Elasticsearch-Filebeat-Kibana stack to monitor Nginx logs

Contents
- Nginx: containing build image nginx web server
- Elasticsearch: containing build image and configuration for Elasticsearch
- Filebeat: containing build image and configuration for Filebeat to stream nginx logs Elasticsearch
- Kibana: containing build image and configure for Kibana to visualize data from an Elasticsearch index

How it works

- Nginx access and error logs are written to a directory. The directory is mapped to a local volume.
- Filebeat reads the nginx logs from the local volume and sends it to an Elasticsearch index [filebeat-*].
- Kibana uses the index to visualize the access and the error logs.

How to run it

Pre-requisites
```bash
- docker
- docker-compose
```

To run this stack, run the following command

```bash
docker-compose up -d
```

Accessing the components :

nginx : `http://localhost`

Kibana : `http://localhost:5601`

Kibana credentials :
- Username: elastic
- Password: changeme%

Directory structure:

```
nginx-elk-stack/
├── docker-compose.yml
├── filebeat/
│   └── filebeat.yml
└── nginx/
    └── nginx.conf
```

docker-compose.yml

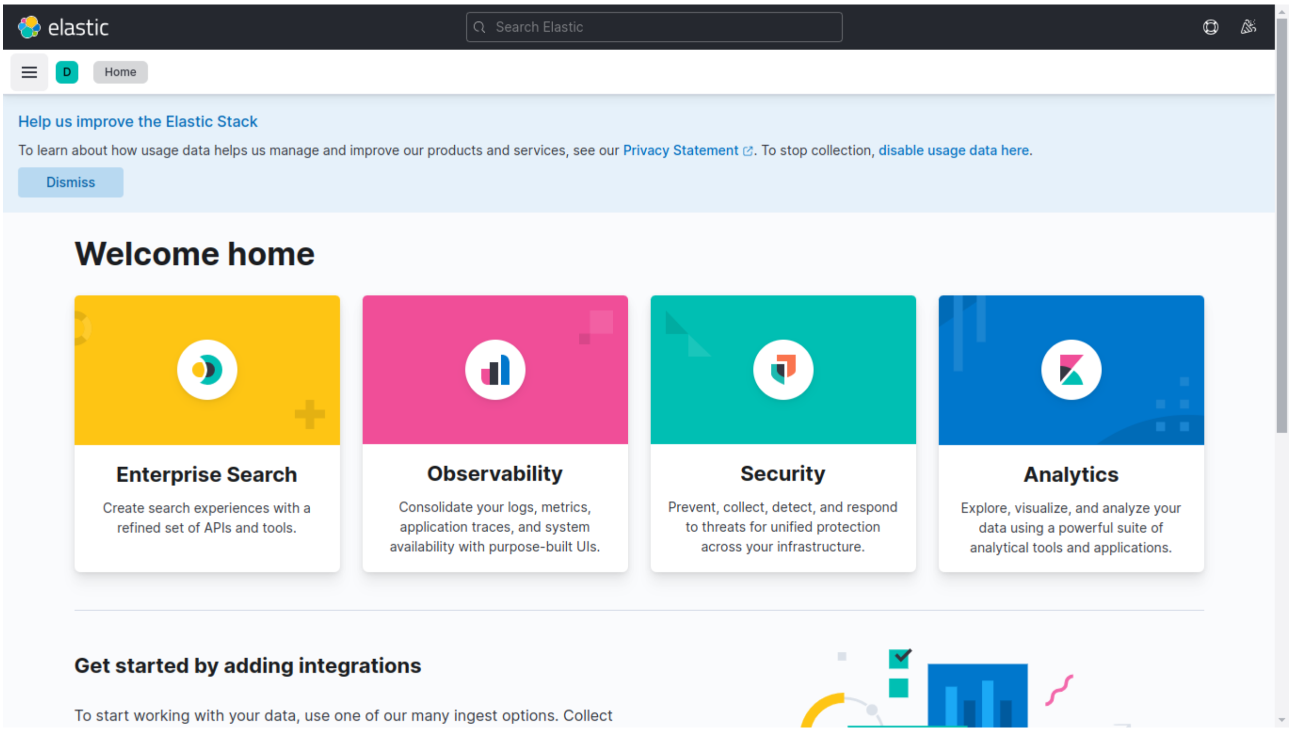
```
version: '3.8'  # Remove this line if you get a warning about obsolescence

services:
  nginx:
    image: nginx:latest
    volumes:
      - ./nginx:/var/log/nginx
    ports:
      - "8080:80"

  elasticsearch:
    image: elasticsearch:7.17.0
    environment:
      - discovery.type=single-node
      - ELASTIC_PASSWORD=changeme%
    volumes:
      - esdata:/usr/share/elasticsearch/data
    ports:
      - "9200:9200"

  filebeat:
    image: docker.elastic.co/beats/filebeat:7.17.0
    volumes:
      - ./filebeat/filebeat.yml:/usr/share/filebeat/filebeat.yml
      - ./nginx:/var/log/nginx
    depends_on:
      - elasticsearch

  kibana:
    image: kibana:7.17.0
    environment:
      - ELASTICSEARCH_HOSTS=http://elasticsearch:9200
      - ELASTICSEARCH_USERNAME=elastic
      - ELASTICSEARCH_PASSWORD=changeme%
    ports:
      - "5601:5601"

volumes:
  esdata:
```

