**DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS**

**TEAM MEMBERS**

Vineeth E (771772114316)

Vairavel S(71772114148)

Mugunthan R(71772114305)

Soukanth V(71772114142)

**Problem statement:**

• Safeguard business operations 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

**Phase 2: Innovation**

**Assessment and Planning:**

* Identify Critical Systems and Data: Determine which virtual servers and data are critical to your business operations. This includes applications, databases, and other resources.
* Risk Assessment: Evaluate potential risks and threats that could lead to a disaster scenario. This could include natural disasters, hardware failures, cyberattacks, etc.
* RTO and RPO Definitions: Define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO is the maximum tolerable downtime, while RPO is the maximum amount of data loss that is acceptable.Budgeting and Resource Allocation: Determine the budget for the project and allocate resources accordingly. This includes hardware, software, and personnel.

**Selecting a DR Strategy**:

* Backup and Restore: This involves regularly backing up data and configurations from the production environment and restoring them in the event of a disaster.
* High Availability (HA): Implement technologies like clustering or load balancing to ensure continuous availability of services.
* Hot Site, Warm Site, Cold Site: Decide on the level of redundancy required. A hot site is fully operational, a warm site requires some setup, and a cold site is a location with power and networking but no equipment.
* Cloud-Based DR: Leverage cloud platforms like IBM Cloud for DR purposes, which offer scalability and flexibility.

**Design the DR Architecture**:

* Network Design: Set up the networking infrastructure to support the DR solution. This includes VPNs, VLANs, and routing configurations.
* Storage Configuration: Define how data will be stored, replicated, and accessed in the DR environment. This could involve technologies like RAID, SAN, or NAS.
* Server and Hypervisor Configuration: Set up virtual servers in the DR environment, ensuring they mirror the production environment in terms of configurations and applications.
* Security and Access Control: Implement security measures to protect the DR environment, including firewalls, access controls, and encryption.

**Implementation:**

* Provisioning Resources: Set up the necessary hardware and software components according to the design plan.
* Replication and Synchronization: Configure the mechanisms for replicating data and configurations from the production environment to the DR environment. This could be synchronous or asynchronous.
* Testing: Conduct thorough testing of the DR solution to ensure that it meets the defined RTO and RPO objectives. This includes failover tests, data consistency checks, and application functionality tests.

**Documentation and Training:**

* Document the DR Plan: Create detailed documentation outlining the DR procedures, including step-by-step instructions, contact information, and escalation paths.
* Training and Awareness: Train relevant personnel on the DR plan and procedures. Ensure that everyone understands their roles and responsibilities in the event of a disaster.

**Monitoring and Maintenance:**

* Continuous Monitoring: Implement monitoring tools to keep an eye on the health and performance of the DR environment. This includes monitoring for replication status, storage capacity, and server health.
* Regular Testing and Drills: Schedule periodic tests and drills to validate the effectiveness of the DR solution. This helps identify any potential issues and allows for adjustments.
* Update and Maintenance: Keep the DR solution up-to-date with the latest patches, configurations, and technologies.
* Periodic Review: Conduct regular reviews of the DR plan to ensure it remains aligned with the organization's needs and technologies.