Name: Espiritu, Diego Angelo Espiritu	**Date Performed: 10/23/2023**
Course/Section: CPE232/CPE31S6	**Date Submitted: 10/23/2023**
Instructor: Dr. Jonathan Vidal Taylar	**Semester and SY: 1st sem 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.

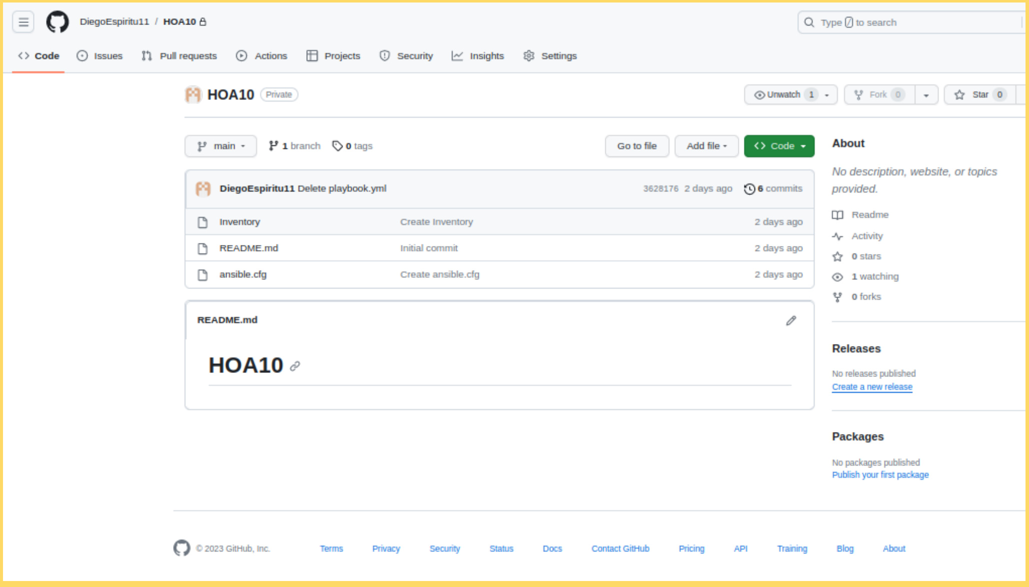
Source: https://www.graylog.org/products/open-source

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)

Step 1: Create a repository in github.



HOA10 Private

1 branch 0 tags

DiegoEspiritu11 Delete playbook.yml 3628176 2 days ago 6 commits

Inventory	Create Inventory	2 days ago
README.md	Initial commit	2 days ago
ansible.cfg	Create ansible.cfg	2 days ago

README.md

HOA10

About

No description, website, or topics provided.

Readme
Activity
0 stars
1 watching
0 forks

Releases

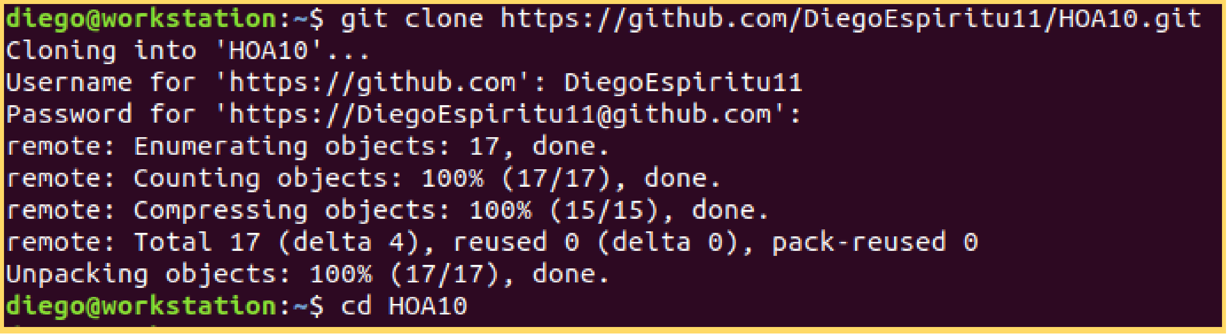
No releases published
Create a new release

Packages

No packages published
Publish your first package

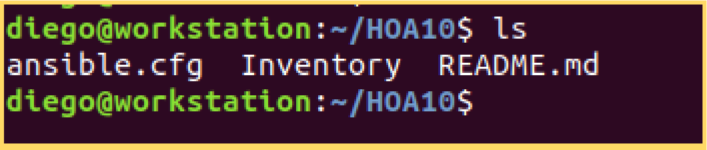
© 2023 GitHub, Inc. Terms Privacy Security Status Docs Contact GitHub Pricing API Training Blog About

Step 2: Clone the created repository.



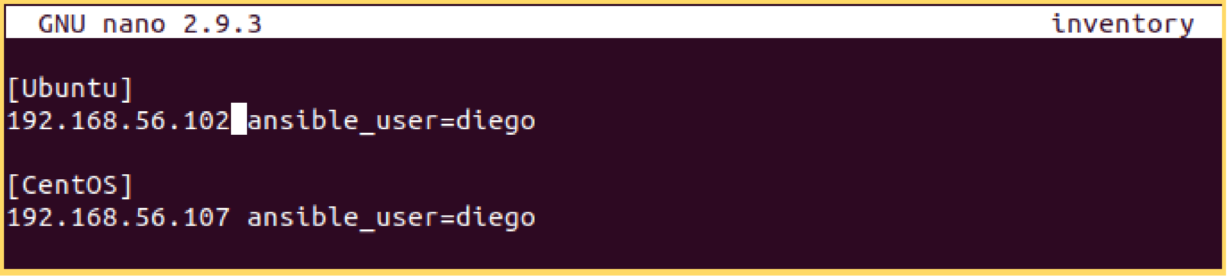
```
diego@workstation:~$ git clone https://github.com/DiegoEspiritu11/HOA10.git
Cloning into 'HOA10'...
Username for 'https://github.com': DiegoEspiritu11
Password for 'https://DiegoEspiritu11@github.com':
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 17 (delta 4), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (17/17), done.
diego@workstation:~$ cd HOA10
```

Step 3: Creating a file inside the directory (ansible.cfg, inventory).



