Name: Pastrana, Mark Laurenz	Date Performed: Oct 24, 2023
Course/Section: CPE 232 - CPE31S5	Date Submitted: Oct 24, 2023
Instructor: Engr. Richard Roman	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

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.

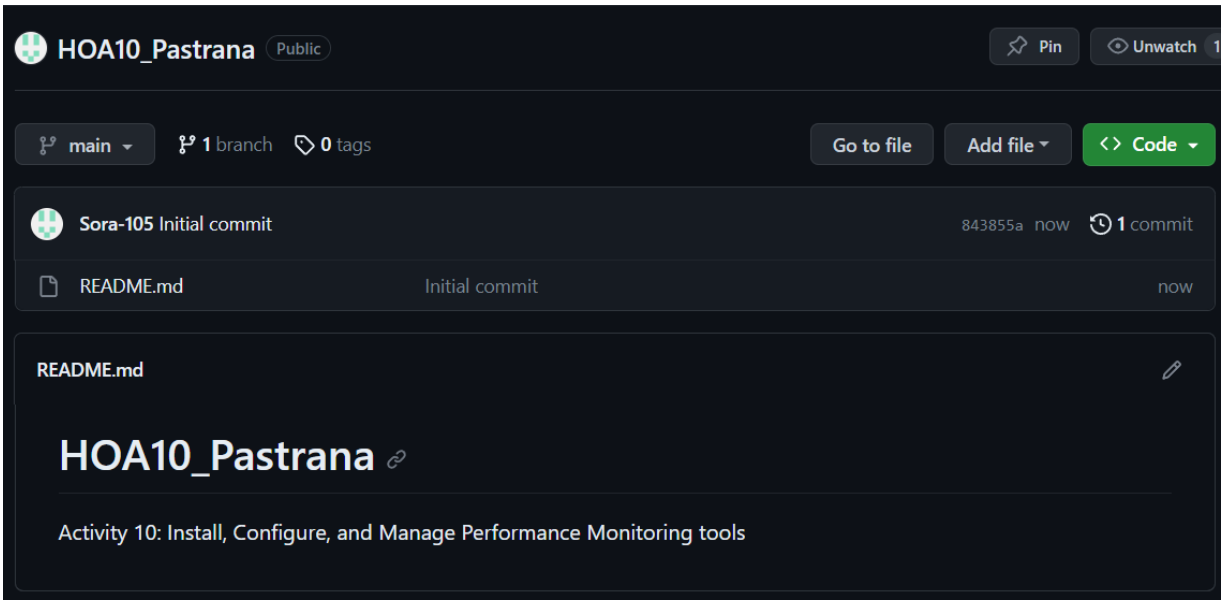
Source: https://www.graylog.org/products/open-source

3. Tasks

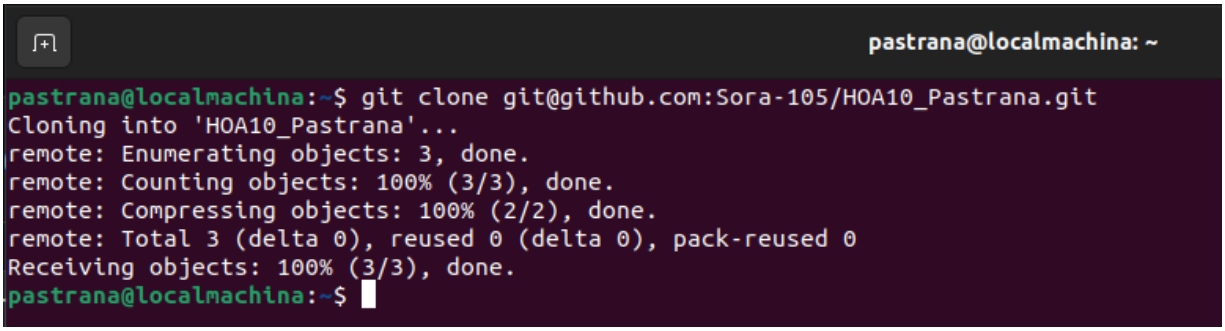
1. Create a playbook that:
    a. Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)
2. Apply the concept of creating roles.
3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like 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)

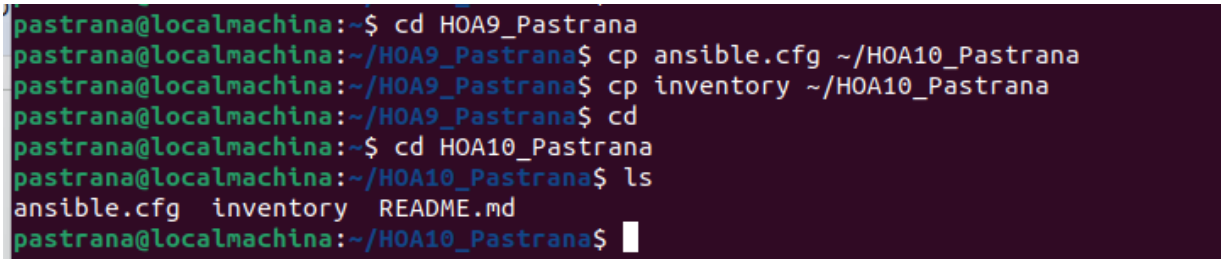
- First we need to create a new repository just like in the previous activity.



- And then we have to clone it into our virtual machine.

