ELK Stack Installation

System Requirements:

- Ubuntu 20.04 Operating System
- 4GB of RAM
- 2 CPUs
- A Non-root user account with sudo privileges.
- OpenJDK 11 installed.
- Nginx

Note: Kibana will be proxied over Nginx server to make it available in a browser. This is because it is available only in Localhost.

Notes: The following other requirements need to be fulfilled:

- After completing step 2 of the tutorial, we will have to secure the Nginx Server.
- We need a fully qualified domain name (FQDN).
- We need to set up Digital Ocean DNS Records for our server.

We need to import the elasticsearch public **gpg** key and elastic package source list in order to install elasticsearch.

To install elasticsearch, use: **sudo apt install elasticsearch.**

The **elasticsearch.yml** file provides configuration options for your cluster, node, paths, memory, network, discovery, and gateway. Here, we are installing it only on a single server and will change only the network host to **localhost**.

We have specified localhost so that Elasticsearch listens on all interfaces and bound IPs. If you want it to listen only on a specific interface, you can specify its IP in place of localhost.

Then, we need to start elasticsearch and enable it by using systemctl.

Installing Kibana:

We need to install kibana only after installing elasticsearch. This will ensure that all the correct components for both the products are in place.

- Install Kibana using : **sudo apt-get install kibana**.
- Then we need to enable kibana by: **sudo systemctl enable kibana**.
- We can start kibana using: **sudo systemctl start kibana**.
- Since kibana is configured to listen only on **localhost**, so we need to set up a reverse proxy to allow external access to it.
- A reverse proxy is a type of proxy server that handles and redistributes client requests to a server. They can offer SSL encryption.

Installing Logstash:

- Even though it is possible for Beats to directly send the data to the elasticsearch database, Installing Logstash to process the data allows us more flexibility to collect data from different sources, process it to a common format and export it.
- We need to create a config file to set up FileBeat input.
- We need to create another configuration file to allow Logstash to store the Beats data in Elasticsearch.
- After testing the configuration format, we need to start logstash using **systemctl** and then enable it.

Installing FileBeat:

- A beat is a lightweight data shipper to collect data from various sources and transport to Elasticsearch or Logstash. The **FileBeat** Beat collects and ships log files.
- We have to enable it to collect logs from our NodeJS server and send it to ElasticSearch or Logstash.
- Start and enable FileBeat using systemctl.
- There are two ways to send log data to elasticsearch from NodeJS: directly by using the **winston-elasticsearch** transport or by sending it to FileBeat and then to ElasticSearch.