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

STG338

Beyond 11 9s of durability: Data protection with Amazon S3

Peter Imming
Amazon S3, Product Management
AWS

David DeLuca
Senior Storage Solutions Architect
AWS

Yuri Zarubin
Principal Engineer, S3
AWS

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

Agenda

Amazon S3: A safe place to store your data

What do I need to protect against?

How do I view my protection levels in all of my buckets?

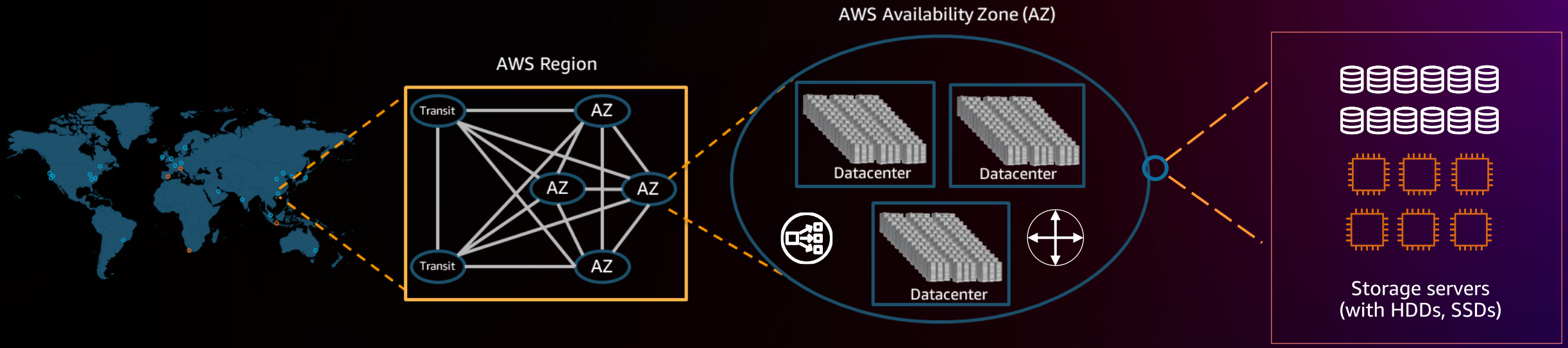
Supplemental protection

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

Amazon S3: A safe place to store your data

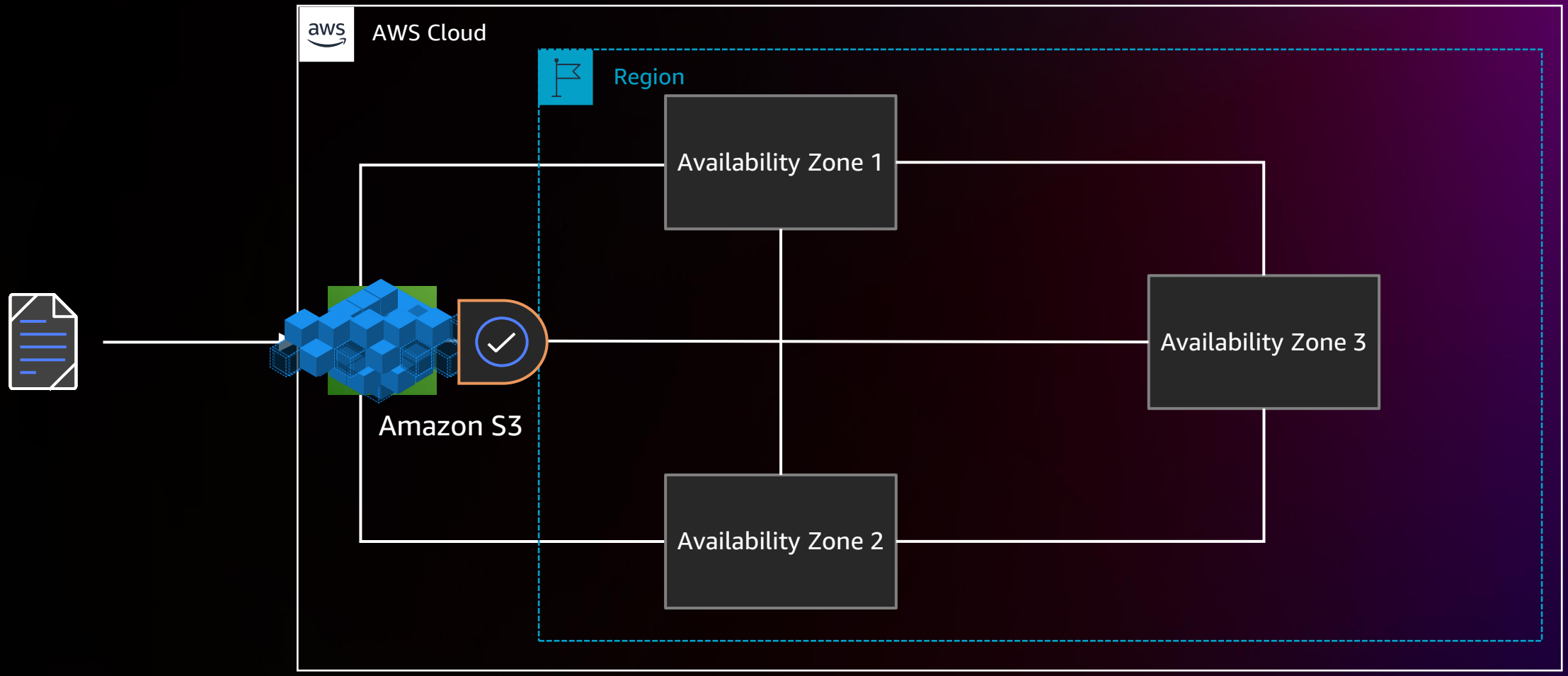
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 architecture: 10,000 foot view



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

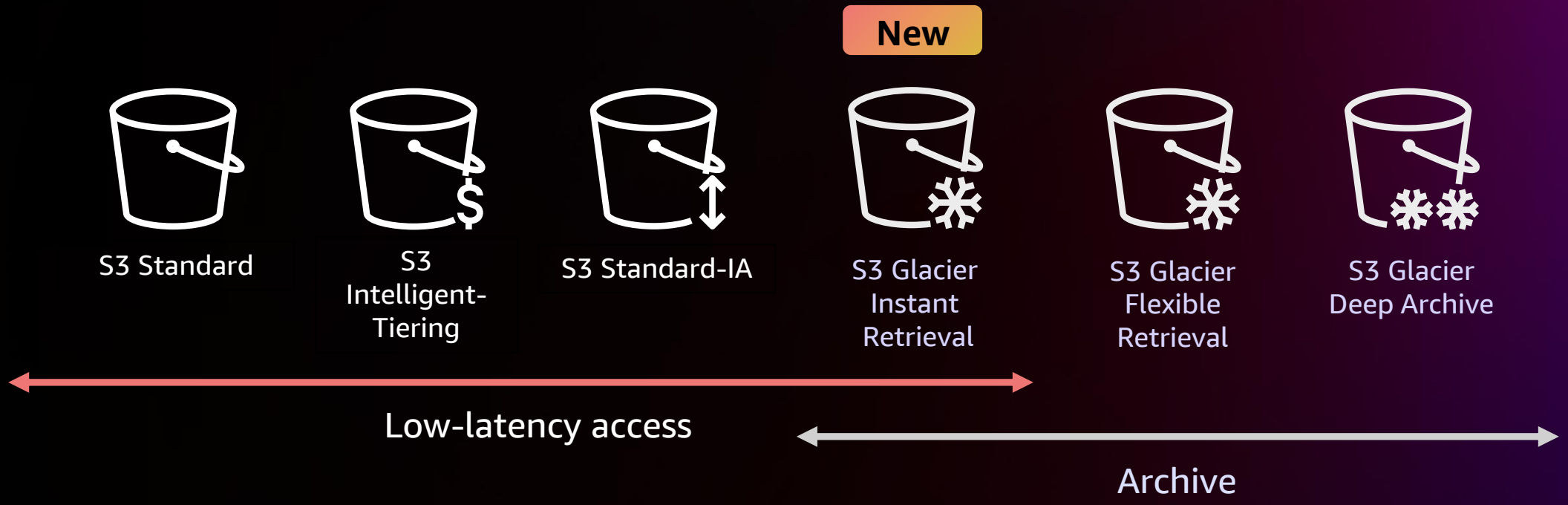
Highly resilient and durable by default



Designed for 99.999999999% of durability

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

Amazon S3 storage classes



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

What do I need to protect against?

