

S3 Simple storage service – it is unlimited storage service (global service)

S3 simple storage service it is unlimited storage service

EBS elastic block storage – region specific, 16tb block level storage instance level

S3 simple storage service – global specific, unlimited it is object level, scalability and security

s3 keypoints

- * it giving 99.99% availability**
- * it giving 99.999999999% durability**
- * bucket level propertise**
- * object level properties**
- * storage class - 7 types**

Bucket 100 per account objects unlimited

(*) create bucket

(*) Object ownership

(*)

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

aws1434

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Asia Pacific (Singapore) ap-southeast-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Object Ownership [Info](#)


Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☐ ACLs disabled (recommended)

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☒ ACLs enabled

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

 We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.


Object Ownership

☒ Bucket owner preferred

If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☐ Object writer

The object writer remains the object owner.

 If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)




Upcoming permission changes to enable ACLs

Starting in April 2023, to enable ACLs when creating buckets by using the S3 console, you must have the `s3:PutBucketOwnershipControls` permission. [Learn more](#)

(*) remove 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.




Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☐ I acknowledge that the current settings might result in this bucket and the objects within becoming public.



Upcoming permission changes to disable any Block Public Access setting

Starting in April 2023, to disable any Block Public Access setting when creating buckets by using the S3 console, you must have the `s3:PutBucketPublicAccessBlock` permission. [Learn more](#) 

(*) bucket versioning enable

(*) default encryption disable

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☐ Disable

☒ Enable

Tags (0) - optional

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add tag](#)

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type [Info](#)

☒ Amazon S3 managed keys (SSE-S3)

☐ AWS Key Management Service key (SSE-KMS)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

☐ Disable

☒ Enable

(*) advance setting object lock disabled

▼ Advanced settings

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)

☒ Disable

☐ Enable

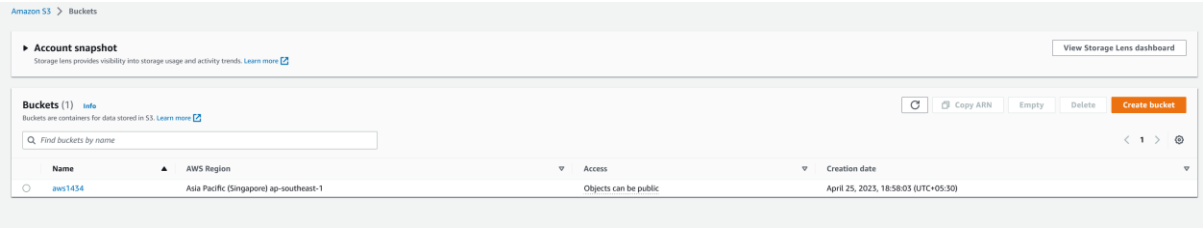
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

[Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.](#)

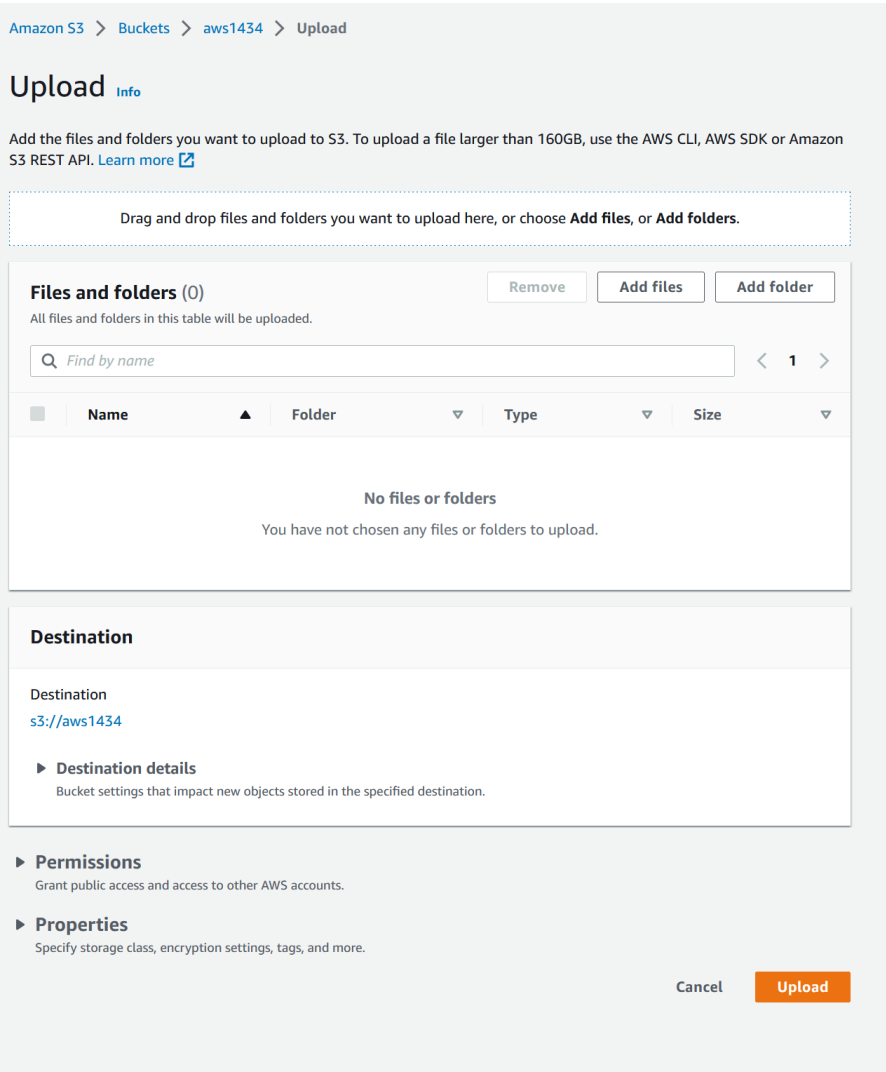
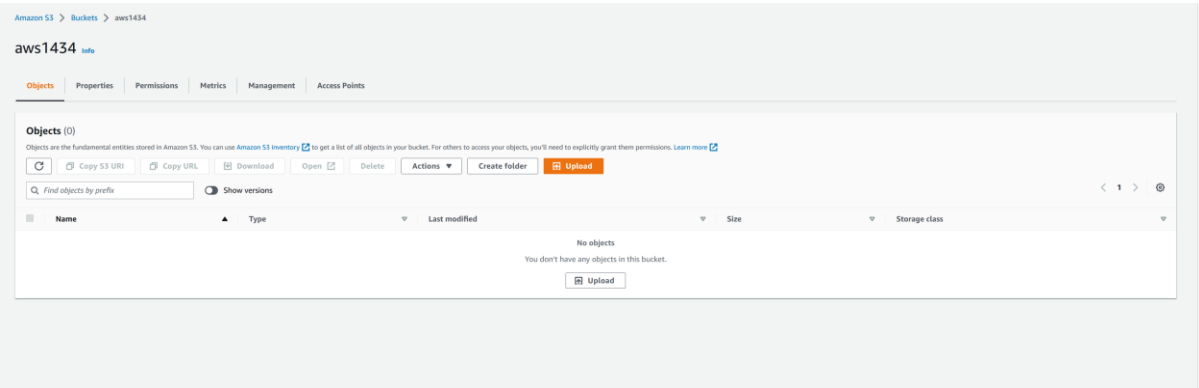
[After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.](#)

[Cancel](#) [Create bucket](#)

