

## Phase-5

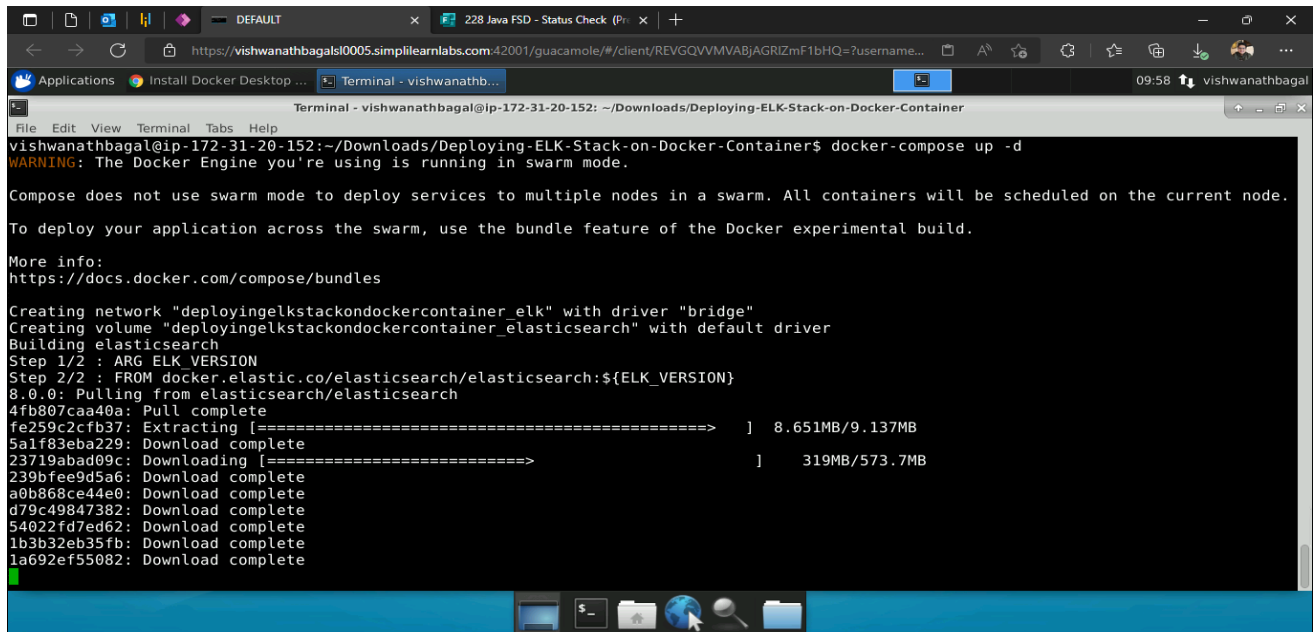
### Deploying ELK Stack on Docker Container

