

S3 (SIMPLE STORAGE SERVICE)

Introduction to S3

Amazon S3 is one of first services introduced by AWS. Amazon S3 provides developers and IT teams with secure, durable, and highly-scalable cloud storage. Amazon S3 is easy-to-use object storage with a simple web service interface that you can use to store and retrieve any amount of data from anywhere on the web. Amazon S3 also allows you to pay only for the storage you actually use, which eliminates the capacity planning and capacity constraints associated with traditional storage.

Block storage operates at a lower level, the raw storage device level and manages data as a set of numbered, fixed-size blocks. Object storage or File storage operates at a higher level, the operating system level, and manages data as a named hierarchy of files and folders.

- S3 is Object based i.e. allows you to upload, Download, Share files.
- All our Objects reside in containers called **buckets**.
- S3 is a universal namespace that means **name of your bucket must be unique globally**.
- Amazon S3 is cloud object storage. Instead of being closely associated with a server, Amazon S3 storage is independent of a server and is accessed over the Internet.
- You can create and use multiple buckets; you can have up to **100 per account by default**, this is a soft limit, you can increase this at any time by creating a service limit increase ticket with AWS.
- File Size can be from 0/1 Byte to 5TB
- Single bucket can store an unlimited number of files.
- You can create buckets in your nearby region which is located close to a particular set of end users or customers in order to minimize latency.
- Or, Create bucket and store data far away from your primary facilities in order to satisfy disaster recovery and compliance needs
- Amazon S3 objects are automatically replicated on multiple devices in multiple facilities within a region
- Every Amazon S3 object can be addressed by a unique URL i.e; <http://mybucket.s3.amazonaws.com/document.doc>
- You can access using this URL also <https://s3-region.amazonaws.com/uniquebucketName/objectname>
- Bucket names must be at least 3 and no more than 63 characters long
- Bucket names must not be formatted as an IP address (e.g., 192.168.5.4).

Invalid Name	Bucket	Comment
--------------	--------	---------

.myawsbucket	Bucket name cannot start with a period (.).
myawsbucket.	Bucket name cannot end with a period (.).
my..examplebucket	There can be only one period between labels

S3 Storage classes:

S3-Standard – Amazon S3 Standard offers high durability, high availability, low latency, and high performance object storage for general purpose use. 99.99% availability, 99.999999999% durability, stored redundantly across multiple devices in multiple facilities and is designed to sustain the loss of 2 facilities concurrently.

S3 - IA (Infrequently Accessed) For data that is accessed less frequently, but requires rapid access when needed. Lower fee than S3, but you are charged a retrieval fee. Min Obj Size is 128Kb.

- Lower Price than S3 Standard
- Designed for storing less frequently accessed data.
- Minimum duration 30 days
- Retrieval charges applicable

Reduced Redundancy Storage - Designed to provide 99.99% durability and 99.99% availability of objects over a given year. It is most appropriate for derived data that can be easily reproduced, such as image thumbnails.

Glacier - Amazon Glacier is an extremely low-cost storage service that provides durable, secure, and flexible storage for data archiving and online backup. Storage class offers secure, durable, and extremely low-cost cloud storage for data that does not require real-time access, such as archives and long-term backups.

- **Archives:** In Amazon Glacier, data is stored in archives. An archive can contain up to 40TB of data, and you can have an unlimited number of archives.
- **Vaults:** Vaults are containers for archives. Each AWS account can have up to 1,000 vaults.
- After requesting for data three to five hours later, the Amazon Glacier object is copied to Amazon S3 RRS.
- Amazon Glacier allows you to retrieve up to 5% of the Amazon S3 data stored in Amazon Glacier for free each month.

Availability and Durability chart

Storage Class	Durability (designed for)	Availability (designed for)	Other Considerations
STANDARD	99.999999999%	99.99%	None
STANDARD_IA	99.999999999%	99.9%	There is a retrieval fee associated with STANDARD_IA objects which makes it most suitable for infrequently accessed data.
GLACIER	99.999999999%	99.99% (after you restore objects)	GLACIER objects are not available for real-time access. You must first restore archived objects before you can access them.
RRS	99.99%	99.99%	None

S3 Bucket Creation:

Create bucket

1 Name and region

2 Set properties

3 Set permissions

4 Review

Name and region

Bucket name ⓘ

Enter DNS-compliant bucket name

Region

Asia Pacific (Mumbai) ▾

Copy settings from an existing bucket

Select bucket (optional)

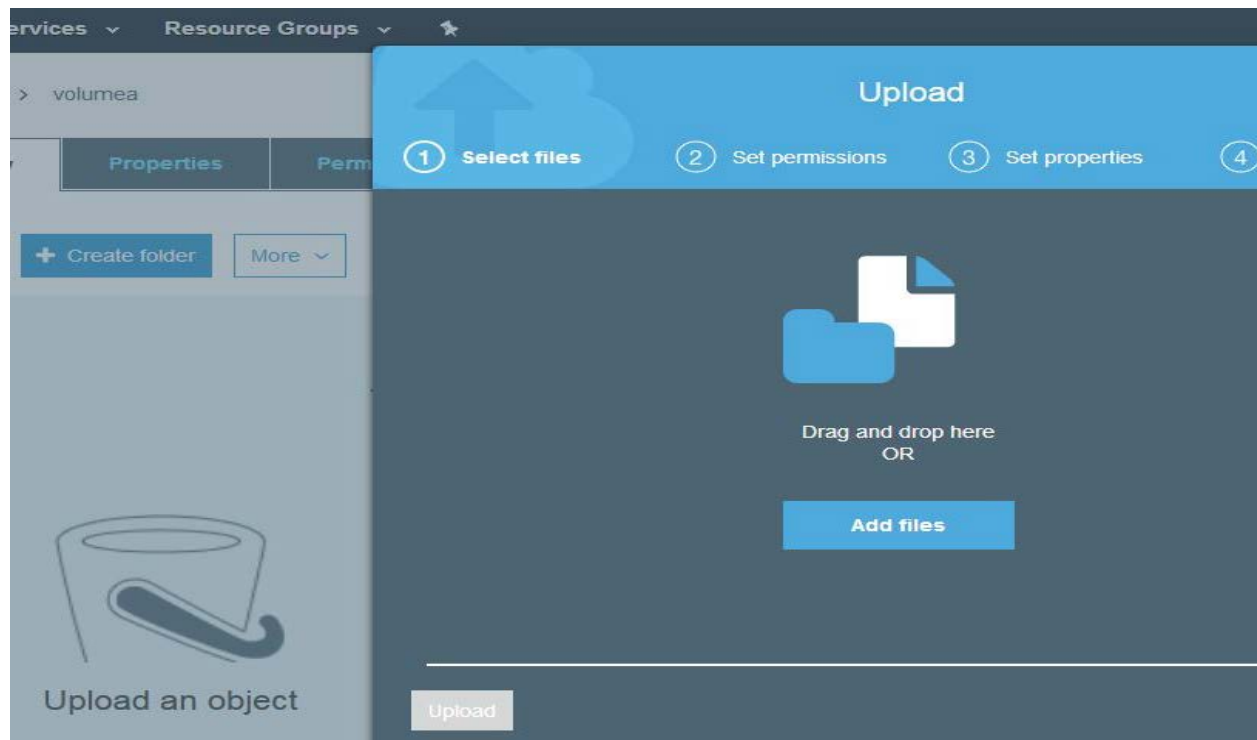
4 Buckets ▾

Create

Cancel

Next

- We can Drag & Drop objects to upload the objects.



