Name: Jose Mari T. Dela Peña	**Date Performed:** 10/30/2024
Course/Section: CPE31S2	**Date Submitted:** 11/04/2024
Instructor: Engr. Robin Valenzuela	**Semester and SY:** 1st Sem 2024-2025

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 it 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.

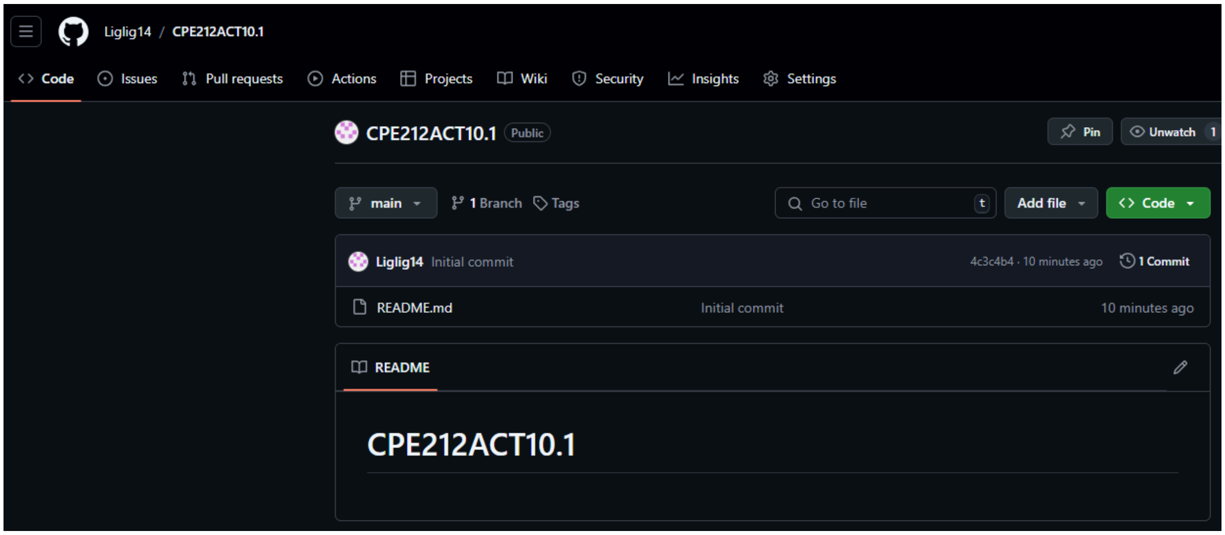
Source: https://www.graylog.org/products/open-source

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)

Step 1: Create and clone a new repository for this activity



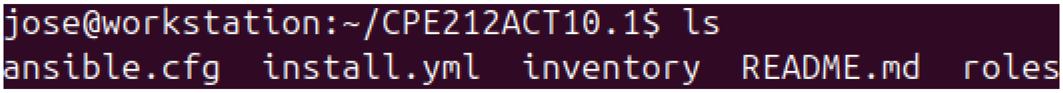
Liglig14 Initial commit 4c3c4b4 · 10 minutes ago 1 Commit

