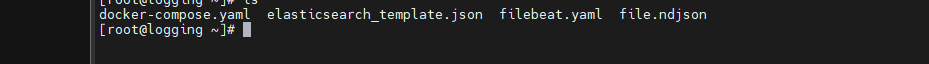
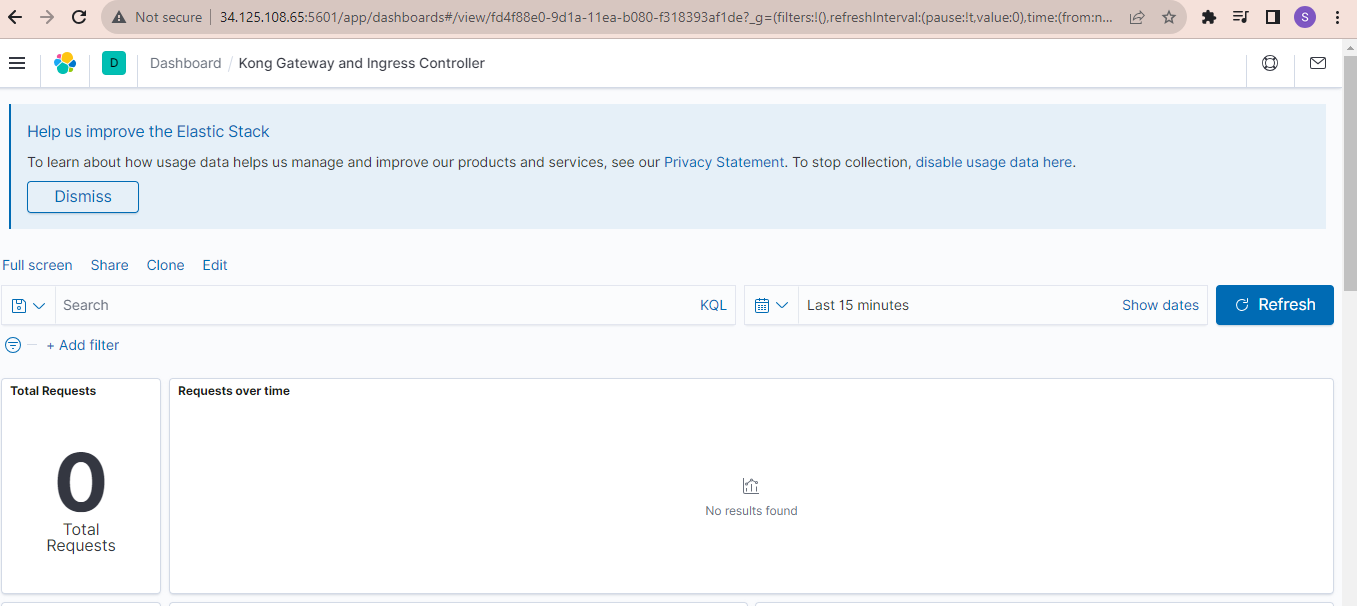
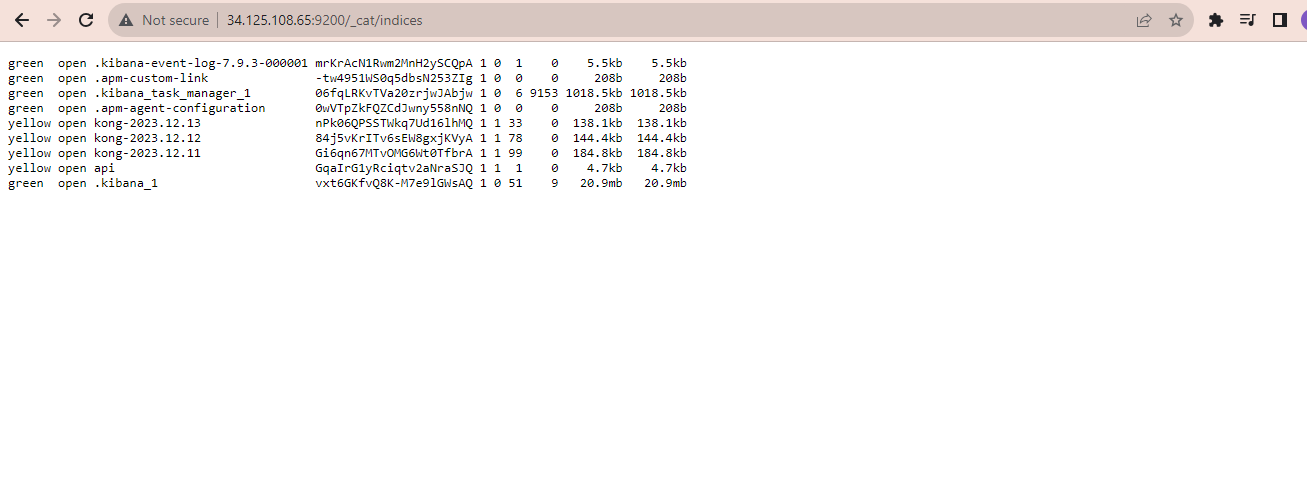
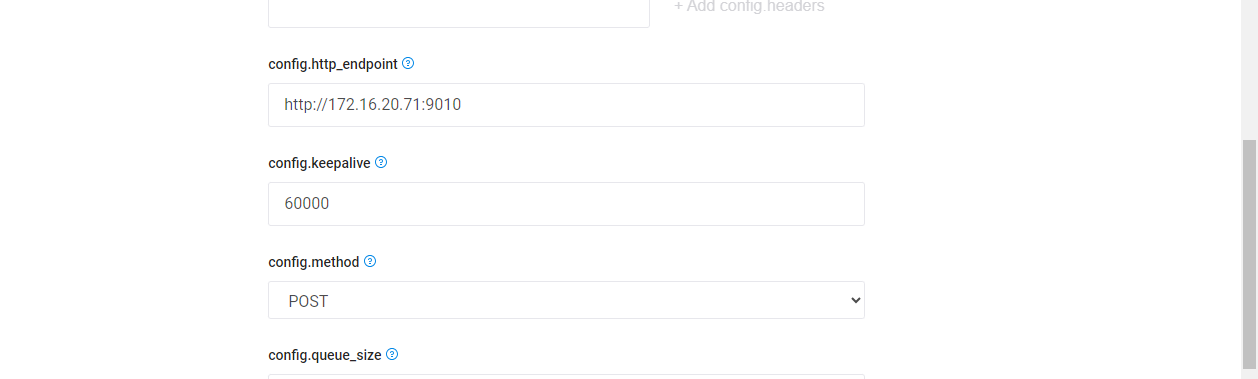
**Setup for elastic search, kibana and filebeat**

* These setup has been done in the redhat os version 8
* Here we installed these setup using docker compose file
* Main requirement for efk setup is u need to install java in the machine
* Commands are given below
* Sudo dnf update
* Sudo dnf install java-11-openjdk-devel
* and then you need to install docker in the redhat os.
* After that you need to install docker compose in redhat os
* Then you can create a docker-compose.yaml file using vi also, create filebeat.yaml file using vi, then create elasticsearch\_template.json using vi and then create ndjson file which we will be using later
* Code for elastic search is given below
* services:
* elasticsearch:
* image: docker.elastic.co/elasticsearch/elasticsearch:7.9.3
* container\_name: elasticsearch
* environment:
* - discovery.type=single-node
* - xpack.security.enabled=false
* - "ES\_JAVA\_OPTS=-Xms256m -Xmx256m"
* ports:
* - 9200:9200
* - 9300:9300
* networks:
* - elastic
* Code for kibana is given below
* kibana:
* image: docker.elastic.co/kibana/kibana:7.9.3
* container\_name: kibana
* depends\_on:
* - elasticsearch
* ports:
* - 5601:5601
* networks:
* - elastic
* Code for filebeat is given below
* filebeat:
* image: docker.elastic.co/beats/filebeat:7.9.3
* container\_name: filebeat
* user: root
* ports:
* - 9010:9010
* depends\_on:
* - elasticsearch
* command: ["--strict.perms=false"]
