

```
harish@LAPTOP-ELD1IEGI ~$  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
harish@LAPTOP-ELD1IEGI:~$ ls  
elk temp  
harish@LAPTOP-ELD1IEGI:~$ mkdir elk  
mkdir: cannot create directory 'elk': File exists  
harish@LAPTOP-ELD1IEGI:~$ cd elk  
harish@LAPTOP-ELD1IEGI:~/elk$ mkdir logstash  
harish@LAPTOP-ELD1IEGI:~/elk$ ls  
docker-compose.yml logstash logstash.conf  
harish@LAPTOP-ELD1IEGI:~/elk$ vi logstash.conf
```

```
harish@LAPTOP-ELD1IEGI ~$  
Input {  
  file {  
    path => "/root/temp/inlog.log"  
  }  
}  
output {  
  elasticsearch {  
    hosts => ["http://elasticsearch:9200"]  
  }  
}
```

```
harish@LAPTOP-ELD1IEGI ~$  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
harish@LAPTOP-ELD1IEGI:~$ cd logstash/  
-bash: cd: logstash/: No such file or directory  
harish@LAPTOP-ELD1IEGI:~$ cd elk  
harish@LAPTOP-ELD1IEGI:~/elk$ cd logstash/  
harish@LAPTOP-ELD1IEGI:~/elk/logstash$ ls  
logstash.conf  
harish@LAPTOP-ELD1IEGI:~/elk/logstash$ pwd  
/home/harish/elk/logstash  
harish@LAPTOP-ELD1IEGI:~/elk/logstash$ cd ..  
harish@LAPTOP-ELD1IEGI:~/elk$ ls  
docker-compose.yml logstash logstash logstssh.conf  
harish@LAPTOP-ELD1IEGI:~/elk$ vi docker-compose.yml
```

```
This is a test file  
this is a second line
```

```
:wq!_
```

```
version: '3.6'  
services:  
  Elasticsearch:  
    image: elasticsearch:7.16.2  
    container_name: elasticsearch  
    restart: always  
    volumes:  
      - elastic_data:/usr/share/elasticsearch/data/  
    environment:  
      ES_JAVA_OPTS: "-Xms256m -Xmx256m"  
      discovery.type: single-node  
    ports:  
      - '9200:9200'  
      - '9300:9300'  
    networks:  
      - elk  
  
  Logstash:  
    image: logstash:7.16.2  
    container_name: logstash  
    restart: always  
    volumes:  
      - ./logstash:/logstash_dir  
    command: logstash -f /logstash_dir/logstash.conf  
    depends_on:  
      - Elasticsearch  
    ports:  
      - '5000:5000'  
    environment:  
      LS_JAVA_OPTS: "-Xms256m -Xmx256m"  
    networks:  
      - elk
```

```
:wq!_
```



```

kibana | [{"type": "log", "@timestamp": "2023-07-31T08:07:41+00:00", "tags": ["info", "http", "server", "Preboot"], "pid": 7, "message": "http server running at http://0.0.0.0:5601"}]
kibana | [{"type": "log", "@timestamp": "2023-07-31T08:07:41+00:00", "tags": ["warning", "config", "deprecation"], "pid": 7, "message": "Starting in 8.0, the Kibana logging format will be changing. This may affect you if you are doing any special handling of your Kibana logs, such as ingesting logs into Elasticsearch for further analysis. If you are using the new logging configuration, you are already receiving logs in both old and new formats, and the old format will simply be going away. If you are not yet using the new logging configuration, the log format will change upon upgrade to 8.0. Beginning in 8.0, the format of JSOM logs will be ES5-compatible JSOM, and the default pattern log format will be configurable with our new logging system. Please refer to the documentation for more information about the new logging format."}]
kibana | [{"type": "log", "@timestamp": "2023-07-31T08:07:41+00:00", "tags": ["warning", "config", "deprecation"], "pid": 7, "message": "Use Kibana application privileges to grant reporting privileges. Using 'xpack.reporting.roles.allow' to grant reporting privileges is deprecated. The 'xpack.reporting.roles.enabled' setting will default to false in a future release."}]
kibana | [{"type": "log", "@timestamp": "2023-07-31T08:07:41+00:00", "tags": ["warning", "config", "deprecation"], "pid": 7, "message": "User sessions will automatically time out after 8 hours of inactivity starting in 8.0. Override this value to change the timeout."}]
kibana | [{"type": "log", "@timestamp": "2023-07-31T08:07:41+00:00", "tags": ["warning", "config", "deprecation"], "pid": 7, "message": "Users are automatically required to log in again after 30 days starting in 8.0. Override this value to change the timeout."}]
