

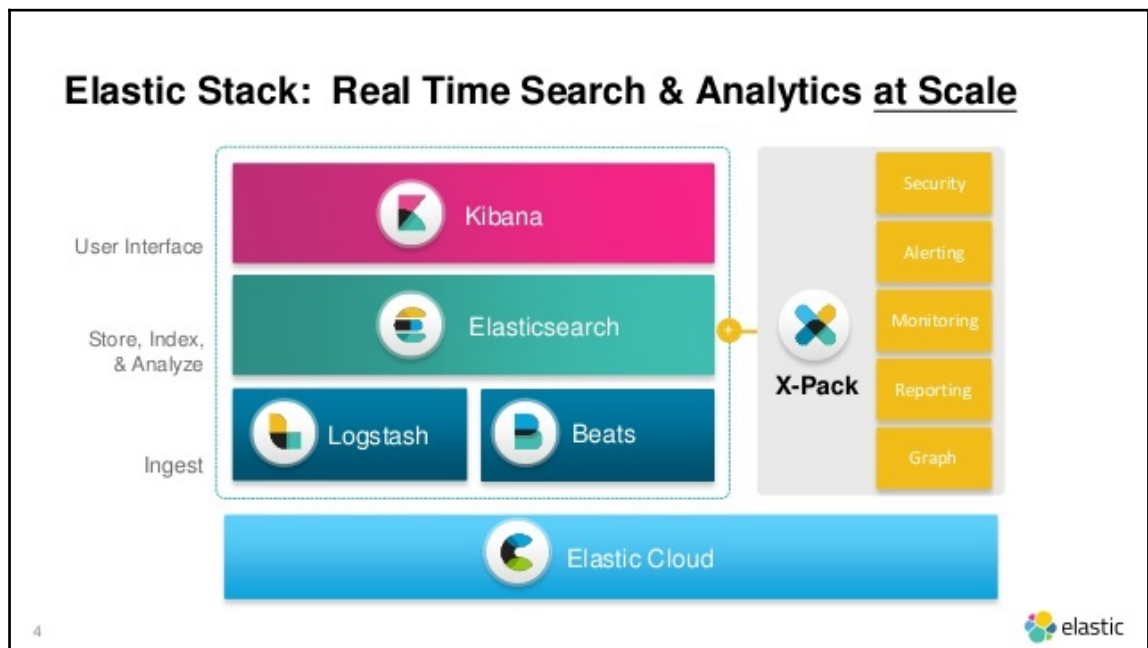
Table of Contents

| | |
|---|-----------|
| Chapter 1: Graphic bundle | 1 |
| Chapter 1: Introducing Elastic Stack | 1 |
| Chapter 2: Getting Started with Elasticsearch | 3 |
| Chapter 3: Searching-What is Relevant | 7 |
| Chapter 4: Analytics with Elasticsearch | 10 |
| Chapter 5: Analyzing Log Data | 12 |
| Chapter 6: Building Data Pipelines with Logstash | 14 |
| Chapter 7: Visualizing data with Kibana | 19 |
| Chapter 8: Elastic X-Pack | 42 |
| Chapter 9: Running Elastic Stack in Production | 59 |
| Chapter 10: Building a Sensor Data Analytics Application | 62 |
| Chapter 11: Monitoring Server Infrastructure | 68 |
| Index | 72 |

1

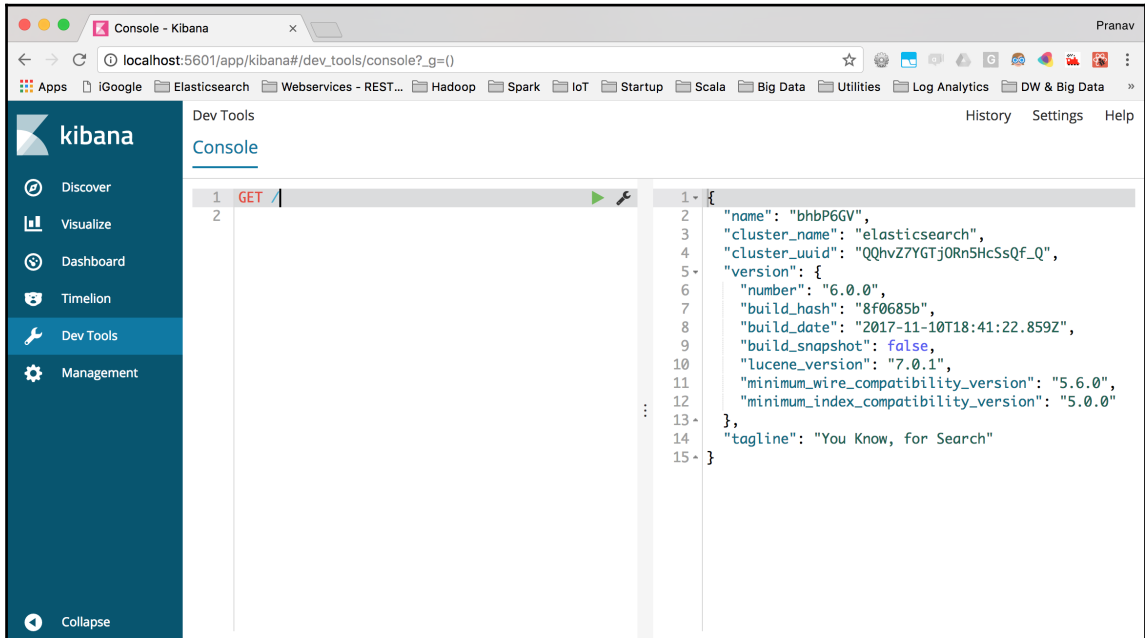
Graphic bundle

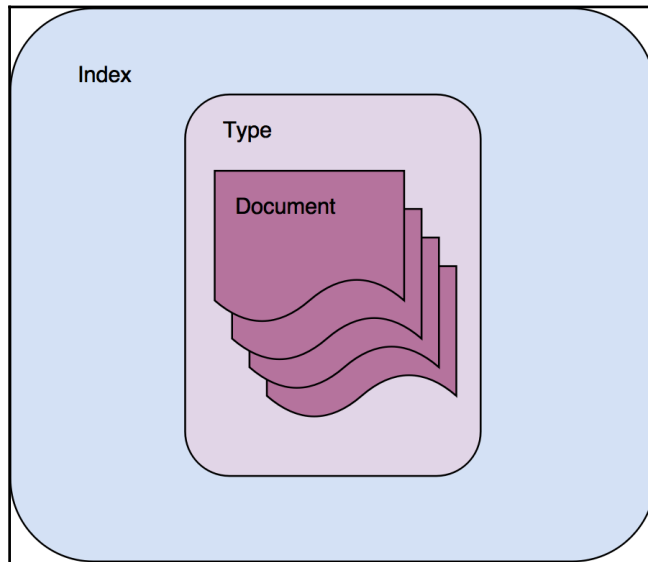
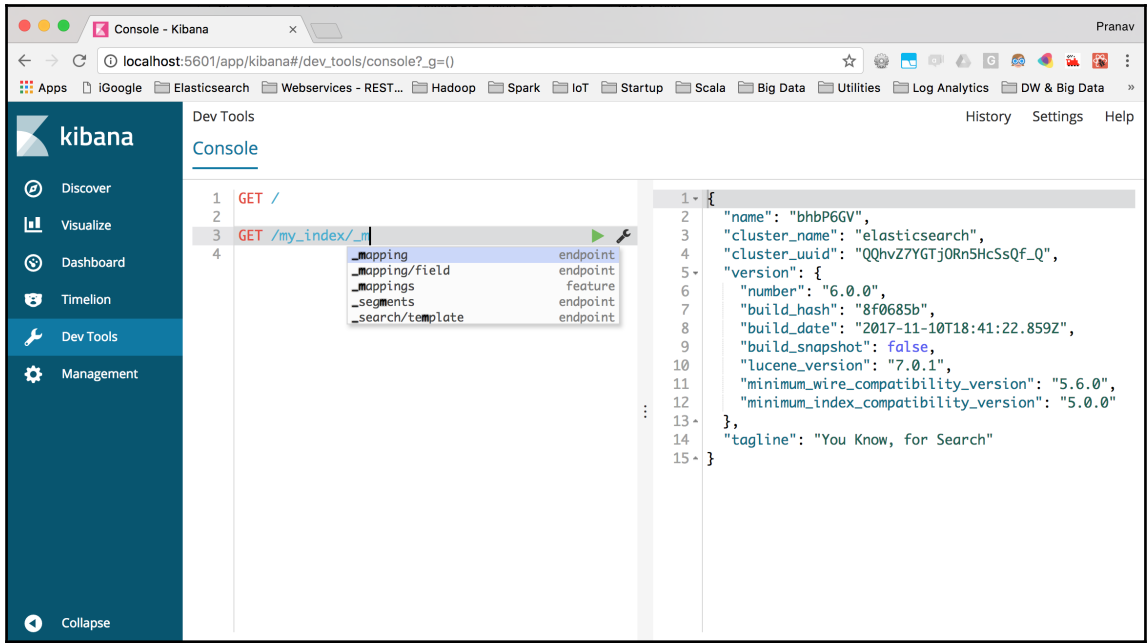
Chapter 1: Introducing Elastic Stack

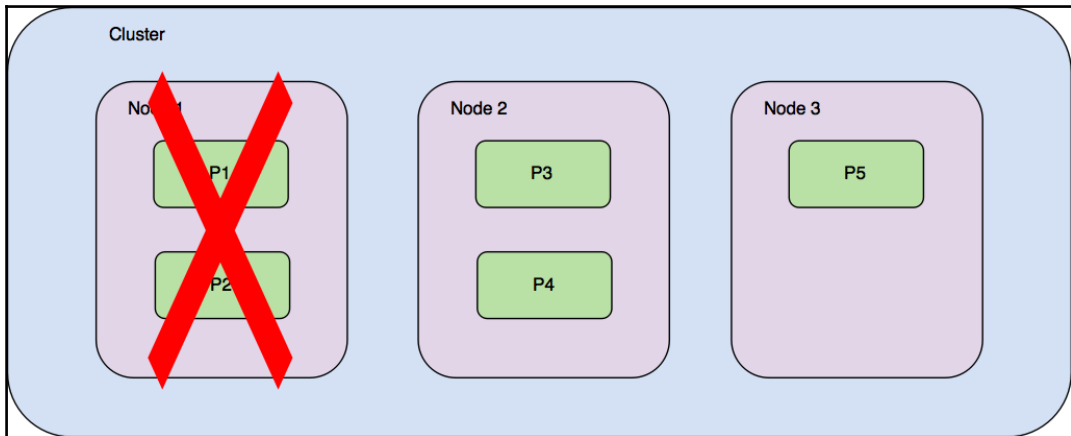
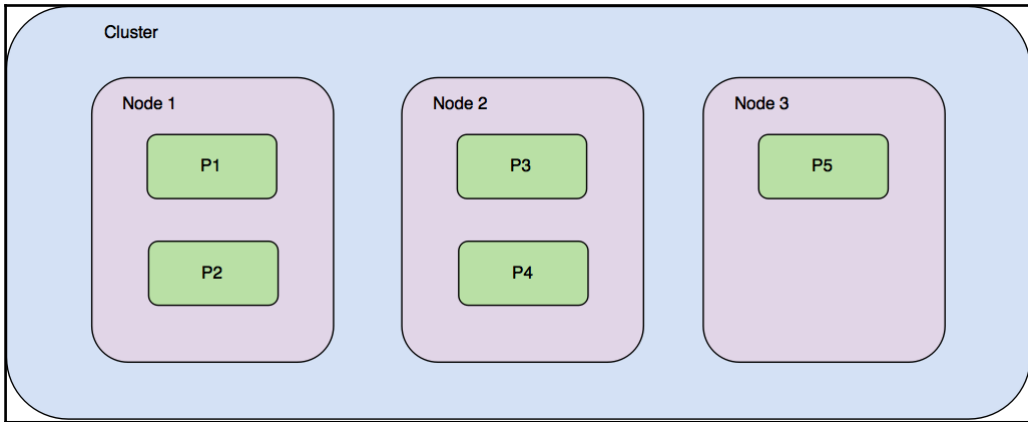


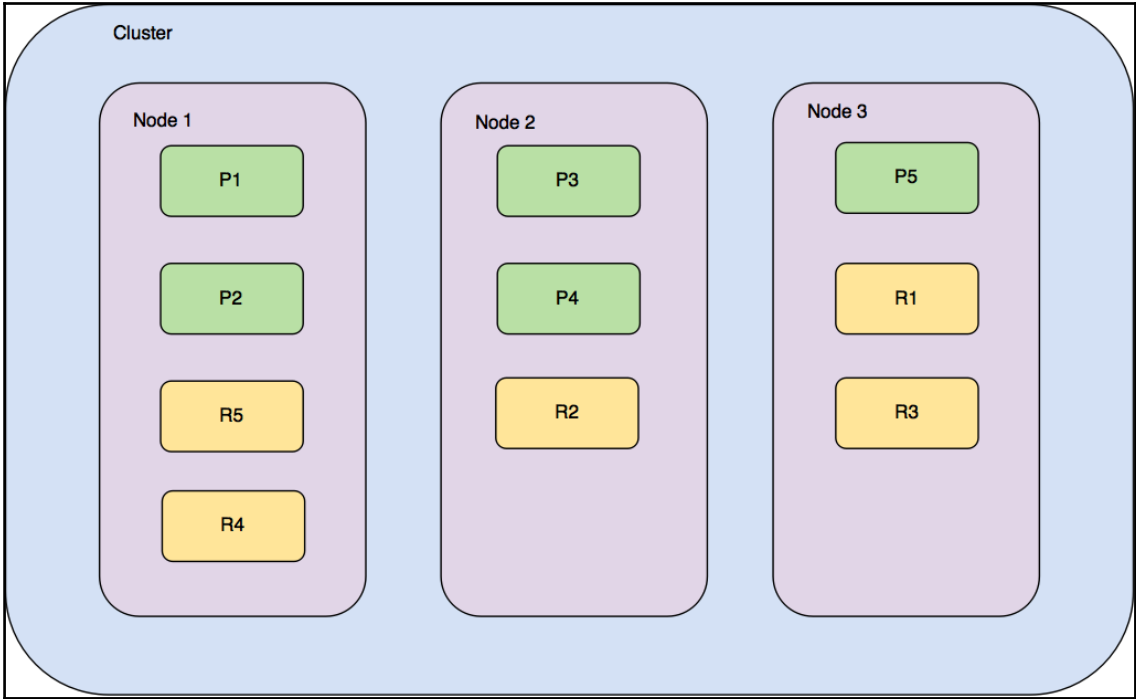
```
$ curl http://localhost:9200?pretty
{
  "name" : "bhbP6GV",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "QQhvZ7YGTjORn5HcSsQf_Q",
  "version" : {
    "number" : "6.0.0",
    "build_hash" : "8f0685b",
    "build_date" : "2017-11-10T18:41:22.859Z",
    "build_snapshot" : false,
    "lucene_version" : "7.0.1",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
$
```

