| **Name:** Torrecampo, Juan Piolo S. | **Date Performed:** Oct 21, 2022 |
| --- | --- |
| **Course/Section:** CPE 232 / CPE31S22 | **Date Submitted:** Oct 24, 2022 |
| **Instructor:** Dr. Jonathan Taylar | **Semester and SY:** 1st Sem, 2022 - 2023 |
| **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. | |
| 1. **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](http://www.g2.com/categories/it-alerting-software), [log analysis software](http://www.g2.com/categories/log-analysis), 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](https://www.elastic.co/elk-stack)).  The Elastic Stack is a group of open source products from [Elastic](https://www.techtarget.com/searchitoperations/definition/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](https://www.techtarget.com/searchitoperations/definition/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](https://www.techtarget.com/searchcloudcomputing/definition/Software-as-a-Service)). Elasticsearch supports Amazon Web Services (AWS), Google Cloud Platform and Microsoft Azure.  Source: <https://www.elastic.co/elastic-stack>  **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-sourc](https://www.graylog.org/products/open-source)e  **Requirements:**   * 3 VMs for ElasticSearch Server, Kibana, and Logstash | |
| 1. **Tasks** | |
| 1. Create a playbook that:    1. 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. | |
| 1. **Output** (screenshots and explanations)   **STEP 1. Create a new repository and clone it into your machine.**    *Figure 1.1. Github page of the new repository.*    *Figure 1.2. Cloning the recently created repository in the host machine.*  **STEP 2. Copy the inventory and ansible.cfg from the previous repository in Activity 9*.***    *Figure 1.3. Copying the inventory and ansible.cfg from the previous repository.*  **STEP 3. Create the needed files and directories, as shown in *Figure 1.4.***    *Figure 1.4. Tree structure of the directory.*    *Figure 1.5. Creating the needed files and directories inside of the repository.*  **STEP 4. Modifying the inventory file to support three servers. Each server corresponds to the**  **three softwares of the elastic stack.**    *FIgure 1.6. The screenshot above shows the contents of the inventory file after modifying it.*  **STEP 5. Creating the tasks of install\_elastic\_stack.yml. This serves as your main control to the whole playbook.**    *Figure 1.7. Contents of install\_elastic\_stack.yml.*  **STEP 6. Adding repo contents to the .repos files. The contents below are the same with logstash.repo.**    *Figure 1.8. Contents of kibana.repo file.*    *Figure 1.9. Contents of logstash.repo file.*  **STEP 7. Adding contents to the roles.**      *Figure 1.10. The screenshot above shows the installing and configuration script for elastic search where the roles are implemented.*    *Figure 1.11. The screenshot above shows the installing and configuration script for logstash where the roles are implemented.*      *Figure 1.12. The screenshot above shows the installing and configuration script for kibana where the roles are implemented.*  **STEP 8. Checking SSH connection and for syntax errors by running “ansible all -m ping” for the remote connection and ”ansible-playbook –syntax-check file.yml” for syntax checking.**      *Figure 1.13. Conducting a test to make sure the three servers are capable in running ssh.*    *Figure 1.14. Verifying that the playbook has no errors.*  **STEP 9. Run the playbook. The provided tags can be used to install the applications separately.**      *Figure 1.15. The screenshot above shows the result after running the install\_elastic\_stack.yml with the tag of es that stands for elastic search.*      *Figure 1.16. The screenshot above shows the result after running the install\_elastic\_stack.yml with the tags of kibana.*    *Figure 1.17. The screenshot above shows the result after running the install\_elastic\_stack.yml with the tags of logstash.*  **STEP 10. Verifying that the elastic stack is functional.**   | **VERIFYING THE INSTALLATION FOR ELASTIC STACK** | | | | --- | --- | --- | | **Name** | **Screenshot** | | | Kibana | Kibana Service    Kibana’s web page. | | | Elastic Search | Elasticsearch Service    Verifying if the cluster is running.    Elasticsearch Open Ports    Web view of the elastic search cluster. | | | Logstash | Logstash Service    Logstash Open Ports | |   *Table 1.1. The table above shows the proof that the software is currently running on a server.*  **STEP 11. Pushing the updated repo to Github.**    *Figure 1.18. The screenshot above shows the command used in pushing the files.*    *Figure 1.19. The screenshot above shows my updated Github page.*  **References:**  [*https://www.elastic.co/guide/en/logstash/8.4/running-logstash.html*](https://www.elastic.co/guide/en/logstash/8.4/running-logstash.html)  [*https://www.elastic.co/guide/en/elasticsearch/reference/current/deb.html*](https://www.elastic.co/guide/en/elasticsearch/reference/current/deb.html)  [*https://www.elastic.co/guide/en/kibana/current/deb.html*](https://www.elastic.co/guide/en/kibana/current/deb.html)  [*https://thelionping.com/elasticsearch-and-kibana-installation-and-configuration/*](https://thelionping.com/elasticsearch-and-kibana-installation-and-configuration/)  **Github Link:** <https://github.com/piolotorrecampo/CPE232-Activity_10.git> | |
| **Reflections:**  Answer the following:   * 1. What are the benefits of having a log monitoring tool? * The benefits of having a monitoring tool is that a system administrator can monitor multiple servers without physically interacting with it. This activity introduces the concept of elastic stack. The elastic stack is a group of three softwares that focuses on obtaining data from the server and process that data then visualize them. One of the members of the elastic stack is the Logstash. Logstash is used to obtain logs from the servers and filter them and forward them to the elastic search. The elastic search on the other hand is the database wherein the logs are being stored. The visualization of data happens in Kibana. Kibana learns the data and expresses it into a graph form for better understandment. | |
| **Conclusions:**  The activity achieved its goal to install and configure enterprise log monitoring tools. It introduces the new enterprise log monitoring tools called the elastic stack or ELK stack. The ELK stack is abbreviated from Elasticsearch, Logstash and KIbana. Connecting the softwares is called the elastic stack. The Logstash is used to obtain and filter the data from the servers then store them to the Elasticsearch. Therefore, Elasticsearch is the database where this data can be displayed through Kibana. On the other hand the Kibana is used to visualize the data from the server like a spreadsheet with graphs. | |
| **Honor Pledge:**  *“I affirm that I will not give or receive unauthorized help on this activity and that all will be my own.”* | |