Name: Jessie Robert Lazo	Date Performed: 10/30/24
Course/Section:CPE 212-CPE31S2	Date Submitted: 11/4/24
Instructor: Engr. Robin Valenzuela	Semester and SY:

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.

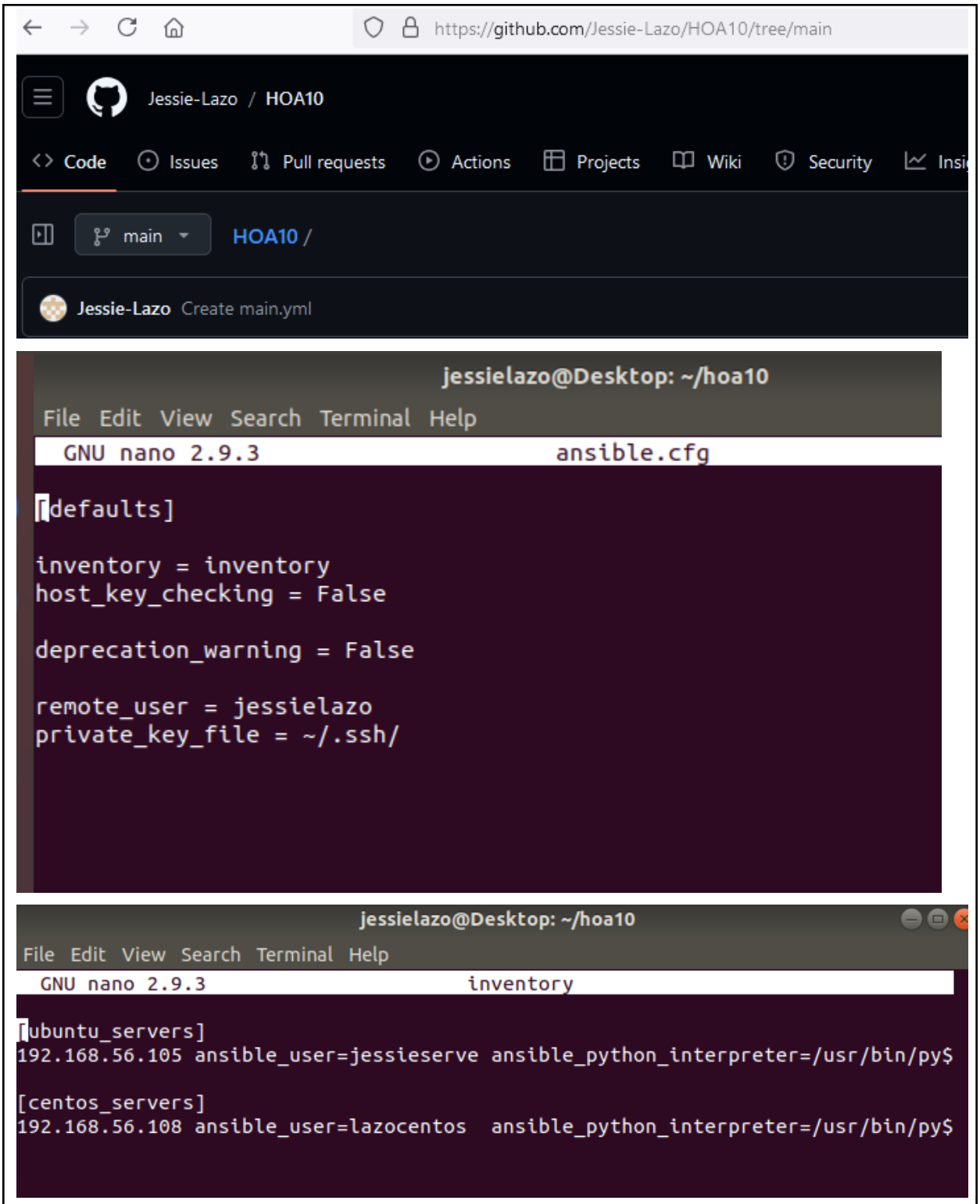
Source: https://www.graylog.org/products/open-source

