**Logs send to Elastic search :**

From Scratch:-

Setup Elk in ubuntu:

---------------

If it is Ubuntu:- sudo apt-get update && apt-get upgrade –y

1)If it is linux:yum update –y

2)sudo apt-get install apt-transport-https -y

3)echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

4) sudo apt-get update && sudo apt-get install elasticsearch

5) sudo apt-get install kibana

Edit the elasticsearch.yml like below:-

Location:=/etc/elasticsearch/elasticsearch.yml

# ======================== Elasticsearch Configuration =========================

#

# NOTE: Elasticsearch comes with reasonable defaults for most settings.

# Before you set out to tweak and tune the configuration, make sure you

# understand what are you trying to accomplish and the consequences.

#`

# The primary way of configuring a node is via this file. This template lists

# the most important settings you may want to configure for a production cluster.

#

# Please consult the documentation for further information on configuration options:

# https://www.elastic.co/guide/en/elasticsearch/reference/index.html

#

# ---------------------------------- Cluster -----------------------------------

#

# Use a descriptive name for your cluster:

#

cluster.name: sai-cluster

#

# ------------------------------------ Node ------------------------------------

#

# Use a descriptive name for the node:

#

node.name: sai-node

#

# Add custom attributes to the node:

#

#node.attr.rack: r1

#

# ----------------------------------- Paths ------------------------------------

#

# Path to directory where to store the data (separate multiple locations by comma):

#

path.data: /var/lib/elasticsearch

#

# Path to log files:

#

path.logs: /var/log/elasticsearch

#

# ----------------------------------- Memory -----------------------------------

#

# Lock the memory on startup:

#

#bootstrap.memory\_lock: true

#

# Make sure that the heap size is set to about half the memory available

# on the system and that the owner of the process is allowed to use this

# limit.

#

# Elasticsearch performs poorly when the system is swapping the memory.

#

# ---------------------------------- Network -----------------------------------

#

# By default Elasticsearch is only accessible on localhost. Set a different

# address here to expose this node on the network:

#

network.host: 0.0.0.0

#

# 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]"]

#

#discovery.seed\_hosts: ["host1", "host2"]

#

# Bootstrap the cluster using an initial set of master-eligible nodes:

#

#cluster.initial\_master\_nodes: ["node-1", "node-2"]

#

# For more information, consult the discovery and cluster formation module documentation.

#

# ---------------------------------- Various -----------------------------------

#

# Require explicit names when deleting indices:

#

#action.destructive\_requires\_name: true

#

# ---------------------------------- Security ----------------------------------

#

discovery.type: single-node

xpack.security.enabled: true

xpack.security.authc.api\_key.enabled: true

xpack.monitoring.enabled: true

# \*\*\* WARNING \*\*\*

#

# Elasticsearch security features are not enabled by default.

# These features are free, but require configuration changes to enable them.

# This means that users don’t have to provide credentials and can get full access

# to the cluster. Network connections are also not encrypted.

#

# To protect your data, we strongly encourage you to enable the Elasticsearch security features.

# Refer to the following documentation for instructions.

#

# <https://www.elastic.co/guide/en/elasticsearch/reference/7.16/configuring-stack-security.html>

Edit thekibana.yml like below:-

Location:=/etc/kibana/kibana.yml

# Kibana is served by a back end server. This setting specifies the port to use.

server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.

# The default is 'localhost', which usually means remote machines will not be able to connect.

# To allow connections from remote users, set this parameter to a non-loopback address.

server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.

# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath

# from requests it receives, and to prevent a deprecation warning at startup.

# This setting cannot end in a slash.

#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with

# `server.basePath` or require that they are rewritten by your reverse proxy.

# This setting was effectively always `false` before Kibana 6.3 and will

# default to `true` starting in Kibana 7.0.

#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If

# `server.basePath` is configured this URL should end with the same basePath.

server.publicBaseUrl: "http://172.31.44.9:5601/"

# The maximum payload size in bytes for incoming server requests.

#server.maxPayload: 1048576

# The Kibana server's name. This is used for display purposes.

server.name: "demo-kibana"

# The URLs of the Elasticsearch instances to use for all your queries.

elasticsearch.hosts: ["http://localhost:9200"]

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and

# dashboards. Kibana creates a new index if the index doesn't already exist.

#kibana.index: ".kibana"

# The default application to load.

#kibana.defaultAppId: "home"

# If your Elasticsearch is protected with basic authentication, these settings provide

# the username and password that the Kibana server uses to perform maintenance on the Kibana

# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which

# is proxied through the Kibana server.

#elasticsearch.username: "kibana\_system"

#elasticsearch.password: "elastic123"

# Kibana can also authenticate to Elasticsearch via "service account tokens".

# If may use this token instead of a username/password.

# elasticsearch.serviceAccountToken: "my\_token"

# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.

