

<b>Name:</b> Victor B. Ortega	<b>Date Performed:</b> 10/25/2023
<b>Course/Section:</b> CPE31S5	<b>Date Submitted:</b> 10/25/2023
<b>Instructor:</b> Engr. Roman Richard	<b>Semester and SY:</b> 2023-2024
<b>Activity 10: Install, Configure, and Manage Log Monitoring tools</b>	
<b>1. Objectives</b>	
Create and design a workflow that installs, configure and manage enterprise log monitoring tools using Ansible as an Infrastructure as Code (IaC) tool.	
<b>2. Discussion</b>	
<p>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.</p> <p>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.</p> <p>To qualify for inclusion in the Log Monitoring category, a product must:</p> <ul style="list-style-type: none"> <li>• Monitor the log files generated by servers, applications, or networks</li> <li>• Alert users when important events are detected</li> <li>• Provide reporting capabilities for log files</li> </ul> <p><b>Elastic Stack</b></p> <p>ELK suite stands for Elasticsearch, Kibana, Beats, and Logstash (also known as the ELK Stack). Source: <a href="https://www.elastic.co/elastic-stack">https://www.elastic.co/elastic-stack</a></p> <p>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.</p> <p><b>GrayLog</b></p>	

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)

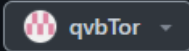
## Step 1: Making a repository.

### Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? [Import a repository.](#)

