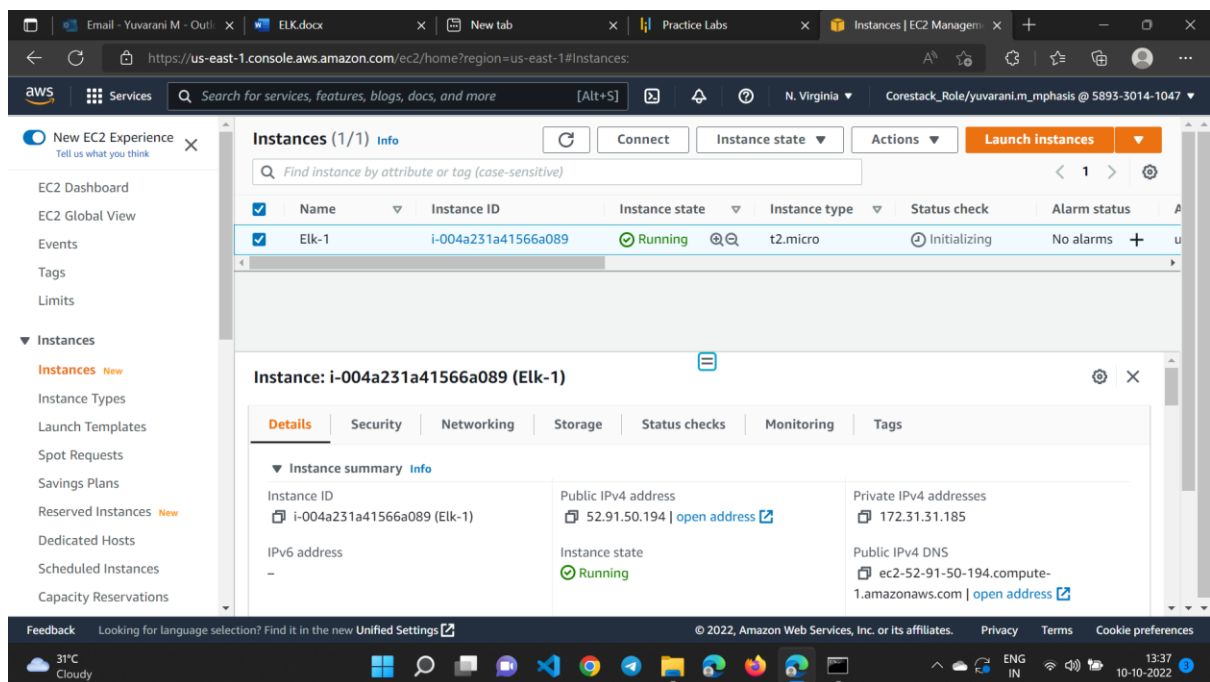
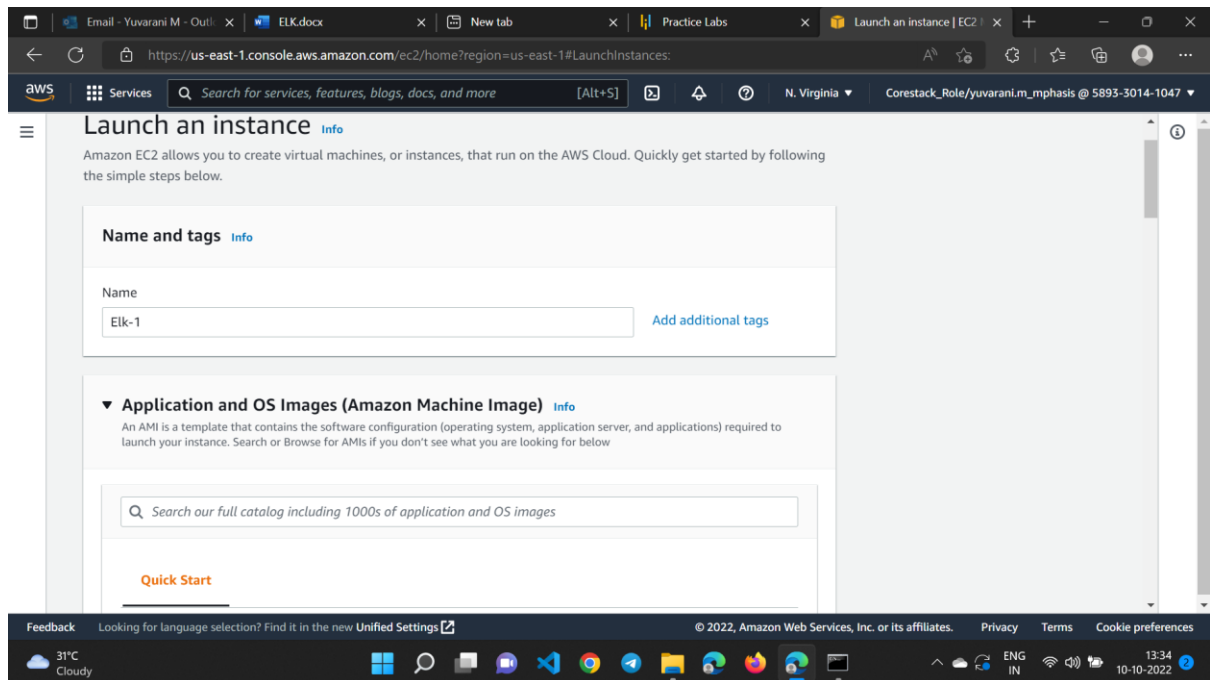
