Name: Repani, Justin Jello J.	**Date Performed:** October 23, 2023
Course/Section: CPE31S6 - CPE232	**Date Submitted:** October 23, 2023
Instructor: Dr. Jonathan V. Taylar	**Semester and SY:** 1st Sem - SY: 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.

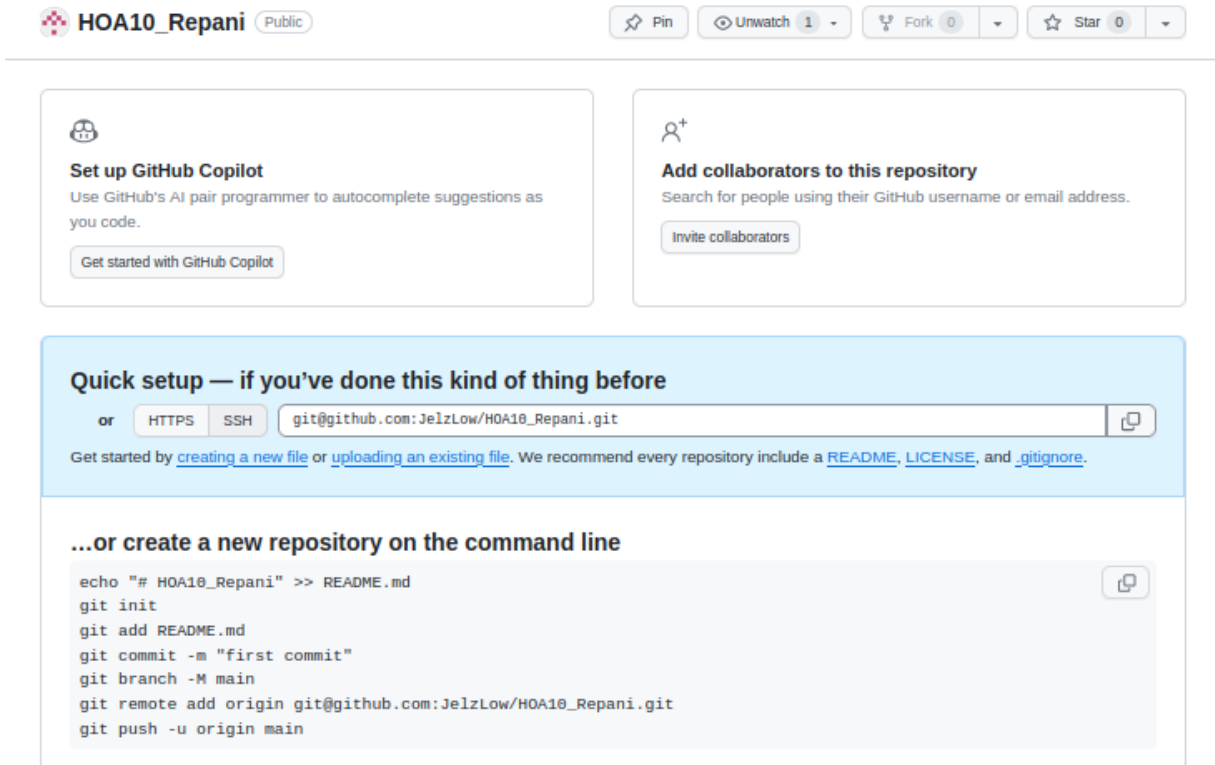
Source: https://www.graylog.org/products/open-source

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 step is to create a new git repository for activity 10. And then clone this into the workstation




```
jello@workstation:~$ git clone git@github.com:JelzLow/HOA10_Repani.git
Cloning into 'HOA10_Repani'...
warning: You appear to have cloned an empty repository.
jello@workstation:~$ ls
CPE232_hoa6    Downloads         HOA8_Repani  Public             Videos
CPE232_Repani  examples.desktop  HOA9_Repani  Repani_PrelimExam
Desktop        HOA10_Repani      Music        Templates
Documents      HOA7_Repani       Pictures     token.txt
jello@workstation:~$ cd HOA10_Repani
jello@workstation:~/HOA10_Repani$
```

