Name: Recto, Jon Jeous J.	**Date Performed:** Mar 27, 2024
Course/Section: CPE31S1	**Date Submitted:** Mar 30, 2024
Instructor: Dr. Taylar	**Semester and SY:** 2nd 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)

a. Add the necessary files and its contents

```
jonjeous@localmachine-VirtualBox:~$ cd Recto_HOA10
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$ ls
ansible.cfg  inventory  playbook.yml  README.md  roles
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$ cat ansible.cfg
[defaults]
inventory = inventory
private_key_file = ~/.ssh/ansible
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$ cat inventory
[ubuntu_servers]
192.168.56.129 #Server1
192.168.56.130 #Server2
192.168.56.128 #ManagedNode

[centos_servers]
192.168.56.125 #CentOS


[elasticsearch]
192.168.56.129
192.168.56.130


[kibana]
192.168.56.125


[logstash]
192.168.56.128
```

```
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$ cat playbook.yml
---
- name: Deploy Elastic Stack on Ubuntu and CentOS
  hosts: elasticsearch:kibana:logstash
  roles:
    - base
    - java
    - elasticsearch
    - kibana
    - logstash
```

b. Roles

```
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$ tree roles
roles
├── base
│   └── tasks
│       └── main.yml
├── elasticsearch
│   └── tasks
│       └── main.yml
├── java
│   └── tasks
│       └── main.yml
├── kibana
│   └── tasks
│       └── main.yml
└── logstash
    └── tasks
        └── main.yml
```

c. Tasks for each role.

```
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$ cat roles/base/tasks/main.yml
---
- name: update repository index (CentOS)
  yum:
    update_cache: yes
  changed_when: false
  when: ansible_distribution == "CentOS"
  become: true

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

```
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$ cat roles/java/tasks/main.yml
---
- name: Install OpenJDK 11 on CentOS
  yum:
    name: java-11-openjdk-devel
    state: present
  when: ansible_distribution == "CentOS"
  become: true

- name: Install OpenJDK 11 on Ubuntu
  apt:
    name: openjdk-11-jre-headless
    state: present
  when: ansible_distribution == "Ubuntu"
  become: true
```

```
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$ cat roles/elasticsearch/tasks/main.yml
---
- name: Add Elasticsearch GPG key (CentOS)
  rpm_key:
    key: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    state: present
  when: ansible_distribution == "CentOS"
  become: true

- name: Add Elasticsearch repository (CentOS)
  yum_repository:
    name: elasticsearch
    description: Elasticsearch repository
    baseurl: https://artifacts.elastic.co/packages/7.x/yum
    gpgcheck: yes
    gpgkey: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    enabled: yes
  when: ansible_distribution == "CentOS"
  become: true

- name: Install Elasticsearch (CentOS)
  yum:
    name: elasticsearch
    state: present
  when: ansible_distribution == "CentOS"
  become: true
```

```
- name: Add Elasticsearch APT key (Ubuntu)
  apt_key:
    url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    state: present
  when: ansible_distribution == "Ubuntu"
  become: true

- name: Add Elasticsearch repository (Ubuntu)
  apt_repository:
    repo: deb https://artifacts.elastic.co/packages/7.x/apt stable main
    state: present
    update_cache: yes
  when: ansible_distribution == "Ubuntu"
  become: true

- name: Install Elasticsearch (Ubuntu)
  apt:
    name: elasticsearch
    state: present
  when: ansible_distribution == "Ubuntu"
  become: true
```

```
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$ cat roles/kibana/tasks/main.yml
---
- name: Add Kibana GPG key (CentOS)
  rpm_key:
    key: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    state: present
  when: ansible_distribution == "CentOS"
  become: true

- name: Add Kibana repository (CentOS)
  yum_repository:
    name: kibana
    description: Kibana repository
    baseurl: https://artifacts.elastic.co/packages/7.x/yum
    gpgcheck: yes
    gpgkey: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    enabled: yes
  when: ansible_distribution == "CentOS"
  become: true

- name: Install Kibana (CentOS)
  yum:
    name: kibana
    state: present
  when: ansible_distribution == "CentOS"
  become: true
```

```
- name: Add Kibana APT key (Ubuntu)
  apt_key:
    url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    state: present
  when: ansible_distribution == "Ubuntu"
  become: true

