Name: KEVIN ROI A. SUMAYA	**Date Performed: October 23 2023**
Course/Section: CPE31S6	**Date Submitted: October 23 2023**
Instructor: Jonathan Taylar	**Semester and 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.

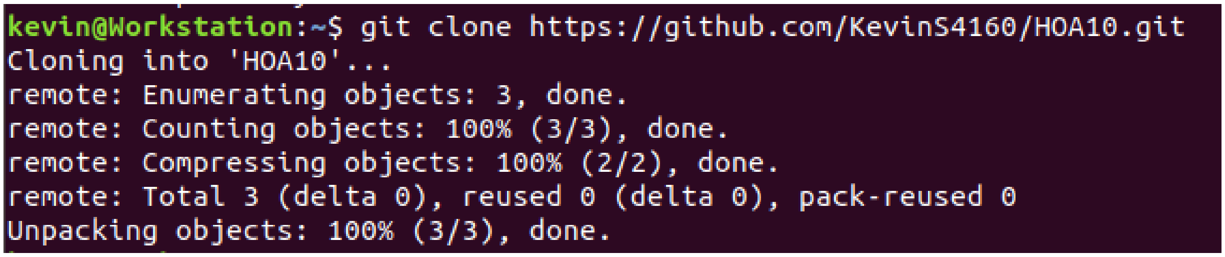
Source: https://www.graylog.org/products/open-source

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.

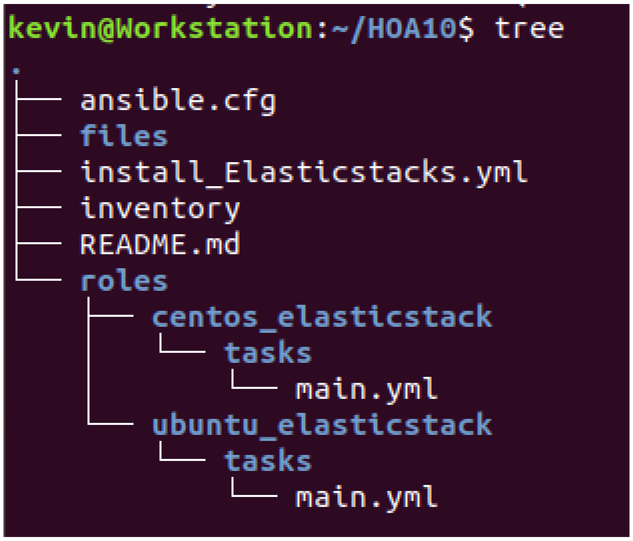
4. **Output** (screenshots and explanations)

Step 1: Create a Repository and Clone it



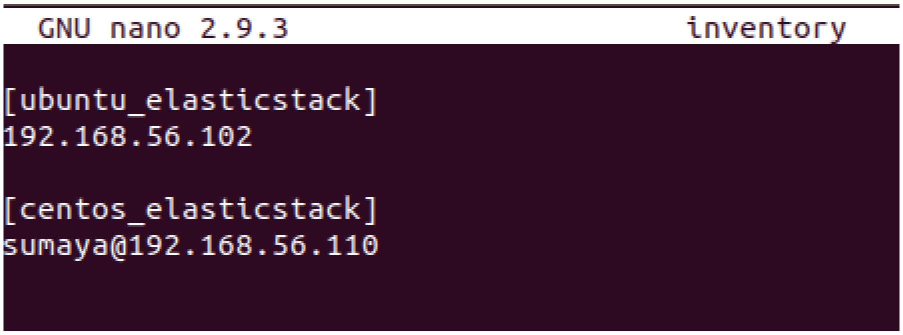
```
kevin@Workstation:~$ git clone https://github.com/KevinS4160/HOA10.git
Cloning into 'HOA10'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (3/3), done.
```

Step 2: I created a Playbook that install the Elastic Stacks



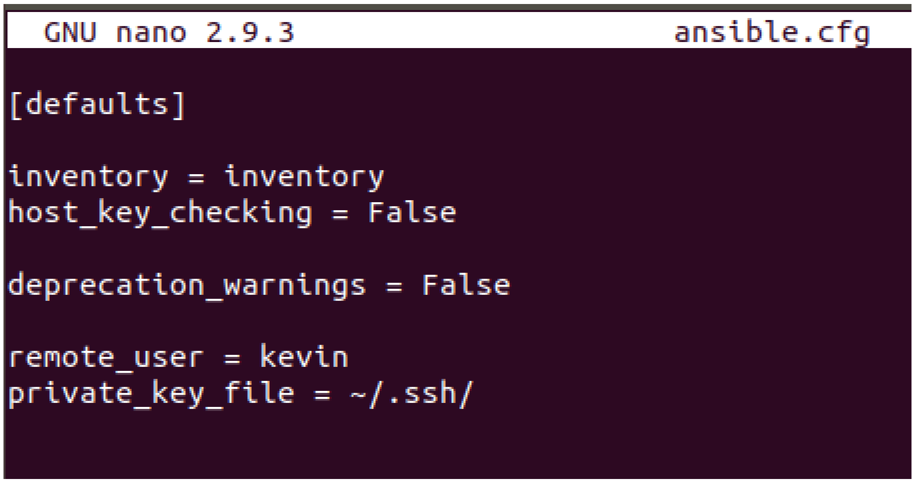
```
kevin@Workstation:~/HOA10$ tree
.
├── ansible.cfg
├── files
├── install_Elasticstacks.yml
├── inventory
├── README.md
└── roles
    ├── centos_elasticstack
    │   └── tasks
    │       └── main.yml
    └── ubuntu_elasticstack
        └── tasks
            └── main.yml
```

Step 3: This is my inventory to know where ElasticStack to be installed.



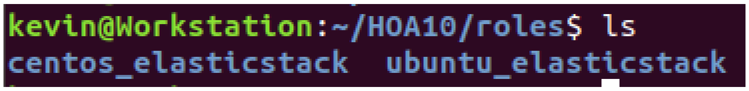
```
  GNU nano 2.9.3                              inventory

[ubuntu_elasticstack]
192.168.56.102

[centos_elasticstack]
sumaya@192.168.56.110
```