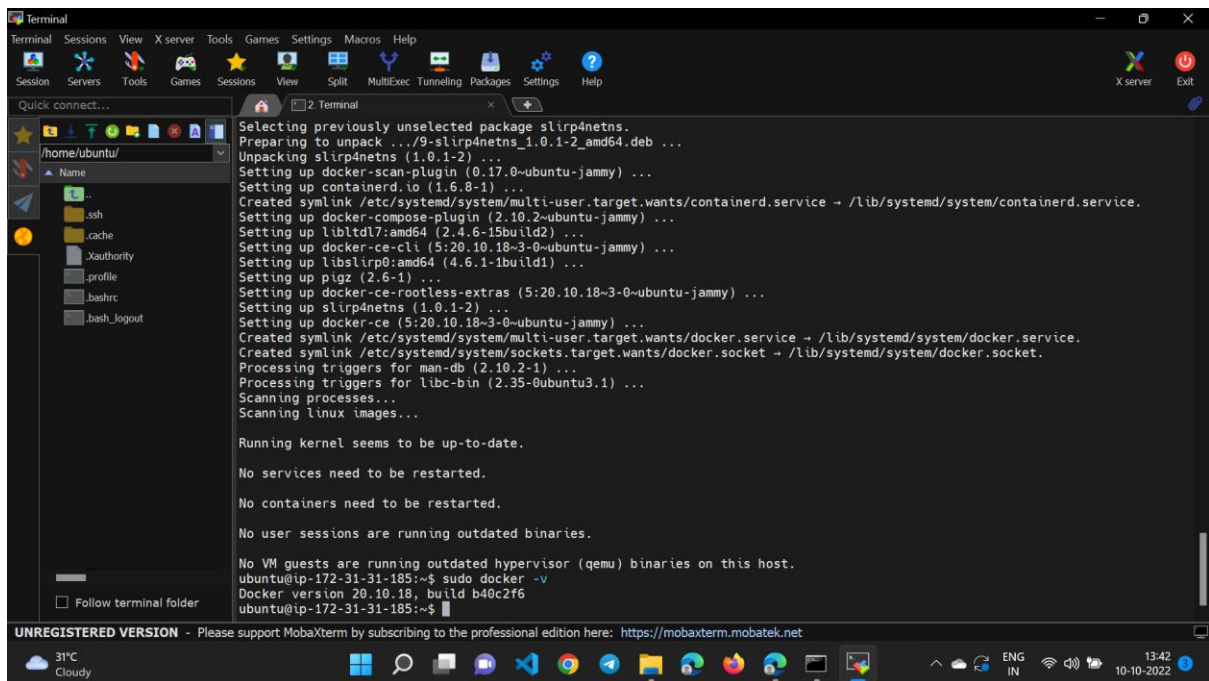


