Elasticsearch-Filebeat-Kibana Stack to Monitor Nginx Logs

- **Nginx** logs are written to a local volume.
- **Filebeat** reads the Nginx access and error logs from the local volume and forwards them to **Elasticsearch**.
- **Kibana** visualizes the Nginx logs using an Elasticsearch index (e.g., `filebeat-*`).

Steps to Build the EFK

1. **Create Docker Compose File**
    - Create docker-compose.yml defines all services required for the project.
    - In the `docker-compose.yml`, define services such as Nginx, Elasticsearch, Filebeat, and Kibana, each specifying its image, container settings, ports, and volumes.
    - Use Docker's `networks` feature to create a bridge network (e.g., `efk`), enabling communication between the Nginx, Filebeat, Elasticsearch, and Kibana containers.

```yaml
version: '3'
services:
  nginx:
    image: nginx:latest
    volumes:
      - ./nginx/log:/var/log/nginx
    ports:
      - "80:80"

  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:7.9.3
    environment:
      - discovery.type=single-node
    ports:
      - "9200:9200"
    volumes:
      - es_data:/usr/share/elasticsearch/data

  kibana:
    image: docker.elastic.co/kibana/kibana:7.9.3
    ports:
      - "5601:5601"
    environment:
      ELASTICSEARCH_HOSTS: "http://elasticsearch:9200"

  filebeat:
    image: docker.elastic.co/beats/filebeat:7.9.3
    volumes:
      - ./filebeat.yml:/usr/share/filebeat/filebeat.yml
      - ./nginx/log:/var/log/nginx
    environment:
      ELASTICSEARCH_HOSTS: "http://elasticsearch:9200"
      SETUP_KIBANA_HOST: "http://kibana:5601"
volumes:
  es_data:
```

2. **Configure Filebeat**
   - **Filebeat** reads the logs from Nginx and sends them to Elasticsearch.
   - Create filebeat.yml file

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /var/log/nginx/access.log
    - /var/log/nginx/error.log

