

Name: Shaniah Rose Hope M. Sumaoang	Date Performed: October 26, 2023
Course/Section: CPE 232-CPE31S5	Date Submitted: October 26, 2023
Instructor: Engr. Roman Richard	Semester and SY: 1st Sem 23-24
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.

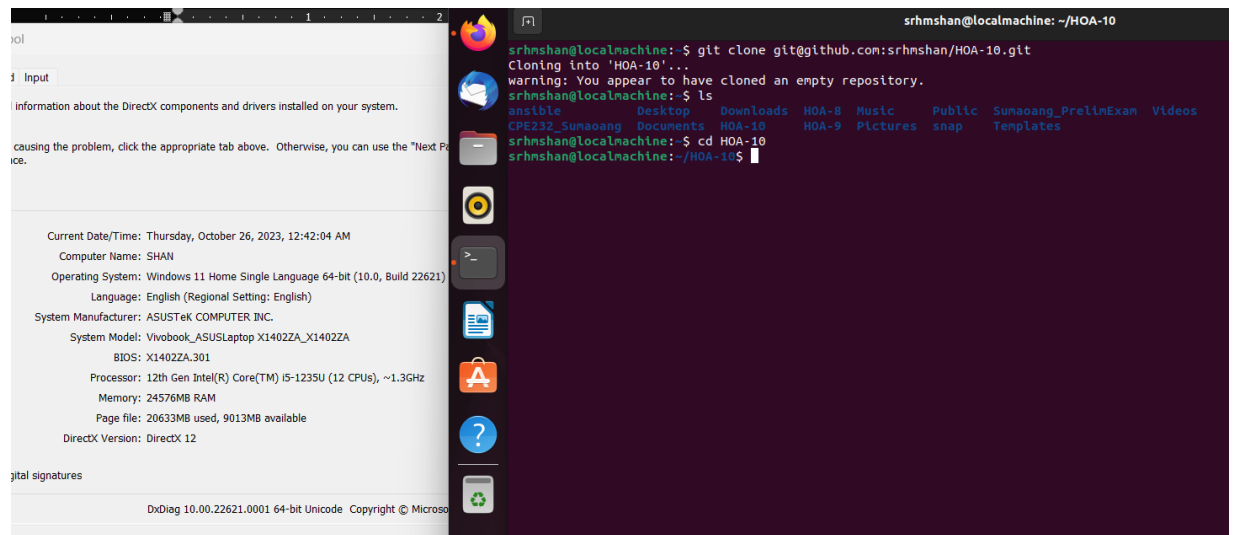
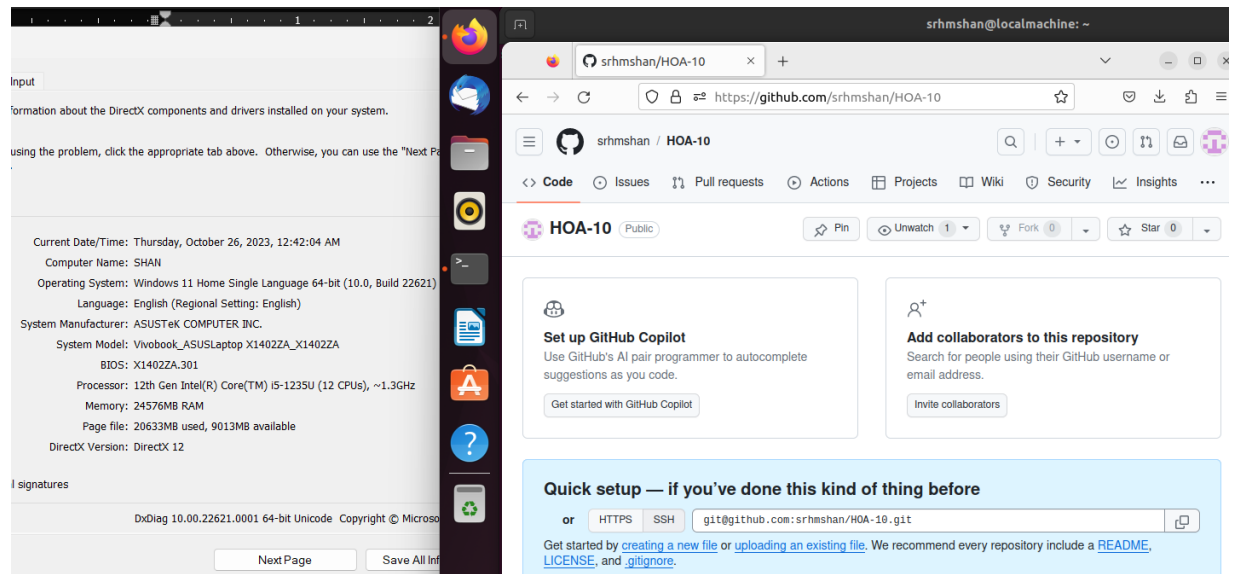
Source: <https://www.graylog.org/products/open-source>

