Name: Jefferson Langbid	Date Performed:
Course/Section: CPE232-CPE31S23	Date Submitted:
Instructor: Dr. Taylar	Semester and SY:

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.

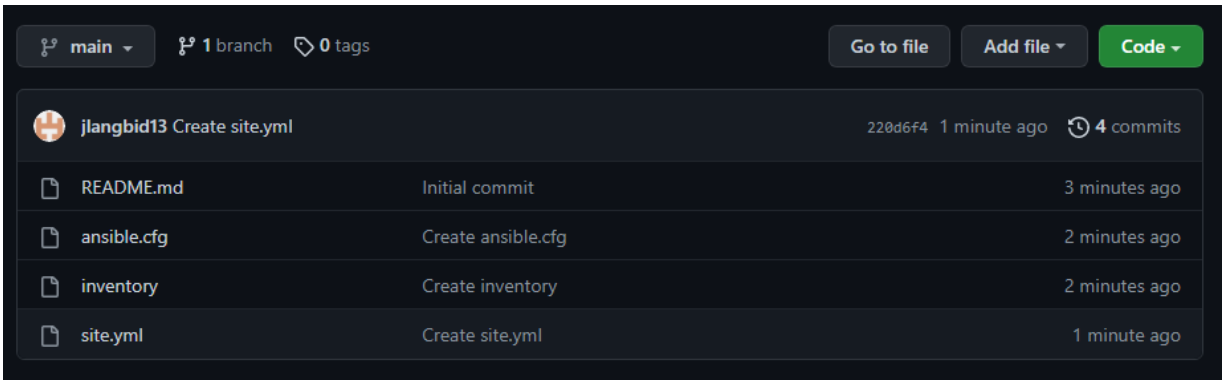
We use Graylog primarily as the stash for the logs of the web applications we build. However, it is also effective when working with raw strings (i.e. syslog): the tool parses it into the structured data we need. It also allows advanced custom search in the logs using structured queries. In other words, 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.

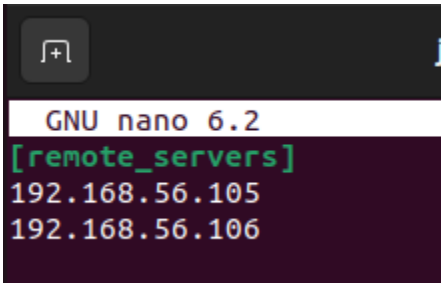
4. Output (screenshots and explanations)



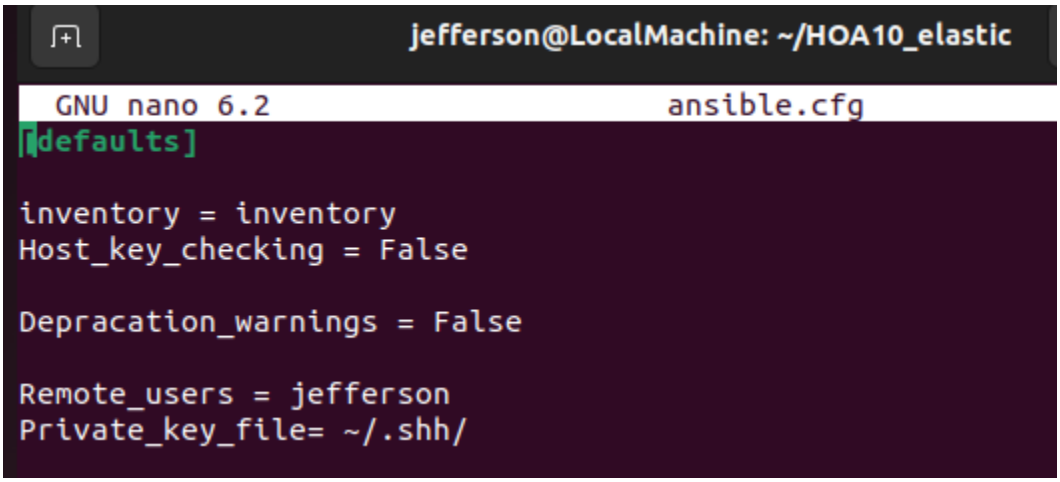
Create new repository in the github

```
jefferson@LocalMachine:~$ git clone git@github.com:jlangbid13/HOA10_elastic.git
Cloning into 'HOA10_elastic'...
remote: Enumerating objects: 12, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (9/9), done.
remote: Total 12 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (12/12), done.
Resolving deltas: 100% (2/2), done.
```

Clone the github repository in the local machine.



