Name: Aaron Valencia	Date Performed: 11/04/2024
Course/Section: CPE 212-CPE31S2	Date Submitted: 11/04/2024
Instructor: Robin Valenzuela	Semester and SY: 1st sem

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.

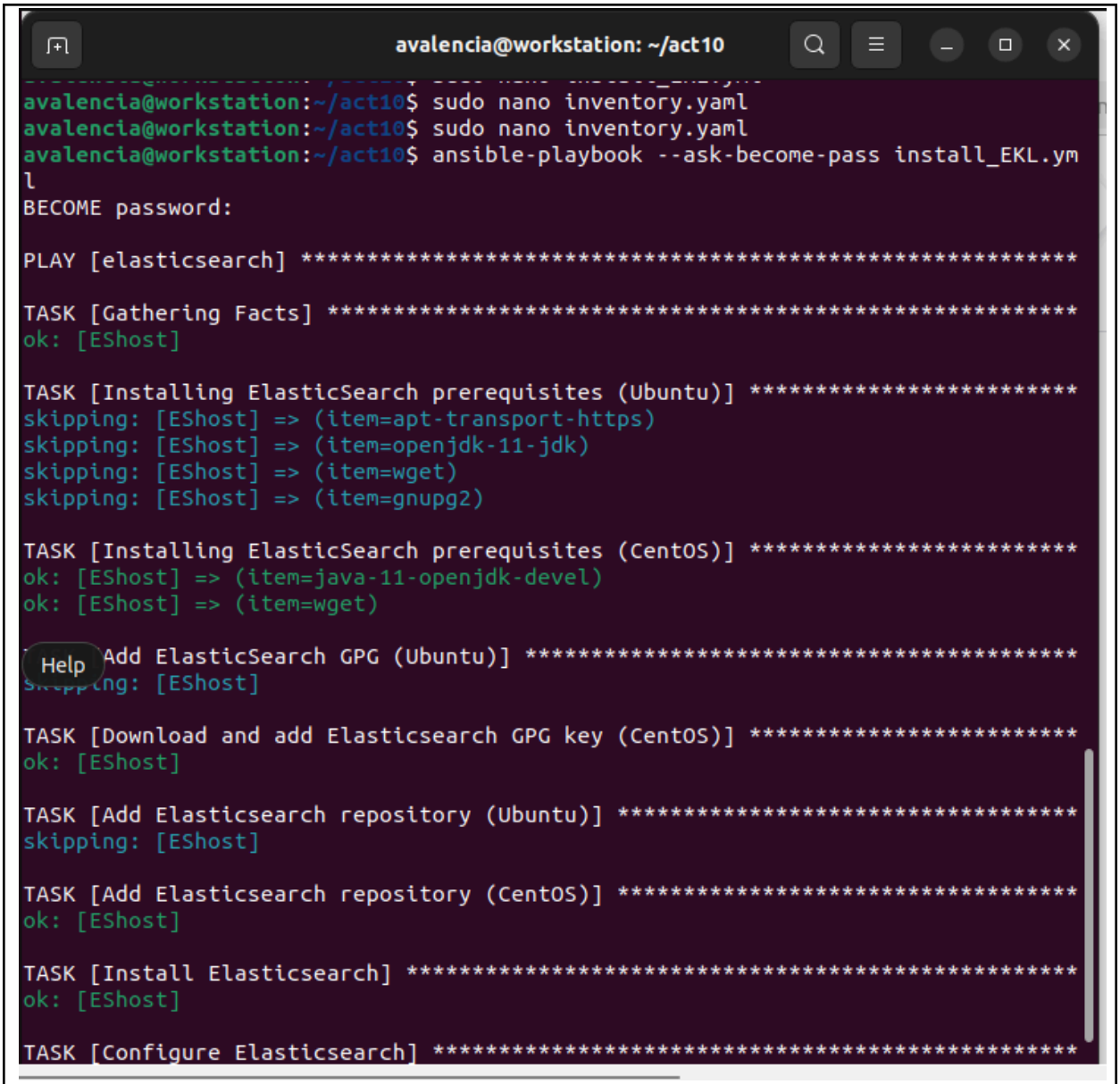
We use Graylog primarily as the stash for the logs of the web applications we build. However, it is also effective when working with raw strings (i.e. syslog): the tool parses it into the structured data we need. It also allows advanced custom search in the logs using structured queries. In other words,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



- I did step one by downloading each package for ElasticSearch, Kibana, and Logstash

Code | Blame | 20 lines (20 loc) · 430 Bytes | Code 55% faster with GitHub Copilot

```
all:
  vars:
    ansible_user: avalencia
    ansible_ssh_private_key_file: /home/avalencia/.ssh/id_rsa
  hosts:
  children:
    elasticsearch:
      hosts:
        EShost1:
          ansible_host: 192.168.56.112
        EShost2:
          ansible_host: 192.168.56.119
    kibana:
      hosts:
        Khost1:
          ansible_host: 192.168.56.113
    logstash:
      hosts:
        Lhost1:
          ansible_host: 192.168.56.115
```

- I applied roles in the inventory.yaml so different server hosts will have different roles like for example server1 and server2 is for ElasticSearch, server3 is for Kibana and CentOS for logstash

- I first installed the needed prerequisite for installing and configuring for each package like here in ElasticSearch

```
---
- hosts: elasticsearch
  become: true
  tasks:
    - name: Installing ElasticSearch prerequisites (Ubuntu)
      apt:
        name: "{{item}}"
        state: present
      loop:
        - apt-transport-https
        - openjdk-11-jdk
        - wget
        - gnupg2
      when: ansible_distribution == "Ubuntu"

    - name: Installing ElasticSearch prerequisites (CentOS)
      yum:
        name: "{{item}}"
        state: present
      loop:
        - java-11-openjdk-devel
        - wget
      when: ansible_distribution == "CentOS"
```

- Then added the GPG key and repository of each packages also
- After that is the main installation
- Then configuring
- And lastly, enabling the services of EKL

Reflections:

Answer the following:

1. What are the benefits of having log monitoring tool?
   Having a log monitoring tool such as the ELK stack is having a tool for managing and analyzing the logs. It has great flexibility, scalability and security in terms of handling many servers/hosts

Conclusions:

Log monitoring is a must especially in larger scale project servers. It needs great security and management in handling that many server hosts in one admin. Tools such as the ELK stack offers a set of tools for handling and analyzing log data instantly in a manner, like real time analysis capabilities and scalability options that improve security monitoring and application performance for organizations seeking to boost their data analysis efforts.