

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	
<p>Log monitoring software scans and monitors log files generated by servers, applications, and networks. By detecting and alerting users to patterns in these log files, log monitoring software helps solve performance and security issues. System administrators use log monitoring software to detect common important events indicated by log files.</p> <p>Log monitoring software helps maintain IT infrastructure performance and pinpoints issues to prevent downtime and mitigate risks. These tools will often integrate with IT alerting software, log analysis software, and other IT issue resolution products to more aptly flesh out the IT infrastructure maintenance ecosystem.</p> <p>To qualify for inclusion in the Log Monitoring category, a product must:</p> <ul style="list-style-type: none"> • Monitor the log files generated by servers, applications, or networks • Alert users when important events are detected • Provide reporting capabilities for log files <p>Elastic Stack</p> <p>ELK suite stands for Elasticsearch, Kibana, Beats, and Logstash (also known as the ELK Stack). Source: https://www.elastic.co/elastic-stack</p> <p>The Elastic Stack is a group of open source products from Elastic designed to help users take data from any type of source and in any format, and search, analyze and visualize that data in real time. The product group was formerly known as the ELK Stack for the core products in the group -- Elasticsearch, Logstash and Kibana -- but has been rebranded as the Elastic Stack. A fourth product, Beats, was subsequently added to the stack. The Elastic Stack can be deployed on premises or made available as software as a service (SaaS). Elasticsearch supports Amazon Web Services (AWS), Google Cloud Platform and Microsoft Azure.</p> <p>GrayLog</p>	

Graylog is a powerful platform that allows for easy log management of both structured and unstructured data along with debugging applications.

It is based on Elasticsearch, MongoDB, and Scala. Graylog has a main server, which receives data from its clients installed on different servers, and a web interface, which visualizes the data and allows to work with logs aggregated by the main server.

We use Graylog primarily as the stash for the logs of the web applications we build. However, it is also effective when working with raw strings (i.e. syslog): the tool parses it into the structured data we need. It also allows advanced custom search in the logs using structured queries. In other words, when integrated properly with a web app, Graylog helps engineers to analyze the system behavior on almost per code line basis.

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

3. Tasks

1. Create a playbook that:
 - a. Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)
2. Apply the concept of creating roles.
3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like a manual.)
4. Show an output of the installed Elastic Stack for both Ubuntu and CentOS.
5. Make sure to create a new repository in GitHub for this activity.

4. Output (screenshots and explanations)

Start a new repository

A repository contains all of your project's files, revision history, and collaborator discussion.

atomcarino91 / HOA10

Public

Anyone on the internet can see this repository

Private

You choose who can see and commit to this repository

Create a new repository

Introduce yourself with a profile README

Share information about yourself by creating a profile README page.

atomcarino91 / README.md

1 - 🙋 Hi, I'm @atomcarino91

2 - ** I'm interested in ...

3 - 🌱 I'm currently learning ...

4 - ❤️ I'm looking to collaborate on ...

5 - 📧 How to reach me ...

6

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: Friday, October 27, 2023, 7:52:10 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: 9644MB used, 11278MB 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

- Creating a new repository named HOA10.

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: Friday, October 27, 2023, 7:52:10 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: 9644MB used, 11278MB available

