Name: Bernice M. Peña	**Date Performed:** 10/26/2023
Course/Section: Managing Enterprise Servers / CPE31S5	**Date Submitted:** 10/27/2023
Instructor: Engr. Roman Richard	**Semester and SY:** 1st semester, 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.

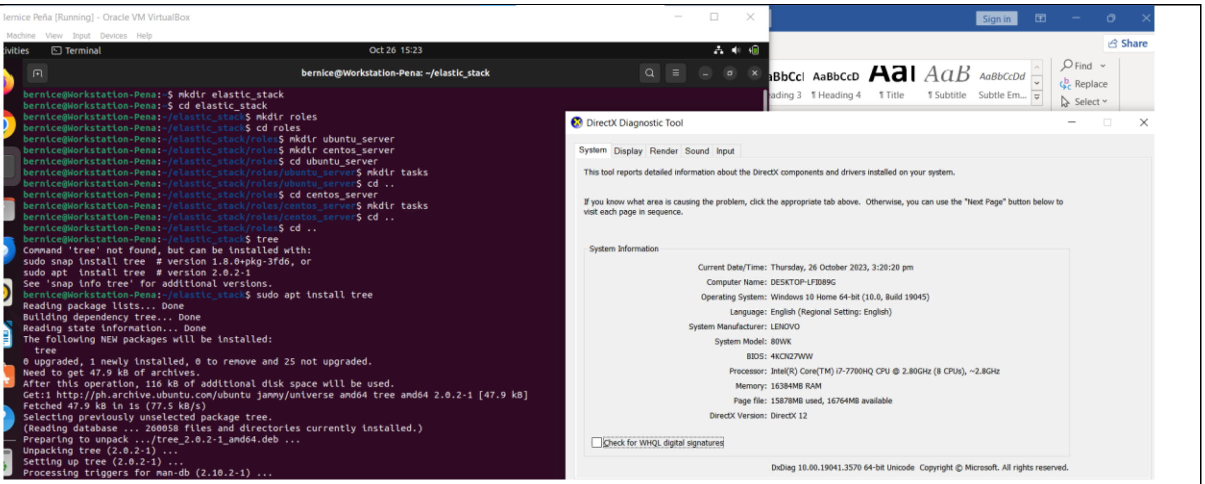
We use Graylog primarily as the stash for the logs of the web applications we build. However, it is also effective when working with raw strings (i.e. syslog): the tool parses it into the structured data we need. It also allows advanced custom search in the logs using structured queries. In other words,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


Bernice Peña [Running] - Oracle VM VirtualBox
Machine View Input Devices Help
Activities
Terminal
Oct 26 15:23
bernice@Workstation-Pena: ~/elastic_stack
DirectX Diagnostic Tool
System Display Render Sound Input
Find
Replace
Select
Share
Sign in

```
bernice@Workstation-Pena:~$ mkdir elastic_stack
bernice@Workstation-Pena:~$ cd elastic_stack
bernice@Workstation-Pena:~/elastic_stack$ mkdir roles
bernice@Workstation-Pena:~/elastic_stack$ cd roles
bernice@Workstation-Pena:~/elastic_stack/roles$ mkdir ubuntu_server
bernice@Workstation-Pena:~/elastic_stack/roles$ mkdir centos_server
bernice@Workstation-Pena:~/elastic_stack/roles$ cd ubuntu_server
bernice@Workstation-Pena:~/elastic_stack/roles/ubuntu_server$ mkdir tasks
bernice@Workstation-Pena:~/elastic_stack/roles/ubuntu_server$ cd ..
bernice@Workstation-Pena:~/elastic_stack/roles$ cd centos_server
bernice@Workstation-Pena:~/elastic_stack/roles/centos_server$ mkdir tasks
bernice@Workstation-Pena:~/elastic_stack/roles/centos_server$ cd ..
bernice@Workstation-Pena:~/elastic_stack/roles$ cd ..
bernice@Workstation-Pena:~/elastic_stack$ tree
Command 'tree' not found, but can be installed with:
sudo snap install tree  # version 1.8.0+pkg-3fd6, or
sudo apt  install tree  # version 2.0.2-1
See 'snap info tree' for additional versions.
bernice@Workstation-Pena:~/elastic_stack$ sudo apt install tree
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  tree
0 upgraded, 1 newly installed, 0 to remove and 25 not upgraded.
Need to get 47.9 kB of archives.
After this operation, 116 kB of additional disk space will be used.
Get:1 http://ph.archive.ubuntu.com/ubuntu jammy/universe amd64 tree amd64 2.0.2-1 [47.9 kB]
Fetched 47.9 kB in 1s (77.5 kB/s)
Selecting previously unselected package tree.
(Reading database ... 260058 files and directories currently installed.)
Preparing to unpack .../tree_2.0.2-1_amd64.deb ...
Unpacking tree (2.0.2-1) ...
Setting up tree (2.0.2-1) ...
Processing triggers for man-db (2.10.2-1) ...
```

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.

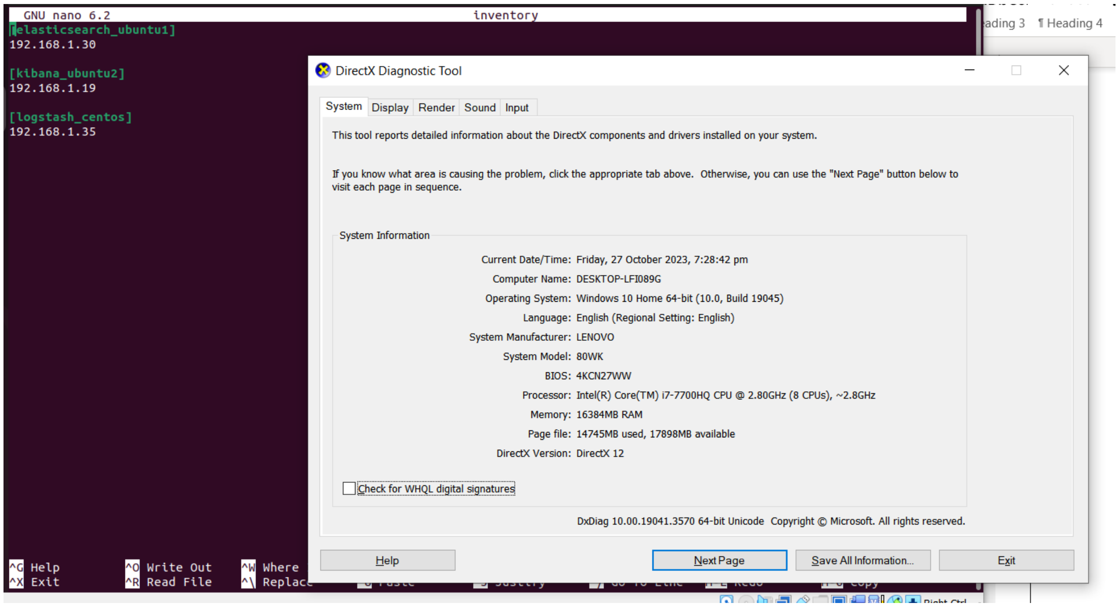
System Information

```
   Current Date/Time: Thursday, 26 October 2023, 3:20:20 pm
       Computer Name: DESKTOP-LFI089G
    Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
            Language: English (Regional Setting: English)
 System Manufacturer: LENOVO
        System Model: 80WK
                BIOS: 4KCN27WW
           Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
              Memory: 16384MB RAM
           Page file: 15878MB used, 16764MB available
     DirectX Version: DirectX 12
```

