Disaster Recovery & High Availability Strategy

This document outlines the Disaster Recovery (DR) strategy for implementing backup and recovery   
 processes for an enterprise application hosted on Microsoft Azure. The strategy focuses on minimizing downtime,   
 ensuring data integrity, and automating recovery procedures to ensure business continuity in case of disasters.

# 1. Key Objectives

- Minimize downtime for critical applications.  
  
 - Preserve data integrity during and after a disaster.  
  
 - Ensure service availability across regions.  
  
 - Automate backup and recovery processes to reduce manual intervention.

# 2. Key Terms

Below are the key terms used to describe our DR strategy metrics:  
 - \*\*RTO (Recovery Time Objective)\*\*: The maximum time allowable to restore services after a failure or disaster.   
 - \*\*RPO (Recovery Point Objective)\*\*: The maximum allowable amount of data loss in terms of time.

# 3. Target Metrics

The following are the target RTO and RPO for our enterprise application in Azure:  
 - \*\*RTO\*\*: 30 minutes (Time to restore full service)  
 - \*\*RPO\*\*: 15 minutes (Max allowable data loss in the event of a failure)

# 4. Disaster Recovery Architecture in Azure

The Disaster Recovery architecture for this application involves utilizing Azure services to ensure high availability and   
 automated backup strategies for rapid recovery. Key components include:  
 - \*\*Azure Site Recovery (ASR)\*\* for VM replication across regions.  
 - \*\*Azure Backup\*\* to automate disk, database, and file share backups.  
 - \*\*Availability Zones\*\* to provide high availability for critical workloads.  
 - \*\*Traffic Manager or Azure Front Door\*\* for DNS-based failover between regions in case of a failure.

# 5. Disaster Recovery Tiers

We categorize applications into different recovery tiers based on their criticality:  
 - \*\*Tier 1 (Critical apps)\*\*: Active-Active deployment with real-time replication across multiple regions.  
 - \*\*Tier 2 (Important apps)\*\*: Active-Passive setup with warm standby and ASR.  
 - \*\*Tier 3 (Non-critical apps)\*\*: Cold backup with automated Azure Backup only, suitable for less critical workloads.

# 6. Testing & Monitoring

The Disaster Recovery plan should be tested regularly to ensure it works during actual failure scenarios. We recommend:  
 - Performing \*\*quarterly DR drills\*\* to validate the recovery process.  
 - Using \*\*Azure Monitor\*\* and \*\*Log Analytics\*\* for continuous monitoring of backups and alerts for failures.  
 - Setting up automatic \*\*alerts\*\* for any backup failures or DR triggers.

# 7. Roles & Responsibilities

The following table outlines the key roles and responsibilities for disaster recovery management:  
 - \*\*DevOps\*\*: Setting up and maintaining the disaster recovery configuration.  
 - \*\*Cloud Admin\*\*: Monitoring backup policies, retention, and recovery status.  
 - \*\*Application Owner\*\*: Validating application recovery and ensuring data integrity after a failure.

# 8. Example of Setting up Automated Backups in Azure

To set up automated backups for an Azure Virtual Machine, you can use Azure CLI. The following steps show how to configure backups:  
 - \*\*Step 1: Create a Recovery Services Vault\*\*

```bash  
 az backup vault create --resource-group myResourceGroup --name myRecoveryServicesVault --location eastus  
 ```

- \*\*Step 2: Set backup properties for redundancy\*\*:

```bash  
 az backup vault backup-properties set --name myRecoveryServicesVault --resource-group myResourceGroup --backup-storage-redundancy GeoRedundant  
 ```

- \*\*Step 3: Register VM with the Recovery Services Vault\*\*:

```bash  
 az backup protection enable-for-vm --resource-group myResourceGroup --vault-name myRecoveryServicesVault --vm myVM --policy-name DefaultPolicy  
 ```

# 9. Backup Schedule

We will configure daily full backups and retention for up to 30 days based on our RPO. Alerts will be set up to notify the team of any issues with the backup schedule.

# 10. Conclusion

This Disaster Recovery strategy ensures that critical applications hosted on Azure are protected, can be quickly recovered, and meet business continuity requirements. Automation of backup and recovery processes minimizes human error, while testing and monitoring the system ensures that recovery is achievable within the set RTO and RPO.