

ELK homework.

Configuring kibana and elastic search.

I downloaded both elastic search and kibana, versions 6.5.1 from the official website.

Here's elastic search running:

```
maria_dev@sandbox-hdp:~$ cat /opt/elasticsearch/logs/gc.log
[2018-11-29T15:29:40S][INFO ][o.e.n.Node ][yjcspzp] version[6.5.1], pid[16792], build[default/tar/8c58350/2018-11-16T02:22:42.18Z257Z], OS[Linux/4.17.2-1.el7.elrepo.x86_64/amd64], JVM[Oracle Corporation/OpenJDK 64-Bit Server VM/1.8.0_175-171-b18]
[2018-11-29T15:29:40S][INFO ][o.e.n.Node ][yjcspzp] JVM arguments [-Xmsg, -Xmxg, -XX:UseConcMarkSweepGC, -XX:CMSInitiatingOccupancyFraction=75, -XX:UseCMSInitiatingOccupancyOnly, -XX:+AlwaysPreTouch, -Xssm, -Djava.net.headers=, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-DattStackTraceAfterThrow, -Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=true, -Dio.netty.recycler.maxCapacityPerThread=, -Dlog4j.shutdownHookEnabled=false, -Dlog4j.disable.jmx=true, -Djava.io.tmpdir=/tmp/elasticsearch-qlh0uqV, -XX:-HeapDumpOnOutOfMemoryError, -XX:HeapDumpPath=data, -XX:ErrorFile=logs/es_err_pid6g.log, -XX:PrintGCDetails, -XX:PrintGCDateStamps, -XX:+PrintGCTimeStamps, -XX:PrintGCApplicationStoppedTime, -Xloggc:logs/gc.log, -XX:UseG1GCLogFileRotation, -XX:NumberOfGCLogFiles=32, -XX:G1LogFileSize=6m, -Des.path.home=/opt/elasticsearch, -Des.path.conf=/opt/elasticsearch/config, -Des.distribution.flavor=default, -Des.distribution.type=tar]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [aggs-matrix-stats]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [analysis-common]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [ingest-common]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [lang-expression]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [lang-mustache]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [lang-painless]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [mapper-extras]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [parent-join]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [percolator]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [rank-eval]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [reindex]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [repository-url]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [transport-netty4]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [tribe]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-ccr]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-core]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-deprecation]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-graph]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-logstash]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-ml]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-monitoring]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-rollback]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-security]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-sql]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-upgrade]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] loaded module [x-pack-watcher]
