AWS Resilience Immersion Day

Mandeep Singh
Principal PDS, Resilience

Natarajan Elayappan
Sr Partner Solution Architect

Puneet Arora
Sr Partner Solution Architect

Sankar Cherukuri
Partner Solution Architect

AWS Resilience Immersion Day Agenda

Schedule	Topic	Type
11:00 - 11:10	**Introduction**	
11:10 - 11:30	**Prepare and Protect Your Applications From Disruption with AWS Resilience Hub**	Presentation
11:30 - 12:00	**Disaster Recovery Strategy Overview**	Presentation
12:00 - 12:30	**Lunch**	
12:30-13:30	**Prepare and Protect Your Applications From Disruption with AWS Resilience Hub**	Lab
13:30-13:40	**Break**	
13:40-14:10	**AWS Elastic Disaster Recovery**	Presentation
14:10-15:00	**AWS Elastic Disaster Recovery**	Lab

Prepare and Protect Your Applications From Disruption

with AWS Resilience Hub

Natarajan Elayappan
Sr Partner Solution Architect

Agenda

- Why Is Resilience So Important?
- The problem AWS Resilience Hub solves
- AWS Resilience Hub – Use Cases
- AWS Resilience Hub Supported Resources
- How AWS Resilience Hub Works ?
- Workshop

Why Is Resilience So Important ?

“Failures are a given, and everything will eventually fail over time.”

Werner Vogels

CTO, Amazon.com

The Cost of Downtime

$1.25 to $2.5B

Annual Fortune 1000 app downtime costs (IDC)

$474K

Cost/hour of downtime (IDC)

$500K to $1M

Cost/hour of a critical app failure (IDC)

$100K

Cost/hour of an infra. failure (IDC)

What are the categories of failure which affects your application downtime ?

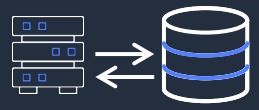
Categories of Failure

Code deployments & configuration

e.g. bad deployment, cred expiration

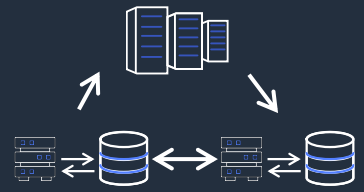
Core infrastructure

e.g. datacenter failure, host failure



Data and state

e.g. data corruption



Dependencies

e.g. infrastructure, external APIs

Highly unlikely scenarios

e.g. All of internet failure, environmental disasters,

Challenge – Enabling Resilience

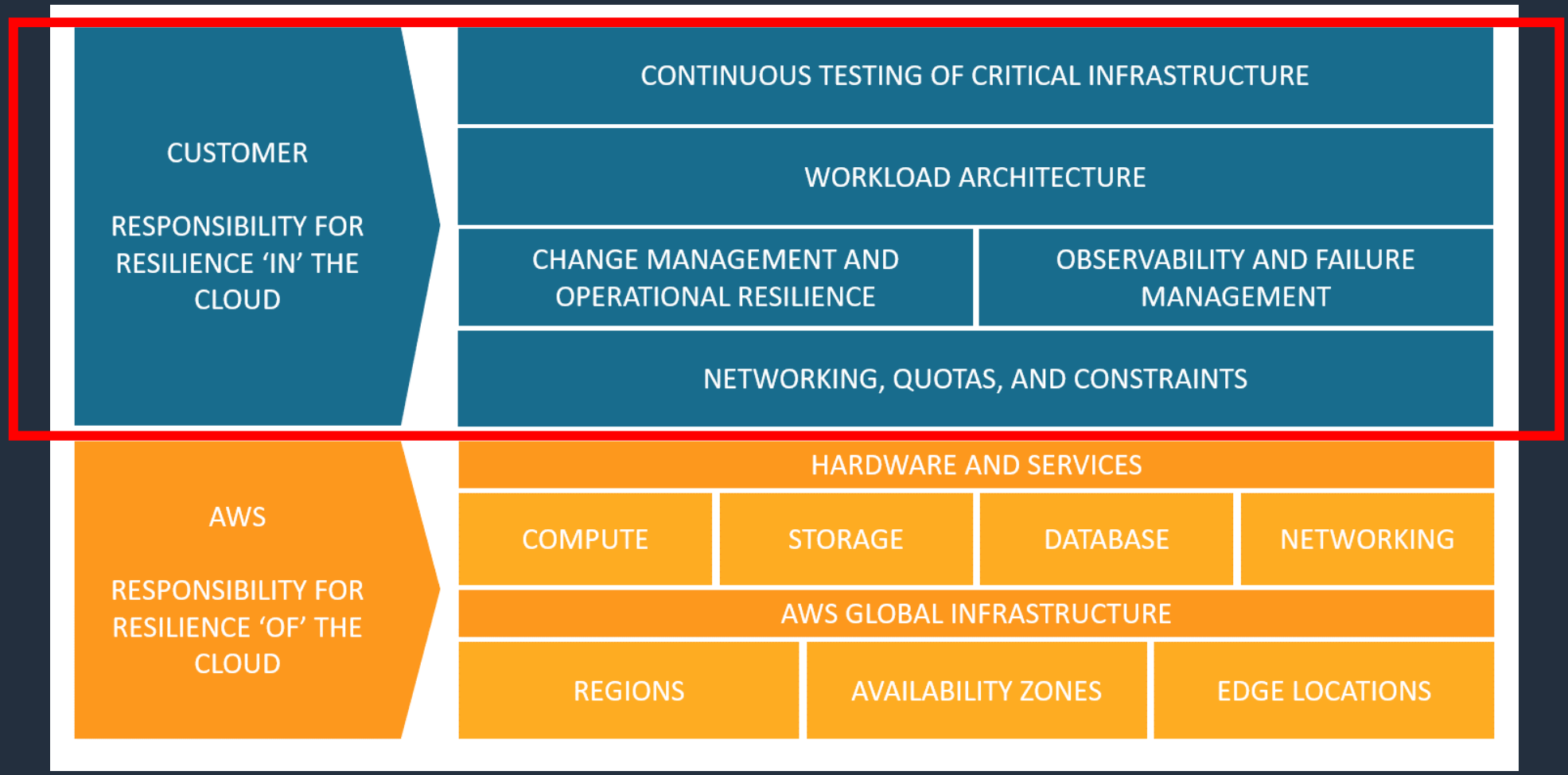
Business

- Potential high overhead costs
- No defined resilience policies

Technical

- Difficult to prioritize (where do I start?)
- Lack of centralized monitoring and testing
- Ambiguity

Shared Responsibility Model for Resilience



What is application resilience?

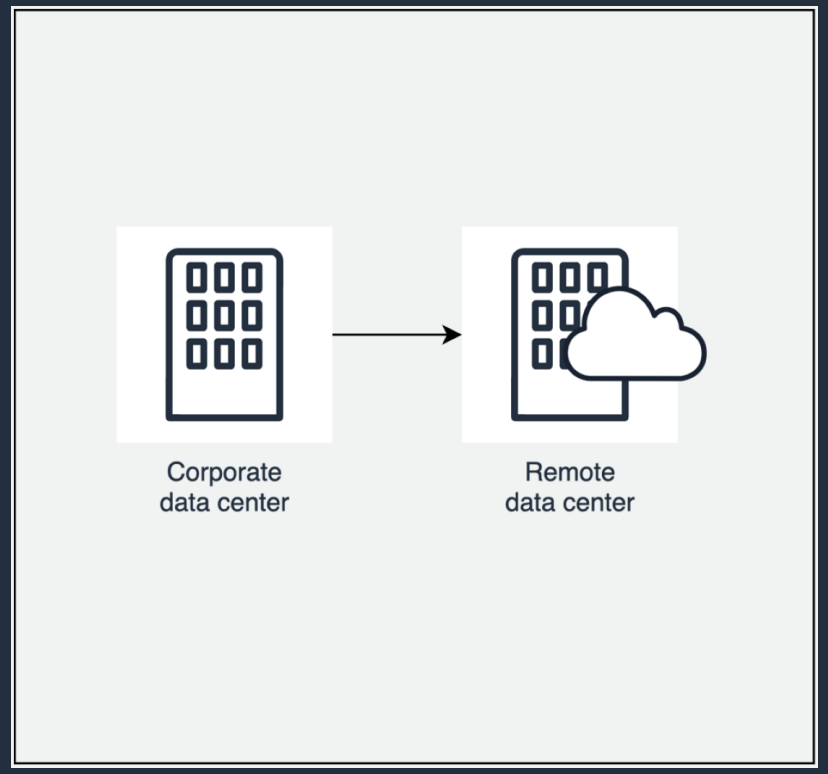
How much data can you afford to recreate or lose?

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

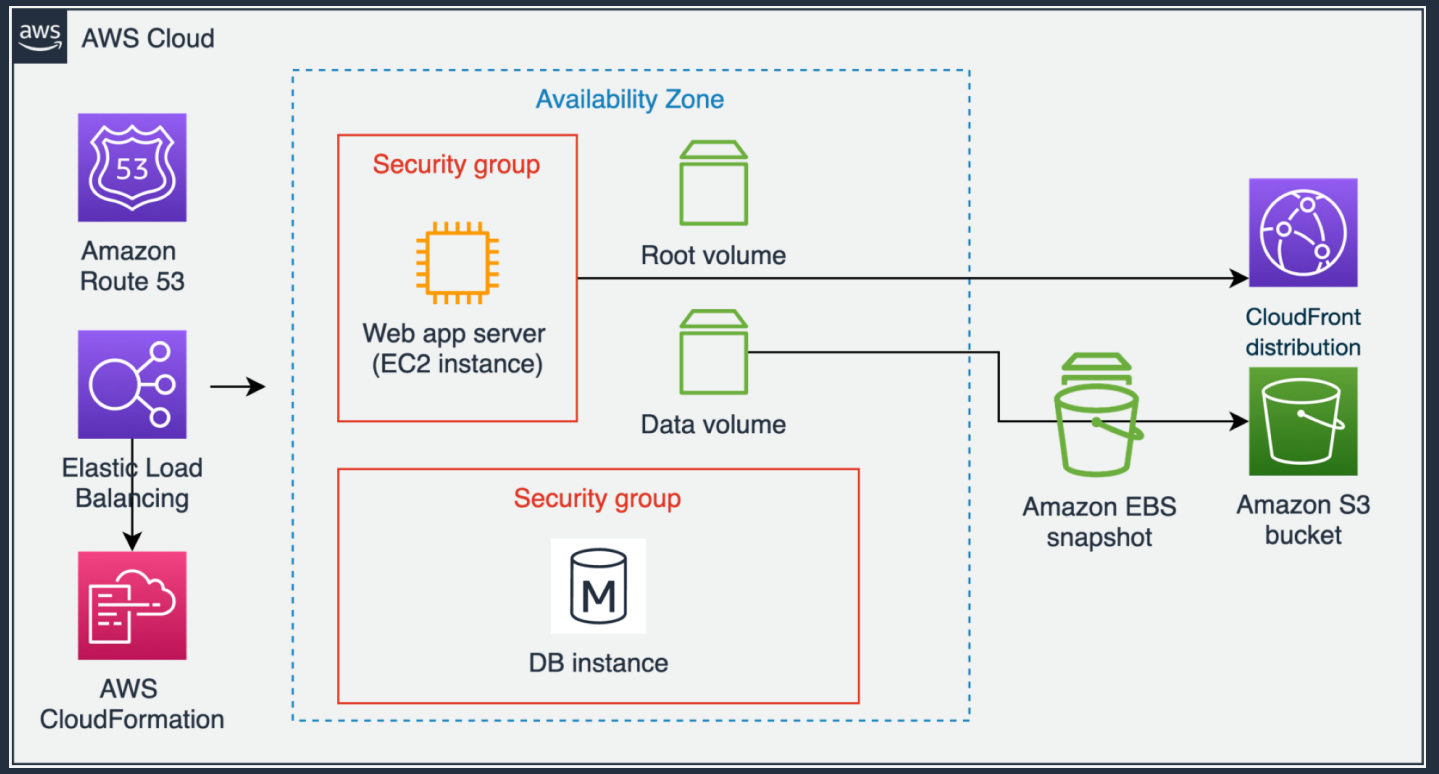
The problem AWS Resilience Hub solves?

