Arkime with Elasticsearch in ubuntu 22.04.3

You can either go with the official documentation of Arkime installation

https://raw.githubusercontent.com/arkime/arkime/main/release/README.txt

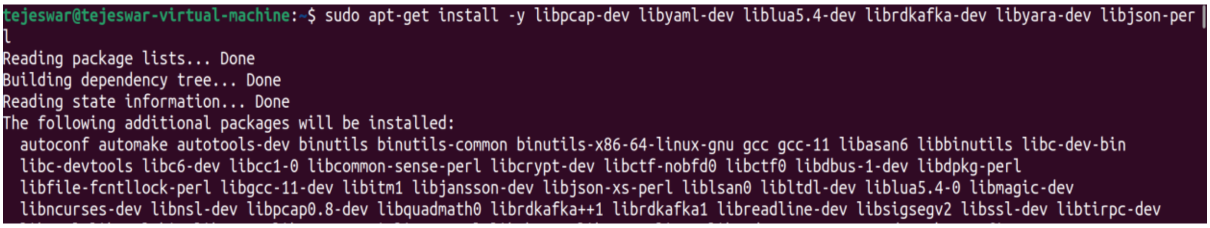
OR

You can follow the process, in which I have configured the elastic first and then configured elastic with Arkime.

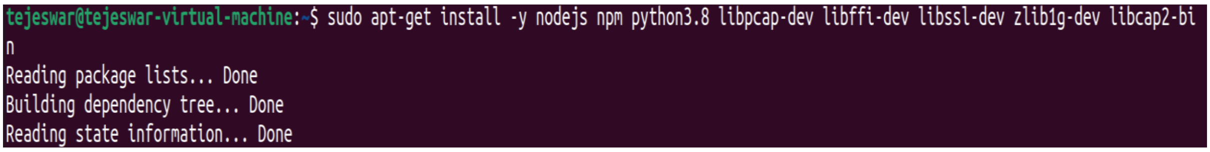
For that

First Install all the dependencies needed for the smoother handing of arkime along with elasticsearch

- **sudo apt-get install -y nodejs npm python3.8 libpcap-dev libffi-dev libssl-dev zlib1g-dev libcap2-bin libyaml-dev liblua5.4-dev librdkafka-dev libyara-dev libjson-perl**



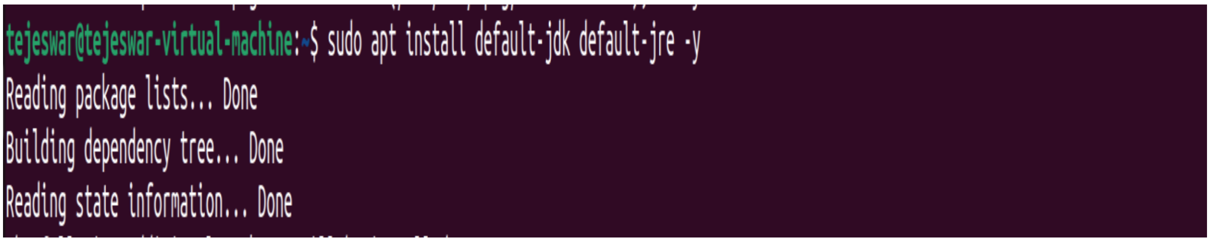
```
tejeswar@tejeswar-virtual-machine:~$ sudo apt-get install -y libpcap-dev libyaml-dev liblua5.4-dev librdkafka-dev libyara-dev libjson-per
l
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  autoconf automake autotools-dev binutils binutils-common binutils-x86-64-linux-gnu gcc gcc-11 libasan6 libbinutils libc-dev-bin
  libc-devtools libc6-dev libcc1-0 libcommon-sense-perl libcrypt-dev libctf-nobfd0 libctf0 libdbus-1-dev libdpkg-perl
  libfile-fcntllock-perl libgcc-11-dev libitm1 libjansson-dev libjson-xs-perl liblsan0 libltdl-dev liblua5.4-0 libmagic-dev
  libncurses-dev libnsl-dev libpcap0.8-dev libquadmath0 librdkafka++1 librdkafka1 libreadline-dev libsigsegv2 libssl-dev libtirpc-dev
```



```
tejeswar@tejeswar-virtual-machine:~$ sudo apt-get install -y nodejs npm python3.8 libpcap-dev libffi-dev libssl-dev zlib1g-dev libcap2-bi
n
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Install Default Java Development Kit(**JDK**) and Java Runtime Environment(**JRE**) in linux(in my case)

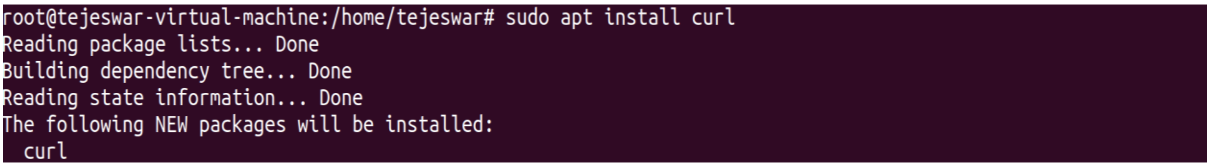
- **sudo apt install default-jdk default-jre -y**



```
tejeswar@tejeswar-virtual-machine:~$ sudo apt install default-jdk default-jre -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Install “**curl**”, which is used to interact with Elasticsearch, which is the backend storage system used to store and retrieve network traffic data.