[2018-11-29T15:29:40S][INFO ][o.e.p.PluginsService ][yjcspzp] no plugins loaded
[2018-11-29T15:29:40S][INFO ][o.e.x.s.a.s.FileBasedStore][yjcspzp] parsed [0] roles from file [/opt/elasticsearch/config/roles.yml]
[2018-11-29T15:29:40S][INFO ][o.e.x.s.a.s.ClusterSettingsModule][yjcspzp] Using REST wrapper from plugin org.elasticsearch.xpack.security.Security
[2018-11-29T15:29:40S][INFO ][o.e.d.DiscoveryModule ][yjcspzp] using discovery type [zen] and host providers [settings]
[2018-11-29T15:30:15S][INFO ][o.e.n.Node ][yjcspzp] initialized
[2018-11-29T15:30:15S][INFO ][o.e.n.Node ][yjcspzp] starting ...
[2018-11-29T15:30:15S][INFO ][o.e.t.TransportService ][yjcspzp] publish_address [127.0.0.1:9300], bound_addresses [127.0.0.1:9300]
[2018-11-29T15:30:15S][INFO ][o.e.h.BootstrapChecks ][yjcspzp] max virtual memory areas vm.max_map_count [65536] is too low, increase to at least [262144]
[2018-11-29T15:30:15S][INFO ][o.e.c.s.MasterService ][yjcspzp] zen-disco-elected-as-master ([0] nodes joined), reason: new_master [yjcspzp_QdCobuFsZtI-Q](hSzgTxX58iugVvghQhQ)(127.0.0.1)(127.0.0.1:9300)[ml.machine_memory=1478999040, spack_installed=true, ml_max_open_jobs=20, ml_enabled=true]
[2018-11-29T15:30:15S][INFO ][o.e.c.s.ClusterApplierService ][yjcspzp] new_master [yjcspzp_QdCobuFsZtI-Q](hSzgTxX58iugVvghQhQ)(127.0.0.1)(127.0.0.1:9300)[ml.machine_memory=1478999040, spack_installed=true, ml_max_open_jobs=20, ml_enabled=true], reason: apply cluster state (from master (master [yjcspzp_QdCobuFsZtI-Q](hSzgTxX58iugVvghQhQ)(127.0.0.1)(127.0.0.1:9300)[ml.machine_memory=1478999040, spack_installed=true, ml_max_open_jobs=20, ml_enabled=true] committed version [1] source [zen-disco-elected-as-master ([0] nodes joined)])
[2018-11-29T15:30:15S][INFO ][o.e.x.s.t.n.SecurityMetadataService][yjcspzp] publish_address [127.0.0.1:9300], bound_addresses [127.0.0.1:9300]
[2018-11-29T15:30:15S][INFO ][o.e.n.Node ][yjcspzp] started
[2018-11-29T15:30:15S][INFO ][o.e.c.s.ClusterSettings ][yjcspzp] updating [xpack.monitoring.collection.enabled] from [false] to [true]
[2018-11-29T15:30:15S][INFO ][o.e.x.s.a.s.HotWaterfallingUpStore ][yjcspzp] Failed to clear cache for realm [I]
[2018-11-29T15:30:15S][INFO ][o.e.l.LicenseService ][yjcspzp] license [e46d8bc-6cf1-4c4d-bd28-d3d6d607f14] mode [basic] - valid
[2018-11-29T15:30:15S][INFO ][o.e.g.GatewayService ][yjcspzp] recovered [11] indices into cluster state
[2018-11-29T15:30:15S][INFO ][o.e.x.s.a.AllocationService ][yjcspzp] Cluster health status changed from [RED] to [YELLOW] (reason: [shards started [[spark][3]], [spark][2]], [spark][1]], [.kibana_1][0] ...]).
```

