Name: Buenvenida, Ken Benedict	**Date Performed: 10-30-2023**
Course/Section: CPE232-CPE31S4	**Date Submitted: 10-30-2023**
Instructor: Engr. Jonathan Taylar	**Semester and SY: 1st Semester 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: Pull or Clone the Repository that you just created

```
ken@controlNode:~$ git clone git@github.com:KBDBuenvenida/HOA10.git
Cloning into 'HOA10'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
```

Step 2: Create a Playbook named 'elastic.yml'

```
ken@controlNode:~/HOA10$ sudo nano elastic.yml
[sudo] password for ken:
```

Step 3: Create an ansible.cfg or copy the old ansible.cfg in your other directories

```
ken@controlNode:~/HOA9$ sudo cp ansible.cfg ~/HOA10
```

Step 4: Check if the ansible.cfg is in HOA10 directory

```
ken@controlNode:~$ cd HOA10
ken@controlNode:~/HOA10$ ls
ansible.cfg  elastic.yml  README.md
```

Step 5: Create or copy the Inventory file

```
ken@controlNode:~/HOA9$ sudo cp inventory ~/HOA10
```

Step 6: Check if the inventory file is in HOA10 directory

```
ken@controlNode:~/HOA9$ sudo cp inventory ~/HOA10
```

Step 7: Create a directory named 'roles'

```
ken@controlNode:~/HOA10$ mkdir roles
```

Step 8: Create a directory inside roles and name it as elasticsearch, kibana, and logstash

```
ken@controlNode:~/HOA10/roles$ mkdir elasticsearch kibana logstash
ken@controlNode:~/HOA10/roles$ ls
elasticsearch  kibana  logstash
```

Step 9: Create a directory inside each roles named 'tasks'

```
ken@controlNode:~/HOA10/roles/elasticsearch$ mkdir tasks
ken@controlNode:~/HOA10/roles/elasticsearch$ ls
tasks
```

```
ken@controlNode:~/HOA10/roles/kibana$ mkdir tasks
ken@controlNode:~/HOA10/roles/kibana$ ls
tasks
```

```
ken@controlNode:~/HOA10/roles/logstash$ mkdir tasks
ken@controlNode:~/HOA10/roles/logstash$ ls
tasks
```

Step 10: Create a main.yml for Ubuntu

INPUT	`ken@controlNode:~/HOA10/roles/logstash/tasks$ sudo nano main.yml`

PROCESS	`---`
	`- name: Install Logstash in CentOS`
	`  yum:`
	`  name: logstash`
	`  state: present`
	`  when: ansible_distribution == "CentOS"`
	
	`- name: Install Logstash in Ubuntu`
	`  apt:`
	`  name: logstash`
	`  state: present`
	`  when: ansible_distribution == "Ubuntu"`
	
	`- name: Start Logstash`
	`  service:`
	`  name: logstash`
	`  state: started`
	`  enabled: yes`

Step 11: Create a main.yml for CentOS

INPUT	`ken@controlNode:~/HOA10/roles/CentOS/tasks$ sudo nano main.yml` `[sudo] password for ken:`

PROCESS	

```
---
  - name: Enable and start ElasticSearch service
    service:
      name: elasticsearch
      enabled: yes
      state: started

  - name: Enable and start Kibana Service
    service:
      name: kibana
      enabled: true
      state: restarted

  - name: Enable and Start Logstash service
    service:
      name: logstash
      enabled: yes
      state: started
```

Step 12: Test the playbook

INPUT	

```
ken@controlNode:~/HOA10$ sudo nano Elastic.yml
[sudo] password for ken:
```

PROCESS

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

  - name: Install updates (CentOS)
    yum:
      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
```

OUTPUT

```
ken@controlNode:~/HOA10$ ansible-playbook --ask-become-pass Elastic.yml
BECOME password:

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

TASK [Gathering Facts] *********************************************************
ok: [10.0.2.15]
ok: [192.168.56.102]

TASK [Install updates (CentOS)] ************************************************
skipping: [192.168.56.102]
skipping: [10.0.2.15]

TASK [Install updates (Ubuntu)] ************************************************
ok: [10.0.2.15]
ok: [192.168.56.102]

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

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

TASK [Ubuntu : Update apt cache] ***********************************************
changed: [192.168.56.102]
```

```
TASK [Ubuntu : Update apt cache] ************************************************
changed: [192.168.56.102]

TASK [Ubuntu : Install Java] ****************************************************
ok: [192.168.56.102]

