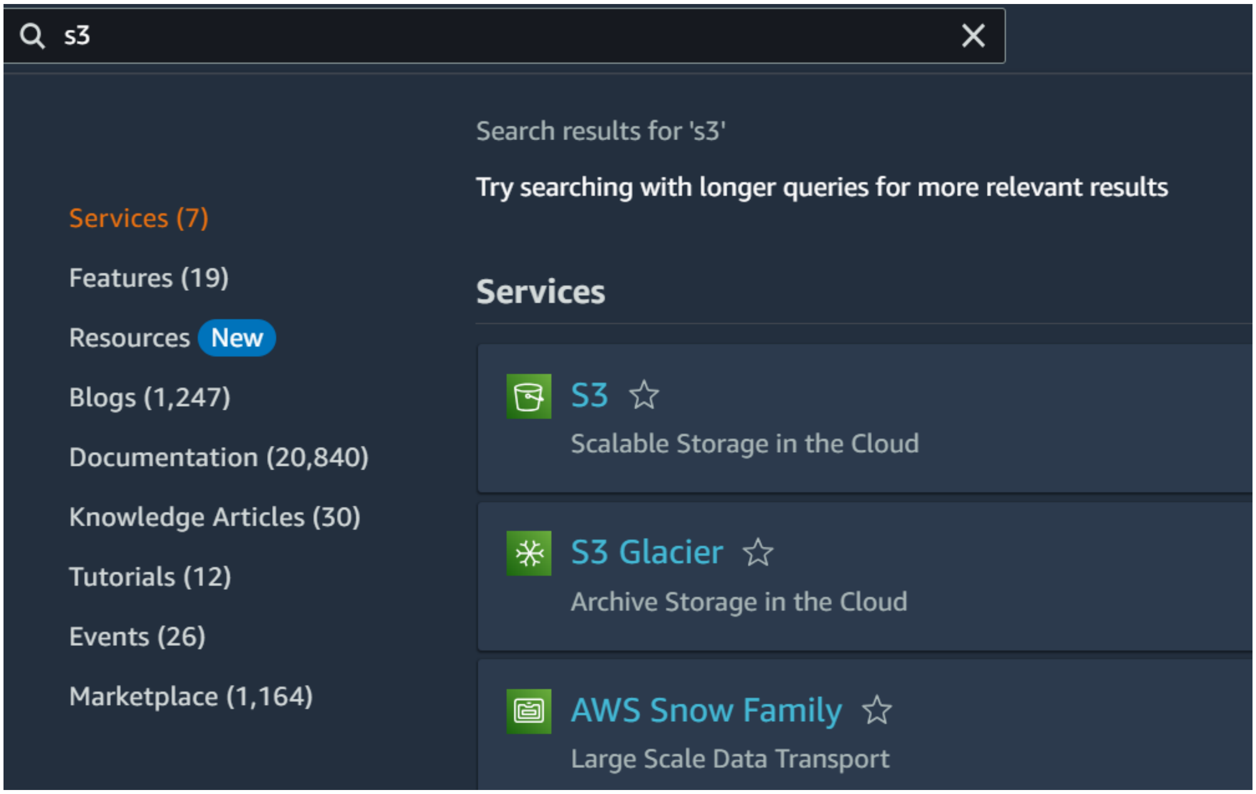
A PRACTICAL APPROACH: CREATING AN S3 BUCKET USING AWS MANAGEMENT CONSOLE AND CLI

Section 1: Creating an S3 Bucket using the AWS Management Console

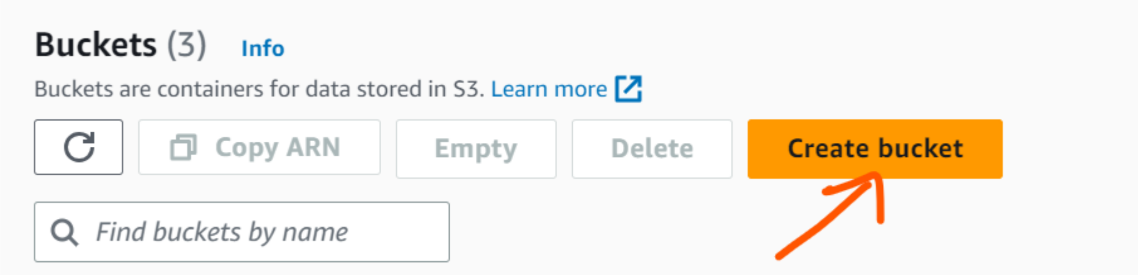
- Log in to the AWS Management Console: Open your web browser and navigate to the AWS Management Console (https://console.aws.amazon.com). Sign in with your AWS account credentials.
- Open the S3 Service: Once logged in, search for "S3" in the AWS Management Console search bar, and click on the "Amazon S3" service.



Search results for 's3'

Try searching with longer queries for more relevant results

- Click "Create Bucket": In the S3 console, click the “Create bucket” button to create a new bucket**.**

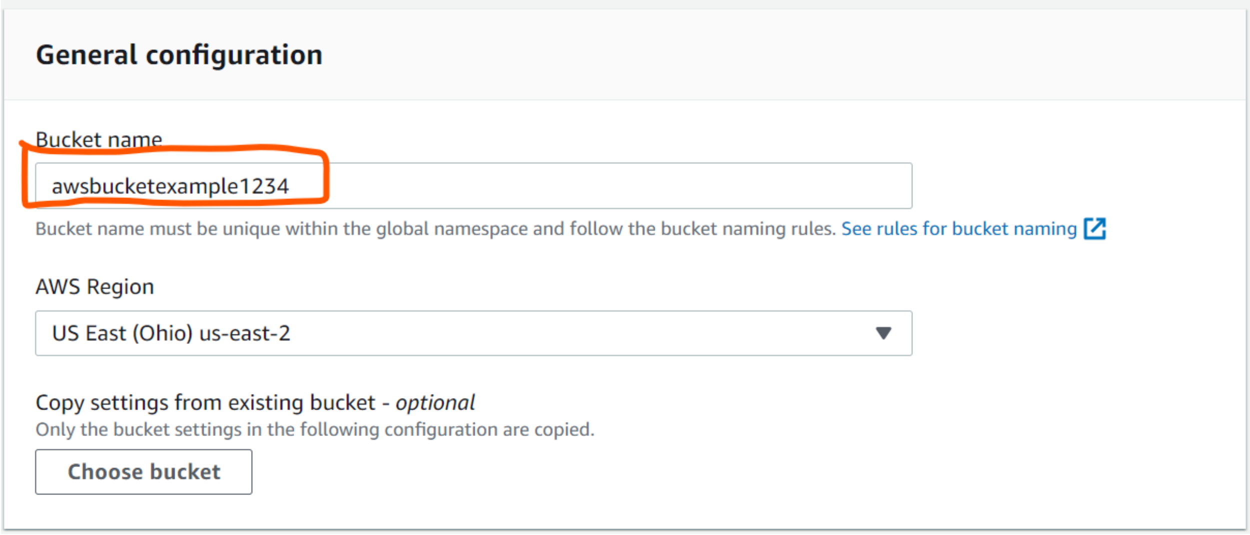


Buckets (3) Info

Buckets are containers for data stored in S3. Learn more

Configure Bucket Properties:

- Bucket Name: Enter a unique name for your bucket. Note that bucket names must be globally unique across all of AWS.
- Region: Select the AWS region where you want to create the bucket.
- Configure options as needed: Enable or disable options like versioning, server access logging, and default encryption.