And here's kibana running:

```
maria_dev@sandbox-hdp:~$ cd /opt/kibana/bin
maria_dev@sandbox-hdp:~$ ./kibana
log [13:46:36.187] [info][status][plugin:kibana@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:36.250] [info][status][plugin:elasticsearch@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.255] [info][status][plugin:xpack_main@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.266] [info][status][plugin:searchprofiler@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.271] [info][status][plugin:ml@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.329] [info][status][plugin:tilemap@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.332] [info][status][plugin:watcher@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.354] [info][status][plugin:license_management@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:36.358] [info][status][plugin:index_management@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.376] [info][status][plugin:rollup@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.630] [info][status][plugin:notification@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:36.641] [info][status][plugin:graph@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.656] [info][status][plugin:monitoring@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:36.663] [info][status][plugin:spaces@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.678] [warning][security] Generating a random key for xpack.security.encryptionKey. To prevent sessions from being invalidated on restart, please set xpack.security.encryptionKey in kibana.yml
log [13:46:36.686] [warning][security] Session cookies will be transmitted over insecure connections. This is not recommended.
log [13:46:36.695] [info][status][plugin:security@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.728] [info][status][plugin:grokdebugger@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.736] [info][status][plugin:dashboard_model@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:36.742] [info][status][plugin:logstash@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.755] [info][status][plugin:beats_management@6.5.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [13:46:36.792] [info][status][plugin:apm@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:37.147] [info][status][plugin:elasticsearch@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.345] [info][status][plugin:canvas@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:37.361] [info][status][plugin:console@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:37.366] [info][status][plugin:console_extensions@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:37.374] [info][status][plugin:notifications@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:37.439] [info][status][plugin:infra@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:37.447] [info][status][plugin:metrics@6.5.1] Status changed from uninitialized to green - Ready
log [13:46:37.466] [info][license][xpack] Imported license information from Elasticsearch for the [data] cluster: mode: basic | status: active
log [13:46:37.471] [info][status][plugin:xpack_main@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.472] [info][status][plugin:searchprofiler@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.473] [info][status][plugin:ml@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.474] [info][status][plugin:tilemap@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.475] [info][status][plugin:watcher@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.476] [info][status][plugin:index_management@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.477] [info][status][plugin:rollup@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.478] [info][status][plugin:graph@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.480] [info][status][plugin:grokdebugger@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.481] [info][status][plugin:logstash@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.481] [info][status][plugin:beats_management@6.5.1] Status changed from yellow to green - Ready
log [13:46:37.482] [info][kibana-monitoring][monitoring-ui] Starting monitoring stats collection
log [13:46:37.494] [info][status][plugin:security@6.5.1] Status changed from yellow to green - Ready
log [13:46:38.065] [warning][reporting] Generating a random key for xpack.reporting.encryptionKey. To prevent pending reports from failing on restart, please set xpack.reporting.encryptionKey in kibana.yml
log [13:46:38.074] [info][status][plugin:reporting@6.5.1] Status changed from uninitialized to green - Ready
```

