Name: Jaira Biane Maculada	**Date Performed:**10/23/23
Course/Section: CPE232/CPE31S6	**Date Submitted:**10/23/23
Instructor: Dr. Jonathan V. Taylar	**Semester and SY:** 1st Sem(2023-2024)

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

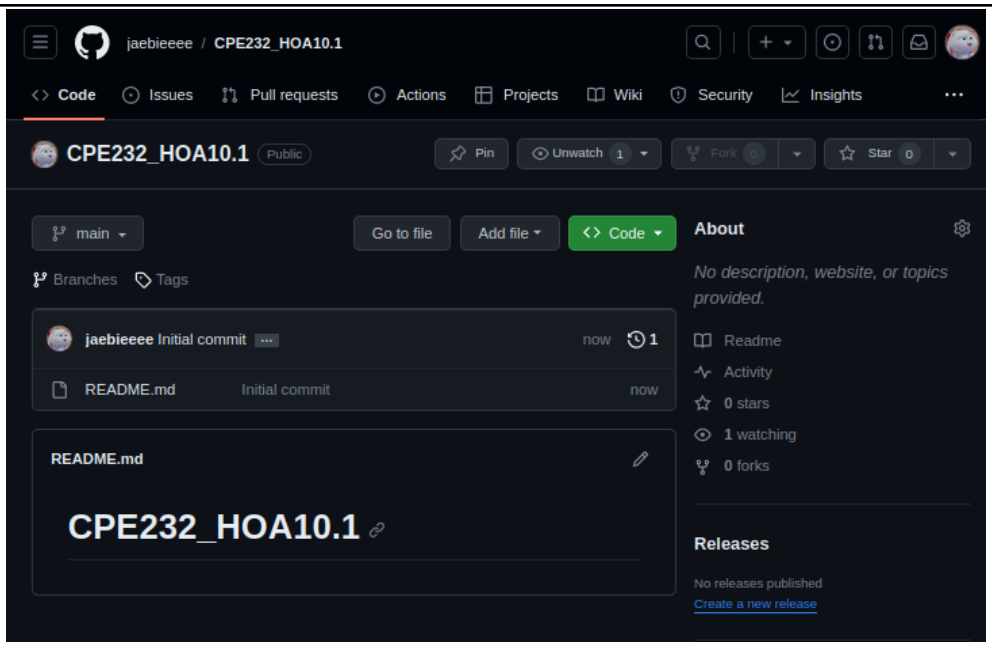
3. Tasks

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.

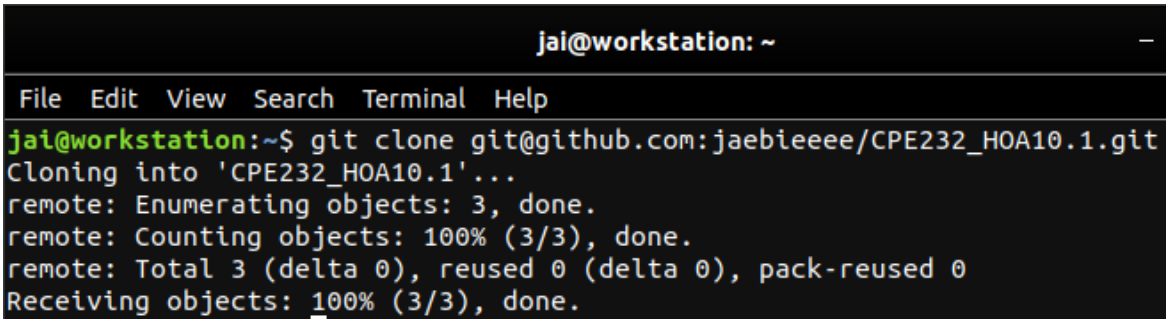
4. Output (screenshots and explanations)

Task 1: Create a File

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



2. Clone the repository to the local machine.



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

```
jai@workstation: ~/CPE232_HOA10.1
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                          ansible.cfg

[defaults]

inventory = inventory
host_key_checking = False

deprecation_warnings = False

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

```
jai@workstation: ~/CPE232_HOA10.1
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                          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

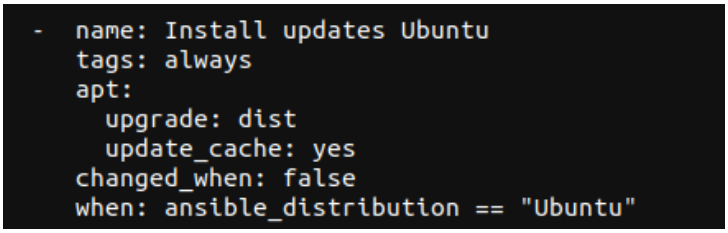
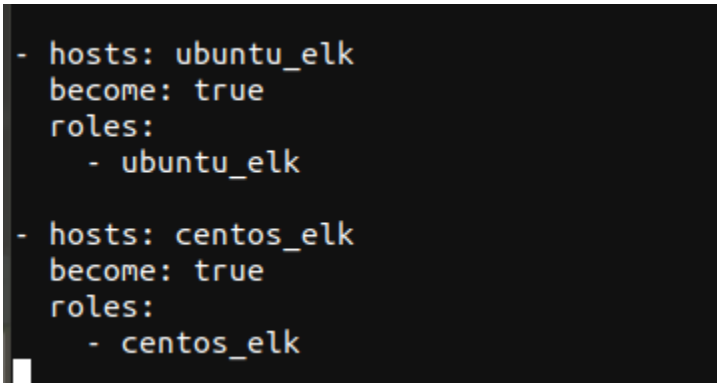
1. Create a playbook and name it install_elk.yml.

```
jai@workstation: ~/CPE232_HOA10.1
File  Edit  View  Search  Terminal  Help
 GNU nano 2.9.3                    install_elk.yml
---

- hosts: all
  become: true
  pre_tasks:

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

package updates.	
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.	
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.	

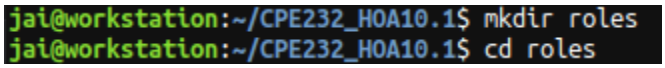
```
- name: Install updates Ubuntu
  tags: always
  apt:
    upgrade: dist
    update_cache: yes
  changed_when: false
  when: ansible_distribution == "Ubuntu"
```

```
- hosts: ubuntu_elk
  become: true
  roles:
    - ubuntu_elk

- hosts: centos_elk
  become: true
  roles:
    - centos_elk
```

2. Save the file and exit.

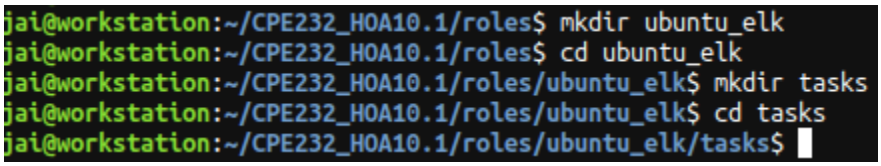
Task 3: Create Roles

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.



