Name: ELK Stack

System Administration Manual

Version 1.0

05,03,2024

Table of Contents

1. Introduction
   1. Scope
   2. Location of Document
2. Operational Process
   1. Requirements needed.
   2. Installation
   3. Running Script
   4. Testing the ELK Stack
3. Troubleshooting
4. **Introduction**

The ELK Stack, which stands for Elasticsearch, Logstash, and Kibana, is a powerful platform for logging, monitoring, and analyzing data. This manual provides key information and Standard Operating Procedures (SOPs) necessary to maintain the ELK Stack environment effectively. The manual covers the definition of the software support environment, the roles and responsibilities of the various personnel, and the regular activities essential to the support and maintenance of the ELK Stack.

The ELK Stack has become increasingly popular in recent years due to its flexibility, scalability, and ease of use. It is widely used in various industries, including finance, healthcare, and e-commerce, to collect, store, and analyze large volumes of data. The ELK Stack can help organizations gain valuable insights into their operations, identify potential issues, and make data-driven decisions.

This manual is designed to help you understand and manage your ELK Stack environment effectively. It provides detailed instructions for testing and configuring the ELK Stack components, as well as guidance on best practices for maintaining your ELK Stack environment.

1. **Scope**

The scope of this Systems Administration Manual covers the ELK Stack environment, which includes the following components:

* Elasticsearch: A powerful and scalable search engine based on Lucene, ideal for indexing and searching large volumes of data in real-time. It's commonly used for log and event data analysis, full-text search, and application performance monitoring.
* Kibana: A data visualization tool that works seamlessly with Elasticsearch, allowing users to explore, visualize, and analyze data through dynamic dashboards and charts. It's commonly used for monitoring, troubleshooting, and data-driven decision-making.
* Logstash: A flexible and extensible data processing pipeline that ingests, transforms, and enriches data from various sources before sending it to a destination, often Elasticsearch. It's commonly used for log and event data collection, parsing, and normalization in centralized logging and monitoring systems.
* Docker: A containerization platform that allows developers to package applications and their dependencies into isolated, lightweight containers, making it easier to deploy and manage applications consistently across different environments. It provides a standardized way to build, ship, and run applications, enabling greater efficiency, scalability, and portability in software development and deployment.

The manual provides detailed instructions for installing and configuring each component, as well as guidance on best practices for maintaining your ELK Stack environment. The ELK Stack environment is essential for organizations that rely on logging, monitoring, and analyzing large volumes of data. By following the instructions and guidance provided in this manual, you can ensure that your ELK Stack environment is properly configured and maintained, allowing you to focus on analyzing and visualizing your data.

1. **Location of Document**

Electronic copies of this document can be copied from the GitHub at <https://github.com/kxs1119/cpsc-327>

1. **Operation Process**

The Operation Process for the ELK Stack environment, as outlined in this manual, focuses on the installation, configuration, and maintenance of the ELK Stack components. This process is designed to help you effectively manage your ELK Stack environment, ensuring that it is properly configured and maintained to support your logging, monitoring, and analysis needs.

1. **Requirements**

You will need a system that is running:

* Ubunutu 20.04 or higher
* Terminal Window
  + With sudo command capability
* 30 GB of Storage Minimum
* 4 GB RAM Minimum
* Understanding of running scripts
* Docker installed

To install the ELK Stack environment on your Linux system, you can either clone the repository or download the ELK Stack components as a zip file. Here are the detailed instructions for each method:

Method 1: Clone from Repository

* Open a terminal window on your Linux system.
* Navigate to the directory where you want to clone the repository.
* Use the following command to clone the repository
  + Git clone https://github.com/kxs1119/cpsc-327.git

Method 2: Download the ELK Stack Components from Repository as a Zip Folder

* Open a web browser on Linux System
* Navigate to <https://github.com/kxs1119/cpsc-327>
* Click on the Download Zip button to download the ELK Stack script

1. **Running Scripts**

* Open a terminal window on your Linux system
* Navigate to the directory containg the ELK Stack and navigate to the following:
  + client.bash
* Make the scripts executable by running the following command:
  + Sudo chmod +x client.bash
* Run the installation script by executing the following command:
  + ./client.bash
* Follow the on-screen instructions provided by the scripts to complete the installation and **configuration process.**

1. **Testing Script**

* To test the ELK Stack installation and configuration, you can navigate to your web browser and enter the following URLs**:**
  + **Elasticsearch ~** [**http://localhost:9200**](http://localhost:9200)
  + **Kibana ~ http:// localhost:5601**