

## PHASE 5

### PRACTICE PROJECT 5

#### Deploy ELK Stack on Docker Container

#### OUTPUT:

#### Run Docker Container:

```
File Edit View Terminal Tabs Help
kaviyaxmphasis@ip-172-31-17-95:~$ sudo docker run hello-world

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
   (amd64)
3. The Docker daemon created a new container from that image which runs the
   executable that produces the output you are currently reading.
4. The Docker daemon streamed that output to the Docker client, which sent it
   to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/
kaviyaxmphasis@ip-172-31-17-95:~$
```

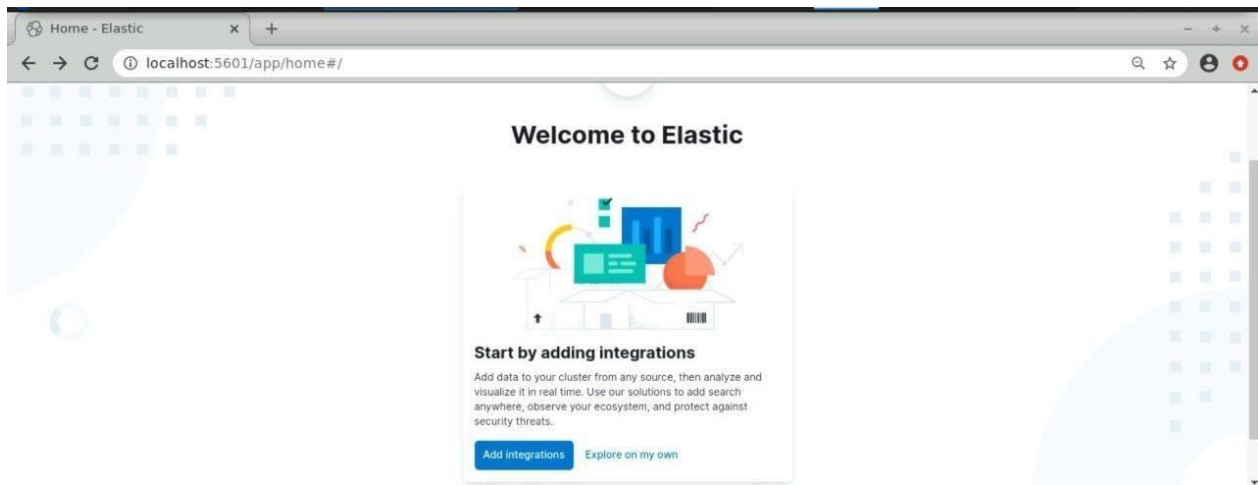
#### Creating yml and log files:

```
File Edit View Terminal Tabs Help
kaviyaxmphasis@ip-172-31-17-95:~$ mkdir elk
mkdir: cannot create directory 'elk': File exists
kaviyaxmphasis@ip-172-31-17-95:~$ cd elk
kaviyaxmphasis@ip-172-31-17-95:~/elk$ mkdir logstash
mkdir: cannot create directory 'logstash': File exists
kaviyaxmphasis@ip-172-31-17-95:~/elk$ ls
logstash
kaviyaxmphasis@ip-172-31-17-95:~/elk$ cd logstash
kaviyaxmphasis@ip-172-31-17-95:~/elk/logstash$ ls
logstash.conf
kaviyaxmphasis@ip-172-31-17-95:~/elk/logstash$ vi.logstash.conf
vi.logstash.conf: command not found
kaviyaxmphasis@ip-172-31-17-95:~/elk/logstash$ vi.logstash.conf
vi.logstash.conf: command not found
kaviyaxmphasis@ip-172-31-17-95:~/elk/logstash$ vi logstash.conf
kaviyaxmphasis@ip-172-31-17-95:~/elk/logstash$ ls
logstash.conf
kaviyaxmphasis@ip-172-31-17-95:~/elk/logstash$ pwd
/home/kaviyaxmphasis/elk/logstash
kaviyaxmphasis@ip-172-31-17-95:~/elk/logstash$ cd ..
kaviyaxmphasis@ip-172-31-17-95:~/elk$ vi docker-compose.yml
kaviyaxmphasis@ip-172-31-17-95:~/elk$ ls
docker-compose.yml logstash
kaviyaxmphasis@ip-172-31-17-95:~/elk$ cd -
kaviyaxmphasis@ip-172-31-17-95:~$ pwd
/home/kaviyaxmphasis
kaviyaxmphasis@ip-172-31-17-95:~$ mkdir temp
kaviyaxmphasis@ip-172-31-17-95:~$ cd temp
kaviyaxmphasis@ip-172-31-17-95:~/temp$ ls
kaviyaxmphasis@ip-172-31-17-95:~/temp$ vi inlog.log
kaviyaxmphasis@ip-172-31-17-95:~/temp$ ls
inlog.log
```