Chapter 2: Getting Started with Elasticsearch

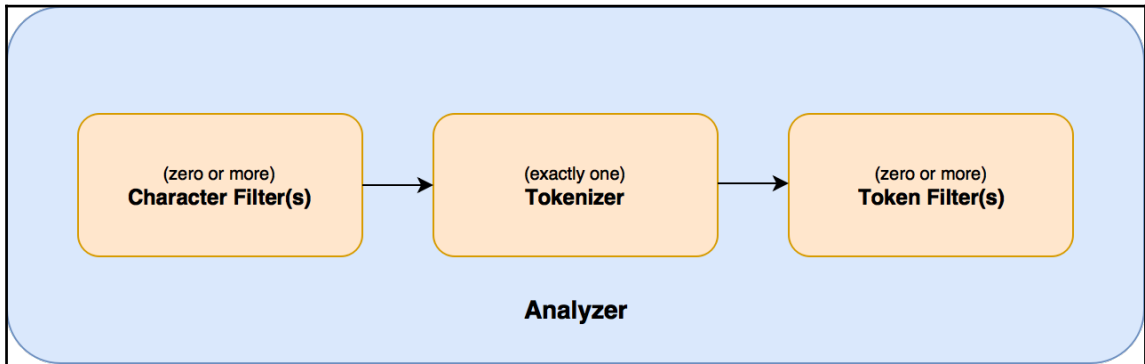


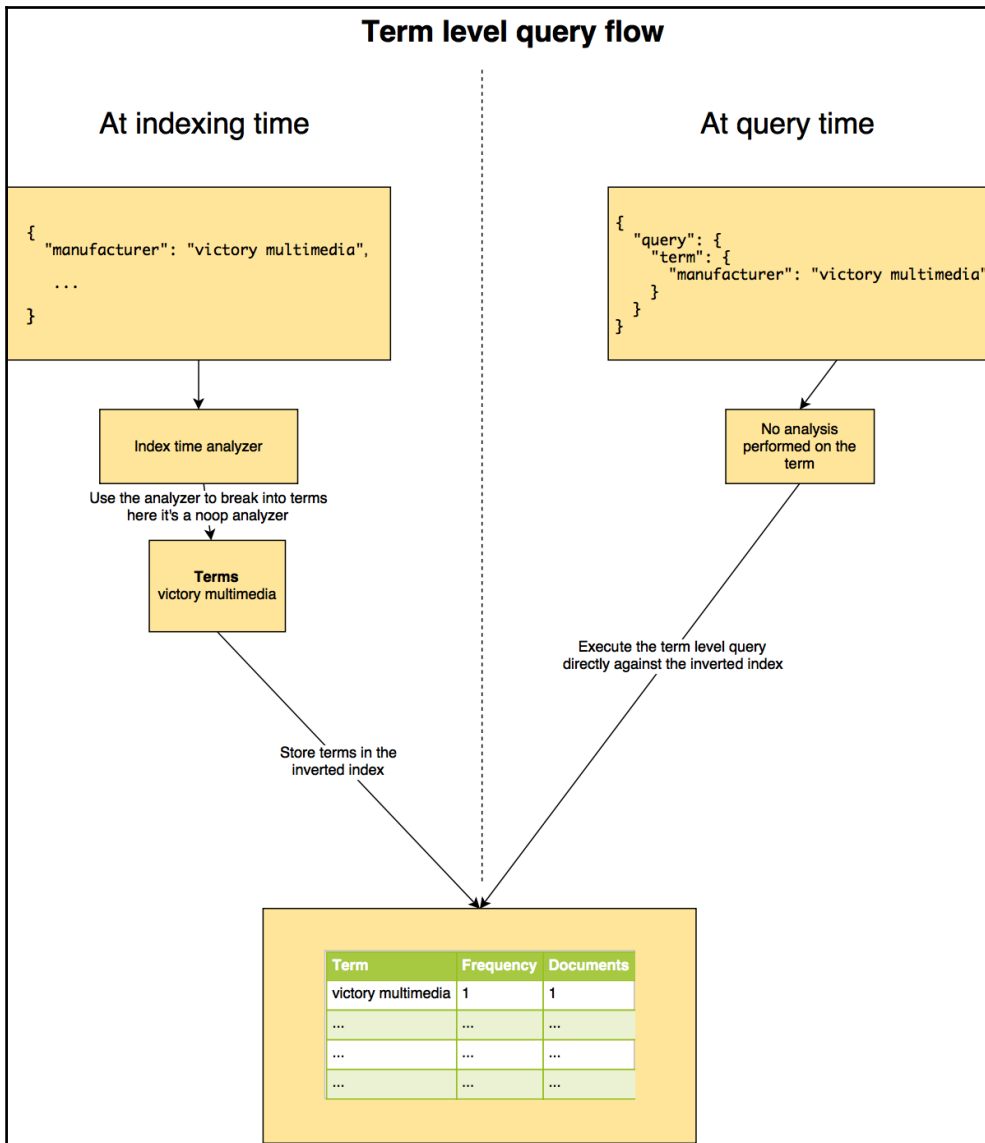


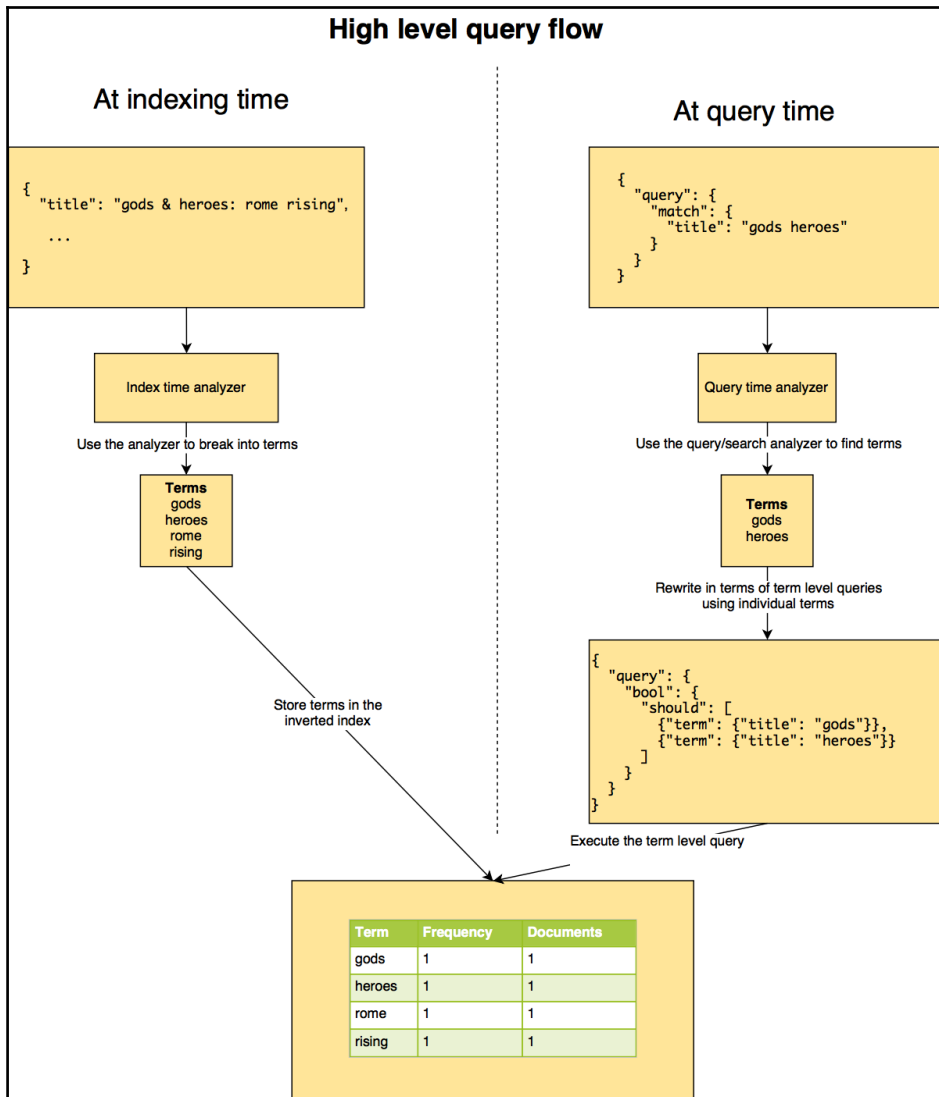




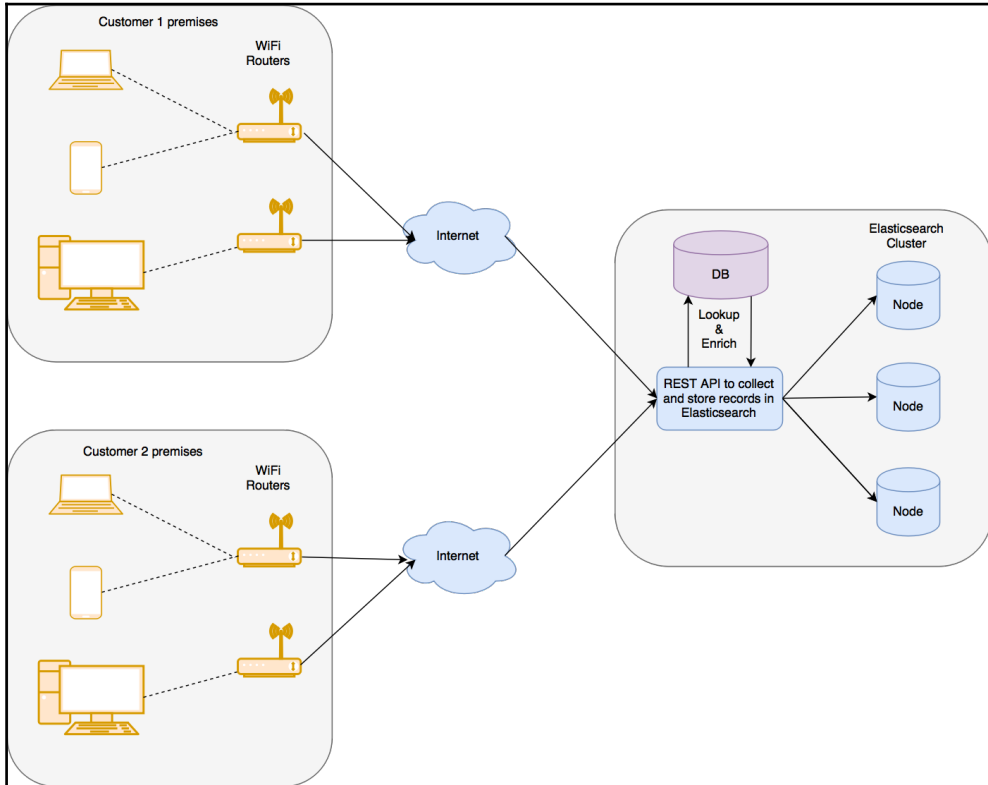
Chapter 3: Searching-What is Relevant

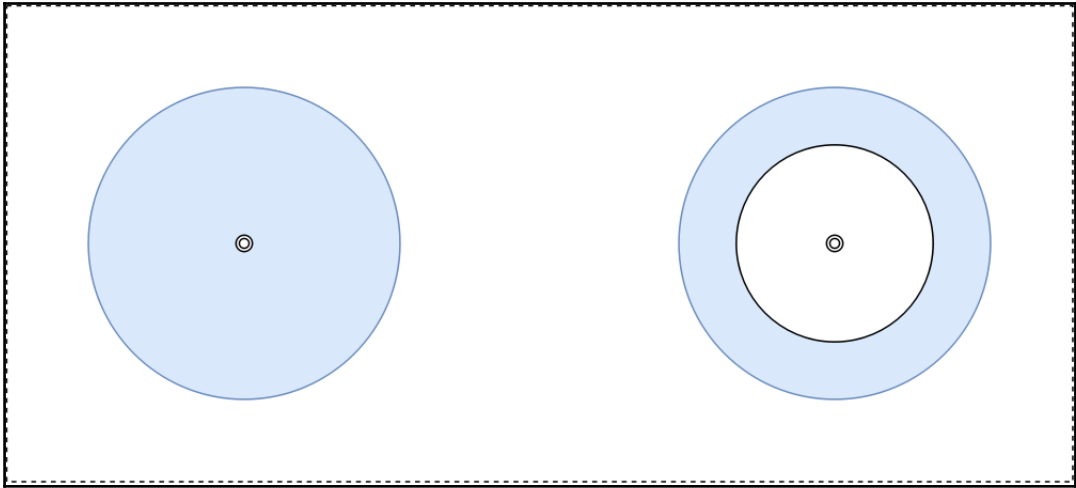






Chapter 4: Analytics with Elasticsearch





Chapter 5: Analyzing Log Data

```

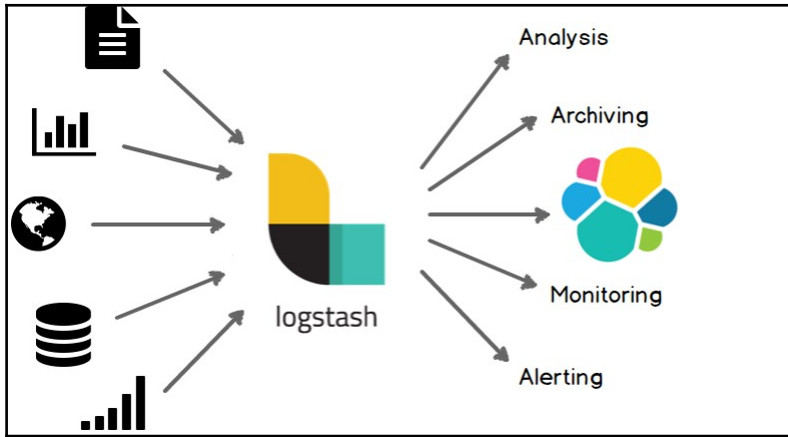
2011-05-20 20:06:06.46 Server      This instance of SQL Server last reported using a process ID of 1760 at 5/20/2011 8:03:41 PM (
2011-05-20 20:06:06.46 Server      Registry startup parameters:
-d C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\master.mdf          SQL Server Logs
-e C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\LOG\ERRORLOG
-l C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\mastlog.ldf
2011-05-20 20:06:06.66 Server      SQL Server is starting at normal priority base (=7). This is an informational message only. No

[2017-09-03 10:26:03.550] [WARN] [index.store      ] [node1] [hc_index][3] failed to build store metadata. checking segment info
integrity (with commit [no])
java.nio.file.NoSuchFileException: /u01/ga/fg/aw/3.2/data/EBCluster/node0/indices/hc_nr_sub_data_hc92stp/3/index/segments_lg
at sun.nio.fs.UnixException.translateToIOException(UnixException.java:84)
at sun.nio.fs.UnixException.throwAsIOException(UnixException.java:103)
at sun.nio.fs.UnixException.throwAsIOException(UnixException.java:107)
at sun.nio.fs.UnixFileSystemProvider.newFileChannel(UnixFileSystemProvider.java:177)
at java.nio.channels.FileChannel.open(FileChannel.java:127)
at java.nio.channels.FileChannel.open(FileChannel.java:335)
at org.apache.lucene.store.SICMDirectory.openInput(SICMDirectory.java:81)
at org.apache.lucene.store.FileSwitchDirectory.openInput(FileSwitchDirectory.java:186)
at org.apache.lucene.store.FilterDirectory.openInput(FilterDirectory.java:19)
at org.apache.lucene.store.FilterDirectory.openInput(FilterDirectory.java:19)
at org.elasticsearch.index.store.StoreMetadataSnapshot.checksumFromLuceneFile(Store.java:930)
at org.elasticsearch.index.store.StoreMetadataSnapshot.loadMetadata(Store.java:1640)
at org.elasticsearch.index.store.StoreMetadataSnapshot.<init>(Store.java:764)
at org.elasticsearch.index.store.Store.getMetadata(Store.java:1233)
at org.elasticsearch.index.store.Store.getMetadataOrEmpty(Store.java:192)
at org.elasticsearch.index.store.TransportNodeList shardStoreMetadata(ListStoreMetadata(TransportNodeListShardStoreMetadata.java:161)
at org.elasticsearch.index.store.TransportNodeListShardStoreMetadata.nodeOperation(TransportNodeListShardStoreMetadata.java:162)
at org.elasticsearch.index.store.TransportNodeListShardStoreMetadata.nodeOperation(TransportNodeListShardStoreMetadata.java:67)
at org.elasticsearch.action.support.nodes.TransportNodeAction.nodeOperation(TransportNodeAction.java:92)
at org.elasticsearch.action.support.nodes.TransportNodeActionNodeTransportHandler.messageReceived(TransportNodeAction.java:230)
at org.elasticsearch.action.support.nodes.TransportNodeActionNodeTransportHandler.messageReceived(TransportNodeAction.java:226)
at org.elasticsearch.transport.RequestHandlerRegistry.processMessageReceived(RequestHandlerRegistry.java:75)
at org.elasticsearch.transport.netty.MessageChannelHandler$RequestHandler.doRun(MessageChannelHandler.java:300)
at org.elasticsearch.common.util.concurrent.AbstractRunnable.run(AbstractRunnable.java:17)


93.180.71.3 -- [17/May/2015:08:05:23 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian
APT-HTTP/1.3 (0.8.16~exp12ubuntu10.21)"
80.91.33.133 -- [17/May/2015:08:05:24 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-" "Debian
APT-HTTP/1.3 (0.8.16~exp12ubuntu10.17)"
    
```

Elasticsearch
Exceptions

NGINX logs



Download Logstash

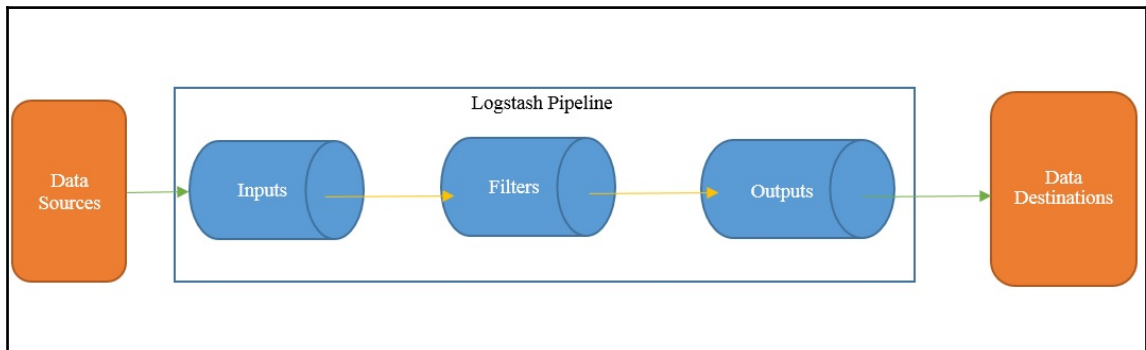
 Want to upgrade? We'll give you a hand. [Migration Guide](#) »

Version: 6.0.0

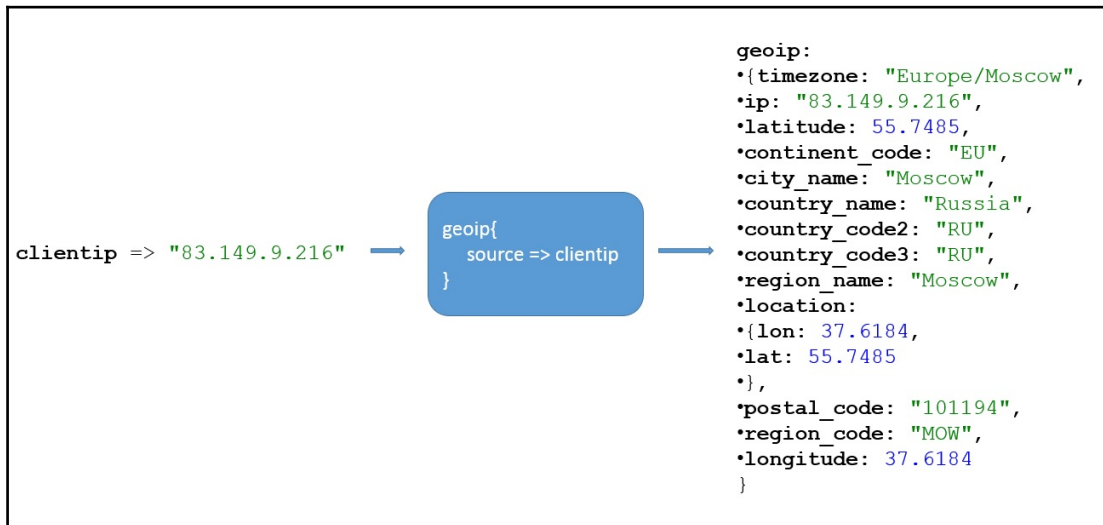
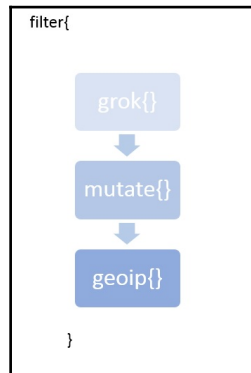
Release date: November 14, 2017

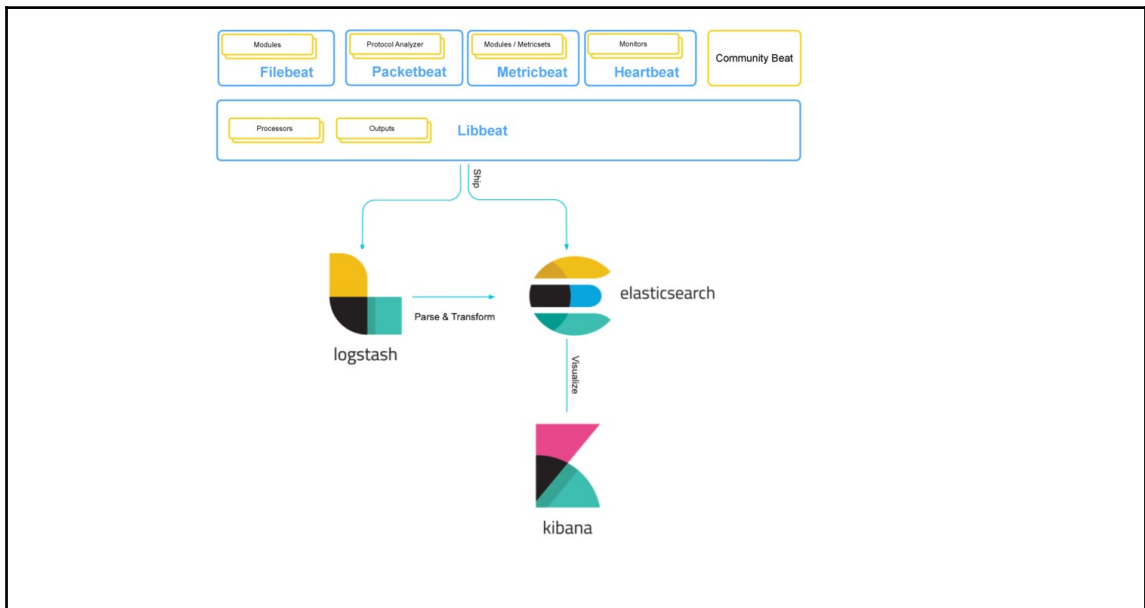
Notes: View detailed [release notes](#).
Not the version you're looking for? View [past releases](#).
Java 8 is required for Logstash 6.x and 5.x.

Downloads: [TAR.GZ sha](#) [ZIP sha](#) [DEB sha](#)
[RPM sha](#)



Chapter 6: Building Data Pipelines with Logstash





Download Filebeat



Want to upgrade? We'll give you a hand. [Migration Guide](#) »

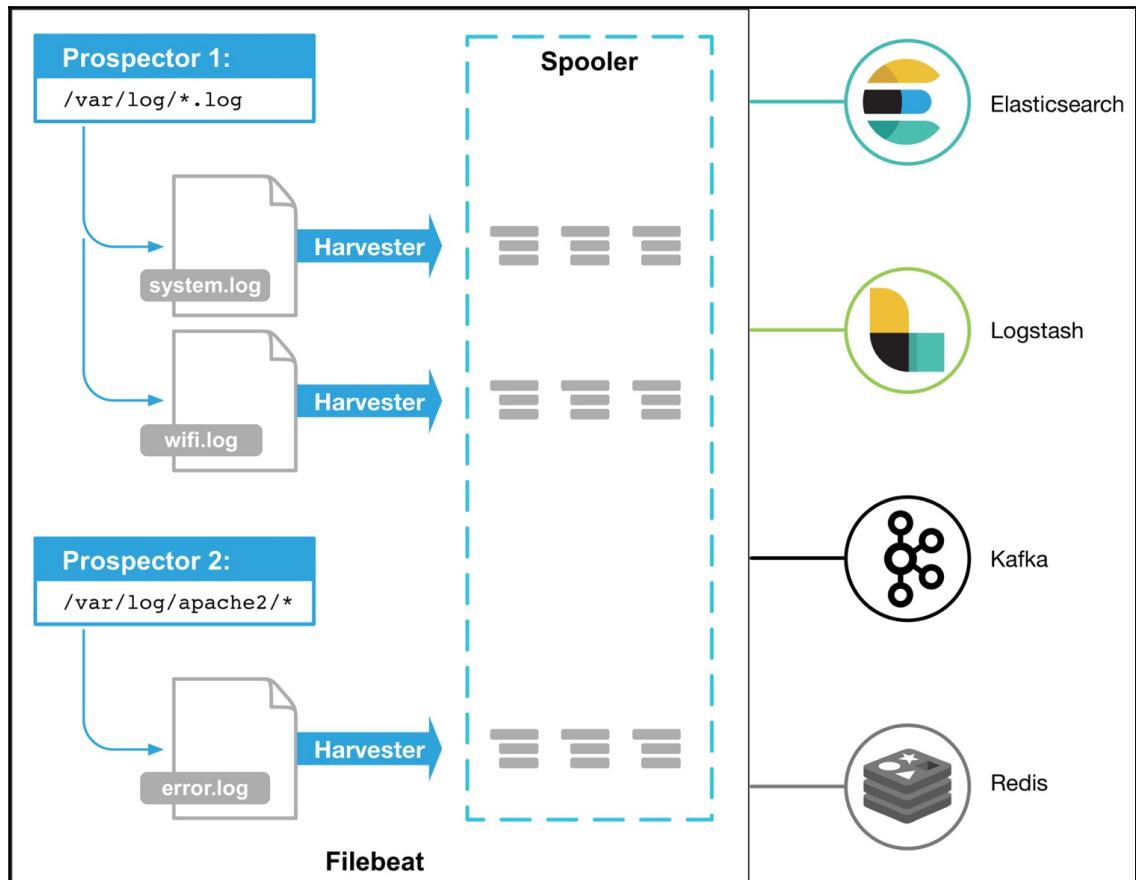
Version: 6.0.0

Release date: November 14, 2017

Notes: View [release notes](#).

Not the version you're looking for? View [past releases](#).

Downloads: [⬇️ DEB 32-BIT sha](#) [⬇️ DEB 64-BIT sha](#) [⬇️ RPM 32-BIT sha](#)
[⬇️ RPM 64-BIT sha](#) [⬇️ LINUX 32-BIT sha](#) [⬇️ LINUX 64-BIT sha](#)
[⬇️ MAC sha](#) [⬇️ WINDOWS 32-BIT sha](#) [⬇️ WINDOWS 64-BIT sha](#)



```
===== Filebeat prospectors =====
filebeat.prospectors:
- input_type: log
  paths:
    - /var/log/*.log
    - /var/log/messages
  # Exclude lines.
  exclude_lines: ["^DBG"]
  # Include lines.
  include_lines: ["^ERR", "^WARN"]

  tags: ["java_logs"]


  fields:
    env: staging

  ### Multiline options
  multiline.pattern: '^[[:space:]]'
  multiline.negate: false
  multiline.match: after

  scan_frequency: 1s
- input_type: log
  paths:
    - /var/log/apache/httpd-*.log
  document_type: apache
```

Chapter 7: Visualizing data with Kibana

Download Kibana

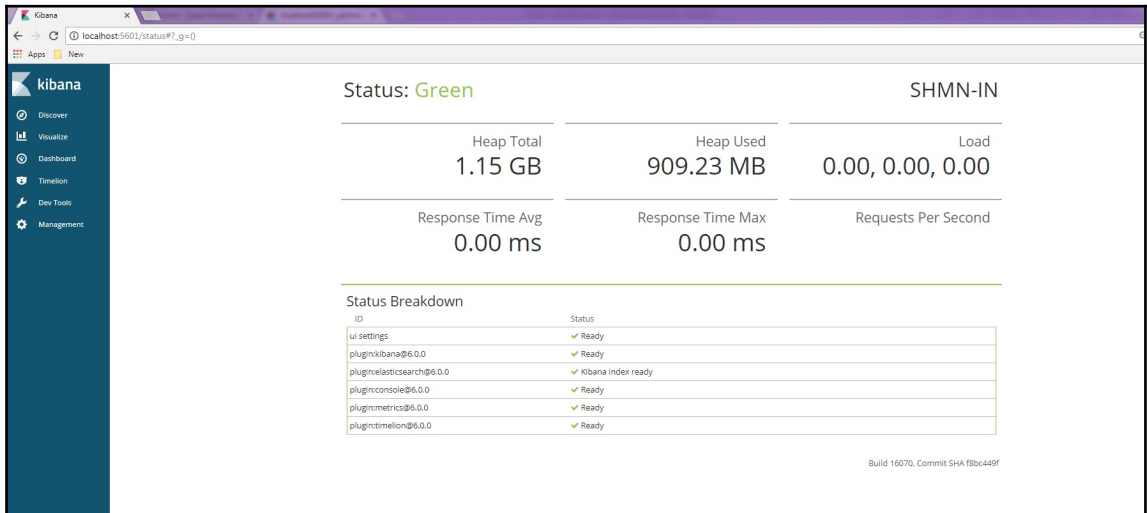
 Want to upgrade? We'll give you a hand. [Migration Guide »](#)

Version: 6.0.0

Release date: November 14, 2017

Notes: View [release notes](#).
Not the version you're looking for? View [past releases](#).

Downloads: [WINDOWS sha](#) [MAC sha](#) [LINUX 64-BIT sha](#)
[RPM 64-BIT sha](#) [DEB 64-BIT sha](#)



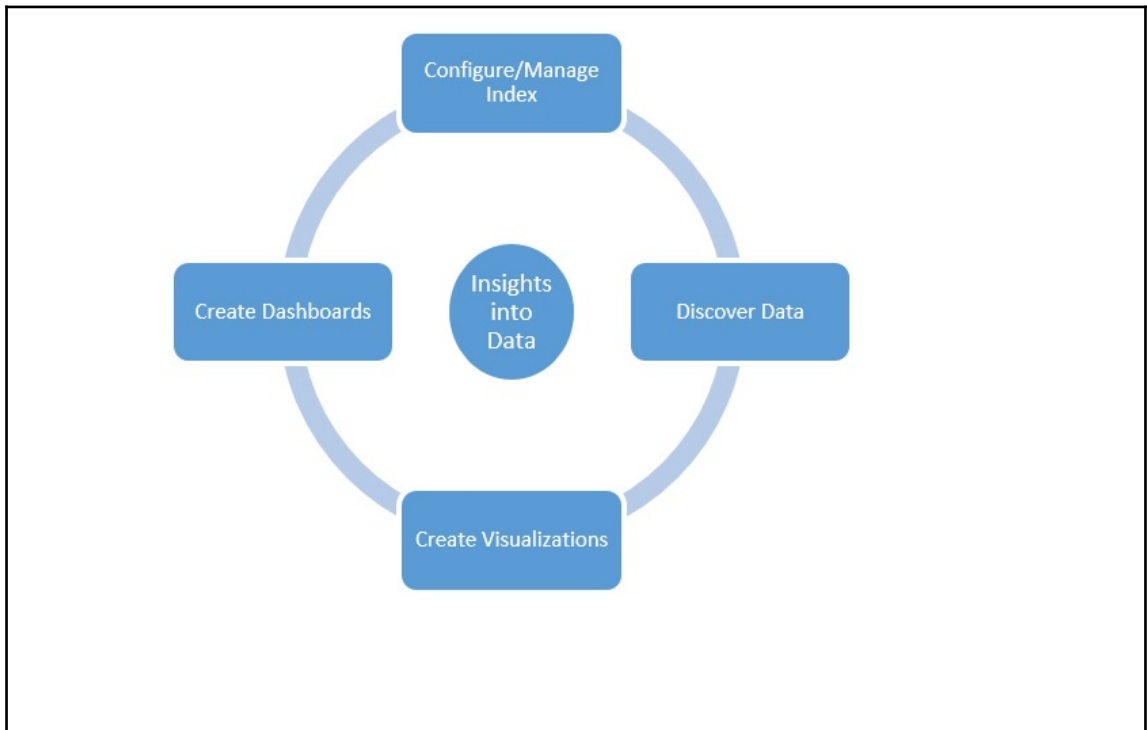
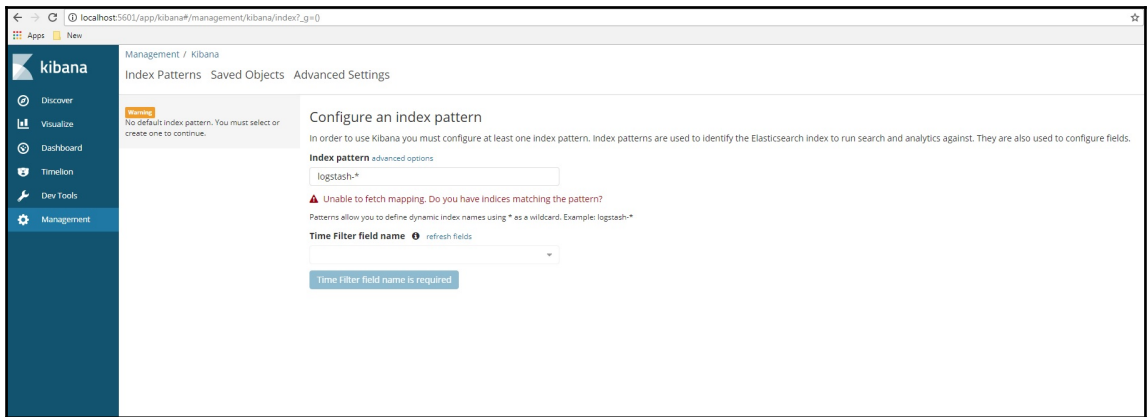
The screenshot shows the Kibana status page in a browser window. The URL is localhost:5601/status#?_g=0. The page features a dark blue sidebar with navigation options: Discover, Visualize, Dashboard, Timeline, Dev Tools, and Management. The main content area displays the following information:

- Status: Green
- SHMN-IN
- Heap Total: 1.15 GB
- Heap Used: 909.23 MB
- Load: 0.00, 0.00, 0.00
- Response Time Avg: 0.00 ms
- Response Time Max: 0.00 ms
- Requests Per Second: (empty)

Below this is a 'Status Breakdown' table:

| ID | Status |
|----------------------------|----------------------|
| ui/settings | ✓ Ready |
| plugin:kibana@6.0.0 | ✓ Ready |
| plugin:elasticsearch@6.0.0 | ✓ Kibana index ready |
| plugin:console@6.0.0 | ✓ Ready |
| plugin:metrics@6.0.0 | ✓ Ready |
| plugin:timelion@6.0.0 | ✓ Ready |

Build 16070, Commit SHA f8bc449f



Management / Kibana
 Index Patterns Saved Objects Advanced Settings
 + Create Index Pattern
 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 (50) scripted fields (0) source filters (0)

Q Filter

| name | type | format | searchable | aggregatable | excluded | controls |
|-----------------------------|---------|--------|------------|--------------|----------|----------|
| @timestamp | date | | ✓ | ✓ | | ✓ |
| @version | string | | ✓ | | | ✓ |
| _id | string | | ✓ | ✓ | | ✓ |
| _index | string | | ✓ | ✓ | | ✓ |
| _score | number | | | | | ✓ |
| _source | _source | | | | | ✓ |
| _type | string | ✓ | | ✓ | | ✓ |
| agent | string | | ✓ | | | ✓ |
| agent.keyword | string | | ✓ | ✓ | | ✓ |
| auth | string | | ✓ | | | ✓ |
| auth.keyword | string | | ✓ | ✓ | | ✓ |
| bytes | number | | ✓ | ✓ | | ✓ |
| clientip | string | | ✓ | | | ✓ |
| clientip.keyword | string | | ✓ | ✓ | | ✓ |
| geop.city_name | string | | ✓ | | | ✓ |
| geop.city_name.keyword | string | | ✓ | ✓ | | ✓ |
| geop.continent_code | string | | ✓ | | | ✓ |
| geop.continent_code.keyword | string | | ✓ | ✓ | | ✓ |
| geop.country_code2 | string | | ✓ | | | ✓ |
| geop.country_code2.keyword | string | | ✓ | ✓ | | ✓ |
| geop.country_code3 | string | | ✓ | | | ✓ |
| geop.country_code3.keyword | string | | ✓ | ✓ | | ✓ |

0 hits

New Save Open Share Auto-refresh Last 15 minutes

Time Range

From 2014-05-28 00:00:00.000 To 2014-07-01 00:00:00.000

May 2014 July 2014

04 05 06 07 08 09 10 06 07 08 09 10 11 12
 11 12 13 14 15 16 17 13 14 15 16 17 18 19
 18 19 20 21 22 23 24 20 21 22 23 24 25 26
 25 26 27 28 29 30 31 27 28 29 30 31

Go

Search... (e.g. status:200 AND extension:PHP)

Add a filter

logstash-*

Selected Fields
 _source

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 are some ideas:

Expand your time range

Kibana interface showing a logstash-* dashboard. The search bar contains the query: `Search... (e.g. status:200 AND extension:PHP)`. The dashboard displays a bar chart of log events over time from May 28th 2014 to July 1st 2014. A red number '6' is shown on the chart.

Selected Fields: `@timestamp`, `_id`, `_score`, `_type`, `_source`, `agent`, `auth`, `bytes`, `clientip`, `geop_city_name`, `geop_country_code`, `geop_country_name`, `geop_dma_code`, `geop_ip`, `geop_latitude`, `geop_location`, `geop_longitude`, `geop_postal_code`, `geop_region_code`, `geop_region_name`, `request`, `response`, `status`, `type`.

