Module 4: Adding a Storage Layer with Amazon S3

Monday, October 6, 2025 1:59 PM

A. Defining Amazon S3:

- Types of storage:
  + ***Block Storage***: Data is stored on a device in fix-sized blocks
  + ***File Storage***: Data is stored in a hierarchical structure.
  + ***Object Storage***: Data is stored as objects based on attributes and metadata

NOTE: **Image the data is the content of the book and metadata is the cover of the book**

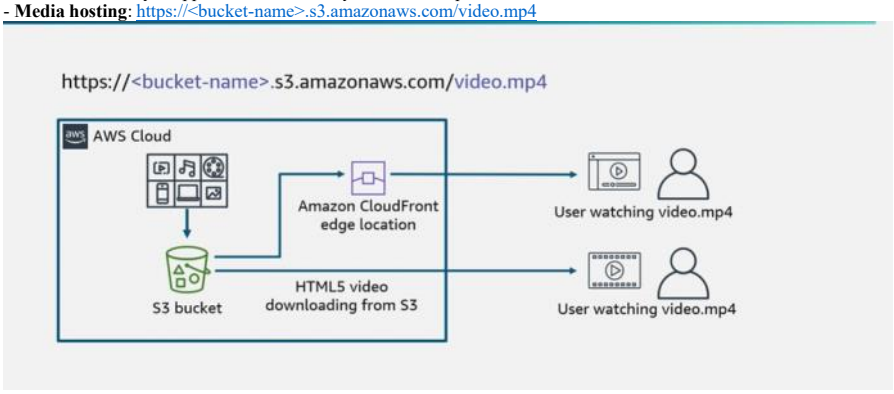
- Amazon S3:
  + Amazon S3 stores **massive (unlimited)** amounts of unstructured datas
  + Amazon S3 stores data file as objects in a bucket that you define
  + Five TB is the maximum file size of a single object
  + Objects have a globally unique URL (universal)
  + Objects have a key, version ID, value, metadata, and sub-resources.

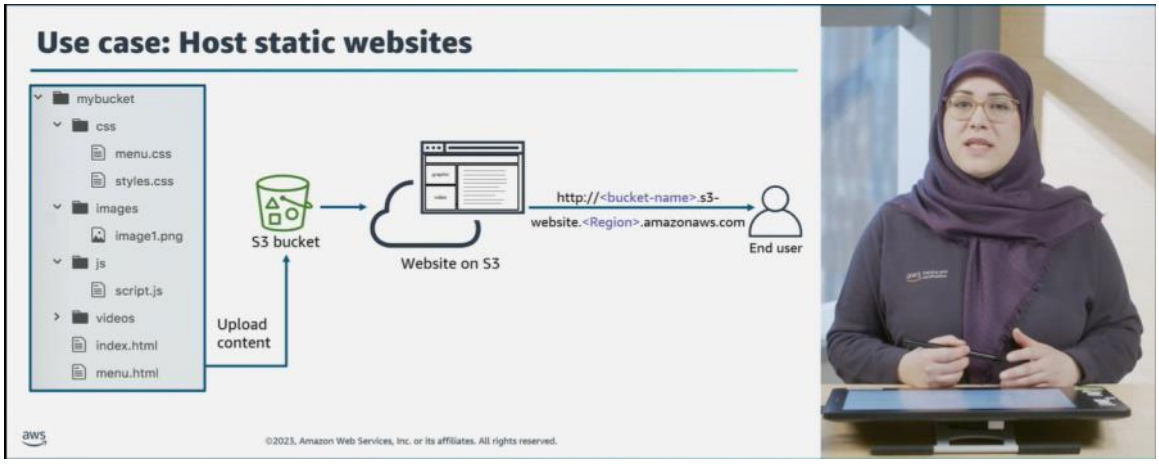
- Prefixes to imply a folder structure in an S3 bucket
- Amazon S3 benefits:

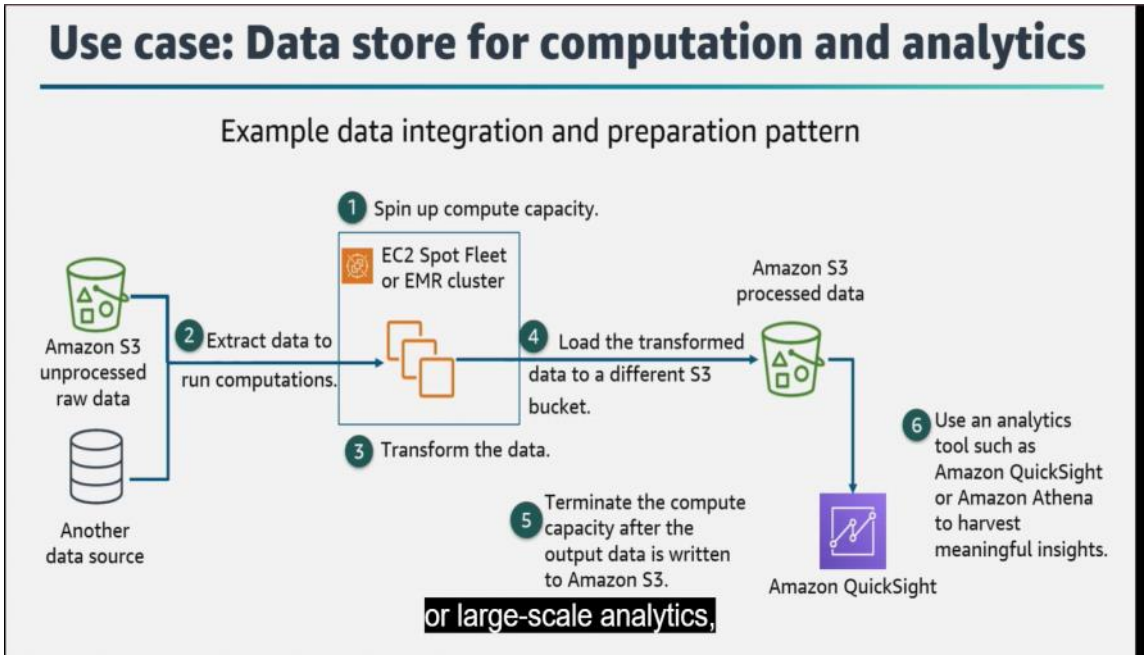
Benefit	Description
Durability	• Helps ensure that **data is not lost** • Provides S3 Standard storage with 11 nines (or 99.99999999999 percent0 of durability
Availability	• Provides access to data when needed • Includes unlimited capacity to store data • Provides S3 Standard storage wuth 4 nines (or 99.99 percent) of availability
High Performance	• Achieves thousands of transactions each second when uploading and retrieving storage • Automatically scales to high request rates

B. UsingAmazon S3:

- Spikes in demand: Host web content that needs bandwidth to address extreme spikes in demand
- Static site: Host a static site that consists of HTML, files, images, and videos
- Financial analysis: Store data that other services can use for analysis.
- Disaster recovery: Support disaster recovery or data backup solutions.
- Media hosting: https://<bucket-name>.s3.amazonaws.com/video.mp4