```
jai@workstation:~/CPE232_HOA10.1$ mkdir roles
jai@workstation:~/CPE232_HOA10.1$ cd roles
```

FOR UBUNTU



```
jai@workstation:~/CPE232_HOA10.1/roles$ mkdir ubuntu_elk
jai@workstation:~/CPE232_HOA10.1/roles$ cd ubuntu_elk
jai@workstation:~/CPE232_HOA10.1/roles/ubuntu_elk$ mkdir tasks
jai@workstation:~/CPE232_HOA10.1/roles/ubuntu_elk$ cd tasks
jai@workstation:~/CPE232_HOA10.1/roles/ubuntu_elk/tasks$
```

FOR CENTOS

```
jai@workstation:~/CPE232_HOA10.1/roles$ mkdir centos_elk
jai@workstation:~/CPE232_HOA10.1/roles$ cd centos_elk
jai@workstation:~/CPE232_HOA10.1/roles/centos_elk$ mkdir tasks
jai@workstation:~/CPE232_HOA10.1/roles/centos_elk$ cd tasks
jai@workstation:~/CPE232_HOA10.1/roles/centos_elk/tasks$
```

```
jai@workstation:~/CPE232_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

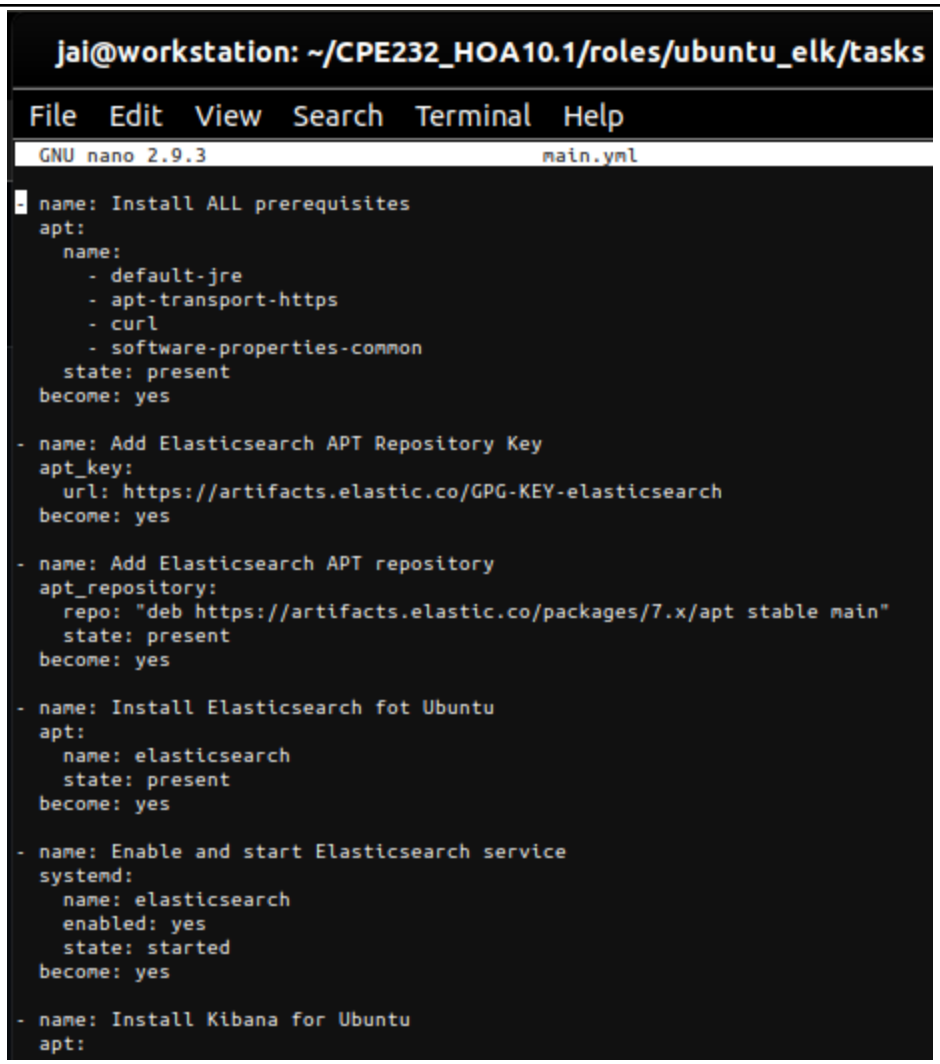
```
jai@workstation:~/CPE232_HOA10.1/roles$ cd ubuntu_elk/tasks
jai@workstation:~/CPE232_HOA10.1/roles/ubuntu_elk/tasks$ sudo nano main.yml
```

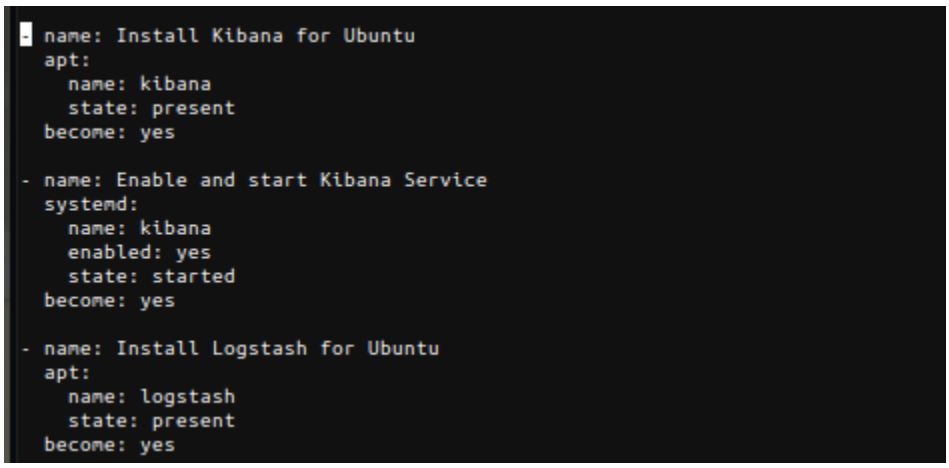
FOR CENTOS

```
jai@workstation:~/CPE232_HOA10.1/roles$ cd centos_elk/tasks
jai@workstation:~/CPE232_HOA10.1/roles/centos_elk/tasks$ sudo nano main.yml
```

```
jai@workstation:~/CPE232_HOA10.1/roles$ tree
.
├── centos_elk
│   └── tasks
│       └── main.yml
└── ubuntu_elk
    └── tasks
        └── main.yml

4 directories, 2 files
```

