Name: Pacinos, Angela Monique A.	**Date Performed:** 10-30-23
Course/Section: CPE232 - CPE31S4	**Date Submitted:** 10-31-23
Instructor: Dr. Jonathan V. Taylar	**Semester and SY:** 1st Sem: ‘23 - ‘24

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.

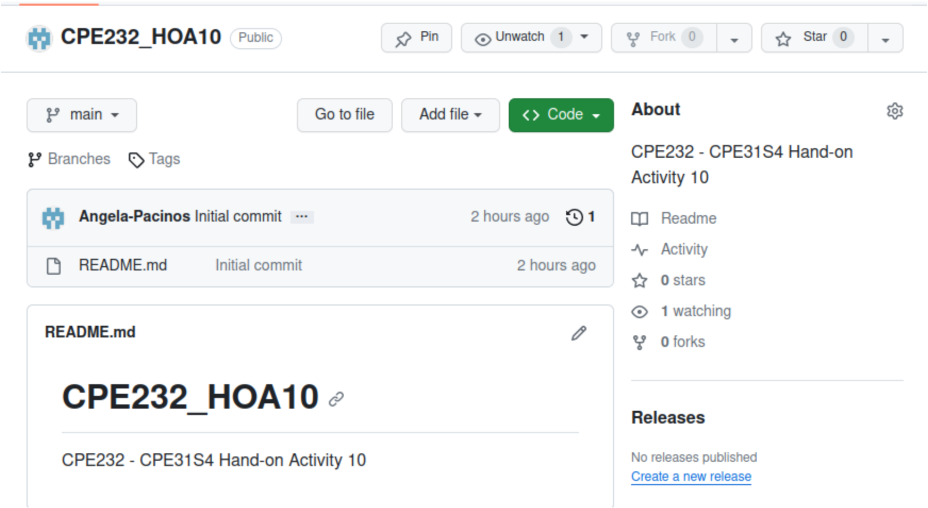
Source: https://www.graylog.org/products/open-source

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)