- name: Add Kibana repository (Ubuntu)
  apt_repository:
    repo: deb https://artifacts.elastic.co/packages/7.x/apt stable main
    state: present
    update_cache: yes
  when: ansible_distribution == "Ubuntu"
  become: true

- name: Install Kibana (Ubuntu)
  apt:
    name: kibana
    state: present
  when: ansible_distribution == "Ubuntu"
  become: true
```

```
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$ cat roles/logstash/tasks/main.yml
---
- name: Add Logstash GPG key (CentOS)
  rpm_key:
    key: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    state: present
  when: ansible_distribution == "CentOS"
  become: true

- name: Add Logstash repository (CentOS)
  yum_repository:
    name: logstash
    description: Logstash repository
    baseurl: https://artifacts.elastic.co/packages/7.x/yum
    gpgcheck: yes
    gpgkey: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    enabled: yes
  when: ansible_distribution == "CentOS"
  become: true

- name: Install Logstash (CentOS)
  yum:
    name: logstash
    state: present
  when: ansible_distribution == "CentOS"
  become: true
```

```
- name: Add Logstash APT key (Ubuntu)
  apt_key:
    url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    state: present
  when: ansible_distribution == "Ubuntu"
  become: true

- name: Add Logstash repository (Ubuntu)
  apt_repository:
    repo: deb https://artifacts.elastic.co/packages/7.x/apt stable main
    state: present
    update_cache: yes
  when: ansible_distribution == "Ubuntu"
  become: true

- name: Install Logstash (Ubuntu)
  apt:
    name: logstash
    state: present
  when: ansible_distribution == "Ubuntu"
  become: true
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$
```

d. Run the playbook.

```
  become: true
jonjeous@localmachine-VirtualBox:~/Recto_HOA10$ ansible-playbook --ask-become-pass play
book.yml
BECOME password:

PLAY [Deploy Elastic Stack on Ubuntu and CentOS] ************************************

TASK [Gathering Facts] *****************************************************************
ok: [192.168.56.129]
ok: [192.168.56.128]
ok: [192.168.56.130]
ok: [192.168.56.125]

TASK [base : update repository index (CentOS)] *****************************************
skipping: [192.168.56.129]
skipping: [192.168.56.130]
skipping: [192.168.56.128]
ok: [192.168.56.125]

TASK [base : install updates (Ubuntu)] *************************************************
skipping: [192.168.56.125]
ok: [192.168.56.129]
ok: [192.168.56.130]
ok: [192.168.56.128]
```

```
TASK [java : Install OpenJDK 11 on CentOS] *********************************************
skipping: [192.168.56.129]
skipping: [192.168.56.130]
skipping: [192.168.56.128]
ok: [192.168.56.125]

TASK [java : Install OpenJDK 11 on Ubuntu] *********************************************
skipping: [192.168.56.125]
ok: [192.168.56.130]
ok: [192.168.56.129]
ok: [192.168.56.128]

TASK [elasticsearch : Add Elasticsearch GPG key (CentOS)] ******************************
skipping: [192.168.56.129]
skipping: [192.168.56.130]
skipping: [192.168.56.128]
ok: [192.168.56.125]

TASK [elasticsearch : Add Elasticsearch repository (CentOS)] ***************************
skipping: [192.168.56.129]
skipping: [192.168.56.130]
skipping: [192.168.56.128]
ok: [192.168.56.125]

TASK [elasticsearch : Install Elasticsearch (CentOS)] **********************************
skipping: [192.168.56.129]
skipping: [192.168.56.130]
skipping: [192.168.56.128]
ok: [192.168.56.125]
```

```
TASK [elasticsearch : Add Elasticsearch APT key (Ubuntu)] ****************************
skipping: [192.168.56.125]
ok: [192.168.56.130]
ok: [192.168.56.129]
ok: [192.168.56.128]

TASK [elasticsearch : Add Elasticsearch repository (Ubuntu)] *************************
skipping: [192.168.56.125]
ok: [192.168.56.129]
ok: [192.168.56.130]
ok: [192.168.56.128]

TASK [elasticsearch : Install Elasticsearch (Ubuntu)] ********************************
skipping: [192.168.56.125]
ok: [192.168.56.129]
ok: [192.168.56.130]
ok: [192.168.56.128]

TASK [kibana : Add Kibana GPG key (CentOS)] ******************************************
skipping: [192.168.56.129]
skipping: [192.168.56.130]
skipping: [192.168.56.128]
ok: [192.168.56.125]

