Deploying ELK Stack on Docker Container

Source Code :

logstash.conf :-

```
Input {
        File {
                Path  => “/root/temp/inlog.log”
        }
}
Output {
        Elasticsearch {
                Hosts => [“ http://elasticsearch:9200 ”]
        }
}
```

docker-componse.yml :-

```
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: "-Xmx256m -Xms256m"
   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:
- '9600:9600'  environment:

   LS_JAVA_OPTS: "-Xmx256m -Xms256m"
 networks:
```

```
    - elk


  Kibana:
    image: kibana:7.16.2
    container_name: kibana
    restart: always  ports:
    - '5601:5601'  environment:
    - ELASTICSEARCH_URL=http://elasticsearch:9
      200  depends_on:
    - Elasticsearch  networks:
    - elk
 volumes:
  elastic_data: {}


 networks:
   elk:
```

inlog.log :-

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

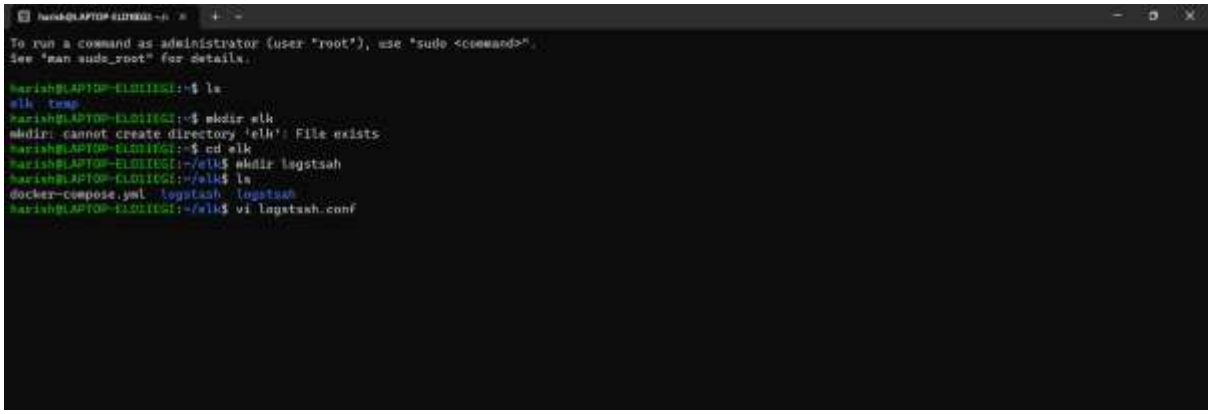
firewall :- sudo firewall-cmd --add-port=9200/tcp

--permanent sudo firewall-cmd --add-port=5601/tcp

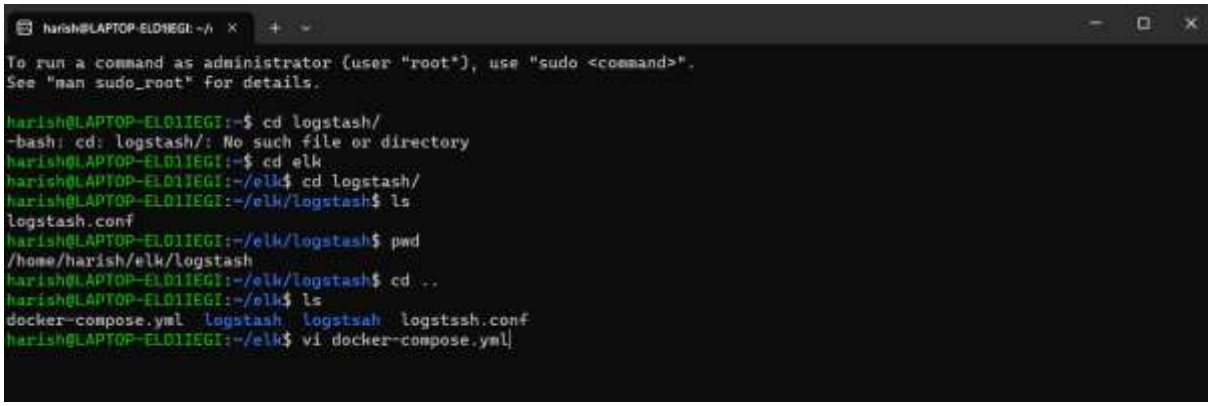
--permanent sudo firewall-cmd --add-port=9600/tcp

