Name: Quizon, Nowell Gabriel C.	**Date Performed:** 10/25/2023
Course/Section: CPE31S5	**Date Submitted:** 10/27/2023
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.

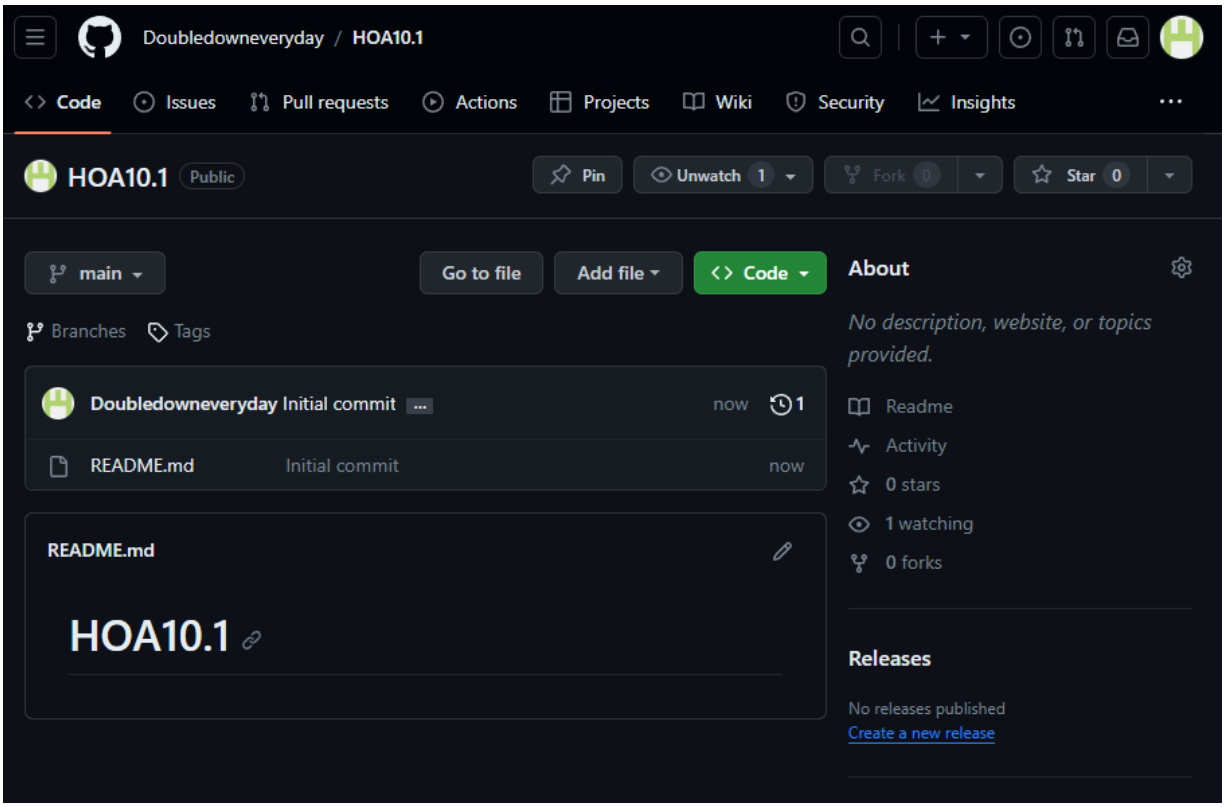
We use Graylog primarily as the stash for the logs of the web applications we build. However, it is also effective when working with raw strings (i.e. syslog): the tool parses it into the structured data we need. It also allows advanced custom search in the logs using structured queries. In other words,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