Logstash-* configuration (numbered 1-4):

- Input: `logstash-*`
- Filter: `geoip`
- Output: `elasticsearch`
- Filter: `geoip`

Logstash-* configuration (numbered 5-8):

- Input: `logstash-*`
- Filter: `geoip`
- Output: `elasticsearch`
- Filter: `geoip`

Logstash-* configuration (numbered 9-12):

- Input: `logstash-*`
- Filter: `geoip`
- Output: `elasticsearch`
- Filter: `geoip`

Logstash-* configuration (numbered 13-16):

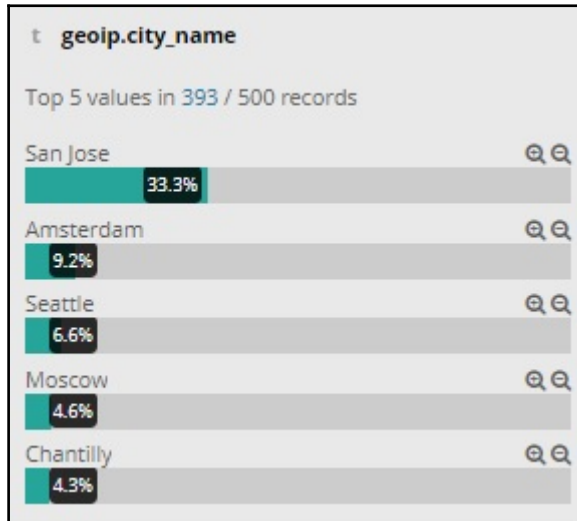
- Input: `logstash-*`
- Filter: `geoip`
- Output: `elasticsearch`
- Filter: `geoip`

Logstash-* configuration (numbered 17-20):

- Input: `logstash-*`
- Filter: `geoip`
- Output: `elasticsearch`
- Filter: `geoip`

Logstash-* configuration (numbered 21-24):

- Input: `logstash-*`
- Filter: `geoip`
- Output: `elasticsearch`
- Filter: `geoip`



Time ▾ _source

Expand Button
 June 27th 2014, 17:43:20.000 request: /scripts/netcat-webserver agent: "Mozilla/5.0 (compatible; EasouSpider; +http://www.easou.com/search/spider.html)" geoi...
 geoiptimezone: Asia/Shanghai geoiip: 183.60.215.50 geoilatitude: 23.117 geoi.country_name: China geoi.country_code2: CN geoi.c...
 geoi.country_code3: CN geoi.region_name: Guangdong geoi.location: { "lon": 113.25, "lat": 23.1167 } geoi.region_code: 44 geoi.long...
 ident: - verb: GET useragent.os: Other useragent.build: useragent.name: EasouSpider useragent.os_name: Other useragent.device: Spider...
 - - [27/Jun/2014:08:00:00 -0400] "GET /scripts/netcat-webserver HTTP/1.1" 200 182 "-" "Mozilla/5.0 (compatible; EasouSpider; +http://

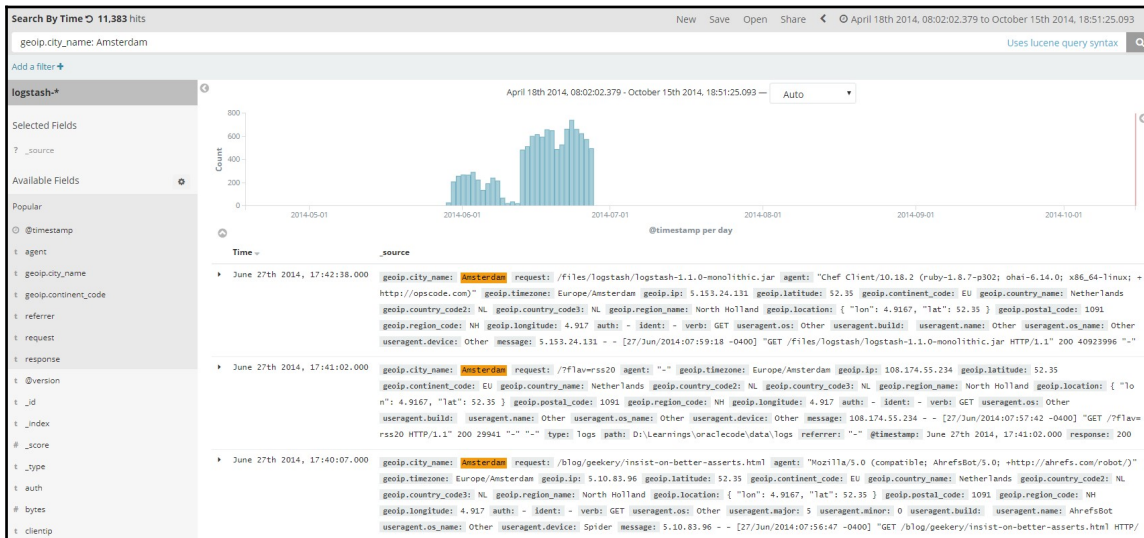
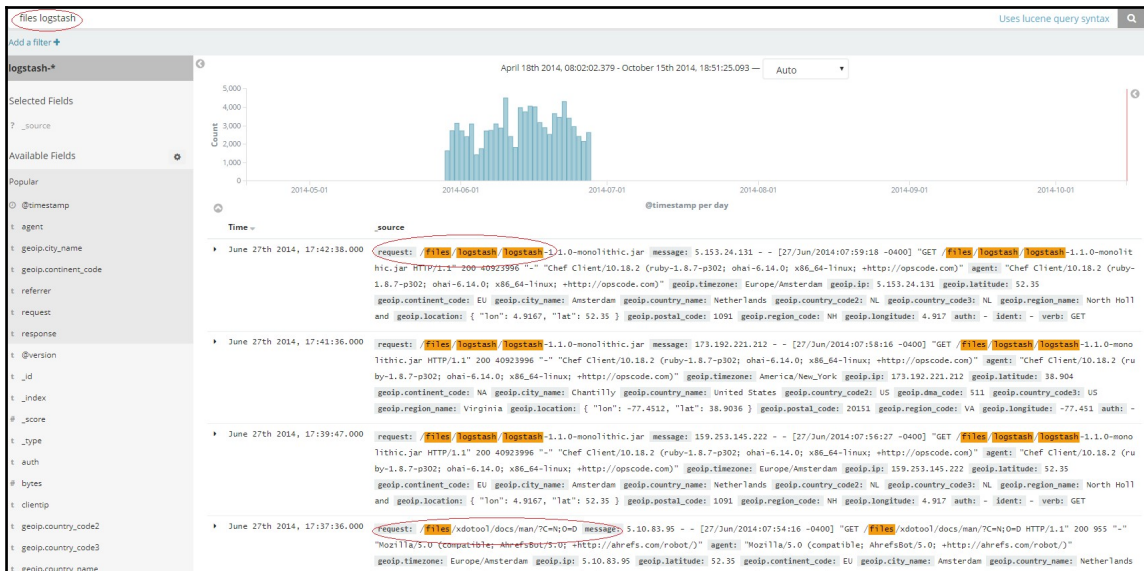
Table JSON [View surrounding data](#)

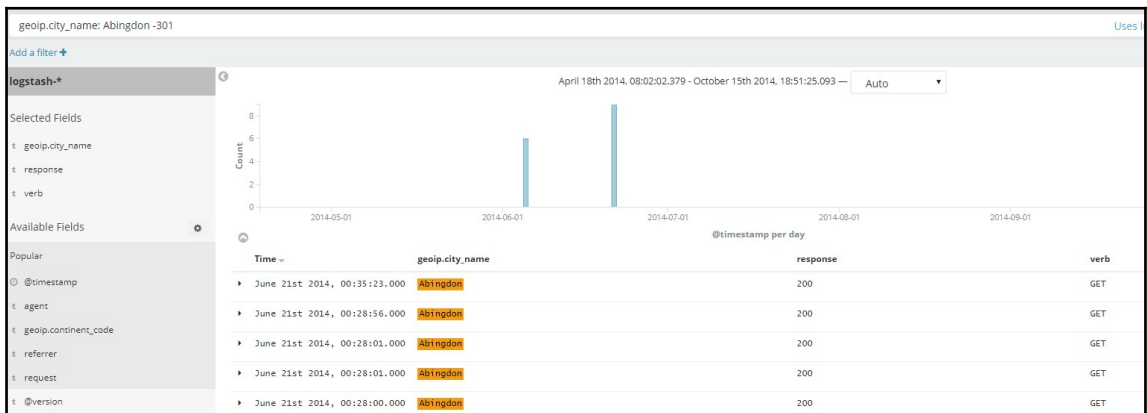
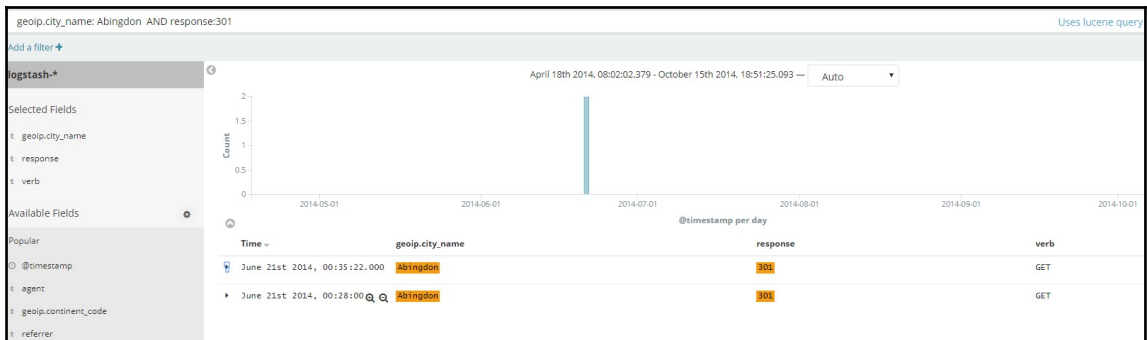
| | |
|---------------------|---|
| @timestamp | June 27th 2014, 17:43:20.000 |
| @version | 1 |
| _id | AV4jH1xYxVeTbjX4rA1W |
| _index | logstash-2014.06.27 |
| _score | - |
| _type | logs |
| agent | "Mozilla/5.0 (compatible; EasouSpider; +http://www.easou.com/search/spider.html)" |
| auth | - |
| # bytes | 182 |
| clientip | 183.60.215.50 |
| geoi.city_name | Guangzhou |
| geoi.continent_code | AS |
| geoi.country_code2 | CN |

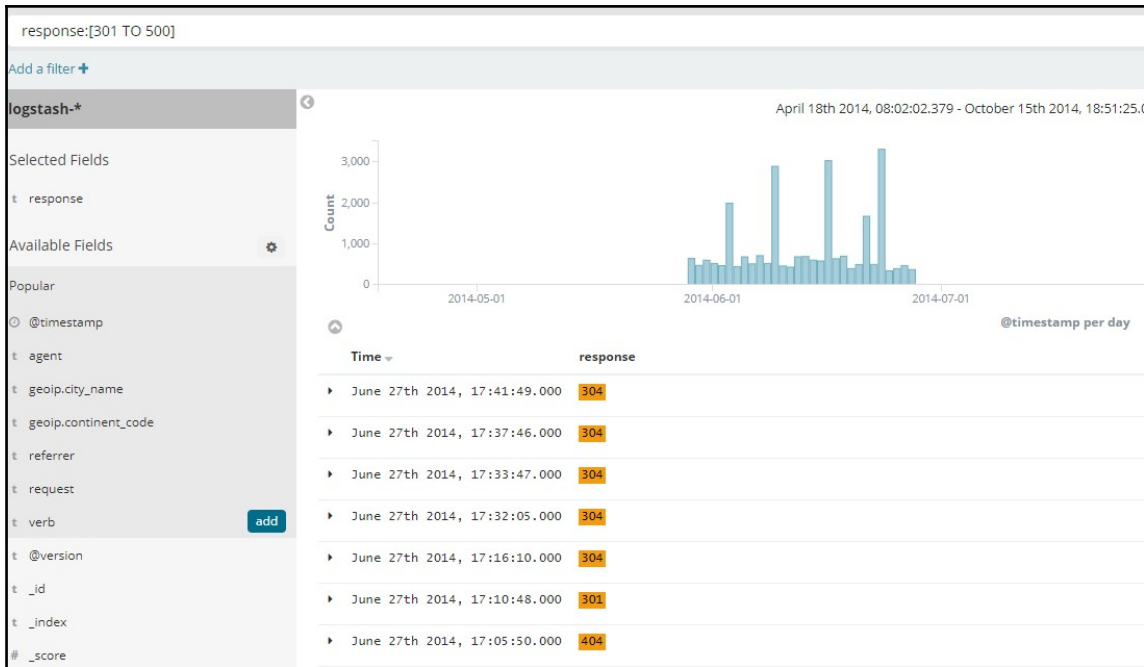
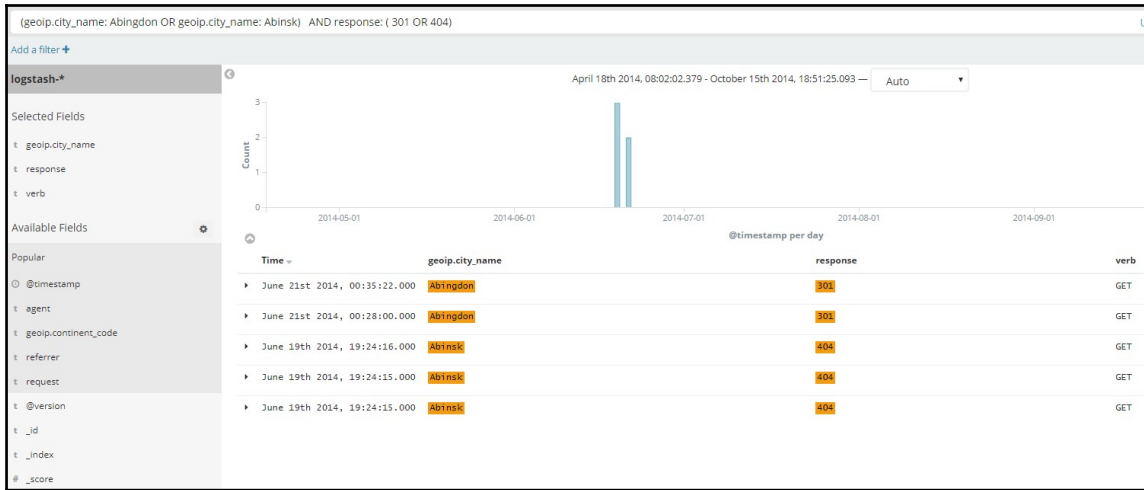
t geoi.country_name China

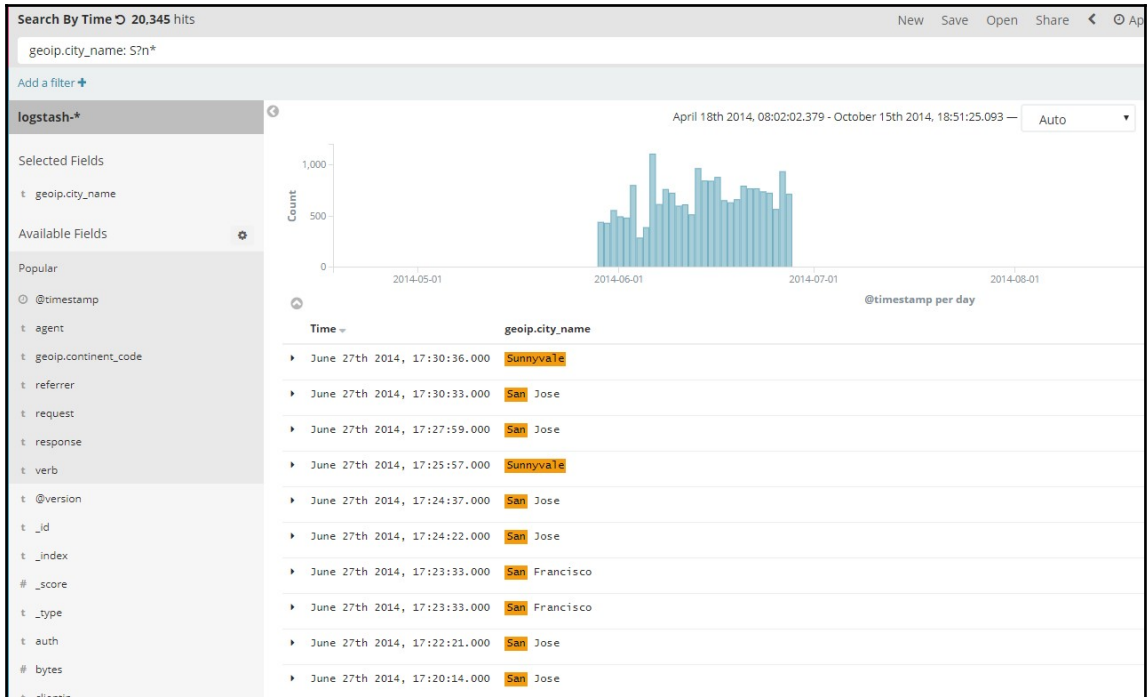
geoi.ip **Toggle column in table**

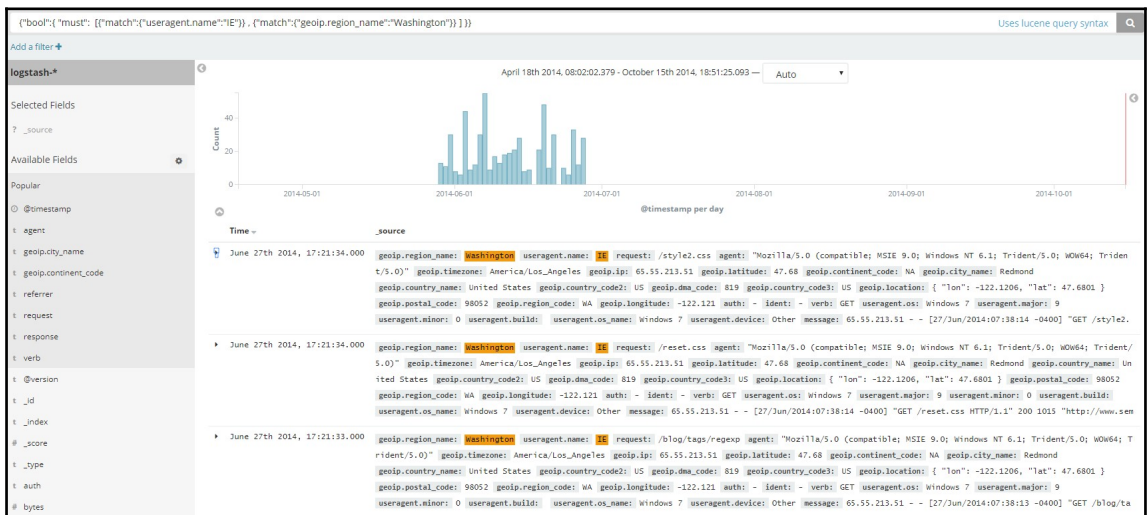
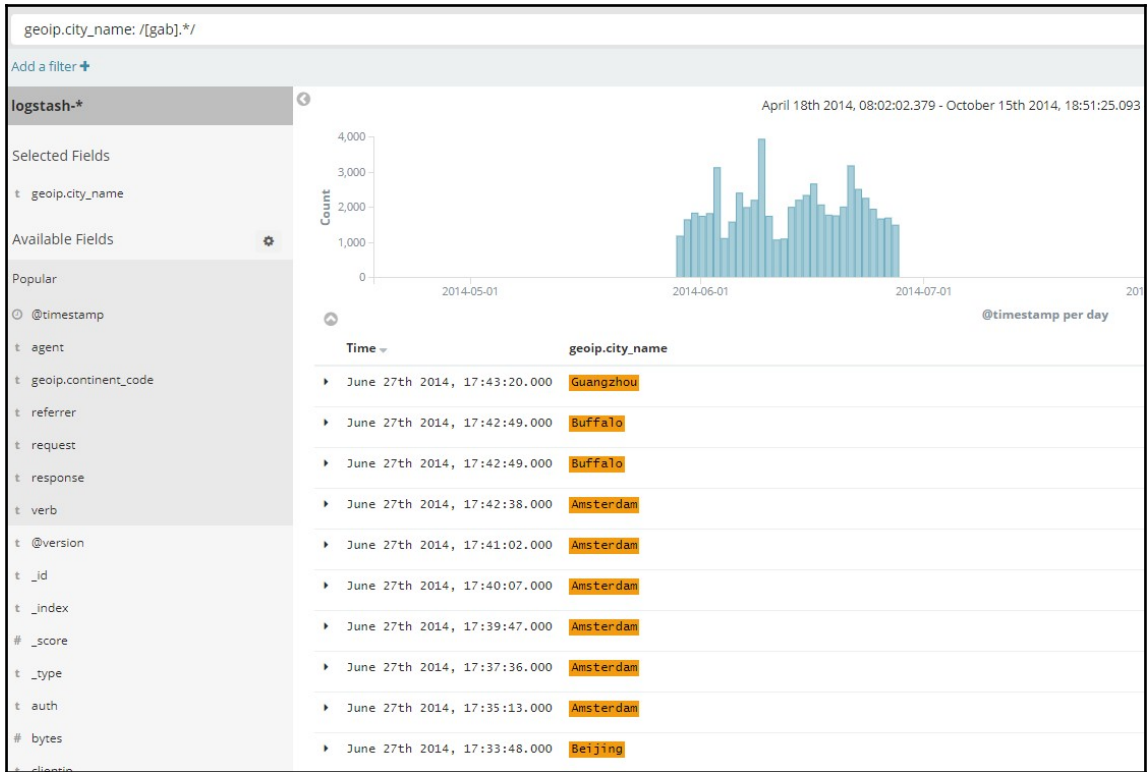
| Time ▾ | geoi.city_name | response | request ✕ << |
|------------------------------|----------------|----------|--|
| June 27th 2014, 17:43:20.000 | Guangzhou | 200 | server |
| June 27th 2014, 17:42:49.000 | Buffalo | 200 | /blog/geekery/solving-good-or-bad-problems.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Fe |
| June 27th 2014, 17:42:49.000 | Buffalo | 200 | /blog/geekery/disabling-battery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Fe |
| June 27th 2014, 17:42:39.000 | - | 200 | /style2.css |
| June 27th 2014, 17:42:38.000 | Amsterdam | 200 | /files/logstash/logstash-1.1.0-monolithic.jar |
| June 27th 2014, 17:42:37.000 | - | 200 | /images/jordan-80.png |
| June 27th 2014, 17:42:35.000 | - | 200 | /reset.css |
| June 27th 2014, 17:42:30.000 | - | 200 | /blog/tags/X11 |
| June 27th 2014, 17:42:12.000 | - | 200 | /images/googledotcom.png |

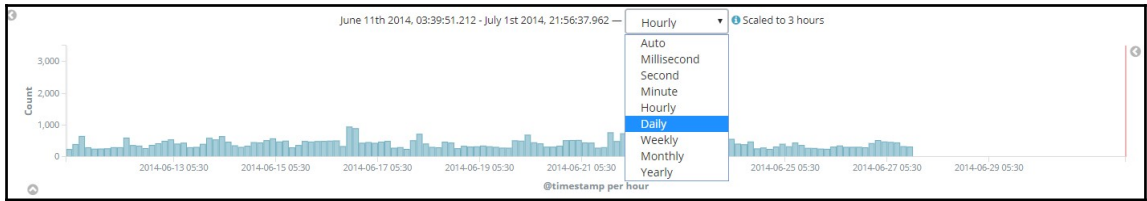












Response_200 18 hits

Save Search

Response_200_Graz

Save as a new search

Save

response:200 AND geoip.city_name:Graz

Search By Time 1 hit

Open Search

Q saved Searches Filter...

Name

Response_200

Search By Time

Response_200 172.688 hits

Share saved search

You can share this URL with people to let them load the most recent saved version of this search.

Link [http://localhost:5601/app/kibana#/discover/d16c7a20-8c02-11e7-8ac5-c321b749bc477_g=\(filters%3A\)%2CrefreshInterval](http://localhost:5601/app/kibana#/discover/d16c7a20-8c02-11e7-8ac5-c321b749bc477_g=(filters%3A)%2CrefreshInterval)

Share Snapshot

Snapshot URLs encode the current state of the search in the URL itself. Edits to the saved search won't be visible via this URL.

Link [http://localhost:5601/app/kibana#/discover/d16c7a20-8c02-11e7-8ac5-c321b749bc477_g=\(filters%3A\)%2CrefreshInterval?displa](http://localhost:5601/app/kibana#/discover/d16c7a20-8c02-11e7-8ac5-c321b749bc477_g=(filters%3A)%2CrefreshInterval?displa)

We recommend sharing shortened snapshot URLs for maximum compatibility. Internet Explorer has URL length restrictions, and some wiki and markup parsers don't do well with the full-length version of the snapshot URL, but the short URL should work great.

