Notes

Setting up greylog to monitor server assets in your networks.

Date: 2023-11-12
By: csr13

Download as PDF

For setting graylog a docker-compose.yml file is enough to do the job; check docker and docker compose are installed on the system and then change to the root user, create a folder on /root/graylog

Create docker-compose.yml file and copy paste this then run: $ docker-compose up

```
version: '3'

services:
  mongo:
    image: mongo:5.0.13
    networks:
      - graylog
    volumes:
      - mongo_data:/data/db

  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch-oss:7.10.2
    environment:
    - http.host=0.0.0.0
    - transport.host=localhost
    - network.host=0.0.0.0
    - "ES_JAVA_OPTS=-Dlog4j2.formatMsgNoLookups=true -Xms512m -Xmx512m"
    ulimits:
      memlock:
        soft: -1
        hard: -1
      deploy:
    resources:
          limits:
            memory: 1g
      networks:
        - graylog
      volumes:
    - es_data:/usr/share/elasticsearch/data

  graylog:
    image: graylog/graylog:5.0
    environment:
      - GRAYLOG_PASSWORD_SECRET=logginglogger123
      - GRAYLOG_ROOT_PASSWORD_SHA2=8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918
      - GRAYLOG_HTTP_EXTERNAL_URI=http://127.0.0.1:9000/
    entrypoint: /usr/bin/tini -- wait-for-it elasticsearch:9200 --  /docker-entrypoint.sh
    networks:
      - graylog
    restart: always
    depends_on:
      - mongo
      - elasticsearch
    ports:
  # Graylog web interface and REST API
      - 9000:9000
  # Syslog TCP
      - 1514:1514
  # Syslog UDP
      - 1514:1514/udp
  # GELF TCP
      - 12201:12201
  # GELF UDP
      - 12201:12201/udp
  # TST TCP
      - 5555:5555
    volumes:
      - graylog_data:/usr/share/graylog/data

volumes:
  mongo_data:
    driver: local
  es_data:
    driver: local
  graylog_data:
    driver: local

networks:
  graylog:
    driver: bridge
```

This will expose the application on port 9000, redirect with nginx to port 80 or establish a piped connection to graylog via ssh to your localhost:5000 :

```
ssh -i <pem file> -L 127.0.0.1:5000:127.0.0.1:9000 <user>@<log-server-ip>
```

Default credentials:

```
Username: admin
Password: admin
```