Name: Rustom C. Cariño	Date Performed:10/26/2023
Course/Section:CPE31S5	Date Submitted:10/28/2023
Instructor: Engr. 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.

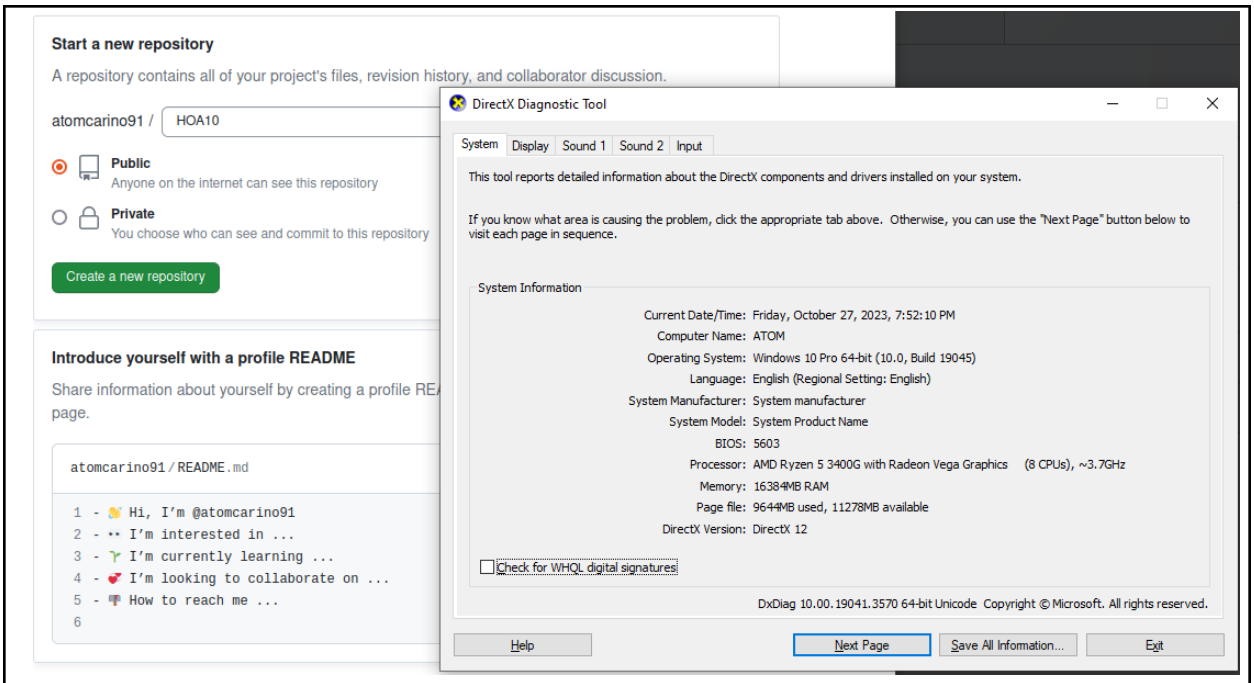
We use Graylog primarily as the stash for the logs of the web applications we build. However, it is also effective when working with raw strings (i.e. syslog): the tool parses it into the structured data we need. It also allows advanced custom search in the logs using structured queries. In other words,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

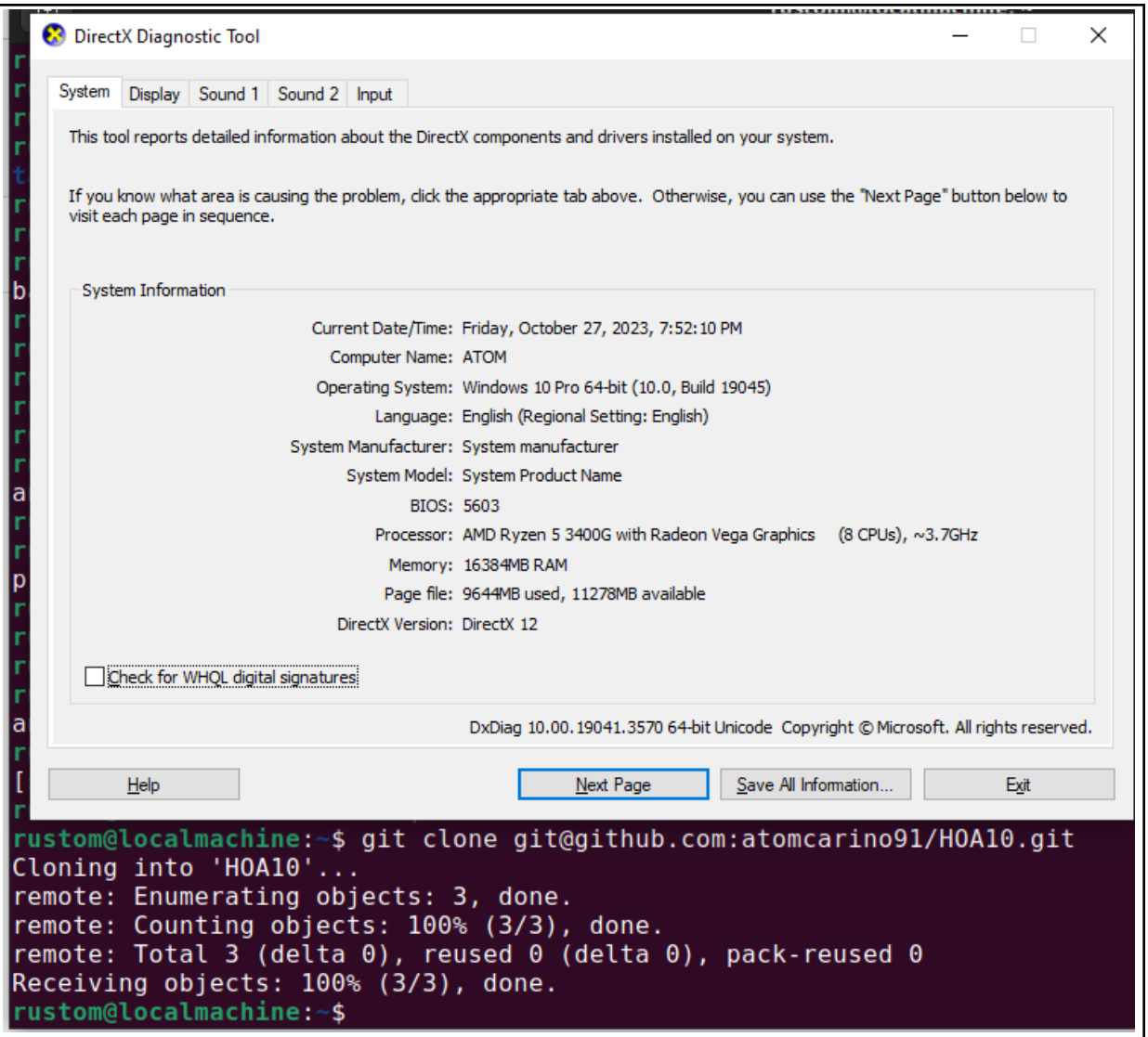
3. Tasks

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.

