ALX - Web infrastructure design
1-distributed_web_infrastructure

Additional Elements and Their Purpose:

Firewalls: Firewalls are added to enhance security by controlling incoming and outgoing network traffic. They act as barriers against unauthorized access and potential threats.

SSL Certificate: An SSL certificate is used to encrypt the communication between users' browsers and the web server. This ensures secure transmission of sensitive information and enhances data protection.

Monitoring Clients: Monitoring clients collect data on server performance and other metrics. This data is sent to the monitoring service for analysis and issue detection.

Load Balancer Distribution Algorithm:

The load balancer is configured with a Round Robin distribution algorithm. It works by distributing incoming requests equally among the available application servers in a circular manner.

Load Balancer Setup - Active-Active vs. Active-Passive:

The load balancer is enabling an Active-Passive setup. In an Active-Passive setup, one load balancer is actively managing the traffic, while the other serves as a standby. If the active load balancer fails, the passive one takes over.

Database Primary-Replica (Master-Slave) Cluster:

In a Primary-Replica (Master-Slave) cluster, the Primary (Master) database handles write operations and updates. The Replica (Slave) database(s) replicate data from the Primary and handle read operations. This improves read scalability and provides redundancy.

Difference between Primary and Replica in Regard to the Application:

Primary Node: The primary database handles write operations and updates from the application. It's the authoritative source of data and processes data modifications.

Replica Node: The replica database serves read requests from the application. It mirrors data from the primary and provides scalability for read-heavy operations. However, it's read-only and can't be used for write operations.

Issues with the Infrastructure:

Single Point of Failure (SPOF): Single points of failure exist in the setup, such as having only one MySQL master. If it fails, it could disrupt the entire database operation.

Security Issues (No Firewall, No HTTPS): The absence of firewalls leaves the infrastructure vulnerable to unauthorized access and cyberattacks. Not using HTTPS exposes user data to interception and compromise.

No Monitoring: Without monitoring, it's challenging to detect performance issues or security breaches promptly. Lack of monitoring reduces visibility into the health and performance of the infrastructure.

Addressing these issues involves implementing redundancy, firewall protection, HTTPS encryption, and setting up monitoring to ensure a more secure, resilient, and reliable infrastructure.