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.
- Explore high availability architectures like active-active or active-passive configurations to further minimize downtime.
- Establishing a regular testing schedule for disaster recovery drills. Collect user feedback to identify areas for improvement and iterate on the design to enhance the user experience.
- Integrate DevOps practices to automate provisioning, configuration, and deployment of virtual servers, enhancing agility and reducing manual errors.