DreamsPlus™
India | Singapore

AWS S3 - Properties

DreamsPlus™
India | Singapore

AWS S3 - Properties

- Versioning
- Server Access Logging
- Static Website Hosting
- Object Level Logging
- Default Encryption
- Object Lock
- Tags
- Transfer Acceleration
- Events
- Requester Pays

DreamsPlus™
India | Singapore

Versioning

- Versioning enables you to keep multiple versions of an object in one bucket.
- When versioning is enable, a version ID is associated with every version of the object.
- Once versioning is enabled on the bucket, it cannot be turned off, it can only be suspended.
- When versioning is suspended, we will not have multiple versions of the same object in the bucket.
- Versioning is one way to safeguard the objects in the S3 bucket. Another way to safeguard the objects in the S3 bucket is to use MFA Delete.
- To enable versioning on the bucket – Go to properties – Versioning – Enable Versioning.
- To suspend versioning on the bucket – Go to properties – Versioning – Suspend Versioning.

DreamsPlus™
India | Singapore

Server Access Logging

- Server access logging provides detailed records for the requests that are made to a bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits. It can also help you learn about your customer base and understand your Amazon S3 bill.
- To track requests for access to your bucket, you can enable server access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and an error code, if relevant
- Turn on the log delivery by adding logging configuration on the bucket for which you want Amazon S3 to deliver access logs. We refer to this bucket as the *source bucket*.
- Grant the Amazon S3 Log Delivery group write permission on the bucket where you want the access logs saved. We refer to this bucket as the *target bucket*

DreamsPlus™
India | Singapore

Static Website Hosting

- You can host a static website on Amazon S3. On a static website, individual webpages include static content. They might also contain client-side scripts. By contrast, a dynamic website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting.
- To host a static website using S3, one has to enable to setting on the properties section of the S3 bucket.
- Create an index.html file and place it in the root of the S3 bucket.
- Enable public read for all objects, using a bucket policy on the S3 bucket.
- View the website from the auto-generated endpoint provided to us by AWS.
- One can optionally configure an error.html file too incase there are any 400,500 errors on the website.

DreamsPlus™
India | Singapore

Object Level Logging

Data Events : Data events provide insight into the resource operations performed on or within a resource. These are also known as data plane operations. Data events are often high-volume activities.

Example data events include:

- Amazon S3 object-level API activity (for example, GetObject, DeleteObject, and PutObject API operations)
- AWS Lambda function execution activity (the Invoke API)

To enable Object Level Logging – Create a CloudTrail trail in CloudTrail's console. Choose all S3 buckets. Choose all regions. Choose all actions. Create the trail. Log the activities or data events to another S3 bucket for auditing purposes or to a CloudWatch log group.

Therefore by default when enabled for all S3 buckets, any new buckets that are created also will be enabled with this setting on the properties.

DreamsPlus™
India | Singapore

Default Encryption

- Amazon S3 default encryption provides a way to set the default encryption behaviour for an S3 bucket. You can set default encryption on a bucket so that all new objects are encrypted when they are stored in the bucket. The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or customer master keys (CMKs) stored in AWS Key Management Service (AWS KMS).
- When you use server-side encryption, Amazon S3 encrypts an object before saving it to disk and decrypts it when you download the objects.
- There is no change to the encryption of the objects that existed in the bucket before default encryption was enabled.

When you upload objects after enabling default encryption:

- If your PUT request headers don't include encryption information, Amazon S3 uses the bucket’s default encryption settings to encrypt the objects.
- If your PUT request headers include encryption information, Amazon S3 uses the encryption information from the PUT request to encrypt objects before storing them in Amazon S3.

DreamsPlus™
India | Singapore

Object Lock

- With Amazon S3 object lock, you can store objects using a *write-once-read-many* (WORM) model. You can use it to prevent an object from being deleted or overwritten for a fixed amount of time or indefinitely.
- Amazon S3 object lock helps you meet regulatory requirements that require WORM storage, or simply add another layer of protection against object changes and deletion.
- Amazon S3 object lock has been assessed by Cohasset Associates for use in environments that are subject to SEC 17a-4, CTCC, and FINRA regulations

Amazon S3 object lock provides two ways to manage object retention: retention periods and legal holds.

- A *retention period* specifies a fixed period of time during which an object remains locked. During this period, your object is WORM-protected and can't be overwritten or deleted.
- A *legal hold* provides the same protection as a retention period, but it has no expiration date. Instead, a legal hold remains in place until you explicitly remove it. Legal holds are independent from retention periods.

