Name: Kenn Cherwin C. Yu	**Date Performed:** 02/04/2024
Course/Section: CPE31S1	**Date Submitted:** 02/04/2024
Instructor: Dr. Jonathan Taylar	**Semester and SY:** 2nd SEM

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.

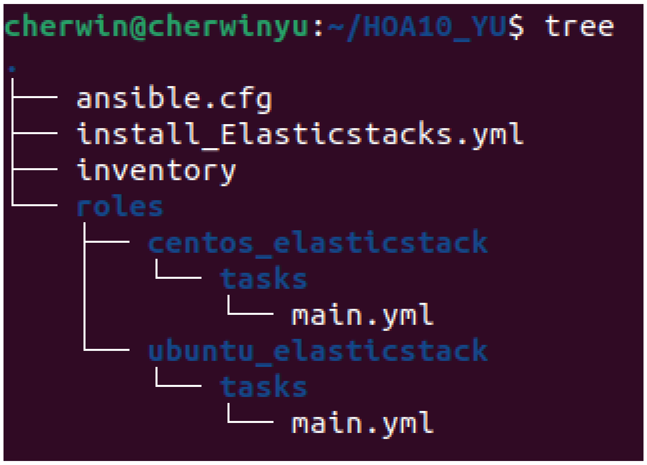
Source: https://www.graylog.org/products/open-source

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.

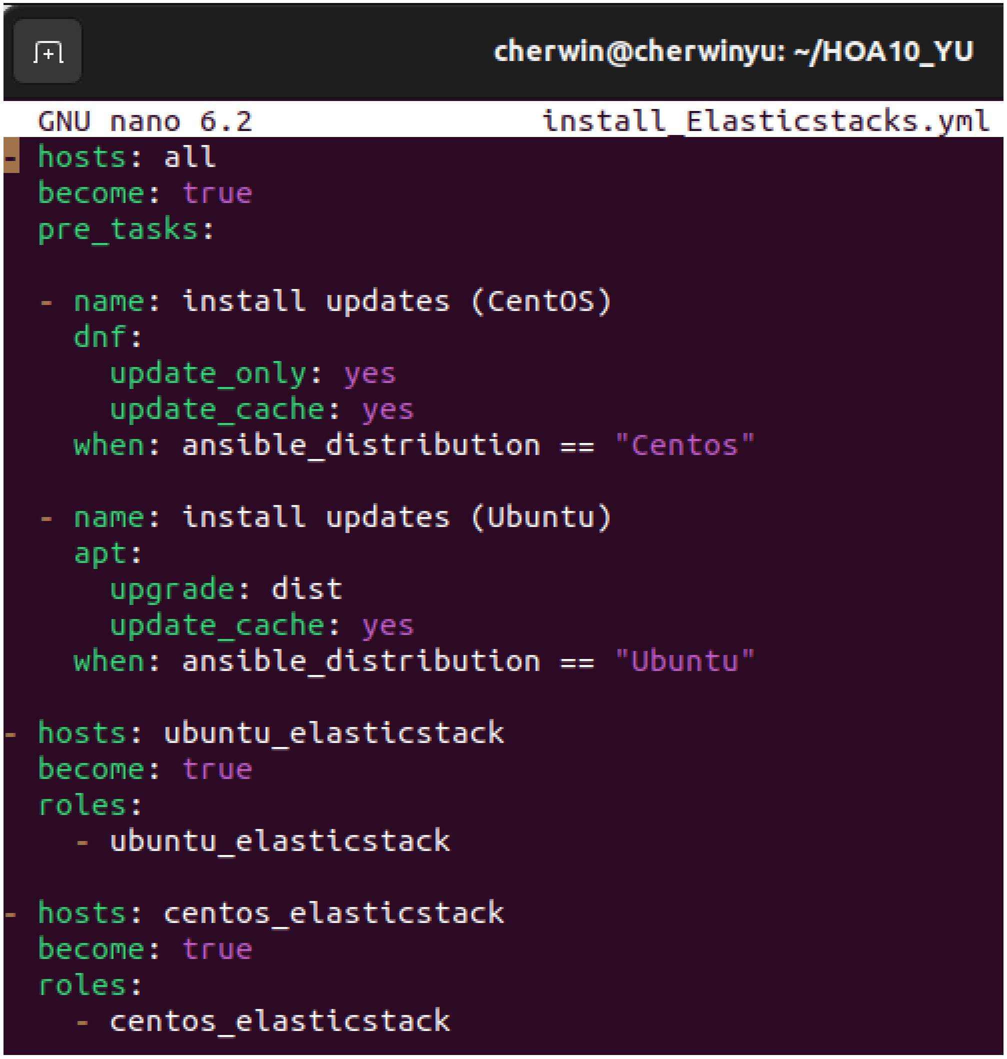
4. **Output** (screenshots and explanations)

