

AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV



STG337

Best practices for managing S3 data at scale, with Bridgewater Associates

Shakhi Hali (she/her)

Senior PMT – External
Services, Amazon S3
AWS

Rob Wilson (he/him)

Senior Manager, Product
Management, Amazon S3
AWS

Robin Anil (he/him)

Director, Research Technology
Bridgewater Associates



Agenda

Overview of Amazon S3

Use case deep dives

- Securing your data
- Accessing archive data
- Monitoring access
- Managing storage spend

Customer voice: Bridgewater Associates

Recap



Overview of Amazon S3



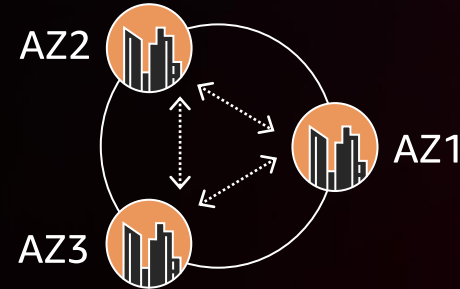
Operate at scale with Amazon S3

DESIGNED FOR 11 9S OF DURABILITY



30 Regions

Geographic locations with multiple AZs, separated physically by miles and isolated



96 Availability Zones (AZs)

Objects stored across multiple devices spanning a minimum of 3 AZs

Multi-AZ storage classes function normally if an AZ is lost



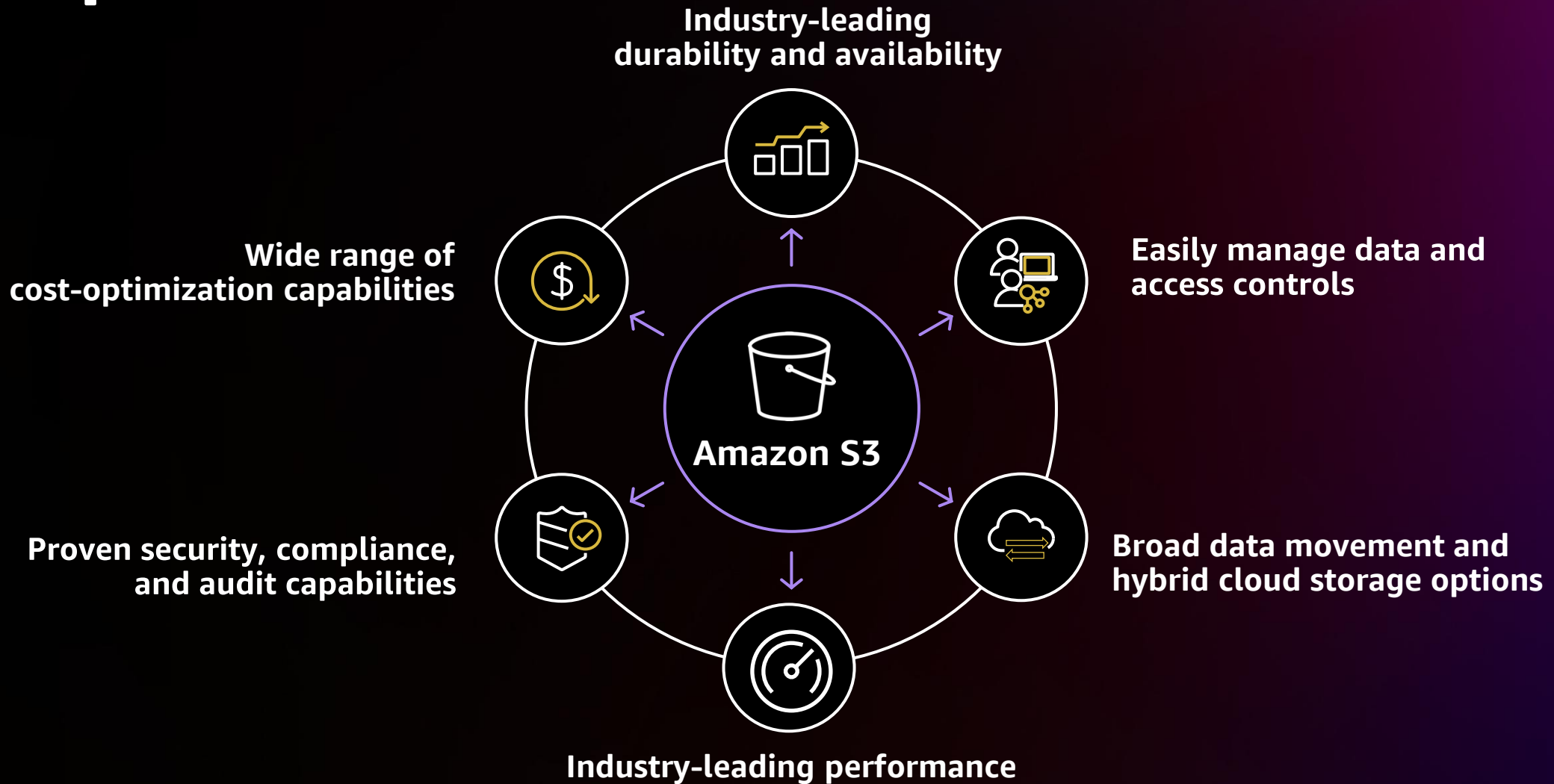
Highly durable

Designed to sustain concurrent device failures and data in the event of an entire AZ loss

Operational performance is second only to security



Industry-leading durability, availability, and performance



AWS storage customers



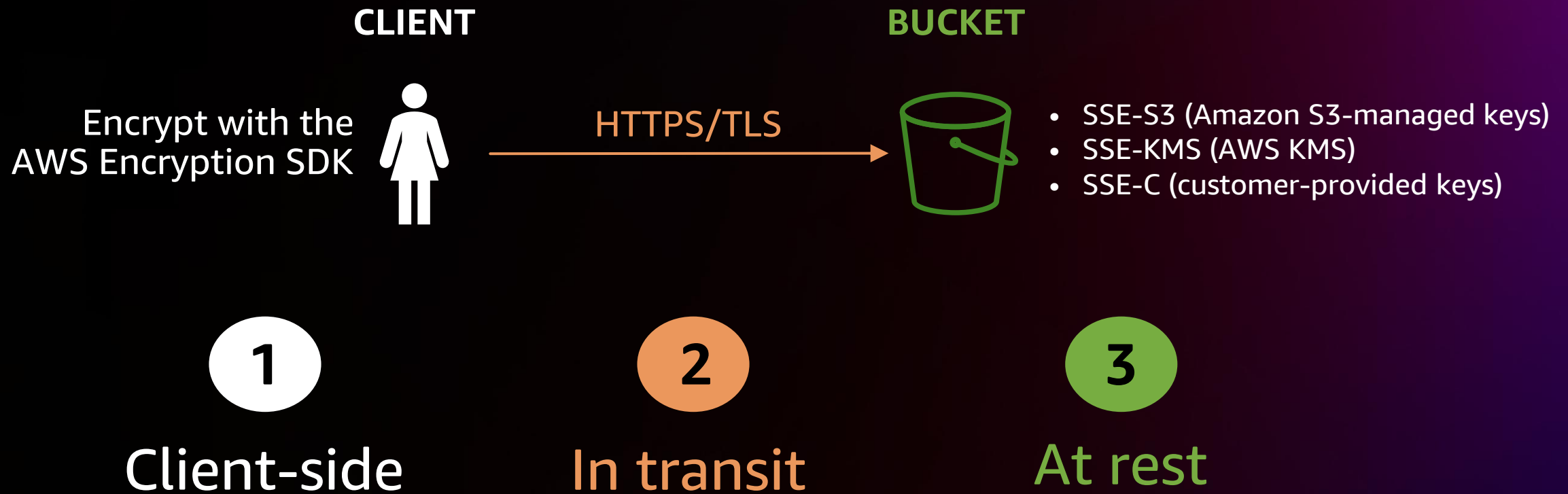
Use case deep dives



Securing your data: Encryption at scale



Amazon S3 encryption support



Amazon S3 default encryption



Bucket-level
setting



Automatically
encrypt all new
objects



Simplified
compliance



Supports SSE-S3
and SSE-KMS

Provides Amazon S3 encryption-at-rest support for applications that do not otherwise support encrypting data in Amazon S3

Customer use case 1

The cloud security lead calls a meeting for a detailed security review

The objects stored in Amazon S3 are subject to a wide range of regulatory guidelines

You need to provide a compliance report proving that all the objects stored are encrypted

Default encryption

S3 Inventory

S3 Batch Operations

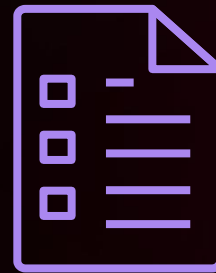
Approach to encrypting your existing objects



Default encryption



S3 Storage Lens



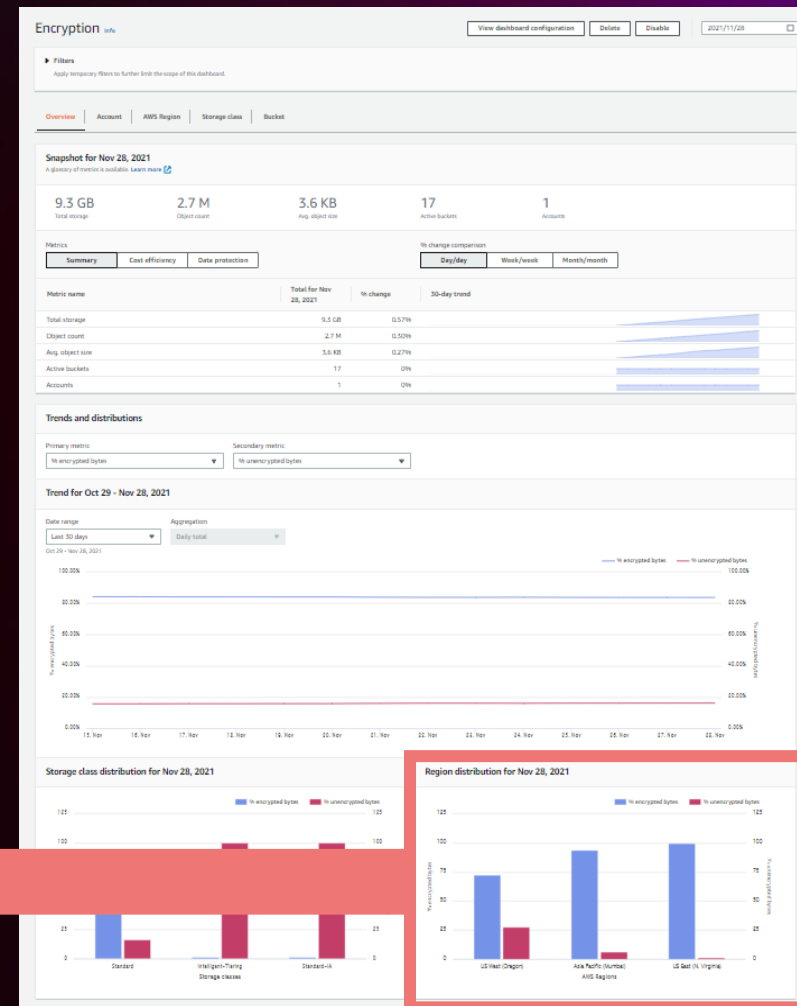
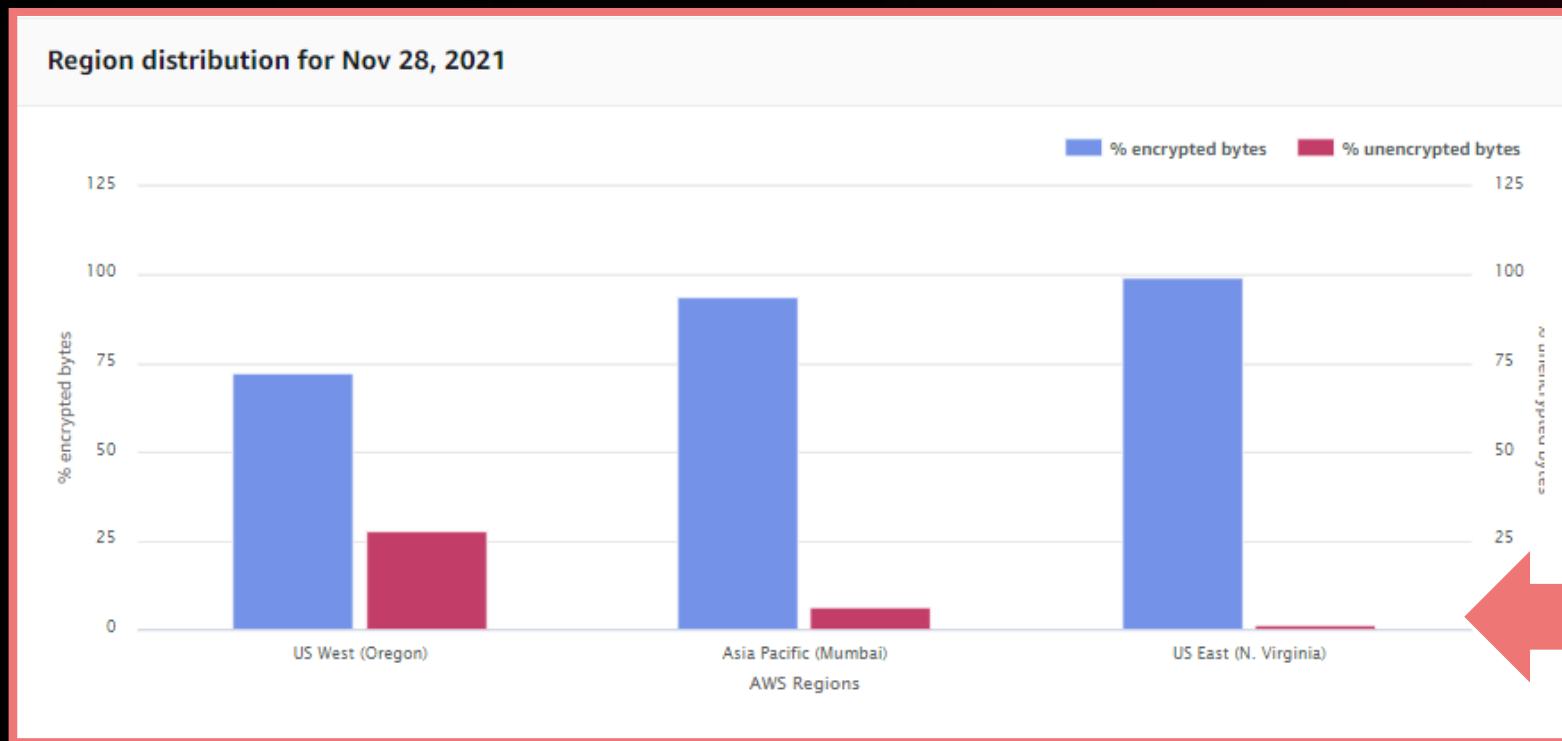
Inventory



S3 Batch Operations

Encryption insights on your existing objects in S3 Storage Lens

UNDERSTAND YOUR ORGANIZATION-WIDE PERCENTAGE ENCRYPTION BYTES BY REGION AND BUCKETS



Set up S3 Inventory to identify existing objects

Amazon S3 > managing-storage-at-scale-reinvent-bucket-005 > Management > Inventory configurations > Create inventory configuration

Create inventory configuration

Inventory configuration name

Inventory configuration name

The name can contain up to 64 characters using letters, numbers, underscores, periods, or dashes.

