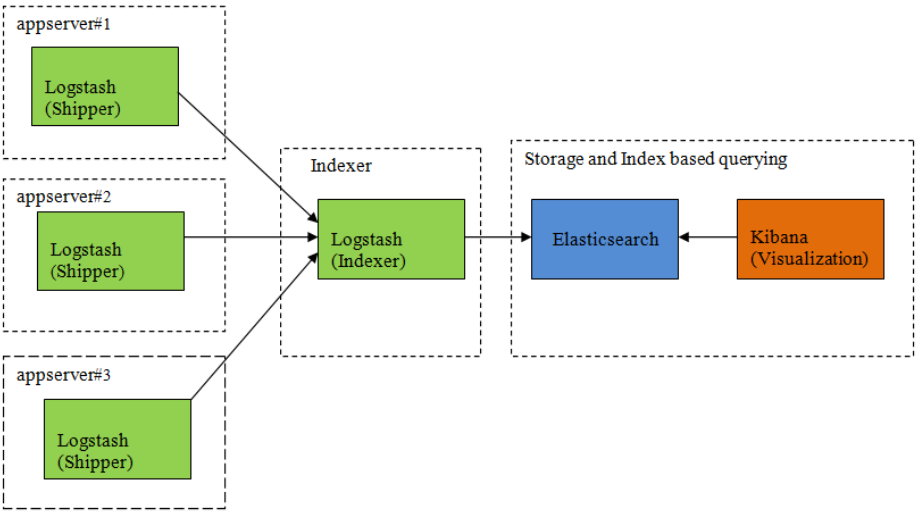
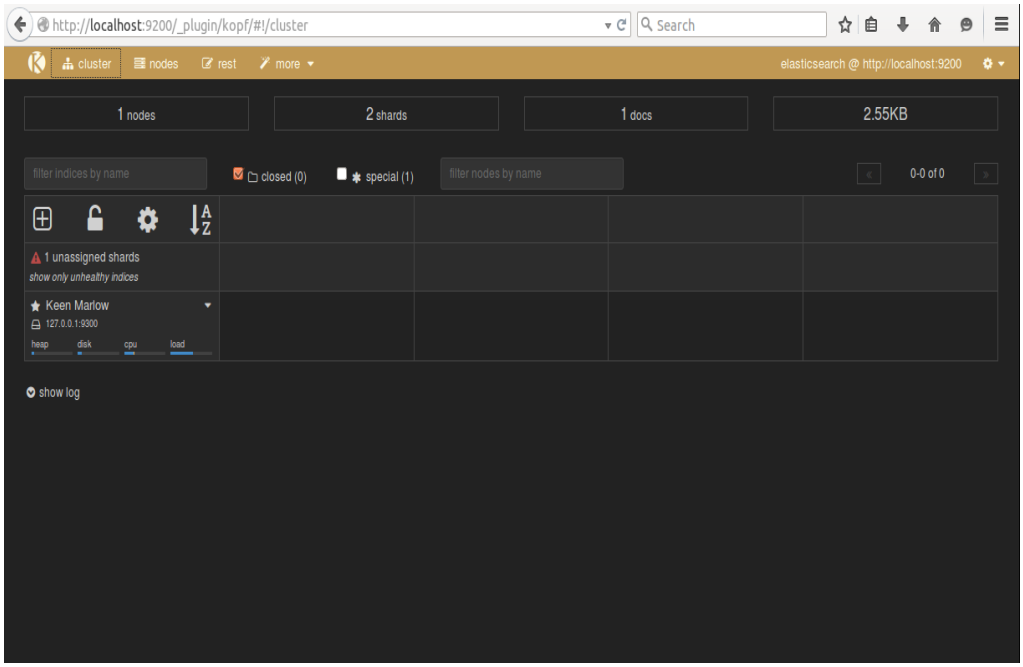
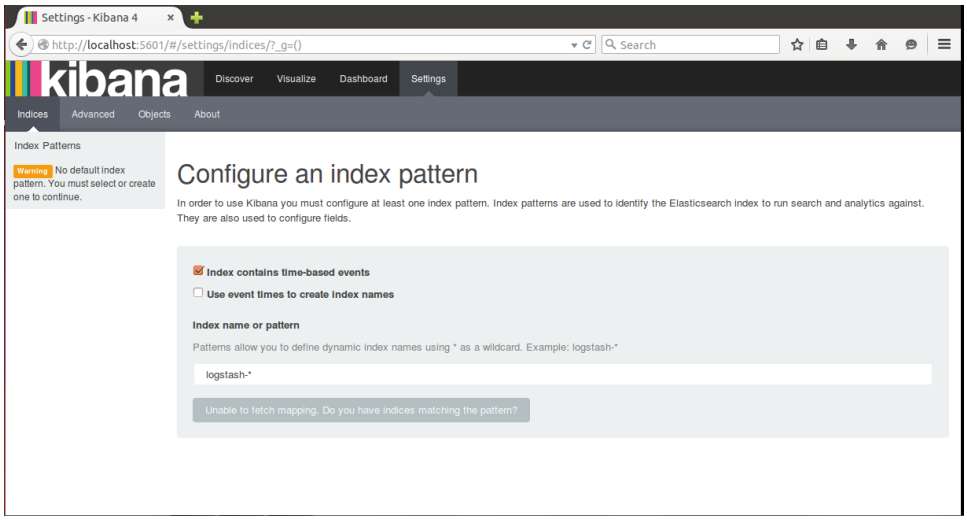
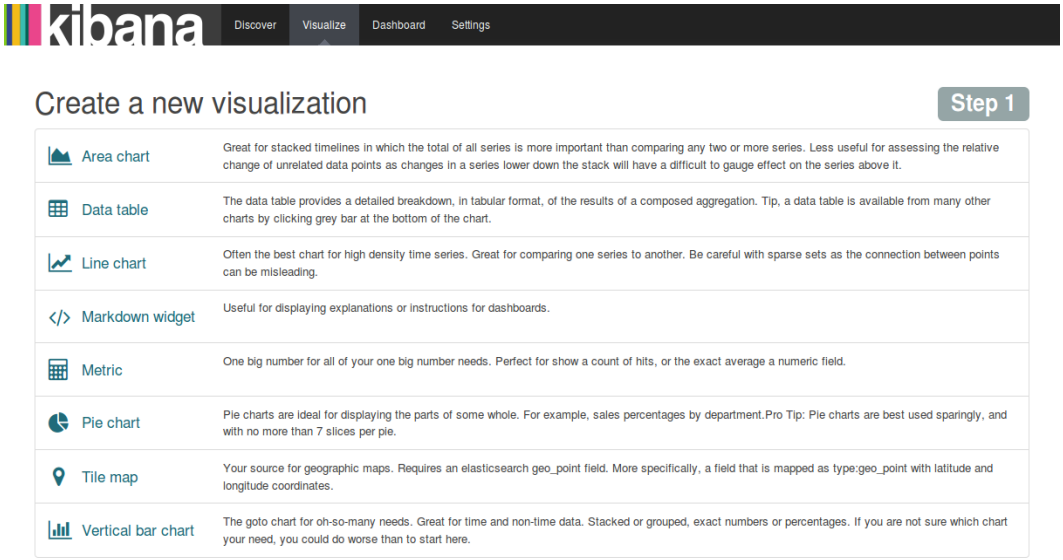
Chapter 1


appserver#1
Logstash
(Shipper)
appserver#2
Logstash
(Shipper)
appserver#3
Logstash
(Shipper)
Indexer
Logstash
(Indexer)
Storage and Index based querying
Elasticsearch
Kibana
(Visualization)

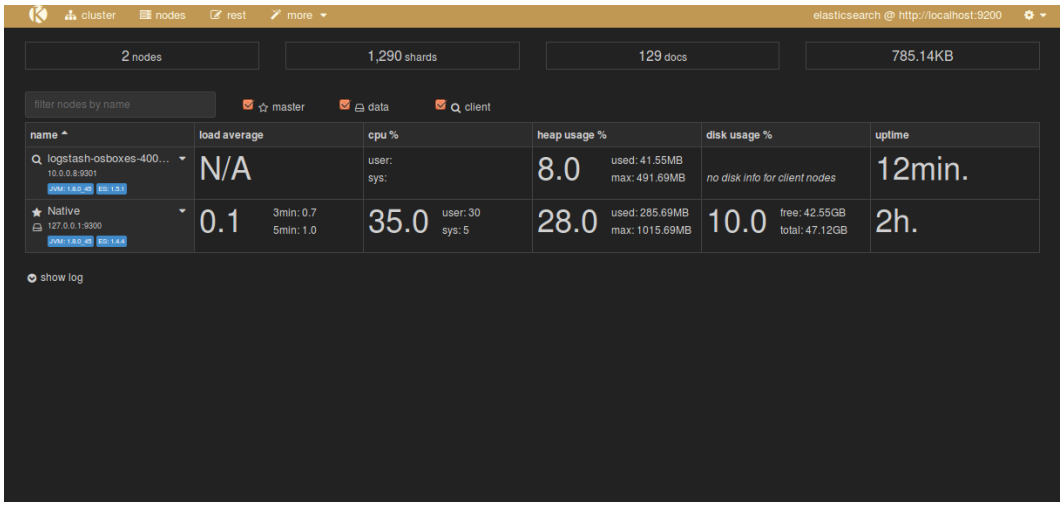

http://localhost:9200/_plugin/kopf/#!/cluster
Search
cluster
nodes
rest
more
elasticsearch @ http://localhost:9200
1 nodes
2 shards
1 docs
2.55KB
filter indices by name
closed (0)
special (1)
filter nodes by name
0-0 of 0
1 unassigned shards
show only unhealthy indices
Keen Marlow
127.0.0.1:9300
heap
disk
cpu
load
show log

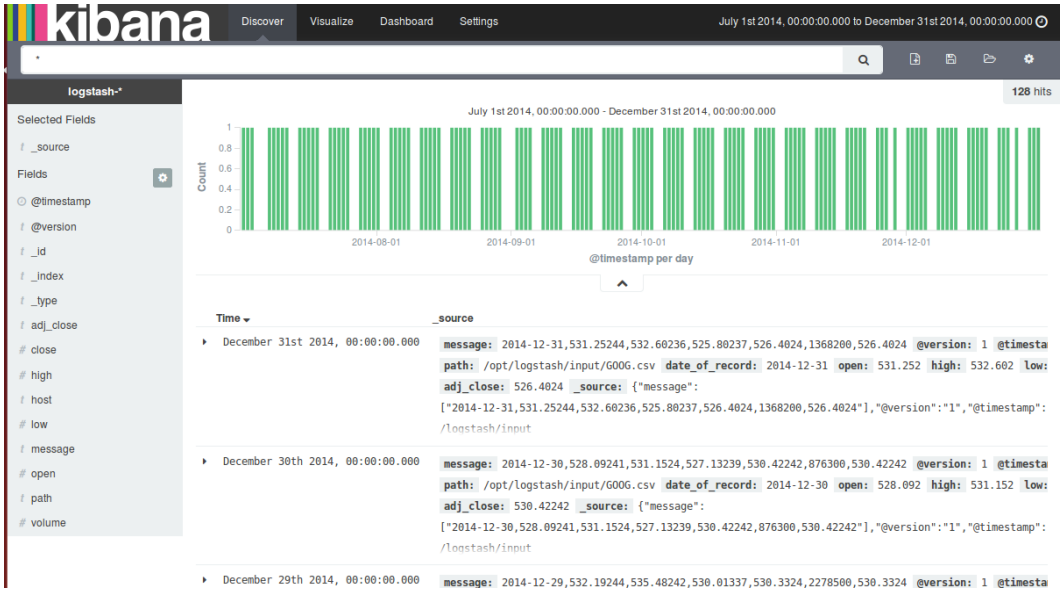

Settings - Kibana 4
http://localhost:5601/#/settings/indices/?_g=()
Search
kibana
Discover
Visualize
Dashboard
Settings
Indices
Advanced
Objects
About
Index Patterns
Warning No default index pattern. You must select or create one to continue.
Configure an index pattern
In order to use Kibana you must 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?

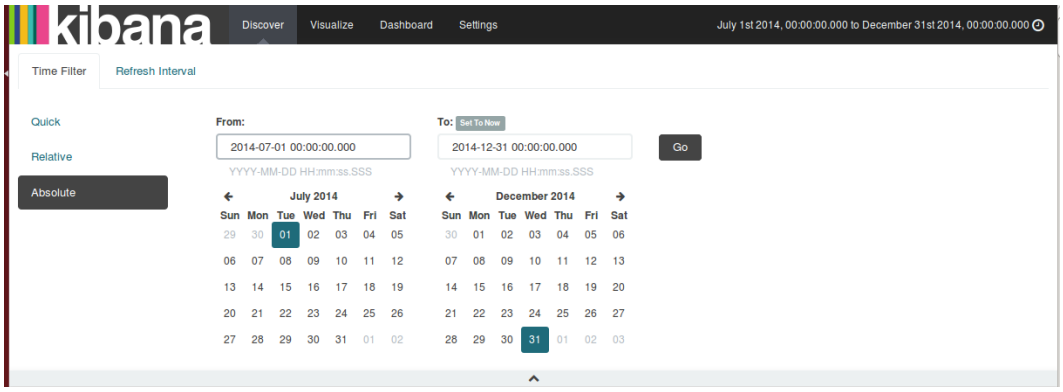

http://localhost:5601/#/discover?_g=(time:(from:now-30d,mode:quick,to:now))&_a=(columns:!(_s
Search
kibana
Discover
Visualize
Dashboard
Settings
Last 30 days
logstash-*
21 hits
Selected Fields
_source
Fields
@timestamp
@version
_id
_index
_type
adj_close
close_price
date_of_record
high_price
host
low_price
message
open_price
April 24th 2015, 18:19:36.759 - May 24th 2015, 18:19:36.764
Count
2015-04-27 01:00
2015-05-01 01:00
2015-05-05 01:00
2015-05-09 01:00
2015-05-13 01:00
2015-05-17 01:00
2015-05-21 01:00
@timestamp per 12 hours
Time
_source
May 22nd 2015, 00:00:00.000
May 21st 2015, 00:00:00.000

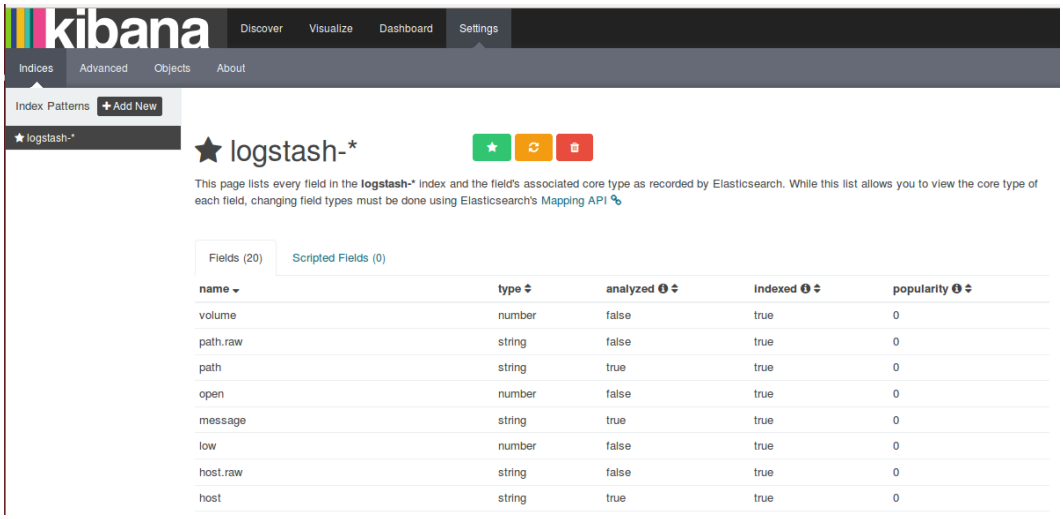

kibana
Discover
Visualize
Dashboard
Settings
Create a new visualization
Step 1
Area chart
Great for stacked timelines in which the total of all series is more important than comparing any two or more series. Less useful for assessing the relative change of unrelated data points as changes in a series 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.

