

AWS ARCHITECTURAL RESILIENCE

Copebit Meetup

Michael Schmid

Area Partner Solution Architect

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Q: How do we build systems that will never fail?

A: Systems will always fail. It’s what happens when systems fail that matters.

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Definitions

Reliability

Ability of a workload to perform its required function correctly and consistently…

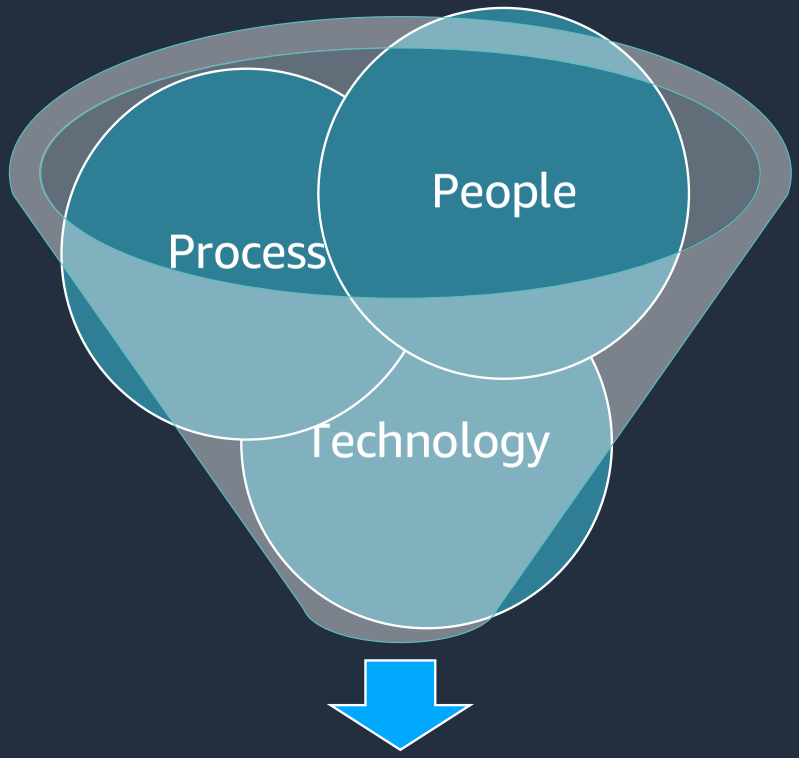
Resilience

Ability of a workload to recover from infrastructure or service disruptions…

– Reliability Pillar, AWS Well-Architected Framework

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

People, Process and Technology



PRO TIP

Most customers start with technology. But, without people and process, the tech doesn't matter. Testing and validation are crucial.

aws
© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resilience

ABILITY OF A WORKLOAD TO RECOVER FROM INFRASTRUCTURE OR SERVICE DISRUPTIONS

The mental model

High availability

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



Core services, design goals to meet availability goals

Disaster recovery

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



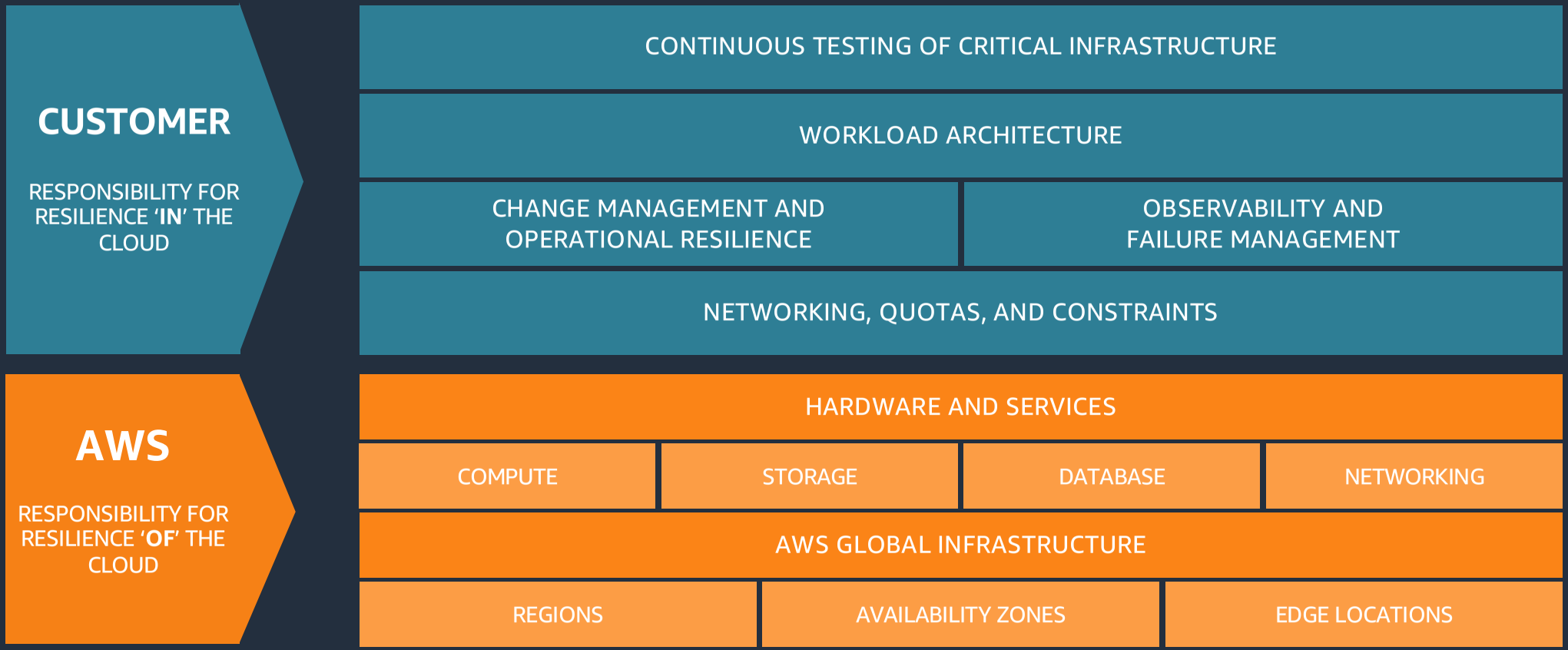
Backup and recovery, data bunkering, managed recovery objectives

