Name: Karlo Santos	Date Performed:10/27/23
Course/Section: CPE31S5/CPE232	Date Submitted: 10/28/23
Instructor: Engr. Roman Richard	Semester and SY: 1st sem SY 23-24

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.

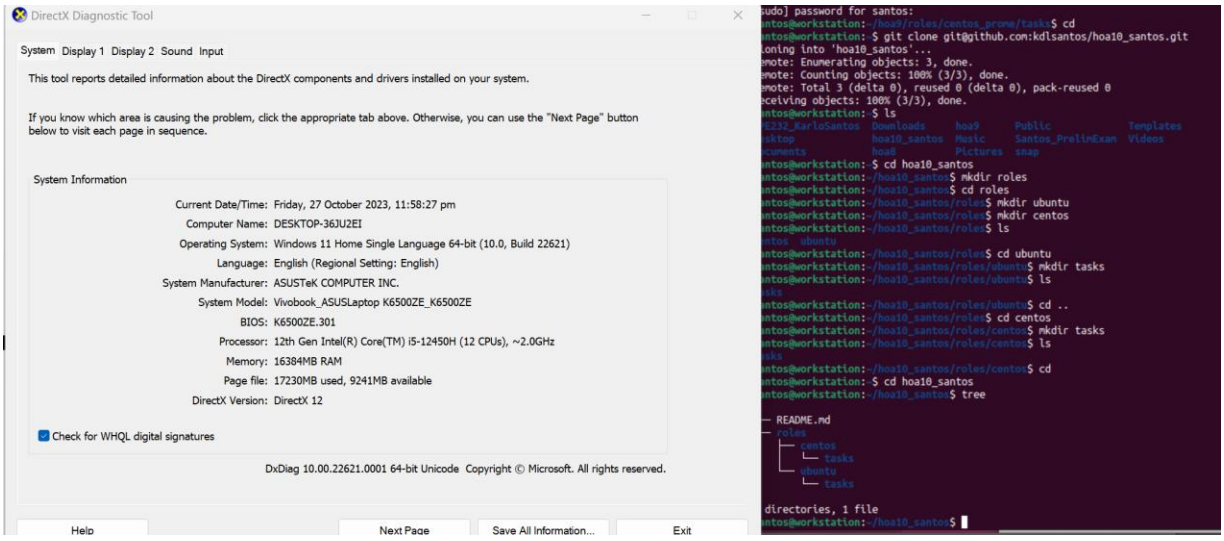
Source: https://www.graylog.org/products/open-source

3. Tasks

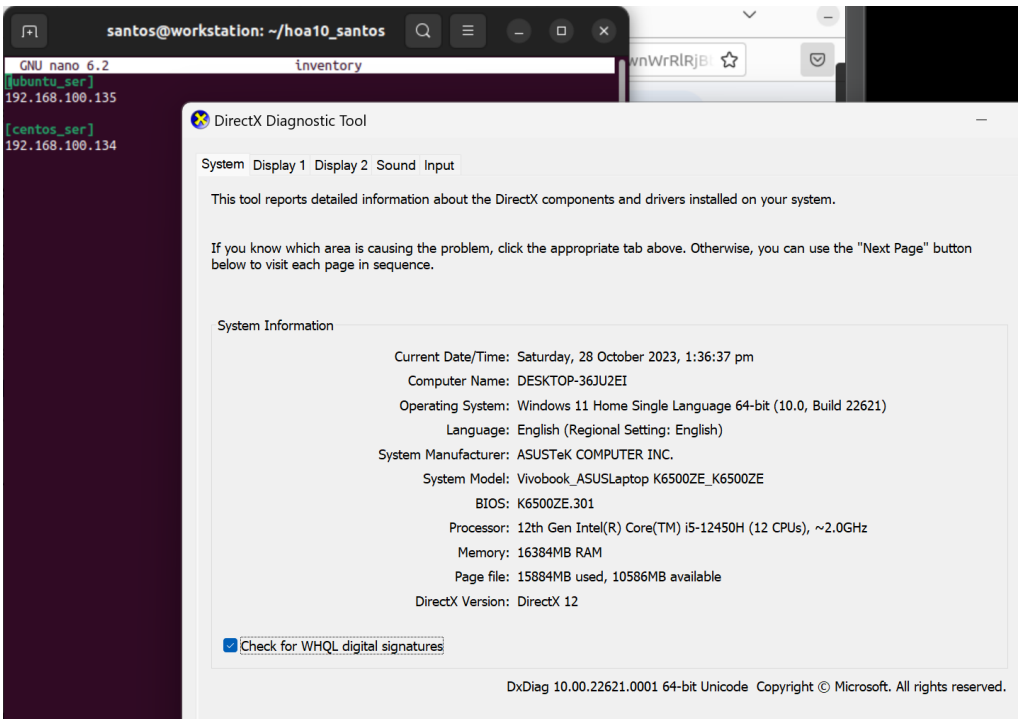
1. Create a playbook that:
    a. Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)
2. Apply the concept of creating roles.
3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like 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)