--permanent sudo firewall-cmd --add-port=9300/tcp

--permanent sudo firewall-cmd --reload

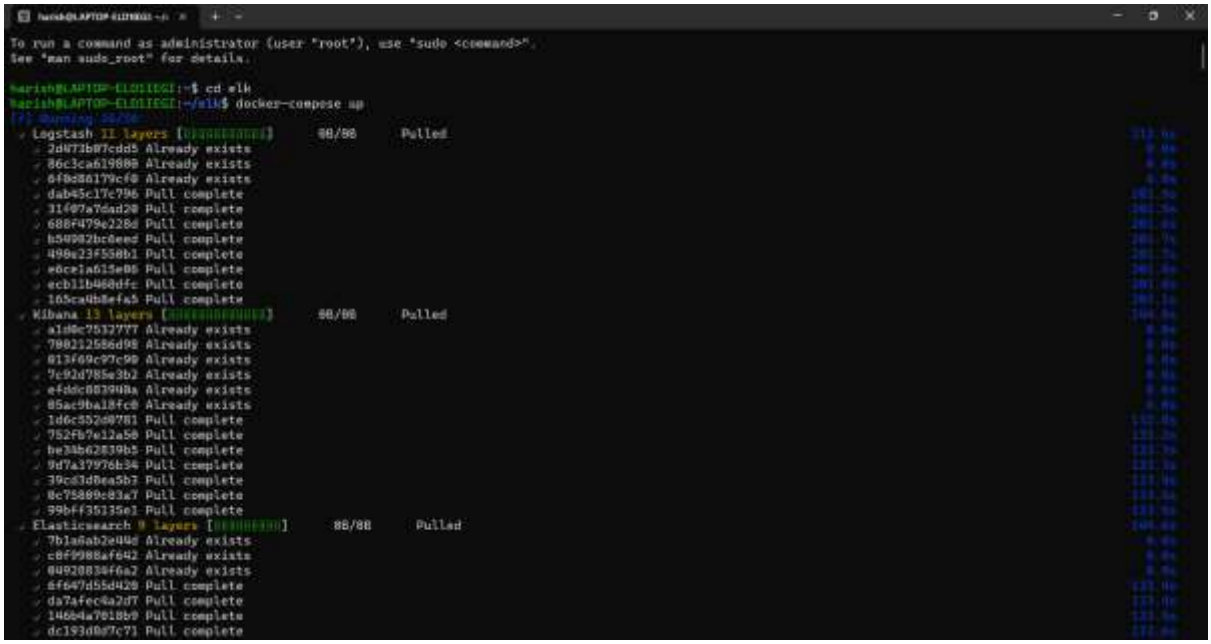

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
harish@LAPTOP-ELO1IEGI:~$ ls
elk temp
harish@LAPTOP-ELO1IEGI:~$ mkdir elk
mkdir: cannot create directory 'elk': File exists
harish@LAPTOP-ELO1IEGI:~$ cd elk
harish@LAPTOP-ELO1IEGI:~/elk$ mkdir logstsah
harish@LAPTOP-ELO1IEGI:~/elk$ ls
docker-compose.yml logstash logstsah
harish@LAPTOP-ELO1IEGI:~/elk$ vi logstssh.conf