Create the inventory file



Create the ansible.cfg file to configure the remote users.

```
jefferson@LocalMachine: ~/HOA10_elastic
  GNU nano 6.2                                site.yml
---
- hosts: all
  become: true
  pre_tasks:

  - name: update repository index (CentOS)
    tags: always
    dnf:
      update_cache: yes
    changed_when: false
    when: ansible_distribution == "CentOS"
  - name: install updates (Ubuntu)
    tags: always
    apt:
      update_cache: yes
    changed_when: false
    when: ansible_distribution == "Ubuntu"
```

Create the site.yml for the pretask and later on the code to run the roles.

```
jefferson@LocalMachine: ~/HOA10_elastic/roles
jefferson@LocalMachine:~$ cd HOA10_elastic
jefferson@LocalMachine:~/HOA10_elastic$ ls
ansible.cfg  inventory  README.md  site.yml
jefferson@LocalMachine:~/HOA10_elastic$ mkdir roles
jefferson@LocalMachine:~/HOA10_elastic$ cd roles
jefferson@LocalMachine:~/HOA10_elastic/roles$ mkdir install
jefferson@LocalMachine:~/HOA10_elastic/roles$ cd install
jefferson@LocalMachine:~/HOA10_elastic/roles/install$ mkdir tasks
jefferson@LocalMachine:~/HOA10_elastic/roles/install$ cd tasks
jefferson@LocalMachine:~/HOA10_elastic/roles/install/tasks$ sudo nano main.yml
jefferson@LocalMachine:~/HOA10_elastic/roles/install/tasks$ cd ..
jefferson@LocalMachine:~/HOA10_elastic/roles/install$ cd ..
jefferson@LocalMachine:~/HOA10_elastic/roles$ tree
.
└── install
    └── tasks
        └── main.yml

2 directories, 1 file
```

Create a new directory for the roles and a new directory which is Install and inside it will be the tasks where I will put the main.yml file.

jefferson@LocalMachine: ~/HOA10_elastic/roles/install/tasks

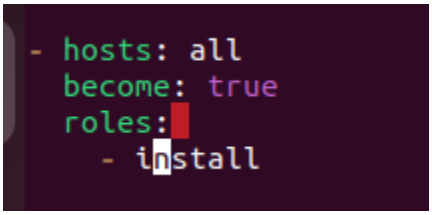
GNU nano 6.2 main.yml

```
- name: install elastic stack for ubuntu
  apt:
    name:
      - elasticsearch
      - kibana
      - logstash
    state: latest
    update_cache: yes
  when: ansible_distribution == "Ubuntu"

- name: install elastic stack for centos
  dnf:
    name:
      - elasticsearch
      - kibana
      - logstash
    state: latest
    update_cache: yes
  when: ansible_distribution == "CentOS"
```

