Name: Aldwin Joseph B. Revilla	**Date Performed:** 10/26/2023
Course/Section: CPE31S5	**Date Submitted:** 10/28/2023
Instructor: Roman Richard	**Semester and SY:** 1st Sem 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.

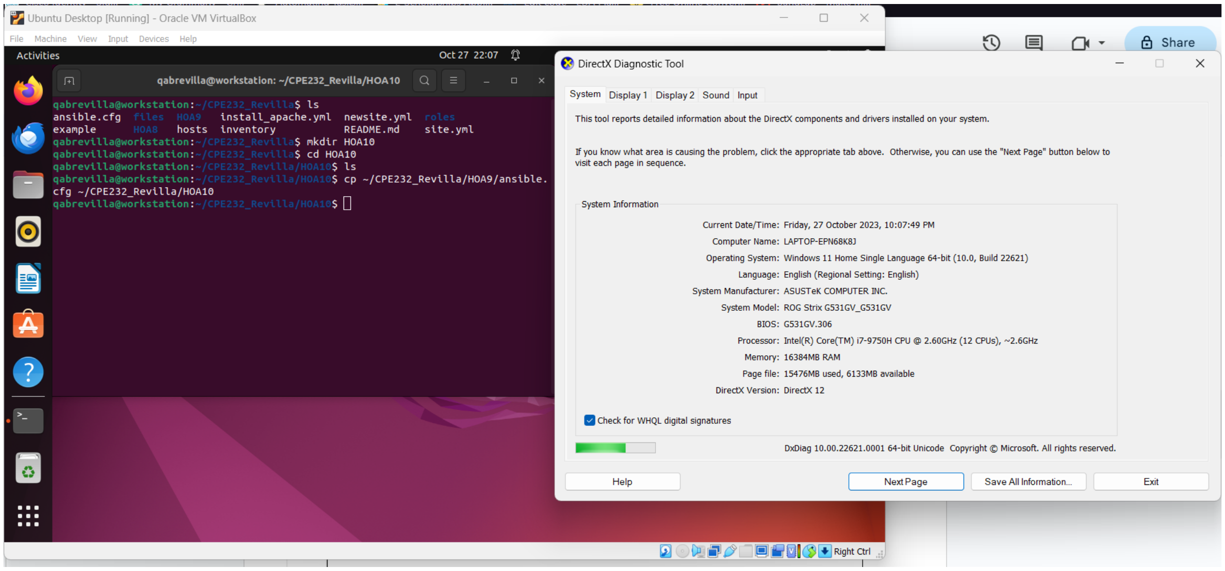
Source: https://www.graylog.org/products/open-source

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)

The set up:



Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Oct 27 22:07
qabrevilla@workstation: ~/CPE232_Revilla/HOA10

```
qabrevilla@workstation:~/CPE232_Revilla$ ls
ansible.cfg  files  HOA9   install_apache.yml  newsite.yml  roles
example      HOA8   hosts  inventory           README.md    site.yml
qabrevilla@workstation:~/CPE232_Revilla$ mkdir HOA10
qabrevilla@workstation:~/CPE232_Revilla$ cd HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ ls
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ cp ~/CPE232_Revilla/HOA9/ansible.
cfg ~/CPE232_Revilla/HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ 
```

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

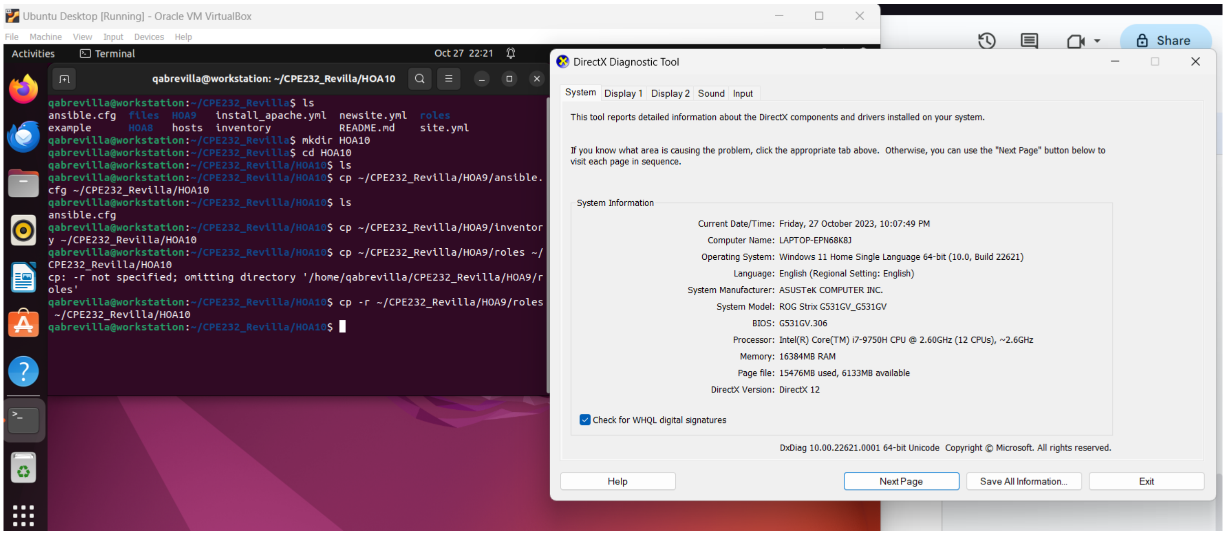
Current Date/Time: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Figure 0.1 Creating new directory

I’ve created a new directory for the Hands-on Activity 10. The command I used is mkdir [name of directory].



```
qabrevilla@workstation:~/CPE232_Revilla$ ls
ansible.cfg  files  HOA9   install_apache.yml  newsite.yml  roles
example      HOA8   hosts  inventory           README.md    site.yml
qabrevilla@workstation:~/CPE232_Revilla$ mkdir HOA10
qabrevilla@workstation:~/CPE232_Revilla$ cd HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ ls
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ cp ~/CPE232_Revilla/HOA9/ansible.
cfg ~/CPE232_Revilla/HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ ls
ansible.cfg
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ cp ~/CPE232_Revilla/HOA9/inventor
y ~/CPE232_Revilla/HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ cp ~/CPE232_Revilla/HOA9/roles ~/
CPE232_Revilla/HOA10
cp: -r not specified; omitting directory '/home/qabrevilla/CPE232_Revilla/HOA9/r
oles'
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ cp -r ~/CPE232_Revilla/HOA9/roles
 ~/CPE232_Revilla/HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ 
```

DirectX Diagnostic Tool

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: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

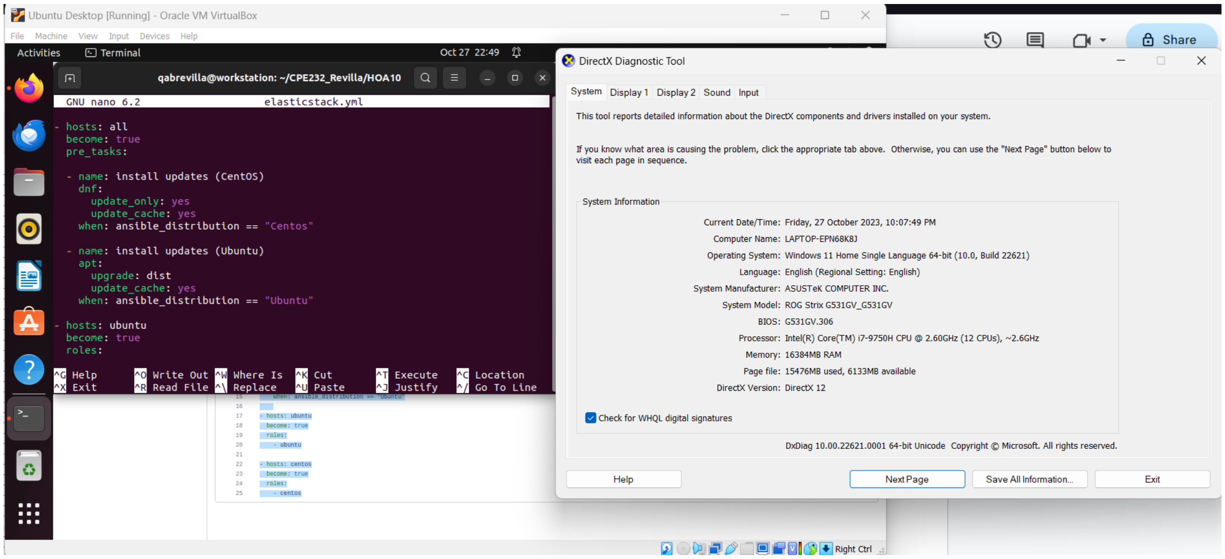
Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 22:21
qabrevilla@workstation: ~/CPE232_Revilla/HOA10
System
Display 1
Display 2
Sound
Input
Help
Next Page
Save All Information...
Exit
Share

