**Phase 2: Design – Cloud-Based Disaster Recovery**

**1. System Architecture Overview**

The disaster recovery (DR) solution is built using AWS services. The architecture is designed to ensure data availability, automated failover, and minimal manual intervention.

**Components:**

* **Primary Region**: Hosts the live production environment.
* **DR Region**: Contains standby instances and services activated during a failure.
* **AWS Services Used**:
  + **EC2** – Compute instances for applications.
  + **RDS** – Databases with replication and failover.
  + **S3** – Backup storage for data and configurations.
  + **Route 53** – DNS management with health checks and failover.
  + **CloudFormation** – Infrastructure as Code (IaC).
  + **Lambda** – Automates recovery operations.

**2. High-Level Workflow**

1. **Backup Phase**
   * EC2 and RDS data are regularly backed up to S3 using automated scripts (backup\_to\_s3.sh).
2. **Monitoring Phase**
   * Route 53 health checks monitor service availability.
   * CloudWatch captures logs and metrics for alerting.
3. **Failover Trigger**
   * Upon detecting failure, Route 53 redirects traffic to the DR region.
   * Lambda (lambda\_start\_ec2.py) spins up the required infrastructure.
4. **Recovery & Continuity**
   * CloudFormation (cloud\_dr\_resources.yaml) deploys infrastructure in DR region.
   * Application resumes with minimal disruption.

**3. Key Design Considerations**

| **Factor** | **Design Approach** |
| --- | --- |
| Availability | Multi-AZ, multi-region redundancy using RDS and Route 53 |
| Scalability | Auto-scaling enabled for EC2 using CloudFormation templates |
| Automation | Failover process automated via Lambda and IaC |
| Security | IAM policies, encrypted S3, VPC-level isolation |
| Cost Optimization | Cold standby model: resources activated only during failover |

**4. Infrastructure as Code (IaC)**

The CloudFormation template (cloud\_dr\_resources.yaml) automates provisioning of:

* VPCs, Subnets
* EC2 instances and Auto Scaling groups
* RDS databases with replication
* Lambda functions for orchestration
* Security groups and IAM roles

This enables reproducible deployments across regions and faster DR readiness.

**5. Design Diagram (Suggested)**

Here’s a suggested architecture flow:

User → Route 53 → EC2 (Primary Region) → RDS (Primary)

↓

CloudWatch + Lambda

Failure Detected → Route 53 → EC2 (DR Region) → RDS Replica / Restored DB