| | |
|---|---|
| Name: Abigail Laxamana | Date Performed: October 26, 2023 |
| Course/Section: CPE 232 – CPE31S6 | Date Submitted: October 26, 2023 |
| Instructor: Dr. Jonathan V. Taylar | Semester and SY: 1st sem, SY: 2023 - 2024 |

**Activity 10: Install, Configure, and Manage Log Monitoring tools**

**1.** Objectives

Create and design a workflow that installs, configure and manage enterprise log monitoring tools using Ansible as an Infrastructure as Code (IaC) tool.

**2.** Discussion

Log monitoring software scans and monitors log files generated by servers, applications, and networks. By detecting and alerting users to patterns in these log files, log monitoring software helps solve performance and security issues. System administrators use log monitoring software to detect common important events indicated by log files.

Log monitoring software helps maintain IT infrastructure performance and pinpoints issues to prevent downtime and mitigate risks. These tools will often integrate with IT alerting software, log analysis software, and other IT issue resolution products to more aptly flesh out the IT infrastructure maintenance ecosystem.

To qualify for inclusion in the Log Monitoring category, a product must:

- Monitor the log files generated by servers, applications, or networks
- Alert users when important events are detected
- Provide reporting capabilities for log files

Elastic Stack

ELK suite stands for Elasticsearch, Kibana, Beats, and Logstash (also known as the ELK Stack). Source: https://www.elastic.co/elastic-stack

The Elastic Stack is a group of open source products from Elastic designed to help users take data from any type of source and in any format, and search, analyze and visualize that data in real time. The product group was formerly known as the ELK

Stack for the core products in the group -- Elasticsearch, Logstash and Kibana -- but has been rebranded as the Elastic Stack. A fourth product, Beats, was subsequently added to the stack. The Elastic Stack can be deployed on premises or made available as software as a service (SaaS). Elasticsearch supports Amazon Web Services (AWS), Google Cloud Platform and Microsoft Azure.

GrayLog

Graylog is a powerful platform that allows for easy log management of both structured and unstructured data along with debugging applications.

It is based on Elasticsearch, MongoDB, and Scala. Graylog has a main server, which receives data from its clients installed on different servers, and a web interface, which visualizes the data and allows to work with logs aggregated by the main server.

We use Graylog primarily as the stash for the logs of the web applications we build. However, it is also effective when working with raw strings (i.e. syslog): the tool parses it into the structured data we need. It also allows advanced custom search in the logs using structured queries. In other words, when integrated properly with a web app, Graylog helps engineers to analyze the system behavior on almost per code line basis.

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

**3.** Tasks

1. Create a playbook that:
    a. Install and configure Elastic Stack in separate hosts (Elastic Search, Kibana, Logstash)
2. Apply the concept of creating roles.
3. Describe how you did step 1. (Provide screenshots and explanations in your report. Make your report detailed such that it will look like a manual.)
4. Show an output of the installed Elastic Stack for both Ubuntu and CentOS.
5. Make sure to create a new repository in GitHub for this activity.

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

In this activity, you'll create a tree that would look like the image below. You will implement creating roles again and putting tasks inside it that contains a file. First, you need to clone the newly created repository from your github to your remote server first using the **git clone** command.

**Tree**

```
laxamana_ubuntu@workstation:~/hoa10$ tree
.
├── abbyhoa10.yml
├── ansible.cfg
├── inventory
└── roles
    ├── centOS
    │   └── tasks
    │       └── main.yml
    └── ubuntu
        └── tasks
            └── main.yml

5 directories, 5 files
```

After cloning, you will have to create files named **inventory** and **ansible.cfg**.

**ansible.cfg**

*The content of **ansible.cfg** file should look like this.*

```
laxamana_ubuntu@workstation:~/hoa10$ cat ansible.cfg
[defaults]

inventory = inventory
host_key_checking = False

deprecation_warnings = False

remote_user = laxamana_ubuntu

private_key_file = ~/.ssh/
```

*The **inventory** file should contain the ip addresses of the server you'd want to manipulate and metagroups must also be stated. It should look like this.*

```
laxamana_ubuntu@workstation:~/hoa10$ cat inventory
[ubuntu]
192.168.56.103

[centOS]
Laxamana@192.168.56.110
```

To create the *tree*, you have to make a directory named **roles**. Inside the roles directory, create another directories, one for centos, and one for ubuntu server, called

**centOS** and **ubuntu** (suggested but not required names). Then, create another directory called **tasks** inside of each. The **tasks** directory will contain the playbooks called **main.yml**.

