Name: De Omampo, Julius Mark A.	**Date Performed:** 11/03/24
Course/Section: CPE212 – CPE31S2	**Date Submitted:** 11/03/24
Instructor:	**Semester and SY:** 1st (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 to work with logs aggregated by the main server.

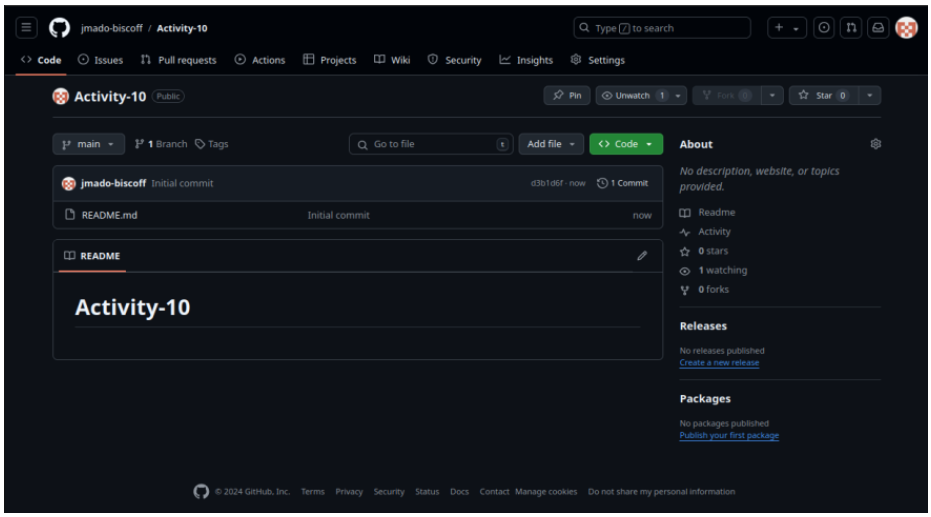
We use Graylog primarily as the stash for the logs of the web applications we build. However, it is also effective when working with raw strings (i.e. syslog): the tool parses it into the structured data we need. It also allows advanced custom search in the logs using structured queries. In other words, 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)



Repository Creation

```
 GNU nano 7.2                                ansible.cfg *
[defaults]
inventory = ~/Activity-10/inventory.yaml
remote_user = julius-de-omampo
host_key_checking = True
```

ansible.cfg File Configuration

```
 GNU nano 7.2                              inventory.yaml *
[ElasticSearch]
192.168.56.104

[Kibana]
192.168.56.106

[Logstash]
192.168.56.108
```

inventory.yaml File Configuration

```
julius-de-omampo@workstation:~/Activity-10$ mkdir roles
julius-de-omampo@workstation:~/Activity-10$ cd roles
julius-de-omampo@workstation:~/Activity-10/roles$ mkdir ElasticSearch Kibana Logstash
julius-de-omampo@workstation:~/Activity-10/roles$ ls
ElasticSearch  Kibana  Logstash
julius-de-omampo@workstation:~/Activity-10/roles$ mkdir ElasticSearch/tasks Kibana/tasks Logstash/tasks
julius-de-omampo@workstation:~/Activity-10/roles$ ls -Ra
.:
.  ..  ElasticSearch  Kibana  Logstash

./ElasticSearch:
.  ..  tasks

./ElasticSearch/tasks:
.  ..

./Kibana:
.  ..  tasks

./Kibana/tasks:
.  ..

./Logstash:
.  ..  tasks

./Logstash/tasks:
.  ..
```

Roles Creation for Managed Nodes

```
 GNU nano 7.2                                    ElasticStack.yml
---

- hosts: all
  become: true
  pre_tasks:

  - name: Install Updates (Ubuntu)
    tags: always
    apt:
      upgrade: dist
      update_cache: yes
    when: ansible_distribution === "Ubuntu"

  - name: Install Updates (CentOS)
    tags: always
    dnf:
      update_cache: yes
    when: ansible_distribution == "CentOS"

- hosts: server1
  become: true
  roles:
    - ElasticSearch

- hosts: server2
  become: true
  roles:
    - Kibana
```

ElasticStack.yaml File Configuration (1)

```
- hosts: server3
  become: true
  roles:
    - Logstash
```