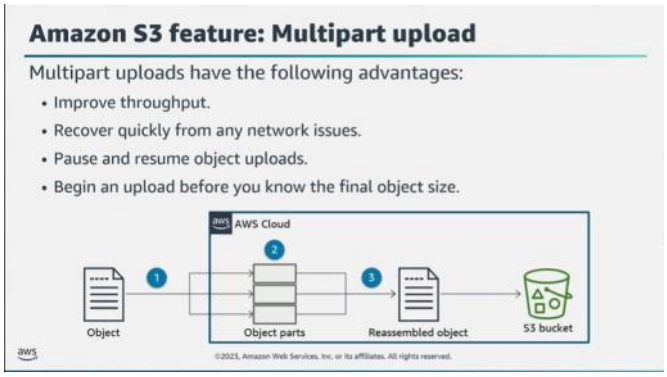


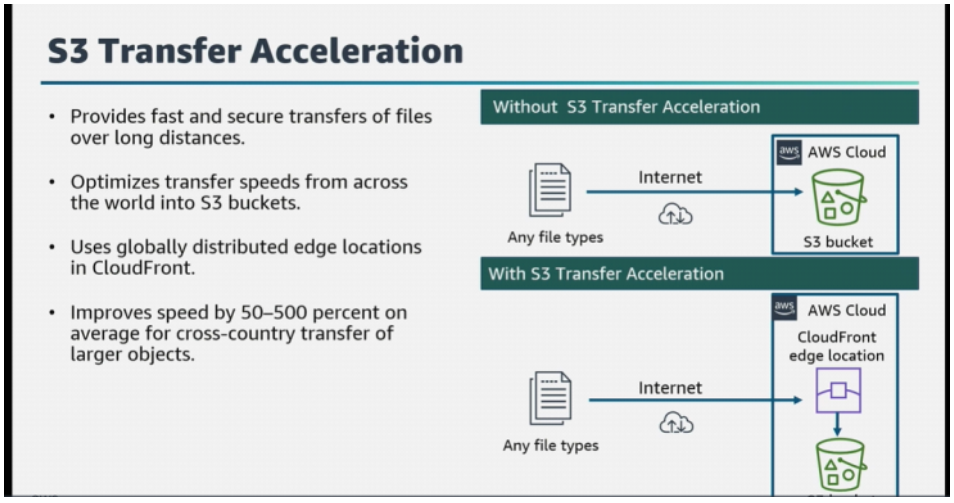
C. Moving daya to and from Amazon S3

- Storing objects in Amazon S3:
  + There is no limit to the number of objects in a bucket
  + Uploading an object requres write permission to the bucket.
  + Objects are encrypted by default:
    * Dyring upload, objects are automatically encrypted by using server-side encryption
    * During download, objects are decrypted

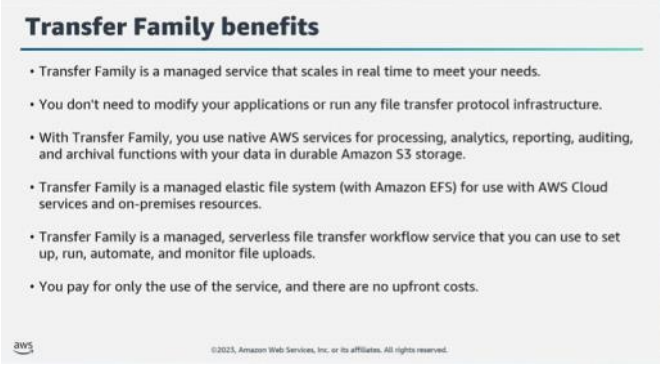
- Options for uploading objects to Amazon S3

Uploading Amazon S3	Description
AWS Management Console	Use a wizard-based approach to move data into or out of Amazon S3, including the option to drag amd drop files (max is 160GB)
AWS Command Line Interface (AWS CLI)	Upload or download from a terminal command prompt or in a call from a script
AWS SDKs	Use AWS SDKs to upload objects programatically
Amazon S3 REST API	Send a PUT request to upload data in a single operation