☐ Check for WHQL digital signatures

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

I created directories wherein I can store my yml files for specific server, I made a directory for ubuntu server and for CentOS server. Those directories will be used for yml files for the installation of Elastic Stack.



```
[elasticsearch_ubuntu1]
192.168.1.30

[kibana_ubuntu2]
192.168.1.19

[logstash_centos]
192.168.1.35
```

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.

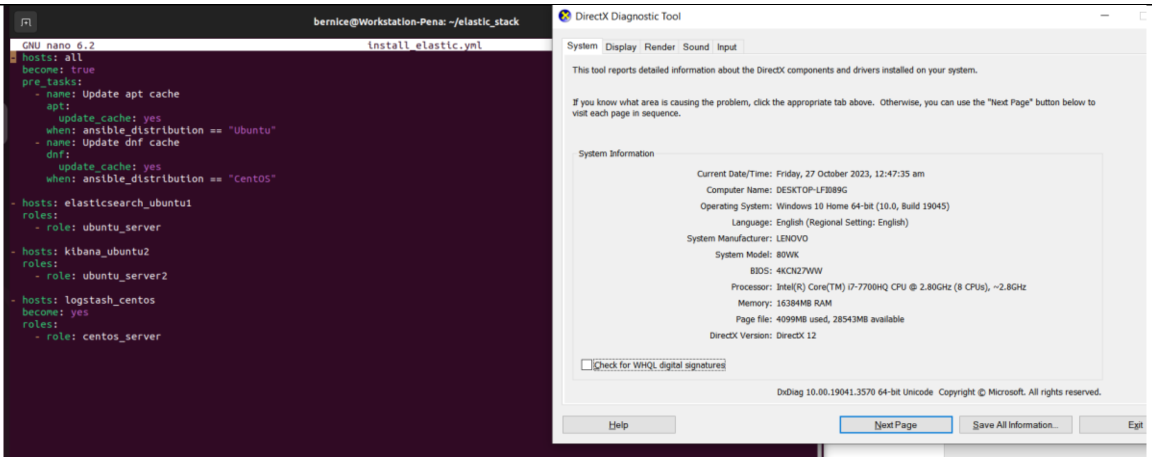
System Information

```
   Current Date/Time: Friday, 27 October 2023, 7:28:42 pm
       Computer Name: DESKTOP-LFI089G
    Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
            Language: English (Regional Setting: English)
 System Manufacturer: LENOVO
        System Model: 80WK
                BIOS: 4KCN27WW
           Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
              Memory: 16384MB RAM
           Page file: 14745MB used, 17898MB available
     DirectX Version: DirectX 12
```

☐ Check for WHQL digital signatures

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

Inside my elastic_stack directory, I created an inventory to list the ip addresses that I will be using for installing elastic stack. I used 2 servers for ubuntu, and one server using my CentOS.



```
GNU nano 6.2                                    install_elastic.yml
- hosts: all
  become: true
  pre_tasks:
    - name: Update apt cache
      apt:
        update_cache: yes
      when: ansible_distribution == "Ubuntu"
    - name: Update dnf cache
      dnf:
        update_cache: yes
      when: ansible_distribution == "CentOS"

- hosts: elasticsearch_ubuntu1
  roles:
    - role: ubuntu_server

- hosts: kibana_ubuntu2
  roles:
    - role: ubuntu_server2

- hosts: logstash_centos
  become: yes
  roles:
    - role: centos_server
```

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.

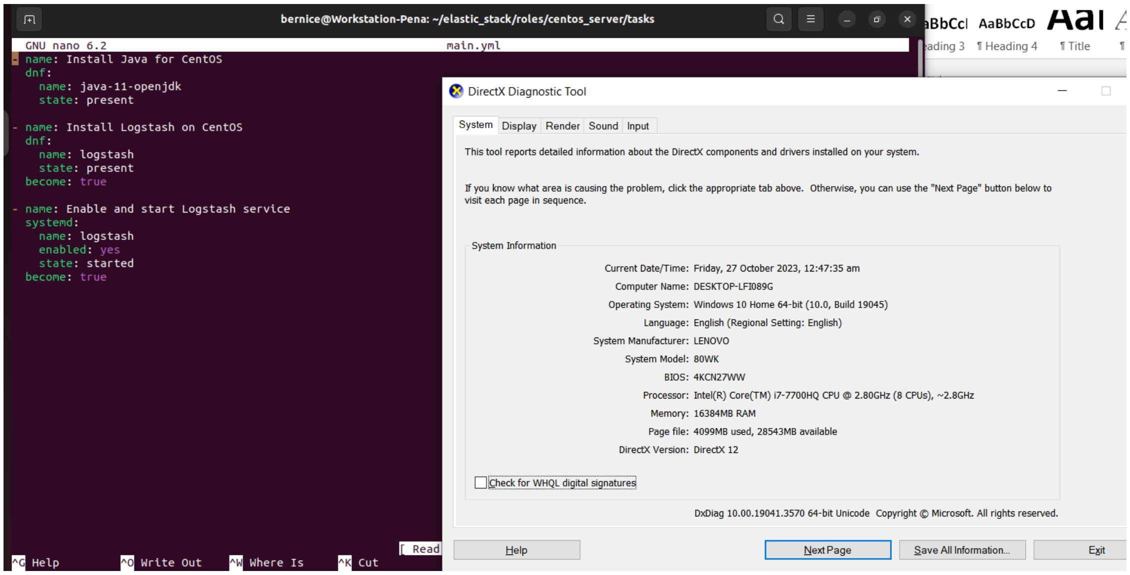
System Information

```
 Current Date/Time: Friday, 27 October 2023, 12:47:35 am
     Computer Name: DESKTOP-LFI089G
  Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
          Language: English (Regional Setting: English)
System Manufacturer: LENOVO
      System Model: 80WK
              BIOS: 4KCN27WW
         Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
            Memory: 16384MB RAM
         Page file: 4099MB used, 28543MB available
   DirectX Version: DirectX 12
```

□ Check for WHQL digital signatures

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

I created a yml file named install_elastic.yml inside my elastic_stack directory. This yml file's purpose to apply the concept of roles to call the tasks in my servers' yml file.


bernice@Workstation-Pena: ~/elastic_stack/roles/centos_server/tasks
aBbCcI
AaBbCcD
AaI
ading 3
¶ Heading 4
¶ Title

```
GNU nano 6.2                                    main.yml
- name: Install Java for CentOS
  dnf:
    name: java-11-openjdk
    state: present

- name: Install Logstash on CentOS
  dnf:
    name: logstash
    state: present
  become: true

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

                                                          [ Read
^G Help         ^O Write Out    ^W Where Is     ^K Cut
```

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.

