Name: Agpaoa, Ma.Diane J.	**Date Performed:** 20/10/2022
Course/Section: CPE232-CPE31S22	**Date Submitted:** 25/10/2022
Instructor: Dr. Jonathan Taylar	**Semester and SY:** 1st Sem 2022-2023

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.

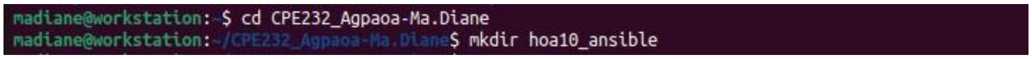
Source: https://www.graylog.org/products/open-source

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)

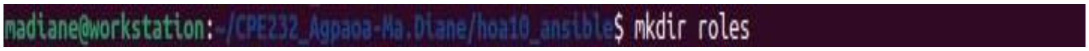
Step 1: Creating new directory for Hands-on Activity 10



```
madiane@workstation:~$ cd CPE232_Agpaoa-Ma.Diane
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane$ mkdir hoa10_ansible
```

Figure 1.1 Creating hoa10_ansible directory

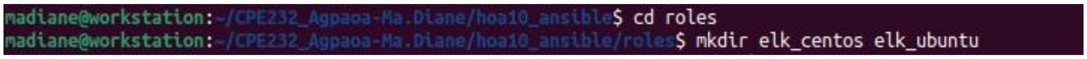
I created a new directory and named it hoa10_ansible by using the command mkdir.



```
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible$ mkdir roles
```

Figure 1.2 Creating roles directory

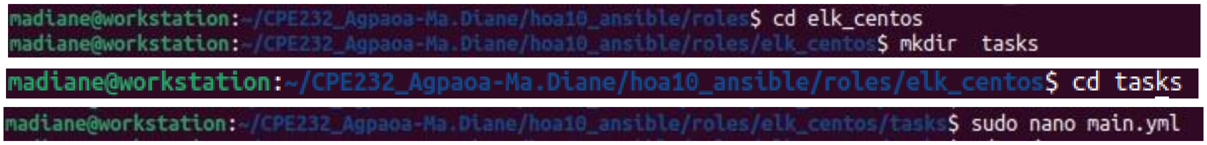
I created a directory for roles within the hoa10_ansible directory and named it as roles by using the command mkdir.



```
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible$ cd roles
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible/roles$ mkdir elk_centos elk_ubuntu
```

Figure 1.3 Creating new directories within the roles directory

I changed the directory from hoa10_ansible directory to roles directory by executing the command “cd roles”. Within the roles directory I created new directories and name it as elk_centos and elk_ubuntu respectively.

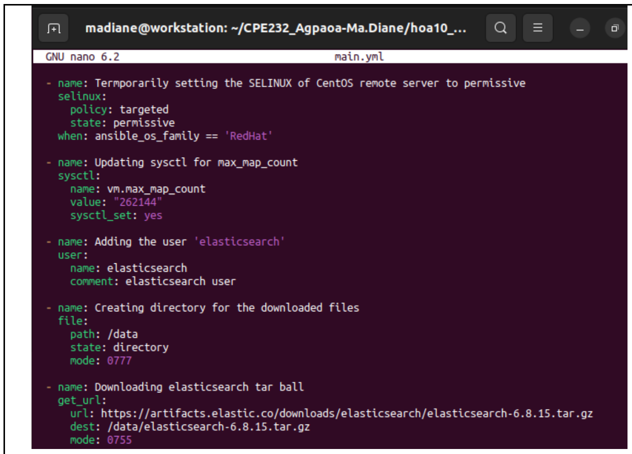


```
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible/roles$ cd elk_centos
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible/roles/elk_centos$ mkdir  tasks
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible/roles/elk_centos$ cd tasks
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible/roles/elk_centos/tasks$ sudo nano main.yml
```

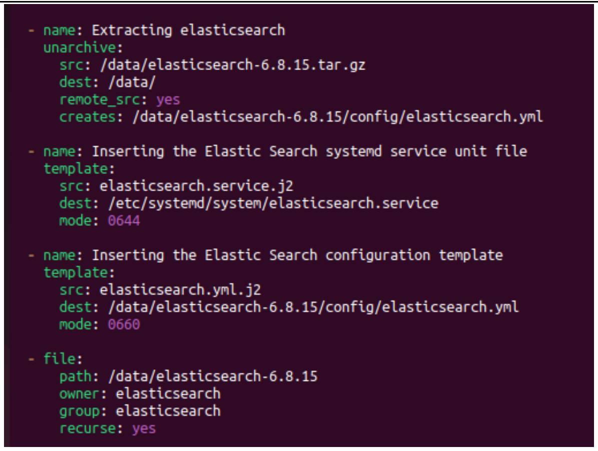
Figure 1.4 Creating main.yml within the newly created tasks directory inside the elk_centos directory

I changed the directory from roles directory to elk_centos directory by using the command cd. After that, I created a new directory and named it as “tasks”, and within the tasks directory I created a playbook and named it as main.yml.

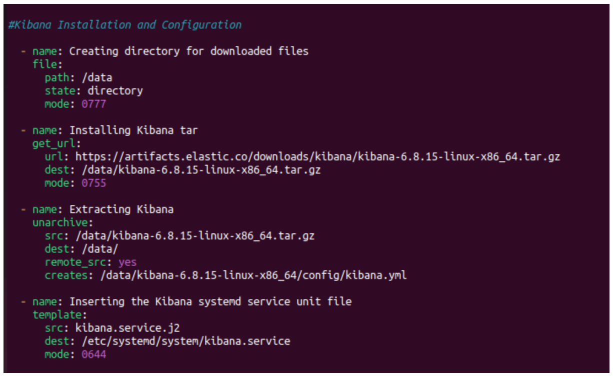
Step 2: Creating the playbook main.yml that will install and configure Elastic Stack (Elastic Search, Kibana and Logstash) in separate hosts



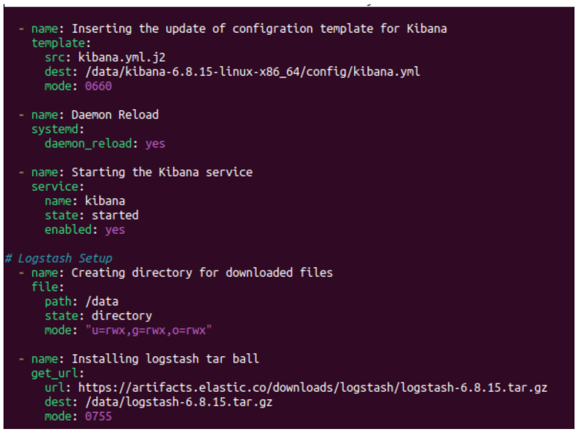
```
- name: Termporarily setting the SELINUX of CentOS remote server to permissive
  selinux:
    policy: targeted
    state: permissive
  when: ansible_os_family == 'RedHat'

- name: Updating sysctl for max_map_count
  sysctl:
    name: vm.max_map_count
    value: "262144"
    sysctl_set: yes

- name: Adding the user 'elasticsearch'
  user:
    name: elasticsearch
    comment: elasticsearch user

- name: Creating directory for the downloaded files
  file:
    path: /data
    state: directory
    mode: 0777

- name: Downloading elasticsearch tar ball
  get_url:
    url: https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.8.15.tar.gz
    dest: /data/elasticsearch-6.8.15.tar.gz
    mode: 0755
```



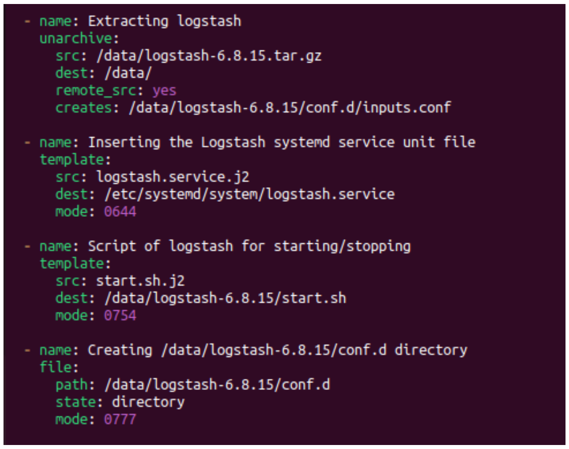
```
- name: Extracting elasticsearch
  unarchive:
    src: /data/elasticsearch-6.8.15.tar.gz
    dest: /data/
    remote_src: yes
    creates: /data/elasticsearch-6.8.15/config/elasticsearch.yml

- name: Inserting the Elastic Search systemd service unit file
  template:
    src: elasticsearch.service.j2
    dest: /etc/systemd/system/elasticsearch.service
    mode: 0644

- name: Inserting the Elastic Search configuration template
  template:
    src: elasticsearch.yml.j2
    dest: /data/elasticsearch-6.8.15/config/elasticsearch.yml
    mode: 0660

- file:
    path: /data/elasticsearch-6.8.15
    owner: elasticsearch
    group: elasticsearch
    recurse: yes
```



