Name: Escosia, Jerico James	Date Performed: 11/15/24
Course/Section: CPE212/CPE31S21	Date Submitted: 11/15/24
Instructor: Engr. Robin Valenzuela	Semester and SY: 1st Sem

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)

```
workstation@workstation:~/Act10$ mkdir -p roles/{elasticsearch,kibana,logstash}/tasks && touch roles/{elasticsearch,
kibana,logstash}/tasks/main.yml
```

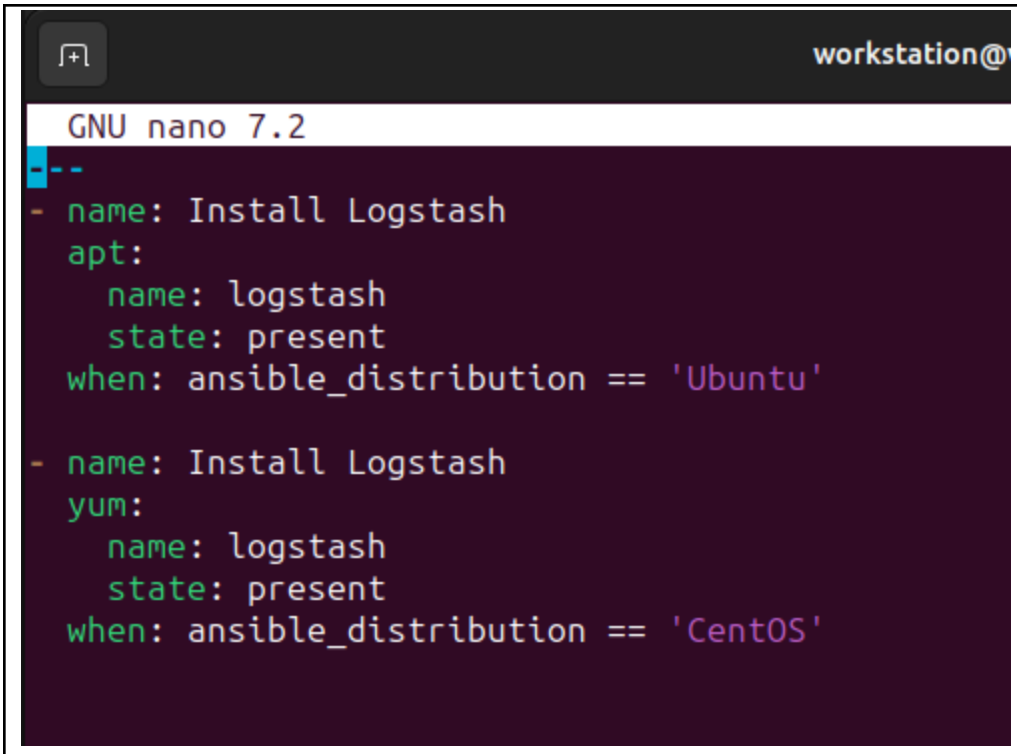
Created the roles inside the Act10 repository.

```
 GNU nano 7.2                                          main.yml
---
- name: Update Grafana Repository Key
  command: apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 8B48AD6246925553
  when: ansible_distribution == 'Ubuntu'

- name: Update APT Cache
  apt:
    update_cache: yes
  when: ansible_distribution == 'Ubuntu'

- name: Install Java
  apt:
    name: openjdk-11-jdk
    state: present
  when: ansible_distribution == 'Ubuntu'

- name: Add Elasticsearch GPG Key
  apt_key:
    url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
  when: ansible_distribution == 'Ubuntu'

- name: Install Elasticsearch
  apt_repository:
    repo: deb https://artifacts.elastic.co/packages/7.x/apt stable main
    state: present
    filename: elasticsearch-7.x
  when: ansible_distribution == 'Ubuntu'

- name: Install Elasticsearch
```