Figure 0.2

From the past activity, I copied the ansible.cfg, inventory, and roles directory from Hands-on-Activity 9. In this way I can save time by utilizing copy commands.

1. Create a playbook that:

4.1 Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)



```
GNU nano 6.2                    elasticstack.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:

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

```
    when: ansible_distribution == "Ubuntu"

- hosts: ubuntu
  become: true
  roles:
    - ubuntu

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

DirectX Diagnostic Tool

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.

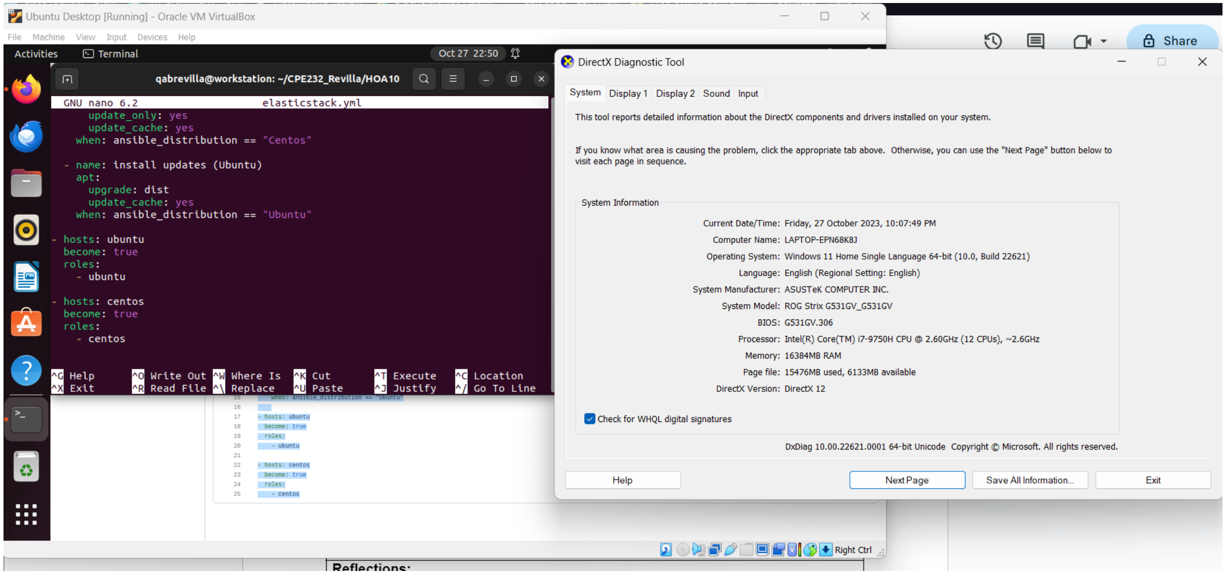
System Information

Current Date/Time: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 22:49
qabrevilla@workstation: ~/CPE232_Revilla/HOA10
System
Display 1
Display 2
Sound
Input
Help
Next Page
Save All Information...
Exit
Share
Right Ctrl



Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 22:50
qabrevilla@workstation: ~/CPE232_Revilla/HOA10
Share
Right Ctrl
Reflections:

```
  GNU nano 6.2                      elasticstack.yml
      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

- hosts: centos
  become: true
  roles:
    - centos

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

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: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

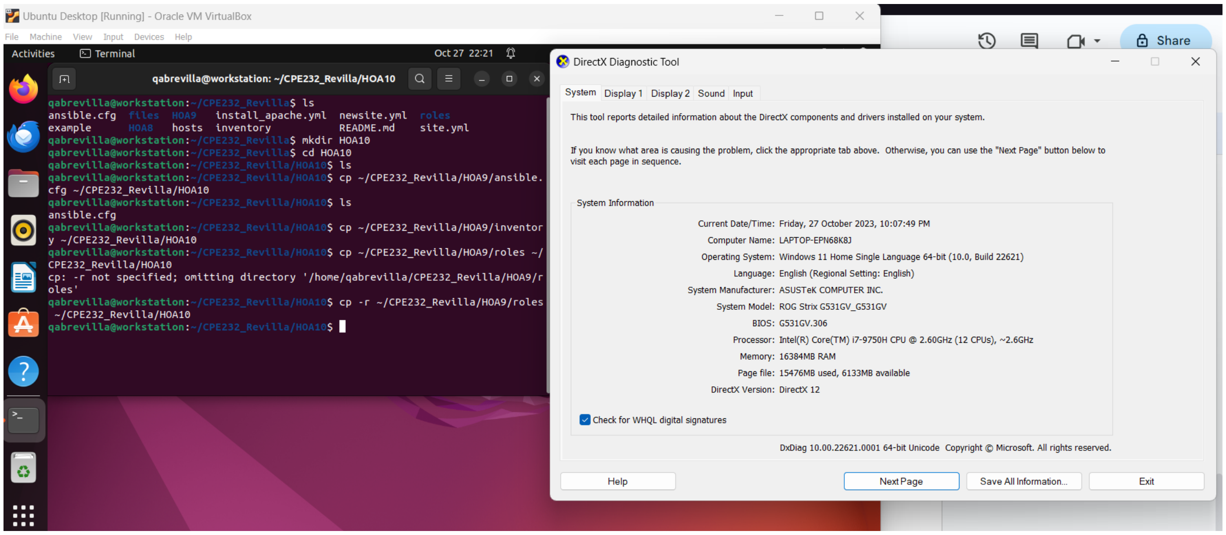
☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Figure 1.1 Elastic Stack

In the main directory of Hands-on-Activity 10, I've created a playbook called elasticstack.yml. This playbook first checks for updates for Ubuntu and Centos, then calls the roles (playbook) for installing elasticsearch and its prerequisites.

2. Apply the concept of creating roles.



Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 22:21
qabrevilla@workstation: ~/CPE232_Revilla/HOA10
Share

