Creating an Elastic Cluster

JANUARY 2024

Abdulfatah Abdillahi

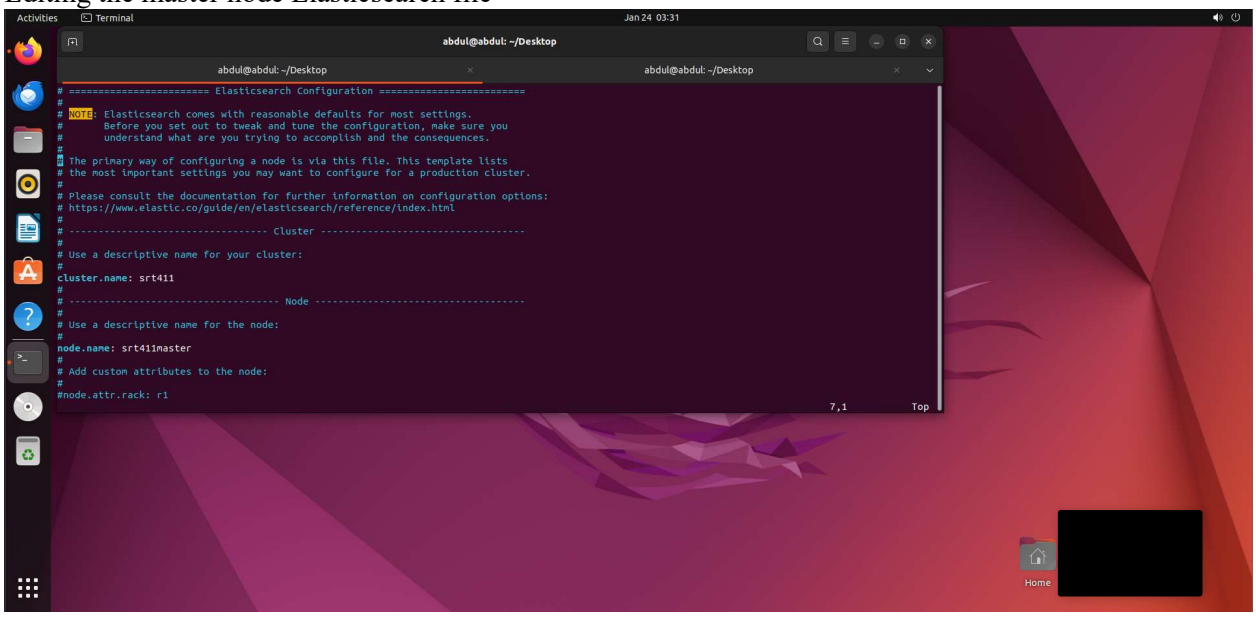
Contents

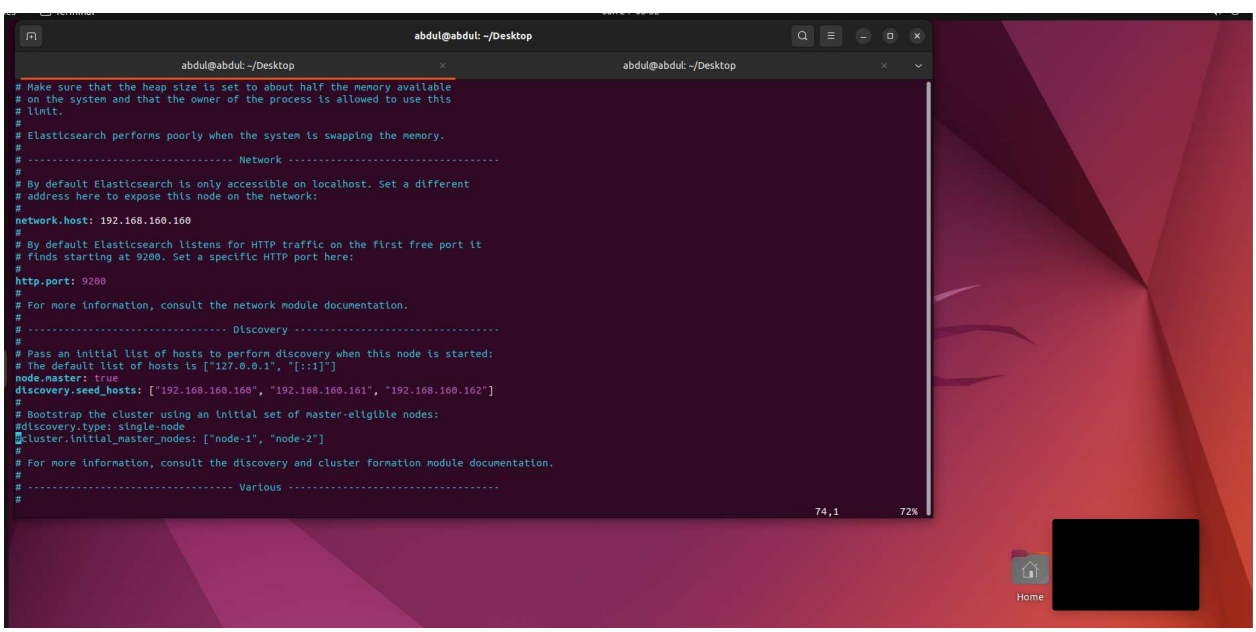
Introduction

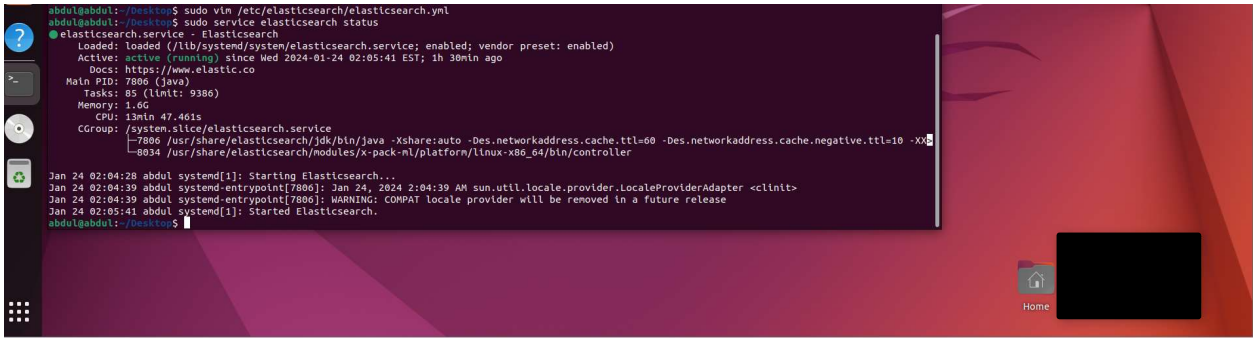
In this lab report, we outline the process of preparing your machine for data analytics by installing and configuring a Linux server with the ELK stack. Objectives include setting up Elasticsearch with Apache logs ingested via Filebeat and exploring data visualizations in Kibana. The report serves as a guide for understanding and implementing these crucial steps in establishing a functional data analytics environment.

