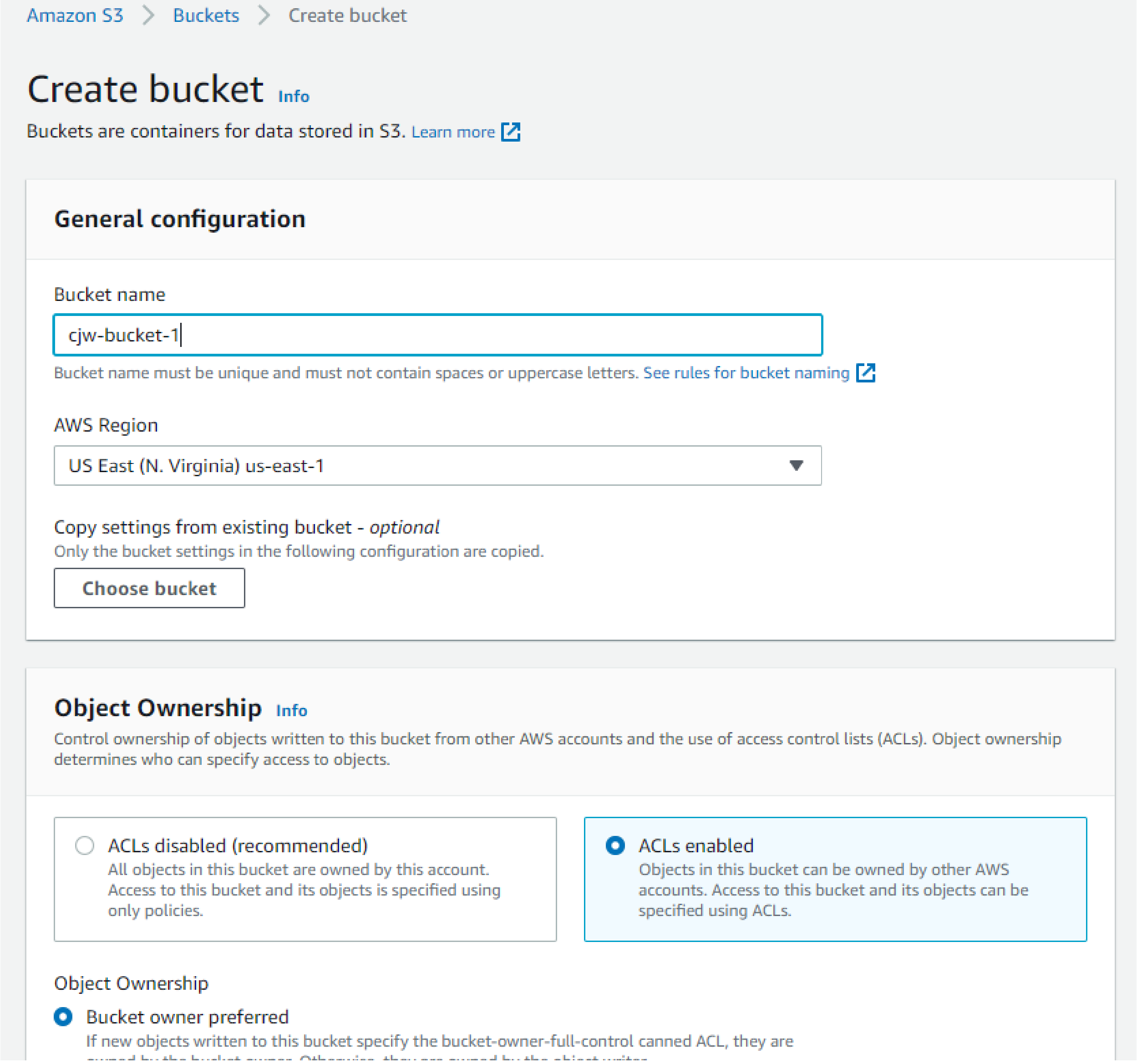
Creating Amazon S3 Buckets, Managing Objects, and Enabling Versioning

Creating a public bucket

1. Upon logging into the AWS console, go into S3 > Create Bucket
2. Remember when naming the bucket, input random string of characters to make the bucket name globally unique. Example: cjw-bucket-1



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

cjw-bucket-1

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.