output.elasticsearch:
  hosts: ["http://elasticsearch:9200"]
setup.kibana:
  host: "http://kibana:5601"
```

3. **Build and Run**

Now that everything is set up, you can use Docker Compose to start the stack.

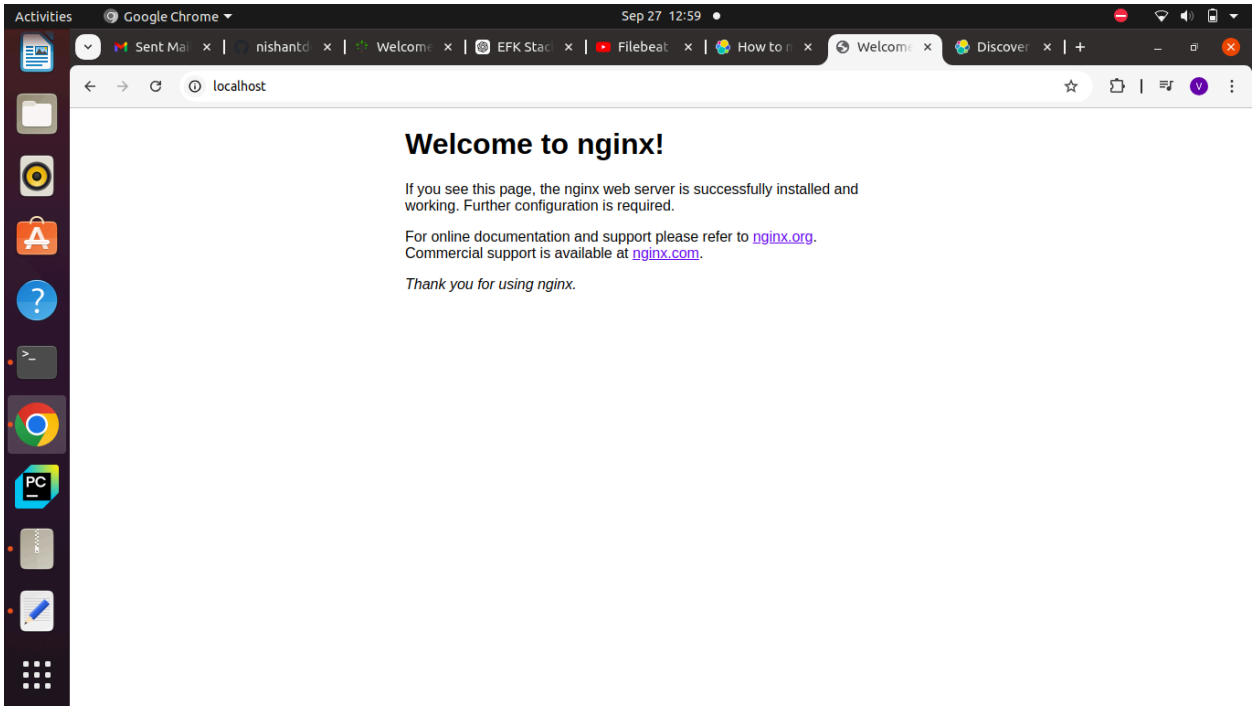
Navigate to the project directory (efk-nginx-monitoring/).

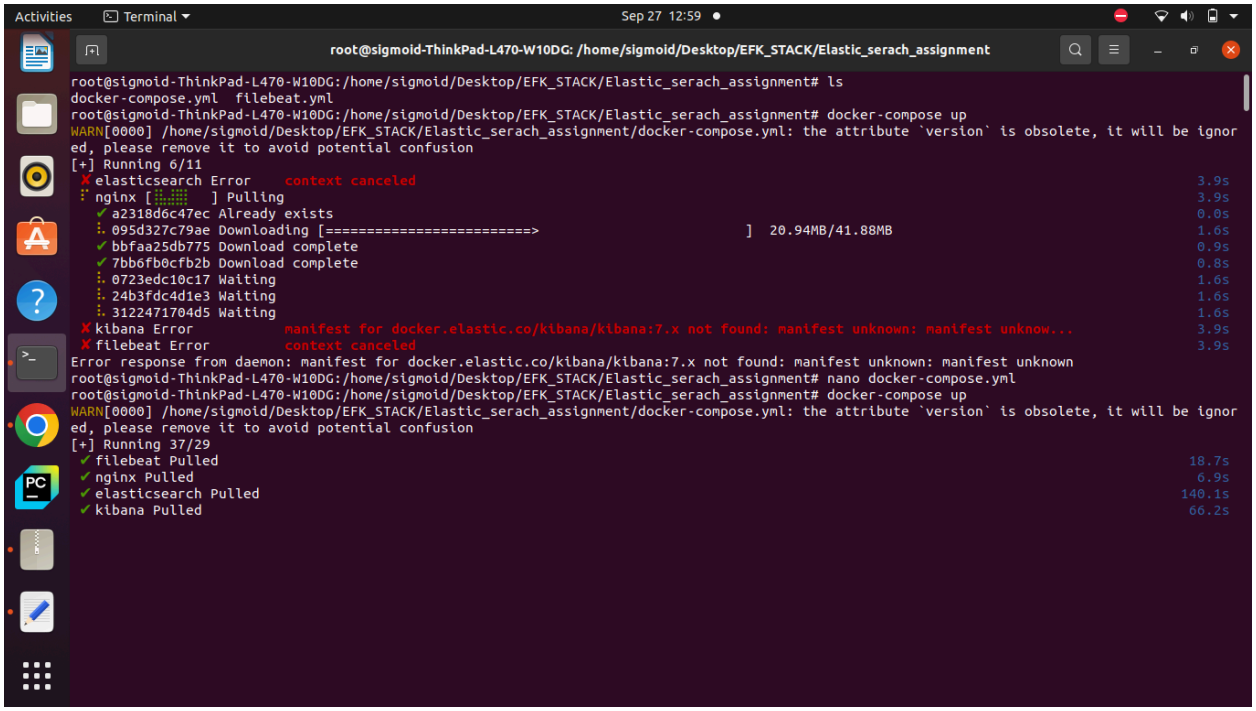
Run the following command to start the services:

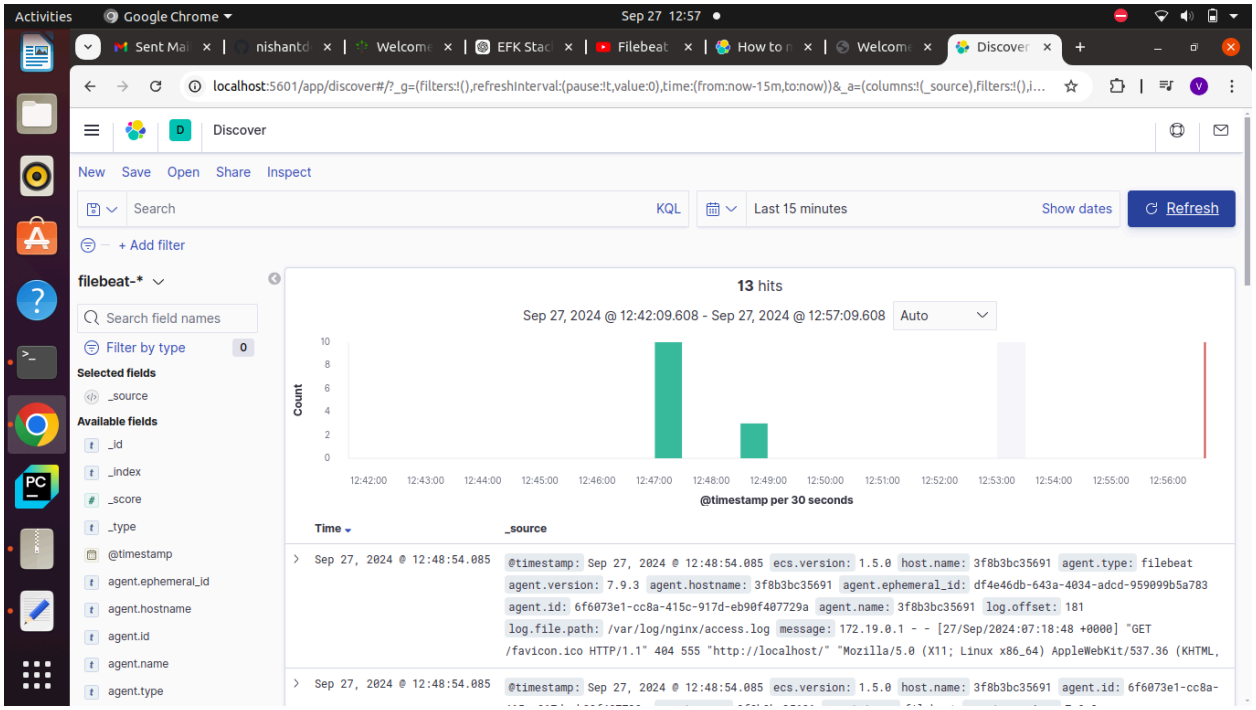
docker-compose up -d

4. **Build and start the Nginx, Elasticsearch, Kibana, and Filebeat containers.**
5. **Map the Nginx logs to the host system so Filebeat can access them.**
6. **Access Kibana to Visualize Logs**
   - To view the logs being collected:
     - Open Kibana by navigating to http://localhost:5601 in your browser.
     - In the Kibana dashboard, choose "Explore your own data". Kibana will automatically detect the filebeat-* index pattern (created by Filebeat in Elasticsearch).