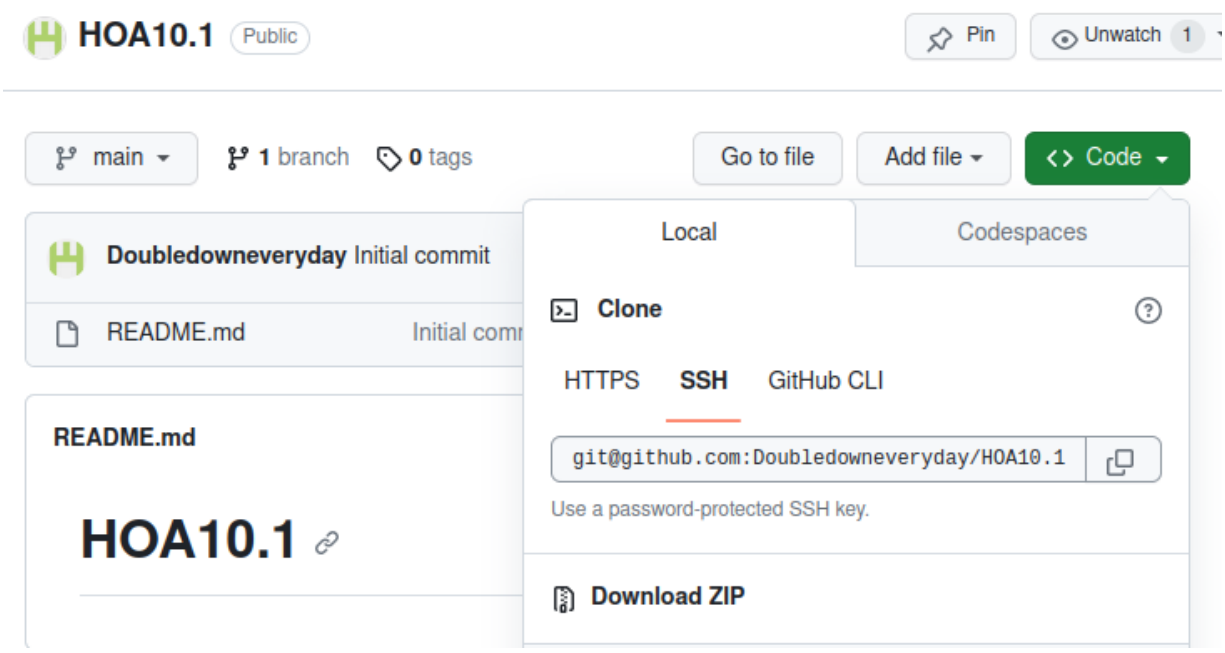
3. Tasks

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.

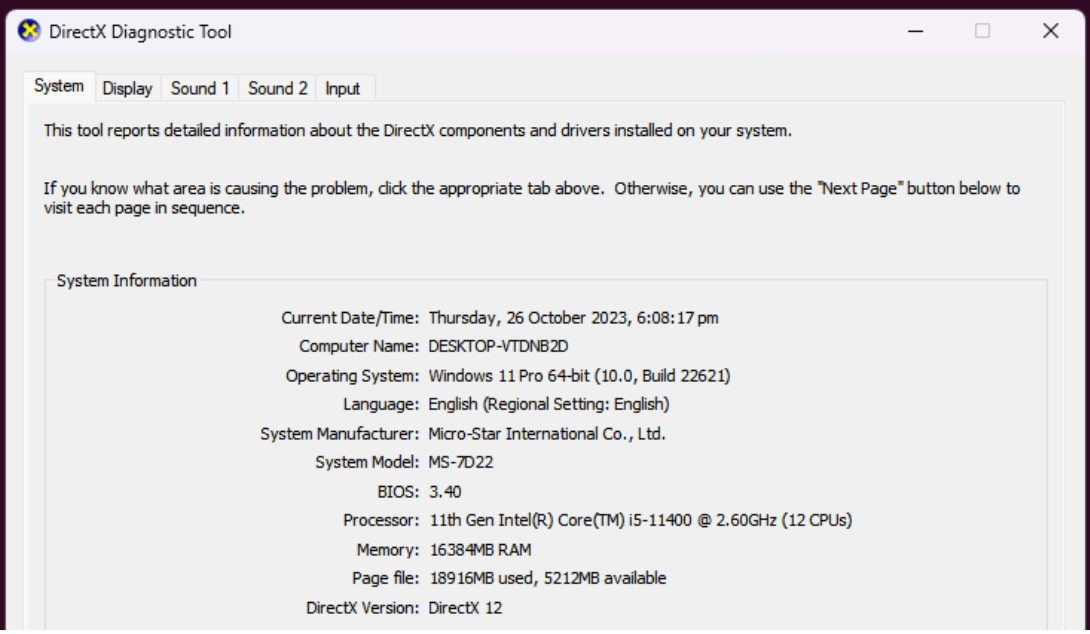
4. Output (screenshots and explanations)



- First, I created a new repository.