ElasticStack.yaml File Configuration (2)

```
GNU nano 7.2                                  roles/ElasticSearch/tasks/main.yml
---

- name: Ensure required GPG keys are added (Ubuntu)
  apt_key:
    url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    state: present
  when: ansible_os_family == "Debian"

- name: Ensure required repositories and keys are added (Ubuntu)
  apt_repository:
    repo: "deb https://artifacts.elastic.co/packages/8.x/apt stable main"
    state: present
    filename: elasticsearch
  when: ansible_os_family == "Debian"

- name: Update apt cache (Ubuntu)
  apt:
    update_cache: yes
  when: ansible_os_family == "Debian"

- name: Install Elasticsearch
  package:
    name: elasticsearch
    state: present
  when: ansible_os_family == "Debian"

- name: Configure Elasticsearch
  lineinfile:
                                                [ Read 39 lines ]
```

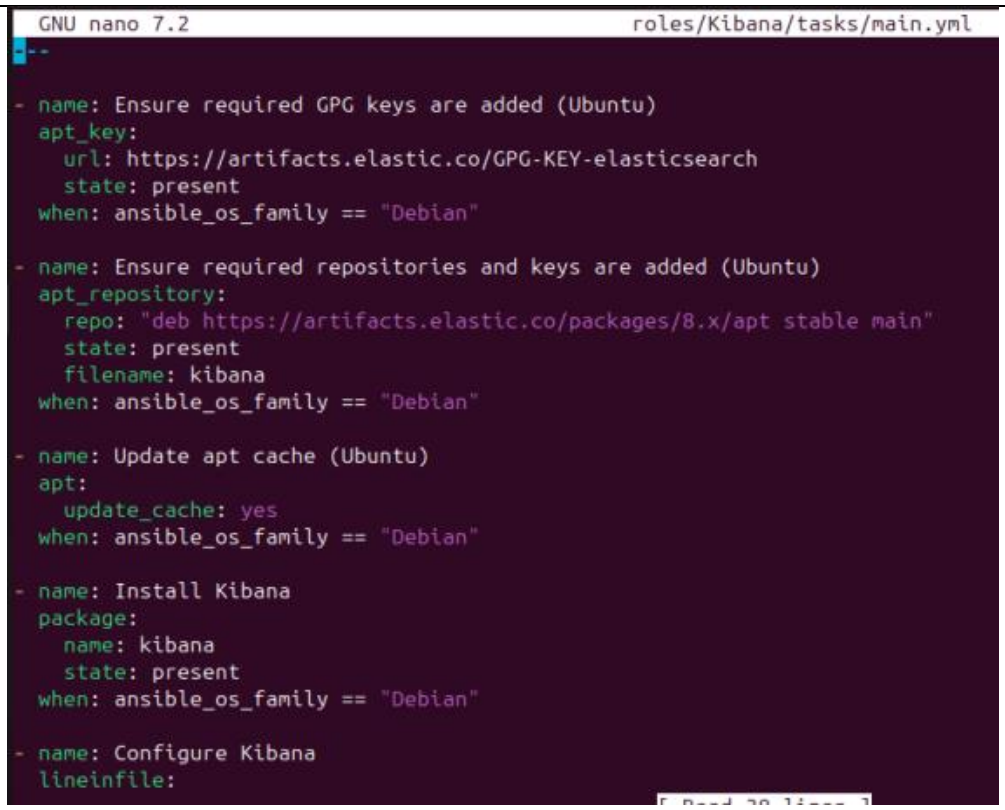
ElasticSearch main.yml File (1)

```
    path: /etc/elasticsearch/elasticsearch.yml
    regexp: "^#?(network.host:)"
    line: "network.host: localhost"
  notify: restart elasticsearch

- name: Ensure Elasticsearch is started and enabled
  service:
    name: elasticsearch
    state: started
    enabled: yes
  notify: restart elasticsearch
```

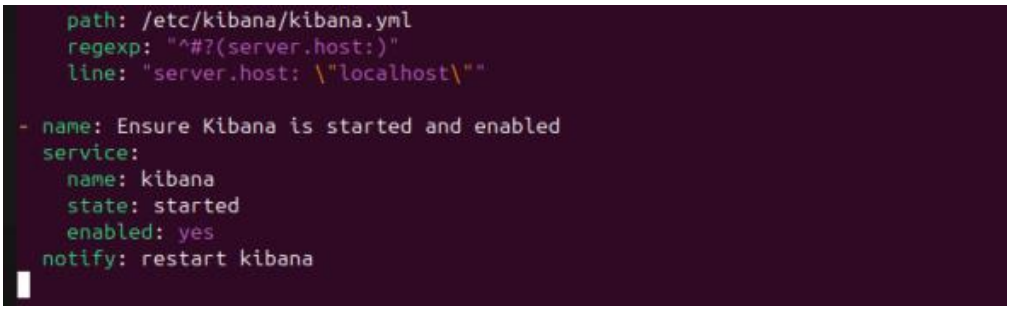
ElasticSearch main.yml File (2)

```
GNU nano 7.2                                  roles/ElasticSearch/handlers/main.yml
---

- name: restart elasticsearch
  service:
    name: elasticsearch
    state: restarted
```