README.md Initial commit 10 minutes ago

README

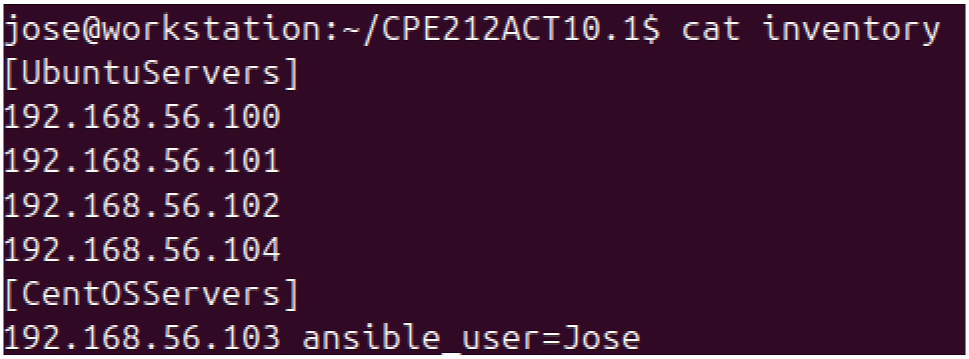
CPE212ACT10.1

Step 2: Set up ansible.cfg, inventory, roles, and install.yml



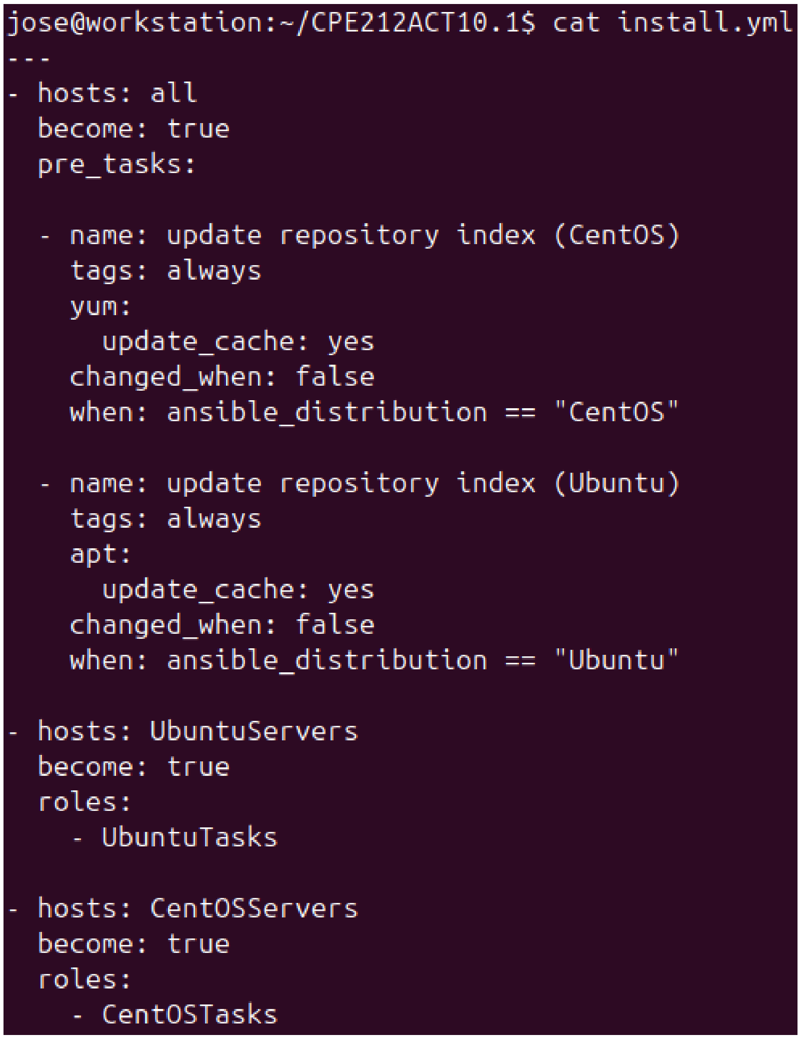
```
jose@workstation:~/CPE212ACT10.1$ ls
ansible.cfg  install.yml  inventory  README.md  roles
```

Step 3: Configure your inventory to group Ubuntu servers from CentOS servers



```
jose@workstation:~/CPE212ACT10.1$ cat inventory
[UbuntuServers]
192.168.56.100
192.168.56.101
192.168.56.102
192.168.56.104
[CentOSServers]
192.168.56.103 ansible_user=Jose
```

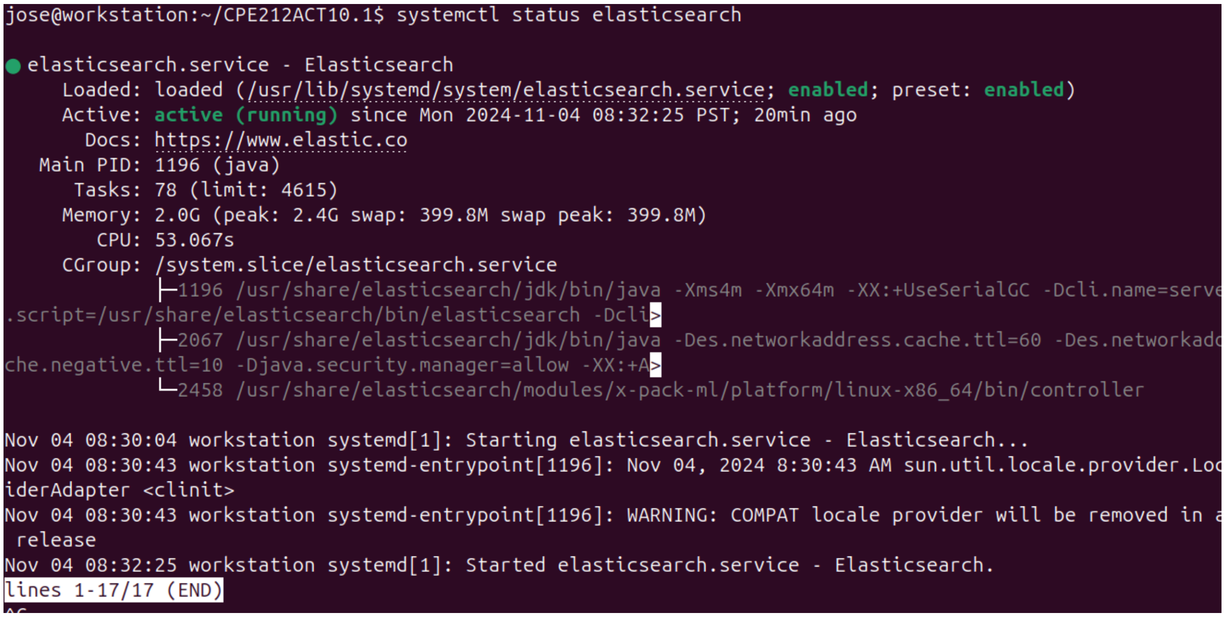
Step 4: Configure your install.yml to have it run the roles