Task 1: create and test the cluster.

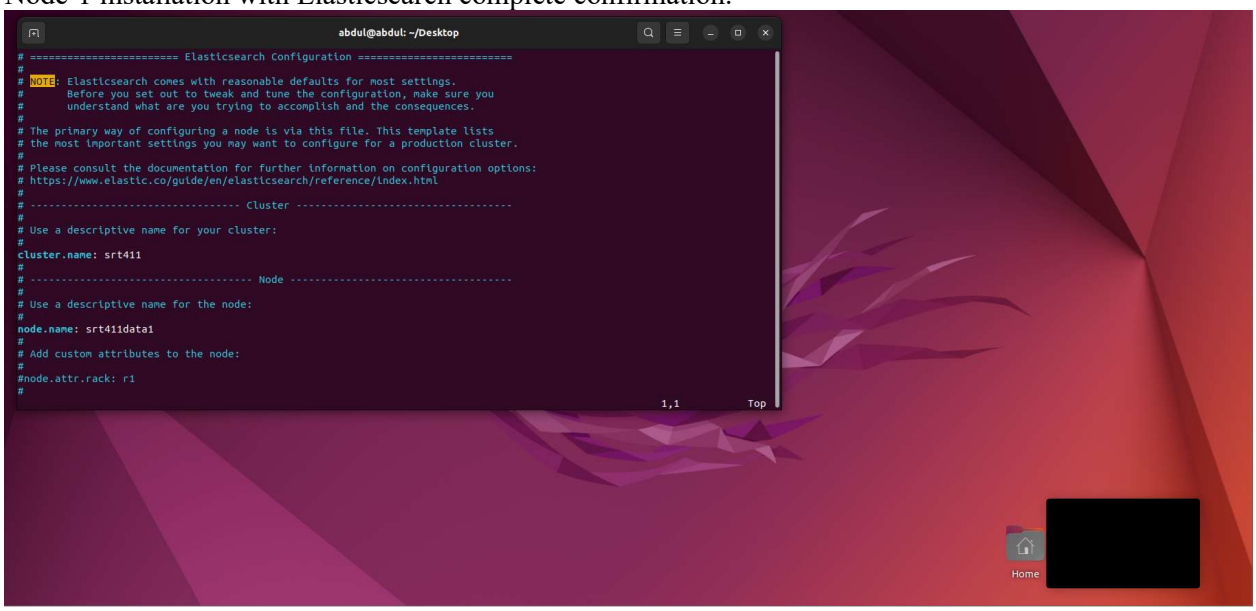
Editing the master node Elasticsearch file