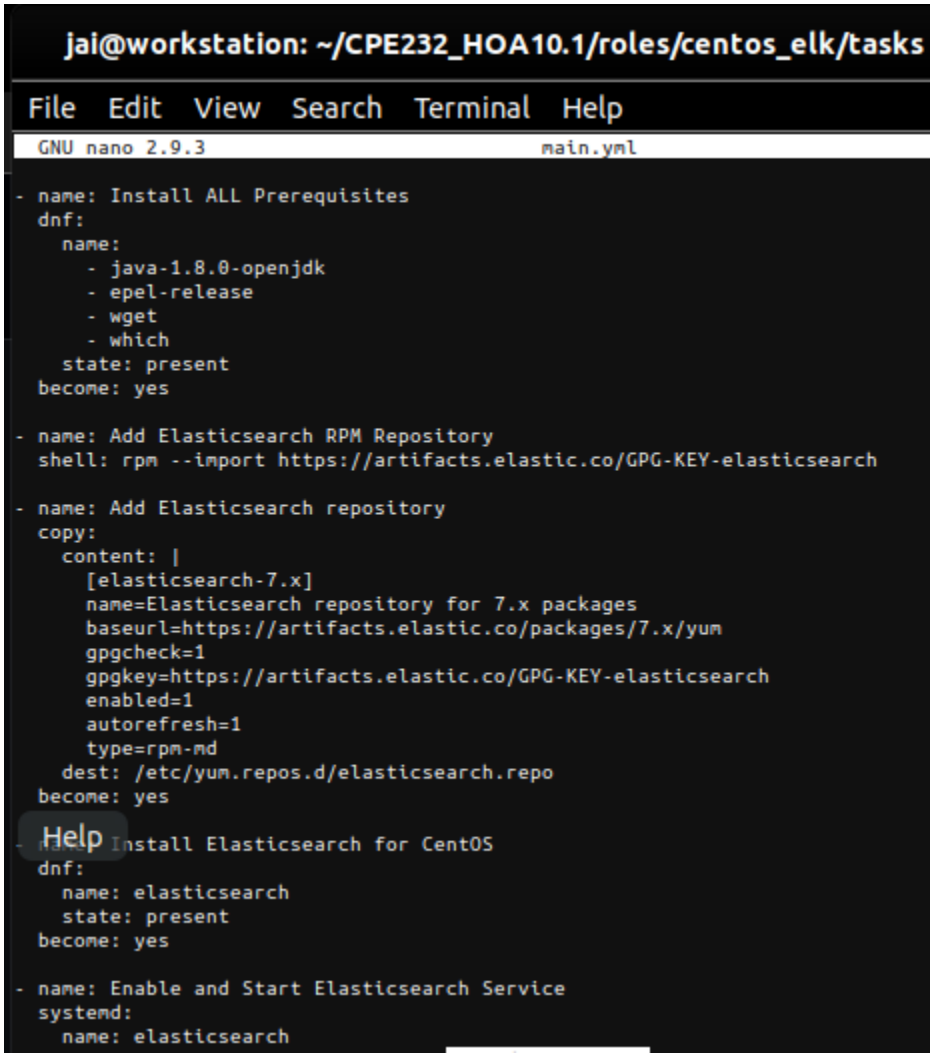
3. Copy the code to the main.yml of the Ubuntu subdirectory.


jai@workstation: ~/CPE232_HOA10.1/roles/ubuntu_elk/tasks
File Edit View Search Terminal Help
GNU nano 2.9.3 main.yml
- 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: Install Kibana for Ubuntu
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 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
```

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



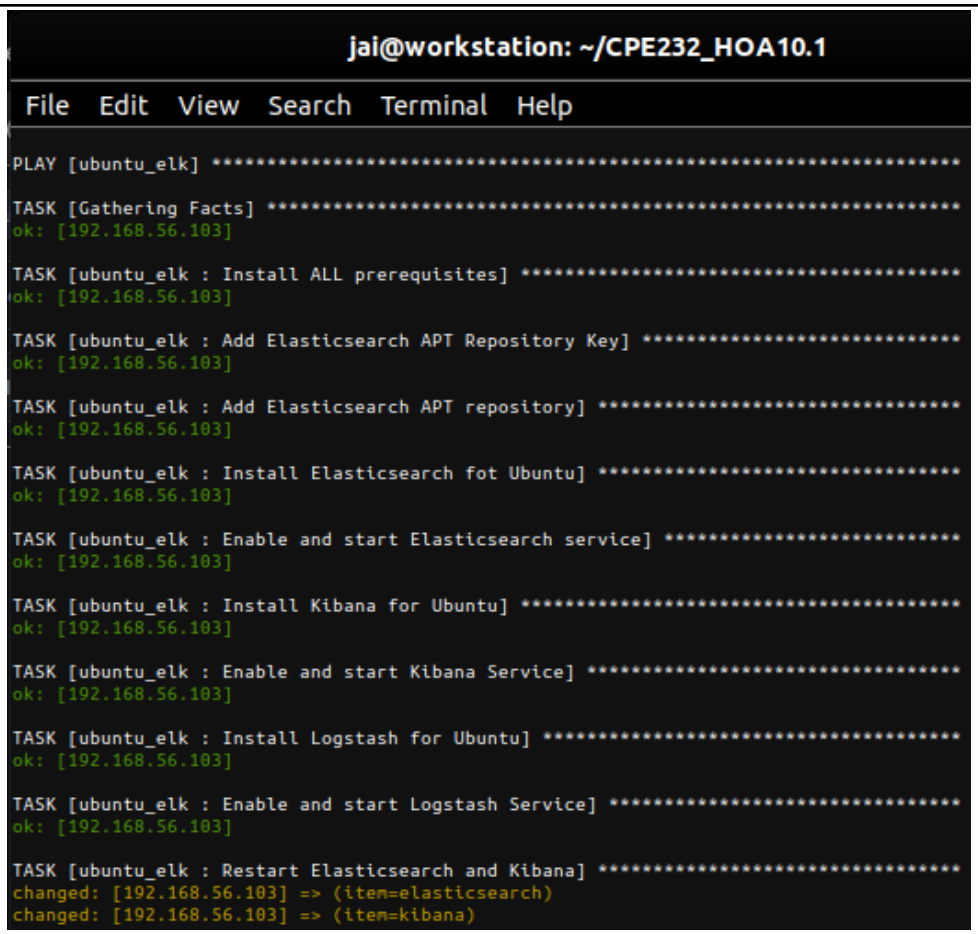
```
    enabled: yes
    state: started
  become: yes