*Required fields are marked with an asterisk (\*).*

Owner \*

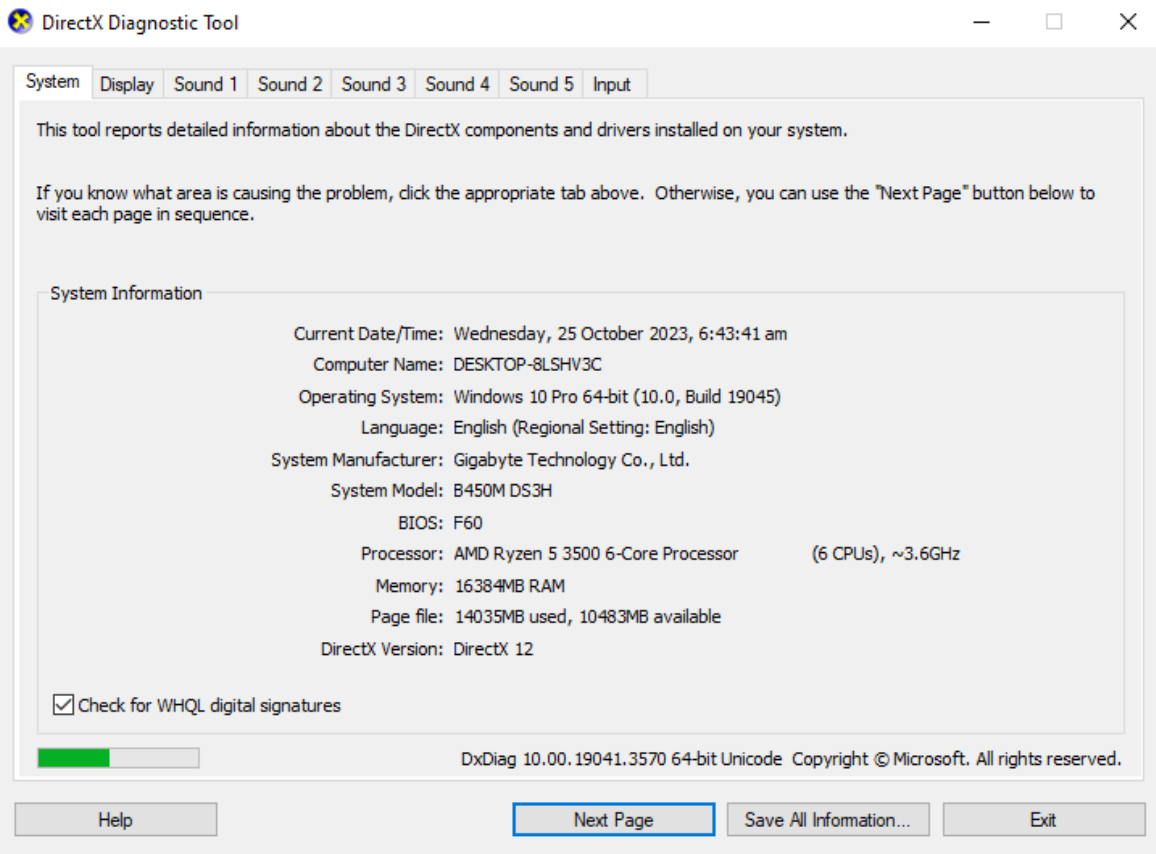


Repository name \*

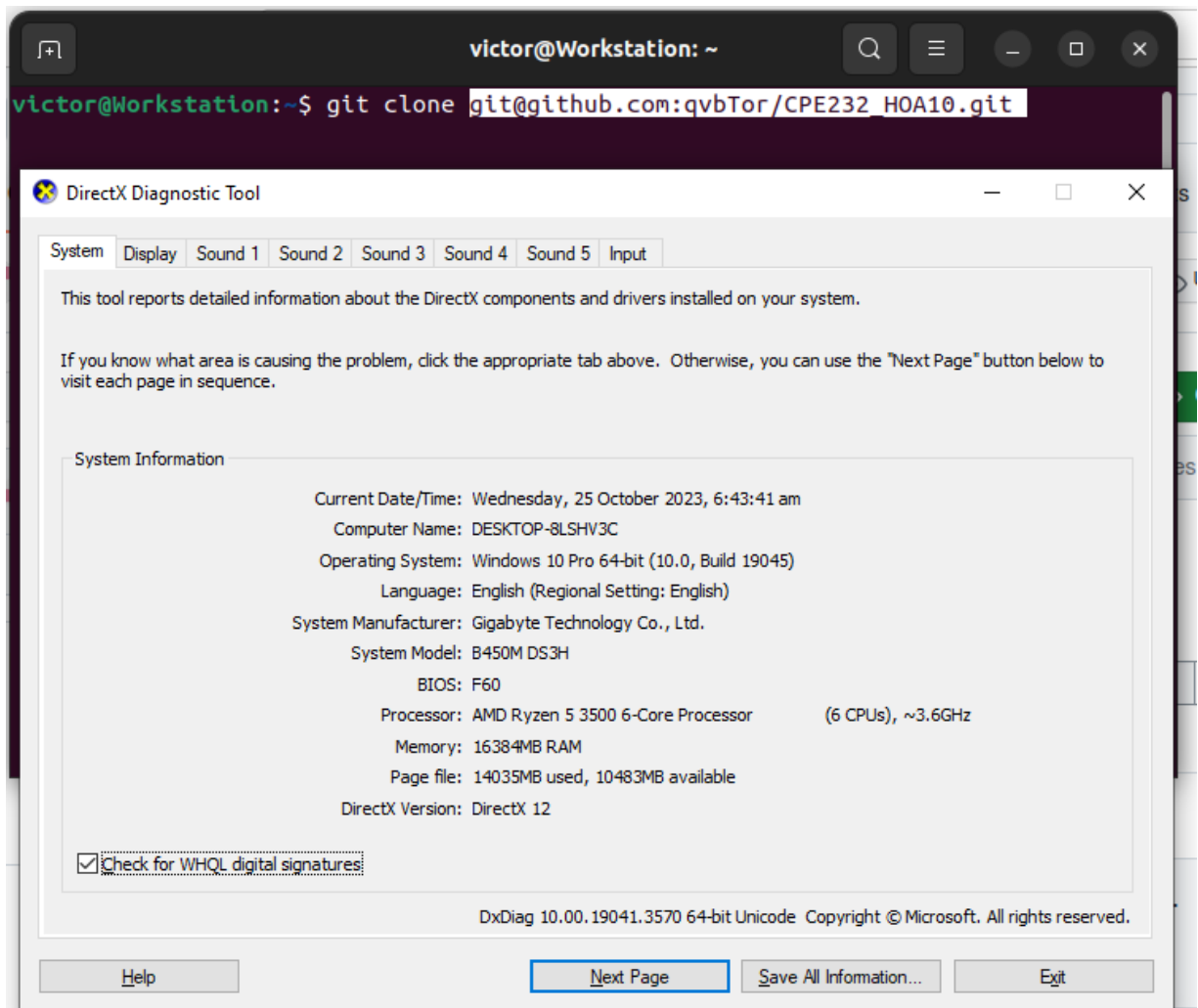
CPE232\_HOA10

✓ CPE232\_HOA10 is available.