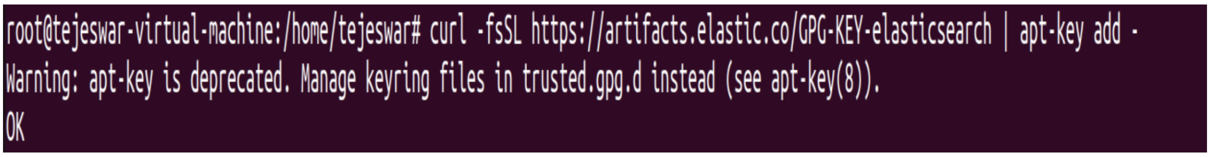
- **sudo apt install curl**



```
root@tejeswar-virtual-machine:/home/tejeswar# sudo apt install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  curl
```

Add this elastic GPG key to your system is to verify the integrity of the Elasticsearch packages you install via apt.

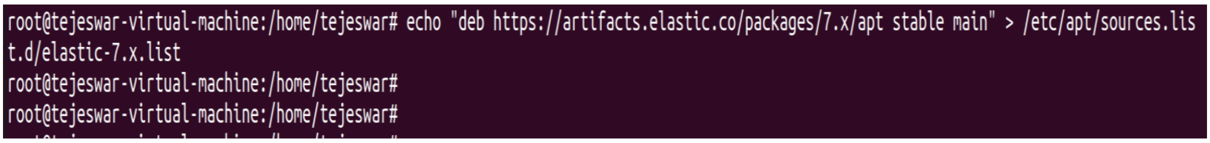
- **curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -**



```
root@tejeswar-virtual-machine:/home/tejeswar# curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
```

Now, add this terminal, which ensures that you're installing Elasticsearch packages from the specified repository, making it easier to manage Elasticsearch installations and updates on your system

- **echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/ elastic-7.x.list**



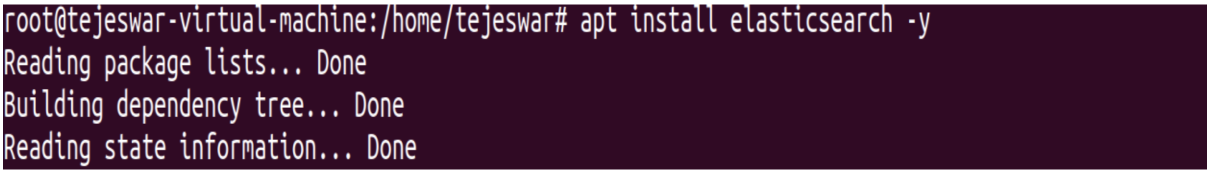
```
root@tejeswar-virtual-machine:/home/tejeswar# echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.lis
t.d/elastic-7.x.list
root@tejeswar-virtual-machine:/home/tejeswar#
root@tejeswar-virtual-machine:/home/tejeswar#
```

For, Resolving Dependencies and Compatibility -

- **sudo apt update**
- **sudo apt upgrade**

Now, install the elasticsearch

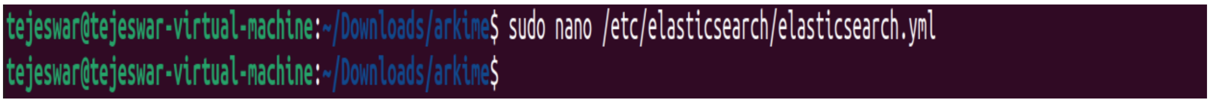
- **sudo apt install elasticsearch -y**



```
root@tejeswar-virtual-machine:/home/tejeswar# apt install elasticsearch -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Now, open the “elasticsearch.yml” file, by giving this path in the terminal with nano

- **sudo nano /etc/elasticsearch/elasticsearch.yml**

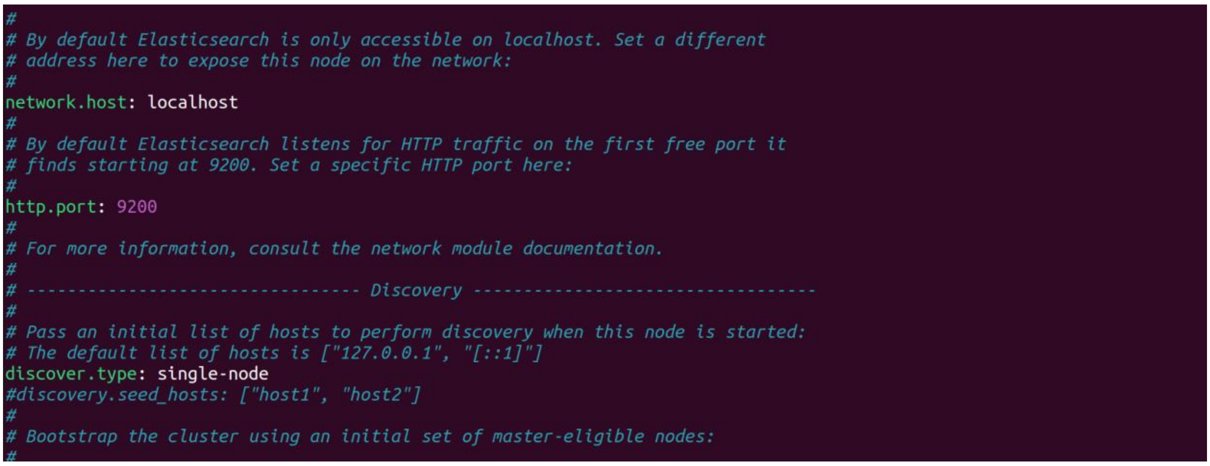


