Disaster Recovery on AWS

Best practices for designing disaster-resilient workloads

Seth Eliot
Principal Reliability SA
AWS Well-Architected

Alex Livingstone
Practice Lead Cloud Operations
AWS Enterprise Support

Presenters

Seth Eliot
Principal Reliability Solutions Architect
AWS Well-Architected

Alex Livingstone
Practice Lead Cloud Operations
AWS Enterprise Support

aws

Disaster Recovery of Workloads on AWS

RECOVERY IN THE CLOUD

AWS whitepaper
February 12, 2021

http://bit.ly/DR_AWS

aws

Why you need a DR plan

```
# rm -rf *
```


aws

Poll

Have you ever deleted anything without intending to?

Yes

No

aws

Disaster recovery and availability

aws

What is disaster recovery?

aws

Everything fails, all the time

Disaster recovery (DR)

About business continuity

Larger scale, less frequent, events:

- Natural disasters
- Technical failures
- Human actions

Measures a one-time event:

- Recovery Time
- Recovery Point

aws

High availability (HA)

About application availability

Smaller scale, more frequent events:

- Component failures
- Network issues
- Load spikes

Measures mean over time:

- “The 9’s” (99.99% available)

aws

What is a disaster?

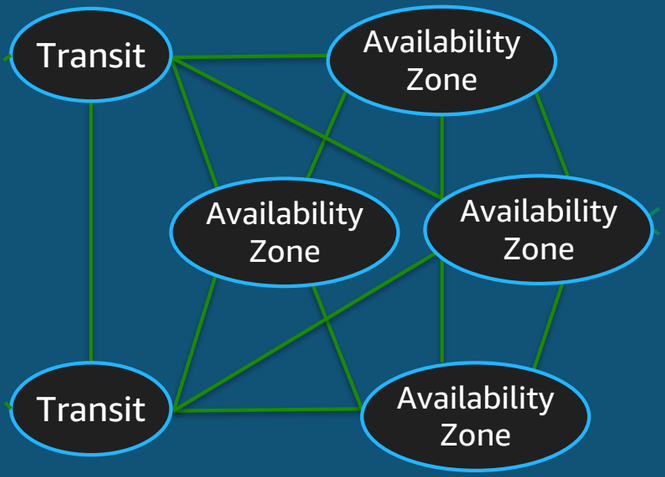
AWS Regions and Availability Zones

AWS Regions are physical locations around the world where we cluster data centers

25 AWS Regions worldwide

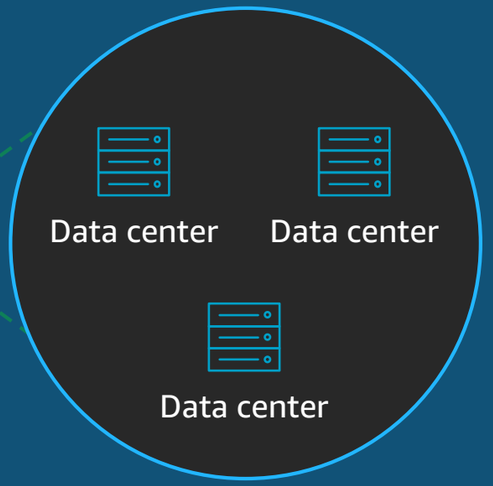
Region and number of Availability Zones

Each AWS Region has multiple Availability Zones



A **Region** is a physical location in the world

Each Availability Zone is one or more discrete data centers

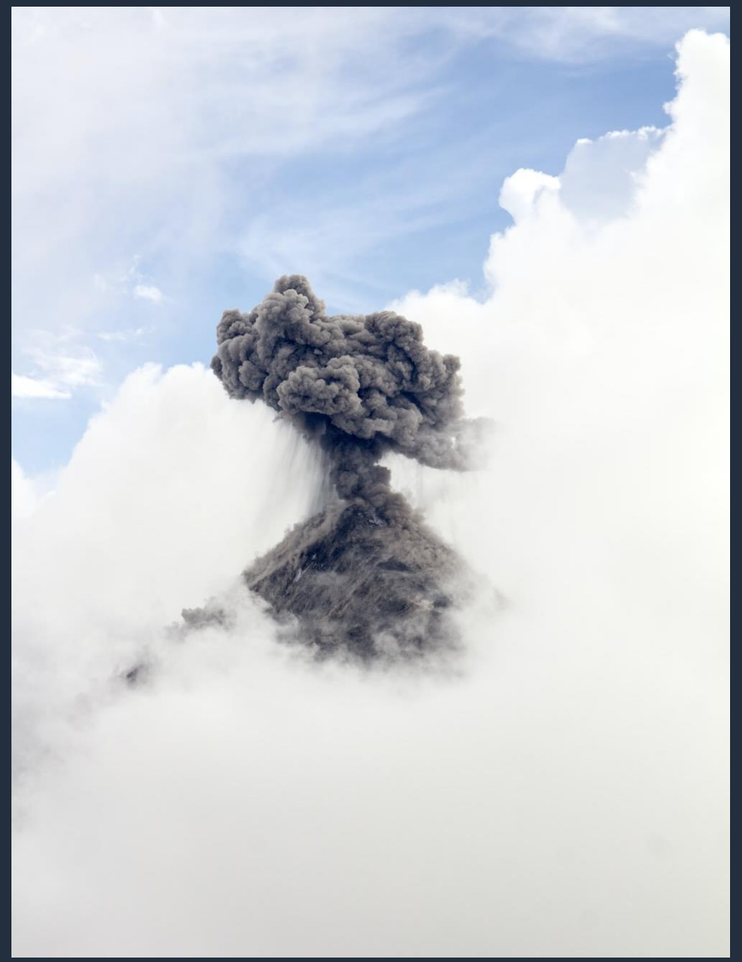


Data centers, each with redundant power, networking, and connectivity, housed in separate facilities

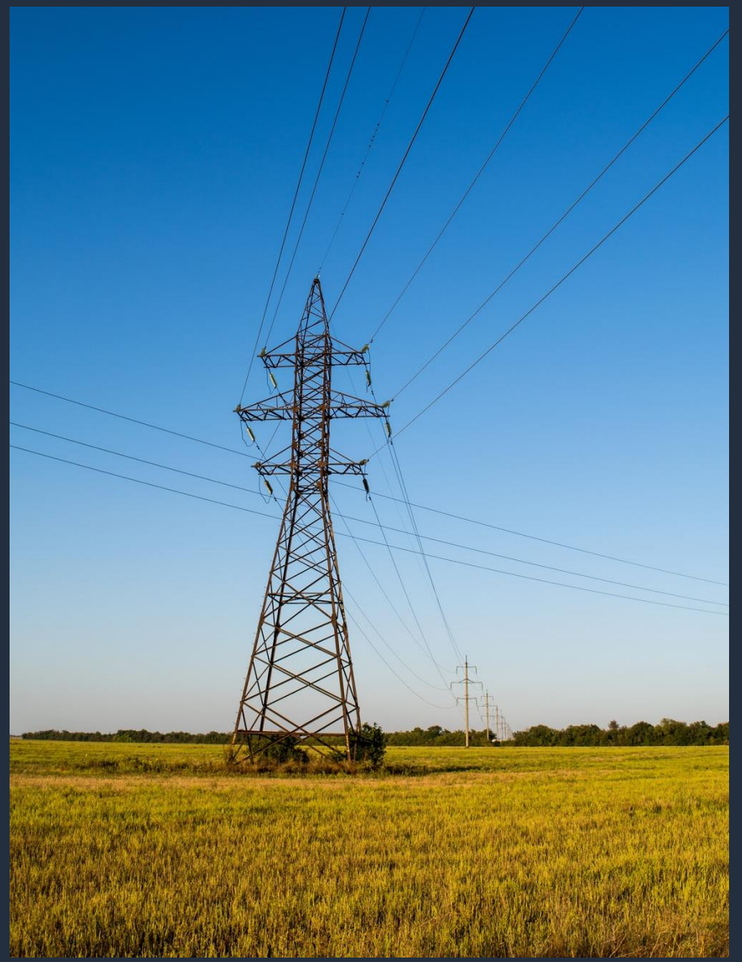
aws

Categories of Disaster

Natural Disaster



Technical Failure



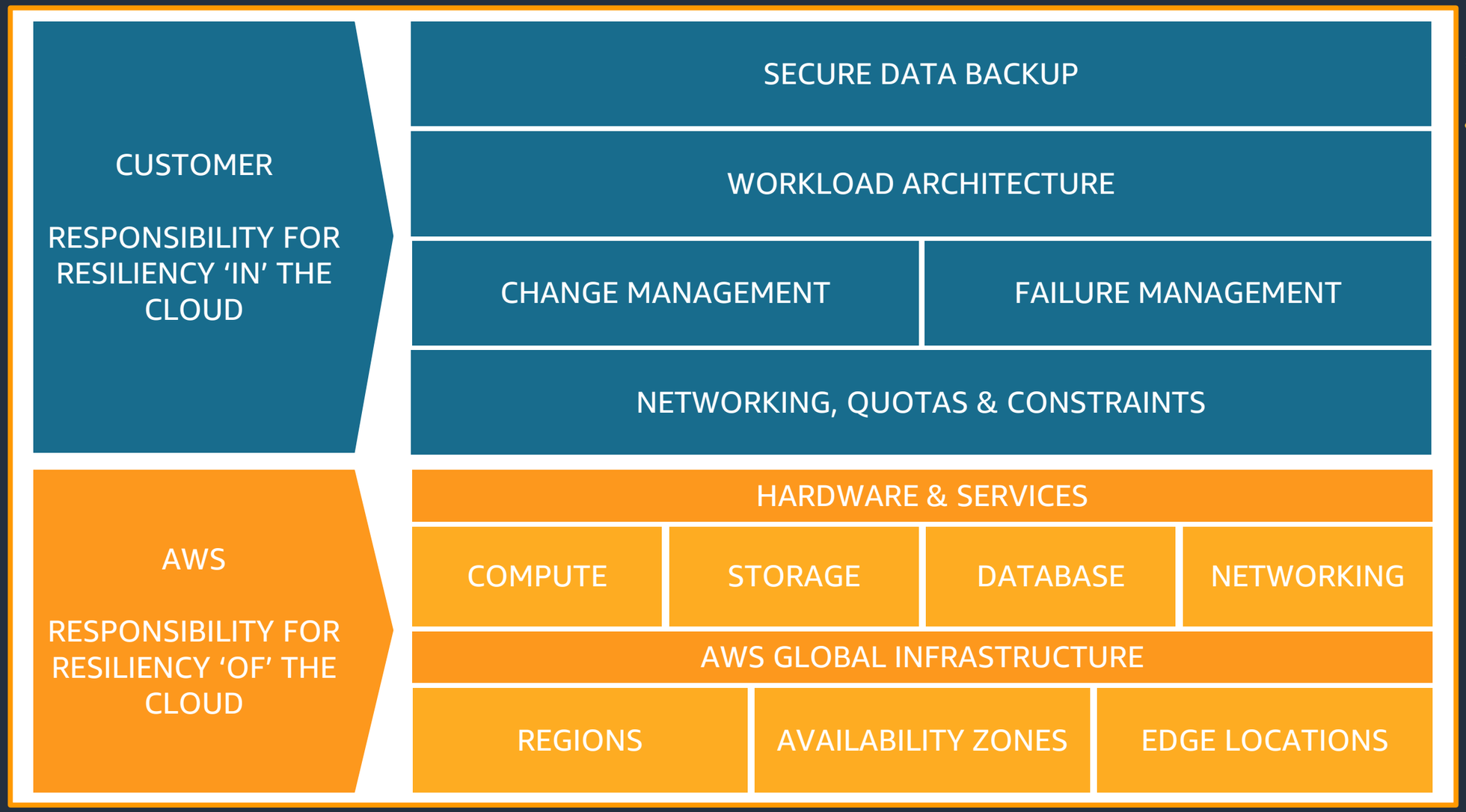
Human Actions

aws

Shared responsibility model for resiliency

AWS and customer responsibilities

Shared responsibility model for resiliency



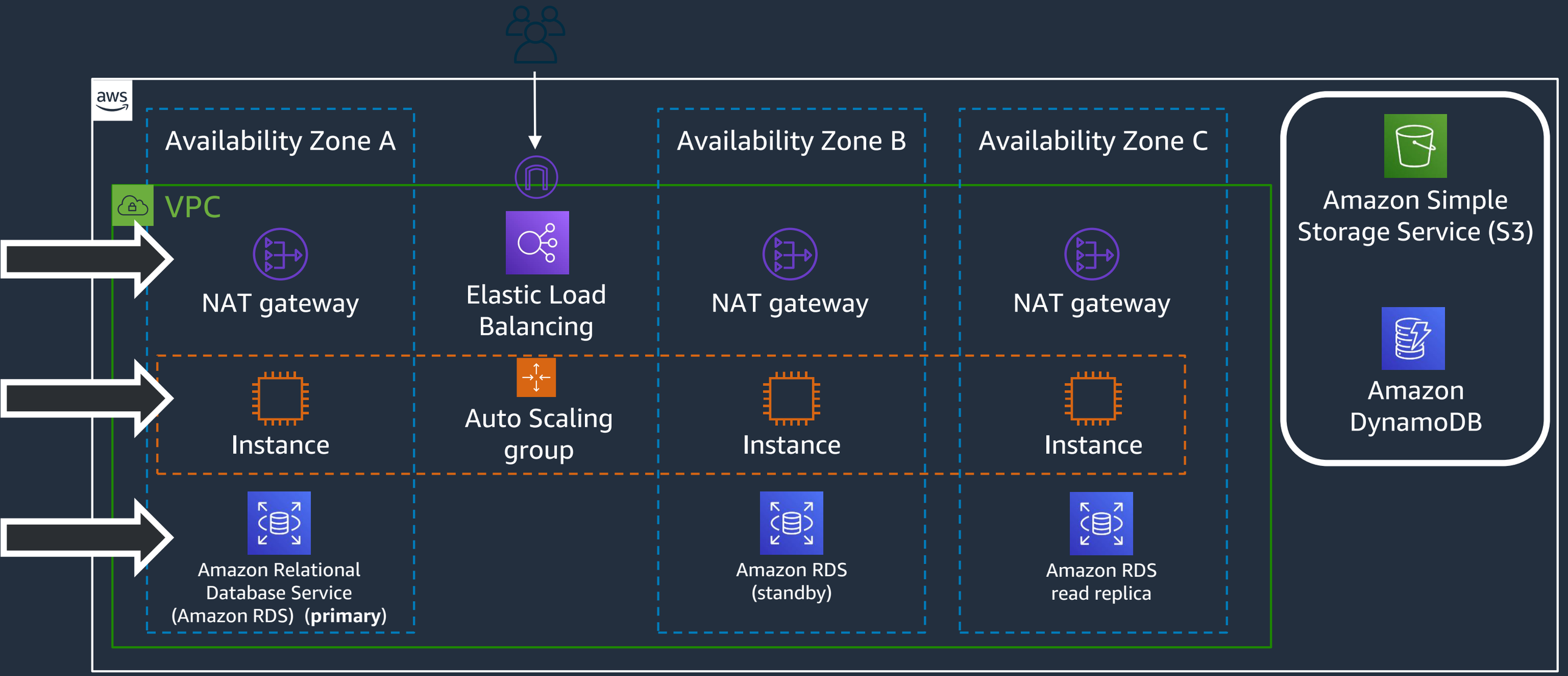
Reliability Pillar
AWS Well-Architected

http://bit.ly/reliability-pillar

High availability is not disaster recovery

aws

Multi-AZ for high availability (HA)

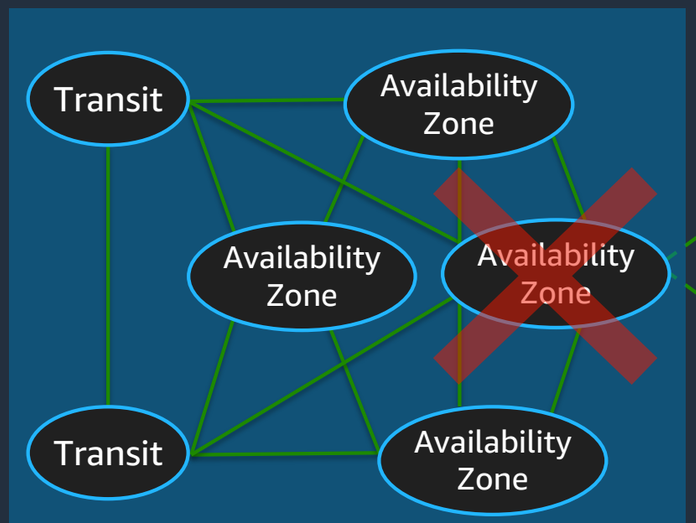


aws

Disaster event scope: Availability Zone

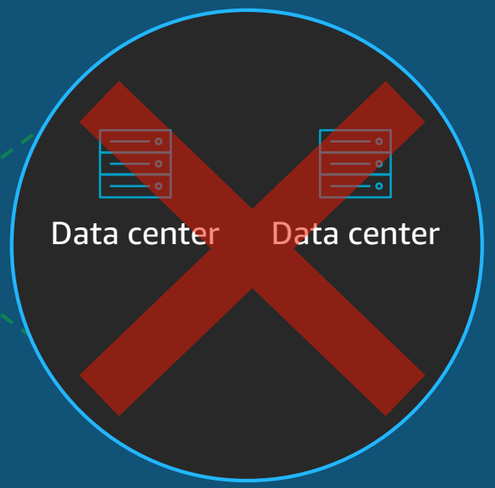
Multi-AZ DR

AWS Region
Multiple Availability Zones

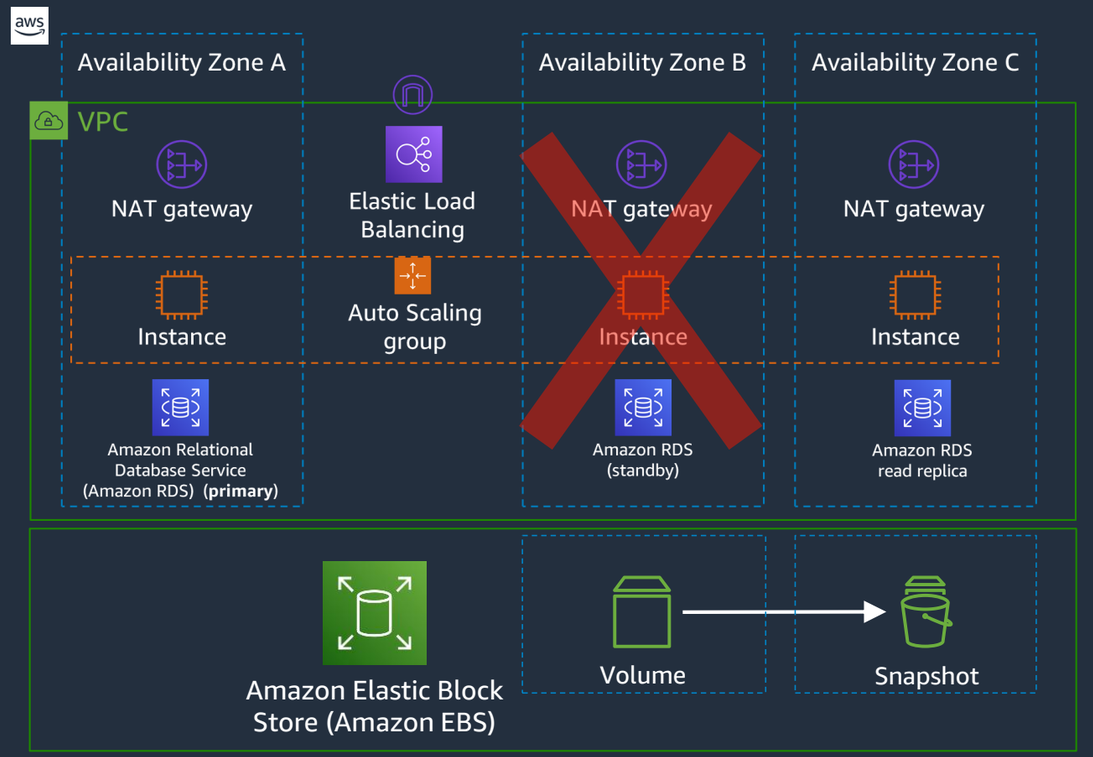


A **Region** is a physical location in the world

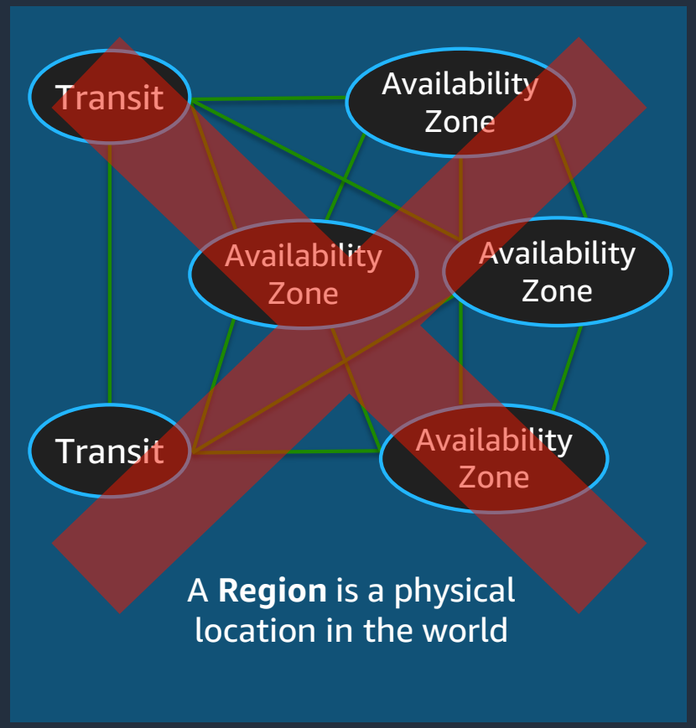
Availability Zone
One or more data centers



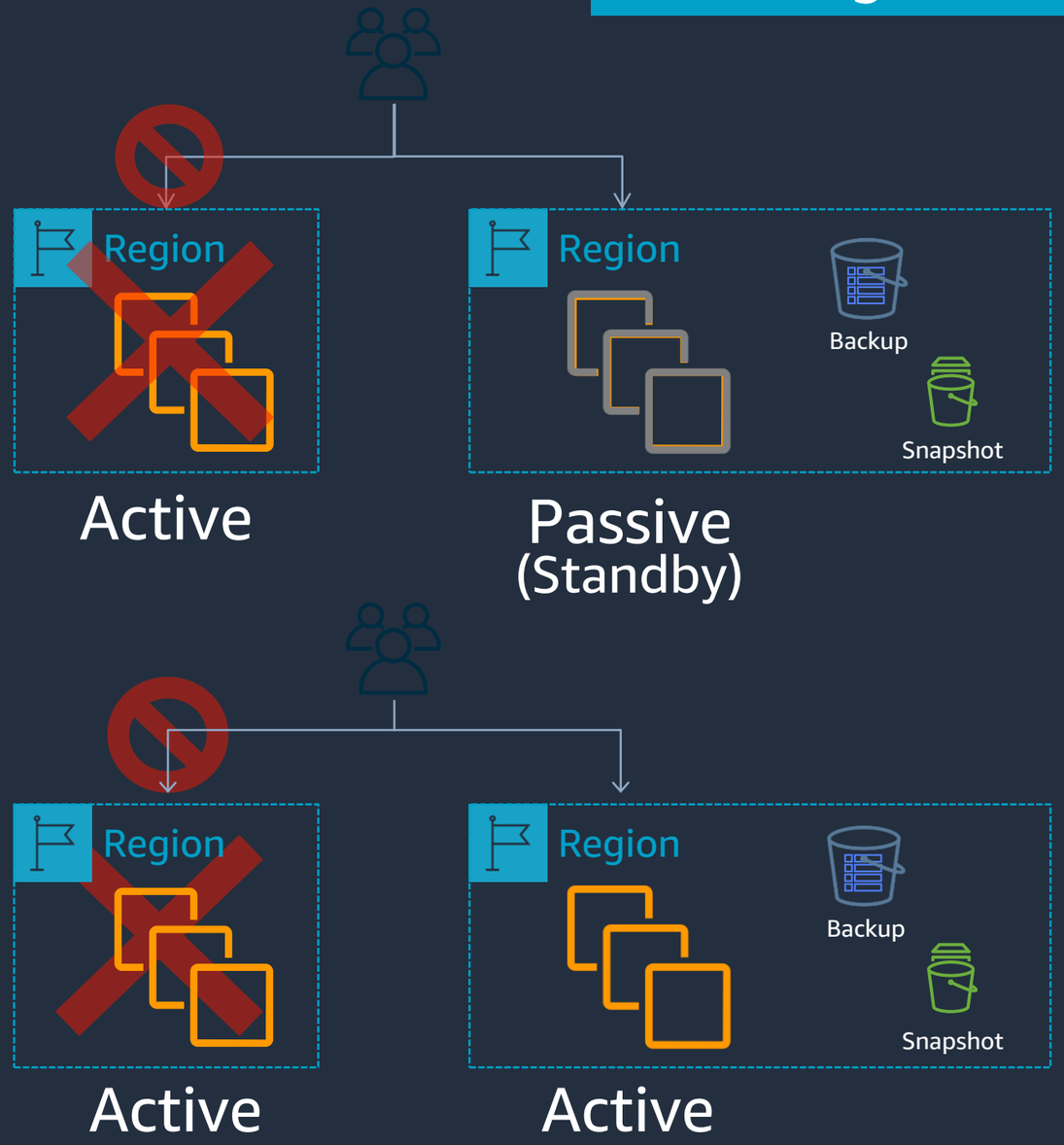
Data centers, each with redundant power, networking, and connectivity, housed in separate facilities



Disaster event scope: AWS Region



Multi-Region DR



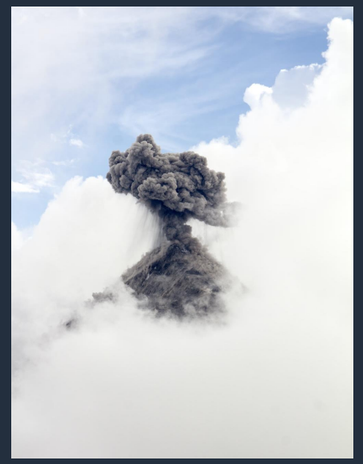
aws

Business continuity plan (BCP)

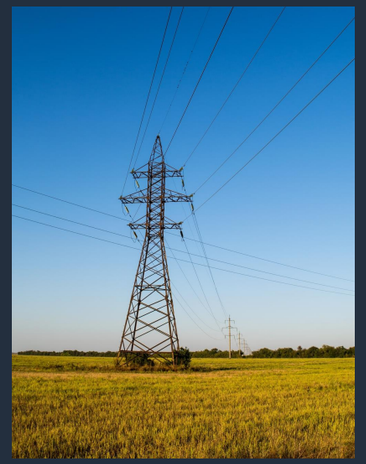
Business Continuity Plan

1. Business Impact Analysis
2. Risk Assessment
3. Business Continuity Plan
4. Disaster recovery plan

Natural Disaster



Technical Failure



Human Actions

aws

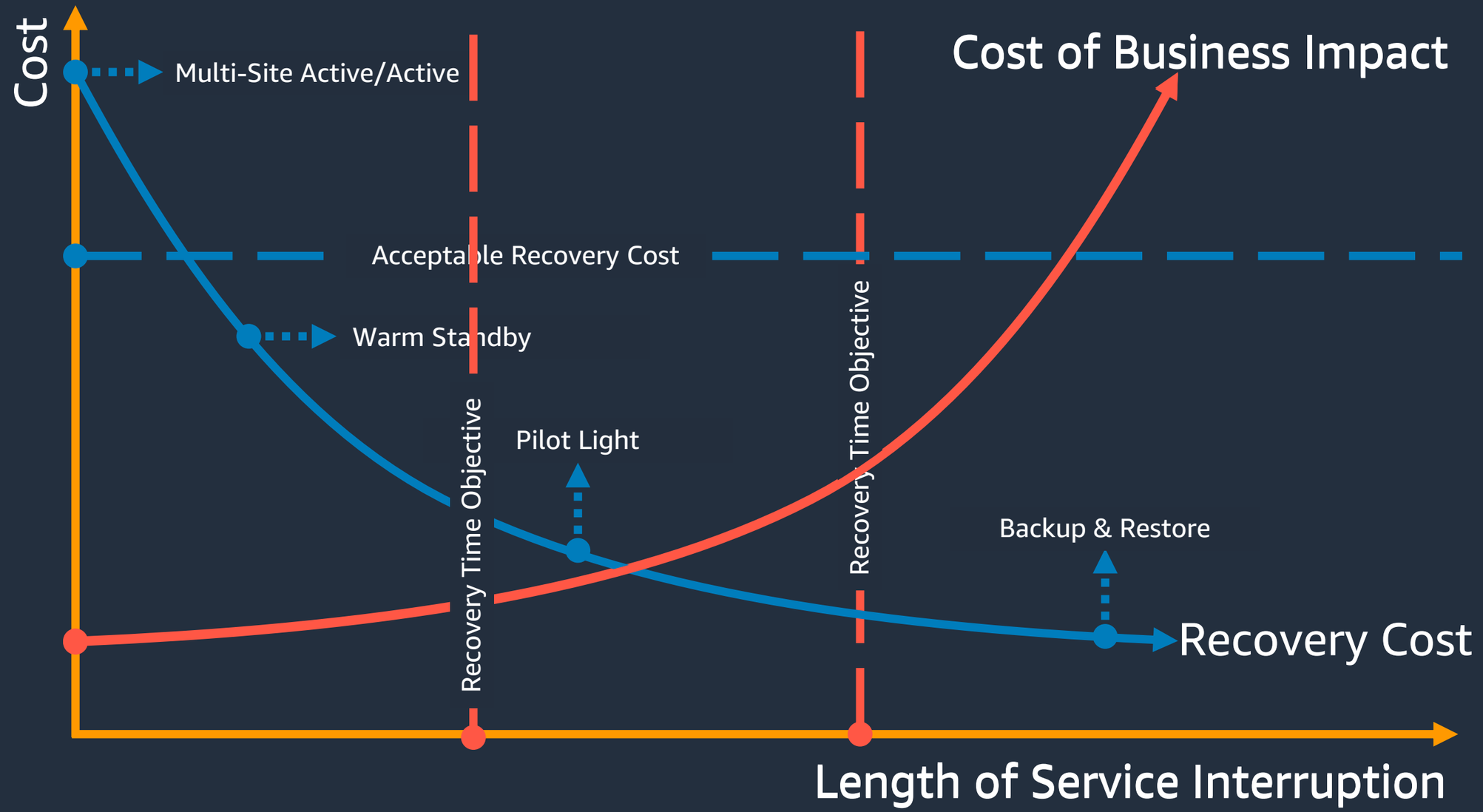
Recovery Objectives

How much data can you afford to recreate or lose?

How quickly must you recover? What is the cost of downtime?

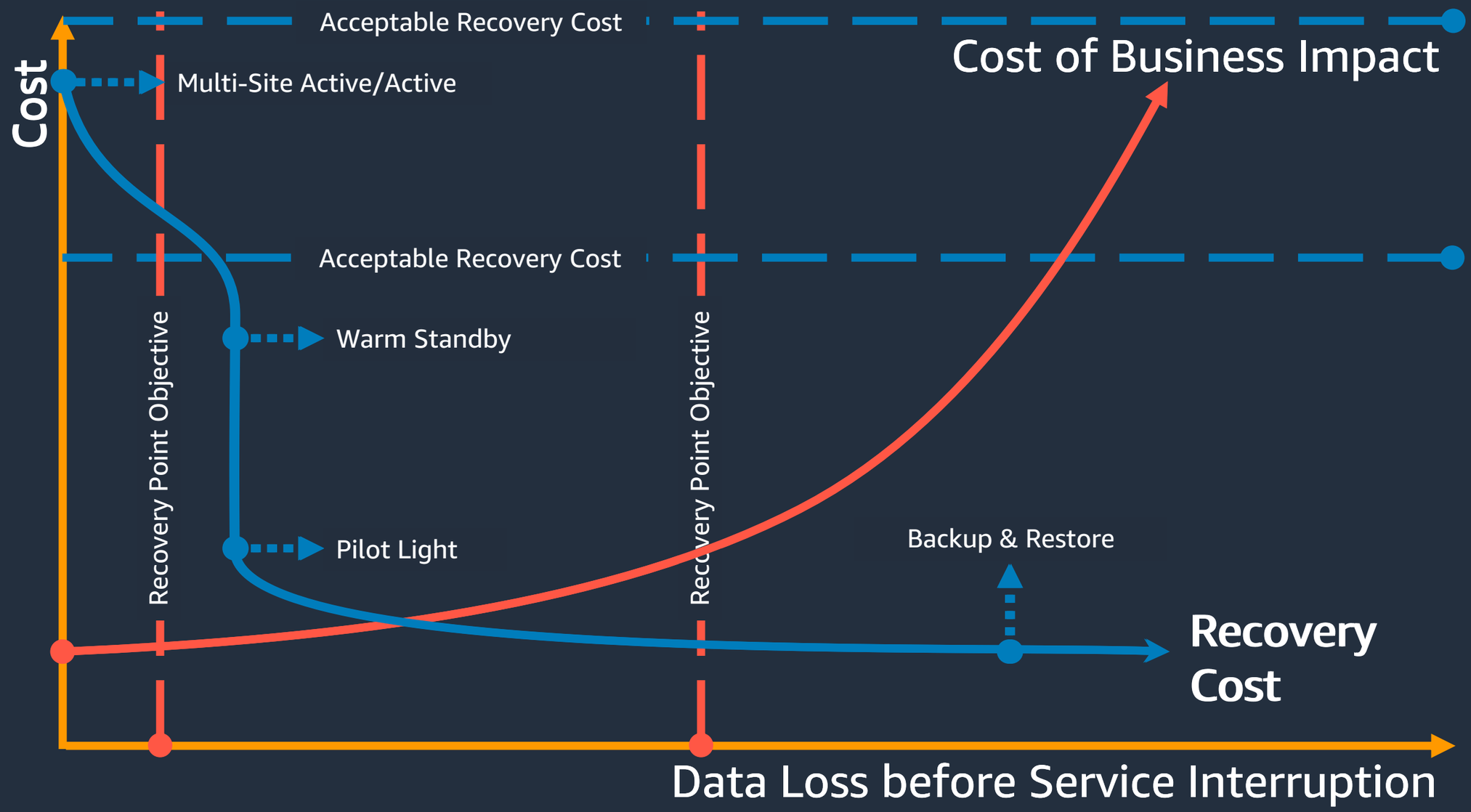
aws

Recovery Time Objective (RTO)



aws

Recovery Point Objective (RPO)



aws

Disaster recovery is different in the cloud

aws

Disaster recovery is different in the cloud

Disaster recover strategies evolve with technology

Single AWS Region
- Risk of disruption or loss of one datacenter
- Implement a highly available workload
- Don’t forget backups!

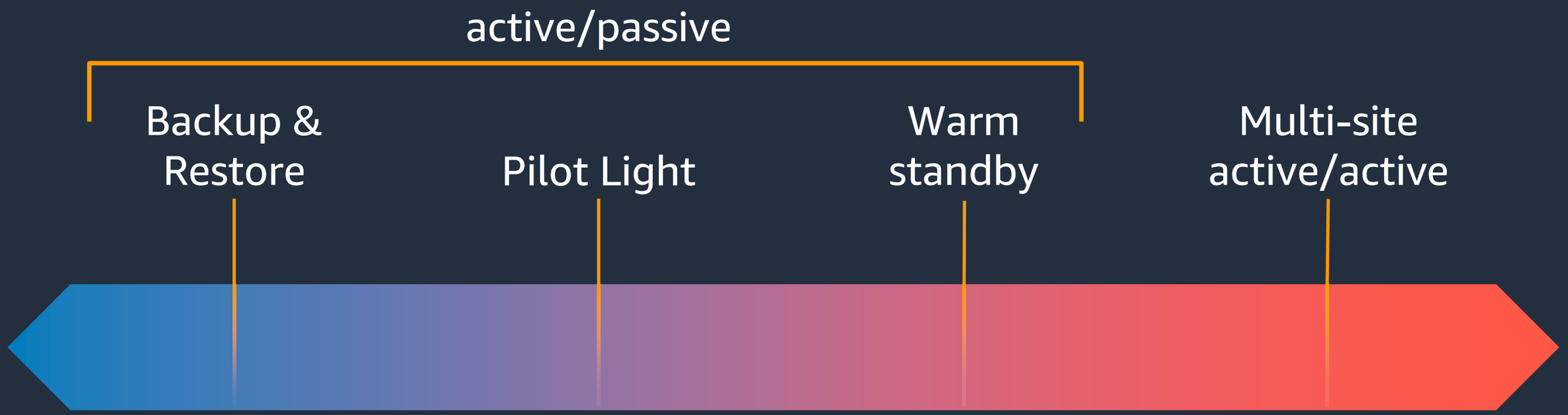
Multiple AWS Regions
- Risk of disruption or loss of multiple datacenters
- Implement cross-region availability
- Don’t forget backups!

aws

Disaster recovery options in the cloud

Strategies and implementation on AWS

Strategies for disaster recovery



RPO / RTO: Hours

- Lower priority use cases
- Provision all AWS resources after event
- Restore backups after event
- Cost $

RPO / RTO: 10s of minutes

- Data live
- Services idle
- Provision some AWS resources and scale after event
- Cost: $$

RPO / RTO: Minutes

- Always running, but smaller
- Business critical
- Scale AWS resources after event
- Cost $$$

RPO / RTO: Real-time

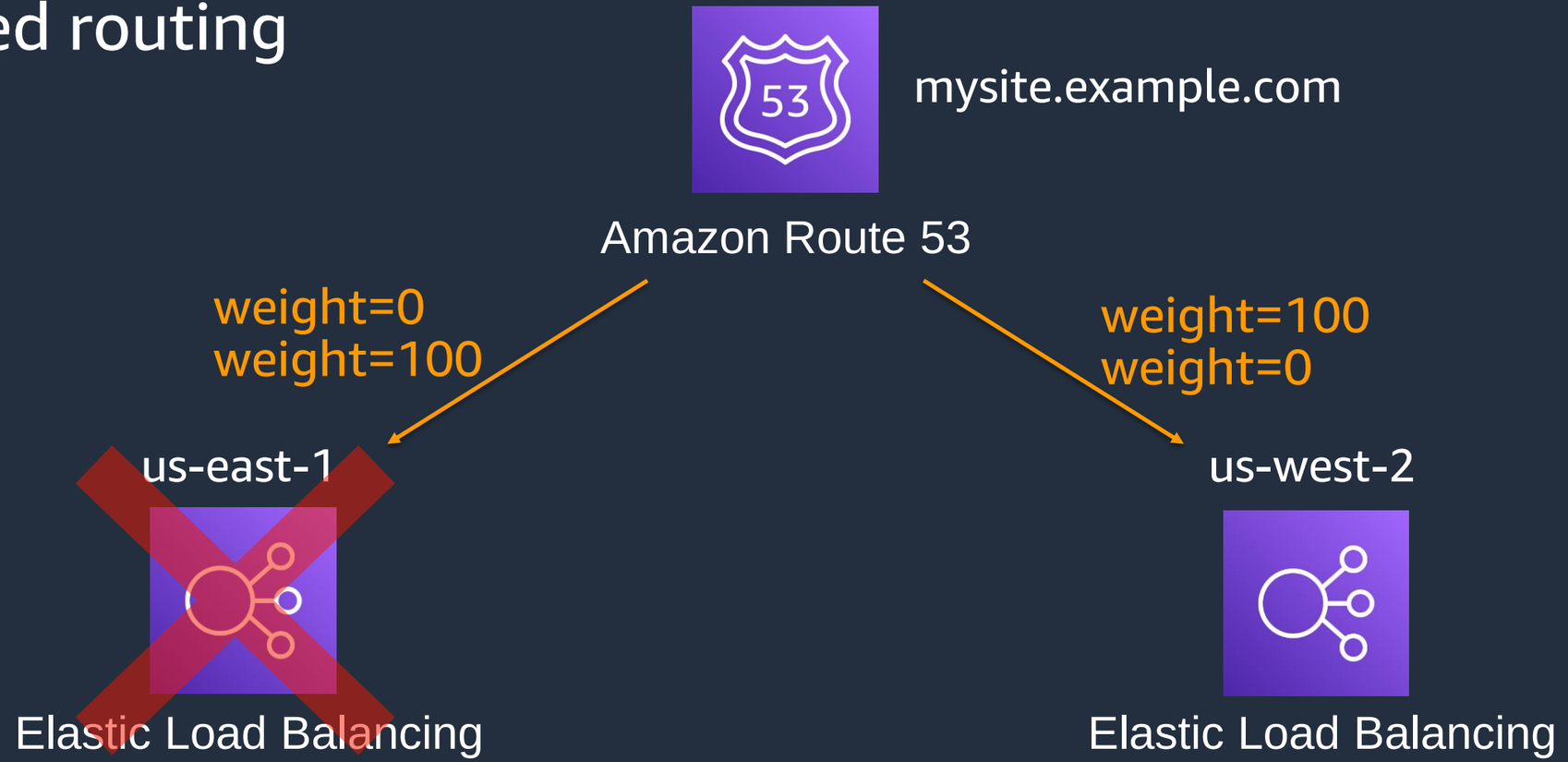
- Zero downtime
- Near zero data loss
- Mission Critical Services
- Cost $$$$

aws

Route 53 – Routing policies for active/passive

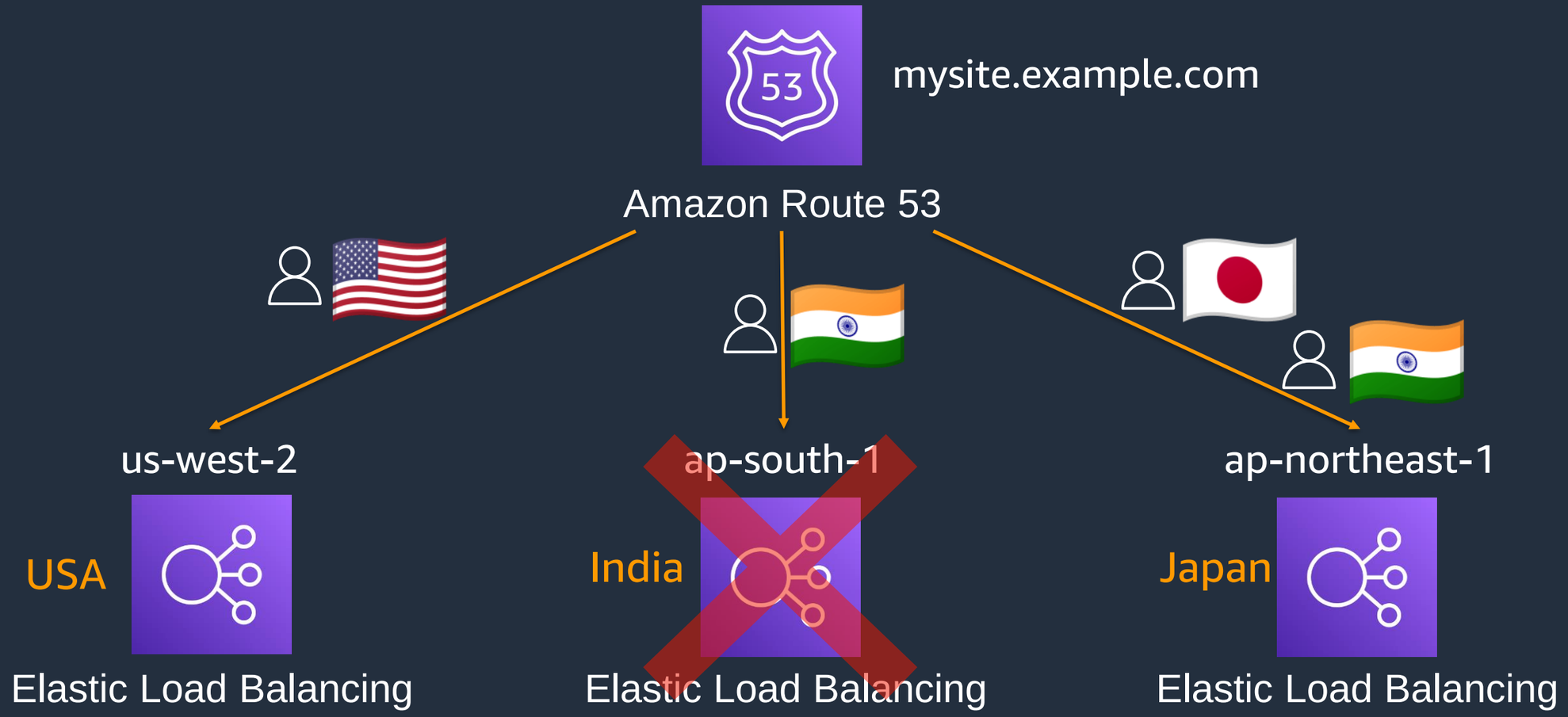
Failover routing

Weighted routing



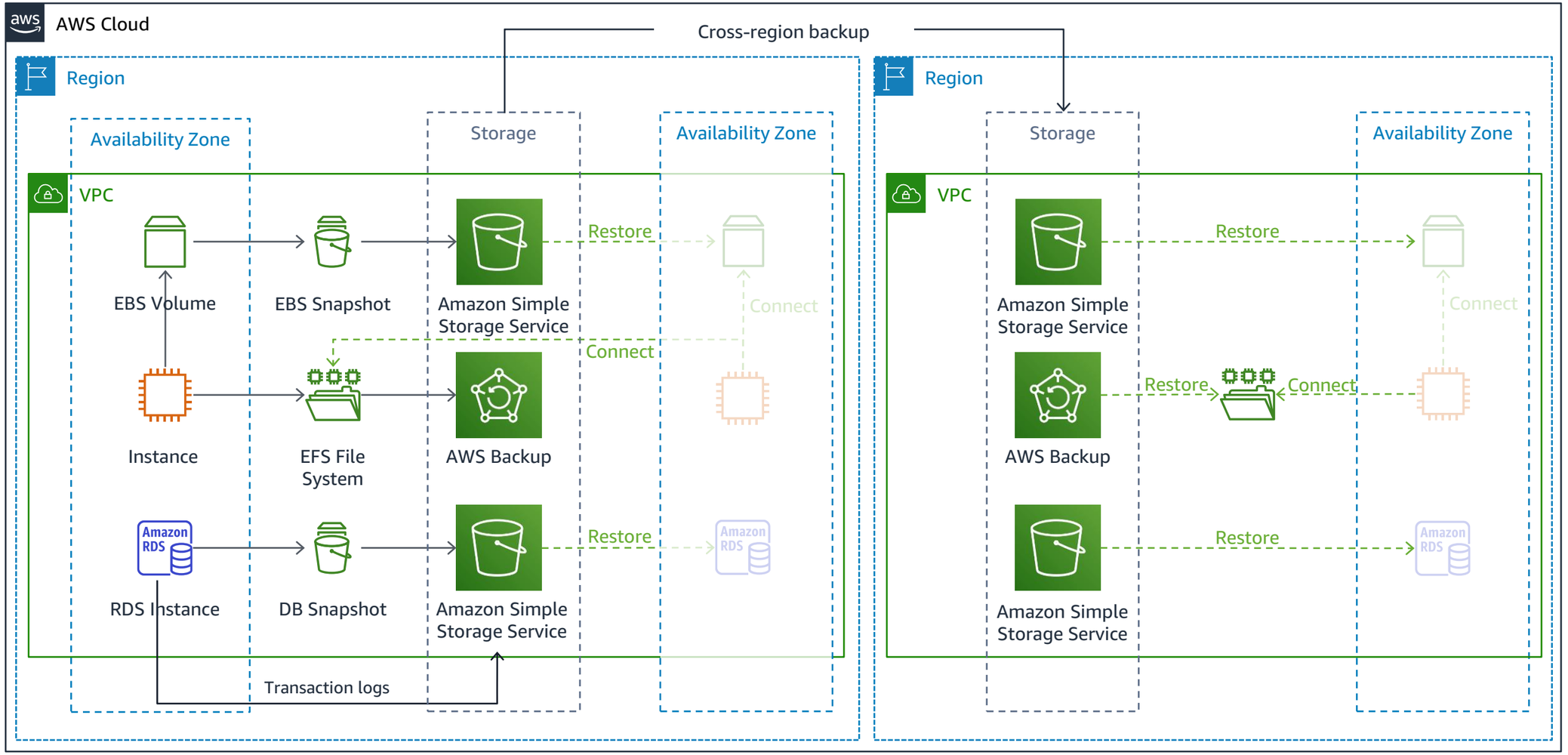
Route 53 – Routing policies for active/active

Geolocation routing

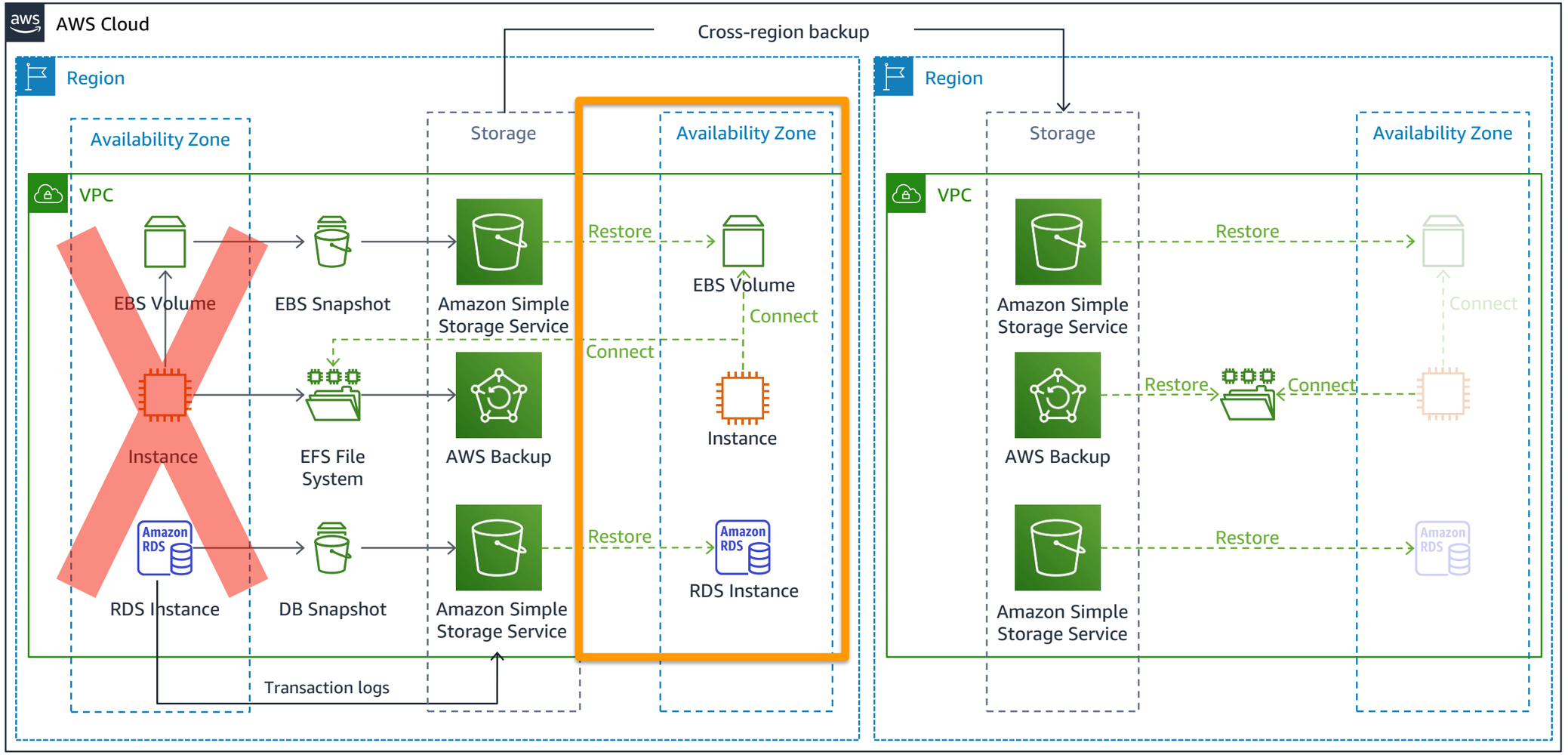


aws

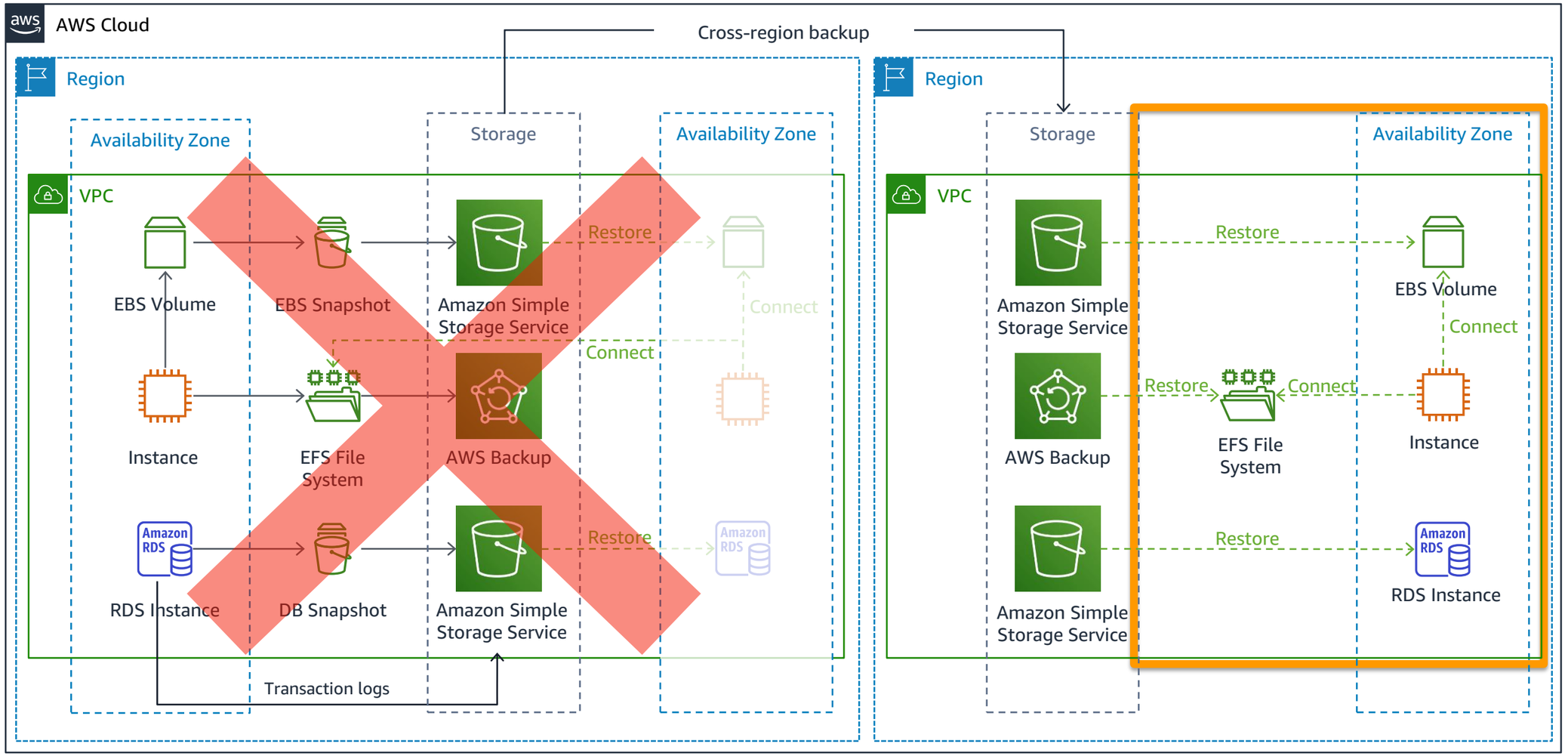
Strategy: Backup and restore



Failover: Backup and restore to AZ



Failover: Backup and restore to region



AWS Backup

Centralize compliance, automate backup, work across services

AWS Backup

Amazon EBS

Amazon EFS

Amazon RDS

Amazon DynamoDB

Amazon EC2

AWS Storage Gateway

Amazon FSx

Centralized view

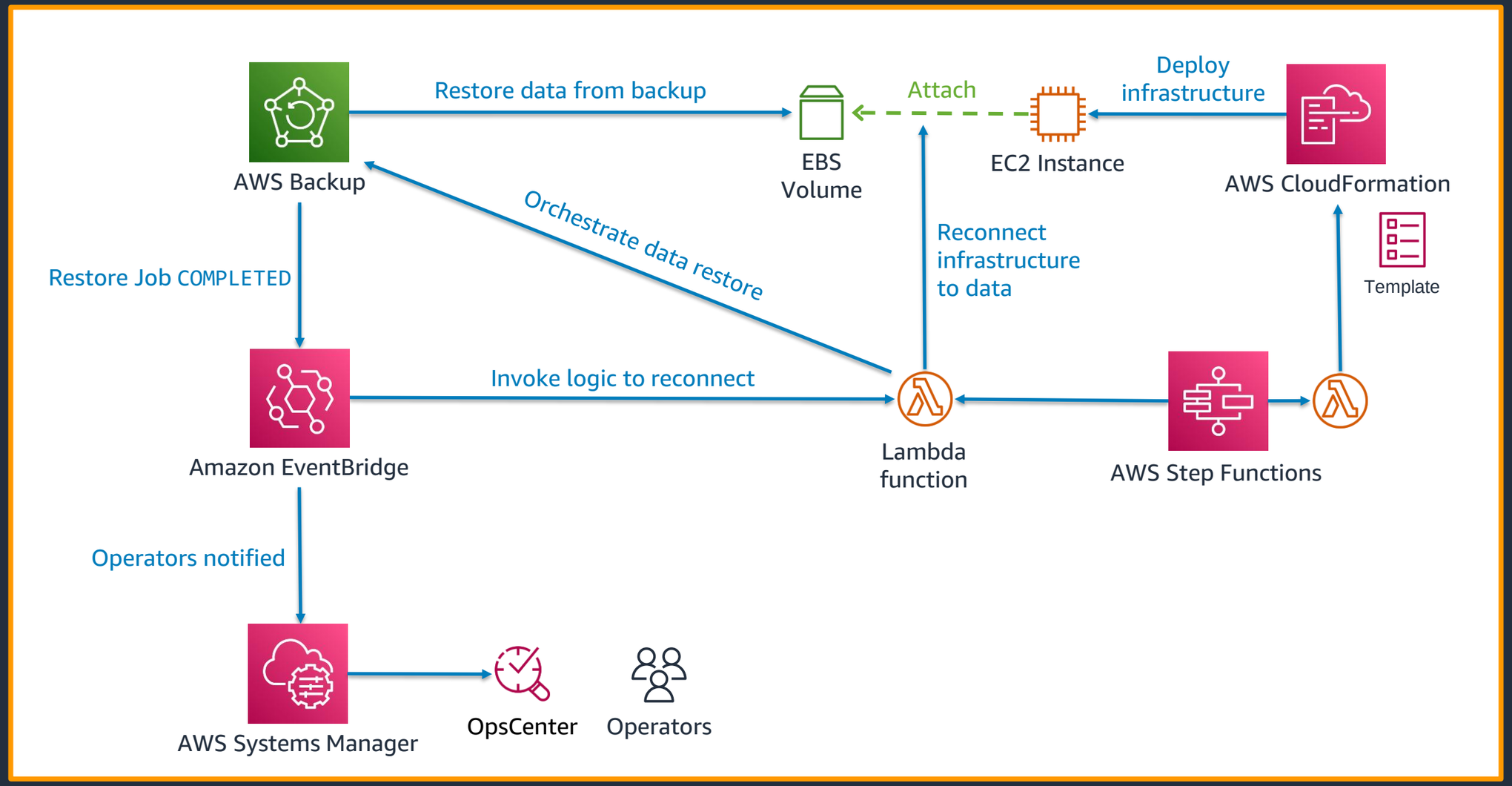
Configure, schedule, monitor backups

Restore

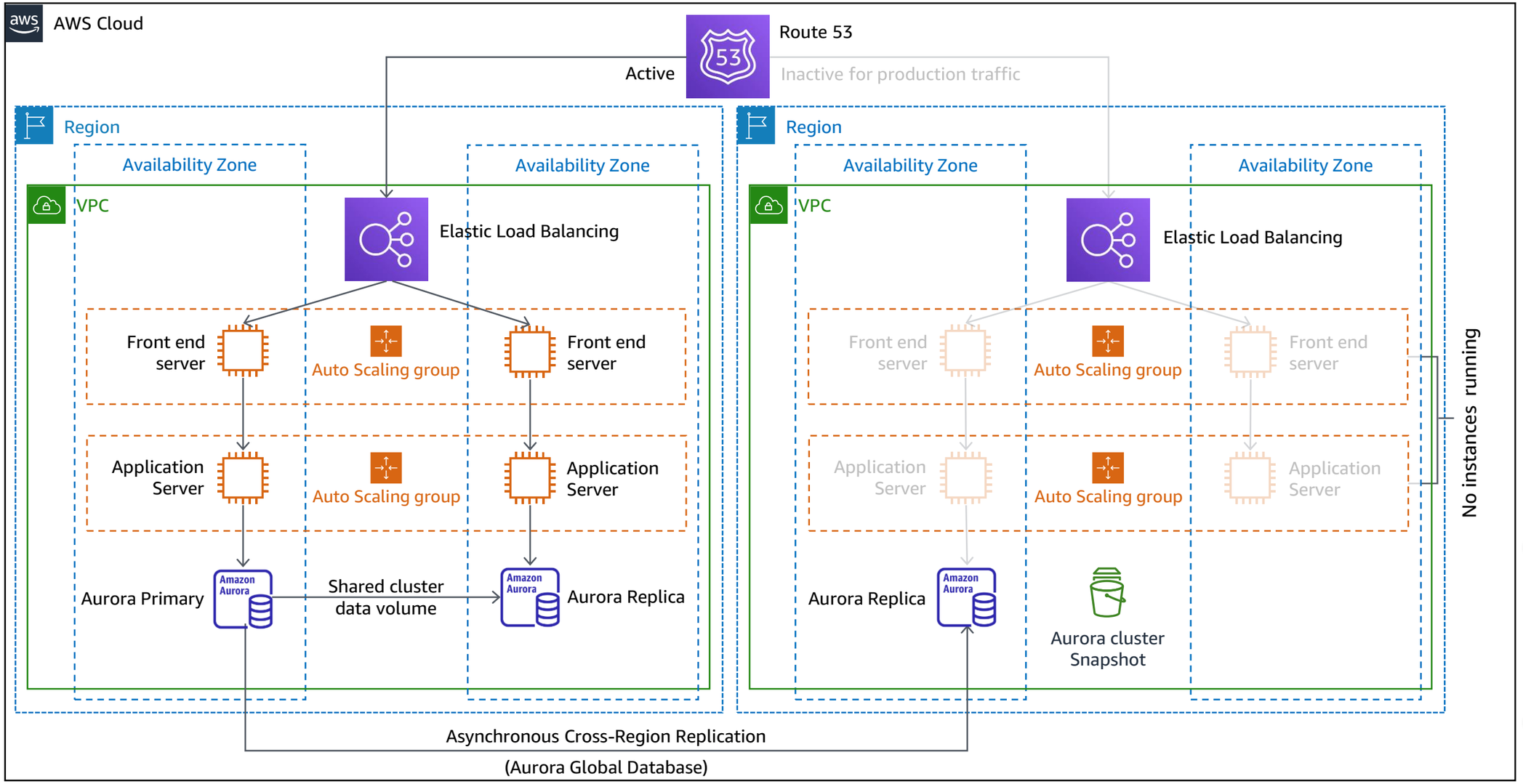
Can copy cross-region

aws

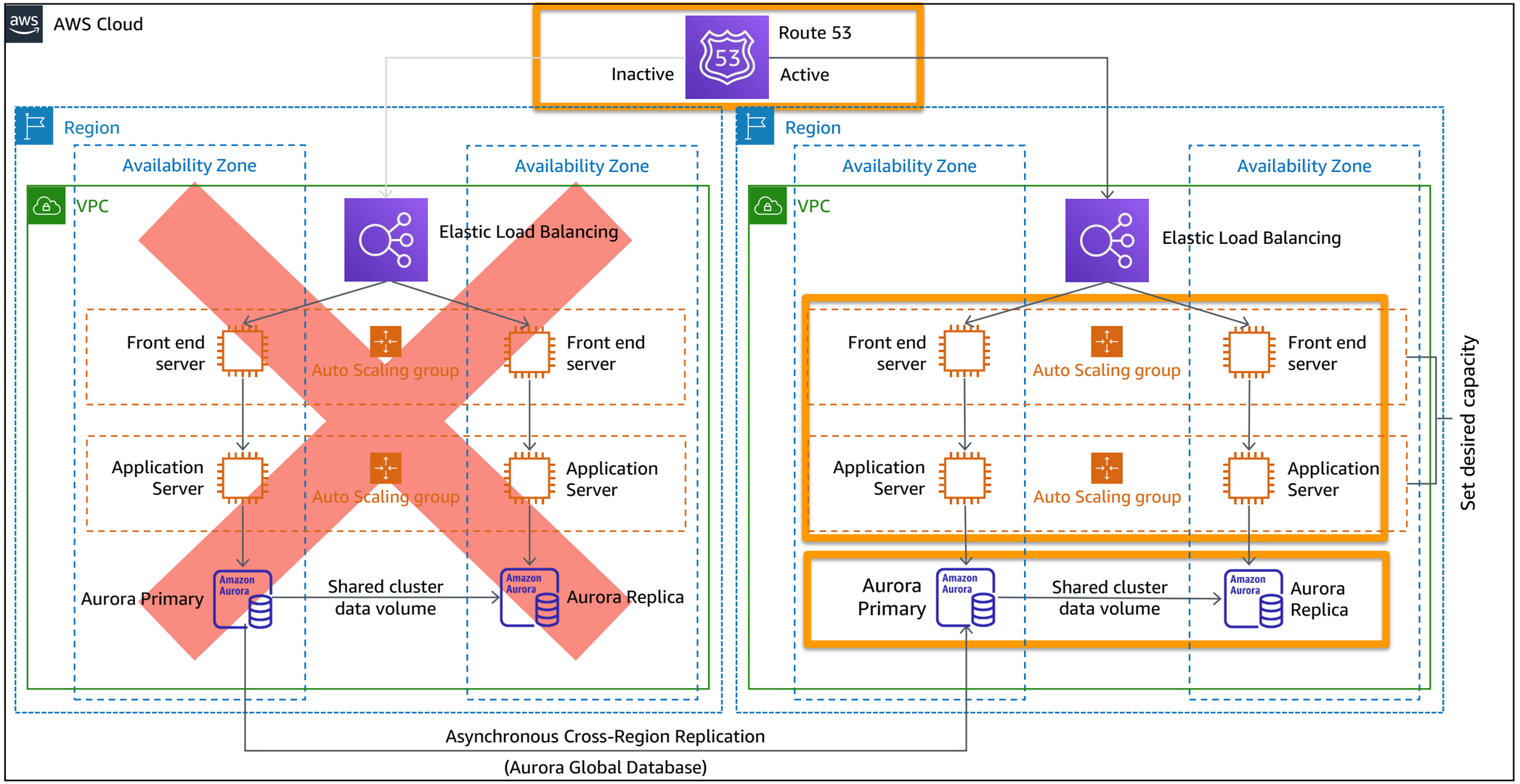
Restore and reconnect the infrastructure



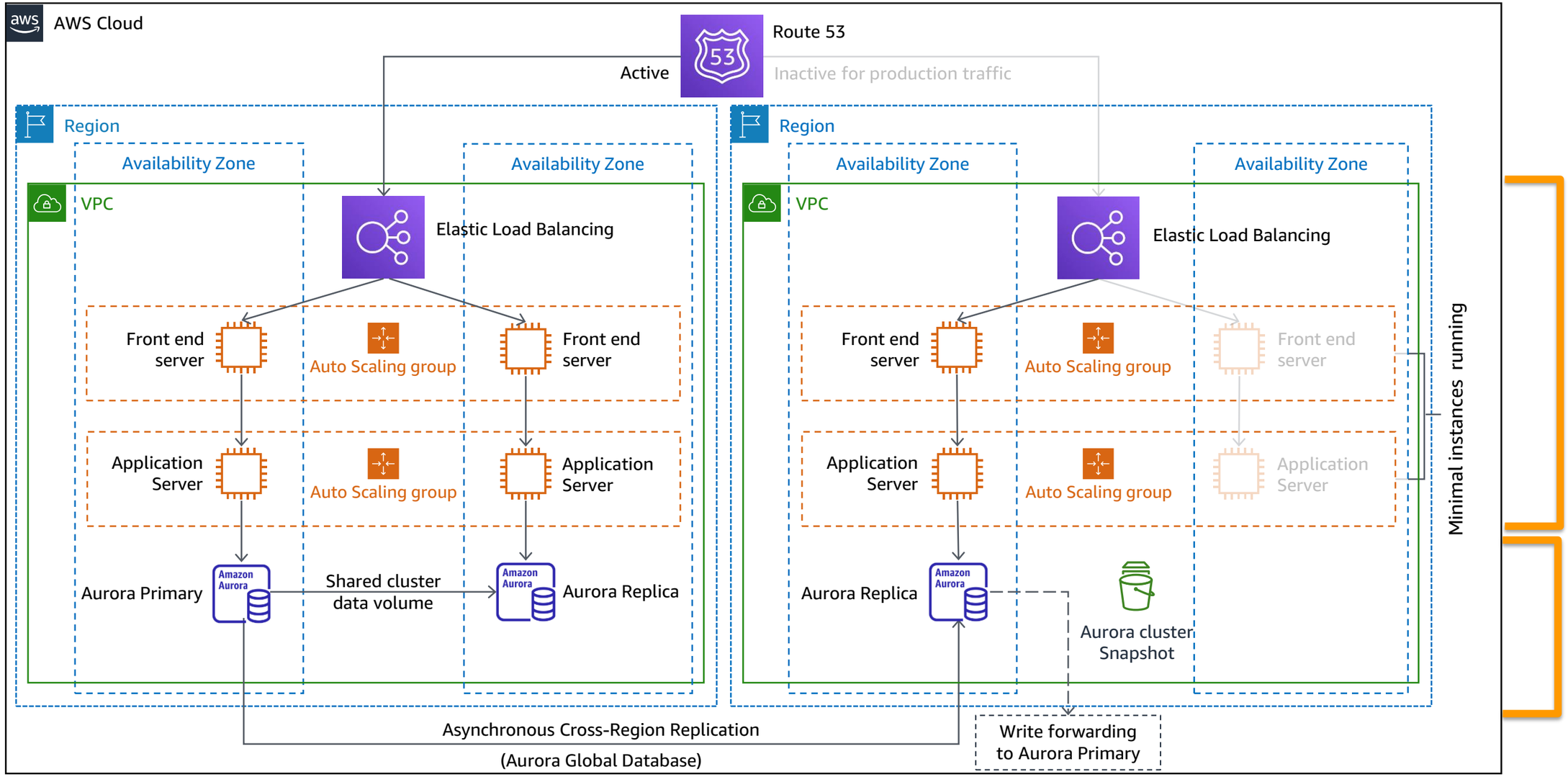
Strategy: Pilot light



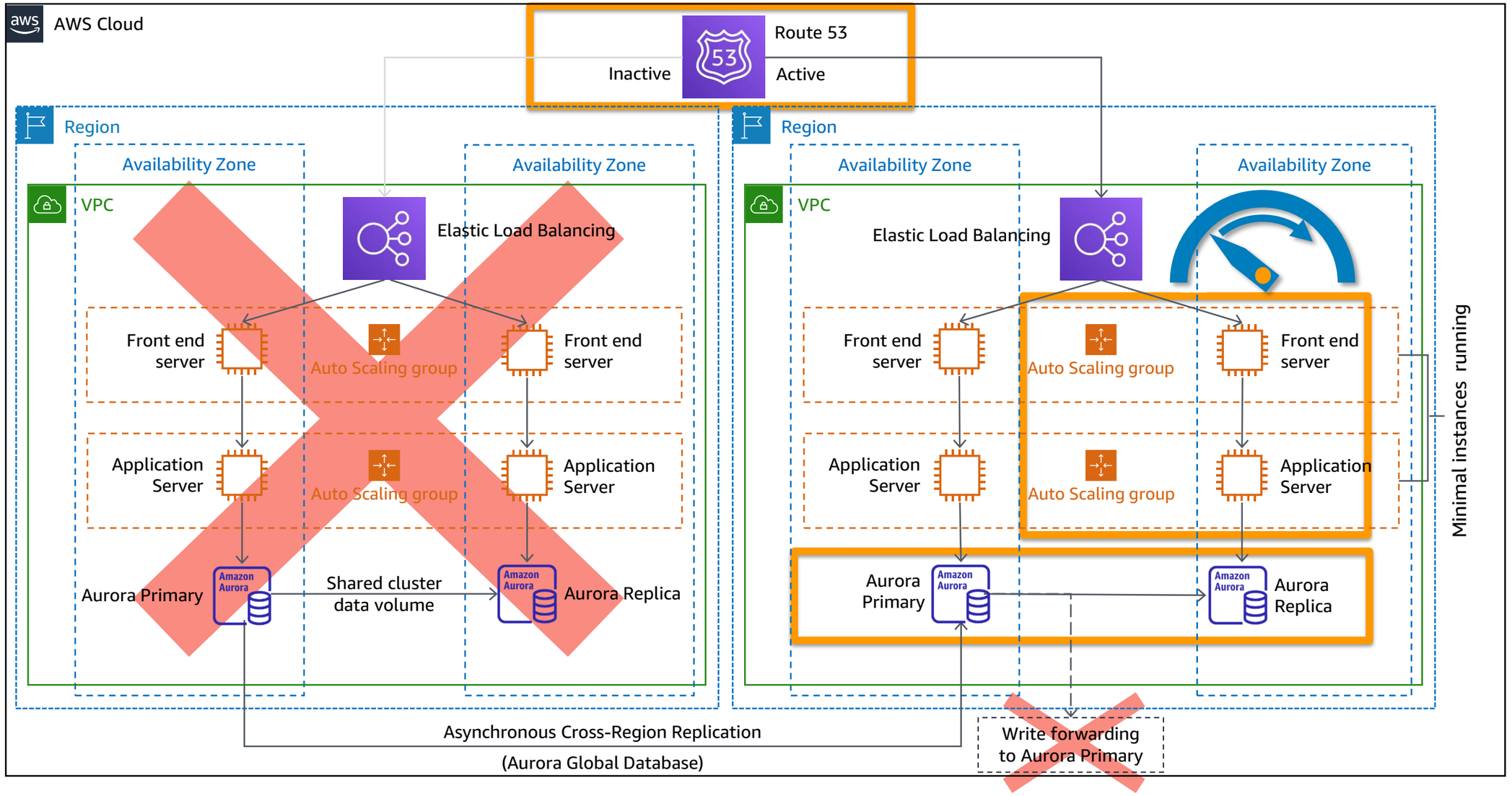
Failover: Pilot light



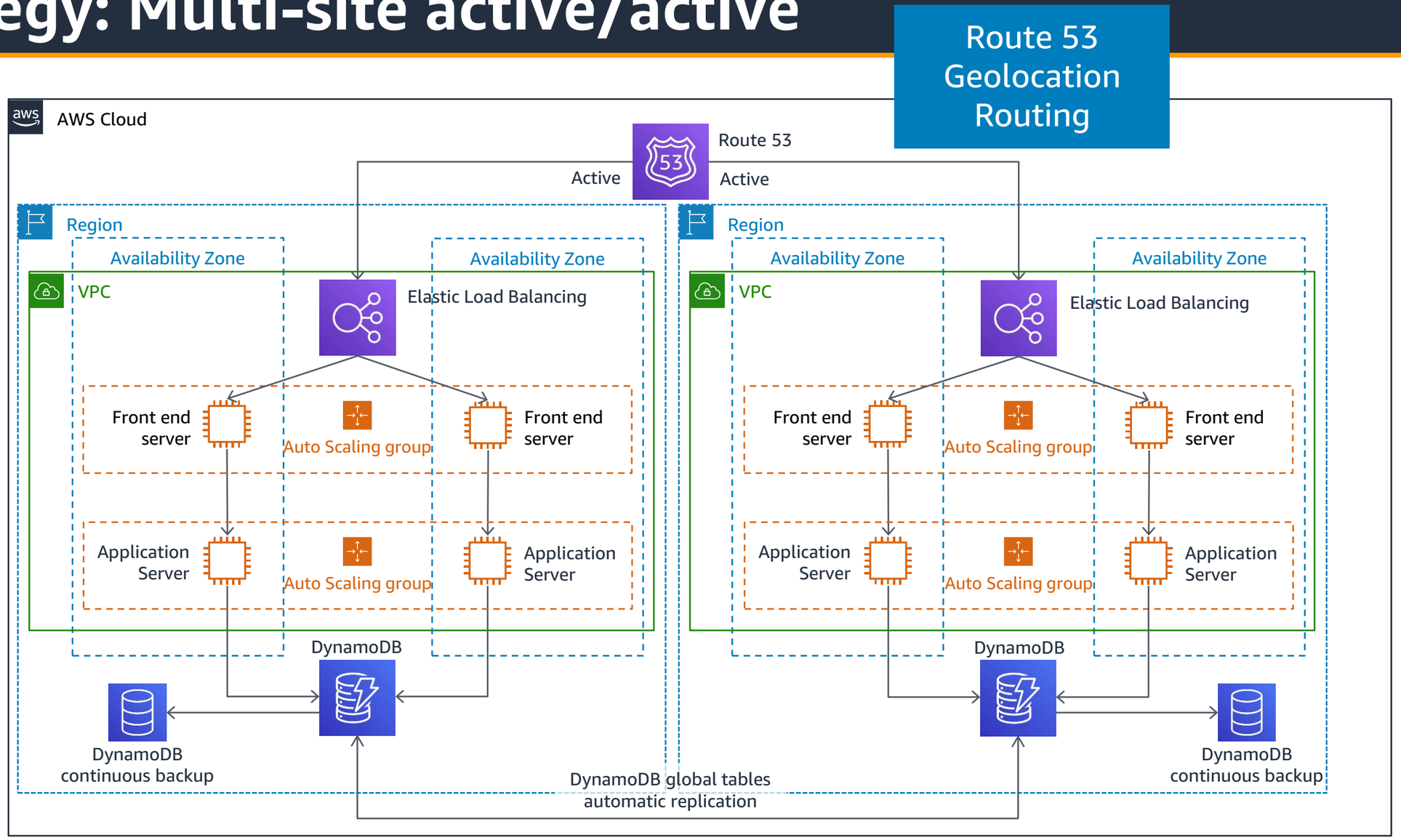
Strategy: Warm standby



Failover: Warm standby



Strategy: Multi-site active/active



Using AZ as your DR site

Data residency requirements

Availability Zones are

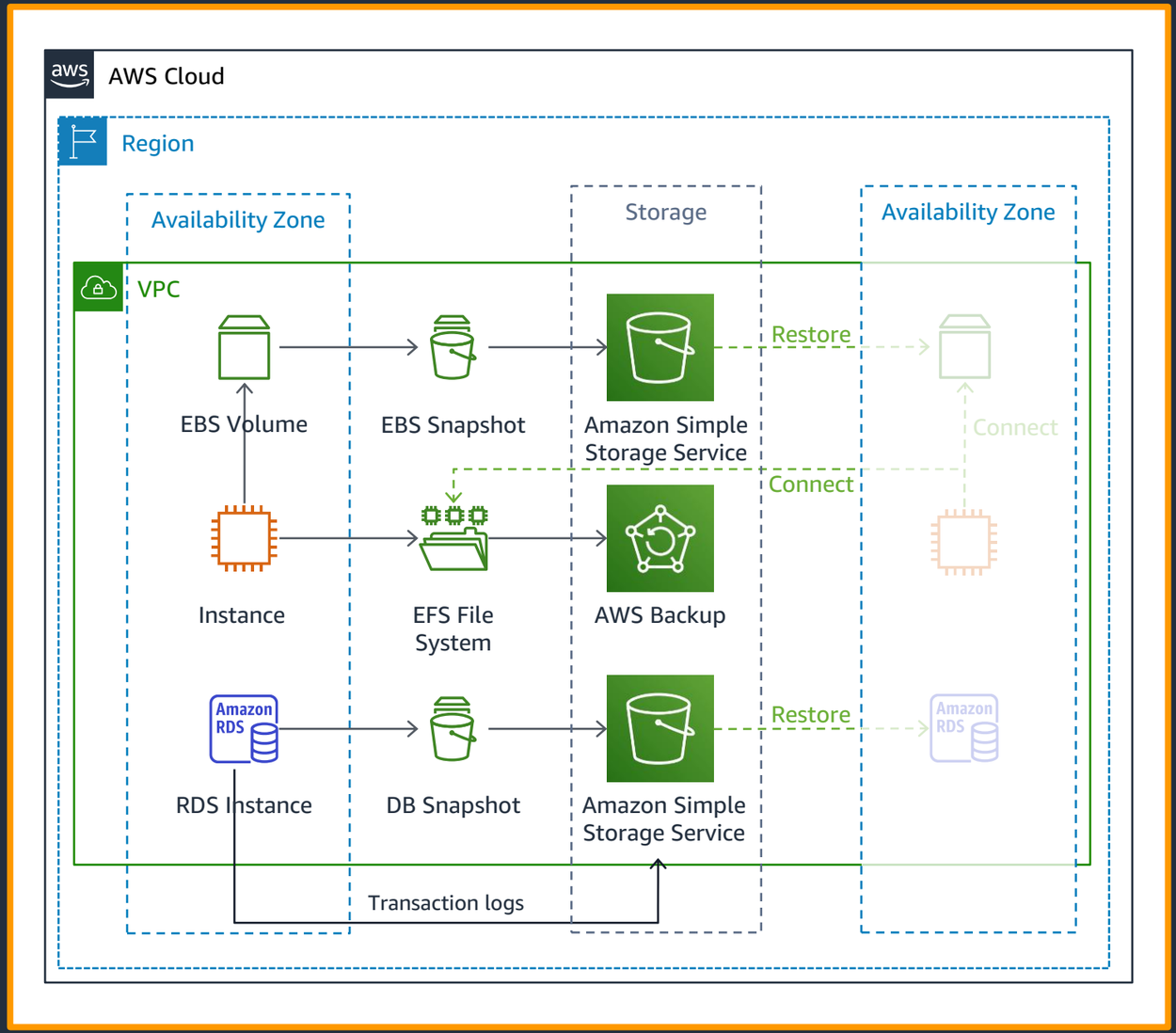
- Separated about 30 mi / 50 km
- Should have no shared fate scenario

utility power disruption
utility water disruption
fiber isolation
floods
lightning strikes
tornadoes
earthquakes

→ independent substations

UPS

onsite generators

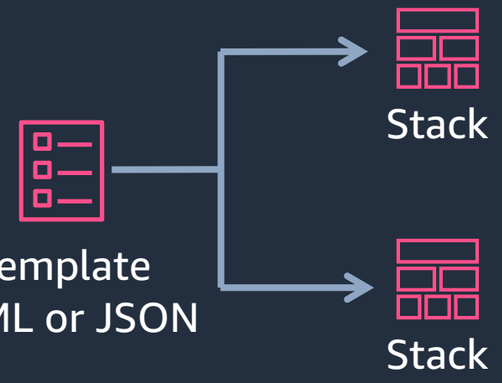


AWS tools to build infrastructure

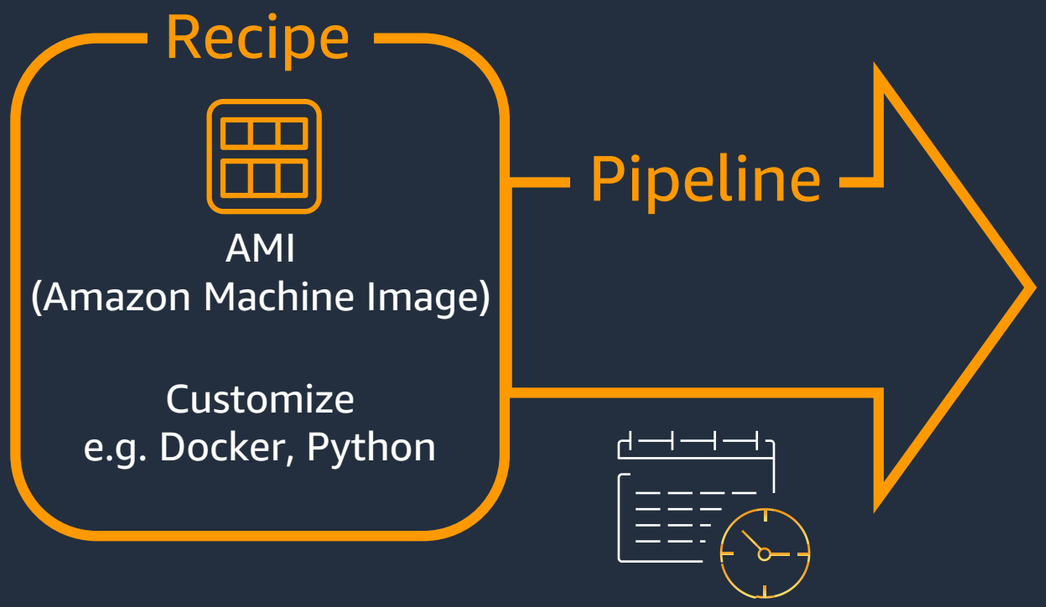
AWS CloudFormation

Infrastructure as code (IaC)

Consistently across accounts and regions



Amazon EC2 Image Builder



aws

AWS as DR site for an on-premises workload

WITH CLOUDENDURE

ASSESSMENT

Map Environment
Identify servers and networking, define recovery objectives

SETUP

Install Agents
Replication begins into lightweight Staging Area

Configure Blueprint
Instance type, subnet, security groups, etc

Blueprint corrections needed?

Test Target Servers
Perform infrastructure and application acceptance tests

OPERATION

Maintain DR Readiness
Ongoing monitoring, periodic tests, add servers

RECOVERY

Failover
Launch servers on AWS and redirect users

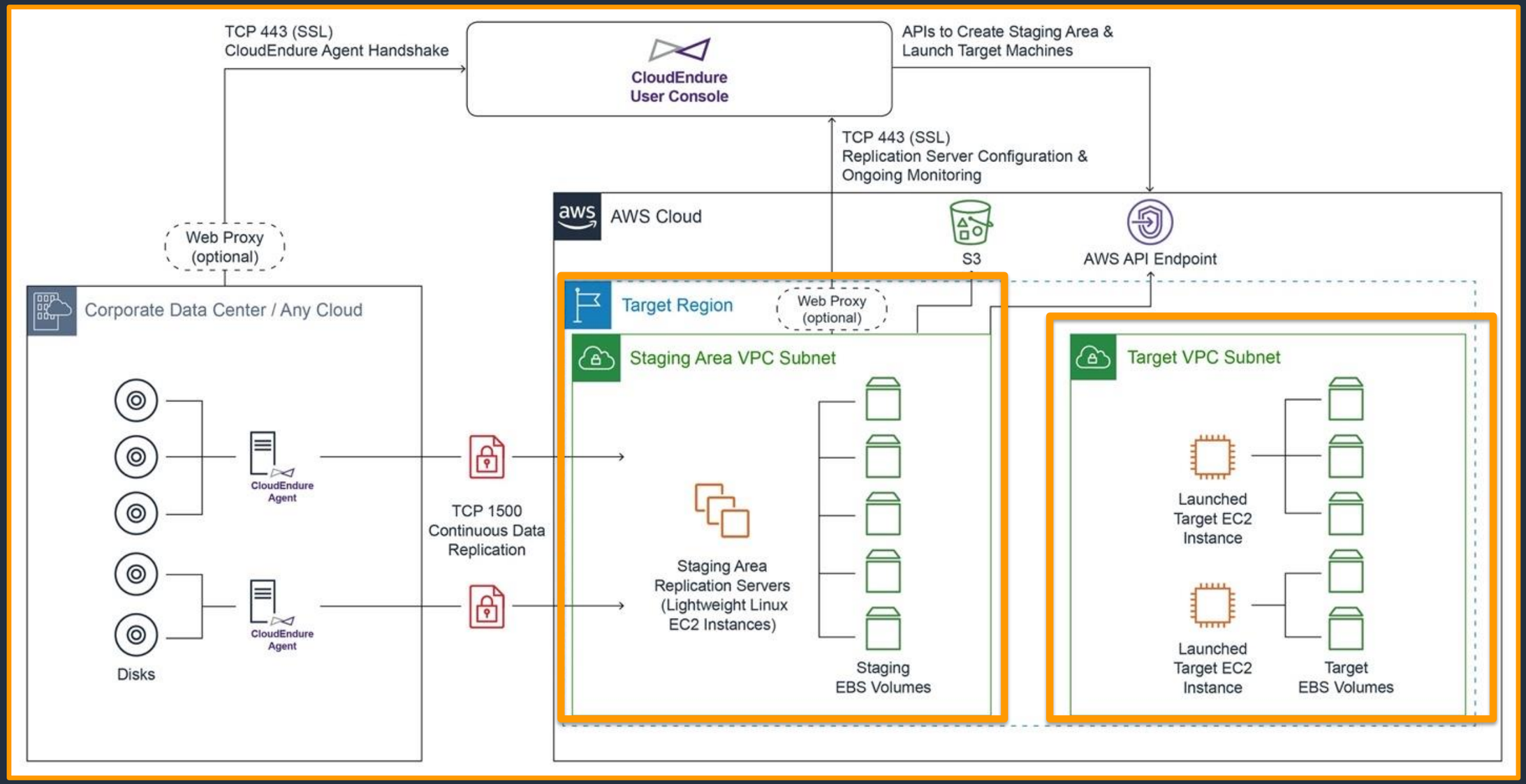
Failback
Reverse replication and redirect users

RPO: Sub-Seconds
RTO: Minutes

CloudEndure
An AWS Company

aws

CloudEndure is a Pilot Light strategy

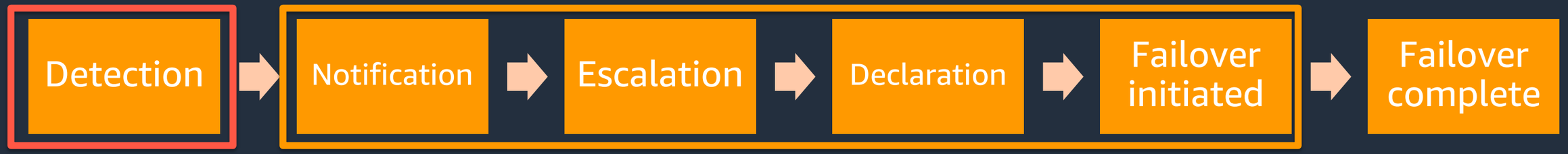


Detection

Quickly recognize and recover from disaster events

Components of RTO

Recovery Time:

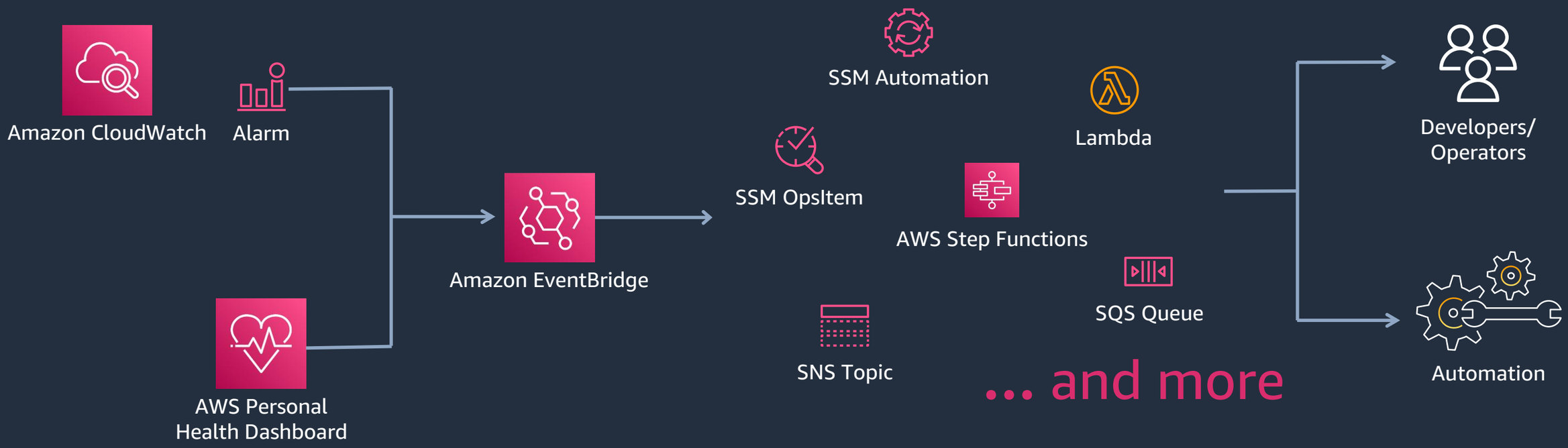


Detect problem by human: NEVER

Failover initiated by human: OK
Failover initiated automatically: OK

aws

AWS Patterns for detecting a disaster




```
{
  "source": ["aws.health"],
  "detail-type": ["AWS Health Event"],
  "detail": {
    "service": ["S3"],
    "eventTypeCategory": ["issue"],
    "eventTypeCode": ["AWS_S3_INCREASED_GET_API_ERROR_RATES", "AWS_S3_INCREASED_PUT_API_ERROR_RATES"]
  }
}
```

Metrics for health: Detect the user experience

Bad: Liveness (ping)

Better: Service call failure (synthetics)

Best: KPI (Key Performance Indicator)

- eCommerce: Order rate drop
- Social Media: Engagement drop

Anomaly detection

aws

Testing disaster recovery

Ensure that RTO and RPO are met


An untested DR strategy…
…is no DR strategy

Poll

Have you been in a situation where a DR Plan was in place but was not invoked due to lack of confidence in the ability to execute?

- Not applicable
- Yes
- No

aws

Summary

1. Business requirements
2. Technical strategies
3. Detection and testing

http://bit.ly/DR_AWS

AWS Well-Architected: Reliability pillar

Learn

Measure

Improve

REL 13. How do you plan for disaster recovery (DR)? Info

Having backups and redundant workload components in place is the start of your DR strategy. RTO and RPO are your objectives for restoration of availability. Set these based on business needs. Implement a strategy to meet these objectives, considering locations and function of workload resources and data.

Question does not apply to this workload Info

Select from the following

- [x] Define recovery objectives for downtime and data loss Info
- [x] Use defined recovery strategies to meet the recovery objectives Info
- [x] Test disaster recovery implementation to validate the implementation Info
- [x] Manage configuration drift at the DR site or region Info
- [x] Automate recovery Info
- [ ] None of these Info

aws

Get Started with AWS Well-Architected

AWS Well-Architected Framework

Key concepts, design principles, and architectural best practices

Learn more about the framework »

AWS Well-Architected Tool

Evaluate workloads, identify high risk issues, record improvements. Available at no cost in the AWS Management Console

Access the tool »

AWS Well-Architected Partners

Team with an AWS Partner to review workloads, uncover potential high-risk issues, and design a plan to make improvements

Find an AWS WA Partner »

Well-Architected Solutions from AWS Partners

Integrated tools to help you automatically discover issues or provide insights against best practices

Explore WA Partner Solutions »

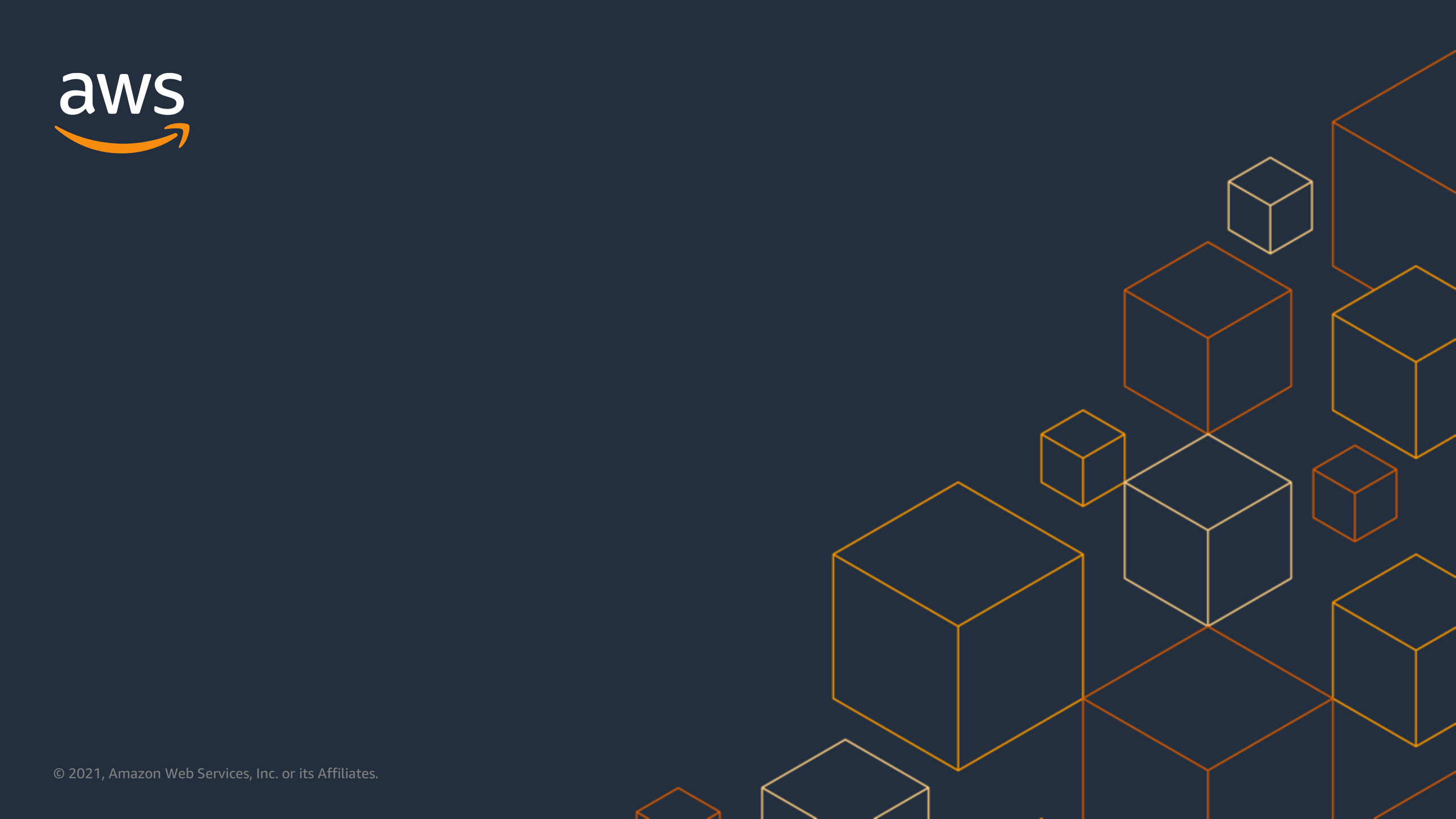
aws

Q&A

http://bit.ly/DR_AWS

Seth Eliot
Principal Reliability Solutions Architect
AWS Well-Architected

Alex Livingstone
Practice Lead Cloud Operations
AWS Enterprise Support



Resources

Q&A

Disaster Recovery of Workloads on AWS: Recovery in the Cloud

http://bit.ly/DR_AWS

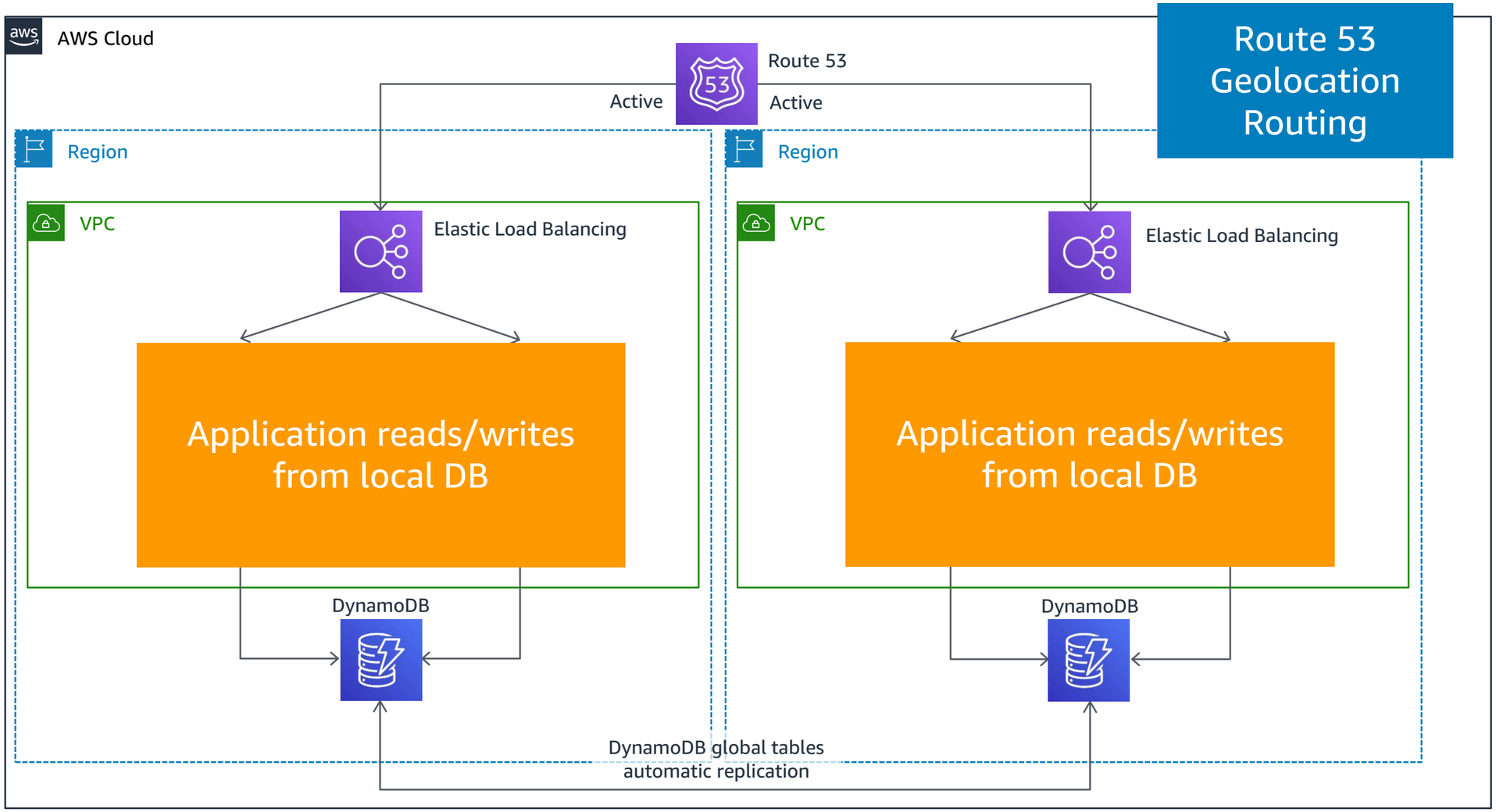
AWS Well-Architected

https://aws.com/well-architected/

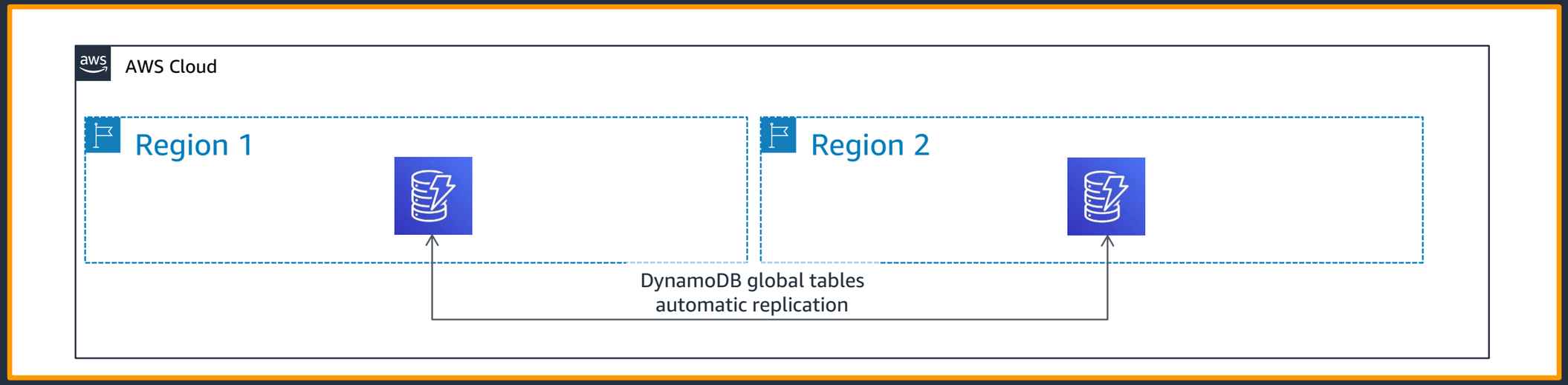
re:Invent 2018: Architecture Patterns for Multi-Region Active-Active Applications (ARC209-R2)

https://youtu.be/2e29I3dA8o4

A/A Pattern 1: Read Local – Write local



Write contention is a concern with “write local”



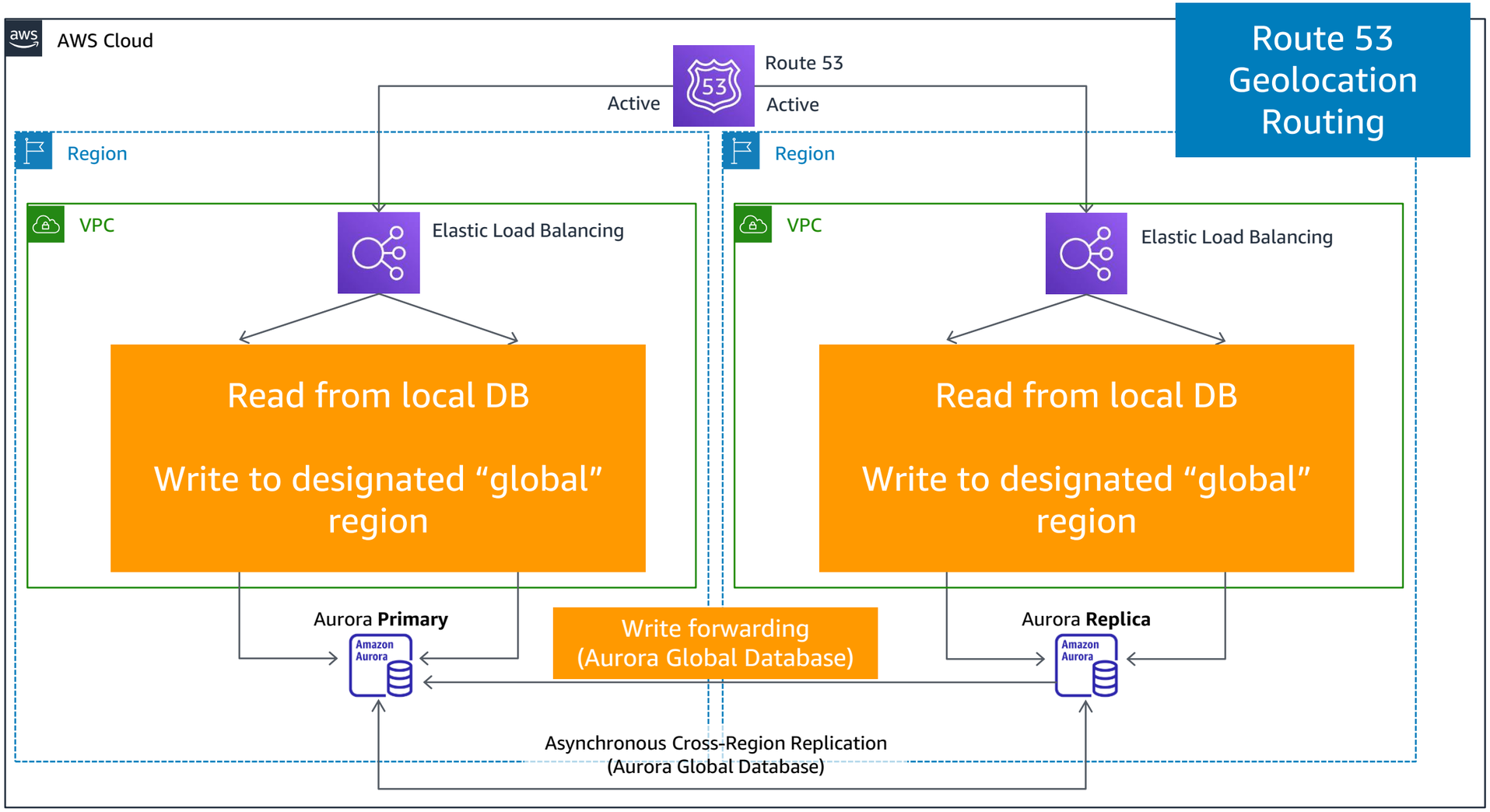
Time (msec)	Operation	Condition check	Ver	Value
1000	READ	-	1	0
1500	WRITE	Ver==1 TRUE	2	100

Time (msec)	Operation	Condition check	Ver	Value
1000	READ	-	1	0
1400	WRITE	Ver==1 TRUE	2	200
1700	Replication		2	100

Ver 2 item not replicated here yet

Last writer wins

A/A Pattern 2: Read Local – Write global



A/A Pattern 3: Read Local – Write partitioned