Name: Rio Marie G. Suzuki	**Date Performed:** 10/23/2023
Course/Section: CPE232S6	**Date Submitted:** 10/23/2023
Instructor: Dr. Jonathan Taylar	**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.

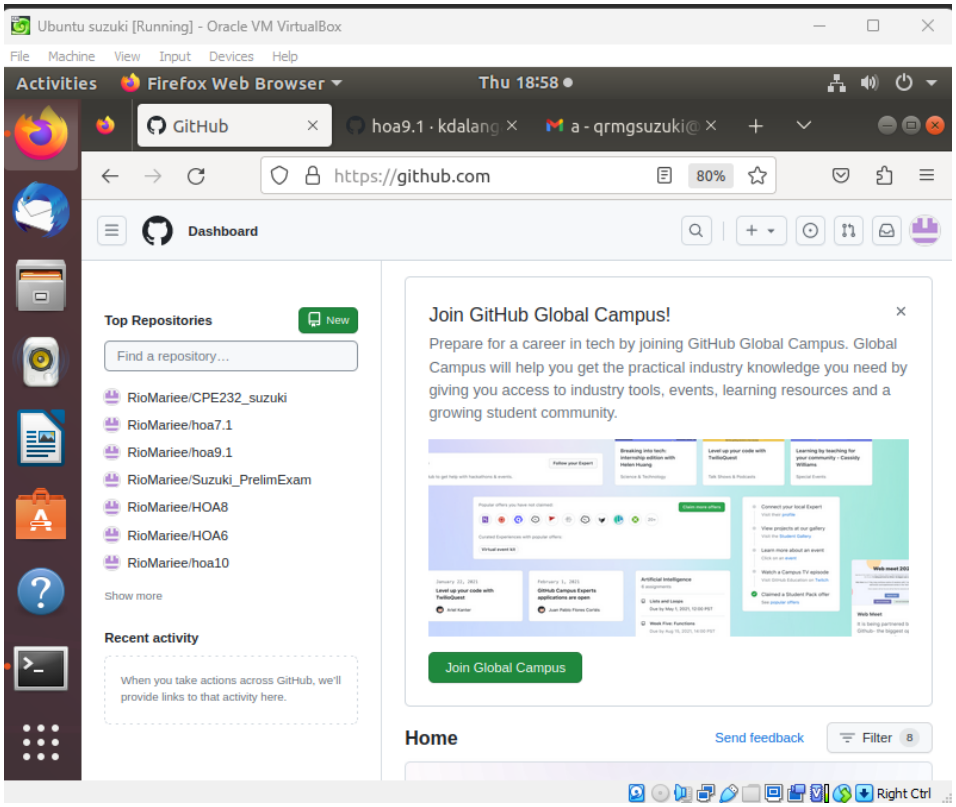
Source: https://www.graylog.org/products/open-source

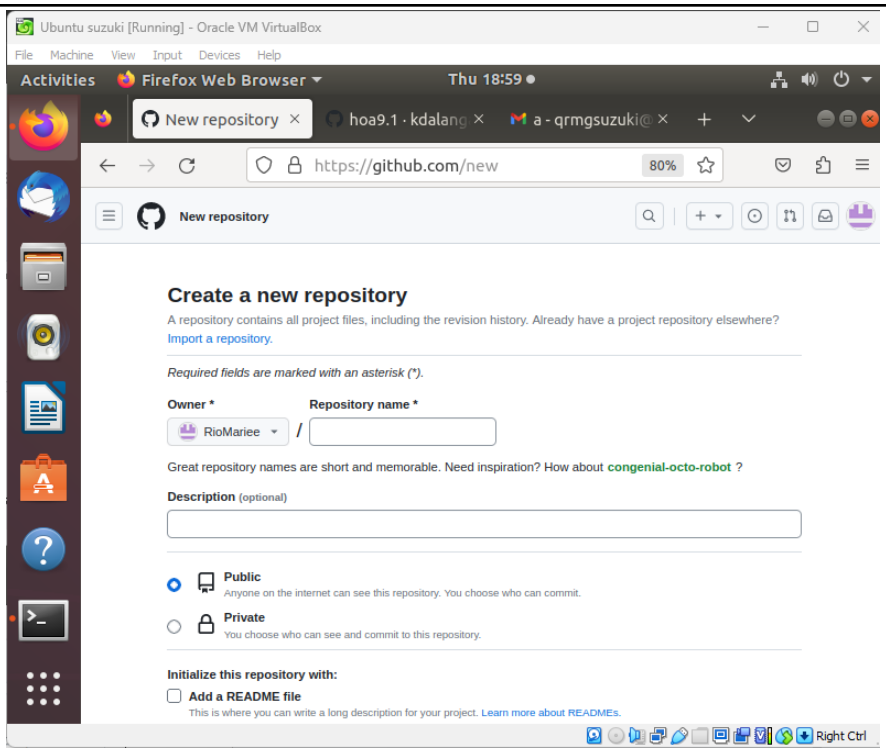
3. Tasks

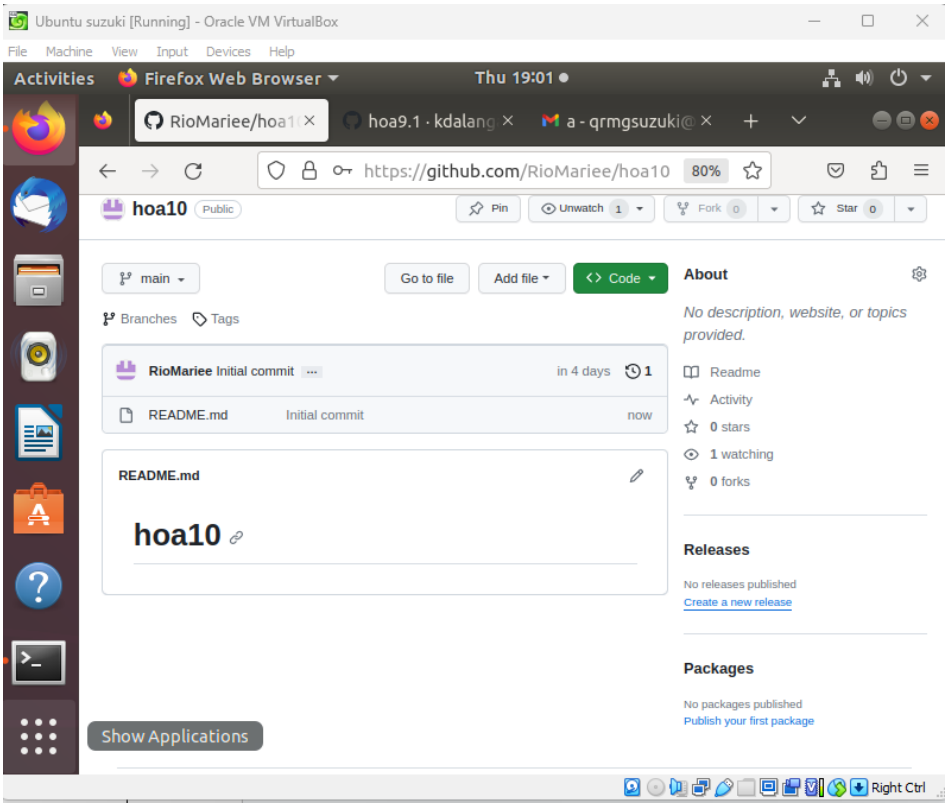
1. Create a playbook that:
    a. Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)
2. Apply the concept of creating roles.
3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like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

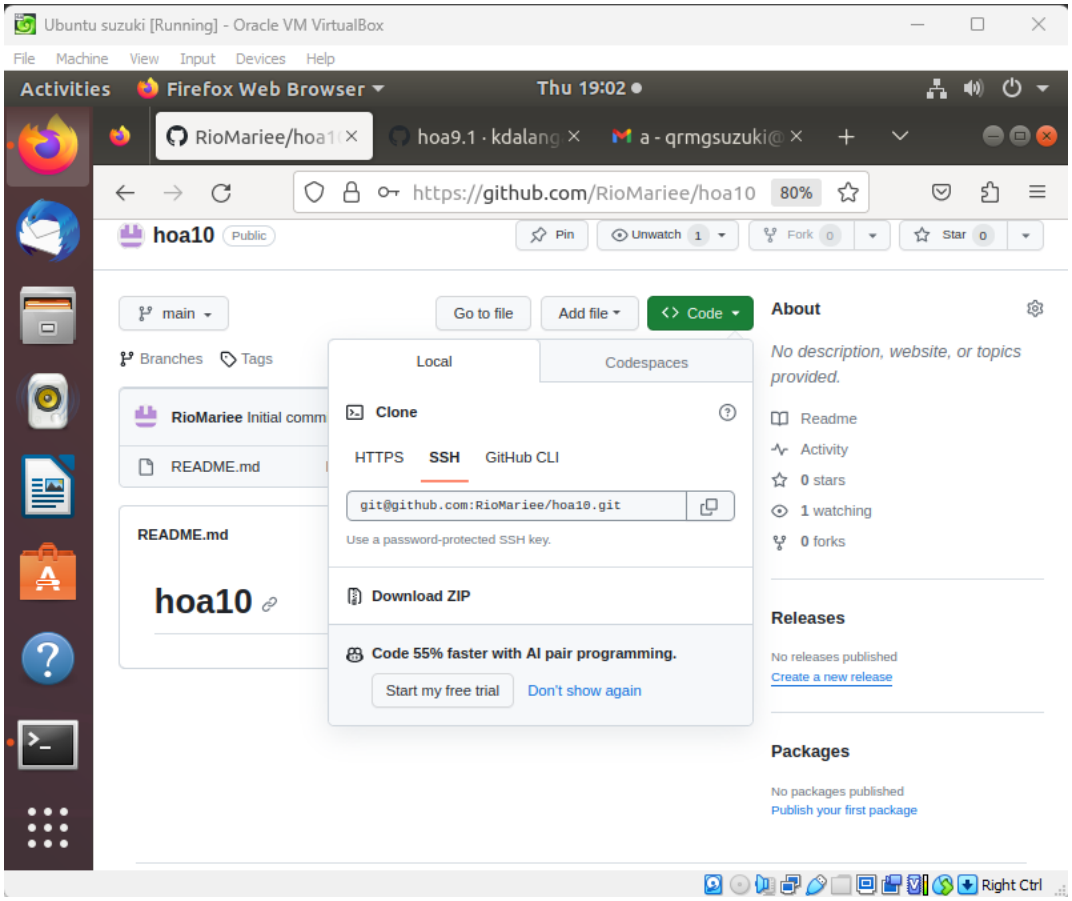
Step 1. First thing first, we will create a new repository for this activity. To create a new repository, we will go to git hub.com and sign in our account. On the left side you will see the list of repositories and click create new repository and name it “hoa10”.