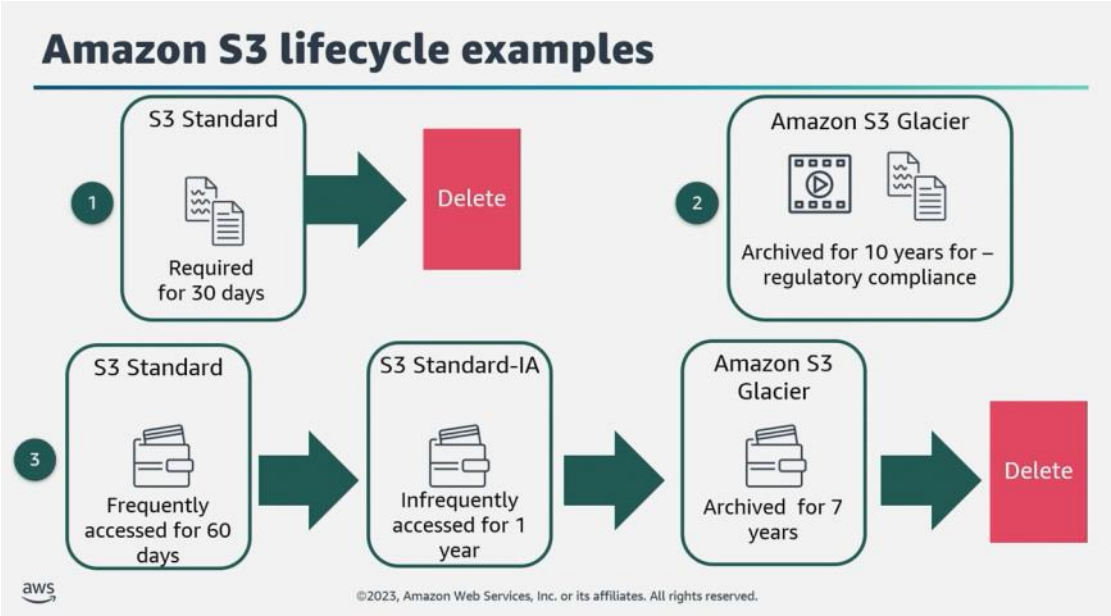
- AWS Transfer Family:
  + Is a fully managed AWS service
  + is used to tranfer files into and out of Amazon S3 storage or Amazon Elastic File System (Amazon EFS0 file systems over the following protocols:
    * Secure Shell (SSH) File Transfer Protocol (SFTP) version 3
    * File Transfer Protocol Secure (FTPS)
    * File Transfer Protocol (FTP)
    * Applicability Statement 2 (AS2)



D. Storing Content with Amazon S3

