Name: Andreu John L. Salvador	**Date Performed: 28/10/2023**
Course/Section: CPE31S5	**Date Submitted: 28/10/2023**
Instructor: Engr. Roman Richard	**Semester and SY: 1st 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.

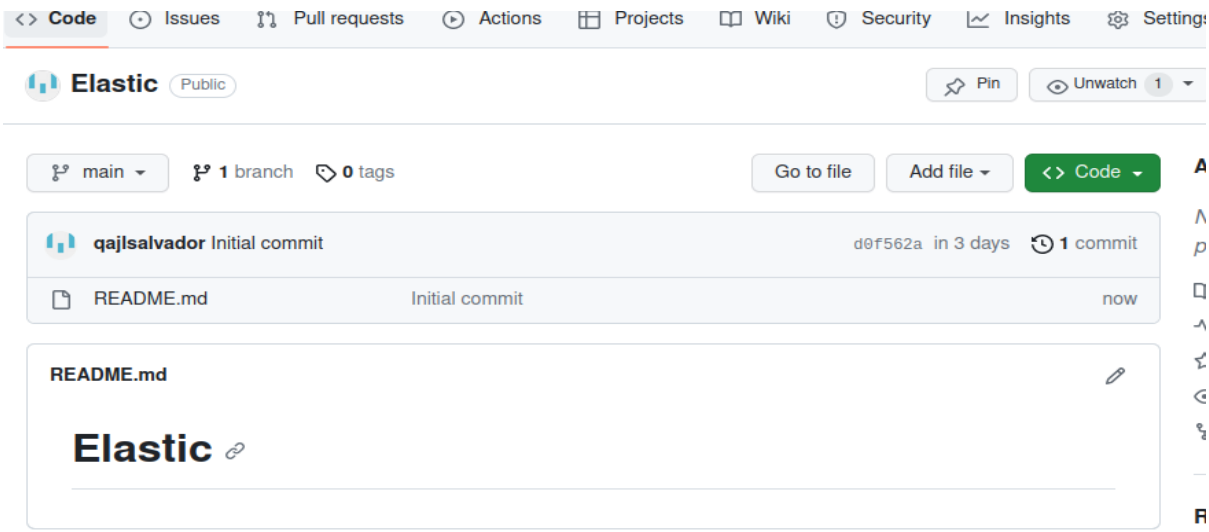
Source: https://www.graylog.org/products/open-source

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: Creating the repository

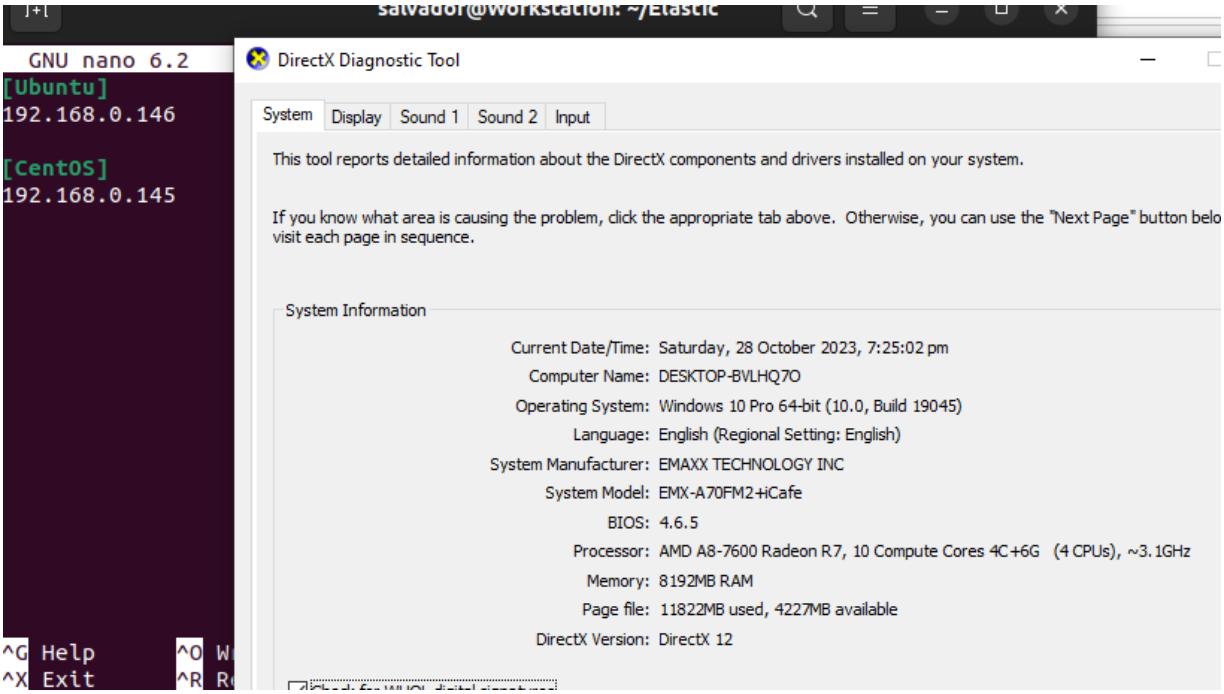


Create the repository where we will put our playbook later.

