

Amazon Simple Storage Service **(S3)**



By:- Kartikay
December Intern

DOCUMENT - 1

Table of Content:-

1. What is AWS ?	3
Benefits of AWS:-	3
2. What is Amazon S3 ?	4
3. Features of Amazon S3:-	5
→ Storage Classes	5
→ Storage Management	5
→ Access Management & Security	6
→ Data processing	6
→ Storage logging & Monitoring	6
4. How Amazon S3 Works	8
Key Points :-	13
(a) Bucket	13
(b) Objects	14
(c) Key	14
(d) S3 Versioning	14
(e) Version Id	14
(f) Bucket Policy	14
(g) S3 Access Point	15
(h) Access Control Lists (ACL)	15
(i) Region	15
# Reference Links	16

DOCUMENT - 1

1. What is AWS ?

- Amazon Web Services (AWS) is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow.



Benefits of AWS:-

- Flexibility
- Cost Effective
- Scalability
- Security
- User-friendly
- Data Encryption

DOCUMENT - 1

2. What is Amazon S3 ?

- Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.
- Store and protect any amount of data for a range of use cases, such as data lakes, websites, cloud-native applications, backups, archive, machine learning, and analytics.



- Amazon S3 is designed for **99.999999999% (11-9's)** of durability, and stores data for millions of customers all around the world.

DOCUMENT - 1

3. Features of Amazon S3:-

→ Storage Classes

Amazon S3 storage classes are designed to give customers flexibility when storing their data on AWS. Four storage classes are available:

- **Standard:** the default storage class and is suitable for most workloads.
- **Standard – Infrequent Access (Standard – IA):** designed for data accessed less frequently but still needs to be quickly accessible.
- **Reduced Redundancy Storage (RRS):** designed for data that can be safely stored with lower levels of redundancy.
- **Glacier:** designed for infrequently accessed data and can be stored for long periods at a lower cost.

→ Storage Management

Amazon S3 storage management lets you control how your data is stored and organized within your Amazon S3 buckets. With storage management, you can specify how Amazon S3 keeps your information, whether held in a standard storage or infrequent access (IA) storage class and stored in a bucket versioning-enabled or versioning-disabled bucket. You can also specify whether Amazon S3 encrypts your data at rest and whether your data is automatically compressed.

DOCUMENT - 1

→ Access Management & Security

Amazon S3's access management features allow you to control who has access to your data securely. You can manage access to your data using access control lists (ACLs) or Amazon S3 bucket policies. ACLs allow you to grant granular permissions to individual users or groups.

→ Data processing

Data processing refers to taking data and manipulating it to extract valuable information. This can be done through various methods.

Amazon S3 offers a variety of features that make it an ideal platform for data processing, including:

- **Scalability:** Amazon S3 can scale to accommodate any amount of data, making it ideal for big data processing.
- **Flexibility:** Amazon S3 supports various data formats, making it easy to process data from multiple sources.
- **Durability:** Amazon S3 is designed to be highly durable, meaning that data is unlikely to be lost even if there are hardware failures.
- **Security:** Amazon S3 offers a variety of security features, making it a safe platform for storing and processing sensitive data.

