Name: Denzel Dinglasan	Date Performed: 23/10/2023
Course/Section:CPE 232 - CPE31S6	Date Submitted: 23/10/2023
Instructor: Dr. Jonathan Vidal Taylar	Semester and SY: 1st Sem 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.

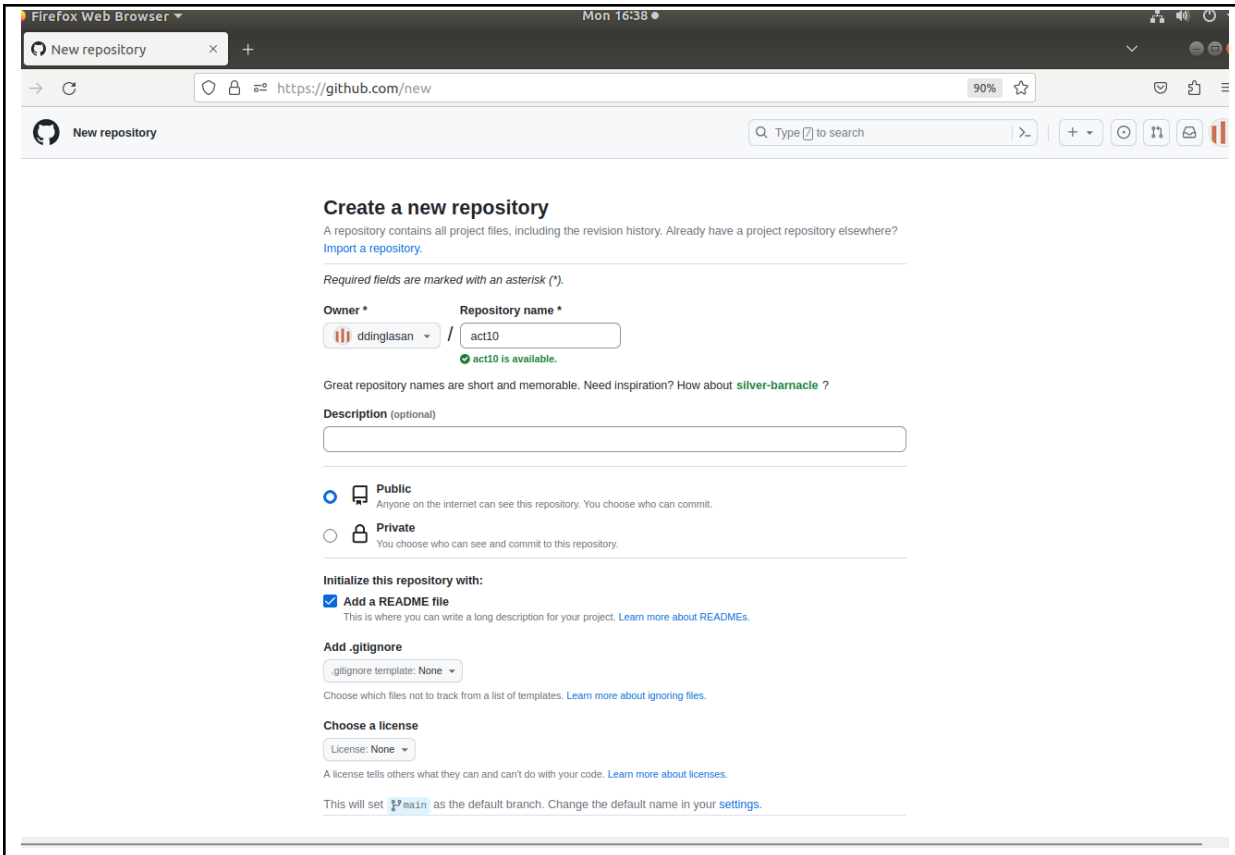
Source: https://www.graylog.org/products/open-source

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)

Step 1: create a new repository and clone the repository in the workstation.




```
dnzl@workstation:~$ git clone https://github.com/ddinglasan/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
Unpacking objects: 100% (3/3), done.
```

