

ELK Stack Configuration Documentation

ELK Stack Configuration Documentation

Overview

This document provides a comprehensive guide for setting up and configuring the ELK Stack (Elasticsearch, Logstash, and Kibana) using Docker Compose, including service token authentication and Java application integration.

Table of Contents

1. [Architecture Overview](#architecture-overview)
2. [Docker Compose Configuration](#docker-compose-configuration)
3. [Service Token Authentication](#service-token-authentication)
4. [Logstash Configuration](#logstash-configuration)
5. [Java Application Integration](#java-application-integration)
6. [Deployment Steps](#deployment-steps)
7. [Troubleshooting](#troubleshooting)

Architecture Overview

The ELK Stack consists of three main components:

- **Elasticsearch**: Search and analytics engine that stores and indexes log data
- **Logstash**: Data processing pipeline that ingests, transforms, and sends data to Elasticsearch
- **Kibana**: Visualization layer that provides a web interface for searching and viewing data

Network Configuration

- **elk-network**: Internal overlay network for ELK services communication
- **proxy_net**: External network for Traefik reverse proxy integration

Docker Compose Configuration

Complete docker-compose.yml

```
version: '3.5'
```

```
networks:
```

```
  elk-network:
```

```
    driver: overlay
```

ELK Stack Configuration Documentation

proxy_net:

external: true

services:

kibana:

image: training.registry:3389/kibana:8.17.3

ports:

- 5601:5601

networks:

- elk-network

- proxy_net

depends_on:

- elasticsearch

environment:

- SERVER_HOST=0.0.0.0

- SERVER_PORT=5601

- ELASTICSEARCH_HOSTS=http://elasticsearch:9200

ELASTICSEARCH_SERVICEACCOUNTTOKEN=AAEAAWVsYXN0aWMva2liYW5hL2tpYmFuYS10b2tlbjo2T1hoMmZR
dIFhbUpkaGV0SnhKZEVR

- XPACK_SECURITY_ENABLED=true

- ELASTICSEARCH_SSL_VERIFICATION_MODE=none

- xpack.actions.enabled=false

- xpack.fleet.enabled=false

- telemetry.enabled=false

- elasticsearch.requestTimeout=60000

- telemetry.optIn=false

- telemetry.allowChangingOptInStatus=false

- xpack.monitoring.collection.enabled=false

- newsfeed.enabled=false

- xpack.reporting.telemetry.enabled=false

- xpack.securitySolution.telemetry.enabled=false

- xpack.security.enrollment.enabled=false

deploy:

labels:

- traefik.enable=true

- traefik.docker.network=proxy_net

- traefik.http.routers.kibana.rule=Host(`kibana.fssai.gov.in`)

- traefik.http.routers.kibana.entrypoints=http

- traefik.http.services.kibana.loadbalancer.server.port=5601

ELK Stack Configuration Documentation

placement:

constraints: [node.labels.eureka1 == true]