Setting up the spark job from the streaming lesson to publish log events into elastic.

First, we need to create a kafka topic that we will be writing into, mine is called “next779”, here’s how to create it:

```
./kafka-topics.sh --create --zookeeper sandbox-hdp.hortonworks.com:2181 --replication-factor 1 --partitions 1 --topic next779
```

Next, we have to publish events into this topic, I downloaded the “test.csv” dataset and published some of its data into kafka:

```
./spark-submit --driver-memory 550m --num-executors 4 --executor-memory 550m /home/maria_dev/producer.jar --topic next779 --url sandbox-hdp.hortonworks.com:6667 --filePath /home/maria_dev/test.csv --nThreads 4
```

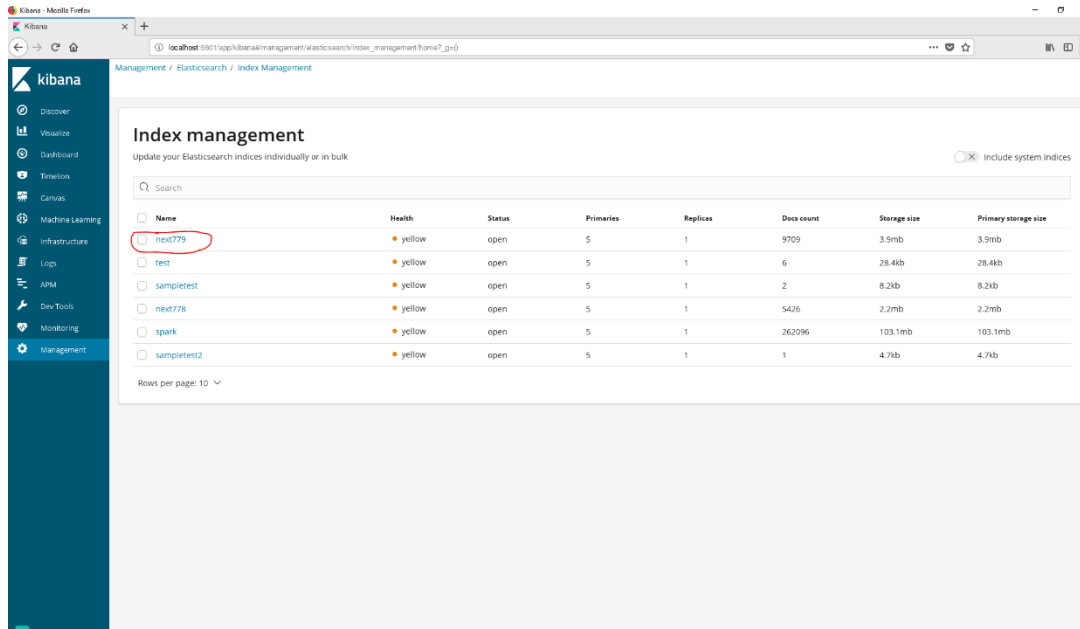
Here’s the execution trace:

```
18/11/29 14:42:59 INFO MessageCallback$: Topic : next779, Offset : 9575, Partition : 0
18/11/29 14:42:59 INFO MessageCallback$: Topic : next779, Offset : 9582, Partition : 0
18/11/29 14:42:59 INFO MessageCallback$: Topic : next779, Offset : 9588, Partition : 0
18/11/29 14:42:59 INFO MessageCallback$: Topic : next779, Offset : 9573, Partition : 0
18/11/29 14:42:59 INFO MessageCallback$: Topic : next779, Offset : 9578, Partition : 0
18/11/29 14:42:59 INFO MessageCallback$: Topic : next779, Offset : 9580, Partition : 0
18/11/29 14:42:59 INFO MessageCallback$: Topic : next779, Offset : 9584, Partition : 0
18/11/29 14:42:59 INFO MessageCallback$: Topic : next779, Offset : 9585, Partition : 0
18/11/29 14:42:59 INFO MessageCallback$: Topic : next779, Offset : 9577, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9589, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9592, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9596, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9600, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9607, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9587, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9590, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9594, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9593, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9595, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9597, Partition : 0
18/11/29 14:43:02 INFO MessageCallback$: Topic : next779, Offset : 9602, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9610, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9608, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9612, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9616, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9609, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9618, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9613, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9619, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9615, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9617, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9601, Partition : 0
18/11/29 14:43:03 INFO MessageCallback$: Topic : next779, Offset : 9591, Partition : 0
18/11/29 14:43:05 INFO MessageCallback$: Topic : next779, Offset : 9603, Partition : 0
18/11/29 14:43:05 INFO MessageCallback$: Topic : next779, Offset : 9620, Partition : 0
18/11/29 14:43:05 INFO MessageCallback$: Topic : next779, Offset : 9623, Partition : 0
18/11/29 14:43:05 INFO MessageCallback$: Topic : next779, Offset : 9605, Partition : 0
18/11/29 14:43:05 INFO MessageCallback$: Topic : next779, Offset : 9625, Partition : 0
18/11/29 14:43:05 INFO MessageCallback$: Topic : next779, Offset : 9627, Partition : 0
18/11/29 14:43:05 INFO MessageCallback$: Topic : next779, Offset : 9611, Partition : 0
18/11/29 14:43:05 INFO MessageCallback$: Topic : next779, Offset : 9598, Partition : 0
18/11/29 14:43:05 INFO MessageCallback$: Topic : next779, Offset : 9629, Partition : 0
18/11/29 14:43:05 INFO MessageCallback$: Topic : next779, Offset : 9614, Partition : 0
```