nginx/nginx.conf

```
server {
    listen 80;
    server_name localhost;

    location / {
        root /usr/share/nginx/html;
        index index.html index.htm;
    }

    access_log /var/log/nginx/access.log;
    error_log /var/log/nginx/error.log;
}
```

filebeat/filebeat.yml

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

output.elasticsearch:
  hosts: ["elasticsearch:9200"]
  username: "elastic"
  password: "changeme%"
```



Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Welcome home

Enterprise Search

Create search experiences with a refined set of APIs and tools.

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

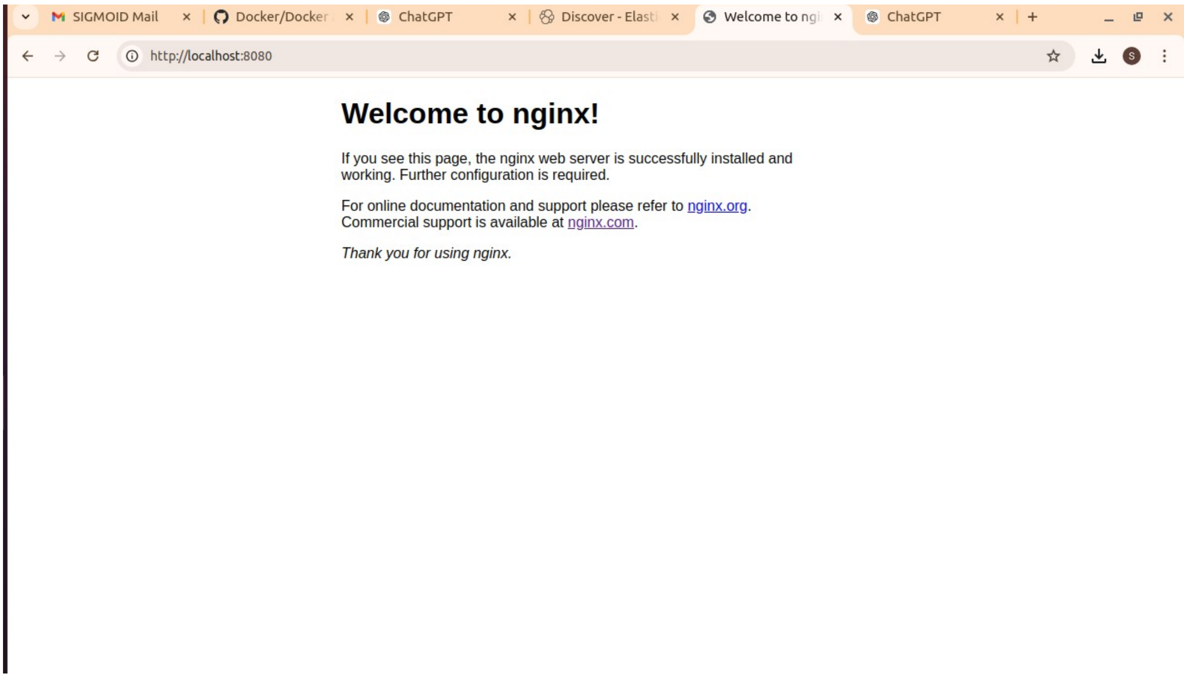
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect



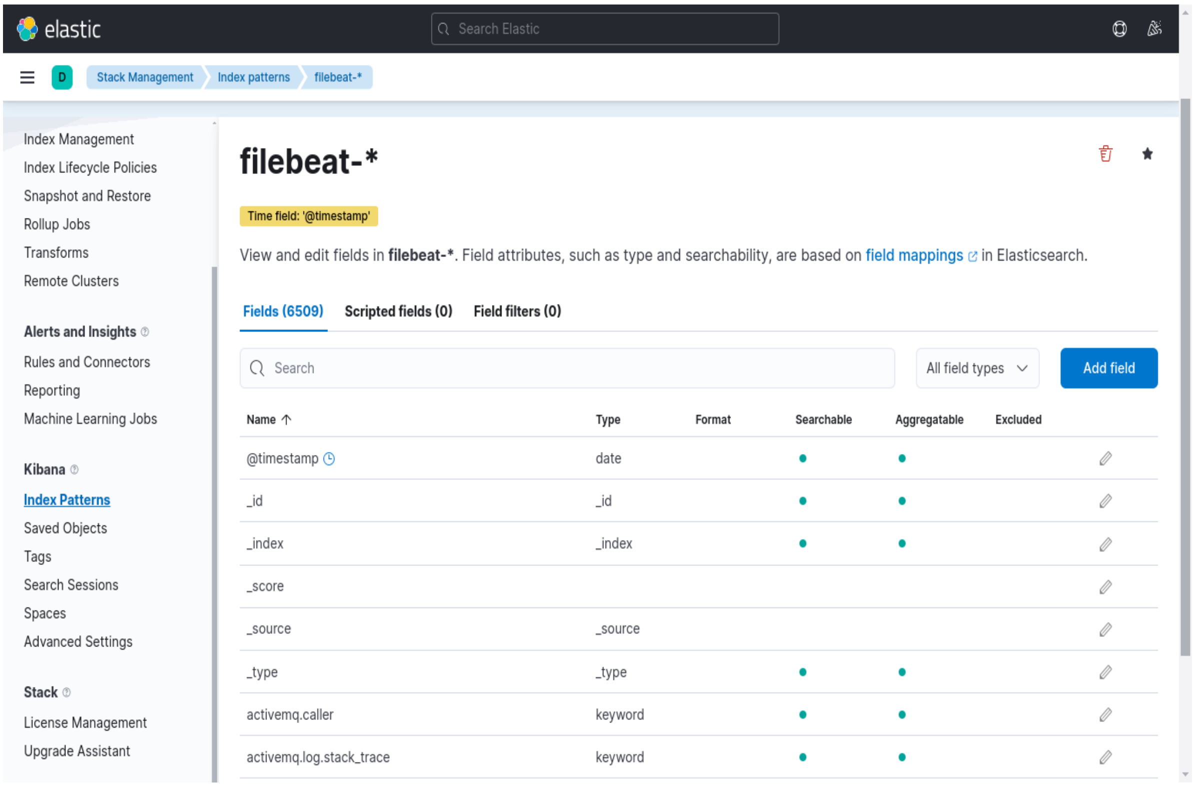
http://localhost:8080

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.

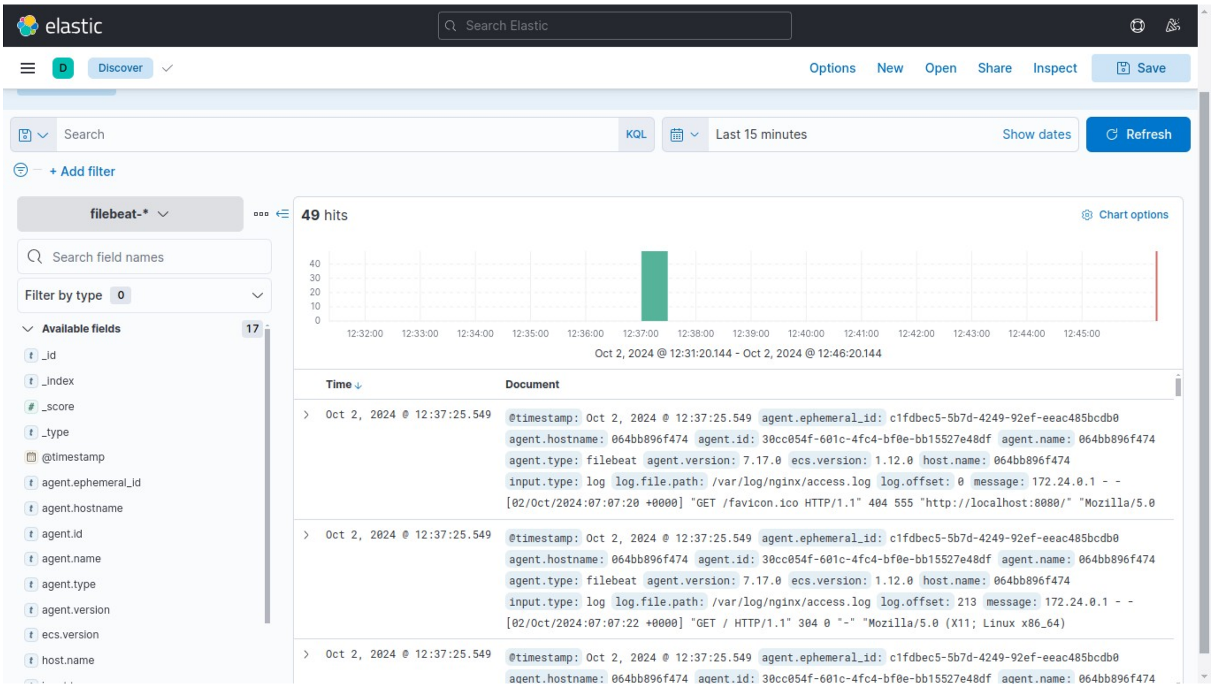


filebeat-*

Time field: '@timestamp'

View and edit fields in **filebeat-***. Field attributes, such as type and searchability, are based on field mappings in Elasticsearch.

Name ↑	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	
_id	_id		●	●	
_index	_index		●	●	
_score					
_source	_source				
_type	_type		●	●	
activemq.caller	keyword		●	●	
activemq.log.stack_trace	keyword		●	●	



