Name:	Date Performed:
Course/Section:	Date Submitted:
Instructor:	Semester and SY:

Activity 10: Install, Configure, and Manage Log Monitoring tools

1. Objectives

Create and design a workflow that installs, configure and manage enterprise log monitoring tools using Ansible as an Infrastructure as Code (IaC) tool.

2. Discussion

Log monitoring software scans and monitors log files generated by servers, applications, and networks. By detecting and alerting users to patterns in these log files, log monitoring software helps solve performance and security issues. System administrators use log monitoring software to detect common important events indicated by log files.

Log monitoring software helps maintain IT infrastructure performance and pinpoints issues to prevent downtime and mitigate risks. These tools will often integrate with IT alerting software, log analysis software, and other IT issue resolution products to more aptly flesh out the IT infrastructure maintenance ecosystem.

To qualify for inclusion in the Log Monitoring category, a product must:

- Monitor the log files generated by servers, applications, or networks
- Alert users when important events are detected
- Provide reporting capabilities for log files

Elastic Stack

ELK suite stands for Elasticsearch, Kibana, Beats, and Logstash (also known as the ELK Stack). Source: https://www.elastic.co/elastic-stack

The Elastic Stack is a group of open source products from Elastic designed to help users take data from any type of source and in any format, and search, analyze and visualize that data in real time. The product group was formerly known as the ELK Stack for the core products in the group -- Elasticsearch, Logstash and Kibana -- but has been rebranded as the Elastic Stack. A fourth product, Beats, was subsequently added to the stack. The Elastic Stack can be deployed on premises or made available as software as a service (SaaS). Elasticsearch supports Amazon Web Services (AWS), Google Cloud Platform and Microsoft Azure.

GrayLog

Graylog is a powerful platform that allows for easy log management of both structured and unstructured data along with debugging applications.

It is based on Elasticsearch, MongoDB, and Scala. Graylog has a main server, which receives data from its clients installed on different servers, and a web interface, which visualizes the data and allows to work with logs aggregated by the main server.

We use Graylog primarily as the stash for the logs of the web applications we build. However, it is also effective when working with raw strings (i.e. syslog): the tool parses it into the structured data we need. It also allows advanced custom search in the logs using structured queries. In other words, when integrated properly with a web app, Graylog helps engineers to analyze the system behavior on almost per code line basis.

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

3. Tasks

1. Create a playbook that:
    a. Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)
2. Apply the concept of creating roles.
3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like a manual.)
4. Show an output of the installed Elastic Stack for both Ubuntu and CentOS.
5. Make sure to create a new repository in GitHub for this activity.

4. Output (screenshots and explanations)

I created a new repository for this activity

```
joshua@ManagedNode:~$ git clone git@github.com:qjlcastillo/HOA10.git
Cloning into 'HOA10'...
warning: You appear to have cloned an empty repository.
joshua@ManagedNode:~$ ls
ANSIBLE_CASTILLO  Desktop    HOA10  Music       Public    Templates
CPE232_CASTILLO   Documents  HOA8   Pictures    site.yml  Videos
CPE232_CASTILLO1  Downloads  HOA9   prometheus  snap
joshua@ManagedNode:~$ cd HOA10
joshua@ManagedNode:~/HOA10$
```

/etc/ansible/ansible.cfg:

```
joshua@ManagedNode: ~/HOA10
  GNU nano 7.2                    /etc/ansible/ansible.cfg
[defaults]
inventory = /etc/ansible/hosts
private_ket_file = ~/.ssh/id_rsa
```

/etc/ansible/hosts:

```
joshua@ManagedNode: ~/HOA10
  GNU nano 7.2                    /etc/ansible/hosts
[ubuntu]
192.168.56.103  ansible_python_interpreter=/usr/bin/python3
[centos]
192.168.56.105  ansible_ssh_user=root ansible_ssh_pass=99Castillo03523  ansible>
```

i created sub directories under HOA10 repository which looks like this:

```
joshua@ManagedNode:~/HOA10/roles$ tree
.
├── centos
│   └── tasks
│       └── main.yaml
└── ubuntu
    └── tasks
        └── main.yaml

5 directories, 2 files
```

