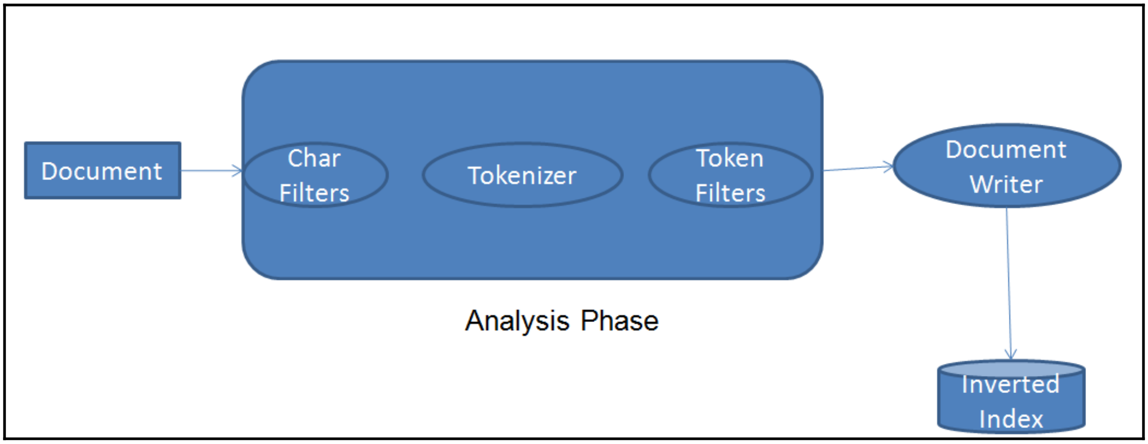
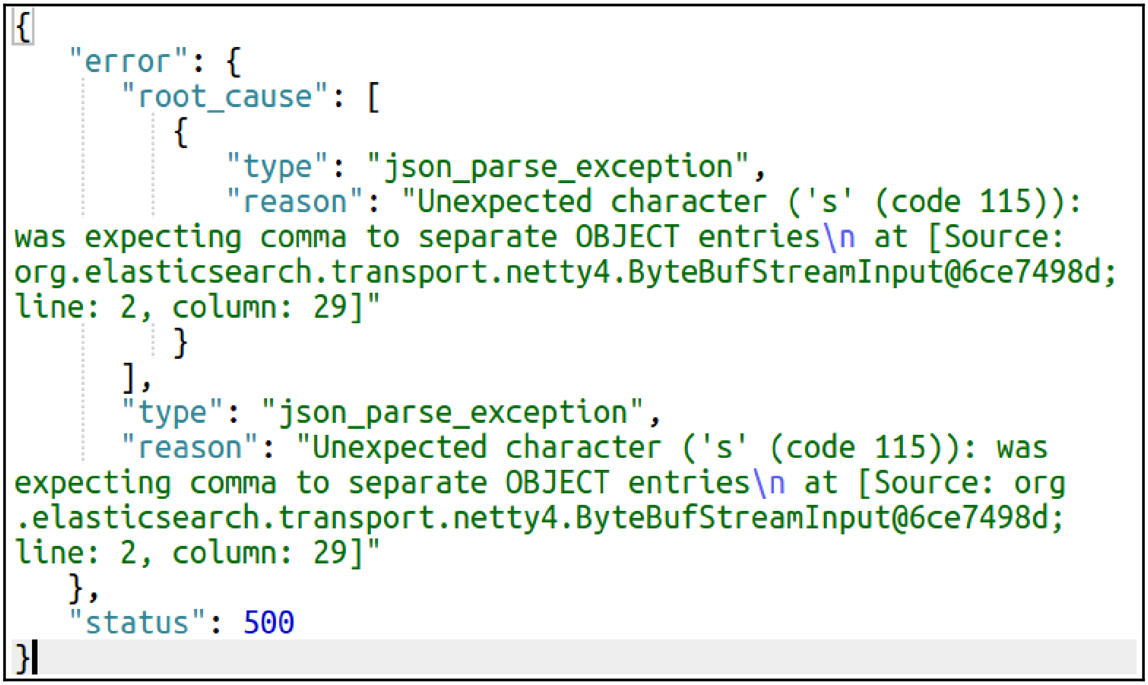
Graphic Bundle

Chapter 1:



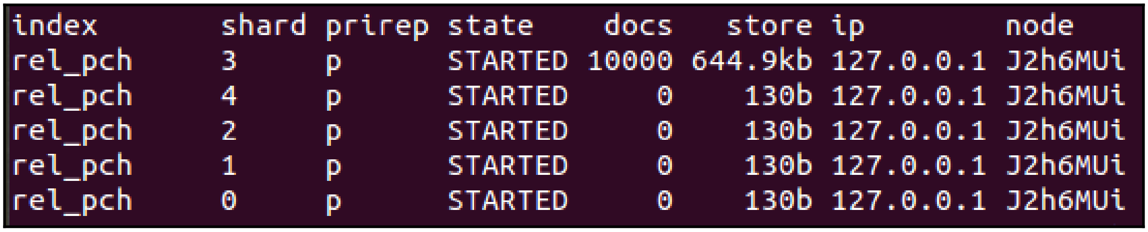
Chapter 2:

$$\mathrm{bm25}(d) = \sum_{t\in q, f_{t,d}>0} \log\left(1+\frac{N-df_t+0.5}{df_t+0.5}\right)\cdot\frac{f_{t,d}}{f_{t,d}+k\cdot(1-b+b\frac{l(d)}{avgdl})}$$



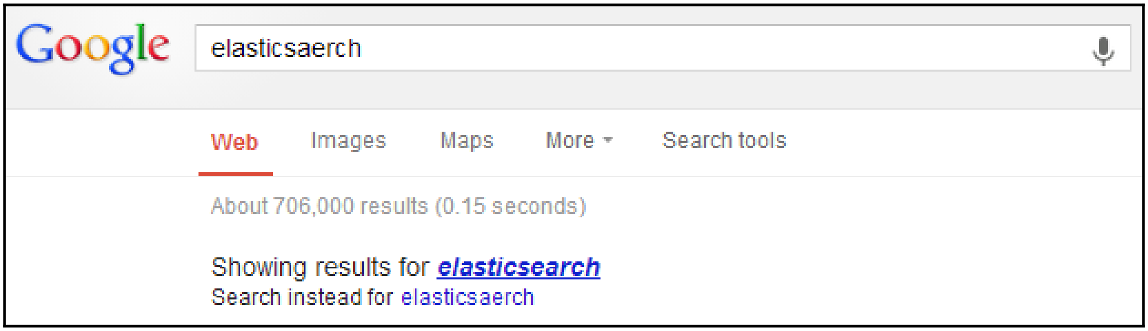
```
{
   "error": {
      "root_cause": [
         {
            "type": "json_parse_exception",
            "reason": "Unexpected character ('s' (code 115)):
was expecting comma to separate OBJECT entries\n at [Source:
org.elasticsearch.transport.netty4.ByteBufStreamInput@6ce7498d;
line: 2, column: 29]"
         }
      ],
      "type": "json_parse_exception",
      "reason": "Unexpected character ('s' (code 115)): was
expecting comma to separate OBJECT entries\n at [Source: org
.elasticsearch.transport.netty4.ByteBufStreamInput@6ce7498d;
line: 2, column: 29]"
   },
   "status": 500
}
```

Chapter 4:



```
index        shard prirep state    docs   store ip        node
rel_pch      3     p      STARTED 10000 644.9kb 127.0.0.1 J2h6MUi
rel_pch      4     p      STARTED     0    130b 127.0.0.1 J2h6MUi
rel_pch      2     p      STARTED     0    130b 127.0.0.1 J2h6MUi
rel_pch      1     p      STARTED     0    130b 127.0.0.1 J2h6MUi
rel_pch      0     p      STARTED     0    130b 127.0.0.1 J2h6MUi
```

Chapter 5:

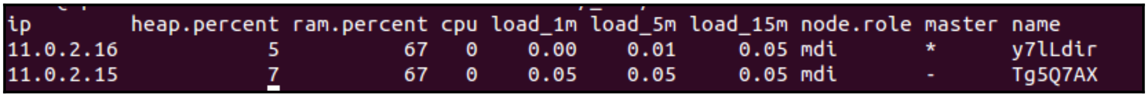


elasticsaerch

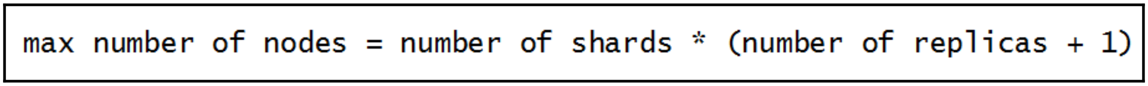
About 706,000 results (0.15 seconds)

Showing results for ***elasticsearch***
Search instead for elasticsaerch

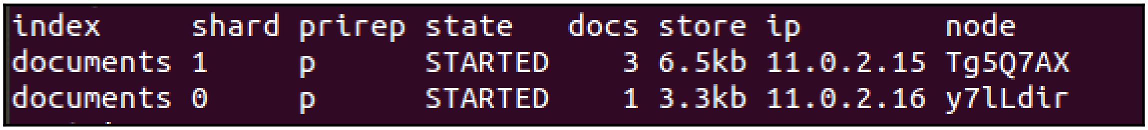
Chapter 6:



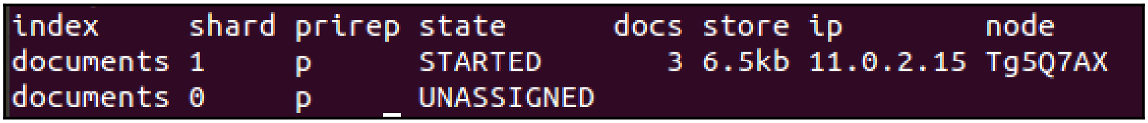
```
ip        heap.percent ram.percent cpu load_1m load_5m load_15m node.role master name
11.0.2.16            5          67   0    0.00    0.01     0.05 mdi       *      y7lLdir
11.0.2.15            7          67   0    0.05    0.05     0.05 mdi       -      Tg5Q7AX
```



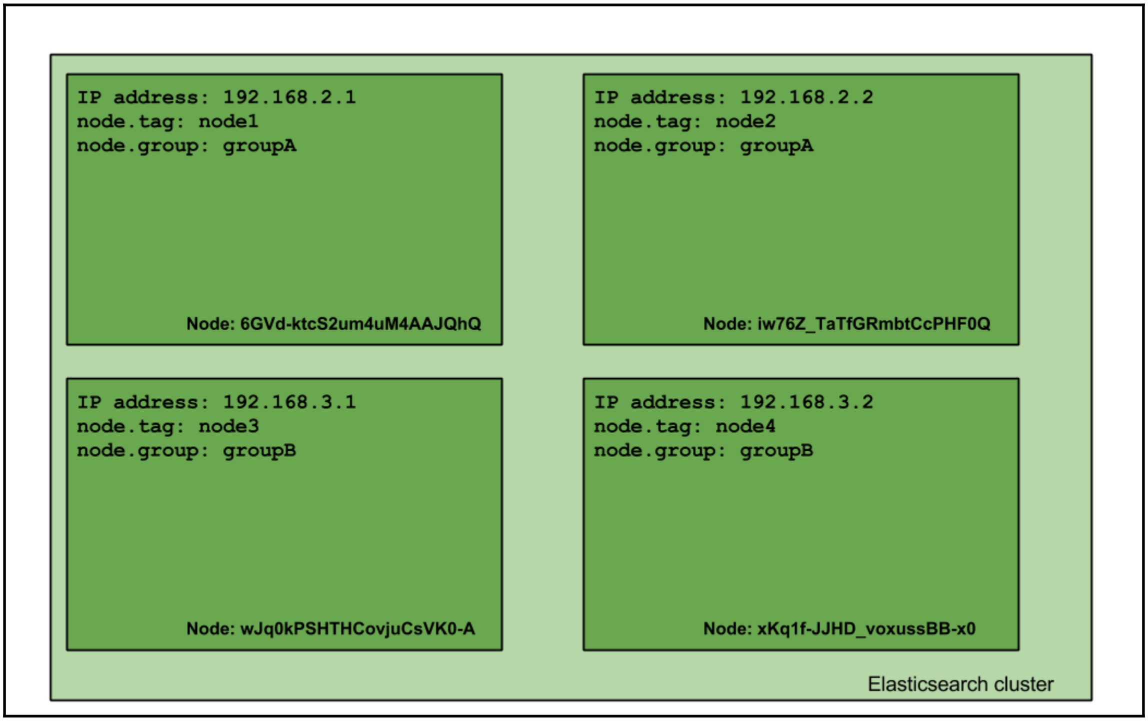
```
max number of nodes = number of shards * (number of replicas + 1)
```

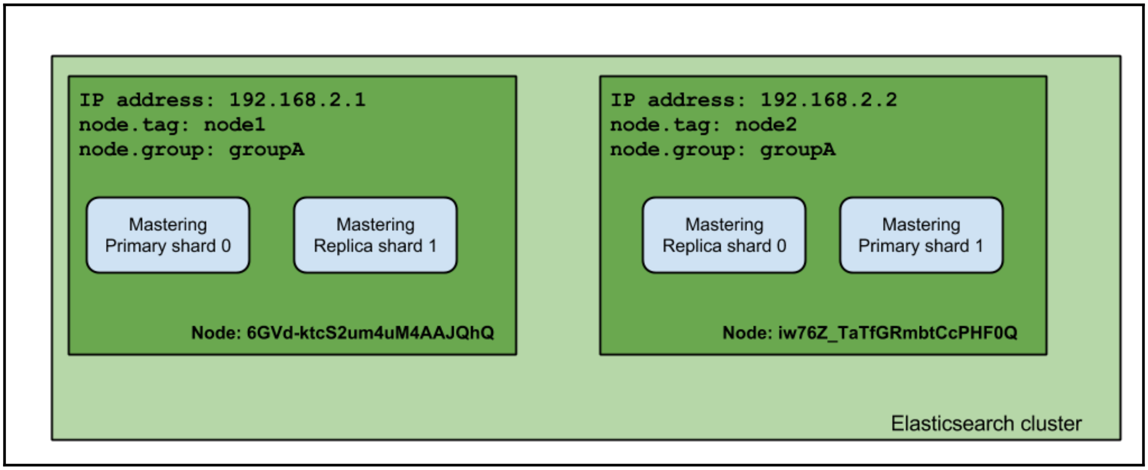


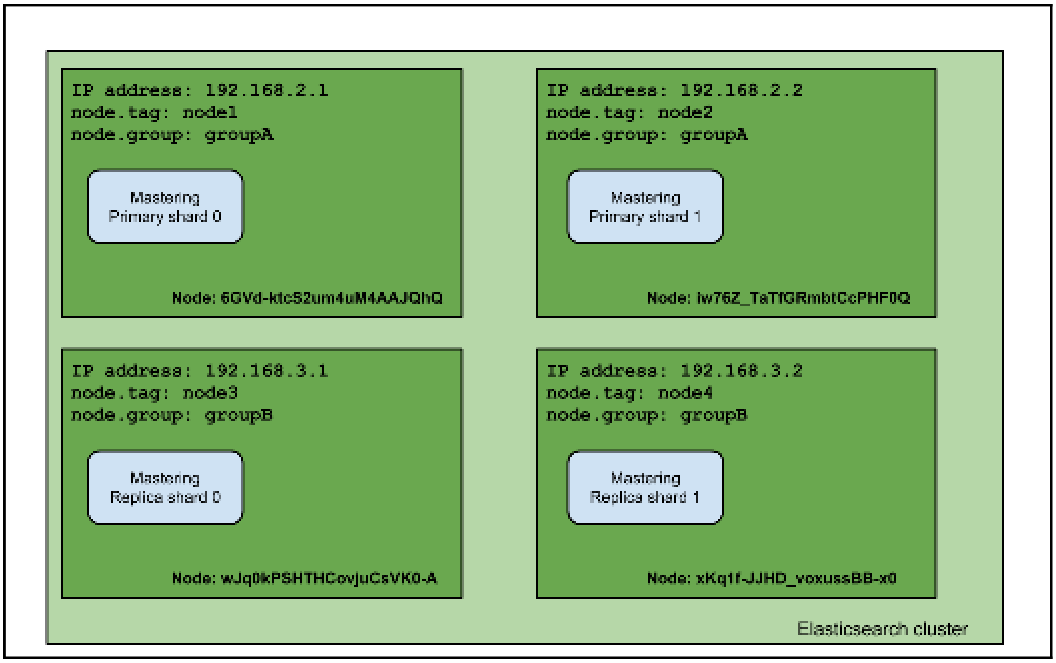
```
index     shard prirep state   docs store ip        node
documents 1     p      STARTED    3 6.5kb 11.0.2.15 Tg5Q7AX
documents 0     p      STARTED    1 3.3kb 11.0.2.16 y7lLdir
```

