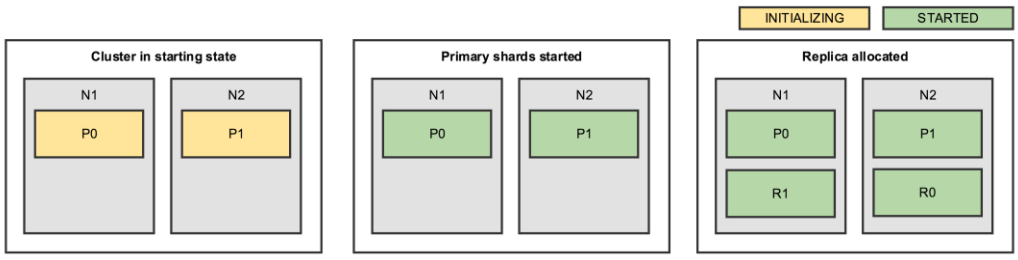

Data sources
Message Brokers
Streaming APIs
Other
Spout
Spout
Bolt
Bolt
Bolt
Bolt
Target
Elasticse arch
HDFS
Other

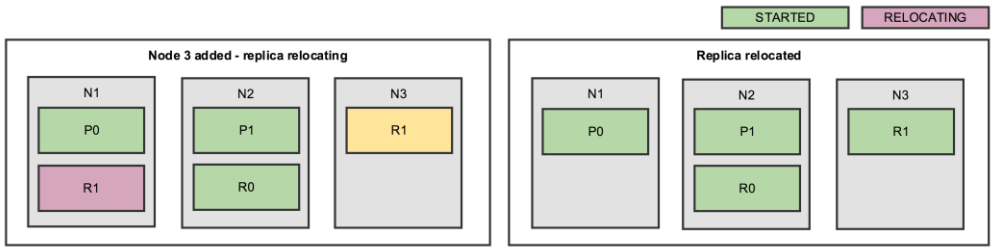

Storm Topology
Streaming tweets
tweets-collector Spout
Emit status
tweets-parser Bolt
Emit fields
es Bolt
ES document
Elastic-search

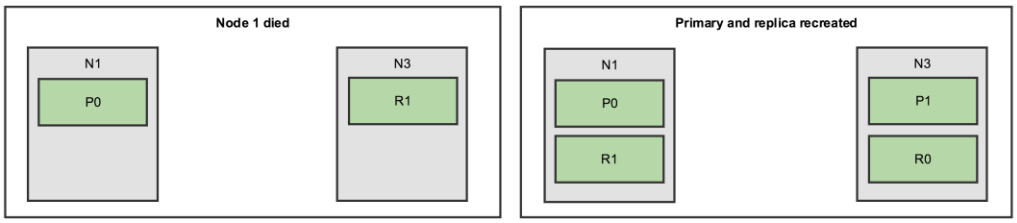

100%
80%
60%
40%
20%
0%
Count
July 10th 2014, 21:48:43.364 to J...
July 3rd 2015, 21:48:43.364 to Ju...
July 9th 2015, 21:48:43.364 to Ju...
time date ranges
Legend
hollywoodchoice
bestfandom
1droasts
100dayssincezaynleft
action1d
multitalentediconmsg
walangpasok
notooldplanes4hajj
ohnoharry
otrasandiego
msgblessedbygod
fanarmyfaceoff