Continuous improvement

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

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

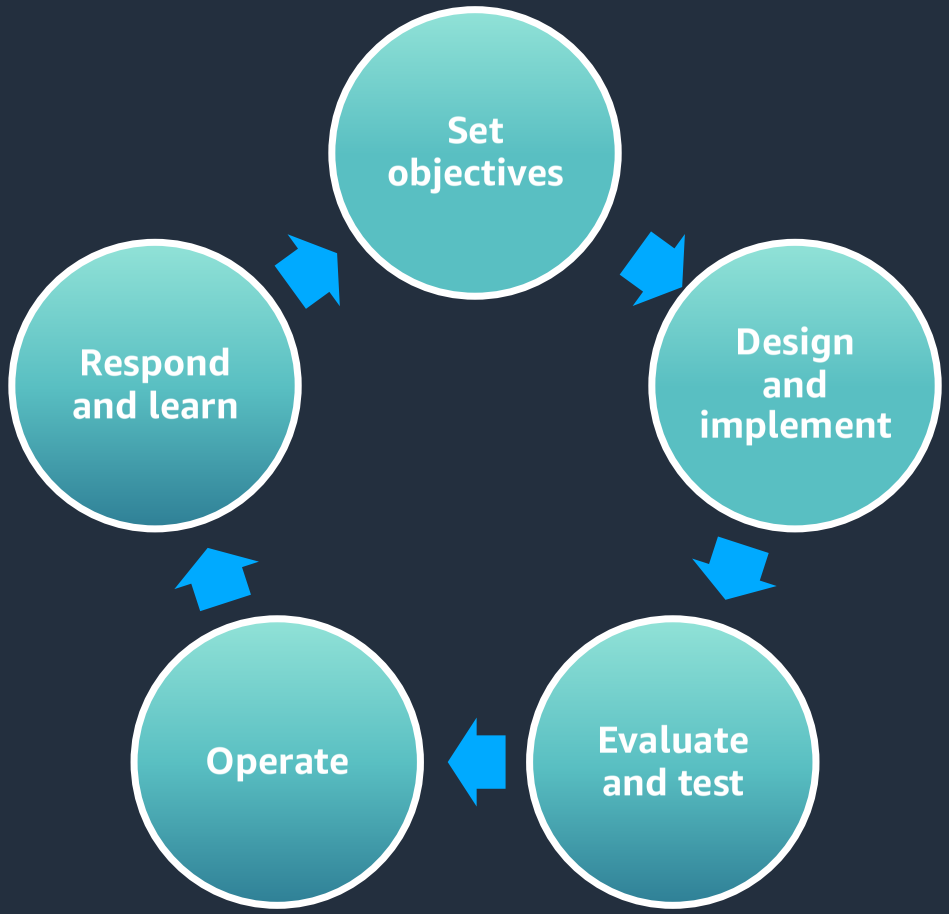
Shared Responsibility for Resilience



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resilience ‘in’ the Cloud

RESILIENCE LIFECYCLE FRAMEWORK



Key Outputs

- Identified priorities
- Better operational practices
- Learning/mitigation capabilities

aws
© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The resilience lifecycle

Set objectives	Design and implement	Evaluate and test	Operate	Respond and learn
• Workload prioritization and tiering • Objective metric identification • Historical event tracking	• Architecture recommendations • Foundational resilience services and features • Dependency mapping • Operational readiness reviews • CI/CD • Backup and disaster recovery	• Risk evaluation • Tracing • Performance benchmarking • Chaos engineering • Load testing • A/B testing • Functional test • Portfolio reporting	• Live traffic • Canary traffic • Alarming • Operational reviews • Ticketing systems • Anomaly detection • Monitoring	• Auto remediation • Alarm tuning • Escalation path • Runbooks • Event management • Correction of errors • Incident knowledge base

Key outputs

- Identified priorities
- Better operational practices
- Learning/mitigation capabilities

aws

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Developing a new operating model

Reactive → Proactive → Ingrained







Resilient standards and patterns	Architecture and design principles	Deployments and automated checks	Validate and operate	Recovery and realign
Set objective	Design and implement	Evaluate and test	Operate	Respond and learn

aws

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Set Objectives



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The Business Impact of Failure

WHAT ARE THE RISKS?

Animation studio deleted almost completed movie

Studio had backups, but they had failed to work for the past month. (Independent)

Global community platform lost $8.2M in revenue due to an outage (Reuters)

A leading U.S. airline lost $150M in profits due to an outage (Forbes)

Average hourly cost of infrastructure failure is $100K per hour among Fortune 1000 (IDC)

aws

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traditional Resilience Model

Tier	Availability	Loss Impact	RTO/RPO
Silver	99.95%	Standard business systems	24 Hours/12 Hours
Gold	99.99%	Mission/Safety/Security/Business Critical	1 Hour / 30 Minutes
Platinum	99.995%	National/Critical infrastructure	15 Minutes / 1 Minute

