Name: PEREZ, DEAN LENARD D	**Date Performed:12/11/2024**
Course/Section: CPE 212-CPE31S21	**Date Submitted:12/11/2024**
Instructor: Engr. Robin Valenzuela	**Semester and SY: 2024-2025**

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.

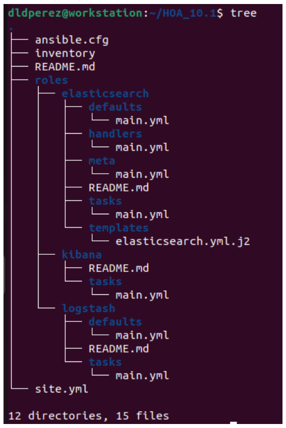
Source: https://www.graylog.org/products/open-source

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)

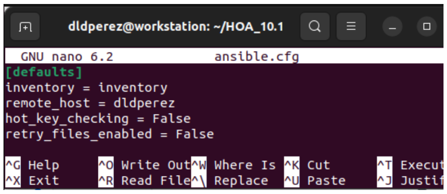
DIRECTORY LAYOUT



```
dldperez@workstation:~/HOA_10.1$ tree
.
├── ansible.cfg
├── inventory
├── README.md
├── roles
│   ├── elasticsearch
│   │   ├── defaults
│   │   │   └── main.yml
│   │   ├── handlers
│   │   │   └── main.yml
│   │   ├── meta
│   │   │   └── main.yml
│   │   ├── README.md
│   │   ├── tasks
│   │   │   └── main.yml
│   │   └── templates
│   │       └── elasticsearch.yml.j2
│   ├── kibana
│   │   ├── README.md
│   │   └── tasks
│   │       └── main.yml
│   └── logstash
│       ├── defaults
│       │   └── main.yml
│       ├── README.md
│       └── tasks
│           └── main.yml
└── site.yml

12 directories, 15 files
```

This is the main layout of the directory. This includes the concept of roles.

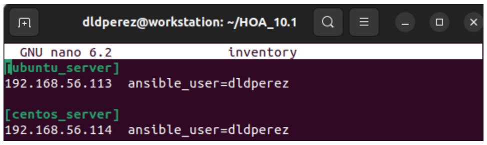
ANSIBLE.CFG FILE



```
  GNU nano 6.2                ansible.cfg
[defaults]
inventory = inventory
remote_host = dldperez
hot_key_checking = False
retry_files_enabled = False

^G Help      ^O Write Out^W Where Is ^K Cut       ^T Execut
^X Exit      ^R Read File^\ Replace  ^U Paste     ^J Justif
```

This file consists of the remote host and the inventory where the ansible will read the ip addresses.

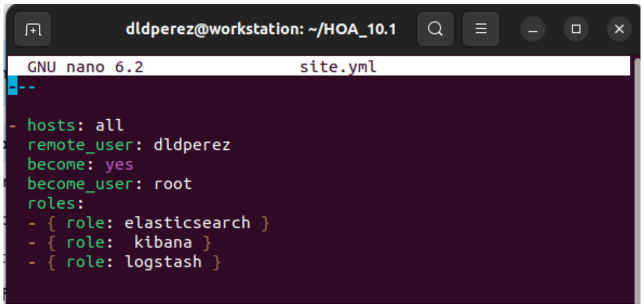
INVENTORY FILE



```
  GNU nano 6.2                    inventory
[ubuntu_server]
192.168.56.113  ansible_user=dldperez

[centos_server]
192.168.56.114  ansible_user=dldperez
```

This inventory file consists of the IP address of ubuntu server (192.168.56.113) and centos server (192.168.56.114).

SITE.YML FILE

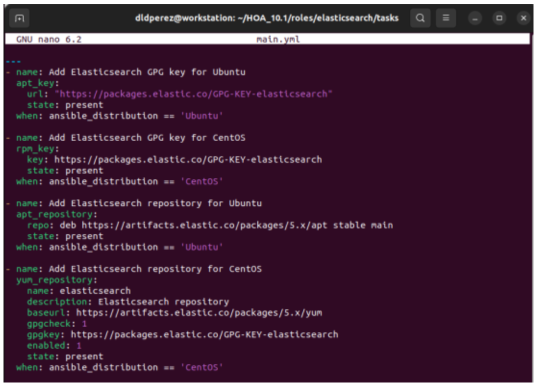


```
  GNU nano 6.2                    site.yml
---

- hosts: all
  remote_user: dldperez
  become: yes
  become_user: root
  roles:
  - { role: elasticsearch }
  - { role:  kibana }
  - { role: logstash }
```