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.

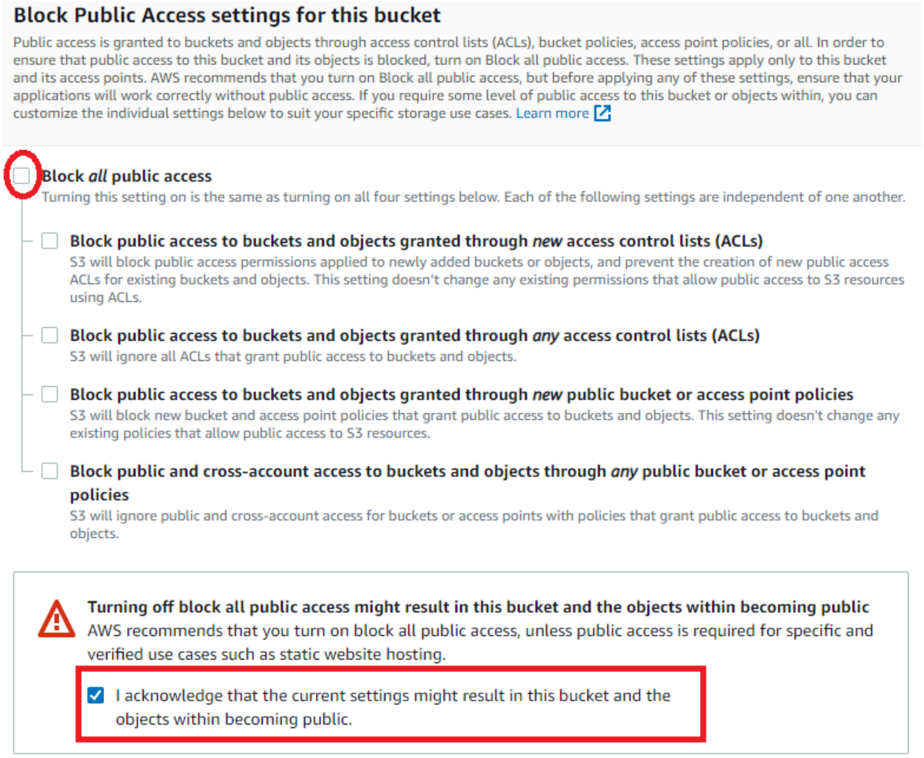
○ ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

● 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 preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

3. Unchecking the "Block all public access" makes this public. Below this, you would have to ack that you understand the bucket is going to be public.



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.

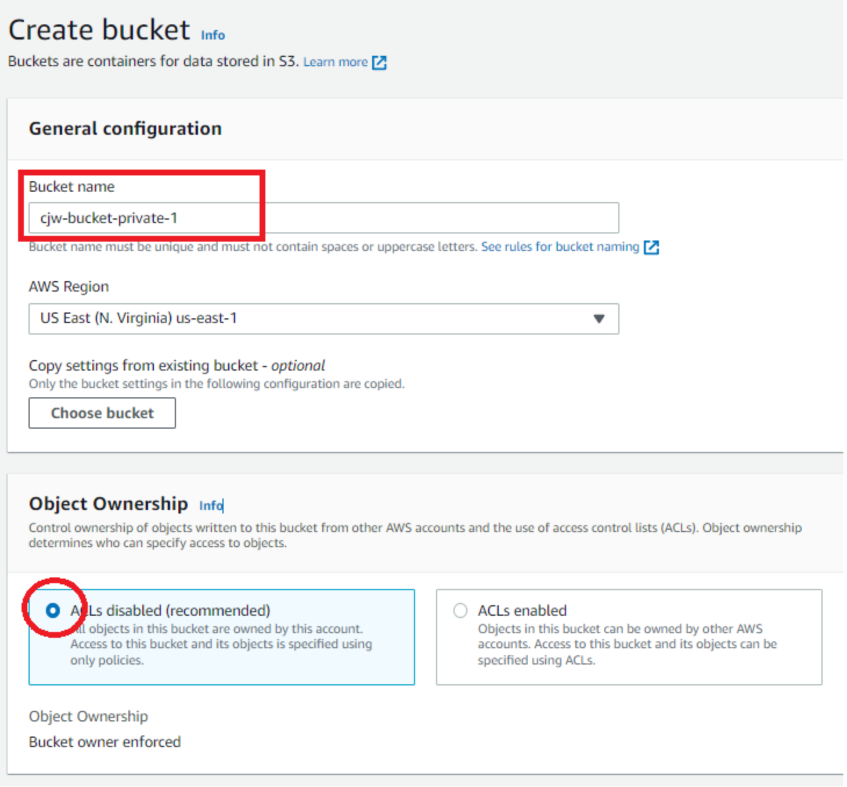
⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