# These settings enable SSL for outgoing requests from the Kibana server to the browser.

#server.ssl.enabled: false

#server.ssl.certificate: /path/to/your/server.crt

#server.ssl.key: /path/to/your/server.key

# Optional settings that provide the paths to the PEM-format SSL certificate and key files.

# These files are used to verify the identity of Kibana to Elasticsearch and are required when

# xpack.security.http.ssl.client\_authentication in Elasticsearch is set to required.

#elasticsearch.ssl.certificate: /path/to/your/client.crt

#elasticsearch.ssl.key: /path/to/your/client.key

# Optional setting that enables you to specify a path to the PEM file for the certificate

# authority for your Elasticsearch instance.

#elasticsearch.ssl.certificateAuthorities: [ "/path/to/your/CA.pem" ]

# To disregard the validity of SSL certificates, change this setting's value to 'none'.

#elasticsearch.ssl.verificationMode: full

# Time in milliseconds to wait for Elasticsearch to respond to pings. Defaults to the value of

# the elasticsearch.requestTimeout setting.

#elasticsearch.pingTimeout: 1500

# Time in milliseconds to wait for responses from the back end or Elasticsearch. This value

# must be a positive integer.

#elasticsearch.requestTimeout: 30000

# List of Kibana client-side headers to send to Elasticsearch. To send \*no\* client-side

# headers, set this value to [] (an empty list).

#elasticsearch.requestHeadersWhitelist: [ authorization ]

# Header names and values that are sent to Elasticsearch. Any custom headers cannot be overwritten

# by client-side headers, regardless of the elasticsearch.requestHeadersWhitelist configuration.

#elasticsearch.customHeaders: {}

# Time in milliseconds for Elasticsearch to wait for responses from shards. Set to 0 to disable.

#elasticsearch.shardTimeout: 30000

# Logs queries sent to Elasticsearch. Requires logging.verbose set to true.

#elasticsearch.logQueries: false

# Specifies the path where Kibana creates the process ID file.

#pid.file: /run/kibana/kibana.pid

# Enables you to specify a file where Kibana stores log output.

#logging.dest: stdout

# Set the value of this setting to true to suppress all logging output.

#logging.silent: false

# Set the value of this setting to true to suppress all logging output other than error messages.

#logging.quiet: false

# Set the value of this setting to true to log all events, including system usage information

# and all requests.

#logging.verbose: false

# Set the interval in milliseconds to sample system and process performance

# metrics. Minimum is 100ms. Defaults to 5000.

#ops.interval: 5000

# Specifies locale to be used for all localizable strings, dates and number formats.

# Supported languages are the following: English - en , by default , Chinese - zh-CN .

#i18n.locale: "en"

systemctl enable elasticsearch

systemctl start elasticsearch

systemctl start kibana

systemctl enable kibana

**give the security credentials to elastic and kibana pages:**

put the below commands on the down of the elasticsearch.yml page which is under the keyword is security.

xpack.security.enabled: true

xpack.security.authc.api\_key.enabled: true

xpack:

security:

authc:

realms:

native:

native1:

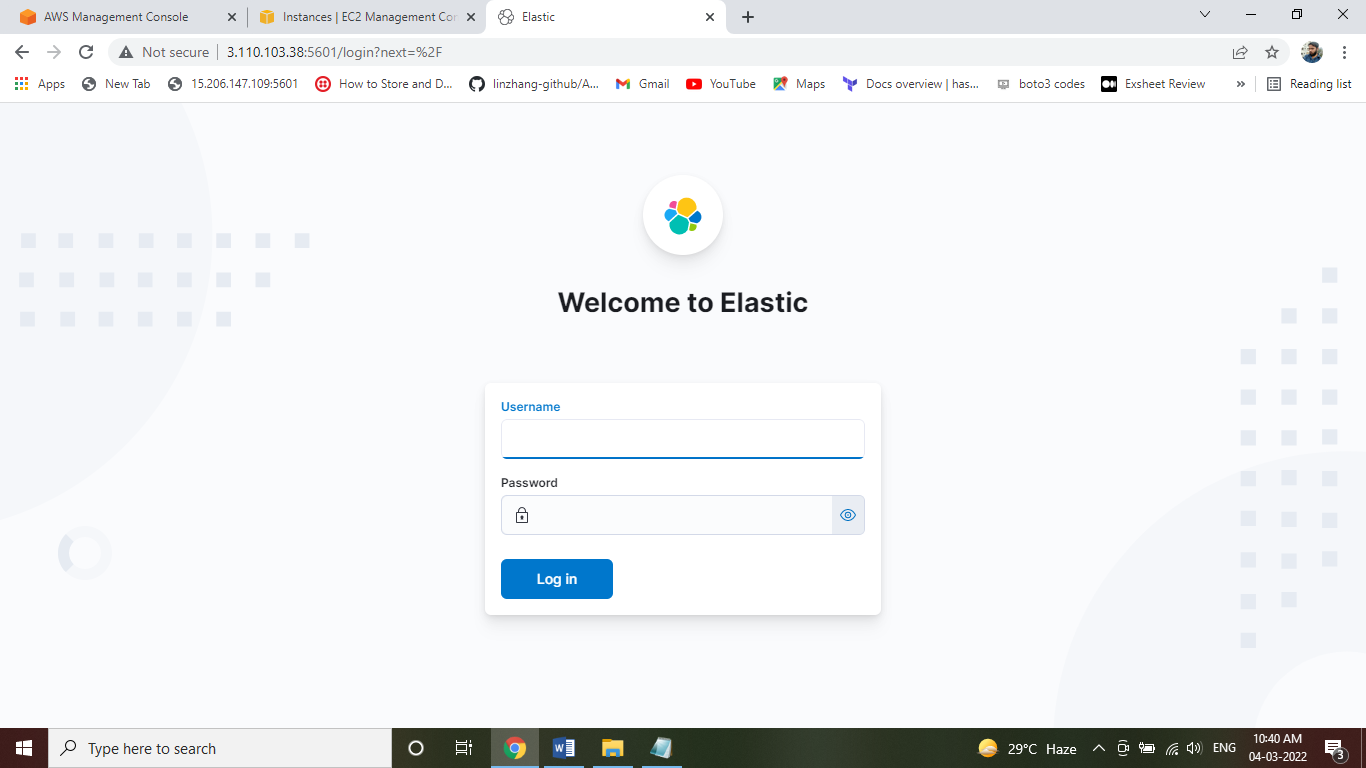
order: 0

after run the below command and set up the security cresentials=

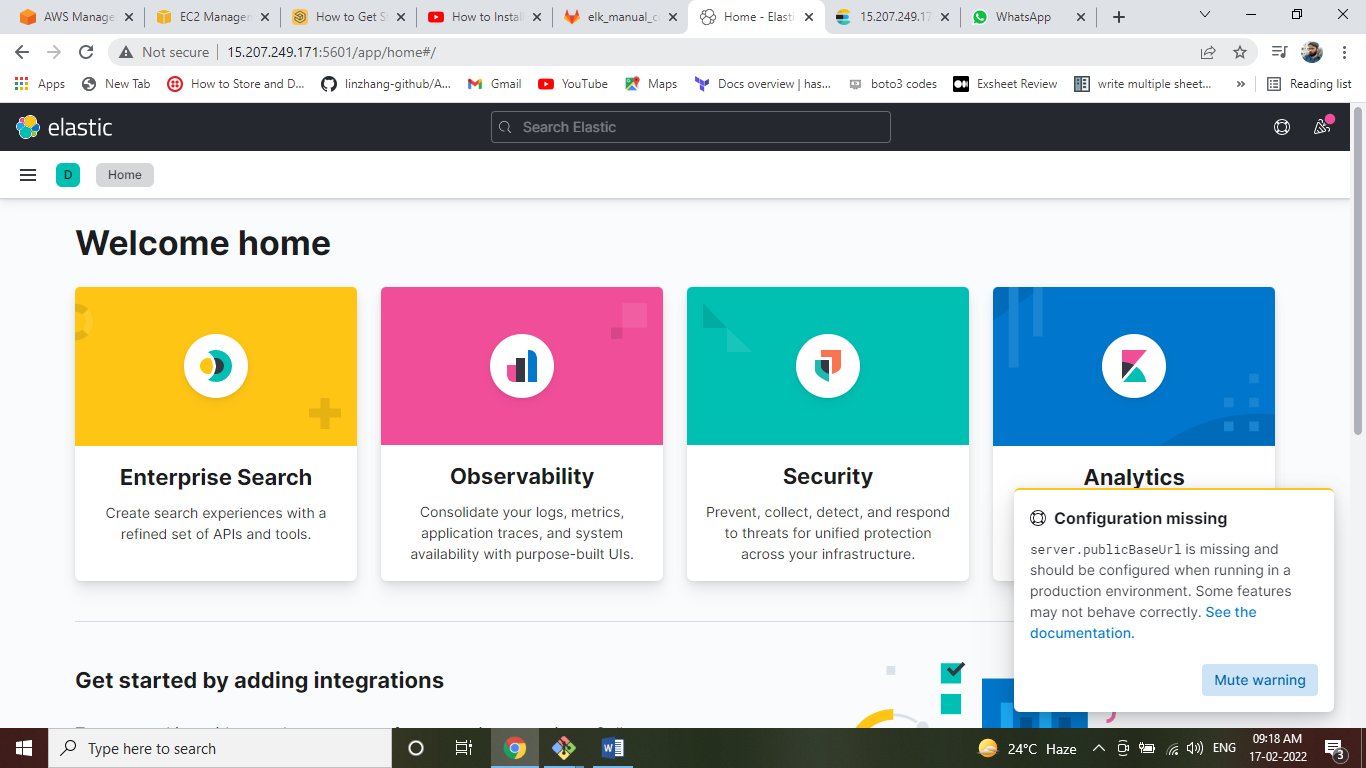
cmd:-/usr/share/elasticsearch/bin/elasticsearch-setup-passwords interactive

note:-if you want to run the above command must and should your elasticsearch and kibana in running state.otherwise is not possible.

Image:-



After login we got home page:



**Setup logstash:**

**Logstash in linux:**

Logstash

---------

rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

vi /etc/yum.repos.d/logstash.repo

[logstash-7.x]

name=Elastic repository for 7.x packages

baseurl=https://artifacts.elastic.co/packages/7.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

yum install logstash -y

systemctl enable logstash.service

systemctl start logstash.service

----------------

finally install java where the logstash is installed

yum install java -y (or)

amazon-linux-extras install java-openjdk11 –y

we have to setup only one file whichis the conf file:

location or path:

vi /etc/elasticsearch/conf.d/sample.conf

edit the below conf file like below:

location of file is:-

----------------------

/etc/logstash/config.d/sample.conf

input {

file {

path => "/var/log/httpd/access\_log"

type => "syslog"

}

file {

path => "/var/log/httpd/error\_log"

type => "syslog"

}

}

filter {

if [type] == "apache-access" {

grok {

match => [ "message", "%{COMBINEDAPACHELOG}" ]

}

}

}

output {

elasticsearch {

hosts => ["private ip of elasticsearch:9200"]

user => "elastic"

password => "elastic123"

index => "apachelog-1"

manage\_template => false

}

}

to configure the conf file to logstash using below command.and if you want to run this cmd you need to install java.

Cmd:-**/usr/share/logstash/bin/logstash –f /etc/logstash/conf.d/sample.conf &**

->access the apache page and refresh the some times.

And go to kibana page.

🡪and go to main left dash board panel

🡪select the management and select the stack management

🡪see the indexes of elasticsearch the index of apache logs has created we have to see here.

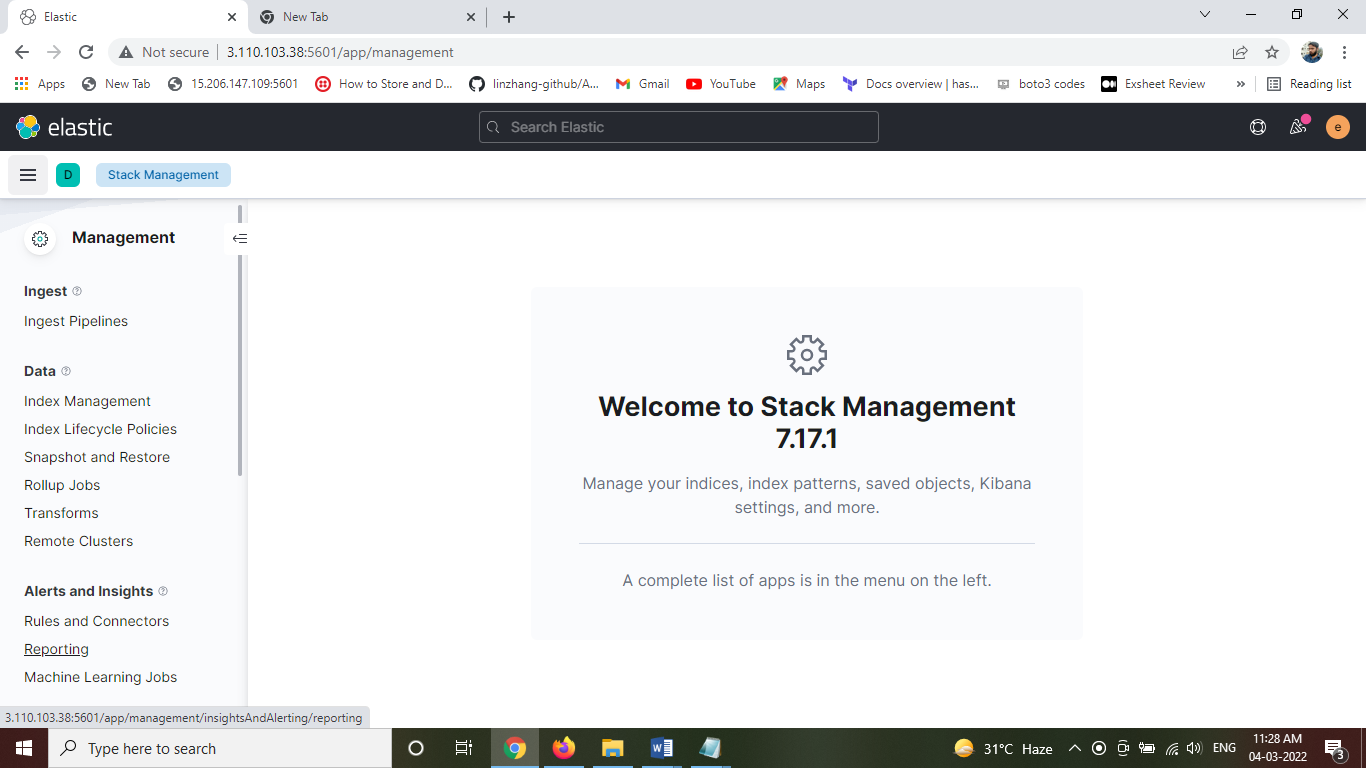
🡪later if you want to monitor the all logs in kibana we have to create index.

🡪In the same path we have to the kibana index using the same name of elasticsearch index name.