Next step is to copy the ansible.cfg and inventory files from the previous activity and create a roles directory that contains centos and ubuntu each with their own tasks and

main.yml

```
jello@workstation:~/HOA10_Repani$ tree
.
├── ansible.cfg
├── inventory
└── roles
    ├── centos
    │   └── tasks
    │       └── main.yml
    └── ubuntu
        └── tasks
            └── main.yml

5 directories, 4 files
```

The elasticstack.yml file is then created. This will contain the playbook commands that will initialize and update the servers and as well as call on to the main.yml playbooks in their respective roles.

```
jello@workstation: ~/HOA10_Repani
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                    elasticstack.yml                    Modified

- 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
```

Open the the main.yml in the ubuntu role using the command sudo nano main.yml in the roles/ubuntu/tasks directory. The playbook contains the necessary commands to install all the prerequisites to make the Elastic Stack work on Ubuntu. After this part it will then add the APT repository key and apt repository of Elasticsearch before finally installing Elasticsearch and Kibana. Once installed these processes are enabled and

started.

```
jello@workstation: ~/HOA10_Repani
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                    ./roles/ubuntu/tasks/main.yml

---
    - 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
      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

    - 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

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

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

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

The main.yml of the centos role is also created. It contains the same flow of functions but some of the syntaxes for the functions are changed to fit CentOS.

```
jello@workstation: ~/HOA10_Repani
File  Edit  View  Search  Terminal  Help
 GNU nano 2.9.3                    ./roles/centos/tasks/main.yml

---
  - 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 packages
        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
    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
```

```
      enabled: yes
      state: started
    become: yes

  - name: Install Logstash
    yum:
      name: logstash
      state: present
    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:
      name: "{{ item }}"
      state: restarted
    loop:
      - elasticsearch
      - kibana
```

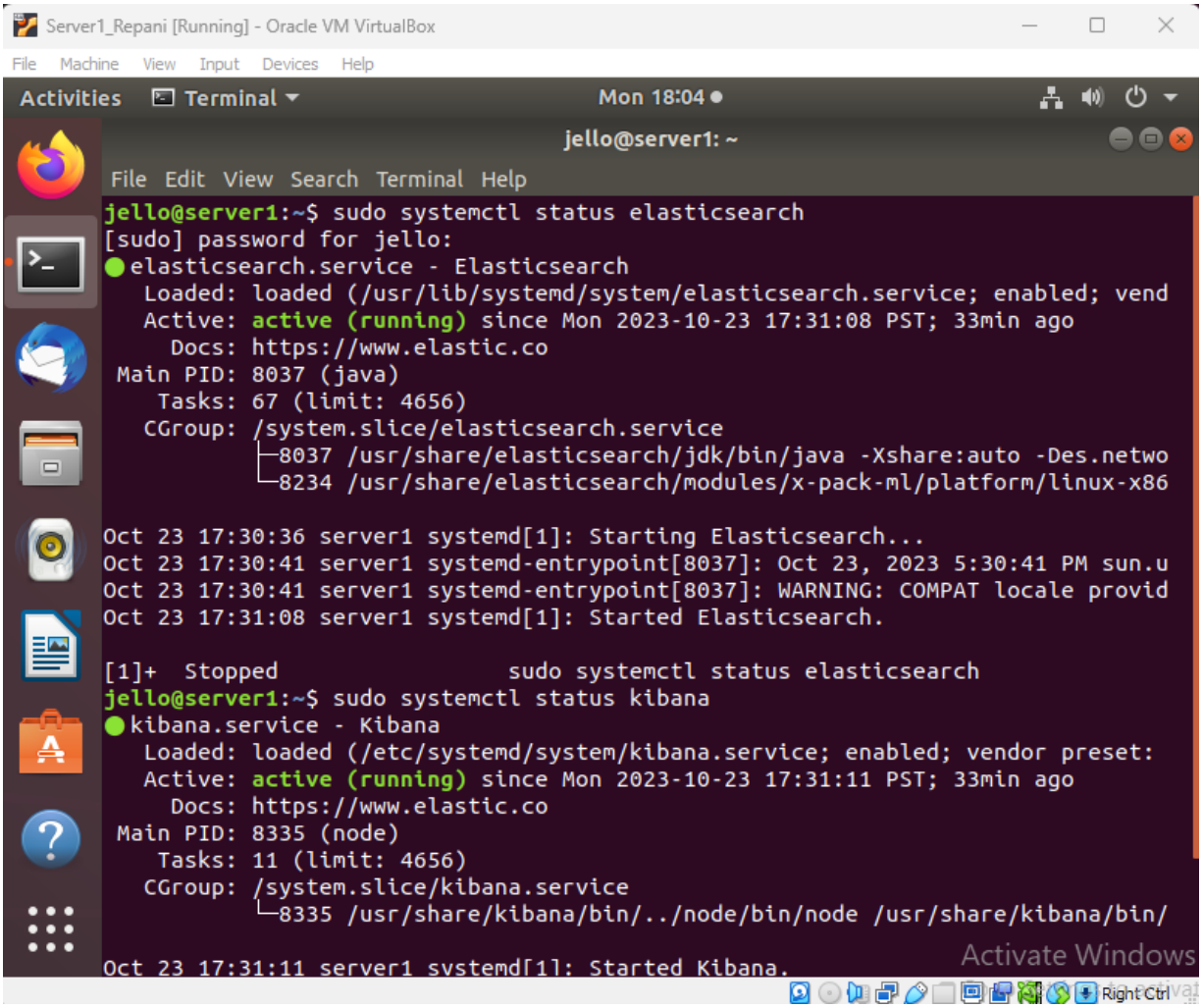
Running the elasticstack.yml playbook successfully