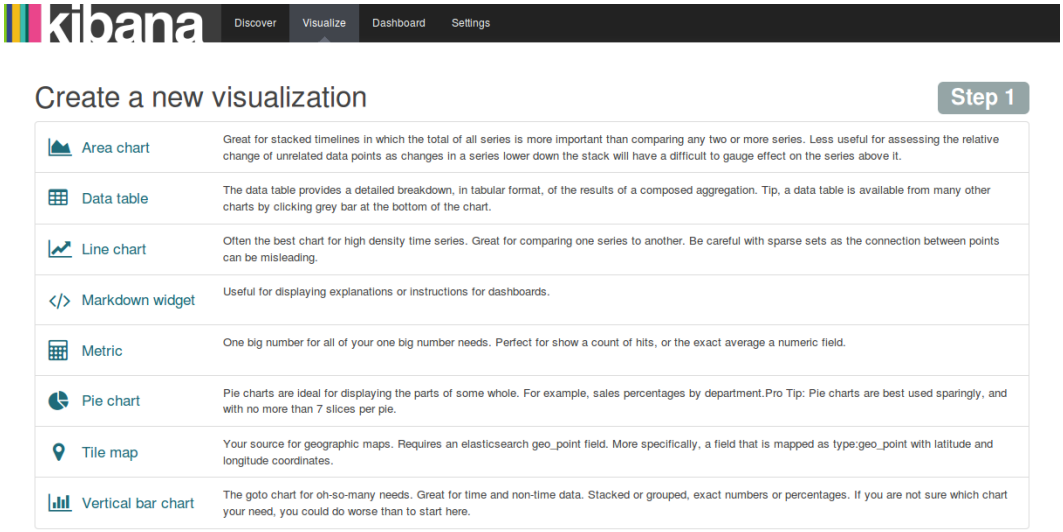
Chapter 2

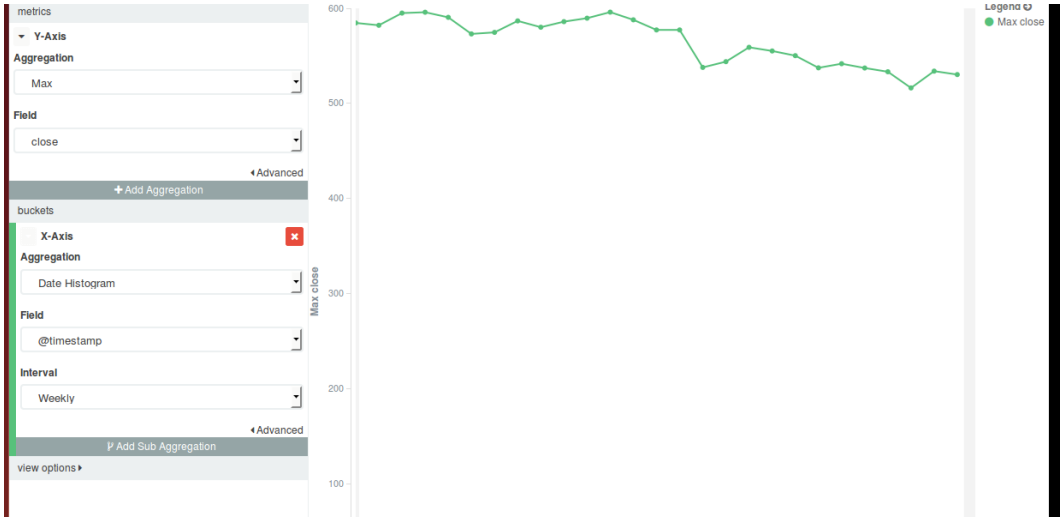

cluster
nodes
rest
more
elasticsearch @ http://localhost:9200
2 nodes
1,290 shards
129 docs
785.14KB
filter nodes by name
master
data
client
name
load average
cpu %
heap usage %
disk usage %
uptime
logstash-osboxes-400...
10.0.0.8:9301
N/A
user:
sys:
8.0
used: 41.55MB
max: 491.69MB
no disk info for client nodes
12min.
Native
127.0.0.1:9300
0.1
3min: 0.7
5min: 1.0
35.0
user: 30
sys: 5
28.0
used: 285.69MB
max: 1015.69MB
10.0
free: 42.55GB
total: 47.12GB
2h.
show log

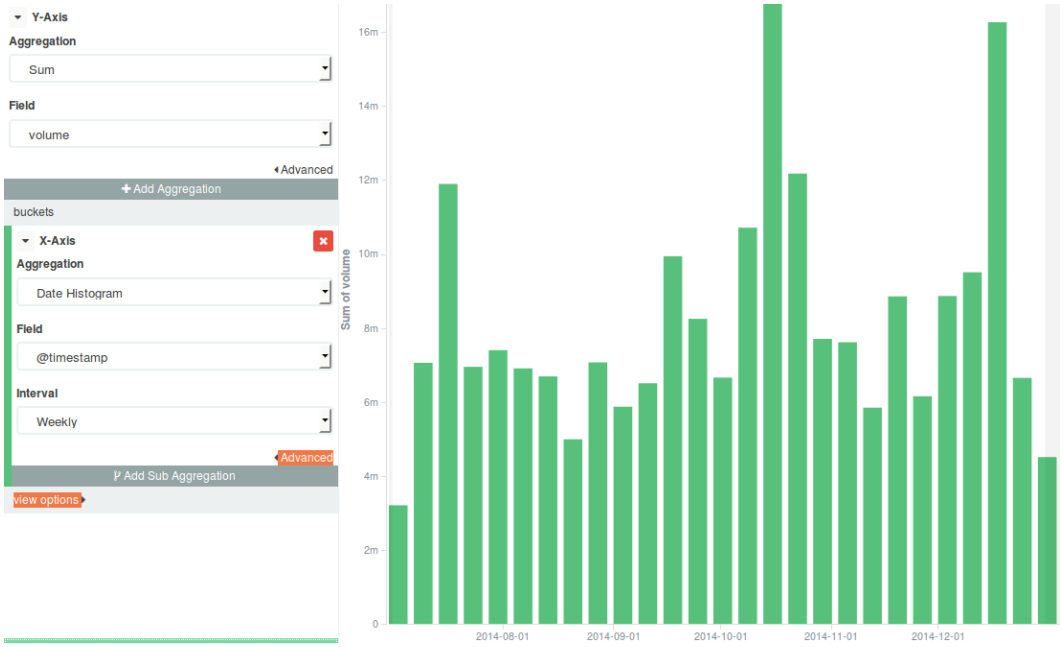

kibana
Discover
Visualize
Dashboard
Settings
July 1st 2014, 00:00:00.000 to December 31st 2014, 00:00:00.000
*
logstash-*
128 hits
Selected Fields
_source
Fields
@timestamp
@version
_id
_index
_type
adj_close
close
high
host
low
message
open
path
volume
July 1st 2014, 00:00:00.000 - December 31st 2014, 00:00:00.000
Count
2014-08-01
2014-09-01
2014-10-01
2014-11-01
2014-12-01
@timestamp per day
Time
_source
December 31st 2014, 00:00:00.000
message: 2014-12-31,531.25244,532.60236,525.80237,526.4024,1368200,526.4024 @version: 1 @timesta
path: /opt/logstash/input/GOOG.csv date_of_record: 2014-12-31 open: 531.252 high: 532.602 low:
adj_close: 526.4024 _source: {"message":
["2014-12-31,531.25244,532.60236,525.80237,526.4024,1368200,526.4024"],"@version":"1","@timestamp":
/logstash/input
December 30th 2014, 00:00:00.000
message: 2014-12-30,528.09241,531.1524,527.13239,530.42242,876300,530.42242 @version: 1 @timesta
path: /opt/logstash/input/GOOG.csv date_of_record: 2014-12-30 open: 528.092 high: 531.152 low:
adj_close: 530.42242 _source: {"message":
["2014-12-30,528.09241,531.1524,527.13239,530.42242,876300,530.42242"],"@version":"1","@timestamp":
/logstash/input
December 29th 2014, 00:00:00.000
message: 2014-12-29,532.19244,535.48242,530.01337,530.3324,2278500,530.3324 @version: 1 @timesta

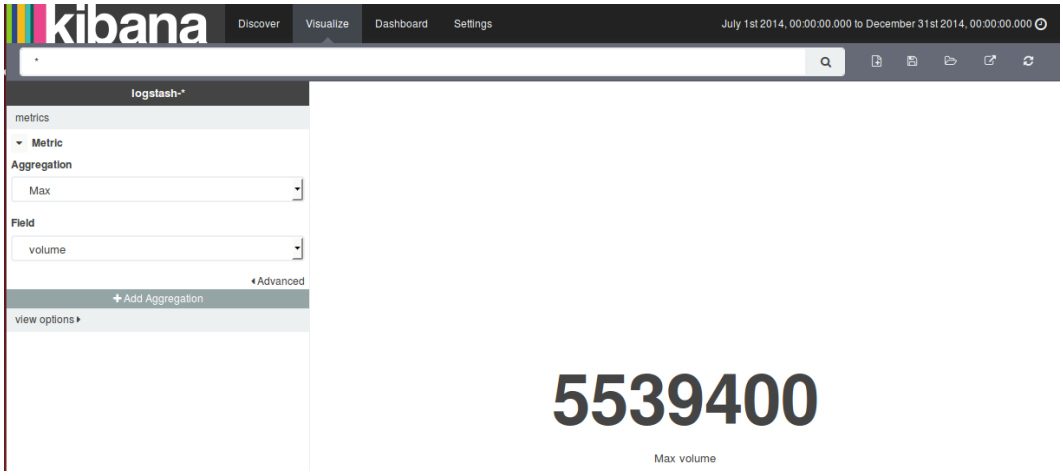

kibana
Discover
Visualize
Dashboard
Settings
July 1st 2014, 00:00:00.000 to December 31st 2014, 00:00:00.000
Time Filter
Refresh Interval
Quick
Relative
Absolute
From:
2014-07-01 00:00:00.000
YYYY-MM-DD HH:mm:ss.SSS
To:
Set To Now
2014-12-31 00:00:00.000
YYYY-MM-DD HH:mm:ss.SSS
Go
July 2014
Sun Mon Tue Wed Thu Fri Sat
29 30 01 02 03 04 05
06 07 08 09 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31 01 02
December 2014
Sun Mon Tue Wed Thu Fri Sat
30 01 02 03 04 05 06
07 08 09 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31 01 02 03

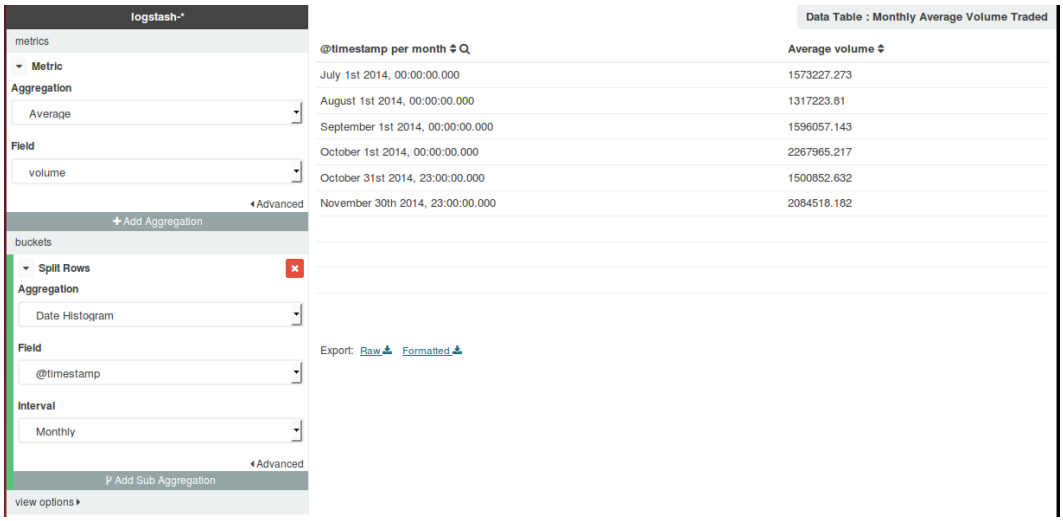

kibana
Discover
Visualize
Dashboard
Settings
Indices
Advanced
Objects
About
Index Patterns
Add New
logstash-*
logstash-*
This page lists every field in the logstash-* index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API
Fields (20)
Scripted Fields (0)
name
type
analyzed
indexed
popularity
volume number false true 0
path.raw string false true 0
path string true true 0
open number false true 0
message string true true 0
low number false true 0
host.raw string false true 0
host string true true 0

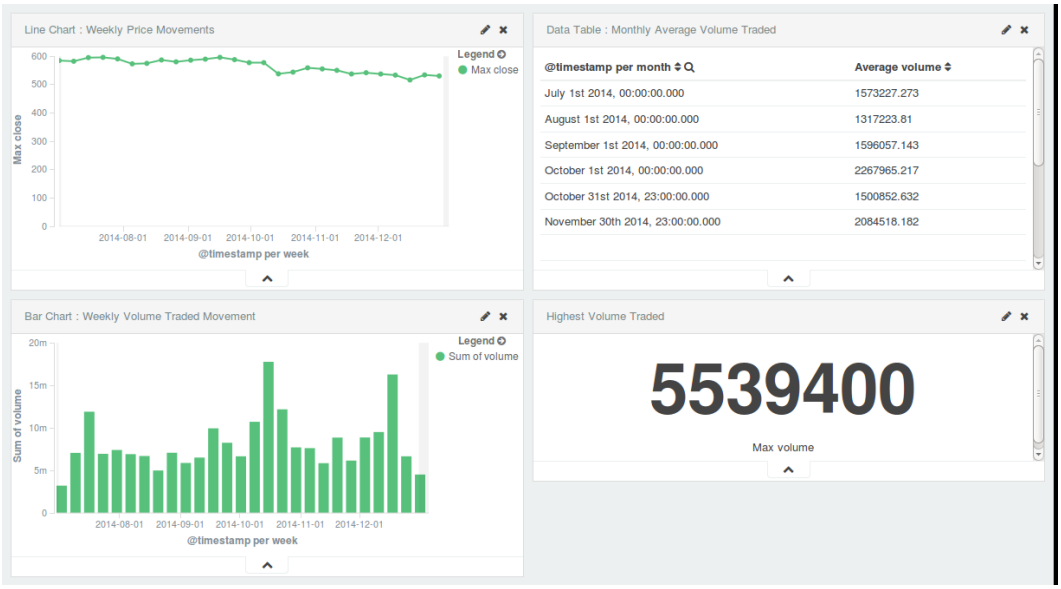

kibana
Discover
Visualize
Dashboard
Settings
Create a new visualization
Step 1
Area chart
Great for stacked timelines in which the total of all series is more important than comparing any two or more series. Less useful for assessing the relative change of unrelated data points as changes in a series 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.

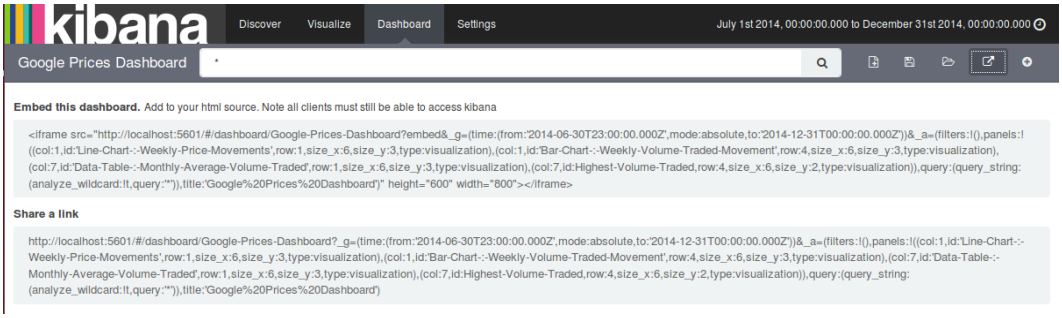

metrics
Y-Axis
Aggregation
Max
Field
close
Advanced
Add Aggregation
buckets
X-Axis
Aggregation
Date Histogram
Field
@timestamp
Interval
Weekly
Advanced
Add Sub Aggregation
view options
600
500
400
300
200
100
Max close
Legend
Max close


Y-Axis
Aggregation
Sum
Field
volume
Advanced
Add Aggregation
buckets
X-Axis
Aggregation
Date Histogram
Field
@timestamp
Interval
Weekly
Advanced
Add Sub Aggregation
view options
16m
14m
12m
10m
8m
6m
4m
2m
0
Sum of volume
2014-08-01
2014-09-01
2014-10-01
2014-11-01
2014-12-01

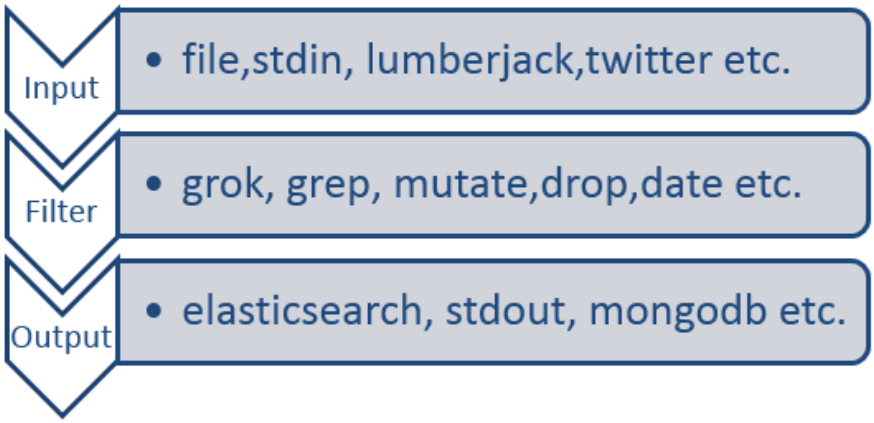

kibana
Discover
Visualize
Dashboard
Settings
July 1st 2014, 00:00:00.000 to December 31st 2014, 00:00:00.000
*
logstash-*
metrics
Metric
Aggregation
Max
Field
volume
Advanced
+ Add Aggregation
view options
5539400
Max volume


logstash-*
metrics
Metric
Aggregation
Average
Field
volume
Advanced
+ Add Aggregation
buckets
Split Rows
Aggregation
Date Histogram
Field
@timestamp
Interval
Monthly
Advanced
Add Sub Aggregation
view options
Data Table : Monthly Average Volume Traded
@timestamp per month
Average volume
July 1st 2014, 00:00:00.000 1573227.273
August 1st 2014, 00:00:00.000 1317223.81
September 1st 2014, 00:00:00.000 1596057.143
October 1st 2014, 00:00:00.000 2267965.217
October 31st 2014, 23:00:00.000 1500852.632
November 30th 2014, 23:00:00.000 2084518.182
Export: Raw Formatted


Line Chart : Weekly Price Movements
Legend
Max close
Max close
600
500
400
300
200
100
0
2014-08-01
2014-09-01
2014-10-01
2014-11-01
2014-12-01
@timestamp per week
Data Table : Monthly Average Volume Traded
@timestamp per month
Average volume
July 1st 2014, 00:00:00.000
1573227.273
August 1st 2014, 00:00:00.000
1317223.81
September 1st 2014, 00:00:00.000
1596057.143
October 1st 2014, 00:00:00.000
2267965.217
October 31st 2014, 23:00:00.000
1500852.632
November 30th 2014, 23:00:00.000
2084518.182
Bar Chart : Weekly Volume Traded Movement
Legend
Sum of volume
Sum of volume
20m
15m
10m
5m
0
2014-08-01
2014-09-01
2014-10-01
2014-11-01
2014-12-01
@timestamp per week
Highest Volume Traded
5539400
Max volume

