

Name: Seruelas, Ronn Kristoper H.	Date Performed: 10-23-2023
Course/Section: CPE232 - CPE31S4	Date Submitted: 10-31-2023
Instructor: Dr. Jonathan V. Taylar	Semester and SY: 1st Sem SY23-24
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	
<p>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.</p> <p>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.</p> <p>To qualify for inclusion in the Log Monitoring category, a product must:</p> <ul style="list-style-type: none"> • Monitor the log files generated by servers, applications, or networks • Alert users when important events are detected • Provide reporting capabilities for log files <p>Elastic Stack</p> <p>ELK suite stands for Elasticsearch, Kibana, Beats, and Logstash (also known as the ELK Stack). Source: https://www.elastic.co/elastic-stack</p> <p>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.</p> <p>GrayLog</p>	

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>

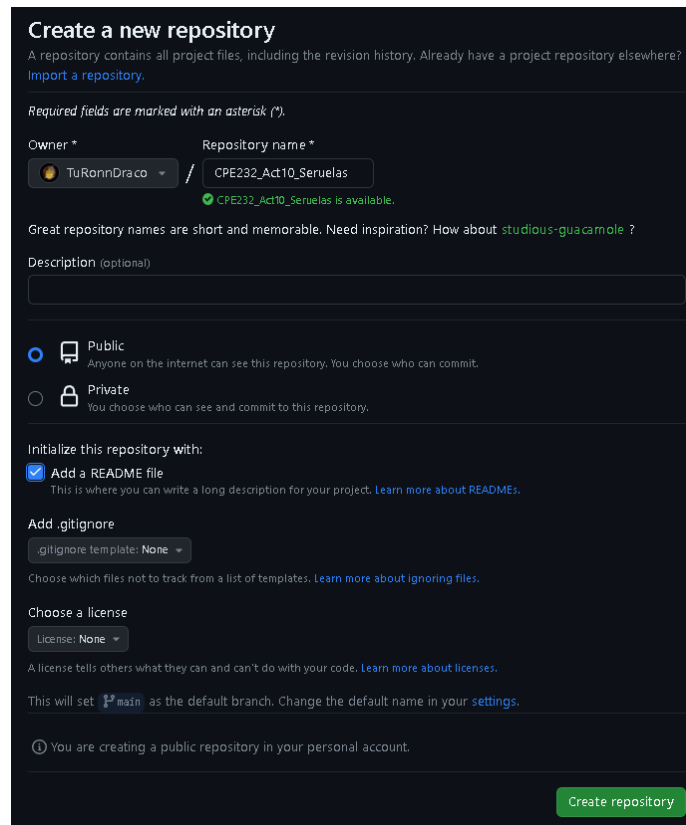
3. Tasks

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)

Task 1: Preparation of Repository

1. Create a new repository in GitHub that will be used for the installation of Elastic Stack for both Ubuntu and CentOS.



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 * TuRonnDraco / Repository name * CPE232_Act10_Seruelas
✓ CPE232_Act10_Seruelas is available.

Great repository names are short and memorable. Need inspiration? How about [studious-guacamole](#)?

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.

[Create repository](#)

Figure 1.1.1 - Creation of CPE232_Act10_Seruelas repository.

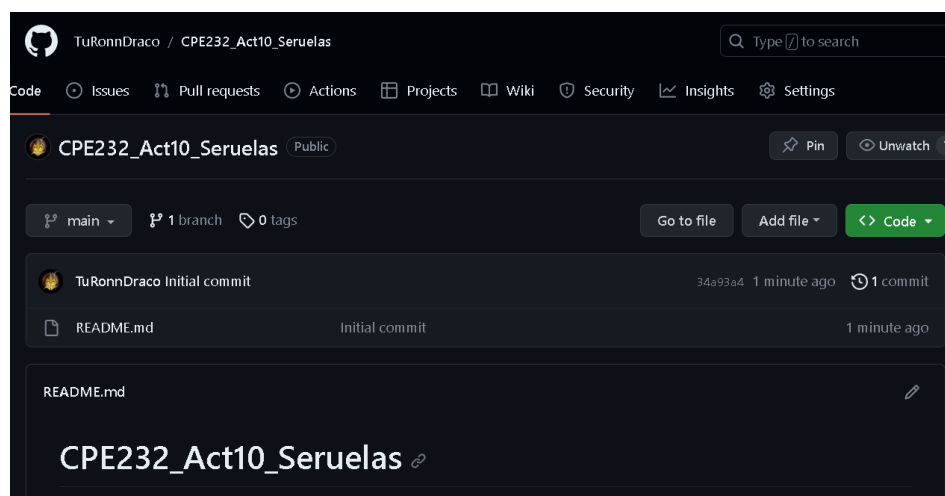


Figure 1.1.2 - CPE232_Act10_Seruelas repository.

2. Clone the GitHub repository to the local workstation.

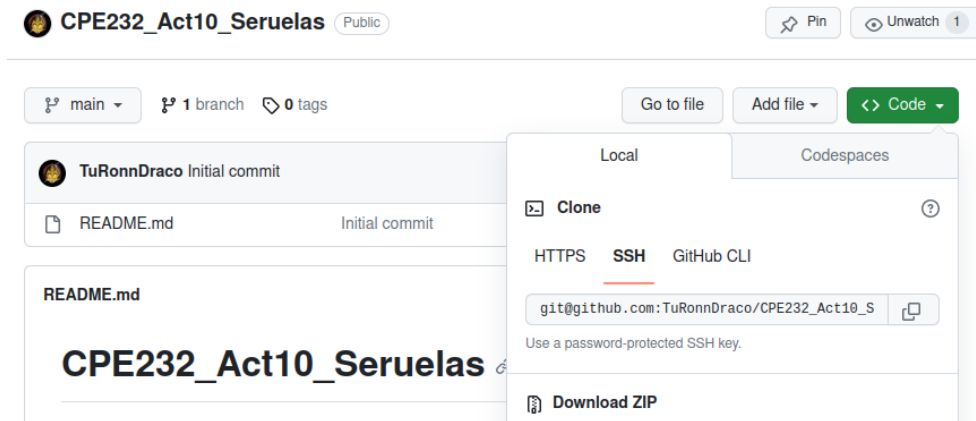


Figure 1.2.1 - Copying SSH code for cloning the repository to the local workstation.

