
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC211

Disaster recovery and resiliency for AWS data protection services

Ajit Puthiyavettle
Sr. Solutions Architect
AWS

Arnab Ghosh
Sr. Solutions Architect
AWS

Jigna Gandhi
Sr. Solutions Architect
AWS

Patrick Gryczka
Sr. Solutions Architect
AWS

Vin Dahake
Senior Leader SA
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Resiliency and disaster recovery

AWS Key Management Service (AWS KMS)/AWS Secrets Manager

AWS Backup

Workshop details

Call to action

Survey

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resiliency/disaster recovery

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

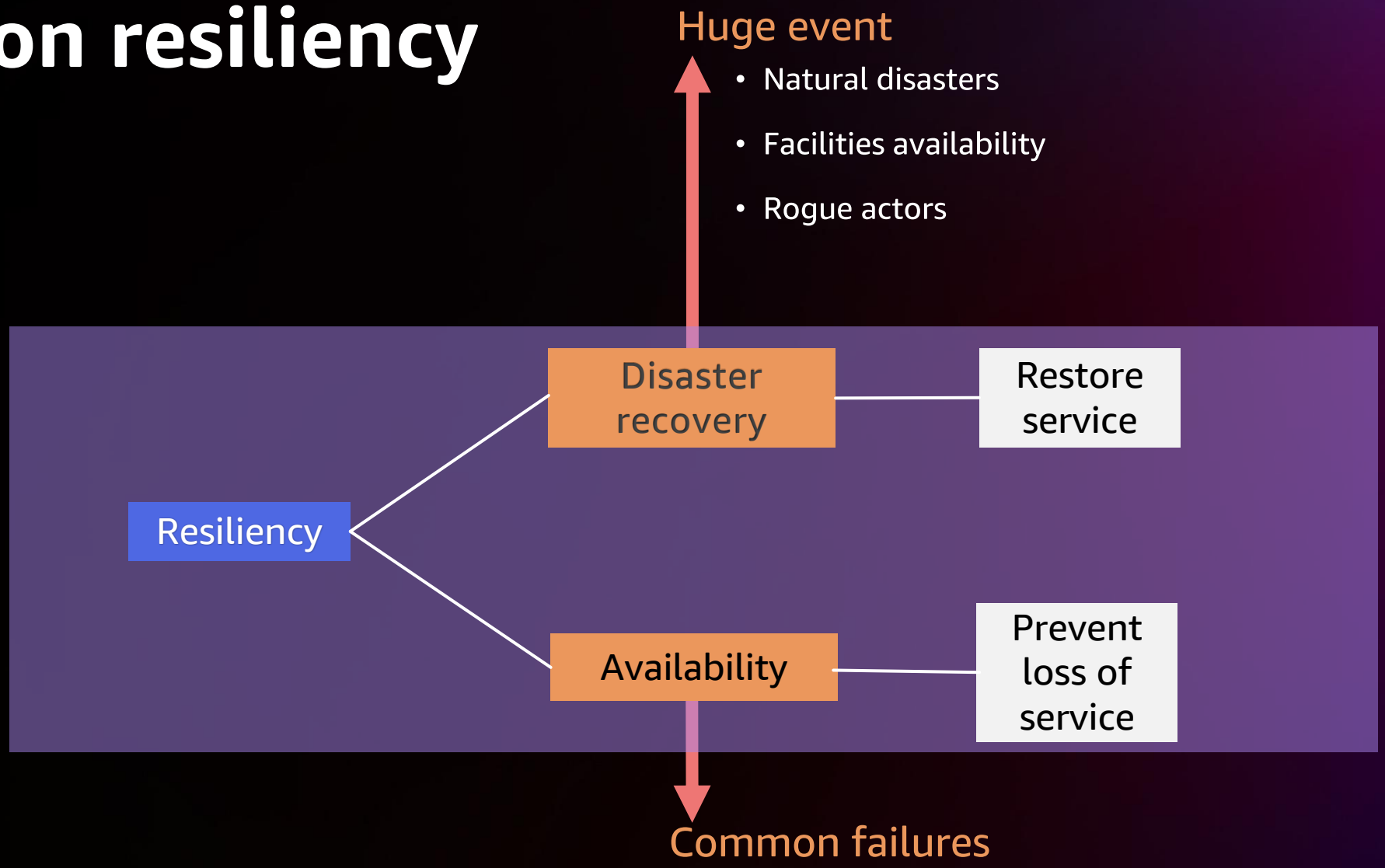
“Everything fails all the time.”