- **Tree**



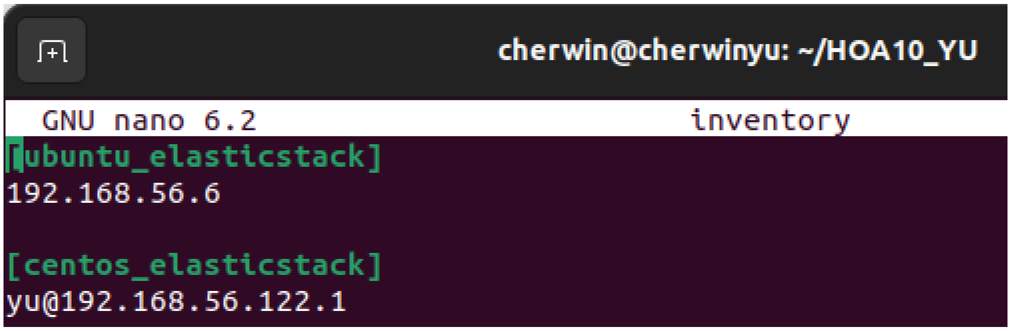
```
cherwin@cherwinyu:~/HOA10_YU$ tree
.
├── ansible.cfg
├── install_Elasticstacks.yml
├── inventory
└── roles
    ├── centos_elasticstack
    │   └── tasks
    │       └── main.yml
    └── ubuntu_elasticstack
        └── tasks
            └── main.yml
```

- **Elastickstacks.yml**



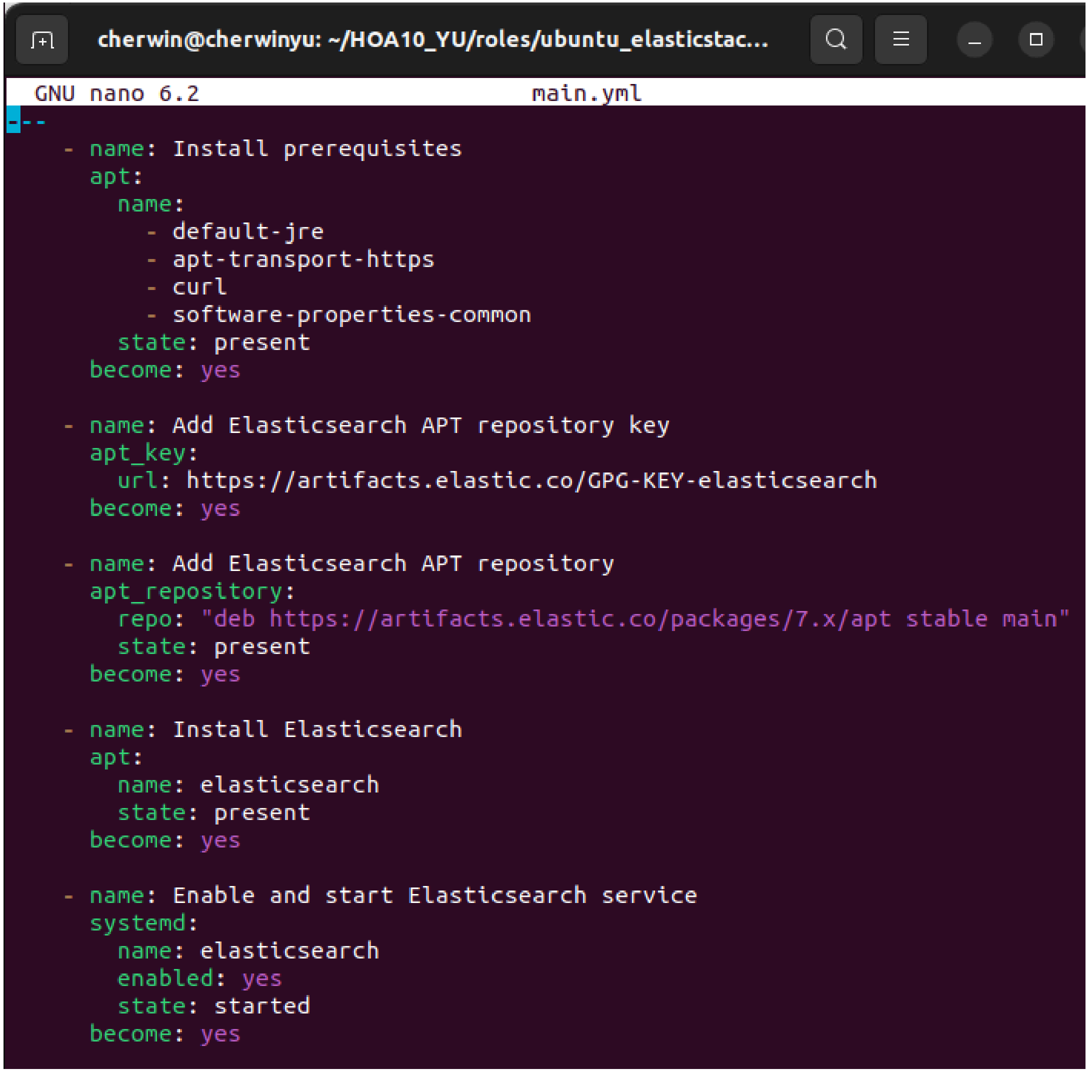
```
GNU nano 6.2                     install_Elasticstacks.yml
- hosts: all
  become: true
  pre_tasks:

  - name: install updates (CentOS)
    dnf:
      update_only: yes
      update_cache: yes
    when: ansible_distribution == "Centos"

  - name: install updates (Ubuntu)
    apt:
      upgrade: dist
      update_cache: yes
    when: ansible_distribution == "Ubuntu"

- hosts: ubuntu_elasticstack
  become: true
  roles:
    - ubuntu_elasticstack

- hosts: centos_elasticstack
  become: true
  roles:
    - centos_elasticstack
```

