Name: Tamayo, Ray Lan A.	**Date Performed: 11/12/2024**
Course/Section: CPE 212-CPE31S21	**Date Submitted: 11/12/2024**
Instructor: Engr. Robin Villanueva	**Semester and SY: First 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

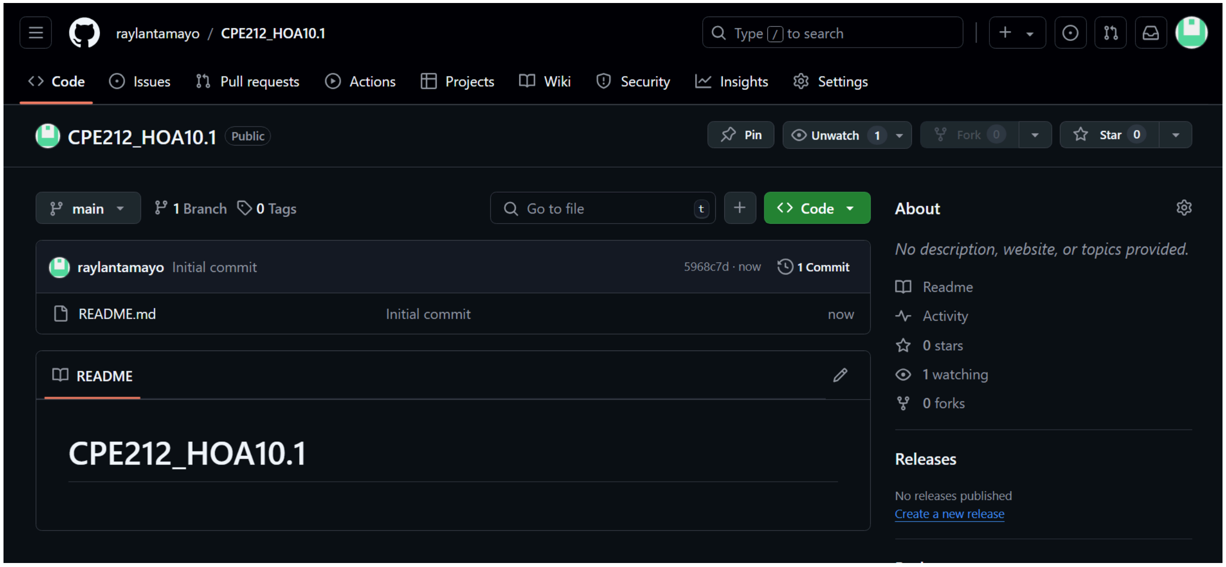
3. Tasks

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)

Task 1: Create a File

1. Create a new repository for this Hands-On Activity.



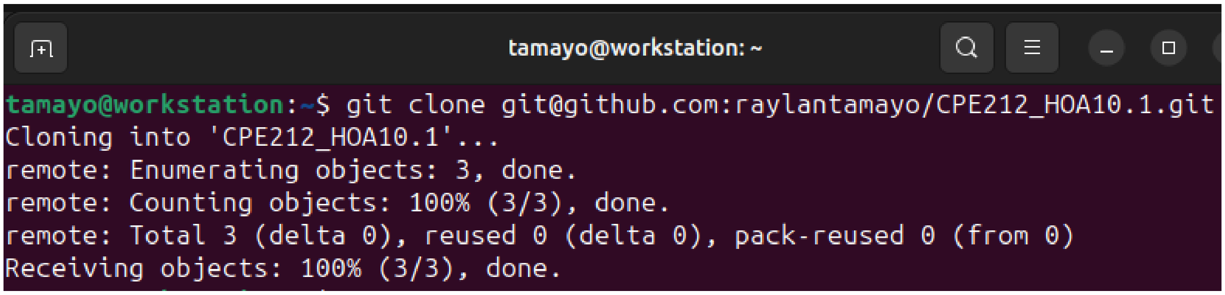
raylantamayo Initial commit 5968c7d · now 1 Commit

README.md Initial commit now

README

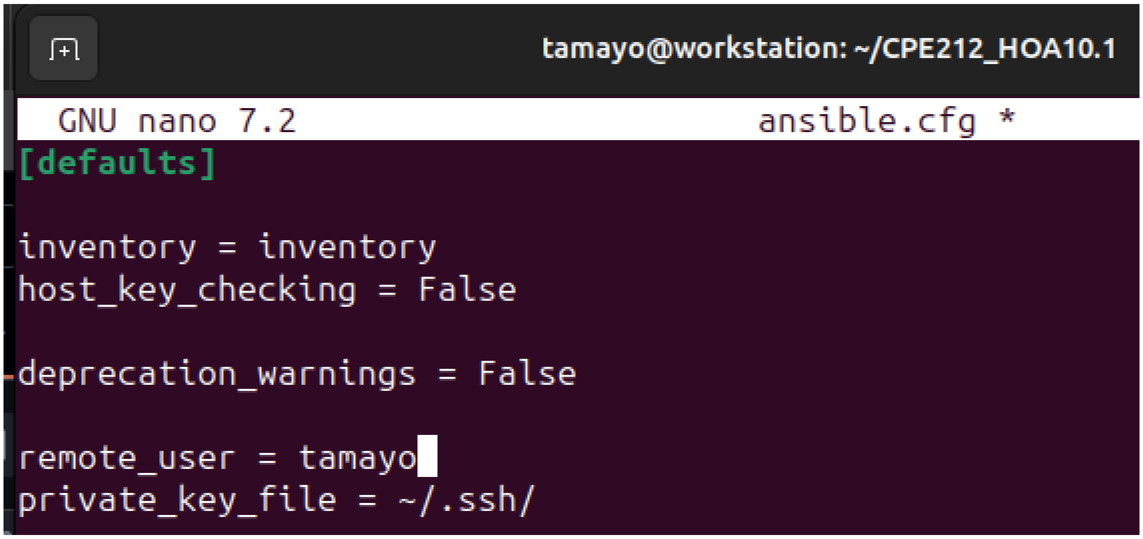
CPE212_HOA10.1

2. Clone the repository to the local machine.

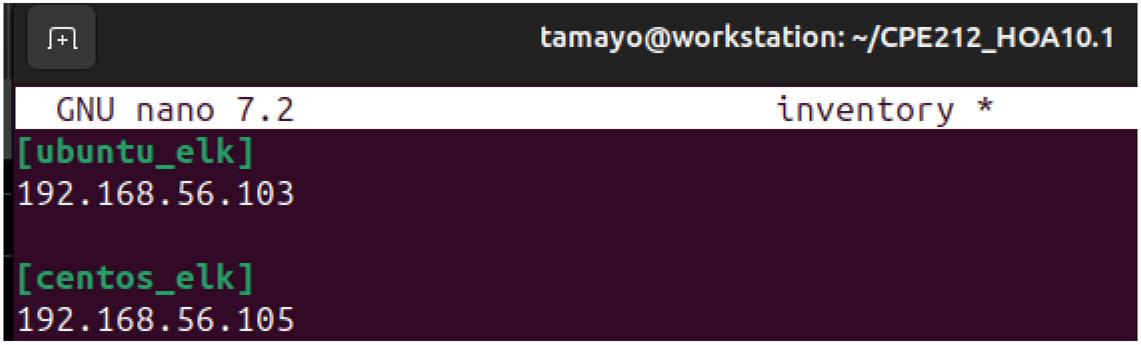


```
tamayo@workstation:~$ git clone git@github.com:raylantamayo/CPE212_HOA10.1.git
Cloning into 'CPE212_HOA10.1'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (3/3), done.
```

3. Create the ansible.cfg and inventory file (must include one Ubuntu and CentOS)



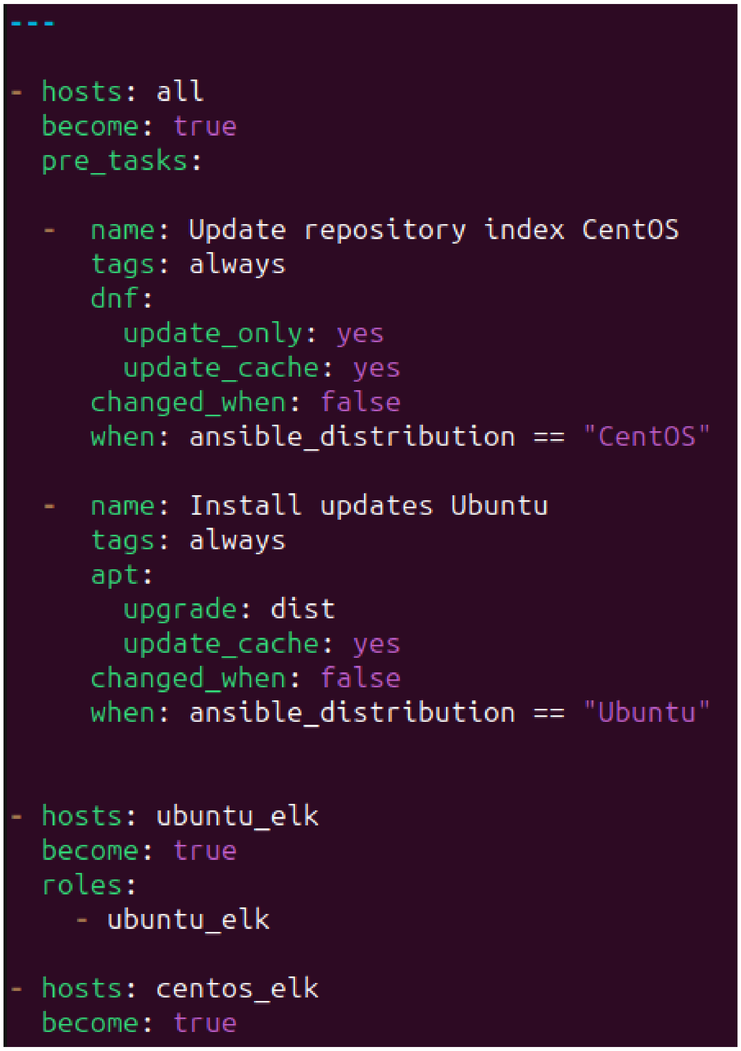
```
[defaults]

inventory = inventory
host_key_checking = False

deprecation_warnings = False

remote_user = tamayo
private_key_file = ~/.ssh/
```