Werner Vogels

CTO and VP, Amazon.com

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Focus on resiliency



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resiliency choice

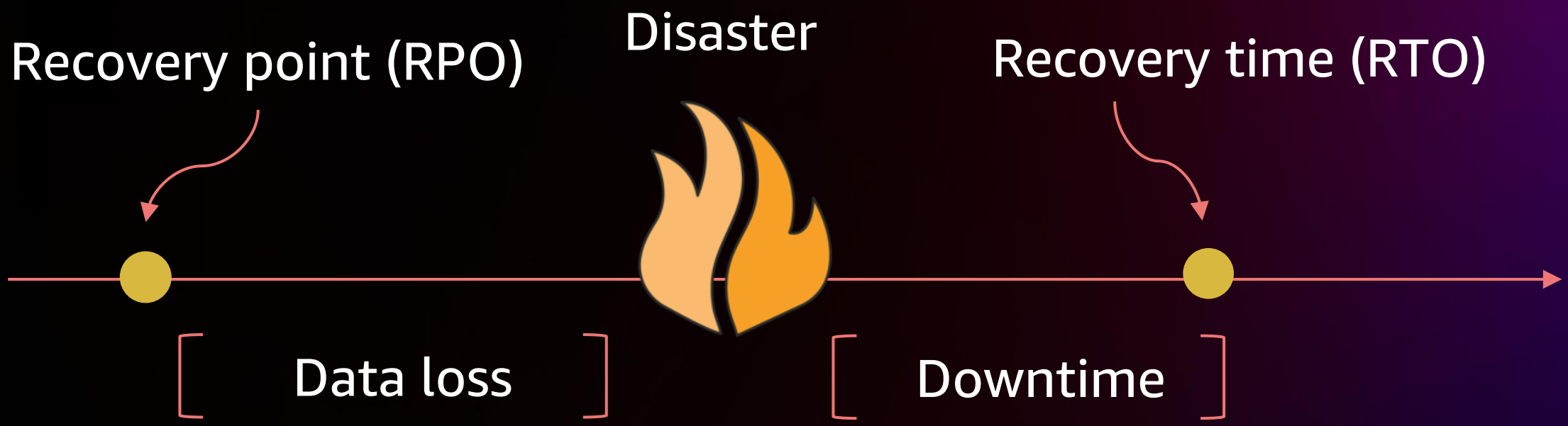
- Resiliency with single AWS Region
  - Zone failure
  - RPO and RTO allow you to wait out regional disaster
  - Service failure (for example, power, internet)
  - Complexity of multi-Region failover setup
- Resiliency with multiple AWS Regions
  - Risk of disruption or loss of multiple data centers
  - Implement cross-Region availability

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Objectives and impacts

How much data can you afford to re-create or lose?

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



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cross-Region services in this workshop

- Amazon DynamoDB Global tables
- Amazon Aurora Global databases
- AWS KMS multi-Region keys
- AWS Secrets Manager key replication to multiple Regions

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“Security is the top priority.”

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS KMS

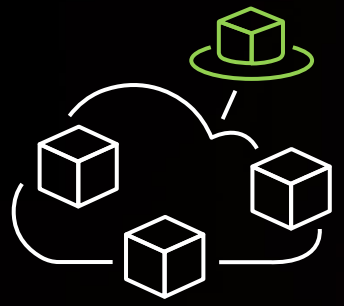
- Centrally manage keys and define access policies
- Encrypt application data using SDK
- Perform signing operations using asymmetric key pairs
- Securely generate hash-based messages (HMAC) that ensures message integrity and authenticity

AWS Secrets Manager

- Securely encrypt and centrally audit secrets
- Manage access using AWS Identity and Access Management (IAM)
- Rotate secrets automatically
- Create and store secrets so that developers don’t view or handle secrets

