Definitions and Explanations

Purpose of Adding Additional Elements: The addition of new servers serves two key purposes: firstly, to implement a load balancer capable of managing high incoming traffic loads, and secondly, to eliminate the risk of a single point of failure, which can arise when relying on a single server.

Load Balancer Distribution Algorithm and Functionality: Our load balancer employs the Round Robin algorithm, which sequentially connects requests to servers unless a server is offline. Requests are served in a cycle from the first to the last server, then the cycle repeats. This algorithm suits cases where servers have equal specifications and there are limited persistent connections.

Active-Active vs. Active-Passive Load-Balancer Setup: The load balancer is configured with an Active-Active setup, where both nodes (servers) actively run the same service concurrently. In contrast, an Active-Passive setup involves only some nodes being active. For example, if one node is active, the other remains passive. The key distinction lies in performance: Active-Active allows continuous resource utilization, while Active-Passive mainly relies on the backup server during failover.

Database Primary-Replica (Master-Slave) Cluster Operation: Master-slave replication involves the master database server sending data updates to one or more slave database servers. Changes made on the master replicate across the slaves. Replication can be synchronous (immediate) or asynchronous (queued). This setup aids scalability by distributing read access across multiple servers. It can also serve other purposes like failover or data analysis without overloading the master.

Primary Node vs. Replica Node in Application Context: In terms of the application, the replica node is an identical copy of the primary node. Replica nodes ensure redundancy of the application codebase, safeguarding against hardware failures, and bolstering capacity for serving read requests.

Issues

A. Single Point of Failure (SPOF): The main vulnerability in this setup involves having just one load balancer, which, if it fails, could disrupt the entire system's functioning.

B. Security Concerns (Lack of Firewall, No HTTPS): Notable security issues include the application's reliance on the insecure HTTP protocol, enabling attackers to view sensitive information. The absence of a firewall exposes the system to denial of service (DoS or DDoS) attacks and potential data breaches through unidentified open ports.

C. Lack of Monitoring: The absence of monitoring prevents the identification and prompt resolution of problems, downtime, or security threats. Monitoring enhances productivity, reduces IT support costs, and ultimately improves the user experience.