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

Time Range Quick **Relative** Absolute [⌵]

From Set To Now **To** Set To Now

December 15th 2013, 12:28:47.432 December 15th 2014, 12:28:47.432

Years ago Years ago

round to the year round to the year

Go

Time Range Quick Relative **Absolute** [⌵]

From Set To Now **To** Set To Now

YYYY-MM-DD HH:mm:ss.SSS YYYY-MM-DD HH:mm:ss.SSS

< **May 2014** > < **July 2014** >

| Sun | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|-----|-----|-----|-----------|-----|-----|-----|-----|-----|-----------|-----|-----|-----|-----|
| | | | | 01 | 02 | 03 | | | 01 | 02 | 03 | 04 | 05 |
| 04 | 05 | 06 | 07 | 08 | 09 | 10 | 06 | 07 | 08 | 09 | 10 | 11 | 12 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 27 | 28 | 29 | 30 | 31 | | |

Go

Response_200 [⌵] 34,474 hits New Save Open Share Auto-refresh

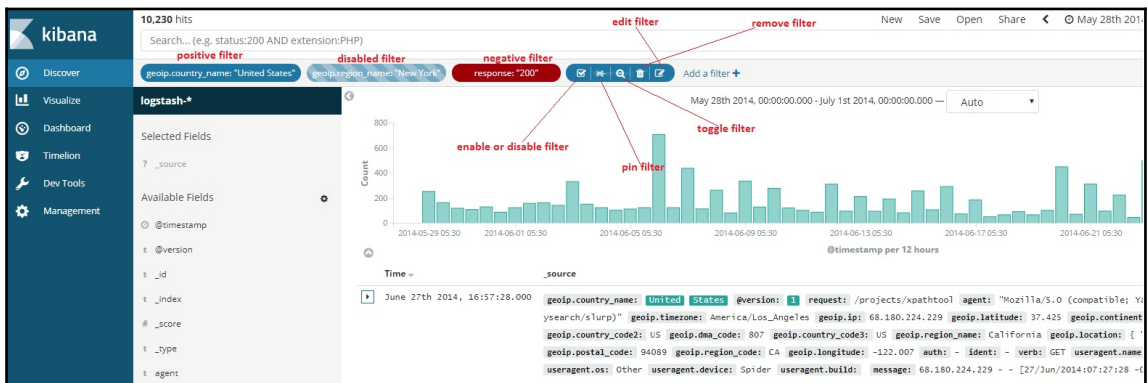
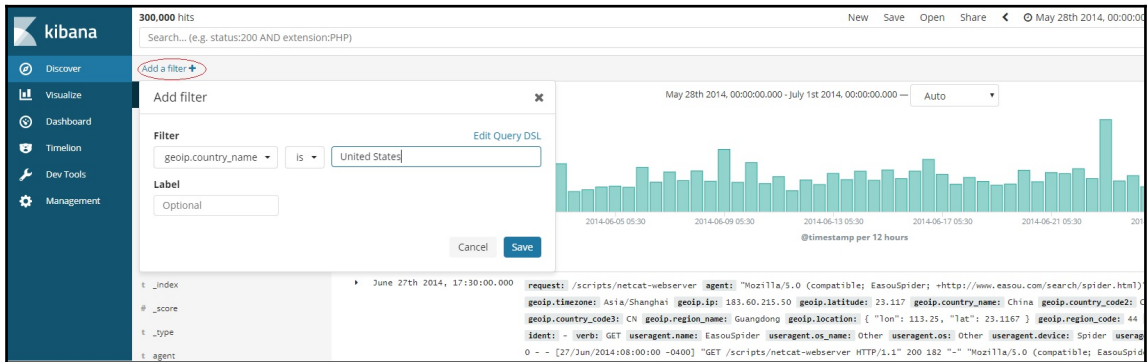
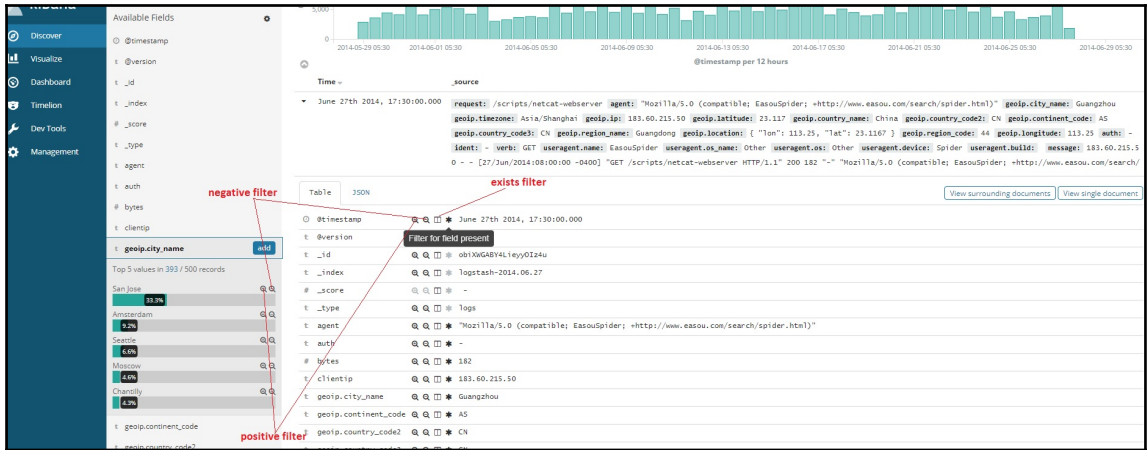
Refresh Interval

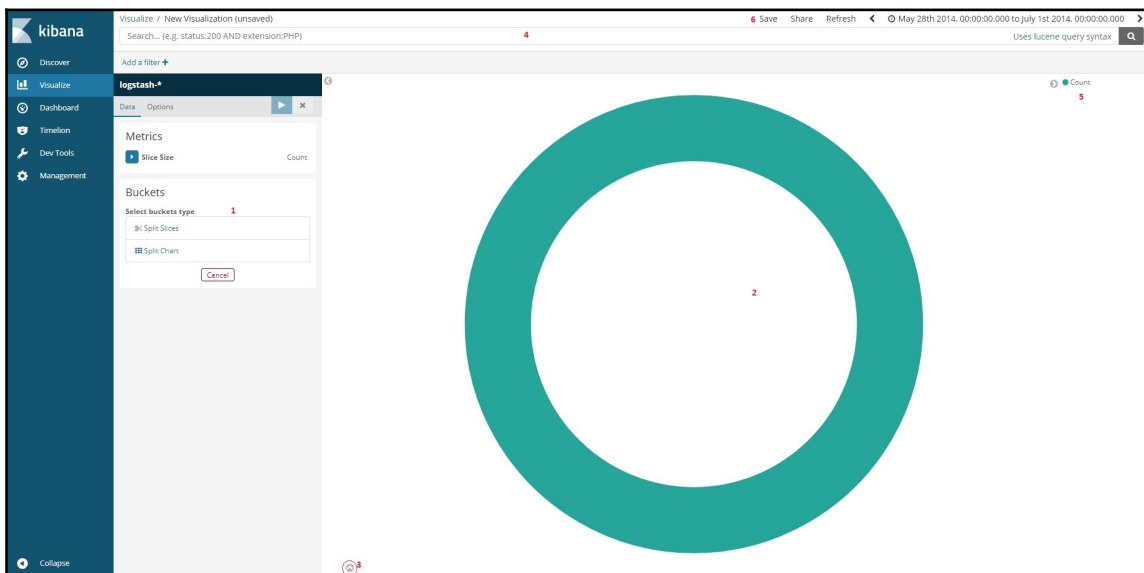
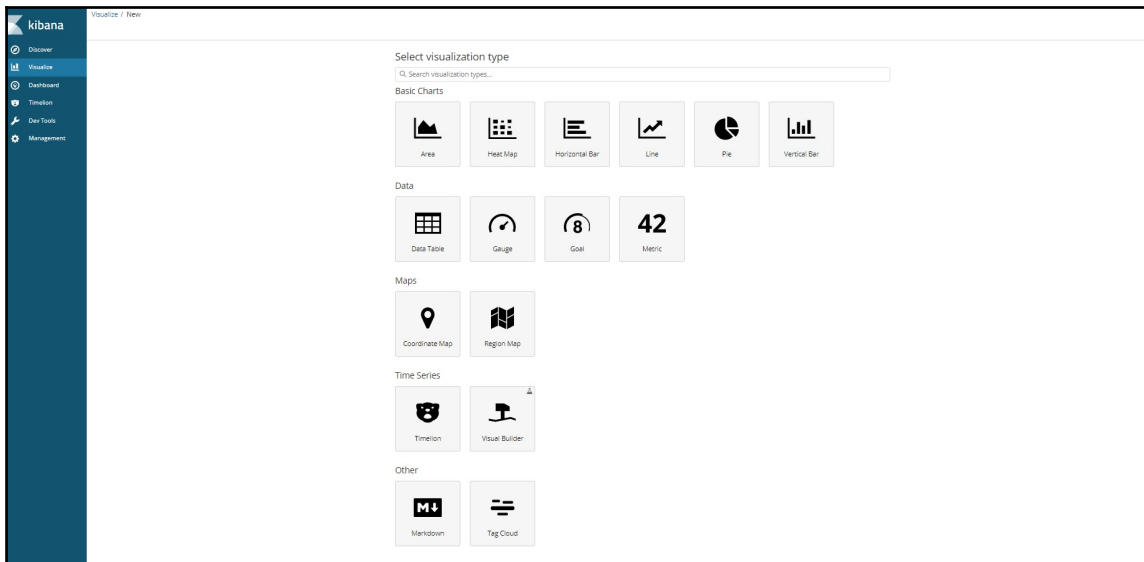
Off 5 seconds 1 minute 1 hour

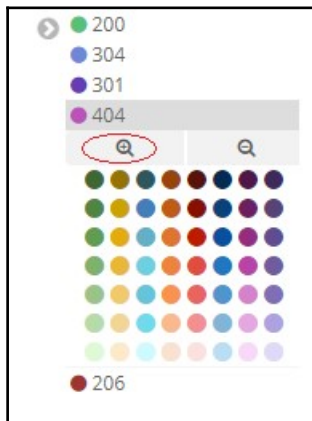
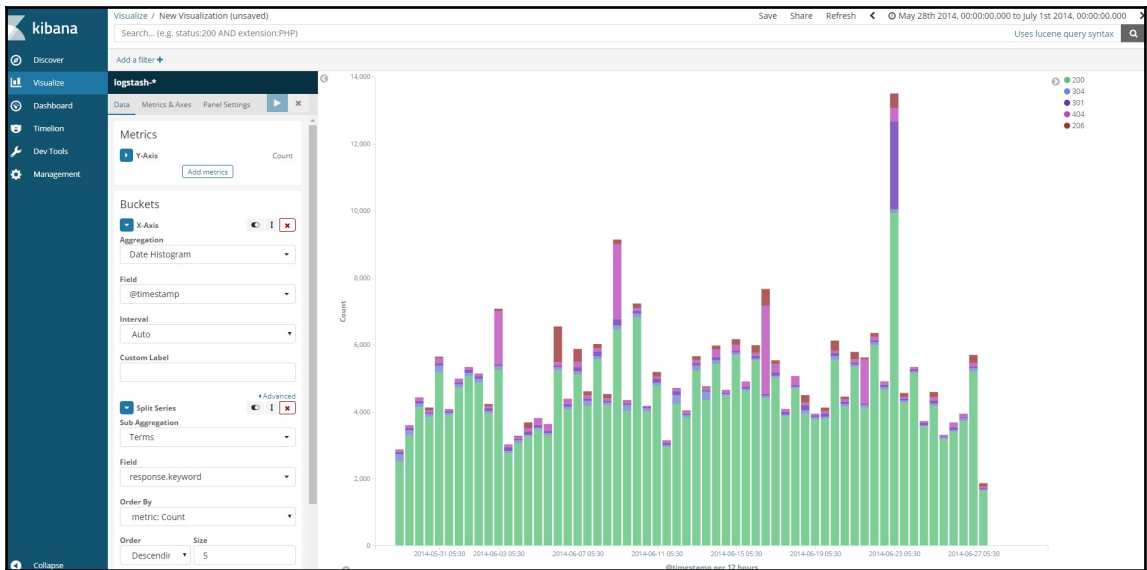
10 seconds 5 minutes 2 hour

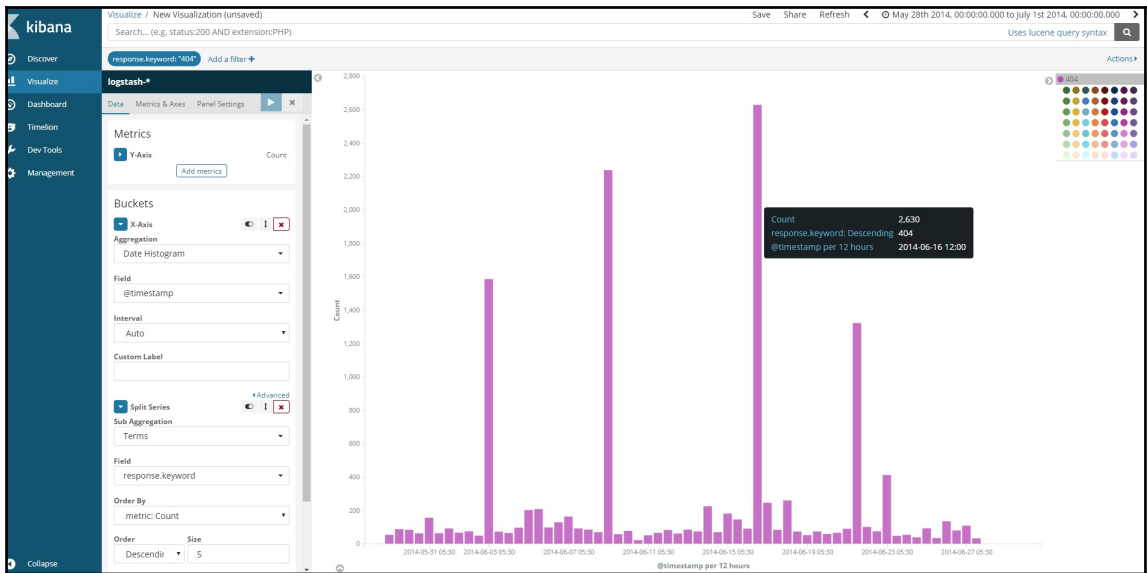
30 seconds 15 minutes 12 hour

45 seconds 30 minutes 1 day



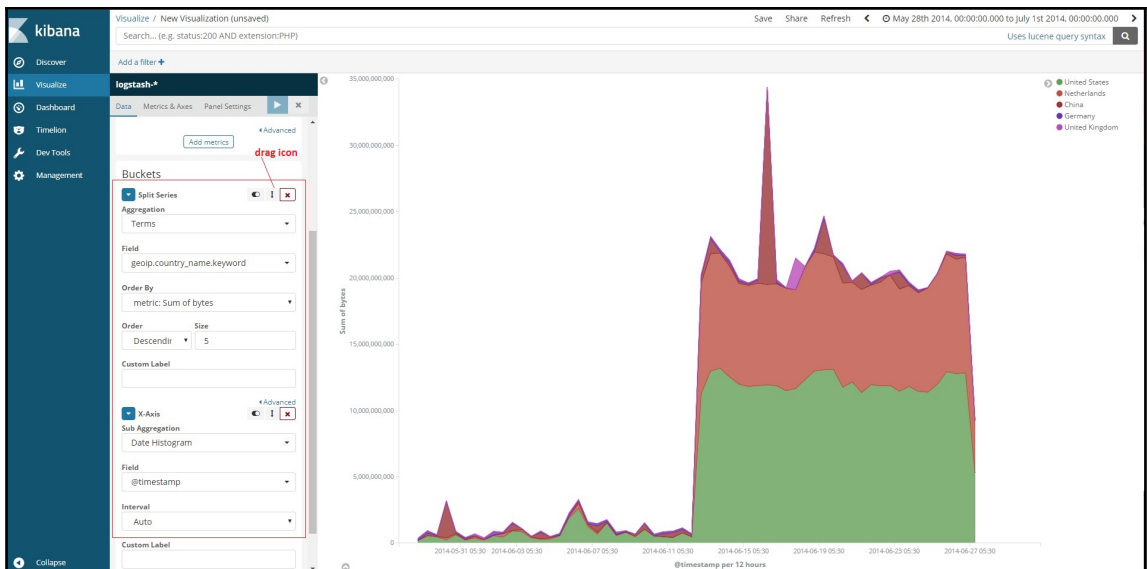
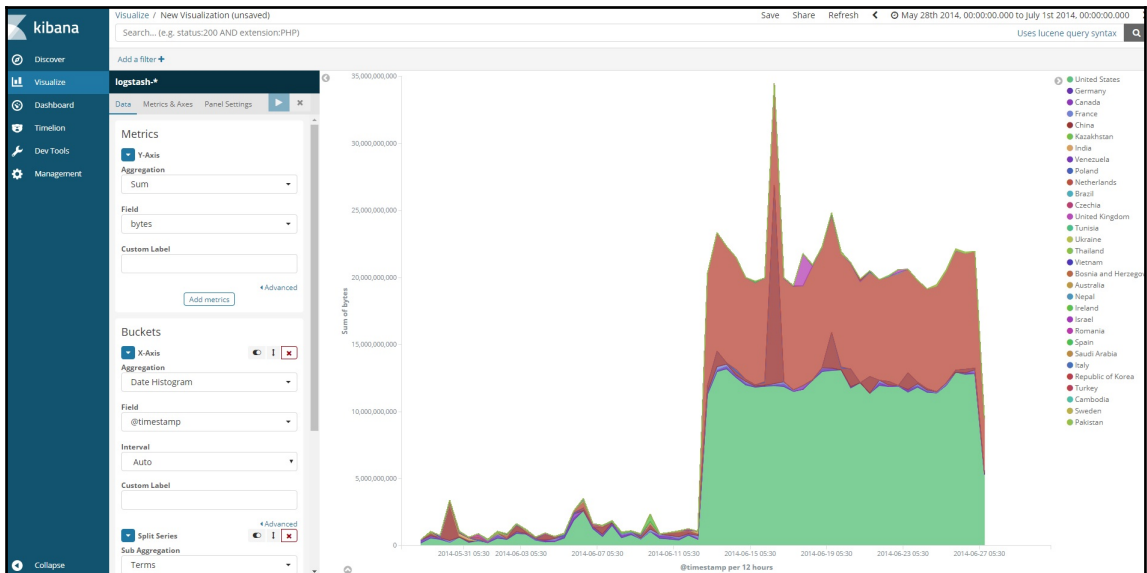


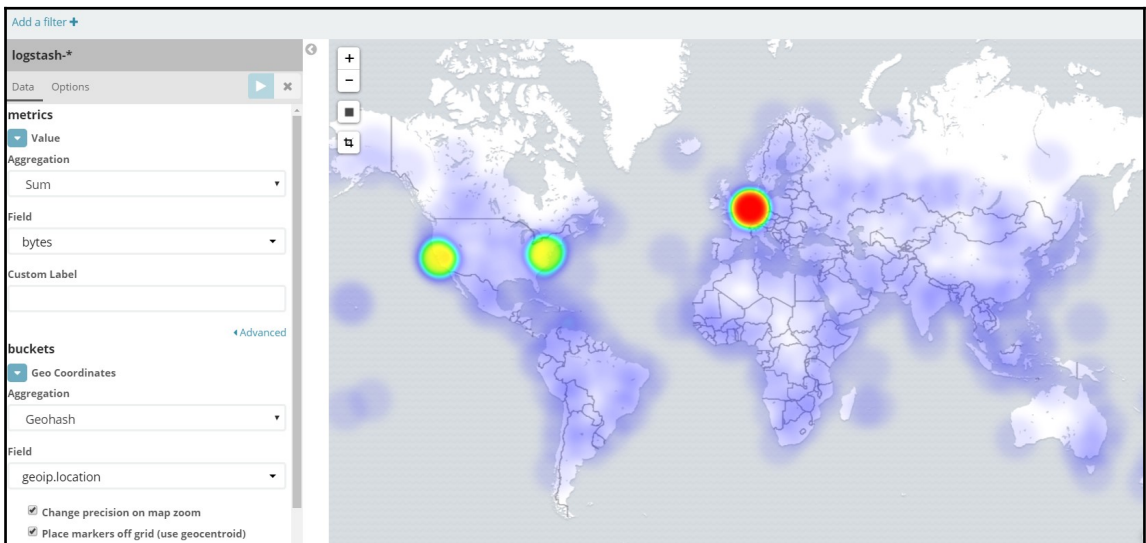
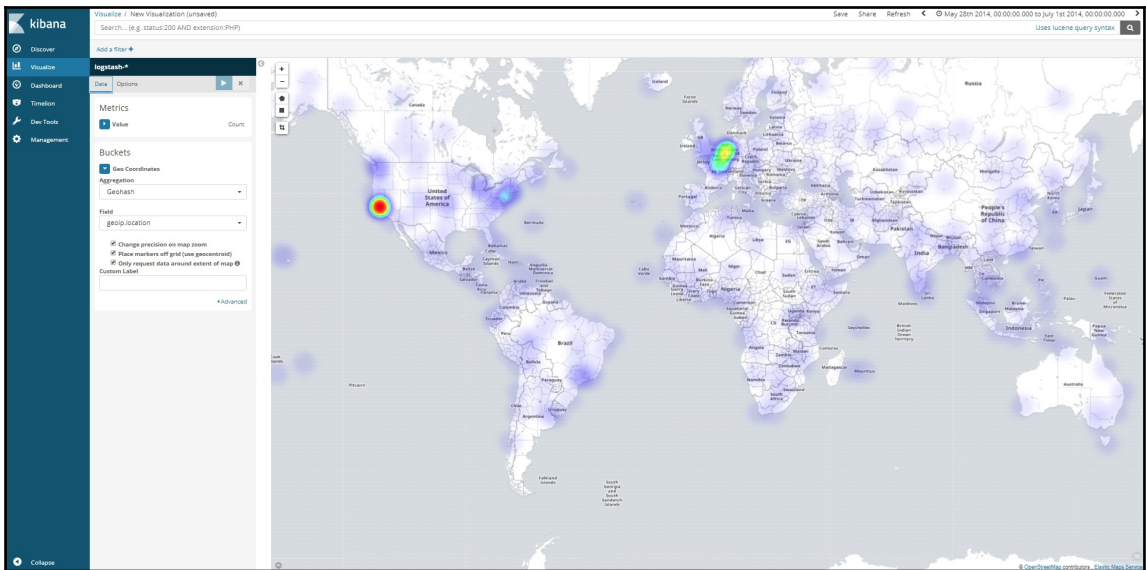


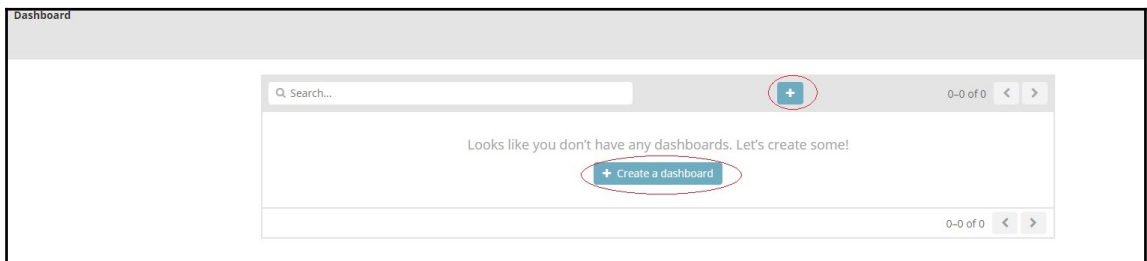
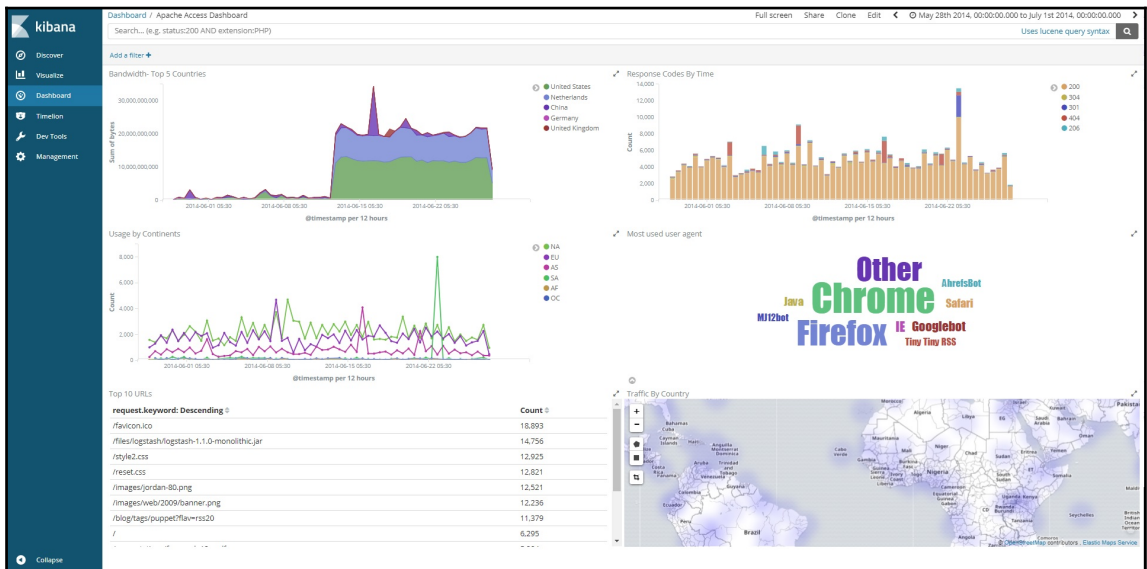
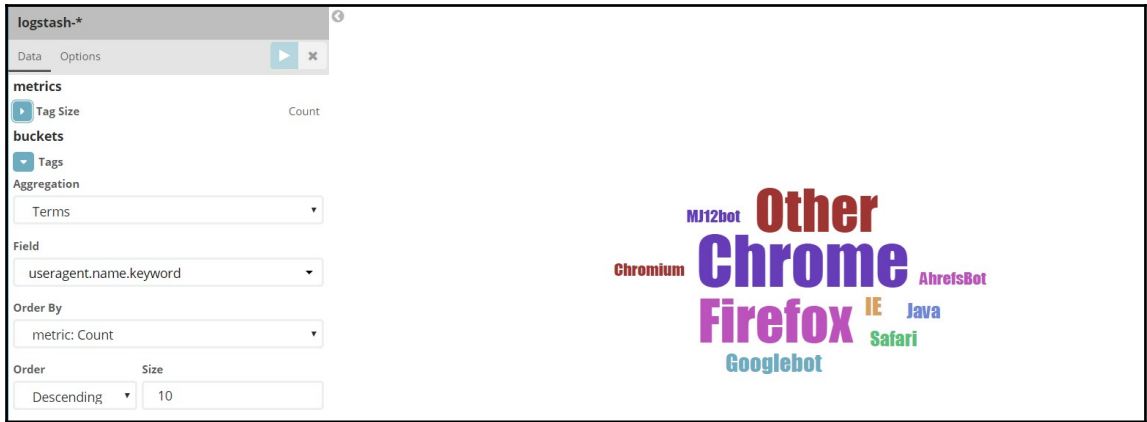


