

Name: Andreu John L. Salvador	Date Performed: 28/10/2023
Course/Section: CPE31S5	Date Submitted: 28/10/2023
Instructor: Engr. Roman Richard	Semester and SY: 1st 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>	

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.

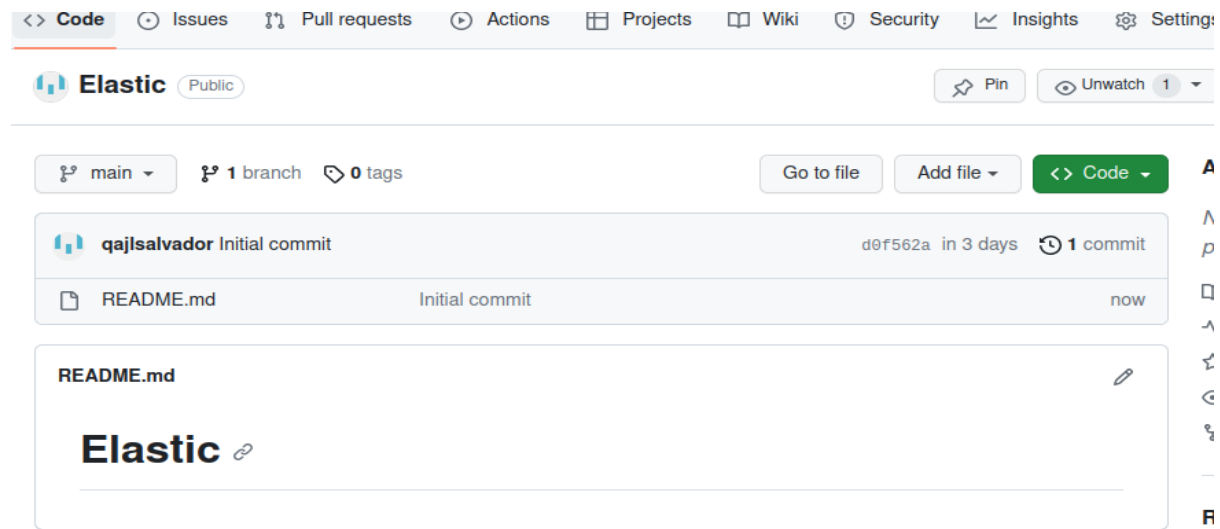
Source: <https://www.graylog.org/products/open-source>

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)

Part 1: Creating the repository

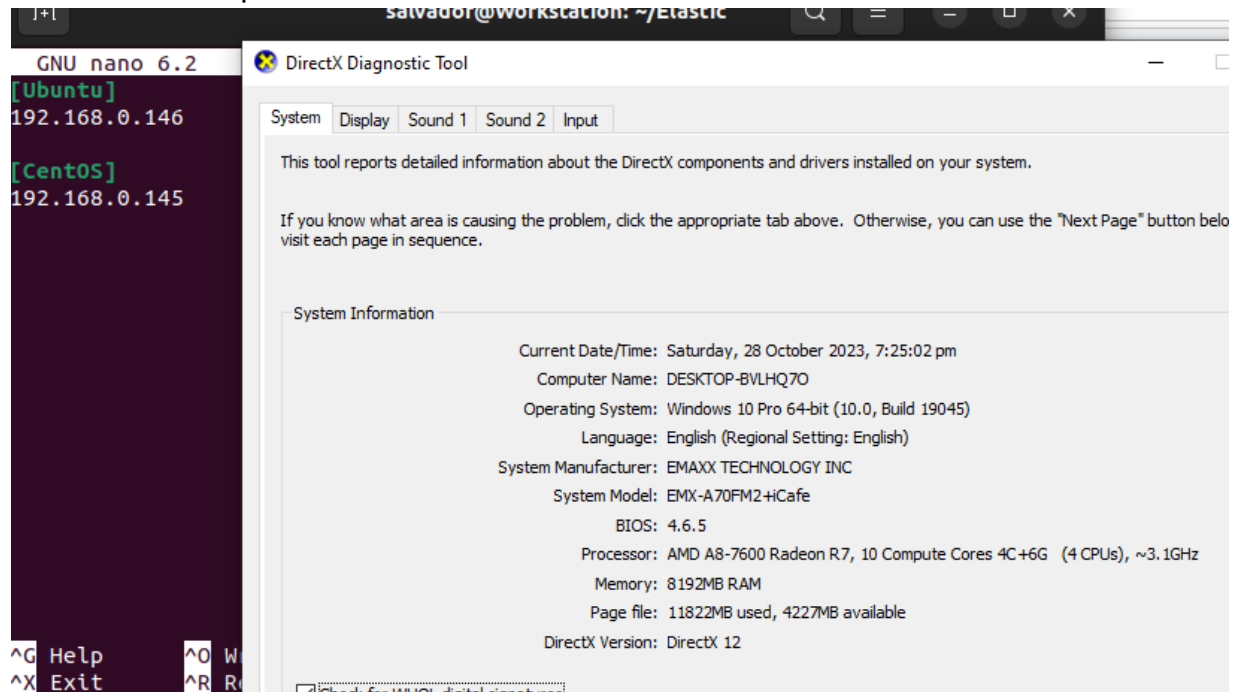


Create the repository where we will put our playbook later.