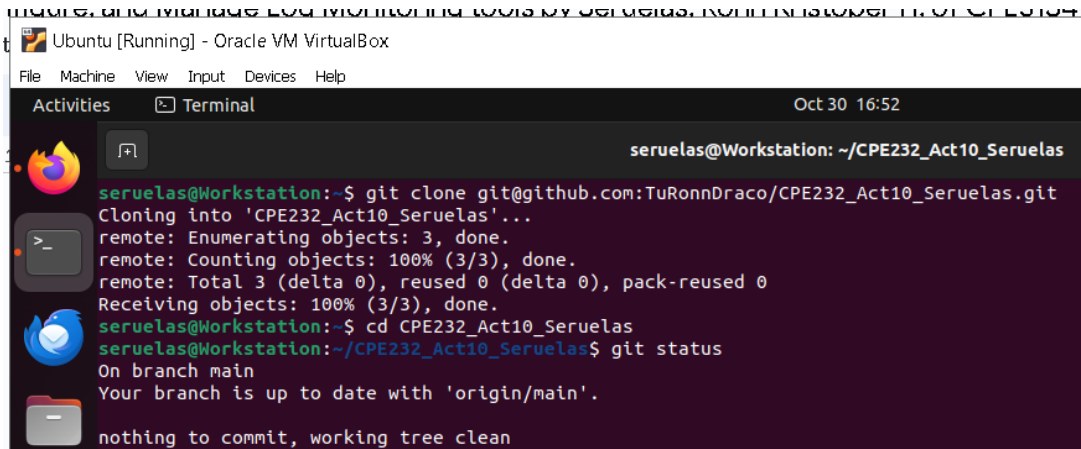


Figure 1.2.2 - Cloning the CPE232_Act10_Seruelas successfully to the local workstation.

3. Create the **roles** directory that will be used or utilized by the repository later on.

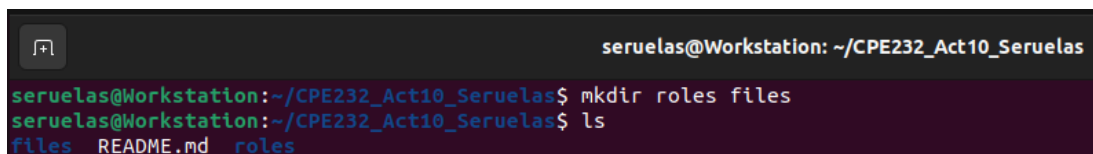
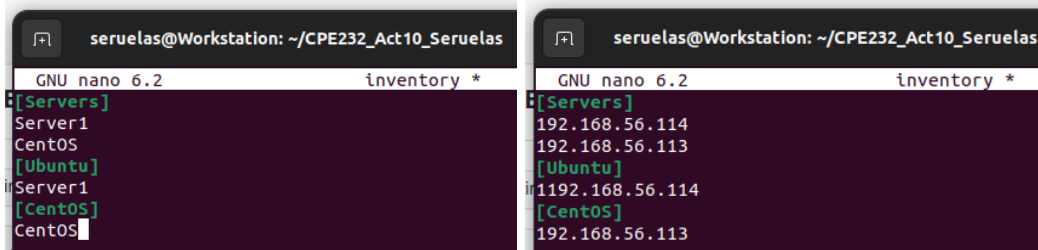


Figure 1.3.1 - Creation of the roles and files directory for the repository.

4. Create the **inventory** file that will contain the remote hosts that will have received the installation of Elastic Stack. You can create the inventory file by using the **nano** command. In the inventory file, you may specify the remote hosts via their IP addresses or hostnames.



The image shows two terminal windows side-by-side, both with the title bar 'seruelas@Workstation: ~/CPE232_Act10_Seruelas'. The left window shows the nano editor editing 'inventory *'. The content is:

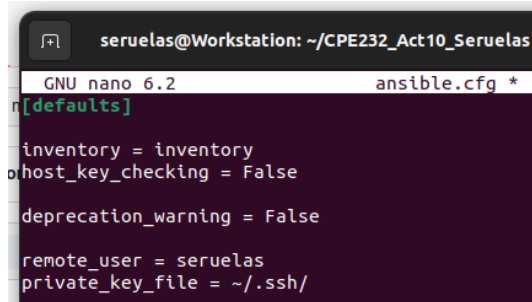
```
GNU nano 6.2 inventory *
[Servers]
Server1
CentOS
[Ubuntu]
Server1
[CentOS]
CentOS
```

The right window shows the same nano editor editing 'inventory *'. The content is:

```
GNU nano 6.2 inventory *
[Servers]
192.168.56.114
192.168.56.113
[Ubuntu]
1192.168.56.114
[CentOS]
192.168.56.113
```

Figure 1.4.1-1.4.2 - Inventory file configuration for the repository, specified in both forms (IP Address and Hostname)

5. Create the **ansible.cfg** that will contain the configuration for ansible to become properly operable for the repository. You can create the ansible.cfg file by using the nano command.