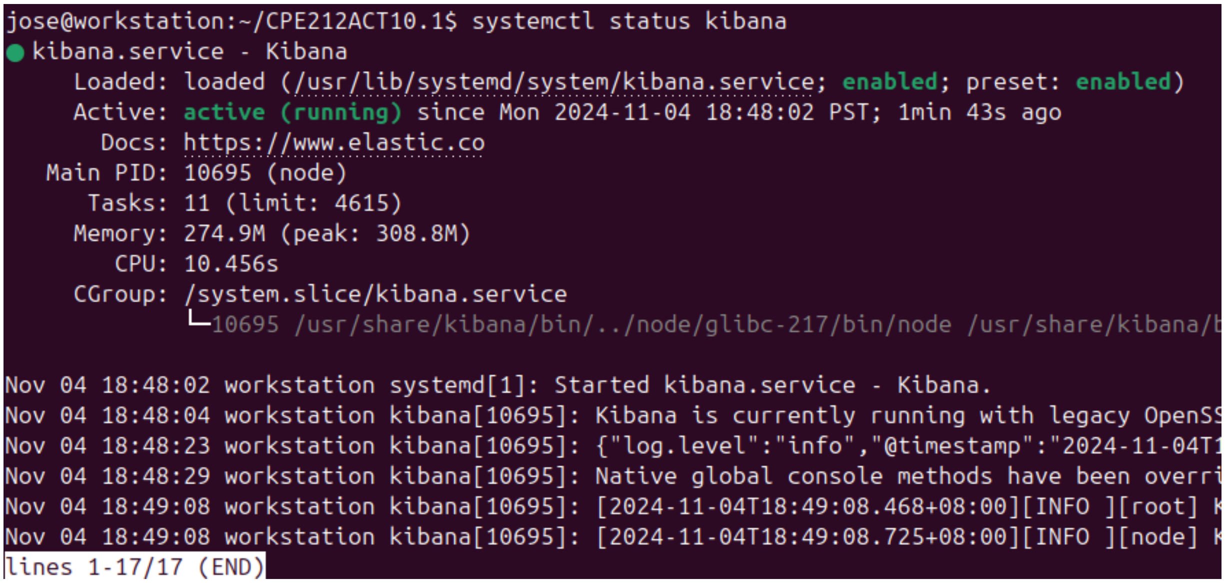
```
jose@workstation:~/CPE212ACT10.1$ cat install.yml
---
- hosts: all
  become: true
  pre_tasks:

  - name: update repository index (CentOS)
    tags: always
    yum:
      update_cache: yes
    changed_when: false
    when: ansible_distribution == "CentOS"

  - name: update repository index (Ubuntu)
    tags: always
    apt:
      update_cache: yes
    changed_when: false
    when: ansible_distribution == "Ubuntu"

- hosts: UbuntuServers
  become: true
  roles:
    - UbuntuTasks

- hosts: CentOSServers
  become: true
  roles:
    - CentOSTasks
```