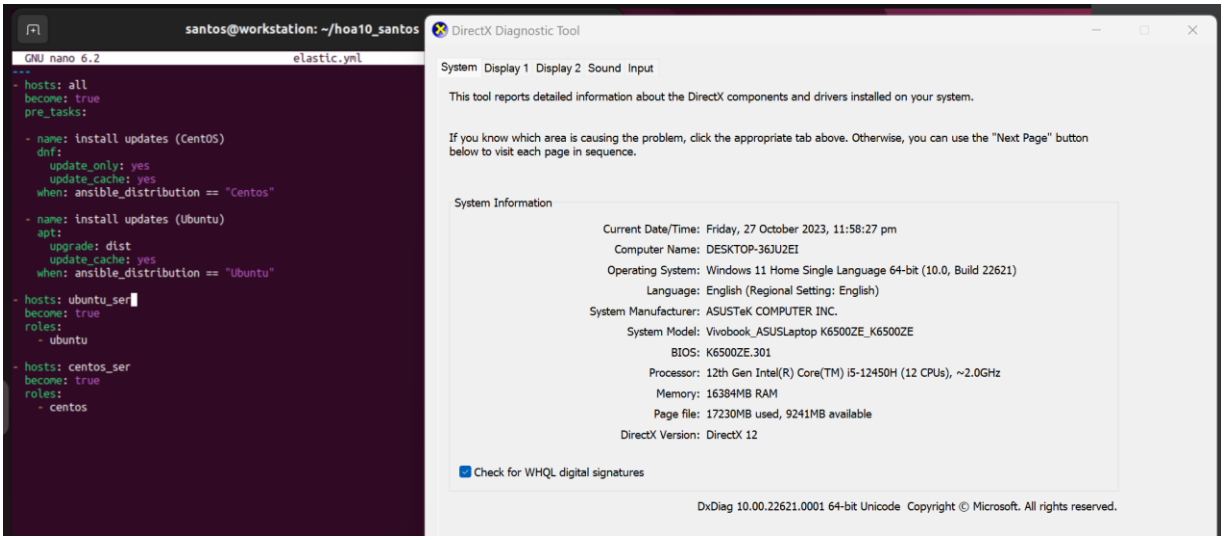
Create a playbook



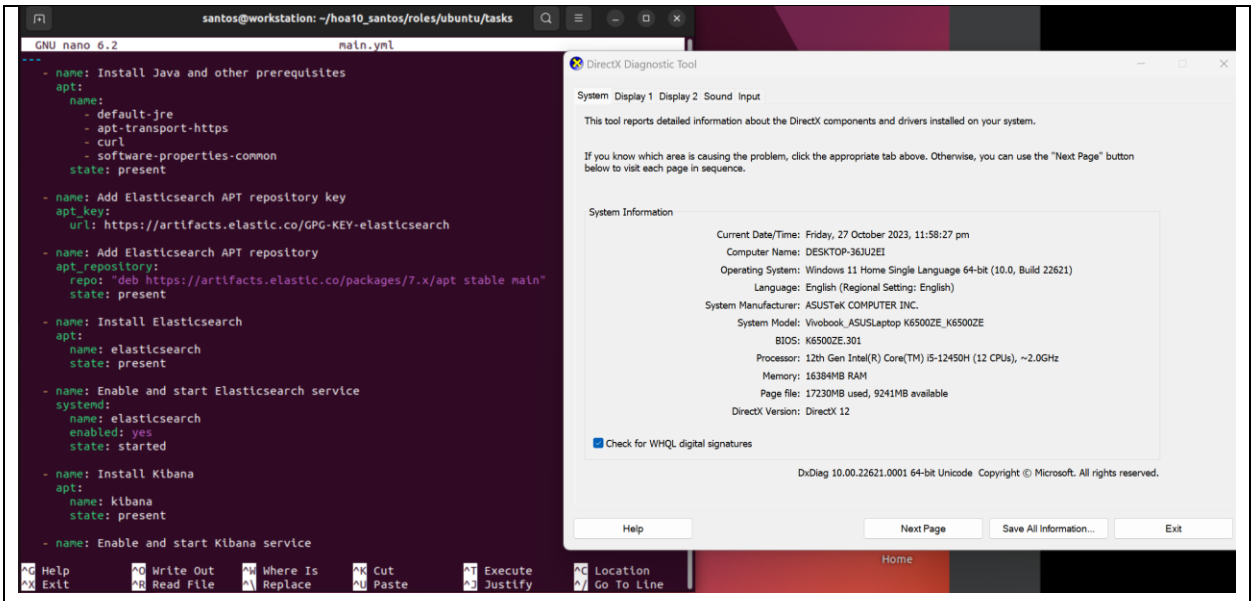
First, I clone the repository that I made in GitHub and make a directory that is needed for this activity. I made a roles directory where it contains the directory for ubuntu and centos server.