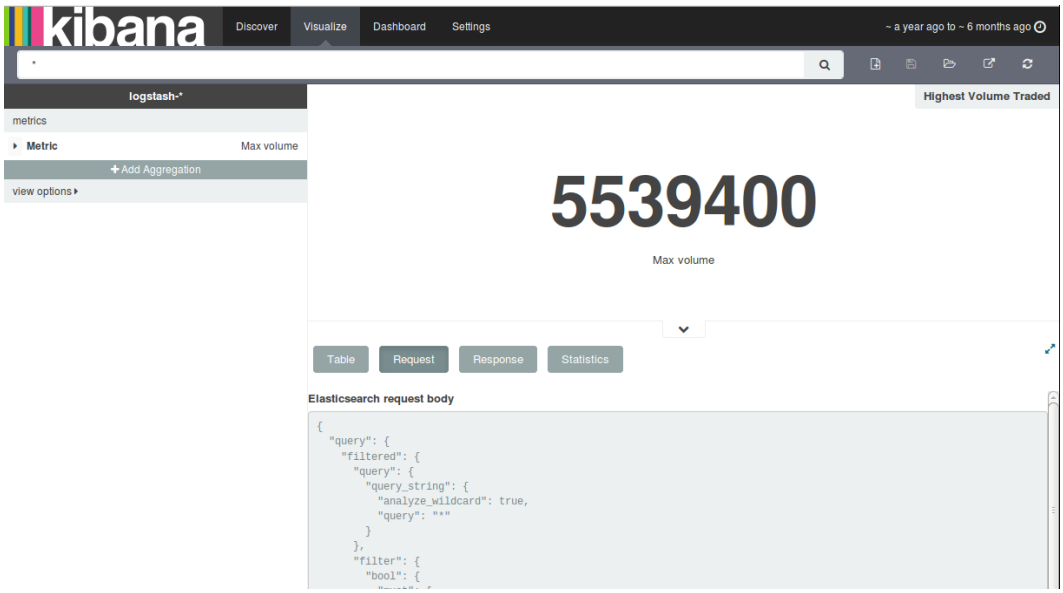

kibana
Discover
Visualize
Dashboard
Settings
July 1st 2014, 00:00:00.000 to December 31st 2014, 00:00:00.000
Google Prices Dashboard
*
Embed this dashboard. Add to your html source. Note all clients must still be able to access kibana
<iframe src="http://localhost:5601/#/dashboard/Google-Prices-Dashboard?embed&_g=(time:(from:'2014-06-30T23:00:00.000Z',mode:absolute,to:'2014-12-31T00:00:00.000Z'))&_a=(filters:!(),panels:!((col:1,id:'Line-Chart-:-Weekly-Price-Movements',row:1,size_x:6,size_y:3,type:visualization),(col:1,id:'Bar-Chart-:-Weekly-Volume-Traded-Movement',row:4,size_x:6,size_y:3,type:visualization),(col:7,id:'Data-Table-:-Monthly-Average-Volume-Traded',row:1,size_x:6,size_y:3,type:visualization),(col:7,id:Highest-Volume-Traded,row:4,size_x:6,size_y:2,type:visualization)),query:(query_string:(analyze_wildcard:!t,query:'*')),title:'Google%20Prices%20Dashboard')" height="600" width="800"></iframe>
Share a link
http://localhost:5601/#/dashboard/Google-Prices-Dashboard?_g=(time:(from:'2014-06-30T23:00:00.000Z',mode:absolute,to:'2014-12-31T00:00:00.000Z'))&_a=(filters:!(),panels:!((col:1,id:'Line-Chart-:-Weekly-Price-Movements',row:1,size_x:6,size_y:3,type:visualization),(col:1,id:'Bar-Chart-:-Weekly-Volume-Traded-Movement',row:4,size_x:6,size_y:3,type:visualization),(col:7,id:'Data-Table-:-Monthly-Average-Volume-Traded',row:1,size_x:6,size_y:3,type:visualization),(col:7,id:Highest-Volume-Traded,row:4,size_x:6,size_y:2,type:visualization)),query:(query_string:(analyze_wildcard:!t,query:'*')),title:'Google%20Prices%20Dashboard')

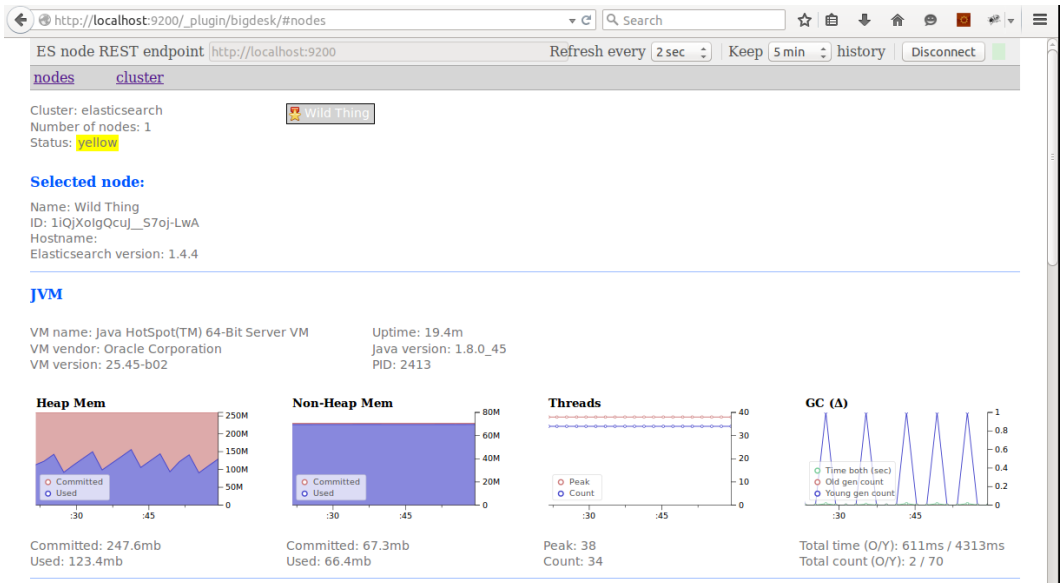
Chapter 3

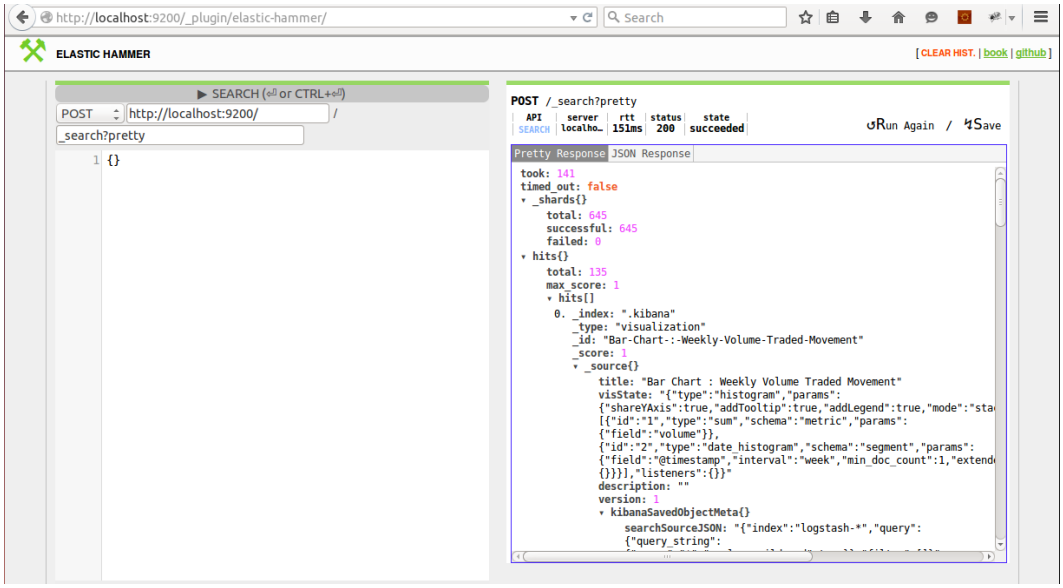


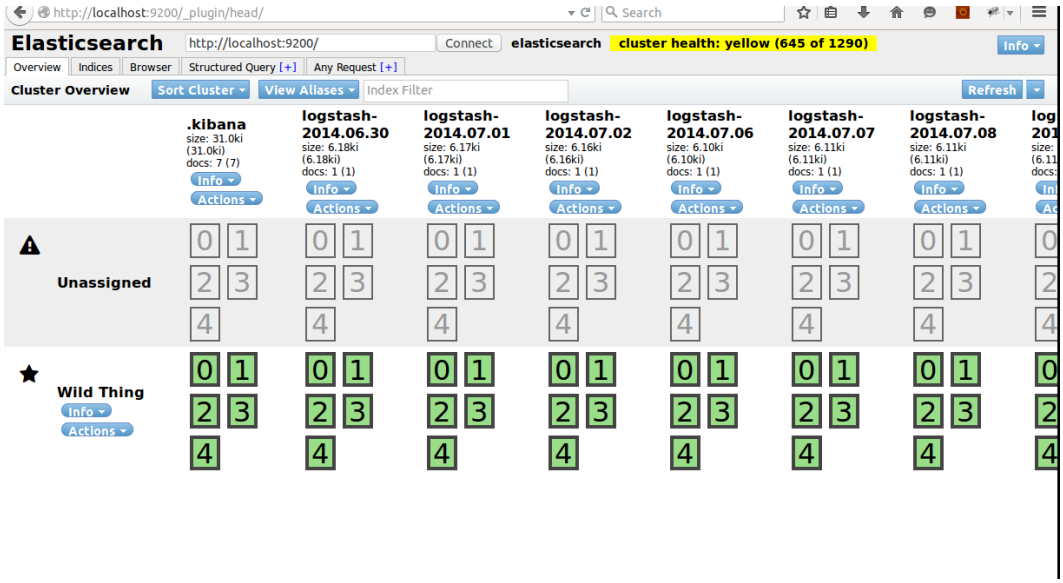
Chapter 4

Chapter 5

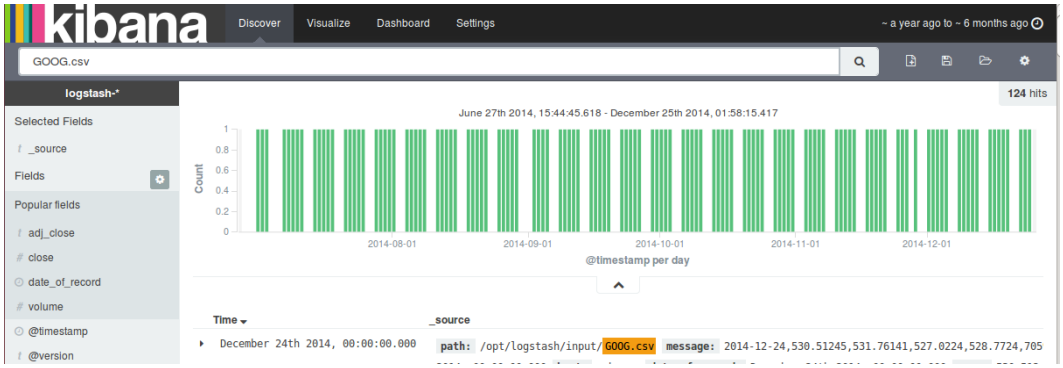

kibana
Discover
Visualize
Dashboard
Settings
~ a year ago to ~ 6 months ago
logstash-*
metrics
Metric
Max volume
Add Aggregation
view options
Highest Volume Traded
5539400
Max volume
Table
Request
Response
Statistics
Elasticsearch request body
{
"query": {
"filtered": {
"query": {
"query_string": {
"analyze_wildcard": true,
"query": "*"
}
},
"filter": {
"bool": {

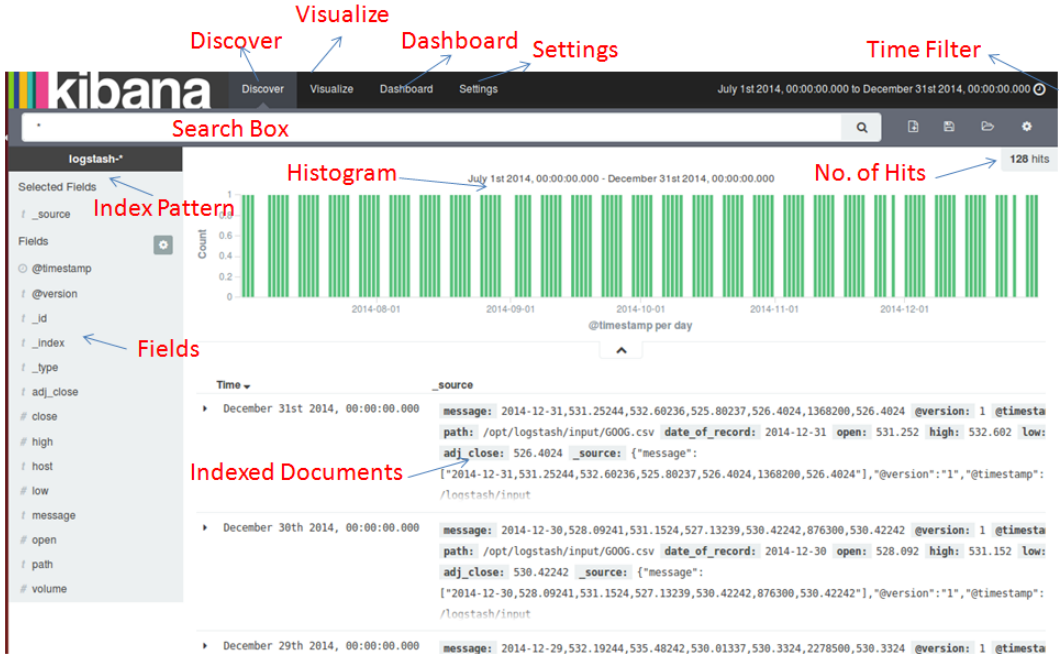

http://localhost:9200/_plugin/bigdesk/#nodes
Search
ES node REST endpoint
http://localhost:9200
Refresh every
2 sec
Keep
5 min
history
Disconnect
nodes
cluster
Cluster: elasticsearch
Number of nodes: 1
Status: yellow
Wild Thing
Selected node:
Name: Wild Thing
ID: 1iQjXoIgQcuJ__S7oj-LwA
Hostname:
Elasticsearch version: 1.4.4
JVM
VM name: Java HotSpot(TM) 64-Bit Server VM
VM vendor: Oracle Corporation
VM version: 25.45-b02
Uptime: 19.4m
Java version: 1.8.0_45
PID: 2413
Heap Mem
Committed
Used
Committed: 247.6mb
Used: 123.4mb
Non-Heap Mem
Committed
Used
Committed: 67.3mb
Used: 66.4mb
Threads
Peak
Count
Peak: 38
Count: 34
GC (Δ)
Time both (sec)
Old gen count
Young gen count
Total time (O/Y): 611ms / 4313ms
Total count (O/Y): 2 / 70

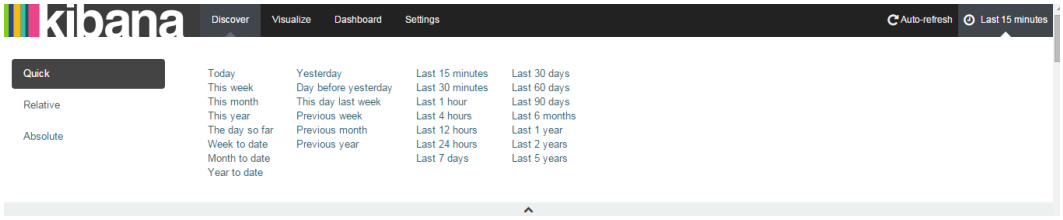

http://localhost:9200/_plugin/elastic-hammer/
Search
ELASTIC HAMMER
[CLEAR HIST. | book | github]
▶ SEARCH (⏎ or CTRL+⏎)
POST
http://localhost:9200/
/
_search?pretty
1 {}
POST /_search?pretty
API SEARCH
server localho…
rtt 151ms
status 200
state succeeded
↺Run Again / ↯Save
Pretty Response
JSON Response
took: 141
timed_out: false
▾ _shards{}
total: 645
successful: 645
failed: 0
▾ hits{}
total: 135
max_score: 1
▾ hits[]
0. _index: ".kibana"
_type: "visualization"
_id: "Bar-Chart-:-Weekly-Volume-Traded-Movement"
_score: 1
▾ _source{}
title: "Bar Chart : Weekly Volume Traded Movement"
description: ""
version: 1
▾ kibanaSavedObjectMeta{}

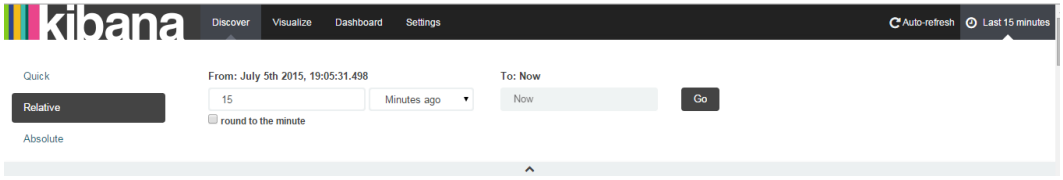

http://localhost:9200/_plugin/head/
Search
Elasticsearch
http://localhost:9200/
Connect
elasticsearch
cluster health: yellow (645 of 1290)
Info
Overview
Indices
Browser
Structured Query [+]
Any Request [+]
Cluster Overview
Sort Cluster
View Aliases
Index Filter
Refresh
.kibana
size: 31.0ki (31.0ki)
docs: 7 (7)
logstash-2014.06.30
size: 6.18ki (6.18ki)
docs: 1 (1)
logstash-2014.07.01
size: 6.17ki (6.17ki)
docs: 1 (1)
logstash-2014.07.02
size: 6.16ki (6.16ki)
docs: 1 (1)
logstash-2014.07.06
size: 6.10ki (6.10ki)
docs: 1 (1)
logstash-2014.07.07
size: 6.11ki (6.11ki)
docs: 1 (1)
logstash-2014.07.08
size: 6.11ki (6.11ki)
docs: 1 (1)
Info
Actions
Unassigned
Wild Thing
Info
Actions

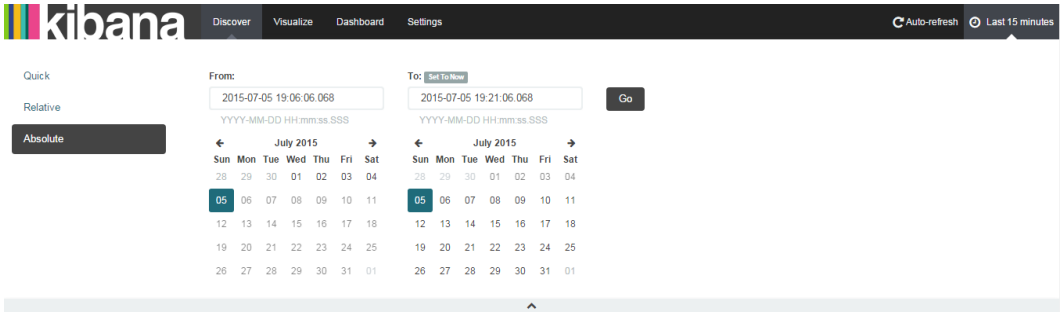
Chapter 6

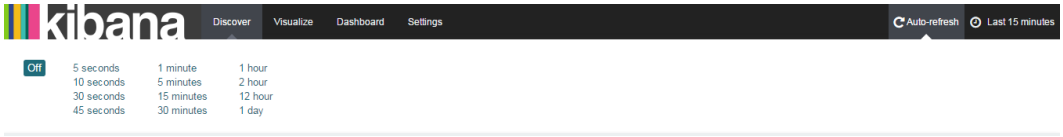

kibana
Discover
Visualize
Dashboard
Settings
~ a year ago to ~ 6 months ago
GOOG.csv
logstash-*
124 hits
Selected Fields
_source
Fields
Popular fields
adj_close
close
date_of_record
volume
@timestamp
@version
June 27th 2014, 15:44:45.618 - December 25th 2014, 01:58:15.417
Count
2014-08-01
2014-09-01
2014-10-01
2014-11-01
2014-12-01
@timestamp per day
Time
_source
December 24th 2014, 00:00:00.000
path: /opt/logstash/input/GOOG.csv message: 2014-12-24,530.51245,531.76141,527.0224,528.7724,705