The problem we are trying to solve

Traditional



Today



AWS Resilience Hub – key capabilities

- Define application RTO and RPO in a resilience policy
- Assessment to uncover resilience weaknesses
- Recommendations on SOPs and alarms
- Resilience testing and verification
- Dashboard to view application portfolio resilience posture
- CI/CD integrations
- Resilience score indicates likelihood of meeting RTO and RPO
- Audit trail for compliance

AWS Resilience Hub – key benefits

Continuously validate and track application resilience

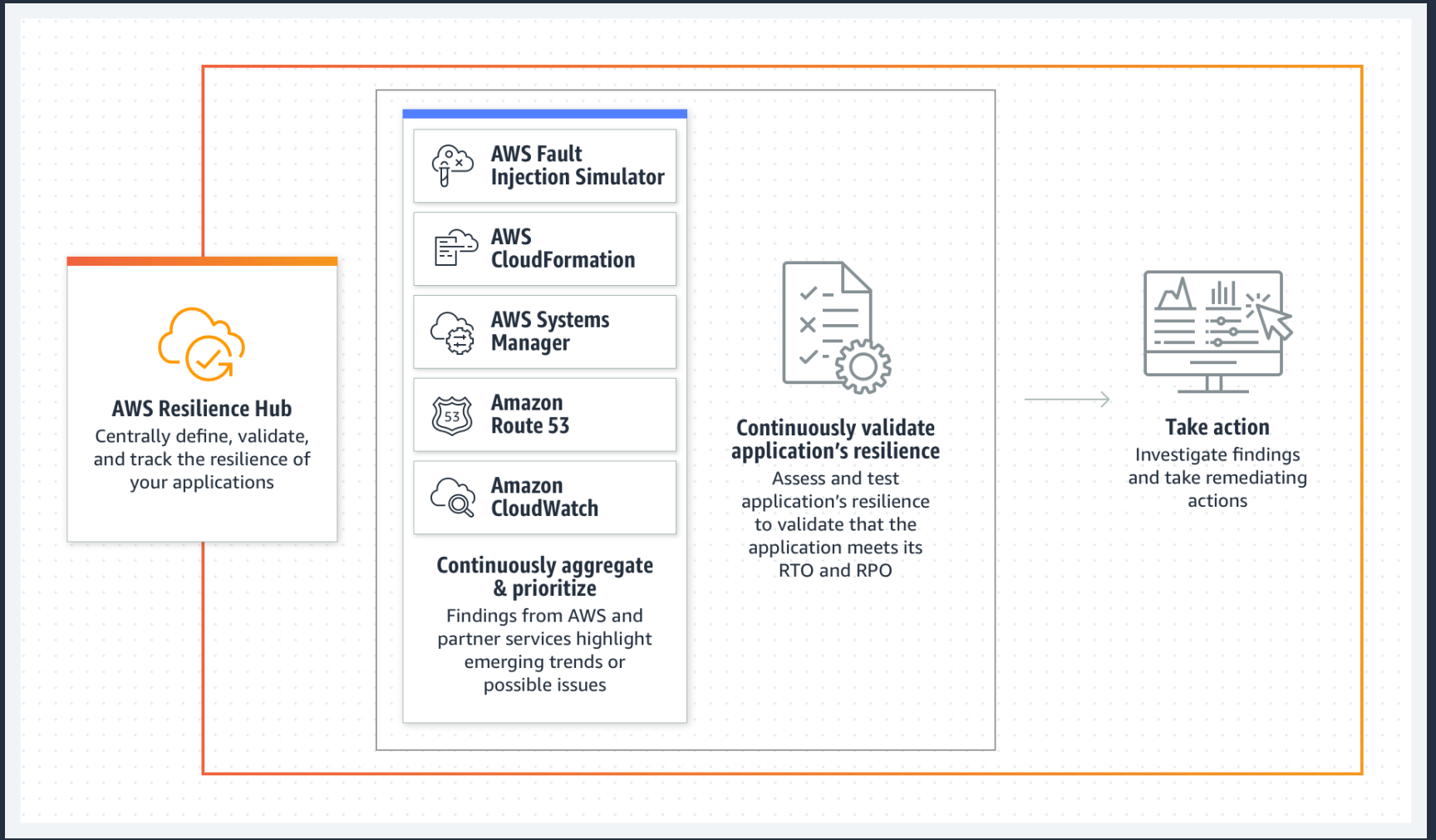
Consistently meet resilience targets (RTO and RPO)

Identify and resolve resilience-related issues before they occur in production

Reduce application-related outages

AWS Resilience Hub – overview

Provides a central place to define, validate, and track the resilience of your applications on AWS



AWS Resilience Hub – use cases

Protect mission-critical applications

Fault-injection simulations of real-world failures help validate the effectiveness of recovery standard operating procedures (SOP) and alarms

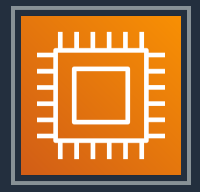
Reduce costs

Uses the cost effectiveness of the AWS cloud to help optimize business continuity while reducing recovery costs

Help meet contractual and regulatory requirements

Keeps an audit trail of events during planned and unplanned outages, helping meet compliance and regulatory requirements.

AWS Resilience Hub | Supported Resources*



Compute

Amazon EC2,
Amazon ECS,
Amazon EKS,
AWS Lambda,
AWS Auto Scaling

Networking

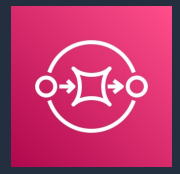
NAT Gateway,
Amazon Route 53,
Elastic Load Balancing,
Amazon Route53 ARC

Database

Amazon RDS,
Amazon Aurora,
Amazon DynamoDB,
Amazon DocumentDB

Storage

Amazon S3,
Amazon EBS,
Amazon EFS



Others

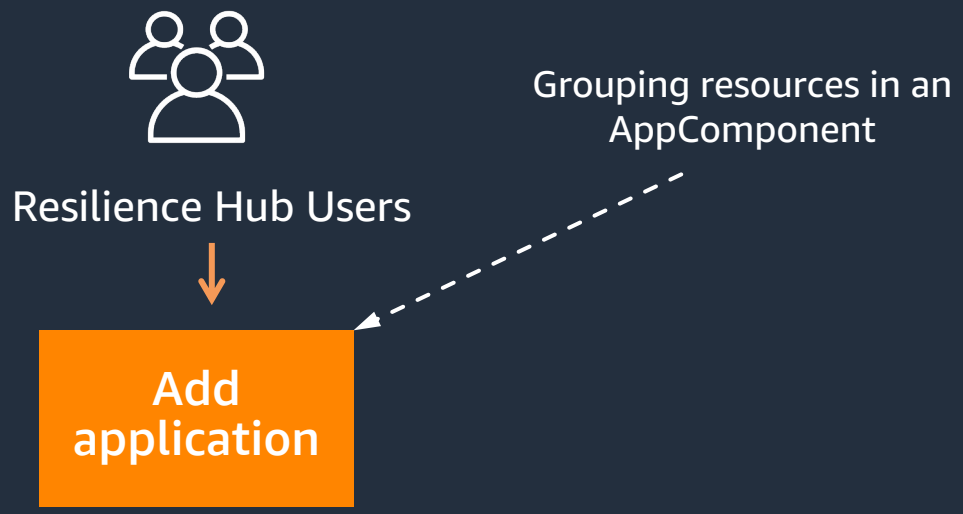
Amazon SQS,
Amazon SNS,
AWS Backup,
Amazon API Gateway
AWS Elastic Disaster Recovery

*Latest : https://docs.aws.amazon.com/resilience-hub/latest/userguide/supported-resources.html

How AWS Resilience Hub works?

AWS Resilience Hub – how does it work? (1 of 6)

- Import Infra-as-code files – CloudFormation stacks or Terraform State Files
- Select from Service Catalog App Registry
- Select Resource Groups
- Supports multi-region applications
- Supports cross accounts



https://docs.aws.amazon.com/resilience-hub/latest/userguide/discover-structure.html

AWS Resilience Hub – how does it work? (2 of 6)

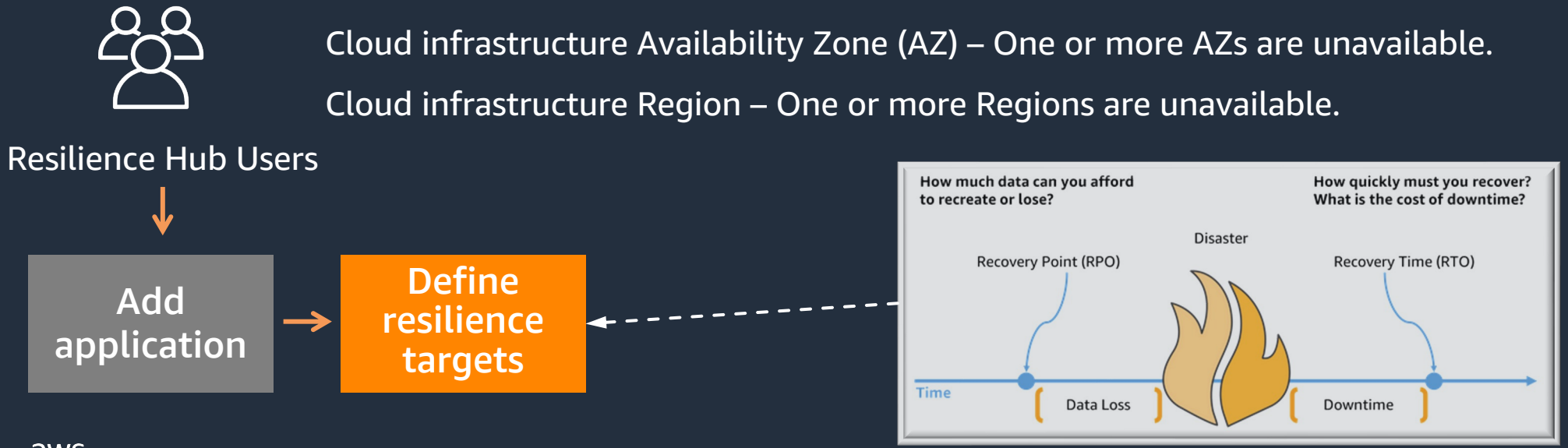
- Define resilience targets (RTO and RPO) per application
- Use build-in resilience targets templates
- AWS Resilience Hub uses your RTO and RPO targets to measure resiliency for these potential types of disruptions:

  Application – Loss of a required software service or process.

  Cloud infrastructure – Loss of hardware, such as EC2 instances.

  Cloud infrastructure Availability Zone (AZ) – One or more AZs are unavailable.

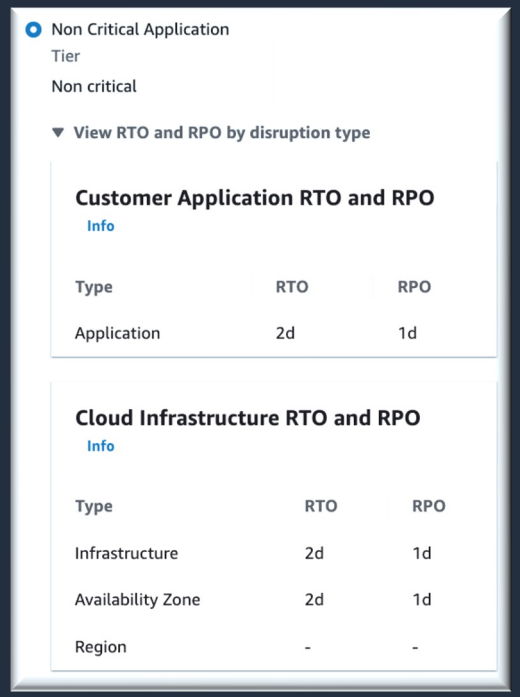
  Cloud infrastructure Region – One or more Regions are unavailable.



