Kibana Installation on Docker

Docker Installation on Ubuntu

- Update the apt package index and install packages to allow apt to use a repository over HTTPS:

```
sudo apt-get update
sudo apt-get install \
 ca-certificates \
 curl \
 gnupg \
 lsb-release
```

- Add Docker's official GPG key:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
```

- Update the apt package index, and install the *latest version* of Docker Engine and containerd, or go to the next step to install a specific version:

```
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io
```

- Install Docker package:

```
sudo apt-get install docker-ce=<VERSION_STRING> docker-ce-cli=<VERSION_STRING> containerd.io
```

- Verify that Docker Engine is installed correctly by running the hello-world image.

```
sudo docker run hello-world
```

- Upgrade Docker Package:

sudo apt-get update

Elastic Search – Kibana Installation

- Start an Elasticsearch container

docker network create elastic

docker pull docker.elastic.co/elasticsearch/elasticsearch:8.1.2

docker run --name es-node01 --net elastic -p 9200:9200 -p 9300:9300 -t docker.elastic.co/elasticsearch/elasticsearch:8.1.2

- Start Kibana and connect it to your Elasticsearch container

docker pull docker.elastic.co/kibana/kibana:8.1.2

docker run --name kib-01 --net elastic -p 5601:5601 docker.elastic.co/kibana/kibana:8.1.2

Apache Installation

To install Apache, install the latest meta-package apache2 by running:

sudo apt update

sudo apt install apache2

Setup Apache log location

Apache logs

---

nano /var/ossec/etc/ossec.conf

<!-- Apache -->

```
  <localfile>
    <location>/var/log/apache2/access.log</location>
    <log_format>apache</log_format>
  </localfile>

  <localfile>
    <location>/var/log/apache2/error.log</location>
    <log_format>apache</log_format>
  </localfile>
<!-- End of Apache -->
```

```
systemctl reload-or-restart agent.service
```