- After selection of files, we can give access to other users who required permissions.
- We can Manage Public Permissions or give permissions for other AWS account users.

Upload

1 Select files 2 **Set permissions** 3 Set properties 4 Review

Manage users

User ID	Objects	Object permissions
(Owner)	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write

Access for other AWS account [+ Add account](#)

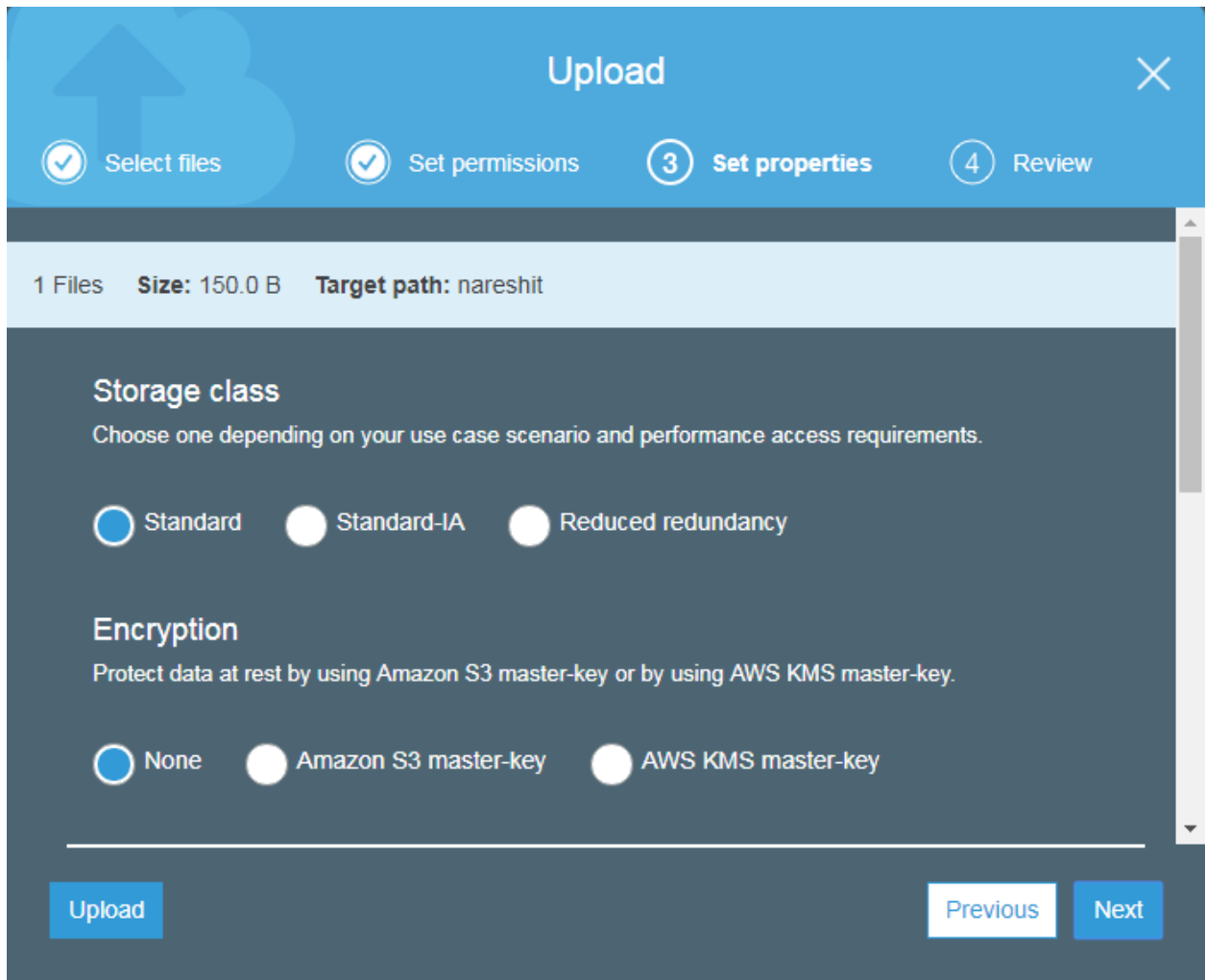
Account	Objects	Object permissions
---------	---------	--------------------

Manage public permissions

Do not grant public read access to this object(s) (Recommended)

[Upload](#) [Previous](#) [Next](#)

- Here we can select the object Properties, We can select the Object storage class of the object, Encryption methods, Metadata and tags for the object.



The screenshot shows the AWS S3 Upload console interface. At the top, there's a blue header with the word 'Upload' and a close button. Below the header, a progress bar shows four steps: 'Select files' (checked), 'Set permissions' (checked), 'Set properties' (active, highlighted with a blue circle and number 3), and 'Review' (numbered 4). Below the progress bar, a summary bar shows '1 Files', 'Size: 150.0 B', and 'Target path: nareshit'. The main content area is divided into two sections: 'Storage class' and 'Encryption'. The 'Storage class' section has a subtitle 'Choose one depending on your use case scenario and performance access requirements.' and three radio button options: 'Standard' (selected), 'Standard-IA', and 'Reduced redundancy'. The 'Encryption' section has a subtitle 'Protect data at rest by using Amazon S3 master-key or by using AWS KMS master-key.' and three radio button options: 'None' (selected), 'Amazon S3 master-key', and 'AWS KMS master-key'. At the bottom, there are three buttons: 'Upload' (blue), 'Previous' (white), and 'Next' (blue).

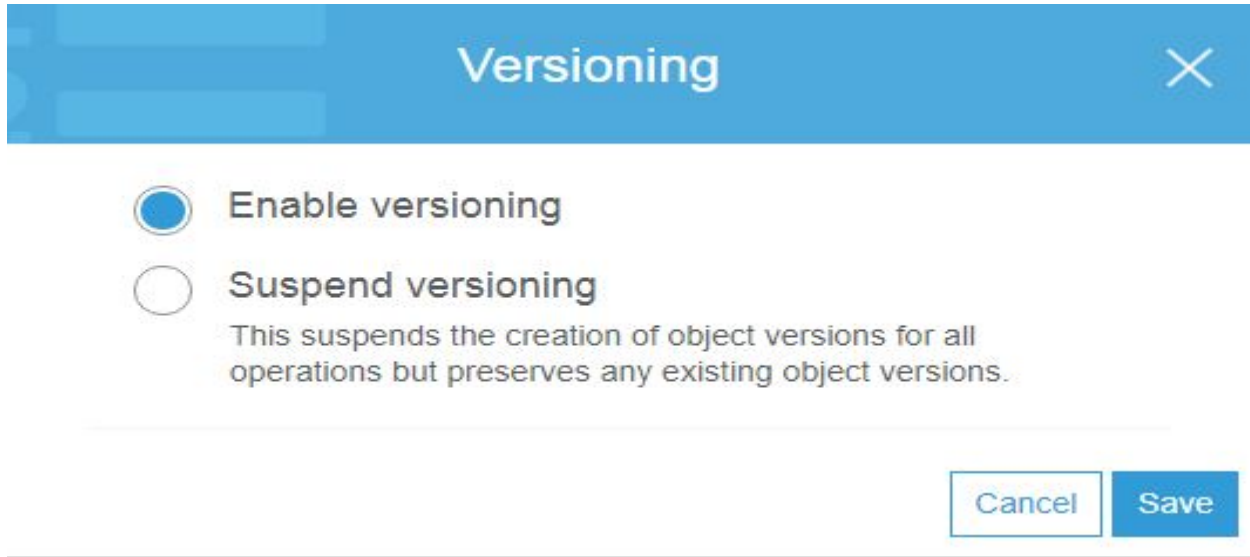
- Then we can review and click on upload option to upload the object into S3 bucket.

Versioning

Versioning helps protect your data against accidental or malicious deletion by keeping multiple versions of each object in the bucket, identified by a unique version ID.

- Versioning is turned on at the bucket level.
- Once enabled, versioning cannot be removed from a bucket; it can only be suspended.
- If you enable versioning you will get Current version files and previous version files in your bucket.
- If you delete current version file, it will overwrite with a Delete Marker, if you want to get that object back to your S3 bucket, you can delete the delete marker.

To enable versioning on bucket, navigate to properties of the respective bucket and select versioning and select “Enable versioning” option.



The screenshot shows the 'Versioning' configuration window for an Amazon S3 bucket. The window has a blue header with the title 'Versioning' and a close button (X). Below the header, there are two radio button options: 'Enable versioning' (which is selected) and 'Suspend versioning'. Under 'Suspend versioning', there is a descriptive text: 'This suspends the creation of object versions for all operations but preserves any existing object versions.' At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Lifecycle Management

By using Life cycle management we can automate the storage tiers in s3 buckets. We can move objects from one storage class/tier to another storage class/tier based on our business requirements.

Here is the possible scenarios:

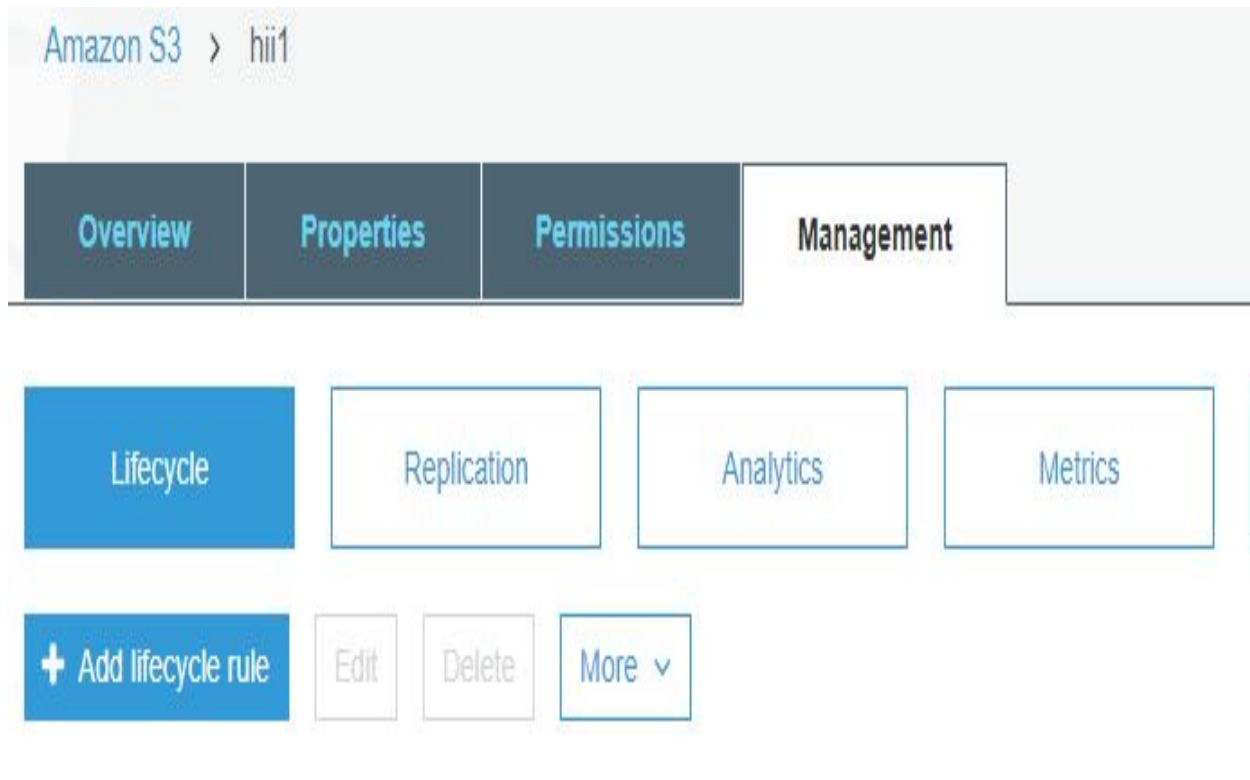
S3-Standard → S3-IA → Glacier → Delete

S3-Standard → Glacier → Delete

S3-Standard → Delete

Steps to enable lifecycle management rules:

- Select the S3 bucket which we want to add life cycle rule.
- Go to management option after selecting the bucket.



- Select Add Lifecycle rule and then give a valid name for the life cycle rule. We can add prefix, If LC rule will apply to the entire buckets objects.

The screenshot shows the 'Lifecycle rule' configuration dialog box. The title bar is blue with the text 'Lifecycle rule' and a close button (X). Below the title bar is a progress indicator with four steps: 1. Name and scope (active), 2. Transitions, 3. Expiration, and 4. Review. The main content area is dark blue. It starts with the text 'Enter a rule name' followed by a text input field containing the word 'cycle'. Below this is the text 'Add filter to limit scope to prefix/tags' with an information icon (i). Underneath is another text input field with the placeholder text 'Type to add prefix/tag filter'. At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Next'.

- After entering “name and scope” we need to configure the transitions. We can configure transitions for current version and previous versions. Click “add transition” and enter the days count from “Object creation”.

The screenshot shows the 'Lifecycle rule' configuration window in AWS. The top navigation bar has four steps: 1. Name and scope (checked), 2. Transitions (active), 3. Expiration, and 4. Review. The main section is titled 'Configure transition' with a help icon. Below this, there are two checkboxes: 'Current version' (checked) and 'Previous versions' (unchecked). Under the heading 'For current version of objects', there is a table with two columns: 'Object creation' and 'Days after object creation'. A '+ Add transition' link is present. One transition is configured: 'Transition to Standard-IA after' (selected from a dropdown) and '30' (entered in the days field). At the bottom right, there are 'Previous' and 'Next' buttons.

Object creation	Days after object creation
Transition to Standard-IA after	30

- For S3-IA We need to store the object for minimum of 30 days and for Glacier 60 days from object creation date.

Lifecycle rule

1 Name and scope 2 **Transitions** 3 Expiration 4 Review

For current version of objects

Object creation Days after object creation

+ Add transition

Transition to Standard-IA after 29 X

! A minimum of 30 days is required before transitioning to the Standard-IA storage class
Enter an integer value greater than or equal to 30.

Previous Next

- In Next step we can configure object expirations.
 - For current version Expiration creates a Delete Marker if Versioning is enabled on this bucket.
 - For Previous version object will delete permanently.