TASK [Ubuntu : Enable and Start ElasticSearch service] *************************
ok: [192.168.56.102]

TASK [Ubuntu : Start Elasticsearch service] ************************************
ok: [192.168.56.102]

TASK [Ubuntu : Enable Kibana] ***************************************************
ok: [192.168.56.102]

TASK [Ubuntu : Start Kibana] ****************************************************
ok: [192.168.56.102]

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

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

TASK [Gathering Facts] **********************************************************
ok: [192.168.56.106]

TASK [CentOS : Enable and start ElasticSearch service] *************************
ok: [192.168.56.106]

TASK [CentOS : Enable and start Kibana Service] ********************************
changed: [192.168.56.106]

TASK [CentOS : Enable and Start Logstash service] ******************************
ok: [192.168.56.106]

PLAY RECAP **********************************************************************
192.168.56.102             : ok=10   changed=1    unreachable=0    failed=0    s
kipped=1    rescued=0    ignored=0
192.168.56.106             : ok=6    changed=1    unreachable=0    failed=0    s
kipped=1    rescued=0    ignored=0
```

Step 13: Test if Elasticsearch, Kibana, and Logstash is active

Elasticsearch

```
ken@controlNode2:~$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor>
     Active: active (running) since Sun 2023-10-29 22:44:27 PST; 3h 56min ago
       Docs: https://www.elastic.co
   Main PID: 901 (java)
      Tasks: 65 (limit: 6896)
     Memory: 3.2G
        CPU: 1min 42.095s
     CGroup: /system.slice/elasticsearch.service
             ├─ 901 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+U>
             ├─2853 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.c>
             └─3447 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>

Oct 29 22:36:49 controlNode2 systemd[1]: Starting Elasticsearch...
Oct 29 22:39:19 controlNode2 systemd-entrypoint[901]: Oct 29, 2023 10:39:19 PM >
Oct 29 22:39:19 controlNode2 systemd-entrypoint[901]: WARNING: COMPAT locale pr>
Oct 29 22:44:27 controlNode2 systemd[1]: Started Elasticsearch.
lines 1-17/17 (END)
```

```
[ken@localhost ~]$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vend>
   Active: active (running) since Mon 2023-10-30 02:37:57 PST; 57s ago
     Docs: https://www.elastic.co
 Main PID: 2982 (java)
    Tasks: 82 (limit: 23004)
   Memory: 1.6G
   CGroup: /system.slice/elasticsearch.service
           ├─2982 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+Use>
           ├─3075 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cac>
           └─3134 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86>

Oct 30 02:29:49 localhost.localdomain systemd[1]: Starting Elasticsearch...
Oct 30 02:32:55 localhost.localdomain systemd-entrypoint[2982]: Oct 30, 2023 2:>
Oct 30 02:32:55 localhost.localdomain systemd-entrypoint[2982]: WARNING: COMPAT>
Oct 30 02:37:57 localhost.localdomain systemd[1]: Started Elasticsearch.
lines 1-16/16 (END)
```

Kibana

```
ken@controlNode2:~$ systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/lib/systemd/system/kibana.service; enabled; vendor preset>
     Active: active (running) since Sun 2023-10-29 22:23:55 PST; 5s ago
       Docs: https://www.elastic.co
   Main PID: 5231 (node)
      Tasks: 7 (limit: 4599)
     Memory: 43.2M
        CPU: 709ms
     CGroup: /system.slice/kibana.service
             └─5231 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bi>

Oct 29 22:23:55 controlNode2 systemd[1]: Started Kibana.
Oct 29 22:23:56 controlNode2 kibana[5231]: Kibana is currently running with leg>
lines 1-13/13 (END)
[2]+  Stopped                 systemctl status kibana
^Z
```

```
[ken@localhost ~]$ systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; vendor pres>
   Active: active (running) since Sun 2023-10-29 22:34:03 PST; 4s ago
     Docs: https://www.elastic.co
 Main PID: 45175 (node)
    Tasks: 7 (limit: 10927)
   Memory: 16.0M
   CGroup: /system.slice/kibana.service
           └─45175 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin>

Oct 29 22:34:03 localhost.localdomain systemd[1]: Started Kibana.
Oct 29 22:34:06 localhost.localdomain kibana[45175]: Kibana is currently runnin>
lines 1-12/12 (END)
```

Logstash

