ALX PROJECT: Web Infrastructure Design

Task 2. Secured and monitored web infrastructure

Definitions and Explanations.

1. For every additional element, why you are adding it:

Three new elements have been incorporated: an individual firewall for each server to shield them from potential attacks and exploitation, the implementation of an SSL certificate on the server www.foobar.com to ensure secure communication over HTTPS, and the integration of three monitoring clients responsible for collecting logs and forwarding them to our data collector, Sumologic

2. What are firewalls for:

Functions as a network security mechanism that observes and manages both incoming and outgoing network traffic according to predefined security rules. Essentially, it creates a protective barrier between a network considered trustworthy and one deemed untrustworthy.

3. Why is the traffic served over HTTPS:

Previously, data transmission occurred through the Hypertext Transfer Protocol (HTTP), which transfers information in plain text. In contrast, HTTPS ensures security by encrypting data through Transport Layer Security (TLS).

4. What monitoring is used for:

It furnishes the ability to identify and proactively diagnose any performance issues in web applications.

5. How the monitoring tool is collecting data:

Gathers logs from the application server, MySQL Database, and Nginx web server. In the realm of computing, a log refers to the automatically generated and timestamped documentation of events pertinent to a specific system

6. Explain what to do if you want to monitor your web server QPS:

one web server handles 1K queries per second (QPS), I would basically monitor it from the network and application level.

Issues

A. Why terminating SSL at the load balancer level is an issue:

Terminating SSL (Secure Sockets Layer) at the load balancer means that the load balancer decrypts the incoming SSL traffic and then forwards the requests to the backend servers over an unencrypted connection.

B. Why having only one MySQL server capable of accepting writes is an issue:

In a web application, the MySQL server is responsible for handling database read and write operations. Having only one MySQL server that can accept write operations introduces several issues.

C. Why having servers with all the same components (database, web server and application server) might be a problem:

this is because once you have a bug in one of the components in one of the servers then the bug will be valid in the other servers.