RTO/RPO typical Targets by critical Tiers

Non-Critical Application

- RTO 2d
- RPO 1d


Non Critical Application
Tier
Non critical
View RTO and RPO by disruption type
Customer Application RTO and RPO
Info

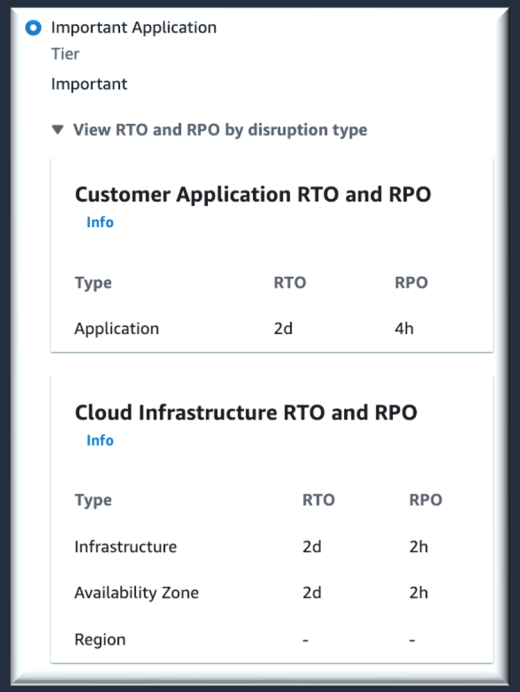
Type	RTO	RPO
Application	2d	1d

Cloud Infrastructure RTO and RPO
Info

Type	RTO	RPO
Infrastructure	2d	1d
Availability Zone	2d	1d
Region	-	-

Important Application

- RTO 2d
- RPO 4h


Important Application
Tier
Important
View RTO and RPO by disruption type
Customer Application RTO and RPO
Info

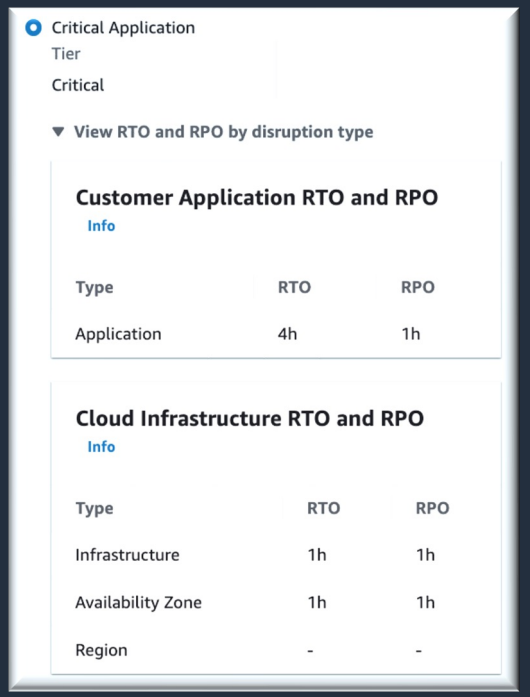
Type	RTO	RPO
Application	2d	4h

Cloud Infrastructure RTO and RPO
Info

Type	RTO	RPO
Infrastructure	2d	2h
Availability Zone	2d	2h
Region	-	-

Critical Application

- RTO 4h
- RPO 1h


Critical Application
Tier
Critical
View RTO and RPO by disruption type
Customer Application RTO and RPO
Info

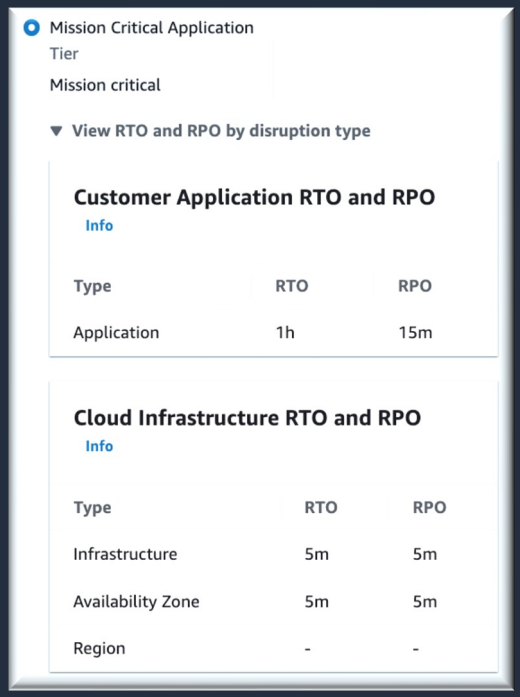
Type	RTO	RPO
Application	4h	1h

Cloud Infrastructure RTO and RPO
Info

Type	RTO	RPO
Infrastructure	1h	1h
Availability Zone	1h	1h
Region	-	-

Mission Critical Application

- RTO 1h
- RPO 15m


Mission Critical Application
Tier
Mission critical
View RTO and RPO by disruption type
Customer Application RTO and RPO
Info

Type	RTO	RPO
Application	1h	15m

Cloud Infrastructure RTO and RPO
Info

Type	RTO	RPO
Infrastructure	5m	5m
Availability Zone	5m	5m
Region	-	-

AWS Resilience Hub – how does it work? (3 of 6)

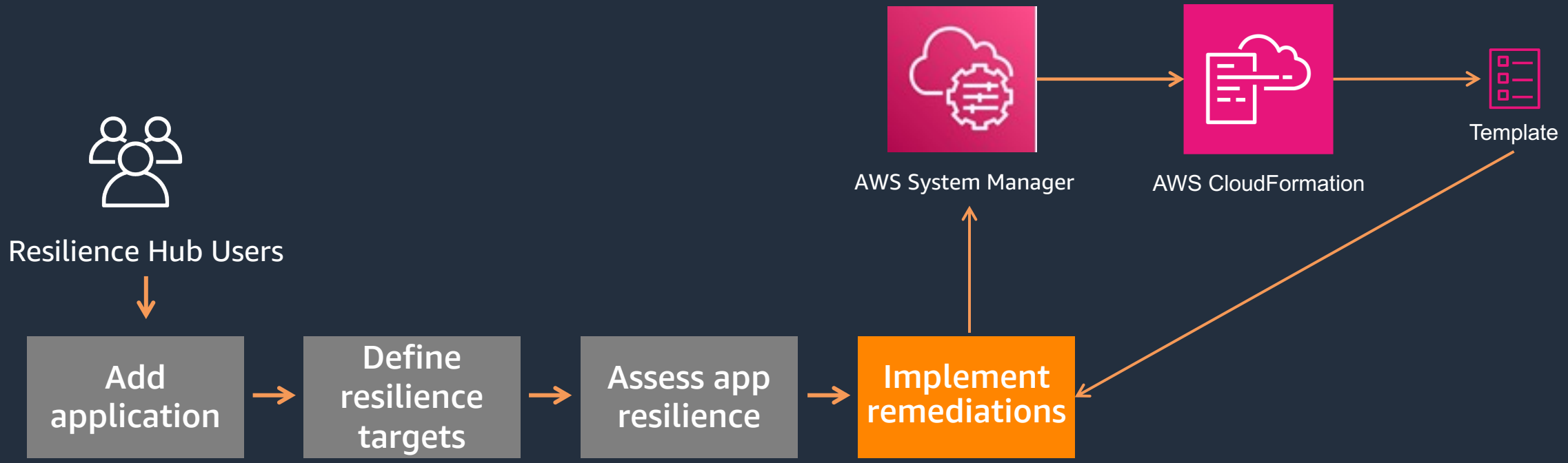
- Assess the resilience of the application and uncover resilience weaknesses
- Receive cost-effective recommendations to improve the resilience posture of the application –
  - Configuration adjustments
  - CloudWatch monitors and alarms
  - Resilience tests
  - SOP for recovery

Resilience Hub Users

https://aws.amazon.com/blogs/mt/resilience-reporting-dashboard-aws-resilience-hub/

AWS Resilience Hub – how does it work? (4 of 6)

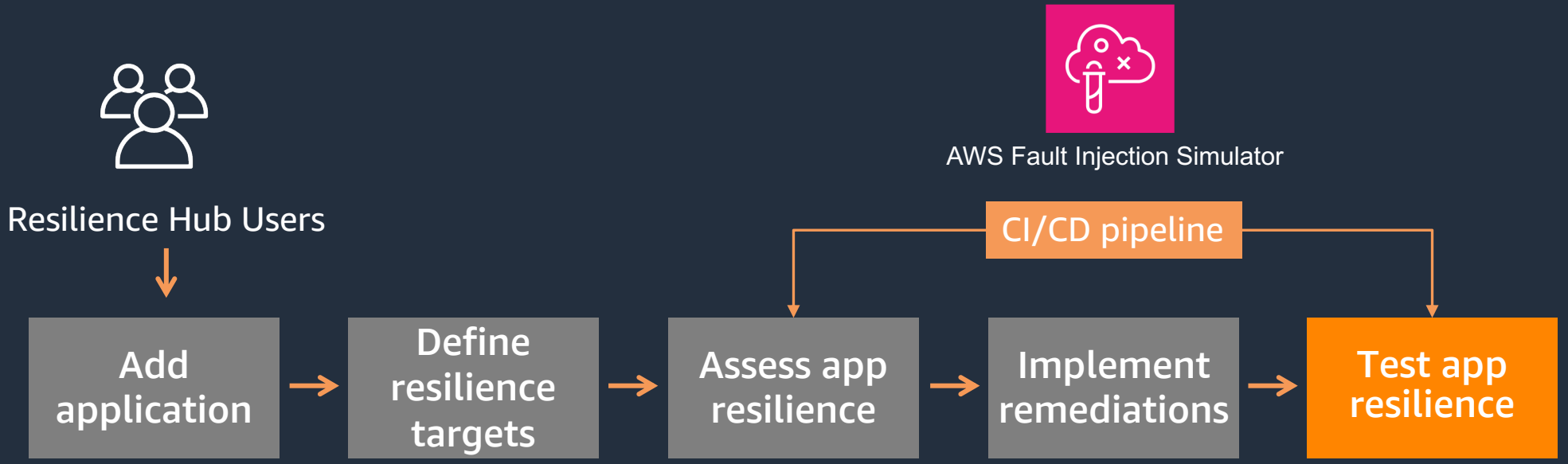
- Update the application and SOPs to incorporate recommendations from the resilience assessment