TASK [kibana : Add Kibana repository (CentOS)] ***************************************
skipping: [192.168.56.129]
skipping: [192.168.56.130]
skipping: [192.168.56.128]
ok: [192.168.56.125]
```

```
TASK [kibana : Install Kibana (CentOS)] **********************************************
skipping: [192.168.56.129]
skipping: [192.168.56.130]
skipping: [192.168.56.128]
ok: [192.168.56.125]

TASK [kibana : Add Kibana APT key (Ubuntu)] ******************************************
skipping: [192.168.56.125]
ok: [192.168.56.129]
ok: [192.168.56.130]
ok: [192.168.56.128]

TASK [kibana : Add Kibana repository (Ubuntu)] ***************************************
skipping: [192.168.56.125]
ok: [192.168.56.129]
ok: [192.168.56.130]
ok: [192.168.56.128]

TASK [kibana : Install Kibana (Ubuntu)] **********************************************
skipping: [192.168.56.125]
ok: [192.168.56.129]
ok: [192.168.56.128]
ok: [192.168.56.130]

TASK [logstash : Add Logstash GPG key (CentOS)] **************************************
skipping: [192.168.56.129]
skipping: [192.168.56.130]
skipping: [192.168.56.128]
ok: [192.168.56.125]
```

```
TASK [logstash : Add Logstash repository (CentOS)] ***********************************
skipping: [192.168.56.129]
skipping: [192.168.56.130]
skipping: [192.168.56.128]
ok: [192.168.56.125]

TASK [logstash : Install Logstash (CentOS)] ******************************************
skipping: [192.168.56.129]
skipping: [192.168.56.130]
skipping: [192.168.56.128]
ok: [192.168.56.125]

TASK [logstash : Add Logstash APT key (Ubuntu)] **************************************
skipping: [192.168.56.125]
ok: [192.168.56.130]
ok: [192.168.56.129]
ok: [192.168.56.128]

TASK [logstash : Add Logstash repository (Ubuntu)] ***********************************
skipping: [192.168.56.125]
ok: [192.168.56.129]
ok: [192.168.56.130]
ok: [192.168.56.128]

TASK [logstash : Install Logstash (Ubuntu)] ******************************************
skipping: [192.168.56.125]
ok: [192.168.56.130]
ok: [192.168.56.129]
ok: [192.168.56.128]
```

```
PLAY RECAP *********************************************************************
192.168.56.125             : ok=12   changed=0    unreachable=0    failed=0    skipped=
11   rescued=0    ignored=0
192.168.56.128             : ok=12   changed=0    unreachable=0    failed=0    skipped=
11   rescued=0    ignored=0
192.168.56.129             : ok=12   changed=0    unreachable=0    failed=0    skipped=
11   rescued=0    ignored=0
192.168.56.130             : ok=12   changed=0    unreachable=0    failed=0    skipped=
11   rescued=0    ignored=0

jonjeous@localmachine-VirtualBox:~/Recto_HOA10$
```

e. Edit the elasticsearch.yml, kibana.yml, logstash.conf files for both ubuntu and centos

```
  GNU nano 6.2          /etc/elasticsearch/elasticsearch.yml *
#
# ---------------------------------- Security ----------------------------------
#
#                                    *** WARNING ***
#
# Elasticsearch security features are not enabled by default.
# These features are free, but require configuration changes to enable them.
# This means that users don't have to provide credentials and can get full acce>
# to the cluster. Network connections are also not encrypted.
#
# To protect your data, we strongly encourage you to enable the Elasticsearch s>
# Refer to the following documentation for instructions.
#
# https://www.elastic.co/guide/en/elasticsearch/reference/7.16/configuring-stac>