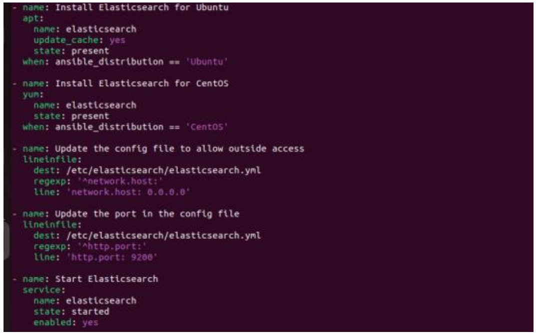
This will run the playbook for elasticsearch, kibana, logstash on ubuntu_server and centos_server by using the concept of roles.

ROLE/ELASTICSEARCH

ELASTICSEARCH /TASKS/MAIN.YML

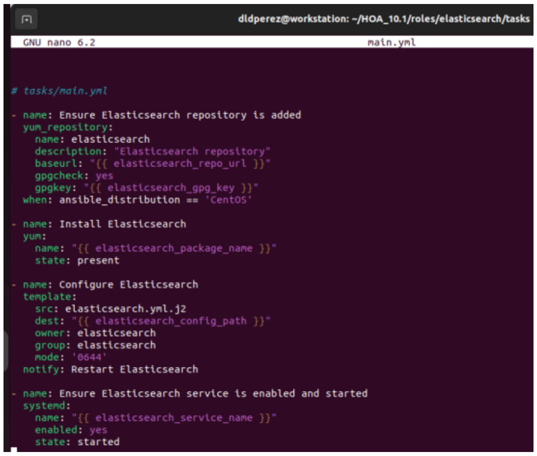


```
---
- name: Add Elasticsearch GPG key for Ubuntu
  apt_key:
    url: "https://packages.elastic.co/GPG-KEY-elasticsearch"
    state: present
  when: ansible_distribution == 'Ubuntu'

- name: Add Elasticsearch GPG key for CentOS
  rpm_key:
    key: https://packages.elastic.co/GPG-KEY-elasticsearch
    state: present
  when: ansible_distribution == 'CentOS'

- name: Add Elasticsearch repository for Ubuntu
  apt_repository:
    repo: deb https://artifacts.elastic.co/packages/5.x/apt stable main
    state: present
  when: ansible_distribution == 'Ubuntu'

- name: Add Elasticsearch repository for CentOS
  yum_repository:
    name: elasticsearch
    description: Elasticsearch repository
    baseurl: https://artifacts.elastic.co/packages/5.x/yum
    gpgcheck: 1
    gpgkey: https://packages.elastic.co/GPG-KEY-elasticsearch
    enabled: 1
    state: present
  when: ansible_distribution == 'CentOS'
```



```
- name: Install Elasticsearch for Ubuntu
  apt:
    name: elasticsearch
    update_cache: yes
    state: present
  when: ansible_distribution == 'Ubuntu'

- name: Install Elasticsearch for CentOS
  yum:
    name: elasticsearch
    state: present
  when: ansible_distribution == 'CentOS'

- name: Update the config file to allow outside access
  lineinfile:
    dest: /etc/elasticsearch/elasticsearch.yml
    regexp: '^network.host:'
    line: 'network.host: 0.0.0.0'

- name: Update the port in the config file
  lineinfile:
    dest: /etc/elasticsearch/elasticsearch.yml
    regexp: '^http.port:'
    line: 'http.port: 9200'

- name: Start Elasticsearch
  service:
    name: elasticsearch
    state: started
    enabled: yes
```

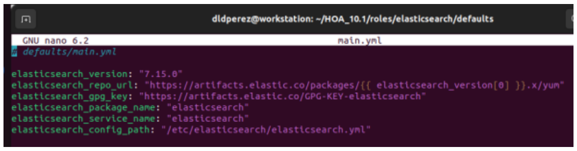
This will install elasticsearch and run all necessary steps to successfully install it on Ubuntu.



```
# tasks/main.yml

- name: Ensure Elasticsearch repository is added
  yum_repository:
    name: elasticsearch
    description: "Elasticsearch repository"
    baseurl: "{{ elasticsearch_repo_url }}"
    gpgcheck: yes
    gpgkey: "{{ elasticsearch_gpg_key }}"
  when: ansible_distribution == 'CentOS'

- name: Install Elasticsearch
  yum:
    name: "{{ elasticsearch_package_name }}"
    state: present

- name: Configure Elasticsearch
  template:
    src: elasticsearch.yml.j2
    dest: "{{ elasticsearch_config_path }}"
    owner: elasticsearch
    group: elasticsearch
    mode: '0644'
  notify: Restart Elasticsearch

- name: Ensure Elasticsearch service is enabled and started
  systemd:
    name: "{{ elasticsearch_service_name }}"
    enabled: yes
    state: started
```

This will install elasticsearch and run all necessary steps to successfully install it on CentOS.