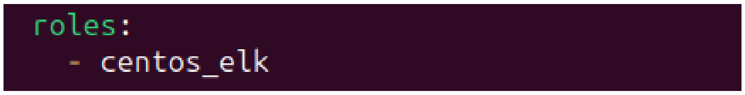
```
  GNU nano 7.2                           inventory *
[ubuntu_elk]
192.168.56.103

[centos_elk]
192.168.56.105
```

Task 2: Create Playbook for Installing ELK Stack in Ubuntu and CentOS

1. Create a playbook and name it install_elk.yml.

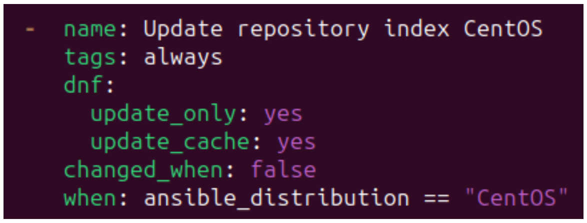


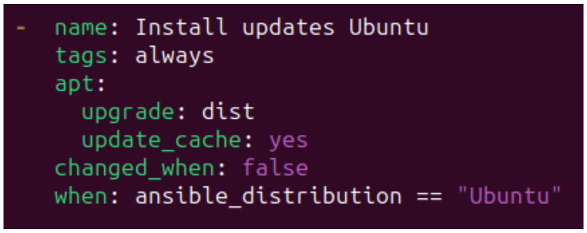
```
---

- hosts: all
  become: true
  pre_tasks:

  -  name: Update repository index CentOS
     tags: always
     dnf:
       update_only: yes
       update_cache: yes
     changed_when: false
     when: ansible_distribution == "CentOS"

  -  name: Install updates Ubuntu
     tags: always
     apt:
       upgrade: dist
       update_cache: yes
     changed_when: false
     when: ansible_distribution == "Ubuntu"


- hosts: ubuntu_elk
  become: true
  roles:
    - ubuntu_elk

- hosts: centos_elk
  become: true
```

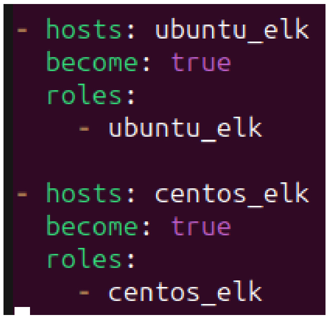


```
  roles:
    - centos_elk
```

Code explanation:

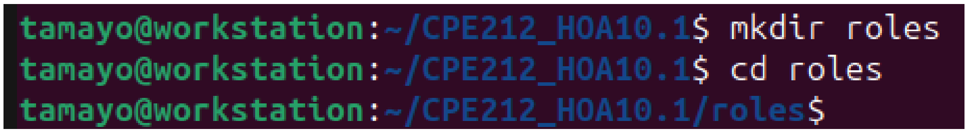
It refreshes the package cache (update_cache) as well as updtes only the installed packages (update_only). This task runs when the trget system is CentOS in order to make sure thatCentOS servers stay updated wth the latest package updates.	
	- name: Update repository index CentOS
	  tags: always
	  dnf:
	    update_only: yes
	    update_cache: yes
	  changed_when: false
	  when: ansible_distribution == "CentOS"

It upgrades all packages to their latest versions (upgrade: dist) and refreshes the package cache (update_cache). This task runs only when the target system is Ubuntu in order to make sure tht Ubuntu servers are kept updated with the latest package updates.	
	- name: Install updates Ubuntu
	  tags: always
	  apt:
	    upgrade: dist
	    update_cache: yes
	  changed_when: false
	  when: ansible_distribution == "Ubuntu"

It uses roles and the playbook first installs in Ubuntu and then in CentOS which allows ELK Stack monitoring on both. The "become: true" option grants administrative privileges to execute tasks.	 - hosts: ubuntu_elk become: true roles: - ubuntu_elk - hosts: centos_elk become: true roles: - centos_elk

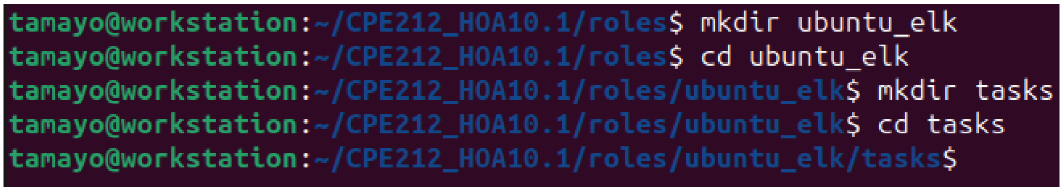
Task 3: Create Roles

1. Create a new directory and name it roles. Enter the roles directory and create new directories: centos_elk and ubuntu_elk. For each directory, create a directory and name it tasks.

.65  ’

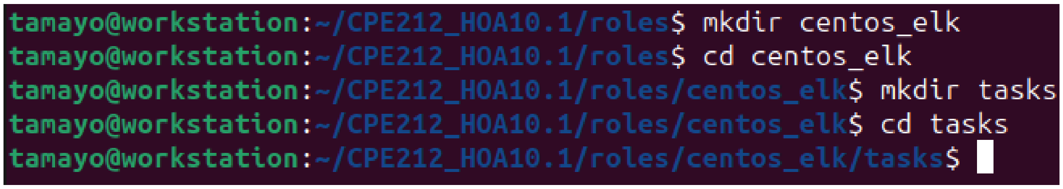
```
tamayo@workstation:~/CPE212_HOA10.1$ mkdir roles
tamayo@workstation:~/CPE212_HOA10.1$ cd roles
tamayo@workstation:~/CPE212_HOA10.1/roles$
```

FOR UBUNTU

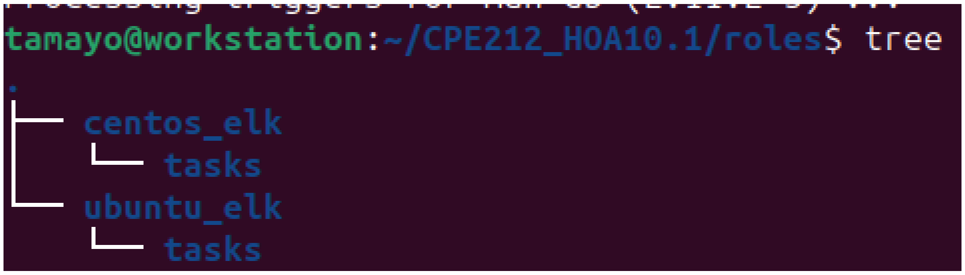


```
tamayo@workstation:~/CPE212_HOA10.1/roles$ mkdir ubuntu_elk
tamayo@workstation:~/CPE212_HOA10.1/roles$ cd ubuntu_elk
tamayo@workstation:~/CPE212_HOA10.1/roles/ubuntu_elk$ mkdir tasks
tamayo@workstation:~/CPE212_HOA10.1/roles/ubuntu_elk$ cd tasks
tamayo@workstation:~/CPE212_HOA10.1/roles/ubuntu_elk/tasks$
```

FOR CENTOS



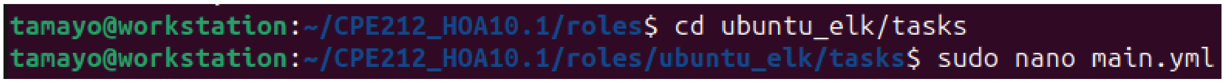
```
tamayo@workstation:~/CPE212_HOA10.1/roles$ mkdir centos_elk
tamayo@workstation:~/CPE212_HOA10.1/roles$ cd centos_elk
tamayo@workstation:~/CPE212_HOA10.1/roles/centos_elk$ mkdir tasks
tamayo@workstation:~/CPE212_HOA10.1/roles/centos_elk$ cd tasks
tamayo@workstation:~/CPE212_HOA10.1/roles/centos_elk/tasks$ 
```



```
tamayo@workstation:~/CPE212_HOA10.1/roles$ tree
.
├── centos_elk
│   └── tasks
└── ubuntu_elk
    └── tasks
```

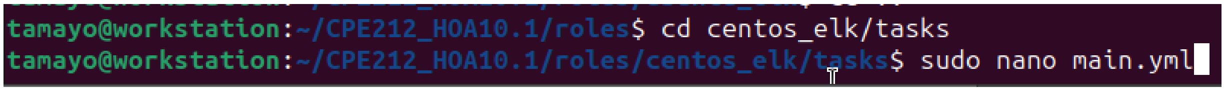
2. In each of the tasks for the two directory (centos_elk and ubuntu_elk), create another file and name it main.yml.

