Name: Aducal, John Mark S.	**Date Performed: 10 / 26 / 2022**
Course/Section: CPE232 – CPE31S24	**Date Submitted: 10 / 28 / 2022**
Instructor: Engr. Jonathan V. Taylar	**Semester and SY: 1st Sem SY 2022-2023**

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.

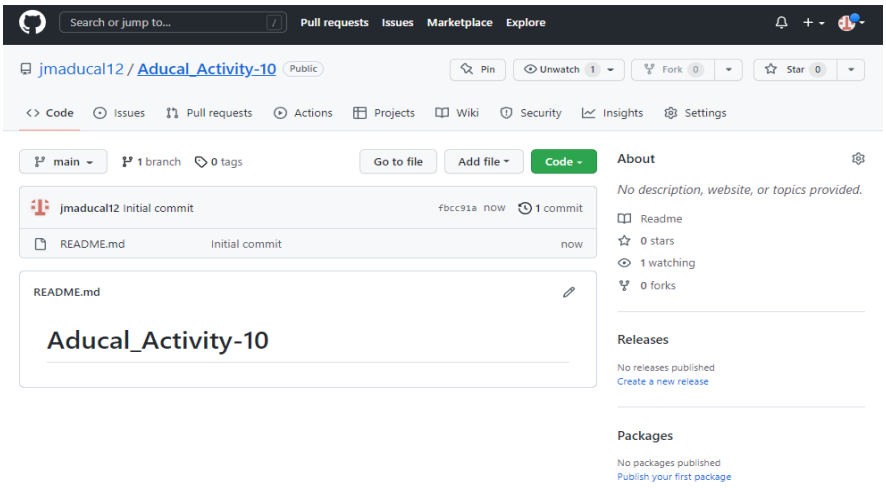
Source: https://www.graylog.org/products/open-source

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)

Task 1: Create a new repository in GitHub



I created a new repository named Aducal_Activity-10

```
jmaducal@workstation: ~
jmaducal@workstation:~$ git clone git@github.com:jmaducal12/Aducal_Activity-10.
git
Cloning into 'Aducal_Activity-10'...
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.
jmaducal@workstation:~$
```

I used git clone command to copy the new repository I have created into my workstation.

```
jmaducal@workstation: ~/Aducal_Activity-10
jmaducal@workstation:~$ git clone git@github.com:jmaducal12/Aducal_Activity-10.
git
Cloning into 'Aducal_Activity-10'...
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.
jmaducal@workstation:~$ ls
Act-4.1-CPE232_ADUCAL  CPE232_John-Mark-Aducal  Music      Templates
Aducal_Activity-10     Desktop                  Pictures   Videos
Aducal_Activity-8      Documents                Public
Aducal_Activity-9      Downloads                README.md
Aducal_PrelimExam      HOA4.1_CPE232_ADUCAL     snap
jmaducal@workstation:~$ cd Aducal_Activity-10
jmaducal@workstation:~/Aducal_Activity-10$
```

Now we can use the new repository we created earlier, using cd command to change directory into Aducal_Activity-10.

Task 2: Targeting Specific Nodes

```
jmaducal@workstation:~/Aducal_Activity-10$ nano inventory
jmaducal@workstation:~/Aducal_Activity-10$ nano ansible.cfg
```

I created new inventory and ansible.cfg file

```
jmaducal@workstation: ~/Aducal_Activity-10
  GNU nano 6.2                          inventory
[Web_server]
CentOS ansible_host=192.168.56.108

[Application_server]
server3 ansible_host=192.168.56.110
```

The new Inventory file contains the groups Web_server and Application_server together with the IP Addresses of Ubuntu server3 and CentOS.

```
jmaducal@workstation: ~/Aducal_Activity-10
  GNU nano 6.2                          ansible.cfg
[defaults]
inventory = inventory
host_key_checking = False

deprecation_warnings = False

remote_user = jmaducal
private_key_file = ~/.ssh/
```

The ansible.cfg file contains the ansible configurations need to administer the behavior of the task performed by control node used to manage the remote hosts or managed nodes.

