High Availability and Disaster Recovery Architecture Document

1. Introduction

This document outlines the high availability (HA) and disaster recovery (DR) architecture for the system. It includes objectives, architecture overview, and recovery procedures.

2. Objectives

- Ensure minimal downtime for critical services
- Protect data integrity in case of failures
- Enable fast recovery from disaster events

3. Architecture Overview

3.1 System Components

- Application Servers (App1, App2)
- Load Balancers
- Database Cluster
- Storage (Primary & Backup)
- Networking Components

3.2 High Availability Topology

The architecture utilizes redundant servers and components across multiple availability zones. Load balancers ensure failover and traffic distribution.

3.3 Disaster Recovery Site

A secondary site is maintained with asynchronous data replication for critical databases and file storage. DNS failover ensures traffic redirection.

4. Recovery Point Objective (RPO) & Recovery Time Objective (RTO)

Component	RPO	RTO
Application Service	< 5 minutes	< 30 minutes
Database	< 1 minute	< 15 minutes
Storage	< 10 minutes	< 30 minutes

5. Backup and Replication

- Daily full and hourly incremental backups
- Asynchronous data replication to the DR site

6. Failover and Recovery Process

- Automatic failover for application services via load balancer

- Manual failover to DR site triggered by operations team
- Restoration of services and data verification

7. Roles and Responsibilities

Role	Responsibility
Operations Team	Monitor systems & initiate failover
DBA	Maintain replication and backups
Network Engineer	Configure and test failover routing

8. Testing & Validation

- Quarterly DR drills
- Regular backup restoration tests
- HA failover simulations

9. Document History

Version	Date	Changes
1.0	2024-06-12	Initial draft