Name: Shaniah Rose Hope M. Sumaoang	Date Performed: October 26, 2023
Course/Section: CPE 232-CPE31S5	Date Submitted: October 26, 2023
Instructor: Engr. Roman Richard	Semester and SY: 1st Sem 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.

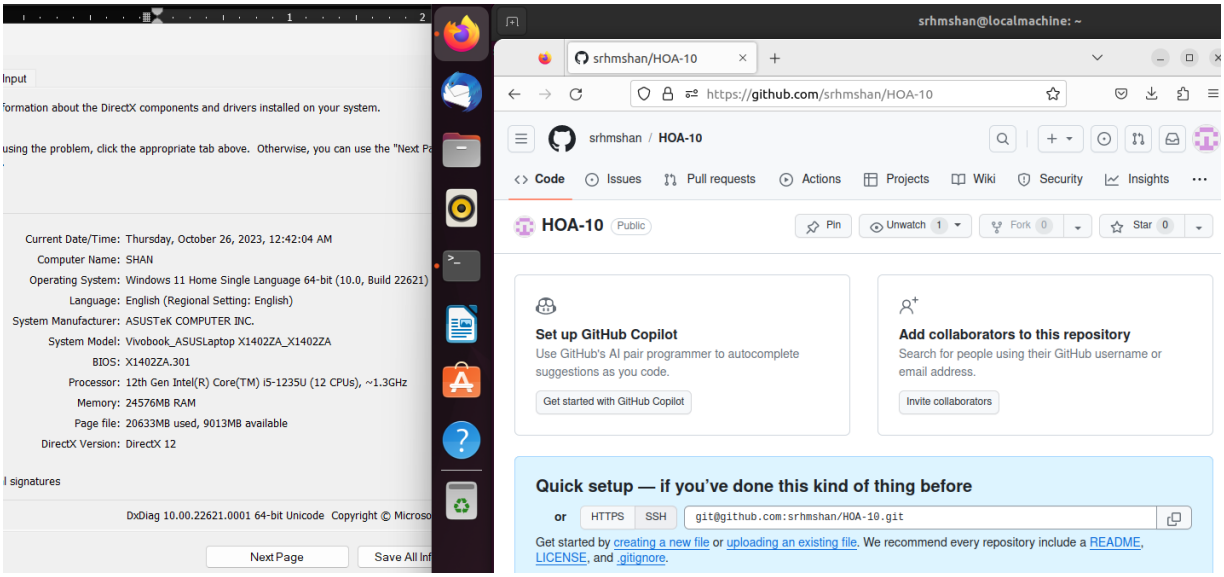
Source: https://www.graylog.org/products/open-source

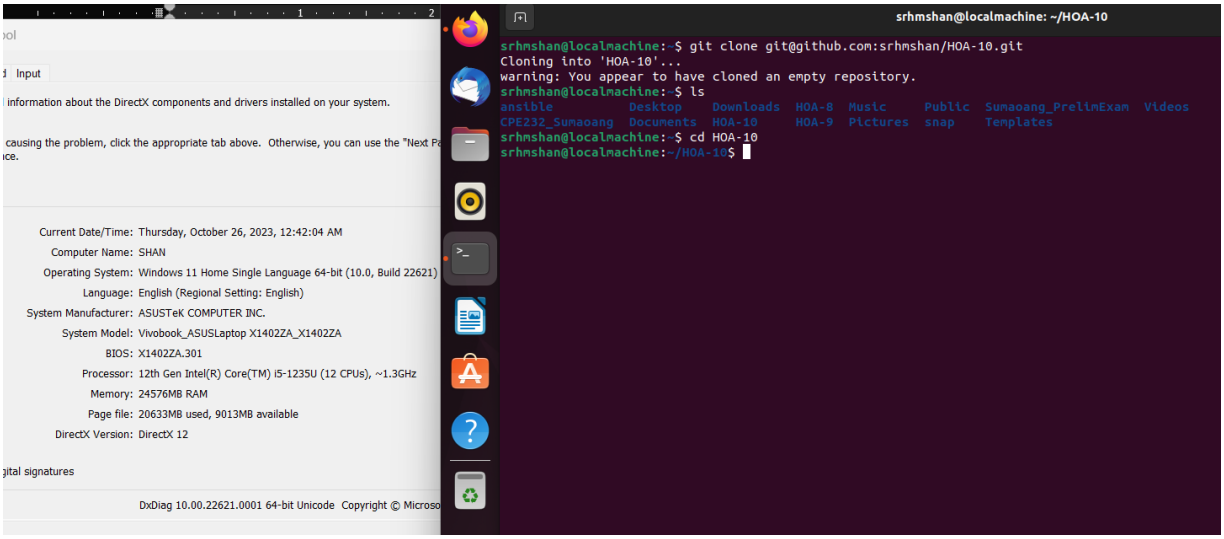
3. Tasks

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.

