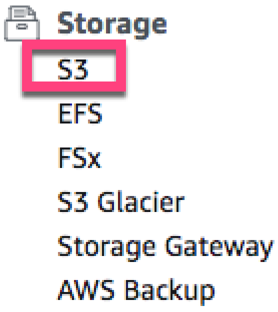
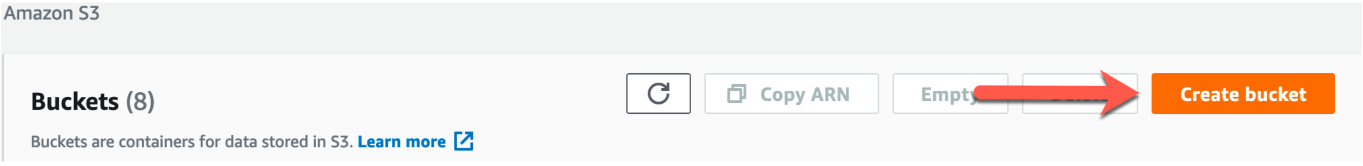
Cloud Storage on S3

- Go to **console.aws.amazon.com** and select **S3** under **Storage**.



- Click **Create bucket**.

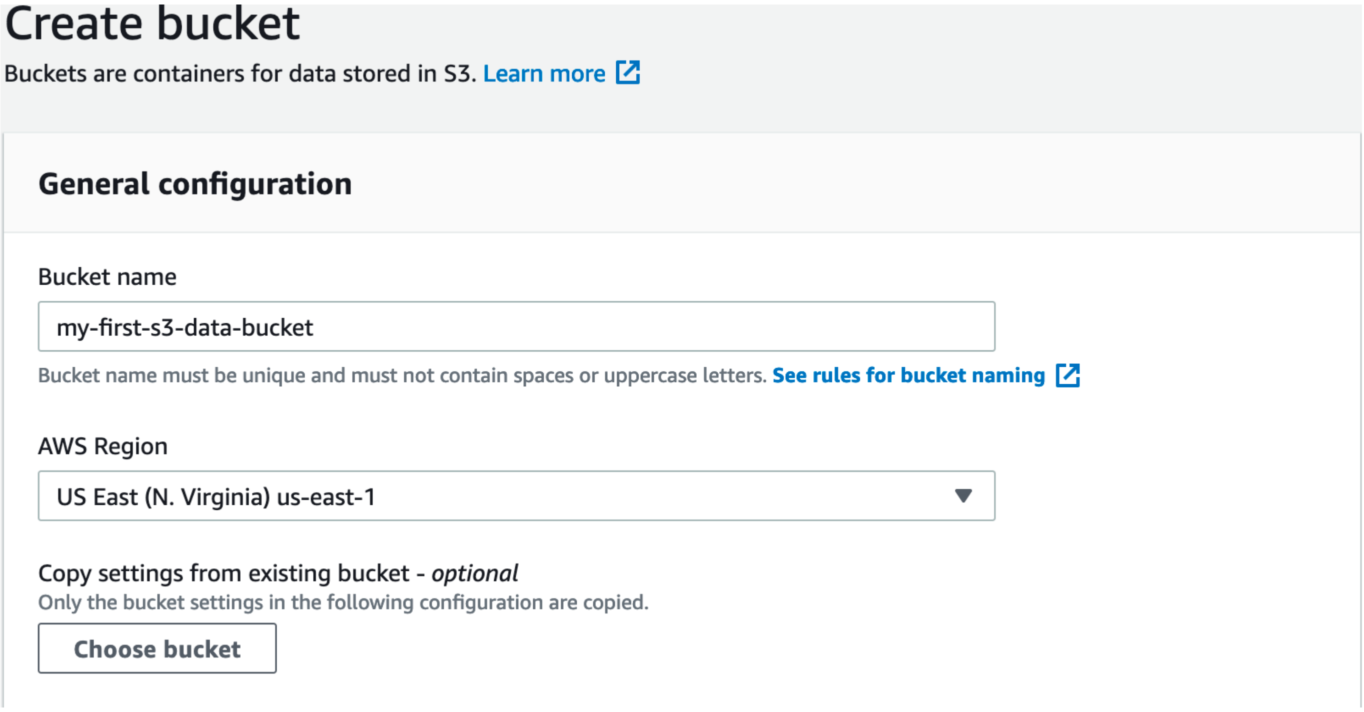


Buckets are containers for data stored in S3. Learn more

- Create a bucket name and choose the region.