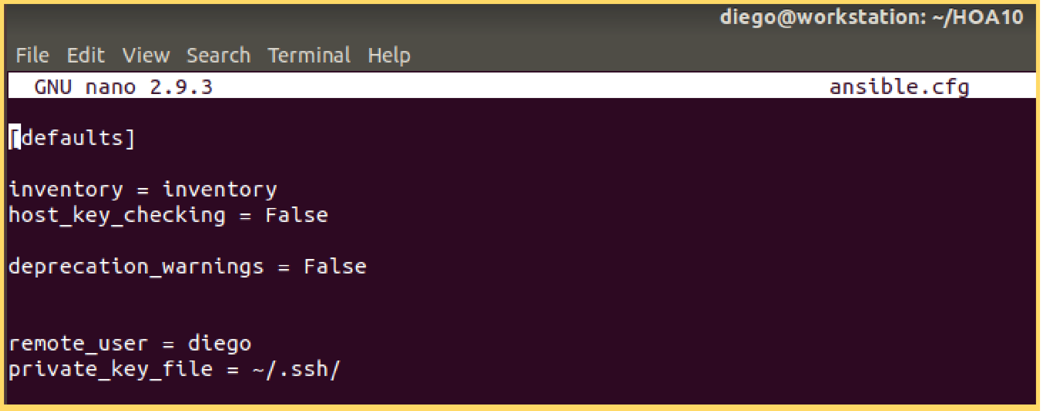
```
diego@workstation:~/HOA10$ ls
ansible.cfg  Inventory  README.md
diego@workstation:~/HOA10$
```

Step 4: Put the ip address of server1 and CentOS in the inventory.



```
  GNU nano 2.9.3                                              inventory

[Ubuntu]
192.168.56.102 ansible_user=diego

[CentOS]
192.168.56.107 ansible_user=diego
```

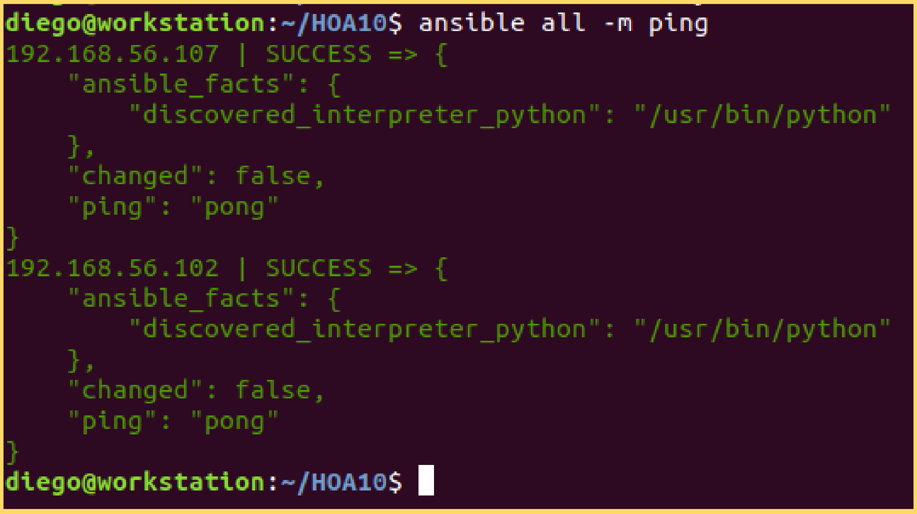
Step 5: Necessary file for ansible.cfg



diego@workstation: ~/HOA10
File Edit View Search Terminal Help

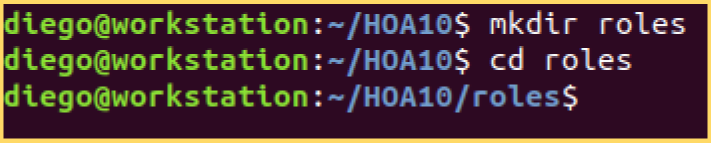
```
  GNU nano 2.9.3                                  ansible.cfg

[defaults]

inventory = inventory
host_key_checking = False

deprecation_warnings = False


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

Step 6: Ping the servers in ansible to make sure it is working and connected.



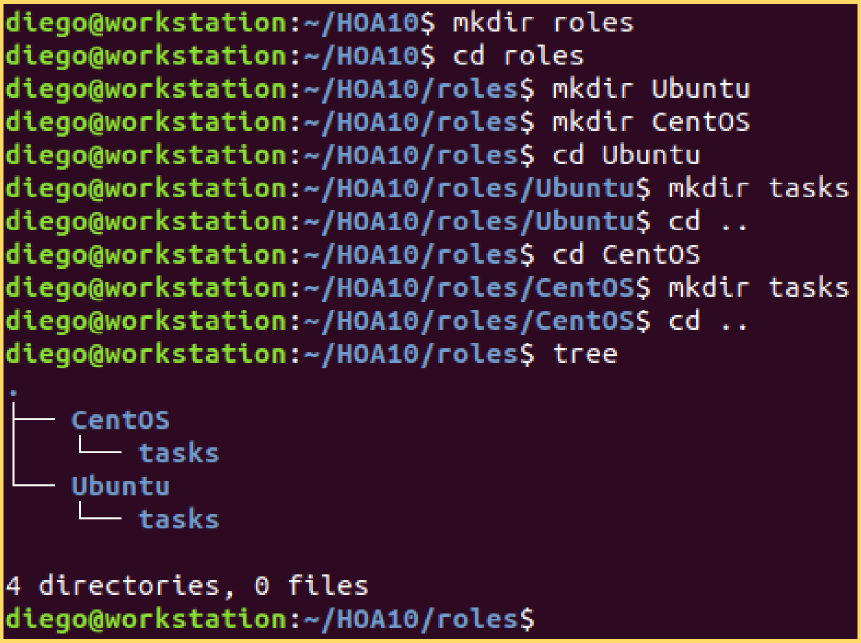
```
diego@workstation:~/HOA10$ ansible all -m ping
192.168.56.107 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python"
    },
    "changed": false,
    "ping": "pong"
}
192.168.56.102 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python"
    },
    "changed": false,
    "ping": "pong"
}
diego@workstation:~/HOA10$ 
```

Step 7: Apply the concept of creating roles under the same directory, create a new directory and name it roles.



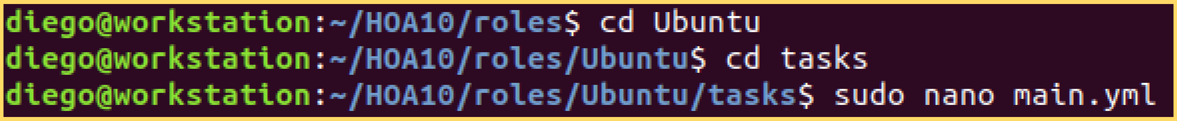
```
diego@workstation:~/HOA10$ mkdir roles
diego@workstation:~/HOA10$ cd roles
diego@workstation:~/HOA10/roles$
```

Step 8: Create new directories: Ubuntu, CentOS. For each directory, create a directory and name it tasks.

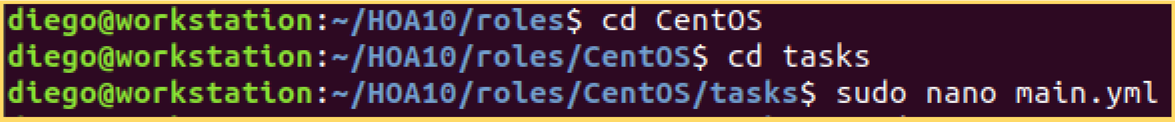