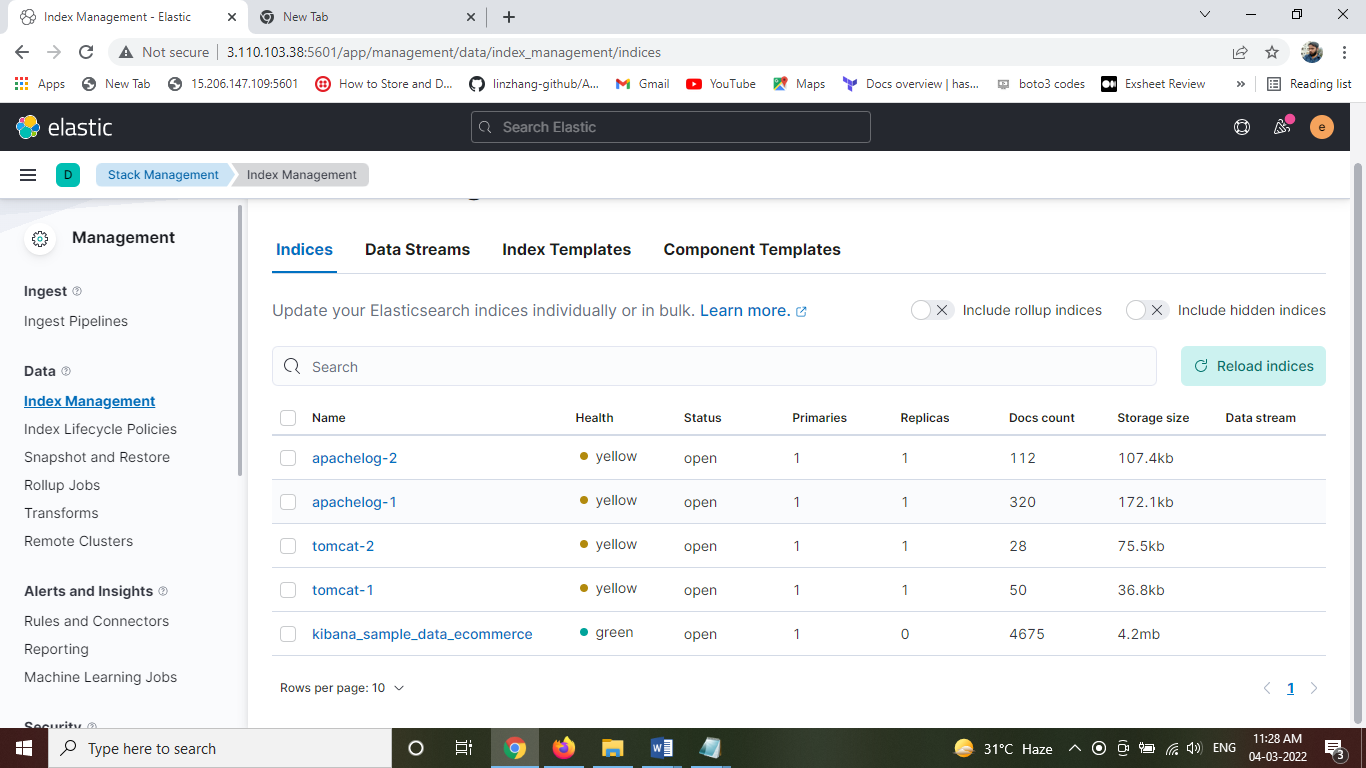
🡪After we have to monitor the all logs in discover panel.

🡪should follow the images.

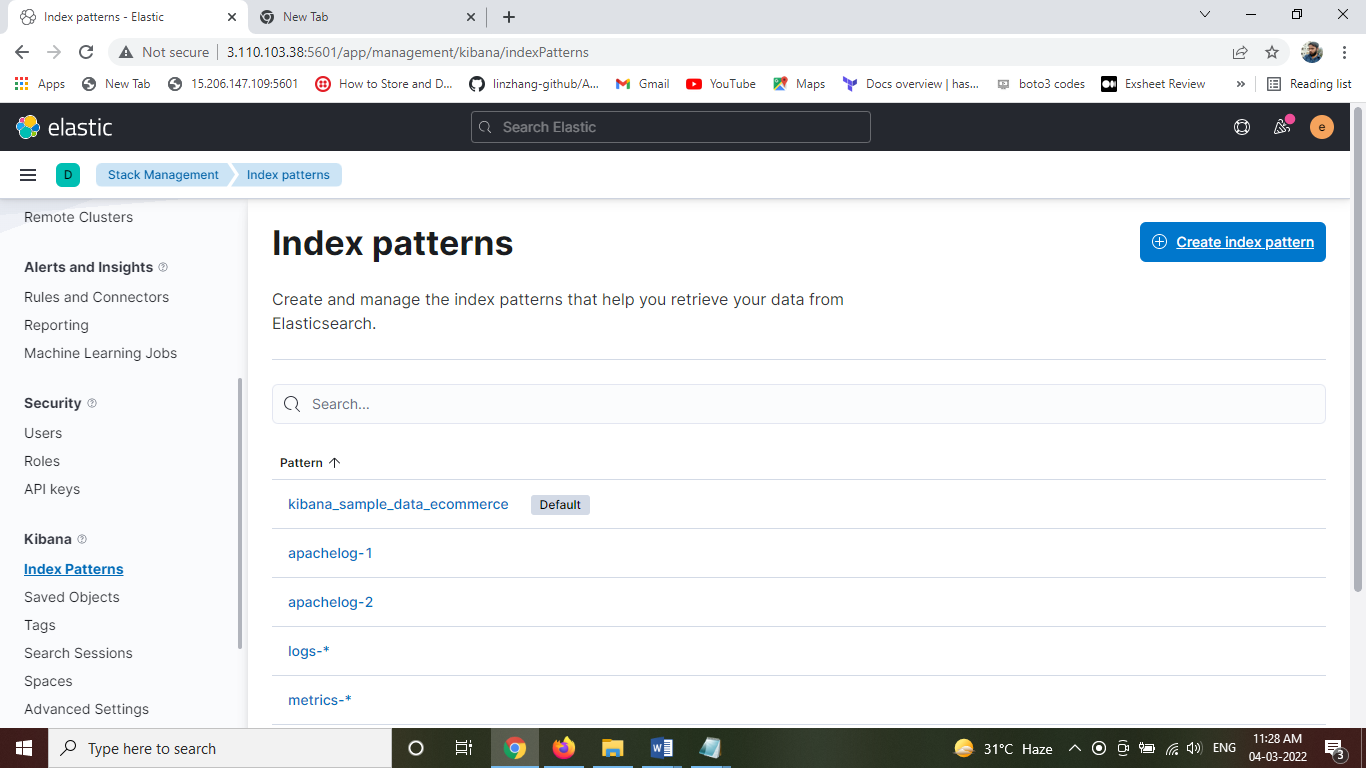
1)