Step 4: This is my Ansible.cfg



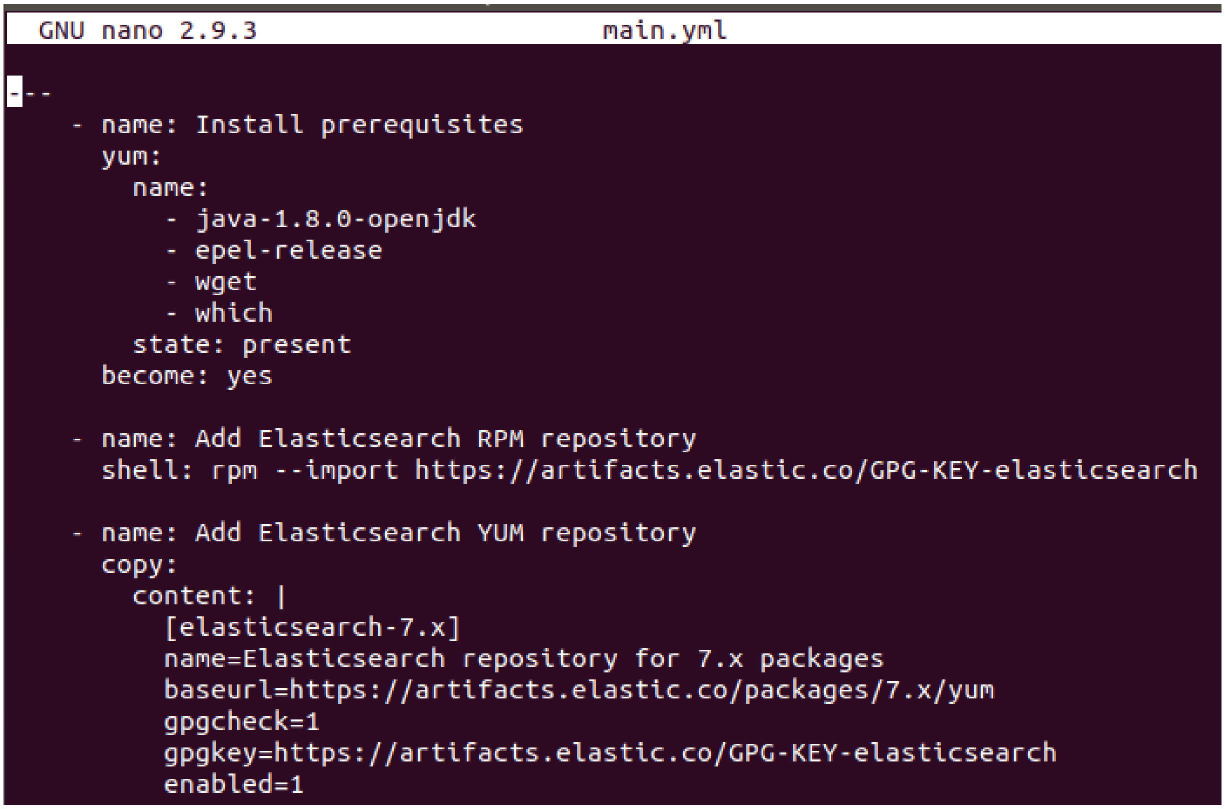
```
  GNU nano 2.9.3                              ansible.cfg

[defaults]

inventory = inventory
host_key_checking = False

deprecation_warnings = False

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

Step 5: I created 2 directories for me to install the Elastic search on both Ubuntu and CentOS.

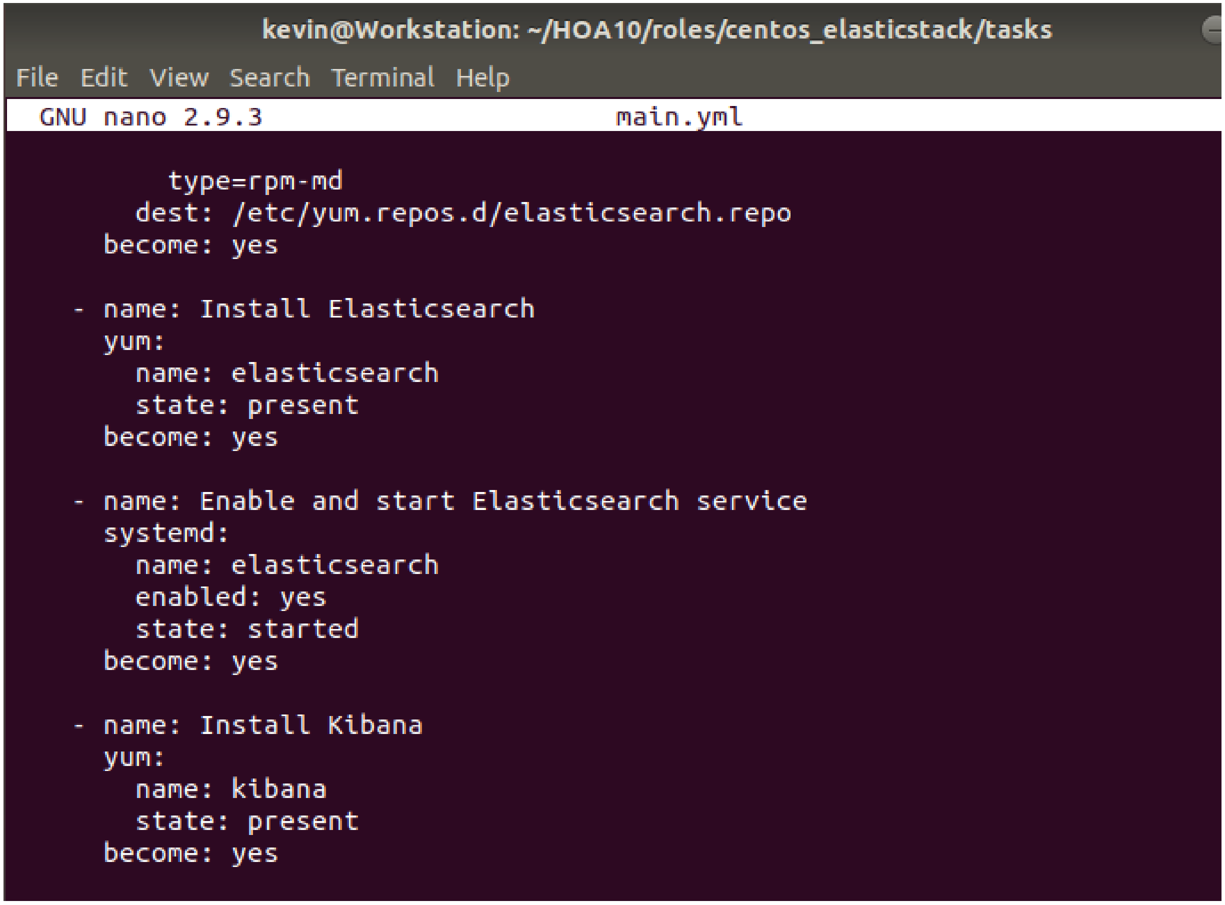


```
kevin@Workstation:~/HOA10/roles$ ls
centos_elasticstack  ubuntu_elasticstack
```

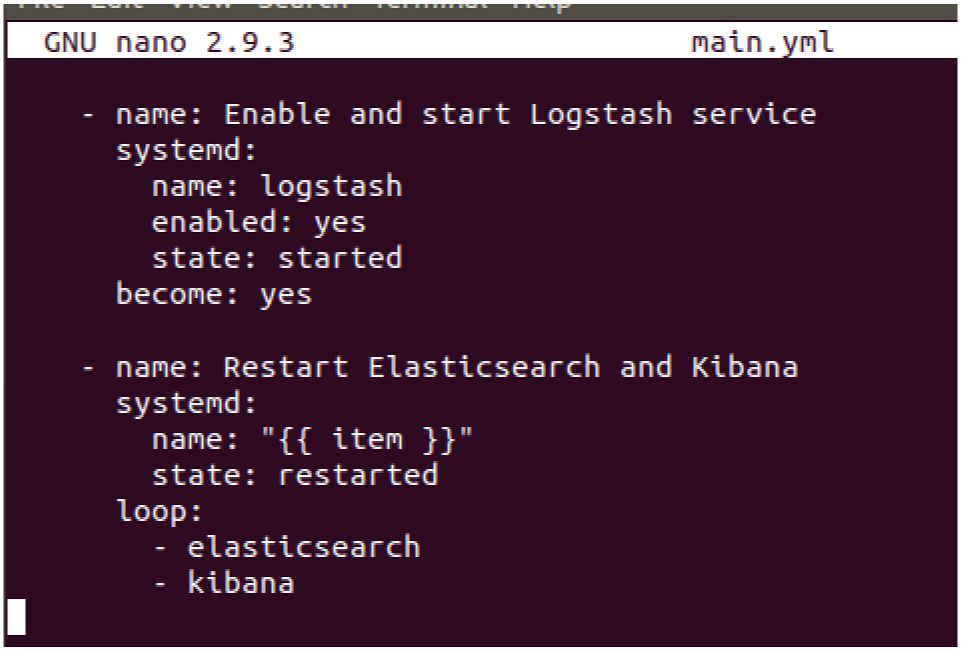
Step 6: For the first directory(centos_elasticstack) I created an installation code for me to install ElasticStacks on Centos



```
  GNU nano 2.9.3                        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
```

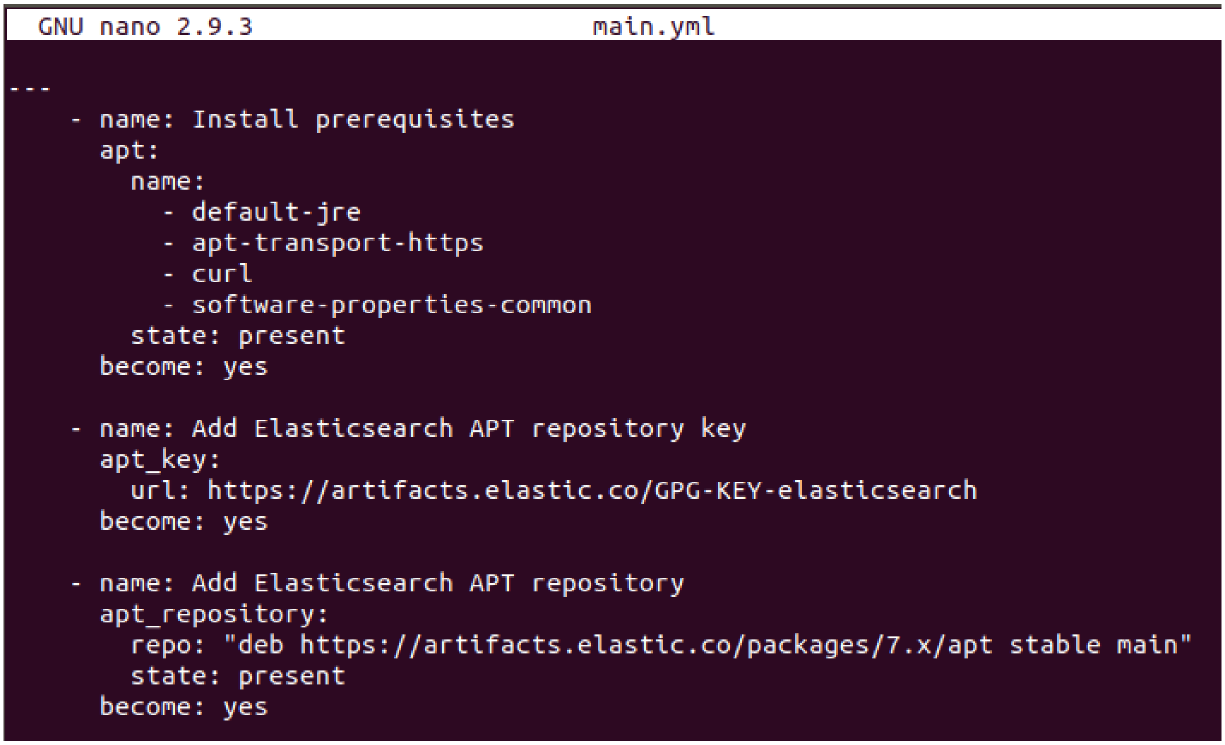

kevin@Workstation: ~/HOA10/roles/centos_elasticstack/tasks
File Edit View Search Terminal Help