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why AWS Backup



Simplify backup operations



Ensure compliance and security



Reduce cost and save time

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

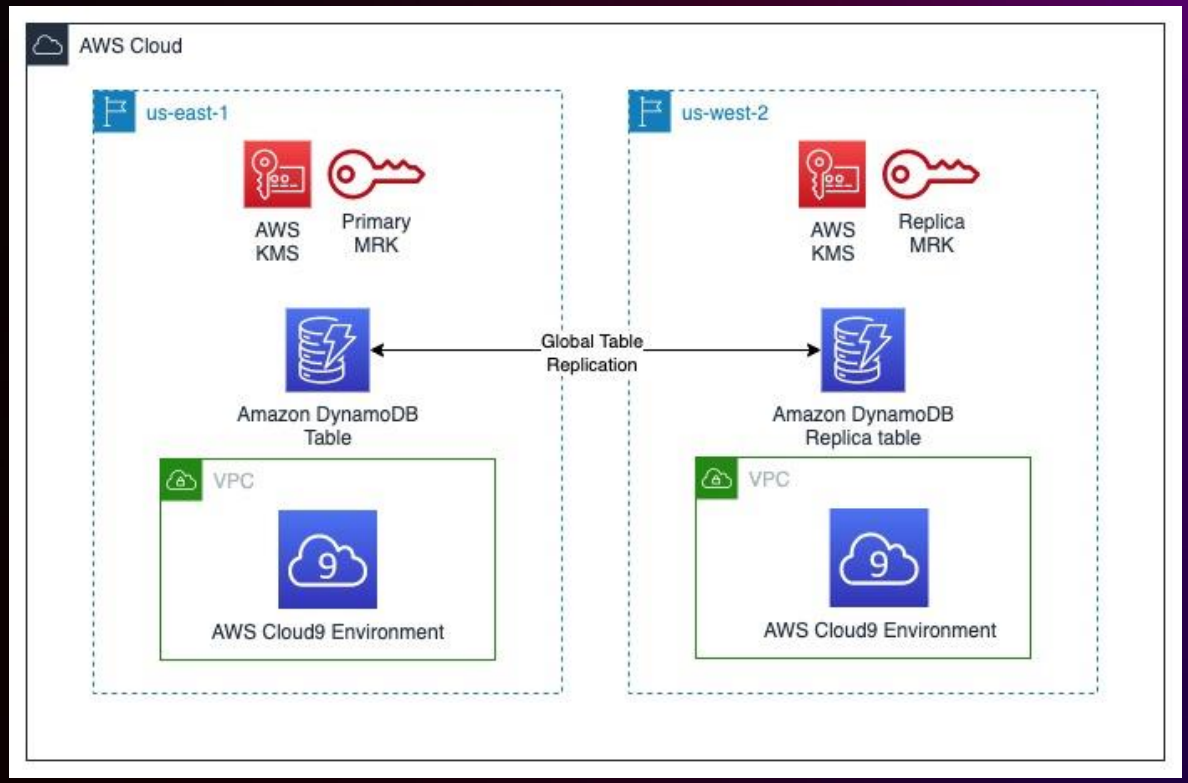
Workshop details

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Builders' session overview

AWS KMS (20 MIN)

- Create multi-Region keys in the primary Region to replicate the key to DR Region
- DR strategy – multi-site/active-active
  - Create a DynamoDB global table and write encrypted data using SDK and AWS KMS multi-Region key
  - Retrieve the data in DR Region by decrypting using AWS KMS multi-Region replica key
- DR strategy – backup and restore
  - Create a DynamoDB table and write encrypted data using AWS KMS multi-Region key
  - Use AWS Backup to create and copy the backup to DR Region
  - Restore the backup to a new table in DR Region
  - Retrieve the data in DR Region by decrypting using AWS KMS multi-Region replica key