```
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$ sudo nano /etc/elasticsearch/elasticsearch.yml
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$
```

After, opening elasticsearch.yml file, now modify the configurations based on your systems configurations,

Here, i have un commented “network.host” and configured it locally and uncommented its port

And have added “discover.type: single-node”



```
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: localhost
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# --------------------------------- Discovery ----------------------------------
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
discover.type: single-node
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
```

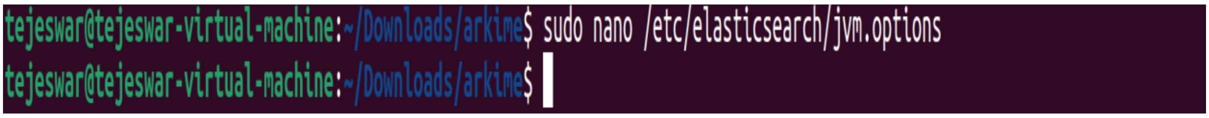
Now, save this file(ctrl+0)

save changes and file name as it is(ctrl + s)

exit(ctrl o)

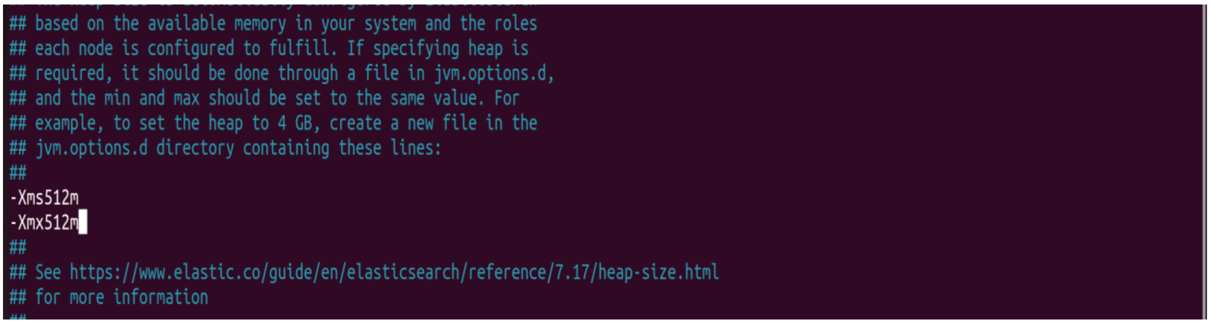
Similarly, enter this path in terminal and open it with nano

- **sudo nano /etc/elasticsearch/jvm.options**



```
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$ sudo nano /etc/elasticsearch/jvm.options
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$ 
```

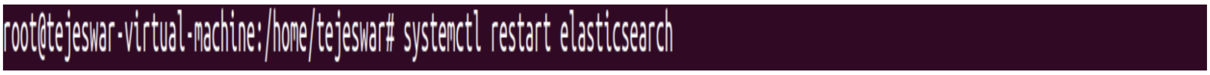
Here, I have uncommented the both and modified it based on my preferences[specify the initial and maximum heap size for the Java Virtual Machine (JVM)]



```
## based on the available memory in your system and the roles
## each node is configured to fulfill. If specifying heap is
## required, it should be done through a file in jvm.options.d,
## and the min and max should be set to the same value. For
## example, to set the heap to 4 GB, create a new file in the
## jvm.options.d directory containing these lines:
##
-Xms512m
-Xmx512m
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/heap-size.html
## for more information
```

Now, restart the elastic service to get update the preferences that we have added and modified

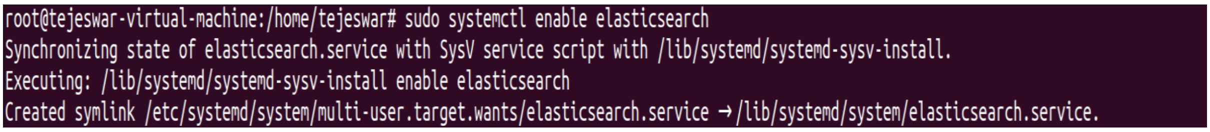
- **sudo systemctl restart elasticsearch**



