Name: Andaya, Lyka C.	**Date Performed: October 29, 2023**
Course/Section: CPE31S4	**Date Submitted: October 31, 2023**
Instructor: Dr. 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.

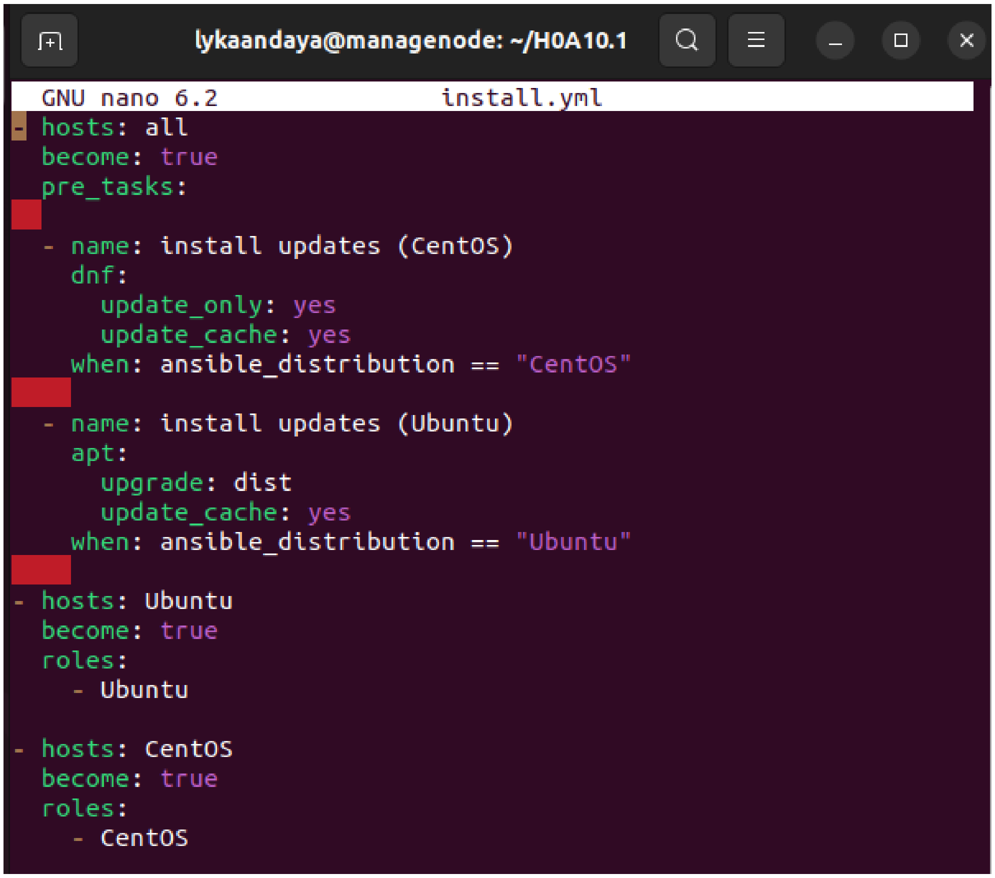
Source: https://www.graylog.org/products/open-source

3. Tasks

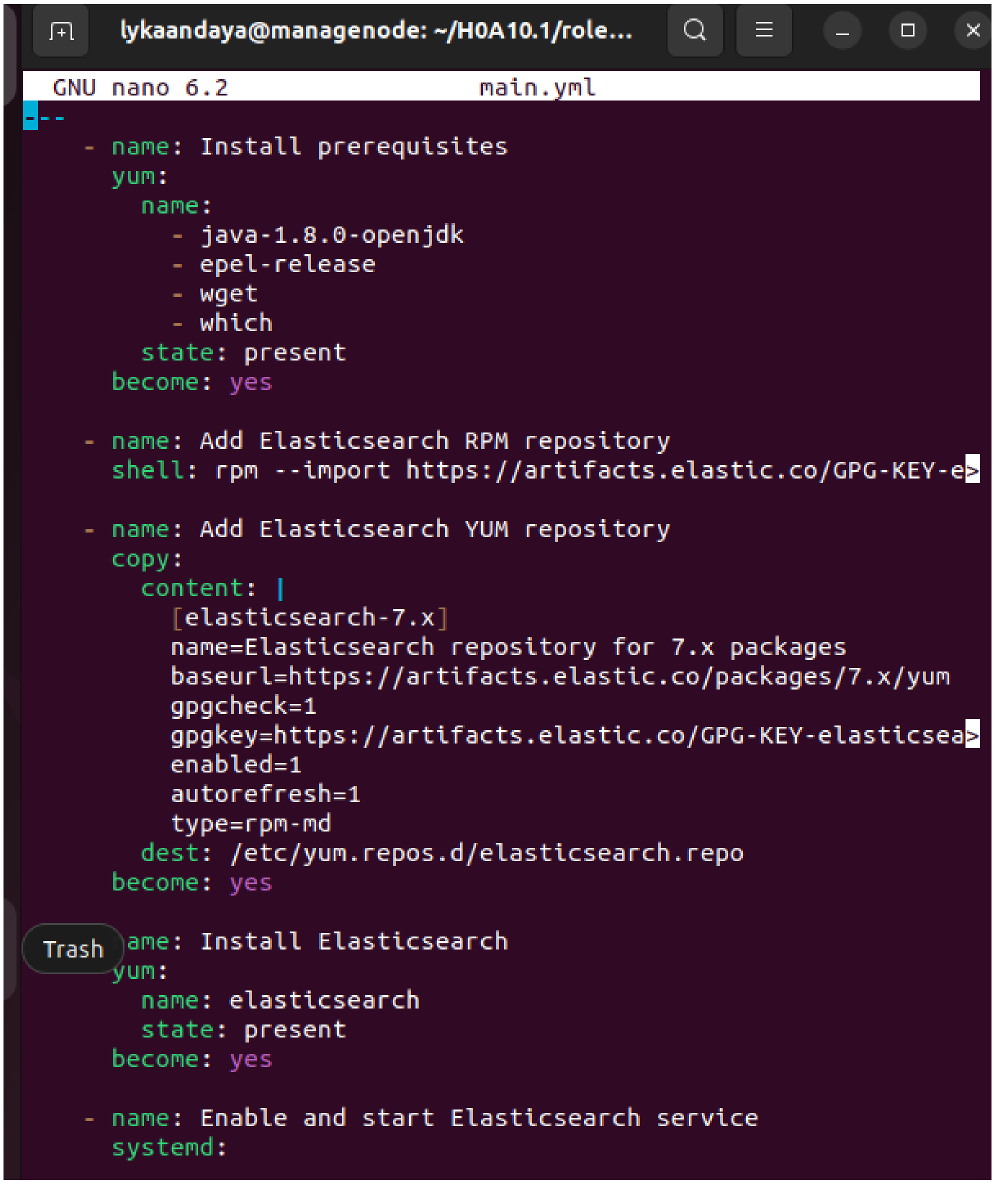
1. Create a playbook that:
    a. Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)
2. Apply the concept of creating roles.
3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like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

