Name: Gayao, Froilan M.	**Date Performed: 12/11/24**
Course/Section: BSCPE - CPE31S4	**Date Submitted: 12/11/24**
Instructor: Engr. Robin Valenzuela	**Semester and SY: 1st 24-25**

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.

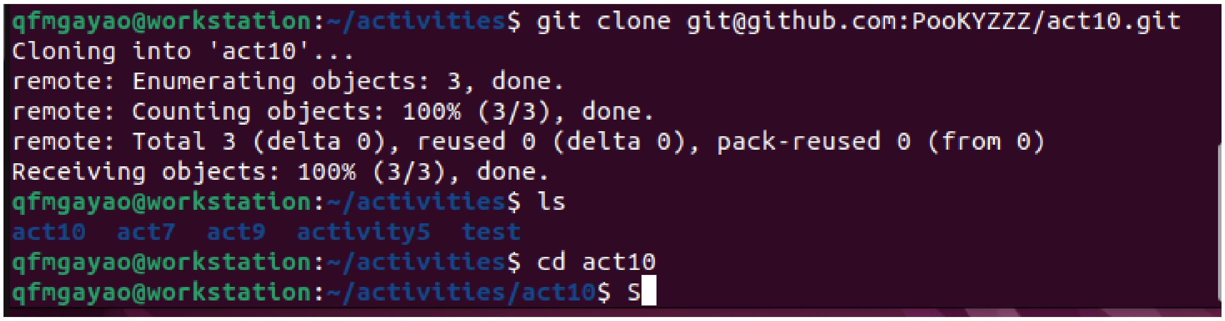
We use Graylog primarily as the stash for the logs of the web applications we build. However, it is also effective when working with raw strings (i.e. syslog): the tool parses it into the structured data we need. It also allows advanced custom search in the logs using structured queries. In other words,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

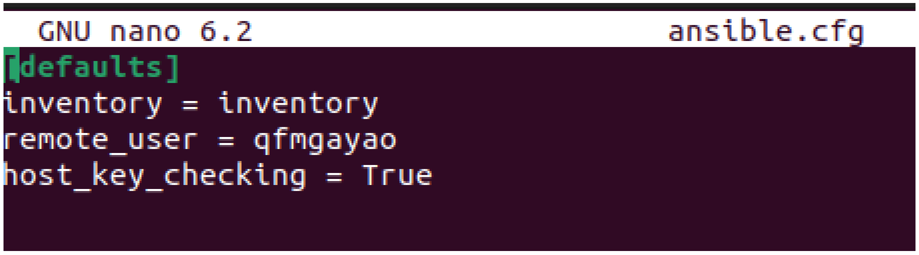
1. Create a playbook that:
    a. Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)
2. Apply the concept of creating roles.
3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like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



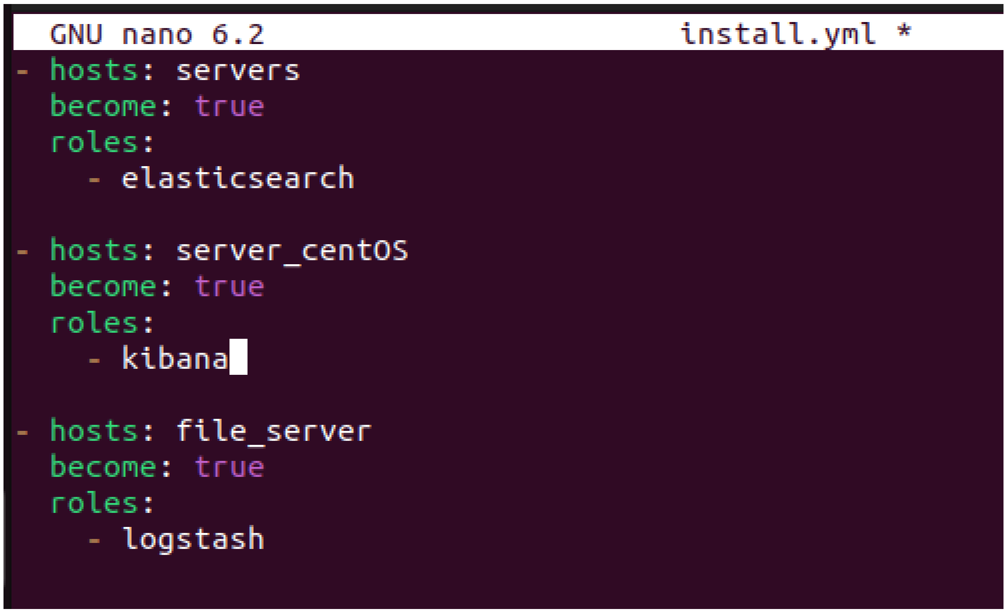
```
qfmgayao@workstation:~/activities$ git clone git@github.com:PooKYZZZ/act10.git
Cloning into 'act10'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (3/3), done.
qfmgayao@workstation:~/activities$ ls
act10  act7  act9  activity5  test
qfmgayao@workstation:~/activities$ cd act10
qfmgayao@workstation:~/activities/act10$ S
```

Here, I created a new repository in my github account and I clone it to my workstation.



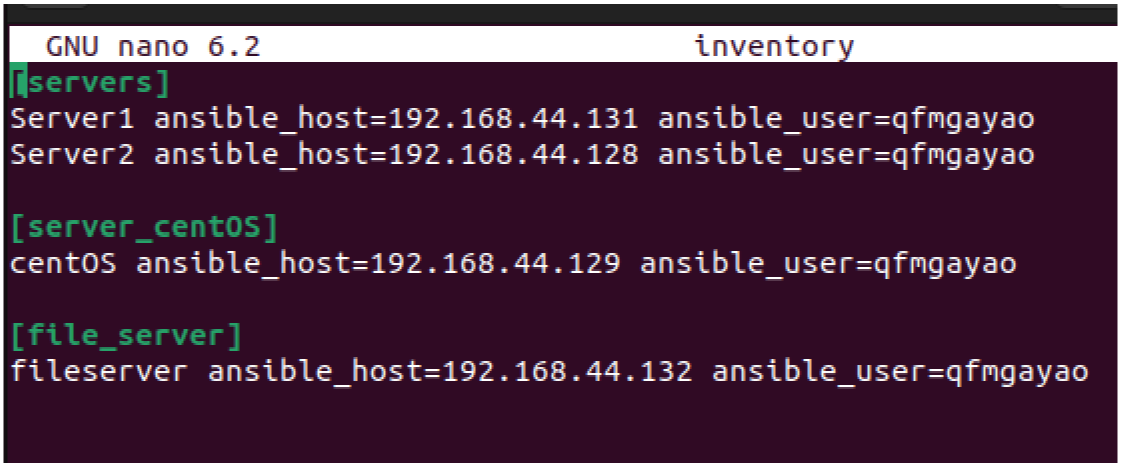
```
  GNU nano 6.2                          ansible.cfg
[defaults]
inventory = inventory
remote_user = qfmgayao
host_key_checking = True
```

I created an ansible.cfg which contains the default configuration for ansible playbook



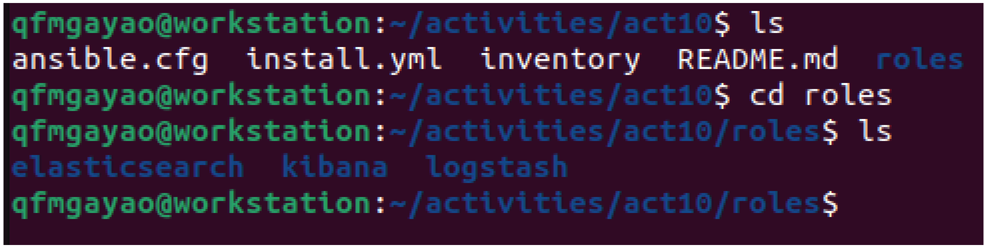
```
  GNU nano 6.2                          install.yml *
- hosts: servers
  become: true
  roles:
    - elasticsearch

- hosts: server_centOS
  become: true
  roles:
    - kibana

- hosts: file_server
  become: true
  roles:
    - logstash
```

I created my installation.yml file, which contains the roles and will install Elastic Stack.