General configuration

Bucket name

awsbucketexample1234

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

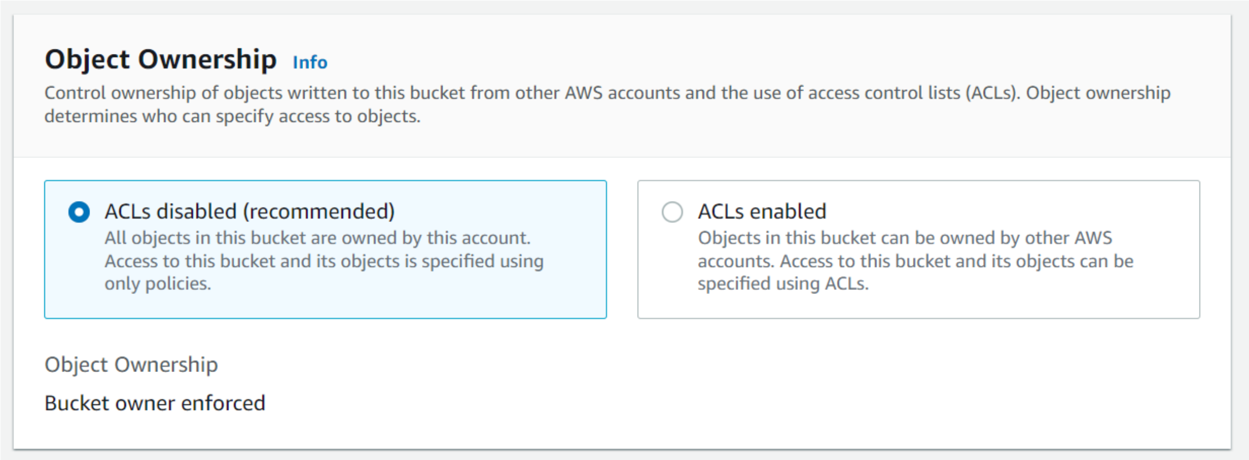
AWS Region

US East (Ohio) us-east-2

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

- Object ownership in the context of AWS S3 refers to the entity or AWS account that has control over an object stored within an S3 bucket. By default, the AWS account that uploads an object becomes its owner.



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.

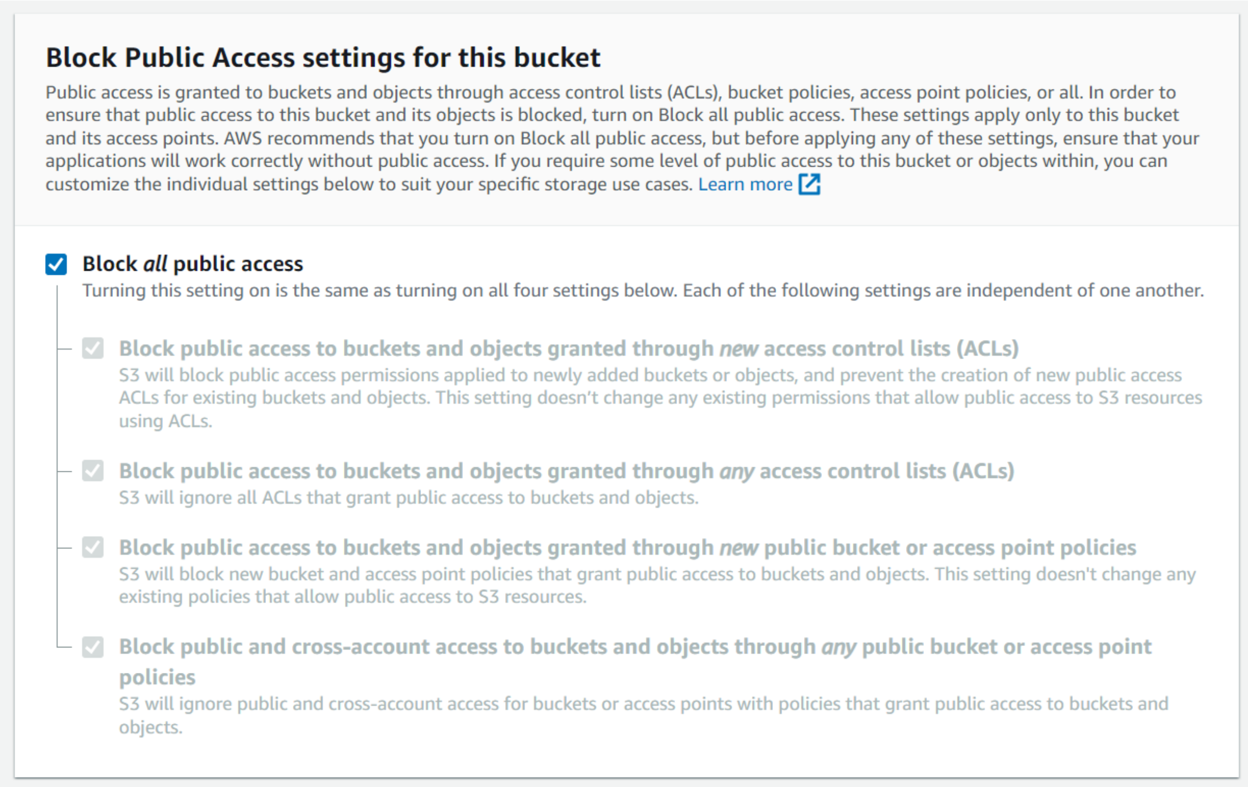
○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

Set Bucket Permissions:

- Block Public Access: Choose the level of public access to your bucket. Consider best practices and your specific requirements.
- Access Control List (ACL): Specify access permissions for individual users or groups.
- Bucket Policy: Define fine-grained access policies using JSON syntax.



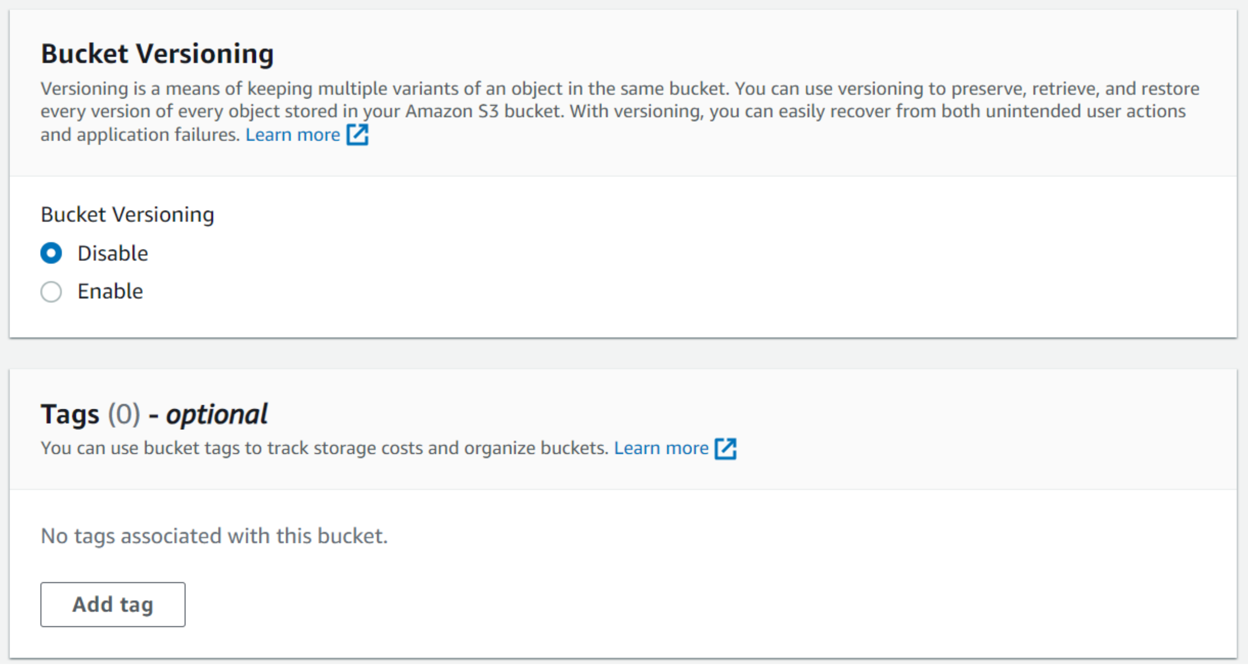
Block Public Access settings for this bucket

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.

- When creating an S3 bucket, you have the option to enable bucket versioning, which allows you to store and manage multiple versions of objects within the bucket, enhancing data protection and enabling easy recovery when needed.



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

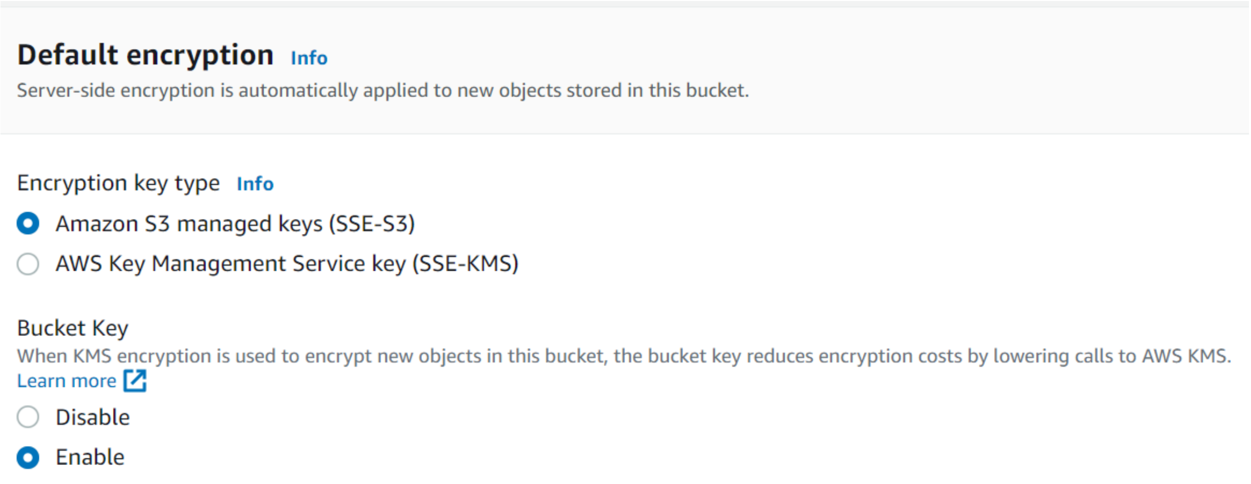
● Disable

○ Enable

Tags (0) **- *optional***

You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.



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)

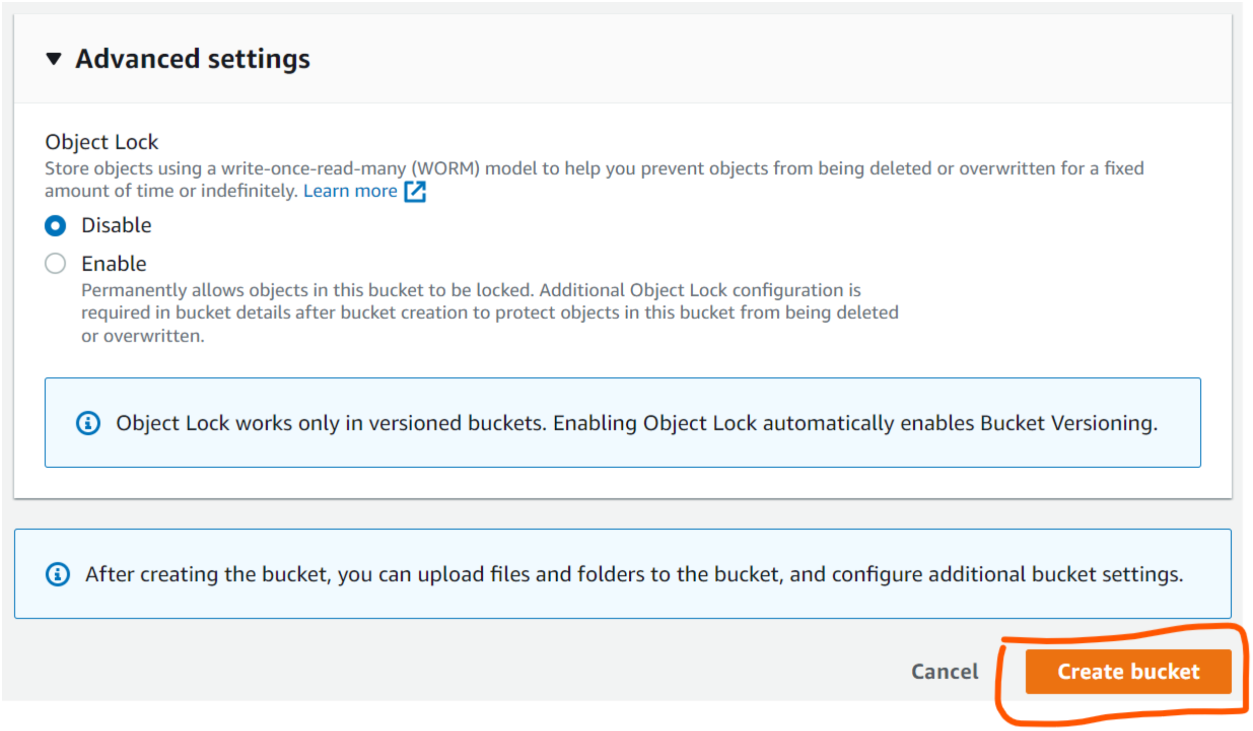
Bucket Key

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

- Review your configuration settings and click on the "Create bucket" button to create the S3 bucket.



▼ 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

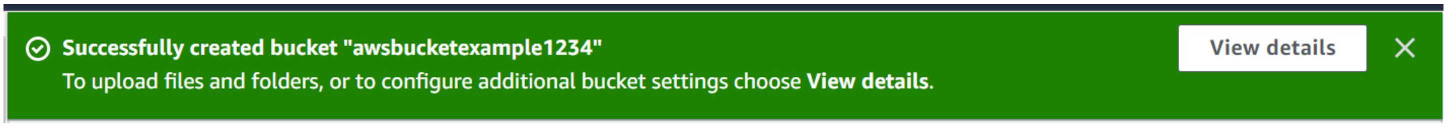
○ Enable

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.

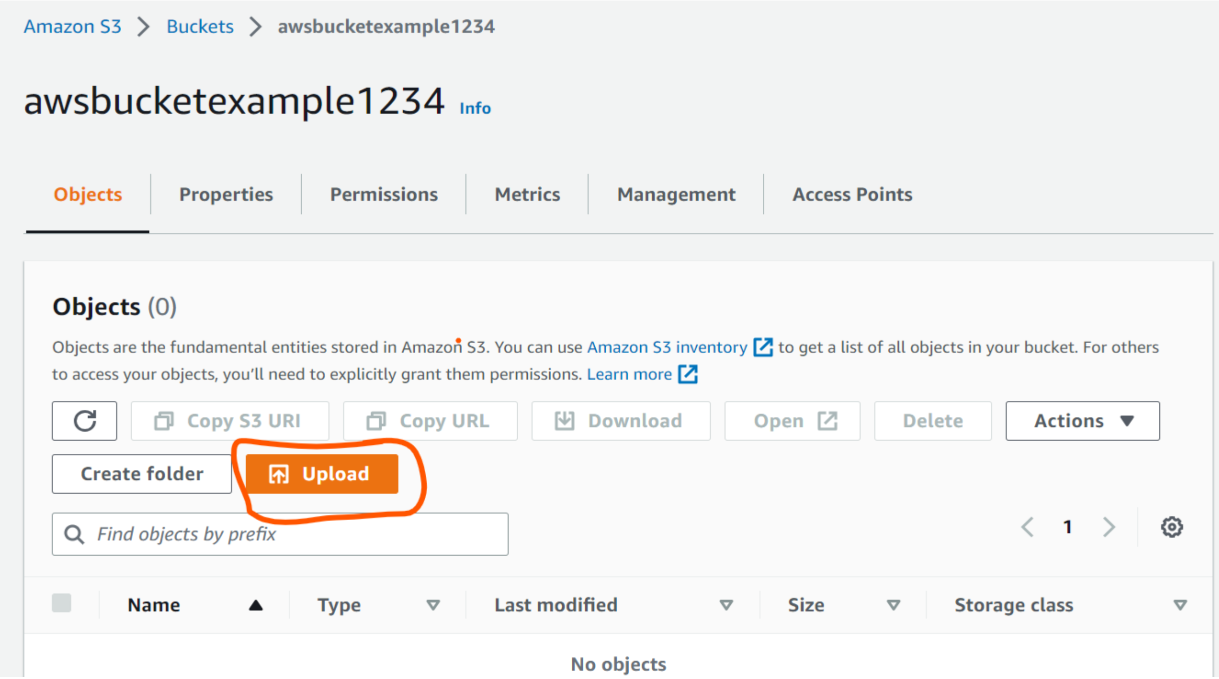
- Once it is created, you will see this on the top of the page.