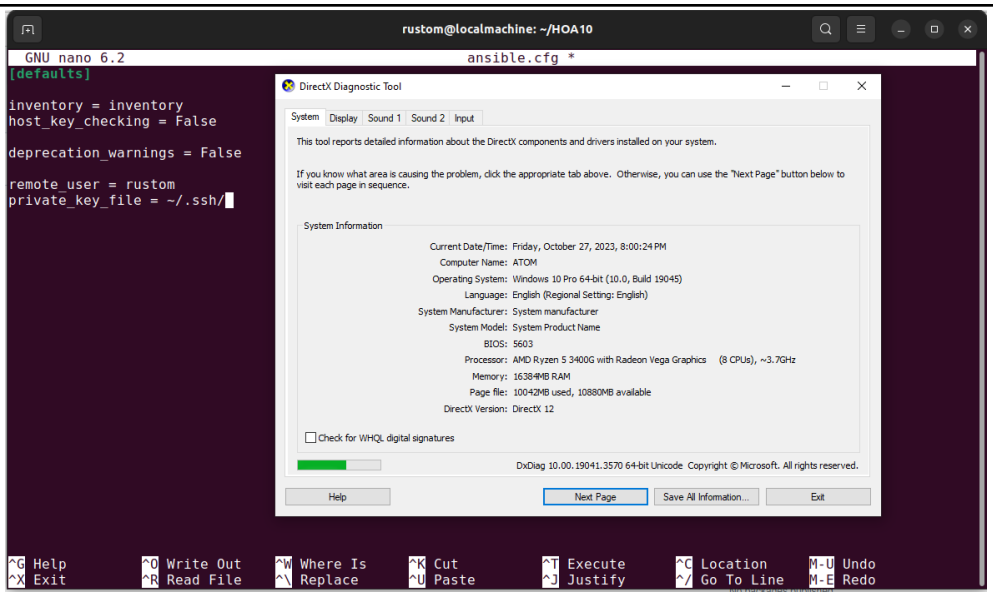
4. Output (screenshots and explanations)

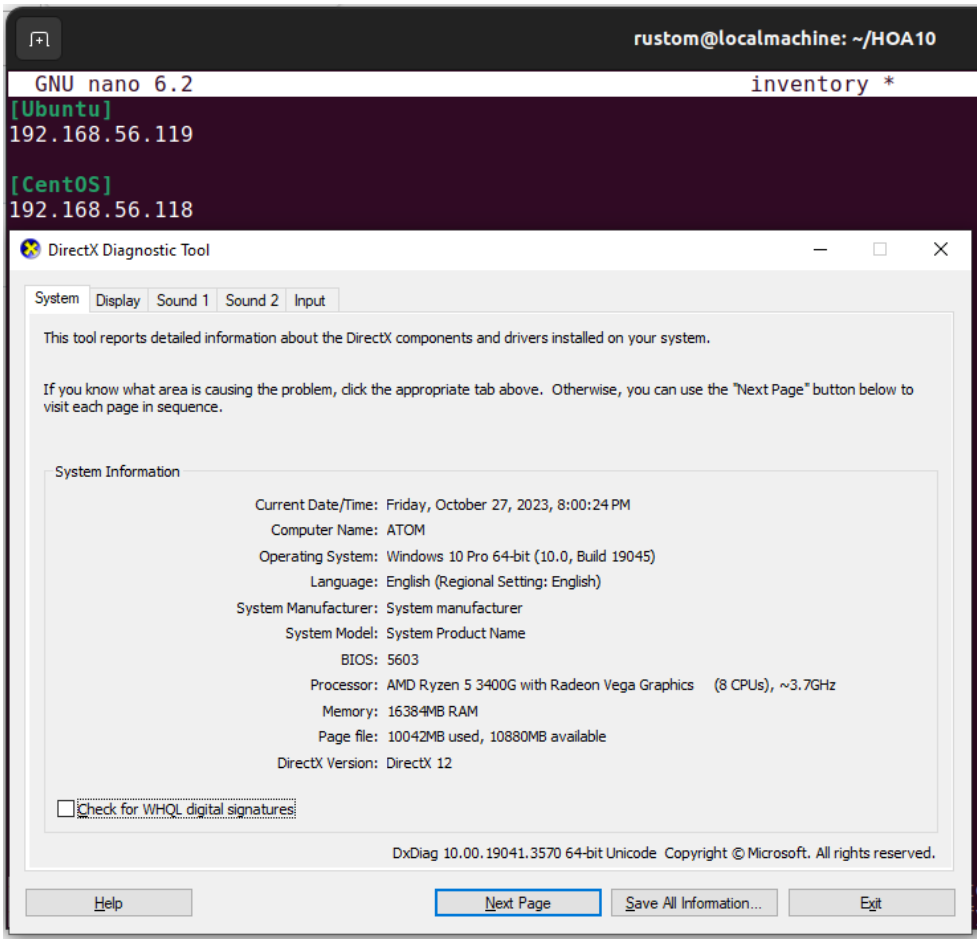


- Creating a new repository named HOA10.

