

# Deploying ELK Stack on Docker Container

## WRITEUPS

- Set up the Docker Environment: Install Docker from the official website, verify the installation with `docker --version`.
- Clone ELK Stack Configuration: Create a directory, clone the ELK Stack config from GitHub using `git clone`.
- Configure ELK Stack: Review and modify config files for Elasticsearch, Logstash, and Kibana based on project needs.
- Create Docker Compose File: In the `docker-elk` dir, create `docker-compose.yml` defining services for ELK components.
- Build and Run ELK Stack: In `docker-elk`, run `docker-compose up -d` to build and start the ELK Stack.
- Access Kibana: Open a web browser and go to `http://localhost:5601` to access the Kibana dashboard.
- Index Data in Elasticsearch: Configure Logstash to collect and process data, send it to Elasticsearch for indexing.
- Continuous Monitoring: With ELK Stack running, it continuously monitors and analyzes data in real-time.
- Git Setup and Tracking: Initialize Git repo, add files, create `.gitignore`, commit changes.
- Create GitHub Repository and Push: Create a new GitHub repo, connect local Git repo, and push code using provided commands.