Successfully created bucket "awsbucketexample1234"

To upload files and folders, or to configure additional bucket settings choose **View details**.

- Once the bucket is created, you can create folders, and also upload the files from your local machine to the cloud using the upload icon present inside the bucket.



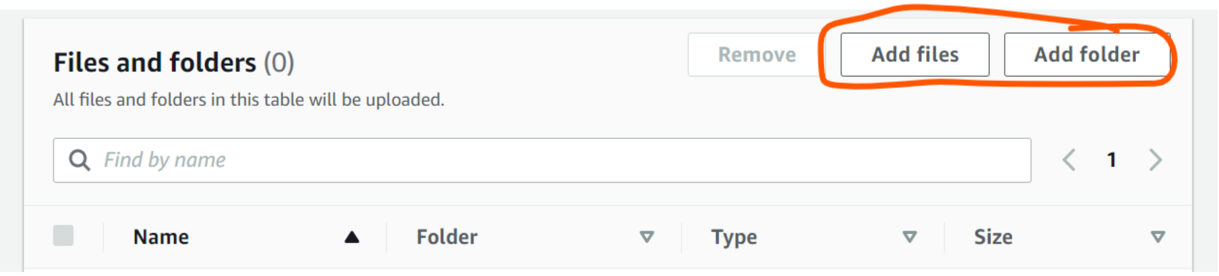
awsbucketexample1234

Objects (0)

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

□	Name ▲	Type ▽	Last modified ▽	Size ▽	Storage class ▽
			No objects		

- We can add files or folders using the Add files and Add folder icon.

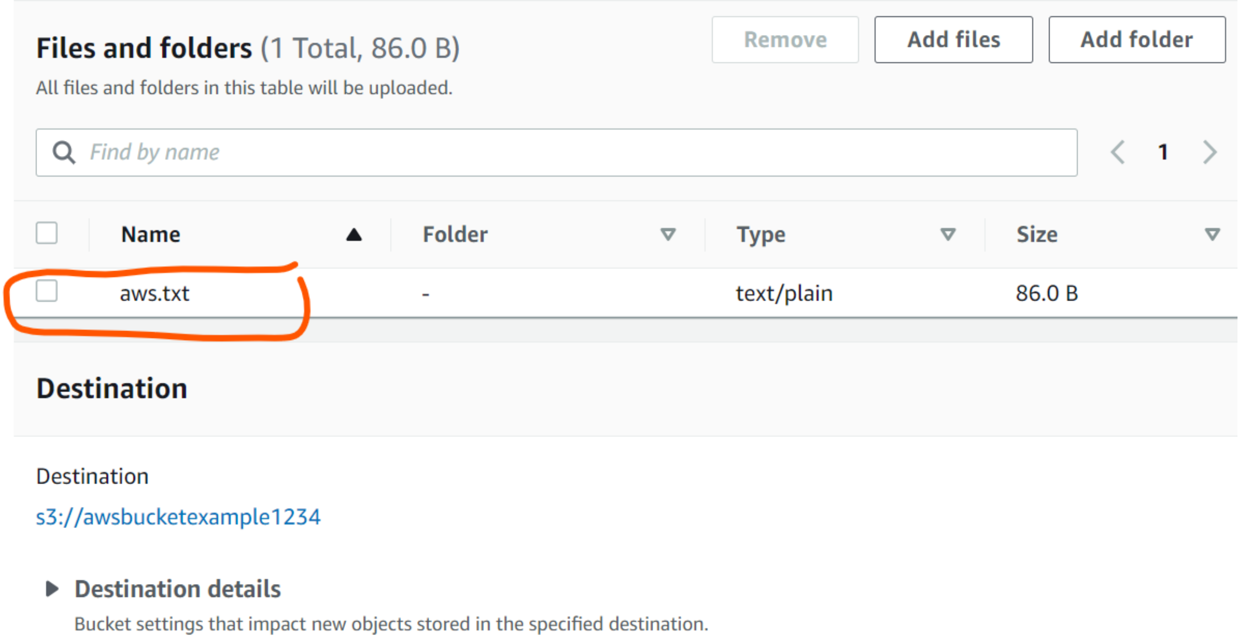


Files and folders (0)

All files and folders in this table will be uploaded.

□	Name ▲	Folder ▽	Type ▽	Size ▽

- I have uploaded a text file and it is shown its name, type, size, and destination information.



Files and folders (1 Total, 86.0 B)

All files and folders in this table will be uploaded.

