

1.Run Docker Container:

2.Creating yml and log files:

```
ip-172-31-27-237:~$ mkdir elk
ip-172-31-27-237:~$ cd elk
ip-172-31-27-237:~/elk$ ls
ip-172-31-27-237:~/elk$ mkdir logstash
ip-172-31-27-237:~/elk$ ls

ip-172-31-27-237:~/elk$ cd logstash
ip-172-31-27-237:~/elk/logstash$ ls
ip-172-31-27-237:~/elk/logstash$ vi logstash.conf
ip-172-31-27-237:~/elk/logstash$ ls

ip-172-31-27-237:~/elk/logstash$ pwd
hirmpp/elk/logstash
ip-172-31-27-237:~/elk/logstash$ cd ..
ip-172-31-27-237:~/elk$ ls

ip-172-31-27-237:~/elk$ vi docker-compose.yml
ip-172-31-27-237:~/elk$ ls
ml  logstash
ip-172-31-27-237:~/elk$ cd ~
ip-172-31-27-237:~$ pwd
hirmpp
ip-172-31-27-237:~$ mkdir temp
ip-172-31-27-237:~$ cd temp
ip-172-31-27-237:~/temp$ ls
ip-172-31-27-237:~/temp$ vi inlog.log
ip-172-31-27-237:~/temp$ █
```

```
ip-172-31-27-237:~/elk/logstash$ vi logstash.conf
ip-172-31-27-237:~/elk/logstash$ ls

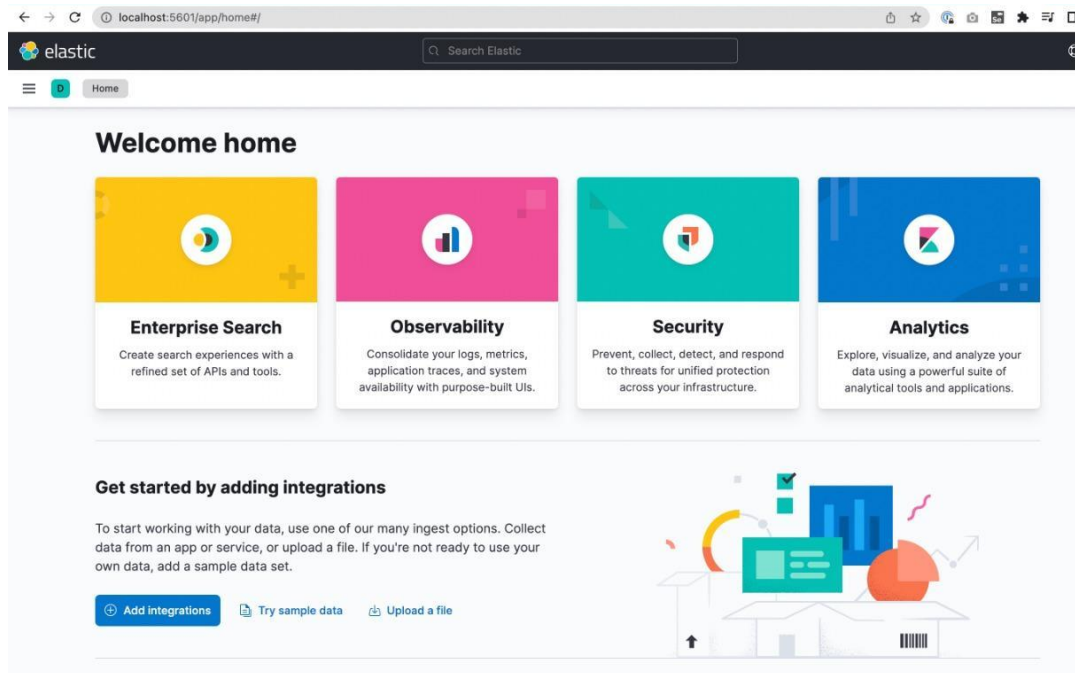
ip-172-31-27-237:~/elk/logstash$ pwd
hirmpp/elk/logstash
ip-172-31-27-237:~/elk/logstash$ cd ..
ip-172-31-27-237:~/elk$ ls

ip-172-31-27-237:~/elk$ vi docker-compose.yml
ip-172-31-27-237:~/elk$ ls
ml  logstash
ip-172-31-27-237:~/elk$ cd ~
ip-172-31-27-237:~$ pwd
hirmpp
ip-172-31-27-237:~$ mkdir temp
ip-172-31-27-237:~$ cd temp
ip-172-31-27-237:~/temp$ ls
ip-172-31-27-237:~/temp$ vi inlog.log
ip-172-31-27-237:~/temp$ cd ..
ip-172-31-27-237:~$ ls
elk  Documents  elk  Pictures  temp  thinclient_drives
python  Downloads  Music  Public  Templates  Videos
ip-172-31-27-237:~$ cd elk
ip-172-31-27-237:~/elk$ ls
ml  logstash
ip-172-31-27-237:~/elk$ docker-compose up -d
docker-compose is currently not installed. To run 'docker-compose' please ask your administrator to install the package
```