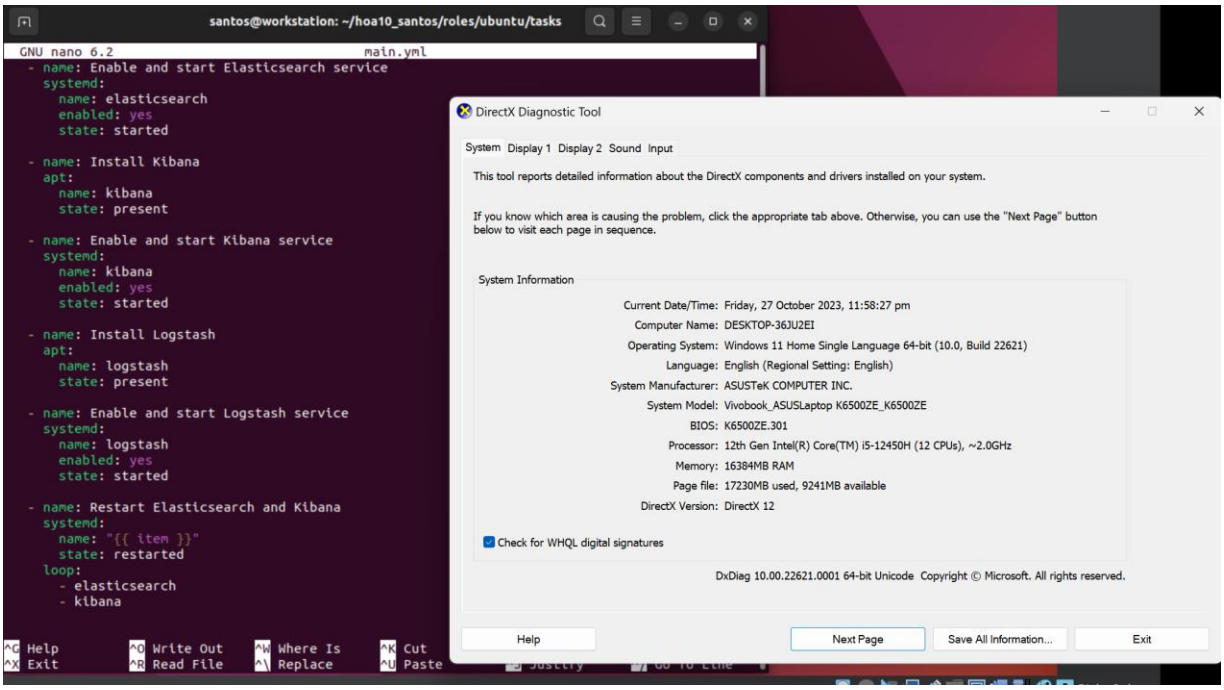
After that I made an inventory files where it contain all the ip address for ubuntu and centos server.



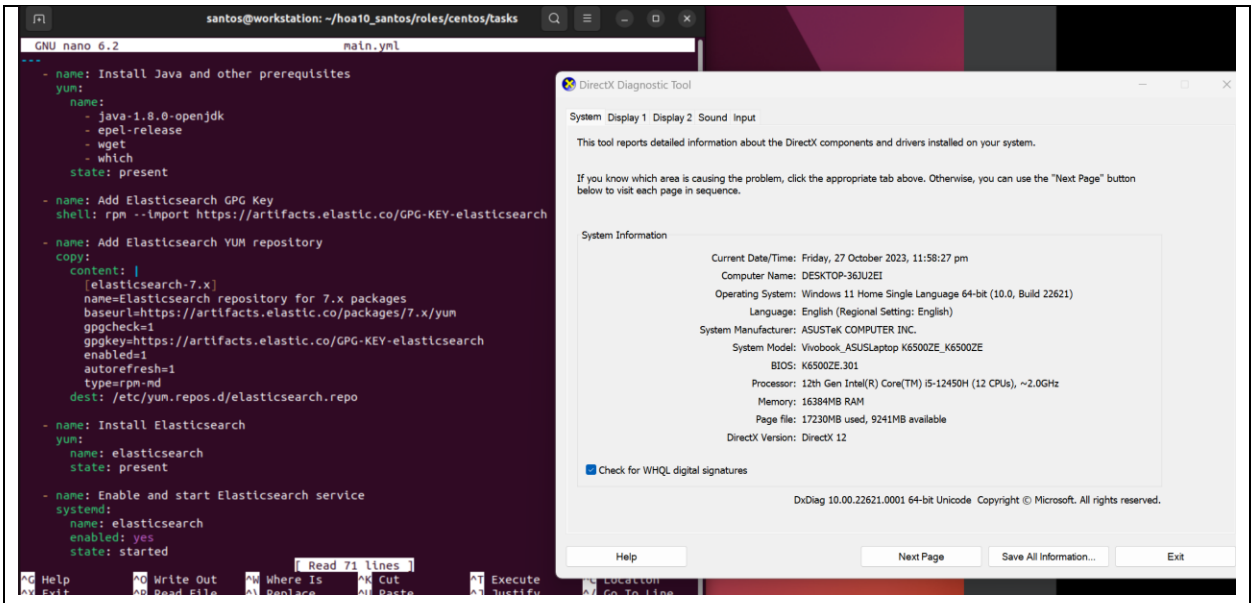
Next, I made a yml file that named elastic.yml. It contains a pre-tasks where it will make an updare in the servers in the inventory. Then, it will call the tasks for ubuntu and centos that is inside of the roles directory.