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

Protect against these events

Human error

Malicious activity

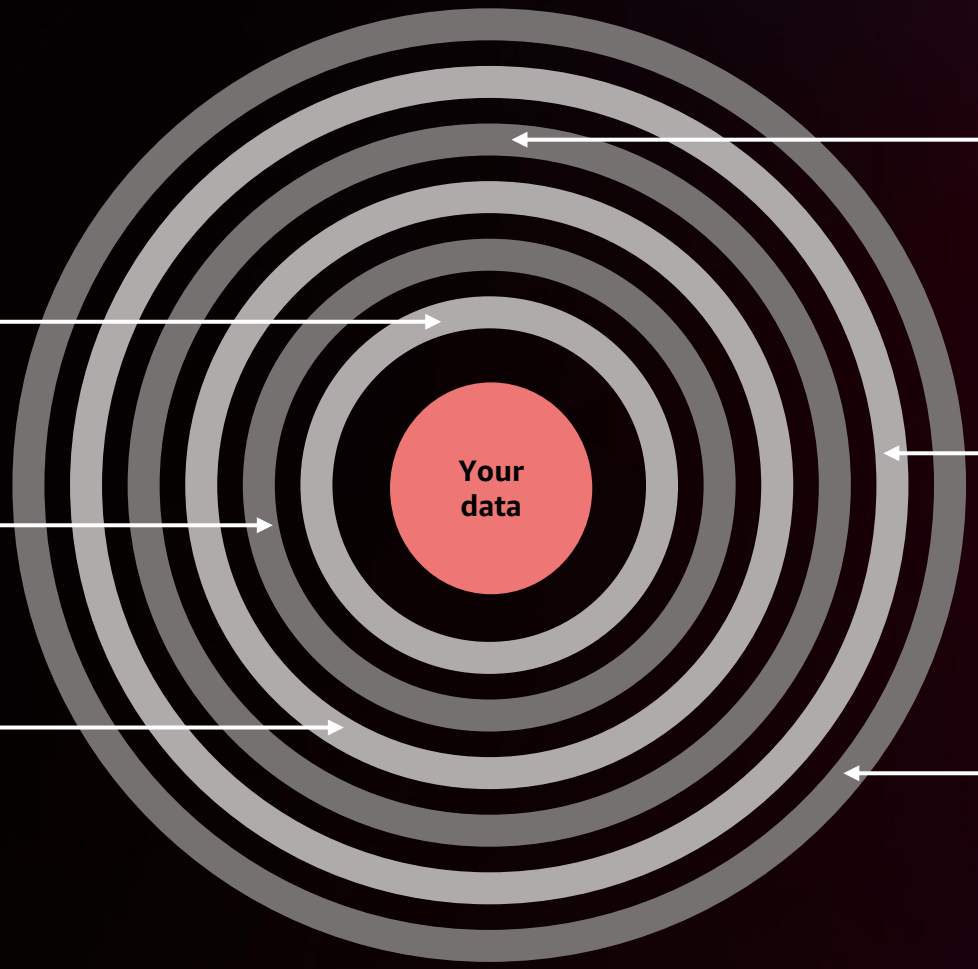
Regional disruption

?

aws

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

Multi-layer data protection



1. IAM policies to restrict user access
2. Enable object-versioning on your S3 buckets
3. Make your data in S3 Immutable (data and backups)
4. Enable replication; use S3 Replication with S3 Replication Time Control for SLA-backed replication performance
5. S3 Storage Lens: Enable S3 Storage Lens to get multi-account level view of data protection settings and risk levels
6. Enhance S3 data protection with supplemental AWS services and AWS Storage Partners

aws

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

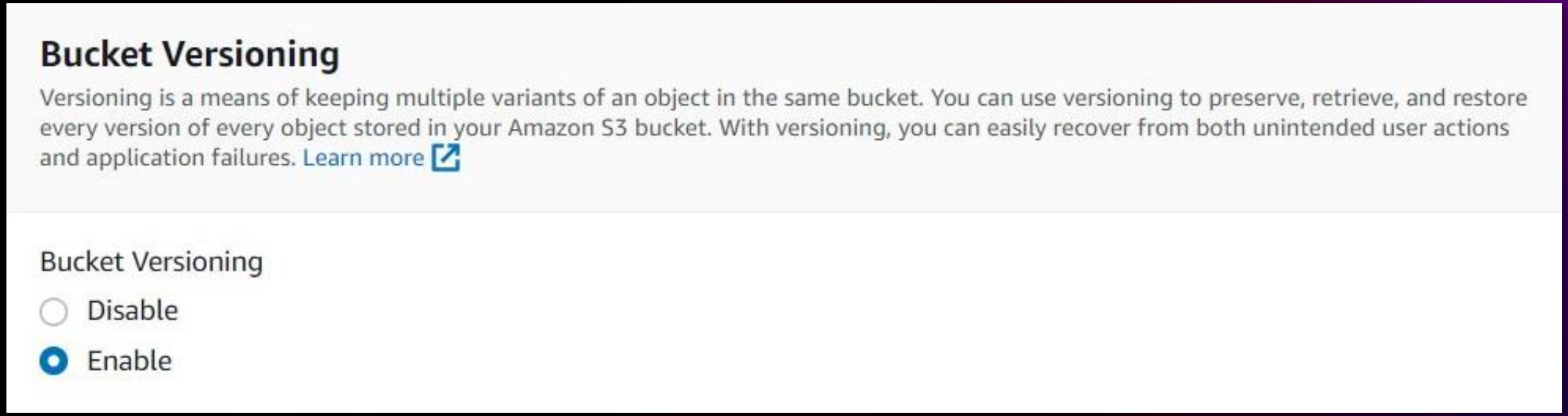


What if I want to protect my data from human error?