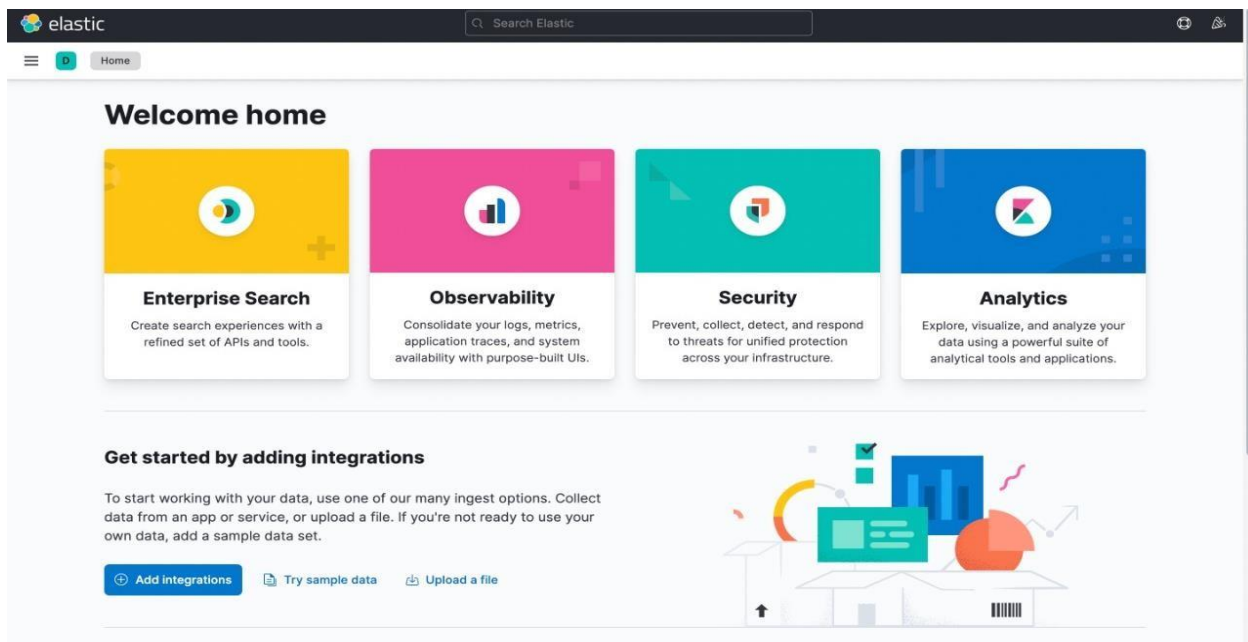
```
File Edit View Terminal Tabs Help
docker-compose.yml logstash
kaviyaxmphasis@ip-172-31-17-95:~/elk$ cd -
kaviyaxmphasis@ip-172-31-17-95:~$ pwd
/home/kaviyaxmphasis
kaviyaxmphasis@ip-172-31-17-95:~$ mkdir temp
kaviyaxmphasis@ip-172-31-17-95:~$ cd temp
kaviyaxmphasis@ip-172-31-17-95:~/temp$ ls
kaviyaxmphasis@ip-172-31-17-95:~/temp$ vi inlog.log
kaviyaxmphasis@ip-172-31-17-95:~/temp$ ls
inlog.log
kaviyaxmphasis@ip-172-31-17-95:~/temp$ cd ..
kaviyaxmphasis@ip-172-31-17-95:~$ ls
Desktop Downloads ELK-STACK Pictures temp thinclient_drives
Documents elk Music Public Templates Videos
kaviyaxmphasis@ip-172-31-17-95:~$ cd elk
kaviyaxmphasis@ip-172-31-17-95:~/elk$ ls
docker-compose.yml logstash
kaviyaxmphasis@ip-172-31-17-95:~/elk$ docker-compose up
The program 'docker-compose' is currently not installed. To run 'docker-compose'
please ask your administrator to install the package 'docker-compose'
kaviyaxmphasis@ip-172-31-17-95:~/elk$ docker-compose version
The program 'docker-compose' is currently not installed. To run 'docker-compose'
please ask your administrator to install the package 'docker-compose'
kaviyaxmphasis@ip-172-31-17-95:~/elk$ sudo amazon-linux-extras install docker
sudo: amazon-linux-extras: command not found
kaviyaxmphasis@ip-172-31-17-95:~/elk$ sudo service docker start
kaviyaxmphasis@ip-172-31-17-95:~/elk$ sudo usermod -a -G docker ec2-user
usermod: user 'ec2-user' does not exist
kaviyaxmphasis@ip-172-31-17-95:~/elk$ sudo chkconfig docker on
sudo: chkconfig: command not found
kaviyaxmphasis@ip-172-31-17-95:~/elk$ sudo yum install -y git
sudo: yum: command not found
```