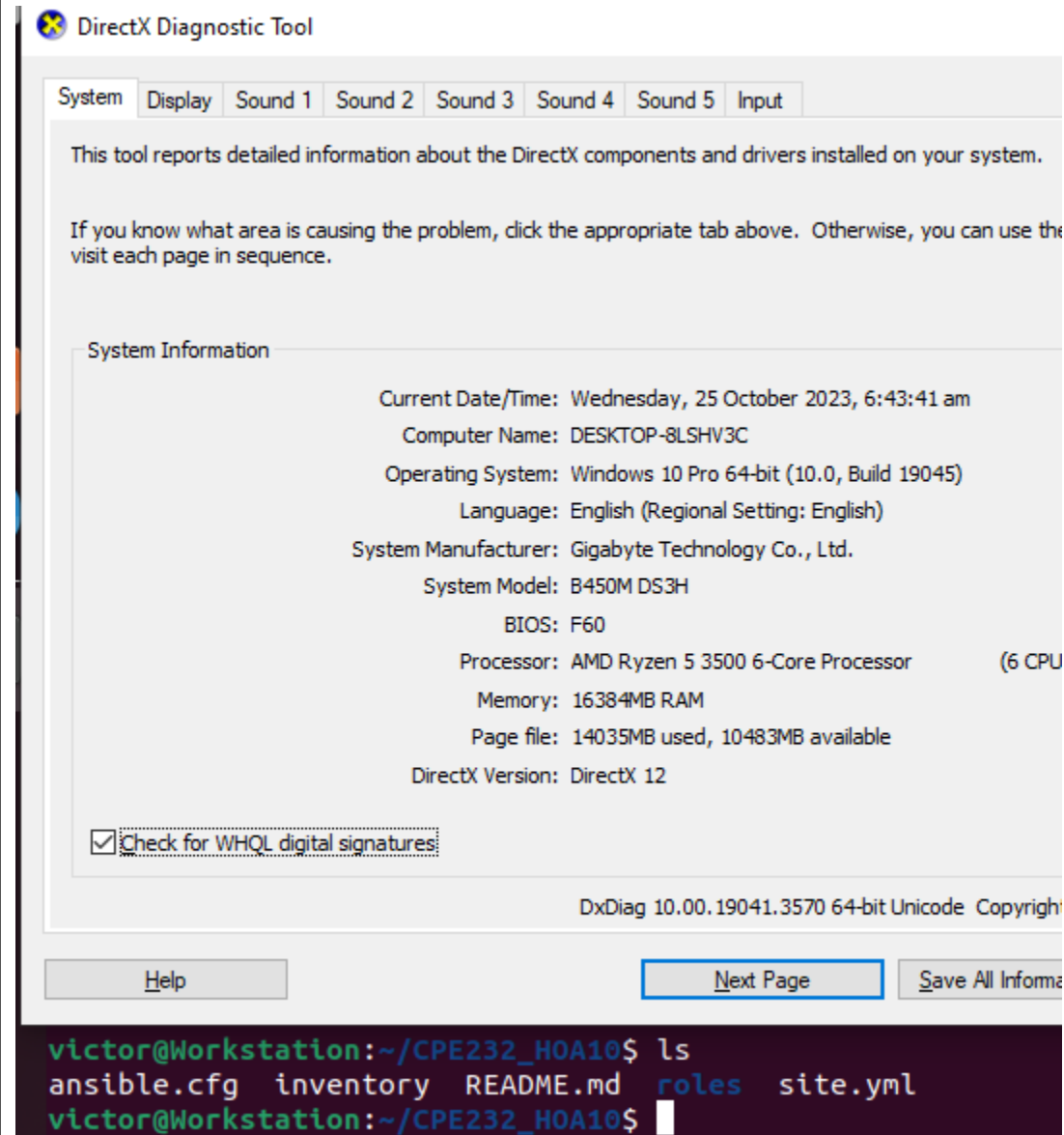
Great repository names are short and memorable. Need inspiration? How about [expert-parakeet](#) ?



Step 2: git cloning.



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



The image shows a Windows window titled "DirectX Diagnostic Tool". It has several tabs: "System", "Display", "Sound 1", "Sound 2", "Sound 3", "Sound 4", "Sound 5", and "Input". The "System" tab is selected. The window contains the following text:

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 tool 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)  
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 (c) 2009 Microsoft Corporation. All rights reserved.