```
  GNU nano 2.9.3                            main.yml

          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
```

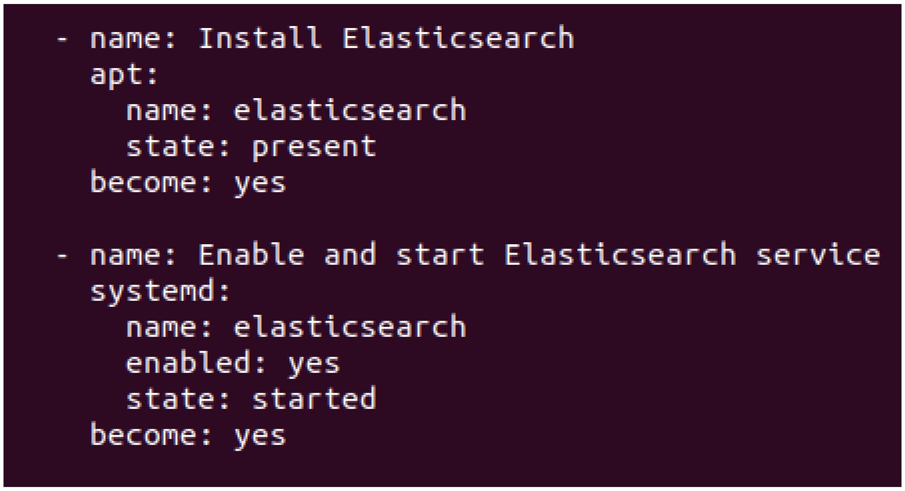


```
  GNU nano 2.9.3                            main.yml

    - 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
```

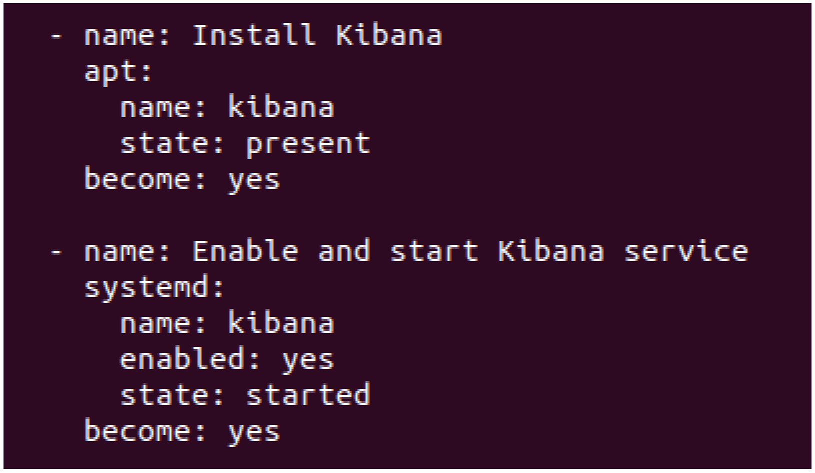
Step 7: For the second directory(ubuntu_elasticstack) I created an installation code for me to install ElasticStacks on Ubuntu.



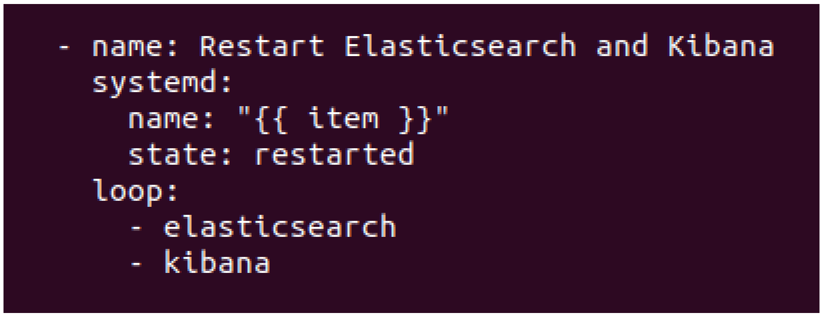
```
  GNU nano 2.9.3                              main.yml

---
    - 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
```

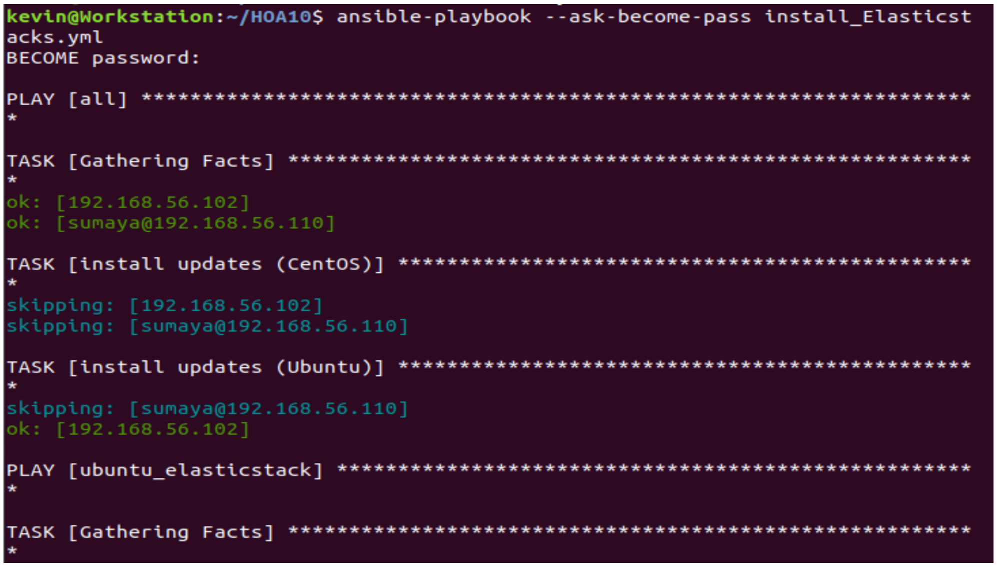


```
  - name: Install Kibana
    apt:
      name: kibana
      state: present
    become: yes

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

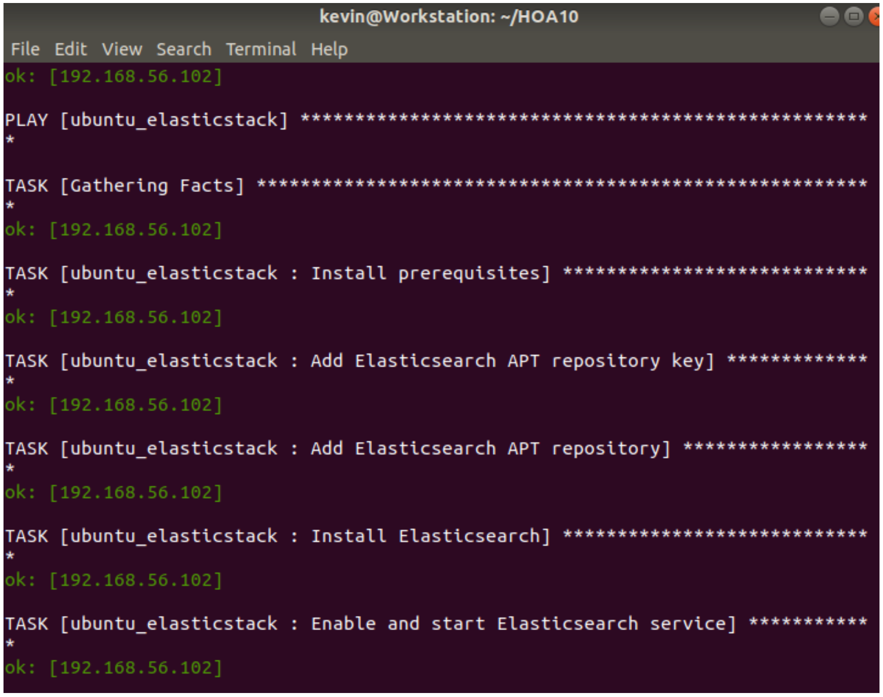


```
  - name: Restart Elasticsearch and Kibana
    systemd:
      name: "{{ item }}"
      state: restarted
    loop:
      - elasticsearch
      - kibana
```

