27.05.2022

DEPLOYING ELK STACK ON DOCKER CONTAINER PROJECT

Prepared by: PRIYANKA DAS

Project Objective :

You have to deploy ELK Stack on a Docker container to implement continuous monitoring.

Following Requirements Should Be Met :

- A few of the source code should be tracked on GitHub repositories. You need to document the tracked files that are ignored during the final push to the GitHub repository.
- Submission of your GitHub repository link is mandatory. In order to track your task, you need to share the link of the repository in the document.
- The step-by-step process involved in completing this task should be documented

Background of the problem statement:

Your manager has asked to create an elegant user interface for data analysis and data visualization as you have worked on ELK stack previously and have the idea of how it works. This will help the DevOps team to monitor and analyze the application behavior.

Step by step process :

Elastic Stack (ELK) Docker Composition, preconfigured with Security, Monitoring, and Tools; Up with a Single Command.
Suitable for Demoing, MVPs and small production deployments.
Stack Version: 8.2.0 - Based on Official Elastic Docker Images
You can change Elastic Stack version by setting ELK_VERSION in .env file and rebuild your images. Any version >= 8.0.0 is compatible with this template.

Main Features :

- Configured as a Production Single Node Cluster. (With a multi-node cluster option for experimenting).
- Security Enabled By Default.
- Configured to Enable:
    - Logging & Metrics Ingestion
    - APM
    - Alerting
    - Machine Learning
    - SIEM
    - Enabling Trial License

Main Features :

- Use Docker-Compose and .env to configure your entire stack parameters.
- Persist Elasticsearch's Keystore and SSL Certifications.
- Self-Monitoring Metrics Enabled.
- Prometheus Exporters for Stack Metrics.
- Collect Docker Host Logs to ELK via make collect-docker-logs.
- Embedded Container Healthchecks for Stack Images.
- Rubban for Kibana curating tasks.
- One of the most popular ELK on Docker repositories is the awesome deviantony/docker-elk. Elastdocker differs from deviantony/docker-elk in the following points.
- Security enabled by default using Basic license, not Trial.
- Persisting data by default in a volume.
- Run in Production Mode (by enabling SSL on Transport Layer, and add initial master node settings).

Main Features :

- Persisting Generated Keystore, and create an extendable script that makes it easier to recreate it every-time the container is created.
- Parameterize credentials in .env instead of hardcoding elastich:changeme in every component config.
- Parameterize all other Config like Heap Size.
- Add recommended environment configurations as Ulimits and Swap disable to the docker-compose.
- Make it ready to be extended into a multinode cluster.
- Configuring the Self-Monitoring and the Filebeat agent that ship ELK logs to ELK itself. (as a step to shipping it to a monitoring cluster in the future).
- Configured tools and Prometheus Exporters.
- The Makefile that simplifies everything into some simple commands.

Configuration :

- Some Configuration are parameterized in the .env file.
    - ELASTIC_PASSWORD, user elastic's password (default: changeme pls).
    - ELK_VERSION Elastic Stack Version (default: 8.2.0)
    - ELASTICSEARCH_HEAP, how much Elasticsearch allocate from memory (default: 1GB -good for development only-)
    - LOGSTASH_HEAP, how much Logstash allocate from memory.
    - Other configurations which their such as cluster name, and node name, etc.
- Elasticsearch Configuration in elasticsearch.yml at ./elasticsearch/config.
- Logstash Configuration in logstash.yml at ./elasticsearch/config/logstash.yml.
- Logstash Pipeline in main.conf at ./elasticsearch/pipeline/main.conf.
- Kibana Configuration in kibana.yml at ./kibana/config.
- Rubban Configuration using Docker-Compose passed Environment Variables.