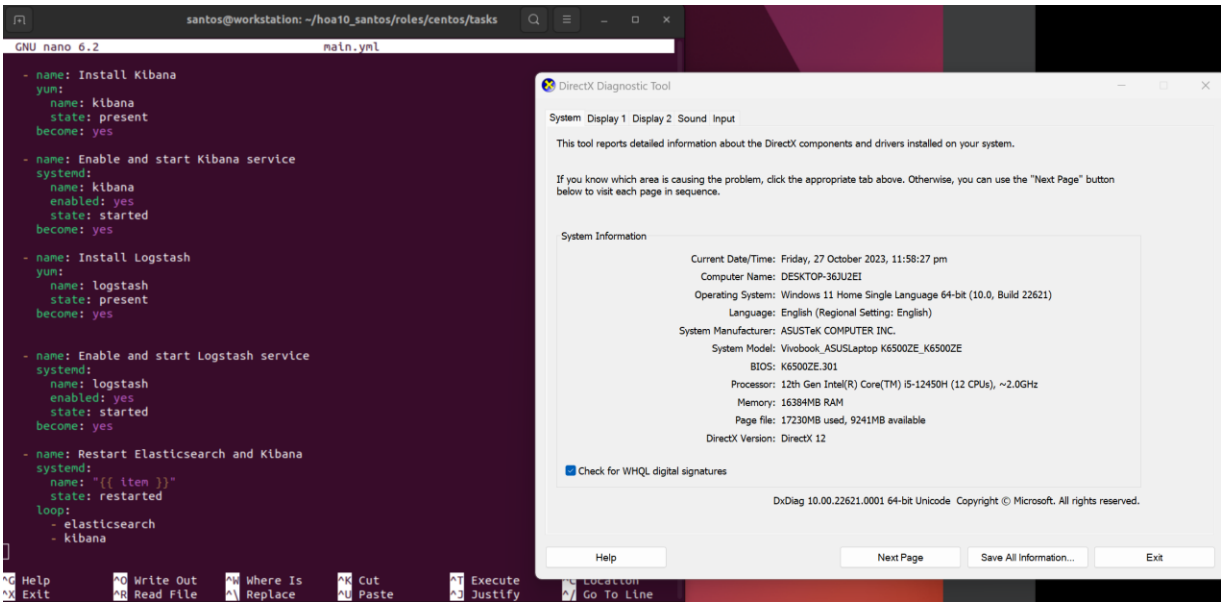
Inside of ubuntu roles, I made a tasks directory where I put the main.yml file fo the different task for ubuntu. The first task is for the installation of java and other prerequisites that is needed for Elasticsearch. Then the next is for adding Elasticsearch apt repository key and it will follow by installation of Elasticsearch. After that it will enable and start Elasticsearch, then it will proceed in installing Kibana.



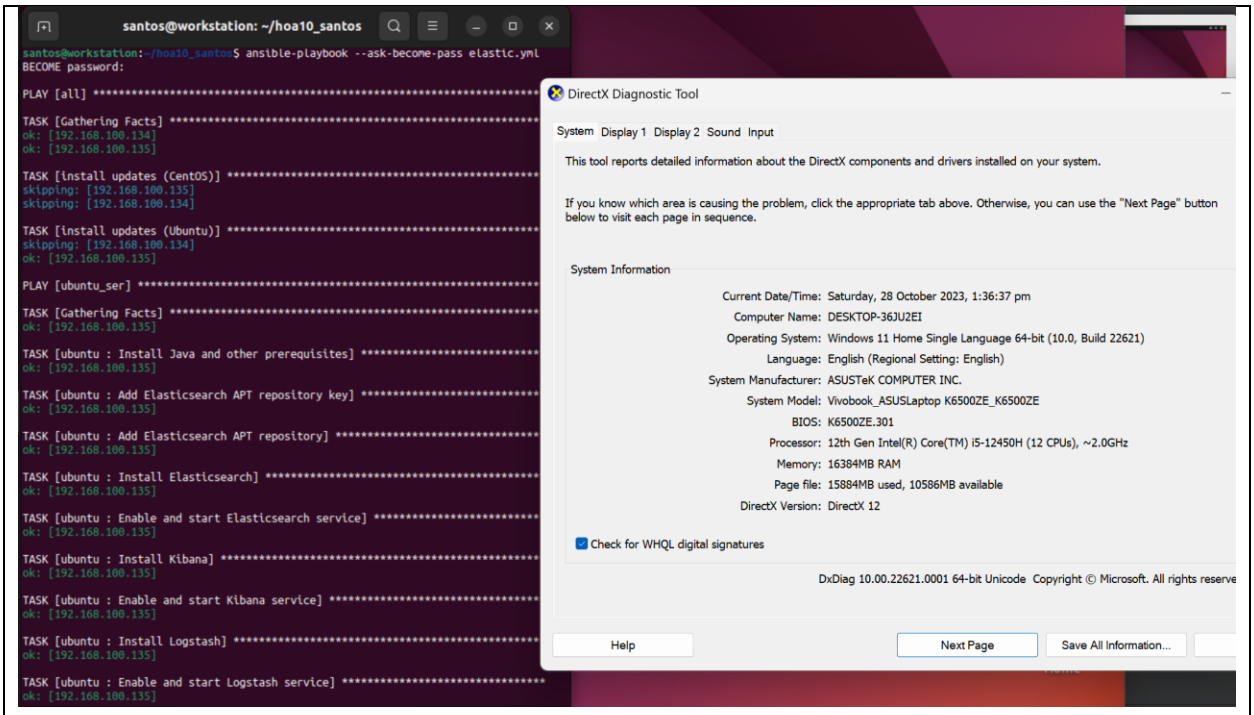
Next, it will enable and start the Kibana. After that it will install the Logstash and proceed in enabling it and start the service. Lastly it will restart the Elasticsearch and Kibana since some files need to have restart to completely start.