```
jello@workstation: ~/HOA10_Repani
File  Edit  View  Search  Terminal  Help
jello@workstation:~/HOA10_Repani$ ansible-playbook --ask-become-pass elasticstack.yml
BECOME password:

PLAY [all] *********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.56.102]
ok: [192.168.56.104]

TASK [install updates (CentOS)] ************************************************
skipping: [192.168.56.102]
skipping: [192.168.56.104]

TASK [install updates (Ubuntu)] ************************************************
skipping: [192.168.56.104]
ok: [192.168.56.102]

PLAY [ubuntu] ******************************************************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.56.102]

TASK [ubuntu : Install prerequisites] ******************************************
changed: [192.168.56.102]

TASK [ubuntu : Add Elasticsearch APT repository key] ***************************
changed: [192.168.56.102]

TASK [ubuntu : Add Elasticsearch APT repository] *******************************
changed: [192.168.56.102]

TASK [ubuntu : Install Elasticsearch] ******************************************
changed: [192.168.56.102]
```

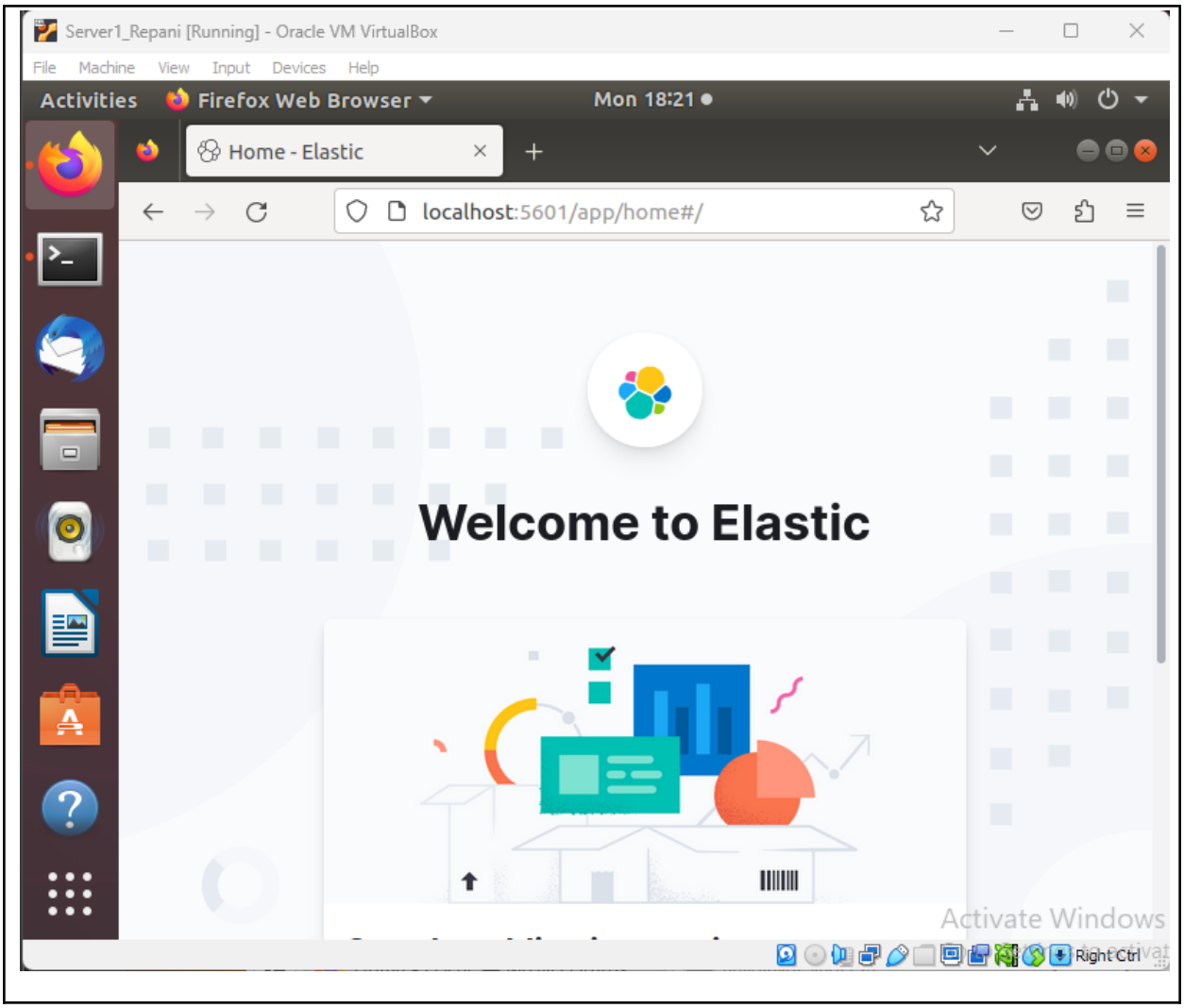
```
TASK [ubuntu : Enable and start Elasticsearch service] *************************
changed: [192.168.56.102]

TASK [ubuntu : Install Kibana] *************************************************
changed: [192.168.56.102]

TASK [ubuntu : Enable and start Kibana service] ********************************
changed: [192.168.56.102]

TASK [ubuntu : Install Logstash] ***********************************************
changed: [192.168.56.102]

TASK [ubuntu : Enable and start Logstash service] ******************************
changed: [192.168.56.102]

TASK [ubuntu : Restart Elasticsearch and Kibana] *******************************
changed: [192.168.56.102] => (item=elasticsearch)
changed: [192.168.56.102] => (item=kibana)