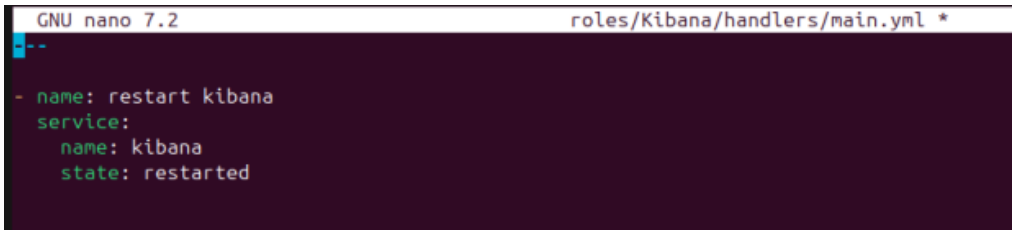
ElasticSearch Handler File



Kibana main.yml File (1)



Kibana main.yml File (2)



Kibana Handlers File

```
GNU nano 7.2                                    roles/Logstash/tasks/main.yml
---

- name: Ensure required repositories and keys are added (CentOS)
  yum_repository:
    name: logstash
    description: "Logstash repository"
    baseurl: "https://artifacts.elastic.co/packages/8.x/yum"
    gpgcheck: yes
    gpgkey: "https://artifacts.elastic.co/GPG-KEY-elasticsearch"
    enabled: yes
  when: ansible_os_family == "RedHat"

- name: Update package cache (CentOS)
  yum:
    name: "*"
    state: latest
  when: ansible_os_family == "RedHat"

- name: Install Logstash
  package:
    name: logstash
    state: present

- name: Configure Logstash
  copy:
    src: ~/Activity-10/logstash.conf
    dest: /etc/logstash/conf.d/logstash.conf
```

Logstash main.yml File (1)

```
- name: Start and enable Logstash
  service:
    name: logstash
    state: started
    enabled: yes
  notify: restart logstash
```

Logstash main.yml File (2)

```
GNU nano 7.2                                  roles/Logstash/handlers/main.yml
---

- name: restart logstash
  service:
    name: logstash
    state: restarted
```

Logstash Handlers File

```
julius-de-omampo@workstation:~/Activity-10$ ansible-playbook --ask-become-pass ElasticStack.yml
BECOME password:

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

TASK [Gathering Facts] *********************************************************************************************
ok: [192.168.56.108]
ok: [192.168.56.106]
ok: [192.168.56.104]

TASK [Install Updates (Ubuntu)] ************************************************************************************
skipping: [192.168.56.108]
ok: [192.168.56.106]
ok: [192.168.56.104]

TASK [Install Updates (CentOS)] ************************************************************************************
skipping: [192.168.56.104]
skipping: [192.168.56.106]
ok: [192.168.56.108]

PLAY [server1] *****************************************************************************************************

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

TASK [ElasticSearch : Ensure required GPG keys are added (Ubuntu)] *************************************************
ok: [192.168.56.104]

TASK [ElasticSearch : Ensure required repositories and keys are added (Ubuntu)] ************************************
ok: [192.168.56.104]
```

Playbook Report (1)

```
TASK [ElasticSearch : Update apt cache (Ubuntu)] *******************************************************************
changed: [192.168.56.104]

TASK [ElasticSearch : Install Elasticsearch] ***********************************************************************
ok: [192.168.56.104]

TASK [ElasticSearch : Configure Elasticsearch] *********************************************************************
ok: [192.168.56.104]

TASK [ElasticSearch : Ensure Elasticsearch is started and enabled] *************************************************
ok: [192.168.56.104]

PLAY [server2] *****************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************
ok: [192.168.56.106]

TASK [Kibana : Ensure required GPG keys are added (Ubuntu)] ********************************************************
ok: [192.168.56.106]

TASK [Kibana : Ensure required repositories and keys are added (Ubuntu)] *******************************************
ok: [192.168.56.106]

TASK [Kibana : Update apt cache (Ubuntu)] **************************************************************************
changed: [192.168.56.106]

TASK [Kibana : Install Kibana] *************************************************************************************
ok: [192.168.56.106]
```