The image shows a terminal window with the title bar 'seruelas@Workstation: ~/CPE232_Act10_Seruelas'. The nano editor is editing 'ansible.cfg *'. The content is:

```
GNU nano 6.2 ansible.cfg *
[defaults]
inventory = inventory
host_key_checking = False
deprecation_warning = False
remote_user = seruelas
private_key_file = ~/.ssh/
```

Figure 1.5.1 - Ansible.cfg for the repository.

6. Save the files and changes done in the local repository and push it to the GitHub repository, by first using **git add *** to add all files recently created and changed, second by using **git commit -m "<message>"** to commit the changes and using **git push origin** to finalize and save all changes to GitHub.

```
seruelas@Workstation: ~/CPE232_Act10_Seruelas
seruelas@Workstation:~/CPE232_Act10_Seruelas$ git add *
seruelas@Workstation:~/CPE232_Act10_Seruelas$ git commit -m "5:09pm at 10-30-2023"
[main d58efce] 5:09pm at 10-30-2023
2 files changed, 16 insertions(+)
create mode 100644 ansible.cfg
create mode 100644 inventory
seruelas@Workstation:~/CPE232_Act10_Seruelas$ git push origin
Enumerating objects: 5, done.
Counting objects: 100% (5/5), done.
Delta compression using up to 2 threads
Compressing objects: 100% (4/4), done.
Writing objects: 100% (4/4), 474 bytes | 474.00 KiB/s, done.
Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
To github.com:TuRonnDraco/CPE232_Act10_Seruelas.git
34a93a4..d58efce main -> main
```

Figure 1.6.1 - Saving all changes to GitHub repository from Local Workstation.

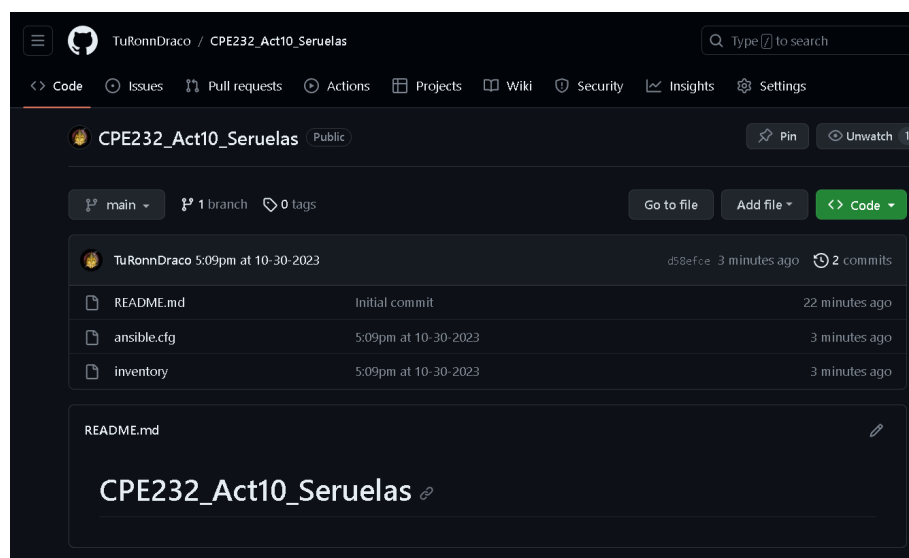


Figure 1.6.2 - Saved changes present in GitHub repository.

Task 2: Creation and Preparation of `install_elasticstack.yml`

1. By using **nano**, create the **install_elasticstack.yml** with its default syntaxes that includes allowing sudo or higher privileges of executing the commands that require higher permissions than the standard user. Include also a pre-task that will update the repository index of the remote hosts, as well as update them to their latest versions.

```
seruelas@Workstation: ~/CPE232_Act10_Seruelas
GNU nano 6.2 install_elasticstack.yml *
---
- hosts: all
  become: true
  pre_tasks:

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

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

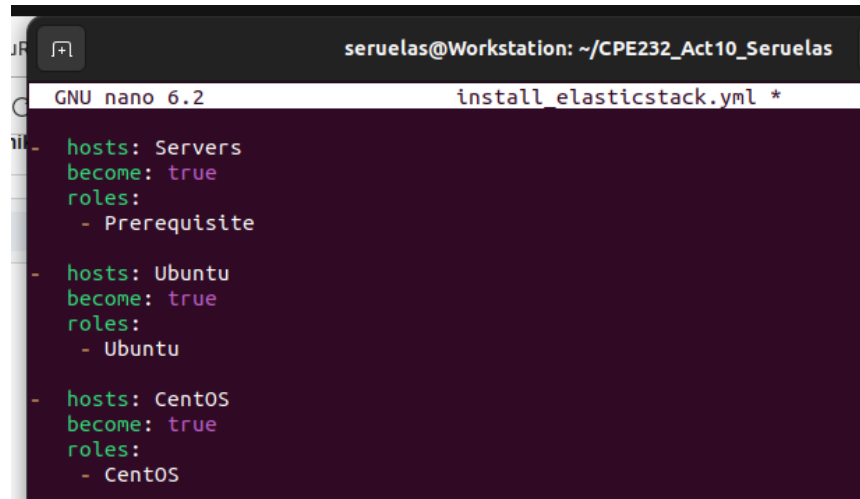
Figure 2.1.1 - Inside of install_elasticstack.yml, with pre-tasks set to update the cache and the remote hosts to the latest version.

2. Inside the roles directory, create the three new directories: **Prerequisite**, **Ubuntu**, and **CentOS**, in which each directory will contain another directory named **tasks**, with a file **main.yml**, that will serve as the script for that role.

