ELASTICSEARCH AND KIBANA

Table of Content

Perquisites :-

JDK installed

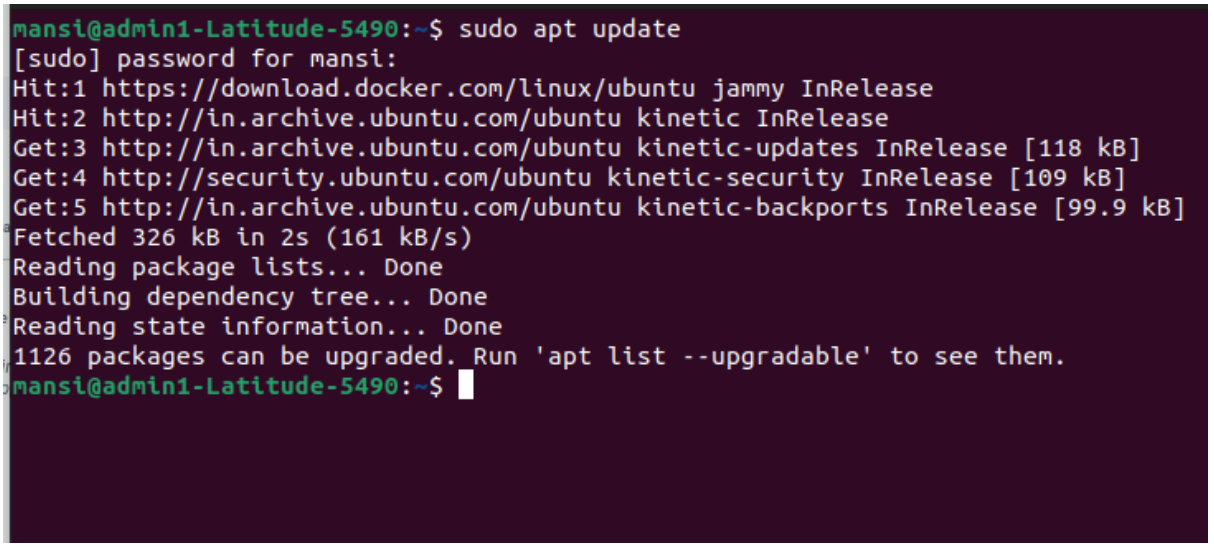
What is Elasticsearch?

- Elasticsearch is a distributed, open source and analytics engine for all types of data, including textual , numerical , geospatial , structured and unstructured.
- Elasticsearch is built on Apache lucene and was first released in 2010.
- Elasticsearch is the central component of Elastic Stack.
- Elastic search is a database that stores , retrieves and manages document-oriented and semi structured data.

Installation of Elasticsearch?

1. First Update your system.

   ```
   $ sudo apt update
   ```

2. we will install the dependencies to our system that are essential for adding an HTTP repository:

   ```
   $ sudo apt install apt-transport-https ca-certificates wget
   ```

```
mansi@admin1-Latitude-5490:~$ sudo apt install apt-transport-https ca-certificates wget

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apt-transport-https is already the newest version (2.5.3).
ca-certificates is already the newest version (20230311ubuntu0.22.10.1).
The following packages were automatically installed and are no longer required:
  bridge-utils libatk1.0-data libffi7 ubuntu-fan wmdocker
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
  wget
1 upgraded, 0 newly installed, 0 to remove and 1125 not upgraded.
Need to get 334 kB of archives.
After this operation, 53.2 kB disk space will be freed.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu kinetic/main amd64 wget amd64 1.21.3-1ubuntu1 [334 kB]
Fetched 334 kB in 2s (157 kB/s)
(Reading database ... 184411 files and directories currently installed.)
Preparing to unpack .../wget_1.21.3-1ubuntu1_amd64.deb ...
Unpacking wget (1.21.3-1ubuntu1) over (1.21.2-2ubuntu1) ...
Setting up wget (1.21.3-1ubuntu1) ...
Processing triggers for install-info (6.8-4build1) ...
Processing triggers for man-db (2.10.2-1) ...
mansi@admin1-Latitude-5490:~$
```

3. Now, it's time to import the GPG's key of the Elasticsearch repository:

```
$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
```

```
mansi@admin1-Latitude-5490:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
mansi@admin1-Latitude-5490:~$
```

4. we will add the Elasticsearch repository

```
$ sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list'
```

```
mansi@admin1-Latitude-5490:~$ sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.l
ist'
mansi@admin1-Latitude-5490:~$
mansi@admin1-Latitude-5490:~$
```

