Disaster Recovery & High Availability

Key Elements of a DR Strategy

Recovery Time Objective (RTO)

Definition: Maximum acceptable downtime duration before service restoration. **Example Target:** 2 hours (system must be fully functional within 2 hours of incident).

Recovery Point Objective (RPO)

Definition: Maximum acceptable data loss measured in time before failure. **Example Target:** 15 minutes (data loss should not exceed the last 15 minutes of transactions).

Backup Strategy

- **Automated Backups:** Schedule regular backups using AWS Backup or native service features.
- **Geographical Redundancy:** Store critical backups in a separate AWS Region.
- **Testing and Validation:** Regularly test restore procedures to validate RTO and RPO targets.
- **Backup Security:** Encrypt all backups using AWS KMS and restrict access using IAM policies.

High Availability (HA) Implementation

- **Multi-AZ Deployments:** Deploy across multiple Availability Zones within an AWS Region.
- **Replication:** Utilize synchronous or near-synchronous replication for critical data.
- **Load Balancing:** Use Elastic Load Balancing to distribute traffic across healthy instances.
- **Automated Failover:** Configure services like Amazon RDS Multi-AZ for automatic failover.

Example: Automated Backup Setup using AWS Backup

1. Create a Backup Vault:

bash

```
aws backup create-backup-vault \
    --backup-vault-name MyBackupVault \
    --region us-east-1
```

2. Define and Assign a Backup Plan:

Create a JSON file (backup-plan.json):

json

```
{
    "BackupPlanName": "DailyBackupPlan",
    "Rules": [
        {
            "RuleName": "DailyFullBackup",
            "TargetBackupVaultName": "MyBackupVault",
            "ScheduleExpression": "cron(0 2 * * ? *)",
            "StartWindowMinutes": 60,
            "CompletionWindowMinutes": 180,
            "Lifecycle": {
                "DeleteAfterDays": 30
            }
        }
    ]
}
```

Create the backup plan:

bash

```
aws backup create-backup-plan --backup-plan
file://backup-plan.json

aws backup create-backup-selection \
    --backup-plan-id <your-backup-plan-id> \
    --backup-selection '{
        "SelectionName": "EC2Selection",
        "IamRoleArn":
"arn:aws:iam::<account-id>:role/service-role/AWSBackupDefaultServi
ceRole",
        "Resources": [

"arn:aws:ec2:us-east-1:<account-id>:instance/<instance-id>"
        ]
    }' \
    --creator-request-id $(uuidgen)
```

Example: Setting Up Automated Backups in AWS

AWS offers automated backup solutions integrated with many of its services. For instance, using AWS Backup you can centralize the backup of EC2 instances, RDS databases, and more. Below is an example using AWS CLI commands:

Create a Backup Vault:

```
aws backup create-backup-vault \
  --backup-vault-name MyBackupVault \
  --region us-east-1
```

1. *This command creates a backup vault in the specified region to store your backup data.*

Create and Assign a Backup Plan:

First, create a JSON file (e.g., `backup-plan.json`) with your backup plan details:

```
{
  "BackupPlanName": "DailyBackupPlan",
  "Rules": [
    {
      "RuleName": "DailyFullBackup",
      "TargetBackupVaultName": "MyBackupVault",
      "ScheduleExpression": "cron(0 2 * * ? *)",
      "StartWindowMinutes": 60,
      "CompletionWindowMinutes": 180,
      "Lifecycle": {
        "DeleteAfterDays": 30
      }
    }
  ]
}
```

Then, apply the backup plan and assign resources (for example, an EC2 instance):

```
# Create the backup plan
aws backup create-backup-plan --backup-plan file://backup-plan.json

# Assign resources (example for EC2, ensuring the resource ARN is correct)
aws backup create-backup-selection \
  --backup-plan-id <your-backup-plan-id> \
  --backup-selection '{
    "SelectionName": "EC2Selection",
    "IamRoleArn": "arn:aws:iam::<account-id>:role/AWSBackupDefaultServiceRole",
    "Resources": ["arn:aws:ec2:us-east-1:<account-id>:instance/<instance-id>"]
  }'
```

2. *This setup schedules a daily full backup for the specified EC2 instance, using AWS Backup with defined retention and scheduling, ensuring compliance with defined RTO and RPO.*