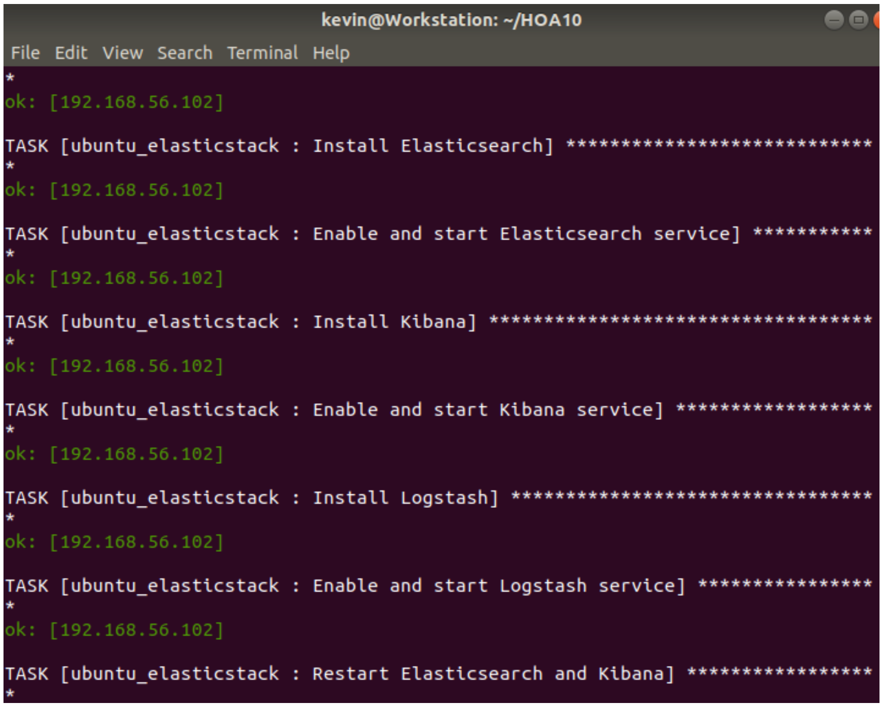
Step 8: I run the installation with ansible-playbook –ask-become-pass install_Elasticstack.yml and this is the result.



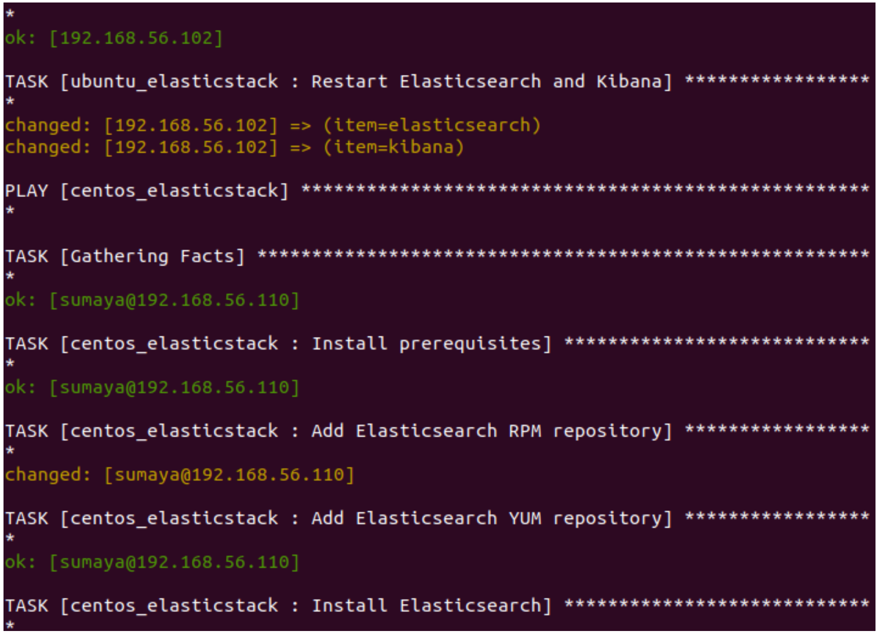
```
kevin@Workstation:~/HOA10$ ansible-playbook --ask-become-pass install_Elasticst
acks.yml
BECOME password:

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

TASK [Gathering Facts] *********************************************************
*
ok: [192.168.56.102]
ok: [sumaya@192.168.56.110]

TASK [install updates (CentOS)] ************************************************
*
skipping: [192.168.56.102]
skipping: [sumaya@192.168.56.110]

TASK [install updates (Ubuntu)] ************************************************
*
skipping: [sumaya@192.168.56.110]
ok: [192.168.56.102]

PLAY [ubuntu_elasticstack] *****************************************************
*

TASK [Gathering Facts] *********************************************************
*
```


kevin@Workstation: ~/HOA10
File Edit View Search Terminal Help

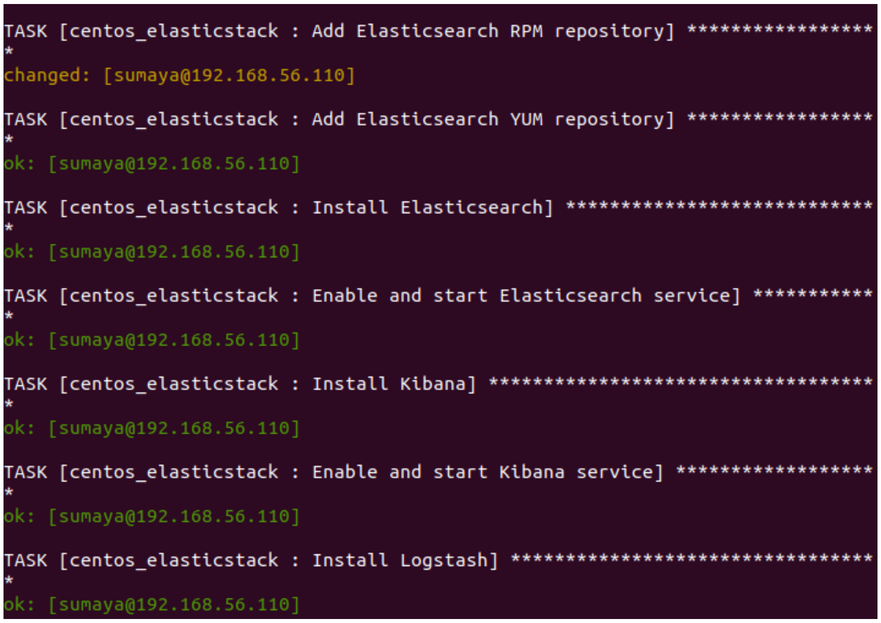
```
ok: [192.168.56.102]

PLAY [ubuntu_elasticstack] ****************************************************
*

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

TASK [ubuntu_elasticstack : Install prerequisites] ****************************
*
ok: [192.168.56.102]

TASK [ubuntu_elasticstack : Add Elasticsearch APT repository key] *************
*
ok: [192.168.56.102]

TASK [ubuntu_elasticstack : Add Elasticsearch APT repository] *****************
*
ok: [192.168.56.102]

TASK [ubuntu_elasticstack : Install Elasticsearch] ****************************
*
ok: [192.168.56.102]

TASK [ubuntu_elasticstack : Enable and start Elasticsearch service] ***********
*
ok: [192.168.56.102]
```


