**Deploying ELK Stack on Docker Container.**

DESCRIPTION

**Project objective:**

You have to deploy ELK Stack on a Docker container to implement continuous monitoring.

**Background of the problem statement:**

Your manager has asked to create an elegant user interface for data analysis and data visualization as you have worked on ELK stack previously and have the idea of how it works. This will help the DevOps team to monitor and analyze the application behavior.

**You must use the following:**

* Docker: To create a container for installing ELK Stack
* ELK Stack: To implement continuous monitoring
* Git: To connect and push files from the local system to GitHub
* GitHub: To store the Angular application

**Following requirements should be met:**

* A few of the source code should be tracked on GitHub repositories. You need to document the tracked files that are ignored during the final push to the GitHub repository.
* Submission of your GitHub repository link is mandatory. In order to track your task, you need to share the link of the repository in the document.
* The step-by-step process involved in completing this task should be documented.

**Commands:-**

ubuntu@ip-172-31-95-17:~$ sudo apt-get update

Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal InRelease

Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates InRelease

Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports InRelease

Get:4 https://download.docker.com/linux/ubuntu focal InRelease [57.7 kB]

Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease

Get:6 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages [15.5 kB]

Fetched 73.1 kB in 0s (170 kB/s)

Reading package lists... Done

ubuntu@ip-172-31-95-17:~$ sudo apt-get install ca-certificates curl gnupg lsb-release Reading package lists... Done

Building dependency tree

Reading state information... Done

lsb-release is already the newest version (11.1.0ubuntu2).

ca-certificates is already the newest version (20210119~20.04.2).

curl is already the newest version (7.68.0-1ubuntu2.7).

gnupg is already the newest version (2.2.19-3ubuntu2.1).

0 upgraded, 0 newly installed, 0 to remove and 110 not upgraded.

ubuntu@ip-172-31-95-17:~$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg

File '/usr/share/keyrings/docker-archive-keyring.gpg' exists. Overwrite? (y/N) Y

ubuntu@ip-172-31-95-17:~$ echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu $(lsb\_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list /dev/null

deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu focal stable

ubuntu@ip-172-31-95-17:~$ sudo apt-get update

Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal InRelease

Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates InRelease

Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports InRelease

Hit:4 https://download.docker.com/linux/ubuntu focal InRelease

Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease

Reading package lists... Done

ubuntu@ip-172-31-95-17:~$ sudo apt-get install docker-ce docker-ce-cli containerd.io

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following additional packages will be installed:

docker-ce-rootless-extras docker-scan-plugin pigz slirp4netns

Suggested packages:

aufs-tools cgroupfs-mount | cgroup-lite

The following NEW packages will be installed:

containerd.io docker-ce docker-ce-cli docker-ce-rootless-extras docker-scan-plugin pigz slirp4netns

0 upgraded, 7 newly installed, 0 to remove and 110 not upgraded.

Need to get 96.4 MB of archives.

After this operation, 405 MB of additional disk space will be used.

Do you want to continue? [Y/n] y

Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal/universe amd64 pigz amd64 2.4-1 [57.4 kB]

Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal/universe amd64 slirp4netns amd64 0.4.3-1 [74.3 kB]

Get:3 https://download.docker.com/linux/ubuntu focal/stable amd64 containerd.io amd64 1.5.11-1 [22.9 MB]

Get:4 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-ce-cli amd64 5:20.10.14~3-0~ubuntu-focal [41.0 MB]

Get:5 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-ce amd64 5:20.10.14~3-0~ubuntu-focal [20.9 MB]

Get:6 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-ce-rootless-extras amd64 5:20.10.14~3-0~ubuntu-focal [7932 kB]

Get:7 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-scan-plugin amd64 0.17.0~ubuntu-focal [3521 kB]

Fetched 96.4 MB in 2s (52.7 MB/s)

Selecting previously unselected package pigz.

(Reading database ... 63895 files and directories currently installed.)

Preparing to unpack .../0-pigz\_2.4-1\_amd64.deb ...

Unpacking pigz (2.4-1) ...

Selecting previously unselected package containerd.io.

Preparing to unpack .../1-containerd.io\_1.5.11-1\_amd64.deb ...

Unpacking containerd.io (1.5.11-1) ...