Buttons at the bottom: Help, Next Page, Save All Information

```
victor@Workstation:~/CPE232_H0A10$ ls
ansible.cfg  inventory  README.md  roles  site.yml
victor@Workstation:~/CPE232_H0A10$
```

```
centos_ela defaults
victor@Workstation:~/
victor@Workstation:~/S
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:

```
GNU nano 6.2 main.yml
--
- name: Install prerequisites
  apt:
    name:
      - default-jre
      - apt-transport-https
      - curl
      - software-properties-common
    state: present
    become: yes

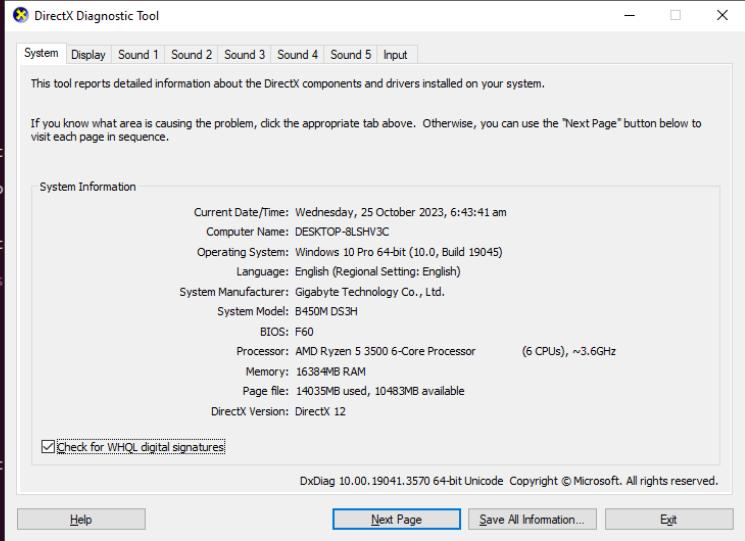
- name: Add Elasticsearch APT repository
  apt_key:
    url: https://artifacts.elastic.co
  become: yes

- name: Add Elasticsearch APT repository
  apt_repository:
    repo: "deb https://artifacts.elastic.co
    state: present
    become: yes

- name: Install Elasticsearch
  apt:
    name: elasticsearch
    state: present
    become: yes

- name: Enable and start Elasticsearch
  systemd:
    name: elasticsearch
    enabled: yes
    state: started
    become: yes

- name: Install Kibana
  Read 68 lines (Converted from DOS format)
^O Help ^O Write Out ^O Where Is ^K Cut ^T Execute ^d Location M-U Undo M-A Set Mark
```



The screenshot shows a Windows window titled "DirectIX Diagnostic Tool". It has tabs for "System", "Display", "Sound 1", "Sound 2", "Sound 3", "Sound 4", "Sound 5", and "Input". The "System" tab is selected. The window contains the following text:

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.

Buttons: Help, Next Page, Save All Information..., Exit

## CentOS:

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.elastic.co/gpg/public-key-gpg-7.x.gpg

- name: Add Elasticsearch YUM repository
  copy:
    content: |
      [elasticsearch-7.x]
      name=Elasticsearch repository for 7.x
      baseurl=https://artifacts.elastic.co/gpg/public-key-gpg-7.x.gpg
      gpgkey=https://artifacts.elastic.co/gpg/public-key-gpg-7.x.gpg
      enabled=1
      autorefresh=1
      type=rpm-md
    dest: /etc/yum.repos.d/elasticsearch.repo
    become: yes

- name: Install Elasticsearch
  yum:
    name: elasticsearch
    state: present
    become: yes

- name: Enable and start Elasticsearch service
  systemd:
    name: elasticsearch
    state: started
    enabled: true
```

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

Read 74 lines (Converted from DOS format)

Help Write Out Where Is Cut Execute Location M-U Undo M-A Set Mark  
Exit Read File Replace Paste Justify Go To Line M-E Redo M-G Copy



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
```

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" 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.
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 © Mic

Help | Next Page | Save All Information...

## Step 7: Run the playbook.

The screenshot shows a VirtualBox Workstation window titled "Workstation [Running] - Oracle VM VirtualBox". The interface includes a menu bar (File, Machine, View, Input, Devices, Help), an "Activities" sidebar with application icons, and a main terminal window. The terminal displays the output of an Ansible playbook, showing several tasks completed successfully (ok) and a final "PLAY RECAP" summary.

Overlaid on the terminal is the "DirectX Diagnostic Tool" window. It has tabs for System, Display, Sound 1, Sound 2, Sound 3, Sound 4, Sound 5, and Input. The "System" tab is active, showing system information and a "Check for WHQL digital signatures" checkbox.

**Terminal Output:**

```
TASK [Gathering Facts] *****
ok: [192.168.56.115]

TASK [centos_ela : Install p] *****
ok: [192.168.56.115]

TASK [centos_ela : Add Elast] *****
changed: [192.168.56.115]