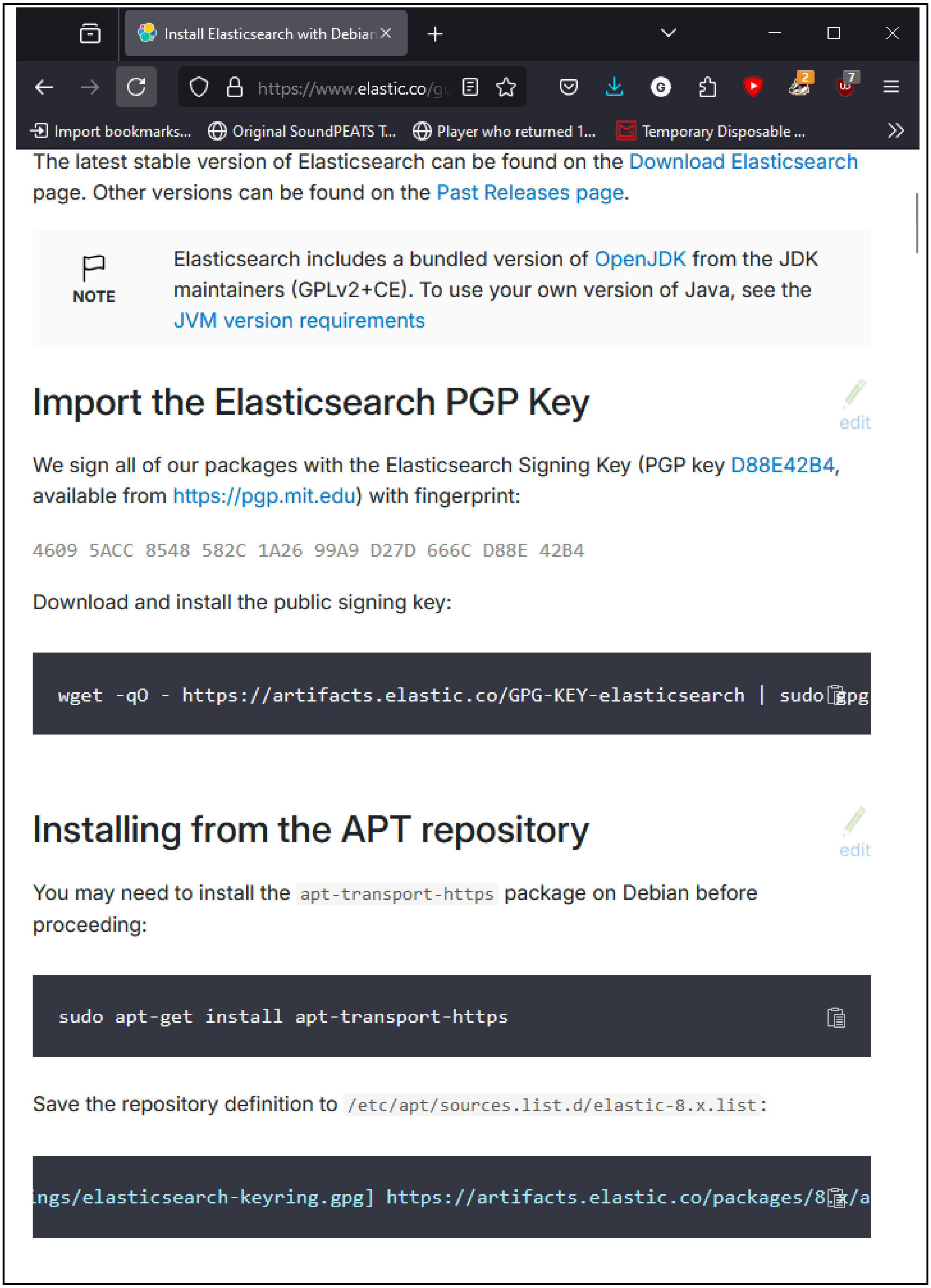
```
  GNU nano 6.2                          inventory
[servers]
Server1 ansible_host=192.168.44.131 ansible_user=qfmgayao
Server2 ansible_host=192.168.44.128 ansible_user=qfmgayao

[server_centOS]
centOS ansible_host=192.168.44.129 ansible_user=qfmgayao

[file_server]
fileserver ansible_host=192.168.44.132 ansible_user=qfmgayao
```

Here is my inventory, which contains the IP addresses of my servers and their assigned names. The yml file can call these to install the required software onto the servers.



```
qfmgayao@workstation:~/activities/act10$ ls
ansible.cfg  install.yml  inventory  README.md  roles
qfmgayao@workstation:~/activities/act10$ cd roles
qfmgayao@workstation:~/activities/act10/roles$ ls
elasticsearch  kibana  logstash
qfmgayao@workstation:~/activities/act10/roles$
```

I created a new folder named roles. This folder contains the roles I will assign to my Ubuntu and CentOS servers, each with its own main.yml file.



The latest stable version of Elasticsearch can be found on the Download Elasticsearch page. Other versions can be found on the Past Releases page.

Elasticsearch includes a bundled version of OpenJDK from the JDK maintainers (GPLv2+CE). To use your own version of Java, see the JVM version requirements

Import the Elasticsearch PGP Key

We sign all of our packages with the Elasticsearch Signing Key (PGP key D88E42B4, available from https://pgp.mit.edu) with fingerprint:

```
4609 5ACC 8548 582C 1A26 99A9 D27D 666C D88E 42B4
```

Download and install the public signing key:

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg
```

Installing from the APT repository

You may need to install the `apt-transport-https` package on Debian before proceeding:

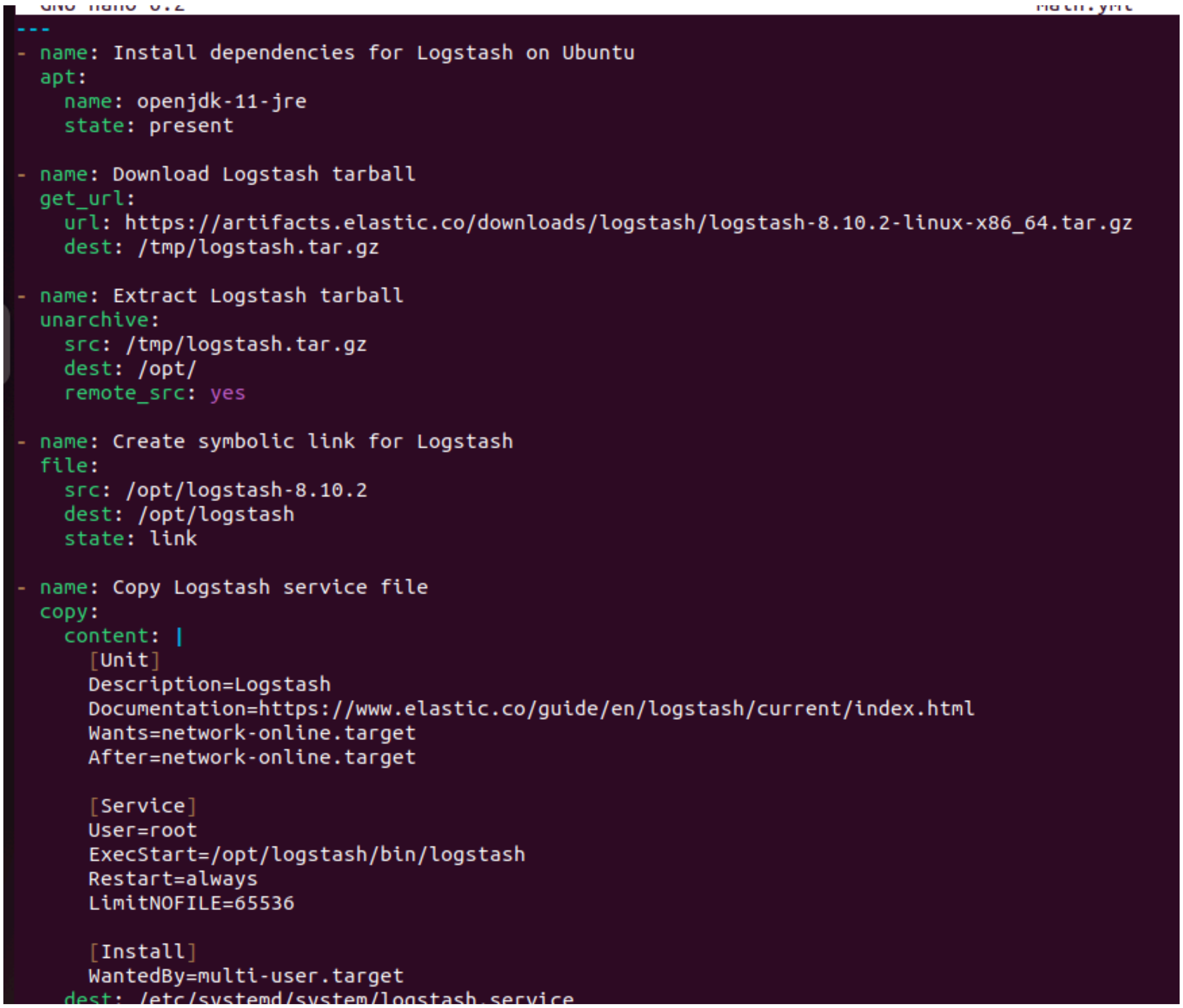
```
sudo apt-get install apt-transport-https
```

Save the repository definition to `/etc/apt/sources.list.d/elastic-8.x.list`:

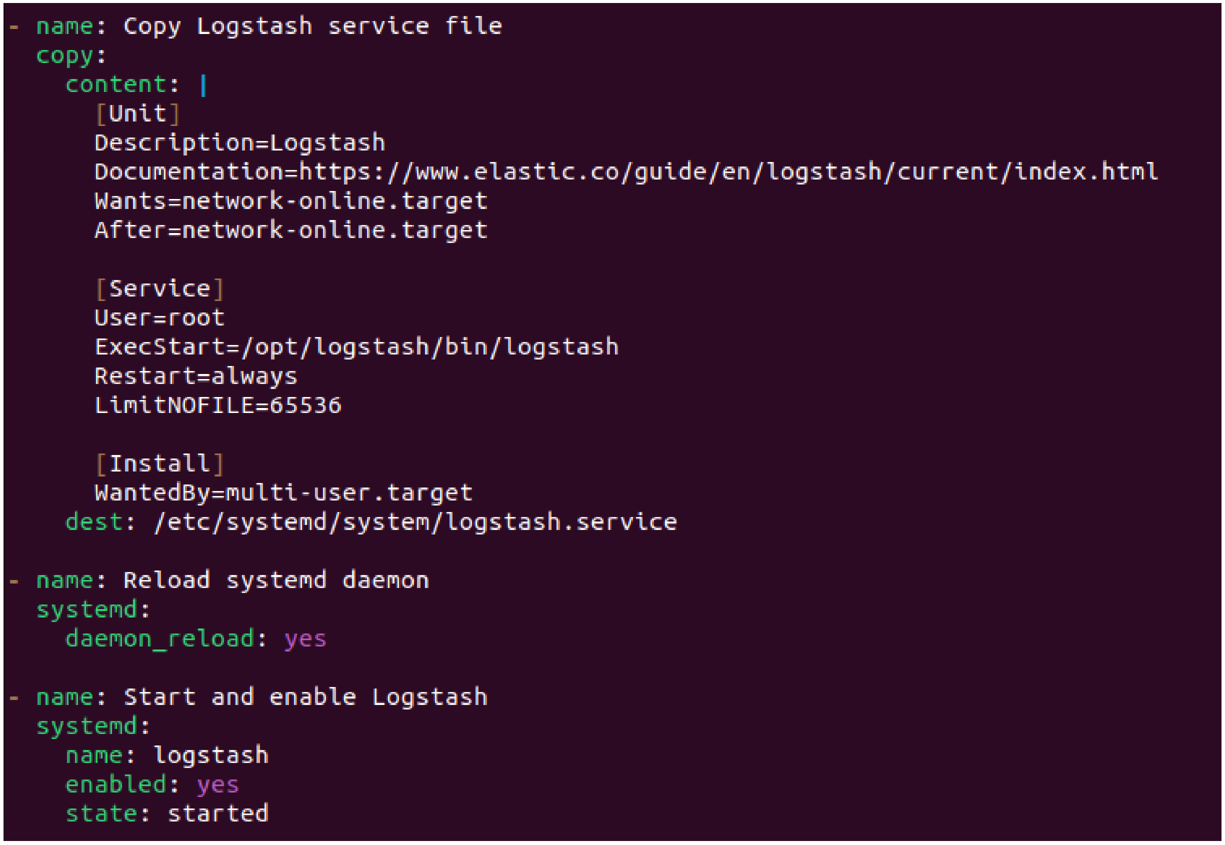
```
ings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/a
```

To install the Elastic package, I have to install the package with debian which I put inside the source list. I follow this website, which helps me install the elastic package.

LOGSTASH codes



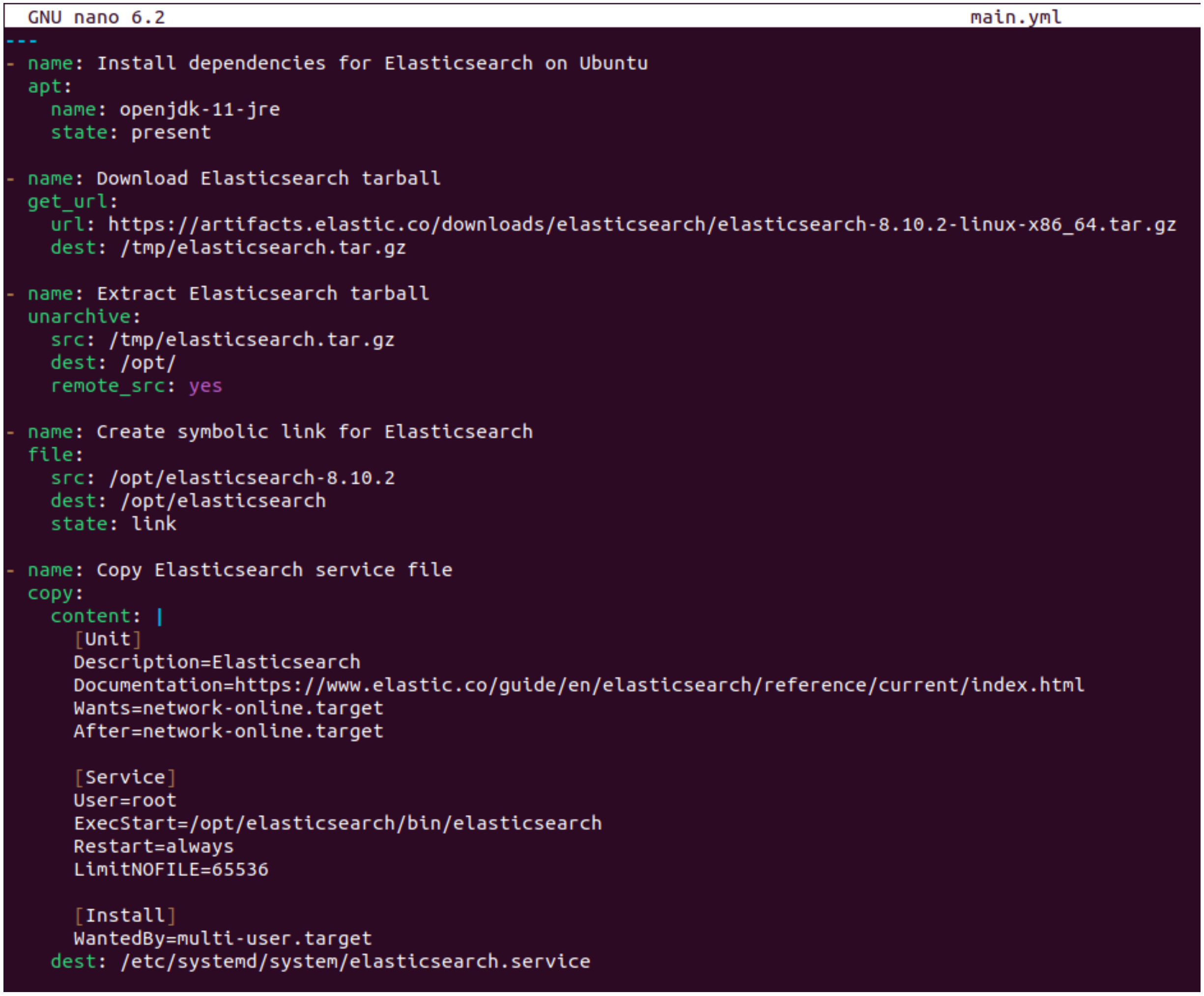
```
---
- name: Install dependencies for Logstash on Ubuntu
  apt:
    name: openjdk-11-jre
    state: present