□	Name ▲	Folder ▽	Type ▽	Size ▽
□	aws.txt	-	text/plain	86.0 B

Destination

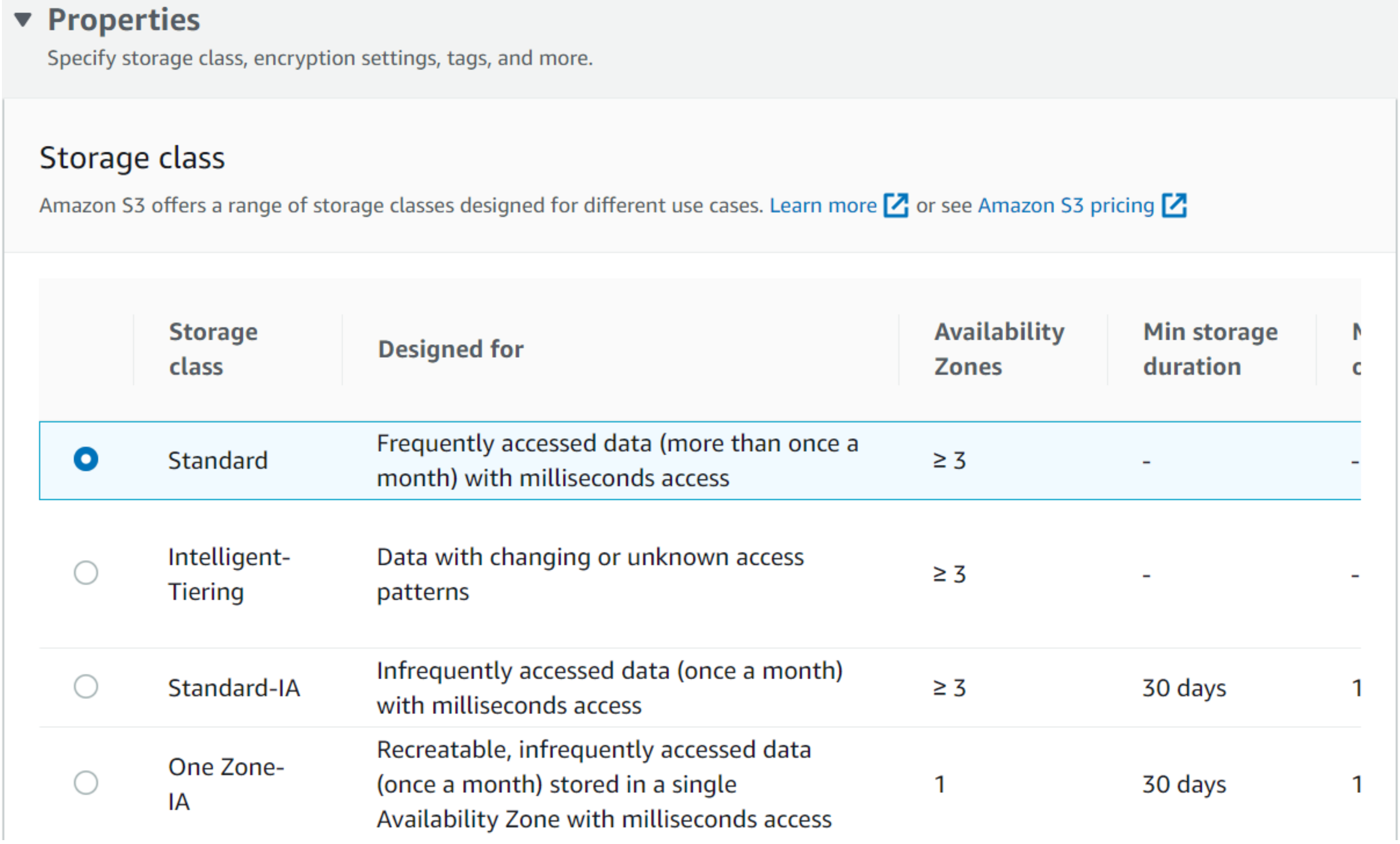
Destination

s3://awsbucketexample1234

▶ **Destination details**

Bucket settings that impact new objects stored in the specified destination.

- Under the properties tab, we can see the different S3 Storage types that can be selected based on our usage.



▼ Properties

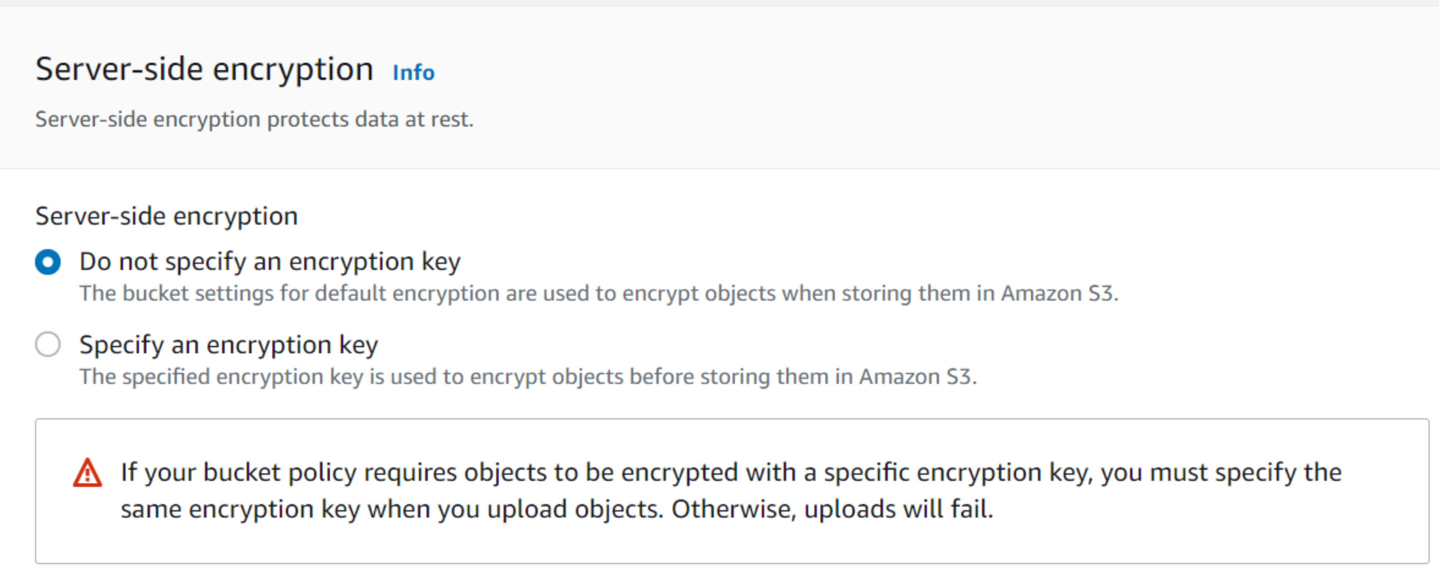
Specify storage class, encryption settings, tags, and more.

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	N c
●	Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-	-
○	Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-	-
○	Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days	1
○	One Zone-IA	Recreatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days	1

- We can choose the Server-side encryption and by default, it is “Do not specify an encryption key”.



Server-side encryption Info

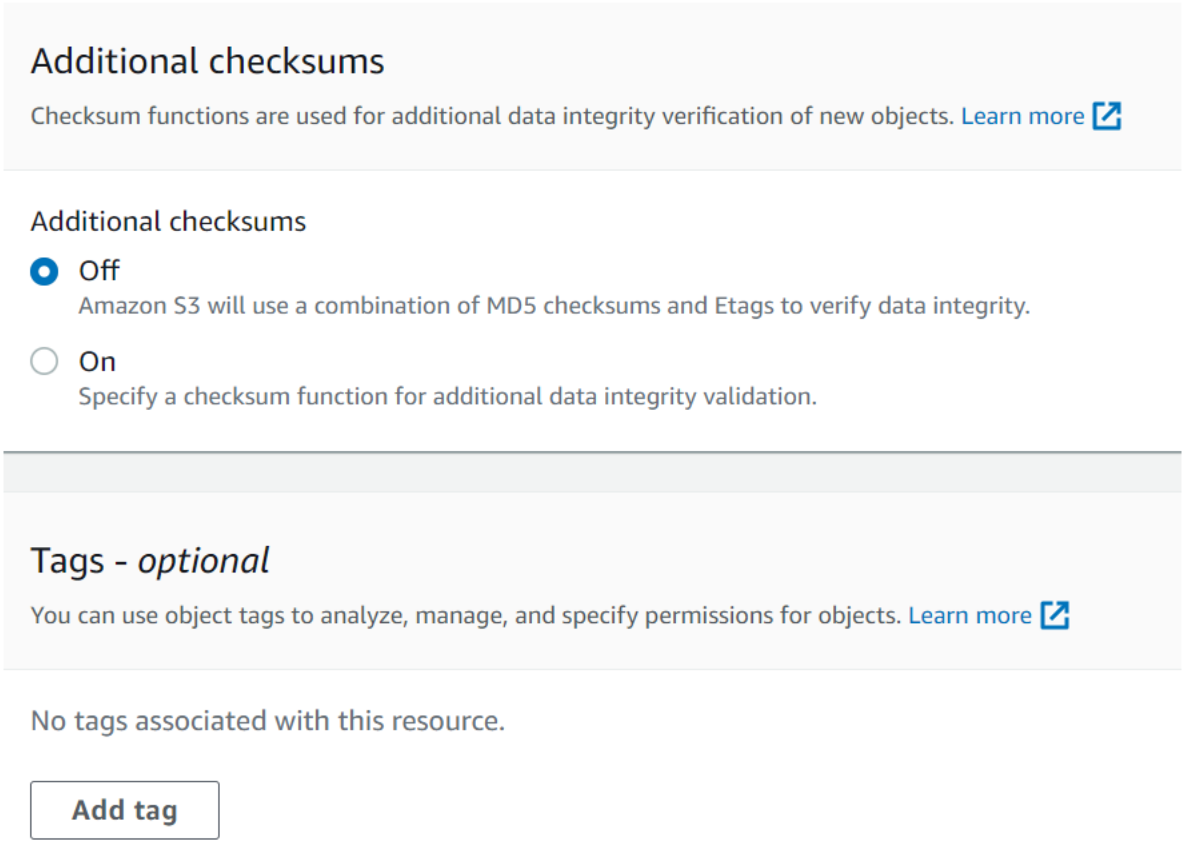
Server-side encryption protects data at rest.

Server-side encryption

● Do not specify an encryption key
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.