```
seruelas@Workstation: ~/CPE232_Act10_Seruelas
seruelas@Workstation:~/CPE232_Act10_Seruelas$ cd roles
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles$ mkdir Prerequisite Ubuntu CentOS
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles$ cd Prerequisite
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/Prerequisite$ mkdir tasks
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/Prerequisite/tasks$ touch main.yml
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/Prerequisite/tasks$ cd ..
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/Prerequisite$ cd ..
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles$ cd Ubuntu
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/Ubuntu$ mkdir tasks
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/Ubuntu$ cd tasks
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/Ubuntu/tasks$ touch main.yml
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/Ubuntu/tasks$ cd ..
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/Ubuntu$ cd ..
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles$ cd CentOS
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/CentOS$ mkdir tasks
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/CentOS$ cd tasks
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/CentOS/tasks$ touch main.yml
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/CentOS/tasks$ cd ..
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles/CentOS$ cd ..
seruelas@Workstation:~/CPE232_Act10_Seruelas/roles$ cd ..
seruelas@Workstation:~/CPE232_Act10_Seruelas$ tree roles
roles
├── CentOS
│   ├── tasks
│   └── main.yml
├── Prerequisite
│   ├── tasks
│   └── main.yml
└── Ubuntu
    ├── tasks
    └── main.yml
```

Figure 2.2.1 - Creation of the roles: **Prerequisite**, **Ubuntu**, and **CentOS**, proven by using the **tree** command to show the file hierarchy of the **roles** directory.

3. Modify the **install_elasticstack.yml** to include tasks that will allow the playbook to execute multiple commands from multiple roles according to their hosts.



```
seruelas@Workstation: ~/CPE232_Act10_Seruelas
GNU nano 6.2      install_elasticstack.yml *
- hosts: Servers
  become: true
  roles:
    - Prerequisite

- hosts: Ubuntu
  become: true
  roles:
    - Ubuntu

- hosts: CentOS
  become: true
  roles:
    - CentOS
```

Figure 2.3.1 - Modified **install_elasticstack.yml** that allows the playbook to run multiple scripts for each role made.

Task 3: Scripting of **main.yml** of the **Prerequisite** role

1. Edit the **main.yml** of the **Prerequisite** role by using the **nano** command. In the **main.yml**, create a module that will download the prerequisite files or packages that will be needed by Elastic Stack.

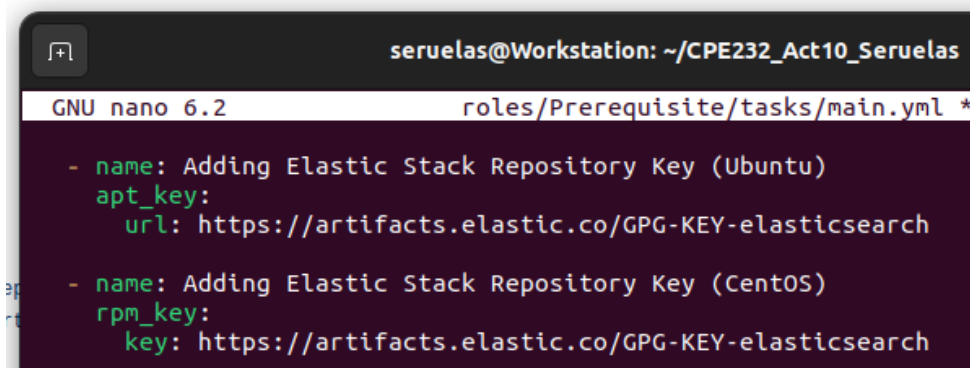
```
- name: Install Prerequisites (Ubuntu)
  apt:
    name:
      - openjdk-11-jdk
      - openjdk-8-jre
      - apt-transport-https
      - software-properties-common
      - curl
    state: present
    when: ansible_distribution == "Ubuntu"

- name: Install Prerequisites (CentOS)
  yum:
    name:
      - java-1.8.0-openjdk
      - epel-release
      - curl
    state: present
    when: ansible_distribution == "CentOS"
```

Figure 3.1.1 - Module/s that will download the pre-requisite files and packages for ElasticStack.

2. To install the Elastic Stack (ElasticSearch, Kibana and Logstash) in the remote hosts, they first require a repository key that they will use to access a repository that includes the packages of Elastic Stack that can be installed for each remote host with different ansible distribution. Create a

module that will import a public key for the repository in both ansible distributions.

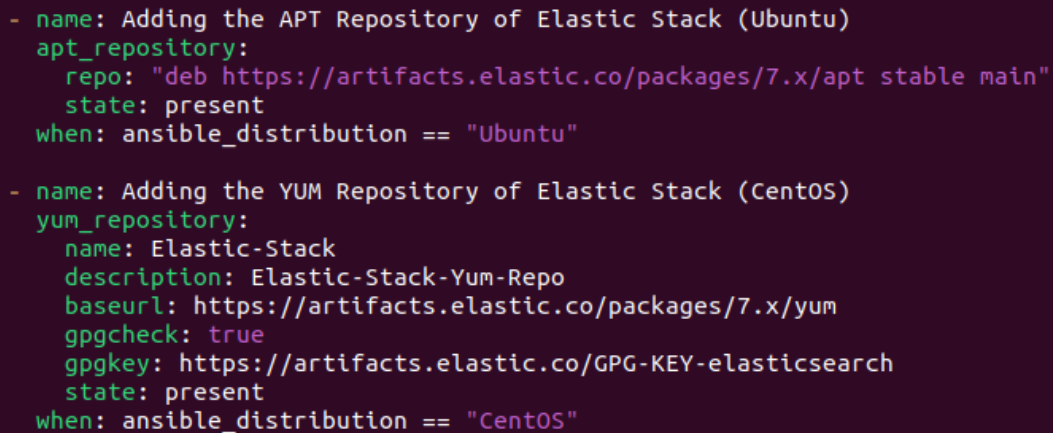
A screenshot of a terminal window with a dark background. The prompt is 'seruelas@Workstation: ~/CPE232_Act10_Seruelas'. The terminal shows the content of a file named 'roles/Prerequisite/tasks/main.yml' in nano 6.2. The file contains two Ansible tasks: one for Ubuntu using 'apt_key' and one for CentOS using 'rpm_key', both pointing to the Elastic Stack GPG key URL.