*The content of the main.yml file for centOS in the directory ~/**HOA9Laxamana/roles/centOS/tasks/main.yml** should look like this.*

```
laxamana_ubuntu@workstation:~/hoa10/roles/centOS/tasks$ cat 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 Kibana
    yum:
      name: kibana
      state: present
    become: yes

  - name: Enable and start Kibana service
    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

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

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

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

*The content of the main.yml file for centOS in the directory ~/**HOA9Laxamana/roles/ubuntu/tasks/main.yml** should look like this.*

```
laxamana_ubuntu@workstation:~/hoa10/roles/ubuntu/tasks$ cat 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 Kibana service
    systemd:
      name: kibana
      enabled: yes
      state: started
    become: yes

  - name: Install Logstash
    apt:
      name: logstash
      state: present
    become: yes

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

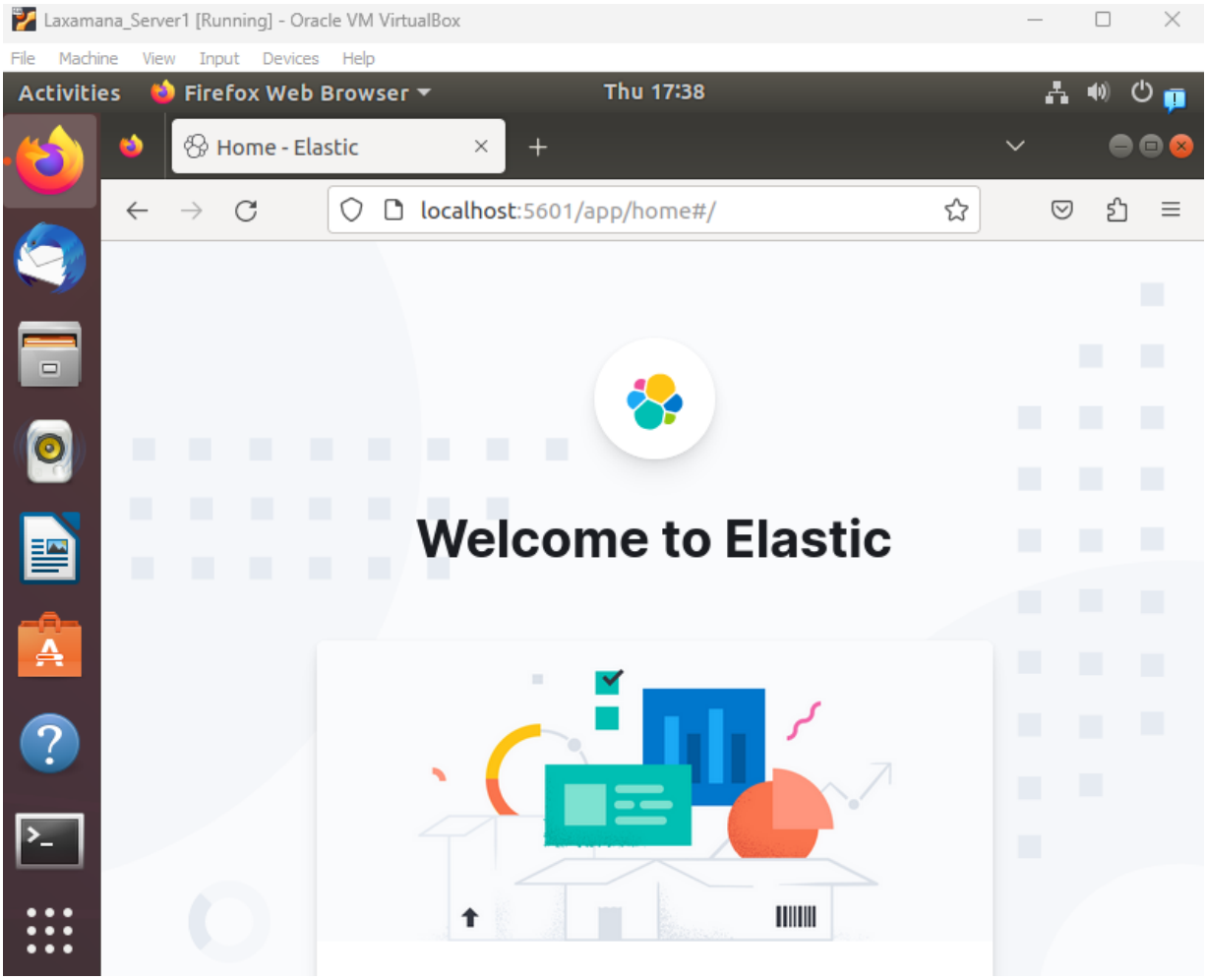
```
  - name: Restart Elasticsearch and Kibana
    systemd:
      name: "{{ item }}"
      state: restarted
    loop:
      - elasticsearch
      - kibana
```