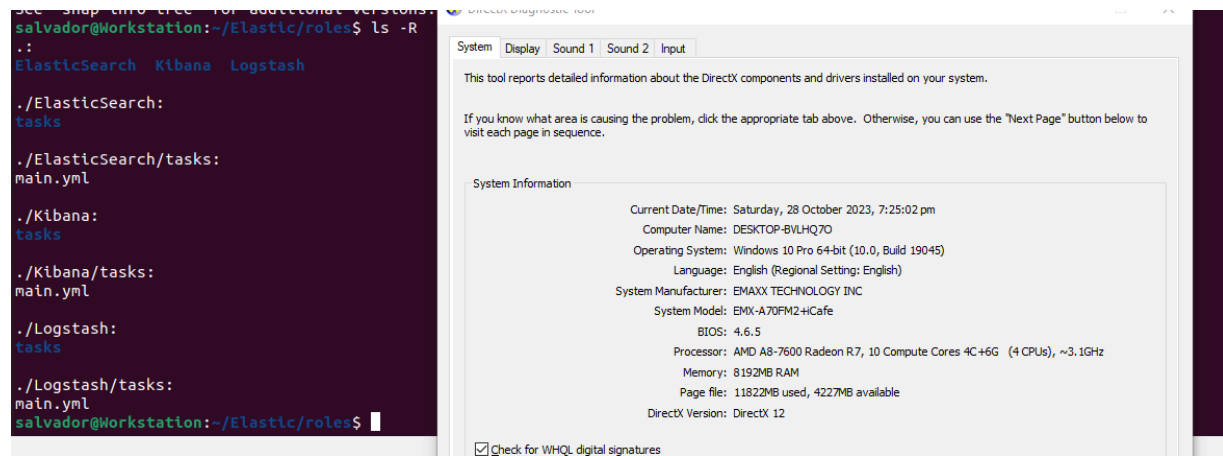
```
salvador@Workstation:~$ git clone git@github.com:qajlsalvador/Elastic.git
Cloning into 'Elastic'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
salvador@Workstation:~$ ls
ansible          Elastic          nagios-ansible   snap
CPE232_AndreuSalvador id_rsa          Pictures          Templates
Desktop          id_rsa.pub      Prometheus        Videos
Documents         Music           Public
Downloads         Nagios          Salvador_PrelimExam
salvador@Workstation:~$ cd Elastic
salvador@Workstation:~/Elastic$
```

Part 2: Installing Elastic Stack on Ubuntu server

1. Create our inventory where we will put the ip address of our live servers and group them in their respective roles.

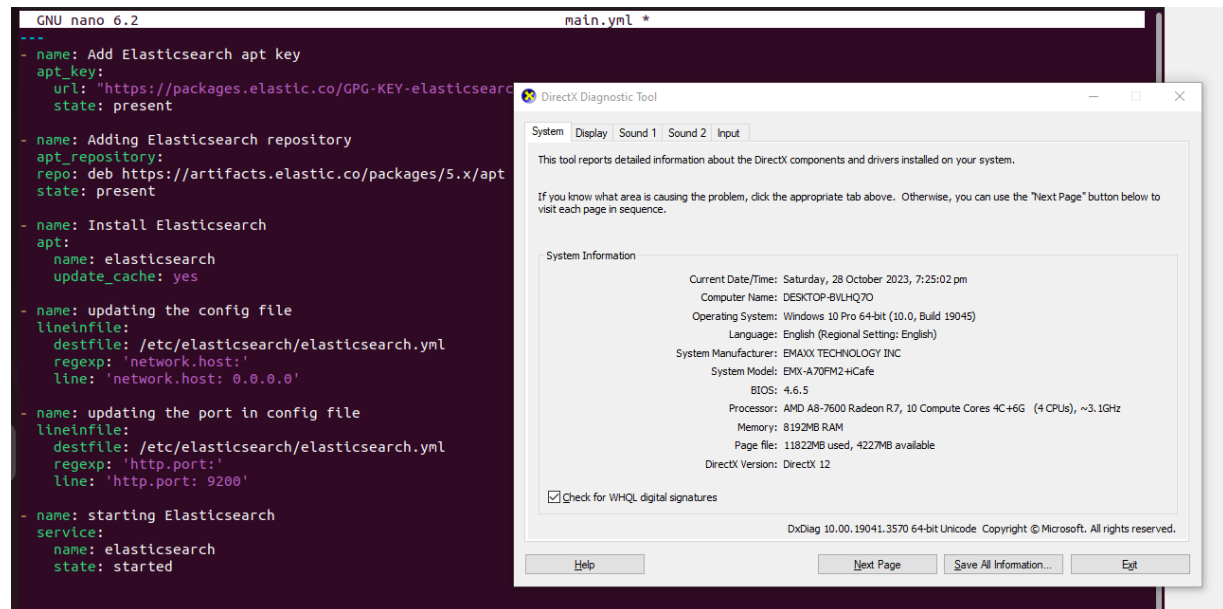


2. create roles directory and within the roles directory create the necessary roles for our Ubuntu server.