```
seruelas@Workstation: ~/CPE232_Act10_Seruelas
GNU nano 6.2 roles/Prerequisite/tasks/main.yml *
- name: Adding Elastic Stack Repository Key (Ubuntu)
  apt_key:
    url: https://artifacts.elastic.co/GPG-KEY-elasticsearch

- name: Adding Elastic Stack Repository Key (CentOS)
  rpm_key:
    key: https://artifacts.elastic.co/GPG-KEY-elasticsearch
```

Figure 3.2.1 - Module/s that will import the public repository key to the remote hosts.

3. After importing the repository key to both remote hosts, create a module that will add the repository to the remote hosts, allowing both hosts to download and install the Elastic Stack packages.

A screenshot of a terminal window showing the content of an Ansible playbook. It contains two tasks: one for Ubuntu using 'apt_repository' and one for CentOS using 'yum_repository', both adding the Elastic Stack repository.

```
- name: Adding the APT Repository of Elastic Stack (Ubuntu)
  apt_repository:
    repo: "deb https://artifacts.elastic.co/packages/7.x/apt stable main"
    state: present
  when: ansible_distribution == "Ubuntu"

- name: Adding the YUM Repository of Elastic Stack (CentOS)
  yum_repository:
    name: Elastic-Stack
    description: Elastic-Stack-Yum-Repo
    baseurl: https://artifacts.elastic.co/packages/7.x/yum
    gpgcheck: true
    gpgkey: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    state: present
  when: ansible_distribution == "CentOS"
```

Figure 3.3.1 - Module/s that will add the repositories to the remote hosts.

4. To apply all changes in each remote host, create a module that will update each remote host in order for each system to recognize the new repositories and keys added to be installed by each machine.

```
seruelas@Workstation: ~/CPE232_Act10_Seruelas
GNU nano 6.2 roles/Prerequisite/tasks/main.yml *

- name: Reloading Packages via Update (Ubuntu)
  apt:
    upgrade: dist
    update_cache: yes
  when: ansible_distribution == "Ubuntu"

- name: Reloading Packages via Update (CentOS)
  yum:
    update_only: yes
    update_cache: yes
  when: ansible_distribution == "CentOS"
```

Figure 3.4.1 - Module/s that will update each remote host.

Task 4: Scripting of main.yml of the Ubuntu and CentOS role.

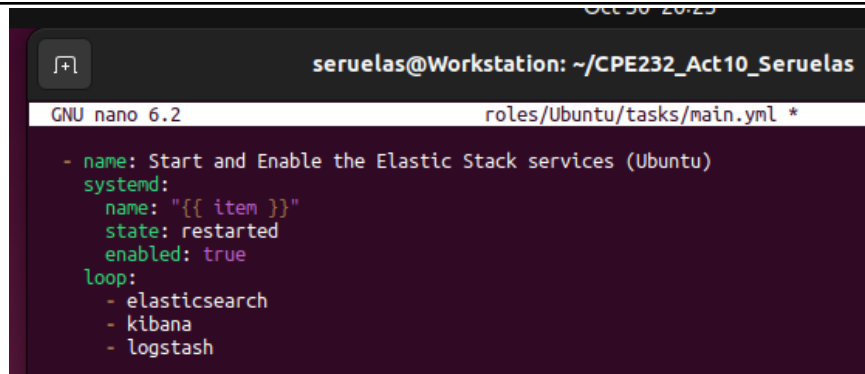
1. Modify the main.yml file of the Ubuntu role, then create a module in which it will install the **Elastic Stack** packages: **Elastic Search**, **Kibana**, **Logstash**.

```
seruelas@Workstation: ~/CPE232_Act10_Seruelas
GNU nano 6.2 roles/Ubuntu/tasks/main.yml *

- name: Install Elastic Search, Kibana, and Logstash (Ubuntu)
  apt:
    name:
      - elasticsearch
      - kibana
      - logstash
```

Figure 4.1.1 - Module that will install the Elastic Stack packages in Ubuntu.

2. Create a module that will restart and enable the Elastic Stack services.

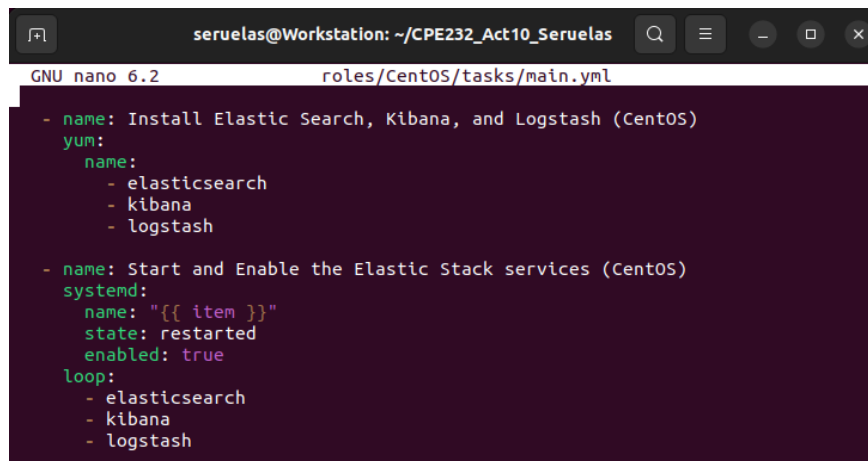


```
seruelas@Workstation: ~/CPE232_Act10_Seruelas
GNU nano 6.2 roles/Ubuntu/tasks/main.yml *

- name: Start and Enable the Elastic Stack services (Ubuntu)
  systemd:
    name: "{{ item }}"
    state: restarted
    enabled: true
  loop:
    - elasticsearch
    - kibana
    - logstash
```

Figure 4.4.1 - Module that will restart and enable the Elastic Stack services.

3. The script for the main.yml of the Ubuntu role will be the same as the script of the CentOS script.