#### DESCRIPTION

##### Project objective:

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

#### Screenshots



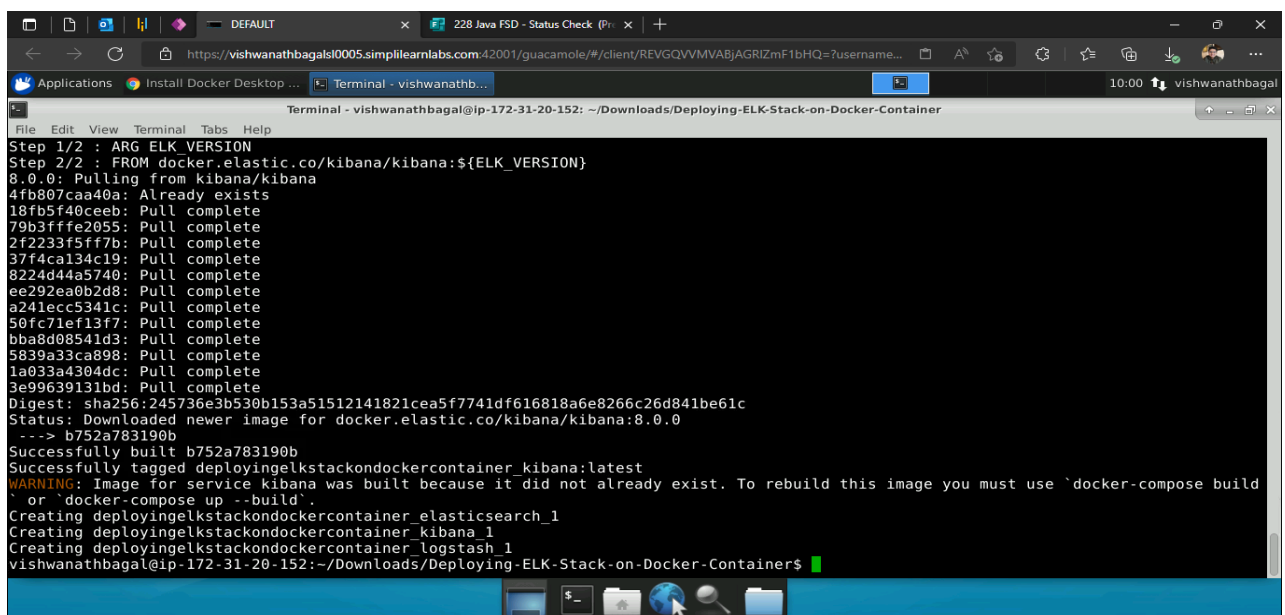
```
vishwanathbaga@ip-172-31-20-152:~/Downloads/Deploying-ELK-Stack-on-Docker-Container$ docker-compose up -d
WARNING: The Docker Engine you're using is running in swarm mode.

Compose does not use swarm mode to deploy services to multiple nodes in a swarm. All containers will be scheduled on the current node.
To deploy your application across the swarm, use the bundle feature of the Docker experimental build.

More info:
https://docs.docker.com/compose/bundles

Creating network "deployingelkstackondockercontainer_elk" with driver "bridge"
Creating volume "deployingelkstackondockercontainer_elasticsearch" with default driver
Building elasticsearch
Step 1/2 : ARG ELK_VERSION
Step 2/2 : FROM docker.elastic.co/elasticsearch/elasticsearch:${ELK_VERSION}
8.0.0: Pulling from elasticsearch/elasticsearch
4fb807caa40a: Pull complete
fe259c2cfb37: Extracting [=====] 8.651MB/9.137MB
5a1f83eba229: Download complete
23719abad09c: Downloading [=====] 319MB/573.7MB
239bf9e9d5a6: Download complete
a0b868ce44e0: Download complete
d79c49847382: Download complete
54022fd7ed62: Download complete
1b3b32eb35fb: Download complete
1a692ef55082: Download complete
```

#### Executing docker-compose up -d



```
Step 1/2 : ARG ELK_VERSION
Step 2/2 : FROM docker.elastic.co/kibana/kibana:${ELK_VERSION}
8.0.0: Pulling from kibana/kibana
4fb807caa40a: Already exists
18fb5f40ceeb: Pull complete
79b3fffe2055: Pull complete
2f2233f5ff7b: Pull complete
37f4ca134c19: Pull complete
8224d44a5740: Pull complete
ee292ea0b2d8: Pull complete
a241ecc5341c: Pull complete
50fc71ef13f7: Pull complete
bba8d08541d3: Pull complete
5839a33ca898: Pull complete
1a033a4304dc: Pull complete
3e99639131bd: Pull complete
Digest: sha256:245736e3b530b153a51512141821cea5f7741df616818a6e8266c26d841be61c
Status: Downloaded newer image for docker.elastic.co/kibana/kibana:8.0.0
--> b752a783190b
Successfully built b752a783190b
Successfully tagged deployingelkstackondockercontainer_kibana:latest
WARNING: Image for service kibana was built because it did not already exist. To rebuild this image you must use `docker-compose build` or `docker-compose up --build`.
Creating deployingelkstackondockercontainer_elasticsearch_1
Creating deployingelkstackondockercontainer_kibana_1
Creating deployingelkstackondockercontainer_logstash_1
vishwanathbaga@ip-172-31-20-152:~/Downloads/Deploying-ELK-Stack-on-Docker-Container$
```