cluster.name: my_cluster
node.name: localhost.localdomain
network.host: 0.0.0.0
http.port: 9200
cluster.initial_master_nodes: ["localhost.localdomain"]
```

sudo systemctl restart elasticsearch

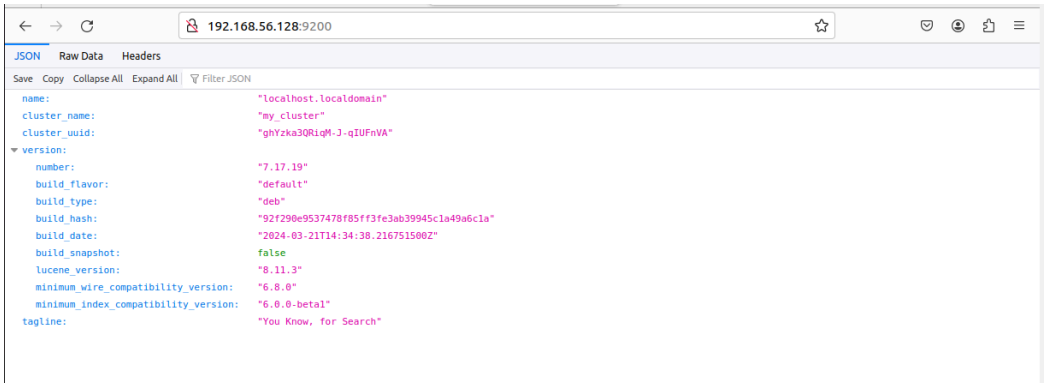
```
  GNU nano 6.2                  /etc/kibana/kibana.yml *
#logging.silent: false

# Set the value of this setting to true to suppress all logging output other th>
#logging.quiet: false

# Set the value of this setting to true to log all events, including system usa>
# and all requests.
#logging.verbose: false

# Set the interval in milliseconds to sample system and process performance
# metrics. Minimum is 100ms. Defaults to 5000.
#ops.interval: 5000

# Specifies locale to be used for all localizable strings, dates and number for>
# Supported languages are the following: English - en , by default , Chinese - >
#i18n.locale: "en"

server.host: 0.0.0.0
server.port: 5601
elasticsearch.hosts: ["http://localhost:9200"]
```

sudo systemctl restart kibana

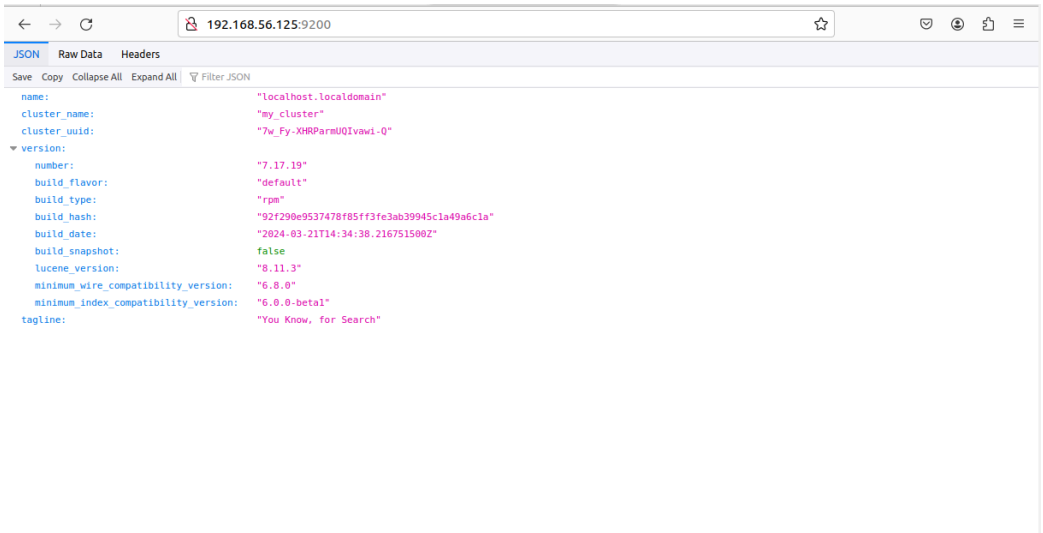
```
  GNU nano 6.2                /etc/logstash/logstash.conf
input {
  file {
    path => "/var/log/*.log"
    start_position => "beginning"
    sincedb_path => "/dev/null"
  }
}