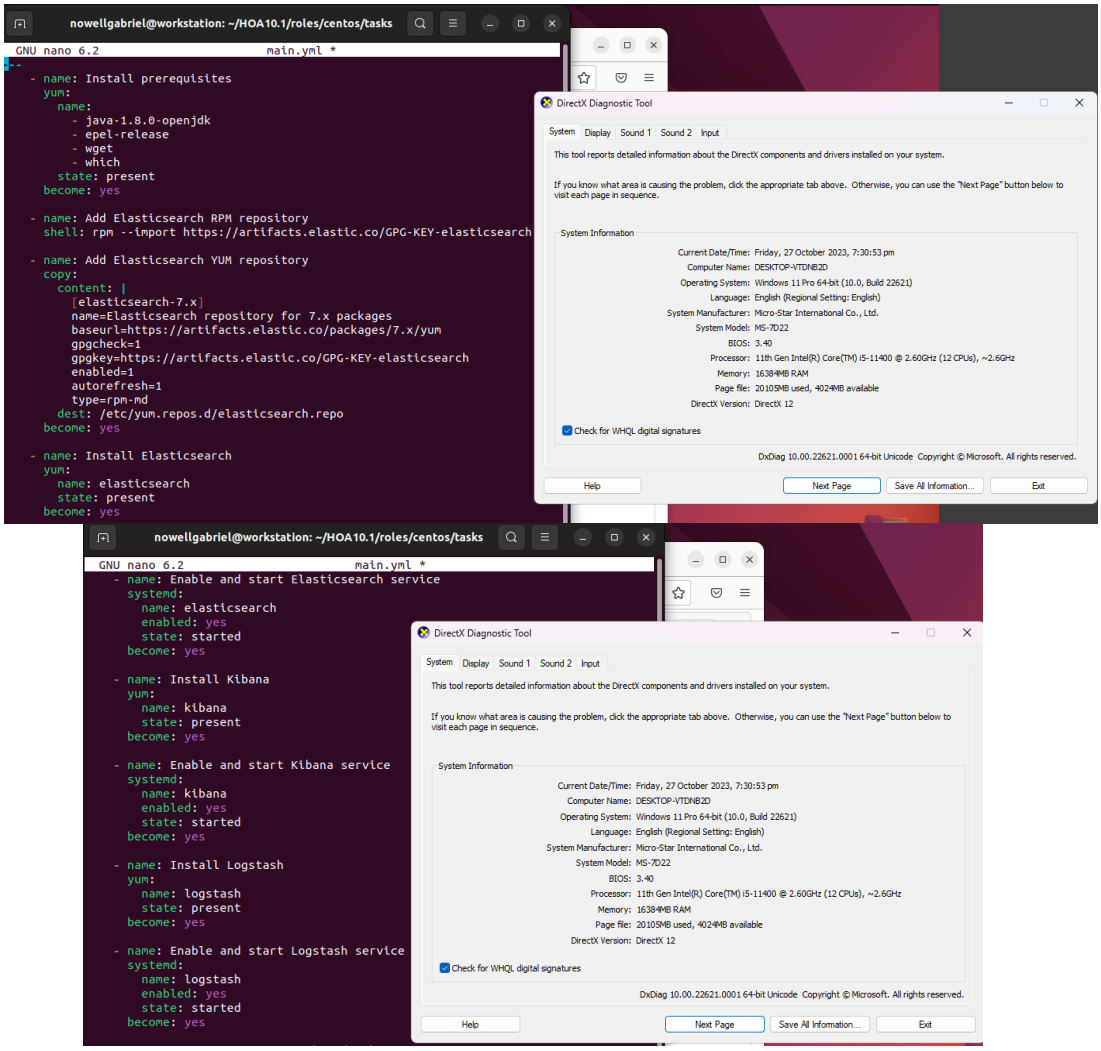
```
nowellgabriel@workstation:~$ git clone git@github.com:Doubledowneveryday/HOA10.1.git
Cloning into 'HOA10.1'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
nowellgabriel@workstation:~$
```



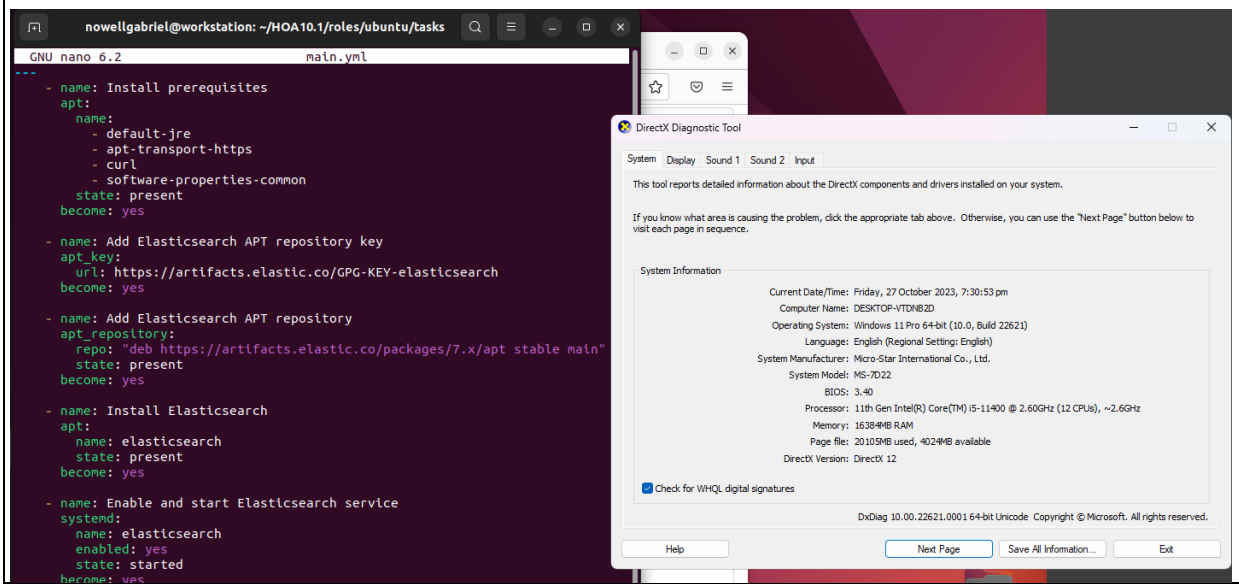
- Then, I cloned the repository into my local machine.