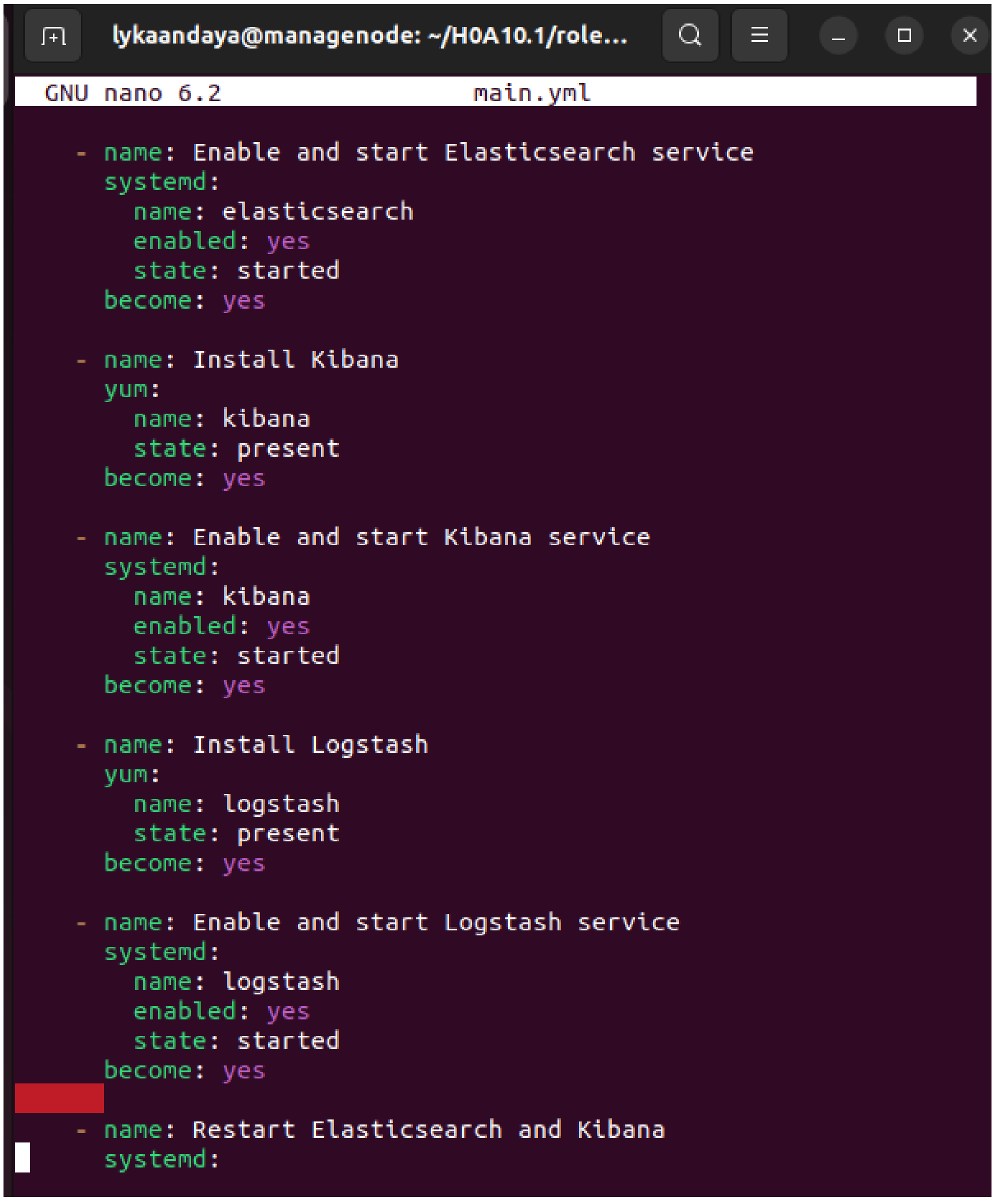
INPUT



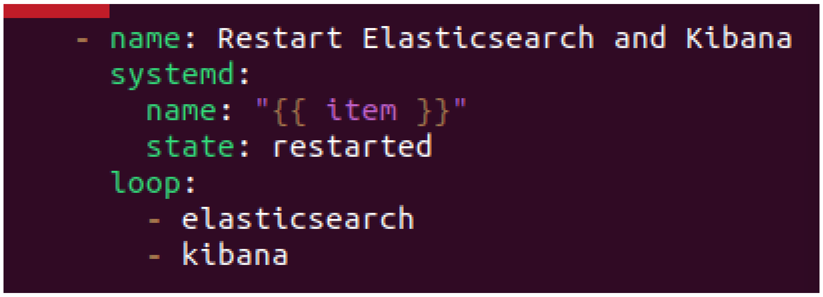
```
  GNU nano 6.2                  install.yml
- hosts: all
  become: true
  pre_tasks:

  - 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
```