```
qabrevilla@workstation:~/CPE232_Revilla$ ls
ansible.cfg  files  HOA9   install_apache.yml  newsite.yml  roles
example      HOA8   hosts  inventory           README.md    site.yml
qabrevilla@workstation:~/CPE232_Revilla$ mkdir HOA10
qabrevilla@workstation:~/CPE232_Revilla$ cd HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ ls
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ cp ~/CPE232_Revilla/HOA9/ansible.
cfg ~/CPE232_Revilla/HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ ls
ansible.cfg
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ cp ~/CPE232_Revilla/HOA9/inventor
y ~/CPE232_Revilla/HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ cp ~/CPE232_Revilla/HOA9/roles ~/
CPE232_Revilla/HOA10
cp: -r not specified; omitting directory '/home/qabrevilla/CPE232_Revilla/HOA9/r
oles'
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ cp -r ~/CPE232_Revilla/HOA9/roles
 ~/CPE232_Revilla/HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ 
```

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: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

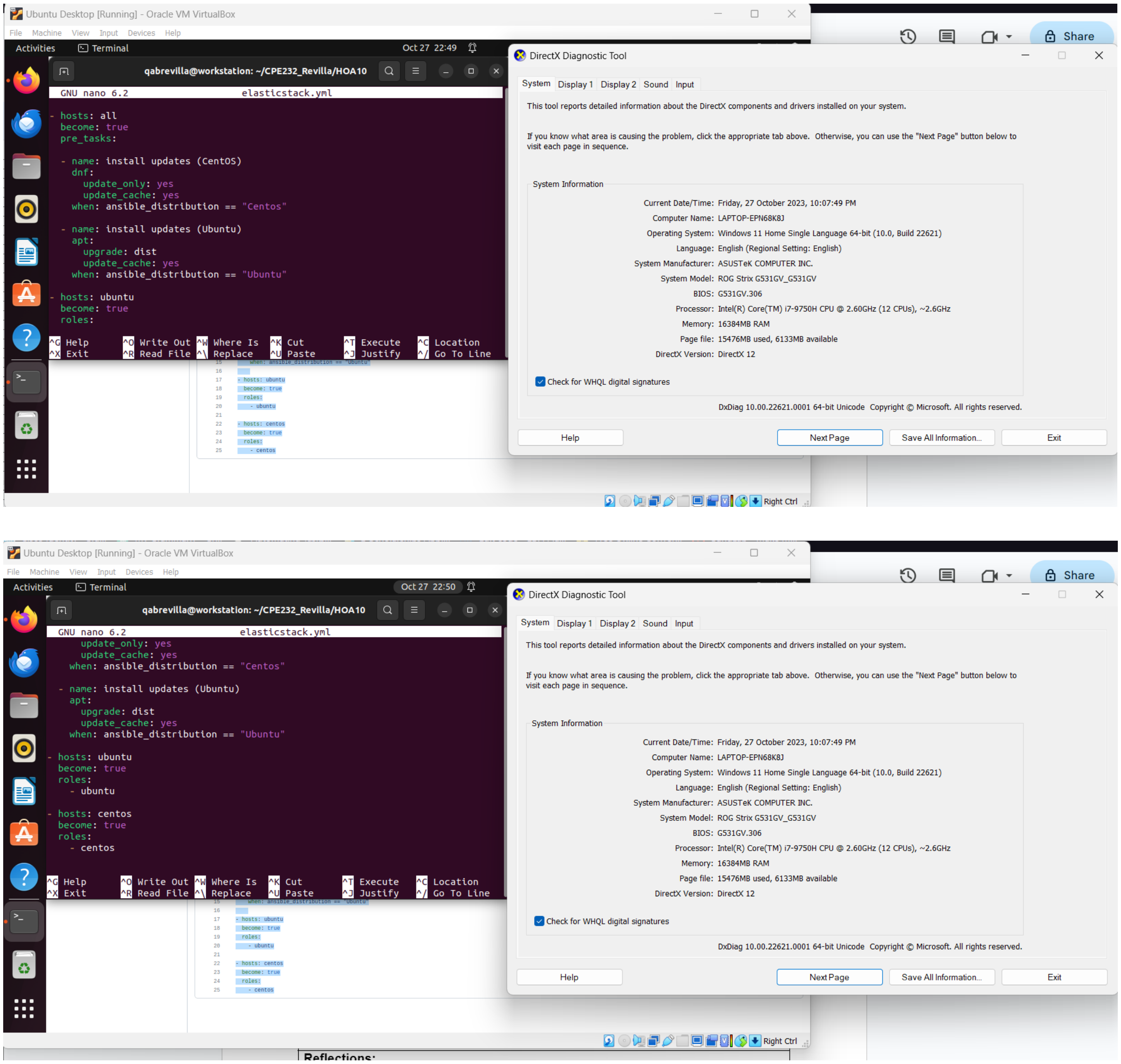
☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Figure 2.1

From the past activity, I copied the ansible.cfg, inventory, and roles directory from Hands-on-Activity 9. In this way I can save time by utilizing copy commands.

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.)



```
GNU nano 6.2                    elasticstack.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:
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

```
    when: ansible_distribution == "Ubuntu"

- hosts: ubuntu
  become: true
  roles:
    - ubuntu

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

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: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 22:50
qabrevilla@workstation: ~/CPE232_Revilla/HOA10
DirectX Diagnostic Tool
Reflections:

```
GNU nano 6.2                    elasticstack.yml
      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

- hosts: centos
  become: true
  roles:
    - centos

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

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

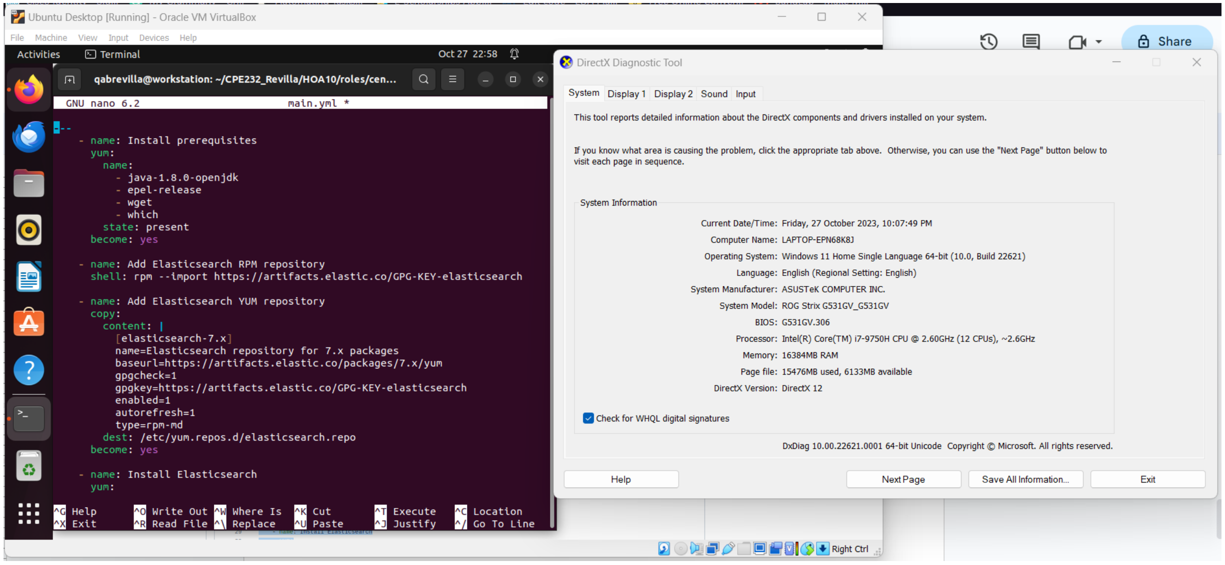
Current Date/Time: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Figure 3.1 Elastic Stack

In the main directory of Hands-on-Activity 10, I've created a playbook called elasticstack.yml. This playbook first checks for updates for Ubuntu and Centos, then calls the roles (playbook) for installing elasticsearch and its prerequisites.



Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 22:58
qabrevilla@workstation: ~/CPE232_Revilla/HOA10/roles/cen...
Share

```
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-KEY-elasticsearch

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

    - name: Install Elasticsearch
      yum:
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

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.

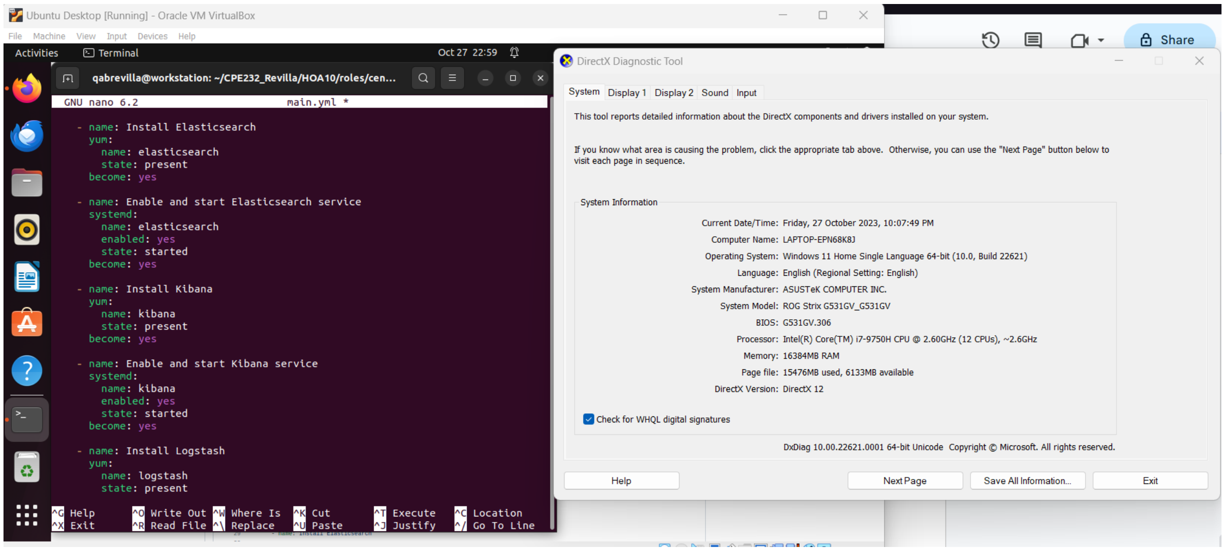
System Information

```
   Current Date/Time: Friday, 27 October 2023, 10:07:49 PM
       Computer Name: LAPTOP-EPN68K8J
    Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
            Language: English (Regional Setting: English)
 System Manufacturer: ASUSTeK COMPUTER INC.
        System Model: ROG Strix G531GV_G531GV
                BIOS: G531GV.306
           Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
              Memory: 16384MB RAM
           Page file: 15476MB used, 6133MB available
     DirectX Version: DirectX 12
```

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Help
Next Page
Save All Information...
Exit
Right Ctrl



Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 22:59
qabrevilla@workstation: ~/CPE232_Revilla/HOA10/roles/cen...
Share

```
GNU nano 6.2                          main.yml *

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

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

    - name: Install Kibana
      yum:
        name: kibana
        state: present
      become: yes

    - name: Enable and start Kibana service
      systemd:
        name: kibana
        enabled: yes
        state: started
      become: yes

    - name: Install Logstash
      yum:
        name: logstash
        state: present
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

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

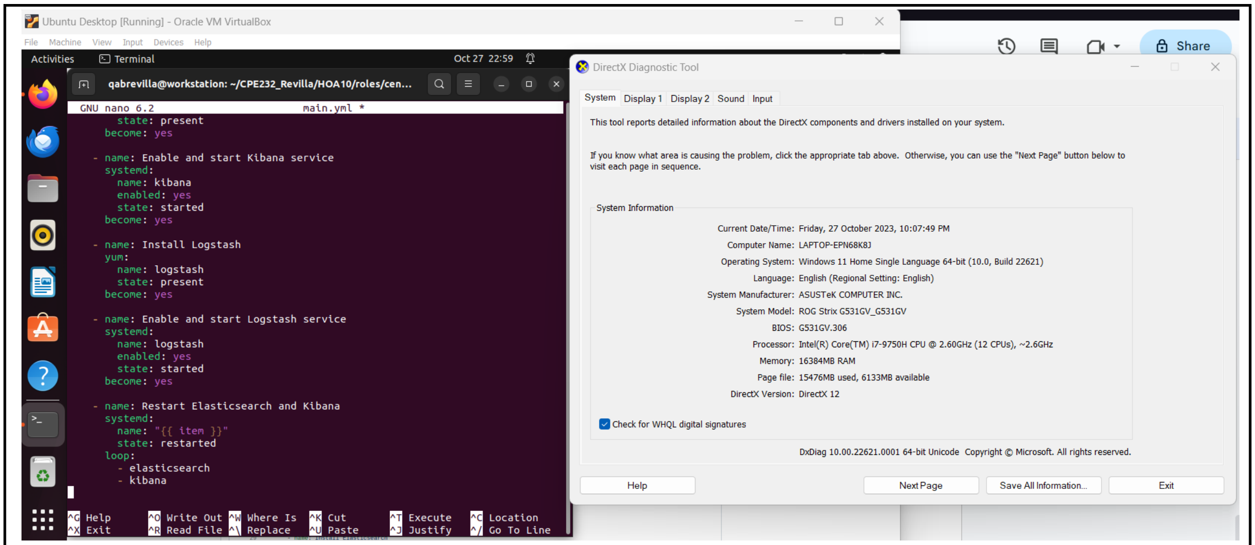
If you know what area is causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button below to visit each page in sequence.

System Information

```
   Current Date/Time: Friday, 27 October 2023, 10:07:49 PM
       Computer Name: LAPTOP-EPN68K8J
    Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
            Language: English (Regional Setting: English)
 System Manufacturer: ASUSTeK COMPUTER INC.
        System Model: ROG Strix G531GV_G531GV
                BIOS: G531GV.306
           Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
              Memory: 16384MB RAM
           Page file: 15476MB used, 6133MB available
     DirectX Version: DirectX 12
```

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.



Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 22:59
qabrevilla@workstation: ~/CPE232_Revilla/HOA10/roles/cen...
DirectX Diagnostic Tool
System Display 1 Display 2 Sound Input
Help
Next Page
Save All Information...
Exit
Share

```
  GNU nano 6.2                      main.yml *
      state: present
    become: yes

  - name: Enable and start Kibana service
    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

  - name: Install Logstash
    yum:
      name: logstash
      state: present
    become: yes

  - name: Enable and start Logstash service
    systemd:
      name: logstash
      enabled: yes
      state: started
    become: yes

  - name: Restart Elasticsearch and Kibana
    systemd:
      name: "{{ item }}"
      state: restarted
    loop:
      - elasticsearch
      - kibana

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

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

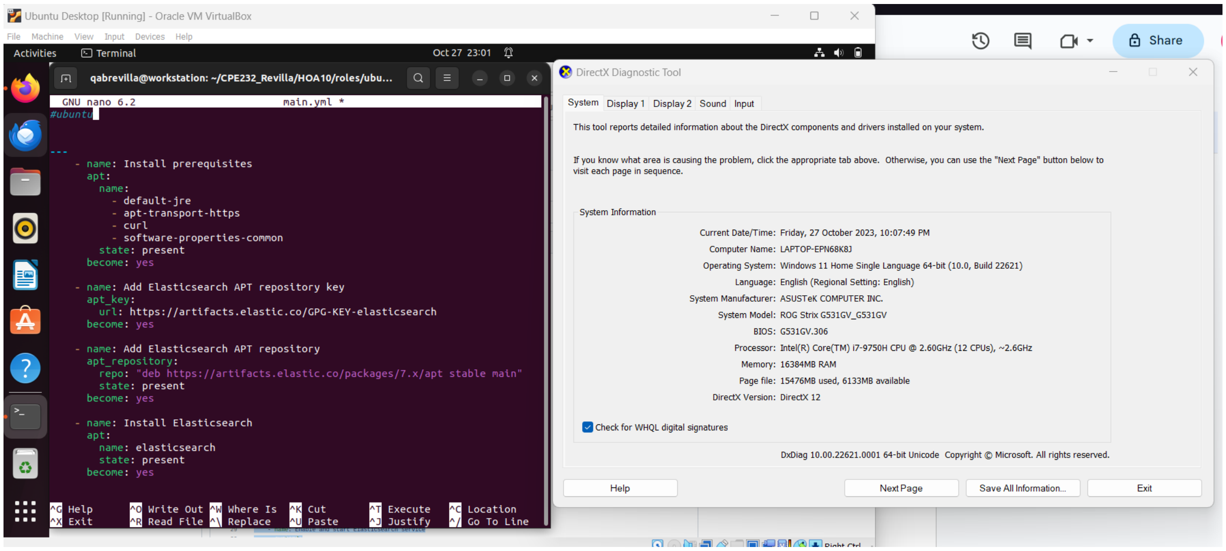
Current Date/Time: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Figure 3.2 ElasticStack for CentOS

First I need to understand how ElasticStack installation works. We need to add the requirements in order for it to install. I've added many software prerequisites in the playbook with the installation of the elasticsearch.



Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 23:01
qabrevilla@workstation: ~/CPE232_Revilla/HOA10/roles/ubu...
DirectX Diagnostic Tool
System Display 1 Display 2 Sound Input
Help
Next Page
Save All Information...
Exit
Share