○ Specify an encryption key
The specified encryption key is used to encrypt objects before storing them in Amazon S3.

⚠ If your bucket policy requires objects to be encrypted with a specific encryption key, you must specify the same encryption key when you upload objects. Otherwise, uploads will fail.



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.

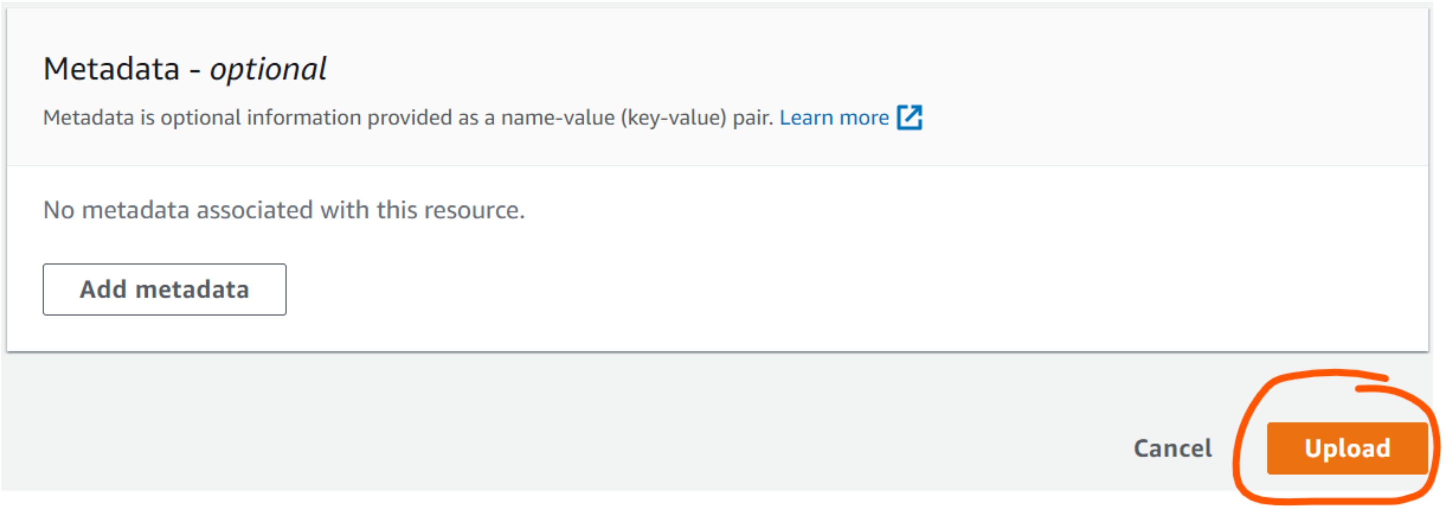
○ On
Specify a checksum function for additional data integrity validation.

Tags - *optional*

You can use object tags to analyze, manage, and specify permissions for objects. Learn more

No tags associated with this resource.

- Finally you can click on the upload.

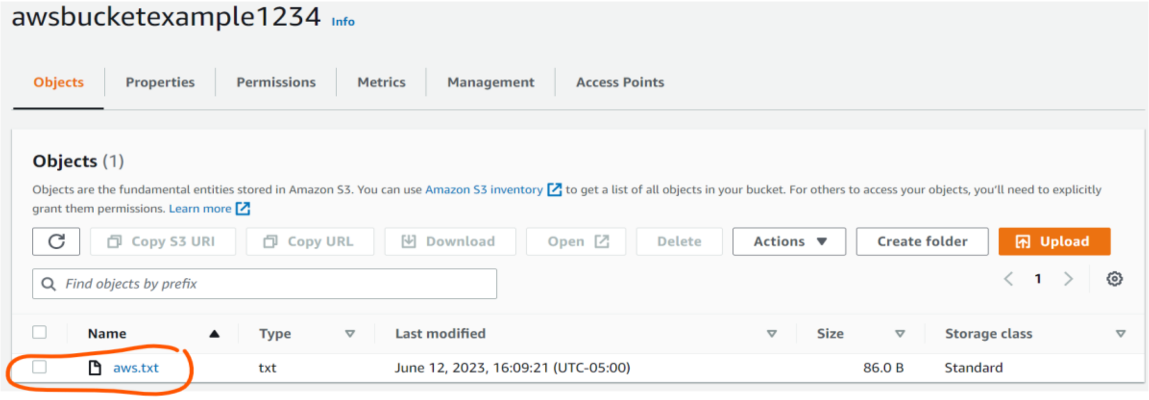


Metadata - *optional*

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

No metadata associated with this resource.

- Now, you can see that the file is uploaded into the bucket.

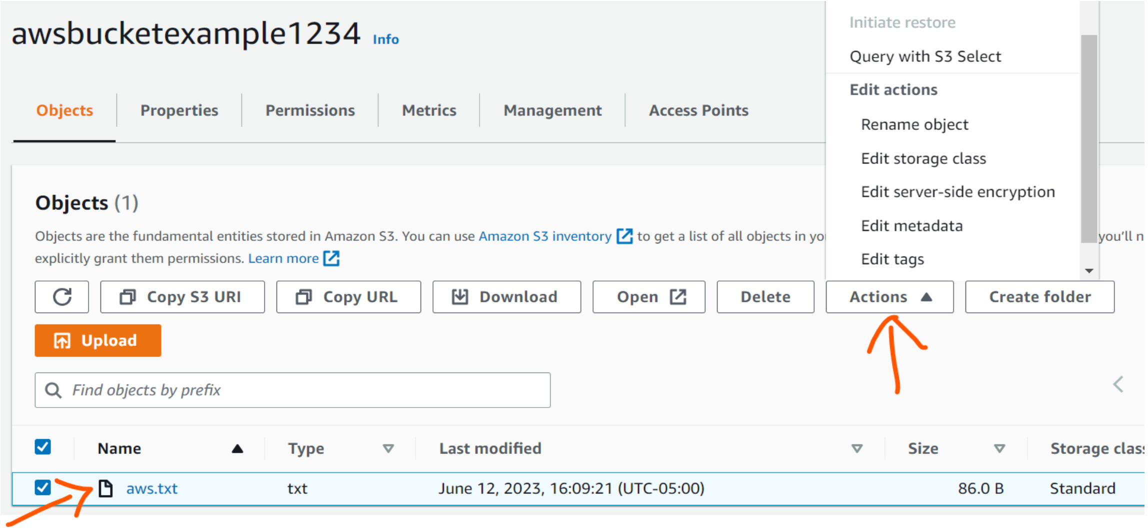


Objects (1)

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

	Name	Type	Last modified	Size	Storage class
□	aws.txt	txt	June 12, 2023, 16:09:21 (UTC-05:00)	86.0 B	Standard

- We can edit all the selections that we have made during uploading the file by clicking the check box next to the file that is uploaded and then click on “Actions”.