Inventory scope

Prefix - optional
Limit the scope of this configuration to a single prefix.

Don't include the bucket name in the prefix.

Object versions

Current version only

Include all versions

Report details

Destination bucket
Choose the destination bucket where you want reports to be saved. The destination bucket must be in the same AWS Region as the source bucket. [Learn more](#)

This account

A different account

Destination
Choose or enter the destination bucket that will receive the inventory reports.

Format: s3://bucket/prefix

The following statement will be added to the destination bucket policy to allow Amazon S3 to place data in that bucket. [Learn more](#)

```
{
  "Sid": "InventoryAndAnalyticsExamplePolicy",
  "Effect": "Allow",
  "Principal": {
    "Service": "s3.amazonaws.com"
  },
  "Action": [
    "s3:PutObject"
  ]
}
```

Frequency
Choose how often the report will be generated.

Daily
The first report will be delivered within 48 hours.

Weekly
The first report will be delivered within 48 hours and subsequent reports will be delivered on Sundays.

Output format
Choose an output format based on the number of objects that you expect to list or the analysis tool that you want to use. [Learn more](#)

CSV
Choose this format if you plan to use Batch Operations or if you plan to analyze S3 Inventory with tools like Microsoft Excel.

Apache ORC

Apache Parquet

Status
Choose whether the configuration will be enabled to publish inventory reports.

Disable

Enable

Server-side encryption

Server-side encryption

Disable

Enable

Additional fields - optional
Choose the metadata that should be included for each listed object in the report. [Learn more](#)

Fields

Size

Last modified

Storage class

ETag

Multipart upload

Replication status

Encryption

Intelligent-Tiering: Access tier

All Object Lock configurations

- Object Lock: Retention mode
- Object Lock: Retain until date
- Object Lock: Legal hold status

Use Amazon Athena to filter objects "NOT-SSE" in S3 Inventory

The screenshot displays the Amazon Athena Query Editor interface. The main area shows a SQL query for "New query 8":

```
1 SELECT *  
2 FROM s3_inventory_database  
3 WHERE encryption_status="NOT-SSE"
```

The interface includes a left sidebar with "Data" settings (Data source: AwsDataCatalog, Database: demographic) and a "Tables and views" section listing tables like "australia", "canada", "uk", and "unitedstates". The bottom section shows the "Query results" area, which currently displays "Results (0)" and "No results".

Use S3 Batch Operations to operate on millions and billions of objects

Choose objects

- S3 Inventory report
- CSV list

Select an operation

- Copy
- Invoke Lambda functions
- Replace all object tags
- Replace access control list (ACL)
- Restore from S3 Glacier
- Set Object Lock retention
- Set Object Lock legal hold
- Delete object tags

View progress

- Object-level progress
- Job notifications
- Completion report

S3 Batch Operations code for creating encrypted copy of objects

```
aws s3control create-job \  
  --region us-west-2 \  
  --account-id 12345678\  
  --operation '{"S3PutObjectCopy": { "TargetResource": "arn:aws:s3:::destination-bucket" }}' \  
  --manifest  
  '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":["Bucket","Key"],"Location":{"ObjectArn":"arn:aws:s3:::my_manifests/manifest.csv","ETag":"60e460c9d1046e73f7dde5043ac3ae85"}}}' \  
  --report '{"Bucket":"arn:aws:s3:::bucket-where-completion-report-goes","Prefix":"final-reports",  
"Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \  
  --priority 42 \  
  --role-arn IAM-role \  
  --client-request-token $(uuidgen) \  
  --description "job Description" \  
  --no-confirmation-required
```

Accessing archive data from Amazon S3 Glacier



Why archive to AWS?



Lowest
cost



Durability
& resilience



Security &
compliance

S3 Glacier storage classes



S3 Intelligent-Tiering



S3 Standard



S3 Standard-IA



S3 Glacier Instant Retrieval



S3 Glacier Flexible Retrieval (formerly S3 Glacier)



S3 Glacier Deep Archive



S3 One Zone-IA



S3 on Outposts

AWS Region | 3 Availability Zones (AZs)

Data with changing access patterns

- Millisecond access
- No retrieval fees
- Object monitoring charge
- Opt-in async archive tiers
- **Archive Instant Access tier**

Frequently accessed data

- Millisecond access

Infrequently accessed data

- Millisecond access

Rarely accessed data

Millisecond access

Archive data

- Retrieval options from minutes to hours
- **Free bulk retrievals**

Long-term archive data

- Retrieval in hours

AWS AZ

Re-creatable, infrequently accessed data

- Millisecond access
- Single AZ resiliency

AWS Outposts

On-premises data

- Millisecond access

Increased throughput (10x) for Amazon S3 Glacier

New!

UP TO 90% FASTER RETRIEVALS FROM S3 GLACIER FLEXIBLE RETRIEVAL, S3 GLACIER DEEP ARCHIVE



Launch blog

Automatically applies to S3 Glacier Flexible Retrieval and S3 Glacier Deep Archive (standard and bulk retrievals) at no additional cost

Supports restore requests at a rate of up to 1,000 transactions per second, per account in an AWS Region

Ideal for restoring backups, responding to audit requests, retraining machine learning models, and performing analytics on historical data

Significantly reduces the restore completion time for datasets composed of small objects

Customer use case 2

Your data science team now wants to access long-term archival datasets to train their machine learning model

How can you provide quick and easy access to archives to your data science teams?

S3 Glacier storage classes

S3 Glacier increase in throughput 

Restore using S3 Batch Operations

Restore notifications using S3 Event Notifications

Use S3 Batch Operations to restore your data from S3 Glacier Deep Archive

1. Choose your AWS Region and input (manifest or CSV) to select objects to be restored

Choose Region and manifest [Info](#)

AWS Region
Choose the AWS Region where you want to create your job. For all operations except Copy, you must create the job in the same Region where the objects referenced in the manifest are located. For Copy operations, you must create the job in the same Region as the destination bucket.

US West (Oregon) us-west-2

Manifest
Manifests must only reference objects in a single S3 bucket. To generate a new manifest, [configure an S3 inventory list for a bucket or prefix](#).

Manifest format

S3 inventory report (manifest.json)

CSV
CSV format must be either 2 or 3 columns in the following order: bucket name, object key, and optionally version ID.

Create manifest using S3 Replication configuration
A list of objects will be generated using the replication configuration and optionally saved to the destination you choose. When using a replication configuration to generate the manifest, the only operation that will be available is replicate. [Learn more](#) or [see pricing](#)

Manifest object

s3://shakihali/au-500-1.csv [View](#) [Browse S3](#)

Format s3://bucket/prefix/object. [Learn more](#)

Manifest object version ID - optional
For objects in a bucket with bucket versioning enabled, you can enter a version ID to use a previous version of the object. If you don't specify a version ID, Batch Operations uses the most recent version of the object. [Learn more](#)

2AKMdMXuk6VMfZEVqObA6ZgG5pcqjKOq

Manifest object ETag
The ETag is used to verify that you have selected the correct manifest object.
b8b055c794badfa517f4857374c45da5

[Cancel](#) [Next](#)

Use S3 Batch Operations to restore your data from S3 Glacier Deep Archive

2. Select **Restore** operation

Choose operation [Info](#)

Operation

Operation type
Choose the operation that you want to perform on all objects listed in the manifest. [Learn more](#)


Manifest must include version ID for Replicate operations.

- Copy**
Copies every object to the specified destination.
- Invoke AWS Lambda function**
AWS Lambda is a compute service that lets you run code without provisioning or managing servers.
- Replace all object tags**
Replaces the Amazon S3 object tags on every object.
- Delete all object tags**
Deletes the Amazon S3 object tags on every object.
- Replace access control list (ACL)**
Replaces the Amazon S3 access control lists (ACLs) for every object.
- Restore**
Initiates restore requests for archived objects.
- Object Lock retention**
Prevents objects from being deleted or overwritten for a fixed amount of time.
- Object Lock legal hold**
Prevents objects from being deleted or overwritten until the legal hold is removed.
- Replicate**
Replicates every object to the destinations specified in the replication configuration.

Use S3 Batch Operations to restore your data from S3 Glacier Deep Archive

3. Select restore configurations

Restore

Retrieval fees apply. See [S3 pricing](#) 

Restore source

Glacier Flexible Retrieval (formerly Glacier) or Glacier Deep Archive

Intelligent-Tiering Archive Access tier or Deep Archive Access tier

Number of days that the restored copy is available

The restored copy is automatically deleted after a specified number of days.

Retrieval tier

Bulk retrieval
Typically within 5-12 hours for Glacier Flexible Retrieval (formerly Glacier) and within 48 hours for Glacier Deep Archive.

Standard retrieval
Typically within 3-5 hours for Glacier Flexible Retrieval (formerly Glacier) and within 12 hours for Glacier Deep Archive.

Use S3 Batch Operations to restore your data from S3 Glacier Deep Archive

4. Select additional configurations and create job

✔ Successfully created Job ID `dc85cc40-9e5d-426c-8d38-dabde90627f2`

The time it takes to prepare a job is based on the size of the job's manifest and the time required to complete higher-priority jobs.

Amazon S3 > Batch Operations

Batch Operations [Info](#)

A job is used to execute batch operations on a list of S3 objects. The list of S3 objects is contained in a manifest object, which can be an S3 inventory report or a list of objects that you generate. After the total number of objects listed in the manifest has been completed, the job either finishes or fails. [Learn more](#)

Jobs (1)

🔍 Search by job ID or description

All status types

US West (Oregon) us-west-2

| Job ID | Status | Description | Operation | Date created | Total objects |
|--|--------|--------------------------|-----------|--|---------------|
| dc85cc40-9e5d-426c-8d38-dabde90627f2 | New | Restore-Glacier-Dec-2022 | Restore | October 10, 2022, 09:08:58 (UTC-07:00) | |


Activate S3 Event Notifications for restores in your bucket properties

Amazon S3 > Buckets > archive-bucket-shakhi

archive-bucket-shakhi [Info](#)

Objects | **Properties** | Permissions | Metrics | Management | Access Points

Bucket overview

| | |
|--|--|
| AWS Region US West (Oregon) us-west-2 | Amazon Resource Name (ARN)  arn:aws:s3:::archive-bucket-shakhi |
|--|--|



Event notifications (0)

Send a notification when specific events occur in your bucket. [Learn more](#)

[Edit](#) [Delete](#) [Create event notification](#)

| Name | Event types | Filters | Destination type | Destination |
|--|-------------|---------|------------------|-------------|
| <p>No event notifications</p> <p>Choose Create event notification to be notified when a specific event occurs.</p> <p>Create event notification</p> | | | | |

Set up S3 Event Notification configuration and destination

Create event notification info

To enable notifications, you must first add a notification configuration that identifies the events you want Amazon S3 to publish and the destinations where you want Amazon S3 to send the notifications.

General configuration

Event name
RestoreGDANotification
Event name can contain up to 255 characters.

Prefix - optional
Limit the notifications to objects with key starting with specified characters.
images/

Suffix - optional
Limit the notifications to objects with key ending with specified characters.
.jpg

Event types
Specify at least one event for which you want to receive notifications. For each group, you can choose an event type for all events, or you can choose one or more individual events.

Object creation

All object create events
s3:ObjectCreated:*

Put
s3:ObjectCreated:Put

Post
s3:ObjectCreated:Post

Copy
s3:ObjectCreated:Copy

Multipart upload completed
s3:ObjectCreated:CompleteMultipartUpload

Object removal

All object removal events
s3:ObjectRemoved:*

Permanently deleted
s3:ObjectRemoved:Delete

Delete markers created
s3:ObjectRemoved:DeleteMarkerCreated

Object restore

All restore object events
s3:ObjectRestore:*

Restore initiated
s3:ObjectRestore:Post

Restore completed
s3:ObjectRestore:Completed

Restored object expired
s3:ObjectRestore:Delete

Destination

Destination
Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. [Learn more](#)

Destination
Choose a destination to publish the event. [Learn more](#)

Lambda function
Run a Lambda function script based on S3 events.