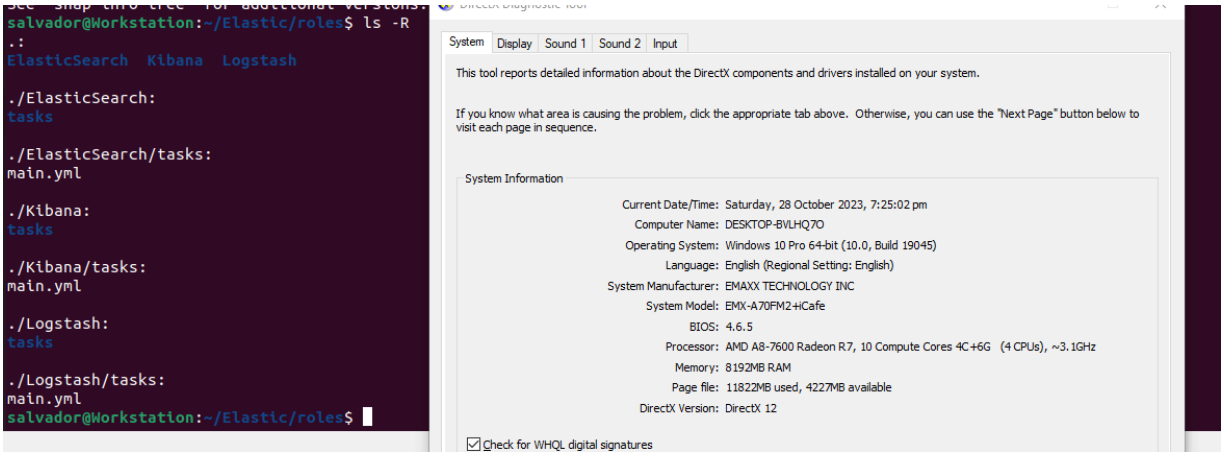
```
salvador@Workstation:~$ git clone git@github.com:qajlsalvador/Elastic.git
Cloning into 'Elastic'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
salvador@Workstation:~$ ls
ansible                 Elastic      nagios-ansible       snap
CPE232_AndreuSalvador   id_rsa       Pictures             Templates
Desktop                 id_rsa.pub   Prometheus           Videos
Documents               Music        Public
Downloads               Nagios       Salvador_PrelimExam
salvador@Workstation:~$ cd Elastic
salvador@Workstation:~/Elastic$
```