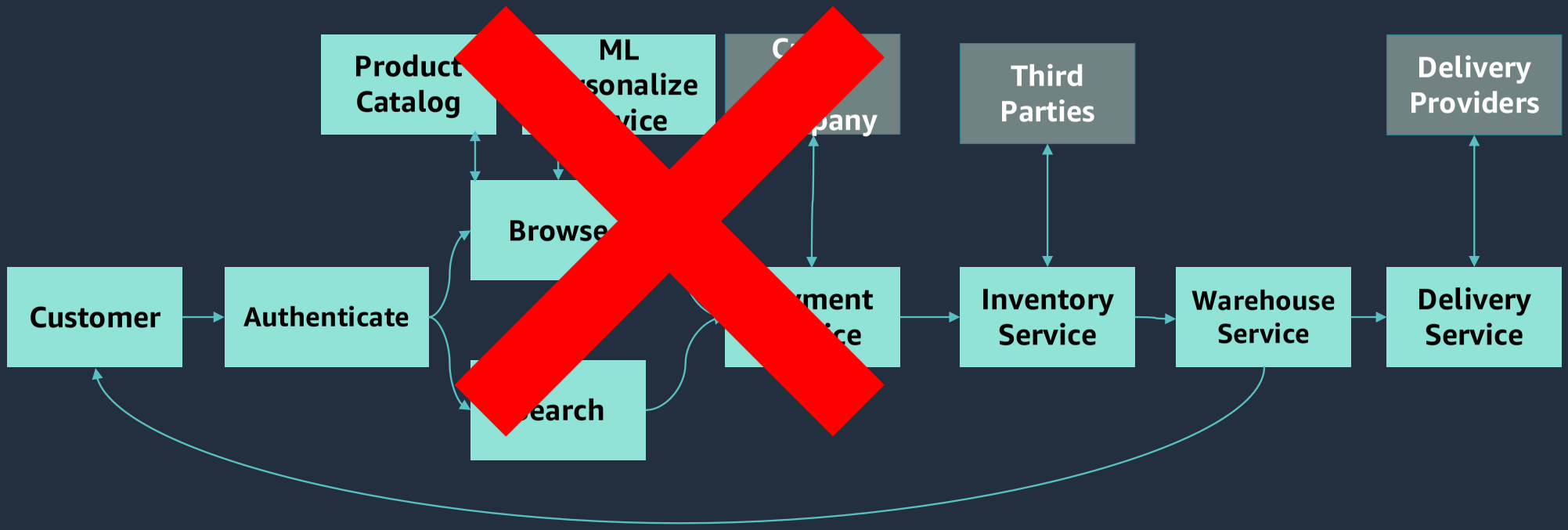
PRO TIP

Customers typically use a combination of **revenue, regulation, and reputation** to define these. This may typically be done through a risk ranking business function.

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Impact – Entire System

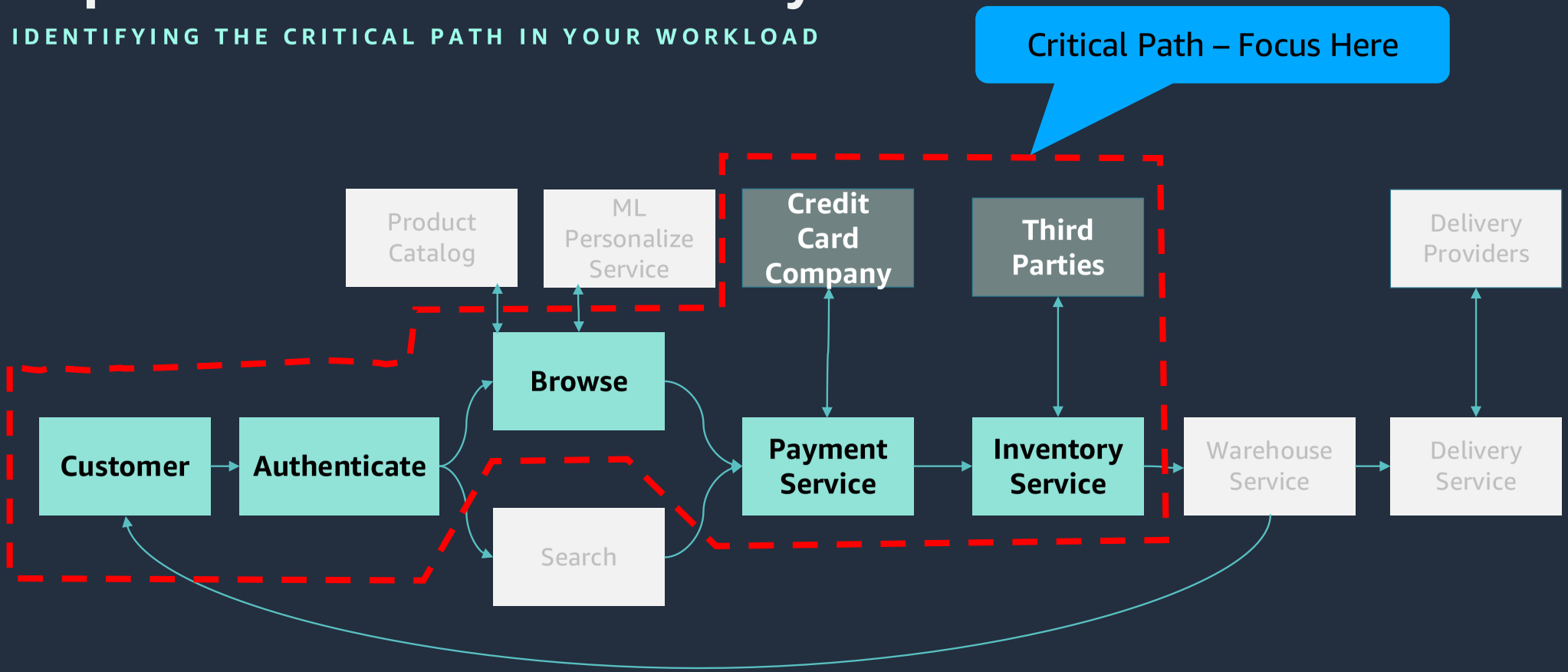
ORDER MANAGEMENT SYSTEM



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Impact – Critical User Journey