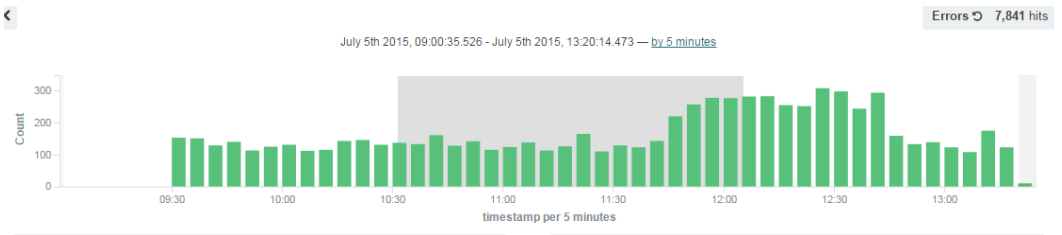

Visualize
Discover
Dashboard
Settings
Time Filter
kibana
Discover
Visualize
Dashboard
Settings
July 1st 2014, 00:00:00.000 to December 31st 2014, 00:00:00.000
Search Box
logstash-*
Histogram
July 1st 2014, 00:00:00.000 - December 31st 2014, 00:00:00.000
No. of Hits
128 hits
Selected Fields
_source
Index Pattern
Fields
@timestamp
@version
_id
_index
_type
adj_close
close
high
host
low
message
open
path
volume
Count
2014-08-01
2014-09-01
2014-10-01
2014-11-01
2014-12-01
@timestamp per day
Time
_source
December 31st 2014, 00:00:00.000
message: 2014-12-31,531.25244,532.60236,525.80237,526.4024,1368200,526.4024 @version: 1 @timesta
path: /opt/logstash/input/GOOG.csv date_of_record: 2014-12-31 open: 531.252 high: 532.602 low:
adj_close: 526.4024 _source: {"message":
["2014-12-31,531.25244,532.60236,525.80237,526.4024,1368200,526.4024"],"@version":"1","@timestamp":
/logstash/input
Indexed Documents
December 30th 2014, 00:00:00.000
message: 2014-12-30,528.09241,531.1524,527.13239,530.42242,876300,530.42242 @version: 1 @timesta
path: /opt/logstash/input/GOOG.csv date_of_record: 2014-12-30 open: 528.092 high: 531.152 low:
adj_close: 530.42242 _source: {"message":
["2014-12-30,528.09241,531.1524,527.13239,530.42242,876300,530.42242"],"@version":"1","@timestamp":
/logstash/input
December 29th 2014, 00:00:00.000
message: 2014-12-29,532.19244,535.48242,530.01337,530.3324,2278500,530.3324 @version: 1 @timesta


kibana
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

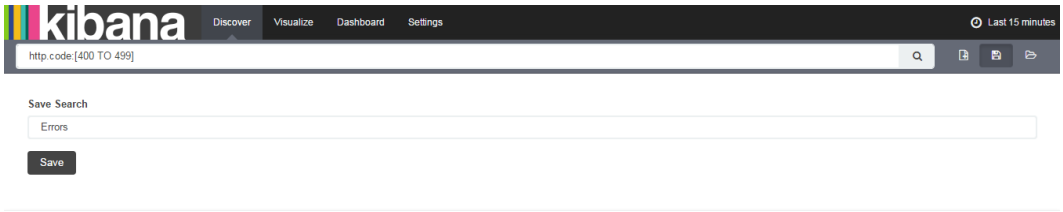

kibana
Discover
Visualize
Dashboard
Settings
Auto-refresh
Last 15 minutes
Quick
Relative
Absolute
From: July 5th 2015, 19:05:31.498
15
Minutes ago
round to the minute
To: Now
Now
Go

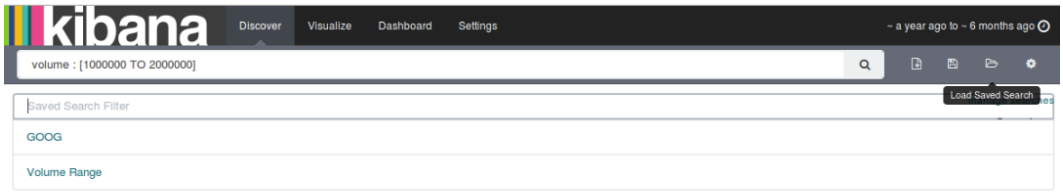

kibana
Discover
Visualize
Dashboard
Settings
Auto-refresh
Last 15 minutes
Quick
Relative
Absolute
From:
2015-07-05 19:06:06.068
YYYY-MM-DD HH:mm:ss.SSS
To:
Set To Now
2015-07-05 19:21:06.068
YYYY-MM-DD HH:mm:ss.SSS
Go
July 2015
Sun Mon Tue Wed Thu Fri Sat

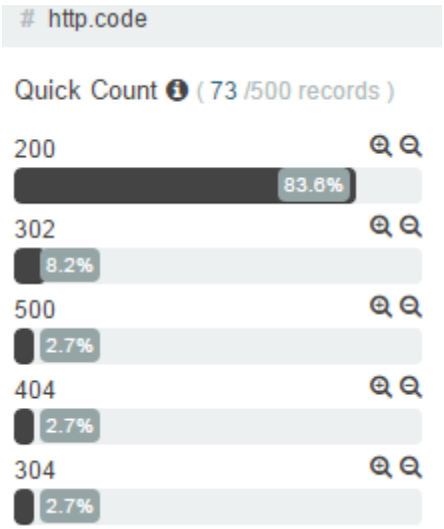

kibana
Discover
Visualize
Dashboard
Settings
Auto-refresh
Last 15 minutes
Off
5 seconds
10 seconds
30 seconds
45 seconds
1 minute
5 minutes
15 minutes
30 minutes
1 hour
2 hour
12 hour
1 day

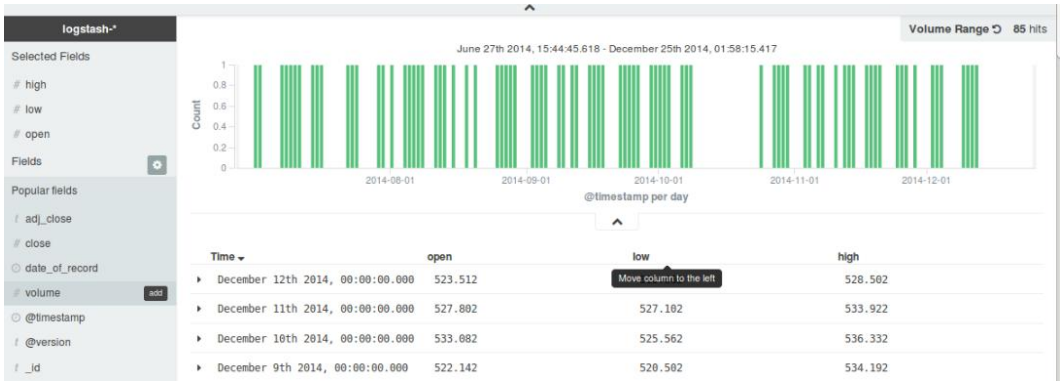

Errors
7,841 hits
July 5th 2015, 09:00:35.526 - July 5th 2015, 13:20:14.473 — by 5 minutes
Count
300
200
100
0
09:30
10:00
10:30
11:00
11:30
12:00
12:30
13:00
timestamp per 5 minutes


kibana
Discover
Visualize
Dashboard
Settings
Last 15 minutes
http.code:[400 TO 499]
New Search
46 hits

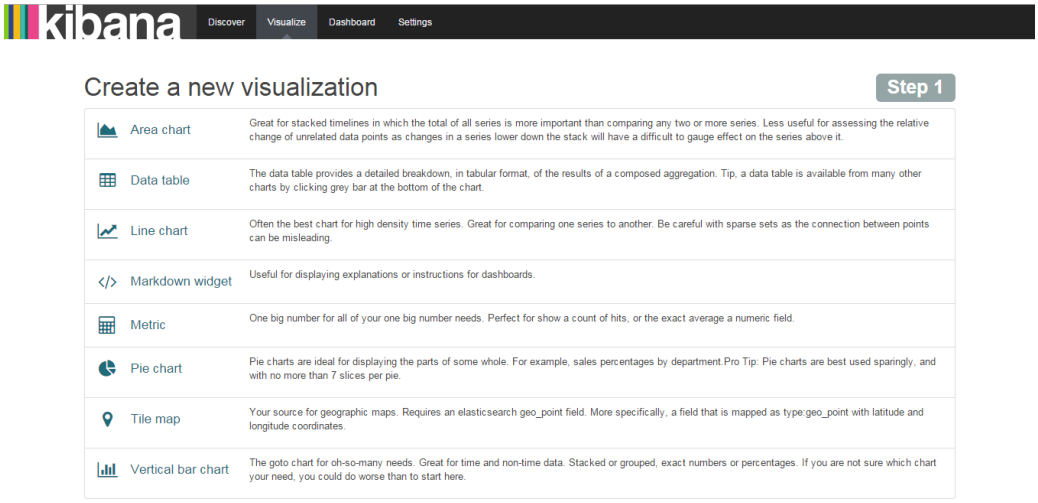

kibana
Discover
Visualize
Dashboard
Settings
Last 15 minutes
http.code:[400 TO 499]
Save Search
Errors
Save

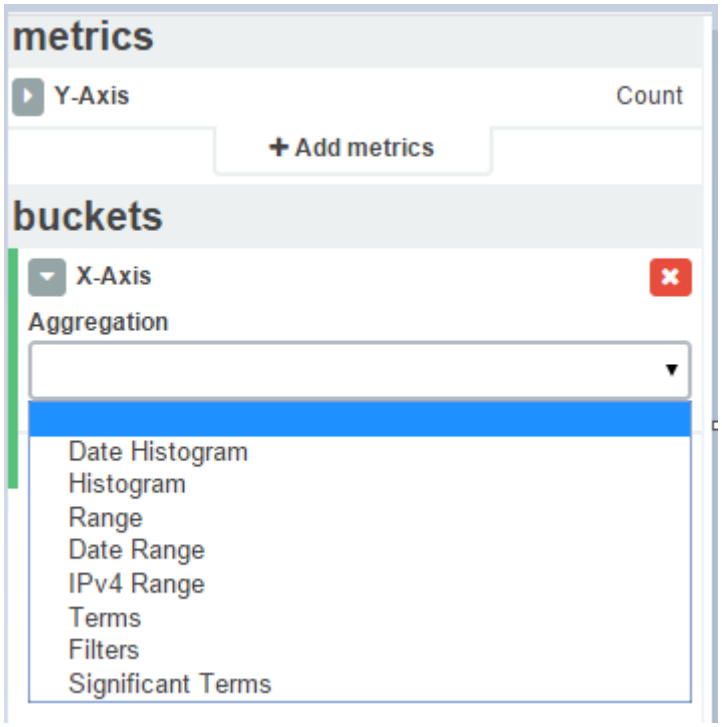

kibana
Discover
Visualize
Dashboard
Settings
~ a year ago to ~ 6 months ago
volume : [1000000 TO 2000000]
Load Saved Search
Saved Search Filter
GOOG
Volume Range

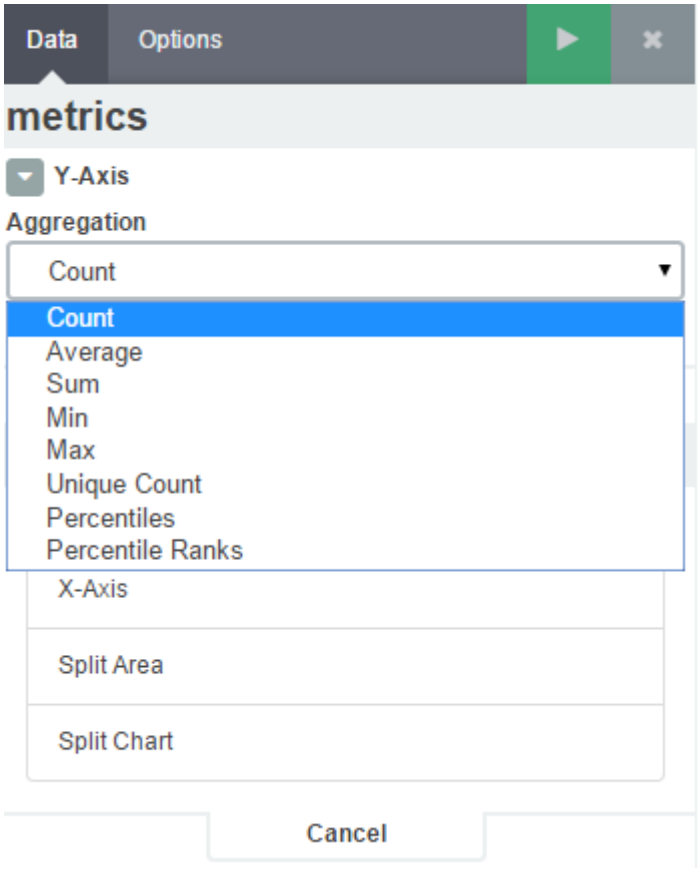

http.code
Quick Count (73 /500 records)
200
83.6%
302
8.2%
500
2.7%
404
2.7%
304
2.7%


logstash-*
Selected Fields
high
low
open
Fields
Popular fields
adj_close
close
date_of_record
volume
add
@timestamp
@version
_id
Volume Range
85 hits
June 27th 2014, 15:44:45.618 - December 25th 2014, 01:58:15.417
Count
2014-08-01
2014-09-01
2014-10-01
2014-11-01
2014-12-01
@timestamp per day
Time
open
low
high
Move column to the left
December 12th 2014, 00:00:00.000 523.512 528.502
December 11th 2014, 00:00:00.000 527.802 527.102 533.922
December 10th 2014, 00:00:00.000 533.082 525.562 536.332
December 9th 2014, 00:00:00.000 522.142 520.502 534.192

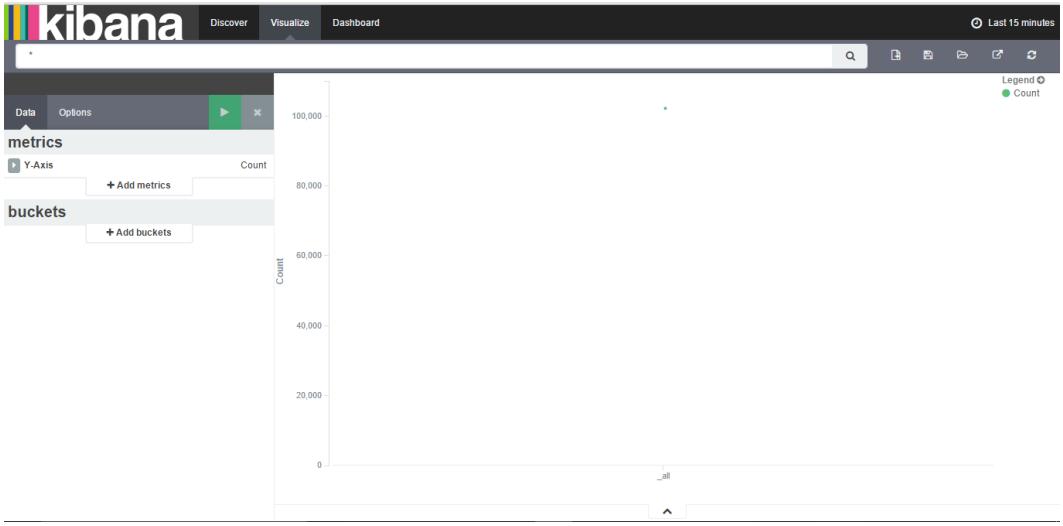
Chapter 7


kibana
Discover
Visualize
Dashboard
Settings
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.

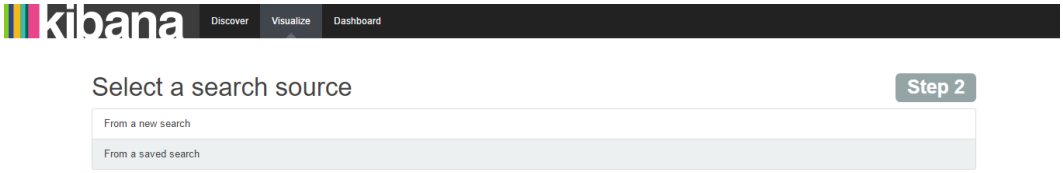

metrics
Y-Axis
Count
+ Add metrics
buckets
X-Axis
Aggregation
Date Histogram
Histogram
Range
Date Range
IPv4 Range
Terms
Filters
Significant Terms

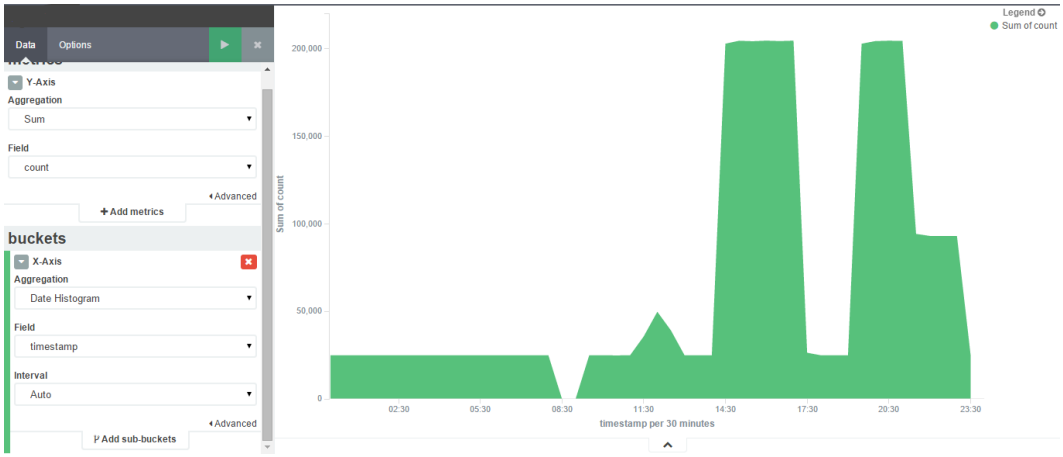

Data
Options
metrics
Y-Axis
Aggregation
Count
Count
Average
Sum
Min
Max
Unique Count
Percentiles
Percentile Ranks
X-Axis
Split Area
Split Chart
Cancel

