Name: Victor B. Ortega	**Date Performed:** 10/25/2023
Course/Section: CPE31S5	**Date Submitted:** 10/25/2023
Instructor: Engr. Roman Richard	**Semester and SY:** 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.

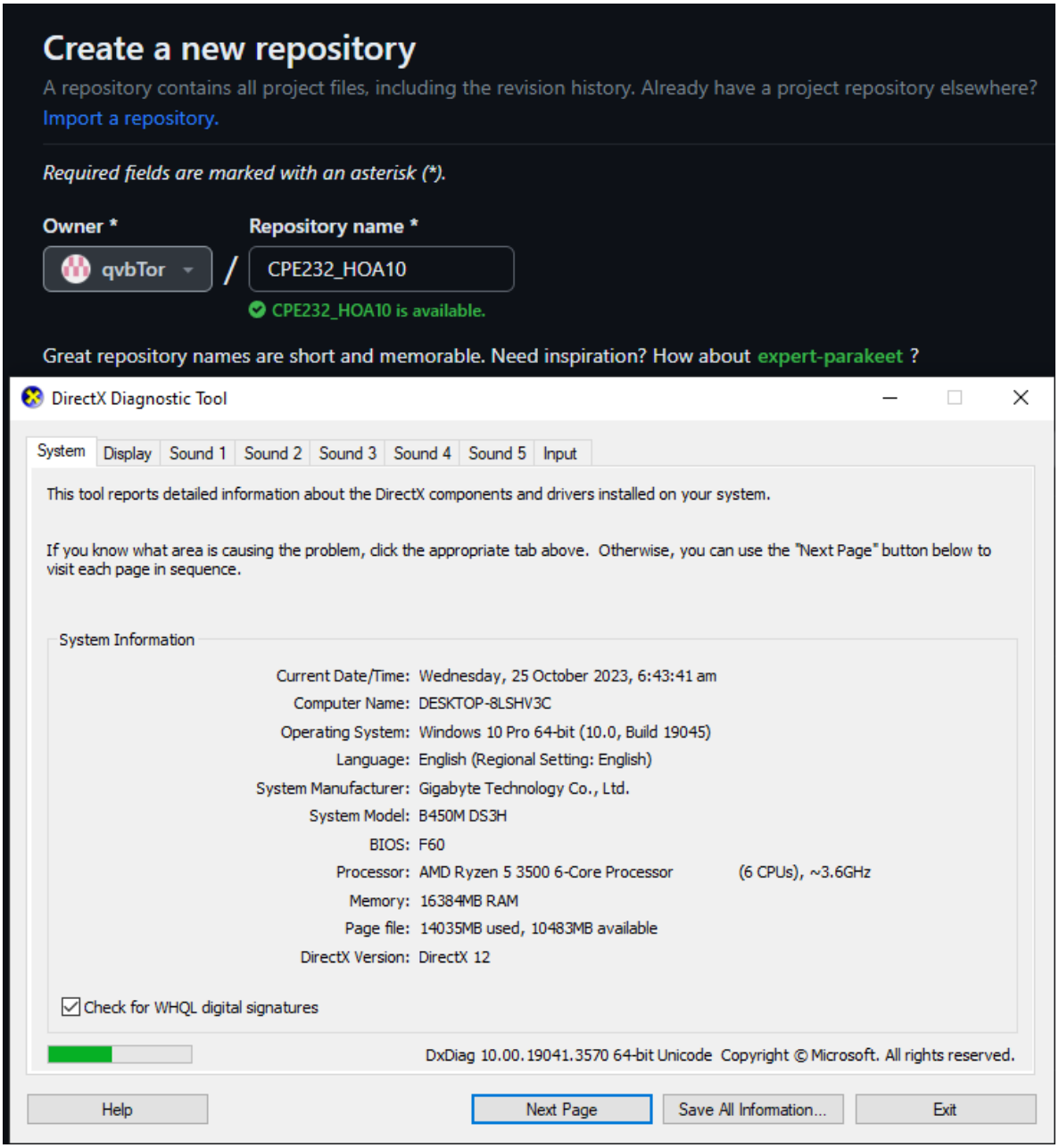
Source: https://www.graylog.org/products/open-source

3. Tasks

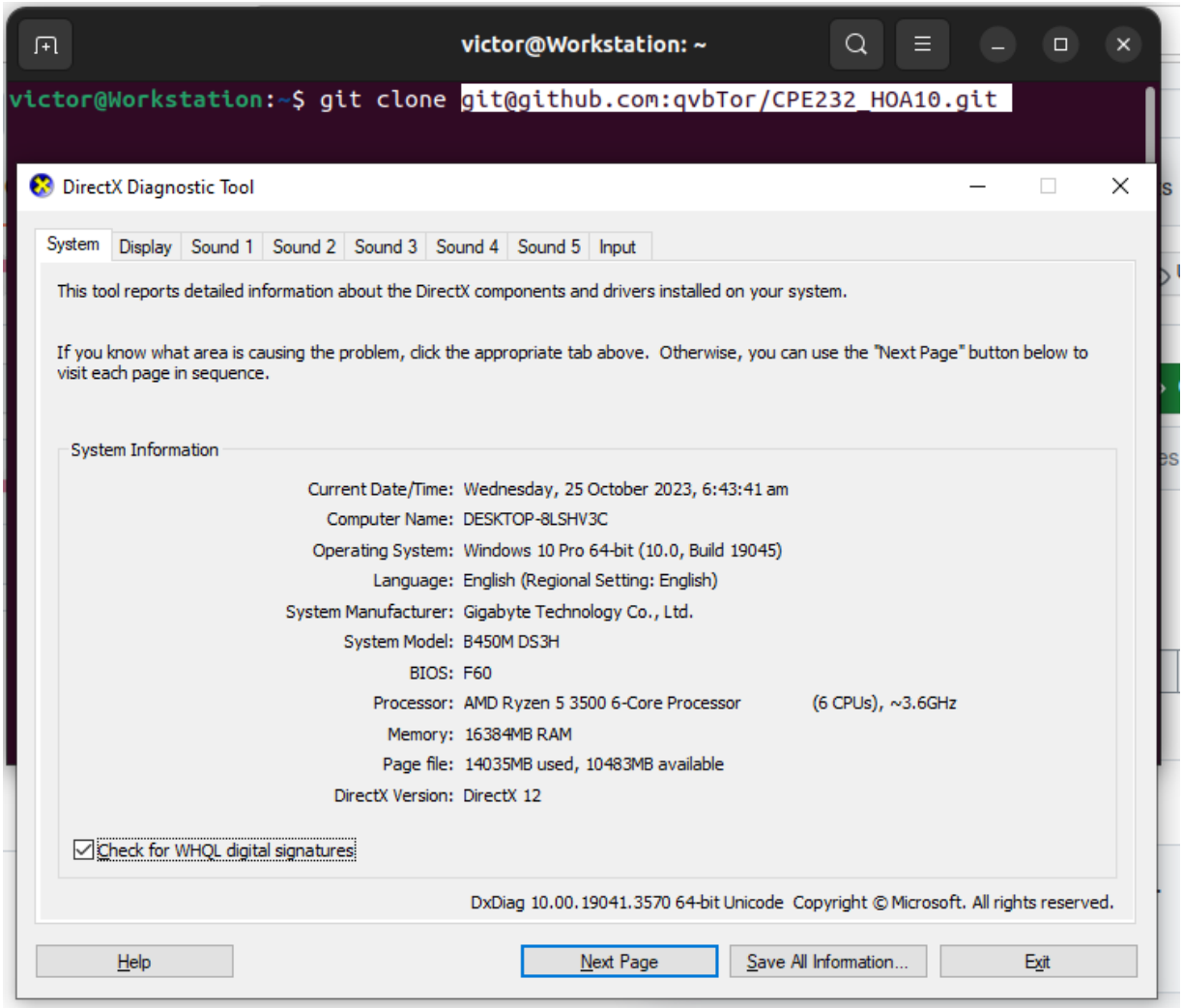
1. Create a playbook that:
    a. Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)
2. Apply the concept of creating roles.
3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like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

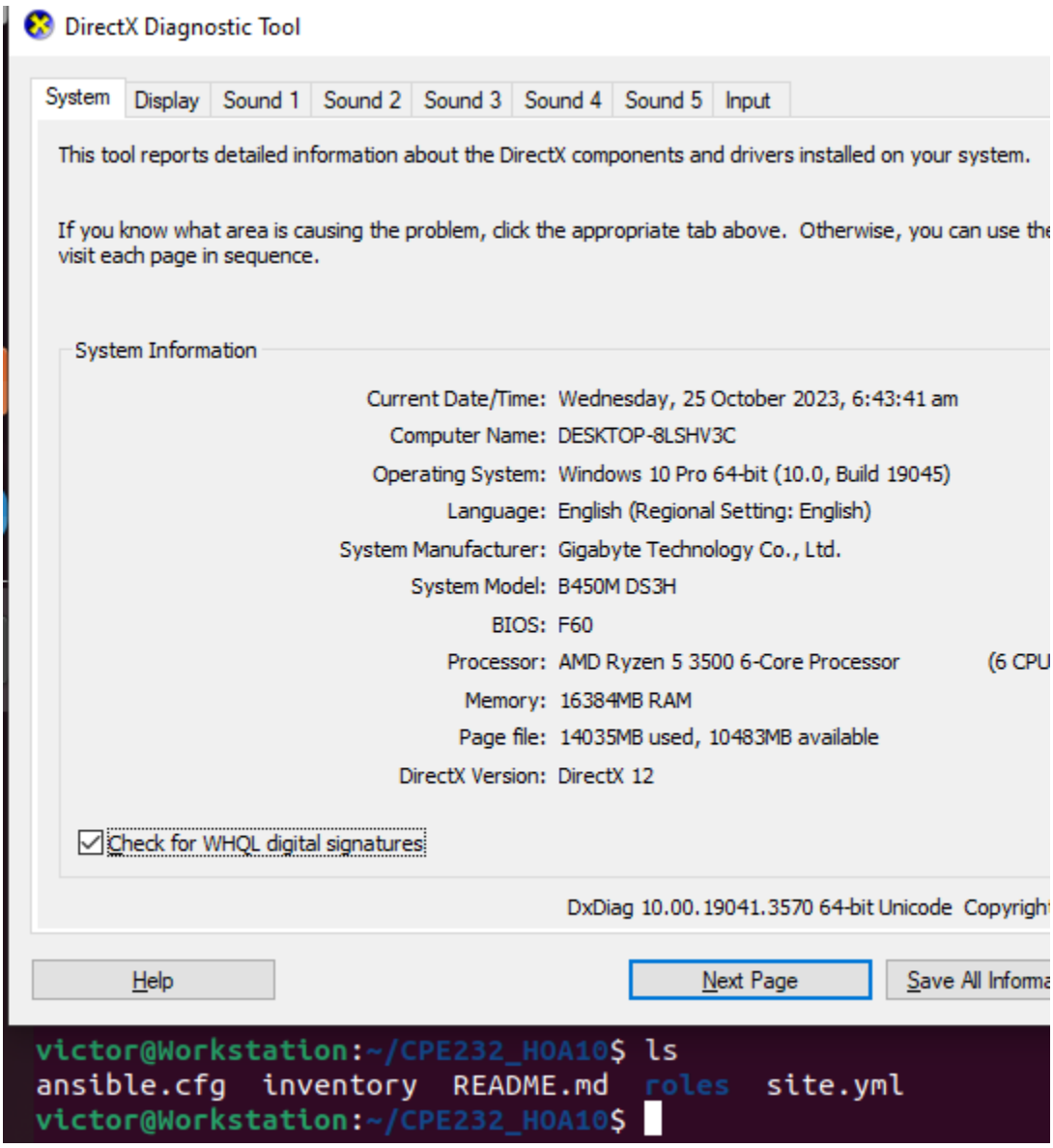
Step 1: Making a repository.



Step 2: git cloning.



Step 3: Setting up for playbook such as ansible.cfg and inventory then creating galaxy as well.



```
victor@Workstation:~/
victor@Workstation:~$
victor@Workstation:~/
.
├── ansible.cfg
├── inventory
├── README.md
├── roles
│   ├── centos_ela
│   │   └── main.yml
│   ├── defaults
│   │   └── main.yml
│   ├── handlers
│   │   └── main.yml
│   ├── meta
│   │   └── main.yml
│   ├── README.md
│   ├── tasks
│   │   └── main.yml
│   ├── tests
│   │   └── main.yml
│   ├── ubuntu_ela
│   │   └── main.yml
│   └── vars
│       └── main.yml
└── site.yml

9 directories, 13 fil
victor@Workstation:~/
```

DirectX Diagnostic Tool

System | Display | Sound 1 | Sound 2 | Sound 3 | Sound 4 | Sound 5 | 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 the "Next Page" but visit each page in sequence.

System Information

Current Date/Time:	Wednesday, 25 October 2023, 6:43:41 am
Computer Name:	DESKTOP-8LSHV3C
Operating System:	Windows 10 Pro 64-bit (10.0, Build 19045)
Language:	English (Regional Setting: English)
System Manufacturer:	Gigabyte Technology Co., Ltd.
System Model:	B450M DS3H
BIOS:	F60
Processor:	AMD Ryzen 5 3500 6-Core Processor (6 CPUs), ~3.6GHz
Memory:	16384MB RAM
Page file:	14035MB used, 10483MB available
DirectX Version:	DirectX 12