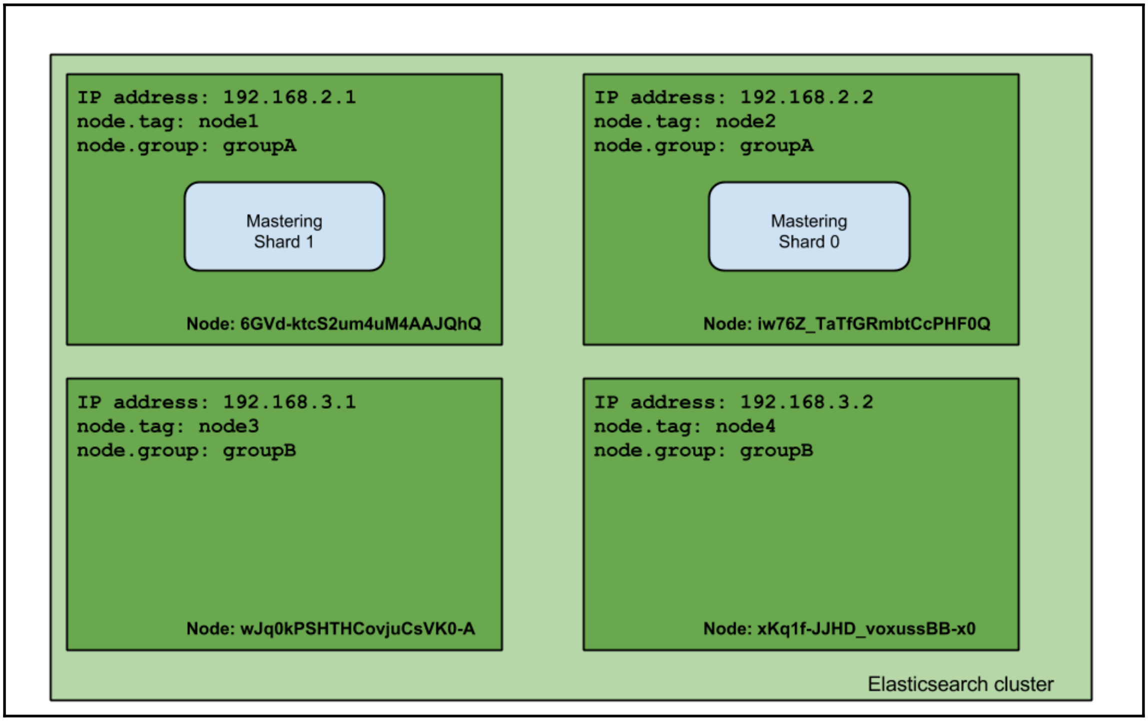


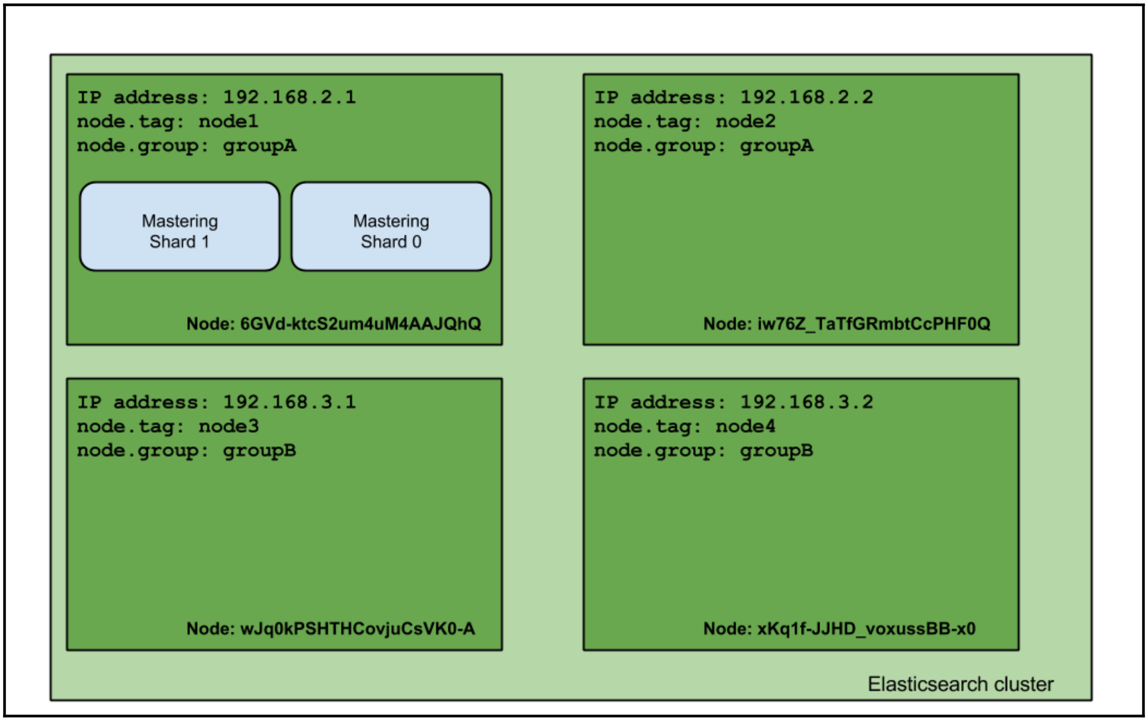
```
index     shard prirep state      docs store ip        node
documents 1     p      STARTED       3 6.5kb 11.0.2.15 Tg5Q7AX
documents 0     p      UNASSIGNED
```

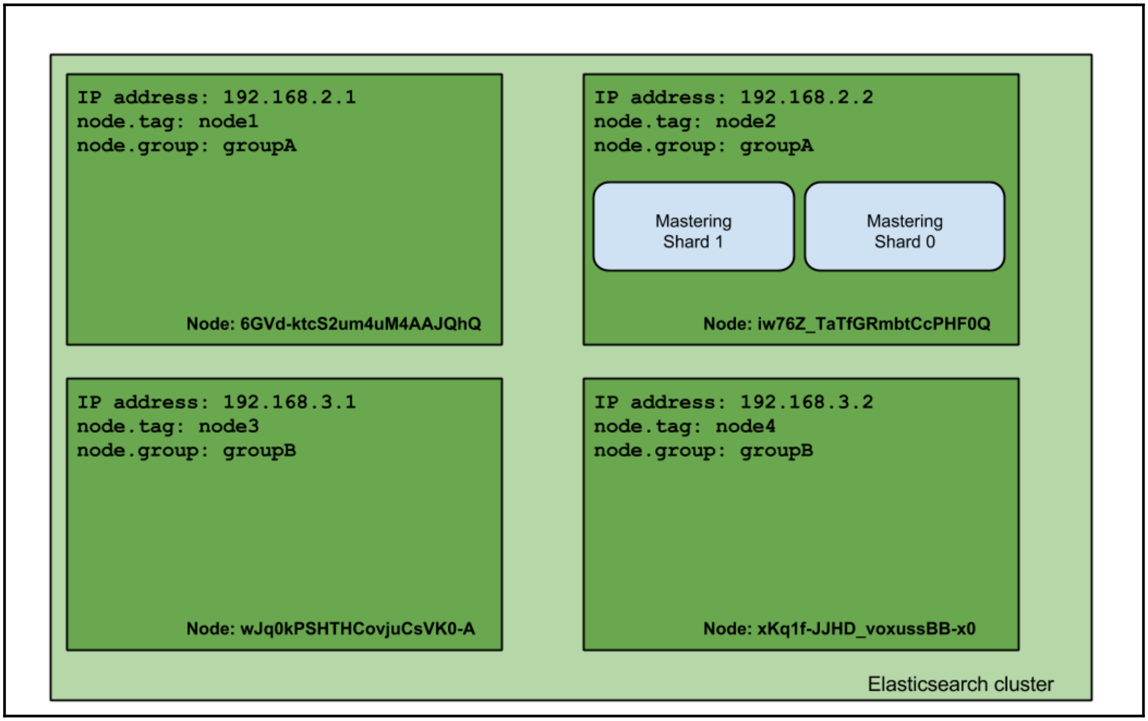



IP address: 192.168.2.1
node.tag: node1
node.group: groupA
Mastering Primary shard 0
Mastering Replica shard 1
Node: 6GVd-ktcS2um4uM4AAJQhQ
IP address: 192.168.2.2
node.tag: node2
node.group: groupA
Mastering Replica shard 0
Mastering Primary shard 1
Node: iw76Z_TaTfGRmbtCcPHF0Q
Elasticsearch cluster

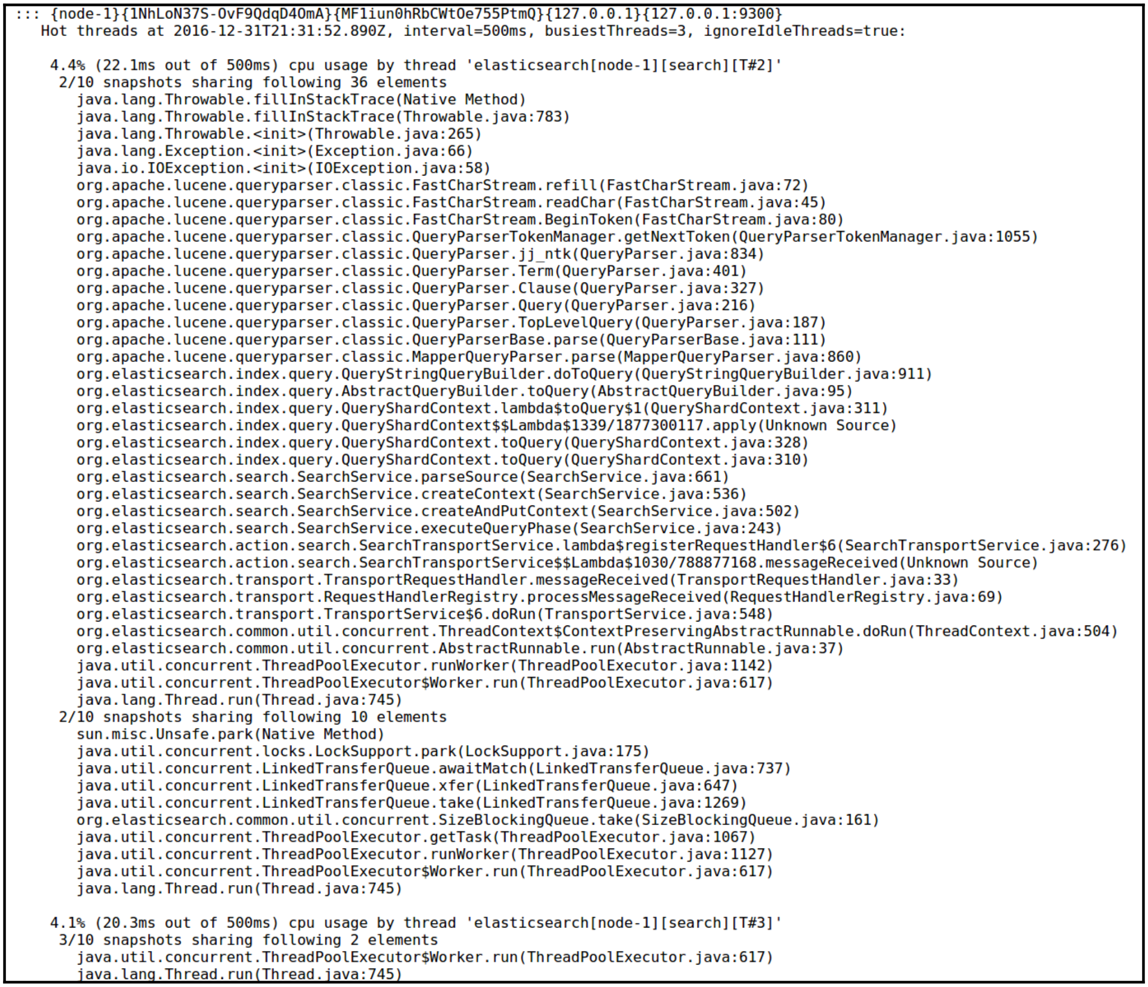

IP address: 192.168.2.1
node.tag: node1
node.group: groupA
Mastering Primary shard 0
Node: 6GVd-ktcS2um4uM4AAJQhQ
IP address: 192.168.2.2
node.tag: node2
node.group: groupA
Mastering Primary shard 1
Node: iw76Z_TaTfGRmbtCcPHF0Q
IP address: 192.168.3.1
node.tag: node3
node.group: groupB
Mastering Replica shard 0
Node: wJq0kPSHTHCovjuCsVK0-A
IP address: 192.168.3.2
node.tag: node4
node.group: groupB
Mastering Replica shard 1
Node: xKq1f-JJHD_voxussBB-x0
Elasticsearch cluster


IP address: 192.168.2.1
node.tag: node1
node.group: groupA
Mastering
Shard 1
Node: 6GVd-ktcS2um4uM4AAJQhQ
IP address: 192.168.2.2
node.tag: node2
node.group: groupA
Mastering
Shard 0
Node: iw76Z_TaTfGRmbtCcPHF0Q
IP address: 192.168.3.1
node.tag: node3
node.group: groupB
Node: wJq0kPSHTHCovjuCsVK0-A
IP address: 192.168.3.2
node.tag: node4
node.group: groupB
Node: xKq1f-JJHD_voxussBB-x0
Elasticsearch cluster