elasticsearch | [{"type": "server", "timestamp": "2023-07-31T08:07:42.307Z", "level": "INFO", "component": "o.s.t.TransportService", "cluster.name": "docker-cluster", "node.name": "a6505677429a", "message": "publish_address [172.18.0.2:9300], bound_addresses [0.0.0.0:9300]"}]
kibana | [{"type": "log", "@timestamp": "2023-07-31T08:07:42+00:00", "tags": ["info", "plugins-system", "standard"], "pid": 7, "message": "Setting up [113] plugins: [translations, licensing, globalSearch, globalSearchProviders, features, licenseApiGuard, code, usageCollection, spackLegacy, taskManager, telemetryCollectionManager, telemetryCollection, kibanaAllStageCollection, share, embeddable, uiActionsEnhanced, screenshotMode, banners, telemetry, newsfeed, mapsEms, mapsLegacy, kibanaLegacy, fieldFormats, expressions, dataViews, charts, adUShared, fetch, data, savedObjects, presentationUtil, expressionShape, expressionRevealImage, expressionRepeatImage, expressionMetric, expressionImage, customIntegrations, home, searchProfiler, painlessLab, grokDebugger, management, watcher, licenseManagement, advancedSettings, spaces, security, savedObjectsIngestion, reporting, canvas, lists, inputPipeline, fileUpload, encryptedSavedObjects, dataEnhanced, cloud, snapshotRestore, eventing, action, alerting, triggerActionsUI, transform, stackAlerts, ruleRegistry, visualizations, visTypeKy, visTypeVizlib, visTypeVega, visTypeTimeline, visTypeTagcloud, visTypeTable, visTypePie, visTypeMetric, visTypeStacked, tileMap, regionMap, expressionTagcloud, expressionMetricViz, console, graph, fleet, indexManagement, remoteClusters, crs, clusterReplication, indexLifecycleManagement, dashboard, maps, dashboardMode, dashboardEnhanced, visualize, visTypeTimeSeries, rollup, indexPatternFieldEditor, lens, cases, timelines, discover, query, observability, discoverEnhanced, dataVisualizer, el, uptime, securitydetection, infra, upgradeAssistant, monitoring, logstash, enterpriseSearch, agw, savedObjectsManagement, indexPatternManagement]}]
kibana | [{"type": "log", "@timestamp": "2023-07-31T08:07:43+00:00", "tags": ["info", "plugins", "taskManager"], "pid": 7, "message": "TaskManager is identified by the Kibana UUID: a6e833b2-6718-4c64-8d94-13e603247158"}]
elasticsearch | [{"type": "server", "timestamp": "2023-07-31T08:07:43.357Z", "level": "WARN", "component": "o.s.b.BootstrapChecks", "cluster.name": "docker-cluster", "node.name": "a6505677429a", "message": "max virtual memory area vm.max_map_count [65536] is too low, increase to at least [262144]"}]
elasticsearch | [{"type": "server", "timestamp": "2023-07-31T08:07:43.640Z", "level": "INFO", "component": "o.s.c.c.Coordinator", "cluster.name": "docker-cluster", "node.name": "a6505677429a", "message": "setting initial configuration to VotingConfiguration{vhyxCe2Thy9tFltLORfww}"}]
kibana | [{"type": "log", "@timestamp": "2023-07-31T08:07:43+00:00", "tags": ["warning", "plugins", "security", "config"], "pid": 7, "message": "Generating a random key for xpack.security.encryptionKey. To prevent sessions from being invalidated on restart, please set xpack.security.encryptionKey in the kibana.yml or use the bin/kibana-encryption-keys command."}]
kibana | [{"type": "log", "@timestamp": "2023-07-31T08:07:43+00:00", "tags": ["warning", "plugins", "security", "config"], "pid": 7, "message": "Session cookies will be transmitted over insecure connections. This is not recommended."}]
kibana | [{"type": "log", "@timestamp": "2023-07-31T08:07:44+00:00", "tags": ["warning", "plugins", "security", "config"], "pid": 7, "message": "Generating a random key for xpack.security.encryptionKey. To prevent sessions from being invalidated on restart, please set xpack.security.encryptionKey in the kibana.yml or use the bin/kibana-encryption-keys command."}]