IDENTIFYING THE CRITICAL PATH IN YOUR WORKLOAD



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resilience Trade-offs

Cost & effort



Complexity



Operational burden

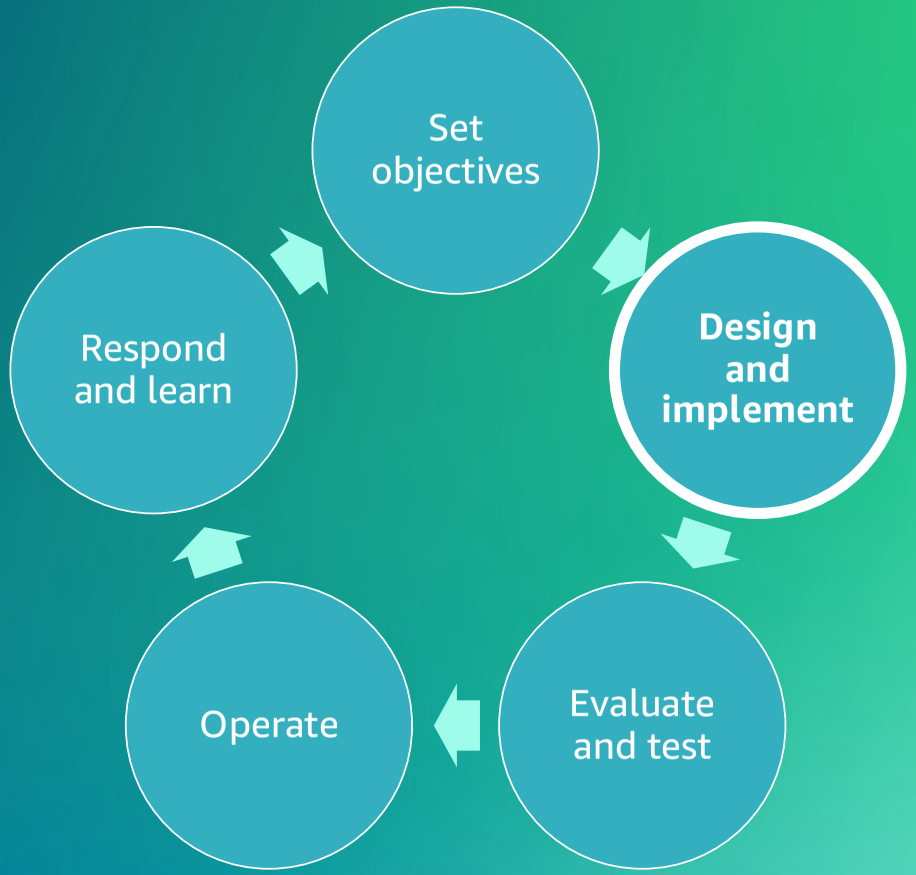


Consistency & latency



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Design and Implement



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Desired Resilience Properties



Timely output



Correct output



Fault isolation



Sufficient capacity



Redundancy

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resilient Software Design Patterns

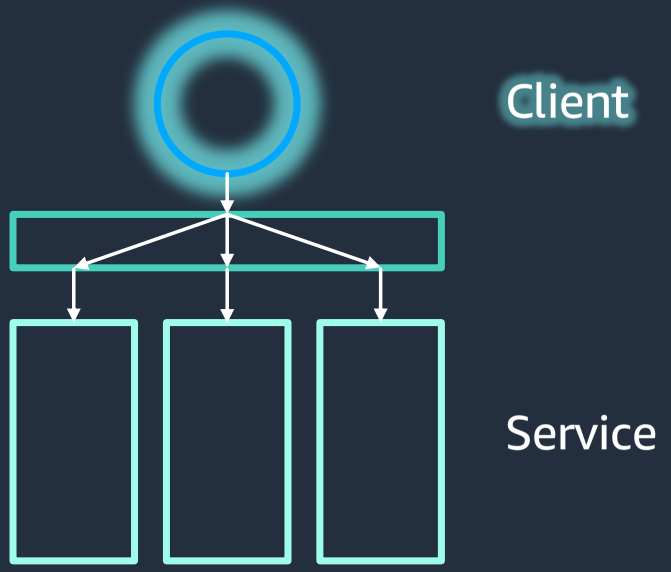


© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Failure-oriented Patterns

Client (Front-End)

- Timeouts
- Retries w/back off
- Jitter
- Limit queue sizes
- Caching

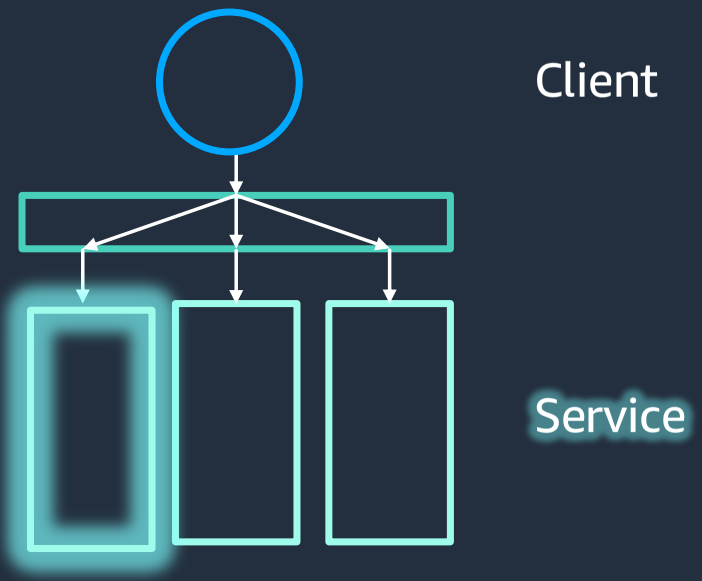


© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Failure-oriented Patterns

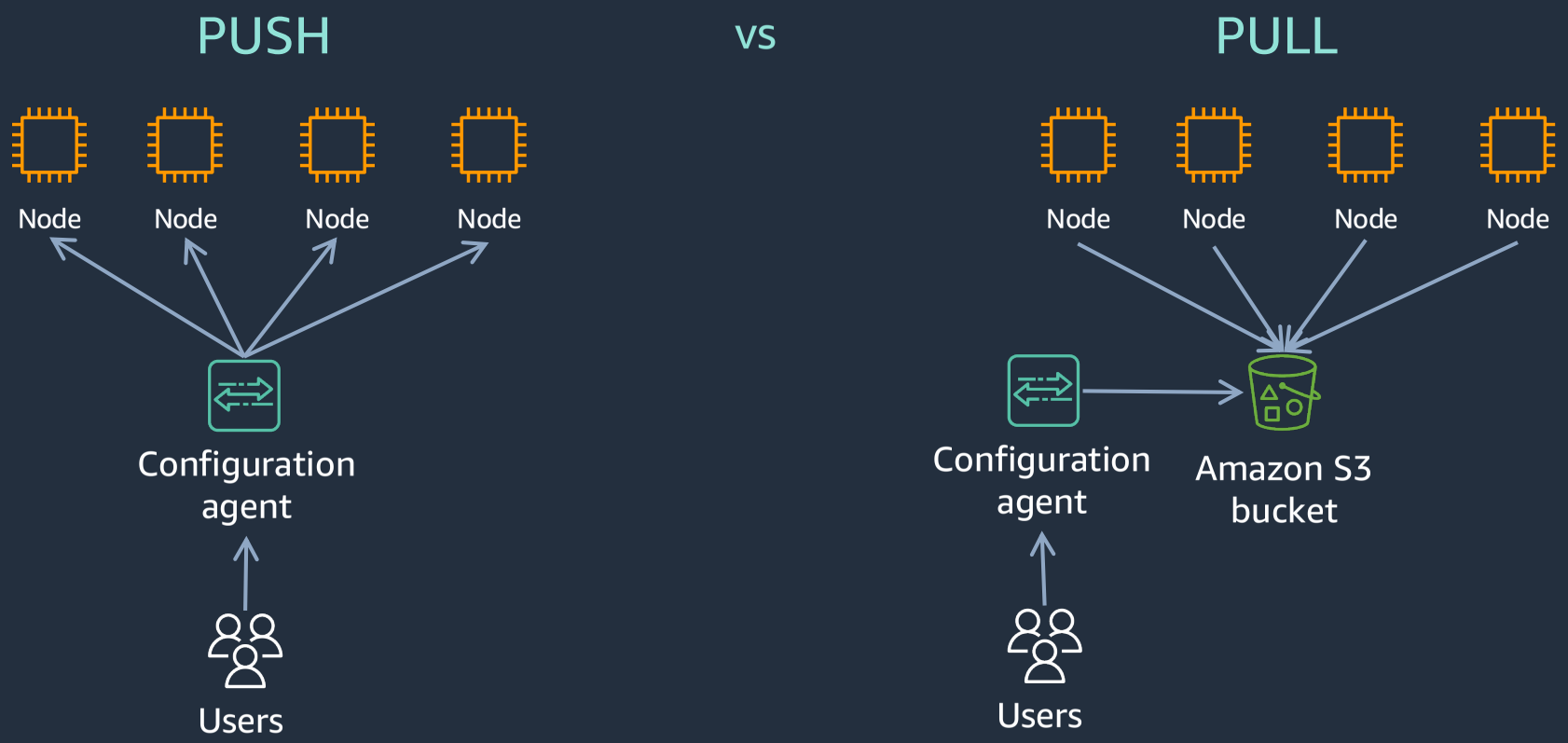
Service (Back-End)

- Rate limit
- Rejection (load shedding)
- Caching
- Circuit breaker



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

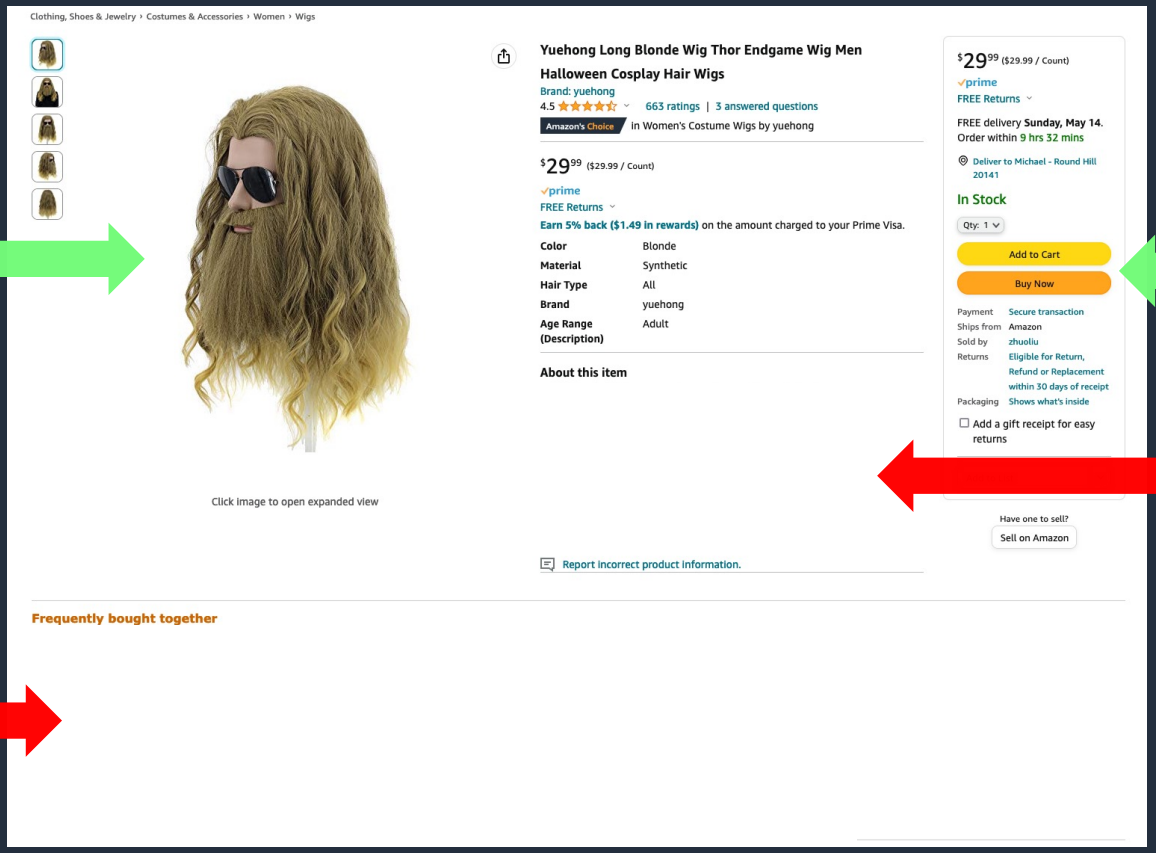
Simple Designs and Constant Work



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Graceful Degradation (Static Stability)

Can still browse images



Can still add to cart

Missing the item description

Missing frequently bought together

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Avoid Bimodal – Fallback Processing

Prevent bimodal behavior:

Bimodal behavior is when your workload exhibits different behavior under failure modes




```
try paypal.pay(who, howMuch) :
   # paypal processing
exception:
   # venmo processing
   venmo.pay(telNo, howMuch, fromWhere) :
```

Convert to something that regularly exercise both paths

```
if mod(requestNum, 100) == 0:
   venmo.pay(telNo, howMuch, fromWhere)
else
   paypal.pay(who, howMuch)
   exception:
      venmo.pay(telNo, howMuch, fromWhere)
```

aws
© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

https://aws.amazon.com/builders-library/avoiding-fallback-in-distributed-systems/?did=ba_card&trk=ba_card