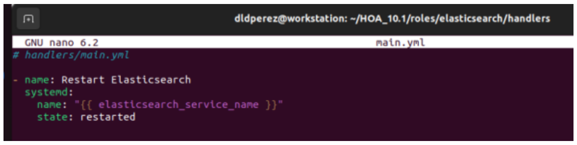
ELASTICSEARCH /DEFAULTS/MAIN.YML


dldperez@workstation: ~/HOA_10.1/roles/elasticsearch/defaults
GNU nano 6.2
main.yml

```
# defaults/main.yml

elasticsearch_version: "7.15.0"
elasticsearch_repo_url: "https://artifacts.elastic.co/packages/{{ elasticsearch_version[0] }}.x/yum"
elasticsearch_gpg_key: "https://artifacts.elastic.co/GPG-KEY-elasticsearch"
elasticsearch_package_name: "elasticsearch"
elasticsearch_service_name: "elasticsearch"
elasticsearch_config_path: "/etc/elasticsearch/elasticsearch.yml"
```

Additional playbook for CENTOS for defaults.

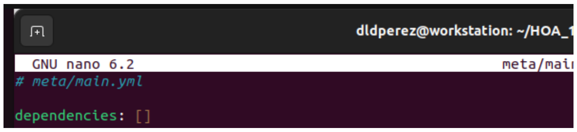
ELASTICSEARCH /HANDLERS/MAIN.YML


dldperez@workstation: ~/HOA_10.1/roles/elasticsearch/handlers
GNU nano 6.2
main.yml

```
# handlers/main.yml

- name: Restart Elasticsearch
  systemd:
    name: "{{ elasticsearch_service_name }}"
    state: restarted
```

Additional playbook for CENTOS that is about the handlers

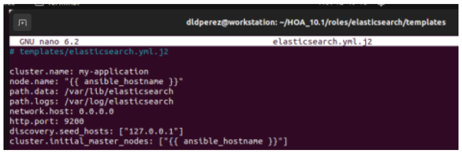
ELASTICSEARCH /META/MAIN.YML



```
# meta/main.yml

dependencies: []
```

Additional playbook for CENTOS that handles meta.

ELASTICSEARCH/TEMPLATES/ELASTICSEARCH.YML.J2

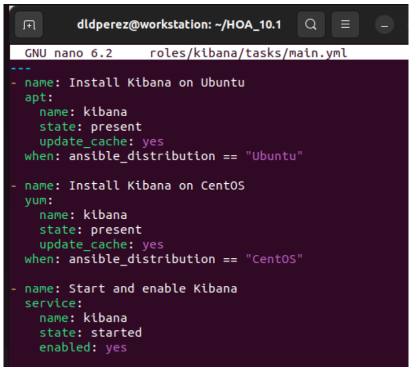

dldperez@workstation: ~/HOA_10.1/roles/elasticsearch/templates
GNU nano 6.2
elasticsearch.yml.j2

```
# templates/elasticsearch.yml.j2

cluster.name: my-application
node.name: "{{ ansible_hostname }}"
path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch
network.host: 0.0.0.0
http.port: 9200
discovery.seed_hosts: ["127.0.0.1"]
cluster.initial_master_nodes: ["{{ ansible_hostname }}"]
```

Additional playbook for CENTOS that handles templates.

ROLES/KIBANA

KIBANA MAIN.YML

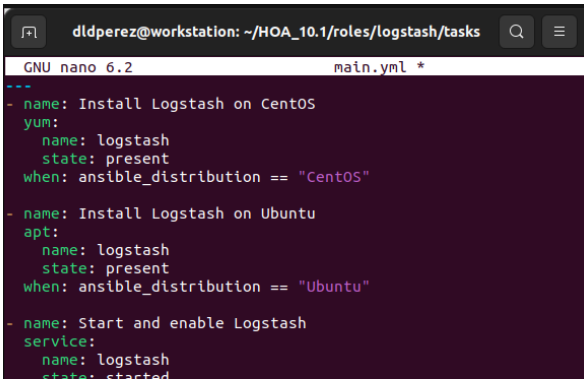


```
  GNU nano 6.2      roles/kibana/tasks/main.yml
---
- name: Install Kibana on Ubuntu
  apt:
    name: kibana
    state: present
    update_cache: yes
  when: ansible_distribution == "Ubuntu"

- name: Install Kibana on CentOS
  yum:
    name: kibana
    state: present
    update_cache: yes
  when: ansible_distribution == "CentOS"

- name: Start and enable Kibana
  service:
    name: kibana
    state: started
    enabled: yes
```

This will install Kibana on Ubuntu and CentOS and will enable and start it on both servers.