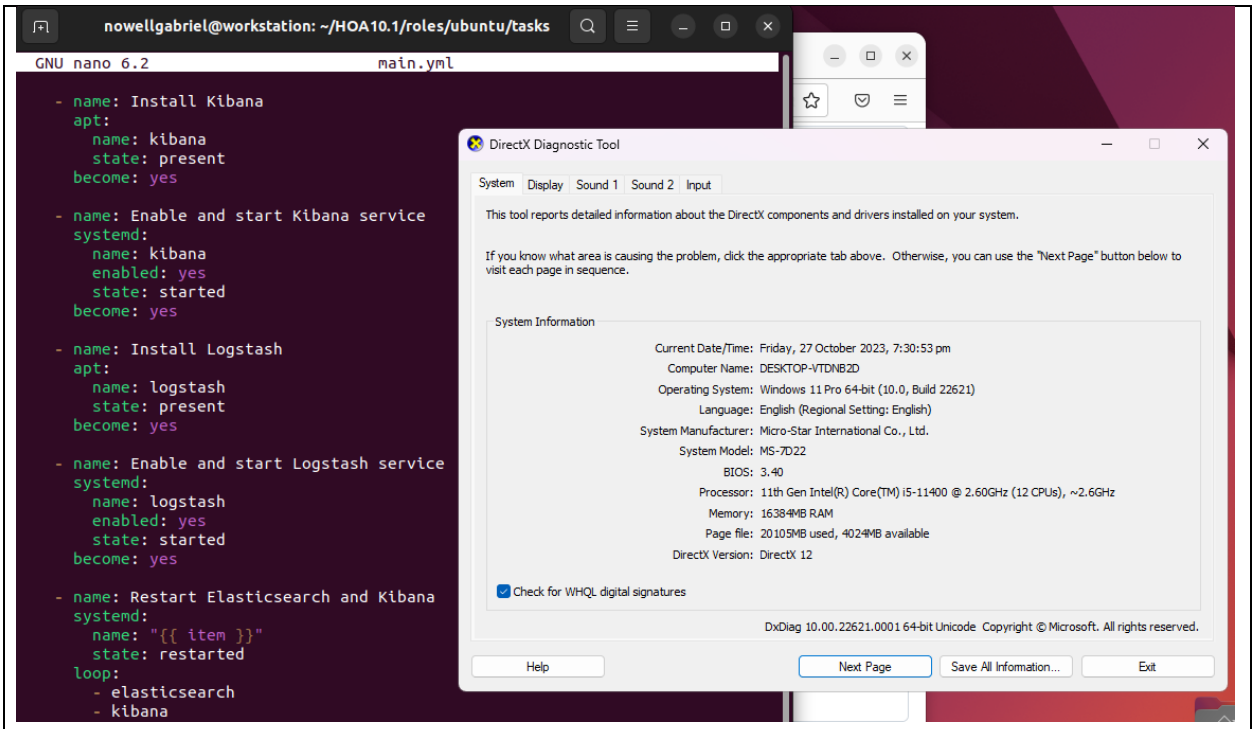
```
nowellgabriel@workstation:~/HOA10.1$ tree
.
├── ansible.cfg
├── elstickstack.yml
├── inventory
├── README.md
└── roles
    ├── centos
    │   └── tasks
    │       └── main.yml
    └── ubuntu
        └── tasks
            └── main.yml

5 directories, 6 files
```

- After entering the directory, I created the ansible.cfg, inventory and elastickstack.yml files. Also, I created the roles directory and everything needed inside.