FOR UBUNTU

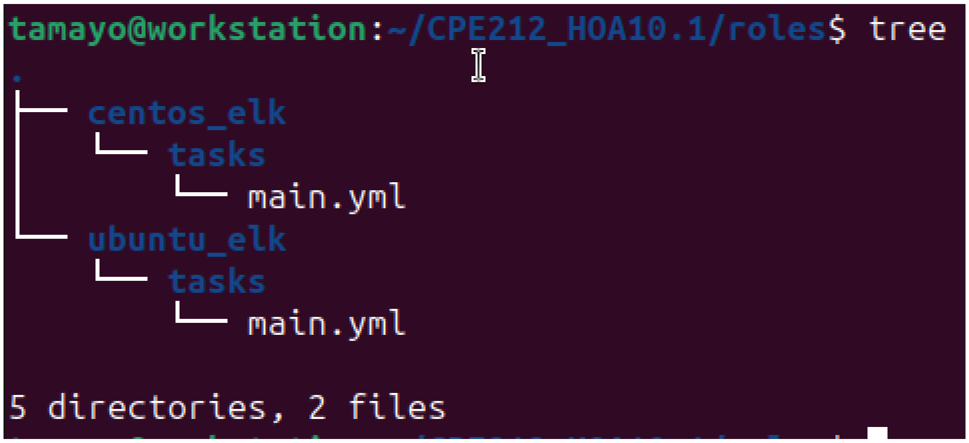


```
tamayo@workstation:~/CPE212_HOA10.1/roles$ cd ubuntu_elk/tasks
tamayo@workstation:~/CPE212_HOA10.1/roles/ubuntu_elk/tasks$ sudo nano main.yml
```

FOR CENTOS

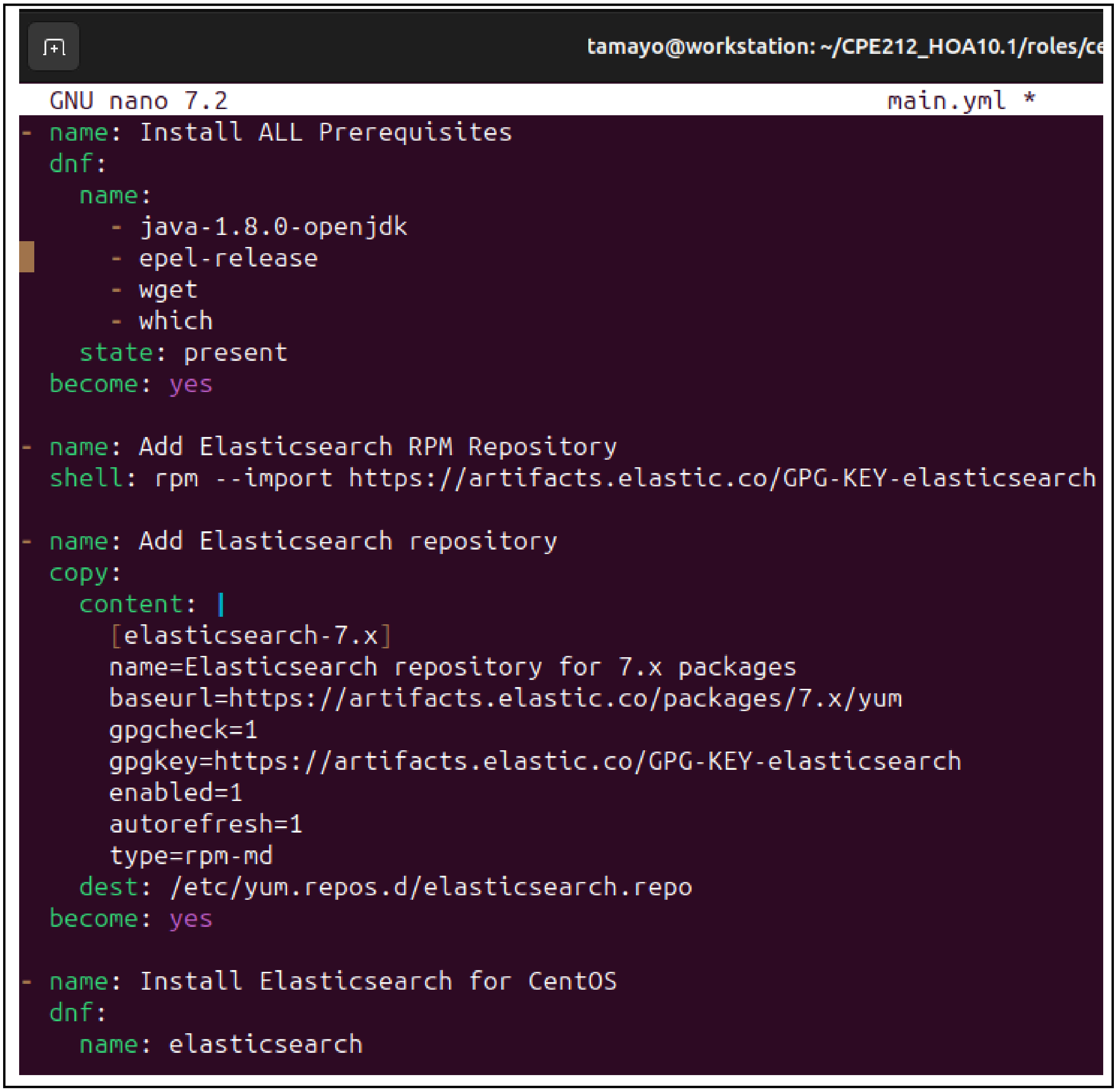


```
tamayo@workstation:~/CPE212_HOA10.1/roles$ cd centos_elk/tasks
tamayo@workstation:~/CPE212_HOA10.1/roles/centos_elk/tasks$ sudo nano main.yml
```



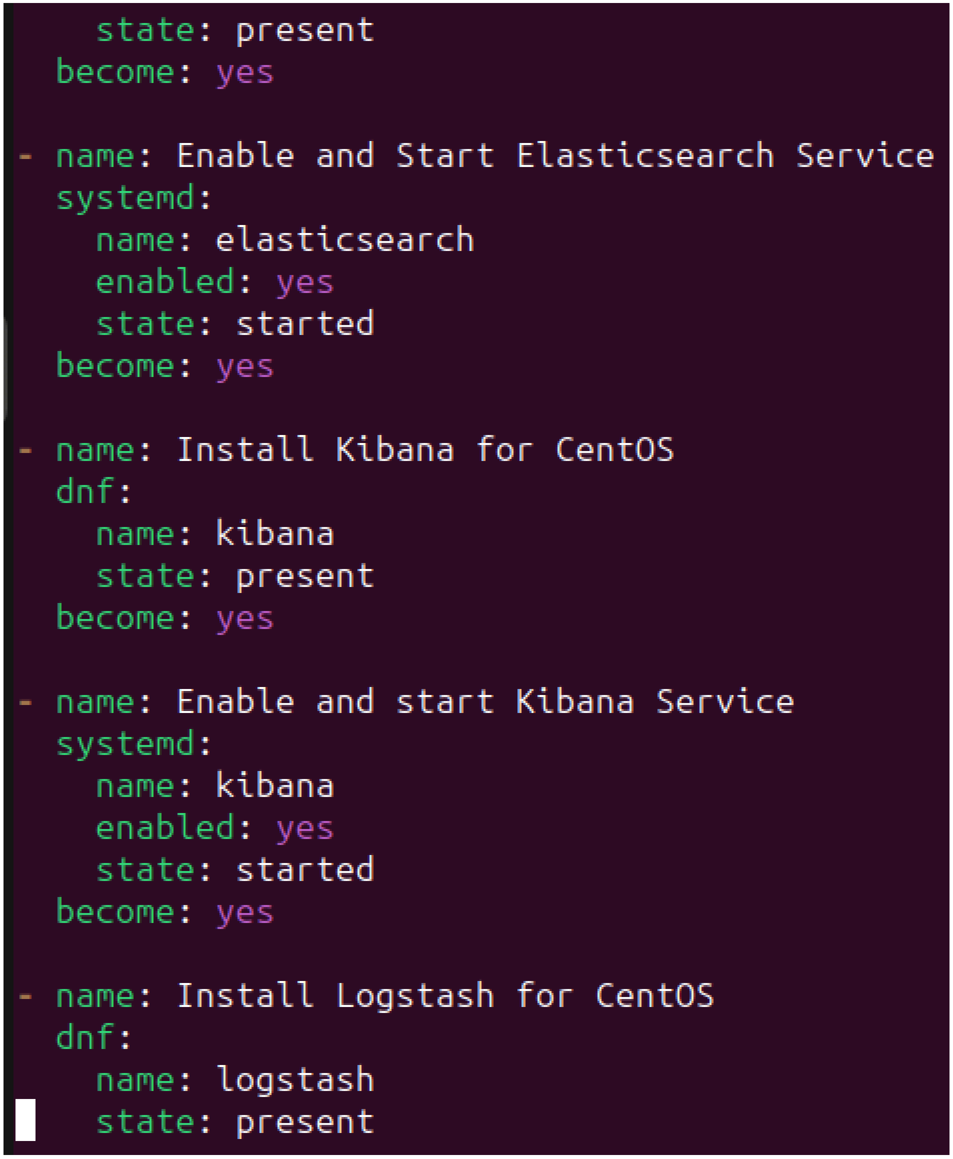
```
tamayo@workstation:~/CPE212_HOA10.1/roles$ tree
.
├── centos_elk
│   └── tasks
│       └── main.yml
└── ubuntu_elk
    └── tasks
        └── main.yml

5 directories, 2 files
```

3. Copy the code to the main.yml of the CentOS subdirectory.

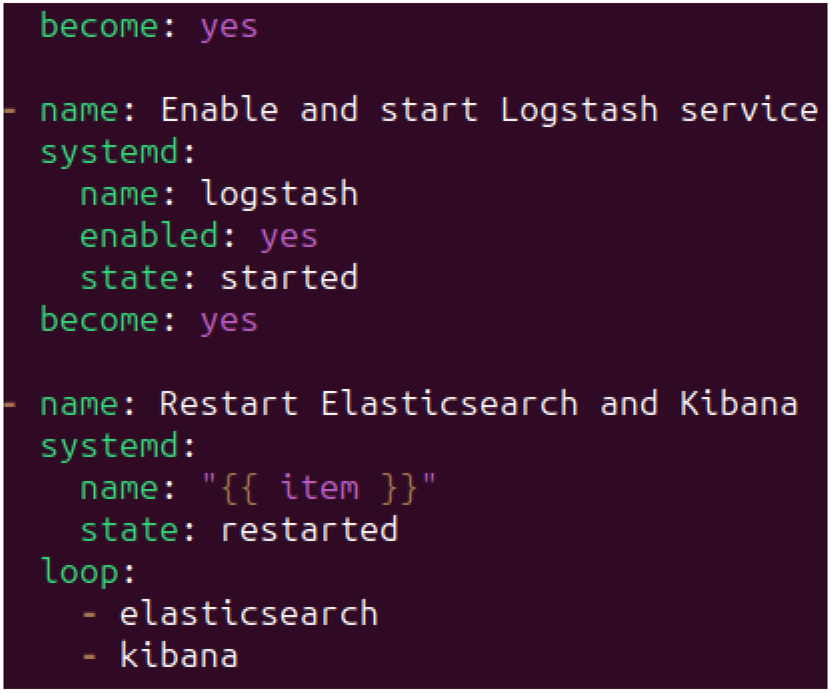


tamayo@workstation: ~/CPE212_HOA10.1/roles/ce

```
  GNU nano 7.2                                              main.yml *
- name: Install ALL Prerequisites
  dnf:
    name:
      - java-1.8.0-openjdk
      - epel-release
      - wget
      - which
    state: present
  become: yes

- name: Add Elasticsearch RPM Repository
  shell: rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

- name: Add Elasticsearch repository
  copy:
    content: |
      [elasticsearch-7.x]
      name=Elasticsearch repository for 7.x packages
      baseurl=https://artifacts.elastic.co/packages/7.x/yum
      gpgcheck=1
      gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
      enabled=1
      autorefresh=1
      type=rpm-md
    dest: /etc/yum.repos.d/elasticsearch.repo
  become: yes

- name: Install Elasticsearch for CentOS
  dnf:
    name: elasticsearch
```