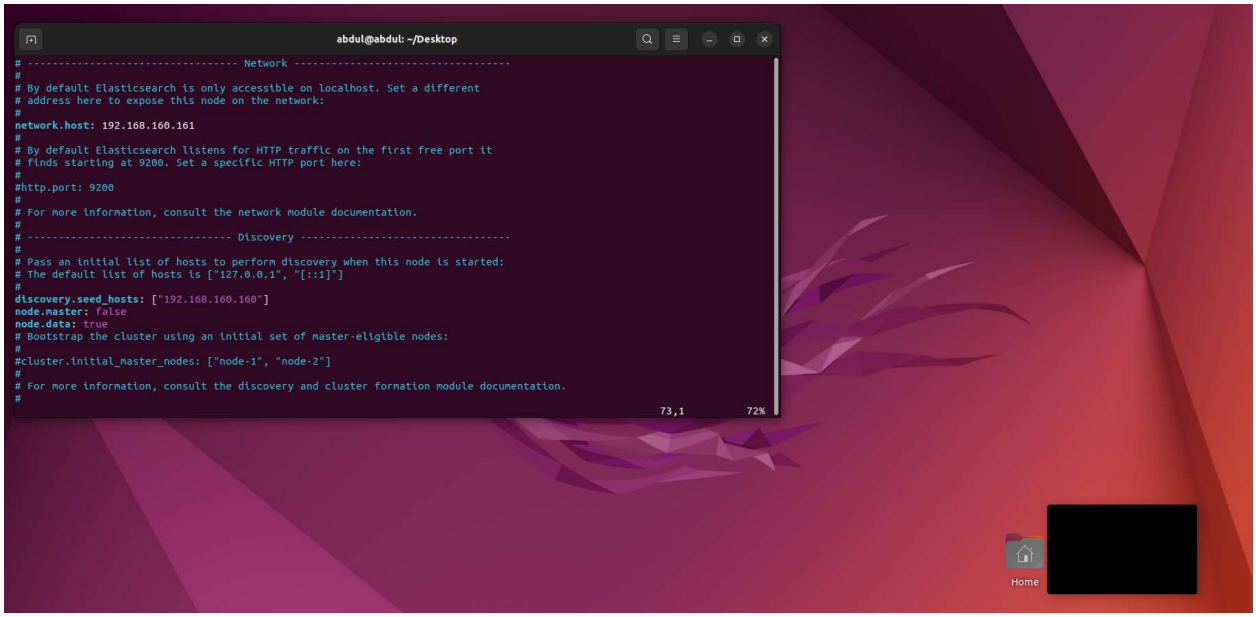


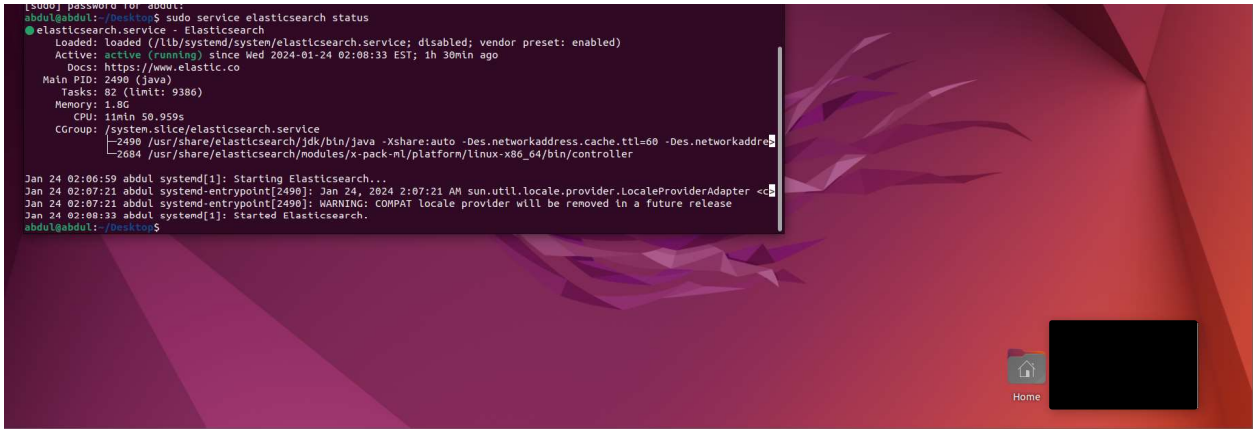




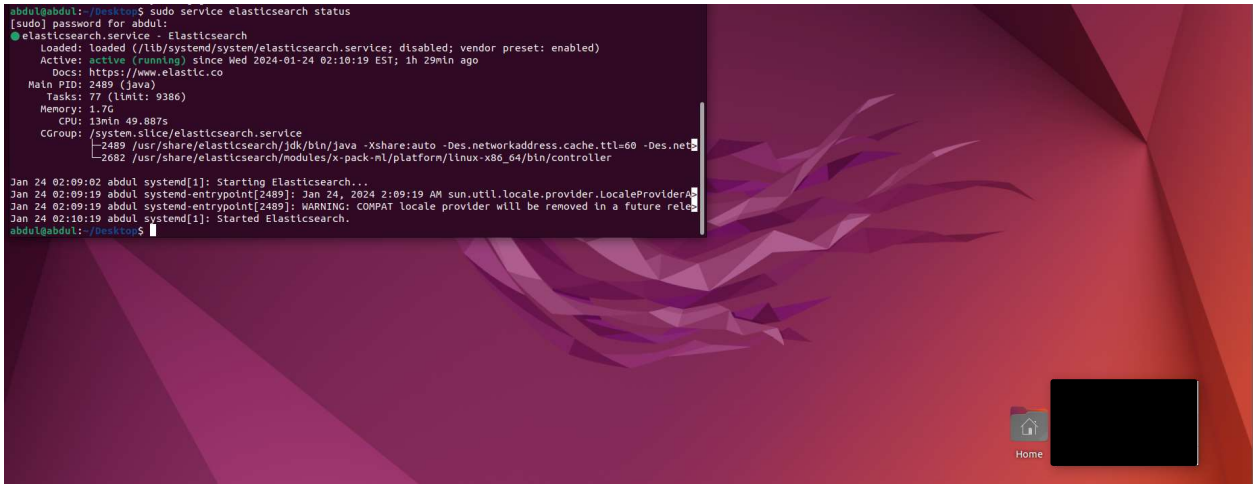
Node-1 installation with Elasticsearch complete confirmation.



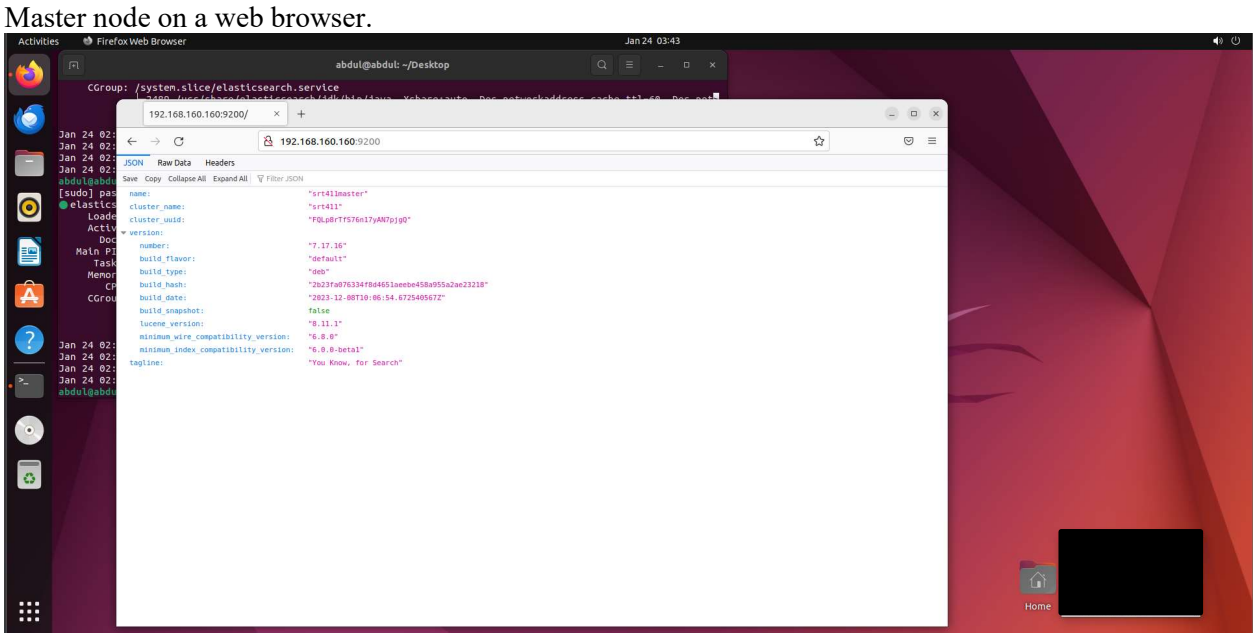




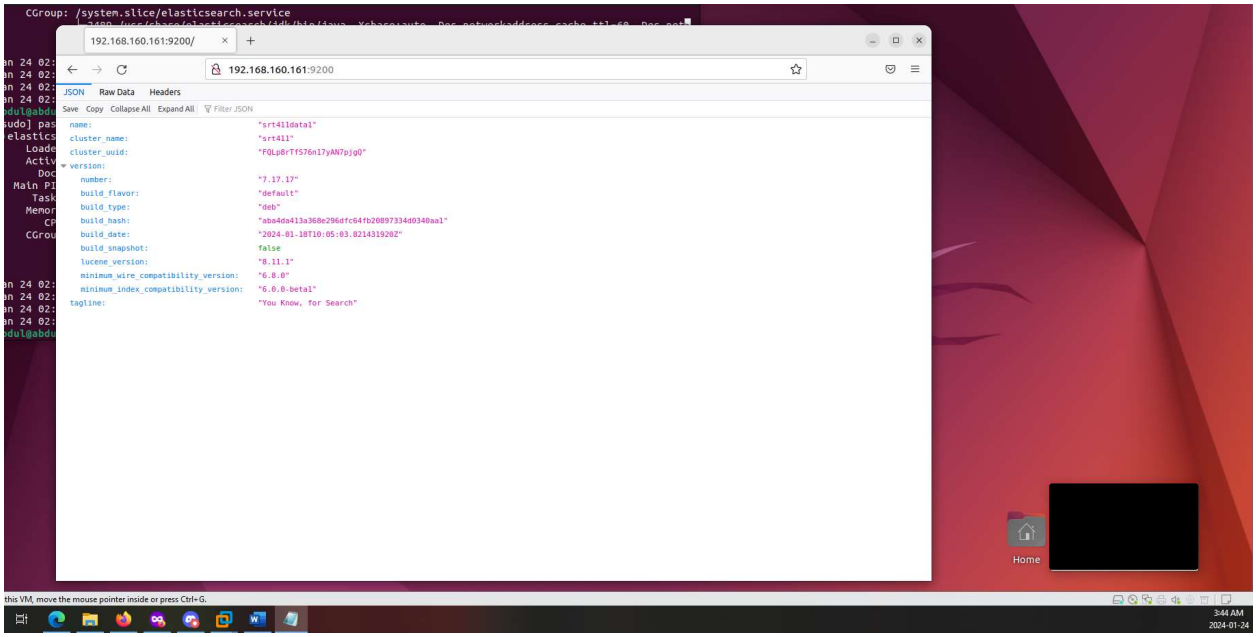
Node-2 installation with Elasticsearch confirmation