kevin@Workstation: ~/HOA10
File Edit View Search Terminal Help

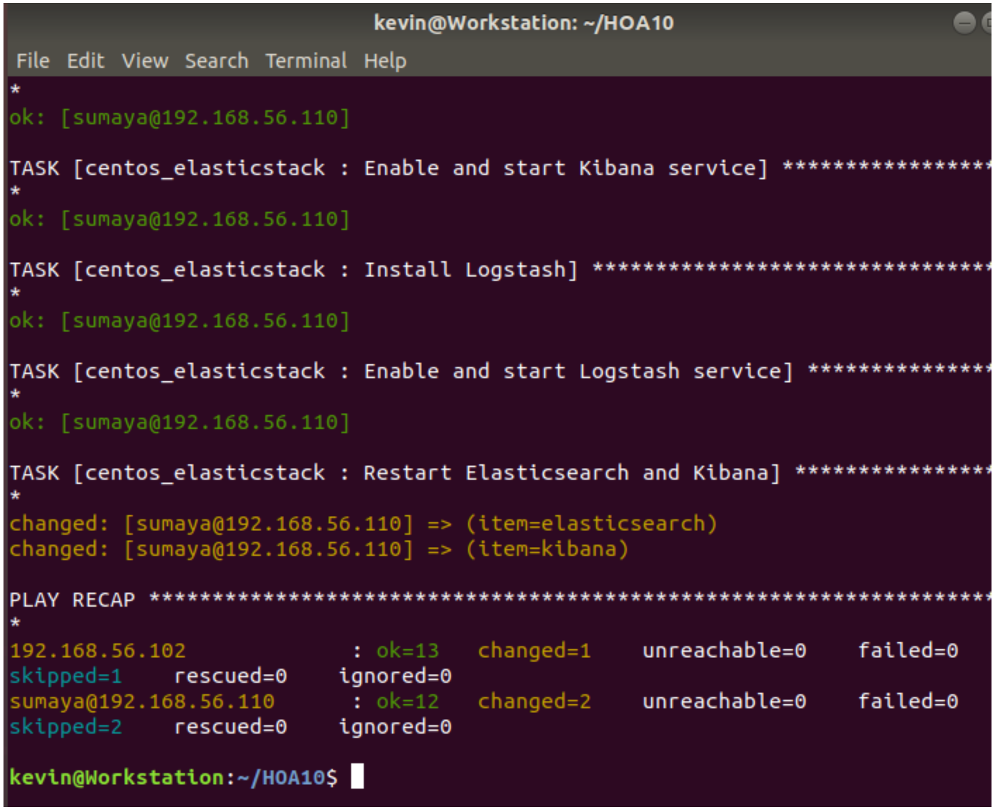
```
*
ok: [192.168.56.102]

TASK [ubuntu_elasticstack : Install Elasticsearch] ****************************
*
ok: [192.168.56.102]

TASK [ubuntu_elasticstack : Enable and start Elasticsearch service] ***********
*
ok: [192.168.56.102]

TASK [ubuntu_elasticstack : Install Kibana] ***********************************
*
ok: [192.168.56.102]

TASK [ubuntu_elasticstack : Enable and start Kibana service] ******************
*
ok: [192.168.56.102]

TASK [ubuntu_elasticstack : Install Logstash] *********************************
*
ok: [192.168.56.102]

TASK [ubuntu_elasticstack : Enable and start Logstash service] ****************
*
ok: [192.168.56.102]

TASK [ubuntu_elasticstack : Restart Elasticsearch and Kibana] *****************
*
```



```
*
ok: [192.168.56.102]

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

PLAY [centos_elasticstack] ****************************************************
*

TASK [Gathering Facts] ********************************************************
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Install prerequisites] ****************************
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Add Elasticsearch RPM repository] *****************
*
changed: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Add Elasticsearch YUM repository] *****************
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Install Elasticsearch] ****************************
*
```

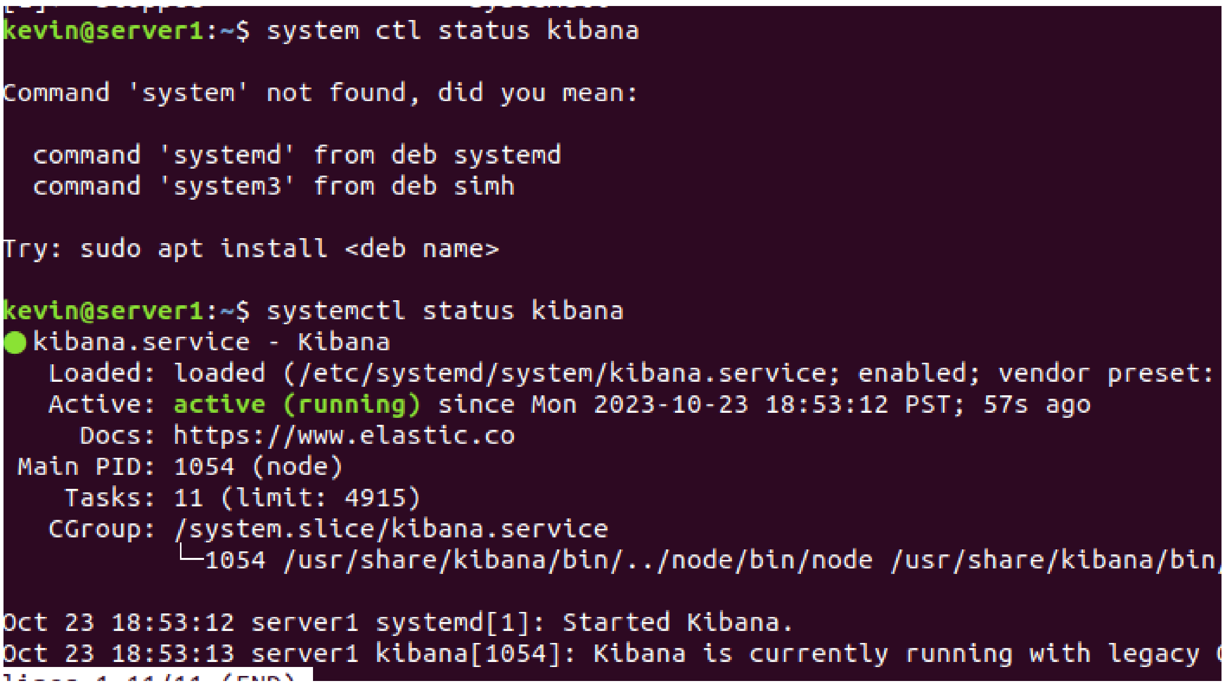


```
TASK [centos_elasticstack : Add Elasticsearch RPM repository] *****************
*
changed: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Add Elasticsearch YUM repository] *****************
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Install Elasticsearch] ****************************
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Enable and start Elasticsearch service] ***********
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Install Kibana] ***********************************
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Enable and start Kibana service] ******************
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Install Logstash] *********************************
*
ok: [sumaya@192.168.56.110]
```


kevin@Workstation: ~/HOA10
File Edit View Search Terminal Help

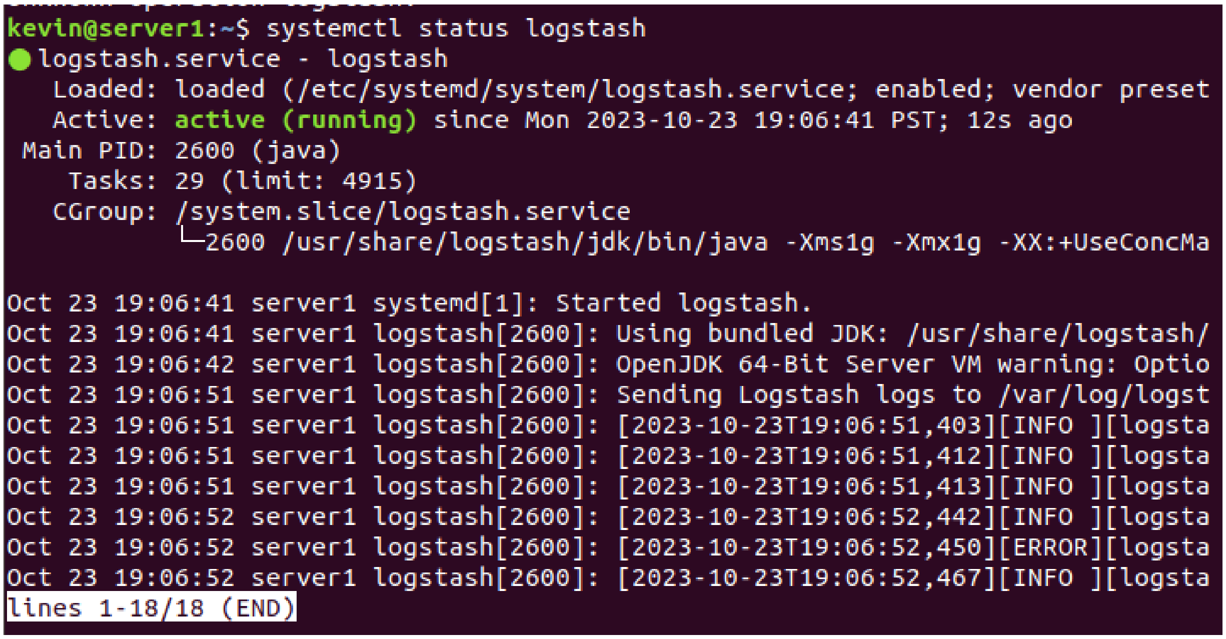
```
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Enable and start Kibana service] *****************
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Install Logstash] ********************************
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Enable and start Logstash service] ***************
*
ok: [sumaya@192.168.56.110]

TASK [centos_elasticstack : Restart Elasticsearch and Kibana] ****************
*
changed: [sumaya@192.168.56.110] => (item=elasticsearch)
changed: [sumaya@192.168.56.110] => (item=kibana)

PLAY RECAP *******************************************************************
*
192.168.56.102             : ok=13   changed=1    unreachable=0    failed=0
skipped=1    rescued=0    ignored=0
sumaya@192.168.56.110      : ok=12   changed=2    unreachable=0    failed=0
skipped=2    rescued=0    ignored=0

kevin@Workstation:~/HOA10$ 
```

