PROJECT TITLE:Disaster recovery with IBM cloud virtual servers.

Problem Statement:

In this part you will need to understand the problem statement and create a document on what have you understood and how will you proceed ahead with solving the problem. Please think on a design and present in form of a document.

Project steps;

Phase 1: Problem Definition and Design Thinking

Problem Definition: The project involves creating a disaster recovery plan using IBM Cloud Virtual Servers. The objective is to safeguard business operations by developing a plan that ensures continuity for an on-premises virtual machine in unforeseen events. This plan will include setting up backup strategies, configuring replication, testing the recovery process, and guaranteeing minimal downtime. The project encompasses defining the disaster recovery strategy, implementing backup and replication, validating recovery procedures, and ensuring business continuity.

Design Thinking:

Disaster Recovery Strategy: Define the disaster recovery strategy and objectives, including recovery time objectives (RTO) and recovery point objectives (RPO).

Backup Configuration: Configure regular backups of the on-premises virtual machine to capture critical data and configurations.

Replication Setup: Implement replication of data and virtual machine images to IBM Cloud Virtual Servers to ensure up-to-date copies.

Phase2:consider incorporating automated Recovery scripts or proactive monitoring for quicker response During disasters

Disaster recovery strategies available to you within AWS can be broadly categorized into four Approaches, ranging from the low cost and low complexity of making backups to more complex Strategies using multiple active Regions. Active/passive strategies use an active site (such as an AWS Region) to host the workload and serve traffic. The passive site (such as a different AWS Region) is used For recovery. The passive site does not actively serve traffic until a failover event is triggered It is critical to regularly assess and test your disaster recovery strategy so that you have confidence in Invoking it, should it become necessary. Use AWS Resilience Hub to continuously validate and track the Resilience of your AWS workloads, including whether you are likely to meet your RTO and RPO targets.

AWS services

Your workload data will require a backup strategy that runs periodically or is continuous. How often you Run your backup will determine your achievable recovery point (which should align to meet your RPO).

The backup should also offer a way to restore it to the point in time in which it was taken.

Backup and restore

Backup and restore is a suitable approach for mitigating against data loss or corruption. This approach Can also be used to mitigate against a regional disaster by replicating data to other AWS Regions, or to Mitigate lack of redundancy for workloads deployed to a single Availability Zone. In addition to data, you Must redeploy the infrastructure, configuration, and application code in the recovery Region.

Phase 3: Development Part 1

IBM Cloud Disaster Recovery

Creating a disaster recovery plan using IBM Cloud Virtual Servers involves several key steps. Here's an Overview of the process:

Assessment and Planning:

Identify critical virtual machines (VMs) and their specific roles in your infrastructure.

Determine your Recovery Time Objective (RTO), i.e., how quickly you need to recover after a disaster.

Define your Recovery Point Objective (RPO), which establishes how much data loss is acceptable.

Prioritize VMs based on their importance to your business operations.

Selecting IBM Cloud Services:

Choose appropriate IBM Cloud Virtual Server configurations to host your VMs.

Consider IBM Cloud services like Block Storage, Object Storage, and Load Balancers for redundancy and

Data integrity.

Setting up Regular Backups:

Use IBM Cloud's backup and snapshot features for regular backups.

Configure backup schedules and retention policies based on your RPO requirements.

Testing and Validation:

Regularly test your disaster recovery plan to ensure it meets your RTO and RPO goals.

Conduct failover and failback tests to confirm the effectiveness of your strategy.

For example, the following are all data plane responsibilities:

*Running and hosting the Virtual Server Instance (VSI)

*Reading and writing to block storage volumes

*Getting and setting objects into Cloud Object Storage Buckets

*Running, processing queries and updates to IBM Cloud Databases PostegreSQL database.

Limit of what they can spend on their data recovery strategy. Of the four DR strategies, either Pilot Lighty Options include any which would enable resumption of a business process in a time frame at or near the RPO/RTO.

PHASE 4: Development Part 2

Continue building the disaster recovery plan by configuration replication and testing recovery

Procedures.

1)Set Up Data Replication:

*Identify critical data and systems to replicate.

*Replication mechanisms such as AWS S3 Cross-Region Replication.

2)Create Automated Backups:

*Use automated backup services like AWS RDS automated backups for databases.

3) Implement Disaster Recovery Testing:

*Create scripts or automation for testing recovery procedures.

4) Regularly Test Failover:

*Schedule regular tests of failover to ensure the process works.

The code for execution is given:

https://github.com/Smiruti/Naan-mudhalvan/blob/main/CAD_Phase4.pdf

The readme file gives a detailed information about the disaster recovery with IBM cloud virtual servers.

https://github.com/Smiruti/Naan-mudhalvan/blob/76898711361837598b01ad8bbf10b471c6b65fe/README.md