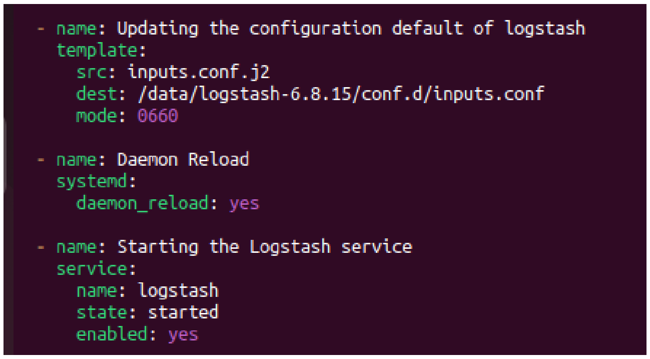
```
#Kibana Installation and Configuration

  - name: Creating directory for downloaded files
    file:
      path: /data
      state: directory
      mode: 0777

  - name: Installing Kibana tar
    get_url:
      url: https://artifacts.elastic.co/downloads/kibana/kibana-6.8.15-linux-x86_64.tar.gz
      dest: /data/kibana-6.8.15-linux-x86_64.tar.gz
      mode: 0755

  - name: Extracting Kibana
    unarchive:
      src: /data/kibana-6.8.15-linux-x86_64.tar.gz
      dest: /data/
      remote_src: yes
      creates: /data/kibana-6.8.15-linux-x86_64/config/kibana.yml

  - name: Inserting the Kibana systemd service unit file
    template:
      src: kibana.service.j2
      dest: /etc/systemd/system/kibana.service
      mode: 0644
```



```
  - name: Inserting the update of configration template for Kibana
    template:
      src: kibana.yml.j2
      dest: /data/kibana-6.8.15-linux-x86_64/config/kibana.yml
      mode: 0660

  - name: Daemon Reload
    systemd:
      daemon_reload: yes

  - name: Starting the Kibana service
    service:
      name: kibana
      state: started
      enabled: yes

# Logstash Setup
  - name: Creating directory for downloaded files
    file:
      path: /data
      state: directory
      mode: "u=rwx,g=rwx,o=rwx"

  - name: Installing logstash tar ball
    get_url:
      url: https://artifacts.elastic.co/downloads/logstash/logstash-6.8.15.tar.gz
      dest: /data/logstash-6.8.15.tar.gz
      mode: 0755
```



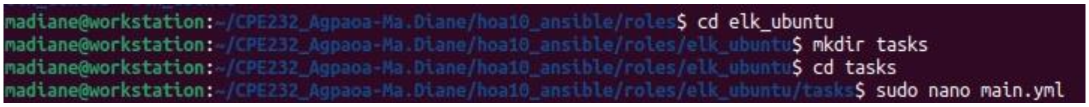
```
  - name: Extracting logstash
    unarchive:
      src: /data/logstash-6.8.15.tar.gz
      dest: /data/
      remote_src: yes
      creates: /data/logstash-6.8.15/conf.d/inputs.conf

  - name: Inserting the Logstash systemd service unit file
    template:
      src: logstash.service.j2
      dest: /etc/systemd/system/logstash.service
      mode: 0644

  - name: Script of logstash for starting/stopping
    template:
      src: start.sh.j2
      dest: /data/logstash-6.8.15/start.sh
      mode: 0754

  - name: Creating /data/logstash-6.8.15/conf.d directory
    file:
      path: /data/logstash-6.8.15/conf.d
      state: directory
      mode: 0777
```



```
  - name: Updating the configuration default of logstash
    template:
      src: inputs.conf.j2
      dest: /data/logstash-6.8.15/conf.d/inputs.conf
      mode: 0660

  - name: Daemon Reload
    systemd:
      daemon_reload: yes

  - name: Starting the Logstash service
    service:
      name: logstash
      state: started
      enabled: yes
```

Figure 2.1 Contents of the playbook main.yml within the elk_centos

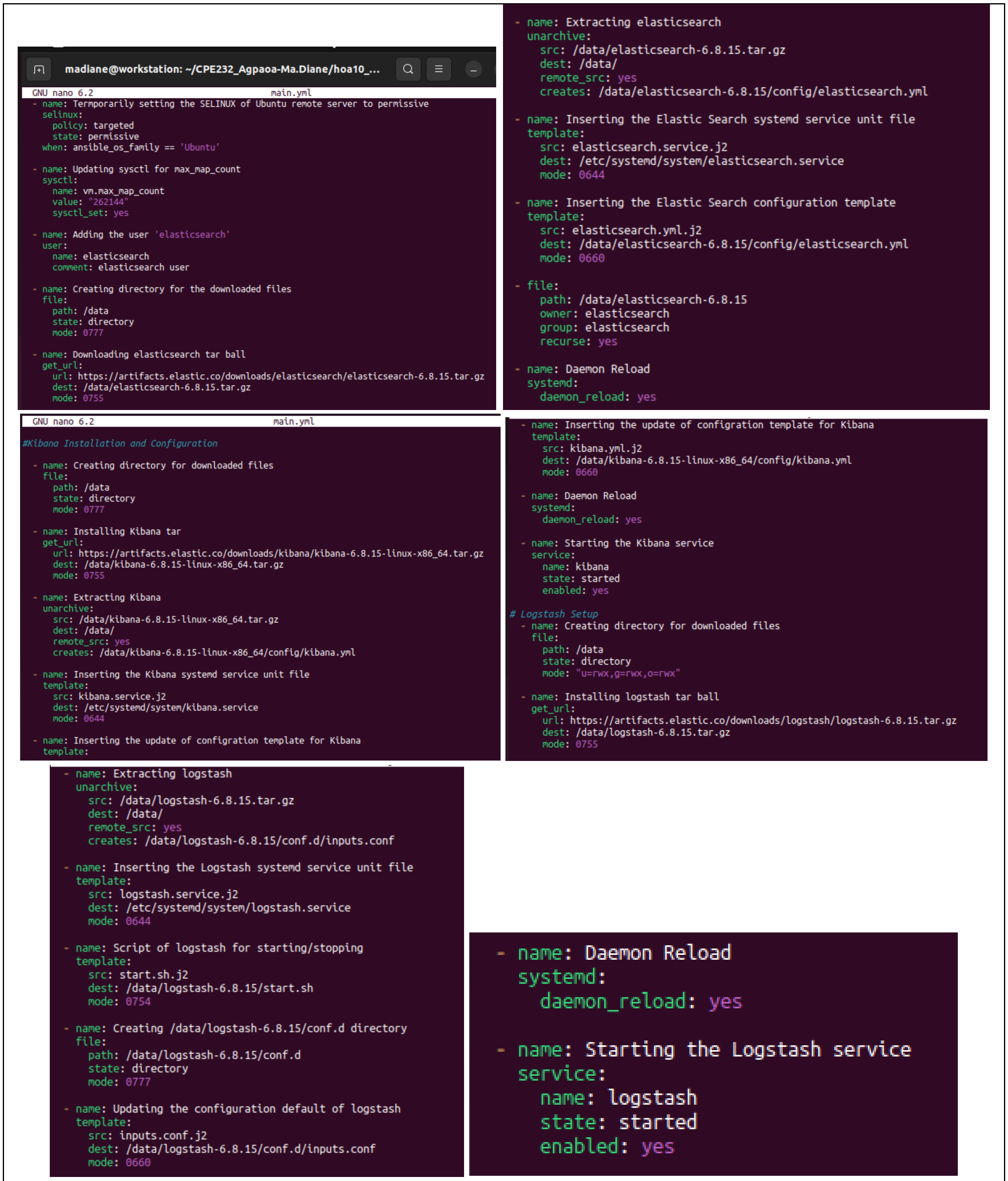
This playbook contains the installation and configuration of Elastic search, Kibana, and Logstash for remote servers with an operating system of CentOS.



```
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible/roles$ cd elk_ubuntu
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible/roles/elk_ubuntu$ mkdir tasks
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible/roles/elk_ubuntu$ cd tasks
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible/roles/elk_ubuntu/tasks$ sudo nano main.yml
```

Figure 2.2 Creating main.yml within the newly created tasks directory inside the elk_ubuntu directory