```
seruelas@Workstation: ~/CPE232_Act10_Seruelas
GNU nano 6.2 roles/CentOS/tasks/main.yml

- name: Install Elastic Search, Kibana, and Logstash (CentOS)
  yum:
    name:
      - elasticsearch
      - kibana
      - logstash

- name: Start and Enable the Elastic Stack services (CentOS)
  systemd:
    name: "{{ item }}"
    state: restarted
    enabled: true
  loop:
    - elasticsearch
    - kibana
    - logstash
```

Figure 4.5.1 - CentOS Script copied from Ubuntu Script.

Task 5: Execution of Playbook

1. After finalizing and debugging the playbook and scripts, run the playbook and show its output, and verify its functionality or operation.

```

seruelas@Workstation: ~/CPE232_Act10_Seruelas
seruelas@Workstation:~/CPE232_Act10_Seruelas$ ansible-playbook --ask-become-pass
install_elasticstack.yml
BECOME password:
[WARNING]: Found both group and host with same name: CentOS

PLAY [all] *****

TASK [Gathering Facts] *****
ok: [Server1]
fatal: [CentOS]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect to
the host via ssh: ssh: connect to host centos port 22: No route to host", "unre
achable": true}

TASK [Install updates (Ubuntu)] *****
changed: [Server1]

PLAY [Servers] *****

TASK [Gathering Facts] *****
ok: [Server1]

TASK [Prerequisite : Install Prerequisites (Ubuntu)] *****
changed: [Server1]

TASK [Prerequisite : Install Prerequisites (CentOS)] *****
skipping: [Server1]

TASK [Prerequisite : Adding Elastic Stack Repository Key (Ubuntu)] *****
changed: [Server1]

TASK [Prerequisite : Adding Elastic Stack Repository Key (CentOS)] *****
skipping: [Server1]

TASK [Prerequisite : Adding the APT Repository of Elastic Stack (Ubuntu)] *****
changed: [Server1]

TASK [Prerequisite : Adding the YUM Repository of Elastic Stack (CentOS)] *****
skipping: [Server1]

TASK [Prerequisite : Reloading Packages via Update (Ubuntu)] *****
ok: [Server1]

TASK [Prerequisite : Reloading Packages via Update (CentOS)] *****
skipping: [Server1]

PLAY [Ubuntu] *****

TASK [Gathering Facts] *****
ok: [Server1]

TASK [Ubuntu : Install Elastic Search, Kibana, and Logstash (Ubuntu)] *****
changed: [Server1]

TASK [Ubuntu : Start and Enable the Elastic Stack services (Ubuntu)] *****
changed: [Server1] => (item=elasticsearch)
changed: [Server1] => (item=kibana)
changed: [Server1] => (item=logstash)

PLAY RECAP *****
CentOS      : ok=0    changed=0    unreachable=1    failed=0    s
kipped=0    rescued=0    ignored=0
Server1     : ok=10   changed=6    unreachable=0    failed=0    s
kipped=4    rescued=0    ignored=0

```

Figure 5.1.1.1 - install_elasticsearch.yml Play Recap for Ubuntu (done separately due to hardware capabilities and limitations)

```

seruelas@Server1:~$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-10-31 10:55:56 +08; 6min ago
     Docs: https://www.elastic.co
   Main PID: 35335 (java)
    Tasks: 65 (limit: 2262)
   Memory: 649.3M
      CPU: 1min 13.794s
   CGroup: /system.slice/elasticsearch.service
           └─35335 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.ne
              └─35517 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux->
lines 1-11/11 (END)

```

Figure 5.1.1.2 - Systemctl status of Elastic Search in Ubuntu

```

seruelas@Server1:~$ curl -X -GET "localhost:9200"
curl: (6) Could not resolve host: X
{
  "name" : "Server1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "yBGoV04ASc03B19a049ZTQ",
  "version" : {
    "number" : "7.17.14",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "774e3bfa4d52e2834e4d9d8d669d77e4e5c1017f",
    "build_date" : "2023-10-05T22:17:33.780167078Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}

```

Figure 5.1.1.2 - Verification of Elastic Search in Ubuntu via Curl command
(Unable to verify through browser due to hardware limitations)

```

seruelas@Server1:~$ systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-10-31 10:56:17 +08; 6min ago
     Docs: https://www.elastic.co
   Main PID: 35663 (node)
    Tasks: 11 (limit: 2262)
   Memory: 259.0M
      CPU: 24.364s
   CGroup: /system.slice/kibana.service
           └─35663 /usr/share/kibana/bin/../../node/bin/node /usr/share/kibana/b>

```

Figure 5.1.1.3 - Systemctl status of Kibana in Ubuntu

```

seruelas@Server1: ~
seruelas@Server1:~$ curl -GET "localhost:5601/status"
<!DOCTYPE html><html lang="en"><head><meta charset="utf-8"/><meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=
1"/><meta name="viewport" content="width=device-width"/><title>Elastic</title><style>