Step 9: This is the proof that the installed packages are working. (KIBANA)



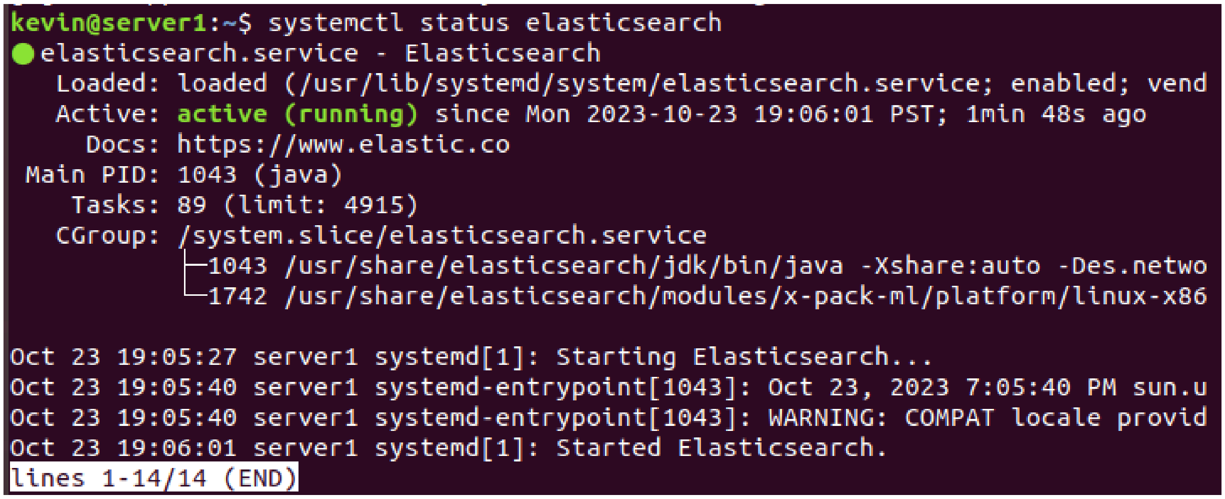
```
kevin@server1:~$ system ctl status kibana

Command 'system' not found, did you mean:

  command 'systemd' from deb systemd
  command 'system3' from deb simh

Try: sudo apt install <deb name>

kevin@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 18:53:12 PST; 57s ago
     Docs: https://www.elastic.co
 Main PID: 1054 (node)
    Tasks: 11 (limit: 4915)
   CGroup: /system.slice/kibana.service
           └─1054 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin

Oct 23 18:53:12 server1 systemd[1]: Started Kibana.
Oct 23 18:53:13 server1 kibana[1054]: Kibana is currently running with legacy 
lines 1-11/11 (END)
```

UBUNTU Server 2 (LOGSTASH)

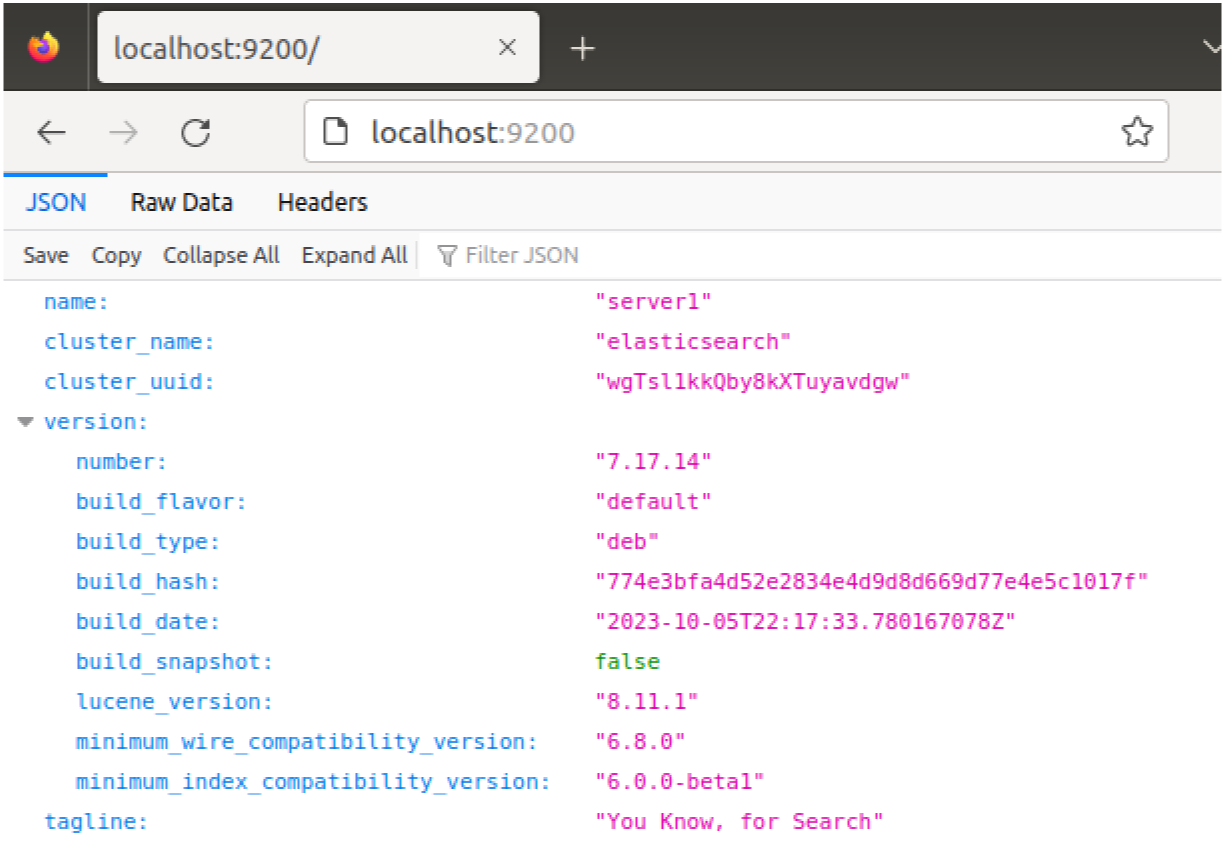


```
kevin@server1:~$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset
   Active: active (running) since Mon 2023-10-23 19:06:41 PST; 12s ago
 Main PID: 2600 (java)
    Tasks: 29 (limit: 4915)
   CGroup: /system.slice/logstash.service
           └─2600 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMa

Oct 23 19:06:41 server1 systemd[1]: Started logstash.
Oct 23 19:06:41 server1 logstash[2600]: Using bundled JDK: /usr/share/logstash/
Oct 23 19:06:42 server1 logstash[2600]: OpenJDK 64-Bit Server VM warning: Optio
Oct 23 19:06:51 server1 logstash[2600]: Sending Logstash logs to /var/log/logst
Oct 23 19:06:51 server1 logstash[2600]: [2023-10-23T19:06:51,403][INFO ][logsta
Oct 23 19:06:51 server1 logstash[2600]: [2023-10-23T19:06:51,412][INFO ][logsta
Oct 23 19:06:51 server1 logstash[2600]: [2023-10-23T19:06:51,413][INFO ][logsta
Oct 23 19:06:52 server1 logstash[2600]: [2023-10-23T19:06:52,442][INFO ][logsta
Oct 23 19:06:52 server1 logstash[2600]: [2023-10-23T19:06:52,450][ERROR][logsta
Oct 23 19:06:52 server1 logstash[2600]: [2023-10-23T19:06:52,467][INFO ][logsta
lines 1-18/18 (END)
```

UBUNTU Server 1 (ELASTICSEARCH)