- name: Download Logstash tarball
  get_url:
    url: https://artifacts.elastic.co/downloads/logstash/logstash-8.10.2-linux-x86_64.tar.gz
    dest: /tmp/logstash.tar.gz

- name: Extract Logstash tarball
  unarchive:
    src: /tmp/logstash.tar.gz
    dest: /opt/
    remote_src: yes

- name: Create symbolic link for Logstash
  file:
    src: /opt/logstash-8.10.2
    dest: /opt/logstash
    state: link

- name: Copy Logstash service file
  copy:
    content: |
      [Unit]
      Description=Logstash
      Documentation=https://www.elastic.co/guide/en/logstash/current/index.html
      Wants=network-online.target
      After=network-online.target

      [Service]
      User=root
      ExecStart=/opt/logstash/bin/logstash
      Restart=always
      LimitNOFILE=65536

      [Install]
      WantedBy=multi-user.target
    dest: /etc/systemd/system/logstash.service
```



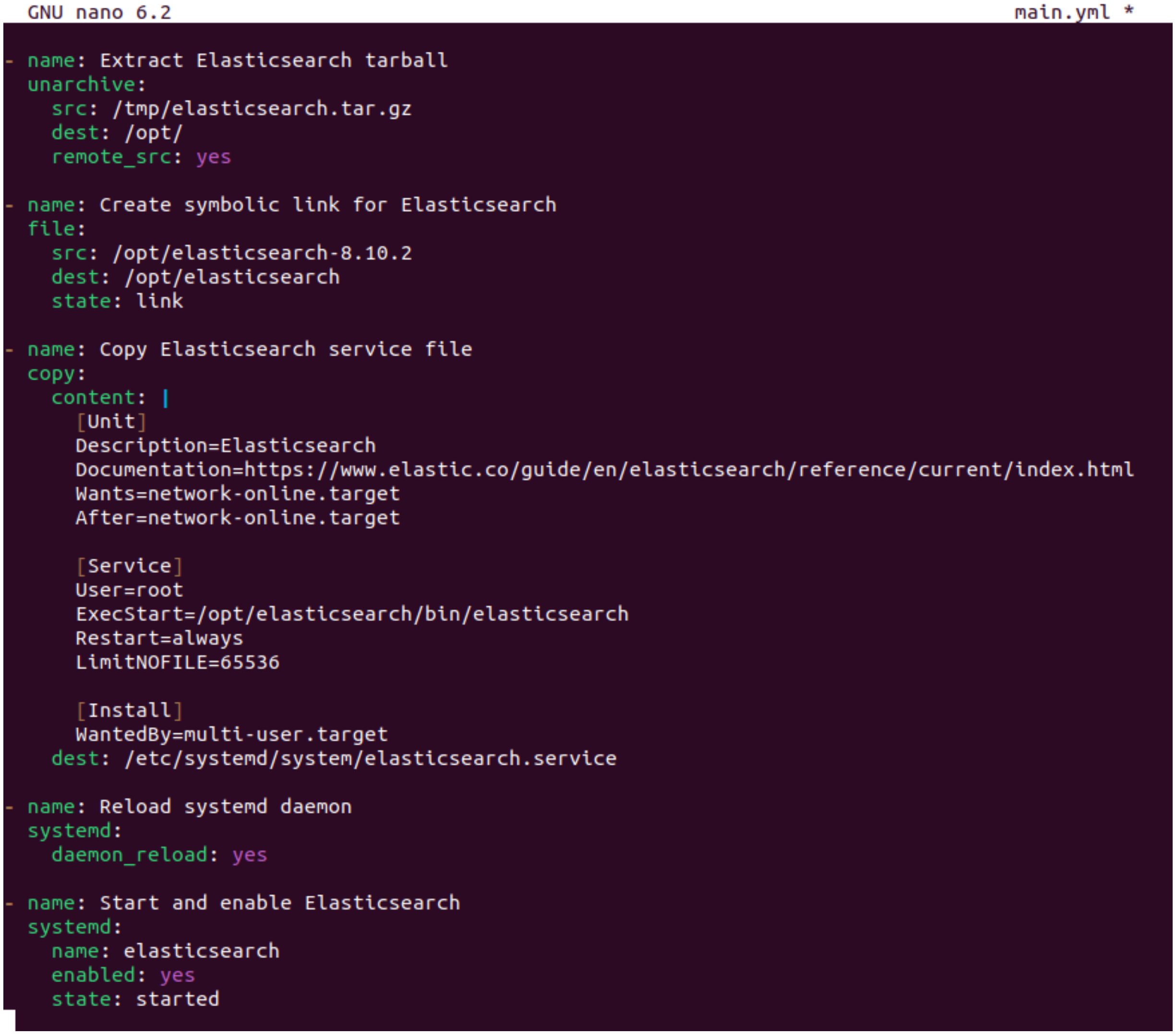
```
- name: Copy Logstash service file
  copy:
    content: |
      [Unit]
      Description=Logstash
      Documentation=https://www.elastic.co/guide/en/logstash/current/index.html
      Wants=network-online.target
      After=network-online.target

      [Service]
      User=root
      ExecStart=/opt/logstash/bin/logstash
      Restart=always
      LimitNOFILE=65536

      [Install]
      WantedBy=multi-user.target
    dest: /etc/systemd/system/logstash.service