```
diego@workstation:~/HOA10$ mkdir roles
diego@workstation:~/HOA10$ cd roles
diego@workstation:~/HOA10/roles$ mkdir Ubuntu
diego@workstation:~/HOA10/roles$ mkdir CentOS
diego@workstation:~/HOA10/roles$ cd Ubuntu
diego@workstation:~/HOA10/roles/Ubuntu$ mkdir tasks
diego@workstation:~/HOA10/roles/Ubuntu$ cd ..
diego@workstation:~/HOA10/roles$ cd CentOS
diego@workstation:~/HOA10/roles/CentOS$ mkdir tasks
diego@workstation:~/HOA10/roles/CentOS$ cd ..
diego@workstation:~/HOA10/roles$ tree
.
├── CentOS
│   └── tasks
└── Ubuntu
    └── tasks

4 directories, 0 files
diego@workstation:~/HOA10/roles$
```

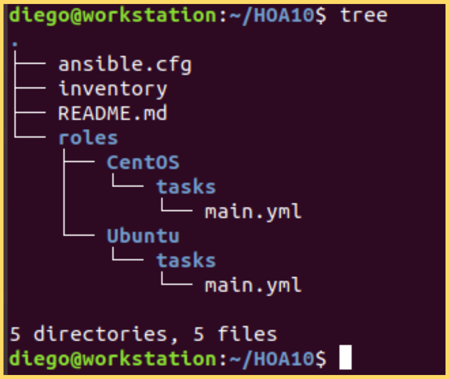
Step 9: Go to tasks for all directory and create a file. Name it main.yml for each of the tasks for all directories.



```
diego@workstation:~/HOA10/roles$ cd Ubuntu
diego@workstation:~/HOA10/roles/Ubuntu$ cd tasks
diego@workstation:~/HOA10/roles/Ubuntu/tasks$ sudo nano main.yml
```

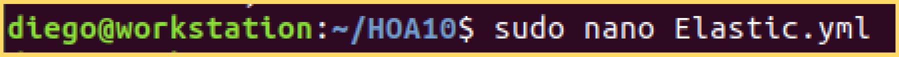


```
diego@workstation:~/HOA10/roles$ cd CentOS
diego@workstation:~/HOA10/roles/CentOS$ cd tasks
diego@workstation:~/HOA10/roles/CentOS/tasks$ sudo nano main.yml
```

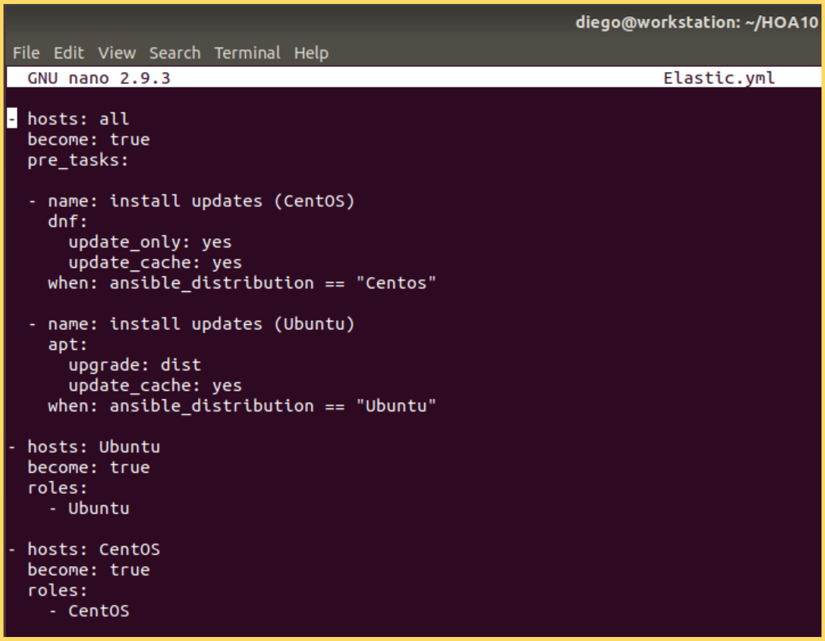


```
diego@workstation:~/HOA10$ tree
.
├── ansible.cfg
├── inventory
├── README.md
└── roles
    ├── CentOS
    │   └── tasks
    │       └── main.yml
    └── Ubuntu
        └── tasks
            └── main.yml

5 directories, 5 files
diego@workstation:~/HOA10$
```

Step 10: Create a file inside of the main directory (HOA10) and name it Elastic.yml, create a playbook for running the installation of ElasticSearch, Kibana, Logstash in both Ubuntu and CentOS.



```
diego@workstation:~/HOA10$ sudo nano Elastic.yml
```

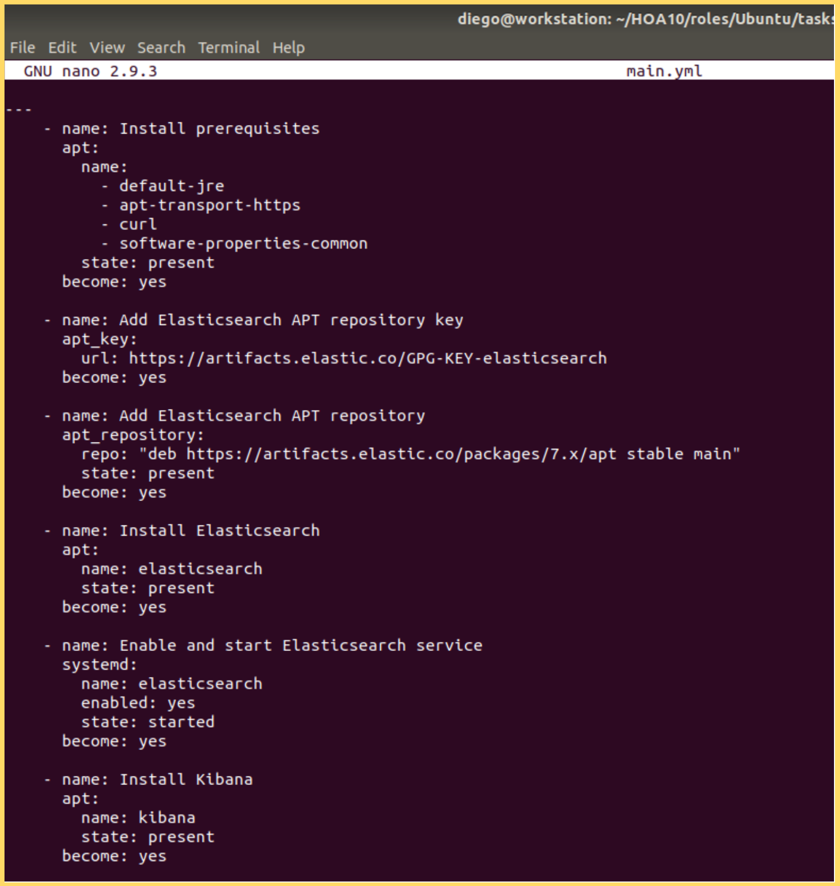


diego@workstation: ~/HOA10
File Edit View Search Terminal Help

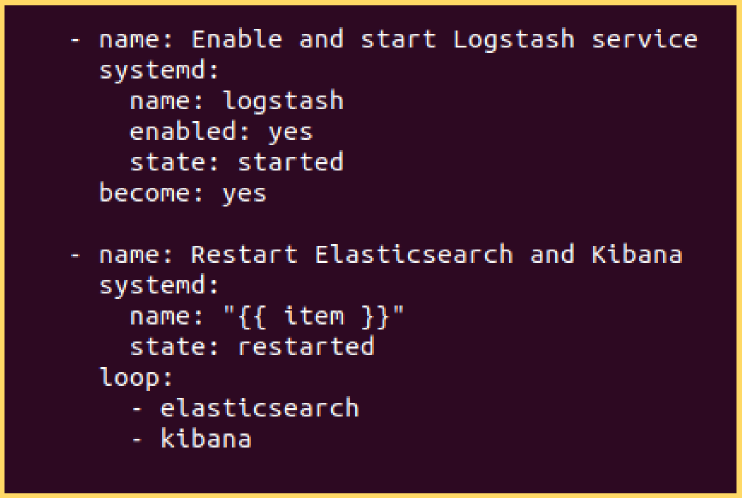
```
  GNU nano 2.9.3                                        Elastic.yml

