

# 2022 Filebeat

Local setup:

1. Install:

<https://www.elastic.co/downloads/beats/filebeat>

`tar xzvf filebeat-8.4.3-darwin-x86_64.tar.gz`

2. Edit the filebeat.yml configuration file

3. Start the daemon

Start the daemon by running `sudo ./filebeat -e -c filebeat.yml`

## filestream input



Use the `filestream` input to read lines from active log files. It is the new, improved alternative to the `log` input. It comes with various improvements to the existing input:

## Docker Commands

`docker build -f Dockerfile -t ms/filebeat-fileio:1.0 .`

##Run a container and execute bash without starting filebeat:

`docker run -it --entrypoint=/bin/bash ms/filebeat-fileio:1.0`

Run container:

`docker run -it --name=filebeat-ms ms/filebeat-fileio:1.0`

Run container and remove after it is done:

`docker run -it --rm --name=filebeat-ms ms/filebeat-fileio:1.0 filebeat -e`

Access the container via 'sh' :

```
docker ps -a
```

```
docker exec -it filebeat-ms bash
```

**start apache/filebeat docker**

```
docker-compose -p filebeat -f docker-compose-lab7.yml up
```

**stop apache/filebeat docker and remove containers**

```
docker-compose -p filebeat -f docker-compose-lab7.yml down
```