- name: Reload systemd daemon
  systemd:
    daemon_reload: yes

- name: Start and enable Logstash
  systemd:
    name: logstash
    enabled: yes
    state: started
```

Here, I copied the format from my Activity 9 main.yml file to create the logstash main.yml

ELASTICSEARCH code



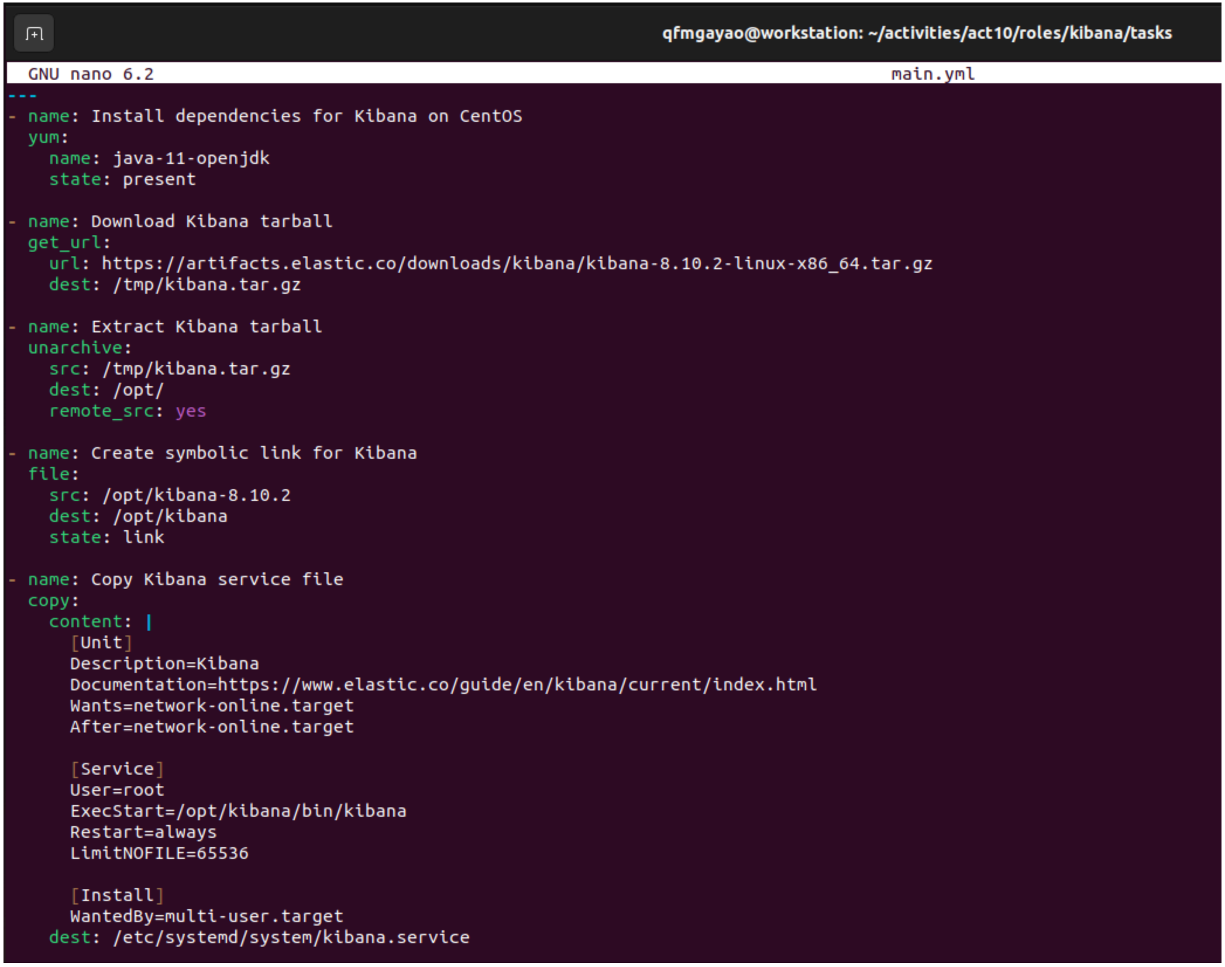
```yaml
---
- name: Install dependencies for Elasticsearch on Ubuntu
  apt:
    name: openjdk-11-jre
    state: present

- name: Download Elasticsearch tarball
  get_url:
    url: https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.10.2-linux-x86_64.tar.gz
    dest: /tmp/elasticsearch.tar.gz

- name: Extract Elasticsearch tarball
  unarchive:
    src: /tmp/elasticsearch.tar.gz
    dest: /opt/
    remote_src: yes

- name: Create symbolic link for Elasticsearch
  file:
    src: /opt/elasticsearch-8.10.2
    dest: /opt/elasticsearch
    state: link

- name: Copy Elasticsearch service file
  copy:
    content: |
      [Unit]
      Description=Elasticsearch
      Documentation=https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html
      Wants=network-online.target
      After=network-online.target

      [Service]
      User=root
      ExecStart=/opt/elasticsearch/bin/elasticsearch
      Restart=always
      LimitNOFILE=65536

      [Install]
      WantedBy=multi-user.target
    dest: /etc/systemd/system/elasticsearch.service
```



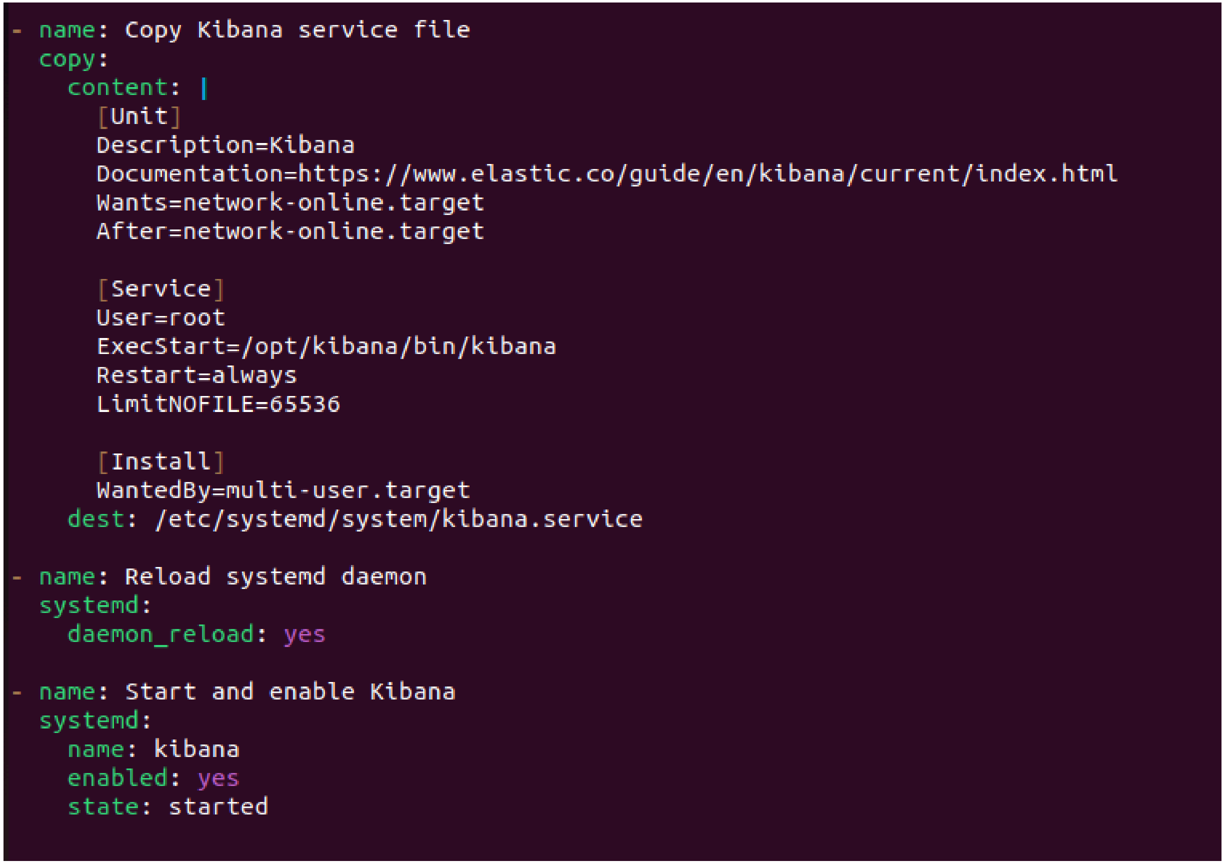
```
  GNU nano 6.2                                                          main.yml *

- name: Extract Elasticsearch tarball
  unarchive:
    src: /tmp/elasticsearch.tar.gz
    dest: /opt/
    remote_src: yes

- name: Create symbolic link for Elasticsearch
  file:
    src: /opt/elasticsearch-8.10.2
    dest: /opt/elasticsearch
    state: link

- name: Copy Elasticsearch service file
  copy:
    content: |
      [Unit]
      Description=Elasticsearch
      Documentation=https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html
      Wants=network-online.target
      After=network-online.target

      [Service]
      User=root
      ExecStart=/opt/elasticsearch/bin/elasticsearch
      Restart=always
      LimitNOFILE=65536

      [Install]
      WantedBy=multi-user.target
    dest: /etc/systemd/system/elasticsearch.service