```
ken@controlNode2:~$ systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/lib/systemd/system/logstash.service; enabled; vendor pres>
     Active: active (running) since Sun 2023-10-29 22:27:51 PST; 7s ago
   Main PID: 5473 (java)
      Tasks: 14 (limit: 4599)
     Memory: 150.5M
        CPU: 2.518s
     CGroup: /system.slice/logstash.service
             └─5473 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.h>

Oct 29 22:27:51 controlNode2 systemd[1]: Started logstash.
Oct 29 22:27:55 controlNode2 logstash[5473]: Using bundled JDK: /usr/share/logs>
lines 1-12/12 (END)
```

```
[ken@localhost ~]$ sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /
usr/lib/systemd/system/logstash.service.
[ken@localhost ~]$ sudo systemctl start logstash
[ken@localhost ~]$ systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/usr/lib/systemd/system/logstash.service; enabled; vendor pr>
   Active: active (running) since Mon 2023-10-30 02:05:35 PST; 10s ago
 Main PID: 9091 (java)
    Tasks: 14 (limit: 10927)
   Memory: 172.8M
   CGroup: /system.slice/logstash.service
           └─9091 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.hea>

Oct 30 02:05:35 localhost.localdomain systemd[1]: Started logstash.
Oct 30 02:05:35 localhost.localdomain logstash[9091]: Using bundled JDK: /usr/s>
lines 1-11/11 (END)
```

Step 14: Check if its working in the web browser
Ubuntu

localhost:9200/

localhost:9200

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON


```
name:                                  "controlNode2"
cluster_name:                          "elasticsearch"
cluster_uuid:                          "SJ6gfrWnSwa_VppTO7ozsA"
version:
  number:                              "8.10.4"
  build_flavor:                        "default"
  build_type:                          "deb"
  build_hash:                          "b4a62ac808e886ff032700c391f45f1408b2538c"
  build_date:                          "2023-10-11T22:04:35.506990650Z"
  build_snapshot:                      false
  lucene_version:                      "9.7.0"
  minimum_wire_compatibility_version:  "7.17.0"
  minimum_index_compatibility_version: "7.0.0"
tagline:                               "You Know, for Search"
```


Home - Elastic

localhost:5601/app/home#/

Welcome to Elastic

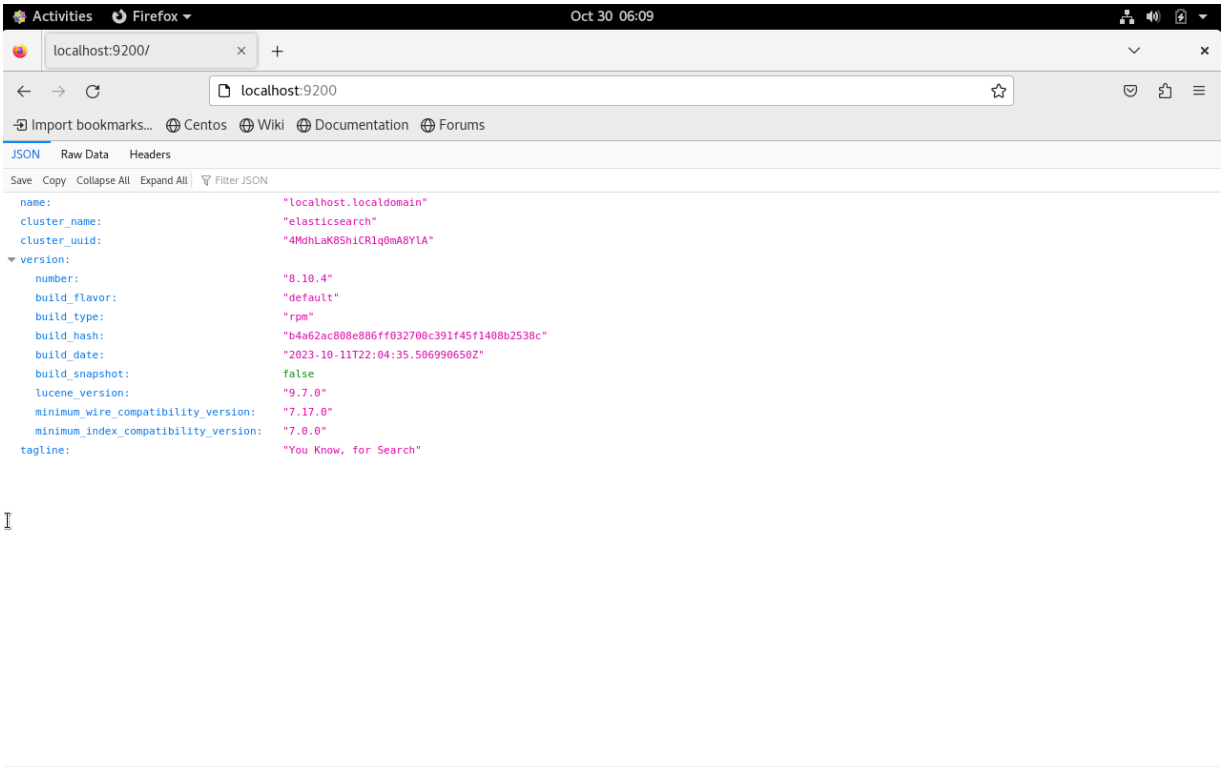
Start by adding integrations

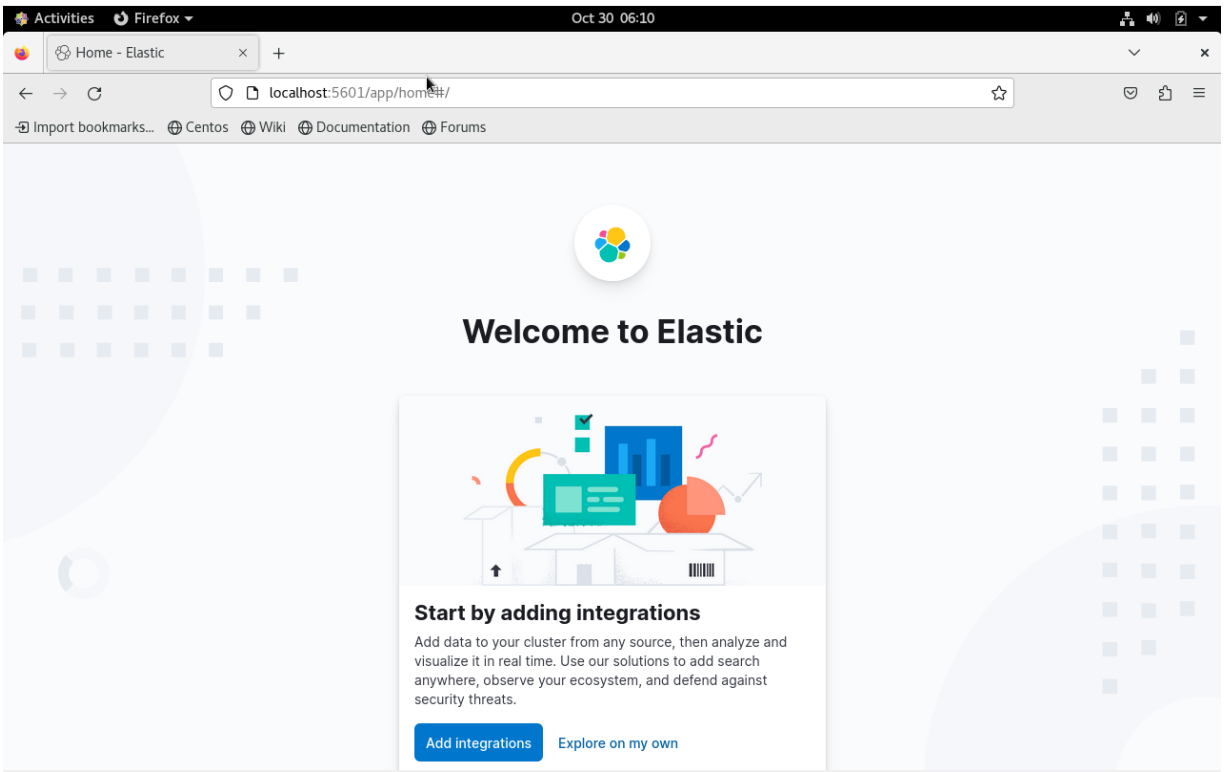
Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and defend against security threats.

Add integrations Explore on my own

Usage collection is enabled. This allows us to learn what our users

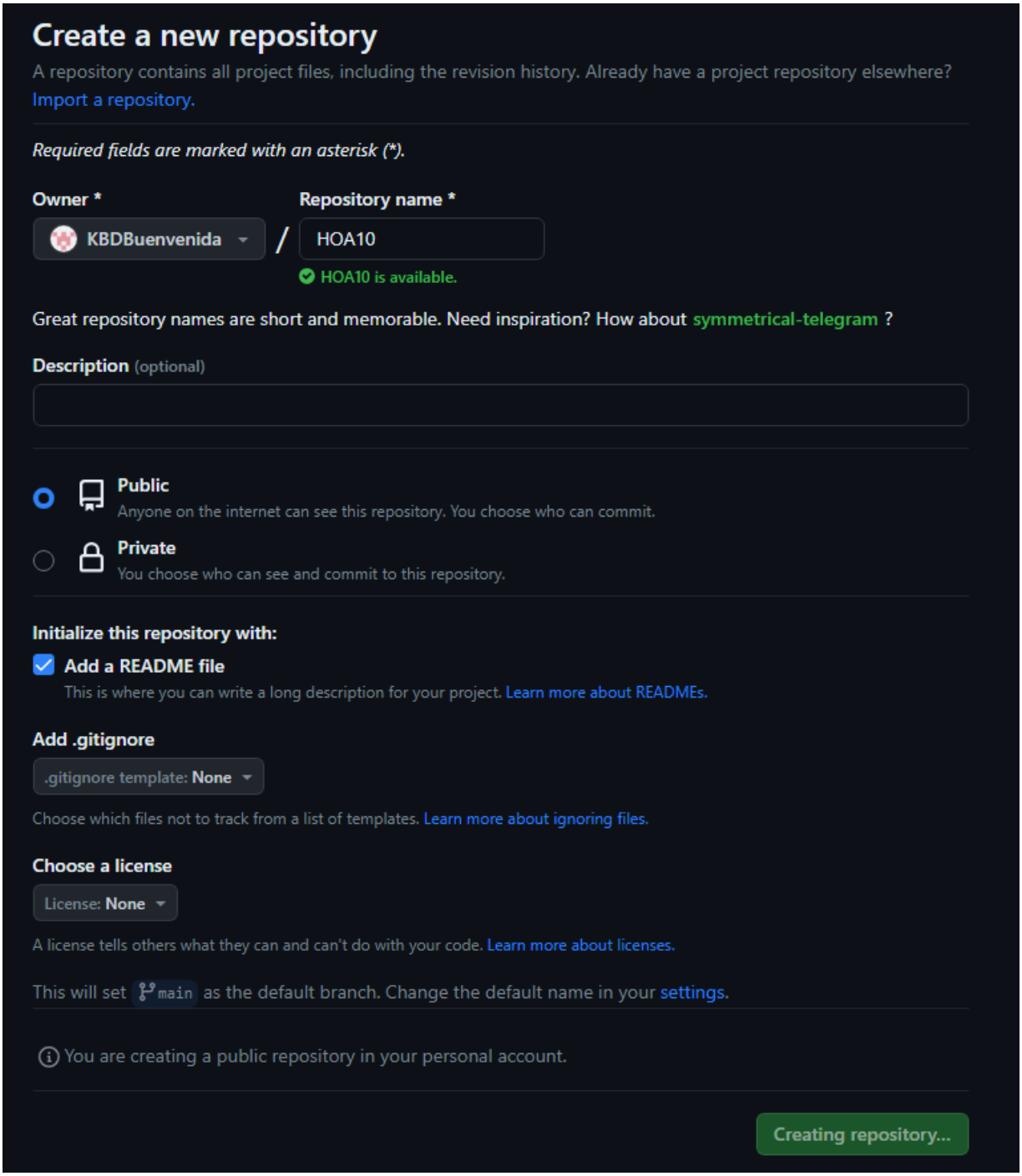
