Name: Gabiano, Chris Leonard A.	Date Performed: 10/23/23
Course/Section: CPE31s6	Date Submitted:10/23/23
Instructor: Dr. Jonathan Taylar	Semester and SY: 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)

PART 1: create repository

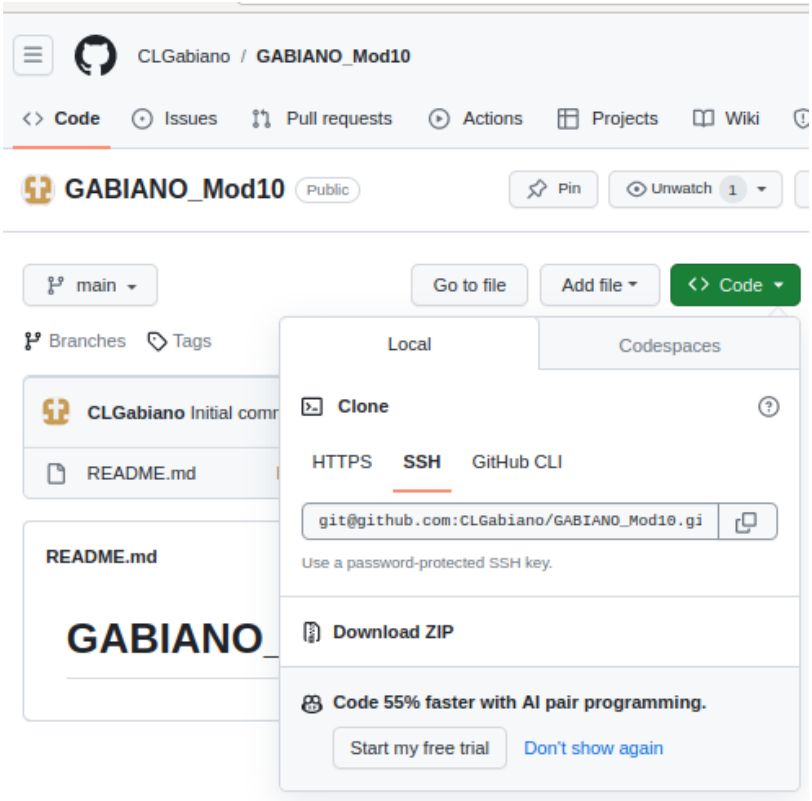


fig 1: create Activity 10 repository

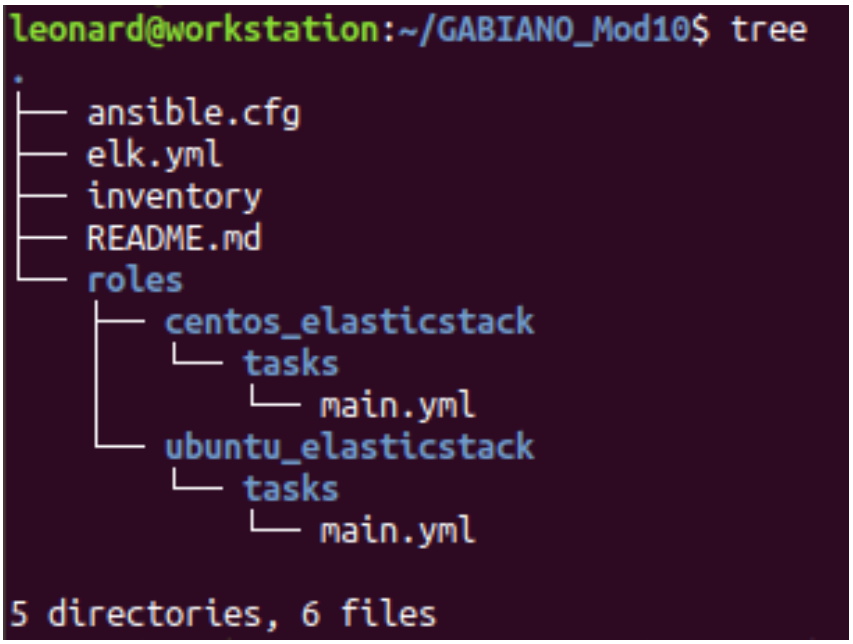


fig 2: files ansible.cfg, inventory created among directories.

