



Resilience best practices

Well-architected applications on AWS

Alex Markley

Solutions Architect
World Wide Public Sector, State & Local Government
Amazon Web Services
awsalex@amazon.com

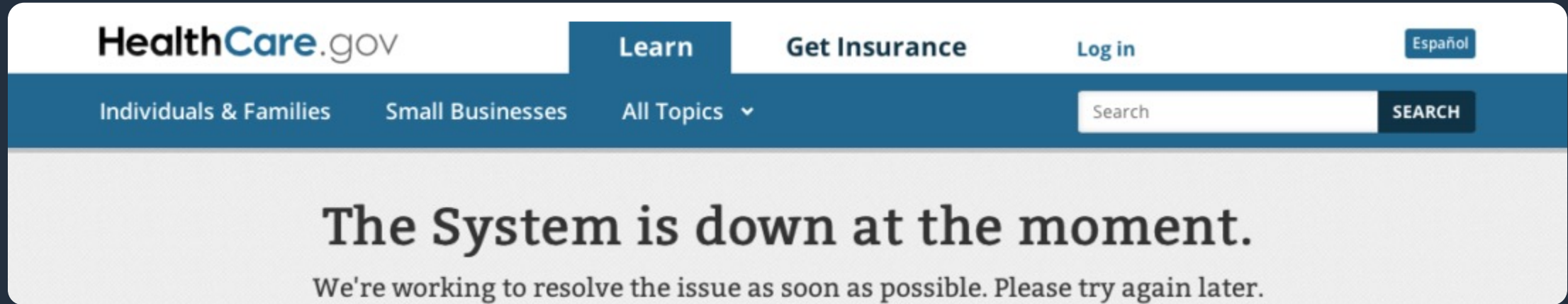
Vishal Lakhotia

Senior Solutions Architect
World Wide Public Sector, State & Local Government
Amazon Web Services
lakhov@amazon.com

What is your plan to keep things running?



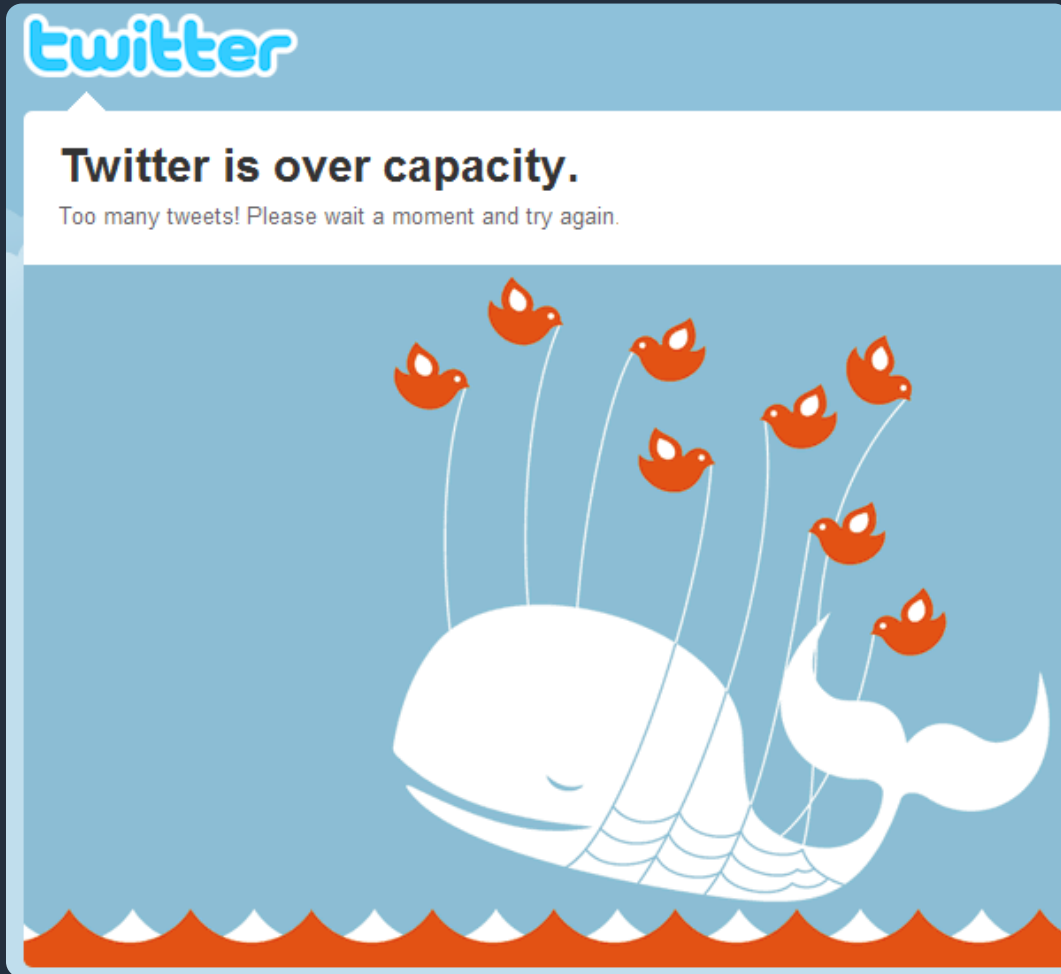
HealthCare.gov launch - 2013



A total of **six users** completed and submitted their applications and selected a health insurance plan on the first day

Performance: System was slow and unresponsive

Twitter: The early days



Reliability: Could not handle the traffic levels

United States FAA ground stop - January 2023

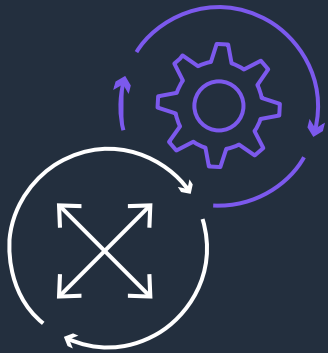


More than 9,500 U.S. flights were delayed

An engineer replaced one file with another
...led to a "cascading" series of IT failures
culminating in this morning's disruption

Operational excellence: Operator error;
untested changes

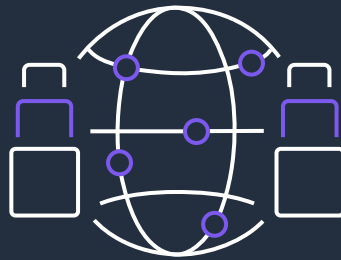
AWS Well-Architected Framework: Best practices across six pillars



Operational
excellence



Security



Reliability



Performance
efficiency



Cost
optimization



Sustainability

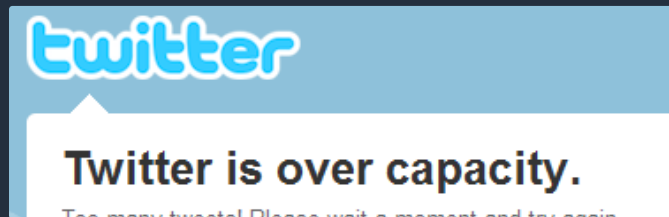


Best practices help you build reliable applications



Performance best practice (PERF BP):

- Load test your workload
- Use the available elasticity of resources
- Understand the areas where performance is most critical



Reliability best practice (REL BP):

- Obtain resources upon detection that more resources are needed
- Use automation when obtaining or scaling resources



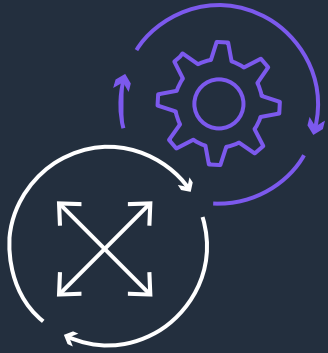
Operations best practice (OPS BP):

- Test and validate changes
- Use multiple environments
- Make frequent, small, reversible changes

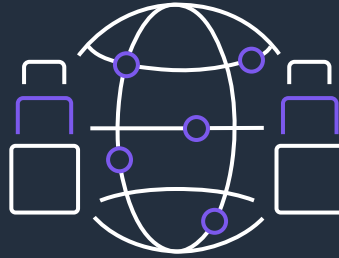
Resilience in the cloud



Resilience in AWS Well-Architected Framework

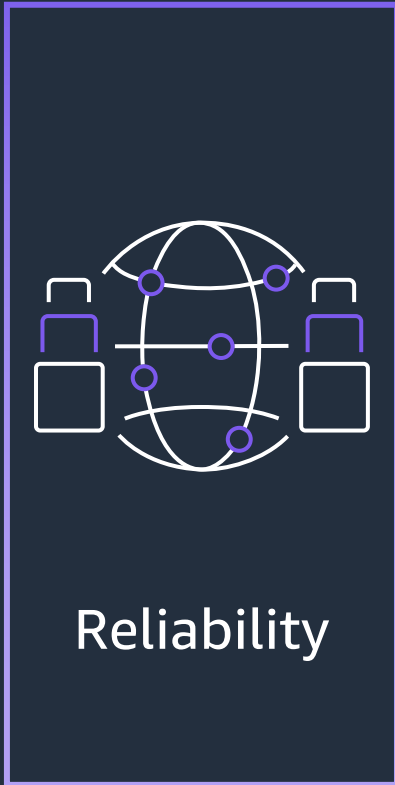


Operational
excellence



Reliability

Reliability pillar: Definitions



Reliable

Application performs its intended function correctly and consistently when it's expected to