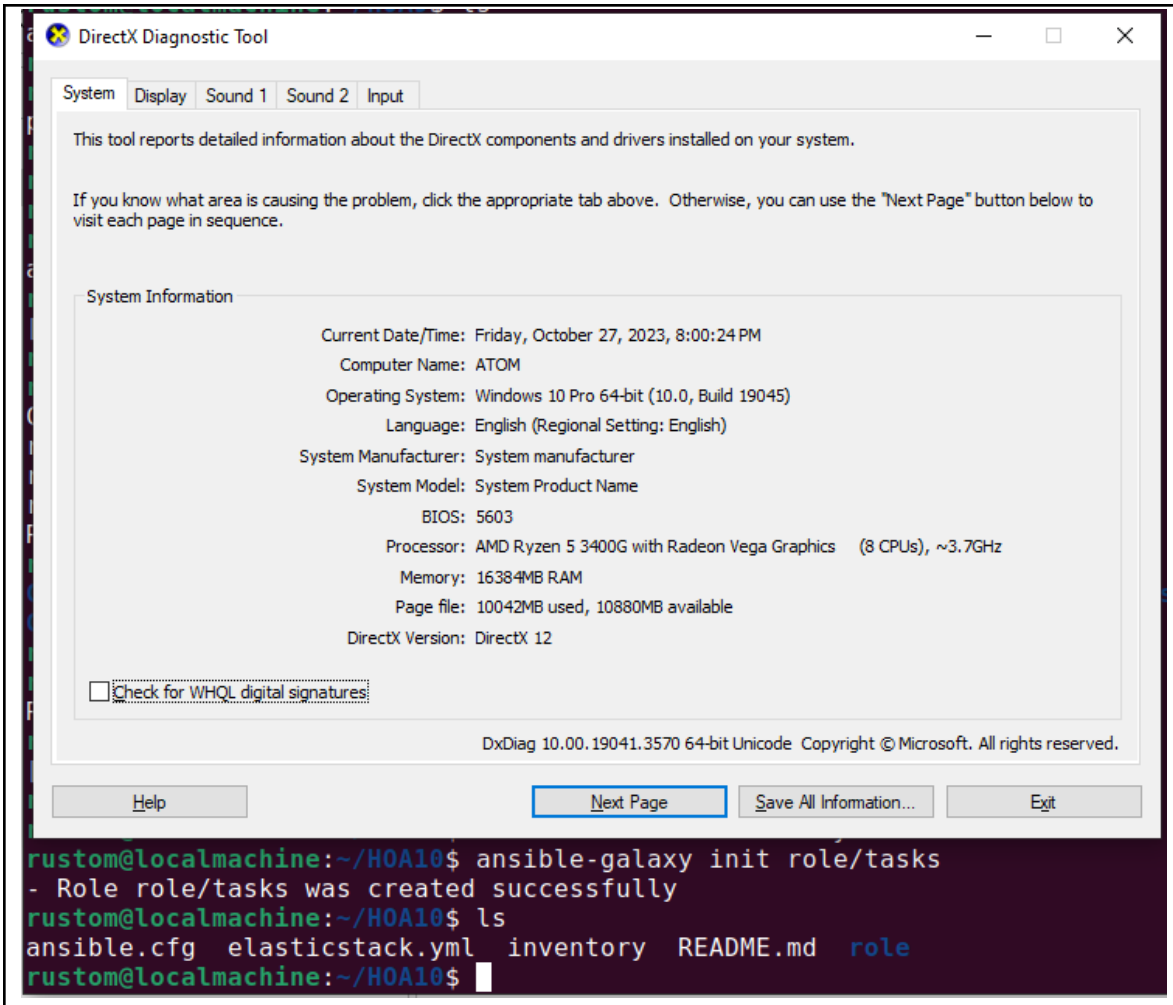


- Cloning the new repository using the git clone command.