```

localhost:9200 x WhatsApp x Dashboard x

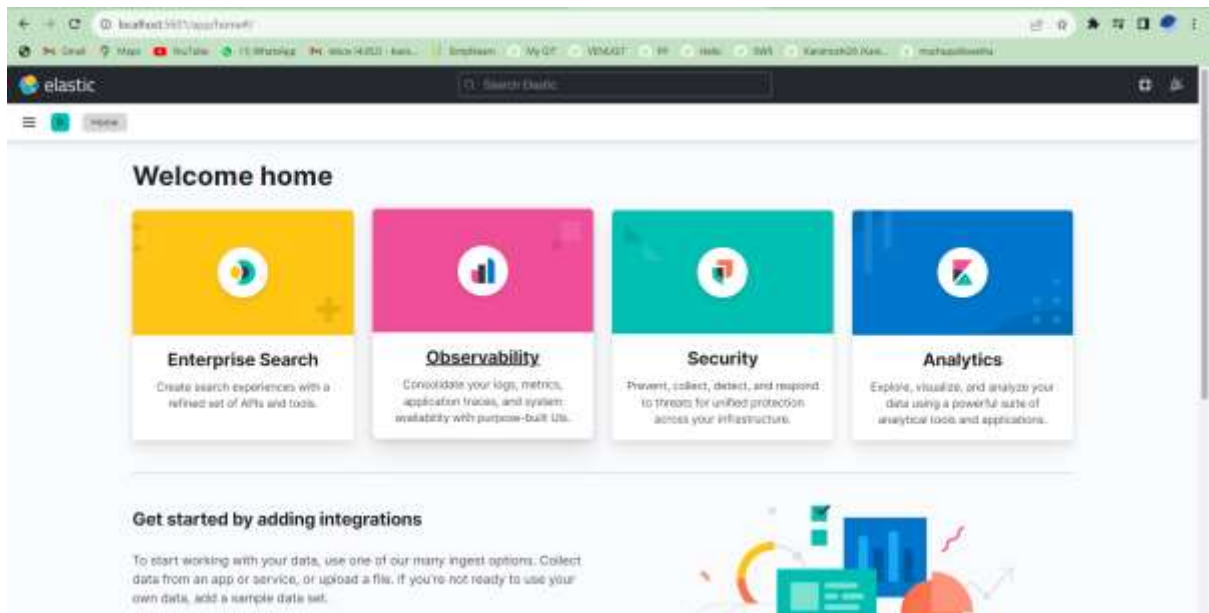
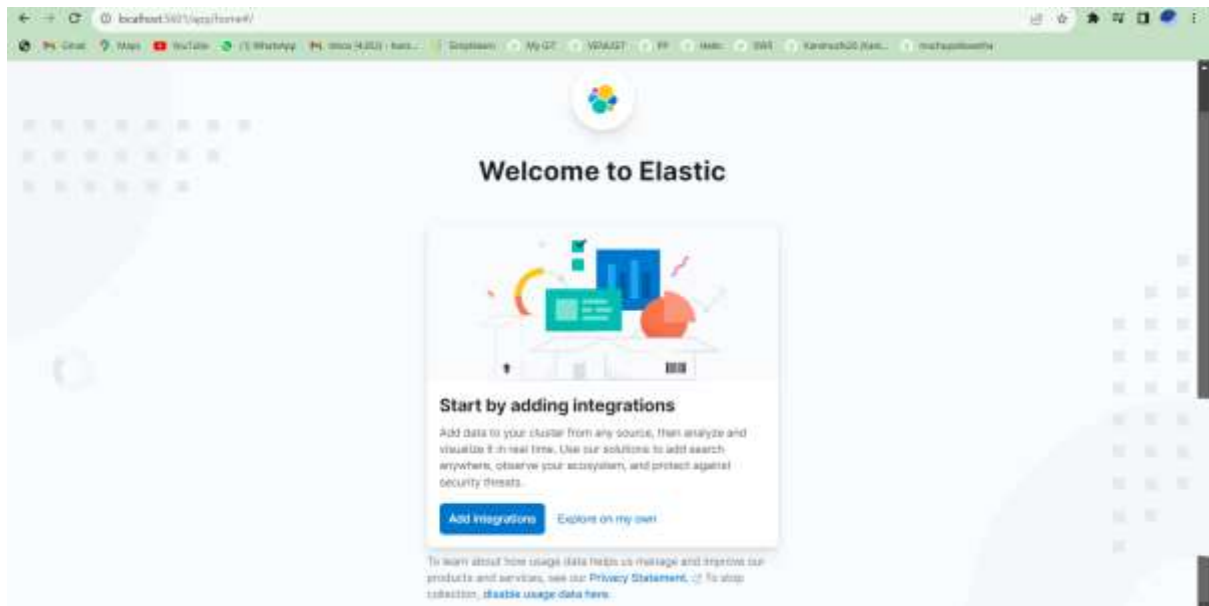
localhost:9200

