Name: Tendencia, Jasmin Raiza S.	**Date Performed:** 10/23/2023
Course/Section: CPE232-CPE31S4	**Date Submitted:** 10/31/2023
Instructor: Dr. Jonathan Taylar	**Semester and SY:** 1st/2023-2024

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

1. Objectives

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

2. Discussion

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

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

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

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

Elastic Stack

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

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

GrayLog

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

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

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

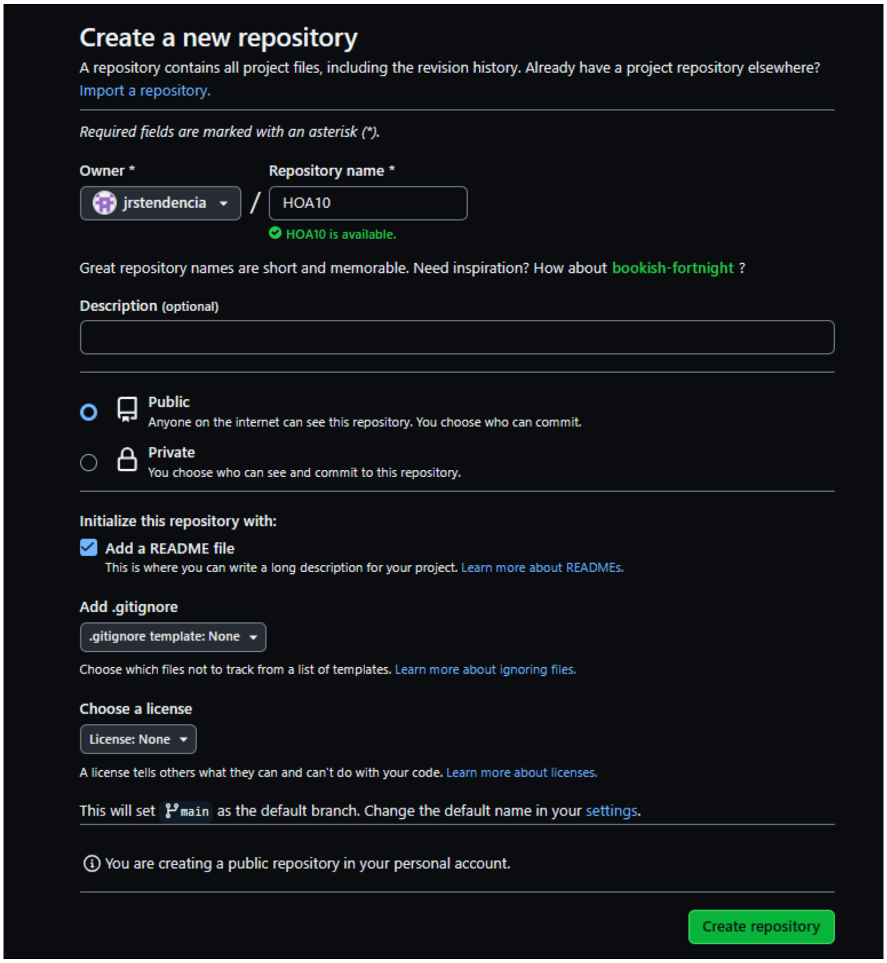
Source: https://www.graylog.org/products/open-source

3. Tasks

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

4. **Output** (screenshots and explanations)

1. Create a new repository in Github.



Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? Import a repository.

Required fields are marked with an asterisk (*).

Owner * jrstendencia / Repository name * HOA10

✓ HOA10 is available.

Great repository names are short and memorable. Need inspiration? How about bookish-fortnight ?

Description (optional)

● Public
Anyone on the internet can see this repository. You choose who can commit.

○ Private
You choose who can see and commit to this repository.

Initialize this repository with:

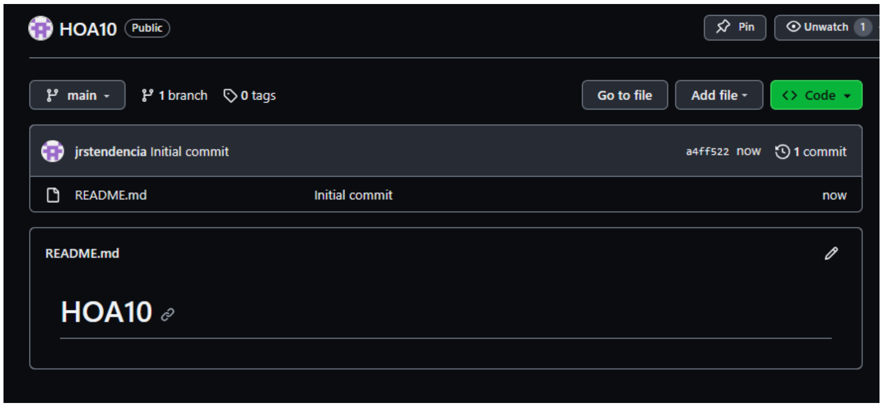
☑ Add a README file
This is where you can write a long description for your project. Learn more about READMEs.

Add .gitignore
.gitignore template: None
Choose which files not to track from a list of templates. Learn more about ignoring files.

Choose a license
License: None
A license tells others what they can and can't do with your code. Learn more about licenses.

This will set `main` as the default branch. Change the default name in your settings.

ⓘ You are creating a public repository in your personal account.



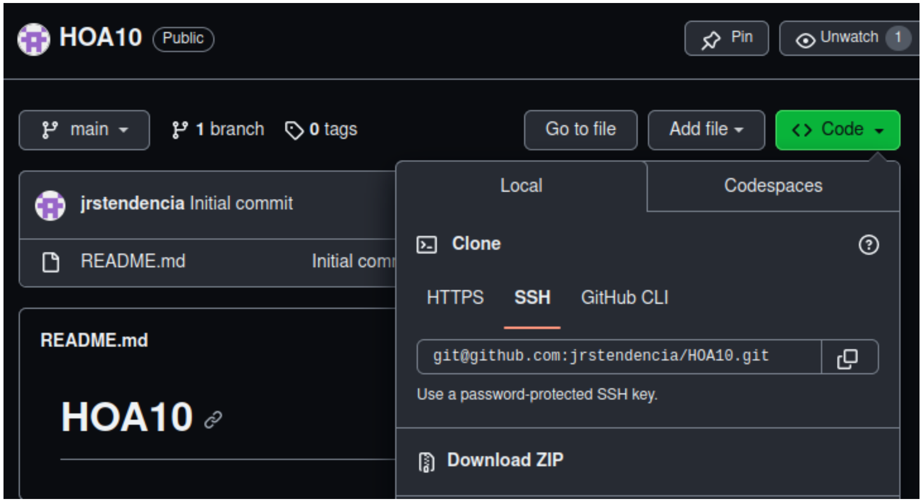
HOA10 Public

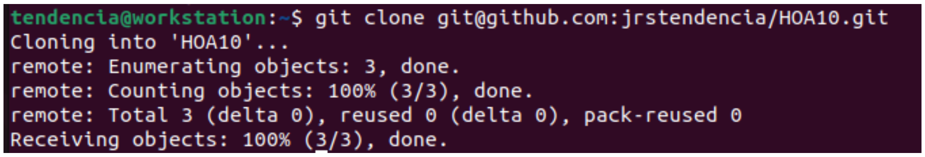
jrstendencia Initial commit a4ff522 now 1 commit

README.md Initial commit now

README.md

HOA10

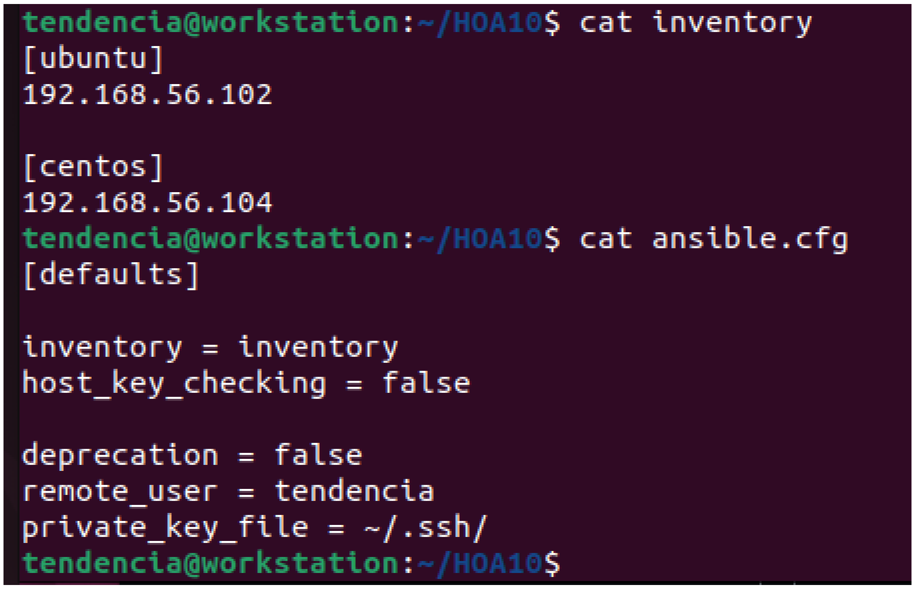




```
tendencia@workstation:~$ git clone git@github.com:jrstendencia/HOA10.git
Cloning into 'HOA10'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
```

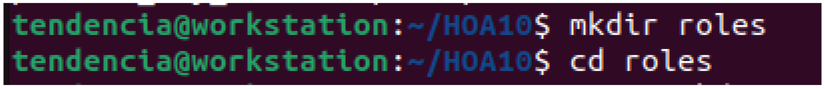
Explanation: A new repository named HOA10 is created in Github for this activity.

