DISASTER RECOVERY WITH IMB CLOUD VIRTUAL SERVERS

PHASE-1

Problem Definition:

A disaster recovery plan defines instructions that standardize how a particular organization responds to disruptive events, such as cyber attacks, natural disasters, and power outages. A disruptive event may result in loss of brand authority, loss of customer trust, or financial loss.

Design Thinking:

- Implementation of a multi-region approach by deploying IBM Cloud Virtual Servers in geographically diverse regions or availability zones. This ensures redundancy and minimizes the risk of a single point of failure.
- Designing an automated failover strategy that can swiftly redirect traffic from the primary site to the secondary site (IBM Cloud Virtual Servers) in case of a disaster.
- Implementation of robust security measures, including data encryption in transit and at rest, access controls, and comprehensive logging.
- Utilizing IBM Cloud monitoring tools to continuously monitor the health and performance of IBM Cloud Virtual Servers and associated services. Configure alerting systems to notify IT personnel promptly of any anomalies or issues.
- Establishing a regular testing schedule for disaster recovery drills. These tests should simulate real-world disaster scenarios and involve failover procedures.
- Considering the integrating third-party disaster recovery and monitoring tools if they align with the needs of your organization. These tools can enhance visibility, automation, and reporting capabilities.