TASK [centos_ela : Add Elast] *****
ok: [192.168.56.115]

TASK [centos_ela : Install E] *****
ok: [192.168.56.115]

TASK [centos_ela : Enable an] *****
ok: [192.168.56.115]

TASK [centos_ela : Install K] *****
ok: [192.168.56.115]

TASK [centos_ela : Enable an] *****
ok: [192.168.56.115]

TASK [centos_ela : Install L] *****
ok: [192.168.56.115]

TASK [centos_ela : Enable and start Logstash service] *****
ok: [192.168.56.115]

TASK [centos_ela : Restart Elasticsearch and Kibana] *****
changed: [192.168.56.115] => (item=elasticsearch)
changed: [192.168.56.115] => (item=kibana)

PLAY RECAP *****
192.168.56.113      : ok=13  changed=1  unreachable=0  failed=0  skipped=1  rescued=0  ignored=0
192.168.56.115      : ok=12  changed=2  unreachable=0  failed=0  skipped=2  rescued=0  ignored=0

victor@Workstation: ~/CPE232_H0A10$
```

**DirectX Diagnostic Tool - System Information:**

- Current Date/Time: Wednesday, 25 October 2023, 10:46:48 pm
- Computer Name: DESKTOP-BLSHV3C
- 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: 17847MB used, 6671MB available
- DirectX Version: DirectX 12

☒ Check for WHQL digital signatures

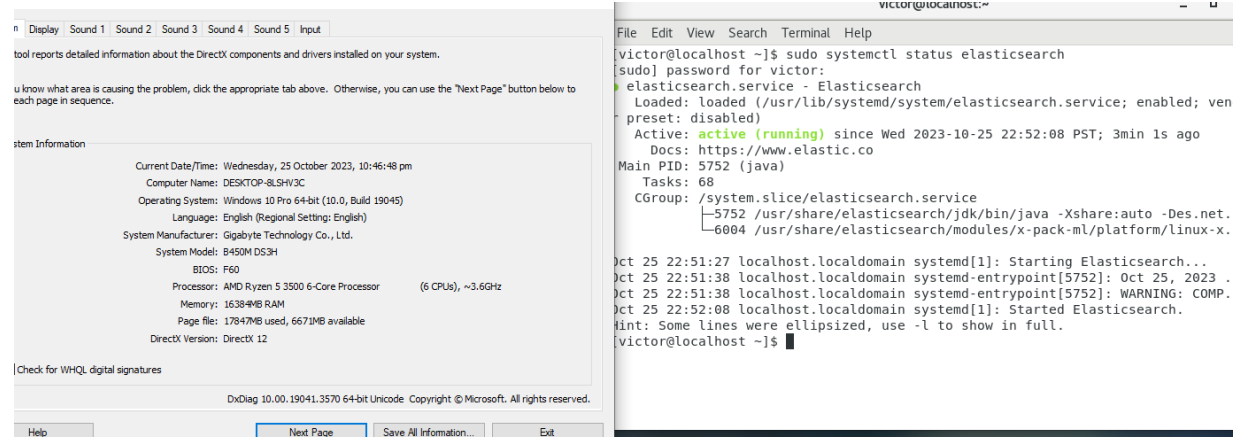
DxDiag 10.00.19041.3570 64-bit Unicode Copyright © Microsoft. All rights reserved.

Buttons: Help, Next Page, Save All Information..., Exit

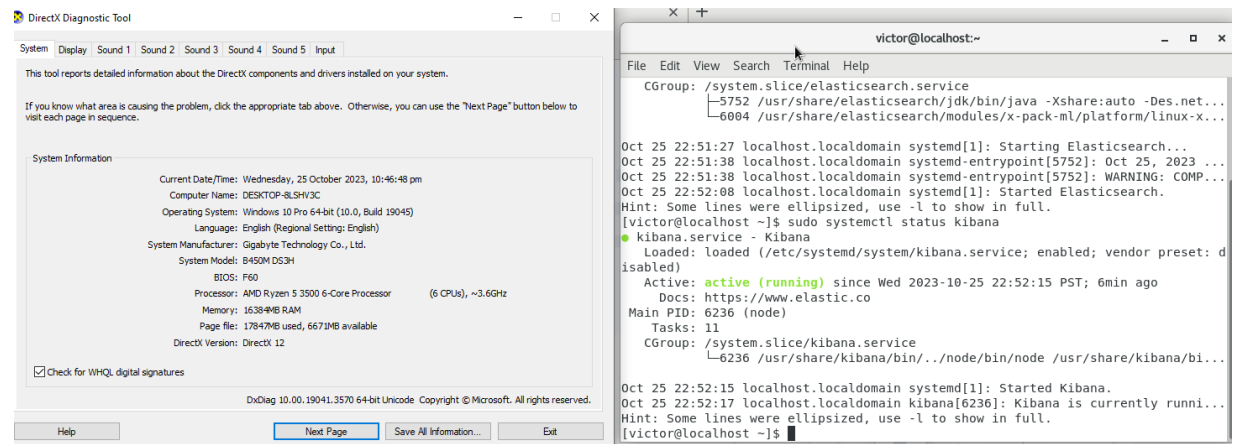
## Step 8: Checking if the elasticsearch, kibana and logstash are installed.

### CentOS (Server 2):

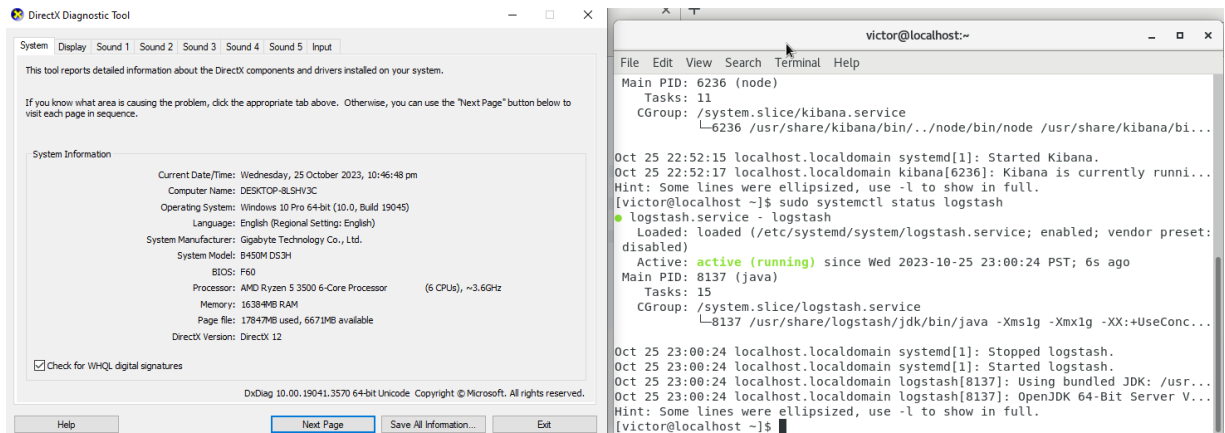
#### 1. elasticsearch:



#### 2. Kibana:



### 3. logstash



DirectX Diagnostic Tool

System Information

Current Date/Time: Wednesday, 25 October 2023, 10:46:48 pm  
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: 17847MB used, 6671MB available  
DirectX Version: DirectX 12

Check for WHQL digital signatures

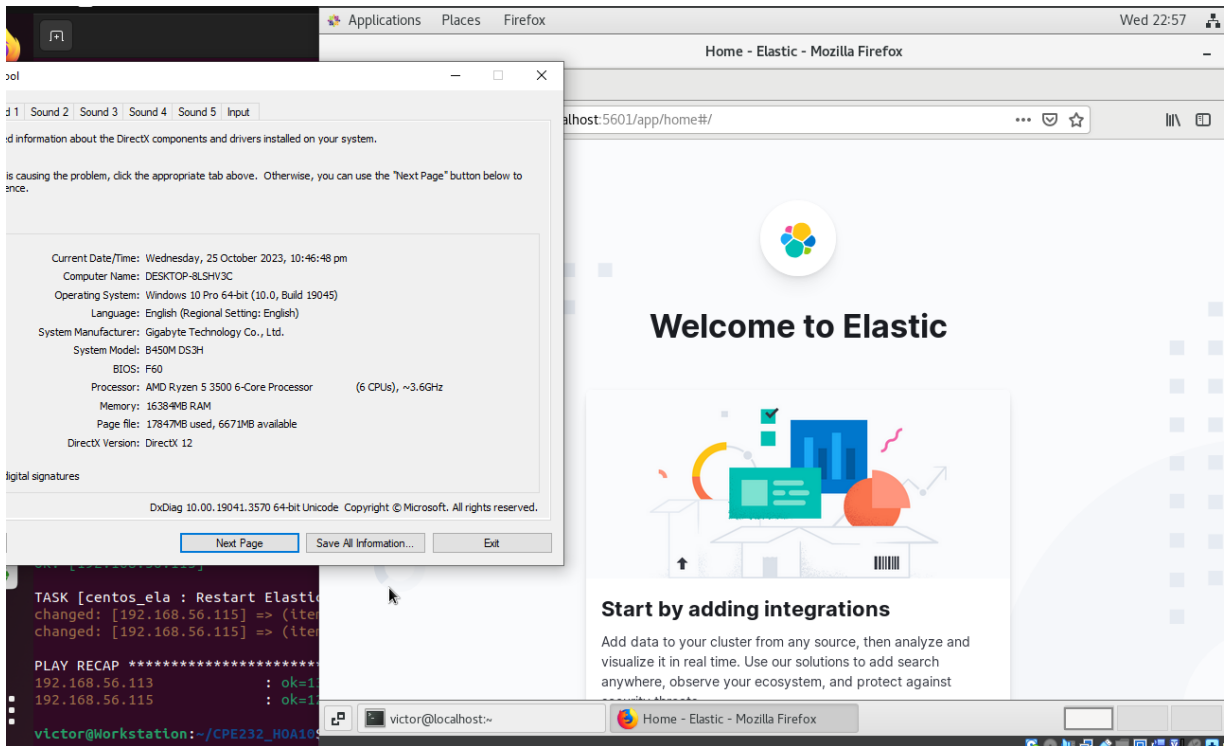
DxDiag 10.00.19041.3570 64-bit Unicode Copyright © Microsoft. All rights reserved.

Help Next Page Save All Information... Exit

terminal