Step 5: Verify that you have successfully have Elastic Stack on all servers

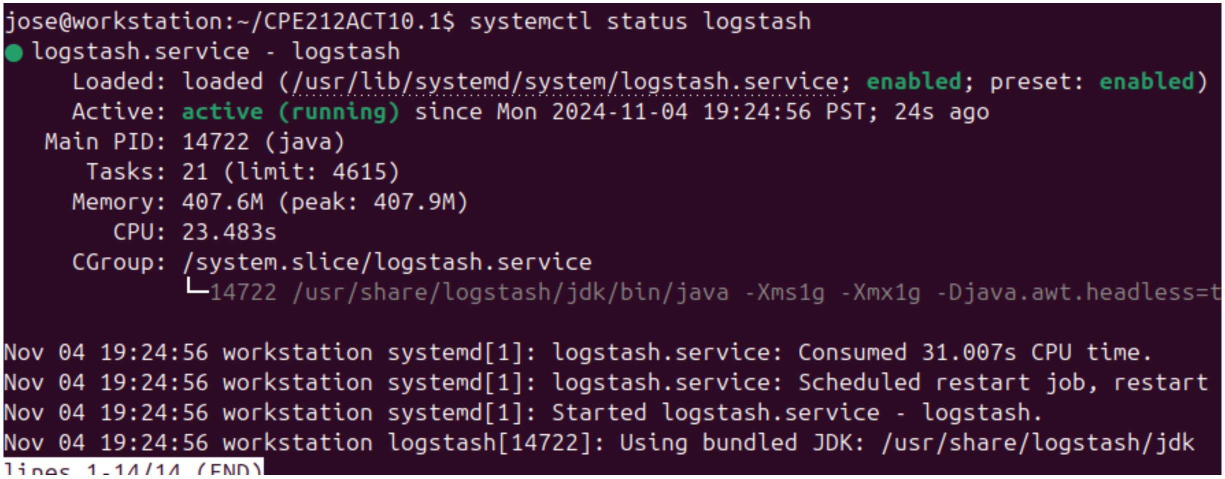
Ubuntu



```
jose@workstation:~/CPE212ACT10.1$ systemctl status elasticsearch

● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-11-04 08:32:25 PST; 20min ago
       Docs: https://www.elastic.co
   Main PID: 1196 (java)
      Tasks: 78 (limit: 4615)
     Memory: 2.0G (peak: 2.4G swap: 399.8M swap peak: 399.8M)
        CPU: 53.067s
     CGroup: /system.slice/elasticsearch.service
             ├─1196 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=serve
.script=/usr/share/elasticsearch/bin/elasticsearch -Dcli>
             ├─2067 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkadd
che.negative.ttl=10 -Djava.security.manager=allow -XX:+A>
             └─2458 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Nov 04 08:30:04 workstation systemd[1]: Starting elasticsearch.service - Elasticsearch...
Nov 04 08:30:43 workstation systemd-entrypoint[1196]: Nov 04, 2024 8:30:43 AM sun.util.locale.provider.Loc
iderAdapter <clinit>
Nov 04 08:30:43 workstation systemd-entrypoint[1196]: WARNING: COMPAT locale provider will be removed in a
 release
Nov 04 08:32:25 workstation systemd[1]: Started elasticsearch.service - Elasticsearch.
lines 1-17/17 (END)
```

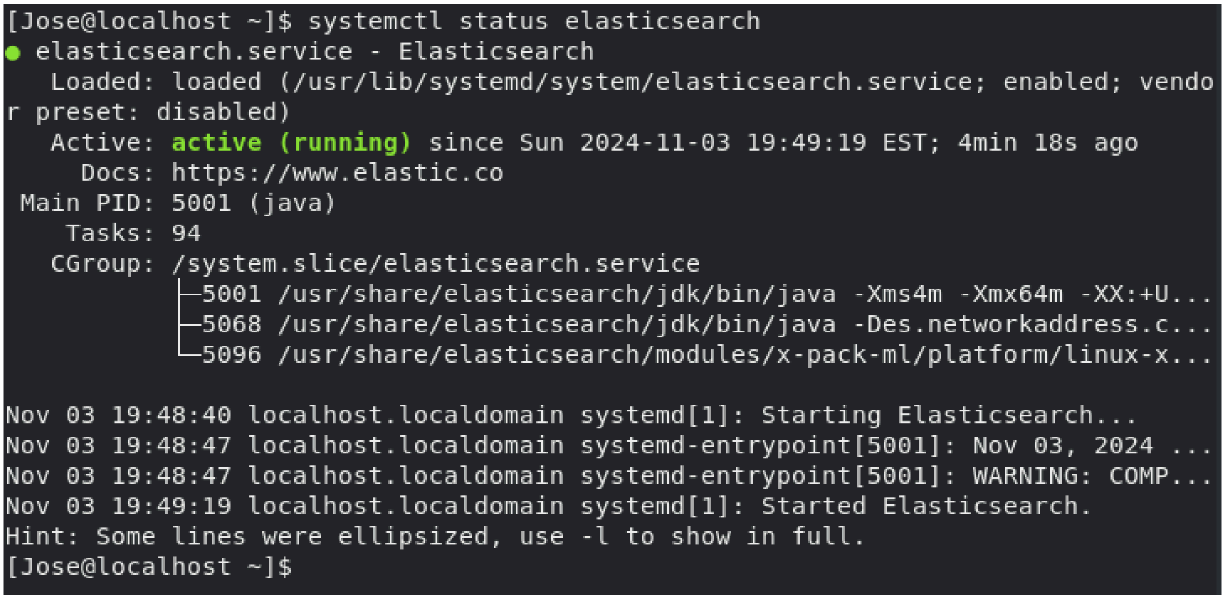


```
jose@workstation:~/CPE212ACT10.1$ systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-11-04 18:48:02 PST; 1min 43s ago
       Docs: https://www.elastic.co
   Main PID: 10695 (node)
      Tasks: 11 (limit: 4615)
     Memory: 274.9M (peak: 308.8M)
        CPU: 10.456s
     CGroup: /system.slice/kibana.service
             └─10695 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/b

Nov 04 18:48:02 workstation systemd[1]: Started kibana.service - Kibana.
Nov 04 18:48:04 workstation kibana[10695]: Kibana is currently running with legacy OpenSS
Nov 04 18:48:23 workstation kibana[10695]: {"log.level":"info","@timestamp":"2024-11-04T1
Nov 04 18:48:29 workstation kibana[10695]: Native global console methods have been overri
Nov 04 18:49:08 workstation kibana[10695]: [2024-11-04T18:49:08.468+08:00][INFO ][root] K
Nov 04 18:49:08 workstation kibana[10695]: [2024-11-04T18:49:08.725+08:00][INFO ][node] K
lines 1-17/17 (END)
```