DirectX Version: DirectX 12

☐ Check for WHQL digital signatures

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

Help

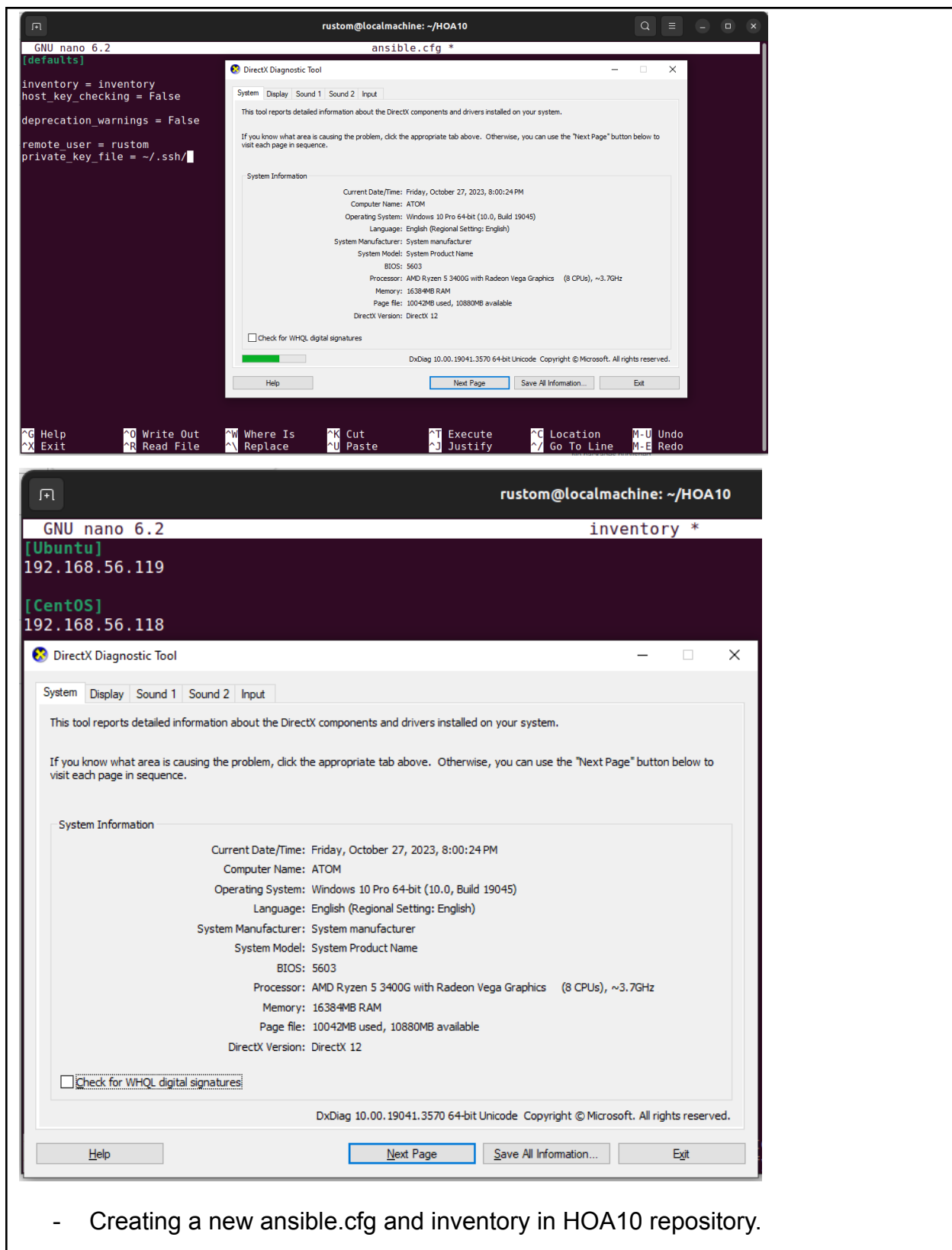
Next Page

Save All Information...

Exit

```
rustom@localmachine:~$ git clone git@github.com:atomcarino91/H0A10.git
Cloning into 'H0A10'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
rustom@localmachine:~$
```

- Cloning the new repository using the git clone command.



DirectX Diagnostic Tool

SystemDisplaySound 1Sound 2Input

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, October 27, 2023, 8:00:24 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: 10042MB used, 10880MB available

DirectX Version: DirectX 12

☐ Check for WHQL digital signatures

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

HelpNext PageSave All Information...Exit

```
rustom@localmachine:~/HOA10$ ansible-galaxy init role/tasks
- Role role/tasks was created successfully
rustom@localmachine:~/HOA10$ ls
ansible.cfg  elasticstack.yml  inventory  README.md  role
rustom@localmachine:~/HOA10$
```

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

The screenshot shows a terminal window with the GNU nano 6.2 editor open, editing a file named `elasticstack.yml`. The terminal title bar indicates the user is `rustom@localmachine` in the directory `~/HOA10`. The playbook content is as follows:

```
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:
    - ubuntu

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

Below the terminal window, a DirectX Diagnostic Tool window is open, displaying system information. The window title is "DirectX Diagnostic Tool". It has tabs for "System", "Display", "Sound 1", "Sound 2", and "Input". The "System" tab is selected. The text inside the window reads:

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, October 27, 2023, 8:00:24 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: 10042MB used, 10880MB available
DirectX Version: DirectX 12

☐ Check for WHQL digital signatures

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

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

Terminal shortcuts at the bottom:

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute	^C Location	M-U Undo
^X Exit	^R Read File	^N Replace	^U Paste	^J Justify	^/_ Go To Line	M-E Redo

- 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 image displays two screenshots of Ansible playbooks and a DirectXTX Diagnostic Tool window.

Top Screenshot (Ubuntu Role): The terminal shows the `main.yml` file for the `ubuntu` role. The playbook includes tasks for installing prerequisites (apt, curl, software-properties-common), adding the Elasticsearch APT repository, installing Elasticsearch, and enabling the service.

