

Lesson 05 Demo 01

Setting up and Configuring Elasticsearch for Log Storage

Objective: To implement Elasticsearch as a monitoring tool for storing application logs, enhancing log management, and improving observability with real-time performance insights

Tools required: Elasticsearch

Prerequisites: None

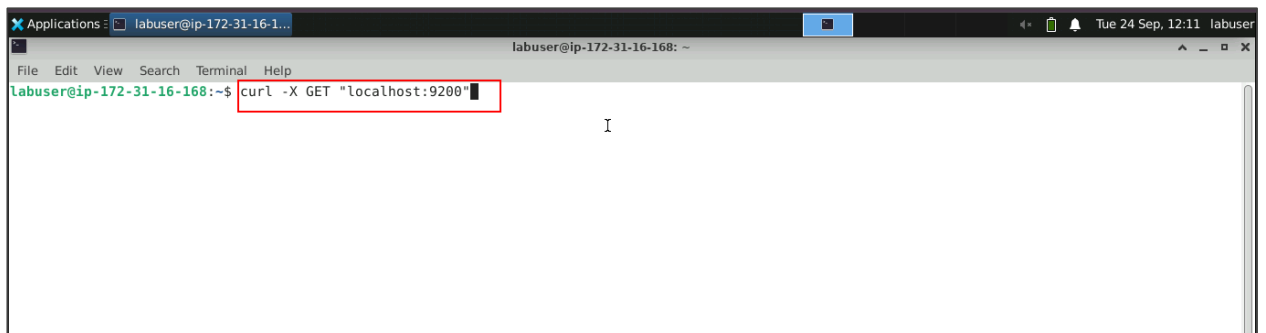
Steps to be followed:

1. Configure Elasticsearch for log storage

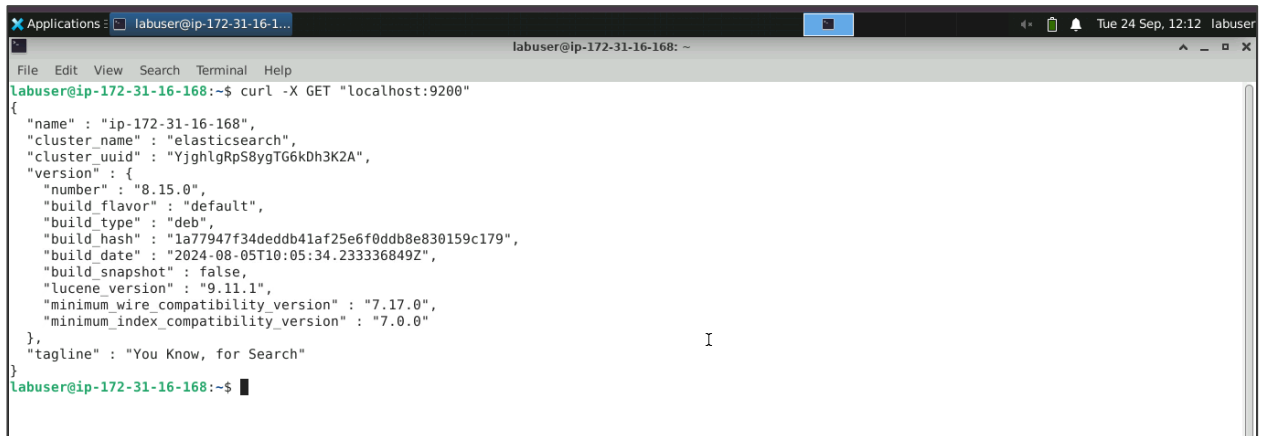
Step 1: Configure Elasticsearch for log storage

- 1.1 Run the command given below to verify that Elasticsearch is running by sending an HTTP request:

curl -X GET "localhost:9200"

A screenshot of a terminal window. The window title is "Applications: labuser@ip-172-31-16-1...". The terminal shows the prompt "labuser@ip-172-31-16-168: ~" and the command "curl -X GET \"localhost:9200\"" being typed. The command is highlighted with a red box. The terminal also shows a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The system tray at the bottom right shows the date and time "Tue 24 Sep, 12:11" and the username "labuser".