Step 2: Create the basic files needed(ansible.cfg & inventory) and create the roles needed for the Ubuntu and CentOS computer with the main.yml file for their own tasks. Also created a task.yml file to run the tasks of the roles.

```
dnzl@workstation:~/act10$ mkdir roles
dnzl@workstation:~/act10$
dnzl@workstation:~/act10$
dnzl@workstation:~/act10$ sudo nano ansible.cfg
[sudo] password for dnzl:
dnzl@workstation:~/act10$ sudo nano inventory
dnzl@workstation:~/act10$ sudo nano task.yml
dnzl@workstation:~/act10$ cd roles
dnzl@workstation:~/act10/roles$ mkdir Ubuntu
dnzl@workstation:~/act10/roles$ mkdir CentOS
dnzl@workstation:~/act10/roles$ cd Ubuntu
dnzl@workstation:~/act10/roles/Ubuntu$ mkdir tasks
dnzl@workstation:~/act10/roles/Ubuntu$ cd tasks
dnzl@workstation:~/act10/roles/Ubuntu/tasks$ touch main.yml
dnzl@workstation:~/act10/roles/Ubuntu/tasks$ cd ~/act10/roles/CentOS
dnzl@workstation:~/act10/roles/CentOS$ mkdir tasks
dnzl@workstation:~/act10/roles/CentOS$ cd tasks
dnzl@workstation:~/act10/roles/CentOS/tasks$ touch main.yml
dnzl@workstation:~/act10/roles/CentOS/tasks$ tree
.
└── main.yml

0 directories, 1 file
dnzl@workstation:~/act10/roles/CentOS/tasks$ cd
dnzl@workstation:~$ cd act10
dnzl@workstation:~/act10$ tree
.
├── ansible.cfg
├── inventory
├── README.md
├── roles
│   ├── CentOS
│   │   └── tasks
│   │       └── main.yml
│   └── Ubuntu
│       └── tasks
│           └── main.yml
└── task.yml
```

Step 3: Paste this on the main.yml of the Ubuntu role.

```
dnzl@workstation: ~/act10/roles/Ubuntu/tasks
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                                                    main.yml

  - name: Install prerequisites
    apt:
      name:
        - default-jre
        - apt-transport-https
        - curl
        - software-properties-common
      state: present
    become: yes

  - name: Add Elasticsearch APT repository key
    apt_key:
      url: https://artifacts.elastic.co/GPG-KEY-elasticsearch
    become: yes

  - name: Add Elasticsearch APT repository
    apt_repository:
      repo: "deb https://artifacts.elastic.co/packages/7.x/apt stable main"
      state: present
    become: yes

  - name: Install Elasticsearch
    apt:
      name: elasticsearch
      state: present
    become: yes

  - name: Enable and start Elasticsearch service
    systemd:
      name: elasticsearch
      enabled: yes
      state: started
    become: yes

  - name: Install Kibana
    apt:
      name: kibana
      state: present
    become: yes
```

```
- name: Enable and start 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
```

Step 4: Paste this on the main.yml of the CentOS role.

```
---
  - 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
```

Step 5: Paste this on the task.yml in the main directory.

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

  - name: centos  upd and upg
    dnf:
      update_cache: yes
      name: "*"
      state: latest
    when: ansible_distribution == "CentOS"

  - name: install wget (CentOS)
    package:
      name: wget
      state: latest
    when: ansible_distribution == "CentOS"

  - name: ubuntu upd and upg
    apt:
      update_cache: yes
      upgrade: yes
    when: ansible_distribution == "Ubuntu"