## Installing ELK Stacks:

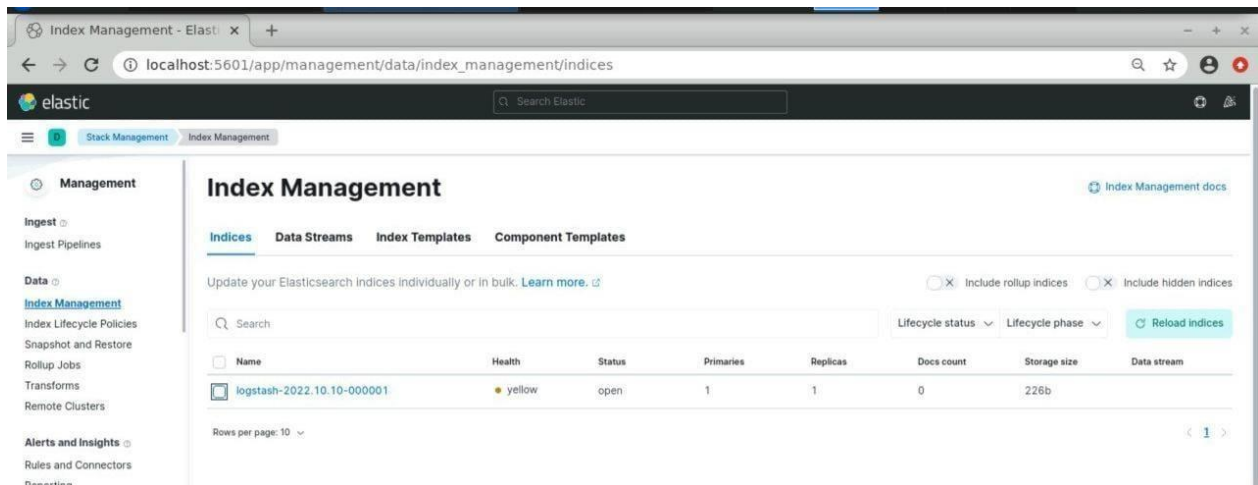
## Run Localhost:5601 to connect with Elastic:



## Explore the Integrations:



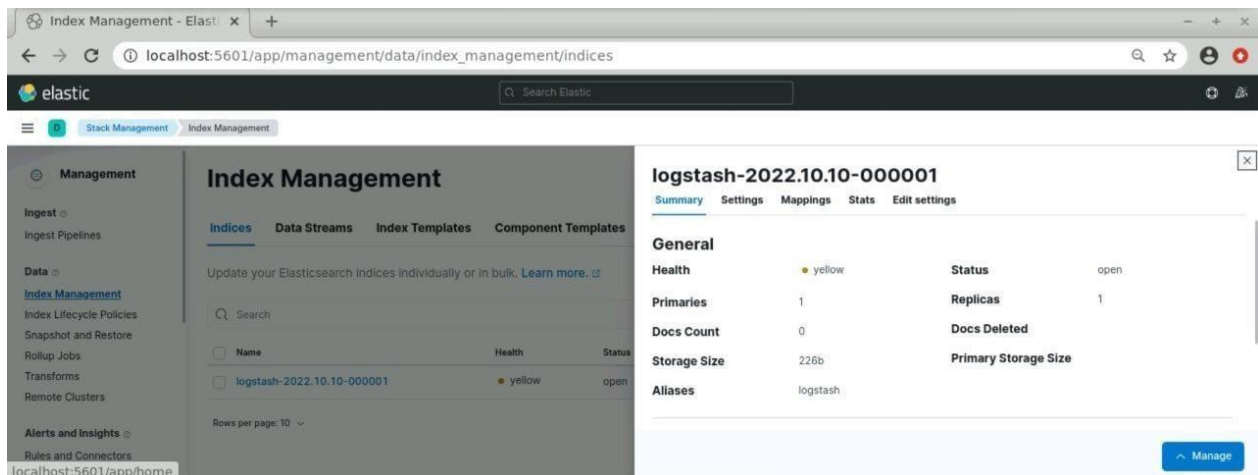
## Index Management:



The screenshot shows the Elastic Index Management interface. The left sidebar contains navigation links for Management, Ingest, Data, and Alerts and Insights. The main content area is titled "Index Management" and includes tabs for Indices, Data Streams, Index Templates, and Component Templates. A search bar and filters for Lifecycle status and Lifecycle phase are present. A table lists indices with columns for Name, Health, Status, Primaries, Replicas, Docs count, Storage size, and Data stream. The index "logstash-2022.10.10-000001" is highlighted.

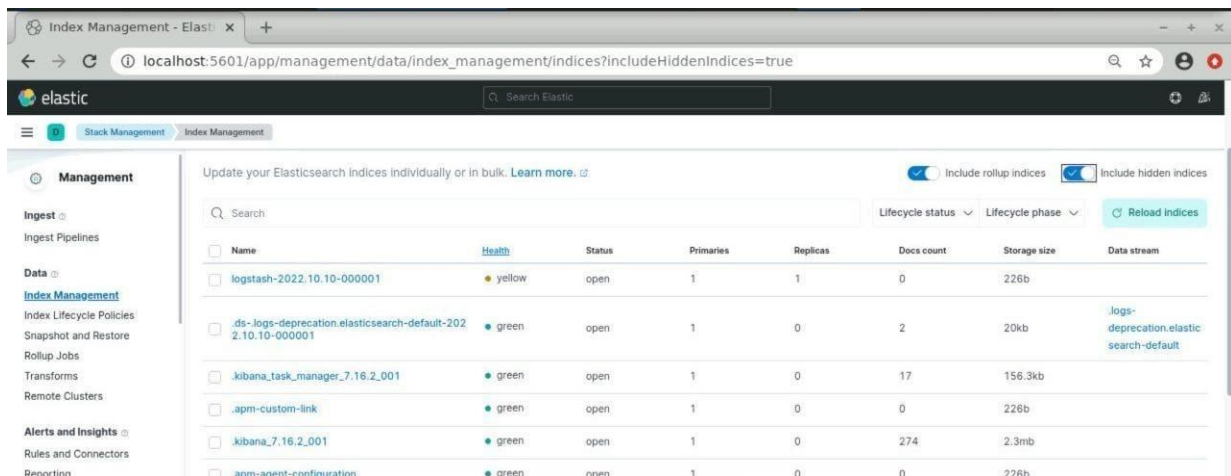
Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
logstash-2022.10.10-000001	yellow	open	1	1	0	226b	

## Check Status of log file:



The screenshot shows the details of the "logstash-2022.10.10-000001" index. The left sidebar is the same as the previous screenshot. The main content area is titled "logstash-2022.10.10-000001" and includes tabs for Summary, Settings, Mappings, Stats, and Edit settings. The "General" section displays the index's Health (yellow), Status (open), Primaries (1), Replicas (1), Docs Count (0), Storage Size (226b), and Aliases (logstash).

Health	Status	Primaries	Replicas	Docs Count	Storage Size	Aliases
yellow	open	1	1	0	226b	logstash



The screenshot shows the Elastic Index Management interface with the "Include hidden indices" checkbox checked. The table lists several indices, including "logstash-2022.10.10-000001" and ".ds-logs-deprecation.elasticsearch-default-2022.10.10-000001".

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
logstash-2022.10.10-000001	yellow	open	1	1	0	226b	
.ds-logs-deprecation.elasticsearch-default-2022.10.10-000001	green	open	1	0	2	20kb	.logs-deprecation.elasticsearch-default
.kibana_task_manager_7.16.2_001	green	open	1	0	17	156.3kb	
.apm-custom-link	green	open	1	0	0	226b	
.kibana_7.16.2_001	green	open	1	0	274	2.3mb	
.apm-agent-configuration	green	open	1	0	0	226b	