You will see the following output:



```
Applications: labuser@ip-172-31-16-1...
labuser@ip-172-31-16-168: ~
File Edit View Search Terminal Help
labuser@ip-172-31-16-168:~$ curl -X GET "localhost:9200"
{
  "name" : "ip-172-31-16-168",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "YjghlgRpS8ygTG6kDh3K2A",
  "version" : {
    "number" : "8.15.0",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "1a77947f34deddb41af25e6f0ddb8e830159c179",
    "build_date" : "2024-08-05T10:05:34.233336849Z",
    "build_snapshot" : false,
    "lucene_version" : "9.11.1",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
labuser@ip-172-31-16-168:~$
```

1.2 Run the command below to create a document in Elasticsearch:

curl -X PUT "localhost:9200/my-index" -H 'Content-Type: application/json' -d'

```
{
  "settings": {
    "number_of_shards": 3,
    "number_of_replicas": 1
  },
  "mappings": {
    "properties": {
      "field1": { "type": "text" },
      "field2": { "type": "keyword" }
    }
  }
}
```

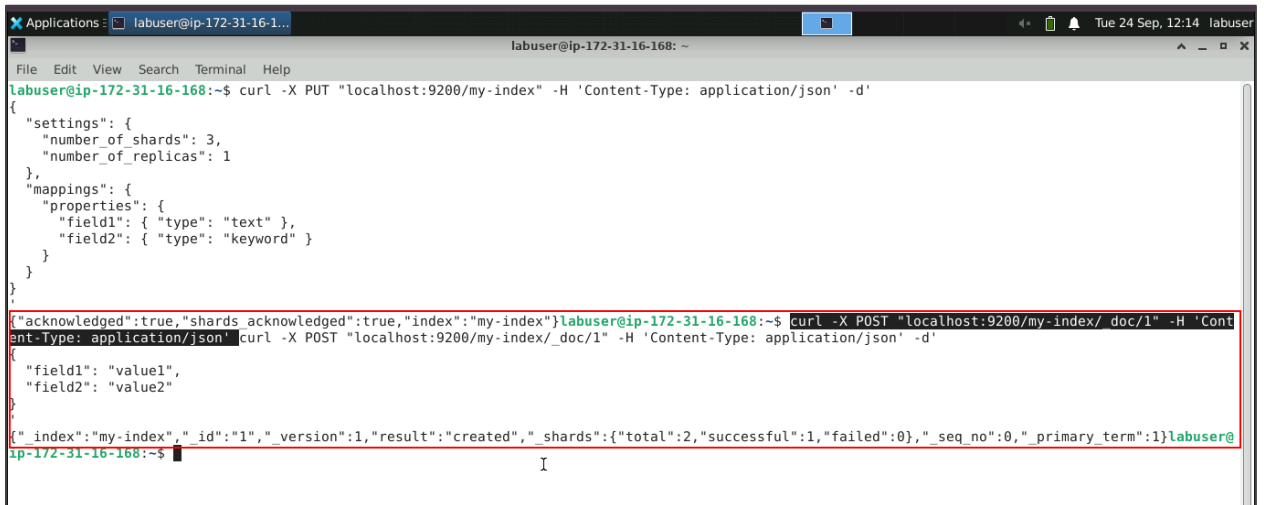


```
Applications: labuser@ip-172-31-16-1...
labuser@ip-172-31-16-168: ~
File Edit View Search Terminal Help
labuser@ip-172-31-16-168:~$ curl -X PUT "localhost:9200/my-index" -H 'Content-Type: application/json' -d'
{
  "settings": {
    "number_of_shards": 3,
    "number_of_replicas": 1
  },
  "mappings": {
    "properties": {
      "field1": { "type": "text" },
      "field2": { "type": "keyword" }
    }
  }
}
{"acknowledged":true,"shards_acknowledged":true,"index":"my-index"}labuser@ip-172-31-16-168:~$
```