- **Note:** The bucket name must be unique across all existing bucket names in Amazon S3. Buckets cannot be renamed or created inside of another bucket.

- Leave the region as the default— for example, `US East (N. Virginia)`. Changing the region will change the object URL used in all examples today.



Create bucket

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name: my-first-s3-data-bucket

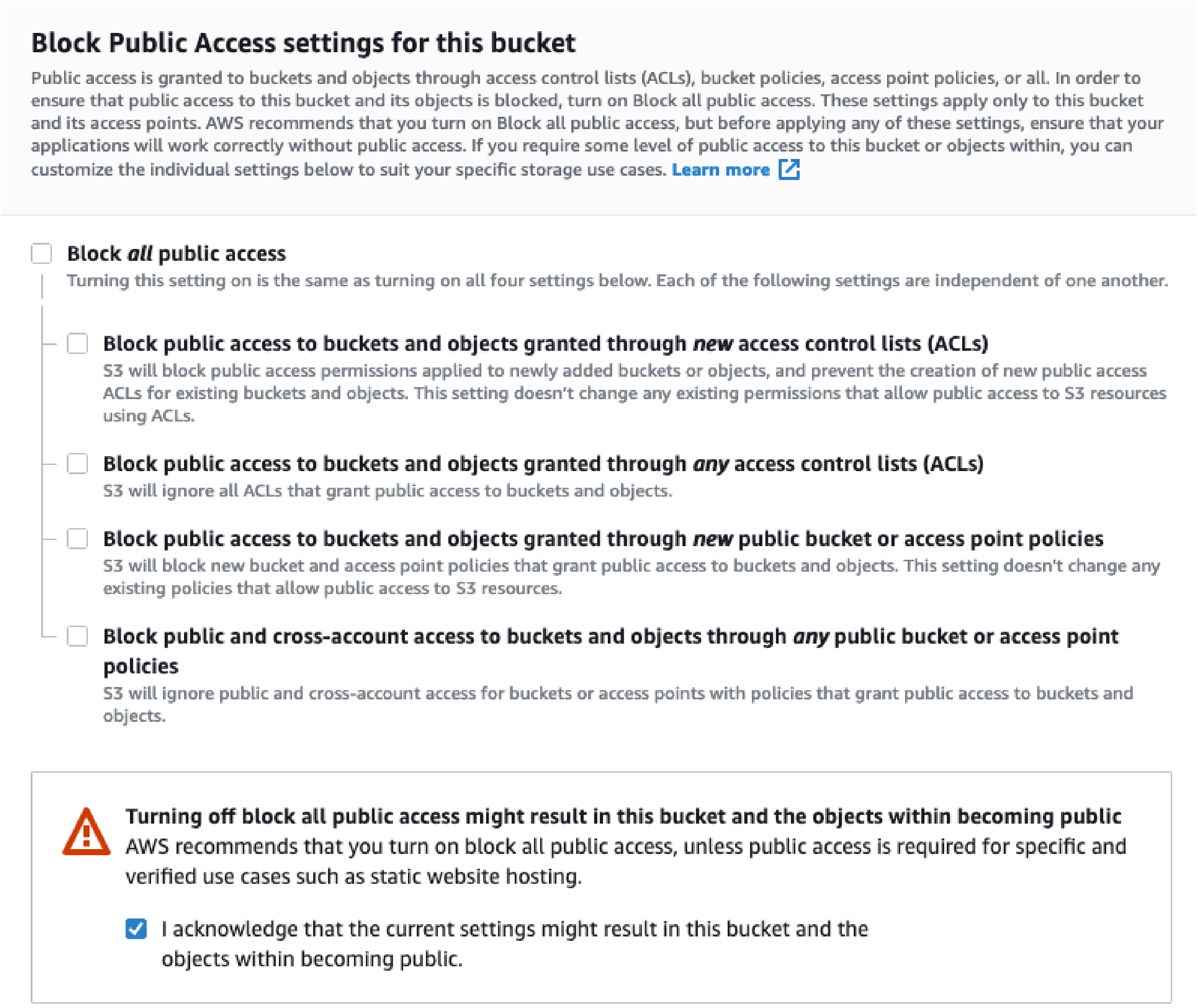
Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region: US East (N. Virginia) us-east-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

- Under **Block Public Access setting for this bucket**, uncheck the **Block all public access** option and check the box to acknowledge the change.



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

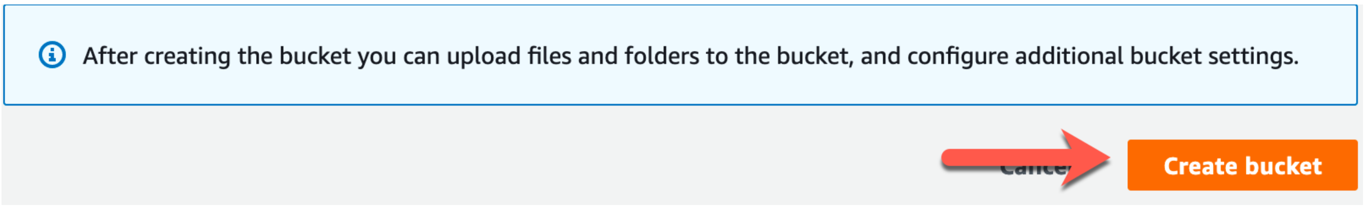
□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **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.

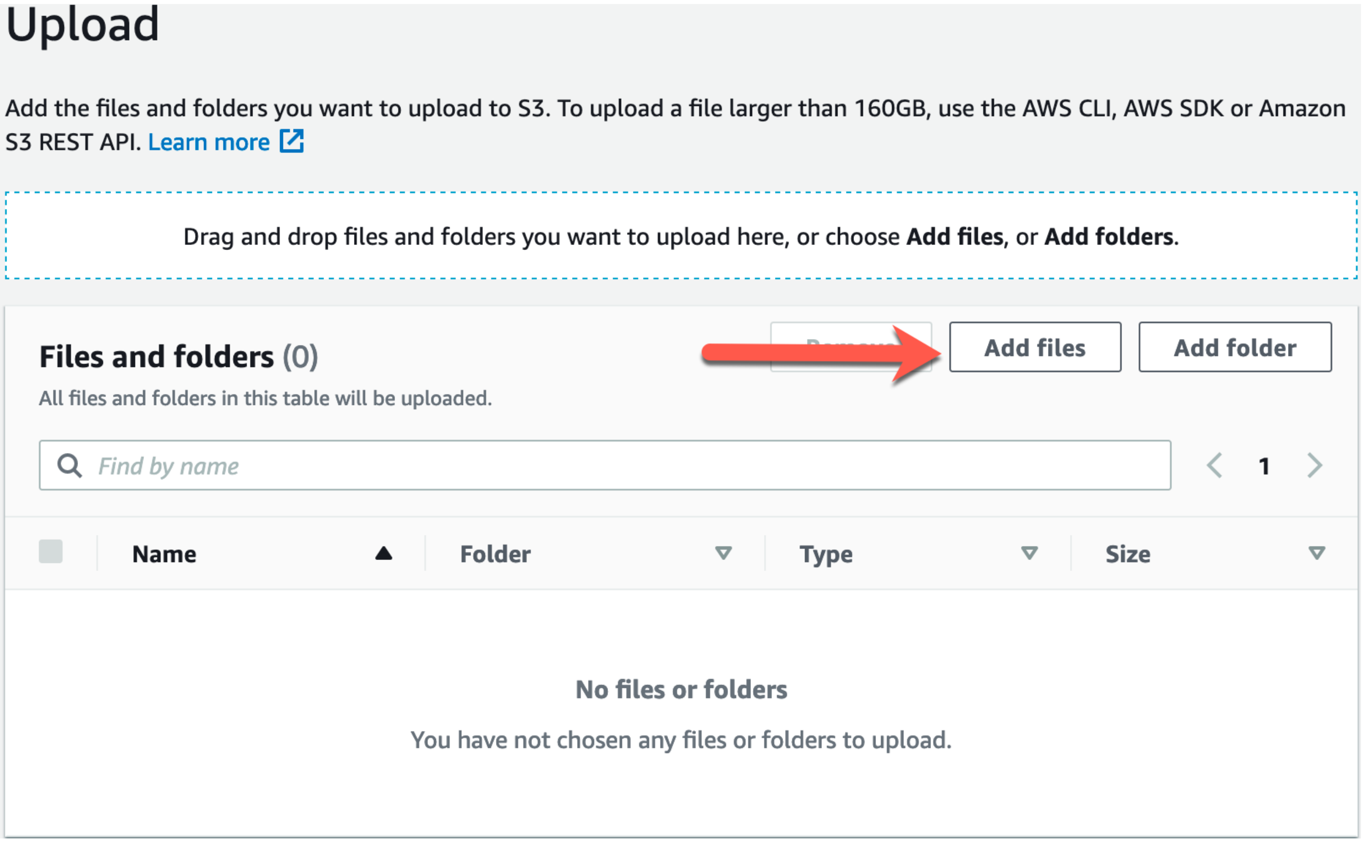
- Multiple security breaches have been caused by unsecured S3 buckets.
- Public access is denied by default; for our ease of use, we will allow public access, but for production-ready storage, it's best to limit access to an as-needed basis TODO: link to privileges.
- The rest of the options can be left as the default values.
- **Tags** are user-defined key-value pairs of information that can help keep track of buckets.
- Scroll to the bottom and click **Create bucket**.



After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

- You will be redirected to the main S3 page; click on the bucket you just created.
- We'll now upload an image file to the newly created bucket. Click the bucket name, then click **Upload**. This will direct you to a new page where you can add files or folders to your bucket.

- Click the **Add files** box, which will allow you to upload local files.



Upload

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (0)