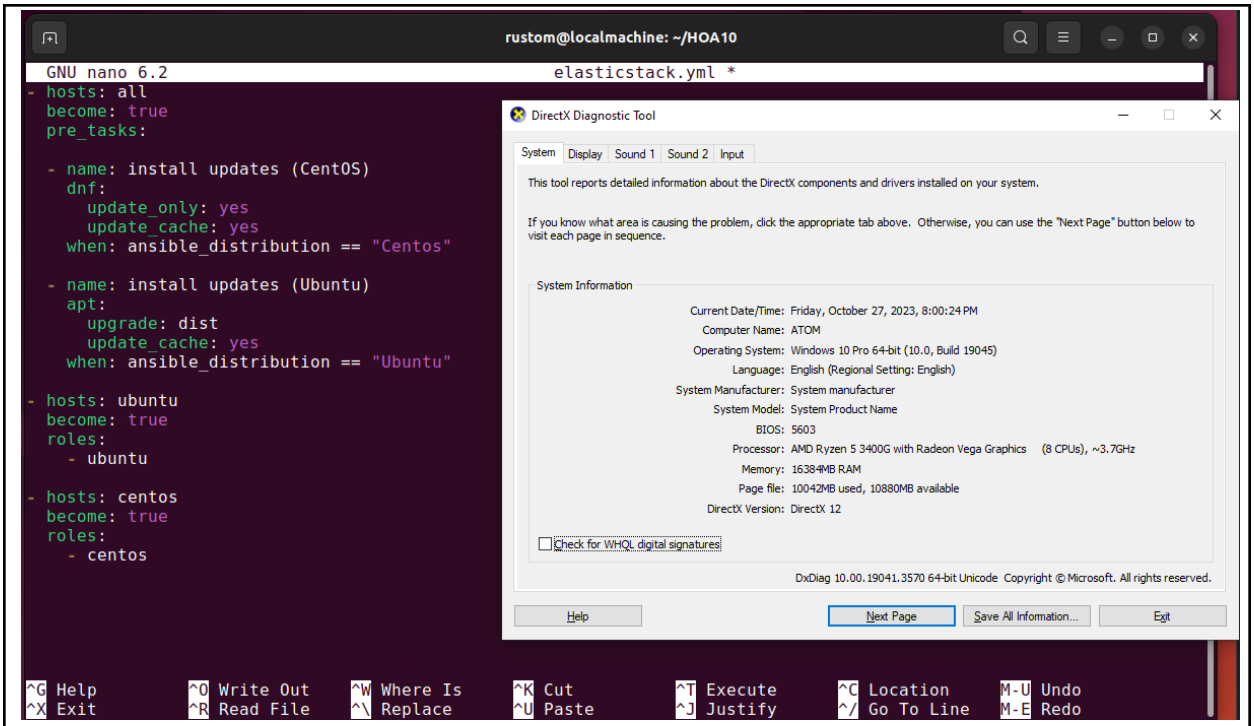




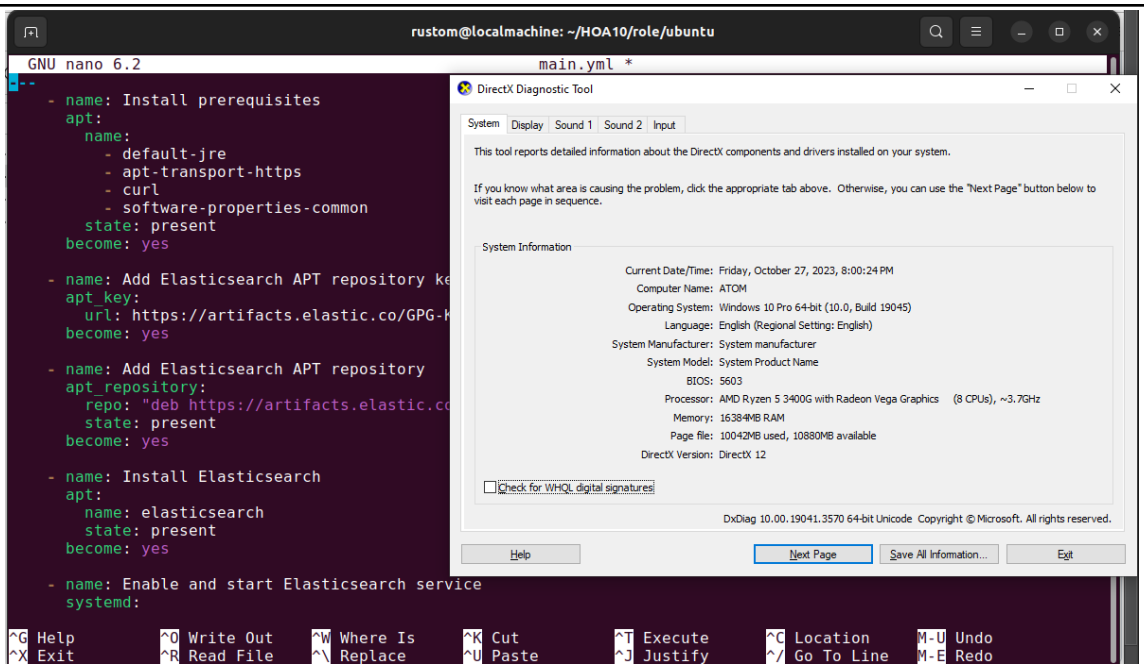
- Creating a new ansible.cfg and inventory in HOA10 repository.

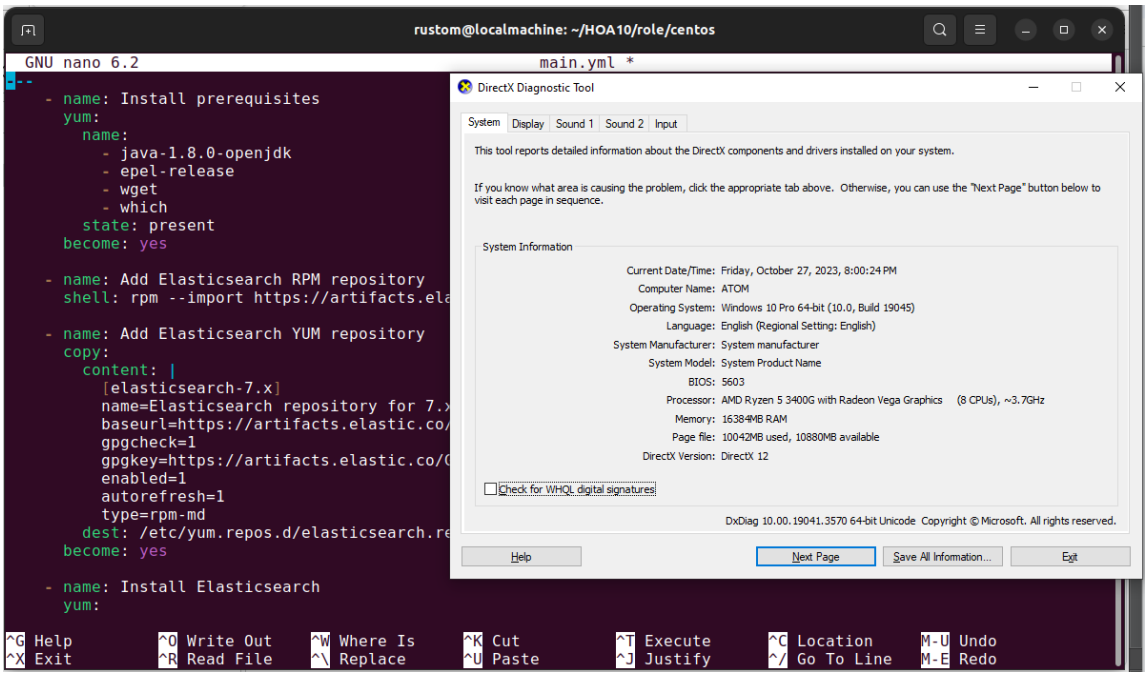


- Creating a role using the ansible-galaxy then it will automatically create a directory that you can implement the roles.