- 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
```

Step 11: Create a playbook in main.yml for both Ubuntu and CentOS for the installation of ElasticSearch, Kibana, Logstash in Ubuntu and CentOS.

Ubuntu:

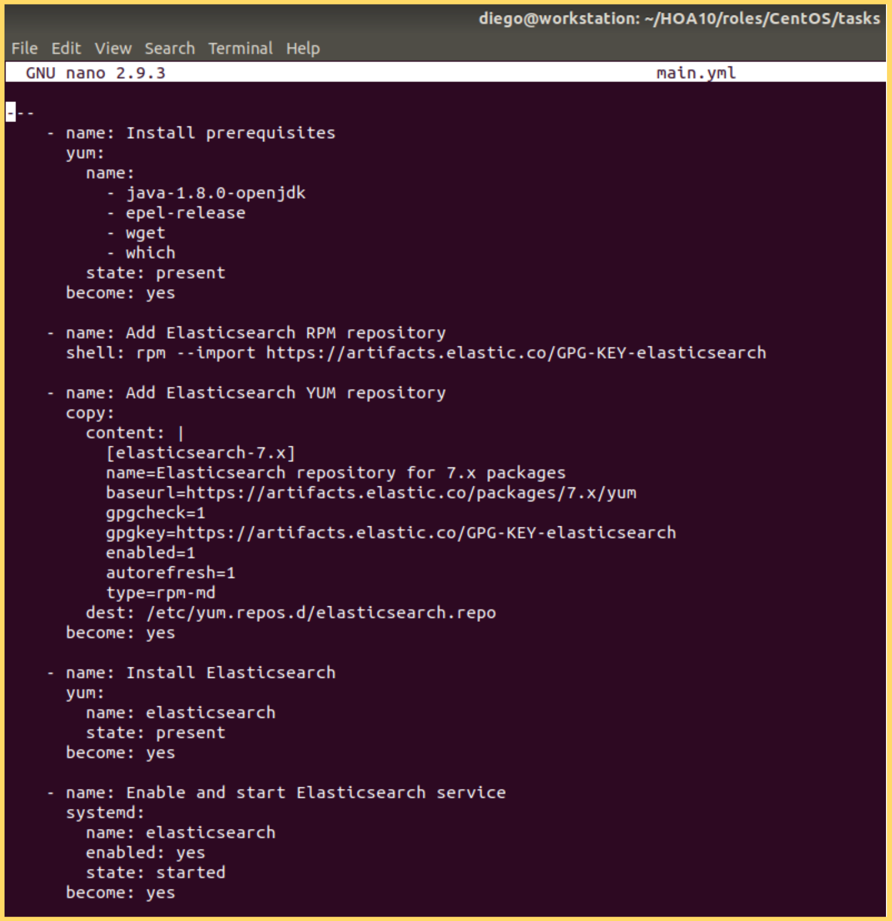

diego@workstation: ~/HOA10/roles/Ubuntu/task
File Edit View Search Terminal Help

```
  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
```

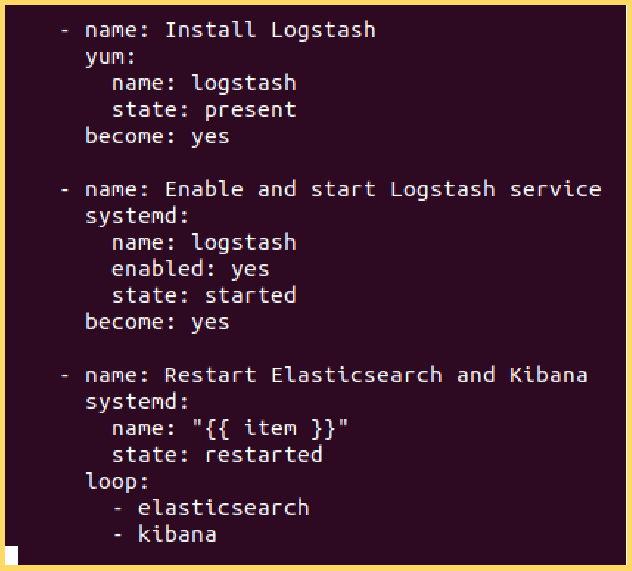


```
    - name: Enable and start Logstash service
      systemd:
        name: logstash
        enabled: yes
        state: started
      become: yes

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

CentOS:

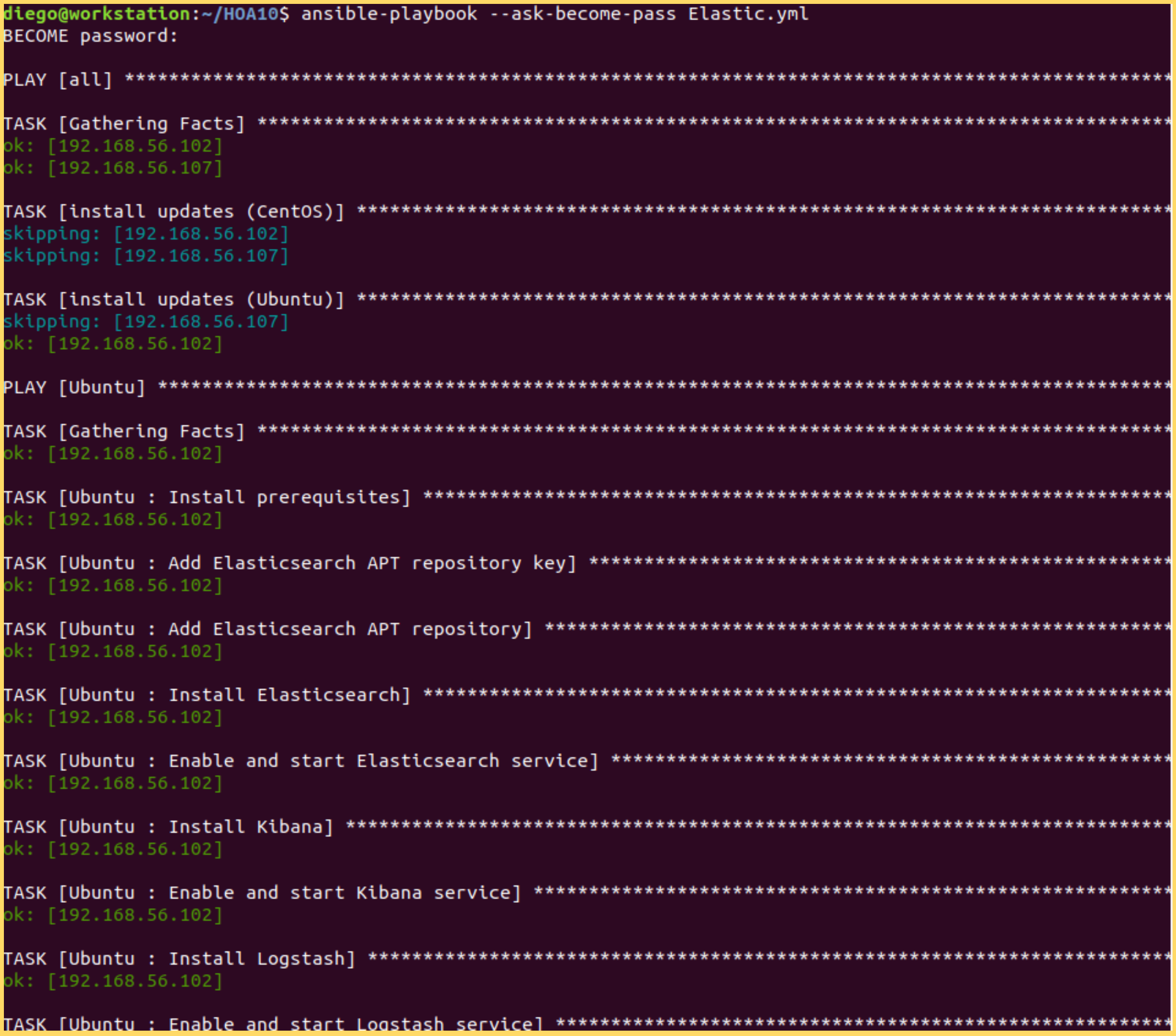

diego@workstation: ~/HOA10/roles/CentOS/tasks
File Edit View Search Terminal Help

```
  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
          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
```

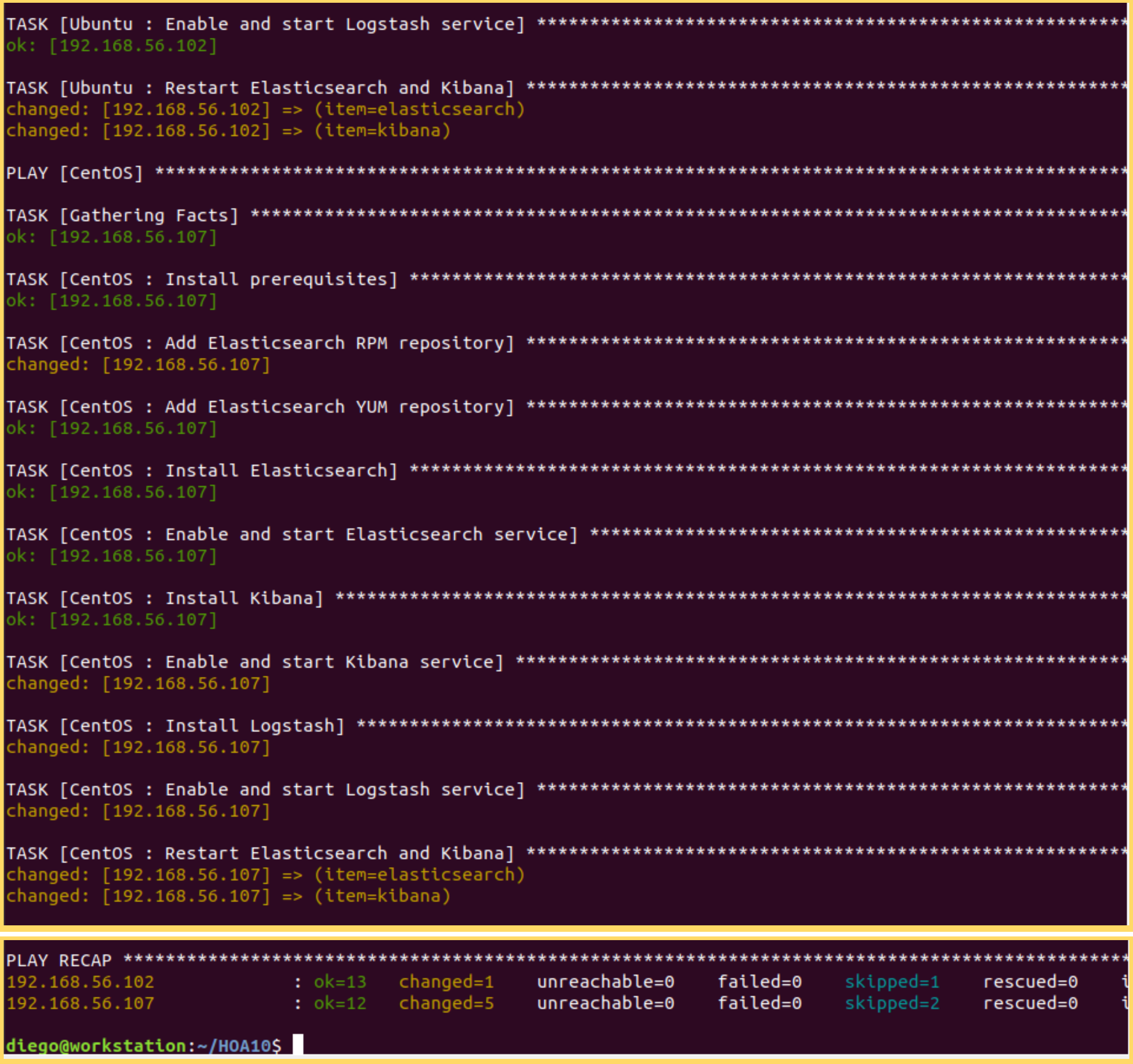


```
    - name: Install Logstash
      yum:
        name: logstash
        state: present
      become: yes

    - 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
```