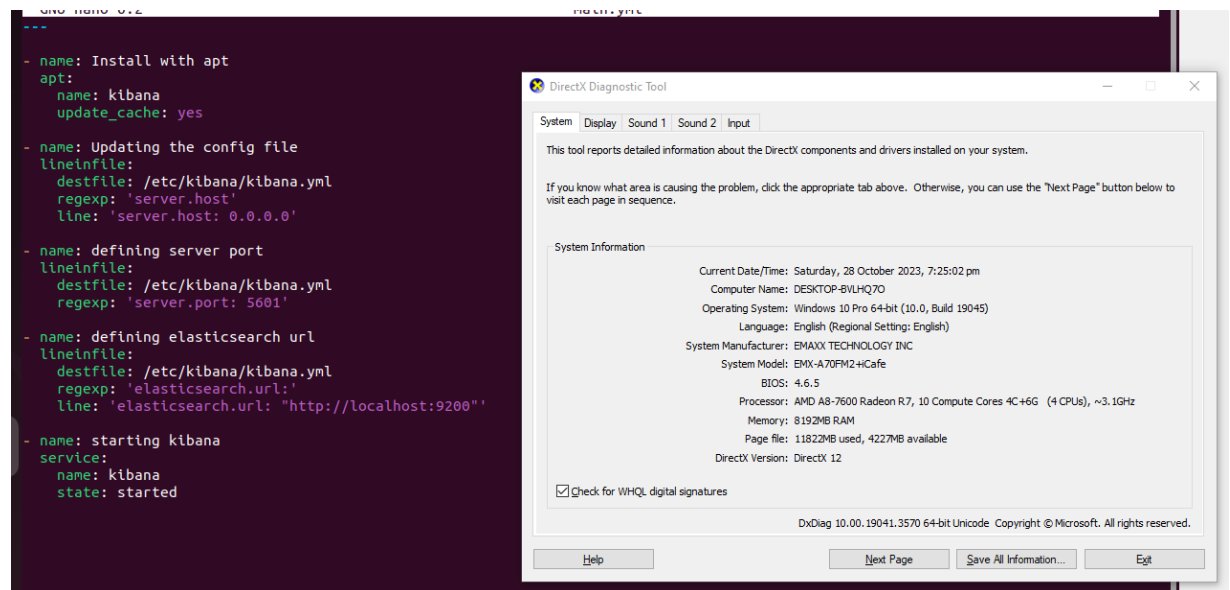


3. inside the roles, create a directory named tasks and inside the directory tasks create the .yml file as main.yml, lastly put the necessary tasks inside the .yml file.

ElasticSearch:



Kibana:



The terminal window shows the following commands and output:

```
--  
- name: Install with apt  
  apt:  
    name: kibana  
    update_cache: yes  
  
- name: Updating the config file  
  lineinfile:  
    destfile: /etc/kibana/kibana.yml  
    regexp: 'server.host'  
    line: 'server.host: 0.0.0.0'  
  
- name: defining server port  
  lineinfile:  
    destfile: /etc/kibana/kibana.yml  
    regexp: 'server.port: 5601'  
  
- name: defining elasticsearch url  
  lineinfile:  
    destfile: /etc/kibana/kibana.yml  
    regexp: 'elasticsearch.url:'  
    line: 'elasticsearch.url: "http://localhost:9200"'  
  
- name: starting kibana  
  service:  
    name: kibana  
    state: started
```

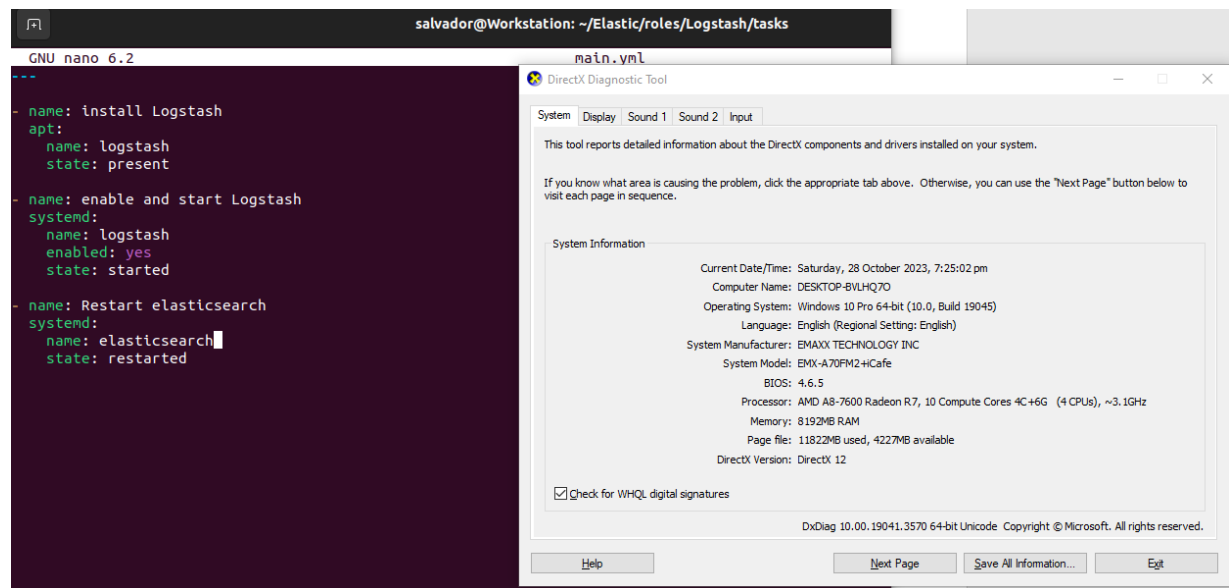
The DirectX Diagnostic Tool window displays the following system information:

System Information	
Current Date/Time:	Saturday, 28 October 2023, 7:25:02 pm
Computer Name:	DESKTOP-BVLHQ70
Operating System:	Windows 10 Pro 64-bit (10.0, Build 19045)
Language:	English (Regional Setting: English)
System Manufacturer:	EMAXX TECHNOLOGY INC
System Model:	EMX-A70FM2-HCafe
BIOS:	4.6.5
Processor:	AMD A8-7600 Radeon R7, 10 Compute Cores 4C+6G (4 CPUs), ~3.1GHz
Memory:	8192MB RAM
Page file:	11822MB used, 4227MB available
DirectX Version:	DirectX 12

Check for WHQL digital signatures: ☒

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

Logstash:



The terminal window shows the following commands and output:

```
--  
- name: install Logstash  
  apt:  
    name: logstash  
    state: present  
  
- name: enable and start Logstash  
  systemd:  
    name: logstash  
    enabled: yes  
    state: started  
  
- name: Restart elasticsearch  
  systemd:  
    name: elasticsearch  
    state: restarted
```

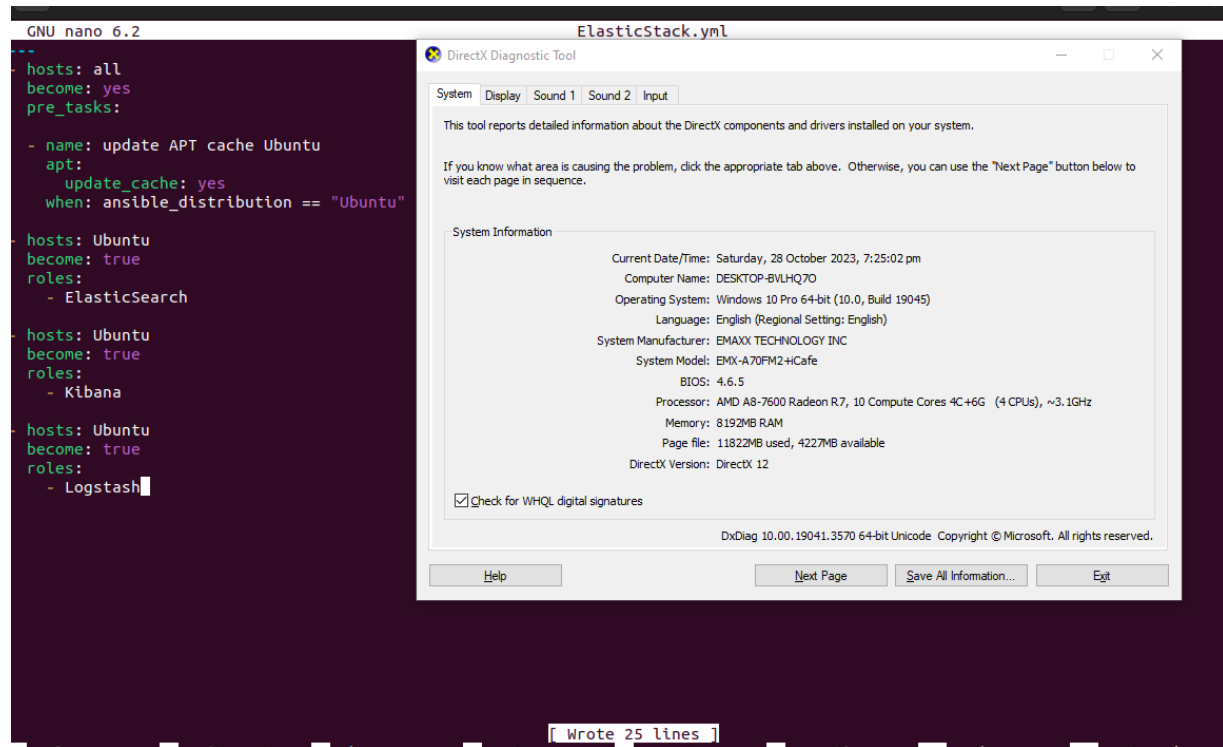
The DirectX Diagnostic Tool window displays the same system information as the Kibana section:

System Information	
Current Date/Time:	Saturday, 28 October 2023, 7:25:02 pm
Computer Name:	DESKTOP-BVLHQ70
Operating System:	Windows 10 Pro 64-bit (10.0, Build 19045)
Language:	English (Regional Setting: English)
System Manufacturer:	EMAXX TECHNOLOGY INC
System Model:	EMX-A70FM2-HCafe
BIOS:	4.6.5
Processor:	AMD A8-7600 Radeon R7, 10 Compute Cores 4C+6G (4 CPUs), ~3.1GHz
Memory:	8192MB RAM
Page file:	11822MB used, 4227MB available
DirectX Version:	DirectX 12