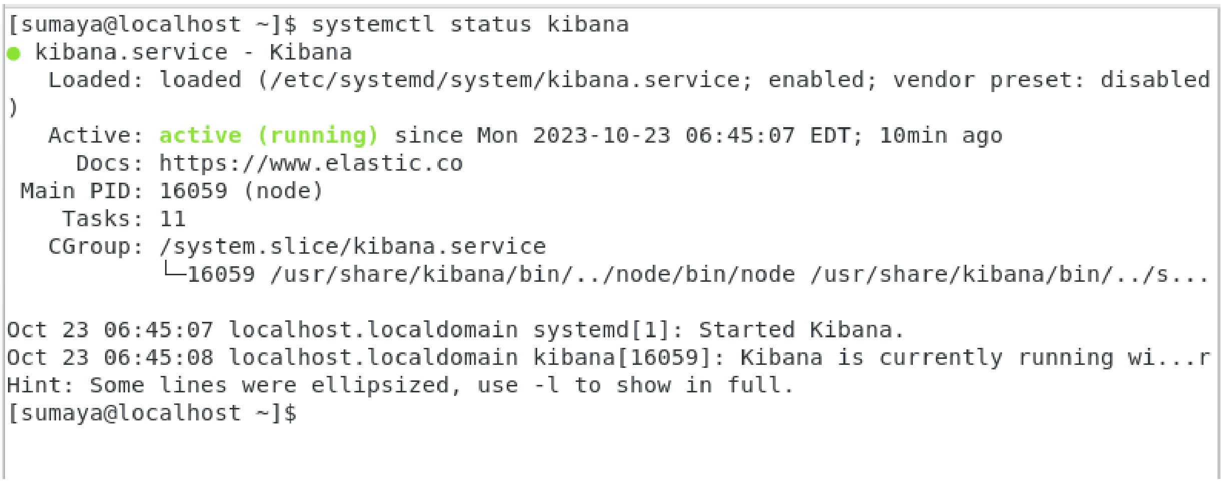


```
kevin@server1:~$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vend
   Active: active (running) since Mon 2023-10-23 19:06:01 PST; 1min 48s ago
     Docs: https://www.elastic.co
 Main PID: 1043 (java)
    Tasks: 89 (limit: 4915)
   CGroup: /system.slice/elasticsearch.service
           ├─1043 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.netwo
           └─1742 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86

Oct 23 19:05:27 server1 systemd[1]: Starting Elasticsearch...
Oct 23 19:05:40 server1 systemd-entrypoint[1043]: Oct 23, 2023 7:05:40 PM sun.u
Oct 23 19:05:40 server1 systemd-entrypoint[1043]: WARNING: COMPAT locale provid
Oct 23 19:06:01 server1 systemd[1]: Started Elasticsearch.
lines 1-14/14 (END)
```



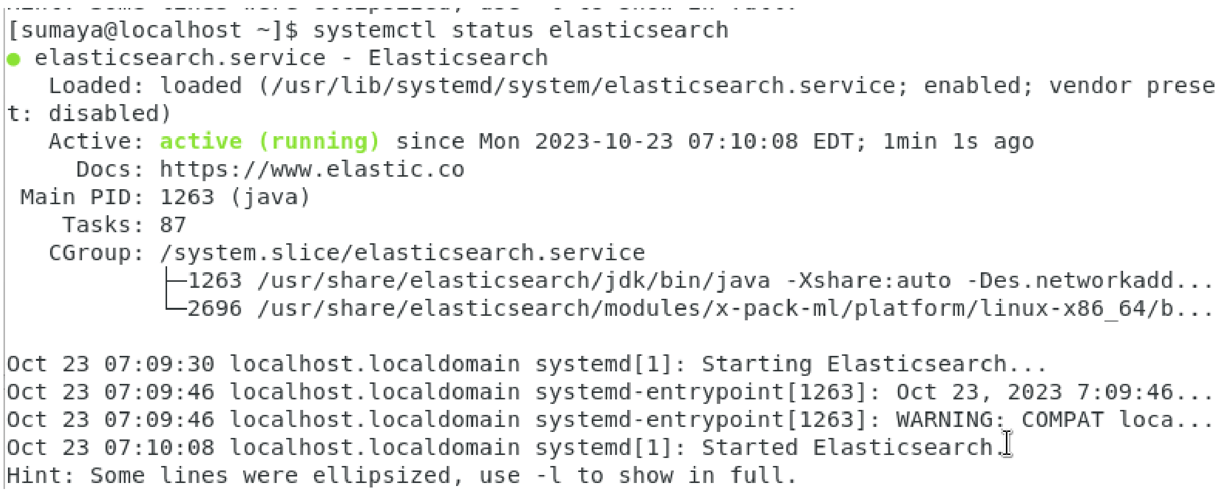
```
  name:                                   "server1"
  cluster_name:                           "elasticsearch"
  cluster_uuid:                           "wgTsl1kkQby8kXTuyavdgw"
▼ version:
    number:                               "7.17.14"
    build_flavor:                         "default"
    build_type:                           "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"
```

CENTOS KIBANA



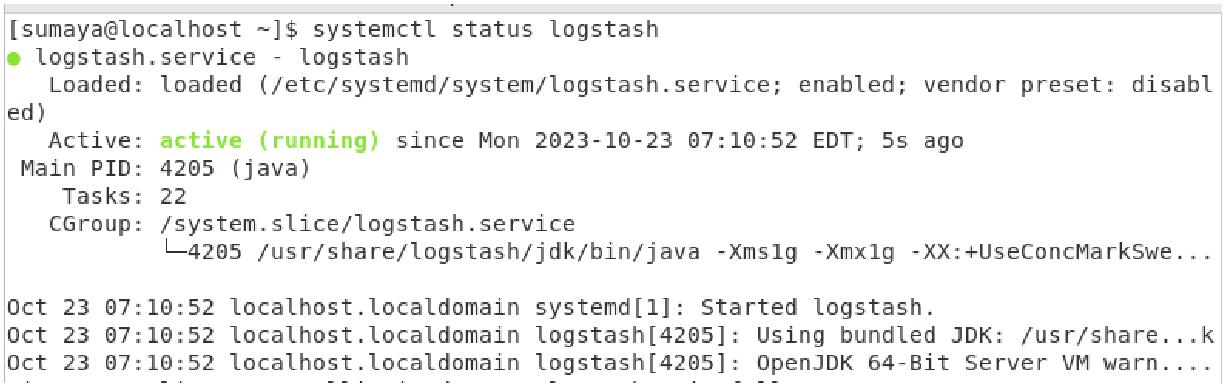
```
[sumaya@localhost ~]$ systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled
)
   Active: active (running) since Mon 2023-10-23 06:45:07 EDT; 10min ago
     Docs: https://www.elastic.co
 Main PID: 16059 (node)
    Tasks: 11
   CGroup: /system.slice/kibana.service
           └─16059 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../s...

Oct 23 06:45:07 localhost.localdomain systemd[1]: Started Kibana.
Oct 23 06:45:08 localhost.localdomain kibana[16059]: Kibana is currently running wi...r
Hint: Some lines were ellipsized, use -l to show in full.
[sumaya@localhost ~]$
```

CENTOS ELASTICSEARCH



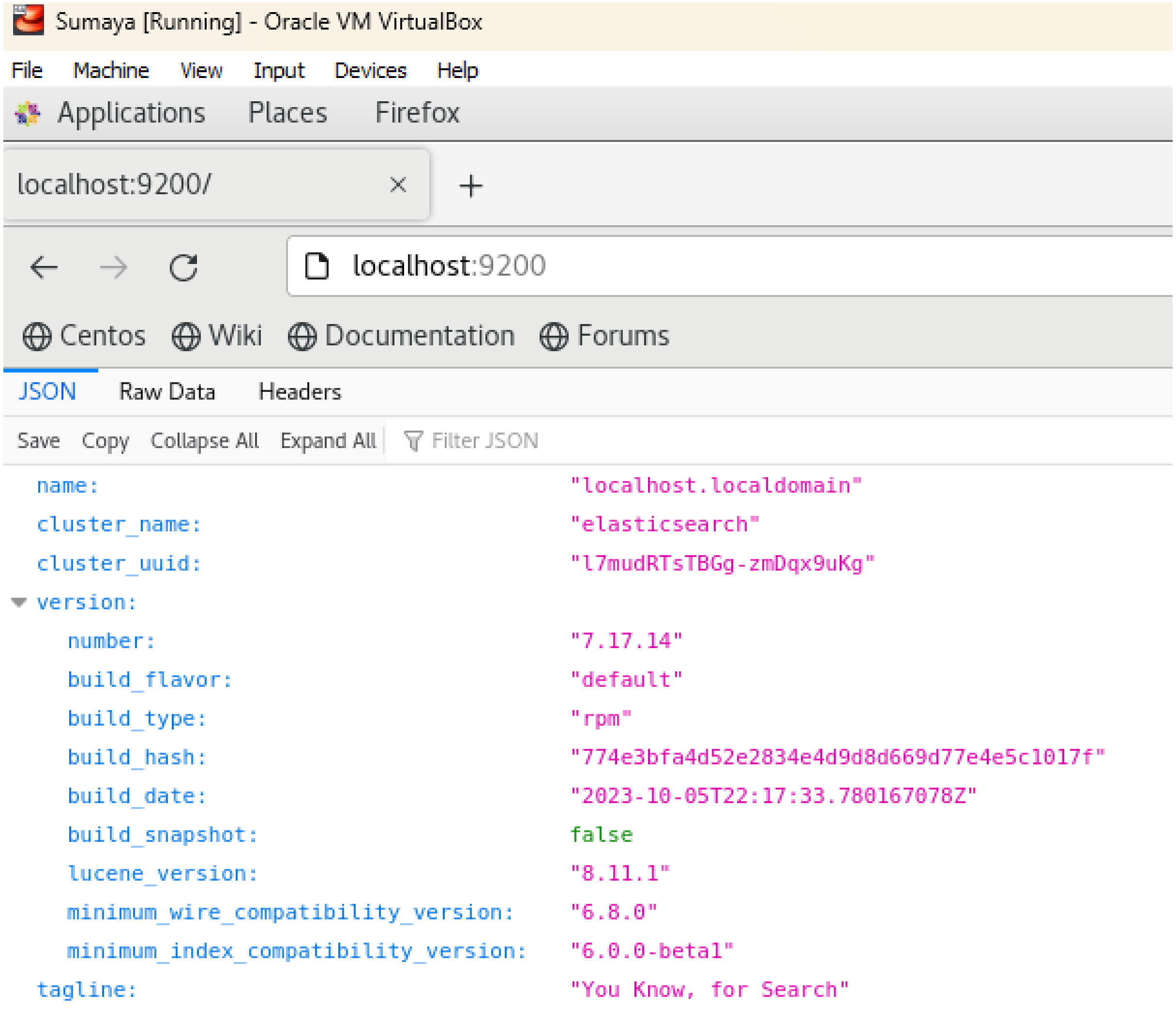
```
[sumaya@localhost ~]$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor prese
t: disabled)
   Active: active (running) since Mon 2023-10-23 07:10:08 EDT; 1min 1s ago
     Docs: https://www.elastic.co
 Main PID: 1263 (java)
    Tasks: 87
   CGroup: /system.slice/elasticsearch.service
           ├─1263 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkadd...
           └─2696 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/b...

Oct 23 07:09:30 localhost.localdomain systemd[1]: Starting Elasticsearch...
Oct 23 07:09:46 localhost.localdomain systemd-entrypoint[1263]: Oct 23, 2023 7:09:46...
Oct 23 07:09:46 localhost.localdomain systemd-entrypoint[1263]: WARNING: COMPAT loca...
Oct 23 07:10:08 localhost.localdomain systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
```