3. Tasks

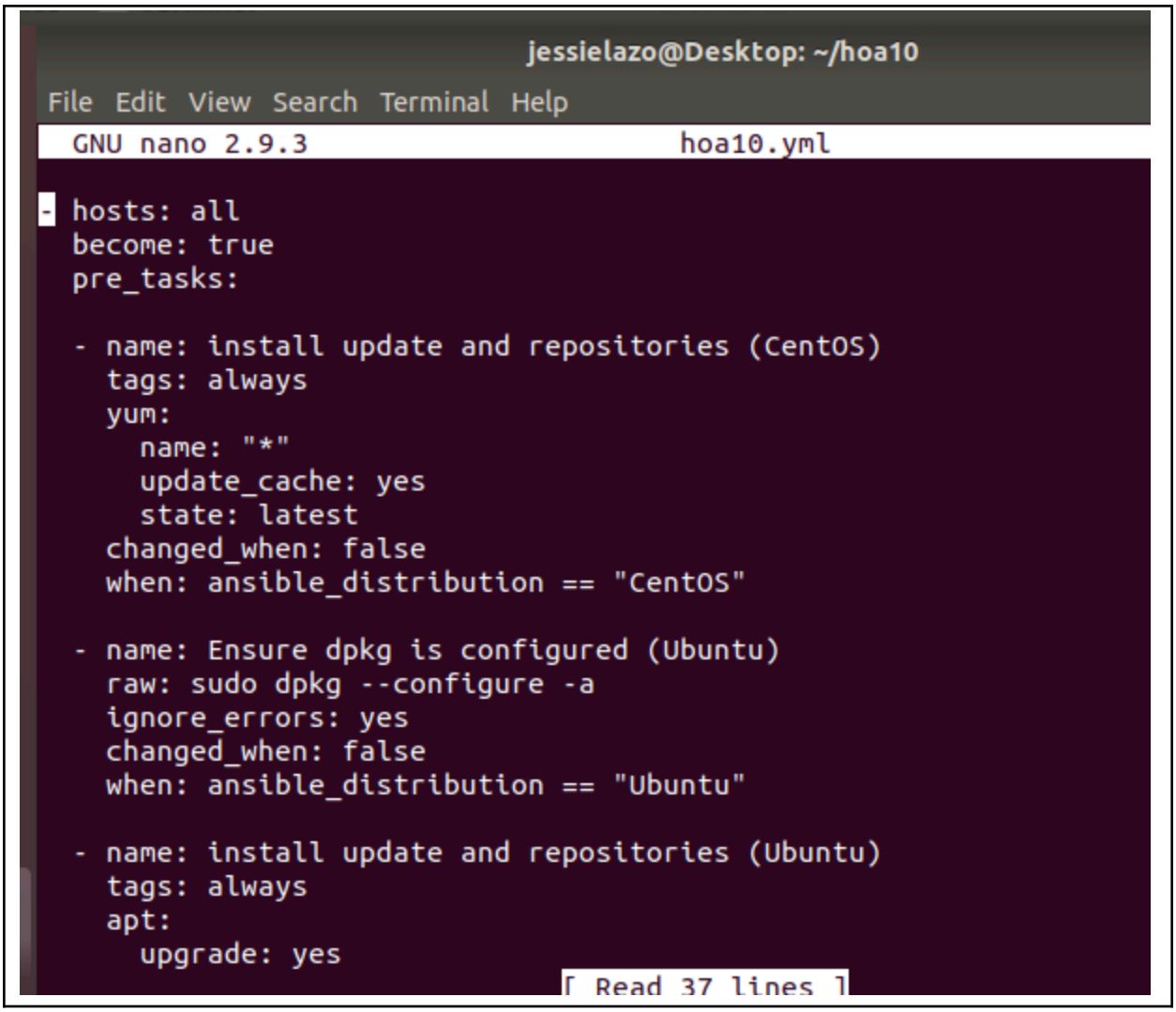
1. Create a playbook that:
    a. Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)
2. Apply the concept of creating roles.
3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like 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.