- name: Reload systemd daemon
  systemd:
    daemon_reload: yes

- name: Start and enable Elasticsearch
  systemd:
    name: elasticsearch
    enabled: yes
    state: started
```

Here, I copied the format from my Activity 9 main.yml file to create the elastic search main.yml

KIBANA code



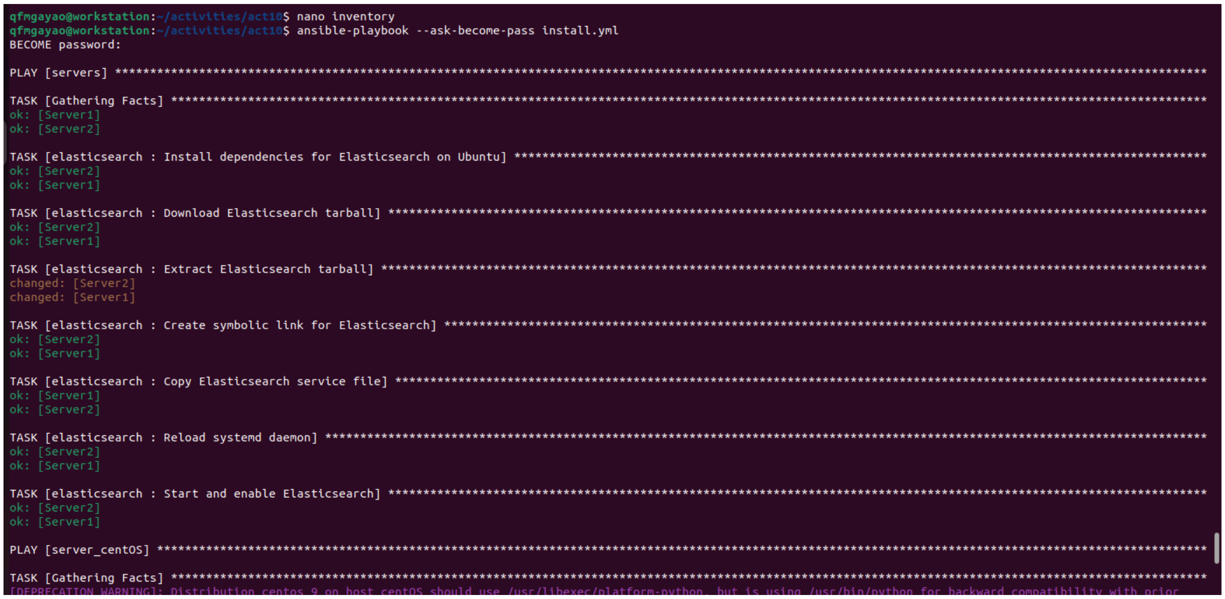
```
---
- name: Install dependencies for Kibana on CentOS
  yum:
    name: java-11-openjdk
    state: present

- name: Download Kibana tarball
  get_url:
    url: https://artifacts.elastic.co/downloads/kibana/kibana-8.10.2-linux-x86_64.tar.gz
    dest: /tmp/kibana.tar.gz

- name: Extract Kibana tarball
  unarchive:
    src: /tmp/kibana.tar.gz
    dest: /opt/
    remote_src: yes

- name: Create symbolic link for Kibana
  file:
    src: /opt/kibana-8.10.2
    dest: /opt/kibana
    state: link

- name: Copy Kibana service file
  copy:
    content: |
      [Unit]
      Description=Kibana
      Documentation=https://www.elastic.co/guide/en/kibana/current/index.html
      Wants=network-online.target
      After=network-online.target

      [Service]
      User=root
      ExecStart=/opt/kibana/bin/kibana
      Restart=always
      LimitNOFILE=65536

      [Install]
      WantedBy=multi-user.target
    dest: /etc/systemd/system/kibana.service
```



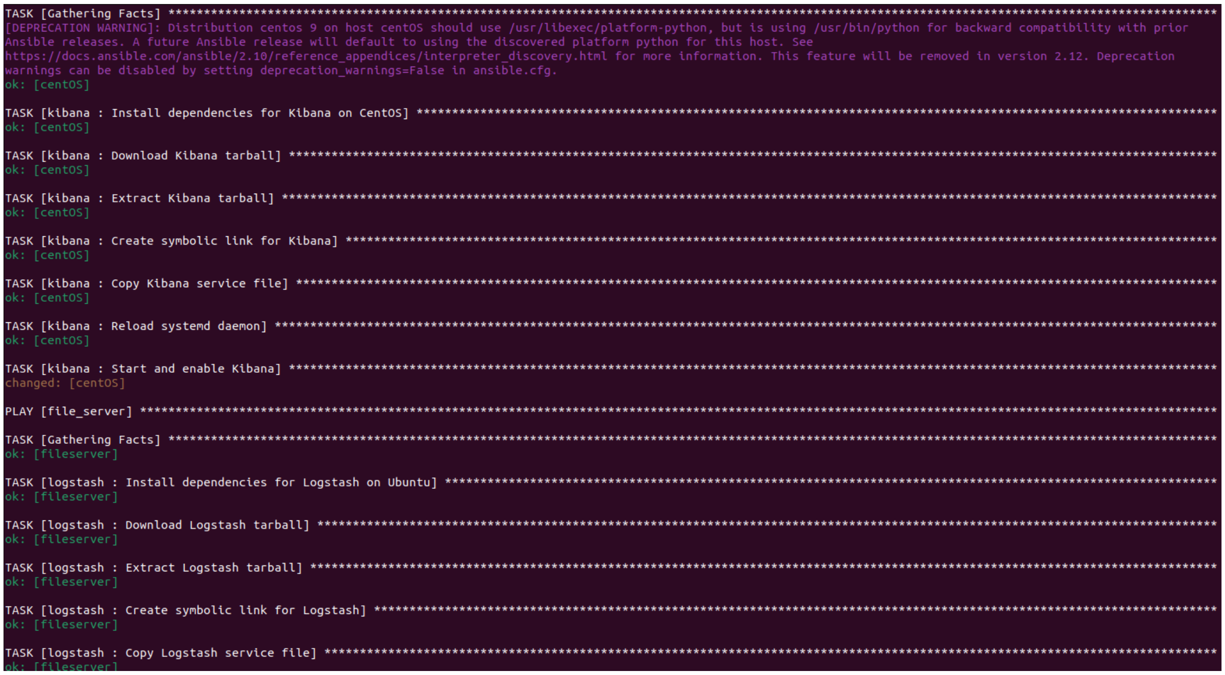
```
- name: Copy Kibana service file
  copy:
    content: |
      [Unit]
      Description=Kibana
      Documentation=https://www.elastic.co/guide/en/kibana/current/index.html
      Wants=network-online.target
      After=network-online.target

      [Service]
      User=root
      ExecStart=/opt/kibana/bin/kibana
      Restart=always
      LimitNOFILE=65536

      [Install]
      WantedBy=multi-user.target
    dest: /etc/systemd/system/kibana.service

- name: Reload systemd daemon
  systemd:
    daemon_reload: yes

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

Same format with the elasticsearch,and logstash, you just need to find the correct link in the elastic website then copy the format from the act 9.