I changed the directory from roles directory to elk_ubuntu directory by using the command cd. After that, I created a new directory and named it as “tasks”, and within the tasks directory I created a playbook and named it as main.yml.



```
GNU nano 6.2                              main.yml
- name: Termporarily setting the SELINUX of Ubuntu remote server to permissive
  selinux:
    policy: targeted
    state: permissive
  when: ansible_os_family == 'Ubuntu'

- name: Updating sysctl for max_map_count
  sysctl:
    name: vm.max_map_count
    value: "262144"
    sysctl_set: yes

- name: Adding the user 'elasticsearch'
  user:
    name: elasticsearch
    comment: elasticsearch user

- name: Creating directory for the downloaded files
  file:
    path: /data
    state: directory
    mode: 0777

- name: Downloading elasticsearch tar ball
  get_url:
    url: https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.8.15.tar.gz
    dest: /data/elasticsearch-6.8.15.tar.gz
    mode: 0755
```

```
- name: Extracting elasticsearch
  unarchive:
    src: /data/elasticsearch-6.8.15.tar.gz
    dest: /data/
    remote_src: yes
    creates: /data/elasticsearch-6.8.15/config/elasticsearch.yml

- name: Inserting the Elastic Search systemd service unit file
  template:
    src: elasticsearch.service.j2
    dest: /etc/systemd/system/elasticsearch.service
    mode: 0644

- name: Inserting the Elastic Search configuration template
  template:
    src: elasticsearch.yml.j2
    dest: /data/elasticsearch-6.8.15/config/elasticsearch.yml
    mode: 0660

- file:
    path: /data/elasticsearch-6.8.15
    owner: elasticsearch
    group: elasticsearch
    recurse: yes

- name: Daemon Reload
  systemd:
    daemon_reload: yes
```

```
GNU nano 6.2                              main.yml

#Kibana Installation and Configuration

  - name: Creating directory for downloaded files
    file:
      path: /data
      state: directory
      mode: 0777

  - name: Installing Kibana tar
    get_url:
      url: https://artifacts.elastic.co/downloads/kibana/kibana-6.8.15-linux-x86_64.tar.gz
      dest: /data/kibana-6.8.15-linux-x86_64.tar.gz
      mode: 0755

  - name: Extracting Kibana
    unarchive:
      src: /data/kibana-6.8.15-linux-x86_64.tar.gz
      dest: /data/
      remote_src: yes
      creates: /data/kibana-6.8.15-linux-x86_64/config/kibana.yml

  - name: Inserting the Kibana systemd service unit file
    template:
      src: kibana.service.j2
      dest: /etc/systemd/system/kibana.service
      mode: 0644

  - name: Inserting the update of configration template for Kibana
    template:
```

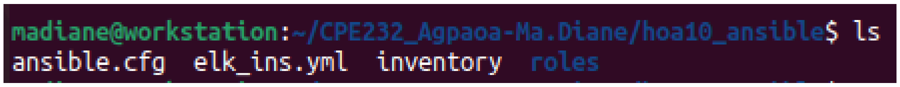
```
  - name: Inserting the update of configration template for Kibana
    template:
      src: kibana.yml.j2
      dest: /data/kibana-6.8.15-linux-x86_64/config/kibana.yml
      mode: 0660

  - name: Daemon Reload
    systemd:
      daemon_reload: yes

  - name: Starting the Kibana service
    service:
      name: kibana
      state: started
      enabled: yes

# Logstash Setup
  - name: Creating directory for downloaded files
    file:
      path: /data
      state: directory
      mode: "u=rwx,g=rwx,o=rwx"

  - name: Installing logstash tar ball
    get_url:
      url: https://artifacts.elastic.co/downloads/logstash/logstash-6.8.15.tar.gz
      dest: /data/logstash-6.8.15.tar.gz
      mode: 0755
```

```
  - name: Extracting logstash
    unarchive:
      src: /data/logstash-6.8.15.tar.gz
      dest: /data/
      remote_src: yes
      creates: /data/logstash-6.8.15/conf.d/inputs.conf

  - name: Inserting the Logstash systemd service unit file
    template:
      src: logstash.service.j2
      dest: /etc/systemd/system/logstash.service
      mode: 0644

  - name: Script of logstash for starting/stopping
    template:
      src: start.sh.j2
      dest: /data/logstash-6.8.15/start.sh
      mode: 0754

  - name: Creating /data/logstash-6.8.15/conf.d directory
    file:
      path: /data/logstash-6.8.15/conf.d
      state: directory
      mode: 0777

  - name: Updating the configuration default of logstash
    template:
      src: inputs.conf.j2
      dest: /data/logstash-6.8.15/conf.d/inputs.conf
      mode: 0660
```

```
- name: Daemon Reload
  systemd:
    daemon_reload: yes

- name: Starting the Logstash service
  service:
    name: logstash
    state: started
    enabled: yes
```

Figure 2.3 Contents of the playbook main.yml within the elk_ubuntu

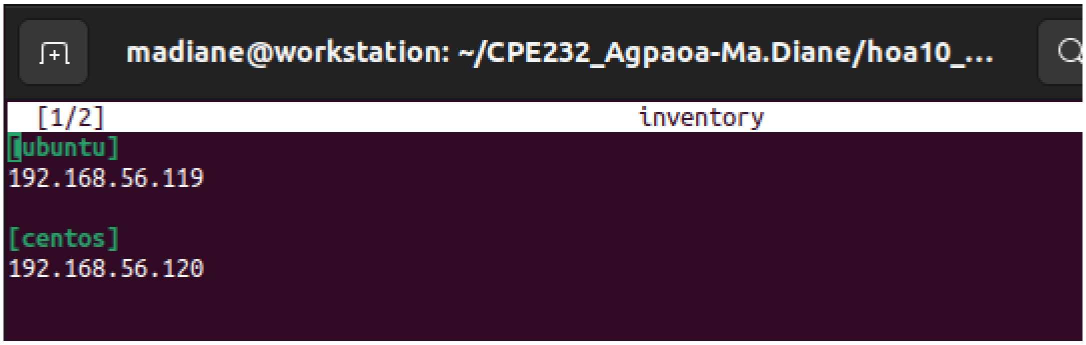
This playbook contains the installation and configuration of Elastic search, Kibana, and Logstash for remote servers with an operating system of Ubuntu.



```
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible$ ls
ansible.cfg  elk_ins.yml  inventory  roles
```

Figure 2.4 Contents of hoa10_ansible directory

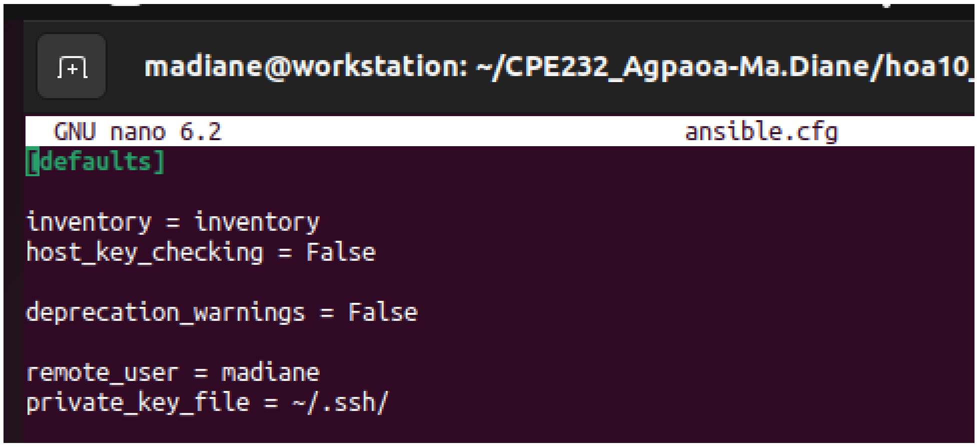
The files within hoa10_ansible directory are the ansible.cfg, elk_ins.yml, inventory and the roles directory.



```
  [1/2]                                     inventory
[ubuntu]
192.168.56.119

[centos]
192.168.56.120
```