Part 2: Installing Elastic Stack on Ubuntu server

1. Create our inventory where we will put the ip address of our live servers and group them in their respective roles.

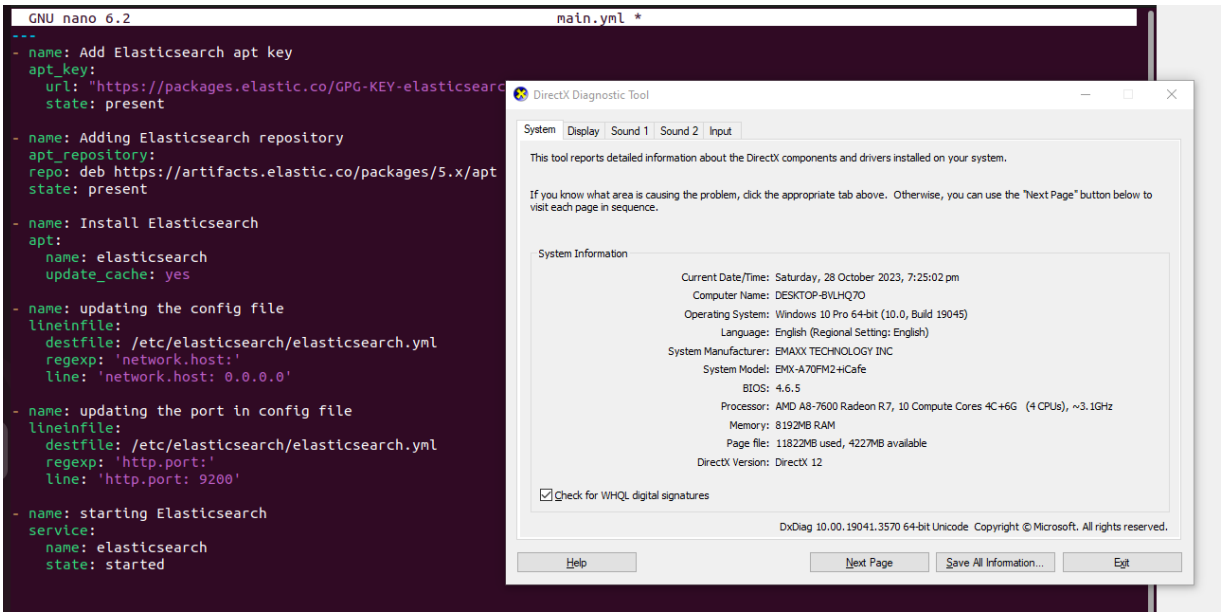


2. create roles directory and within the roles directory create the necessary roles for our Ubuntu server.



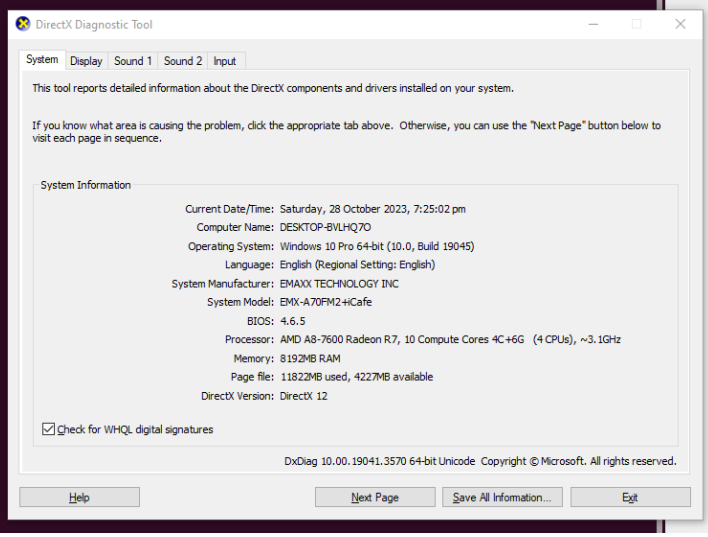
3. inside the roles, create a directory named tasks and inside the directory tasks create the .yml file as main.yml, lastly put the necessary tasks inside the .yml file.

ElasticSearch:

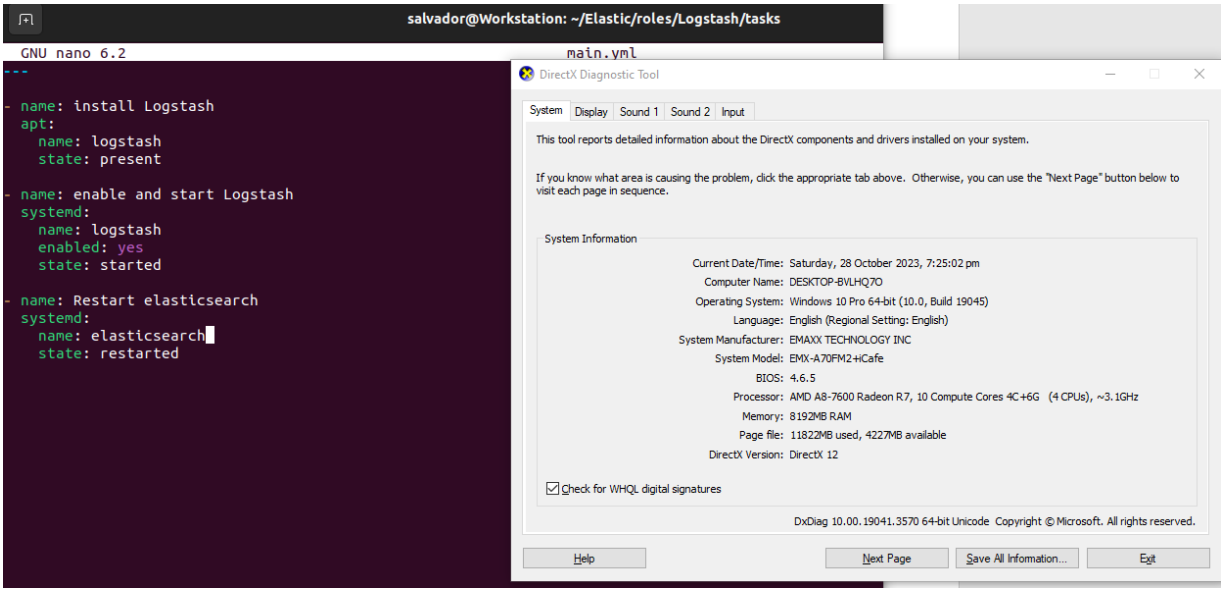


Kibana:

```
---

- name: Install with apt
  apt:
    name: kibana
    update_cache: yes

- name: Updating the config file
  lineinfile:
    destfile: /etc/kibana/kibana.yml
    regexp: 'server.host'
    line: 'server.host: 0.0.0.0'

- name: defining server port
  lineinfile:
    destfile: /etc/kibana/kibana.yml
    regexp: 'server.port: 5601'

- name: defining elasticsearch url
  lineinfile:
    destfile: /etc/kibana/kibana.yml
    regexp: 'elasticsearch.url:'
    line: 'elasticsearch.url: "http://localhost:9200"'

- name: starting kibana
  service:
    name: kibana
    state: started
```

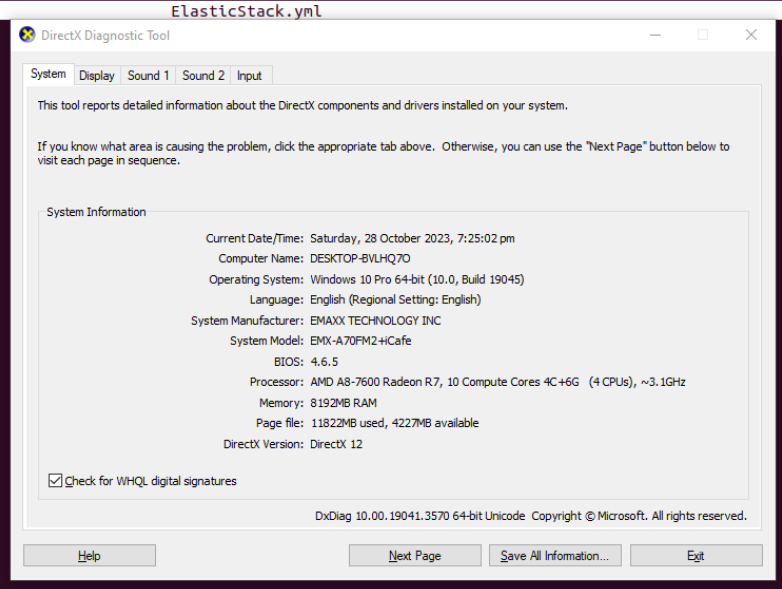


Logstash:



4. Create the main yml file to play the tasks.

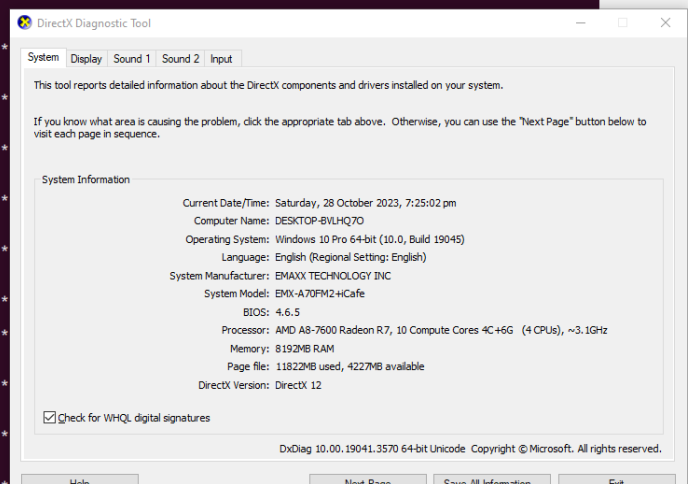
```
GNU nano 6.2                                   ElasticStack.yml
---
- hosts: all
  become: yes
  pre_tasks:

  - name: update APT cache Ubuntu
    apt:
      update_cache: yes
    when: ansible_distribution == "Ubuntu"

- hosts: Ubuntu
  become: true
  roles:
    - ElasticSearch

- hosts: Ubuntu
  become: true
  roles:
    - Kibana

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