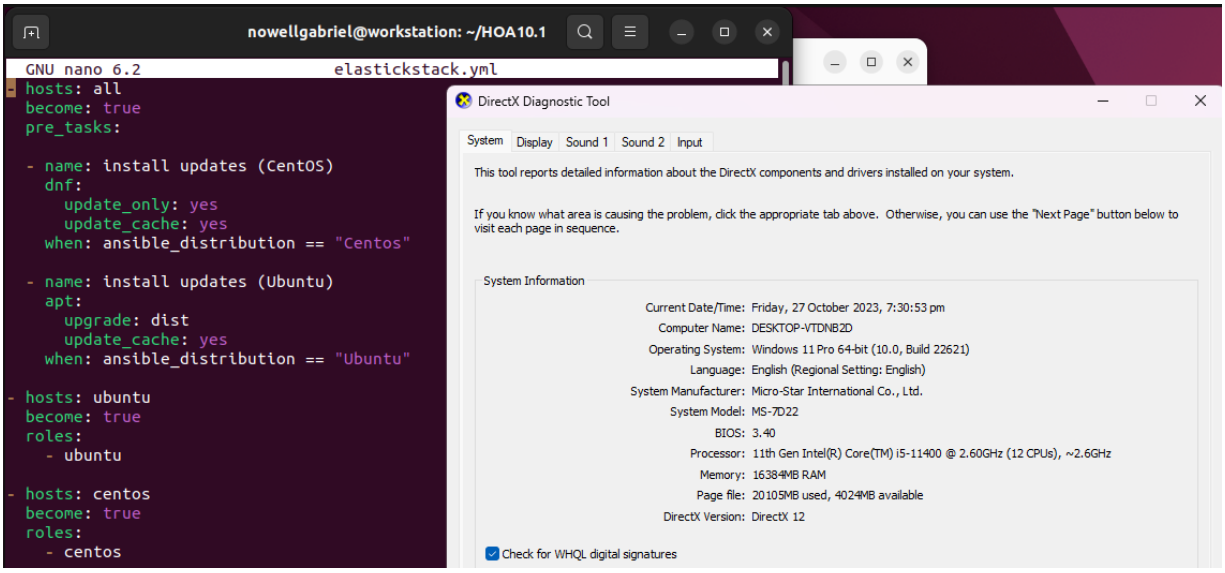


- Created the main.yml file for centos

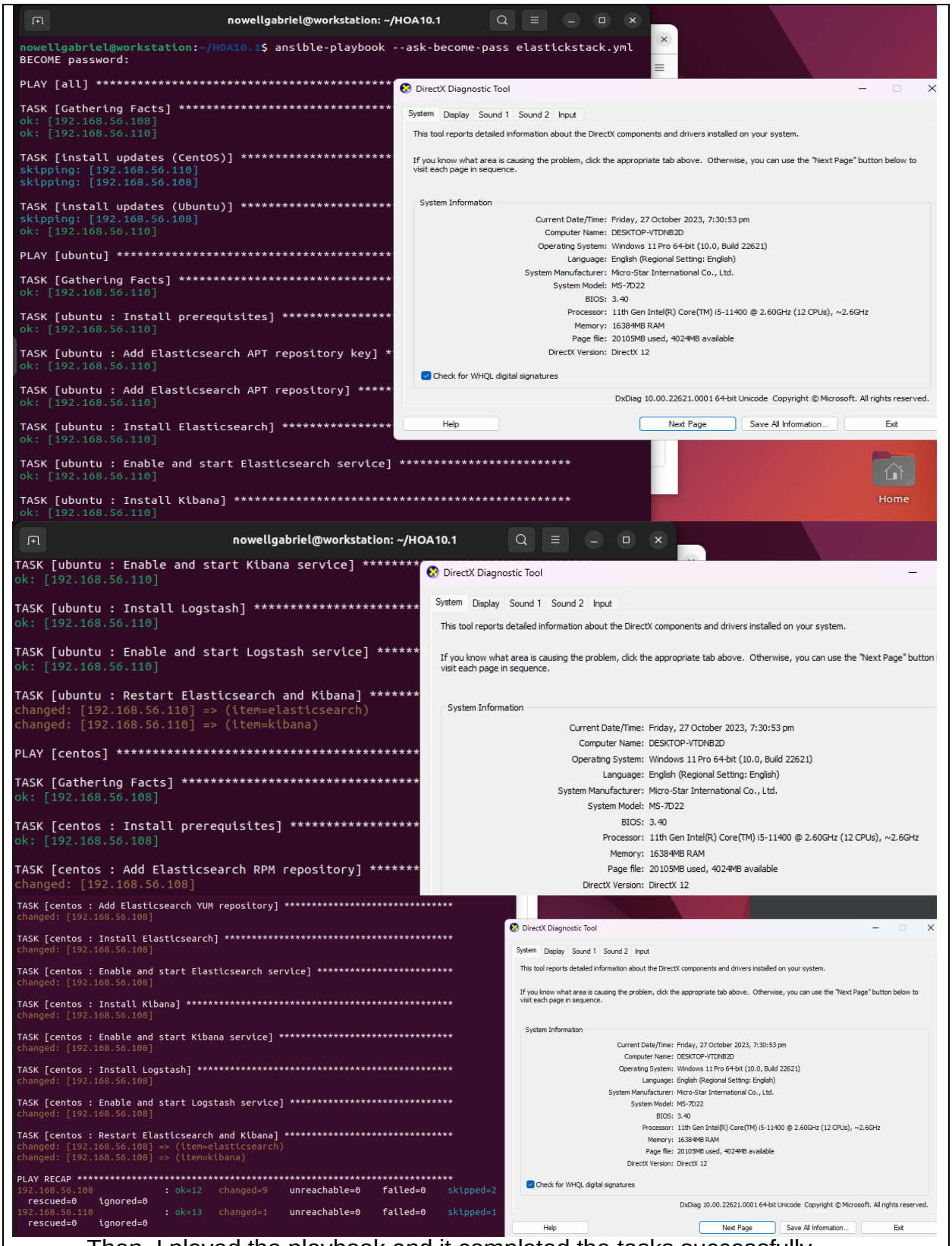