Resources



Reliability Pillar: AWS Well-Architected Framework



Amazon Builder’s Library



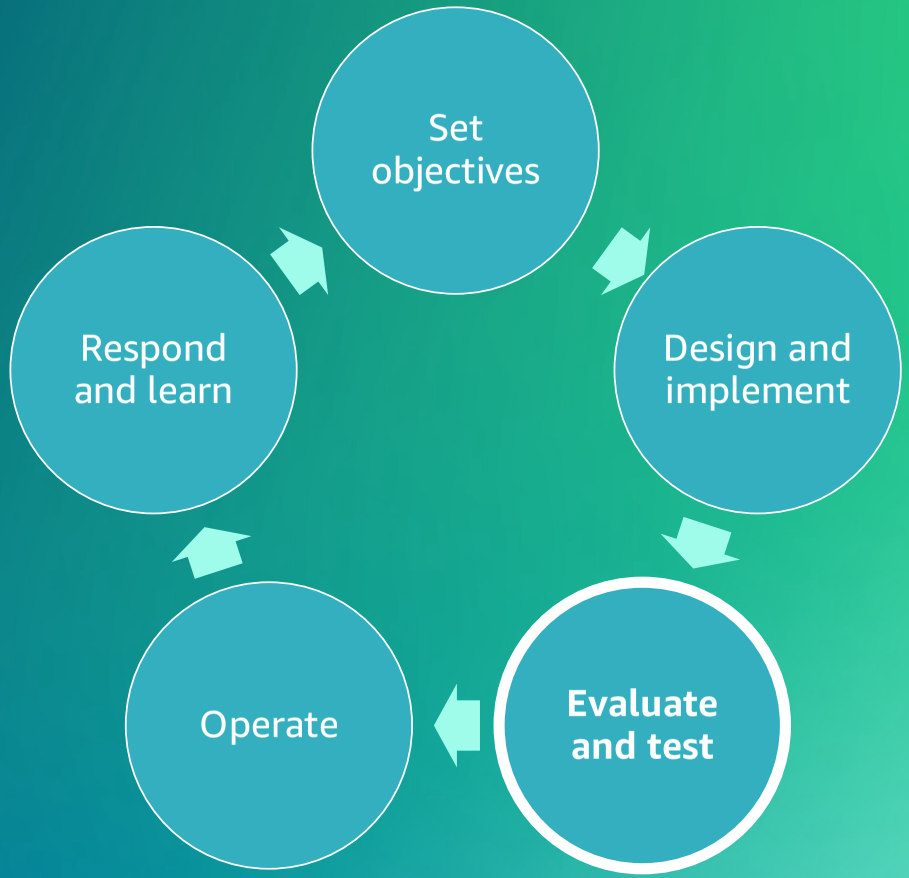
Advanced Multi-AZ Resilience Patterns



AWS Fault Isolation Boundaries

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Evaluate and Test



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traditional Tests

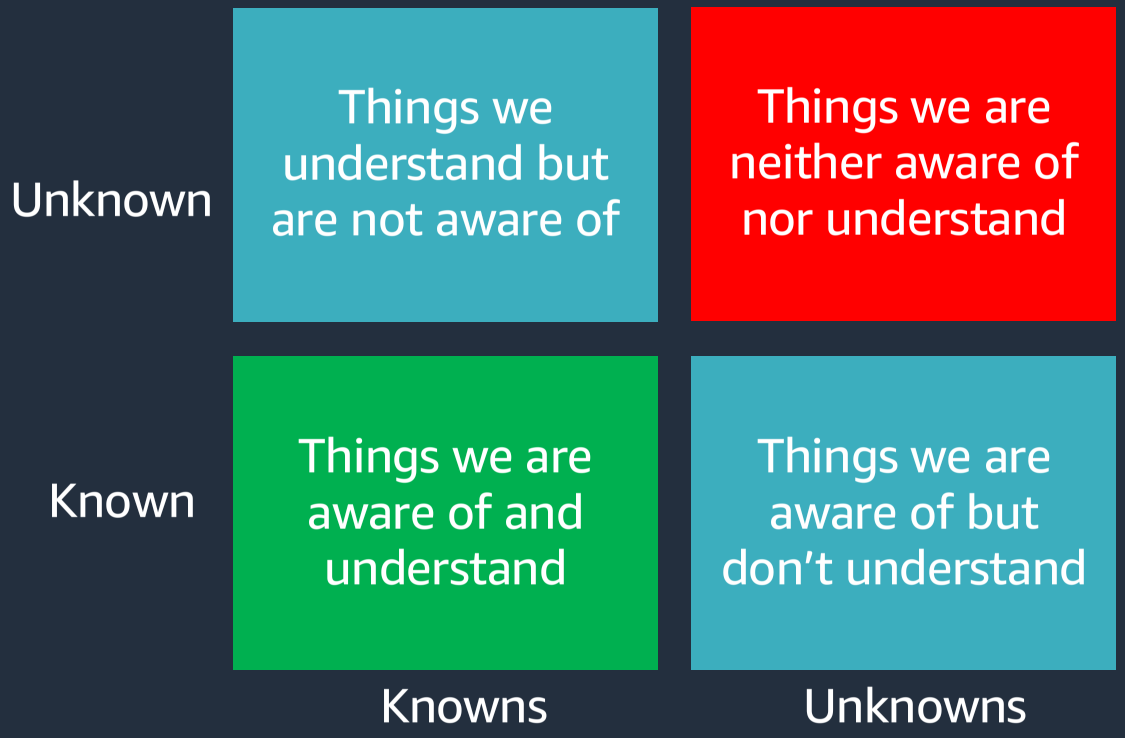
Type of tests:

- Unit
- Integration
- Functional
- Performance and load
- Smoke
- Regression

AUTOMATE

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Chasing The Unknowns in Your Environments