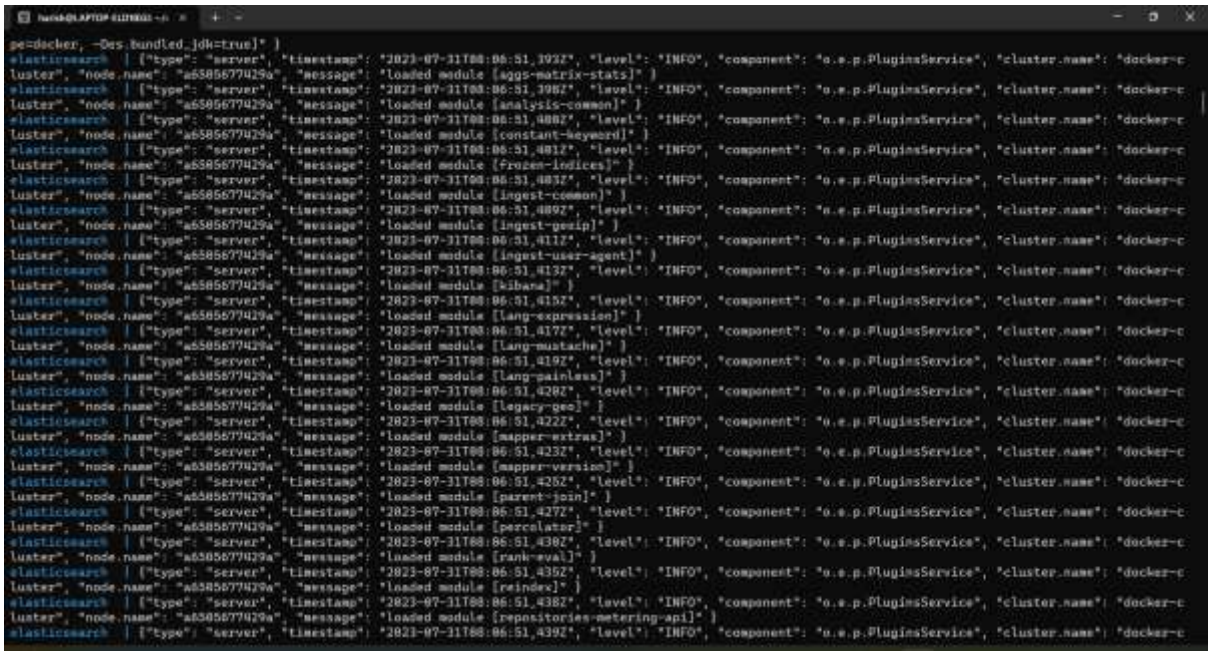

input {
file {
path => "/root/temp/inlog.log"
}
}
ouput
elasticsearch {
hosts => ["http://elasticsearch:9200"]
}


harish@LAPTOP-ELO1IEGI: ~/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
harish@LAPTOP-ELO1IEGI:~$ cd logstash/
-bash: cd: logstash/: No such file or directory
harish@LAPTOP-ELO1IEGI:~$ cd elk
harish@LAPTOP-ELO1IEGI:~/elk$ cd logstash/
harish@LAPTOP-ELO1IEGI:~/elk/logstash$ ls
logstash.conf
harish@LAPTOP-ELO1IEGI:~/elk/logstash$ pwd
/home/harish/elk/logstash
harish@LAPTOP-ELO1IEGI:~/elk/logstash$ cd ..
harish@LAPTOP-ELO1IEGI:~/elk$ ls
docker-compose.yml logstash logstsah logstssh.conf
harish@LAPTOP-ELO1IEGI:~/elk$ vi docker-compose.yml