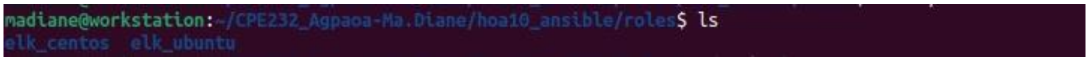
Figure 2.5 Contents of inventory file

The contents of inventory file are the group of IP addresses of the managed remote servers. The IP address 192.168.56.119 is the remote server with an operating system of Ubuntu. While the 192.168.56.120 is the remote server with an operating system of CentOS.



```
  GNU nano 6.2                                ansible.cfg
[defaults]

inventory = inventory
host_key_checking = False

deprecation_warnings = False

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

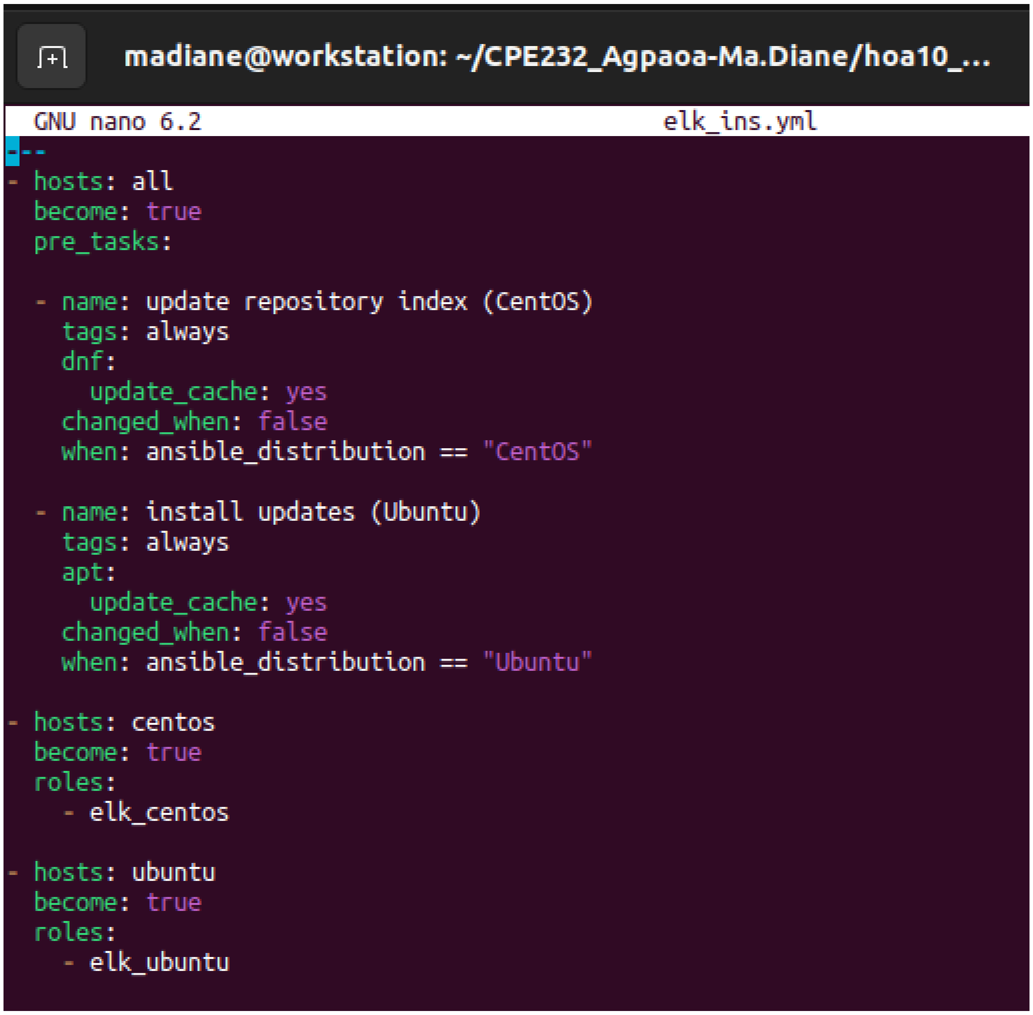
2.6 Contents of ansible.cfg



```
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible/roles$ ls
elk_centos  elk_ubuntu
```

Figure 2.7 Contents of roles directory

Inside the roles directory there are two directories named as elk_centos and elk_ubuntu. These directories contain playbooks that will install and configure the Elastic search, Kibana and Logstash to group of remote servers that has an operating system of either CentOS and Ubuntu.

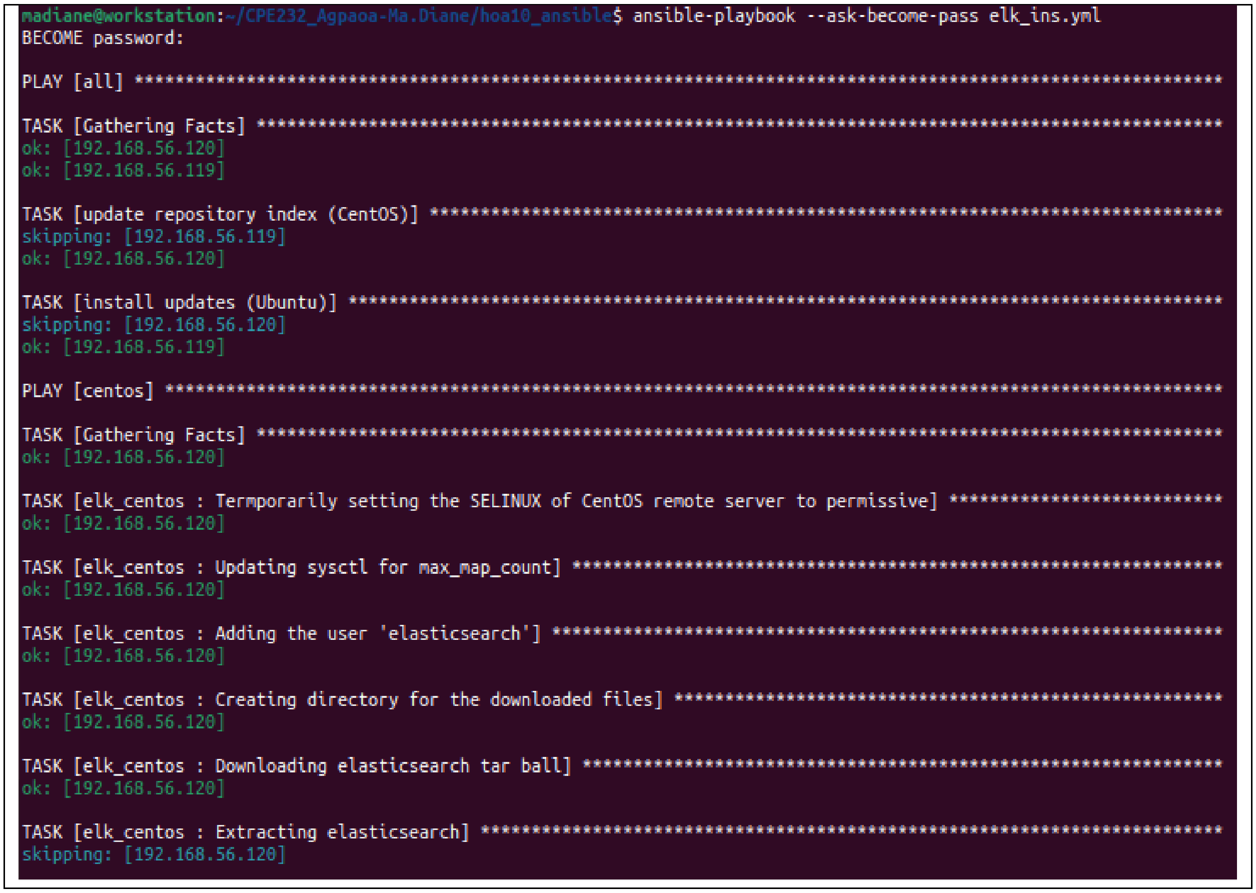


```
GNU nano 6.2                                   elk_ins.yml
---
- hosts: all
  become: true
  pre_tasks:

  - name: update repository index (CentOS)
    tags: always
    dnf:
      update_cache: yes
    changed_when: false
    when: ansible_distribution == "CentOS"

  - name: install updates (Ubuntu)
    tags: always
    apt:
      update_cache: yes
    changed_when: false
    when: ansible_distribution == "Ubuntu"