     - Visualize your Nginx logs by creating custom dashboards or using pre-built Filebeat dashboards in Kibana.

OUTPUT:


Activities
Google Chrome
Sep 27 12:59
localhost
Welcome to nginx!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.


Activities
Terminal
Sep 27 12:59
root@sigmoid-ThinkPad-L470-W10DG: /home/sigmoid/Desktop/EFK_STACK/Elastic_serach_assignment
root@sigmoid-ThinkPad-L470-W10DG:/home/sigmoid/Desktop/EFK_STACK/Elastic_serach_assignment# ls
docker-compose.yml filebeat.yml
root@sigmoid-ThinkPad-L470-W10DG:/home/sigmoid/Desktop/EFK_STACK/Elastic_serach_assignment# docker-compose up
WARN[0000] /home/sigmoid/Desktop/EFK_STACK/Elastic_serach_assignment/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Running 6/11
✘ elasticsearch Error context canceled 3.9s
⠏ nginx [⣿⣿⣿] Pulling 3.9s
✔ a2318d6c47ec Already exists 0.0s
⠙ 095d327c79ae Downloading [==========>] 20.94MB/41.88MB 1.6s
✔ bbfaa25db775 Download complete 0.9s
✔ 7bb6fb0cfb2b Download complete 0.8s
⠙ 0723edc10c17 Waiting 1.6s
⠙ 24b3fdc4d1e3 Waiting 1.6s
⠙ 3122471704d5 Waiting 1.6s
✘ kibana Error manifest for docker.elastic.co/kibana/kibana:7.x not found: manifest unknown: manifest unknow... 3.9s
✘ filebeat Error context canceled 3.9s
Error response from daemon: manifest for docker.elastic.co/kibana/kibana:7.x not found: manifest unknown: manifest unknown
root@sigmoid-ThinkPad-L470-W10DG:/home/sigmoid/Desktop/EFK_STACK/Elastic_serach_assignment# nano docker-compose.yml
root@sigmoid-ThinkPad-L470-W10DG:/home/sigmoid/Desktop/EFK_STACK/Elastic_serach_assignment# docker-compose up
WARN[0000] /home/sigmoid/Desktop/EFK_STACK/Elastic_serach_assignment/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Running 37/29
✔ filebeat Pulled 18.7s
✔ nginx Pulled 6.9s
✔ elasticsearch Pulled 140.1s
✔ kibana Pulled 66.2s


Activities
Google Chrome
Sep 27 12:57
Discover
localhost:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(_source),filters:!(),i...
New
Save
Open
Share
Inspect
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
filebeat-*
Search field names
Filter by type
0
Selected fields
_source
Available fields
_id
_index
_score
_type
@timestamp
agent.ephemeral_id
agent.hostname
agent.id
agent.name
agent.type
13 hits
Sep 27, 2024 @ 12:42:09.608 - Sep 27, 2024 @ 12:57:09.608
Auto
Count
@timestamp per 30 seconds
Time
_source
Sep 27, 2024 @ 12:48:54.085
@timestamp: Sep 27, 2024 @ 12:48:54.085 ecs.version: 1.5.0 host.name: 3f8b3bc35691 agent.type: filebeat agent.version: 7.9.3 agent.hostname: 3f8b3bc35691 agent.ephemeral_id: df4e46db-643a-4034-adcd-959099b5a783 agent.id: 6f6073e1-cc8a-415c-917d-eb90f407729a agent.name: 3f8b3bc35691 log.offset: 181 log.file.path: /var/log/nginx/access.log message: 172.19.0.1 - - [27/Sep/2024:07:18:48 +0000] "GET /favicon.ico HTTP/1.1" 404 555 "http://localhost/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
Sep 27, 2024 @ 12:48:54.085
@timestamp: Sep 27, 2024 @ 12:48:54.085 ecs.version: 1.5.0 host.name: 3f8b3bc35691 agent.id: 6f6073e1-cc8a-