```
--
- 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
    state: present
    become: yes

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

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

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

Bottom Screenshot (CentOS Role): The terminal shows the `main.yml` file for the `centos` role. The playbook includes tasks for installing prerequisites (java, epel-release, wget, which), adding the Elasticsearch RPM repository, installing Elasticsearch, and enabling the service.

```
--
- 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
      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
    dest: /etc/yum.repos.d/elasticsearch.repo
    become: yes

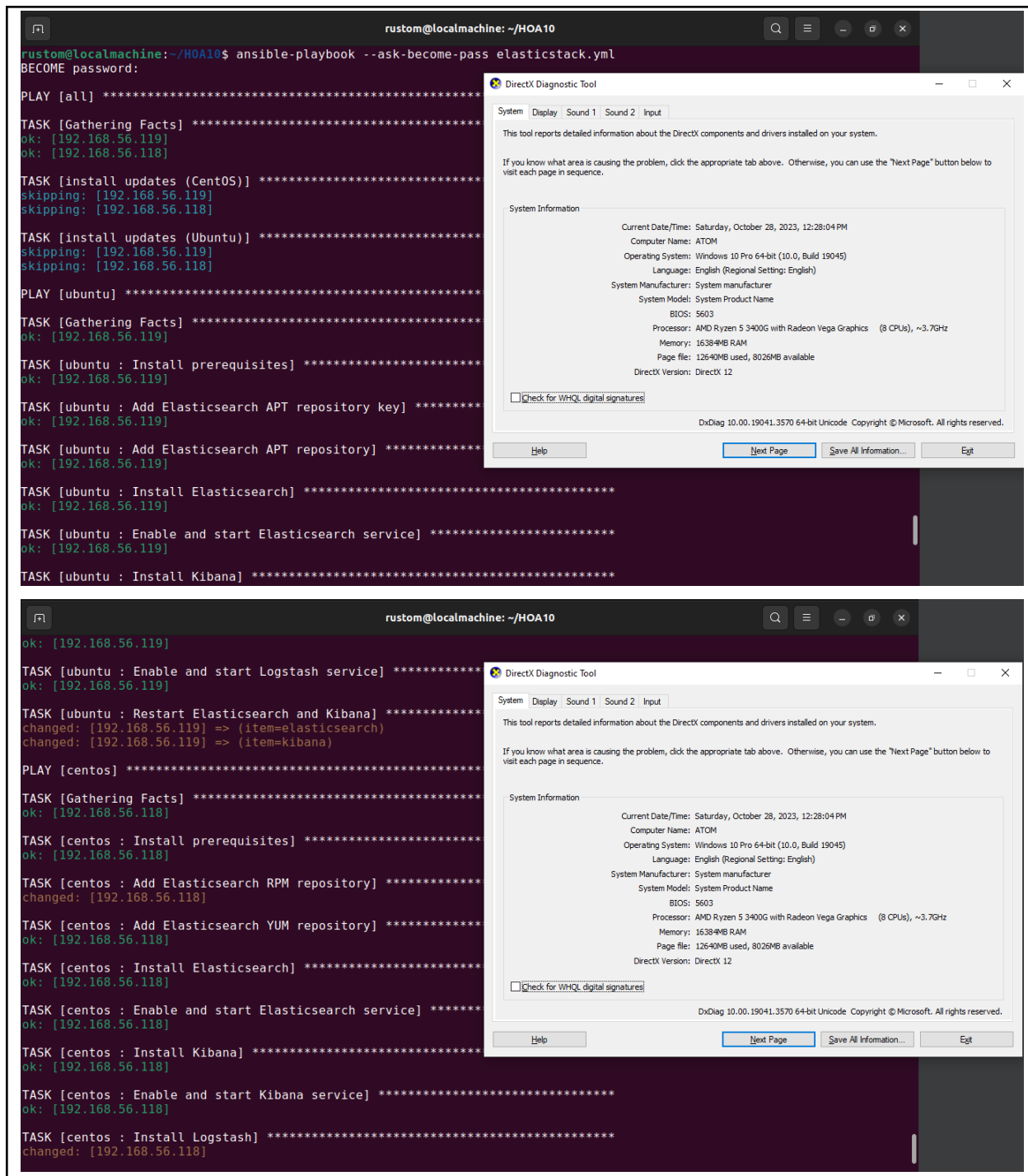
- name: Install Elasticsearch
  yum:
    name: elasticsearch
    state: present
    enabled: true
    restart: true
```