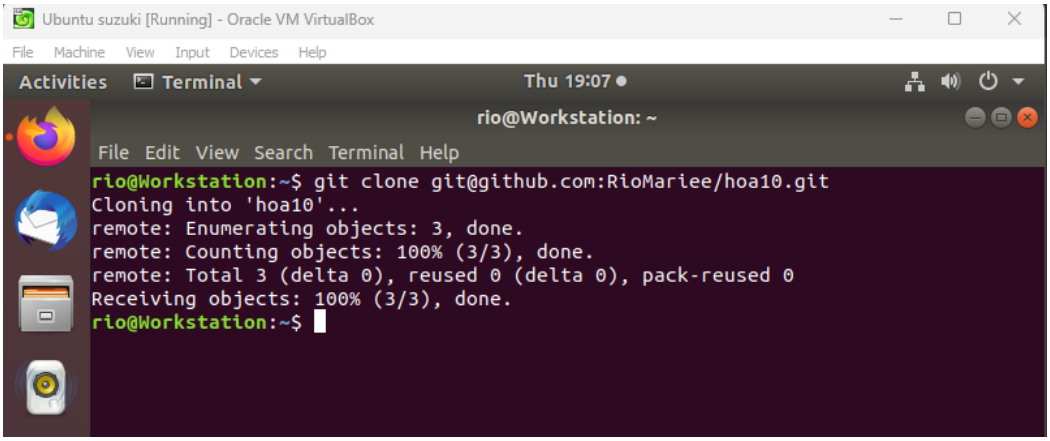

Ubuntu suzuki [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Thu 18:59
New repository
hoa9.1 · kdalang
a - qrmgsuzuki@
https://github.com/new
80%
New repository
Create a new repository
A repository contains all project files, including the revision history. Already have a project repository elsewhere?
Import a repository.
Required fields are marked with an asterisk (*).
Owner *
Repository name *
RioMariee
Great repository names are short and memorable. Need inspiration? How about congenial-octo-robot ?
Description (optional)
Public
Anyone on the internet can see this repository. You choose who can commit.
Private
You choose who can see and commit to this repository.
Initialize this repository with:
Add a README file
This is where you can write a long description for your project. Learn more about READMEs.
Right Ctrl


Ubuntu suzuki [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Thu 19:01
RioMariee/hoa1
hoa9.1 · kdalang
a - qrmgsuzuki@
https://github.com/RioMariee/hoa10
80%
hoa10
Public
Pin
Unwatch 1
Fork 0
Star 0
main
Go to file
Add file
Code
Branches
Tags
RioMariee Initial commit
in 4 days
1
README.md
Initial commit
now
README.md
hoa10
About
No description, website, or topics provided.
Readme
Activity
0 stars
1 watching
0 forks
Releases
No releases published
Create a new release
Packages
No packages published
Publish your first package
Show Applications
Right Ctrl

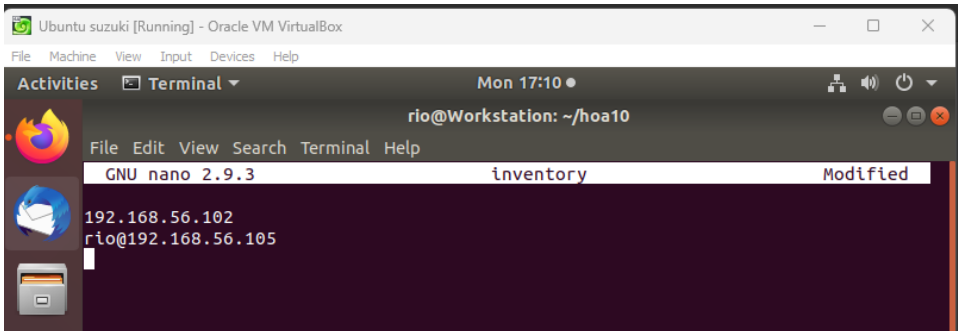
Step 2. Next step we will copy the link of the created new repository by clicking the code and select “ssh” then click the copy button. After copying the ssh we will now paste it in the Ubuntu terminal together with the command “git clone (ssh of the repository)”.



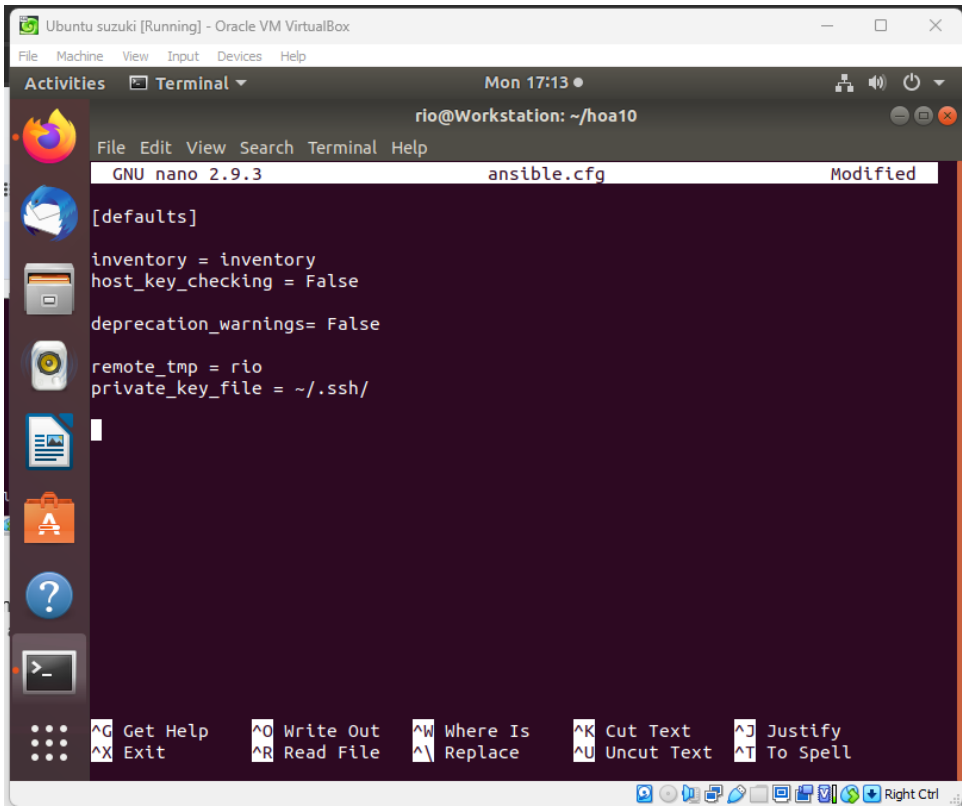
Output:



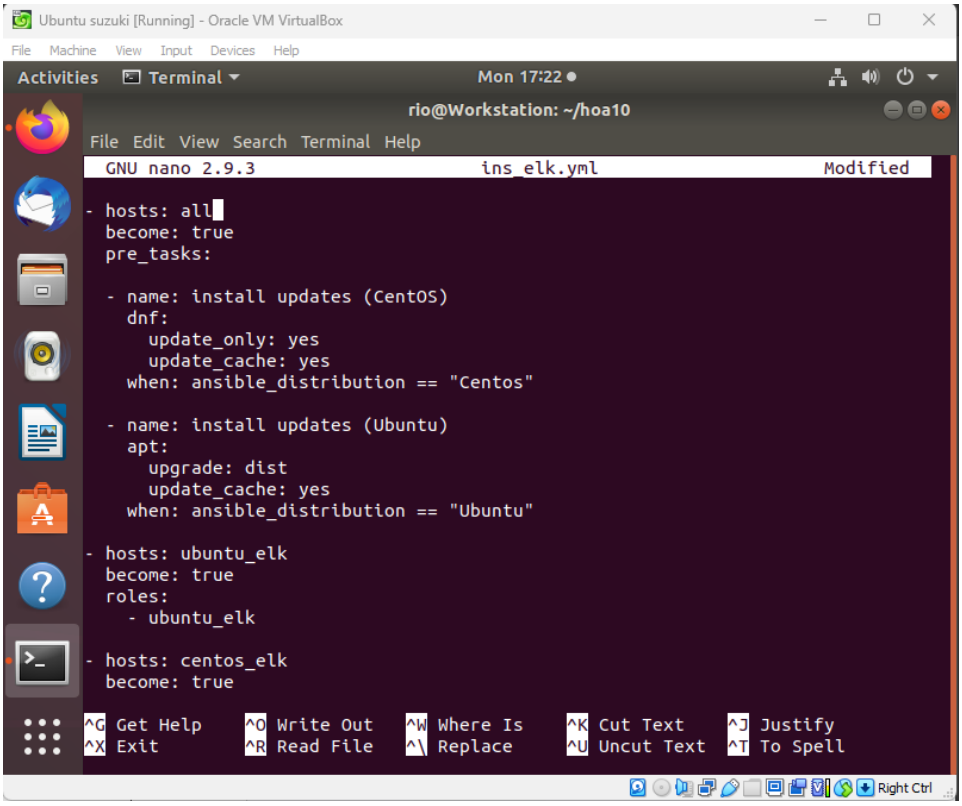
Step 3. After cloning the repository we will now enter the repository we created in Ubuntu and create the inventory using the command “sudo nano inventory” and put the ip address of the centos and the server 1 ip address, and don’t forget to save it.



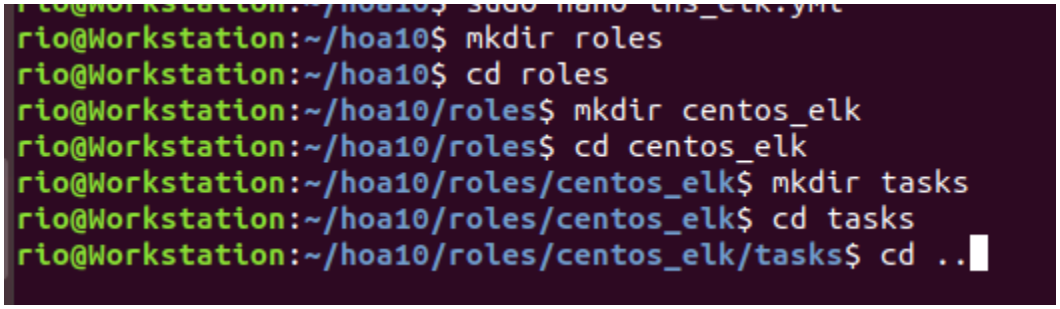
Step 4. After creating the inventory we will now also create the ansible.cfg. The contents of the ansible.cfg will remain the same just like in the previous activities. Press ctrl+z then press y to confirm the save settings.