CENTOS LOGSTASH



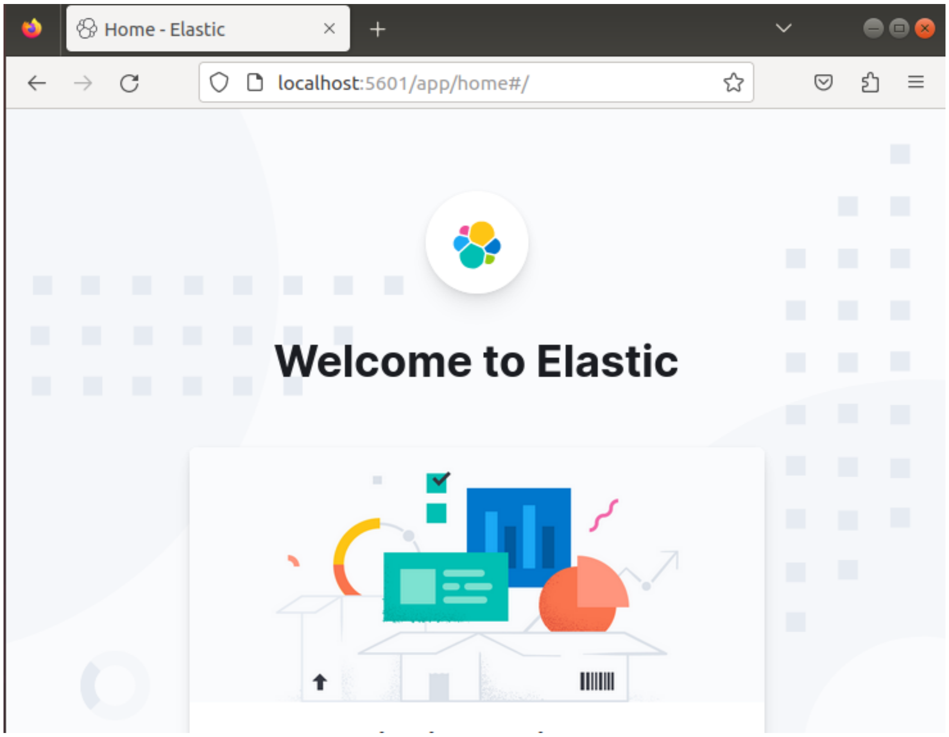
```
[sumaya@localhost ~]$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabl
ed)
   Active: active (running) since Mon 2023-10-23 07:10:52 EDT; 5s ago
 Main PID: 4205 (java)
    Tasks: 22
   CGroup: /system.slice/logstash.service
           └─4205 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSwe...

Oct 23 07:10:52 localhost.localdomain systemd[1]: Started logstash.
Oct 23 07:10:52 localhost.localdomain logstash[4205]: Using bundled JDK: /usr/share...k
Oct 23 07:10:52 localhost.localdomain logstash[4205]: OpenJDK 64-Bit Server VM warn....
```

CENTOS



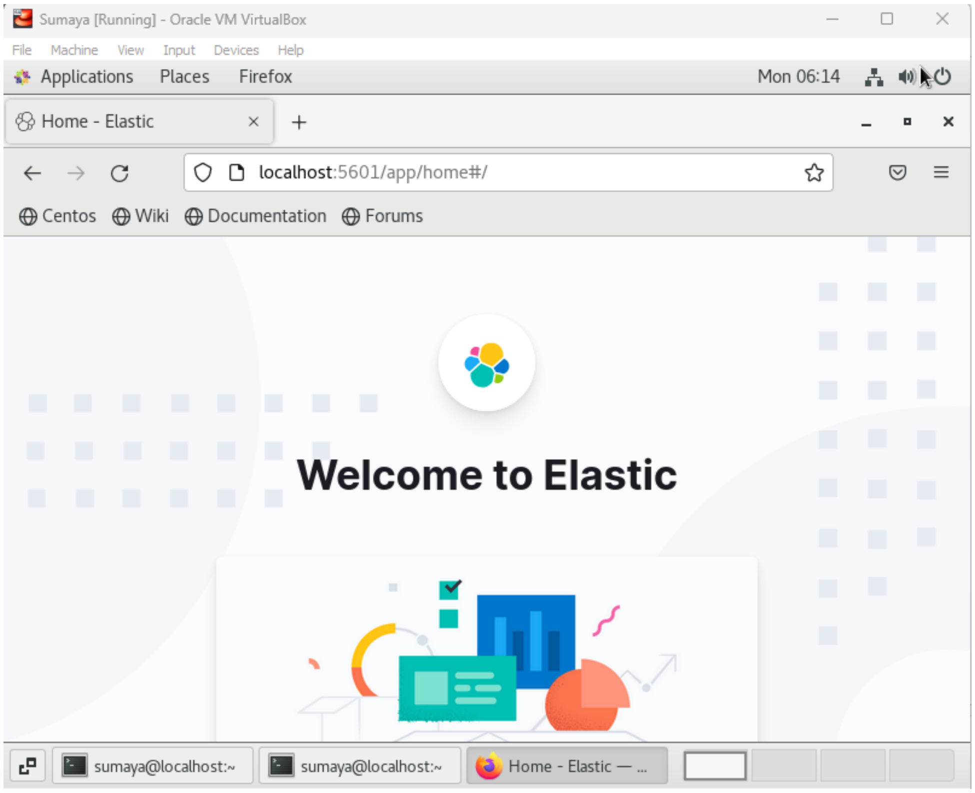
```
  name:                                   "localhost.localdomain"
  cluster_name:                           "elasticsearch"
  cluster_uuid:                           "l7mudRTsTBGg-zmDqx9uKg"
▼ version:
    number:                               "7.17.14"
    build_flavor:                         "default"
    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"
```

UBUNTU



Welcome to Elastic

CENTOS



Welcome to Elastic

THIS IS THE REPOSITORY LINK:

https://github.com/KevinS4160/HOA10.git

Reflections:

Answer the following:

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

    - Log monitoring tools can provide a number of significant benefits to organizations of all sizes. By helping organizations to improve detection and response to problems, reduce downtimes, improve the security als log monitoring tool can help organizations to improve their overall performance and efficiency. Log monitoring tools play a crucial role in maintaining the health, security, and performance of the systems and also the application, while also aiding in compliance and user experience improvement.

Conclusions:

- After doing the Activity I learned how to install ElasticSearch just like the last activity. I concluded that it is just the same as installing a Prometheus on both Ubuntu and CentOS so I have no problem dealing with installing ElasticSearch. I also learned that this ElasticSearch tool helps for log analytics, full-text search, security intelligence, business analytics, and operational intelligence use cases.