4. Create Bucket

Creating a private bucket

1. When creating a private bucket it is the same as creating a public but a few differences



Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

cjw-bucket-private-1

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.

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.

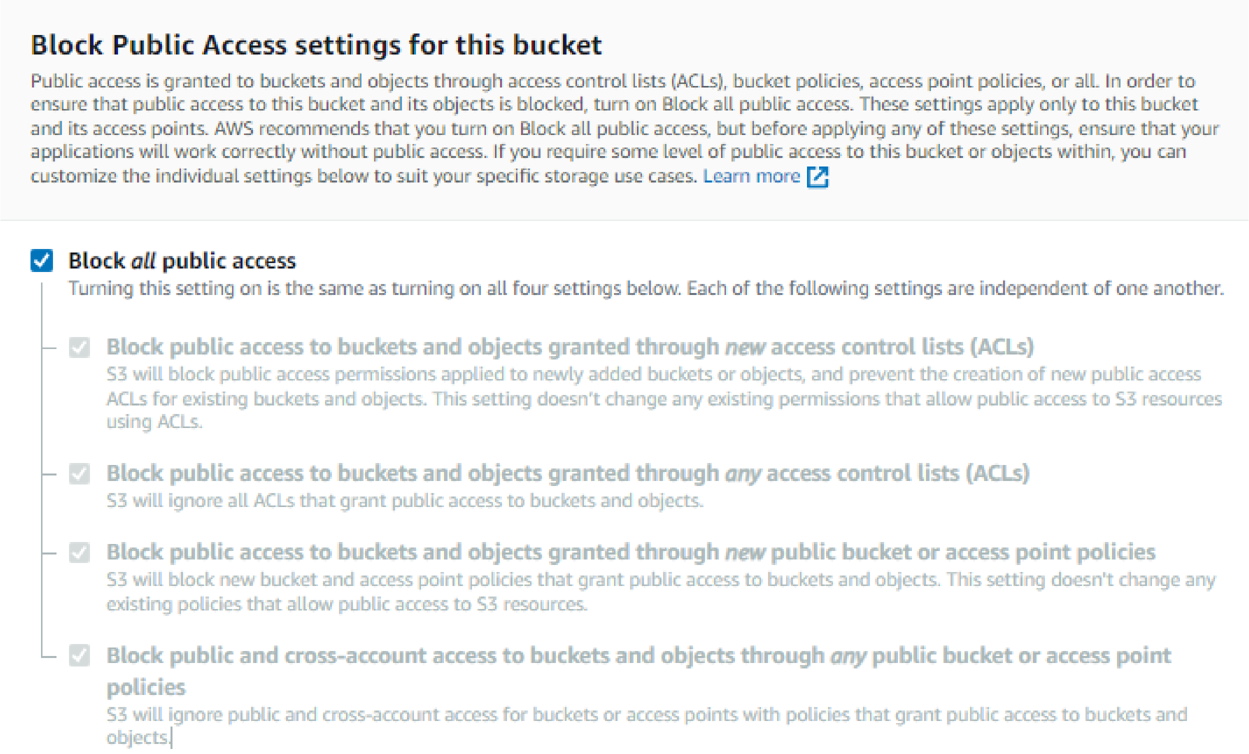
● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ 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

2. Keep the ACLs (Access Control List) disabled
3. Next step you would keep this selected as this will be a private bucket



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.