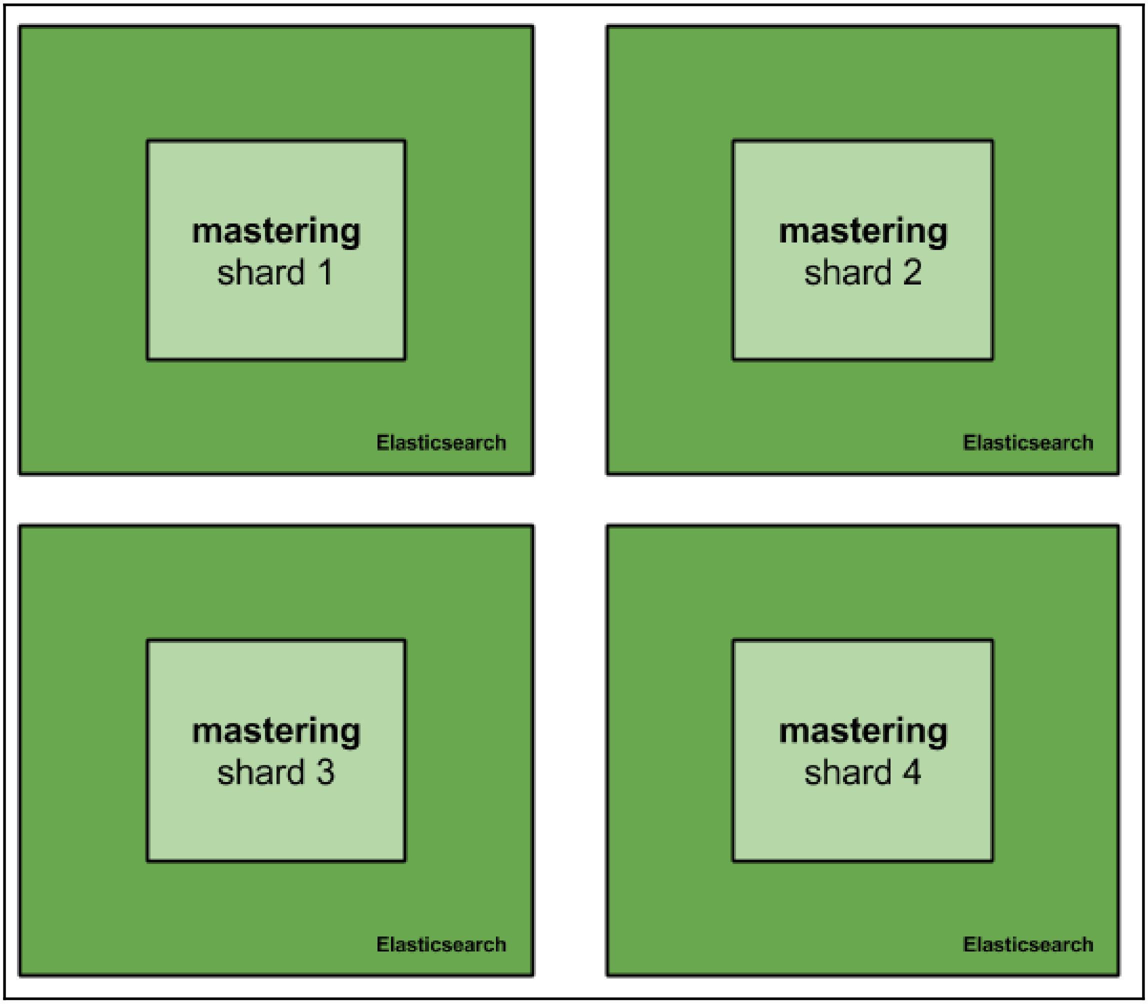

IP address: 192.168.2.1
node.tag: node1
node.group: groupA
Mastering
Shard 1
Mastering
Shard 0
Node: 6GVd-ktcS2um4uM4AAJQhQ
IP address: 192.168.2.2
node.tag: node2
node.group: groupA
Node: iw76Z_TaTfGRmbtCcPHF0Q
IP address: 192.168.3.1
node.tag: node3
node.group: groupB
Node: wJq0kPSHTHCovjuCsVK0-A
IP address: 192.168.3.2
node.tag: node4
node.group: groupB
Node: xKq1f-JJHD_voxussBB-x0
Elasticsearch cluster

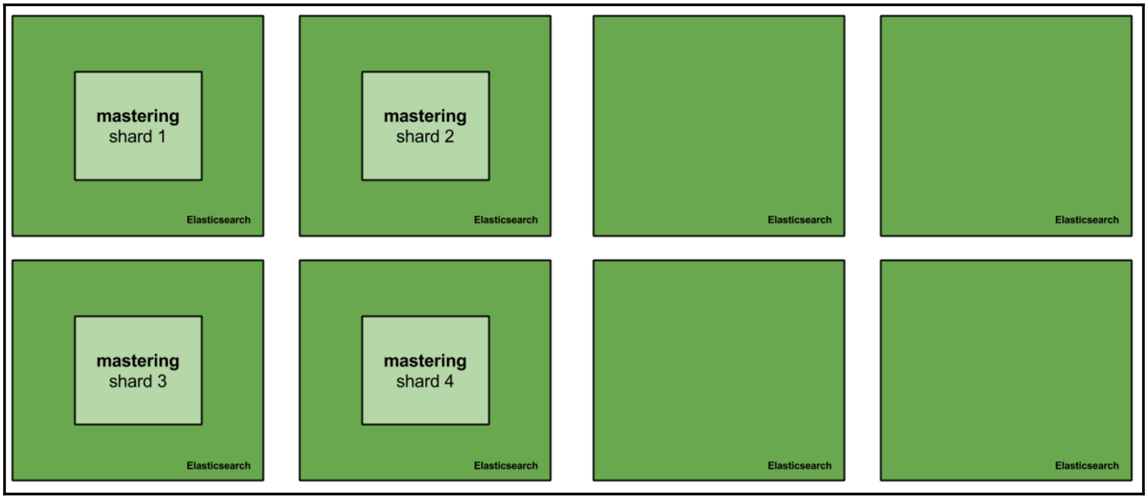

IP address: 192.168.2.1
node.tag: node1
node.group: groupA
Node: 6GVd-ktcS2um4uM4AAJQhQ
IP address: 192.168.2.2
node.tag: node2
node.group: groupA
Mastering Shard 1
Mastering Shard 0
Node: iw76Z_TaTfGRmbtCcPHF0Q
IP address: 192.168.3.1
node.tag: node3
node.group: groupB
Node: wJq0kPSHTHCovjuCsVK0-A
IP address: 192.168.3.2
node.tag: node4
node.group: groupB
Node: xKq1f-JJHD_voxussBB-x0
Elasticsearch cluster

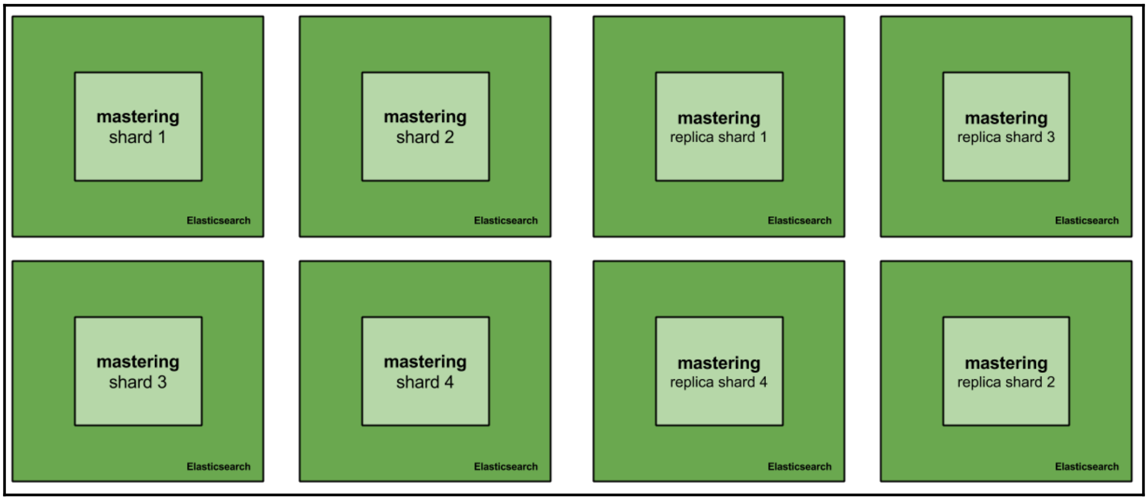
Chapter 10:

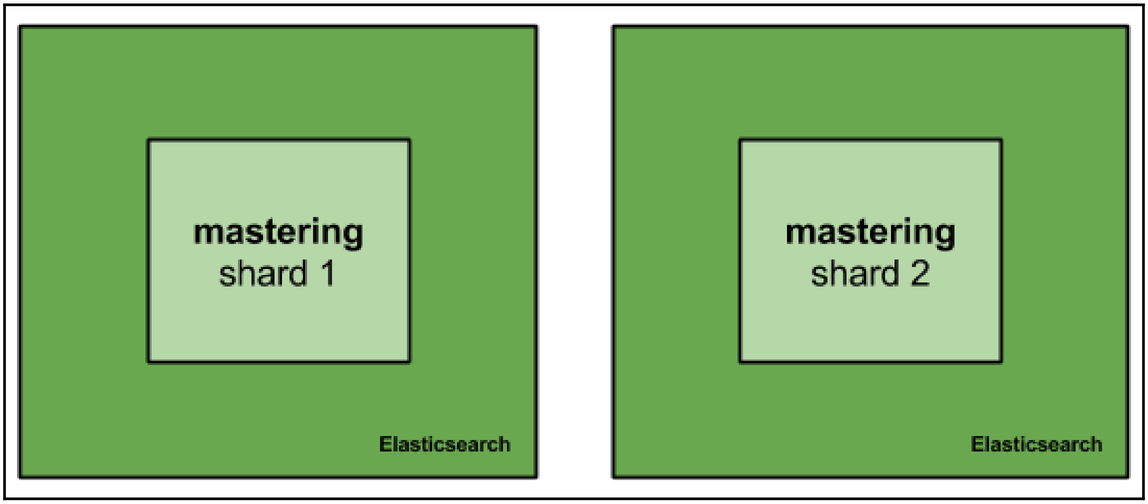


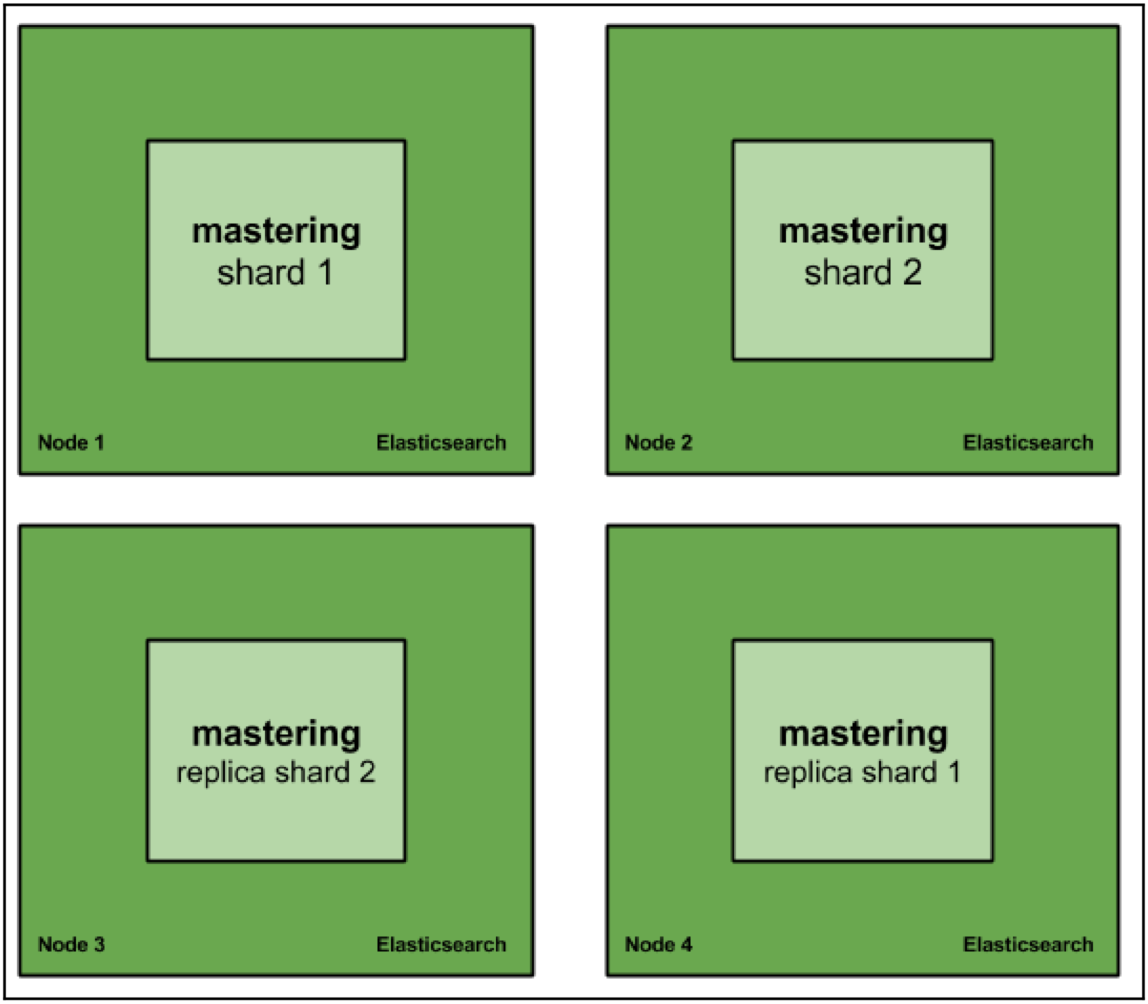
```
::: {node-1}{1NhLoN37S-OvF9QdqD40mA}{MF1iun0hRbCWtOe755PtmQ}{127.0.0.1}{127.0.0.1:9300}
   Hot threads at 2016-12-31T21:31:52.890Z, interval=500ms, busiestThreads=3, ignoreIdleThreads=true:

    4.4% (22.1ms out of 500ms) cpu usage by thread 'elasticsearch[node-1][search][T#2]'
     2/10 snapshots sharing following 36 elements
       java.lang.Throwable.fillInStackTrace(Native Method)
       java.lang.Throwable.fillInStackTrace(Throwable.java:783)
       java.lang.Throwable.<init>(Throwable.java:265)
       java.lang.Exception.<init>(Exception.java:66)
       java.io.IOException.<init>(IOException.java:58)
       org.apache.lucene.queryparser.classic.FastCharStream.refill(FastCharStream.java:72)
       org.apache.lucene.queryparser.classic.FastCharStream.readChar(FastCharStream.java:45)
       org.apache.lucene.queryparser.classic.FastCharStream.BeginToken(FastCharStream.java:80)
       org.apache.lucene.queryparser.classic.QueryParserTokenManager.getNextToken(QueryParserTokenManager.java:1055)
       org.apache.lucene.queryparser.classic.QueryParser.jj_ntk(QueryParser.java:834)
       org.apache.lucene.queryparser.classic.QueryParser.Term(QueryParser.java:401)
       org.apache.lucene.queryparser.classic.QueryParser.Clause(QueryParser.java:327)
       org.apache.lucene.queryparser.classic.QueryParser.Query(QueryParser.java:216)
       org.apache.lucene.queryparser.classic.QueryParser.TopLevelQuery(QueryParser.java:187)
       org.apache.lucene.queryparser.classic.QueryParserBase.parse(QueryParserBase.java:111)
       org.apache.lucene.queryparser.classic.MapperQueryParser.parse(MapperQueryParser.java:860)
       org.elasticsearch.index.query.QueryStringQueryBuilder.doToQuery(QueryStringQueryBuilder.java:911)
       org.elasticsearch.index.query.AbstractQueryBuilder.toQuery(AbstractQueryBuilder.java:95)
       org.elasticsearch.index.query.QueryShardContext.lambda$toQuery$1(QueryShardContext.java:311)
       org.elasticsearch.index.query.QueryShardContext$$Lambda$1339/1877300117.apply(Unknown Source)
       org.elasticsearch.index.query.QueryShardContext.toQuery(QueryShardContext.java:328)
       org.elasticsearch.index.query.QueryShardContext.toQuery(QueryShardContext.java:310)
       org.elasticsearch.search.SearchService.parseSource(SearchService.java:661)
       org.elasticsearch.search.SearchService.createContext(SearchService.java:536)
       org.elasticsearch.search.SearchService.createAndPutContext(SearchService.java:502)
       org.elasticsearch.search.SearchService.executeQueryPhase(SearchService.java:243)
       org.elasticsearch.action.search.SearchTransportService.lambda$registerRequestHandler$6(SearchTransportService.java:276)
       org.elasticsearch.action.search.SearchTransportService$$Lambda$1030/788877168.messageReceived(Unknown Source)
       org.elasticsearch.transport.TransportRequestHandler.messageReceived(TransportRequestHandler.java:33)
       org.elasticsearch.transport.RequestHandlerRegistry.processMessageReceived(RequestHandlerRegistry.java:69)
       org.elasticsearch.transport.TransportService$6.doRun(TransportService.java:548)
       org.elasticsearch.common.util.concurrent.ThreadContext$ContextPreservingAbstractRunnable.doRun(ThreadContext.java:504)
       org.elasticsearch.common.util.concurrent.AbstractRunnable.run(AbstractRunnable.java:37)
       java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
       java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
       java.lang.Thread.run(Thread.java:745)
     2/10 snapshots sharing following 10 elements
       sun.misc.Unsafe.park(Native Method)
       java.util.concurrent.locks.LockSupport.park(LockSupport.java:175)
       java.util.concurrent.LinkedTransferQueue.awaitMatch(LinkedTransferQueue.java:737)
       java.util.concurrent.LinkedTransferQueue.xfer(LinkedTransferQueue.java:647)
       java.util.concurrent.LinkedTransferQueue.take(LinkedTransferQueue.java:1269)
       org.elasticsearch.common.util.concurrent.SizeBlockingQueue.take(SizeBlockingQueue.java:161)
       java.util.concurrent.ThreadPoolExecutor.getTask(ThreadPoolExecutor.java:1067)
       java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1127)
       java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
       java.lang.Thread.run(Thread.java:745)

    4.1% (20.3ms out of 500ms) cpu usage by thread 'elasticsearch[node-1][search][T#3]'
     3/10 snapshots sharing following 2 elements
       java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
       java.lang.Thread.run(Thread.java:745)
```