```
victor@localhost:~$ sudo systemctl status logstash
logstash.service - logstash
Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabled)
Active: active (running) since Wed 2023-10-25 23:00:24 PST; 6s ago
Main PID: 8137 (java)
Tasks: 15
CGroup: /system.slice/logstash.service
└─8137 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConc...
```

### 4. localhost:5601



Applications Places Firefox

Home - Elastic - Mozilla Firefox

Wed 22:57

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.

TASK [centos\_elas : Restart Elasticsearch] changed: [192.168.56.115] => (item)

PLAY RECAP \*\*\*\*\* 192.168.56.113 : ok=1 192.168.56.115 : ok=1

victor@Workstation:~/CPE232\_HOA10

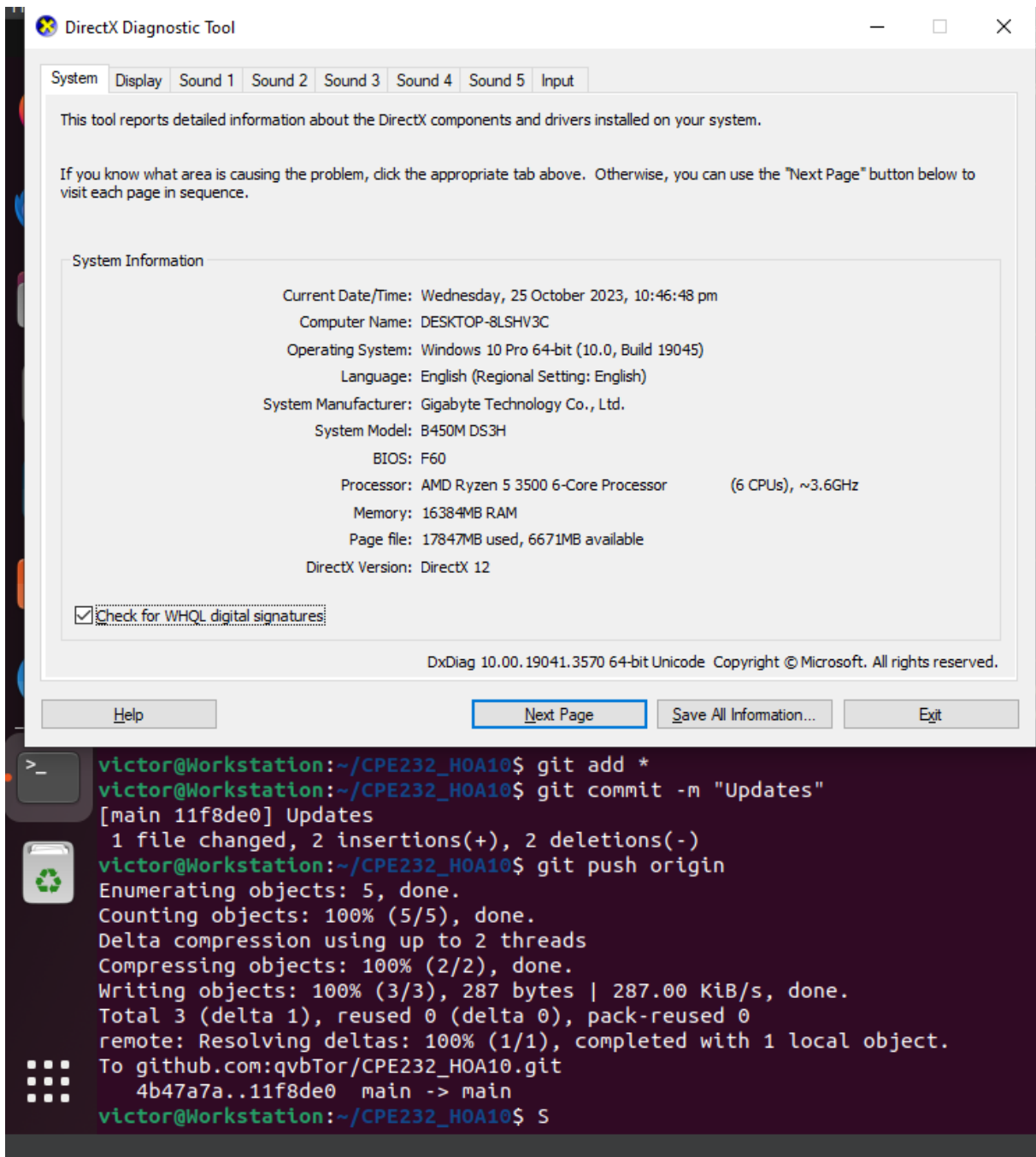
## Ubuntu (Server 3):

The screenshot displays the Ubuntu Server 3 environment. In the foreground, the DirectX Diagnostic Tool is open, showing system information: Current Date/Time: Wednesday, 25 October 2023, 10:46:48 pm; Computer Name: DESKTOP-8L5HV3C; 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: 17847MB used, 6671MB available; DirectX Version: DirectX 12. The tool also includes a checkbox for 'Check for WHQL digital signatures' and buttons for 'Help', 'Next Page', 'Save All Information...', and 'Exit'.

In the background, a terminal window shows the command `sudo systemctl status elasticsearch` being executed. The output indicates that the `elasticsearch.service` is loaded, enabled, and active (running) since Wednesday, 2023-10-25 23:07:07 +08; 25s ago. The main PID is 869 (java). The tasks are 66 (limit: 7344). The memory is 3.4G. The CPU is 34.547s. The CGroup is `/system.slice/elasticsearch.service`. The service is running on `869 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.net` and `1361 /usr/share/elasticsearch/modules/x-pack-nl/platform/linux-x86_64/bin/java`. The log shows the service starting at 23:04:45, the endpoint starting at 23:05:31, and a warning about COMPAT locale properties at 23:05:31. The service started at 23:07:07.