```
[ Wrote 25 lines ]
```

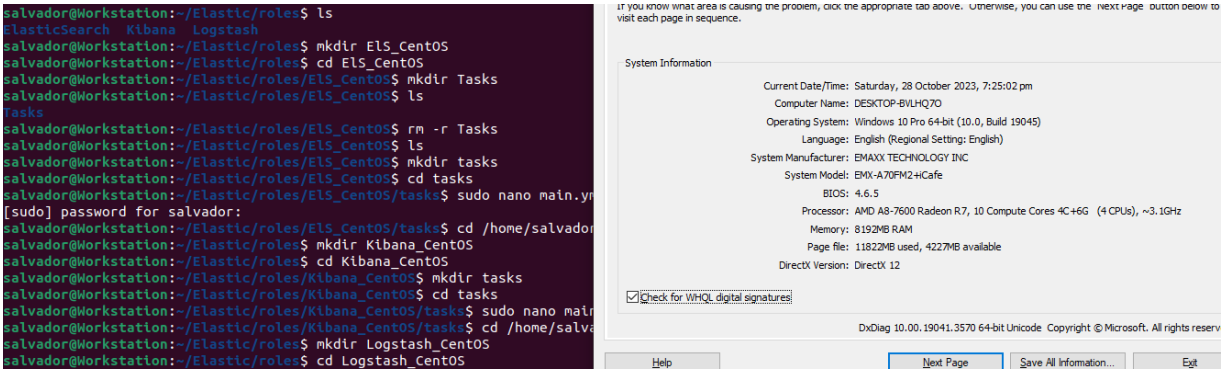
5. Run the playbook

```
TASK [Gathering Facts] ***********************************************************************************************
ok: [192.168.0.146]

TASK [Kibana : Install with apt] *******************************
ok: [192.168.0.146]

TASK [Kibana : Updating the config file] ***********************
ok: [192.168.0.146]

TASK [Kibana : defining server port] ***************************
ok: [192.168.0.146]

TASK [Kibana : defining elasticsearch url] *********************
ok: [192.168.0.146]

TASK [Kibana : starting kibana] ********************************
ok: [192.168.0.146]

PLAY [Ubuntu] ****************************************************

TASK [Gathering Facts] *******************************************
ok: [192.168.0.146]

TASK [Logstash : install Logstash] *****************************
ok: [192.168.0.146]

TASK [Logstash : Restart elasticsearch] ************************
changed: [192.168.0.146]

PLAY RECAP *******************************************************
192.168.0.145              : ok=0    changed=0    unreachable=1
192.168.0.146              : ok=18   changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