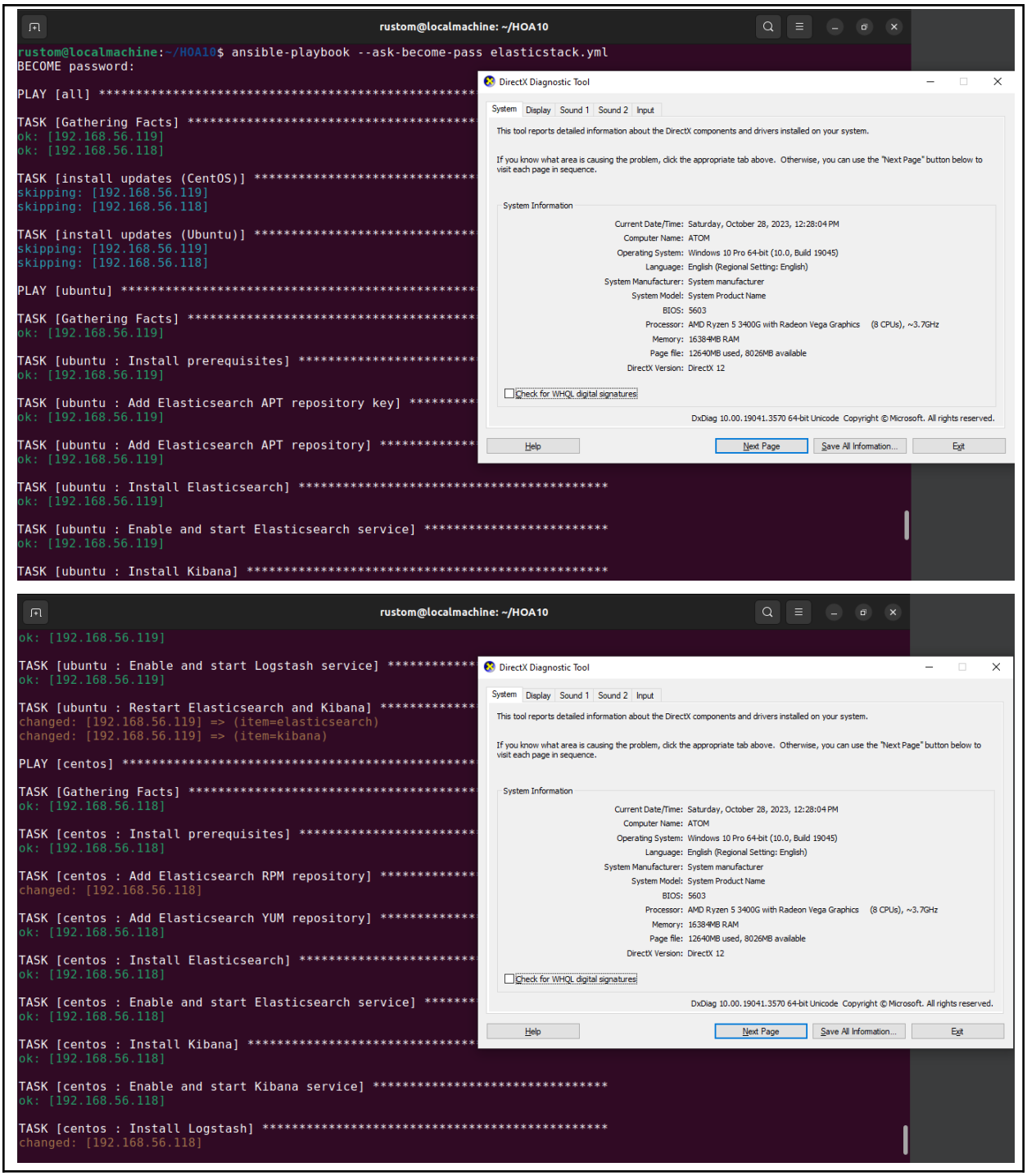


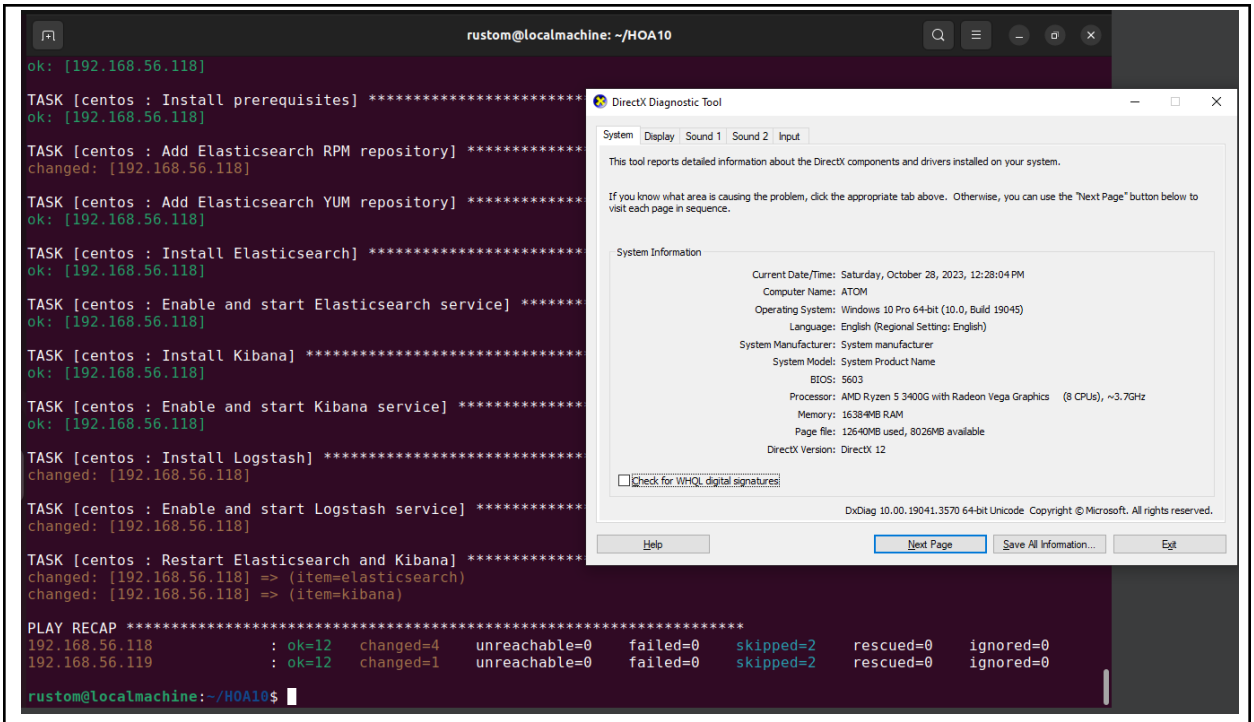
- I created the elasticstack.yml file. This will include the playbook instructions for setting up and maintaining the servers, as well as calls to the main.yml playbooks for their respective functions.