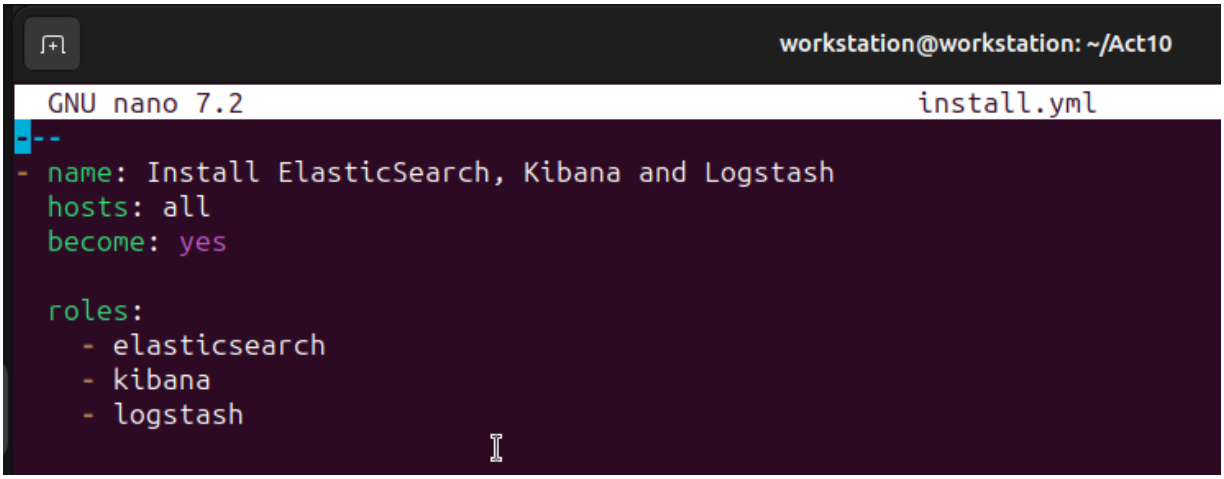
Created the main.yml playbook for Elasticsearch installation.

```
workstation@workstati
 GNU nano 7.2
---
- name: Install Kibana
  apt:
    name: kibana
    state: present
  when: ansible_distribution == 'Ubuntu'

- name: Install Kibana
  yum:
    name: kibana
    state: present
  when: ansible_distribution == 'CentOS'
```

Created the main.yml playbook for Kibana installation.



Created the main.yml playbook for Logstash installation.



Created the install.yml to perform the playbooks inside the roles.

```
TASK [elasticsearch : Install Elasticsearch] ***********************************************************
skipping: [server1]
ok: [centos]

TASK [elasticsearch : Install Elasticsearch] ***********************************************************
ok: [server1]
ok: [centos]

TASK [kibana : Install Kibana] *************************************************************************
skipping: [centos]
ok: [server1]

TASK [kibana : Install Kibana] *************************************************************************
skipping: [server1]
ok: [centos]

TASK [logstash : Install Logstash] *********************************************************************
skipping: [centos]
ok: [server1]

TASK [logstash : Install Logstash] *********************************************************************
skipping: [server1]
ok: [centos]

PLAY RECAP *********************************************************************************************
centos                     : ok=5    changed=0    unreachable=0    failed=0    skipped=7    rescued=0    ignored=0

server1                    : ok=9    changed=2    unreachable=0    failed=0    skipped=3    rescued=0    ignored=0
```

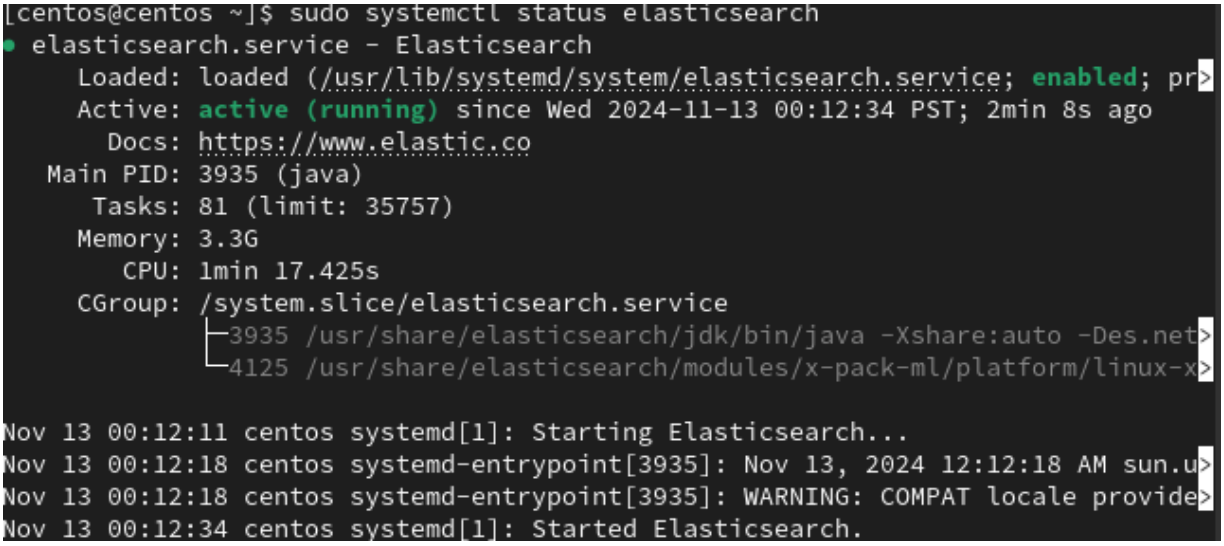
Successfully installed the Elasticsearch, Kibana and Logstash on the manage nodes after playing the install.yml playbook.

```
workstation@server1:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; preset>
     Active: active (running) since Wed 2024-11-13 00:12:08 PST; 14s ago
       Docs: https://www.elastic.co
   Main PID: 6604 (java)
      Tasks: 79 (limit: 5626)
     Memory: 2.5G
        CPU: 53.617s
     CGroup: /system.slice/elasticsearch.service
             ├─6604 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.net>
             └─6909 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>
```