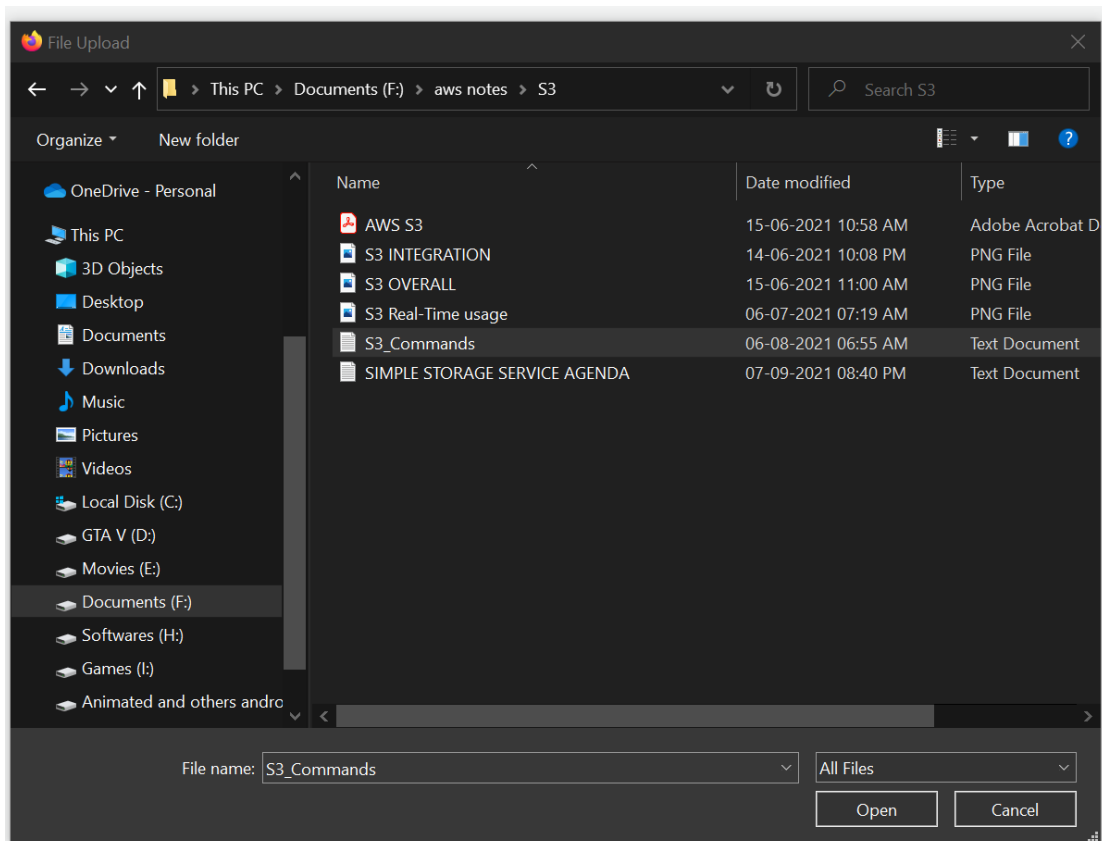
(*) bucket created



(*) upload objects



(*) add files from computer



Files and folders (1 Total, 4.7 KB)

RemoveAdd filesAdd folder

All files and folders in this table will be uploaded.

< 1 >


<input type="checkbox"/>	Name▲	Folder▼	Type▼	Size▼
<input type="checkbox"/>	S3_Commands.txt	-	text/plain	4.7 KB



(*) permissions

▼ Permissions

Grant public access and access to other AWS accounts.




Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#) 

 AWS recommends using S3 bucket policies or IAM policies for access control. [Learn more](#) 

Access control list (ACL)

- ☐ Choose from predefined ACLs
- ☒ Specify individual ACL permissions

Grantee	Objects	Object ACL
Object owner (your AWS account) Canonical ID:  72fef970a927c2705f89cab616b842d9b0651eff8a1b8a357a4e642a088e49bc	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group:  http://acs.amazonaws.com/groups/global/AllUsers	<input type="checkbox"/> Read	<input type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group:  http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> Read	<input type="checkbox"/> Read <input type="checkbox"/> Write

Access for other AWS accounts

No other AWS accounts associated with the resource.

Add grantee

(*) grant public read access

Access control list (ACL)

- ☒ Choose from predefined ACLs
- ☐ Specify individual ACL permissions

Predefined ACLs

- ☐ Private (recommended)
Only the object owner will have read and write access.
- ☒ Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. [Learn more](#)



Granting public-read access is not recommended
Anyone in the world will be able to access the specified objects. [Learn more](#)

☐ I understand the risk of granting public-read access to the specified objects.

(*) properties 7 properties

▼ Properties

Specify storage class, encryption settings, tags, and more.

Storage class

Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

	Storage class	Designed for	Availability Zones	Min storage duration	M
<input checked="" type="radio"/>	Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-	-
<input type="radio"/>	Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-	-
<input type="radio"/>	Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days	1
<input type="radio"/>	One Zone-IA	Recreatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days	1
<input type="radio"/>	Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	≥ 3	90 days	1
<input type="radio"/>	Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	≥ 3	90 days	-
<input type="radio"/>	Glacier Deep Archive	Long-lived archive data accessed less than once a year with retrieval of hours	≥ 3	180 days	-
<input type="radio"/>	Reduced redundancy	Noncritical, frequently accessed data with milliseconds access (not recommended as S3 Standard is more cost effective)	≥ 3	-	-

(*) s3 standard pricing

Region: Asia Pacific (Singapore) +

Storage pricing	
S3 Standard - General purpose storage for any type of data, typically used for frequently accessed data	
First 50 TB / Month	\$0.025 per GB
Next 450 TB / Month	\$0.024 per GB
Over 500 TB / Month	\$0.023 per GB

(*) upload

Additional checksums

Checksum functions are used for additional data integrity verification of new objects. [Learn more](#)

Additional checksums

- ☒ **Off**
Amazon S3 will use a combination of MD5 checksums and Etags to verify data integrity.
- ☐ **On**
Specify a checksum function for additional data integrity validation.

Tags - optional

You can use object tags to analyze, manage, and specify permissions for objects. [Learn more](#)

No tags associated with this resource.

Add tag

Metadata - optional

Metadata is optional information provided as a name-value (key-value) pair. [Learn more](#)

No metadata associated with this resource.

Add metadata

Cancel

Upload

(*) upload status

Upload: status

Close

The information below will no longer be available after you navigate away from this page.

Summary

Destination

s3://aws1434

Succeeded

1 file, 4.7 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 4.7 KB)

Find by name

Name

Folder

Type

Size

Status

Error

s3_Commands.txt

-

text/plain

4.7 KB

Succeeded

-

(*) copy URL PASTE in browser

Amazon S3 > Buckets > aws1434

aws1434

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

Objects are the fundamental entity.

Object URL Copied

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

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

Show versions

Name

Type

Last modified

Size

Storage class

s3_Commands.txt

txt

April 25, 2023, 19:36:13 (UTC+05:30)

4.7 KB

Standard

(*) create lifecycle rule

Amazon S3 > Buckets > aws1434

aws1434

Objects

Properties

Permissions

Metrics

Management

Access Points

Lifecycle rules (0)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. Learn more

View details

Edit

Delete

Actions

Create lifecycle rule

Lifecycle rule name

Status

Scope

Current version actions

Noncurrent versions actions

Expired object delete markers

Incomplete multipart uploads

No lifecycle rules

There are no lifecycle rules for this bucket.

Create lifecycle rule

Replication rules (0)

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transmitting replicas to another storage class, and more. Learn more

View details

Edit rule

Delete

Actions

Create replication rule

Replication rule name

Status

Destination bucket

Destination Region

Priority

Scope

Storage class

Replica owner

Replication Time Control

KMS-encrypted objects

Replica modification sync

No replication rules

You don't have any rules in the replication configuration.

Create replication rule

Inventory configurations (0)

You can create inventory configurations on a bucket to generate a flat file list of your objects and metadata. These scheduled reports can include all objects in the bucket or be limited to a shared prefix. Learn more

View details

Edit

Delete

Create job from manifest

Create inventory configuration

Name

Status

Scope

Destination

Frequency

Last export

Format

No configurations

No configurations to display

Create inventory configuration

(*) properties – intelligent archive configuration

Intelligent-Tiering Archive configurations (0)

Intelligent objects stored in the Intelligent-Tiering storage class can be tiered down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. Learn more

View details

Edit

Delete

Create configuration

Find Intelligent-Tiering Archive configurations

Name

Status

Scope

Days until transition to Archive Access tier

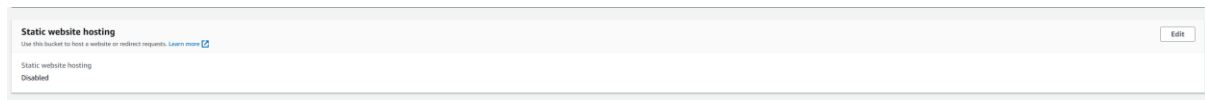
Days until transition to Deep Archive Access tier

