Name: Campo, Keneth	**Date Performed: November 12, 2024**
Course/Section: CPE31S21	**Date Submitted: November 12, 2024**
Instructor: Engr. Robin Villanueva	**Semester and SY: 1st Semester/ 2024-2025**

Activity 10: Install, Configure, and Manage Log Monitoring tools

1. Objectives

Create and design a workflow that installs, configure and manage enterprise log monitoring tools using Ansible as an Infrastructure as Code (IaC) tool.

2. Discussion

Log monitoring software scans and monitors log files generated by servers, applications, and networks. By detecting and alerting users to patterns in these log files, log monitoring software helps solve performance and security issues. System administrators use log monitoring software to detect common important events indicated by log files.

Log monitoring software helps maintain IT infrastructure performance and pinpoints issues to prevent downtime and mitigate risks. These tools will often integrate with IT alerting software, log analysis software, and other IT issue resolution products to more aptly flesh out the IT infrastructure maintenance ecosystem.

To qualify for inclusion in the Log Monitoring category, a product must:

- Monitor the log files generated by servers, applications, or networks
- Alert users when important events are detected
- Provide reporting capabilities for log files

Elastic Stack

ELK suite stands for Elasticsearch, Kibana, Beats, and Logstash (also known as the ELK Stack). Source: https://www.elastic.co/elastic-stack

The Elastic Stack is a group of open source products from Elastic designed to help users take data from any type of source and in any format, and search, analyze and visualize that data in real time. The product group was formerly known as the ELK Stack for the core products in the group -- Elasticsearch, Logstash and Kibana -- but has been rebranded as the Elastic Stack. A fourth product, Beats, was subsequently added to the stack. The Elastic Stack can be deployed on premises or made available as software as a service (SaaS). Elasticsearch supports Amazon Web Services (AWS), Google Cloud Platform and Microsoft Azure.

GrayLog

Graylog is a powerful platform that allows for easy log management of both structured and unstructured data along with debugging applications.

It is based on Elasticsearch, MongoDB, and Scala. Graylog has a main server, which receives data from its clients installed on different servers, and a web interface, which visualizes the data and allows to work with logs aggregated by the main server.

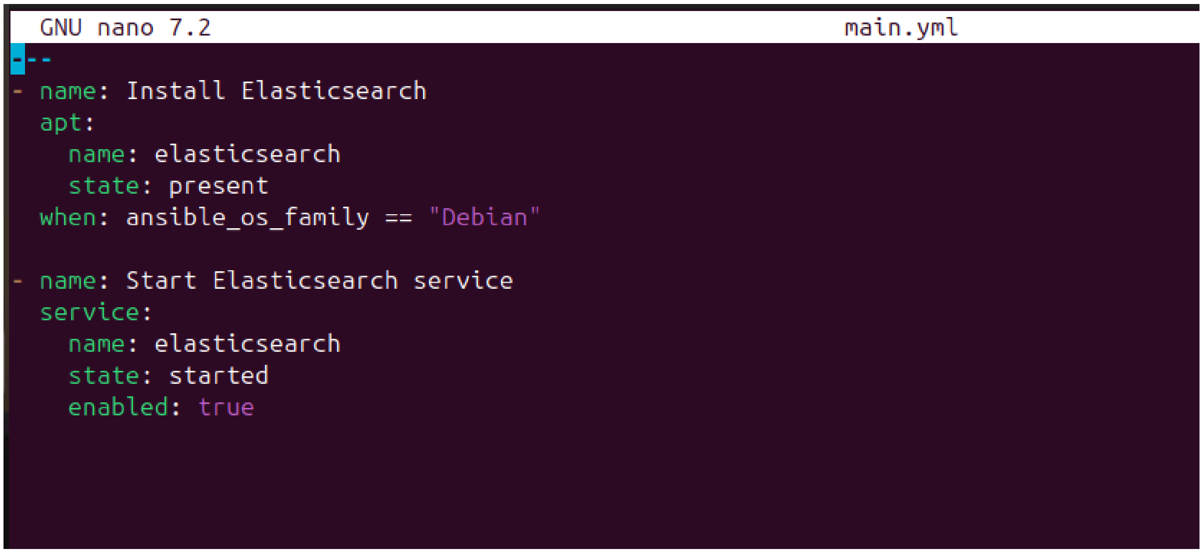
We use Graylog primarily as the stash for the logs of the web applications we build. However, it is also effective when working with raw strings (i.e. syslog): the tool parses it into the structured data we need. It also allows advanced custom search in the logs using structured queries. In other words, when integrated properly with a web app, Graylog helps engineers to analyze the system behavior on almost per code line basis.