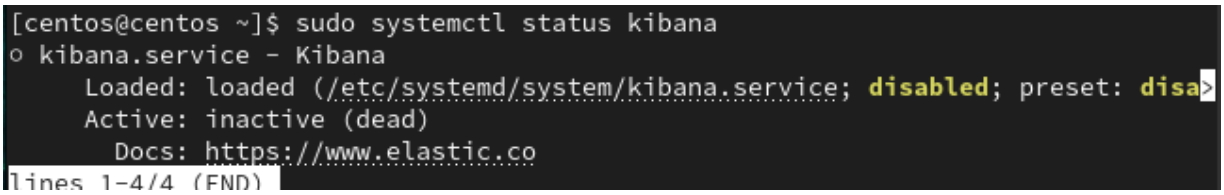
Proof that elasticsearch is installed in the manage node.

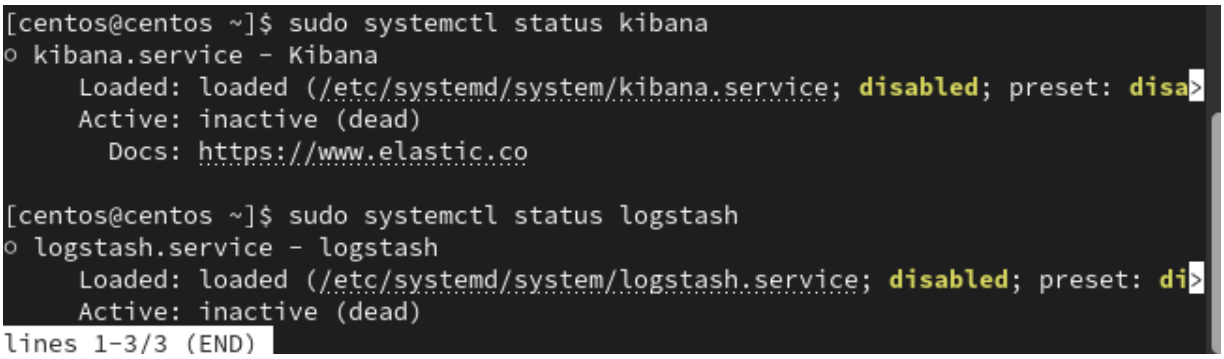
```
workstation@server1:~$ sudo systemctl status kibana
○ kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; disabled; preset: enab>
     Active: inactive (dead)
       Docs: https://www.elastic.co

workstation@server1:~$ sudo systemctl status logstash
○ logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; disabled; preset: en>
     Active: inactive (dead)
lines 1-3/3 (END)
```

Proof that the Kibana and Logstash is installed in the ubuntu manage node.



Proof that elasticsearch is installed in the Centos manage node.





Proof that the Kibana and Logstash is installed in the Centos manage node.

Reflections:

Answer the following:

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

   Log monitoring tools help gather logs from different systems into one place, making it easier to spot issues in real-time. They improve security by catching

unusual activity quickly and are also useful for investigating problems after they happen.

Conclusions:

In conclusion, log monitoring tools play a vital role in keeping our systems healthy by offering timely insights, spotting issues early, and boosting security. They're essential for minimizing downtime, improving performance, and supporting compliance through centralized log management and proactive upkeep.