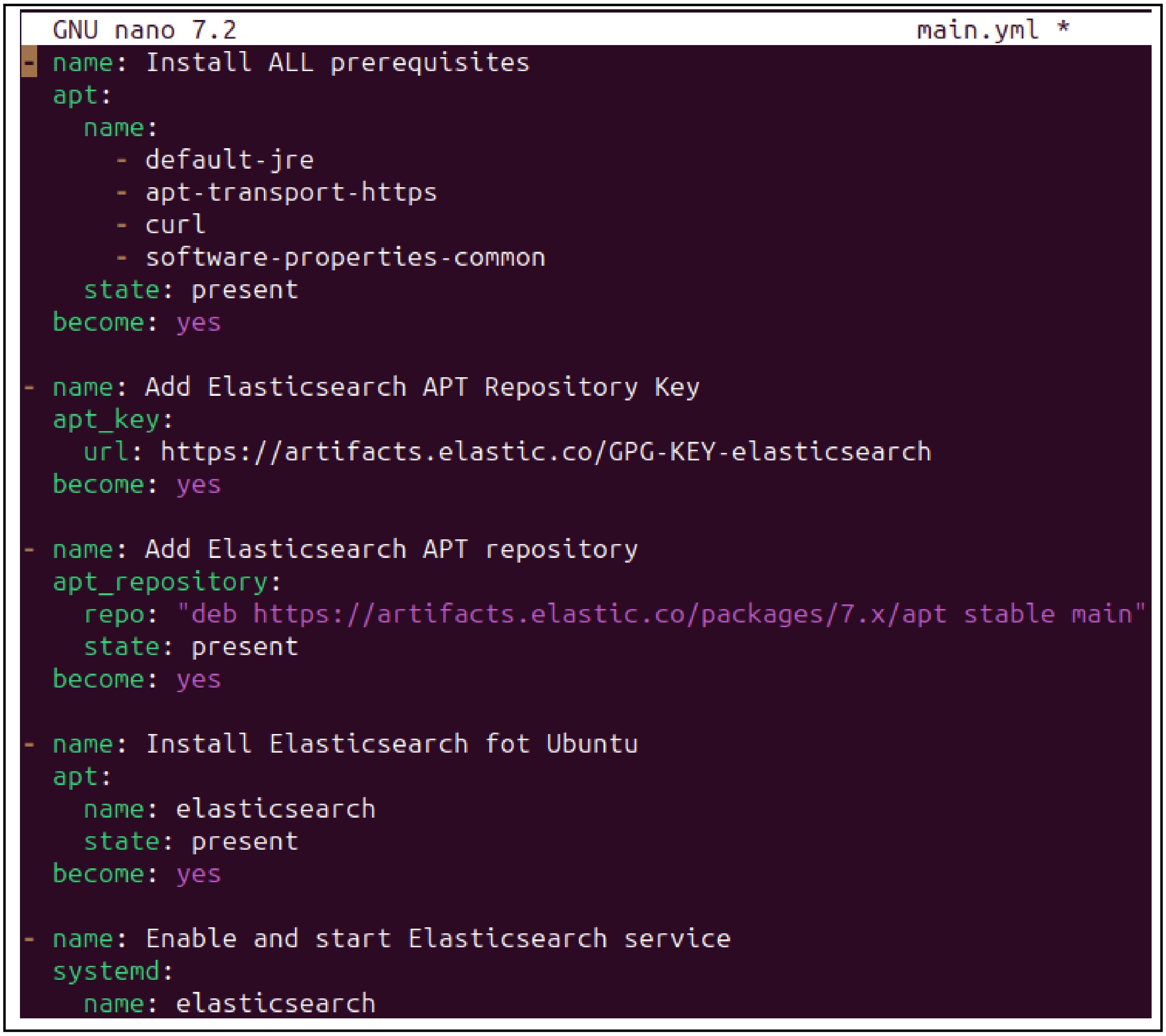


```
    state: present
  become: yes

- name: Enable and Start Elasticsearch Service
  systemd:
    name: elasticsearch
    enabled: yes
    state: started
  become: yes

- name: Install Kibana for CentOS
  dnf:
    name: kibana
    state: present
  become: yes

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

- name: Install Logstash for CentOS
  dnf:
    name: logstash
    state: present
```

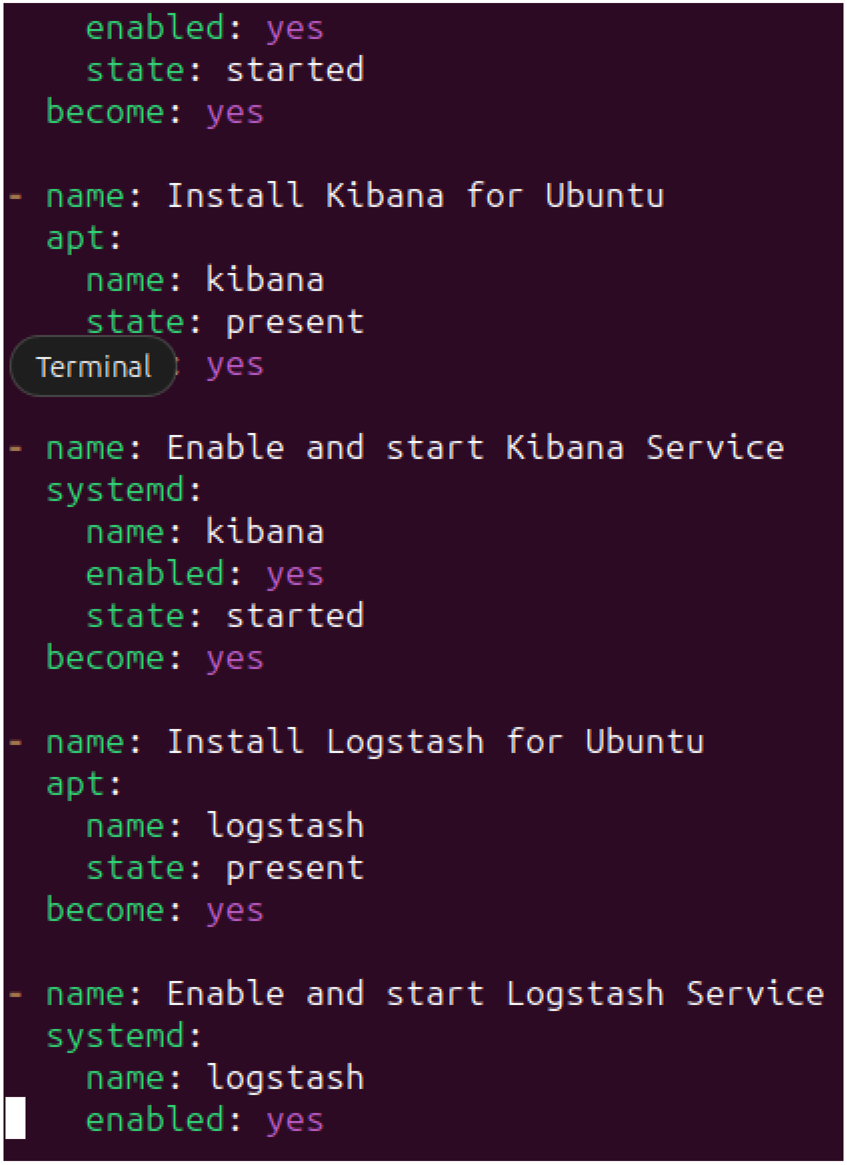


```yaml
  become: yes

- 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
```

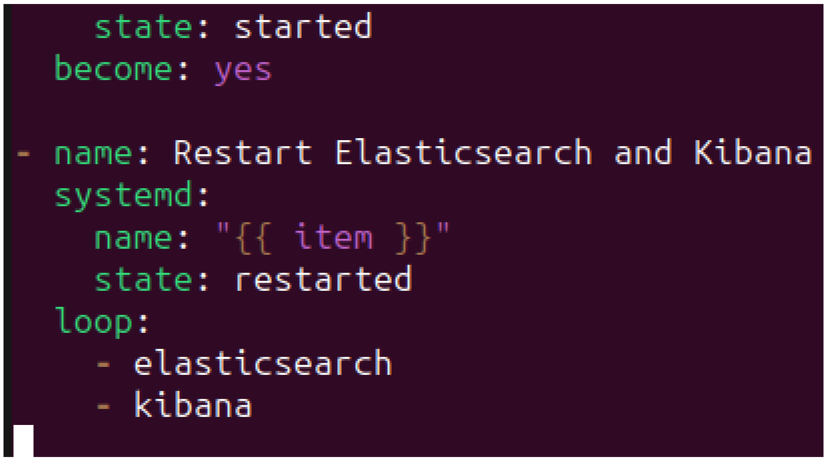
4. Copy the code to the main.yml of the Ubuntu subdirectory.



```
- name: Install ALL 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 fot Ubuntu
  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 for Ubuntu
  apt:
    name: kibana
    state: present
        : yes

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

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

- name: Enable and start Logstash Service
  systemd:
    name: logstash
    enabled: yes
```