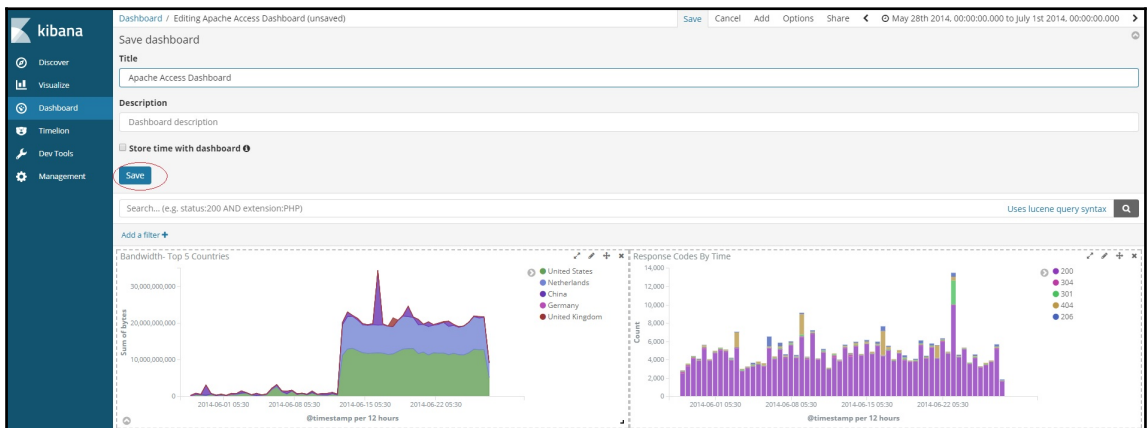
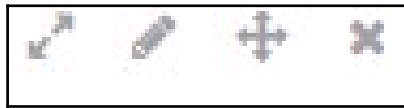
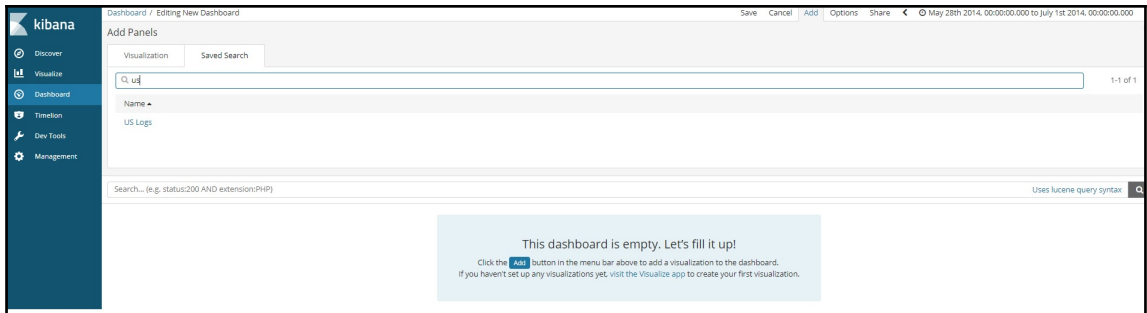
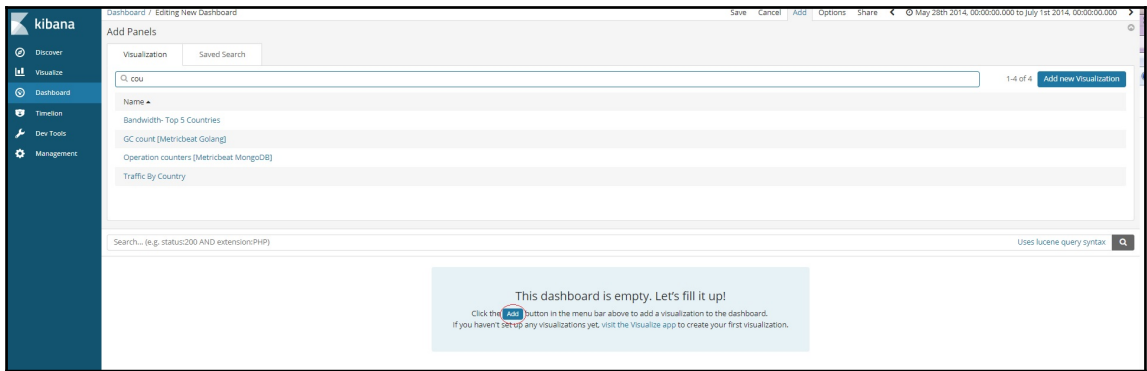
| logstash-* | Urls | Total Requests |
|------------|---|----------------|
| | /favicon.ico | 18,893 |
| | /files/logstash/logstash-1.1.0-monolithic.jar | 14,752 |
| | /style2.css | 12,925 |
| | /reset.css | 12,821 |
| | /images/jordan-80.png | 12,521 |
| | /images/web/2009/banner.png | 12,236 |
| | /blog/tags/puppetflav-rss20 | 11,379 |
| | / | 6,295 |
| | /presentations/fpm-scale12x.pdf | 5,268 |
| | /flav-rss20 | 5,103 |

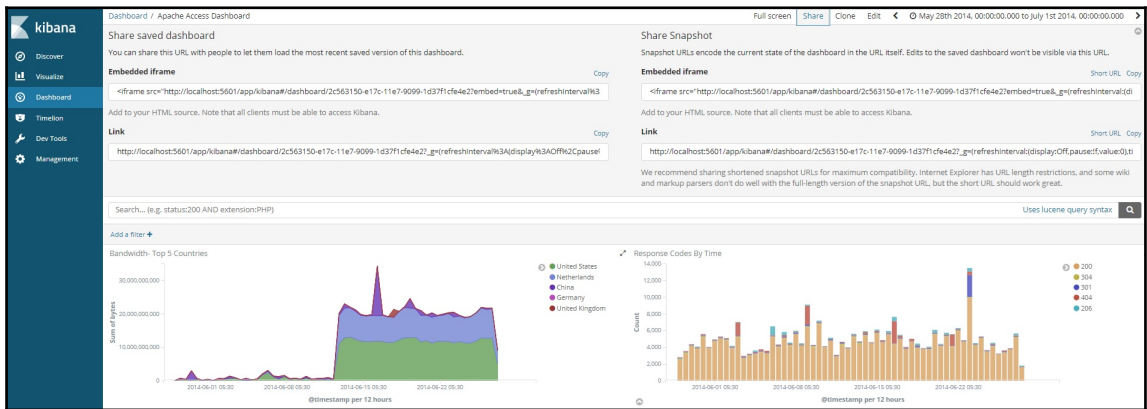
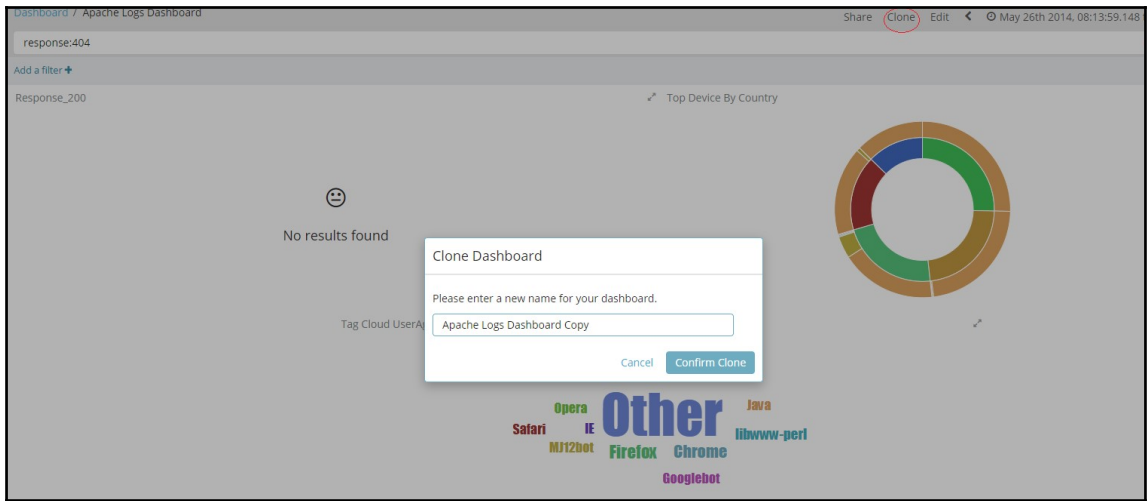
Export: [Raw](#) [Formatted](#)





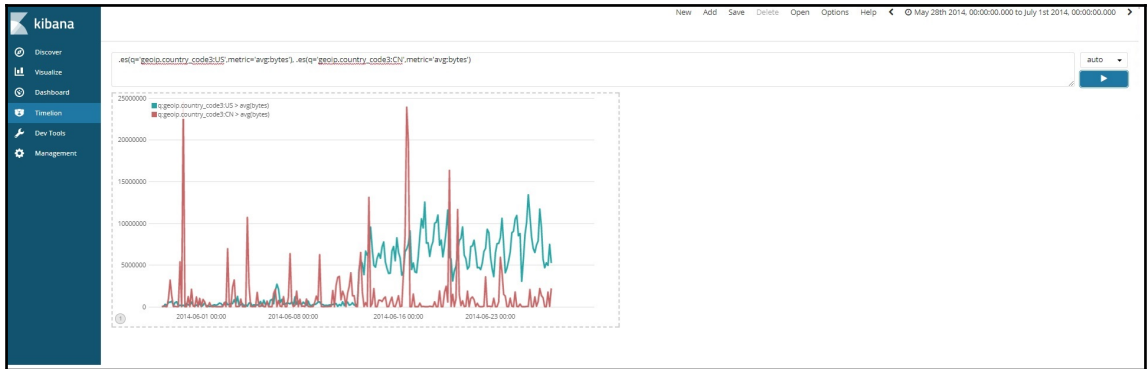
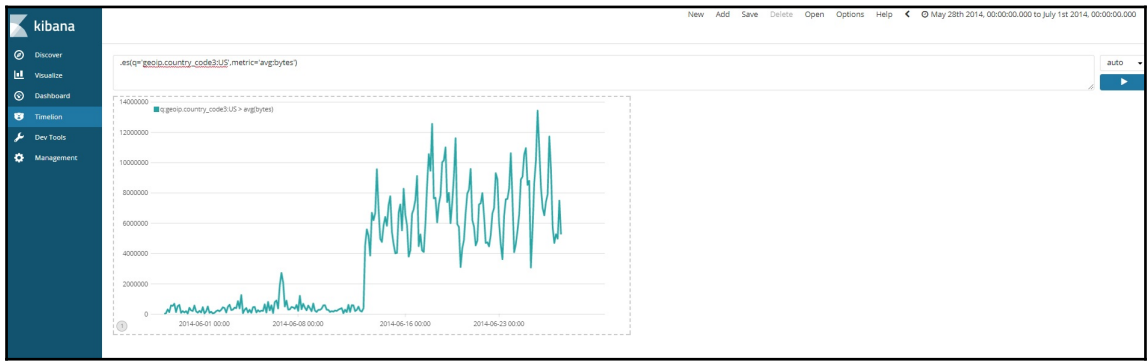


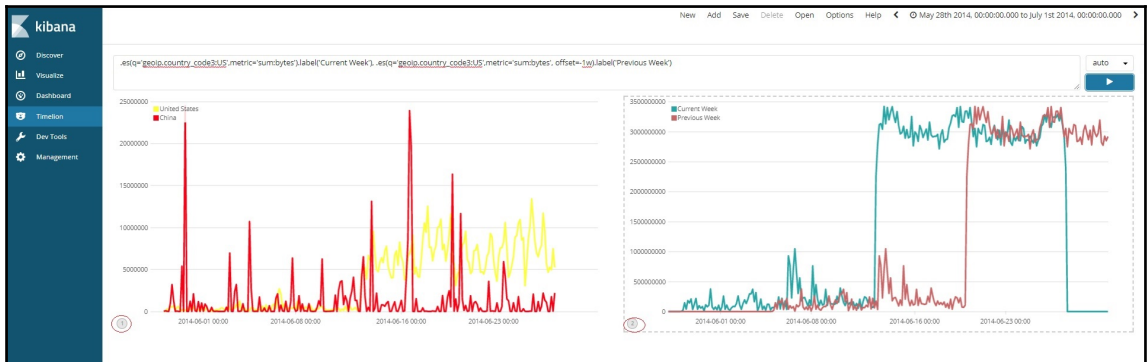




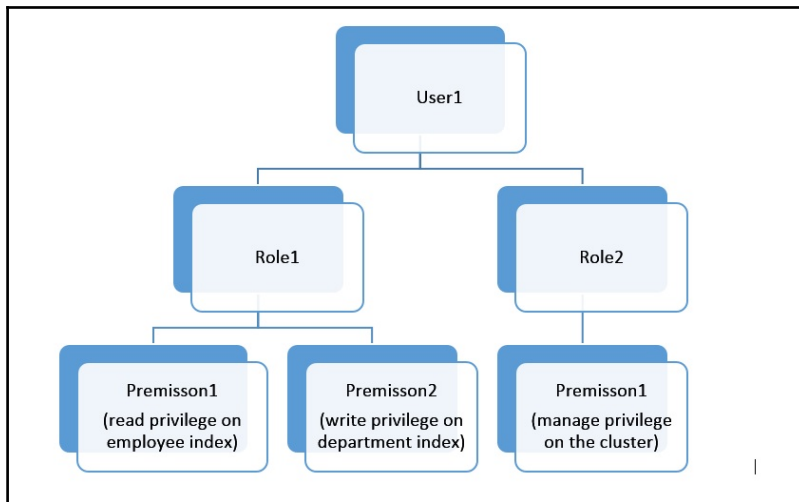
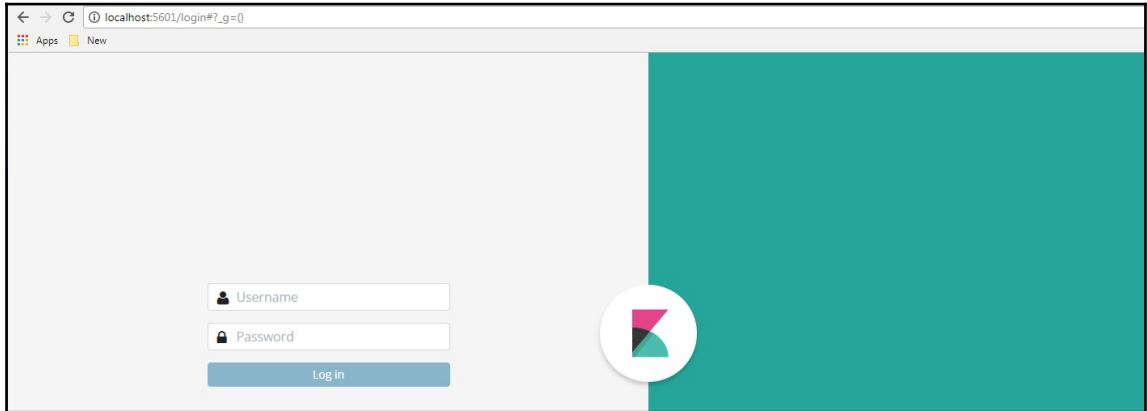
This screenshot shows the Kibana interface with a sidebar on the left containing navigation options: Discover, Visualize, Dashboard, Timeline, Dev Tools, and Management. The main content area displays a list of visualization functions:

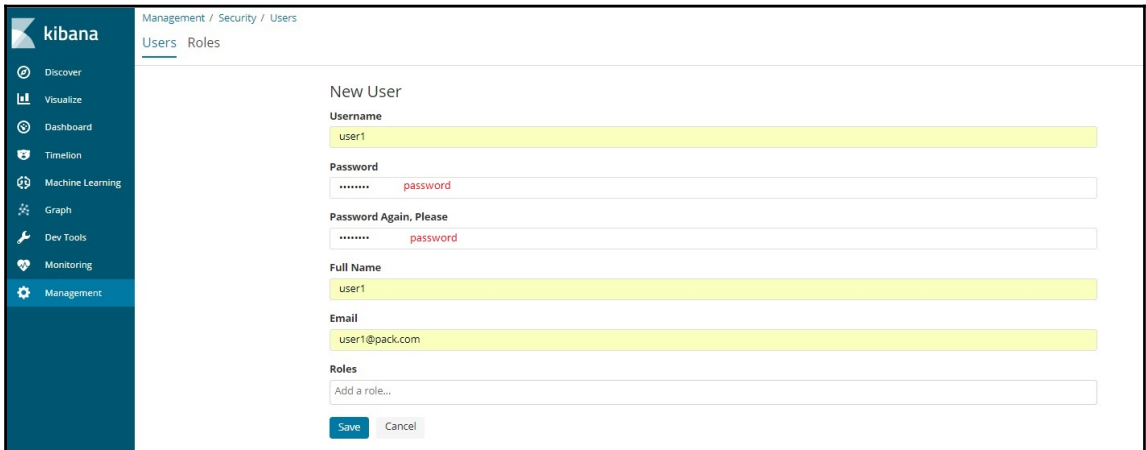
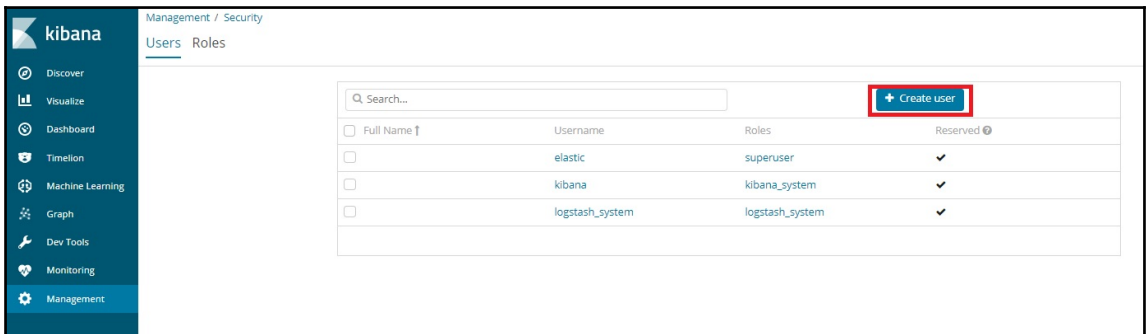
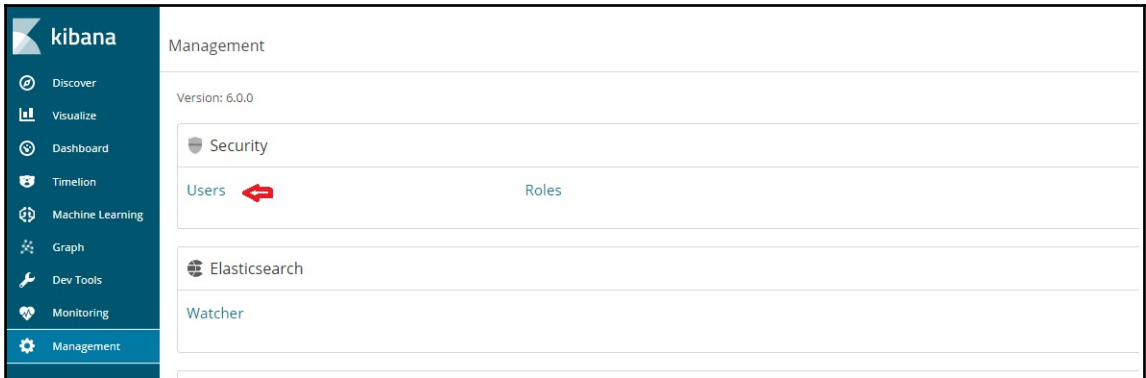
- .abs()** Return the absolute value of each value in the series list (Chainable)
- .add()** Adds the values of one or more series in a seriesList to each position, in each series, of the input seriesList (Chainable)
Arguments: term=seriesList / number
- .aggregate()** Creates a static line based on result of processing all points in the series. Available functions: avg, cardinality, min, max, last, first, sum (Chainable)
Arguments: function=(string)
- .bars()** Show the seriesList as bars (Chainable)
Arguments: width=(number / null), stack=(boolean / null)
- .color()** Change the color of the series (Chainable)
Arguments: color=(string)

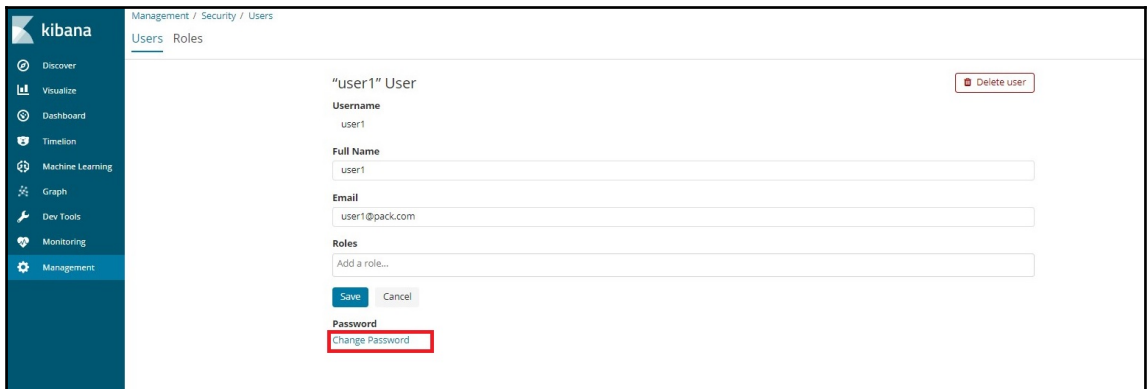
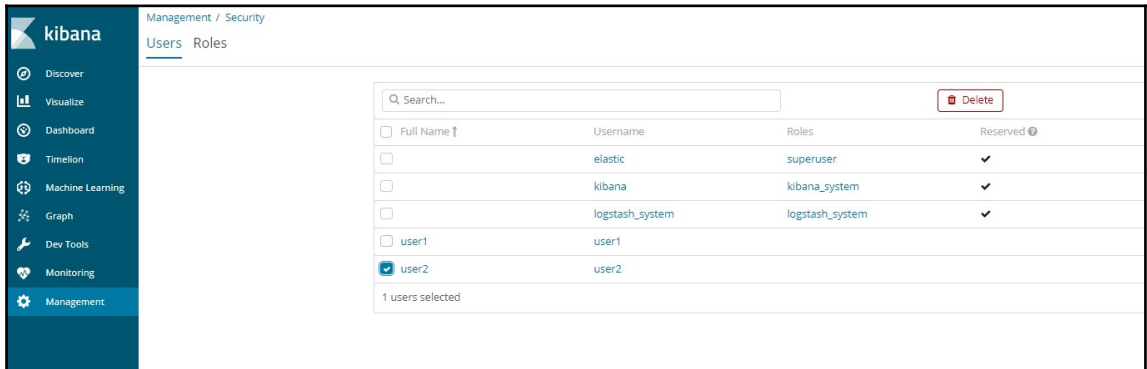
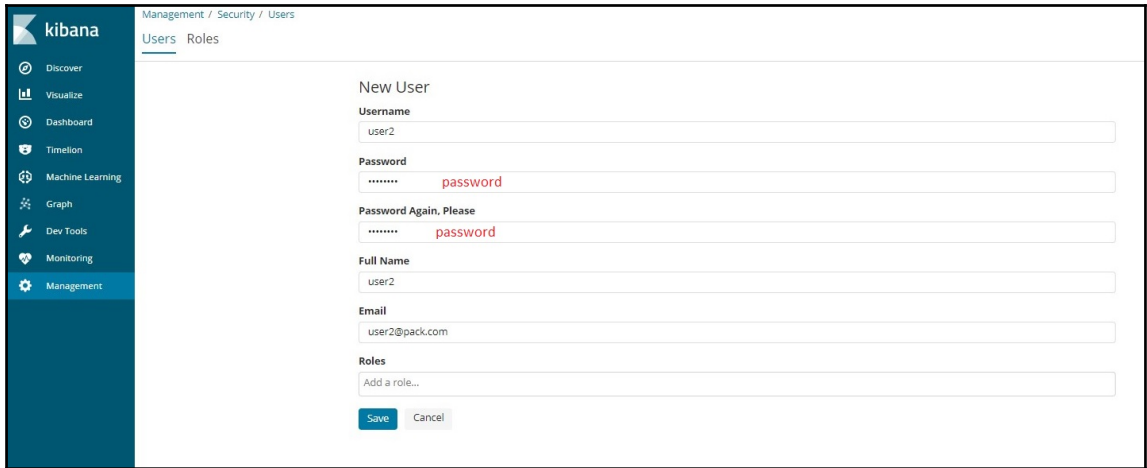


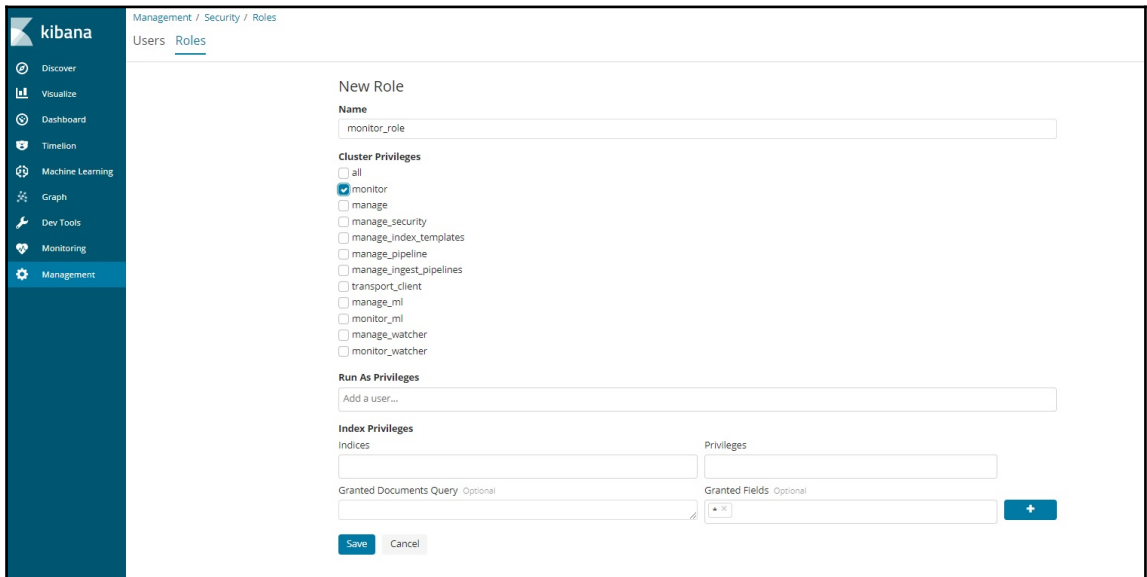
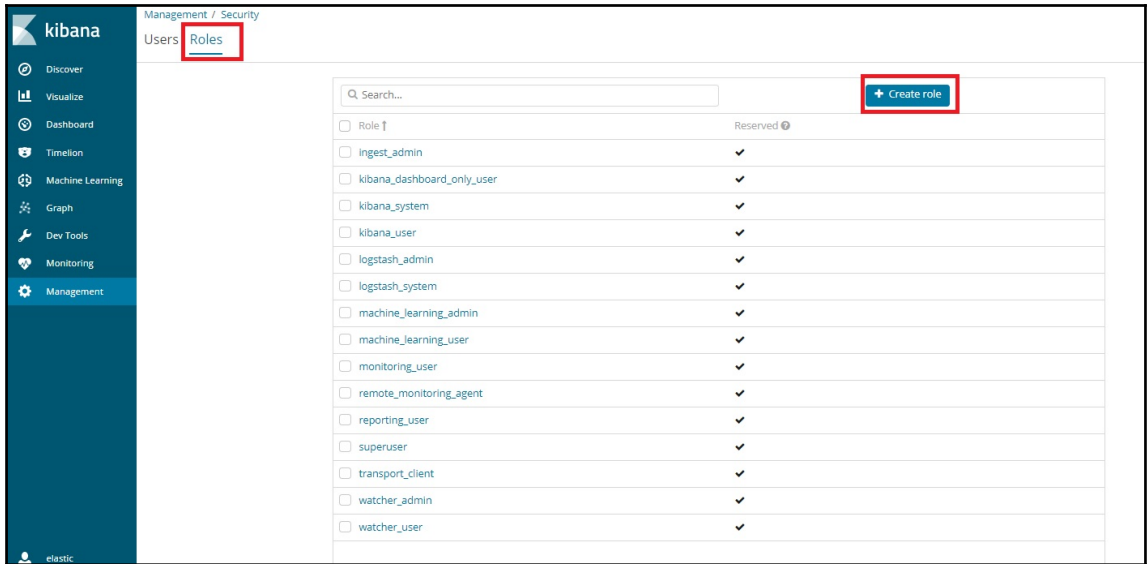