- hosts: Ubuntu
  become: true
  roles:
    - Ubuntu

- hosts: CentOS
  become: true
  roles:
    - CentOS
```

Step 6: Run the playbook with the command *ansible-playbook –ask-become-pass task.yml*

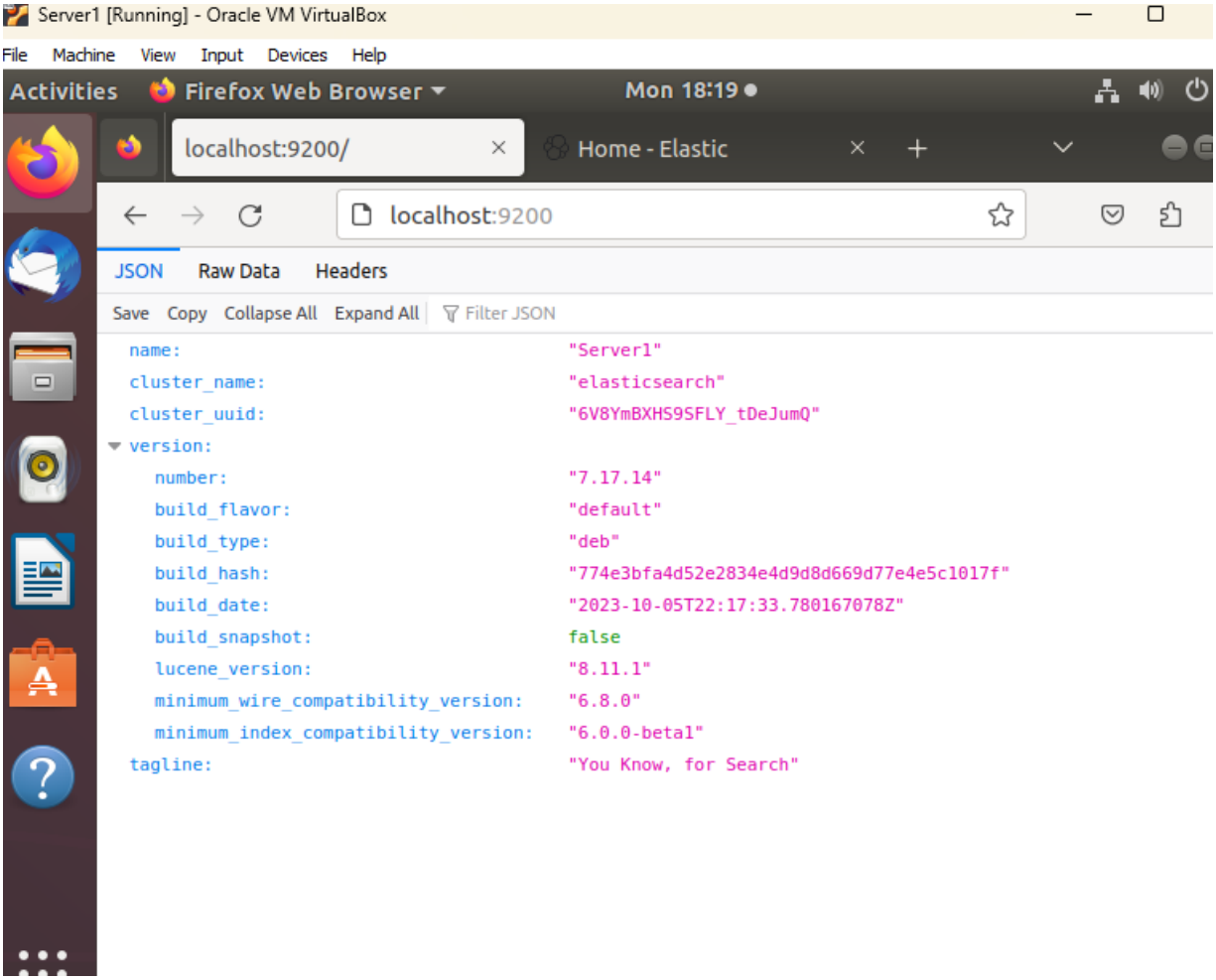
```
dnzl@workstation:~/act10$ ansible-playbook --ask-become-pass task.yml
BECOME password:

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

TASK [Gathering Facts] *********************************************************************************************************
ok: [192.168.56.102]
ok: [192.168.56.105]

TASK [centos  upd and upg] *****************************************************************************************************
skipping: [192.168.56.102]
ok: [192.168.56.105]

TASK [install wget (CentOS)] ***************************************************************************************************
skipping: [192.168.56.102]
ok: [192.168.56.105]

TASK [ubuntu upd and upg] ******************************************************************************************************
skipping: [192.168.56.105]
ok: [192.168.56.102]