CentOS


Activities
Firefox
Oct 30 06:09
localhost:9200/
localhost:9200
Import bookmarks...
Centos
Wiki
Documentation
Forums
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON
name: "localhost.localdomain"
cluster_name: "elasticsearch"
cluster_uuid: "4MdhLaK8ShiCR1q0mA8YlA"
version:
number: "8.10.4"
build_flavor: "default"
build_type: "rpm"
build_hash: "b4a62ac808e886ff032700c391f45f1408b2538c"
build_date: "2023-10-11T22:04:35.506990650Z"
build_snapshot: false
lucene_version: "9.7.0"
minimum_wire_compatibility_version: "7.17.0"
minimum_index_compatibility_version: "7.0.0"
tagline: "You Know, for Search"

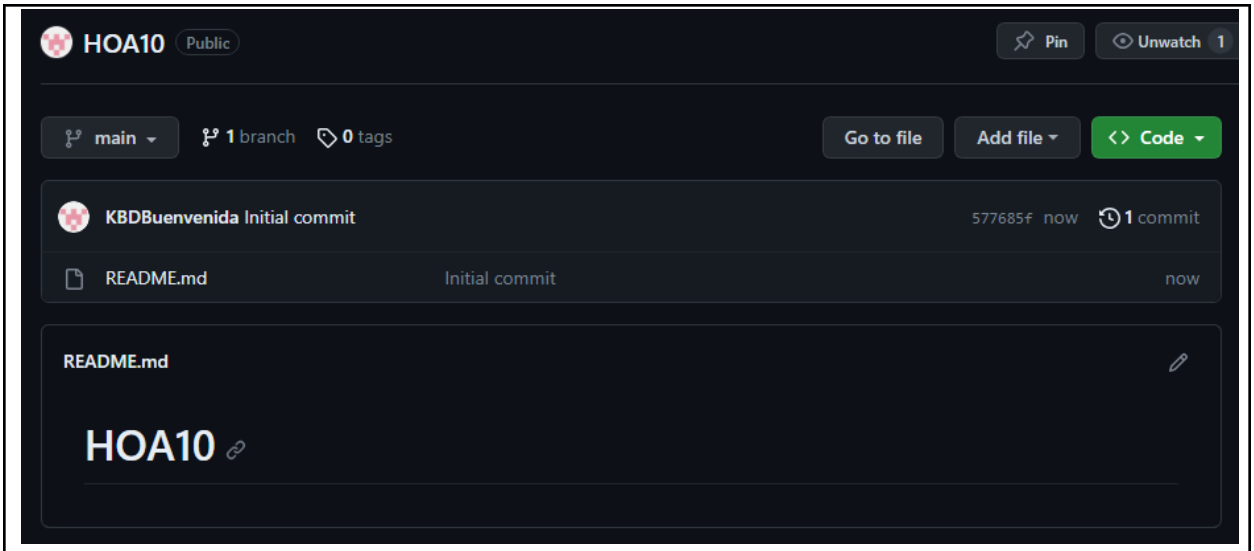

Activities
Firefox
Oct 30 06:10
Home - Elastic
localhost:5601/app/home#/
Import bookmarks...
Centos
Wiki
Documentation
Forums
Welcome to Elastic
Start by adding integrations
Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and defend against security threats.
Add integrations
Explore on my own

5. Make sure to create a new repository in GitHub for this activity.

Step 15:Create a Repository named 'HOA10'



Step 16:Check if the new repository is created



Step 17: Git add *

