

AMAZON WEB SERVICES

AGENDA

2

AWS S3 Features- Versioning, Lifecycle Rules, Encryption types ,
Storage classes(Standard, IA, Glacier)

Access Management- Bucket policies vs IAM policies , public vs
private access, screenshot of setting permission

Static website hosting- steps to host a static website using S3 , show
screenshot of setting and example HTML.

AWS S3 FEATURES

S3 Versioning

- Allows you to keep multiple versions of an object in a bucket.
- Protects against accidental deletes and overwrites.
- Restore older versions anytime.
- Each object has a unique Version ID
- Old versions remain until permanently deleted
- Enable at bucket level (can only be suspended, not disabled)
- Use cases: Backup, recovery, audit trail, rollback

Lifecycle Rules

- Automates transition of objects between storage classes
- Helps **optimize cost** by moving infrequently used data to cheaper storage
- Can **expire (delete)** objects automatically after a defined time
- Applied at **bucket level** or to **specific objects (prefix/tags)**
- Common rules:
 - Move to **S3 Standard-IA** after 30 days
 - Move to **Glacier/Deep Archive** after 90 days
 - **Delete** after 365 days

Encryption Types

- SSE-S3 (Server-Side, S3 Managed Keys)
AWS manages the encryption keys
Simplest option(AES-256)
- SSE-KMS (Server-Side, KMS Keys)
Uses **AWS Key Management Service (KMS)**
More control + audit logs
You manage keys & permissions
- SSE-C (Server-Side, Customer-Provided Keys)
You provide your own encryption keys
AWS never stores the key
- Client-Side Encryption
Data encrypted **before upload**
Decrypted **after download**



AWS Storage Classes

6

- S3 Standard

For frequently accessed data

High durability (99.999999999%) and availability

Used for general-purpose storage

S3 Standard-IA (Infrequent Access)

Lower cost than Standard

For data accessed less often but still needs quick retrieval

Retrieval fee applies

S3 Glacier

Very low-cost archival storage

Retrieval within minutes to hours

Suitable for compliance and long-term backup

ACCESS MANAGEMENT

7

Bucket Policies vs IAM Policies

IAM Policies

Applied to users, groups, roles

Define what actions they can perform across AWS services

Example: Allow user to list all S3 buckets

Bucket Policies

Applied **directly to an S3 bucket**

JSON-based access rules

Control who can access the bucket and what actions they can perform

Example: Make bucket objects read-only to the public

- Public vs Private Access

Public Access

Anyone on the internet can access objects (if allowed)

Used for static websites, public datasets

Private Access

Only authenticated IAM users/roles can access

Default setting for all new S3 buckets

Recommended for sensitive data



Setting Permissions

9

aws

Search [Alt+S]

Europe (Stockholm)

Account ID: 5289-0924-4047
Rajnish%20Anand

Amazon S3

Buckets

demo-bucket-rajnish

Table buckets

Vector buckets

Access Grants

Access Points (General Purpose Buckets, FSx file systems)

Access Points (Directory Buckets)

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight 11

demo-bucket-rajnish

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)

[View analyzer for eu-north-1](#)

Block public access (bucket settings)

Edit

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

On

Individual Block Public Access settings for this bucket

Bucket policy

Edit

Delete



STATIC WEBSITE HOSTING ON AMAZON S3

10

Steps to Host a Static Website on S3

1.Create an S3 Bucket

- Bucket name must be globally unique.
- Uncheck Block all public access.

2.Upload Website Files

- Upload index.html, error.html, CSS, JS etc

- **3.Enable Static Website Hosting**

Go to Properties → Static Website Hosting.

Select “Use this bucket to host a website”.







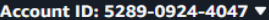

Enter index.html, error.html




- **4.Set Bucket Policy for Public Access**

Add bucket policy to allow public GetObject request

- **5.Access Website**

Use the given **S3 website endpoint URL**.

  [Alt+S]     Europe (Stockholm)  

Amazon S3 > Buckets > demo-bucket-rajnish > Edit static website hosting   

Amazon S3

<

General purpose buckets

Directory buckets

Table buckets

Vector buckets

Access Grants

Access Points (General Purpose Buckets, FSx file systems)

Access Points (Directory Buckets)

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting


☐ Disable

☒ Enable

Hosting type

☒ Host a static website
Use the bucket endpoint as the web address. [Learn more](#)

☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

 For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document
Specify the home or default page of the website.

Error document - optional
This is returned when an error occurs.

Redirection rules – optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

Example HTML

```
<!DOCTYPE html>  
<html>  
  <head>  
    <title>My Static Website</title>  
  </head>  
  <body>  
    <h1>Welcome to My S3 Hosted Website!</h1>  
    <p>This is a static website hosted on Amazon S3.</p>  
  </body>  
</html>
```