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

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

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

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

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

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

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

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

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

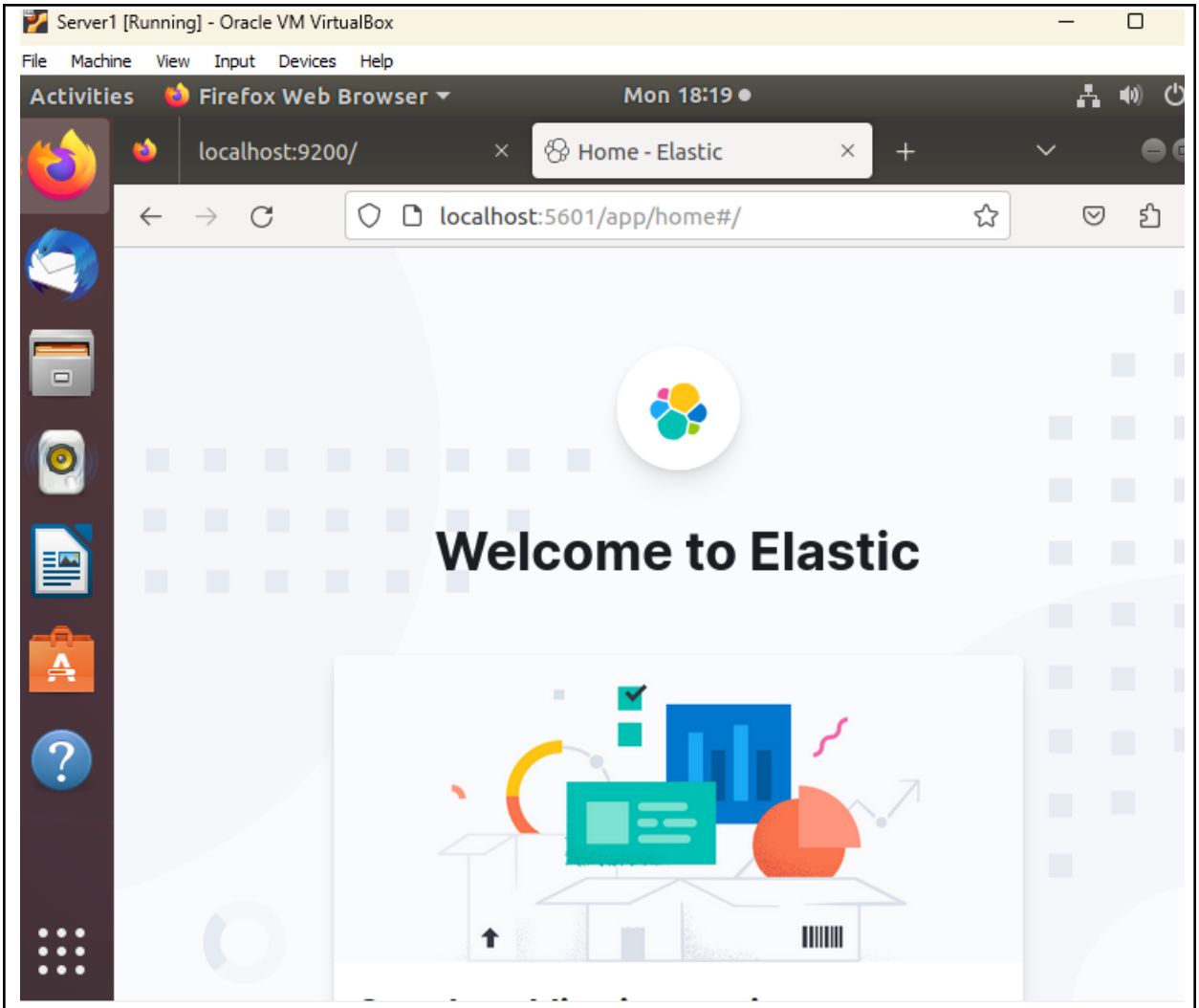
```
TASK [Ubuntu : Enable and start Kibana service] ********************************************************************************
changed: [192.168.56.102]

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

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

TASK [Ubuntu : Restart Elasticsearch and Kibana] *******************************************************************************
changed: [192.168.56.102] => (item=elasticsearch)
changed: [192.168.56.102] => (item=kibana)

PLAY [CentOS] ******************************************************************************************************************

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

TASK [CentOS : Install prerequisites] ******************************************************************************************
ok: [192.168.56.105]

TASK [CentOS : Add Elasticsearch RPM repository] *******************************************************************************
changed: [192.168.56.105]

TASK [CentOS : Add Elasticsearch YUM repository] *******************************************************************************
changed: [192.168.56.105]

TASK [CentOS : Install Elasticsearch] ******************************************************************************************
changed: [192.168.56.105]

TASK [CentOS : Enable and start Elasticsearch service] *************************************************************************
changed: [192.168.56.105]

TASK [CentOS : Install Kibana] *************************************************************************************************
changed: [192.168.56.105]

TASK [CentOS : Enable and start Kibana service] ********************************************************************************
changed: [192.168.56.105]

TASK [CentOS : Install Logstash] ***********************************************************************************************
changed: [192.168.56.105]

TASK [CentOS : Enable and start Logstash service] ******************************************************************************
changed: [192.168.56.105]
```

```
TASK [CentOS : Restart Elasticsearch and Kibana] *******************************************************************************
changed: [192.168.56.105] => (item=elasticsearch)
changed: [192.168.56.105] => (item=kibana)

PLAY RECAP *********************************************************************************************************************
192.168.56.102             : ok=13   changed=9    unreachable=0    failed=0    skipped=2    rescued=0    ignored=0
192.168.56.105             : ok=14   changed=9    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0

dnzl@workstation:~/act10$
```

Step 7: Test if it runs on the Ubuntu and CentOS computer.