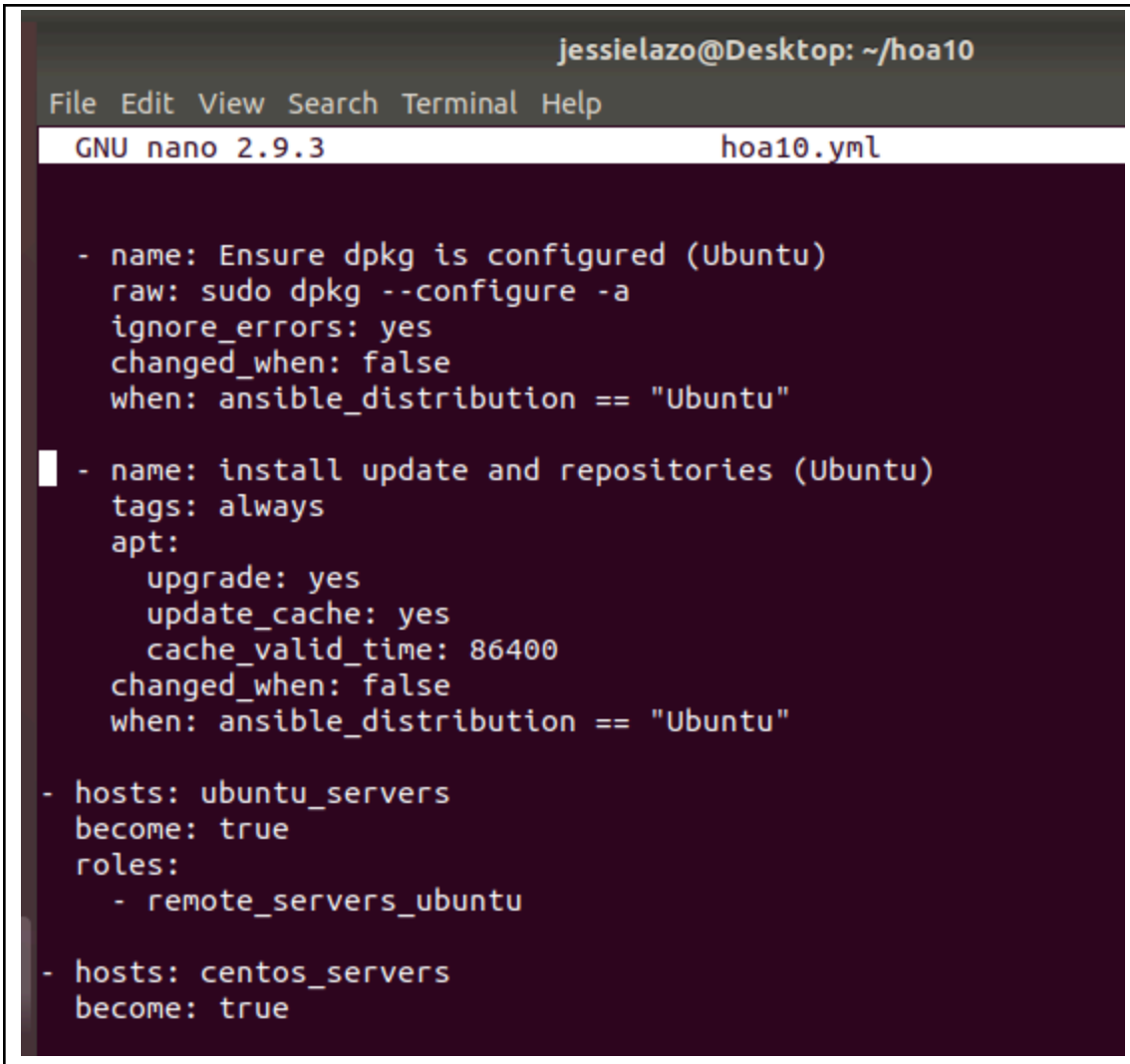
Tasks:

1. Before beginning the activity, the first thing to do is create a new repository, creating the ansible configuration file and inventory file needed to establish a working ansible environment between one local machine (ubuntu), and two remote machines (Ubuntu, and CentOS). Next is to make the necessary folders for implementing the roles in ansible-playbook