```
Oct 2, 2024 @ 12:37:25.549  @timestamp: Oct 2, 2024 @ 12:37:25.549 agent.ephemeral_id: c1fdbec5-5b7d-4249-92ef-eeac485bcdb0
                            agent.hostname: 064bb896f474 agent.id: 30cc054f-601c-4fc4-bf0e-bb15527e48df agent.name: 064bb896f474
                            agent.type: filebeat agent.version: 7.17.0 ecs.version: 1.12.0 host.name: 064bb896f474
                            input.type: log log.file.path: /var/log/nginx/access.log log.offset: 0 message: 172.24.0.1 - -
                            [02/Oct/2024:07:07:20 +0000] "GET /favicon.ico HTTP/1.1" 404 555 "http://localhost:8080/" "Mozilla/5.0

Oct 2, 2024 @ 12:37:25.549  @timestamp: Oct 2, 2024 @ 12:37:25.549 agent.ephemeral_id: c1fdbec5-5b7d-4249-92ef-eeac485bcdb0
                            agent.hostname: 064bb896f474 agent.id: 30cc054f-601c-4fc4-bf0e-bb15527e48df agent.name: 064bb896f474
                            agent.type: filebeat agent.version: 7.17.0 ecs.version: 1.12.0 host.name: 064bb896f474
                            input.type: log log.file.path: /var/log/nginx/access.log log.offset: 213 message: 172.24.0.1 - -
                            [02/Oct/2024:07:07:22 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Linux x86_64)

Oct 2, 2024 @ 12:37:25.549  @timestamp: Oct 2, 2024 @ 12:37:25.549 agent.ephemeral_id: c1fdbec5-5b7d-4249-92ef-eeac485bcdb0
                            agent.hostname: 064bb896f474 agent.id: 30cc054f-601c-4fc4-bf0e-bb15527e48df agent.name: 064bb896f474
```