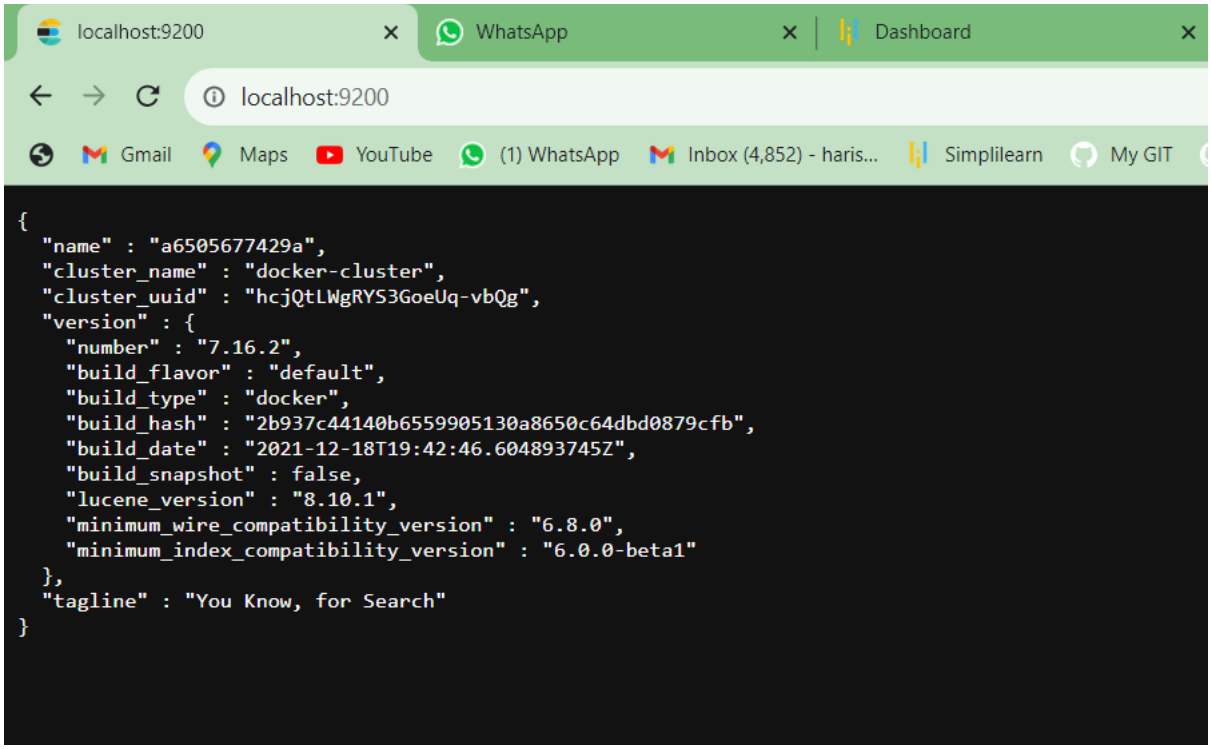
```
This is a test file
this is a second line
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq!
```

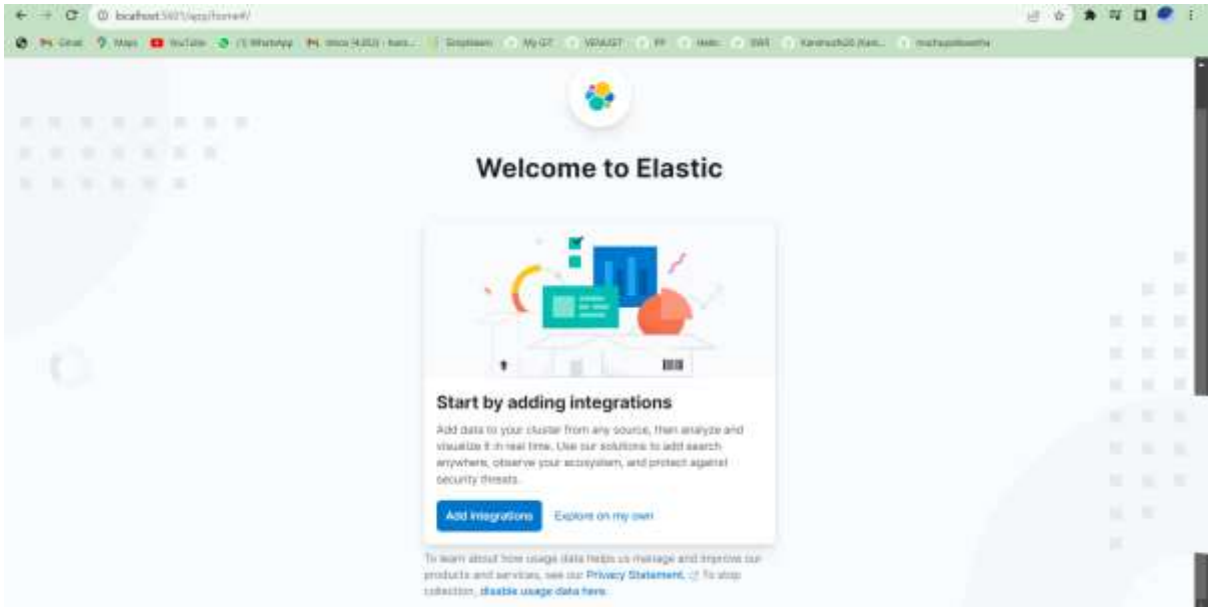
```
version: '3.6'
services:
  Elasticsearch:
    image: elasticsearch:7.16.2
    container_name: elasticsearch
    restart: always
    volumes:
    - elastic_data:/usr/share/elasticsearch/data/
    environment:
      ES_JAVA_OPTS: "-Xms256m -Xmx256m"
      discovery.type: single-node
    ports:
    - '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:
    - '9600:9600'
    environment:
      LS_JAVA_OPTS: "-Xms256m -Xmx256m"
    networks:
      - elk
:wq!
```

