# This workflow uses actions that are not certified by GitHub.

# They are provided by a third-party and are governed by

# separate terms of service, privacy policy, and support

# documentation.

# A sample workflow which checks out the code, builds a container

# image using Docker and scans that image for vulnerabilities using

# Snyk. The results are then uploaded to GitHub Security Code Scanning

#

# For more examples, including how to limit scans to only high-severity

# issues, monitor images for newly disclosed vulnerabilities in Snyk and

# fail PR checks for new vulnerabilities, see https://github.com/snyk/actions/

name: Build

on:

push:

branches: [ main ]

pull\_request:

# The branches below must be a subset of the branches above

branches: [ main ]

jobs:

Run:

runs-on: ubuntu-latest

steps:

- uses: actions/checkout@v2

- name: Build & Deploy

run: make setup && make up

- name: Test Elasticsearch

run: timeout 240s sh -c "until curl https://elastic:changeme@localhost:9200 --insecure --silent; do echo 'Elasticsearch Not Up, Retrying...'; sleep 3; done" && echo 'Elasticsearch is up'

- name: Test Kibana

run: timeout 240s sh -c "until curl https://localhost:5601 --insecure --silent -I; do echo 'Kibana Not Ready, Retrying...'; sleep 3; done" && echo 'Kibana is up'