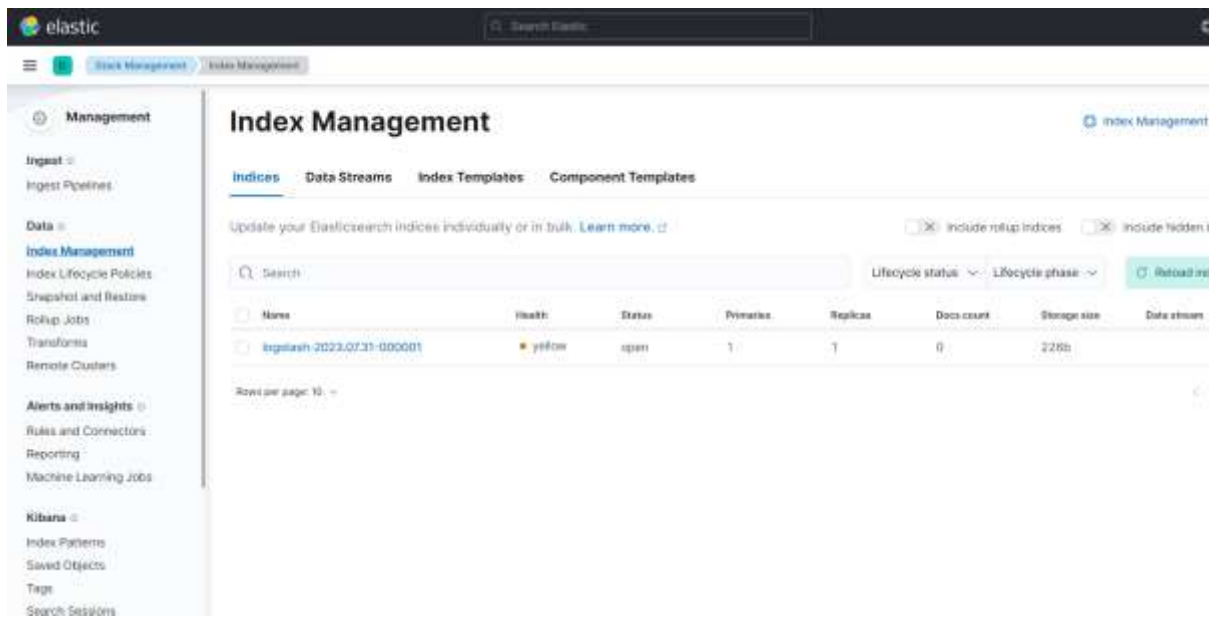
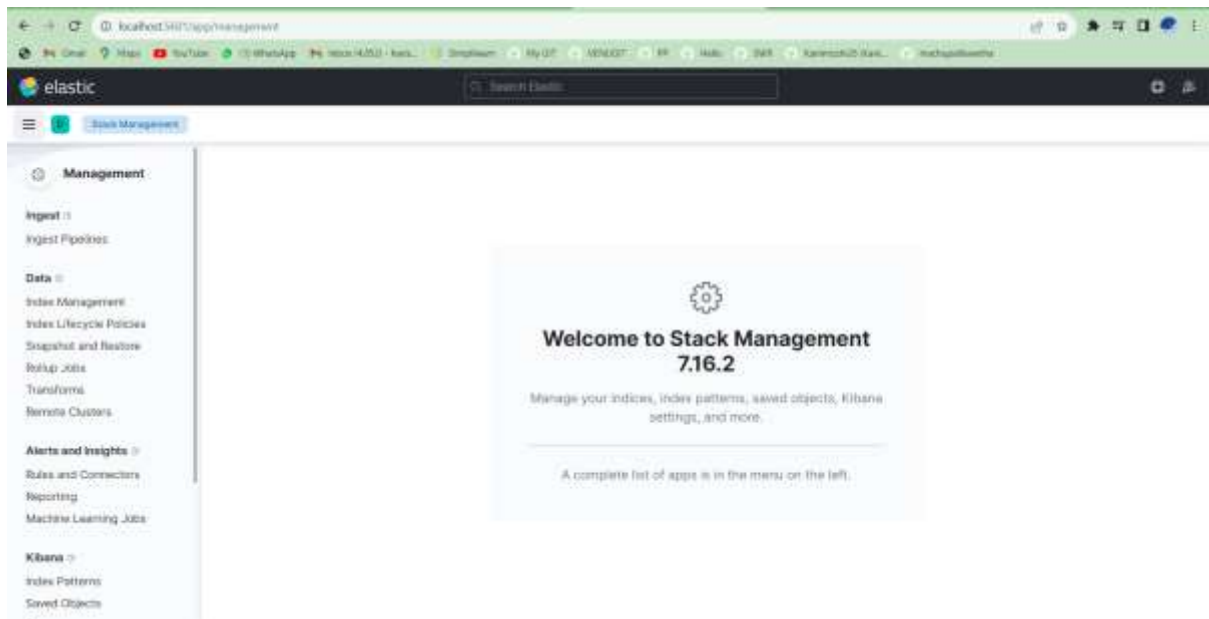
Gmail Maps YouTube (1) WhatsApp Inbox (4,852) - haris... Simplilearn My GIT

```

{
  "name": "a6505677429a",
  "cluster_name": "docker-cluster",
  "cluster_uuid": "hcjQtLWgRYS3GoeUq-vbQg",
  "version": {
    "number": "7.16.2",
    "build_flavor": "default",
    "build_type": "docker",
    "build_hash": "2b937c44140b6559905130a8650c64dbd0879cfb",
    "build_date": "2021-12-18T19:42:46.604893745Z",
    "build_snapshot": false,
    "lucene_version": "8.10.1",
    "minimum_wire_compatibility_version": "6.8.0",
    "minimum_index_compatibility_version": "6.0.0-beta1"
  },
  "tagline": "You Know, for Search"
}

```







elastic

Search Elastic

Stack Management

Index Management

Management

Ingest

Ingest Pipelines

Data

Index Management

Index Lifecycle Policies

Snapshots and Restore

Rollup Jobs

Transforms

Remote Clusters

Alerts and Insights

Rules and Connectors

Reporting

Machine Learning Jobs

Kibana

Index Patterns

Saved Objects

Tags

Search Settings

Index Management

Indices

Data Streams

Index Templates

Component Templates

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

Search

Index

Health

Size

logstash-2023.07.31-000001

yellow

10 GB

Rows per page: 10

logstash-2023.07.31-000001

Summary

Settings

Mappings

Stats

Edit settings

General

Health

Primarys

Docs Count

Storage Size

Aliases

Status

Replicas

Docs Deleted

Primary Storage Size

logstash

Index lifecycle management

Lifecycle policy

Current phase

Current action

Failed step

logstash-policy

not

rollover

Current phase time

Phase definition

2023-07-31 11:34

[Show definition](#)

Manage