INPUT
● **Create a new repository and configure it with the needed files.**



Angela-Pacinos Initial commit ··· 2 hours ago 1

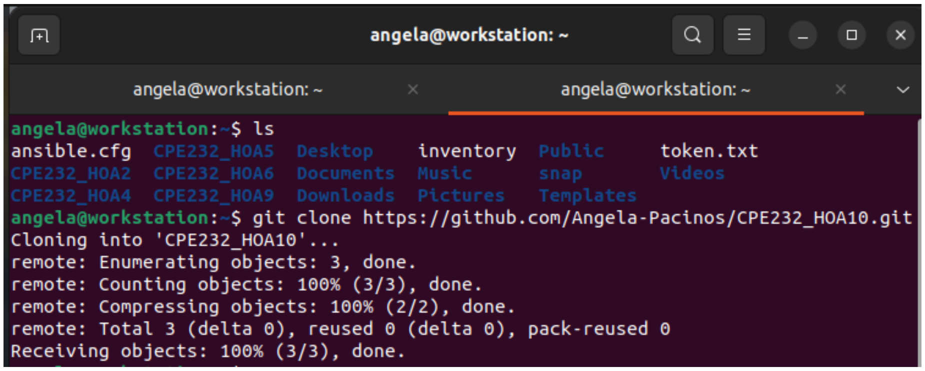
README.md Initial commit 2 hours ago

CPE232 - CPE31S4 Hand-on Activity 10

README.md

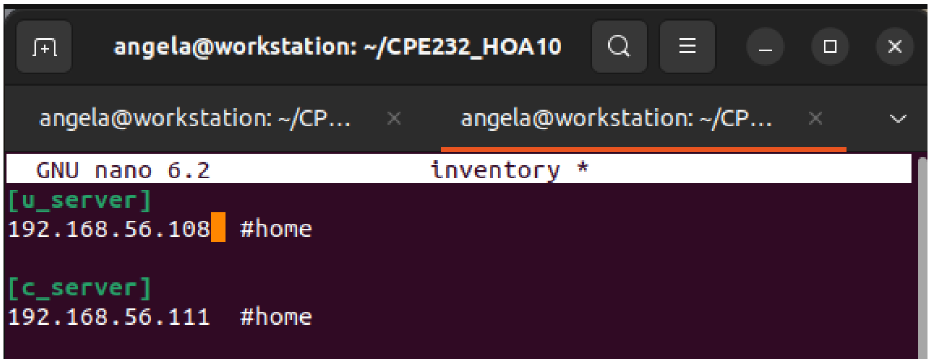
CPE232_HOA10

CPE232 - CPE31S4 Hand-on Activity 10

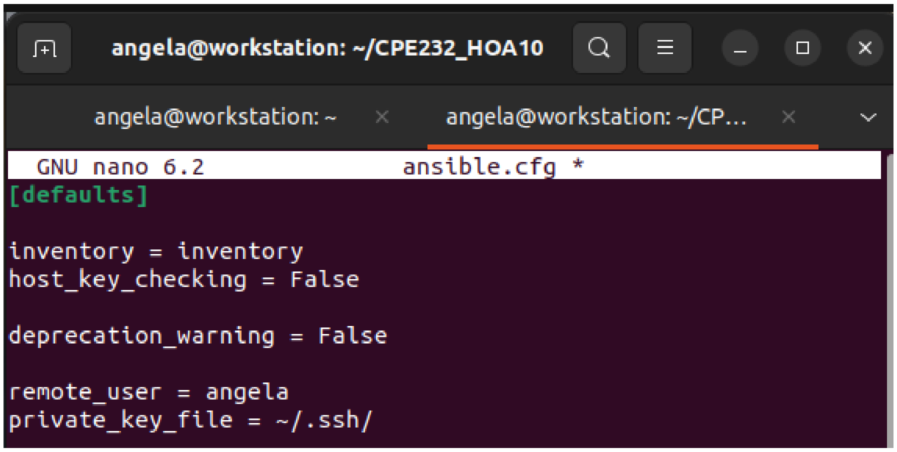


```
angela@workstation:~$ ls
ansible.cfg  CPE232_HOA5  Desktop    inventory  Public     token.txt
CPE232_HOA2  CPE232_HOA6  Documents  Music      snap       Videos
CPE232_HOA4  CPE232_HOA9  Downloads  Pictures   Templates
angela@workstation:~$ git clone https://github.com/Angela-Pacinos/CPE232_HOA10.git
Cloning into 'CPE232_HOA10'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
```

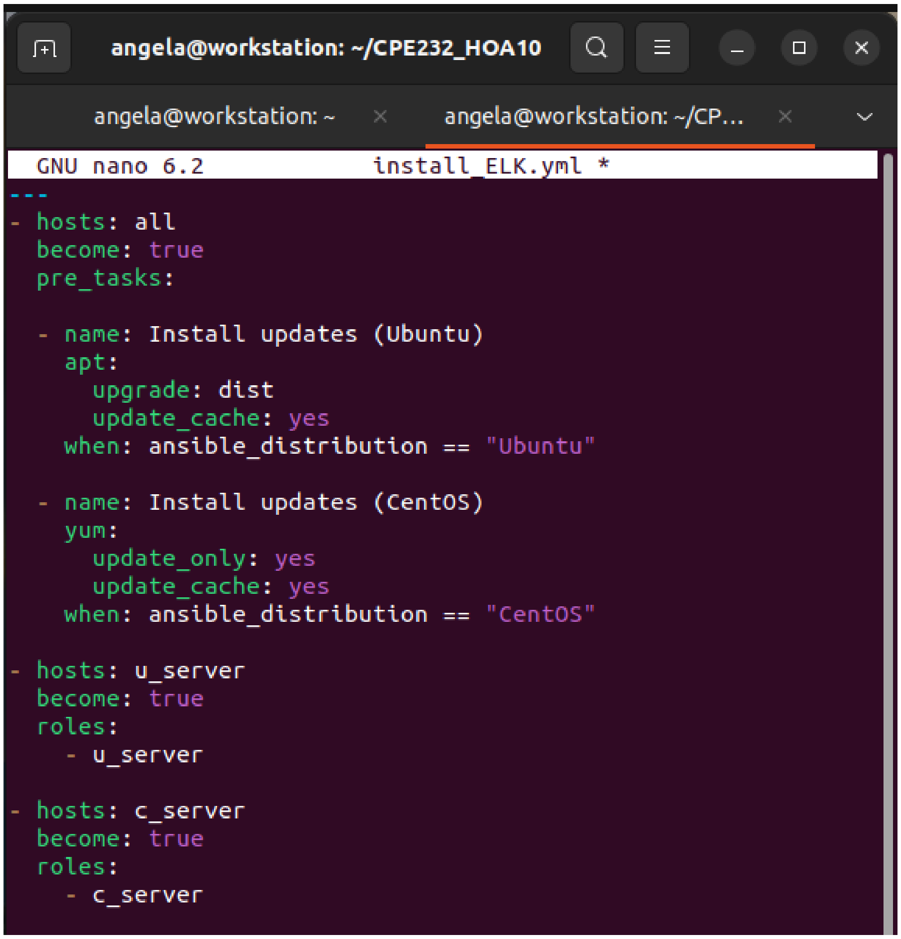
Create the inventory, ansible.cfg, and your yml playbook then configure as follows.


angela@workstation: ~/CPE232_HOA10
angela@workstation: ~/CP...
angela@workstation: ~/CP...

```
  GNU nano 6.2                  inventory *
[u_server]
192.168.56.108  #home

[c_server]
192.168.56.111  #home
```

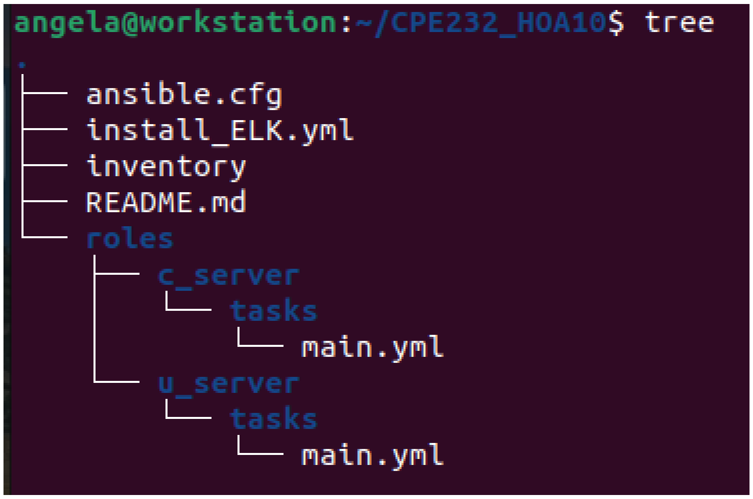

angela@workstation: ~/CPE232_HOA10
angela@workstation: ~
angela@workstation: ~/CP...