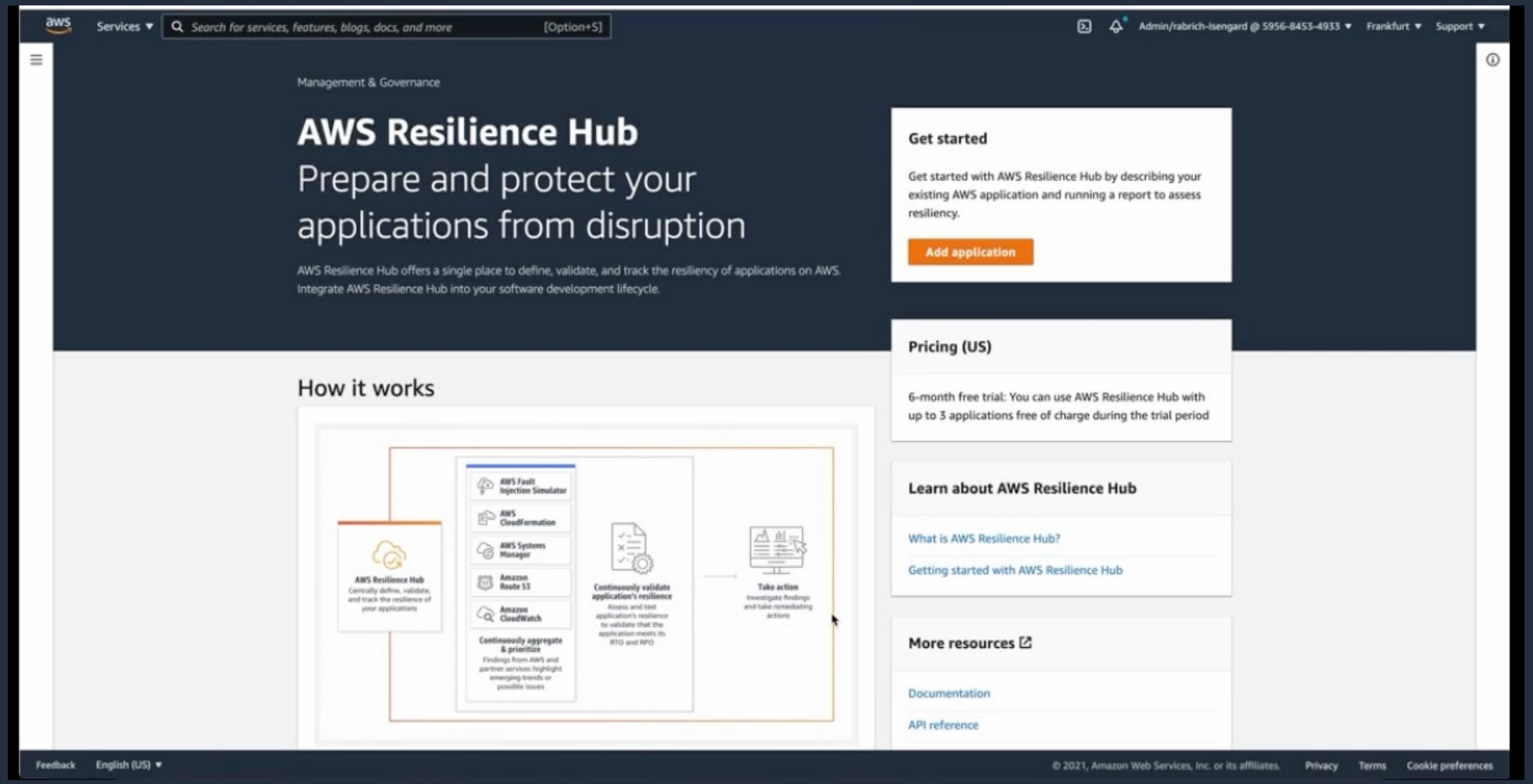
https://docs.aws.amazon.com/resilience-hub/latest/userguide/sops.html

AWS Resilience Hub – how does it work? (5 of 6)

- Simulate a wide range of failures
- Validate that monitors and alarms identify the correct outage
- Validate that SOP recovered the application within its resilience targets
- (GA) Integration with AWS Failure Injection Simulator
- Integrate into CI/CD pipelines for continuous assessment and testing



AWS Resilience Hub - Demo



Resources

AWS Resilience Hub: aws.amazon.com/resilience-hub/resources/

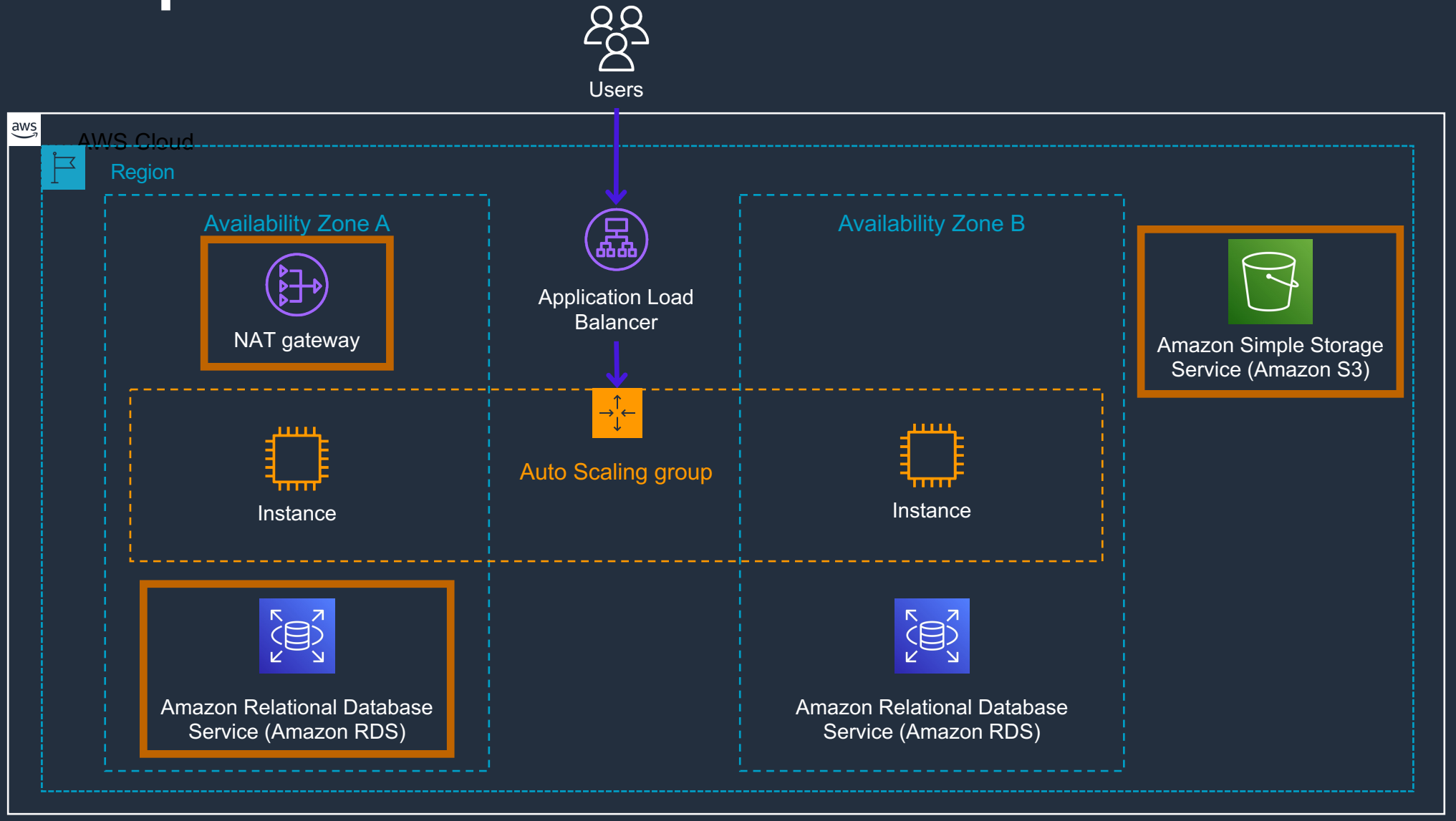
- What's new
- Training
- Videos
- Blog posts

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

- Design principles
- Questions
- Best practices

Workshop Architecture

Workshop Architecture



Disaster Recovery Strategies on AWS

Puneet Arora
Sr Partner Solution Architect

Agenda

Why Disaster Recovery

High Availability and Disaster Recovery

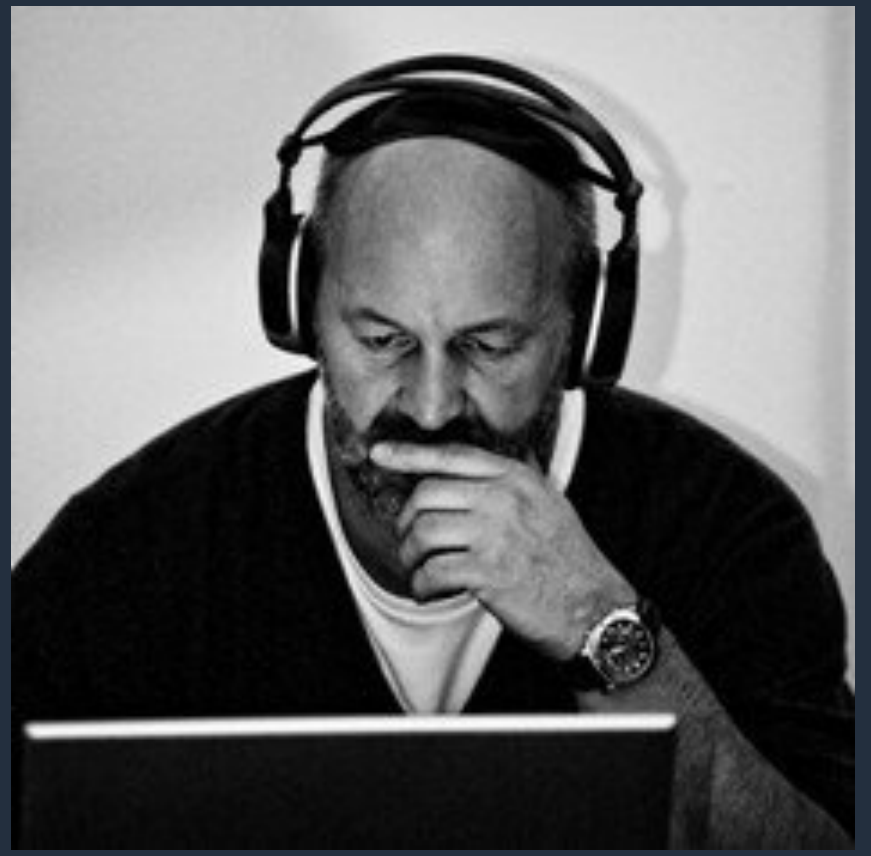
RTO/RPO - Business Continuity Plan (BCP)

Disaster Recovery in Cloud

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

Werner Vogels

Amazon CTO



Resilience

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

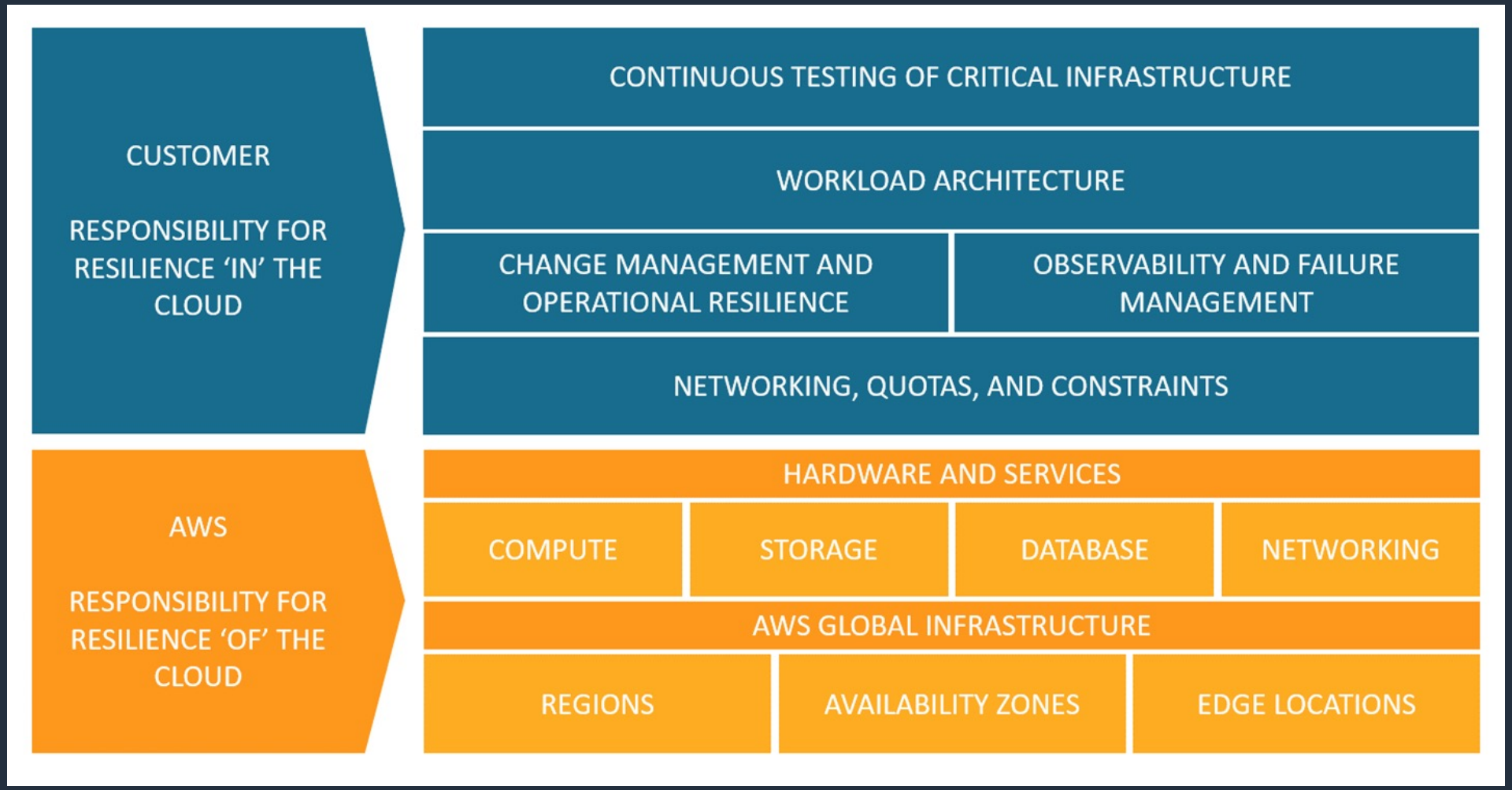
Returning to normal operations within specific targets at an **alternate site** for failures that cannot be handled by HA