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)

Step 1: Create a new repository in GitHub for this activity. Adding anything to it is optional. Next, copy your new repository in your CN using the code in the 2nd image.



Step 2: Create your ansible.cfg and inventory files using the sudo nano command.

Information about the DirectX components and drivers installed on your system.

causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button.

Current Date/Time: Thursday, October 26, 2023, 12:52:49 AM

Computer Name: SHAN

Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22H2)

Language: English (Regional Setting: English)

System Manufacturer: ASUSTeK COMPUTER INC.

System Model: Vivobook_ASUSLaptop X1402ZA_X1402ZA

BIOS: X1402ZA.301

Processor: 12th Gen Intel(R) Core(TM) i5-1235U (12 CPUs), ~1.3GHz

Memory: 24576MB RAM

Page file: 18848MB used, 10799MB available

DirectX Version: DirectX 12

digital signatures

GNU nano 6.2

[defaults]
inventory = inventory
private_key_file = ~/.ssh/id_rsa

ansible.cfg

Clipboard

Copy

Format Painter

Font

Information about the DirectX components and drivers installed on your system.

causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button.

Current Date/Time: Thursday, October 26, 2023, 12:52:49 AM

Computer Name: SHAN

Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22H2)

Language: English (Regional Setting: English)

System Manufacturer: ASUSTeK COMPUTER INC.

System Model: Vivobook_ASUSLaptop X1402ZA_X1402ZA

BIOS: X1402ZA.301

Processor: 12th Gen Intel(R) Core(TM) i5-1235U (12 CPUs), ~1.3GHz

Memory: 24576MB RAM

Page file: 18848MB used, 10799MB available

DirectX Version: DirectX 12

digital signatures

GNU nano 6.2

[ubuntu]
192.168.5.59 ansible_python_interpreter=/usr/bin/python3

[centos]
192.168.5.215

Server2_Sumaoang [running] - Oracle VM VirtualBox

File Machine View Input Devices Help

srhmschandserver2:~\$ ifconfig

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.5.59 netmask 255.255.255.0 broadcast 192.168.5.255

inet6 fe80::a001:27ff:fe5e:8ac5 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:5e:8a:c5 txqueuelen 1000 (Ethernet)

RX packets 0 dropped 0 overruns 0 frame 0

TX packets 17943 bytes 3947474 (3.9 MB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 14336 bytes 18359293 (18.3 MB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 14336 bytes 18359293 (18.3 MB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Sumaoang_CentOS [running] - Oracle VM VirtualBox

File Machine View Input Devices Help

srhmschan@CentOS:~\$ ifconfig

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.5.215 netmask 255.255.255.0 broadcast 192.168.5.255

inet6 fe80::7d4c:b43:d83c:39c3 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:0f:50:e8 txqueuelen 1000 (Ethernet)

RX packets 1324394 bytes 1697452954 (1.5 GiB)

RX errors 0 dropped 1 overruns 0 frame 0

TX packets 302276 bytes 27306449 (26.0 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 17786 bytes 7202968 (6.8 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 17786 bytes 7202968 (6.8 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500

inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.2

ether 52:54:00:16:38:36 txqueuelen 1000 (Ethernet)