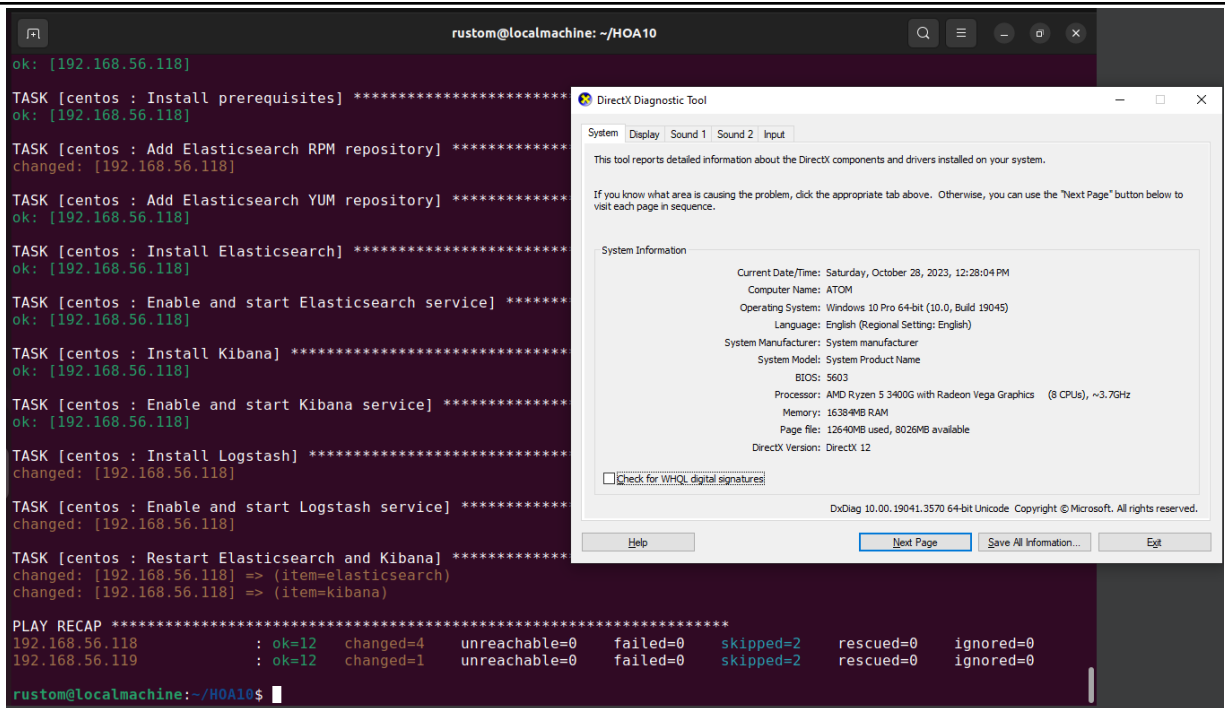
DirectXTX Diagnostic Tool: The window shows system information for a Windows 10 Pro 64-bit system. The system information includes:

- Current Date/Time: Friday, October 27, 2023, 8:00:24 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: 10042MB used, 10880MB available
- DirectX Version: DirectX 12

The window also includes a checkbox for "Check for WHQL digital signatures" and buttons for "Help", "Next Page", "Save All Information...", and "Exit".

- 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.