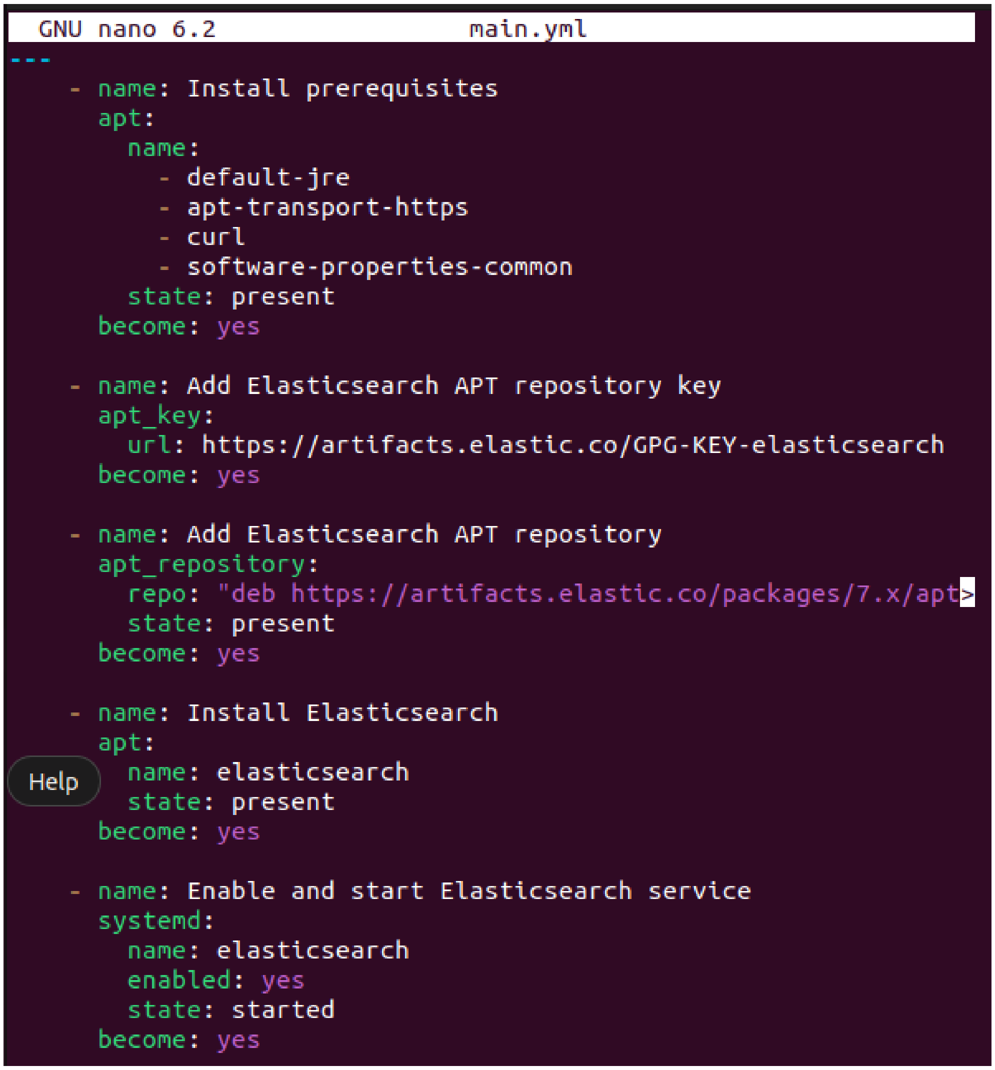
```
  GNU nano 6.2                    main.yml
---
    - name: Install prerequisites
      yum:
        name:
          - java-1.8.0-openjdk
          - epel-release
          - wget
          - which
        state: present
      become: yes

    - name: Add Elasticsearch RPM repository
      shell: rpm --import https://artifacts.elastic.co/GPG-KEY-e>

    - 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-elasticsea>
          enabled=1
          autorefresh=1
          type=rpm-md
        dest: /etc/yum.repos.d/elasticsearch.repo
      become: yes

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

    - name: Enable and start Elasticsearch service
      systemd:
```



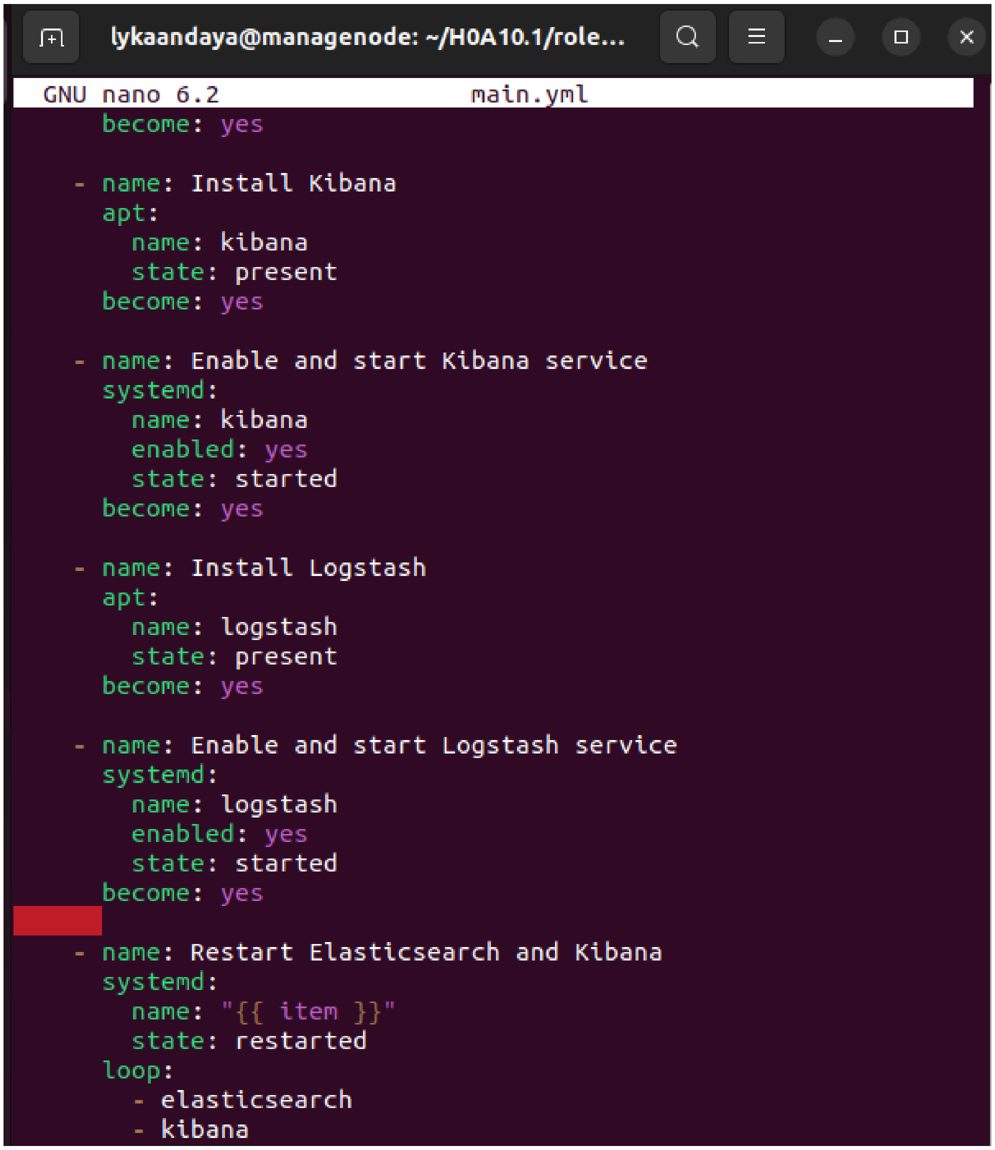
```
GNU nano 6.2                  main.yml

    - 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

    - 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

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

    - name: Restart Elasticsearch and Kibana
      systemd:
```