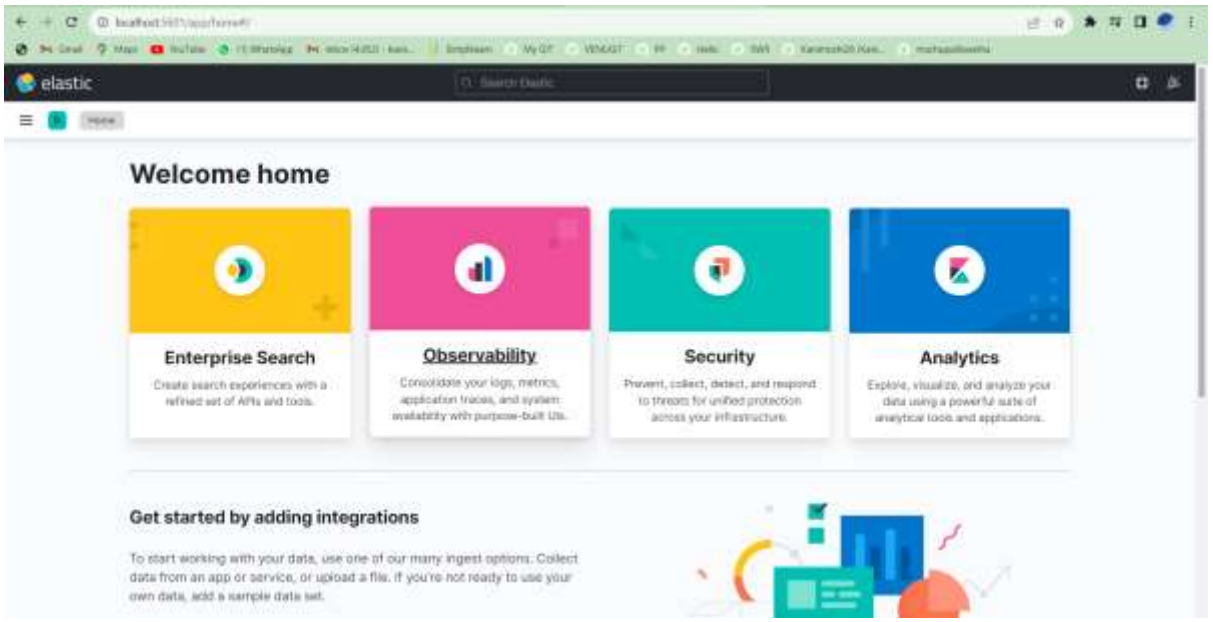

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
harish@LAPTOP-ELDJIEGI:~$ cd elk
harish@LAPTOP-ELDJIEGI:~/elk$ docker-compose up
[+] Running 28/28
✔ Logstash 11 layers [⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿] 88/88 Pulled
✔ Kibana 13 layers [⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿⣿] 88/88 Pulled
✔ Elasticsearch 9 layers [⣿⣿⣿⣿⣿⣿⣿⣿⣿] 88/88 Pulled

