V . Theivamani,

au620321106070

III[rd] Year ECE,

College Code:6203,

Bharathiyar institution of engineering for women, thalaivasal

Title: **DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS**

DEFINITION:

In today's digitally-driven world, businesses rely heavily on their IT infrastructure to deliver services, store critical data, and maintain operations. However, unforeseen disasters, whether natural or technological, can disrupt these essential functions, leading to financial losses and reputational damage. To mitigate these risks, organizations are increasingly turning to cloud-based solutions, such as IBM Cloud Virtual Servers, to build robust disaster recovery (DR) strategies.

SOLUTION:

1. *Assessment and Planning:*

- Identify critical applications and data that require DR protection.

- Determine your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each application.

- Choose the appropriate IBM Cloud Virtual Server offerings based on your workload requirements.

2. *Geographic Redundancy:*

- Deploy your primary workload in one IBM Cloud data center or region.

- Establish a secondary site in a geographically separate IBM Cloud data center or region to ensure redundancy.

3. *Data Replication:*

- Implement data replication mechanisms, such as block-level storage replication or database replication, to keep data synchronized between the primary and secondary sites.

- Utilize IBM Cloud services like IBM Cloud Object Storage for backup and long-term data retention.

- Implement an automated failover mechanism that can detect failures in the primary site and initiate failover to the secondary site.

- Use load balancers and DNS-based traffic management to reroute traffic to the secondary site during failover.

5. *Testing and Validation:*

- Regularly test your DR solution to ensure it meets the defined RTO and RPO objectives.

- Conduct both planned and unplanned failover tests to validate the system's resilience.

6. *Monitoring and Alerting:*

- Implement robust monitoring and alerting systems to detect issues in real-time.

- Use IBM Cloud monitoring services and third-party tools to track the health of your infrastructure.

7. *Backup and Snapshot Strategy:*

- Implement a backup and snapshot strategy for your virtual servers to facilitate data recovery and rollbacks if necessary.

8. *Security and Access Control:*

- Ensure that security policies and access controls are consistent between the primary and secondary sites.

- Use IBM Cloud Identity and Access Management (IAM) to manage user access.

9. *Documentation and Runbooks:*

- Create comprehensive runbooks that outline the steps to follow during a DR event.

- Maintain up-to-date documentation of your DR solution's architecture and configuration.

10. *Cost Management:*

- Understand the cost implications of maintaining a DR solution and optimize resources to minimize costs when not in use.

11. *Compliance and Regulations:*

- Ensure your DR solution complies with industry-specific regulations and data protection requirements.

12. *Third-Party Integration:*

- Consider integrating third-party DR solutions and tools that can enhance the automation and efficiency of your DR processes.

13. *Continuous Improvement:*

- Regularly review and update your DR plan based on changing business needs, technology advancements, and lessons learned from testing and real-world events.