/ubuntu/tasks/main.yml:

```yaml
---

- name: Install necessary prerequisites
  apt:
    name:
      - default-jre
      - apt-transport-https
      - curl
      - software-properties-common
    state: present
  become: yes

- name: Add Elasticsearch APT repository GPG key
  apt_key:
    url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
  become: yes

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

- name: Install Elasticsearch
  apt:
    name: elasticsearch
    state: present
  become: yes
```

```yaml
- name: Enable and start Elasticsearch service
  systemd:
    name: elasticsearch
    enabled: yes
    state: started
  become: yes

- name: Install Kibana
  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
  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 services
  systemd:
    name: "{{ item }}"
    state: restarted
  loop:
    - elasticsearch
    - kibana
```

/centos/tasks/main.yml:

```yaml
---

- name: Install necessary prerequisites
  dnf:
    name:
      - java-1.8.0-openjdk
      - epel-release
      - wget
      - which
    state: present
  become: yes

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

- name: Add the Elasticsearch YUM 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
  dnf:
    name: elasticsearch
    state: present
  become: yes
```

```yaml
- name: Enable and start Elasticsearch service
  systemd:
    name: elasticsearch
    enabled: yes
    state: started
  become: yes

- name: Install Kibana
  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
  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 services
  systemd:
    name: "{{ item }}"
    state: restarted
  loop:
    - elasticsearch
    - kibana
```

elasticstack.yml:

```yaml
- hosts: all
  become: true
  pre_tasks:

  - name: install updates (CentOS)
    dnf:
      update_only: yes
      update_cache: yes
    when: ansible_distribution == "Centos"

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

- hosts: centos
  become: true
  roles:
    - elastic_centos

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

run the elasticstack.yml (main playbook):

```
joshua@ManagedNode:~/HOA10$ ansible-playbook --ask-become-pass elasticstack.yml
BECOME password:

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

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

TASK [install updates (CentOS)] ************************************************
skipping: [192.168.56.103]
skipping: [192.168.56.105]

TASK [install updates (Ubuntu)] ************************************************
skipping: [192.168.56.105]
ok: [192.168.56.103]