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

```
rustom@server3: ~  
rustom@server3:~$ sudo systemctl status elasticsearch  
[sudo] password for rustom:  
Unit elasticsearch.service could not be found.  
rustom@server3:~$ sudo systemctl status elasticsearch  
● elasticsearch.service - Elasticsearch  
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)  
   Active: active (running) since Fri 2023-10-27 21:34:52 CST; 15h ago  
     Docs: https://www.elastic.co  
   Main PID: 15784 (java)  
    Tasks: 64 (limit: 2261)  
   Memory: 656.2M  
      CPU: 3min 31.807s  
   CGroup: /system.slice/elasticsearch.service  
           └─15784 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -D  
           └─15965 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/java  
  
Oct 27 21:34:03 server3 systemd[1]: Starting Elasticsearch...  
Oct 27 21:34:13 server3 systemd-entrpoint[15784]: Oct 27, 2023 9:34:13 PM sun.  
Oct 27 21:34:13 server3 systemd-entrpoint[15784]: WARNING: COMPAT locale provider.  
Oct 27 21:34:52 server3 systemd[1]: Started Elasticsearch.  
lines 1-16/16 (END)  
[1]+ Stopped sudo systemctl status elasticsearch  
rustom@server3:~$ 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 21:35:05 CST; 15h ago  
     Docs: https://www.elastic.co  
   Main PID: 16099 (node)  
    Tasks: 11 (limit: 2261)  
   Memory: 113.2M  
      CPU: 1min 3.224s  
   CGroup: /system.slice/kibana.service  
           └─16099 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/kibana  
  
Oct 27 21:35:05 server3 systemd[1]: Started Kibana.  
Oct 27 21:35:08 server3 Kibana[16099]: Kibana is currently running with legacy.  
lines 1-13/13 (END)  
[2]+ Stopped sudo systemctl status kibana  
rustom@server3:~$ sudo systemctl status logstash  
● logstash.service - logstash  
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)  
   Active: active (running) since Sat 2023-10-28 17:15:22 CST; 7s ago  
     Docs: https://www.elastic.co  
   Main PID: 21944 (java)  
    Tasks: 15 (limit: 2261)  
   Memory: 330.3M  
      CPU: 13.079s  
   CGroup: /system.slice/logstash.service  
           └─21944 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseG1GC  
  
Oct 28 17:15:22 server3 systemd[1]: Started logstash.  
Oct 28 17:15:22 server3 logstash[21944]: Using bundled JDK: /usr/share/logstash/jdk  
Oct 28 17:15:22 server3 logstash[21944]: OpenJDK 64-Bit Server VM warning: ...  
lines 1-13/13 (END)  
[4]+ Stopped sudo systemctl status logstash  
rustom@server3:~$
```

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@server3: ~  
rustom@server3:~$ sudo systemctl status logstash  
[sudo] password for rustom:  
● logstash.service - logstash  
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)  
   Active: active (running) since Sat 2023-10-28 17:15:22 CST; 7s ago  
     Docs: https://www.elastic.co  
   Main PID: 21944 (java)  
    Tasks: 15 (limit: 2261)  
   Memory: 330.3M  
      CPU: 13.079s  
   CGroup: /system.slice/logstash.service  
           └─21944 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseG1GC  
  