salvador@Workstation:~/Elastic$
```



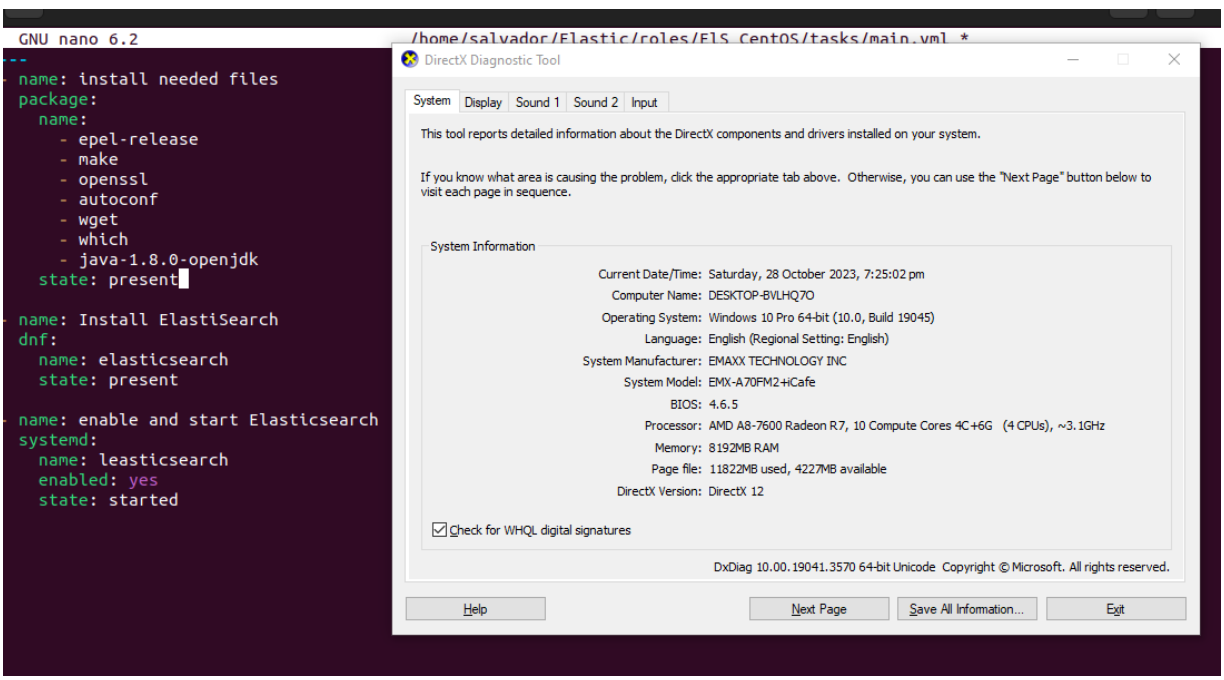
Part 3: Installing Elastic Search on CentOS

1. Create the necessary roles in installing the ElasticStack on CentOS

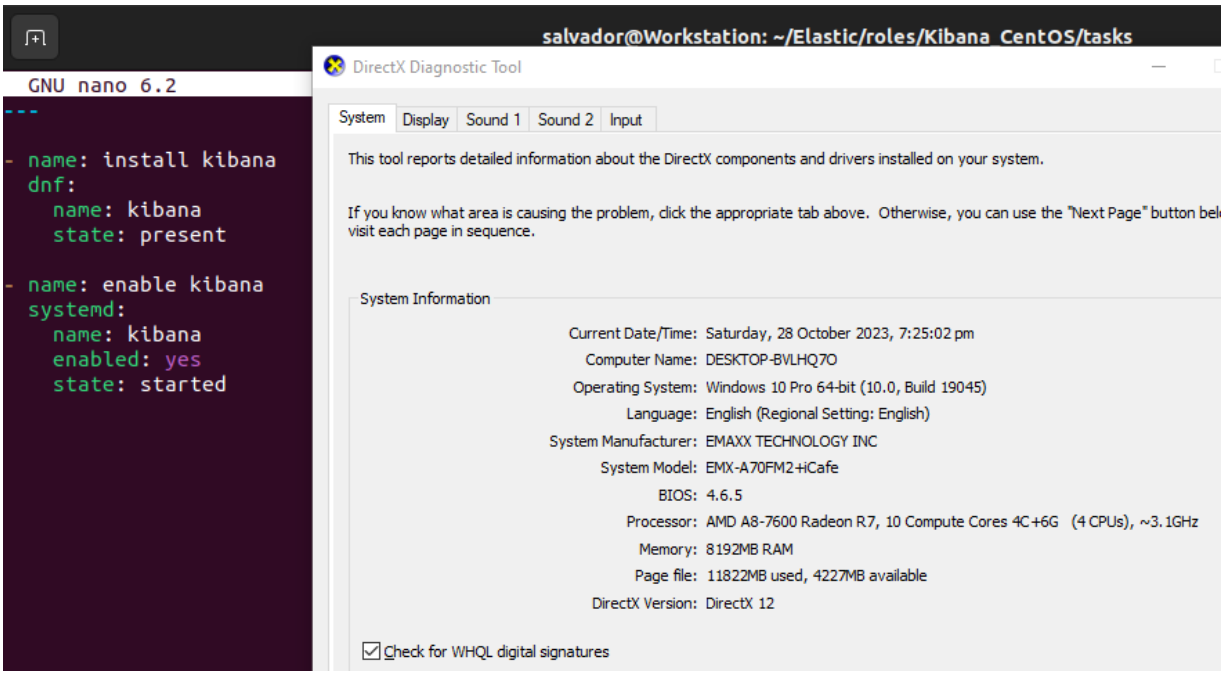


2. Just like on the part 2 inside the roles, create a directory named tasks and inside the directory tasks create the .yml file as main.yml, lastly put the necessary tasks inside the .yml file.

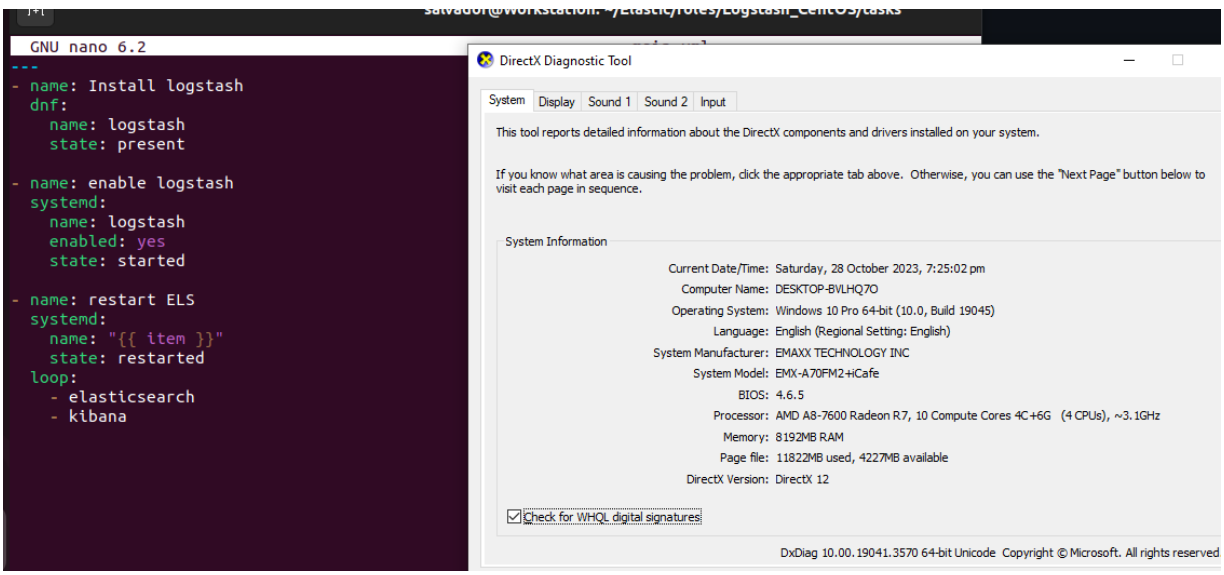
ElasticSearch:



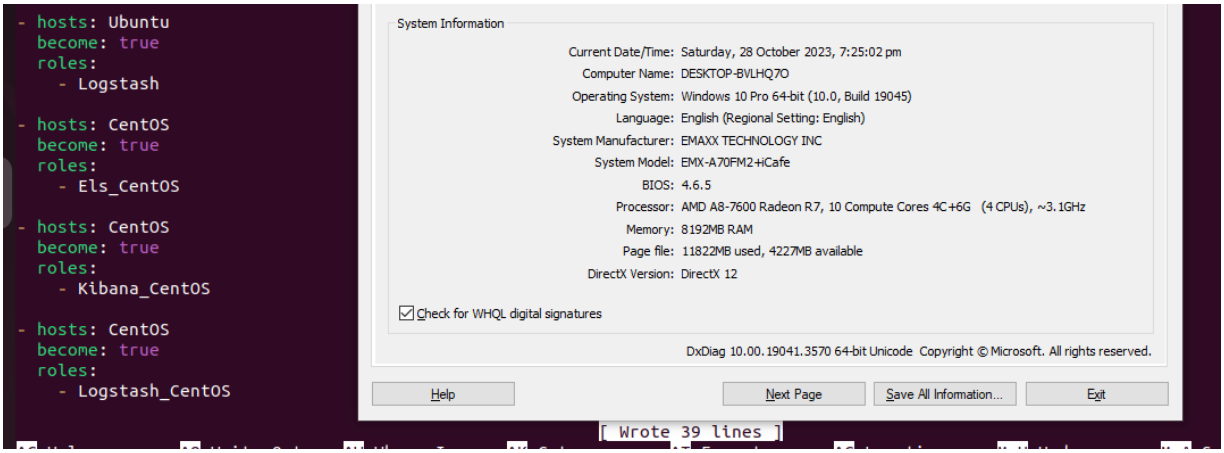
Kibana:



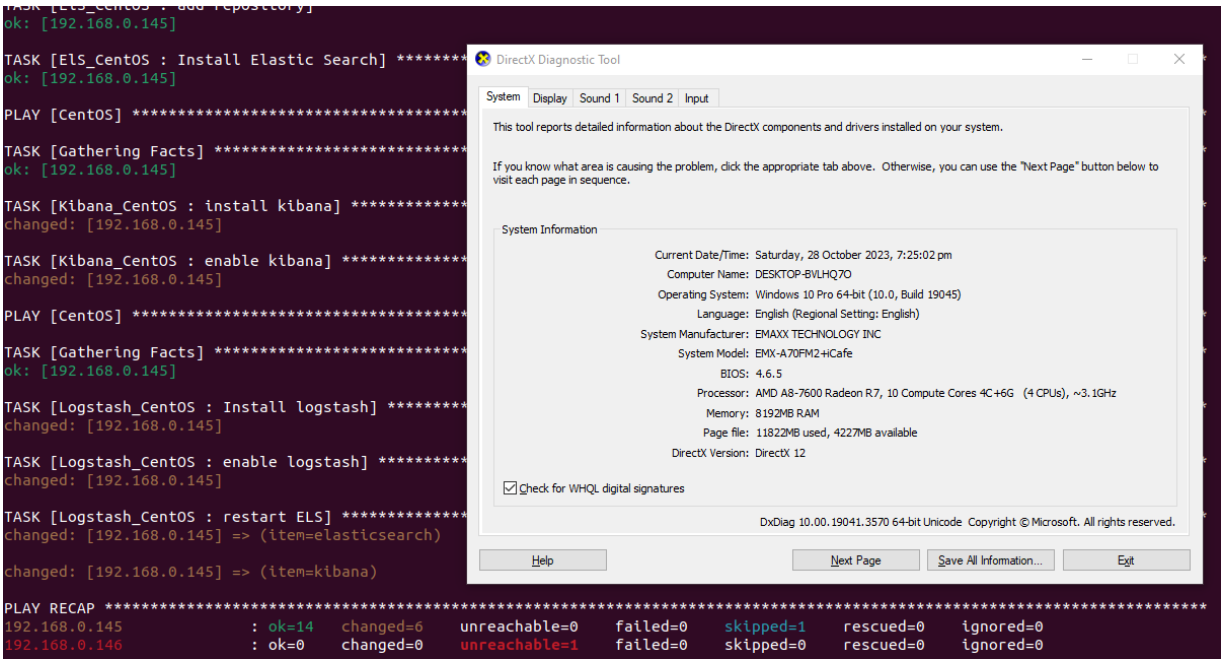
Logstash:



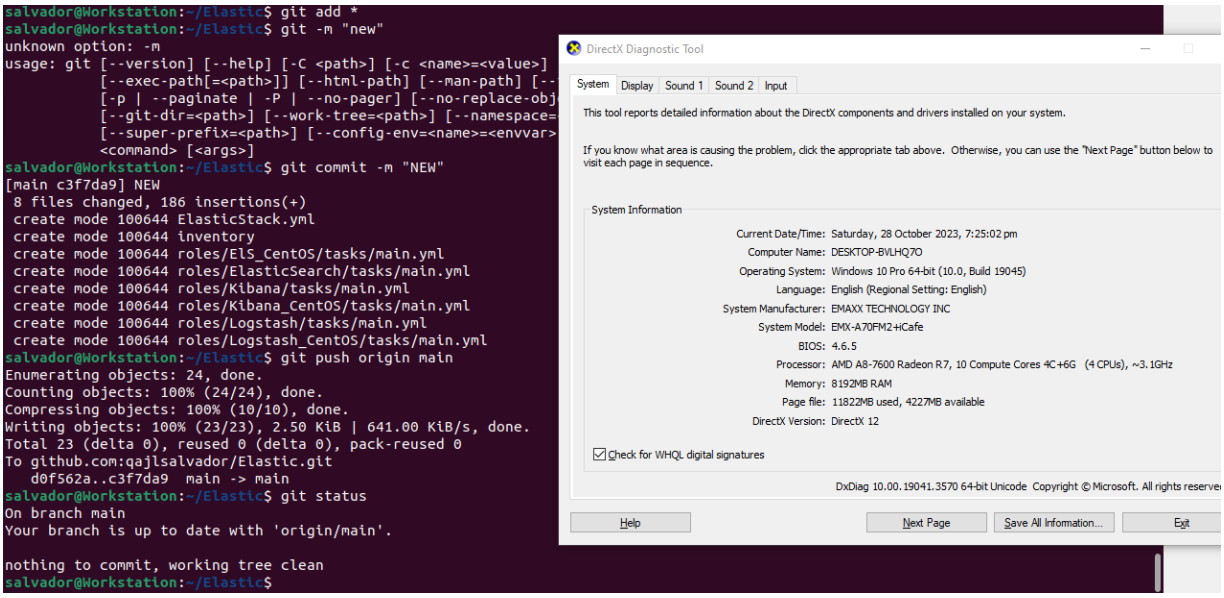
3. Add the roles inside the main ElasticStack .yml file in order to play it in the playbook.



4. Run the Playbook



Part 5: adding everything to github



Reflections:

Answer the following:

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

Its importance is akin to what security cameras are for. Logs monitoring tools are important to use and to have since it helps the you monitor security issues that occurred in the system as well as helps you solve performance related problems.

Conclusions:

In installing the log monitoring tool there are thing that you should keep in mind; first is what monitoring tool you need, second what does it do, and etc. In the activity it let us install the log monitoring tool called Elastic stack, this tool is made up of software such as the Elastic Searc, Kibana, beats, and Logstash. These are necessary in building the monitoring tool. I've used the function of roles in creating an ansible playbook to further assimilate and made it easy to debug problems since the used of the roles is to lessen the burden for you when finding the error when playing the playbook. Creating roles for both the Ubuntu and CentOS server was a challenge since the code for the two are not that easy to write. In the end the installation was a success and the goal was achieved which is installing the Monitoring tool in both servers using the Playbook.