Backup & Recovery, Data Bunkering, Managed RPO/RTO

Continuous Improvement

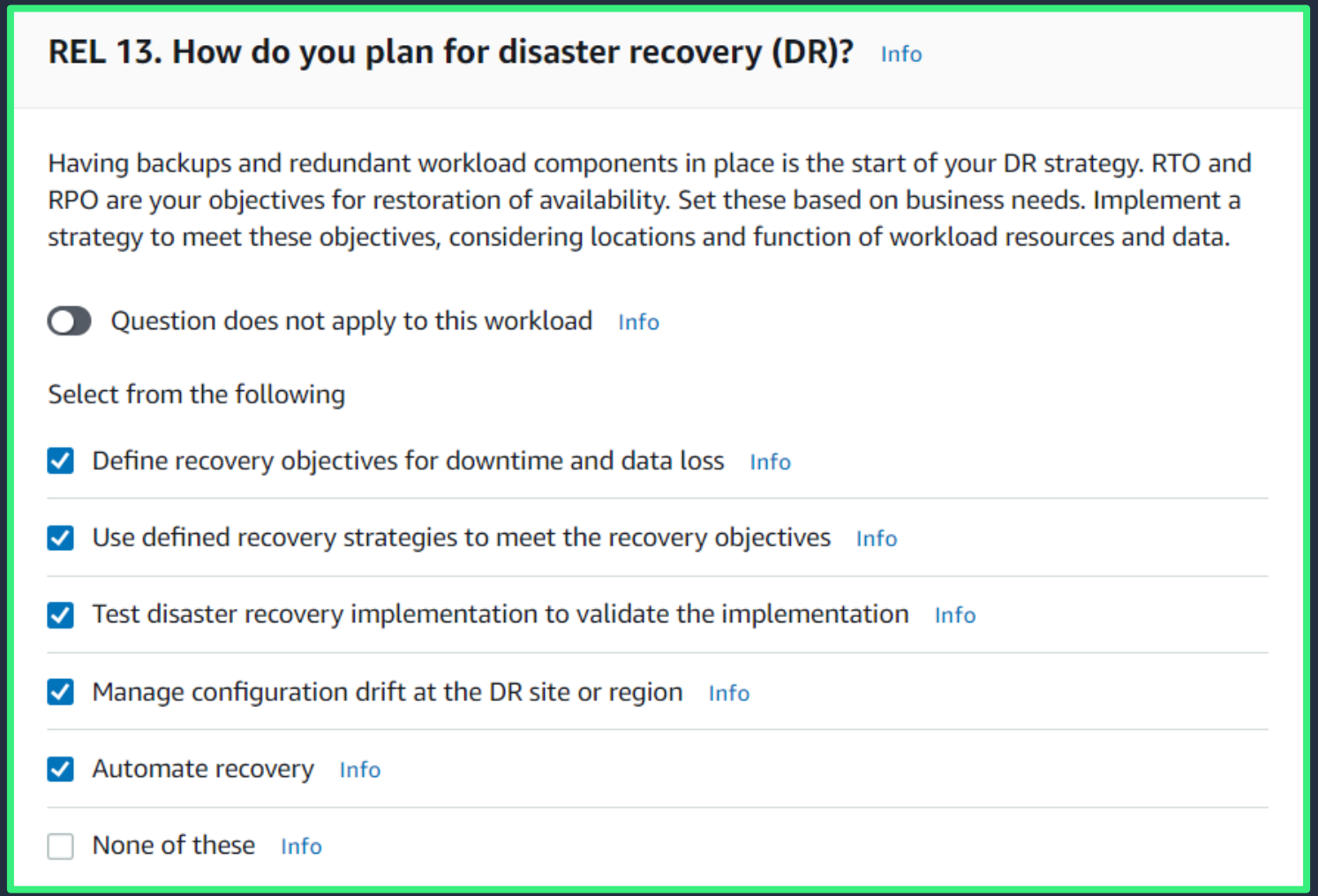
Moving beyond pre-deployment testing towards chaos engineering patterns

Shared Responsibility Model for Resilience



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.

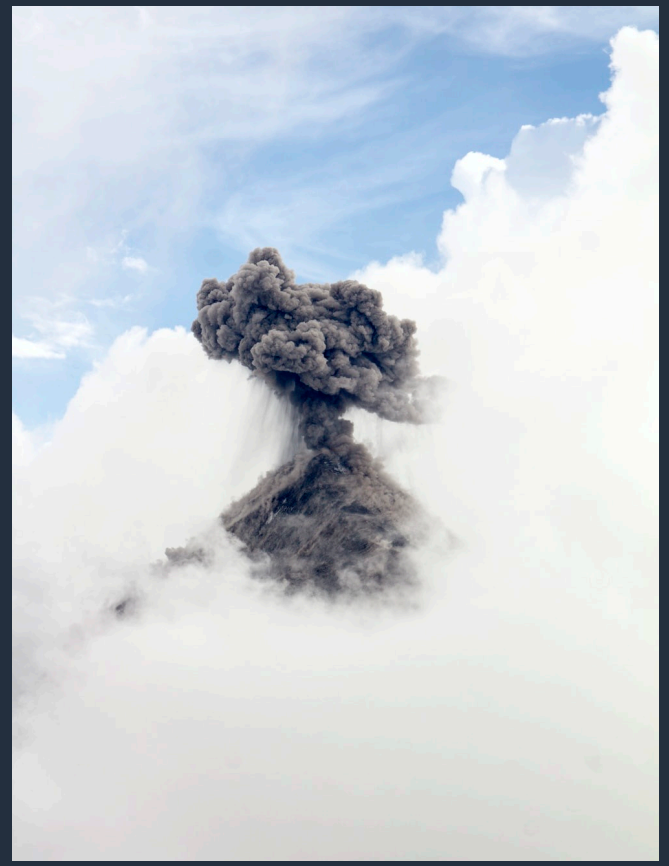
Question does not apply to this workload Info

Select from the following

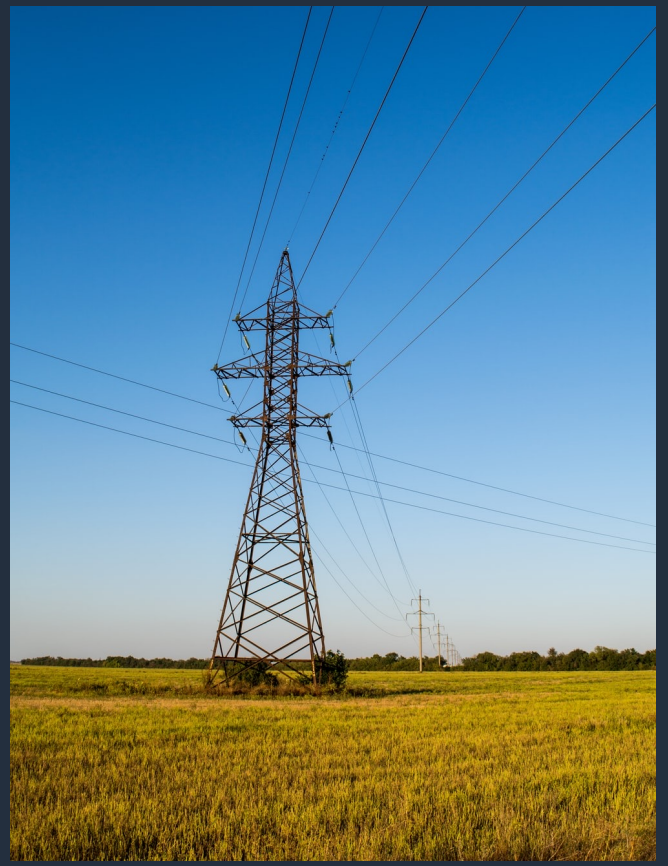
- [x] Define recovery objectives for downtime and data loss Info
- [x] Use defined recovery strategies to meet the recovery objectives Info
- [x] Test disaster recovery implementation to validate the implementation Info
- [x] Manage configuration drift at the DR site or region Info
- [x] Automate recovery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

Categories of Disaster

Natural Disaster



Technical Failure



Human Actions

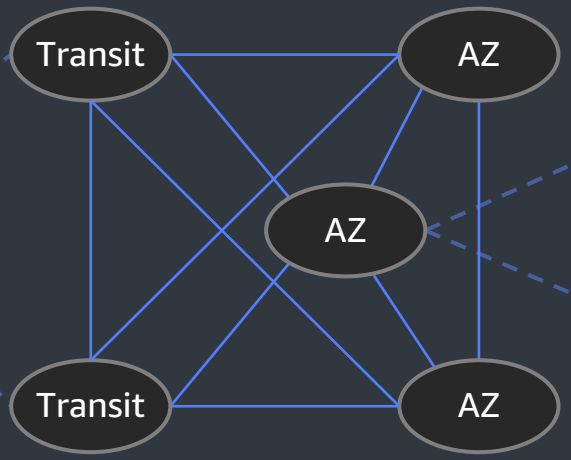
AWS Regions and Availability Zones (AZs)

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

31 AWS Regions worldwide

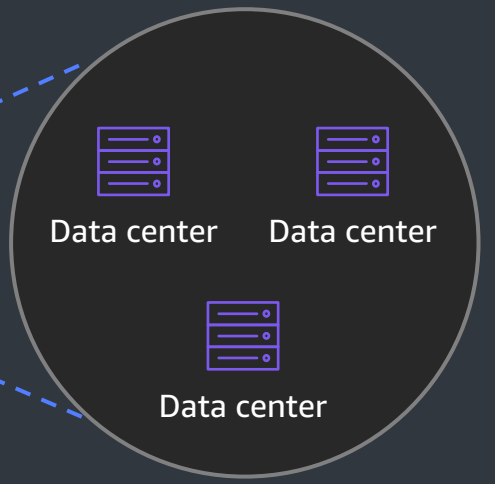
- AWS Regions
- Announced Regions

Each AWS Region has multiple AZs



A Region is a physical location in the world

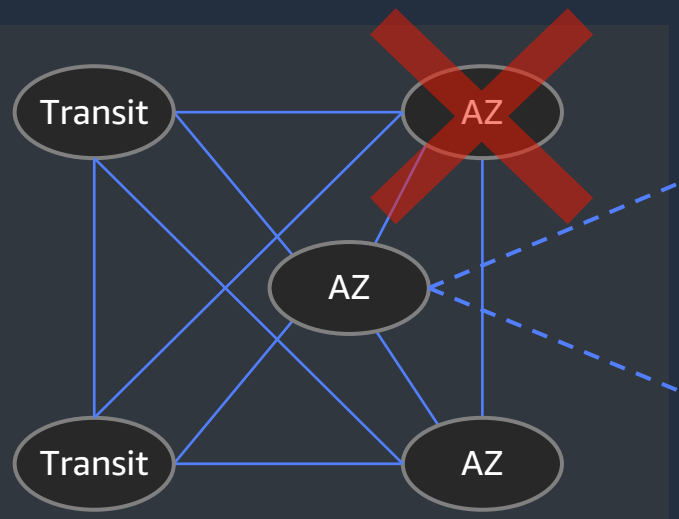
Each AZ includes one or more discrete data centers



