**ELK**

Reliably and securely take data from any source, in any format, then search, analyse, and visualize it in real time.

**E:** Elastic Search

**L:** Logstash

**K:** Kibana

**Elastic Search:**

Elasticsearch is a search engine based on the Lucene library. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents. Elasticsearch is developed in Java.

**Full-text search** queries and performs linguistic searches against documents. It includes single or multiple words or phrases and returns documents that match search condition

**Logstash:**

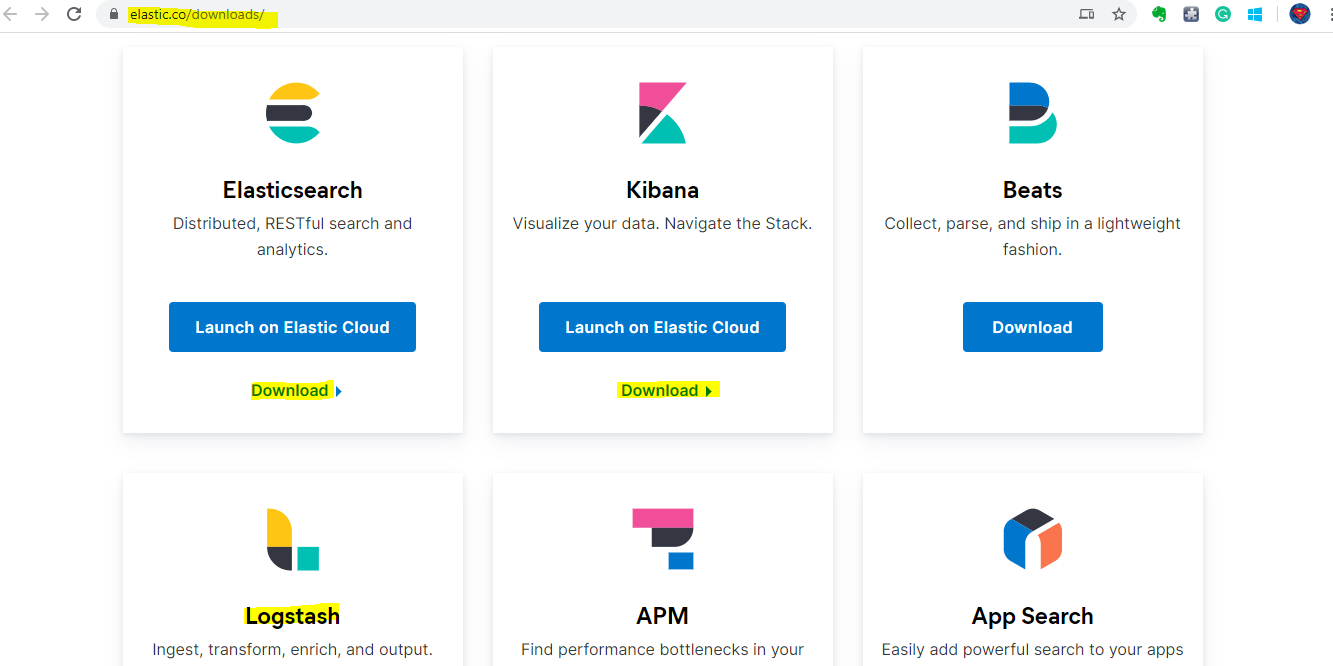
Logstash is an open source, server-side *data processing pipeline* that ingests data from a multitude of sources simultaneously, transforms it, and then sends it to your favorited "stash."

**Kibana:**

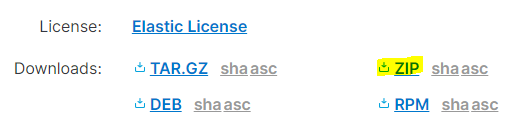
Kibana is an open source data visualization dashboard for Elasticsearch. It provides visualization capabilities on top of the content indexed on an Elasticsearch cluster. Users can create bar, line and scatter plots, or pie charts and maps on top of large volumes of data.

**Setting up ELK in local Windows Machine:**

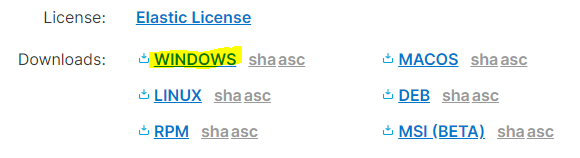
**Step 1:**

Download the zip file from <https://www.elastic.co/downloads/>

For logstash download 🡪 **ZIP**

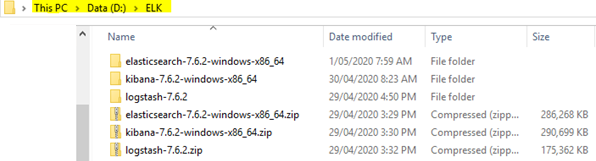


For Elastic search and Kiban download 🡪 **WINDOWS**

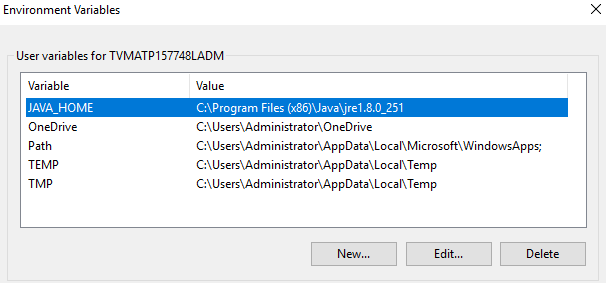


**Step 2:**

Extract the downloaded file into windows folder (e.g.:



**Step 4:**

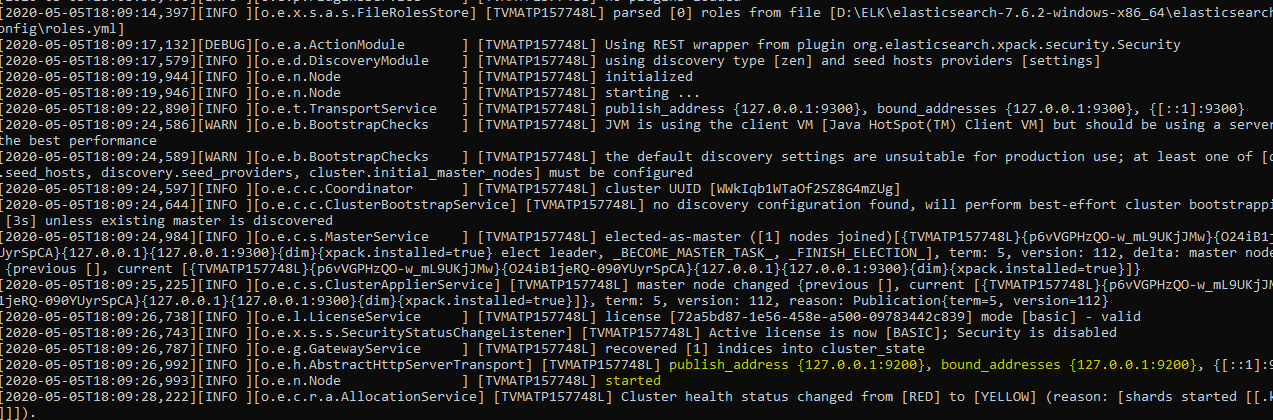
Download JDK and install and set the JAVA\_HOME in environment variable.

**Step 5:**

**Run Elastic Search:**

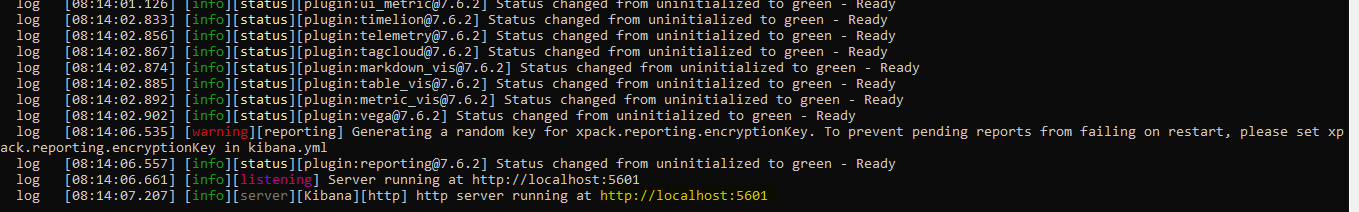
* Run command prompt as administrator.
* Change directory to Elastic Search bin folder (e.g.: D:\ELK\elasticsearch-7.6.2-windows-x86\_64\elasticsearch-7.6.2\bin)
* Then type **elasticsearch** and enter (.bat file in folder)
* Check for cmd prompt message , if successfully ran you will get below result
* If error, got to folder (e.g.: D:\ELK\elasticsearch-7.6.2-windows-x86\_64\elasticsearch-7.6.2\logs) and analyse.
* If any issue related to Machine learning (May be because of old JDK)

The put entry (***xpack.ml.enabled: false***) in elasticsearch.yml (D:\ELK\elasticsearch-7.6.2-windows-x86\_64\elasticsearch-7.6.2\config)



**Run Kibana:**

* Run command prompt as administrator.
* Change directory to Kibana bin folder (e.g.: D:\ELK\kibana-7.6.2-windows-x86\_64\kibana-7.6.2-windows-x86\_64\bin)
* Then type **kibana** and enter (.bat file in the folder)
* Check for cmd prompt message, if successfully ran you will get below result