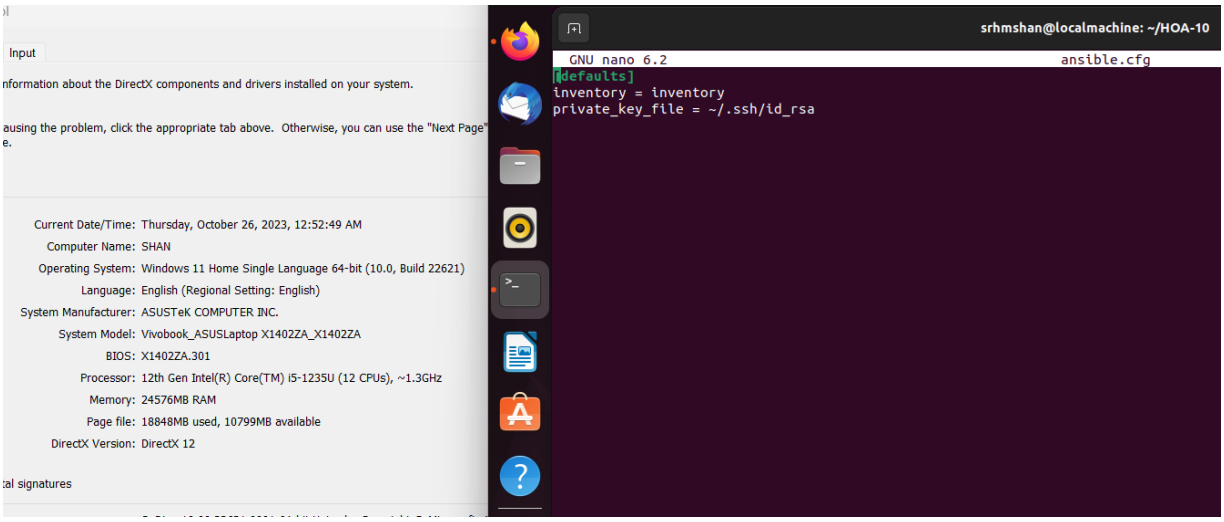
4. Output (screenshots and explanations)

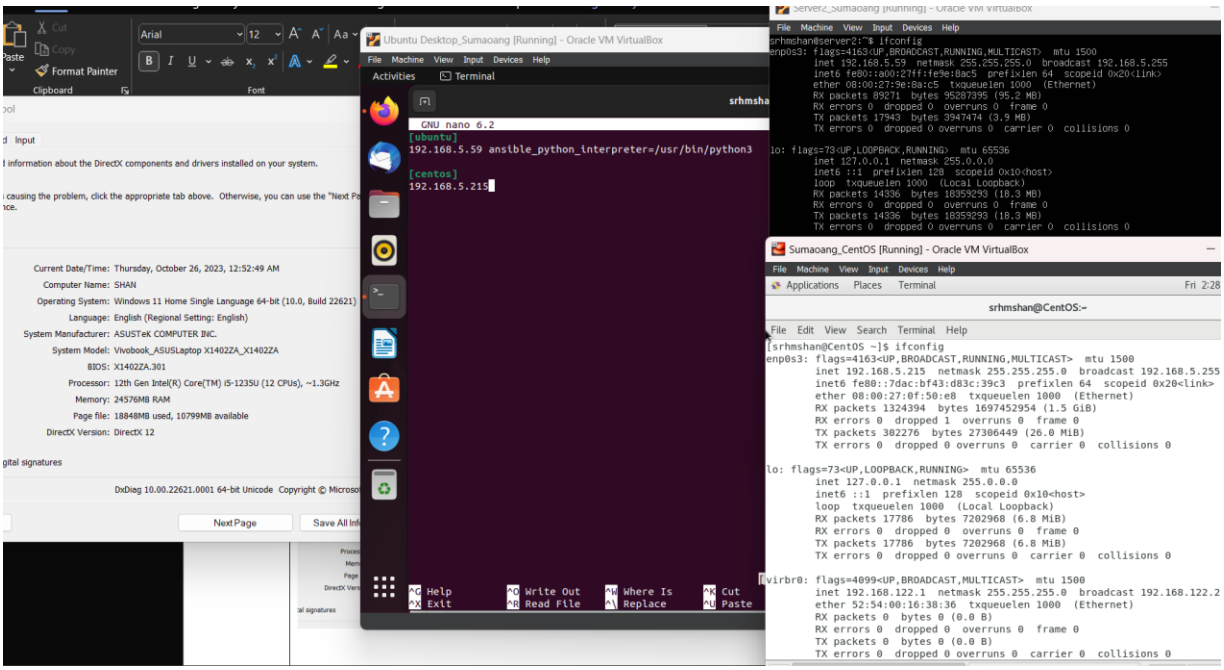
Step 1: Create a new repository in GitHub for this activity. Adding anything to it is optional. Next, copy your new repository in your CN using the code in the 2nd image.