- 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
  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
```

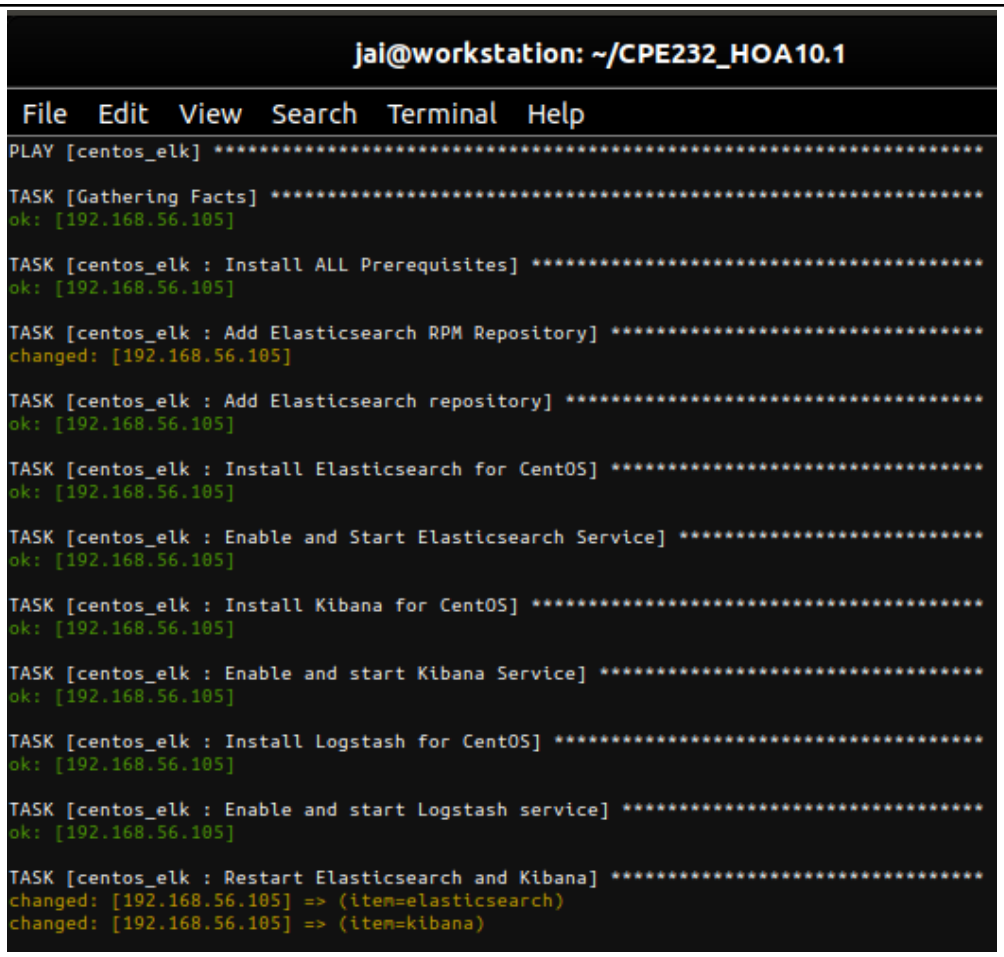
Task 4: Run and Verify

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

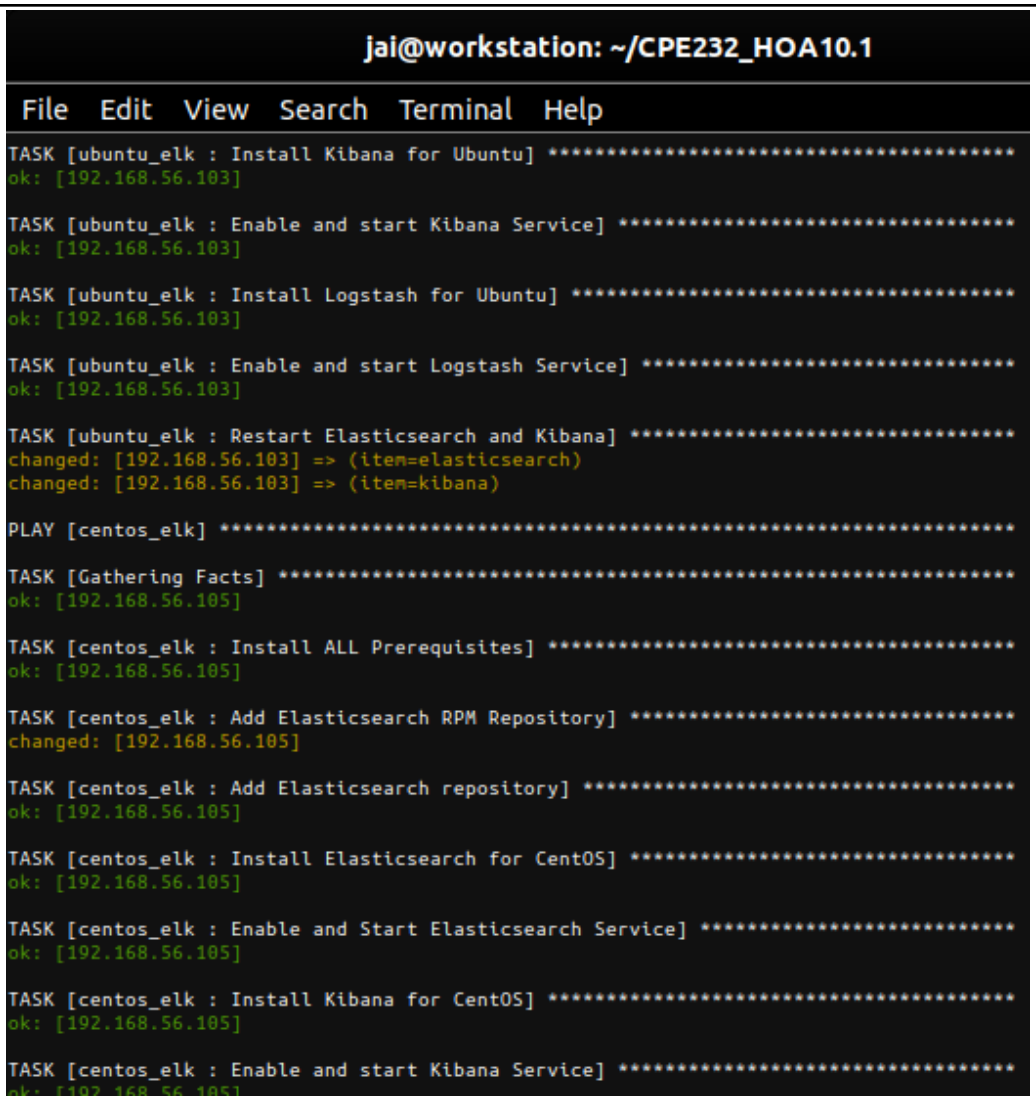

jai@workstation: ~/CPE232_HOA10.1
File Edit View Search Terminal Help
PLAY [ubuntu_elk] **
TASK [Gathering Facts] **
ok: [192.168.56.103]
TASK [ubuntu_elk : Install ALL prerequisites] **
ok: [192.168.56.103]
TASK [ubuntu_elk : Add Elasticsearch APT Repository Key] *****************************
ok: [192.168.56.103]
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)

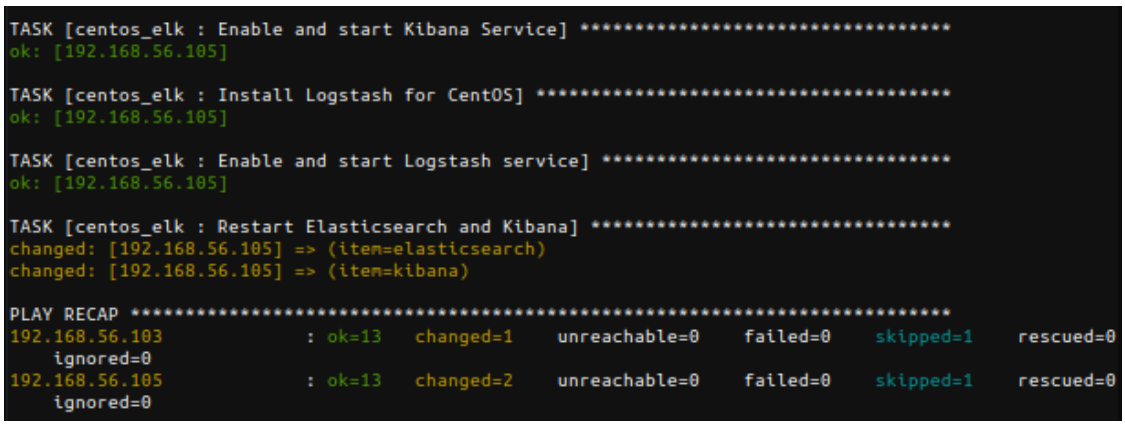
CENTOS_ELK



ENTIRE ansible-playbook