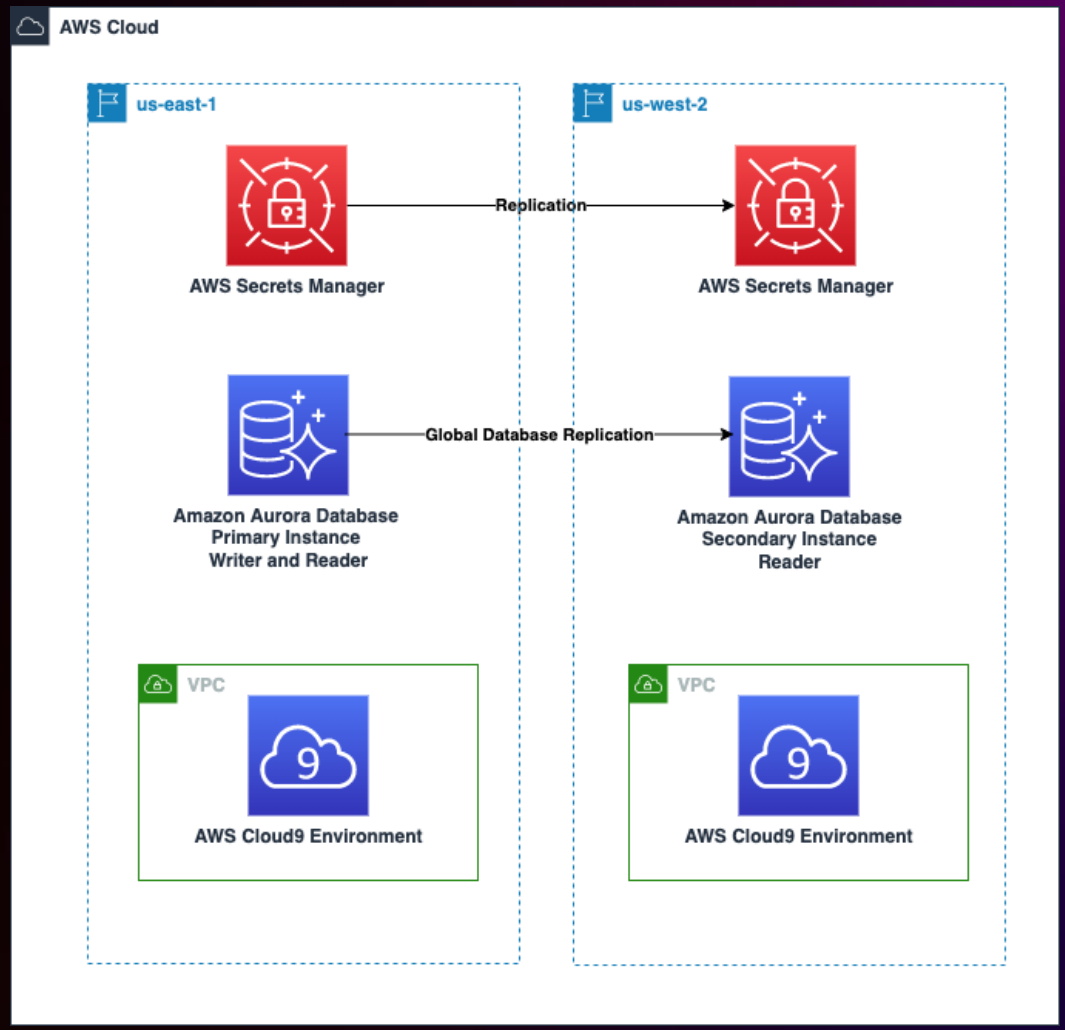


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Builders' session overview

AWS SECRETS MANAGER (20 MIN)

- Create secrets in the primary Region to store DB credentials and replicate the secret to DR Region
- DR strategy – multi-site/active-active
  - Create Amazon Aurora global database, connect to the database using stored credentials in Secrets Manager, and write the data
  - Retrieve the data in DR Region by connecting to the database using stored credentials in Secrets Manager
- DR strategy – backup and restore
  - Create Amazon Aurora global database, connect to the database using stored credentials in Secrets Manager, and write the data
  - Use AWS Backup to create and copy the backup to DR Region
  - Restore the backup to a new database cluster in DR Region
  - Retrieve the data in DR Region by connecting to the database using stored credentials in Secrets Manager



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Logistics for this workshop

Join the workshop:

https://catalog.workshops.aws/join

Event access code:

83a2-09bf69-e3

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Call to action

- Define your disaster recovery strategy
- Review critical services that require low RPO and RTO
- Choose between in-Region resiliency or resiliency across Regions
- Choice of backup/restore or active/passive DR setup
- Set up and test DR

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.