ROLES/LOGSTASH

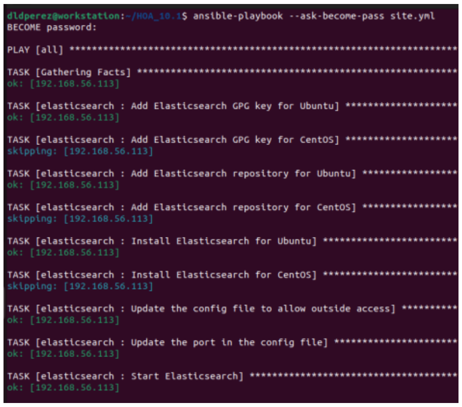
LOGSTASH.YML



```
  GNU nano 6.2                          main.yml *
---
- name: Install Logstash on CentOS
  yum:
    name: logstash
    state: present
  when: ansible_distribution == "CentOS"

- name: Install Logstash on Ubuntu
  apt:
    name: logstash
    state: present
  when: ansible_distribution == "Ubuntu"

- name: Start and enable Logstash
  service:
    name: logstash
    state: started
```

PROCESSES

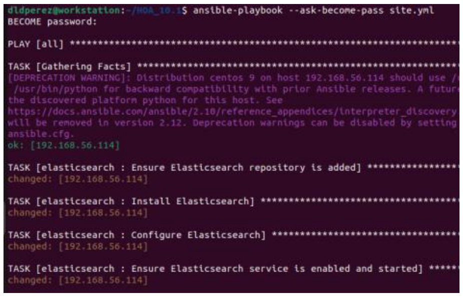
ELASTICSEARCH ON UBUNTU



```
dldperez@workstation:~/HOA_10.1$ ansible-playbook --ask-become-pass site.yml
BECOME password:

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

TASK [Gathering Facts] **********************************************************
ok: [192.168.56.113]

TASK [elasticsearch : Add Elasticsearch GPG key for Ubuntu] *********************
ok: [192.168.56.113]

TASK [elasticsearch : Add Elasticsearch GPG key for CentOS] *********************
skipping: [192.168.56.113]

TASK [elasticsearch : Add Elasticsearch repository for Ubuntu] ******************
ok: [192.168.56.113]

TASK [elasticsearch : Add Elasticsearch repository for CentOS] ******************
skipping: [192.168.56.113]

TASK [elasticsearch : Install Elasticsearch for Ubuntu] *************************
ok: [192.168.56.113]

TASK [elasticsearch : Install Elasticsearch for CentOS] *************************
skipping: [192.168.56.113]

TASK [elasticsearch : Update the config file to allow outside access] ***********
ok: [192.168.56.113]

TASK [elasticsearch : Update the port in the config file] ***********************
ok: [192.168.56.113]

TASK [elasticsearch : Start Elasticsearch] **************************************
ok: [192.168.56.113]
```

This shows that elasticsearch is being installed on ubuntu server

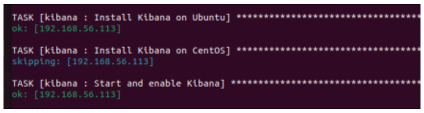
ELASTICSEARCH ON CENTOS



```
dldperez@workstation:~/HOA_10.1$ ansible-playbook --ask-become-pass site.yml
BECOME password:

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

TASK [Gathering Facts] **********************************************************
[DEPRECATION WARNING]: Distribution centos 9 on host 192.168.56.114 should use /
 /usr/bin/python for backward compatibility with prior Ansible releases. A futur
the discovered platform python for this host. See
https://docs.ansible.com/ansible/2.10/reference_appendices/interpreter_discovery
will be removed in version 2.12. Deprecation warnings can be disabled by setting
ansible.cfg.
ok: [192.168.56.114]

TASK [elasticsearch : Ensure Elasticsearch repository is added] *****************
changed: [192.168.56.114]

TASK [elasticsearch : Install Elasticsearch] ************************************
changed: [192.168.56.114]

TASK [elasticsearch : Configure Elasticsearch] **********************************
changed: [192.168.56.114]

TASK [elasticsearch : Ensure Elasticsearch service is enabled and started] ******
changed: [192.168.56.114]
```

This shows that elasticsearch is being installed on centOS.

