# Description:

Recovery from the IBM Cloud servers in the design, general steps and process also including the fail over recovers, defining the recover for cloud computing.

Here's a recovery disaster with IBM cloud server

# Disaster recovery with IBM cloud server

Disaster recovery with IBM Cloud servers typically involves setting up a plan to ensure that your data and applications are protected and can be quickly restored in case of a disaster. Here are the general steps to implement disaster recovery on IBM Cloud servers:

1. A**ssessment:**

Start by assessing your business's critical applications and data. Identify what needs to be protected and prioritize them based on their importance to your operations.

2. Backup and Replication:

Utilize IBM Cloud's backup and replication services to regularly back up your data and server configurations. You can use tools like IBM Cloud Backup or third-party solutions for this purpose.

3. Failover Planning:

Plan for how you will handle failovers in case of a disaster. IBM Cloud offers features like Virtual Server Recovery, which can automate failovers to a secondary location.

4. Secondary Data Center:

Set up a secondary data center or location in a different geographic region. This is essential for redundancy. IBM Cloud offers multiple data centers in various regions.

5. Network Configuration:

Ensure that network configurations are in place to redirect traffic to the secondary location when a failover occurs. This might involve using a global load balancer or DNS management.

6.Testing:

Regularly test your disaster recovery plan to ensure it works as expected. Simulate different disaster scenarios to validate your recovery procedures.

6. Monitoring and Alerts:

Implement monitoring and alerting systems to be notified of any issues with your primary server environment. IBM Cloud provides monitoring tools for this purpose.

7. Documentation:

Document your disaster recovery plan comprehensively, including step-by-step procedures, contact information, and recovery time objectives (RTOs).

8. Security:

Ensure that your disaster recovery environment is as secure as your primary environment. This includes access controls, encryption, and compliance with security best practices.

9. Staff Training:

Train your IT staff on the disaster recovery plan, and make sure they are familiar with the procedures to follow during a disaster.

10. Regular Updates:

Continuously update and refine your disaster recovery plan to adapt to changes in your infrastructure, applications, and business needs.

11. Compliance:

Ensure that your disaster recovery plan complies with any regulatory or industry-specific requirements that apply to your business.

- IBM Cloud provides various services and tools to assist with disaster recovery, including virtual servers, storage options, and networking capabilities. You can tailor your disaster recovery strategy to your specific needs and budget using these resources.

- Remember that disaster recovery is a critical aspect of business continuity, and it's essential to invest the necessary time and resources to implement a robust plan that can minimize downtime and data loss during unexpected events.

K. Sandhiya sree

NANDHA COLLEGE OF TECHNOLOGY

27.09.2023