

ALTA DISPONIBILIDAD Y DISASTER RECOVERY

Estrategia Multi-Región

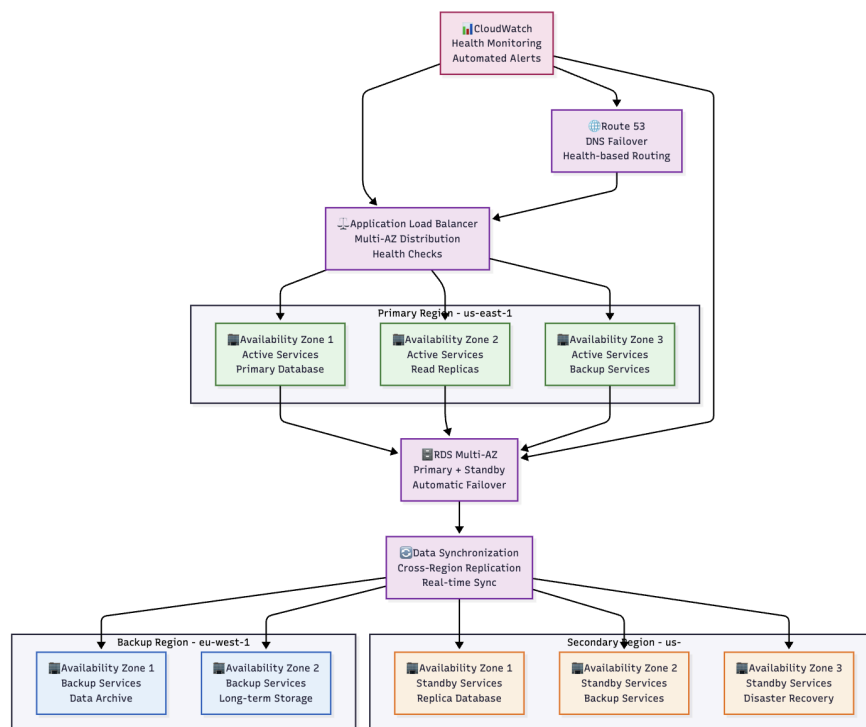
La estrategia multi-región garantiza continuidad del negocio ante fallos de región completa, cumpliendo con SLAs de 99.99% de disponibilidad.

Regiones:

- us-east-1 : Región Primaria
- us-east-2 : Región Secundaria
- eu-west-1 : Región Back Up

Arquitectura Multi-Región:

- Región Primaria: Servicios activos, base de datos principal
- Región Secundaria: Servicios en standby, réplicas de base de datos
- Región de Backup: Servicios de backup, archivo a largo plazo
- Sincronización: Replicación en tiempo real entre regiones
- Failover: Automático y manual con Route 53



ALTA DISPONIBILIDAD Y DISASTER RECOVERY

Disaster Recovery Plan

Escenarios de Desastre:

- Fallo Completo de Región: Desastres naturales, fallos de infraestructura
- Fallo Parcial de Servicio: Corrupción de base de datos, degradación de servicios
- Brecha de Seguridad: Compromiso de datos, shutdown de servicios

Procedimientos de Recuperación:

- Detección: Monitoreo automatizado y sistemas de alerta
- Evaluación: Análisis de impacto y estimación de tiempo de recuperación
- Activación: Procedimientos de failover y restauración de servicios
- Validación: Verificación de integridad de datos y funcionalidad de servicios
- Comunicación: Notificación a stakeholders y actualizaciones de estado

Implementación de Alta Disponibilidad

Load Balancing

- Application Load Balancer: Distribución multi-AZ con health checks
- Health Checks: Verificación cada 30 segundos con timeout de 5 segundos
- Target Groups: Configuración específica por servicio
- Failover: Automático cuando health checks fallan

Auto Scaling

- ECS Auto Scaling: Escalado automático basado en métricas
- Métricas: CPU (70%), Memoria (80%)
- Capacidad: Mínimo 2, máximo 10, objetivo 5
- Cooldown: 300 segundos para scale out/in

Database High Availability

- RDS Multi-AZ: Failover automático con standby
- Read Replicas: Réplicas en múltiples regiones
- Backup: Retención de 30 días con ventana de 3-4 AM
- DynamoDB Global Tables: Replicación automática entre regiones

ALTA DISPONIBILIDAD Y DISASTER RECOVERY

Estrategias de Backup

Backup Continuo

- RDS Automated Backups: Backups automáticos diarios
- S3 Cross-Region Replication: Replicación en tiempo real
- Point-in-Time Recovery: Recuperación a cualquier punto en el tiempo
- Integridad: Verificación automática de integridad de backups

Backup Programado

- Lambda Backup Function: Backups diarios a las 2 AM
- Snapshots: Snapshots de RDS con nomenclatura por fecha
- DynamoDB: Backup de tablas DynamoDB
- S3 Buckets: Backup de buckets S3
- Verificación: Verificación de integridad post-backup

Archivo a Largo Plazo

- S3 Glacier: Archivo de datos antiguos
- Lifecycle Policies: Transición automática por edad
- Storage Classes: STANDARD_IA → GLACIER → DEEP_ARCHIVE
- Compliance: Almacenamiento para cumplimiento regulatorio

Monitoreo y Alertas

CloudWatch Alarms

- Alarmas Críticas: CPU > 80%, Database Connections > 100
- Evaluación: 2 períodos de evaluación de 5 minutos
- Acciones: Scale out, alertas al equipo, auto-scaling
- Notificaciones: SNS, Slack, email

Health Monitoring

- Liveness Probe: Verificación de que el servicio está vivo
- Readiness Probe: Verificación de que el servicio está listo
- Dependencies: Verificación de dependencias críticas
- Status Codes: 200 OK para liveness, 503 para readiness

ALTA DISPONIBILIDAD Y DISASTER RECOVERY

Procedimientos de Failover

Failover Automático

- Route 53 Health Checks: Verificación cada 30 segundos
- Failure Threshold: 3 fallos consecutivos
- Health Threshold: 2 verificaciones exitosas
- DNS Failover: Cambio automático de DNS a región secundaria

Failover Manual

- Scripts de Failover: Scripts automatizados para failover manual
- Route 53 Records: Actualización de registros DNS
- Load Balancer: Modificación de target groups
- Scaling: Escalado de región secundaria
- Notificaciones: Notificación automática al equipo