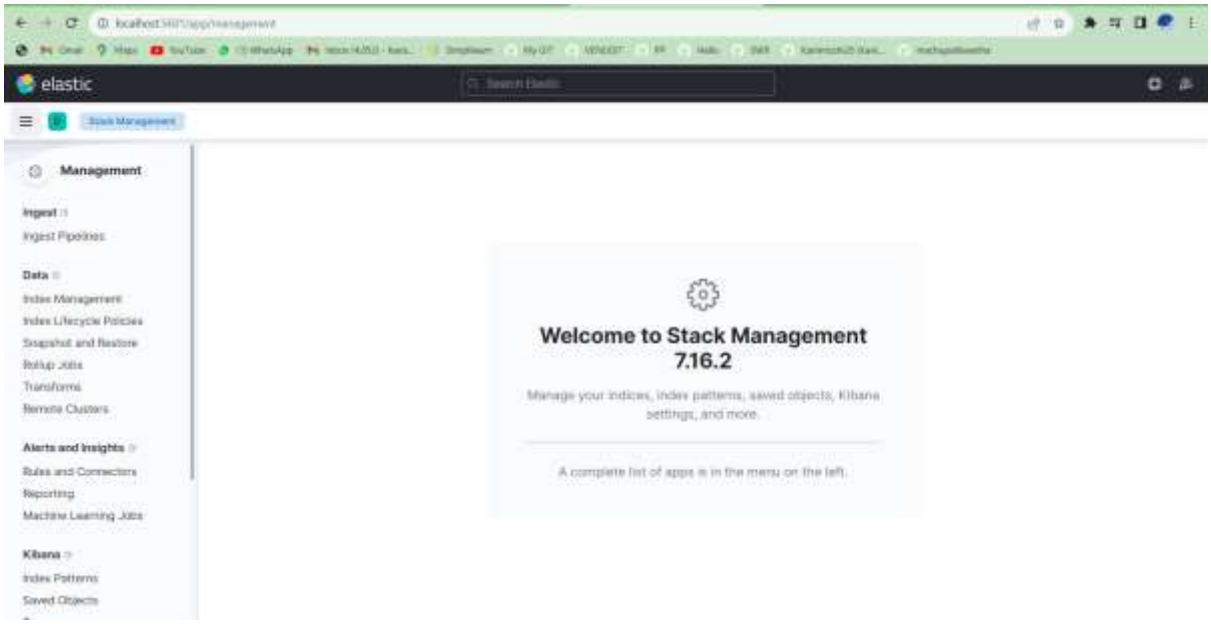

pe=docker, -Des.bundled_jdk=true]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,393Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [aggs-matrix-stats]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,398Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [analysis-common]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,408Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [constant-keyword]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,481Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [frozen-indices]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,483Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [ingest-common]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,489Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [ingest-geoip]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,411Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [ingest-user-agent]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,413Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [kibana]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,415Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [lang-expression]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,417Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [lang-mustache]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,419Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [lang-painless]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,420Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [legacy-geo]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,422Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [mapper-extras]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,423Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [mapper-version]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,425Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [parent-join]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,427Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [percolator]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,430Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [rank-eval]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,435Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [reindex]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,438Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c
luster", "node.name": "a6585677429a", "message": "loaded module [repositories-metering-api]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:06:51,439Z", "level": "INFO", "component": "o.e.p.PluginsService", "cluster.name": "docker-c