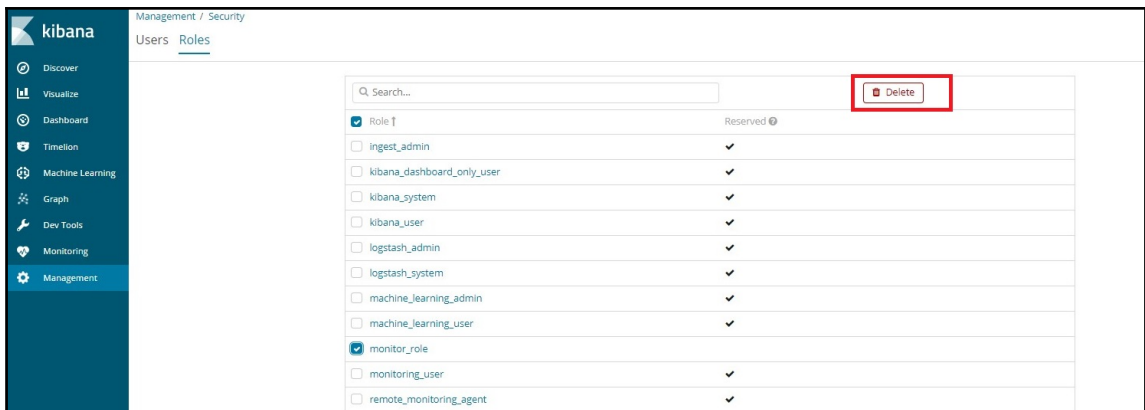
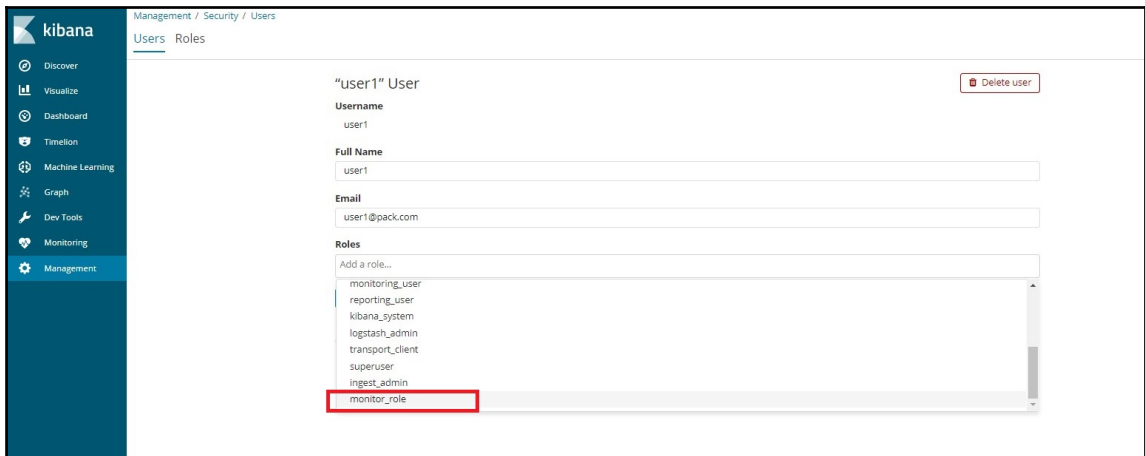
Chapter 8: Elastic X-Pack

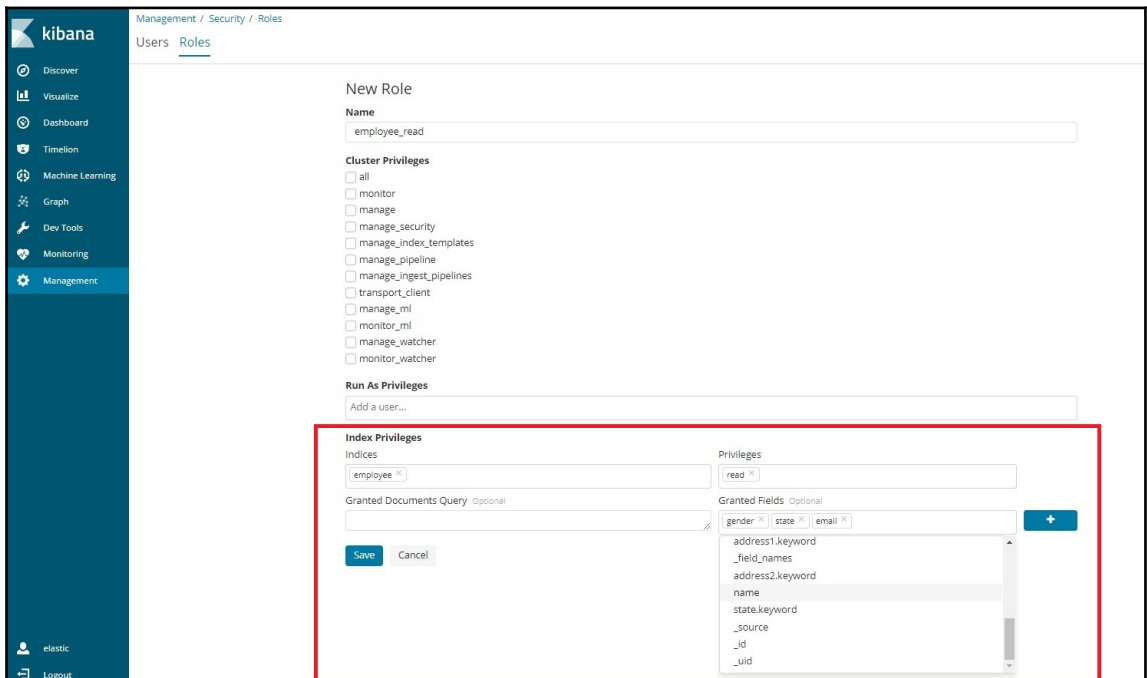
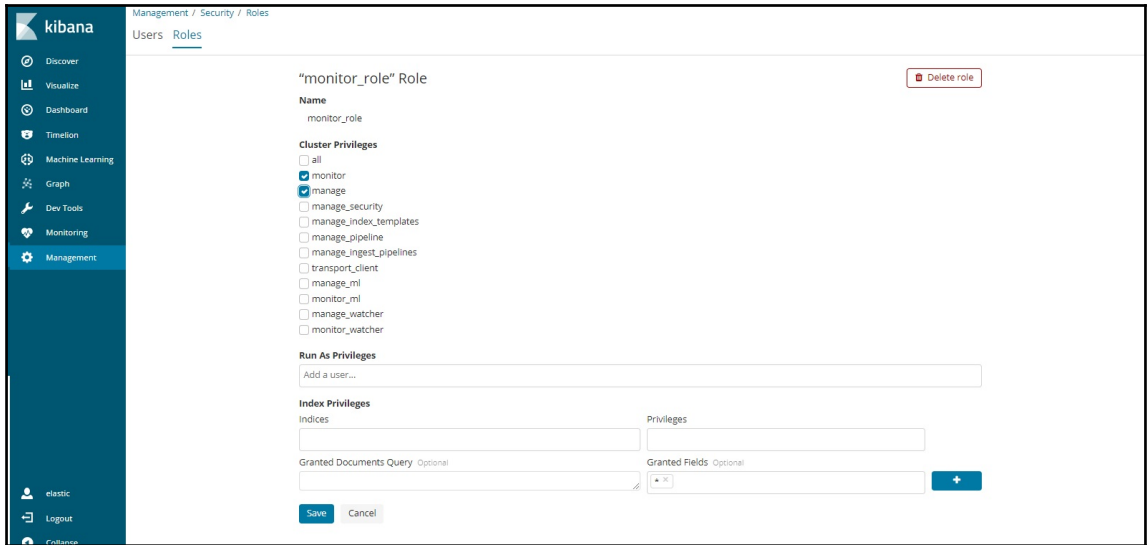


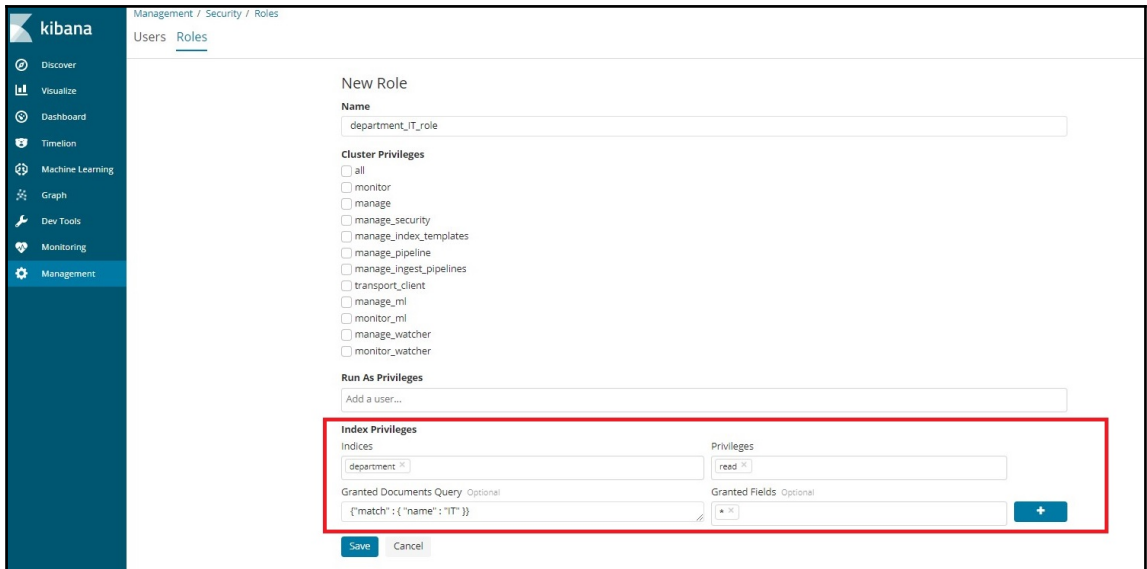
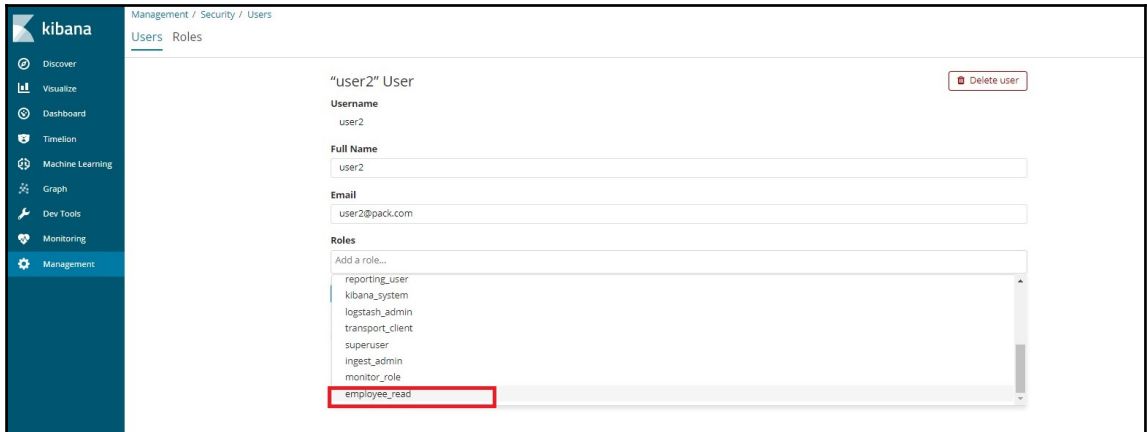


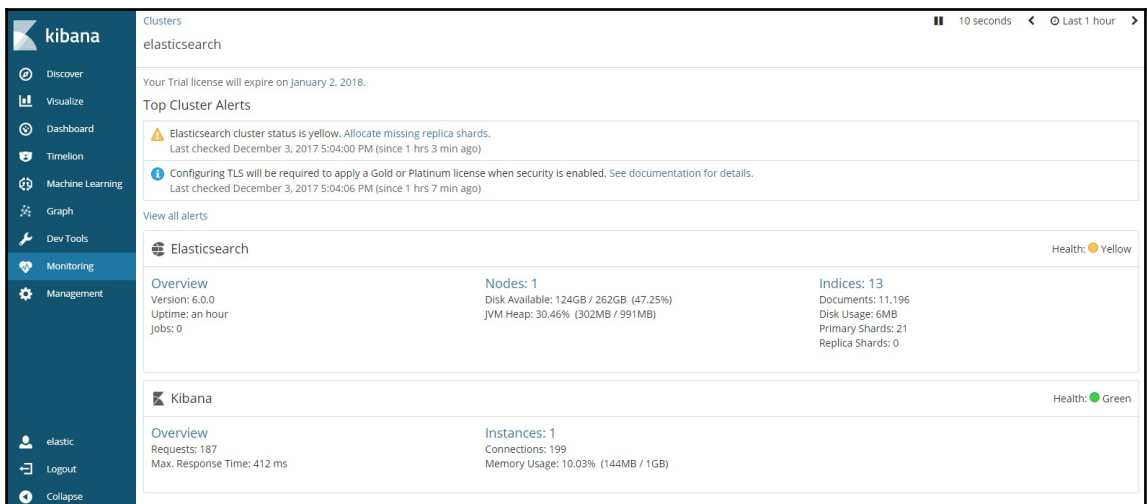
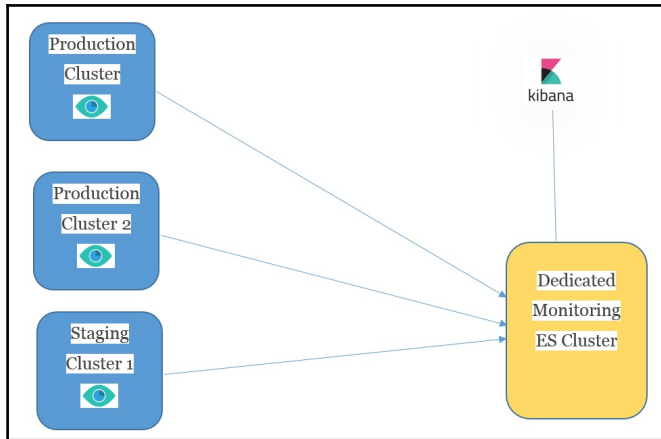
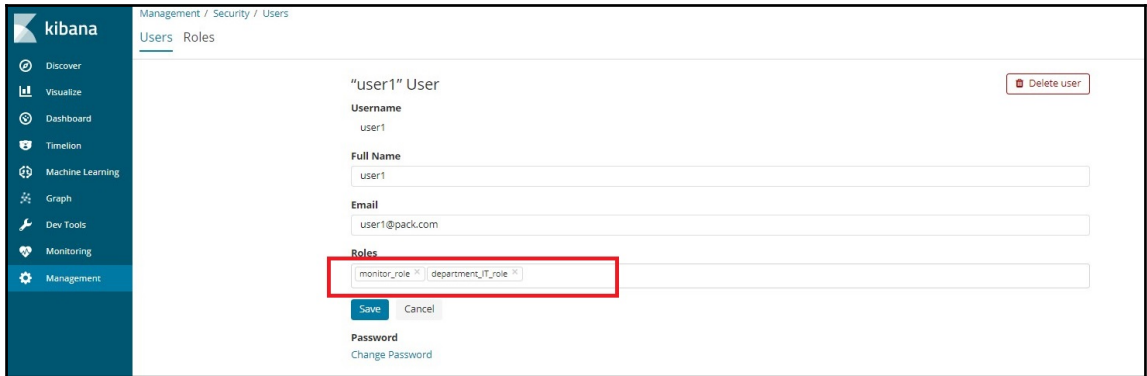


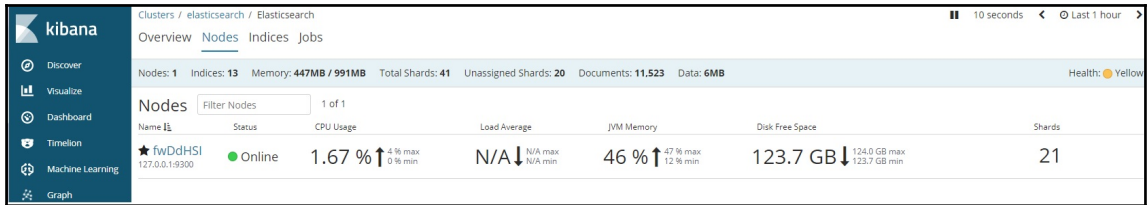
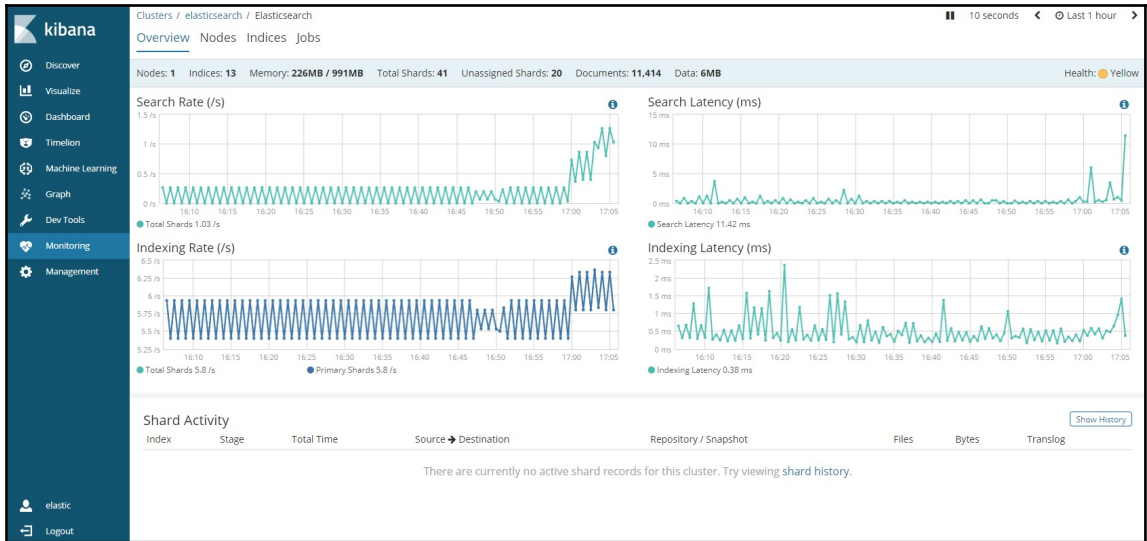


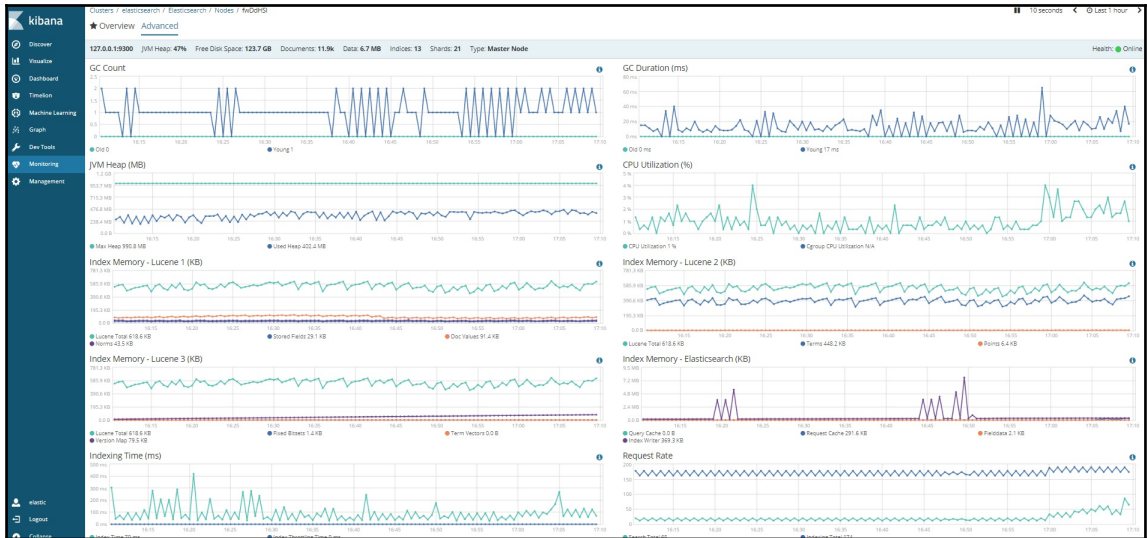








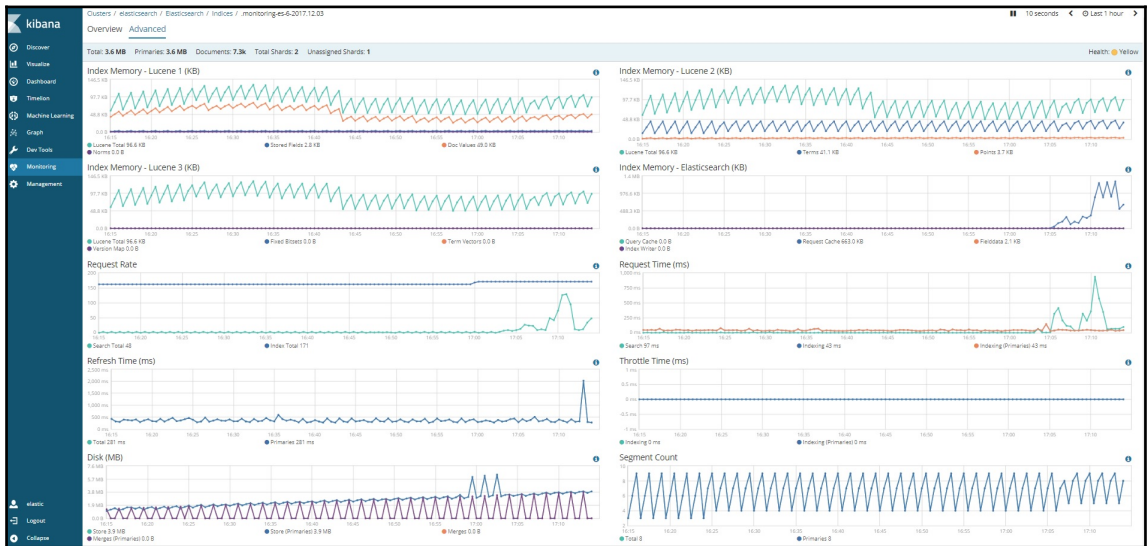


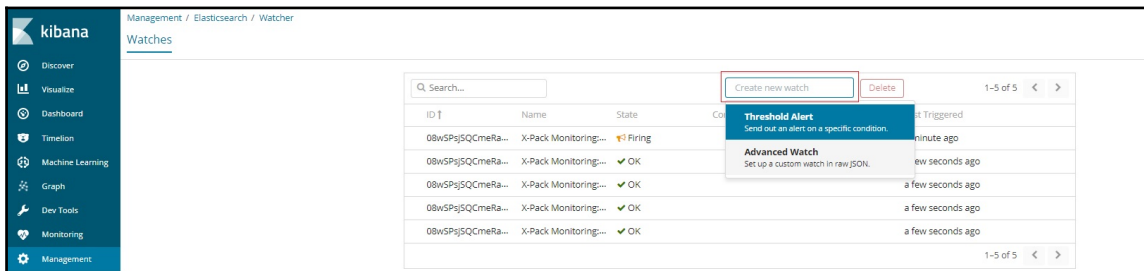
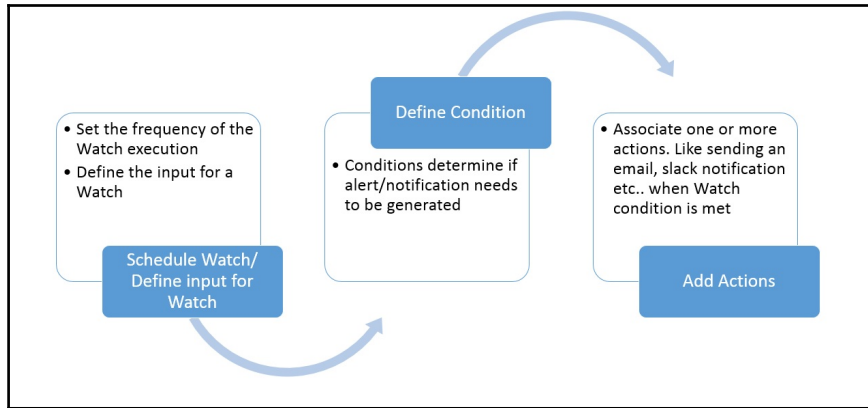


Clusters / elasticsearch / Elasticsearch
Overview Nodes Indices Jobs

Nodes: 1 Indices: 13 Memory: 432MB / 991MB Total Shards: 41 Unassigned Shards: 20 Documents: 12,044 Data: 7MB Health: Yellow

| Indices | Status | Document Count | Data | Index Rate | Search Rate | Unassigned Shards |
|---------------------------------|--------|----------------|----------|------------|-------------|-------------------|
| metricbeat-6.0.0-2017.11.12 | Yellow | 0 | 264.0 B | 0 /s | 0 /s | 1 |
| .monitoring.kibana-6-2017.12.03 | Yellow | 70 | 100.6 KB | 0.1 /s | 0.2 /s | 1 |
| .kibana | Yellow | 108 | 290.3 KB | 0 /s | 0.4 /s | 1 |
| sk12-6.0.0-2017.12.02 | Yellow | 99 | 544.4 KB | 0 /s | 0 /s | 5 |
| sk-6.0.0-2017.12.02 | Yellow | 22 | 187.6 KB | 0 /s | 0 /s | 5 |
| metricbeat-6.0.0-2017.11.27 | Yellow | 210 | 219.3 KB | 0 /s | 0 /s | 1 |
| metricbeat-6.0.0-2017.11.26 | Yellow | 4,1k | 915.3 KB | 0 /s | 0 /s | 1 |
| .monitoring-alerts-6 | Yellow | 1 | 8.8 KB | 0.03 /s | 0.17 /s | 1 |
| .watches | Yellow | 5 | 103.1 KB | 0.17 /s | 0 /s | 1 |
| .watcher-history-6-2017.12.03 | Yellow | 497 | 741.0 KB | 0.17 /s | 0 /s | 1 |
| .triggered_watches | Yellow | 0 | 16.2 KB | 0.17 /s | 0 /s | 1 |
| .monitoring-es-6-2017.12.03 | Yellow | 6.9k | 3.8 MB | 5.7 /s | 4.3 /s | 1 |





Management / Elasticsearch / Watcher / Watches / New Watch

New Watch

Create a new threshold alert
Send out an alert when specific conditions are met. This will run once every 30 seconds.