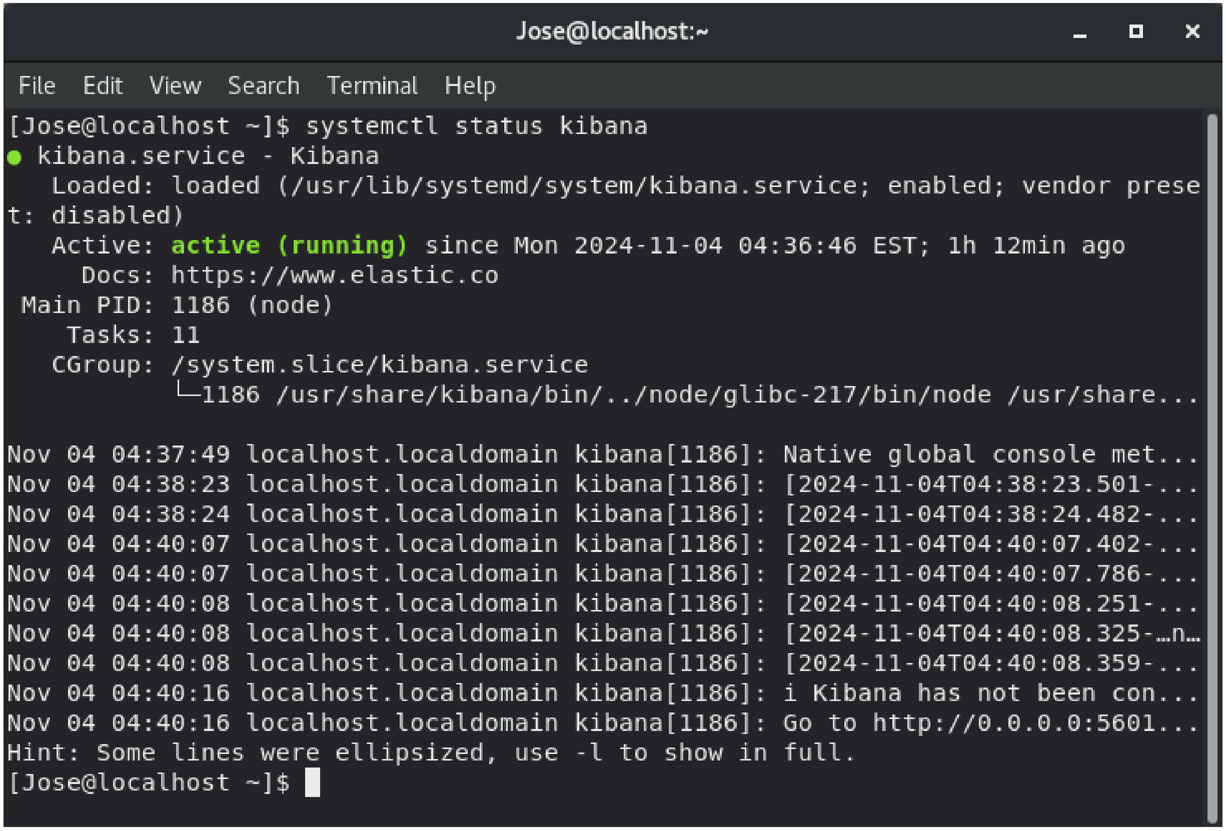


```
jose@workstation:~/CPE212ACT10.1$ systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/usr/lib/systemd/system/logstash.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-11-04 19:24:56 PST; 24s ago
   Main PID: 14722 (java)
      Tasks: 21 (limit: 4615)
     Memory: 407.6M (peak: 407.9M)
        CPU: 23.483s
     CGroup: /system.slice/logstash.service
             └─14722 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=t

Nov 04 19:24:56 workstation systemd[1]: logstash.service: Consumed 31.007s CPU time.
Nov 04 19:24:56 workstation systemd[1]: logstash.service: Scheduled restart job, restart
Nov 04 19:24:56 workstation systemd[1]: Started logstash.service - logstash.
Nov 04 19:24:56 workstation logstash[14722]: Using bundled JDK: /usr/share/logstash/jdk
lines 1-14/14 (END)
```