2. Setup the ansible environment by creating an inventory file to specify the target hosts (Ubuntu and CentOS) to be configured. Also, create the ansible.cfg.



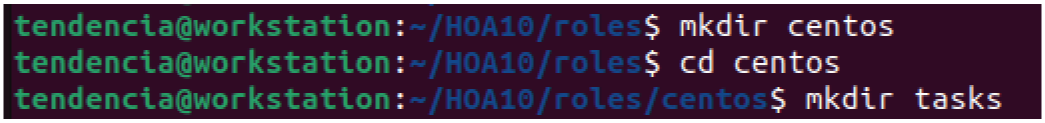
```
tendencia@workstation:~/HOA10$ cat inventory
[ubuntu]
192.168.56.102

[centos]
192.168.56.104
tendencia@workstation:~/HOA10$ cat ansible.cfg
[defaults]

inventory = inventory
host_key_checking = false

deprecation = false
remote_user = tendencia
private_key_file = ~/.ssh/
tendencia@workstation:~/HOA10$
```

3. Create a role for elastic stack installation for Ubuntu and CentOS by generating the role structure. Then, create a directory named *tasks* that contains a *main.yml* file.

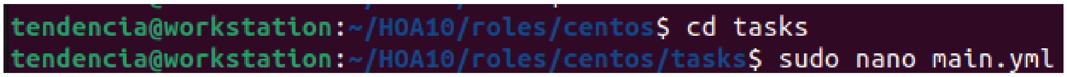


```
tendencia@workstation:~/HOA10$ mkdir roles
tendencia@workstation:~/HOA10$ cd roles
```

CentOS:

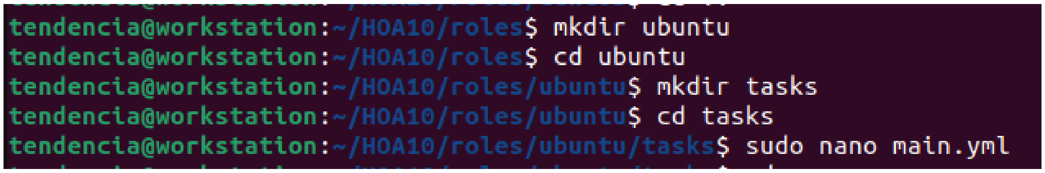


```
tendencia@workstation:~/HOA10/roles$ mkdir centos
tendencia@workstation:~/HOA10/roles$ cd centos
tendencia@workstation:~/HOA10/roles/centos$ mkdir tasks
```



```
tendencia@workstation:~/HOA10/roles/centos$ cd tasks
tendencia@workstation:~/HOA10/roles/centos/tasks$ sudo nano main.yml
```

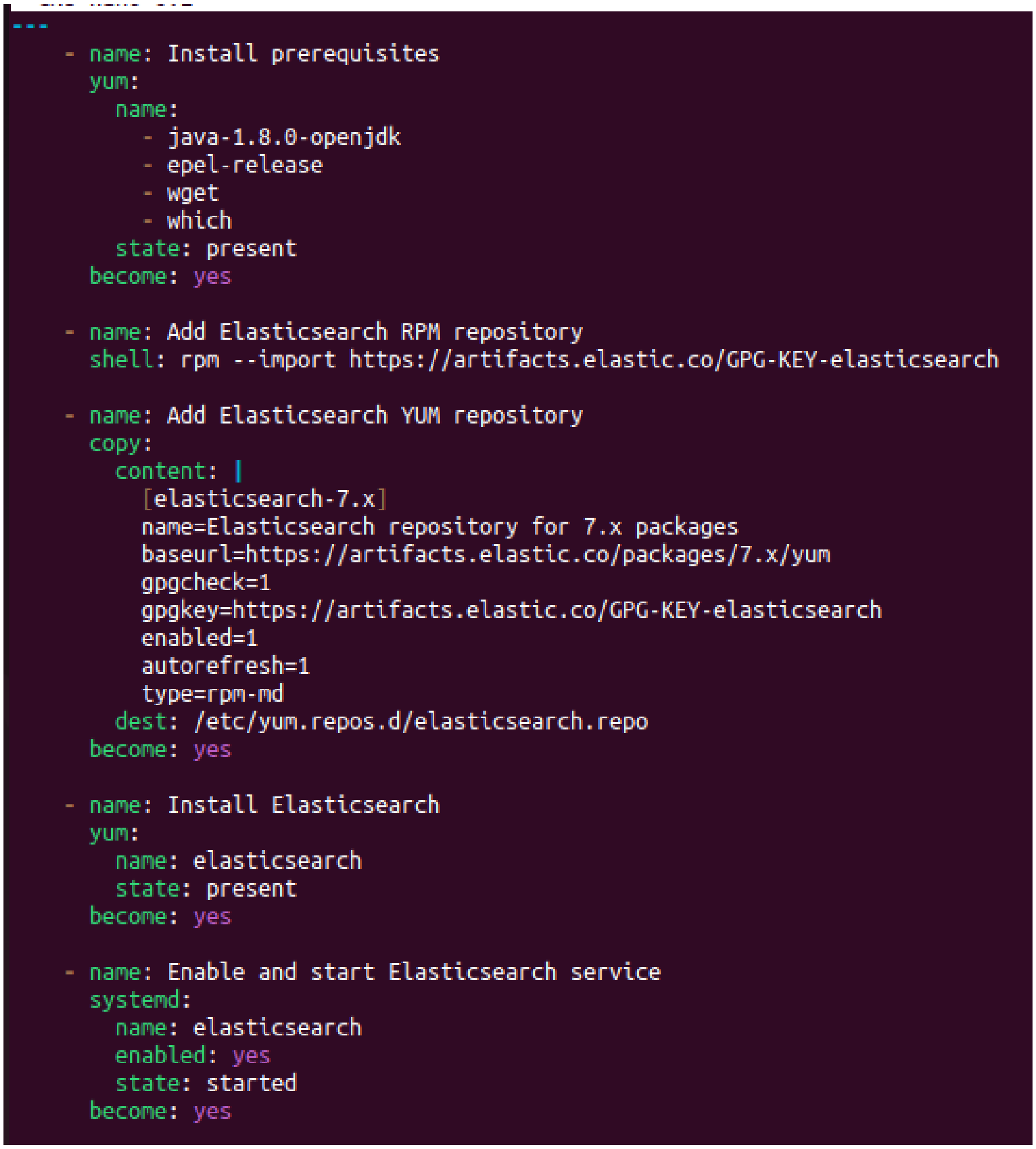
Ubuntu:



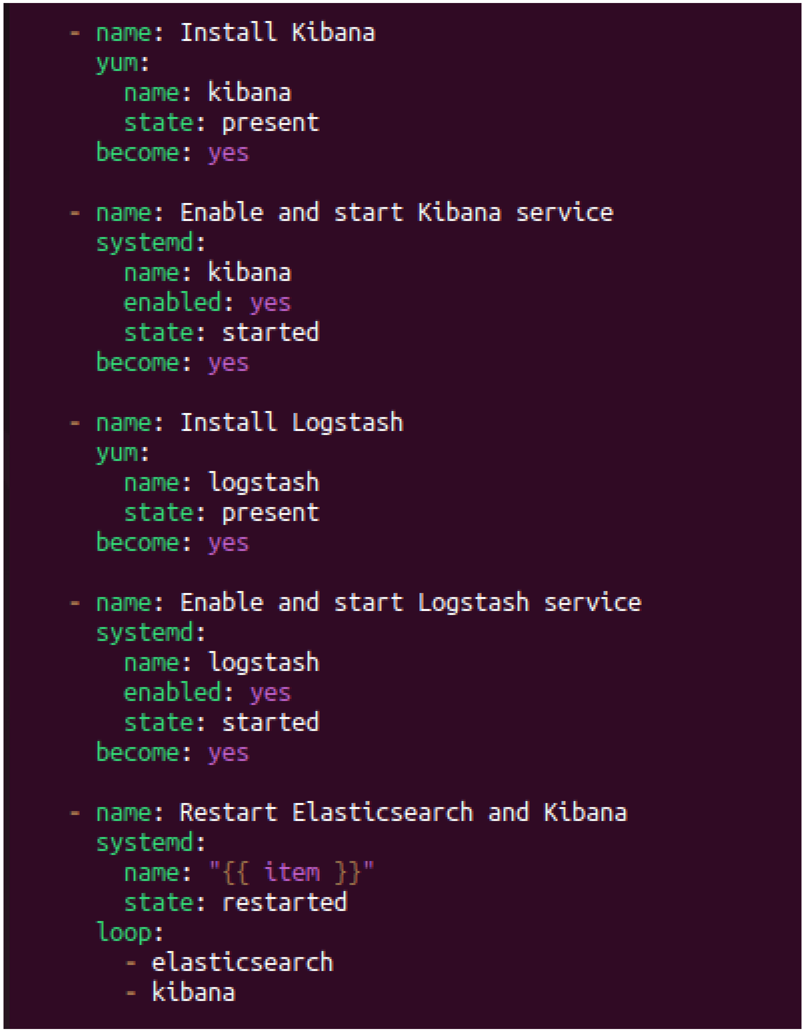
```
tendencia@workstation:~/HOA10/roles$ mkdir ubuntu
tendencia@workstation:~/HOA10/roles$ cd ubuntu
tendencia@workstation:~/HOA10/roles/ubuntu$ mkdir tasks
tendencia@workstation:~/HOA10/roles/ubuntu$ cd tasks
tendencia@workstation:~/HOA10/roles/ubuntu/tasks$ sudo nano main.yml
```

4. Inside the main.yml file, the script should define the tasks for Elastic Stack installation for both Ubuntu and CentOS.

CentOS:

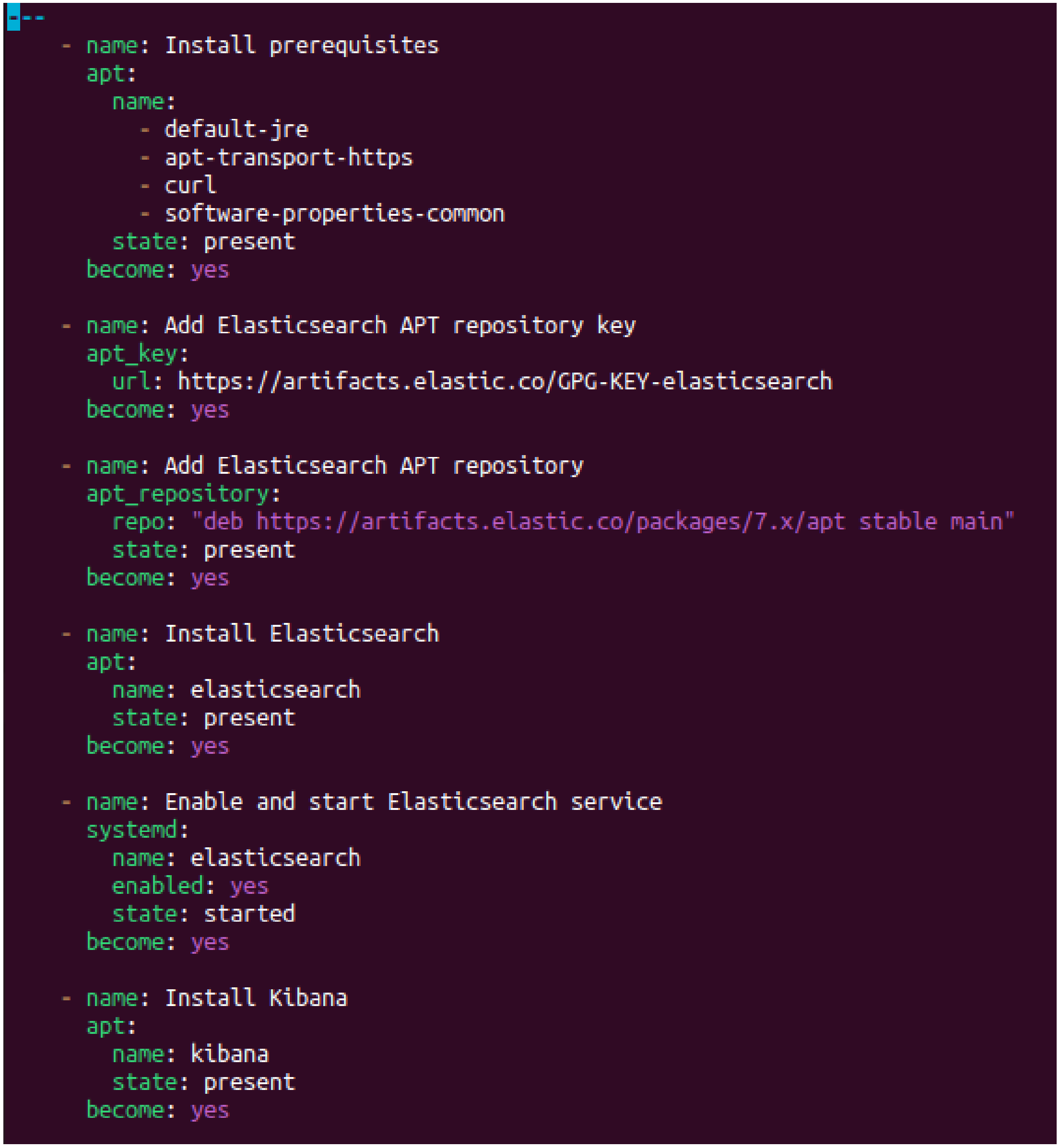


```
---
    - name: Install prerequisites
      yum:
        name:
          - java-1.8.0-openjdk
          - epel-release
          - wget
          - which
        state: present
      become: yes

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

    - name: Add 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
      yum:
        name: elasticsearch
        state: present
      become: yes

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

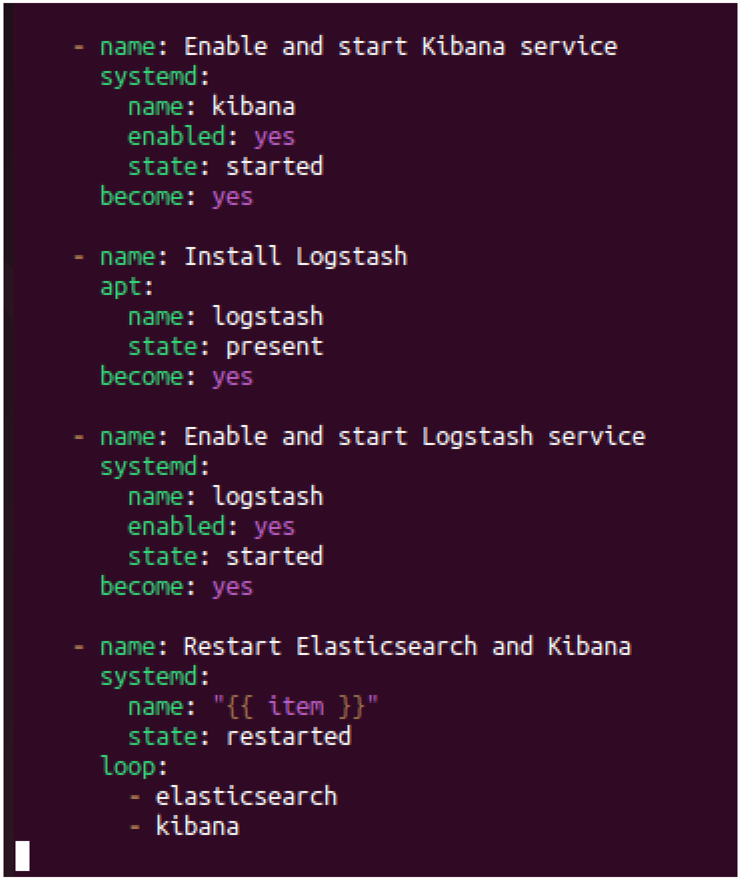


```
  - name: Install Kibana
    yum:
      name: kibana
      state: present
    become: yes

  - name: Enable and start Kibana service
    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

  - name: Install Logstash
    yum:
      name: logstash
      state: present
    become: yes

  - name: Enable and start Logstash service
    systemd:
      name: logstash
      enabled: yes
      state: started
    become: yes