    @font-face {
      font-family: 'Inter';
      font-style: normal;
      font-weight: 100;
      src: url('/ui/fonts/inter/Inter-Thin.woff2') format('woff2'), url('/ui/fonts/inter/Inter-Thin.woff') format('
woff');
    }

    @font-face {
      font-family: 'Inter';
      font-style: italic;
      font-weight: 100;
      src: url('/ui/fonts/inter/Inter-ThinItalic.woff2') format('woff2'), url('/ui/fonts/inter/Inter-ThinItalic.wof
f') format('woff');
    }

    @font-face {
      font-family: 'Inter';
      font-style: normal;
      font-weight: 200;
      src: url('/ui/fonts/inter/Inter-ExtraLight.woff2') format('woff2'), url('/ui/fonts/inter/Inter-ExtraLight.wof
f') format('woff');
    }

    @font-face {
      font-family: 'Inter';
      font-style: italic;
      font-weight: 200;
      src: url('/ui/fonts/inter/Inter-ExtraLightItalic.woff2') format('woff2'), url('/ui/fonts/inter/Inter-ExtraLig
htItalic.woff') format('woff');
    }

```

Figure 5.1.1.4 - Verification of Kibana in Ubuntu via Curl command
(Unable to verify through browser due to hardware limitations)

```

seruelas@Server1:~$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor pres
   Active: active (running) since Tue 2023-10-31 11:01:49 +08; 1min 16s ago
   Main PID: 35876 (java)
     Tasks: 15 (limit: 2262)
    Memory: 412.9M
       CPU: 30.902s
   CGroup: /system.slice/logstash.service
           └─35876 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCon
lines 1-9/9 (END)

```

Figure 5.1.1.5 - Systemctl status of Logstash
(Unable to verify through browser due to hardware limitations)

```

seruelas@Workstation: ~/CPE232_Act10_Seruelas
seruelas@Workstation:~/CPE232_Act10_Seruelas$ ansible-playbook --ask-become-pass
install_elasticstack.yml
BECOME password:
[WARNING]: Found both group and host with same name: CentOS

PLAY [all] *****

TASK [Gathering Facts] *****
fatal: [Server1]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect t
o the host via ssh: ssh: connect to host server1 port 22: No route to host", "un
reachable": true}
ok: [CentOS]

TASK [Install updates (CentOS)] *****
ok: [CentOS]

PLAY [Servers] *****

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

TASK [Prerequisite : Install Prerequisites (Ubuntu)] *****
skipping: [CentOS]

TASK [Prerequisite : Install Prerequisites (CentOS)] *****
changed: [CentOS]

TASK [Prerequisite : Adding Elastic Stack Repository Key (Ubuntu)] *****
skipping: [CentOS]

TASK [Prerequisite : Adding Elastic Stack Repository Key (CentOS)] *****
changed: [CentOS]

TASK [Prerequisite : Adding the APT Repository of Elastic Stack (Ubuntu)] *****
skipping: [CentOS]

TASK [Prerequisite : Adding the YUM Repository of Elastic Stack (CentOS)] *****
changed: [CentOS]

TASK [Prerequisite : Reloading Packages via Update (Ubuntu)] *****
skipping: [CentOS]

TASK [Prerequisite : Reloading Packages via Update (CentOS)] *****
ok: [CentOS]

PLAY [CentOS] *****

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

TASK [CentOS : Install Elastic Search, Kibana, and Logstash (CentOS)] *****
changed: [CentOS]

TASK [CentOS : Start and Enable the Elastic Stack services (CentOS)] *****
changed: [CentOS] => (item=elasticsearch)
changed: [CentOS] => (item=kibana)
changed: [CentOS] => (item=logstash)

PLAY RECAP *****
CentOS                : ok=10    changed=5    unreachable=0    failed=0    s
kipped=4      rescued=0    ignored=0
Server1          : ok=0    changed=0    unreachable=1    failed=0    s
kipped=0      rescued=0    ignored=0

```

Figure 5.1.2.1 - install_elasticstack.yml Play Recap done in CentOS
(done separately due to hardware limitations)

```
[seruelas@localhost ~]$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-10-31 11:44:56 PST; 10min ago
     Docs: https://www.elastic.co
   Main PID: 4796 (java)
    Tasks: 66
   CGroup: /system.slice/elasticsearch.service
           └─4796 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.net...
             4989 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x...

Oct 31 11:44:12 localhost.localdomain systemd[1]: Starting Elasticsearch...
Oct 31 11:44:19 localhost.localdomain systemd-entrypoint[4796]: Oct 31, 2023 ...
Oct 31 11:44:19 localhost.localdomain systemd-entrypoint[4796]: WARNING: COMP...
Oct 31 11:44:56 localhost.localdomain systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
[seruelas@localhost ~]$ curl -GET "localhost:9200"
{
  "name" : "localhost.localdomain",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "k--IoAbeQci6EeaGkMLtGg",
  "version" : {
    "number" : "7.17.14",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "774e3bfa4d52e2834e4d9d8d669d77e4e5c1017f",
    "build_date" : "2023-10-05T22:17:33.780167078Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Figure 5.1.2.2 - Verification of elasticsearch service running in CentOS, verified by systemctl and curl
(Unable to verify via browser due to hardware limitations)

```
[seruelas@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 11:45:05 PST; 13min ago
     Docs: https://www.elastic.co
   Main PID: 5186 (node)
    Tasks: 11
   CGroup: /system.slice/kibana.service
           └─5186 /usr/share/kibana/bin/./node/bin/node /usr/share/kibana/bi...

Oct 31 11:45:05 localhost.localdomain systemd[1]: Started Kibana.
Oct 31 11:45:10 localhost.localdomain kibana[5186]: Kibana is currently runn...
Hint: Some lines were ellipsized, use -l to show in full.
[seruelas@localhost ~]$ curl -GET "localhost:5601/status"
<!DOCTYPE html><html lang="en"><head><meta charset="utf-8"/><meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"/><meta name="viewport" content="width=device-width"/><title>Elastic</title><style>

    @font-face {
      font-family: 'Inter';
      font-style: normal;
      font-weight: 100;
      src: url('/ui/fonts/inter/Inter-Thin.woff2') format('woff2'), url('/ui/fonts/inter/Inter-Thin.woff') format('woff');
    }

    @font-face {
      font-family: 'Inter';
      font-style: italic;
      font-weight: 100;
      src: url('/ui/fonts/inter/Inter-ThinItalic.woff2') format('woff2'), url('/ui/fonts/inter/Inter-ThinItalic.woff') format('woff');
    }
  </style>
```