Lifecycle rule

1 Name and scope 2 Transitions 3 **Expiration** 4 Review

Configure expiration

☒ Current version ☐ Previous versions

☒ Expire current version of object **i**

After 395 days from object creation

Clean up expired object delete markers and incomplete multipart uploads

☐ Clean up expired object delete markers **i**

You cannot enable clean up expired object delete markers if you enable Expiration.

Previous Next

- This is the review status for the lifecycle rule that we have created. Review the Lifecycle rule and click on “Save”, Created lifecycle rule will apply on bucket.

Lifecycle rule

✓ Name and scope ✓ Transitions ✓ Expiration ④ Review

Name and scope [Edit](#)

Name cycle

Scope Whole bucket

Transitions [Edit](#)

For current version of objects

Transition to Standard-IA after 30 days

Expiration [Edit](#)

Expire after 395 days

Check rule **lifecycle**. It has prefix(es) that are overlapping.

[Previous](#) [Save](#)

Logging

By enabling logs we can track requests on our Amazon S3 bucket. Logging is off by default. You can enable it from bucket properties.

Every log will contains the below information

- Requestor account and IP address
- Bucket name
- Request time
- Action (GET, PUT, LIST, and so forth)
- Response status or error code

The screenshot shows the AWS S3 console interface for a bucket named 'volumea'. At the top, there are tabs for 'Properties', 'Permissions', and 'Management'. On the left, there is a 'Versioning' section with a description and a 'Learn more' link. The main area is titled 'Logging' and contains two radio buttons: 'Enable logging' (selected) and 'Disable logging'. Below the 'Enable logging' option, there is a 'Target bucket' dropdown menu set to 'volumea' and a 'Target prefix' text input field with the placeholder 'Enter target prefix'. An information icon is next to the input field. A 'Cancel' button is located at the bottom right of the logging configuration area.

Cross-Region Replication:

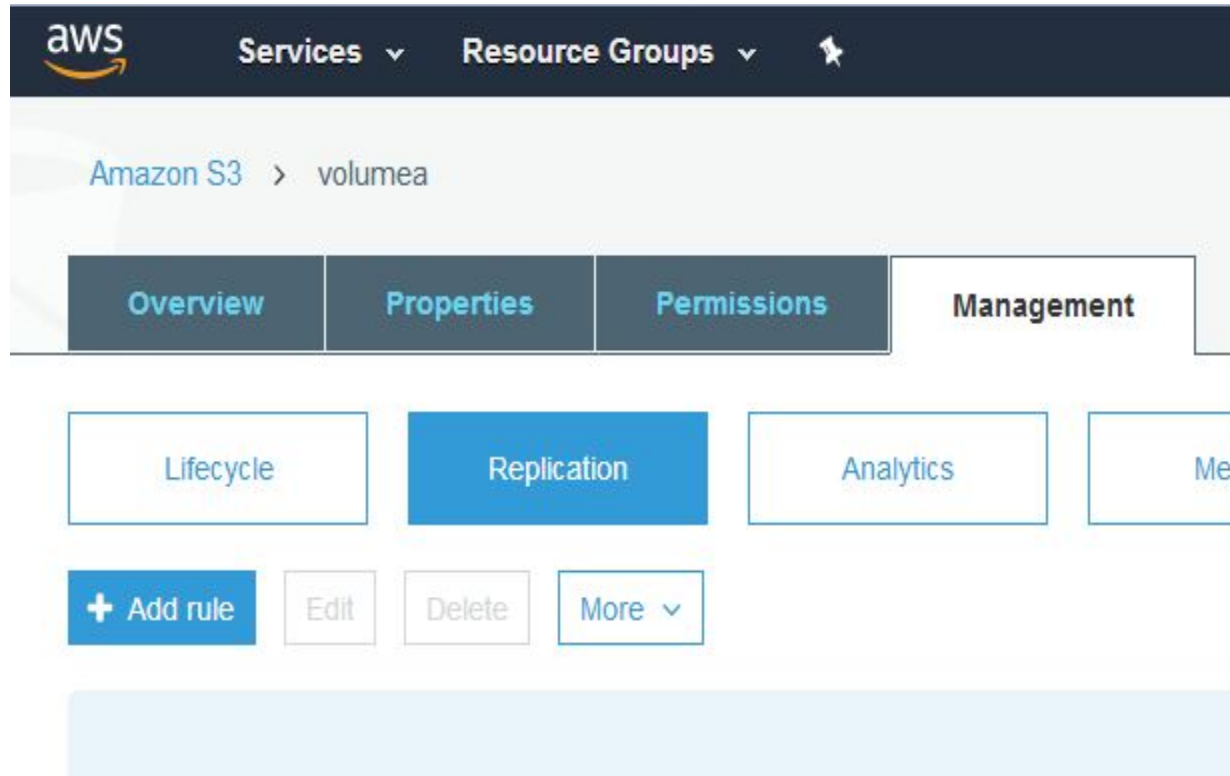
With Cross-region replication Amazon S3 allows you to asynchronously replicate all new objects in the source bucket in one AWS region to a target bucket in another region.

- Versioning must be enabled on both the source and destination buckets.
- Regions must be unique
- Files in an existing bucket are not replicated automatically. All subsequent/future updated files will be replicated automatically.
- You cannot replicate to multiple buckets or use daisy chaining (at this time).
- Delete markers are replicated.
- Deleting individual versions or delete markers will not be replicated.
- Cross-region replication is used to reduce the latency required to access objects in Amazon S3 by placing objects closer to a set of users or to meet requirements to store backup data at a certain distance from the original source data.
- Amazon S3 must have permission to replicate objects from that source bucket to the destination bucket on your behalf.

- You can grant these permissions by creating an IAM role that Amazon S3 can assume.

Steps to enable cross region replication:

- Select S3 bucket that you want to replicate, Select Replication option under Management.




- We can replicate the entire bucket or we can use particular prefixes (i.e; all objects that have names that begin with the string pictures)

The screenshot shows the 'Replication rule' configuration page in the AWS IAM console. The page has a blue header with the title 'Replication rule' and a navigation bar with four steps: 1 Source, 2 Destination, 3 Permissions, and 4 Review. The 'Source' step is currently active. Below the header, there are two sections: 'Source' and 'Status'. In the 'Source' section, there are two radio button options: 'All contents in' (selected) and 'Prefix in this bucket'. In the 'Status' section, there are two radio button options: 'Enabled' (selected) and 'Disabled'. At the bottom right, there are 'Cancel' and 'Next' buttons.