Name

Select an Index

Select a time field: timestamp | Run this watch every: 30 seconds

Broad searches can be done by adding + to your query



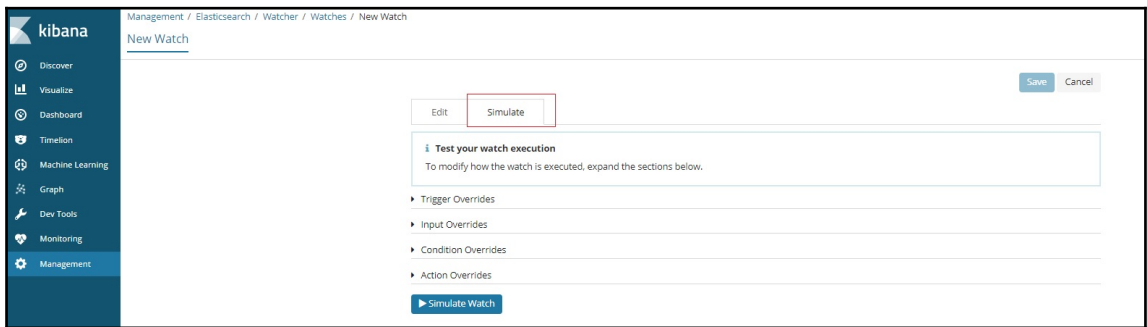
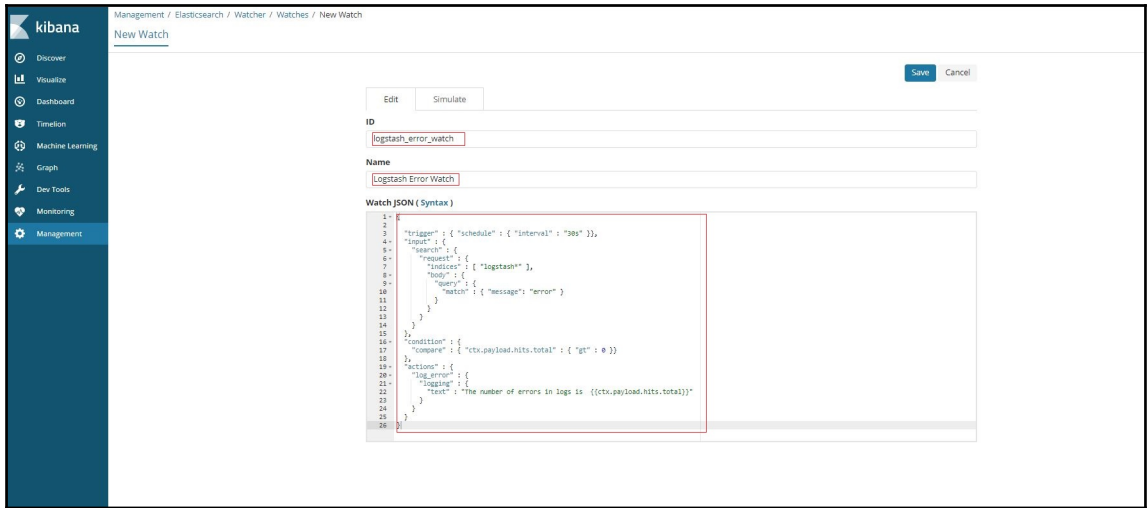
Will perform 1 action once met

Logging

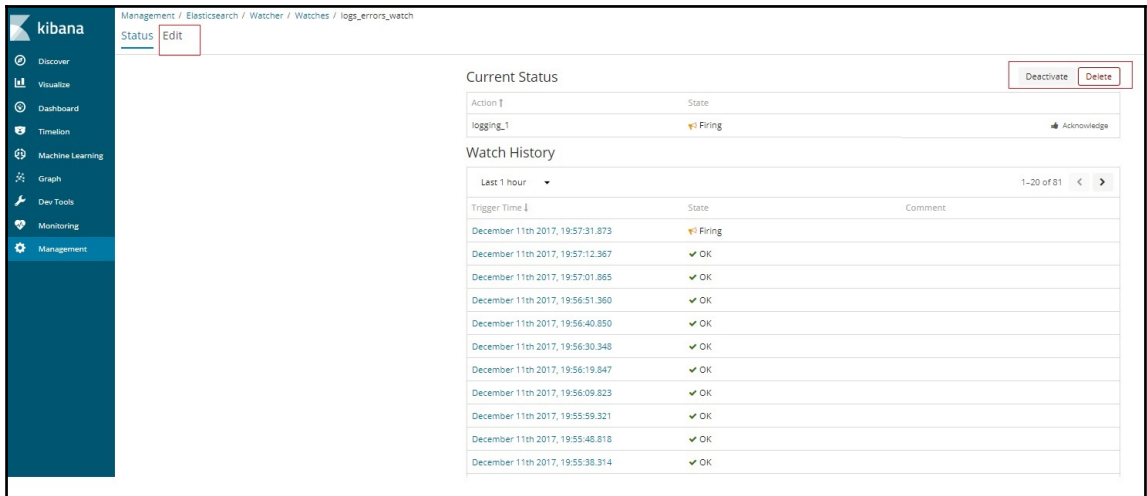
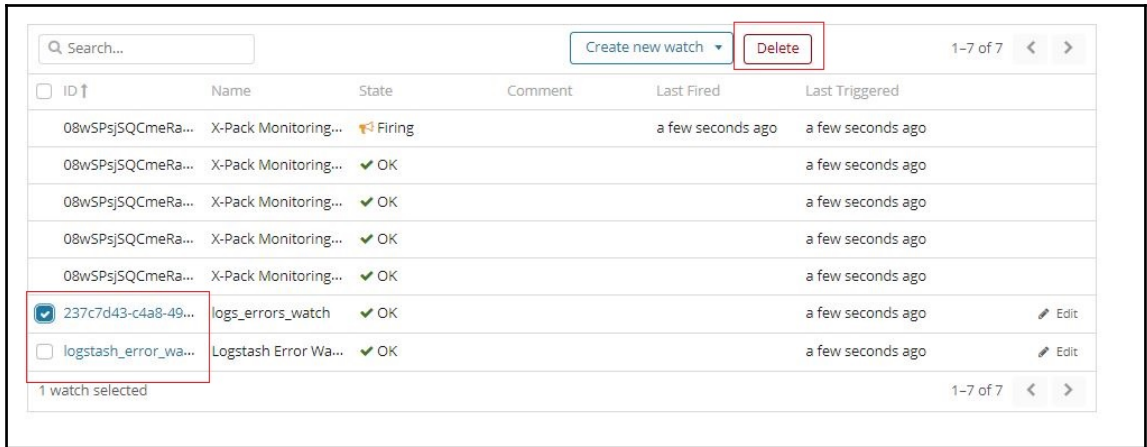
Log text

```
localhost:9200/.watches/_search
Apps New

{
  "_index": ".watches",
  "_type": "doc",
  "_id": "237c7d43-c4a8-498f-9ed7-b168318ac1eb",
  "_score": 1,
  "_source": {
    - trigger: {
      - schedule: {
        - interval: "1es"
      }
    },
    - input: {
      - search: {
        - request: {
          - search_type: "query_then_fetch",
          - indices: [
            "logs"
          ],
          - types: [ ],
          - body: {
            - size: 0,
            - query: {
              - bool: {
                - filter: {
                  - range: {
                    - timestamp: {
                      gte: "{{ctx.trigger.scheduled_time}}|-10m",
                      lte: "{{ctx.trigger.scheduled_time}}",
                      format: "strict_date_optional_time||epoch_millis"
                    }
                  }
                }
              }
            }
          }
        }
      }
    },
    - condition: {
      - script: {
        - sources: "if (ctx.payload.hits.total > params.threshold) { return true; } return false;",
        - lang: "painless",
        - params: {
          - threshold: 20
        }
      }
    },
    - transform: {
      - script: {
        - sources: "HashMap result = new HashMap(); result.result = ctx.payload.hits.total; return result;",
        - lang: "painless",
        - params: {
          - threshold: 20
        }
      }
    },
    - actions: {
      - logging_1: {
        - logging: {
          - level: "info",
          - text: "Number of Logs Reported is above the threshold is {{ctx.payload.result}}"
        }
      }
    },
    - metadata: {
      - name: "logs_errors_watch",
      - watcher: {
        - trigger_interval_unit: "s",
        - agg_type: "count",
        - time_field: "timestamp",
        - trigger_interval_size: 10,
        - term_size: 5,
        - time_window_unit: "m",
        - threshold_comparator: ">",
        - term_field: null,
        - index: [
          "logs"
        ]
      }
    }
  }
}
```

```
localhost:9200/.watches/_search
Apps New
- {
  _index: ".watches",
  _type: "doc",
  _id: "logstash_error_watch",
  _score: 1,
  _source: {
    - trigger: {
      - schedule: {
        interval: "30s"
      }
    },
    - input: {
      - search: {
        - request: {
          search_type: "query_then_fetch",
          - indices: [
            "logstash*"
          ],
          types: [ ],
          - body: {
            - query: {
              - match: {
                message: "error"
              }
            }
          }
        }
      }
    },
    - condition: {
      - compare: {
        - ctx.payload.hits.total: {
          gt: 0
        }
      }
    },
    - actions: {
      - log_error: {
        - logging: {
          level: "info",
          text: "The number of errors in logs is {{ctx.payload.hits.total}}"
        }
      }
    },
    - metadata: {
      name: "Logstash Error Watch",
      - xpack: {
        type: "json"
      }
    },
    + status: {...}
  }
},
```



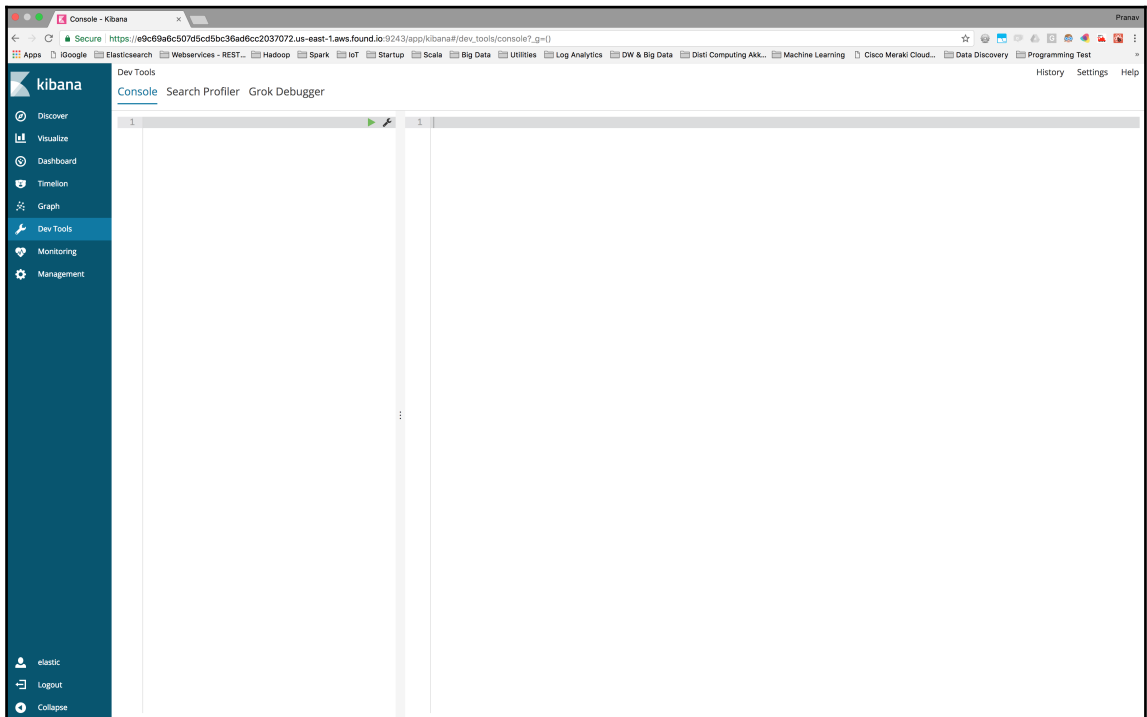
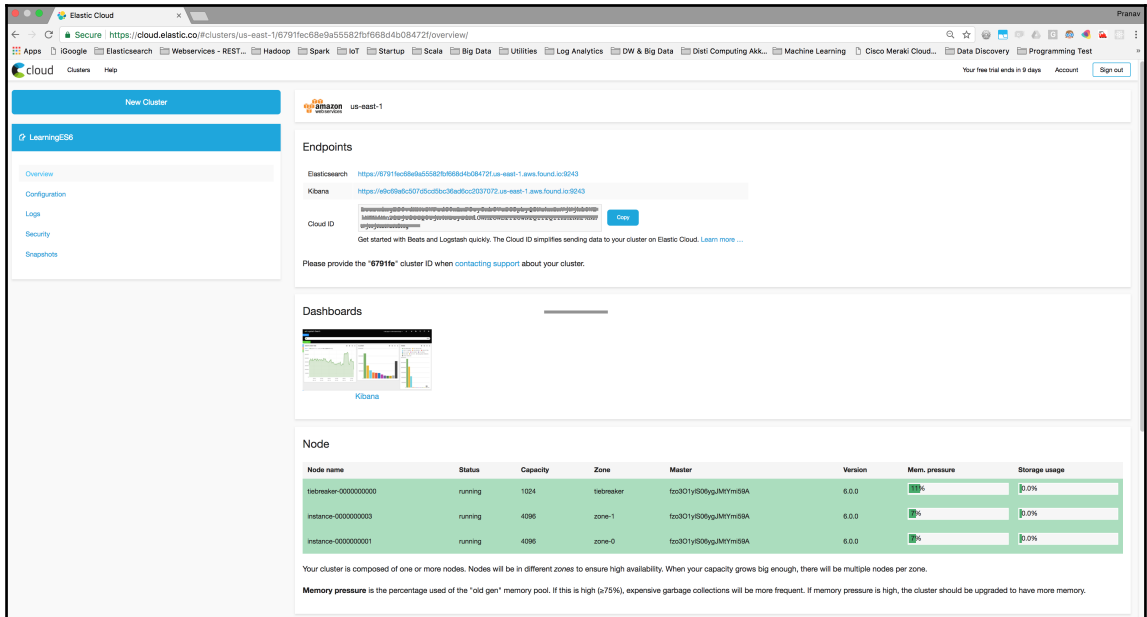
Chapter 9: Running Elastic Stack in Production

The screenshot displays the Elastic Cloud console interface for creating a new cluster. The browser address bar shows the URL `https://cloud.elastic.co/#/clusters/create/`. The page is divided into several sections:

- Summary:** A table listing configuration details:

| | |
|-------------------|-----------------------|
| Platform | Amazon Web Services |
| Region | US East (N. Virginia) |
| Memory | 4 GB |
| Storage | 96 GB |
| SSD | Yes |
| High availability | Yes |
| Hourly rate | \$0.3125 |
| Monthly rate | \$228 |

 A blue "Create" button is located below the table.
- Get started with Elastic Cloud:** A text block providing information about the free trial period and the 14-day limit. It includes links for [Shield](#), [Watcher](#), [Marvel](#), and [Kibana](#). It also mentions that adding a credit card prevents the cluster from being stopped after 14 days and allows for larger clusters. A 4GB cluster with HA remains free for 14 days. Support contact information is provided: support@elastic.co.
- Cluster Size:** A slider interface for selecting a cluster size. The slider ranges from 1GB (24GB) to 256GB (6144GB). The current selection is 4GB (96GB). A blue dot on the slider indicates the selected size. A legend shows "Memory" in blue and "Storage" in light blue. A note states "Cluster size can be changed later without downtime." A "Recommended for production" arrow points to the 4GB (96GB) selection. A checkbox for "SSD" is checked, with a note "Selected for improved storage performance." A link "Need a larger cluster? Contact us." is present.
- Cloud Platform:** A section titled "Pick your cloud:" with two options: "amazon web services" (selected) and "Google Cloud Platform".
- Choose a region near you:** A row of buttons for different regions: "US East (N. Virginia)" (selected), "US West (N. California)", "US West (Oregon)", "EU (Ireland)", "Asia Pacific (Singapore)", "Asia Pacific (Tokyo)", "South America East", and "Asia Pacific (Sydney)".



Snapshots are taken every 30 minutes. Click on a snapshot for more details and for restoring options.

| When | Status | # Shards | # Indexes |
|--------------------------|---------|----------|-----------|
| 2017-11-22T04:42:30.854Z | SUCCESS | 15 / 15 | 15 |
| 2017-11-22T04:12:34.070Z | SUCCESS | 15 / 15 | 15 |
| 2017-11-22T03:42:17.216Z | SUCCESS | 16 / 16 | 16 |
| 2017-11-22T03:12:05.363Z | SUCCESS | 15 / 15 | 15 |
| 2017-11-22T02:41:54.722Z | SUCCESS | 15 / 15 | 15 |
| 2017-11-22T02:11:46.656Z | SUCCESS | 15 / 15 | 15 |
| 2017-11-22T01:41:39.708Z | SUCCESS | 15 / 15 | 15 |
| 2017-11-22T01:11:33.414Z | SUCCESS | 15 / 15 | 15 |
| 2017-11-22T00:41:27.497Z | SUCCESS | 16 / 16 | 16 |
| 2017-11-22T00:11:19.073Z | SUCCESS | 16 / 16 | 16 |
| 2017-11-21T23:41:11.914Z | SUCCESS | 14 / 14 | 14 |
| 2017-11-21T23:11:04.897Z | SUCCESS | 14 / 14 | 14 |
| 2017-11-21T22:40:55.100Z | SUCCESS | 14 / 14 | 14 |
| 2017-11-21T22:10:47.847Z | SUCCESS | 14 / 14 | 14 |
| 2017-11-21T21:40:41.807Z | SUCCESS | 14 / 14 | 14 |

Snapshot details

ID: schackled-1511318514-instance-000000001

Indices: .monitoring-kibana-6-2017.11.21, .triggered_watches-6, .watcher-history-6-2017.11.21, .watcher-history-6-2017.11.18, .watcher-history-6-2017.11.16, .security-6, amazon_products, .watcher-history-6-2017.11.17, .monitoring-kibana-6-2017.11.20, .watcher-history-6-2017.11.19, .watches-6, .monitoring-kibana-6-2017.11.22, .watcher-history-6-2017.11.20, kibana-6, .watcher-history-6-2017.11.22

Shards: Successful: 15 Failed: 0 Total: 15

When: 2017-11-22T02:41:54.722Z

Took: 938 ms

Restore

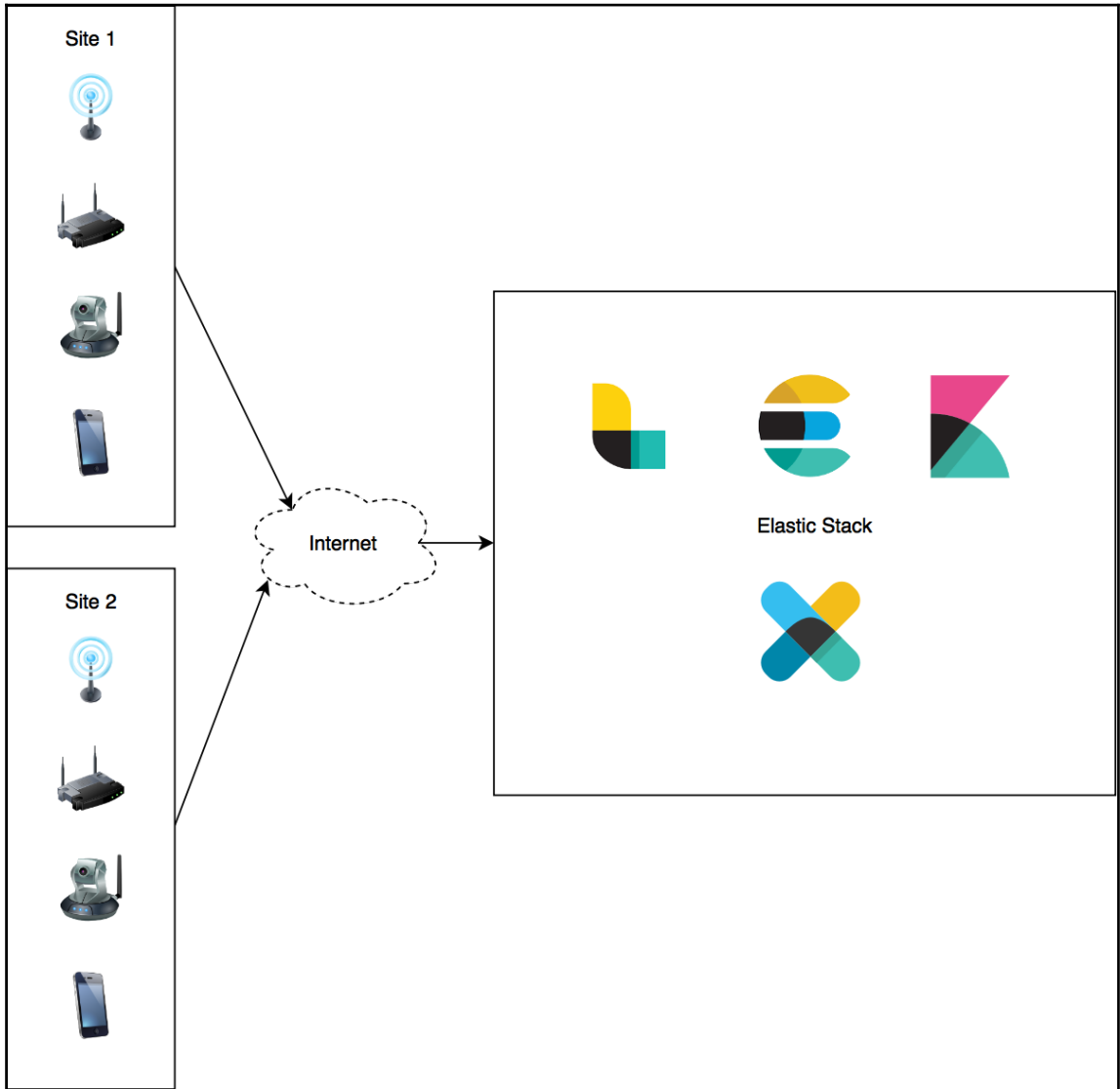
Indices: All indexes in the snapshot as well as cluster state are restored. Specify indexes with `[index1,index2,index3]` if you only want to restore specific ones.

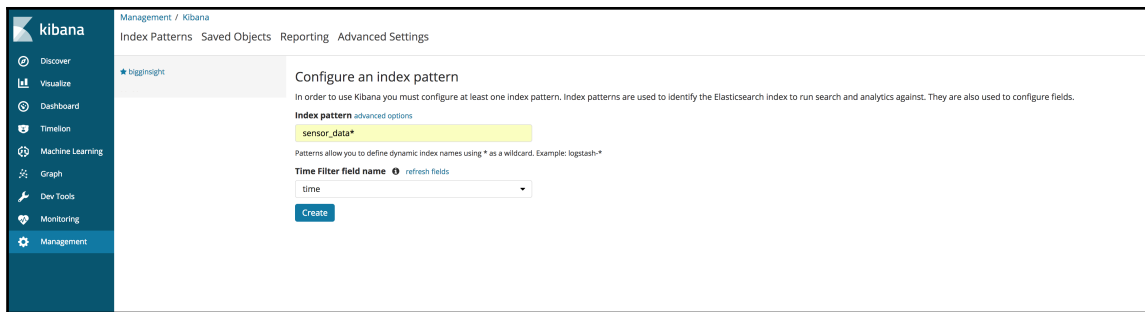
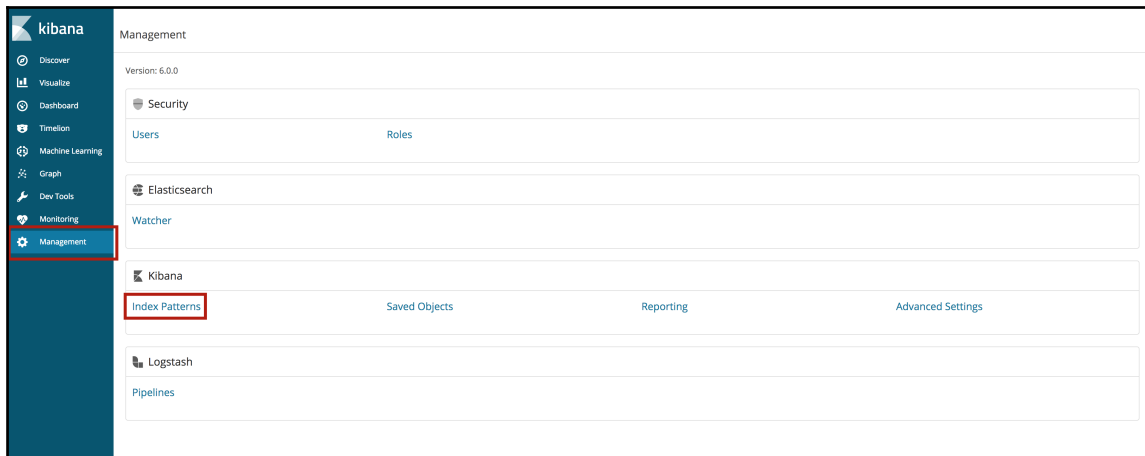
Rename pattern: `rename_pattern` and `rename_replacement` options can also be used to rename index on restore using regular expression that supports referencing the original text.