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

inventory = inventory
host_key_checking = False

deprecation_warning = False

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


angela@workstation: ~/CPE232_HOA10
angela@workstation: ~
angela@workstation: ~/CP...

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

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

  - name: Install updates (CentOS)
    yum:
      update_only: yes
      update_cache: yes
    when: ansible_distribution == "CentOS"

- hosts: u_server
  become: true
  roles:
    - u_server

- hosts: c_server
  become: true
  roles:
    - c_server
```

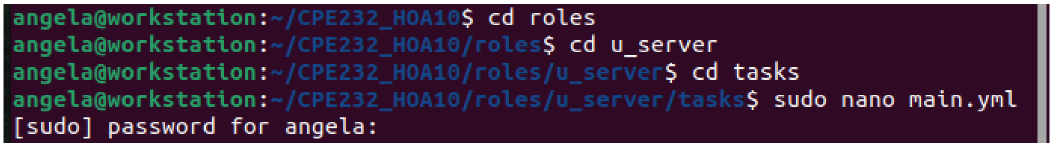
Under the same directory, create a new directory and name it roles. Enter the roles directory and create new directories: Ubuntu and CentOS. For each directory, create a directory and name it tasks.



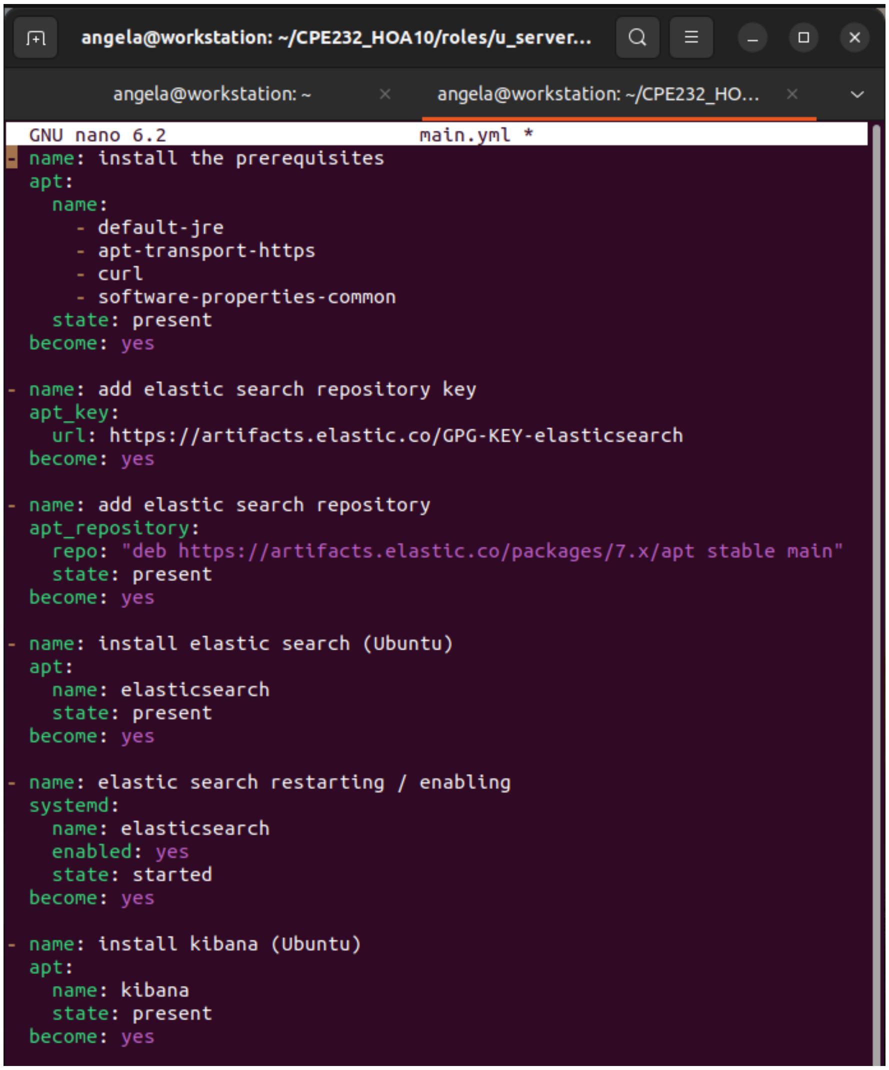
```
angela@workstation:~/CPE232_HOA10$ tree
.
├── ansible.cfg
├── install_ELK.yml
├── inventory
├── README.md
└── roles
    ├── c_server
    │   └── tasks
    │       └── main.yml
    └── u_server
        └── tasks
            └── main.yml
```

- **Install Elastic Stack package**
  Edit the main.yml for both Ubuntu and CentOS directory as follows. Save and exit

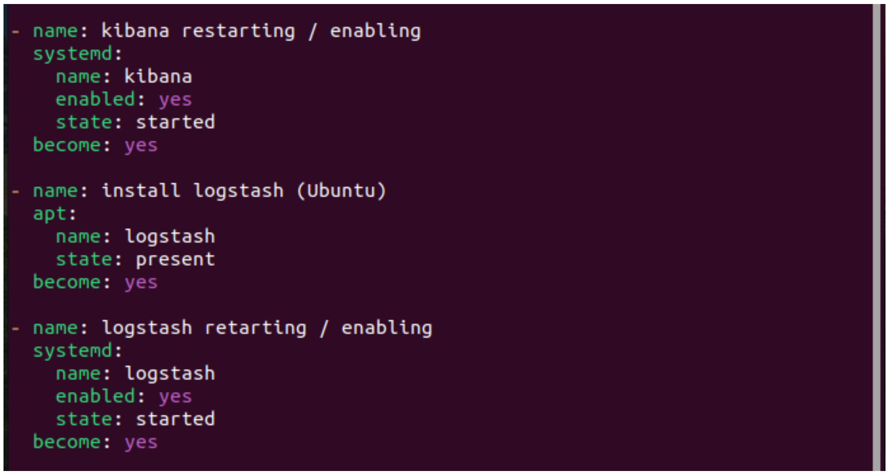
Ubuntu