SNS topic
Fanout messages to systems for parallel processing or directly to people.

SQS queue
Send notifications to an SQS queue to be read by a server.

Specify SQS queue

Choose from your SQS queues

Enter SQS queue ARN

SQS queue

Choose SQS queue

Cancel **Save changes**

Monitoring access: Querying request logs

Overview: Insights features in Amazon S3

S3 Storage Lens



Organization-wide visibility into pre-aggregated usage and activity metrics

Free and paid versions available

S3 Inventory



Object-level metadata

S3 storage class analysis



Access patterns by bucket, prefix, tags

S3 CloudWatch Metrics



Monitoring and alarms

S3 server access logs



Detailed request logging

Amazon S3 Storage Lens

Overview | Account | AWS Region | Storage class | Bucket

Snapshot for Sep 28, 2022

A glossary of metrics is available. [Learn more](#)

| | | | | |
|---------------------------------|------------------------------|-----------------------------------|-----------------------------|----------------------|
| 28.0 TB Total storage | 5.1 G Object count | 5.8 KB Avg. object size | 26 Active buckets | 1 Accounts |
|---------------------------------|------------------------------|-----------------------------------|-----------------------------|----------------------|

Metrics

Summary | Cost efficiency | Data protection

% change comparison

Day/day | Week/week | Month/month

| Metric name | Total for Sep 28, 2022 | % change | 30-day trend |
|------------------|------------------------|----------|--------------|
| Total storage | 28.0 TB | 0.00% | |
| Object count | 5.1 G | 0.00% | |
| Avg. object size | 5.8 KB | 0% | |
| Active buckets | 26 | 0% | |
| Accounts | 1 | 0% | |



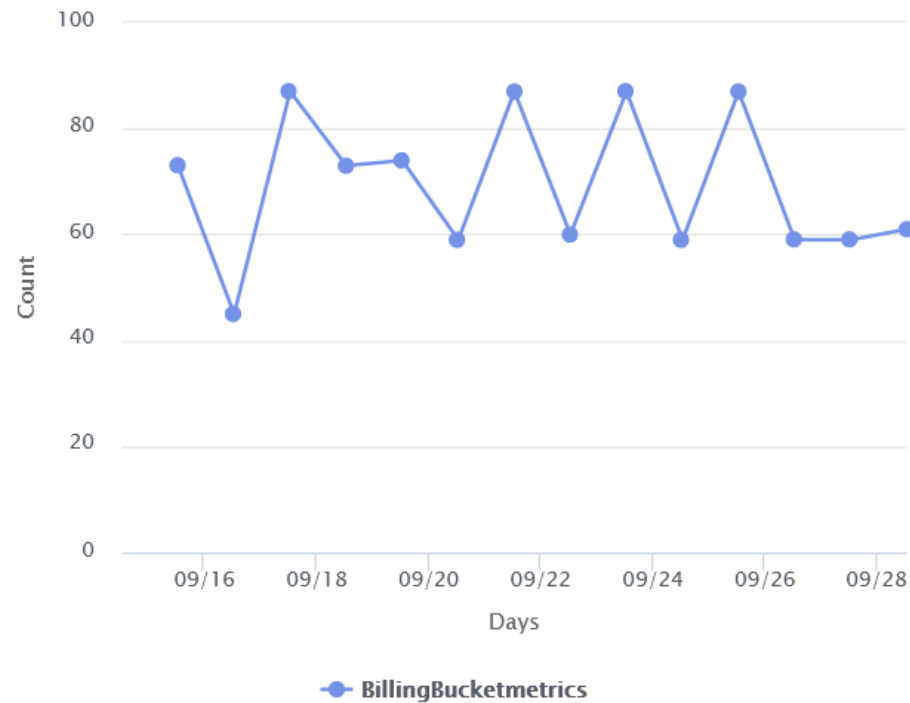
Amazon CloudWatch S3 request metrics

1h 3h 12h 1d 1w 2w 

All requests

All HTTP requests made to this bucket.

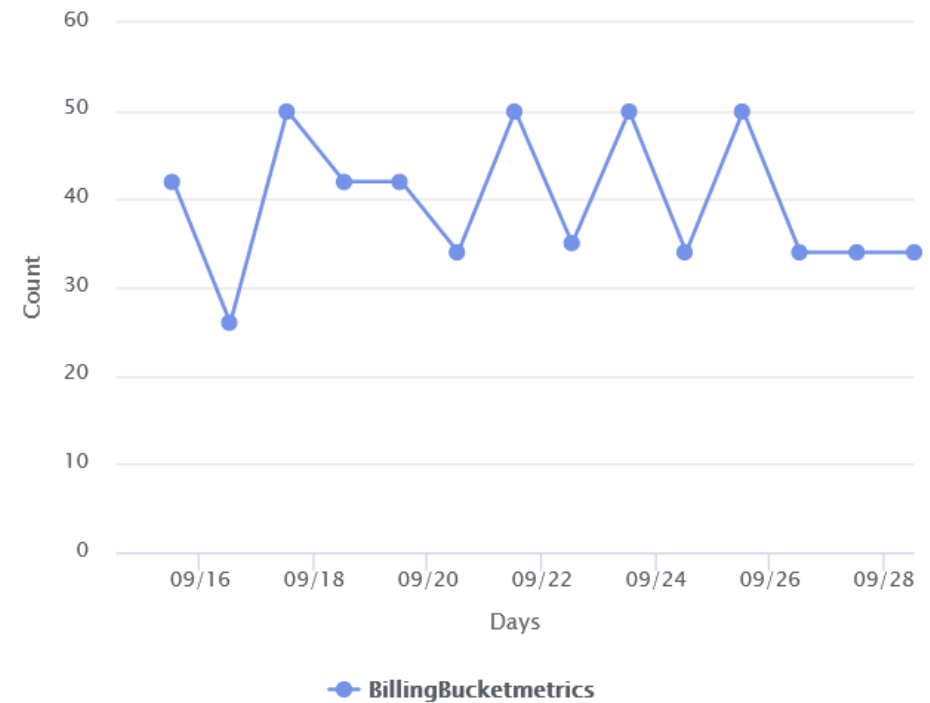
[View in CloudWatch](#) 



Get requests

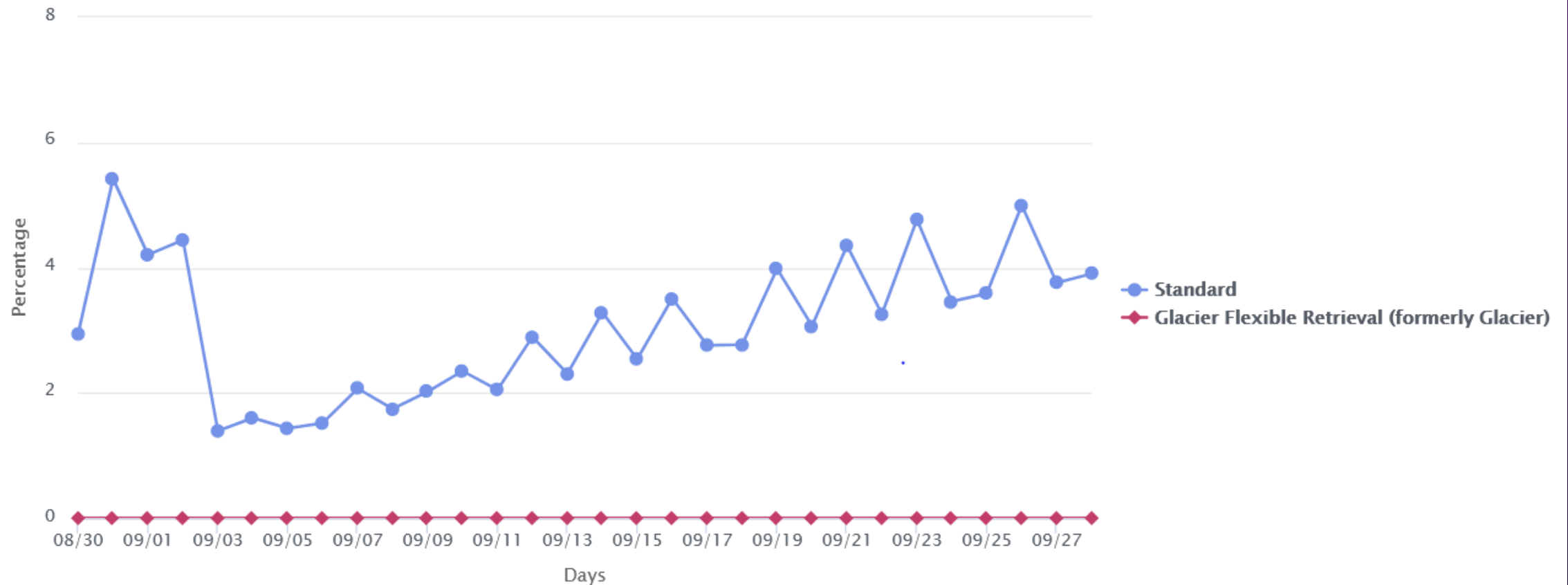
HTTP GET requests for objects in bucket.

[View in CloudWatch](#) 



Amazon S3 storage class analysis

What percent of storage did I retrieve?



Overview: Options for Amazon S3 logging



Overview: Options for Amazon S3 logging

Amazon S3 server access logs

Requests to a bucket

Space-delineated format

Pay for log storage

Logs for S3 Lifecycle actions

Overview: Options for Amazon S3 logging

Amazon S3 server access logs

Requests to a bucket

Space-delineated format

Pay for log storage

Logs for S3 Lifecycle actions

AWS CloudTrail

Management and data events

JSON format

Pay for log storage, events delivered

Forward to CloudWatch
Logs, CloudWatch Events

AWS CloudTrail: Amazon S3 data event

```
"eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:user/myUserName",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "myUserName"
  },
  "eventTime": "2019-02-01T03:18:19Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "ListBuckets",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "127.0.0.1",
  "userAgent": "[]",
  "requestParameters": {
    "host": [
      "s3.us-west-2.amazonaws.com"
    ]
  }
```



Information shown in S3 server access logs



Information shown in S3 server access logs

Bucket owner

HTTP status

Host ID

Bucket

Error code

Signature version

Time

Bytes sent

Cipher suite

Remote IP

Object size

Authentication type

Requester

Total time

Host header

Request ID

Turn-around time

TLS version

Operation

Referrer

Access point ARN

Key

User-agent

Request URI

Version id



Customer use case 3



Phone rings . . .

Colleague calling . . .

Needs help unblocking a demo . . .

Colleague needs detailed error information on requests made to Amazon S3

AWS CloudTrail: S3 data events
Amazon Athena

Common log analyses

1. Finding a specific request ID or error message

Common log analyses

1. Finding a specific request ID or error message
2. Analyzing S3 request latency as you make changes to an application

Common log analyses

1. Finding a specific request ID or error message
2. Analyzing S3 request latency as you make changes to an application
3. Understanding who is accessing data in a bucket

Common log analyses

1. Finding a specific request ID or error message
2. Analyzing S3 request latency as you make changes to an application
3. Understanding who is accessing data in a bucket
4. Investigating access patterns in the bucket

Log-query approach using AWS CloudTrail

Key steps

1. Create a trail in AWS CloudTrail
 - a) Specify S3 location for your logs
2. Enable AWS CloudTrail: S3 data events
 - a) Select all buckets or filter your data events
3. Set up an Amazon Athena table
4. Run queries

Create a trail

Trail name

Enter a display name for your trail.

management-events

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. [See all accounts](#) 

Storage location [Info](#)

Create new S3 bucket
Create a bucket to store logs for the trail.

Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

aws-cloudtrail-logs-903062817049-84f30c3e

Logs will be stored in aws-cloudtrail-logs-903062817049-84f30c3e/AWSLogs/903062817049

Log file SSE-KMS encryption [Info](#)

Enabled

▼ Additional settings

Log file validation [Info](#)

Enabled

SNS notification delivery [Info](#)

Enabled



Specify AWS CloudTrail data events

Data events [Info](#)
[Additional charges apply](#) Data events show information about the resource operations performed on or within a resource.

Basic event selectors are enabled
Switch to advanced data event selectors for fine-grained control over the data events captured by your trail.

[Switch to advanced event selectors](#)

Data event: S3 [Info](#) [Remove](#)

Data event source
Select source of data events to log

S3 ▼

S3 bucket
You can choose to log read and/or write events for all buckets. You can also choose individual buckets.


All current and future S3 buckets Read Write

Individual bucket selection
Choose Browse to select multiple buckets, then choose to log Read, Write or both event types on all selected buckets.