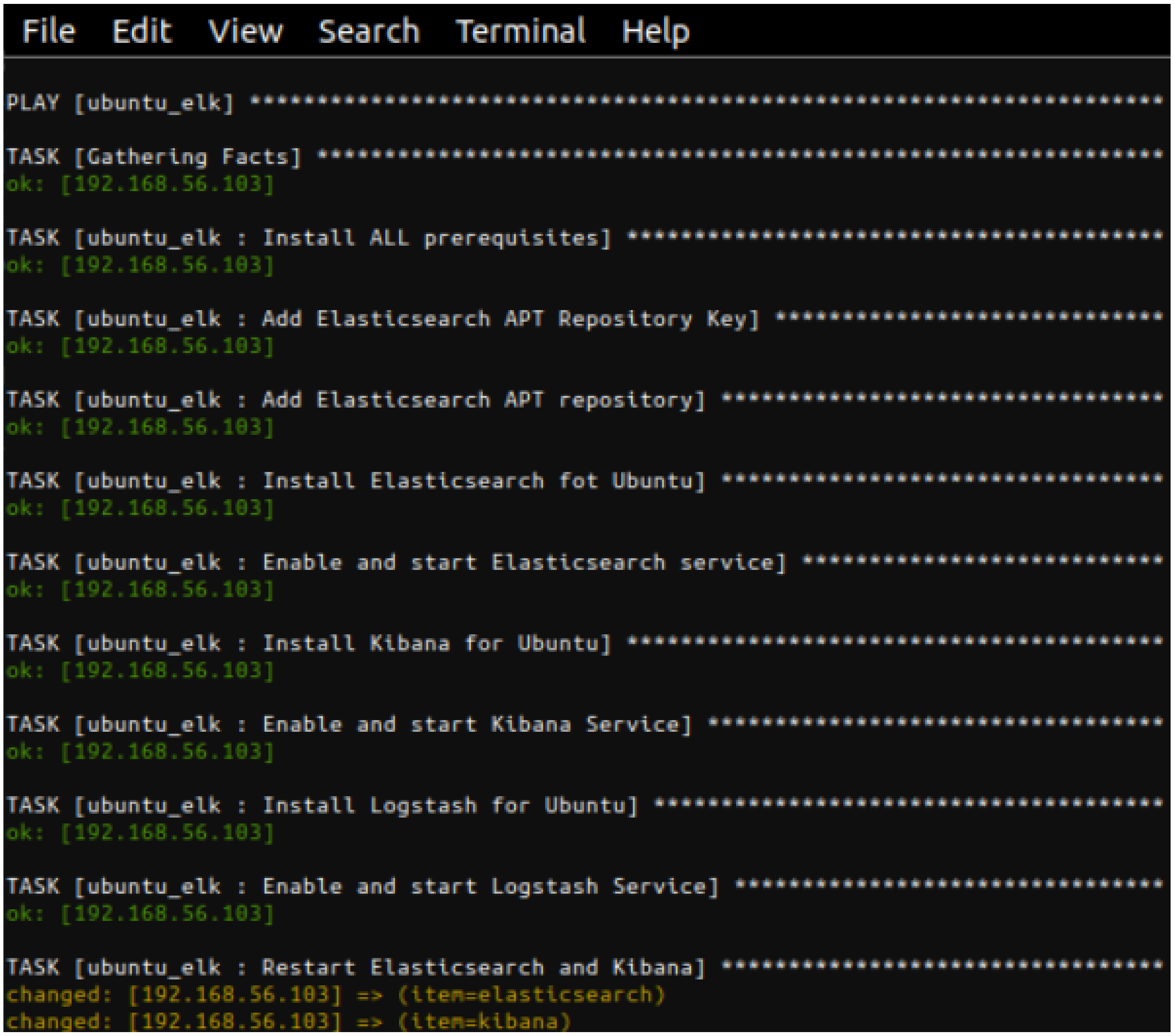


```
    state: started
  become: yes

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

Task 4: Run and Verify

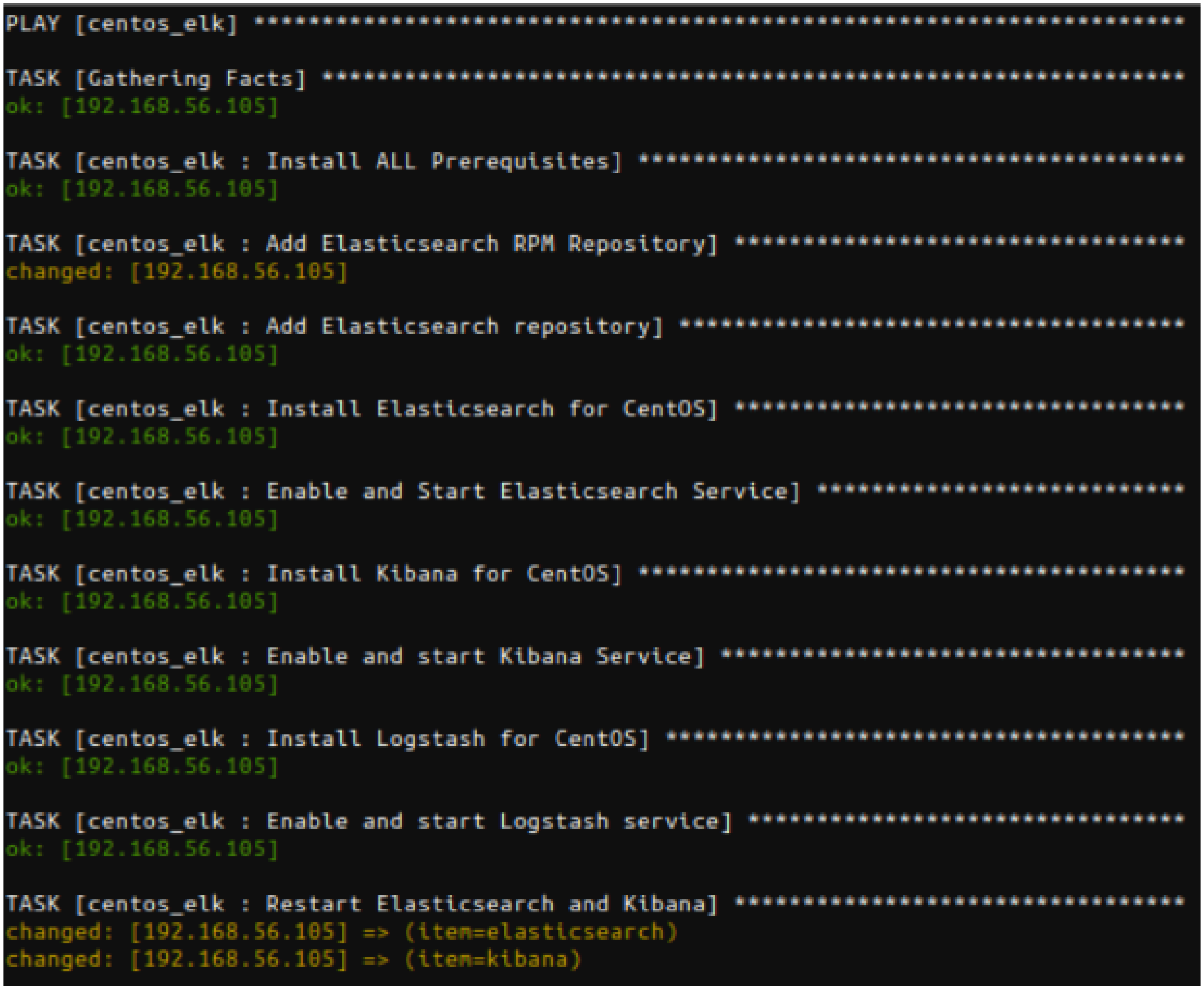
1. Run the command ansible-playbook - - ask-become-pass install_elk.yml to completely install ELK Stack in both Ubuntu server and CentOS.

UBUNTU_ELK



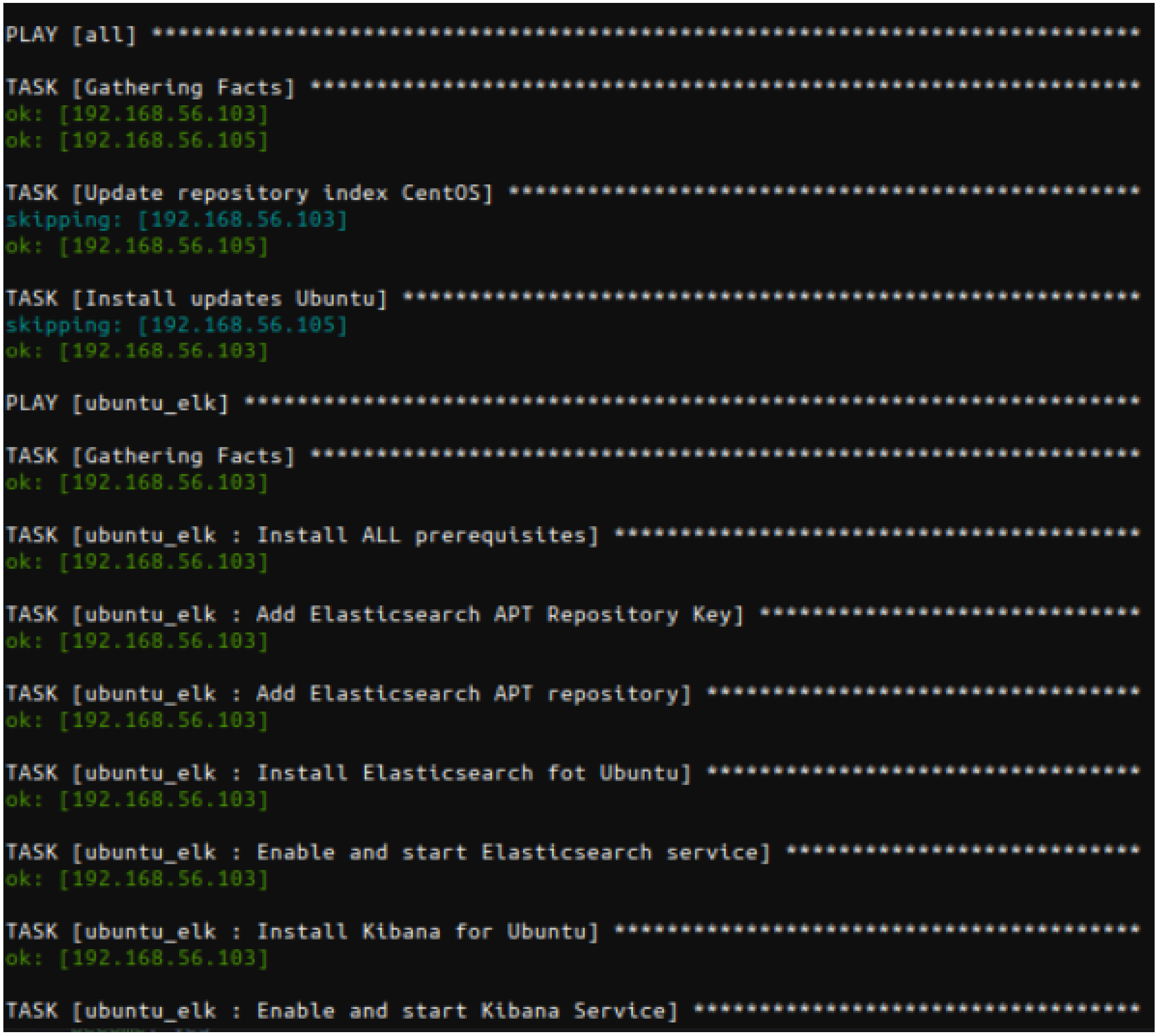
```
PLAY [ubuntu_elk] ********************************************************************