```
angela@workstation:~/CPE232_HOA10$ cd roles
angela@workstation:~/CPE232_HOA10/roles$ cd u_server
angela@workstation:~/CPE232_HOA10/roles/u_server$ cd tasks
angela@workstation:~/CPE232_HOA10/roles/u_server/tasks$ sudo nano main.yml
[sudo] password for angela:
```

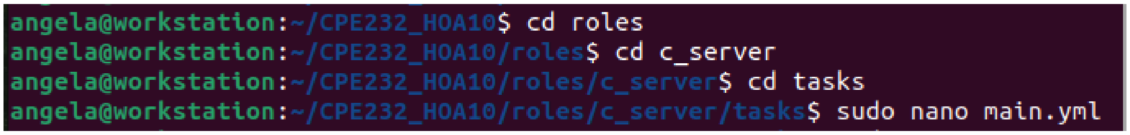

angela@workstation: ~/CPE232_HOA10/roles/u_server...
angela@workstation: ~
angela@workstation: ~/CPE232_HO...

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

- name: add elastic search repository key
  apt_key:
    url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
  become: yes

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

- name: install elastic search (Ubuntu)
  apt:
    name: elasticsearch
    state: present
  become: yes

- name: elastic search restarting / enabling
  systemd:
    name: elasticsearch
    enabled: yes
    state: started
  become: yes

- name: install kibana (Ubuntu)
  apt:
    name: kibana
    state: present
  become: yes
```

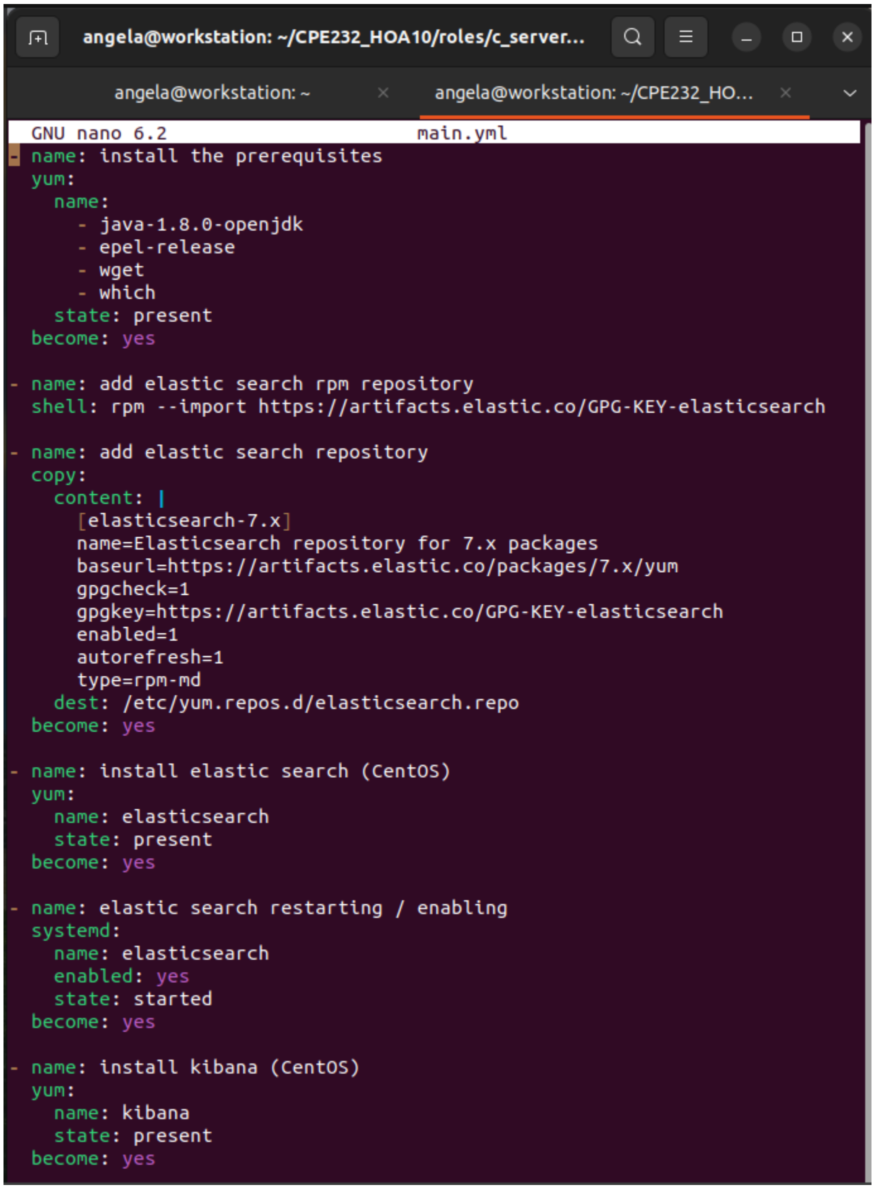


```
- name: kibana restarting / enabling
  systemd:
    name: kibana
    enabled: yes
    state: started
  become: yes

- name: install logstash (Ubuntu)
  apt:
    name: logstash
    state: present
  become: yes

- name: logstash retarting / enabling
  systemd:
    name: logstash
    enabled: yes
    state: started
  become: yes
```