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



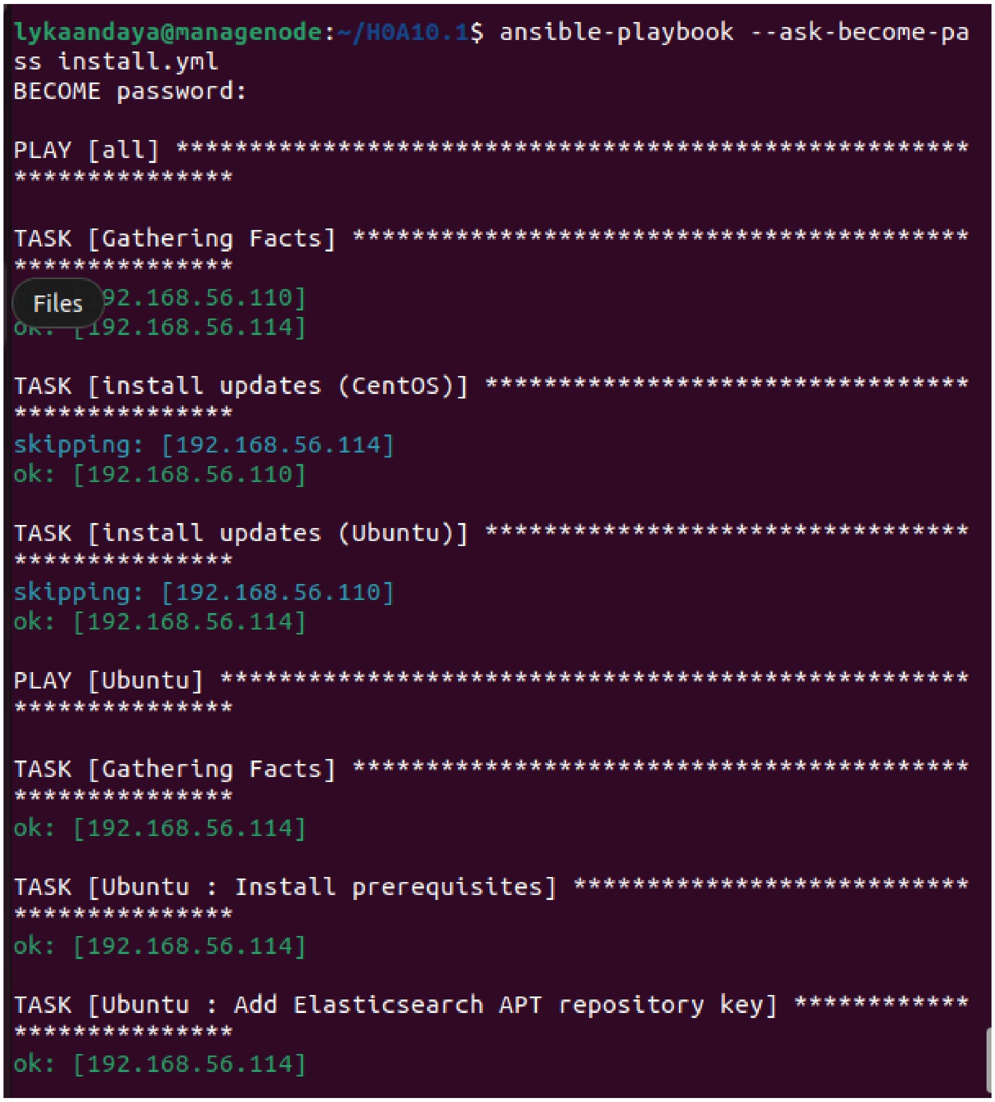
```
---
    - name: Install prerequisites
      apt:
        name:
          - default-jre
          - apt-transport-https
          - curl
          - software-properties-common
        state: present
      become: yes

    - 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>
        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
```



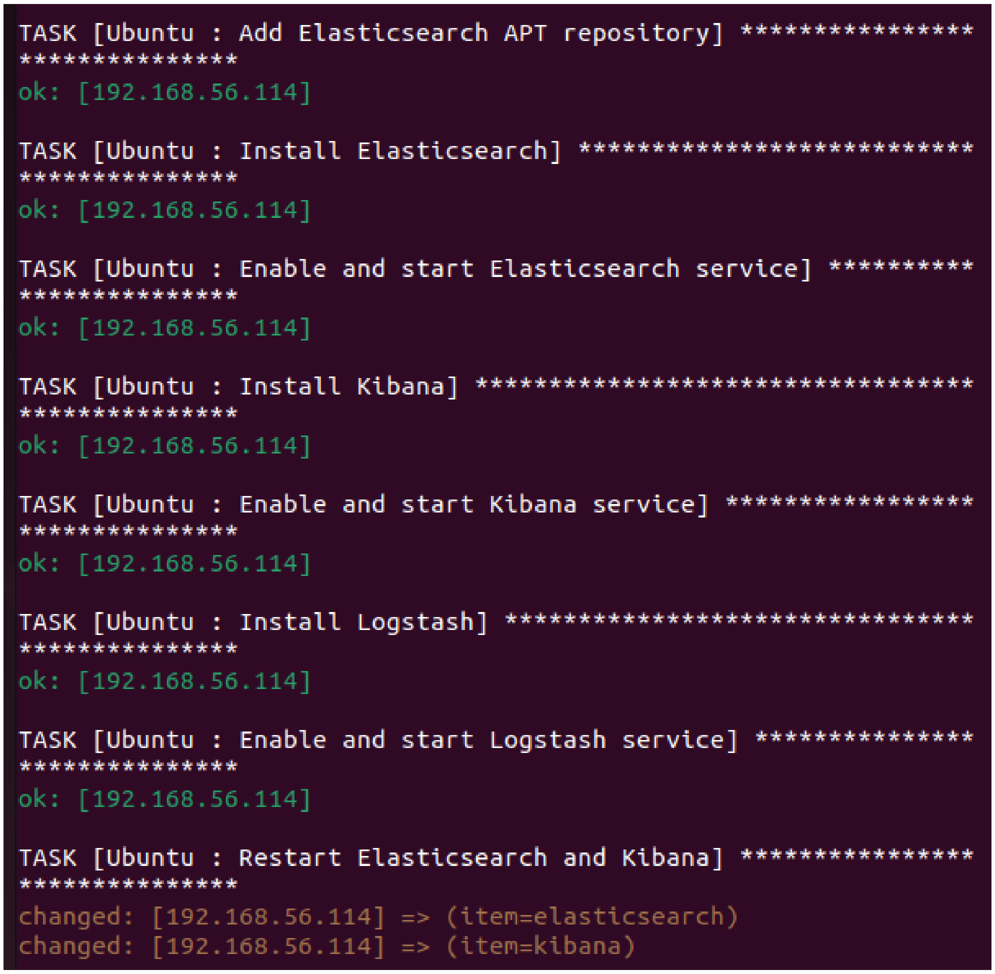
```
  GNU nano 6.2                  main.yml
    become: yes

  - 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
    become: yes

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

Explanation: In this playbook it will install updates, prerequisites, elasticsearch, kibana and logstash on Ubuntu server 1 and also on CentOS.

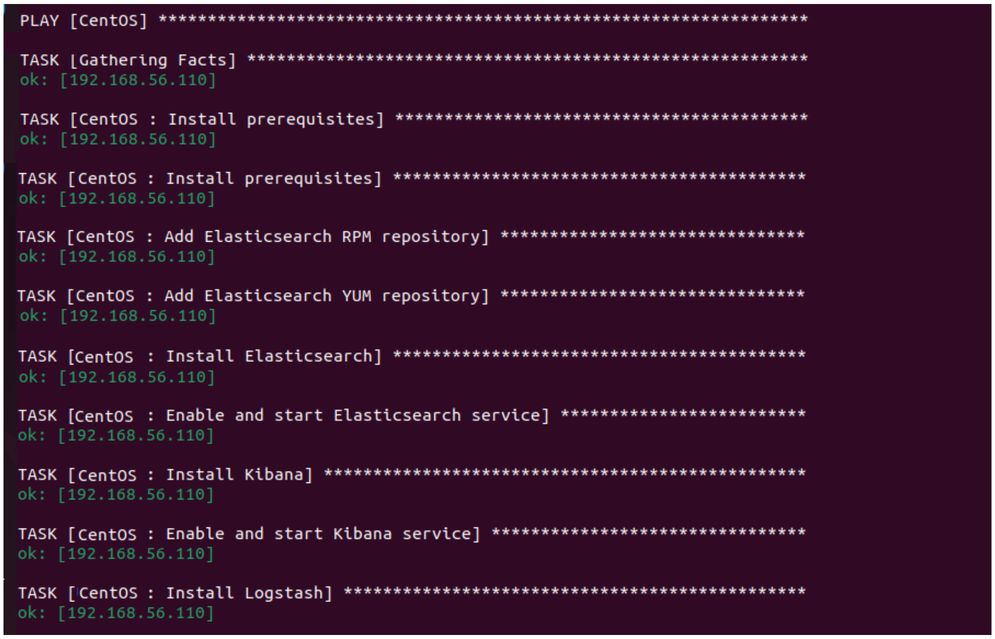
PROCESS



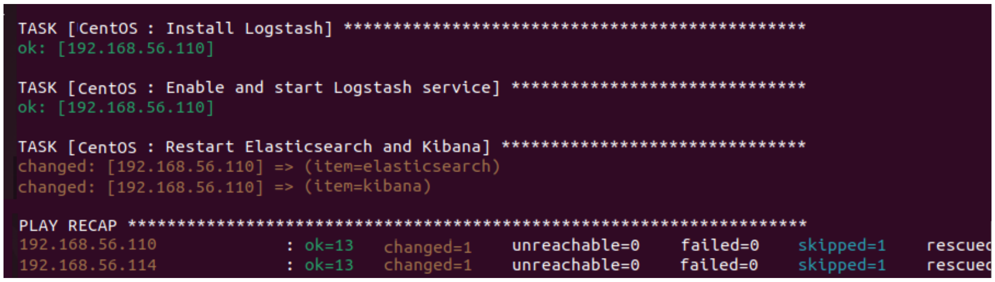
```
lykaandaya@managenode:~/HOA10.1$ ansible-playbook --ask-become-pa
ss install.yml
BECOME password:

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

TASK [Gathering Facts] *****************************************************
***************
        92.168.56.110]
ok: [192.168.56.114]

TASK [install updates (CentOS)] ********************************************
***************
skipping: [192.168.56.114]
ok: [192.168.56.110]

TASK [install updates (Ubuntu)] ********************************************
***************
skipping: [192.168.56.110]
ok: [192.168.56.114]

PLAY [Ubuntu] **************************************************************
***************

TASK [Gathering Facts] *****************************************************
***************
ok: [192.168.56.114]

TASK [Ubuntu : Install prerequisites] **************************************
***************
ok: [192.168.56.114]

TASK [Ubuntu : Add Elasticsearch APT repository key] ***********************
***************
ok: [192.168.56.114]
```



```
TASK [Ubuntu : Add Elasticsearch APT repository] *****************
***************
ok: [192.168.56.114]

TASK [Ubuntu : Install Elasticsearch] ***************************
***************
ok: [192.168.56.114]

TASK [Ubuntu : Enable and start Elasticsearch service] **********
***************
ok: [192.168.56.114]

TASK [Ubuntu : Install Kibana] **********************************
***************
ok: [192.168.56.114]

TASK [Ubuntu : Enable and start Kibana service] *****************
***************
ok: [192.168.56.114]

TASK [Ubuntu : Install Logstash] ********************************
***************
ok: [192.168.56.114]

TASK [Ubuntu : Enable and start Logstash service] ***************
***************
ok: [192.168.56.114]

TASK [Ubuntu : Restart Elasticsearch and Kibana] ****************
***************
changed: [192.168.56.114] => (item=elasticsearch)
changed: [192.168.56.114] => (item=kibana)
```



```
PLAY [CentOS] *******************************************************************

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

TASK [CentOS : Install prerequisites] *******************************************
ok: [192.168.56.110]

TASK [CentOS : Install prerequisites] *******************************************
ok: [192.168.56.110]

TASK [CentOS : Add Elasticsearch RPM repository] ********************************
ok: [192.168.56.110]

TASK [CentOS : Add Elasticsearch YUM repository] ********************************
ok: [192.168.56.110]

TASK [CentOS : Install Elasticsearch] *******************************************
ok: [192.168.56.110]

TASK [CentOS : Enable and start Elasticsearch service] **************************
ok: [192.168.56.110]

TASK [CentOS : Install Kibana] **************************************************
ok: [192.168.56.110]

TASK [CentOS : Enable and start Kibana service] *********************************
ok: [192.168.56.110]

TASK [CentOS : Install Logstash] ************************************************
ok: [192.168.56.110]
```

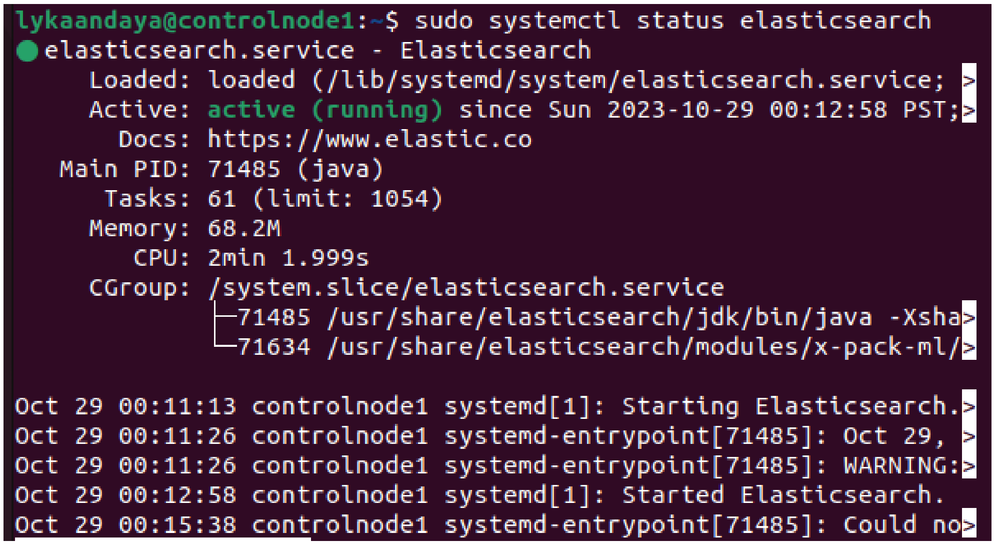


