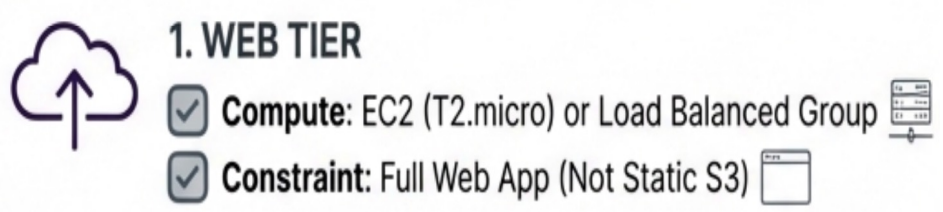
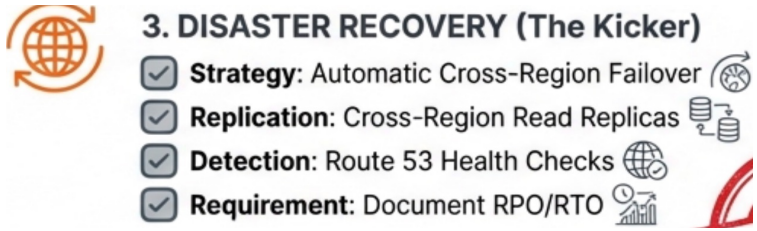
AWS Multi-Region High-Availability Project

Primary Objective: This project establishes a highly secure, resilient, and automated **Active-Active** infrastructure across two AWS regions. It is engineered to maintain application availability even during a complete regional outage by utilizing automated failover and secure, event-driven configuration updates.

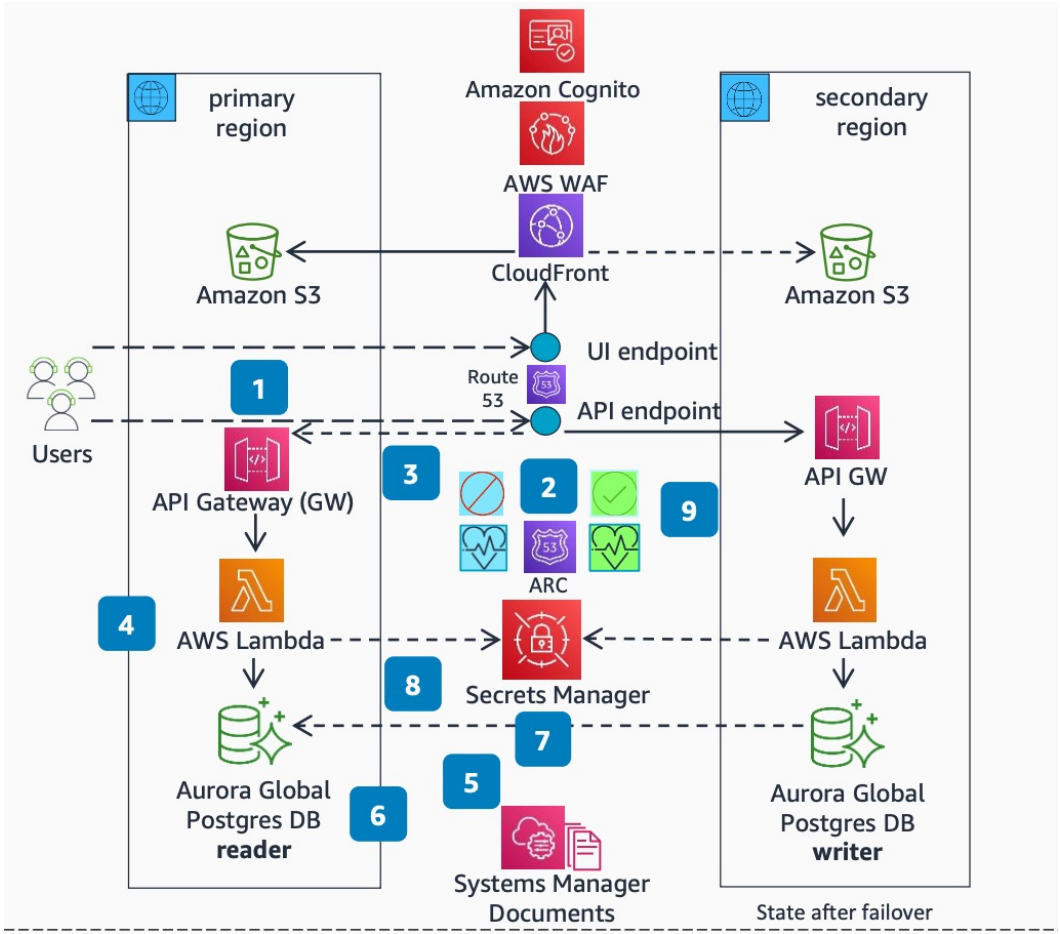
- Core Architecture Components:





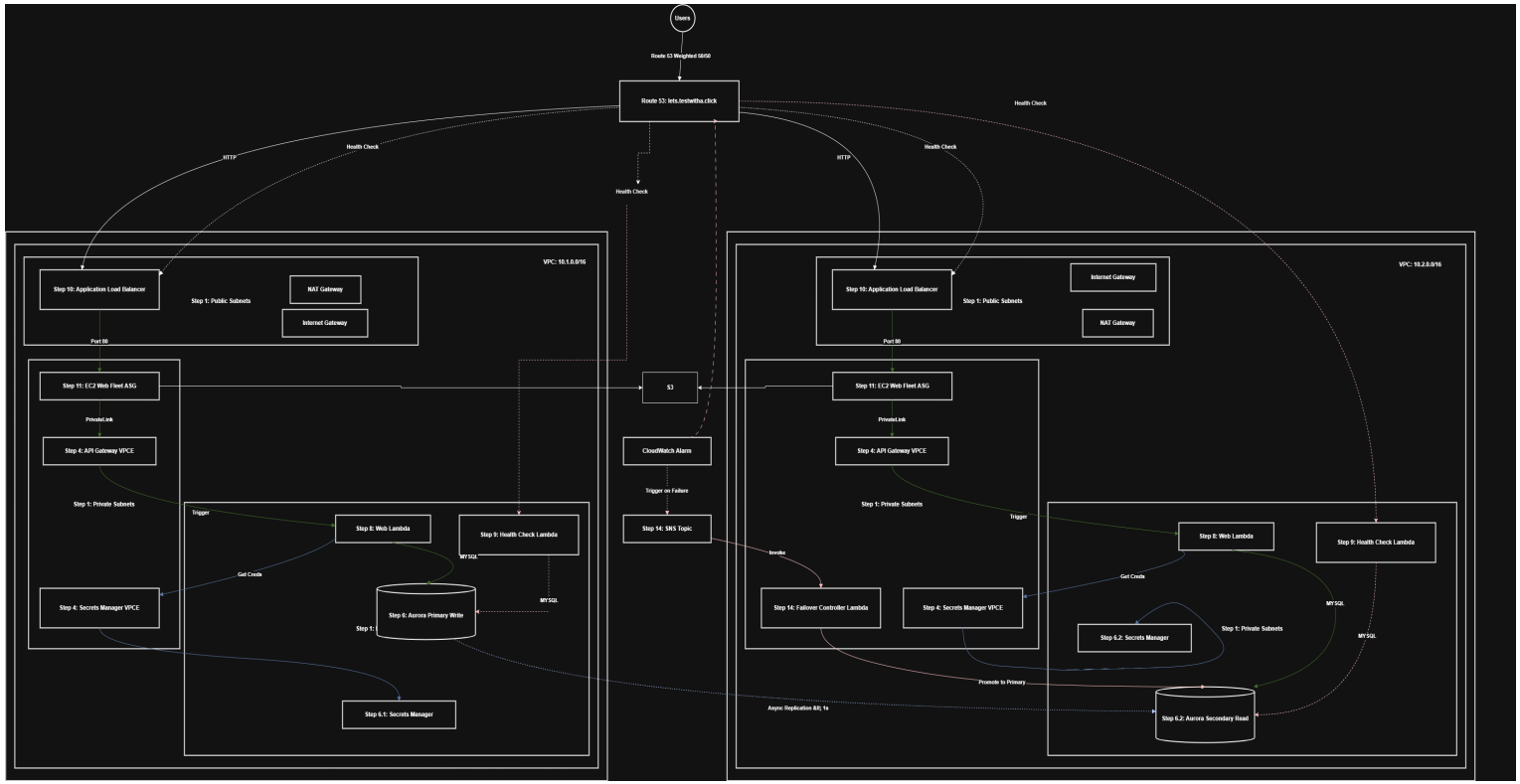
Architecture Diagram

- Global Routing: Route 53 directs traffic to regional ALBs.
- Data Resilience: Aurora Primary (R1) with Async Replication (R2).
- Automated Failover 'Brain':
  - EventBridge: Detects primary DB failure events.
  - Lambda: Decision-maker promoting R2 Replica to Writer.
  - Secrets Manager: Automated endpoint updates for app tier.