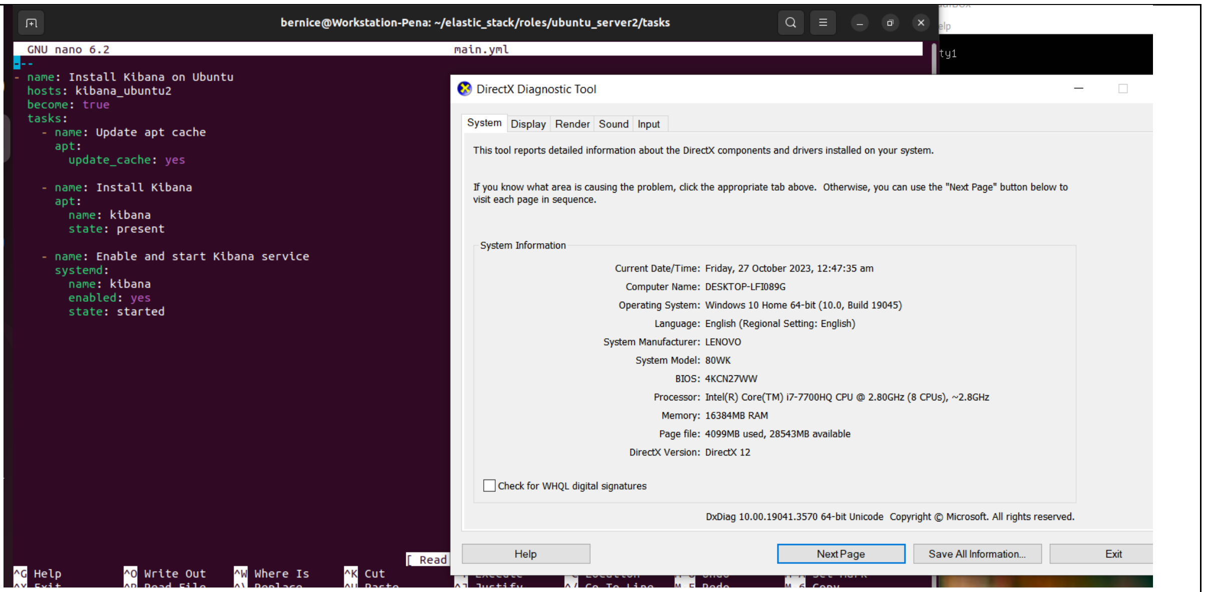
System Information

```
 Current Date/Time: Friday, 27 October 2023, 12:47:35 am
     Computer Name: DESKTOP-LFI089G
  Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
          Language: English (Regional Setting: English)
System Manufacturer: LENOVO
      System Model: 80WK
              BIOS: 4KCN27WW
         Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
            Memory: 16384MB RAM
         Page file: 4099MB used, 28543MB available
   DirectX Version: DirectX 12
```

□ Check for WHQL digital signatures

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

Inside my roles/centos_server/tasks directory, I created a main.yml file that consists of the tasks to be executed in installing Logstash.



bernice@Workstation-Pena: ~/elastic_stack/roles/ubuntu_server2/tasks

```
  GNU nano 6.2                                       main.yml
---
- name: Install Kibana on Ubuntu
  hosts: kibana_ubuntu2
  become: true
  tasks:
    - name: Update apt cache
      apt:
        update_cache: yes

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

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

                                                    [ Read
^G Help        ^O Write Out   ^W Where Is    ^K Cut
```

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.

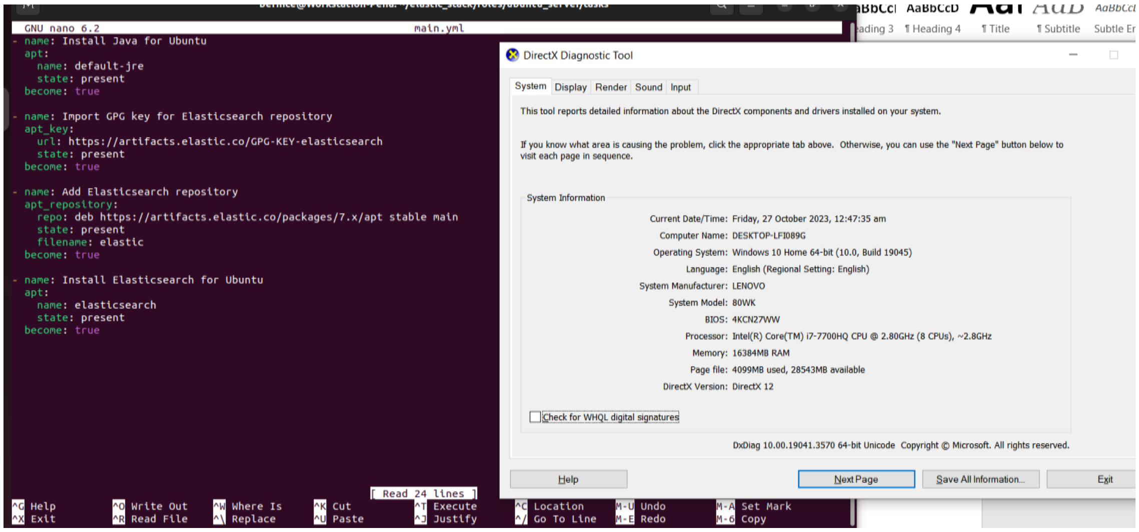
System Information

```
   Current Date/Time: Friday, 27 October 2023, 12:47:35 am
       Computer Name: DESKTOP-LFI089G
    Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
            Language: English (Regional Setting: English)
 System Manufacturer: LENOVO
        System Model: 80WK
                BIOS: 4KCN27WW
           Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
              Memory: 16384MB RAM
           Page file: 4099MB used, 28543MB available
     DirectX Version: DirectX 12
```