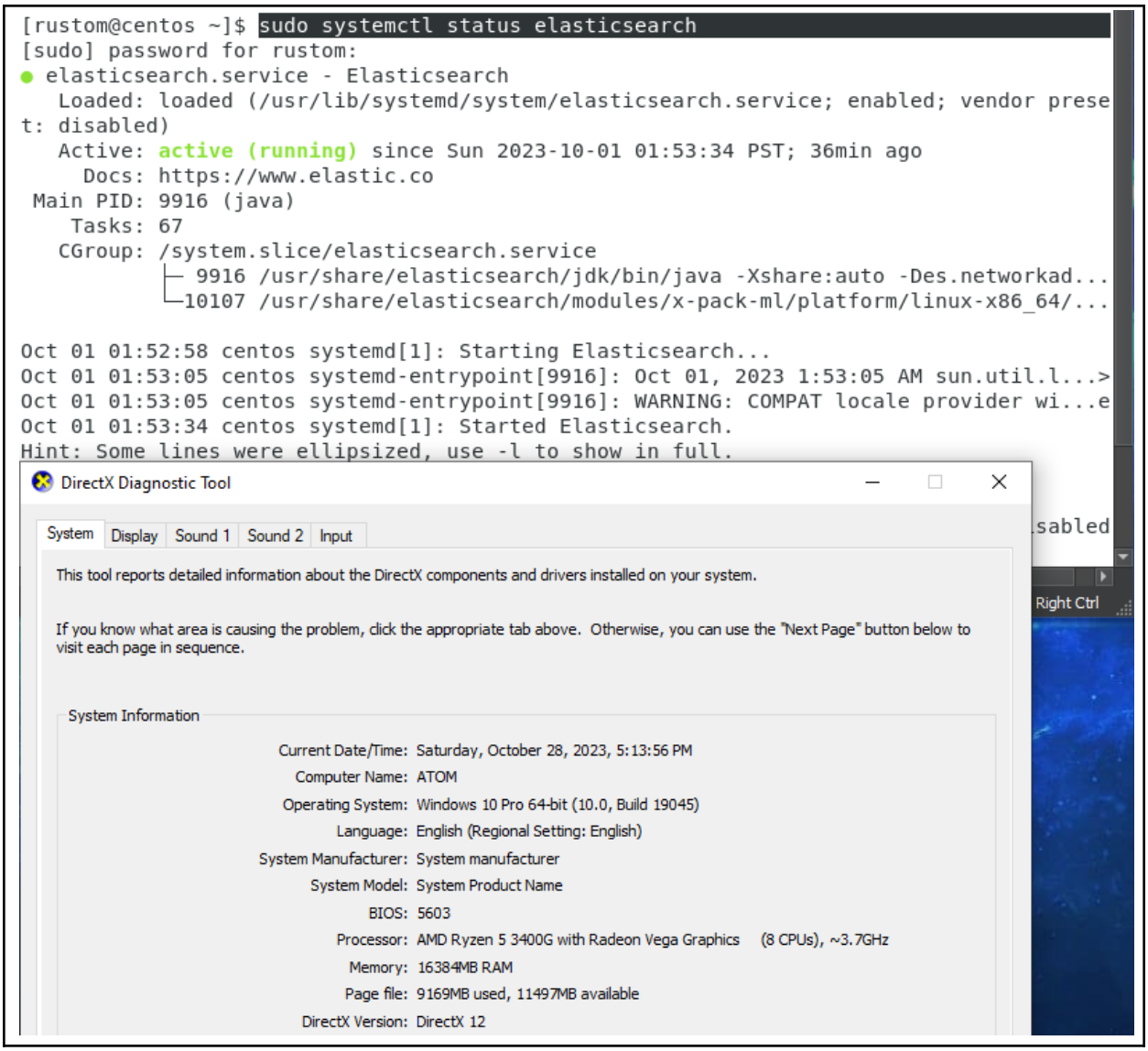
- The playbook includes all the essential instructions to set up every need for the Elastic Stack to function on Ubuntu and Centos. After this, it will add the Elasticsearch APT repository key and apt repository before completing the installation of Elasticsearch and Kibana. These procedures are activated and started after installation. The playbook in each role has the same content since it will just install ElasticSearch, Kibana and Logstash.