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

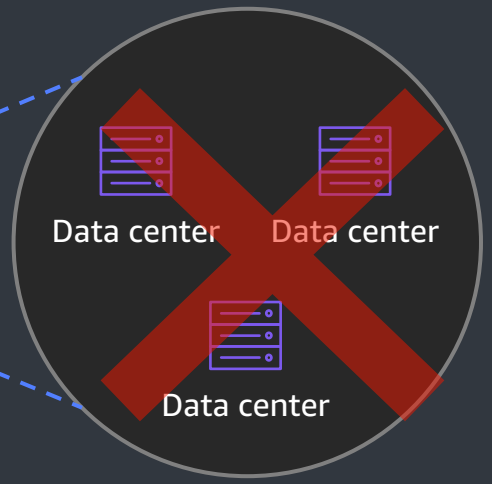
Multi-AZ for Disaster Recovery (DR)

Each AWS Region has multiple AZs

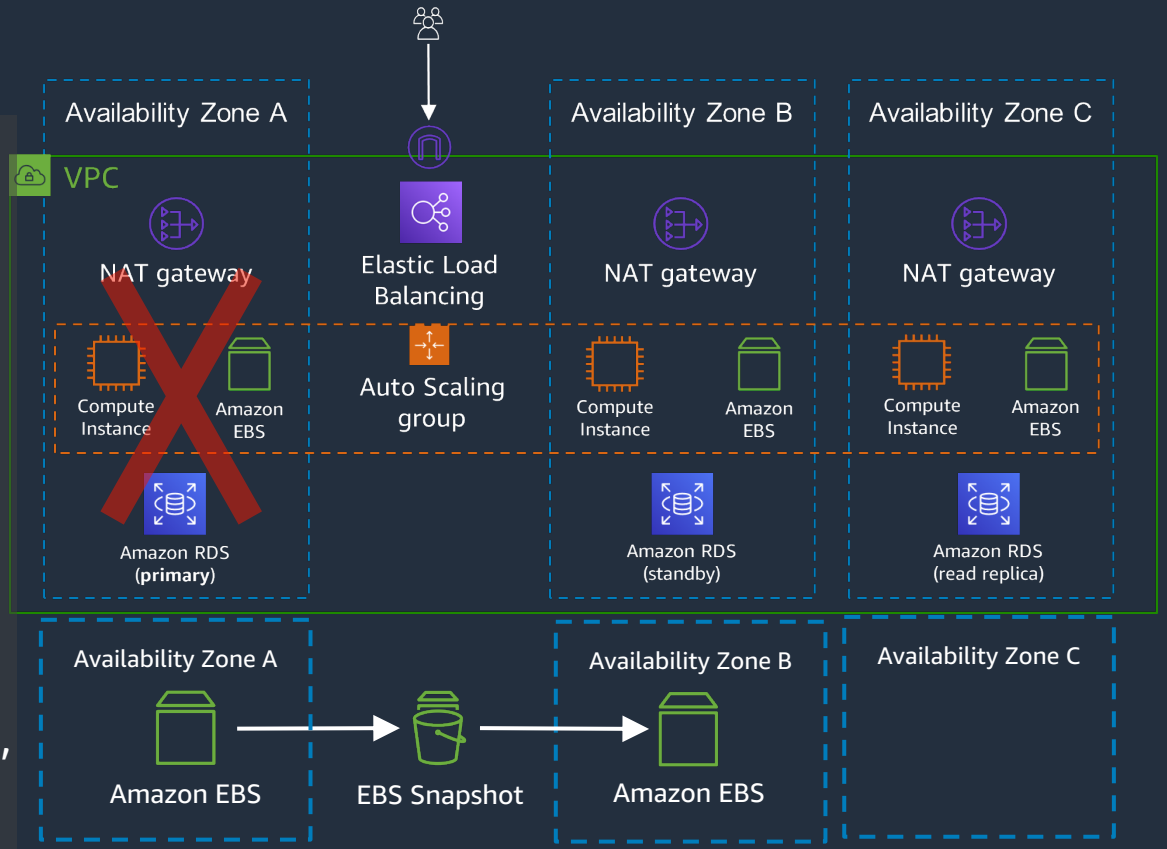


A **Region** is a physical location in the world

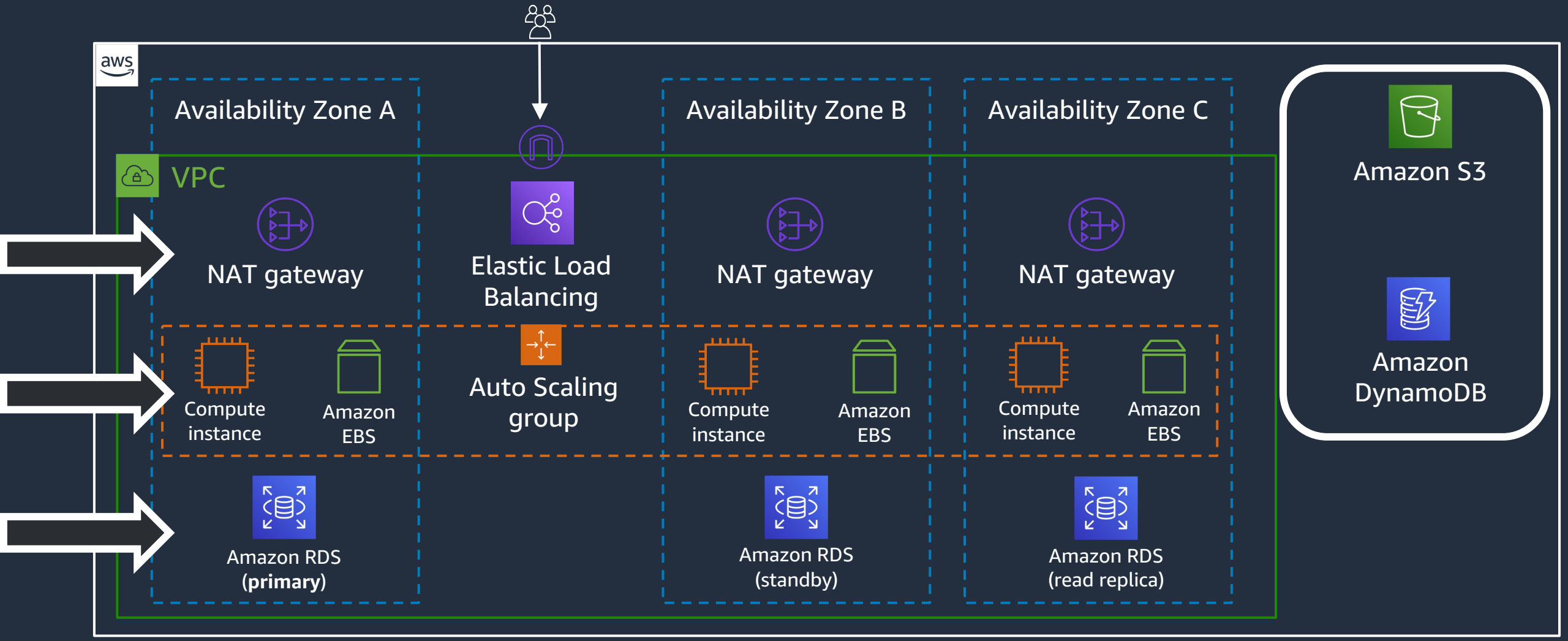
Each AZ includes one or more discrete data centers



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

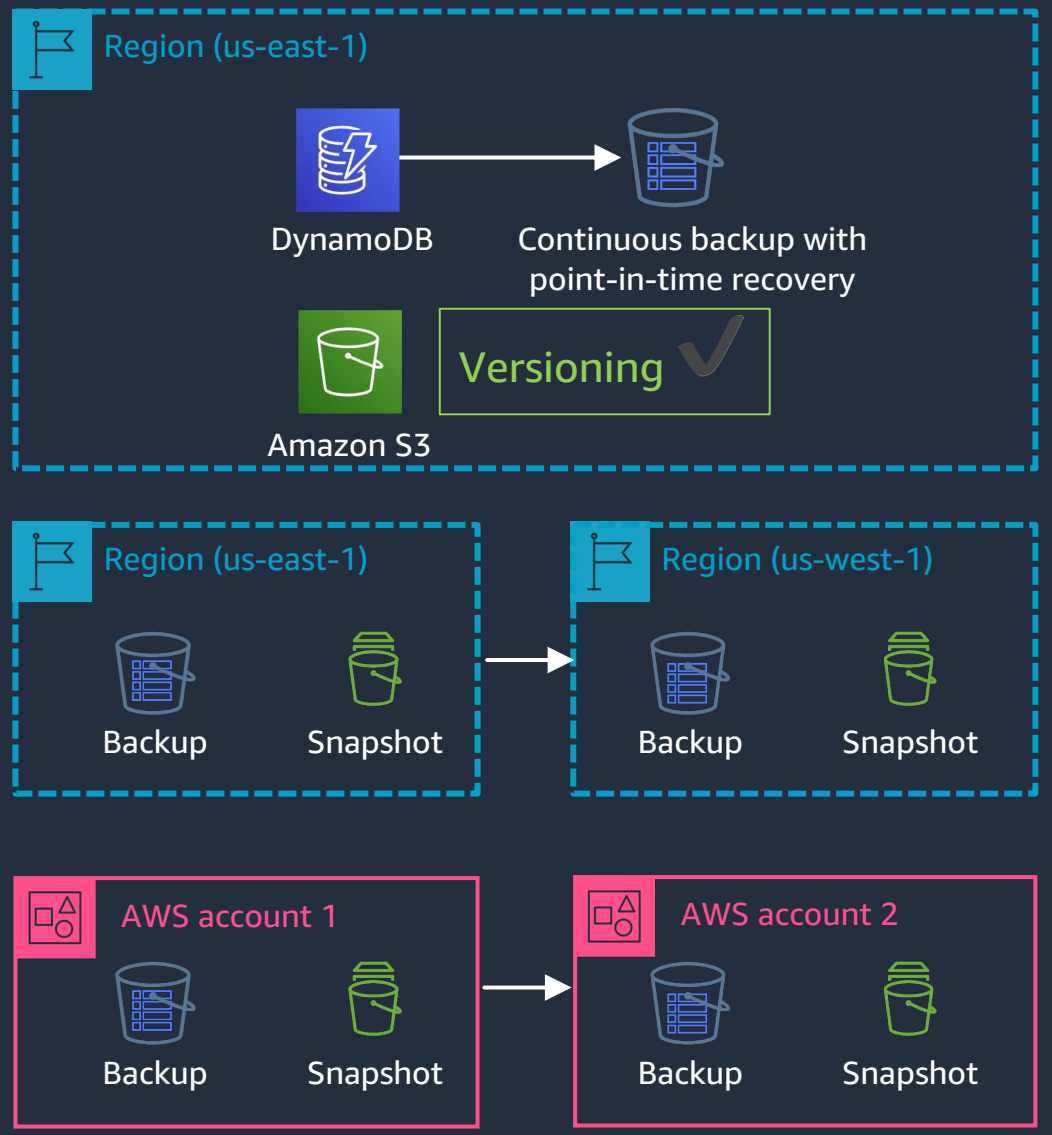


Multi-AZ For High Availability (HA)