Step 5. Next we will create the ins_elk.yml, this will contain the updates needed for both Ubuntu and CentOS. After creating the ins_elk.yml don't forget to save it.



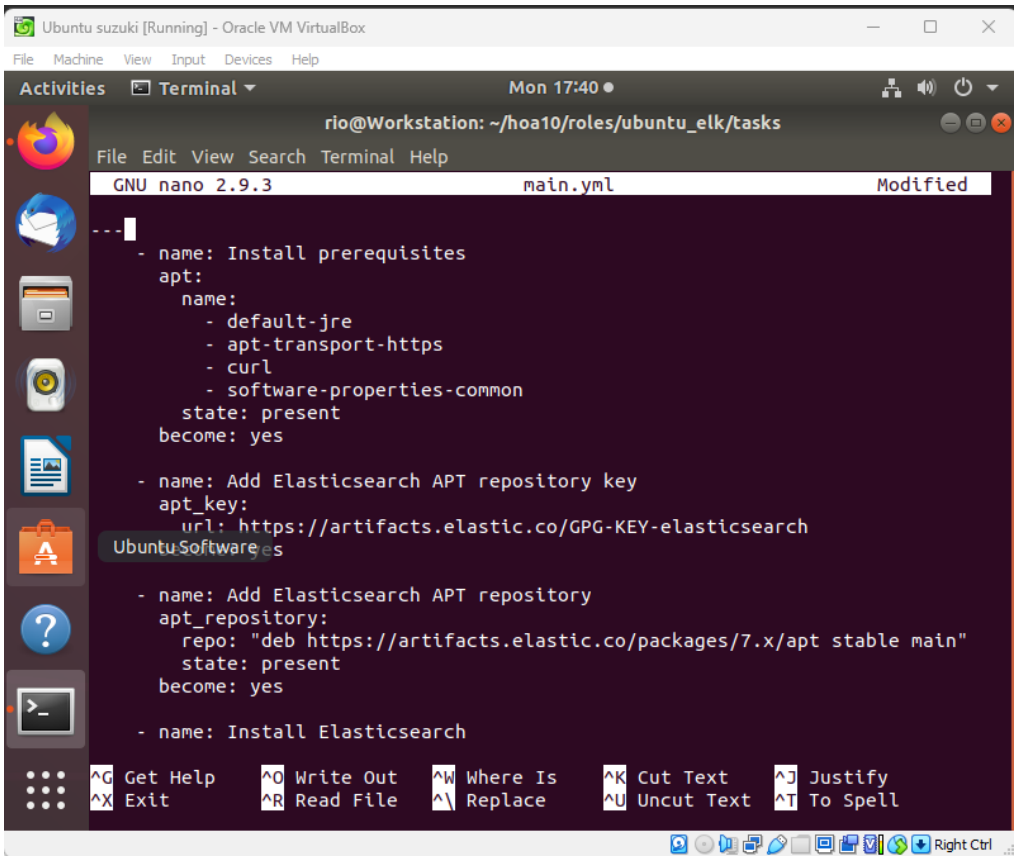
Step 6. After we created the ins_elk.yml, we will now create a tree consisting of roles and centos_elk and ubuntu_elk under each of them will be the tasks and the main.yml. to create the tree we will use the command "mkdir (name of the directory)" and the command "cd (name of the created new directory)" to change directory, and "cd .." to go back.



```
rio@Workstation:~/hoa10/roles$ cd ubuntu_elk
rio@Workstation:~/hoa10/roles/ubuntu_elk$ mkdir tasks
rio@Workstation:~/hoa10/roles/ubuntu_elk$ cd tasks
rio@Workstation:~/hoa10/roles/ubuntu_elk/tasks$ sudo nano main.yml
```

Step 7. After creating the ubuntu_elk and the centos_elk, we will now create the main.yml under the ubuntu_elk and centos_elk. Also, don't forget to save your work.

Input: Ubuntu_elk main.yml contents:



Ubuntu suzuki [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 17:41

rio@Workstation: ~/hoa10/roles/ubuntu_elk/tasks

File Edit View Search Terminal Help

```
GNU nano 2.9.3                    main.yml                    Modified

    apt_key:
      url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    become: yes

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

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

  - name: Enable and start Elasticsearch service
    systemd:
      name: elasticsearch
      enabled: yes
      state: started
    become: yes

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Right Ctrl

Ubuntu suzuki [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 17:41

rio@Workstation: ~/hoa10/roles/ubuntu_elk/tasks

File Edit View Search Terminal Help

```
GNU nano 2.9.3                    main.yml                    Modified

      name: elasticsearch
      state: present
    become: yes

  - name: Enable and start Elasticsearch service
    systemd:
      name: elasticsearch
      enabled: yes
      state: started
    become: yes

  - name: Install Kibana
    apt:
      name: kibana
      state: present
    become: yes

  - name: Enable and start Kibana service
    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Right Ctrl

Ubuntu suzuki [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 17:41

rio@Workstation: ~/hoa10/roles/ubuntu_elk/tasks

File Edit View Search Terminal Help

```
GNU nano 2.9.3                    main.yml                    Modified

    apt:
      name: kibana
      state: present
    become: yes

  - name: Enable and start Kibana service
    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

  - name: Install Logstash
    apt:
      name: logstash
      state: present
    become: yes

  - name: Enable and start Logstash service
    systemd:
      name: logstash
      enabled: yes
      state: started

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Right Ctrl

Ubuntu suzuki [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 17:42

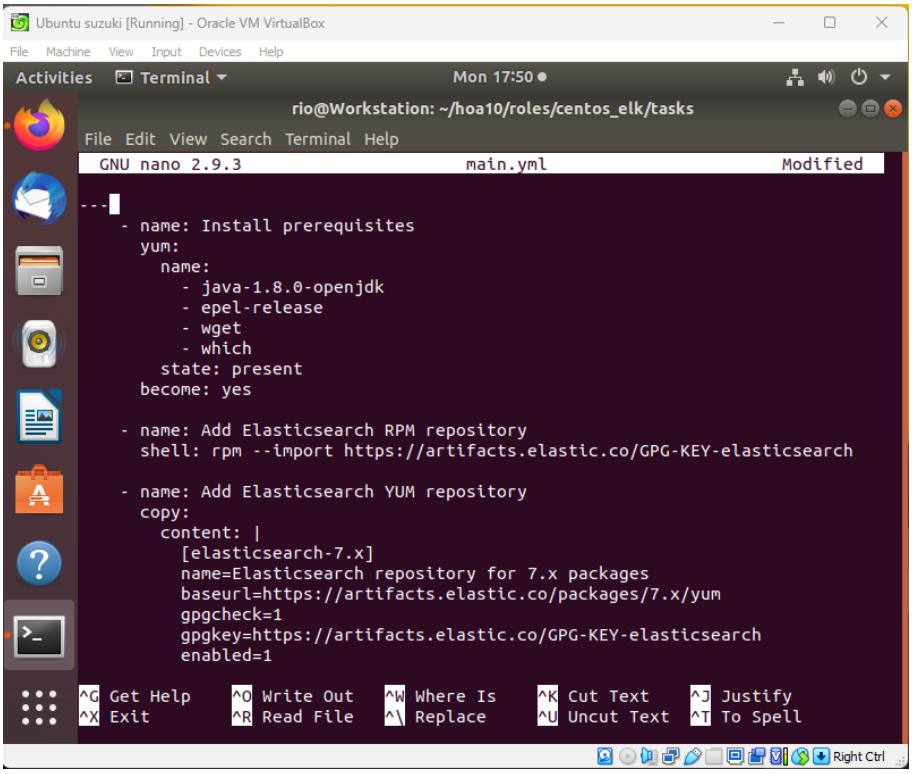
rio@Workstation: ~/hoa10/roles/ubuntu_elk/tasks

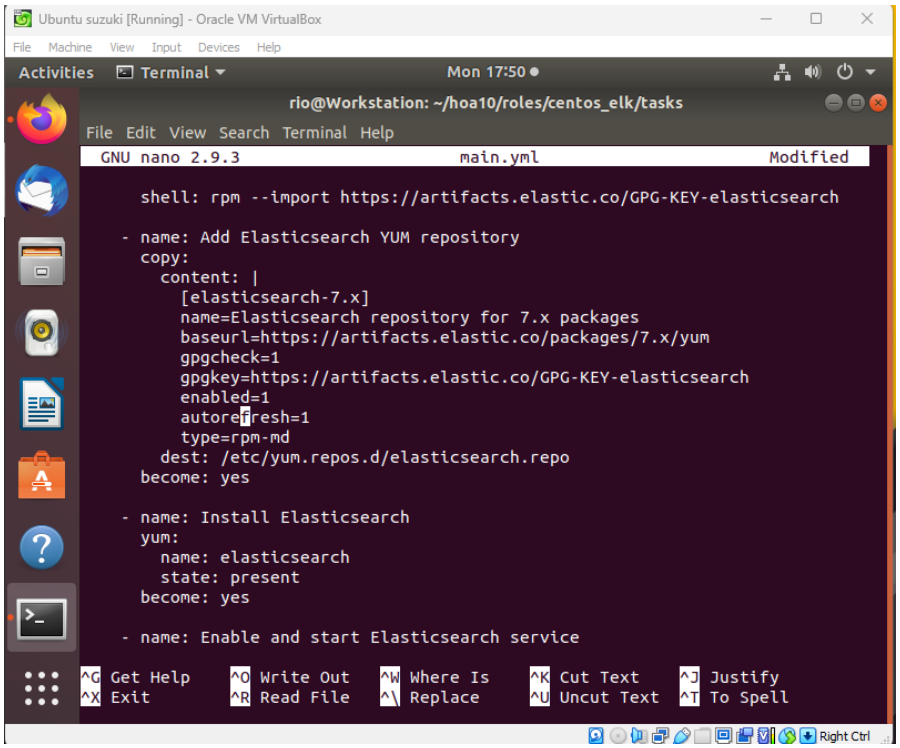
File Edit View Search Terminal Help

```
GNU nano 2.9.3                    main.yml                    Modified

  - name: Install Logstash
    apt:
      name: logstash
      state: present
    become: yes

  - name: Enable and start Logstash service
    systemd:
      name: logstash
      enabled: yes
      state: started
    become: yes

  - name: Restart Elasticsearch and Kibana
    systemd:
      name: "{{ item }}"
      state: restarted
    loop:
      - elasticsearch
      - kibana

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Right Ctrl

Input: contents of centos_elk main.yml.