#### Aggregating the containers (Elasticsearch, Logstash, Kibana)

```
Terminal - vishwanathbagal@ip-172-31-20-152: ~/Downloads/Deploying-ELK-Stack-on-Docker-Container
kibana 1 | [2022-10-19T10:00:23.271+00:00][INFO ][plugins.ruleRegistry] Installed resources for index .alerts-observability.up
time.alerts
elasticsearch 1 | {"@timestamp":"2022-10-19T10:00:34.233Z", "log.level": "INFO", "message":"adding component template [metrics-elasti
c_agent.cloudbeat@settings]", "ecs.version": "1.2.0", "service.name":"ES_ECS", "event.dataset":"elasticsearch.server", "process.thread.name":
"elasticsearch[60a830712620][masterService#updateTask][T#1]", "log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplat
eService", "elasticsearch.cluster.uuid":"XNsIJR4gS12_ubVXnKZJ0w", "elasticsearch.node.id":"TAlqa45UTqS4uCFLy6p0bA", "elasticsearch.node.n
ame":"60a830712620", "elasticsearch.cluster.name":"docker-cluster"}
elasticsearch 1 | {"@timestamp":"2022-10-19T10:00:34.290Z", "log.level": "INFO", "message":"adding component template [logs-elastic a
gent.osquerybeat@settings]", "ecs.version": "1.2.0", "service.name":"ES_ECS", "event.dataset":"elasticsearch.server", "process.thread.name":
"elasticsearch[60a830712620][masterService#updateTask][T#1]", "log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplat
eService", "elasticsearch.cluster.uuid":"XNsIJR4gS12_ubVXnKZJ0w", "elasticsearch.node.id":"TAlqa45UTqS4uCFLy6p0bA", "elasticsearch.node.na
me":"60a830712620", "elasticsearch.cluster.name":"docker-cluster"}
kibana 1 | [2022-10-19T10:00:23.403+00:00][INFO ][plugins.ruleRegistry] Installed resources for index .alerts-security.alerts
kibana 1 | [2022-10-19T10:00:23.502+00:00][INFO ][plugins.ruleRegistry] Installed resources for index .alerts-observability.me
trics.alerts
kibana 1 | [2022-10-19T10:00:24.039+00:00][INFO ][plugins.ruleRegistry] Installed resources for index .preview.alerts-security
.alerts
kibana 1 | [2022-10-19T10:00:24.441+00:00][INFO ][plugins.securitySolution.endpoint.metadata:check-transforms-task:0.0.1] no e
ndpoint metadata transforms found
kibana 1 | [2022-10-19T10:00:27.181+00:00][INFO ][status] Kibana is now available (was degraded)
elasticsearch 1 | {"@timestamp":"2022-10-19T10:00:34.347Z", "log.level": "INFO", "message":"adding component template [logs-elastic a
gent.osquerybeat@custom]", "ecs.version": "1.2.0", "service.name":"ES_ECS", "event.dataset":"elasticsearch.server", "process.thread.name":
"elasticsearch[60a830712620][masterService#updateTask][T#1]", "log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplat
eService", "elasticsearch.cluster.uuid":"XNsIJR4gS12_ubVXnKZJ0w", "elasticsearch.node.id":"TAlqa45UTqS4uCFLy6p0bA", "elasticsearch.node.name":
"60a830712620", "elasticsearch.cluster.name":"docker-cluster"}
kibana 1 | [2022-10-19T10:00:27.194+00:00][INFO ][plugins.reporting.store] Creating ILM policy for managing reporting indices:
kibana-reporting
```

