Elasticsearch, Logstash, Kibana (ELK demo)

Maciej Łotysz

June 5, 2017

Install

- Install docker
- Install docker-compose
- Create working directory for demo and sample data

  ```
  mkdir -p ~/elk/sample
  ```

- Clone ELK + x-pack from git repository

  ```
  git clone --depth 1 git@github.com:deviantony/docker-elk.git ~/elk/docker
  git checkout x-pack
  ```

Manage dockerized ELK instances

Start

```
cd ~/elk/docker &&
    docker-compose up -d
```

Stop but not destroy data

```
cd ~/elk/docker &&
    docker-compose stop
```

Start fresh

- stop first
- remove

```
cd ~/elk/docker &&
    docker-compose rm
```

Check status

```
cd ~/elk/docker &&
    docker-compose ps
```

Elastic search and Kibana

Pump some data to ES

Download

Get sample data in JSONP format from site: Tutorial and put it and/or unzip it in ~/elk/sample.

Define schema for shakespeare data set

Tutorial

```
curl -XPUT -u elastic:changeme \
     'localhost:9200/shakespeare?pretty' \
     -H 'Content-Type: application/json' -d'
{
 "mappings" : {
  "_default_" : {
   "properties" : {
    "speaker" : {"type": "keyword" },
    "play_name" : {"type": "keyword" },
    "line_id" : { "type" : "integer" },
    "speech_number" : { "type" : "integer" }
   }}}}'
```

keyword - not analyzed

Define schema for logs data set - 2015.05.18

```
curl -XPUT -u elastic:changeme \
     'localhost:9200/logstash-2015.05.18?pretty' \
     -H 'Content-Type: application/json' -d'
{
  "mappings": {
    "log": {
      "properties": {
        "geo": {
          "properties": {
            "coordinates": {
              "type": "geo_point"
            }}}}}}}'
```

Define schema for logs data set - 2015.05.19

```
curl -XPUT -u elastic:changeme \
     'localhost:9200/logstash-2015.05.19?pretty' \
     -H 'Content-Type: application/json' -d'
{
  "mappings": {
    "log": {
      "properties": {
        "geo": {
          "properties": {
            "coordinates": {
              "type": "geo_point"
            }}}}}}}'
```

Define schema for logs data set - 2015.05.20

```
curl -XPUT -u elastic:changeme \
     'localhost:9200/logstash-2015.05.20?pretty' \
     -H 'Content-Type: application/json' -d'
{
  "mappings": {
    "log": {
      "properties": {
        "geo": {
          "properties": {
            "coordinates": {
              "type": "geo_point"
            }}}}}}} '
```

Loading bulk bank accounts data

Note: no schema is required

```
cd ~/elk/sample &&
    curl -u elastic:changeme \
         -H 'Content-Type: application/x-ndjson' -XPOST \
         'localhost:9200/bank/account/_bulk?pretty' \
         --data-binary @accounts.json
```

Loading shakespeare data

```
cd ~/elk/sample && \
    curl -u elastic:changeme \
         -H 'Content-Type: application/x-ndjson' \
         -XPOST 'localhost:9200/shakespeare/_bulk?pretty' \
         --data-binary @shakespeare.json
```

Loading logs data

```
cd ~/elk/sample && \
    curl -u elastic:changeme \
         -H 'Content-Type: application/x-ndjson' \
         -XPOST 'localhost:9200/_bulk?pretty' \
         --data-binary @logs.jsonl
```

Cope with java.lang.OutOfMemoryError: Java heap space

Workaround: Increase JVM -Xmx (RAM) for elastic to 1 GB (was 256 MB).

Verify indices state

```
curl -XGET -u elastic:changeme \
     'localhost:9200/_cat/indices?v&pretty'
```

Defining index patterns

Open kibana
Define indices:

- logstash-* (with time series), use @timestamp as time series field
- ba* and shakes* not contain time series

Discovering and visualizing

- check out great introductory videos by Tim Roes on youtube

References

- Elasticsearch home
- Manage ES cluster by X-Pack extension
- Kibana official guide
- Add some ES replicas - scaling (for adventurous)
- Dockerized ELK documentation

Thank you!

Have fun!