

<b>Name: Jessie Robert Lazo</b>	<b>Date Performed: 10/30/24</b>
<b>Course/Section: CPE 212-CPE31S2</b>	<b>Date Submitted: 11/4/24</b>
<b>Instructor: Engr. Robin Valenzuela</b>	<b>Semester and SY:</b>
<b>Activity 10: Install, Configure, and Manage Log Monitoring tools</b>	
<b>1. Objectives</b>	
Create and design a workflow that installs, configure and manage enterprise log monitoring tools using Ansible as an Infrastructure as Code (IaC) tool.	
<b>2. Discussion</b>	
<p>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.</p> <p>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.</p> <p>To qualify for inclusion in the Log Monitoring category, a product must:</p> <ul style="list-style-type: none"> <li>• Monitor the log files generated by servers, applications, or networks</li> <li>• Alert users when important events are detected</li> <li>• Provide reporting capabilities for log files</li> </ul> <p><b>Elastic Stack</b></p> <p>ELK suite stands for Elasticsearch, Kibana, Beats, and Logstash (also known as the ELK Stack). Source: <a href="https://www.elastic.co/elastic-stack">https://www.elastic.co/elastic-stack</a></p> <p>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.</p> <p><b>GrayLog</b></p>	

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.

Tasks:

1. Before beginning the activity, the first thing to do is create a new repository, creating the ansible configuration file and inventory file needed to establish a working ansible environment between one local machine (ubuntu), and two remote machines (Ubuntu, and CentOS). Next is to make the necessary folders for implementing the roles in ansible-playbook

← → ↻ 🏠 <https://github.com/Jessie-Lazo/HOA10/tree/main>

☰  Jessie-Lazo / HOA10

<> Code ⓘ Issues 🔗 Pull requests ▶ Actions 📁 Projects 📖 Wiki 🛡 Security 📄 Ins

📁 main ▾ HOA10 /

👤 Jessie-Lazo Create main.yml

---

jessielazo@Desktop: ~/hoa10

File Edit View Search Terminal Help

GNU nano 2.9.3 ansible.cfg

```
[defaults]

inventory = inventory
host_key_checking = False

deprecation_warning = False

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

---

jessielazo@Desktop: ~/hoa10

File Edit View Search Terminal Help

GNU nano 2.9.3 inventory

```
[ubuntu_servers]
192.168.56.105 ansible_user=jessieserve ansible_python_interpreter=/usr/bin/py$

[centos_servers]
192.168.56.108 ansible_user=lazocentos ansible_python_interpreter=/usr/bin/py$
```

2. Create a playbook named hoa10.yml and implement basic update and upgrade commands for Ubuntu and CentOS machines. hoa10.yml

jessielazo@Desktop: ~/hoa10

File Edit View Search Terminal Help

GNU nano 2.9.3

hoa10.yml

```
- hosts: all
  become: true
  pre_tasks:

  - name: install update and repositories (CentOS)
    tags: always
    yum:
      name: "*"
      update_cache: yes
      state: latest
      changed_when: false
      when: ansible_distribution == "CentOS"

  - name: Ensure dpkg is configured (Ubuntu)
    raw: sudo dpkg --configure -a
    ignore_errors: yes
    changed_when: false
    when: ansible_distribution == "Ubuntu"

  - name: install update and repositories (Ubuntu)
    tags: always
    apt:
      upgrade: yes
```

Read 37 lines |

```
jessielazo@Desktop: ~/hoa10
File Edit View Search Terminal Help
GNU nano 2.9.3          hoa10.yml

- name: Ensure dpkg is configured (Ubuntu)
  raw: sudo dpkg --configure -a
  ignore_errors: yes
  changed_when: false
  when: ansible_distribution == "Ubuntu"

- name: install update and repositories (Ubuntu)
  tags: always
  apt:
    upgrade: yes
    update_cache: yes
    cache_valid_time: 86400
    changed_when: false
    when: ansible_distribution == "Ubuntu"

- hosts: ubuntu_servers
  become: true
  roles:
    - remote_servers_ubuntu

- hosts: centos_servers
  become: true
```

3. Next is we install the necessary packages for the installation of Elastic Search, Kibana, and Logstash. For Ubuntu:

```
jessielazo@Desktop: ~/hoa10/roles/remote_servers_ubuntu/tasks
File Edit View Search Terminal Help
GNU nano 2.9.3 main.yml

- name: install required packages (Ubuntu)
  apt:
    name:
      - apt-transport-https
    state: latest

- name: Install the Elasticsearch GPG key (Ubuntu)
  apt_key:
    url: https://artifacts.elastic.co/GPG-KEY-elasticsearch

- name: Add Elasticsearch APT repository (Ubuntu)
  apt_repository:
    repo: deb https://artifacts.elastic.co/packages/7.x/apt stable main
    state: present
```

For Centos:

```
jessielazo@Desktop: ~/hoa10/roles/remote_servers_centos/tasks
File Edit View Search Terminal Help
GNU nano 2.9.3 main.yml

- name: install required packages (CentOS)
  yum:
    name:
      - epel-release
    state: latest

- name: Add Elasticsearch YUM repository (CentOS)
  yum_repository:
    name: elasticsearch
    description: Elasticsearch repository
    baseurl: https://artifacts.elastic.co/packages/7.x/yum
    gpgcheck: yes
    gpgkey: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    enabled: yes
```

4. Next is we need to manually create a configuration file for ElasticSearch.

For Ubuntu:

```
jessielazo@Desktop: ~/hoa10/roles/remote_servers_ubuntu/tasks
File Edit View Search Terminal Help
GNU nano 2.9.3 elasticsearch.yml.j2

cluster.name: my-elasticsearch-cluster
node.name: {{ inventory_hostname }}
path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch
network.host: 0.0.0.0
http.port: 9200 # Specify the desired HTTP port here
discovery.seed_hosts: ["192.168.56.105"]
cluster.initial_master_nodes: ["192.168.56.105"]
```

ForCentos:

```
es Terminal Wed 08:38
jessielazo@Desktop: ~/hoa10/roles/remote_servers_centos/tasks
File Edit View Search Terminal Help
GNU nano 2.9.3 elasticsearch.yml.j2

cluster.name: my-elasticsearch-cluster
node.name: {{ inventory_hostname }}
path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch
network.host: 0.0.0.0
http.port: 9200 # Specify the desired HTTP port here
discovery.seed_hosts: ["192.168.56.108"]
cluster.initial_master_nodes: ["192.168.56.108"]
```

5. Then we can proceed with the installation of ElasticSearch,Kibana,and Logstash.  
ForUbuntu:

```
- name: Install Elasticsearch (Ubuntu)
  apt:
    name: elasticsearch
    state: present

- name: Copy Elasticsearch configuration file (Ubuntu)
  template:
    src: elasticsearch.yml.j2
    dest: /etc/elasticsearch/elasticsearch.yml
  #notify: Restart Elasticsearch

- name: Install Kibana (Ubuntu)
  apt:
    name: kibana
    state: present

- name: Install Logstash (Ubuntu)
  apt:
    name: logstash
    state: present
```

For Centos:

```
- name: Install Elasticsearch (Centos)
  package:
    name: elasticsearch
    state: present

- name: Copy Elasticsearch configuration file (Centos)
  template:
    src: elasticsearch.yml.j2
    dest: /etc/elasticsearch/elasticsearch.yml
  #notify: Restart Elasticsearch

- name: Install Kibana (Centos)
  yum:
    name: kibana
    state: present

- name: Install Logstash (Centos)
  yum:
    name: logstash
```



6. After the installation, we need to make sure that the service is enabled.

For Ubuntu:

```
jessielazo@Desktop: ~/hoa10/roles/remote_servers_ubuntu/tasks
File Edit View Search Terminal Help
GNU nano 2.9.3 main.yml

- name: Enable / Restart Elasticsearch (Ubuntu)
  service:
    name: elasticsearch
    state: started

- name: Enable / Restart Kibana (Ubuntu)
  service:
    name: elasticsearch
    state: started

- name: Enable / Restart Logstash (Ubuntu)
  service:
    name: logstash
    state: started
```

For Centos:

es

Terminal

wed 08:43

jessielazo@Desktop: ~/hoa10/roles/remote\_servers\_centos/tasks

File Edit View Search Terminal Help

GNU nano 2.9.3main.yml

