ALX PROJECT: Web Infrastructure Design

Task 1: Distributed Web Infrastructure

1. Purpose of Adding Additional Elements:

   Adding more servers is crucial for introducing a load balancer, which helps manage high traffic efficiently. This step not only deals with potential traffic spikes but also reduces the risk of system failure that comes with relying on a single server.

2. Load Balancer Distribution Algorithm:

   Our load balancer uses the Round Robin algorithm, which distributes requests to servers in a sequential order, unless a server is offline. It systematically sends requests to each server one by one, starting from the first server after reaching the last. This algorithm works well when servers have similar specifications and there are limited persistent connections.

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

   Our load balancer is configured for an Active-Active setup, where both servers operate simultaneously. In contrast, an Active-Passive setup has one server active while the other remains in standby. Active-Active provides continuous access to resources from all servers, while Active-Passive only activates backup servers during failover events.

4. Master-Slave Replication:

   In Master-Slave replication, data from a master database server is copied to one or more slave servers. The master records updates, which are then replicated to the slaves. Replication can be synchronous (updates happen simultaneously) or asynchronous (updates are queued and written later). This method enhances scalability and can serve failover or data analysis purposes.

5. Primary vs. Replica Node:

   A replica node duplicates the primary node, serving as a backup with redundant copies of the application codebase. This redundancy protects against hardware failures and improves the system's ability to handle read requests, such as document retrieval.

Issues:

A. Single Point of Failure (SPOF):

The reliance on a single load balancer creates a vulnerability known as Single Point Of Failure (SPOF).

B. Security Concerns:

Security issues include the absence of a firewall and the use of the insecure HTTP protocol, which exposes sensitive information to potential interception. Lack of a firewall makes the system vulnerable to denial-of-service (DoS or DDoS) attacks.

C. Absence of Monitoring:

Monitoring is essential for identifying and addressing issues, downtimes, or security threats proactively. It helps improve productivity, reduce IT support costs, and enhance user experience.