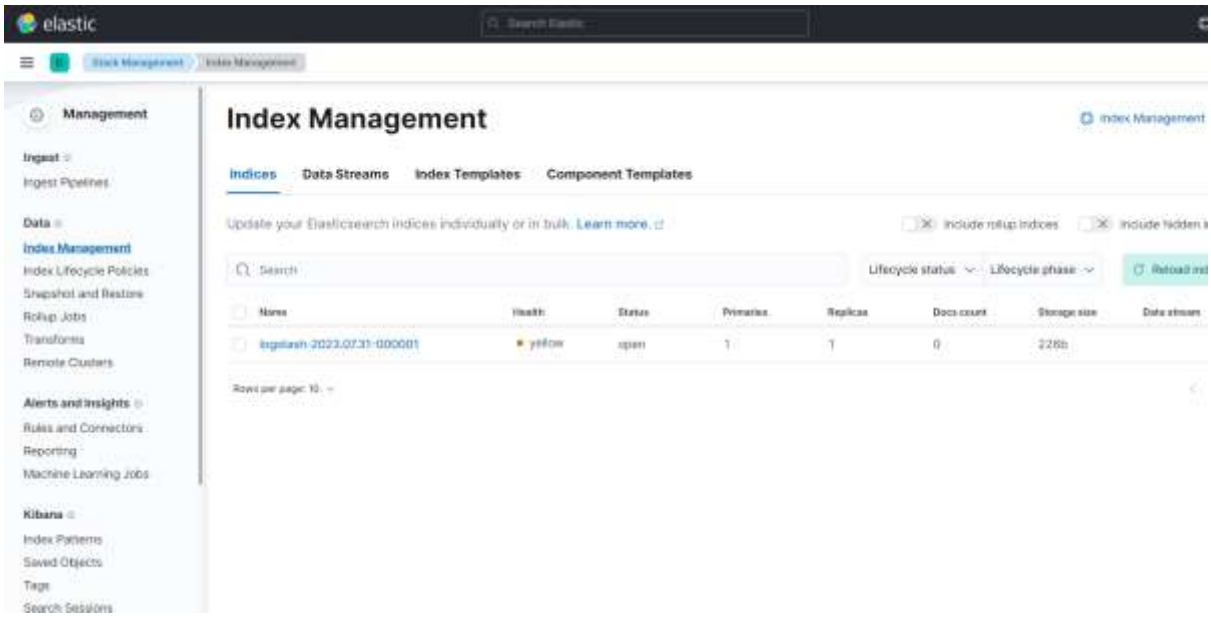

kibana | {"type":"log","@timestamp":"2023-07-31T08:07:41+00:00","tags":["info","http","server","Preboot"],"pid":7,"message":"http server running at http://0.0.0.0:5601"}
kibana | {"type":"log","@timestamp":"2023-07-31T08:07:41+00:00","tags":["warning","config","deprecation"],"pid":7,"message":"Starting 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 JSON logs will be ECS-compatible JSON, 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": "2023-07-31T08:07:42.387Z", "level": "INFO", "component": "o.e.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,xpackLegacy,taskManager,telemetryCollectionManager,telemetryCollectionXpack,kibanaUsageCollection,share,embeddable,uiActionsEnhanced,screenshotMode,banners,telemetry,newsfeed,mapsEms,mapsLegacy,kibanaLegacy,fieldFormats,expressions,dataViews,charts,esUiShared,bfetch,data,savedObjects,presentationUtil,expressionShape,expressionRevealImage,expressionRepeatImage,expressionMetric,expressionImage,customIntegrations,home,searchprofiler,painlessLab,grokdebugger,management,watcher,licenseManagement,advancedSettings,spaces,security,savedObjectsTagging,reporting,canvas,lists,ingestPipelines,fileUpload,encryptedSavedObjects,dataEnhanced,cloud,snapshotRestore,eventLog,actions,alerting,triggersActionsUi,transform,stackAlerts,ruleRegistry,visualizations,visTypeXy,visTypeVislib,visTypeVega,visTypeTimelion,visTypeTagcloud,visTypeTable,visTypePie,visTypeMetric,visTypeMarkdown,tileMap,regionMap,expressionTagcloud,expressionMetricVis,console,graph,fleet,indexManagement,remoteClusters,crossClusterReplication,indexLifecycleManagement,dashboard,maps,dashboardMode,dashboardEnhanced,visualize,visTypeTimeseries,rollup,indexPatternFieldEditor,lens,cases,timelines,discover,osquery,observability,discoverEnhanced,dataVisualizer,ml,uptime,securitySolution,infra,upgradeAssistant,monitoring,logstash,enterpriseSearch,apm,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: a6e833b2-6718-4c64-8d94-13e6083247158"}
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:07:43.557Z", "level": "WARN", "component": "o.e.b.BootstrapChecks", "cluster.name": "docker-cluster", "node.name": "a6505677429a", "message": "max virtual memory areas vm.max_map_count [65530] is too low, increase to at least [262144]" }
elasticsearch | {"type": "server", "timestamp": "2023-07-31T08:07:43.840Z", "level": "INFO", "component": "o.e.c.c.Coordinator", "cluster.name": "docker-cluster", "node.name": "a6505677429a", "message": "setting initial configuration to VotingConfiguration{vhyxCerzTHy9tFltLOHTmw}" }
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 ran