jai@workstation: ~/CPE232_HOA10.1
File Edit View Search Terminal Help
jai@workstation:~/CPE232_HOA10.1$ ansible-playbook --ask-become-pass install_elk.yml
BECOME password:
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] *****************************

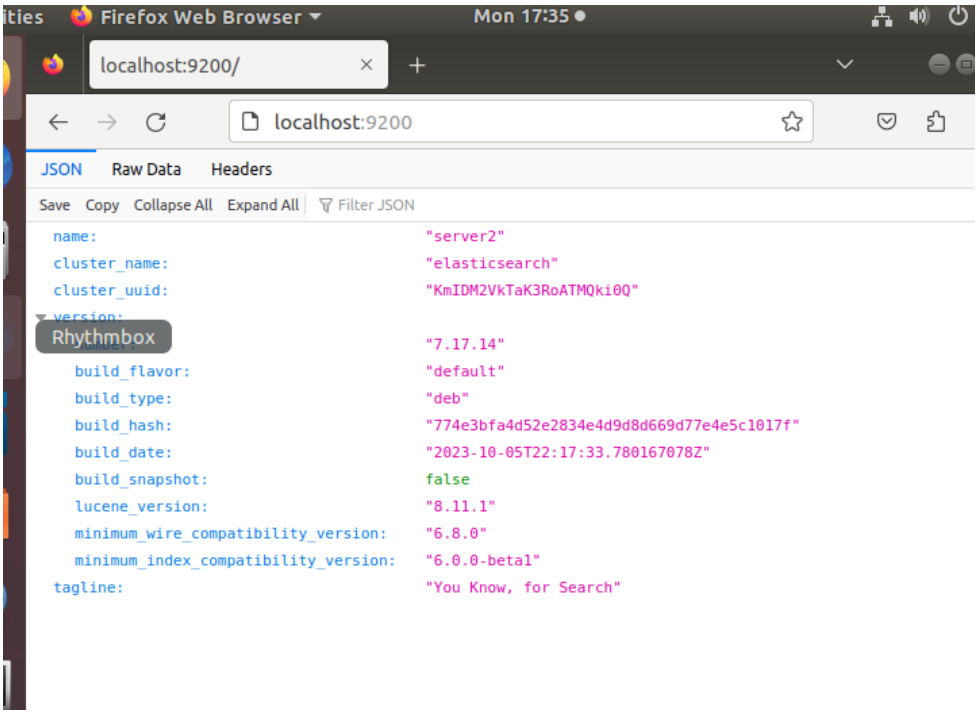

jai@workstation: ~/CPE232_HOA10.1
File Edit View Search Terminal Help
TASK [ubuntu_elk : Install Kibana for Ubuntu] ***********************************
ok: [192.168.56.103]
TASK [ubuntu_elk : Enable and start Kibana Service] *****************************
ok: [192.168.56.103]
TASK [ubuntu_elk : Install 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] *****************************

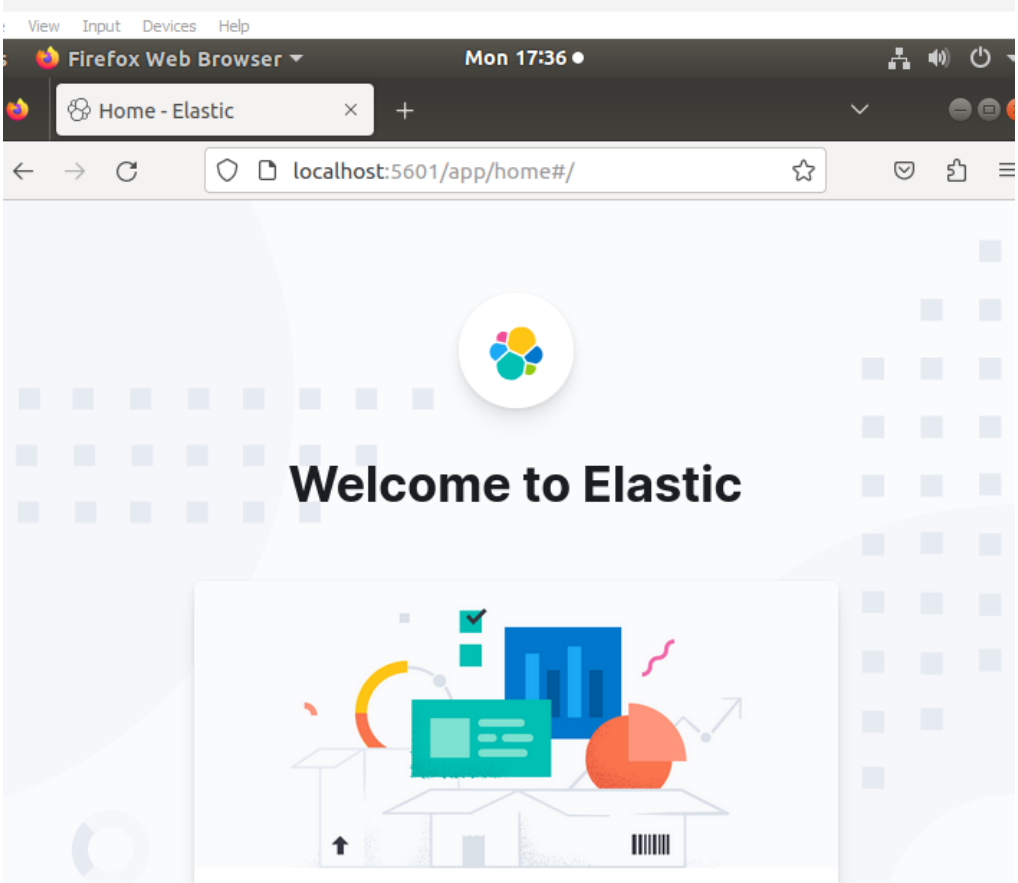

