ALX Web Infrastructure Tasks:

task1:

1. **Additional Elements and Their Purpose**: Each additional element, such as load balancers, additional web servers, and database replicas, is added to improve the reliability, scalability, and performance of the infrastructure. Load balancers distribute incoming traffic across multiple servers, additional web servers handle increased demand, and database replicas improve data availability and resilience.
2. **Load Balancer Distribution Algorithm**: The load balancer is configured with a round-robin distribution algorithm. This algorithm evenly distributes incoming requests across the available servers in a sequential order, ensuring a balanced workload distribution.
3. **Active-Active vs. Active-Passive Setup**: The load balancer enables an Active-Active setup. In an Active-Active setup, all servers actively handle incoming requests simultaneously, providing redundancy and load distribution. In contrast, an Active-Passive setup involves one server (active) handling traffic while the other(s) remain idle (passive) until failover is needed.
4. **Database Primary-Replica Cluster**: In a Primary-Replica (Master-Slave) cluster, the primary node (master) handles write operations and replicates data changes to replica nodes (slaves). Replica nodes serve read requests and provide redundancy in case the primary node fails.
5. **Difference Between Primary and Replica Nodes**: The primary node is responsible for handling write operations, ensuring data consistency and integrity. The replica nodes primarily serve read requests, offloading the read workload from the primary node and providing scalability and fault tolerance. In regard to the application, the primary node affects write performance and data consistency, while replica nodes impact read performance and data availability.

Issues with the infrastructure:

1. **SPOF**: Single points of failure exist in the infrastructure, such as the load balancer or the primary database node. If any of these components fail, it could lead to service disruption or downtime.
2. **Security Issues**: Lack of firewall protection exposes the infrastructure to various security threats, including unauthorized access, data breaches, and malicious attacks. Additionally, the absence of HTTPS encryption poses a risk of data interception and compromise during transmission over the network.
3. **No Monitoring**: Without proper monitoring tools and procedures in place, it's challenging to detect and respond to performance issues, security breaches, or infrastructure failures promptly. Lack of monitoring increases the risk of prolonged downtime, data loss, and compromised

References

1st Reference

2nd Reference

3rd Reference