```
root@tejeswar-virtual-machine:/home/tejeswar# systemctl restart elasticsearch
```

Now, run this command in the terminal. Which is used to enable the Elasticsearch service to start automatically during system boot on a Linux system that uses the systemd init system

- **sudo systemctl enable elasticsearch**



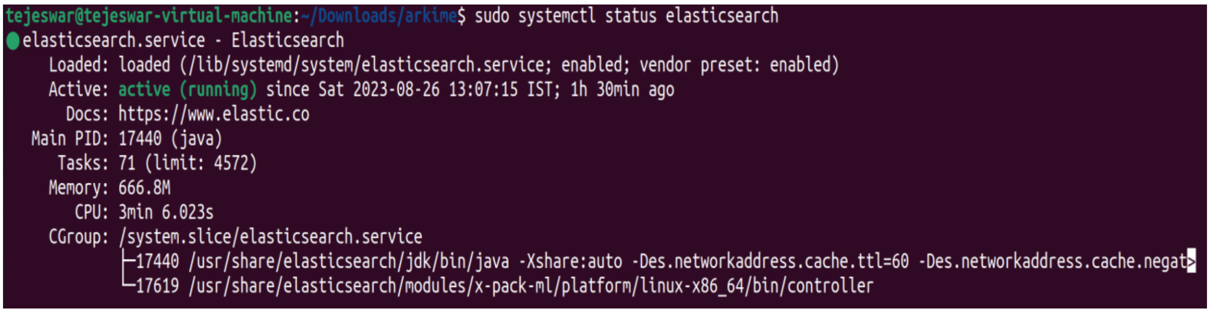
```
root@tejeswar-virtual-machine:/home/tejeswar# sudo systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
```

Now, check for the status of elastic search,

- **sudo systemctl status elasticsearch**

If, inactive

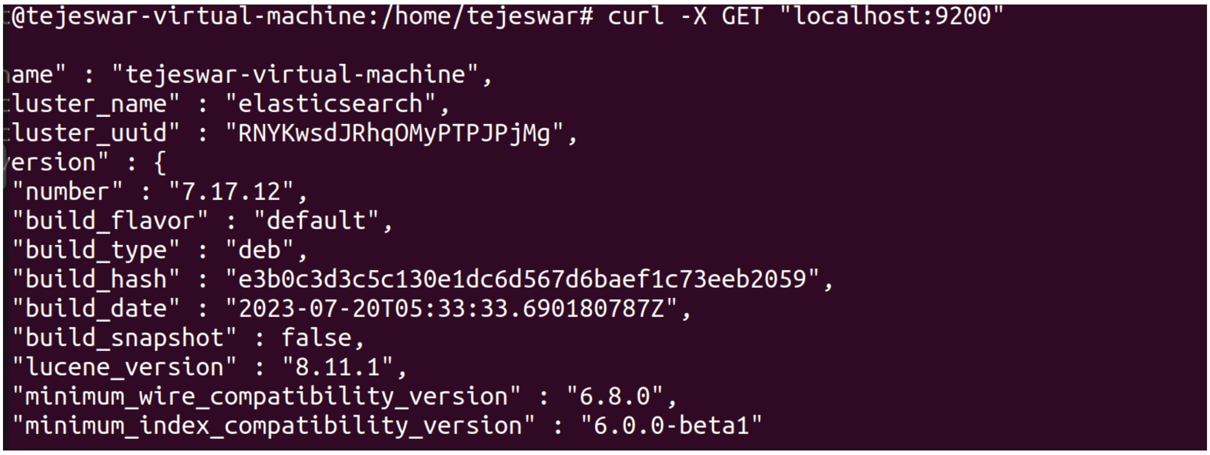
- **sudo systemctl start elasticsearch**



```
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2023-08-26 13:07:15 IST; 1h 30min ago
       Docs: https://www.elastic.co
   Main PID: 17440 (java)
      Tasks: 71 (limit: 4572)
     Memory: 666.8M
        CPU: 3min 6.023s
     CGroup: /system.slice/elasticsearch.service
             ├─17440 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negat>
             └─17619 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller
```

Enter this command in the terminal, which sends a GET request to the Elasticsearch server running on the local machine (hence "localhost") on port 9200. (to know in active state or not).

- **curl -X GET “localhost:9200”**

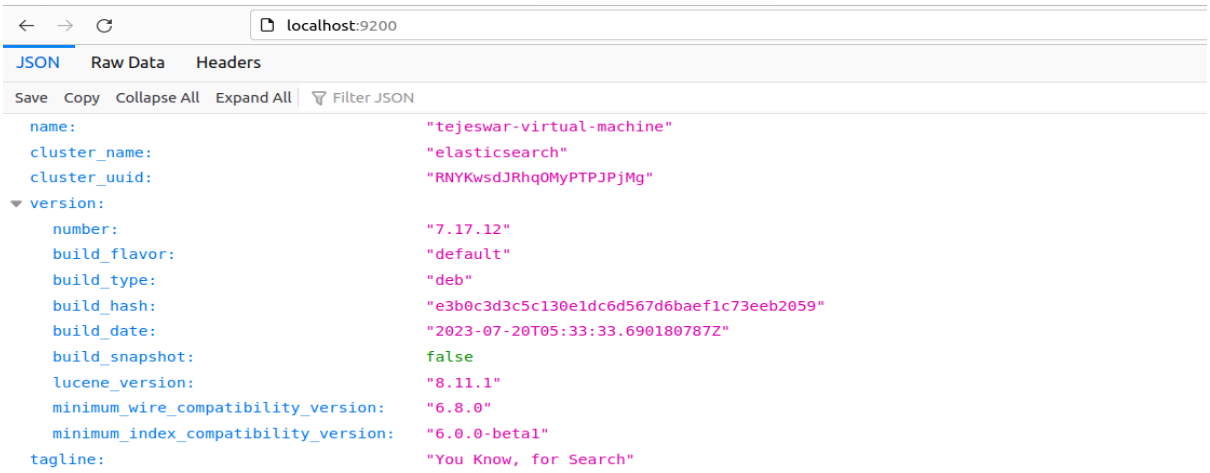