CentOS

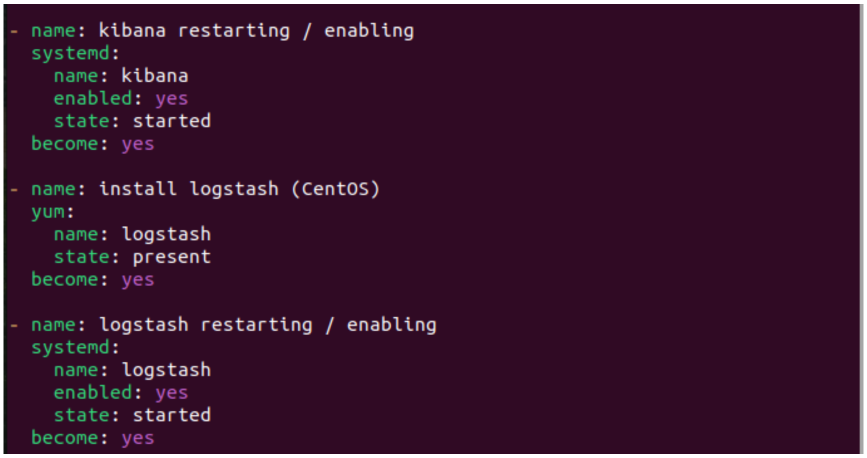


```
angela@workstation:~/CPE232_HOA10$ cd roles
angela@workstation:~/CPE232_HOA10/roles$ cd c_server
angela@workstation:~/CPE232_HOA10/roles/c_server$ cd tasks
angela@workstation:~/CPE232_HOA10/roles/c_server/tasks$ sudo nano main.yml
```



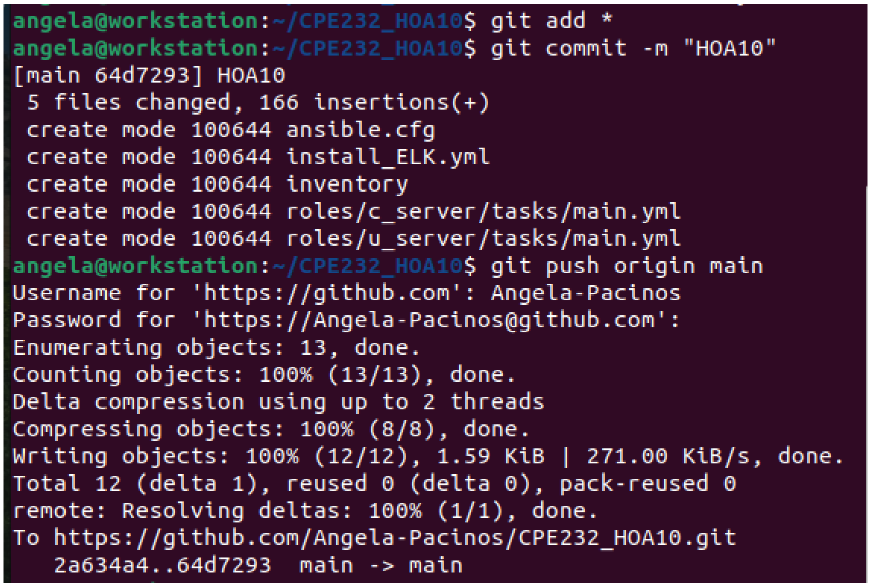
angela@workstation: ~/CPE232_HOA10/roles/c_server...
angela@workstation: ~
angela@workstation: ~/CPE232_HO...

```
GNU nano 6.2                          main.yml
- name: install the prerequisites
  yum:
    name:
      - java-1.8.0-openjdk
      - epel-release
      - wget
      - which
    state: present
  become: yes

- name: add elastic search rpm repository
  shell: rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

- name: add elastic search 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 elastic search (CentOS)
  yum:
    name: elasticsearch
    state: present
  become: yes

- name: elastic search restarting / enabling
  systemd:
    name: elasticsearch
    enabled: yes
    state: started
  become: yes

- name: install kibana (CentOS)
  yum:
    name: kibana
    state: present
  become: yes
```



```
- name: kibana restarting / enabling
  systemd:
    name: kibana
    enabled: yes
    state: started
  become: yes

- name: install logstash (CentOS)
  yum:
    name: logstash
    state: present
  become: yes

- name: logstash restarting / enabling
  systemd:
    name: logstash
    enabled: yes
    state: started
  become: yes
```