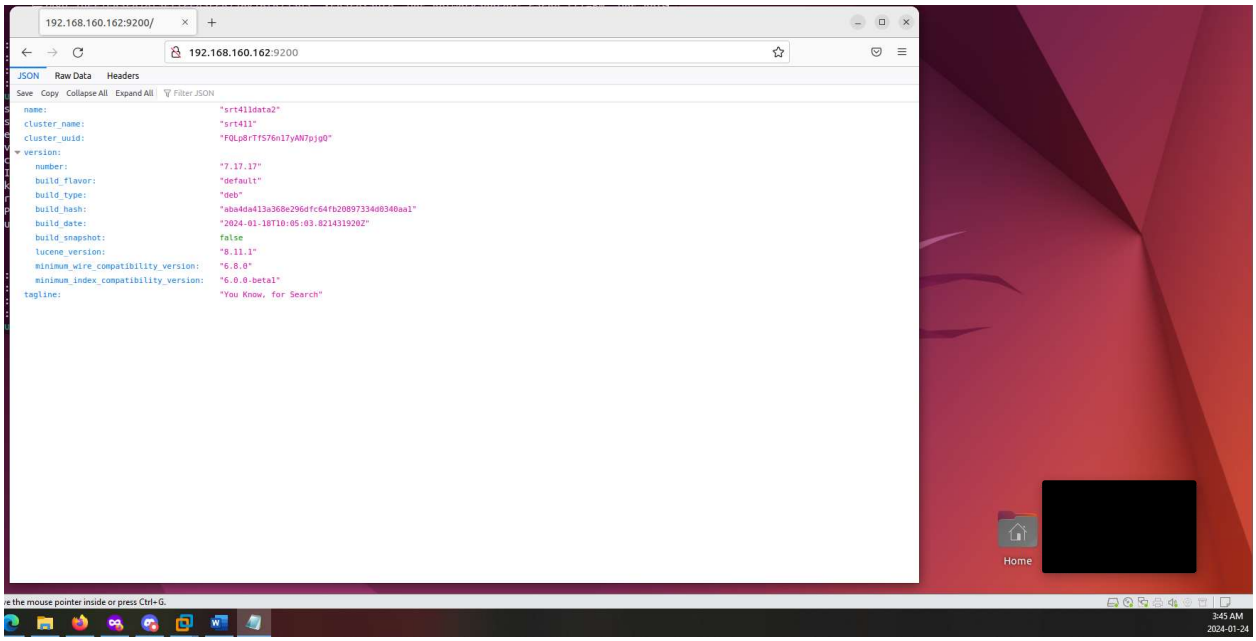
Master node on a web browser.