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

Amazon S3 Bucket Versioning – The foundation

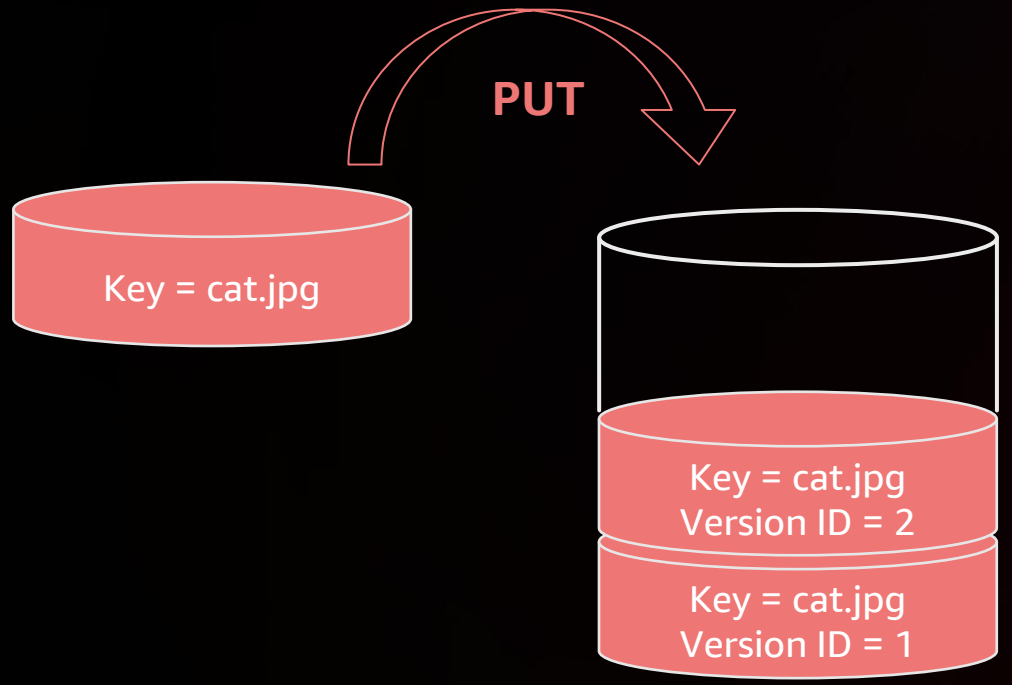
PROTECT YOUR DATA FROM ACCIDENTAL DELETION



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

Amazon S3 Bucket Versioning – The foundation

PROTECT YOUR DATA FROM ACCIDENTAL DELETION



Create a new version with every upload

Previous versions are retained, not overwritten

Protect from unintended user delete

Delete requests without version ID removes access to object but keeps the data

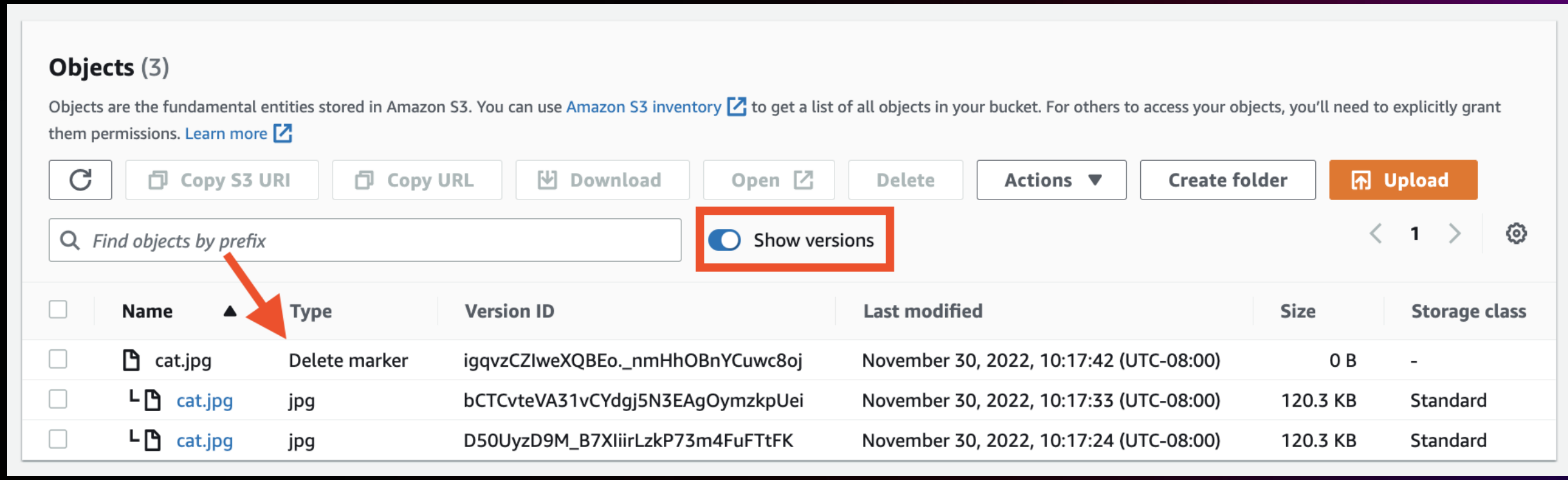
Manage previous versions with lifecycle

Transition or expire objects a specified number of days after they are no longer the current version

aws

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

Amazon S3 Bucket Versioning – The foundation



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

Amazon S3 Bucket Versioning – The foundation

Two ways to permanently delete versioned data:

1. Issuing a delete request against a specific version
2. Using a non-current S3 Lifecycle expiration policy **[recommended]**

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



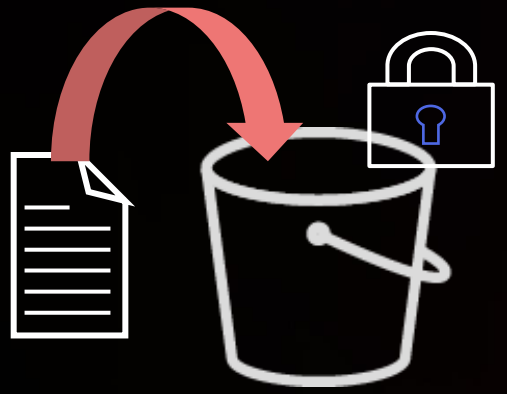
What if I want to protect my data against malicious activity?

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

Amazon S3 Object Lock – Immutable storage

Per object version lock on upload to S3





Bucket default object lock on all new objects

De facto standard

- Enforce write-once-read-many (WORM) policies
- Prevents permanently deleted or overwritten data
- Meet regulatory requirements (SEC 17a-4, CFTC and FINRA)

