## Project - Disaster Recovery with IBM Cloud Virtual Servers

**TEAM MEMBERS**

**210621205001– Abhishekaraj**

**210621205009-Aswin Raj**

**210621205022-Jai Sabari Ganesh**

**210621205031-Maju mon**

**210621205035-Niranchan**

**Phase-1 Document Submission**

# Problem Definition

**Scope:** The scope of disaster recovery with IBM Cloud Virtual Servers includes planning, implementing, and maintaining strategies to ensure the continuity of critical systems and data in the event of disruptions or disasters. This encompasses defining recovery objectives, selecting appropriate technologies, establishing testing procedures, and maintaining compliance with regulations to safeguard business operations and data integrity.

**Objectives:**

**1.Minimize Downtime:** Ensure rapid failover and recovery of virtual servers to minimize downtime, meeting specific Recovery Time Objectives (RTOs) for critical systems.

**2.Data Integrity:** Maintain data integrity by implementing reliable data replication and backup mechanisms, meeting Recovery Point Objectives (RPOs) for data loss tolerance.

**3.Cost-Efficiency:** Optimize resource allocation and costs by balancing performance requirements with budget constraints in the disaster recovery strategy.

**4.Compliance and Security:** Ensure compliance with industry regulations and data protection standards while maintaining the security of data during disaster recovery processes.

**5.Regular Testing and Validation:** Establish a routine testing schedule to validate the effectiveness of the disaster recovery plan and maintain readiness for potential disasters.

**Challenges**:

**1.Complexity of Configurations:** Managing and configuring virtual server replication, networking, and failover processes can be complex, requiring skilled IT personnel.

**2.Data Transfer Speed:** Transferring large volumes of data between on-premises environments and IBM Cloud Virtual Servers can be time-consuming, impacting RTO objectives.

**3.Cost Management:** Balancing the costs of maintaining standby resources in the cloud for disaster recovery against the potential downtime costs can be challenging.

**4.Data Consistency:** Ensuring data consistency and synchronization between primary and secondary virtual servers can be a significant challenge, particularly in real-time replication scenarios.

**5.Security and Compliance:** Maintaining robust security measures and compliance standards during data replication and recovery processes can be complex, especially for regulated industries.

**Success Criteria**:

**1.Achieving RPO and RTO Targets:** Meeting or exceeding the defined Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) for critical virtual servers and applications.

**2.Minimal Downtime:** Ensuring minimal downtime during disaster recovery events, allowing for near-seamless failover and recovery of services.

**3.Data Integrity:** Maintaining data integrity and consistency across primary and secondary virtual servers, with minimal data loss or corruption.

**4 Regular Testing:** Conducting routine testing and validation exercises to ensure the disaster recovery plan works as expected.

**5.Cost-Efficiency**: Managing disaster recovery costs within budgetary constraints while still providing effective recovery solutions.

# Design Thinking

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

**1. Define Recovery Time Objectives (RTO):**

* RTO is the maximum allowable downtime for your systems or services after a disaster occurs. It represents the time it takes to recover and restore functionality. To define RTO:
* Identify critical systems and applications.
* Consult with stakeholders to determine the acceptable downtime for each system or application.
* Set specific RTO values for each, such as "less than 1 hour" or "within 4 hours."
* Ensure that RTO values align with the business's operational needs and financial constraints.

**2. Define Recovery Point Objectives (RPO):**

* RPO represents the maximum amount of data loss that can be tolerated during a disaster event. It defines how often data should be backed up or replicated to ensure minimal data loss. To define RPO:
* Identify critical data and databases.
* Determine how frequently data changes and the importance of up-to-date information.
* Set specific RPO values, such as “15 minutes” or “daily.”
* Ensure that RPO values are in line with data recovery needs and the impact of data loss on operation.

**3. Align Strategy with RTO and RPO:**

• Once RTO and RPO objectives are defined, design a disaster recovery strategy that aligns with these objectives.

•Select appropriate technologies and solutions, such as data replication, backups, virtual server failover, and cloud resources, to meet RTO and RPO goals.

•Ensure that the strategy accounts for the prioritization of systems and data based on their criticality.

**4. Document the Strategy:**

•Create a comprehensive disaster recovery plan that outlines the chosen strategy, roles and responsibilities, contact information, and step-by-step procedures.

•Document the specific measures to be taken to achieve the defined RTO and RPO objectives.

**5. Regularly Review and Update:**

Disaster recovery strategies should be reviewed and updated regularly to reflect changes in the IT environment, business needs, and technological advancements.

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

To configure regular backups of on-premises virtual machines to capture critical data and configurations, you can follow these steps:

1. **Select Backup Solution:**
   1. Choose a backup solution that fits your needs. Options include cloud-based backup services, on-premises backup appliances, or a combination of both.
2. **Identify Critical Data and Configurations:**
   1. Determine what data and configurations are critical and need to be backed up. This may include databases, application configurations, and user data.
3. **Backup Schedule:**
   1. Establish a regular backup schedule based on the frequency of data changes and the importance of up-to-date backups. Common schedules include daily, hourly, or real-time backups.
4. **Backup Storage Location:**
   1. Decide where the backups will be stored. Options include on-premises storage devices, remote servers, or cloud storage solutions like AWS S3, Azure Blob Storage, or IBM Cloud Object Storage.
5. **Backup Retention Policy:**
   1. Define a backup retention policy that specifies how long backups should be retained. Consider compliance requirements and the need for historical data.
6. **Backup Methods:**
   1. Choose the appropriate backup methods:
      * Full Backups: Capture the entire virtual machine image.
      * Incremental Backups: Capture only changes made since the last backup.
      * Differential Backups: Capture changes made since the last full backup.
7. **Automation and Scripts:**
   1. Use automation scripts or backup software to streamline the backup process. This ensures consistency and reduces the risk of human error.
8. **Testing Backups:**
   1. Regularly test backups to verify their integrity and the ability to restore data and configurations successfully.
9. **Encryption and Security:**
   1. Implement encryption for data in transit and at rest to maintain data security and compliance.
10. **Monitoring and Alerts:**
    1. Set up monitoring and alerts to be notified of backup failures or issues promptly.
11. **Documentation:**
    1. Document the backup configuration, including schedules, retention policies, and recovery procedures. Make sure relevant staff members are aware of the documentation.
12. **Regularly Review and Update:**
    1. Periodically review and update the backup configuration to adapt to changing business needs and technology advancements

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

**1.Choose Replication Solution:**

Select a replication solution that meets your needs. IBM Cloud provides services like IBM Cloud Object Storage and IBM Cloud Virtual Servers for replication purposes.

**2. Prepare Source Environment:**

- Ensure that your source virtual machines and data are ready for replication.

- Install and configure any necessary software on the source VMs, such as backup agents or replication agents.

**3. Set Up Target Environment:**

- Create and configure IBM Cloud Virtual Servers to serve as the target environment for replication.

- Ensure you have sufficient storage and compute resources on the target servers.

**4. Select Replication Method:**

- Decide on the replication method based on your requirements. Common methods include:

Snapshot-based replication: Taking periodic snapshots of virtual machines and copying them to the target servers.

Continuous data replication: Replicating changes in real-time from source to target using technologies like block-level replication.

**5. Configure Replication:**

- Set up replication policies and rules to define which data and VMs should be replicated and how often.

- Configure bandwidth throttling and network settings to optimize replication traffic.

**6. Monitor and Test:**

- Implement monitoring tools to keep an eye on the replication process and ensure it’s working as expected.

- Regularly test the failover process to ensure that you can quickly switch to the replicated environment in case of a disaster.

**7. Security and Access Control:**

- Implement security measures such as encryption for data in transit and at rest.

- Manage access controls to restrict who can access and manage the replication setup.

**8. Documentation and Training:**

- Document the entire replication setup, including configurations, policies, and procedures.

- Train your team on how to use and maintain the replication solution.

**9. Failover and Disaster Recovery Plan:**

- Develop a clear disaster recovery plan that outlines the steps to follow in case of a failure in the source environment.

- Ensure that you can seamlessly failover to the replicated environment when needed.

**10. Regular Testing and Maintenance:**

- Regularly test your disaster recovery plan to confirm its effectiveness.

- Keep your replication solution and target environment up to date with security patches and software updates.

**Recovery Testing: Design and conduct recovery tests to validate the recovery process and guarantee minimal downtime.**

**Identify Critical Systems and Data:** Determine which systems and data are critical to your organization’s operations. These are the ones that need to be tested for recovery.

**Define Recovery Objectives:** Clearly outline what you aim to achieve with the recovery tests. Specify recovery time objectives (RTOs) and recovery point objectives (RPOs) for each system or data set.

1. **Select Recovery Scenarios:** Design different recovery scenarios based on potential failure points. This might include hardware failures, software glitches, data corruption, or even natural disasters.
2. **Create Test Plans:** Develop detailed test plans for each recovery scenario. Define the steps to be taken during the test, the expected outcomes, and the success criteria.
3. **Set up Test Environments:** Create isolated test environments that mimic your production systems as closely as possible. This ensures that the recovery tests are realistic.
4. **Execute Recovery Tests:** Conduct the recovery tests according to the predefined scenarios and test plans. Document the results, including the time taken to recover and whether the objectives were met.
5. **Analyze Results:** Analyze the test results to identify any weaknesses or areas for improvement in your recovery process. This might involve adjusting configurations, improving documentation, or enhancing staff training.
6. **Iterate and Improve:** Based on the findings, make necessary improvements to your recovery process, infrastructure, or procedures. Then, repeat the recovery tests periodically to ensure ongoing effectiveness.
7. **Document Everything:** Maintain detailed records of all recovery tests, including the scenarios, results, and any changes made. This documentation is crucial for compliance and auditing purposes.
8. **Train Staff:** Ensure that your staff is well-trained in the recovery procedures and can execute them effectively during real incidents.
9. **Automate Where Possible:** Consider automating parts of the recovery process to minimize human error and reduce recovery times.
10. **Regularly Review and Update:** As your systems and infrastructure evolve, regularly review and update your recovery testing procedures to stay aligned with your organization’s needs and technological advancements.

**Business Continuity: Ensure that the disaster recovery plan aligns with the organization’s overall business continuity strategy.**

Aligning the disaster recovery plan with the organization’s overall business continuity strategy is crucial for seamless operations during disruptions. This entails ensuring that the recovery objectives, priorities, and resources are in sync with broader business continuity goals. Regular testing and updates are key to maintaining alignment and readiness.