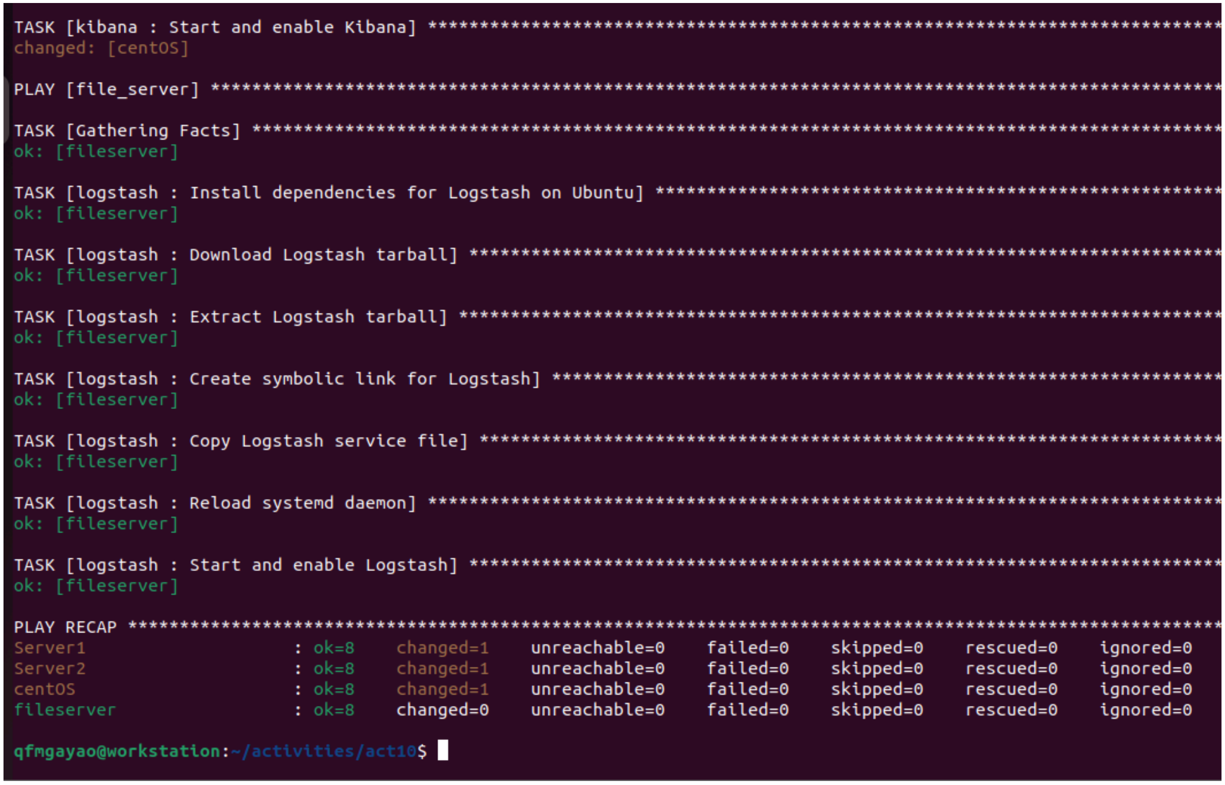
PLAYBOOK



```
qfmgayao@workstation:~/activities/act10$ nano inventory
qfmgayao@workstation:~/activities/act10$ ansible-playbook --ask-become-pass install.yml
BECOME password:

PLAY [servers] ***********************************************************************************************************************************************************

TASK [Gathering Facts] ***************************************************************************************************************************************************
ok: [Server1]
ok: [Server2]

TASK [elasticsearch : Install dependencies for Elasticsearch on Ubuntu] **************************************************************************************************
ok: [Server2]
ok: [Server1]

TASK [elasticsearch : Download Elasticsearch tarball] ********************************************************************************************************************
ok: [Server2]
ok: [Server1]

TASK [elasticsearch : Extract Elasticsearch tarball] *********************************************************************************************************************
changed: [Server2]
changed: [Server1]

TASK [elasticsearch : Create symbolic link for Elasticsearch] ************************************************************************************************************
ok: [Server2]
ok: [Server1]

TASK [elasticsearch : Copy Elasticsearch service file] *******************************************************************************************************************
ok: [Server1]
ok: [Server2]

TASK [elasticsearch : Reload systemd daemon] *****************************************************************************************************************************
ok: [Server2]
ok: [Server1]

TASK [elasticsearch : Start and enable Elasticsearch] ********************************************************************************************************************
ok: [Server2]
ok: [Server1]

PLAY [server_centOS] *****************************************************************************************************************************************************

TASK [Gathering Facts] ***************************************************************************************************************************************************
[DEPRECATION WARNING]: Distribution centos 9 on host centOS should use /usr/libexec/platform-python, but is using /usr/bin/python for backward compatibility with prior
```

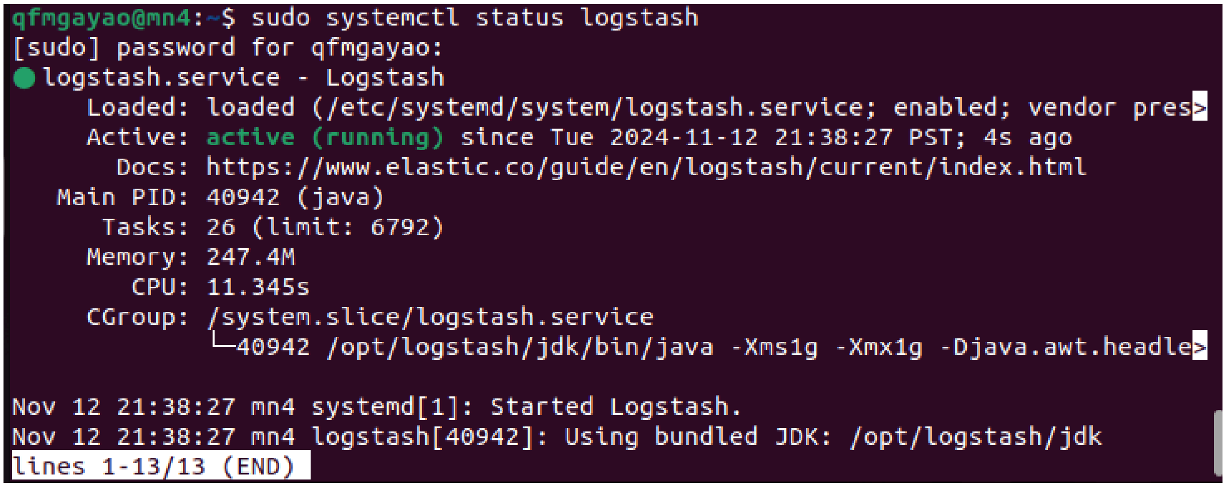


```
TASK [Gathering Facts] ****************************************************************************************************************************************************
[DEPRECATION WARNING]: Distribution centos 9 on host centOS should use /usr/libexec/platform-python, but is using /usr/bin/python for backward compatibility with prior
Ansible releases. A future Ansible release will default to using the discovered platform python for this host. See
https://docs.ansible.com/ansible/2.10/reference_appendices/interpreter_discovery.html for more information. This feature will be removed in version 2.12. Deprecation
warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
ok: [centOS]

TASK [kibana : Install dependencies for Kibana on CentOS] *****************************************************************************************************************
ok: [centOS]

TASK [kibana : Download Kibana tarball] ***********************************************************************************************************************************
ok: [centOS]

TASK [kibana : Extract Kibana tarball] ************************************************************************************************************************************
ok: [centOS]

TASK [kibana : Create symbolic link for Kibana] ***************************************************************************************************************************
ok: [centOS]

TASK [kibana : Copy Kibana service file] **********************************************************************************************************************************
ok: [centOS]

TASK [kibana : Reload systemd daemon] *************************************************************************************************************************************
ok: [centOS]

TASK [kibana : Start and enable Kibana] ***********************************************************************************************************************************
changed: [centOS]

PLAY [file_server] ********************************************************************************************************************************************************

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

TASK [logstash : Install dependencies for Logstash on Ubuntu] *************************************************************************************************************
ok: [fileserver]

TASK [logstash : Download Logstash tarball] *******************************************************************************************************************************
ok: [fileserver]

TASK [logstash : Extract Logstash tarball] ********************************************************************************************************************************
ok: [fileserver]

TASK [logstash : Create symbolic link for Logstash] ***********************************************************************************************************************
ok: [fileserver]

TASK [logstash : Copy Logstash service file] ******************************************************************************************************************************
ok: [fileserver]
```