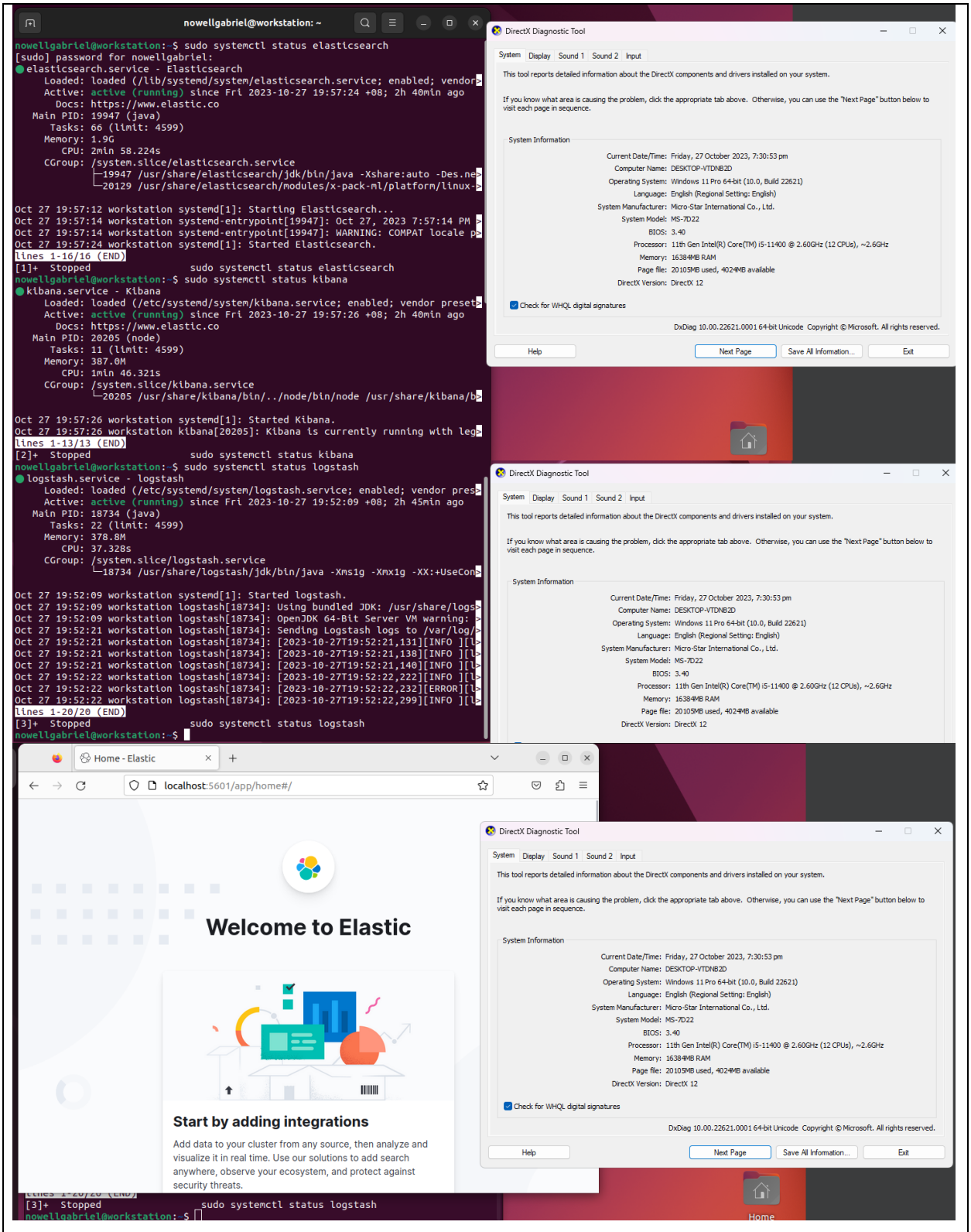
- Created the main.yml file for ubuntu.