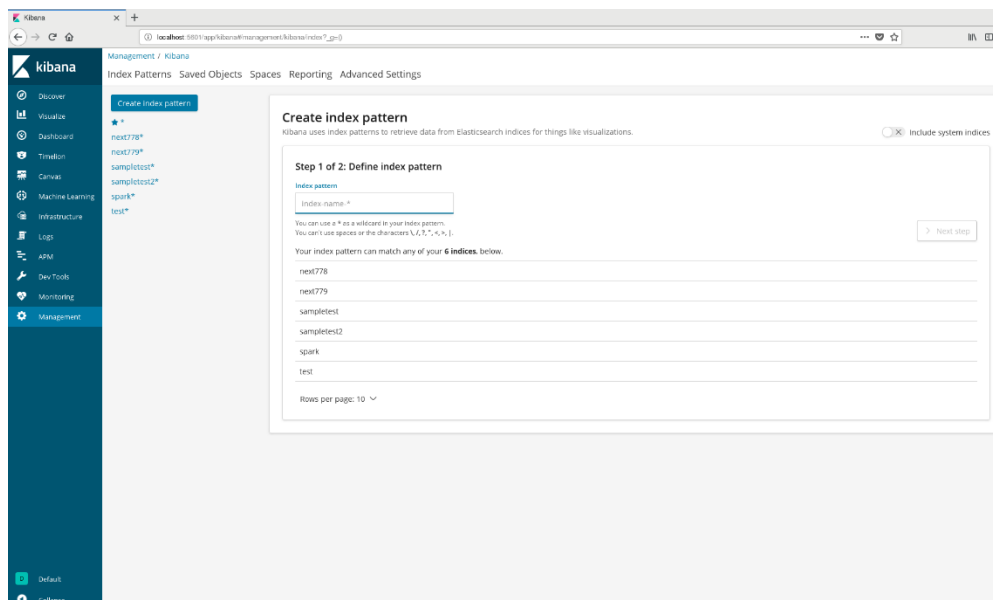
Once we are done publishing events into kafka, we can consume them from kafka into elastic. Like so:

```
./spark-submit --packages org.apache.spark:spark-sql-kafka-0-10_2.11:2.3.2 --master yarn-client
--driver-memory 550m --num-executors 4 --executor-memory 550m /home/maria_dev/consumer.jar -topic next779
-url sandbox-hdp.hortonworks.com:6667 -filePath next779/test_csv -fileFormat org.elasticsearch.spark.sql
-doBatch
false
```

The -filePath argument is in the format “index/type”, so, once this command completes, we will see the “next779” index:



After we uploaded our data into elastic, we need to create an index pattern for kibana, in order to be able to use that data in kibana dashboard:



Once created, our data can be viewed in the discover tab:

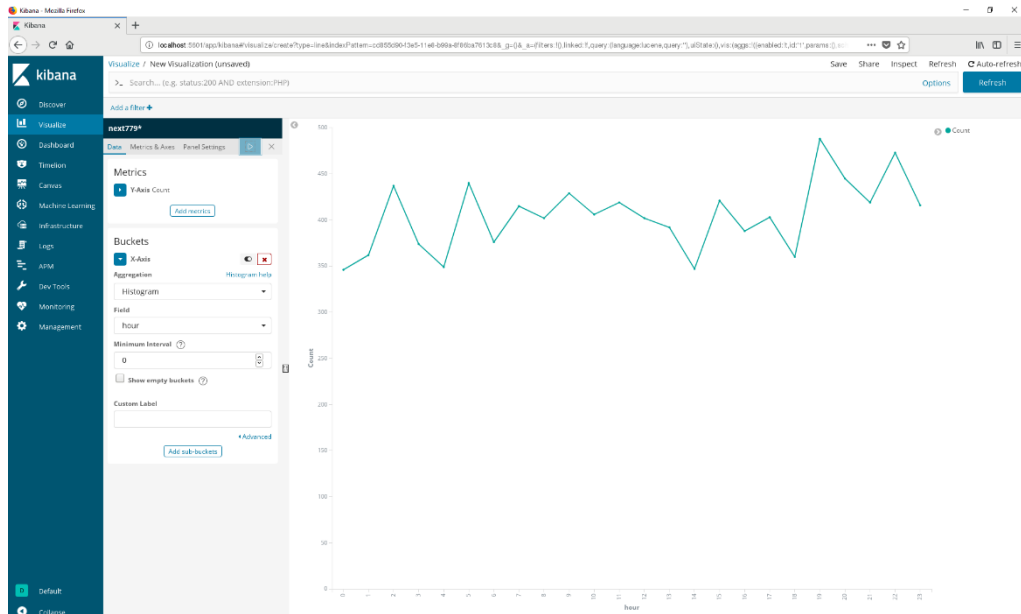
The screenshot shows the Kibana Discover interface. On the left, there's a sidebar with navigation options: Discover (selected), Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring, and Management. The main area displays a table of data with columns for _source, _type, _id, _score, and _type. The data rows show various fields like hour, line, and _source, with values ranging from 0 to 1000. The table is sorted by _score in descending order.