```
  GNU nano 6.2                      main.yml *
#ubuntu


---
  - name: Install prerequisites
    apt:
      name:
        - default-jre
        - apt-transport-https
        - curl
        - software-properties-common
      state: present
    become: yes

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

  - name: Add Elasticsearch APT repository
    apt_repository:
      repo: "deb https://artifacts.elastic.co/packages/7.x/apt stable main"
      state: present
    become: yes

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

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

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

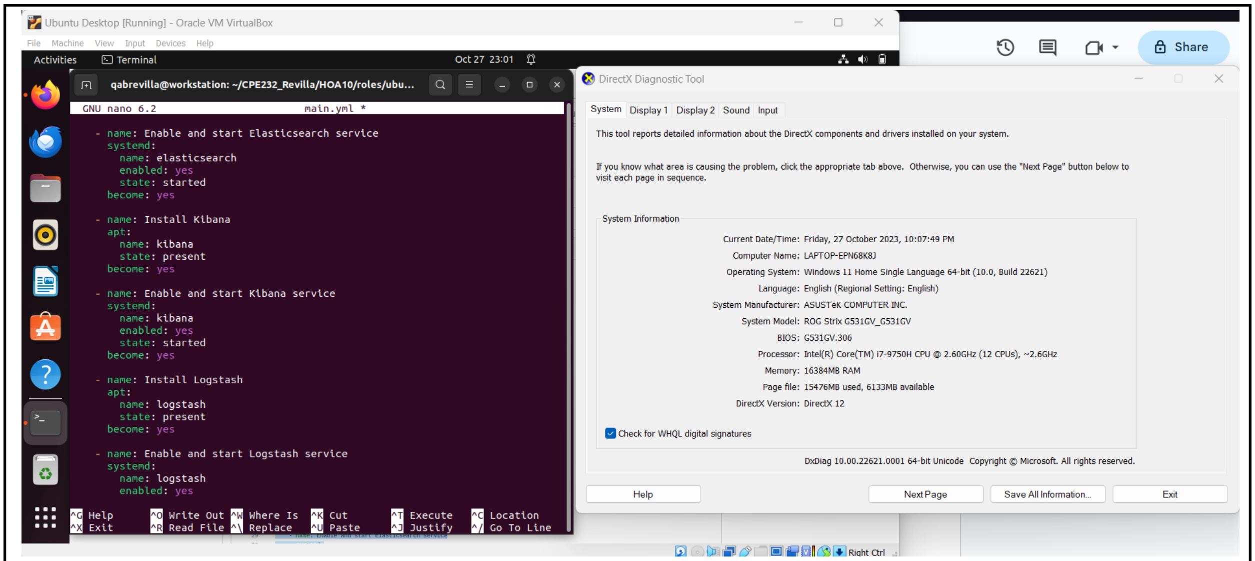
If you know what area is causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button below to visit each page in sequence.

System Information

Current Date/Time: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.



Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 23:01
qabrevilla@workstation: ~/CPE232_Revilla/HOA10/roles/ubu...
DirectX Diagnostic Tool
Share

```
  GNU nano 6.2                         main.yml *

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

  - name: Install Kibana
    apt:
      name: kibana
      state: present
    become: yes

  - name: Enable and start Kibana service
    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

  - name: Install Logstash
    apt:
      name: logstash
      state: present
    become: yes

  - name: Enable and start Logstash service
    systemd:
      name: logstash
      enabled: yes
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

System | Display 1 | Display 2 | Sound | 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.

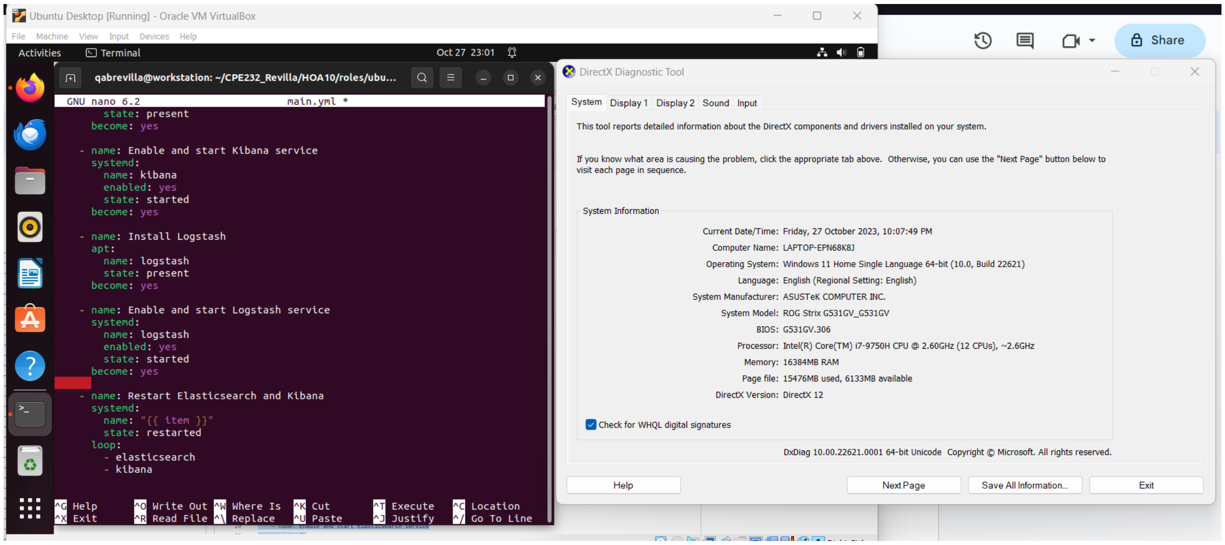
System Information

```
Current Date/Time: Friday, 27 October 2023, 10:07:49 PM
    Computer Name: LAPTOP-EPN68K8J
 Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
         Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
     System Model: ROG Strix G531GV_G531GV
             BIOS: G531GV.306
        Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
           Memory: 16384MB RAM
        Page file: 15476MB used, 6133MB available
  DirectX Version: DirectX 12
```

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Help | Next Page | Save All Information... | Exit



Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 23:01
qabrevilla@workstation: ~/CPE232_Revilla/HOA10/roles/ubu...
DirectX Diagnostic Tool
Share

```
  GNU nano 6.2                         main.yml *
      state: present
    become: yes

  - name: Enable and start Kibana service
    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

  - name: Install Logstash
    apt:
      name: logstash
      state: present
    become: yes

  - name: Enable and start Logstash service
    systemd:
      name: logstash
      enabled: yes
      state: started
    become: yes

  - name: Restart Elasticsearch and Kibana
    systemd:
      name: "{{ item }}"
      state: restarted
    loop:
      - elasticsearch
      - kibana

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

System | Display 1 | Display 2 | Sound | 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: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

