**ELK Stack**

The steps followed to set up ELK stack on Kali Linux for log analysis and monitoring project include:

* 1. **Set up KaliLinux VM on Virtual Box.**
  2. **Installing Dependencies- OpenJDK, Nginx**
     + Install dependencies (java ang nginx) before installing elastic stack

**sudo apt install openjdk-11-jdk**

**sudo apt install nginx**

* 1. **Installing, configuring, starting, and testing Elasticsearch.**
     + To install Elasticsearch on KaliLinux

**sudo apt install elasticsearch**

* + - Elasticsearch configuration files are in YML format. Make necessary changes in the configuration file (elasticsearch.yml file) , save the changes and start the elasticsearch service.

**sudo nano /etc/elasticsearch/elasticsearch.yml**

Under the “Network section” uncomment the below line (remove '#')

**network.host: localhost**

**http.port: 9200**

Add the below line under the “Discovery” section.

**discovery.type: single-node**

**A computer screen shot of a computer

Description automatically generated**

* Start the elasticsearch service by entering the below command.

**sudo systemctl start elasticsearch**

* + - To check elasticsearch is working properly, we will send a GET request to elasticsearch server. Run the below command to check if the server is up and running.

**curl -X GET “localhost:9200”**

**A screen shot of a computer

Description automatically generated**

One can also check if elasticsearch is working properly by visiting the browser and typing [**http://localhost:9200**](http://localhost:9200)

**A screenshot of a computer

Description automatically generated**

* To enable elacticsearch at system startup

**sudo systemctl enable elasticsearch**

* To check elasticsearch service pid

**sudo systemctl status elasticsearch**

**A screen shot of a computer screen

Description automatically generated**

* 1. **Installing, configuring, starting, and testing Kibana.**
     + To install kibana on Kali Linux

**sudo apt-get install kibana**

* + - Make necessary modifications to the kibana configuration file.

**sudo nano /etc/kibana/kibana.yml**

Uncomment the below lines in the kibana.yml configuration file

**server.port: 5601**

**server.host: "localhost"**

**elasticsearch.hosts: ["http://localhost:9200"]**

**A screenshot of a computer screen

Description automatically generated**

* To start the kibana service

**sudo systemctl start kibana**

* To enable kibana at system startup

**sudo systemctl enable kibana**

* To check the status of kibana service

**sudo systemctl status kibana**

**A computer screen shot of a program

Description automatically generated**

* Testing Kibana

Go to the browser and run [**http://localhost:5601**](http://localhost:5601/)

**A screenshot of a computer

Description automatically generated**

* 1. **Installing, configuring, starting, and testing Logstash.**
* To install logstash on KaliLinux

**sudo apt-get install logstash**

* Make modification in the sudo nano /etc/logstash/conf.d/2-beats-input.conf file. Insert the below code in the conf file.

input {

beats {

port => 5044

}}

sudo nano /etc/logstash/conf.d/2-elasticsearch-output.conf

output {

elasticsearch {

hosts => ["localhost:9200"]

manage\_template => false

index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"

}}

**A computer screen shot of a computer program

Description automatically generated**

* To start logstash service

**sudo systemctl start logstash**

* To enable logstash at system startup

**sudo systemctl enable logstash**

* To check status of logstash

**sudo systemctl status logstash**

**A screen shot of a computer code

Description automatically generated**

* 1. **Install Filebeat, a lightweight plugin used to collect and ship log files to Logstash. It is the most used Beats module.**
     + **Install filebeats on KaliLinux**

**sudo apt install Filebeats**

* Make modifications in the filebeat configuration file

**sudo nano /etc/filebeat/filebeat.yml**

* Comment the below lines

**#output.elasticsearch:**

**#Array of hosts to connect to.**

**#hosts: ["localhost:9200"]**

Uncomment the below lines

**output.logs tash: hosts: ["localhost:5044"]**

**A screenshot of a computer

Description automatically generated**

* To start filebeat service

**sudo systemctl start filebeat**

* To enable filebeat at system startup

**sudo systemctl enable filebeat**

* To check status of filebeat service

**sudo systemctl status filebeat**

**A screen shot of a computer program

Description automatically generated**

* 1. **Configuring and enabling the Filebeat system module, which will examine local system logs.**
* Enable filebeat system module by entering the below command

**sudo filebeat modules enable system**

* Enable filebeat logstash module by entering the below command

**sudo filebeat modules enable logstash**

**A screenshot of a computer

Description automatically generated**

* 1. **Verify Elasticsearch Reception of Data.**
     + Load the index template by using the below command

**filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["localhost:9200"]'**

**A screenshot of a computer program

Description automatically generated**

* + - Now checking whether elasticsearch is receiving data log from filebeat by using the below command

**curl -XGET**[**http://localhost:9200/\_cat/indices?v**](http://localhost:9200/_cat/indices?v)

**A computer screen shot of a computer

Description automatically generated**

* 1. **Lookup the visuals and analyze the logs on Kibana interface.**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated