Compound & Term explanations:

Addition of Elements: The addition of elements to an infrastructure usually serves specific purposes like scalability, redundancy, or performance enhancement. For instance, additional servers or instances are added for load balancing to evenly distribute incoming traffic.

Load Balancer Distribution Algorithm: The distribution algorithm can be Round Robin, Least Connections, or IP Hashing. Round Robin distributes requests sequentially, Least Connections directs requests to the server with the fewest active connections, and IP Hashing uses the client's IP address to determine which server receives the request.

Active-Active vs. Active-Passive Load-Balancer Setup: Active-Active setup means both load balancers are actively distributing traffic at the same time. Active-Passive setup involves one load balancer actively managing traffic while the other remains on standby, only becoming active when the primary load balancer fails.

Database Primary-Replica (Master-Slave) Cluster: In this setup, the Primary node handles all write operations and replicates data to the Replica nodes, which serve read operations. It ensures data redundancy and fault tolerance.

Difference between Primary and Replica nodes: The Primary node accepts write operations and is responsible for the most recent data. Replica nodes replicate data from the Primary and serve read operations, ensuring scalability and redundancy but might lag slightly behind the Primary in terms of data updates.

Issue explanations:

Single Point of Failure (SPOF):SPOFs are areas within the infrastructure where if a failure occurs, the entire system goes down. It could be the absence of redundancy in critical components like a single database server or load balancer.

Security Issues: Lack of firewall protection leaves the infrastructure vulnerable to unauthorized access or attacks. Additionally, the absence of HTTPS encryption exposes data transmitted between the server and clients to potential interception.(Cache poisoning, MITM..etc)

No Monitoring: Without monitoring, there's no proactive way to identify issues, performance bottlenecks, or potential security breaches. It increases the risk of system downtime or data compromise going unnoticed until a significant problem occurs.