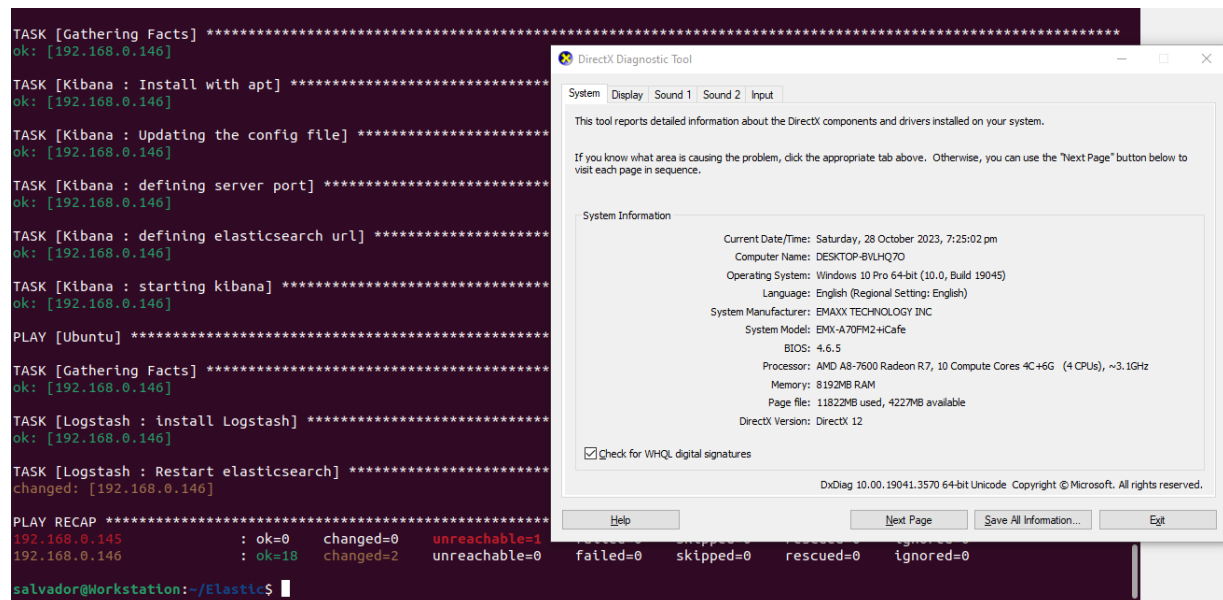
Check for WHQL digital signatures: ☒

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

4. Create the main yml file to play the tasks.



5. Run the playbook



Part 3: Installing Elastic Search on CentOS

1. Create the necessary roles in installing the ElasticStack on CentOS

```
salvador@Workstation:~/Elastic/roles$ ls
ElasticSearch Kibana Logstash
salvador@Workstation:~/Elastic/roles$ mkdir EL5_CentOS
salvador@Workstation:~/Elastic/roles$ cd EL5_CentOS
salvador@Workstation:~/Elastic/roles/EL5_CentOS$ mkdir Tasks
salvador@Workstation:~/Elastic/roles/EL5_CentOS$ ls
Tasks
salvador@Workstation:~/Elastic/roles/EL5_CentOS$ rm -r Tasks
salvador@Workstation:~/Elastic/roles/EL5_CentOS$ ls
salvador@Workstation:~/Elastic/roles/EL5_CentOS$ mkdir tasks
salvador@Workstation:~/Elastic/roles/EL5_CentOS$ cd tasks
salvador@Workstation:~/Elastic/roles/EL5_CentOS/tasks$ sudo nano main.yml
[sudo] password for salvador:
salvador@Workstation:~/Elastic/roles/EL5_CentOS/tasks$ cd /home/salvador
salvador@Workstation:~/Elastic/roles$ mkdir Kibana_CentOS
salvador@Workstation:~/Elastic/roles$ cd Kibana_CentOS
salvador@Workstation:~/Elastic/roles/Kibana_CentOS$ mkdir tasks
salvador@Workstation:~/Elastic/roles/Kibana_CentOS$ cd tasks
salvador@Workstation:~/Elastic/roles/Kibana_CentOS/tasks$ sudo nano main.yml
salvador@Workstation:~/Elastic/roles/Kibana_CentOS/tasks$ cd /home/salvador
salvador@Workstation:~/Elastic/roles$ mkdir Logstash_CentOS
salvador@Workstation:~/Elastic/roles$ cd Logstash_CentOS
```

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, 7:25:02 pm

Computer Name: DESKTOP-BVLHQ70

Operating System: Windows 10 Pro 64-bit (10.0, Build 19045)

Language: English (Regional Setting: English)

System Manufacturer: EMAXX TECHNOLOGY INC

System Model: EMX-A70FM2-HiCafe

BIOS: 4.6.5

Processor: AMD A8-7600 Radeon R7, 10 Compute Cores 4C+6G (4 CPUs), ~3.1GHz

Memory: 8192MB RAM

Page file: 11822MB used, 4227MB 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

2. Just like on the part 2 inside the roles, create a directory named tasks and inside the directory tasks create the .yml file as main.yml, lastly put the necessary tasks inside the .yml file.

ElasticSearch:

GNU nano 6.2

```
--
name: install needed files
package:
  name:
    - epel-release
    - make
    - openssl
    - autoconf
    - wget
    - which
    - java-1.8.0-openjdk
  state: present

name: Install ElasticSearch
dnf:
  name: elasticsearch
  state: present

name: enable and start Elasticsearch
systemd:
  name: leasticsearch
  enabled: yes
  state: started
```

/home/salvador/Elastic/roles/EL5_CentOS/tasks/main.yml *

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, 28 October 2023, 7:25:02 pm

Computer Name: DESKTOP-BVLHQ70

Operating System: Windows 10 Pro 64-bit (10.0, Build 19045)

Language: English (Regional Setting: English)