Ubuntu suzuki [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 17:50

rio@Workstation: ~/hoa10/roles/centos_elk/tasks

File Edit View Search Terminal Help

```
GNU nano 2.9.3                    main.yml                    Modified

        type=rpm-md
      dest: /etc/yum.repos.d/elasticsearch.repo
    become: yes

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

  - name: Enable and start Elasticsearch service
    systemd:
      name: elasticsearch
      enabled: yes
      state: started
    become: yes

  - name: Install Kibana
    yum:
      name: kibana
      state: present
    become: yes

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Right Ctrl

Ubuntu suzuki [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 17:51

rio@Workstation: ~/hoa10/roles/centos_elk/tasks

File Edit View Search Terminal Help

```
GNU nano 2.9.3                    main.yml                    Modified

      name: elasticsearch
      enabled: yes
      state: started
    become: yes

  - name: Install Kibana
    yum:
      name: kibana
      state: present
    become: yes

  - name: Enable and start Kibana service
    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

  - name: Install Logstash
    yum:
      name: logstash
      state: present
    become: yes

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Right Ctrl

Ubuntu suzuki [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 17:51

rio@Workstation: ~/hoa10/roles/centos_elk/tasks

File Edit View Search Terminal Help

```
GNU nano 2.9.3                    main.yml                    Modified

    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

  - name: Install Logstash
    yum:
      name: logstash
      state: present
    become: yes

  - name: Enable and start Logstash service
    systemd:
      name: logstash
      enabled: yes
      state: started
    become: yes

  - name: Restart Elasticsearch and Kibana
    systemd:
Terminaname: "{{ item }}"
      state: restarted

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Right Ctrl

Ubuntu suzuki [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 17:51

rio@Workstation: ~/hoa10/roles/centos_elk/tasks

File Edit View Search Terminal Help

```
GNU nano 2.9.3                    main.yml                    Modified

  - name: Enable and start Logstash service
    systemd:
      name: logstash
      enabled: yes
      state: started
    become: yes

  - name: Restart Elasticsearch and Kibana
    systemd:
      name: "{{ item }}"
      state: restarted
    loop:
      - elasticsearch
      - kibana

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Right Ctrl

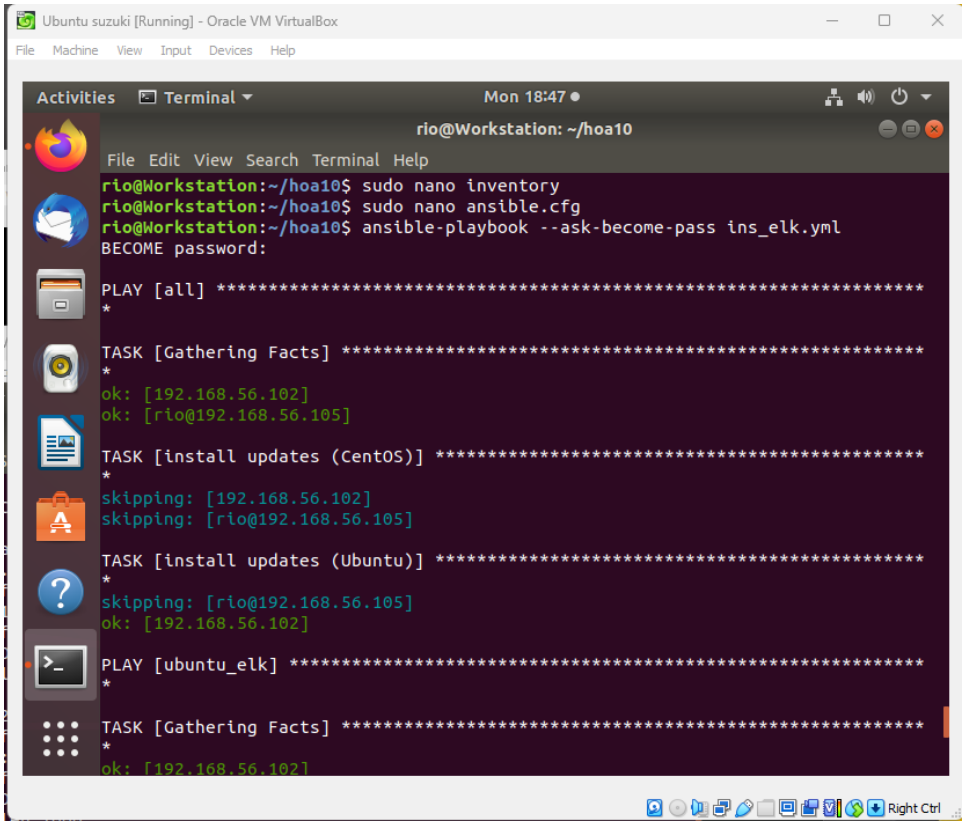
Step 8. After creating the main.yml of the activities we will now issue the command “tree” to double check if we did the tree right. To exit the directory you are currently in use the command “cd ..”.

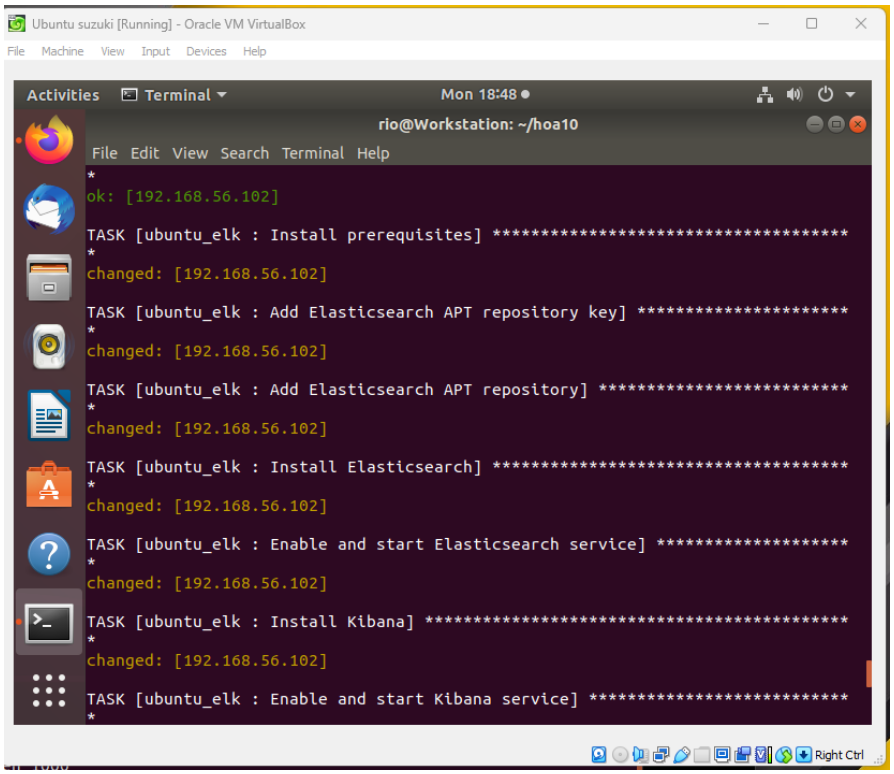
```
rio@Workstation:~/hoa10/roles/centos_elk/tasks$ cd ..
rio@Workstation:~/hoa10/roles/centos_elk$ cd ..
rio@Workstation:~/hoa10/roles$ cd ..
rio@Workstation:~/hoa10$
```

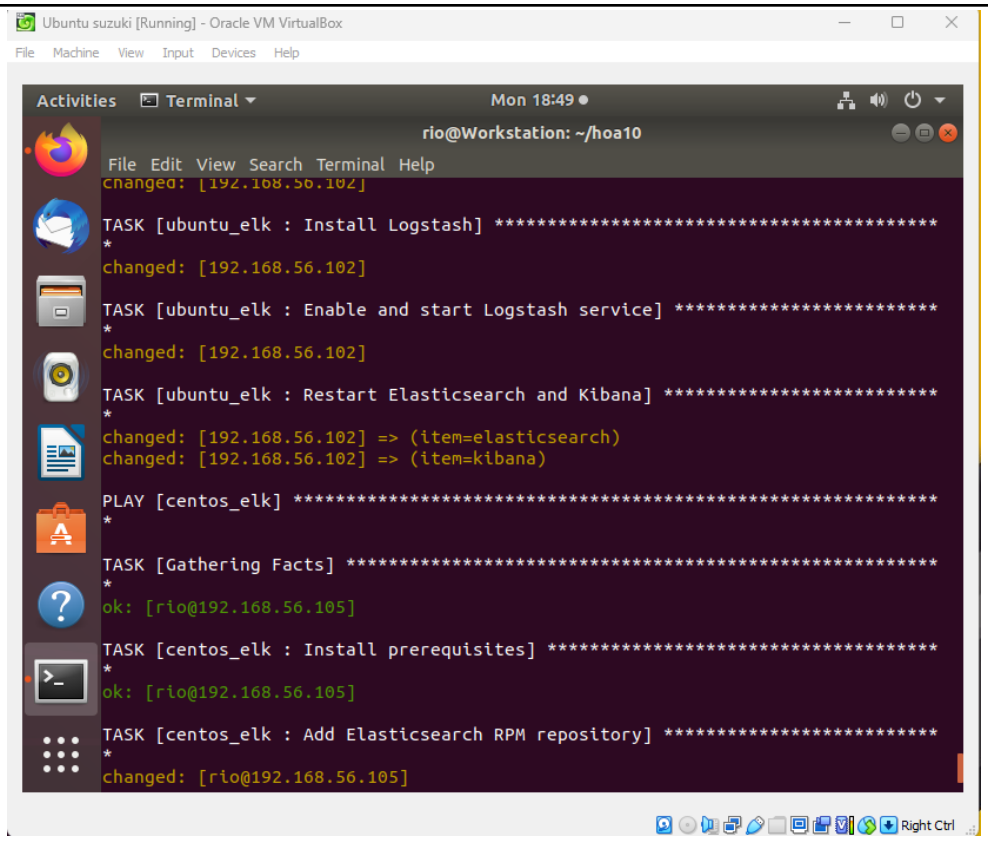
```
rio@Workstation:~/hoa10$ tree
.
├── ansible.cfg
├── ins_elk.yml
├── inventory
├── README.md
└── roles
    ├── centos_elk
    │   └── tasks
    │       └── main.yml
    └── ubuntu_elk
        └── tasks
            └── main.yml

5 directories, 6 files
rio@Workstation:~/hoa10$
```

