Set Up Elastic Search and Kibana on Windows

Author: Zakaria Benmounah

21/10/2023

1-Download Elastic Search and Kibana from these links and extract the files (use 7-zip):

- Elastic search: https://www.elastic.co/downloads/elasticsearch
- Kibana: https://www.elastic.co/downloads/kibana

2- Open a new command prompt

3- Inside elastic search extracted folder type: bin\elasticsearch.bat

```
C:\Users\zakar\elasticstack\elasticsearch\elasticsearch-8.10.4-windows-x86_64\elasticsearch-8.10.4>bin\elasticsearch.bat
Oct 21, 2023 1:45:19 PM sun.util.locale.provider.LocaleProviderAdapter <clinit>
WARNING: COMPAT locale provider will be removed in a future release
[2023-10-21T13:45:21,702][INFO ][o.a.l.u.VectorUtilPanamaProvider] [ZAKARIA] Java vector incubator API enabled; uses prefe
[2023-10-21T13:45:23,627][INFO ][o.e.n.Node ] [ZAKARIA] version[8.10.4], pid[20560], build[zip/b4a62ac808e88]
35.506990650Z], OS[Windows 11/10.0/amd64], JVM[Oracle Corporation/OpenJDK 64-Bit Server VM/21/21+35-2513]
[2023-10-21T13:45:23,635][INFO ][o.e.n.Node ] [ZAKARIA] JVM home [C:\Users\zakar\elasticstack\elasticsearch\arch=8.10.4\jdk], using bundled JDK [true]
[2023-10-21T13:45:23,636][INFO ][o.e.n.Node ] [ZAKARIA] JVM arguments [-Des.networkaddress.cache.ttl=60, -De
```

4- Wait till Elastic Search finishes setting up the environnement

Once everything is set save the following text in a separate note as we will be needing them later on:

- 1. Elastic search password
- 2. Certificate
- 3. Enrollment token

```
Oäij 'eÅ Password for the elastic user (reset with 'bin/elasticsearch-reset-password -u elastic'):

+RjQcOLORIUMeRpJ4ITN

Oäij 'eÅ HTTP CA certificate SHA-256 fingerprint:
14bd5eba15c18142e294a85dfdb5e85be847d4bc90f6ec4af91dda32db87bb52

Oäij 'eÅ Configure Kibana to use this cluster:

Oçō Run Kibana and click the configuration link in the terminal when Kibana starts.

Oçō Copy the following enrollement token and paste it into Kibana in your browser (valid for the next 30 minutes):

ey.2ZZXIOII-ULjEwLjoiL-CJAZHIOLSHTINJLSEDC40HYW430DoSHJAWTl0SIMTZNCIIGIJE0YMQ1ZWJMMTVJMTgxNDJLMJk0YTg1ZGZkYJVLODVIZTg0NZQ0YMMSMGY2ZWM0YWY5MWRkYTMyZGI4N2JiNTIILCJrZXkiO

iJCREpGVW9ZQkctSkgwT3Qyam59cTprNXVCSTZHTVQ3cTJnVHJLbE94c3dnIn0=

Oäij 'eÅ Configure other nodes to join this cluster:

Oäi 'eA configure other nodes to join this cluster:

Oäi Create an enrollment token with 'bin/elasticsearch-create-enrollment-token -s node'.

Oää Acstart Elasticsearch.
```

5- Open a new command prompt, now once you have extracted the Kibana file, write this command inside the bin folder: kibana.bat

(It is better to use 7-zip software for the extraction)

