Amazon Simple Storage Service (S3)

amazon
S3

By:- Kartikay
December Intern

Table of Content:-

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

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.

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.

➔ 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.

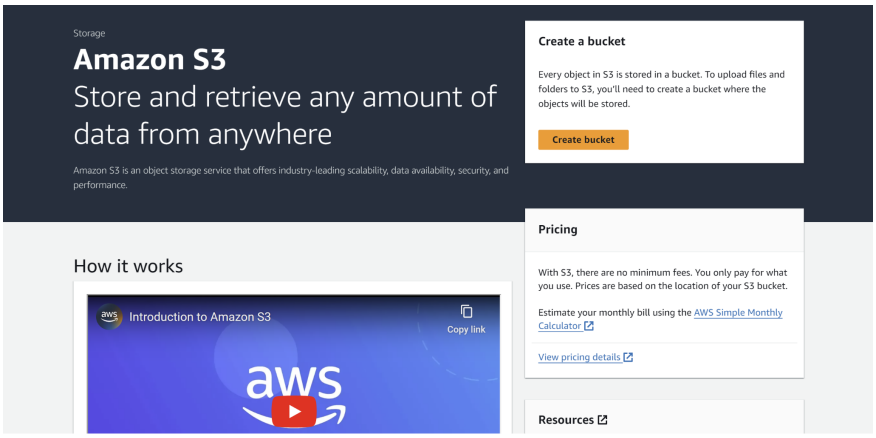
➔ Storage logging & Monitoring

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

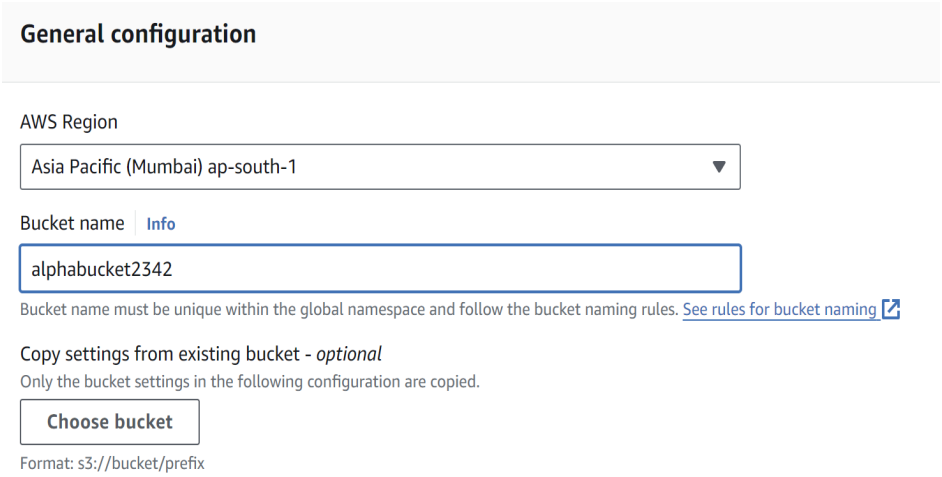
request method, the request headers, and the request-response headers. Amazon S3 access logs also give you the identity of the requester:

- 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.

