Deploying ELK Stack on Docker Container write up

By following these steps and running the Docker Compose command, the ELK stack will be set up in Docker containers, allowing you to use Elasticsearch for data storage and Kibana for visualizing and analyzing the data.

Step 1: Create a Directory/Folder with the name "ELK."
- This step involves creating a new folder (also called a directory) on your computer or server. You can give it the name "ELK."

Step 2: Create a File named "docker-compose.yml" in this directory.
- In the "ELK" directory you just created, make a new file and name it "docker-compose.yml." This file will contain the configuration for Docker Compose, which will help us set up the ELK stack.

Step 3: Paste the provided code into the "docker-compose.yml" file.
- Open the "docker-compose.yml" file in a text editor and copy-paste the provided code into it. This code specifies the services (Elasticsearch and Kibana) that will be run in Docker containers.

Step 4: Start Docker on your system.
- Before we can run the ELK stack, Docker needs to be running on your computer or server. Docker is a platform that allows you to create, deploy, and run applications in containers.

Step 5: Run the Docker Compose command to set up the ELK stack.
- Open a terminal or command prompt, navigate to the "ELK" directory, and run the command "docker-compose -f docker-compose.yml up -d." This command tells Docker Compose to read the configuration from the "docker-compose.yml" file and create and start the containers accordingly.

Explanation of the "docker-compose.yml" file:
- The file is written in YAML format, which is easy to read and understand.
- It defines two services: "elasticsearch" and "kibana."
- "elasticsearch" service uses the official Elasticsearch Docker image version 7.12.0.
- "kibana" service uses the official Kibana Docker image version 7.12.0.
- Elasticsearch and Kibana will restart automatically if the containers stop unexpectedly (due to the "restart: always" setting).
- The "elasticsearch" service has environment variables set to disable security features and run Elasticsearch as a single node for simplicity.
- Volume is created to store Elasticsearch data outside the container for persistence.
- Ports are mapped from the host machine to access Elasticsearch on port 9200 and Kibana on port 5601.