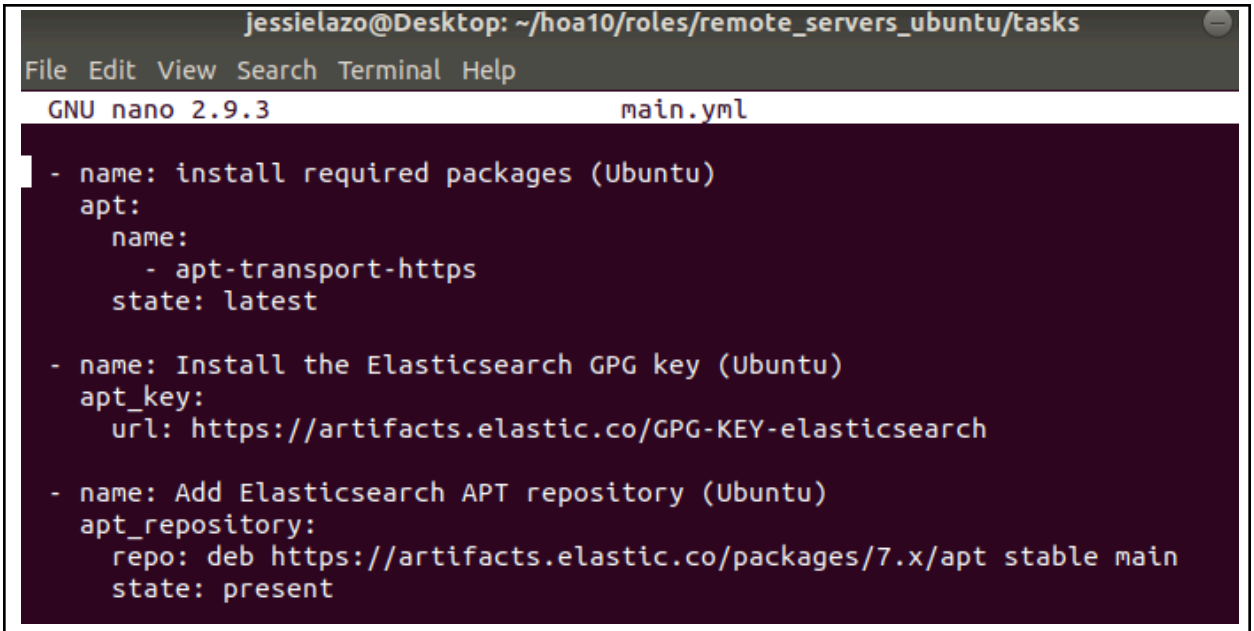


2. Create a playbook named hoa10.yml and implement basic update and upgrade commands for Ubuntu and CentOS machines. hoa10.yml