TASK [Gathering Facts] ***************************************************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Install ALL prerequisites] ****************************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Add Elasticsearch APT Repository Key] *****************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Add Elasticsearch APT repository] *********************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Install Elasticsearch fot Ubuntu] *********************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Enable and start Elasticsearch service] ***************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Install Kibana for Ubuntu] ****************************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Enable and start Kibana Service] **********************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Install Logstash for Ubuntu] **************************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Enable and start Logstash Service] ********************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Restart Elasticsearch and Kibana] *********************************
changed: [192.168.56.103] => (item=elasticsearch)
changed: [192.168.56.103] => (item=kibana)
```

CENTOS_ELK

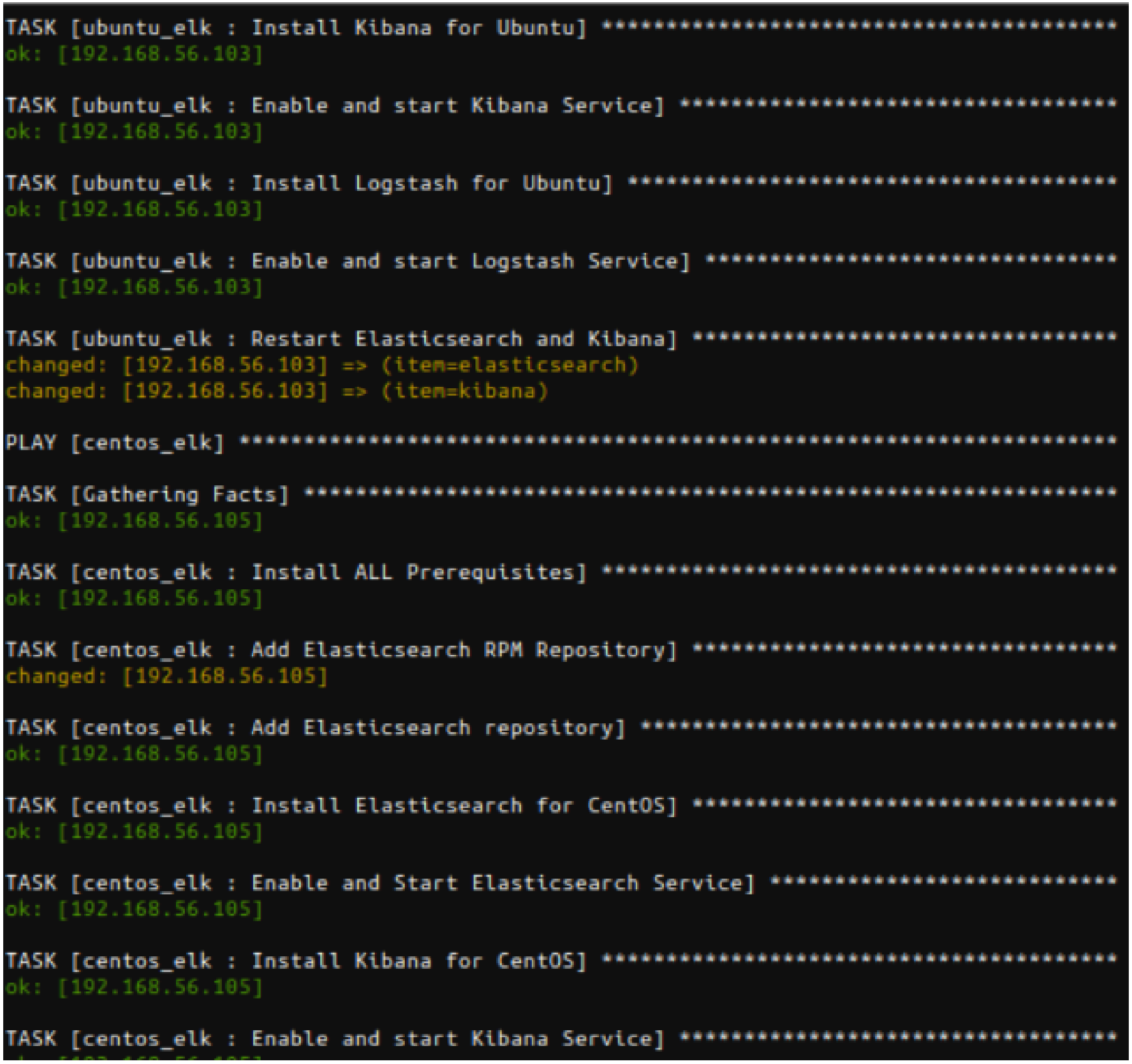


```
PLAY [centos_elk] ********************************************************************

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

TASK [centos_elk : Install ALL Prerequisites] ****************************************
ok: [192.168.56.105]

TASK [centos_elk : Add Elasticsearch RPM Repository] *********************************
changed: [192.168.56.105]

TASK [centos_elk : Add Elasticsearch repository] *************************************
ok: [192.168.56.105]

TASK [centos_elk : Install Elasticsearch for CentOS] *********************************
ok: [192.168.56.105]

TASK [centos_elk : Enable and Start Elasticsearch Service] ***************************
ok: [192.168.56.105]

TASK [centos_elk : Install Kibana for CentOS] ****************************************
ok: [192.168.56.105]

TASK [centos_elk : Enable and start Kibana Service] **********************************
ok: [192.168.56.105]

TASK [centos_elk : Install Logstash for CentOS] **************************************
ok: [192.168.56.105]

TASK [centos_elk : Enable and start Logstash service] ********************************
ok: [192.168.56.105]

TASK [centos_elk : Restart Elasticsearch and Kibana] *********************************
changed: [192.168.56.105] => (item=elasticsearch)
changed: [192.168.56.105] => (item=kibana)
```

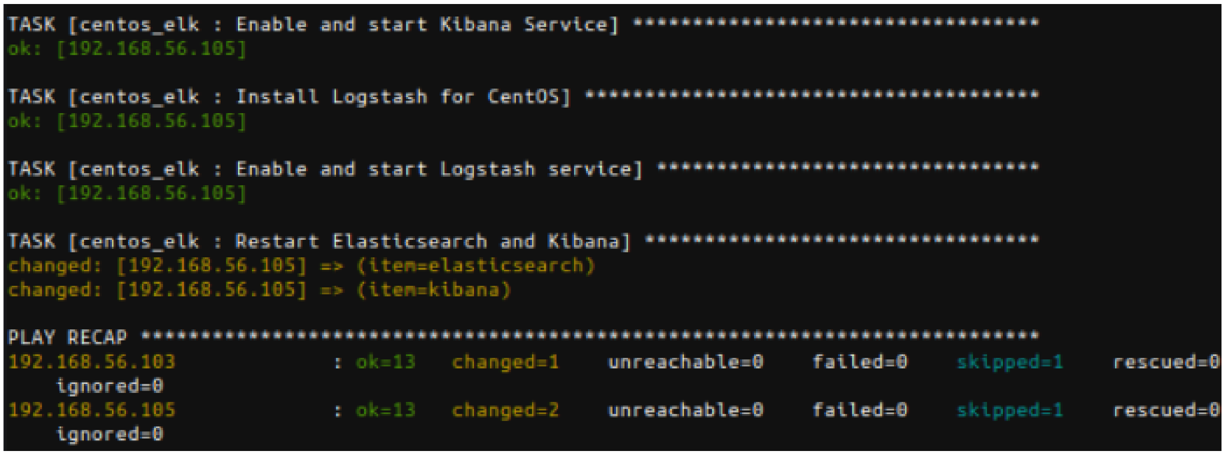
ENTIRE ansible-playbook



```
PLAY [all] ***************************************************************************

TASK [Gathering Facts] ***************************************************************
ok: [192.168.56.103]
ok: [192.168.56.105]

TASK [Update repository index CentOS] ************************************************
skipping: [192.168.56.103]
ok: [192.168.56.105]

TASK [Install updates Ubuntu] ********************************************************
skipping: [192.168.56.105]
ok: [192.168.56.103]

PLAY [ubuntu_elk] ********************************************************************

