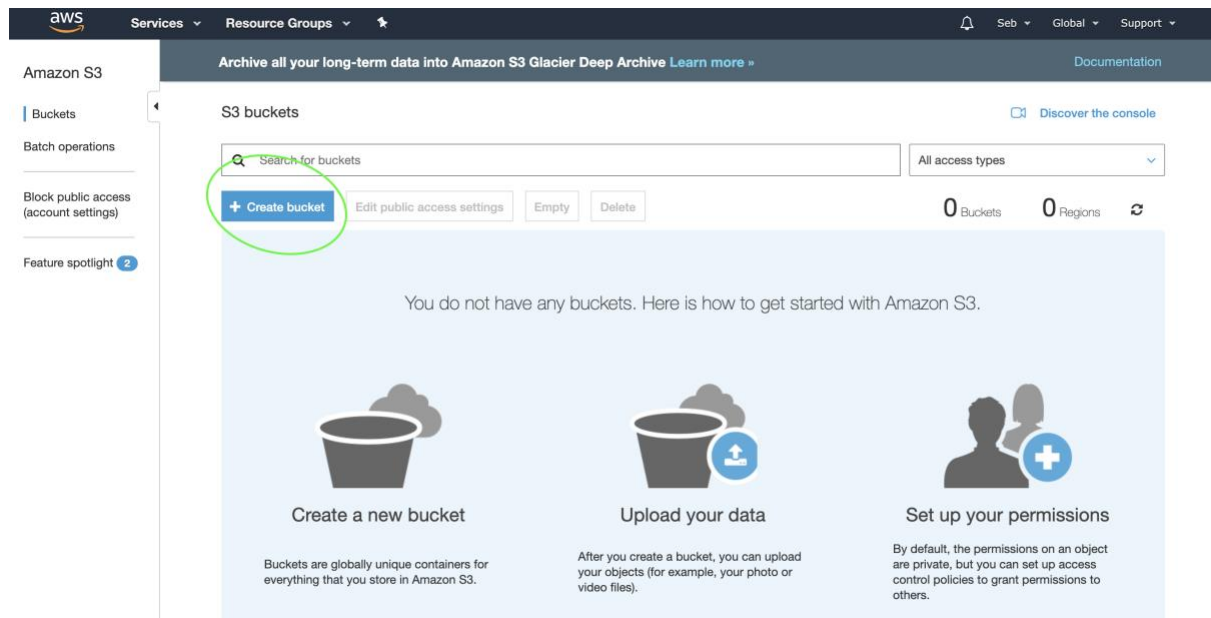
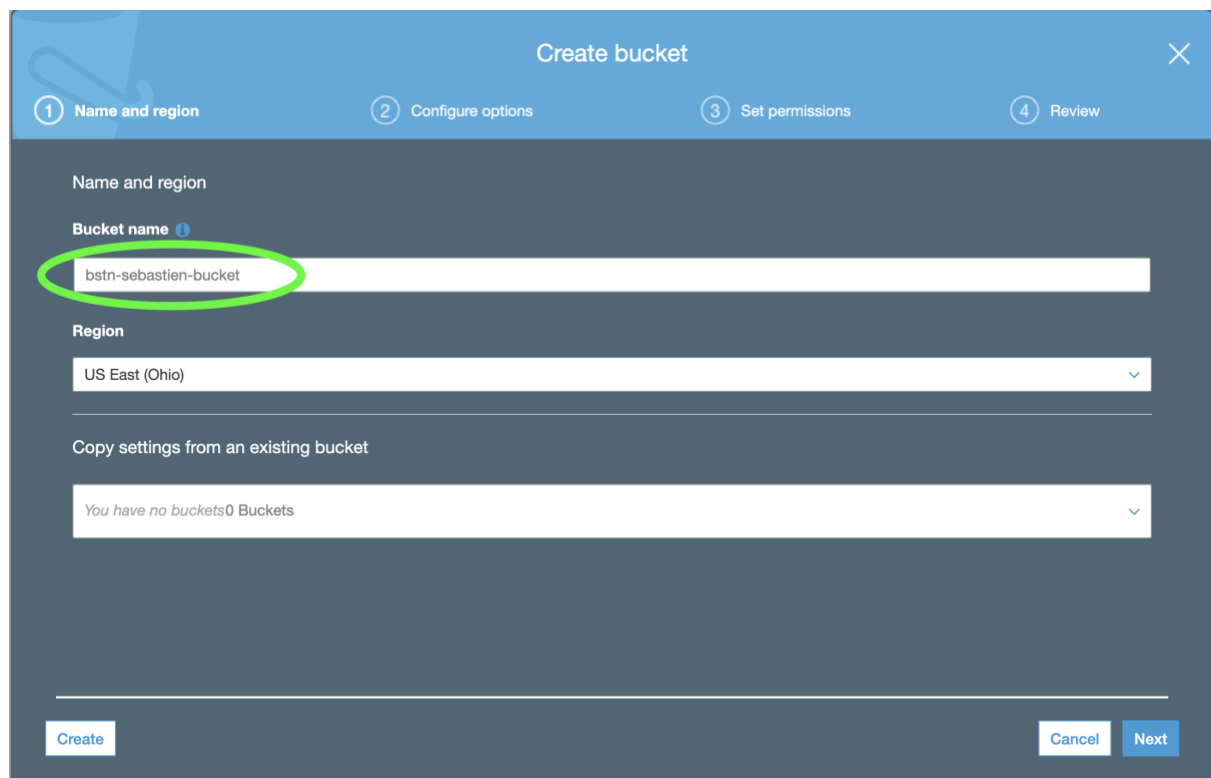