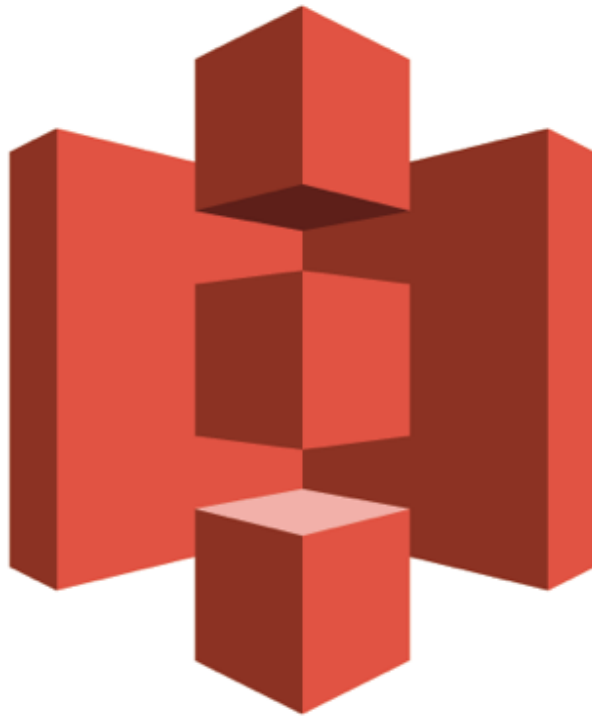
→ Storage logging & Monitoring

Amazon S3 storage logging and monitoring provide visibility into the requests made to your Amazon S3 bucket. Amazon S3 storage logs give you information about when each request was made, the request path, the

DOCUMENT - 1

request method, the request headers, and the request-response headers. Amazon S3 access logs also give you the identity of the requester:

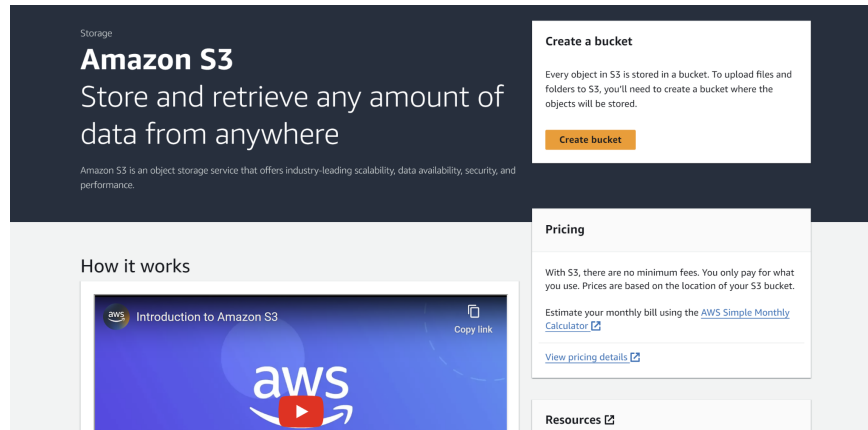
- With Amazon S3 storage logging and monitoring, you can track the data access patterns in your Amazon S3 bucket and use the information to troubleshoot issues, audit compliance, or analyze data usage trends.
- Amazon S3 storage logging and monitoring are disabled by default. To enable storage logging and tracking, you must create an Amazon S3 bucket and then allow logging on the bucket.



Amazon S3

DOCUMENT - 1

4. How Amazon S3 Works



I. Create a bucket with a unique name.

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name [Info](#)

alphabucket2342

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

II. Block all public access.

Block Public Access settings for this bucket

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 this bucket and its 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☒ Block public access to buckets and objects granted through *new* access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☒ Block public access to buckets and objects granted through *any* access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☒ Block public access to buckets and objects granted through *new* public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☒ Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

DOCUMENT - 1

III. Then click on “Create Bucket”.

► Advanced settings

i After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel Create bucket

IV. After that upload (object) file in the bucket.

Objects (0) [Info](#)
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Refresh Copy S3 URI Copy URL Download Open Delete Actions ▼ Create folder Upload

	Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.					

Upload

Files and folders (1 Total, 7.0 KB)
All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	FOSTERING.webp		image/webp	7.0 KB

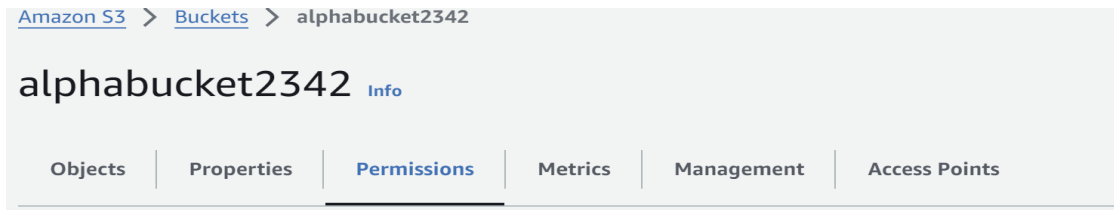
Destination [Info](#)
Destination
[s3://alphabucket2342](#)
► Destination details
Bucket settings that impact new objects stored in the specified destination.
► Permissions
Grant public access and access to other AWS accounts.
► Properties
Specify storage class, encryption settings, tags, and more.