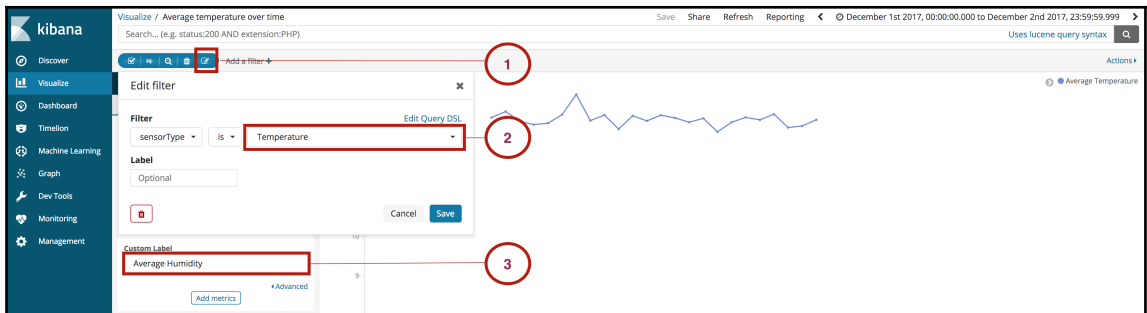
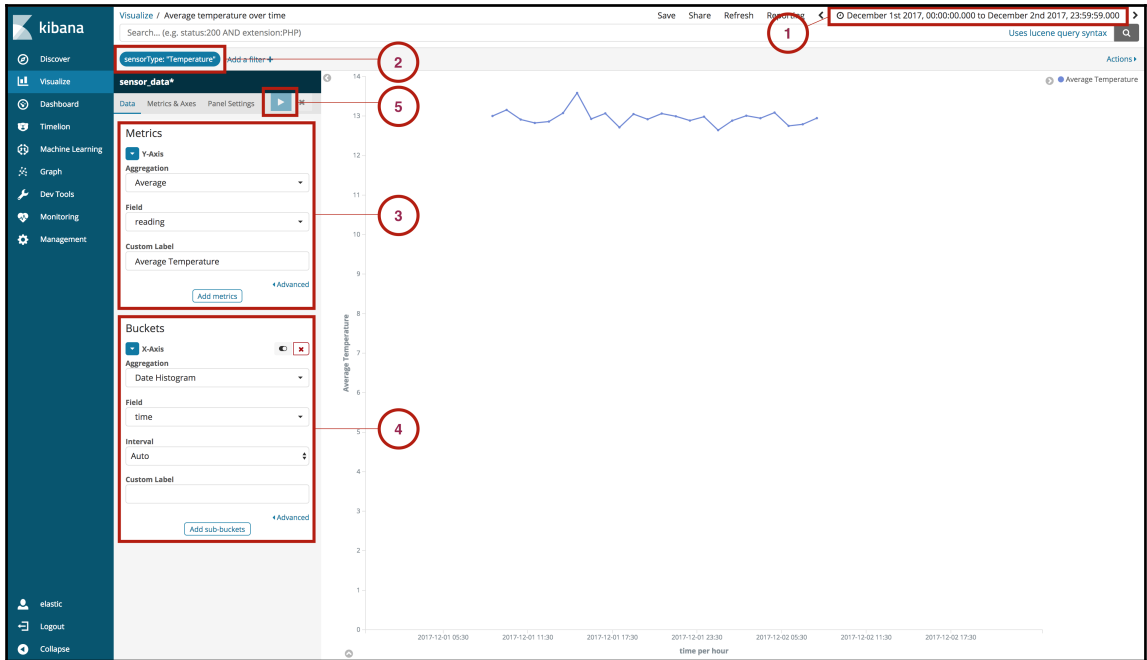
Rename replacement:

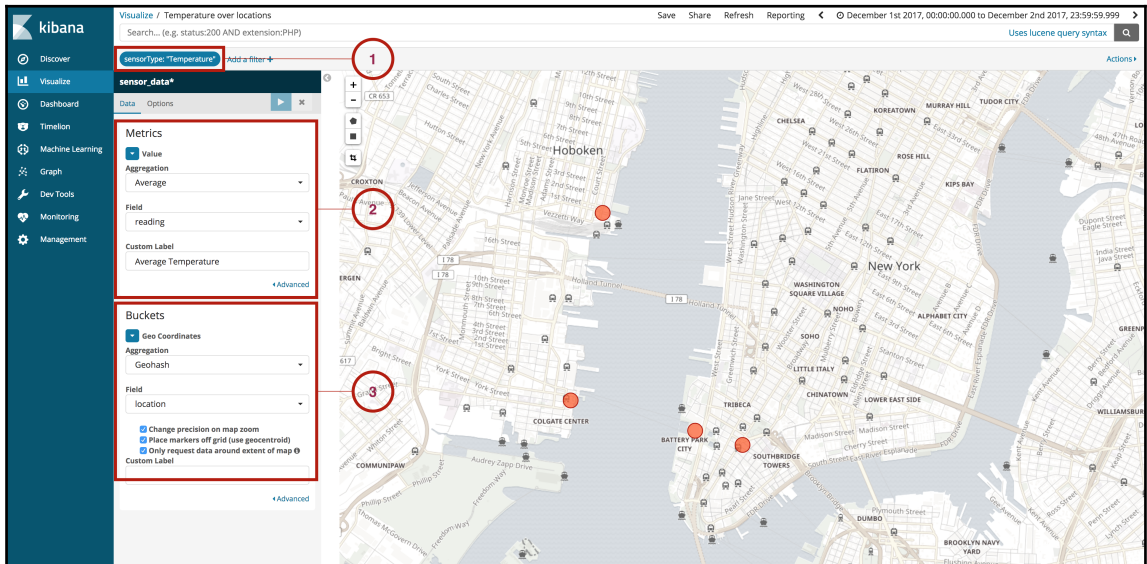
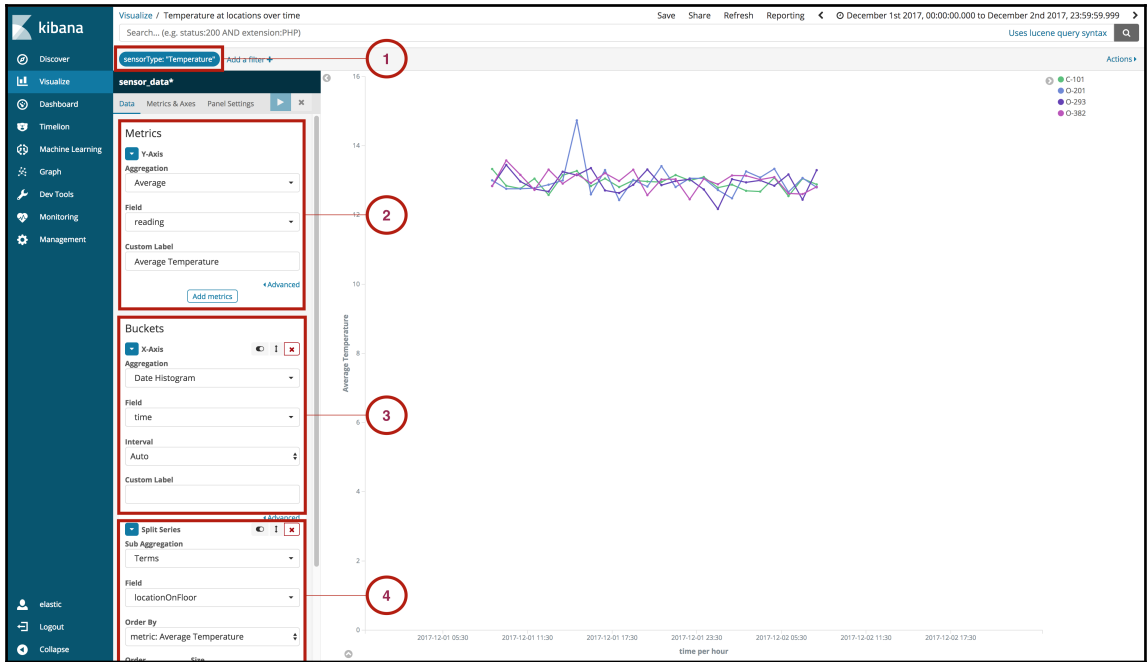
Cluster: By default the snapshot is restored to this cluster but you can choose to restore to a different cluster. The target cluster must be in the same region and have an equal or higher version of Elasticsearch running.

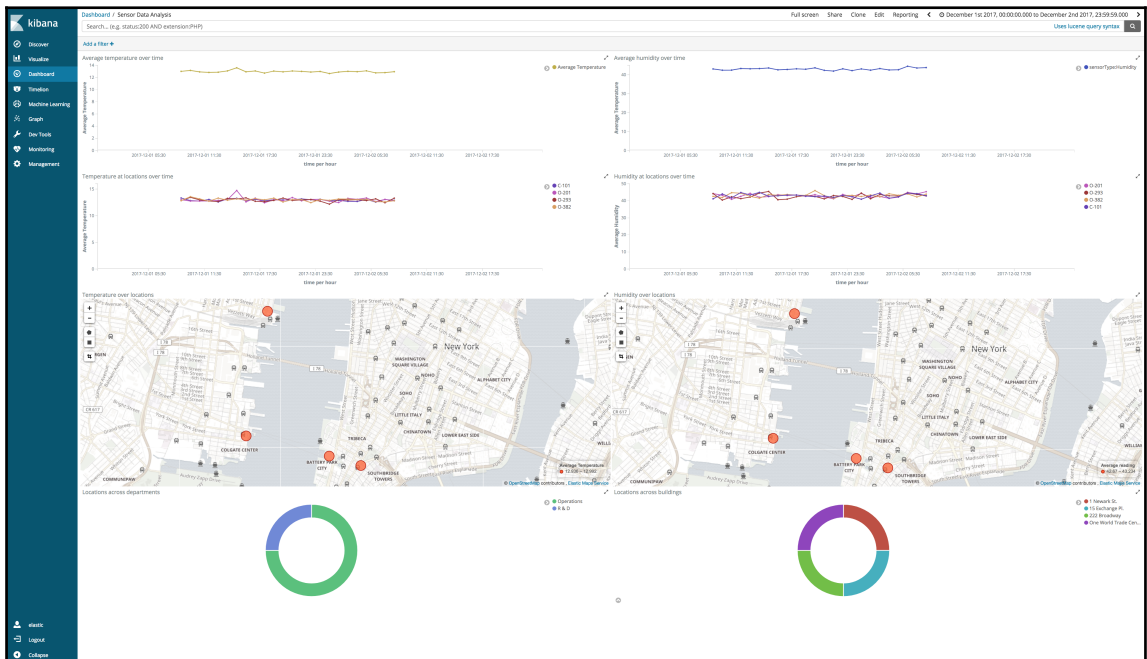
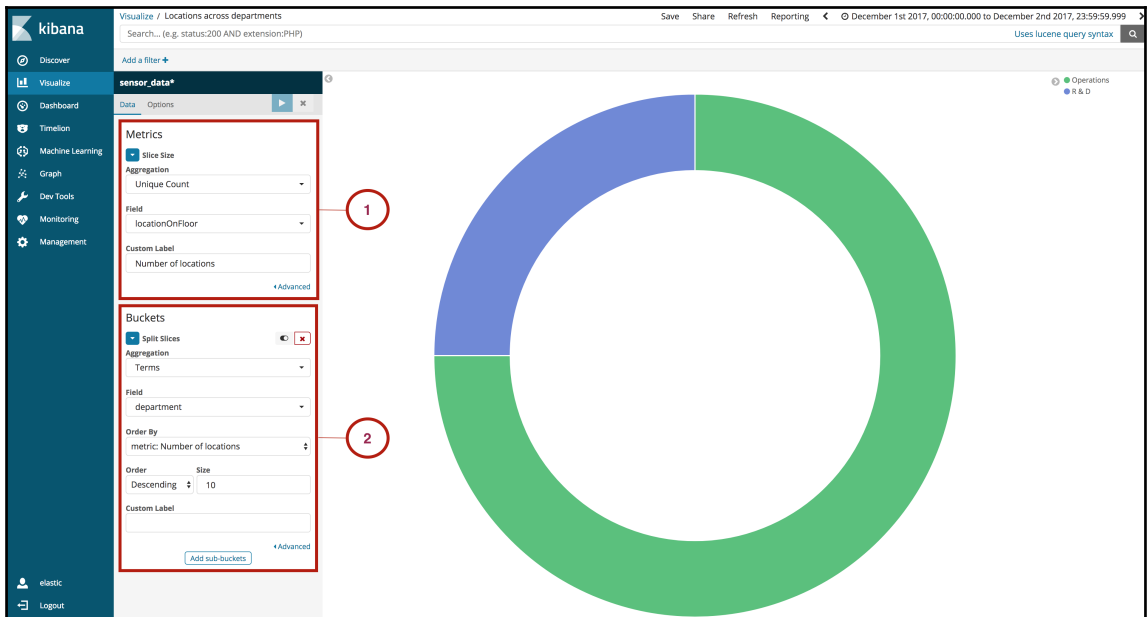
Chapter 10: Building a Sensor Data Analytics Application

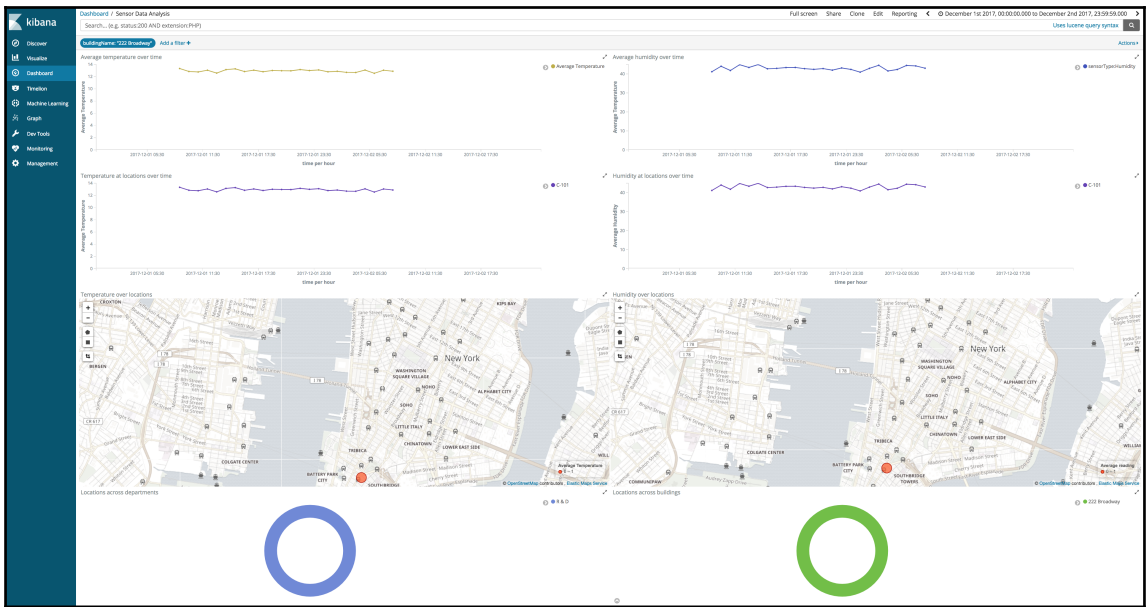













Chapter 11: Monitoring Server Infrastructure

Download Metricbeat

 Want to upgrade? We'll give you a hand. [Migration Guide](#) »

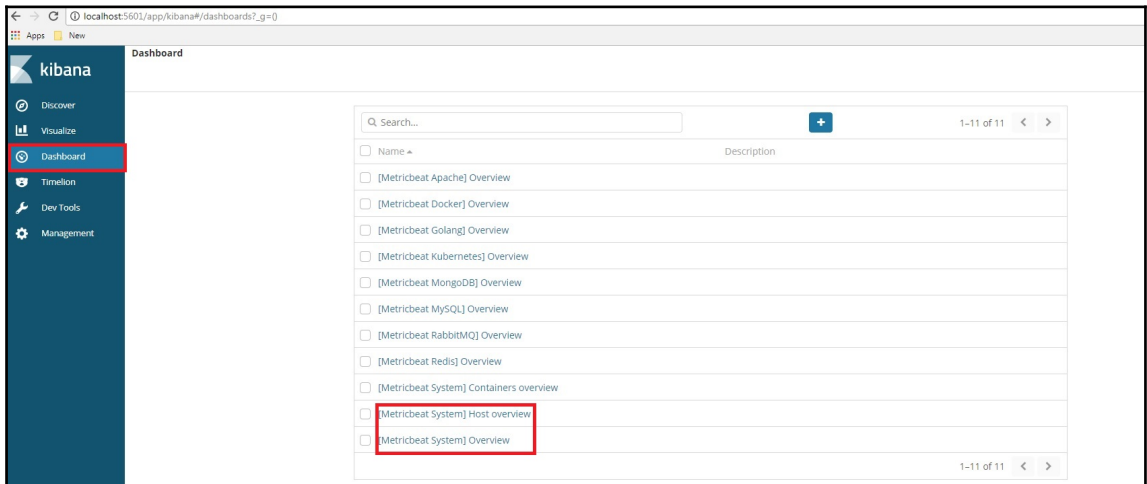
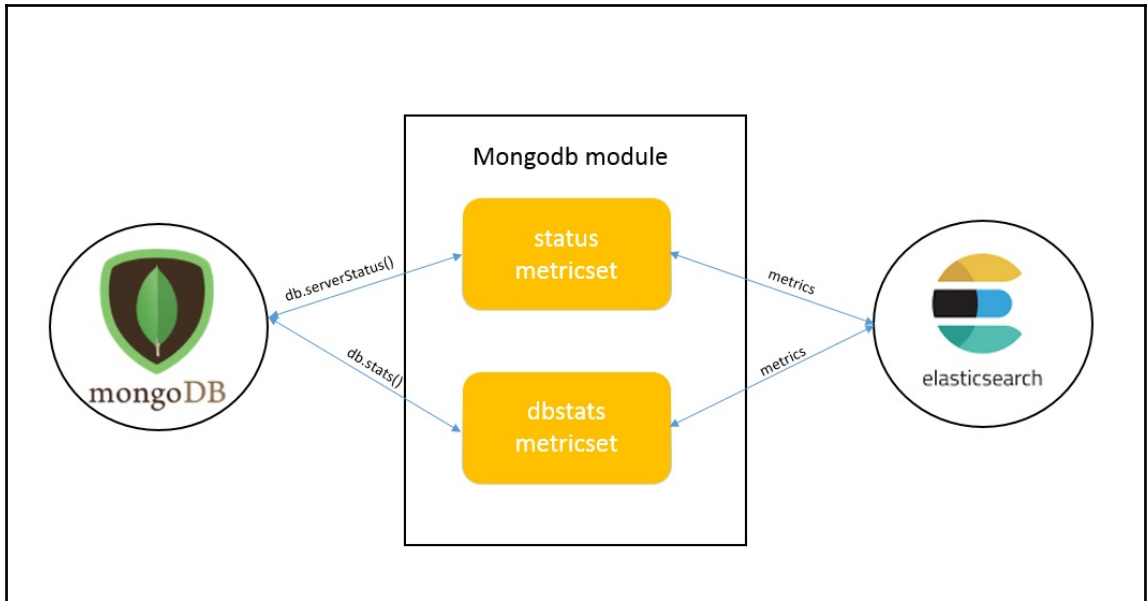
Version: 6.0.0

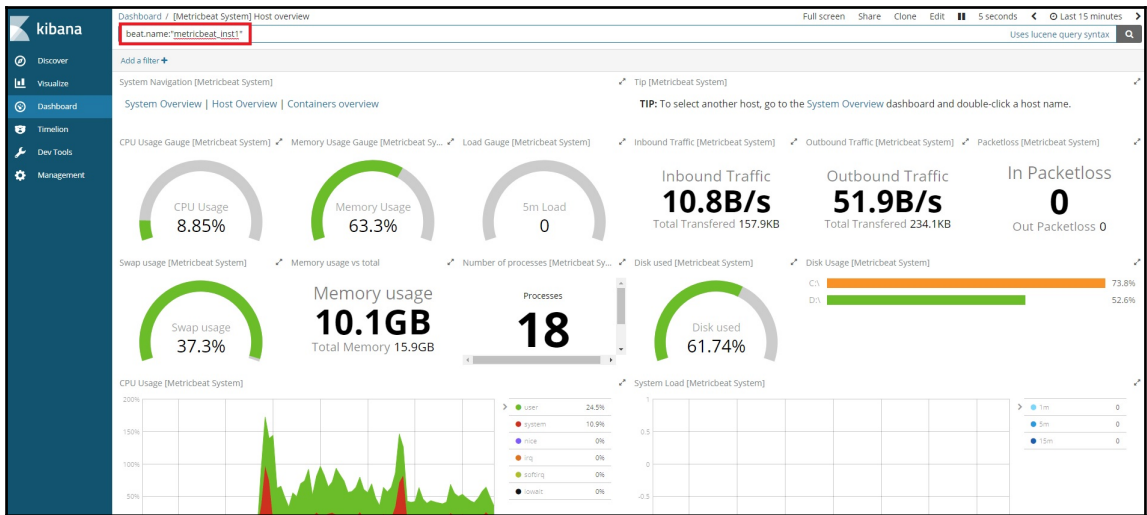
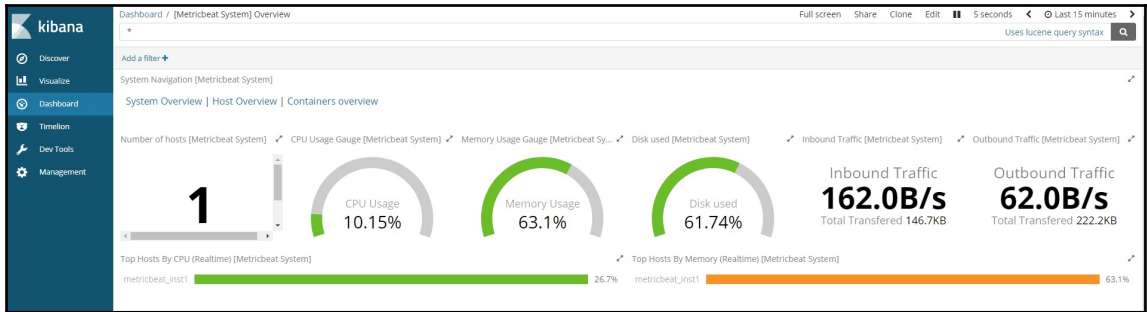
Release date: November 14, 2017

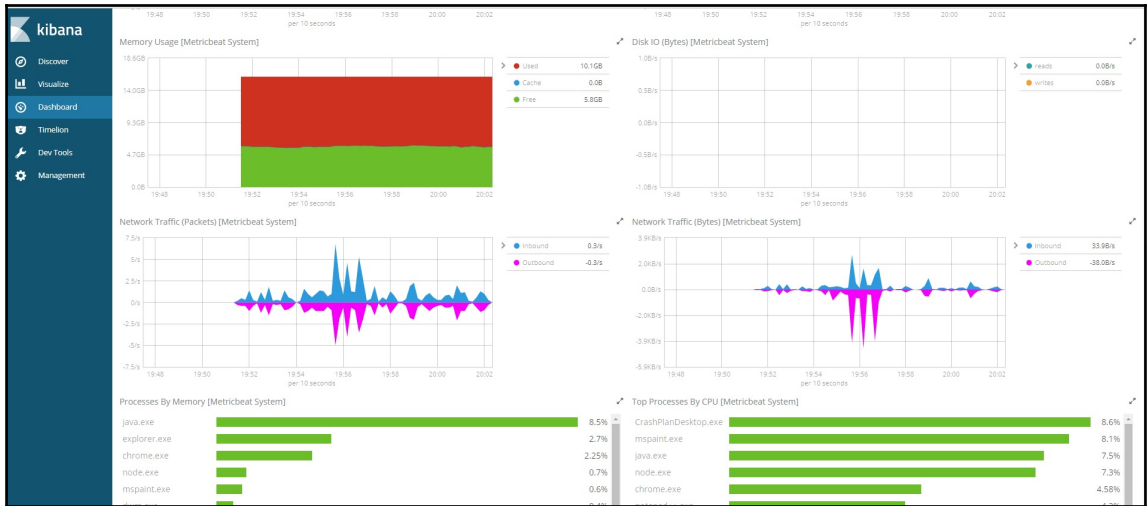
Notes: View [release notes](#).
Not the version you're looking for? View [past releases](#).
Looking for Topbeat? Download [the 1.x release](#).

Downloads:

| | | |
|--------------------------------|------------------------------------|------------------------------------|
| DEB 32-BIT sha | DEB 64-BIT sha | RPM 32-BIT sha |
| RPM 64-BIT sha | LINUX 32-BIT sha | LINUX 64-BIT sha |
| MAC sha | WINDOWS 32-BIT sha | WINDOWS 64-BIT sha |



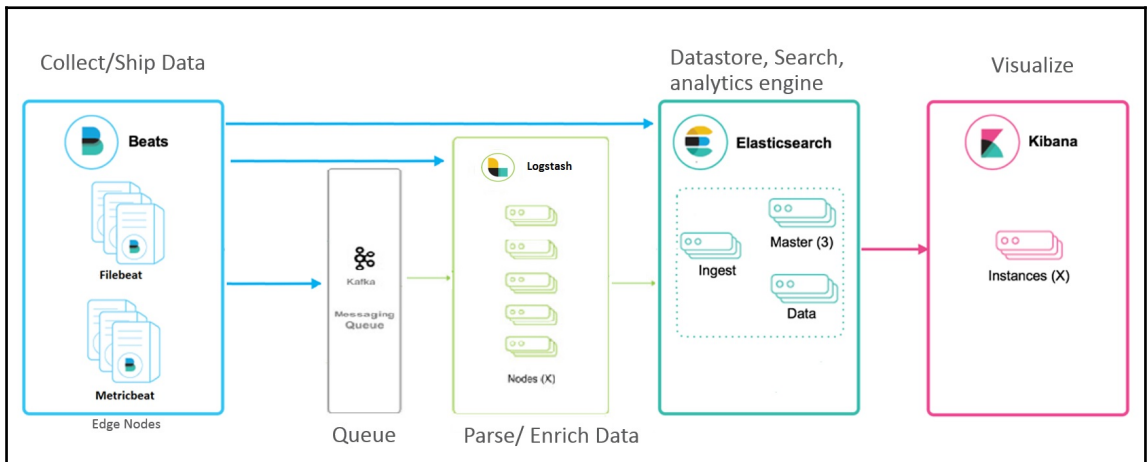




Full screen Share Clone Edit 5 seconds Last 15 minutes

Refresh Interval

- 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



Index