TASK [centos_elk : Enable and start Kibana Service] *****************************
ok: [192.168.56.105]
TASK [centos_elk : Install Logstash for CentOS] **********************************
ok: [192.168.56.105]
TASK [centos_elk : Enable and start Logstash service] ***************************
ok: [192.168.56.105]
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

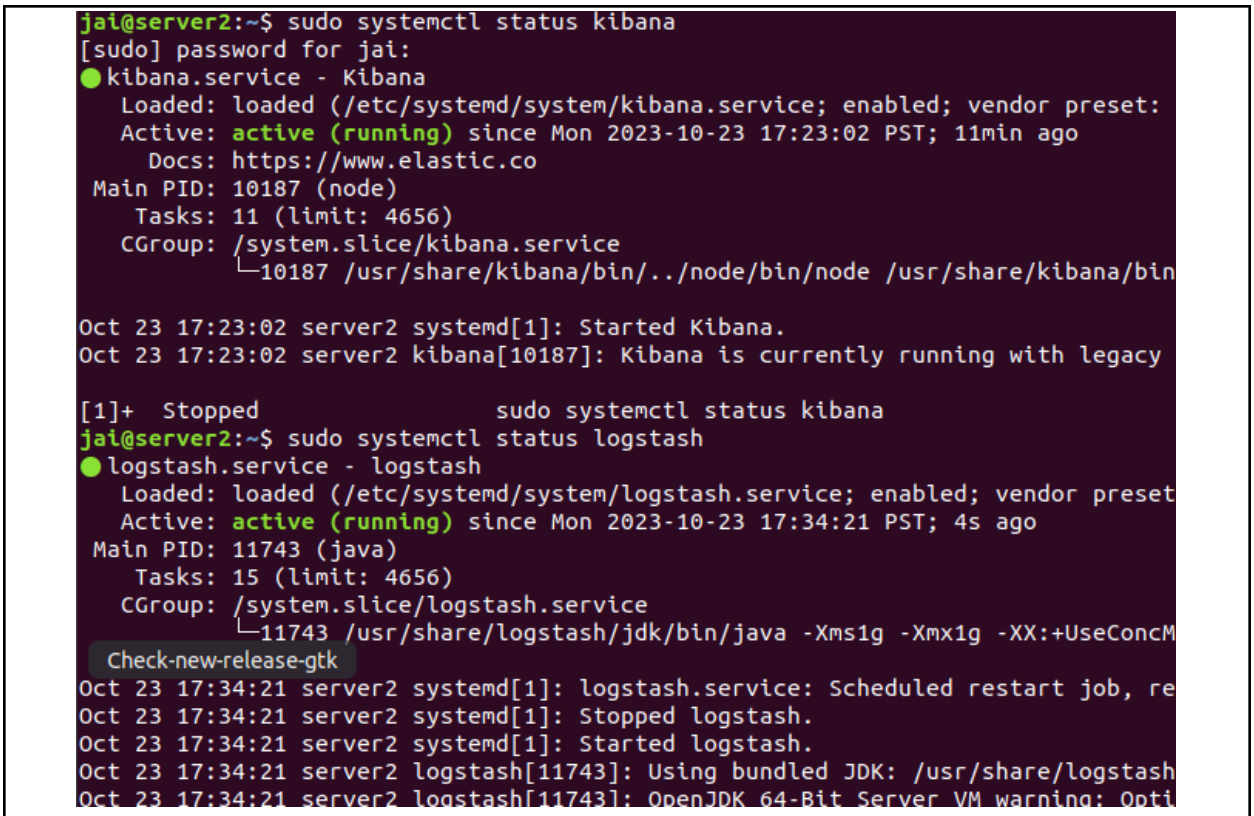
2. Show the screenshot of the ELK Stack in both Server 2 and CentOS by simply typing localhost:5601 in the web browser.

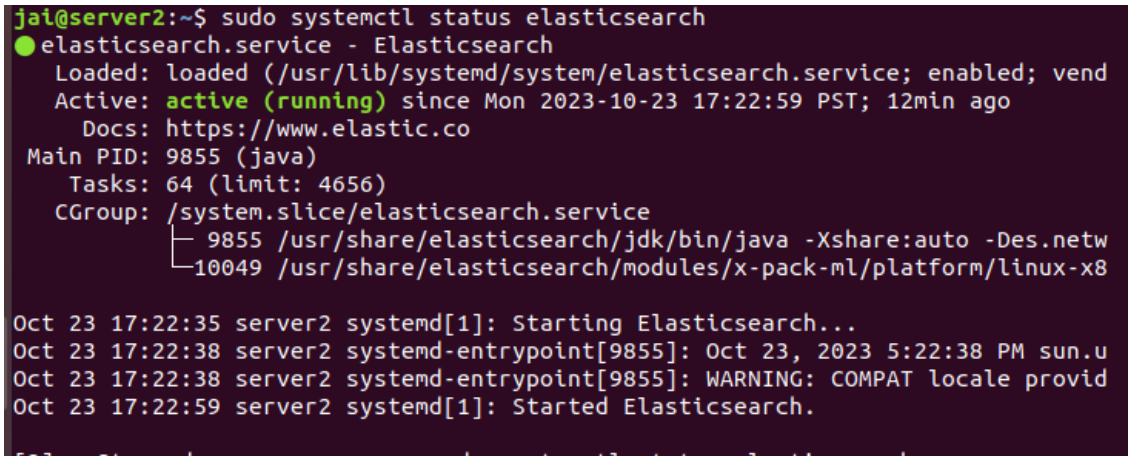
OUTPUT:

SERVER2 (Kibana, Elasticsearch, Logstash)

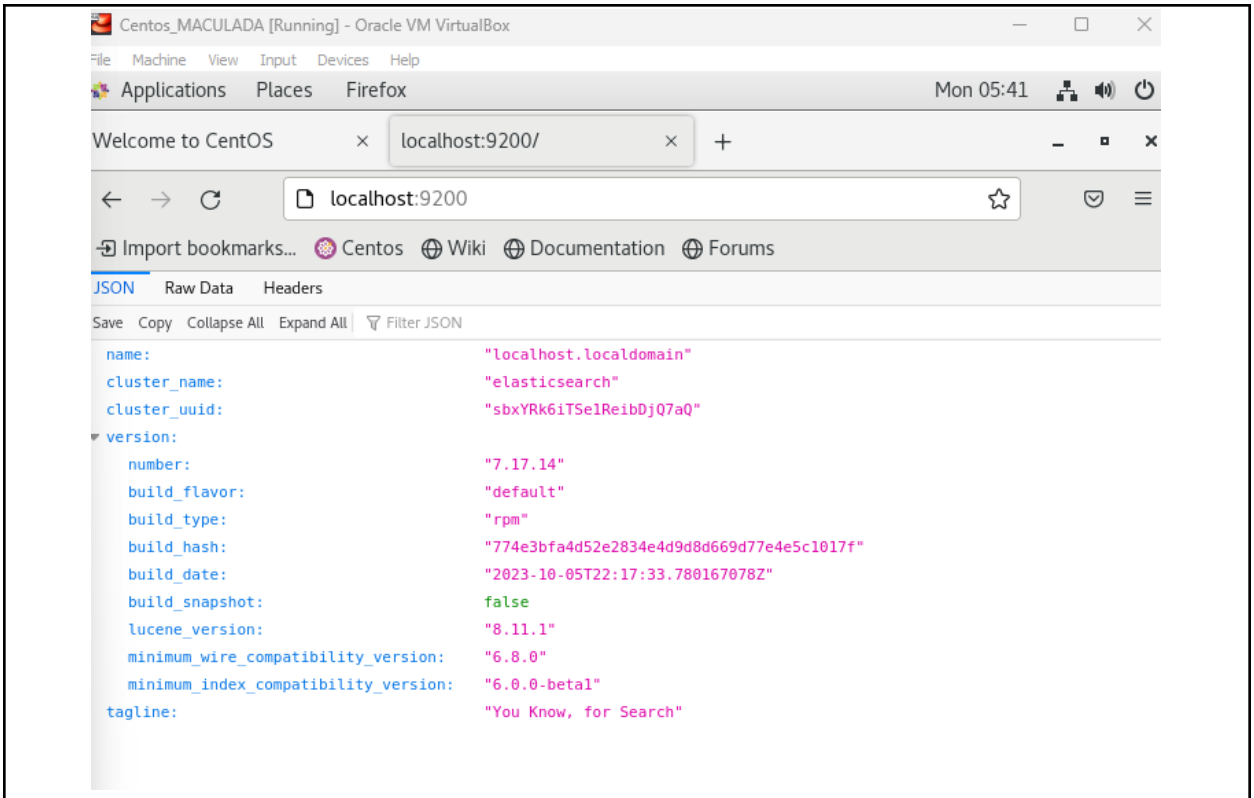


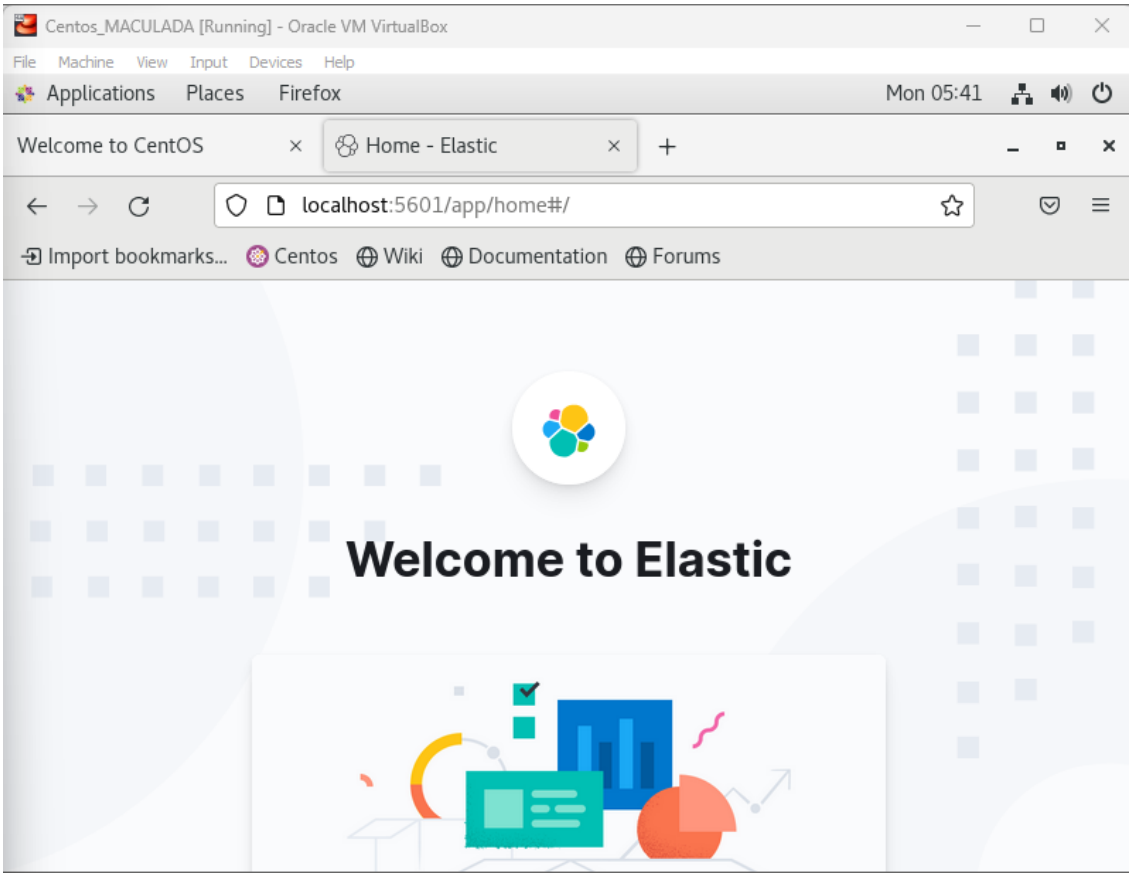