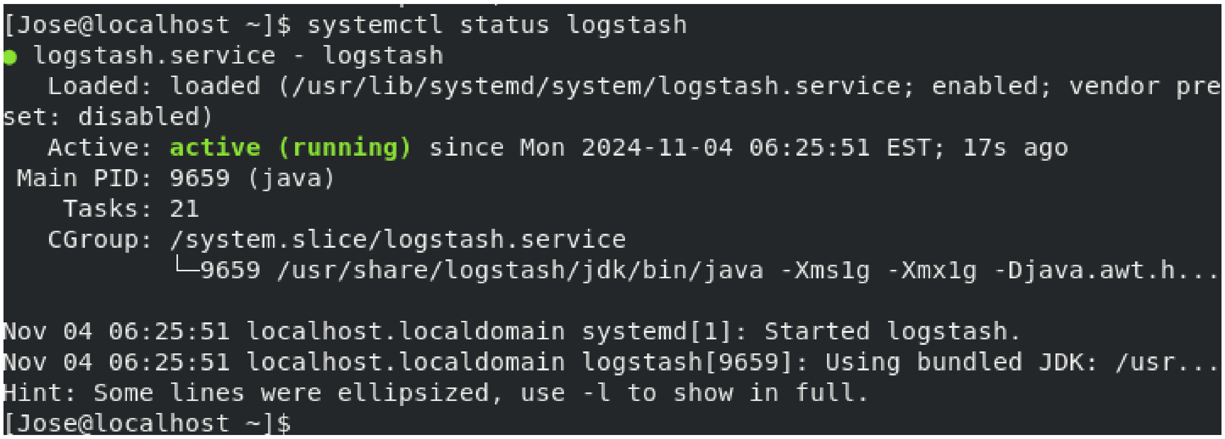
CentOS



```
[Jose@localhost ~]$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendo
r preset: disabled)
   Active: active (running) since Sun 2024-11-03 19:49:19 EST; 4min 18s ago
     Docs: https://www.elastic.co
 Main PID: 5001 (java)
    Tasks: 94
   CGroup: /system.slice/elasticsearch.service
           ├─5001 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+U...
           ├─5068 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.c...
           └─5096 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x...

Nov 03 19:48:40 localhost.localdomain systemd[1]: Starting Elasticsearch...
Nov 03 19:48:47 localhost.localdomain systemd-entrypoint[5001]: Nov 03, 2024 ...
Nov 03 19:48:47 localhost.localdomain systemd-entrypoint[5001]: WARNING: COMP...
Nov 03 19:49:19 localhost.localdomain systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
[Jose@localhost ~]$
```