```
TASK [CentOS : Install Logstash] ***********************************************
ok: [192.168.56.110]

TASK [CentOS : Enable and start Logstash service] ******************************
ok: [192.168.56.110]

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

PLAY RECAP *********************************************************************
192.168.56.110             : ok=13   changed=1    unreachable=0    failed=0    skipped=1    rescued
192.168.56.114             : ok=13   changed=1    unreachable=0    failed=0    skipped=1    rescued
```

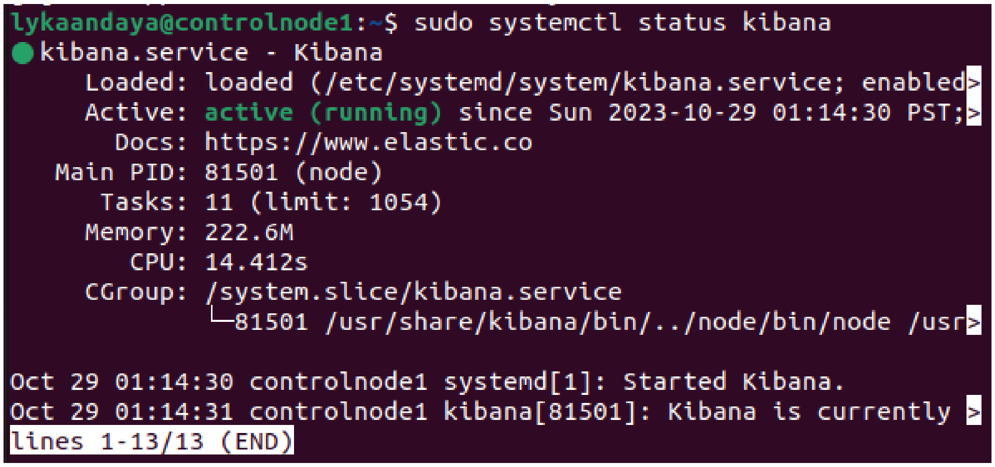
Explanation: It shows that it executed the instructions in the tasks of the playbook that I created

OUTPUT

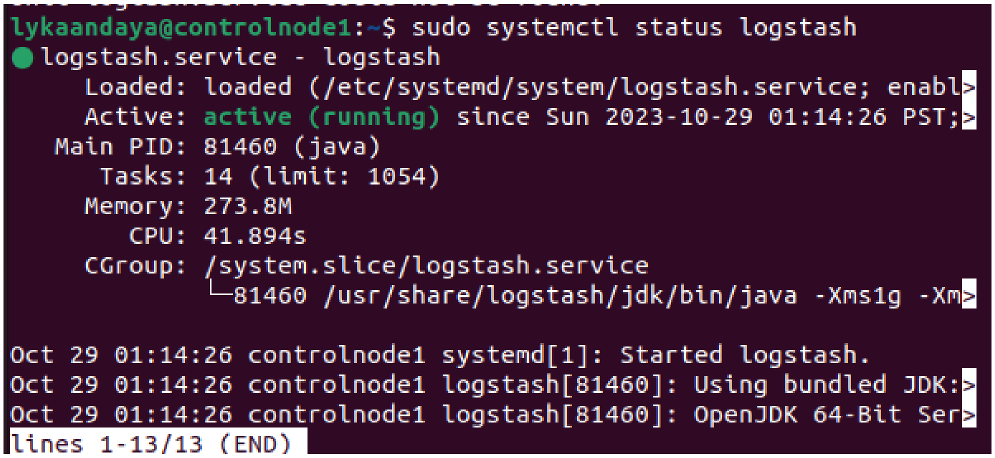
Ubuntu



```
lykaandaya@controlnode1:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; >
     Active: active (running) since Sun 2023-10-29 00:12:58 PST;>
       Docs: https://www.elastic.co
   Main PID: 71485 (java)
      Tasks: 61 (limit: 1054)
     Memory: 68.2M
        CPU: 2min 1.999s
     CGroup: /system.slice/elasticsearch.service
             ├─71485 /usr/share/elasticsearch/jdk/bin/java -Xsha>
             └─71634 /usr/share/elasticsearch/modules/x-pack-ml/>

Oct 29 00:11:13 controlnode1 systemd[1]: Starting Elasticsearch.>
Oct 29 00:11:26 controlnode1 systemd-entrypoint[71485]: Oct 29, >
Oct 29 00:11:26 controlnode1 systemd-entrypoint[71485]: WARNING:>
Oct 29 00:12:58 controlnode1 systemd[1]: Started Elasticsearch.
Oct 29 00:15:38 controlnode1 systemd-entrypoint[71485]: Could no>
```

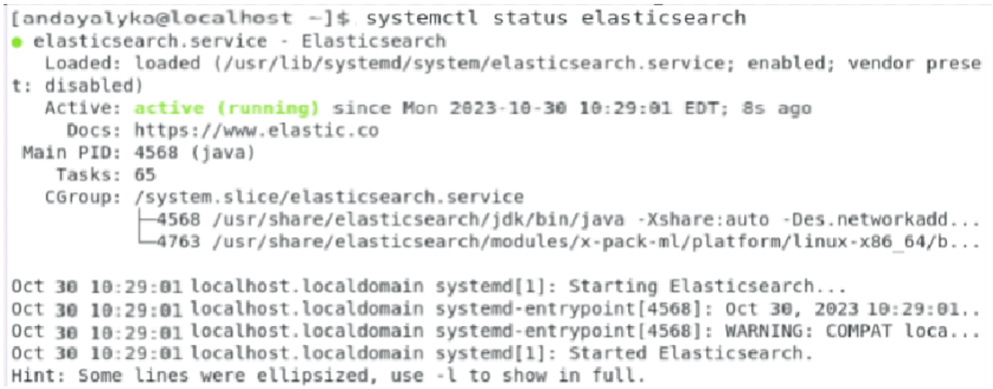


```
lykaandaya@controlnode1:~$ sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled>
     Active: active (running) since Sun 2023-10-29 01:14:30 PST;>
       Docs: https://www.elastic.co
   Main PID: 81501 (node)
      Tasks: 11 (limit: 1054)
     Memory: 222.6M
        CPU: 14.412s
     CGroup: /system.slice/kibana.service
             └─81501 /usr/share/kibana/bin/../node/bin/node /usr>