System Manufacturer: EMAXX TECHNOLOGY INC

System Model: EMX-A70FM2-HiCafe

BIOS: 4.6.5

Processor: AMD A8-7600 Radeon R7, 10 Compute Cores 4C+6G (4 CPUs), ~3.1GHz

Memory: 8192MB RAM

Page file: 11822MB used, 4227MB available

DirectX Version: DirectX 12

☒ Check for WHQL digital signatures

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

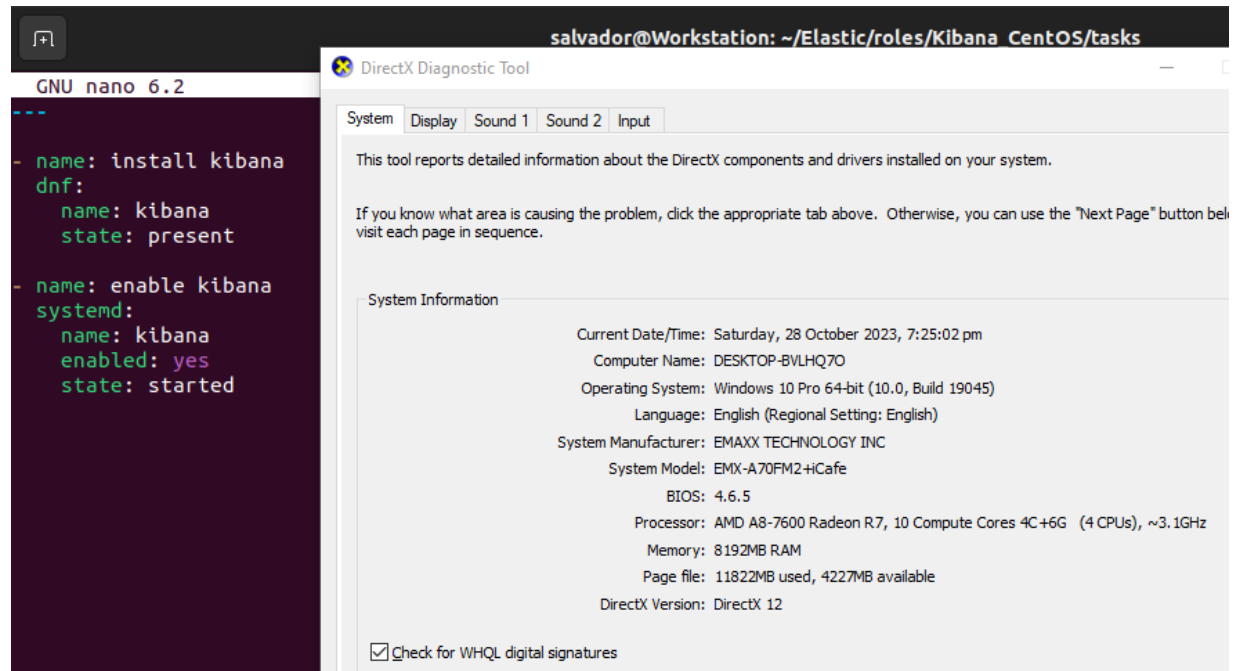
Help

Next Page

Save All Information...

Exit

Kibana:



The screenshot shows a terminal window with the GNU nano 6.2 editor and a DirectX Diagnostic Tool window. The terminal displays the installation and enabling of Kibana. The DirectX Diagnostic Tool shows system information for a Windows 10 Pro 64-bit system.

```
salvador@Workstation: ~/Elastic/roles/Kibana CentOS/tasks
```

GNU nano 6.2

```
--
- name: install kibana
  dnf:
    name: kibana
    state: present

- name: enable kibana
  systemd:
    name: kibana
    enabled: yes
    state: started
```

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.

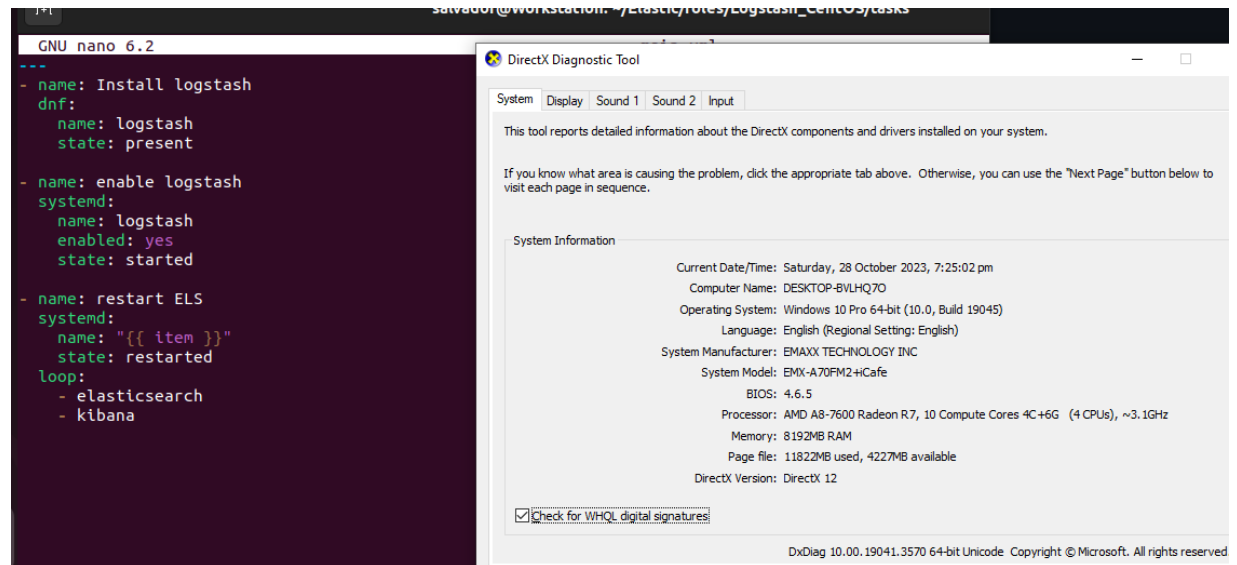
If you know what area is causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button below to visit each page in sequence.