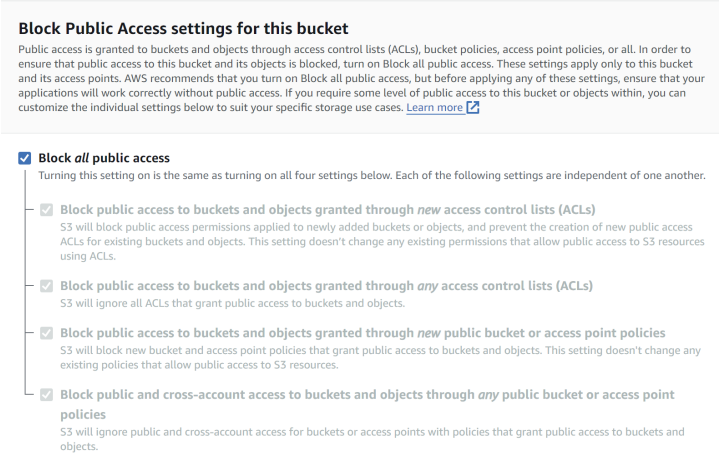
4. How Amazon S3 Works



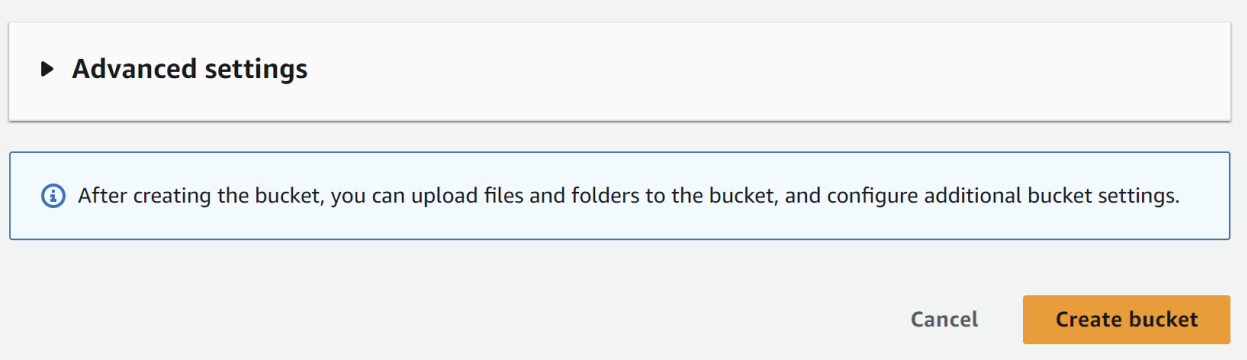
I. Create a bucket with a unique name.



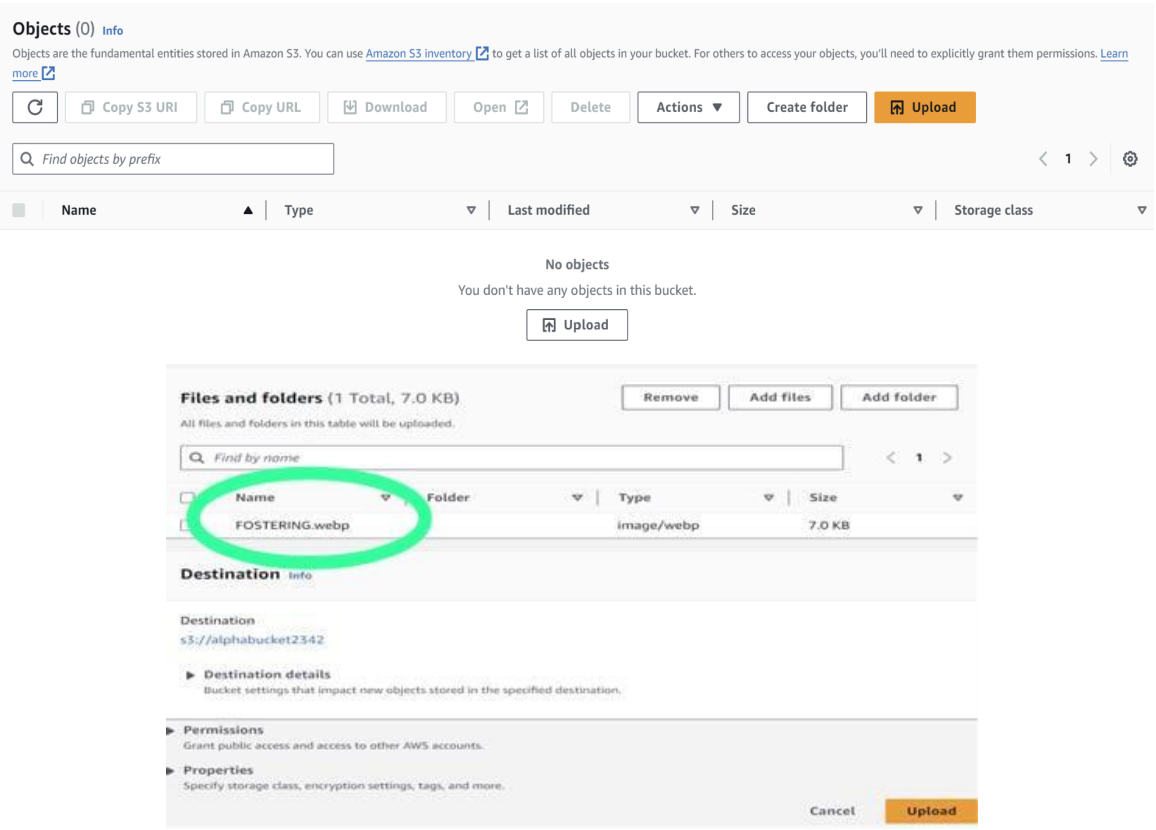
II. Block all public access.



