ALX Web Infrastructure Tasks:

task2:

1. **Purpose of Additional Elements**:
    - Load Balancers: Added to distribute incoming traffic evenly across multiple servers, ensuring high availability and scalability.
    - Firewalls: Implemented to control and monitor incoming and outgoing network traffic, enhancing security by filtering out potentially malicious or unauthorized access attempts.
    - HTTPS: Ensures secure communication over the internet by encrypting data transmitted between clients and servers, protecting against eavesdropping and data tampering.
    - Monitoring Tools: Deployed to track system performance, detect anomalies, and troubleshoot issues proactively, ensuring optimal operation and minimizing downtime.
2. **Purpose of Firewalls**: Firewalls are used to monitor and control incoming and outgoing network traffic based on predetermined security rules. They serve to protect the infrastructure from unauthorized access, malware, and other cyber threats by filtering and blocking potentially harmful traffic.
3. **HTTPS for Traffic**: HTTPS encrypts data transmitted between clients and servers, providing confidentiality and integrity during communication. It prevents eavesdropping, data tampering, and man-in-the-middle attacks, ensuring secure transmission of sensitive information over the internet.
4. **Purpose of Monitoring**: Monitoring is used to track system performance, detect issues or anomalies, and ensure the availability, reliability, and security of the infrastructure. It helps identify potential problems before they escalate, allowing for proactive maintenance and troubleshooting.
5. **Data Collection by Monitoring Tool**: Monitoring tools collect data through various means, such as system logs, performance metrics, network traffic analysis, and application instrumentation. They utilize agents, sensors, or APIs to gather information from different components of the infrastructure, providing insights into system health and performance.
6. **Monitoring Web Server QPS**:
    - Install a monitoring agent or software on the web server.
    - Configure the monitoring tool to collect and analyze data related to request counts or queries processed per second (QPS).
    - Set up alerts or notifications to notify administrators of any unusual spikes or drops in QPS.
    - Monitor server performance metrics to ensure optimal operation and scalability.

Issues with the infrastructure:

1. **Terminating SSL at Load Balancer Level**: Terminating SSL at the load balancer exposes decrypted data within the internal network, increasing the risk of data exposure or interception. This undermines end-to-end encryption and compromises data confidentiality and integrity.

2. **Single MySQL Server for Writes**: Relying on a single MySQL server for write operations introduces a single point of failure. If the server fails, it can result in data loss, downtime, and service disruption, impacting the availability and reliability of the application.
3. **Identical Components on Servers**: Having servers with identical components (database, web server, and application server) may lead to homogeneity-related issues. For instance, if a vulnerability affects one component, it could potentially impact all servers simultaneously, increasing the likelihood of widespread service outages or security breaches. Additionally, it may hinder scalability and flexibility in optimizing server resources for different workload demands.

References

1st Reference

2nd Reference

3rd Reference