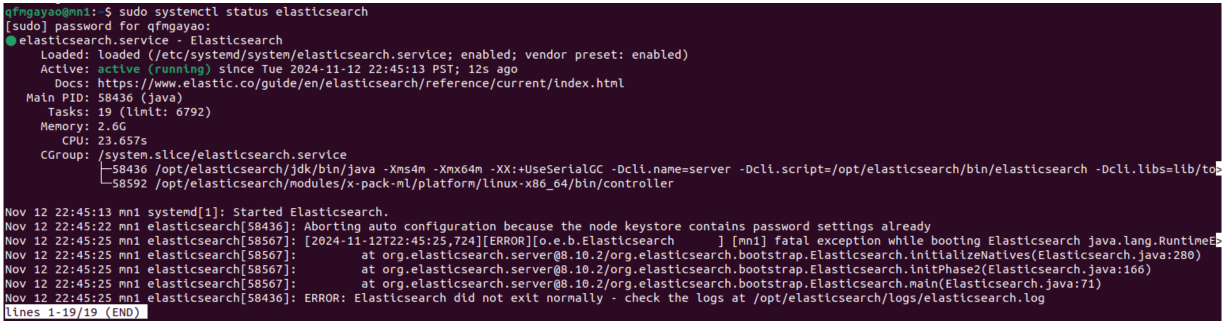
```
TASK [kibana : Start and enable Kibana] ****************************************************************
changed: [centOS]

PLAY [file_server] *************************************************************************************

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

TASK [logstash : Install dependencies for Logstash on Ubuntu] ******************************************
ok: [fileserver]

TASK [logstash : Download Logstash tarball] ************************************************************
ok: [fileserver]

TASK [logstash : Extract Logstash tarball] *************************************************************
ok: [fileserver]

TASK [logstash : Create symbolic link for Logstash] ****************************************************
ok: [fileserver]

TASK [logstash : Copy Logstash service file] ***********************************************************
ok: [fileserver]

TASK [logstash : Reload systemd daemon] ****************************************************************
ok: [fileserver]

TASK [logstash : Start and enable Logstash] ************************************************************
ok: [fileserver]

PLAY RECAP *********************************************************************************************
Server1                    : ok=8    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
Server2                    : ok=8    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
centOS                     : ok=8    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
fileserver                 : ok=8    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

qfmgayao@workstation:~/activities/act10$ 
```

Here, we can see that my code works, successfully changing my Ubuntu and CentOS servers.



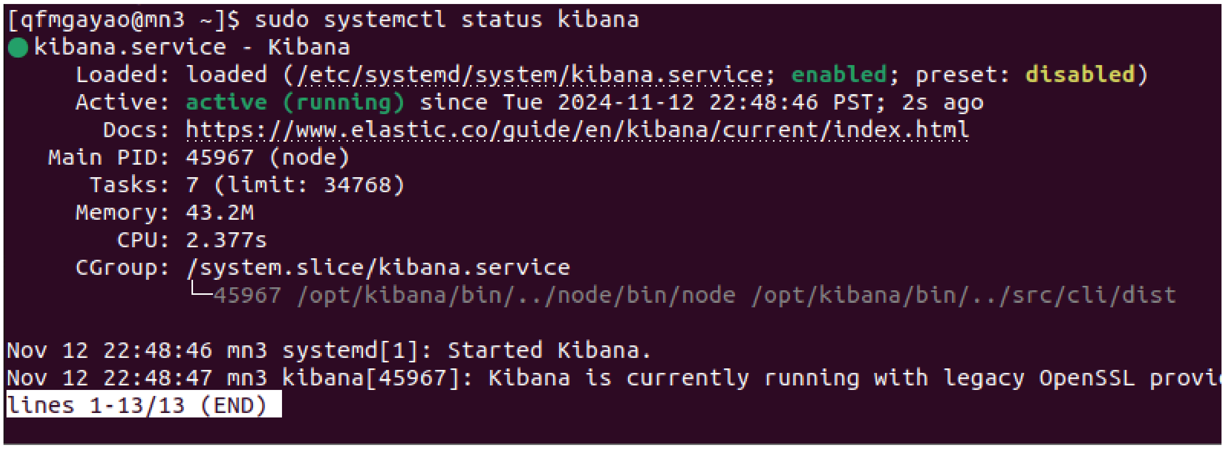
```
qfmgayao@mn4:~$ sudo systemctl status logstash
[sudo] password for qfmgayao:
● logstash.service - Logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor pres>
     Active: active (running) since Tue 2024-11-12 21:38:27 PST; 4s ago
       Docs: https://www.elastic.co/guide/en/logstash/current/index.html
   Main PID: 40942 (java)
      Tasks: 26 (limit: 6792)
     Memory: 247.4M
        CPU: 11.345s
     CGroup: /system.slice/logstash.service
             └─40942 /opt/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headle>

Nov 12 21:38:27 mn4 systemd[1]: Started Logstash.
Nov 12 21:38:27 mn4 logstash[40942]: Using bundled JDK: /opt/logstash/jdk
lines 1-13/13 (END)
```

I SSH into my managenode 4, which hosts my Logstash, and then run the command sudo systemctl status logstash to check if Logstash is working.



```
qfmgayao@mn1:~$ sudo systemctl status elasticsearch
[sudo] password for qfmgayao:
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/etc/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-11-12 22:45:13 PST; 12s ago
       Docs: https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html
   Main PID: 58436 (java)
      Tasks: 19 (limit: 6792)
     Memory: 2.6G
        CPU: 23.657s
     CGroup: /system.slice/elasticsearch.service
             ├─58436 /opt/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/opt/elasticsearch/bin/elasticsearch -Dcli.libs=lib/to>
             └─58592 /opt/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Nov 12 22:45:13 mn1 systemd[1]: Started Elasticsearch.
Nov 12 22:45:22 mn1 elasticsearch[58436]: Aborting auto configuration because the node keystore contains password settings already
Nov 12 22:45:25 mn1 elasticsearch[58567]: [2024-11-12T22:45:25,724][ERROR][o.e.b.Elasticsearch      ] [mn1] fatal exception while booting Elasticsearch java.lang.RuntimeE>
Nov 12 22:45:25 mn1 elasticsearch[58567]:         at org.elasticsearch.server@8.10.2/org.elasticsearch.bootstrap.Elasticsearch.initializeNatives(Elasticsearch.java:280)
Nov 12 22:45:25 mn1 elasticsearch[58567]:         at org.elasticsearch.server@8.10.2/org.elasticsearch.bootstrap.Elasticsearch.initPhase2(Elasticsearch.java:166)
Nov 12 22:45:25 mn1 elasticsearch[58567]:         at org.elasticsearch.server@8.10.2/org.elasticsearch.bootstrap.Elasticsearch.main(Elasticsearch.java:71)
Nov 12 22:45:25 mn1 elasticsearch[58436]: ERROR: Elasticsearch did not exit normally - check the logs at /opt/elasticsearch/logs/elasticsearch.log
lines 1-19/19 (END)
```

I ssh into mn1, where I installed my elasticsearch, then run the same command for logstash, and in the screenshot I can say that my playbook works.



```
[qfmgayao@mn3 ~]$ sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; preset: disabled)
     Active: active (running) since Tue 2024-11-12 22:48:46 PST; 2s ago
       Docs: https://www.elastic.co/guide/en/kibana/current/index.html
   Main PID: 45967 (node)
      Tasks: 7 (limit: 34768)
     Memory: 43.2M
        CPU: 2.377s
     CGroup: /system.slice/kibana.service
             └─45967 /opt/kibana/bin/../node/bin/node /opt/kibana/bin/../src/cli/dist

Nov 12 22:48:46 mn3 systemd[1]: Started Kibana.
Nov 12 22:48:47 mn3 kibana[45967]: Kibana is currently running with legacy OpenSSL provi
lines 1-13/13 (END)
```

I SSH into my CentOS server, which is mn3, using the same command for all servers. The status shows 'active,' indicating that the code is working properly.

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool?
    - Log monitoring tools like the Elastic Stack package offer centralized log management, real-time monitoring, and quick issue detection, which improves our system visibility and performance. They also enhance our security by detecting anomalies and maintaining compliance audit trails.These tools reduce downtime, optimize resource use, and streamline operations, making them vital for efficient system management.

Conclusions:

I therefore conclude that Log monitoring tools are crucial for maintaining our system health by providing real-time insights, detecting issues, and enhancing security. They also help us by reducing downtime, optimizing performance, and ensure compliance through centralized log management and proactive maintenance.