*The content of the abbyhoa10.yml or the main ansible playbook inside the directory ~/**HOA9Laxamana/abbyhoa10.yml** should look like this.*

```
laxamana_ubuntu@workstation:~/hoa10$ cat abbyhoa10.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
```

**verification**

**server1**

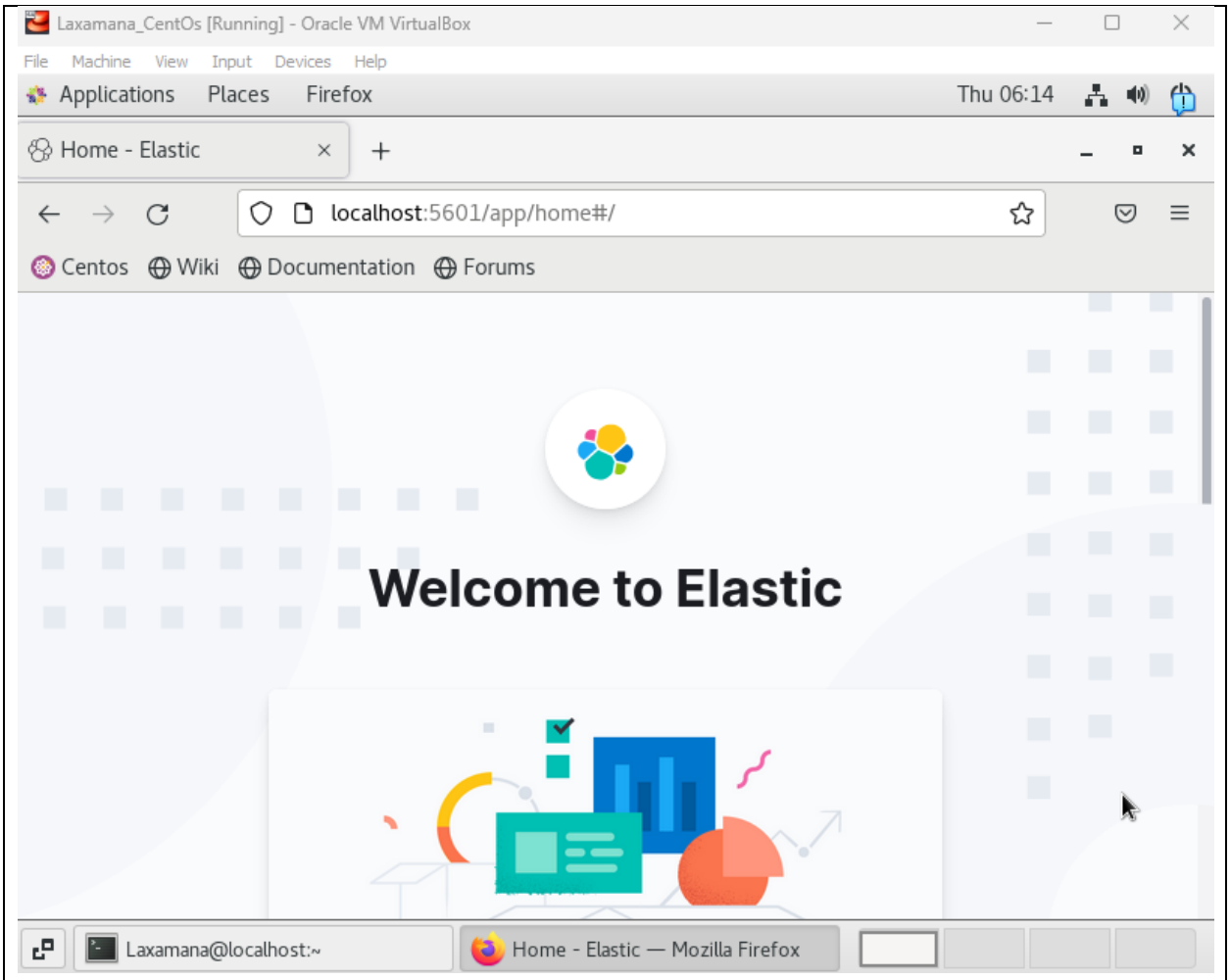



```
laxamana_ubuntu@server1:~$ sudo systemctl status elasticsearch
[sudo] password for laxamana_ubuntu:
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vend
   Active: active (running) since Thu 2023-10-26 17:32:48 PST; 6min ago
     Docs: https://www.elastic.co
 Main PID: 6919 (java)
    Tasks: 65 (limit: 4656)
   CGroup: /system.slice/elasticsearch.service
           ├─6919 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.netwo
           └─7116 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86

Oct 26 17:32:16 server1 systemd[1]: Starting Elasticsearch...
Oct 26 17:32:22 server1 systemd-entrypoint[6919]: Oct 26, 2023 5:32:22 PM sun.u
Oct 26 17:32:22 server1 systemd-entrypoint[6919]: WARNING: COMPAT locale provid
Oct 26 17:32:48 server1 systemd[1]: Started Elasticsearch.
lines 1-14/14 (END)
```

```
laxamana_ubuntu@server1:~$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset:
   Active: active (running) since Thu 2023-10-26 17:32:51 PST; 6min ago
     Docs: https://www.elastic.co
 Main PID: 7217 (node)
    Tasks: 11 (limit: 4656)
   CGroup: /system.slice/kibana.service
           └─7217 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/

Oct 26 17:32:51 server1 systemd[1]: Started Kibana.
Oct 26 17:32:52 server1 kibana[7217]: Kibana is currently running with legacy O
lines 1-11/11 (END)
```

```
laxamana_ubuntu@server1:~$ sudo systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset
   Active: active (running) since Thu 2023-10-26 17:39:55 PST; 2s ago
 Main PID: 8833 (java)
    Tasks: 15 (limit: 4656)
   CGroup: /system.slice/logstash.service
           └─8833 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMa

Oct 26 17:39:55 server1 systemd[1]: logstash.service: Scheduled restart job, re
Oct 26 17:39:55 server1 systemd[1]: Stopped logstash.
Oct 26 17:39:55 server1 systemd[1]: Started logstash.
Oct 26 17:39:55 server1 logstash[8833]: Using bundled JDK: /usr/share/logstash/
Oct 26 17:39:55 server1 logstash[8833]: OpenJDK 64-Bit Server VM warning: Optio
lines 1-13/13 (END)
```