  - name: Restart Elasticsearch and Kibana
    systemd:
      name: "{{ item }}"
      state: restarted
    loop:
      - elasticsearch
      - kibana
```

Ubuntu:



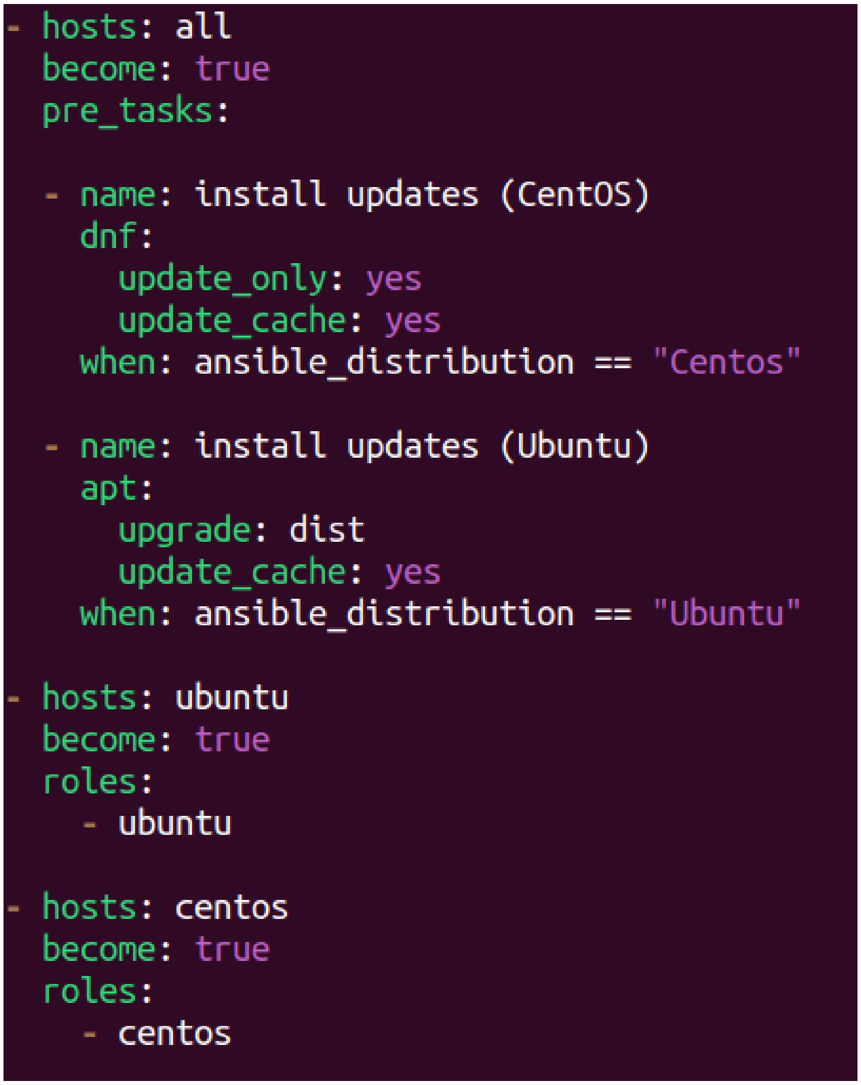
```yaml
---
    - name: Install prerequisites
      apt:
        name:
          - default-jre
          - apt-transport-https
          - curl
          - software-properties-common
        state: present
      become: yes

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

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

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

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

    - name: Install Kibana
      apt:
        name: kibana
        state: present
      become: yes
```



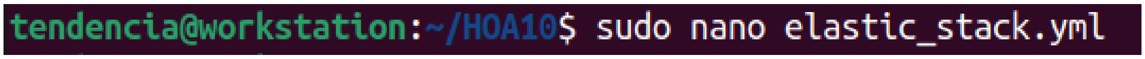
```
  - name: Enable and start Kibana service
    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

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

5. Create a playbook in the current working directory. This playbook will use the Elastic Stack role.

elastic_slack.yml:

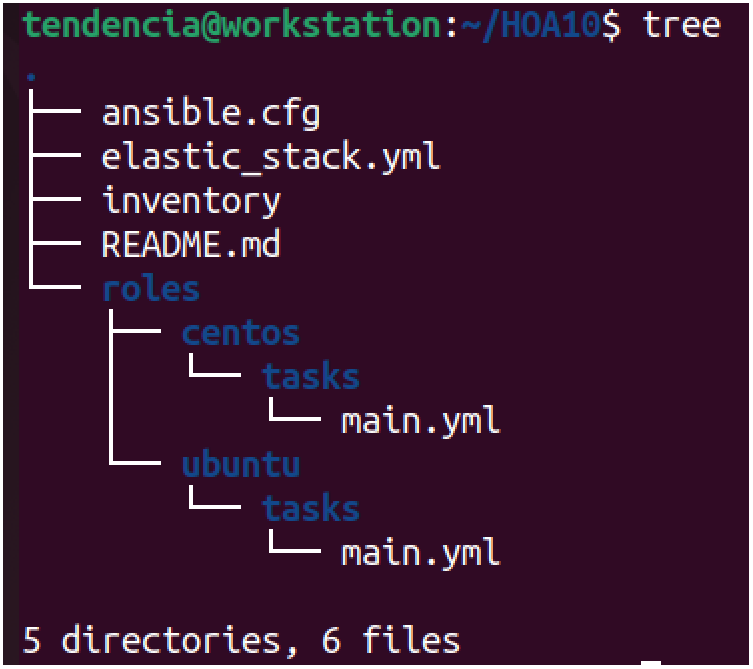


```
- hosts: all
  become: true
  pre_tasks:

  - 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: ubuntu
  become: true
  roles:
    - ubuntu

- hosts: centos
  become: true
  roles:
    - centos
```



```
tendencia@workstation:~/HOA10$ sudo nano elastic_stack.yml
```

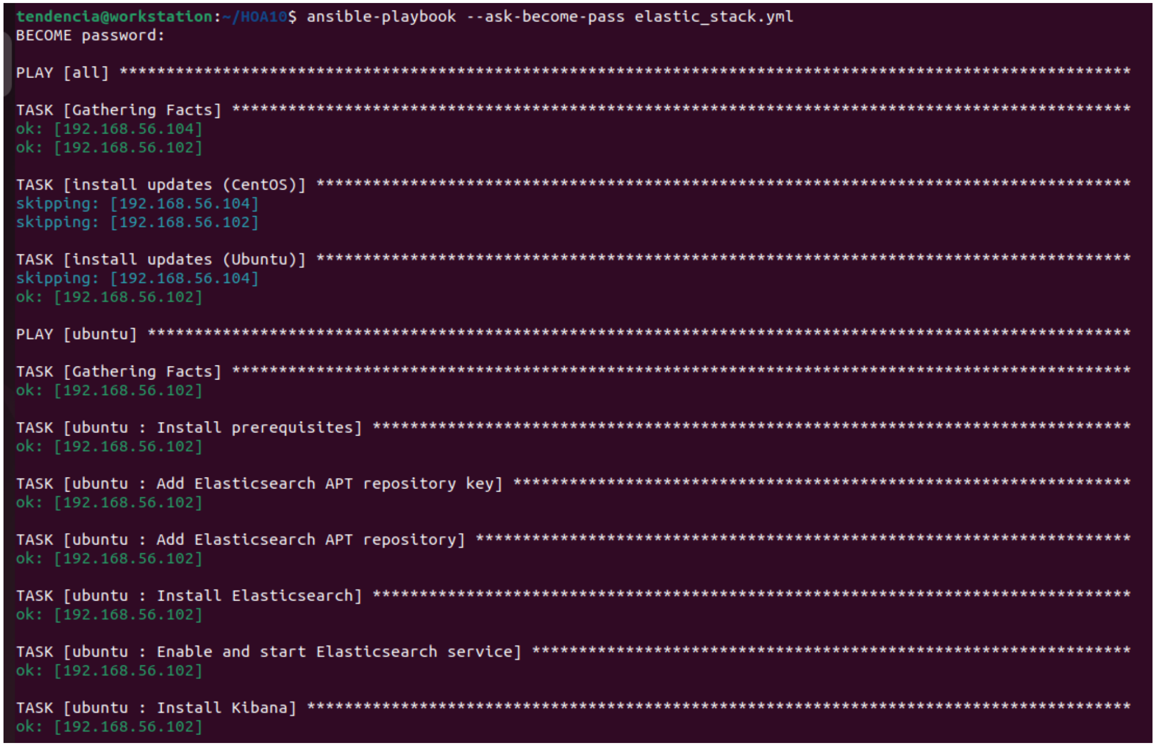
Tree:



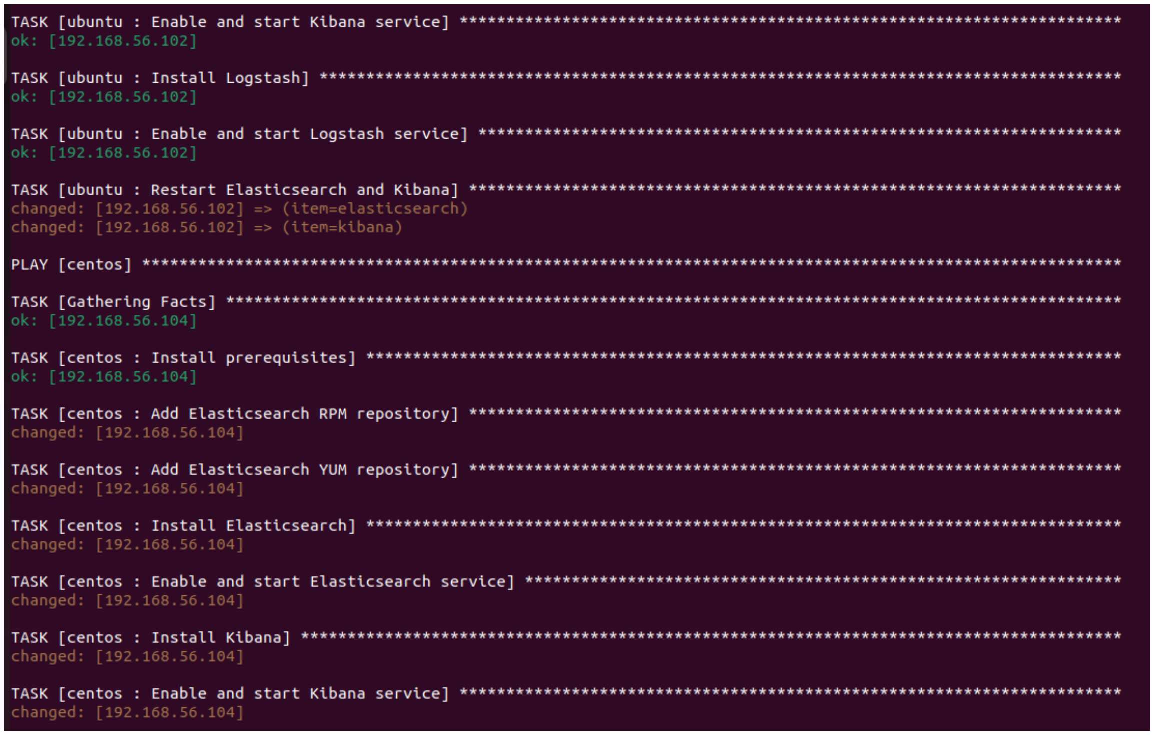
```
tendencia@workstation:~/HOA10$ tree
.
├── ansible.cfg
├── elastic_stack.yml
├── inventory
├── README.md
└── roles
    ├── centos
    │   └── tasks
    │       └── main.yml
    └── ubuntu
        └── tasks
            └── main.yml

5 directories, 6 files
```

6. Run the playbook to install Elastic Stack (elastic search, logstash, kibana) on the target hosts using the command *ansible-playbook –ask-become-pass elastic_stack.yml*.

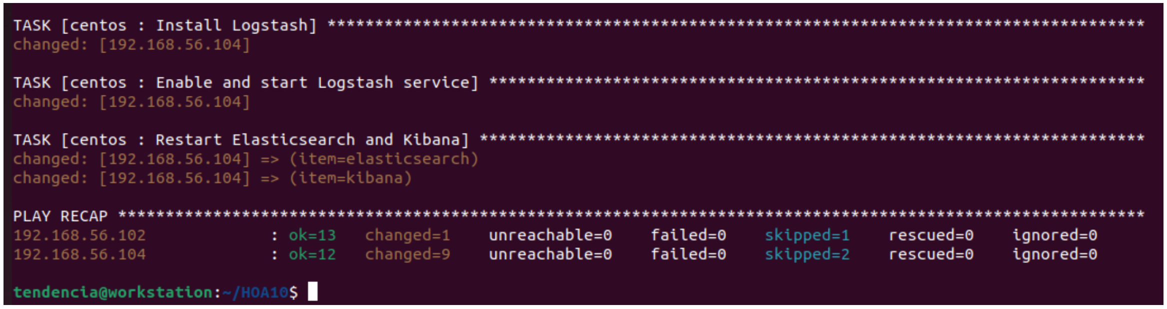
Output:



```
tendencia@workstation:~/HOA10$ ansible-playbook --ask-become-pass elastic_stack.yml
BECOME password:

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

TASK [Gathering Facts] ************************************************************************************************
ok: [192.168.56.104]
ok: [192.168.56.102]

TASK [install updates (CentOS)] ***************************************************************************************
skipping: [192.168.56.104]
skipping: [192.168.56.102]

TASK [install updates (Ubuntu)] ***************************************************************************************
skipping: [192.168.56.104]
ok: [192.168.56.102]

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

TASK [Gathering Facts] ************************************************************************************************
ok: [192.168.56.102]

TASK [ubuntu : Install prerequisites] *********************************************************************************
ok: [192.168.56.102]

TASK [ubuntu : Add Elasticsearch APT repository key] ******************************************************************
ok: [192.168.56.102]

TASK [ubuntu : Add Elasticsearch APT repository] **********************************************************************
ok: [192.168.56.102]

TASK [ubuntu : Install Elasticsearch] *********************************************************************************
ok: [192.168.56.102]

TASK [ubuntu : Enable and start Elasticsearch service] ****************************************************************
ok: [192.168.56.102]

TASK [ubuntu : Install Kibana] ****************************************************************************************
ok: [192.168.56.102]
```



```
TASK [ubuntu : Enable and start Kibana service] ***********************************************************************
ok: [192.168.56.102]

TASK [ubuntu : Install Logstash] **************************************************************************************
ok: [192.168.56.102]

TASK [ubuntu : Enable and start Logstash service] *********************************************************************
ok: [192.168.56.102]

TASK [ubuntu : Restart Elasticsearch and Kibana] **********************************************************************
changed: [192.168.56.102] => (item=elasticsearch)
changed: [192.168.56.102] => (item=kibana)

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

TASK [Gathering Facts] ************************************************************************************************
ok: [192.168.56.104]

TASK [centos : Install prerequisites] *********************************************************************************
ok: [192.168.56.104]

TASK [centos : Add Elasticsearch RPM repository] **********************************************************************
changed: [192.168.56.104]

TASK [centos : Add Elasticsearch YUM repository] **********************************************************************
changed: [192.168.56.104]

TASK [centos : Install Elasticsearch] *********************************************************************************
changed: [192.168.56.104]

TASK [centos : Enable and start Elasticsearch service] ****************************************************************
changed: [192.168.56.104]

TASK [centos : Install Kibana] ****************************************************************************************
changed: [192.168.56.104]

TASK [centos : Enable and start Kibana service] ***********************************************************************
changed: [192.168.56.104]
```

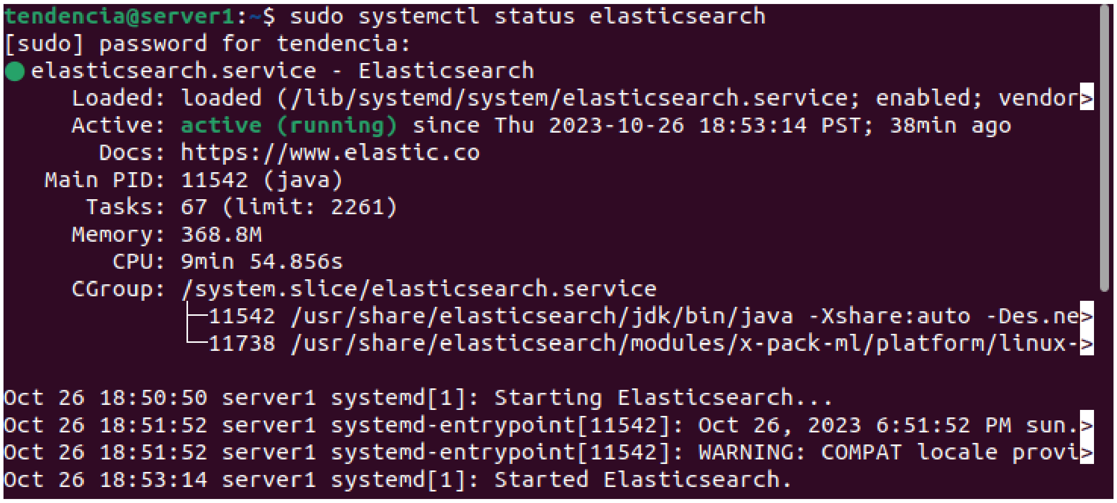


```
TASK [centos : Install Logstash] ***************************************************************************
changed: [192.168.56.104]

TASK [centos : Enable and start Logstash service] **********************************************************
changed: [192.168.56.104]

TASK [centos : Restart Elasticsearch and Kibana] ***********************************************************
changed: [192.168.56.104] => (item=elasticsearch)
changed: [192.168.56.104] => (item=kibana)

PLAY RECAP *************************************************************************************************
192.168.56.102             : ok=13   changed=1    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0
192.168.56.104             : ok=12   changed=9    unreachable=0    failed=0    skipped=2    rescued=0    ignored=0

tendencia@workstation:~/HOA10$ 
```