```
ken@controlNode:~/HOA10$ git add *
```

Step 18: Git commit -m “HOA10”

```
ken@controlNode:~/HOA10$ git commit -m "HOA10"
[main b64a5b0] HOA10
 6 files changed, 144 insertions(+)
 create mode 100644 Elastic.yml
 create mode 100644 ansible.cfg
 create mode 100644 inventory
 create mode 100644 roles/CentOS/tasks/main.yml
 create mode 100644 roles/Ubuntu/main.yml
 create mode 100644 roles/Ubuntu/tasks/main.yml
```

Step 19: Git push origin

```
ken@controlNode:~/HOA10$ git push origin
Enumerating objects: 14, done.
Counting objects: 100% (14/14), done.
Compressing objects: 100% (10/10), done.
Writing objects: 100% (13/13), 1.62 KiB | 1.62 MiB/s, done.
Total 13 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), done.
To github.com:KBDBuenvenida/HOA10.git
   577685f..b64a5b0  main -> main
```

Reflections:

Answer the following:

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

- **ELK Stack can be used to monitor performance and health of the user's system and application. The user can use it to track CPU usage, memory usage, and response times. It can also be used to provide alerts when errors or problems are detected. ELK Stack can also be used to analyze the user's business data to gain insights to customers, products, and operations. ELK Stack is a good choice for organizations that are looking to improve their log management and analytics capabilities.**

Conclusions:

- **What I did in this activity is to manually install ELK Stack since everytime I try to install it using a playbook it displays an error or it corrupts my virtual machine. In conclusion, I learned a lot about ELK Stack in this activity and that it can be used to monitor my machine performance and health. It was stressful to do at first but once I was able to start the ELK Stack it was smooth after that, I was able to use and setup elasticsearch, kibana, and logstash. I was able to use ELK Stack in a browser where I can use a lot of their features.**