View Input Devices Help
Firefox Web Browser
Mon 17:36
Home - Elastic
localhost:5601/app/home#/
Welcome to Elastic





CENTOS (Kibana, Elasticsearch, Logstash)


Centos_MACULADA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Firefox
Mon 05:41
Welcome to CentOS
localhost:9200/
localhost:9200
Import bookmarks... Centos Wiki Documentation Forums
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
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"

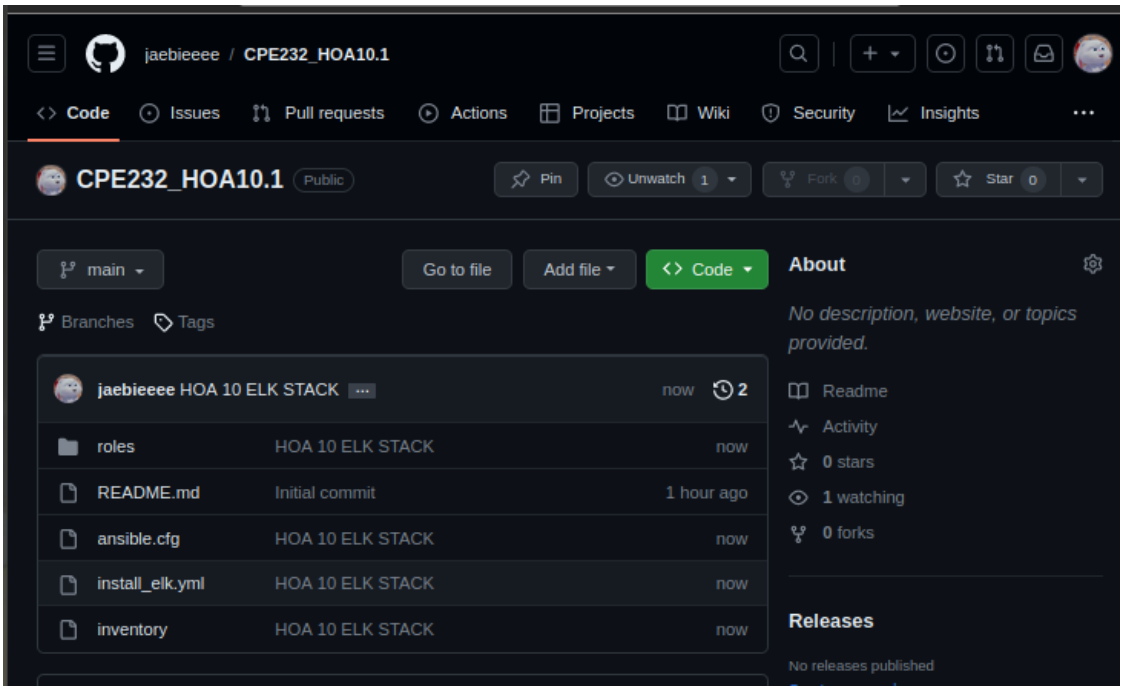

Centos_MACULADA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Firefox
Mon 05:41
Welcome to CentOS
Home - Elastic
localhost:5601/app/home#/
Import bookmarks... Centos Wiki Documentation Forums
Welcome to Elastic

