Task 1 - distributed_web_infrastructure

Definitions and Explanations

1.For every additional element, why you are adding it?

We added two new servers to eliminate a single point of failure and we added a load-balancer to handle too much incoming traffic.

2.What distribution algorithm your load balancer is configured with and how it works?

Load balancer that uses the Round Robin algorithm distributes incoming network traffic across multiple servers in a circular, sequential fashion. Each server is selected in turn to handle a new connection or request.

3.Is your load-balancer enabling an Active-Active or Active-Passive setup, explain the difference between both?

The load-balancer have Active-Active setup where all nodes actively handle incoming requests simultaneously while in Active-Passive one node is active, but the others remain in passive. If the active node fails, one of the passive nodes takes over to maintain service.

4.How a database Primary-Replica (Master-Slave) cluster works?

In a Primary-Replica (Master-Slave) database cluster, one node serves as the primary (master), handling both read and write operations. The other nodes are replicas (slaves), replicating data from the primary. Replicas primarily handle read operations and serve as backups in case the primary node fails.

5.What is the difference between the Primary node and the Replica node regarding the application?

A replica node is a copy of the primary node, they provide copies of the application codebase to protect against hardware failure and increase the capacity of serving read requests like searching or retrieving document.

Issues

1.Where are SPOF ?

There is one SPOF because we have only one load balancer.

2.Security issues (no firewall, no HTTPS)?

Using only HTTP can allow an attacker to view sensitive information like passwords, and having no firewall can allow an attacker to perform a denial service attack that may cause a major downtime in the system. Firewalls enforce access control policies, helping to ensure that only legitimate traffic is allowed and HTTPS encrypts the data, providing a secure channel for communication.

3.No monitoring

Since we do not use any monitoring component in the current architecture, we won't be able to identify problems, downtime or security threats.