Replication rule

1 Source 2 Destination 3 Permissions 4 Review

Source

☒ All contents in  volumea

☐ Prefix in this bucket

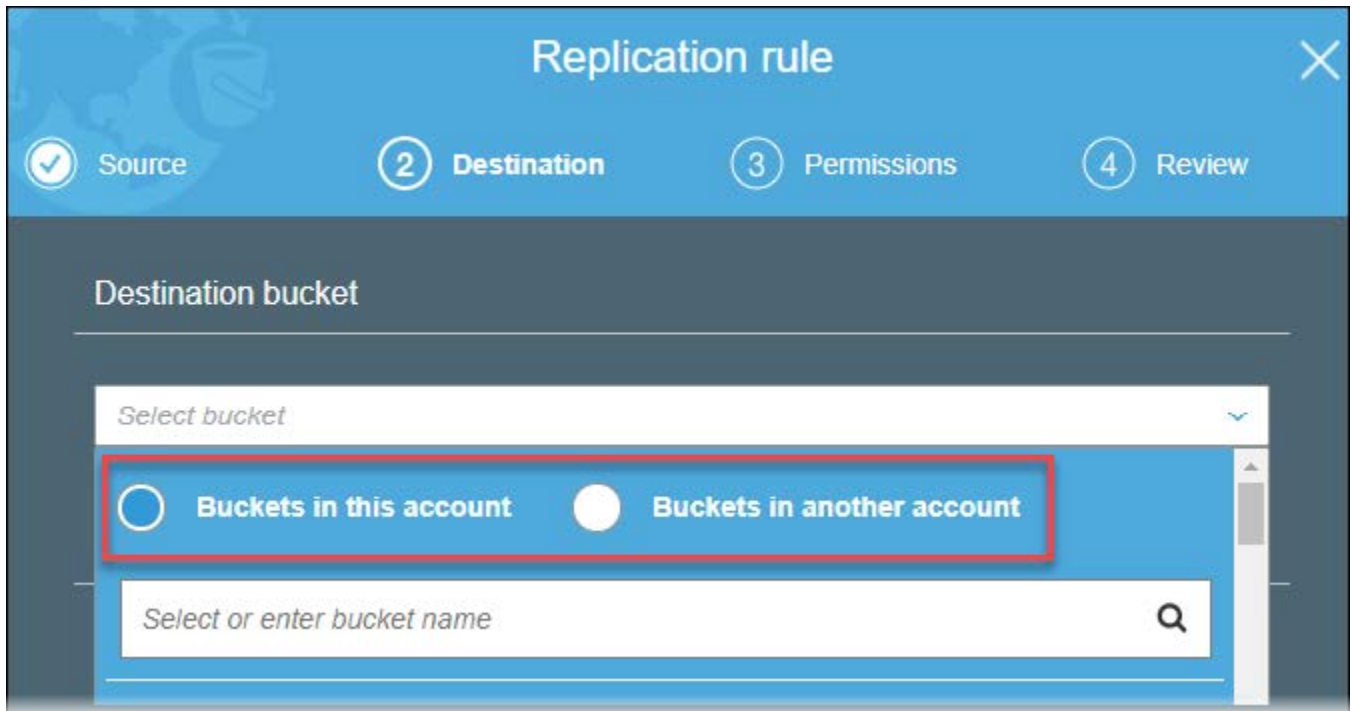
Status

☒ Enabled

☐ Disabled

Cancel Next

- On the **Destination** tab, under **Destination bucket**, select destination bucket for the replication. You can choose a destination bucket from same account or we can choose to create new bucket, or else we can replicate the data to a destination bucket from a different AWS account.



Replication rule

1 Source 2 **Destination** 3 Permissions 4 Review

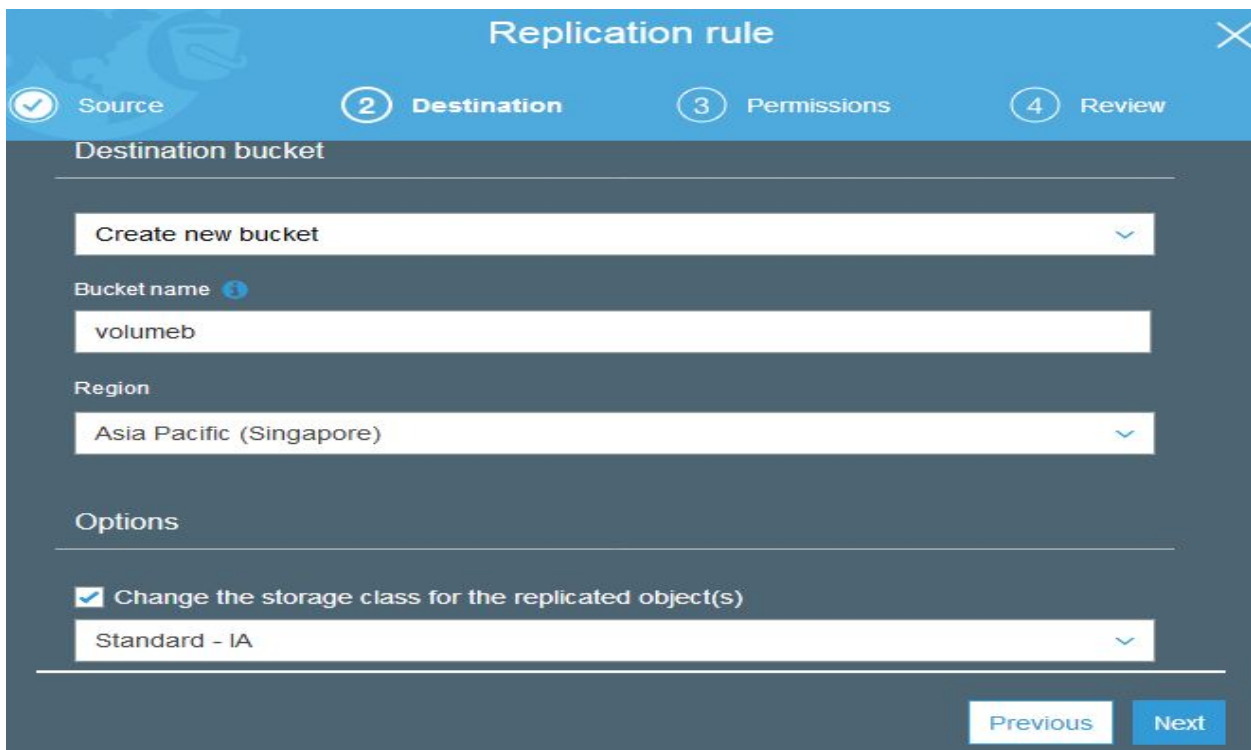
Destination bucket

Select bucket

☒ Buckets in this account ☐ Buckets in another account

Select or enter bucket name

- Give a valid name for the replication rule
- We can change the object storage class for the destination bucket, if required.



Replication rule

1 Source 2 **Destination** 3 Permissions 4 Review

Destination bucket

Create new bucket

Bucket name ⓘ
volumeb

Region
Asia Pacific (Singapore)

Options

☒ Change the storage class for the replicated object(s)

Standard - IA

Previous Next

- We have to create an IAM role for replication. Role is “s3crr_role_for_source_to_destination”

Replication rule

Source Destination 3 Permissions 4 Review

Select IAM role

Create new role

Previous Next

- Review and click on save to activate the cross region replication on the bucket.

Replication rule

Source Destination Permissions 4 Review

Source Edit

Bucket volumea

All the objects in the bucket

Region Asia Pacific (Mumbai)

Status Enabled

Destination Edit

Bucket volumeb

Region Asia Pacific (Singapore)

Storage class Standard - IA

Permissions Edit

Previous Save

- After you save your rule, you can edit, enable, disable, or delete your rule on the **Replication** page.