- hosts: centos
  become: true
  roles:
    - elk_centos

- hosts: ubuntu
  become: true
  roles:
    - elk_ubuntu
```

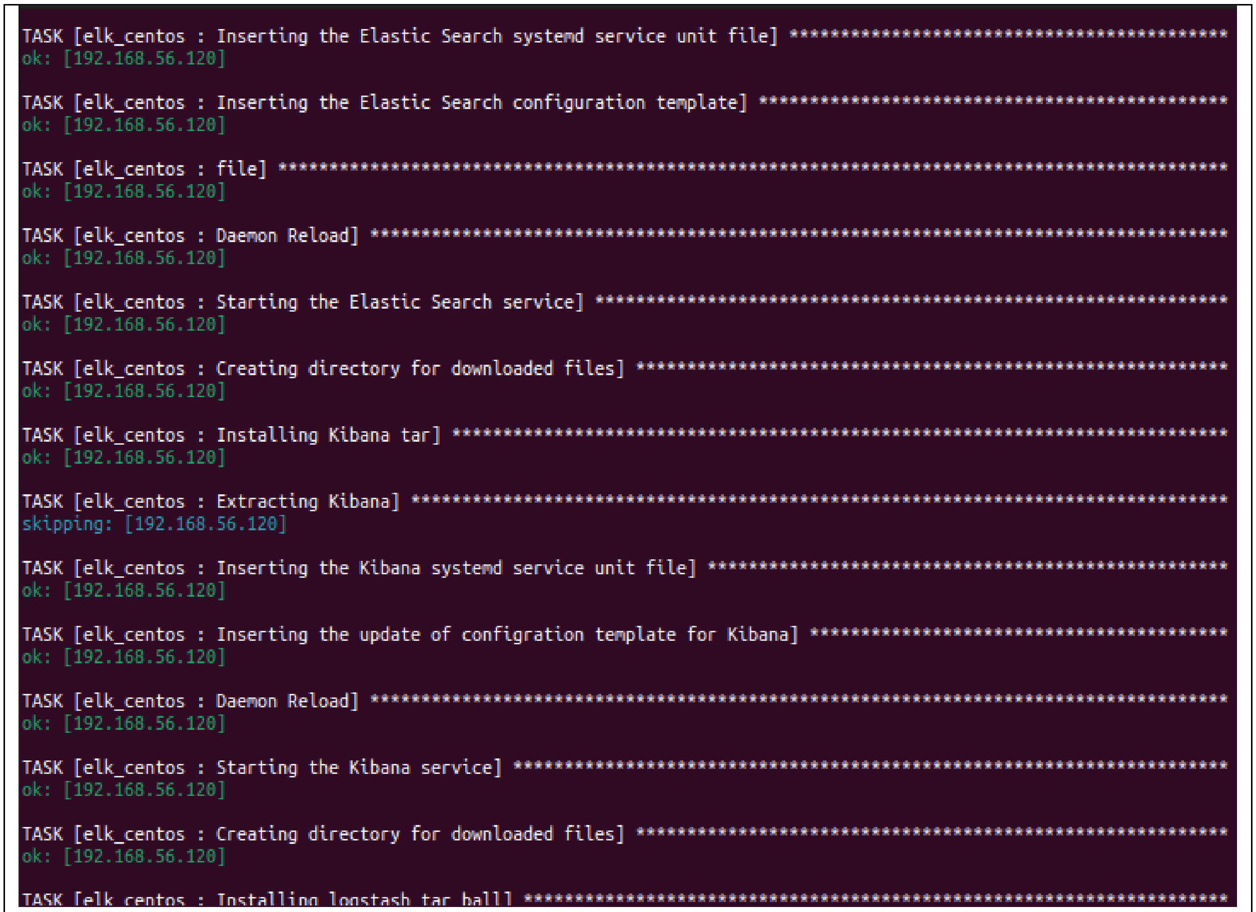
Figure 2.8 Contents of the elk_ins.yml playbook

This playbook contains the pre-tasks for all the remote servers and the plays for installing the Elastic Stack in separate hosts that have an operating system of either CentOS and Ubuntu.

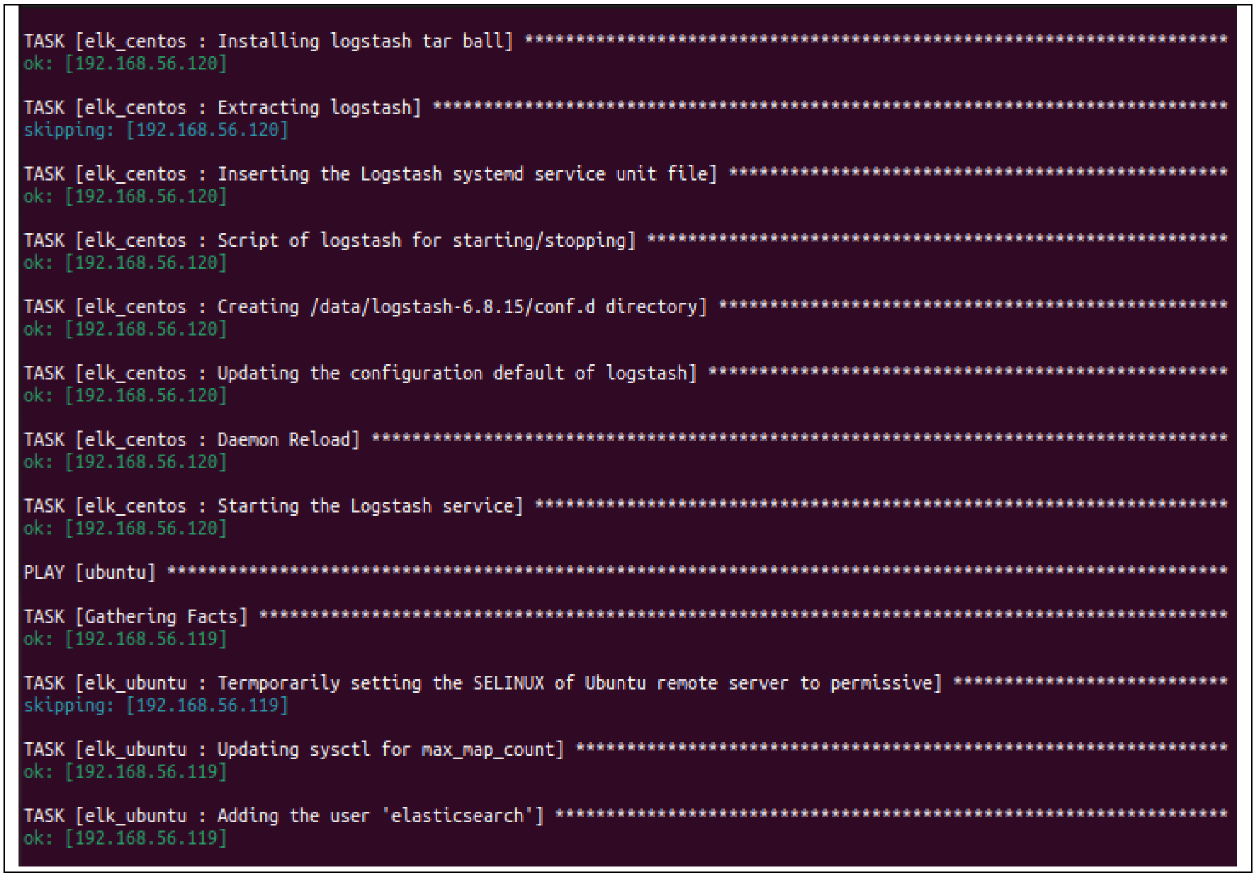
Step 3: Running the created playbook for installing and configuring of Elastic Stack



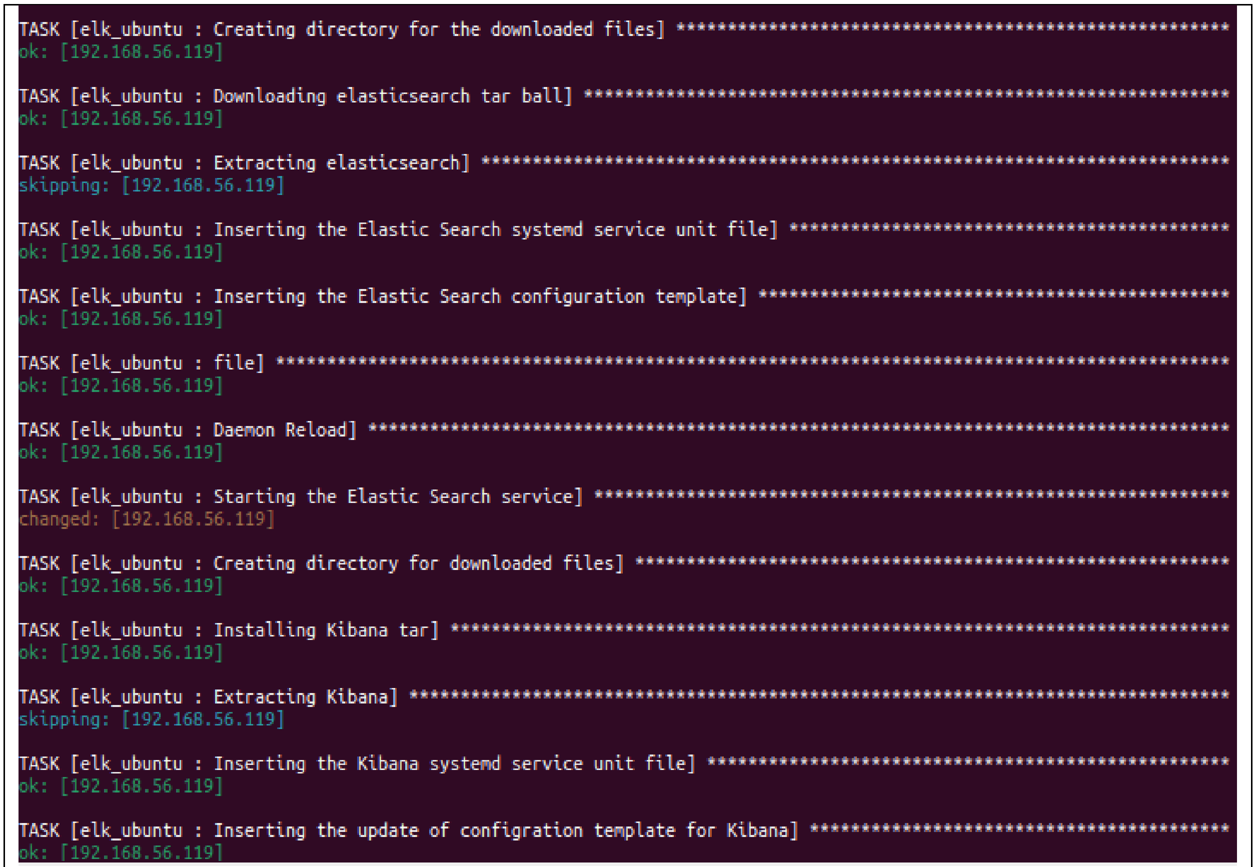
```
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane/hoa10_ansible$ ansible-playbook --ask-become-pass elk_ins.yml
BECOME password:

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

TASK [Gathering Facts] ***********************************************************************************************
ok: [192.168.56.120]
ok: [192.168.56.119]

TASK [update repository index (CentOS)] ******************************************************************************
skipping: [192.168.56.119]
ok: [192.168.56.120]

TASK [install updates (Ubuntu)] **************************************************************************************
skipping: [192.168.56.120]
ok: [192.168.56.119]

PLAY [centos] ********************************************************************************************************

TASK [Gathering Facts] ***********************************************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Termporarily setting the SELINUX of CentOS remote server to permissive] ***************************
ok: [192.168.56.120]

TASK [elk_centos : Updating sysctl for max_map_count] ****************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Adding the user 'elasticsearch'] ******************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Creating directory for the downloaded files] ******************************************************
ok: [192.168.56.120]