```
@tejeswar-virtual-machine:/home/tejeswar# curl -X GET "localhost:9200"

ame" : "tejeswar-virtual-machine",
luster_name" : "elasticsearch",
luster_uuid" : "RNYKwsdJRhqOMyPTPJPjMg",
ersion" : {
"number" : "7.17.12",
"build_flavor" : "default",
"build_type" : "deb",
"build_hash" : "e3b0c3d3c5c130e1dc6d567d6baef1c73eeb2059",
"build_date" : "2023-07-20T05:33:33.690180787Z",
"build_snapshot" : false,
"lucene_version" : "8.11.1",
"minimum_wire_compatibility_version" : "6.8.0",
"minimum_index_compatibility_version" : "6.0.0-beta1"
```

Or, you can open your browser and type this url, to know if its active or not

- **http://localhost:9200/**



```
name:                                  "tejeswar-virtual-machine"
cluster_name:                          "elasticsearch"
cluster_uuid:                          "RNYKwsdJRhqOMyPTPJPjMg"
▼ version:
  number:                              "7.17.12"
  build_flavor:                        "default"
  build_type:                          "deb"
  build_hash:                          "e3b0c3d3c5c130e1dc6d567d6baef1c73eeb2059"
  build_date:                          "2023-07-20T05:33:33.690180787Z"
  build_snapshot:                      false
  lucene_version:                      "8.11.1"
  minimum_wire_compatibility_version:  "6.8.0"
  minimum_index_compatibility_version: "6.0.0-beta1"
tagline:                               "You Know, for Search"
```

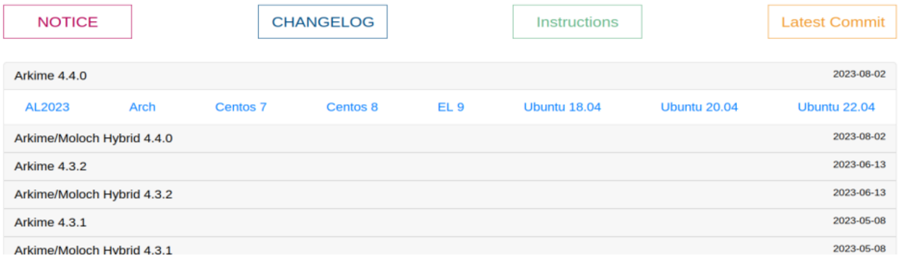
Upto here, we have installed and configured elasticsearch successfully.

ARKIME INSTALLATION

Go to the official website of arkime and install arkime file based on the system configuration.

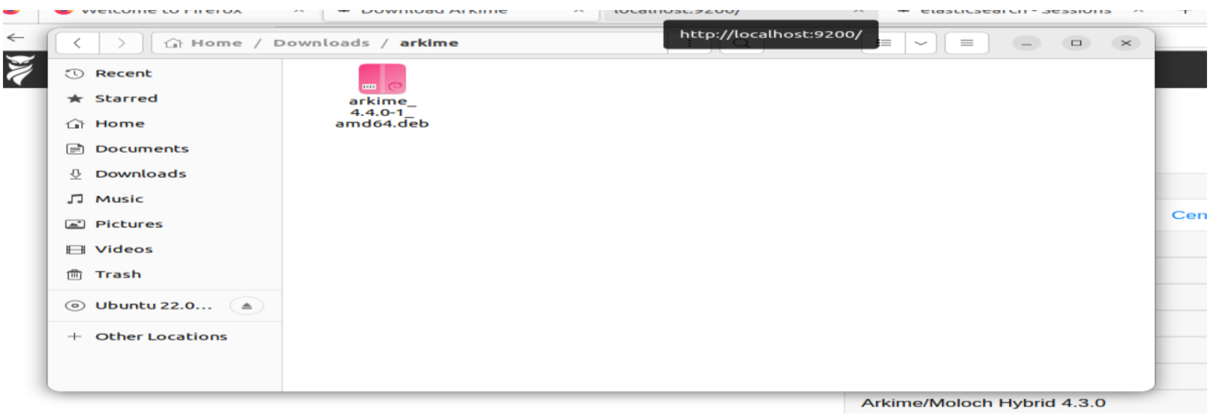
In my case, since I have ubuntu 22.04.3, I have installed Ubuntu 22.04 file from arkime official website.

- https://arkime.com/downloads



Arkime 4.4.0	2023-08-02
AL2023 Arch Centos 7 Centos 8 EL 9 Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04	
Arkime/Moloch Hybrid 4.4.0	2023-08-02
Arkime 4.3.2	2023-06-13
Arkime/Moloch Hybrid 4.3.2	2023-06-13
Arkime 4.3.1	2023-05-08
Arkime/Moloch Hybrid 4.3.1	2023-05-08

The, downloaded file gets saved in your downloads folder in the form of zip file.

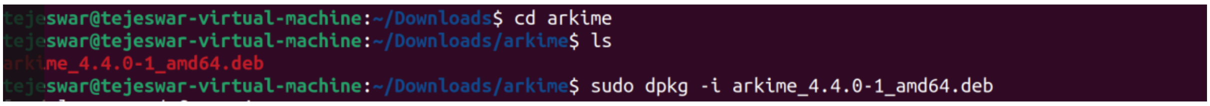


Now, change your pwd(present working directory) to the file where it got stored(Downloads)

And now I have unzipped the file by using the following command

sudo dpkg -i (foldername), in my case

- **sudo dpkg -I arkime_4.4.0-1_amd64.deb**



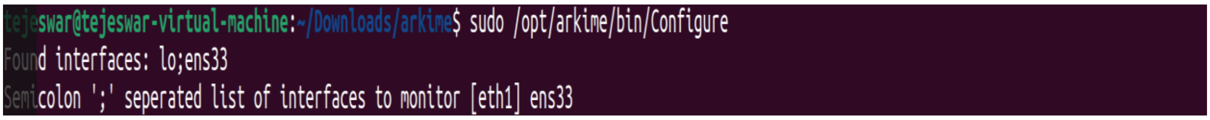
```
tejeswar@tejeswar-virtual-machine:~/Downloads$ cd arkime
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$ ls
arkime_4.4.0-1_amd64.deb
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$ sudo dpkg -i arkime_4.4.0-1_amd64.deb
```

Now, run the following command and select the network interface you want to monitor and capture the traffic. In my case its "**ens33**".[That's why, I have entered ens33].

- **Sudo /opt/arkime/bin/configure**

To, know the interfaces available. Enter this command in your terminal.

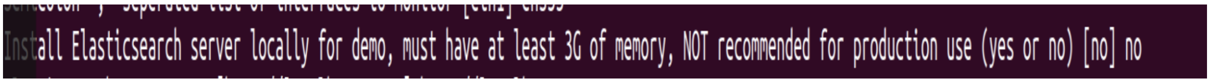
- **Ifconfig -a.**