□ Check for WHQL digital signatures

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

Inside my roles/ubuntu_server2/tasks directory, I created a main.yml file that consists of the tasks to be executed in installing Kibana on my ubuntu server 2.



```
  GNU nano 6.2                                  main.yml
- name: Install Java for Ubuntu
  apt:
    name: default-jre
    state: present
  become: true

- name: Import GPG key for Elasticsearch repository
  apt_key:
    url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    state: present
  become: true

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

- name: Install Elasticsearch for Ubuntu
  apt:
    name: elasticsearch
    state: present
  become: true

                                                [ Read 24 lines ]
^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

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.

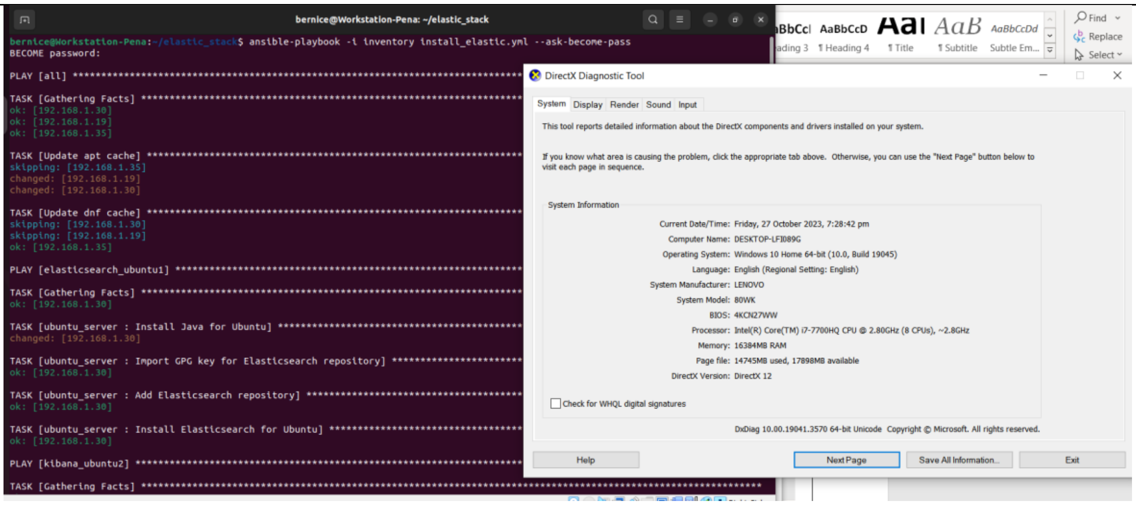
System Information

Current Date/Time: Friday, 27 October 2023, 12:47:35 am
Computer Name: DESKTOP-LFI089G
Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: LENOVO
System Model: 80WK
BIOS: 4KCN27WW
Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
Memory: 16384MB RAM
Page file: 4099MB used, 28543MB available
DirectX Version: DirectX 12

□ Check for WHQL digital signatures

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

In my roles/ubuntu_server/tasks directory, I created a main.yml file that consists of the tasks to be executed for installing Elasticsearch on my ubuntu server 1.



bernice@Workstation-Pena: ~/elastic_stack
AaBbCcI AaBbCcD AaI AaB AaBbCcDd
ading 3 ¶ Heading 4 ¶ Title ¶ Subtitle Subtle Em...
Find
Replace
Select

```
bernice@Workstation-Pena:~/elastic_stack$ ansible-playbook -i inventory install_elastic.yml --ask-become-pass
BECOME password:

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

TASK [Gathering Facts] ******************************************************************
ok: [192.168.1.30]
ok: [192.168.1.19]
ok: [192.168.1.35]

TASK [Update apt cache] *****************************************************************
skipping: [192.168.1.35]
changed: [192.168.1.19]
changed: [192.168.1.30]

TASK [Update dnf cache] *****************************************************************
skipping: [192.168.1.30]
skipping: [192.168.1.19]
ok: [192.168.1.35]

PLAY [elasticsearch_ubuntu1] ************************************************************

TASK [Gathering Facts] ******************************************************************
ok: [192.168.1.30]

TASK [ubuntu_server : Install Java for Ubuntu] ******************************************
changed: [192.168.1.30]

TASK [ubuntu_server : Import GPG key for Elasticsearch repository] **********************
ok: [192.168.1.30]

TASK [ubuntu_server : Add Elasticsearch repository] *************************************
ok: [192.168.1.30]

TASK [ubuntu_server : Install Elasticsearch for Ubuntu] *********************************
ok: [192.168.1.30]

PLAY [kibana_ubuntu2] *******************************************************************

TASK [Gathering Facts] ******************************************************************
```

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

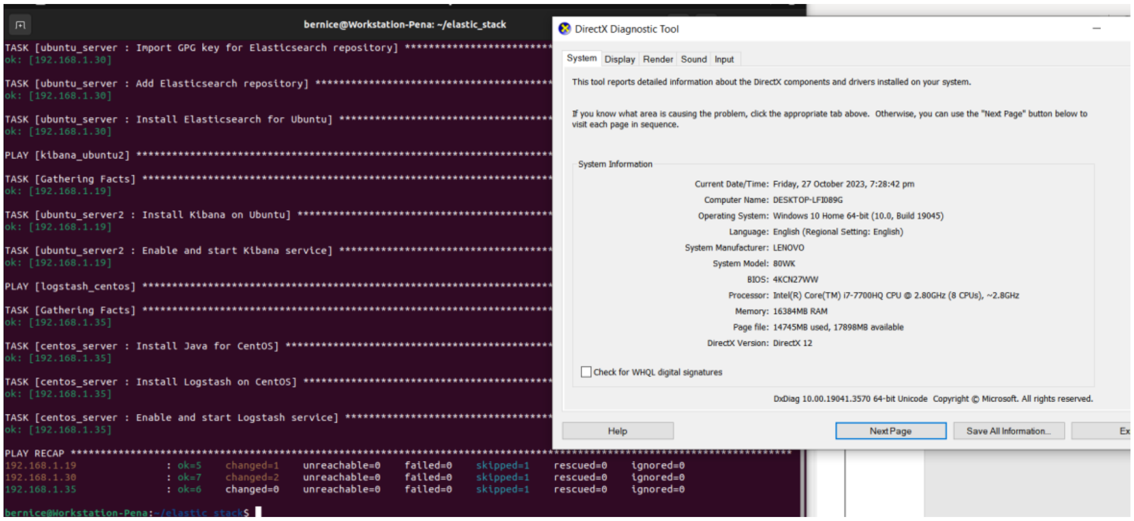
If you know what area is causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button below to visit each page in sequence.

System Information

Current Date/Time:	Friday, 27 October 2023, 7:28:42 pm
Computer Name:	DESKTOP-LFI089G
Operating System:	Windows 10 Home 64-bit (10.0, Build 19045)
Language:	English (Regional Setting: English)
System Manufacturer:	LENOVO
System Model:	80WK
BIOS:	4KCN27WW
Processor:	Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
Memory:	16384MB RAM
Page file:	14745MB used, 17898MB available
DirectX Version:	DirectX 12

☐ Check for WHQL digital signatures

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