Playbook Report (2)

```
TASK [Kibana : Configure Kibana] ***********************************************************************************
ok: [192.168.56.106]

TASK [Kibana : Ensure Kibana is started and enabled] ***************************************************************
ok: [192.168.56.106]

PLAY [server3] *****************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************
ok: [192.168.56.108]

TASK [Logstash : Ensure required repositories and keys are added (CentOS)] *****************************************
ok: [192.168.56.108]

TASK [Logstash : Update package cache (CentOS)] ********************************************************************
ok: [192.168.56.108]

TASK [Logstash : Install Logstash] *********************************************************************************
ok: [192.168.56.108]

TASK [Logstash : Configure Logstash] *******************************************************************************
ok: [192.168.56.108]

TASK [Logstash : Start and enable Logstash] ************************************************************************
changed: [192.168.56.108]

RUNNING HANDLER [Logstash : restart logstash] **********************************************************************
changed: [192.168.56.108]
```

Playbook Report (3)

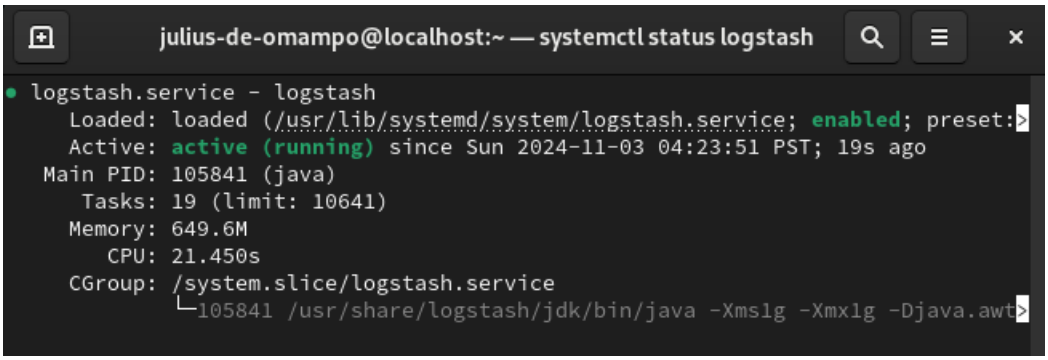
```
PLAY RECAP *********************************************************************************************************
192.168.56.104             : ok=9    changed=1    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0
192.168.56.106             : ok=9    changed=1    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0
192.168.56.108             : ok=9    changed=2    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0
```

Playbook Report (4)

```
julius-de-omampo@server1: ~
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-11-02 18:58:48 UTC; 1h 22min ago
       Docs: https://www.elastic.co
   Main PID: 19663 (java)
      Tasks: 99 (limit: 2219)
     Memory: 839.6M (peak: 1.1G swap: 572.8M swap peak: 573.6M)
        CPU: 1min 971ms
     CGroup: /system.slice/elasticsearch.service
             ├─19663 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.scri>
             ├─19725 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.n>
             └─19747 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller
```

ElasticSearch Server1 systemctl

Kibana Server2 systemctl



Logstash Server3 systemctl

Github Link: https://github.com/jmado-biscoff/Activity-10.git

Reflections:

Answer the following:

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

Using log monitoring tools like the Elastic Stack (Elasticsearch, Kibana, and Logstash) offers comprehensive insights into system and application logs, enabling real-time detection of issues and anomalies. These tools streamline the collection, processing, and visualization of log data, making it easier to identify performance bottlenecks, troubleshoot errors, and enhance security by spotting suspicious activities. The Elastic Stack also scales well, allowing efficient data management and enabling teams to respond proactively, reduce downtime, and maintain smooth operations.

Conclusions:

This activity demonstrates the process of configuring and managing a multi-component Elastic Stack setup—Elasticsearch, Kibana, and Logstash—across different environments (Ubuntu and CentOS) using both manual commands and Ansible

automation. It emphasizes the importance of precise configuration, service management, and troubleshooting across distributed nodes. By leveraging Ansible, repetitive tasks are streamlined, ensuring consistency and scalability in deployment, essential for efficient log management and data visualization within a networked infrastructure.