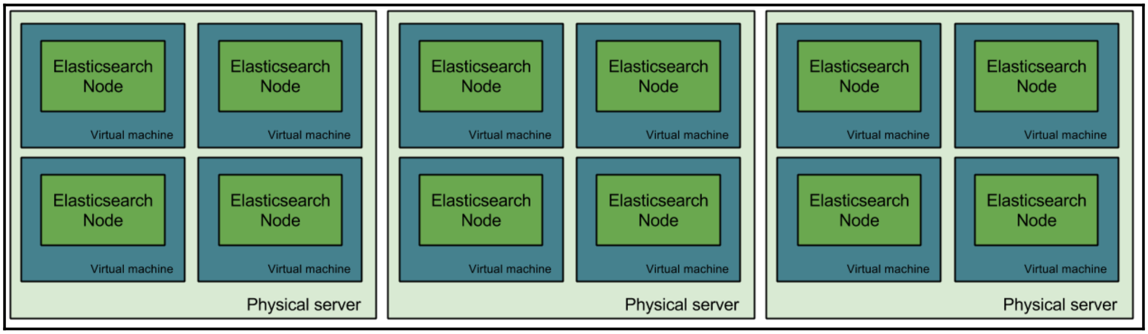

mastering
shard 1
Elasticsearch
mastering
shard 2
Elasticsearch
mastering
shard 3
Elasticsearch
mastering
shard 4
Elasticsearch

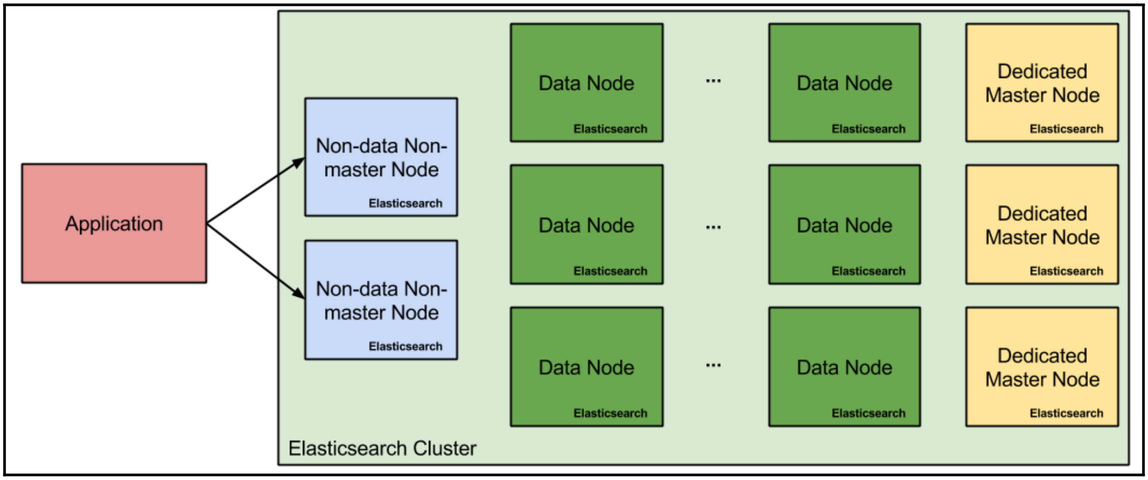

mastering
shard 1
Elasticsearch
mastering
shard 2
Elasticsearch
Elasticsearch
Elasticsearch
mastering
shard 3
Elasticsearch
mastering
shard 4
Elasticsearch
Elasticsearch
Elasticsearch

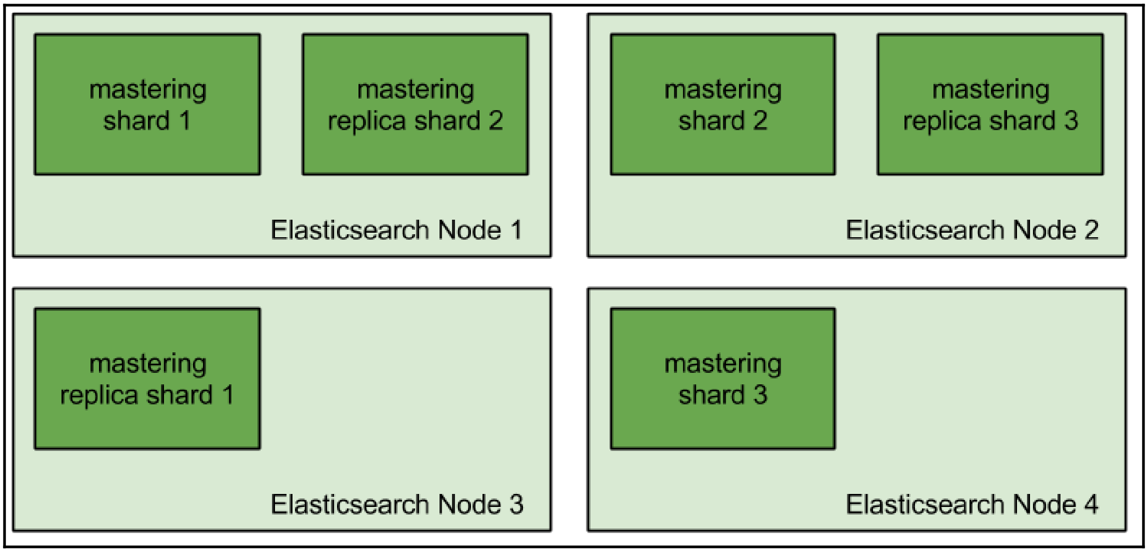

mastering
shard 1
Elasticsearch
mastering
shard 2
Elasticsearch
mastering
replica shard 1
Elasticsearch
mastering
replica shard 3
Elasticsearch
mastering
shard 3
Elasticsearch
mastering
shard 4
Elasticsearch
mastering
replica shard 4
Elasticsearch
mastering
replica shard 2
Elasticsearch

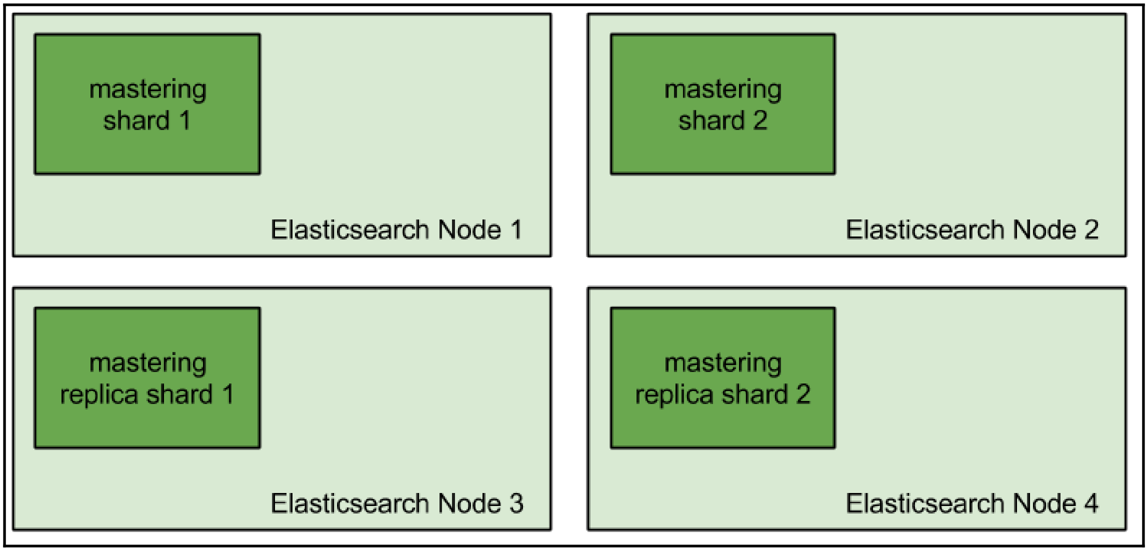

mastering
shard 1
Elasticsearch
mastering
shard 2
Elasticsearch

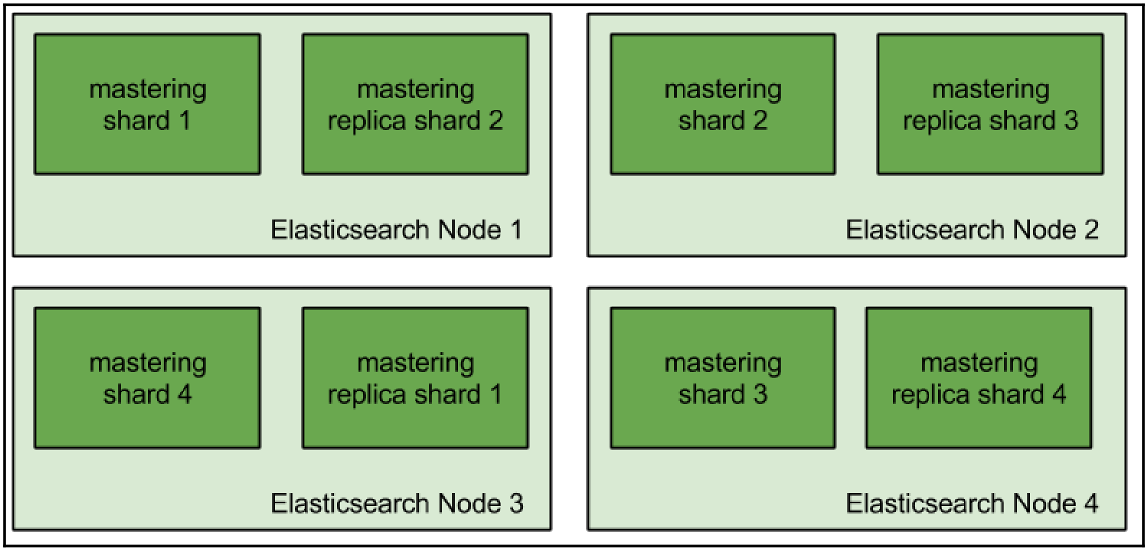

mastering
shard 1
Node 1
Elasticsearch
mastering
shard 2
Node 2
Elasticsearch
mastering
replica shard 2
Node 3
Elasticsearch
mastering
replica shard 1
Node 4
Elasticsearch

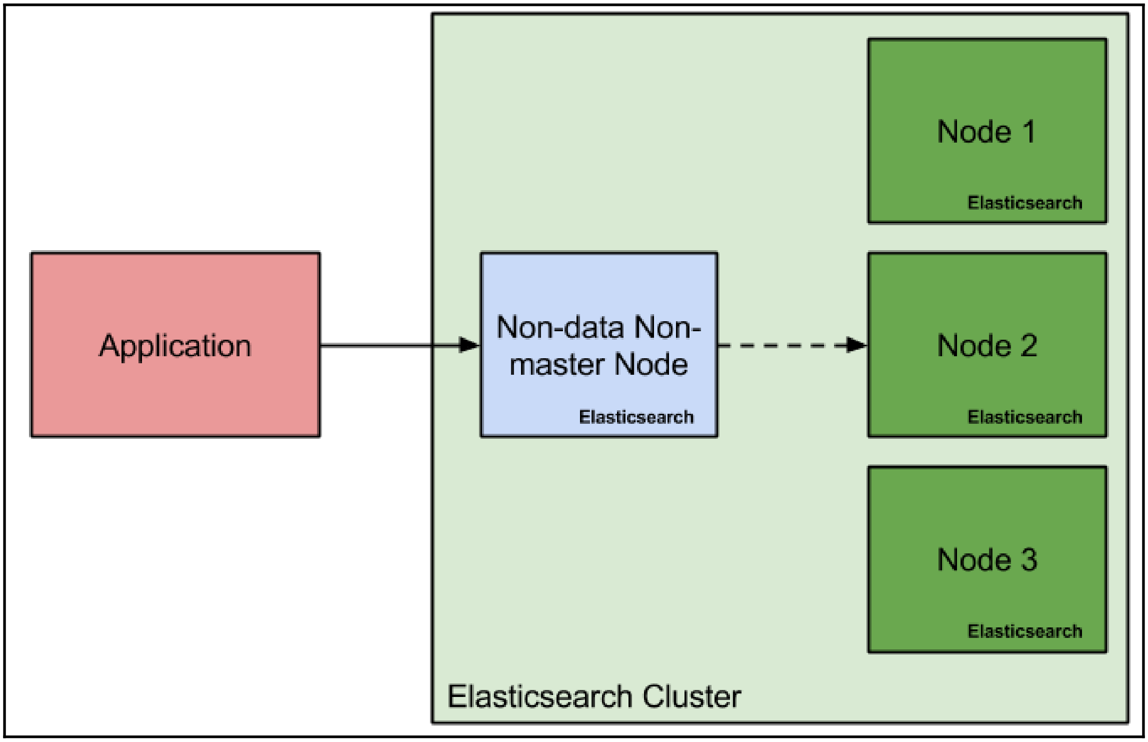

Elasticsearch Node
Virtual machine
Elasticsearch Node
Virtual machine
Elasticsearch Node
Virtual machine
Elasticsearch Node
Virtual machine
Physical server
Elasticsearch Node
Virtual machine
Elasticsearch Node
Virtual machine
Elasticsearch Node
Virtual machine
Elasticsearch Node
Virtual machine
Physical server
Elasticsearch Node
Virtual machine
Elasticsearch Node
Virtual machine
Elasticsearch Node
Virtual machine
Elasticsearch Node
Virtual machine
Physical server