5. Now update.

```
$ sudo apt update
```

```
mansi@admin1-Latitude-5490:~$ sudo apt update
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.7 kB]
Get:2 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [111 kB]
Get:3 https://artifacts.elastic.co/packages/7.x/apt stable/main i386 Packages [81.3 kB]
Get:4 http://security.ubuntu.com/ubuntu kinetic-security InRelease [109 kB]
Hit:5 http://in.archive.ubuntu.com/ubuntu kinetic InRelease
Hit:6 https://download.docker.com/linux/ubuntu jammy InRelease
Get:7 http://in.archive.ubuntu.com/ubuntu kinetic-updates InRelease [118 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu kinetic-backports InRelease [99.9 kB]
Fetched 532 kB in 2s (310 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1126 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the D
EPRECATION section in apt-key(8) for details.
mansi@admin1-Latitude-5490:~$
```

6. Installing elasticsearch on your system:

```
$ sudo apt install elasticsearch
```

```
mansi@admin1-Latitude-5490:~$  sudo apt install elasticsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  bridge-utils libatk1.0-data libffi7 ubuntu-fan wmdocker
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
  elasticsearch
1 upgraded, 0 newly installed, 0 to remove and 1125 not upgraded.
Need to get 317 MB of archives.
After this operation, 39.6 MB disk space will be freed.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 elasticsearch amd64 7.17.10 [317 MB]
Fetched 317 MB in 17s (18.9 MB/s)
(Reading database ... 184411 files and directories currently installed.)
Preparing to unpack .../elasticsearch_7.17.10_amd64.deb ...
Unpacking elasticsearch (7.17.10) over (7.15.0) ...
Setting up elasticsearch (7.17.10) ...
Installing new version of config file /etc/elasticsearch/elasticsearch.yml ...
Installing new version of config file /etc/elasticsearch/jvm.options ...
Installing new version of config file /etc/elasticsearch/log4j2.properties ...
Installing new version of config file /etc/init.d/elasticsearch ...
Created elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
mansi@admin1-Latitude-5490:~$
```

7. Next, start the service of the installed engine by executing this command:

```
$ systemctl daemon-reload
```

```
hansi@admin1-Latitude-5490:~$ systemctl daemon-reload
hansi@admin1-Latitude-5490:~$ sudo systemctl start elasticsearch
hansi@admin1-Latitude-5490:~$
```

8. You can confirm if Elasticsearch is successfully running on your system by using the curl command. For this purpose, write out the curl command for submitting an HTTP request to your system's port 9200:

```
$ curl -X GET "localhost:9200/"
```

```
hansi@admin1-Latitude-5490:~$ curl -X GET "localhost:9200/"
{
  "name" : "admin1-Latitude-5490",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "osXzBoewQWaacDKuvsvp3Q",
  "version" : {
    "number" : "7.15.0",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "79d65f6e357953a5b3cbcc5e2c7c21073d89aa29",
    "build_date" : "2021-09-16T03:05:29.143308416Z",
    "build_snapshot" : false,
    "lucene_version" : "8.9.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
hansi@admin1-Latitude-5490:~$
```

Components of Elasticsearch

1. **Cluster:**

   In Elasticsearch, a cluster is a group of computers that work together. They team up to store and manage large amounts of data and handle search requests. It's like having a team of computers that collaborate to make sure everything runs smoothly and quickly. The cluster ensures that your data is available even if some computers in the team go offline, so you don't lose any information.

2. **Node:**

   In Elasticsearch, a node is like a computer or server. It stores and manages data and helps with searching. It's like having a member of the group who contributes to the overall work. Nodes communicate with each other to share data, handle search requests, and make sure everything is running smoothly. If one node is busy or not available, the others take over to ensure your data is still accessible.

3. **Index:**

   In Elasticsearch, an index is like a collection or category where you store and organize your data. Its purpose is to assist in searching and retrieving data.

4. **Shard:**

In Elasticsearch, a shard is like a smaller piece of an index. When you make an index, it can be split into smaller parts called shards.

5. Document:

In Elasticsearch, a document is like a single item of information. It could be a piece of text, an image, or any other data you want to store. Think of it as a single file that holds specific details. Each document is stored in a structured way and can be searched, accessed, or analyzed separately.

6. Mapping:

In Elasticsearch, mapping is like a blueprint that defines how your data is organized and structured within an index. It tells Elasticsearch the data types of the fields, such as text, numbers, dates, or geographic locations, and how they should be analyzed and indexed for efficient searching.

7. Query:

In Elasticsearch, a query is like a question you ask to find specific information in your stored documents. It helps you search for data, sort out the results you want, and collect data based on specific conditions or rules. It's a way to get the exact information you're looking for from your indexed documents.