Selecting previously unselected package docker-ce-cli.

Preparing to unpack .../2-docker-ce-cli\_5%3a20.10.14~3-0~ubuntu-focal\_amd64.deb ...

Unpacking docker-ce-cli (5:20.10.14~3-0~ubuntu-focal) ...

Selecting previously unselected package docker-ce.

Preparing to unpack .../3-docker-ce\_5%3a20.10.14~3-0~ubuntu-focal\_amd64.deb ...

Unpacking docker-ce (5:20.10.14~3-0~ubuntu-focal) ...

Selecting previously unselected package docker-ce-rootless-extras.

Preparing to unpack .../4-docker-ce-rootless-extras\_5%3a20.10.14~3-0~ubuntu-focal\_amd64.deb ...

Unpacking docker-ce-rootless-extras (5:20.10.14~3-0~ubuntu-focal) ...

Selecting previously unselected package docker-scan-plugin.

Preparing to unpack .../5-docker-scan-plugin\_0.17.0~ubuntu-focal\_amd64.deb ...

Unpacking docker-scan-plugin (0.17.0~ubuntu-focal) ...

Selecting previously unselected package slirp4netns.

Preparing to unpack .../6-slirp4netns\_0.4.3-1\_amd64.deb ...

Unpacking slirp4netns (0.4.3-1) ...

Setting up slirp4netns (0.4.3-1) ...

Setting up docker-scan-plugin (0.17.0~ubuntu-focal) ...

Setting up containerd.io (1.5.11-1) ...

Created symlink /etc/systemd/system/multi-user.target.wants/containerd.service → /lib/systemd/system/containerd.service.

Setting up docker-ce-cli (5:20.10.14~3-0~ubuntu-focal) ...

Setting up pigz (2.4-1) ...

Setting up docker-ce-rootless-extras (5:20.10.14~3-0~ubuntu-focal) ...

Setting up docker-ce (5:20.10.14~3-0~ubuntu-focal) ...

Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /lib/systemd/system/docker.service.

Created symlink /etc/systemd/system/sockets.target.wants/docker.socket → /lib/systemd/system/docker.socket.

Processing triggers for man-db (2.9.1-1) ...

Processing triggers for systemd (245.4-4ubuntu3.13) ...

ubuntu@ip-172-31-95-17:~$ sudo sysctl -w vm.max\_map\_count=262144

vm.max\_map\_count = 262144

ubuntu@ip-172-31-95-17:~$ sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/elk

Unable to find image 'sebp/elk:latest' locally

latest: Pulling from sebp/elk

35807b77a593: Pull complete

ccfecfa17ed6: Pull complete

499764c8dc6b: Pull complete

7678f89d74e0: Pull complete

a508f189fe8d: Pull complete

e1613802b0fc: Pull complete

b8401e2d7854: Pull complete

ba4f36e3b49c: Pull complete

f8f7494c3ae5: Pull complete

99f78801c68f: Pull complete

02a1381b2e66: Pull complete

fdc1ebd1a364: Pull complete

0a9b3a7d3093: Pull complete

80774fa6fdfb: Pull complete

c6f298ef7e89: Pull complete

26adf53f302f: Pull complete

6bfa07b4e369: Pull complete

0a3d4e063607: Pull complete

c432e077377e: Pull complete

a7d2deb9fa28: Pull complete

13544f67f141: Pull complete

6fd7701a5ae9: Pull complete

8a50efbbf19a: Pull complete

a9247e321de6: Pull complete

e653f6b251c4: Pull complete

077bb10f53d0: Pull complete

0d3c7f4d911b: Pull complete

4f4fb700ef54: Pull complete

25d07ca55aac: Pull complete

39d5b5b660b8: Pull complete

9b2c97c0be76: Pull complete

Digest: sha256:64b4aa22cf6eb6d428bc48eaffdc75e550f9e832d1f9bd135d588896facfba69

Status: Downloaded newer image for sebp/elk:latest

\* Starting periodic command scheduler cron [ OK ]