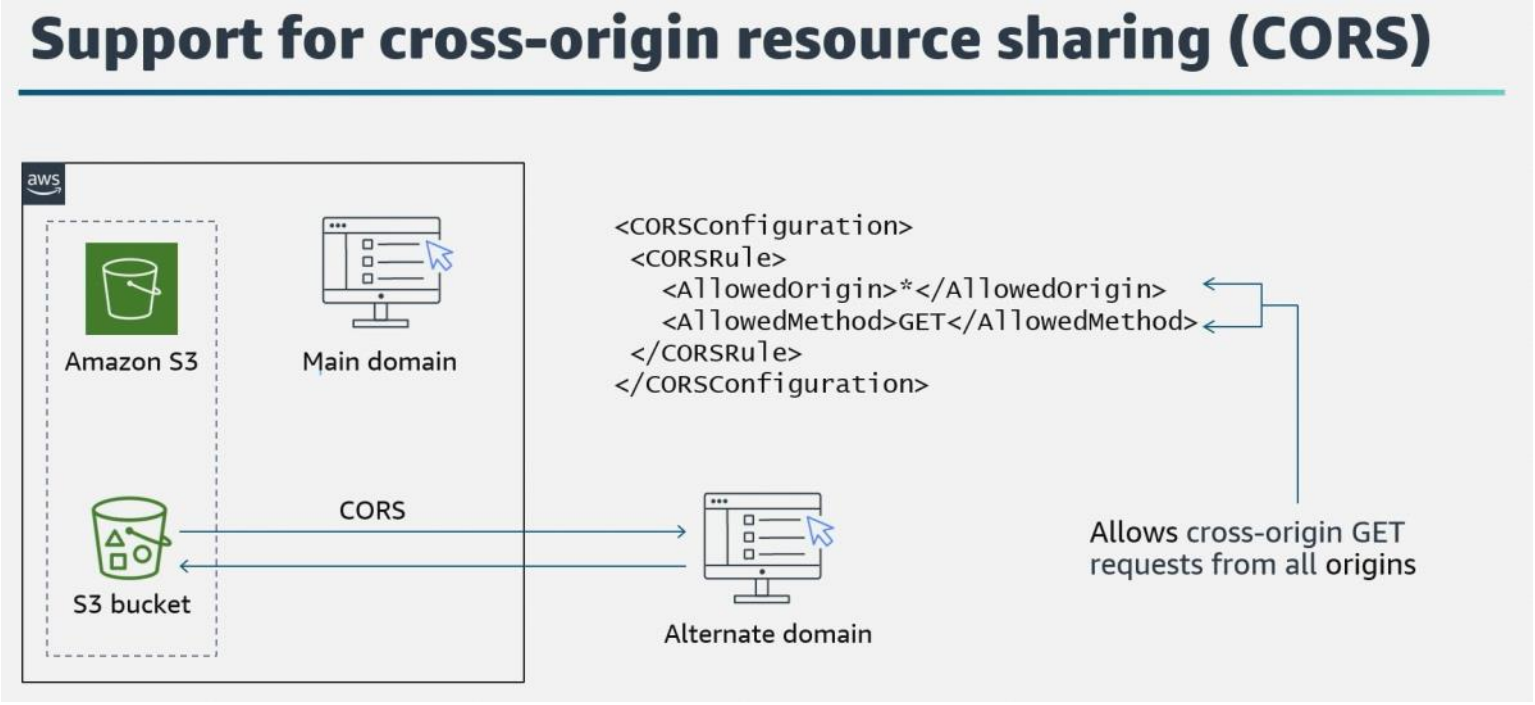
	S3 Standard	S3 Intelligent-Tiering	S3 Standard-IA	S3 One Zone-IA	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Availability Zones	≥3	≥3	≥3	1	≥3	≥3	≥3
Minimum capacity charge for each object	N/A	N/A	128 KB	128 KB	128 KB	N/A	N/A
Minimum storage duration charge	N/A	N/A	30 days	30 days	90 days	90 days	180 days
Retrieval charge	N/A	N/A	Per GB retrieved	Per GB retrieved	Per GB retrieved	Per GB retrieved	Per GB retrieved