Oct 28 17:15:22 server3 systemd[1]: Started logstash.  
Oct 28 17:15:22 server3 logstash[21944]: Using bundled JDK: /usr/share/logstash/jdk  
Oct 28 17:15:22 server3 logstash[21944]: OpenJDK 64-Bit Server VM warning: ...  
lines 1-13/13 (END)  
[4]+ Stopped sudo systemctl status logstash  
rustom@server3:~$
```

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

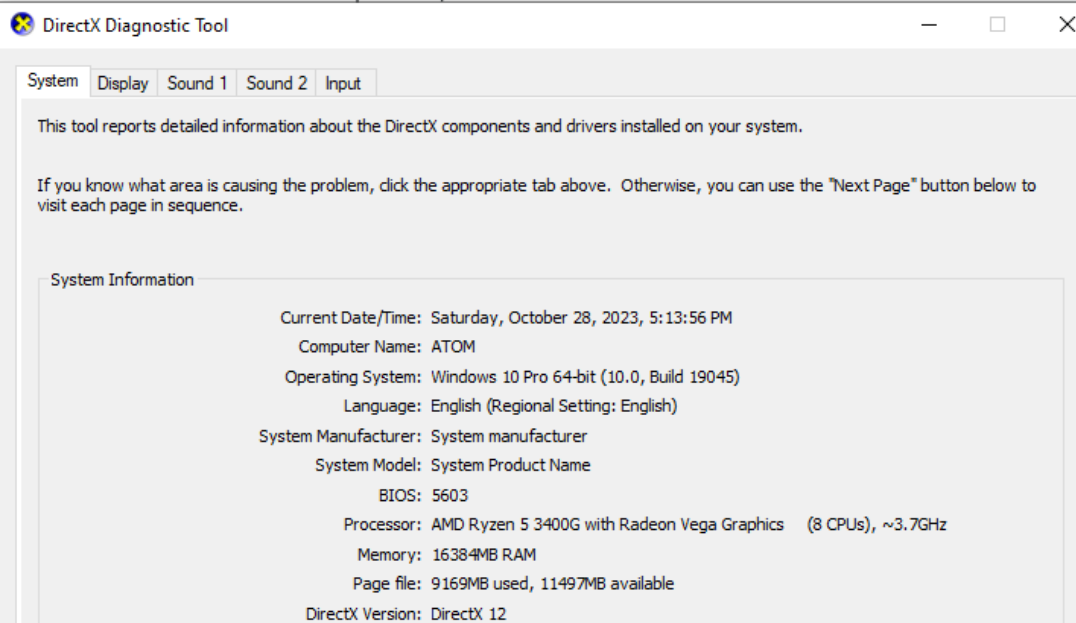
DxDiag 10.00.19041.3570 64-bit Unicode Copyright © Microsoft. All rights reserved.

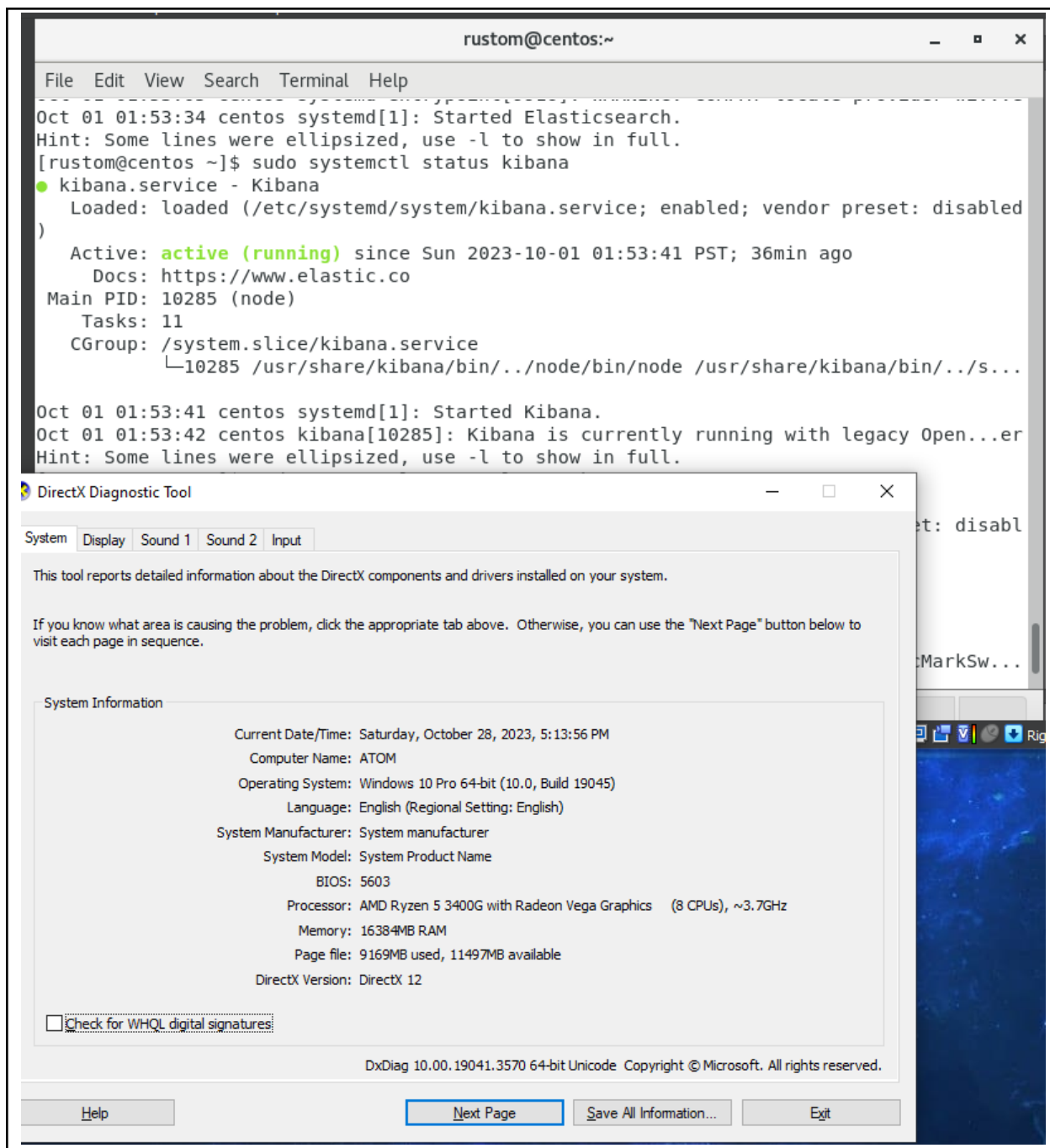
Help Next Page Save All Information... Exit

- 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.
```