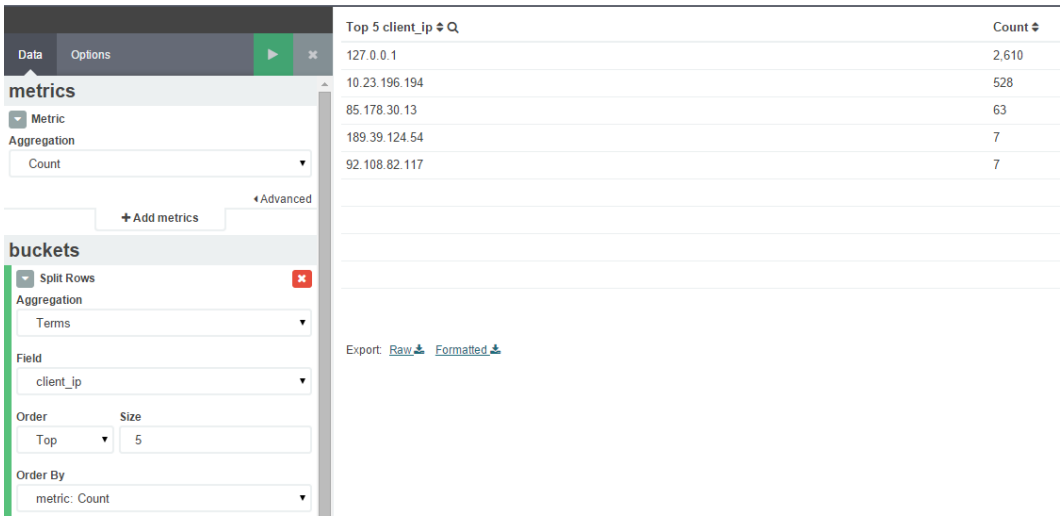

Advanced
JSON Input
Any JSON formatted properties you add here will be merged with the elasticsearch aggregation definition for this section. For example *shard_size* on a *terms* aggregation


kibana
Discover
Visualize
Dashboard
Last 15 minutes
Data
Options
metrics
Y-Axis
Count
+ Add metrics
buckets
+ Add buckets
Legend
Count
100,000
80,000
60,000
40,000
20,000
0
Count
_all

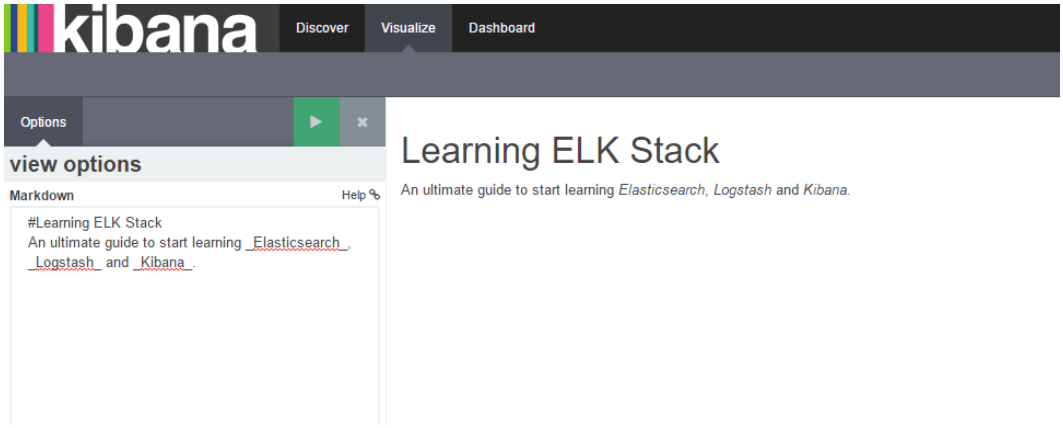

kibana
Discover
Visualize
Dashboard
Last 15 minutes
New Visualization
Legend
Count

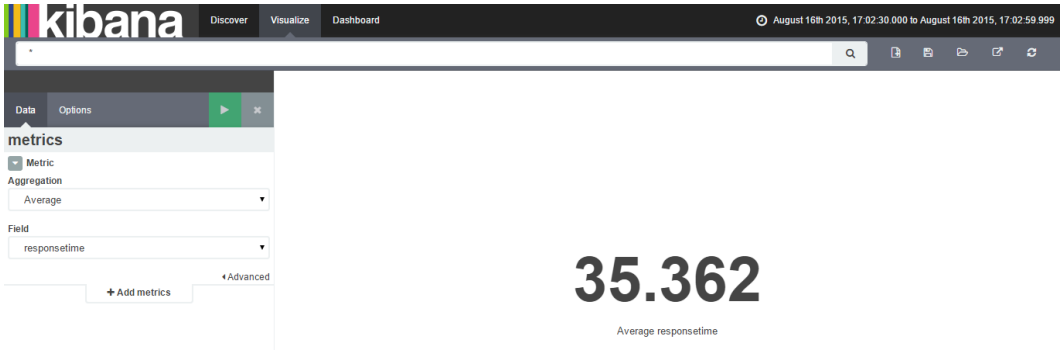

kibana
Discover
Visualize
Dashboard
Select a search source
Step 2
From a new search
From a saved search

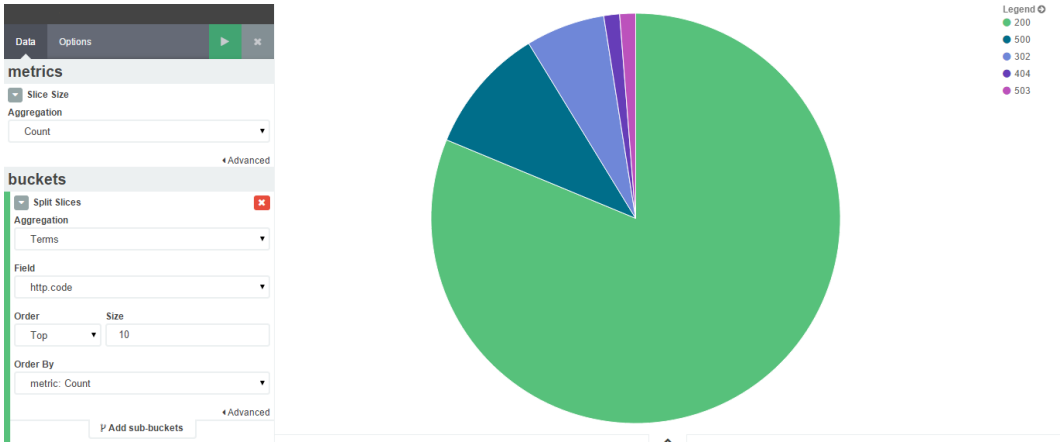

Data
Options
Y-Axis
Aggregation
Sum
Field
count
Advanced
Add metrics
buckets
X-Axis
Aggregation
Date Histogram
Field
timestamp
Interval
Auto
Advanced
Add sub-buckets
Legend
Sum of count
200,000
150,000
100,000
50,000
0
Sum of count
02:30
05:30
08:30
11:30
14:30
17:30
20:30
23:30
timestamp per 30 minutes


Data
Options
metrics
Metric
Aggregation
Count
Advanced
Add metrics
buckets
Split Rows
Aggregation
Terms
Field
client_ip
Order
Top
Size
5
Order By
metric: Count
Top 5 client_ip
Count
127.0.0.1
2,610
10.23.196.194
528
85.178.30.13
63
189.39.124.54
7
92.108.82.117
7
Export: Raw Formatted

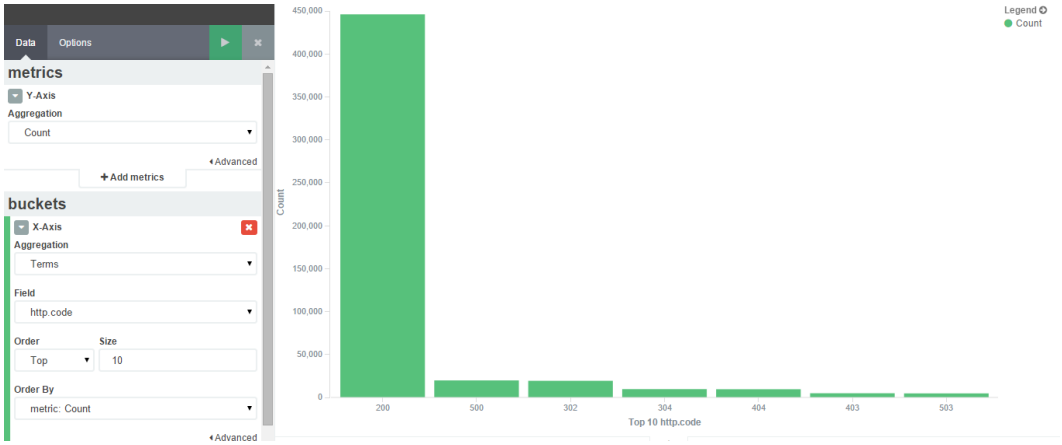

Data
Options
metrics
Y-Axis
Aggregation
Count
Advanced
+ Add metrics
buckets
X-Axis
Aggregation
Date Histogram
Field
timestamp
Interval
Auto
Advanced
Add sub-buckets
Count
Legend
timestamp per second

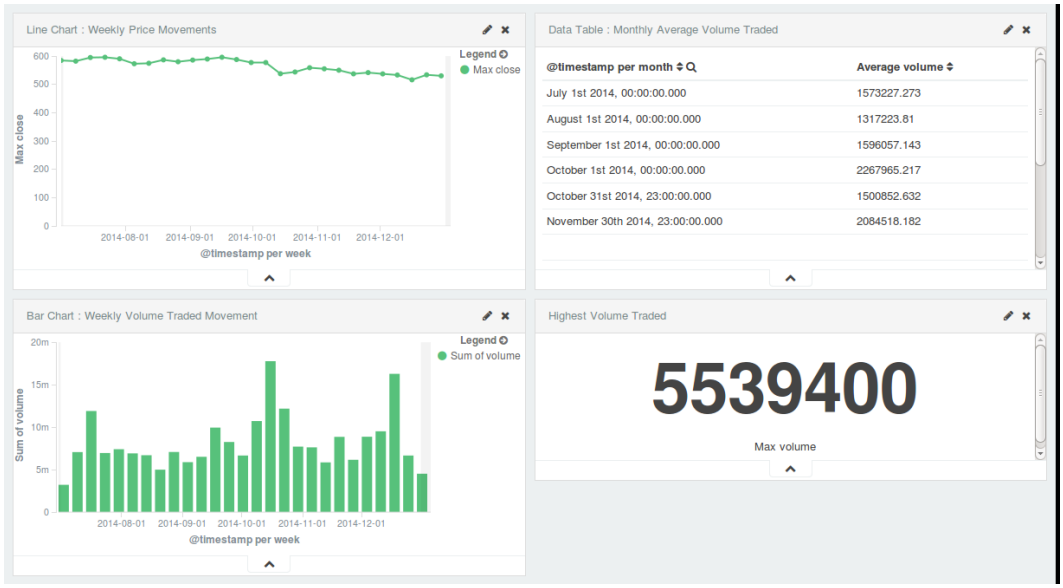

kibana
Discover
Visualize
Dashboard
Options
view options
Markdown
Help
#Learning ELK Stack
An ultimate guide to start learning _Elasticsearch_, _Logstash_ and _Kibana_.
Learning ELK Stack
An ultimate guide to start learning Elasticsearch, Logstash and Kibana.

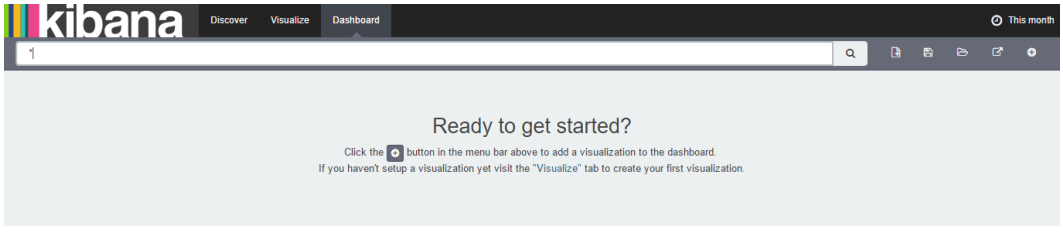

kibana
Discover
Visualize
Dashboard
August 16th 2015, 17:02:30.000 to August 16th 2015, 17:02:59.999
Data
Options
metrics
Metric
Aggregation
Average
Field
responsetime
Advanced
+ Add metrics
35.362
Average responsetime

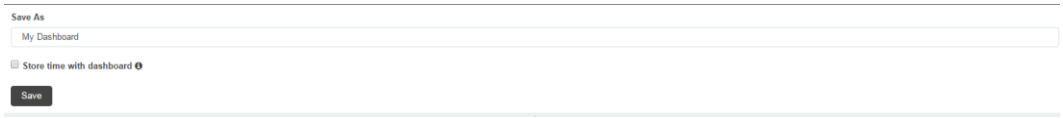

Data
Options
metrics
Slice Size
Aggregation
Count
Advanced
buckets
Split Slices
Aggregation
Terms
Field
http.code
Order
Top
Size
10
Order By
metric: Count
Advanced
Add sub-buckets
Legend
200
500
302
404
503

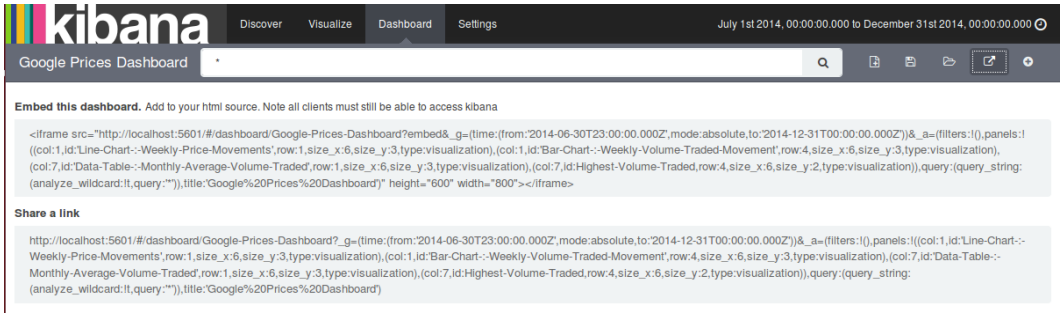

Data
Options
metrics
Value
Count
buckets
Geo Coordinates
Aggregation
Geohash
Field
client_location
Change precision on map zoom
Advanced
Add sub-buckets
NORTH AMERICA
EUROPE
ASIA
Siberia
AFRICA
Sahara
Arabian Peninsula
Gobi
Indonesia
SOUTH AMERICA
AUSTRALIA
Amazon Basin
Congo Basin
North Atlantic Ocean
South Atlantic Ocean
North Pacific Ocean
South Pacific Ocean
Indian Ocean
EQUATOR
10,455 – 16,982.8
16,982.8 – 23,510.6
23,510.6 – 30,038.4
30,038.4 – 36,566.2
36,566.2 – 43,094


Data
Options
metrics
Y-Axis
Aggregation
Count
Advanced
+ Add metrics
buckets
X-Axis
Aggregation
Terms
Field
http.code
Order
Top
Size
10
Order By
metric: Count
Advanced
Count
Legend
Count
200
500
302
304
404
403
503
Top 10 http.code

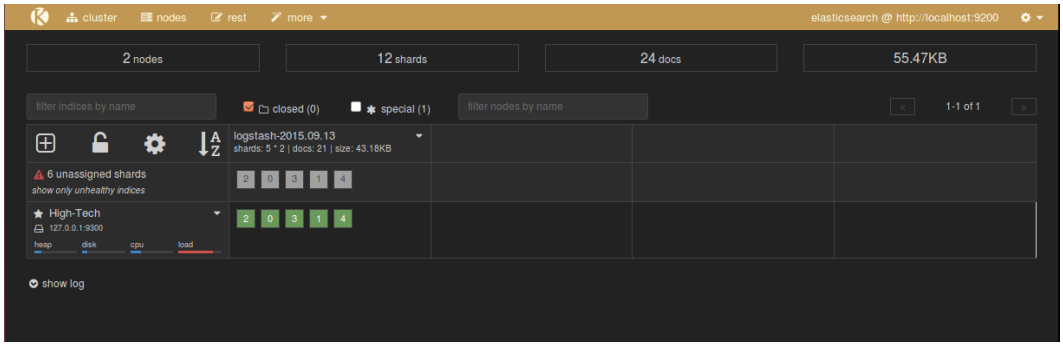

Line Chart : Weekly Price Movements
Legend
Max close
Max close
@timestamp per week
Data Table : Monthly Average Volume Traded
@timestamp per month
Average volume
July 1st 2014, 00:00:00.000
1573227.273
August 1st 2014, 00:00:00.000
1317223.81
September 1st 2014, 00:00:00.000
1596057.143
October 1st 2014, 00:00:00.000
2267965.217
October 31st 2014, 23:00:00.000
1500852.632
November 30th 2014, 23:00:00.000
2084518.182
Bar Chart : Weekly Volume Traded Movement
Legend
Sum of volume
Sum of volume
@timestamp per week
Highest Volume Traded
5539400
Max volume

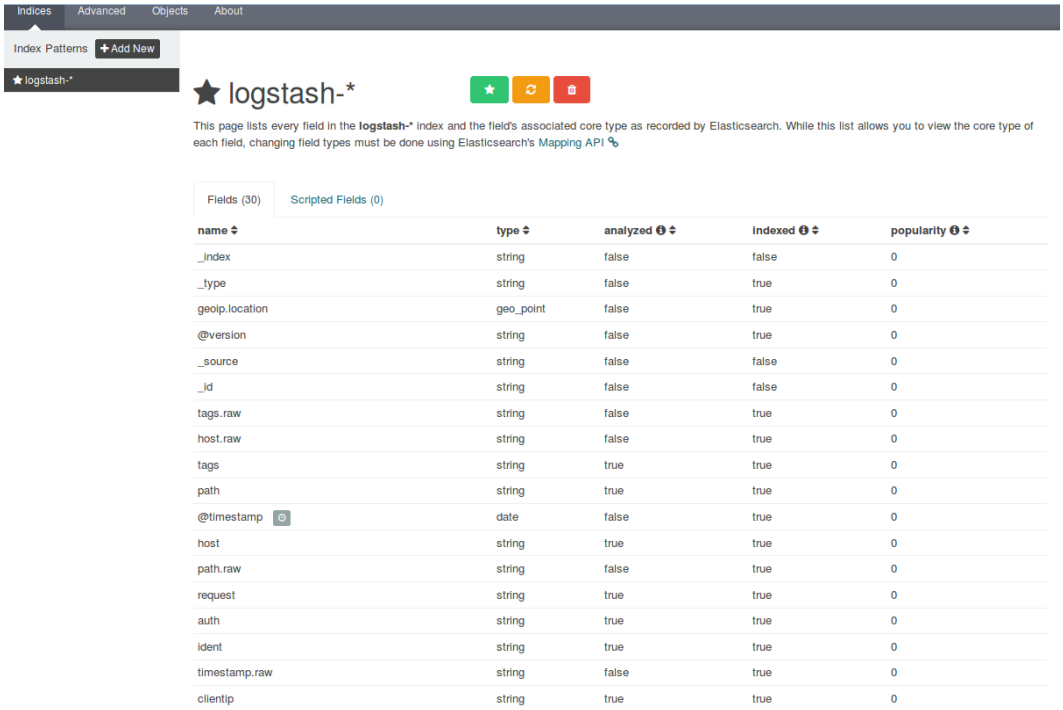

kibana
Discover
Visualize
Dashboard
This month
Ready to get started?
Click the button in the menu bar above to add a visualization to the dashboard.
If you haven't setup a visualization yet visit the "Visualize" tab to create your first visualization.