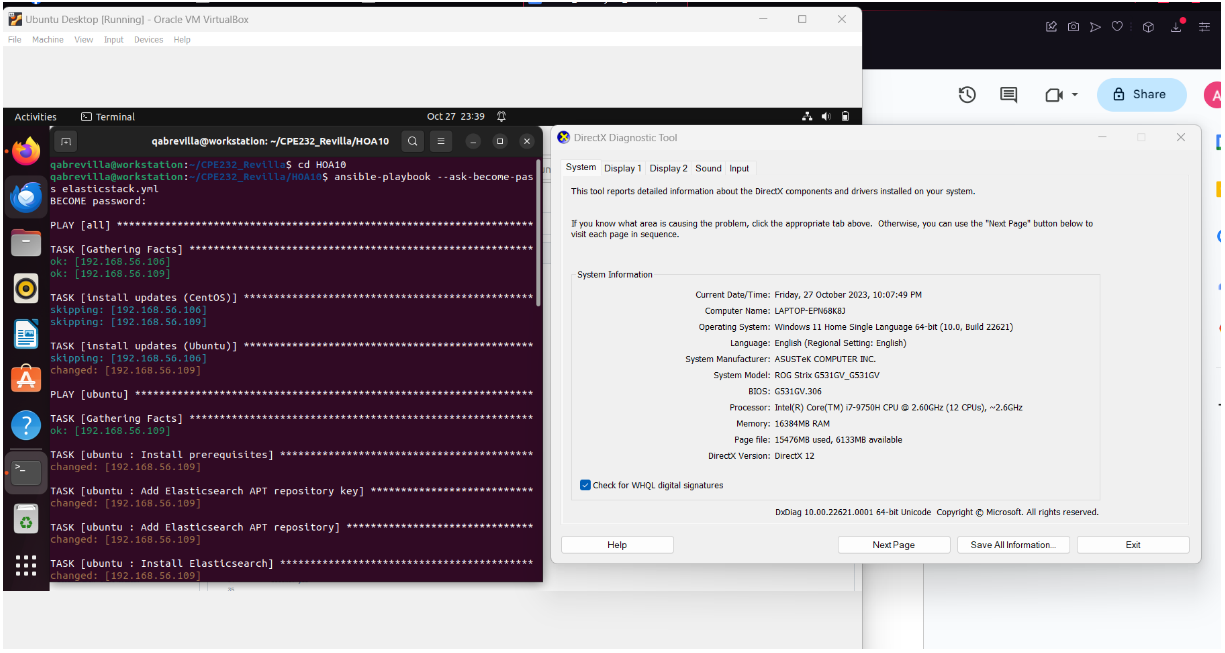
DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Help | Next Page | Save All Information... | Exit

Figure 3.3 ElasticStack for Ubuntu

It is the same as for the centos. The difference is that some installations required a different structure of command in order to install in ubuntu.

4. Show an output of the installed Elastic Stack for both Ubuntu and CentOS.


Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 23:39
Share

qabrevilla@workstation: ~/CPE232_Revilla/HOA10

```
qabrevilla@workstation:~/CPE232_Revilla$ cd HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ ansible-playbook --ask-become-pas
s elasticstack.yml
BECOME password:

PLAY [all] ***********************************************************************

TASK [Gathering Facts] ***********************************************************
ok: [192.168.56.106]
ok: [192.168.56.109]

TASK [install updates (CentOS)] **************************************************
skipping: [192.168.56.106]
skipping: [192.168.56.109]

TASK [install updates (Ubuntu)] **************************************************
skipping: [192.168.56.106]
changed: [192.168.56.109]

PLAY [ubuntu] ********************************************************************

TASK [Gathering Facts] ***********************************************************
ok: [192.168.56.109]

TASK [ubuntu : Install prerequisites] ********************************************
changed: [192.168.56.109]

TASK [ubuntu : Add Elasticsearch APT repository key] *****************************
changed: [192.168.56.109]

TASK [ubuntu : Add Elasticsearch APT repository] *********************************
changed: [192.168.56.109]

TASK [ubuntu : Install Elasticsearch] ********************************************
changed: [192.168.56.109]
```

DirectX Diagnostic Tool

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.

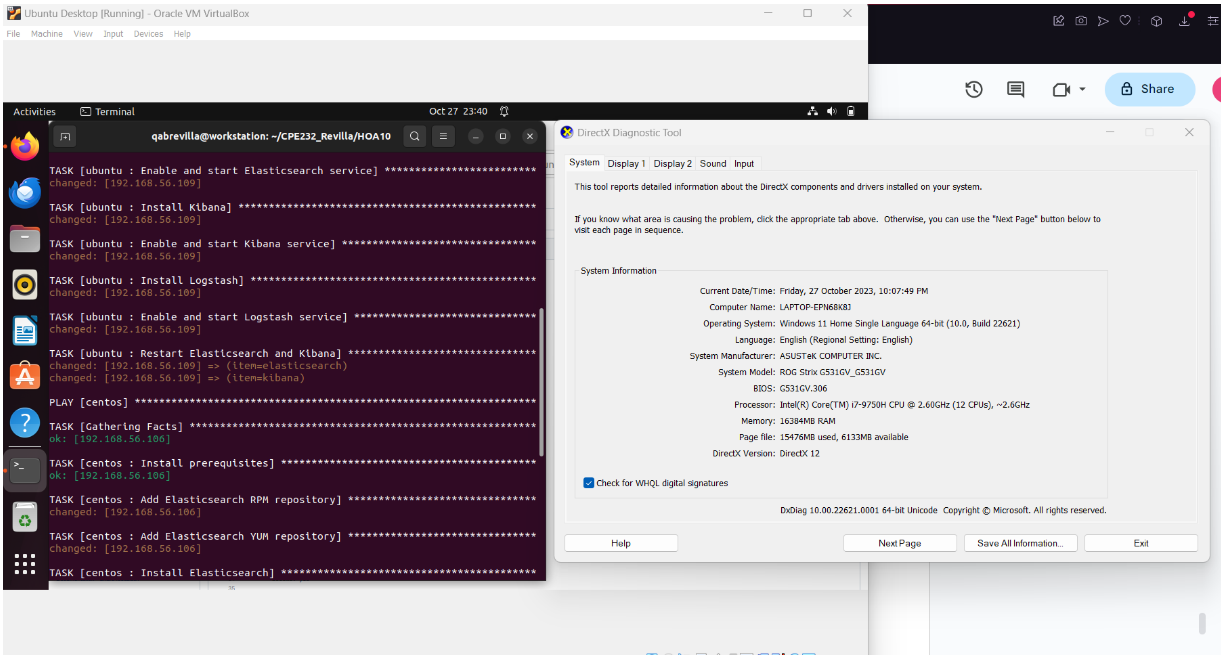
System Information

Current Date/Time: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Help
Next Page
Save All Information...
Exit


Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 27 23:40
Share

qabrevilla@workstation: ~/CPE232_Revilla/HOA10

```
TASK [ubuntu : Enable and start Elasticsearch service] ***************************
changed: [192.168.56.109]

TASK [ubuntu : Install Kibana] ***************************************************
changed: [192.168.56.109]

TASK [ubuntu : Enable and start Kibana service] **********************************
changed: [192.168.56.109]

TASK [ubuntu : Install Logstash] *************************************************
changed: [192.168.56.109]

TASK [ubuntu : Enable and start Logstash service] ********************************
changed: [192.168.56.109]

TASK [ubuntu : Restart Elasticsearch and Kibana] *********************************
changed: [192.168.56.109] => (item=elasticsearch)
changed: [192.168.56.109] => (item=kibana)

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

TASK [Gathering Facts] ***********************************************************
ok: [192.168.56.106]

TASK [centos : Install prerequisites] ********************************************
ok: [192.168.56.106]

TASK [centos : Add Elasticsearch RPM repository] *********************************
changed: [192.168.56.106]

TASK [centos : Add Elasticsearch YUM repository] *********************************
changed: [192.168.56.106]

TASK [centos : Install Elasticsearch] ********************************************
```