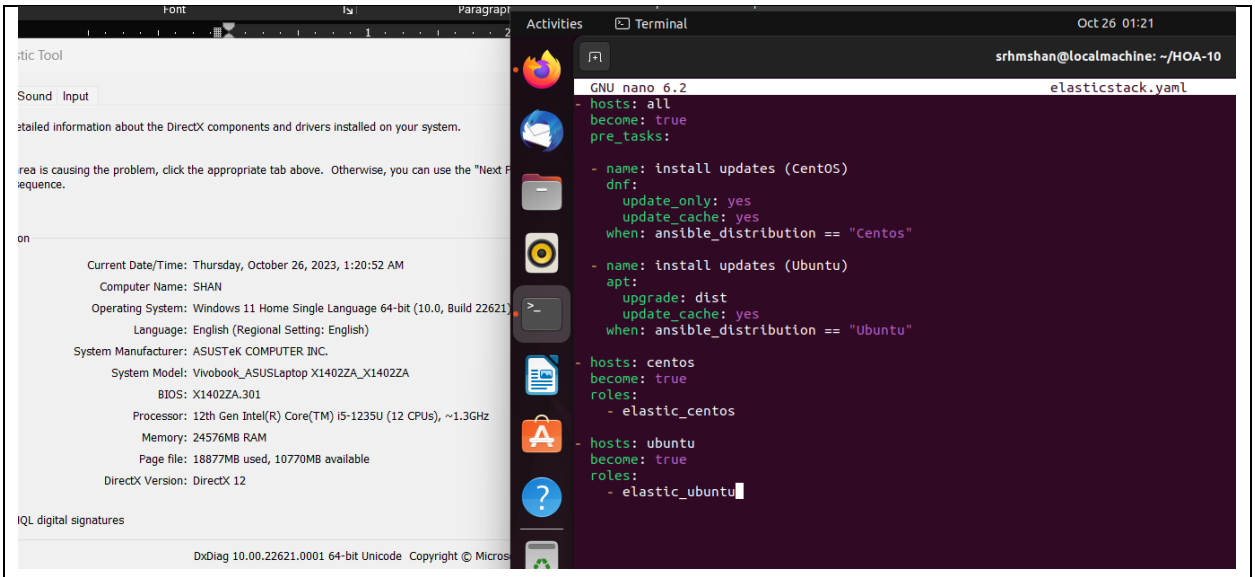


Step 2: Create your ansible.cfg and inventory files using the sudo nano command.



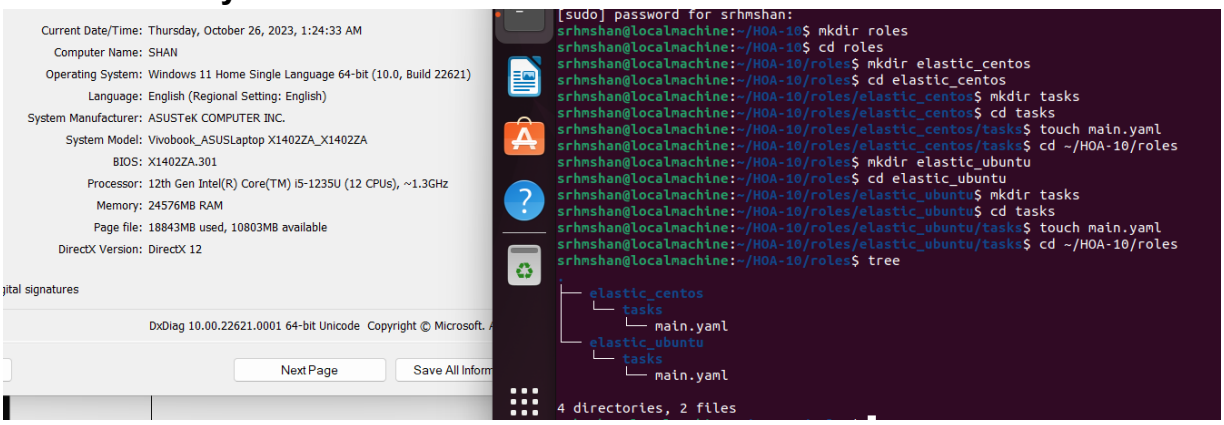


Step 3: Create an elasticstack.yaml file with the following tasks:



This is the main playbook wherein the roles are defined.