Task 3: Create roles

```
jmaducal@workstation: ~/Aducal_Activity-10
jmaducal@workstation:~/Aducal_Activity-10$ nano ELKstack.yml
```

I create a new file name ELKstack.yml

```
jmaducal@workstation: ~/Aducal_Activity-10
  GNU nano 6.2                          ELKstack.yml
---

- hosts: all
  become: true
  pre_tasks:

  - name: install updates (CentOS)
    tags: always
    dnf:
      update_only: yes
      update_cache: yes
    when: ansible_distribution == "CentOS"

  - name: install updates (Ubuntu)
    tags: always
    apt:
      upgrade: dist
      update_cache: yes
    when: ansible_distribution == "Ubuntu"
```

```
- hosts: Web_server
  become: true
  roles:
    - Web_server

- hosts: Application_server
  become: true
  roles:
    - Application_server
```

Inside of ELKstack file, there are pre_tasks for installing updates for CentOS and Ubuntu and particular roles for Web_server and Application_server.

```
jmaducal@workstation: ~/Aducal_Activity-10/roles
jmaducal@workstation:~/Aducal_Activity-10$ mkdir roles
jmaducal@workstation:~/Aducal_Activity-10$ cd roles
jmaducal@workstation:~/Aducal_Activity-10/roles$ mkdir Web_server
jmaducal@workstation:~/Aducal_Activity-10/roles$ mkdir Application_server
jmaducal@workstation:~/Aducal_Activity-10/roles$ ls
Application_server  Web_server
jmaducal@workstation:~/Aducal_Activity-10/roles$ cd Web_server
jmaducal@workstation:~/Aducal_Activity-10/roles/Web_server$ mkdir tasks
jmaducal@workstation:~/Aducal_Activity-10/roles/Web_server$ cd tasks
jmaducal@workstation:~/Aducal_Activity-10/roles/Web_server/tasks$ nano main.yml
jmaducal@workstation:~/Aducal_Activity-10/roles/Web_server/tasks$ cd ..
jmaducal@workstation:~/Aducal_Activity-10/roles/Web_server$ cd ..
jmaducal@workstation:~/Aducal_Activity-10/roles$ cd Application_server
jmaducal@workstation:~/Aducal_Activity-10/roles/Application_server$ mkdir tasks
jmaducal@workstation:~/Aducal_Activity-10/roles/Application_server$ cd tasks
jmaducal@workstation:~/Aducal_Activity-10/roles/Application_server/tasks$ nano
main.yml
```

```
jmaducal@workstation:~/Aducal_Activity-10/roles$ tree
.
├── Application_server
│   └── tasks
│       └── main.yml
└── Web_server
    └── tasks
        └── main.yml

4 directories, 2 files
```

I create a new directory roles inside Aducal_Activity-10 directory. And then, Inside the roles directory, I created Web_server and Application_Server directory. Inside of both directories I create again new directory named tasks. Inside the directory tasks for both directories I created a file named main.yml

```
jmaducal@workstation: ~/Aducal_Activity-10/roles/Web_se...
GNU nano 6.2                                main.yml
- name: install Elastic stack on Ubuntu
  apt:
    name:
      - elasticsearch
      - kibana
      - logstash
    state: latest
    update_cache: yes
  when: ansible_distribution == "Ubuntu"

- name: install Elastic stack on CentOS
  dnf:
    name:
      - elasticsearch
      - kibana
      - logstash
    state: latest
    update_cache: yes
  when: ansible_distribution == "CentOS"
```

The contents of main.yml file inside of tasks of Web_server directory.

```
jmaducal@workstation: ~/Aducal_Activity-10/roles/Applicat...
GNU nano 6.2                                main.yml
- name: install Elastic stack on Ubuntu
  apt:
    name:
      - elasticsearch
      - kibana
      - logstash
    state: latest
    update_cache: yes
  when: ansible_distribution == "Ubuntu"

- name: install Elastic stack on CentOS
  dnf:
    name:
      - elasticsearch
      - kibana
      - logstash
    state: latest
    update_cache: yes
  when: ansible_distribution == "CentOS"
```

The contents of main.yml file inside of tasks of Application_server directory.