Multiple Object Lock types

- Governance Mode
- Compliance Mode
- Legal Hold

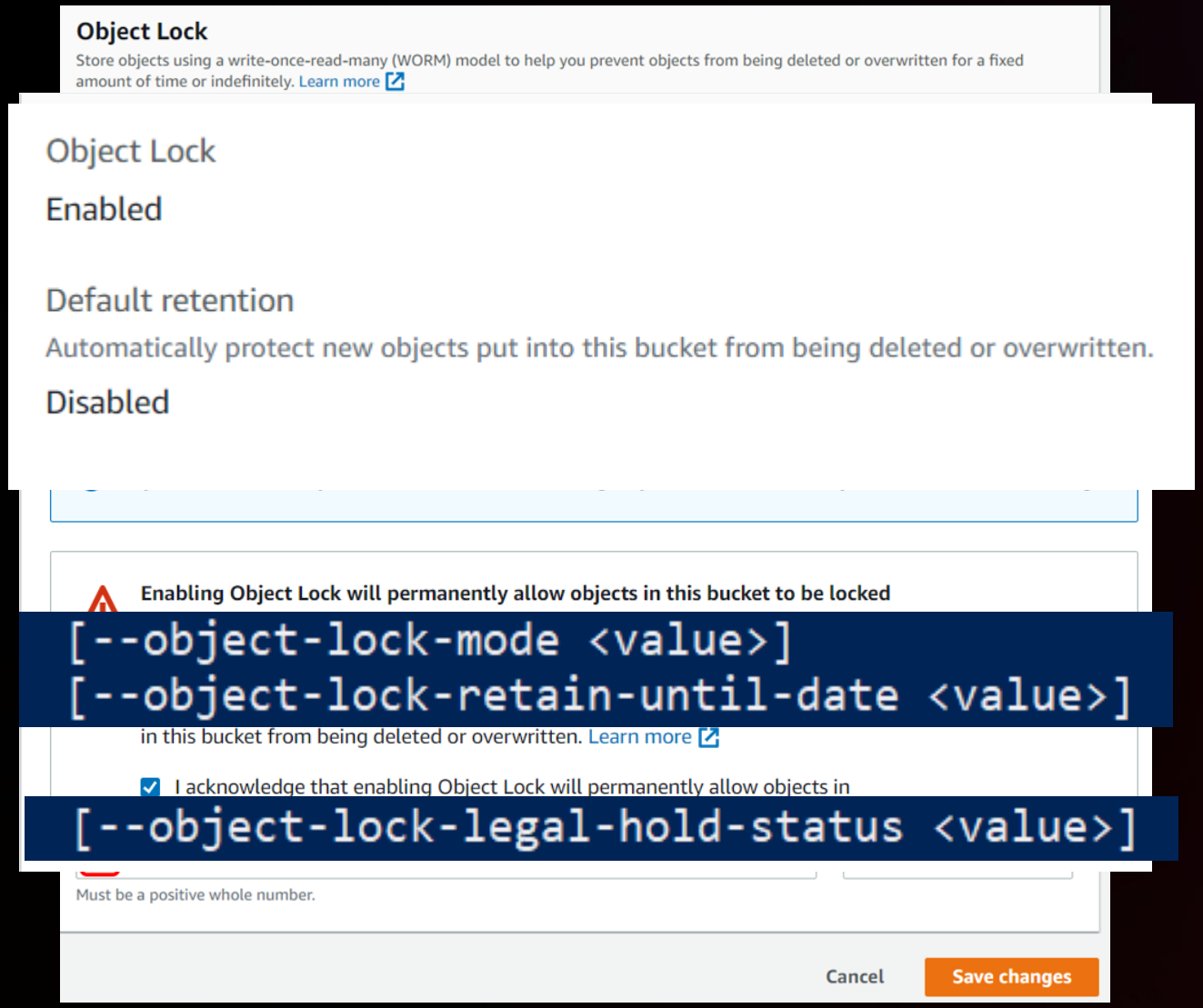
Managing Object Lock at scale

- Batch Operations

aws

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

S3 Object Lock – Configuration



Flexible configuration

- Enable at the bucket level
- Apply custom retention for individual objects
  - Object Lock mode and Retention Period
  - Legal Hold

Optional default retention settings

- Apply to objects placed in bucket unless you explicitly specify different settings at upload

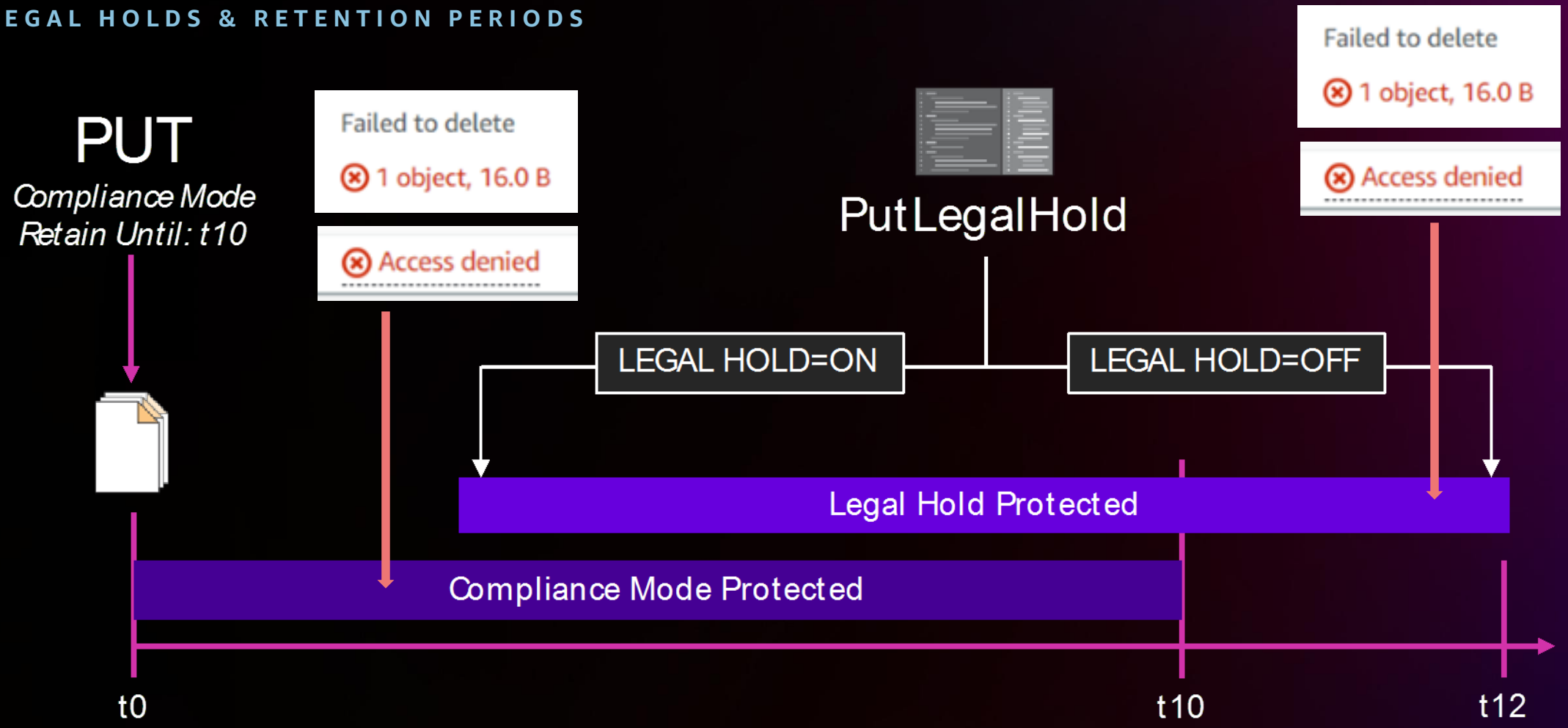
Integration with other S3 features

- Versioning
- Lifecycle
- Replication

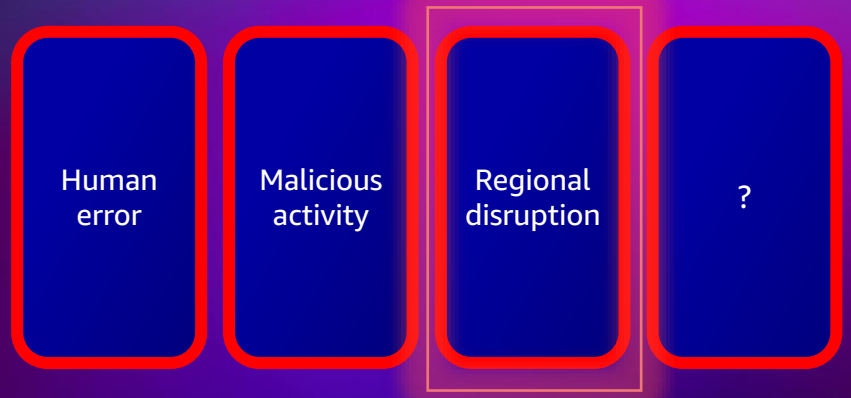
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3 Object Lock – How it works

LEGAL HOLDS & RETENTION PERIODS



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



What if I want to protect my data from regional disruptions?