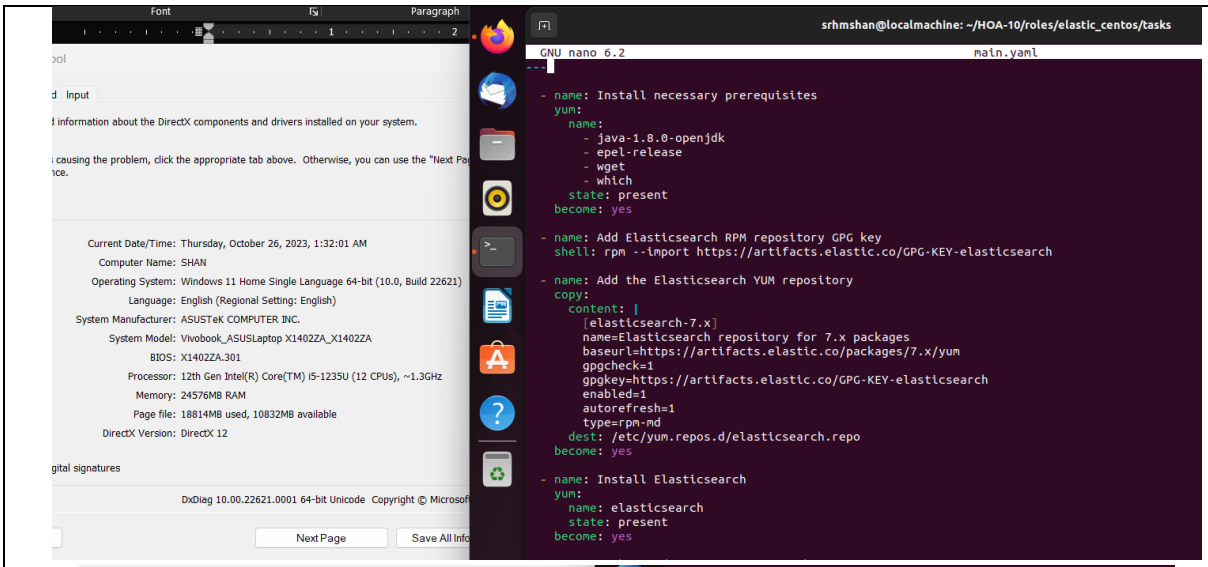
Step 4: Create a “roles” directory under your current directory. Under the “roles” directory, make 2 more directories according to the roles you defined in the elasticstack.yaml. Under each directory, create a “tasks” directory and make a “main.yaml” file.