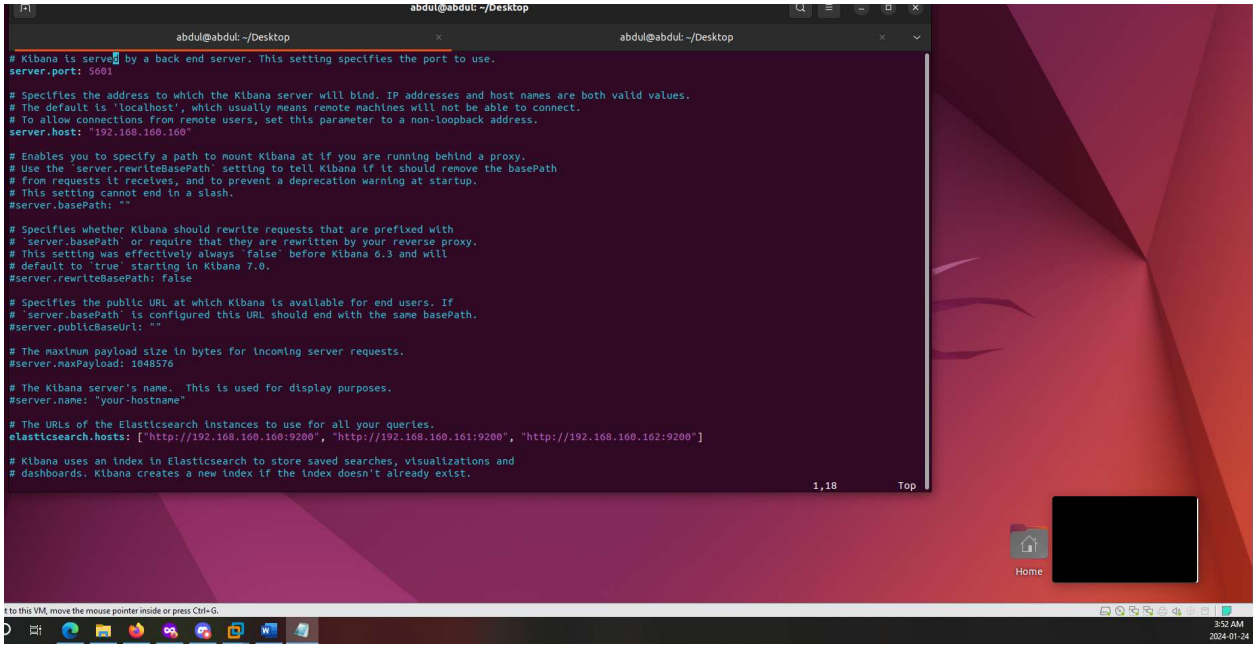
Node-1 status on web browser



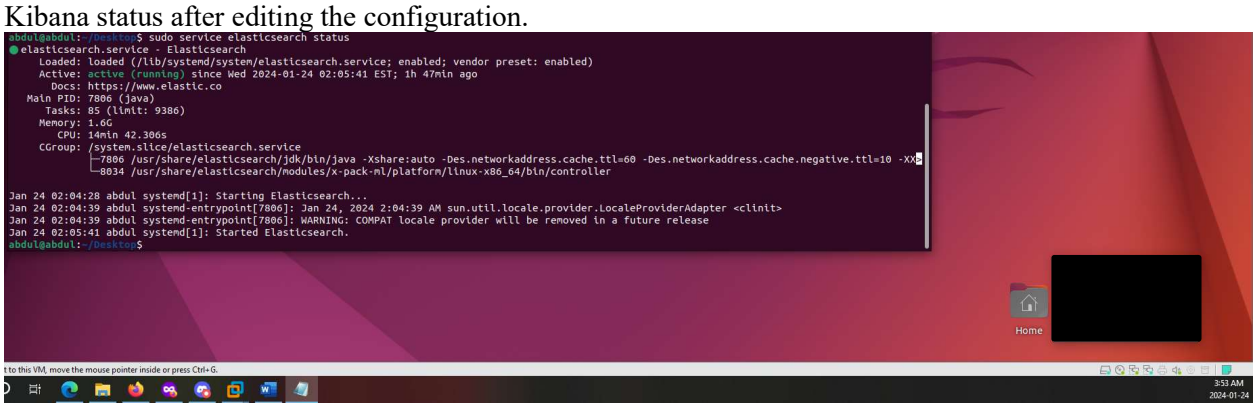
Node-2 status on web browser



Editing Kibana Configuration File

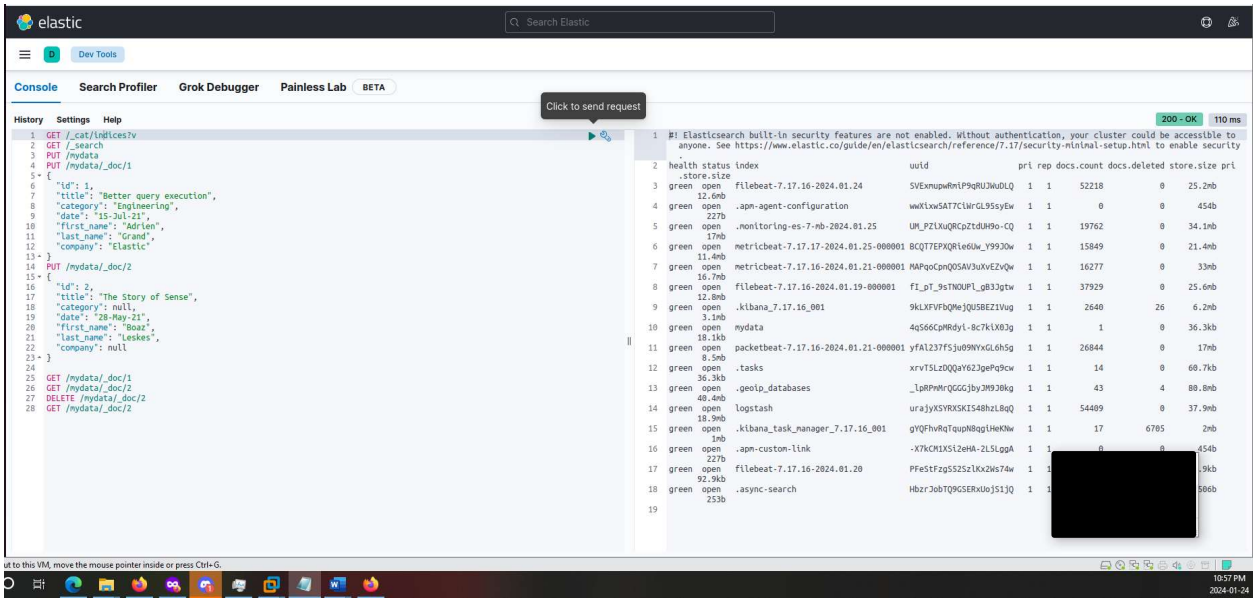


Kibana status after editing the configuration.

