Web Infrastructure Design

Task 1: Definitions and Explanations

1. Why add additional elements? Adding a new server allows us to implement a load balancer to manage high incoming traffic and eliminate the risk of a single point of failure inherent in using just one server.

2. What distribution algorithm does your load balancer use and how does it work? Our load balancer employs the Round Robin algorithm, distributing requests sequentially among servers unless one is unavailable. This ensures even distribution of workload.

3. Is your load balancer set up as Active-Active or Active-Passive, and what's the difference? Our load balancer is set up as Active-Active, where both servers actively provide the same service simultaneously. In contrast, an Active-Passive setup means not all servers are active at once. For example, in a two-node setup, if the first node is active, the second remains on standby. The key difference lies in performance, with Active-Active allowing access to all resources during normal operation.

4. How does a database Primary-Replica (Master-Slave) cluster operate? Master-slave replication involves the master database server replicating data to one or more slave servers. Updates made on the master propagate to the slaves. This replication can occur synchronously or asynchronously, commonly used to distribute read access for scalability and for failover purposes.

5. What distinguishes the Primary node from the Replica node in application terms? The Replica node mirrors the Primary node, providing redundant copies of the application codebase to enhance resilience against hardware failures and increase capacity for serving read requests, such as searches or document retrieval.

Issues:

A. Single Point of Failure (SPOF): The primary single point of failure in our infrastructure is having only one load balancer.

B. Security vulnerabilities : Security concerns the insecure HTTP protocol using, risking exposure of sensitive information to attackers. Additionally, without a firewall, the system is vulnerable to denial of service (DOS or DDOS) attacks or unauthorized access through open ports, leading to potential downtime and data breaches.

C. Lack of monitoring: Monitoring is crucial for identifying and addressing issues promptly, preventing downtime, security threats, and enhancing overall user experience. It allows for proactive maintenance and cost savings on IT support.