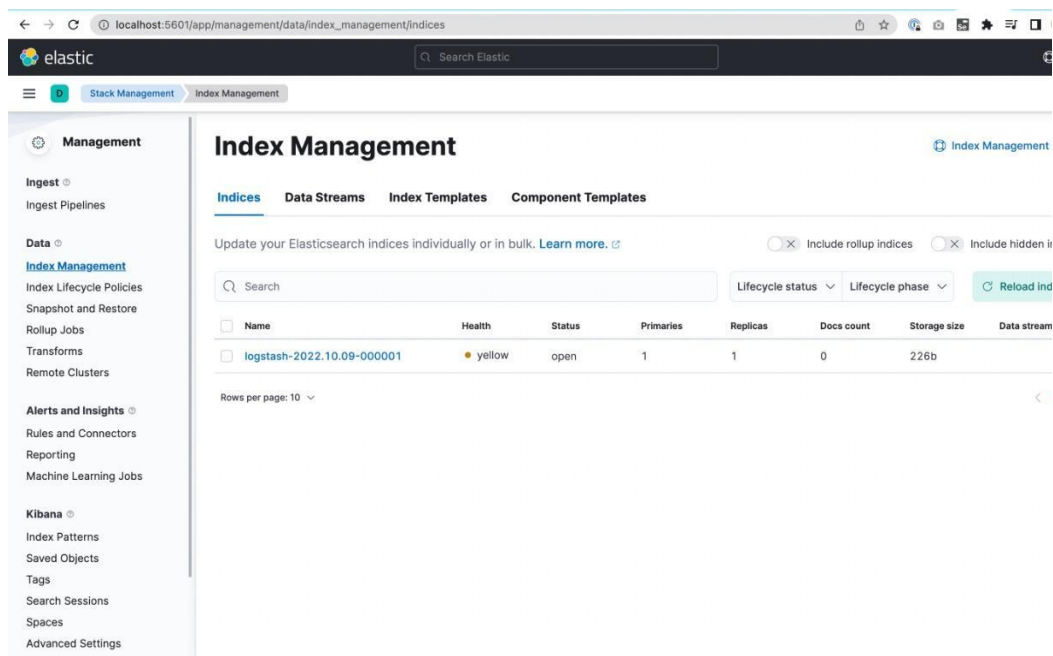
[illegible]