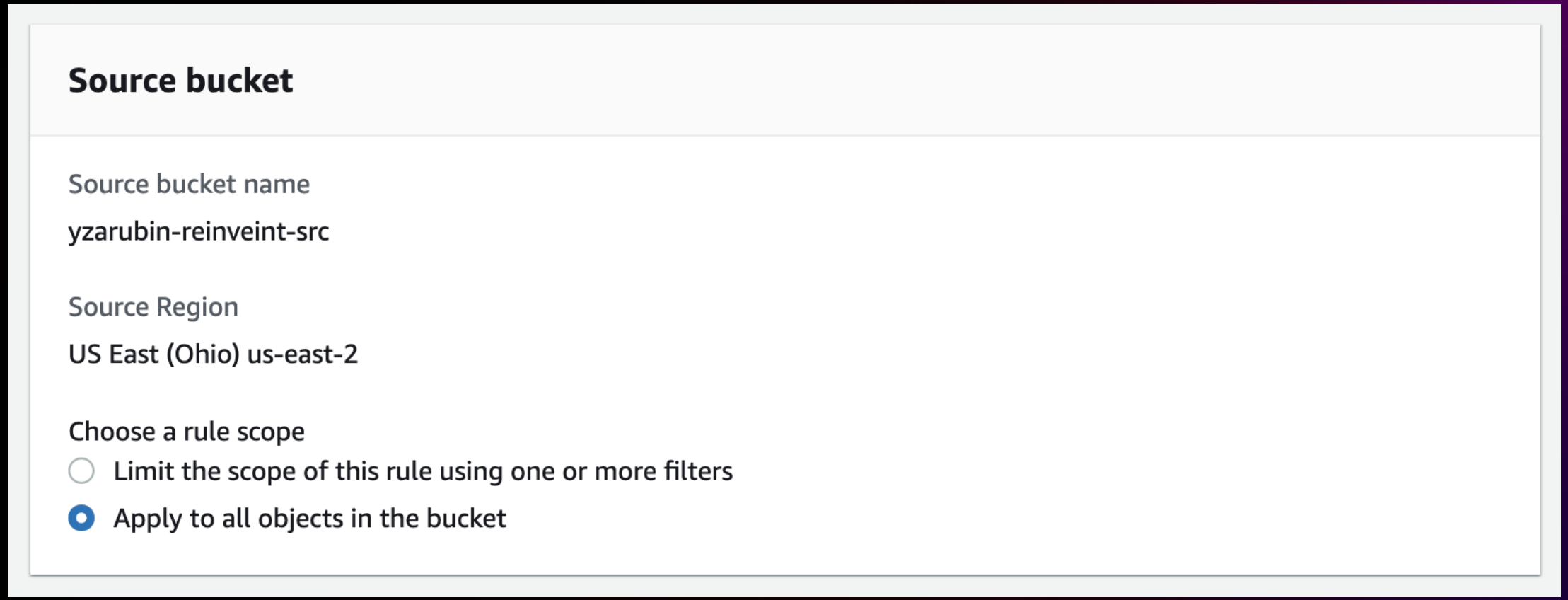
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 Replication

100 PB

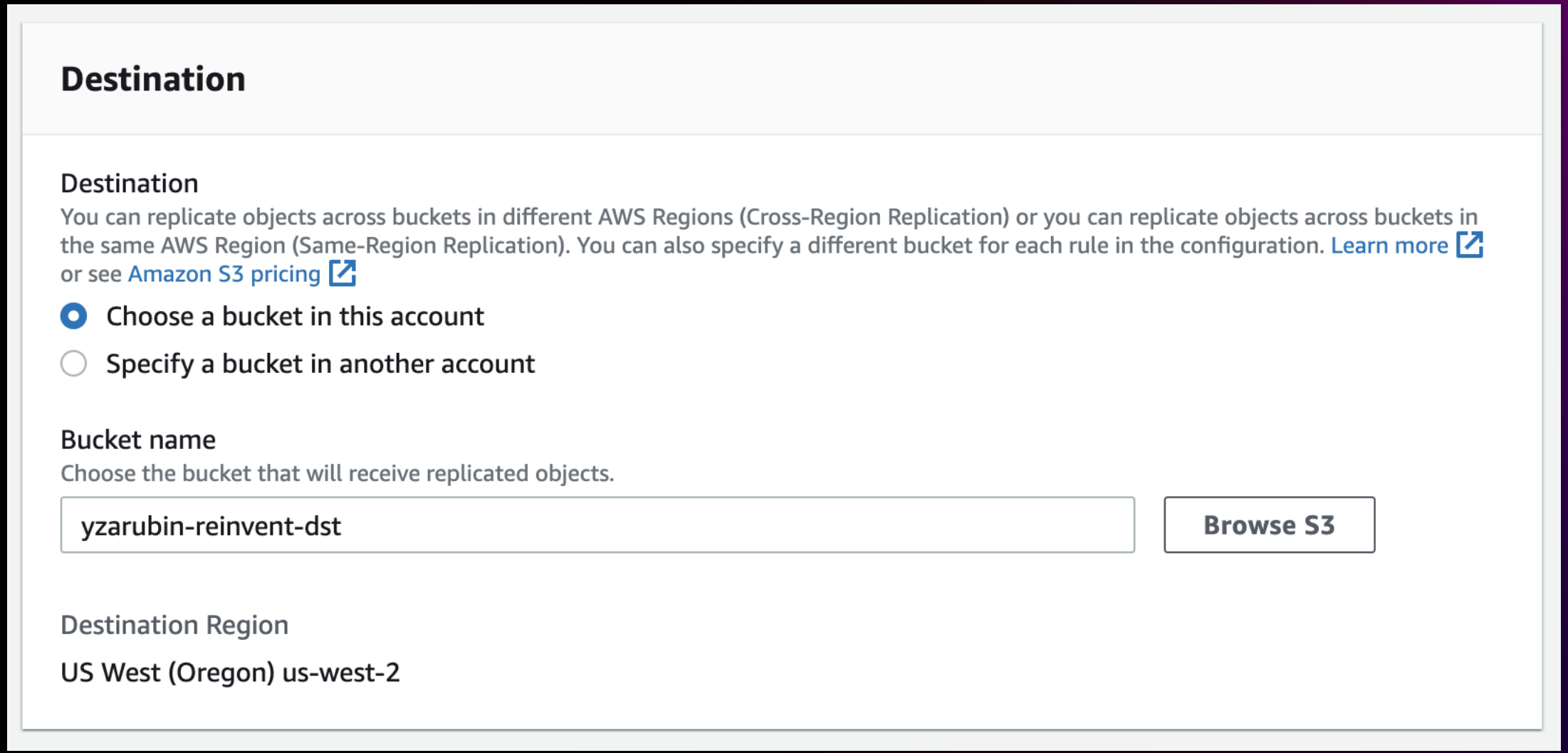
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 Replication