[Browse](#) Read Write [X](#)

Create a table in Amazon Athena

Create a table in Amazon Athena ✕

You can use Amazon Athena to analyze events that are stored in a trail's Amazon S3 bucket. Athena is an interactive query service that helps you analyze data in S3 buckets by using standard SQL. Athena charges for running queries. [Learn more](#) 


Storage location

Choose an S3 bucket that contains CloudTrail log files

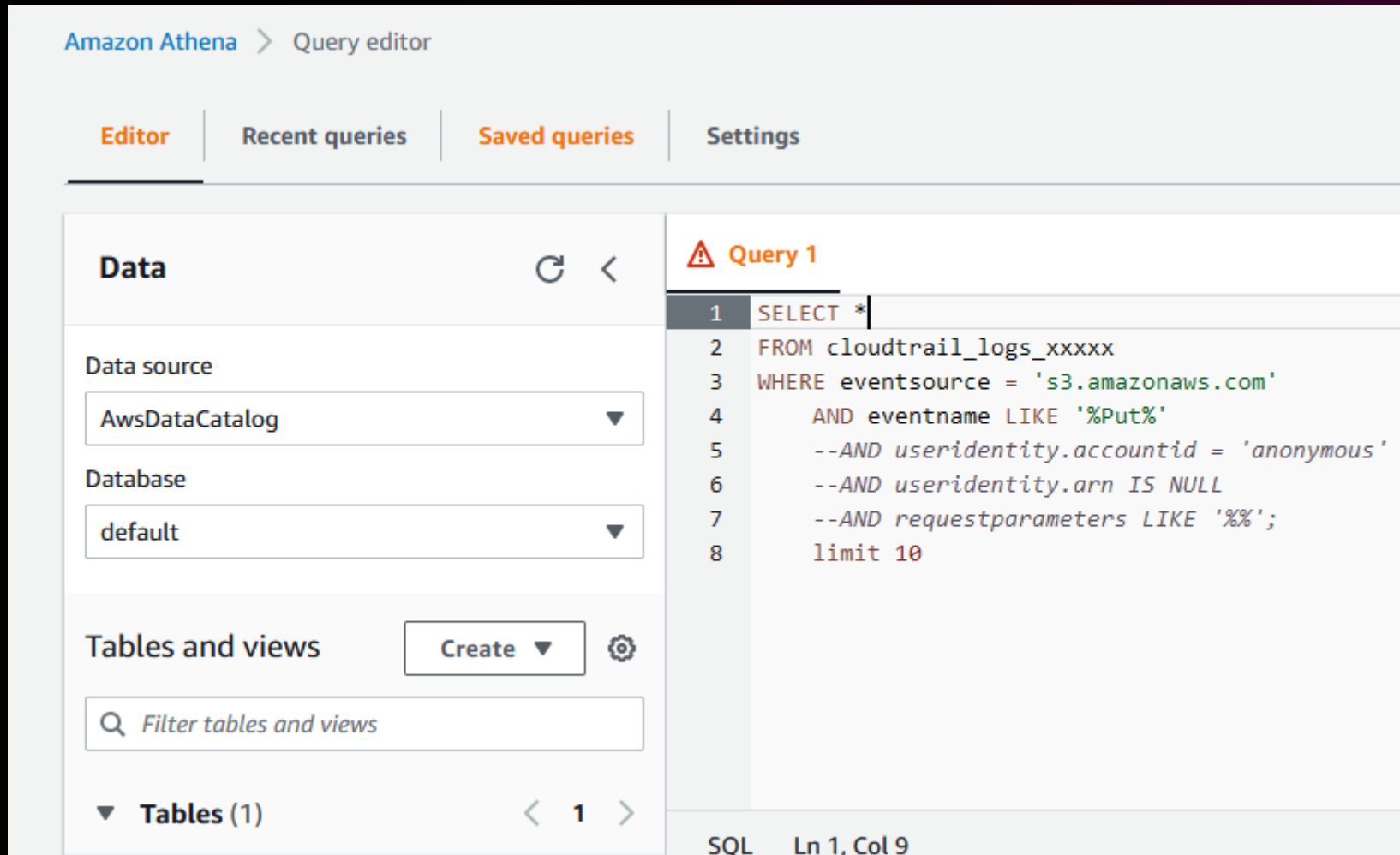
Athena table name

This name is auto-generated. You can rename it in Amazon Athena.

```
1 CREATE EXTERNAL TABLE [TABLE_NAME] (  
2     eventVersion STRING,  
3     userIdentity STRUCT<  
4         type: STRING,  
5         principalId: STRING,  
6         arn: STRING,  
7         accountId: STRING,  
8         invokedBy: STRING,  
9         accessKeyId: STRING,  
10        userName: STRING,  
11        sessionContext: STRUCT<  
12            attributes: STRUCT<  
13                mfaAuthenticated: STRING,
```

 Copy

Run query



The screenshot displays the Amazon Athena Query Editor interface. At the top, the breadcrumb navigation shows "Amazon Athena > Query editor". Below this, there are four tabs: "Editor" (which is active), "Recent queries", "Saved queries", and "Settings".

The main interface is divided into two main sections. On the left, there is a "Data" panel with a refresh icon and a back arrow. It contains two dropdown menus: "Data source" set to "AwsDataCatalog" and "Database" set to "default". Below these is a "Tables and views" section with a "Create" button and a search box labeled "Filter tables and views". At the bottom of this panel, it shows "Tables (1)" with navigation arrows and the number "1".

On the right, the "Query 1" editor shows a SQL query being typed on line 1: "SELECT *". The rest of the query is as follows:

```
1 SELECT *
2 FROM cloudtrail_logs_xxxxx
3 WHERE eventsource = 's3.amazonaws.com'
4     AND eventname LIKE '%Put%'
5     --AND useridentity.accountid = 'anonymous'
6     --AND useridentity.arn IS NULL
7     --AND requestparameters LIKE '%%';
8     limit 10
```

At the bottom right of the editor, the status bar indicates "SQL Ln 1, Col 9".

Query example

```
SELECT
    awsregion,
    replace(unnested.resources_entry.ARN, 'arn:aws:s3:::') as s3_resource,
    eventname,
    eventtime,
    useragent
FROM cloudtrail_logs t
CROSS JOIN UNNEST(t.resources) unnested (resources_entry)
WHERE unnested.resources_entry.ARN LIKE '%example/datafile.txt'
ORDER BY eventtime
```



Query example

```
SELECT
    useridentity.arn,
    Count(requestid) as RequestCount
FROM s3_cloudtrail_events_db.cloudtrail_awsexamplebucket_table
WHERE eventsource='s3.amazonaws.com'
and json_extract_scalar(additionalEventData, '$.SignatureVersion')='sigv2'
Group by useridentity.arn
```

Query results

| eventversion | eventtime | eventsources | eventname | awsregion | sourceipaddress |
|--------------|----------------------|------------------|-------------------|----------------|-----------------|
| 1.05 | 2017-10-01T20:34:50Z | s3.amazonaws.com | GetBucketLocation | ap-northeast-1 | 52.xxx.xxx.xxx |
| 1.05 | 2017-10-01T20:34:53Z | s3.amazonaws.com | GetBucketLocation | ap-northeast-1 | 52.xxx.xxx.xxx |
| 1.05 | 2017-10-01T20:34:52Z | s3.amazonaws.com | GetBucketLocation | ap-northeast-1 | 52.xxx.xxx.xxx |
| 1.05 | 2017-10-01T20:34:53Z | s3.amazonaws.com | GetBucketLocation | ap-northeast-1 | 52.xxx.xxx.xxx |
| 1.05 | 2017-10-01T20:34:52Z | s3.amazonaws.com | GetBucketLocation | ap-northeast-1 | 52.xxx.xxx.xxx |
| 1.05 | 2017-10-01T20:34:51Z | s3.amazonaws.com | GetBucketLocation | ap-northeast-1 | 52.xxx.xxx.xxx |
| 1.05 | 2017-10-01T20:34:51Z | s3.amazonaws.com | GetBucketLocation | ap-northeast-1 | 52.xxx.xxx.xxx |
| 1.05 | 2017-10-01T20:34:51Z | s3.amazonaws.com | GetBucketLocation | ap-northeast-1 | 52.xxx.xxx.xxx |
| 1.05 | 2017-10-01T20:34:52Z | s3.amazonaws.com | GetBucketLocation | ap-northeast-1 | 52.xxx.xxx.xxx |
| 1.04 | 2017-08-13T22:15:22Z | s3.amazonaws.com | GetBucketLocation | ap-northeast-1 | 52.xxx.xxx.xxx |



Visualizing log data: CloudWatch Insights

The screenshot displays the AWS CloudWatch Logs Insights interface. The top navigation bar includes the AWS logo, a search bar with the text "Search for services, features, blogs, docs, and more", and the user's name "Admin/rwx-lsengar" in "N. Virginia" region. The left sidebar shows the "CloudWatch" navigation menu with categories like "Alarms", "Logs", "Metrics", "X-Ray traces", "Events", and "Application monitoring". The "Logs Insights" section is active, showing a query editor with the following query:

```
1 fields @timestamp, @message
2 | .sort @timestamp .desc
3 | .limit 20
```

Below the query editor are buttons for "Run query", "Cancel", "Save", and "History". A note states: "Queries are allowed to run for up to 15 minutes." The "Visualization" tab is selected, displaying a histogram of log records over time. The histogram shows a peak in activity around 07 PM and 01 AM. Text above the histogram reads: "Showing 20 of 47,624 records matched" and "47,641 records (63.3 MB) scanned in 4.3s @ 11,159 records/s (14.8 MB/s)". A "Hide histogram" link is visible in the top right of the visualization area. Below the histogram is a table of log records:

| # | @timestamp | @message |
|-----|----------------------------|--|
| ▶ 1 | 2022-10-13T05:47:54.662... | {"eventVersion": "1.08", "userIdentity": {"type": "AWSService", "invokedBy": "s3.amazonaws.com"}, "eventTime": "2022-10-13T12:45:08Z", "ever |

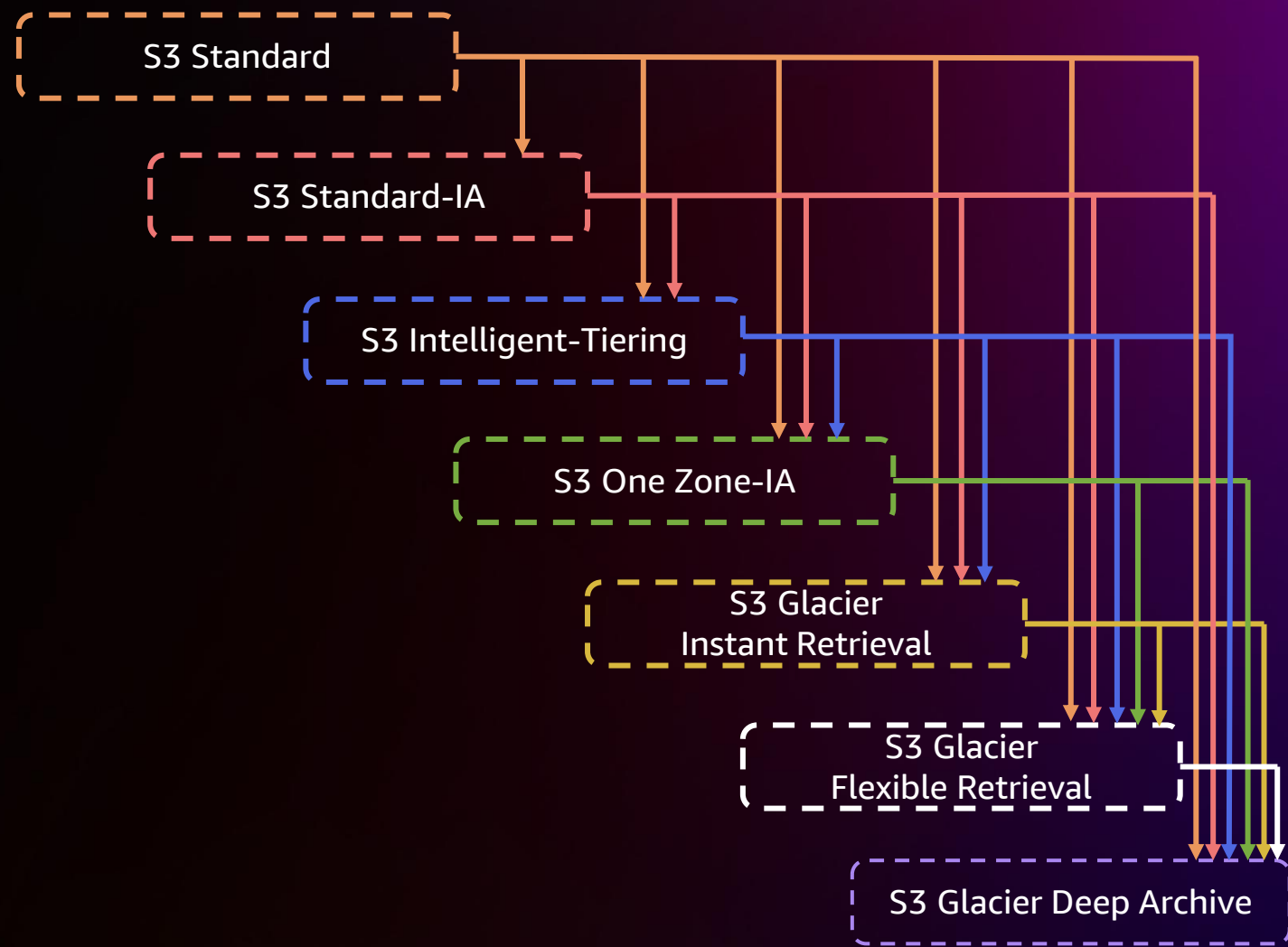
Managing storage spend



Amazon S3 Lifecycle helps optimize storage spend

Transition actions: Define when objects transition to other Amazon S3 storage classes as they age

Expiration actions: Define when objects expire; Amazon S3 deletes expired objects on your behalf



Applying insights to create S3 Lifecycle configurations

S3 Lifecycle rules take action based on object age; here's an example

1. Move objects older than 30 days to S3 Standard-IA
2. Move objects older than 365 days to S3 Glacier Deep Archive



Anatomy of an S3 Lifecycle configuration

Lifecycle configuration elements

ID

Filters

Status

Actions

```
<LifecycleConfiguration>
  <Rule>
    <ID>ExampleRule</ID>
    <Filter>
      <Prefix>tax/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
      <Days>3650</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

Use object versioning to protect your objects

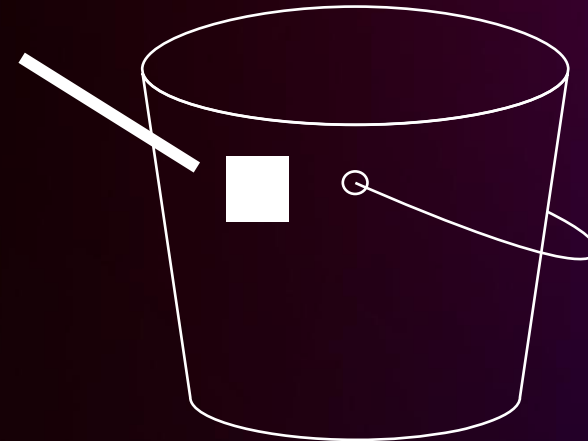
Versioning prevents overwrites by creating new versions of the object

Use object versioning to protect your objects

Versioning prevents overwrites by creating new versions of the object

exampleAWSbucket/drafts/novel

Version A

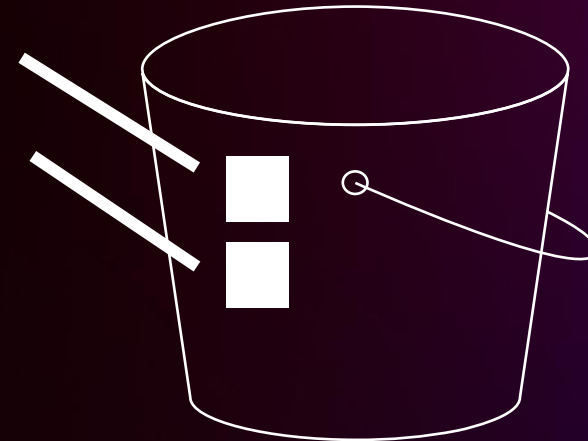


Use object versioning to protect your objects

Versioning prevents overwrites by creating new versions of the object

exampleAWSbucket/drafts/novel
exampleAWSbucket/drafts/novel

Version A
Version B

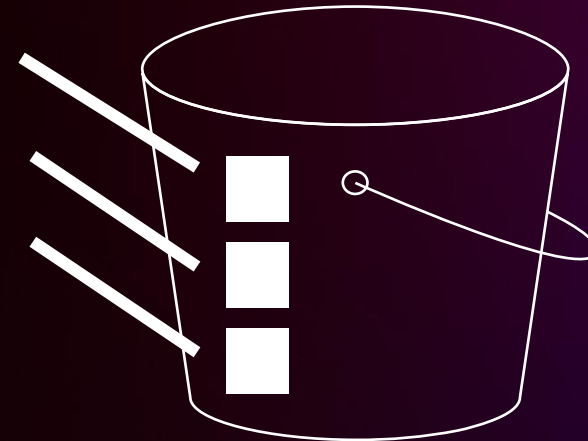


Use object versioning to protect your objects

Versioning prevents overwrites by creating new versions of the object

exampleAWSbucket/drafts/novel
exampleAWSbucket/drafts/novel
exampleAWSbucket/drafts/novel

Version A
Version B
Version C



Versioning also provides deletion protection

Versioning can also provide deletion protection

- Deletions without a version ID create a delete marker
- The prior version of the object is retained
- GET requests return a 404, NOT FOUND error



When the version ID is specified in a deletion, that version is deleted

Best practice: Consider an S3 Lifecycle configuration for all versioned buckets

Set retention policy with Amazon S3 Lifecycle

Current version S3 Lifecycle rule

Noncurrent version S3 Lifecycle rule

Expired object delete marker rule

Incomplete multipart upload retention



Customer use case 4



Email from analyst on the finance team . . .

Meeting underway, many questions about month-over-month changes . . .

Why did storage spend on AWS rise 15% last month in our testing account?

Amazon S3 Storage Lens
Amazon S3 Lifecycle

Let's start with S3 Storage Lens

| Top 3 regions | | | |
|---------------------------------------|---------------|------------|----------|
| AWS Region | Total storage | % of total | % change |
| US East (N. Virginia) | 15.4 TB | 54.89% | 0.00% |
| US West (Oregon) | 12.1 TB | 43.26% | -0.00% |
| US East (Ohio) | 528.5 GB | 1.85% | 0.00% |

| Top 3 buckets | | | |
|--------------------|---------------|------------|----------|
| Bucket | Total storage | % of total | % change |
| rw | 8.9 TB | 31.92% | 14.95% |
| rw | 7.1 TB | 25.53% | 0% |
| rw | 5.7 TB | 20.24% | 0.00% |

Let's start with S3 Storage Lens

| Top 3 regions | | | |
|---------------------------------------|---------------|------------|----------|
| AWS Region | Total storage | % of total | % change |
| US East (N. Virginia) | 15.4 TB | 54.89% | 0.00% |
| US West (Oregon) | 12.1 TB | 43.26% | -0.00% |
| US East (Ohio) | 528.5 GB | 1.85% | 0.00% |

| Top 3 buckets | | | |
|--------------------|---------------|------------|----------|
| Bucket | Total storage | % of total | % change |
| rw | 8.9 TB | 31.92% | 14.95% |
| rw | 7.1 TB | 25.53% | 0% |
| rw | 5.7 TB | 20.24% | 0.00% |

Let's start with S3 Storage Lens

Overview | Account | AWS Region | Storage class | Bucket

Snapshot for Sep 28, 2022

A glossary of metrics is available. [Learn more](#)

| | | |
|--------------------------|-----------------------|----------------------------|
| 28.0 TB Total storage | 5.1 G Object count | 5.8 KB Avg. object size |
|--------------------------|-----------------------|----------------------------|

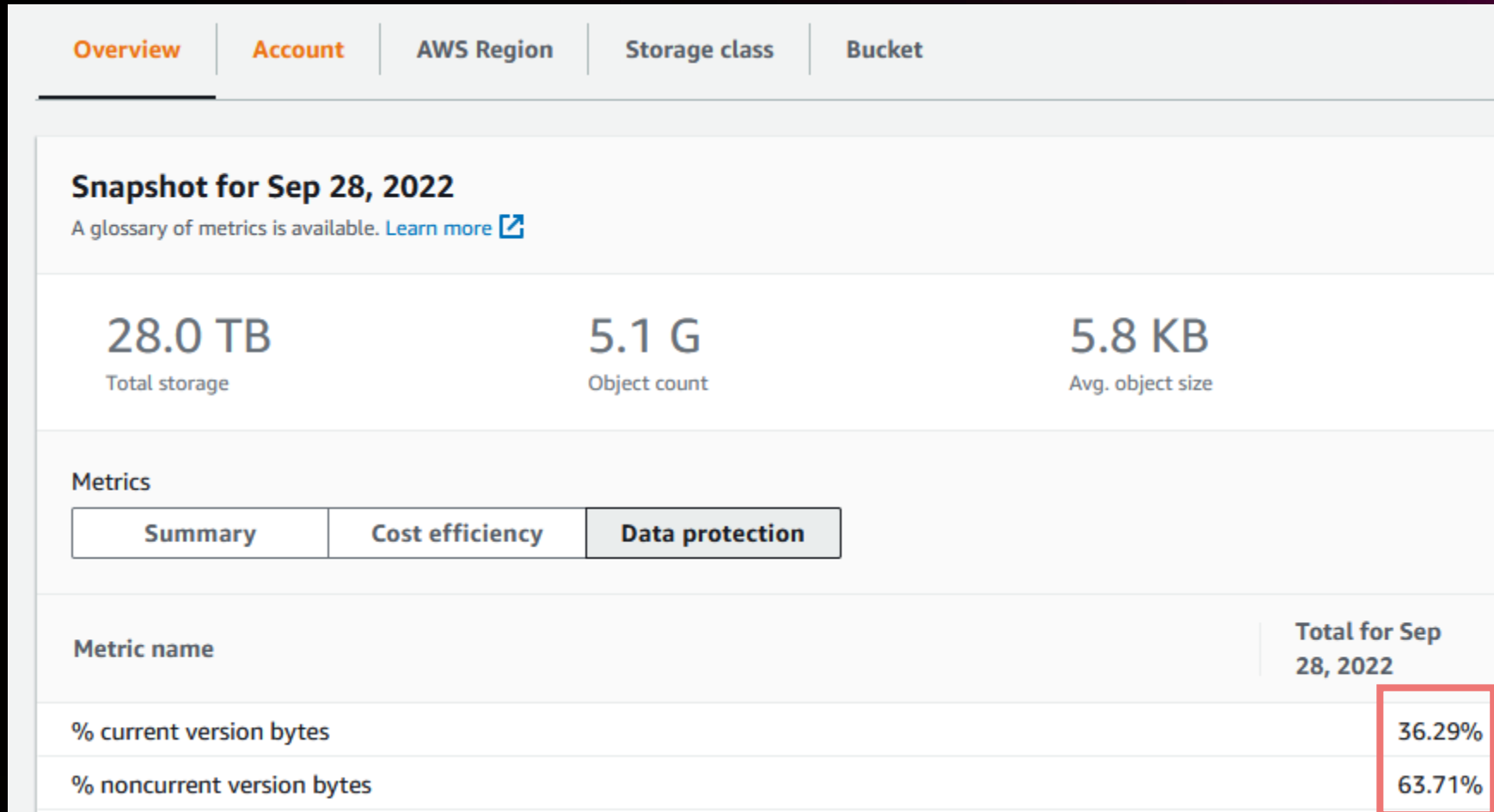
Metrics

| | | |
|---------|-----------------|-----------------|
| Summary | Cost efficiency | Data protection |
|---------|-----------------|-----------------|

| Metric name | Total for Sep 28, 2022 |
|----------------------------|------------------------|
| % current version bytes | 36.29% |
| % noncurrent version bytes | 63.71% |



Let's start with S3 Storage Lens



Decide your retention needs

Does this workload/application require

- Retention for a specific period of time?
- Retention of overwritten data?
- Different rules based on object size?

Example configurations: Unversioned buckets

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition and Expiration Rule</ID>
    <Filter>
      <Prefix>tax/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>S3 Glacier Flexible Retrieval</StorageClass>
    </Transition>
    <Expiration>
      <Days>3650</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```



Example configurations: Unversioned buckets

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition and Expiration Rule</ID>
    <Filter>
      <Prefix>tax/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>S3 Glacier Flexible Retrieval</StorageClass>
    </Transition>
    <Expiration>
      <Days>3650</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```



Example configurations: Unversioned buckets

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition and Expiration Rule</ID>
    <Filter>
      <Prefix>tax/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>S3 Glacier Flexible Retrieval</StorageClass>
    </Transition>
    <Expiration>
      <Days>3650</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```



Example configurations: Versioned buckets

```
<LifecycleConfiguration>
  <Rule>
    <ID>VersionRetention</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>30</Days>
      <StorageClass>STANDARD_IA</StorageClass>
    </Transition>
    <NoncurrentVersionTransition>
      <NoncurrentDays>7</NoncurrentDays>
      <StorageClass>S3 Glacier Flexible Retrieval</StorageClass>
    </NoncurrentVersionTransition>
    <NoncurrentVersionExpiration>
      <NewerNoncurrentVersions>5</NewerNoncurrentVersions>
      <NoncurrentDays>365</NoncurrentDays>
    </NoncurrentVersionExpiration>
  </Rule>
</LifecycleConfiguration>
```



Example configurations: Versioned buckets

```
<LifecycleConfiguration>
  <Rule>
    <ID>VersionRetention</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>30</Days>
      <StorageClass>STANDARD_IA</StorageClass>
    </Transition>
    <NoncurrentVersionTransition>
      <NoncurrentDays>7</NoncurrentDays>
      <StorageClass>S3 Glacier Flexible Retrieval</StorageClass>
    </NoncurrentVersionTransition>
    <NoncurrentVersionExpiration>
      <NewerNoncurrentVersions>5</NewerNoncurrentVersions>
      <NoncurrentDays>365</NoncurrentDays>
    </NoncurrentVersionExpiration>
  </Rule>
</LifecycleConfiguration>
```

Example configurations: Versioned buckets