```
- name: Enable / Restart Logstash (Centos)
  systemd:
    name: logstash-service
    state: started

- name: Enable / Restart Elasticsearch (Centos)
  service:
    name: elasticsearch
    state: started

- name: Enable / Restart Kibana (Centos)
  service:
    name: kibana
    state: started
```

7. Debug for errors and show complete proof of working playbook.

8. Sync the local repository to Github.

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

```
jessielazo@Desktop:~/hoa10$ tree
.
├── ansible.cfg
├── hoa10.retry
├── hoa10.yml
├── inventory
└── roles
    ├── remote_servers_centos
    │   └── tasks
    │       ├── elasticsearch.yml.j2
    │       └── main.yml
    └── remote_servers_ubuntu
        └── tasks
            ├── elasticsearch.yml.j2
            └── main.yml

5 directories, 8 files
jessielazo@Desktop:~/hoa10$
```

```
TASK [Ensure dpkg is configured (Ubuntu)] *****
*
ok: [192.168.56.105]

TASK [install update and repositories (Ubuntu)] *****
*
[WARNING]: Could not find aptitude. Using apt-get instead.
ok: [192.168.56.105]

PLAY [ubuntu_servers] *****
*

TASK [Gathering Facts] *****
*
ok: [192.168.56.105]

TASK [remote_servers_ubuntu : install required packages (Ubuntu)] *****
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Install the Elasticsearch GPG key (Ubuntu)] *****
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Add Elasticsearch APT repository (Ubuntu)] *****
```

```
TASK [remote_servers_ubuntu : Install the Elasticsearch GPG key (Ubuntu)] *****
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Add Elasticsearch APT repository (Ubuntu)] *****
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Install Elasticsearch (Ubuntu)] *****
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Copy Elasticsearch configuration file (Ubuntu)] *
**
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Install Kibana (Ubuntu)] *****
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Install Logstash (Ubuntu)] *****
*
changed: [192.168.56.105]

TASK [remote_servers_ubuntu : Enable / Restart Elasticsearch (Ubuntu)] *****
*
```

```
TASK [remote_servers_centos : install required packages (CentOS)] *****
*
changed: [192.168.56.108]

TASK [remote_servers_centos : Add Elasticsearch YUM repository (CentOS)] *****
*
changed: [192.168.56.108]

TASK [remote_servers_centos : Install Elasticsearch (Centos)] *****
*
changed: [192.168.56.108]

TASK [remote_servers_centos : Copy Elasticsearch configuration file (Centos)] *
**
changed: [192.168.56.108]

TASK [remote_servers_centos : Install Kibana (Centos)] *****
```

```
jessieserve@Server2:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vend
   Active: active (running) since Wed 2024-10-30 09:52:52 +08; 1min 11s ago
     Docs: https://www.elastic.co
   Main PID: 1918 (java)
    Tasks: 60 (limit: 2318)
   CGroup: /system.slice/elasticsearch.service
           └─1918 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.netwo
             └─2136 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86

Oct 30 09:49:38 Server2 systemd[1]: Starting Elasticsearch...
Oct 30 09:50:39 Server2 systemd-entrypoint[1918]: Oct 30, 2024 9:50:39 AM sun.u
Oct 30 09:50:39 Server2 systemd-entrypoint[1918]: WARNING: COMPAT locale provid
Oct 30 09:52:52 Server2 systemd[1]: Started Elasticsearch.
lines 1-14/14 (END)
```

### Reflections:

Answer the following:

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

It does help the system administrator gather, analyze, and even visualize the log data and thereby allow them to diagnose problems better, improve the security system, and eventually enhance its performance, so time would be saved for a better and more efficient system.

### Conclusions:

I have now completely understood how to install, configure, and manage log monitoring software. These are very important for maintaining safety and welfare within computer systems. Log monitoring solutions are of utmost importance for day-to-day activities in this high-tech world where the reliability of data and system is at its top. They give real-time information about system performance.

Facilitate early issue detection and enhance security by allowing rapid identification and response to potential threats. The knowledge gathered from this activity is critical in ensuring that computer systems work securely and effectively within the modern digital environment.