PART 2: creating files for playbooks

```
 GNU nano 2.9.3                                ansible.cfg

[defaults]

inventory = inventory
host_key_checking = False

deprecation_warnings = False

remote_user = leonard
private_key_file = ~/.ssh/
```

```
leonard@workstation:~/GABIANO_Mod10$ cat inventory
[ubuntu_elasticstack]
192.168.56.102

[centos_elasticstack]
192.168.56.109
```

```
 GNU nano 2.9.3

---

- hosts: all
  become: true
  pre_tasks:

  -  name: Update repository index CentOS
     tags: always
     dnf:
       update_only: yes
       update_cache: yes
     changed_when: false
     when: ansible_distribution == "CentOS"

  -  name: Install updates Ubuntu
     tags: always
     apt:
       upgrade: dist
       update_cache: yes
     changed_when: false
     when: ansible_distribution == "Ubuntu"


- hosts: ubuntu_elasticstack
  become: true
  roles:
    - ubuntu_elasticstack

- hosts: centos_elasticstack
  become: true
  roles:
    - centos_elasticstack
```

CentOS main.yml

```
GNU nano 2.9.3                                  main.yml

- name: Install ALL Prerequisites
  dnf:
    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 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 for CentOS
  dnf:
    name: elasticsearch
    state: present
  become: yes

- name: Enable and Start Elasticsearch Service
  systemd:
    name: elasticsearch
    enabled: yes
    state: started
                                                [ Read 73 lines ]
```

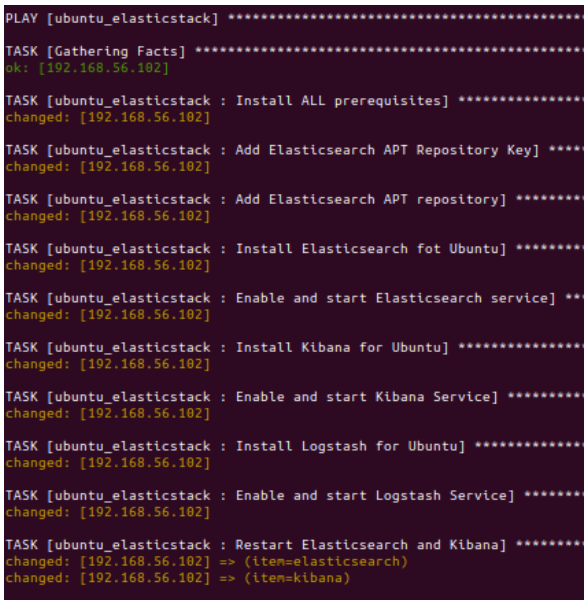
```
GNU nano 2.9.3

  become: yes

- name: Install Kibana for CentOS
  dnf:
    name: kibana
    state: present
  become: yes

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

- name: Install Logstash for CentOS
  dnf:
    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
```

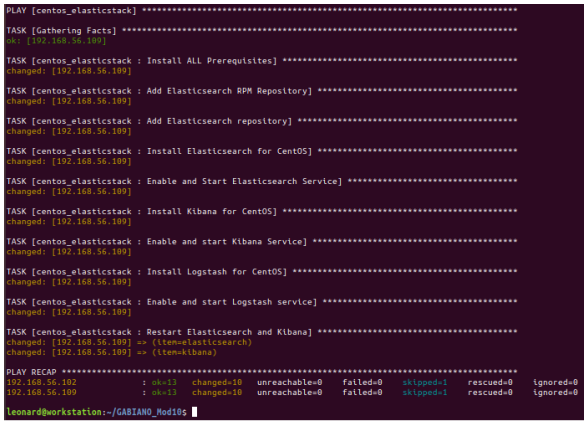
Ubuntu main.yml

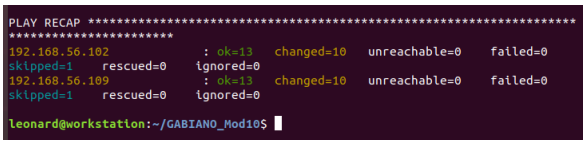
```
GNU nano 2.9.3                                          main.yml

- name: Install ALL 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 fot Ubuntu
  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 for Ubuntu
  apt:
    name: kibana
    state: present
```