7. Verify elastic stack installation in both Ubuntu and CentOS by using the command *systemctl status* <>.

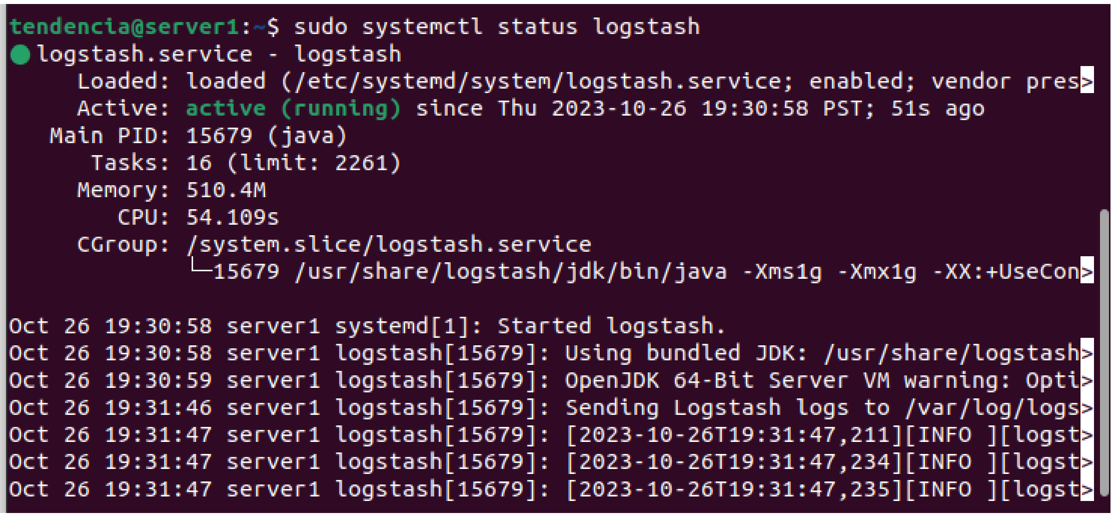
Ubuntu:

a. Elastic



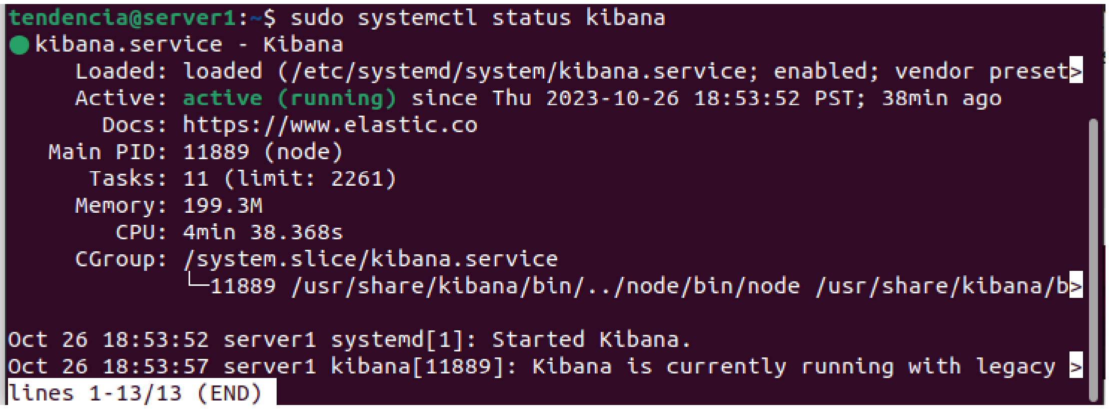
```
tendencia@server1:~$ sudo systemctl status elasticsearch
[sudo] password for tendencia:
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor>
     Active: active (running) since Thu 2023-10-26 18:53:14 PST; 38min ago
       Docs: https://www.elastic.co
   Main PID: 11542 (java)
      Tasks: 67 (limit: 2261)
     Memory: 368.8M
        CPU: 9min 54.856s
     CGroup: /system.slice/elasticsearch.service
             ├─11542 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.ne>
             └─11738 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux->

Oct 26 18:50:50 server1 systemd[1]: Starting Elasticsearch...
Oct 26 18:51:52 server1 systemd-entrypoint[11542]: Oct 26, 2023 6:51:52 PM sun.>
Oct 26 18:51:52 server1 systemd-entrypoint[11542]: WARNING: COMPAT locale provi>
Oct 26 18:53:14 server1 systemd[1]: Started Elasticsearch.
```

b. Logstash



```
tendencia@server1:~$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor pres>
     Active: active (running) since Thu 2023-10-26 19:30:58 PST; 51s ago
   Main PID: 15679 (java)
      Tasks: 16 (limit: 2261)
     Memory: 510.4M
        CPU: 54.109s
     CGroup: /system.slice/logstash.service
             └─15679 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCon>

Oct 26 19:30:58 server1 systemd[1]: Started logstash.
Oct 26 19:30:58 server1 logstash[15679]: Using bundled JDK: /usr/share/logstash>
Oct 26 19:30:59 server1 logstash[15679]: OpenJDK 64-Bit Server VM warning: Opti>
Oct 26 19:31:46 server1 logstash[15679]: Sending Logstash logs to /var/log/logs>
Oct 26 19:31:47 server1 logstash[15679]: [2023-10-26T19:31:47,211][INFO ][logst>
Oct 26 19:31:47 server1 logstash[15679]: [2023-10-26T19:31:47,234][INFO ][logst>
Oct 26 19:31:47 server1 logstash[15679]: [2023-10-26T19:31:47,235][INFO ][logst>
```

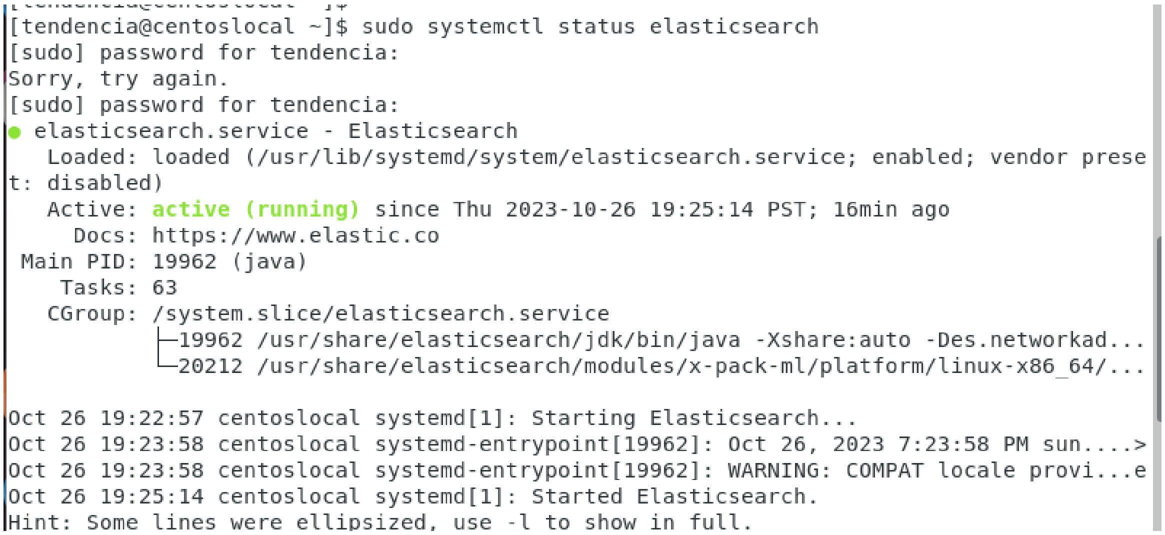
c. Kibana



```
tendencia@server1:~$ sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset>
     Active: active (running) since Thu 2023-10-26 18:53:52 PST; 38min ago
       Docs: https://www.elastic.co
   Main PID: 11889 (node)
      Tasks: 11 (limit: 2261)
     Memory: 199.3M
        CPU: 4min 38.368s
     CGroup: /system.slice/kibana.service
             └─11889 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/b>

Oct 26 18:53:52 server1 systemd[1]: Started Kibana.
Oct 26 18:53:57 server1 kibana[11889]: Kibana is currently running with legacy >
lines 1-13/13 (END)
```