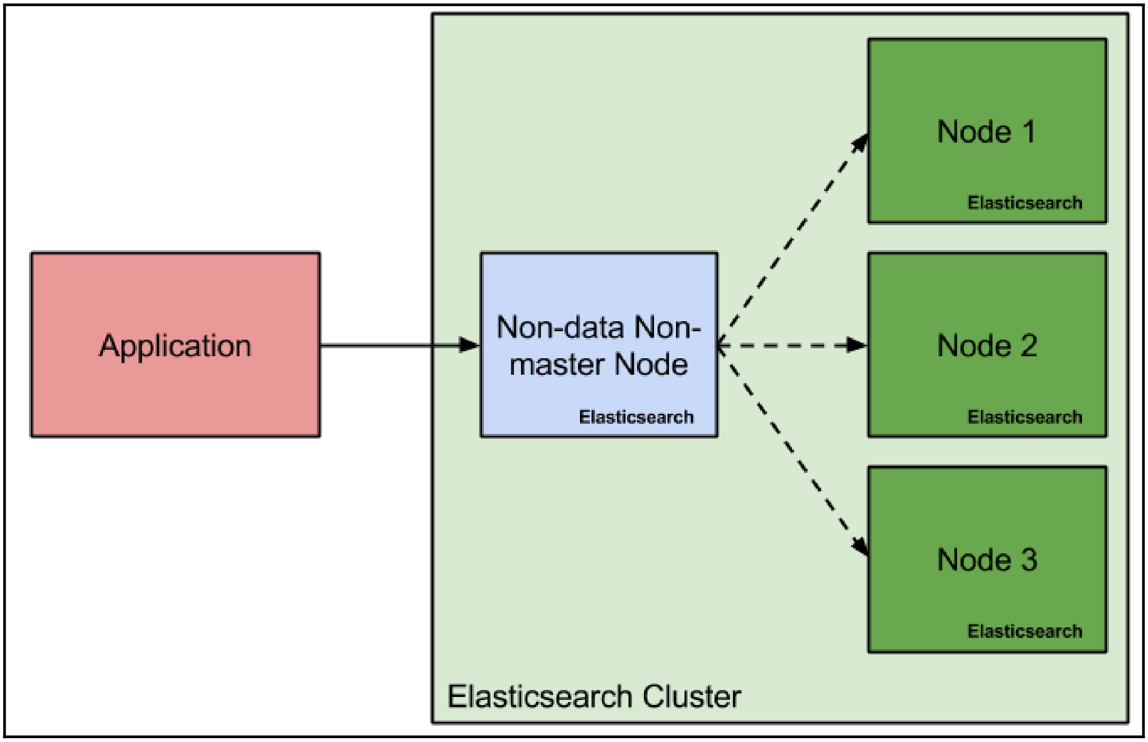

Application
Non-data Non-master Node
Elasticsearch
Non-data Non-master Node
Elasticsearch
Data Node
Elasticsearch
...
Data Node
Elasticsearch
Dedicated Master Node
Elasticsearch
Data Node
Elasticsearch
...
Data Node
Elasticsearch
Dedicated Master Node
Elasticsearch
Data Node
Elasticsearch
...
Data Node
Elasticsearch
Dedicated Master Node
Elasticsearch
Elasticsearch Cluster

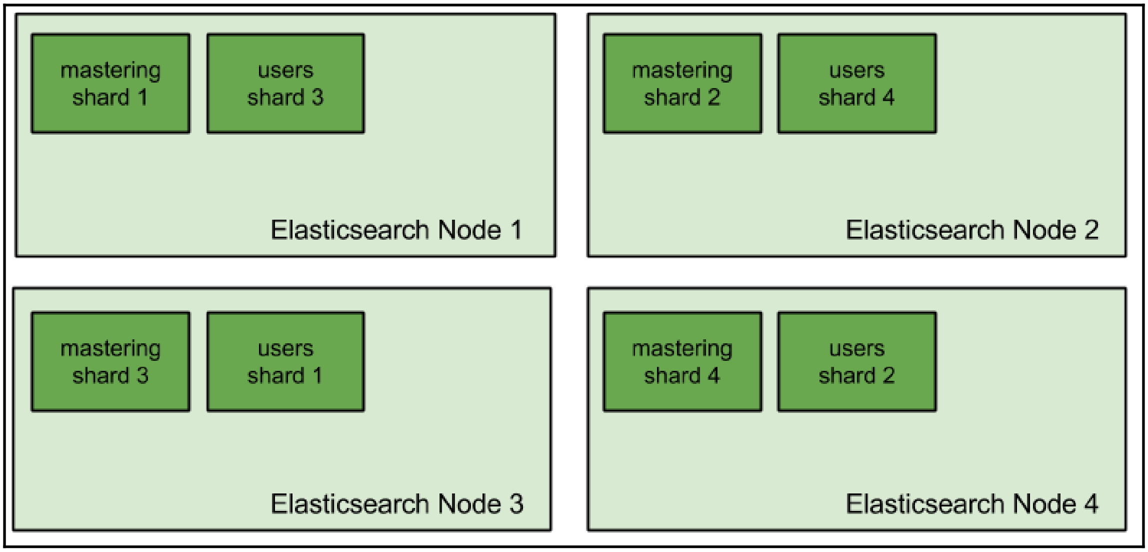

mastering shard 1
mastering replica shard 2
Elasticsearch Node 1
mastering shard 2
mastering replica shard 3
Elasticsearch Node 2
mastering replica shard 1
Elasticsearch Node 3
mastering shard 3
Elasticsearch Node 4

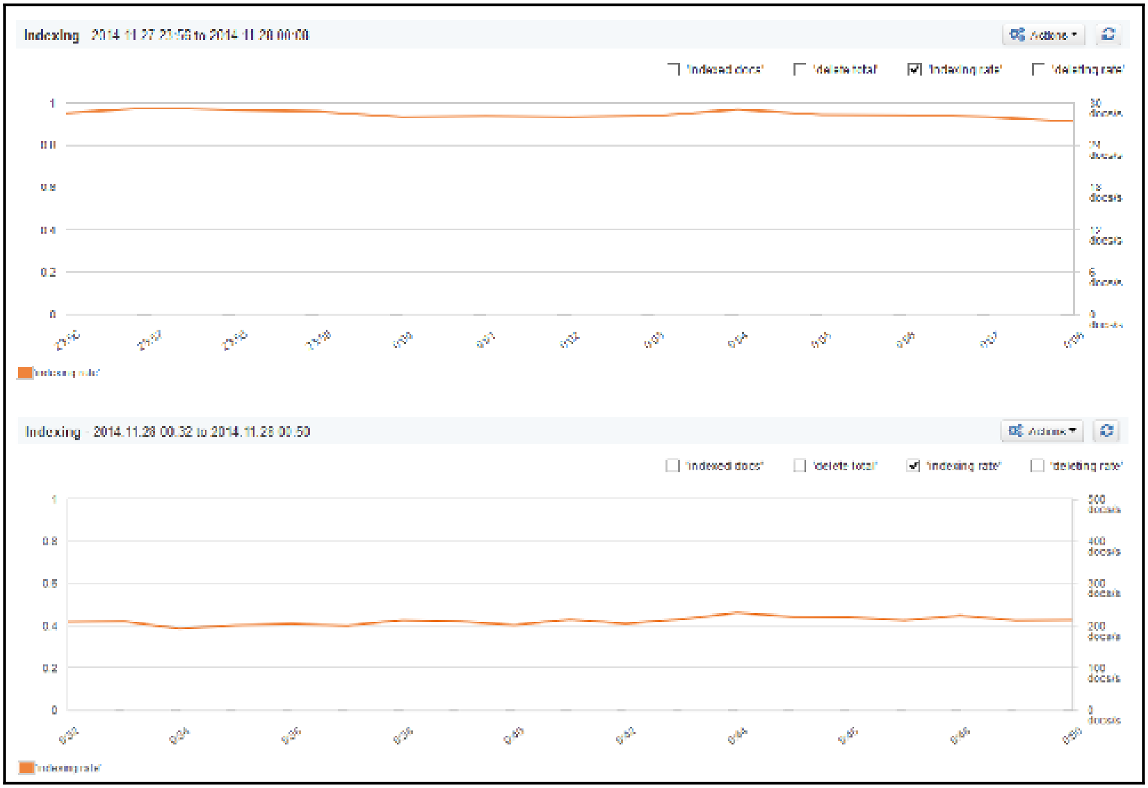

mastering shard 1
Elasticsearch Node 1
mastering shard 2
Elasticsearch Node 2
mastering replica shard 1
Elasticsearch Node 3
mastering replica shard 2
Elasticsearch Node 4


mastering shard 1
mastering replica shard 2
Elasticsearch Node 1
mastering shard 2
mastering replica shard 3
Elasticsearch Node 2
mastering shard 4
mastering replica shard 1
Elasticsearch Node 3
mastering shard 3
mastering replica shard 4
Elasticsearch Node 4


Application
Non-data Non-master Node
Elasticsearch
Node 1
Elasticsearch
Node 2
Elasticsearch
Node 3
Elasticsearch
Elasticsearch Cluster


Application
Non-data Non-master Node
Elasticsearch
Node 1
Elasticsearch
Node 2
Elasticsearch
Node 3
Elasticsearch
Elasticsearch Cluster


mastering shard 1
users shard 3
Elasticsearch Node 1
mastering shard 2
users shard 4
Elasticsearch Node 2
mastering shard 3
users shard 1
Elasticsearch Node 3
mastering shard 4
users shard 2
Elasticsearch Node 4

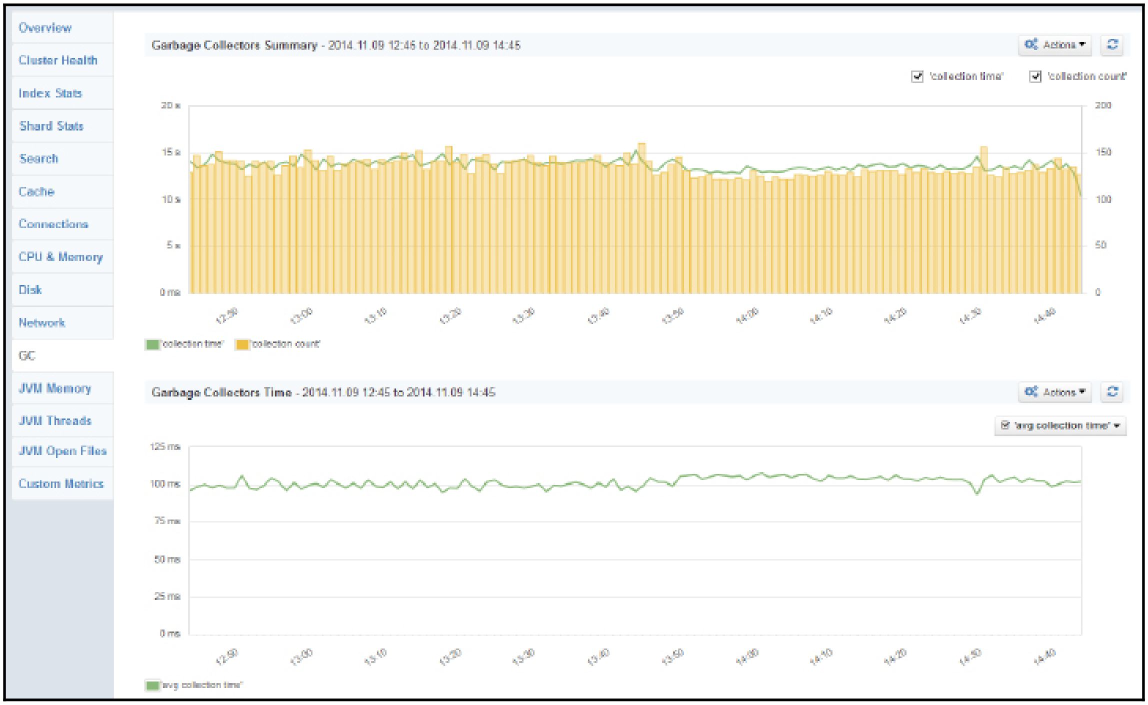


Indexing 2014.11.27 23:56 to 2014.11.28 00:08

□ 'indexed docs' □ 'delete total' ☑ 'indexing rate' □ 'deleting rate'

Indexing 2014.11.28 00:32 to 2014.11.28 00:50

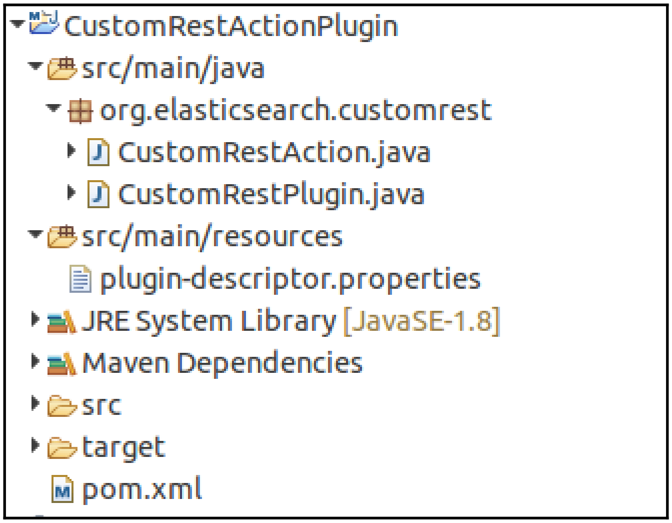
□ 'indexed docs' □ 'delete total' ☑ 'indexing rate' □ 'deleting rate'