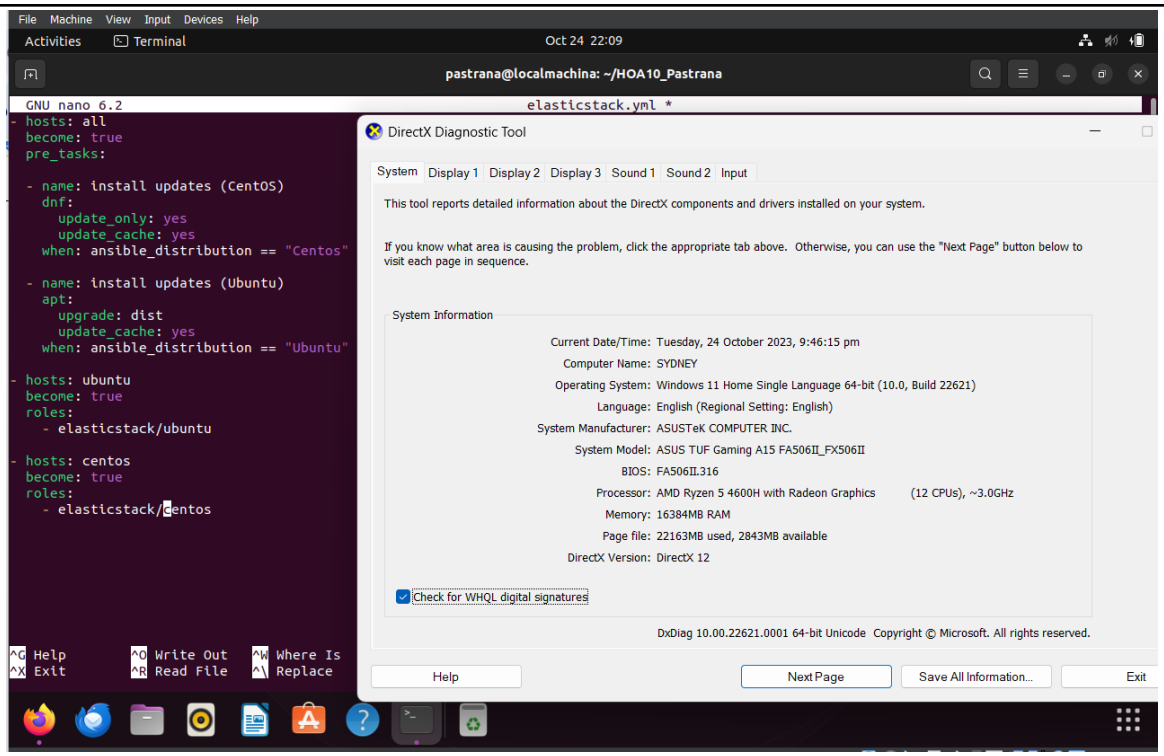


- We need to copy the ansible.cfg and inventory file into the new repository so that it will be easier for us not to type everything. In order to do this we have to type “cp <file> ~/<destination>”.



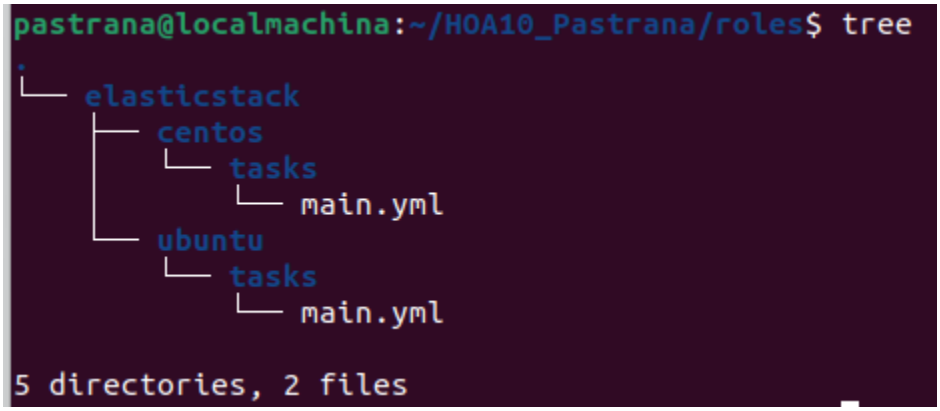
1. Create a playbook that:
   Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)

- I created the elasticstack.yml file. This will include the playbook commands for initializing and updating the servers, as well as calling on the main.yml playbooks in their respective roles.



