1. Cấu hình Elasticsearch và Kibana trên Docker

version: "3.3"

services:

  elasticsearch:

    image: docker.elastic.co/elasticsearch/elasticsearch:7.4.0

    container\_name: elasticsearch

    restart: always

    environment:

      - xpack.security.enabled=false

      - discovery.type=single-node

    ulimits:

      memlock:

        soft: -1

        hard: -1

      nofile:

        soft: 65536

        hard: 65536

    cap\_add:

      - IPC\_LOCK

    volumes:

      - elasticsearch-data:/usr/share/elasticsearch/data

    ports:

      - 9200:9200

  kibana:

    container\_name: kibana

    image: docker.elastic.co/kibana/kibana:7.4.0

    restart: always

    environment:

      - ELASTICSEARCH\_HOSTS=http://elasticsearch:9200    # address of elasticsearch docker container which kibana will connect

    ports:

      - 5601:5601

    depends\_on:

      - elasticsearch                                   # kibana will start when elasticsearch has started

  logstash:

    image: docker.elastic.co/logstash/logstash:8.12.2

    volumes:

      - ./elk/logstash.conf:/usr/share/logstash/pipeline/logstash.conf

    environment:

      - ELASTIC\_USER=elastic

      - ELASTIC\_PASSWORD=myelasticpass

      - ELASTIC\_HOSTS=http://elastic:9200

    depends\_on:

      - elasticsearch

volumes:

  elasticsearch-data:

\_ Ngoài ra chúng ta tạo thư mục elk và file config cho logstash như sau

input {

  beats {

    port => 5044

  }

}

filter {

    json {

        source => "message"

        target => "parseJson"

    }

    grok {

        match => {

            "message" => "%{IPV6:ipv6}:%{IPV4:ipv4} - - \[%{DATA:parsed\_timestamp}\] \\"%{WORD:verb} %{URIPATHPARAM:request} HTTP/%{NUMBER:httpversion}\\" %{NUMBER:response}"

        }

    }

    date {

        match => [ "parsed\_timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]

    }

}

output {

    elasticsearch {

        hosts => "${ELASTIC\_HOSTS}"

        user => "${ELASTIC\_USER}"

        password => "${ELASTIC\_PASSWORD}"

        index => "my-log-%{+YYYY.MM.dd}"

    }

}

1. Thực thi & Kiểm tra  
   \_B1: Chạy docker-compose up -d để tiến hành thực thi  
   \_B2: Truy cập vào địa chỉ localhost:5601 để kiểm tra, nếu kết quả như hình là cài đặt thành công
2. A screenshot of a computer

   Description automatically generated