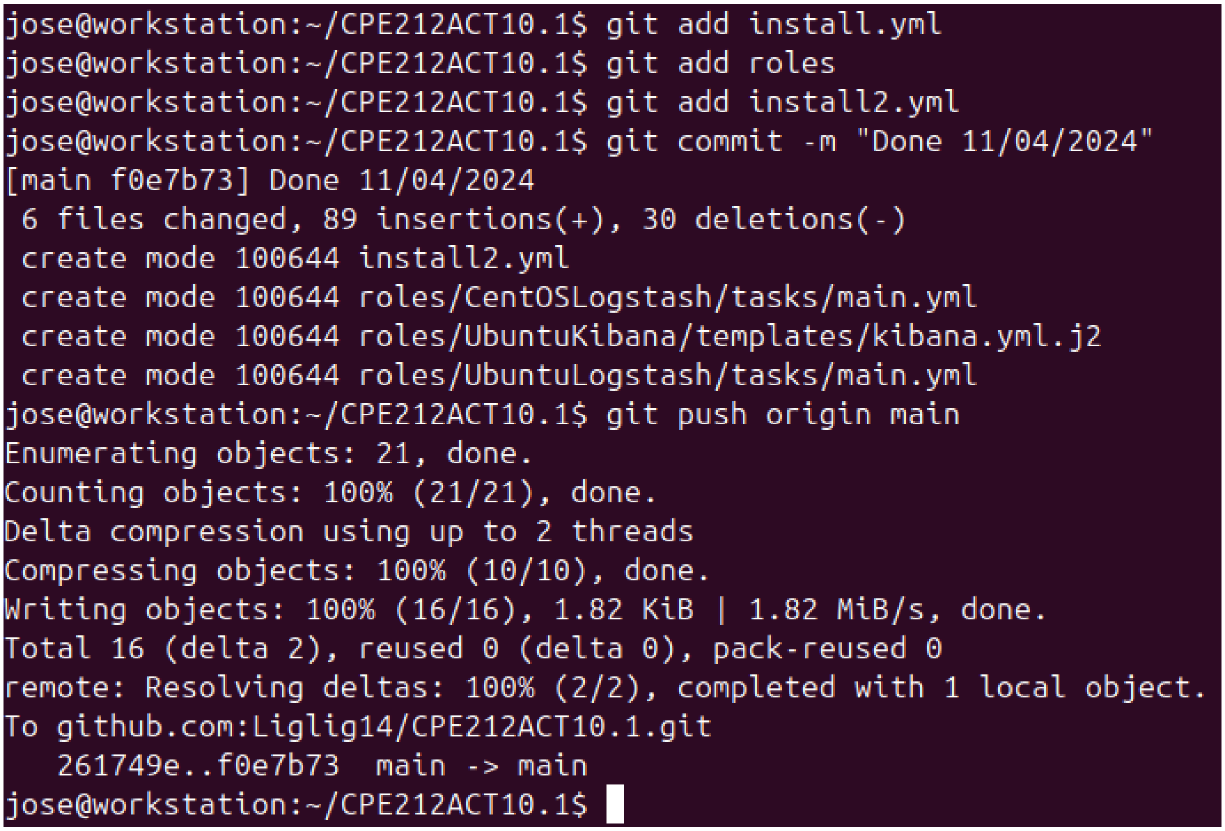


```
[Jose@localhost ~]$ systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; vendor prese
t: disabled)
   Active: active (running) since Mon 2024-11-04 04:36:46 EST; 1h 12min ago
     Docs: https://www.elastic.co
 Main PID: 1186 (node)
    Tasks: 11
   CGroup: /system.slice/kibana.service
           └─1186 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share...

Nov 04 04:37:49 localhost.localdomain kibana[1186]: Native global console met...
Nov 04 04:38:23 localhost.localdomain kibana[1186]: [2024-11-04T04:38:23.501-...
Nov 04 04:38:24 localhost.localdomain kibana[1186]: [2024-11-04T04:38:24.482-...
Nov 04 04:40:07 localhost.localdomain kibana[1186]: [2024-11-04T04:40:07.402-...
Nov 04 04:40:07 localhost.localdomain kibana[1186]: [2024-11-04T04:40:07.786-...
Nov 04 04:40:08 localhost.localdomain kibana[1186]: [2024-11-04T04:40:08.251-...
Nov 04 04:40:08 localhost.localdomain kibana[1186]: [2024-11-04T04:40:08.325-…n…
Nov 04 04:40:08 localhost.localdomain kibana[1186]: [2024-11-04T04:40:08.359-...
Nov 04 04:40:16 localhost.localdomain kibana[1186]: i Kibana has not been con...
Nov 04 04:40:16 localhost.localdomain kibana[1186]: Go to http://0.0.0.0:5601...
Hint: Some lines were ellipsized, use -l to show in full.
[Jose@localhost ~]$
```