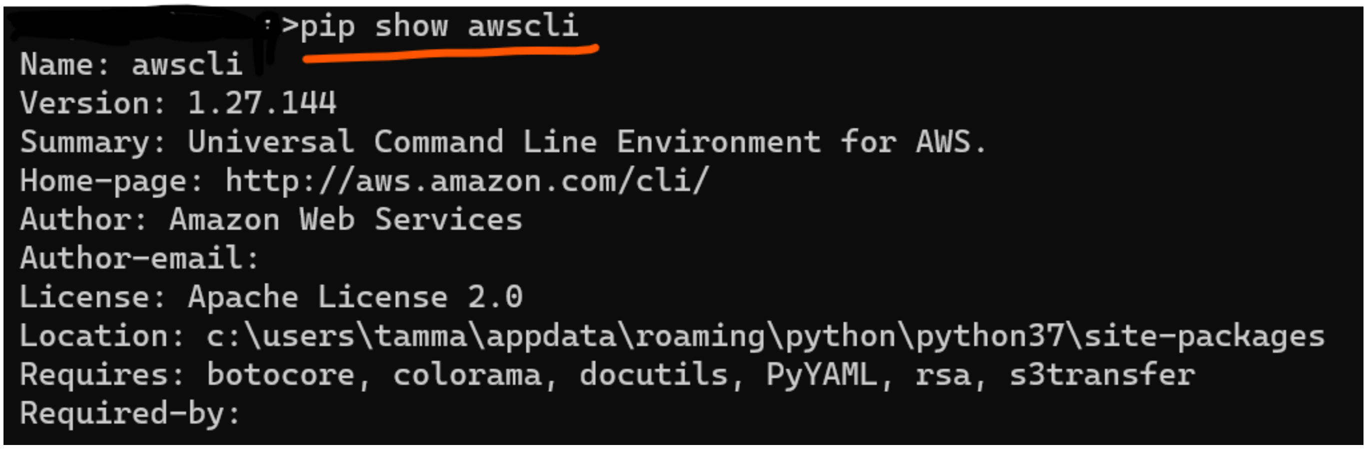
Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in yo you'll n explicitly grant them permissions. Learn more

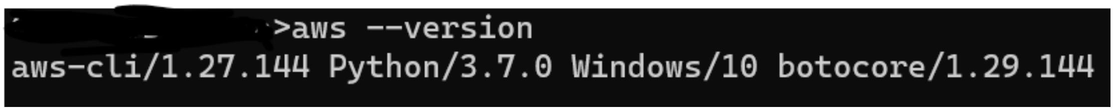
☑	Name	Type	Last modified	Size	Storage clas
☑	aws.txt	txt	June 12, 2023, 16:09:21 (UTC-05:00)	86.0 B	Standard

Section 2: Creating an S3 Bucket using the AWS CLI

- Install and Configure AWS CLI: Ensure you have the AWS CLI installed on your local machine. If not, follow the installation instructions provided by AWS.
- We can check the installation using the command **pip show awscli** in the command prompt.

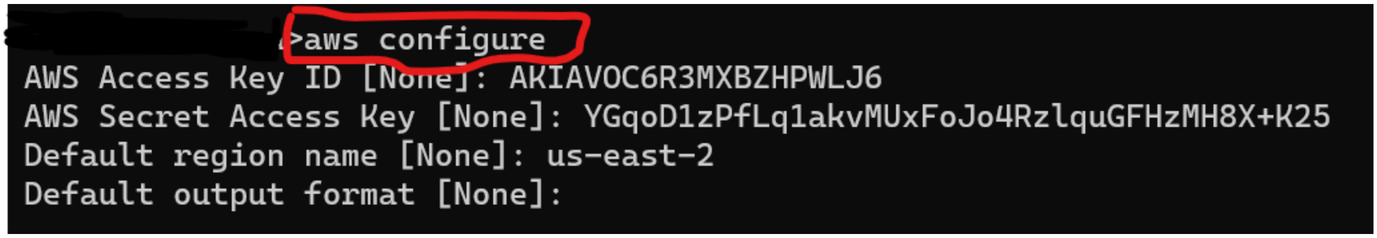


```
[redacted]:>pip show awscli
Name: awscli
Version: 1.27.144
Summary: Universal Command Line Environment for AWS.
Home-page: http://aws.amazon.com/cli/
Author: Amazon Web Services
Author-email:
License: Apache License 2.0
Location: c:\users\tamma\appdata\roaming\python\python37\site-packages
Requires: botocore, colorama, docutils, PyYAML, rsa, s3transfer
Required-by:
```



```
[redacted]>aws --version
aws-cli/1.27.144 Python/3.7.0 Windows/10 botocore/1.29.144
```

- Configure the CLI by running **aws configure** and enter your AWS Access Key ID, Secret Access Key, default region, and output format.

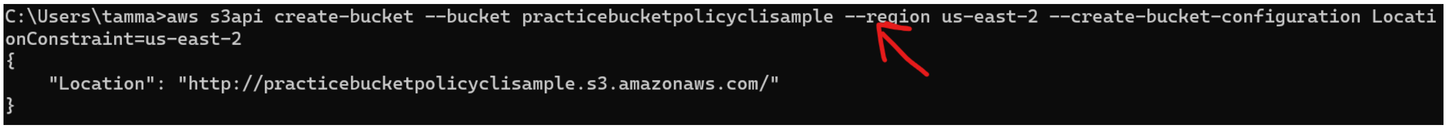


```
[redacted]>aws configure
AWS Access Key ID [None]: AKIAVOC6R3MXBZHPWLJ6
AWS Secret Access Key [None]: YGqoD1zPfLq1akvMUxFoJo4RzlquGFHzMH8X+K25
Default region name [None]: us-east-2
Default output format [None]:
```

- To create a bucket, use the following command:

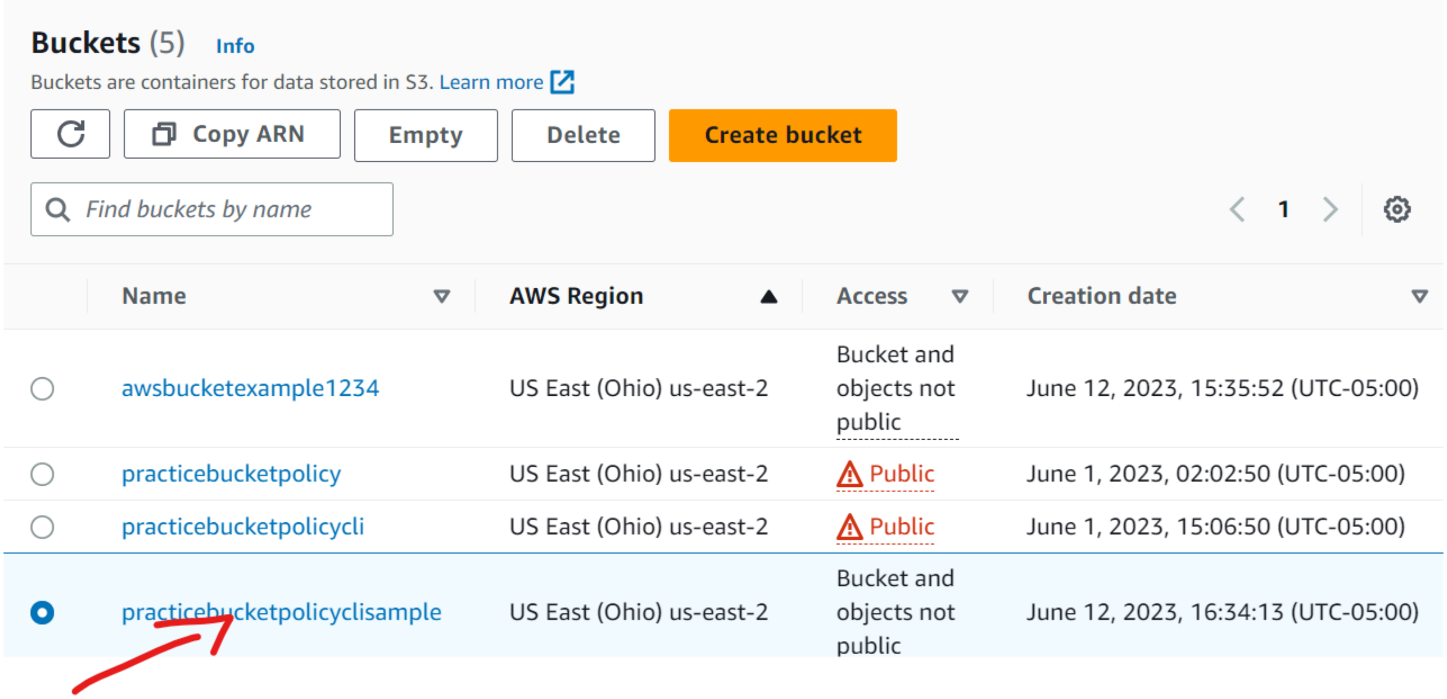
  aws s3api create-bucket --bucket your-bucket-name --region your-region –create-bucket-configuration LocationConstraint=your-region

  Replace **your-bucket-name** with your desired bucket name, and **your-region** with your preferred AWS region.



```
C:\Users\tamma>aws s3api create-bucket --bucket practicebucketpolicyclisample --region us-east-2 --create-bucket-configuration Locati
onConstraint=us-east-2
{
    "Location": "http://practicebucketpolicyclisample.s3.amazonaws.com/"
}
```

- We can verify the same on the console and can see that the bucket is created.



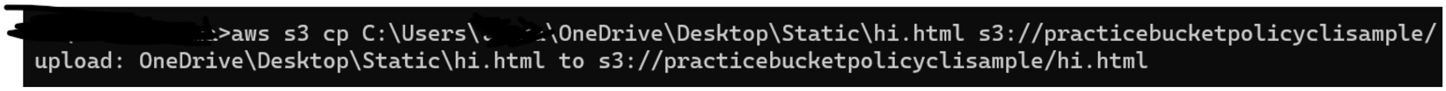
Buckets (5)

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	awsbucketexample1234	US East (Ohio) us-east-2	Bucket and objects not public	June 12, 2023, 15:35:52 (UTC-05:00)
○	practicebucketpolicy	US East (Ohio) us-east-2	⚠ Public	June 1, 2023, 02:02:50 (UTC-05:00)
○	practicebucketpolicycli	US East (Ohio) us-east-2	⚠ Public	June 1, 2023, 15:06:50 (UTC-05:00)
●	practicebucketpolicyclisample	US East (Ohio) us-east-2	Bucket and objects not public	June 12, 2023, 16:34:13 (UTC-05:00)

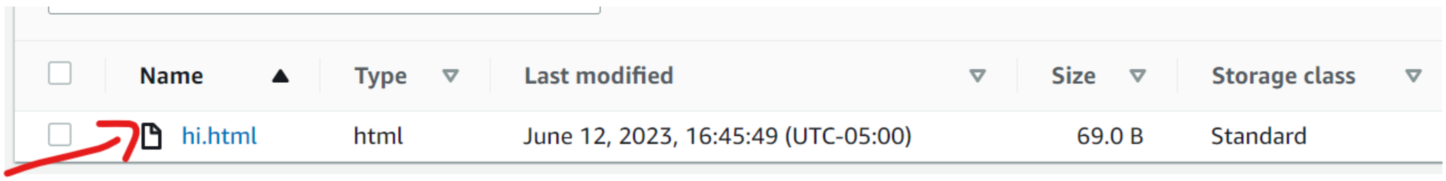
- We can upload the files on the local machine using the below command:

  aws s3 cp your-local-machine-file-path s3://your-bucketname-key



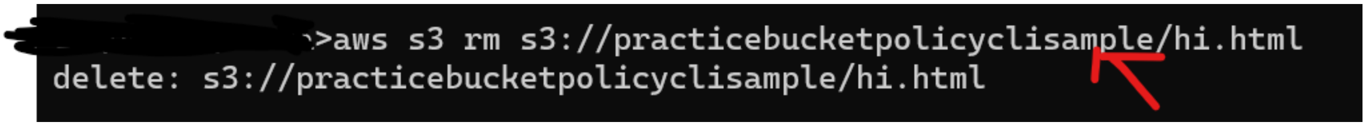
```
[redacted]>aws s3 cp C:\Users\[redacted]\OneDrive\Desktop\Static\hi.html s3://practicebucketpolicyclisample/
upload: OneDrive\Desktop\Static\hi.html to s3://practicebucketpolicyclisample/hi.html
```

- We can verify it on the console if the file is uploaded or not by navigating into the bucket.

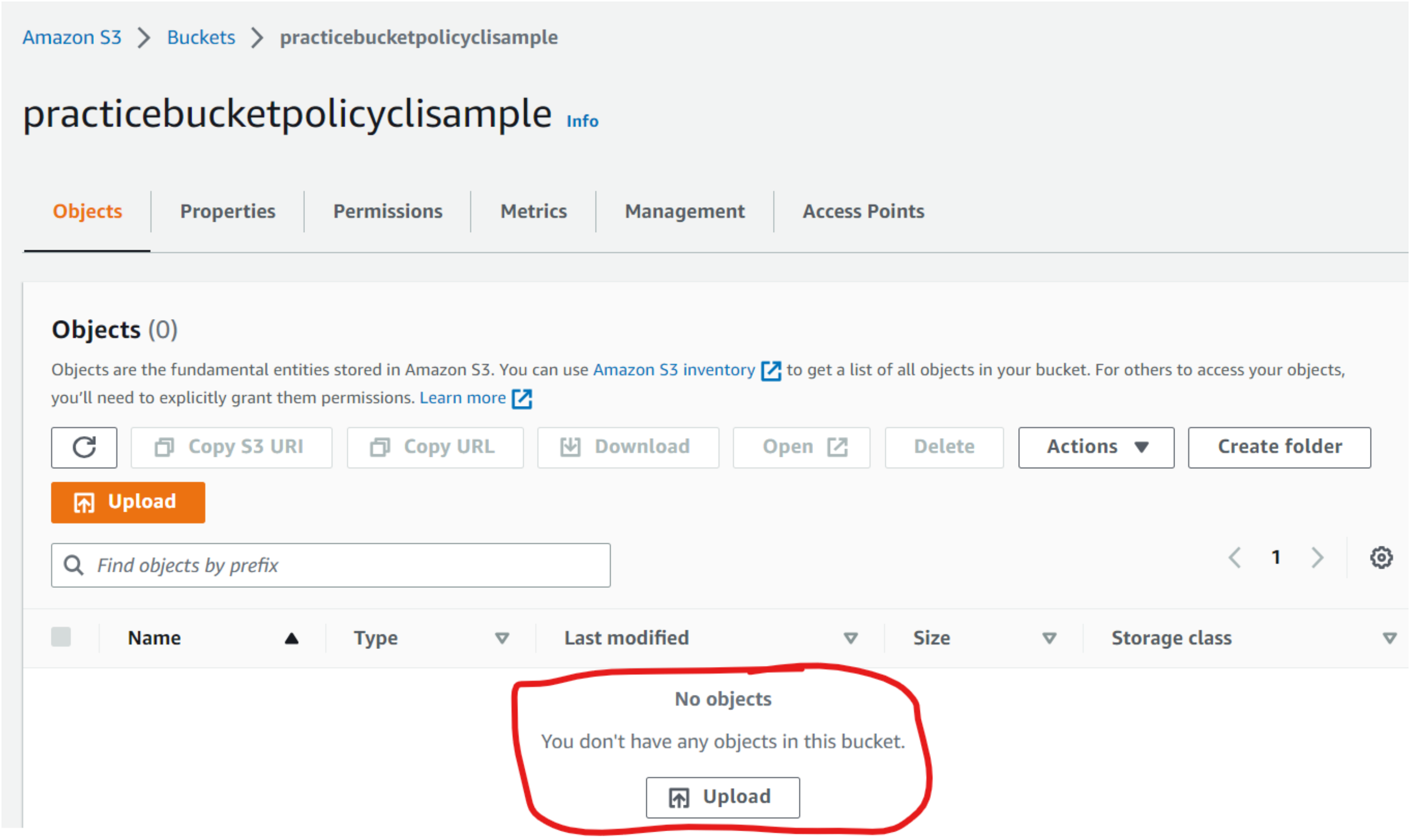


□	Name ▲	Type	Last modified	Size	Storage class
□	hi.html	html	June 12, 2023, 16:45:49 (UTC-05:00)	69.0 B	Standard

- We can also remove the files using the rm command as follows, and check with the same on the console.



```
[redacted]>aws s3 rm s3://practicebucketpolicyclisample/hi.html
delete: s3://practicebucketpolicyclisample/hi.html
```



Amazon S3 > Buckets > practicebucketpolicyclisample
practicebucketpolicyclisample Info
Objects
Properties
Permissions
Metrics
Management
Access Points

Objects (0)

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

□	Name ▲	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.