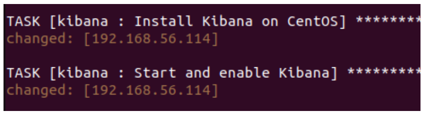
KIBANA ON UBUNTU



```
TASK [kibana : Install Kibana on Ubuntu] ***************************************
ok: [192.168.56.113]

TASK [kibana : Install Kibana on CentOS] ***************************************
skipping: [192.168.56.113]

TASK [kibana : Start and enable Kibana] ****************************************
ok: [192.168.56.113]
```

This shows that kibana is being installed and started in ubuntu server.

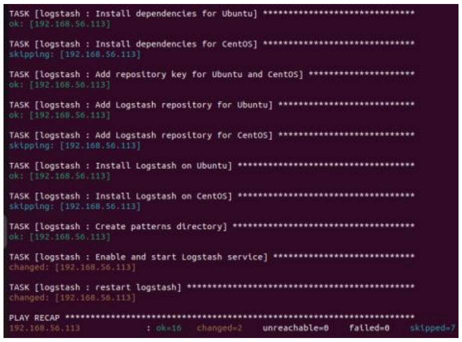
KIBANA ON CENTOS



```
TASK [kibana : Install Kibana on CentOS] ********
changed: [192.168.56.114]

TASK [kibana : Start and enable Kibana] *********
changed: [192.168.56.114]
```

This shows that kibana is being installed and started in centOS server.

LOGSTASH ON UBUNTU



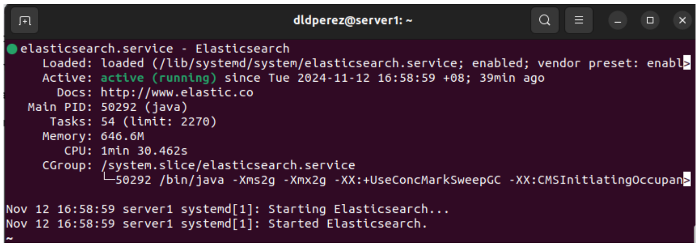
```
TASK [logstash : Install dependencies for Ubuntu] ******************************
ok: [192.168.56.113]

TASK [logstash : Install dependencies for CentOS] ******************************
skipping: [192.168.56.113]

TASK [logstash : Add repository key for Ubuntu and CentOS] *********************
ok: [192.168.56.113]

TASK [logstash : Add Logstash repository for Ubuntu] ***************************
ok: [192.168.56.113]

TASK [logstash : Add Logstash repository for CentOS] ***************************
skipping: [192.168.56.113]

TASK [logstash : Install Logstash on Ubuntu] ***********************************
ok: [192.168.56.113]

TASK [logstash : Install Logstash on CentOS] ***********************************
skipping: [192.168.56.113]

TASK [logstash : Create patterns directory] ************************************
ok: [192.168.56.113]

TASK [logstash : Enable and start Logstash service] ****************************
changed: [192.168.56.113]

TASK [logstash : restart logstash] *********************************************
changed: [192.168.56.113]

PLAY RECAP *********************************************************************
192.168.56.113             : ok=16   changed=2    unreachable=0    failed=0    skipped=7
```

This shows that logstash is being installed on ubuntu.

LOGSTASH FOR CENTOS

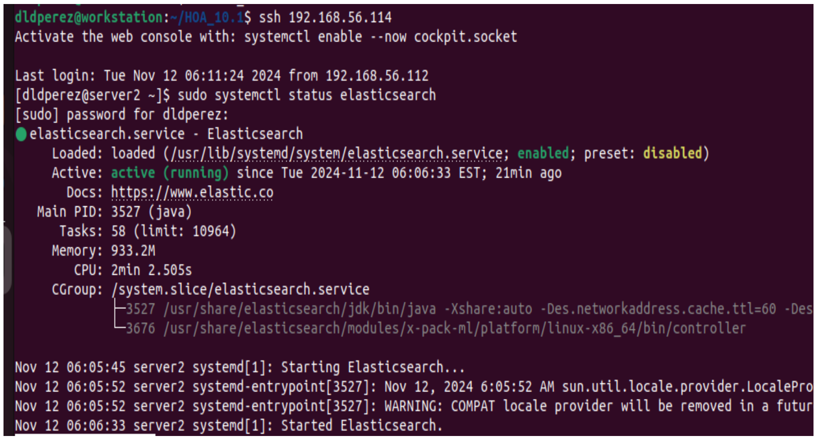
CONFIRMATION/PROOF THAT IT WAS INSTALLED