Note: To create an index, you need to define the settings and mappings; use a PUT request

1.3 Run the command below to add a document using the POST request:

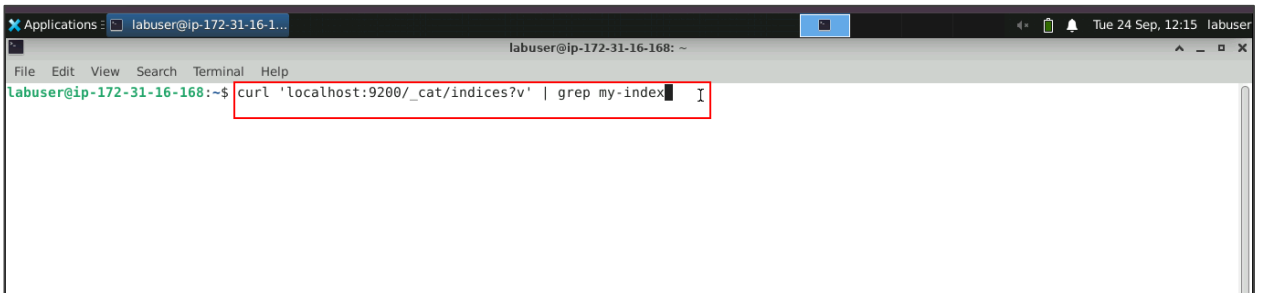
```
curl -X POST "localhost:9200/my-index/_doc/1" -H 'Content-Type: application/json' -d'
{
  "field1": "value1",
  "field2": "value2"
}
'
```

A terminal window titled 'labuser@ip-172-31-16-168: ~' shows the execution of two curl commands. The first command is a PUT request to create an index named 'my-index' with specific settings and mappings. The second command is a POST request to add a document to the 'my-index' at the path '_doc/1'. The output of the second command is highlighted with a red box, showing a successful response with document details and shard information.

```
labuser@ip-172-31-16-168:~$ curl -X PUT "localhost:9200/my-index" -H 'Content-Type: application/json' -d'
{
  "settings": {
    "number_of_shards": 3,
    "number_of_replicas": 1
  },
  "mappings": {
    "properties": {
      "field1": { "type": "text" },
      "field2": { "type": "keyword" }
    }
  }
}
'
{"acknowledged":true,"shards_acknowledged":true,"index":"my-index"}labuser@ip-172-31-16-168:~$ curl -X POST "localhost:9200/my-index/_doc/1" -H 'Content-Type: application/json' -d'
{
  "field1": "value1",
  "field2": "value2"
}
'
{"_index":"my-index","_id":"1","_version":1,"result":"created","shards":{"total":2,"successful":1,"failed":0},"seq_no":0,"primary_term":1}labuser@ip-172-31-16-168:~$
```

1.4 Run the command below to fetch the content of the index:

```
curl 'localhost:9200/_cat/indices?v' | grep my-index
```

A terminal window titled 'labuser@ip-172-31-16-168: ~' shows the command 'curl 'localhost:9200/_cat/indices?v' | grep my-index' being entered. The command is highlighted with a red box.

```
labuser@ip-172-31-16-168:~$ curl 'localhost:9200/_cat/indices?v' | grep my-index
```

The output of this is as shown:

```
Applications: labuser@ip-172-31-16-1...
labuser@ip-172-31-16-168: ~
File Edit View Search Terminal Help
labuser@ip-172-31-16-168:~$ curl 'localhost:9200/_cat/indices?v' | grep my-index
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left  Speed
100 3500    0 3500    0    0 18565    0 --:--:-- --:--:-- --:--:-- 18617
yellow open my-index 681b BH6v--53TzW35KvSfew02w 3 1 0 0 681b
labuser@ip-172-31-16-168:~$
```