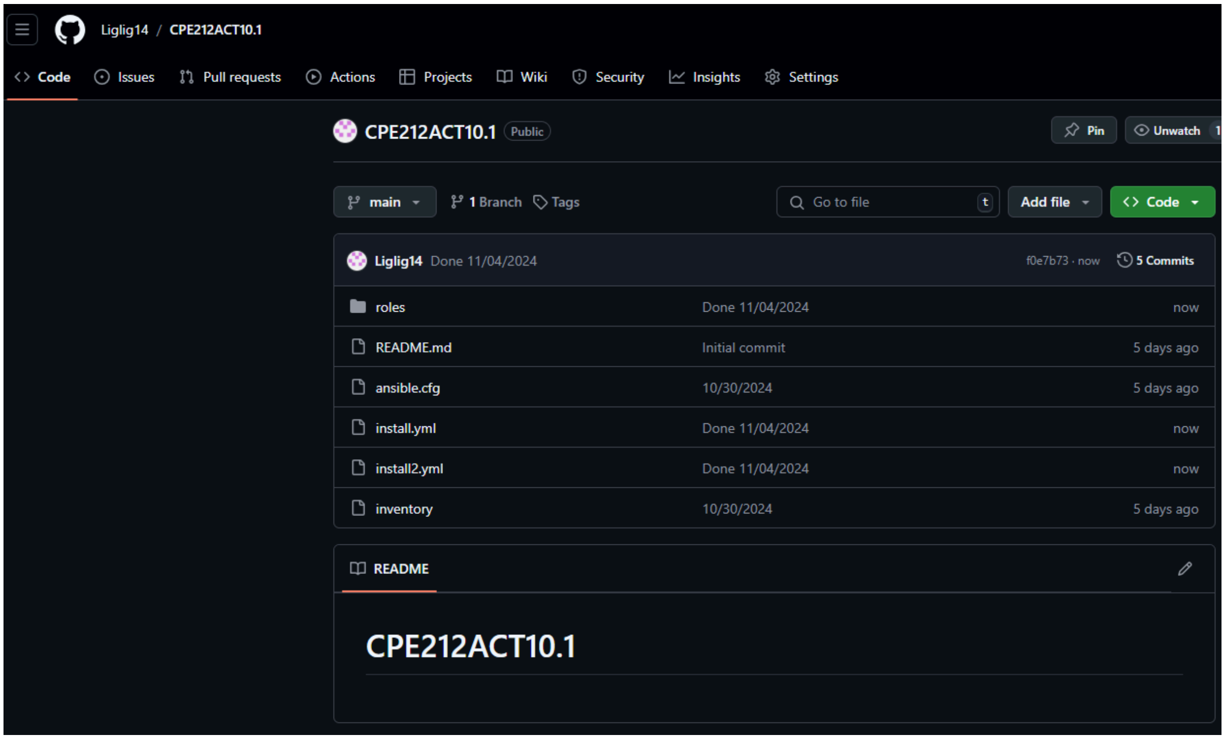


```
[Jose@localhost ~]$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/usr/lib/systemd/system/logstash.service; enabled; vendor pre
set: disabled)
   Active: active (running) since Mon 2024-11-04 06:25:51 EST; 17s ago
 Main PID: 9659 (java)
    Tasks: 21
   CGroup: /system.slice/logstash.service
           └─9659 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.h...

Nov 04 06:25:51 localhost.localdomain systemd[1]: Started logstash.
Nov 04 06:25:51 localhost.localdomain logstash[9659]: Using bundled JDK: /usr...
Hint: Some lines were ellipsized, use -l to show in full.
[Jose@localhost ~]$
```

Step 7: Push all the files to your Github repository



```
jose@workstation:~/CPE212ACT10.1$ git add install.yml
jose@workstation:~/CPE212ACT10.1$ git add roles
jose@workstation:~/CPE212ACT10.1$ git add install2.yml
jose@workstation:~/CPE212ACT10.1$ git commit -m "Done 11/04/2024"
[main f0e7b73] Done 11/04/2024
 6 files changed, 89 insertions(+), 30 deletions(-)
 create mode 100644 install2.yml
 create mode 100644 roles/CentOSLogstash/tasks/main.yml
 create mode 100644 roles/UbuntuKibana/templates/kibana.yml.j2
 create mode 100644 roles/UbuntuLogstash/tasks/main.yml
jose@workstation:~/CPE212ACT10.1$ git push origin main
Enumerating objects: 21, done.
Counting objects: 100% (21/21), done.
Delta compression using up to 2 threads
Compressing objects: 100% (10/10), done.
Writing objects: 100% (16/16), 1.82 KiB | 1.82 MiB/s, done.
Total 16 (delta 2), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (2/2), completed with 1 local object.
To github.com:Liglig14/CPE212ACT10.1.git
   261749e..f0e7b73  main -> main
jose@workstation:~/CPE212ACT10.1$ 
```



Ligllg14 Done 11/04/2024 f0e7b73 · now 5 Commits

roles	Done 11/04/2024	now
README.md	Initial commit	5 days ago
ansible.cfg	10/30/2024	5 days ago
install.yml	Done 11/04/2024	now
install2.yml	Done 11/04/2024	now
inventory	10/30/2024	5 days ago

README

CPE212ACT10.1

Reflections:

Answer the following:

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

- The Elastic Stack (ELK Stack: Elasticsearch, Logstash, and Kibana) gives numerous benefits for real time, it permits storage, and analysis of logs from various sources so that insights on system performance and security or application behavior may be reviewed without delay. Their search features in the Elasticsearch helps users in observing the issues while Logstash helps with the data processing and transformation. Also, the easy visualization tools of Kibana help the teams build creative dashboards and reports that improve collaboration and decision-making. Logs centralized creates an ideal operational efficiency and security structure.

Conclusions:

- In conclusion, implementing Elastic Stack via an Ansible playbook using roles quickens this process. This role-based approach structure allows easy updates and maintenance, while also promoting best practices for automation. With usage and emphasis on roles, one can organize tasks and dependencies effectively, which makes the process of installing Elastic Stack manageable and efficient.

Github Repository Link: **https://github.com/Liglig14/CPE212ACT10.1**