\* Starting Elasticsearch Server [ OK ]

waiting for Elasticsearch to be up (1/30)

waiting for Elasticsearch to be up (2/30)

waiting for Elasticsearch to be up (3/30)

waiting for Elasticsearch to be up (4/30)

waiting for Elasticsearch to be up (5/30)

waiting for Elasticsearch to be up (6/30)

waiting for Elasticsearch to be up (7/30)

waiting for Elasticsearch to be up (8/30)

waiting for Elasticsearch to be up (9/30)

waiting for Elasticsearch to be up (10/30)

waiting for Elasticsearch to be up (11/30)

waiting for Elasticsearch to be up (12/30)

waiting for Elasticsearch to be up (13/30)

waiting for Elasticsearch to be up (14/30)

waiting for Elasticsearch to be up (15/30)

waiting for Elasticsearch to be up (16/30)

waiting for Elasticsearch to be up (17/30)

waiting for Elasticsearch to be up (18/30)

waiting for Elasticsearch to be up (19/30)

waiting for Elasticsearch to be up (20/30)

waiting for Elasticsearch to be up (21/30)

waiting for Elasticsearch to be up (22/30)

waiting for Elasticsearch to be up (23/30)

waiting for Elasticsearch to be up (24/30)

waiting for Elasticsearch to be up (25/30)

waiting for Elasticsearch to be up (26/30)

waiting for Elasticsearch to be up (27/30)

waiting for Elasticsearch to be up (28/30)

waiting for Elasticsearch to be up (29/30)

waiting for Elasticsearch to be up (30/30)

Couldn't start Elasticsearch. Exiting.

Elasticsearch log follows below.

[2022-04-17T19:58:02,351][INFO ][o.e.n.Node ] [elk] version[8.1.0], pid[253], build[default/tar/3700f7679f7d95e36da0b43762189bab189bc53a/2022-03-03T14:20:00.690422633Z], OS[Linux/5.11.0-1022-aws/amd64], JVM[Eclipse Adoptium/OpenJDK 64-Bit Server VM/17.0.2/17.0.2+8]

[2022-04-17T19:58:02,364][INFO ][o.e.n.Node ] [elk] JVM home [/opt/elasticsearch/jdk], using bundled JDK [true]

[2022-04-17T19:58:02,364][INFO ][o.e.n.Node ] [elk] JVM arguments [-Xshare:auto, -Des.networkaddress.cache.ttl=60, -Des.networkaddress.cache.negative.ttl=10, -Djava.security.manager=allow, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -XX:+ShowCodeDetailsInExceptionMessages, -Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=true, -Dio.netty.recycler.maxCapacityPerThread=0, -Dio.netty.allocator.numDirectArenas=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=true, -Dlog4j2.formatMsgNoLookups=true, -Djava.locale.providers=SPI,COMPAT, --add-opens=java.base/java.io=ALL-UNNAMED, -XX:+UseG1GC, -Djava.io.tmpdir=/tmp/elasticsearch-13977701492846746519, -XX:+HeapDumpOnOutOfMemoryError, -XX:+ExitOnOutOfMemoryError, -XX:HeapDumpPath=data, -XX:ErrorFile=logs/hs\_err\_pid%p.log, -Xlog:gc\*,gc+age=trace,safepoint:file=logs/gc.log:utctime,pid,tags:filecount=32,filesize=64m, -Xms387m, -Xmx387m, -XX:MaxDirectMemorySize=203423744, -XX:G1HeapRegionSize=4m, -XX:InitiatingHeapOccupancyPercent=30, -XX:G1ReservePercent=15, -Des.path.home=/opt/elasticsearch, -Des.path.conf=/etc/elasticsearch, -Des.distribution.flavor=default, -Des.distribution.type=tar, -Des.bundled\_jdk=true]

[2022-04-17T19:58:09,999][INFO ][o.e.p.PluginsService ] [elk] loaded module [aggs-matrix-stats]

[2022-04-17T19:58:10,000][INFO ][o.e.p.PluginsService ] [elk] loaded module [analysis-common]

[2022-04-17T19:58:10,000][INFO ][o.e.p.PluginsService ] [elk] loaded module [constant-keyword]

[2022-04-17T19:58:10,000][INFO ][o.e.p.PluginsService ] [elk] loaded module [data-streams]

[2022-04-17T19:58:10,001][INFO ][o.e.p.PluginsService ] [elk] loaded module [frozen-indices]

[2022-04-17T19:58:10,001][INFO ][o.e.p.PluginsService ] [elk] loaded module [ingest-common]

[2022-04-17T19:58:10,001][INFO ][o.e.p.PluginsService ] [elk] loaded module [ingest-geoip]

[2022-04-17T19:58:10,001][INFO ][o.e.p.PluginsService ] [elk] loaded module [ingest-user-agent]

[2022-04-17T19:58:10,006][INFO ][o.e.p.PluginsService ] [elk] loaded module [kibana]

[2022-04-17T19:58:10,006][INFO ][o.e.p.PluginsService ] [elk] loaded module [lang-expression]

[2022-04-17T19:58:10,007][INFO ][o.e.p.PluginsService ] [elk] loaded module [lang-mustache]

[2022-04-17T19:58:10,007][INFO ][o.e.p.PluginsService ] [elk] loaded module [lang-painless]

[2022-04-17T19:58:10,008][INFO ][o.e.p.PluginsService ] [elk] loaded module [legacy-geo]

[2022-04-17T19:58:10,008][INFO ][o.e.p.PluginsService ] [elk] loaded module [mapper-extras]

[2022-04-17T19:58:10,008][INFO ][o.e.p.PluginsService ] [elk] loaded module [mapper-version]

[2022-04-17T19:58:10,009][INFO ][o.e.p.PluginsService ] [elk] loaded module [old-lucene-versions]

[2022-04-17T19:58:10,009][INFO ][o.e.p.PluginsService ] [elk] loaded module [parent-join]

[2022-04-17T19:58:10,009][INFO ][o.e.p.PluginsService ] [elk] loaded module [percolator]

[2022-04-17T19:58:10,010][INFO ][o.e.p.PluginsService ] [elk] loaded module [rank-eval]

[2022-04-17T19:58:10,010][INFO ][o.e.p.PluginsService ] [elk] loaded module [reindex]

[2022-04-17T19:58:10,010][INFO ][o.e.p.PluginsService ] [elk] loaded module [repositories-metering-api]

[2022-04-17T19:58:10,010][INFO ][o.e.p.PluginsService ] [elk] loaded module [repository-azure]

[2022-04-17T19:58:10,010][INFO ][o.e.p.PluginsService ] [elk] loaded module [repository-encrypted]

[2022-04-17T19:58:10,014][INFO ][o.e.p.PluginsService ] [elk] loaded module [repository-gcs]

[2022-04-17T19:58:10,014][INFO ][o.e.p.PluginsService ] [elk] loaded module [repository-s3]

[2022-04-17T19:58:10,014][INFO ][o.e.p.PluginsService ] [elk] loaded module [repository-url]

[2022-04-17T19:58:10,015][INFO ][o.e.p.PluginsService ] [elk] loaded module [runtime-fields-common]

[2022-04-17T19:58:10,015][INFO ][o.e.p.PluginsService ] [elk] loaded module [search-business-rules]

[2022-04-17T19:58:10,015][INFO ][o.e.p.PluginsService ] [elk] loaded module [searchable-snapshots]

[2022-04-17T19:58:10,015][INFO ][o.e.p.PluginsService ] [elk] loaded module [snapshot-based-recoveries]

[2022-04-17T19:58:10,015][INFO ][o.e.p.PluginsService ] [elk] loaded module [snapshot-repo-test-kit]

[2022-04-17T19:58:10,016][INFO ][o.e.p.PluginsService ] [elk] loaded module [spatial]

[2022-04-17T19:58:10,017][INFO ][o.e.p.PluginsService ] [elk] loaded module [transform]

[2022-04-17T19:58:10,017][INFO ][o.e.p.PluginsService ] [elk] loaded module [transport-netty4]

[2022-04-17T19:58:10,018][INFO ][o.e.p.PluginsService ] [elk] loaded module [unsigned-long]

[2022-04-17T19:58:10,018][INFO ][o.e.p.PluginsService ] [elk] loaded module [vector-tile]

[2022-04-17T19:58:10,022][INFO ][o.e.p.PluginsService ] [elk] loaded module [vectors]

[2022-04-17T19:58:10,022][INFO ][o.e.p.PluginsService ] [elk] loaded module [wildcard]

[2022-04-17T19:58:10,022][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-aggregate-metric]