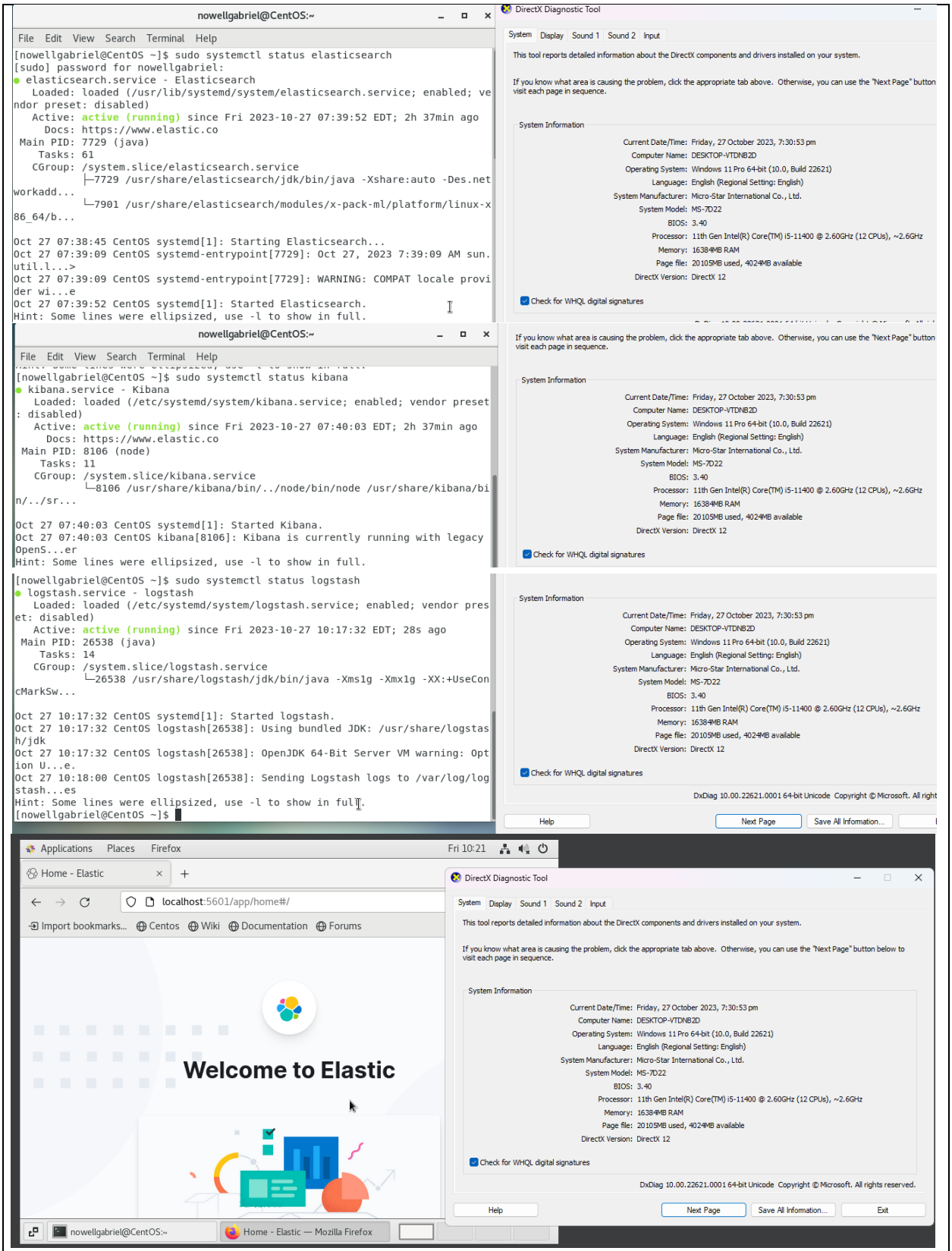
- Then, created the elastickstack.yml file.