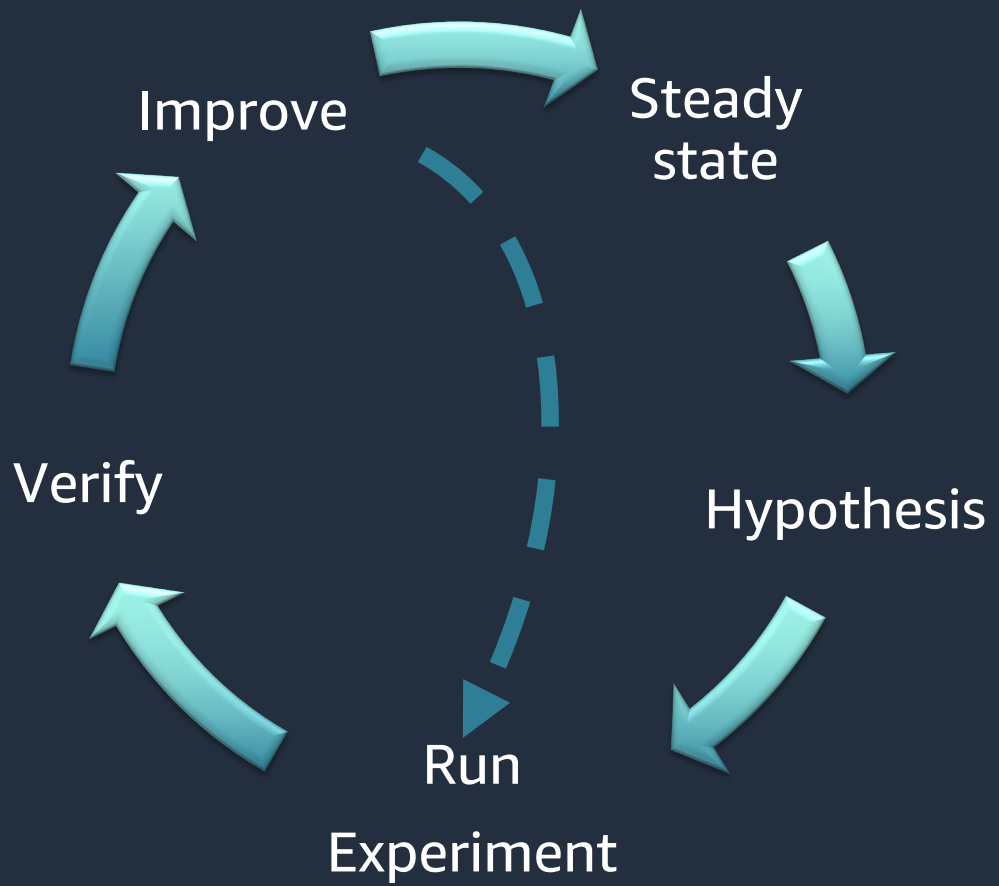


PRO TIP

Customers often ask what key things they should measure to understand when a system is becoming impaired. You should test for known and unknown conditions to identify and refine what you **should** measure.

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Chaos Engineering



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Typical Chaos Experiment

Inject events that simulate:

- Hardware failures, like servers dying
- Software failures, like malformed responses
- Nonfailure events, like spikes in traffic or scaling events
- Of-the-cloud impairments

Any event capable of disrupting steady state



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Chaos Experiment Definition - Hypothesis

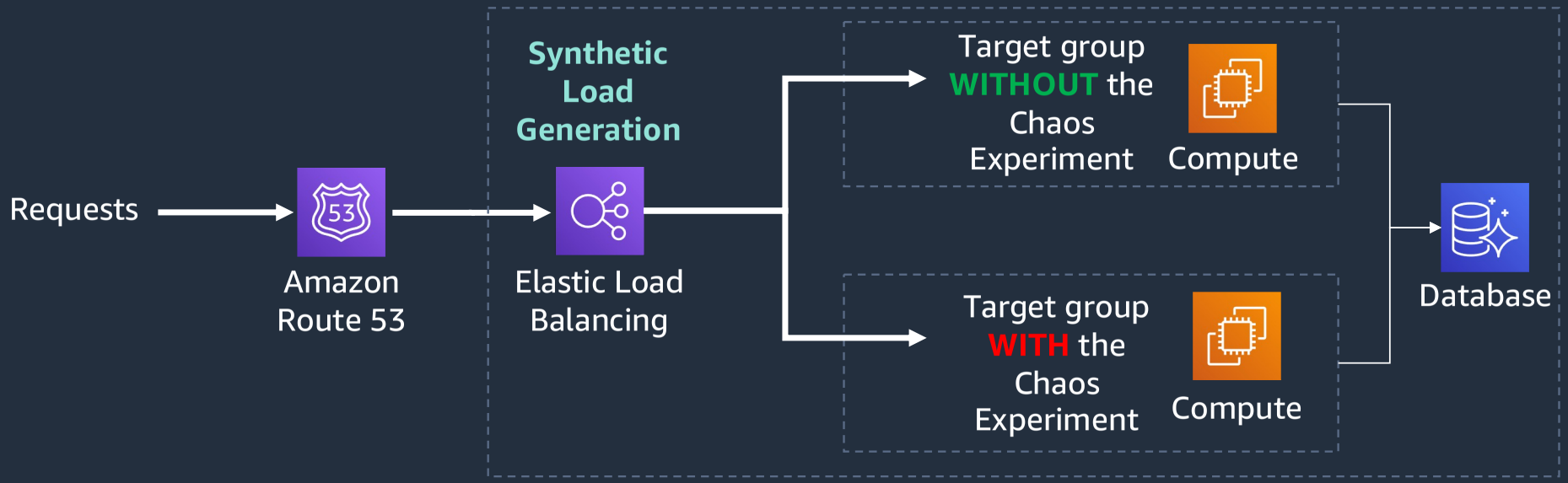
At a rate of 300 TPS, if 40% of the nodes in the EKS node-group are terminated, the Transaction Create API continues to serve the 99th percentile of requests in under 100 ms (steady state)

The EKS nodes will recover within 5 minutes, and pods will get scheduled and process traffic within 8 minutes after the initiation of the experiment

Alerts will fire within 3 minutes

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Controlled Experiments Through Canary Deployments