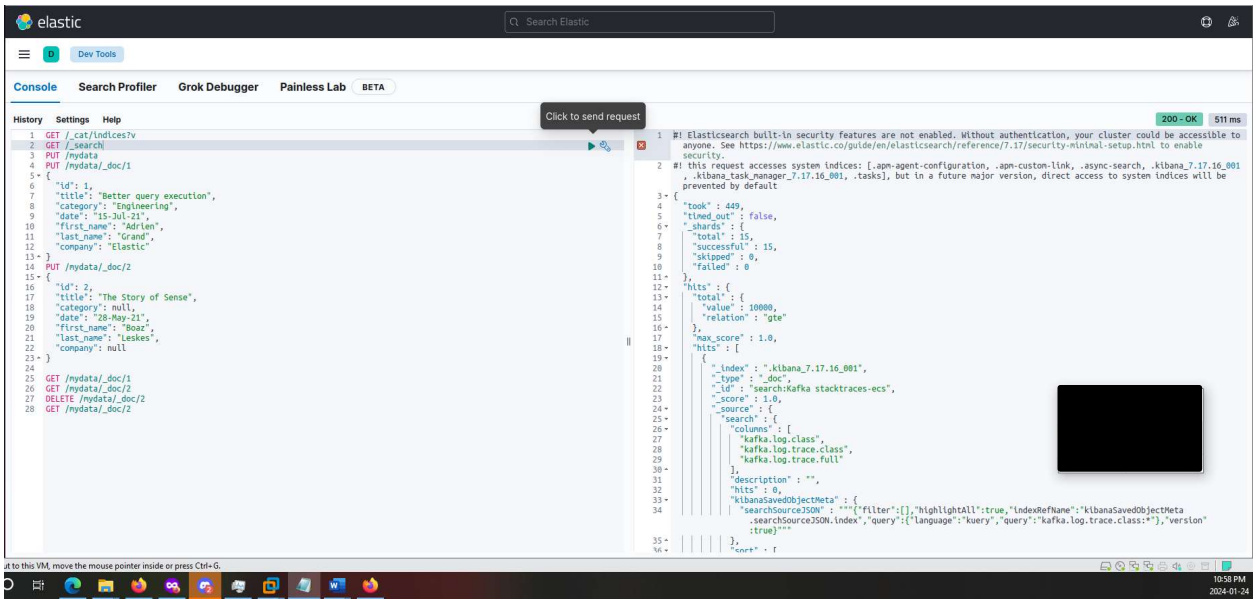


Task 2: Data Query

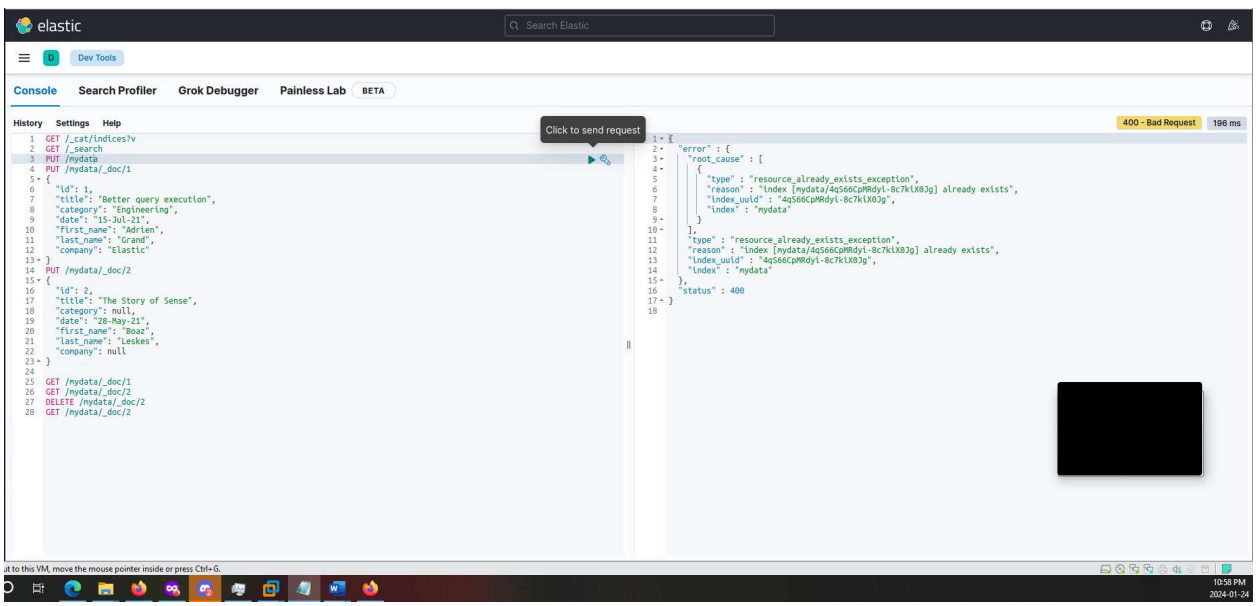
1. Write the command to query how many indices are there in the cluster and what are their names?



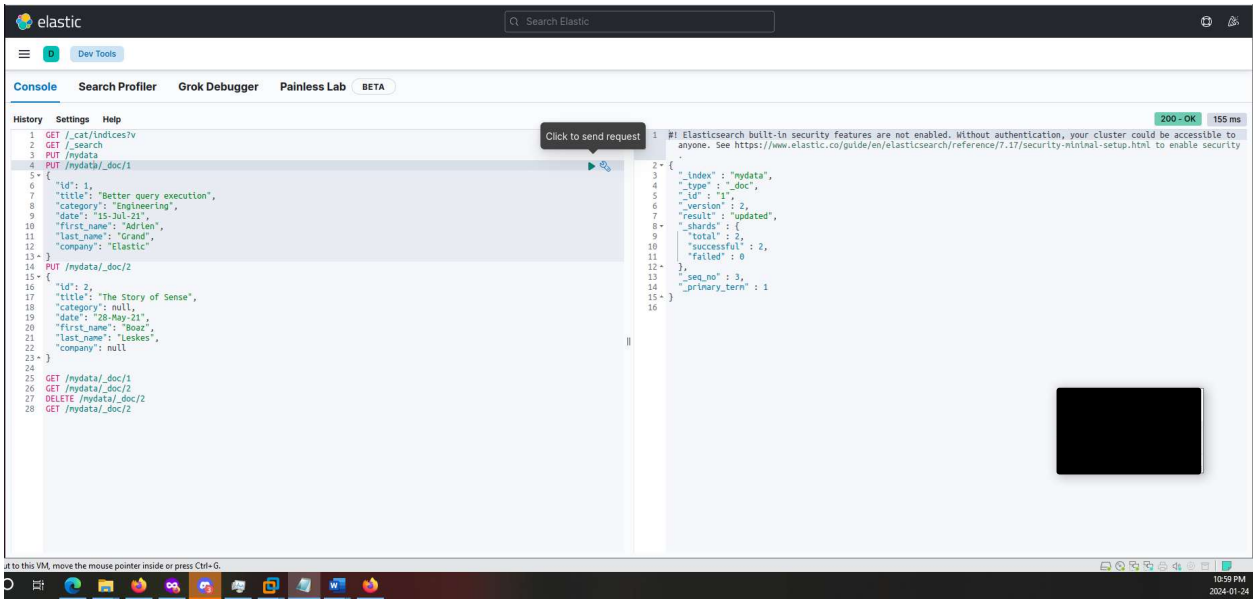
2. Write the command to query all documents in all indices of your cluster. By default, only the first 10 rows will be displayed.



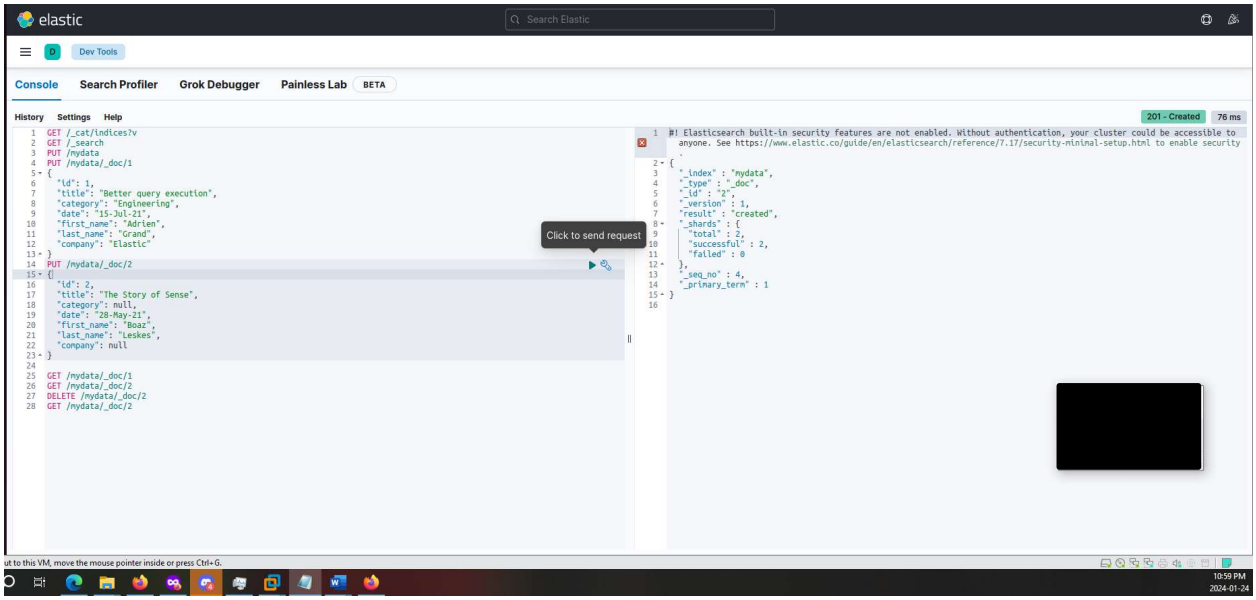
3. Write the command to create a new index named “mydata”.