## AWS – Upload file:

On your AWS account dashboard, go onto S3 and click on create bucket:



Enter a name of your choosing for the bucket name and then keep on clicking on next:

A screenshot of the 'Create bucket' wizard in the AWS console. The wizard has four steps: 1. Name and region, 2. Configure options, 3. Set permissions, and 4. Review. The first step is active. It contains a 'Bucket name' field with the text 'bstn-sebastien-bucket' (circled in green), a 'Region' dropdown menu set to 'US East (Ohio)', and a 'Copy settings from an existing bucket' dropdown menu showing 'You have no buckets 0 Buckets'. At the bottom, there are 'Create', 'Cancel', and 'Next' buttons.

When you get onto this screen it's up to you if you want to make it private or public. I just make it public by unselecting it.

Create bucket

1 Name and region 2 Configure options 3 Set permissions 4 Review

Note: You can grant access to specific users after you create the bucket.

### Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block *all* public access. These settings apply only to this bucket. 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 your buckets 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 policies**  
S3 will block new bucket 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 policies**  
S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.

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

When you have created your bucket click on the upload button.

Amazon S3 > bstn-sebastien-bucket

Overview Properties Permissions Management

[Upload](#) [+ Create folder](#) [Download](#) [Actions](#)

US East (Ohio)

This bucket is empty. Upload new objects to get started.

### Upload an object

Buckets are globally unique containers for everything that you store in Amazon S3.

[Learn more](#)

### Set object properties

After you create a bucket, you can upload your objects (for example, your photo or video files).

[Learn more](#)

### Set object permissions

By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.

[Learn more](#)

Select the Standard storage class.

Upload

Select files

Set permissions

3 Set properties

4 Review

Storage class

Choose a storage class based on your use case and access requirements. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
<input checked="" type="radio"/> Standard	Frequently accessed data	≥ 3	-	-	-	-
<input type="radio"/> Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
<input type="radio"/> Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> Glacier	Archive data with retrieval times ranging from minutes to hours	≥ 3	90 days	40KB	-	Per-GB fees apply
<input type="radio"/> Glacier Deep Archive	Archive data that rarely, if ever, needs to be accessed with retrieval times in hours	≥ 3	180 days	40KB	-	Per-GB fees apply
<input type="radio"/> Reduced Redundancy (Not recommended)	Frequently accessed, non-critical data	≥ 3	-	-	-	-

Upload

PreviousNext

You have created a storage file.

Congratulations!!