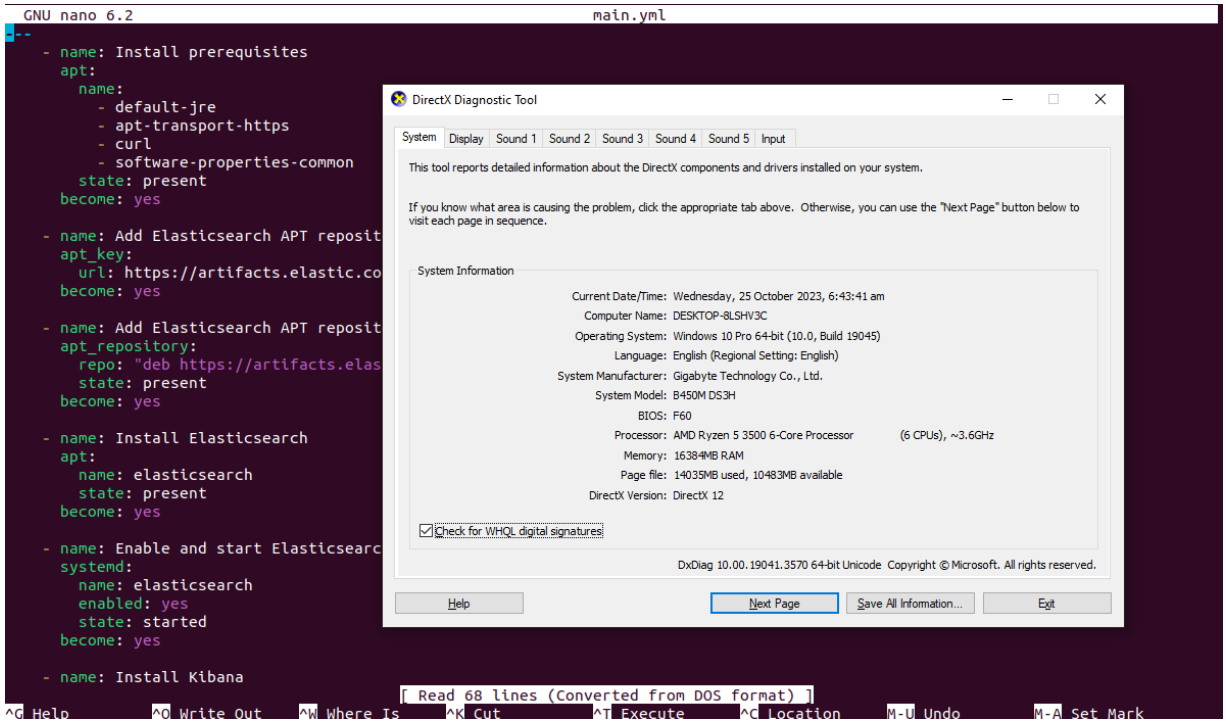
☑ Check for WHQL digital signatures

DxDiag 10.00.19041.3570 64-bit Unicode Copyright © Microsoft. All

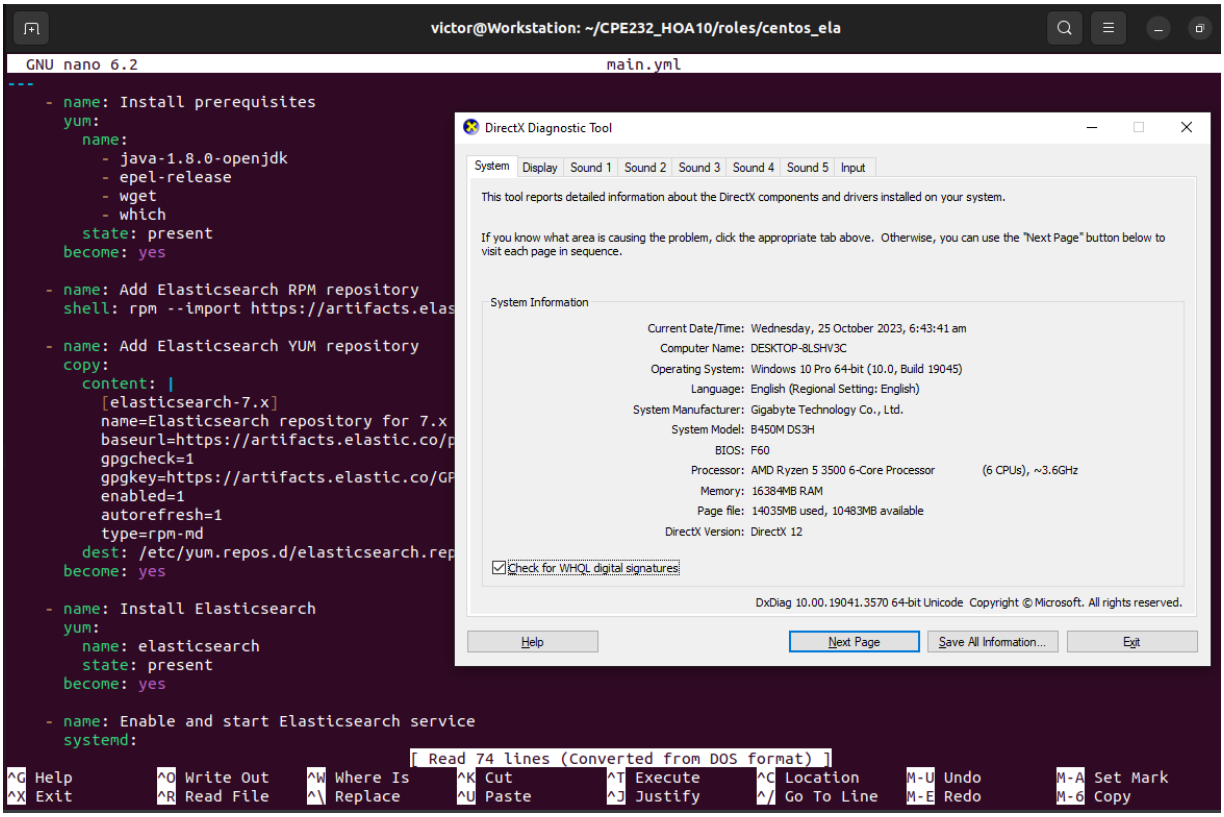
Help | Next Page | Save All Information...

Step 4. Creating main.yml, and adding installation command of prometheus both ubuntu and centos.

Ubuntu:



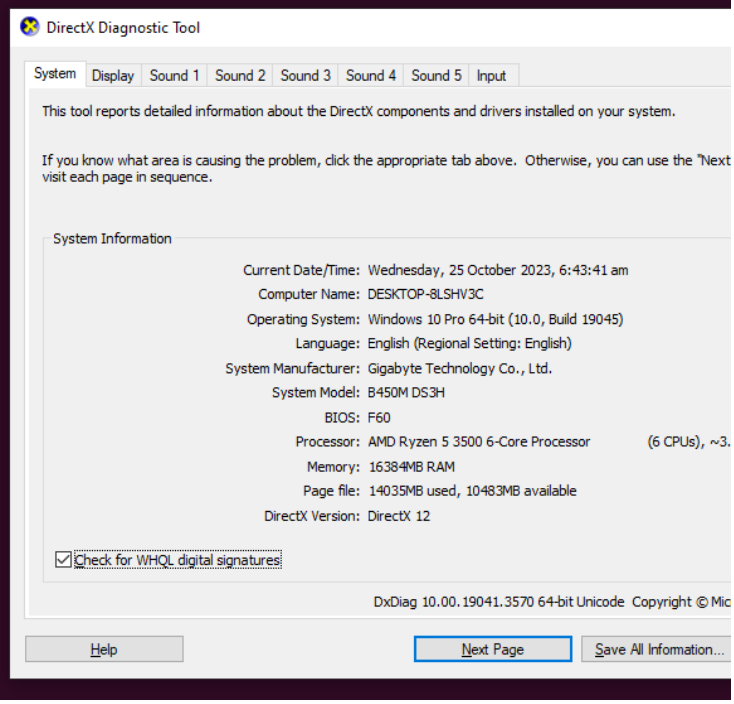
CentOS:


victor@Workstation: ~/CPE232_HOA10/roles/centos_ela
GNU nano 6.2
main.yml

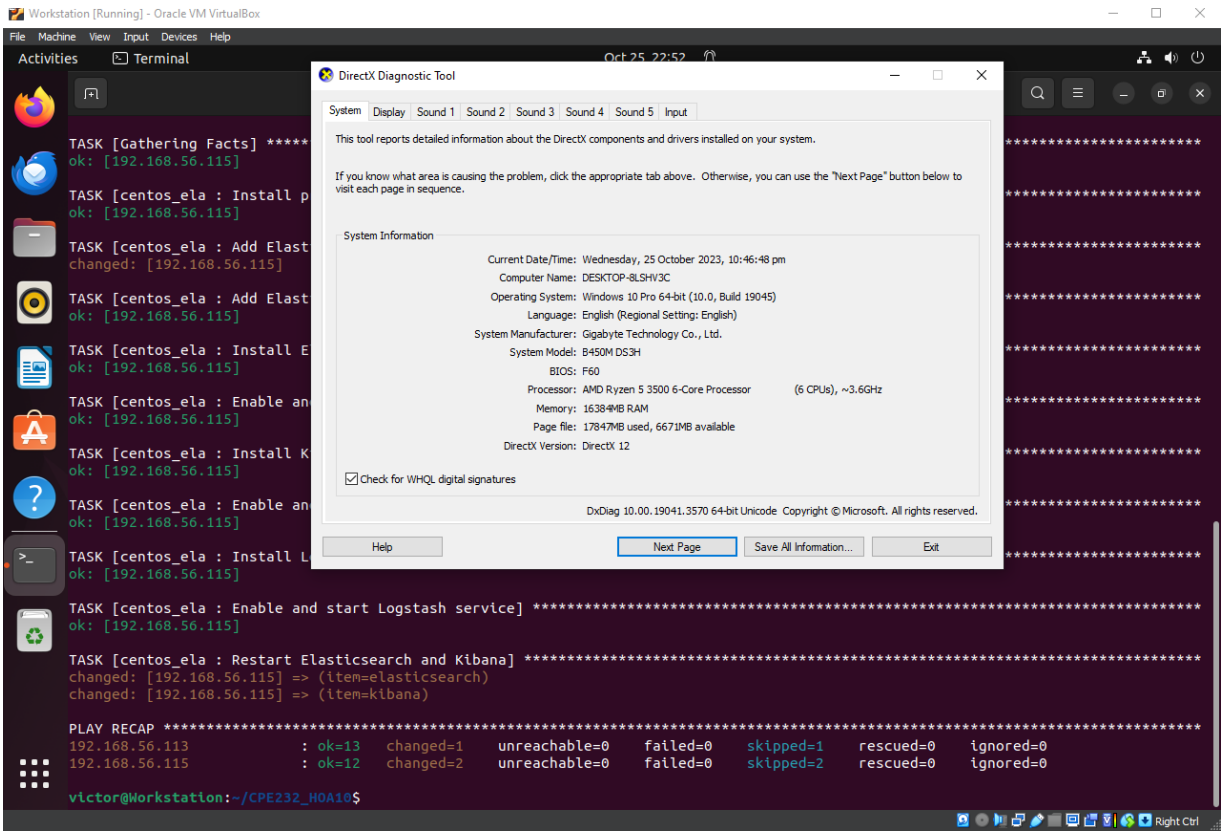
- name: Install prerequisites
yum:
name:
- java-1.8.0-openjdk
- epel-release
- wget
- which
state: present
become: yes
- name: Add Elasticsearch RPM repository
shell: rpm --import https://artifacts.elas
- name: Add Elasticsearch YUM repository
copy:
content: |
[elasticsearch-7.x]
name=Elasticsearch repository for 7.x
baseurl=https://artifacts.elastic.co/p
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GP
enabled=1
autorefresh=1
type=rpm-md
dest: /etc/yum.repos.d/elasticsearch.rep
become: yes
- name: Install Elasticsearch
yum:
name: elasticsearch
state: present
become: yes
- name: Enable and start Elasticsearch service
systemd:
[Read 74 lines (Converted from DOS format)]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy
DirectX Diagnostic Tool
System Display Sound 1 Sound 2 Sound 3 Sound 4 Sound 5 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 the "Next Page" button below to visit each page in sequence.
System Information
Current Date/Time: Wednesday, 25 October 2023, 6:43:41 am
Computer Name: DESKTOP-8LSHV3C
Operating System: Windows 10 Pro 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: Gigabyte Technology Co., Ltd.
System Model: B450M DS3H
BIOS: F60
Processor: AMD Ryzen 5 3500 6-Core Processor (6 CPUs), ~3.6GHz
Memory: 16384MB RAM
Page file: 14035MB used, 10483MB available
DirectX Version: DirectX 12
Check for WHQL digital signatures
DxDiag 10.00.19041.3570 64-bit Unicode Copyright © Microsoft. All rights reserved.
Help
Next Page
Save All Information...
Exit

Setup 5: Calling the main.yml under centos_prm and ubuntu_prm directories using roles.

```
GNU nano 6.2                                        site.yml *
- hosts: all
  become: true
  pre_tasks:

  - name: install updates (CentOS)
    dnf:
      update_only: yes
      update_cache: yes
    when: ansible_distribution == "Centos"

  - name: install updates (Ubuntu)
    apt:
      upgrade: dist
      update_cache: yes
    when: ansible_distribution == "Ubuntu"

- hosts: ubuntu
  become: true
  roles:
    - ubuntu_ela

- hosts: centos
  become: true
  roles:
    - centos_ela
```



