Resilience on AWS
Using the shared responsibility model
What is your plan?
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
# Shared responsibility for resilience

<table>
<thead>
<tr>
<th>CUSTOMER</th>
<th>AWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESPONSIBILITY FOR RESILIENCE ‘IN’ THE CLOUD</td>
<td>RESPONSIBILITY FOR RESILIENCE ‘OF’ THE CLOUD</td>
</tr>
</tbody>
</table>

## AWS Global Infrastructure
- **Regions**
- **Availability Zones**
- **Edge Locations**

## Hardware and Services
- **Compute**
- **Storage**
- **Database**
- **Networking**

## AWS Shared Responsibility
- **Continuous Testing**
- **Workload Architecture**
- **Change Management**
- **Failure Management**
- **Quotas, and Constraints**
AWS responsibility / Customer responsibility

**EC2**
- Local disk (Instance store)
- **CUSTOMER**
  - Backup
  - Scaling
  - Multi-zone replication
  - Security config and updates
  - Patching
  - Operating system config and maintenance
- **AWS**
  - Physical hardware, software, networking, and facilities

**Amazon S3**
- Serverless object storage
- **CUSTOMER**
  - Backup
- **AWS**
  - Physical hardware, software, networking, and facilities

© 2023, Amazon Web Services, Inc. or its affiliates.
A model for resilience

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

**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 operations within specific targets at an recovery site for failures that cannot be handled by HA

- Backup & Recovery, Data Bunkering, Managed RPO/RTO

**Continuous Improvement**
Moving beyond pre-deployment testing towards chaos engineering patterns
Resilience of the Cloud
Cloud is an abstraction on top of physical infrastructure
AWS Regions and Availability Zones (AZs)

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

- **32 AWS Regions worldwide**
- Each AWS Region has multiple AZs
- Each AZ includes one or more discrete data centers

A Region is a physical location in the world, housed in separate facilities, with redundant power, networking, and connectivity.
Resilience ‘of’ the cloud

A CULTURE BUILT AROUND RESILIENCE

Service ownership model
Incentivizes continuous improvement of operations

Operational Readiness Reviews (ORR)
Ensures compliance to best practices prior to a service launch

Safe, continuous deployment
Minimizes impact on production caused by faulty deployments

Correction of Error (CoE) processes
Helps teams understand the root cause and prevents reoccurrence
Service Ownership Model

Two-pizza teams are fast and agile, fostering ownership and autonomy

Small, decentralized, nimble teams

Own and run what you build
Anatomy of an Operational Readiness Review (ORR)

Uses the learning from COEs and other operational experience

**System Architecture**
- API diagram and workflow
- Retry/back-off strategy
- Dependencies?

**Release Quality and Procedures**
- What mechanisms do you use to deploy?
- Automatically roll back incorrect deployments?

**Incident and Event Management**
- What operational goals have you identified?
- Preventive measures?
Safe, continuous deployments

Load balancer

One-box

Completed

In progress

To do

Production One-Box
Correction of error (COE)

- Objective deep dive into customer impacting events
- Blameless - Conducted with a learning mindset
- Senior leader engagement

- Generates action items
Weekly operations review

Senior leadership + Open to every engineer

• Success stories
• Metrics review (The Wheel)
• COE review
• What can improve?

Open to every engineer, leader
Resilience in the Cloud
Building a modern reality: resilient architectures

- Extreme automation everywhere
- Continuous resilience of unknowns
- Integrated observability beyond infrastructure

Make frequent small changes

Low Frequency High
AWS Well-Architected: Best practices across six pillars

Operational Excellence
Security
Reliability
Performance Efficiency
Cost Optimization
Sustainability

AWS Well-Architected
https://aws.com/well-architected
Well-Architected is a Set of Best Practices
Resilience in AWS Well-Architected

Operational Excellence

Reliability
Reliability pillar

- Automatically recover from failure
- Test recovery procedures
- Scale horizontally to increase aggregate workload availability
- Stop guessing capacity
- Manage change in automation

Resources

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

Labs: Well-Architected Reliability
wellarchitectedlabs.com/reliability

AWS blog posts
buildon.aws/tags/resilience
aws.amazon.com/blogs/architecture/tag/resilience
aws.amazon.com/blogs/architecture/tag/disaster-recovery

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

Please complete the survey