**Continuous Monitoring on Docker with ELK Stack**

**Phase 5 Project**

My git [URL:-](https://d.docs.live.net/936fd11abb85565b/Documents/-) <https://github.com/siddharth0206/simplelearn-projects>

# Introduction

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: [8.0.1](https://www.elastic.co/blog/whats-new-elastic-8-0-0) 🎉 - Based on [Official Elastic Docker Images](https://www.docker.elastic.co/)

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
* 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](https://github.com/sherifabdlnaby/rubban) for Kibana curating tasks.

#### More points

And comparing Elastdocker and the popular [deviantony/docker-elk](https://github.com/deviantony/docker-elk)

Expand...

# Requirements

* [Docker 20.05 or higher](https://docs.docker.com/install/)
* [Docker-Compose 1.29 or higher](https://docs.docker.com/compose/install/)
* 4GB RAM (For Windows and MacOS make sure Docker's VM has more than 4GB+ memory.)

# Setup

1. Clone the Repository

git clone https://github.com/siddharth0206/simplelearn-projects.git

1. Initialize Elasticsearch Keystore and TLS Self-Signed Certificates

$ make setup

**For Linux's docker hosts only**. By default virtual memory [is not enough](https://www.elastic.co/guide/en/elasticsearch/reference/current/vm-max-map-count.html) so run the next command as root sysctl -w vm.max\_map\_count=262144

1. Start Elastic Stack

$ make elk <OR> $ docker-compose up -d

1. Visit Kibana at [https://localhost:5601](https://localhost:5601/) or https://<your\_public\_ip>:5601

Default Username: elastic, Password: changeme

* + Notice that Kibana is configured to use HTTPS, so you'll need to write https:// before localhost:5601 in the browser.
  + Modify .env file for your needs, most importantly ELASTIC\_PASSWORD that setup your superuser elastic's password, ELASTICSEARCH\_HEAP & LOGSTASH\_HEAP for Elasticsearch & Logstash Heap Size.

Whatever your Host (e.g AWS EC2, Azure, DigitalOcean, or on-premise server), once you expose your host to the network, ELK component will be accessible on their respective ports. Since the enabled TLS uses a self-signed certificate, it is recommended to SSL-Terminate public traffic using your signed certificates.

🏃🏻‍♂️ To start ingesting logs, you can start by running make collect-docker-logs which will collect your host's container logs.

## Additional Commands

Expand

# Configuration

* Some Configuration are parameterized in the .env file.
  + ELASTIC\_PASSWORD, user elastic's password (default: changeme pls).
  + ELK\_VERSION Elastic Stack Version (default: 8.0.1)
  + 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.

### Setting Up Keystore

You can extend the Keystore generation script by adding keys to ./setup/keystore.sh script. (e.g Add S3 Snapshot Repository Credentials)

To Re-generate Keystore:

make keystore

### Notes

* ⚠️ Elasticsearch HTTP layer is using SSL, thus mean you need to configure your elasticsearch clients with the CA in secrets/certs/ca/ca.crt, or configure client to ignore SSL Certificate Verification (e.g --insecure in curl).
* Adding Two Extra Nodes to the cluster will make the cluster depending on them and won't start without them again.
* Makefile is a wrapper around Docker-Compose commands, use make help to know every command.
* Elasticsearch will save its data to a volume named elasticsearch-data
* Elasticsearch Keystore (that contains passwords and credentials) and SSL Certificate are generated in the ./secrets directory by the setup command.
* Make sure to run make setup if you changed ELASTIC\_PASSWORD and to restart the stack afterwards.
* For Linux Users it's recommended to set the following configuration (run as root)
* sysctl -w vm.max\_map\_count=262144

# Monitoring The Cluster

### Via Self-Monitoring

Head to Stack Monitoring tab in Kibana to see cluster metrics for all stack components.

In Production, cluster metrics should be shipped to another dedicated monitoring cluster.