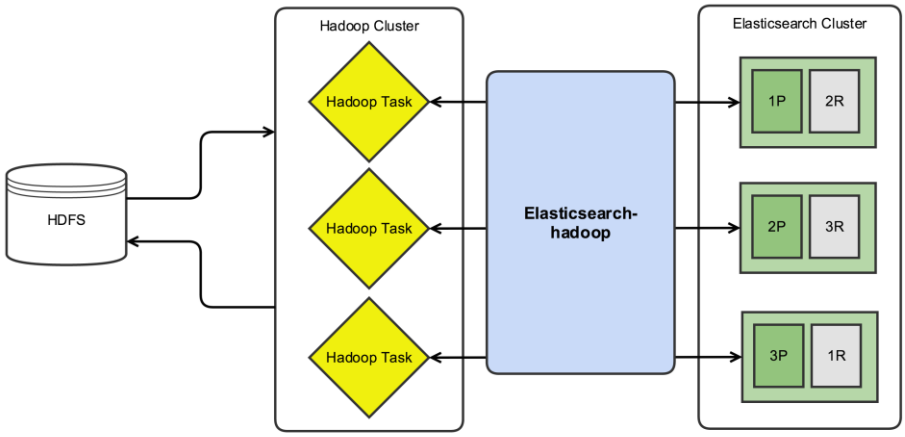

Elasticsearch
tweet: "Some agile talk"
Percolate
[3]
Response
tweet: "Some BigData hack here"
Percolate
[1,2]
Response
Match query tweet:["BigData", "Lucene", "Elasticsearch"]
Match query tweet:["Hack", "Hackers", "Cybercrime"]
Match query tweet:["Agile", "Scrum", "xp"]

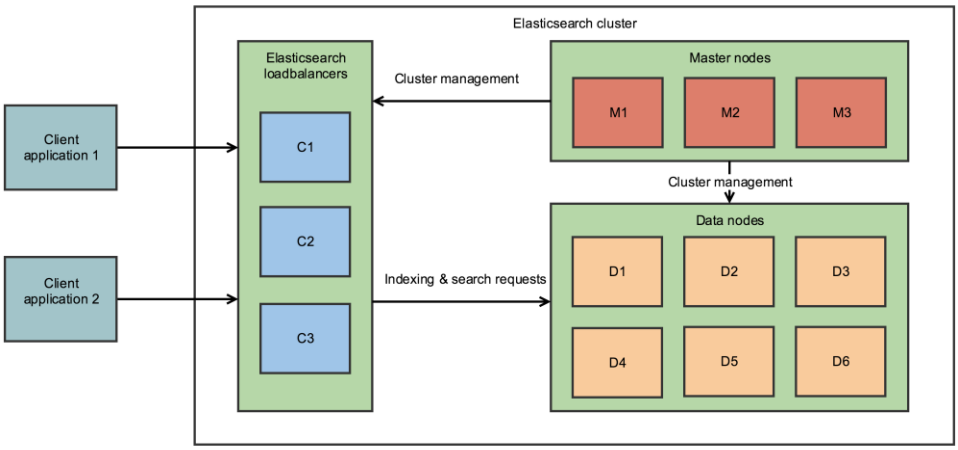
Chapter 6

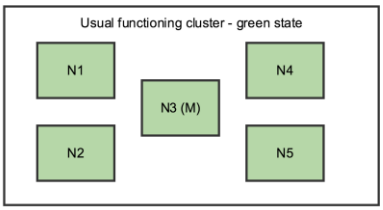

INITIALIZING
STARTED
Cluster in starting state
Primary shards started
Replica allocated
N1
N2
P0
P1
R1
R0

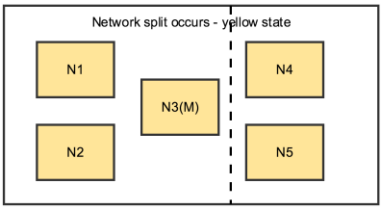

STARTED
RELOCATING
Node 3 added - replica relocating
N1
P0
R1
N2
P1
R0
N3
R1
Replica relocated
N1
P0
N2
P1
R0
N3
R1

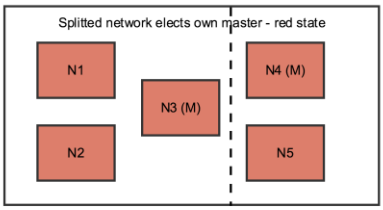

Node 1 died
N1
P0
N3
R1
Primary and replica recreated
N1
P0
R1
N3
P1
R0


Hadoop Cluster
Hadoop Task
Hadoop Task
Hadoop Task
HDFS
Elasticsearch-hadoop
Elasticsearch Cluster
1P
2R
2P
3R
3P
1R


Elasticsearch cluster
Elasticsearch loadbalancers
C1
C2
C3
Cluster management
Master nodes
M1
M2
M3
Cluster management
Data nodes
D1
D2
D3
D4
D5
D6
Indexing & search requests
Client application 1
Client application 2


Usual functioning cluster - green state
N1
N2
N3 (M)
N4
N5


Network split occurs - yellow state
N1
N2
N3(M)
N4
N5


Splitted network elects own master - red state
N1
N2
N3 (M)
N4 (M)
N5