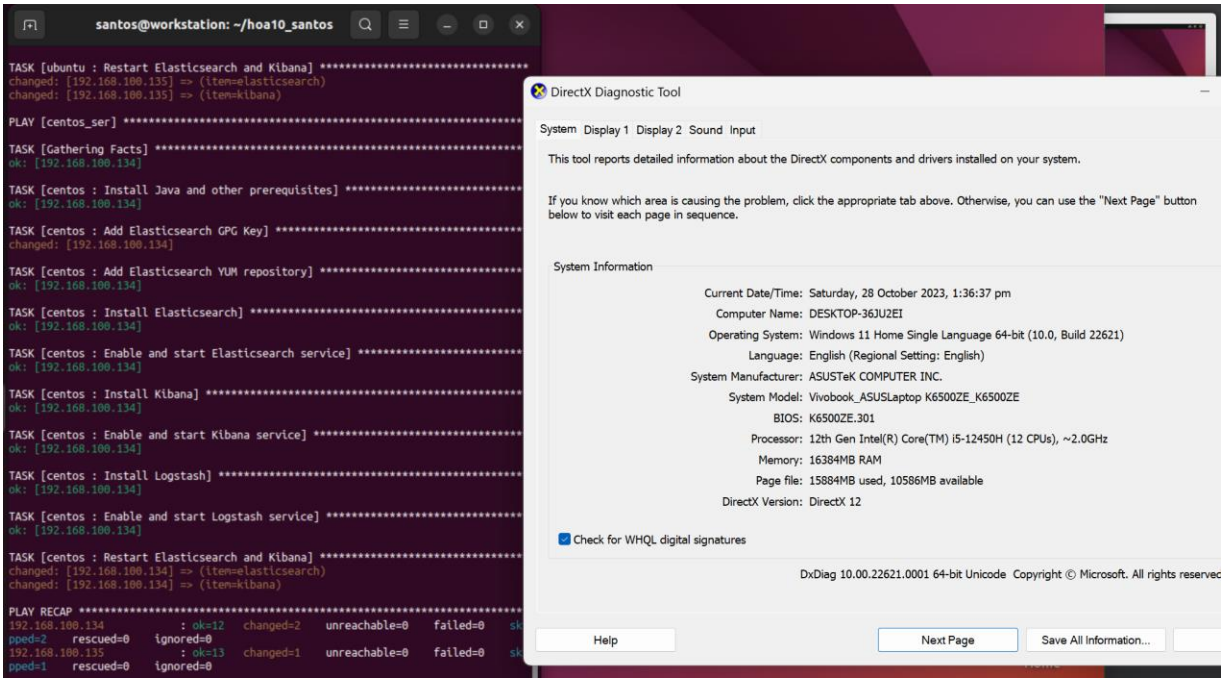


This is the main.yml for centos. It is similar to the content for the ubuntu server. It contains the installation of prerequisites, and proceed in installation of Elasticsearch. Then it will install the Kibana and enable it.



Lastly it will install the Logstash and enable and start it also. I also put a task to restart the Elasticsearch and Kibana.

