**ELK setup -**

**Elasticsearch installation for each node** :-

* Downloading binaries with command -

wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.7.0-linux-x86\_64.tar.gz

* Extract by : tar -xzf elasticsearch-7.7.0-linux-x86\_64.tar.gz or do it manually by double clicking on .gz file and extracting to desired deirectory

**Java OpenJDK installation** :

* Check wether java is install properly by typing : java -version. If java is installed it will give - openjdk version "version\_no.".
* If not then install it by : sudo apt install openjdk-11-jdk

**Kibana binaries installation** :

* wget https://artifacts.elastic.co/downloads/kibana/kibana-7.2.0-linux-x86\_64.tar.gz
* Extraction: tar -xzf kibana-7.2.0-linux-x86\_64.tar.gz or do it manually by double clicking on .gz file and extracting to desired deirectory

**Making changes to Elasticsearch configuration files**.

* Go to elasticsearch directory (where it was extracted) → config → elasticsearch.yml

Everything is commented out initially. Things to specify

* <cluster.name: *my\_cluster\_name*>
* <node.name: *node\_name*>
* For Master node: <node.master: true>
* For Data nodes: <node.data: true>
* <network.host: *host\_ip\_address*>
* <http.port: 9200>

**To start elasticsearch,**

* Enter <su *username*> and enter password,
* <cd *elasticsearch\_directory*> // Deirectory Where you have extracted elasticsearch.gz file
* Type : bin/elasticsearch // It will start elastic search cluster

**Setting up Kibana**

Make changes in “kibana.yml” file in config directory of Kibana.

* <cd *kibana\_directory*/config>
* Open “kibana.yml” file in it. Enter the following :
* <server.port: 5601>
* <server.host: *host\_ip\_address*> i.e. IP of node that contains Kibana
* <elasticsearch.hosts: ["http://*host\_ip\_address*:9200"]>

**To start kibana:**

* <cd *kibana\_directory*>
* <bin/ki bana>

**Setting up Kibana Index Pattern**

Let’s say the name of the index (data) that we pushed through Spark is *coriolis\_data.*

And this data contains many fields including a field named, say “*image”* which contains base64 string of an image.

To view data, we need to **create an “Index Pattern”**. Following are the steps :

* On left most part of Kibana page, there is a panel of different tools. Select “Management” tab from it which is at the bottom.
* Inside it, go to “Index patterns” tab and click on “Create new Index pattern”.
* Then it prompts to provide a name for “Index pattern” which must be either the same as the name of “index” (data) or at least a prefix of the index name.
* Once the index pattern is created, you can see different fields and their types.
* Go to “image” field, click the edit icon at the rightmost end and make the following changes:
* Format → <Url>
* Type → <Image>
* URL template → <data:image/jpeg;base64,{{rawValue}}>
* and click on “save field”.

Kibana is ready now with an Index pattern which allows to do all searches, visualizations, etc.