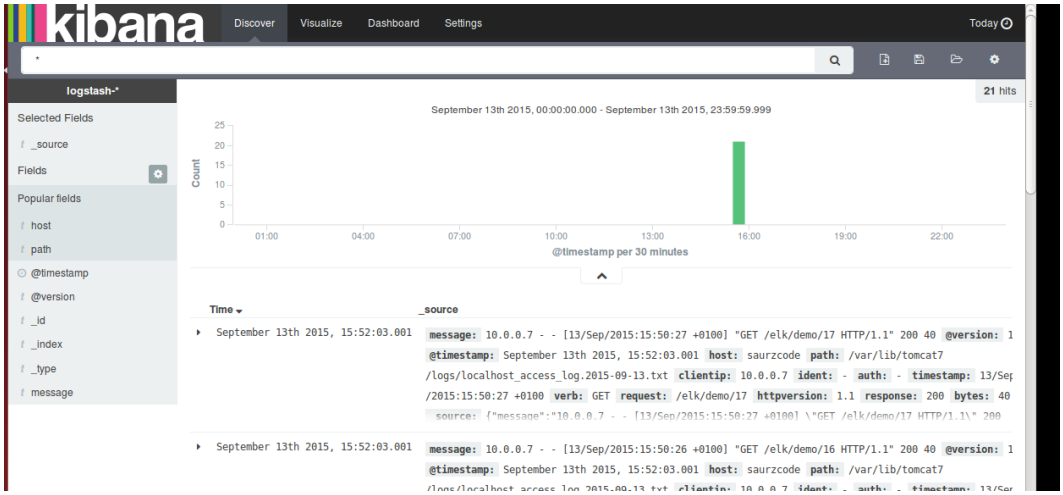

Save As
My Dashboard
Store time with dashboard
Save

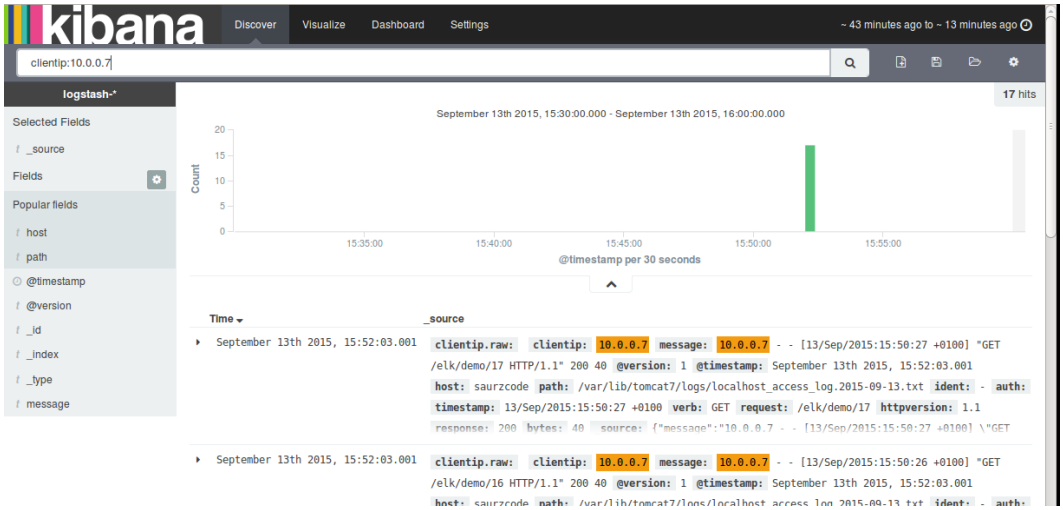

kibana
Discover
Visualize
Dashboard
Settings
July 1st 2014, 00:00:00.000 to December 31st 2014, 00:00:00.000
Google Prices Dashboard
*
Embed this dashboard. Add to your html source. Note all clients must still be able to access kibana
<iframe src="http://localhost:5601/#/dashboard/Google-Prices-Dashboard?embed&_g=(time:(from:'2014-06-30T23:00:00.000Z',mode:absolute,to:'2014-12-31T00:00:00.000Z'))&_a=(filters:!(),panels:!((col:1,id:'Line-Chart-:-Weekly-Price-Movements',row:1,size_x:6,size_y:3,type:visualization),(col:1,id:'Bar-Chart-:-Weekly-Volume-Traded-Movement',row:4,size_x:6,size_y:3,type:visualization),(col:7,id:'Data-Table-:-Monthly-Average-Volume-Traded',row:1,size_x:6,size_y:3,type:visualization),(col:7,id:Highest-Volume-Traded,row:4,size_x:6,size_y:2,type:visualization)),query:(query_string:(analyze_wildcard:!t,query:'*')),title:'Google%20Prices%20Dashboard')" height="600" width="800"></iframe>
Share a link
http://localhost:5601/#/dashboard/Google-Prices-Dashboard?_g=(time:(from:'2014-06-30T23:00:00.000Z',mode:absolute,to:'2014-12-31T00:00:00.000Z'))&_a=(filters:!(),panels:!((col:1,id:'Line-Chart-:-Weekly-Price-Movements',row:1,size_x:6,size_y:3,type:visualization),(col:1,id:'Bar-Chart-:-Weekly-Volume-Traded-Movement',row:4,size_x:6,size_y:3,type:visualization),(col:7,id:'Data-Table-:-Monthly-Average-Volume-Traded',row:1,size_x:6,size_y:3,type:visualization),(col:7,id:Highest-Volume-Traded,row:4,size_x:6,size_y:2,type:visualization)),query:(query_string:(analyze_wildcard:!t,query:'*')),title:'Google%20Prices%20Dashboard')

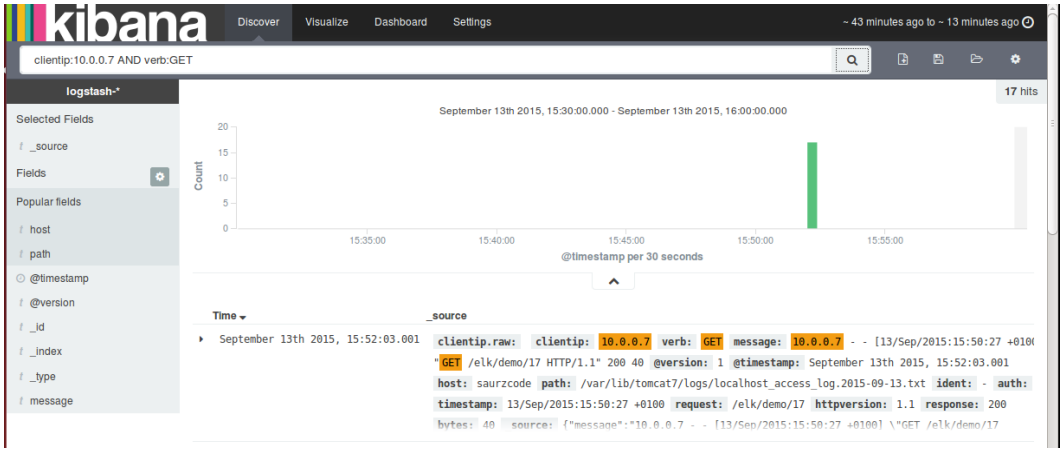
Chapter 8

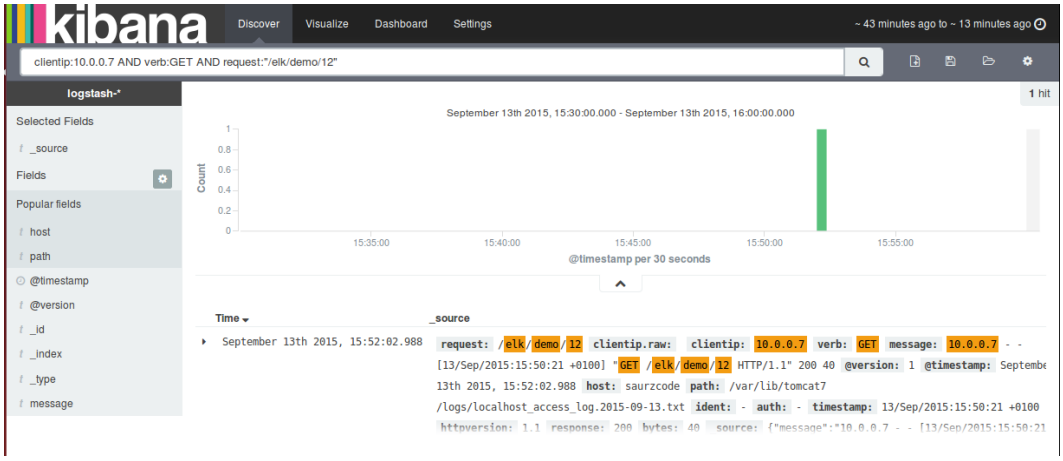

cluster
nodes
rest
more
elasticsearch @ http://localhost:9200
2 nodes
12 shards
24 docs
55.47KB
filter indices by name
closed (0)
special (1)
filter nodes by name
1-1 of 1
logstash-2015.09.13
shards: 5 * 2 | docs: 21 | size: 43.18KB
6 unassigned shards
show only unhealthy indices
High-Tech
127.0.0.1:9300
heap
disk
cpu
load
show log


Indices
Advanced
Objects
About
Index Patterns
Add New
logstash-*
logstash-*
This page lists every field in the logstash-* index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API
Fields (30)
Scripted Fields (0)
name
type
analyzed
indexed
popularity
_index string false false 0
_type string false true 0
geoip.location geo_point false true 0
@version string false true 0
_source string false false 0
_id string false false 0
tags.raw string false true 0
host.raw string false true 0
tags string true true 0
path string true true 0
@timestamp date false true 0
host string true true 0
path.raw string false true 0
request string true true 0
auth string true true 0
ident string true true 0
timestamp.raw string false true 0
clientip string true true 0

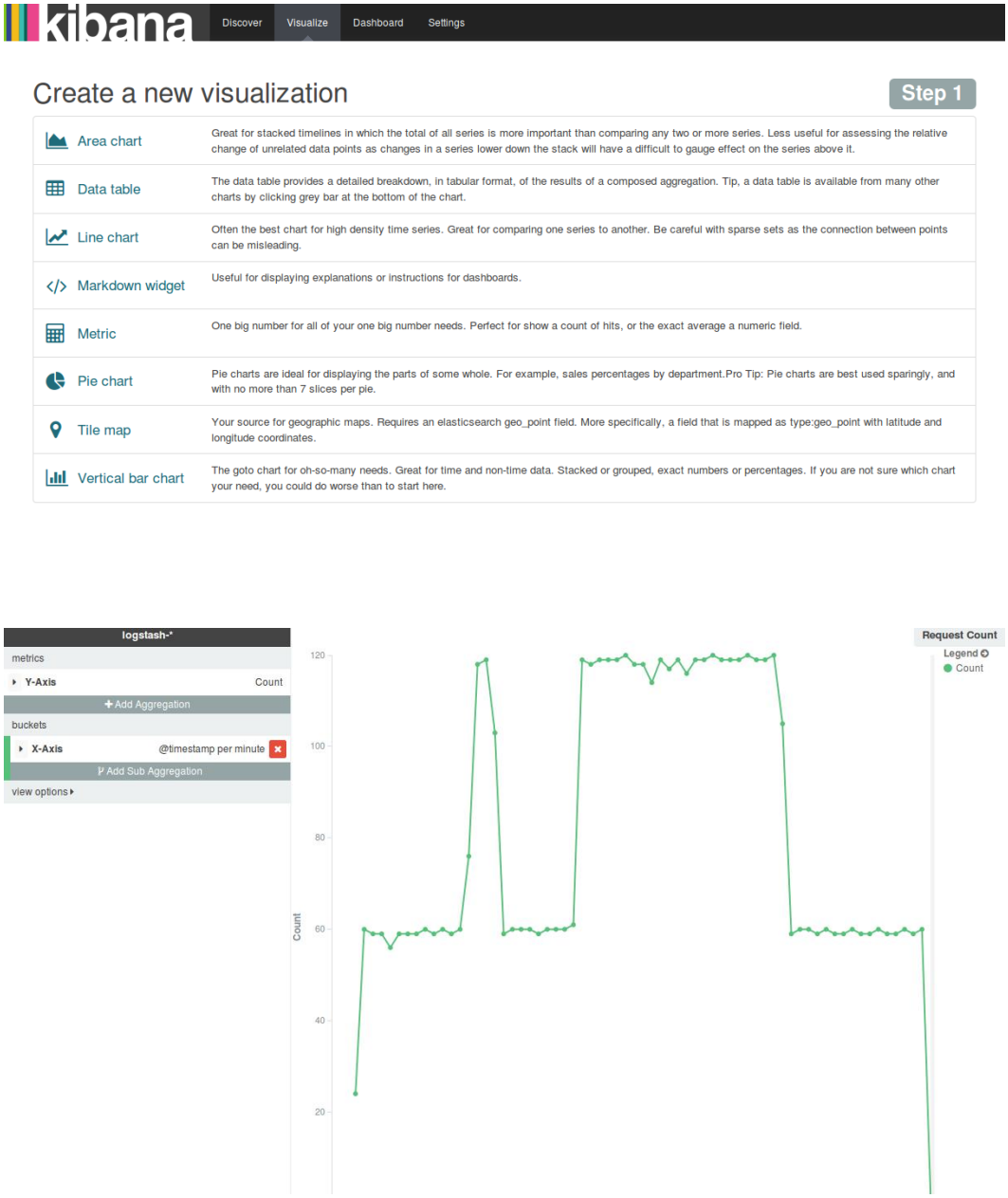

kibana
Discover
Visualize
Dashboard
Settings
Today
logstash-*
Selected Fields
_source
Fields
Popular fields
host
path
@timestamp
@version
_id
_index
_type
message
21 hits
September 13th 2015, 00:00:00.000 - September 13th 2015, 23:59:59.999
Count
@timestamp per 30 minutes
Time
_source
September 13th 2015, 15:52:03.001
message: 10.0.0.7 - - [13/Sep/2015:15:50:27 +0100] "GET /elk/demo/17 HTTP/1.1" 200 40 @version: 1 @timestamp: September 13th 2015, 15:52:03.001 host: saurzcode path: /var/lib/tomcat7 /logs/localhost_access_log.2015-09-13.txt clientip: 10.0.0.7 ident: - auth: - timestamp: 13/Sep /2015:15:50:27 +0100 verb: GET request: /elk/demo/17 httpversion: 1.1 response: 200 bytes: 40
September 13th 2015, 15:52:03.001
message: 10.0.0.7 - - [13/Sep/2015:15:50:26 +0100] "GET /elk/demo/16 HTTP/1.1" 200 40 @version: 1 @timestamp: September 13th 2015, 15:52:03.001 host: saurzcode path: /var/lib/tomcat7


kibana
Discover
Visualize
Dashboard
Settings
~ 43 minutes ago to ~ 13 minutes ago
clientip:10.0.0.7
logstash-*
Selected Fields
_source
Fields
Popular fields
host
path
@timestamp
@version
_id
_index
_type
message
17 hits
September 13th 2015, 15:30:00.000 - September 13th 2015, 16:00:00.000
Count
@timestamp per 30 seconds
Time
_source
September 13th 2015, 15:52:03.001
clientip.raw: clientip: 10.0.0.7 message: 10.0.0.7 - - [13/Sep/2015:15:50:27 +0100] "GET /elk/demo/17 HTTP/1.1" 200 40 @version: 1 @timestamp: September 13th 2015, 15:52:03.001 host: saurzcode path: /var/lib/tomcat7/logs/localhost_access_log.2015-09-13.txt ident: - auth: timestamp: 13/Sep/2015:15:50:27 +0100 verb: GET request: /elk/demo/17 httpversion: 1.1
September 13th 2015, 15:52:03.001
clientip.raw: clientip: 10.0.0.7 message: 10.0.0.7 - - [13/Sep/2015:15:50:26 +0100] "GET /elk/demo/16 HTTP/1.1" 200 40 @version: 1 @timestamp: September 13th 2015, 15:52:03.001

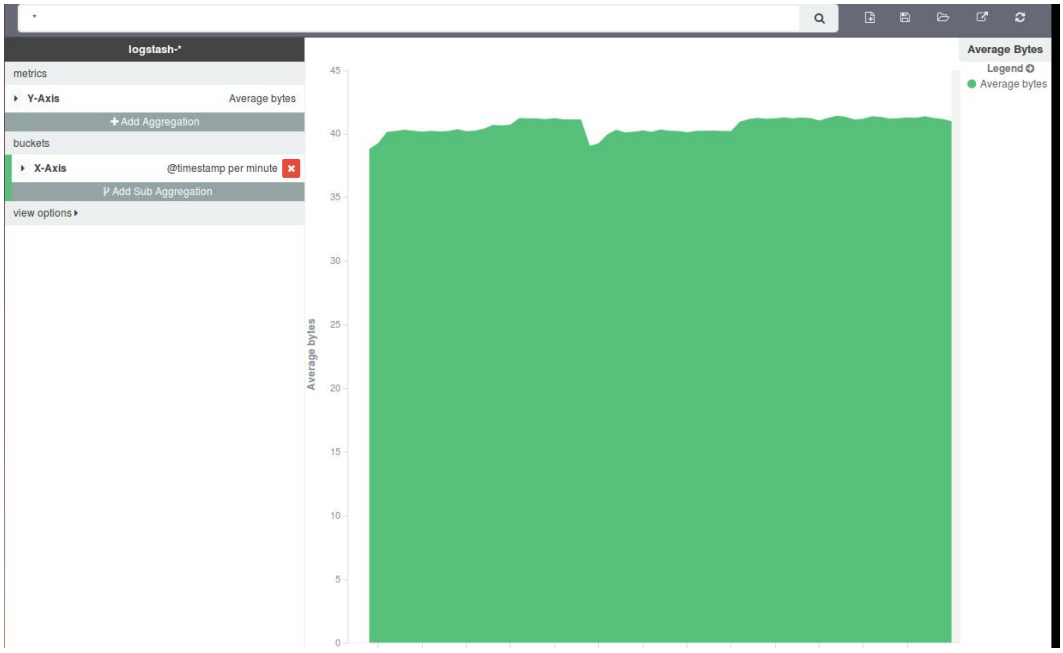

kibana
Discover
Visualize
Dashboard
Settings
~ 43 minutes ago to ~ 13 minutes ago
clientip:10.0.0.7 AND verb:GET
logstash-*
Selected Fields
_source
Fields
Popular fields
host
path
@timestamp
@version
_id
_index
_type
message
17 hits
September 13th 2015, 15:30:00.000 - September 13th 2015, 16:00:00.000
Count
@timestamp per 30 seconds
Time
_source
September 13th 2015, 15:52:03.001
clientip.raw: clientip: 10.0.0.7 verb: GET message: 10.0.0.7 - - [13/Sep/2015:15:50:27 +0100 "GET /elk/demo/17 HTTP/1.1" 200 40 @version: 1 @timestamp: September 13th 2015, 15:52:03.001 host: saurzcode path: /var/lib/tomcat7/logs/localhost_access_log.2015-09-13.txt ident: - auth: timestamp: 13/Sep/2015:15:50:27 +0100 request: /elk/demo/17 httpversion: 1.1 response: 200


kibana
Discover
Visualize
Dashboard
Settings
~ 43 minutes ago to ~ 13 minutes ago
clientip:10.0.0.7 AND verb:GET AND request:"/elk/demo/12"
logstash-*
Selected Fields
_source
Fields
Popular fields
host
path
@timestamp
@version
_id
_index
_type
message
1 hit
September 13th 2015, 15:30:00.000 - September 13th 2015, 16:00:00.000
Count
@timestamp per 30 seconds
Time
_source
September 13th 2015, 15:52:02.988
request: /elk/demo/12 clientip.raw: clientip: 10.0.0.7 verb: GET message: 10.0.0.7 - - [13/Sep/2015:15:50:21 +0100] "GET /elk/demo/12 HTTP/1.1" 200 40 @version: 1 @timestamp: September 13th 2015, 15:52:02.988 host: saurzcode path: /var/lib/tomcat7 /logs/localhost_access_log.2015-09-13.txt ident: - auth: - timestamp: 13/Sep/2015:15:50:21 +0100