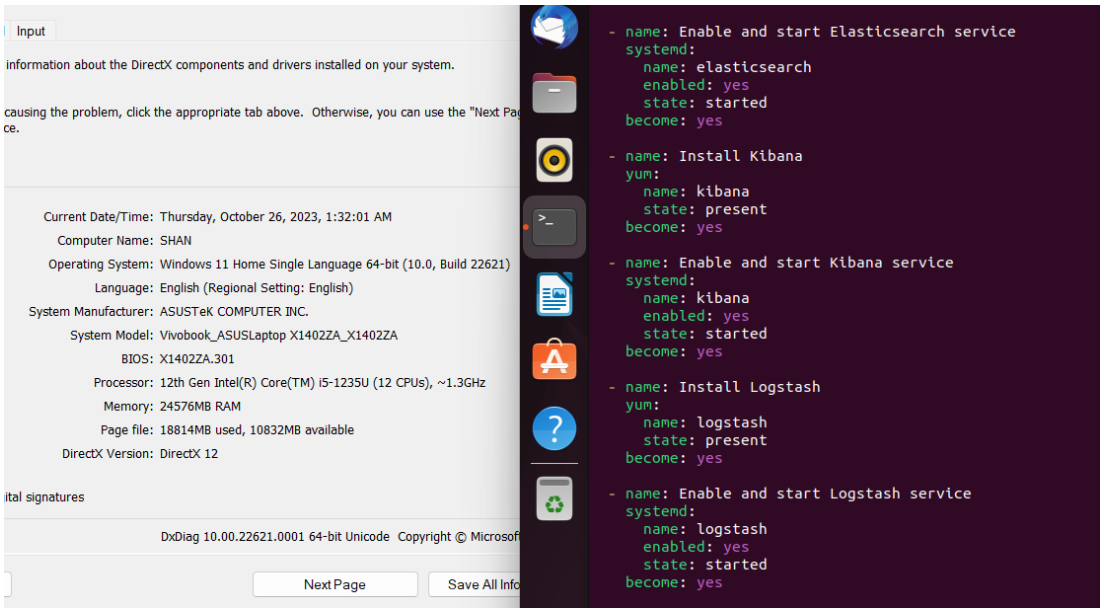


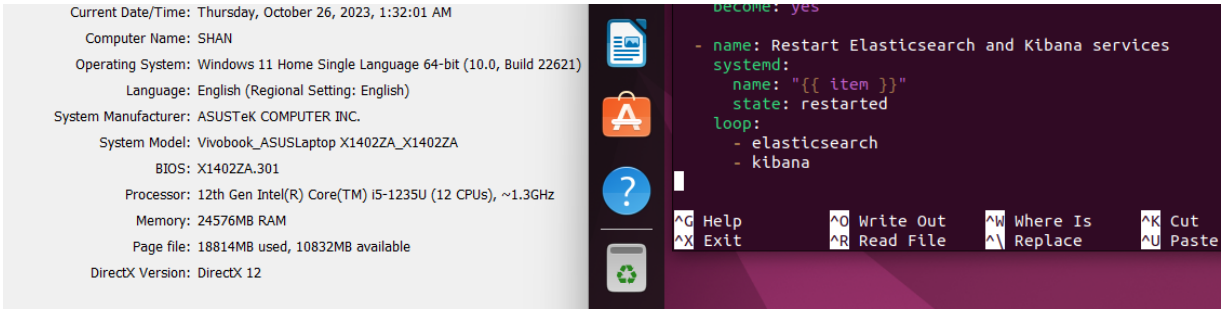
I applied the concept of creating roles.

Step 5: Edit your main.yaml files and input all the needed tasks to install Elastic Stack.

[CentOS]