The screenshot shows the Elastic search engine homepage in a web browser. The browser's address bar at the top displays 'localhost:5601/app/home#/' with navigation icons on the left and extension icons on the right. The main content area has a light gray background with a subtle pattern of squares on the left. At the top center is the Elastic logo, a circle containing five colored dots (blue, green, yellow, orange, red). Below the logo is the heading 'Welcome to Elastic' in a large, bold, black font. Underneath the heading is a white rectangular box containing an illustration of a warehouse with a forklift, overlaid with various data visualization icons like a bar chart, a line graph, and a pie chart. Below the illustration, the text 'Start by adding integrations' is displayed in bold. This is followed by a paragraph: 'Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats.' At the bottom of this white box are two buttons: a blue button labeled 'Add Integrations' and a gray button labeled 'Explore on my own'. Below the white box, a paragraph of text reads: 'To learn about how usage data helps us manage and improve our products and services, see our [Privacy Statement](#). To stop collection, [disable usage data here](#).' The browser window's right edge shows a portion of the operating system's taskbar.

## 5.Explore the Integrations:



## 6.Index Management:



7 Check Status of log file:

The screenshot shows the Elastic Index Management interface. On the left is a sidebar with navigation links for Management, Ingest, Data, Alerts and Insights, and Kibana. The main panel is titled 'Index Management' and has tabs for Indices, Data Streams, Index Templates, and Component Templates. The 'Indices' tab is active, showing a table of indices. The index 'logstash-2022.10.09-000001' is highlighted. On the right, a detailed view for this index is shown, including a 'General' section with health status (yellow), primaries (1), docs count (0), storage size (226b), and aliases (logstash). Below this is the 'Index lifecycle management' section, showing the lifecycle policy (logstash-policy), current phase (hot), current action (rollover), and failed step (-).

**Index Management**

Update your Elasticsearch indices individually or in bulk. [Learn more.](#)

Search

Name	Health
logstash-2022.10.09-000001	yellow

Rows per page: 10

### logstash-2022.10.09-000001

Summary Settings Mappings Stats Edit settings

#### General

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

#### Index lifecycle management

Lifecycle policy	logstash-policy	Current phase	hot
Current action	rollover	Current action time	2022-10-09 18:44:44
Failed step	-	Phase definition	<a href="#">Show definition</a>

[Manage](#)

The screenshot shows the Elastic Index Management interface with the 'Indices' tab selected. It displays a table of indices with columns for Name, Health, Status, Primaries, Replicas, Docs count, Storage size, and Data stream. The index 'logstash-2022.10.09-000001' is highlighted. The table also includes checkboxes for each index. The 'Data stream' column shows the data stream for each index, such as 'ilm-history-5' and 'logs-deprecation-elasticsearch-default'.

← → ↻ localhost:5601/app/management/data/index\_management/indices?includeHiddenIndices=true

**elastic** Search Elastic

Stack Management Index Management

### Management

Ingest Ingest Pipelines

Data Index Management Index Lifecycle Policies Snapshot and Restore Rollup Jobs Transforms Remote Clusters

Alerts and Insights Rules and Connectors Reporting Machine Learning Jobs

Kibana Index Patterns Saved Objects Tags Search Sessions Spaces Advanced Settings

#### Indices

Update your Elasticsearch indices individually or in bulk. [Learn more.](#)

Include rollout indices Include hidden indices

Search Lifecycle status Lifecycle phase Reload indices

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
.apm-custom-link	green	open	1	0	0	226b	
.kibana_task_manager_7.16.2_001	green	open	1	0	17	261.2kb	
.kibana_7.16.2_001	green	open	1	0	43	4.8mb	
logstash-2022.10.09-000001	yellow	open	1	1	0	226b	
.apm-agent-configuration	green	open	1	0	0	226b	
.ds-ilm-history-5-2022.10.09-000001	green	open	1	0	12	36.7kb	ilm-history-5
.kibana-event-log-7.16.2-000001	green	open	1	0	4	23.6kb	
.tasks	green	open	1	0	4	27.4kb	
.ds-logs-deprecation.elasticsearch-default-2022.10.09-000001	green	open	1	0	25	81.5kb	logs-deprecation-elasticsearch-default

Rows per page: 10