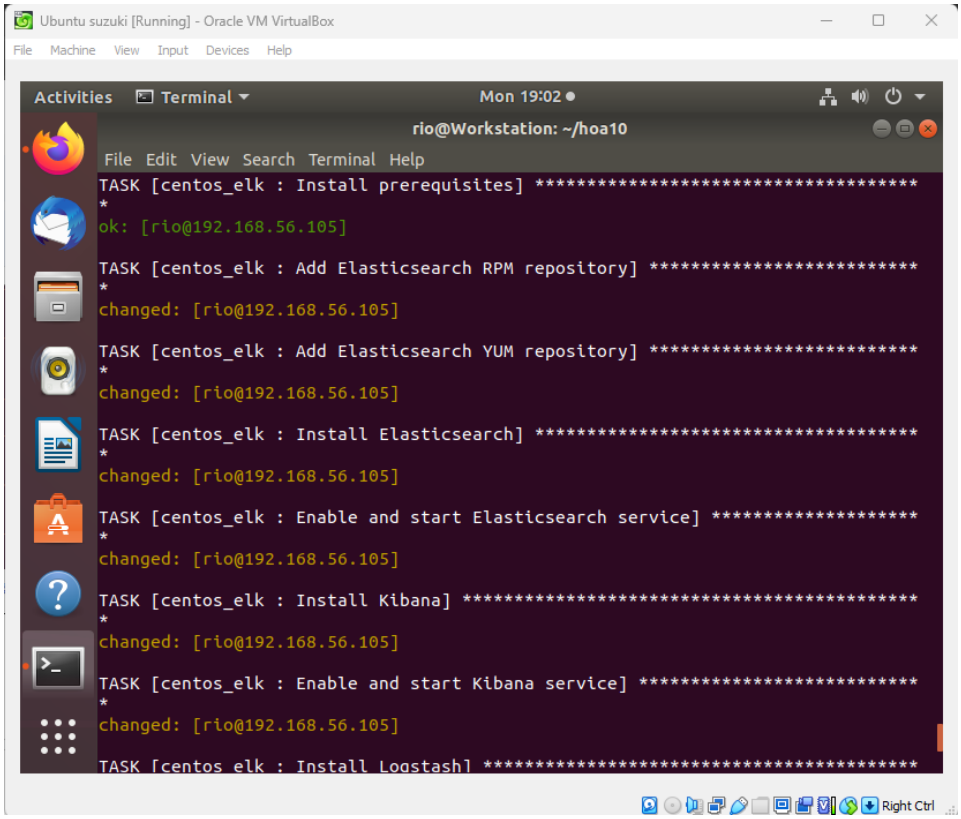
Step 9. Now run the command “Ansible-playbook –ask-become-pass ins_elk” and enter your workstation password this will run the commands we have in the ins_elk and if it has no error then the command is right and working.

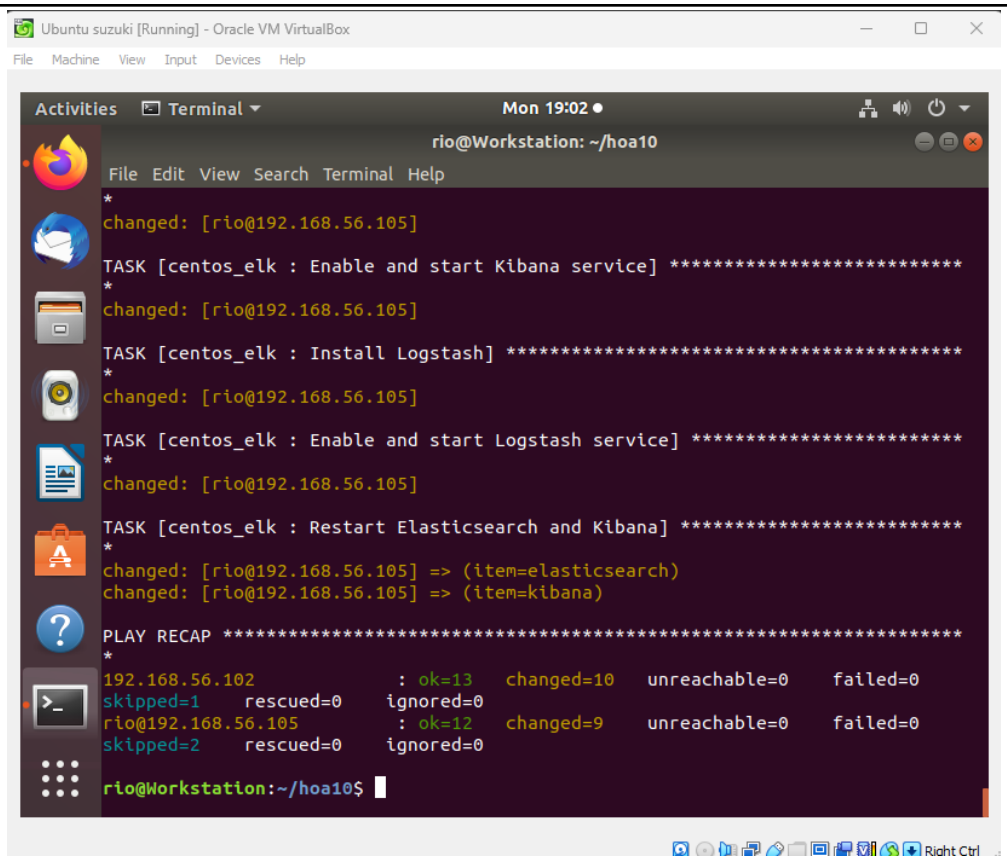
Process:


Ubuntu suzuki [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mon 18:47
rio@Workstation: ~/hoa10
File Edit View Search Terminal Help
rio@Workstation:~/hoa10$ sudo nano inventory
rio@Workstation:~/hoa10$ sudo nano ansible.cfg
rio@Workstation:~/hoa10$ ansible-playbook --ask-become-pass ins_elk.yml
BECOME password:
PLAY [all] ***
*
TASK [Gathering Facts] ***
*
ok: [192.168.56.102]
ok: [rio@192.168.56.105]
TASK [install updates (CentOS)] **
*
skipping: [192.168.56.102]
skipping: [rio@192.168.56.105]
TASK [install updates (Ubuntu)] **
*
skipping: [rio@192.168.56.105]
ok: [192.168.56.102]
PLAY [ubuntu_elk] **
*
TASK [Gathering Facts] ***
*
ok: [192.168.56.102]
Right Ctrl


Ubuntu suzuki [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mon 18:48
rio@Workstation: ~/hoa10
File Edit View Search Terminal Help
*
ok: [192.168.56.102]
TASK [ubuntu_elk : Install prerequisites] ***********************************
*
changed: [192.168.56.102]
TASK [ubuntu_elk : Add Elasticsearch APT repository key] ********************
*
changed: [192.168.56.102]
TASK [ubuntu_elk : Add Elasticsearch APT repository] ************************
*
changed: [192.168.56.102]
TASK [ubuntu_elk : Install Elasticsearch] ***********************************
*
changed: [192.168.56.102]
TASK [ubuntu_elk : Enable and start Elasticsearch service] ******************
*
changed: [192.168.56.102]
TASK [ubuntu_elk : Install Kibana] **
*
changed: [192.168.56.102]
TASK [ubuntu_elk : Enable and start Kibana service] *************************
*
Right Ctrl


Ubuntu suzuki [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mon 18:49
rio@Workstation: ~/hoa10
File Edit View Search Terminal Help
changed: [192.168.56.102]
TASK [ubuntu_elk : Install Logstash] ***********
changed: [192.168.56.102]
TASK [ubuntu_elk : Enable and start Logstash service] ***********
changed: [192.168.56.102]
TASK [ubuntu_elk : Restart Elasticsearch and Kibana] ***********
changed: [192.168.56.102] => (item=elasticsearch)
changed: [192.168.56.102] => (item=kibana)
PLAY [centos_elk] ***********
TASK [Gathering Facts] ***********
ok: [rio@192.168.56.105]
TASK [centos_elk : Install prerequisites] ***********
ok: [rio@192.168.56.105]
TASK [centos_elk : Add Elasticsearch RPM repository] ***********
changed: [rio@192.168.56.105]
Right Ctrl