TASK [elk_centos : Downloading elasticsearch tar ball] ***************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Extracting elasticsearch] *************************************************************************
skipping: [192.168.56.120]
```



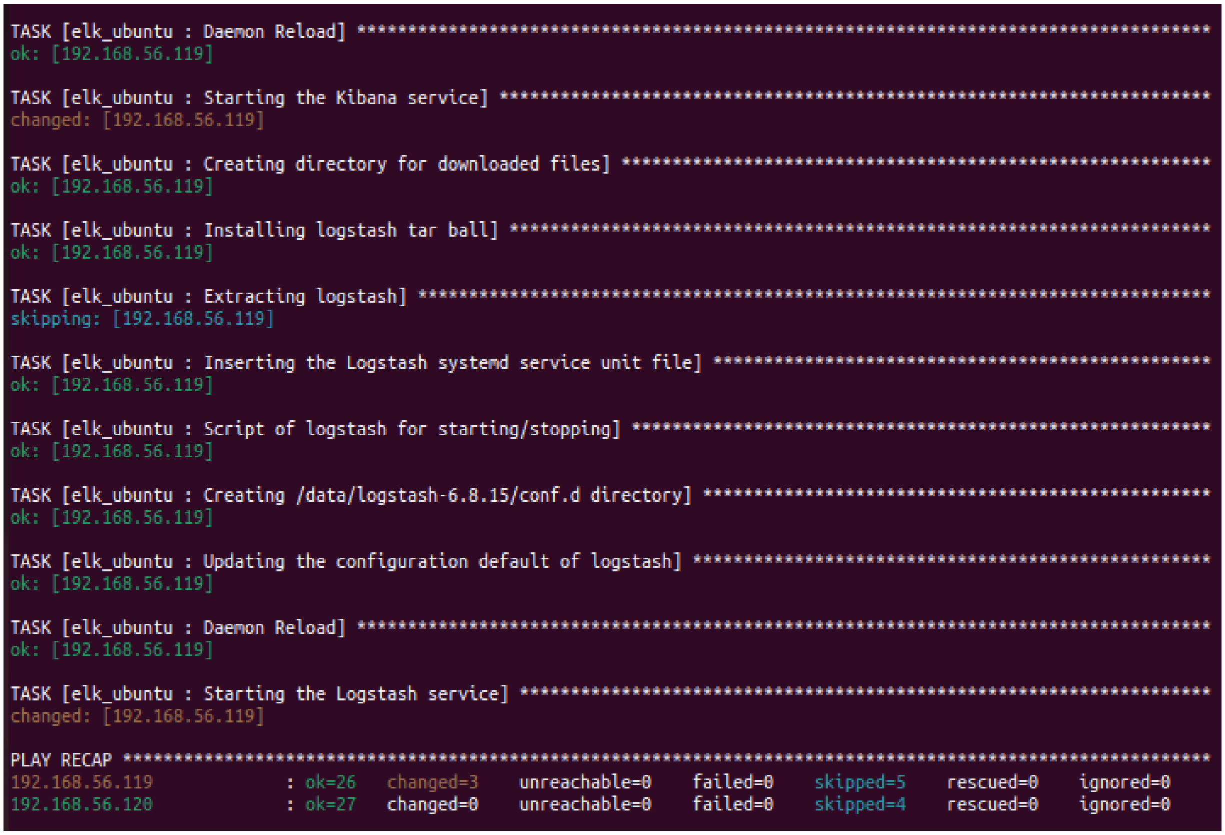
```
TASK [elk_centos : Inserting the Elastic Search systemd service unit file] *******************************************
ok: [192.168.56.120]

TASK [elk_centos : Inserting the Elastic Search configuration template] **********************************************
ok: [192.168.56.120]

TASK [elk_centos : file] *********************************************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Daemon Reload] ************************************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Starting the Elastic Search service] **************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Creating directory for downloaded files] **********************************************************
ok: [192.168.56.120]

TASK [elk_centos : Installing Kibana tar] ****************************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Extracting Kibana] ********************************************************************************
skipping: [192.168.56.120]

TASK [elk_centos : Inserting the Kibana systemd service unit file] ***************************************************
ok: [192.168.56.120]

TASK [elk_centos : Inserting the update of configration template for Kibana] *****************************************
ok: [192.168.56.120]

TASK [elk_centos : Daemon Reload] ************************************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Starting the Kibana service] **********************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Creating directory for downloaded files] **********************************************************
ok: [192.168.56.120]

TASK [elk_centos : Installing logstash tar ball] *********************************************************************
```



```
TASK [elk_centos : Installing logstash tar ball] *********************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Extracting logstash] ******************************************************************************
skipping: [192.168.56.120]

TASK [elk_centos : Inserting the Logstash systemd service unit file] *************************************************
ok: [192.168.56.120]

TASK [elk_centos : Script of logstash for starting/stopping] *********************************************************
ok: [192.168.56.120]

TASK [elk_centos : Creating /data/logstash-6.8.15/conf.d directory] **************************************************
ok: [192.168.56.120]

TASK [elk_centos : Updating the configuration default of logstash] ***************************************************
ok: [192.168.56.120]

TASK [elk_centos : Daemon Reload] ************************************************************************************
ok: [192.168.56.120]

TASK [elk_centos : Starting the Logstash service] ********************************************************************
ok: [192.168.56.120]

PLAY [ubuntu] ********************************************************************************************************

TASK [Gathering Facts] ***********************************************************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Termporarily setting the SELINUX of Ubuntu remote server to permissive] ***************************
skipping: [192.168.56.119]

TASK [elk_ubuntu : Updating sysctl for max_map_count] ****************************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Adding the user 'elasticsearch'] ******************************************************************
ok: [192.168.56.119]
```



```
TASK [elk_ubuntu : Creating directory for the downloaded files] *****************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Downloading elasticsearch tar ball] **************************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Extracting elasticsearch] ************************************************************************
skipping: [192.168.56.119]

TASK [elk_ubuntu : Inserting the Elastic Search systemd service unit file] ******************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Inserting the Elastic Search configuration template] *********************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : file] ********************************************************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Daemon Reload] ***********************************************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Starting the Elastic Search service] *************************************************************
changed: [192.168.56.119]

TASK [elk_ubuntu : Creating directory for downloaded files] *********************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Installing Kibana tar] ***************************************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Extracting Kibana] *******************************************************************************
skipping: [192.168.56.119]

TASK [elk_ubuntu : Inserting the Kibana systemd service unit file] **************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Inserting the update of configration template for Kibana] ****************************************
ok: [192.168.56.119]
```

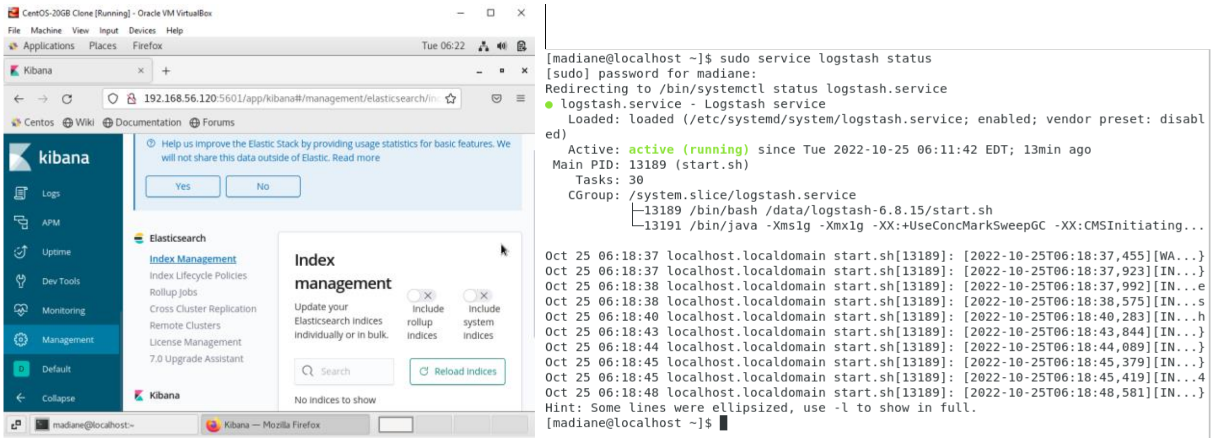


```
TASK [elk_ubuntu : Daemon Reload] ***********************************************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Starting the Kibana service] *********************************************************************
changed: [192.168.56.119]

TASK [elk_ubuntu : Creating directory for downloaded files] *********************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Installing logstash tar ball] ********************************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Extracting logstash] *****************************************************************************
skipping: [192.168.56.119]

TASK [elk_ubuntu : Inserting the Logstash systemd service unit file] ************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Script of logstash for starting/stopping] ********************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Creating /data/logstash-6.8.15/conf.d directory] *************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Updating the configuration default of logstash] **************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Daemon Reload] ***********************************************************************************
ok: [192.168.56.119]

TASK [elk_ubuntu : Starting the Logstash service] *******************************************************************
changed: [192.168.56.119]