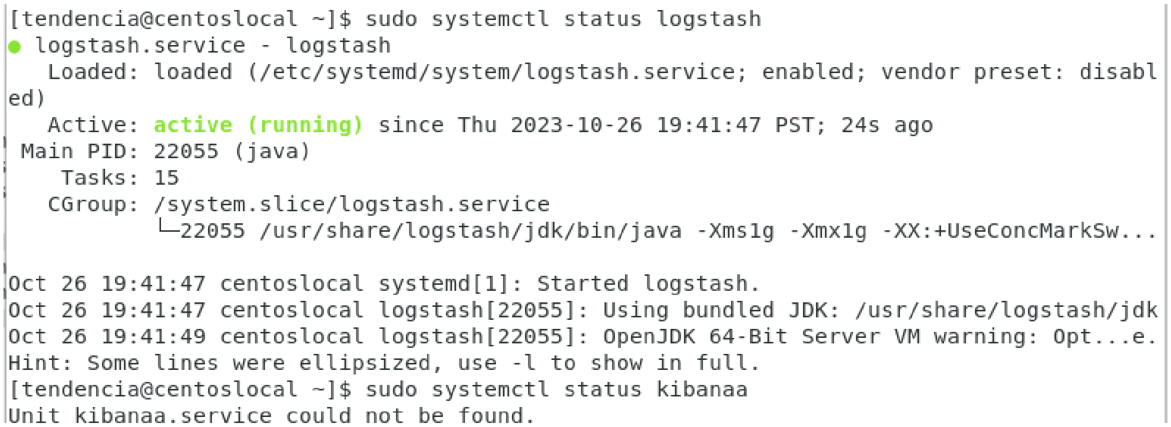
CentOS:

a. Elastic



```
[tendencia@centoslocal ~]$ sudo systemctl status elasticsearch
[sudo] password for tendencia:
Sorry, try again.
[sudo] password for tendencia:
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor prese
t: disabled)
   Active: active (running) since Thu 2023-10-26 19:25:14 PST; 16min ago
     Docs: https://www.elastic.co
 Main PID: 19962 (java)
    Tasks: 63
   CGroup: /system.slice/elasticsearch.service
           ├─19962 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkad...
           └─20212 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/...

Oct 26 19:22:57 centoslocal systemd[1]: Starting Elasticsearch...
Oct 26 19:23:58 centoslocal systemd-entrypoint[19962]: Oct 26, 2023 7:23:58 PM sun....>
Oct 26 19:23:58 centoslocal systemd-entrypoint[19962]: WARNING: COMPAT locale provi...e
Oct 26 19:25:14 centoslocal systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
```

b. Logstash



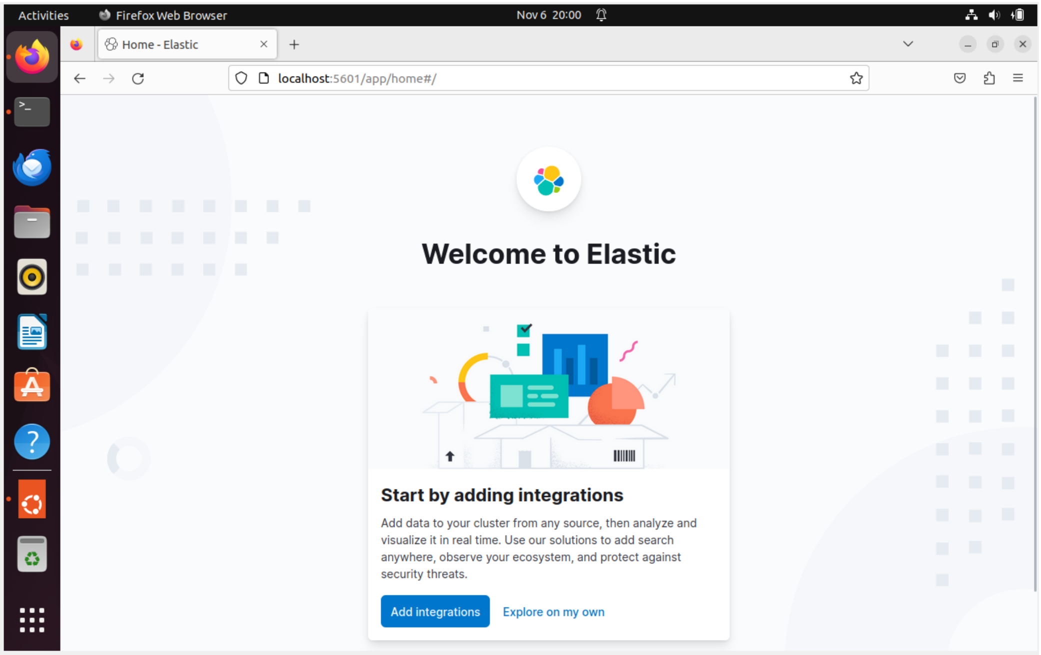
```
[tendencia@centoslocal ~]$ sudo systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabl
ed)
   Active: active (running) since Thu 2023-10-26 19:41:47 PST; 24s ago
 Main PID: 22055 (java)
    Tasks: 15
   CGroup: /system.slice/logstash.service
           └─22055 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSw...

Oct 26 19:41:47 centoslocal systemd[1]: Started logstash.
Oct 26 19:41:47 centoslocal logstash[22055]: Using bundled JDK: /usr/share/logstash/jdk
Oct 26 19:41:49 centoslocal logstash[22055]: OpenJDK 64-Bit Server VM warning: Opt...e.
Hint: Some lines were ellipsized, use -l to show in full.
[tendencia@centoslocal ~]$ sudo systemctl status kibanaa
Unit kibanaa.service could not be found.
```

c. Kibana

```
[tendencia@centoslocal ~]$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled
)
   Active: active (running) since Thu 2023-10-26 19:25:36 PST; 16min ago
     Docs: https://www.elastic.co
 Main PID: 20498 (node)
    Tasks: 11
   CGroup: /system.slice/kibana.service
           └─20498 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../s...

Oct 26 19:25:36 centoslocal systemd[1]: Started Kibana.
Oct 26 19:25:44 centoslocal kibana[20498]: Kibana is currently running with legacy...er
Hint: Some lines were ellipsized, use -l to show in full.
```

Web interface:

Ubuntu:

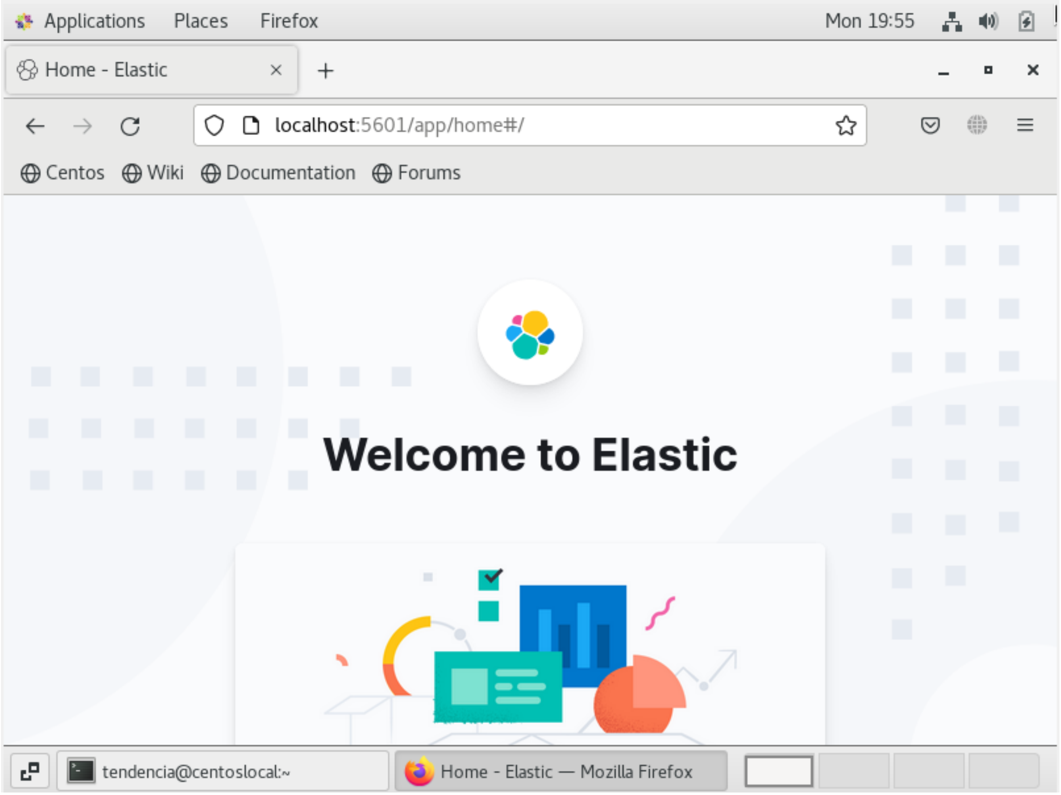


Welcome to Elastic

Start by adding integrations

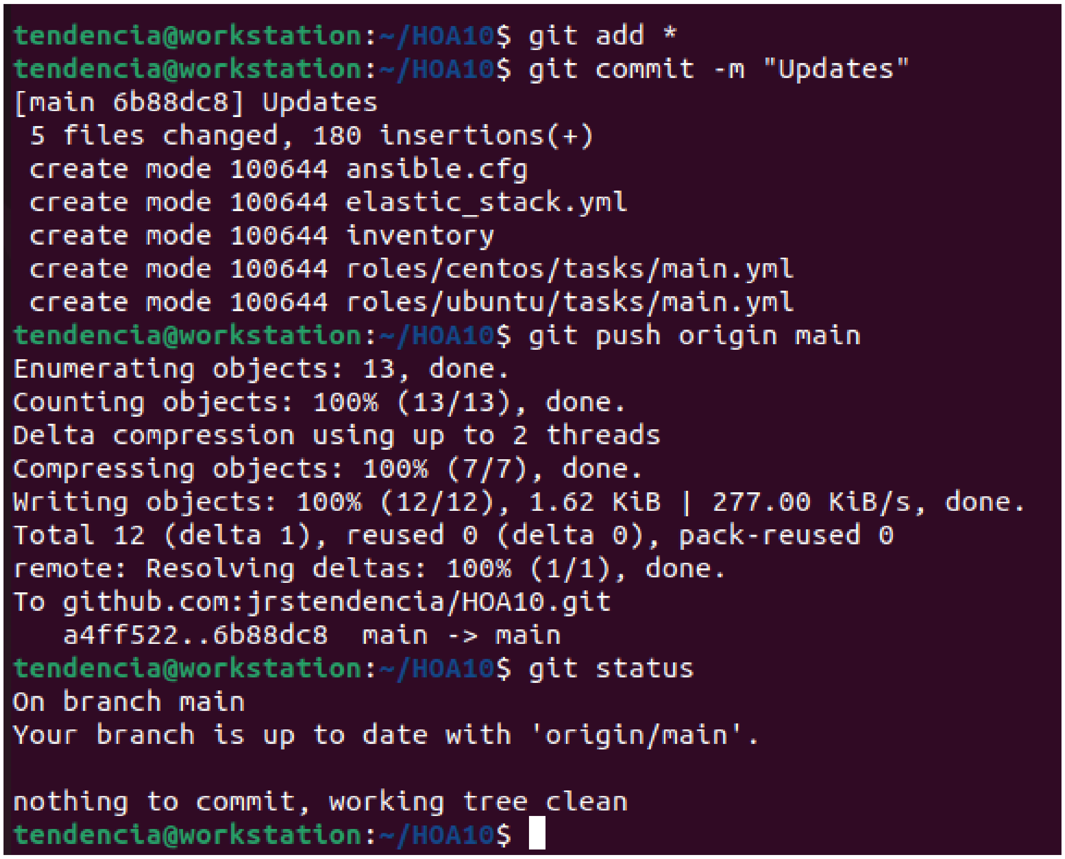
Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats.

CentOS:



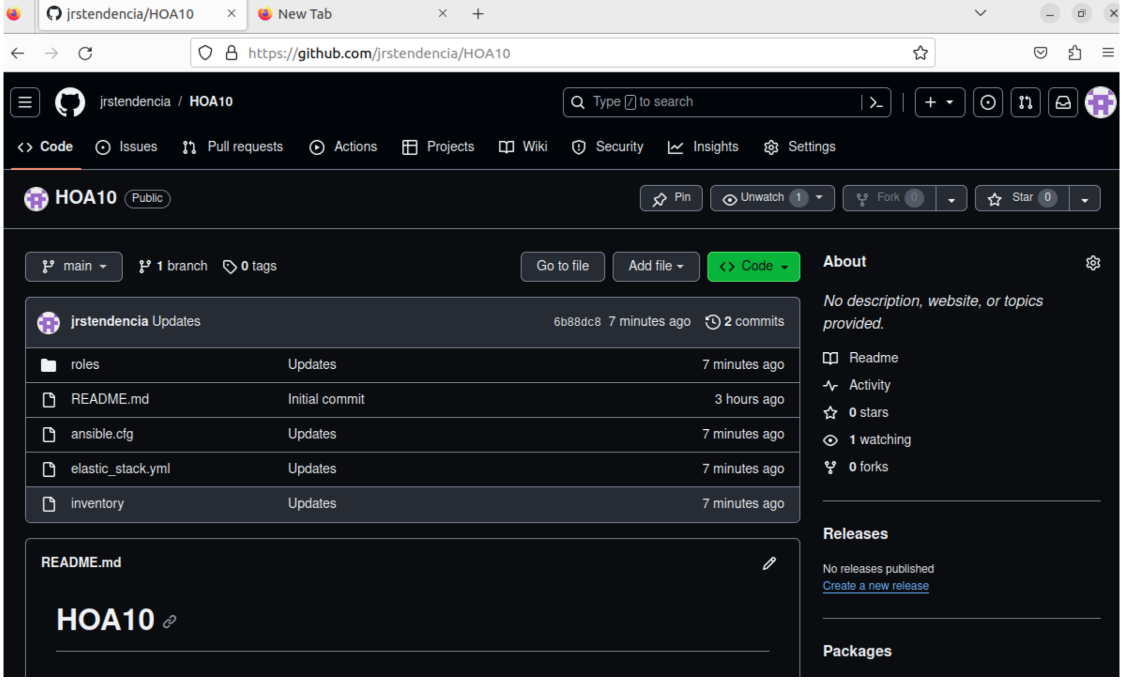
Welcome to Elastic

8. Sync the changes in github.



```
tendencia@workstation:~/HOA10$ git add *
tendencia@workstation:~/HOA10$ git commit -m "Updates"
[main 6b88dc8] Updates
 5 files changed, 180 insertions(+)
 create mode 100644 ansible.cfg
 create mode 100644 elastic_stack.yml
 create mode 100644 inventory
 create mode 100644 roles/centos/tasks/main.yml
 create mode 100644 roles/ubuntu/tasks/main.yml
tendencia@workstation:~/HOA10$ git push origin main
Enumerating objects: 13, done.
Counting objects: 100% (13/13), done.
Delta compression using up to 2 threads
Compressing objects: 100% (7/7), done.
Writing objects: 100% (12/12), 1.62 KiB | 277.00 KiB/s, done.
Total 12 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), done.
To github.com:jrstendencia/HOA10.git
   a4ff522..6b88dc8  main -> main
tendencia@workstation:~/HOA10$ git status
On branch main
Your branch is up to date with 'origin/main'.

nothing to commit, working tree clean
tendencia@workstation:~/HOA10$ 
```

Github repository:



jrstendencia Updates 6b88dc8 7 minutes ago 2 commits

roles	Updates	7 minutes ago
README.md	Initial commit	3 hours ago
ansible.cfg	Updates	7 minutes ago
elastic_stack.yml	Updates	7 minutes ago
inventory	Updates	7 minutes ago

No description, website, or topics provided.

No releases published
Create a new release

README.md

HOA10

Reflections:

Answer the following:

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

   Log monitoring tools like the Elastic Stack offer real-time visibility into logs, centralize log data, and provide scalability, security, and compliance benefits. They streamline troubleshooting, offer historical analysis, enable customizations, integrate with other tools, and reduce operational costs. These tools also improve decision-making, facilitate collaboration, and aid in meeting legal and compliance requirements, making them essential for modern IT environments.

Conclusions:

In conclusion, the objectives set out to create and design a workflow using Ansible as an Infrastructure as Code (IaC) tool for installing, configuring, and managing enterprise log monitoring tools have been successfully achieved by the student through their active participation in relevant activities. These activities, involving the Elastic Stack, Logstash, and Kibana, provided hands-on experience and practical insight into log monitoring software's importance and functionality. This practical experience has equipped the student with the skills and knowledge necessary to effectively implement and utilize log monitoring tools, ultimately contributing to improved performance, enhanced security, and streamlined maintenance of the IT infrastructure.