Figure 5.1.2.3 - Verification of kibana service running in CentOS, verified by systemctl and curl
(Unable to verify via browser due to hardware limitations)


```
[seruelas@localhost ~]$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-10-31 11:59:15 PST; 20s ago
 Main PID: 6503 (java)
    Tasks: 15
   CGroup: /system.slice/logstash.service
           └─6503 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConc...

Oct 31 11:59:15 localhost.localdomain systemd[1]: Started logstash.
Oct 31 11:59:15 localhost.localdomain logstash[6503]: Using bundled JDK: /usr...
Oct 31 11:59:15 localhost.localdomain logstash[6503]: OpenJDK 64-Bit Server V...
Hint: Some lines were ellipsized, use -l to show in full.
```

Figure 5.1.2.4 - Verification of logstash service via systemctl in CentOS.
(Unable to verify via browser due to hardware limitations)

2. Save all changes and files to the local repository and push it all to the GitHub repository.

```
seruelas@Workstation: ~/CPE232_Act10_Seruelas
seruelas@Workstation:~/CPE232_Act10_Seruelas$ git add *
seruelas@Workstation:~/CPE232_Act10_Seruelas$ git commit -m "Finished at 12:03pm at 10-31-2023"
[main df86227] Finished at 12:03pm at 10-31-2023
 4 files changed, 56 insertions(+), 47 deletions(-)
seruelas@Workstation:~/CPE232_Act10_Seruelas$ git push origin
The authenticity of host 'github.com (20.205.243.166)' can't be established.
ED25519 key fingerprint is SHA256:+DiY3wvV6TuJJhbpZisF/zLDA0zPMSvHdKr4UvCOQU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'github.com' (ED25519) to the list of known hosts.
Enumerating objects: 24, done.
Counting objects: 100% (24/24), done.
Delta compression using up to 2 threads
Compressing objects: 100% (7/7), done.
Writing objects: 100% (13/13), 1.16 KiB | 238.00 KiB/s, done.
Total 13 (delta 4), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (4/4), completed with 4 local objects.
To github.com:TuRonnDraco/CPE232_Act10_Seruelas.git
 2d0d36b..df86227  main -> main
```

Figure 5.2.1 - Saving all changes of local repository to Github repository

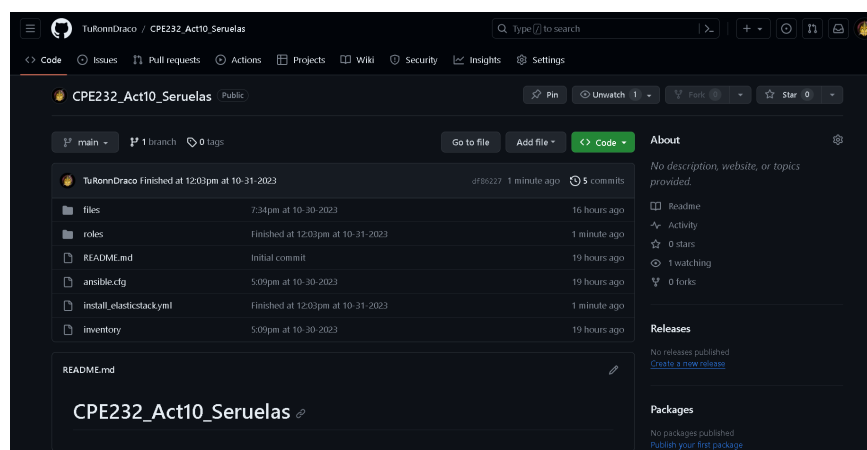


Figure 5.2.2 - CPE232_Act10_Seruelas Github Repository

https://github.com/TuRonnDraco/CPE232_Act10_Seruelas

Reflections:

Answer the following:

1. What are the benefits of having a log monitoring tool?
 - The benefits of having a log monitoring tool as a system administrator is that it allows us to actively track and to monitor the logs of the services, for the administrator to be able to see the patterns and the performance of the services themselves at the same time. With the log monitoring tool, it can detect possible mishaps or discrepancy in the service log, allowing it to be more secure for the service from any malicious problems. With the log monitoring tools, we are able to decrease and prevent most downtimes and slowdowns from the services.

Conclusions:

In this activity, we were able to discuss the importance and the functionalities of log monitoring tools such as the Elastic Stack (Elastic Search, Kibana, Logstash, etc.) and Gray Log, and what benefits they offer a system administrator for their services. We were able to educate ourselves that log monitoring services or tools allow the system administrators to become more efficient and secure as they are able to actively monitor the patterns and the consistency of the service by actively monitoring the logs produced by the services. To conclude this activity, we were able to install the Elastic Stack (Elastic Search, Kibana, and Logstash) in our virtual machines, allowing us system administrators to keep track of our service logs.