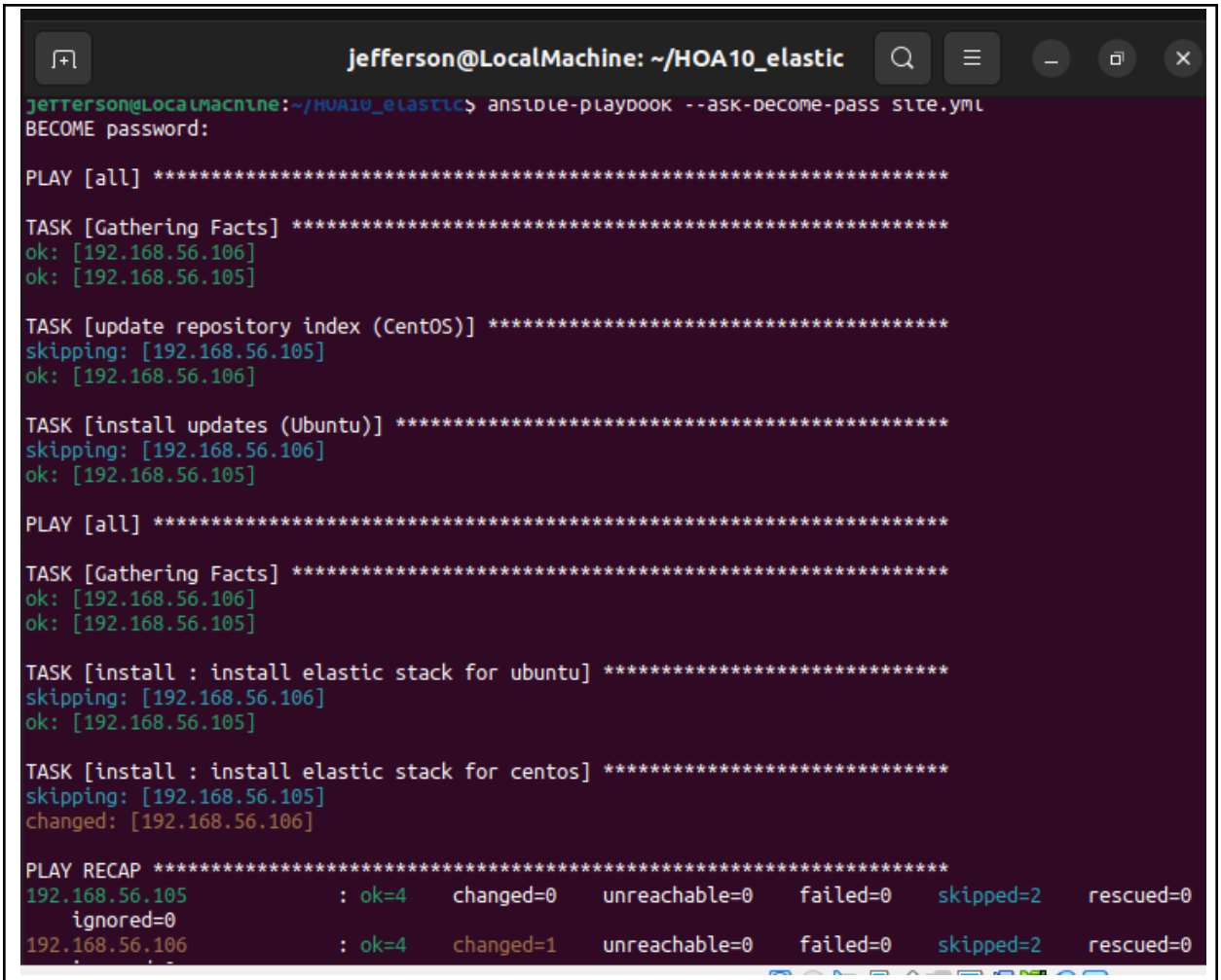
Files

Input the command in the main.yml that installs the elastic stack which is elasticsearch, kibana, and logstash.



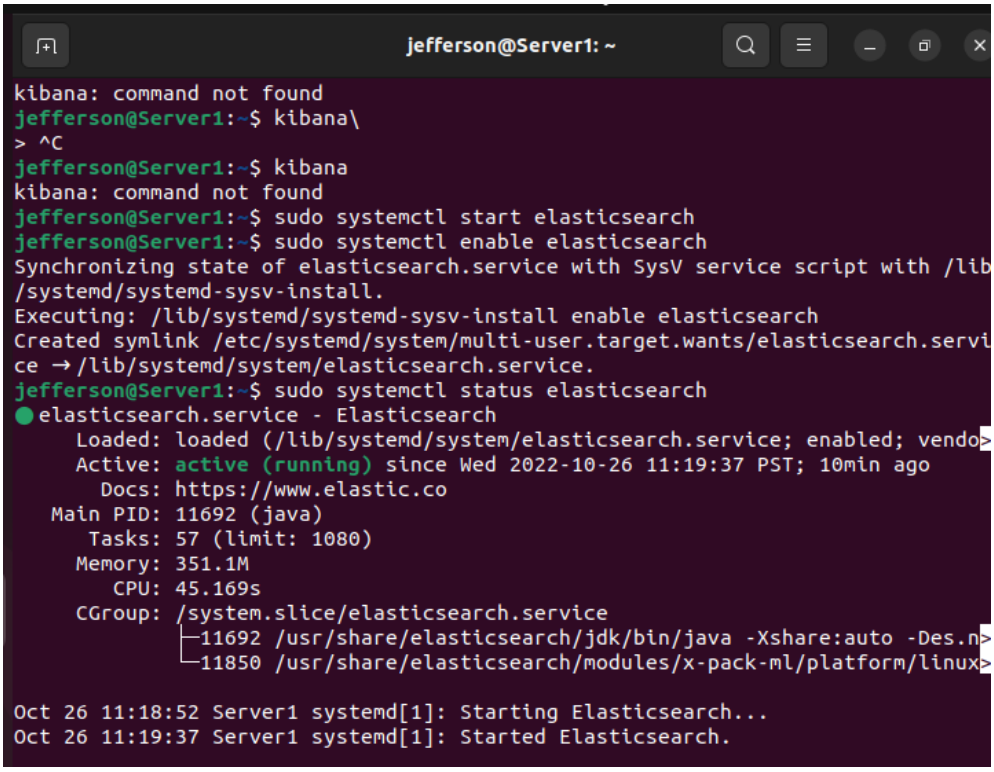
```
- hosts: all
  become: true
  roles:
    - install
```