Cancel Upload

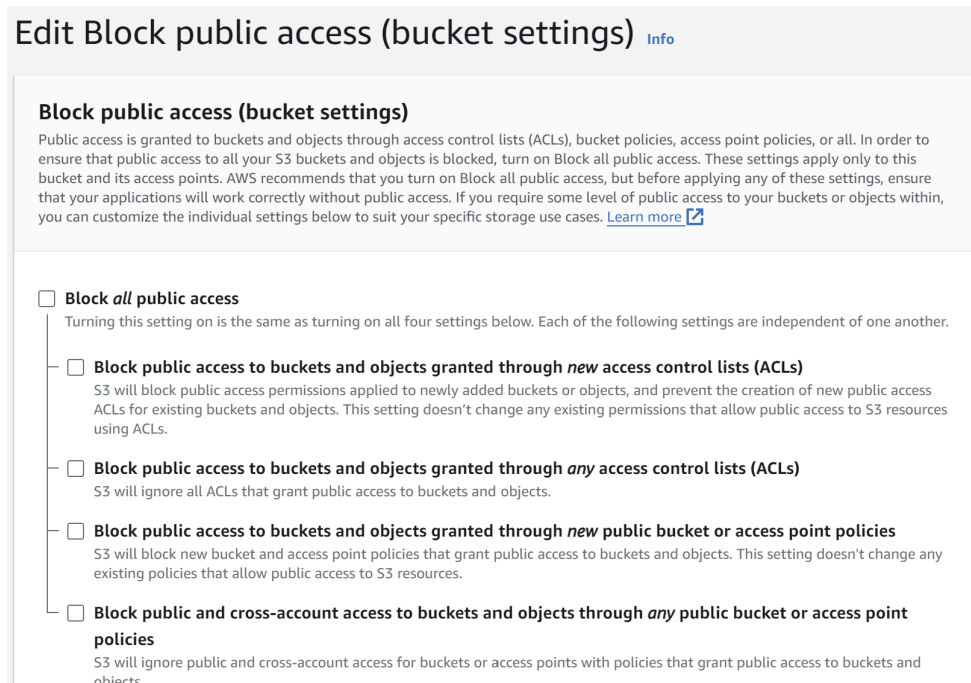
Here FOSTERING.webp is the object that is stored in the bucket (alphabucket2342).

DOCUMENT - 1

V. Then go to “Permissions” in the object.



VI. To access that object we need to unblock the permission of public access. We can do this earlier as well while creating a bucket.



DOCUMENT - 1

- VII. Then go to “Permission” and click on edit in Bucket Policy then click on edit then click on “Policy Generator”.

Bucket policy

EditDelete

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket policy

Policy examplesPolicy generator

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket ARN

arn:aws:s3:::alphabucket2342

- VIII. After this, complete the Step-1, Step-2 and Step-3.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3 ☐ All Services (*)

Use multiple statements to add permissions for more than one service.

Actions 1 Action(s) Selected ☐ All Actions (*)

Amazon Resource Name (ARN) arn:aws:s3:::alphabucket234

ARN should follow the following format: arn:aws:s3:::(BucketName)/(Key/KeyName).
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