```
TASK [ubuntu_server : Import GPG key for Elasticsearch repository] **********************
ok: [192.168.1.30]

TASK [ubuntu_server : Add Elasticsearch repository] *************************************
ok: [192.168.1.30]

TASK [ubuntu_server : Install Elasticsearch for Ubuntu] *********************************
ok: [192.168.1.30]

PLAY [kibana_ubuntu2] *******************************************************************

TASK [Gathering Facts] ******************************************************************
ok: [192.168.1.19]

TASK [ubuntu_server2 : Install Kibana on Ubuntu] ****************************************
ok: [192.168.1.19]

TASK [ubuntu_server2 : Enable and start Kibana service] *********************************
ok: [192.168.1.19]

PLAY [logstash_centos] ******************************************************************

TASK [Gathering Facts] ******************************************************************
ok: [192.168.1.35]

TASK [centos_server : Install Java for CentOS] ******************************************
ok: [192.168.1.35]

TASK [centos_server : Install Logstash on CentOS] ***************************************
ok: [192.168.1.35]

TASK [centos_server : Enable and start Logstash service] ********************************
ok: [192.168.1.35]

PLAY RECAP ******************************************************************************
192.168.1.19               : ok=5    changed=1    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0
192.168.1.30               : ok=7    changed=2    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0
192.168.1.35               : ok=6    changed=0    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0

bernice@Workstation-Pena:~/elastic_stack$
```

DirectX Diagnostic Tool

System Display Render 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

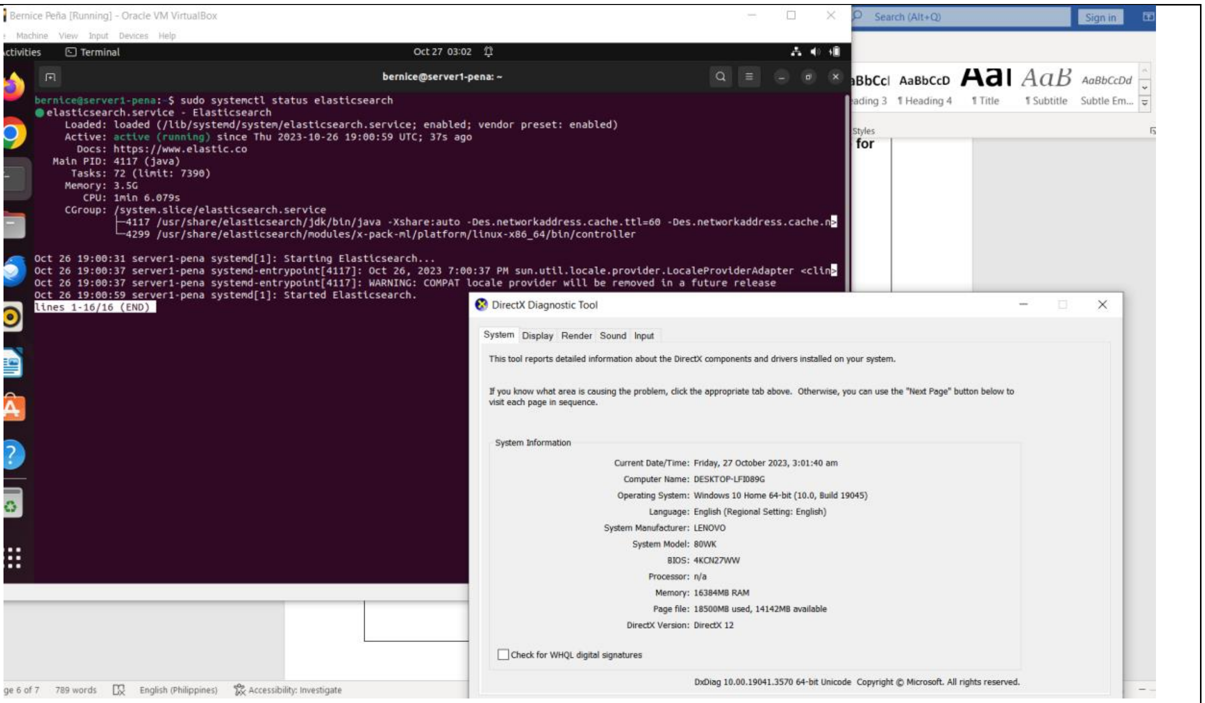
Current Date/Time: Friday, 27 October 2023, 7:28:42 pm
Computer Name: DESKTOP-LFI089G
Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: LENOVO
System Model: 80WK
BIOS: 4KCN27WW
Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
Memory: 16384MB RAM
Page file: 14745MB used, 17898MB 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... Ex

After executing my playbook install_elastic.yml, the installation process for Elastic Stack that includes Elasticsearch, Kibana, and Logstash was successfully installed. As it is stated in the results, the status for the installation of Elastic Stack for a specific server indicates a status of “ok” and “changed”, this is because of the installation process that I’ve made for the servers.


Bernice Peña [Running] - Oracle VM VirtualBox
Machine View Input Devices Help
Activities
Terminal
Oct 27 03:02
bernice@server1-pena: ~
Search (Alt+Q)
Sign in
AaBbCcI AaBbCcD AaI AaB AaBbCcDd
Heading 3 ¶ Heading 4 ¶ Title ¶ Subtitle Subtle Em...
Styles
for
DirectX Diagnostic Tool
System Display Render Sound Input
Page 6 of 7 789 words English (Philippines) Accessibility: Investigate

```
bernice@server1-pena:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-10-26 19:00:59 UTC; 37s ago
       Docs: https://www.elastic.co
   Main PID: 4117 (java)
      Tasks: 72 (limit: 7390)
     Memory: 3.5G
        CPU: 1min 6.079s
     CGroup: /system.slice/elasticsearch.service
             ├─4117 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.n>
             └─4299 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Oct 26 19:00:31 server1-pena systemd[1]: Starting Elasticsearch...
Oct 26 19:00:37 server1-pena systemd-entrypoint[4117]: Oct 26, 2023 7:00:37 PM sun.util.locale.provider.LocaleProviderAdapter <clin>
Oct 26 19:00:37 server1-pena systemd-entrypoint[4117]: WARNING: COMPAT locale provider will be removed in a future release
Oct 26 19:00:59 server1-pena 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.