Resilient

Application resists failures, or recovers from them quickly

<https://bit.ly/reliability-pillar>

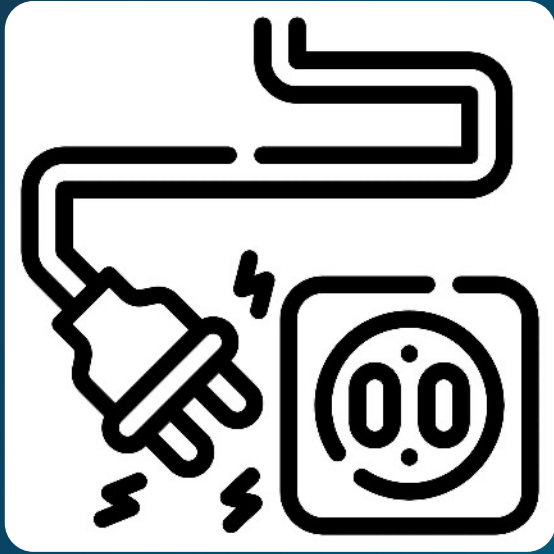


“We needed to build systems that embrace failure as a natural occurrence.”

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

Cloud providers: Many data centers all over the world

Physical infrastructure in data centers

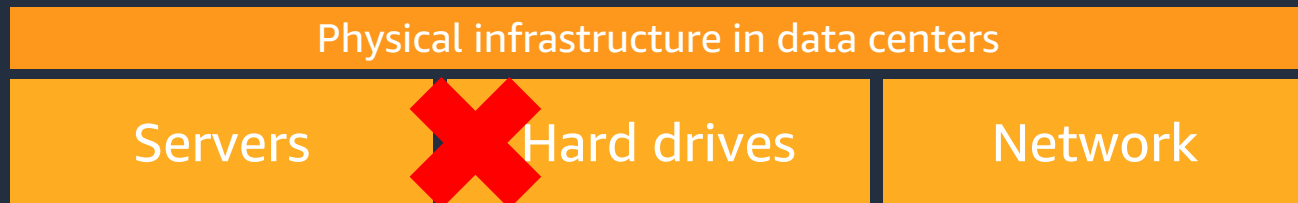
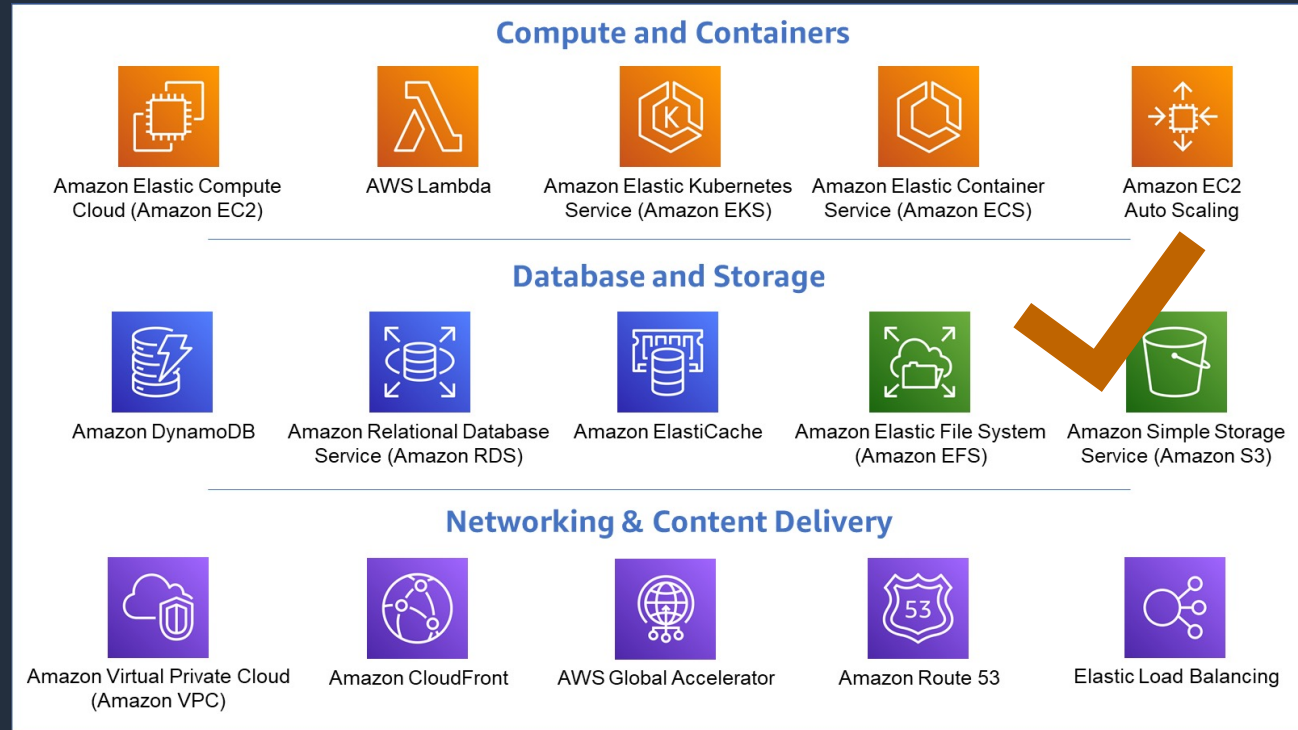
Servers

Hard drives

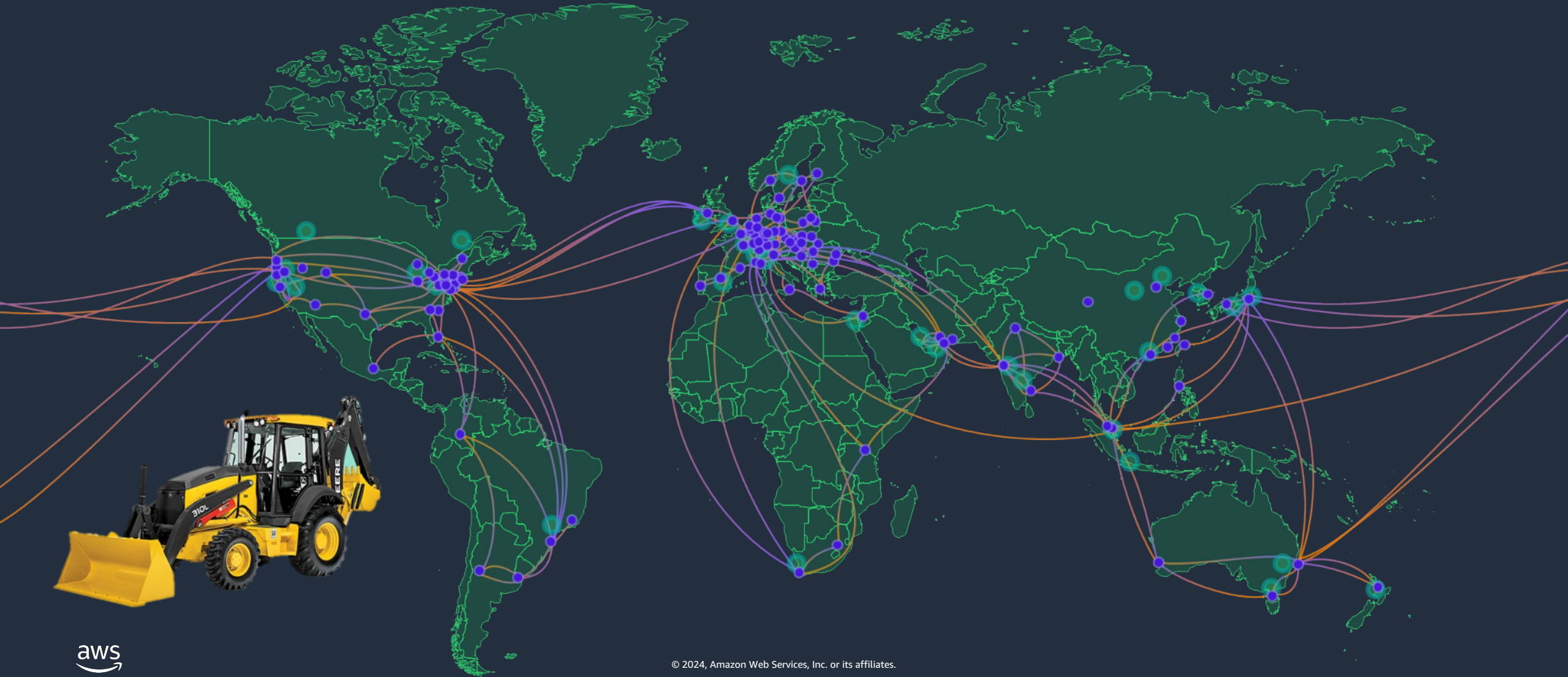
Network



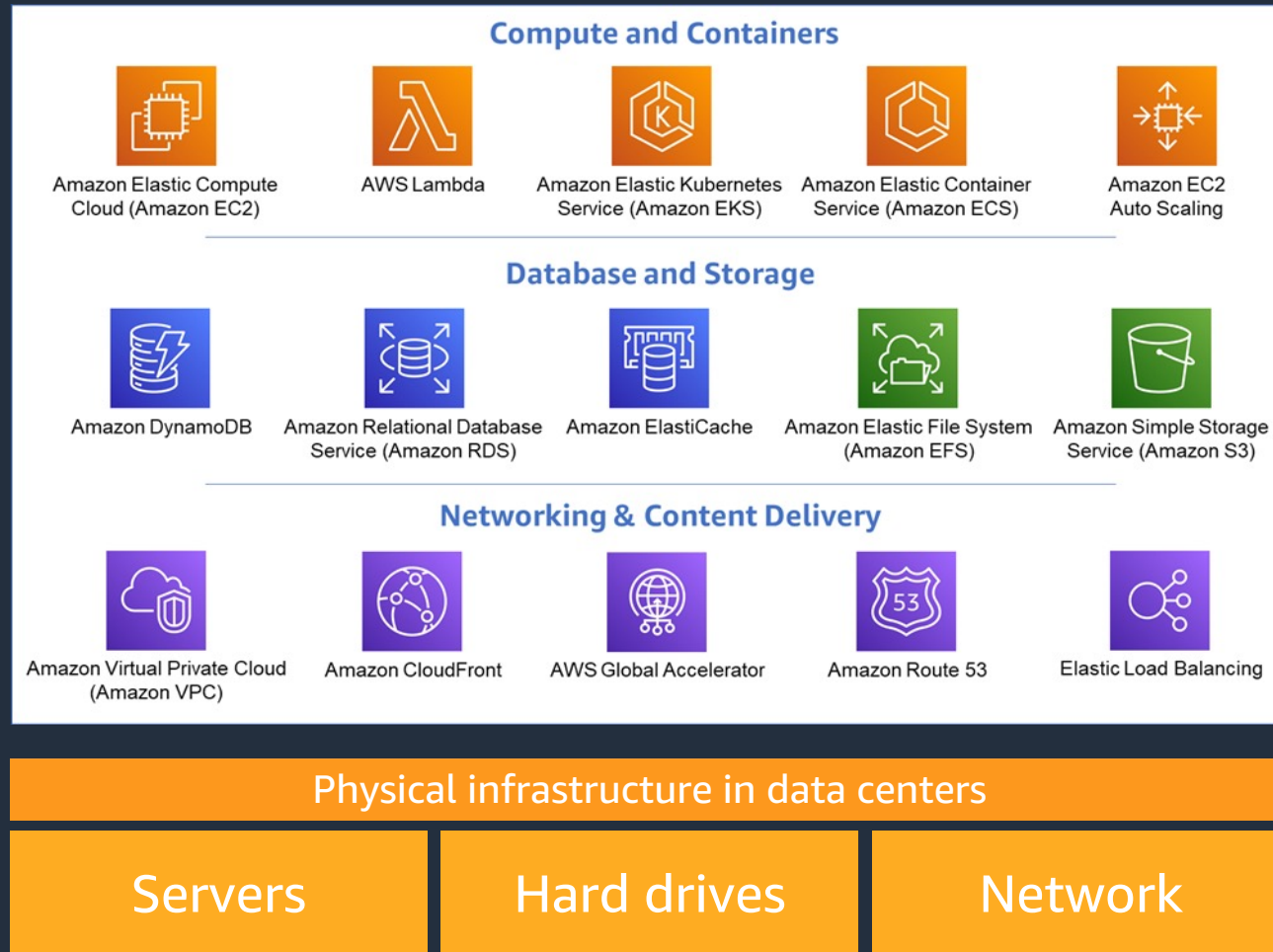
Cloud is an abstraction on top of physical infrastructure



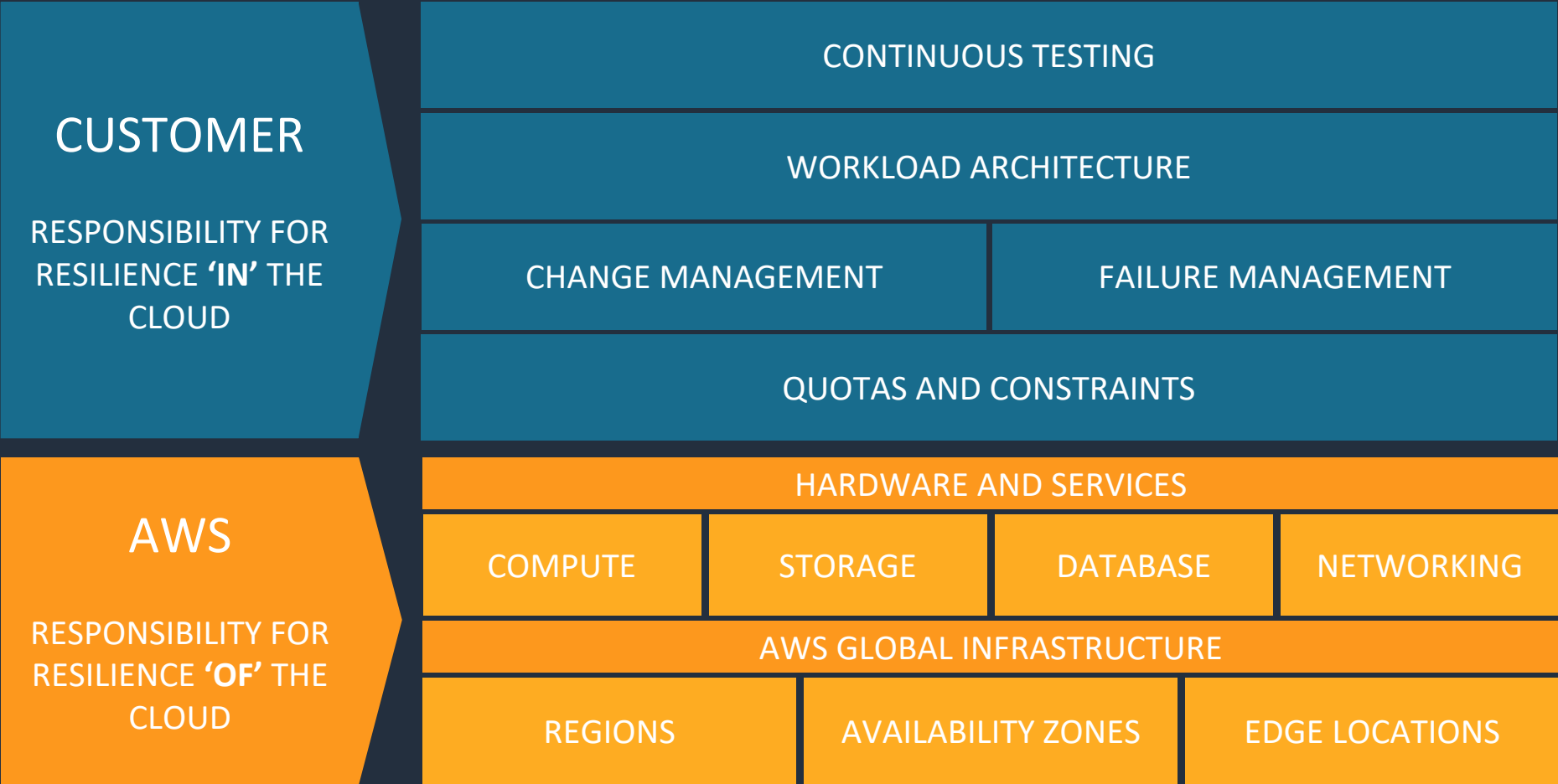
AWS Global Network Infrastructure



AWS runs the infrastructure and the services on it



Shared responsibility for resilience



You need both pieces

- You **can** make it more resilient by putting it on the cloud
- You **must also** build it using the best practices and tools



AWS Regions and Availability Zones (AZs)

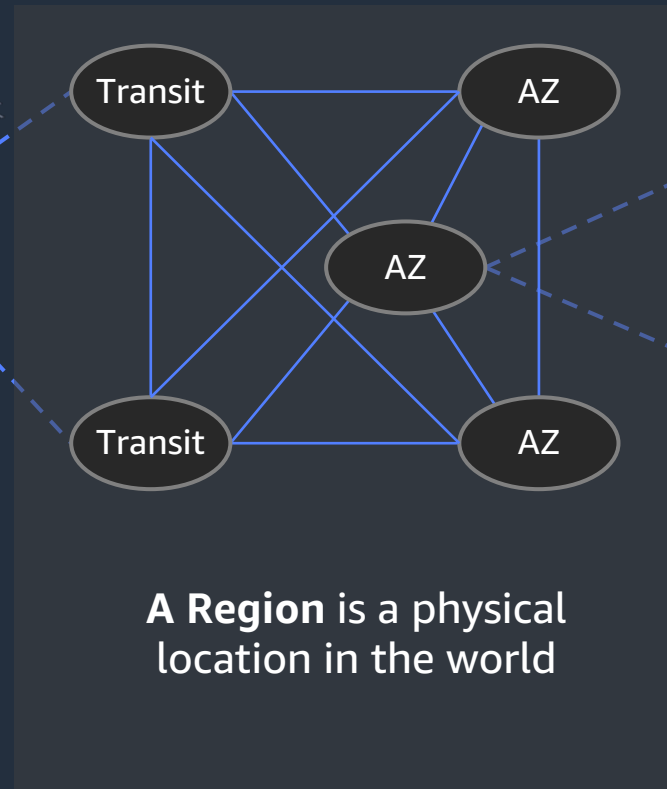
AWS REGIONS ARE PHYSICAL LOCATIONS AROUND THE WORLD WHERE WE CLUSTER DATA CENTERS

32 AWS Regions worldwide

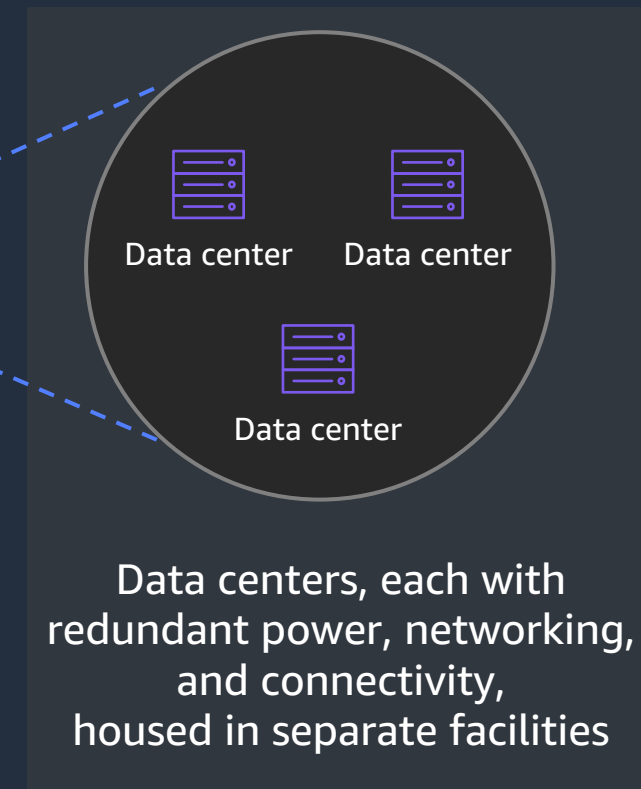


- AWS Regions
- Announced Regions

Each AWS Region has multiple AZs



Each AZ includes one or more discrete data centers



Mental model for resilience

The mental model

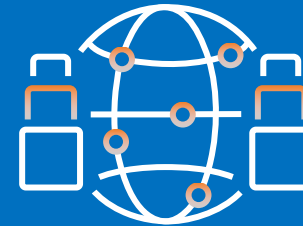
High availability (HA)

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

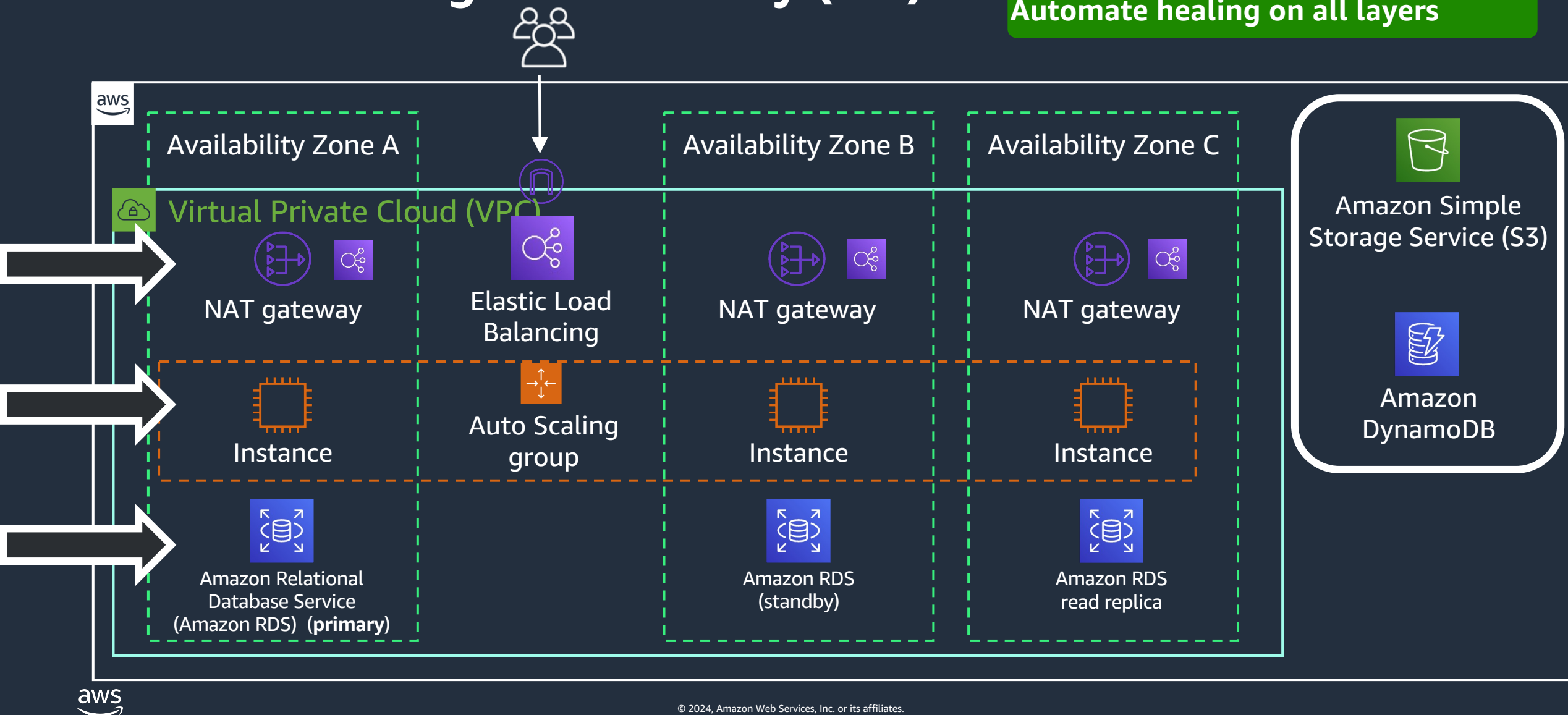
Moving beyond pre-deployment testing towards CI/CD, observability, and chaos engineering patterns