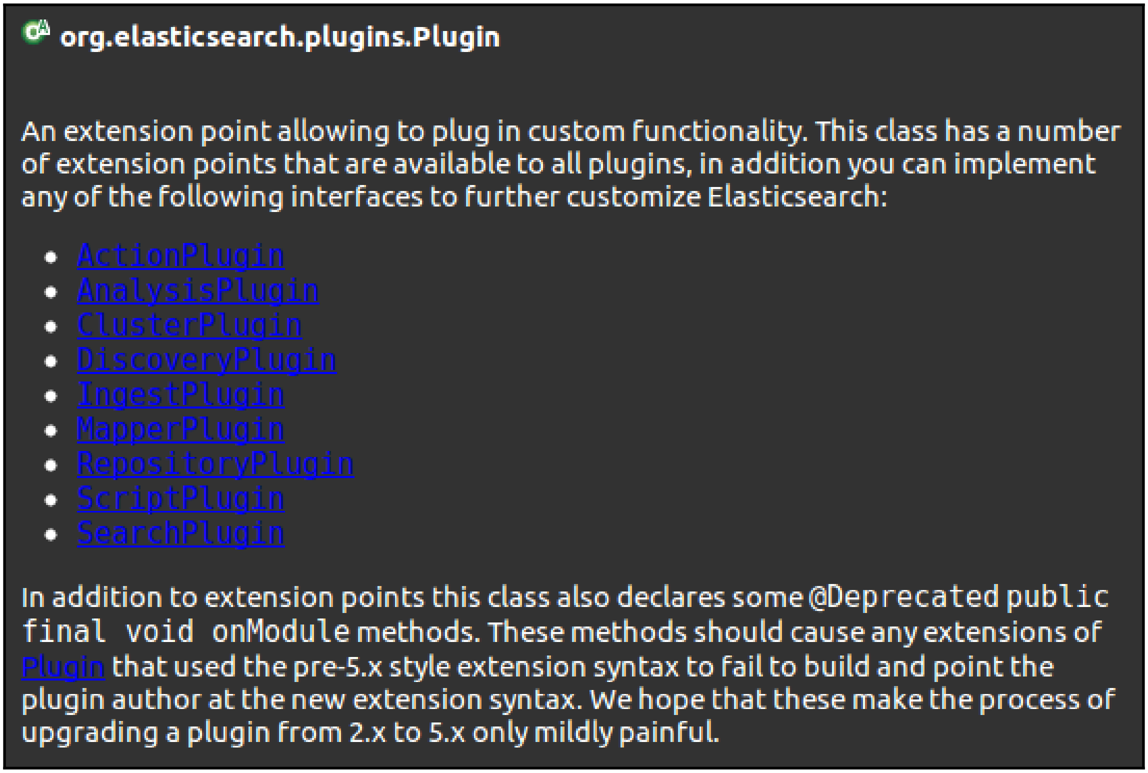
Garbage Collectors Summary - 2014.11.09 12:45 to 2014.11.09 14:45

Garbage Collectors Time - 2014.11.09 12:45 to 2014.11.09 14:45

Chapter 11:



```
CustomRestActionPlugin
  src/main/java
    org.elasticsearch.customrest
      CustomRestAction.java
      CustomRestPlugin.java
  src/main/resources
    plugin-descriptor.properties
  JRE System Library [JavaSE-1.8]
  Maven Dependencies
  src
  target
  pom.xml
```



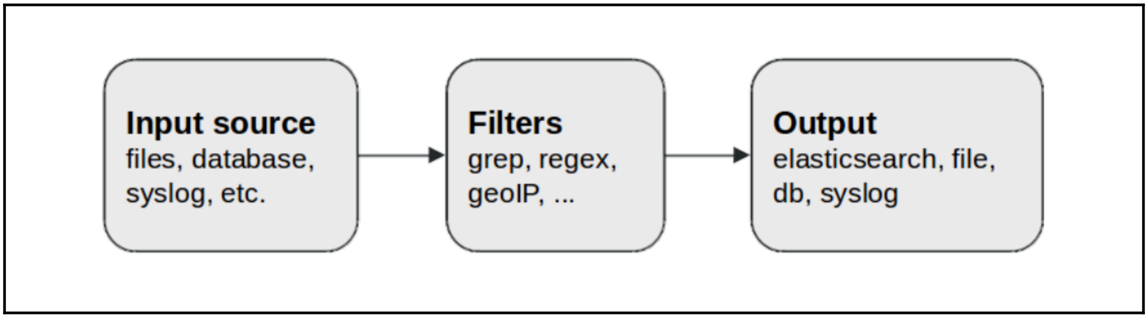
org.elasticsearch.plugins.Plugin

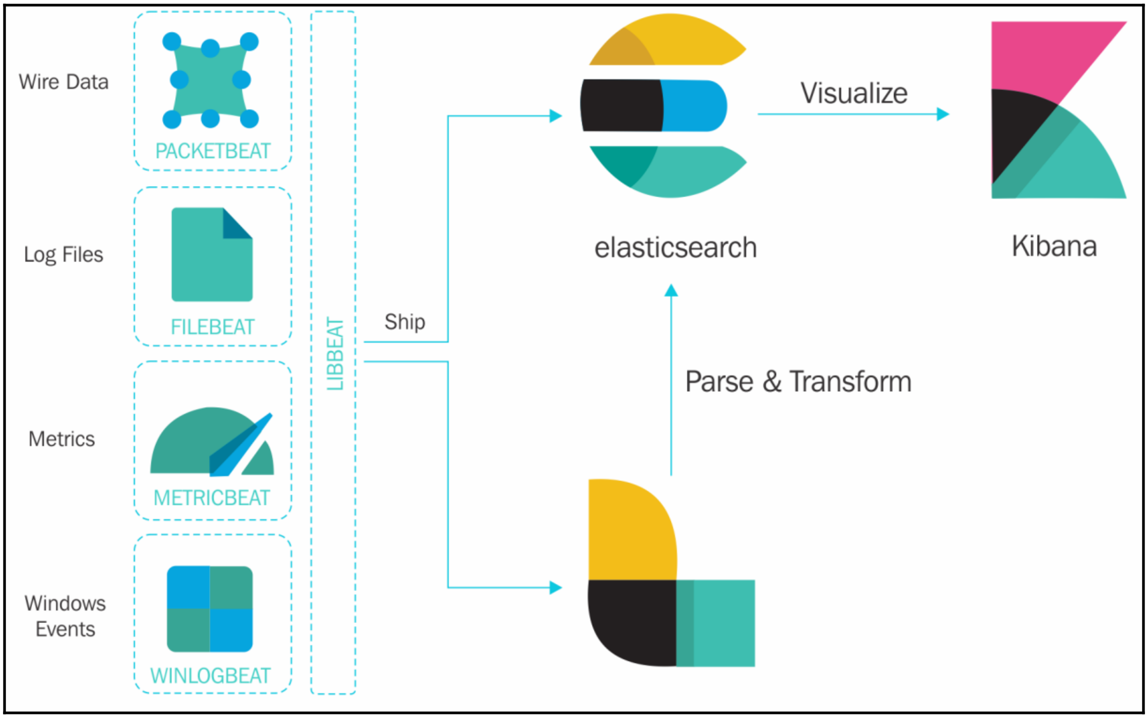
An extension point allowing to plug in custom functionality. This class has a number of extension points that are available to all plugins, in addition you can implement any of the following interfaces to further customize Elasticsearch:

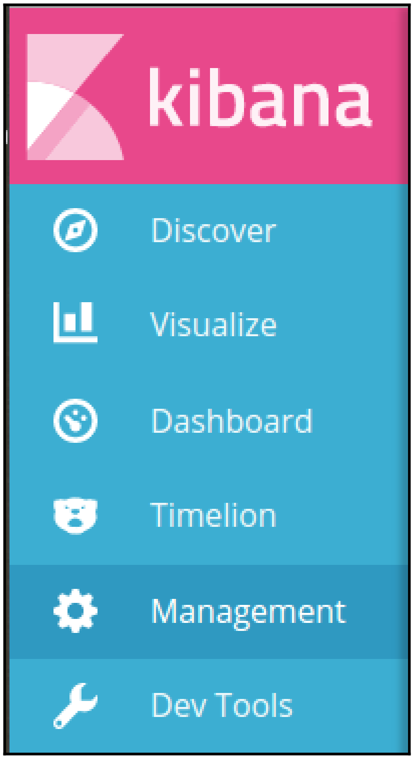
- `ActionPlugin`
- `AnalysisPlugin`
- `ClusterPlugin`
- `DiscoveryPlugin`
- `IngestPlugin`
- `MapperPlugin`
- `RepositoryPlugin`
- `ScriptPlugin`
- `SearchPlugin`

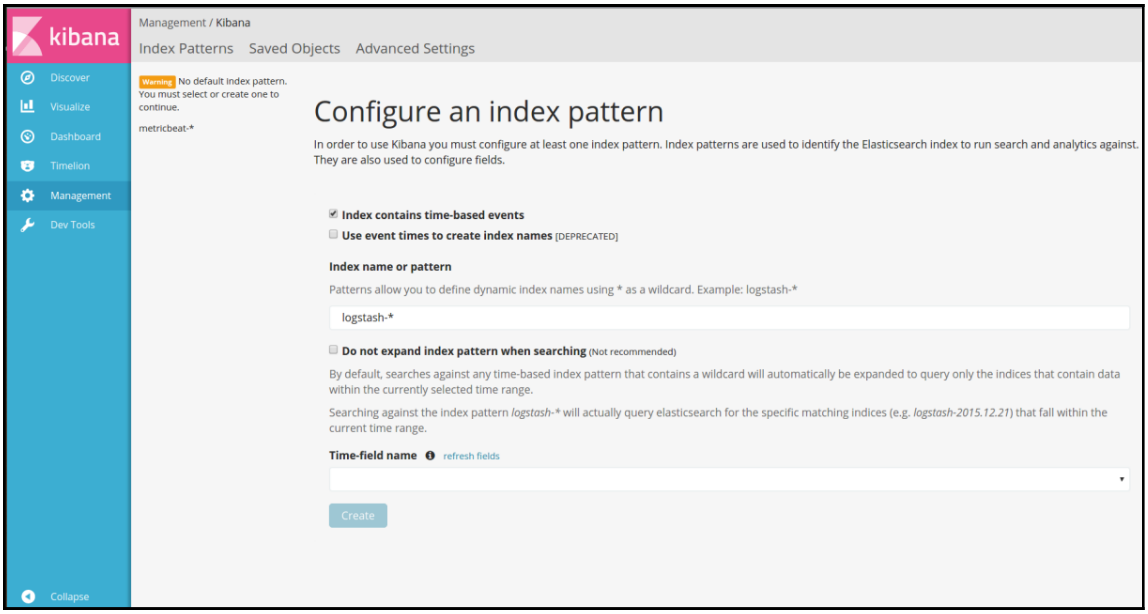
In addition to extension points this class also declares some `@Deprecated public final void onModule` methods. These methods should cause any extensions of Plugin that used the pre-5.x style extension syntax to fail to build and point the plugin author at the new extension syntax. We hope that these make the process of upgrading a plugin from 2.x to 5.x only mildly painful.

Chapter 12:


Input source
files, database,
syslog, etc.
Filters
grep, regex,
geoIP, ...
Output
elasticsearch, file,
db, syslog


Wire Data
PACKETBEAT
Log Files
FILEBEAT
Metrics
METRICBEAT
Windows
Events
WINLOGBEAT
LIBBEAT
Ship
elasticsearch
Visualize
Kibana
Parse & Transform





Warning No default index pattern. You must select or create one to continue.

metricbeat-*

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** [DEPRECATED]

Index name or pattern

Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

logstash-*

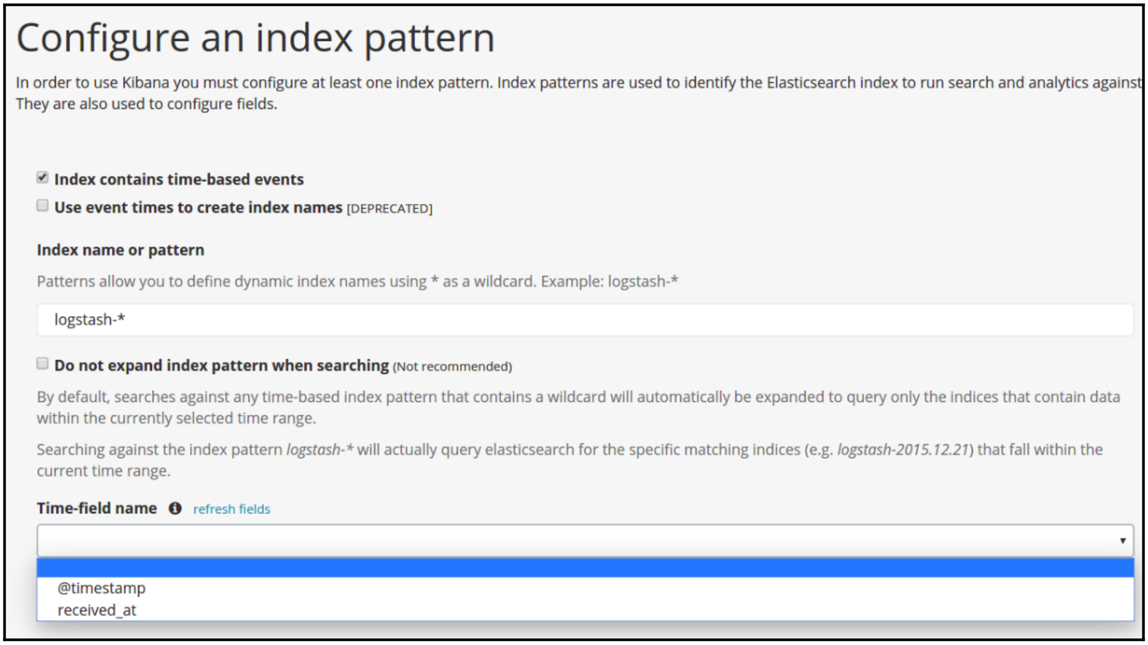
□ **Do not expand index pattern when searching** (Not recommended)

By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

Searching against the index pattern *logstash-** will actually query elasticsearch for the specific matching indices (e.g. *logstash-2015.12.21*) that fall within the current time range.

Time-field name refresh fields

Create



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** [DEPRECATED]

Index name or pattern

Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

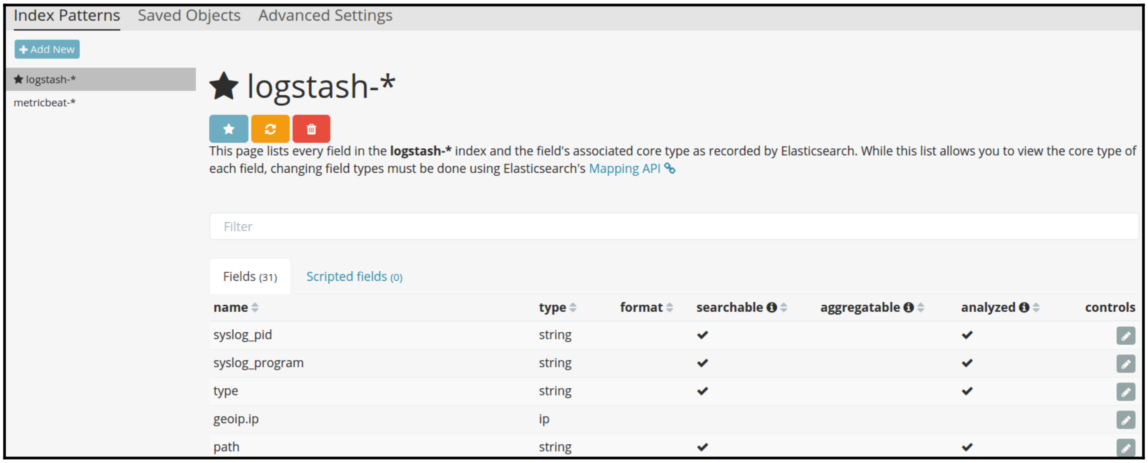
logstash-*

□ **Do not expand index pattern when searching** (Not recommended)

By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

Searching against the index pattern *logstash-** will actually query elasticsearch for the specific matching indices (e.g. *logstash-2015.12.21*) that fall within the current time range.