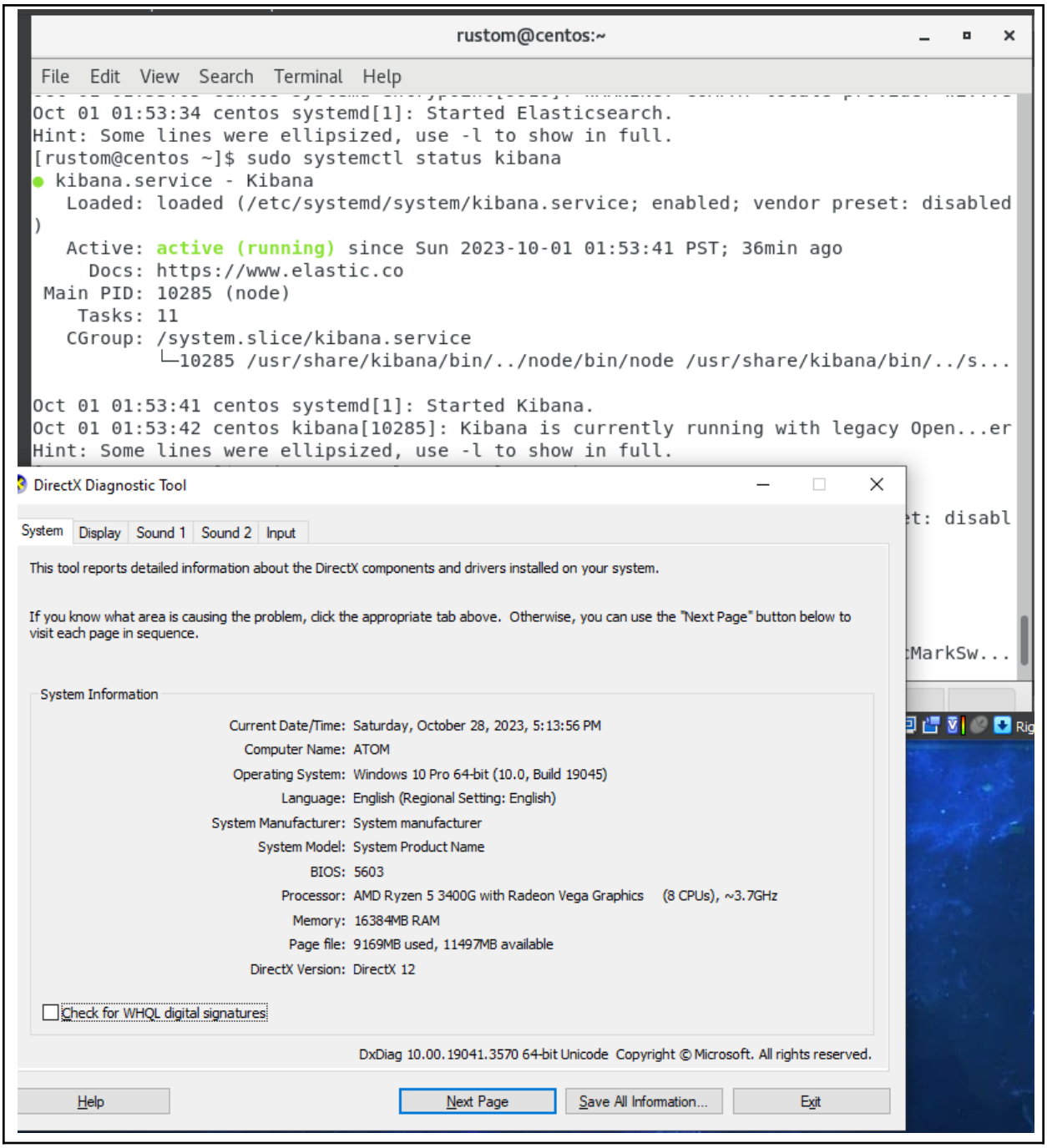

rustom@localmachine: ~/HOA10
rustom@localmachine:~/HOA10$ ansible-playbook --ask-become-pass elasticstack.yml
BECOME password:
PLAY [all] ***********
TASK [Gathering Facts] ***********
ok: [192.168.56.119]
ok: [192.168.56.118]
TASK [install updates (CentOS)] ***********
skipping: [192.168.56.119]
skipping: [192.168.56.118]
TASK [install updates (Ubuntu)] ***********
skipping: [192.168.56.119]
skipping: [192.168.56.118]
PLAY [ubuntu] ***********
TASK [Gathering Facts] ***********
ok: [192.168.56.119]
TASK [ubuntu : Install prerequisites] ***********
ok: [192.168.56.119]
TASK [ubuntu : Add Elasticsearch APT repository key] ***********
ok: [192.168.56.119]
TASK [ubuntu : Add Elasticsearch APT repository] ***********
ok: [192.168.56.119]
TASK [ubuntu : Install Elasticsearch] ***********
ok: [192.168.56.119]
TASK [ubuntu : Enable and start Elasticsearch service] ***********
ok: [192.168.56.119]
TASK [ubuntu : Install Kibana] ***********
DirectX Diagnostic Tool
System Display Sound 1 Sound 2 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: Saturday, October 28, 2023, 12:28:04 PM
Computer Name: ATOM
Operating System: Windows 10 Pro 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: System manufacturer
System Model: System Product Name
BIOS: 5603
Processor: AMD Ryzen 5 3400G with Radeon Vega Graphics (8 CPUs), ~3.7GHz
Memory: 16384MB RAM
Page file: 12640MB used, 8026MB 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
rustom@localmachine: ~/HOA10
ok: [192.168.56.119]
TASK [ubuntu : Enable and start Logstash service] ***********
ok: [192.168.56.119]
TASK [ubuntu : Restart Elasticsearch and Kibana] ***********
changed: [192.168.56.119] => (item=elasticsearch)
changed: [192.168.56.119] => (item=kibana)
PLAY [centos] ***********
TASK [Gathering Facts] ***********
ok: [192.168.56.118]
TASK [centos : Install prerequisites] ***********
ok: [192.168.56.118]
TASK [centos : Add Elasticsearch RPM repository] ***********
changed: [192.168.56.118]
TASK [centos : Add Elasticsearch YUM repository] ***********
ok: [192.168.56.118]
TASK [centos : Install Elasticsearch] ***********
ok: [192.168.56.118]
TASK [centos : Enable and start Elasticsearch service] ***********
ok: [192.168.56.118]
TASK [centos : Install Kibana] ***********
ok: [192.168.56.118]
TASK [centos : Enable and start Kibana service] ***********
ok: [192.168.56.118]
TASK [centos : Install Logstash] ***********
changed: [192.168.56.118]
DirectX Diagnostic Tool
System Display Sound 1 Sound 2 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: Saturday, October 28, 2023, 12:28:04 PM
Computer Name: ATOM
Operating System: Windows 10 Pro 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: System manufacturer
System Model: System Product Name
BIOS: 5603
Processor: AMD Ryzen 5 3400G with Radeon Vega Graphics (8 CPUs), ~3.7GHz
Memory: 16384MB RAM
Page file: 12640MB used, 8026MB 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



- Executing the playbook resulted in the play recap of the managed node being changed.