output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "logs-%{+YYYY.MM.dd}"
  }
}
```

sudo systemctl restart logstash

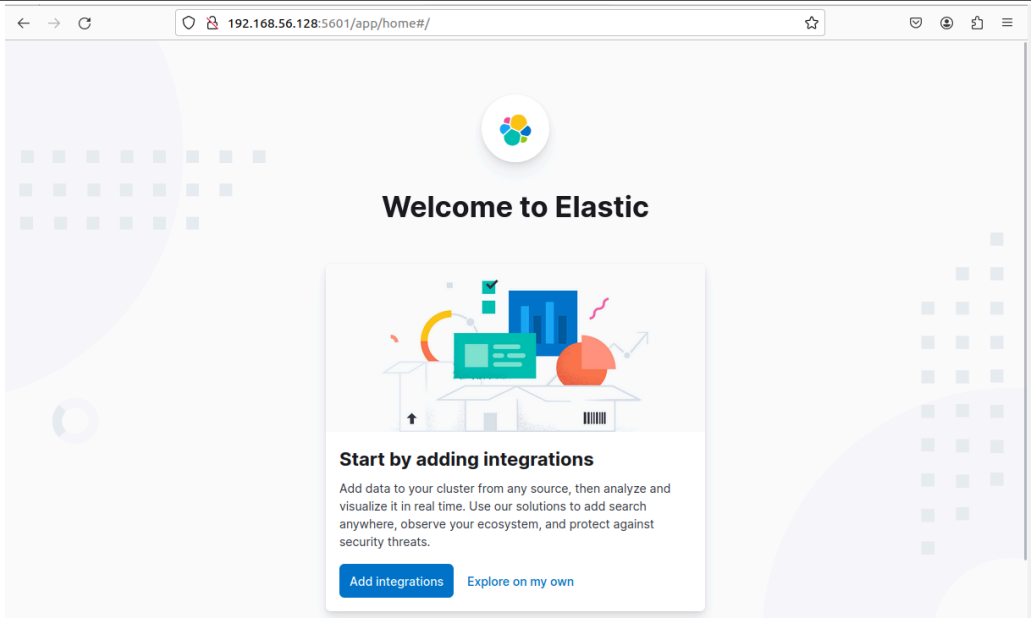
f. Check if it is installed properly



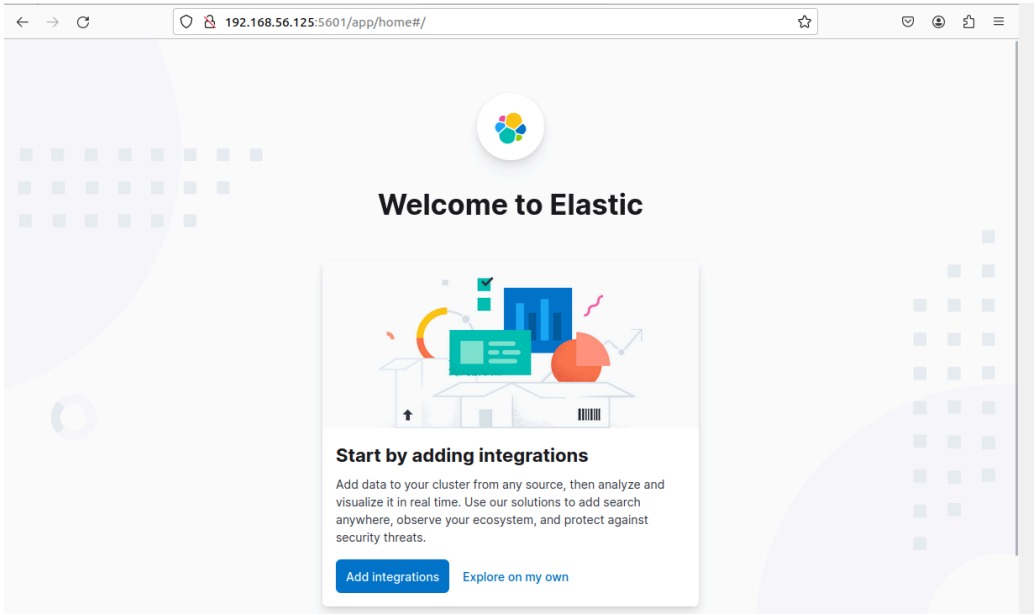
Ubuntu elasticsearch



CentOS elasticsearch



Ubuntu kibana



CentOS kibana

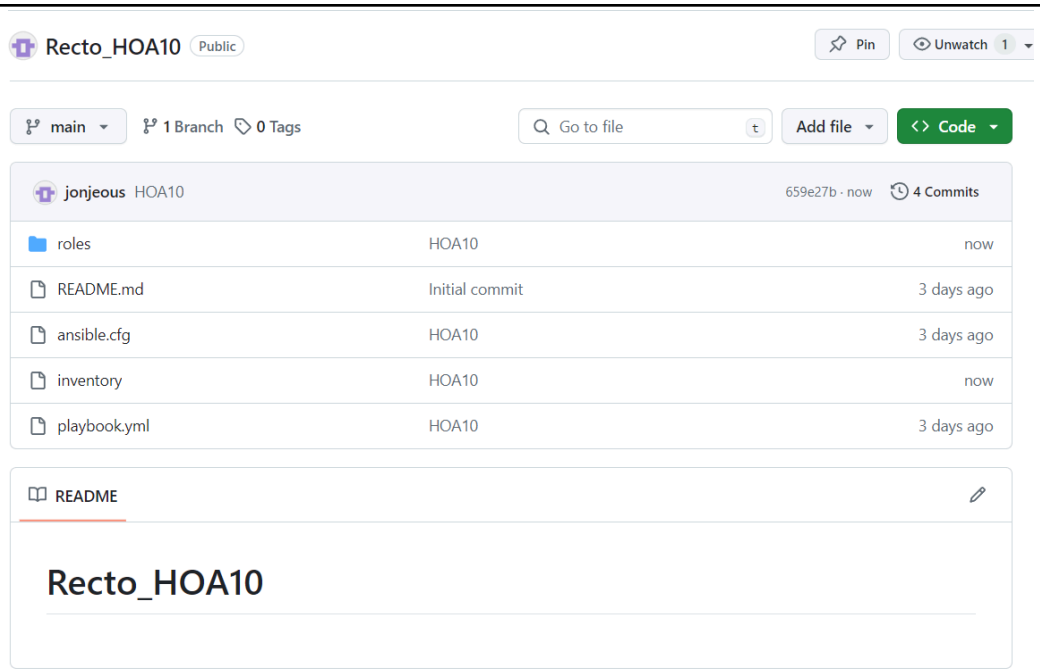
```
root@localmachine-VirtualBox:~# sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; disabled; vendor pre>
     Active: active (running) since Sat 2024-03-30 17:28:07 PST; 7s ago
   Main PID: 14424 (java)
      Tasks: 14 (limit: 4598)
     Memory: 206.4M
        CPU: 5.324s
     CGroup: /system.slice/logstash.service
             └─14424 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCon>