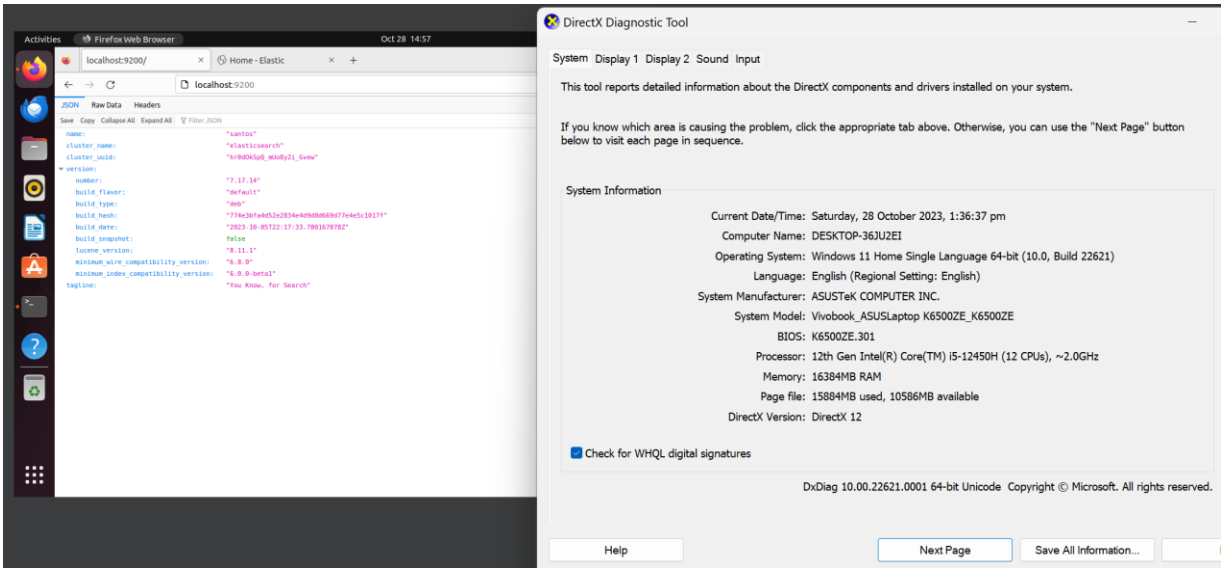




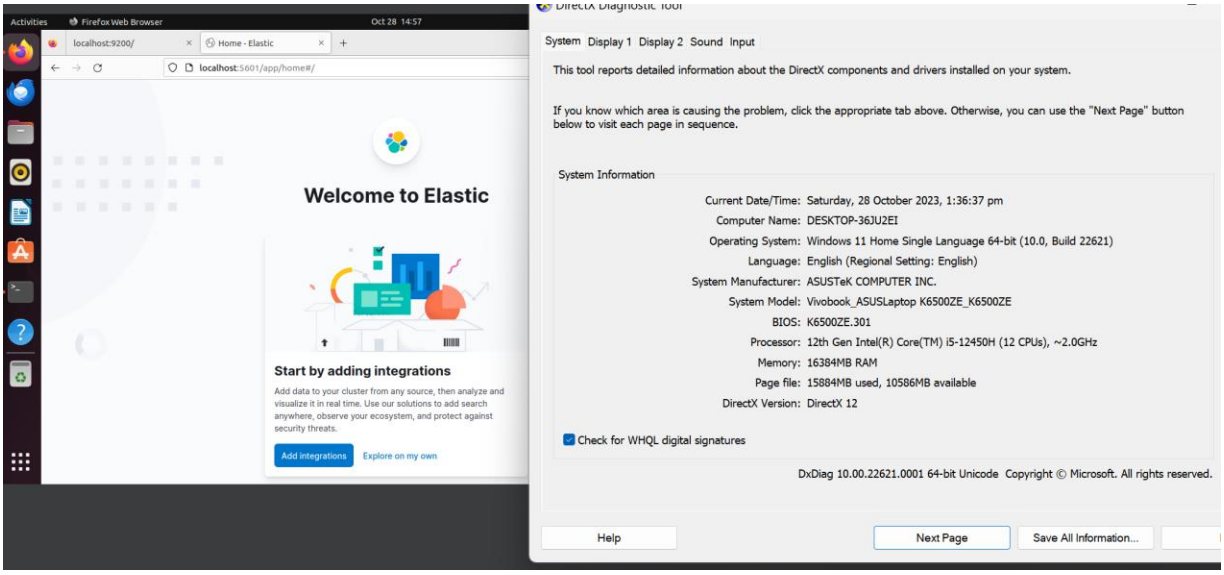
This is the screenshot of the results after I run the playbook. As you can see it shows that all the task are okay and execute well. It also shows ok and changed so it means that the code work and it just need to verify it in checking.

CentOS server

Elasticsearch (use “localhost:9200”)

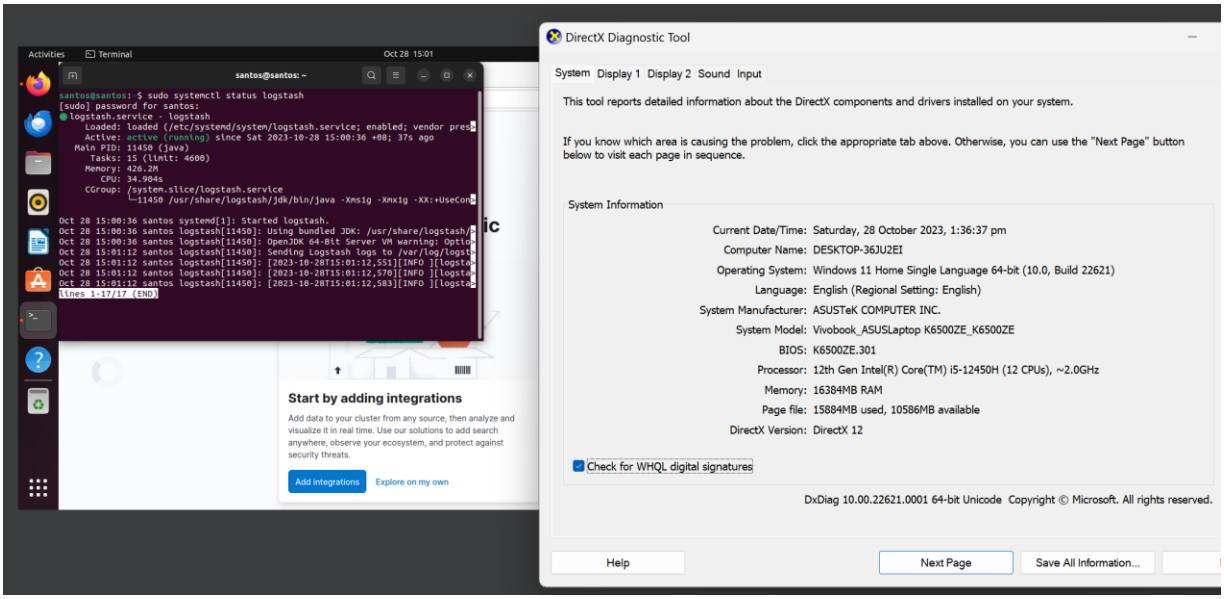


Kibana(use “localhost:5601”)



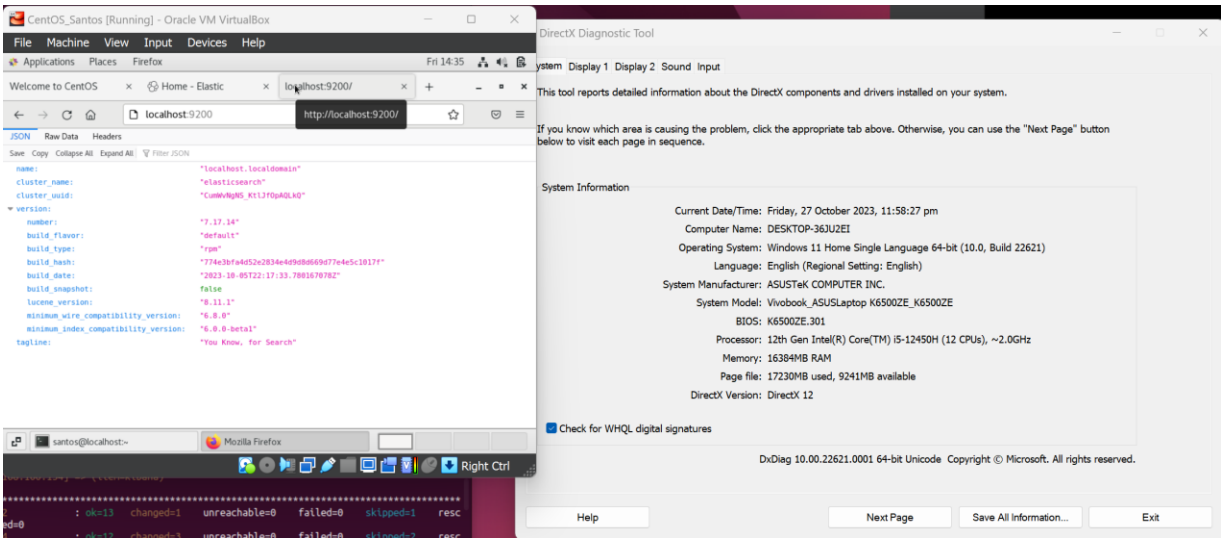
Logstash

I used systemctl status logstash to check if it active and running.

