**CAD PHASE 3**

**DISASTER RECOVERY WITH IBM CLOUD**

**VIRTUAL SERVERS**

**INTRODUCTION**

After completing our major ideas and plans on phase 2 , here we are at phase 3 , elaborating our project with detailed explanation and building , through an completely evaluated documentation of the given phase

Developing a disaster recovery (DR) plan for a project using IBM Cloud virtual servers involves several key steps to ensure the continuity of your business operations in the event of a disaster or service interruption. Here's a step by step guide to create a robust disaster recovery plan for IBM Cloud virtual server environment

1. Assessment and Requirements Gathering

2. Backup and Replication

3. Failover Planning

4. Network and Connectivity

5. Testing and Validation

6. Monitoring and Alerting

7. Documentation and Communication

Let's dive deeper into the steps and considerations for developing a disaster recovery (DR) plan using IBM Cloud virtual servers:

**1. Assessment and Requirements Gathering**

First ,identify Critical Assets . List all critical applications, data, and virtual servers in your environment. Determine your Recovery Time Objectives and Recovery Point Objectives (RPO) for each asset. RTO specifies how quickly an asset must be recovered, while RPO sets the acceptable data loss threshold.

**2. Backup and Replication**

In this subphase , we need to configure automated, regular backups of your virtual server instances and data using IBM Cloud services like IBM Cloud Object Storage and I Implement data replication to another geographic region using IBM Cloud's Cross Region Resiliency or similar services. This provides redundancy in case of a regional disaster.

**3. Failover Planning**

For a failover plan , we are going to choose one or more failover locations within IBM Cloud's infrastructure or in a different geographic region. Firstly ,determine which assets will be moved to these locations. Then , document step by step procedures for initiating failover, including DNS updates, provisioning new virtual servers, and data restoration.

**4. Network and Connectivity**

Network and connectivity is an important role in this phase. Establish a secure and reliable network connection between your primary and failover data centers using VPN, Direct Link, or similar technologies. Also ,test network configurations to ensure that applications and services will function seamlessly during a failover event.

**5. Testing and Validation**

After setting up proper network and connectivity , conduct regular disaster recovery drills to test the effectiveness of your plan. This helps identify any weaknesses or areas for improvement. Keep detailed records of test results, and update your DR plan based on lessons learned during these drills.

**6. Monitoring and Alerting**

To monitor our process , we need to set up monitoring tools to continuously track the health and performance of your virtual servers, applications, and data. Configure alerting mechanisms with defined thresholds and notification processes to respond quickly to issues or anomalies.

**7. Documentation and Communication**

Create a comprehensive DR plan document that includes all procedures, contact information, and recovery strategies. Define communication channels and procedures for notifying stakeholders, team members, and third party providers during a disaster.

By continually reviewing, testing, and updating our DR plan, we can maintain a high level of resilience and preparedness for unexpected disruptions, ensuring the continuity of our business operations. IBM Cloud offers various services and resources to assist in implementing a robust disaster recovery strategy.

Let's break down the project into more detail starting from setting up the IBM Cloud account and provisioning virtual servers:



**Setting Up an IBM Cloud Account :**

1. Go to the IBM Cloud website (https://cloud.ibm.com/).

2. Sign up for an IBM Cloud account by clicking on "Sign Up" or "Create an IBM Cloud account."

3. Follow the on-screen instructions to complete the registration process.

4. Verify your email and log in to your IBM Cloud account.

**Provisioning Virtual Servers:**

1. Log in to your IBM Cloud account.

2. Click on the "Create Resource" button.

3. Under "Compute," select "Virtual Server."

4. Follow the steps to create a virtual server. You can choose a basic configuration to keep it simple for this project.

- Choose your preferred data center location for the primary server.

- Select a minimal configuration, such as a small virtual server.

- Set the SSH key for secure access to the server.

- Assign a hostname and domain name (you can use fictitious names).

- Review your selections and click "Create."

Repeat the same process to create a second virtual server that will serve as your backup.

**Data Backup:**

For this basic project, you can perform a simple data backup by setting up a data copy from your primary server to the backup server. You can use SSH and `rsync` for this purpose:

1. On your primary server, install `rsync` if it's not already installed.



```

sudo apt-get install rsync

```

2. Create a script on your primary server to periodically copy your application data to the backup server using `rsync`. You can schedule this script to run at regular intervals. Create a script file (e.g., `backup.sh`) and add the following content:



```bash

rsync -avz /path/to/your/application/data/ user@backup-server-ip:/backup/location/

```

3. Set up passwordless SSH login from the primary server to the backup server to allow the script to run without manual intervention. Here's a high-level overview (make sure to replace `user` and `backup-server-ip` with your actual values): Generate an SSH key pair on the primary server if you haven't already:

```

ssh-keygen

```

Copy the public key to the backup server:

```

ssh-copy-id user@backup-server-ip

```

Test SSH to ensure passwordless login is working:

```

ssh user@backup-server-ip

```

4. Schedule the backup script to run periodically (e.g., using `cron`). For example, you can schedule it to run every night:



```

crontab -

Add the following line to the crontab (adjust the schedule as needed):

```

0 0 \* \* \* /path/to/backup.sh

```

This basic setup will periodically copy your application data from the primary server to the backup server. In the event of a failure, you can access your data on the backup server.

**So , what is an application here ??**

In the context of the project we're discussing, an "application" refers to the software or program that is hosted on your virtual server within IBM Cloud. It's the software that provides specific functionality, whether it's a website, web service, database, or any other type of program.

**Here are a few examples to illustrate what an "application" could be:**

**1. Website:** Your application could be a simple website that provides information about a topic, a blog, or an e-commerce site.

**2. Web Service:** It could be a RESTful API or a web service that provides functionality to other software applications.

**3. Database:** The application could be a database server that stores and manages data, such as customer records, product information, or financial transactions.

**4. Content Management System (CMS):** It might be a CMS like WordPress that powers a blog or content-driven website.

**5. Custom Software:** The application could be custom software that you or your team have developed for a specific purpose, such as inventory management, order processing, or customer relationship management.

In the context of this project, the application is what we're protecting with our disaster recovery plan. The goal is to ensure that the application's data and services remain available even in the event of server failures or other disruptions.