III. Then click on “Create Bucket”.

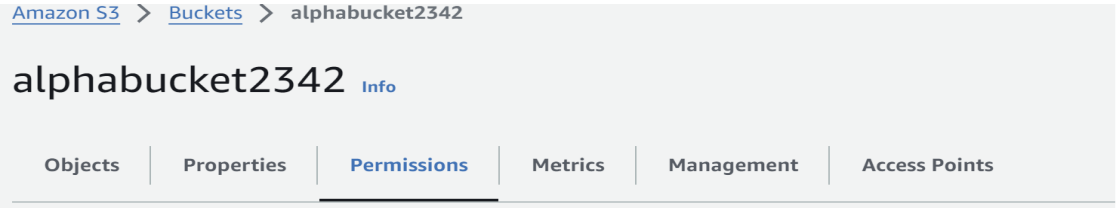


IV. After that upload (object) file in the bucket.

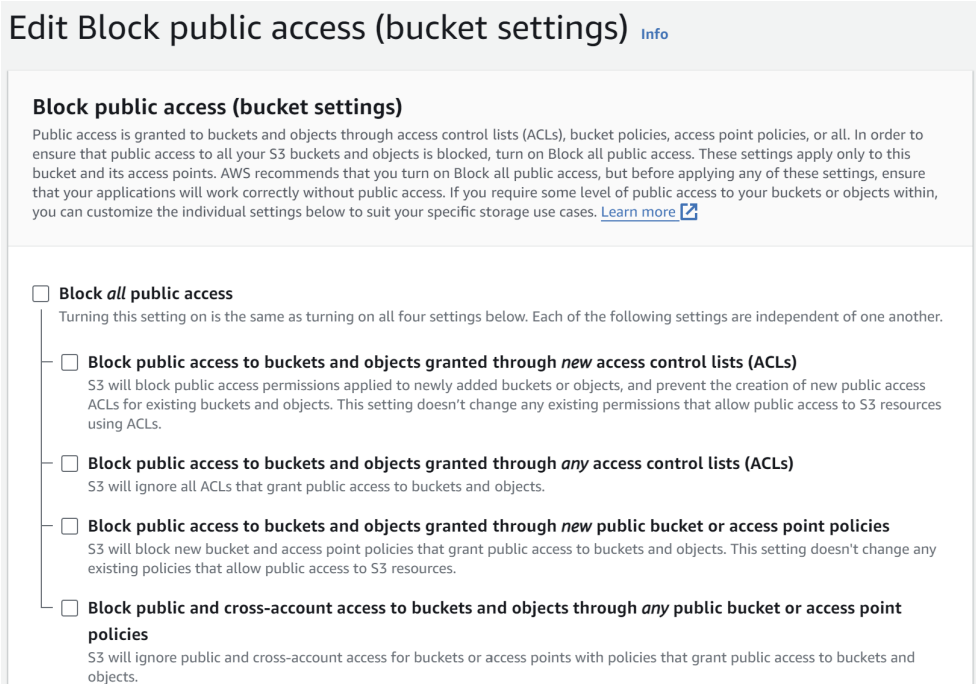


Here FOSTERING.webp is the object that is stored in the bucket (alphabucket2342).