Ubuntu:






```
dnzl@Server1:~$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset
   Active: active (running) since Mon 2023-10-23 18:25:41 PST; 11s ago
 Main PID: 18863 (java)
    Tasks: 15 (limit: 4656)
   CGroup: /system.slice/logstash.service
           └─18863 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcM

Oct 23 18:25:41 Server1 systemd[1]: Stopped logstash.
Oct 23 18:25:41 Server1 systemd[1]: Started logstash.
Oct 23 18:25:41 Server1 logstash[18863]: Using bundled JDK: /usr/share/logstash
Oct 23 18:25:41 Server1 logstash[18863]: OpenJDK 64-Bit Server VM warning: Opti
lines 1-12/12 (END)
```

CentOS:

Centos [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places Firefox

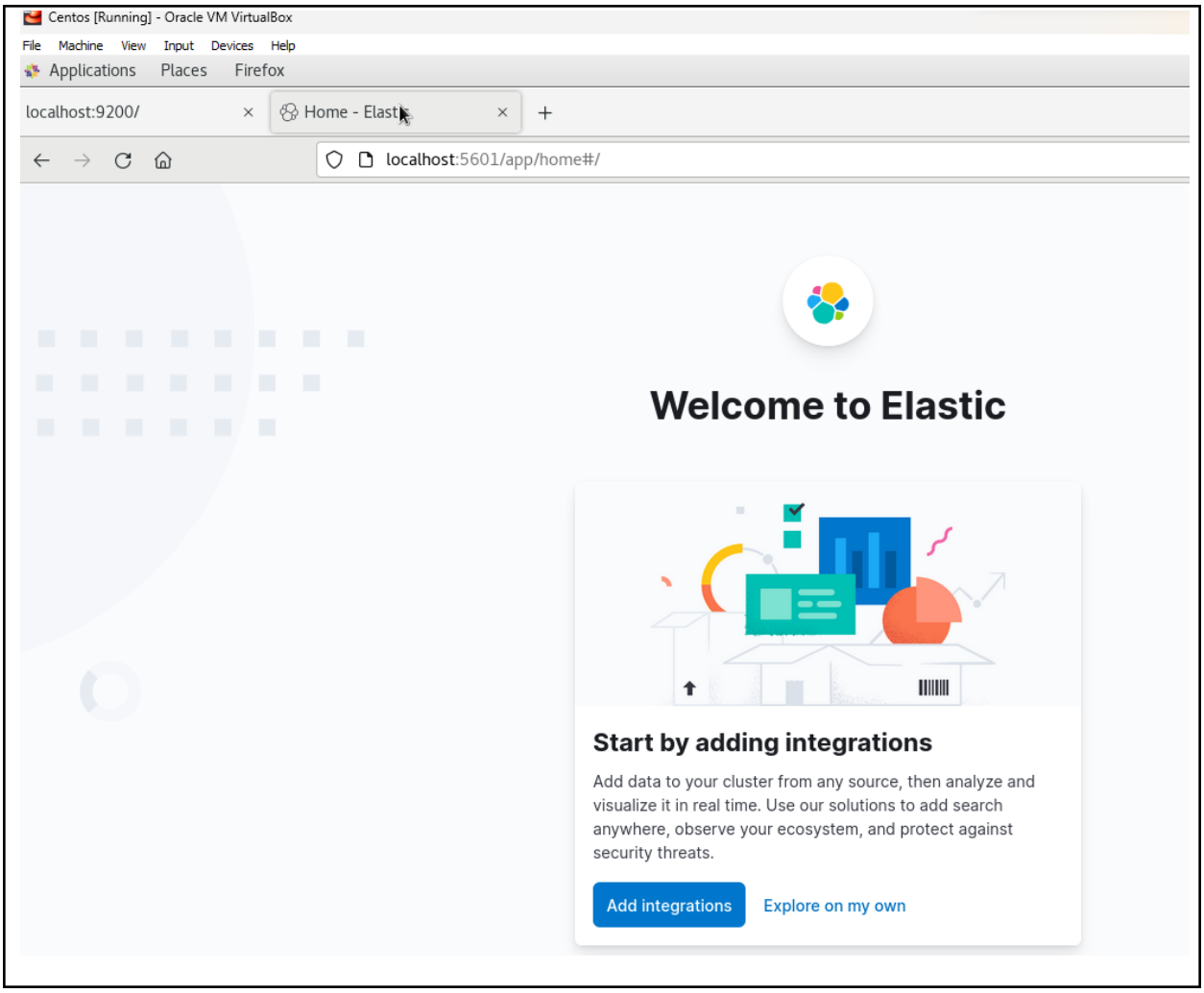
localhost:9200/ × Home - Elastic × +

localhost:9200

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON


```
name:                                  "localhost.localdomain"
cluster_name:                          "elasticsearch"
cluster_uuid:                          "kc00GaYPTfOoXpiNTWn5vQ"
version:
  number:                              "7.17.14"
  build_flavor:                        "default"
  build_type:                          "rpm"
  build_hash:                          "774e3bfa4d52e2834e4d9d8d669d77e4e5c1017f"
  build_date:                          "2023-10-05T22:17:33.780167078Z"
  build_snapshot:                      false
  lucene_version:                      "8.11.1"
  minimum_wire_compatibility_version:  "6.8.0"
  minimum_index_compatibility_version: "6.0.0-beta1"
tagline:                               "You Know, for Search"
```


Centos [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Firefox
localhost:9200/
Home - Elast
localhost:5601/app/home#/
Welcome to Elastic
Start by adding integrations
Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats.
Add integrations
Explore on my own

```
dnzl@localhost:~
File  Edit  View  Search  Terminal  Help
[dnzl@localhost ~]$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset:
 disabled)
   Active: active (running) since Mon 2023-10-23 06:26:27 EDT; 20s ago
 Main PID: 2086 (java)
    Tasks: 22
   CGroup: /system.slice/logstash.service
           └─2086 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConc...

Oct 23 06:26:27 localhost.localdomain systemd[1]: Started logstash.
Oct 23 06:26:27 localhost.localdomain logstash[2086]: Using bundled JDK: /usr...
