TASK 1

Definitions and Explanations.

1. **For every additional element, why you are adding it:** The incorporation of an additional server into the infrastructure serves a dual purpose. Firstly, it facilitates the integration of a load balancer, thereby enhancing the system's capacity to manage burgeoning incoming traffic. Secondly, it mitigates the risk of a single point of failure, a scenario wherein the failure of a singular component disrupts the entire system's functionality. By dispersing the workload across multiple servers, the infrastructure achieves enhanced fault tolerance and reliability.
2. **What distribution algorithm your load balancer is configured with and how it works:** Our load balancer operates on the Round Robin algorithm, a sophisticated mechanism designed to distribute incoming requests across multiple servers in a sequential manner. Under this algorithm, requests are systematically routed to servers in a cyclic fashion, ensuring equitable distribution of workload. This approach is particularly effective in scenarios where servers exhibit uniform specifications and where persistent connections are not overly prevalent.
3. **What distribution algorithm your load balancer is configured with and how it works:** The load balancer facilitates an Active-Active setup wherein all nodes (servers) actively participate in service provision concurrently. In contrast, an Active-Passive setup entails the deployment of standby nodes that remain inactive unless invoked during failover scenarios. The key distinction between these configurations lies in their operational dynamics. Active-active clusters afford uninterrupted access to all server resources during normal operations, whereas active-passive clusters leverage standby resources solely during failover events, thereby optimizing resource utilization.
4. **What distribution algorithm your load balancer is configured with and how it works:** The primary-replica (master-slave) replication mechanism facilitates the dissemination of data from a primary

database server (master) to one or more secondary servers (replicas). Through this process, updates initiated on the master server are systematically propagated to the replica servers, thereby ensuring data consistency across the cluster. Depending on the synchronization mode employed, replication may occur synchronously or asynchronously, catering to diverse scalability and failover requirements. This architecture not only enhances read scalability by distributing read access across multiple servers but also augments fault tolerance and data redundancy within the database ecosystem.

5. **What is the difference between the Primary node and the Replica node in regard to the application:** In the context of application architecture, a replica node functions as a mirrored replica of the primary node, housing redundant copies of the application codebase. This redundancy serves to bolster system resilience by safeguarding against hardware failures and augmenting the system's capacity to cater to read-intensive operations, such as document retrieval or search queries.

Issues with the Infrastructure.

1. **SPOF:** The central vulnerability in the existing infrastructure lies in the sole reliance on a single load balancer. By introducing redundancy measures or deploying additional load balancers, the infrastructure can mitigate the risk of downtime and service disruptions associated with load balancer failures.B
2. **Security issues (no firewall, no HTTPS):** A glaring security lapse stems from the absence of essential security measures such as firewalls and HTTPS encryption. This exposes the application to a plethora of potential threats, including interception attacks and denial -of-service (DoS) assaults. By implementing robust firewall configurations and HTTPS encryption protocols, the infrastructure can fortify its defenses against malicious intrusions and data breaches.
3. **No monitoring:** In alignment with the adage "You cannot fix or improve what you cannot measure," the absence of comprehensive

monitoring poses a significant operational risk. By instituting robust monitoring protocols encompassing server, website, and application performance, stakeholders can proactively identify and mitigate potential issues before they escalate into critical failures. This not only enhances operational efficiency and cost-effectiveness but also fosters a superior user experience by averting service disruptions and downtime incidents.