**Project Title:** IBM Disaster Recovery

**Problem Statement :**

* Safeguard business op erations with IBM Cloud Virtual Servers. Create a disaster recovery plan for an on-premises virtual machine, ensuring continuity in unforeseen events.
* Test and validate the recovery process to guarantee minimal downtime. Become the guardian of business continuity, securing the future of your organization!

**Design Thinking Disaster Recovery**

**Disaster Recovery Strategy**

A disaster recovery strategy is a comprehensive plan that outlines how an organization will recover its critical systems, applications, and data in the event of a disaster or disruptive incident. Key components of this strategy include defining recovery time objectives (RTO) and recovery point objectives (RPO).

**1.Recovery Time Objective (RTO):**

* The Recovery Time Objective (RTO) is the maximum allowable downtime for a system or application following a disaster or disruption. It represents the target time within which the organization must restore the system to normal operation to minimize business impact. The RTO is determined based on business needs, criticality of the system, and the potential impact of downtime**.**

**2. Recovery Point Objective (RPO):**

* The Recovery Point Objective (RPO) represents the maximum allowable data loss that an organization can tolerate following a disaster. It defines the point in time to which data must be restored for a system or application. RPO is closely related to data replication and backup strategies and is typically measured in time, such as minutes, hours, or even days.

**Backup Configuration**

Creating a backup configuration for on-premises virtual machines to capture critical data and configurations in cloud computing involves setting up a systematic process to back up your data and virtual machine settings to a cloud-based storage solution.

**1. Choose a Cloud Backup Solution:**

* Select a cloud backup service or solution that suits your needs. Popular options include AWS Backup, Azure Backup, Google Cloud Storage, or third-party backup solutions that work with multiple cloud providers.

**2. Install Backup Agents (if required):**

* Some cloud backup solutions may require the installation of agents on your on-premises virtual machines. These agents facilitate data transfer to the cloud. Follow the installation instructions provided by your chosen backup solution.

**3. Configure Backup Policies:**

* Define backup policies that specify what data and configurations need to be backed up, how often backups should occur, and how long backups should be retained. Ensure that critical data, system files, and configurations are included in these policies.

**Replication Setup**

* Setting up data and virtual machine replication to IBM Cloud Virtual Servers involves creating a process that keeps your data and virtual machine images synchronized with the cloud-based virtual servers.

**1. Choose IBM Cloud Services:**

* Select the appropriate IBM Cloud services and resources for your replication needs. IBM Cloud offers various virtual server options, including virtual machines, containers, and more. Ensure you have the necessary resources provisioned in the IBM Cloud.

**2. Replication Technology:**

* Choose a replication technology or method based on your specific requirements. IBM Cloud provides various options, including IBM Cloud Block Storage, which supports volume replication.

**3. Configure Replication:**

* Configuring replication settings in your on-premises infrastructure or existing virtual machines.
* Defining replication schedules and frequency (e.g., real-time, hourly, daily) to ensure up-to-date copies.
* Specifying the target IBM Cloud Virtual Server where the replicated data or virtual machine images will be stored.

**Recovery Testing**

Recovery testing is a critical element of a disaster recovery strategy in cloud computing environments. Cloud-based disaster recovery offers many advantages, such as scalability, cost-effectiveness, and geographic diversity. However, it also comes with its own set of challenges and considerations. Here are some specific aspects of recovery testing for a disaster recovery strategy in a cloud computing environment.

**1.Data Backup and Recovery Testing:**

* Verify that data backups are regularly scheduled and complete successfully.
* Test the restoration process for various data types and volumes.

**2.Virtual Machine (VM) and Application Recovery Testing:**

* Test the recovery of virtual machines and applications in the cloud environment.
* Validate that the configurations and dependencies are correctly replicated during recovery.

**3.Network and Connectivity Testing:**

* Test network connectivity and routing to the cloud service provider during a disaster.
* Ensure that DNS updates or changes are properly propagated.

**4.Failover and Failback Testing:**

* Test the process of failing over from the primary environment to the cloud-based disaster recovery environment.
* Perform failback tests to return operations to the primary environment when it's safe to do so.

**5. Geographic Redundancy Testing:**

* + If you're using a multi-region cloud strategy, test the failover and recovery between different regions.
  + Ensure data consistency and minimal downtime when switching between regions.

**6.Security and Compliance Testing:**

* + Verify that security controls, encryption, and access management are maintained during recovery.
  + Ensure compliance with regulatory requirements throughout the recovery process.

**Business continuity**

Business continuity planning (BCP) is a comprehensive approach that encompasses disaster recovery and more, ensuring that a business can continue its essential functions during and after a disaster, including in a cloud computing environment. Here are key considerations for business continuity in a cloud-based disaster recovery strategy.

**1.Risk Assessment:**

* + Identify potential risks and threats to your business operations, including those specific to cloud computing, such as data breaches, cloud provider outages, and cyberattacks.

**2.Business Impact Analysis (BIA):**

* + Determine the criticality of different systems, applications, and data hosted in the cloud.
  + Assess the financial and operational impacts of disruptions to those critical resources.

**3. Data Backup and Recovery:**

* + Implement robust data backup and recovery procedures in the cloud.
  + Ensure data is regularly backed up and can be quickly restored to meet recovery time objectives (RTOs) and recovery point objectives (RPOs).

**4.Redundancy and High Availability:**

* + Design cloud architectures with redundancy and failover capabilities to minimize downtime.
  + Leverage cloud services like load balancing, auto-scaling, and region failover for high availability.

**5.Security and Compliance:**

* + Implement strong security controls, encryption, and access management in the cloud.
  + Ensure that your cloud setup complies with industry-specific regulations and standards.

**6. Incident Response Plan:**

* + Develop an incident response plan that outlines the steps to take in the event of a security breach or cloud outage.
  + Define roles and responsibilities for incident response team members.