PLAY RECAP **********************************************************************************************************
192.168.56.119             : ok=26   changed=3    unreachable=0    failed=0    skipped=5    rescued=0    ignored=0
192.168.56.120             : ok=27   changed=0    unreachable=0    failed=0    skipped=4    rescued=0    ignored=0
```

Figure 3.1 Running the elk_ins.yml playbook

After completing all of the playbook (nagio_ins.yml, main.yml for CentOS and Ubuntu remote servers), I execute the playbook by entering the command "ansible-playbook –ask-become-pass nagio_ins.yml". First, it plays the pre-tasks assigned to all of the remote servers. After that, it runs the play for the ubuntu group and centos group consecutively that consists of tasks that would temporarily set the SELINUX of Ubuntu and CentOS to permissive. Next it will update the sysctl, add a user, create directory for downloaded files (Elastic Search, Kibana, and Logstash), download the files for installing Elastic Search, Kibana, and Logstash, extract the downloaded files, inserts the service files, copy the configuration templates, reload and start the daemon and the Elastic Search, Kibana and Logstash services.

Step 4: Output of the Elastic Stack in CentOS and Ubuntu



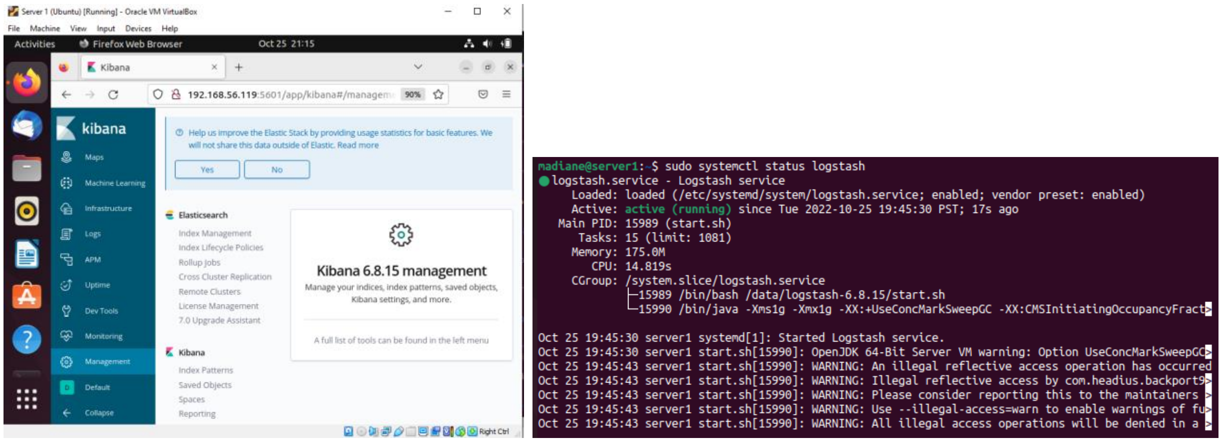
Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. Read more

Update your Elasticsearch indices individually or in bulk.

No indices to show

```
[madiane@localhost ~]$ sudo service logstash status
[sudo] password for madiane:
Redirecting to /bin/systemctl status logstash.service
● logstash.service - Logstash service
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabl
ed)
   Active: active (running) since Tue 2022-10-25 06:11:42 EDT; 13min ago
 Main PID: 13189 (start.sh)
    Tasks: 30
   CGroup: /system.slice/logstash.service
           ├─13189 /bin/bash /data/logstash-6.8.15/start.sh
           └─13191 /bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiating...

Oct 25 06:18:37 localhost.localdomain start.sh[13189]: [2022-10-25T06:18:37,455][WA...}
Oct 25 06:18:37 localhost.localdomain start.sh[13189]: [2022-10-25T06:18:37,923][IN...}
Oct 25 06:18:38 localhost.localdomain start.sh[13189]: [2022-10-25T06:18:37,992][IN...e
Oct 25 06:18:38 localhost.localdomain start.sh[13189]: [2022-10-25T06:18:38,575][IN...s
Oct 25 06:18:40 localhost.localdomain start.sh[13189]: [2022-10-25T06:18:40,283][IN...h
Oct 25 06:18:43 localhost.localdomain start.sh[13189]: [2022-10-25T06:18:43,844][IN...}
Oct 25 06:18:44 localhost.localdomain start.sh[13189]: [2022-10-25T06:18:44,089][IN...}
Oct 25 06:18:45 localhost.localdomain start.sh[13189]: [2022-10-25T06:18:45,379][IN...}
Oct 25 06:18:45 localhost.localdomain start.sh[13189]: [2022-10-25T06:18:45,419][IN...4
Oct 25 06:18:48 localhost.localdomain start.sh[13189]: [2022-10-25T06:18:48,581][IN...}
Hint: Some lines were ellipsized, use -l to show in full.
[madiane@localhost ~]$ █
```

Figure 4.1 Elastic Stack in CentOS



Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. Read more

Kibana 6.8.15 management

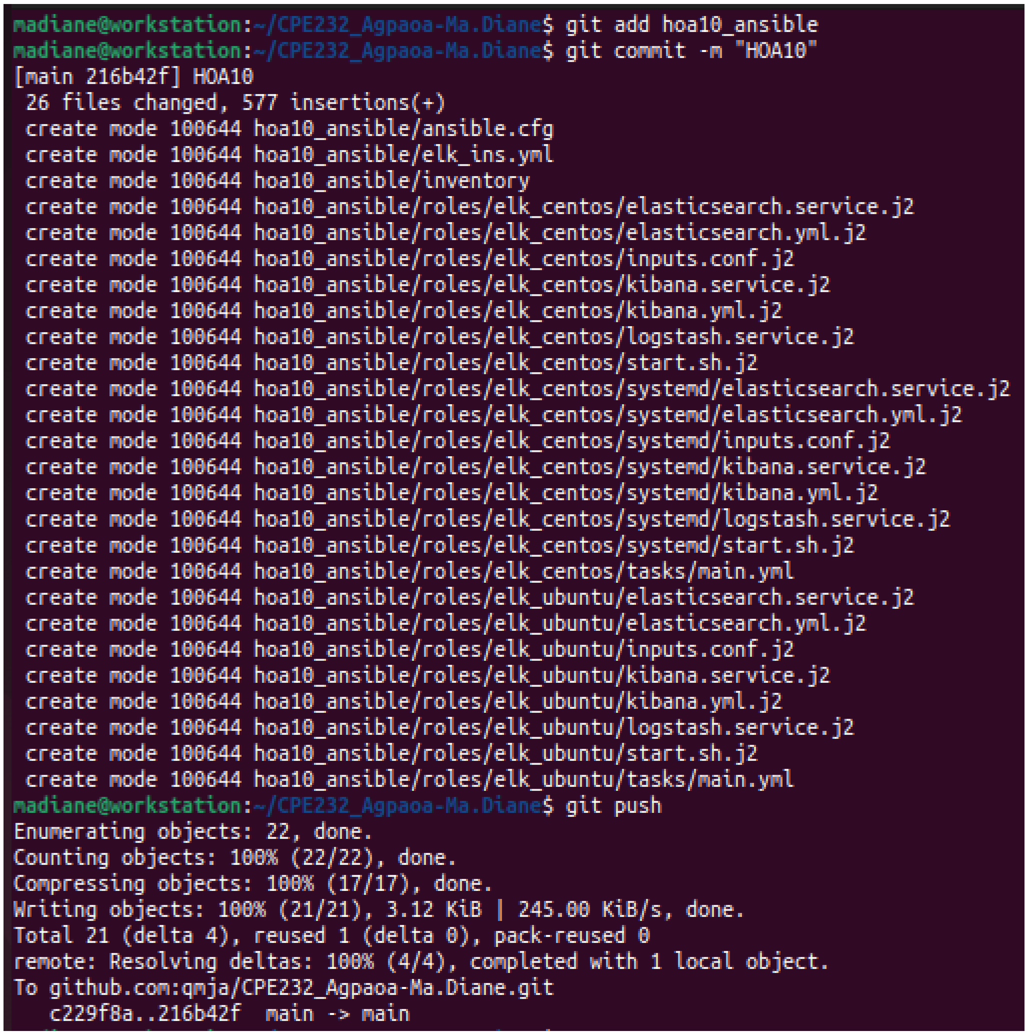
Manage your indices, index patterns, saved objects, Kibana settings, and more.

A full list of tools can be found in the left menu

```
madiane@server1:~$ sudo systemctl status logstash
● logstash.service - Logstash service
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2022-10-25 19:45:30 PST; 17s ago
   Main PID: 15989 (start.sh)
      Tasks: 15 (limit: 1081)
     Memory: 175.0M
        CPU: 14.819s
     CGroup: /system.slice/logstash.service
             ├─15989 /bin/bash /data/logstash-6.8.15/start.sh
             └─15990 /bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFract>