Below the terminal, the Elasticsearch interface is visible. It shows a 'Welcome to Elastic' message and a 'Start by adding integrations' section. The interface includes a search bar, a 'Show Applications' button, and a 'Welcome to Elastic' message. The 'Start by adding integrations' section includes a description: '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.' and two buttons: 'Add integrations' and 'Explore on my own'.

## Step 9: Updating repository in GitHub.



The image shows two windows from a Windows desktop. The top window is the 'DirectX Diagnostic Tool' with the 'System' tab selected. It displays system information including the date, computer name, operating system, language, manufacturer, model, BIOS, processor, memory, page file, and DirectX version. A checkbox for 'Check for WHQL digital signatures' is checked. The bottom window is a terminal showing a series of git commands and their output, including adding files, committing, and pushing to a remote repository.

**DirectX Diagnostic Tool - System Information**

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, 10:46:48 pm  
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: 17847MB used, 6671MB 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

```
victor@Workstation:~/CPE232_H0A10$ git add *
victor@Workstation:~/CPE232_H0A10$ git commit -m "Updates"
[main 11f8de0] Updates
 1 file changed, 2 insertions(+), 2 deletions(-)
victor@Workstation:~/CPE232_H0A10$ git push origin
Enumerating objects: 5, done.
Counting objects: 100% (5/5), done.
Delta compression using up to 2 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 287 bytes | 287.00 KiB/s, done.
Total 3 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), completed with 1 local object.
To github.com:qvbTor/CPE232_H0A10.git
 4b47a7a..11f8de0  main -> main
victor@Workstation:~/CPE232_H0A10$ S
```

**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.