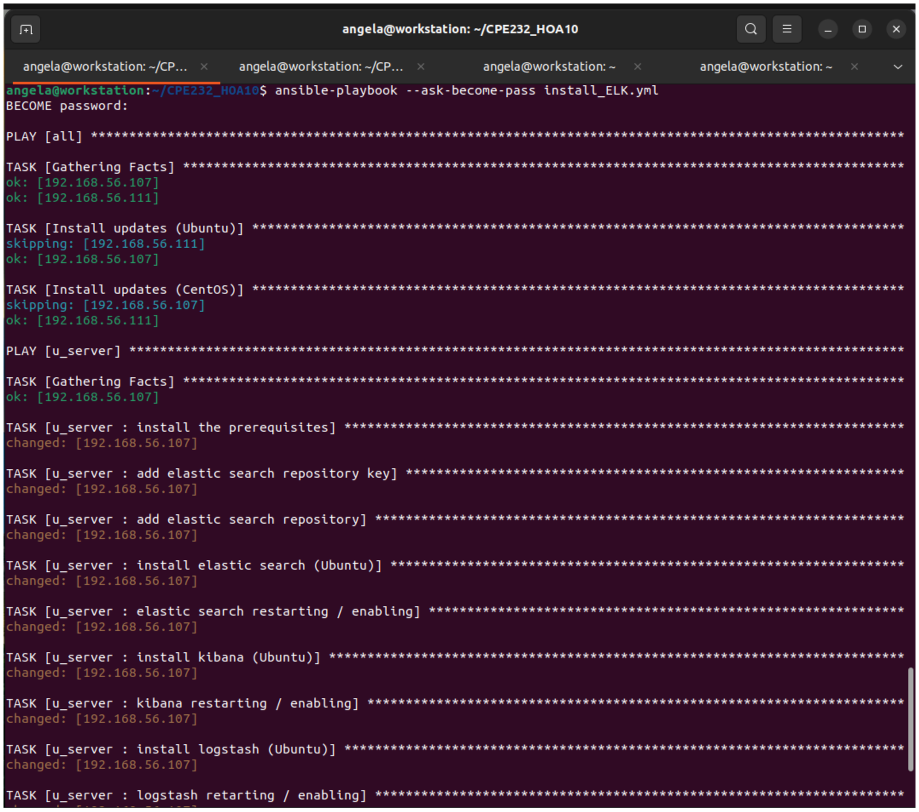
- **Make sure that the repository is sync in the Github**



```
angela@workstation:~/CPE232_HOA10$ git add *
angela@workstation:~/CPE232_HOA10$ git commit -m "HOA10"
[main 64d7293] HOA10
 5 files changed, 166 insertions(+)
 create mode 100644 ansible.cfg
 create mode 100644 install_ELK.yml
 create mode 100644 inventory
 create mode 100644 roles/c_server/tasks/main.yml
 create mode 100644 roles/u_server/tasks/main.yml
angela@workstation:~/CPE232_HOA10$ git push origin main
Username for 'https://github.com': Angela-Pacinos
Password for 'https://Angela-Pacinos@github.com':
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), 1.59 KiB | 271.00 KiB/s, done.
Total 12 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), done.
To https://github.com/Angela-Pacinos/CPE232_HOA10.git
   2a634a4..64d7293  main -> main
```