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

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

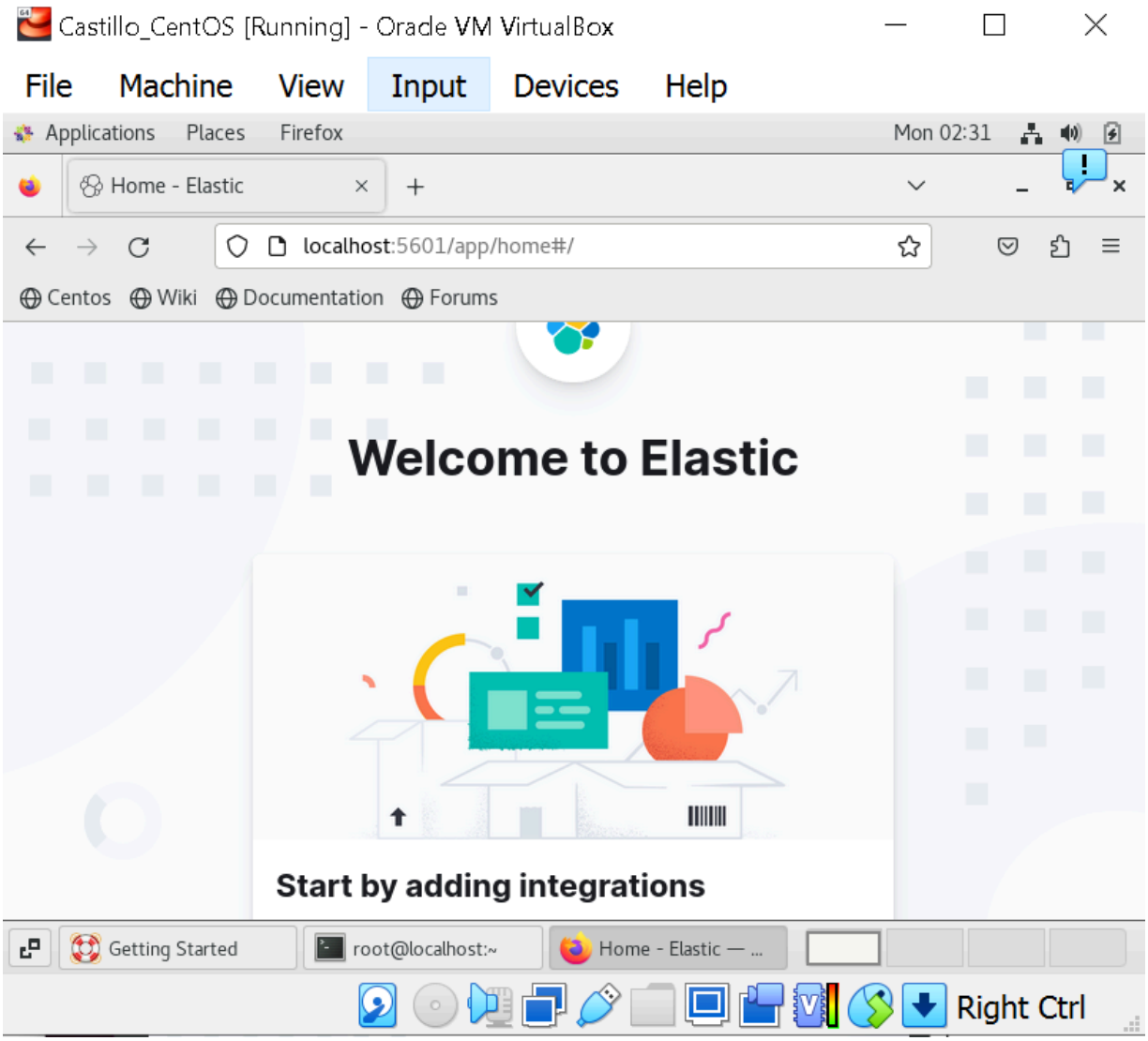
```
TASK [centos : Install necessary prerequisites] ********************************
ok: [192.168.56.105]

TASK [centos : Add Elasticsearch RPM repository GPG key] ***********************
changed: [192.168.56.105]

TASK [centos : Add the Elasticsearch YUM repository] ***************************
changed: [192.168.56.105]

TASK [centos : Install Elasticsearch] ******************************************
changed: [192.168.56.105]

TASK [centos : Enable and start Elasticsearch service] *************************
changed: [192.168.56.105]

TASK [centos : Install Kibana] *************************************************
changed: [192.168.56.105]

TASK [centos : Enable and start Kibana service] ********************************
changed: [192.168.56.105]

TASK [centos : Install Logstash] ***********************************************
changed: [192.168.56.105]
```

```
TASK [centos : Enable and start Logstash service] ******************************
changed: [192.168.56.105]

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

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

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

TASK [ubuntu : Install necessary prerequisites] ********************************
changed: [192.168.56.103]

TASK [ubuntu : Add Elasticsearch APT repository GPG key] ***********************
changed: [192.168.56.103]

TASK [ubuntu : Add the Elasticsearch APT repository] ***************************
changed: [192.168.56.103]

TASK [ubuntu : Install Elasticsearch] ******************************************
changed: [192.168.56.103]
```

```
TASK [ubuntu : Install Kibana] *************************************************
changed: [192.168.56.103]

TASK [ubuntu : Enable and start Kibana service] ********************************
changed: [192.168.56.103]

TASK [ubuntu : Install Logstash] ***********************************************
changed: [192.168.56.103]

TASK [ubuntu : Enable and start Logstash service] ******************************
changed: [192.168.56.103]

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

PLAY RECAP *********************************************************************
192.168.56.103             : ok=13   changed=10   unreachable=0    failed=0    s
kipped=1    rescued=0    ignored=0
192.168.56.105             : ok=12   changed=9    unreachable=0    failed=0    s
kipped=2    rescued=0    ignored=0
```