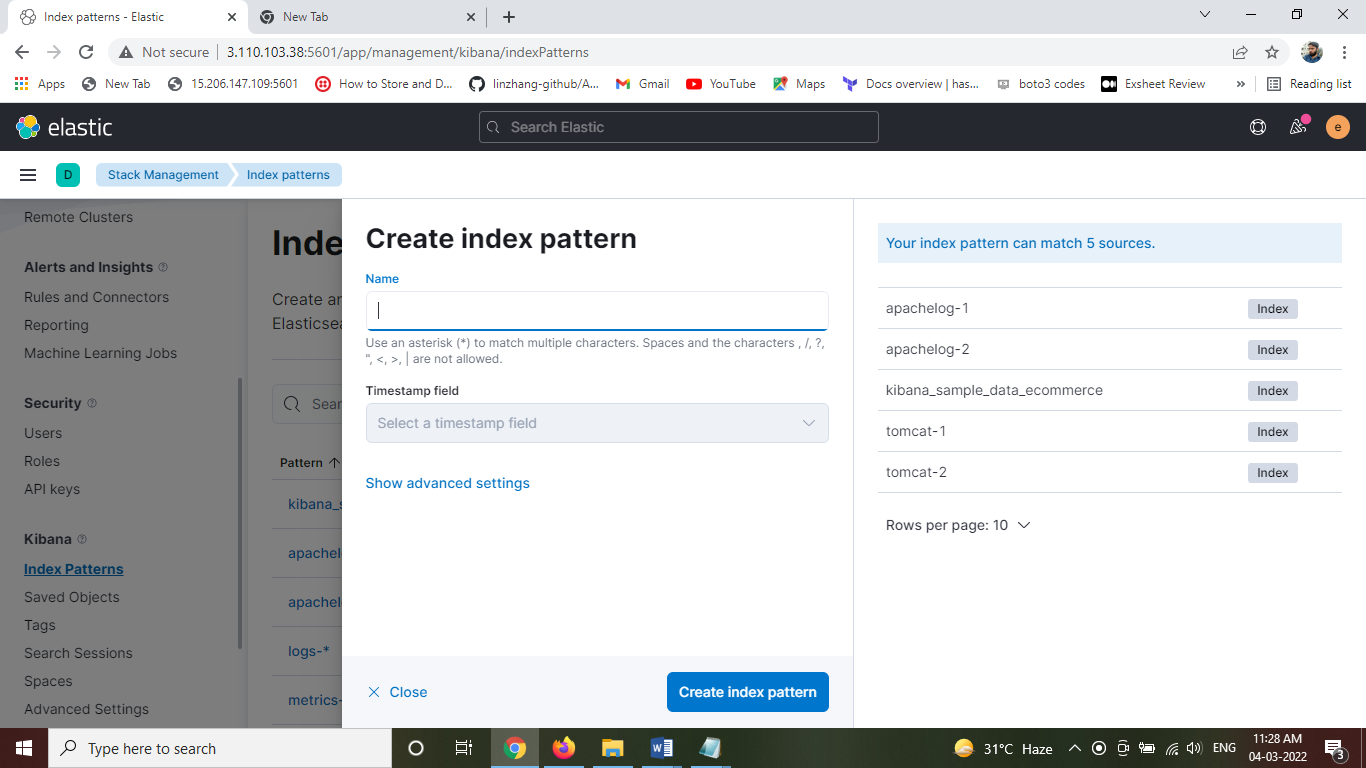
2)