System Information

Current Date/Time: Saturday, 28 October 2023, 7:25:02 pm
Computer Name: DESKTOP-BVLHQ70
Operating System: Windows 10 Pro 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: EMAXX TECHNOLOGY INC
System Model: EMX-A70FM2-HiCafe
BIOS: 4.6.5
Processor: AMD A8-7600 Radeon R7, 10 Compute Cores 4C+6G (4 CPUs), ~3.1GHz
Memory: 8192MB RAM
Page file: 11822MB used, 4227MB available
DirectX Version: DirectX 12

☒ Check for WHQL digital signatures

Logstash:



The screenshot shows a terminal window with the GNU nano 6.2 editor and a DirectX Diagnostic Tool window. The terminal displays the installation and enabling of Logstash, followed by a restart of the Elasticsearch service. The DirectX Diagnostic Tool shows system information for a Windows 10 Pro 64-bit system.

```
salvador@Workstation: ~/Elastic/roles/Logstash CentOS/tasks
```

GNU nano 6.2

```
--
- name: Install logstash
  dnf:
    name: logstash
    state: present

- name: enable logstash
  systemd:
    name: logstash
    enabled: yes
    state: started

- name: restart ELS
  systemd:
    name: "[{ item }]"
    state: restarted
  loop:
    - elasticsearch
    - 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.

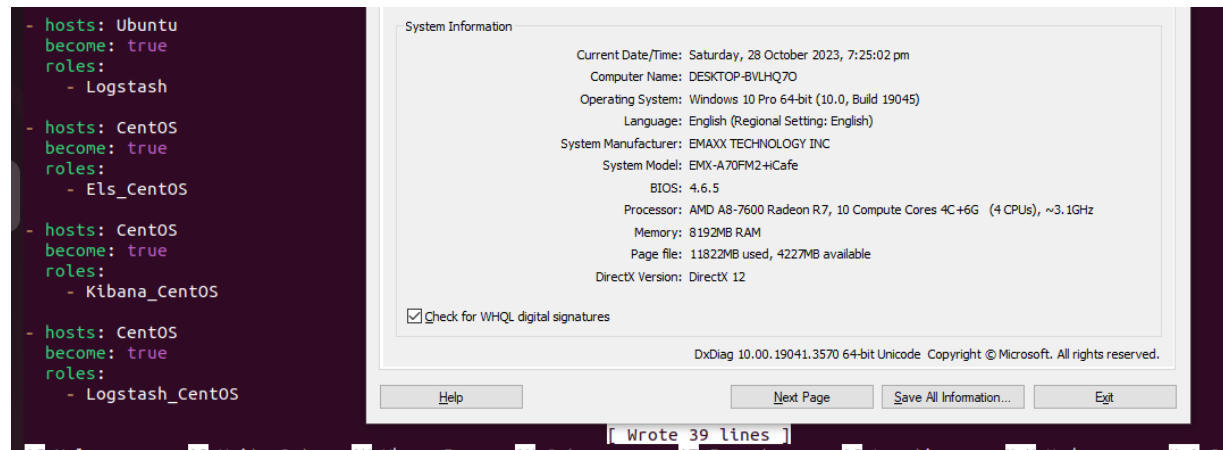
System Information

Current Date/Time: Saturday, 28 October 2023, 7:25:02 pm
Computer Name: DESKTOP-BVLHQ70
Operating System: Windows 10 Pro 64-bit (10.0, Build 19045)
Language: English (Regional Setting: English)
System Manufacturer: EMAXX TECHNOLOGY INC
System Model: EMX-A70FM2-HiCafe
BIOS: 4.6.5
Processor: AMD A8-7600 Radeon R7, 10 Compute Cores 4C+6G (4 CPUs), ~3.1GHz
Memory: 8192MB RAM
Page file: 11822MB used, 4227MB available
DirectX Version: DirectX 12

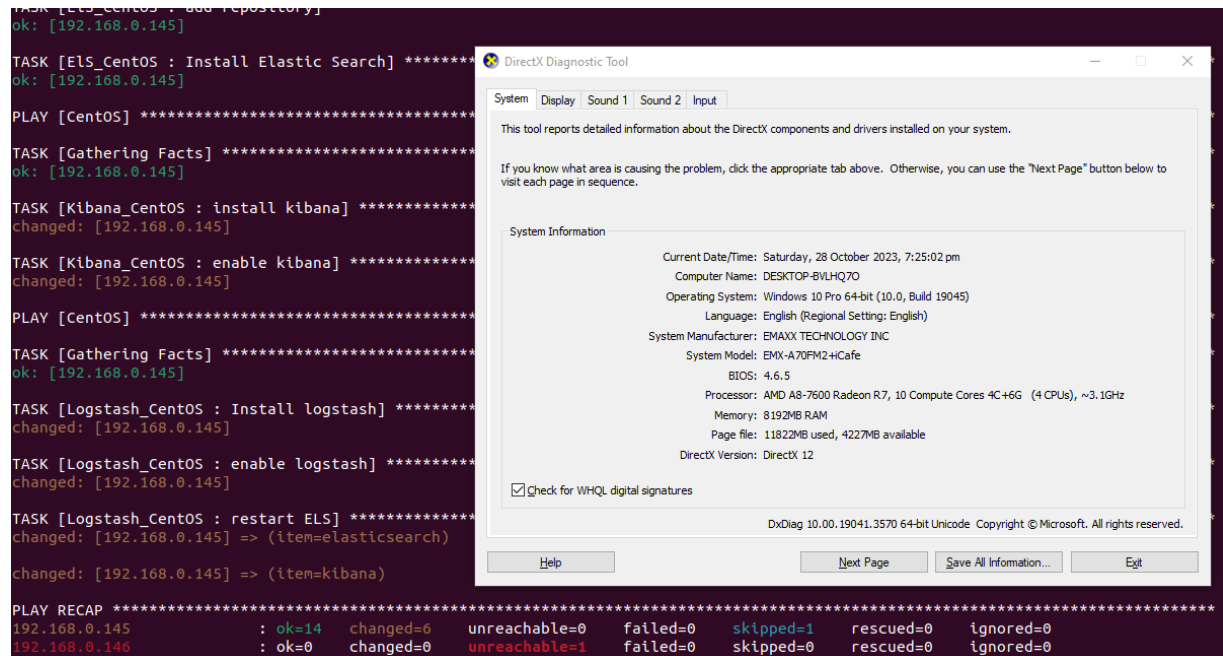
☒ Check for WHQL digital signatures

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

3. Add the roles inside the main ElasticStack .yaml file in order to play it in the playbook.



4. Run the Playbook

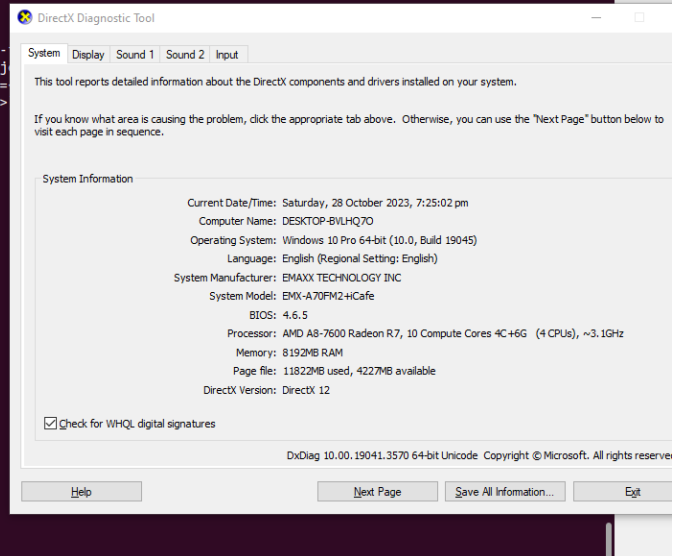


Part 5: adding everything to github