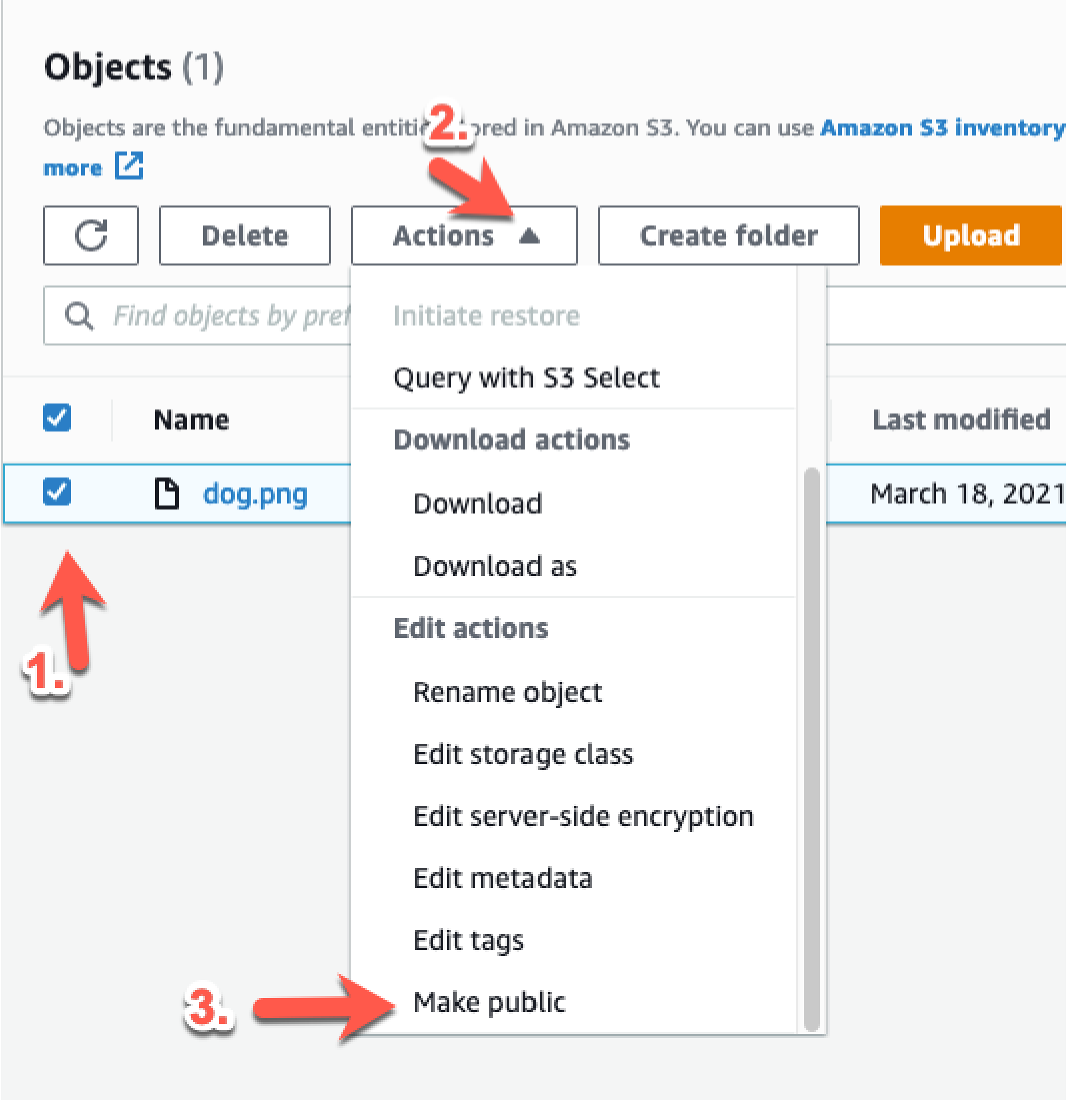
All files and folders in this table will be uploaded.

□	Name ▲	Folder ▽	Type ▽	Size ▽

No files or folders

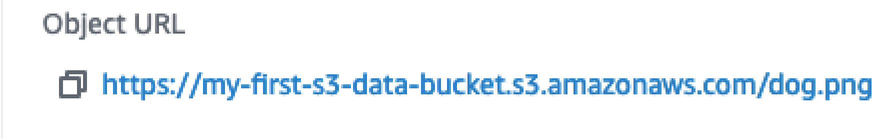
You have not chosen any files or folders to upload.

- Optionally, you can drag in files.
- Once the files have been added, scroll down and click **Upload**.
- After the upload succeeds, click **CLOSE**.
- You will now see your file in the bucket; however, even though we allowed public access to the bucket, the default permission setting for each new file is to deny access to everyone, so it needs to be changed.
- Select the box next to the file, then click **Actions** and select **Make public**.



Objects are the fundamental entiti… ored in Amazon S3. You can use Amazon S3 inventory … more

- From the next screen, click **Make public**.
- Then, click close on the new screen.
- Your file will now be publicly available. To confirm, click on the file to open the **Object overview** page.
- To confirm, click the **Object URL**. If everything is correct, you will be able to download the file.



Object URL

https://my-first-s3-data-bucket.s3.amazonaws.com/dog.png

- You will now be able to publicly access your file!
- **Note:** You will always have the ability to remove public access.