Mar 30 17:28:07 localmachine-VirtualBox systemd[1]: Started logstash.
Mar 30 17:28:07 localmachine-VirtualBox logstash[14424]: Using bundled JDK: /us>
Mar 30 17:28:08 localmachine-VirtualBox logstash[14424]: OpenJDK 64-Bit Server >
lines 1-13/13 (END)
```

Ubuntu logstash

```
[jonjeous@localhost ~]$ sudo systemctl start logstash
[jonjeous@localhost ~]$ sudo systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; disabled; vendor preset
: disabled)
   Active: active (running) since Sat 2024-03-30 18:00:46 PST; 45s ago
 Main PID: 12878 (java)
    Tasks: 14
   CGroup: /system.slice/logstash.service
           └─12878 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCon...

Mar 30 18:00:46 localhost.localdomain systemd[1]: Started logstash.
Mar 30 18:00:47 localhost.localdomain logstash[12878]: Using bundled JDK: /us...
Mar 30 18:00:48 localhost.localdomain logstash[12878]: OpenJDK 64-Bit Server ...
Hint: Some lines were ellipsized, use -l to show in full.
[jonjeous@localhost ~]$
```

CentOS logstash

g. Commit changes to github



https://github.com/jonjeous/Recto_HOA10.git

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool?
   - Log monitoring tools offer a way to continuously analyze log data in real-time, helping detect anomalies and errors within a system. They aid in troubleshooting and debugging by providing insights into system behavior and performance issues. Additionally, log monitoring tools contribute to security efforts by detecting unauthorized access attempts and assisting in compliance with regulatory standards.

Conclusions:

In conclusion, the completion of this activity involved devising a workflow through Ansible to establish and oversee enterprise log monitoring tools, specifically focusing on the Elastic Stack and Graylog. These tools serve as critical components for maintaining the functionality of our IT infrastructure, identifying anomalies, and fortifying security measures. By harnessing Ansible's capabilities, I've automated the deployment process, ensuring uniformity and effectiveness in managing our log monitoring solutions. This approach empowers us to uphold the reliability and performance of our IT environment with greater ease and efficiency.