Assignment Name: Log Management Using ELK
Duration : 2 weeks (Starting from September 3rd , 2021 To 17 th of September)
Operation system: Ubuntu 20.04

Note: Completed assignments should be submitted via http://school.wso2.com. Assignment answer file must be named as Log_Management_Using_ELK.pdf

Create a document that includes necessary screenshots and answer the questions after doing research by yourself.

Log Management Using ELK Stack Assignment

In WSO2 we don't have a proper log management solution for the production environment and the operations team decided to use ELK stack for log management and analysing. Already we have a legacy syslog server environment to collect server logs. We need to collect and analyze those logs as well using the ELK. So as a systems engineer in WSO2 you are going to implement the following solution in the environment.

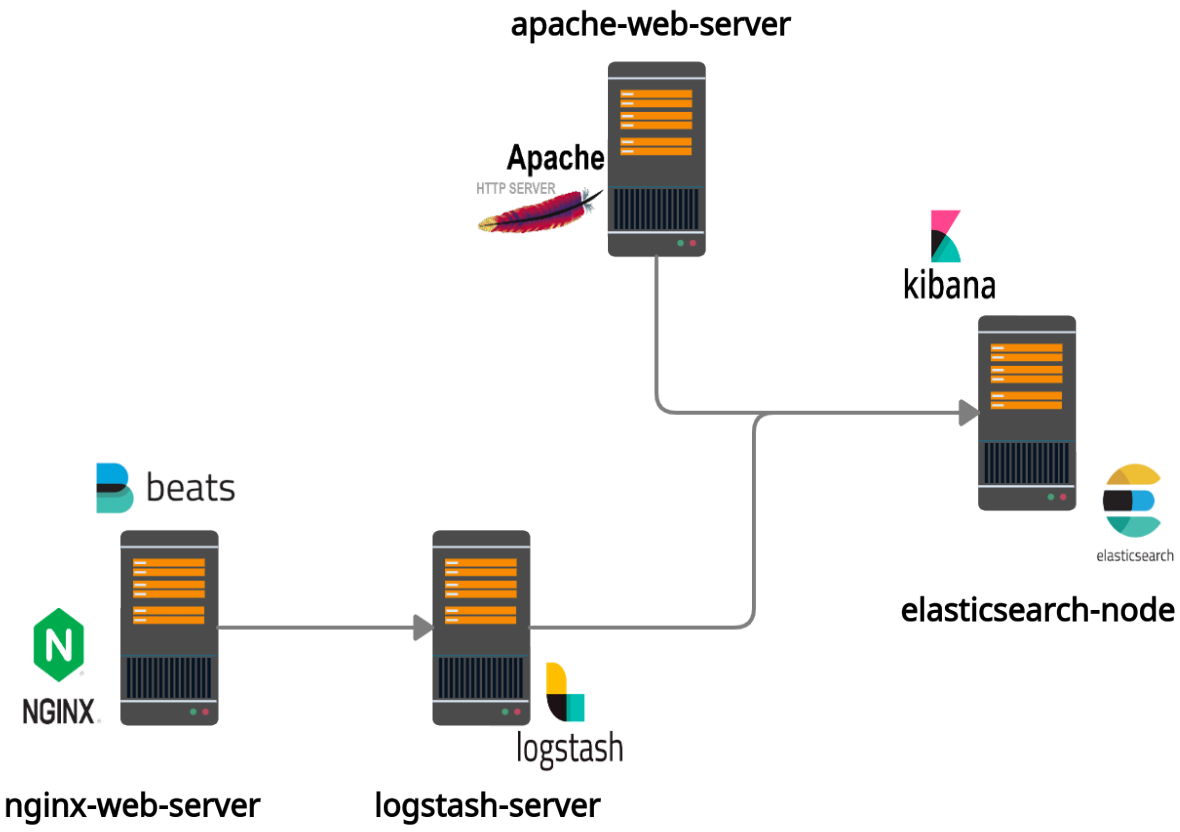
In order to deploy this solution, you need to create at least 5 virtual machines. You can use GCP or a self hosted virtualization platform as your preference.

Part -1

When you are implementing the following solution, make sure to follow the pointed guidelines.
Ref : https://github.com/MadawaLakmal/log-management-using-ELK

1. All hosted os environments should install Ubuntu 20.04 LTS version.
2. You need to set up all the hostnames as follows.
    - Let's consider nginx-web-server,
        - HostName should be "Your User ID-nws" (i.e : LT-xxxxx-nws)
3. For the elasticsearch node, use at least 4GB memory. You can install the kibana dashboard inside the elasticsearch node.
4. Need to install logstash service inside the logstash-server.

5. Apache2 web server needs to be installed inside the apache-web-server and nginx web server should run inside the nginx-web-server.
6. Each web server should serve a web page containing “Hello From $web server name” heading. ($web server name = Nginx or Apache)
7. Change the default syslog template to print syslog severity and severity text on every server as demonstrated.
8. You should send nginx web logs and syslog log data inside nginx web-server to elasticsearch via logstash node. To do that please use filebeat as logshipper in the nginx-webs-erver. [**Don’t customize filebeat log paths for nginx logs in /etc/filebeat/system.yml file, Need to use nginx module instead**]
9. You need to send all the apache-web-server logs and its syslogs directly to elasticsearch node.



Part -2

After the cluster up and running,

1. Create a table which contains **HostName** & **IP Address.**
2. After login to the kibana you need to create a index pattern called filebeat-* and collect all the indexed data under it.Then you can visualize those data inside the kibana **Discover** tab. You need to select the following fields under the filter by type and take a screen-shot to attach.
    - Field types,
        i. clientip
        ii. host
        iii. _index
        iv. message
3. Search for keyword “Severity” in the KQL search bar and attach a screenshot.
4. Search for keyword “your nginx-web-server hostname” in the KQL search bar and attach a screenshot.
5. Search for keyword “your apache-web-server hostname” in the KQL search bar and attach a screenshot.
6. Attach a screen-shot of the main config file respectively to each ELK stack config file and Beat configs that you have added.
    - **I.e :** for **filebeat -> /etc/filebeat/filebeat.yml** file and **/etc/filebeat/modules.d/$module_name** file**.**
7. Demonstrate CRUD operations in Dev Tools and attach a screenshot. You can use any example you wish.

Part- 3

After the previous screenshots, You need to describe the following topics briefly.

1. What is an index, shard and replica-shard?
2. How does sharding help for performance?
3. What is Hot-Warm architecture?
4. How does hot-warm architecture help for data management?
5. Compare the performance of Hot, Warm, Cold and Frozen nodes.
6. Describe How did you achieve the 10th point of Part -1.
7. What are elasticsearch based products currently available in the market as log management solutions.Give a brief comparison about at least 3 products.

Each question of Part- 3 should have more than 75 words in each.

You can contact us regarding any concern at any time through the slack channel or writing to madawa@wso2.com.