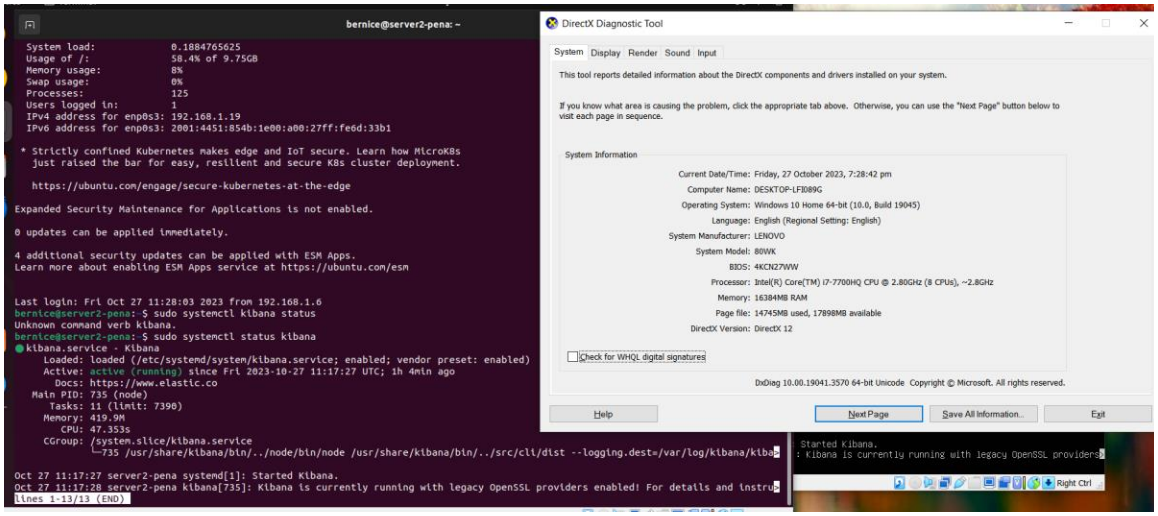
System Information

Current Date/Time: Friday, 27 October 2023, 3:01:40 am
Computer Name: DESKTOP-LFI089G
Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: LENOVO
System Model: 80WK
BIOS: 4KCN27WW
Processor: n/a
Memory: 16384MB RAM
Page file: 18500MB used, 14142MB available
DirectX Version: DirectX 12

☐ Check for WHQL digital signatures

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

I check the status of elasticsearch on my ubuntu server to verify if it is installed. As you can see here, it indicates that the status of it is active(running), this means that the elasticsearch was successfully installed and started.



```
  System load:              0.1884765625
  Usage of /:               58.4% of 9.75GB
  Memory usage:             8%
  Swap usage:               0%
  Processes:                125
  Users logged in:          1
  IPv4 address for enp0s3: 192.168.1.19
  IPv6 address for enp0s3: 2001:4451:854b:1e00:a00:27ff:fe6d:33b1

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

4 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


Last login: Fri Oct 27 11:28:03 2023 from 192.168.1.6
bernice@server2-pena:~$ sudo systemctl kibana status
Unknown command verb kibana.
bernice@server2-pena:~$ sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2023-10-27 11:17:27 UTC; 1h 4min ago
       Docs: https://www.elastic.co
   Main PID: 735 (node)
      Tasks: 11 (limit: 7390)
     Memory: 419.9M
        CPU: 47.353s
     CGroup: /system.slice/kibana.service
             └─735 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist --logging.dest=/var/log/kibana/kiba>

Oct 27 11:17:27 server2-pena systemd[1]: Started Kibana.
Oct 27 11:17:28 server2-pena kibana[735]: Kibana is currently running with legacy OpenSSL providers enabled! For details and instru>
lines 1-13/13 (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

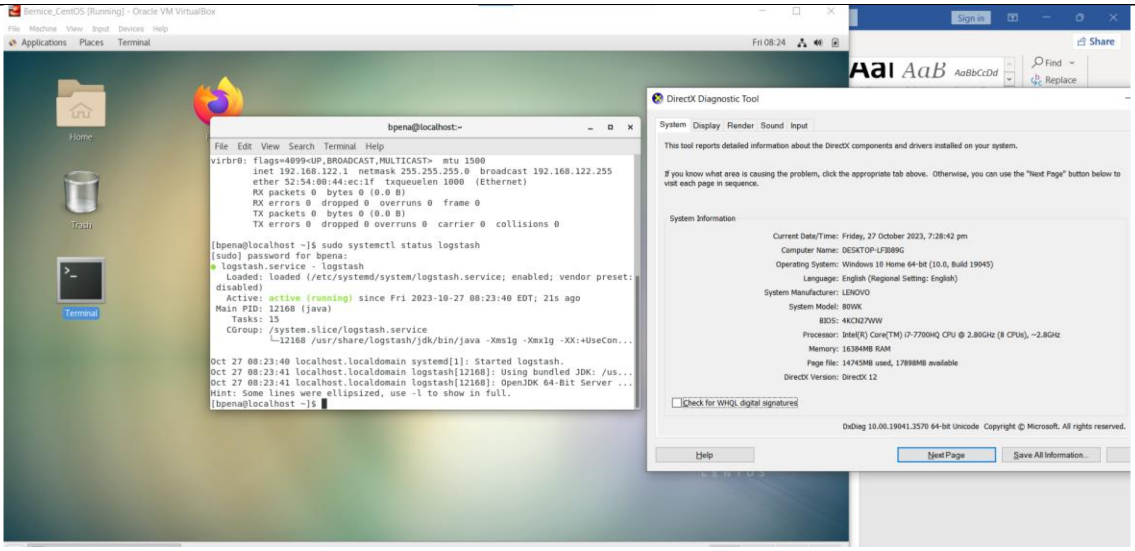
Current Date/Time: Friday, 27 October 2023, 7:28:42 pm
Computer Name: DESKTOP-LFI089G
Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: LENOVO
System Model: 80WK
BIOS: 4KCN27WW
Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
Memory: 16384MB RAM
Page file: 14745MB used, 17898MB available
DirectX Version: DirectX 12

☐ Check for WHQL digital signatures

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

```
Started Kibana.
: Kibana is currently running with legacy OpenSSL providers>
```

This is to verify that the status of Kibana is running and already started.


Bernice_CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Fri 08:24
Home
Trash
Terminal
bpena@localhost:~
File Edit View Search Terminal Help
Sign in
Share
Find
Replace

```
virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:44:ec:1f  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[bpena@localhost ~]$ sudo systemctl status logstash
[sudo] password for bpena:
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset:
 disabled)
   Active: active (running) since Fri 2023-10-27 08:23:40 EDT; 21s ago
 Main PID: 12168 (java)
    Tasks: 15
   CGroup: /system.slice/logstash.service
           └─12168 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCon...