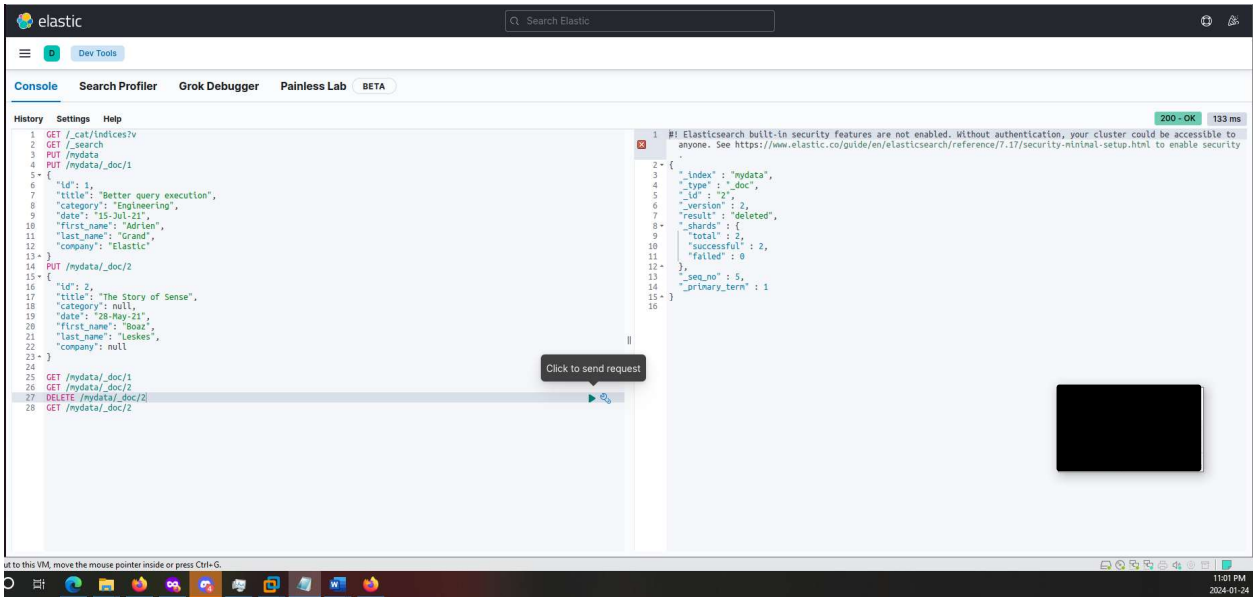
4. Write the command to add the following two documents in the index called “mydata” one by one. Use _doc for the type and their respective ids. You have to provide ids while putting the data in Elasticsearch. Look for PUT and POST commands and should be able to identify the difference and pick the right command for this step.



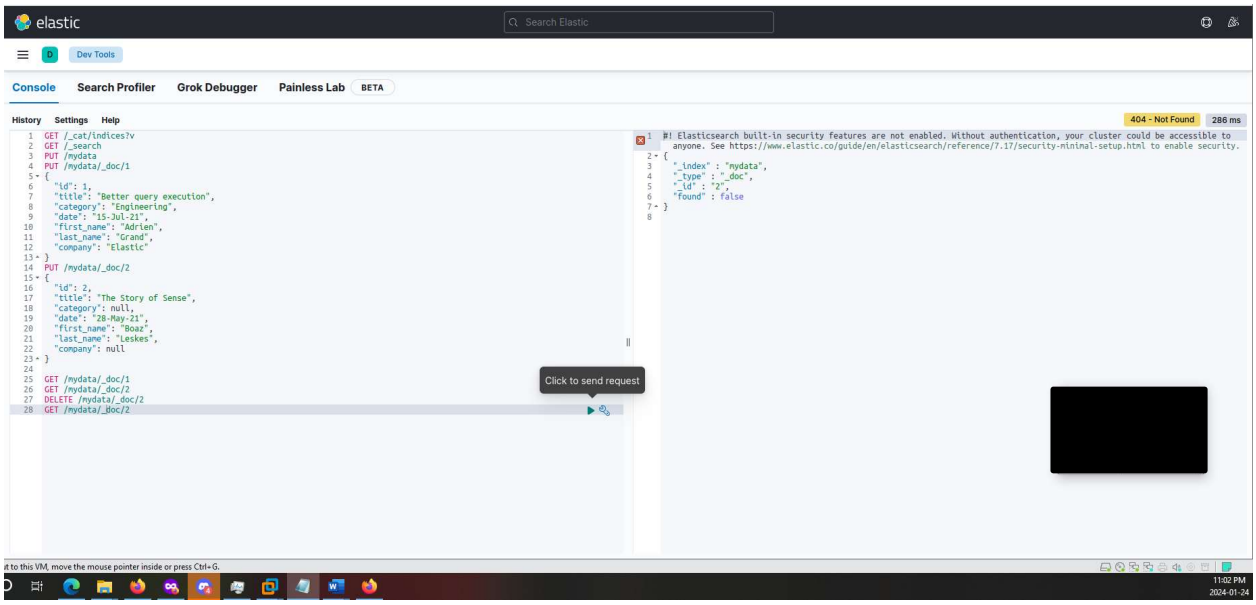
5. Write the GET command to retrieve the document with id of 1 and type _doc from the “myData” index.