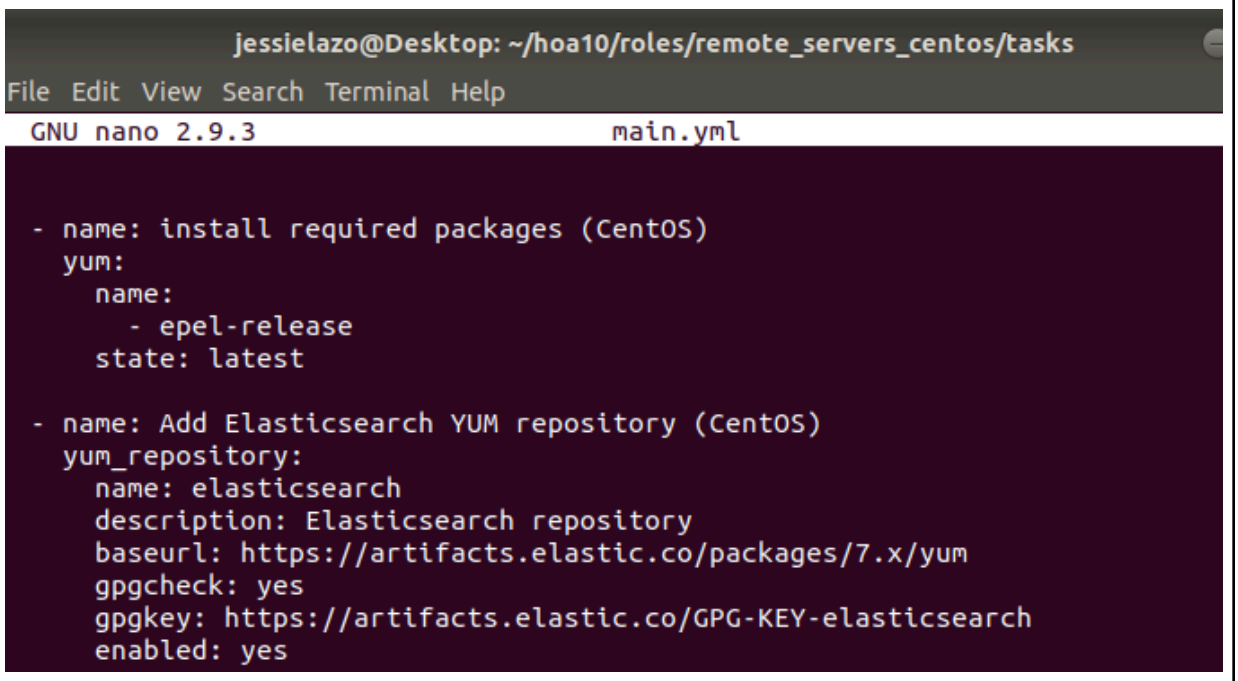

jessielazo@Desktop: ~/hoa10
File Edit View Search Terminal Help
GNU nano 2.9.3 hoa10.yml
- hosts: all
become: true
pre_tasks:
- name: install update and repositories (CentOS)
tags: always
yum:
name: "*"
update_cache: yes
state: latest
changed_when: false
when: ansible_distribution == "CentOS"
- name: Ensure dpkg is configured (Ubuntu)
raw: sudo dpkg --configure -a
ignore_errors: yes
changed_when: false
when: ansible_distribution == "Ubuntu"
- name: install update and repositories (Ubuntu)
tags: always
apt:
upgrade: yes
[Read 37 lines]



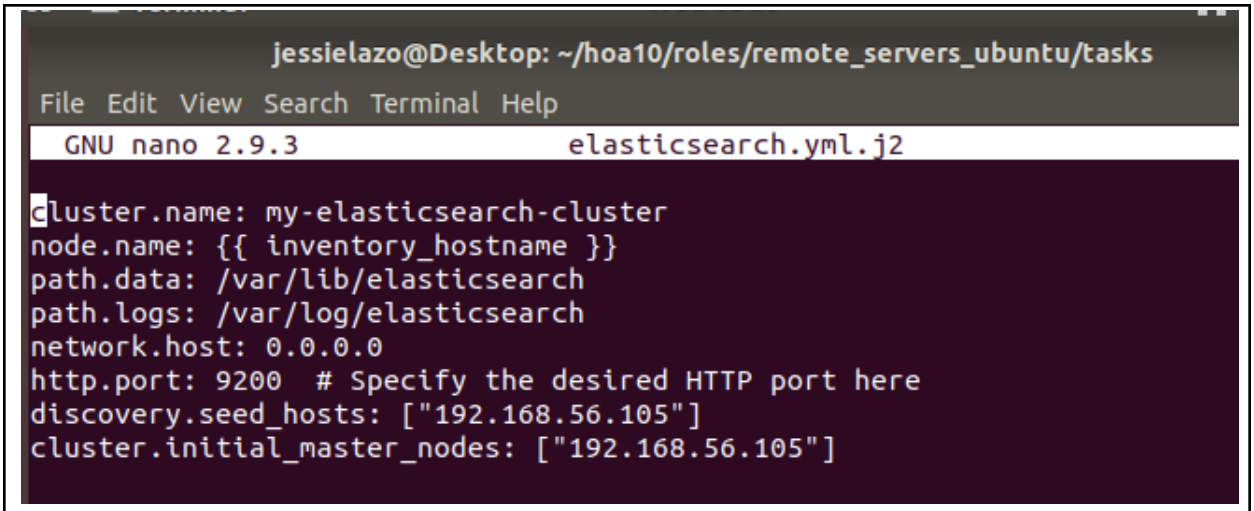
3. Next is we install the necessary packages for the installation of Elastic Search, Kibana, and Logstash. For Ubuntu:



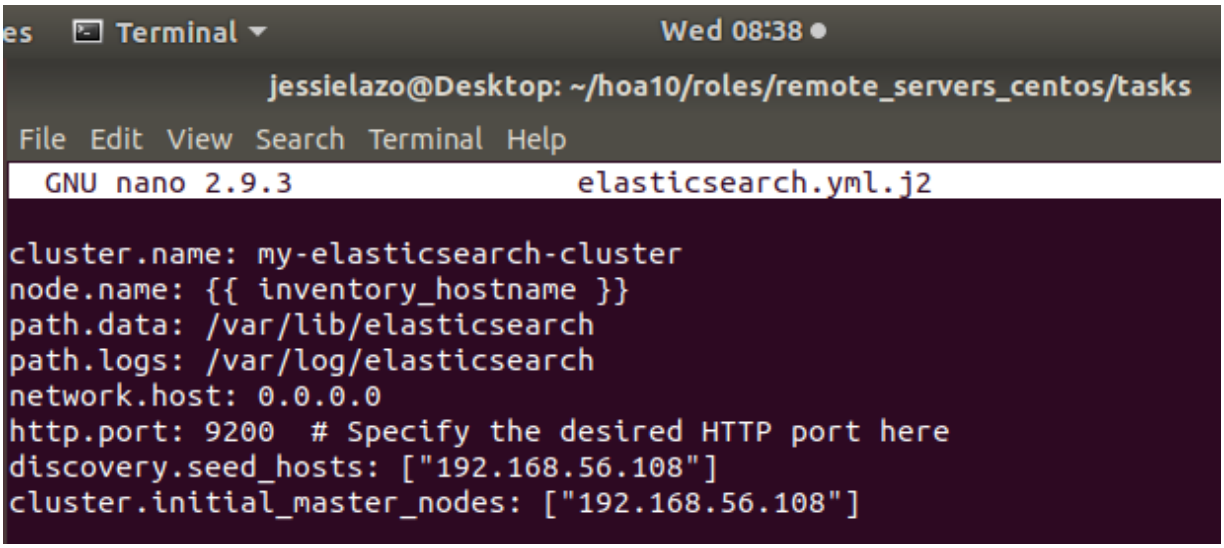
For Centos:



4. Next is we need to manually create a configuration file for ElasticSearch.
For Ubuntu:



ForCentos:



5. Then we can proceed with the installation of ElasticSearch,Kibana,and Logstash. ForUbuntu:

```
- name: Install Elasticsearch (Ubuntu)
  apt:
    name: elasticsearch
    state: present

- name: Copy Elasticsearch configuration file (Ubuntu)
  template:
    src: elasticsearch.yml.j2
    dest: /etc/elasticsearch/elasticsearch.yml
  #notify: Restart Elasticsearch

- name: Install Kibana (Ubuntu)
  apt:
    name: kibana
    state: present

- name: Install Logstash (Ubuntu)
  apt:
    name: logstash
    state: present
```

For Centos:

```
- name: Install Elasticsearch (Centos)
  package:
    name: elasticsearch
    state: present

- name: Copy Elasticsearch configuration file (Centos)
  template:
    src: elasticsearch.yml.j2
    dest: /etc/elasticsearch/elasticsearch.yml
  #notify: Restart Elasticsearch

- name: Install Kibana (Centos)
  yum:
    name: kibana
    state: present

- name: Install Logstash (Centos)
  yum:
    name: logstash
```