TASK [Gathering Facts] ***************************************************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Install ALL prerequisites] ****************************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Add Elasticsearch APT Repository Key] *****************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Add Elasticsearch APT repository] *********************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Install Elasticsearch fot Ubuntu] *********************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Enable and start Elasticsearch service] ***************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Install Kibana for Ubuntu] ****************************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Enable and start Kibana Service] **********************************
```



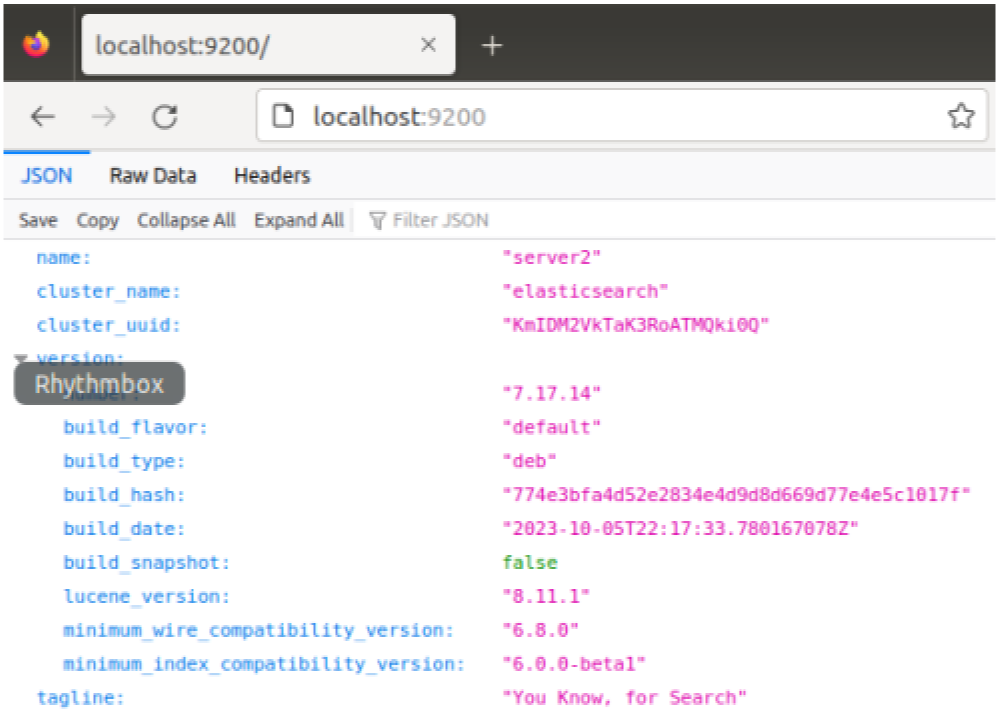
```
TASK [ubuntu_elk : Install Kibana for Ubuntu] ****************************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Enable and start Kibana Service] **********************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Install Logstash for Ubuntu] **************************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Enable and start Logstash Service] ********************************
ok: [192.168.56.103]

TASK [ubuntu_elk : Restart Elasticsearch and Kibana] *********************************
changed: [192.168.56.103] => (item=elasticsearch)
changed: [192.168.56.103] => (item=kibana)

PLAY [centos_elk] ********************************************************************

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

TASK [centos_elk : Install ALL Prerequisites] ****************************************
ok: [192.168.56.105]

TASK [centos_elk : Add Elasticsearch RPM Repository] *********************************
changed: [192.168.56.105]

TASK [centos_elk : Add Elasticsearch repository] *************************************
ok: [192.168.56.105]

TASK [centos_elk : Install Elasticsearch for CentOS] *********************************
ok: [192.168.56.105]

TASK [centos_elk : Enable and Start Elasticsearch Service] ***************************
ok: [192.168.56.105]

TASK [centos_elk : Install Kibana for CentOS] ****************************************
ok: [192.168.56.105]

TASK [centos_elk : Enable and start Kibana Service] **********************************
```



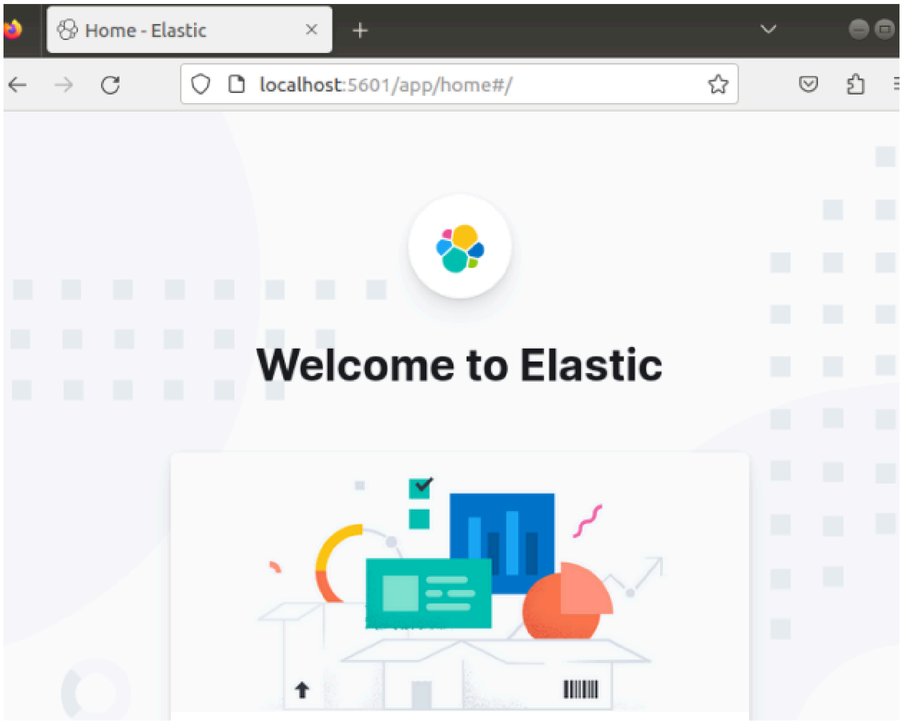
```
TASK [centos_elk : Enable and start Kibana Service] **********************************
ok: [192.168.56.105]

TASK [centos_elk : Install Logstash for CentOS] **************************************
ok: [192.168.56.105]

TASK [centos_elk : Enable and start Logstash service] ********************************
ok: [192.168.56.105]

TASK [centos_elk : Restart Elasticsearch and Kibana] *********************************
changed: [192.168.56.105] => (item=elasticsearch)
changed: [192.168.56.105] => (item=kibana)

PLAY RECAP ***************************************************************************
192.168.56.103             : ok=13   changed=1    unreachable=0    failed=0    skipped=1    rescued=0
    ignored=0
192.168.56.105             : ok=13   changed=2    unreachable=0    failed=0    skipped=1    rescued=0
    ignored=0
```

2. Show the screenshot of the ELK Stack in both Server 2 and CentOS by simply typing localhost:5601 in the web browser

SERVER2 (Kibana, Elasticsearch, Logstash)

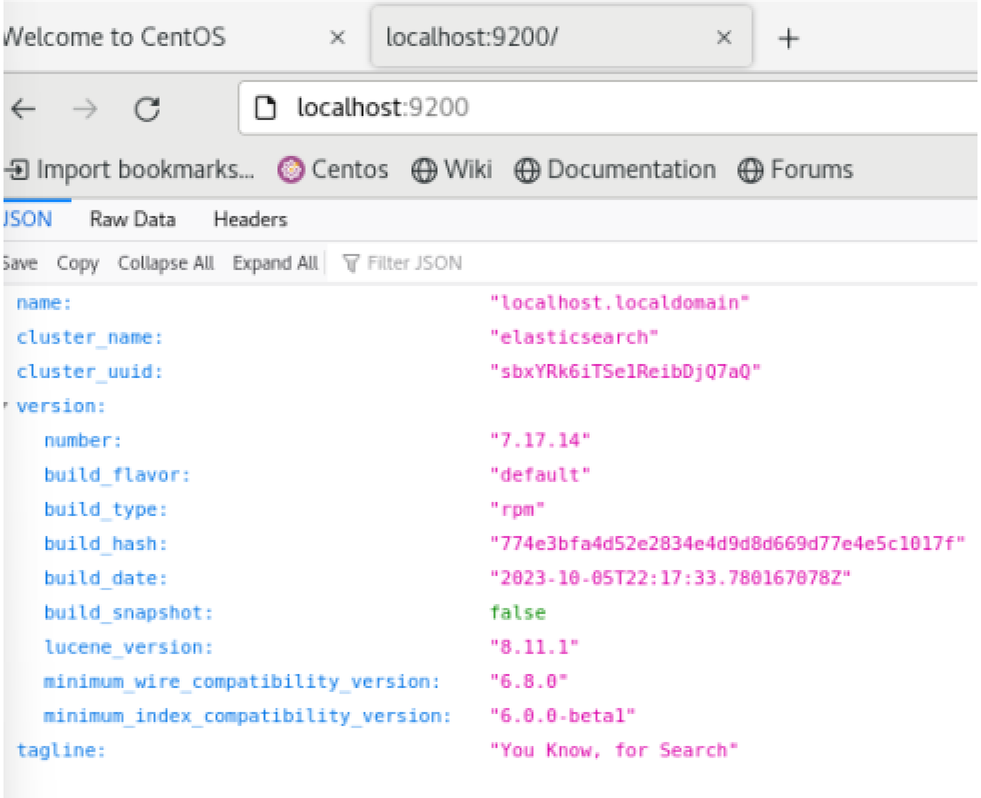


