Disaster Recovery with IBM Cloud Virtual Servers

Phase 4: Developnment

BEST PRACTICES TO CREATE AND IMPLEMENT A DISASTER RECOVERY PLAN
TOOLBOX
Have a Testing Schedule and Stick to It
Create Comprehensive Post-Test Reports
2
3
Maintain a Readily Accessible Disaster Recovery Playbook
1
DISASTER RECOVERY PLAN
4
Protect the Everyday Software

1. Configuring Replication:

a. Data Replication:

1.Assess Data: Identify critical data that needs to be replicated. This might include databases, documents, configurations, etc.

2.Replication Tool: Choose a replication tool compatible with your on-premises infrastructure and IBM Cloud. IBM Cloud offers services like IBM Cloud Object Storage for this purpose.

3.Network Configuration: Set up a secure, high-speed connection between your on-premises servers and IBM Cloud. VPNs or dedicated network connections are common methods.

4.Replication Settings: Configure replication schedules. Decide whether it's continuous, periodic, or triggered by certain events.

b. Virtual Machine Image Replication:

1.Disk Images: Create disk images of your virtual machines. Tools like IBM Cloud Virtual Servers can assist in this process.

2.Replication Method: Choose between snapshot-based replication or real-time replication. This depends on your RTO (Recovery Time Objective) and RPO (Recovery Point Objective) requirements.

3.Image Transfer: Use secure protocols to transfer these images to IBM Cloud. Encrypt the transfer to ensure data security.

2. Testing Recovery Procedures:

a. Disaster Simulation:

1.Scenario Definition: Define disaster scenarios. These could include server failure, data corruption, or a complete site outage.

2.Isolation: Isolate the affected systems from the network to simulate the unavailability of on-premises resources.

b. Recovery Procedure Testing:

1.Activate Replicas: Initiate the recovery process. Activate replicated virtual machines and data stores in IBM Cloud.

2.Configuration Validation: Ensure that the configurations are replicated accurately. IP addresses, domain names, and security settings should match the original setup.

3.Application Testing: Test critical applications to ensure they function correctly with the replicated data and systems.

4.Performance Monitoring: Monitor the performance of the recovered systems. Ensure they meet the required benchmarks for speed and reliability.

5.Data Integrity: Verify the integrity of replicated data. Run checksums or integrity checks to confirm data accuracy.

6.User Access: Confirm that users can access the applications and data seamlessly. Address any authentication or authorization issues promptly.

3. Documentation and Optimization:

1.Document the Process: Document every step of the recovery procedure. Include configurations, settings, and contact information for the team responsible for disaster recovery.

2.Optimization: Analyze the test results and optimize the recovery procedures if necessary. This could involve fine-tuning replication settings or network configurations.

3.Regular Testing: Disaster recovery plans should be regularly tested and updated to ensure they remain effective as your infrastructure evolves.

****