- **Inventory**

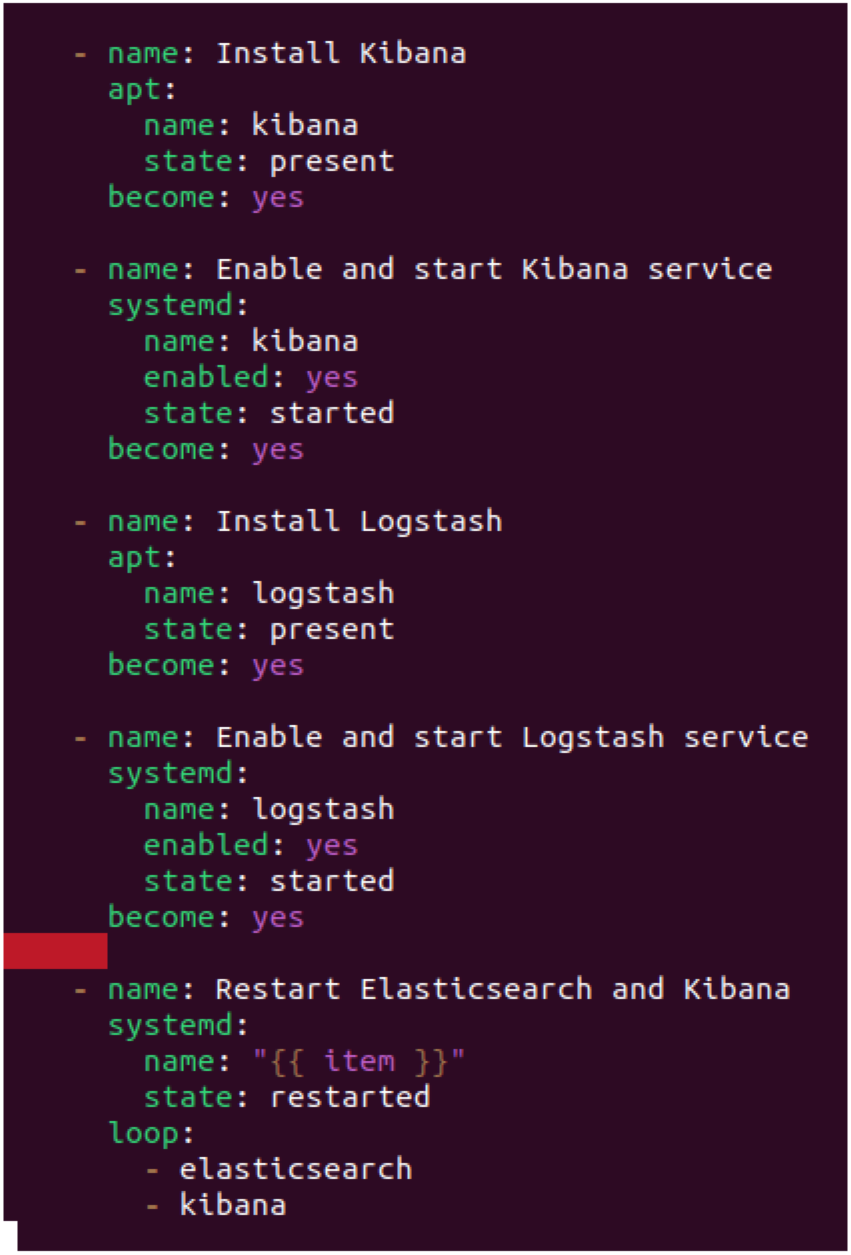


```
  GNU nano 6.2                           inventory
[ubuntu_elasticstack]
192.168.56.6

[centos_elasticstack]
yu@192.168.56.122.1
```