No archive configurations

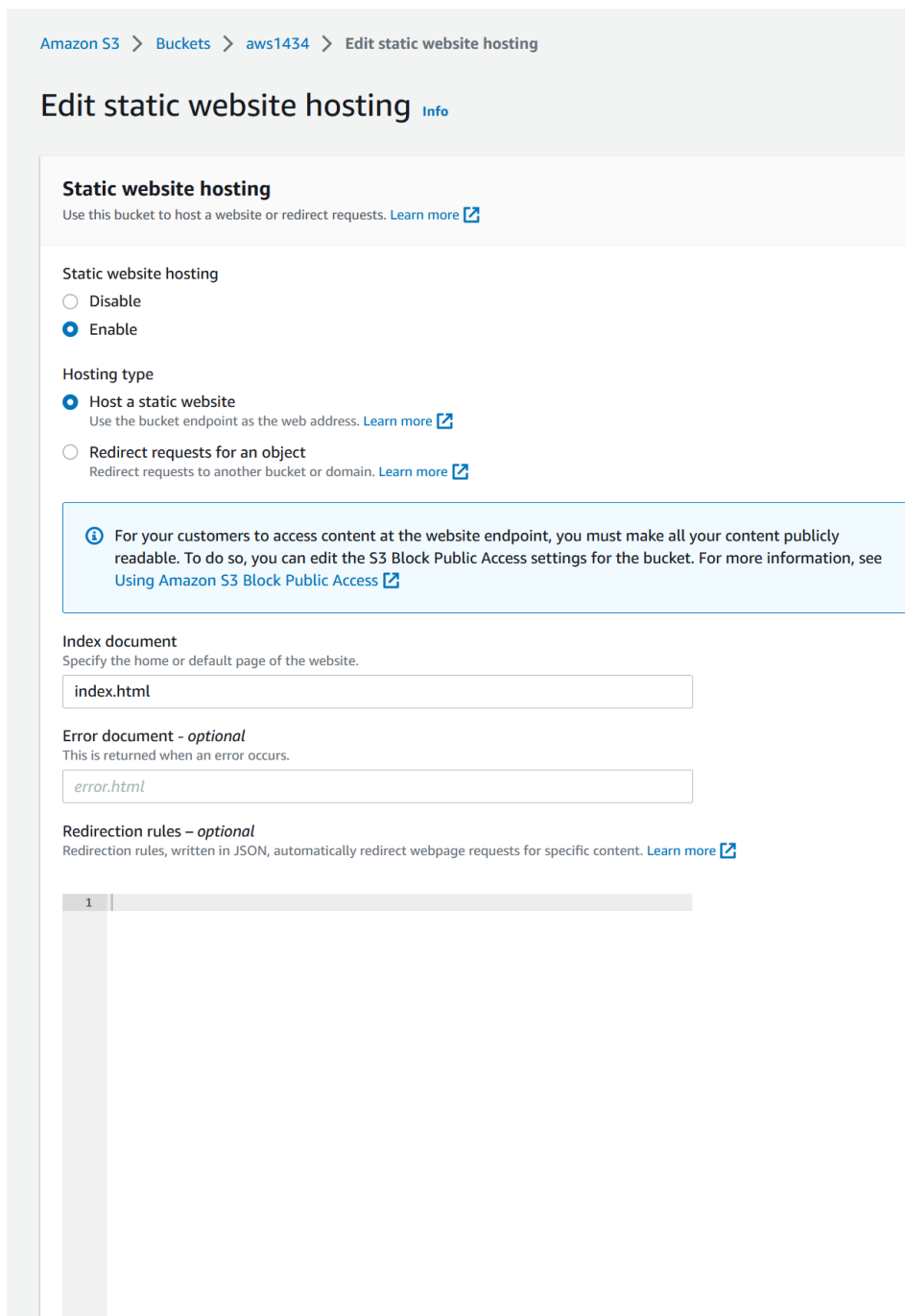
No configurations to display

Create configuration

- (*) Upload an object into the bucket
- (*) then go to static website hosting press edit