Amazon S3 > volumea

Overview Properties Permissions Management

Lifecycle Replication Analytics Metrics Inventory

Source	Destination	Permissions
Scope	Bucket	IAM role
All contents in the bucket	volumeb	s3crr_role_for_volumea_to_volumeb
Region	Region	Bucket policy
Asia Pacific (Mumbai)	Asia Pacific (Singapore)	Copy

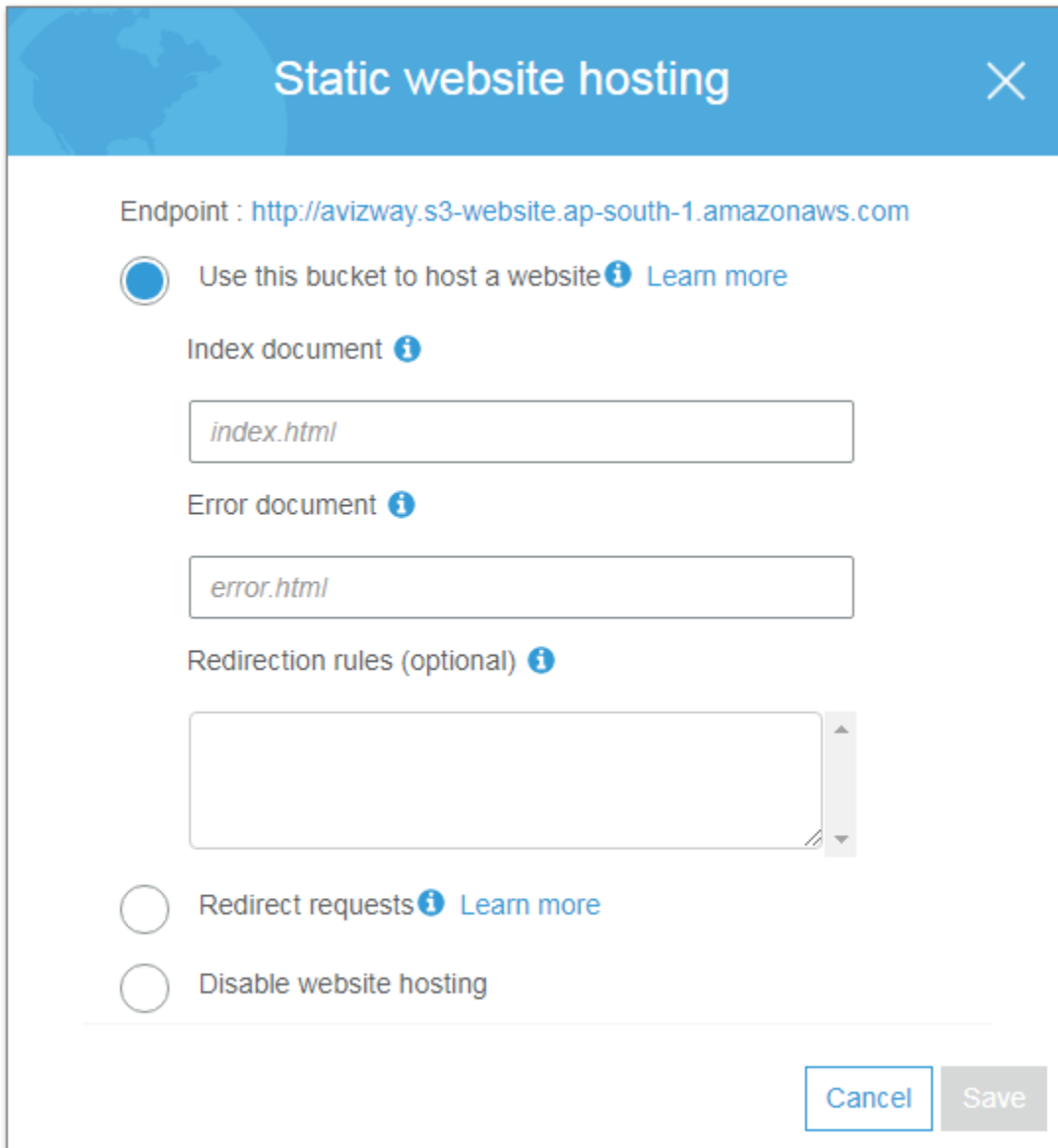
+ Add rule Edit Delete More ▾

Source ⓘ	Status ⓘ	Storage Class ⓘ
<input type="radio"/> Entire bucket	Enabled	Standard - IA

Static Website Hosting

We can host a static website on Amazon Simple Storage Service.

- We need to create a bucket with the same name as the desired website hostname.
- Upload the static files to the bucket (Index.html and error.html).
- Make all the files public, then only website will be readable for all the world.
- Go to Properties of the bucket and Enable static website hosting for the bucket. And mention the specifying an Index.html and an Error.html.
- The website will now be available at the S3 website URL: <bucket-name>.s3-website-<AWS-region>.amazonaws.com.
- We have to create a DNS record in Route53 with purchased Domain name, then all the requests to the domain name will point to S3 bucket.
- If required, We can redirect the requests to another bucket also.



The image shows a 'Static website hosting' configuration window. At the top, there's a blue header with the title 'Static website hosting' and a close button (X). Below the header, the 'Endpoint' is displayed as 'http://avizway.s3-website.ap-south-1.amazonaws.com'. The main configuration area has three sections: 1. 'Use this bucket to host a website' (selected with a radio button), with a 'Learn more' link. 2. 'Index document' (with an info icon), with a text input field containing 'index.html'. 3. 'Error document' (with an info icon), with a text input field containing 'error.html'. Below these is a 'Redirection rules (optional)' section (with an info icon) containing an empty text area with a scrollbar. At the bottom, there are two radio button options: 'Redirect requests' (with an info icon and 'Learn more' link) and 'Disable website hosting'. In the bottom right corner, there are 'Cancel' and 'Save' buttons.

Static website hosting

Endpoint : <http://avizway.s3-website.ap-south-1.amazonaws.com>

☒ Use this bucket to host a website [Learn more](#)

Index document [i](#)

Error document [i](#)

Redirection rules (optional) [i](#)

☐ Redirect requests [Learn more](#)

☐ Disable website hosting

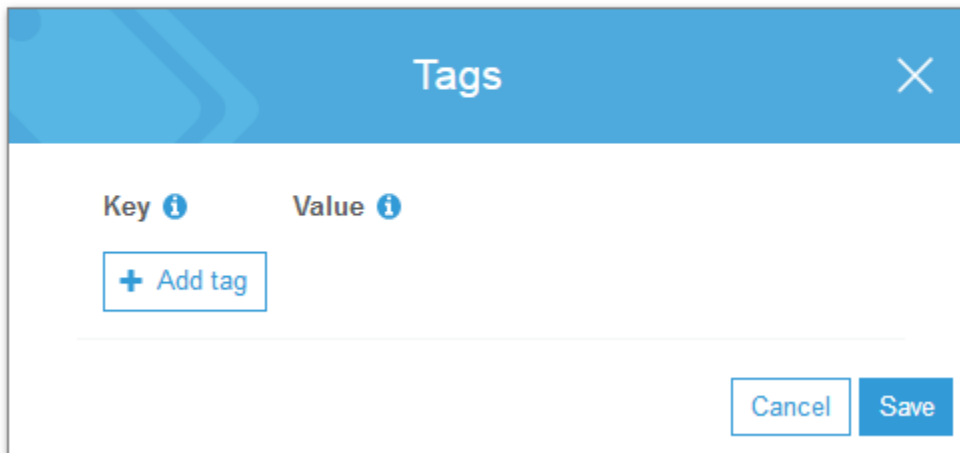
Cancel Save

Tags:

Tags are combination of keys & values. Each tag is a simple label consisting of a customer-defined key and an optional value that can make it easier to manage, search for, and filter resources.