```
name:                                   "server2"
cluster_name:                           "elasticsearch"
cluster_uuid:                           "KmIDM2VkTaK3RoATMQki0Q"
version:
                                        "7.17.14"
    build_flavor:                       "default"
    build_type:                         "deb"
    build_hash:                         "774e3bfa4d52e2834e4d9d8d669d77e4e5c1017f"
    build_date:                         "2023-10-05T22:17:33.780167078Z"
    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"
```

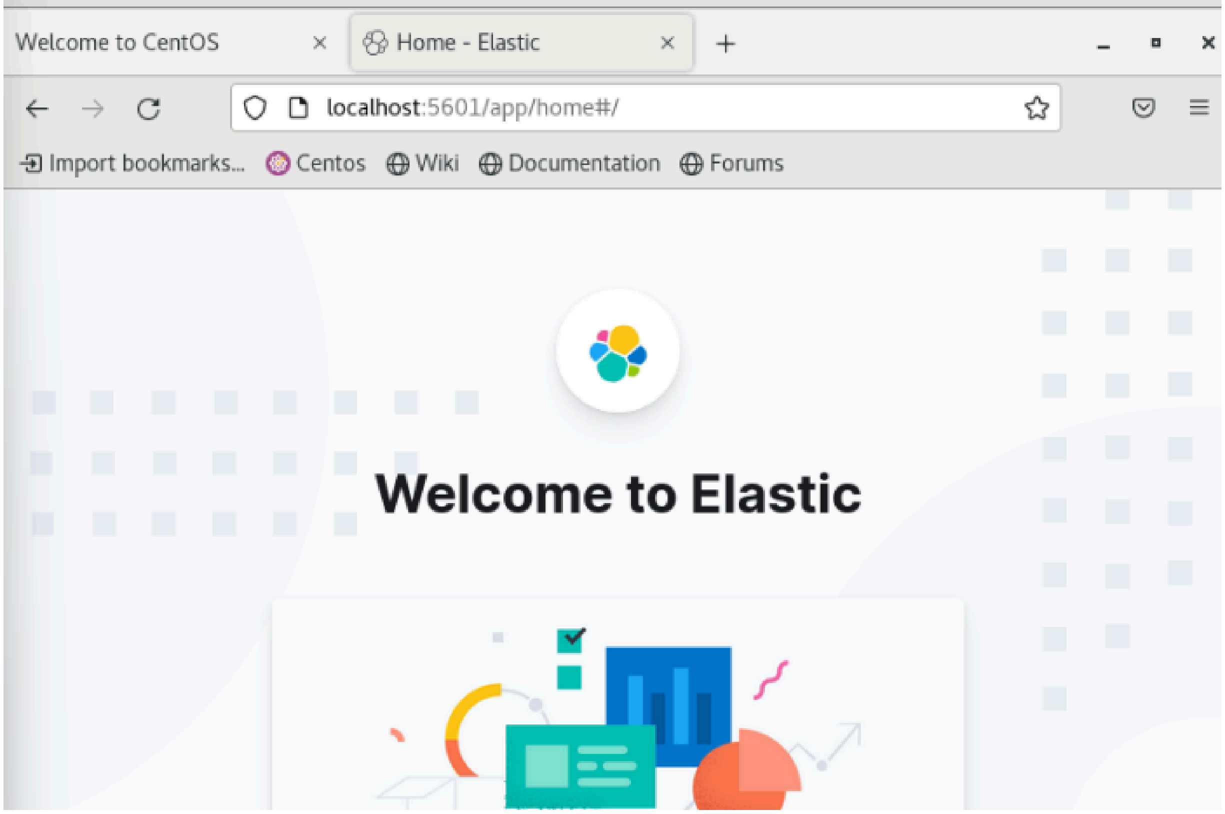


Welcome to Elastic

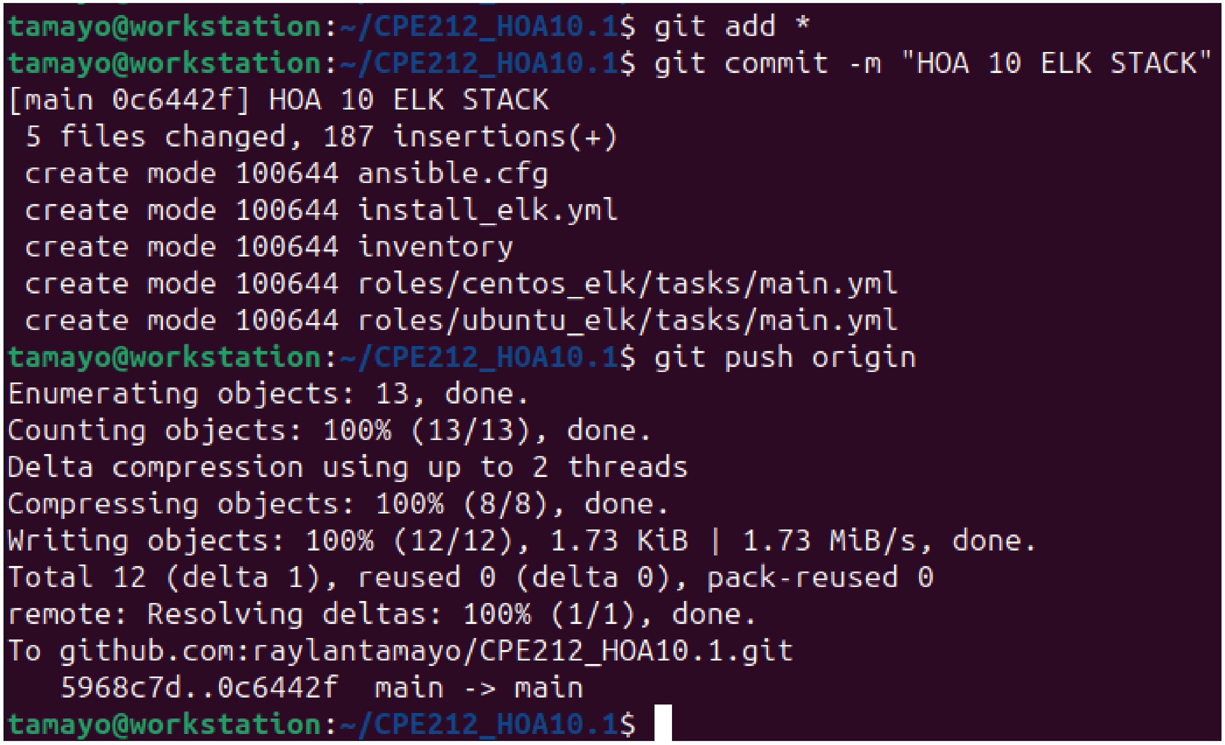
CENTOS (Kibana, Elasticsearch, Logstash)



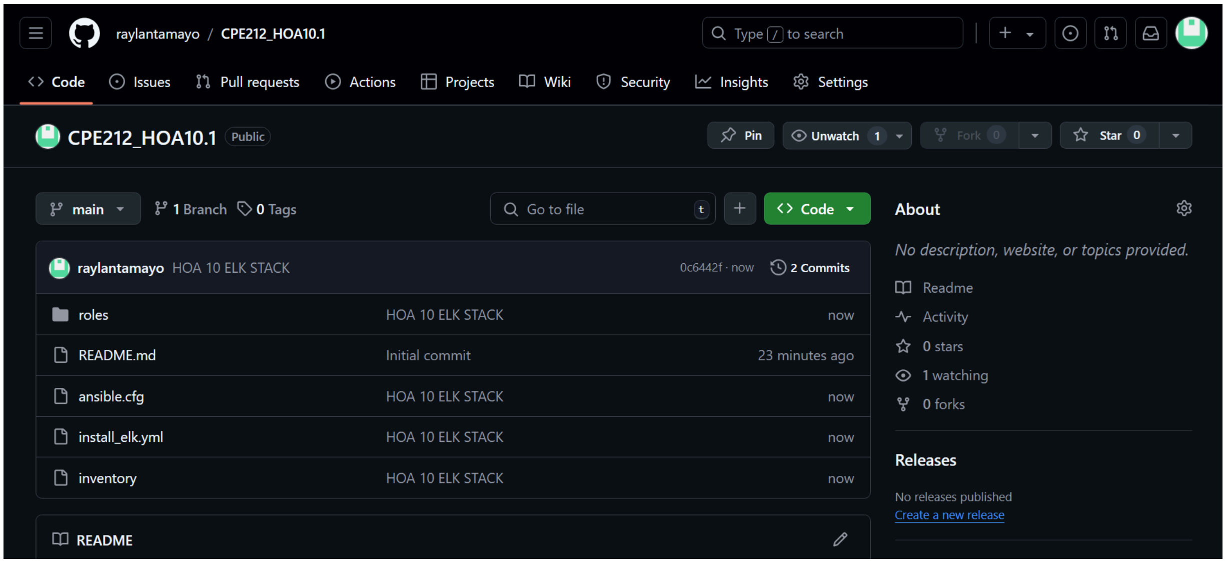
```
name:                                  "localhost.localdomain"
cluster_name:                          "elasticsearch"
cluster_uuid:                          "sbxYRk6iTSe1ReibDjQ7aQ"
version:
  number:                              "7.17.14"
  build_flavor:                        "default"
  build_type:                          "rpm"
  build_hash:                          "774e3bfa4d52e2834e4d9d8d669d77e4e5c1017f"
  build_date:                          "2023-10-05T22:17:33.780167078Z"
  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"
```



Welcome to Elastic



```
tamayo@workstation:~/CPE212_HOA10.1$ git add *
tamayo@workstation:~/CPE212_HOA10.1$ git commit -m "HOA 10 ELK STACK"
[main 0c6442f] HOA 10 ELK STACK
 5 files changed, 187 insertions(+)
 create mode 100644 ansible.cfg
 create mode 100644 install_elk.yml
 create mode 100644 inventory
 create mode 100644 roles/centos_elk/tasks/main.yml
 create mode 100644 roles/ubuntu_elk/tasks/main.yml
tamayo@workstation:~/CPE212_HOA10.1$ git push origin
Enumerating objects: 13, done.
Counting objects: 100% (13/13), done.
Delta compression using up to 2 threads
Compressing objects: 100% (8/8), done.
Writing objects: 100% (12/12), 1.73 KiB | 1.73 MiB/s, done.
Total 12 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), done.
To github.com:raylantamayo/CPE212_HOA10.1.git
   5968c7d..0c6442f  main -> main
tamayo@workstation:~/CPE212_HOA10.1$ 
```



No description, website, or topics provided.

No releases published

raylantamayo HOA 10 ELK STACK 0c6442f · now 2 Commits

roles	HOA 10 ELK STACK	now
README.md	Initial commit	23 minutes ago
ansible.cfg	HOA 10 ELK STACK	now
install_elk.yml	HOA 10 ELK STACK	now
inventory	HOA 10 ELK STACK	now

https://github.com/raylantamayo/CPE212_HOA10.1.git

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool?

   Log monitoring tools, like logstash, bring two crucial advantages to both Ubuntu and CentOS systems. Firstly, they bolster security by identifying and alerting administrators to unusual or potentially malicious activities in system logs, helping

prevent security breaches. Secondly, these tools simplify troubleshooting by offering insights into system performance and errors, enabling faster issue resolution and enhancing overall system reliability.
Conclusions: **In this activity, I was able to encounter the elastic search, kibana, and also the logstash. I haven't heard of these three words before.This activity focused on installation of the Elastic Stack components like thge elasticsearch, kibana, and logstash in both Ubuntu and CentOS has been a highly beneficial and enlightening endeavor. These three tools play pivotal roles in our system management. Elasticsearch efficiently stores and retrieves data, while Logstash acts as the data processing powerhouse, and Kibana offers a user-friendly interface for data visualization. This trio empowers us to analyze system logs comprehensively, ensuring system security, optimizing performance, and expediting issue resolution. Their seamless integration and functionality have undoubtedly elevated our system administration, making it a vital investment for any organization. Overall, I had fun doing this activity but I felt pressured this time since I worked on this activity for a very short period of time.**