**centos**




```
[Laxamana@localhost ~]$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor prese
t: disabled)
   Active: active (running) since Thu 2023-10-26 06:11:15 EDT; 40s ago
     Docs: https://www.elastic.co
 Main PID: 1192 (java)
    Tasks: 71
   CGroup: /system.slice/elasticsearch.service
           ├─1192 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkadd...
           └─2573 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/b...

Oct 26 06:10:47 localhost.localdomain systemd[1]: Starting Elasticsearch...
Oct 26 06:10:59 localhost.localdomain systemd-entrypoint[1192]: Oct 26, 2023 6:10:59...
Oct 26 06:10:59 localhost.localdomain systemd-entrypoint[1192]: WARNING: COMPAT loca...
Oct 26 06:11:15 localhost.localdomain systemd[1]: Started Elasticsearch.
Hint: Some lines were ellipsized, use -l to show in full.
```

```
[Laxamana@localhost ~]$ systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled
)
   Active: active (running) since Thu 2023-10-26 06:10:47 EDT; 1min 42s ago
     Docs: https://www.elastic.co
 Main PID: 1194 (node)
    Tasks: 11
   CGroup: /system.slice/kibana.service
           └─1194 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../sr...

Oct 26 06:10:47 localhost.localdomain systemd[1]: Started Kibana.
Oct 26 06:10:48 localhost.localdomain kibana[1194]: Kibana is currently running wit...r
Hint: Some lines were ellipsized, use -l to show in full.
```

```
[Laxamana@localhost ~]$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabl
ed)
   Active: active (running) since Thu 2023-10-26 06:12:45 EDT; 18s ago
 Main PID: 3712 (java)
    Tasks: 22
   CGroup: /system.slice/logstash.service
           └─3712 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSwe...

Oct 26 06:12:45 localhost.localdomain systemd[1]: Started logstash.
Oct 26 06:12:45 localhost.localdomain logstash[3712]: Using bundled JDK: /usr/share...k
Oct 26 06:12:45 localhost.localdomain logstash[3712]: OpenJDK 64-Bit Server VM warn....
Oct 26 06:12:57 localhost.localdomain logstash[3712]: Sending Logstash logs to /var...s
Oct 26 06:12:58 localhost.localdomain logstash[3712]: [2023-10-26T06:12:58,137][INF...s
Oct 26 06:12:58 localhost.localdomain logstash[3712]: [2023-10-26T06:12:58,155][INF...}
Oct 26 06:12:58 localhost.localdomain logstash[3712]: [2023-10-26T06:12:58,156][INFO...
Oct 26 06:12:59 localhost.localdomain logstash[3712]: [2023-10-26T06:12:59,897][INF...}
Oct 26 06:12:59 localhost.localdomain logstash[3712]: [2023-10-26T06:12:59,919][INF...}
Oct 26 06:12:59 localhost.localdomain logstash[3712]: [2023-10-26T06:12:59,924][ERR....
Hint: Some lines were ellipsized, use -l to show in full.
```

## playbook process

```
laxamana_ubuntu@workstation:~/hoa10$ sudo nano abbyhoa10.yml
laxamana_ubuntu@workstation:~/hoa10$ ansible-playbook --ask-become-pass abbyhoa10.yml
BECOME password:

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

TASK [Gathering Facts] *********************************************************************
ok: [192.168.56.103]
ok: [Laxamana@192.168.56.110]

TASK [install updates (CentOS)] ************************************************************
skipping: [192.168.56.103]
skipping: [Laxamana@192.168.56.110]

TASK [install updates (Ubuntu)] ************************************************************
skipping: [Laxamana@192.168.56.110]