ELASTICSEARCH



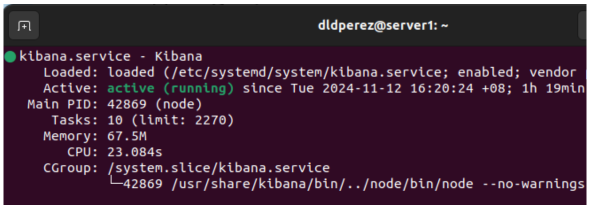
```
dldperez@server1: ~
●elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabl>
     Active: active (running) since Tue 2024-11-12 16:58:59 +08; 39min ago
       Docs: http://www.elastic.co
   Main PID: 50292 (java)
      Tasks: 54 (limit: 2270)
     Memory: 646.6M
        CPU: 1min 30.462s
     CGroup: /system.slice/elasticsearch.service
             └─50292 /bin/java -Xms2g -Xmx2g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupan>

Nov 12 16:58:59 server1 systemd[1]: Starting Elasticsearch...
Nov 12 16:58:59 server1 systemd[1]: Started Elasticsearch.
~
```

It is active and running on ubuntu server



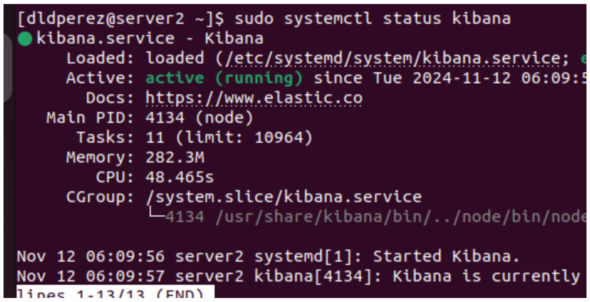
```
dldperez@workstation:~/HOA_10.1$ ssh 192.168.56.114
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Nov 12 06:11:24 2024 from 192.168.56.112
[dldperez@server2 ~]$ sudo systemctl status elasticsearch
[sudo] password for dldperez:
●elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: disabled)
     Active: active (running) since Tue 2024-11-12 06:06:33 EST; 21min ago
       Docs: https://www.elastic.co
   Main PID: 3527 (java)
      Tasks: 58 (limit: 10964)
     Memory: 933.2M
        CPU: 2min 2.505s
     CGroup: /system.slice/elasticsearch.service
             ├─3527 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des
             └─3676 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Nov 12 06:05:45 server2 systemd[1]: Starting Elasticsearch...
Nov 12 06:05:52 server2 systemd-entrypoint[3527]: Nov 12, 2024 6:05:52 AM sun.util.locale.provider.LocalePro
Nov 12 06:05:52 server2 systemd-entrypoint[3527]: WARNING: COMPAT locale provider will be removed in a futur
Nov 12 06:06:33 server2 systemd[1]: Started Elasticsearch.
```

KIBANA



```
dldperez@server1: ~
●kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor
     Active: active (running) since Tue 2024-11-12 16:20:24 +08; 1h 19min
   Main PID: 42869 (node)
      Tasks: 10 (limit: 2270)
     Memory: 67.5M
        CPU: 23.084s
     CGroup: /system.slice/kibana.service
             └─42869 /usr/share/kibana/bin/../node/bin/node --no-warnings
```