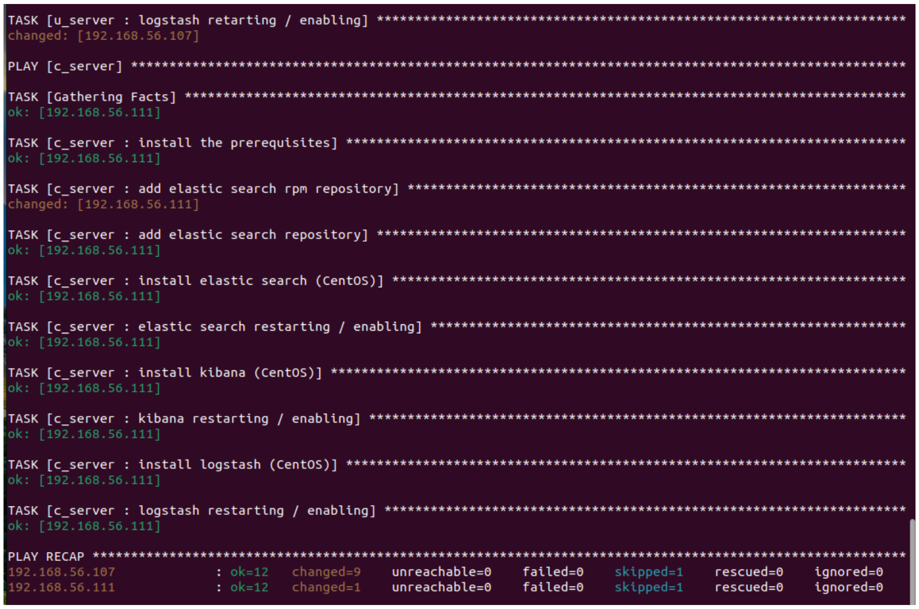
PROCESS

- **Run the install_ELK.yml**



angela@workstation: ~/CPE232_HOA10
angela@workstation: ~/CP...
angela@workstation: ~/CP...
angela@workstation: ~
angela@workstation: ~

```
angela@workstation:~/CPE232_HOA10$ ansible-playbook --ask-become-pass install_ELK.yml
BECOME password:

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

TASK [Gathering Facts] ************************************************************************************
ok: [192.168.56.107]
ok: [192.168.56.111]

TASK [Install updates (Ubuntu)] ***************************************************************************
skipping: [192.168.56.111]
ok: [192.168.56.107]

TASK [Install updates (CentOS)] ***************************************************************************
skipping: [192.168.56.107]
ok: [192.168.56.111]

PLAY [u_server] *******************************************************************************************

TASK [Gathering Facts] ************************************************************************************
ok: [192.168.56.107]

TASK [u_server : install the prerequisites] ***************************************************************
changed: [192.168.56.107]

TASK [u_server : add elastic search repository key] *******************************************************
changed: [192.168.56.107]

TASK [u_server : add elastic search repository] ***********************************************************
changed: [192.168.56.107]

TASK [u_server : install elastic search (Ubuntu)] *********************************************************
changed: [192.168.56.107]

TASK [u_server : elastic search restarting / enabling] ****************************************************
changed: [192.168.56.107]

TASK [u_server : install kibana (Ubuntu)] *****************************************************************
changed: [192.168.56.107]

TASK [u_server : kibana restarting / enabling] ************************************************************
changed: [192.168.56.107]

TASK [u_server : install logstash (Ubuntu)] ***************************************************************
changed: [192.168.56.107]

TASK [u_server : logstash retarting / enabling] ***********************************************************
```

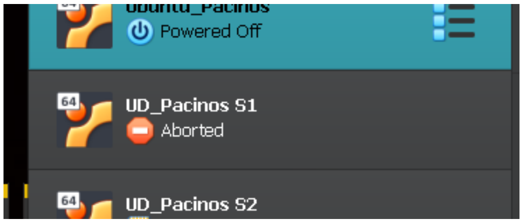


```
TASK [u_server : logstash retarting / enabling] ***********************************************************
changed: [192.168.56.107]

PLAY [c_server] *******************************************************************************************

TASK [Gathering Facts] ************************************************************************************
ok: [192.168.56.111]

TASK [c_server : install the prerequisites] ***************************************************************
ok: [192.168.56.111]

TASK [c_server : add elastic search rpm repository] *******************************************************
changed: [192.168.56.111]

TASK [c_server : add elastic search repository] ***********************************************************
ok: [192.168.56.111]

TASK [c_server : install elastic search (CentOS)] *********************************************************
ok: [192.168.56.111]

TASK [c_server : elastic search restarting / enabling] ****************************************************
ok: [192.168.56.111]

TASK [c_server : install kibana (CentOS)] *****************************************************************
ok: [192.168.56.111]

TASK [c_server : kibana restarting / enabling] ************************************************************
ok: [192.168.56.111]

TASK [c_server : install logstash (CentOS)] ***************************************************************
ok: [192.168.56.111]

TASK [c_server : logstash restarting / enabling] **********************************************************
ok: [192.168.56.111]

PLAY RECAP ************************************************************************************************
192.168.56.107             : ok=12   changed=9    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0
192.168.56.111             : ok=12   changed=1    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0
```

OUTPUT

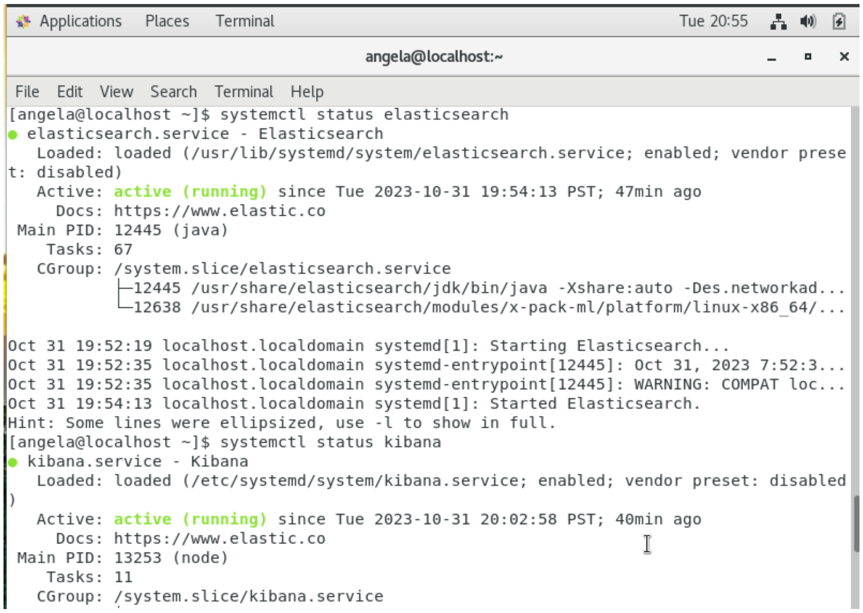
- **Check to see if the prometheus was successfully installed.**