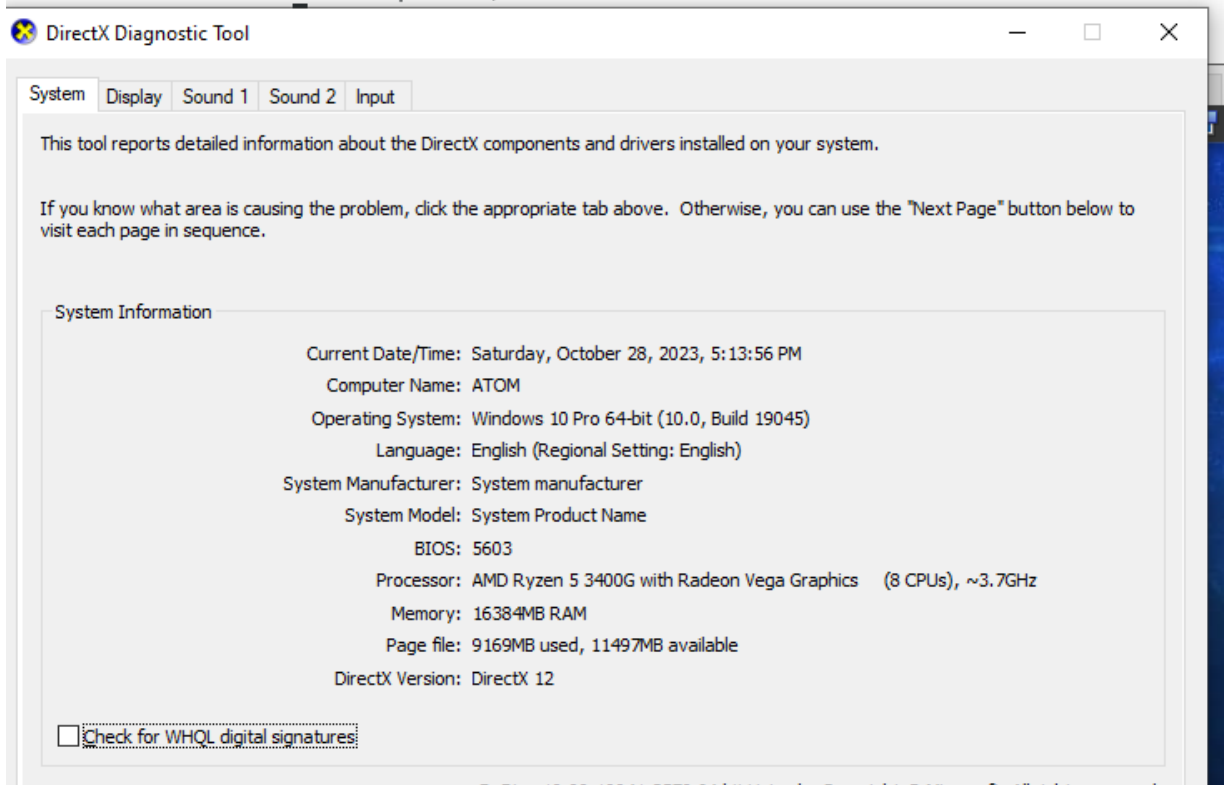


```

[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.