ALX Project

Web Infrastructure Design

Task 2: Definitions and Explanations

1. The rationale behind adding three new components is as follows: implementing a firewall for each server aims to protect them from potential attacks and exploitation. Additionally, an SSL certificate has been applied to the www.foobar.com server over HTTPS to enhance security through encrypted data transfer. Three monitoring clients have been introduced to collect logs systematically and send them to our data collector, Sumologic.

2. Firewalls serve as a network security system that monitors and manages both incoming and outgoing network traffic based on predefined security rules. Essentially, they establish a protective barrier between a trusted network and an untrusted one.

3. The adoption of HTTPS for serving traffic is crucial due to the inherent security enhancements it offers. While HTTP transfers data in plain text, HTTPS encrypts the data using Transport Layer Security (TLS), ensuring a secure and private communication channel.

4. Monitoring is implemented to proactively detect and diagnose any performance issues within the web application, providing a comprehensive view of its operational health.

5. The monitoring tool collects data by capturing logs from the application server, MySQL Database, and Nginx web server. In a computing context, a log is an automatically generated, time-stamped documentation of events relevant to a specific system.

6. To monitor the web server's Query Per Second (QPS), the suggested approach involves monitoring it at both the network and application levels, particularly focusing on its capability to handle 1,000 queries per second.

Issues

A. Terminating SSL at the load balancer level is considered problematic because decryption is resource and CPU-intensive. While it offloads processing power to the server for application tasks, the exact issue may need further clarification and will be updated accordingly.

B. Having only one MySQL server capable of accepting writes is an issue because if it goes down, no new data can be added or updated, impacting the functionality of certain application features.

C. The potential problem with having servers equipped with identical components (database, web server, and application server) lies in the risk of a bug affecting one server propagating to others. If a bug exists in one component on one server, it becomes a universal issue across all servers, potentially causing widespread problems.