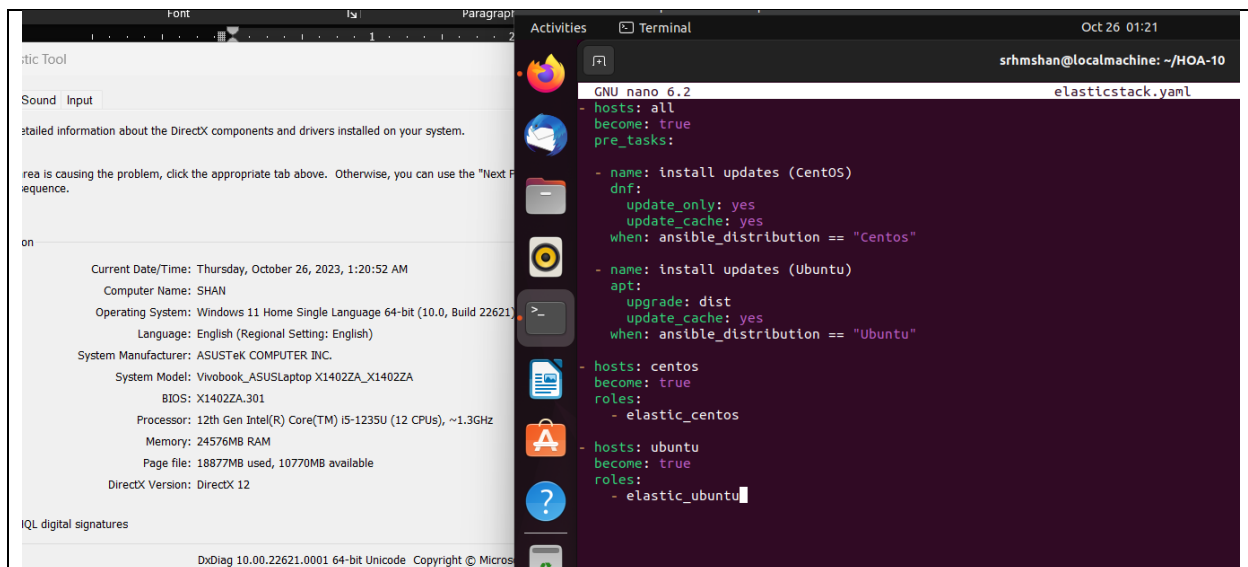
RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

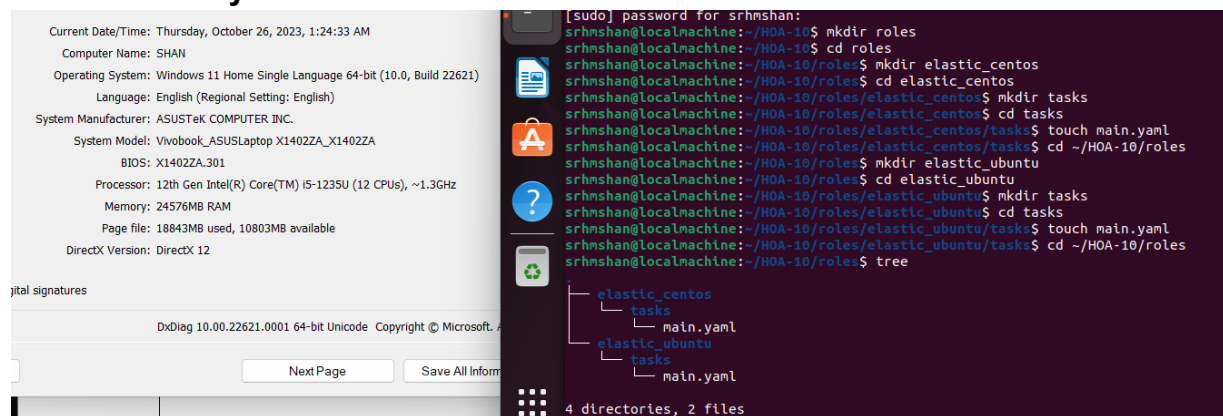
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Step 3: Create an elasticstack.yaml file with the following tasks:



This is the main playbook wherein the roles are defined.

Step 4: Create a “roles” directory under your current directory. Under the “roles” directory, make 2 more directories according to the roles you defined in the elasticstack.yaml. Under each directory, create a “tasks” directory and make a “main.yaml” file.



I applied the concept of creating roles.

Step 5: Edit your main.yaml files and input all the needed tasks to install Elastic Stack.
[CentOS]

[Ubuntu]



This installs and configures the Elastic Stack on Ubuntu. Tasks include prerequisite installation, adding the Elastic APT repository, installing Elasticsearch, Kibana, and Logstash, enabling services, and restarting Elasticsearch and Kibana.