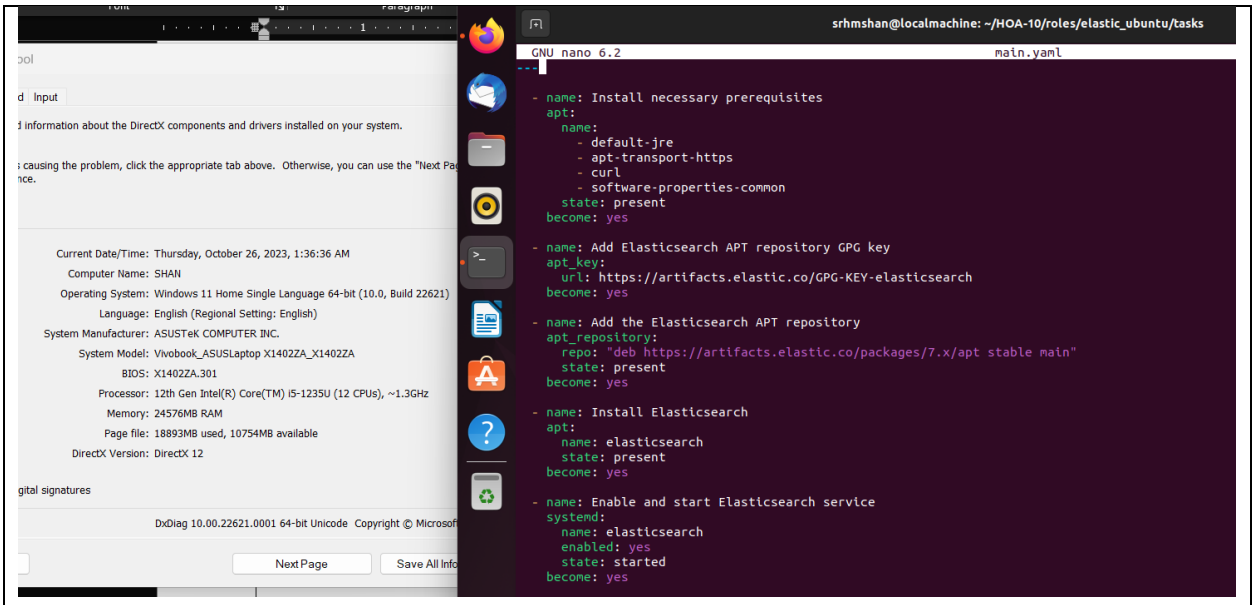


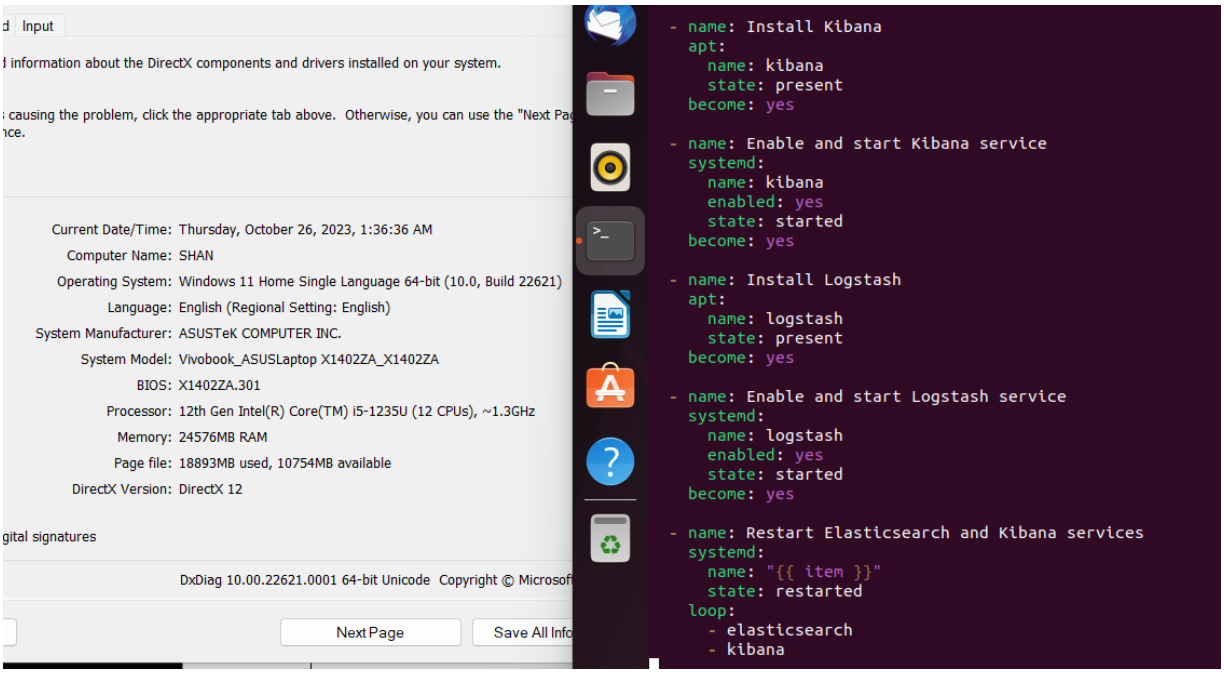




I used YUM for prerequisites, RPM repository for Elasticsearch, and similar service configurations.