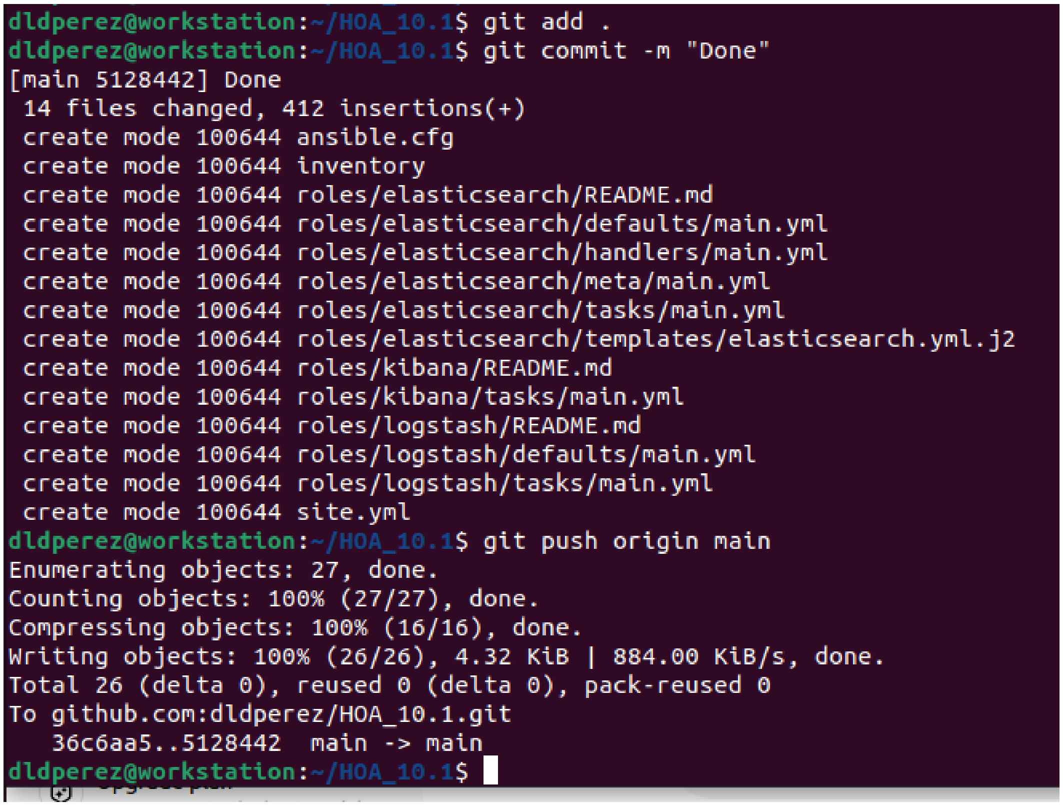
It is active and running on ubuntu server



```
[dldperez@server2 ~]$ sudo systemctl status kibana
●kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; e
     Active: active (running) since Tue 2024-11-12 06:09:5
       Docs: https://www.elastic.co
   Main PID: 4134 (node)
      Tasks: 11 (limit: 10964)
     Memory: 282.3M
        CPU: 48.465s
     CGroup: /system.slice/kibana.service
             └─4134 /usr/share/kibana/bin/../node/bin/node

Nov 12 06:09:56 server2 systemd[1]: Started Kibana.
Nov 12 06:09:57 server2 kibana[4134]: Kibana is currently
lines 1-13/13 (END)
```

It is also running and active on CentOS server

SAVING THE FILES ON GITHUB

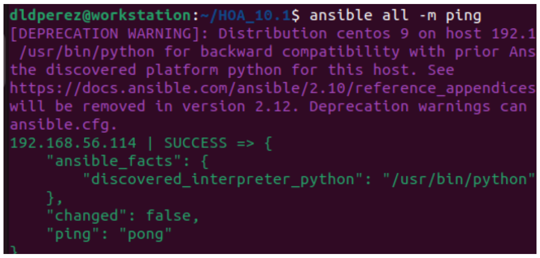


```
dldperez@workstation:~/HOA_10.1$ git add .
dldperez@workstation:~/HOA_10.1$ git commit -m "Done"
[main 5128442] Done
 14 files changed, 412 insertions(+)
 create mode 100644 ansible.cfg
 create mode 100644 inventory
 create mode 100644 roles/elasticsearch/README.md
 create mode 100644 roles/elasticsearch/defaults/main.yml
 create mode 100644 roles/elasticsearch/handlers/main.yml
 create mode 100644 roles/elasticsearch/meta/main.yml
 create mode 100644 roles/elasticsearch/tasks/main.yml
 create mode 100644 roles/elasticsearch/templates/elasticsearch.yml.j2
 create mode 100644 roles/kibana/README.md
 create mode 100644 roles/kibana/tasks/main.yml
 create mode 100644 roles/logstash/README.md
 create mode 100644 roles/logstash/defaults/main.yml
 create mode 100644 roles/logstash/tasks/main.yml
 create mode 100644 site.yml
dldperez@workstation:~/HOA_10.1$ git push origin main
Enumerating objects: 27, done.
Counting objects: 100% (27/27), done.
Compressing objects: 100% (16/16), done.
Writing objects: 100% (26/26), 4.32 KiB | 884.00 KiB/s, done.
Total 26 (delta 0), reused 0 (delta 0), pack-reused 0
To github.com:dldperez/HOA_10.1.git
   36c6aa5..5128442  main -> main
dldperez@workstation:~/HOA_10.1$
```

