# Bucket name demoassignment Bucket name must be unique and must not contain spaces or uppercase letters. 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. 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.

Object Ownership

Bucket owner enforced

## **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

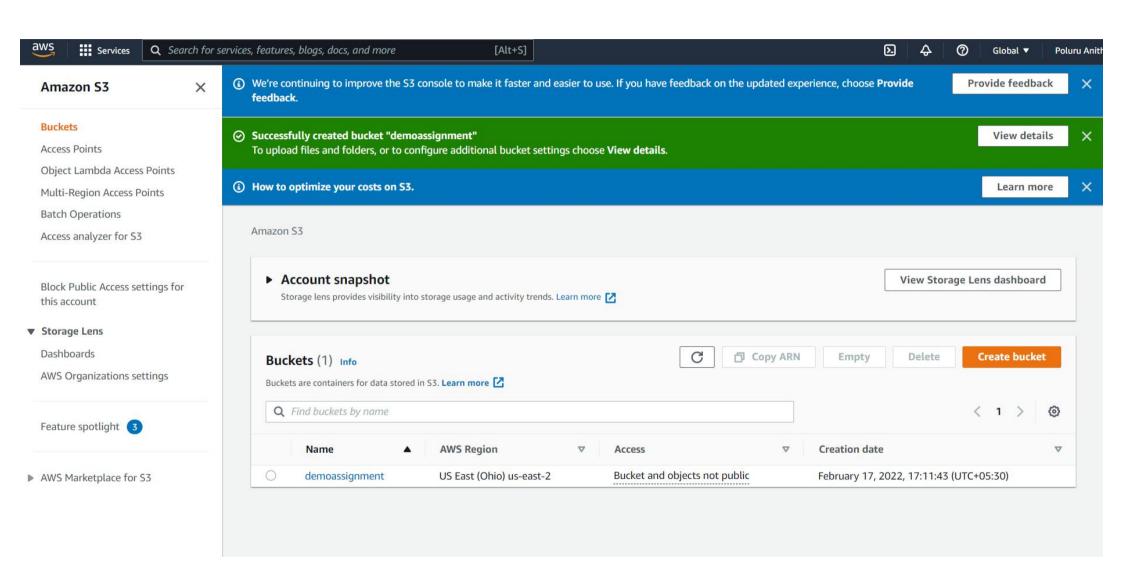
### ✓ Block all public access

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

53 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

	ures. Learn more 🔀
Bucket Versioni	g
<ul><li>Disable</li></ul>	
○ Enable	
Tags (0) - <i>o</i> ړ	tional
Track storage cost	or other criteria by tagging your bucket. Learn more 🔼
No tags associa	ed with this bucket.
Add tag	
Default enc	
Automatically end	ypt new objects stored in this bucket. Learn more 🔼
Server-side end	yption
Server-side enc	yption



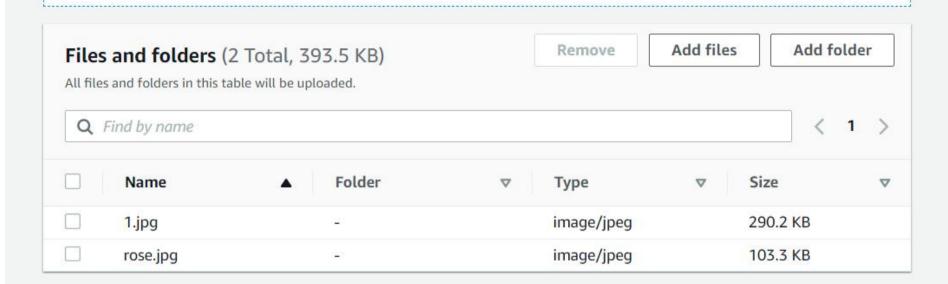
Tollowed by a stash (/). This object then appears as Tolder on the console. Learn more 🗹



## Your bucket policy might block folder creation

If your bucket policy prevents uploading objects without specific tags, metadata, or access control list (ACL) grantees, you will not be able to create a folder using this configuration. Instead, you can use the upload configuration to upload an empty folder and specify the appropriate settings.

older	
Folder name	
img	1
Folder names can't contain "/". See rules for nam	ning 🔀
Server-side encryption	
MA 100 (100 100 100 100 100 100 100 100 10	to the new folder object and not to the objects contained within it.
Server-side encryption  The following settings apply only to the server-side encryption	to the new folder object and not to the objects contained within it.
The following settings apply only t	to the new folder object and not to the objects contained within it.



# **Destination**

Destination

s3://demoassignment/img/

### **▶** Destination details

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

### **▶** Permissions

Grant public access and access to other AWS accounts.

# **▶** Properties

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