DirectX Diagnostic Tool

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

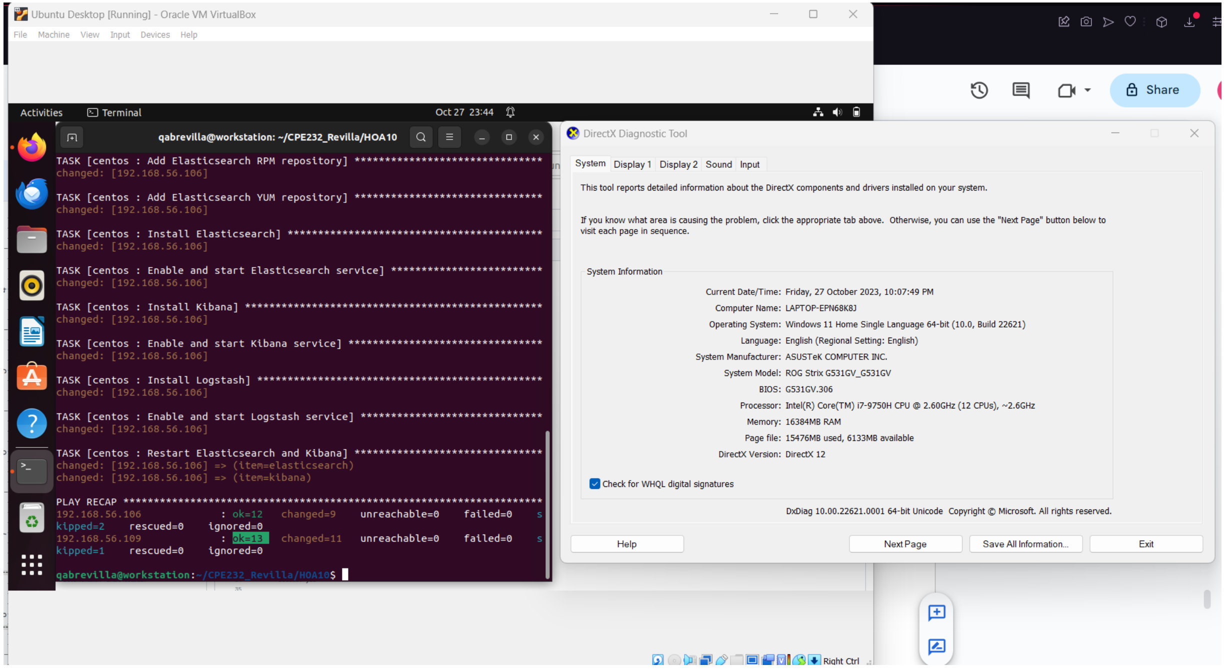
If you know what area is causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button below to visit each page in sequence.

System Information

Current Date/Time: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.



```
TASK [centos : Add Elasticsearch RPM repository] ******************************
changed: [192.168.56.106]

TASK [centos : Add Elasticsearch YUM repository] ******************************
changed: [192.168.56.106]

TASK [centos : Install Elasticsearch] *****************************************
changed: [192.168.56.106]

TASK [centos : Enable and start Elasticsearch service] ************************
changed: [192.168.56.106]

TASK [centos : Install Kibana] ************************************************
changed: [192.168.56.106]

TASK [centos : Enable and start Kibana service] *******************************
changed: [192.168.56.106]

TASK [centos : Install Logstash] **********************************************
changed: [192.168.56.106]

TASK [centos : Enable and start Logstash service] *****************************
changed: [192.168.56.106]

TASK [centos : Restart Elasticsearch and Kibana] ******************************
changed: [192.168.56.106] => (item=elasticsearch)
changed: [192.168.56.106] => (item=kibana)

PLAY RECAP ********************************************************************
192.168.56.106             : ok=12   changed=9    unreachable=0    failed=0    s
kipped=2    rescued=0    ignored=0
192.168.56.109             : ok=13   changed=11   unreachable=0    failed=0    s
kipped=1    rescued=0    ignored=0

qabrevilla@workstation:~/CPE232_Revilla/HOA10$
```

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

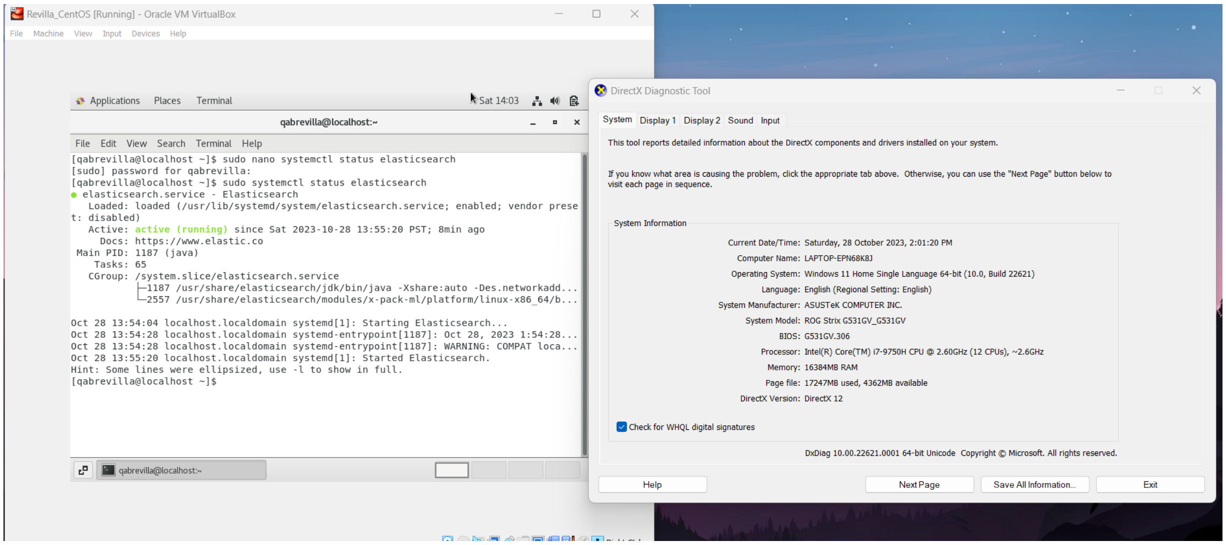
If you know what area is causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button below to visit each page in sequence.

System Information

Current Date/Time: Friday, 27 October 2023, 10:07:49 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 15476MB used, 6133MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.



```
[qabrevilla@localhost ~]$ sudo nano systemctl status elasticsearch
[sudo] password for qabrevilla:
[qabrevilla@localhost ~]$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor prese
t: disabled)
   Active: active (running) since Sat 2023-10-28 13:55:20 PST; 8min ago
     Docs: https://www.elastic.co
 Main PID: 1187 (java)
    Tasks: 65
   CGroup: /system.slice/elasticsearch.service
           ├─1187 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkadd...
           └─2557 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/b...

Oct 28 13:54:04 localhost.localdomain systemd[1]: Starting Elasticsearch...
Oct 28 13:54:28 localhost.localdomain systemd-entrypoint[1187]: Oct 28, 2023 1:54:28...
Oct 28 13:54:28 localhost.localdomain systemd-entrypoint[1187]: WARNING: COMPAT loca...
Oct 28 13:55:20 localhost.localdomain systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
[qabrevilla@localhost ~]$
```