- Amazon S3 lifecycle configurations are a set of rules that define actions that Amazon S3 applies to group of objects:
  + Transition actions transition to another storage class
  + Expiration actions define when objects expire



- Amazon S3 versioning: Amazon S3 versioning protects from accidental overrites and deletes:

Action	Versioning Enabled	Versioning Disbled or Versioning Suspended
Upload an object with the same key	Creates a new object with a different version ID, and both are retrievable by the version ID	Overwirtes the original objects, and the previous object is no longer retrievable
Delete	Adds a delete marker, but the object is still retrievable by the version ID	Deletes the object, and it is no longer retrievable



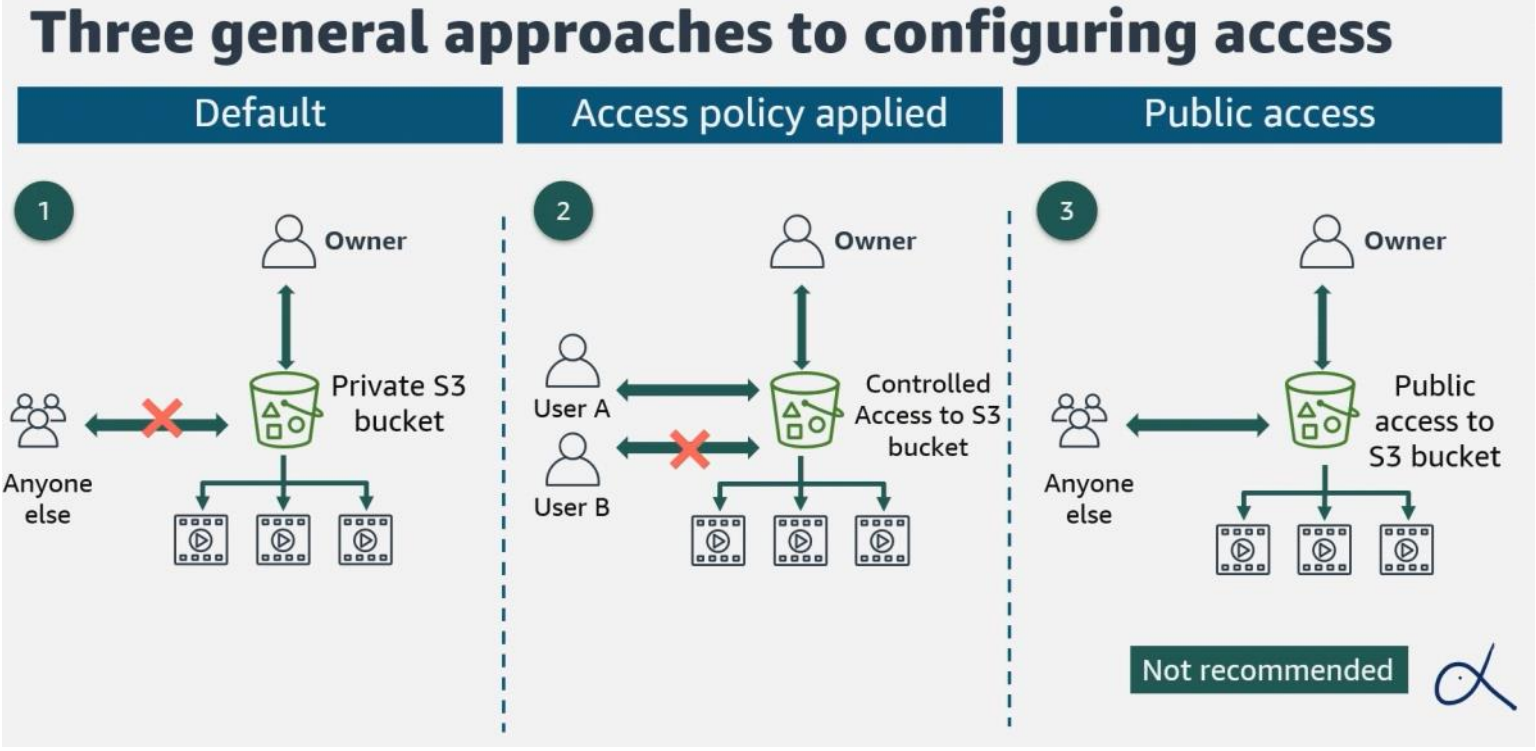
E. Designing with Amazon S3

- S3 buckets and objects created are private and protected by default.
- S3 bucket have encryption configured by default
- Server-side encryption with Amazon S3 managed keys (SSE-S3) is the default encryption
- When use cases must share Amazon S3 data, do the following:
  + Manage and control the data access
  + Follow the principle of elast privilege

- Encrypting objects in Amazon S3: Encryption encodes data with a secret key, which makes it unreadable without a key.
  + Server-side encyption:
    * Amazon S3 encryptes objects before it saves the objects to disk and decrypts the objects when users download them
    * Enable this feature by selecting the defauly encryption on the bucket
  + Client-side encryption:
    * Encrypt data on the client side and upload the encrypted data to Amazon S3
    * In this case, user's manage the encryption process