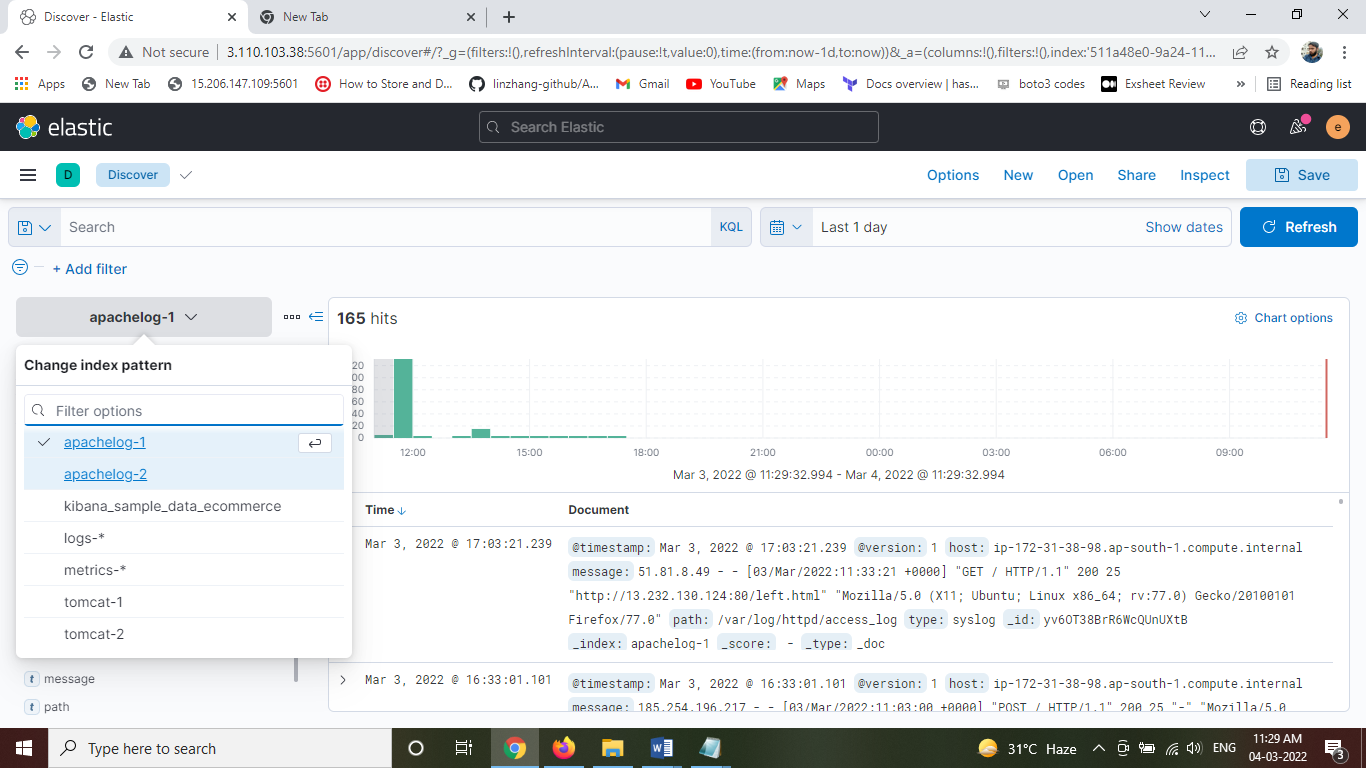
3)



4)



5)



6)