Oct 27 08:23:40 localhost.localdomain systemd[1]: Started logstash.
Oct 27 08:23:41 localhost.localdomain logstash[12168]: Using bundled JDK: /us...
Oct 27 08:23:41 localhost.localdomain logstash[12168]: OpenJDK 64-Bit Server ...
Hint: Some lines were ellipsized, use -l to show in full.
[bpena@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.

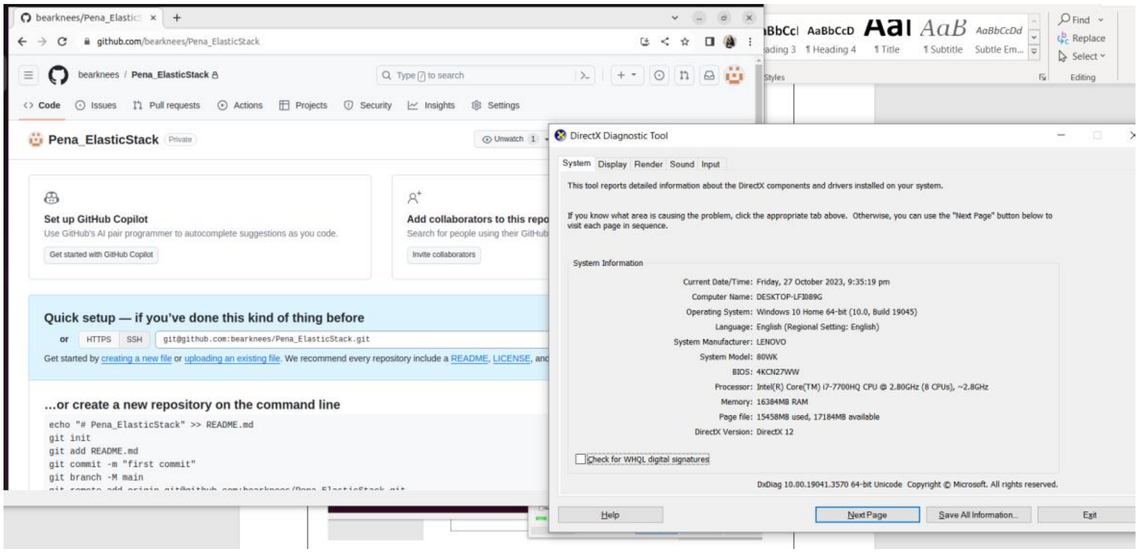
System Information

Current Date/Time: Friday, 27 October 2023, 7:28:42 pm
Computer Name: DESKTOP-LFI089G
Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: LENOVO
System Model: 80WK
BIOS: 4KCN27WW
Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
Memory: 16384MB RAM
Page file: 14745MB used, 17898MB available
DirectX Version: DirectX 12

□ Check for WHQL digital signatures

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

I also checked the status of logstash to verify that it is running and already started.


bearknees/Pena_Elastic
github.com/bearknees/Pena_ElasticStack
bearknees / Pena_ElasticStack
Type / to search
Code Issues Pull requests Actions Projects Security Insights Settings
Unwatch 1
Private
Get started with GitHub Copilot
Invite collaborators
HTTPS SSH
Find
Replace
Select
Styles
Editing

Pena_ElasticStack

Set up GitHub Copilot
Use GitHub's AI pair programmer to autocomplete suggestions as you code.

Add collaborators to this repo
Search for people using their GitHub

Quick setup — if you've done this kind of thing before

or HTTPS SSH git@github.com:bearknees/Pena_ElasticStack.git

Get started by creating a new file or uploading an existing file. We recommend every repository include a README, LICENSE, and

...or create a new repository on the command line

```
echo "# Pena_ElasticStack" >> README.md
git init
git add README.md
git commit -m "first commit"
git branch -M main
```

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.

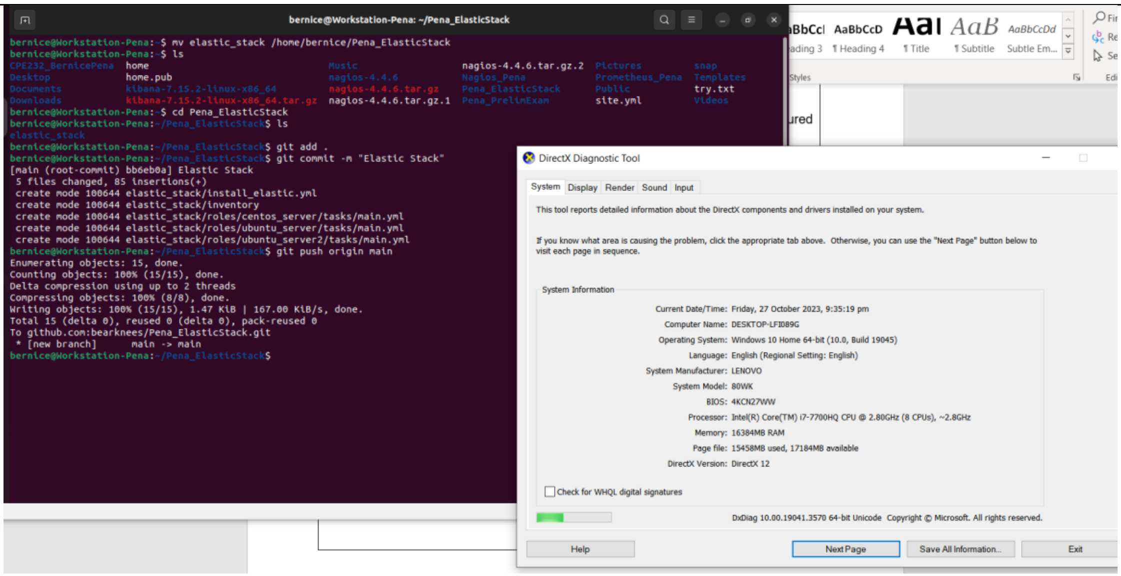
System Information

Current Date/Time: Friday, 27 October 2023, 9:35:19 pm
Computer Name: DESKTOP-LFI089G
Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: LENOVO
System Model: 80WK
BIOS: 4KCN27WW
Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
Memory: 16384MB RAM
Page file: 15458MB used, 17184MB available
DirectX Version: DirectX 12