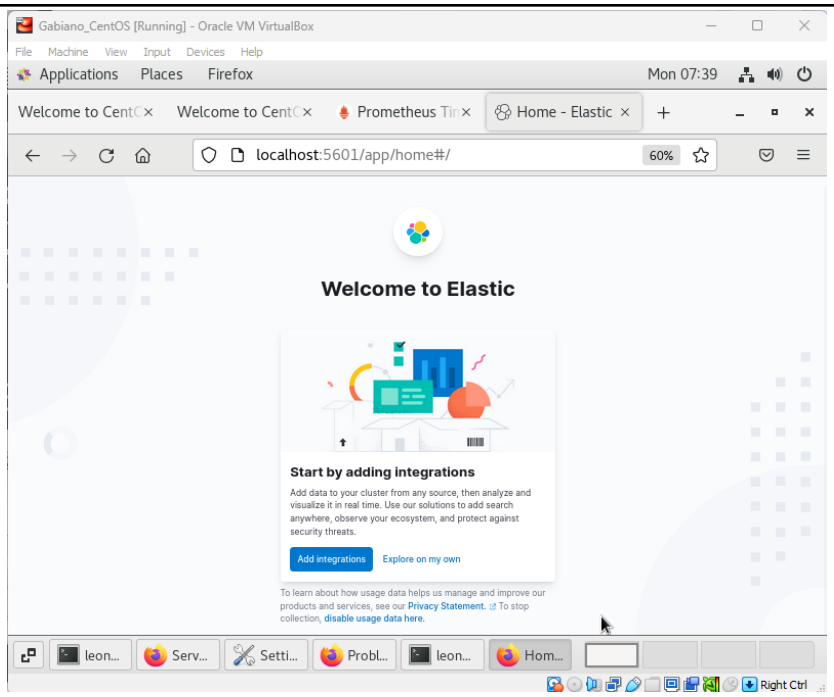
```
GNU nano 2.9.3

  become: yes

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

- name: Install Logstash for Ubuntu
  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
```

PART 3: Installation Verification

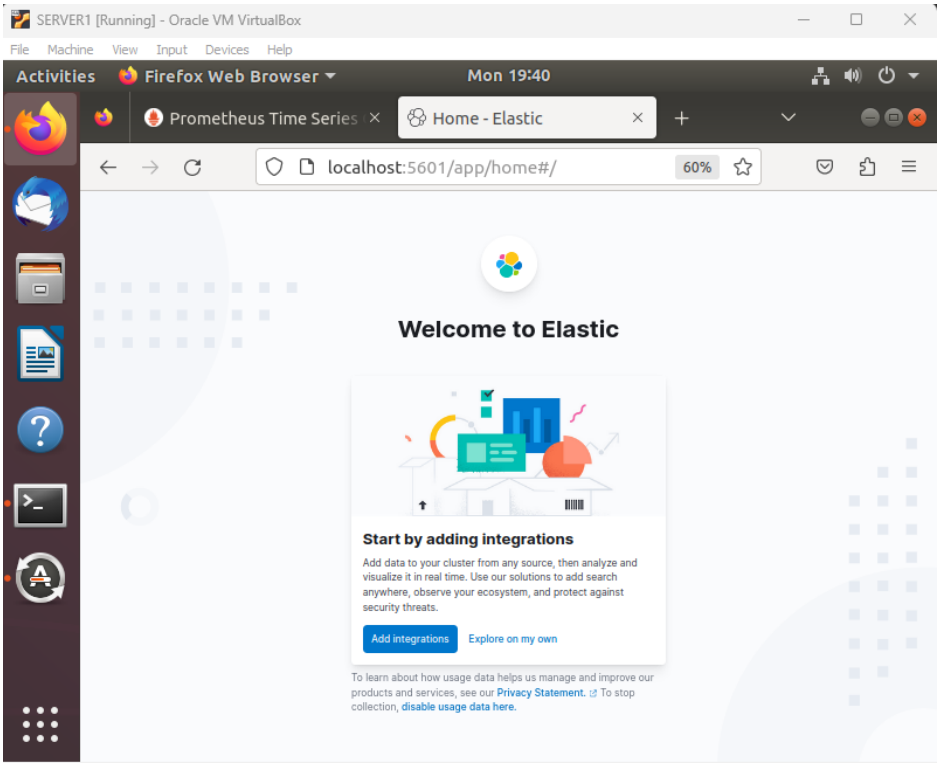








CentOS



Ubuntu

https://github.com/CLGabiano/GABIANO_Mod10.git

Reflections:

Answer the following:

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

   A performance monitoring tool provides real-time insights into system health, enabling proactive issue detection and resolution, thus minimizing downtime and improving overall system reliability. Additionally, it helps optimize resource utilization, leading to cost savings and enhanced user experience.

Conclusions:

In conclusion, we've successfully designed an Ansible workflow for the installation, configuration, and management of log monitoring tools, particularly the Elastic Stack, in separate hosts. By implementing roles, we ensure modularity and ease of maintenance in the playbook. Following a step-by-step process, we've installed the Elastic Stack components, including Elasticsearch, Kibana, and Logstash, on both Ubuntu and CentOS systems. This Infrastructure as Code (IaC) approach simplifies log monitoring and enhances system performance and security. We've also created a GitHub repository to document and version control our activity for future reference.