6. After the installation, we need to make sure that the service is enabled.
For Ubuntu:

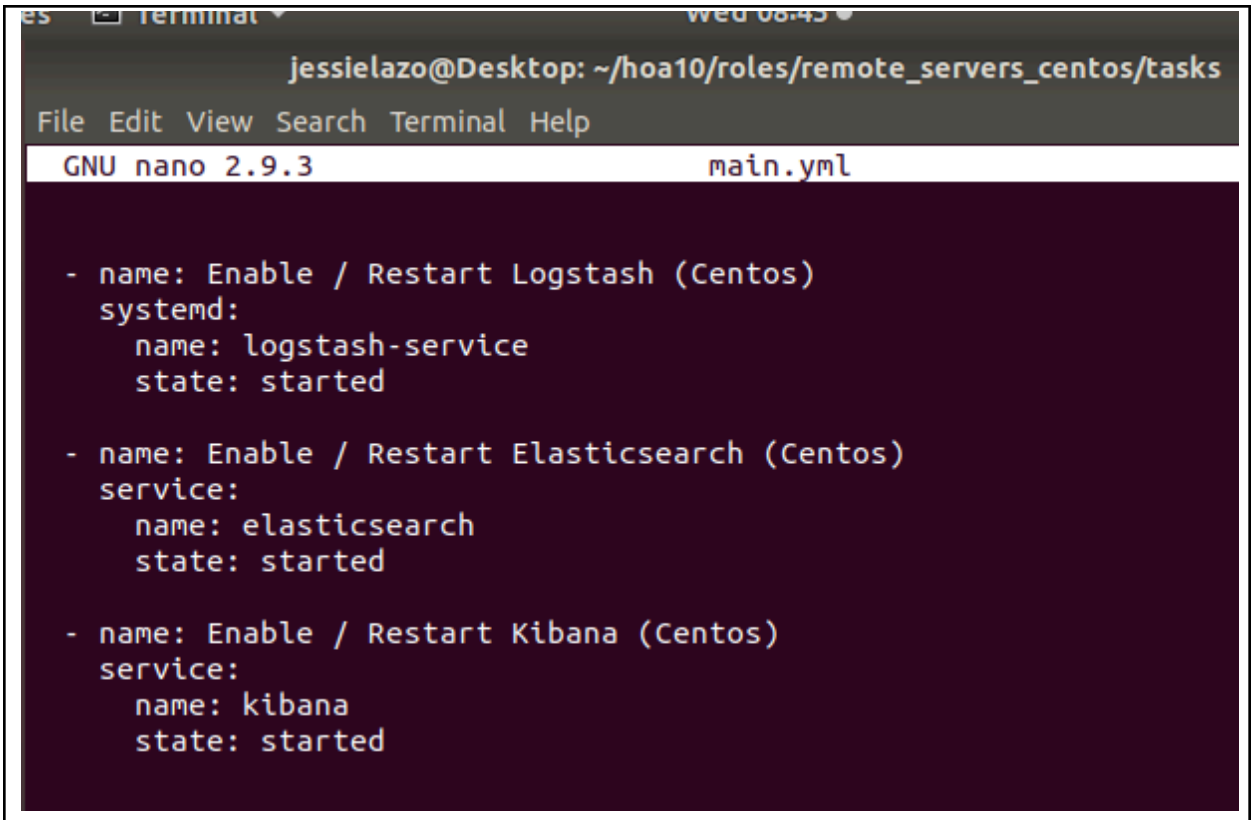
```
jessielazo@Desktop: ~/hoa10/roles/remote_servers_ubuntu/tasks
File  Edit  View  Search  Terminal  Help
 GNU nano 2.9.3                    main.yml

- name: Enable / Restart Elasticsearch (Ubuntu)
  service:
    name: elasticsearch
    state: started

- name: Enable / Restart Kibana (Ubuntu)
  service:
    name: elasticsearch
    state: started

- name: Enable / Restart Logstash (Ubuntu)
  service:
    name: logstash
    state: started
```

For Centos:



7. Debug for errors and show complete proof of working playbook.
8. Sync the local repository to Github.

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

```
jessielazo@Desktop:~/hoa10$ tree
.
├── ansible.cfg
├── hoa10.retry
├── hoa10.yml
├── inventory
└── roles
    ├── remote_servers_centos
    │   └── tasks
    │       ├── elasticsearch.yml.j2
    │       └── main.yml
    └── remote_servers_ubuntu
        └── tasks
            ├── elasticsearch.yml.j2
            └── main.yml

5 directories, 8 files
jessielazo@Desktop:~/hoa10$
```

```
TASK [Ensure dpkg is configured (Ubuntu)] ***********************************
*
ok: [192.168.56.105]

TASK [install update and repositories (Ubuntu)] *****************************
*
 [WARNING]: Could not find aptitude. Using apt-get instead.

ok: [192.168.56.105]

PLAY [ubuntu_servers] *******************************************************
*

TASK [Gathering Facts] ******************************************************
*
ok: [192.168.56.105]

TASK [remote_servers_ubuntu : install required packages (Ubuntu)] ************
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Install the Elasticsearch GPG key (Ubuntu)] *****
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Add Elasticsearch APT repository (Ubuntu)] ******
```

```
TASK [remote_servers_ubuntu : Install the Elasticsearch GPG key (Ubuntu)] *****
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Add Elasticsearch APT repository (Ubuntu)] ******
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Install Elasticsearch (Ubuntu)] ****************
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Copy Elasticsearch configuration file (Ubuntu)] *
**
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Install Kibana (Ubuntu)] ***********************
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Install Logstash (Ubuntu)] *********************
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Enable / Restart Elasticsearch (Ubuntu)] ********
*
```