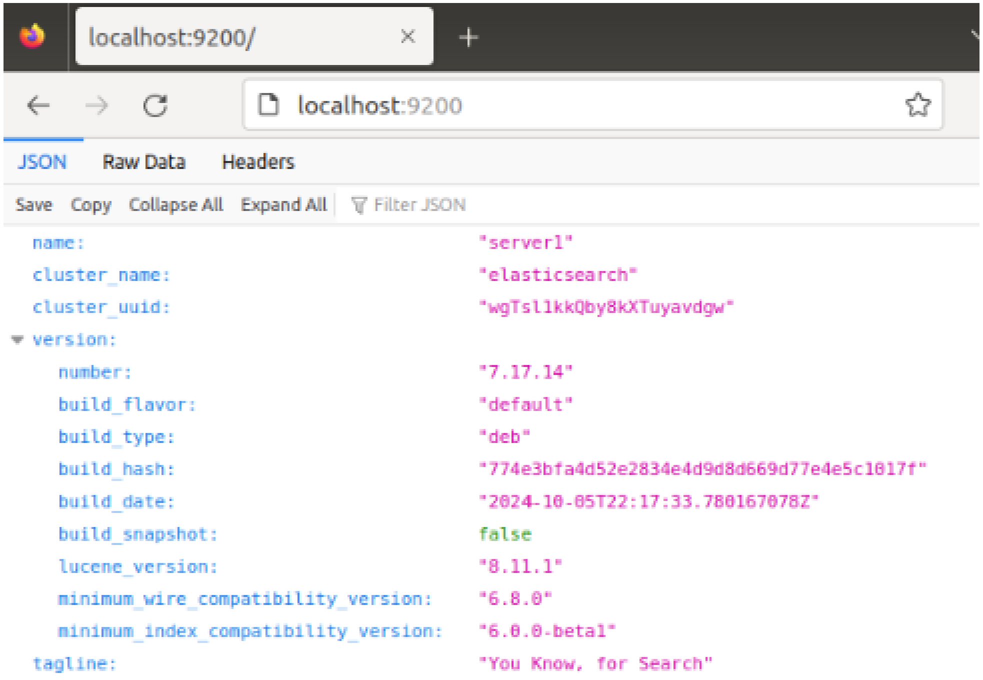
- **main.yml**



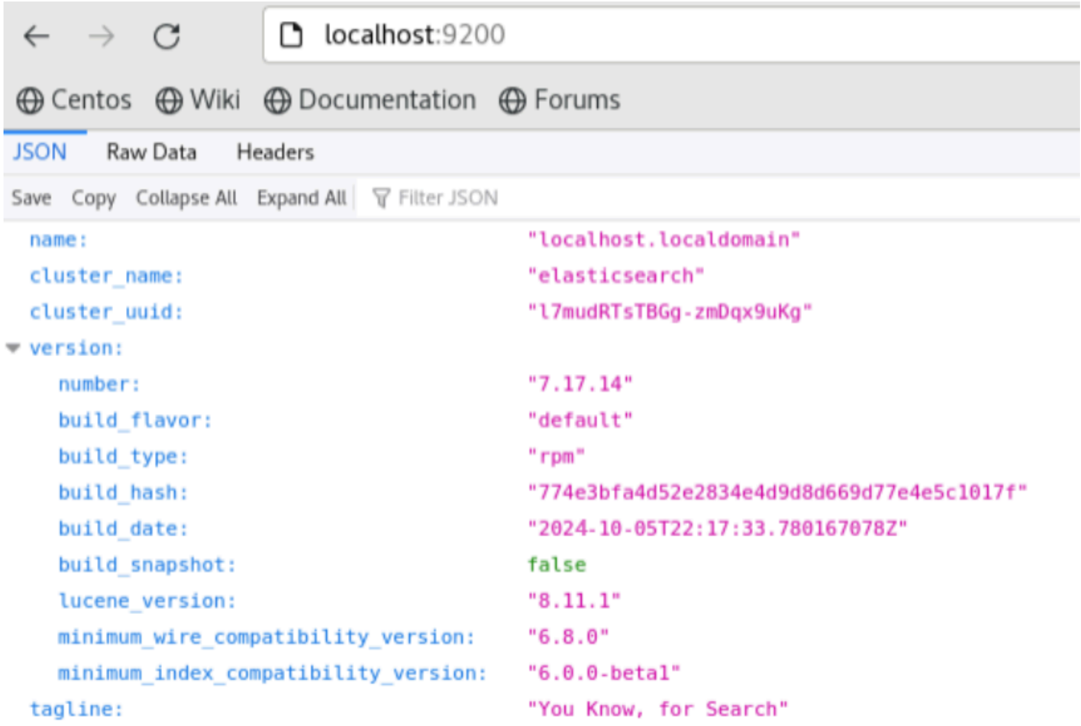
```
  GNU nano 6.2                          main.yml
---
    - name: Install prerequisites
      apt:
        name:
          - default-jre
          - apt-transport-https
          - curl
          - software-properties-common
        state: present
      become: yes

    - name: Add Elasticsearch APT repository key
      apt_key:
        url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
      become: yes

    - name: Add Elasticsearch APT repository
      apt_repository:
        repo: "deb https://artifacts.elastic.co/packages/7.x/apt stable main"
        state: present
      become: yes

    - name: Install Elasticsearch
      apt:
        name: elasticsearch
        state: present
      become: yes

    - name: Enable and start Elasticsearch service
      systemd:
        name: elasticsearch
        enabled: yes
        state: started
      become: yes
```



```
  - name: Install Kibana
    apt:
      name: kibana
      state: present
    become: yes

  - name: Enable and start Kibana service
    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

  - name: Install Logstash
    apt:
      name: logstash
      state: present
    become: yes

  - name: Enable and start Logstash service
    systemd:
      name: logstash
      enabled: yes
      state: started
    become: yes

  - name: Restart Elasticsearch and Kibana
    systemd:
      name: "{{ item }}"
      state: restarted
    loop:
      - elasticsearch
      - kibana
```



```
name:                                   "server1"
cluster_name:                           "elasticsearch"
cluster_uuid:                           "wgTsl1kkQby8kXTuyavdgw"
▼ version:
    number:                             "7.17.14"
    build_flavor:                       "default"
    build_type:                         "deb"
    build_hash:                         "774e3bfa4d52e2834e4d9d8d669d77e4e5c1017f"