```
<LifecycleConfiguration>
  <Rule>
    <ID>VersionRetention</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>30</Days>
      <StorageClass>STANDARD_IA</StorageClass>
    </Transition>
    <NoncurrentVersionTransition>
      <NoncurrentDays>7</NoncurrentDays>
      <StorageClass>S3 Glacier Flexible Retrieval</StorageClass>
    </NoncurrentVersionTransition>
    <NoncurrentVersionExpiration>
      <NewerNoncurrentVersions>5</NewerNoncurrentVersions>
      <NoncurrentDays>365</NoncurrentDays>
    </NoncurrentVersionExpiration>
  </Rule>
</LifecycleConfiguration>
```



Example configurations: Versioned buckets

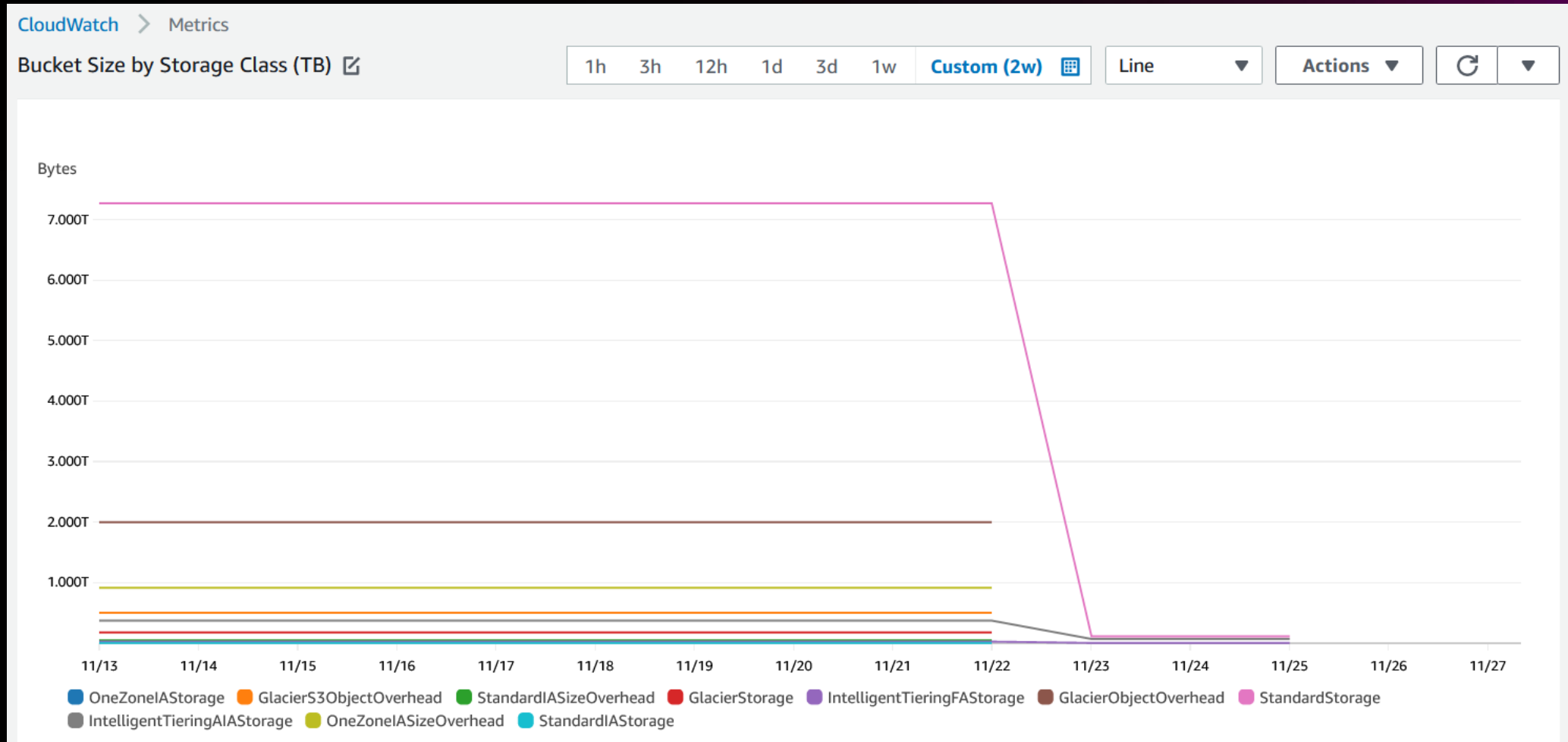
```
<LifecycleConfiguration>
  <Rule>
    <ID>VersionRetention</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>30</Days>
      <StorageClass>STANDARD_IA</StorageClass>
    </Transition>
    <NoncurrentVersionTransition>
      <NoncurrentDays>7</NoncurrentDays>
      <StorageClass>S3 Glacier Flexible Retrieval</StorageClass>
    </NoncurrentVersionTransition>
    <NoncurrentVersionExpiration>
      <NewerNoncurrentVersions>5</NewerNoncurrentVersions>
      <NoncurrentDays>365</NoncurrentDays>
    </NoncurrentVersionExpiration>
  </Rule>
</LifecycleConfiguration>
```



Example configurations: Object size

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition with a prefix and based on size</ID>
    <Filter>
      <And>
        <Prefix>tax/</Prefix>
        <ObjectSizeGreaterThan>131072</ObjectSizeGreaterThan>
      </And>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>S3 Glacier Flexible Retrieval</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Monitor your storage: See the impact

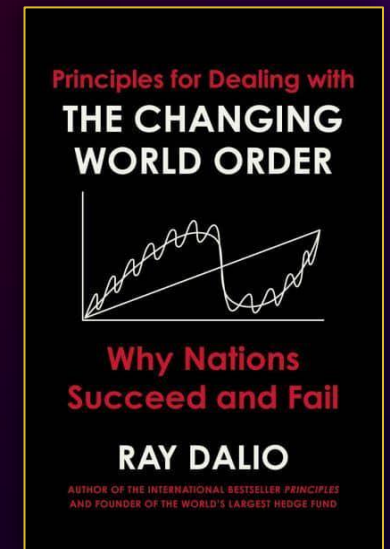
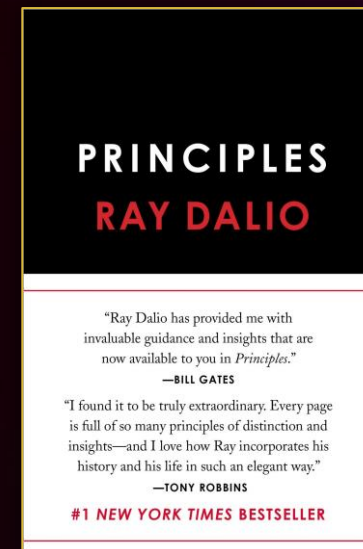


Customer voice: Bridgewater Associates