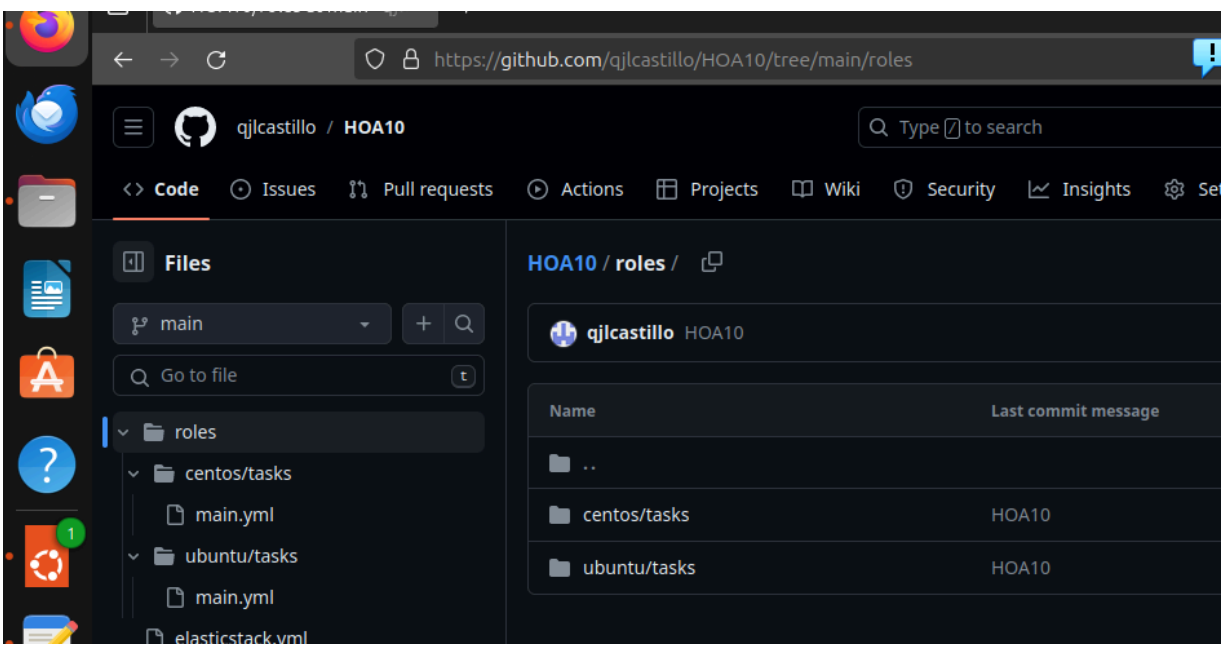
the main playbook which is to install elasticstack for ubuntu and centos is successful.

verify elasticseach installation.



commit and push all to the repository:

```
joshua@ManagedNode:~/HOA10$ git add .
joshua@ManagedNode:~/HOA10$ git status
On branch main

No commits yet

Changes to be committed:
  (use "git rm --cached <file>..." to unstage)
        new file:   elasticstack.yml
        new file:   roles/centos/tasks/main.yml
        new file:   roles/ubuntu/tasks/main.yml

joshua@ManagedNode:~/HOA10$ git commit -m "HOA10"
[main (root-commit) 96ebd5b] HOA10
 3 files changed, 169 insertions(+)
 create mode 100644 elasticstack.yml
 create mode 100644 roles/centos/tasks/main.yml
 create mode 100644 roles/ubuntu/tasks/main.yml
joshua@ManagedNode:~/HOA10$ git push
Enumerating objects: 10, done.
Counting objects: 100% (10/10), done.
Delta compression using up to 2 threads
Compressing objects: 100% (6/6), done.
Writing objects: 100% (10/10), 1.36 KiB | 1.36 MiB/s, done.
Total 10 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), done.
To github.com:qjlcastillo/HOA10.git
 * [new branch]      main -> main
joshua@ManagedNode:~/HOA10$
```



Reflections:

Answer the following:

1. What are the benefits of having a log monitoring tool?
   Log monitoring tools offer a range of benefits. They help detect issues allowing for timely problem resolution. These tools also optimize performance by allocating resources. Enhance security through threat detection. Also, they ensure compliance, with regulatory log management requirements and simplify troubleshooting leading to faster issue resolution. Log monitoring tools store data for analysis and trend identification while automating responses to events. They provide real time alerts for action and facilitate data visualization for log analysis. In summary these tools are crucial in maintaining system health, security, performance and streamlining management tasks while ensuring compliance with standards.

Conclusions:

In this activity, I developed a workflow using Ansible to configure and oversee log monitoring tools such as the Elastic Stack and Logstash. Effective log file analysis heavily relies on log monitoring. I automated the installation process, on Ubuntu and CentOS by executing playbooks while also documenting the deployment in a manner using roles. This activity highlighted the significance of log monitoring and Ansible in installations and management.