hour	line	_source	_type	_id	_score
0	1	0,2015-09-03 17:09:154,2,3,66,174,37449,5539,0567,1,1,0,3,2016-09-19,2016-09-23,2,0,1,10243,6,6,204,27	test_cnv	next779	1
4	1	16,2015-07-22 11:34:00,2,3,57,342,5011,,57,0,0,5,2015-08-16,2015-08-19,2,1,1,8268,1,2,50,682	test_cnv	next779	1
22	1	62,2015-03-04 19:28:11,2,3,66,174,33271,7654,0409,200,0,0,5,2015-04-29,2015-05-06,2,0,1,635,1,2,162,1039	test_cnv	next779	1
22	1	12,2015-06-03 10:45:51,2,3,57,342,5001,,57,0,0,10,2015-06-05,2015-06-08,2,0,1,11353,1,2,50,699	test_cnv	next779	1
1	1	72,2015-07-17 18:50:10,2,3,66,220,30388,4302,5761,350,0,0,0,2016-06-09,2016-06-10,3,1,1,23116,6,6,76,761	test_cnv	next779	1
11	1	23,2015-10-18 08:43:54,2,3,57,342,5001,,57,0,0,5,2015-10-16,2015-10-18,2,0,1,11502,1,4,47,1502	test_cnv	next779	1
20	1	76,2015-08-28 07:08:10,2,3,66,220,35388,4596,0898,250,0,0,10,2015-09-31,2016-06-01,4,0,1,8213,1,6,68,215	test_cnv	next779	1
20	1	45,2015-03-03 20:34:57,2,3,66,248,24562,1003,2867,250,0,1,4,2015-06-01,2015-06-09,5,0,1,11621,1,2,50,700	test_cnv	next779	1
6	1	17,2015-07-23 13:00:59,2,3,57,342,5001,,57,0,0,5,2015-08-01,2015-08-09,3,1,1,12008,1,2,50,686	test_cnv	next779	1
20	1	29,2015-03-04 17:53:44,2,3,66,226,20170,911,1901,108,0,1,0,2015-09-01,2015-09-04,2,0,1,8791,1,4,4,110	test_cnv	next779	1
20	1	33,2015-11-30 22:51:57,2,3,66,174,1071,382,0833,139,0,0,10,2015-12-21,2015-12-24,4,1,1,8206,1,2,50,628	test_cnv	next779	1
1	1	105,2015-07-23 16:37:00,1,1,3,205,312,22856,157,2377,414,0,0,10,2015-08-05,2015-08-07,2,2,1,41560,1,2,198,788	test_cnv	next779	1
4	1	34,2015-10-21 21:32:19,2,3,66,174,8978,28,209,339,0,0,10,2015-12-24,2015-12-25,4,3,1,10269,6,2,50,1039	test_cnv	next779	1
4	1	30,2015-08-28 13:02:56,1,1,3,205,354,41495,3974,6078,109,0,0,10,2015-09-25,2015-09-27,2,0,1,8788,1,6,77,2	test_cnv	next779	1
3	1	78,2015-07-01 00:47:52,2,3,66,311,54505,2872,146,353,0,0,5,2015-11-07,2015-11-09,2,0,1,14985,1,2,50,1241	test_cnv	next779	1
5	1	117,2015-09-17 21:03:10,2,3,1,23,78,55683,,438,0,0,10,2015-09-24,2015-09-27,2,0,1,6581,6,1,171,61	test_cnv	next779	1
12	1	76,2015-09-14 17:10:03,2,3,66,169,8687,279,5186,150,0,0,10,2015-09-21,2015-09-22,2,0,1,20127,1,2,50,1184	test_cnv	next779	1