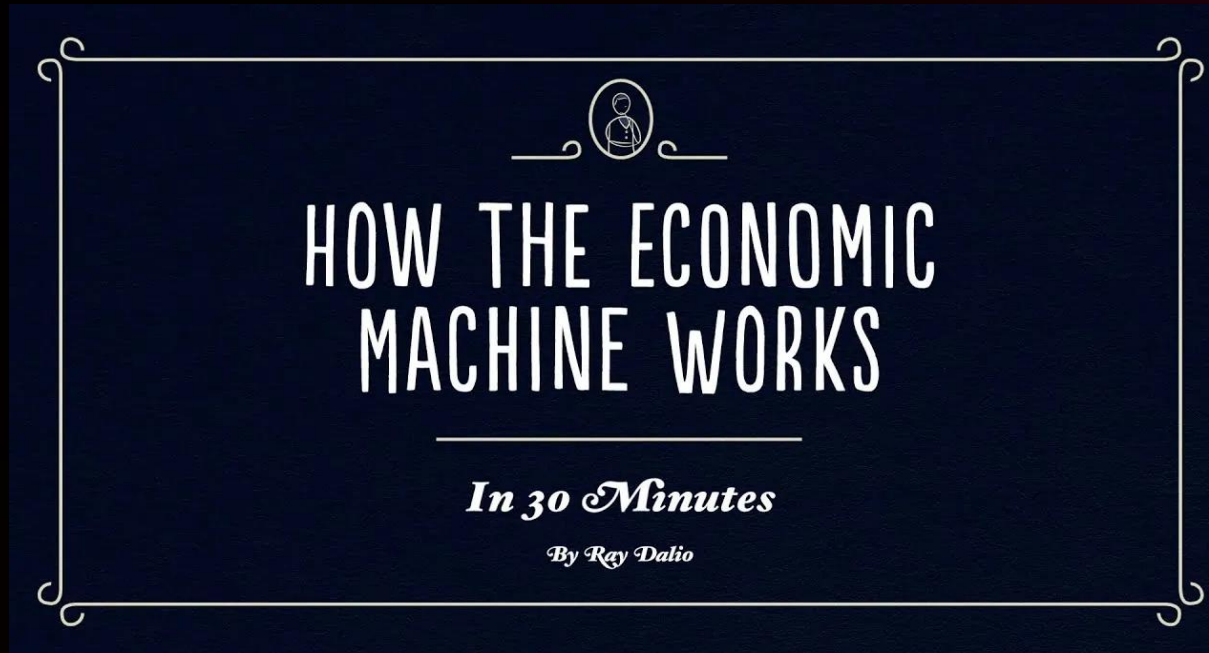
About Bridgewater

- Founded by **Ray Dalio**
- **Global macroeconomic investment manager**
- We endlessly pursue the right answer to how economies work
- Our economic model is complex, constantly evolving for over 45 years



Bridgewater's model of the economy

- Research **timeless and universal** economic and investment principles
- We take these principles and write them as **code**
- We run this code, our **economic model**, continuously

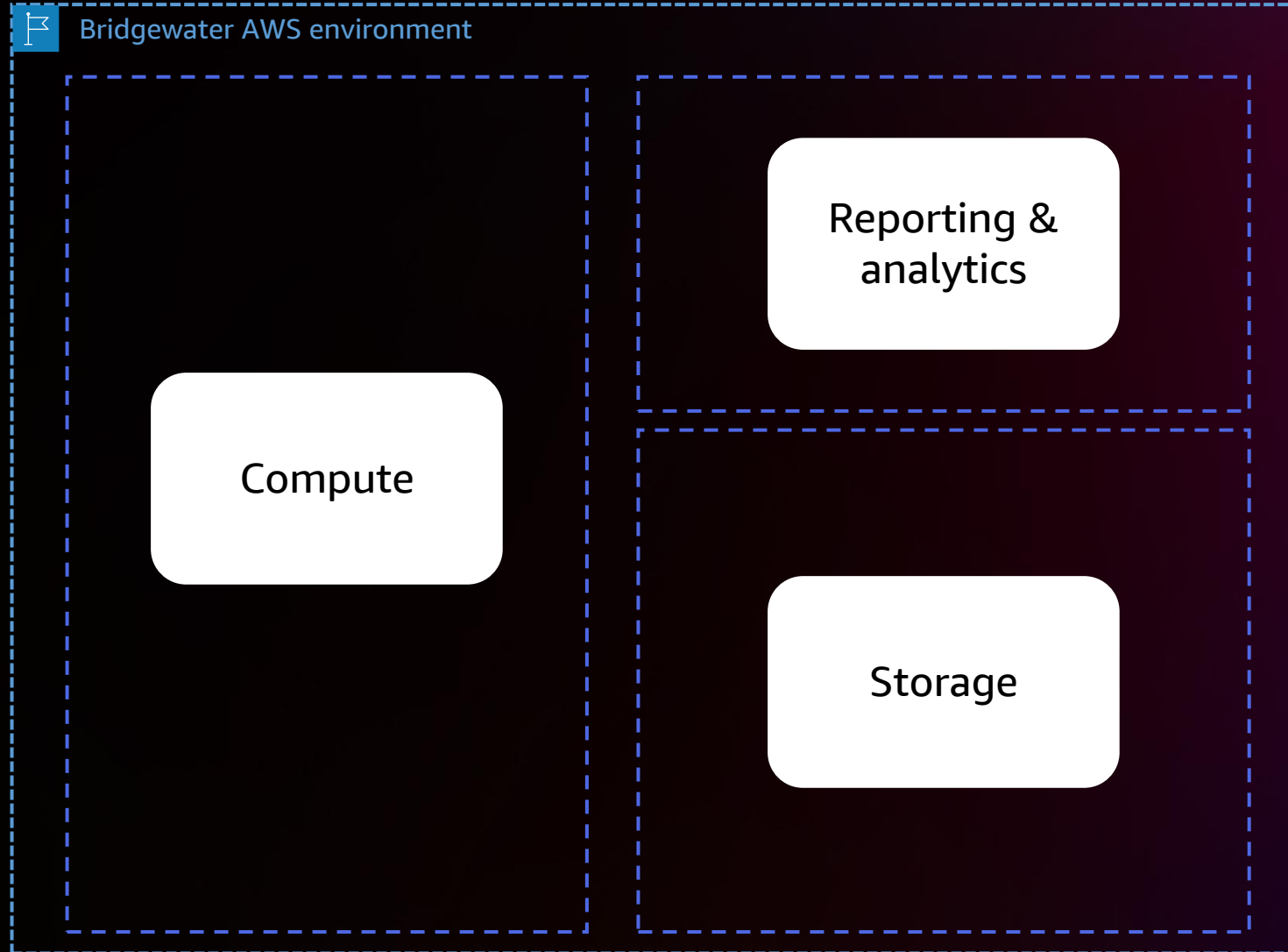


Bridgewater's economic model runs on AWS

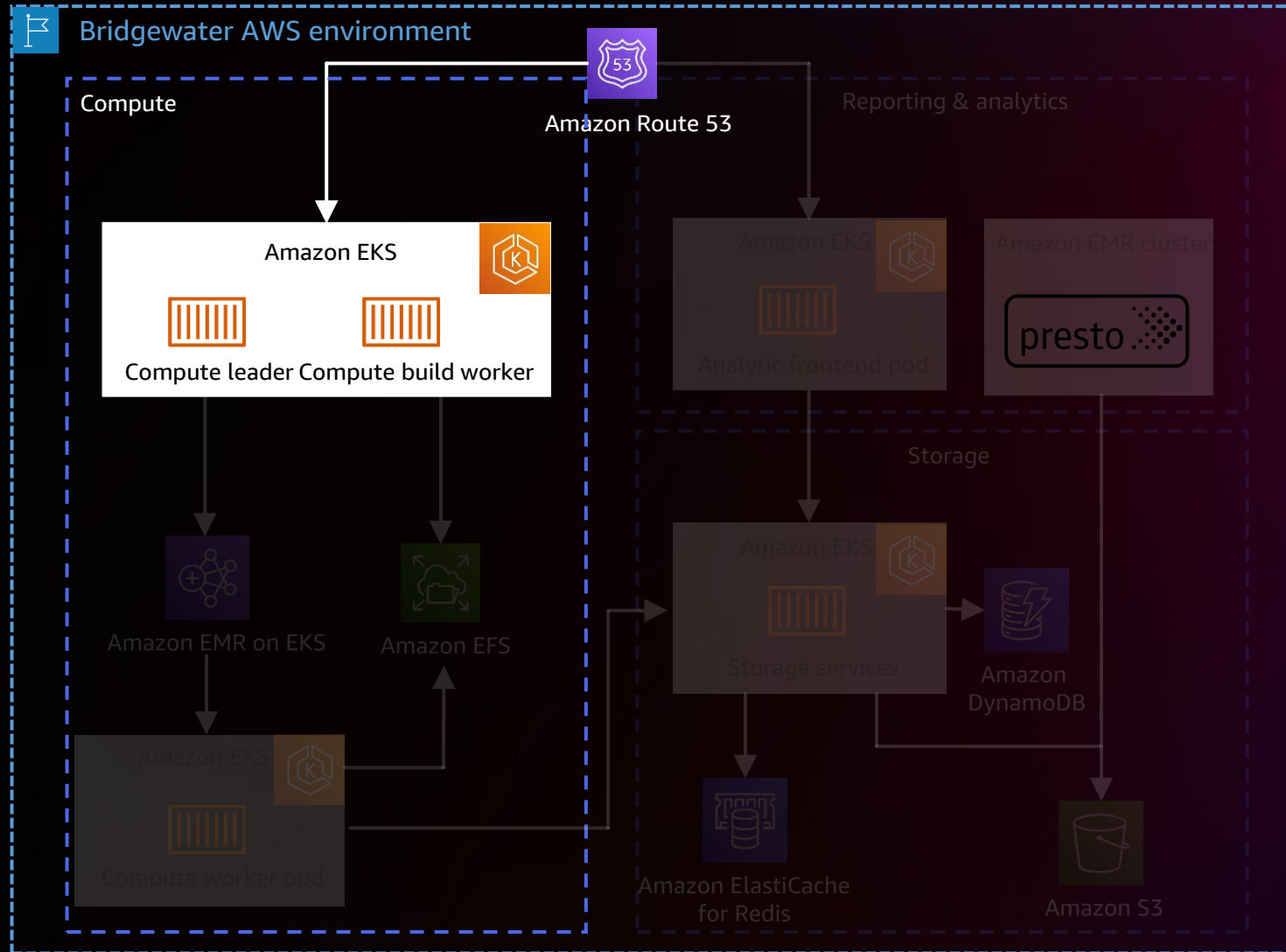
- New data flows in
- Forward-testing every day
- Back-testing all model changes
- Research workflows with hypothetical model changes (what-if scenarios)
- Consistently producing trades in all the markets we operate
- **AWS based architecture allows us to scale out with reliability**

Compute architecture

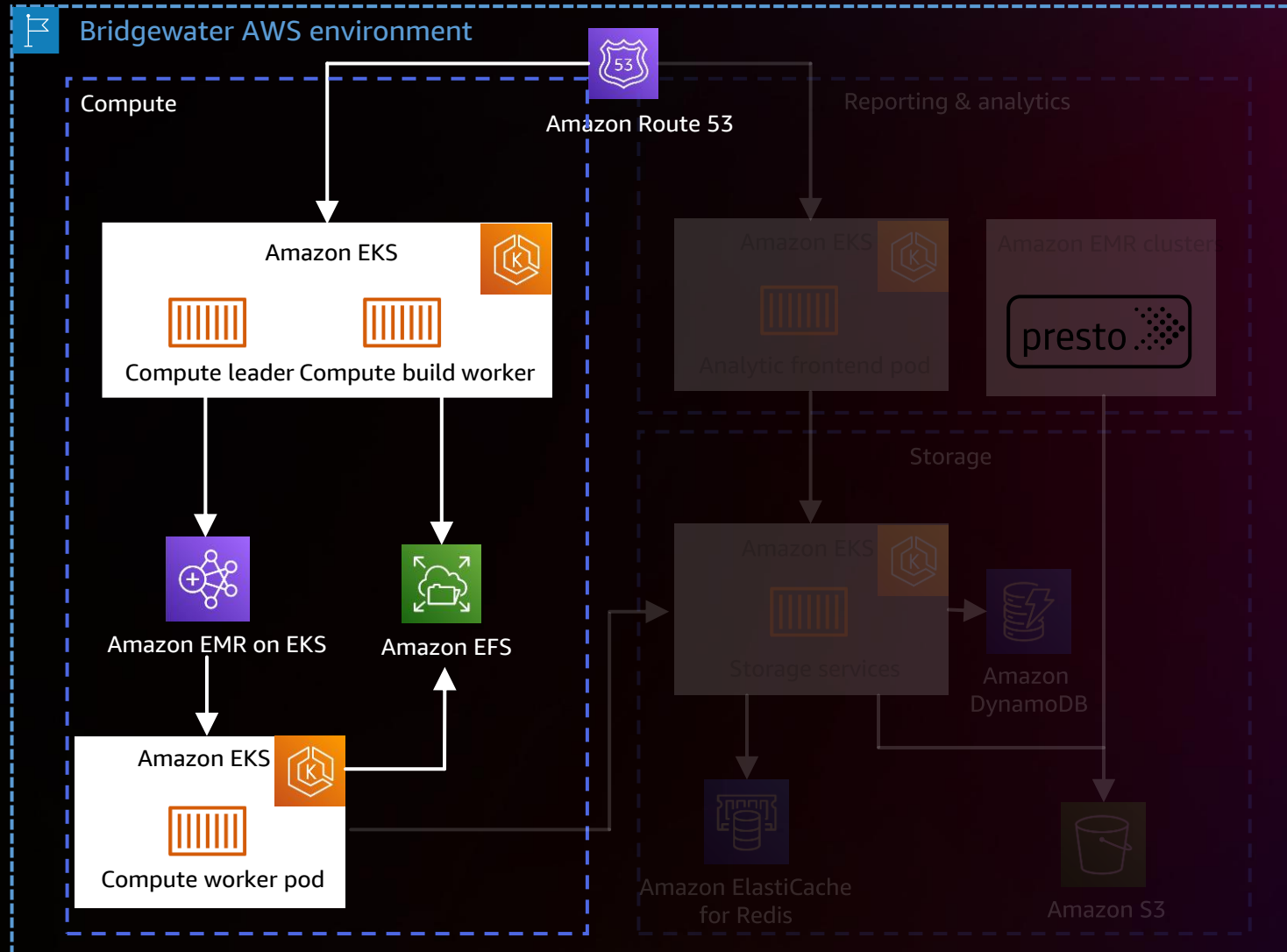
User



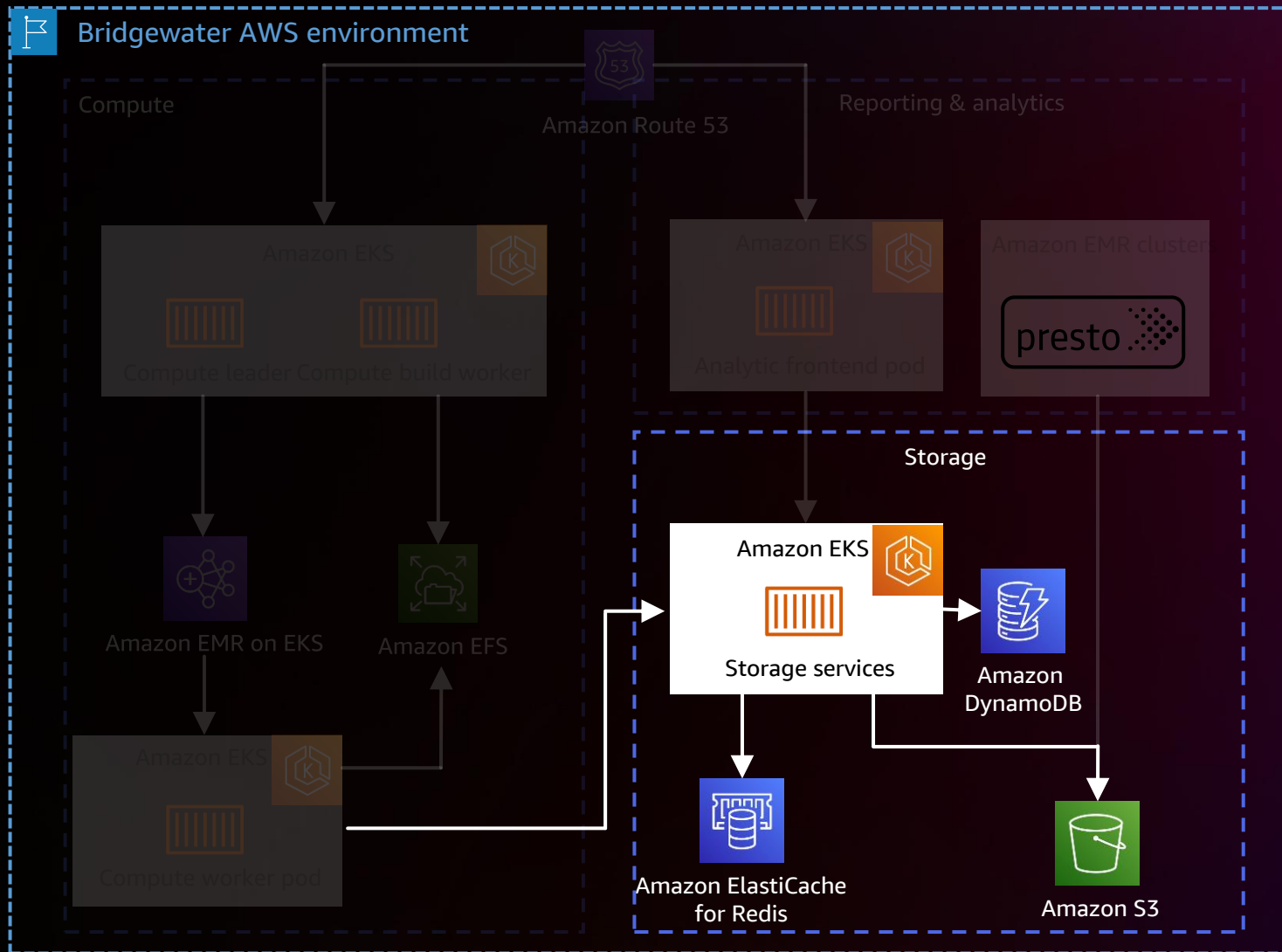
Compute architecture



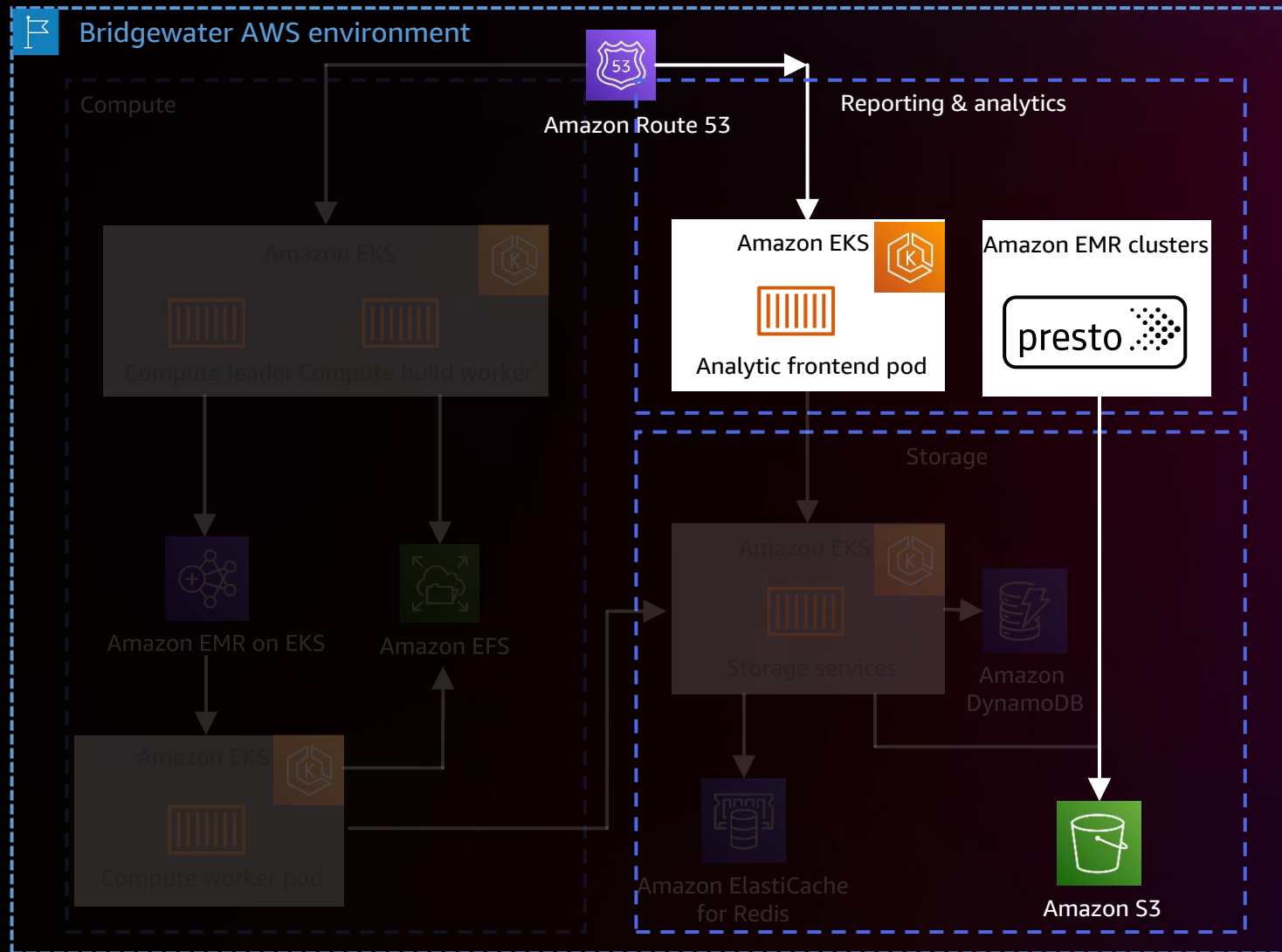
Compute architecture



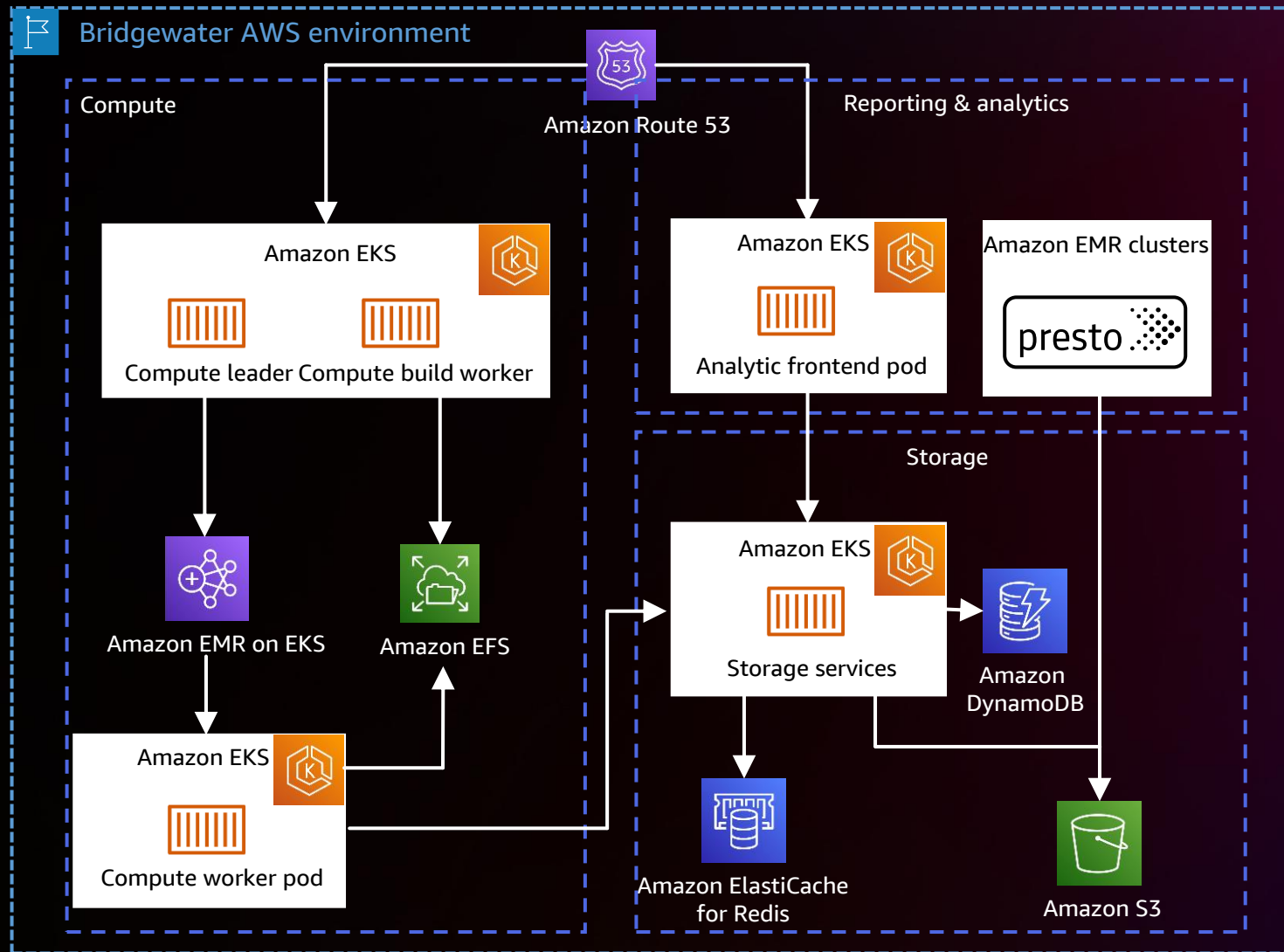
Compute architecture



Compute architecture



Compute architecture



Data storage needs at Bridgewater

Security

Reliability

Cost

**Our users
need scale**

Our storage stack

Proprietary
database built on
top of **Amazon S3**
as the **data store**

**Amazon
DynamoDB**
as the
metadata store

**Amazon
ElastiCache**
to accelerate read-
heavy workloads

Security and compliance at scale

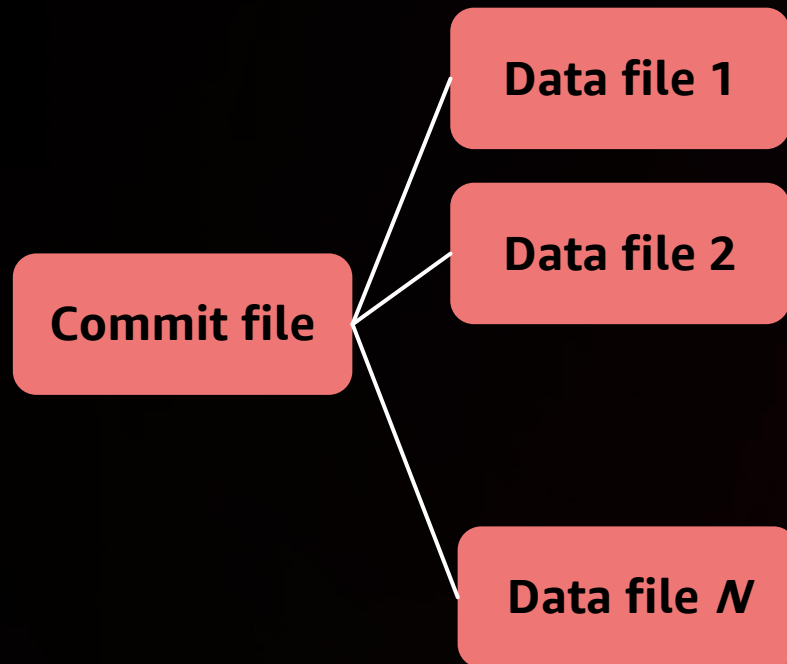
- Customer managed AWS KMS encryption
- Amazon S3 default encryption
- S3 Object Lock to ensure data is never deleted
- Controls to ensure **security and compliance** as we scale tens of petabytes

Reliability and consistency at scale