```
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$ sudo /opt/arkime/bin/Configure
Found interfaces: lo;ens33
Semicolon ';' seperated list of interfaces to monitor [eth1] ens33
```

After entering your network interface, you will be prompted to this.

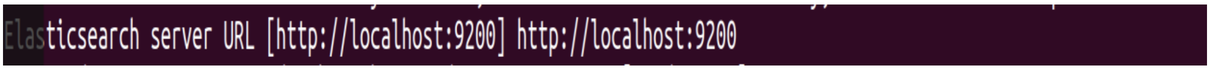
Where, you first type "**no"** (Since, you have already installed Elasticsearch server at the beginning)



```
Install Elasticsearch server locally for demo, must have at least 3G of memory, NOT recommended for production use (yes or no) [no] no
```

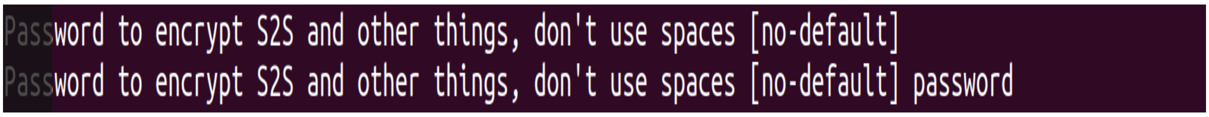
Nxt, you need to enter the details of your cluster and port where it is present, in our case we have installed the elasticsearch server internally and also the port number we have assigned, so I have given like

- http://localhost:9200



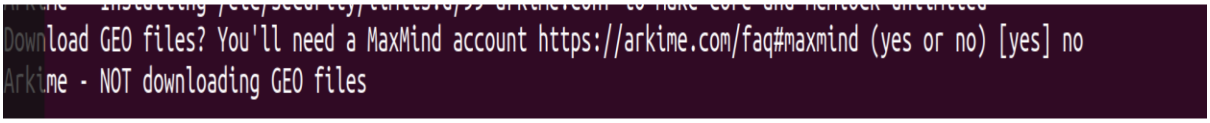
```
Elasticsearch server URL [http://localhost:9200] http://localhost:9200
```

Nxt, I have set the default Password as "**password**"



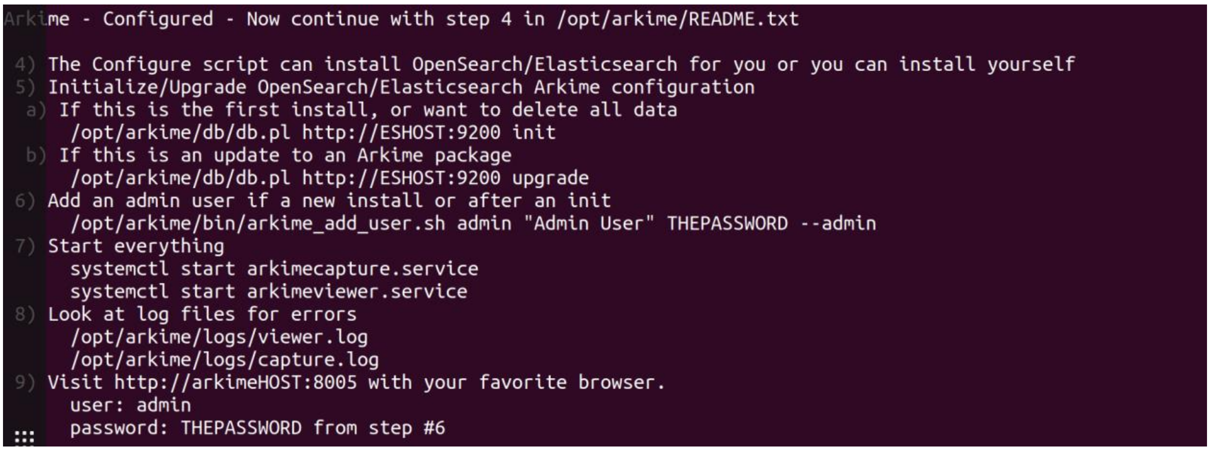
```
Password to encrypt S2S and other things, don't use spaces [no-default]
Password to encrypt S2S and other things, don't use spaces [no-default] password
```

Since, I don't have any account in MaxMind, I have entered "**no"**