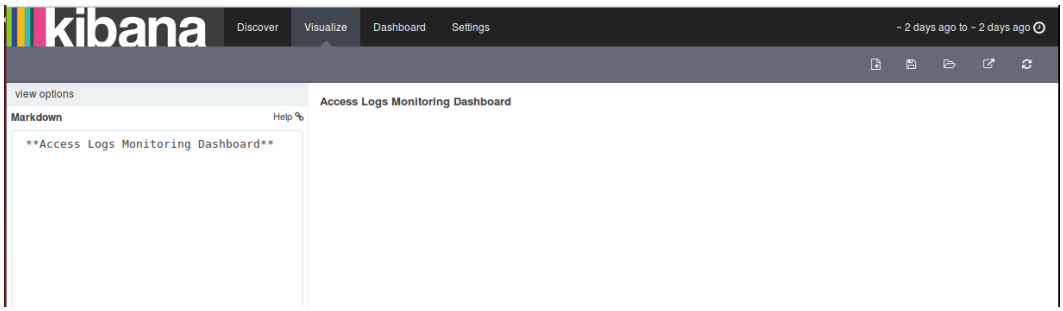

logstash-*
Selected Fields
_source
Fields
@timestamp
@version
_id
_index
_type
auth
bytes
clientip
host
httpversion
ident
message
path
request
response
timestamp
verb
5,473 hits
September 13th 2015, 17:36:48.990 - September 13th 2015, 18:45:00.000
Count
@timestamp per minute
Time
_source
September 13th 2015, 18:45:00.000
message: 10.0.0.2 - - [13/Sep/2015:18:45:00 +0100] "GET /elk/demo/2378 HTTP/1.1" 200 41 @version: 1 @timestamp: September 13th 2015, 18:45:00.000 host: saurzcode path: /var /lib/tomcat7/logs/localhost_access_log.txt clientip: 10.0.0.2 ident: - auth: - timestamp: 13/Sep/2015:18:45:00 +0100 verb: GET request: /elk/demo/2378 httpversion: 1.1
September 13th 2015, 18:44:59.000
message: 10.0.0.2 - - [13/Sep/2015:18:44:59 +0100] "GET /elk/demo/2377 HTTP/1.1" 200 42 @version: 1 @timestamp: September 13th 2015, 18:44:59.000 host: saurzcode path: /var /lib/tomcat7/logs/localhost_access_log.txt clientip: 10.0.0.2 ident: - auth: - timestamp: 13/Sep/2015:18:44:59 +0100 verb: GET request: /elk/demo/2377 httpversion: 1.1
September 13th 2015, 18:44:58.000
message: 10.0.0.2 - - [13/Sep/2015:18:44:58 +0100] "GET /elk/demo/2376 HTTP/1.1" 200 41 @version: 1 @timestamp: September 13th 2015, 18:44:58.000 host: saurzcode path: /var /lib/tomcat7/logs/localhost_access_log.txt clientip: 10.0.0.2 ident: - auth: -

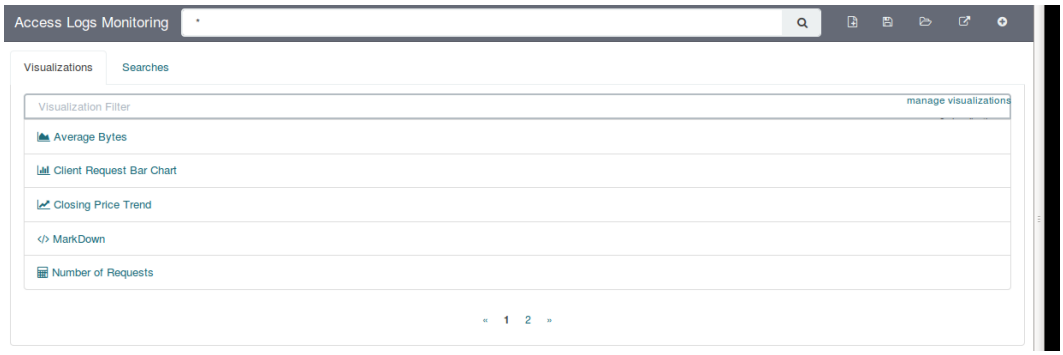

kibana
Discover
Visualize
Dashboard
Settings
Create a new visualization
Step 1
Area chart
Great for stacked timelines in which the total of all series is more important than comparing any two or more series. Less useful for assessing the relative change of unrelated data points as changes in a series 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.

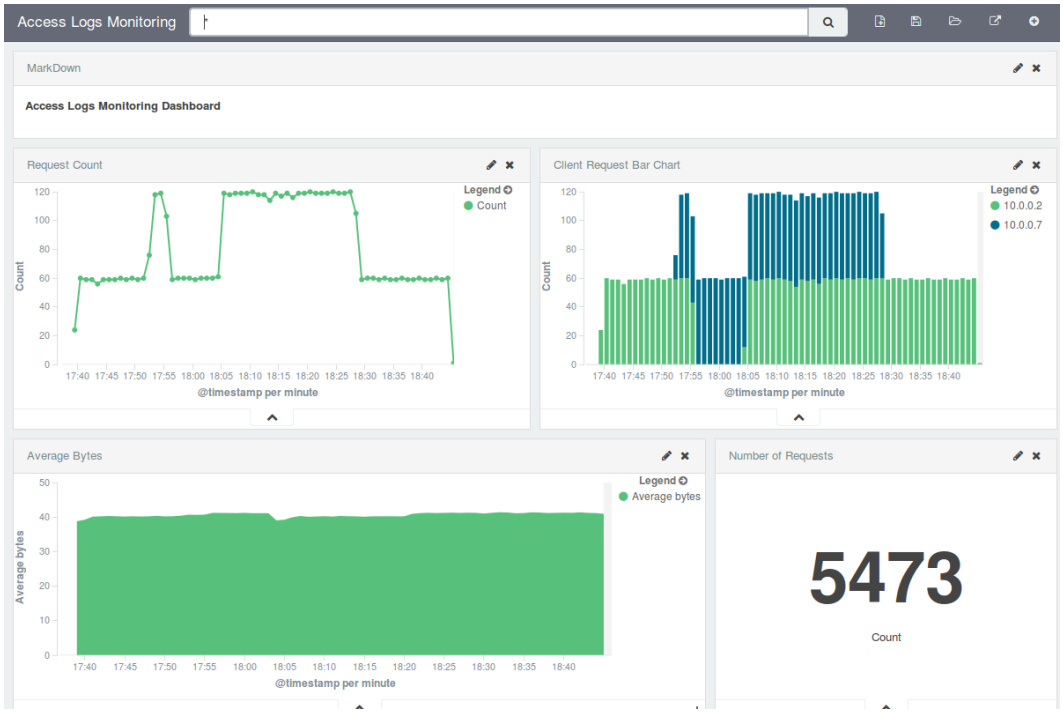
logstash-*
metrics
Y-Axis
Count
Add Aggregation
buckets
X-Axis
@timestamp per minute
Add Sub Aggregation
view options
Request Count
Legend
Count
120
100
80
60
40
20
Count

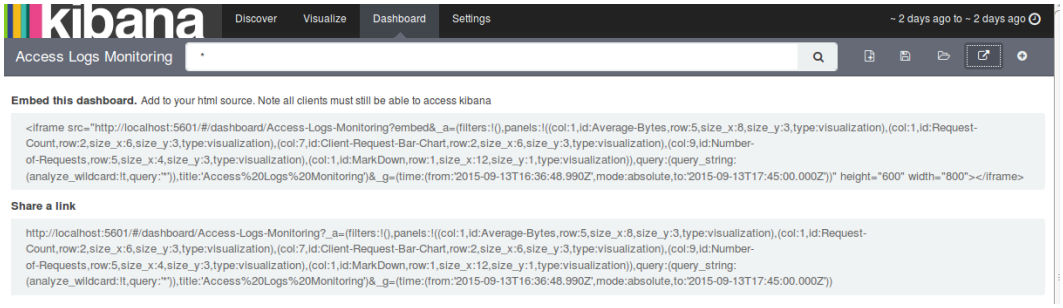

*
logstash-*
metrics
Y-Axis
Average bytes
Add Aggregation
buckets
X-Axis
@timestamp per minute
Add Sub Aggregation
view options
Average Bytes
Legend
Average bytes
Average bytes
45
40
35
30
25
20
15
10
5
0


logstash-*
metrics
Y-Axis
Count
Add Aggregation
buckets
X-Axis
Aggregation
Date Histogram
Field
@timestamp
Interval
Auto
Advanced
Split Bars
Sub Aggregation
Terms
Field
Analyzed Field
clientip
Order
Size
Top
5
Order By
metric: Count
Advanced
Add Sub Aggregation
view options
Client Request Bar Chart
Legend
10.0.0.2
10.0.0.7
Count
120
100
80
60
40
20
0
17:40
17:45
17:50
17:55
18:00
18:05
18:10
18:15
18:20
18:25
18:30
18:35
18:40

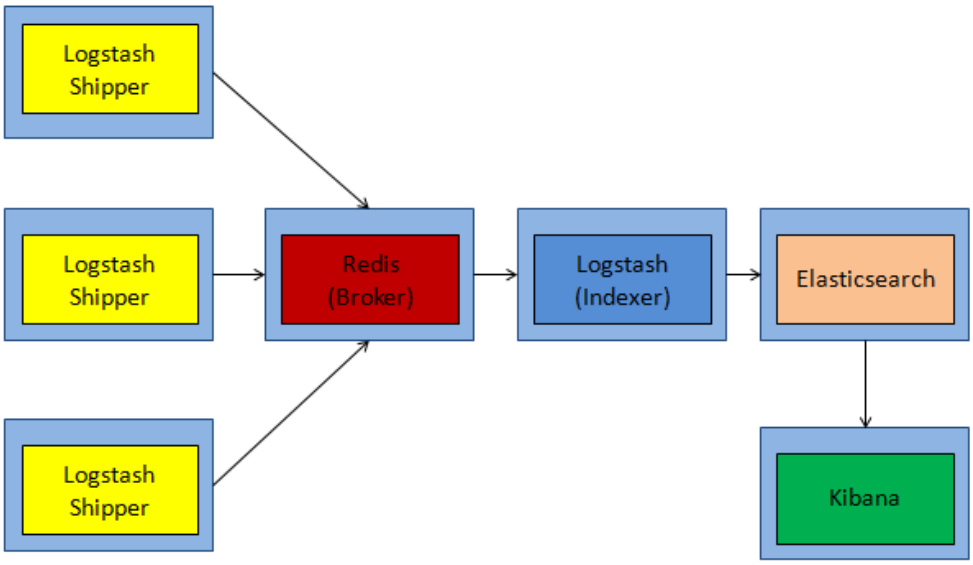

kibana
Discover
Visualize
Dashboard
Settings
~ 2 days ago to ~ 2 days ago
view options
Markdown
Help
Access Logs Monitoring Dashboard
Access Logs Monitoring Dashboard

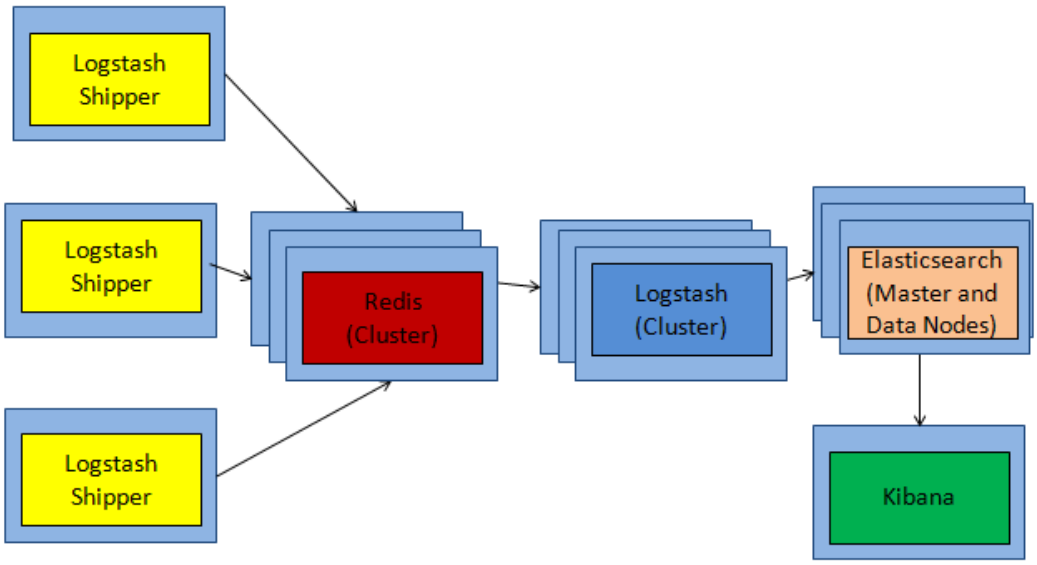

Access Logs Monitoring
*
Visualizations
Searches
Visualization Filter
manage visualizations
Average Bytes
Client Request Bar Chart
Closing Price Trend
MarkDown
Number of Requests
« 1 2 »

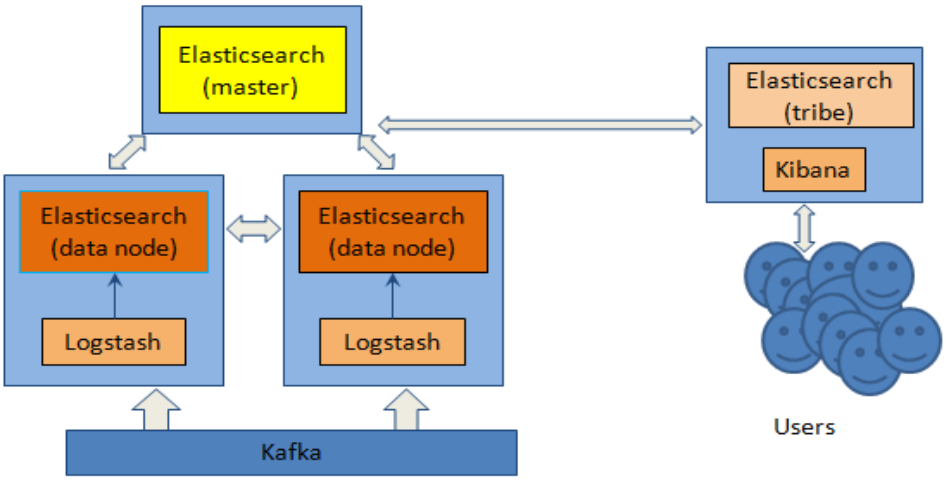

Access Logs Monitoring
MarkDown
Access Logs Monitoring Dashboard
Request Count
Legend
Count
Count
@timestamp per minute
Client Request Bar Chart
Legend
10.0.0.2
10.0.0.7
Count
@timestamp per minute
Average Bytes
Legend
Average bytes
Average bytes
@timestamp per minute
Number of Requests
5473
Count


kibana
Discover
Visualize
Dashboard
Settings
~ 2 days ago to ~ 2 days ago
Access Logs Monitoring
Embed this dashboard. Add to your html source. Note all clients must still be able to access kibana
<iframe src="http://localhost:5601/#/dashboard/Access-Logs-Monitoring?embed&_a=(filters:!(),panels:!((col:1,id:Average-Bytes,row:5,size_x:8,size_y:3,type:visualization),(col:1,id:Request-Count,row:2,size_x:6,size_y:3,type:visualization),(col:7,id:Client-Request-Bar-Chart,row:2,size_x:6,size_y:3,type:visualization),(col:9,id:Number-of-Requests,row:5,size_x:4,size_y:3,type:visualization),(col:1,id:MarkDown,row:1,size_x:12,size_y:1,type:visualization)),query:(query_string:(analyze_wildcard:!t,query:'*')),title:'Access%20Logs%20Monitoring')&_g=(time:(from:'2015-09-13T16:36:48.990Z',mode:absolute,to:'2015-09-13T17:45:00.000Z'))" height="600" width="800"></iframe>
Share a link
http://localhost:5601/#/dashboard/Access-Logs-Monitoring?_a=(filters:!(),panels:!((col:1,id:Average-Bytes,row:5,size_x:8,size_y:3,type:visualization),(col:1,id:Request-Count,row:2,size_x:6,size_y:3,type:visualization),(col:7,id:Client-Request-Bar-Chart,row:2,size_x:6,size_y:3,type:visualization),(col:9,id:Number-of-Requests,row:5,size_x:4,size_y:3,type:visualization),(col:1,id:MarkDown,row:1,size_x:12,size_y:1,type:visualization)),query:(query_string:(analyze_wildcard:!t,query:'*')),title:'Access%20Logs%20Monitoring')&_g=(time:(from:'2015-09-13T16:36:48.990Z',mode:absolute,to:'2015-09-13T17:45:00.000Z'))