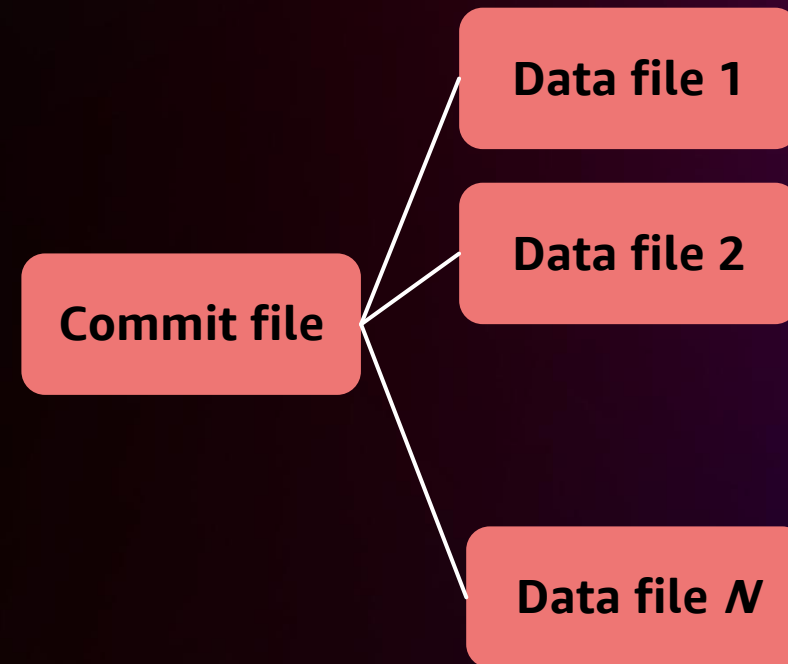
- S3 Replication Time Control with S3 Cross-Region Replication
- Consistent reads in S3 (beyond read-after-write)
- S3 Storage Lens for better analytics
- S3 Multi-Region Access Points
- Designed for **full Region outage scenarios**

Our replication happens at the dataset level

Region 1



Region 2



S3 Replication Time Control monitoring

Track the latest timestamp to know when **100%** is replicated

SLA is 15 mins
We usually see the data replicated in 1–3 minutes

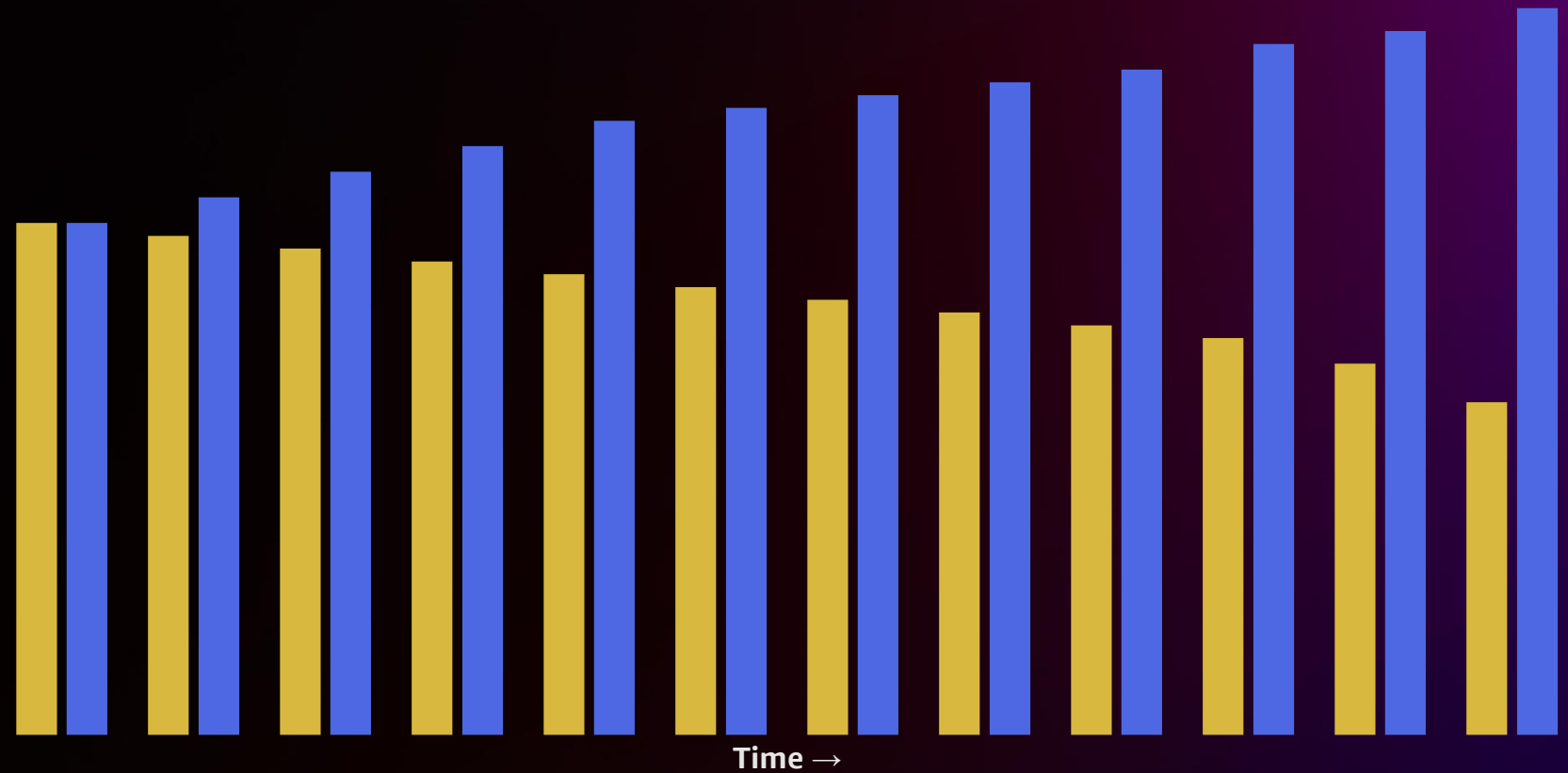
Worst case, we only have a **few minutes** of data loss

Managing cost at scale

■ Cost ■ Usage

S3 Intelligent Tiering:

Monthly storage is **up 42%**, while spend is **down 35%**



Bridgewater tests the scale of Amazon S3

20+
petabytes

120 B+
objects

2 PB/year
growth

AWS services improve our business

2x

reduction in
average runtime

75%+

machine
utilization

5x

scale of
simulations

Session recap

Securing your data – encrypting objects at scale

Use: S3 Inventory, S3 Batch Operations

Accessing archive data – restoring data

Use: S3 Glacier storage classes, S3 Batch Operations, S3 Event Notifications

Monitoring access – querying request logs

Use: AWS CloudTrail, Amazon Athena

Managing storage spend – configuring retention

Use: S3 Storage Lens, S3 Lifecycle

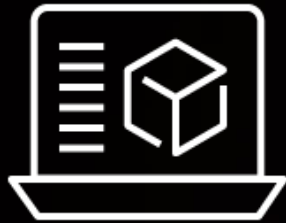
Customer voice – Bridgewater Associates

Use: S3 Intelligent-Tiering, AWS KMS



Continue your AWS storage learning

Build a learning plan



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

Increase your knowledge



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

Earn AWS Storage badges



Demonstrate your knowledge by achieving **digital badges**

aws.training/storage

Thank you!



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