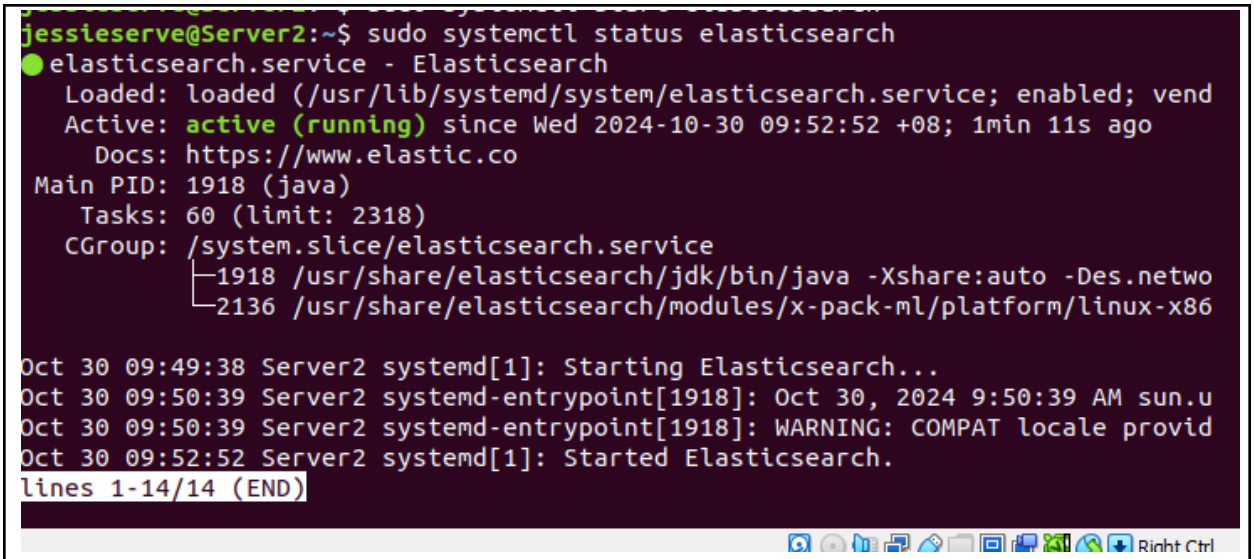
```
TASK [remote_servers_centos : install required packages (CentOS)] *************
*
changed: [192.168.56.108]

TASK [remote_servers_centos : Add Elasticsearch YUM repository (CentOS)] ******
*
changed: [192.168.56.108]

TASK [remote_servers_centos : Install Elasticsearch (Centos)] ****************
*
changed: [192.168.56.108]

TASK [remote_servers_centos : Copy Elasticsearch configuration file (Centos)] *
**
changed: [192.168.56.108]

TASK [remote_servers_centos : Install Kibana (Centos)] ***********************
```



Reflections:

Answer the following:

1. What are the benefits of having a log monitoring tool?
   It does help the system administrator gather, analyze, and even visualize the log data and thereby allow them to diagnose problems better, improve the security system, and eventually enhance its performance, so time would be saved for a better and more efficient system.

Conclusions:

I have now completely understood how to install, configure, and manage log monitoring software. These are very important for maintaining safety and welfare within computer systems. Log monitoring solutions are of utmost importance for day-to-day activities in this high-tech world where the reliability of data and system is at its top. They give real-time information about system performance.

Facilitate early issue detection and enhance security by allowing rapid identification and response to potential threats. The knowledge gathered from this activity is critical in ensuring that computer systems work securely and effectively within the modern digital environment.