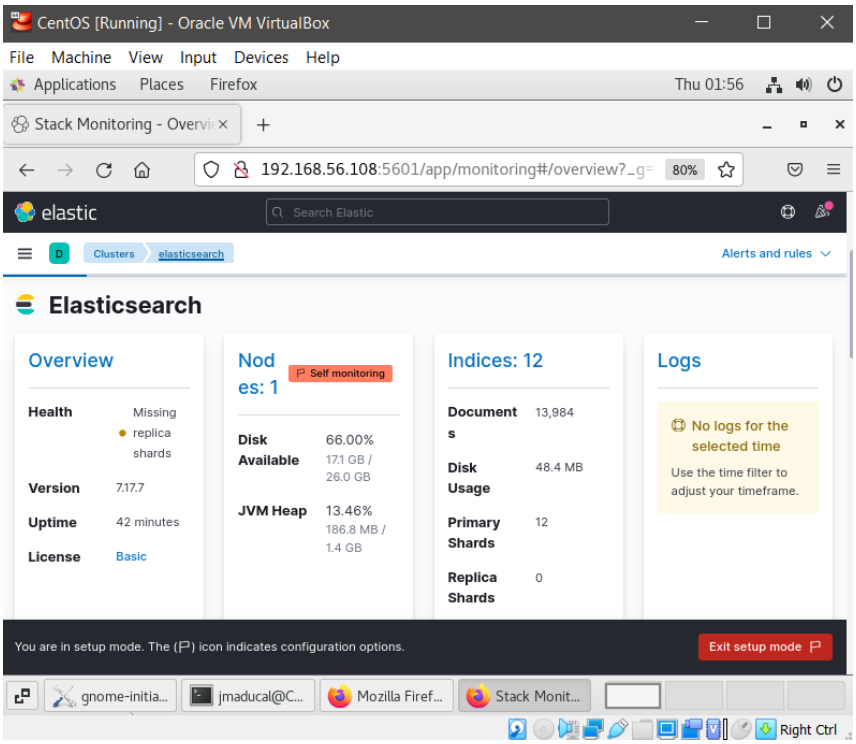
```
jmaducal@workstation: ~/Aducal_Activity-10
jmaducal@workstation:~/Aducal_Activity-10$ ansible-playbook --ask-become-pass E
LKstack.yml
BECOME password:

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

TASK [Gathering Facts] ********************************************************
*
ok: [CentOS]
ok: [server3]

TASK [install updates (CentOS)] ***********************************************
*
skipping: [server3]
ok: [CentOS]

TASK [install updates (Ubuntu)] ***********************************************
*
skipping: [CentOS]
ok: [server3]
```

```
PLAY [Web_server] *************************************************************
*

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

TASK [Web_server : install Elastic stack on Ubuntu] ***************************
*
skipping: [CentOS]

TASK [Web_server : install Elastic stack on CentOS] ***************************
*
changed: [CentOS]
```

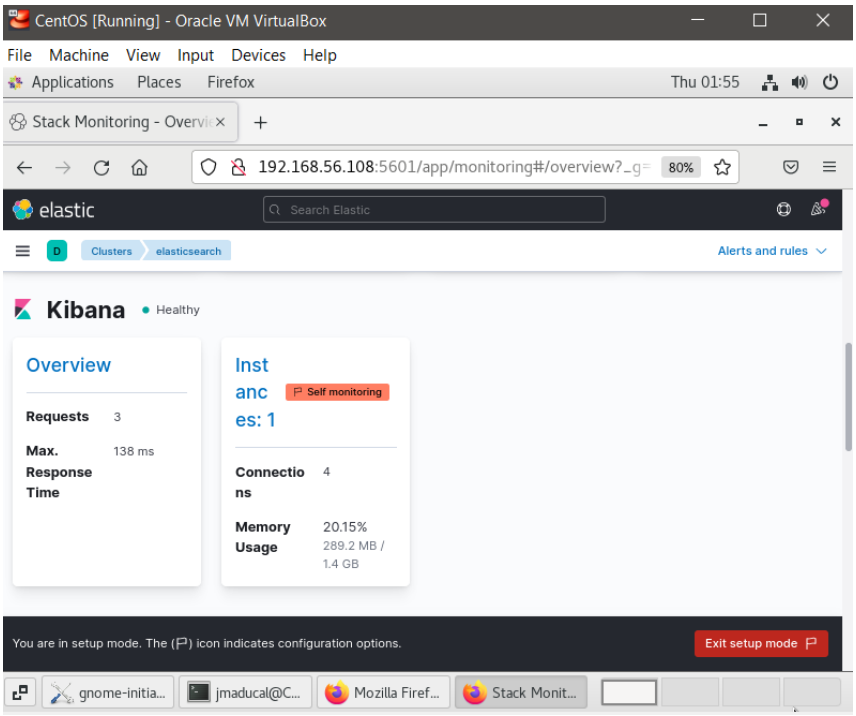
```
PLAY [Application_server] *****************************************************
*

TASK [Gathering Facts] ********************************************************
*
ok: [server3]

TASK [Application_server : install Elastic stack on Ubuntu] *******************
*
changed: [server3]

TASK [Application_server : install Elastic stack on CentOS] *******************
*
skipping: [server3]

PLAY RECAP ********************************************************************
*
CentOS                     : ok=4    changed=1    unreachable=0    failed=0
skipped=2    rescued=0    ignored=0
server3                    : ok=4    changed=1    unreachable=0    failed=0
skipped=2    rescued=0    ignored=0

jmaducal@workstation:~/Aducal_Activity-10$
```

After executing ELKstack.yml, I have notice that roles (Web_server and Application_server) plays the tasks in the main.yml file of Installing the Elastic stacks to remote servers.