## Installation of resources for ELK (Kibana)

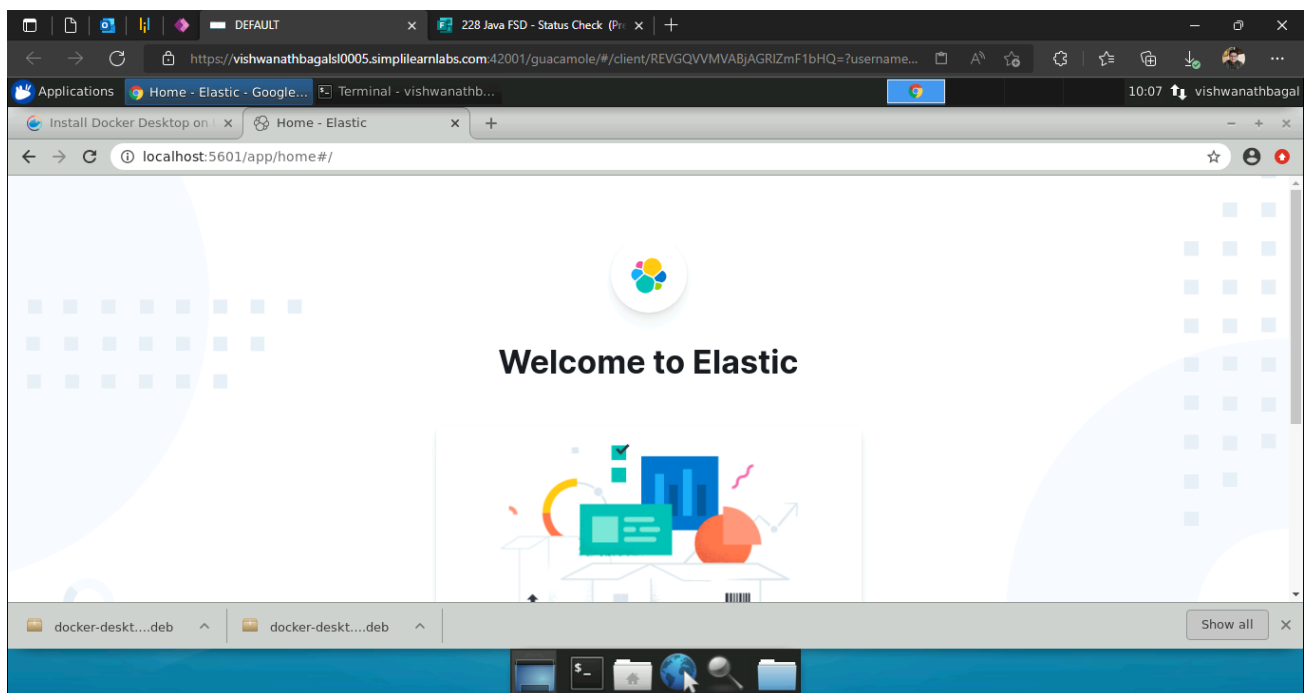
```
Terminal - vishwanathbagal@ip-172-31-20-152: ~/Downloads/Deploying-ELK-Stack-on-Docker-Container
on.initialize(/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/bundler-2.3.6/lib/bundler/definition.rb:133) ~[?:?]
logstash 1 | at usr.share.logstash.vendor.bundle.jruby.2 dot 5 dot 0.gems.bundler.minus 2 dot 3 dot 6.lib.bundler.dsl.to_d
efinition(/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/bundler-2.3.6/lib/bundler/dsl.rb:221) ~[?:?]
logstash 1 | at usr.share.logstash.vendor.bundle.jruby.2 dot 5 dot 0.gems.bundler.minus 2 dot 3 dot 6.lib.bundler.dsl.eval
uate(/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/bundler-2.3.6/lib/bundler/dsl.rb:13) ~[?:?]
logstash 1 | at usr.share.logstash.vendor.bundle.jruby.2 dot 5 dot 0.gems.bundler.minus 2 dot 3 dot 6.lib.bundler.definiti
on.build(/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/bundler-2.3.6/lib/bundler/definition.rb:38) ~[?:?]
logstash 1 | at usr.share.logstash.vendor.bundle.jruby.2 dot 5 dot 0.gems.bundler.minus 2 dot 3 dot 6.lib.bundler.definiti
on(/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/bundler-2.3.6/lib/bundler.rb:197) ~[?:?]
logstash 1 | at usr.share.logstash.vendor.bundle.jruby.2 dot 5 dot 0.gems.bundler.minus 2 dot 3 dot 6.lib.bundler.setup(/u
sr/share/logstash/vendor/bundle/jruby/2.5.0/gems/bundler-2.3.6/lib/bundler.rb:145) ~[?:?]
logstash 1 | at usr.share.logstash.lib.bootstrap.bundler.setup!(/usr/share/logstash/lib/bootstrap/bundler.rb:87) ~[?:?]
logstash 1 | at usr.share.logstash.lib.bootstrap.environment.<main>(/usr/share/logstash/lib/bootstrap/environment.rb:89) ~[
?:?]
deployingelkstackondockercontainer logstash 1 exited with code 1
elasticsearch 1 | {"@timestamp":"2022-10-19T10:05:16.840Z", "log.level": "INFO", "message":"[.kibana 8.0.0_001/VIBc0YSM0yyuEaV1q7DK4w
] update_mapping [ doc]", "ecs.version": "1.2.0", "service.name":"ES_ECS", "event.dataset":"elasticsearch.server", "process.thread.name":
"elasticsearch[60a830712620][masterService#updateTask][T#1]", "log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService",
"elasticsearch.cluster.uuid":"XNsIJR4gS12_ubVXnKZJ0w", "elasticsearch.node.id":"TAlqa45UTqS4uCFLy6p0bA", "elasticsearch.node.name":"60a8
30712620", "elasticsearch.cluster.name":"docker-cluster"}
elasticsearch 1 | {"@timestamp":"2022-10-19T10:05:17.050Z", "log.level": "INFO", "message":"[.kibana 8.0.0_001/VIBc0YSM0yyuEaV1q7DK4w
] update_mapping [ doc]", "ecs.version": "1.2.0", "service.name":"ES_ECS", "event.dataset":"elasticsearch.server", "process.thread.name":
"elasticsearch[60a830712620][masterService#updateTask][T#1]", "log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService",
"elasticsearch.cluster.uuid":"XNsIJR4gS12_ubVXnKZJ0w", "elasticsearch.node.id":"TAlqa45UTqS4uCFLy6p0bA", "elasticsearch.node.name":"60a8
30712620", "elasticsearch.cluster.name":"docker-cluster"}
```