Step 12: Run the created playbook in the main directory.



```
diego@workstation:~/HOA10$ ansible-playbook --ask-become-pass Elastic.yml
BECOME password:

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

TASK [Gathering Facts] *******************************************************************************
ok: [192.168.56.102]
ok: [192.168.56.107]

TASK [install updates (CentOS)] **********************************************************************
skipping: [192.168.56.102]
skipping: [192.168.56.107]

TASK [install updates (Ubuntu)] **********************************************************************
skipping: [192.168.56.107]
ok: [192.168.56.102]

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

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

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

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

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

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

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

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

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

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

TASK [Ubuntu : Enable and start Logstash service] ****************************************************
```

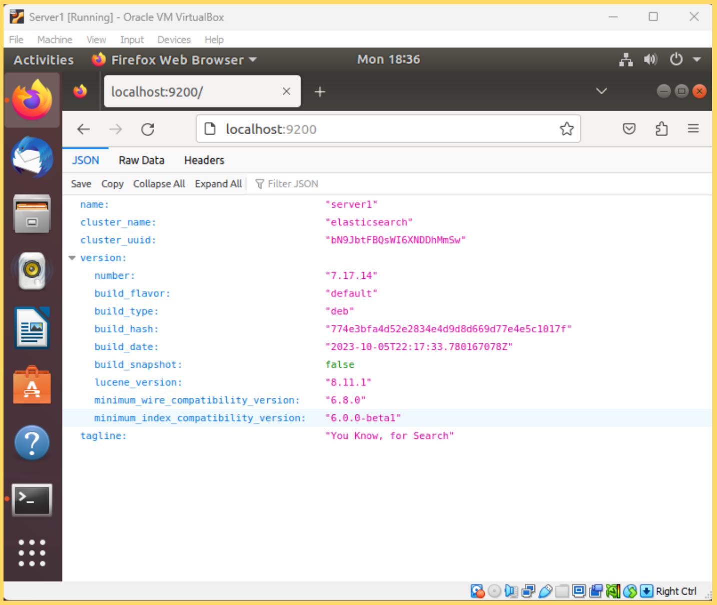


```
TASK [Ubuntu : Enable and start Logstash service] *******************************************************
ok: [192.168.56.102]

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: [192.168.56.107]

TASK [CentOS : Install prerequisites] *******************************************************************
ok: [192.168.56.107]

TASK [CentOS : Add Elasticsearch RPM repository] ********************************************************
changed: [192.168.56.107]

TASK [CentOS : Add Elasticsearch YUM repository] ********************************************************
ok: [192.168.56.107]

TASK [CentOS : Install Elasticsearch] *******************************************************************
ok: [192.168.56.107]

TASK [CentOS : Enable and start Elasticsearch service] **************************************************
ok: [192.168.56.107]

TASK [CentOS : Install Kibana] **************************************************************************
ok: [192.168.56.107]

TASK [CentOS : Enable and start Kibana service] *********************************************************
changed: [192.168.56.107]

TASK [CentOS : Install Logstash] ************************************************************************
changed: [192.168.56.107]

TASK [CentOS : Enable and start Logstash service] *******************************************************
changed: [192.168.56.107]

TASK [CentOS : Restart Elasticsearch and Kibana] ********************************************************
changed: [192.168.56.107] => (item=elasticsearch)
changed: [192.168.56.107] => (item=kibana)
```

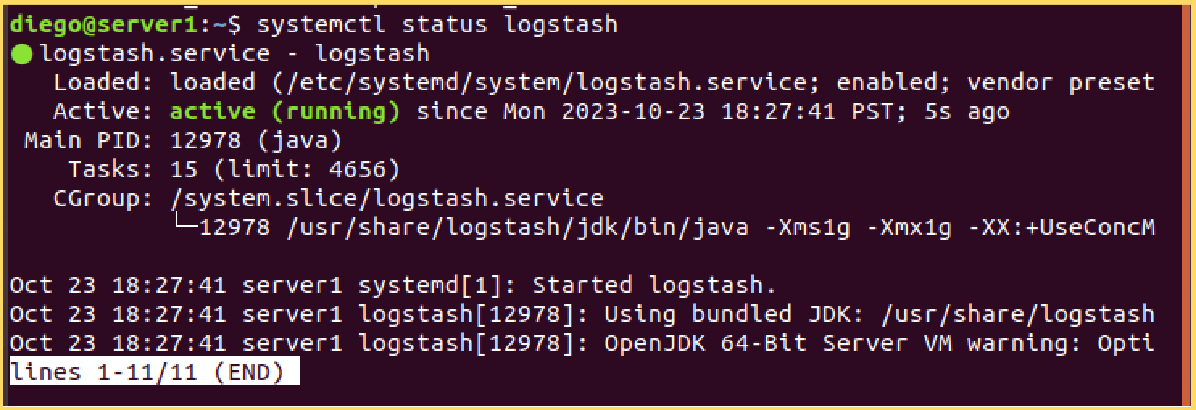
```
PLAY RECAP **********************************************************************************************
192.168.56.102             : ok=13   changed=1    unreachable=0    failed=0    skipped=1    rescued=0    i
192.168.56.107             : ok=12   changed=5    unreachable=0    failed=0    skipped=2    rescued=0    i

diego@workstation:~/HOA10$ 
```

OUTPUT:

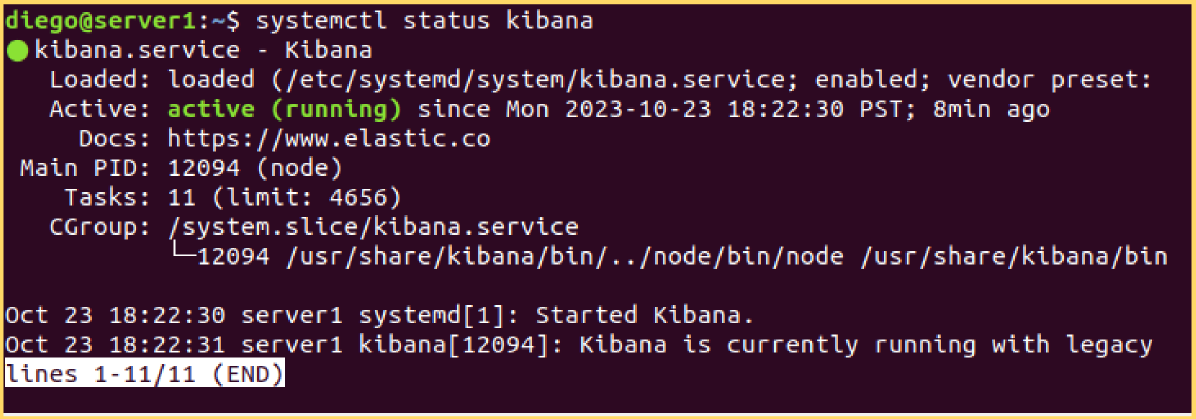
Ubuntu:



```
name:                                   "server1"
cluster_name:                           "elasticsearch"
cluster_uuid:                           "bN9JbtFBQsWI6XNDDhMmSw"
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"
```