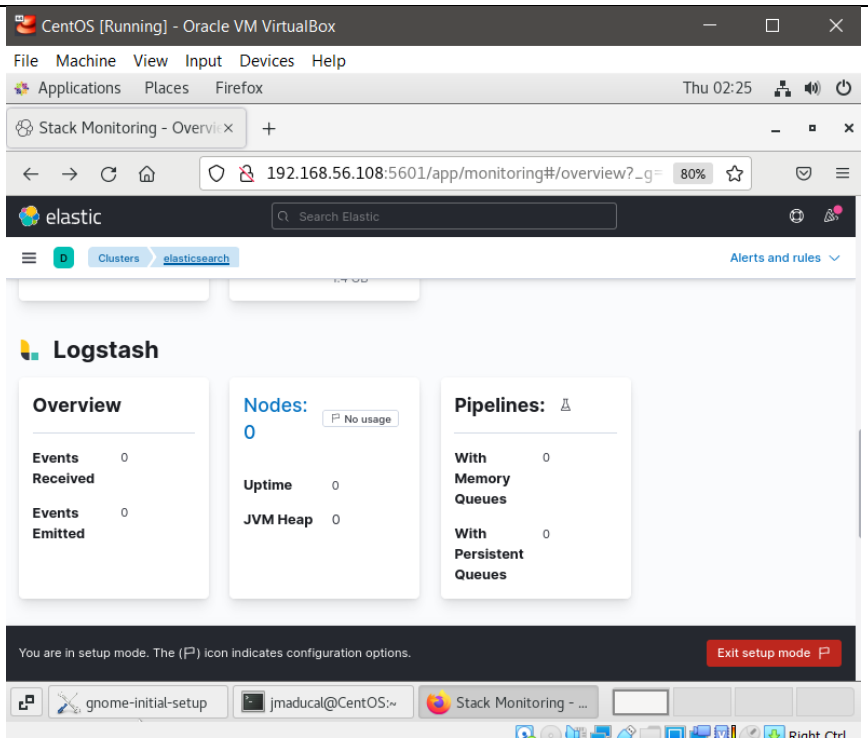
CentOS



Elastic Stack (Elasticsearch) for CentOS

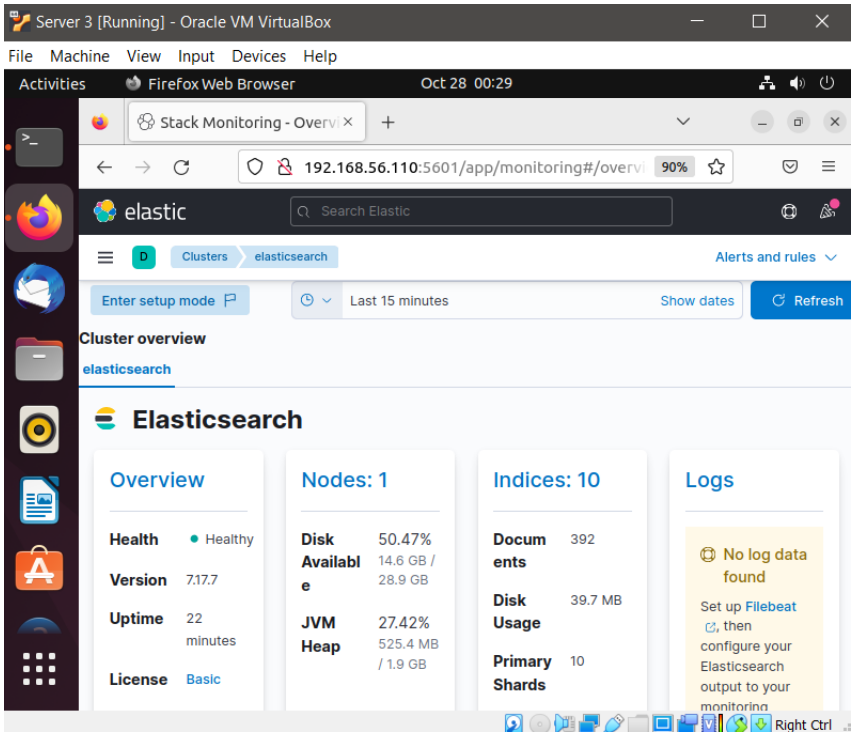


Elastic Stack (Kibana) for CentOS

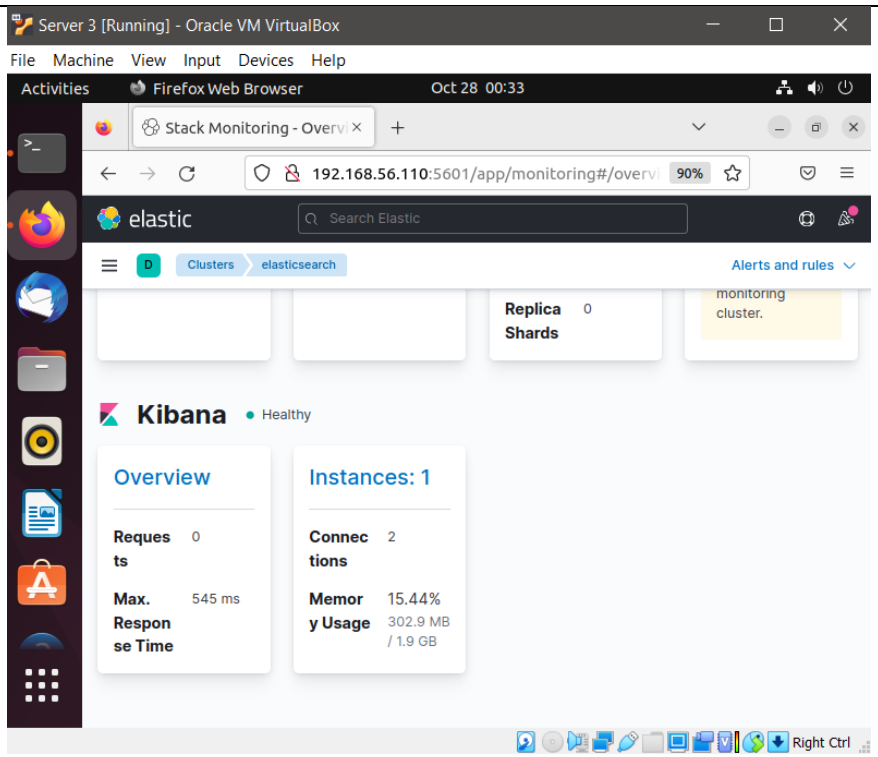


Elastic Stack (Logstash) for CentOS

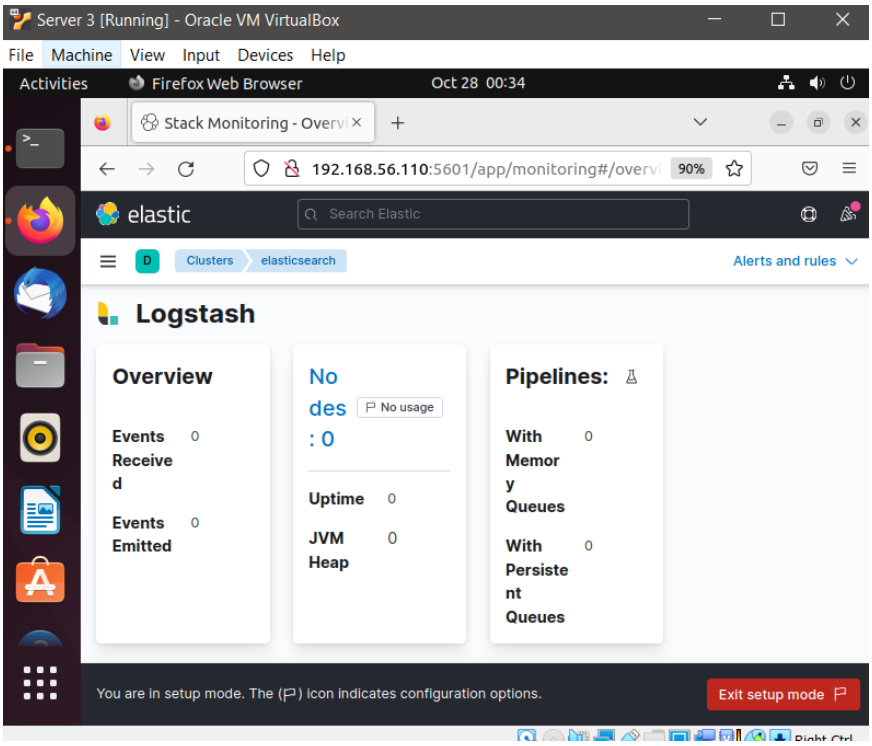
Server 3



Elastic Stack (Elasticsearch) for Server 3



Elastic Stack (Kibana) for Server 3



Elastic Stack (Logstash) for Server 3

```
jmaducal@workstation: ~/Aducal_Activity-10
jmaducal@workstation:~/Aducal_Activity-10$ git status
On branch main
Your branch is up to date with 'origin/main'.

Untracked files:
  (use "git add <file>..." to include in what will be committed)
        ELKstack.yml
        ansible.cfg
        inventory
        roles/

nothing added to commit but untracked files present (use "git add" to track)
jmaducal@workstation:~/Aducal_Activity-10$ git add ELKstack.yml
jmaducal@workstation:~/Aducal_Activity-10$ git add ansible.cfg
jmaducal@workstation:~/Aducal_Activity-10$ git add inventory
jmaducal@workstation:~/Aducal_Activity-10$ git add roles/
jmaducal@workstation:~/Aducal_Activity-10$ git commit -m "Aducal_Act-10"
[main 259fe4a] Aducal_Act-10
 5 files changed, 85 insertions(+)
 create mode 100644 ELKstack.yml
 create mode 100644 ansible.cfg
 create mode 100644 inventory
 create mode 100644 roles/Application_server/tasks/main.yml
 create mode 100644 roles/Web_server/tasks/main.yml
jmaducal@workstation:~/Aducal_Activity-10$
```

```