Oct 25 19:45:30 server1 systemd[1]: Started Logstash service.
Oct 25 19:45:30 server1 start.sh[15990]: OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC>
Oct 25 19:45:43 server1 start.sh[15990]: WARNING: An illegal reflective access operation has occurred
Oct 25 19:45:43 server1 start.sh[15990]: WARNING: Illegal reflective access by com.headius.backport9>
Oct 25 19:45:43 server1 start.sh[15990]: WARNING: Please consider reporting this to the maintainers >
Oct 25 19:45:43 server1 start.sh[15990]: WARNING: Use --illegal-access=warn to enable warnings of fu>
Oct 25 19:45:43 server1 start.sh[15990]: WARNING: All illegal access operations will be denied in a >
```

Figure 4.2 Elastic Stack in Ubuntu

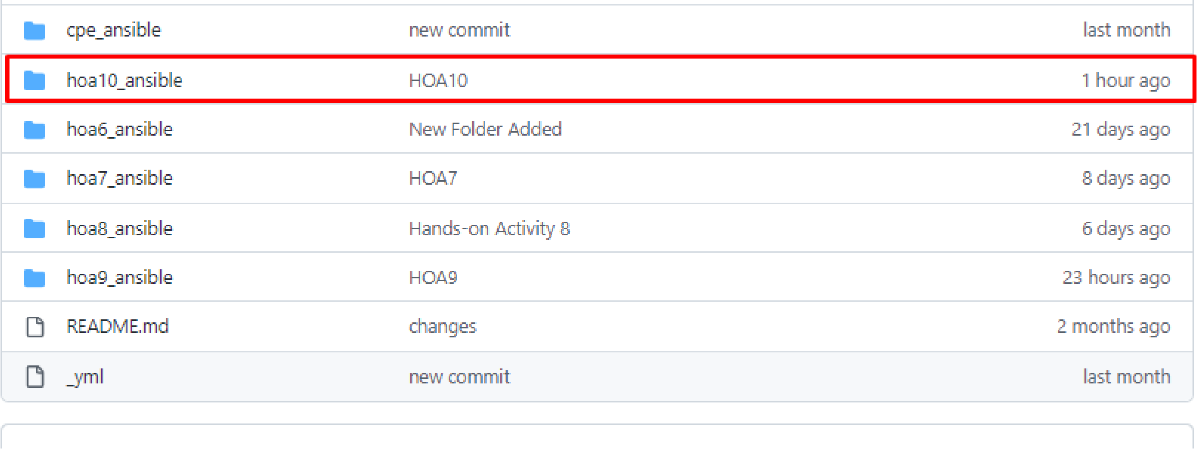
Step 5: Cloning the hoa10_ansible directory to the GitHub



```
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane$ git add hoa10_ansible
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane$ git commit -m "HOA10"
[main 216b42f] HOA10
 26 files changed, 577 insertions(+)
 create mode 100644 hoa10_ansible/ansible.cfg
 create mode 100644 hoa10_ansible/elk_ins.yml
 create mode 100644 hoa10_ansible/inventory
 create mode 100644 hoa10_ansible/roles/elk_centos/elasticsearch.service.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/elasticsearch.yml.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/inputs.conf.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/kibana.service.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/kibana.yml.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/logstash.service.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/start.sh.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/systemd/elasticsearch.service.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/systemd/elasticsearch.yml.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/systemd/inputs.conf.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/systemd/kibana.service.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/systemd/kibana.yml.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/systemd/logstash.service.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/systemd/start.sh.j2
 create mode 100644 hoa10_ansible/roles/elk_centos/tasks/main.yml
 create mode 100644 hoa10_ansible/roles/elk_ubuntu/elasticsearch.service.j2
 create mode 100644 hoa10_ansible/roles/elk_ubuntu/elasticsearch.yml.j2
 create mode 100644 hoa10_ansible/roles/elk_ubuntu/inputs.conf.j2
 create mode 100644 hoa10_ansible/roles/elk_ubuntu/kibana.service.j2
 create mode 100644 hoa10_ansible/roles/elk_ubuntu/kibana.yml.j2
 create mode 100644 hoa10_ansible/roles/elk_ubuntu/logstash.service.j2
 create mode 100644 hoa10_ansible/roles/elk_ubuntu/start.sh.j2
 create mode 100644 hoa10_ansible/roles/elk_ubuntu/tasks/main.yml
madiane@workstation:~/CPE232_Agpaoa-Ma.Diane$ git push
Enumerating objects: 22, done.
Counting objects: 100% (22/22), done.
Compressing objects: 100% (17/17), done.
Writing objects: 100% (21/21), 3.12 KiB | 245.00 KiB/s, done.
Total 21 (delta 4), reused 1 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (4/4), completed with 1 local object.
To github.com:qmja/CPE232_Agpaoa-Ma.Diane.git
   c229f8a..216b42f  main -> main
```

Figure 5.1 Saving the hoa10_ansible directory to the GitHub

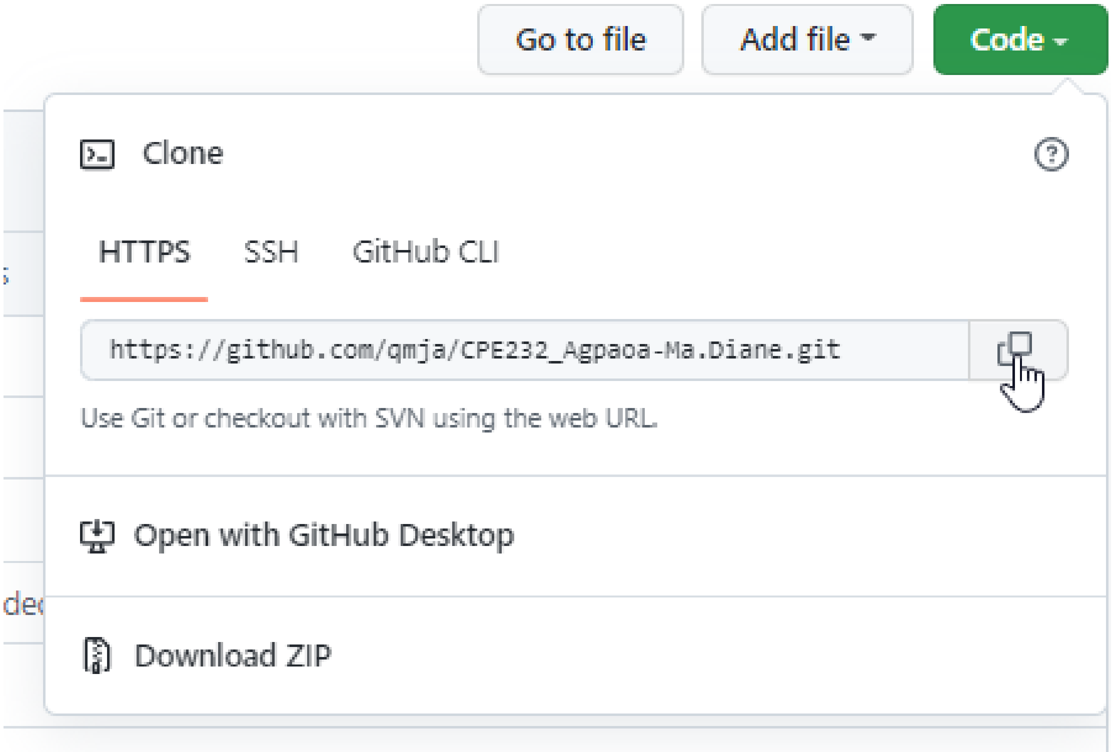
In order to save the hoa10_ansible directory to the GitHub, I entered the command "git add hoa10_ansible", then I committed the changes to GitHub and lastly entered the command git push which will execute the committed changes.



cpe_ansible	new commit	last month
hoa10_ansible	HOA10	1 hour ago
hoa6_ansible	New Folder Added	21 days ago
hoa7_ansible	HOA7	8 days ago
hoa8_ansible	Hands-on Activity 8	6 days ago
hoa9_ansible	HOA9	23 hours ago
README.md	changes	2 months ago
_yml	new commit	last month

Figure 5.2 GitHub Repository

To verify the changes, I checked the GitHub, which will show each of the folders and the last time it was altered, this also shows the “HOA10” phrase that I input in committing the changes which verifies that I successfully added the hoa10_ansible directory in the GitHub.



```
https://github.com/qmja/CPE232_Agpaoa-Ma.Diane.git
```

Use Git or checkout with SVN using the web URL.

Figure 5.2 Copying the HTTP Link of GitHub

GitHub Link: https://github.com/qmja/CPE232_Agpaoa-Ma.Diane.git

Reflections:

Answer the following:

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

   Log monitoring tool collects logs from workloads to centralized the logging capabilities. Some Log monitoring tools such as ELK stack allows the user to aggregate logs from complex cloud environments to searchable index. With this capability the security and root cause analysis capabilities of a user, administrator or company would increase.

Conclusions:

In conclusion, this activity helped me to learn about the installation and configuration of Elastic Stack (Elastic Search, Kibana, and Logstash) using a playbook while implementing roles to consolidate the playbooks. In addition, this activity helped me to learn new codes and ways that can be used in creating ansible playbooks. This activity also helped me to understand more about creating and designing playbooks that bvan be used in installation and configuration of log monitoring tools. Lastly, I learned about the log monitoring tools and its benefits to the users. I learned that using log monitoring tools could help improve a user, administrator or a company’s security and root cause analysis capabilities.