Note : Object Lock requires Bucket Versioning to be enabled.

DreamsPlus™
India | Singapore

Object Lock Modes

Amazon S3 object lock provides two *retention modes*:

- Governance mode
- Compliance mode

Governance mode : In governance mode, users can't overwrite or delete an object version or alter its lock settings unless they have special permissions. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary.

Compliance mode : In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account. When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode ensures that an object version can't be overwritten or deleted for the duration of the retention period.

DreamsPlus™
India | Singapore

Tags

- To track the storage cost or other criteria for individual projects or groups of projects, label your Amazon S3 buckets using cost allocation tags.
- A *cost allocation tag* is a key-value pair that you associate with an S3 bucket. After you activate cost allocation tags, AWS uses the tags to organize your resource costs on your cost allocation report.
- Cost allocation tags can only be used to label buckets.
- AWS provides two types of cost allocation tags, an AWS-generated tag and user-defined tags. AWS defines, creates, and applies the AWS-generated createdBy tag for you after an Amazon S3 CreateBucket event.
- You define, create, and apply *user-defined* tags to your S3 bucket.

DreamsPlus™
India | Singapore

Transfer Acceleration

- Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket.
- Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations.
- As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

You might want to use Transfer Acceleration on a bucket for various reasons, including the following:

- You have customers that upload to a centralized bucket from all over the world.
- You transfer gigabytes to terabytes of data on a regular basis across continents.
- You are unable to utilize all of your available bandwidth over the Internet when uploading to Amazon S3.

DreamsPlus™
India | Singapore

Transfer Acceleration

- You can point your Amazon S3 PUT object and GET object requests to the s3-accelerate endpoint domain name after you enable Transfer Acceleration.
- For example, let's say you currently have a REST API application using PUT Object that uses the host name **mybucket.s3.amazonaws.com** in the PUT request.
- To accelerate the PUT you simply change the host name in your request to **mybucket.s3-accelerate.amazonaws.com**.
- To go back to using the standard upload speed, simply change the name back to **mybucket.s3.amazonaws.com**.

Events

- You can enable certain Amazon S3 bucket events to send a notification message to a destination whenever the events occur.

Amazon S3 can send notifications for the following types of events:

- An object created event
- An object delete event
- Restore object events
- A Reduced Redundancy Storage (RRS) object lost event

Event notification messages can be sent to the following types of destinations:

- An Amazon Simple Notification Service (Amazon SNS) topic
- An Amazon Simple Queue Service (Amazon SQS) queue
- A Lambda function

DreamsPlus™
India | Singapore

Events

- A sample use case : Whenever a user deletes or creates an object in an S3 bucket, the administrator should be notified in his respective mail address of the same API action.
- Step 1 : Create an S3 bucket
- Step 2 : Create an SNS topic
- Step 3 : Subscribe the administrator’s mail address to the SNS topic
- Step 4 : Confirm the subscription in the mail
- Step 5 : Modify the SNS topic policy to use the S3 bucket and topic ARN
- Step 6 : Enable events on the S3 bucket, choose the API actions and SNS topic

DreamsPlus™
India | Singapore

Events

```
{
 "Version": "2008-10-17",
 "Id": "example-ID",
 "Statement": [
  {
   "Sid": "example-statement-ID",
   "Effect": "Allow",
   "Principal": {
     "Service": "s3.amazonaws.com"
   },
   "Action": [
    "SNS:Publish"
   ],
   "Resource": "arn:aws:sns:REGION:ACCOUNT-ID:TOPICNAME",
   "Condition": {
      "ArnLike": { "aws:SourceArn": "arn:aws:s3:*:*:bucket-name" }
   }
  }
 ]
}
```

Requester Pays

- In general, bucket owners pay for all Amazon S3 storage and data transfer costs associated with their bucket. A bucket owner, however, can configure a bucket to be a Requester Pays bucket. With Requester Pays buckets, the requester instead of the bucket owner pays the cost of the request and the data download from the bucket. The bucket owner always pays the cost of storing data
- Typically, you configure buckets to be Requester Pays when you want to share data but not incur charges associated with others accessing the data. You might, for example, use Requester Pays buckets when making available large datasets, such as zip code directories, reference data, geospatial information, or web crawling data.
- When the requester assumes an AWS Identity and Access Management (IAM) role prior to making their request, the account to which the role belongs is charged for the request.