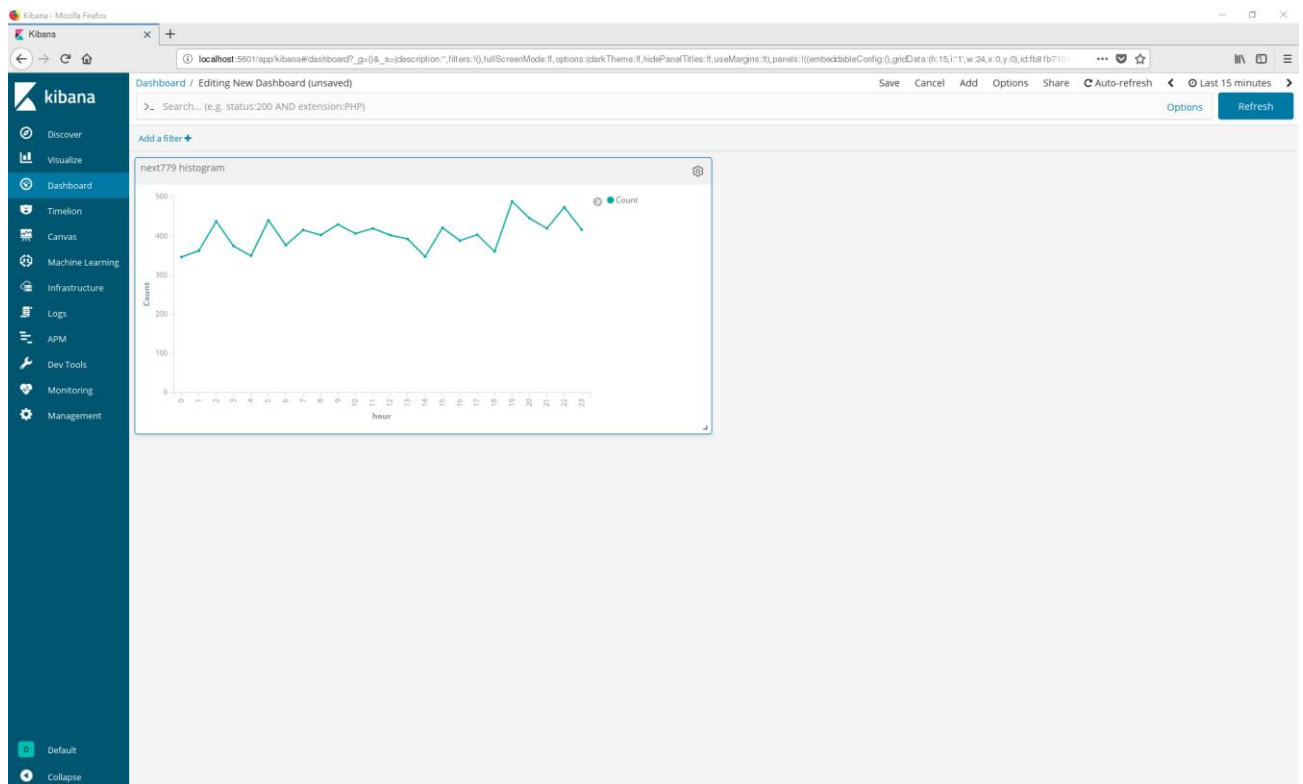
As we can see, we have our data in the proper format. I used the ThreadLocalRandom class in scala to generate random hours that we can use to analyze our “pseudo-data”.

Running the kibana dashboard.