Steps followed in Deploying ELK Stack on Docker Container:

Create an instance:



Create Docker:



```
Terminal
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
/home/ubuntu/
Name
.ssh
.cache
.xauthority
.profile
.bashrc
.bash_logout
Follow terminal folder
Selecting previously unselected package slirp4netns.
Preparing to unpack .../9-slirp4netns_1.0.1-2_amd64.deb ...
Unpacking slirp4netns (1.0.1-2) ...
Setting up docker-scan-plugin (0.17.0-ubuntu-jammy) ...
Setting up containerd.io (1.6.8-1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/containerd.service → /lib/systemd/system/containerd.service.
Setting up docker-compose-plugin (2.10.2-ubuntu-jammy) ...
Setting up libltdl7:amd64 (2.4.6-15build2) ...
Setting up docker-ce-cli (5:20.10.18~3-0-ubuntu-jammy) ...
Setting up libslirp0:amd64 (4.6.1-1build1) ...
Setting up pigz (2.6-1) ...
Setting up docker-ce-rootless-extras (5:20.10.18~3-0-ubuntu-jammy) ...
Setting up slirp4netns (1.0.1-2) ...
Setting up docker-ce (5:20.10.18~3-0-ubuntu-jammy) ...
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 (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

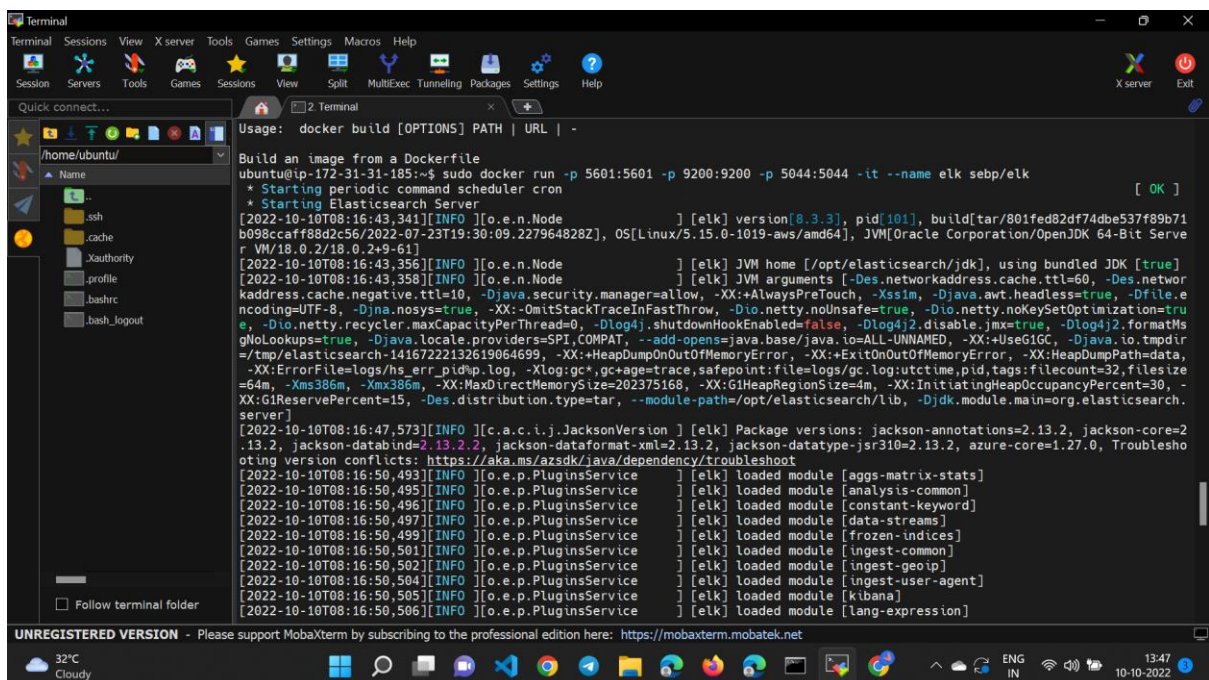
No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-31-185:~$ sudo docker -v
Docker version 20.10.18, build b40c2f6
ubuntu@ip-172-31-31-185:~$
```

Install elastic search:



```
Terminal
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
/home/ubuntu/
Name
.ssh
.cache
.xauthority
.profile
.bashrc
.bash_logout
Follow terminal folder
Usage: docker build [OPTIONS] PATH | URL | -
Build an image from a Dockerfile
ubuntu@ip-172-31-31-185:~$ sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/elk
* Starting periodic command scheduler cron
* Starting Elasticsearch Server
[2022-10-10T08:16:43.341][INFO ][o.e.n.Node               ] [elk] version[8.3.3], pid[101], build[tar/801fed82df74dbe537f89b71
b098ccaff88d2c56/2022-07-23T19:30:09.227964828Z], OS[Linux/5.15.0-1019-aws/amd64], JVM[Oracle Corporation/OpenJDK 64-Bit Serve
r VM/18.0.2/18.0.2+9-61]
[2022-10-10T08:16:43.356][INFO ][o.e.n.Node               ] [elk] JVM home [/opt/elasticsearch/jdk], using bundled JDK [true]
[2022-10-10T08:16:43.358][INFO ][o.e.n.Node               ] [elk] JVM arguments [-Des.networkaddress.cache.ttl=60, -Des.networ
kaddress.cache.negative.ttl=10, -Djava.security.manager=allow, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.e
ncoding=UTF-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=tru
e, -Dio.netty.recycler.maxCapacityPerThread=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=true, -Dlog4j2.formatMs
gNoLookups=true, -Djava.locale.providers=SPI,COMPAT, --add-opens=java.base/java.io=ALL-UNNAMED, -XX:+UseG1GC, -Djava.io.tmpdir
=/tmp/elasticsearch-14167222132619064699, -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, -Xms386m, -Xmx386m, -XX:MaxDirectMemorySize=202375168, -XX:G1HeapRegionSize=4m, -XX:InitiatingHeapOccupancyPercent=30, -
XX:G1ReservePercent=15, -Des.distribution.type=tar, --module-path=/opt/elasticsearch/lib, -Djdk.module.main=org.elasticsearch.
server]
[2022-10-10T08:16:47.573][INFO ][c.a.c.i.j.JacksonVersion ] [elk] Package versions: jackson-annotations=2.13.2, jackson-core=2
.13.2, jackson-databind=2.13.2.2, jackson-dataformat-xml=2.13.2, jackson-datatype-jsr310=2.13.2, jackson-core=1.27.0, Troublesho
oting version conflicts: https://aka.ms/azsdx/java/dependency/troubleshoot
[2022-10-10T08:16:50.493][INFO ][o.e.p.PluginsService     ] [elk] loaded module [aggs-matrix-stats]
[2022-10-10T08:16:50.495][INFO ][o.e.p.PluginsService     ] [elk] loaded module [analysis-common]
[2022-10-10T08:16:50.496][INFO ][o.e.p.PluginsService     ] [elk] loaded module [constant-keyword]
[2022-10-10T08:16:50.497][INFO ][o.e.p.PluginsService     ] [elk] loaded module [data-streams]
[2022-10-10T08:16:50.499][INFO ][o.e.p.PluginsService     ] [elk] loaded module [frozen-indices]
[2022-10-10T08:16:50.501][INFO ][o.e.p.PluginsService     ] [elk] loaded module [ingest-common]
[2022-10-10T08:16:50.502][INFO ][o.e.p.PluginsService     ] [elk] loaded module [ingest-geoip]
[2022-10-10T08:16:50.504][INFO ][o.e.p.PluginsService     ] [elk] loaded module [ingest-user-agent]
[2022-10-10T08:16:50.505][INFO ][o.e.p.PluginsService     ] [elk] loaded module [kibana]
[2022-10-10T08:16:50.506][INFO ][o.e.p.PluginsService     ] [elk] loaded module [lang-expression]
```

The command publishes the following ports:

- 5601 serves the Kibana web interface.
- 9200 for Elasticsearch JSON interface.
- 5044 for Logstash Beats interface.

The three ports are necessary for the stack to work correctly. Additionally, the following ports are exposed but not published:

- 9300 for the transport interface of Elasticsearch (expose with -p 9300:9300).
- 9600 for the Logstash monitoring API (expose with -p 9600:9600).

Access the Kibana web interface with:

<http://<host>:5601>