## Installation of resources for ELK (Logstash)

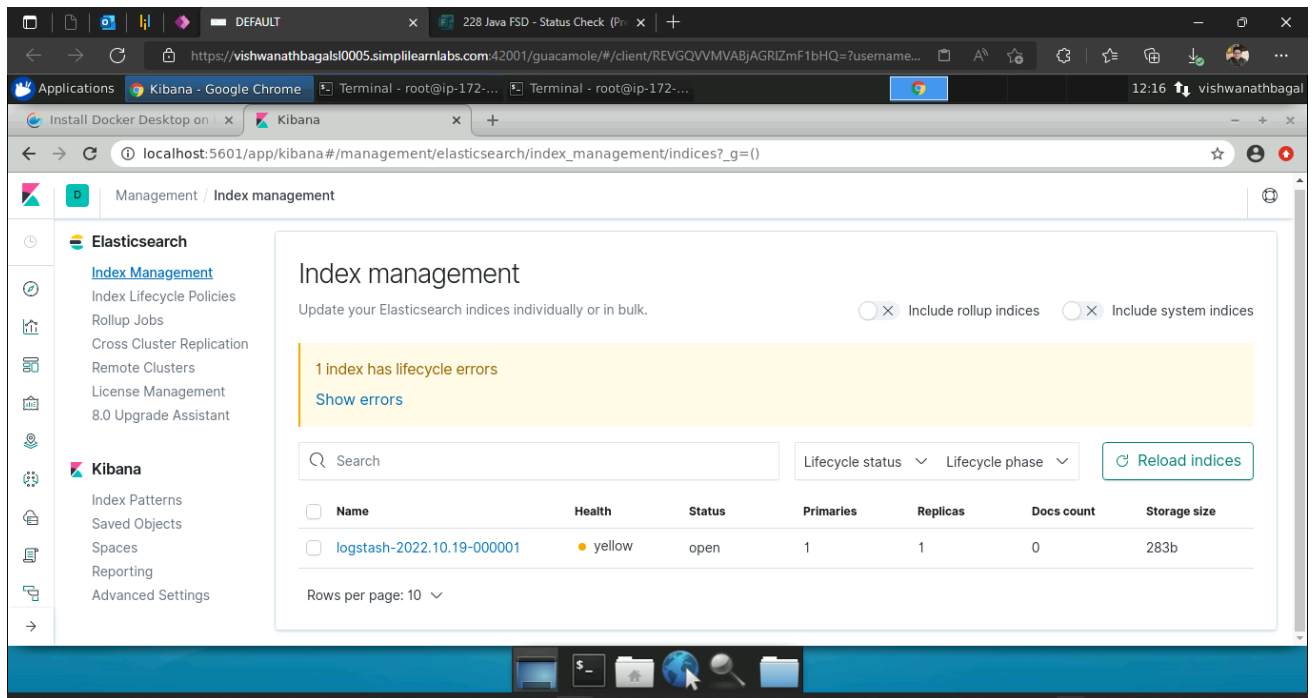
```
Terminal - vishwanathb...
Terminal - vishwanathb@ip-172-31-20-152: ~/Downloads/Deploying-ELK-Stack-on-Docker-Container

S4uCFLy6p0bA", "elasticsearch.node.name": "60a830712620", "elasticsearch.cluster.name": "docker-cluster"}
elasticsearch_1 | {"@timestamp": "2022-10-19T10:00:24.577Z", "log.level": "INFO", "message": "moving index [.kibana-event-log-8.0.0-000001] from [null] to [{\"phase\": \"new\", \"action\": \"complete\", \"name\": \"complete\"}] in policy [kibana-event-log-policy]\", \"ecs.version\": \"1.2.0\", \"service.name\": \"ES_ECS\", \"event.dataset\": \"elasticsearch.server\", \"process.thread.name\": \"elasticsearch[60a830712620][masterService#updateTask][T#1]\", \"log.logger\": \"org.elasticsearch.xpack.ilm.IndexLifecycleTransition\", \"elasticsearch.cluster.uuid\": \"XNsIJR4gS12_ubVXnKZJ0w\", \"elasticsearch.node.id\": \"TAlqa45UTqS4uCFLy6p0bA\", \"elasticsearch.node.name\": \"60a830712620\", \"elasticsearch.cluster.name\": \"docker-cluster\"}
elasticsearch_1 | {"@timestamp": "2022-10-19T10:00:24.823Z", "log.level": "INFO", "message": "[.kibana 8.0.0_001/VIBc0YSMQyyuEaV1q7DK4w] update_mapping [doc]\", \"ecs.version\": \"1.2.0\", \"service.name\": \"ES_ECS\", \"event.dataset\": \"elasticsearch.server\", \"process.thread.name\": \"elasticsearch[60a830712620][masterService#updateTask][T#1]\", \"log.logger\": \"org.elasticsearch.cluster.metadata.MetadataMappingService\", \"elasticsearch.cluster.uuid\": \"XNsIJR4gS12_ubVXnKZJ0w\", \"elasticsearch.node.id\": \"TAlqa45UTqS4uCFLy6p0bA\", \"elasticsearch.node.name\": \"60a830712620\", \"elasticsearch.cluster.name\": \"docker-cluster\"}