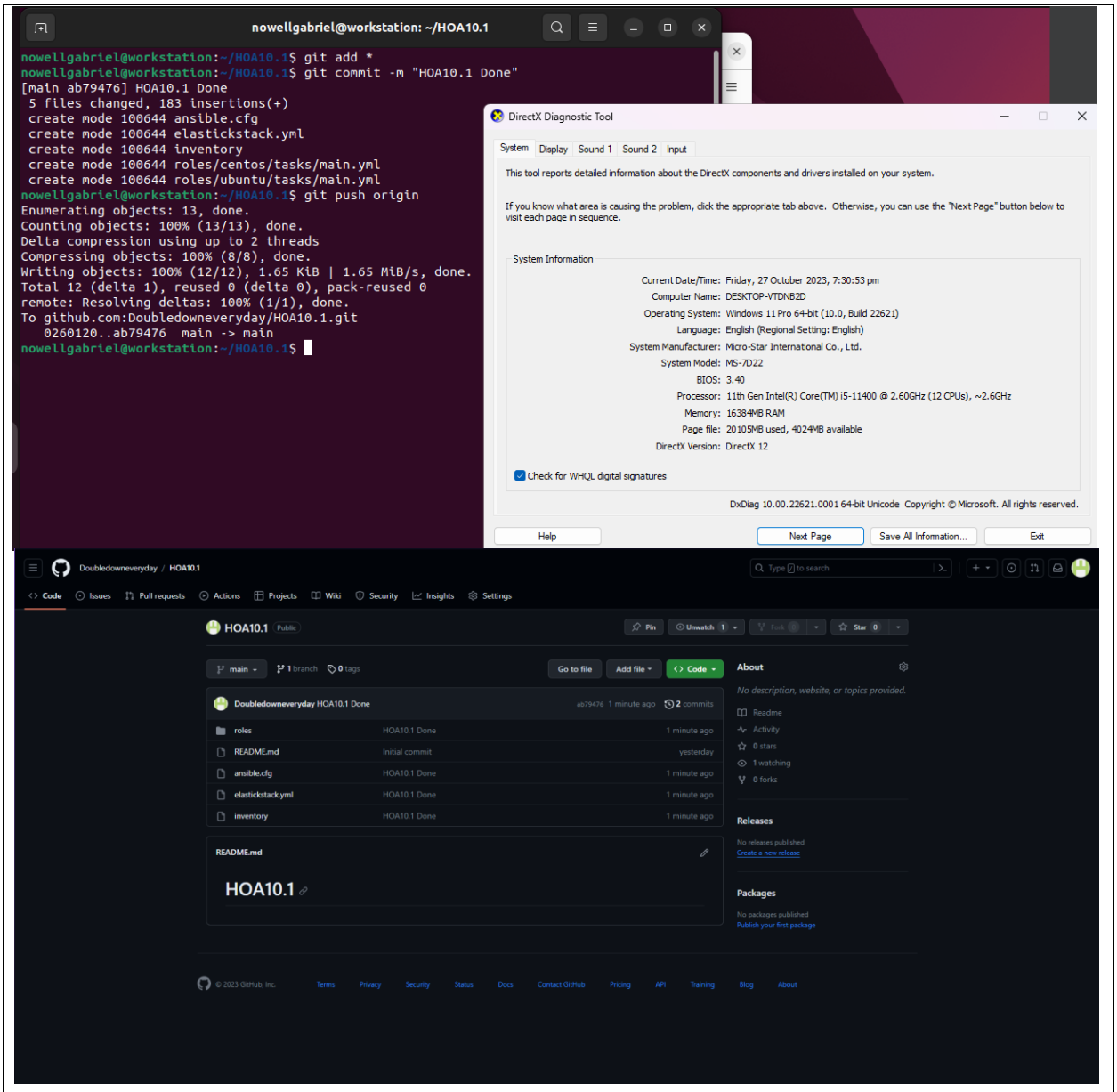
- Then, I played the playbook and it completed the tasks successfully



- This is to confirm that everything was installed in ubuntu.



- This is to confirm that everything was installed in CentOS.



- Committed everything to the repository.

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool?
   - A log monitoring solution has important advantages for businesses. Real-time issue identification is made possible, allowing quick problem-solving. Finding patterns helps with proactive problem solving by averting future issues. By identifying suspect activity, security and compliance are strengthened. Efficiency is improved by the help of past data analysis, performance improvement, and future planning. It offers an audit record for openness and accountability. Gathering data is simplified for easy analysis with centralized log management.

Timely notifications minimize downtime and guarantee high availability. By avoiding expensive outages and security breaches, this solution increases cost-efficiency. Maintaining steady and secure operations ultimately improves client satisfaction.

Conclusions:

- - To sum up, using Ansible as Infrastructure as Code (IaC) to deploy corporate log monitoring solutions simplifies the installation and setup process. When it comes to scanning and analyzing log files to find patterns and handle performance and security concerns, log monitoring software is essential. It makes sure that the computer system is performing at its best, eliminating risks and downtime. The environment for maintaining equipment is further improved by integration with warning and analytical tools. The Elastic Stack, which provides real-time data search, analysis, and visualization, and Graylog, a powerful platform for handling both structured and unstructured log data, are two major technologies in this area. System administrators now have the tools necessary to actively monitor their computer systems and acquire useful data.