Oct 29 01:14:30 controlnode1 systemd[1]: Started Kibana.
Oct 29 01:14:31 controlnode1 kibana[81501]: Kibana is currently >
lines 1-13/13 (END)
```

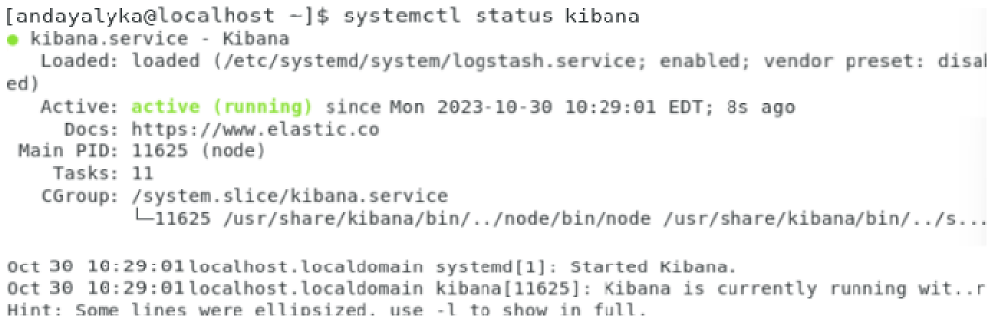


```
lykaandaya@controlnode1:~$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabl>
     Active: active (running) since Sun 2023-10-29 01:14:26 PST;>
   Main PID: 81460 (java)
      Tasks: 14 (limit: 1054)
     Memory: 273.8M
        CPU: 41.894s
     CGroup: /system.slice/logstash.service
             └─81460 /usr/share/logstash/jdk/bin/java -Xms1g -Xm>

Oct 29 01:14:26 controlnode1 systemd[1]: Started logstash.
Oct 29 01:14:26 controlnode1 logstash[81460]: Using bundled JDK:>
Oct 29 01:14:26 controlnode1 logstash[81460]: OpenJDK 64-Bit Ser>
lines 1-13/13 (END)
```

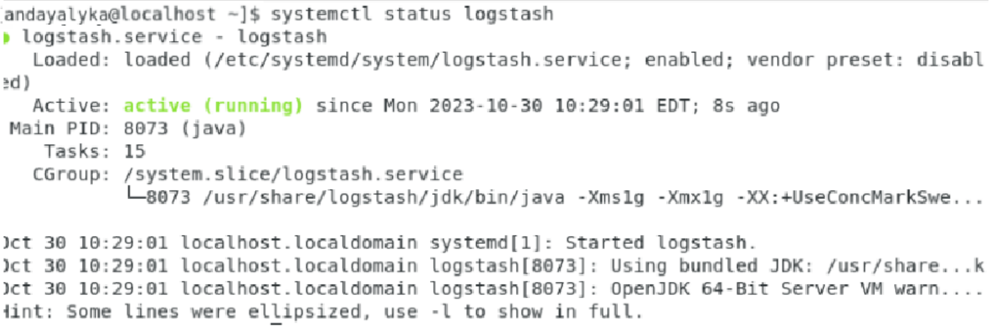
CentOS



```
[andayalyka@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 2023-10-30 10:29:01 EDT; 8s ago
     Docs: https://www.elastic.co
 Main PID: 4568 (java)
    Tasks: 65
   CGroup: /system.slice/elasticsearch.service
           ├─4568 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkadd...
           └─4763 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/b...

Oct 30 10:29:01 localhost.localdomain systemd[1]: Starting Elasticsearch...
Oct 30 10:29:01 localhost.localdomain systemd-entrypoint[4568]: Oct 30, 2023 10:29:01..
Oct 30 10:29:01 localhost.localdomain systemd-entrypoint[4568]: WARNING: COMPAT loca...
Oct 30 10:29:01 localhost.localdomain systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
```

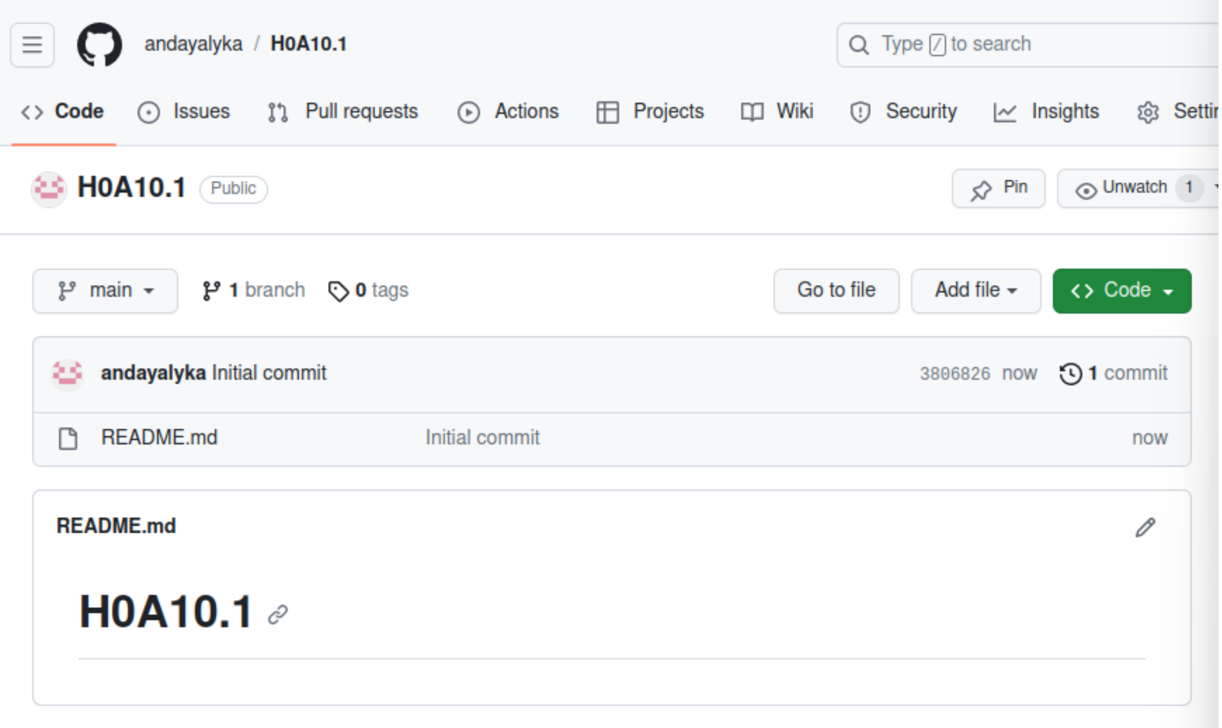


```
[andayalyka@localhost ~]$ systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disal
ed)
   Active: active (running) since Mon 2023-10-30 10:29:01 EDT; 8s ago
     Docs: https://www.elastic.co
 Main PID: 11625 (node)
    Tasks: 11
   CGroup: /system.slice/kibana.service
           └─11625 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../s...