Step 6: Run the ansible playbook.

on about the DirectX components and drivers installed on your system.

ve problem, click the appropriate tab above. Otherwise, you can use the "Next Page

urrent Date/Time: Thursday, October 26, 2023, 2:01:42 AM
Computer Name: SHAN
perating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
m Manufacturer: ASUSTeK COMPUTER INC.
System Model: Vivobook_ASUSLaptop X1402ZA_X1402ZA
BIOS: X1402ZA.301
Processor: 12th Gen Intel(R) Core(TM) i5-1235U (12 CPUs), ~1.3GHz
Memory: 24576MB RAM
Page file: 20919MB used, 8728MB available
DirectX Version: DirectX 12

atures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft

Next Page Save All Info

Font

input

rmation about the DirectX components and drivers installed on your system.

sing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page

Current Date/Time: Thursday, October 26, 2023, 2:01:42 AM
Computer Name: SHAN
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: Vivobook_ASUSLaptop X1402ZA_X1402ZA
BIOS: X1402ZA.301
Processor: 12th Gen Intel(R) Core(TM) i5-1235U (12 CPUs), ~1.3GHz
Memory: 24576MB RAM
Page file: 20919MB used, 8728MB available
DirectX Version: DirectX 12

signatures

DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft

Next Page Save All Info

File Machine View Input Devices Help

Activities Terminal

Oct 26 02:02

srhmshan@localmachine: ~/HOA-10

skipping: [192.168.5.215]
changed: [192.168.5.59]

PLAY [centos] *****

TASK [Gathering Facts] *****
ok: [192.168.5.215]

TASK [elastic_centos : Install necessary prerequisites] *****
ok: [192.168.5.215]

TASK [elastic_centos : Add Elasticsearch RPM repository GPG key] *****
changed: [192.168.5.215]

TASK [elastic_centos : Add the Elasticsearch YUM repository] *****
changed: [192.168.5.215]

TASK [elastic_centos : Install Elasticsearch] *****
changed: [192.168.5.215]

TASK [elastic_centos : Enable and start Elasticsearch service] *****
changed: [192.168.5.215]

TASK [elastic_centos : Install Kibana] *****
changed: [192.168.5.215]

TASK [elastic_centos : Enable and start Kibana service] *****
changed: [192.168.5.215]

TASK [elastic_centos : Install Logstash] *****
changed: [192.168.5.215]

TASK [elastic_centos : Enable and start Logstash service] *****
changed: [192.168.5.215]

TASK [elastic_centos : Restart Elasticsearch and Kibana services] *****
changed: [192.168.5.215] => (item=elasticsearch)
changed: [192.168.5.215] => (item=kibana)

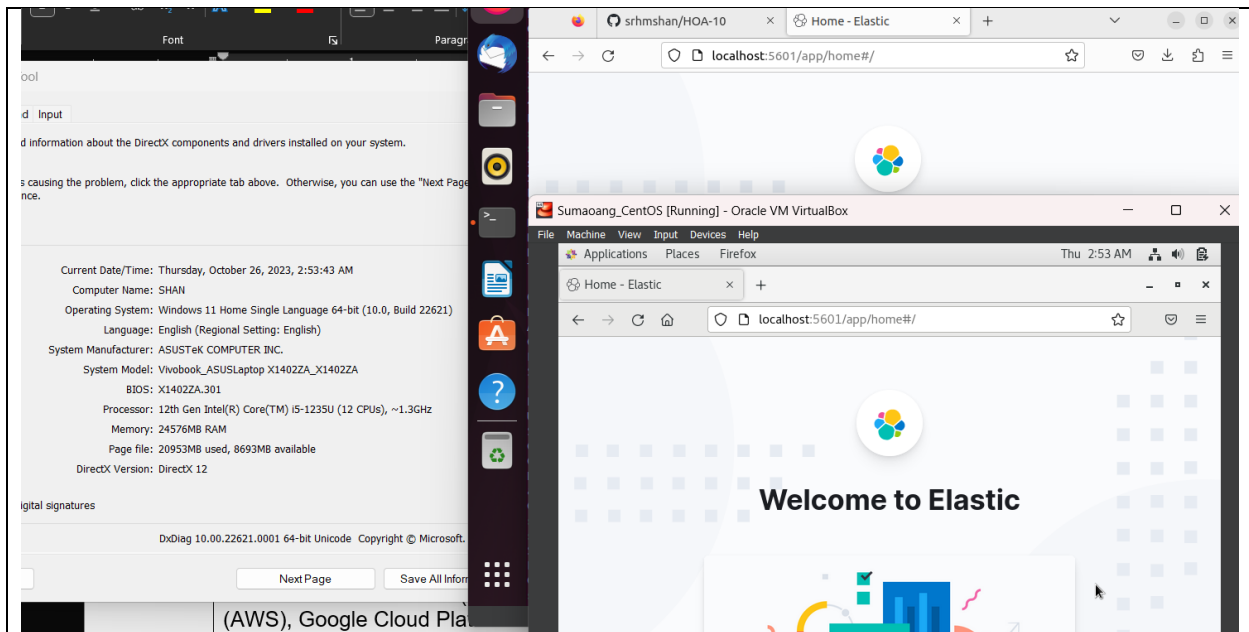
PLAY RECAP *****

192.168.5.215 ok=12 changed=9 unreachable=0 failed=0 skipped=2 rescued=0 ignored=0

