Lab 1 : Elasticsearch & Kibana discovery

Installation

Pre-requisite : create a “workspace” folder

Create a workspace folder in a path with no space and ideally close to root.
Example :

C:/workspace for windows
/Users/cflond/workspace for Linux

Make sure to install Elasticsearch, Kibana, Logstash & Beats in this folder to avoid issues with spaces.

Download / install / start Elasticsearch

Please follow these instructions
(ONLY STEP 1 & 2 of “Run Elasticsearch locally on Linux, macOS, or Windows”) :

https://www.elastic.co/guide/en/elasticsearch/reference/current/getting-started-install.html#run-elasticsearch-local

Change your cluster name by editing elastic-7.*/config/elasticsearch.yml and uncomment (remove the #) the line cluster.name. Set as cluster name : “<your-initials>-cluster”. Example for me : “cf-cluster”. Save the config.

Start Elasticsearch from the bin directory:

Linux and macOS:

```
cd elasticsearch-7.*.* /bin
./elasticsearch
```

Windows:

```
cd elasticsearch-7.*.*\bin
.\elasticsearch.bat
```

And try accessing from your browser http://localhost:9200. You should see something like this :


```
{
  "name" : "cflond-laptop.local",
  "cluster_name" : "cf-cluster",
  "cluster_uuid" : "2Qwb1EUpQH-h9o1SeYnN_w",
  "version" : {
    "number" : "7.3.0",
    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "de777fa",
    "build_date" : "2019-07-24T18:30:11.767338Z",
    "build_snapshot" : false,
    "lucene_version" : "8.1.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

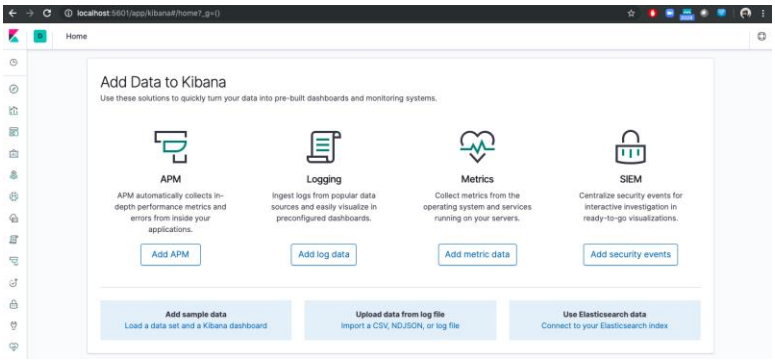
Download & install Kibana

Please follow these instructions for MacOS (only the section install darwin64) to install :
https://www.elastic.co/guide/en/kibana/current/targz.html#install-darwin64
And then to run : https://www.elastic.co/guide/en/kibana/current/start-stop.html#start-start-targz

Please follow these instructions for Linux (only the section install linux64) :
https://www.elastic.co/guide/en/kibana/current/targz.html#install-linux64
And then to run : https://www.elastic.co/guide/en/kibana/current/start-stop.html#start-start-targz

Please follow these instructions for Windows (only the section download and install) :
https://www.elastic.co/guide/en/kibana/current/windows.html#install-windows
And then to run : https://www.elastic.co/guide/en/kibana/current/start-stop.html#start-stop-zip

Try accessing from your browser http://localhost:5601. You should see something like this :



Alternative installation methods (cloud & docker)

If for any reason you cannot install Elasticsearch + Kibana locally, you might consider the free trial of 14 days on https://www.elastic.co/cloud/elasticsearch-service/signup. Please note that logstash & beats are not available in the cloud and should be deployed locally.

Also, please note that Docker versions of Elasticsearch, Kibana, Logstash & Beats are available. Please check online documentation in case you want to use it. Also please only use it if you are familiar with how docker work. Goal of this course is not to spend time on docker it-self.

Load some sample data to discover Kibana

Follow these steps to load some sample data and play with dashboards :
https://www.elastic.co/guide/en/kibana/7.9/tutorial-sample-data.html

1.1 Please select some filters on the [Flights] Global Flight Dashboard, based on your favorite destinations and do a screenshot of it that you will add in your report.

Don't forget to remove the data at the end.

Load your first data into ES and visualize it

To simplify the lab, we have prepared 3 representative set of data :

- The complete works of William Shakespeare : typical data coming from a DB that we would extract using Logstash, and then put it into Elasticsearch for search purpose

- A set of fictitious accounts with randomly generated data : typically coming from a DB that we would extract data from using Logstash, and then put it into Elasticsearch for business analytics purpose

- A set of randomly generated log files : typically coming from web servers that we would collect with beats, transform with logstash and ship to Elasticsearch for Logging Analytics purpose

Please follow these instructions and execute the commands from your command line:
https://www.elastic.co/guide/en/kibana/7.9/tutorial-build-dashboard.html

When you execute CURL commands to load the data, please remove Authentication (-u parameter) and define host as localhost and port as 9200, so the commands are :

```
curl -H 'Content-Type: application/x-ndjson' -XPOST 'localhost:9200/bank/account/_bulk?pretty' --data-binary @accounts.json
curl -H 'Content-Type: application/x-ndjson' -XPOST 'localhost:9200/shakespeare/_bulk?pretty' --data-binary @shakespeare.json
curl -H 'Content-Type: application/x-ndjson' -XPOST 'localhost:9200/_bulk?pretty' --data-binary @logs.jsonl
```

Please go in Kibana and follow these instructions to create the index patterns :
https://www.elastic.co/guide/en/kibana/7.9/tutorial-define-index.html

Start discovering the data in Kibana :
https://www.elastic.co/guide/en/kibana/7.9/tutorial-discovering.html

Explore ba*, shakes*, logstash*

Play with filters, with fulltext search by taking advantage of auto-complete :

1.1 Please specify in your report the total number of documents of each index.

1.2 Please do some screenshots of at least 1 search or filter you applied on each index.

Create 4 visualizations for your data following instructions on :
https://www.elastic.co/guide/en/kibana/7.9/tutorial-visualizing.html

For the markdown visualization, please enter “Lab 1 : School Name + Your names”.

Create a dashboard grouping the 4 visualisations following instructions on :
https://www.elastic.co/guide/en/kibana/7.9/tutorial-dashboard.html

1.3 Do a screenshot of the dashboard and add it to your report