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

Amazon S3 Replication



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

Amazon S3 Replication



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

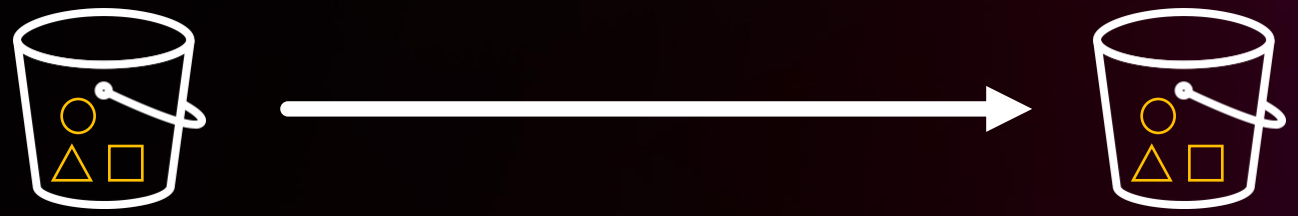
Amazon S3 Replication

```
<ReplicationConfiguration>
     <Role>arn:aws:iam::account-id:role/role-name</Role>
     <Rule>
          <ID>UE2_UW2</ID>
          <Priority>0</Priority>
          <Destination>
               <Bucket>arn:aws:s3:::yzarubin-reinvent-dst</Bucket>
          </Destination>
          <Status>Enabled</Status>
          <DeleteMarkerReplication>
               <Status>Enabled</Status>
          </DeleteMarkerReplication>
          <Filter/>
     </Rule>
<ReplicationConfiguration>
```

aws

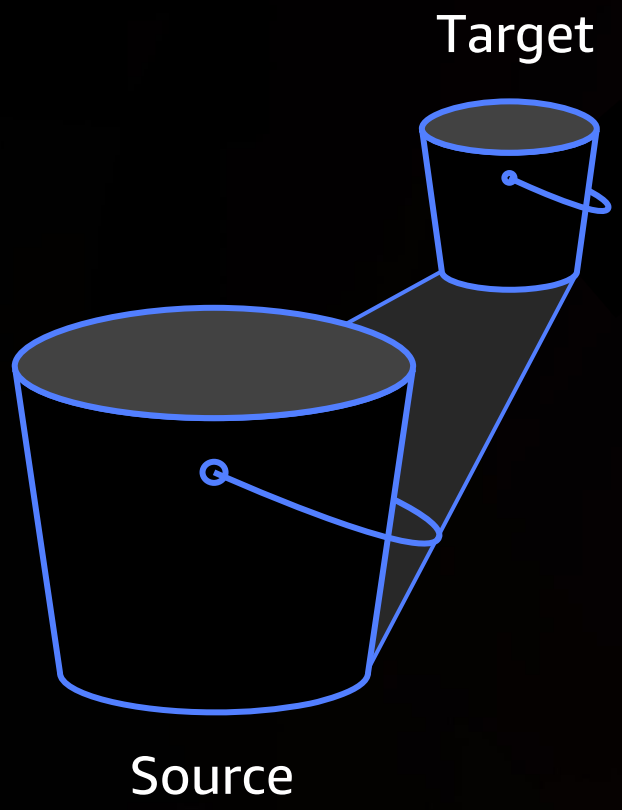
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 Replication



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

Amazon S3 Replication



Select

Select data

Replicate the whole bucket
. . . or based on a prefix
. . . or based on object tags

Protect

Select a Region

Replicate to any second AWS Region
Continuous replication as your data changes
Satisfy distance and residency requirements

Change ownership

Automatically change ACLs on replica objects
Reset object-level permissions
Protect against bad actors & IAM account compromise

Cross-account

Replicate into a second account
Often this is a locked down “Archive” account
Protect against AWS root account compromise

Optimize

Set storage class

Maintain production access characteristics
. . . or put and Lifecycle
. . . or replicate straight to Amazon S3 Glacier

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

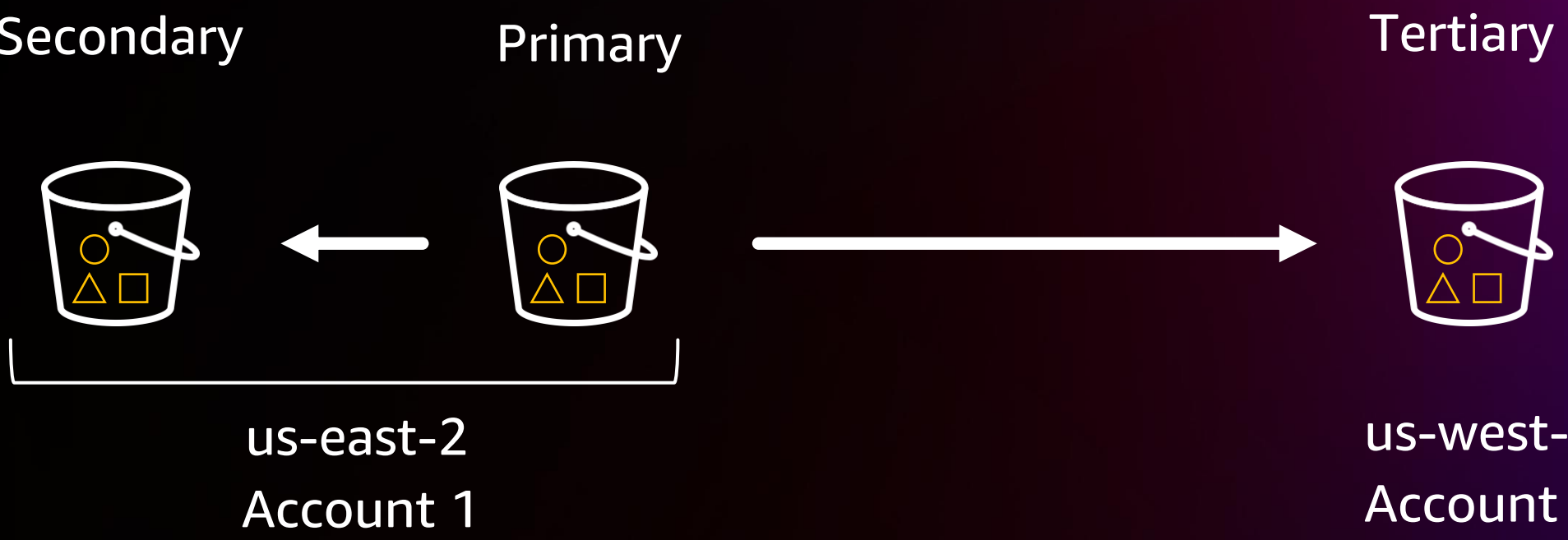
Amazon S3 Replication

The 3-2-1 rule:

- Three copies of data
- Two backup copies on different storage media
- One backup copy offsite