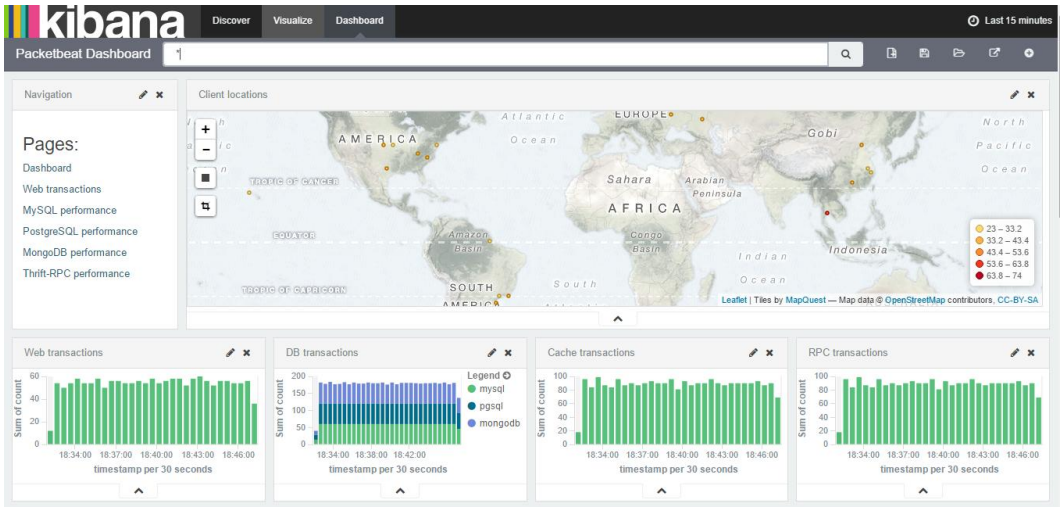
Chapter 9

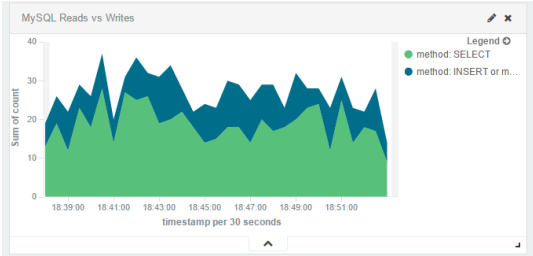

Logstash
Shipper
Logstash
Shipper
Logstash
Shipper
Redis
(Broker)
Logstash
(Indexer)
Elasticsearch
Kibana

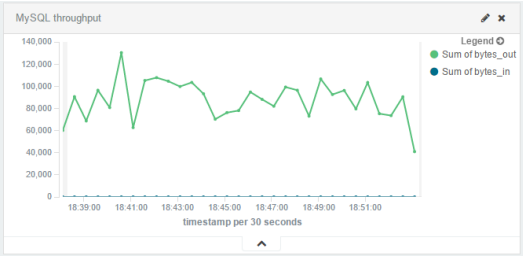

Logstash
Shipper
Logstash
Shipper
Logstash
Shipper
Redis
(Cluster)
Logstash
(Cluster)
Elasticsearch
(Master and
Data Nodes)
Kibana


Elasticsearch
(master)
Elasticsearch
(tribe)
Kibana
Elasticsearch
(data node)
Logstash
Elasticsearch
(data node)
Logstash
Kafka
Users


Analytics
Transformer Inspections
Transformer Types
MAGNEFIX
unset
OPEN RAIL
SVS
SPECIAAL
MAGNEFIX / OPEN
Transformer Count
643
Count of documents
Transformer Status
Existing
Proposed
Abandoned
Transformer Installs
Count of documents
phys.installed_date per 1 year


kibana
Discover
Visualize
Dashboard
Last 15 minutes
Packetbeat Dashboard
Navigation
Pages:
Dashboard
Web transactions
MySQL performance
PostgreSQL performance
MongoDB performance
Thrift-RPC performance
Client locations
AMERICA
EUROPE
AFRICA
Sahara
Gobi
Indonesia
Web transactions
DB transactions
Cache transactions
RPC transactions
Sum of count
timestamp per 30 seconds
Legend
mysql
pgsql
mongodb



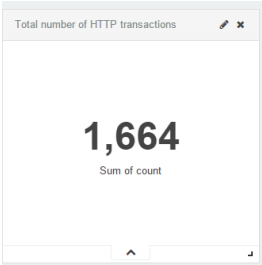


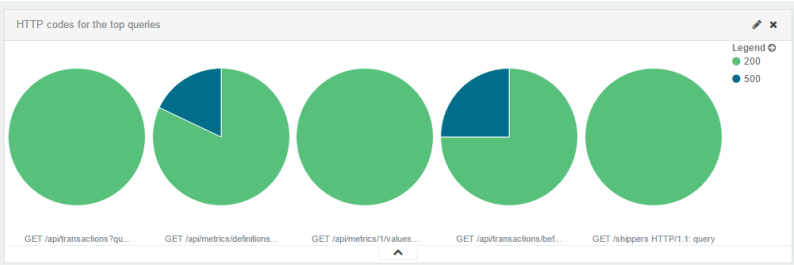
Most frequent MySQL queries

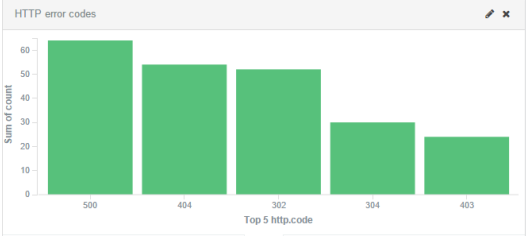
Top 10 query	Sum of count
rollback	687
SELECT post.id AS post_id, post.username AS post_username, post.title AS post_title, post.body AS post_body, post.pub_date AS post_pub_date FROM post ORDER BY post.pub_date	552
commit	279
INSERT INTO post (username, title, body, pub_date) VALUES ('Monica', 'test', 'dashjsa', '2013-10-24 21:31:02')	48
INSERT INTO post (username, title, body, pub_date) VALUES ('Anonymous', 'Bug4', 'Desct.', '2013-10-24 21:32:29')	32
INSERT INTO post (username, title, body, pub_date) VALUES ('Anonymous', 'Bug: Cannot change the info of a user', 'Click on the update user button.', '2013-10-24 21:31:50')	31

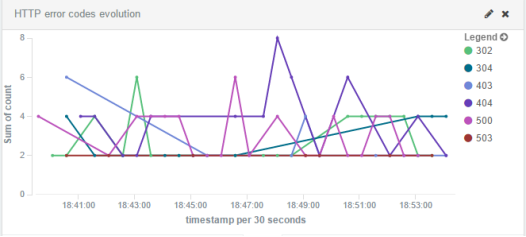
Slowest MySQL queries

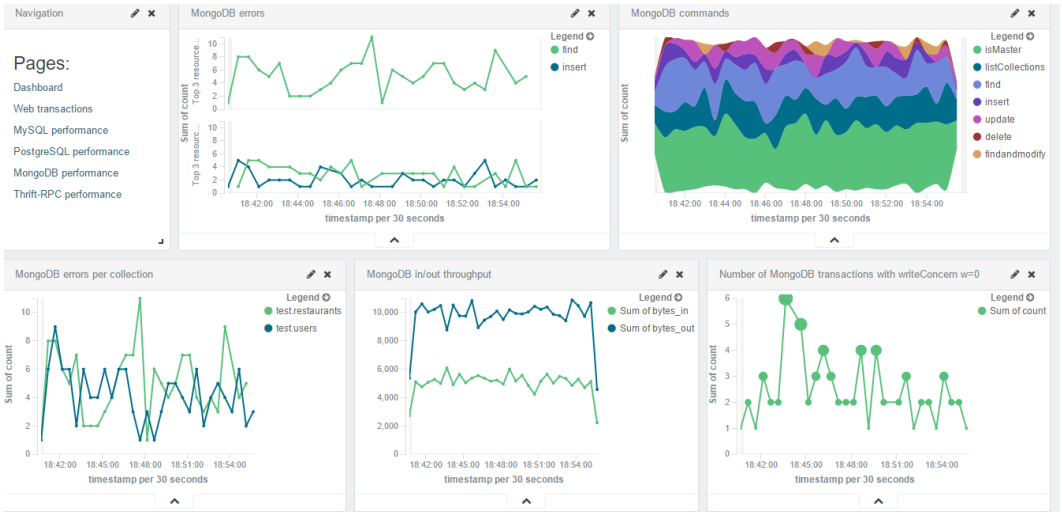
Top 10 query	Average responsetime
SELECT * FROM post WHERE username='fake'	38.893
DELETE FROM post WHERE username='fake'	38.346
UPDATE post SET pub_date='2014-04-09 11:38:05' WHERE username='fake'	36.92
INSERT INTO post (username, title, body, pub_date) VALUES ('Anonymous', 'Bug2', 'Refactoring feature1.', '2013-10-24 21:32:12')	36.455
INSERT INTO post (username, title, body, pub_date) VALUES ('Anonymous', 'Bug: 66 user.', 'Link broken.', '2013-10-24 21:33:06')	34.615
INSERT INTO post (username, title, body, pub_date) VALUES ('Anonymous', 'Bug: Cannot delete user ', '', '2013-10-24 21:32:41')	34.069









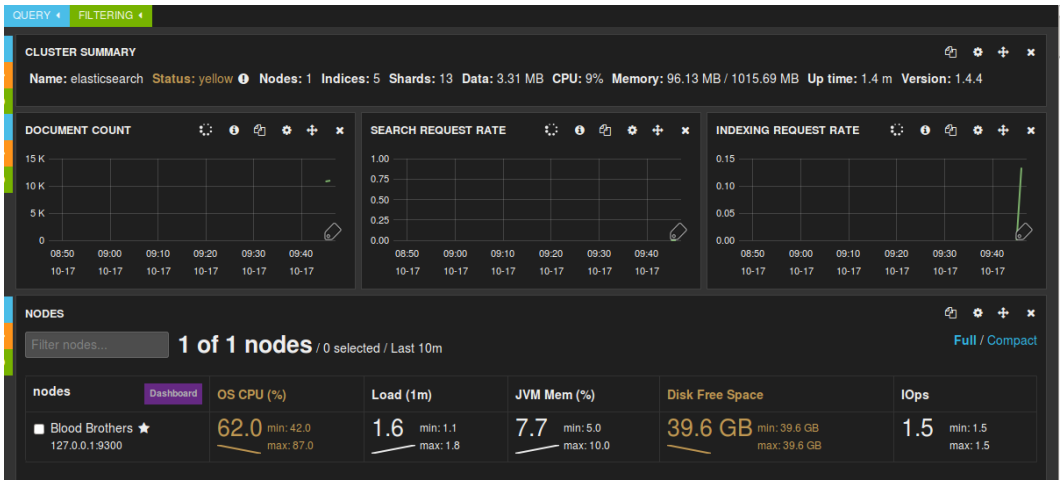


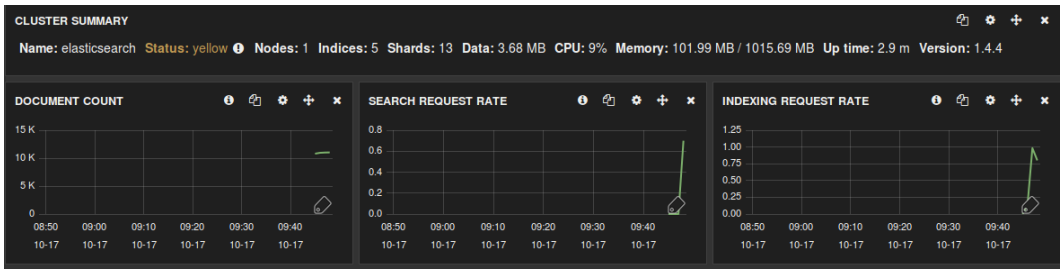
Chapter 10

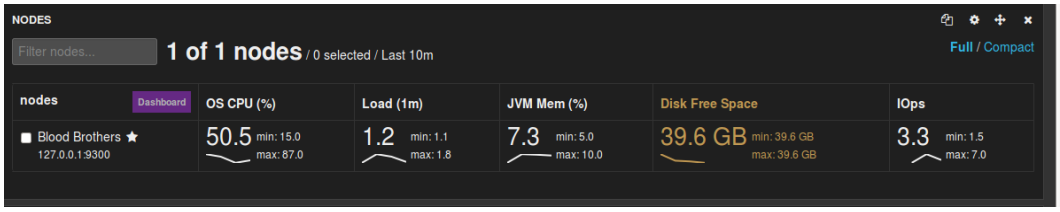
```
packtpub@saurzcode:/usr/share/elasticsearch/bin/shield$ sudo ./esusers useradd es_admin -r admin
Enter new password:
Retype new password:
```

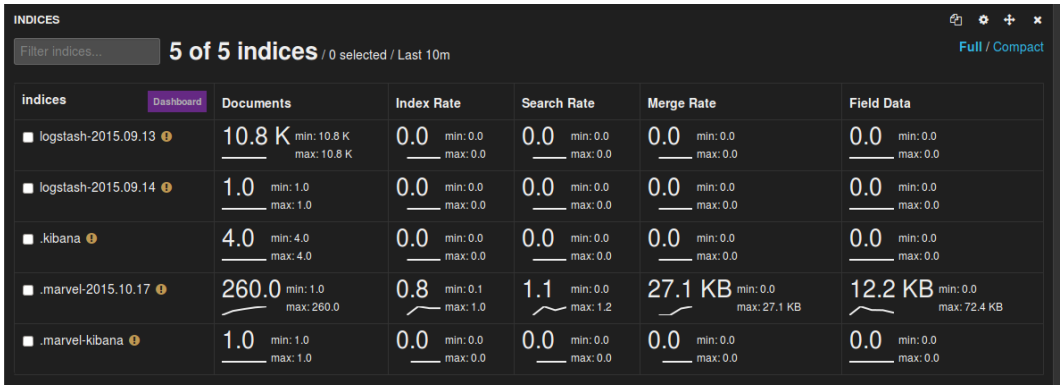
```
packtpub@saurzcode:/usr/share/elasticsearch/bin/shield$ sudo ./esusers list
es_admin        : admin
packtpub@saurzcode:/usr/share/elasticsearch/bin/shield$ sudo ./esusers userdel es_admin
packtpub@saurzcode:/usr/share/elasticsearch/bin/shield$ sudo ./esusers list
No users found
```

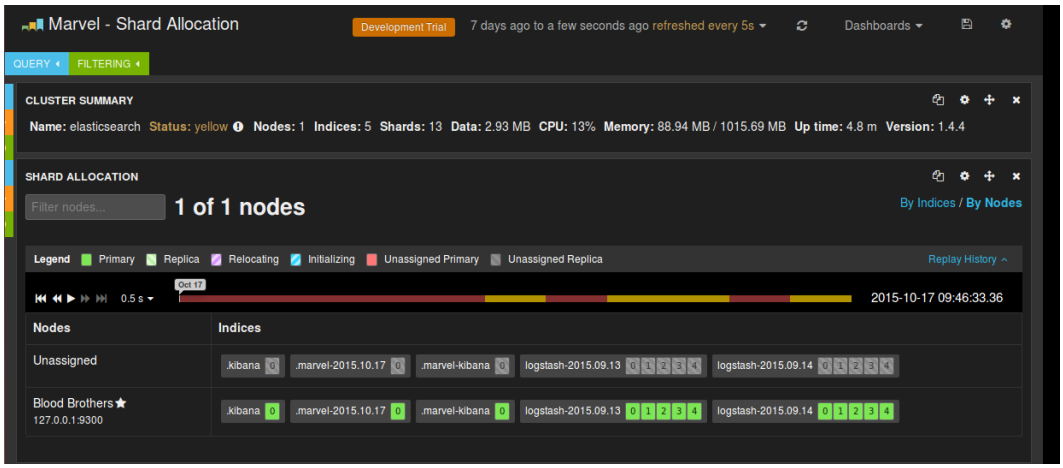
```
packtpub@saurzcode:/usr/share/elasticsearch/bin$ sudo ./plugin -i elasticsearch/marvel/latest
[sudo] password for packtpub:
-> Installing elasticsearch/marvel/latest...
Trying http://download.elasticsearch.org/elasticsearch/marvel/marvel-latest.zip...
Downloading ..................................................................................................
..................................................................................................
..................................................................................................
..................................................................................................
..................................................................................................
..................................................................................................
..................................................................DONE
Installed elasticsearch/marvel/latest into /usr/share/elasticsearch/plugins/marvel
```






NODES
Filter nodes...
1 of 1 nodes / 0 selected / Last 10m
Full / Compact
nodes
Dashboard
OS CPU (%)
Load (1m)
JVM Mem (%)
Disk Free Space
IOps
Blood Brothers
127.0.0.1:9300
50.5 min: 15.0 max: 87.0
1.2 min: 1.1 max: 1.8
7.3 min: 5.0 max: 10.0
39.6 GB min: 39.6 GB max: 39.6 GB
3.3 min: 1.5 max: 7.0


INDICES
Filter indices...
5 of 5 indices / 0 selected / Last 10m
Full / Compact
indices
Dashboard
Documents
Index Rate
Search Rate
Merge Rate
Field Data
logstash-2015.09.13
10.8 K min: 10.8 K max: 10.8 K
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0
logstash-2015.09.14
1.0 min: 1.0 max: 1.0
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0
.kibana
4.0 min: 4.0 max: 4.0
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0
.marvel-2015.10.17
260.0 min: 1.0 max: 260.0
0.8 min: 0.1 max: 1.0
1.1 min: 0.0 max: 1.2
27.1 KB min: 0.0 max: 27.1 KB
12.2 KB min: 0.0 max: 72.4 KB
.marvel-kibana
1.0 min: 1.0 max: 1.0
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0
0.0 min: 0.0 max: 0.0


Marvel - Shard Allocation
Development Trial
7 days ago to a few seconds ago refreshed every 5s
Dashboards
QUERY
FILTERING
CLUSTER SUMMARY
Name: elasticsearch Status: yellow Nodes: 1 Indices: 5 Shards: 13 Data: 2.93 MB CPU: 13% Memory: 88.94 MB / 1015.69 MB Up time: 4.8 m Version: 1.4.4
SHARD ALLOCATION
Filter nodes...
1 of 1 nodes
By Indices / By Nodes
Legend Primary Replica Relocating Initializing Unassigned Primary Unassigned Replica
Replay History
0.5 s
Oct 17
2015-10-17 09:46:33.36
Nodes
Indices
Unassigned
.kibana 0
.marvel-2015.10.17 0
.marvel-kibana 0
logstash-2015.09.13 0 1 2 3 4
logstash-2015.09.14 0 1 2 3 4
Blood Brothers
127.0.0.1:9300
.kibana 0
.marvel-2015.10.17 0
.marvel-kibana 0
logstash-2015.09.13 0 1 2 3 4
logstash-2015.09.14 0 1 2 3 4