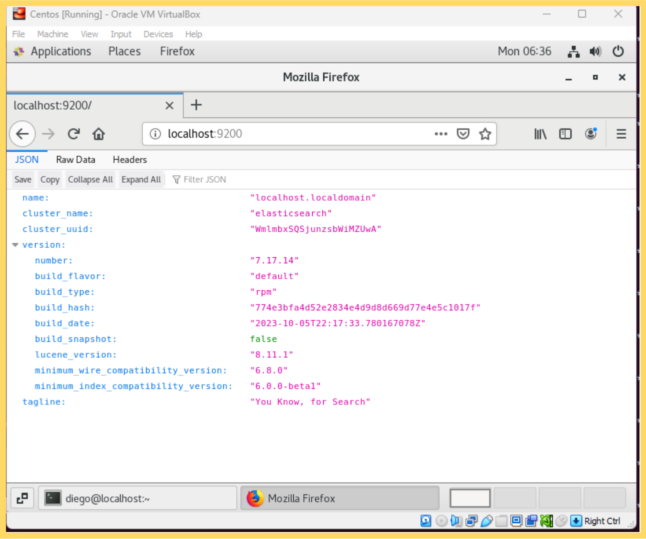


```
diego@server1:~$ systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset
     Active: active (running) since Mon 2023-10-23 18:27:41 PST; 5s ago
   Main PID: 12978 (java)
      Tasks: 15 (limit: 4656)
     CGroup: /system.slice/logstash.service
             └─12978 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcM

Oct 23 18:27:41 server1 systemd[1]: Started logstash.
Oct 23 18:27:41 server1 logstash[12978]: Using bundled JDK: /usr/share/logstash
Oct 23 18:27:41 server1 logstash[12978]: OpenJDK 64-Bit Server VM warning: Opti
lines 1-11/11 (END)
```

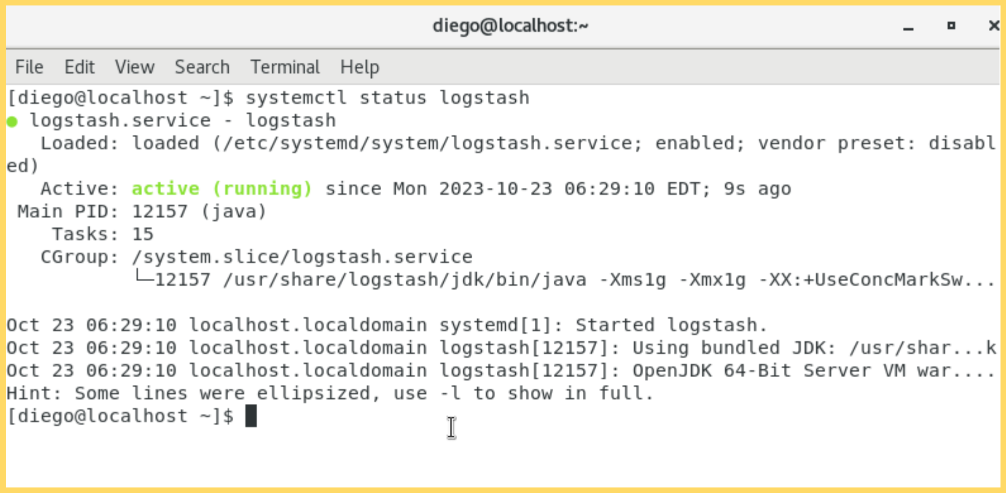


```
diego@server1:~$ systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset:
     Active: active (running) since Mon 2023-10-23 18:22:30 PST; 8min ago
       Docs: https://www.elastic.co
   Main PID: 12094 (node)
      Tasks: 11 (limit: 4656)
     CGroup: /system.slice/kibana.service
             └─12094 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin

Oct 23 18:22:30 server1 systemd[1]: Started Kibana.
Oct 23 18:22:31 server1 kibana[12094]: Kibana is currently running with legacy
lines 1-11/11 (END)
```

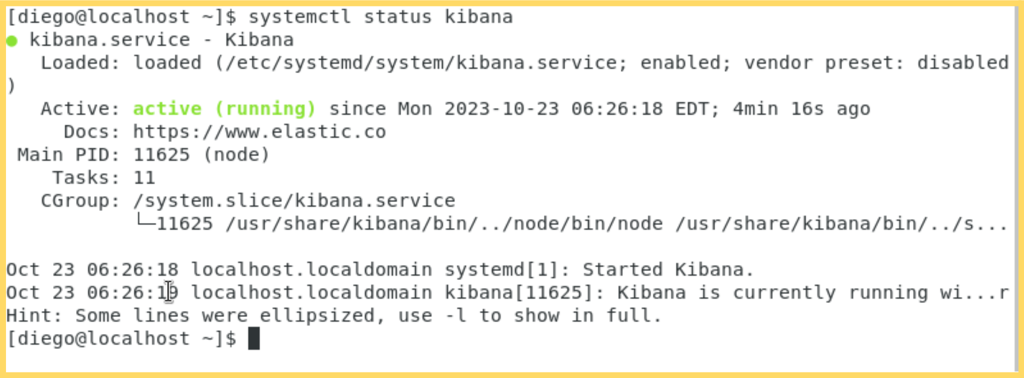
CentOS:


Centos [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Firefox
Mon 06:36
Mozilla Firefox
localhost:9200/
localhost:9200
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
diego@localhost:~
Mozilla Firefox
Right Ctrl