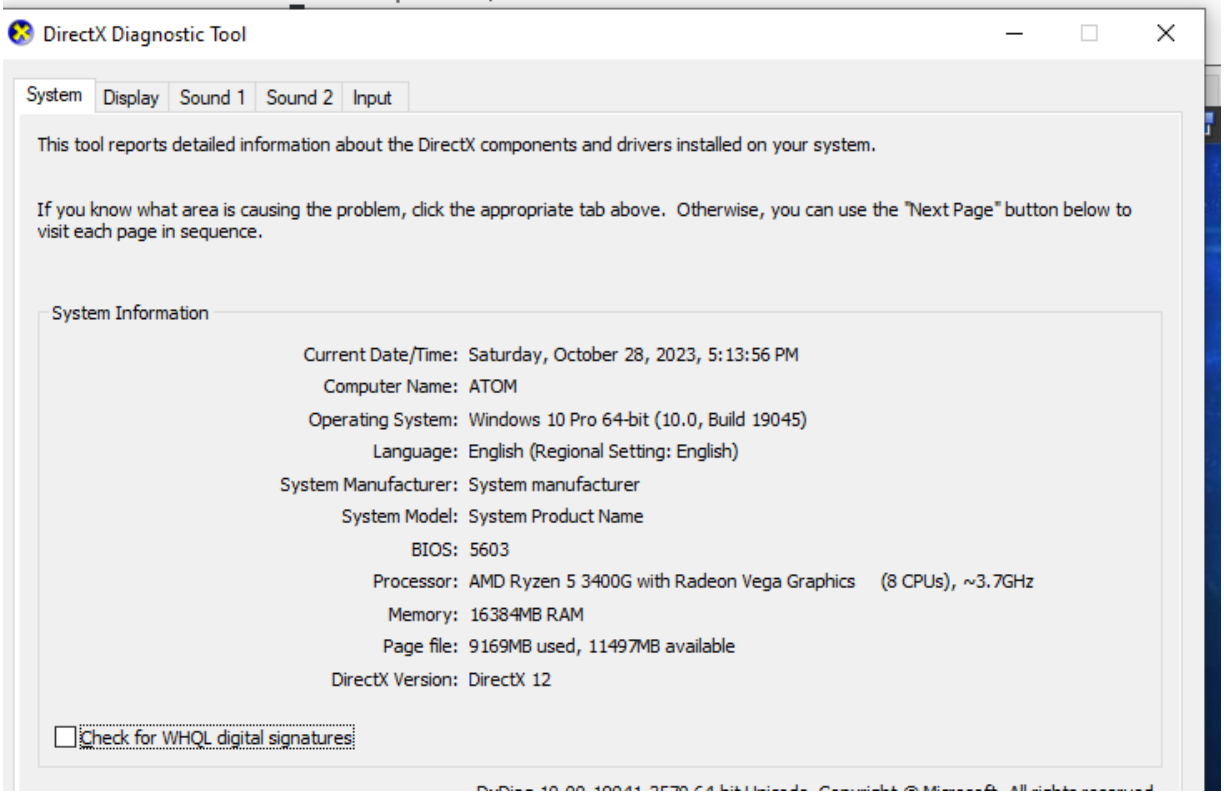
- Proof that the ElasticSearch, Kibana and Logstash were installed in ubuntu.


[rustom@centos ~]$ sudo systemctl status elasticsearch
[sudo] password for rustom:
● elasticsearch.service - Elasticsearch
Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor prese
t: disabled)
Active: active (running) since Sun 2023-10-01 01:53:34 PST; 36min ago
Docs: https://www.elastic.co
Main PID: 9916 (java)
Tasks: 67
CGroup: /system.slice/elasticsearch.service
├─ 9916 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkad...
└─10107 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/...
Oct 01 01:52:58 centos systemd[1]: Starting Elasticsearch...
Oct 01 01:53:05 centos systemd-entrypoint[9916]: Oct 01, 2023 1:53:05 AM sun.util.l...>
Oct 01 01:53:05 centos systemd-entrypoint[9916]: WARNING: COMPAT locale provider wi...e
Oct 01 01:53:34 centos systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
DirectX Diagnostic Tool
System
Display
Sound 1
Sound 2
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: Saturday, October 28, 2023, 5:13:56 PM
Computer Name: ATOM
Operating System: Windows 10 Pro 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: System manufacturer
System Model: System Product Name
BIOS: 5603
Processor: AMD Ryzen 5 3400G with Radeon Vega Graphics (8 CPUs), ~3.7GHz
Memory: 16384MB RAM
Page file: 9169MB used, 11497MB available
DirectX Version: DirectX 12
sabled
Right Ctrl


rustom@centos:~
File Edit View Search Terminal Help
Oct 01 01:53:34 centos systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
[rustom@centos ~]$ sudo systemctl status kibana
● kibana.service - Kibana
Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled
)
Active: active (running) since Sun 2023-10-01 01:53:41 PST; 36min ago
Docs: https://www.elastic.co
Main PID: 10285 (node)
Tasks: 11
CGroup: /system.slice/kibana.service
└─10285 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../s...
Oct 01 01:53:41 centos systemd[1]: Started Kibana.
Oct 01 01:53:42 centos kibana[10285]: Kibana is currently running with legacy Open...er
Hint: Some lines were ellipsized, use -l to show in full.
DirectX Diagnostic Tool
System Display Sound 1 Sound 2 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: Saturday, October 28, 2023, 5:13:56 PM
Computer Name: ATOM
Operating System: Windows 10 Pro 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: System manufacturer
System Model: System Product Name
BIOS: 5603
Processor: AMD Ryzen 5 3400G with Radeon Vega Graphics (8 CPUs), ~3.7GHz
Memory: 16384MB RAM
Page file: 9169MB used, 11497MB 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

```
[rustom@centos ~]$ sudo systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset:
ed)
   Active: active (running) since Sun 2023-10-01 02:30:24 PST; 5s ago
 Main PID: 14674 (java)
    Tasks: 15
   CGroup: /system.slice/logstash.service
           └─14674 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMar

Oct 01 02:30:24 centos systemd[1]: Started logstash.
Oct 01 02:30:24 centos logstash[14674]: Using bundled JDK: /usr/share/logstash/jd
Oct 01 02:30:24 centos logstash[14674]: OpenJDK 64-Bit Server VM warning: Option
Hint: Some lines were ellipsized, use -l to show in full.
```



- Proof that the ElasticSearch, Kibana and Logstash were installed in centos.

Reflections:

Answer the following:

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

   - The benefits of using a log monitoring tool include increased system security. Tools for log monitoring collect and preserve a log of each occasion a system is used or accessed. With the help of preserved logs with the various time stamps, having a copy of these logs may help give an extra degree of protection to the servers and system and assist with resolving any faults that may occur.

Conclusions:

- This hands-on activity focuses on installing, configuring, and managing log monitoring tools, such as the ElasticStack and gray log. The task involves installing and configuring the Elastic Stack, which includes Elasticsearch, Kibana, Beats, and Logstash. Using git and ansible playbook, the tasks can be completed on Ubuntu and CentOS systems. Searching for guides and tutorials online helped in understanding the steps and commands needed, which were then converted into a playbook format.