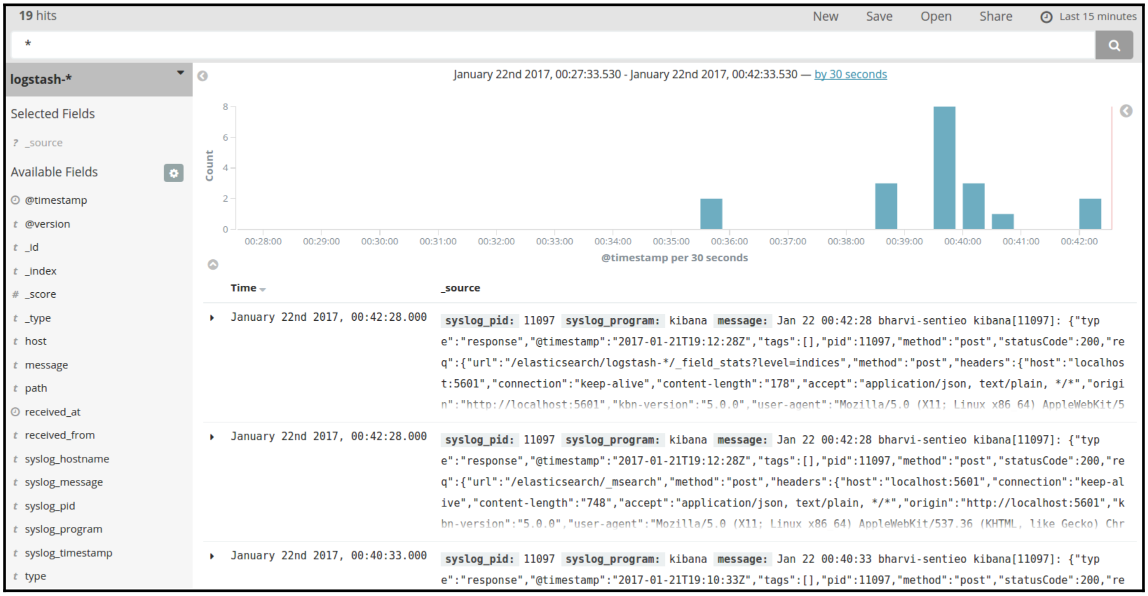
Time-field name ℹ refresh fields



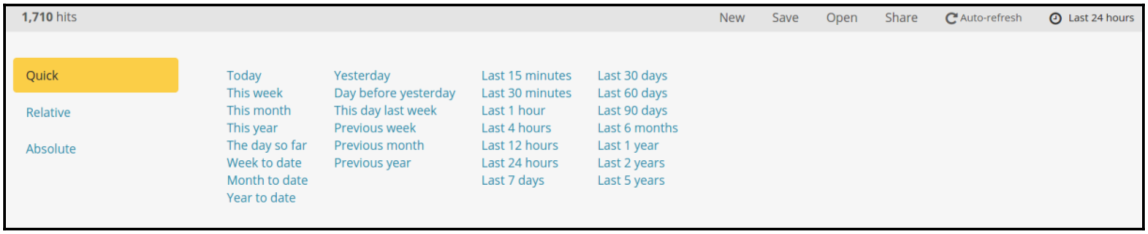
★ logstash-*

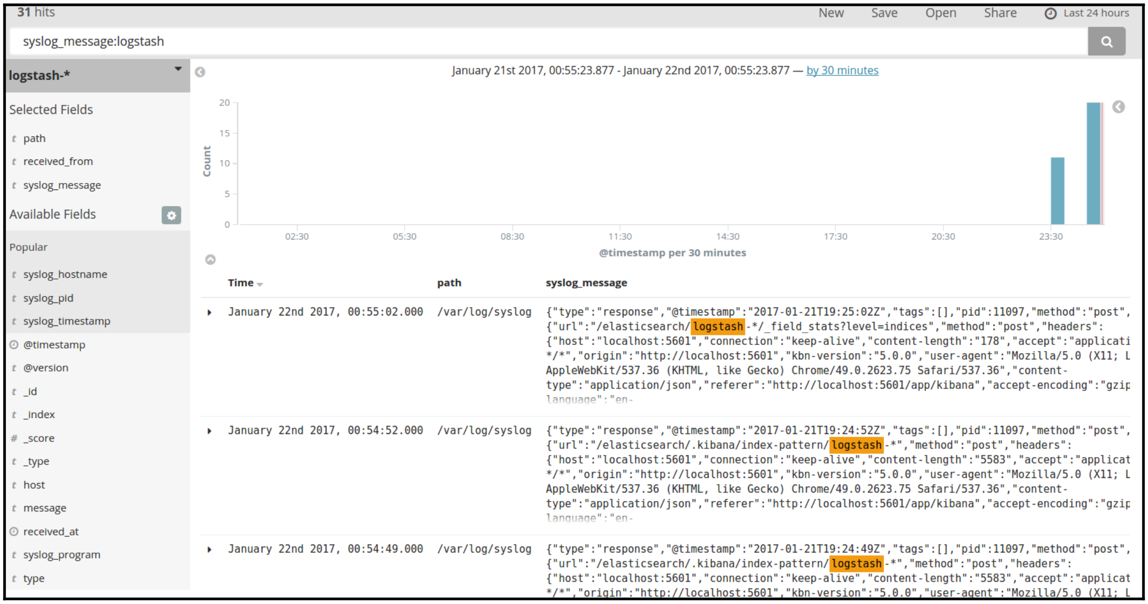
This page lists every field in the **logstash-*** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API

name	type	format	searchable ℹ	aggregatable ℹ	analyzed ℹ	controls
syslog_pid	string		✓		✓	✎
syslog_program	string		✓		✓	✎
type	string		✓		✓	✎
geoip.ip	ip					✎
path	string		✓		✓	✎

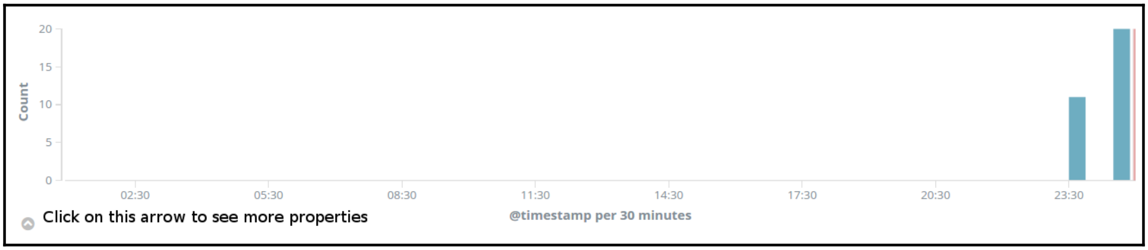


```
January 22nd 2017, 00:42:28.000  syslog_pid: 11097 syslog_program: kibana message: Jan 22 00:42:28 bharvi-sentieo kibana[11097]: {"typ
                                 e":"response","@timestamp":"2017-01-21T19:12:28Z","tags":[],"pid":11097,"method":"post","statusCode":200,"re
                                 q":{"url":"/elasticsearch/logstash-*/_field_stats?level=indices","method":"post","headers":{"host":"localhos
                                 t:5601","connection":"keep-alive","content-length":"178","accept":"application/json, text/plain, */*","origi
                                 n":"http://localhost:5601","kbn-version":"5.0.0","user-agent":"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/5

January 22nd 2017, 00:42:28.000  syslog_pid: 11097 syslog_program: kibana message: Jan 22 00:42:28 bharvi-sentieo kibana[11097]: {"typ
                                 e":"response","@timestamp":"2017-01-21T19:12:28Z","tags":[],"pid":11097,"method":"post","statusCode":200,"re
                                 q":{"url":"/elasticsearch/_msearch","method":"post","headers":{"host":"localhost:5601","connection":"keep-al
                                 ive","content-length":"748","accept":"application/json, text/plain, */*","origin":"http://localhost:5601","k
                                 bn-version":"5.0.0","user-agent":"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chr

January 22nd 2017, 00:40:33.000  syslog_pid: 11097 syslog_program: kibana message: Jan 22 00:40:33 bharvi-sentieo kibana[11097]: {"typ
                                 e":"response","@timestamp":"2017-01-21T19:10:33Z","tags":[],"pid":11097,"method":"post","statusCode":200,"re
```

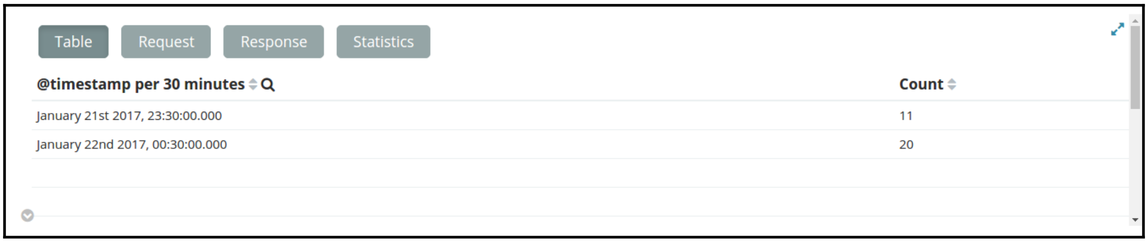




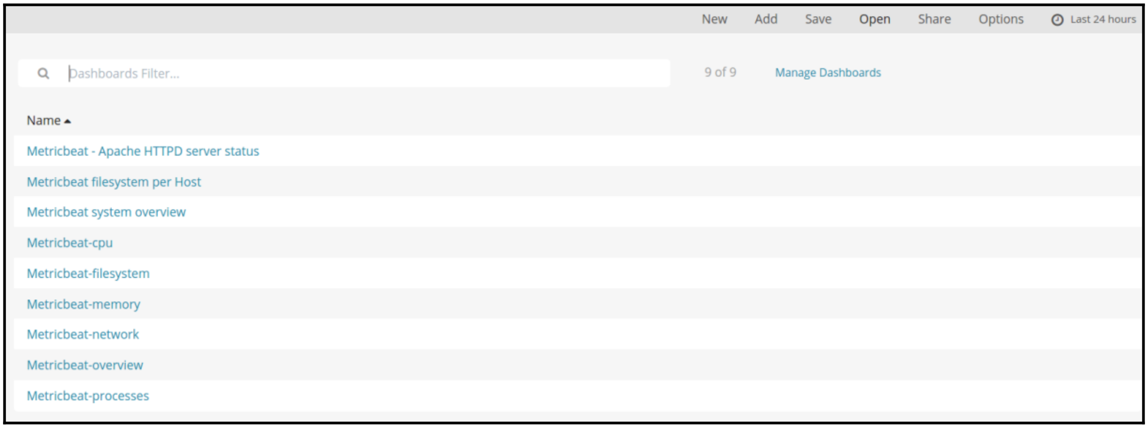
```
Time      path           syslog_message
January 22nd 2017, 00:55:02.000  /var/log/syslog  {"type":"response","@timestamp":"2017-01-21T19:25:02Z","tags":[],"pid":11097,"method":"post",
                                                  {"url":"/elasticsearch/logstash-*/_field_stats?level=indices","method":"post","headers":
                                                  {"host":"localhost:5601","connection":"keep-alive","content-length":"178","accept":"applicati
                                                  */*","origin":"http://localhost:5601","kbn-version":"5.0.0","user-agent":"Mozilla/5.0 (X11; L
                                                  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36","content-
                                                  type":"application/json","referer":"http://localhost:5601/app/kibana","accept-encoding":"gzip
                                                  language":"en-
January 22nd 2017, 00:54:52.000  /var/log/syslog  {"type":"response","@timestamp":"2017-01-21T19:24:52Z","tags":[],"pid":11097,"method":"post",
                                                  {"url":"/elasticsearch/.kibana/index-pattern/logstash-*","method":"post","headers":
                                                  {"host":"localhost:5601","connection":"keep-alive","content-length":"5583","accept":"applicat
                                                  */*","origin":"http://localhost:5601","kbn-version":"5.0.0","user-agent":"Mozilla/5.0 (X11; L
                                                  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36","content-
                                                  type":"application/json","referer":"http://localhost:5601/app/kibana","accept-encoding":"gzip
                                                  language":"en-
January 22nd 2017, 00:54:49.000  /var/log/syslog  {"type":"response","@timestamp":"2017-01-21T19:24:49Z","tags":[],"pid":11097,"method":"post",
                                                  {"url":"/elasticsearch/.kibana/index-pattern/logstash-*","method":"post","headers":
                                                  {"host":"localhost:5601","connection":"keep-alive","content-length":"5583","accept":"applicat
                                                  */*","origin":"http://localhost:5601","kbn-version":"5.0.0","user-agent":"Mozilla/5.0 (X11; L
```



Click on this arrow to see more properties

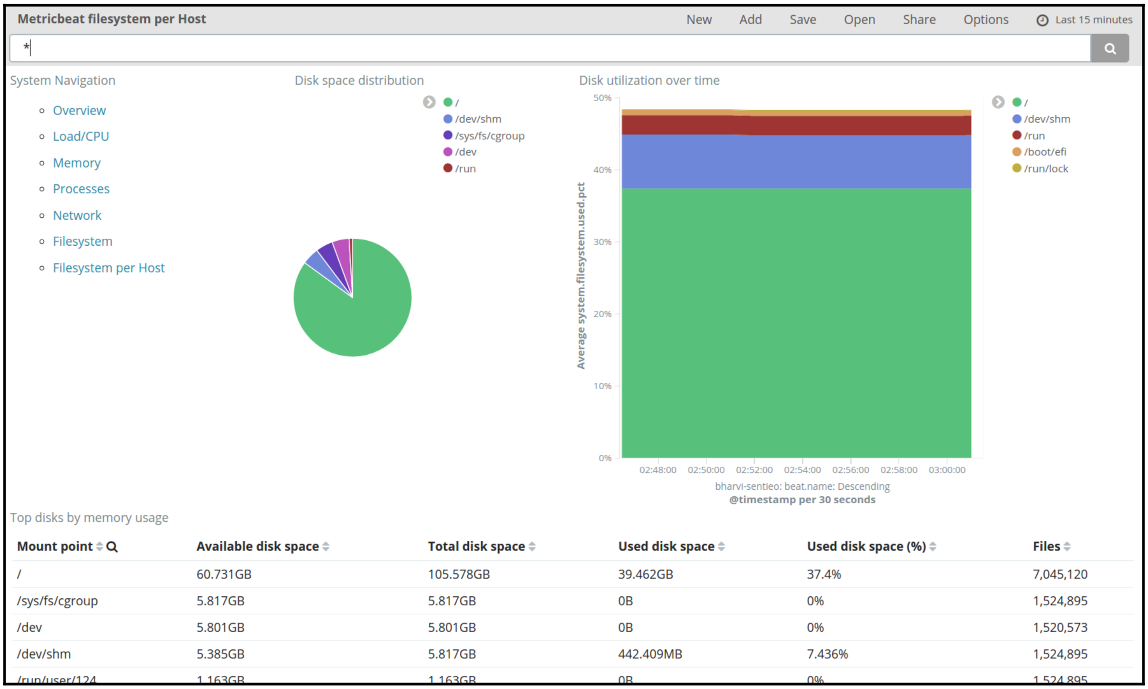


@timestamp per 30 minutes	Count
January 21st 2017, 23:30:00.000	11
January 22nd 2017, 00:30:00.000	20