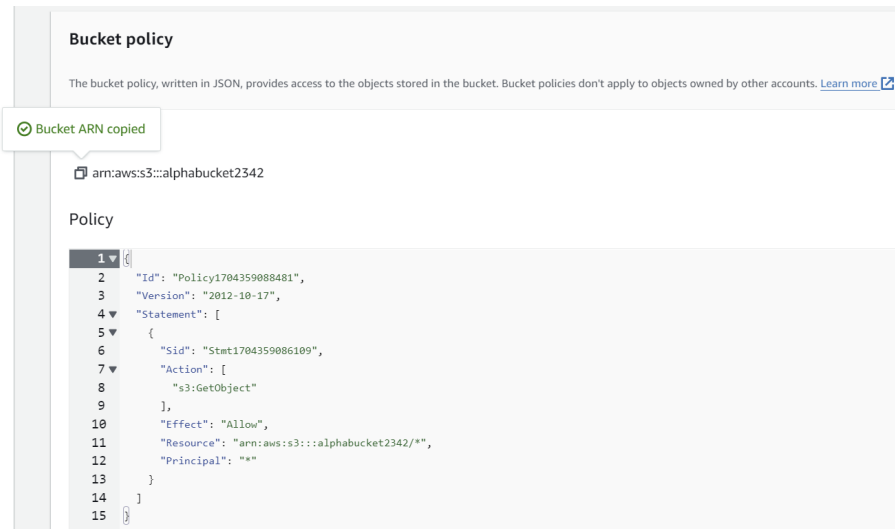
Step 3: Generate Policy

A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

```
{
  "Id": "Policy1704359253385",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmnt1704359248910",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::alphabucket2342",
      "Principal": "*"
    }
  ]
}
```

DOCUMENT - 1

IX. Then go back to “Bucket Policy” and paste that code.



X. Remember one thing write “/*” after the bucket name in the code. Then click on save change.

```
"Effect": "Allow",
"Resource": "arn:aws:s3:::alphabucket2342/*",
"Principal": "*"

```

XI. Then go to the bucket and click on the object and copy the URL of that object.

Object URL

 <https://alphabucket2342.s3.ap-south-1.amazonaws.com/FOSTERING.webp>

DOCUMENT - 1

- XII. Lastly, open a new tab and paste that URL, if that URL runs properly then our data is successfully stored on cloud.



Key Points :-

(a) Bucket

- It is a container to store objects in Amazon S3.
- It also organize the Amazon S3 namespace at the highest level

Buckets also:

- Organize the Amazon S3 namespace at the highest level.
- Identify the account responsible for storage and data transfer charges.
- Provide access control options, such as bucket policies, access control lists (ACLs), and S3 Access Points, that you can use to manage access to your Amazon S3 resources.
- Serve as the unit of aggregation for usage reporting.

DOCUMENT - 1

(b) Objects

- Fundamental entities stored in amazon s3.
- Objects consist of object data and metadata.
- Metadata :- It is a set of name - value pairs that describe the object.
- An object is uniquely identified within a bucket by a key (name) and a version ID.

(c) Key

- An object key is the unique identifier for an object within a bucket.
- Every object in a bucket has exactly one key.

(d) S3 Versioning

- S3 versioning means to keep multiple variants of an object in the same bucket we use S3 versioning.
- We can preserve, retrieve and restore every version of every object stored in a bucket.

(e) Version Id

- When we enable S3 Versioning in the bucket, amazon s3 generates a unique version id for each object added to the bucket.

(f) Bucket Policy

- It is a resource based AWS IAM (Identity & Access Management) policy that is used to grant access permission to the bucket and the object.

DOCUMENT - 1

- Only bucket owners can associate a policy with a bucket.
- Bucket policies are limited to 20 kb in size.

(g) S3 Access Point

- These are named network end points with dedicated access policies that describe how data can be accessed using endpoints.
- It simplifies managing data access at scale for shared dataset in Amazon S3.
- Each access point has its own access point policy.

(h) Access Control Lists (ACL)

- We use ACL to grant read and write permissions to authorized users for individual buckets/objects.
- In modern use cases in Amazon S3 no longer require the use of ACLs.

(i) Region

- Choose a geographical AWS region for storing.
- We might choose a region to optimize latency, minimize cost.
- Objects stored in an AWS region never leave the region unless you transfer or replicate.

DOCUMENT - 1

Reference Links

- https://docs.aws.amazon.com/s3/?nc2=h_gl_doc_s3
- https://youtu.be/sWOkwp4Kd_I?si=RTez-oGOljFGGcVu
- https://youtu.be/k1RI5locZE4?si=E6F_VZJkZUBrO8fO
- https://youtu.be/HTb_VYOE4WM?si=NU6JOY8F13G1wzzb
- https://youtu.be/_I14_sXHO8U