```
Download GEO files? You'll need a MaxMind account https://arkime.com/faq#maxmind (yes or no) [yes] no
Arkime - NOT downloading GEO files
```

Nxt, we need to follow these steps for configuring,



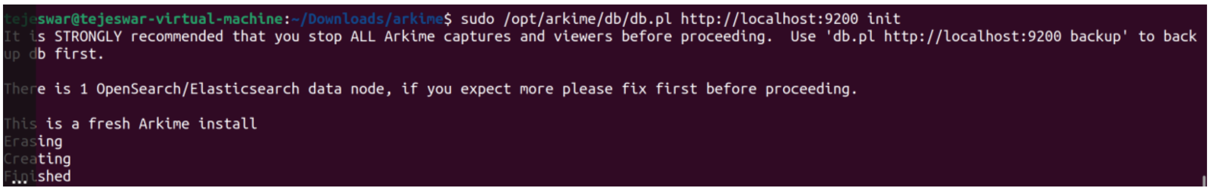
```
Arkime - Configured - Now continue with step 4 in /opt/arkime/README.txt

 4) The Configure script can install OpenSearch/Elasticsearch for you or you can install yourself
 5) Initialize/Upgrade OpenSearch/Elasticsearch Arkime configuration
  a) If this is the first install, or want to delete all data
      /opt/arkime/db/db.pl http://ESHOST:9200 init
  b) If this is an update to an Arkime package
      /opt/arkime/db/db.pl http://ESHOST:9200 upgrade
 6) Add an admin user if a new install or after an init
      /opt/arkime/bin/arkime_add_user.sh admin "Admin User" THEPASSWORD --admin
 7) Start everything
      systemctl start arkimecapture.service
      systemctl start arkimeviewer.service
 8) Look at log files for errors
      /opt/arkime/logs/viewer.log
      /opt/arkime/logs/capture.log
 9) Visit http://arkimeHOST:8005 with your favorite browser.
      user: admin
      password: THEPASSWORD from step #6
```

Since, we have already configured elasticsearch, we will go for step 5

- **Sudo /opt/arkime/db/db.pl http://localhost:9200 init**

Where EHOST [The elasticserver ip address, I our case its our localhost]



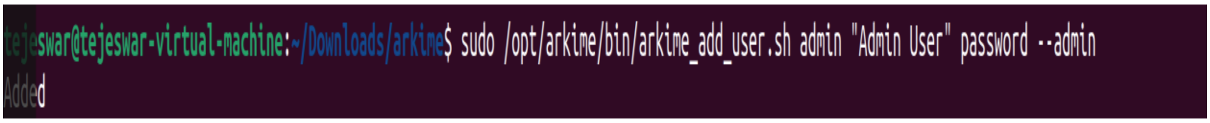
```
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$ sudo /opt/arkime/db/db.pl http://localhost:9200 init
It is STRONGLY recommended that you stop ALL Arkime captures and viewers before proceeding.  Use 'db.pl http://localhost:9200 backup' to back
up db first.

There is 1 OpenSearch/Elasticsearch data node, if you expect more please fix first before proceeding.