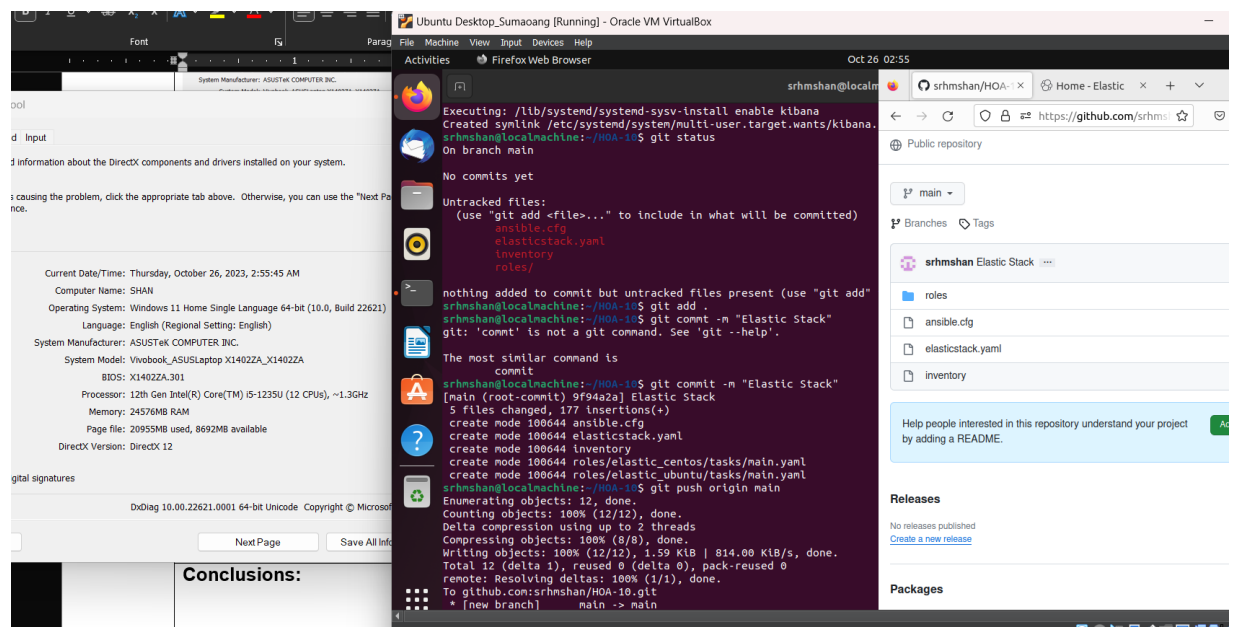
192.168.5.59 ok=13 changed=11 unreachable=0 failed=0 skipped=1 rescued=0 ignored=0

The tasks were successful.

Step 7: Verify if the installation was successful by putting
“http://[ip_address]:5601” in your browser.



Step 8: Commit and push to GitHub.



Reflections:

Answer the following:

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

Log monitoring tools offer a range of benefits. They help detect issues allowing for timely problem resolution. These tools also optimize performance by allocating resources. Enhance security through threat detection. Also, they ensure compliance, with regulatory log management requirements and simplify troubleshooting leading to faster issue resolution. Log monitoring tools store data for analysis and trend identification while automating responses to events. They provide real time alerts for action and facilitate data visualization for log analysis. In summary these tools are crucial in maintaining system health, security, performance and streamlining management tasks while ensuring compliance, with standards.

Conclusions:

In this activity, I developed a workflow using Ansible to configure and oversee log monitoring tools such, as the Elastic Stack and Logstash. Effective log file analysis heavily relies on log monitoring. I automated the installation process, on Ubuntu and CentOS by executing playbooks while also documenting the deployment in a manner using roles. This activity highlighted the significance of log monitoring and Ansible in installations and management.