ok: [192.168.56.103]

PLAY [ubuntu] ******************************************************************************

TASK [Gathering Facts] *********************************************************************
ok: [192.168.56.103]

TASK [ubuntu : Install prerequisites] ******************************************************
changed: [192.168.56.103]

TASK [ubuntu : Add Elasticsearch APT repository key] ***************************************
changed: [192.168.56.103]

TASK [ubuntu : Add Elasticsearch APT repository] *******************************************
changed: [192.168.56.103]
```

```
TASK [ubuntu : Install Elasticsearch] ******************************************************
changed: [192.168.56.103]

TASK [ubuntu : Enable and start Elasticsearch service] *************************************
changed: [192.168.56.103]

TASK [ubuntu : Install Kibana] *************************************************************
changed: [192.168.56.103]

TASK [ubuntu : Enable and start Kibana service] ********************************************
changed: [192.168.56.103]

TASK [ubuntu : Install Logstash] ***********************************************************
changed: [192.168.56.103]

TASK [ubuntu : Enable and start Logstash service] ******************************************
changed: [192.168.56.103]

TASK [ubuntu : Restart Elasticsearch and Kibana] *******************************************
changed: [192.168.56.103] => (item=elasticsearch)
changed: [192.168.56.103] => (item=kibana)
```

```
PLAY [centOS] *****************************************************************************

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

TASK [centOS : Install prerequisites] *****************************************************
ok: [Laxamana@192.168.56.110]

TASK [centOS : Add Elasticsearch RPM repository] ******************************************
changed: [Laxamana@192.168.56.110]

TASK [centOS : Add Elasticsearch YUM repository] ******************************************
changed: [Laxamana@192.168.56.110]

TASK [centOS : Install Elasticsearch] *****************************************************
changed: [Laxamana@192.168.56.110]

TASK [centOS : Enable and start Elasticsearch service] ************************************
changed: [Laxamana@192.168.56.110]

TASK [centOS : Install Kibana] ************************************************************
changed: [Laxamana@192.168.56.110]

TASK [centOS : Enable and start Kibana service] *******************************************
changed: [Laxamana@192.168.56.110]

TASK [centOS : Install Logstash] **********************************************************
changed: [Laxamana@192.168.56.110]

TASK [centOS : Enable and start Logstash service] *****************************************
changed: [Laxamana@192.168.56.110]
```

```
TASK [centOS : Restart Elasticsearch and Kibana] ******************************************
changed: [Laxamana@192.168.56.110] => (item=elasticsearch)
changed: [Laxamana@192.168.56.110] => (item=kibana)

PLAY RECAP ********************************************************************************
192.168.56.103             : ok=13   changed=10   unreachable=0    failed=0    skipped=1    rescued=0
   ignored=0
Laxamana@192.168.56.110    : ok=12   changed=9    unreachable=0    failed=0    skipped=2    rescued=0
   ignored=0
```