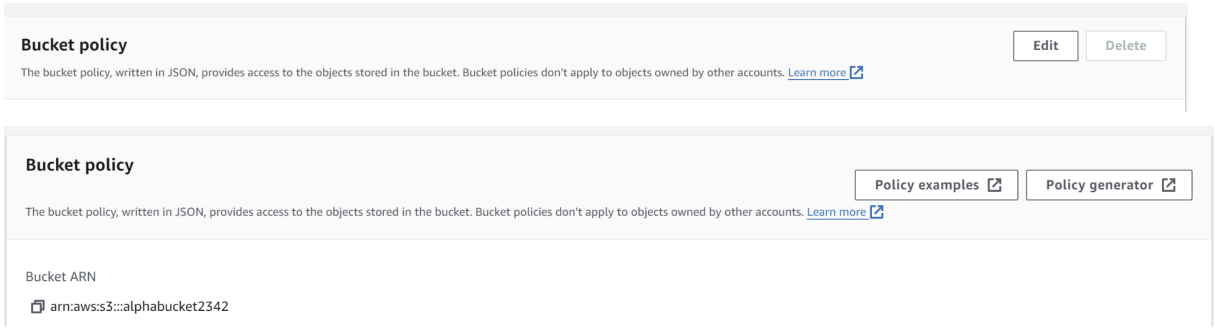
V. Then go to “Permissions” in the object.



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.

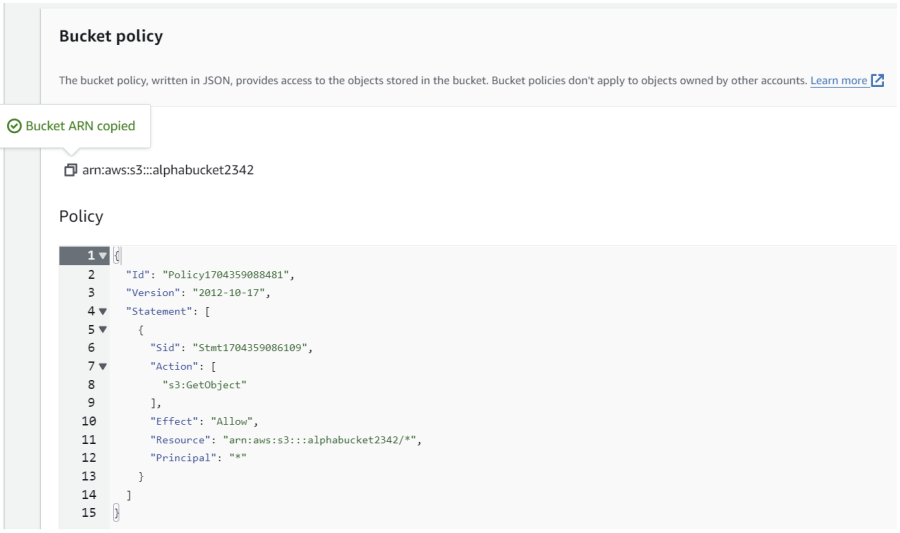


VII. Then go to “Permission” and click on edit in Bucket Policy then click on edit then click on “Policy Generator”.

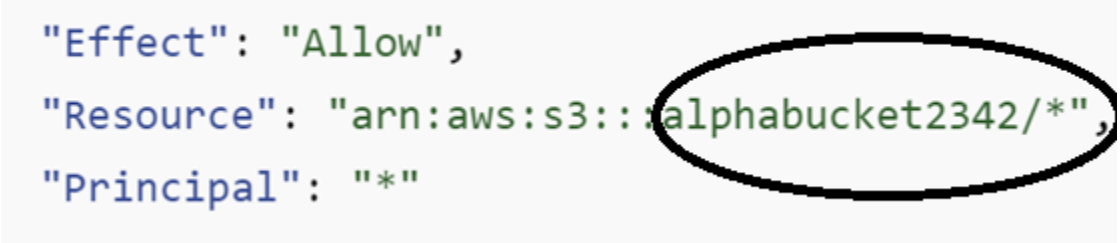


VIII. After this, complete the Step-1, Step-2 and Step-3.

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.**



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

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.

(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.

- 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.

Reference Links

- https://docs.aws.amazon.com/s3/?nc2=h_ql_doc_s3
- https://youtu.be/sWOkwp4Kd_I?si=RTez-oGOIjFGGcVu
- https://youtu.be/k1RI5locZE4?si=E6F_VZJkZUBrO8fO
- https://youtu.be/HTb_VYOE4WM?si=NU6JOY8F13G1wzzb
- https://youtu.be/_I14_sXHO8U