This is a fresh Arkime install
Erasing
Creating
Finished
```

Next, we will set an admin user, by giving username and password, in my case “**admin**” and “**password**”

Thus, we will get a prompt, “**Added**”



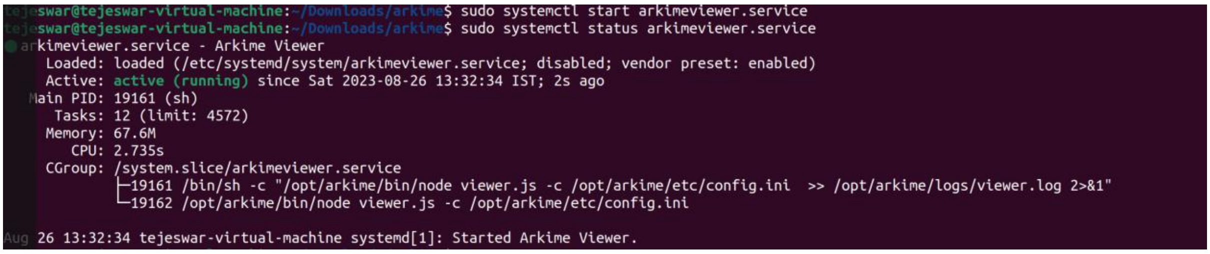
```
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$ sudo /opt/arkime/bin/arkime_add_user.sh admin "Admin User" password --admin
Added
```

To, know the status of viewer service for web-interface mode

- **sudo systemctl status arkimeviewer.service**

if it is inactive, Now you can start the capturing service, by entering the following command in the terminal

- **sudo systemctl start arkimeviewer.service**

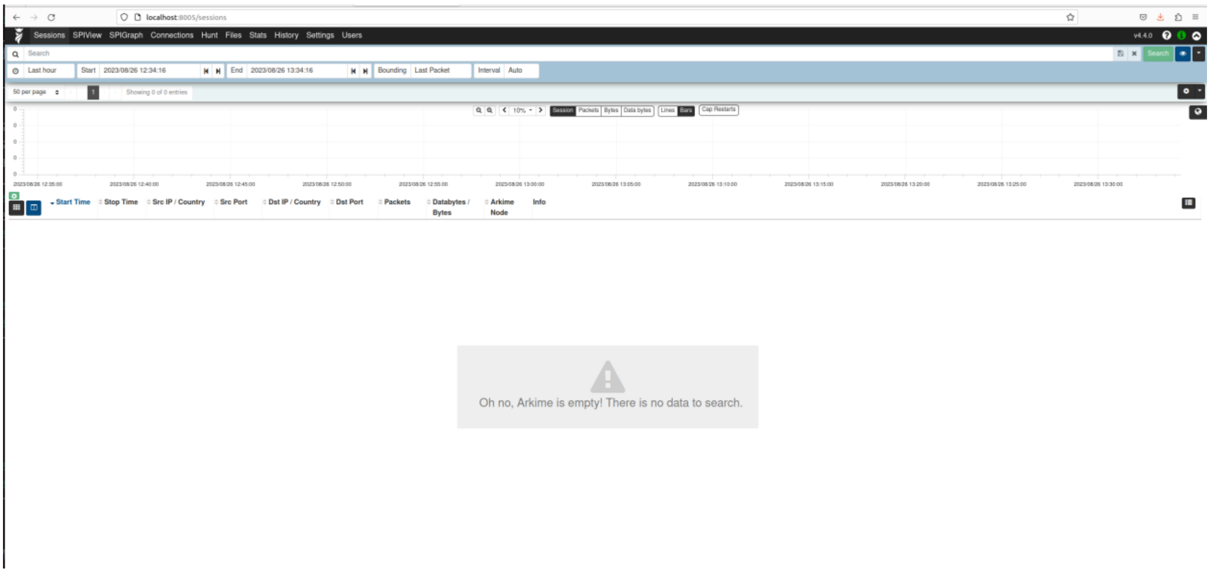


```
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$ sudo systemctl start arkimeviewer.service
tejeswar@tejeswar-virtual-machine:~/Downloads/arkime$ sudo systemctl status arkimeviewer.service
● arkimeviewer.service - Arkime Viewer
     Loaded: loaded (/etc/systemd/system/arkimeviewer.service; disabled; vendor preset: enabled)
     Active: active (running) since Sat 2023-08-26 13:32:34 IST; 2s ago
   Main PID: 19161 (sh)
      Tasks: 12 (limit: 4572)
     Memory: 67.6M
        CPU: 2.735s
     CGroup: /system.slice/arkimeviewer.service
             ├─19161 /bin/sh -c "/opt/arkime/bin/node viewer.js -c /opt/arkime/etc/config.ini  >> /opt/arkime/logs/viewer.log 2>&1"
             └─19162 /opt/arkime/bin/node viewer.js -c /opt/arkime/etc/config.ini

Aug 26 13:32:34 tejeswar-virtual-machine systemd[1]: Started Arkime Viewer.
```

Since, you have started the viewer mode, you can access it using the following url

- **http://localhost:8005/sessions**



Last hour Start 2023/08/26 12:34:16 End 2023/08/26 13:34:16 Bounding Last Packet Interval Auto

50 per page 1 Showing 0 of 0 entries

Oh no, Arkime is empty! There is no data to search.

Since, we haven't started any capture service, theres no record of logs got stored.

Once, you start the capturing service, you will prompt with the activity logs in the web interface. To start the capturing service

- **sudo systemctl start arkimecapture.service**

and to check the its status(either active or inactive)

- **sudo systemctl status arkimecapture.service**