## git commit

```
laxamana_ubuntu@workstation:~/hoa10$ git add .
laxamana_ubuntu@workstation:~/hoa10$ git commit -m "LAXAMANA'S HOA 10 IS A SUCCESS!!!"
git commit -m "LAXAMANA'S HOA 10 IS A SUCCESSgit add .!"
[master (root-commit) 755e78a] LAXAMANA'S HOA 10 IS A SUCCESSgit add .!
 5 files changed, 182 insertions(+)
 create mode 100644 abbyhoa10.yml
 create mode 100644 ansible.cfg
 create mode 100644 inventory
 create mode 100644 roles/centOS/tasks/main.yml
 create mode 100644 roles/ubuntu/tasks/main.yml
laxamana_ubuntu@workstation:~/hoa10$ git push origin master
Counting objects: 12, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (8/8), done.
Writing objects: 100% (12/12), 1.63 KiB | 1.63 MiB/s, done.
Total 12 (delta 1), reused 0 (delta 0)
remote: Resolving deltas: 100% (1/1), done.
To github.com:Abigaiiiil/hoa10.git
 * [new branch]      master -> master
```

**repository link:**

*https://github.com/Abigaiiiil/hoa10.git*

Reflections:

Answer the following:

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

First, they offer advanced issue detection, allowing proactive problem repair before small issues turn into significant interruptions. Log monitoring significantly improves security since it assists in identifying illegal access as well as security breaches, enabling quick reactions to possible threats. Another significant benefit is performance improvement, since log monitoring systems provide information on resource usage and system performance, enabling smoother operations and improved user experiences. These solutions also help businesses comply with regulations and keep records, which is essential for compliance and audits. Detail-rich logs make troubleshooting and debugging more effective and help IT specialists quickly identify and fix problems. Long-term performance analysis is made possible by historical log data, assisting with capacity planning and data-driven decision-making. Additional advantages of log monitoring include less downtime, more effective resource allocation, and an overall increase in user experience. These tools are fundamental for guaranteeing the performance, security, and stability of IT systems and applications, which ultimately results in cost savings and improved service quality.

**Conclusions:**

I now have a thorough grasp of how to install, configure, and maintain log monitoring software as a result of this exercise. These tools are essential for maintaining computer systems' safety and health. Log monitoring solutions are essential for daily operations in the technology-

driven world of today, when the dependability of data and systems is of utmost importance. Real-time insights into system performance are offered, they aid in the early identification of problems, and they improve security by quickly identifying and countering possible attacks. As a result, the information gathered from this activity is both important and crucial for ensuring the safe and efficient operation of computer systems in the modern digital world.