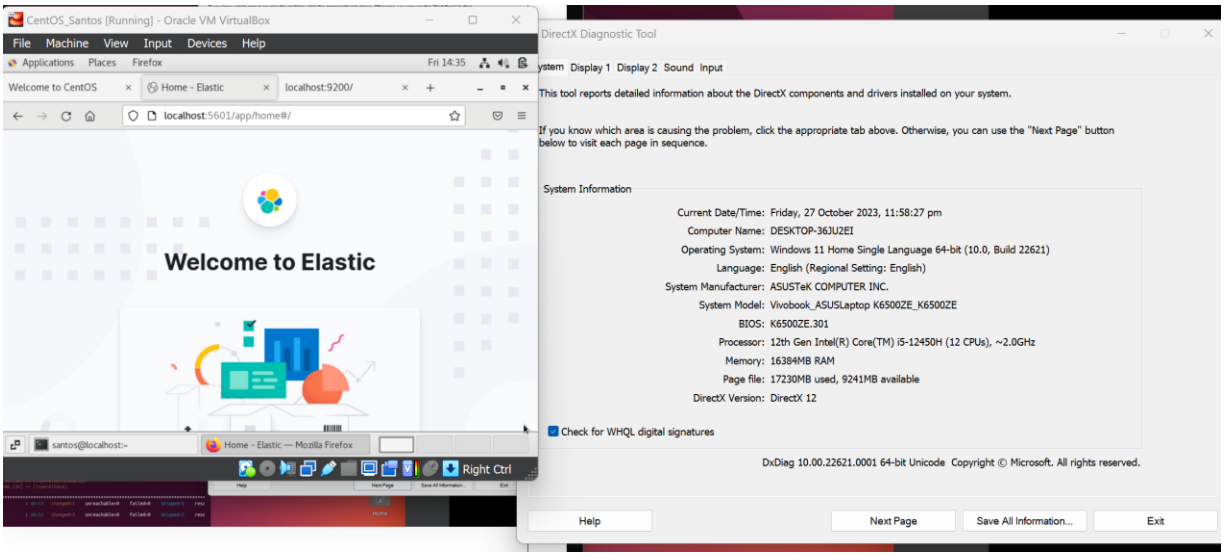


Ubuntu Server

Elasticsearch (use “localhost:9200”)