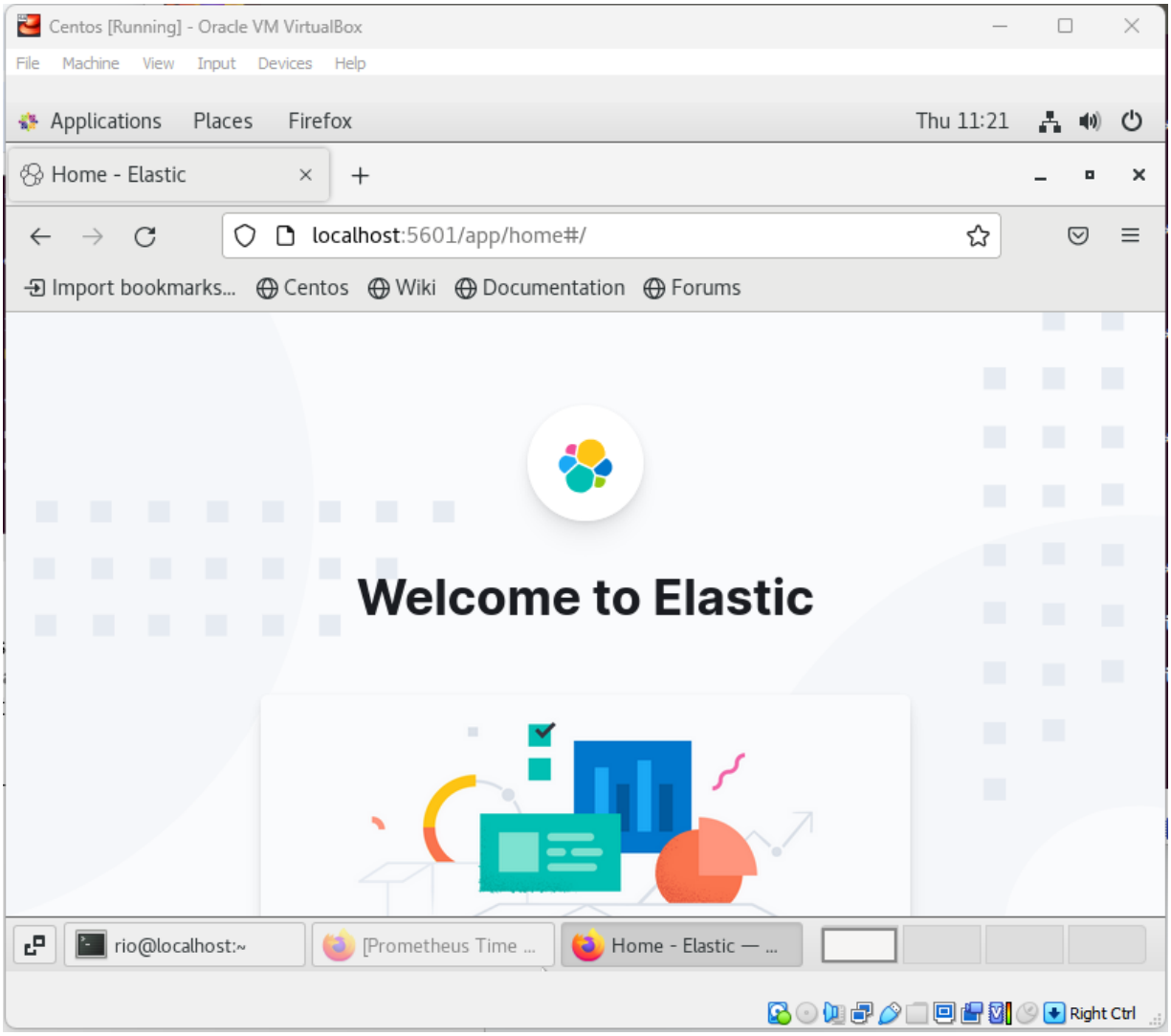

Ubuntu suzuki [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mon 19:02
rio@Workstation: ~/hoa10
File Edit View Search Terminal Help
TASK [centos_elk : Install prerequisites] ***********
ok: [rio@192.168.56.105]
TASK [centos_elk : Add Elasticsearch RPM repository] ***********
changed: [rio@192.168.56.105]
TASK [centos_elk : Add Elasticsearch YUM repository] ***********
changed: [rio@192.168.56.105]
TASK [centos_elk : Install Elasticsearch] ***********
changed: [rio@192.168.56.105]
TASK [centos_elk : Enable and start Elasticsearch service] ***********
changed: [rio@192.168.56.105]
TASK [centos_elk : Install Kibana] ***********
changed: [rio@192.168.56.105]
TASK [centos_elk : Enable and start Kibana service] ***********
changed: [rio@192.168.56.105]
TASK [centos_elk : Install Logstash] ***********
Right Ctrl

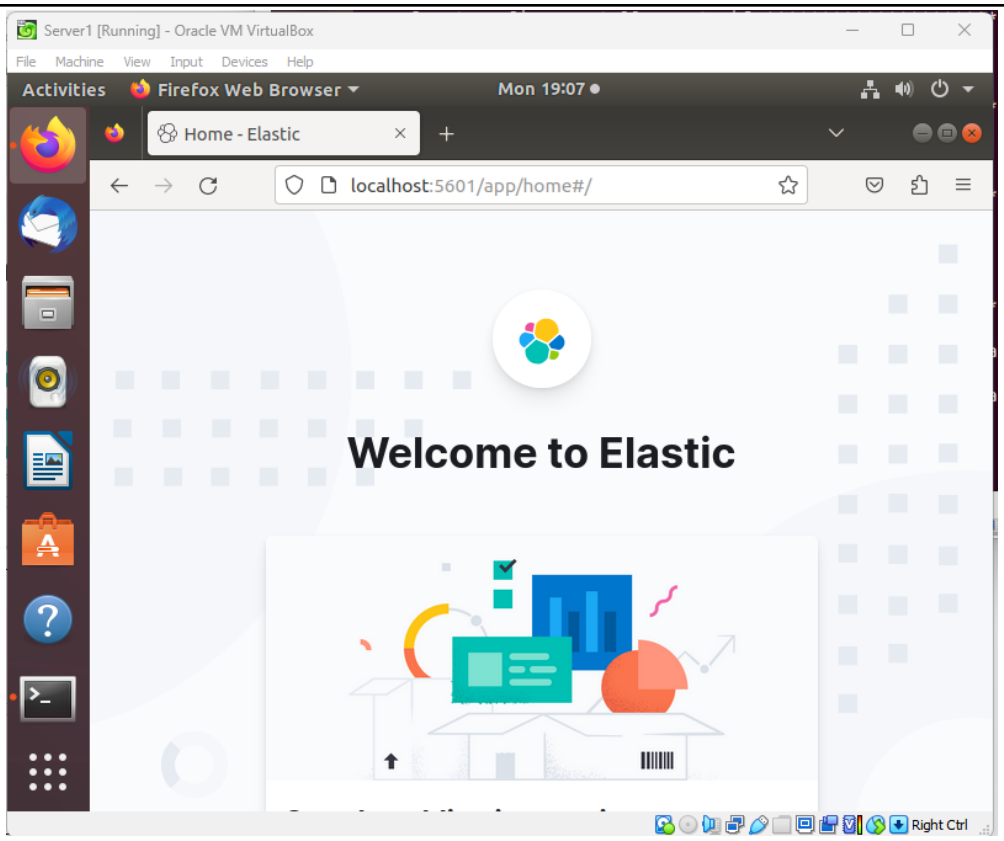


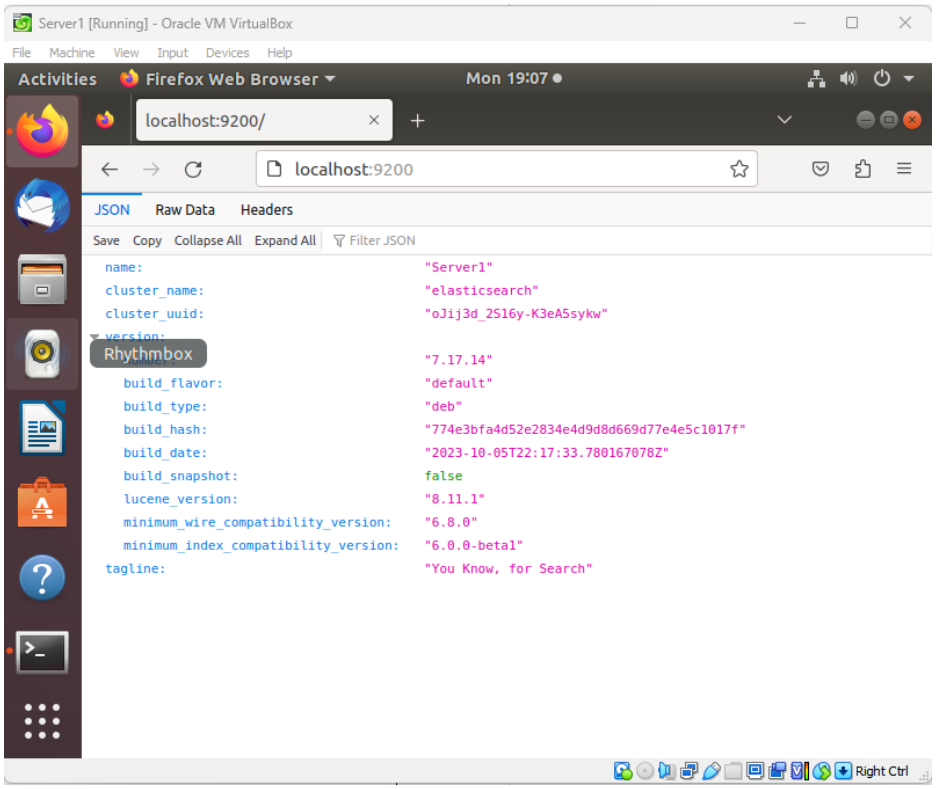
Step 10. We will now check the evidence of the successful installation using the firefox of the centos and ubuntu. To check if we have the successfully install the packages we will use the command “localhost:5601” it should redirect to

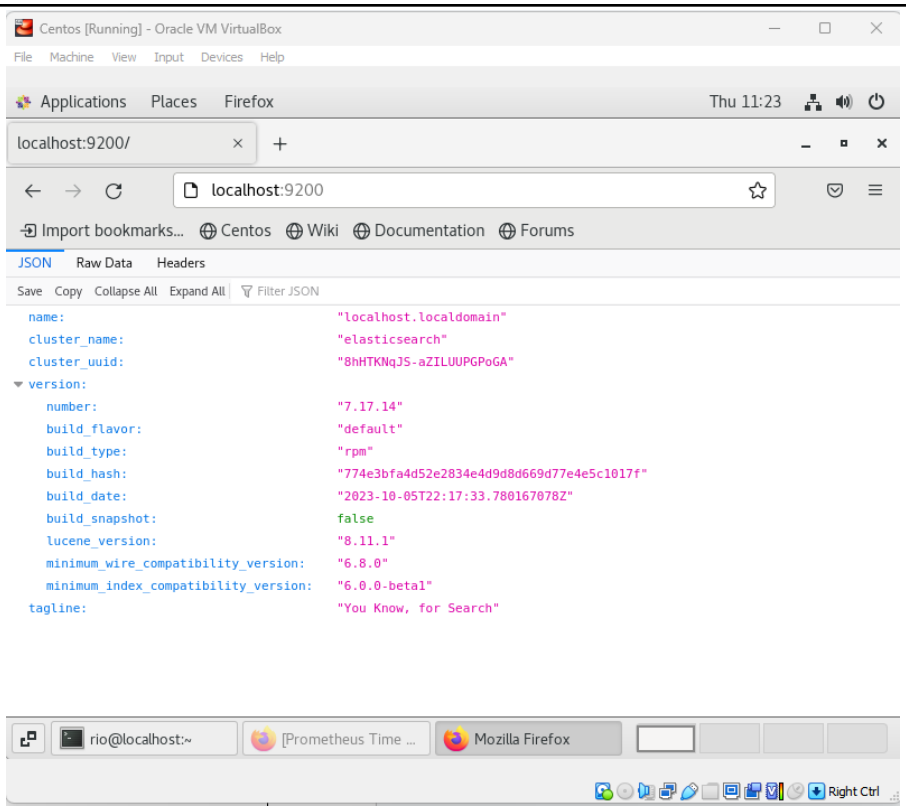
Output:

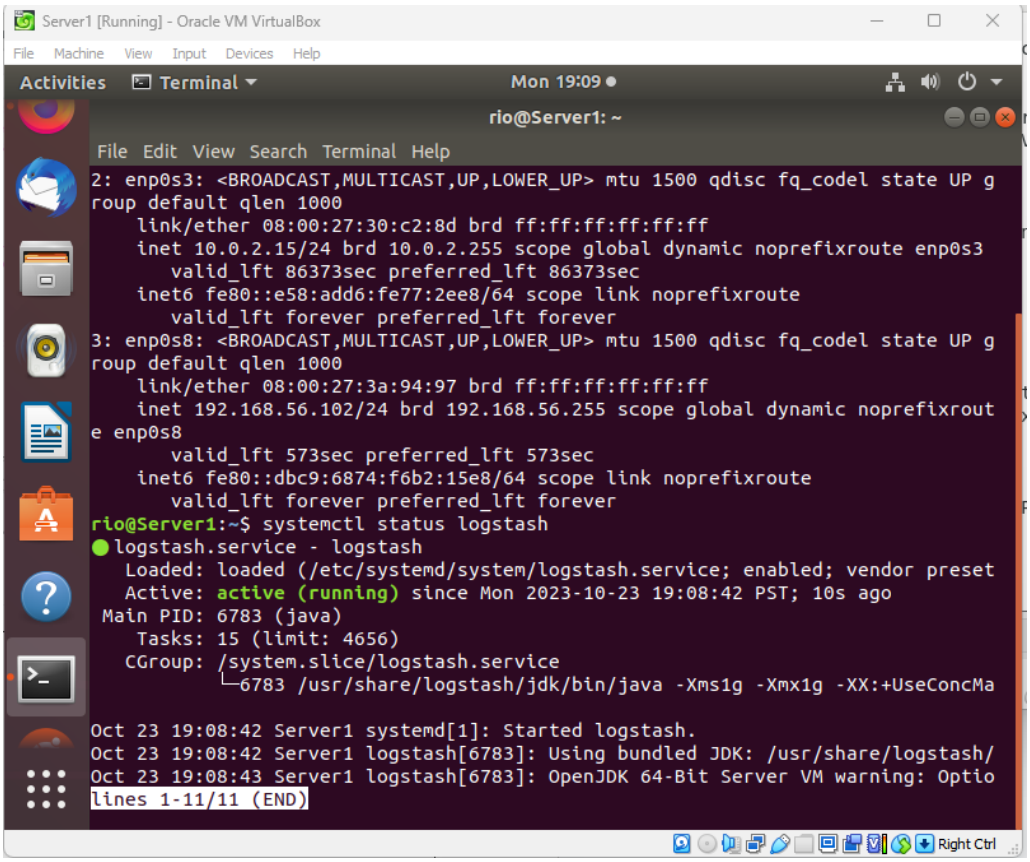
```
[rio@localhost ~]$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabl
ed)
   Active: active (running) since Thu 2023-10-12 11:20:10 EDT; 8s ago
 Main PID: 28103 (java)
    Tasks: 15
   CGroup: /system.slice/logstash.service
           └─28103 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSw...

Oct 12 11:20:10 localhost.localdomain systemd[1]: Started logstash.
Oct 12 11:20:10 localhost.localdomain logstash[28103]: Using bundled JDK: /usr/shar...k
Oct 12 11:20:10 localhost.localdomain logstash[28103]: OpenJDK 64-Bit Server VM war....
Hint: Some lines were ellipsized, use -l to show in full.
[rio@localhost ~]$
```




Server1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Mon 19:07
Home - Elastic
localhost:5601/app/home#/
Welcome to Elastic
Right Ctrl


Server1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Mon 19:07
localhost:9200/
localhost:9200
JSON
Raw Data
Headers
Save Copy Collapse All Expand All
Filter JSON
name: "Server1"
cluster_name: "elasticsearch"
cluster_uuid: "oJij3d_2S16y-K3eA5sykw"
version:
Rhythmbox
"7.17.14"
build_flavor: "default"
build_type: "deb"
build_hash: "774e3bfa4d52e2834e4d9d8d669d77e4e5c1017f"
build_date: "2023-10-05T22:17:33.780167078Z"
build_snapshot: false
lucene_version: "8.11.1"
minimum_wire_compatibility_version: "6.8.0"
minimum_index_compatibility_version: "6.0.0-beta1"
tagline: "You Know, for Search"
Right Ctrl


Centos [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Firefox
Thu 11:23
localhost:9200/
localhost:9200
Import bookmarks... Centos Wiki Documentation Forums
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
name: "localhost.localdomain"
cluster_name: "elasticsearch"
cluster_uuid: "8hHTKNqJS-aZILUUPGPoGA"
version:
number: "7.17.14"
build_flavor: "default"
build_type: "rpm"
build_hash: "774e3bfa4d52e2834e4d9d8d669d77e4e5c1017f"
build_date: "2023-10-05T22:17:33.780167078Z"
build_snapshot: false
lucene_version: "8.11.1"
minimum_wire_compatibility_version: "6.8.0"
minimum_index_compatibility_version: "6.0.0-beta1"
tagline: "You Know, for Search"
rio@localhost:~
[Prometheus Time ...
Mozilla Firefox
Right Ctrl


Server1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Mon 19:09
rio@Server1: ~
File Edit View Search Terminal Help
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:30:c2:8d brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
valid_lft 86373sec preferred_lft 86373sec
inet6 fe80::e58:add6:fe77:2ee8/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:3a:94:97 brd ff:ff:ff:ff:ff:ff
inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s8
valid_lft 573sec preferred_lft 573sec
inet6 fe80::dbc9:6874:f6b2:15e8/64 scope link noprefixroute
valid_lft forever preferred_lft forever
rio@Server1:~$ systemctl status logstash
● logstash.service - logstash
Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset
Active: active (running) since Mon 2023-10-23 19:08:42 PST; 10s ago
Main PID: 6783 (java)
Tasks: 15 (limit: 4656)
CGroup: /system.slice/logstash.service
└─6783 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMa
Oct 23 19:08:42 Server1 systemd[1]: Started logstash.
Oct 23 19:08:42 Server1 logstash[6783]: Using bundled JDK: /usr/share/logstash/
Oct 23 19:08:43 Server1 logstash[6783]: OpenJDK 64-Bit Server VM warning: Optio
lines 1-11/11 (END)
Right Ctrl

Server1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 19:10

rio@Server1: ~

File Edit View Search Terminal Help

```
       valid_lft forever preferred_lft forever
rio@Server1:~$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset
   Active: active (running) since Mon 2023-10-23 19:08:42 PST; 10s ago
 Main PID: 6783 (java)
    Tasks: 15 (limit: 4656)
   CGroup: /system.slice/logstash.service
           └─6783 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMa

Oct 23 19:08:42 Server1 systemd[1]: Started logstash.
Oct 23 19:08:42 Server1 logstash[6783]: Using bundled JDK: /usr/share/logstash/
Oct 23 19:08:43 Server1 logstash[6783]: OpenJDK 64-Bit Server VM warning: Optio

[1]+  Stopped                 systemctl status logstash
rio@Server1:~$ systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset:
   Active: active (running) since Mon 2023-10-23 18:47:39 PST; 22min ago
     Docs: https://www.elastic.co
 Main PID: 2440 (node)
    Tasks: 11 (limit: 4656)
   CGroup: /system.slice/kibana.service
           └─2440 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/

Oct 23 18:47:39 Server1 systemd[1]: Started Kibana.
Oct 23 18:47:39 Server1 kibana[2440]: Kibana is currently running with legacy O
lines 1-11/11 (END)
```