[2022-04-17T19:58:10,022][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-analytics]

[2022-04-17T19:58:10,024][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-async]

[2022-04-17T19:58:10,024][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-async-search]

[2022-04-17T19:58:10,024][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-autoscaling]

[2022-04-17T19:58:10,024][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-ccr]

[2022-04-17T19:58:10,024][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-core]

[2022-04-17T19:58:10,025][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-deprecation]

[2022-04-17T19:58:10,025][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-enrich]

[2022-04-17T19:58:10,025][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-eql]

[2022-04-17T19:58:10,025][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-fleet]

[2022-04-17T19:58:10,027][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-graph]

[2022-04-17T19:58:10,027][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-identity-provider]

[2022-04-17T19:58:10,027][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-ilm]

[2022-04-17T19:58:10,027][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-logstash]

[2022-04-17T19:58:10,027][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-ml]

[2022-04-17T19:58:10,028][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-monitoring]

[2022-04-17T19:58:10,029][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-ql]

[2022-04-17T19:58:10,029][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-rollup]

[2022-04-17T19:58:10,029][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-security]

[2022-04-17T19:58:10,029][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-shutdown]

[2022-04-17T19:58:10,030][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-sql]

[2022-04-17T19:58:10,030][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-stack]

[2022-04-17T19:58:10,030][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-text-structure]

[2022-04-17T19:58:10,030][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-voting-only-node]

[2022-04-17T19:58:10,030][INFO ][o.e.p.PluginsService ] [elk] loaded module [x-pack-watcher]

[2022-04-17T19:58:10,031][INFO ][o.e.p.PluginsService ] [elk] no plugins loaded

[2022-04-17T19:58:10,147][INFO ][o.e.e.NodeEnvironment ] [elk] using [1] data paths, mounts [[/var/lib/elasticsearch (/dev/root)]], net usable\_space [23.7gb], net total\_space [29gb], types [ext4]

[2022-04-17T19:58:10,148][INFO ][o.e.e.NodeEnvironment ] [elk] heap size [388mb], compressed ordinary object pointers [true]

[2022-04-17T19:58:10,204][INFO ][o.e.n.Node ] [elk] node name [elk], node ID [5BPoY4SnTrOmQ\_xiJFVYtQ], cluster name [elasticsearch], roles [data\_cold, data, remote\_cluster\_client, master, data\_warm, data\_content, transform, data\_hot, ml, data\_frozen, ingest]

[2022-04-17T19:58:22,674][INFO ][o.e.x.m.p.l.CppLogMessageHandler] [elk] [controller/283] [Main.cc@123] controller (64 bit): Version 8.1.0 (Build 36e2300340f08a) Copyright (c) 2022 Elasticsearch BV

[2022-04-17T19:58:23,160][INFO ][o.e.x.s.Security ] [elk] Security is disabled

[2022-04-17T19:58:25,860][INFO ][o.e.t.n.NettyAllocator ] [elk] creating NettyAllocator with the following configs: [name=unpooled, suggested\_max\_allocation\_size=1mb, factors={es.unsafe.use\_unpooled\_allocator=null, g1gc\_enabled=true, g1gc\_region\_size=4mb, heap\_size=388mb}]

[2022-04-17T19:58:25,940][INFO ][o.e.i.r.RecoverySettings ] [elk] using rate limit [40mb] with [default=40mb, read=0b, write=0b, max=0b]

[2022-04-17T19:58:26,049][INFO ][o.e.d.DiscoveryModule ] [elk] using discovery type [multi-node] and seed hosts providers [settings]

[2022-04-17T19:58:31,890][INFO ][o.e.n.Node ] [elk] initialized

[2022-04-17T19:58:31,928][INFO ][o.e.n.Node ] [elk] starting ...

[2022-04-17T19:58:34,864][INFO ][o.e.x.s.c.f.PersistentCache] [elk] persistent cache index loaded

[2022-04-17T19:58:36,305][INFO ][o.e.x.d.l.DeprecationIndexingComponent] [elk] deprecation component started

[2022-04-17T19:58:56,458][INFO ][o.e.t.TransportService ] [elk] publish\_address {172.17.0.2:9300}, bound\_addresses {0.0.0.0:9300}