Oct 30 10:29:01localhost.localdomain systemd[1]: Started Kibana.
Oct 30 10:29:01localhost.localdomain kibana[11625]: Kibana is currently running wit..r
Hint: Some lines were ellipsized, use -l to show in full.
```

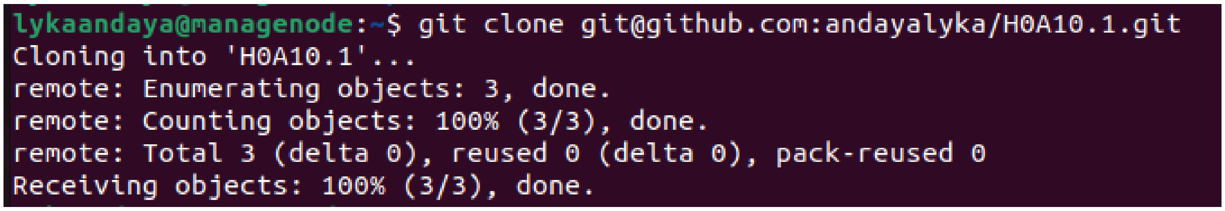


```
andayalyka@localhost ~]$ systemctl status logstash
 logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabl
ed)
   Active: active (running) since Mon 2023-10-30 10:29:01 EDT; 8s ago
 Main PID: 8073 (java)
    Tasks: 15
   CGroup: /system.slice/logstash.service
           └─8073 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSwe...

)ct 30 10:29:01 localhost.localdomain systemd[1]: Started logstash.
)ct 30 10:29:01 localhost.localdomain logstash[8073]: Using bundled JDK: /usr/share...k
)ct 30 10:29:01 localhost.localdomain logstash[8073]: OpenJDK 64-Bit Server VM warn....
Hint: Some lines were ellipsized, use -l to show in full.
```

Explanation: In Ubuntu, it indicates that elasticsearch, kibana and logstash are installed and the service is currently active and running. Also, in CentOS, elasticsearch, kibana, and logstash are installed and its service is also active and running.

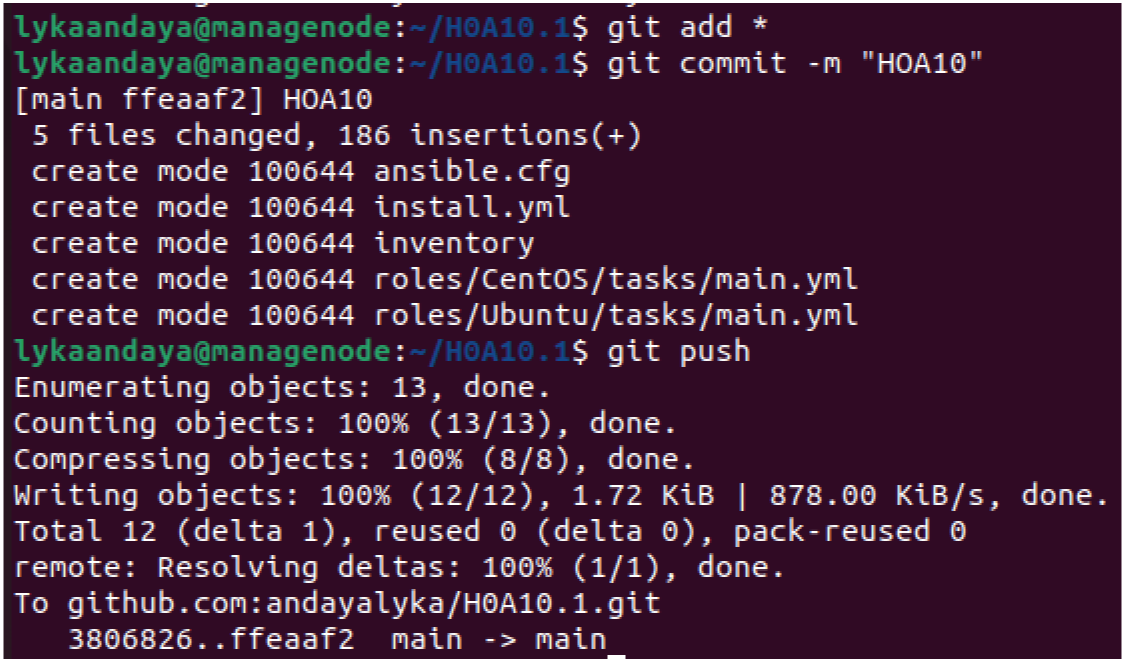


Explanation: I created a new repository named H0A10.1



```
lykaandaya@managenode:~$ git clone git@github.com:andayalyka/H0A10.1.git
Cloning into 'H0A10.1'...
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.
```

Explanation: cloning the created repository in github to the virtual machine



```
lykaandaya@managenode:~/H0A10.1$ git add *
lykaandaya@managenode:~/H0A10.1$ git commit -m "HOA10"
[main ffeaaf2] HOA10
 5 files changed, 186 insertions(+)
 create mode 100644 ansible.cfg
 create mode 100644 install.yml
 create mode 100644 inventory
 create mode 100644 roles/CentOS/tasks/main.yml
 create mode 100644 roles/Ubuntu/tasks/main.yml
lykaandaya@managenode:~/H0A10.1$ git push
Enumerating objects: 13, done.
Counting objects: 100% (13/13), done.
Compressing objects: 100% (8/8), done.
Writing objects: 100% (12/12), 1.72 KiB | 878.00 KiB/s, done.
Total 12 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), done.
To github.com:andayalyka/H0A10.1.git
   3806826..ffeaaf2  main -> main
```

Explanation: It shows that it pushes the 5 files that I created and it has a commit message “HOA10”.

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool?
   - A log monitoring tool provides essential advantages for system administrators and developers. It furnishes immediate insight into system events, allowing swift identification of errors, irregularities, or security breaches. This proactive strategy reduces downtime and improves system dependability. Furthermore, log monitoring assists in problem-solving and determining the underlying causes of issues, hastening their resolution. It plays a pivotal role in upholding compliance and auditing standards, ensuring alignment with industry regulations. It also assists in streamlining performance by identifying bottlenecks or resource-intensive operations. In conclusion, a log monitoring tool is critical for maintaining a safe, dependable, and effective IT infrastructure that allows organizations to run easily and securely.

Conclusions:

Through the process of devising and structuring a workflow for log monitoring using Ansible, I will acquire the knowledge to streamline the setup, configuration, and administration of log monitoring tools in a corporate context. This involves grasping the fundamentals of Infrastructure as Code (IaC) and recognizing Ansible as a potent instrument for this purpose.

The initial step involves comprehending the architecture and prerequisites of log monitoring systems. This encompasses the careful selection of suitable log monitoring tools tailored to the specific requirements of the enterprise. Subsequently, I will delve into Ansible, mastering the creation of playbooks, task definition, and role organization, establishing the groundwork for my automated process.

This endeavor underscores the importance of adhering to best practices when deploying and configuring log monitoring solutions. I will address vital elements such as handling dependencies, safeguarding communications, and ensuring seamless integration with existing infrastructure.

Additionally, I will develop proficiency in the efficient management of logs, including strategies for data retention, analysis, and timely alerting. This involves establishing custom rules and triggers to promptly identify critical events.

Active participation in this endeavor will equip me with hands-on expertise in crafting and executing automated workflows with Ansible. This practical skill set is invaluable for optimizing log monitoring procedures, fortifying security measures, and guaranteeing the dependability of crucial systems within a corporate environment.