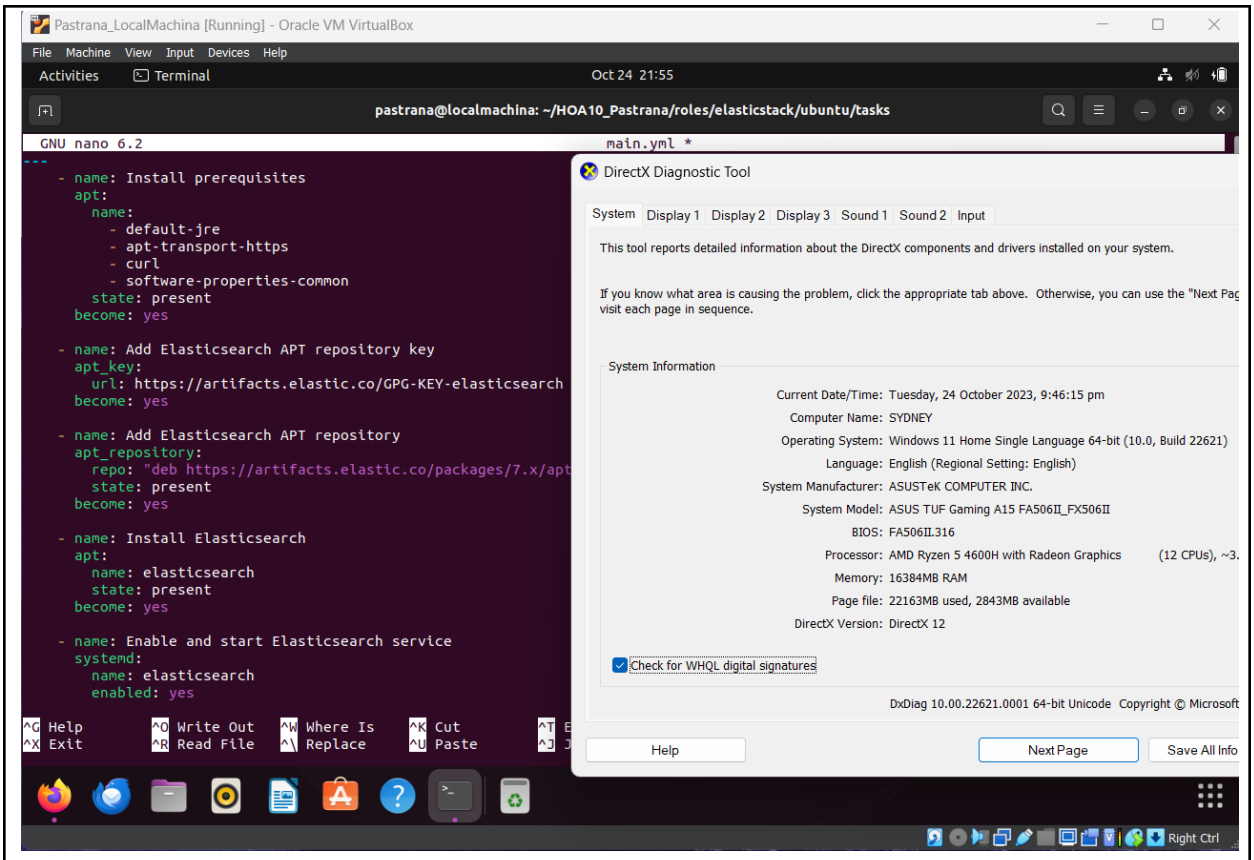
2. Apply the concept of creating roles.

- I created a role directory that contains centos and ubuntu each with their own tasks and main.yml



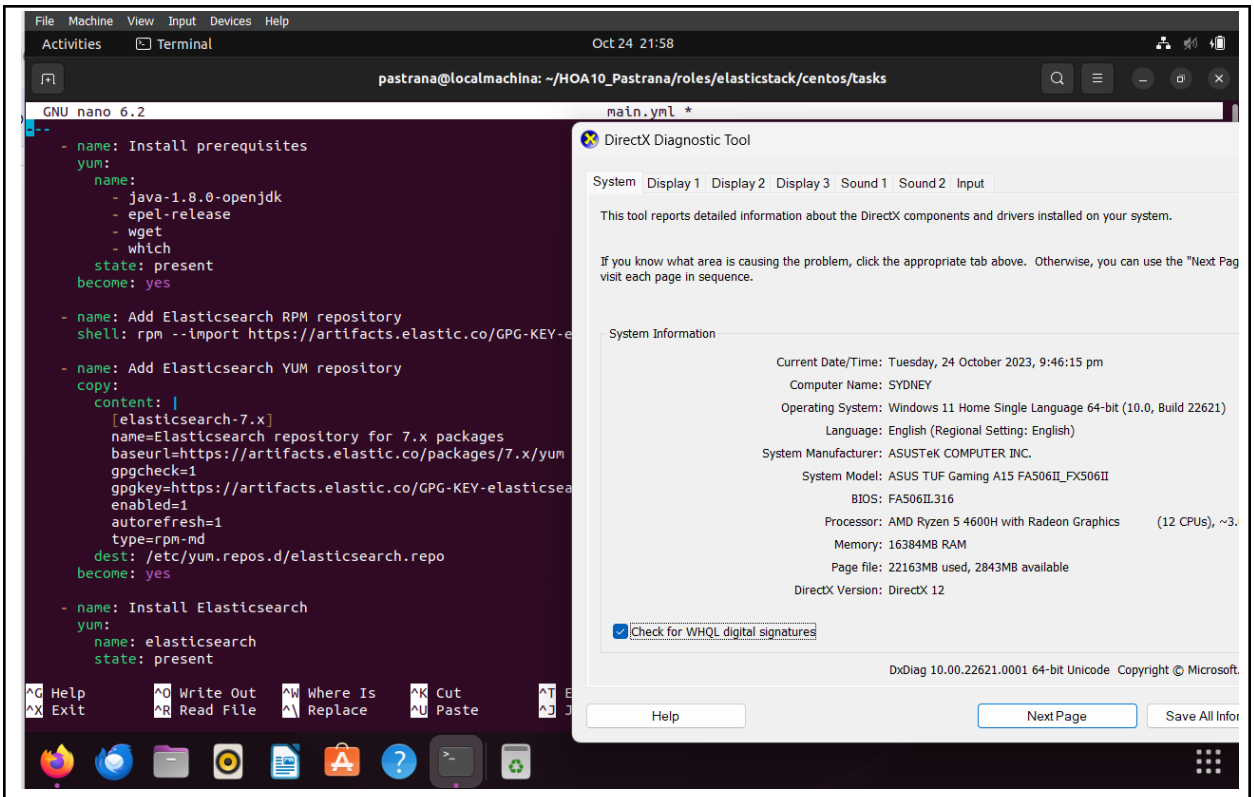
Ubuntu:

- The playbook contains all of the actions required to install all of the prerequisites for the Elastic Stack to work on Ubuntu. Following this, it will add the Elasticsearch APT repository key and apt repository before eventually installing Elasticsearch and Kibana. These processes are enabled and launched after they are installed.