* volumes:
* - ./filebeat.yaml:/usr/share/filebeat/filebeat.yml
* - ./elasticsearch\_template.json:/usr/share/filebeat/elasticsearch\_template.json
* networks:
* - elastic
* Here filebeat.yaml is created in root folder itself and elasticsearch\_template.json is also in the root folder itself
* If your receiving the logs from any other services then only use httpendpoint in the filebeat.yaml otherwise we can use the type as log to collect the data.
* Please do not miss any indentation in filebeat.yaml it will give error
* After file creation u can do docker compose up -d
* Then u can check given below endpoints
* <http://localhost:9200> for elastic search
* <http://localhost:9010> for filebeat
* <http://localhost:5601> for kibana
* File.ndjson should be in the same directory where you have all the docker related files other wont be able to see the dashboard
* 
* 
* 
* 
* Above url should show kong in the dashboard otherwise it will be loop into problem
* The dashboard is only visible only when you upload ndjson file below is the url how you need to hit the endpoint
* File.ndjson file should be present in the server where you have docker compose file then you can hit the below endpoint
* curl -X POST api/saved\_objects/\_import -H "kbn-xsrf: true" --form file=@file.ndjson
* It has to be like <http://localhost:5601/api/saved_objects/_import> -H “kbn-xsrf:true” –form file=@file.ndjson
* These are brief steps for efk installation.
* Mainly you need to install http-log plugin for the service and add below end point
* 
* These helps you to see the logs.