UBUNTU

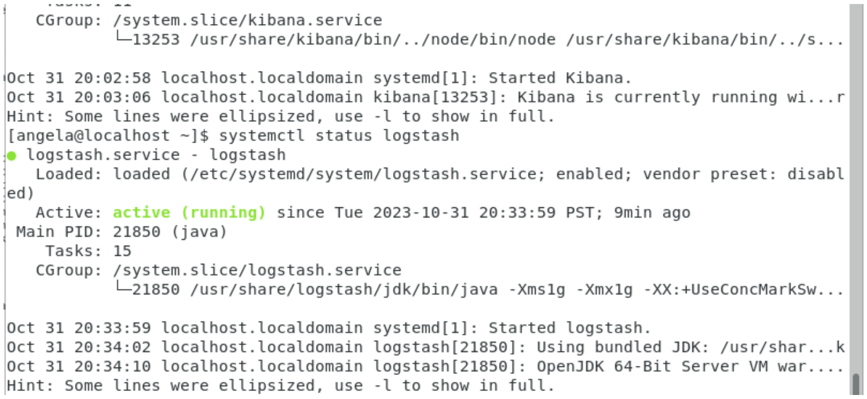


I am once again not able to screenshot the page of the working ELK as the server1 where it was installed abruptly stopped working and not opening. I am not able to use the server2 to do it all again since it is displaying an error of not being able to accept any installation or modification for 2 days.

CENTOS



```
[angela@localhost ~]$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor prese
t: disabled)
   Active: active (running) since Tue 2023-10-31 19:54:13 PST; 47min ago
     Docs: https://www.elastic.co
 Main PID: 12445 (java)
    Tasks: 67
   CGroup: /system.slice/elasticsearch.service
           ├─12445 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkad...
           └─12638 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/...

Oct 31 19:52:19 localhost.localdomain systemd[1]: Starting Elasticsearch...
Oct 31 19:52:35 localhost.localdomain systemd-entrypoint[12445]: Oct 31, 2023 7:52:3...
Oct 31 19:52:35 localhost.localdomain systemd-entrypoint[12445]: WARNING: COMPAT loc...
Oct 31 19:54:13 localhost.localdomain systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
[angela@localhost ~]$ systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled
)
   Active: active (running) since Tue 2023-10-31 20:02:58 PST; 40min ago
     Docs: https://www.elastic.co
 Main PID: 13253 (node)
    Tasks: 11
   CGroup: /system.slice/kibana.service
```



```
   CGroup: /system.slice/kibana.service
           └─13253 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../s...

Oct 31 20:02:58 localhost.localdomain systemd[1]: Started Kibana.
Oct 31 20:03:06 localhost.localdomain kibana[13253]: Kibana is currently running wi...r
Hint: Some lines were ellipsized, use -l to show in full.
[angela@localhost ~]$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabl
ed)
   Active: active (running) since Tue 2023-10-31 20:33:59 PST; 9min ago
 Main PID: 21850 (java)
    Tasks: 15
   CGroup: /system.slice/logstash.service
           └─21850 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSw...

Oct 31 20:33:59 localhost.localdomain systemd[1]: Started logstash.
Oct 31 20:34:02 localhost.localdomain logstash[21850]: Using bundled JDK: /usr/shar...k
Oct 31 20:34:10 localhost.localdomain logstash[21850]: OpenJDK 64-Bit Server VM war....
Hint: Some lines were ellipsized, use -l to show in full.
```

Reflections:

Answer the following:

1. **What are the benefits of having a log monitoring tool?**
   Log monitoring tools are important and provide benefits on the systems. This provides security where it monitors the log files that are generated by the servers means that it can detect if there are any suspicious activities or issues. It is also helpful in maintaining the infrastructure of a system as it can give the history of events that have happened which will make troubleshooting much easier. Overall, this log monitoring tool provides efficiency and effectiveness that maintains the system, its security and performance.

Conclusions:

This activity took more time in creating as it requires to install the Elastic stack into 3 hosts. I also had a problem again with the ubuntu stopping abruptly (server1) and wasn't able to use the server2 as it is displaying an error where it can't be installed or modified for 2 days. I did some search on how to install the packages and what the requirements are for this. For one of the sites, I saw that java should also be installed into the remote server that is why I also incorporated it. For the individual installation of the ELK, I just tried and errored it since I didn't want to copy all of the source. I also had issues again with the install_ELK.yml that I made. That is why I just copied the contents from my install_Prometheus.yml from the last activity. Overall, the waiting time that was allotted to see if every try will succeed was okay since at the end the playbook was working and I got to see different ways to do it.

source: https://logz.io/blog/elk-stack-ansible/

"I affirm that I will not give or receive any unauthorized help on this activity and that all work will be my own."