Setup a Multi-Node Elasticsearch Cluster with Docker Compose

Prerequisites:

- Docker is installed on your system.
- Docker compose is installed on your system.

Step 1: Create a Docker Compose YAML file

1. First i create a directory with name of elasticsearch-cluster.

```
$ mkdir elasticsearch-cluster
```

2. Then go into that directory .

```
$ cd elasticsearch-cluster
```

3. Create a new file named **docker-compose.yml** and open it in a text editor.

```
$ vim docker-compose.yml
```

4. Add the following contents to define the Elasticsearch services:
yaml

```yaml
version: '3'
services:
 node1:
  image: docker.elastic.co/elasticsearch/elasticsearch:7.14.0
  container_name: node1
  environment:
   - discovery.type=single-node
  ports:
   - 9200:9200
   - 9300:9300
  networks:
   - elastic

 node2:
  image: docker.elastic.co/elasticsearch/elasticsearch:7.14.0
  container_name: node2
  environment:
   - discovery.seed_hosts=node1
  ports:
   - 9201:9200
   - 9301:9300
  networks:
   - elastic

 node3:
  image: docker.elastic.co/elasticsearch/elasticsearch:7.14.0
  container_name: node3
  environment:
   - discovery.seed_hosts=node1
  ports:
   - 9202:9200
   - 9302:9300
  networks:
```

```
    - elastic

networks:
  elastic:
    driver: bridge
```

Step 2: Start the Elasticsearch Cluster

```
$ docker-compose up -d
```

Step 3: Verify the Cluster

Use the following command to check the cluster health:
shell

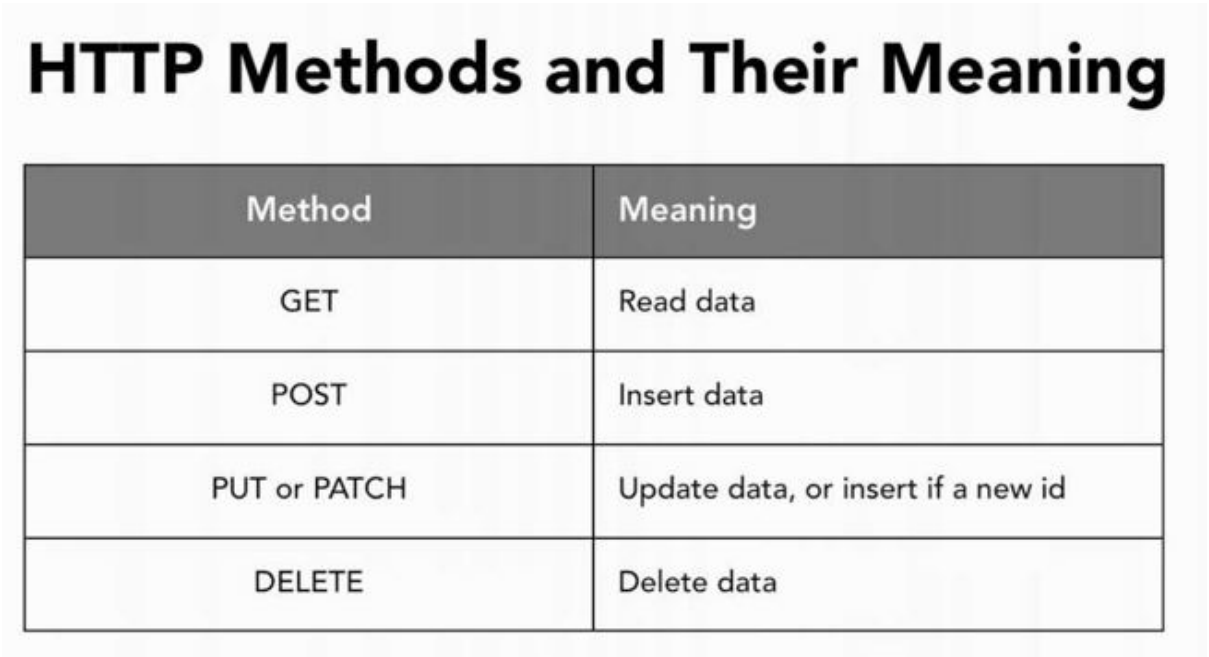
```
$ curl -XGET http://localhost:9200/_cluster/health?pretty=true
```

If the cluster is up and running, you should see a JSON

response indicating the cluster's health status.

PUT, GET, and POST methods are commonly used in Elasticsearch:

In Elasticsearch, the PUT, GET, and POST commands are commonly used to interact with the data stored in the Elasticsearch cluster.