PLAY [centos] ******************************************************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.56.104]

TASK [centos : Install prerequisites] ******************************************
ok: [192.168.56.104]

TASK [centos : Add Elasticsearch RPM repository] *******************************
changed: [192.168.56.104]

TASK [centos : Add Elasticsearch YUM repository] *******************************
changed: [192.168.56.104]
```

```
TASK [centos : Install Elasticsearch] ******************************************
changed: [192.168.56.104]

TASK [centos : Enable and start Elasticsearch service] *************************
changed: [192.168.56.104]

TASK [centos : Install Kibana] *************************************************
changed: [192.168.56.104]

TASK [centos : Enable and start Kibana service] ********************************
changed: [192.168.56.104]

TASK [centos : Install Logstash] ***********************************************
changed: [192.168.56.104]

TASK [centos : Enable and start Logstash service] ******************************
changed: [192.168.56.104]

TASK [centos : Restart Elasticsearch and Kibana] *******************************
changed: [192.168.56.104] => (item=elasticsearch)
changed: [192.168.56.104] => (item=kibana)

PLAY RECAP *********************************************************************
192.168.56.102             : ok=13   changed=10   unreachable=0    failed=0    skipped=1    rescued=0
   ignored=0
192.168.56.104             : ok=12   changed=9    unreachable=0    failed=0    skipped=2    rescued=0
   ignored=0
```

Proof of installation



```
jello@server1:~$ sudo systemctl status logstash
[sudo] password for jello:
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset
   Active: active (running) since Mon 2023-10-23 17:57:45 PST; 26min ago
 Main PID: 14129 (java)
    Tasks: 22 (limit: 4656)
   CGroup: /system.slice/logstash.service
           └─14129 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcM

Oct 23 17:57:45 server1 systemd[1]: Started logstash.
Oct 23 17:57:45 server1 logstash[14129]: Using bundled JDK: /usr/share/logstash
Oct 23 17:57:45 server1 logstash[14129]: OpenJDK 64-Bit Server VM warning: Opti
Oct 23 17:57:57 server1 logstash[14129]: Sending Logstash logs to /var/log/logs
Oct 23 17:57:57 server1 logstash[14129]: [2023-10-23T17:57:57,973][INFO ][logst
Oct 23 17:57:57 server1 logstash[14129]: [2023-10-23T17:57:57,978][INFO ][logst
Oct 23 17:57:58 server1 logstash[14129]: [2023-10-23T17:57:58,015][INFO ][logst
Oct 23 17:57:59 server1 logstash[14129]: [2023-10-23T17:57:59,273][INFO ][logst
Oct 23 17:57:59 server1 logstash[14129]: [2023-10-23T17:57:59,281][ERROR][logst
Oct 23 17:57:59 server1 logstash[14129]: [2023-10-23T17:57:59,315][INFO ][logst
lines 1-18/18 (END)
[3]+  Stopped                 sudo systemctl status logstash
jello@server1:~$
```


Server1_Repani [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Mon 18:21
Home - Elastic
localhost:5601/app/home#/
Welcome to Elastic
Activate Windows
Right Ctrl

CentOS_Repani [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places Terminal Mon 18:05

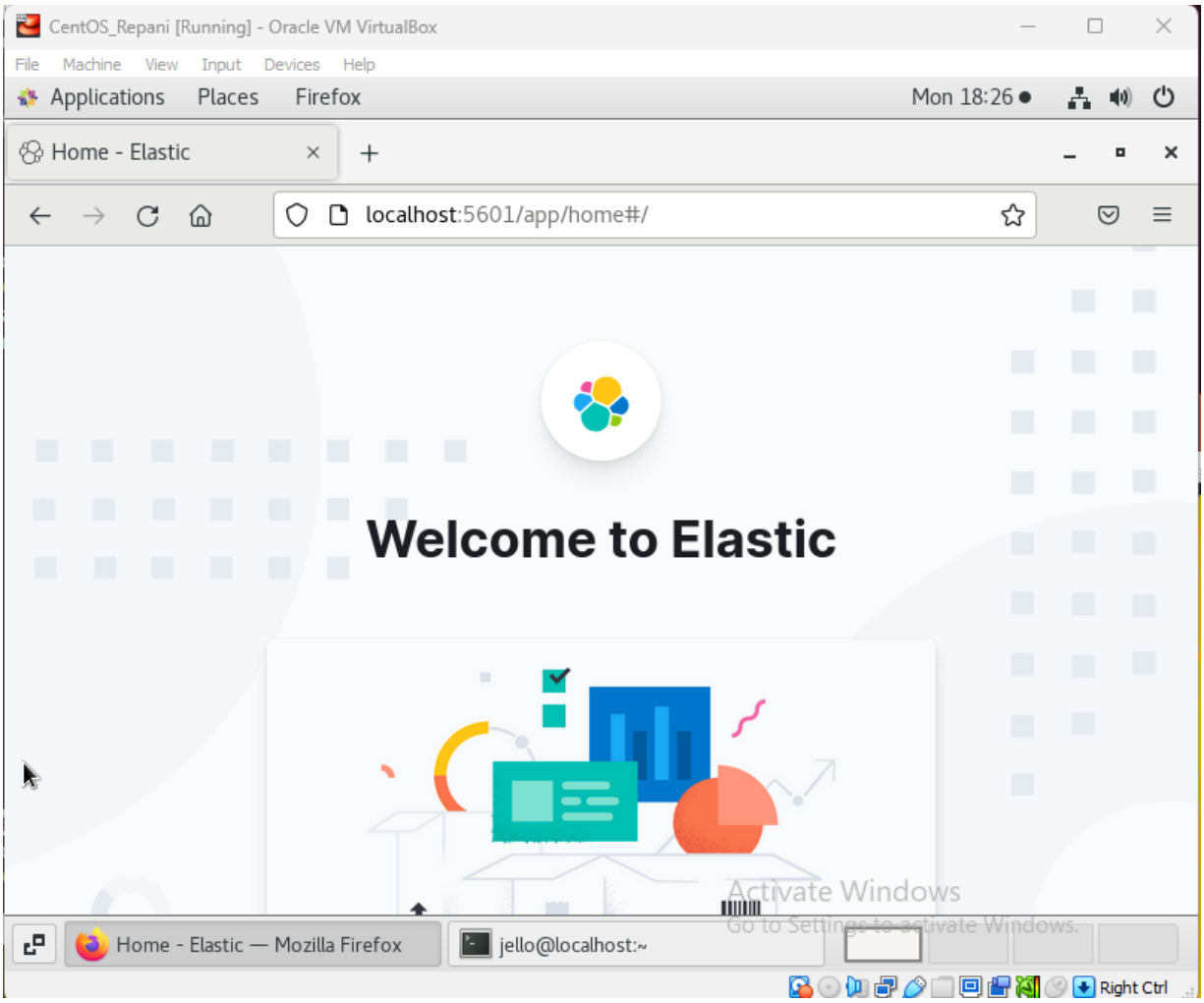
jello@localhost:~

File Edit View Search Terminal Help

