**Install docker**

**Install Docker Compose**

sudo curl -L "<https://github.com/docker/compose/releases/latest/download/docker-compose-$(uname> -s)-$(uname -m)" -o /usr/local/bin/docker-compose

sudo chmod +x /usr/local/bin/docker-compose

docker-compose –version

**docker-compose.yml**

version: '3'

services:

nginx:

image: nginx

ports:

- "80:80"

volumes:

- ./nginx/logs:/var/log/nginx

networks:

- elastic

elasticsearch:

image: docker.elastic.co/elasticsearch/elasticsearch:7.10.0

environment:

- discovery.type=single-node

ports:

- "9200:9200"

networks:

- elastic

filebeat:

image: docker.elastic.co/beats/filebeat:7.10.0

volumes:

- /home/sigmoid/filebeat/filebeat.yml:/usr/share/filebeat/filebeat.yml

- ./nginx/logs:/var/log/nginx

networks:

- elastic

kibana:

image: docker.elastic.co/kibana/kibana:7.10.0

environment:

ELASTICSEARCH\_URL: http://elasticsearch:9200

ports:

- "5601:5601"

networks:

- elastic

networks:

elastic:

**mkdir filebeat**

**cd filebeat**

**nano filebeat.yml**

Only creator should have writable permissions to filebeat.yml

**filebeat.yml**

filebeat.inputs:

- type: log

paths:

- /var/log/nginx/\*.log # Adjust the path accordingly

fields:

log\_type: nginx

fields\_under\_root: true

output.elasticsearch:

hosts: ["elasticsearch:9200"]

setup.template.name: "nginx\_logs"

setup.template.pattern: "nginx\_logs-\*"

setup.kibana:

host: "kibana:5601"

Run stack**: sudo docker-compose up -d**

**sudo ufw allow 80/tcp**

**sudo ufw allow 5601/tcp**

**sudo ufw allow 9200/tcp**

<http://localhost/>

<http://localhost:5601/>

**Create Index Pattern in Kibana:**

* Go to Kibana > Management > Stack Management > Index Patterns.
* Click on "Create index pattern.”
* Enter the pattern you specified in setup.template.pattern (e.g., "nginx\_logs-\*").
* Select @timestamp
* Follow the steps to create the index pattern.

**Explore Nginx Logs in Kibana:**

* Once the index pattern is created, go to "Discover" in Kibana.
* Select the newly created index pattern from the top right.
* You should see Nginx logs in the Discover tab.