**Disaster Recovery & High Availability**

**1. Disaster Recovery Strategy Document**

**Title: Disaster Recovery Plan for Enterprise Application in the Cloud**

**Purpose: To ensure business continuity and minimize downtime in the event of a disaster.**

**Key Components of the DR Strategy**

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

* **Definition: The maximum acceptable downtime after a disaster.**
* **Target: 2 hours (example).**
* **Explanation: The application should be restored and operational within 2 hours of a disaster.**

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

* **Definition: The maximum acceptable data loss measured in time.**
* **Target: 15 minutes (example).**
* **Explanation: Data recovery should ensure no more than 15 minutes of data loss.**

**DR Strategy Overview**

**1. Backup Strategy**

* **Frequency: Daily full backups and hourly incremental backups.**
* **Storage: Backups stored in geographically redundant storage (e.g., Azure Geo-Redundant Storage).**
* **Retention: 30 days for daily backups, 7 days for incremental backups.**

**2. Disaster Recovery Plan**

* **Multi-Region Deployment: Deploy the application in at least two regions (e.g., East US and West US).**
* **Failover Mechanism: Use Azure Site Recovery (ASR) to automate failover to the secondary region.**
* **Data Replication: Replicate databases and storage accounts to the secondary region in real-time.**

**3. Testing and Validation**

* **Regular DR Drills: Conduct quarterly disaster recovery drills to test the failover process.**
* **Automated Monitoring: Use Azure Monitor and Alerts to detect failures and trigger recovery processes.**

**Implementation Steps**

1. **Backup Configuration:**
   * **Use Azure Backup to automate backups of virtual machines, databases, and file storage.**
   * **Configure backup policies to meet RPO and retention requirements.**
2. **Replication Setup:**
   * **Use Azure Site Recovery to replicate VMs and applications to the secondary region.**
   * **Configure replication settings to match RTO and RPO targets.**
3. **Failover Testing:**
   * **Simulate a disaster scenario and validate the failover process.**
   * **Ensure all critical systems and data are functional in the secondary region.**

**Example RTO and RPO Table**

| **Component** | **RTO** | **RPO** | **Strategy** |
| --- | --- | --- | --- |
| **Web Application** | **2 hours** | **15 minutes** | **Multi-region deployment with ASR failover** |
| **Database** | **1 hour** | **5 minutes** | **Real-time replication with Azure SQL** |
| **File Storage** | **2 hours** | **15 minutes** | **Geo-redundant storage with backups** |

**2. Example of Setting Up Automated Backups in Azure**

**Scenario: Automate backups for an Azure Virtual Machine (VM) using Azure Backup.**

**Steps to Set Up Automated Backups**

**Step 1: Create a Recovery Services Vault**

1. **Go to the Azure Portal.**
2. **Search for Recovery Services Vault and click Create.**
3. **Provide a name, select the resource group, and choose a region.**
4. **Click Review + Create and then Create.**

**Step 2: Configure Backup for the VM**

1. **Open the Recovery Services Vault you created.**
2. **Click Backup under the Getting Started section.**
3. **Select Azure Virtual Machine as the workload type and click Backup.**
4. **Choose the VM you want to back up and click OK.**

**Step 3: Set Backup Policy**

1. **In the Backup Policy section, create a new policy or use an existing one.**
2. **Configure the backup schedule:**
   * **Frequency: Daily**
   * **Time: 2:00 AM**
   * **Retention: 30 days**
3. **Click OK to save the policy.**

**Step 4: Enable Backup**

1. **Review the settings and click Enable Backup.**
2. **Azure will start backing up the VM according to the schedule.**

**Automating Backups with Azure CLI**

**You can also automate the backup setup using Azure CLI:**

**# Create a Recovery Services Vault**

**az backup vault create --name MyVault --resource-group MyResourceGroup --location eastus**

**# Enable backup for a VM**

**az backup protection enable-for-vm \**

**--resource-group MyResourceGroup \**

**--vault-name MyVault \**

**--vm MyVM \**

**--policy-name DefaultPolicy**

**Monitoring Backups**

* **Use Azure Monitor to track backup jobs and receive alerts for failures.**
* **Regularly review backup reports in the Recovery Services Vault.**