```
[jello@localhost ~]$ sudo systemctl status elasticsearch
[sudo] password for jello:
Sorry, try again.
[sudo] password for jello:
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor prese
t: disabled)
   Active: active (running) since Mon 2023-10-23 17:34:44 PST; 30min ago
     Docs: https://www.elastic.co
 Main PID: 6775 (java)
    Tasks: 67
   CGroup: /system.slice/elasticsearch.service
           ├─6775 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkadd...
           └─6966 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/b...

Oct 23 17:34:22 localhost.localdomain systemd[1]: Starting Elasticsearch...
Oct 23 17:34:27 localhost.localdomain systemd-entrypoint[6775]: Oct 23, 2023 5:34:27...
Oct 23 17:34:27 localhost.localdomain systemd-entrypoint[6775]: WARNING: COMPAT loca...
Oct 23 17:34:44 localhost.localdomain systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
[jello@localhost ~]$ sudo systemctl status kibana
```

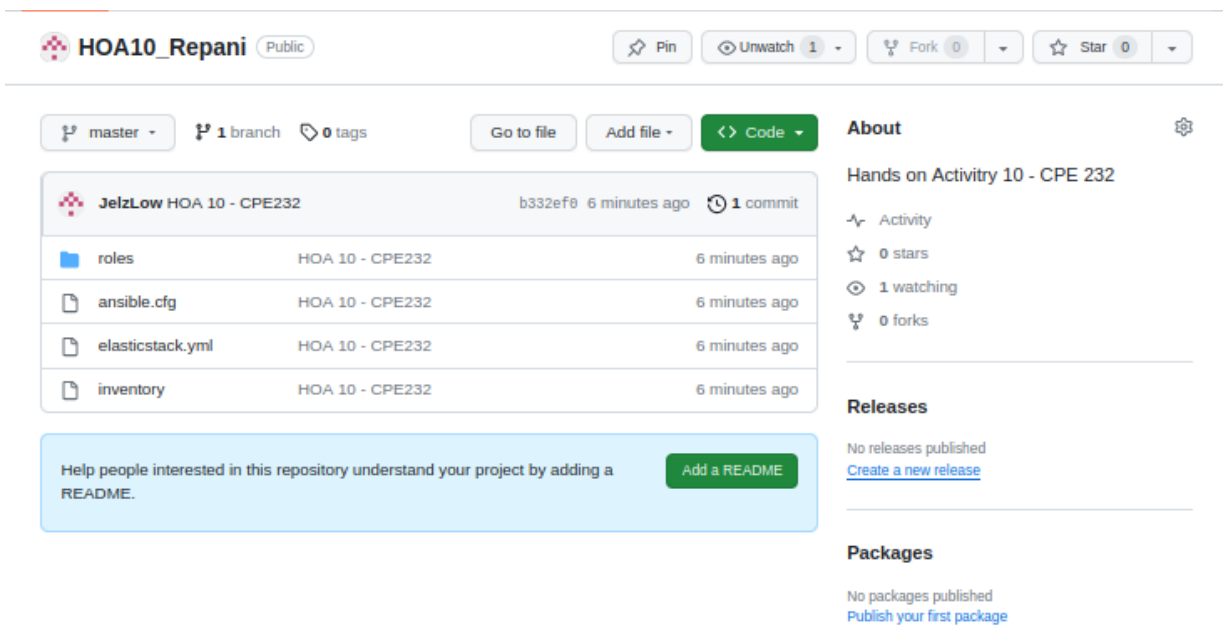
```
[jello@localhost ~]$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled
)
   Active: active (running) since Mon 2023-10-23 17:34:48 PST; 30min ago
     Docs: https://www.elastic.co
 Main PID: 7131 (node)
    Tasks: 11
   CGroup: /system.slice/kibana.service
           └─7131 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../sr...

