🧠 cloudChronicles Lab #001: Disaster Recovery Detective

Lab Type: Idea
Estimated Time: 30–45 mins
Skill Level: Beginner

```
# Let's begin by printing your name to personalize the notebook
your_name = "Raheem Kareem"
print(f"Welcome to the lab, {your_name}!")
```

```
Welcome to the lab, Raheem Kareem!
```

🔍 STAR Method Lab Prompt

Situation:
A critical, customer-facing application hosted on Google Cloud Platform (GCP) experienced a regional outage in us-west2. This outage has rendered all services and data within that region temporarily unavailable, leading to a significant impact on application availability and user experience. The application relies on Cloud SQL for its transactional database and Cloud Storage for static assets and user-uploaded content.

Task:
Develop a comprehensive, STAR-based disaster recovery (DR) plan that ensures business continuity for the application in the event of a us-west2 regional outage. The plan must leverage Google Cloud tools like Cloud SQL replicas, multi-region Cloud Storage, and Pub/Sub alerts to explain the failover and recovery process, while actively reducing Total Cost of Ownership (TCO) and mitigating technical debt.

Action:
Proactive Setup & Redundancy (TCO & Technical Debt Reduction):

Primary Region: us-west2. Secondary (DR) Region: us-central1. Cloud SQL (PostgreSQL or MySQL): Configure the primary Cloud SQL instance in us-west2 with a cross-region read replica in us-central1. Ensure point-in-time recovery is enabled. This provides high availability and a low Recovery Point Objective (RPO) with minimal operational overhead (reduced technical debt) and uses native, cost-effective services (reduced TCO). Cloud Storage: Utilize a multi-region Cloud Storage bucket (e.g., nam5) for critical application data, static assets, and backups. Enable object versioning to protect against accidental deletions. For higher performance or specific regulatory needs, a dual-region bucket (e.g., us-west1 and us-central1 if us-west2 is unavailable) could be configured. This intrinsically provides data resilience across regions, reducing the need for custom replication solutions (technical debt) and leveraging tiered storage for cost optimization (TCO). Compute Resources (GKE or Compute Engine): GKE: Maintain a smaller, pre-provisioned GKE cluster in us-central1 (DR region) with necessary application deployments ready to scale up. Use Istio or similar service mesh for traffic management and resilience. Compute Engine: Utilize Instance Templates and Managed Instance Groups configured across us-west2 and us-central1, with autoscaling policies. TCO/Technical Debt: Leverage Infrastructure as Code (e.g., Terraform, Cloud Deployment Manager) to define and manage infrastructure in both regions. This automates deployment, reduces manual errors (technical debt), and allows for precise resource allocation, preventing over-provisioning (TCO). Networking: Deploy a Global HTTP(S) Load Balancer with backend services pointing to us-west2 and us-central1 compute resources. Use Cloud DNS for external traffic routing with health checks. CI/CD: Implement Cloud Build and Cloud Deploy for automated, multi-region deployments, ensuring consistent application versions across regions and reducing manual intervention during DR. Failover Mechanism & Alerts:

Monitoring & Health Checks (Cloud Monitoring): Configure comprehensive health checks in Cloud Monitoring for critical services (load balancer endpoints, application health, database connectivity) in us-west2. Alerting (Pub/Sub & Cloud Functions/Cloud Workflows): If us-west2 health checks fail repeatedly, Cloud Monitoring triggers an alert. This alert publishes a message to a dedicated Pub/Sub topic (dr-failover-trigger). A Cloud Function or Cloud Workflow subscribed to this Pub/Sub topic is invoked. This function acts as the failover orchestrator. Failover Orchestrator Actions: Cloud SQL Failover: Promote the Cloud SQL read replica in us-central1 to a standalone primary instance. This process is largely automated by Cloud SQL. Traffic Redirection (Cloud DNS & Global Load Balancer): Update Cloud DNS records to prioritize us-central1 endpoints or adjust Global Load Balancer routing preferences to shift all traffic to the healthy us-central1 backends. This can be automated by the Cloud Function interacting with the Load Balancer API. Compute Scaling: Scale up GKE clusters or Managed Instance Groups in us-central1 to handle the full production load. Notification: Send notifications to relevant teams via Cloud Notification channels (e.g., email, PagerDuty). TCO/Technical Debt: Automating the failover with serverless Cloud Functions and Pub/Sub minimizes human error and intervention (technical debt) and incurs costs only when executed (TCO). Recovery & Reversion (us-west2 Restoration):

Initial Verification: Once failover is complete, thoroughly verify application functionality, data consistency, and performance in us-central1. Data Synchronization: Implement robust data synchronization mechanisms (e.g., Cloud Dataflow jobs, database replication tools) to ensure any data generated in us-central1 during the outage is safely replicated or backed up. Post-Incident Analysis: Conduct a comprehensive post-mortem to analyze the outage, identify root causes, and refine the DR plan. Re-establish DR: When us-west2 services are restored and stable: Option A (Replicate Back): Re-establish us-west2 as the primary, replicating data from us-central1 back to us-west2, and then performing a planned failback. Option B (Stay in DR Region): If us-central1 proves stable and performant, consider keeping it as the new primary and establishing a new DR region. TCO/Technical Debt: Documenting and automating these steps reduces recurring manual efforts and builds institutional knowledge, preventing future technical debt. Regular DR drills (game days) further reduce risk and improve response times.

Expected Result:
A highly resilient, multi-region architecture on GCP that ensures RTO < 1 hour and RPO < 5 minutes in the event of a us-west2 regional outage. The implemented plan will provide seamless failover, minimal data loss, and swift recovery, all while demonstrating judicious use of GCP services to optimize costs and maintain a low level of technical debt. A documented, tested, and regularly updated disaster recovery playbook will be the primary deliverable, ensuring operational readiness and compliance.

✍️ Your Assignment

```
Primary Region: us-west2
Backup Location: us-central1
Failover Trigger: Cloud Monitoring health checks + Pub/Sub alerts + Cloud F
Redundancy Services:
Cloud SQL with cross-region read replica (us-central1)
Multi-region Cloud Storage (e.g., nam5) with object versioning
Pre-provisioned GKE cluster/Managed Instance Groups in us-central1
Global HTTP(S) Load Balancer with Cloud DNS
Backup Schedule: Cloud SQL Point-in-Time Recovery (continuous); Multi-regio
```