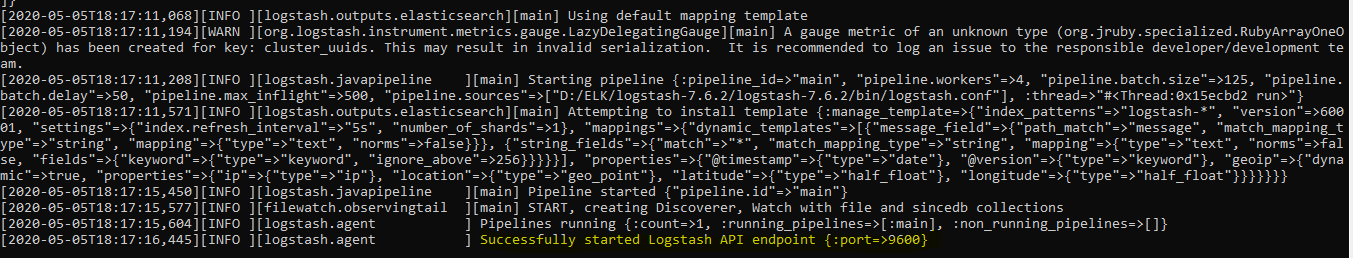


**Run Logstash:**

* Run command prompt as administrator.
* Change directory to Logstash bin folder (e.g.: D:\ELK\logstash-7.6.2\logstash-7.6.2\bin)
* Add this conf file into bin (e.g.: D:\ELK\logstash-7.6.2\logstash-7.6.2\bin)

folder (You can use any name and path for conf files)

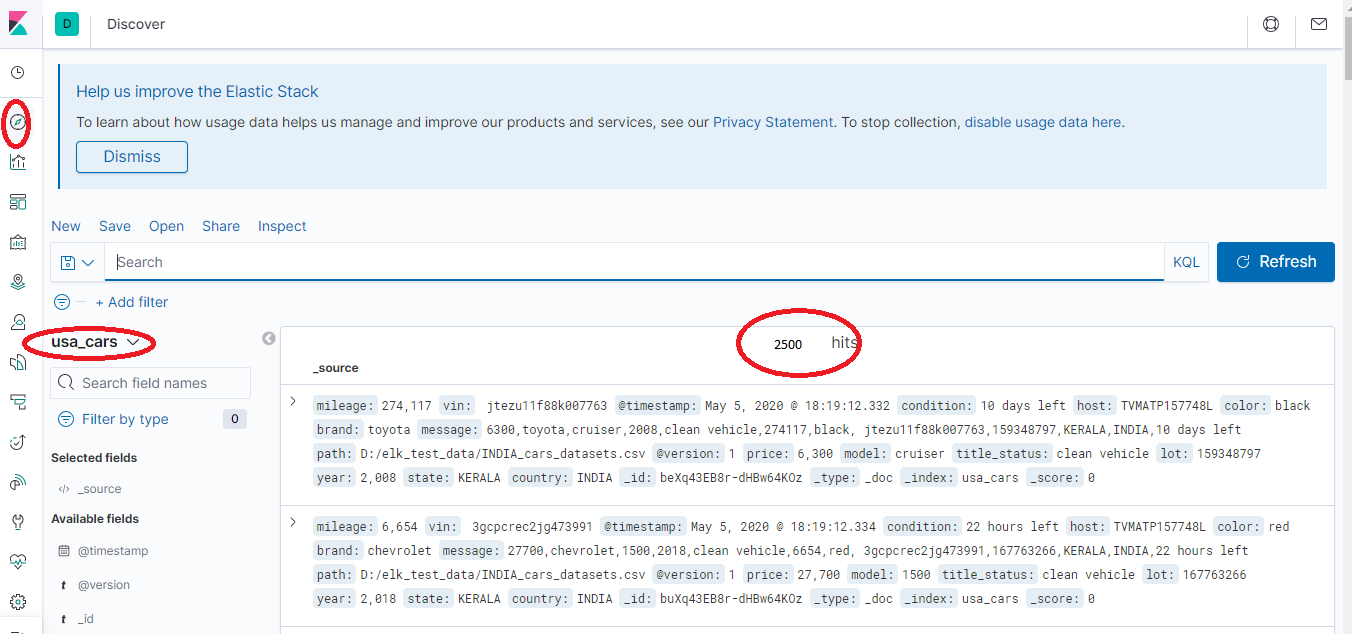
* Run *logstash -f logstash.conf*
* Check for cmd prompt message, if successfully ran you will get below result



* If error, got to folder (e.g.: D:\ELK\logstash-7.6.2\logstash-7.6.2\logs) and analyse.
* Please find below file and place accordingly

After Successfully configure ELK, you can login to Kibana web GUI and check the result.



You can get more video and document from reference

**Reference:**

<https://www.elastic.co/>

[**https://www.youtube.com/watch?v=rKy4sFbIZ3U&list=PLHzSTpk-fHJFSTJOsP9SFYGZUFdIK3tGt&index=3&t=998s**](https://www.youtube.com/watch?v=rKy4sFbIZ3U&list=PLHzSTpk-fHJFSTJOsP9SFYGZUFdIK3tGt&index=3&t=998s)

[**https://www.youtube.com/watch?v=imrKm6dV3NQ&list=PLHzSTpk-fHJFSTJOsP9SFYGZUFdIK3tGt&index=4&t=868s**](https://www.youtube.com/watch?v=imrKm6dV3NQ&list=PLHzSTpk-fHJFSTJOsP9SFYGZUFdIK3tGt&index=4&t=868s)