```
[jai@localhost ~]$ systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2023-10-23 06:02:29 EDT; 15min ago
     Docs: https://www.elastic.co
 Main PID: 14333 (node)
    Tasks: 11
   CGroup: /system.slice/kibana.service
           └─14333 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../s...

Oct 23 06:02:29 localhost.localdomain systemd[1]: Started Kibana.
Oct 23 06:02:30 localhost.localdomain kibana[14333]: Kibana is currently running wi...r
Hint: Some lines were ellipsized, use -l to show in full.
[jai@localhost ~]$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2023-10-23 06:02:21 EDT; 16min ago
     Docs: https://www.elastic.co
 Main PID: 13930 (java)
    Tasks: 65
   CGroup: /system.slice/elasticsearch.service
           ├─13930 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkad...
           └─14170 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/...

Oct 23 06:01:50 localhost.localdomain systemd[1]: Starting Elasticsearch...
Oct 23 06:01:54 localhost.localdomain systemd-entrypoint[13930]: Oct 23, 2023 6:01:5...
Oct 23 06:01:54 localhost.localdomain systemd-entrypoint[13930]: WARNING: COMPAT loc...
Oct 23 06:02:21 localhost.localdomain systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
```

```
[jai@localhost ~]$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2023-10-23 06:18:21 EDT; 13s ago
 Main PID: 16319 (java)
    Tasks: 15
   CGroup: /system.slice/logstash.service
           └─16319 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSw...

Oct 23 06:18:21 localhost.localdomain systemd[1]: Started logstash.
Oct 23 06:18:21 localhost.localdomain logstash[16319]: Using bundled JDK: /usr/shar...k
Oct 23 06:18:21 localhost.localdomain logstash[16319]: OpenJDK 64-Bit Server VM war....
Hint: Some lines were ellipsized, use -l to show in full.
```

3. Upload it in the github.

```
jai@workstation:~/CPE232_HOA10.1$ git add *
jai@workstation:~/CPE232_HOA10.1$ git commit -m "HOA 10 ELK STACK"
[main 1d9d0cc] HOA 10 ELK STACK
 5 files changed, 186 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
jai@workstation:~/CPE232_HOA10.1$ git push origin
Counting objects: 12, 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)
remote: Resolving deltas: 100% (1/1), done.
To github.com:jaebieeee/CPE232_HOA10.1.git
   6f4e34e..1d9d0cc  main -> main
```



GITHUB: https://github.com/jaebieeee/CPE232_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.