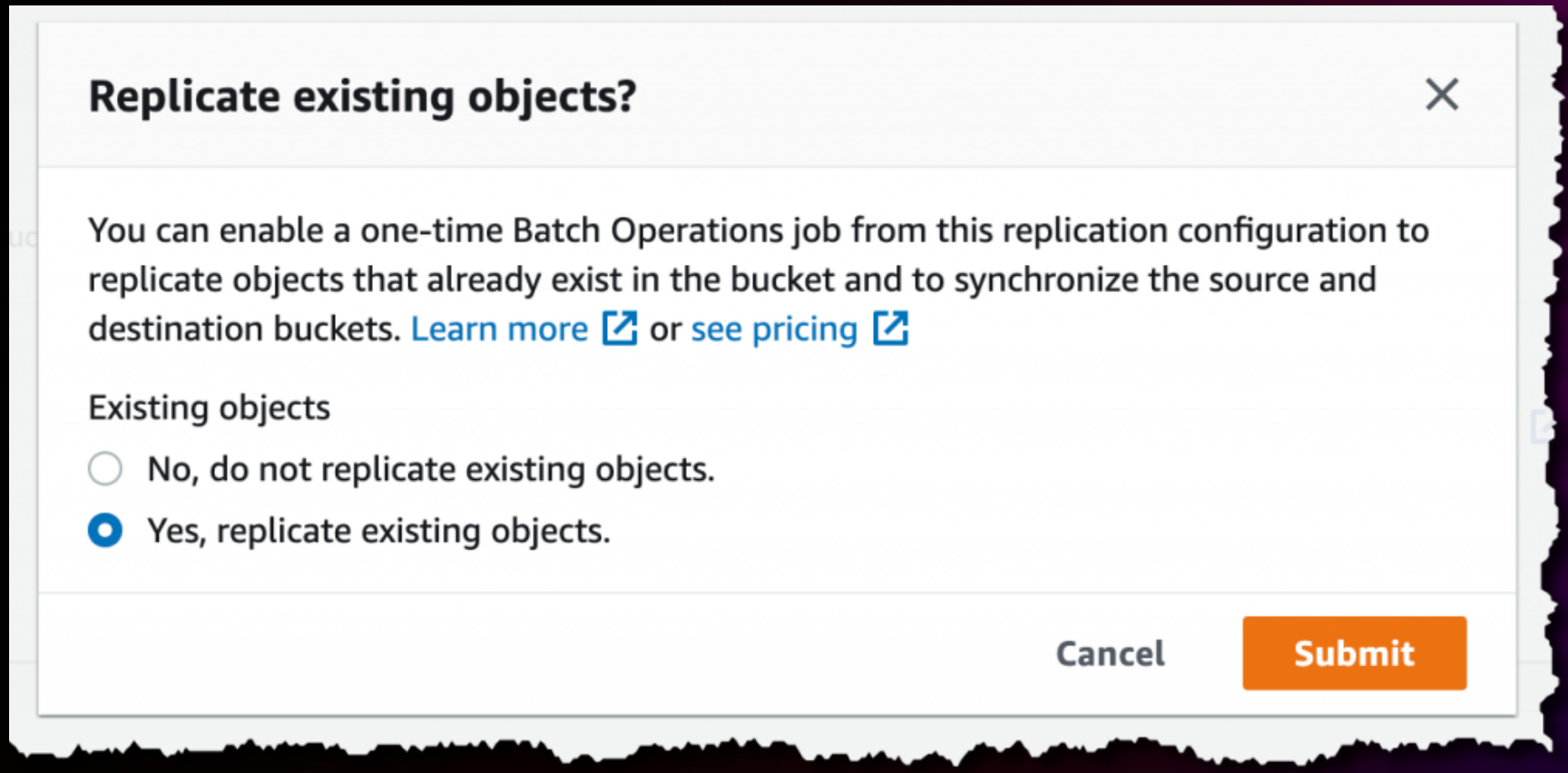
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 Replication



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

Amazon S3 Replication – Existing objects



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

S3 Replication Time Control



Predictable replication time
Replicate objects within 15 mins of upload



SLA-backed replication
Commitment to replicate 99.9% of objects in 15 mins or less

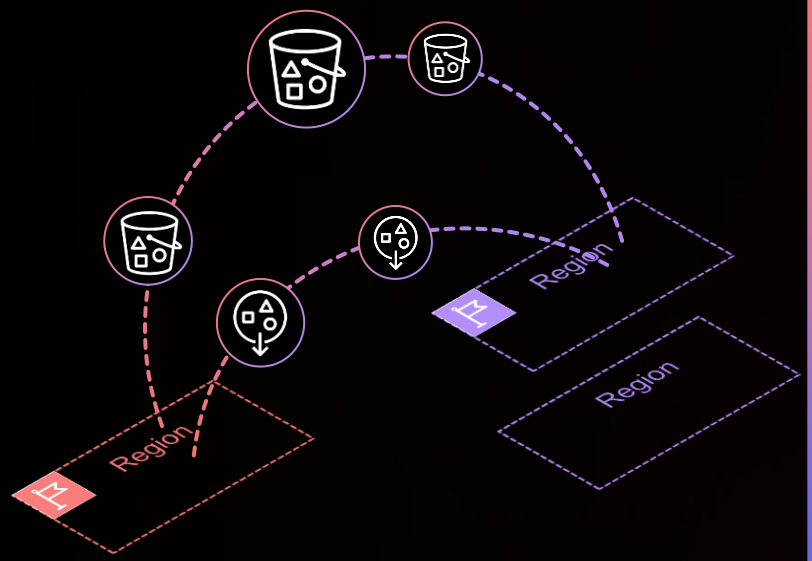
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

re:Invent

AVAILABLE NOW

Amazon S3 Multi-Region Access Points failover controls

SUPPORT AN ACTIVE-PASSIVE CONFIGURATION AND CUSTOMER-INITIATED FAILOVER



Perform disaster recovery and application failover testing in an active-passive configuration

Build high-availability to maximize uptime for business-critical applications

Automatically replicate S3 objects across AWS Regions you define to maintain copies of your data

Shift S3 data access requests to another AWS Region within minutes

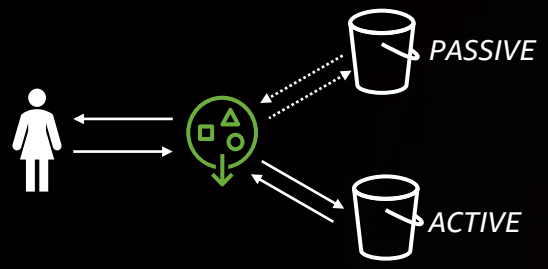
Failover

aws

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

Better together: Combining S3 features

MRAP Failover



Improve **performance** with dynamic request routing

Simplify development of multi-Region apps

Automatic or customer-managed failover

S3 Intelligent-Tiering Class



Automatic cost savings on data in both primary and secondary Regions

No retrieval fees for infrequently accessed data after failover

S3 Replication Time Control



SLA-based bidirectional replication (<15 min for 99.9% of objects)

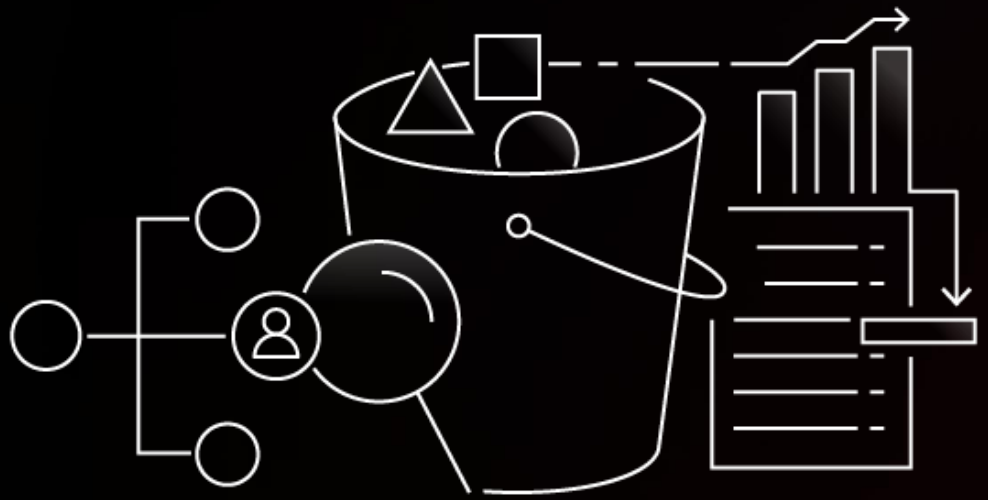
Precisely replicate **some or all** data in a bucket

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

How do I view my protection levels in all of my buckets?