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

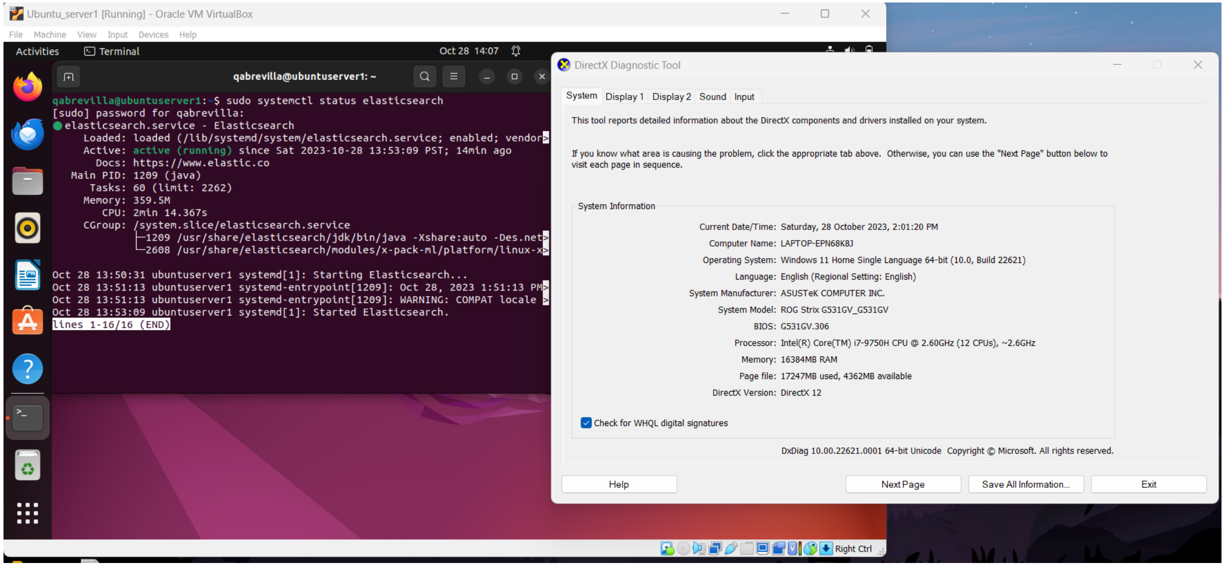
If you know what area is causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button below to visit each page in sequence.

System Information

Current Date/Time: Saturday, 28 October 2023, 2:01:20 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 17247MB used, 4362MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.


Ubuntu_server1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 28 14:07
qabrevilla@ubuntuserver1: ~
DirectX Diagnostic Tool
System Display 1 Display 2 Sound Input
Help
Next Page
Save All Information...
Exit
Right Ctrl

```
qabrevilla@ubuntuserver1:~$ sudo systemctl status elasticsearch
[sudo] password for qabrevilla:
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor>
     Active: active (running) since Sat 2023-10-28 13:53:09 PST; 14min ago
       Docs: https://www.elastic.co
   Main PID: 1209 (java)
      Tasks: 60 (limit: 2262)
     Memory: 359.5M
        CPU: 2min 14.367s
     CGroup: /system.slice/elasticsearch.service
             ├─1209 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.net>
             └─2608 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>

Oct 28 13:50:31 ubuntuserver1 systemd[1]: Starting Elasticsearch...
Oct 28 13:51:13 ubuntuserver1 systemd-entrypoint[1209]: Oct 28, 2023 1:51:13 PM>
Oct 28 13:51:13 ubuntuserver1 systemd-entrypoint[1209]: WARNING: COMPAT locale >
Oct 28 13:53:09 ubuntuserver1 systemd[1]: Started Elasticsearch.
lines 1-16/16 (END)
```

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.

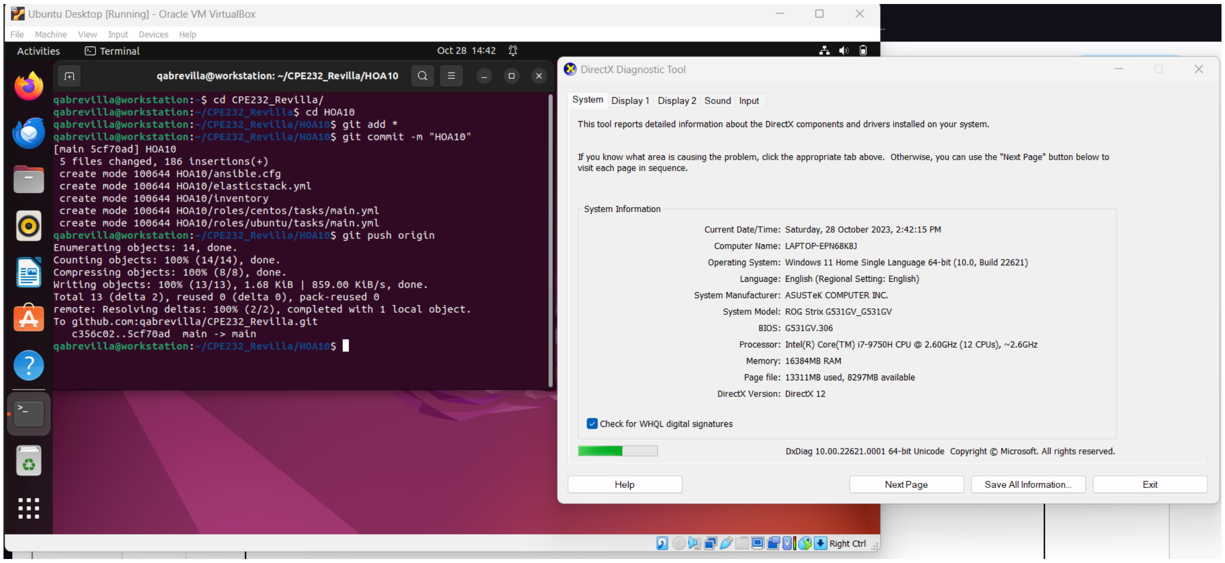
System Information

Current Date/Time: Saturday, 28 October 2023, 2:01:20 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 17247MB used, 4362MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

5. Make sure to create a new repository in GitHub for this activity.


Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 28 14:42
qabrevilla@workstation: ~/CPE232_Revilla/HOA10
DirectX Diagnostic Tool
System Display 1 Display 2 Sound Input
Help
Next Page
Save All Information...
Exit
Right Ctrl

```
qabrevilla@workstation:~$ cd CPE232_Revilla/
qabrevilla@workstation:~/CPE232_Revilla$ cd HOA10
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ git add *
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ git commit -m "HOA10"
[main 5cf70ad] HOA10
 5 files changed, 186 insertions(+)
 create mode 100644 HOA10/ansible.cfg
 create mode 100644 HOA10/elasticstack.yml
 create mode 100644 HOA10/inventory
 create mode 100644 HOA10/roles/centos/tasks/main.yml
 create mode 100644 HOA10/roles/ubuntu/tasks/main.yml
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ git push origin
Enumerating objects: 14, done.
Counting objects: 100% (14/14), done.
Compressing objects: 100% (8/8), done.
Writing objects: 100% (13/13), 1.68 KiB | 859.00 KiB/s, done.
Total 13 (delta 2), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (2/2), completed with 1 local object.
To github.com:qabrevilla/CPE232_Revilla.git
   c356c02..5cf70ad  main -> main
qabrevilla@workstation:~/CPE232_Revilla/HOA10$ 
```

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: Saturday, 28 October 2023, 2:42:15 PM
Computer Name: LAPTOP-EPN68K8J
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ROG Strix G531GV_G531GV
BIOS: G531GV.306
Processor: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
Memory: 16384MB RAM
Page file: 13311MB used, 8297MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

Reflections:

Answer the following:

1. What are the benefits of having a log monitoring tool?
   Log monitoring tool helps users to visually see what is happening on the entire system. This helps users to address issues more efficiently and provide more detail about the cause of the problem. System Administrators or IT can use this tools for decision making and to avoid risk in making a mistake on troubleshooting.

Conclusions:

In this activity, we are able to install softwares that scans and monitors log files such as elastic stack and grayLog. This software detects and alerts users to pattern the log files, monitor the system, and detects software or security issues We focused on installing Elastic Stack in Ubuntu and CentOS. We used Playbooks and roles to install the softwares. Using roles for this activity is crucial because it helps us organize the file and shorten the content of tha main playbook. I really appreciate the experience given for this activity. I had many challenges but it helps me to improve my critical thinking skills and troubleshooting skills. I hope these skills will help me be better in the future and use this knowledge as my references.