Oct 23 17:34:48 localhost.localdomain systemd[1]: Stopped Kibana.
Oct 23 17:34:48 localhost.localdomain systemd[1]: Started Kibana.
Oct 23 17:34:49 localhost.localdomain kibana[7131]: Kibana is currently running wit...r
Hint: Some lines were ellipsized, use -l to show in full.
[jello@localhost ~]$
```

```
[jello@localhost ~]$ sudo systemctl status logstash
[sudo] password for jello:
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabl
ed)
   Active: active (running) since Mon 2023-10-23 18:24:32 PST; 10s ago
 Main PID: 17818 (java)
    Tasks: 15
   CGroup: /system.slice/logstash.service
           └─17818 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSw...

Oct 23 18:24:32 localhost.localdomain systemd[1]: logstash.service holdoff time ove....
Oct 23 18:24:32 localhost.localdomain systemd[1]: Stopped logstash.
Oct 23 18:24:32 localhost.localdomain systemd[1]: Started logstash.
Oct 23 18:24:32 localhost.localdomain logstash[17818]: Using bundled JDK: /usr/shar...k
Oct 23 18:24:32 localhost.localdomain logstash[17818]: OpenJDK 64-Bit Server VM war....
Hint: Some lines were ellipsized, use -l to show in full.
[jello@localhost ~]$
```



Git synchronization

```
jello@workstation:~/HOA10_Repani$ git add *
jello@workstation:~/HOA10_Repani$ git commit -m "HOA 10 - CPE232"
[master (root-commit) b332ef0] HOA 10 - CPE232
 5 files changed, 182 insertions(+)
 create mode 100644 ansible.cfg
 create mode 100644 elasticstack.yml
 create mode 100644 inventory
 create mode 100644 roles/centos/tasks/main.yml
 create mode 100644 roles/ubuntu/tasks/main.yml
jello@workstation:~/HOA10_Repani$ git push origin
Counting objects: 12, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (8/8), done.
Writing objects: 100% (12/12), 1.59 KiB | 1.59 MiB/s, done.
Total 12 (delta 1), reused 0 (delta 0)
remote: Resolving deltas: 100% (1/1), done.
To github.com:JelzLow/HOA10_Repani.git
 * [new branch]      master -> master
jello@workstation:~/HOA10_Repani$
```



https://github.com/JelzLow/HOA10_Repani

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool?
   - The benefits of having a log monitoring tool is added security to the system. Log monitoring tools take a log of the different times a system is used or accessed and saves it. By having a copy of these logs can help provide an

additional layer of security to the servers and system and as well as helping with the troubleshooting of any errors that may arise thanks to the saved logs with the different time stamps.

Conclusions:

In this hands-on activity 10, the topic is about installing, configuring and managing log monitoring tools. From the discussion part of the activity I have learned about log monitoring tools which are important tools when managing servers in a system. There are two examples shown which are the Elastic Stack and the Gray Log. The task for this activity is to install and configure the Elastic Stack which contains Elasticsearch, Kibana, Beats, and Logstash. Using git and the ansible playbook with the roles, I was able to download both of these on the Ubuntu and CentOS systems. It is very confusing to start with because of all the different things you need to install along with its dependencies. Searching the internet for the guides and tutorials helped a lot in this activity because it showed the different steps and commands needed. I simply converted those into a playbook format.

Honor Pledge:

"I affirm that I have not given or received any unauthorized help on this assignment, and that this work is my own."