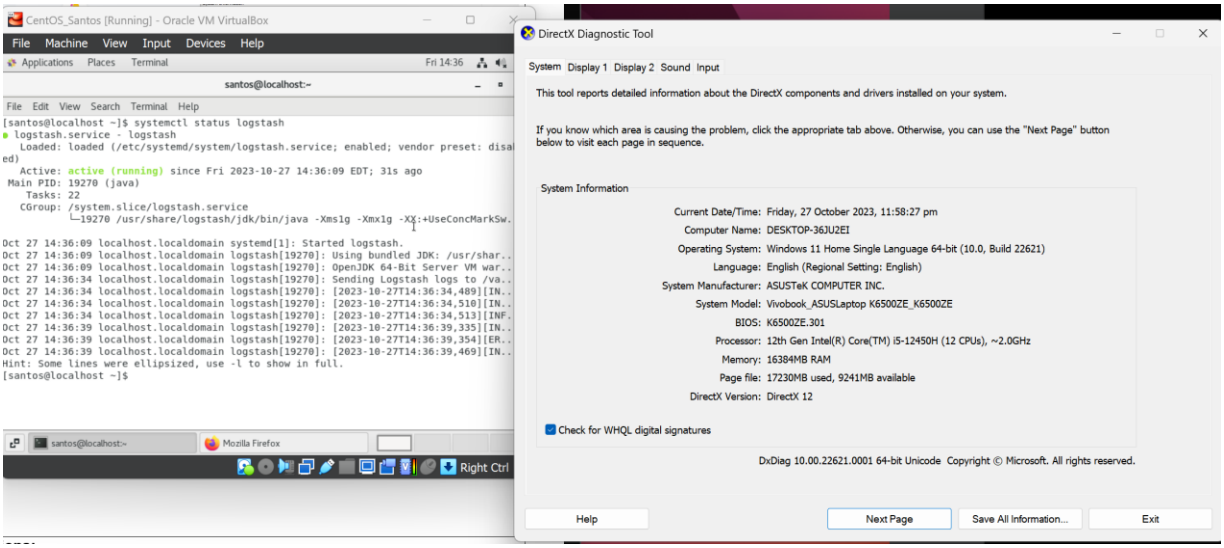


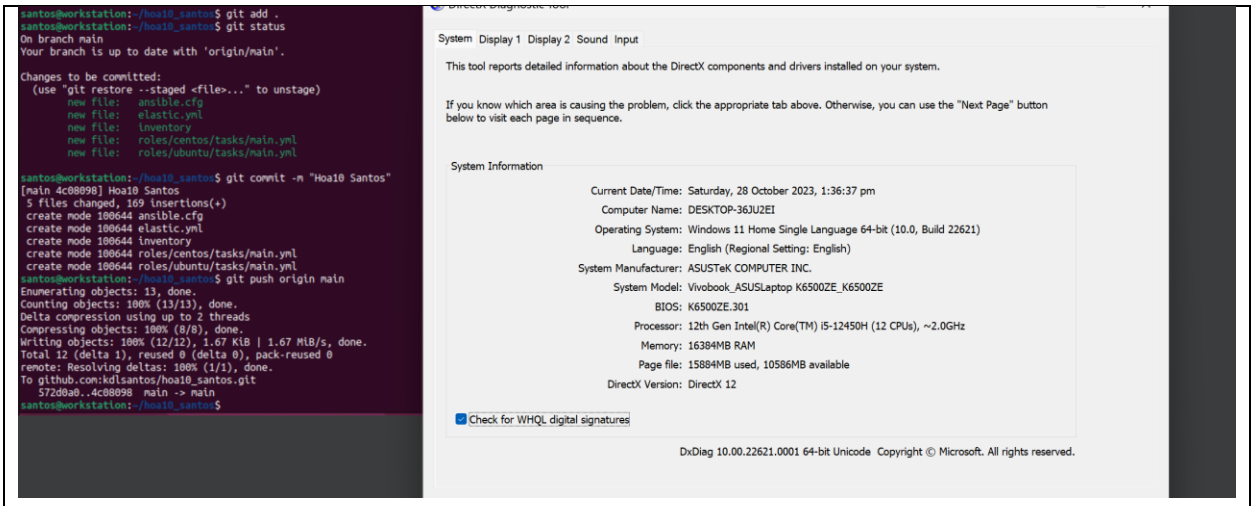
Kibana(use “localhost:5601”)



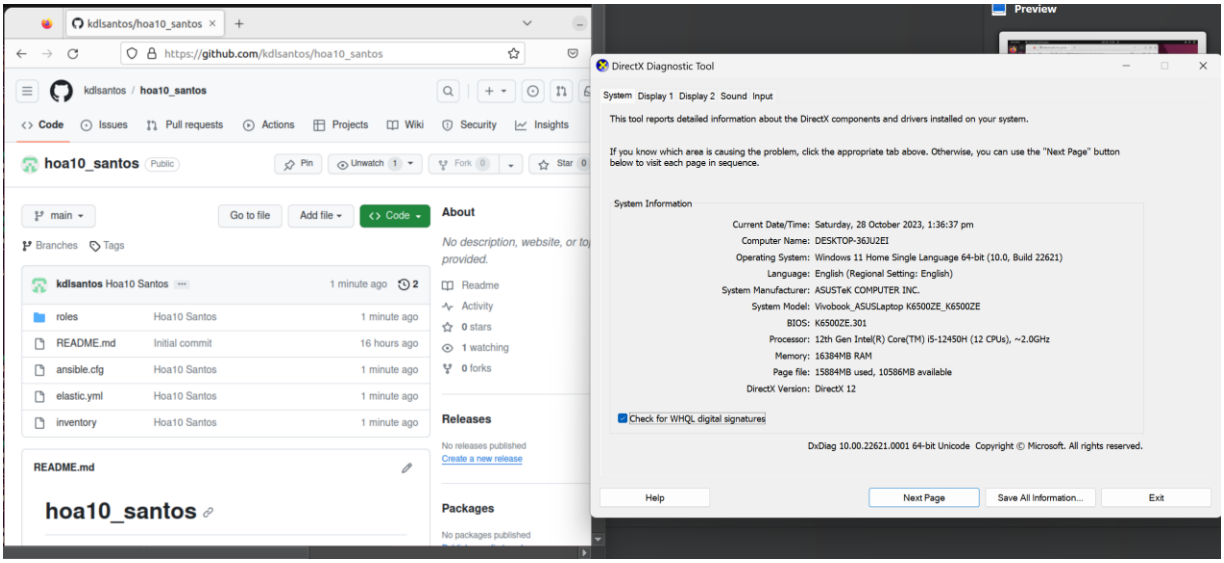
Logstash

I used systemctl status logstash to check if it active and running.





After I verify the all is working and actively running, I update and put all the things I do in my GitHub repository. I use git add . and make a comment using git commit -m. Then use the git push origin main.



GitHub link:

https://github.com/kdlsantos/hoa10_santos

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool?
   - **Using the log monitoring tools help a lot in maintaining the system health. One of its benefits is having a real-time problem detection, since it will**

continuously check and analyze the different log files so it can easily detect the issue right away. That will result in making troubleshooting and debugging much easier since you already have the different data that will help you to solve the problem. Another one is it help in security monitoring since log monitoring can detect and also alert the different unauthorized or threat in the system. We can say that log monitoring tool have gives a lot benefits in making sure that the system is healthy and make sure to that it is problem free.

Conclusions:

In this activity, it introduces a kind of enterprise log monitoring tools. It helps me to be able to create and configure a monitoring tool which is called elastic stack. It is consisting by ELK which means Elasticsearch, Logstash and Kibala. The it is connected to each other, since Logstash is the one that will receive and also filler the data that is from the servers. After that it will be stored in the Elasticsearch, based on that we can say that Elasticsearch is a kind of database. The content of it will be display in the Kibana. Also, in this activity I able to learn the importance and the different benefit that we can get using log monitoring system which it helps maintaining the health of the system. It helps to identify the problem right away, help in security and optimization of the system.