Data Protection

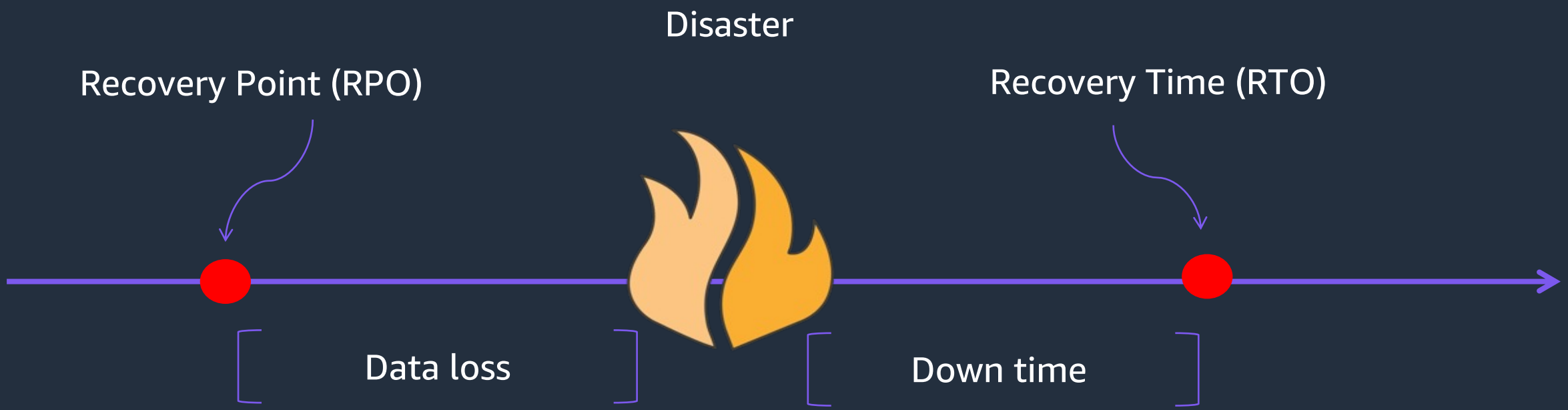
- Accidental deletions
- Regional impairments
- Malicious intent



Recovery Point and Recovery Time Objective (RPO/RTO)

How much data can you afford to recreate or lose?

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



Disaster Recovery Benefits of the Cloud

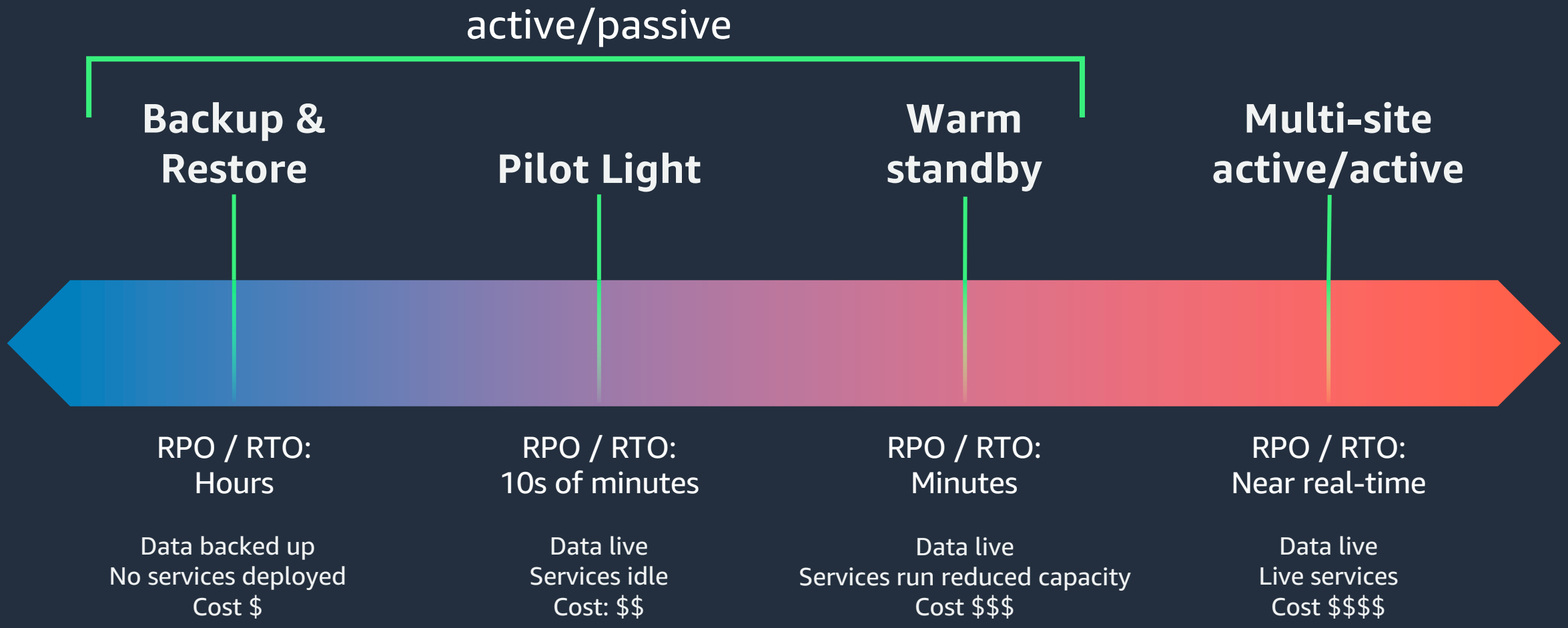
Traditional disaster recovery

- Massive upfront & ongoing hardware cost
- Management and infrastructure overhead
- Data growth increases costs
- Separation of test and production environment
- Vulnerable to cyber threats/hacking

Disaster recovery in the cloud

- Pay as you go for the rightsized compute/storage
- Lower IT overhead
- (MUCH!) More automation
- Easy and repeatable testing
- Systems up in minutes (not hours/days!)

Strategies for Disaster Recovery



DISASTER RECOVERY OVERVIEW

AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery

Sankar Cherukuri

Partner Solution Architect
Amazon Web Services

Agenda

Why Use Cloud-Based Disaster Recovery?

How AWS Elastic Disaster Recovery Enables Business Continuity

AWS Elastic Disaster Recovery Architecture

Workshop Architecture

Workshop

Why Use Cloud-Based Disaster Recovery?

Disaster Recovery Benefits of the Cloud

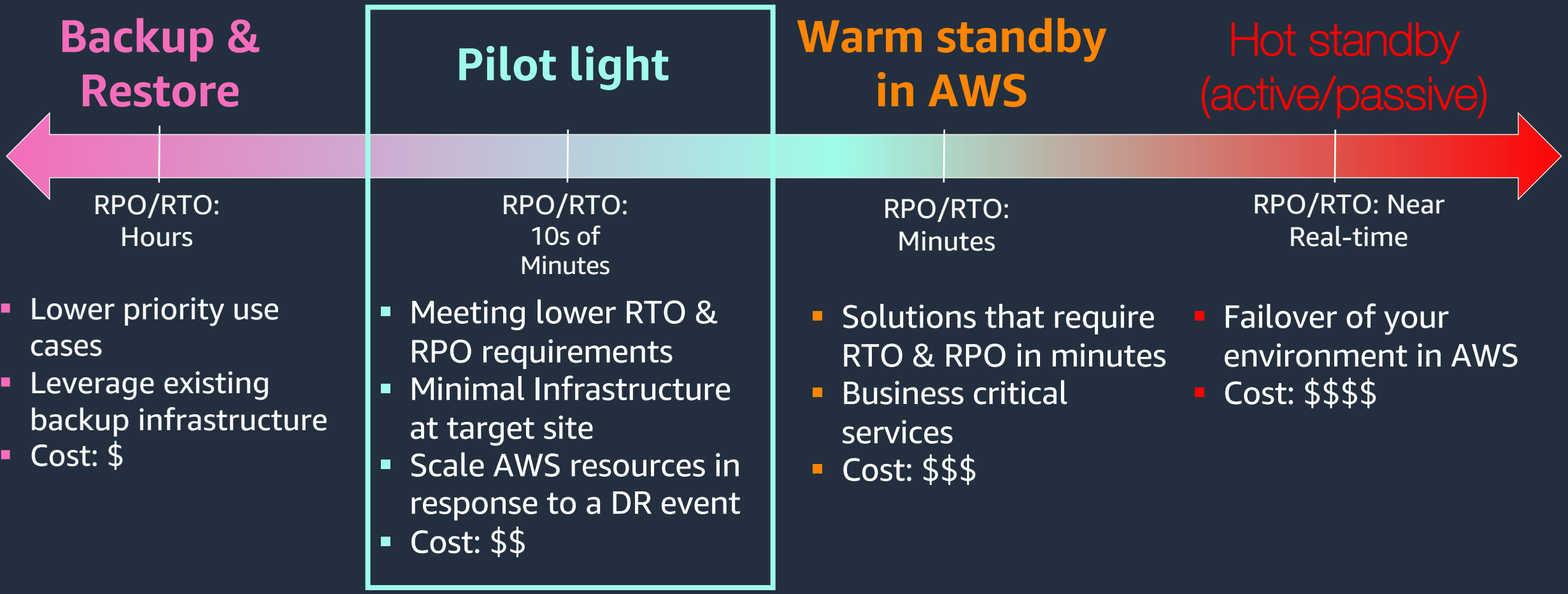
Traditional Disaster Recovery

- Massive upfront & ongoing hardware cost
- Management and infrastructure overhead
- Data growth increases costs
- Separation of test and production environment
- Vulnerable to cyber threats/hacking

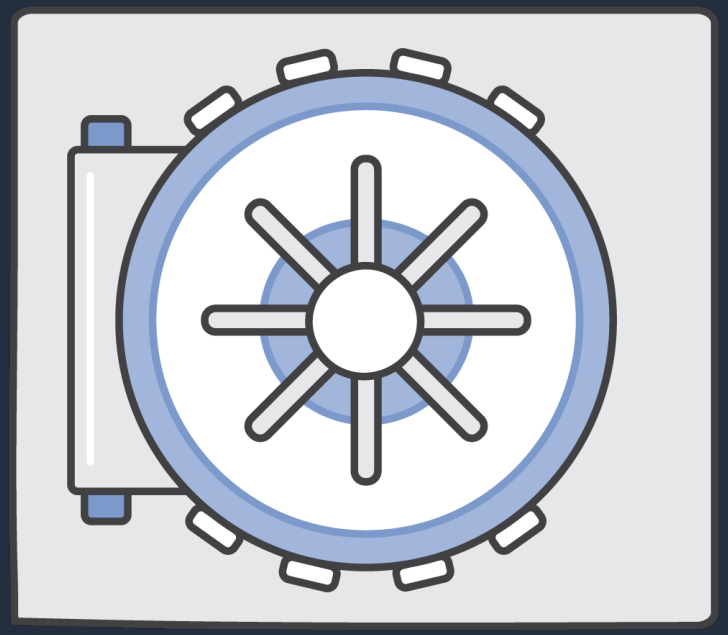
DR in the cloud

- Pay as you go for the right-sized compute/storage
- Lower IT overhead
- More automation
- Easy and repeatable testing
- Systems up in minutes (not hours/days!)