High availability

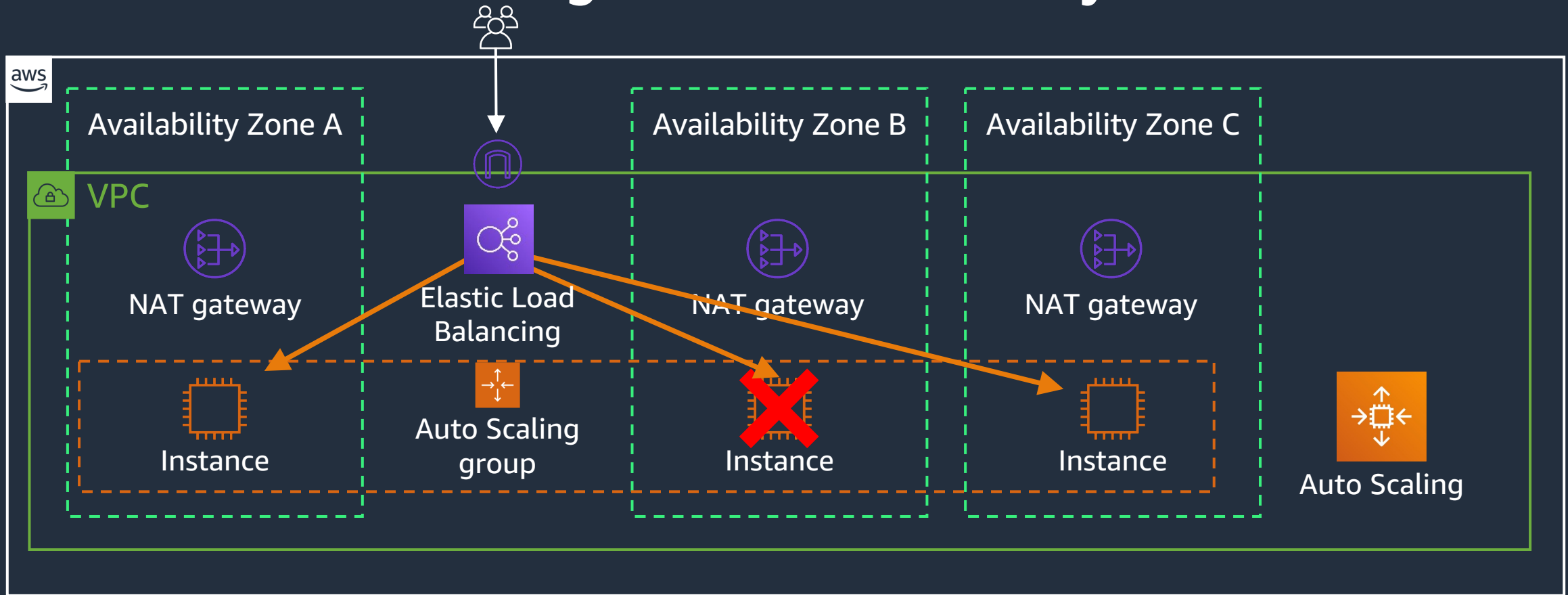


Multi-AZ for high availability (HA)

Reliability best practice (REL BP):
Automate healing on all layers



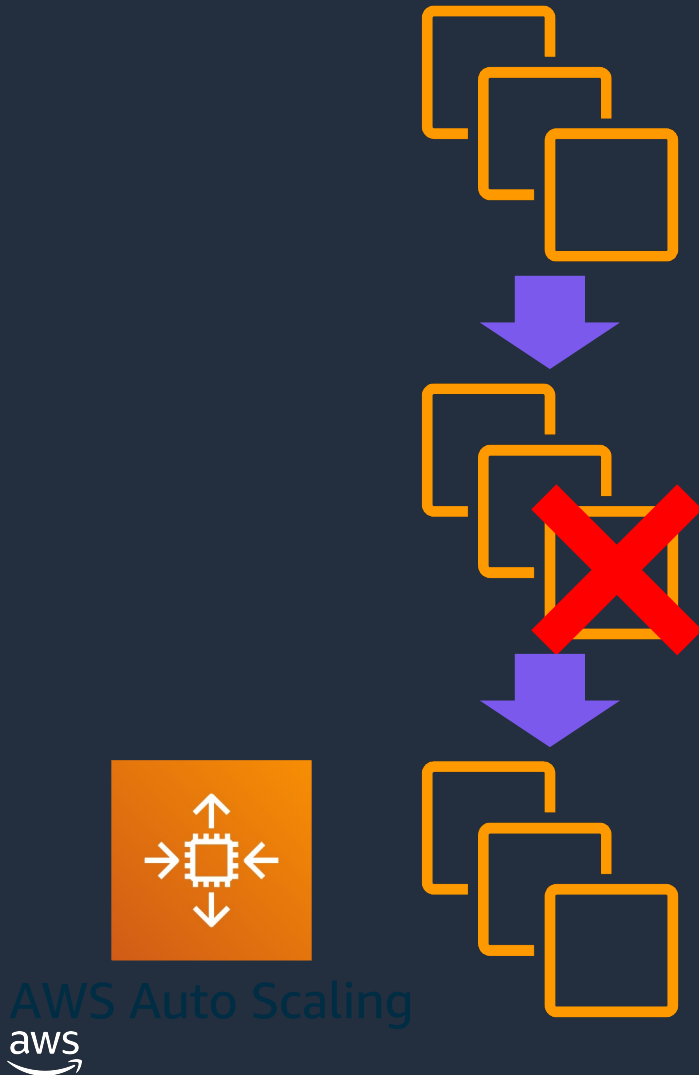
Elastic Load Balancing and auto-recovery



REL BPs:

- Monitor all components for the workload
- Automate responses -- Real-time processing

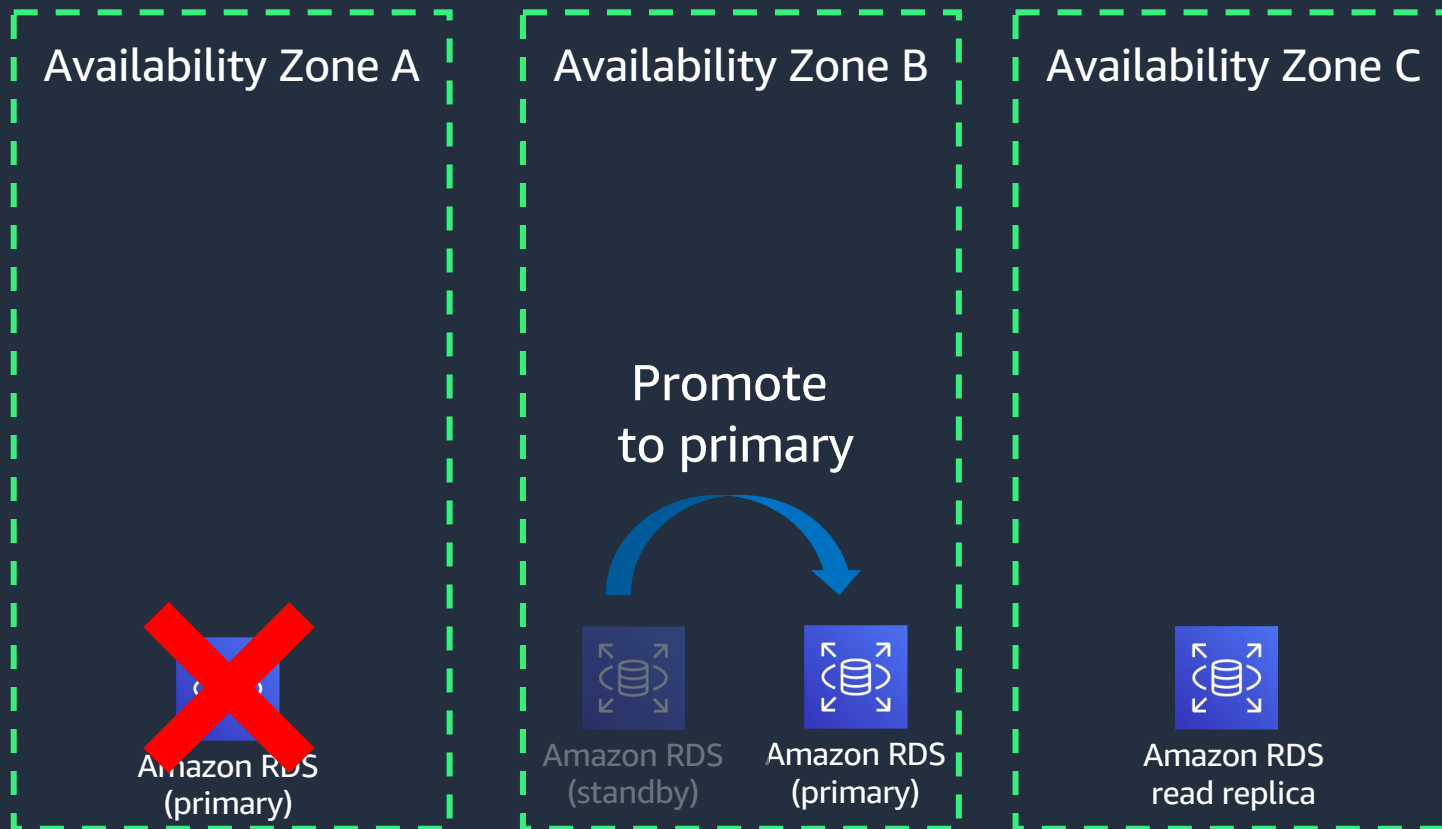
AWS Auto Scaling and auto-recovery



REL BPs:

- Obtain resources upon detection of impairment
- Use automation when obtaining or scaling resources
- Make services stateless where possible

Amazon RDS and auto-recovery



REL BPs:

- Deploy the workload to multiple locations
- Fail over to healthy resources



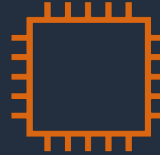
AWS responsibility / customer responsibility

CUSTOMER

RESPONSIBILITY FOR
RESILIENCE 'IN' THE
CLOUD

EC2

Local disk (instance store)



- Backup
- Scaling
- Multi-zone replication
- Security config and updates
- Patching
- Operating system config and maintenance

Amazon S3

Serverless object storage



- Backup

BPs:

- Identify and back up all data that needs to be backed up
- Perform data backup automatically

AWS

RESPONSIBILITY FOR
RESILIENCE 'OF' THE
CLOUD

- Physical hardware, software, networking, and facilities

- Physical hardware, software, networking, and facilities

Disaster recovery



Disaster events

Natural disaster



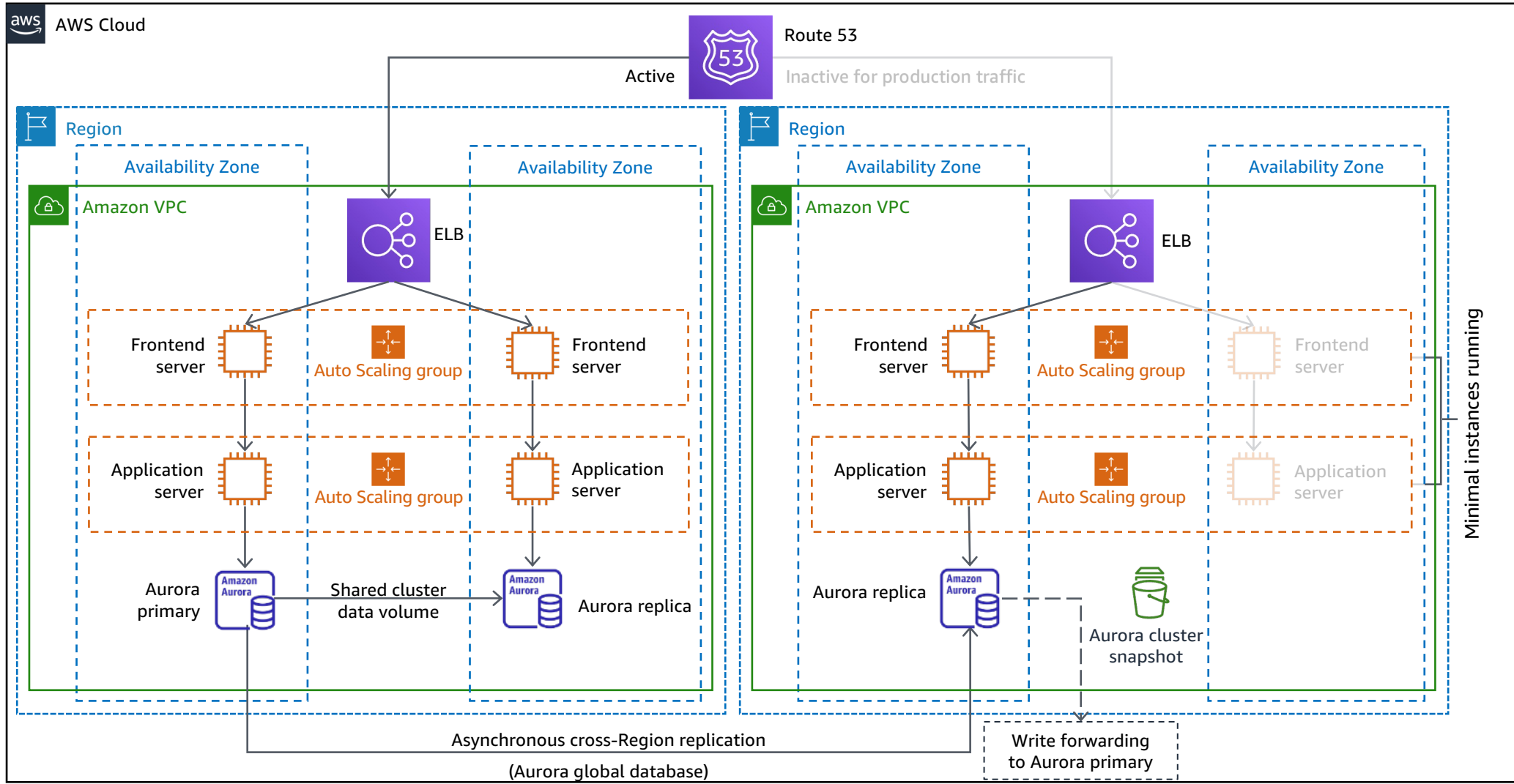
Technical failure



Human actions



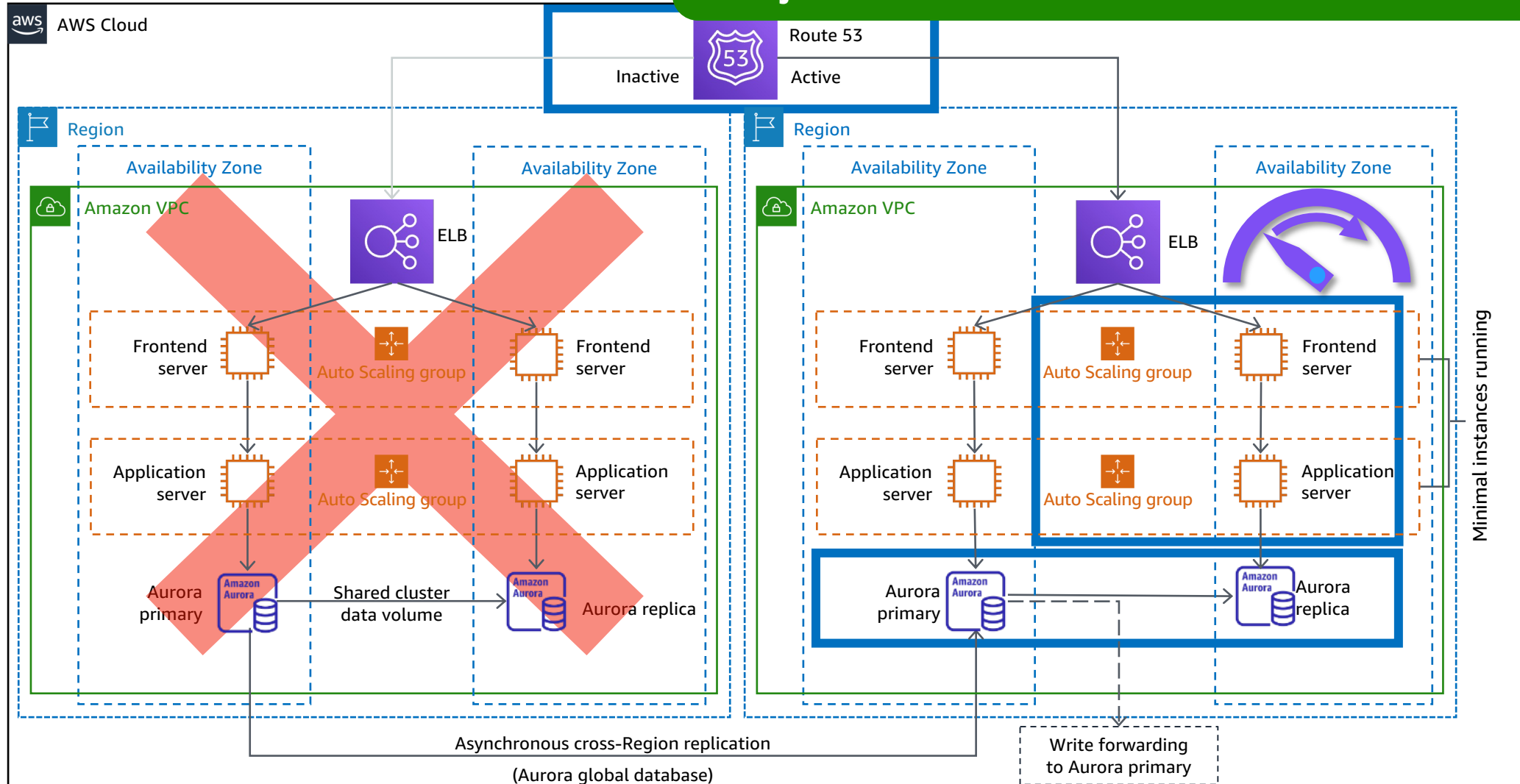
Strategy: Warm standby



Failover: Warm standby

Performance best practice (PERF BP):

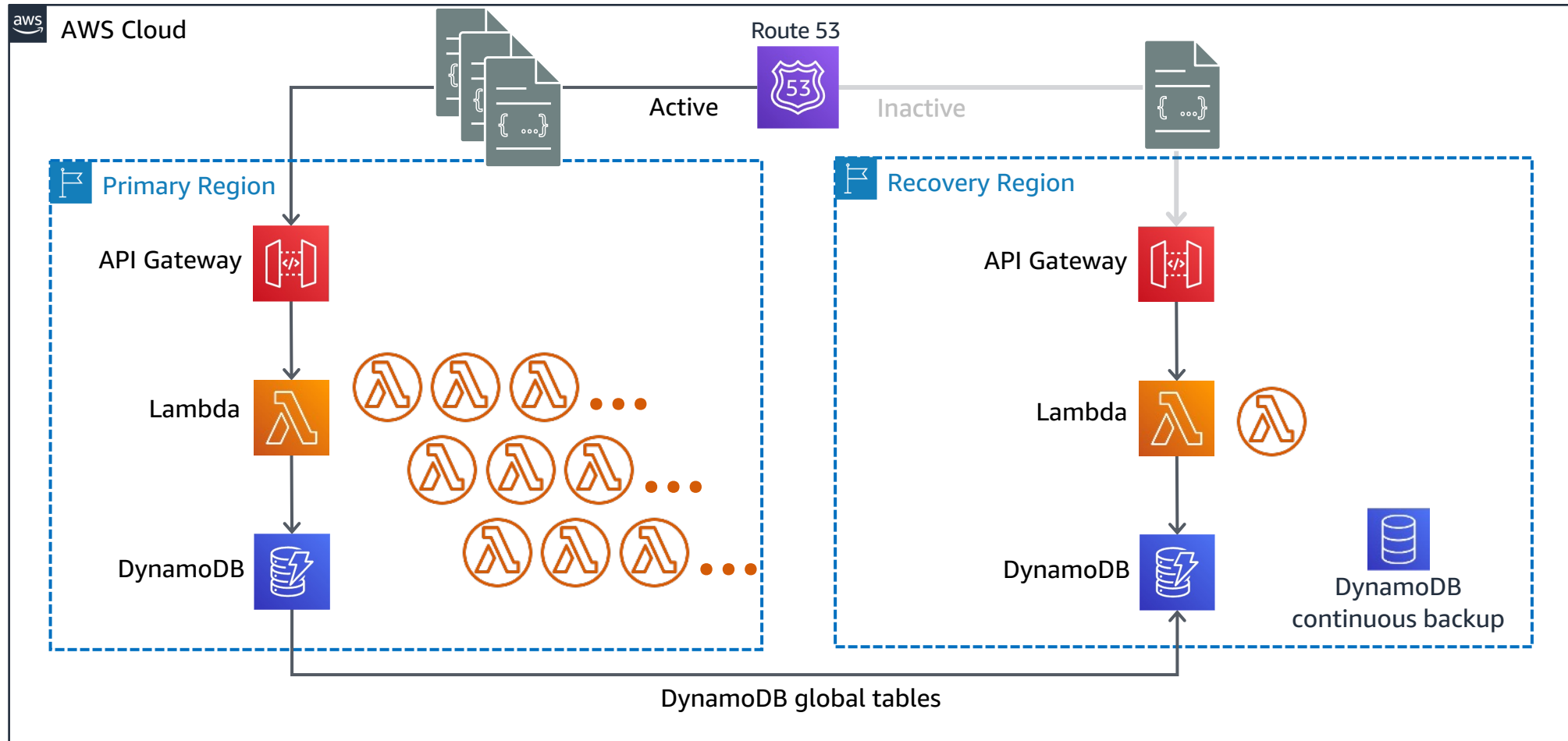
- Define recovery objectives for downtime and data loss
- Use defined recovery strategies to meet the recovery objectives



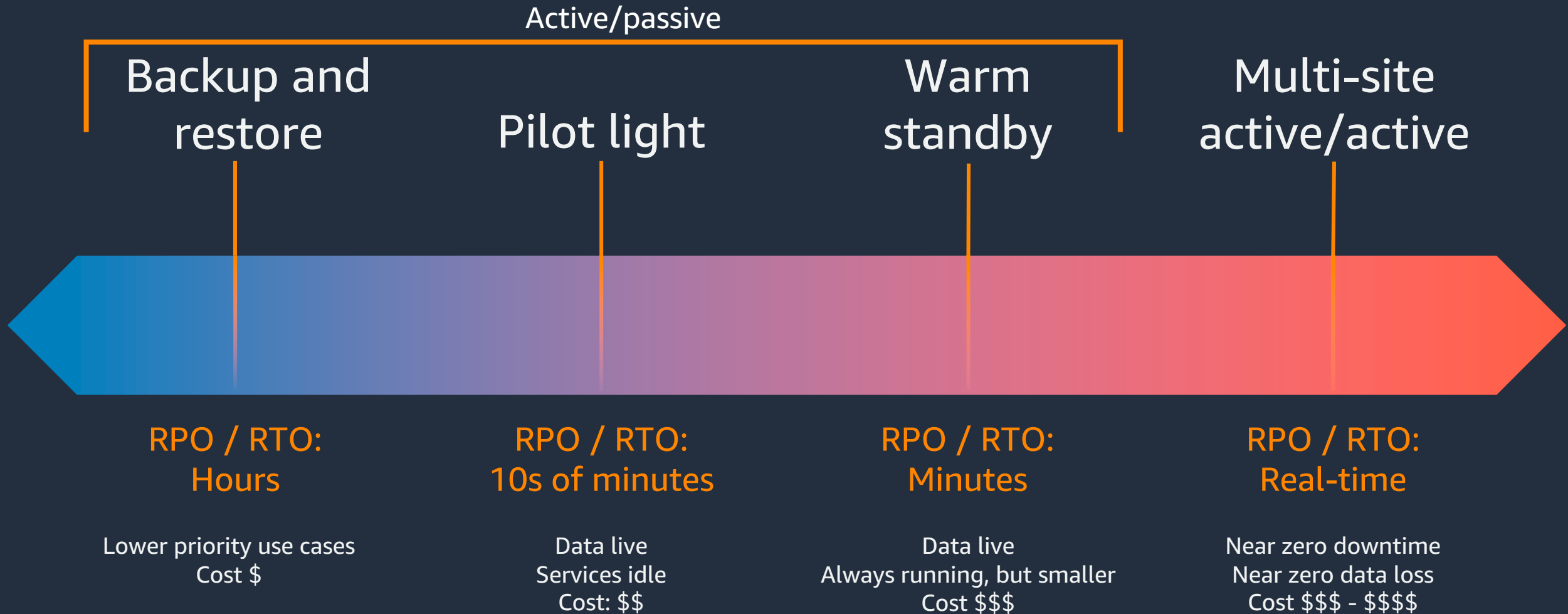
Serverless

PERF BP:

- Aware of service quotas and constraints
- Manage service quotas across accounts and regions



Strategies for disaster recovery



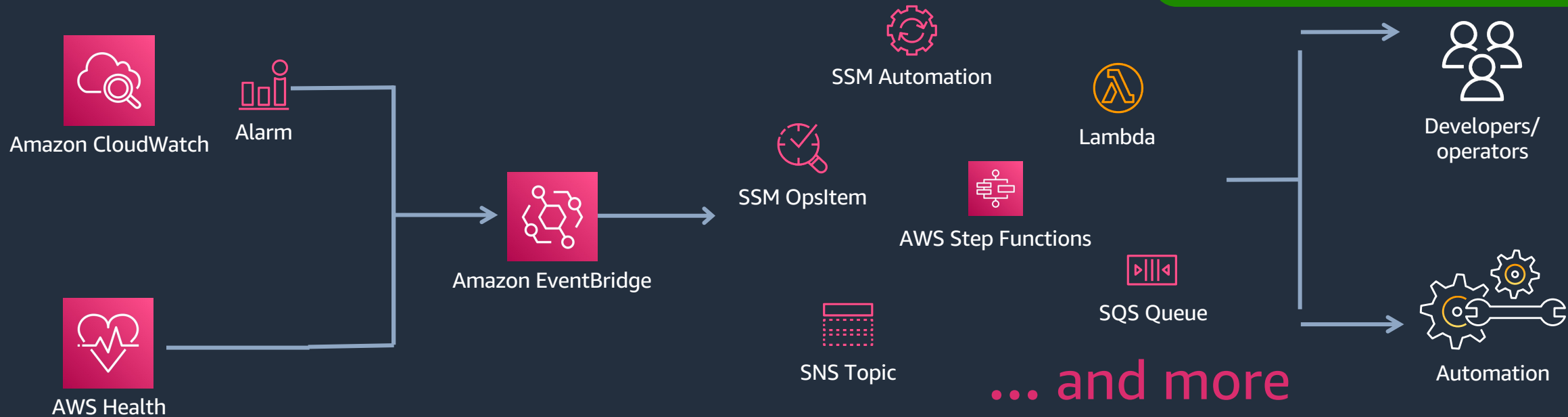
Continuous improvement



AWS monitoring and automation

REL BPs:

- Send notifications – alarming
- Automate responses



```
{
  "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"]
  }
}
```

Steady state: Assessing reliability in real-time

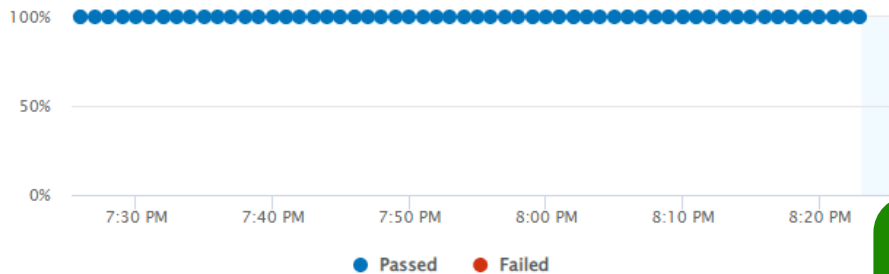
- Your app is steady state if it is operating reliably and as expected
- Not necessarily no impact – impact is within acceptable limits

Canary runs

View Canary troubleshooting documentation for additional information. [Learn more](#)

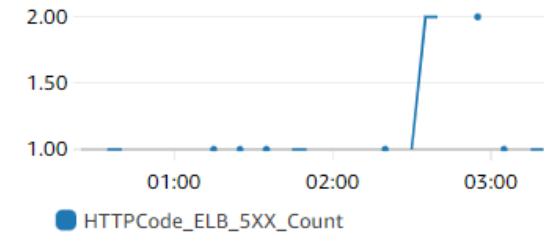
Each point represents a canary run. Click each data point for details.

1 hour ▼



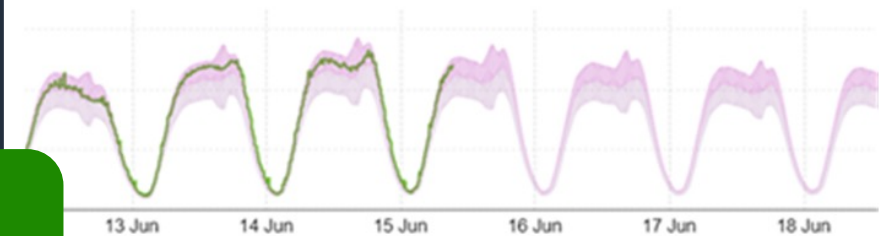
HTTPCode_ELB_5XX_...

No unit



Orders on Amazon.com

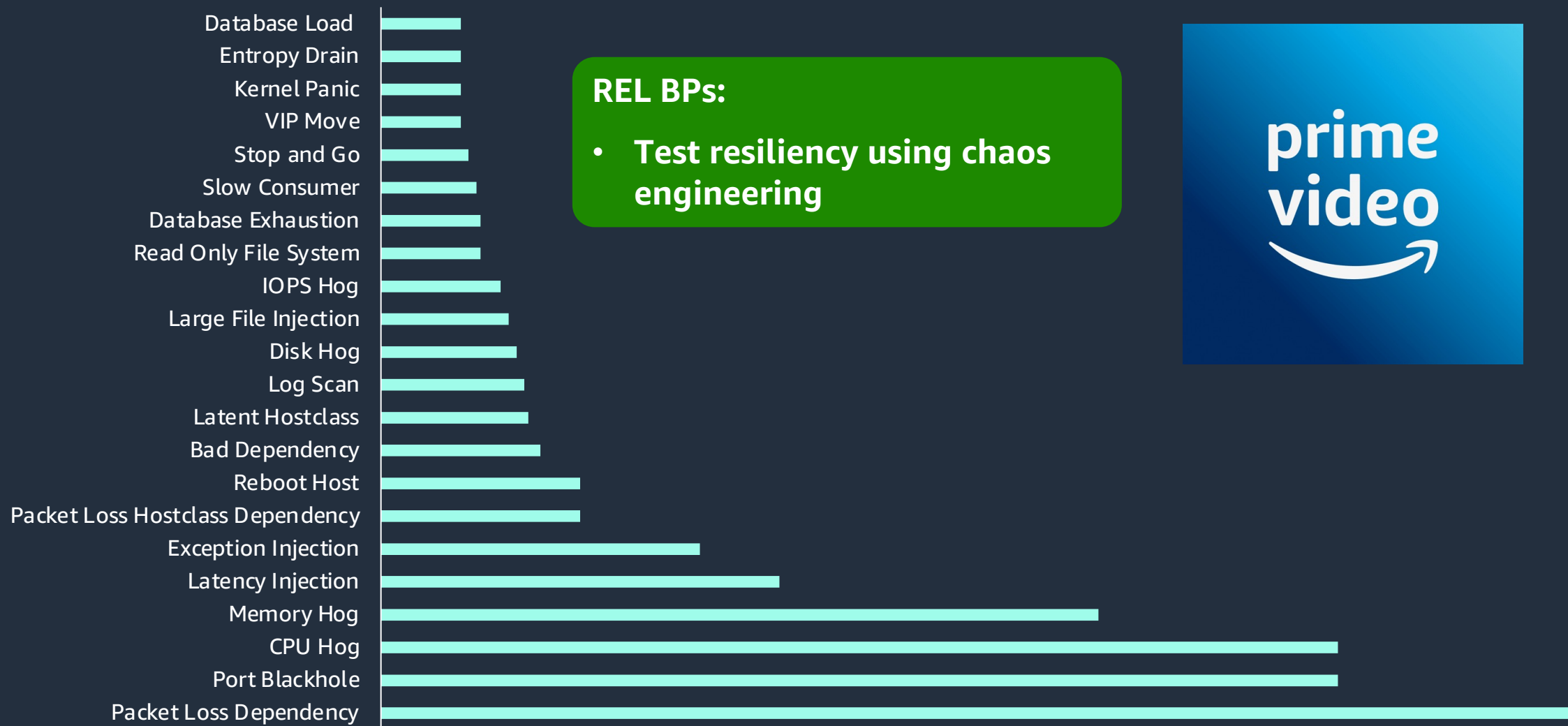
— Actuals
— Prediction



REL BPs:

- Define and calculate metrics
- Send notifications - alarming

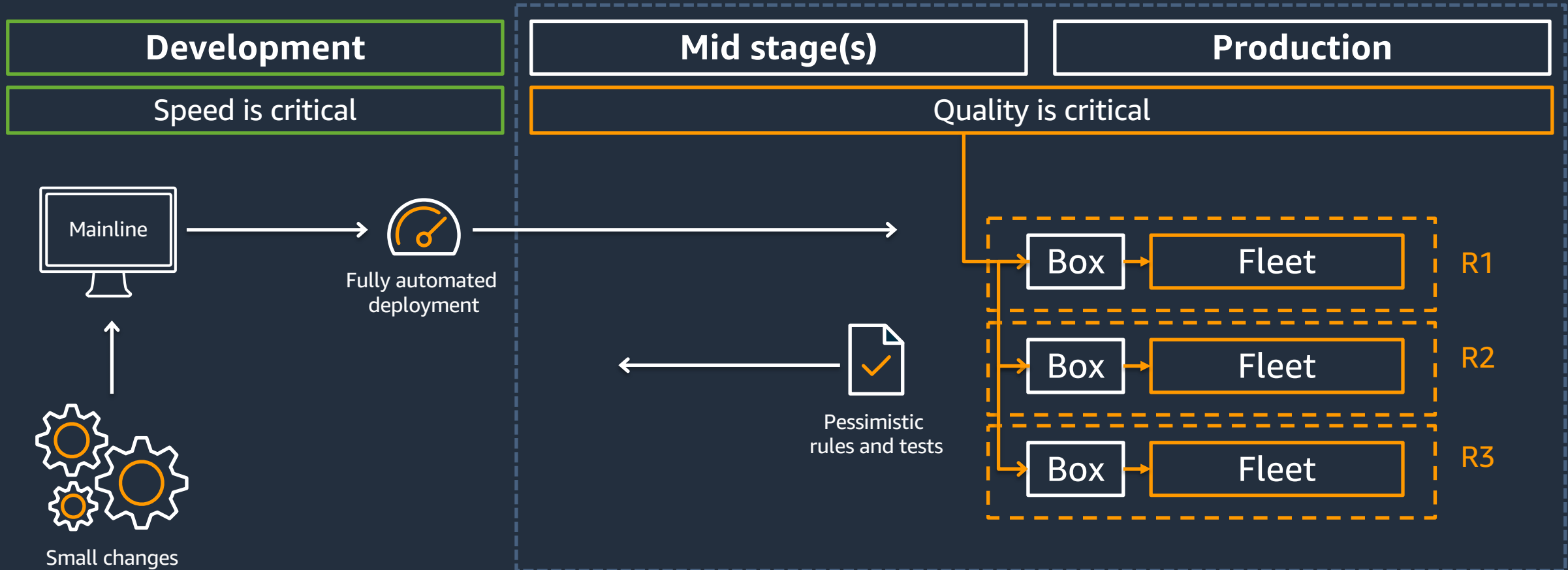
Chaos engineering: Failure injection at Prime Video



Deployment

REL BPs:

- Deploy Changes with Automation
- Integrate testing as part of deployment



Well-Architected Framework is a set of best practices



Whitepapers



AWS Well-Architected Tool



Best practices



Blogs and presentations



Labs

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!

Alex Markley

awsalex@amazon.com

Vishal Lakhotia

lakhov@amazon.com

Please take the session
survey:



Track: Application modernization,
security, and governance

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