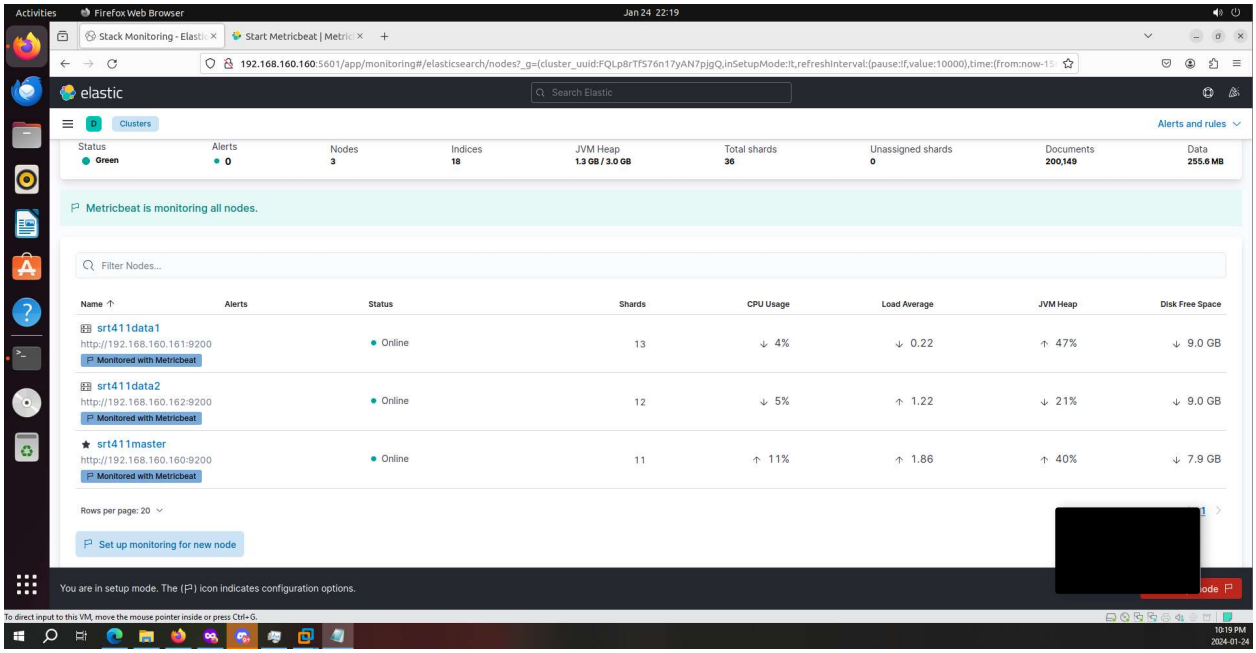
6. Write the command to delete the document with id 2 from the “myData” index

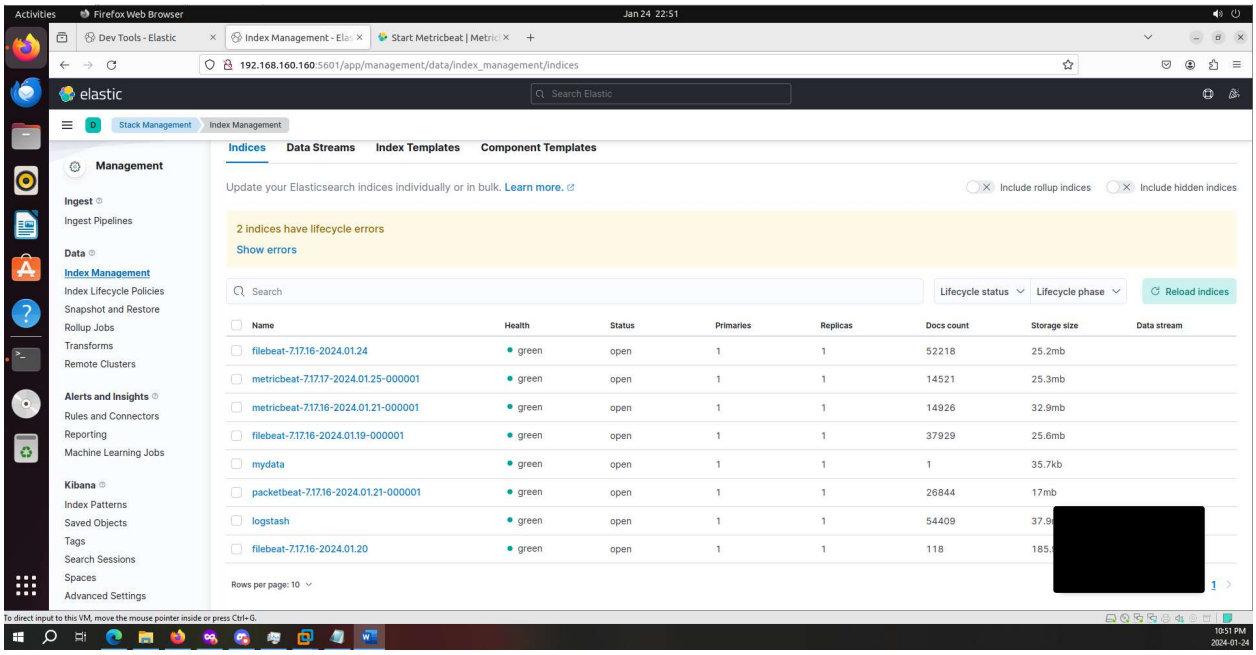


7. Verify it was deleted by trying to GET it again, record the response.



Task 3: Index Manager


Activities
Firefox Web Browser
Jan 24 22:19
Stack Monitoring - Elastic
Start Metricbeat | Metric
192.168.160.160:5601/app/monitoring#/elasticsearch/nodes?_g=(cluster_uuid:FQLp8rTfS76n17yAN7pjgQ,inSetupMode:!t,refreshInterval:(pause:!f,value:10000),time:(from:now-15
elastic
Search Elastic
Clusters
Alerts and rules
Status Green
Alerts 0
Nodes 3
Indices 18
JVM Heap 1.3 GB / 3.0 GB
Total shards 36
Unassigned shards 0
Documents 200,149
Data 255.6 MB
Metricbeat is monitoring all nodes.
Filter Nodes...
Name
Alerts
Status
Shards
CPU Usage
Load Average
JVM Heap
Disk Free Space
srt411data1
http://192.168.160.161:9200
Monitored with Metricbeat
Online
13
4%
0.22
47%
9.0 GB
srt411data2
http://192.168.160.162:9200
Monitored with Metricbeat
Online
12
5%
1.22
21%
9.0 GB
srt411master
http://192.168.160.160:9200
Monitored with Metricbeat
Online
11
11%
1.86
40%
7.9 GB
Rows per page: 20
Set up monitoring for new node
You are in setup mode. The (⚐) icon indicates configuration options.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
10:19 PM
2024-01-24


Activities
Firefox Web Browser
Jan 24 22:51
Dev Tools - Elastic
Index Management - Elas
Start Metricbeat | Metric
192.168.160.160:5601/app/management/data/index_management/indices
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
Data Streams
Index Templates
Component Templates
Update your Elasticsearch indices individually or in bulk. Learn more.
Include rollup indices
Include hidden indices
2 indices have lifecycle errors
Show errors
Search
Lifecycle status
Lifecycle phase
Reload indices
Name
Health
Status
Primaries
Replicas
Docs count
Storage size
Data stream
filebeat-7.17.16-2024.01.24 green open 1 1 52218 25.2mb
metricbeat-7.17.17-2024.01.25-000001 green open 1 1 14521 25.3mb
metricbeat-7.17.16-2024.01.21-000001 green open 1 1 14926 32.9mb
filebeat-7.17.16-2024.01.19-000001 green open 1 1 37929 25.6mb
mydata green open 1 1 1 35.7kb
packetbeat-7.17.16-2024.01.21-000001 green open 1 1 26844 17mb
logstash green open 1 1 54409
filebeat-7.17.16-2024.01.20 green open 1 1 118
Rows per page: 10
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
10:51 PM
2024-01-24