```
salvador@Workstation:~/Elastic$ git add *
salvador@Workstation:~/Elastic$ git -m "new"
unknown option: -m
usage: git [--version] [--help] [-C <path>] [-c <name>=<value>]
[--exec-path[=<path>]] [--html-path] [--man-path] [--]
[-p | --paginate | -P | --no-pager] [--no-replace-obj]
[--git-dir=<path>] [--work-tree=<path>] [--namespace=
<super-prefix>=<path>] [--config-env=<name>=<envvar>]
<command> [<args>]

salvador@Workstation:~/Elastic$ git commit -m "NEW"
[main c3f7da9] NEW
 8 files changed, 186 insertions(+)
 create mode 100644 ElasticStack.yml
 create mode 100644 inventory
 create mode 100644 roles/ELI_CentOS/tasks/main.yml
 create mode 100644 roles/ElasticSearch/tasks/main.yml
 create mode 100644 roles/Kibana/tasks/main.yml
 create mode 100644 roles/Kibana_CentOS/tasks/main.yml
 create mode 100644 roles/Logstash/tasks/main.yml
 create mode 100644 roles/Logstash_CentOS/tasks/main.yml
salvador@Workstation:~/Elastic$ git push origin main
Enumerating objects: 24, done.
Counting objects: 100% (24/24), done.
Compressing objects: 100% (10/10), done.
Writing objects: 100% (23/23), 2.50 KiB | 641.00 KiB/s, done.
Total 23 (delta 0), reused 0 (delta 0), pack-reused 0
To github.com:gajlsalvador/Elastic.git
 d0f562a..c3f7da9  main -> main
salvador@Workstation:~/Elastic$ git status
On branch main
Your branch is up to date with 'origin/main'.

nothing to commit, working tree clean
salvador@Workstation:~/Elastic$
```



Reflections:

Answer the following:

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

Its importance is akin to what security cameras are for. Logs monitoring tools are important to use and to have since it helps the you monitor security issues that occurred in the system as well as helps you solve performance related problems.

Conclusions:

In installing the log monitoring tool there are thing that you should keep in mind; first is what monitoring tool you need, second what does it do, and etc. In the activity it let us install the log monitoring tool called Elastic stack, this tool is made up of software such as the Elastic Searc, Kibana, beats, and Logstash. These are necessary in building the monitoring tool. I've used the function of roles in creating an ansible playbook to further assimilate and made it easy to debug problems since the used of the roles is to lessen the burden for you when finding the error when playing the playbook. Creating roles for both the Ubuntu and CentOS server was a challenge since the code for the two are not that easy to write. In the end the installation was a success and the goal was achieved which is installing the Monitoring tool in both servers using the Playbook.