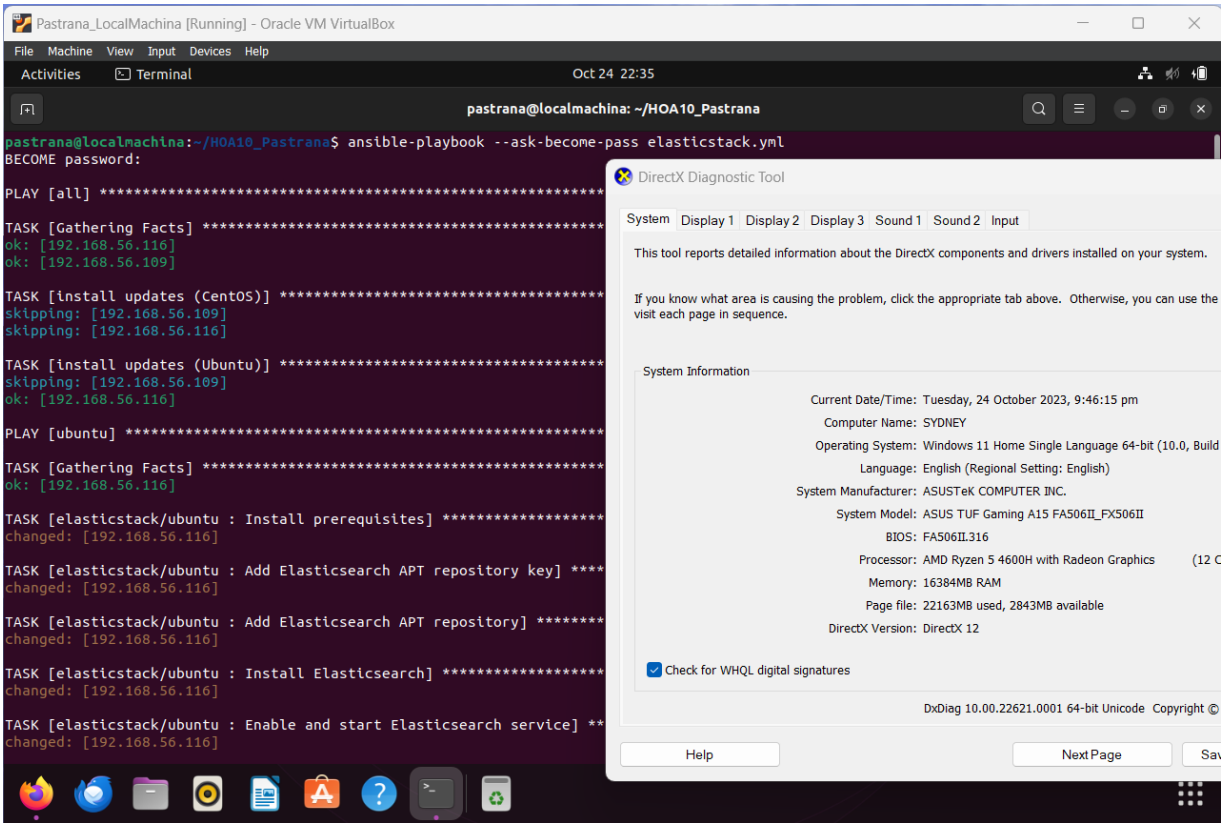


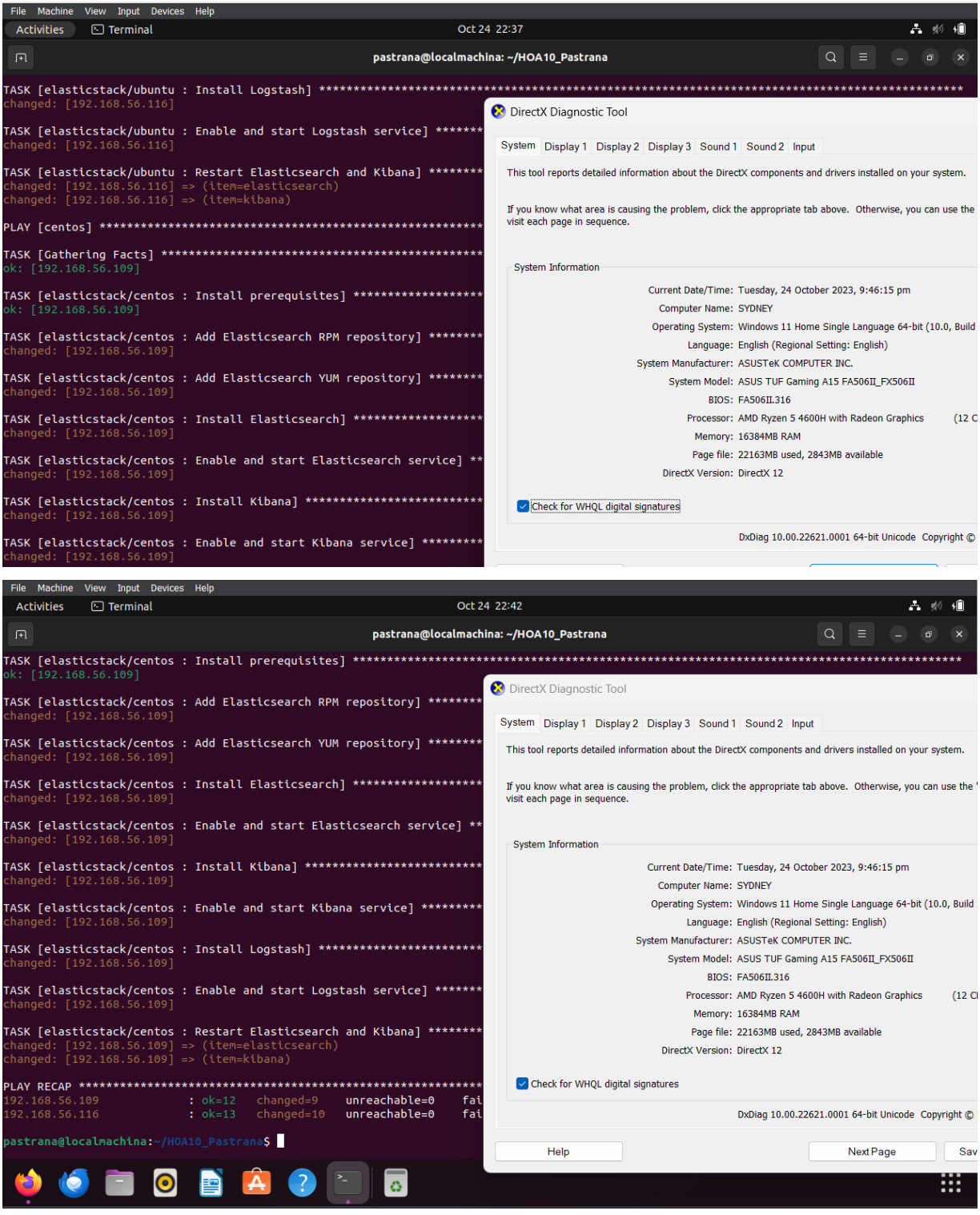
CentOS:

- I also created the main.yml file for the CentOS role. It has the same flow of functions, but some of the syntax has been altered to fit CentOS.



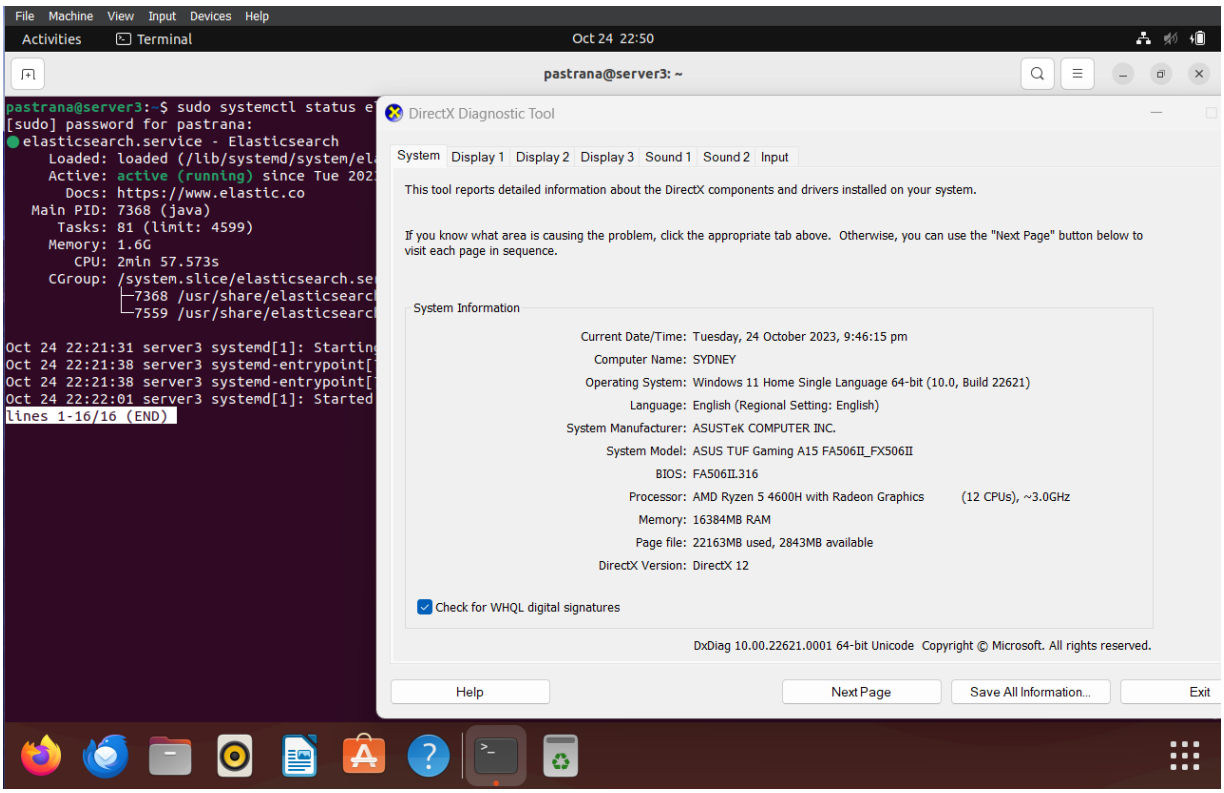
Running the elasticstack.yml playbook successfully.