Name ▲

- Metricbeat - Apache HTTPD server status
- Metricbeat filesystem per Host
- Metricbeat system overview
- Metricbeat-cpu
- Metricbeat-filesystem
- Metricbeat-memory
- Metricbeat-network
- Metricbeat-overview
- Metricbeat-processes


Metricbeat filesystem per Host

System Navigation

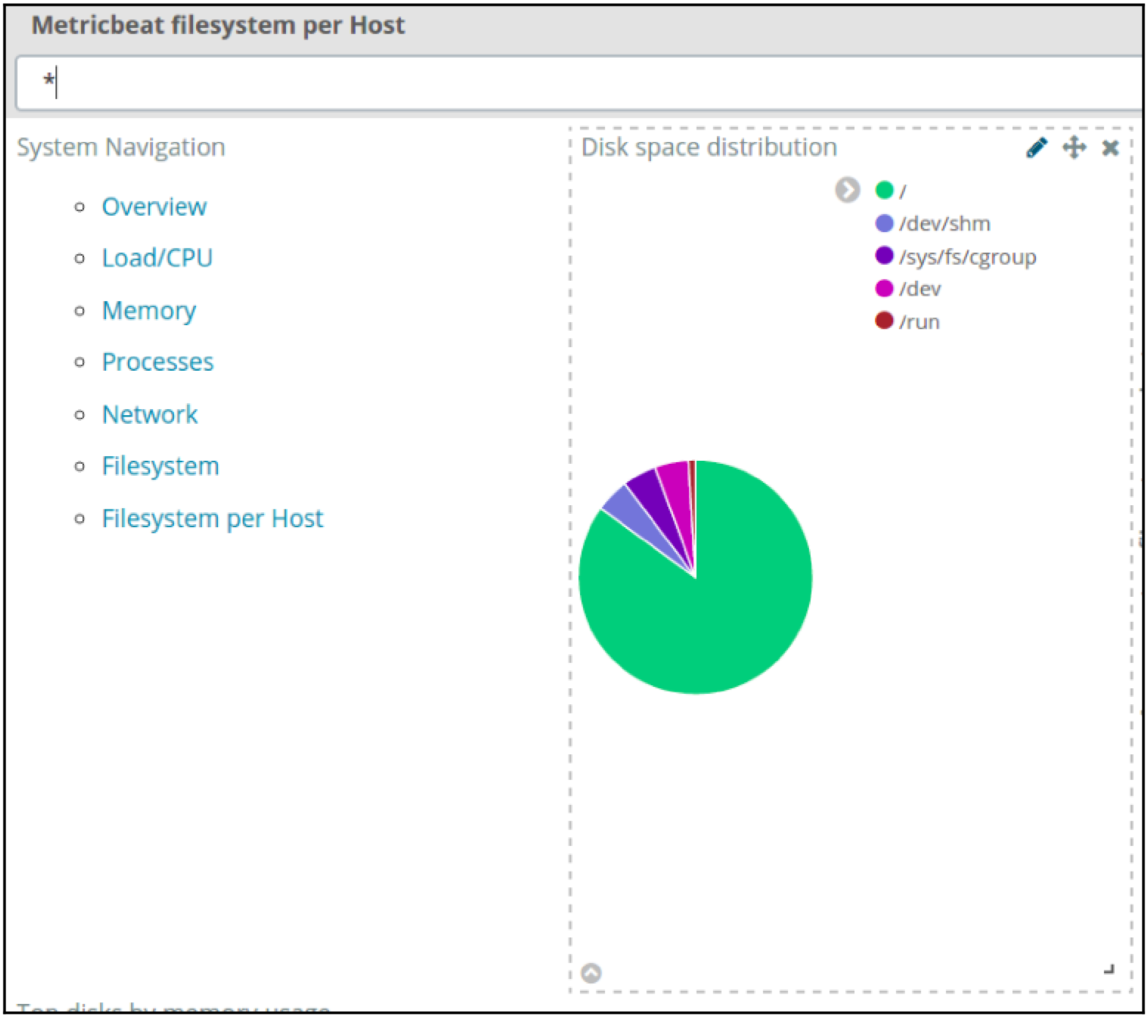
- Overview
- Load/CPU
- Memory
- Processes
- Network
- Filesystem
- Filesystem per Host

Disk space distribution

Disk utilization over time

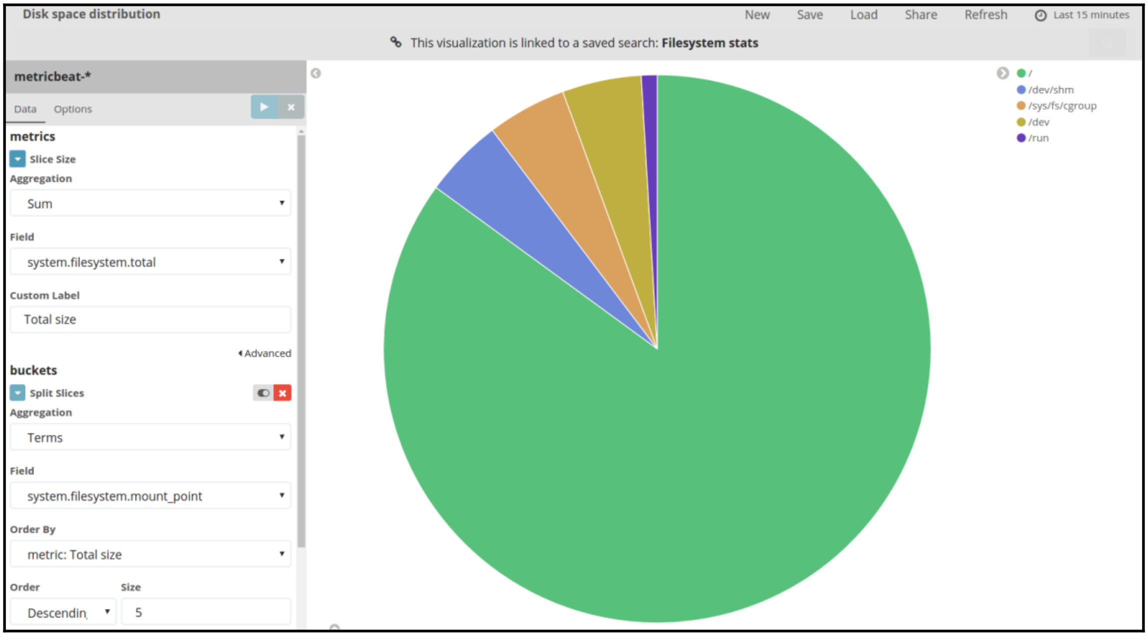
Top disks by memory usage

Mount point	Available disk space	Total disk space	Used disk space	Used disk space (%)	Files
/	60.731GB	105.578GB	39.462GB	37.4%	7,045,120
/sys/fs/cgroup	5.817GB	5.817GB	0B	0%	1,524,895
/dev	5.801GB	5.801GB	0B	0%	1,520,573
/dev/shm	5.385GB	5.817GB	442.409MB	7.436%	1,524,895
/run/user/124	1.163GB	1.163GB	0B	0%	1,524,895



Metricbeat filesystem per Host

*



metrics

Slice Size

Aggregation: Sum

Field: system.filesystem.total

Custom Label: Total size

Advanced

buckets

Split Slices

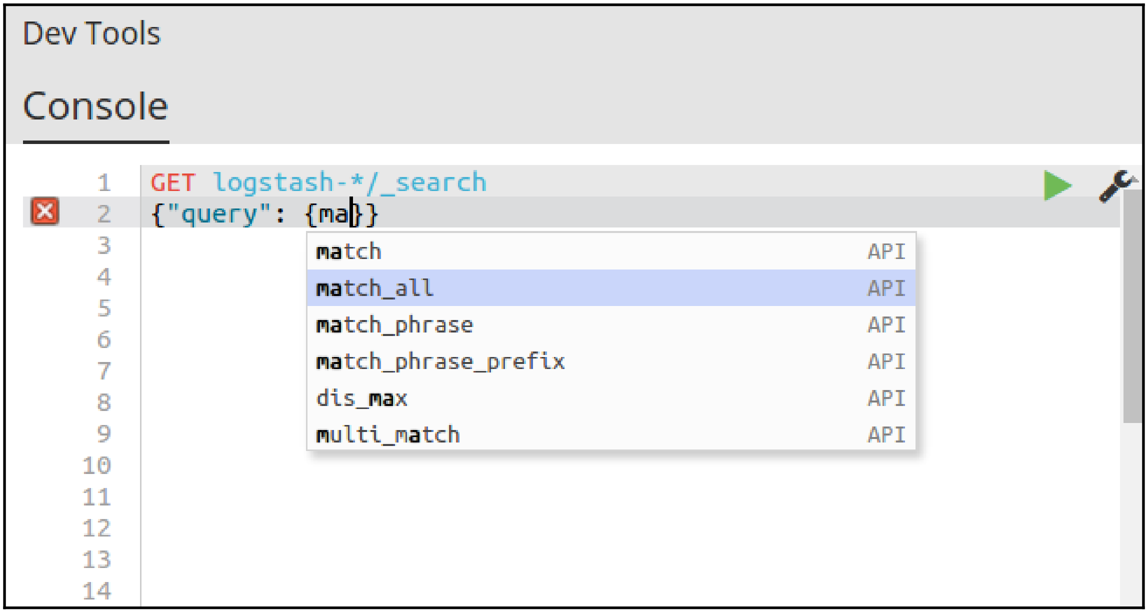
Aggregation: Terms

Field: system.filesystem.mount_point

Order By: metric: Total size

Order: Descendin

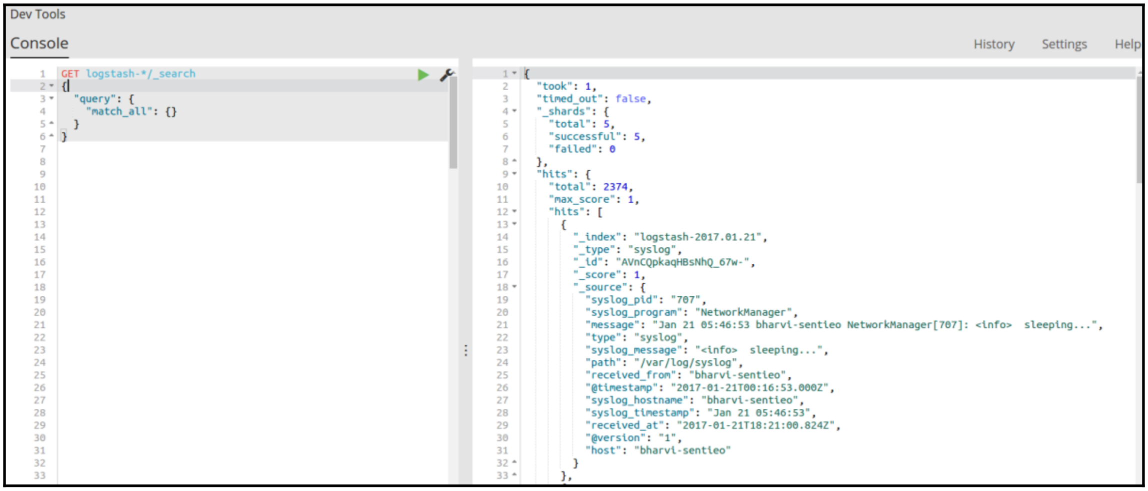
Size: 5



Dev Tools

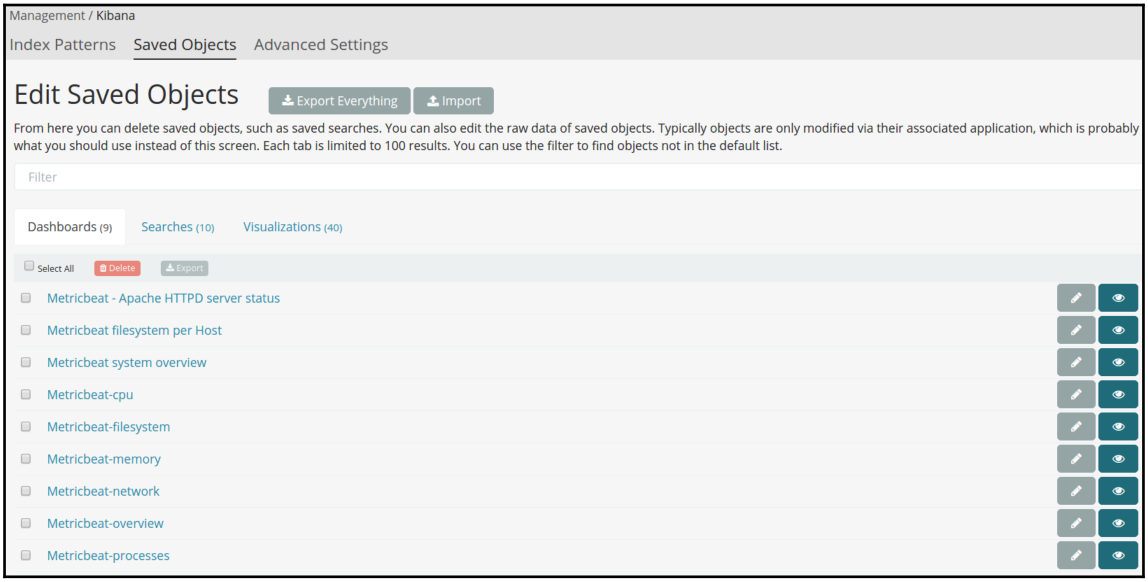
Console

```
GET logstash-*/_search
{"query": {ma}}
```



```
GET logstash-*/_search
{
  "query": {
    "match_all": {}
  }
}
```

```
{
  "took": 1,
  "timed_out": false,
  "_shards": {
    "total": 5,
    "successful": 5,
    "failed": 0
  },
  "hits": {
    "total": 2374,
    "max_score": 1,
    "hits": [
      {
        "_index": "logstash-2017.01.21",
        "_type": "syslog",
        "_id": "AVnCQpkaqHBsNhQ_67w-",
        "_score": 1,
        "_source": {
          "syslog_pid": "707",
          "syslog_program": "NetworkManager",
          "message": "Jan 21 05:46:53 bharvi-sentieo NetworkManager[707]: <info>  sleeping...",
          "type": "syslog",
          "syslog_message": "<info>  sleeping...",
          "path": "/var/log/syslog",
          "received_from": "bharvi-sentieo",
          "@timestamp": "2017-01-21T00:16:53.000Z",
          "syslog_hostname": "bharvi-sentieo",
          "syslog_timestamp": "Jan 21 05:46:53",
          "received_at": "2017-01-21T18:21:00.824Z",
          "@version": "1",
          "host": "bharvi-sentieo"
        }
      },
```



Edit Saved Objects

From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen. Each tab is limited to 100 results. You can use the filter to find objects not in the default list.

☐ Metricbeat - Apache HTTPD server status
☐ Metricbeat filesystem per Host
☐ Metricbeat system overview
☐ Metricbeat-cpu
☐ Metricbeat-filesystem
☐ Metricbeat-memory
☐ Metricbeat-network
☐ Metricbeat-overview
☐ Metricbeat-processes