elasticsearch_1 | {"@timestamp": "2022-10-19T10:00:25.024Z", "log.level": "WARN", "message": "Creating processor [set security user] (tag [null]) on field [security] but authentication is not currently enabled on this cluster - this processor is likely to fail at runtime if it is used\", \"ecs.version\": \"1.2.0\", \"service.name\": \"ES_ECS\", \"event.dataset\": \"elasticsearch.server\", \"process.thread.name\": \"elasticsearch[60a830712620][clusterApplierService#updateTask][T#1]\", \"log.logger\": \"org.elasticsearch.xpack.security.ingest.SetSecurityUserProcessor\", \"elasticsearch.cluster.uuid\": \"XNsIJR4gS12_ubVXnKZJ0w\", \"elasticsearch.node.id\": \"TAlqa45UTqS4uCFLy6p0bA\", \"elasticsearch.node.name\": \"60a830712620\", \"elasticsearch.cluster.name\": \"docker-cluster\"}
elasticsearch_1 | {"@timestamp": "2022-10-19T10:00:25.098Z", "log.level": "INFO", "message": "moving index [.kibana-event-log-8.0.0-000001] from [{\"phase\": \"new\", \"action\": \"complete\", \"name\": \"complete\"}] to [{\"phase\": \"hot\", \"action\": \"unfollow\", \"name\": \"branch-check-unfollow-prerequisites\"}] in policy [kibana-event-log-policy]\", \"ecs.version\": \"1.2.0\", \"service.name\": \"ES_ECS\", \"event.dataset\": \"elasticsearch.server\", \"process.thread.name\": \"elasticsearch[60a830712620][masterService#updateTask][T#1]\", \"log.logger\": \"org.elasticsearch.xpack.ilm.IndexLifecycleTransition\", \"elasticsearch.cluster.uuid\": \"XNsIJR4gS12_ubVXnKZJ0w\", \"elasticsearch.node.id\": \"TAlqa45UTqS4uCFLy6p0bA\", \"elasticsearch.node.name\": \"60a830712620\", \"elasticsearch.cluster.name\": \"docker-cluster\"}
elasticsearch_1 | {"@timestamp": "2022-10-19T10:00:25.335Z", "log.level": "INFO", "message": "moving index [.kibana-event-log-8.0.0-000001] from [{\"phase\": \"hot\", \"action\": \"unfollow\", \"name\": \"branch-check-unfollow-prerequisites\"}] to [{\"phase\": \"hot\", \"action\": \"rollover\", \"name\": \"check-rollover-ready\"}] in policy [kibana-event-log-policy]\", \"ecs.version\": \"1.2.0\", \"service.name\": \"ES_
```