We can add tags under S3 bucket properties tab.

Advanced settings



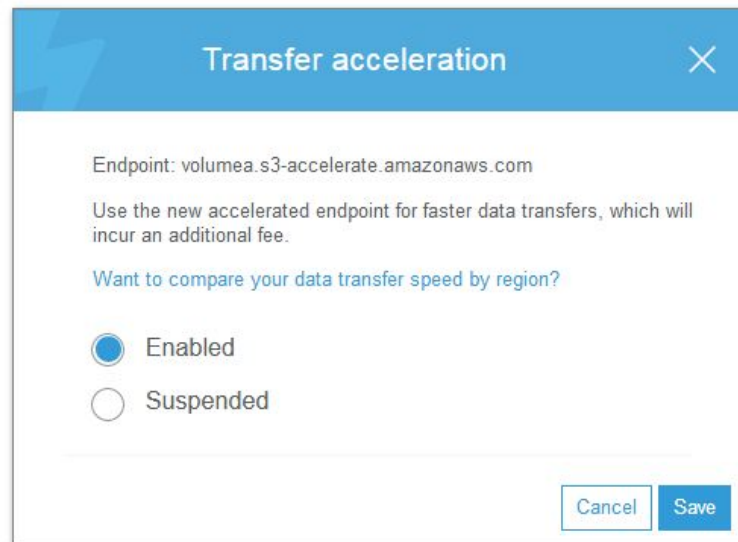
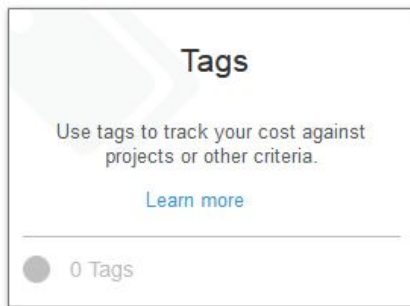
Amazon S3 Transfer Acceleration:

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. Additional data transfer charges will apply for this tool.

- **By Using the Amazon S3 Transfer Acceleration Speed Comparison Tool we can compare the** accelerated and non-accelerated upload speeds across Amazon S3 regions.
- The Speed Comparison tool uses multipart uploads to transfer a file from your browser to various Amazon S3 regions with and without using Transfer Acceleration.

You can enable the Transfer acceleration option under S3 Bucket Properties.

Advanced settings



Here is a sample result for Transfer acceleration result.



Amazon S3 Transfer Acceleration Speed Comparison

Upload speed comparison in the selected region
(Based on the location of bucket: avizway)

Mumbai
(AP-SOUTH-1)

1% slower

S3 Direct Upload Speed



Upload complete

S3 Accelerated Transfer Upload Speed

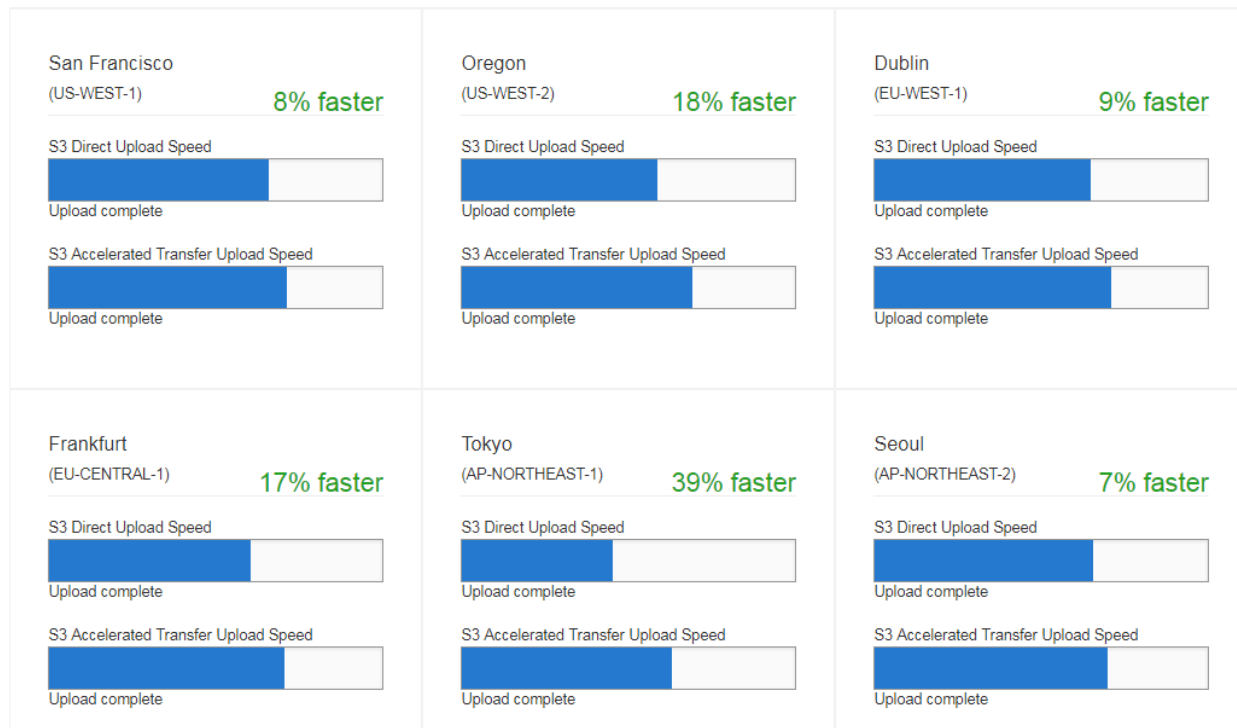


Upload complete

This speed comparison shows the time taken to transfer a file to Amazon S3 using S3 Transfer Acceleration compared to the standard S3 Transfer. The speed result difference is 1% slower.

Note: In general, using Amazon S3 Transfer Acceleration from an Amazon S3 bucket can improve upload speed. However, you see similar results when the acceleration system considers the speed.