Source: https://www.graylog.org/products/open-source

3. Tasks

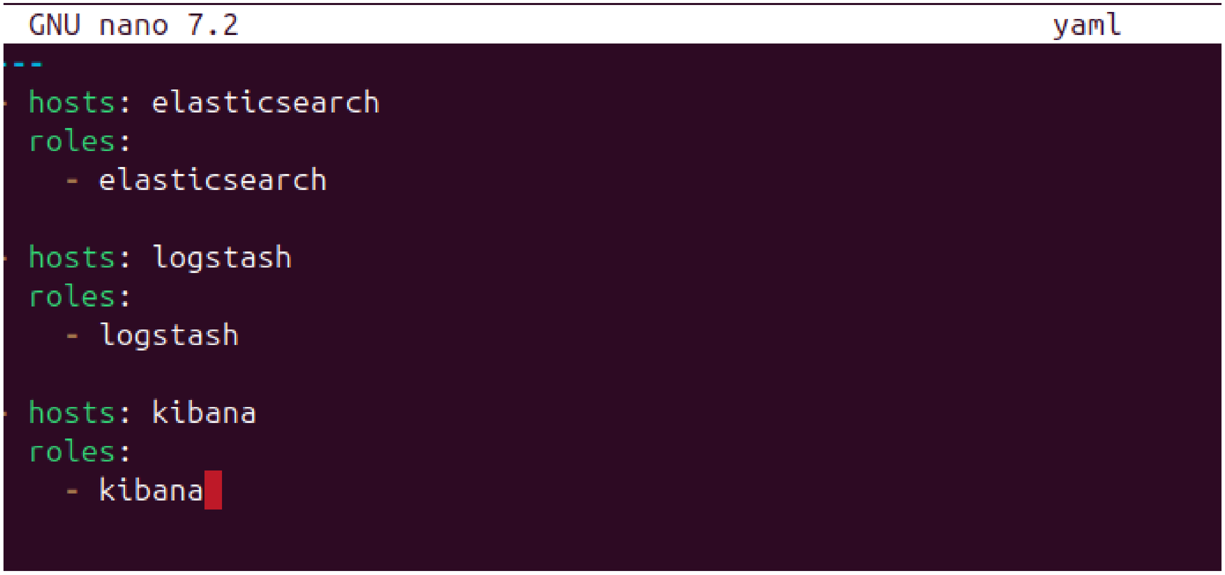
1. Create a playbook that:
    a. Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)
2. Apply the concept of creating roles.
3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like a manual.)
4. Show an output of the installed Elastic Stack for both Ubuntu and CentOS.
5. Make sure to create a new repository in GitHub for this activity.

4. **Output** (screenshots and explanations)



```
  GNU nano 7.2                                                main.yml
---
- name: Install Elasticsearch
  apt:
    name: elasticsearch
    state: present
  when: ansible_os_family == "Debian"

- name: Start Elasticsearch service
  service:
    name: elasticsearch
    state: started
    enabled: true
```



```
  GNU nano 7.2                                                yaml
---
- hosts: elasticsearch
  roles:
    - elasticsearch

- hosts: logstash
  roles:
    - logstash

- hosts: kibana
  roles:
    - kibana
```

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool?
    - log monitoring tools are essential for maintaining system health, enhancing security, optimizing performance, and ensuring compliance, ultimately contributing to more efficient and effective IT operations.

Conclusions:

This guide provided a comprehensive approach to installing and configuring the Elastic Stack (Elasticsearch, Logstash, and Kibana) on separate hosts using Ansible. By employing a role-based structure, we created a modular playbook that simplifies the installation process. Key steps included setting up Ansible roles to organize installation tasks for each component, creating a main playbook to orchestrate the installation across designated hosts, and documenting the process with detailed instructions for installing Ansible, creating an inventory file, and executing the playbook, along with verification steps to ensure successful installation. Additionally, we established a GitHub

repository to share the playbook and facilitate collaboration. The Elastic Stack enhances log monitoring and analysis, enabling organizations to maintain optimal IT performance and respond effectively to security threats. By following this guide, teams can deploy the Elastic Stack consistently, leading to improved data-driven decision-making and proactive system management.