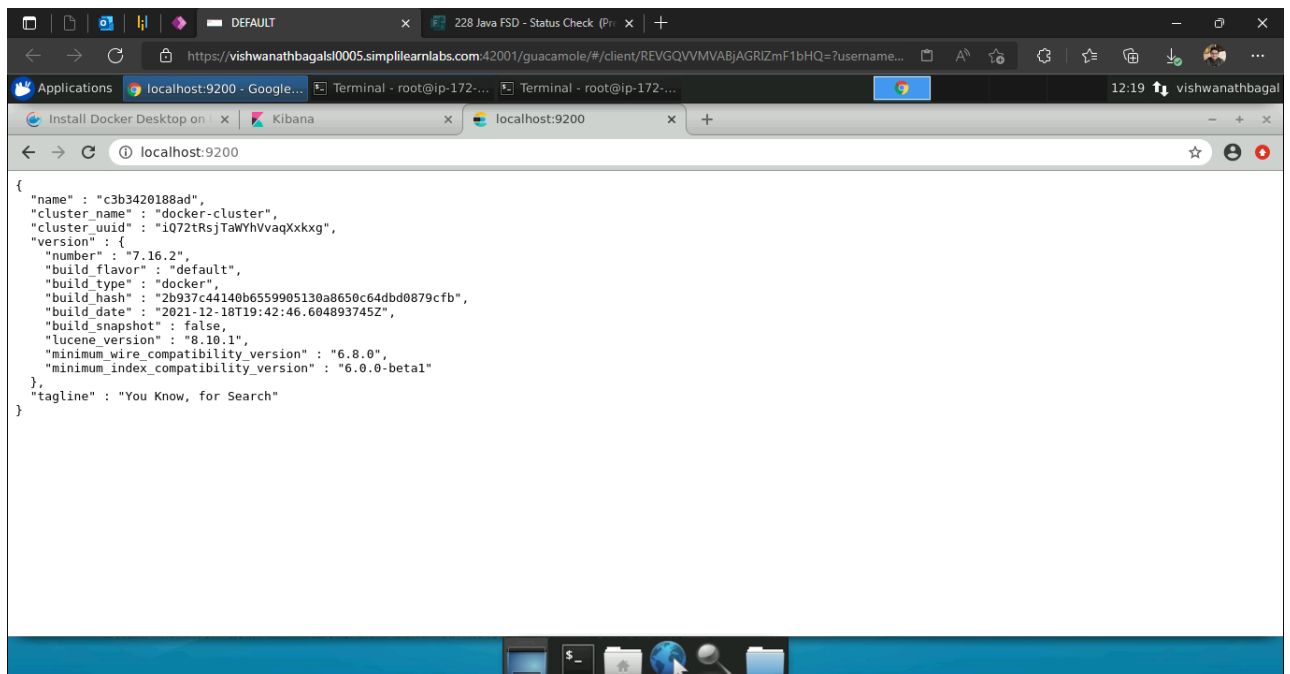
## Installation of resources for ELK (Elasticsearch)