- (*) go to static website hosting enable
- (*) index document index.html



(*) static website hosting URL

Static website hosting

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

Static website hosting

Enabled

Hosting type

Bucket hosting

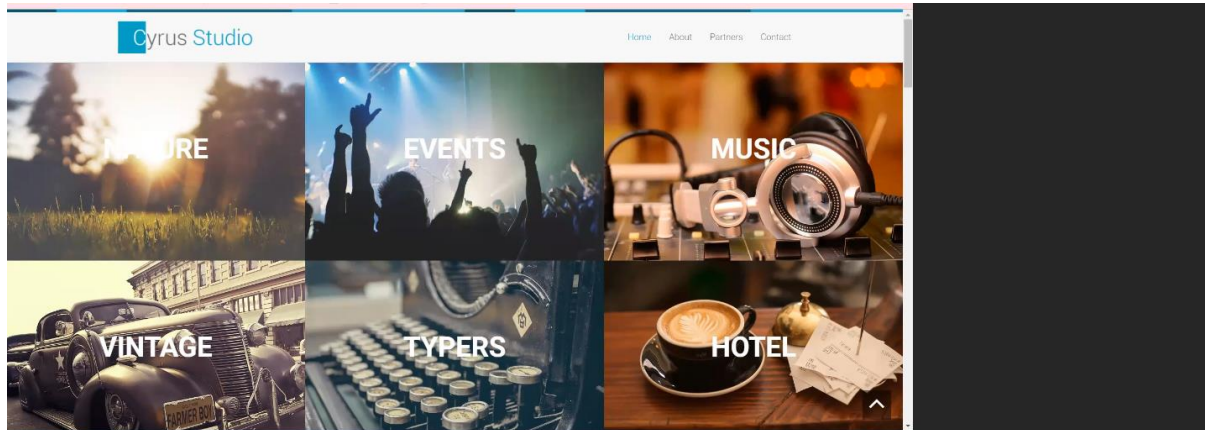
Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

<http://aws1434-s3-website-ap-southeast-1.amazonaws.com>

Edit

(*) copy paste the url in browser index.html



(*) if a source file is deleted

Amazon S3 > Buckets > aws1434 > Delete objects

Delete objects [Info](#)

⚠

- If a folder is selected for deletion, all objects in the folder will be deleted, and any new objects added while the delete action is in progress might also be deleted. If an object is selected for deletion, any new objects with the same name that are uploaded before the delete action is completed will also be deleted.
- Deleting the specified objects can't be undone.

[Learn more](#)

Specified objects

< 1 >

Name	Version ID	Type	Last modified	Size
S3_Commands.txt	7f7otz2gRhPvjp6kR9UL1xjRB7k7QXnE	txt	April 25, 2023, 19:36:13 (UTC+05:30)	4.7 KB

Permanently delete objects?

To confirm deletion, type *permanently delete* in the text input field.

delete

Cancel Delete objects

(*) click on show versions

(*) delete marker -- delete

Objects (4)

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](#)

↻

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

Show versions

< 1 > ⚙

<input type="checkbox"/>	Name	Type	Version ID	Last modified	Size	Storage class
<input type="checkbox"/>	cyrus/	Folder	-	-	-	-
<input type="checkbox"/>	EC2 APPLICATION HOSTING PAINT.png	png	vzN4rtjh8sagJ1ZvMGqrOZZ_z72XriJr	April 17, 2023, 11:14:34 (UTC+05:30)	6.1 KB	Standard
<input checked="" type="checkbox"/>	EC2 APPLICATION HOSTING PAINT.png	Delete marker	jBOHOqudHLajg_nzNAB8fOmOy_d0gB8D	April 17, 2023, 11:14:09 (UTC+05:30)	0 B	-
<input type="checkbox"/>	EC2 APPLICATION HOSTING PAINT.png	png	CYFvFa_d_SCH5tAADzYNXLLTzuutisG2	April 17, 2023, 11:13:54 (UTC+05:30)	6.1 KB	Glacier Instant Retrieval