The command inside the site.yml to run the roles.

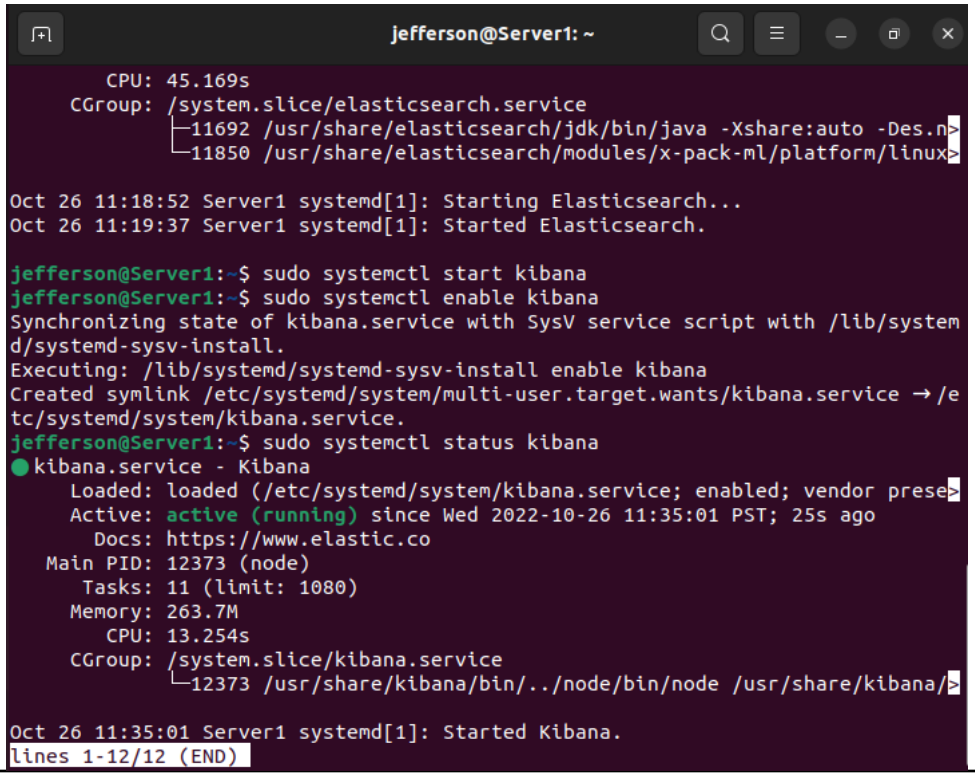


The code ran and it successfully installed the elastic stack (elasticsearch, kibana, and logstash) in both ubuntu and Centos servers.