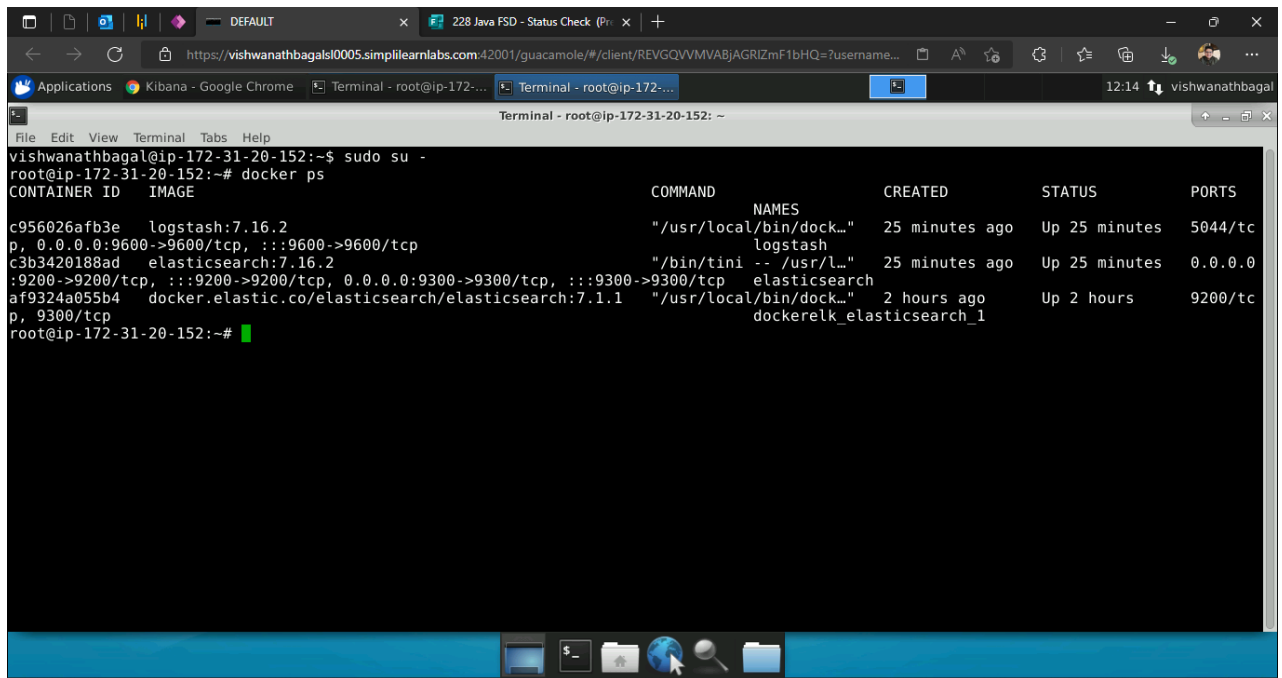
## Accessing the Kibana through browser using localhost:5601



## Index management of Kibana displaying status of Logstash launched



## Container details of Elasticsearch after resources installation



```
vishwanathbagal@ip-172-31-20-152:~$ sudo su -
root@ip-172-31-20-152:~# docker ps
```

CONTAINER ID	IMAGE	COMMAND	NAMES	CREATED	STATUS	PORTS
c956026afb3e	logstash:7.16.2	"/usr/local/bin/dock..."	logstash	25 minutes ago	Up 25 minutes	5044/tcp
p, 0.0.0.0:9600->9600/tcp, :::9600->9600/tcp						
c3b3420188ad	elasticsearch:7.16.2	"/bin/tini -- /usr/l..."	elasticsearch	25 minutes ago	Up 25 minutes	0.0.0.0
:9200->9200/tcp, :::9200->9200/tcp, 0.0.0.0:9300->9300/tcp, :::9300->9300/tcp						
af9324a055b4	docker.elastic.co/elasticsearch/elasticsearch:7.1.1	"/usr/local/bin/dock..."	docker.elastic.co/elasticsearch/elasticsearch_1	2 hours ago	Up 2 hours	9200/tcp
p, 9300/tcp						

```
root@ip-172-31-20-152:~#
```

List containers. The "size" information shows the amount of data (on disk) that is used for the writable layer of each container loaded using **docker ps** command