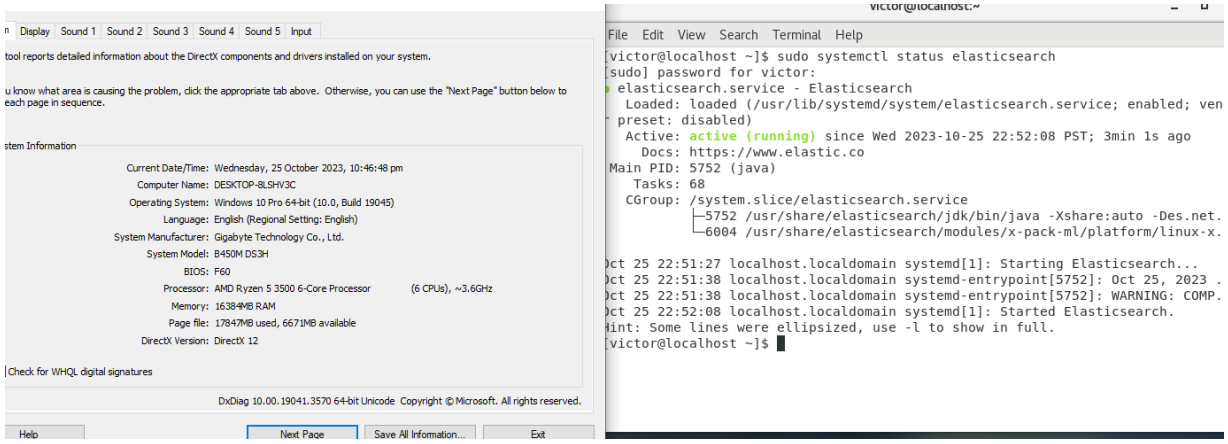
Step 7: Run the playbook.



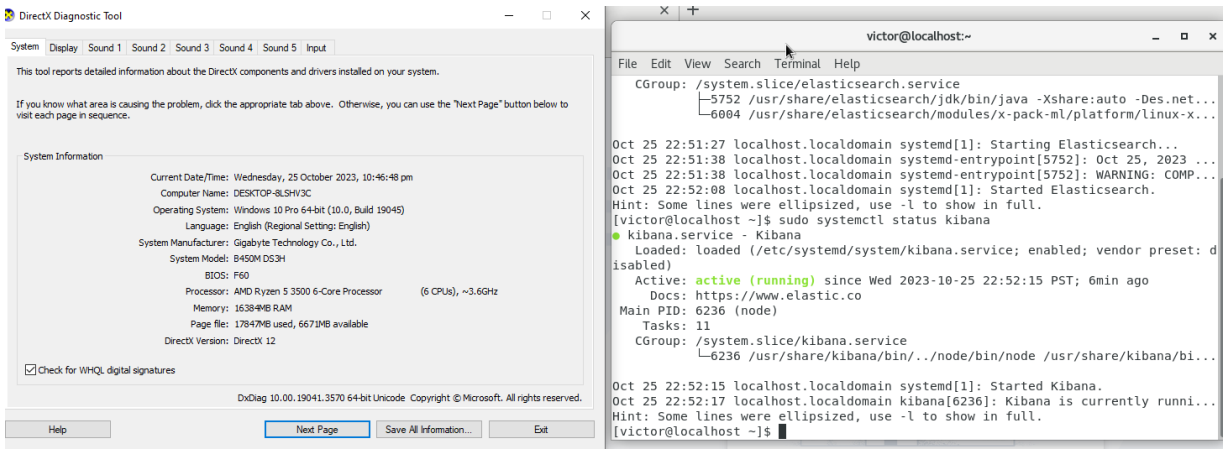
Step 8: Checking if the elasticsearch, kibana and logstach are installed.

CentOS (Server 2):

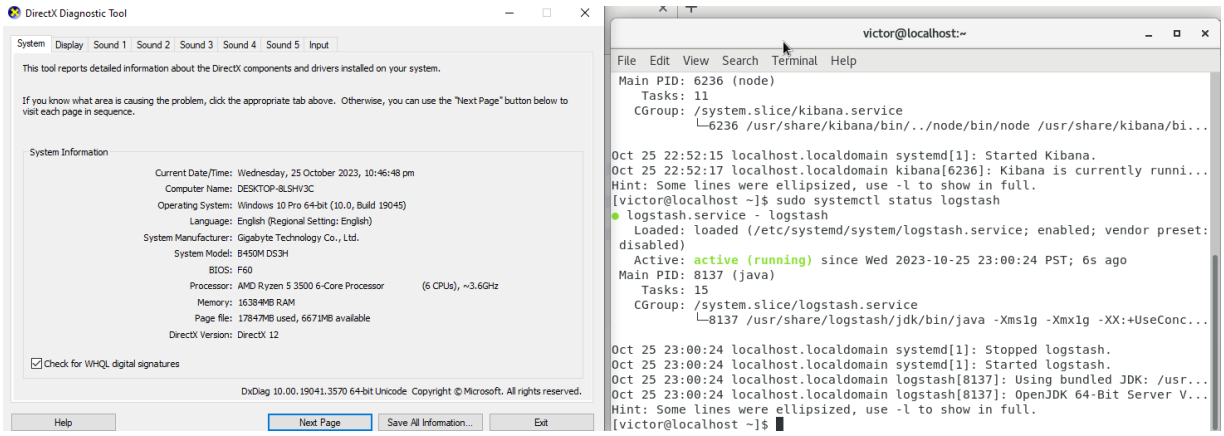
1. elasticsearch:



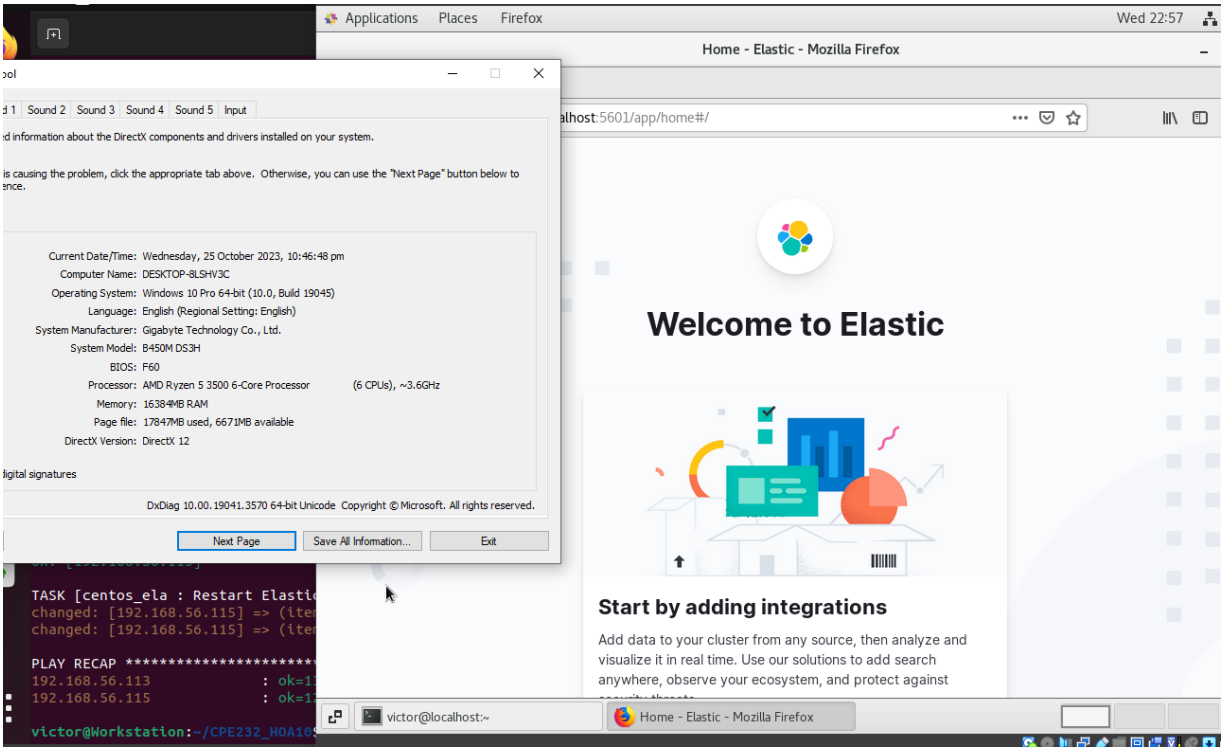
2. Kibana:



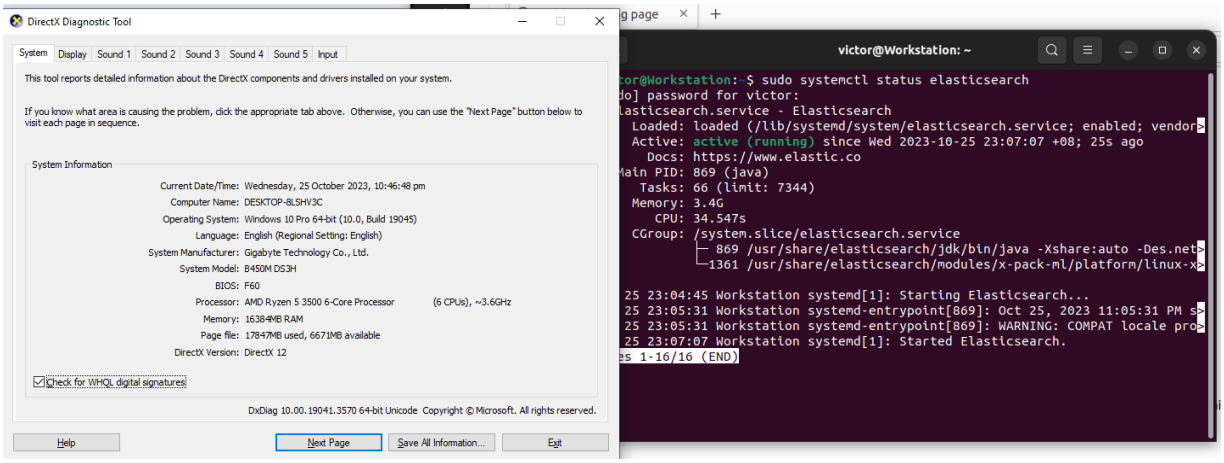
3. logstash

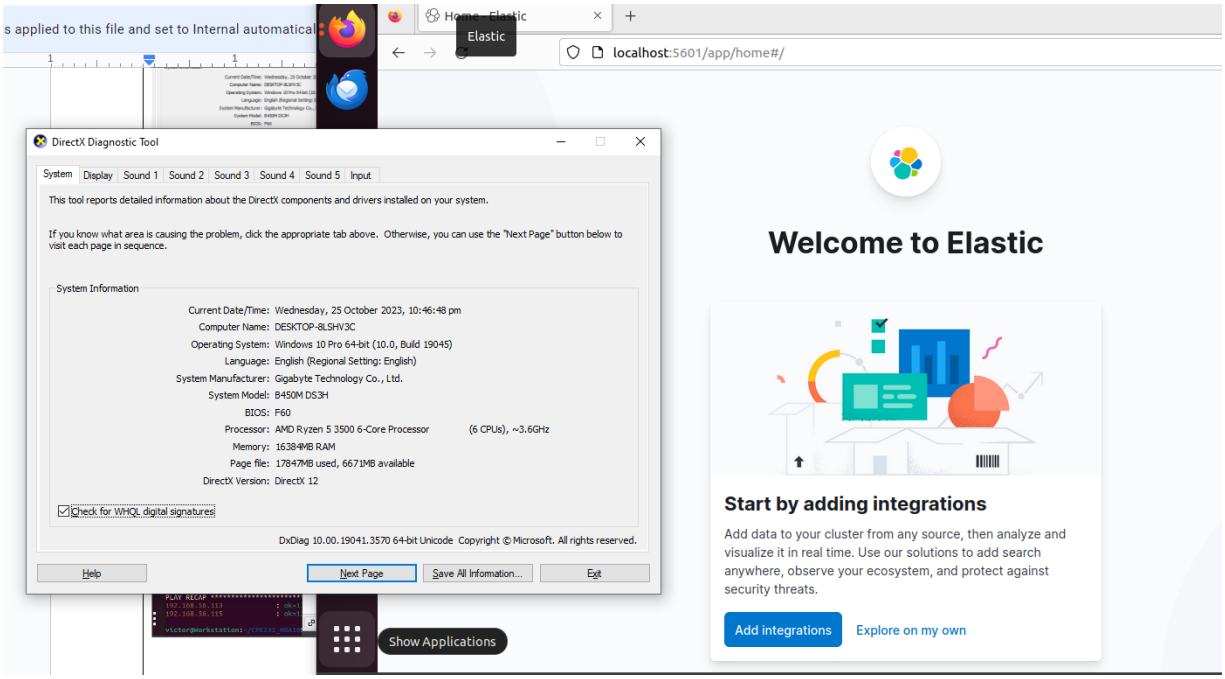


4. localhost:5601

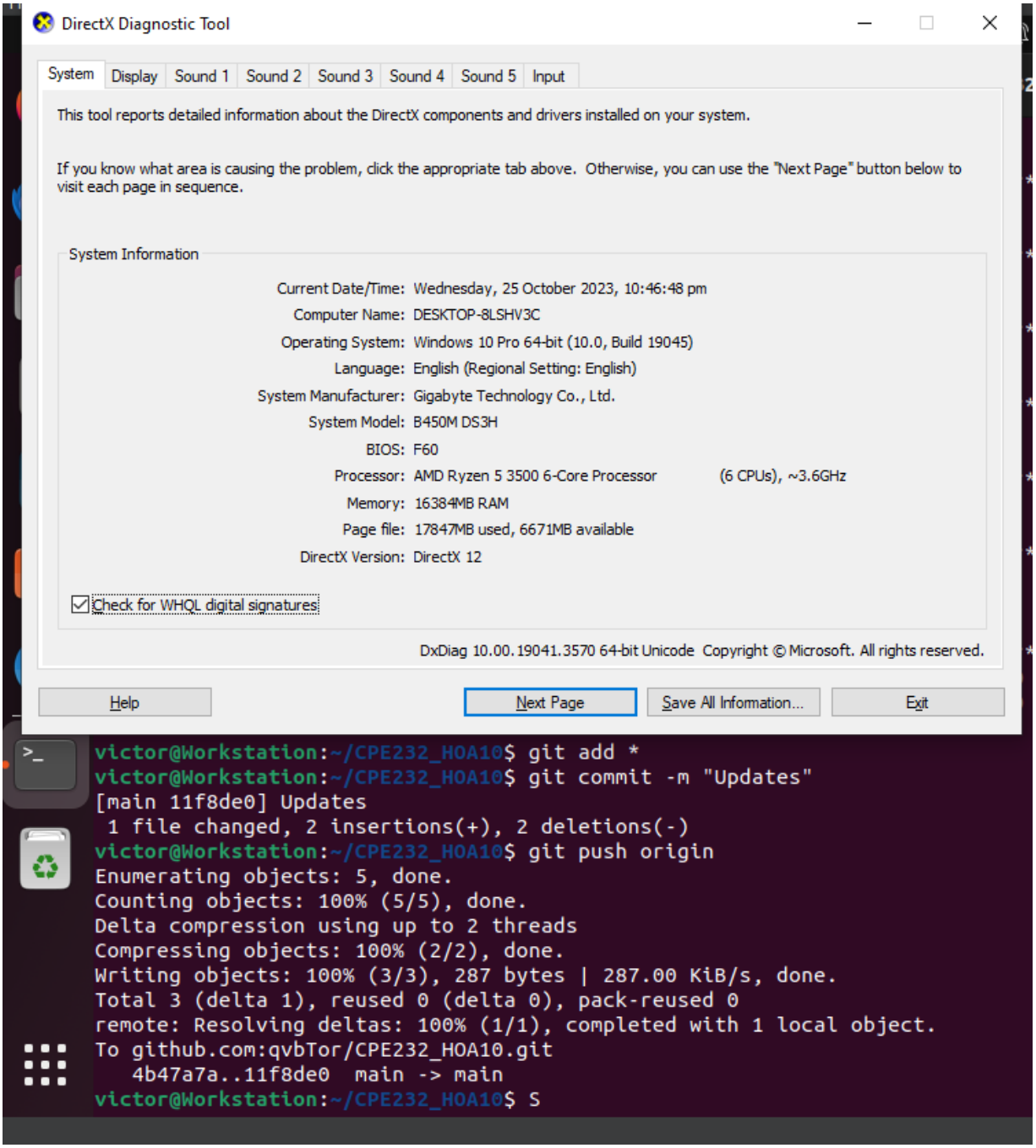


Ubuntu (Server 3):





Step 9: Updating repository in GitHub.



Reflections:

Answer the following:

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

Log monitoring tools empower system administration teams to proactively identify and resolve issues, optimize system performance, and enhance security. By collecting and analyzing log data from disparate systems, these tools provide actionable insights into resource utilization, compliance adherence, and potential security threats. Additionally, they automate alerts and streamline log analysis, contributing to overall system reliability and resilience.

Conclusions:

Implementing a log monitoring tool such as Elasticsearch, Kibana, and Logstash provides real-time issue detection, efficient troubleshooting, and enhanced security. These tools enable centralized log analysis, automate alerts, and contribute to optimal system performance, ensuring a resilient and secure system administration environment.