Right Ctrl

Server1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Mon 19:10

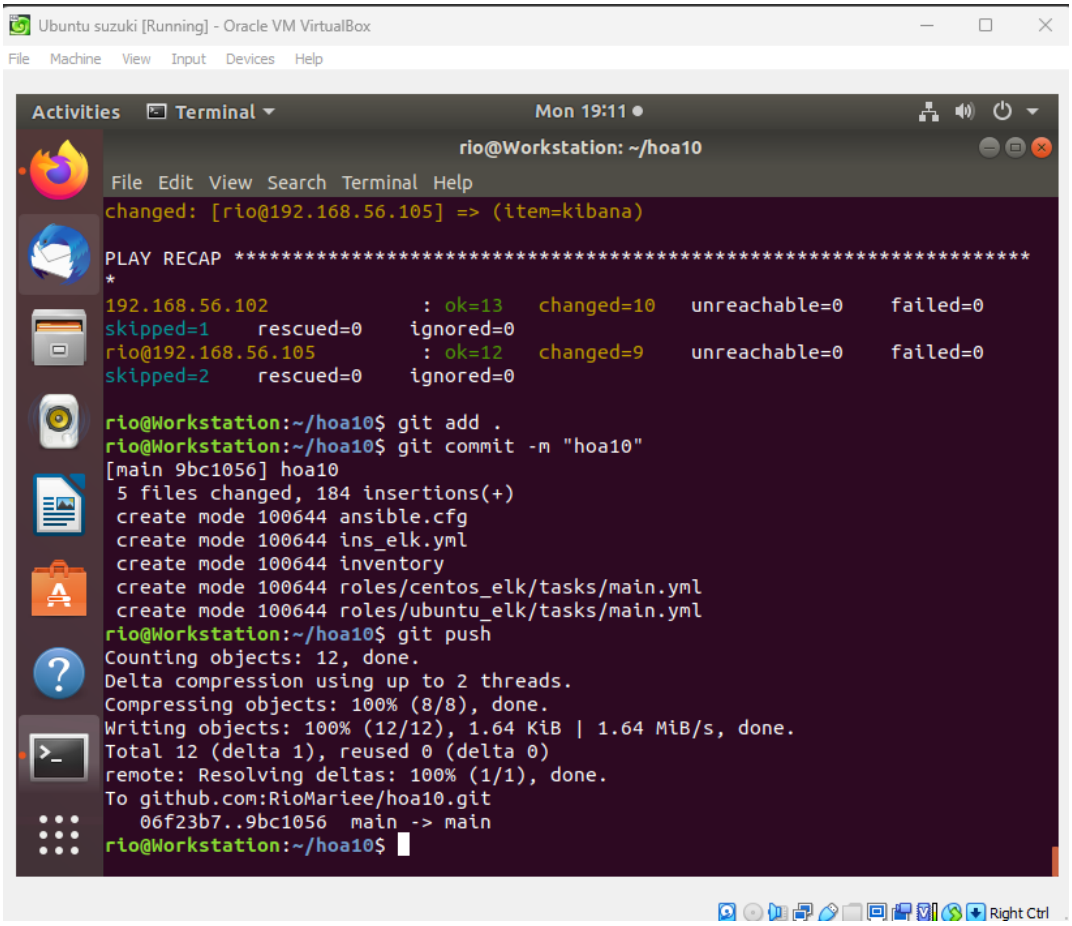
rio@Server1: ~

File Edit View Search Terminal Help

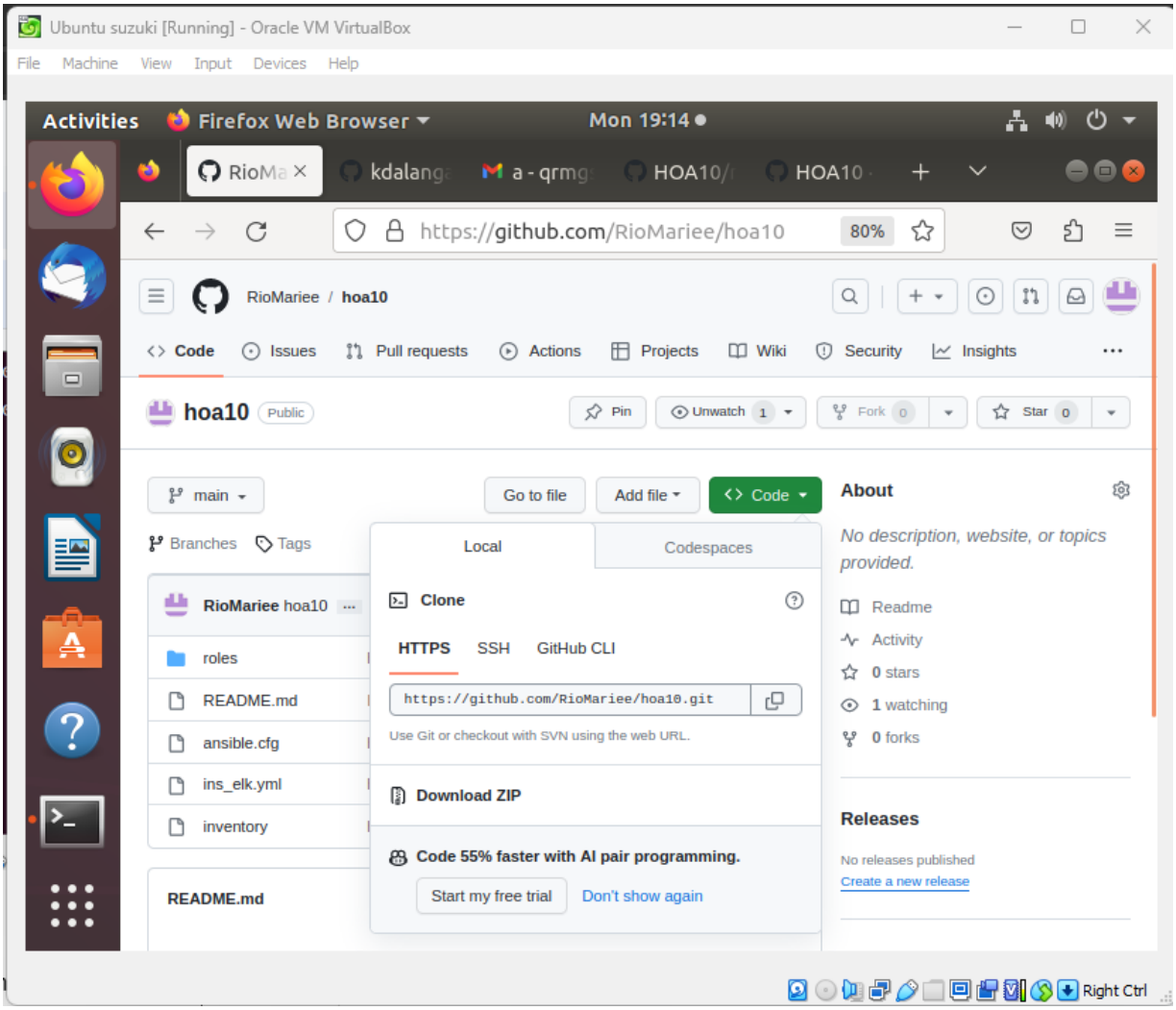
```
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset:
   Active: active (running) since Mon 2023-10-23 18:47:39 PST; 22min ago
     Docs: https://www.elastic.co
 Main PID: 2440 (node)
    Tasks: 11 (limit: 4656)
   CGroup: /system.slice/kibana.service
           └─2440 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/

Oct 23 18:47:39 Server1 systemd[1]: Started Kibana.
Oct 23 18:47:39 Server1 kibana[2440]: Kibana is currently running with legacy O
lines 1-11/11 (END)
[2]+  Stopped                 systemctl status kibana
rio@Server1:~$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vend
   Active: active (running) since Mon 2023-10-23 18:47:37 PST; 22min ago
     Docs: https://www.elastic.co
 Main PID: 2095 (java)
    Tasks: 65 (limit: 4656)
   CGroup: /system.slice/elasticsearch.service
           ├─2095 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.netwo
           └─2302 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86

Oct 23 18:47:13 Server1 systemd[1]: Starting Elasticsearch...
Oct 23 18:47:18 Server1 systemd-entrypoint[2095]: Oct 23, 2023 6:47:18 PM sun.u
Oct 23 18:47:18 Server1 systemd-entrypoint[2095]: WARNING: COMPAT locale provid
Oct 23 18:47:37 Server1 systemd[1]: Started Elasticsearch.
lines 1-14/14 (END)
```

Right Ctrl

Step 11. After processing the ins_elk we will now commit our repository so that the code will be uploaded and updated in the github. The command we will use is “git add .” “git commit -m"hoa10 " and "git push” to upload the latest version of the repository.



Step 12. We will get our repository link and paste it here. To get the repository link go to github.com and click the repository you want to have the link in this case we will choose the hoa10 repository. Copy the http link and paste it here in the document.



Github repository link: https://github.com/RioMariee/hoa10.git

Reflections:

Answer the following:

1. What are the benefits of having a log monitoring tool?
   - Log monitoring tools bring a lot of benefits for organizations in keeping their IT systems secure. These tools secure by spotting and tackling potential cyber threats quickly. They also help in making sure the systems run smoothly and don't crash. In addition, they help keep everything legal by keeping good

records. Also, they don't just fix problems when they pop up, they stop problems from happening in the first place, which is a good practice of prevention. They're also really good at making sure we don't waste our money and tech resources. That's super important for being efficient and saving cash. Also, a log monitoring tool keeps an eye on what people are doing on the network. And if something bad happens, they put up a warning. So, these tools aren't just helpful; they're like our secret weapon for managing in the IT world. They make sure things run well, don't break the rules, and save us time and money.

Conclusions:

To conclude while figuring out how to set up and run the log-monitoring tools using Ansible. It is a super efficient package. This makes our network safe but also helps us to check all those log files. Also, it makes looking way easier and efficient which makes things easier for us. It also helps the network security to be more safer and you can get important log files from the monitoring tool we installed.

Assessment Rubrics

Rubric for SO 7

Criteria	Ratings						Pts
SO 7 PI 1 Acquire and apply new knowledge from outside sources threshold: 4.8 pts	6 pts Excellent | Educational interests and pursuits exist and flourish outside classroom requirements,knowledge and/or experiences are pursued independently and applies knowledge learned into practice	5 pts Good | Educational interests and pursuits exist and flourish outside classroom requirements,knowledge and/or experiences are pursued independently	4 pts Satisfactory | Look beyond classroom requirements, showing interest in pursuing knowledge independently	3 pts Unsatisfactory | Begins to look beyond classroom requirements, showing interest in pursuing knowledge independently	2 pts Poor | Relies on classroom instruction only	1 pts Very Poor | No initiative or interest in acquiring new knowledge	6 pts
SO 7 PI 2 Learn independently. threshold: 4.8 pts	6 pts Excellent | Completes an assigned task independently and practices continuous improvement	5 pts Good | Completes an assigned task without supervision or guidance	4 pts Satisfactory | Requires minimal guidance to complete an assigned task	3 pts Unsatisfactory | Requires detailed or step-by-step instructions to complete a task	2 pts Poor | Shows little interest to complete a task independently	1 pts Very Poor | No interest to complete a task independently	6 pts
SO 7 PI 3 Critical thinking in the broadest context of technological change threshold: 4.8 pts	6 pts Excellent | Synthesizes and integrates information from a variety of sources; formulates a clear and precise perspective; draws appropriate conclusions	5 pts Good | Evaluate information from a variety of sources; formulates a clear and precise perspective.	4 pts Satisfactory | Analyze information from a variety of sources; formulates a clear and precise perspective.	3 pts Unsatisfactory | Apply the gathered information to formulate the problem	2 pts Poor | Gather and summarized the information from a variety of sources but failed to formulate the problem	1 pts Very Poor | Gather information from a variety of sources	6 pts
SO 7 PI 4 Creativity and adaptability to new and emerging technologies threshold: 4.8 pts	6 pts Excellent | Ideas are combined in original and creative ways in line with the new and emerging technology trends to solve a problem or address an issue.	5 pts Good | Ideas are creative and adapt the new knowledge to solve a problem or address an issue	4 pts Satisfactory | Ideas are creative in solving a problem, or address an issue	3 pts Unsatisfactory | Shows some creative ways to solve the problem	2 pts Poor | Shows initiative and attempt to develop creative ideas to solve the problem	1 pts Very Poor | Ideas are copied or restated from the sources consulted	6 pts
							Total Points: 24