1.5 Use the following command to retrieve the document stored in the index:
curl -X GET "localhost:9200/my-index/_doc/1"

```
Applications: labuser@ip-172-31-16-1...
labuser@ip-172-31-16-168: ~
File Edit View Search Terminal Help
labuser@ip-172-31-16-168:~$ curl 'localhost:9200/_cat/indices?v' | grep my-index
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left  Speed
100 3500    0 3500    0    0 18565    0 --:--:-- --:--:-- --:--:-- 18617
yellow open my-index 681b BH6v--53TzW35KvSfew02w 3 1 0 0 681b
labuser@ip-172-31-16-168:~$ curl -X GET "localhost:9200/my-index/_doc/1"
```

You will see the following output:

```
Applications: labuser@ip-172-31-16-1...
labuser@ip-172-31-16-168: ~
File Edit View Search Terminal Help
labuser@ip-172-31-16-168:~$ curl 'localhost:9200/_cat/indices?v' | grep my-index
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left  Speed
100 3500    0 3500    0    0 18565    0 --:--:~ --:~:~ --:~:~ 18617
yellow open my-index 681b BH6v--53TzW35KvSfew02w 3 1 0 0 681b
labuser@ip-172-31-16-168:~$ curl -X GET "localhost:9200/my-index/_doc/1"
{"_index":"my-index","_id":"1","_version":1,"_seq_no":0,"_primary_term":1,"found":true,"_source":
{
  "field1": "value1",
  "field2": "value2"
}
}labuser@ip-172-31-16-168:~$
```

- 1.6 Run the following command to perform index cleanup once the content is fetched and it's confirmed that the log is being stored in the index:

curl -X DELETE "localhost:9200/my-index"

```
Applications: labuser@ip-172-31-16-1...
labuser@ip-172-31-16-168: ~
File Edit View Search Terminal Help
labuser@ip-172-31-16-168:~$ curl 'localhost:9200/_cat/indices?v' | grep my-index
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left  Speed
100 3500    0 3500    0    0 18565    0 --:--:-- --:--:-- --:--:-- 18617
yellow open my-index 681b 681b BH6v--53TzW35KvSfew02w 3 1 0 0 681b
labuser@ip-172-31-16-168:~$ curl -X GET "localhost:9200/my-index/_doc/1"
{"_index":"my-index","_id":"1","_version":1,"_seq_no":0,"_primary_term":1,"found":true,"_source":
{
  "field1": "value1",
  "field2": "value2"
}}
labuser@ip-172-31-16-168:~$ curl -X DELETE "localhost:9200/my-index"
```

You will see the following output:

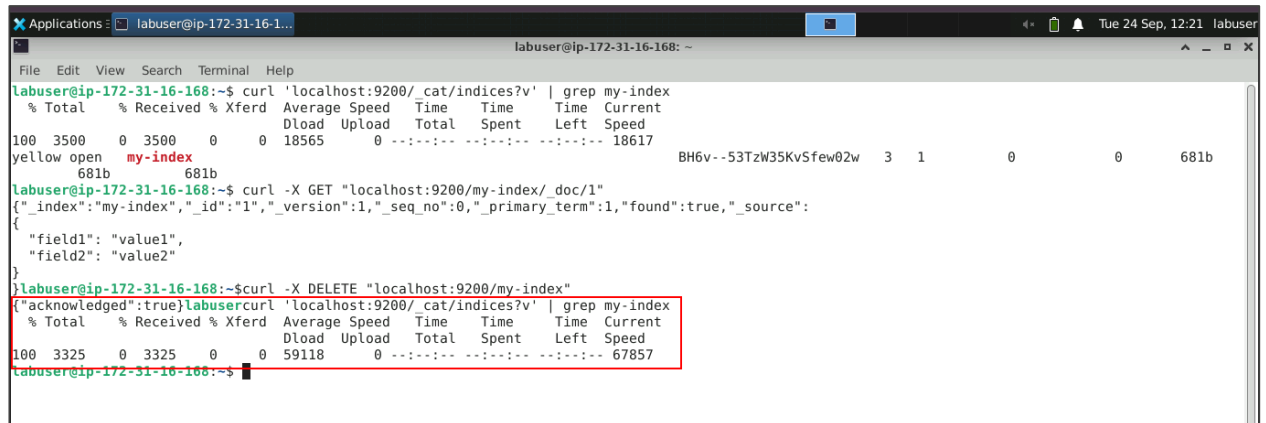
```
Applications: labuser@ip-172-31-16-1...
labuser@ip-172-31-16-168: ~
File Edit View Search Terminal Help
labuser@ip-172-31-16-168:~$ curl 'localhost:9200/_cat/indices?v' | grep my-index
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left  Speed
100 3500    0 3500    0    0 18565    0 --:--:-- --:--:-- --:--:-- 18617
yellow open my-index 681b 681b BH6v--53TzW35KvSfew02w 3 1 0 0 681b
labuser@ip-172-31-16-168:~$ curl -X GET "localhost:9200/my-index/_doc/1"
{"_index":"my-index","_id":"1","_version":1,"_seq_no":0,"_primary_term":1,"found":true,"_source":
{
  "field1": "value1",
  "field2": "value2"
}}
labuser@ip-172-31-16-168:~$ curl -X DELETE "localhost:9200/my-index"
{"acknowledged":true}
labuser@ip-172-31-16-168:~$
```

- 1.7 Execute the following command to check the status of indices and filter for **my-index**:

curl 'localhost:9200/_cat/indices?v' | grep my-index

```
Applications: labuser@ip-172-31-16-1...
labuser@ip-172-31-16-168: ~
File Edit View Search Terminal Help
labuser@ip-172-31-16-168:~$ curl 'localhost:9200/_cat/indices?v' | grep my-index
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left  Speed
100 3500    0 3500    0    0 18565    0 --:--:-- --:--:-- --:--:-- 18617
yellow open my-index 681b 681b BH6v--53TzW35KvSfew02w 3 1 0 0 681b
labuser@ip-172-31-16-168:~$ curl -X GET "localhost:9200/my-index/_doc/1"
{"_index":"my-index","_id":"1","_version":1,"_seq_no":0,"_primary_term":1,"found":true,"_source":
{
  "field1": "value1",
  "field2": "value2"
}}
labuser@ip-172-31-16-168:~$ curl -X DELETE "localhost:9200/my-index"
{"acknowledged":true}
labuser@ip-172-31-16-168:~$ curl 'localhost:9200/_cat/indices?v' | grep my-index
```

You will see the following output:



```
Applications: labuser@ip-172-31-16-1...
labuser@ip-172-31-16-168: ~
File Edit View Search Terminal Help
labuser@ip-172-31-16-168:~$ curl 'localhost:9200/_cat/indices?v' | grep my-index
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 3500    0 3500    0    0 18565    0 --:--:-- --:--:-- --:--:-- 18617
yellow open my-index        BH6v--53TzW35KvSfew02w 3 1      0      0      681b
681b        681b
labuser@ip-172-31-16-168:~$ curl -X GET "localhost:9200/my-index/_doc/1"
{"_index":"my-index","_id":"1","_version":1,"_seq_no":0,"_primary_term":1,"found":true,"_source":
{
  "field1": "value1",
  "field2": "value2"
}}
labuser@ip-172-31-16-168:~$ curl -X DELETE "localhost:9200/my-index"
{"acknowledged":true}labuser@ip-172-31-16-168:~$ curl 'localhost:9200/_cat/indices?v' | grep my-index
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 3325    0 3325    0    0 59118    0 --:--:-- --:--:-- --:--:-- 67857
labuser@ip-172-31-16-168:~$
```

By following the above steps, you have successfully implemented Elasticsearch as a monitoring tool to store application logs, enhancing log management and real-time performance insights.