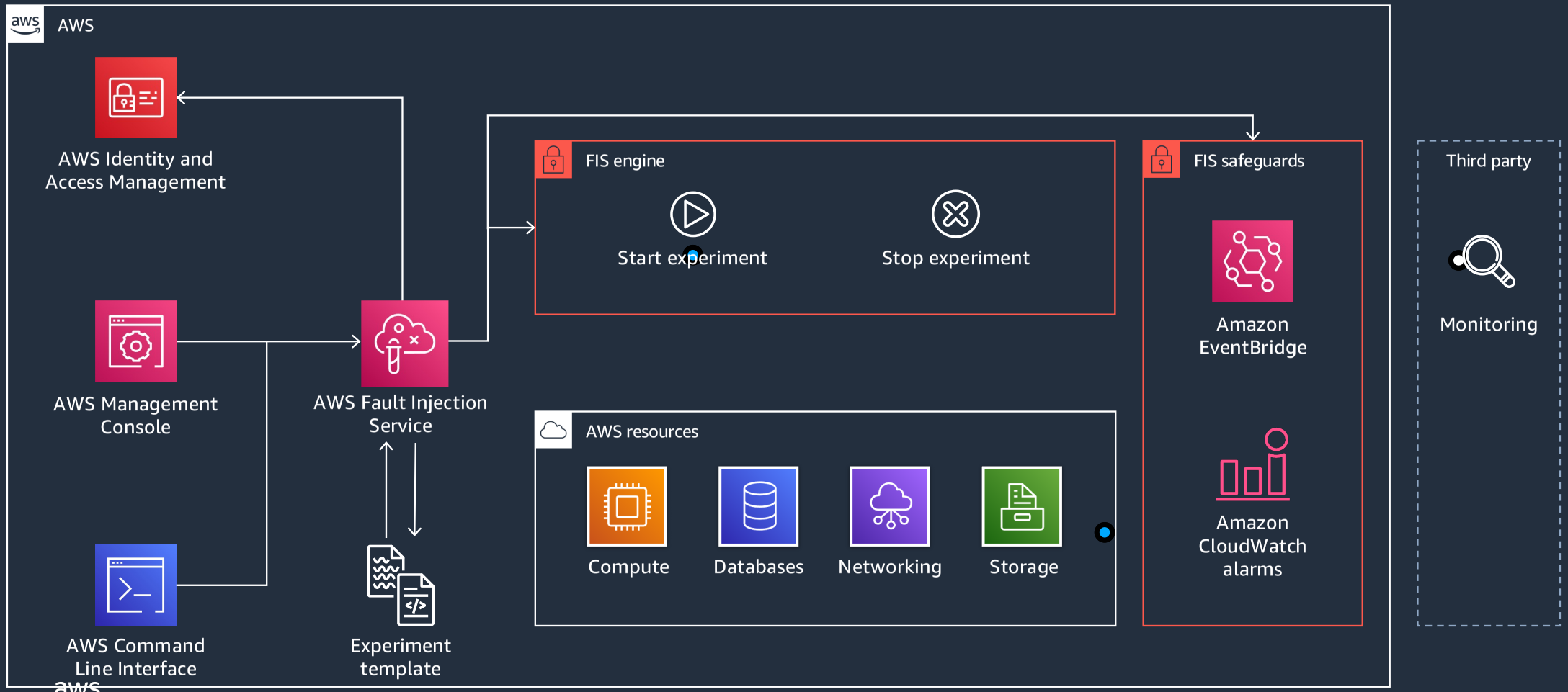


Verify that both groups are healthy before moving forward

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Source: https://medium.com/@adhorn/chaos-engineering-q-a-how-to-safely-inject-failure-ced26e11b3db

AWS Fault Injection Service

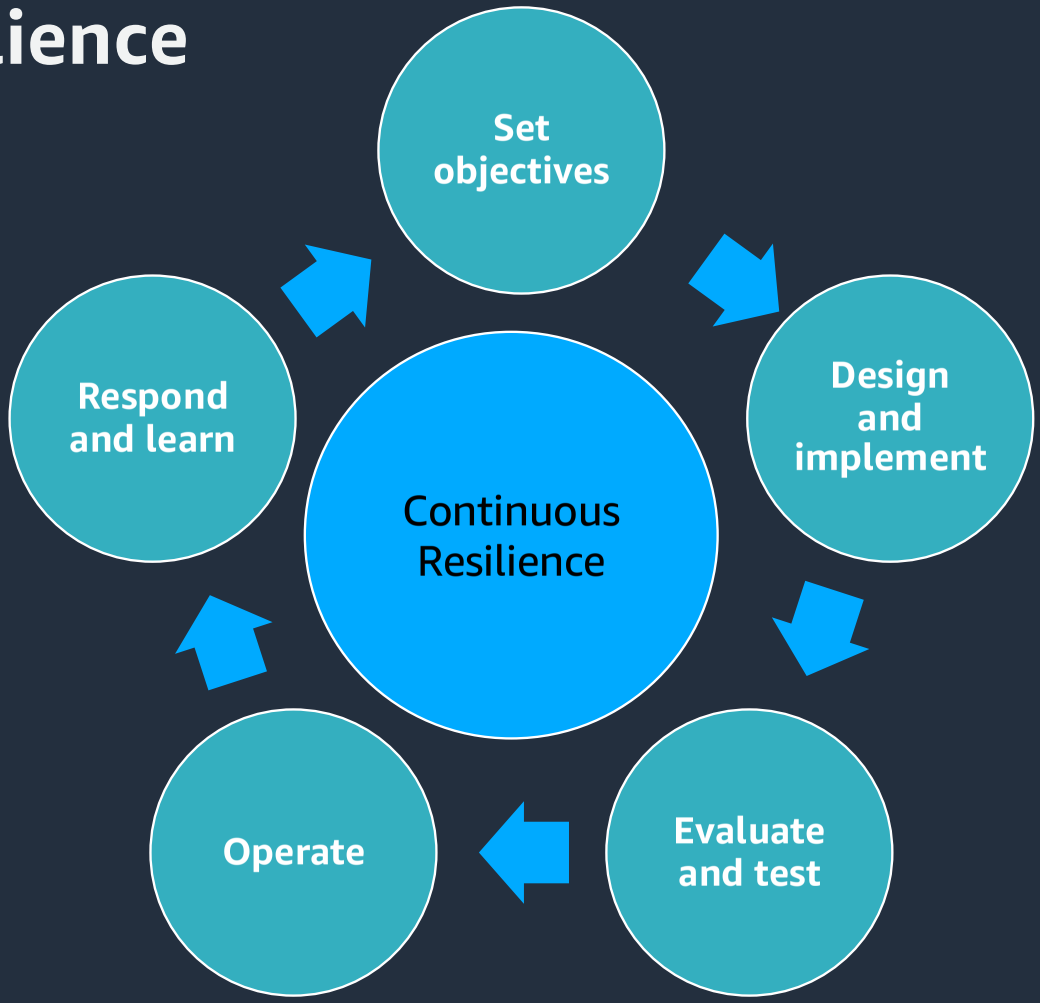


© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Continuous Resilience

PRO TIP

Resilience is a continuous journey. Don't 'set it and forget it'. People and technologies are ever changing. Make sure your resilience changes with them.



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Read the lifecycle whitepaper



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources



Building Resilience One Step at a Time



Learn how the Flexibility of AWS Opens New Doors for Business Continuity



AWS Resilience Hub

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Thank you!

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.