Oct 23 06:26:27 localhost.localdomain logstash[2086]: OpenJDK 64-Bit Server V...
Oct 23 06:26:45 localhost.localdomain logstash[2086]: Sending Logstash logs t...
Oct 23 06:26:45 localhost.localdomain logstash[2086]: [2023-10-23T06:26:45,62...
Oct 23 06:26:45 localhost.localdomain logstash[2086]: [2023-10-23T06:26:45,63...
Oct 23 06:26:45 localhost.localdomain logstash[2086]: [2023-10-23T06:26:45,63...
Oct 23 06:26:47 localhost.localdomain logstash[2086]: [2023-10-23T06:26:47,27...
Oct 23 06:26:47 localhost.localdomain logstash[2086]: [2023-10-23T06:26:47,28...
Oct 23 06:26:47 localhost.localdomain logstash[2086]: [2023-10-23T06:26:47,43...
Hint: Some lines were ellipsized, use -l to show in full.
[dnzl@localhost ~]$
```

Step 8: save in the repository

```
dnzl@workstation:~/act10$ git add *
```

```
dnzl@workstation:~/act10$ git commit -m "finish naa"
[main 6526801] finish naa
 5 files changed, 191 insertions(+)
 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
 create mode 100644 task.yml
dnzl@workstation:~/act10$ git push origin
Username for 'https://github.com': ddinglasan
Password for 'https://ddinglasan@github.com':
Counting objects: 12, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (8/8), done.
Writing objects: 100% (12/12), 1.72 KiB | 1.72 MiB/s, done.
Total 12 (delta 1), reused 0 (delta 0)
remote: Resolving deltas: 100% (1/1), done.
To https://github.com/ddinglasan/act10.git
   5b22904..6526801  main -> main
```

https://github.com/ddinglasan/act10.git

Reflections:

Answer the following:

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

A log monitoring tool performs real-time or periodic analysis of log files created by software and systems. Its primary roles include early issues detection and identification of problems and errors before they affect the system and user experience. Moreover, it provides security by keeping taps on activities that look suspect. Performance optimizing and resource allocation facilitated by log monitoring, compliance by maintaining and auditing logs for regulatory needs, debugging and troubleshooting simplified, trend analysis for capacity planning, scalability insights, and proactive maintenance lower system downtime and improve system health.

Conclusions:

In this activity, I've learned how to install log monitoring tool, specifically Elastic Stack, into Ubuntu and CentOS computers while what I learned these past activities like implementing roles.