GITHUB LINK

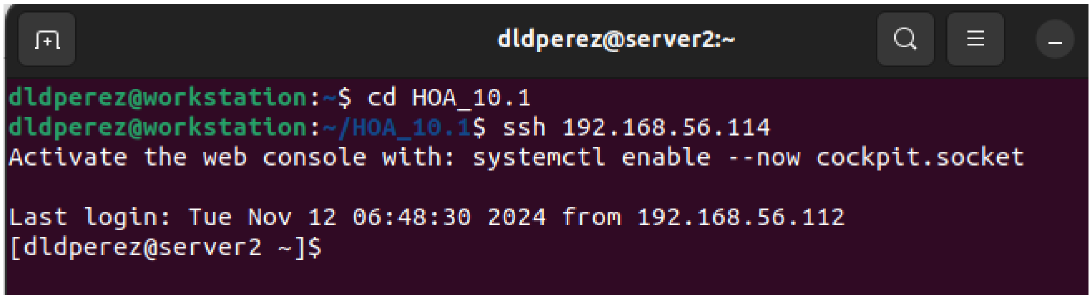
https://github.com/dldperez/HOA_10.1.git

ANSIBLE CONNECTION ON CENTOS_SERVER



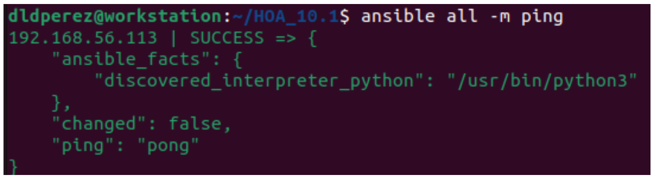
```
dldperez@workstation:~/HOA_10.1$ ansible all -m ping
[DEPRECATION WARNING]: Distribution centos 9 on host 192.1
 /usr/bin/python for backward compatibility with prior Ans
the discovered platform python for this host. See
https://docs.ansible.com/ansible/2.10/reference_appendices
will be removed in version 2.12. Deprecation warnings can
ansible.cfg.
192.168.56.114 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python"
    },
    "changed": false,
    "ping": "pong"
}
```

SSH ON CENTOS_SERVER



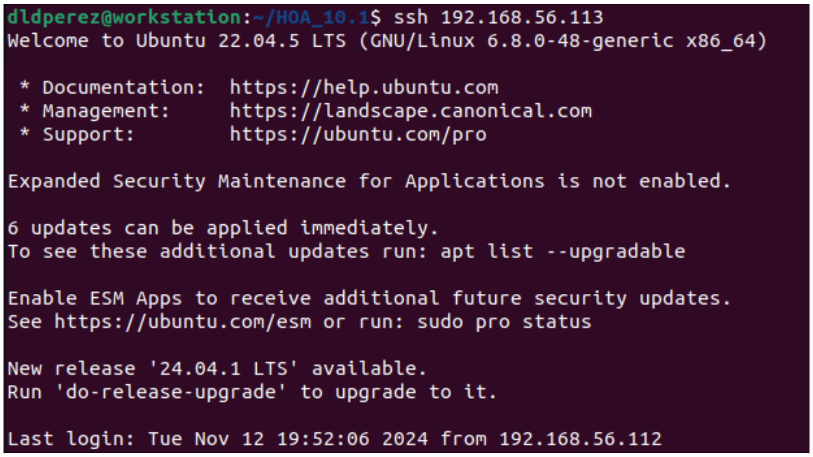
```
dldperez@workstation:~$ cd HOA_10.1
dldperez@workstation:~/HOA_10.1$ ssh 192.168.56.114
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Nov 12 06:48:30 2024 from 192.168.56.112
[dldperez@server2 ~]$
```

ANSIBLE CONNECTION ON UBUNTU_SERVER



```
dldperez@workstation:~/HOA_10.1$ ansible all -m ping
192.168.56.113 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
```

SSH ON UBUNTU SERVER



```
dldperez@workstation:~/HOA_10.1$ ssh 192.168.56.113
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

6 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Nov 12 19:52:06 2024 from 192.168.56.112
```

Reflections:

Answer the following:

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

   The benefit of it is to detect issues early. It helps prevents issues or problems before they escalate into larger failures. It also helps for enhanced security because you can monitor when or if your system is being accessed by unauthorized users.

Conclusions:

Log monitoring tools or software improves the system reliability and security. It provides essential data so that the system is stable and resilient. It also helps the system performance, prevents downtime which is essential for the users.