    build_date:                         "2024-10-05T22:17:33.780167078Z"
    build_snapshot:                     false
    lucene_version:                     "8.11.1"
    minimum_wire_compatibility_version: "6.8.0"
    minimum_index_compatibility_version: "6.0.0-beta1"
tagline:                                "You Know, for Search"
```



```
name:                                   "localhost.localdomain"
cluster_name:                           "elasticsearch"
cluster_uuid:                           "l7mudRTsTBGg-zmDqx9uKg"
▼ version:
    number:                             "7.17.14"
    build_flavor:                       "default"
    build_type:                         "rpm"
    build_hash:                         "774e3bfa4d52e2834e4d9d8d669d77e4e5c1017f"
    build_date:                         "2024-10-05T22:17:33.780167078Z"
    build_snapshot:                     false
    lucene_version:                     "8.11.1"
    minimum_wire_compatibility_version: "6.8.0"
    minimum_index_compatibility_version: "6.0.0-beta1"
tagline:                                "You Know, for Search"
```

Repository Link: https://github.com/qkccyu/HOA10_YU

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool?
    - Log monitoring tools can offer a number of significant advantages to Organizations of every size. By assisting organizations to improve detection respond to problems, reduce downtimes, and improve security as log Monitoring tools can help organizations improve their overall performance. and efficiency. Log monitoring tools are essential for ensuring system and application health, security, and performance, as well as improving user experience and compliance.

Conclusions:

- In this hands on activity, somewhere I’ve managed to create the playbook but it didn’t apply the way it is because I got many errors in my processing work. But in the last activity it was also the same procedure for the installation. Having Elastic Search tool helps log analytics, search, security, text, and other operational intelligence.