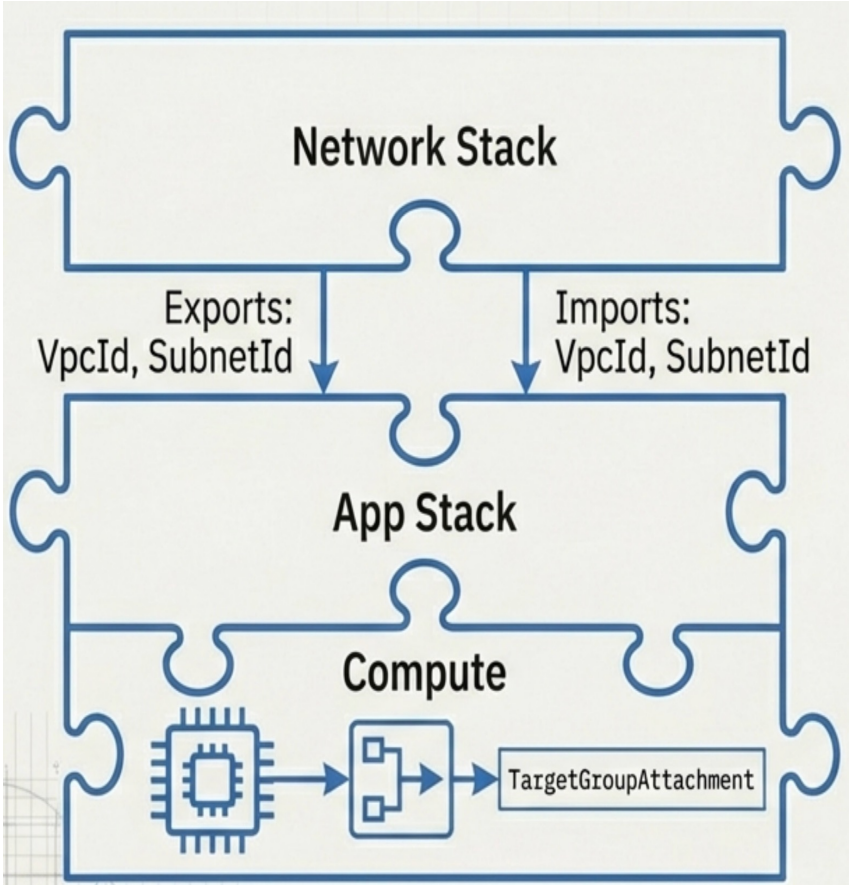
Sample Architecture Diagram

Architecture Diagram and Cloudformation

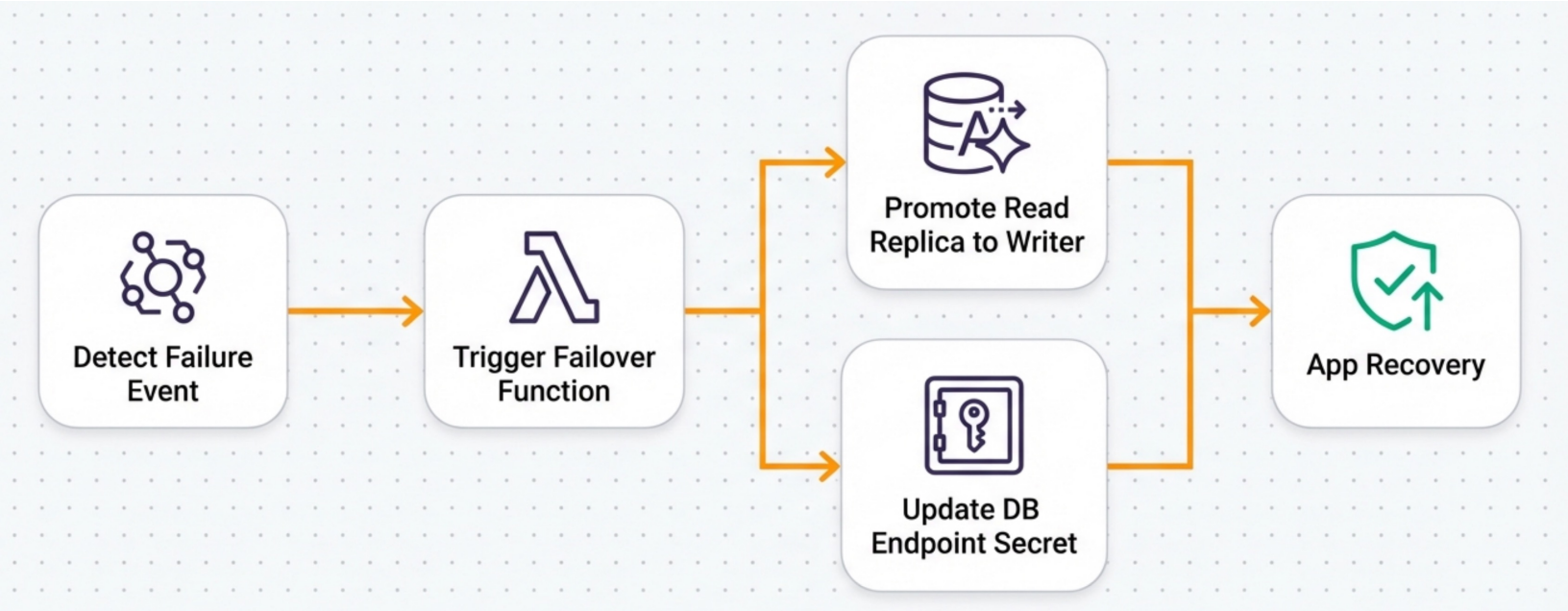


Infrastructure As Code (Phase 1)

- Network Stack: VPC, Subnets
- App Stack: ALB, EC2, Target Groups
- Data Stack: RDS Aurora
- Exports/Imports: Auto linking VpcId and subnetId between stacks
- Dynamic Parameters: Mapping AMI IDs for US-East-1 vs US-East-2

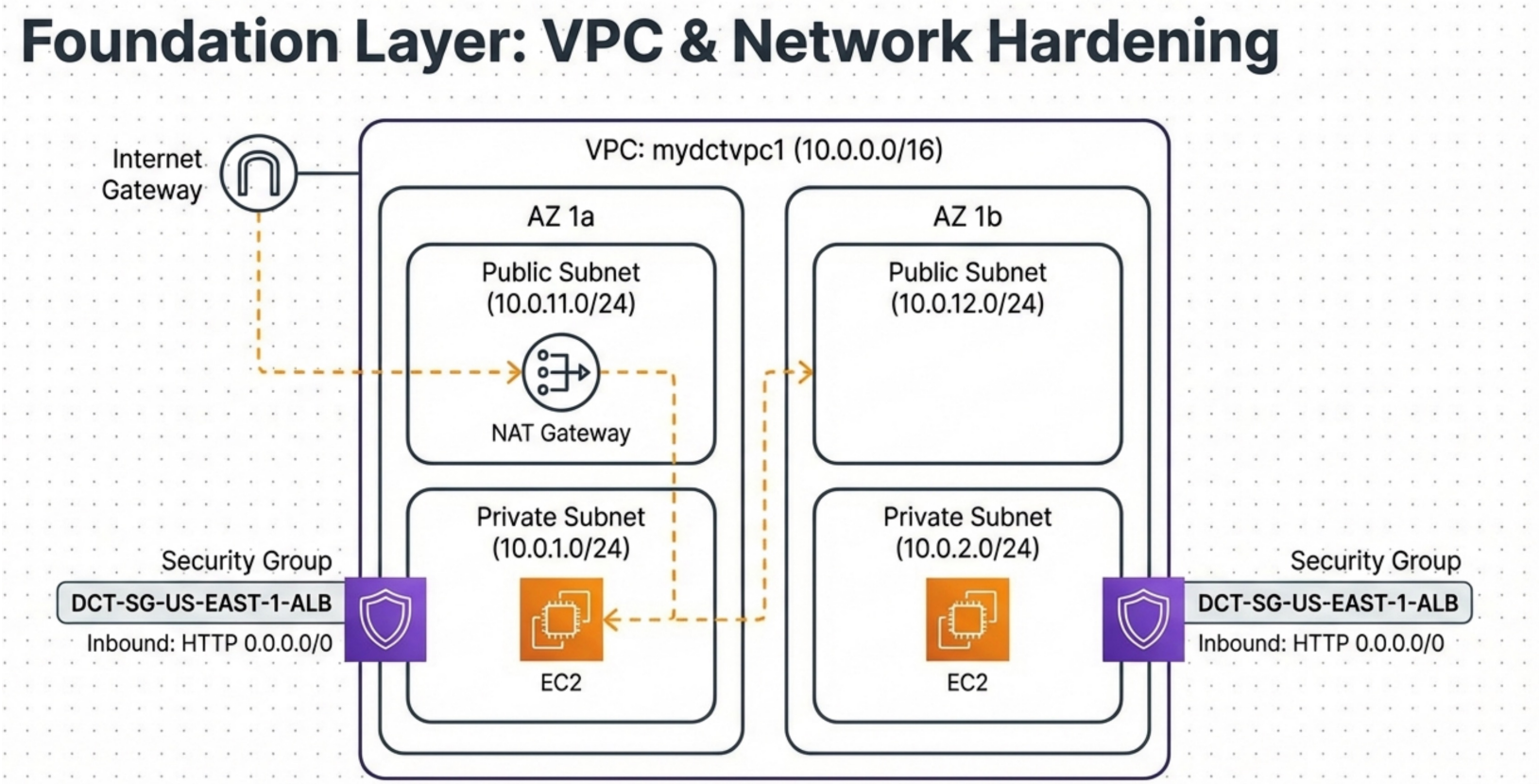


Event-Driven Serverless Logic (Phase 2)



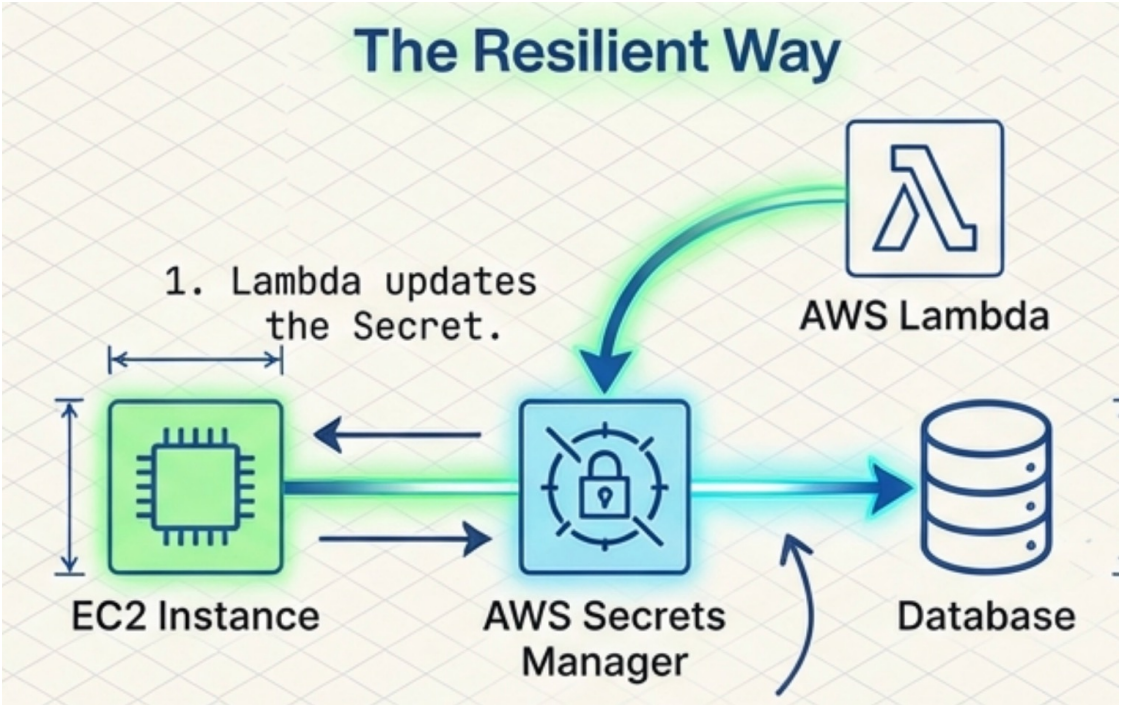
Lambda acts as a Decision Maker. Because the app trusts only Secrets Manager, Lambda controls the traffic flow. Even if the old Primary recovers, it is ignored.

Security and Credential Management(VPC and Network Hardening) – Phase 3



Secret Manager Configuration

- Lambda updates the Secret Manager
- App queries Secret Manager
- Traffic follows the map.



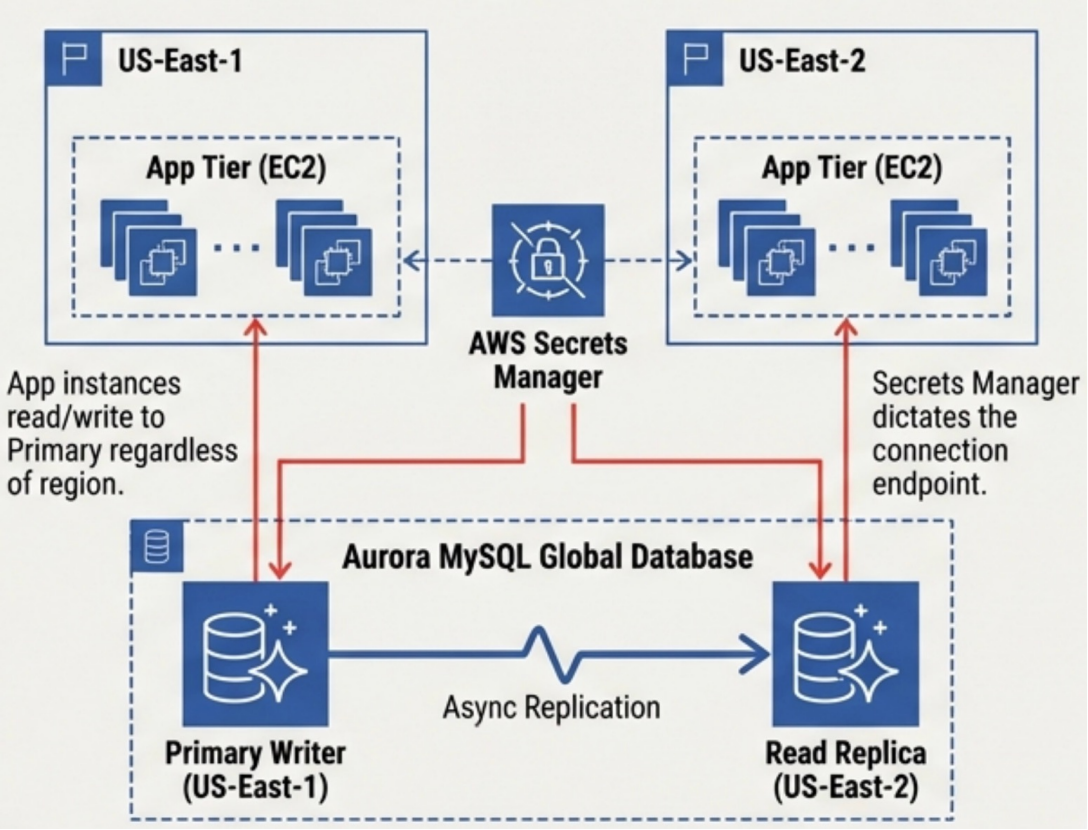
Data Tier and Disaster Recovery – Phase 4

built for durability and cross-region resilience.

Region 1 acts as Primary sites

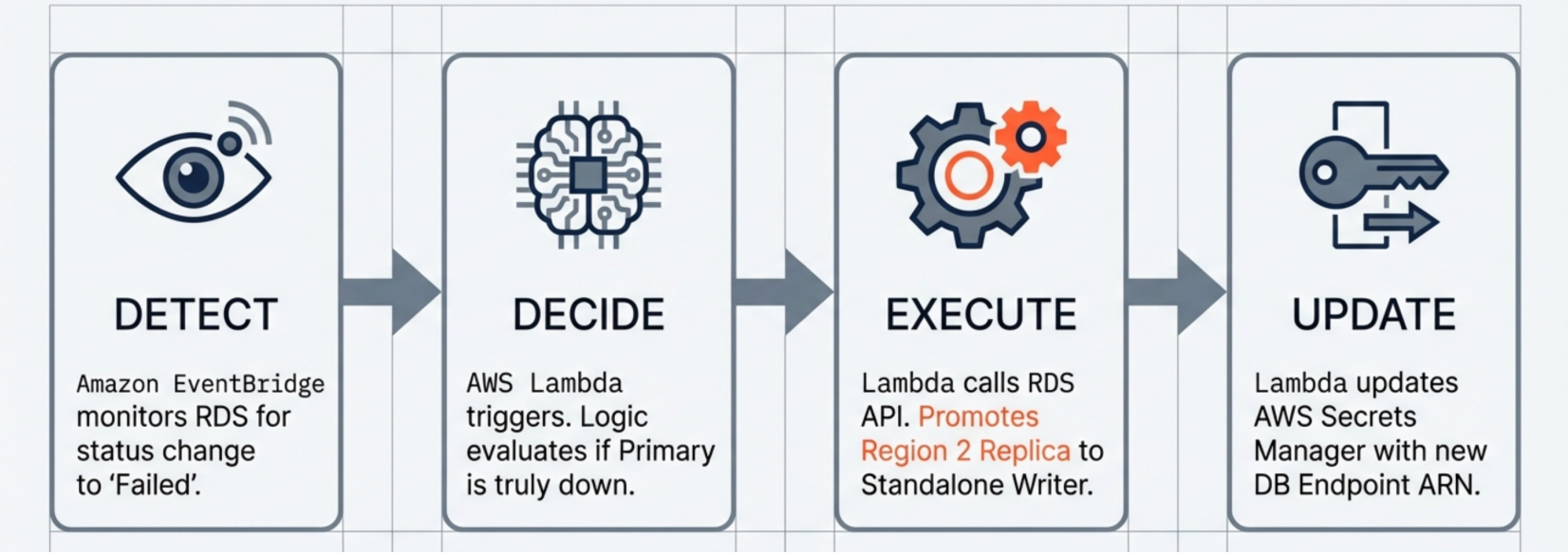
Read Replica synchronized via cross region replication

Failover Protocol

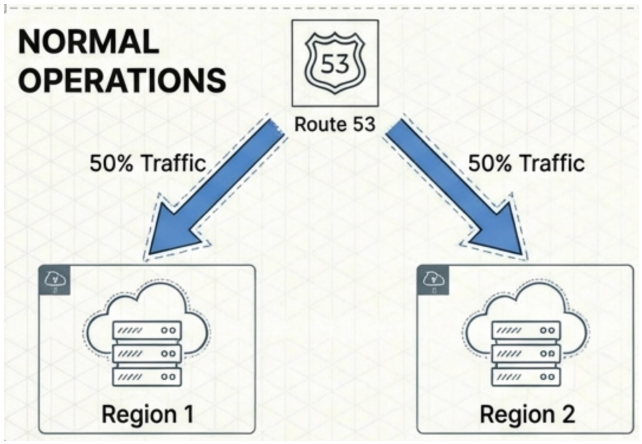


Failover sequence (Phase 5)

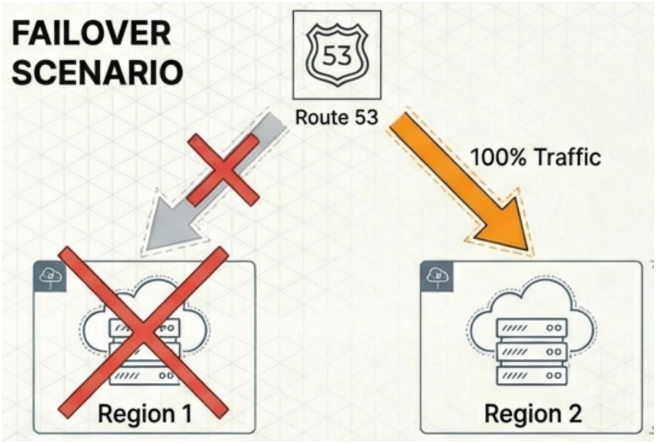
- Amazon EventBridge and AWS Lamba



Web Traffic Management Strategy



Active-Active Split: Immediate availability, no cold starts.



Automated Rerouting: Route 53 Health Checks detect failure and shift traffic instantly.

Network Security Configuration (Security Groups) (Phase 6)

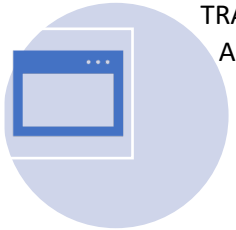
Security Groups act as stateful firewalls at the instance level.

Layer	Inbound Rules	Outbound Rules
ALB Security Group	HTTPS (443) from Public Internet	Limited to EC2 Group on application port
EC2 Security Group	Strictly allows traffic only from ALB Group	HTTPS (443) to Secrets Manager Endpoint & NAT Gateway
Lambda Security Group	Allows traffic only from API Gateway	DB Traffic (3306) to RDS & HTTPS (443) to Secrets Endpoint
VPC Endpoint SG	HTTPS (443) only from EC2 and Lambda Groups	N/A
Database (RDS) SG	DB traffic (3306) **only** from Lambda Group	N/A

Security Implementation Summary

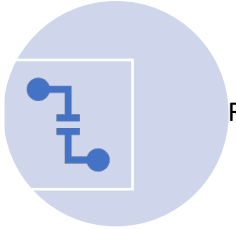
- **Configure IAM Roles:** Create EC2 Instance Profiles and Lambda Execution Roles with restricted policies.
- **Deploy VPC Endpoints:** Establish Interface Endpoints for Secrets Manager in private subnets with restricted VPC Endpoint Policies.
- **Define Security Group Chain:** Create a "chained" model where the Database only accepts traffic from the application layer.
- **Set Up NAT Gateway:** Deploy in the public subnet for secure outbound patching.
- **Enable Automation:** Link EventBridge to Lambda to ensure the DB ARN is updated securely in Secrets Manager immediately upon failover.

Some Major Challenges



TRAFFIC FAILED TO REACH THE APPLICATION SERVERS. THE SETUP MIRRORED THE WORKING REGION 1 CONFIGURATION

ROUTE 53 HEALTH CHECKS FOR REGION 2 FAILED CONSISTENTLY.



DIRECT ACCESS TO THE REGION 2 ALB DNS NAME RESULTED IN TIMEOUTS OR ERROR MESSAGES.

TARGET GROUPS REPORTED "UNHEALTHY" STATUS FOR ALL REGISTERED TARGETS.

Impact: The breakdown in Region 2 jeopardized the **Active-Active** failover strategy required for the project

Troubleshooting and Resolution

Analysis

Verified that Security Groups allowed Port 80 traffic. Validated that Target Groups were created and assigned to the ALB.

Route Tables had correct IGW/NAT Gateway associations.

Security Groups were identical to Region 1.

NACLs were open.

Resolution

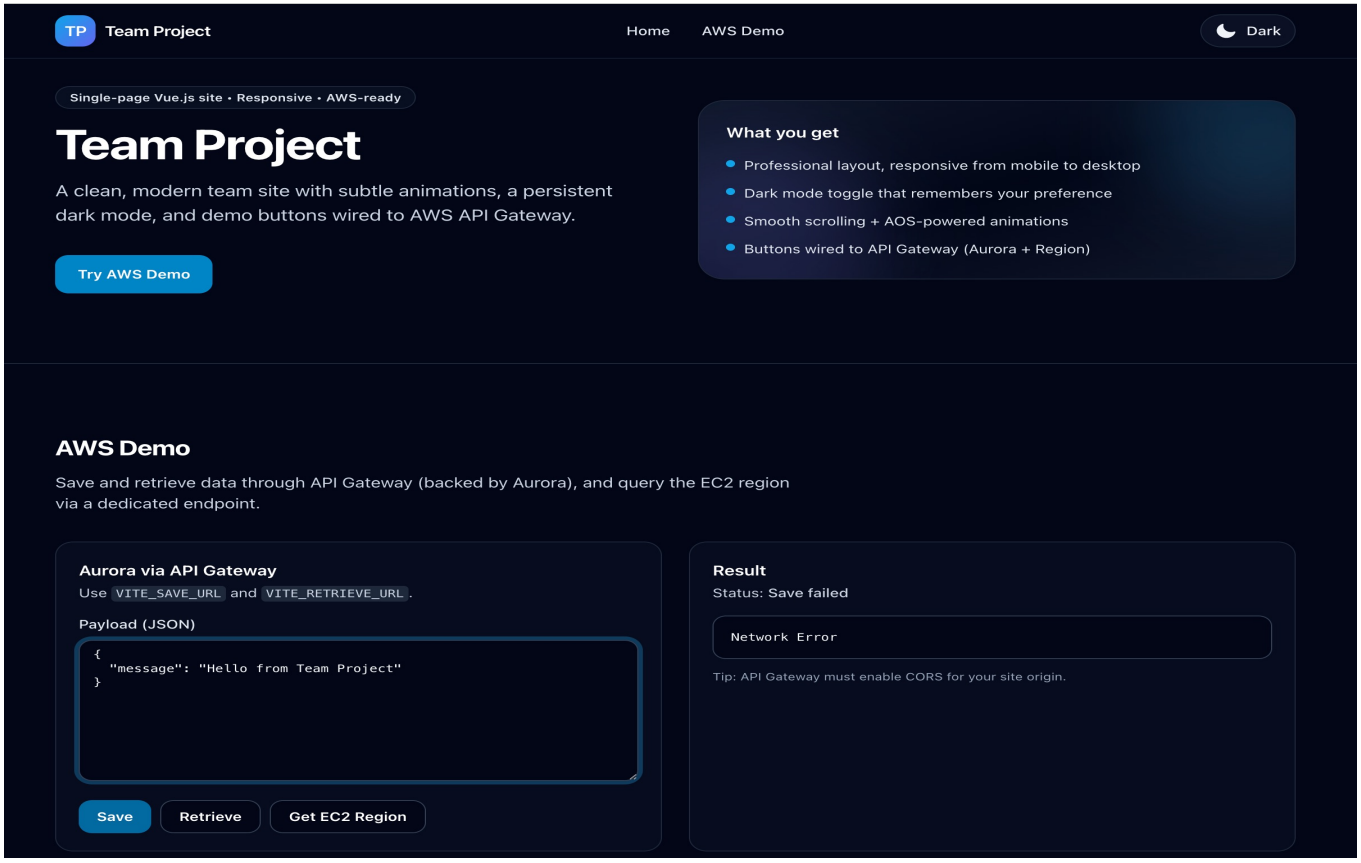
During the manual setup of the Target Groups in the AWS Console, **Port 80** was inadvertently typed into the **"Target control port"**

This misconfiguration overrode the default behavior, causing the Load Balancer to misinterpret the target's availability, effectively severing the connection between the ALB and the EC2 instances.

The incorrect port entry was removed from the "Target control port" field, allowing the ALB to correctly identify and route traffic to the healthy EC2 instances.

Success and Demo

Project Github repo:
https://github.com/Geisel21/aws-team-project/tree/main/team-project

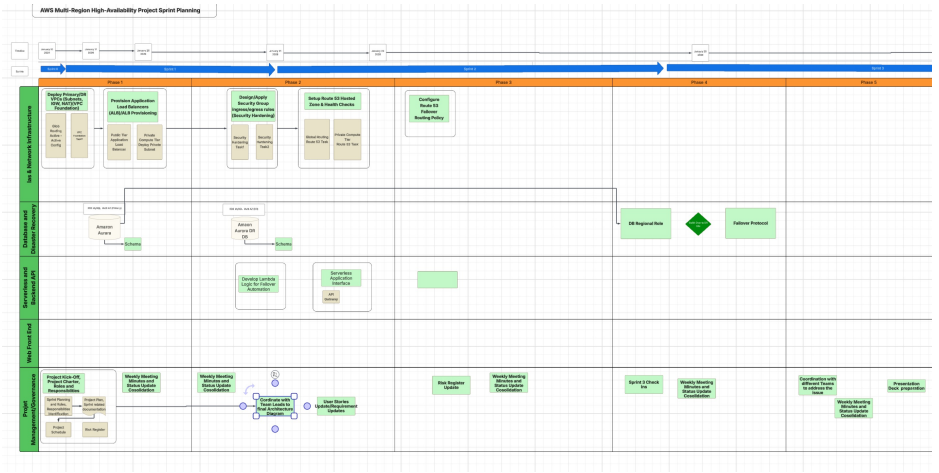


Sprint Planning

- Task Management Via PM best practices
- Sprint planning
- Risk Management
- Change Management
- Communication Management

ID	Task Name	Priority	Assigned To	Start Date	End Date	Dependencies	Status	Sprint	Comments	Impediments/Risks	Risk Heatmap
1	**IaC & NETWORK INFRASTRUCTURE**	High	Anson, Aniket	Jan 17	Jan 30		In Progress				
1.1	Deploy Primary/DR VPCs (Subnets, IGW, NAT)(VPC Foundation)	P1	Anson, Aniket	Jan 17	Jan 23	-	Completed (100%)	1,2	1/20/26 - Private Subnet, Public Subnet, Route table - Done	1/17/26- Need to Update on VPC Foundation status	
1.2	Design/Apply Security Group ingress/egress rules (Security Hardening)	P1	Aniket	Jan 18	Jan 27	1.1	Completed (100%)	1,2,3		1/17/26 - No Known Risks	
1.3	Provision Application Load Balancers (ALB)/ALB Provisioning	P2	Terrence	Jan 20	Jan 28	1.2	In Progress (50%)	1,2,3	1/20/26: Pending 1.1, 1.2 and other dependencies	1/20/26 - Pending 1.1, VPC Foundation, Security Hardening	
1.4	Setup Route 53 Hosted Zone & Health Checks	P1	Terrence, Aniket	Jan 21	Jan 28	1.3	In Progress(50%)	1,2,3	1/20/26 - Pending 1.1, 1.2 and other dependencies	1/20/2026 - Pending 1.1, 1.2	
1.5	Configure Route 53 Failover Routing Policy	P1	Terrence, Aniket	Jan 22	Jan 28	1.4	In Progress	1,2,3	1/20/26 - Pending 1.1, 1.2 and other dependencies		
2	**DATABASE & DISASTER RECOVERY**	High	Aniket, Joseph, Imrus	Jan 17	Jan 30		In Progress				
									1/17/26: Need to find more information on	1/20/26 - Database set up pending, not sure how to start the setup 1/23/26 - We are trying to figure out how the database will be	

Convert to table



Lessons Learned & Roadmap

1. Dependency Management: Compute & Network synchronization.

2. IaC Modularity: Exports/Imports vs. Monolithic Templates.

3. Deploying via **CloudFormation** ensures that configurations are deterministic and consistent across regions

Future deployments will rely strictly on the templates defined in the **IaC & Network Infrastructure** sprint to guarantee architectural parity between US-East-1 and US-East-2

Outcome: Deep understanding of AWS high-availability logic.