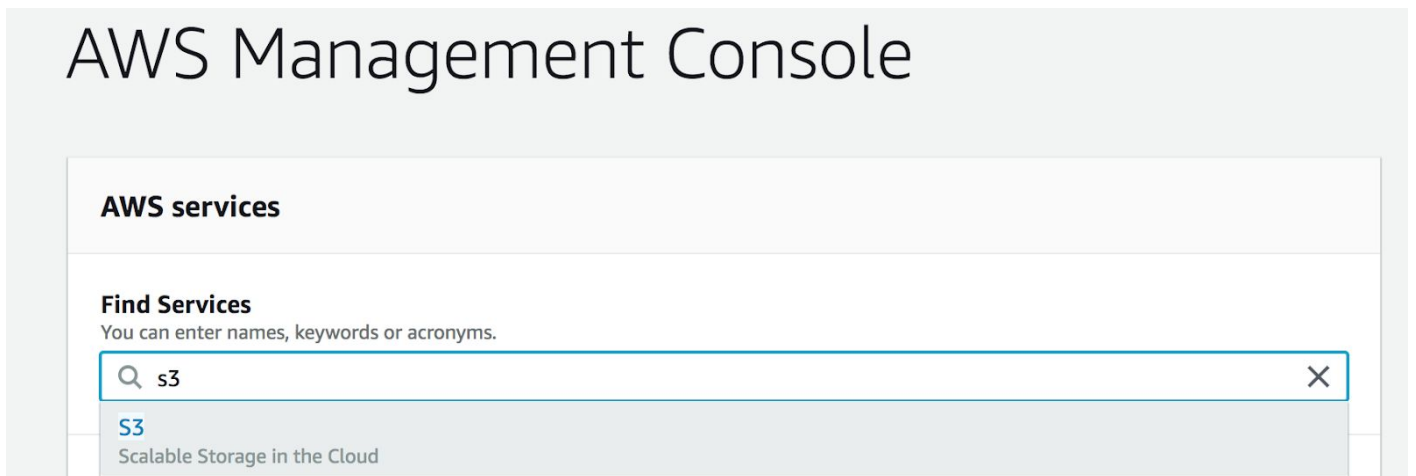


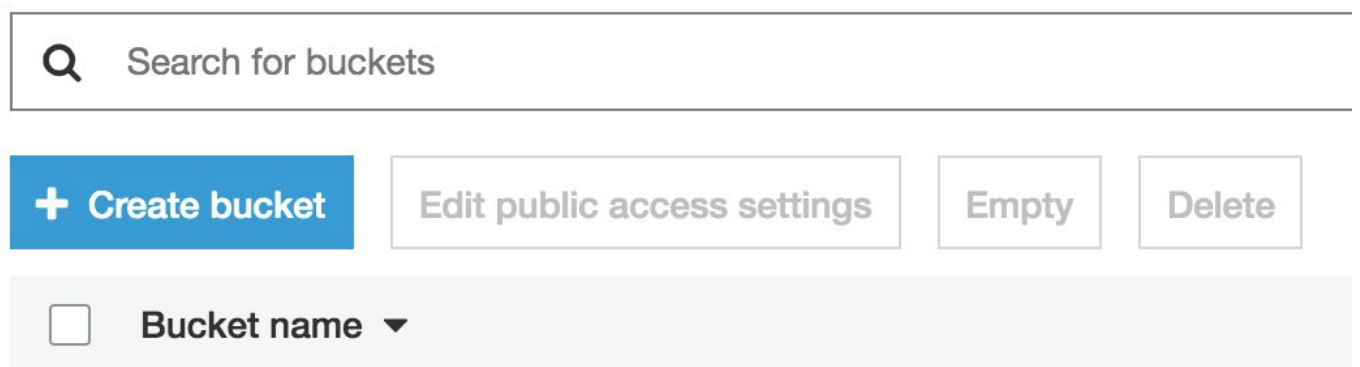
Create S3 Bucket

1. Navigate to the “AWS Management Console” page, type “S3” in the “Find Services” box and then select “S3”.



2. The Amazon S3 dashboard displays. Click “Create bucket”.

S3 buckets



3. Enter a "Bucket name" and click "Next". Note: Bucket names must be globally unique.

The screenshot shows the 'Create bucket' dialog box in the AWS S3 console. The dialog has a blue header with the title 'Create bucket' and a close button (X). Below the header is a progress bar with four steps: 1. Name and region, 2. Configure options, 3. Set permissions, and 4. Review. The first step, 'Name and region', is currently active. It contains three input fields: 'Bucket name' with the value 'udacity-website', 'Region' with the value 'US East (N. Virginia)', and 'Copy settings from an existing bucket' with a dropdown menu showing 'Select bucket (optional)' and '26 Buckets'. At the bottom of the dialog are three buttons: 'Create', 'Cancel', and 'Next'.

Create bucket

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

Name and region

Bucket name ⓘ

udacity-website

Region

US East (N. Virginia) ▾

Copy settings from an existing bucket

Select bucket (optional) 26 Buckets ▾

Create Cancel Next

4. Click "Next" again to skip over "Step 2: Configure Options".
5. On "Step 3: Set Permissions", uncheck "Block all public access".

Create bucket

✓ Name and region

✓ 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.

Previous

Next

- Click "Next" and click "Create bucket".
- Once the bucket is created, click on the name of the bucket to open the bucket to the contents.

Overview

Properties

Permissions

Management

Upload

+ Create folder

Download

Actions

US East (N. Virginia)

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.



Set object properties

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



Set object permissions

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

Operations

0 In progress

1 Success

0 Error