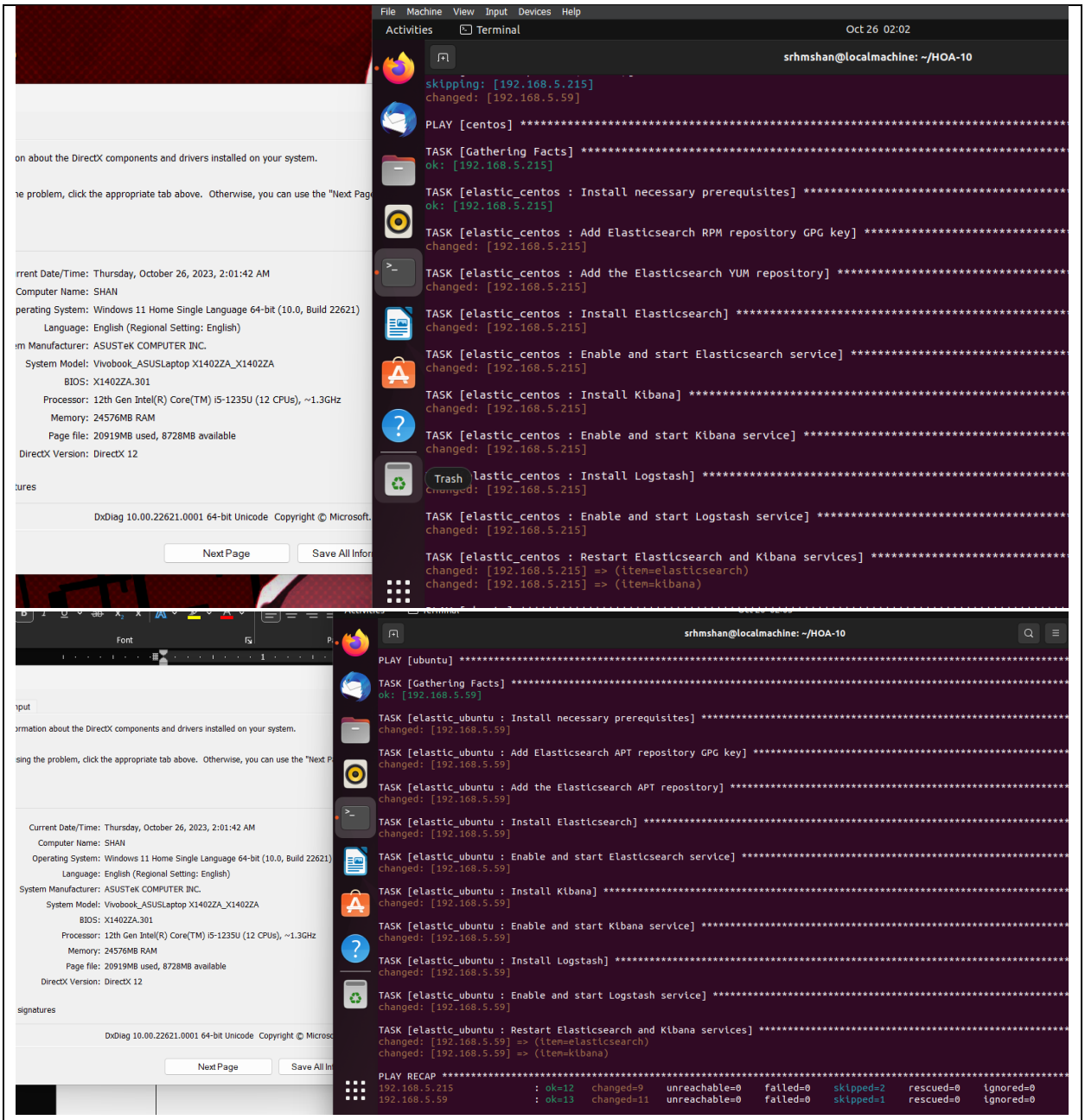
[Ubuntu]





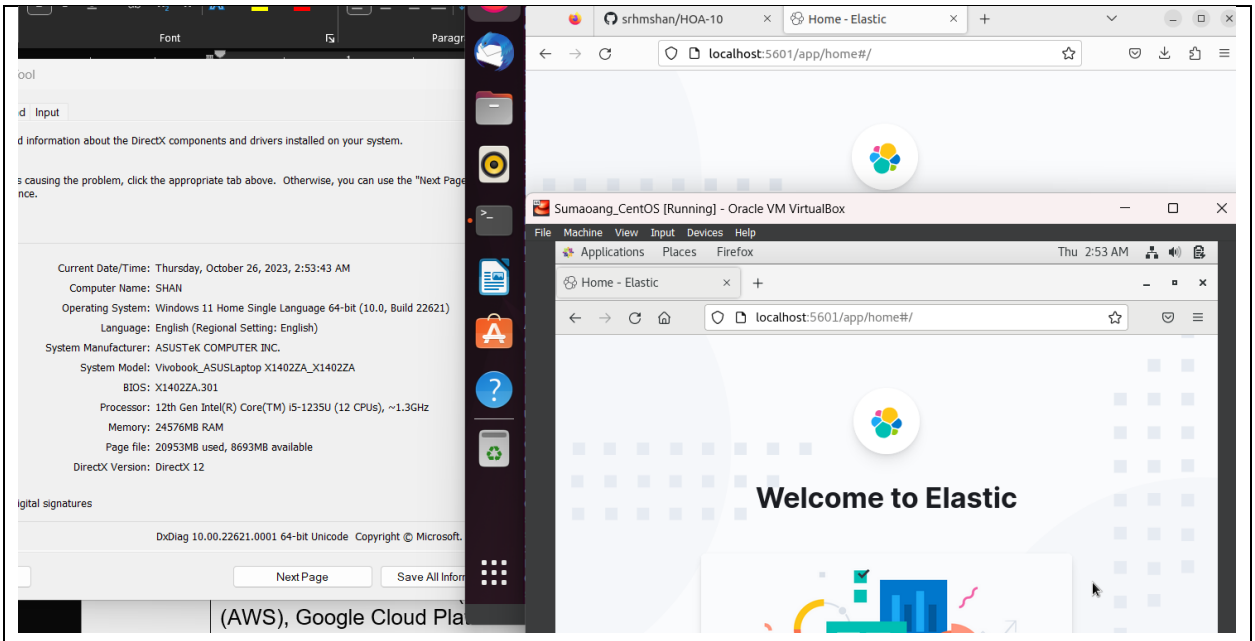
This installs and configures the Elastic Stack on Ubuntu. Tasks include prerequisite installation, adding the Elastic APT repository, installing Elasticsearch, Kibana, and Logstash, enabling services, and restarting Elasticsearch and Kibana.