AWS Elastic Disaster Recovery



Backup & Restore



- Suitable for:
  - Services that can sustain longer recovery times
  - Lower priority use cases
- Point-in-time copy of data (user, configuration, and code)
- Infrastructure restored with backed up data
- Leverage existing backup infrastructure

Pilot Light

- Suitable for:
  - Meeting lower RTO & RPO requirements
  - Business critical services
  - **AWS resources in a switched off state**
  - **Start up resources when events dictate**
  - Match required production capacity through auto-scaling policies
- Mid-range cost option for DR
- **AWS Elastic Disaster Recovery** or third-party options Racemi and others

Warm Standby

- Suitable for:
  - Solutions that require RTO & RPO in minutes
  - Core business-critical functions
  - Match required production capacity through auto-scaling policies
- Higher cost option for DR
- Scaled down, but fully functional copy in another Region
- Allows to easily test DR capability

Hot Standby

- Full replication of your environment running and ready for a failover during a disaster – it runs ‘hot’.
- Active/passive strategy that does not handle production traffic
- Suitable for:
  - Solutions that require RTOs & RPOs of zero
  - Core business-critical functions
  - Multi-site architecture for automated load-balancing of traffic to multiple AZs and even AWS regions
- Higher cost option for DR
- Route 53 Application Recovery Controller

How AWS Elastic Disaster Recovery Enables Business Continuity

AWS Elastic Disaster Recovery Use Cases

On-premises to AWS

Cloud to AWS

AWS Region to AWS Region

Common Disaster Recovery Challenges

- High cost of idle duplicate resources
- Diverse infrastructure and OS types
- Server compatibility issues
- Inability to achieve recovery objectives (RPOs/RTOs)
- Replicating busy, continually changing workloads
- Tests and drills are expensive and disrupt operations
- Different DR tools or processes for different applications
- Scaling DR site when primary environment changes

AWS Elastic Disaster Recovery Benefits

Faster recovery

Recovery time objectives (RTOs) of minutes

Easy testing

Conduct non-disruptive drills to verify readiness

Lower costs

No need to pay for idle recovery site resources

Ransomware recovery

Launch unlocked and unencrypted versions of your applications

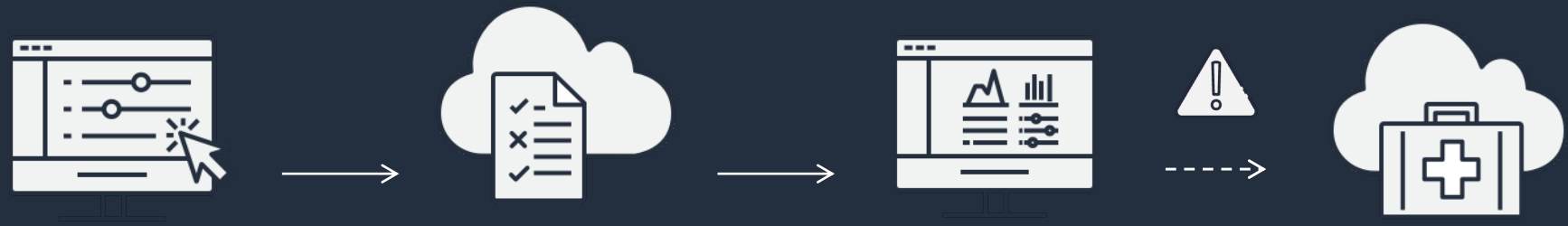
Data protection

Recovery point objectives (RPOs) of seconds

AWS Elastic Disaster Recovery Architecture

AWS Elastic Disaster Recovery lifecycle

Use a single process to recover servers across all supported infrastructure and OS



Set up
Define settings and initiate continuous data replication

Test
Launch instances for non-disruptive tests

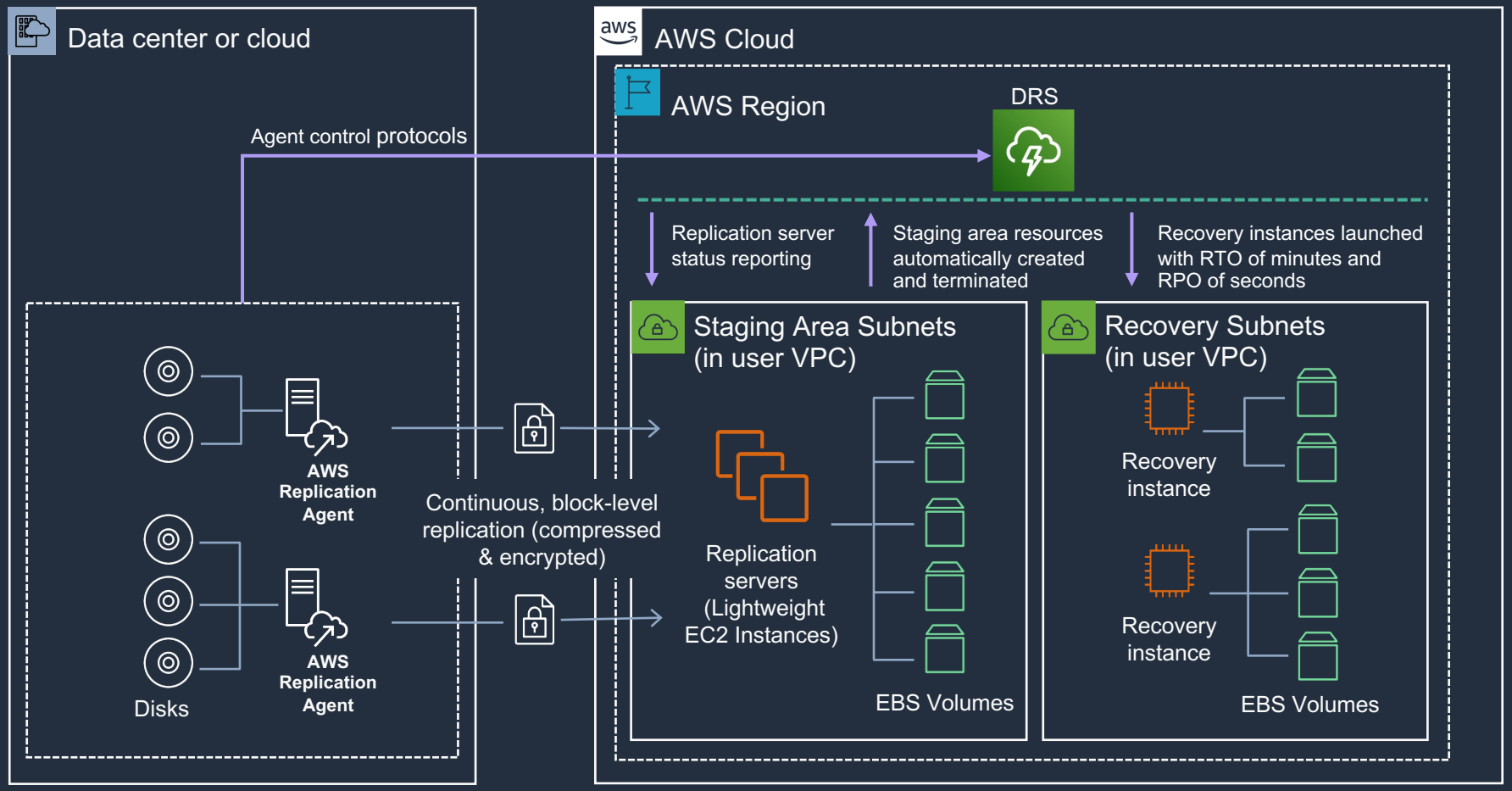
Operate
Maintain readiness with monitoring and periodic drills

Failover
Launch recovery instances on AWS within minutes

Failback
Initiate replication and return to primary site

How AWS Elastic Disaster Recovery Works

CONTINUOUS REPLICATION OF ON-PREMISES AND CLOUD SERVERS WITH AWS AS YOUR ELASTIC RECOVERY SITE



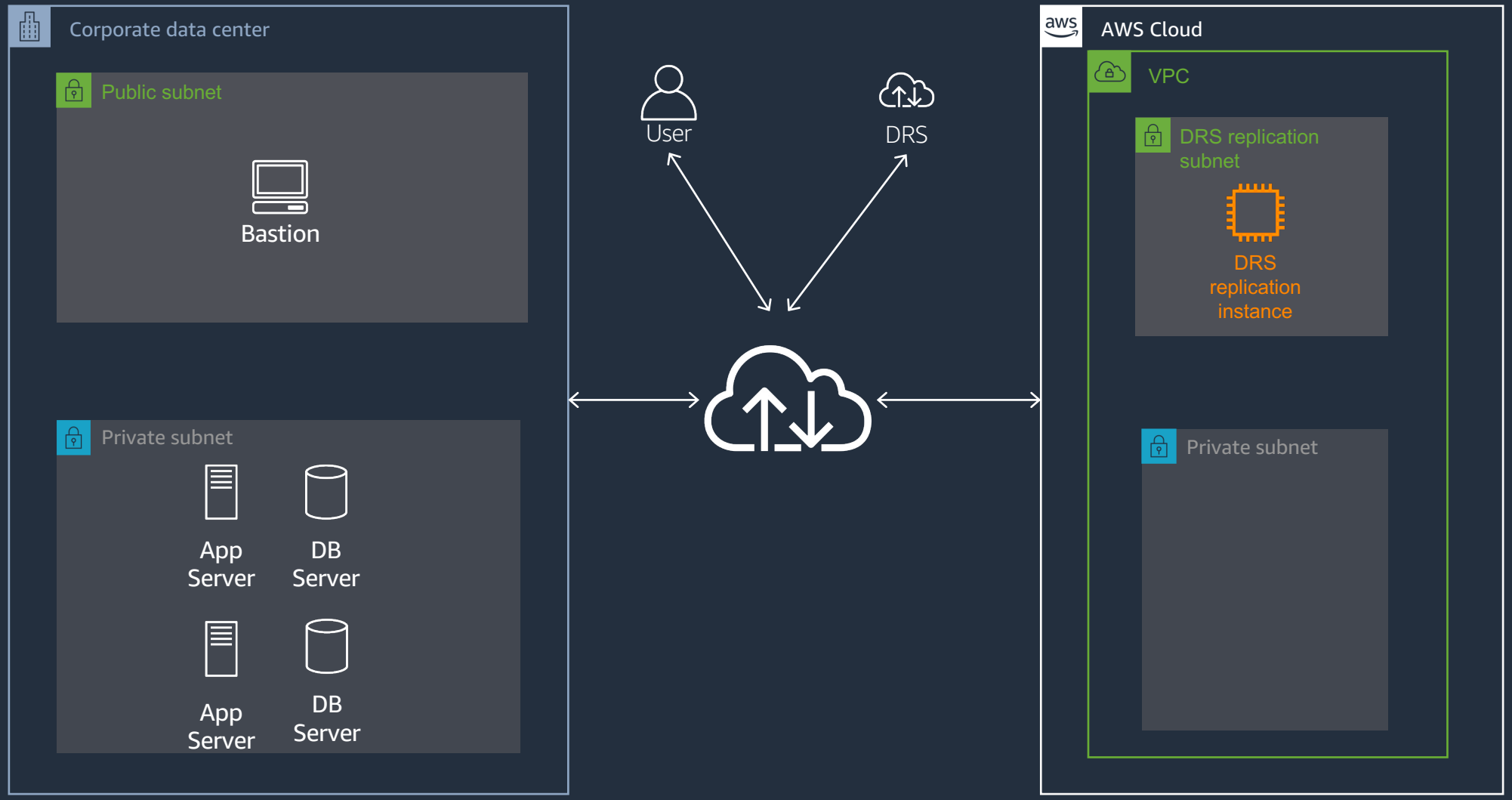
Wide platform support*

Any application	Oracle E-Business Suite, Oracle PeopleSoft, SAP CRM, SAP Hybris, SAP ERP, Apache, SugarCRM, IIS, SharePoint, Active Directory, Exchange, Microsoft Dynamics CRM
Any database	Microsoft SQL Server, Oracle Database, SAP HANA, MySQL, cassandra, mongoDB.
x86 operating systems	Red Hat, CentOS, Oracle Linux, ubuntu, debian, SUSE, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022
Source infrastructure	vmware, Azure, Google Cloud Platform, aws, vmware | aws, Physical Data Centers, Microsoft Hyper-V, openstack., Oracle Cloud, IBM Cloud

Workshop Architecture

AWS ELASTIC DISASTER RECOVERY

Workshop Architecture Reference



2 Mins Survey!

https://survey.immersionday.com/300ldfU4R

Reach out to APJ Partner team at apj-resilience-team@amazon.com for upcoming AWS Resilience sessions or Demos or Labs

Thank you!