HTTP Methods and Their Meaning

Method	Meaning
GET	Read data
POST	Insert data
PUT or PATCH	Update data, or insert if a new id
DELETE	Delete data

Some Commands in ELasticsearch

1. Create an index : -

```
$ curl -XPUT http://localhost:9200/mansi
```

2. To store data in Elasticsearch use POST command: -

```
$ curl -XPOST -H "Content-Type: application/json" -d '{"name": "mansi", "task": "elk", "assigned by": "ashish sir"}' http://localhost:9200/mansi/_doc/?pretty
```

3. To see all index in Elasticsearch.

```
$ curl -XGET "localhost:9200/_cat/indices?v
```

4. To see cluster health :-

```
$ curl localhost:9200/_cat/health?v
```

5. To see data in index :-

```
 $ curl -XGET http://localhost:9200/mansi/_search
```

What is Kibana:

Kibana is open source data visualizations and exploration tool designed for elasticsearch.
It allow users to interact with data stored in elasticsearch and create visualizations , dashboards and reports for easy data analysis and monitoring.

Installation kibana on ubuntu:

1. Add the Kibana APT repository to your system (similar to Elasticsearch):

```
$ sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list'
```

2. Install Kibana:

```
$ sudo apt update
```

```
$ sudo apt install kibana
```

3. Configure Kibana to connect to Elasticsearch:

Open the Kibana configuration file:

```
$ sudo nano /etc/kibana/kibana.yml
```

Find the line that starts with `# server.host:` and replace it with:

```
server.host: "localhost"
```

4. Start and enable the Kibana service:

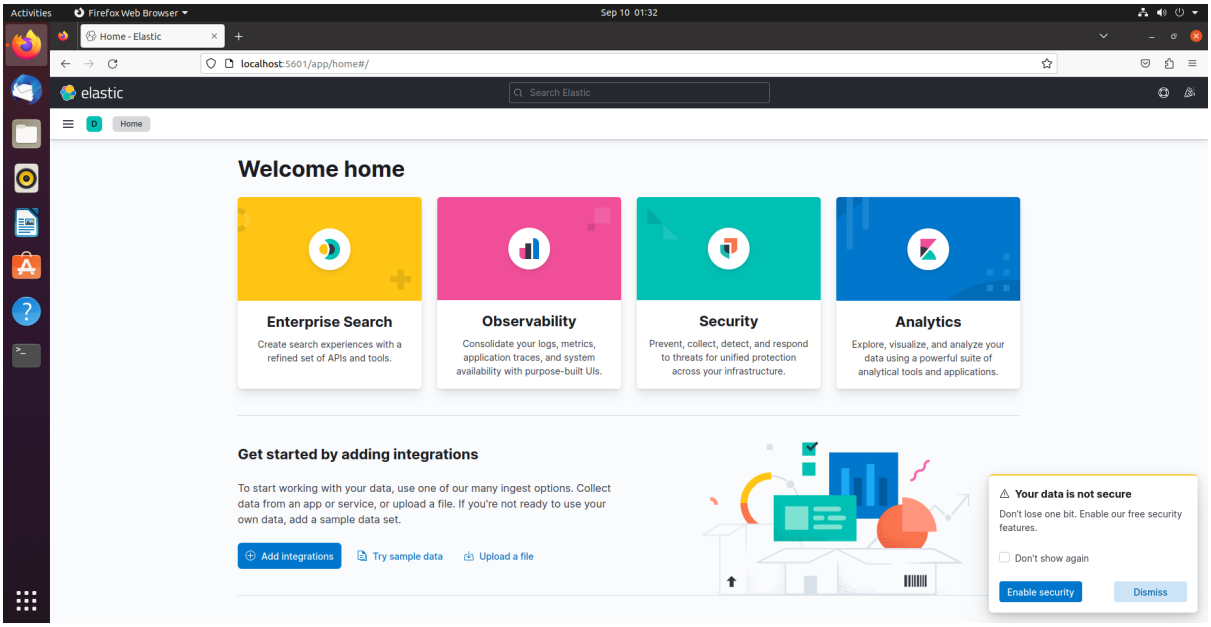
```
sudo systemctl start kibana
```

```
sudo systemctl enable kibana
```

Step 4: Access Kibana

Kibana's default port is 5601. You can access Kibana by opening a web browser and navigating to

http://localhost:5601.


Activities
Firefox Web Browser
Sep 10 01:32
Home - Elastic
localhost:5601/app/home#/
elastic
Search Elastic
D
Home
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.
Add integrations
Try sample data
Upload a file
Your data is not secure
Don't lose one bit. Enable our free security features.
Don't show again
Enable security
Dismiss