Step 6: Run the ansible playbook.

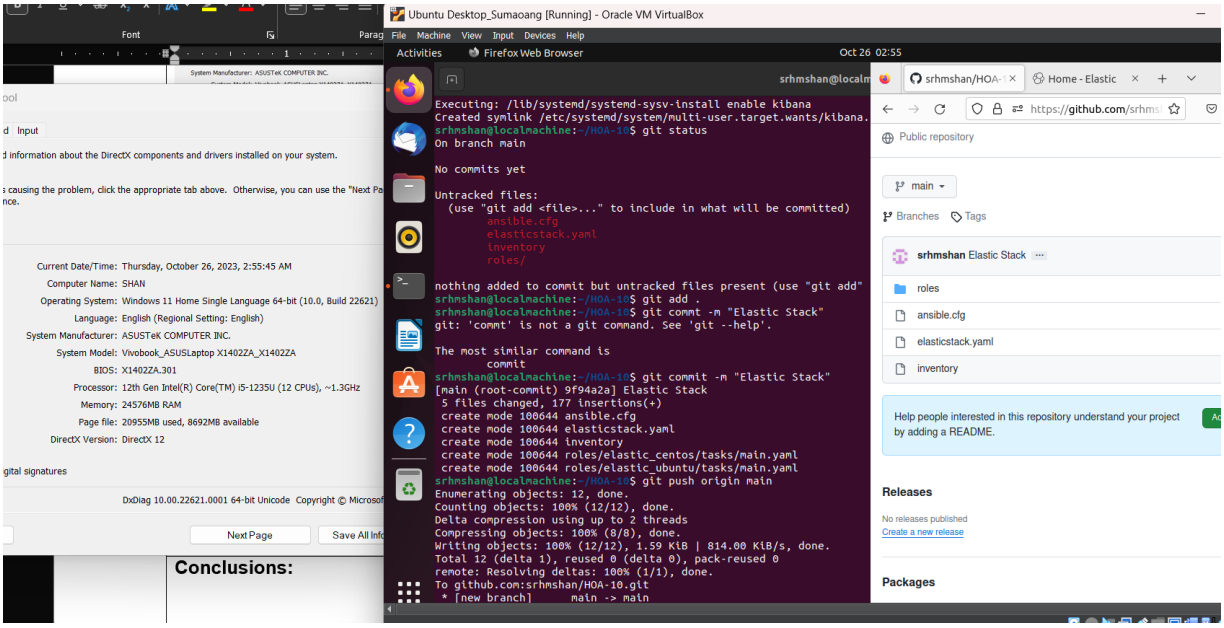


The tasks were successful.

Step 7: Verify if the installation was successful by putting "http://[ip_address]:5601" in your browser.



Step 8: Commit and push to GitHub.



Reflections:

Answer the following:

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

Log monitoring tools offer a range of benefits. They help detect issues allowing for timely problem resolution. These tools also optimize performance by allocating resources. Enhance security through threat detection. Also, they ensure compliance, with regulatory log management requirements and simplify troubleshooting leading to faster issue resolution. Log monitoring tools store data for analysis and trend identification while automating responses to events. They provide real time alerts for action and facilitate data visualization for log analysis. In summary these tools are crucial in maintaining system health, security, performance and streamlining management tasks while ensuring compliance, with standards.

Conclusions:

In this activity, I developed a workflow using Ansible to configure and oversee log monitoring tools such, as the Elastic Stack and Logstash. Effective log file analysis heavily relies on log monitoring. I automated the installation process, on Ubuntu and CentOS by executing playbooks while also documenting the deployment in a manner using roles. This activity highlighted the significance of log monitoring and Ansible in installations and management.