Ubuntu (Elasticsearch)



Ubuntu (Kibana)



Ubuntu (Logstash)

```
jefferson@Server1:~$ sudo systemctl start logstash
jefferson@Server1:~$ sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service →
/etc/systemd/system/logstash.service.
jefferson@Server1:~$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor pre>
     Active: active (running) since Wed 2022-10-26 11:36:29 PST; 21s ago
   Main PID: 12502 (java)
      Tasks: 14 (limit: 1080)
     Memory: 209.8M
        CPU: 8.036s
     CGroup: /system.slice/logstash.service
             └─12502 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCo>

Oct 26 11:36:29 Server1 systemd[1]: Started logstash.
Oct 26 11:36:29 Server1 logstash[12502]: Using bundled JDK: /usr/share/logstas>
Oct 26 11:36:30 Server1 logstash[12502]: OpenJDK 64-Bit Server VM warning: Opt>
lines 1-13/13 (END)
```

CentOS (Elasticsearch)

```
jefferson@localhost:~
File  Edit  View  Search  Terminal  Help
[jefferson@localhost ~]$ sudo systemctl start elasticsearch
[sudo] password for jefferson:
[jefferson@localhost ~]$ sudo systemctl enable elasticsearch
[sudo] password for jefferson:
Created symlink from /etc/systemd/system/multi-user.target.wants/elasticsearch.service
to /usr/lib/systemd/system/elasticsearch.service.
[jefferson@localhost ~]$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor prese
t: disabled)
   Active: active (running) since Wed 2022-10-26 13:26:34 PST; 6min ago
     Docs: https://www.elastic.co
 Main PID: 3274 (java)
   CGroup: /system.slice/elasticsearch.service
           ├─3274 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkadd...
           └─3445 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/b...

Oct 26 13:25:38 localhost.localdomain systemd[1]: Starting Elasticsearch...
Oct 26 13:26:34 localhost.localdomain systemd[1]: Started Elasticsearch.
[jefferson@localhost ~]$ curl -X GET "localhost:9200"
{
  "name" : "localhost.localdomain",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "gVHWxH7xTmeMlk0LIlu8Fg",
  "version" : {
    "number" : "7.17.7",
```

Centos (Kibana)

```
[jefferson@localhost ~]$ sudo systemctl start kibana
[jefferson@localhost ~]$ sudo systemctl enable kibana
Created symlink from /etc/systemd/system/multi-user.target.wants/kibana.service to /etc
/systemd/system/kibana.service.
[jefferson@localhost ~]$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled
)
   Active: active (running) since Wed 2022-10-26 13:33:45 PST; 21s ago
     Docs: https://www.elastic.co
 Main PID: 4301 (node)
    Tasks: 11
   CGroup: /system.slice/kibana.service
           └─4301 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../sr...

Oct 26 13:33:45 localhost.localdomain systemd[1]: Started Kibana.
[jefferson@localhost ~]$
```

Centos (Logstash)

```
[jefferson@localhost ~]$ sudo systemctl start logstash
[jefferson@localhost ~]$ sudo systemctl enable logstash
Created symlink from /etc/systemd/system/multi-user.target.wants/logstash.service to /e
tc/systemd/system/logstash.service.
[jefferson@localhost ~]$ sudo systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabl
ed)
   Active: active (running) since Wed 2022-10-26 13:35:33 PST; 46s ago
 Main PID: 4438 (java)
   CGroup: /system.slice/logstash.service
           └─4438 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSwe...

Oct 26 13:35:33 localhost.localdomain systemd[1]: Started logstash.
Oct 26 13:35:33 localhost.localdomain logstash[4438]: Using bundled JDK: /usr/share...k
Oct 26 13:35:34 localhost.localdomain logstash[4438]: OpenJDK 64-Bit Server VM warn....
Hint: Some lines were ellipsized, use -l to show in full.
[jefferson@localhost ~]$
```

Reflections:

Answer the following:

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

   The advantage of an uptime monitoring tool is that you can monitor what everyone is doing and see if it is good or correct, leading to better work results. Monitoring staff can guide people to improve performance and achieve better work results.

Conclusions:

All in all, I created a new directory for the activity and cloned it in my local machine. I created the file which is the ansible.cfg and inventory to configure the remote user to connect with the ansible. After creating the file I created a new file for the ansible playbook which is the site.yml and input the commands with the pre_tasks. After creating the file I created the roles directory, install directory and tasks to input the main.yml file for the command that will install the elastic stack which os elasticsearch, kibana, and logstash in both Ubuntu and CentOs. After that I ran the site.yml playbook to run and it successfully ran and installed the elastic stack in both Ubuntu and CentOS.