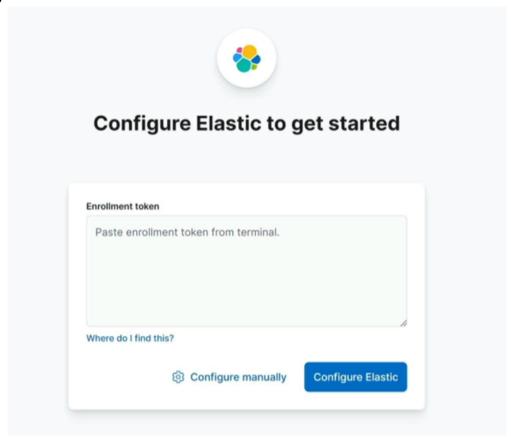
```
C:\Users\zakar\elasticstack\kibana\kibana-8.10.4\bin>kibana.bat
Kibana is currently running with legacy OpenSSL providers enabled! For ction.html#openssl-legacy-provider
{"log.level":"info","@timestamp":"2023-10-21T13:02:27.461Z","log":{"log.level":"info","@timestamp":"2023-10-21T13:02:27.461Z","log":{"log.level":"info","@timestamp":"2023-10-21T13:02:27.461Z","log":{"log.level":"x64","host":"Zakaria",'e":"kibana.bat","os":"win32 10.0.22621","arch":"x64","host":"Zakaria",'e":"kibana","commonName":"service_name"},"serviceVersion":{"source":"ps://kibana-cloud-apm.apm.us-east-1.aws.found.io/","commonName":"service!":"start","value":true},"contextPropagationOnly":{"source":"start","value":f["contextPropagationOnly":{"source":"start","value":f["contextPropagationOnly":{"start","value":f["contextPropagationOnly":{"start","value":f["contextPropagationOnly":{"start","value":f["contextPropagationOnly":{"start","value":f["contextPropagationOnly":{"start","value":f["contextPropagationOnly":{"start","value":f["contextPropagationOnly":{"start","value":f["contextPropagationOnly":{"start","value":f["contextPropagationOnly":{"start","value":f["contextPropagationOnly":{"start","value":f["contextPropagationOnly":{"start","value":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f["contextPropagationOnly":f
```

6- Once Kibana setup has finished open this URL:

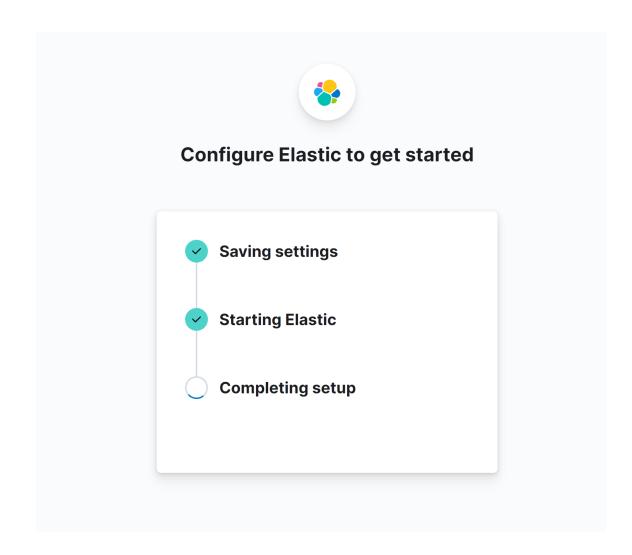
```
i Kibana has not been configured.

Go to <a href="http://localhost:5601/?code=655334">http://localhost:5601/?code=655334</a> to get started.
```

7-Write the enrollment token (3) you have saved from an ElasticSearch here and click Configure Elastic:



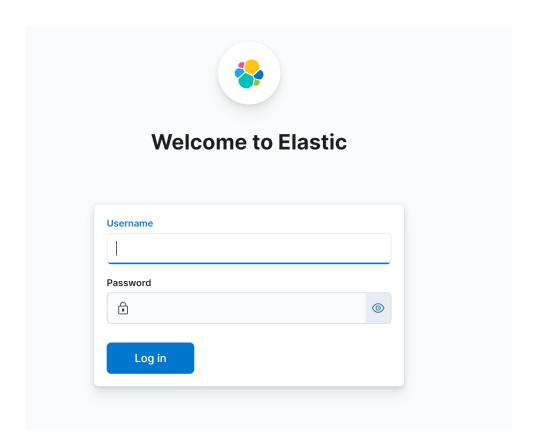
8-Now wait for the process to finish



9- write the following data to log in:

• Username: elastic

• Password: (the one that we have saved from elastic search (1))



10- Welcome to elastic world:

