Resilience Best Practices

Well-Architected Applications on AWS

Ray Chang (he/him)

Principal Solutions Architect
Amazon Web Services

Nick Ragusa (he/him)

Principal Solutions Architect
Amazon Web Services

AWS Well-Architected Framework: Best practices across six pillars

- Operational excellence
- Security
- Reliability
- Performance efficiency
- Cost optimization
- Sustainability

AWS Well-Architected

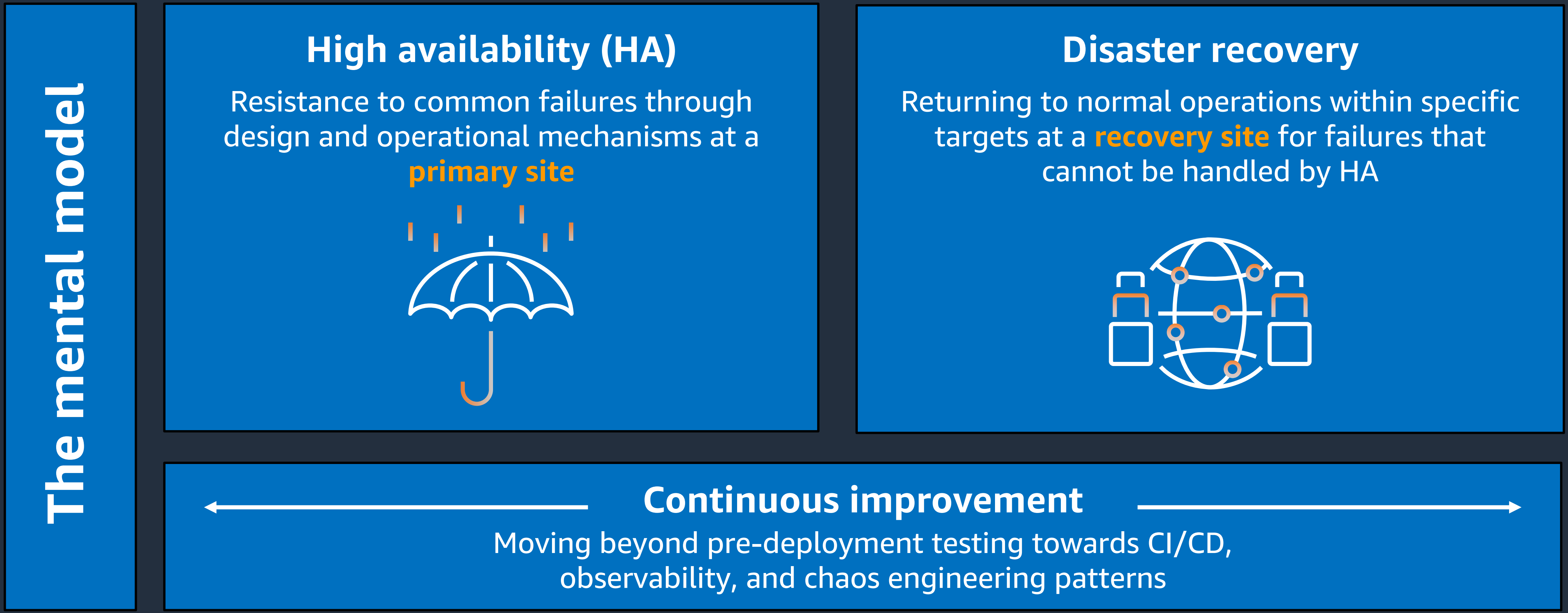
https://aws.com/well-architected

Resilience in AWS Well-Architected Framework

Operational excellence

Reliability

Mental model for resilience



The mental model

High availability (HA)

Resistance to common failures through design and operational mechanisms at a **primary site**

Disaster recovery

Returning to normal operations within specific targets at a **recovery site** for failures that cannot be handled by HA

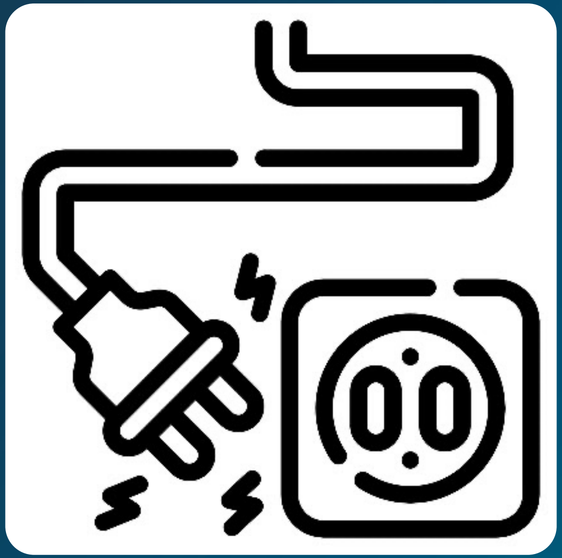
Continuous improvement

Moving beyond pre-deployment testing towards CI/CD, observability, and chaos engineering patterns

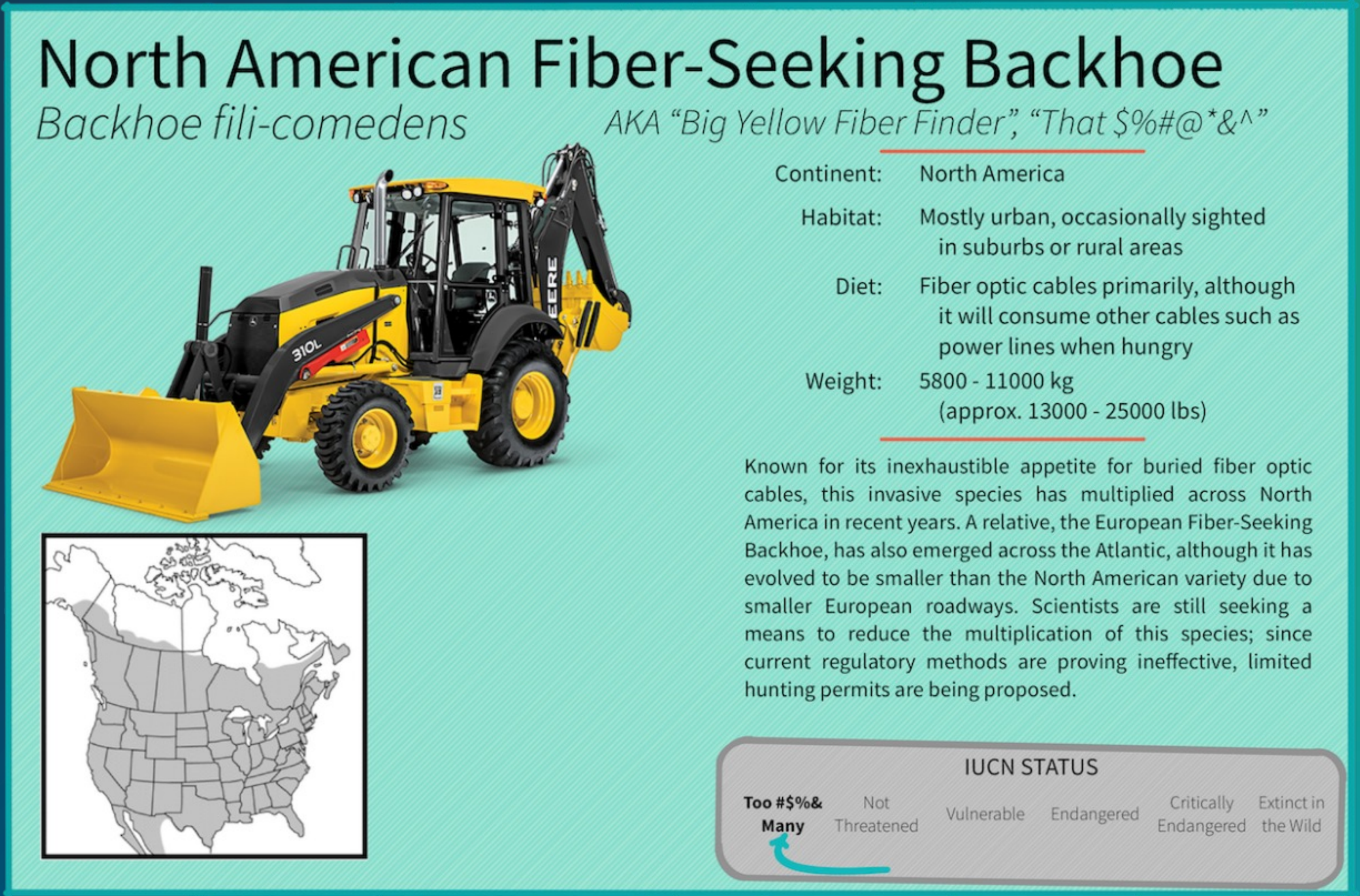
“We needed to build systems that embrace failure as a natural occurrence.”

Dr. Werner Vogels
VP and CTO, Amazon.com

Failure can be one computer



Failure can be multiple data centers



North American Fiber-Seeking Backhoe

Backhoe fili-comedens

AKA "Big Yellow Fiber Finder", "That $%#@&^"*

Continent:	North America
Habitat:	Mostly urban, occasionally sighted in suburbs or rural areas
Diet:	Fiber optic cables primarily, although it will consume other cables such as power lines when hungry
Weight:	5800 - 11000 kg (approx. 13000 - 25000 lbs)

Known for its inexhaustible appetite for buried fiber optic cables, this invasive species has multiplied across North America in recent years. A relative, the European Fiber-Seeking Backhoe, has also emerged across the Atlantic, although it has evolved to be smaller than the North American variety due to smaller European roadways. Scientists are still seeking a means to reduce the multiplication of this species; since current regulatory methods are proving ineffective, limited hunting permits are being proposed.

IUCN STATUS

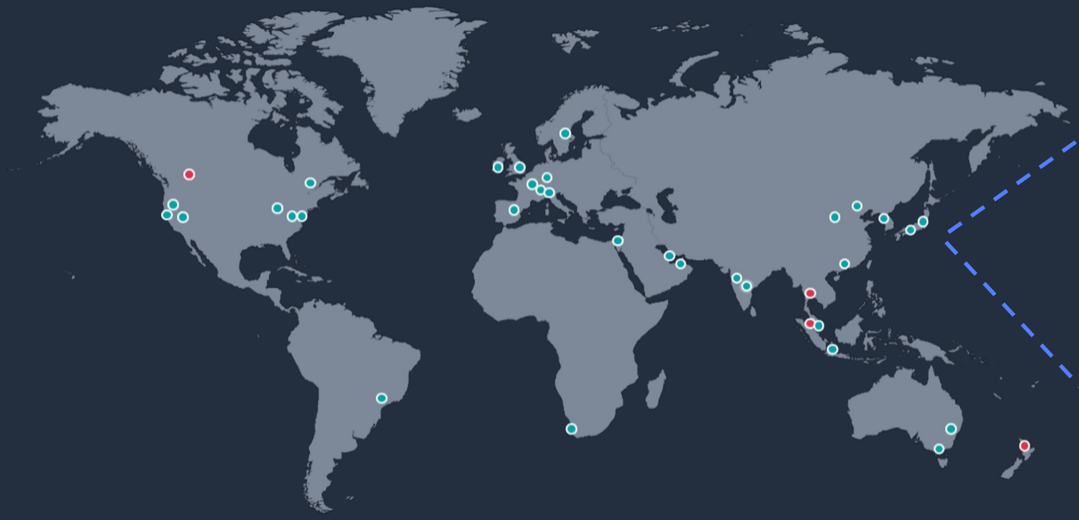
Too #$%& Many	Not Threatened	Vulnerable	Endangered	Critically Endangered	Extinct in the Wild

/u/castillar on Reddit

AWS Regions and Availability Zones (AZs)

AWS REGIONS ARE PHYSICAL LOCATIONS AROUND THE WORLD WHERE WE CLUSTER DATA CENTERS

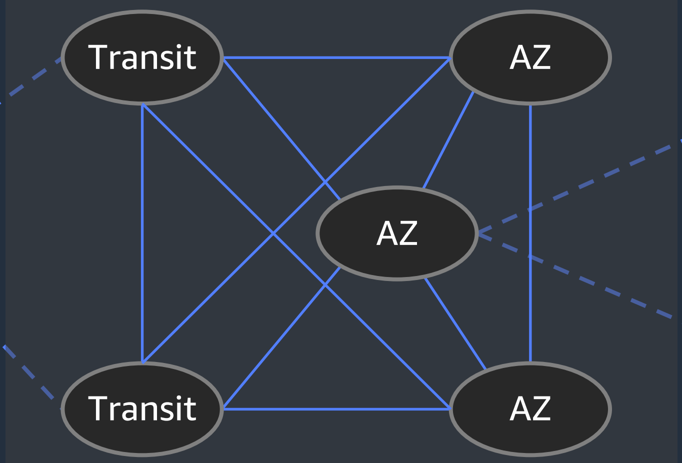
33 AWS Regions worldwide



● AWS Regions

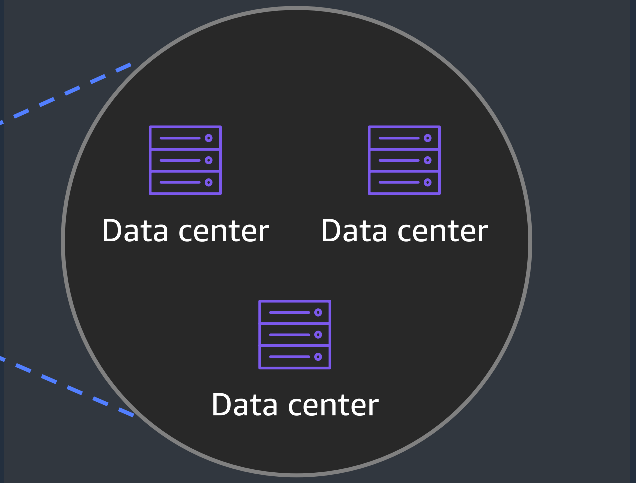
● Announced Regions

Each AWS Region has multiple AZs



A Region is a physical location in the world

Each AZ includes one or more discrete data centers



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

High Availability

Resources as Code >>> Clickops

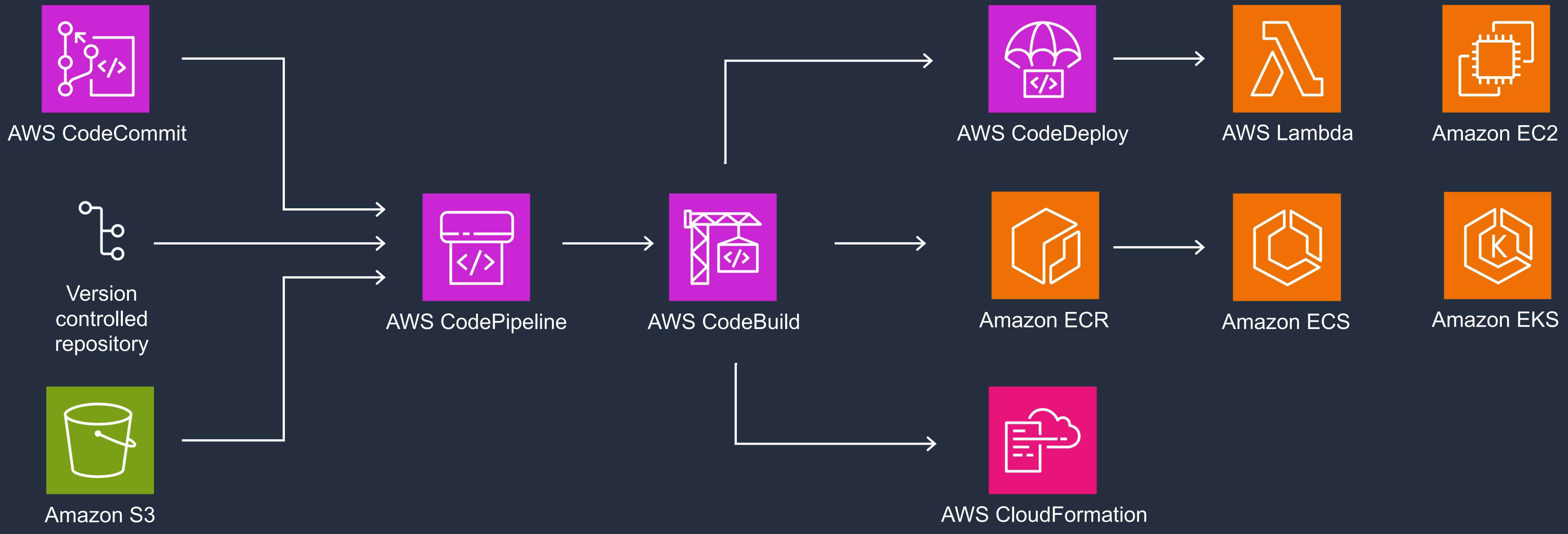
AWS CloudFormation

AWS Cloud Development Kit

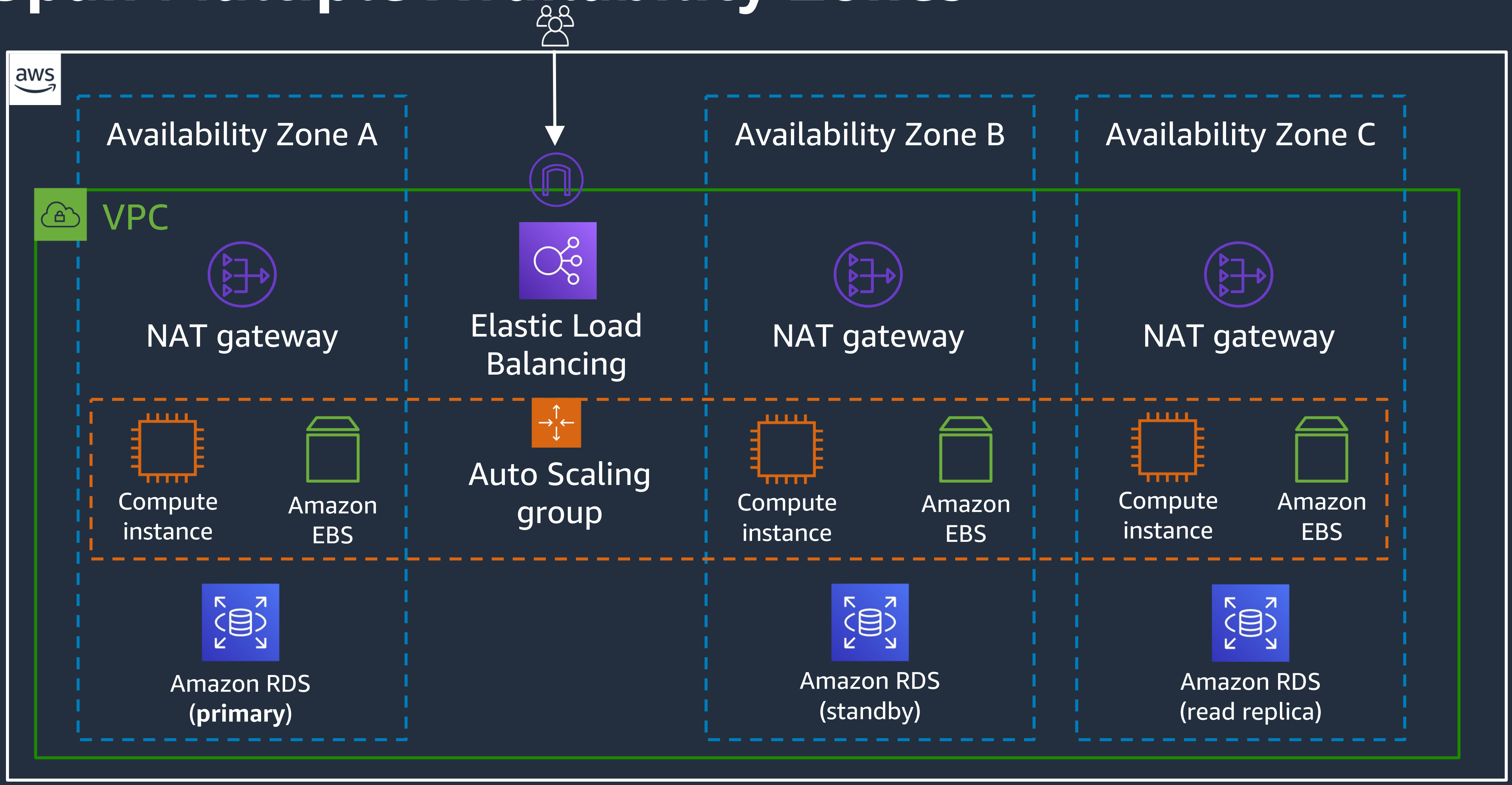
AWS Serverless Application Model

- If it’s code, we can version control it.
- If it’s code, we can detect drift.
- If it’s code, we can update it via automation.

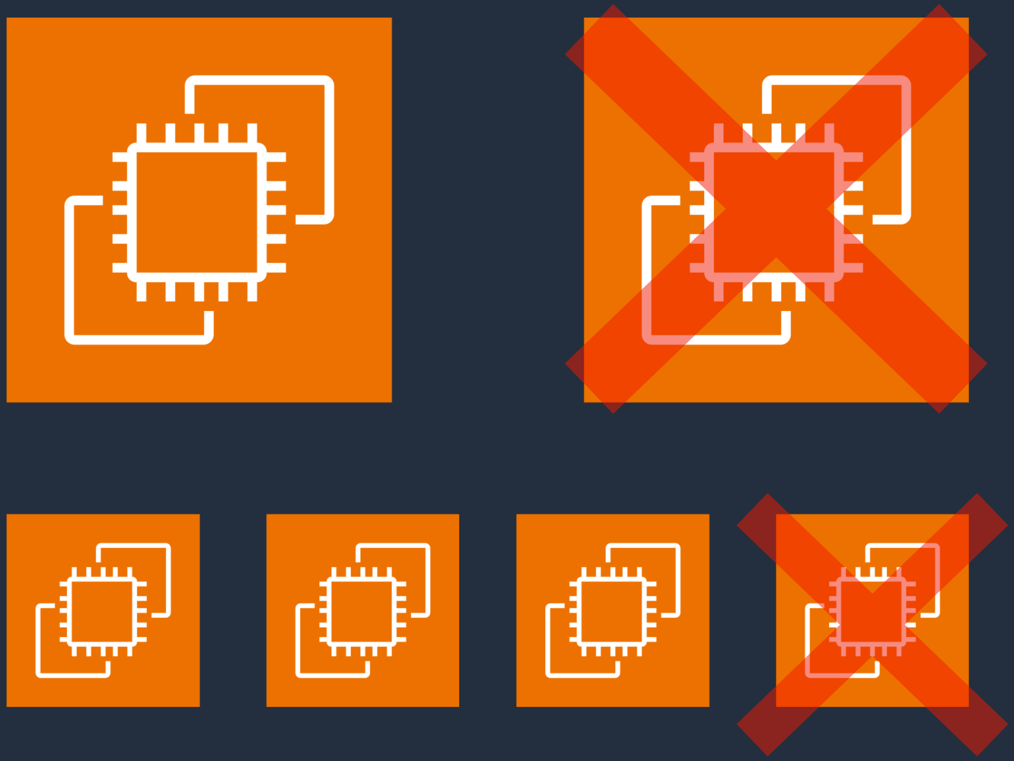
Update Resources via Automation >>> Clickops



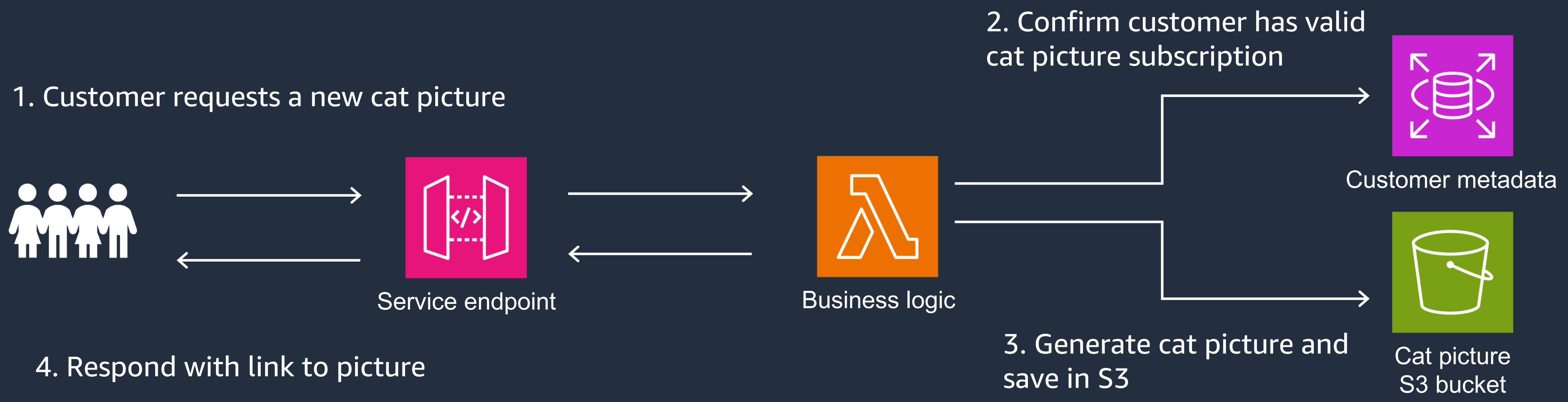
Span Multiple Availability Zones



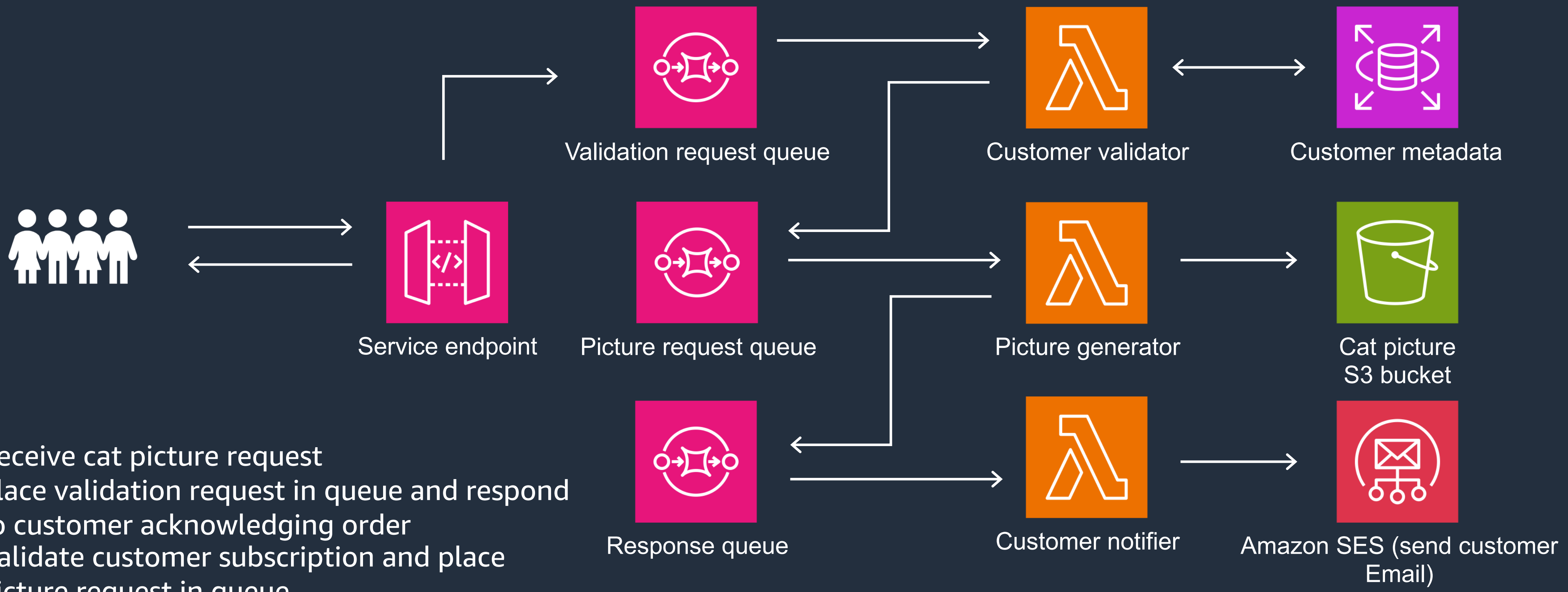
Many small resources >>> Few large resources



Asynchronous Decoupling


1. Customer requests a new cat picture
Service endpoint
Business logic
2. Confirm customer has valid cat picture subscription
Customer metadata
3. Generate cat picture and save in S3
Cat picture S3 bucket
4. Respond with link to picture

Asynchronous Decoupling



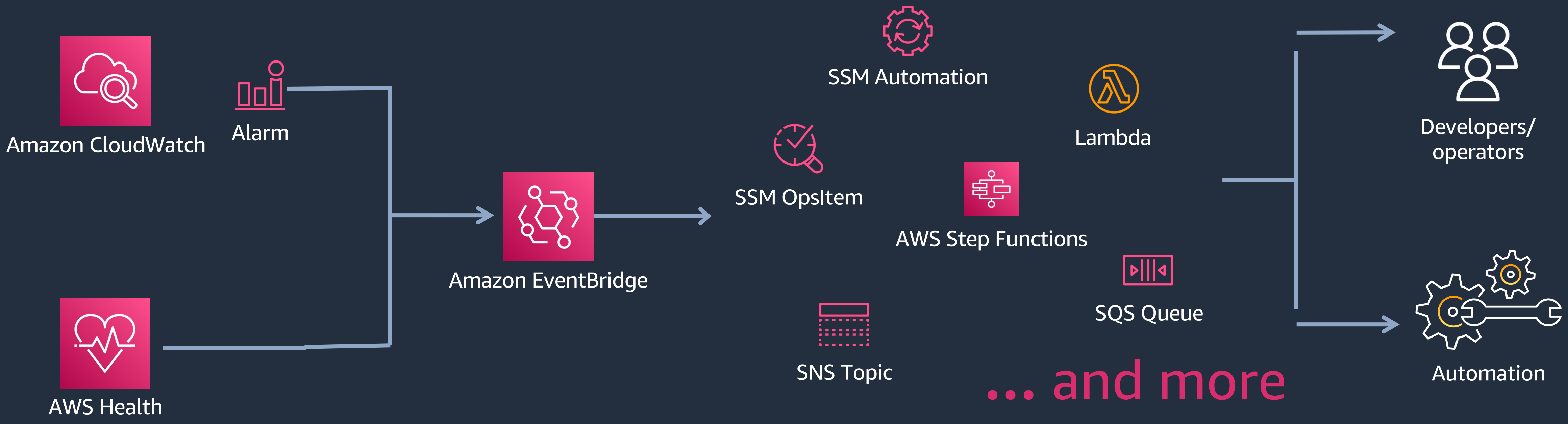
1. Receive cat picture request
2. Place validation request in queue and respond to customer acknowledging order
3. Validate customer subscription and place picture request in queue
4. Generate cat picture in S3 and place communication request in queue
5. Send customer email with link to cat picture

Failures teach – don’t miss the opportunity to learn!

- Test resilience by injecting failures
- Understand your failure conditions, identify new ones
- Learn which metrics are important to you

AWS Fault Injection Simulator

AWS monitoring and automation



Amazon CloudWatch

Alarm

AWS Health

Amazon EventBridge

SSM Automation

SSM OpsItem

SNS Topic

Lambda

AWS Step Functions

SQS Queue

... and more

Developers/ operators

Automation

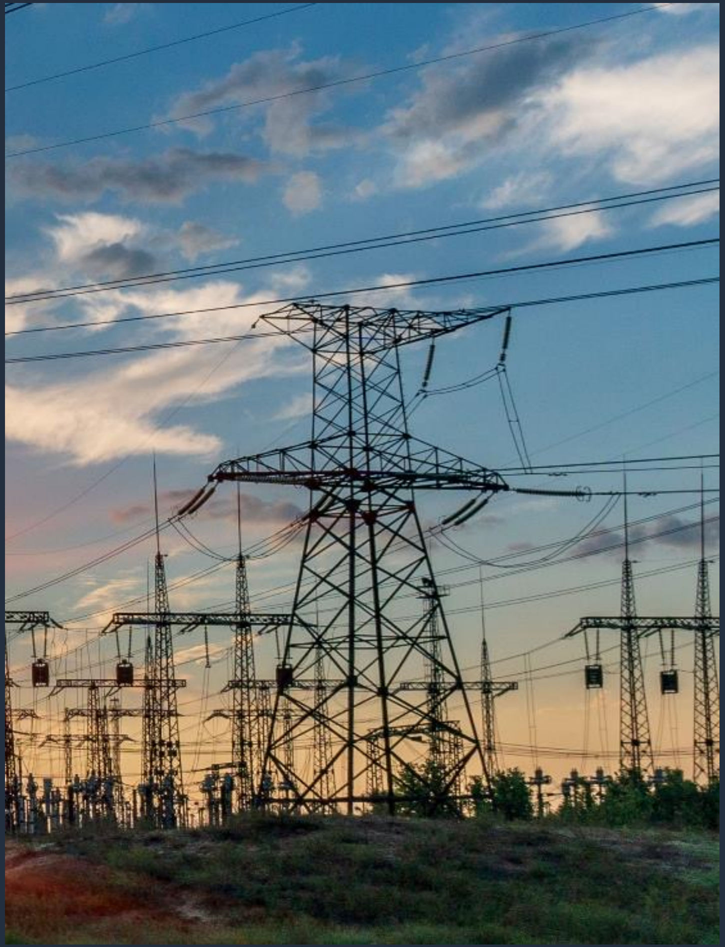
```
{
  "source": ["aws.health"],
  "detail-type": ["AWS Health Event"],
  "detail": {
    "service": ["S3"],
    "eventTypeCategory": ["issue"],
    "eventTypeCode": ["AWS_S3_INCREASED_GET_API_ERROR_RATES", "AWS_S3_INCREASED_PUT_API_ERROR_RATES"]
  }
}
```

Disaster Recovery

Types of Disasters

Natural disaster

Technical failure



Human actions

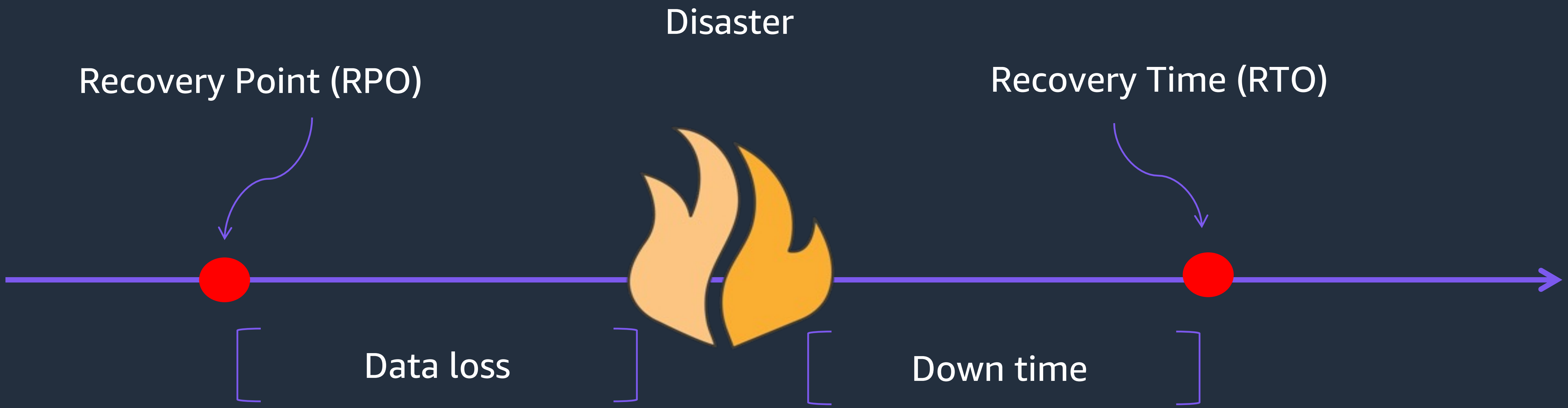
Our TWO Different Objectives

Recovery Point Objective (RPO)

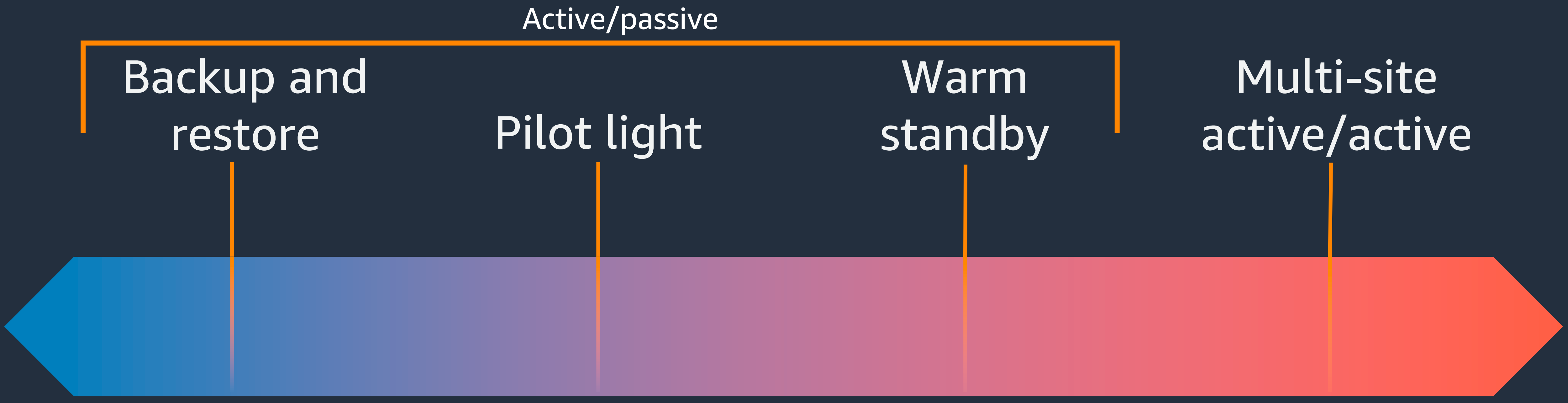
The maximum acceptable amount of time since the last data recovery point

Recovery Time Objective (RTO)

The maximum acceptable delay between the interruption of service and restoration of service



Strategies for disaster recovery



Active/passive

Backup and restore

RPO / RTO:
Hours

Lower priority use cases
Cost $

Pilot light

RPO / RTO:
10s of minutes

Data live
Services idle
Cost: $$

Warm standby

RPO / RTO:
Minutes

Data live
Always running, but smaller
Cost $$$

Multi-site active/active

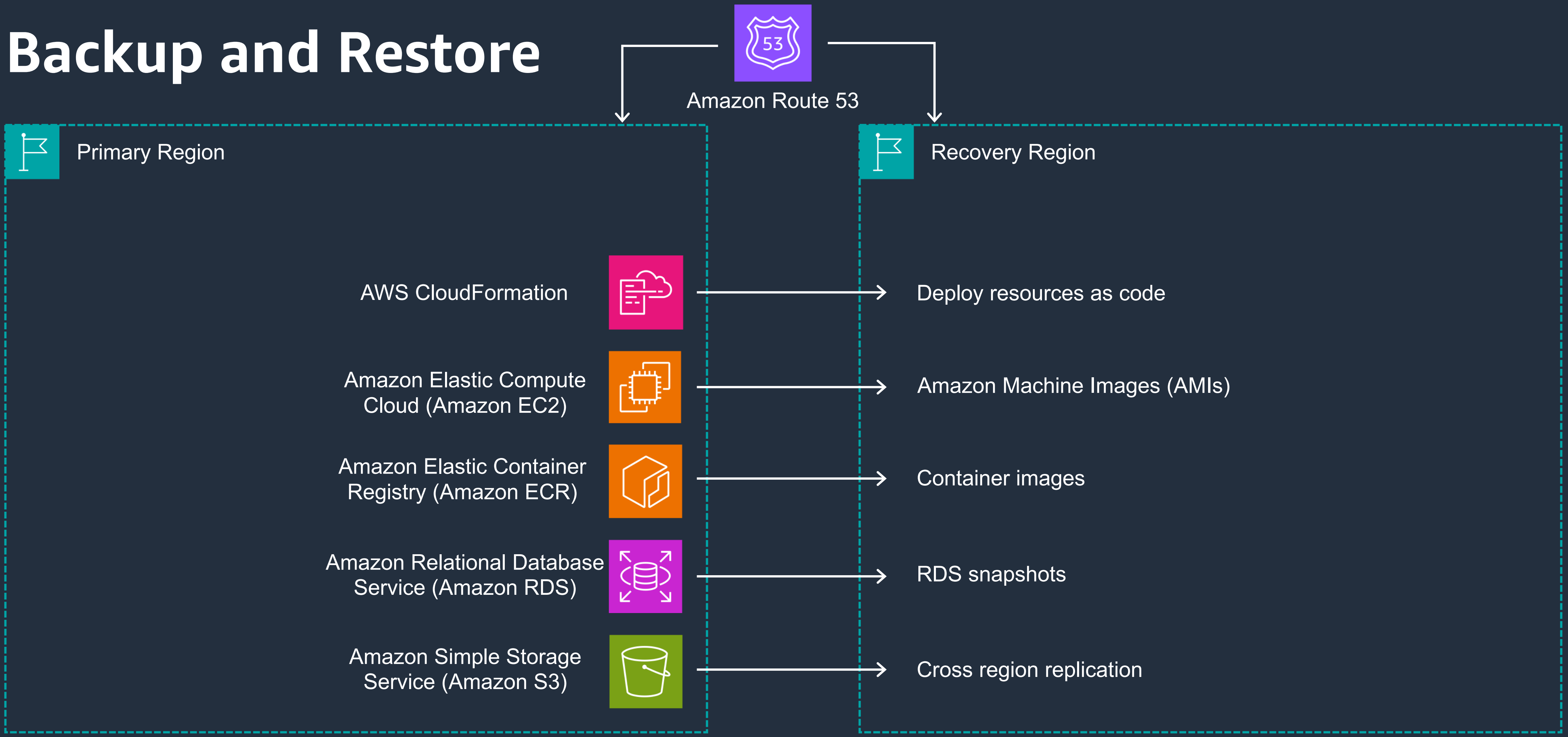
RPO / RTO:
Real-time

Near zero downtime
Near zero data loss
Cost $$$ - $$$$

Resilience isn't an end state, it's a lifestyle

- ”Backups aren't backups until a restore is made.”
  - Steve Jones - https://www.sqlservercentral.com/editorials/backups-arent-backups-until-a-restore-is-made
- Infrastructure/resources-as-code makes life easier.

Backup and Restore



Amazon Route 53

Primary Region

AWS CloudFormation

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Elastic Container Registry (Amazon ECR)

Amazon Relational Database Service (Amazon RDS)

Amazon Simple Storage Service (Amazon S3)

Recovery Region

Deploy resources as code

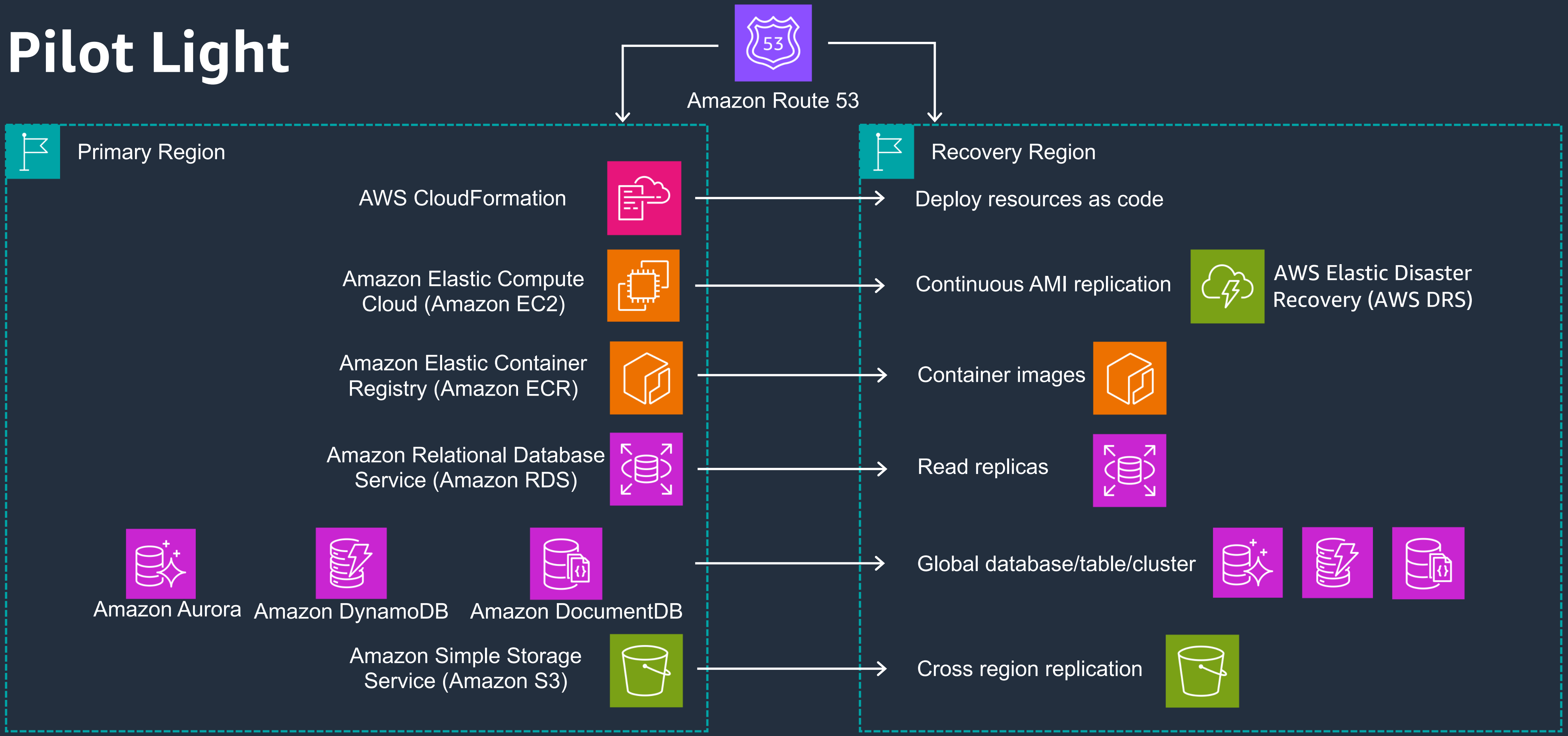
Amazon Machine Images (AMIs)

Container images

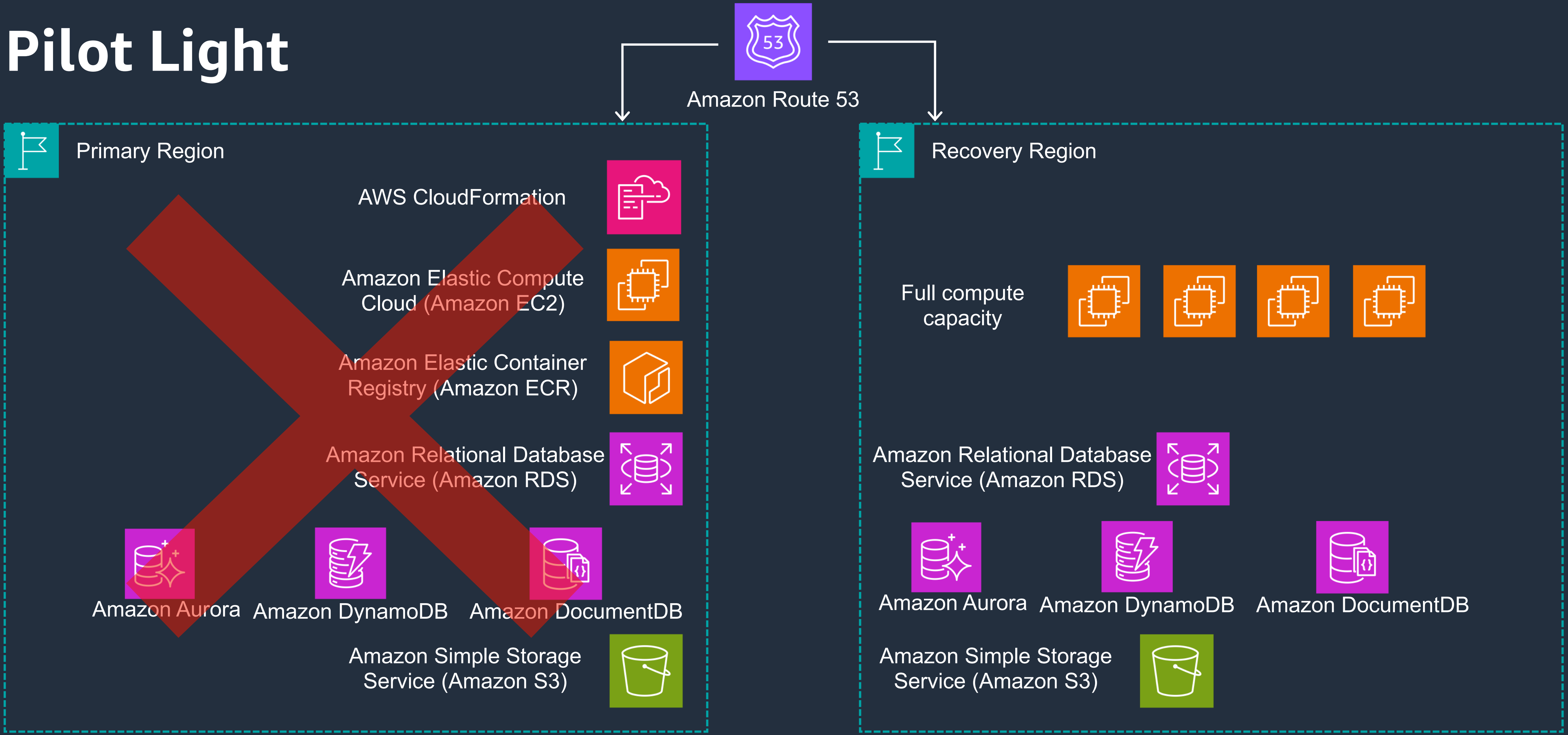
RDS snapshots

Cross region replication

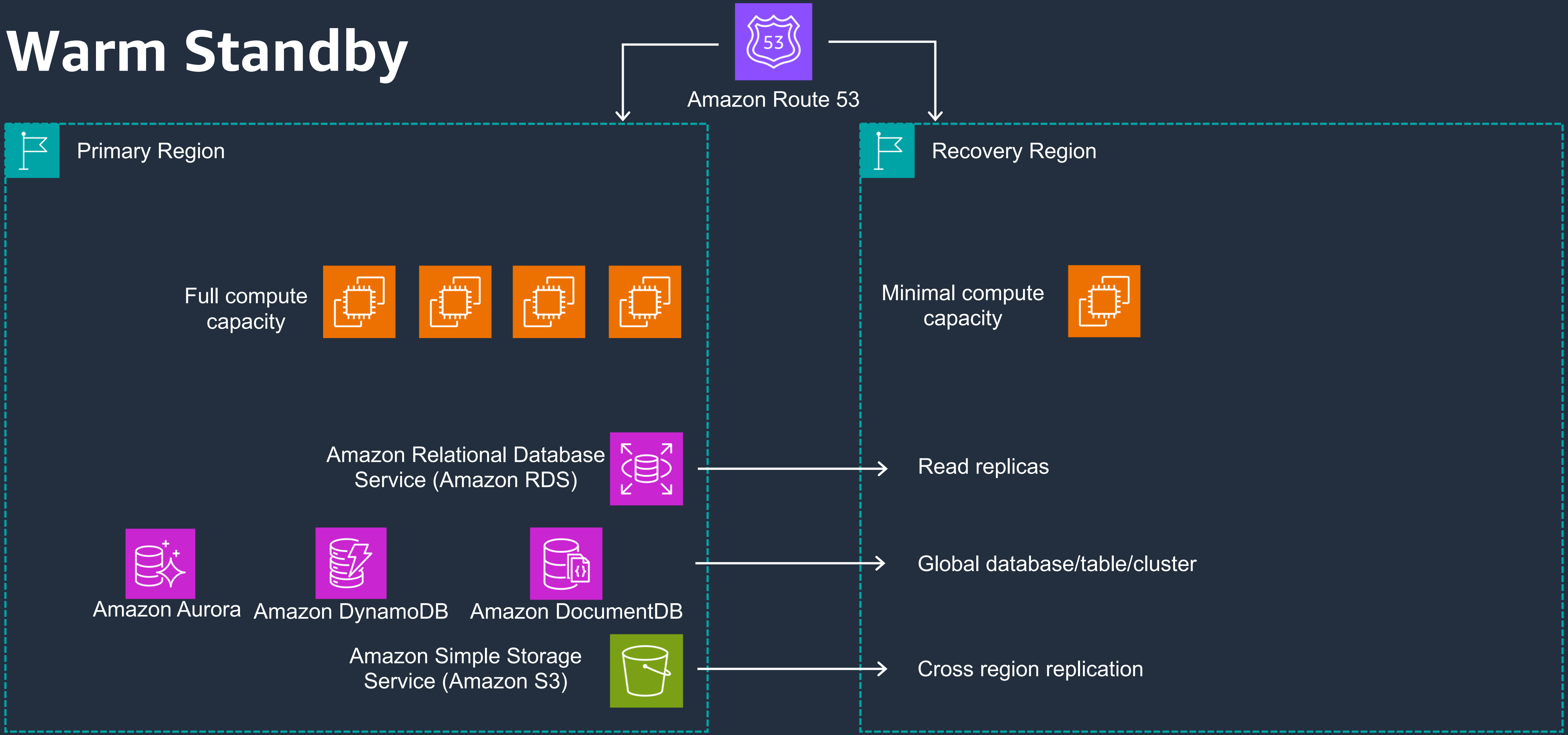
Pilot Light


Amazon Route 53
Primary Region
AWS CloudFormation
Amazon Elastic Compute Cloud (Amazon EC2)
Amazon Elastic Container Registry (Amazon ECR)
Amazon Relational Database Service (Amazon RDS)
Amazon Aurora
Amazon DynamoDB
Amazon DocumentDB
Amazon Simple Storage Service (Amazon S3)
Recovery Region
Deploy resources as code
Continuous AMI replication
AWS Elastic Disaster Recovery (AWS DRS)
Container images
Read replicas
Global database/table/cluster
Cross region replication

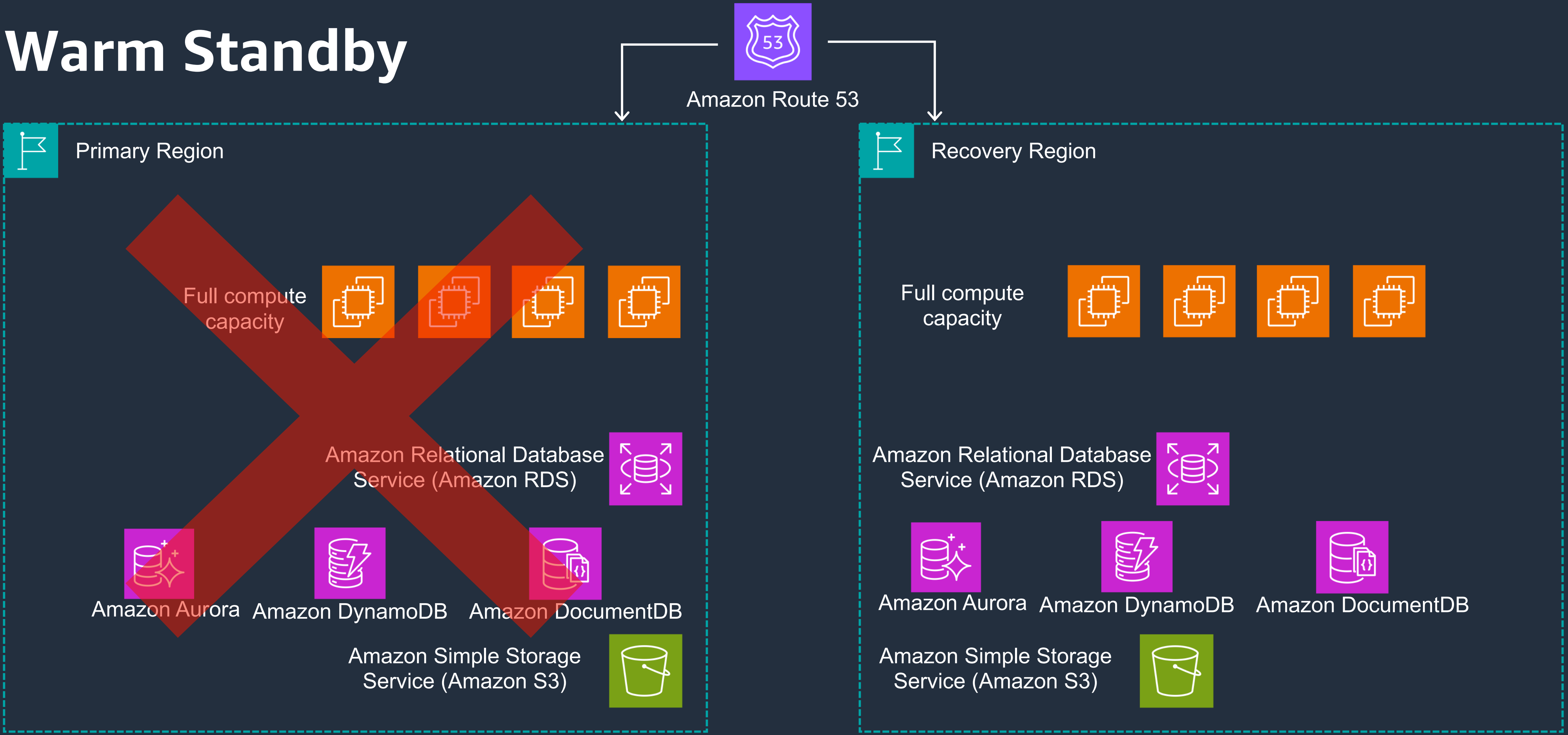
Pilot Light


Amazon Route 53
Primary Region
AWS CloudFormation
Amazon Elastic Compute Cloud (Amazon EC2)
Amazon Elastic Container Registry (Amazon ECR)
Amazon Relational Database Service (Amazon RDS)
Amazon Aurora
Amazon DynamoDB
Amazon DocumentDB
Amazon Simple Storage Service (Amazon S3)
Recovery Region
Full compute capacity
Amazon Relational Database Service (Amazon RDS)
Amazon Aurora
Amazon DynamoDB
Amazon DocumentDB
Amazon Simple Storage Service (Amazon S3)

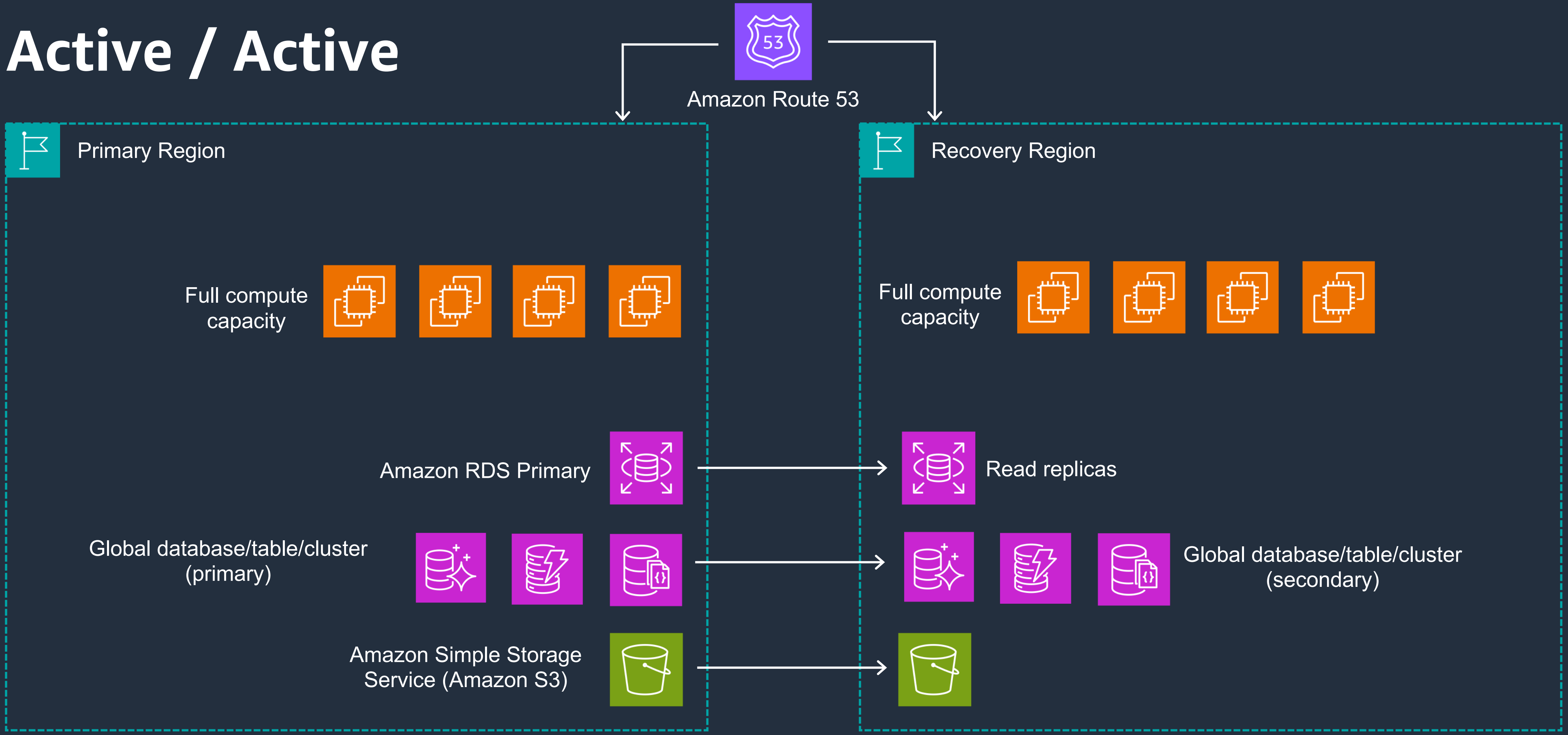
Warm Standby



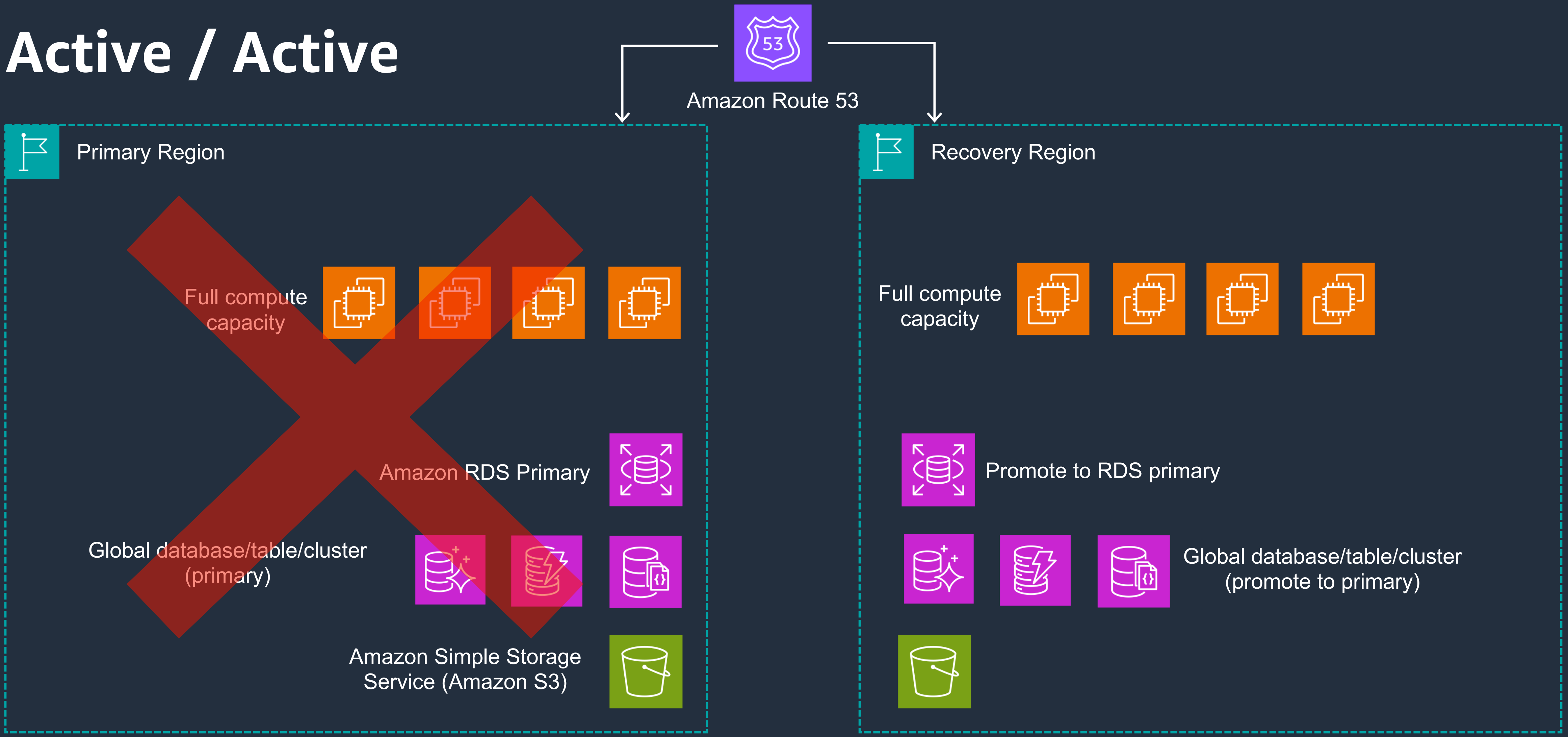
Warm Standby


Amazon Route 53
Primary Region
Full compute capacity
Amazon Relational Database Service (Amazon RDS)
Amazon Aurora
Amazon DynamoDB
Amazon DocumentDB
Amazon Simple Storage Service (Amazon S3)
Recovery Region
Full compute capacity
Amazon Relational Database Service (Amazon RDS)
Amazon Aurora
Amazon DynamoDB
Amazon DocumentDB
Amazon Simple Storage Service (Amazon S3)

Active / Active


Amazon Route 53
Primary Region
Recovery Region
Full compute capacity
Full compute capacity
Amazon RDS Primary
Read replicas
Global database/table/cluster (primary)
Global database/table/cluster (secondary)
Amazon Simple Storage Service (Amazon S3)

Active / Active



Amazon Route 53

Primary Region

Full compute capacity

Amazon RDS Primary

Global database/table/cluster (primary)

Amazon Simple Storage Service (Amazon S3)

Recovery Region

Full compute capacity

Promote to RDS primary

Global database/table/cluster (promote to primary)

AWS **Well-Architected**

Next steps?

- Come see us at the "Ask the Expert" booth.
- Connect with your AWS Account Team.
- Don't forget to take the session survey!

Additional Resources:

Whitepaper: Reliability Pillar: AWS Well-Architected Framework bit.ly/reliability-pillar

AWS Well-Architected tool docs.aws.amazon.com/wellarchitected

Thank you!

Ray Chang
rchang@amazon.com

Nick Ragusa
ragusan@amazon.com

Please take the session survey:

Track: Application modernization, security, and governance

Session: Resilience best practices: Well-architected applications on AWS