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

S3 Storage Lens overview

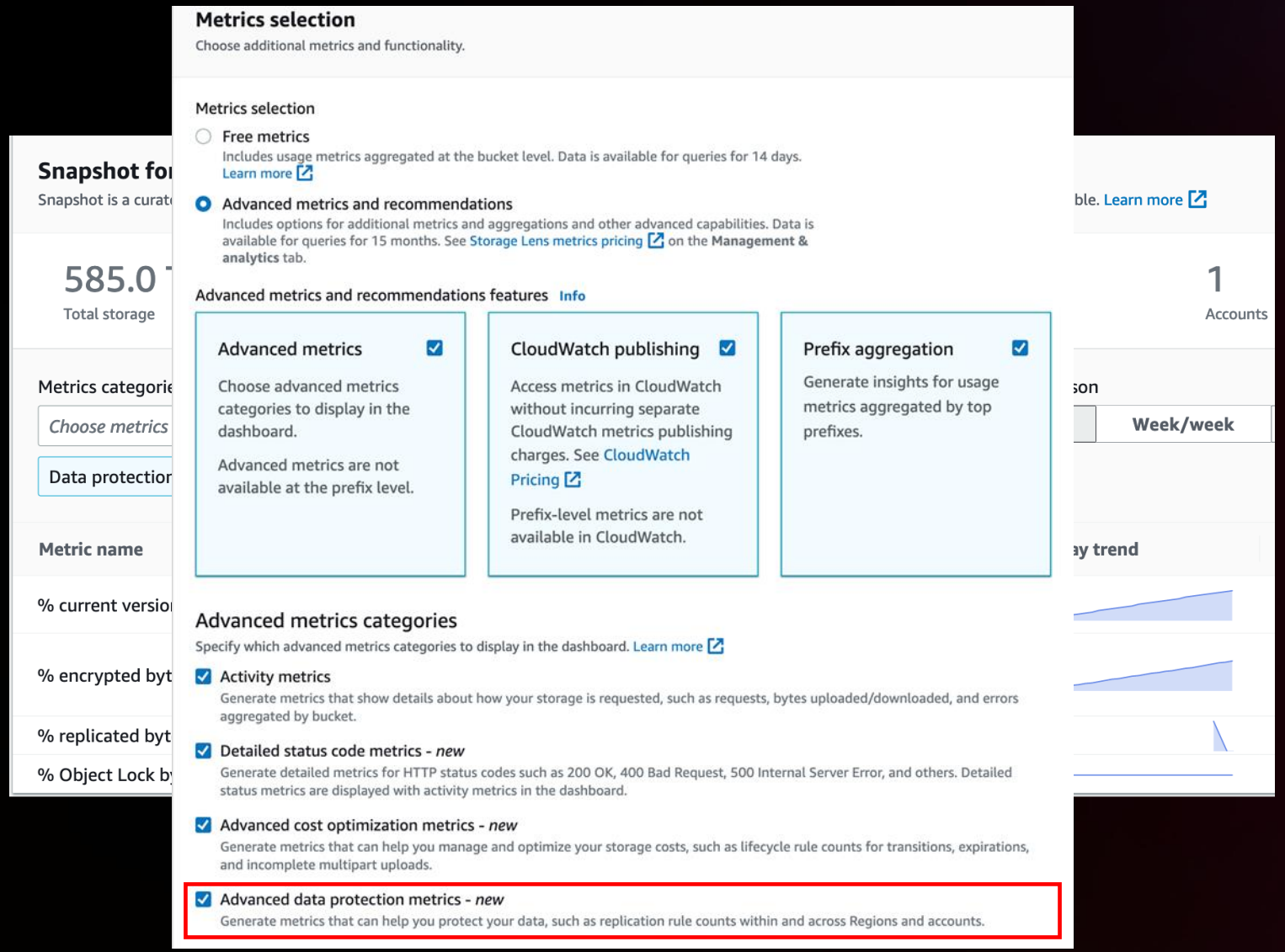


- Interactive dashboard experience in the S3 console – auto-configured
- Organization-wide visibility
- Drill down by Region, storage class, bucket, and prefix
- Granular usage & activity metrics
- Automated alarms & anomaly detection

aws

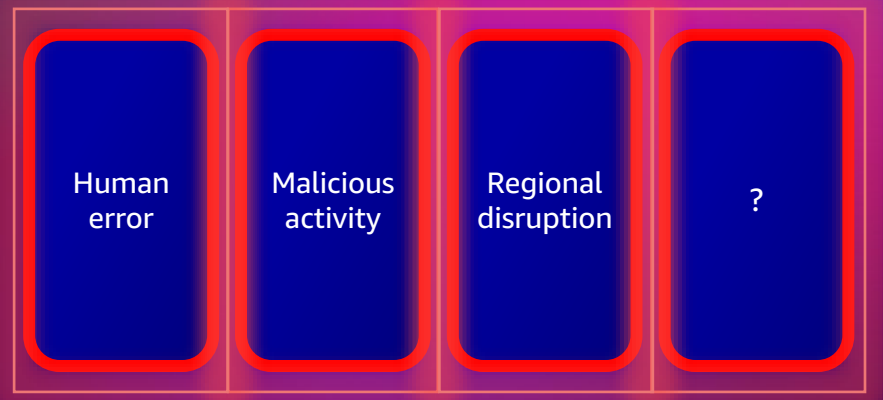
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data protection in S3 Storage Lens



- Every customer gets a default dashboard in S3 Storage Lens
- Automatically includes 14 days of historical data
- Data protection metrics include:
  - **Versioning**
  - **Encryption**
  - **Replication**
  - **Object Lock**

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



Supplemental protection

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

Detection, prevention, and recovery

Configuration
Provides an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance

AWS Config



Identification
Discovery of sensitive data at scale and lowers the cost of protecting your data with Amazon Macie

Amazon Macie



Protection
Enhance S3 data protection with supplemental AWS services and AWS Storage Partners



Partner
Backup Software

Detection
Amazon GuardDuty threat detection service continuously monitors your AWS accounts and workloads for malicious activity

Amazon GuardDuty for S3



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

Key takeaways

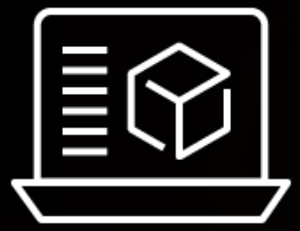
- S3 is **a safe place to store your data**
- Leverage native S3 data protection features: **Versioning, Object Lock, and Replication** – Getting started tutorials and step-by-step guides
- Control **business continuity** with S3 Multi-Region Access Points
- Use S3 Storage Lens to gain visibility into your **data protection levels**
- Enhance S3 **data protection** with supplemental AWS services and AWS Storage Partners

aws

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

Continue your AWS storage learning

Build a learning plan



Set your AWS storage learning plans via **AWS Skill Builder**

Increase your knowledge



Use **AWS Ramp-Up Guides** to build your storage knowledge

Earn AWS storage badges



Demonstrate your knowledge by achieving **digital badges**

aws.training/storage

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

Thank you!

Peter Imming
ptimming@amazon.com

David DeLuca
davdeluc@amazon.com

Yuri Zarubin
yzarubin@amazon.com



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

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