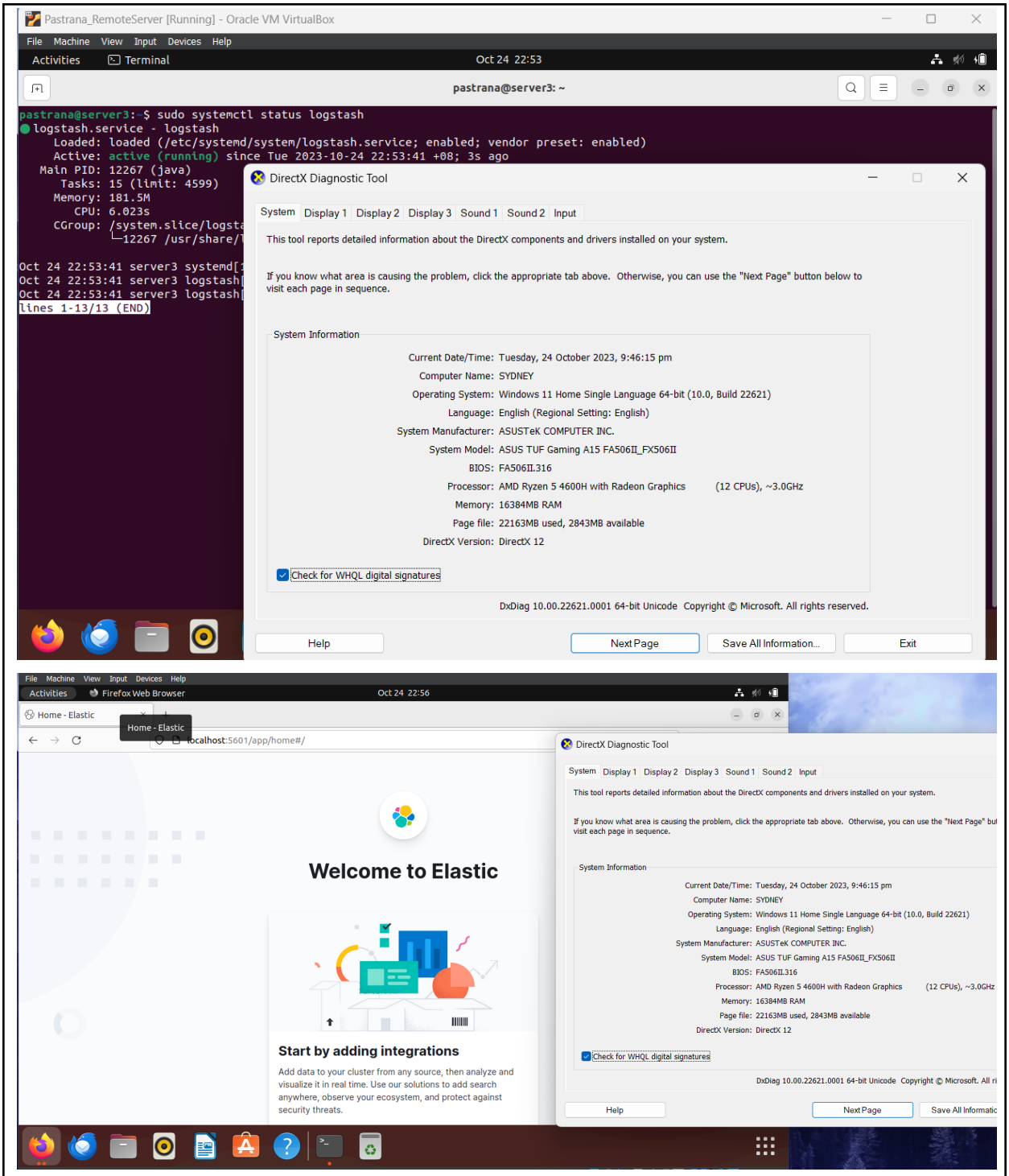




3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like a manual.)

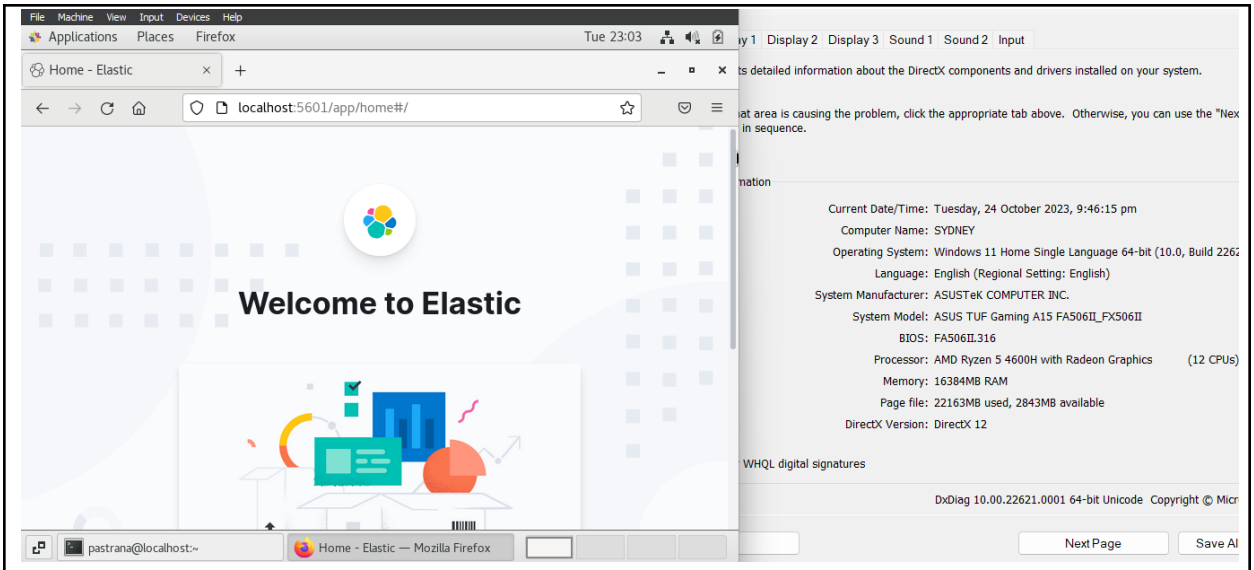
4. Show an output of the installed Elastic Stack for both Ubuntu and CentOS.
   Ubuntu:



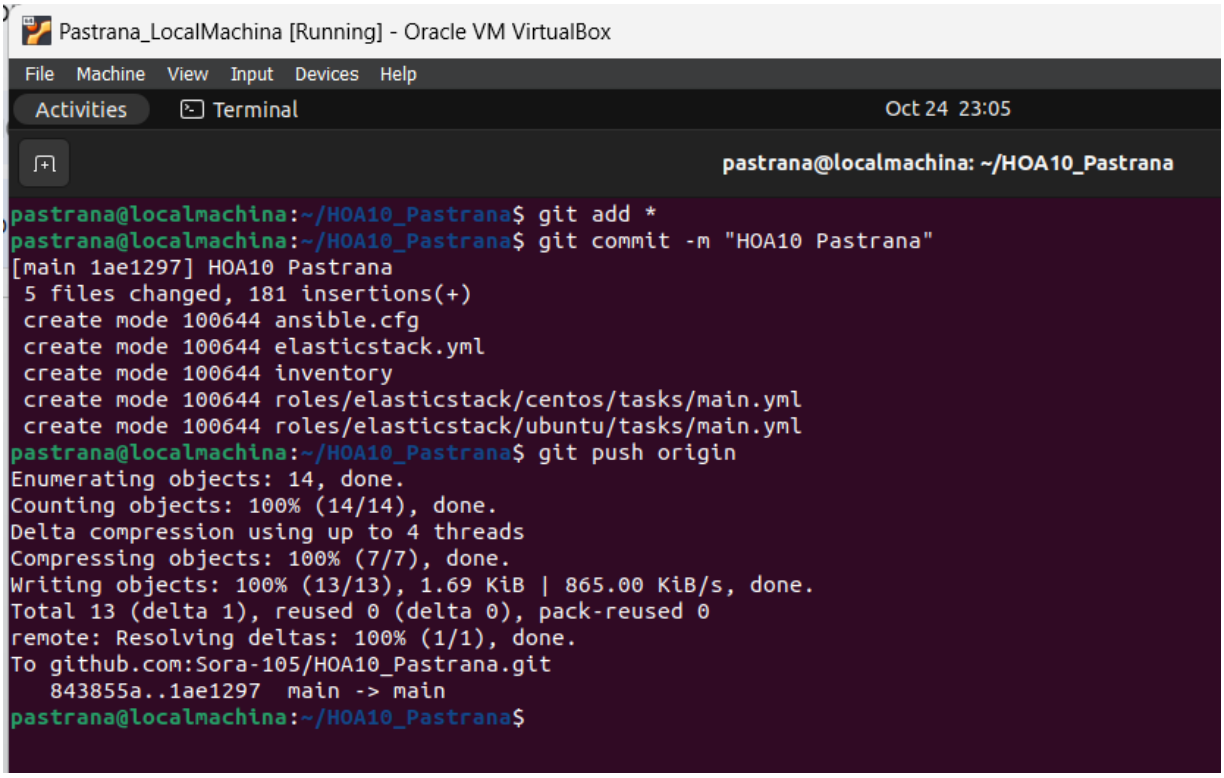

Pastrana_RemoteServer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 24 22:53
pastrana@server3: ~
pastrana@server3:~$ sudo systemctl status logstash
logstash.service - logstash
Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2023-10-24 22:53:41 +08; 3s ago
Main PID: 12267 (java)
Tasks: 15 (limit: 4599)
Memory: 181.5M
CPU: 6.023s
CGroup: /system.slice/logsta
└─12267 /usr/share/
Oct 24 22:53:41 server3 systemd[1
Oct 24 22:53:41 server3 logstash
Oct 24 22:53:41 server3 logstash
lines 1-13/13 (END)
DirectX Diagnostic Tool
System Display 1 Display 2 Display 3 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: Tuesday, 24 October 2023, 9:46:15 pm
Computer Name: SYDNEY
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: ASUS TUF Gaming A15 FA506II_FX506II
BIOS: FA506II.316
Processor: AMD Ryzen 5 4600H with Radeon Graphics (12 CPUs), ~3.0GHz
Memory: 16384MB RAM
Page file: 22163MB used, 2843MB available
DirectX Version: DirectX 12
Check for WHQL digital signatures
DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.
Help
Next Page
Save All Information...
Exit
File Machine View Input Devices Help
Activities
Firefox Web Browser
Oct 24 22:56
Home - Elastic
localhost:5601/app/home#/
Welcome to Elastic
Start by adding integrations
Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats.
DirectX Diagnostic Tool
Help
Next Page

CentOS:


Pastrana_CentOS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Tue 22:57
pastrana@localhost:~
File Edit View Search Terminal Help
[pastrana@localhost ~]$ sudo systemctl status elasticsearch
[sudo] password for pastrana:
● elasticsearch.service - Elasticsearch
Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor prese
t: disabled)
Active: active (running) since Tue 2023-10-24 22:32:47 PST; 24min ago
Docs: https://www.elastic.co
Main PID: 6371 (java)
Tasks: 82
CGroup: /system.slice/elasticsearch.service
├─6371 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkadd...
└─6568 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/b...
Oct 24 22:32:09 localhost.localdomain systemd[1]: Starting Elasticsearch...
Oct 24 22:32:14 localhost.localdomain systemd-entrypoint[6371]: Oct 24, 2023 10:32:1...
Oct 24 22:32:14 localhost.localdomain systemd-entrypoint[6371]: WARNING: COMPAT loca...
Oct 24 22:32:47 localhost.localdomain systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
[pastrana@localhost ~]$
pastrana@localhost:~
Current Date/Time: Tuesday, 24 October 2023, 9:46:15 pm
Computer Name: SYDNEY
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 226
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ASUS TUF Gaming A15 FA506II_FX506II
BIOS: FA506II.316
Processor: AMD Ryzen 5 4600H with Radeon Graphics (12 CPUs)
Memory: 16384MB RAM
Page file: 22163MB used, 2843MB available
DirectX Version: DirectX 12
WHQL digital signatures
DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Micr
Next Page
Save Al
File Machine View Input Devices Help
Applications Places Terminal Tue 22:59
pastrana@localhost:~
File Edit View Search Terminal Help
[pastrana@localhost ~]$ sudo systemctl status kibana
● kibana.service - Kibana
Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled
)
Active: active (running) since Tue 2023-10-24 22:32:52 PST; 26min ago
Docs: https://www.elastic.co
Main PID: 6759 (node)
Tasks: 11
CGroup: /system.slice/kibana.service
└─6759 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../sr...
Oct 24 22:32:52 localhost.localdomain systemd[1]: Started Kibana.
Oct 24 22:32:53 localhost.localdomain kibana[6759]: Kibana is currently running wit...r
Hint: Some lines were ellipsized, use -l to show in full.
[pastrana@localhost ~]$
[pastrana@localhost ~]$
[pastrana@localhost ~]$
[pastrana@localhost ~]$
[pastrana@localhost ~]$
[pastrana@localhost ~]$
[pastrana@localhost ~]$
[pastrana@localhost ~]$
[pastrana@localhost ~]$
[pastrana@localhost ~]$
Current Date/Time: Tuesday, 24 October 2023, 9:46:15 pm
Computer Name: SYDNEY
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 226
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ASUS TUF Gaming A15 FA506II_FX506II
BIOS: FA506II.316
Processor: AMD Ryzen 5 4600H with Radeon Graphics (12 CPUs
Memory: 16384MB RAM
Page file: 22163MB used, 2843MB available
DirectX Version: DirectX 12
WHQL digital signatures
DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Micr
File Machine View Input Devices Help
Applications Places Terminal Tue 23:02
pastrana@localhost:~
File Edit View Search Terminal Help
[pastrana@localhost ~]$ sudo systemctl status logstash
● logstash.service - logstash
Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabl
ed)
Active: active (running) since Tue 2023-10-24 23:01:13 PST; 39s ago
Main PID: 10456 (java)
Tasks: 24
CGroup: /system.slice/logstash.service
└─10456 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSw...
Oct 24 23:01:13 localhost.localdomain systemd[1]: Started logstash.
Oct 24 23:01:13 localhost.localdomain logstash[10456]: Using bundled JDK: /usr/shar...k
Oct 24 23:01:14 localhost.localdomain logstash[10456]: OpenJDK 64-Bit Server VM war....
Oct 24 23:01:47 localhost.localdomain logstash[10456]: Sending Logstash logs to /va...s
Oct 24 23:01:47 localhost.localdomain logstash[10456]: [2023-10-24T23:01:47,304][IN...s
Oct 24 23:01:47 localhost.localdomain logstash[10456]: [2023-10-24T23:01:47,334][IN...}
Oct 24 23:01:47 localhost.localdomain logstash[10456]: [2023-10-24T23:01:47,338][INF...
Oct 24 23:01:49 localhost.localdomain logstash[10456]: [2023-10-24T23:01:49,913][IN...}
Oct 24 23:01:49 localhost.localdomain logstash[10456]: [2023-10-24T23:01:49,925][ER....
Oct 24 23:01:49 localhost.localdomain logstash[10456]: [2023-10-24T23:01:49,932][IN...}
Hint: Some lines were ellipsized, use -l to show in full.
[pastrana@localhost ~]$
[pastrana@localhost ~]$
[pastrana@localhost ~]$
[pastrana@localhost ~]$
Current Date/Time: Tuesday, 24 October 2023, 9:46:15 pm
Computer Name: SYDNEY
Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 226
Language: English (Regional Setting: English)
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: ASUS TUF Gaming A15 FA506II_FX506II
BIOS: FA506II.316
Processor: AMD Ryzen 5 4600H with Radeon Graphics (12 CPUs)
Memory: 16384MB RAM
Page file: 22163MB used, 2843MB available
DirectX Version: DirectX 12
WHQL digital signatures
DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Micr



5. Make sure to create a new repository in GitHub for this activity.



https://github.com/Sora-105/HOA10_Pastrana.git

Reflections:

Answer the following:

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

- The advantages of using a log monitoring program include increased system security. Log monitoring tools save a log of the various times a system is used or accessed. Having a copy of these logs can help offer an extra degree of security to the servers and system, as well as aid in the troubleshooting of any faults that may develop as a result of the saved logs with various time stamps.

Conclusions:

- I gained valuable insights into the significance of log monitoring tools in server management. Two specific tools, namely the Elastic Stack and Graylog, were introduced as examples. The primary objective of this activity was to install and configure the Elastic Stack, comprising Elasticsearch, Kibana, Beats, and Logstash.I successfully accomplished this task by utilizing Git and an Ansible playbook with predefined roles. Initially, I found the process a bit perplexing due to the various components that needed to be installed, along with their corresponding dependencies. In order to troubleshoot this error, I turned to online resources such as guides and tutorials, which provided step-by-step instructions and command references. I then converted this acquired knowledge into a playbook format for implementation on both Ubuntu and CentOS systems.