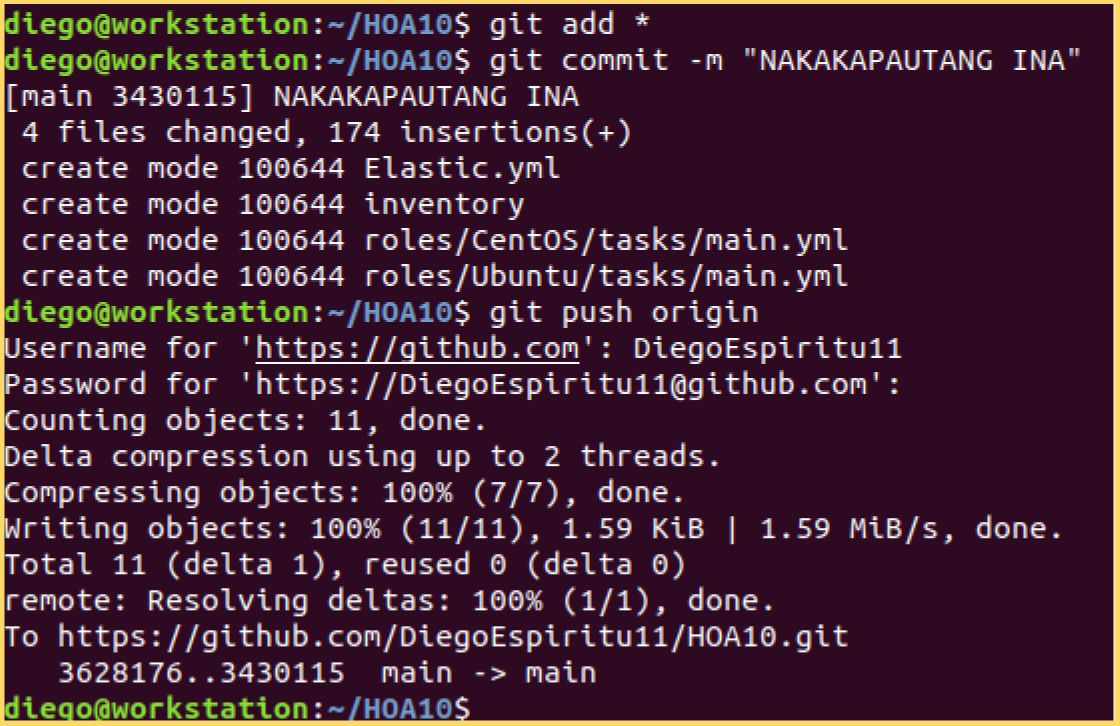
```
name:                                     "localhost.localdomain"
cluster_name:                             "elasticsearch"
cluster_uuid:                             "WmlmbxSQSjunzsbWiMZUwA"
▼ version:
   number:                                "7.17.14"
   build_flavor:                          "default"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



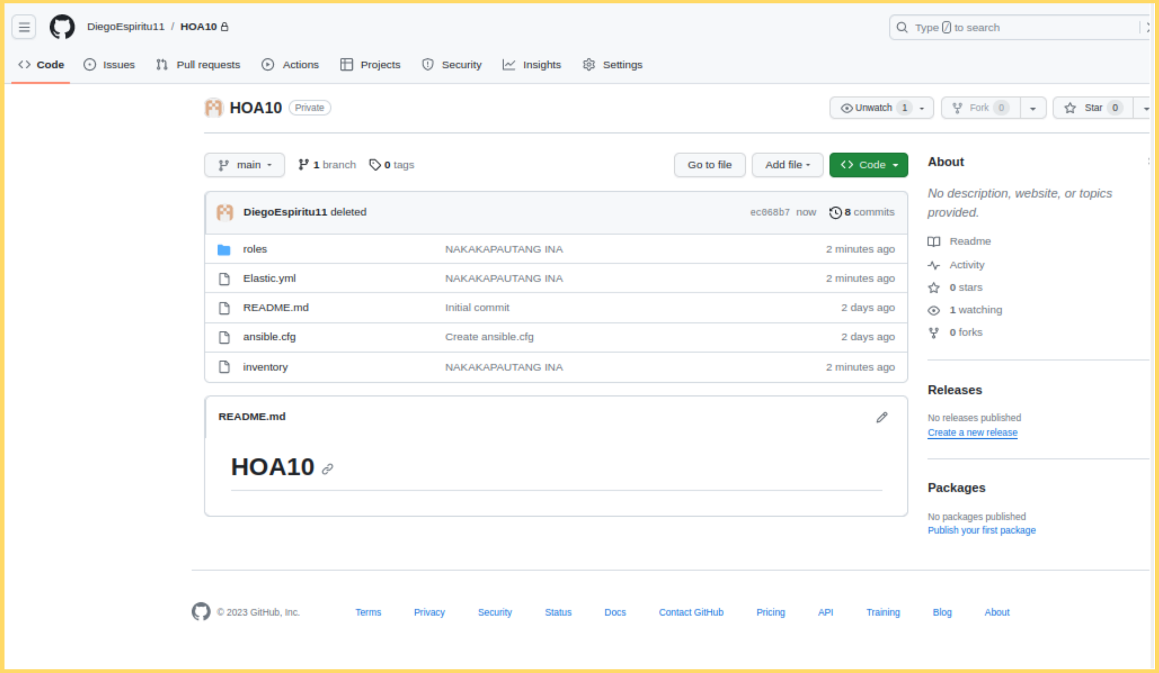
```
[diego@localhost ~]$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabl
ed)
   Active: active (running) since Mon 2023-10-23 06:29:10 EDT; 9s ago
 Main PID: 12157 (java)
    Tasks: 15
   CGroup: /system.slice/logstash.service
           └─12157 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSw...

Oct 23 06:29:10 localhost.localdomain systemd[1]: Started logstash.
Oct 23 06:29:10 localhost.localdomain logstash[12157]: Using bundled JDK: /usr/shar...k
Oct 23 06:29:10 localhost.localdomain logstash[12157]: OpenJDK 64-Bit Server VM war....
Hint: Some lines were ellipsized, use -l to show in full.
[diego@localhost ~]$ █
```



```
[diego@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 06:26:18 EDT; 4min 16s 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 23 06:26:18 localhost.localdomain systemd[1]: Started Kibana.
Oct 23 06:26:18 localhost.localdomain kibana[11625]: Kibana is currently running wi...r
Hint: Some lines were ellipsized, use -l to show in full.
[diego@localhost ~]$ █
```



```
diego@workstation:~/HOA10$ git add *
diego@workstation:~/HOA10$ git commit -m "NAKAKAPAUTANG INA"
[main 3430115] NAKAKAPAUTANG INA
 4 files changed, 174 insertions(+)
 create mode 100644 Elastic.yml
 create mode 100644 inventory
 create mode 100644 roles/CentOS/tasks/main.yml
 create mode 100644 roles/Ubuntu/tasks/main.yml
diego@workstation:~/HOA10$ git push origin
Username for 'https://github.com': DiegoEspiritu11
Password for 'https://DiegoEspiritu11@github.com':
Counting objects: 11, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (7/7), done.
Writing objects: 100% (11/11), 1.59 KiB | 1.59 MiB/s, done.
Total 11 (delta 1), reused 0 (delta 0)
remote: Resolving deltas: 100% (1/1), done.
To https://github.com/DiegoEspiritu11/HOA10.git
   3628176..3430115  main -> main
diego@workstation:~/HOA10$
```



DiegoEspiritu11 deleted ec068b7 now 8 commits

roles	NAKAKAPAUTANG INA	2 minutes ago
Elastic.yml	NAKAKAPAUTANG INA	2 minutes ago
README.md	Initial commit	2 days ago
ansible.cfg	Create ansible.cfg	2 days ago
inventory	NAKAKAPAUTANG INA	2 minutes ago

README.md

HOA10

About

No description, website, or topics provided.

github.com/DiegoEspiritu11/HOA10

Reflections:

Answer the following:

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

   -The advantages of using a log monitoring tool are that it has a specific function, such as Logstash, which can handle the pipeline that takes in data from various sources, transforms it, and sends it to Elasticsearch. Elasticsearch is a search and analytics engine that can be used to analyze and visualize the data.

Conclusions:

To summarize, we can develop and design a process that installs, configures, and maintains enterprise log monitoring tools using Ansible as an infrastructure-as-code tool. Logstash enables you to effortlessly ingest unstructured data from various sources. The significance of the ELK Stack is that it can centralize logging capabilities and enable users to aggregate logs from increasingly complex cloud environments into a single searchable index .