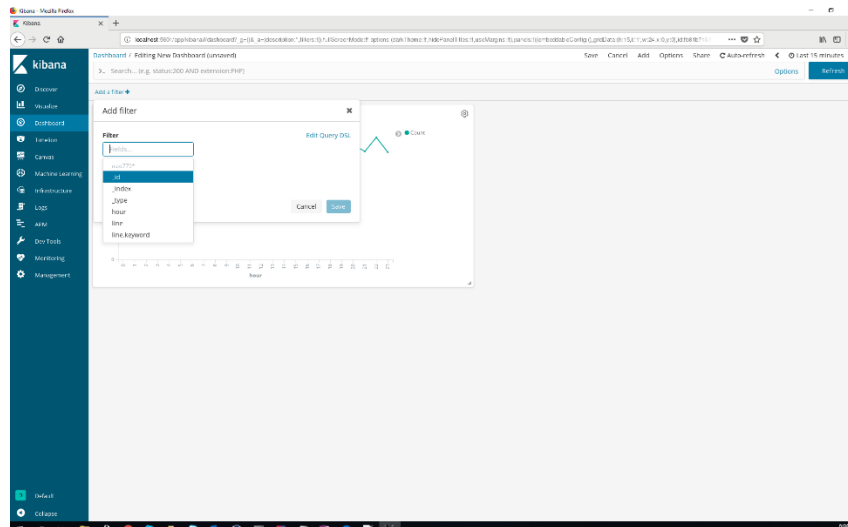
In the visualization tab we can create different kinds of charts to visualize our data, here's one example:



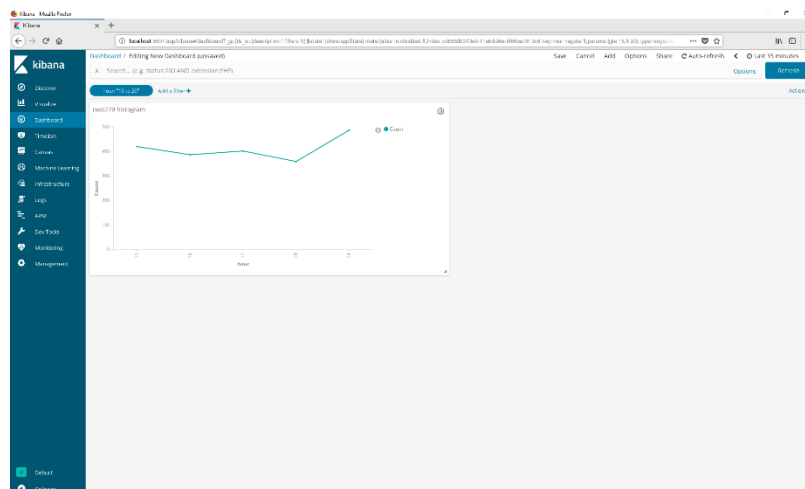
I used the number of logs as the Y-axis, and the X-Axis represents hours. So, each log event belongs to its own hour bucket. The kibana dashboard can be decorated with different kinds of such charts, here's one chart:



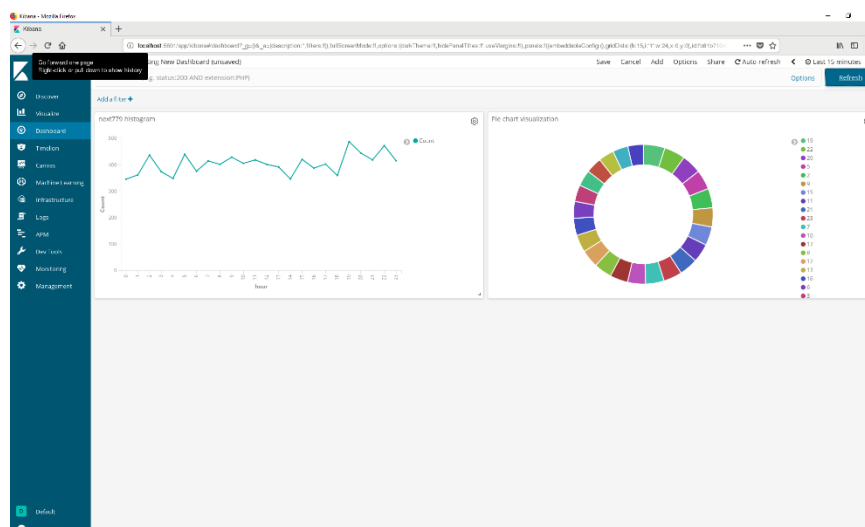
You can add filters in the dashboard to visualize only the subset of your data:



This is what it looks like:



You can also add more visualizations:



And here's the same visualizations with filters applied:

