Name: Mark Andrei Ponayo	**Date Performed:** Oct 25, 2023
Course/Section: BSCPE31S5	**Date Submitted:** Oct 27, 2023
Instructor: Engr. Roman Richard	**Semester and SY:** 1st sem 2022-2023

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

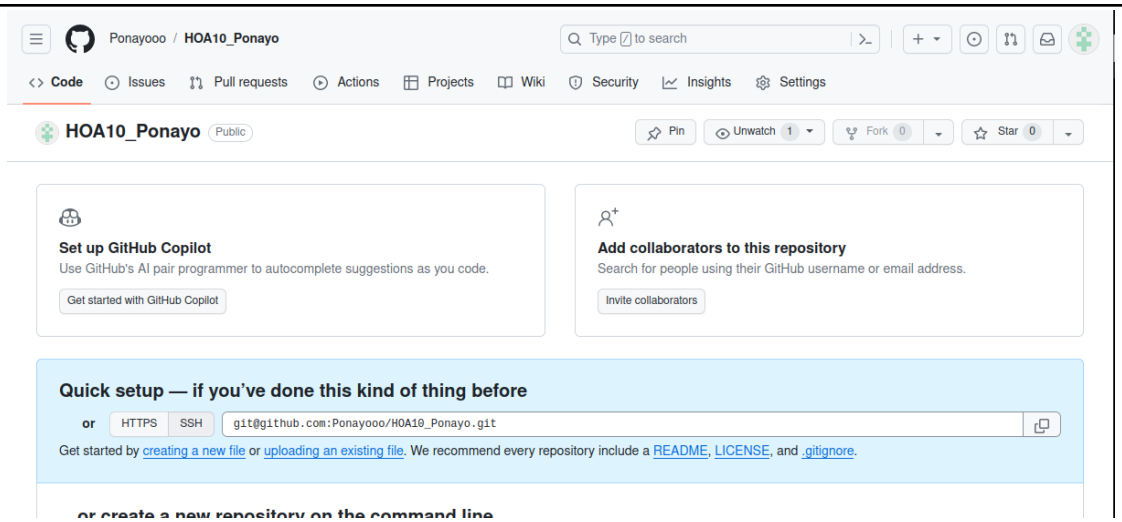
3. Tasks

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)

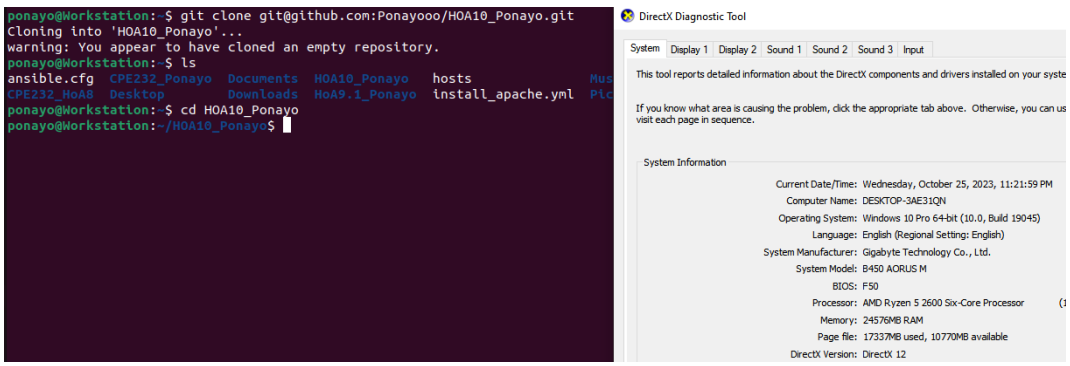
Creating New Repository

On this step,



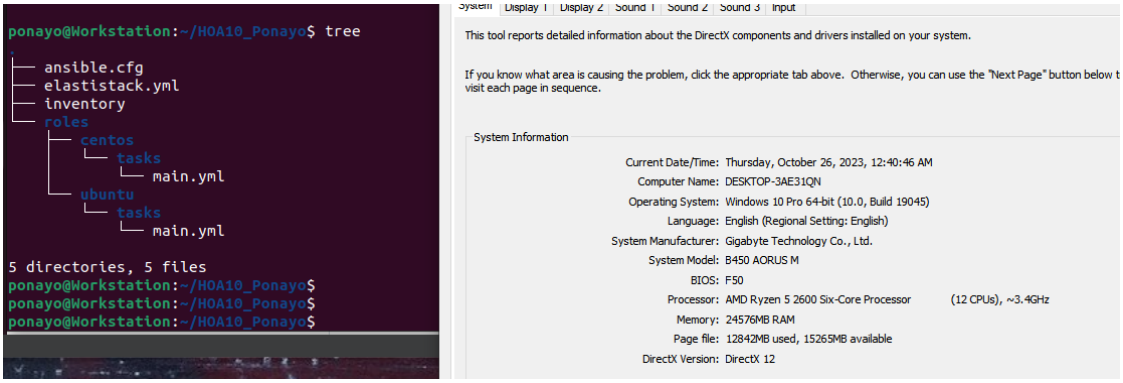
Cloning Repository

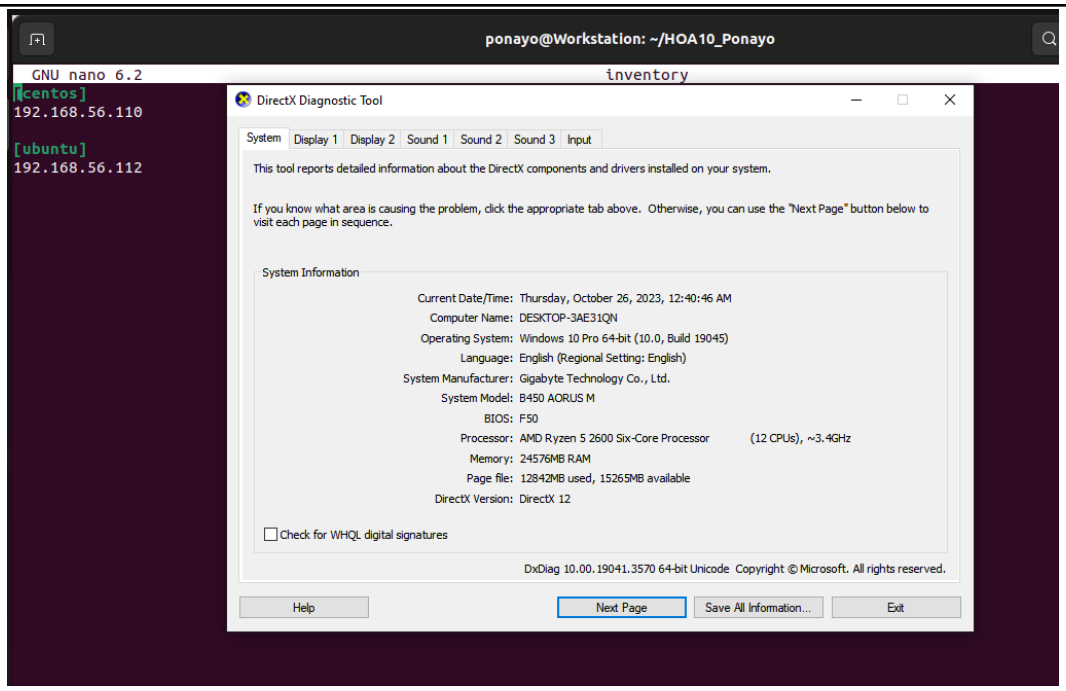
On this step, I use git clone to apply the new repository in the workstation. And use the "ls" command to show if the cloning is successful.



Creating files

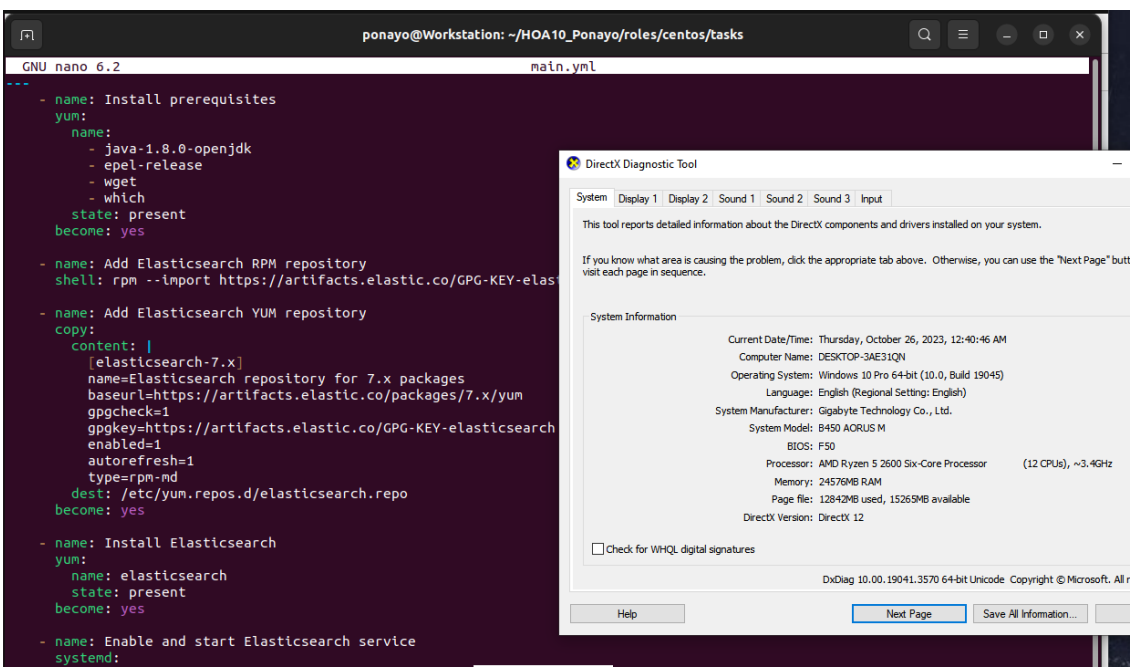
On this step, I created the following files that I need to install the elasticstack.





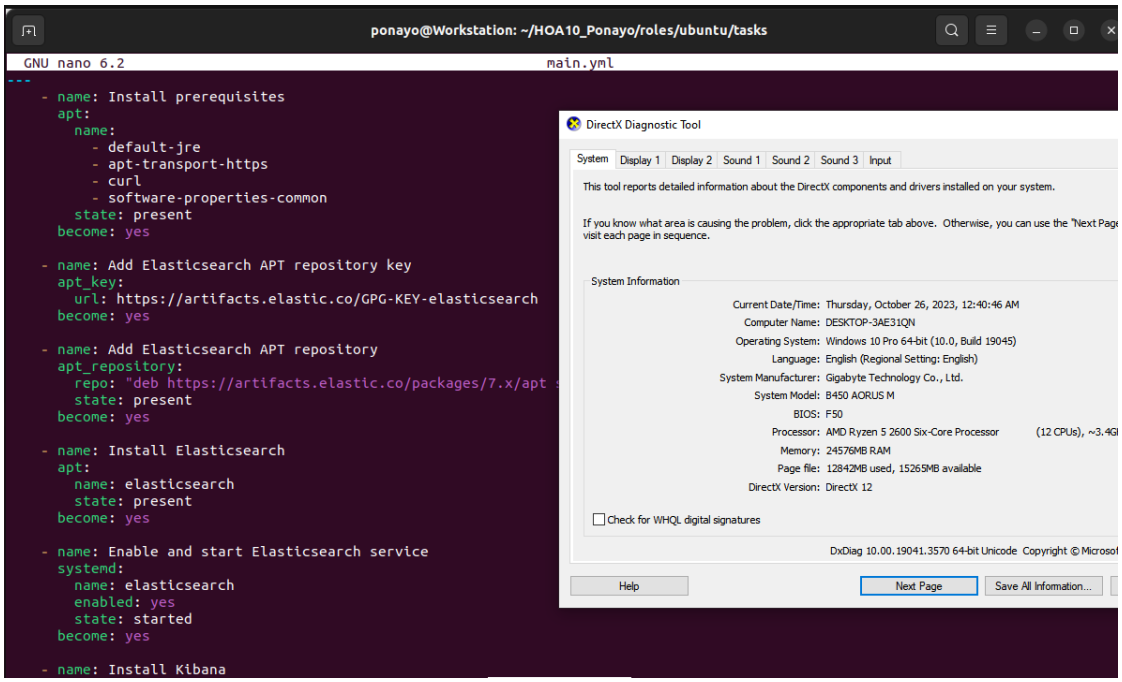
Creating centos tasks

On this step, I created a tasks file that contains the add elasticsearch repository, installation of elasticsearch, install elasticsearch, etc. in the centos.



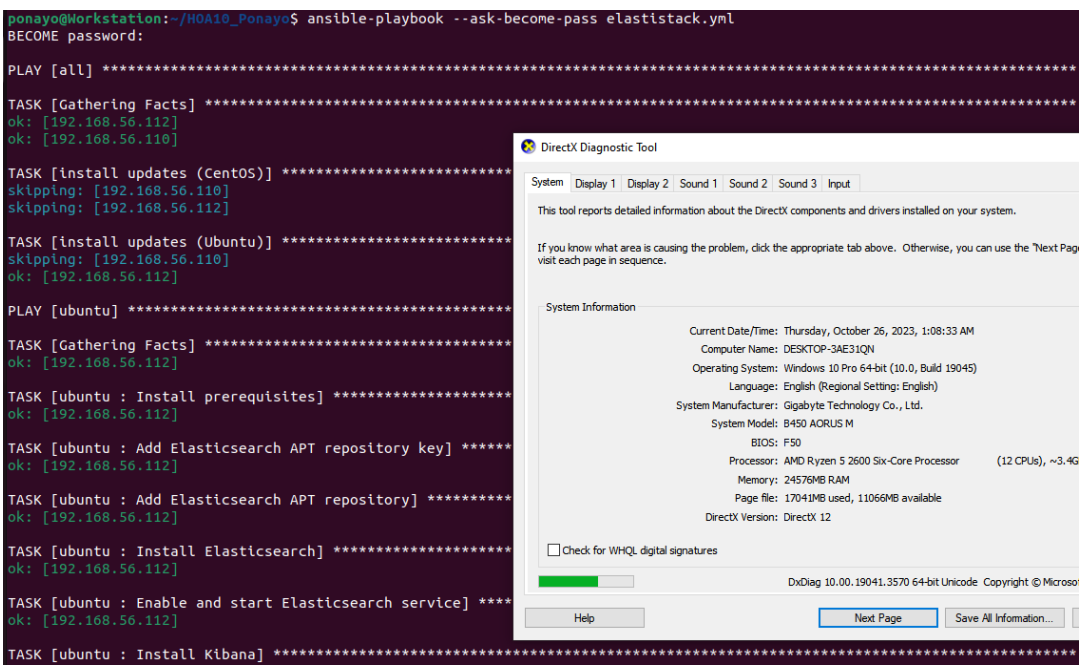
Creating ubuntu tasks

On this step, I created a task file that contains the adding of elasticsearch repository, installation of elasticsearch, and enable/start the elasticsearch service in the ubuntu.

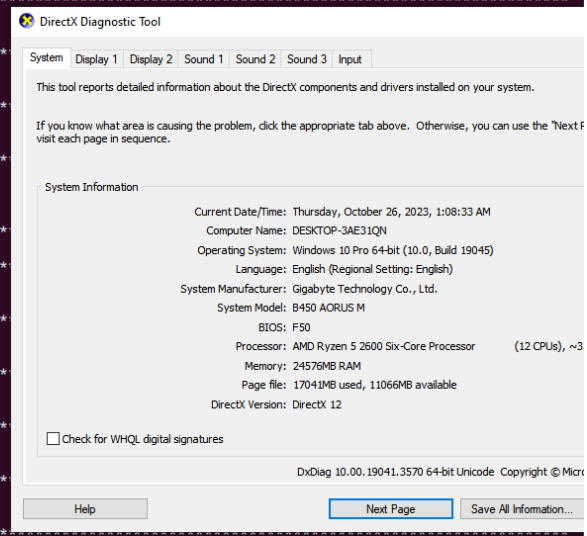


Running the playbook.

On this step, i use the command “ansible-playbook –ask-become-pass elasticstack.yml” to install the files.



```
TASK [ubuntu : Install Kibana] ************************************************************************************
ok: [192.168.56.112]

TASK [ubuntu : Enable and start Kibana service] *******************************************************************
ok: [192.168.56.112]

TASK [ubuntu : Install Logstash] ******************************
ok: [192.168.56.112]

TASK [ubuntu : Enable and start Logstash service] ************
ok: [192.168.56.112]

TASK [ubuntu : Restart Elasticsearch and Kibana] *************
changed: [192.168.56.112] => (item=elasticsearch)
changed: [192.168.56.112] => (item=kibana)

PLAY [centos] *********************************************

TASK [Gathering Facts] ************************************
ok: [192.168.56.110]

TASK [centos : Install prerequisites] *********************
ok: [192.168.56.110]

TASK [centos : Add Elasticsearch RPM repository] *************
changed: [192.168.56.110]

TASK [centos : Add Elasticsearch YUM repository] *************
ok: [192.168.56.110]

TASK [centos : Install Elasticsearch] *********************
ok: [192.168.56.110]

TASK [centos : Enable and start Elasticsearch service] ********************************************************
ok: [192.168.56.110]

TASK [centos : Install Kibana] ************************************************************************************
ok: [192.168.56.110]
```

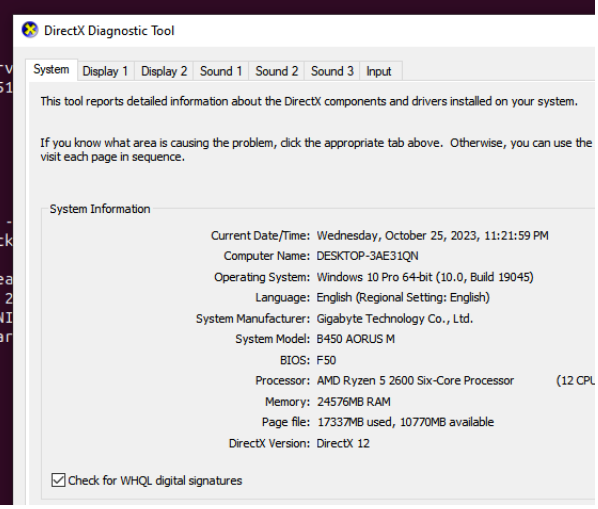


Showing if the installation is successful

Server 1

To verify if the installation is successful. I use the “sudo system status elasticsearch,kibana, and logstash and it shows that the kibana, elasticsearch, and logstash is active.

```
ponayo@Workstation:~$ sudo systemctl status elasticsearch
[sudo] password for ponayo:
Sorry, try again.
[sudo] password for ponayo:
Sorry, try again.
[sudo] password for ponayo:
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.serv
     Active: active (running) since Wed 2023-10-25 23:38:51
       Docs: https://www.elastic.co
   Main PID: 7044 (java)
      Tasks: 64 (limit: 2261)
     Memory: 481.5M
        CPU: 2min 59.053s
     CGroup: /system.slice/elasticsearch.service
             ├─7044 /usr/share/elasticsearch/jdk/bin/java -
             └─7227 /usr/share/elasticsearch/modules/x-pack

Oct 25 23:37:19 Workstation systemd[1]: Starting Elasticsea
Oct 25 23:37:35 Workstation systemd-entrypoint[7044]: Oct 2
Oct 25 23:37:35 Workstation systemd-entrypoint[7044]: WARNI
Oct 25 23:38:51 Workstation systemd[1]: Started Elasticsear
lines 1-16/16 (END)
```



```
     Memory: 481.5M
        CPU: 2min 59.053s
     CGroup: /system.slice/elasticsearch.service
             ├─7044 /usr/share/elasticsearch/jdk/bin/java -Xsha
             └─7227 /usr/share/elasticsearch/modules/x-pack-ml/

Oct 25 23:37:19 Workstation systemd[1]: Starting Elasticsearch.
Oct 25 23:37:35 Workstation systemd-entrypoint[7044]: Oct 25, 2
Oct 25 23:37:35 Workstation systemd-entrypoint[7044]: WARNING:
Oct 25 23:38:51 Workstation systemd[1]: Started Elasticsearch.
lines 1-16/16 (END)
[1]+  Stopped                 sudo systemctl status elasticsear
ponayo@Workstation:~$ sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enable
     Active: active (running) since Wed 2023-10-25 23:38:56 PST
       Docs: https://www.elastic.co
   Main PID: 7309 (node)
      Tasks: 11 (limit: 2261)
     Memory: 89.1M
        CPU: 1min 5.971s
     CGroup: /system.slice/kibana.service
             └─7309 /usr/share/kibana/bin/../node/bin/node /usr

Oct 25 23:38:56 Workstation systemd[1]: Started Kibana.
Oct 25 23:38:57 Workstation kibana[7309]: Kibana is currently r
lines 1-13/13 (END)
```

DirectX Diagnostic Tool

System | Display 1 | Display 2 | Sound 1 | Sound 2 | Sound 3 | Input

This tool reports detailed information about the DirectX components and drivers installed on your system.

If you know what area is causing the problem, click the appropriate tab above. Otherwise, you can use t visit each page in sequence.

System Information

Current Date/Time:	Wednesday, October 25, 2023, 11:21:59 PM
Computer Name:	DESKTOP-3AE31QN
Operating System:	Windows 10 Pro 64-bit (10.0, Build 19045)
Language:	English (Regional Setting: English)
System Manufacturer:	Gigabyte Technology Co., Ltd.
System Model:	B450 AORUS M
BIOS:	F50
Processor:	AMD Ryzen 5 2600 Six-Core Processor (12 C
Memory:	24576MB RAM
Page file:	17337MB used, 10770MB available
DirectX Version:	DirectX 12

☑ Check for WHQL digital signatures

```
Oct 25 23:38:56 Workstation systemd[1]: Started Kibana.
Oct 25 23:38:57 Workstation kibana[7309]: Kibana is currently running with leg
lines 1-13/13 (END)
[2]+  Stopped                 sudo systemctl status kibana
ponayo@Workstation:~$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor pre
     Active: active (running) since Thu 2023-10-26 00:17:41 PST; 43s ago
   Main PID: 11636 (java)
      Tasks: 15 (limit: 2261)
     Memory: 436.8M
        CPU: 33.400s
     CGroup: /system.slice/logstash.service
             └─11636 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCo

Oct 26 00:17:41 Workstation systemd[1]: Started logstash.
Oct 26 00:17:41 Workstation logstash[11636]: Using bundled JDK: /usr/share/log
Oct 26 00:17:41 Workstation logstash[11636]: OpenJDK 64-Bit Server VM warning:
lines 1-13/13 (END)
```

DirectX Diagnostic Tool

System | Display 1 | Display 2 | Sound 1 | Sound 2 | Sound 3 | Input

This tool reports detailed information about the DirectX components and driv

If you know what area is causing the problem, click the appropriate tab abov visit each page in sequence.

System Information

Current Date/Time:	Wednesday, October
Computer Name:	DESKTOP-3AE31QN
Operating System:	Windows 10 Pro 64-bi
Language:	English (Regional Setti
System Manufacturer:	Gigabyte Technology
System Model:	B450 AORUS M
BIOS:	F50
Processor:	AMD Ryzen 5 2600 Si

Firefox Web Browser

Home - Elastic

localhost:5601/app/home#/

Welcome to Elastic

Start by adding integrations

Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats.

Add integrations Explore on my own

DirectX Diagnostic Tool

System | Display 1 | Display 2 | Sound 1 | Sound 2 | Sound 3 | Input

This tool reports detailed information about the DirectX components and d

If you know what area is causing the problem, click the appropriate tab ab visit each page in sequence.

System Information

Current Date/Time:	Wednesday, Octob
Computer Name:	DESKTOP-3AE31QN
Operating System:	Windows 10 Pro 64-
Language:	English (Regional Se
System Manufacturer:	Gigabyte Technolog
System Model:	B450 AORUS M
BIOS:	F50
Processor:	AMD Ryzen 5 2600
Memory:	24576MB RAM
Page file:	17337MB used, 107
DirectX Version:	DirectX 12

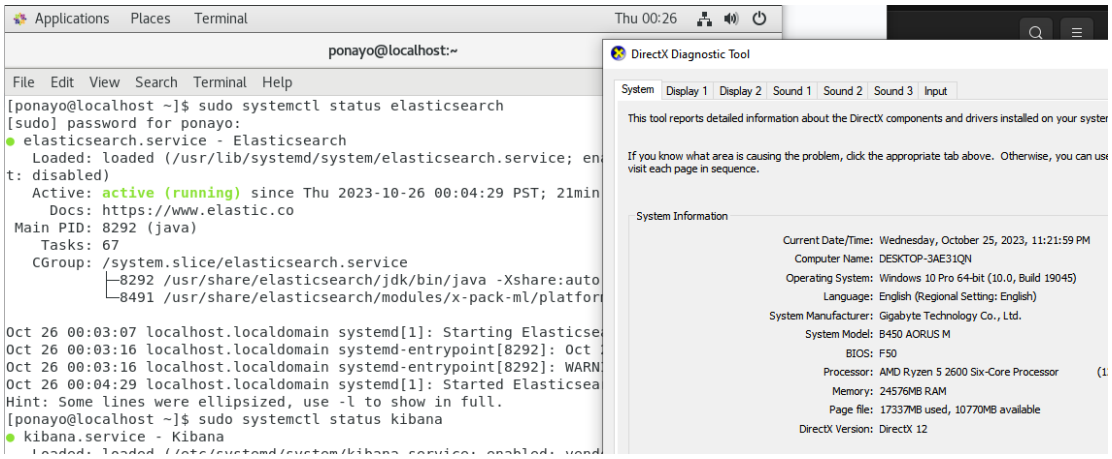
☑ Check for WHQL digital signatures

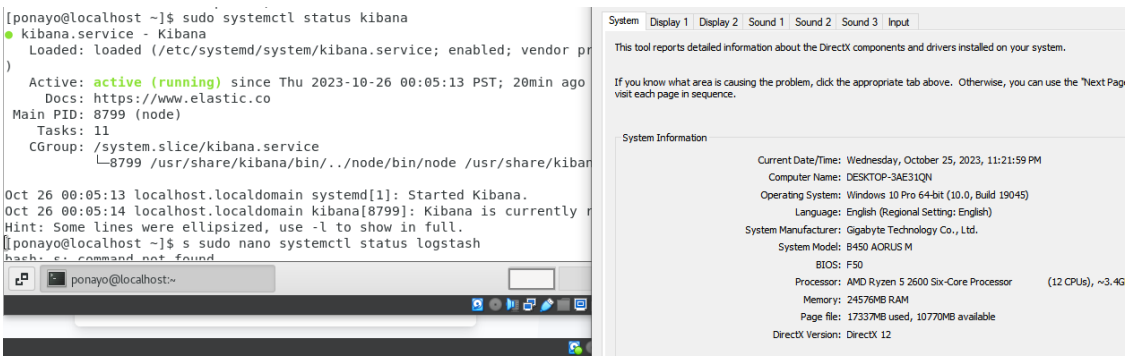
DxDiag 10.00.190

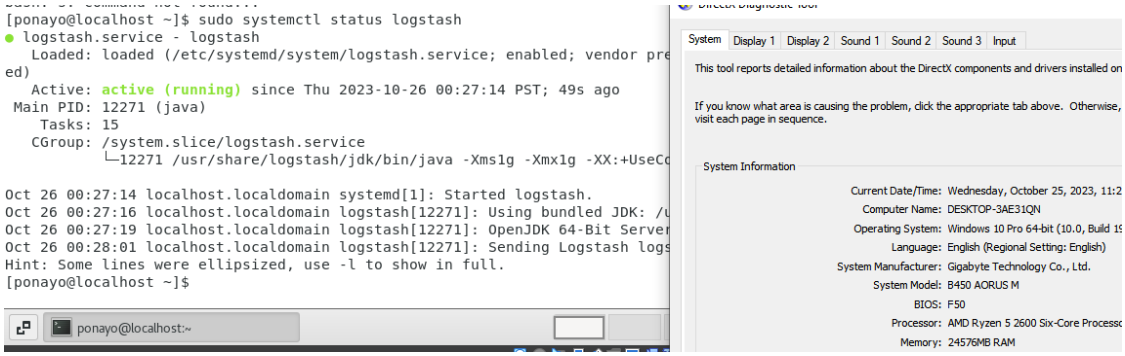
Help Next

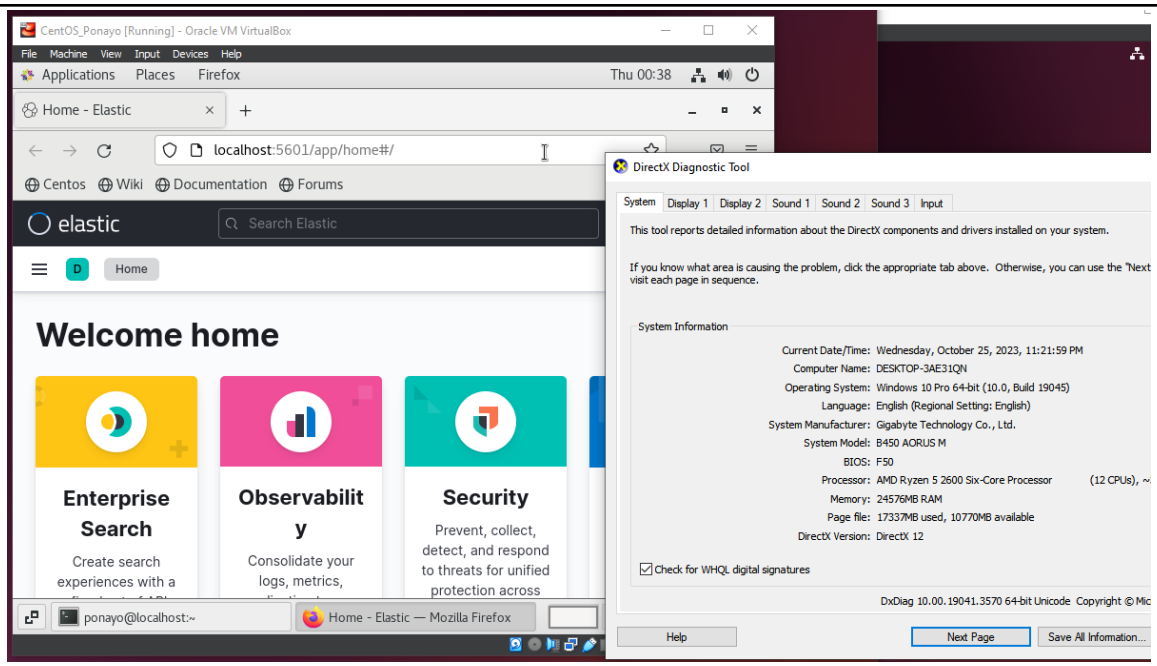
Centos:

To show if the installation is successful. I also run the command elasticsearch, kibana and logstash and the output is successful.









https://github.com/Ponayooo/HOA10_Ponayo

Reflections:

Answer the following:

1. What are the benefits of having a log monitoring tool?
   - Log monitoring tools collect data from all of your systems or applications, it gives you a view into your entire IT infrastructure. By having a log tool, it will improve the visibility to identify potential problems early on before they cause outages or disruptions. Log monitoring tools can help you to quickly identify the root cause of the problem and how to resolve it.

Conclusions:

In conclusion, Implementing log monitoring tools in Ubuntu Workstation and CentOS is a critical step in improving the security, performance, and reliability of your systems. By collecting and analyzing log data, you can quickly identify and resolve potential problems, detect and respond to security threats, and improve the overall health of your IT infrastructure.