- Amazon S3 tools for protecting buckets and objects

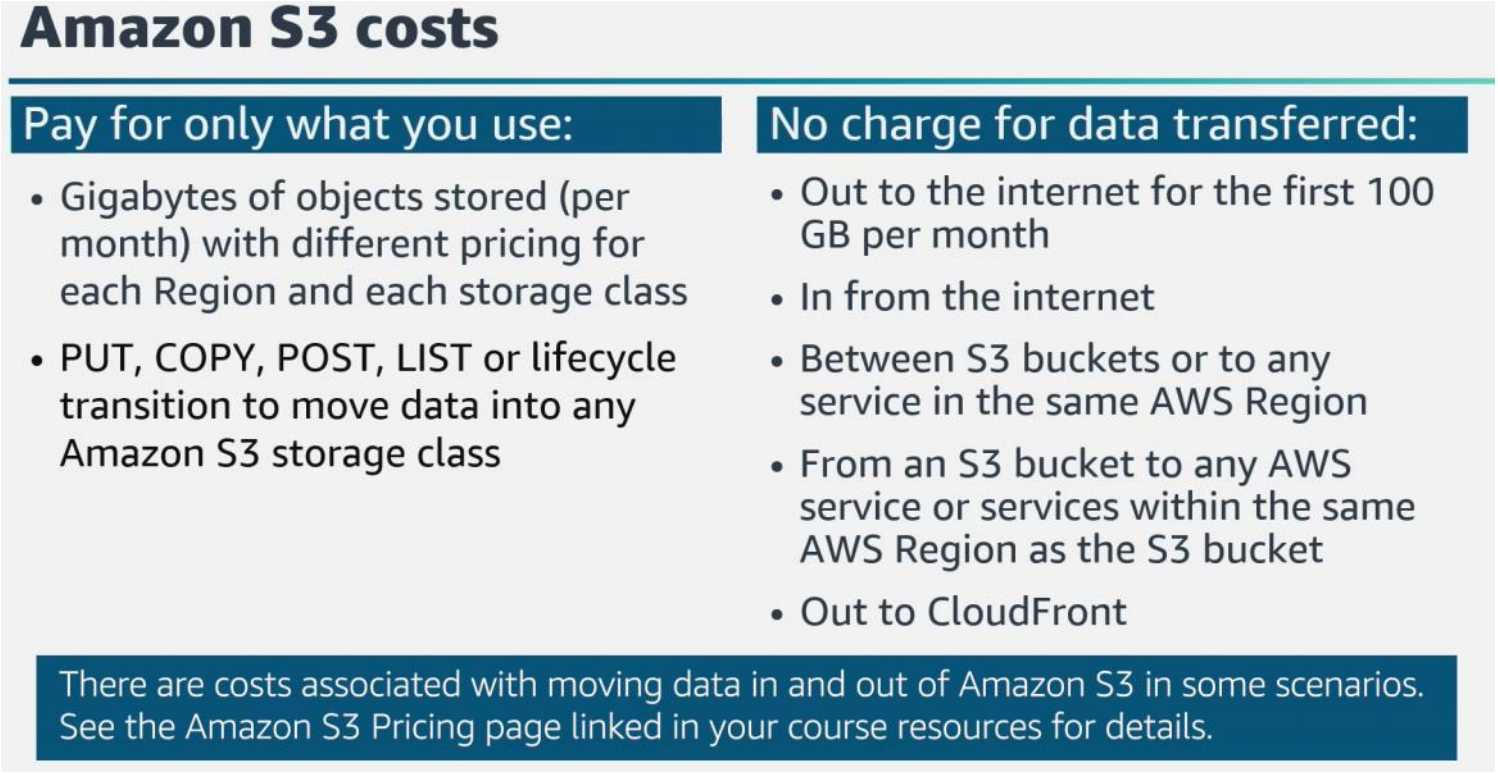
Tool	Description
Block Public Access feature	Makes bucket inaccessible to the public
AWS Identity and Access Managemenr (IAM) policies	Authenticates users by using IAM
Bucket policies	Defines access based on specific written rules
Access Control list (ACLs)	Sets rules for access to buckets and objects (bucket policies are the preferred method for controlling bucjet access)
Amazon S3 access points	Configures access with names and permissions specific to each application
Preassigned URLs	Grants time-limited access to others with temporary URLs
AWS Trysted Advisor	Provides a bucket permission check



- Considerations when choosing a Region;

Considerations	Details
Data privacy laws and regulatory compliance	• Are there relevant Region data privacy laws? • Can customer data be stored outside the country? • Can you meet your governance obligation?
Proximity of users to data	• Small differences in latency can impact customer experience. • Choose the Region closest to your users.
Availability service and feature	• Not all AWS services are available in all Regions. • Services expand to new Regions regularly. • Use some services cross-Region but at increased latency.
Cost-effectiveness	• Costs vary by Region. • Some services such as Amazon S3 have costs for transferring data out. • Consider the cost-effectiveness of replicating the entire environment in another Region.

- Amazon S3 Inventory:
  + Use Amazon S3 Inventory to help manage your storage
  + Use it to audit and report on the replication and encryption status of your objects for business, compliance, and regulatory meeds
  + Speed up business workflows and big data jobs by using Amazon S3 Inventory
  + Provide a scheduled alternative to the Amazon S3 synchronous List API Operations



F. Applying the AWS Well-Architected Framework principles to storage

1. Best practice approach for Security pillar:
- Enforce envryption at rest
- Encrypt objects
- Make private and block public access
- Enfore access control

2. Best practice approach for Performance Efficiency
- Learn about and understand available cloud services and features
- Better cost into architectural decisions

3. Best practice approach for Ccst Optimization:
Perform cost analysis for different usage over time

4. Best practice approach for Reliability
Select the appropriate locations for user's multi-location deployment