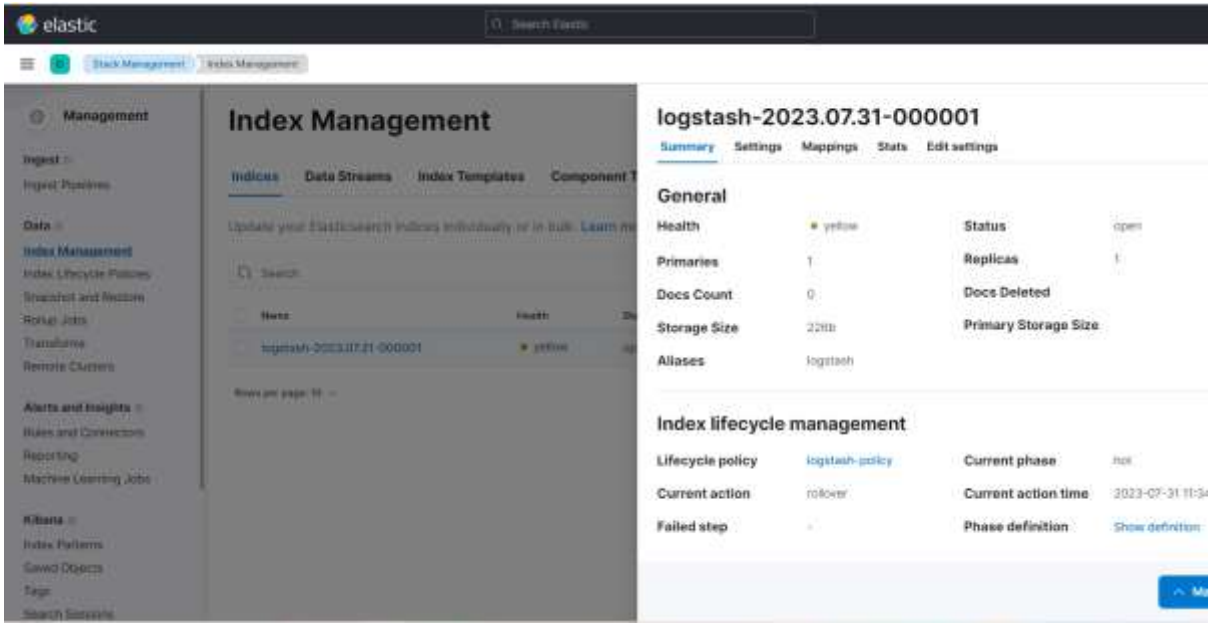

localhost:9200
WhatsApp
Dashboard
localhost:9200
Gmail
Maps
YouTube
(1) WhatsApp
Inbox (4,852) - haris...
Simplilearn
My GIT
{
"name" : "a6505677429a",
"cluster_name" : "docker-cluster",
"cluster_uuid" : "hcjQtLWgRYS3GoeUq-vbQg",
"version" : {
"number" : "7.16.2",
"build_flavor" : "default",
"build_type" : "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"
}


Welcome to Elastic
Start by adding integrations
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.
Add integrations
Explore on my own


elastic
Welcome home
Enterprise Search
Create search experiences with a refined set of APIs and tools.
Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.
Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.
Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.
Get started by adding integrations
To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, add a sample data set.


elastic
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
Welcome to Stack Management 7.16.2
Manage your indices, index patterns, saved objects, Kibana settings, and more.
A complete list of apps is in the menu on the left.


elastic
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
Index Management
Indices
Data Streams
Index Templates
Component Templates
Update your Elasticsearch indices individually or in bulk. Learn more.
Include rollup indices
Search
Lifecycle status
Lifecycle phase
Name
Health
Status
Primaries
Replicas
Docs count
Storage size
logstash-2023.07.31-000001
yellow
open
1
1
0
226b
Rows per page: 10


elastic
Management
Index Management
Indices
Data Streams
Index Templates
logstash-2023.07.31-000001
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
Current action
rollover
Current action time
Failed step
Phase definition
Show definition