□ Check for WHQL digital signatures

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

I create a repository on my GitHub named Pena_ElasticStack, this is where I will commit and push my elastic_stack directory



```
bernice@Workstation-Pena:~$ mv elastic_stack /home/bernice/Pena_ElasticStack
bernice@Workstation-Pena:~$ ls
CPE232_BernicePena  home                              Music                 nagios-4.4.6.tar.gz.2  Pictures          snap
Desktop             home.pub                          nagios-4.4.6          Nagios_Pena            Prometheus_Pena   Templates
Documents           kibana-7.15.2-linux-x86_64        nagios-4.4.6.tar.gz   Pena_ElasticStack      Public            try.txt
Downloads           kibana-7.15.2-linux-x86_64.tar.gz nagios-4.4.6.tar.gz.1 Pena_PrelimExam        site.yml          Videos
bernice@Workstation-Pena:~$ cd Pena_ElasticStack
bernice@Workstation-Pena:~/Pena_ElasticStack$ ls
elastic_stack
bernice@Workstation-Pena:~/Pena_ElasticStack$ git add .
bernice@Workstation-Pena:~/Pena_ElasticStack$ git commit -m "Elastic Stack"
[main (root-commit) bb6eb0a] Elastic Stack
 5 files changed, 85 insertions(+)
 create mode 100644 elastic_stack/install_elastic.yml
 create mode 100644 elastic_stack/inventory
 create mode 100644 elastic_stack/roles/centos_server/tasks/main.yml
 create mode 100644 elastic_stack/roles/ubuntu_server/tasks/main.yml
 create mode 100644 elastic_stack/roles/ubuntu_server2/tasks/main.yml
bernice@Workstation-Pena:~/Pena_ElasticStack$ git push origin main
Enumerating objects: 15, done.
Counting objects: 100% (15/15), done.
Delta compression using up to 2 threads
Compressing objects: 100% (8/8), done.
Writing objects: 100% (15/15), 1.47 KiB | 167.00 KiB/s, done.
Total 15 (delta 0), reused 0 (delta 0), pack-reused 0
To github.com:bearknees/Pena_ElasticStack.git
 * [new branch]      main -> main
bernice@Workstation-Pena:~/Pena_ElasticStack$
```

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.

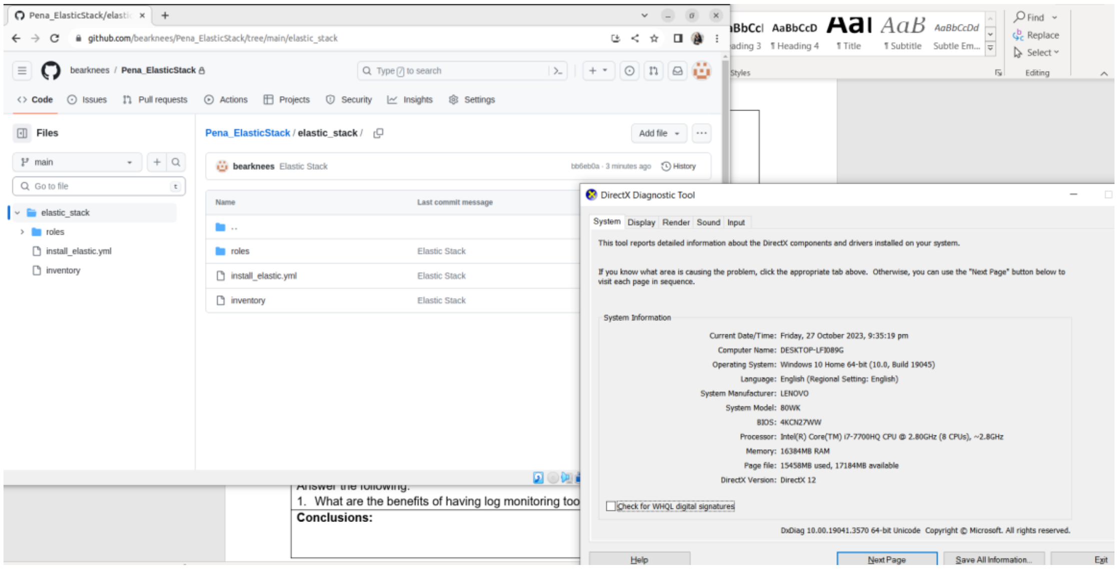
System Information

Current Date/Time: Friday, 27 October 2023, 9:35:19 pm
Computer Name: DESKTOP-LFI089G
Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: LENOVO
System Model: 80WK
BIOS: 4KCN27WW
Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
Memory: 16384MB RAM
Page file: 15458MB used, 17184MB available
DirectX Version: DirectX 12

□ Check for WHQL digital signatures

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

Then I cloned the repository and moved my elastic_stack directory to my Pena_ElasticStack. After this, I used the commit command to add my files in my GitHub repository.



github.com/bearknees/Pena_ElasticStack/tree/main/elastic_stack

bearknees / Pena_ElasticStack

Pena_ElasticStack / elastic_stack /

bearknees Elastic Stack bb6eb0a · 3 minutes ago

Name	Last commit message
..	
roles	Elastic Stack
install_elastic.yml	Elastic Stack
inventory	Elastic Stack

Answer the following:

1. What are the benefits of having log monitoring too

Conclusions:

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, 9:35:19 pm
Computer Name: DESKTOP-LFI089G
Operating System: Windows 10 Home 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: LENOVO
System Model: 80WK
BIOS: 4KCN27WW
Processor: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (8 CPUs), ~2.8GHz
Memory: 16384MB RAM
Page file: 15458MB used, 17184MB available
DirectX Version: DirectX 12

□ Check for WHQL digital signatures

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

After committing and pushing all the files, this is the content of my GitHub repository (Pena_ElasticStack) now.

GitHub repository link: https://github.com/bearknees/Pena_ElasticStack

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool?
   Having log monitoring tools provide benefits such as the increased security through the detection of breaches as well as suspicious activities, it improves performance analysis in order to identify potential issues, this will simplify the troubleshooting for quick issue resolution through detailed logs, predictive maintenance, and capabilities for problem-solving. With this being said, log monitoring tools will increase operational efficiency through centralized log management resulting in reduced downtime.

Conclusions:

In this activity, I was able to understand more about the importance of having log monitoring tools, I looked at how to set up the Elastic Stack which is a great tool for log monitoring and analysis. I began by installing Elasticsearch, Kibana, and logstash, I also delved into stack configuration and troubleshooting making me understand more about the concept of roles and tasks. This activity taught me about the importance of improving security, performance analysis, and troubleshooting among other things. I also learned about the complexities of installing and administering Elasticsearch and Kibana since there are different roles of configuration that needs to be done for this. This activity gave a hands-on understanding of the complications and solutions involved in configuring the Elastic Stack as well as its vital role in ensuring stable and secure operations.