Upload speed comparison in other regions



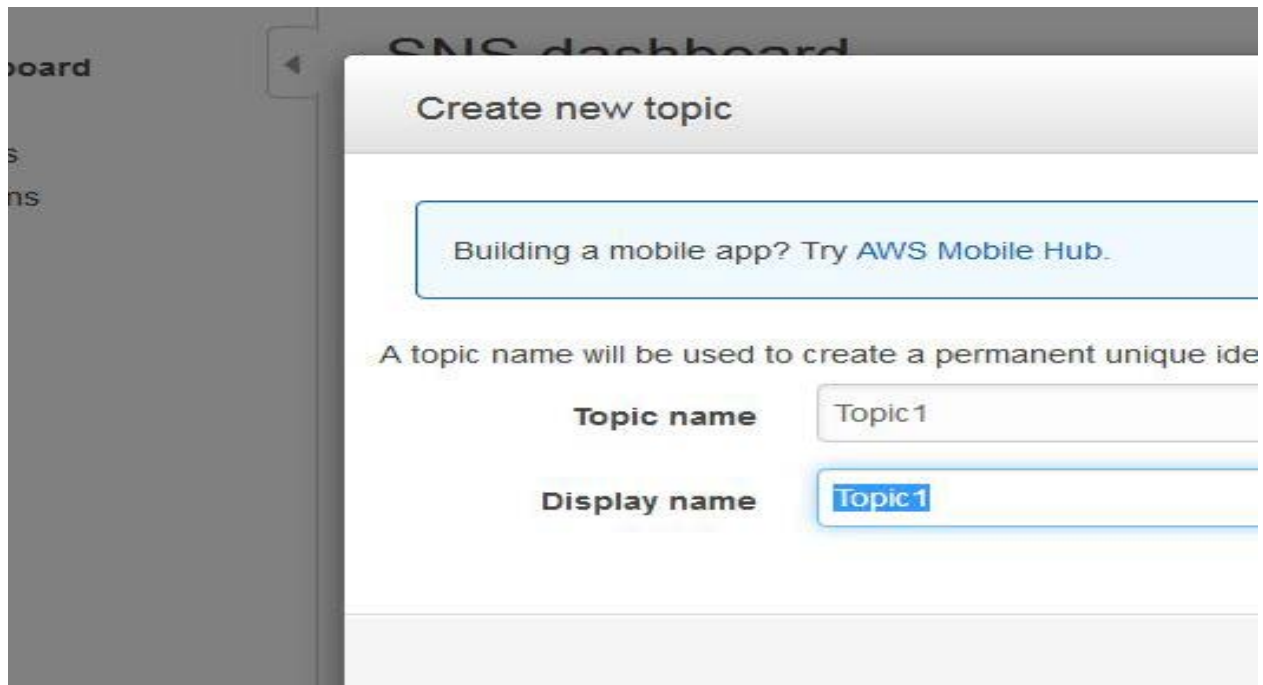
Events

Amazon S3 event notifications can be sent in response to actions taken on objects uploaded or stored in Amazon S3. The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket.

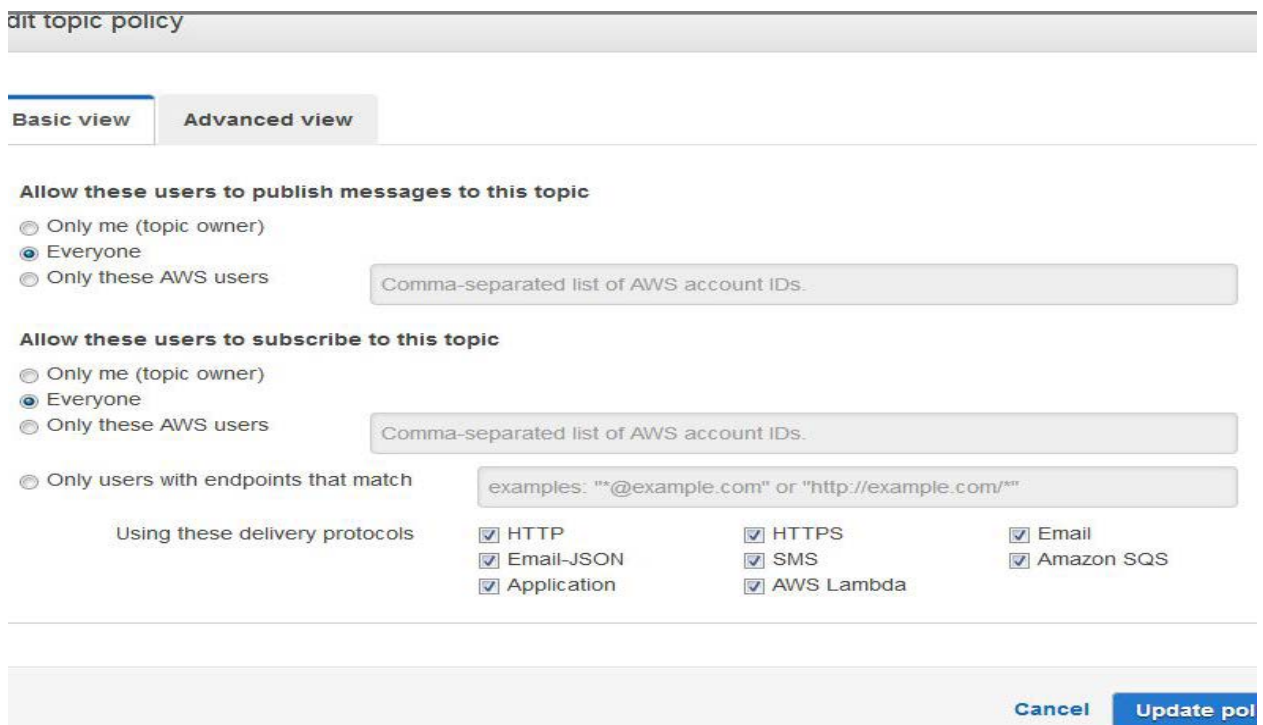
- Notification messages can be sent through either Amazon Simple Notification Service or Amazon Simple Queue Service or delivered directly to AWS Lambda to invoke AWS Lambda functions.

Here is an example to enable Notifications through SNS

- To set event notifications via SNS, Go to services → Messaging → SNS. In SNS dashboard, we have to create topic.



After creating topic, we have to update the topic policy. Next we can give email id for subscription of notifications. Once we select confirm option from email id then that email got subscribed for event notifications



- Now Go to Properties of S3 bucket and select **Events** → Add notification → give event name → select Events → select SNS topic and select save option.

- We can select the Event type to get notified through the Email.

The screenshot shows the 'Event Notification' configuration page for an Amazon S3 bucket. It includes the following sections:

- Name**: A text input field containing 'S3 events'.
- Events**: A list of event types with checkboxes:
 - ☐ RRSObjectLost
 - ☐ Put
 - ☐ Post
 - ☐ Copy
 - ☐ Complete Multipart Upload
 - ☐ Delete
 - ☐ Delete Marker Created
 - ☒ ObjectCreate (All)
 - ☒ ObjectDelete (All)
- Prefix**: A text input field with placeholder text 'e.g. images/'.
- Suffix**: A text input field with placeholder text 'e.g. .jpg'.
- Send to**: A section for configuring email notifications, partially visible at the bottom.

- When the selected action performed on S3 bucket, Subscribed users to that topic will get a notification.

Inventory:

Amazon S3 inventory is one of the tools Amazon S3 provides to help manage your storage. Amazon S3 inventory provides a comma-separated values (CSV) flat-file output of your objects and their corresponding metadata on a daily or weekly basis for an S3 bucket or a shared prefix.

Requester pays

Generally, bucket owners pay for all Amazon S3 storage and data transfer costs associated with their bucket. If you enable Requester pays on the bucket, instead of bucket owner requested user will pay.

- anonymous access to that bucket is not allowed, if we want to enable the requester pays on bucket.

Encryption:

We have three types of encryptions available in S3

1. Server-Side Encryption: All SSE performed by Amazon S3 and AWS Key Management Service (Amazon KMS) uses the 256-bit Advanced Encryption Standard (AES).
 - SSE-S3 (AWS-Managed Keys)
 - SSE-KMS (AWS KMS Keys)
 - SSE-C (Customer-Provided Keys)
2. Client-Side Encryption: We can encrypt the data on the client before sending it to Amazon S3. We have to take care about the encryption and Decryption process.
3. In-Transit Encryption
 - We can use SSL API endpoints, this ensures that all data sent to and from Amazon S3 is encrypted while in transit using the HTTPS protocol.