jmaducal@workstation:~/Aducal_Activity-10$ git push origin main
Enumerating objects: 10, done.
Counting objects: 100% (10/10), done.
Compressing objects: 100% (7/7), done.
Writing objects: 100% (9/9), 1.08 KiB | 1.08 MiB/s, done.
Total 9 (delta 0), reused 0 (delta 0), pack-reused 0
To github.com:jmaducal12/Aducal_Activity-10.git
   fbcc91a..259fe4a  main -> main
```

Search or jump to... / Pull requests Issues Marketplace Explore

jmaducal12 / Aducal_Activity-10 Public

Pin | Unwatch 1 | Fork 0 | Star 0

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights | Settings

main | 1 branch | 0 tags | Go to file | Add file | Code

John Mark Aducal Aducal_Act-10 259fe4a 2 minutes ago 2 commits

roles	Aducal_Act-10	2 minutes ago
ELKstack.yml	Aducal_Act-10	2 minutes ago
README.md	Initial commit	yesterday
ansible.cfg	Aducal_Act-10	2 minutes ago
inventory	Aducal_Act-10	2 minutes ago

README.md

Aducal_Activity-10

About

No description, website, or topics provided.

Readme
0 stars
1 watching
0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

© 2022 GitHub, Inc. Terms Privacy Security Status Docs Contact GitHub Pricing API Training Blog About

GitHub Repository Link:

https://github.com/jmaducal12/Aducal_Activity-10.git

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool? The benefits of having a log monitoring tool like ELK (Elasticsearch, Logstash, and Kibana), which offers engineers and DevSecOps teams a good logging solution and is also useful in diagnosing and fixing bugs and production issues. Logging is becoming increasingly vital with the development in machine data. In order to provide the best possible application performance, it is important for diagnosing and resolving problems. Finding problems is only one aspect of logging. It also serves as a system monitor. You can aggregate logs from all of your systems using the ELK stack.

Conclusions:

In this Activity, I have learned how to install, configure and manage log monitoring tools using ansible. I able to install ELK stack (Elasticsearch, Logstash and Kibana) in our remote servers Ubuntu Server3 and CentOS using ansible command in the local machine or workstation, the most important is I able to apply my knowledge from the past activities such as installing nagios available monitoring tool, installing prometheus performance monitoring tool and creating a roles and targeting specific nodes to install some packages. All in all, this activity helps me to better understand the importance of having a log monitoring tool in your system especially the use of this is to diagnose and resolve a bugs in the system by means of logging. This tool can be useful in tech companies in such way that the DevSecOps team will examine data,adapt and deliver what your system needs by the using ELK stack log monitoring tool.

Honor Pledge:

“I affirm that I will not give or receive any unauthorized help on this activity, and that all work will be my own.

John Mark Aducal