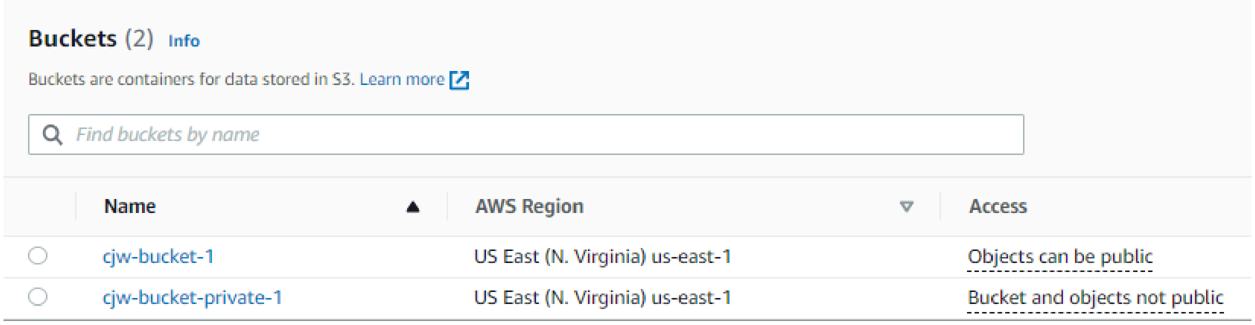
☑ Block public access to buckets and objects granted through *any* access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.

☑ 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.

4. Keep everything else as default
5. Create Bucket

After both the public and private buckets are created they should be shown in the buckets category



Buckets (2) Info

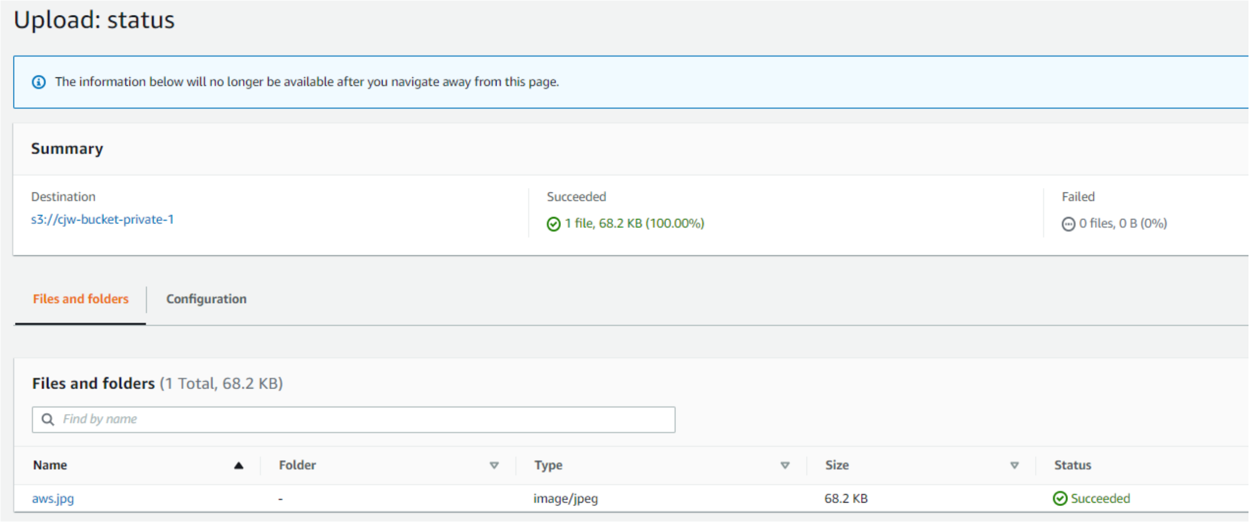
Buckets are containers for data stored in S3. Learn more

Find buckets by name

	Name ▲	AWS Region ▽	Access
○	cjw-bucket-1	US East (N. Virginia) us-east-1	Objects can be public
○	cjw-bucket-private-1	US East (N. Virginia) us-east-1	Bucket and objects not public

Uploading a file to the bucket

1. First we can go into the private bucket
2. Next you want to upload objects, so click the orange "upload" button
3. Once you select the file you want and click upload, it will take you to the upload status



Upload: status

ⓘ The information below will no longer be available after you navigate away from this page.

Summary

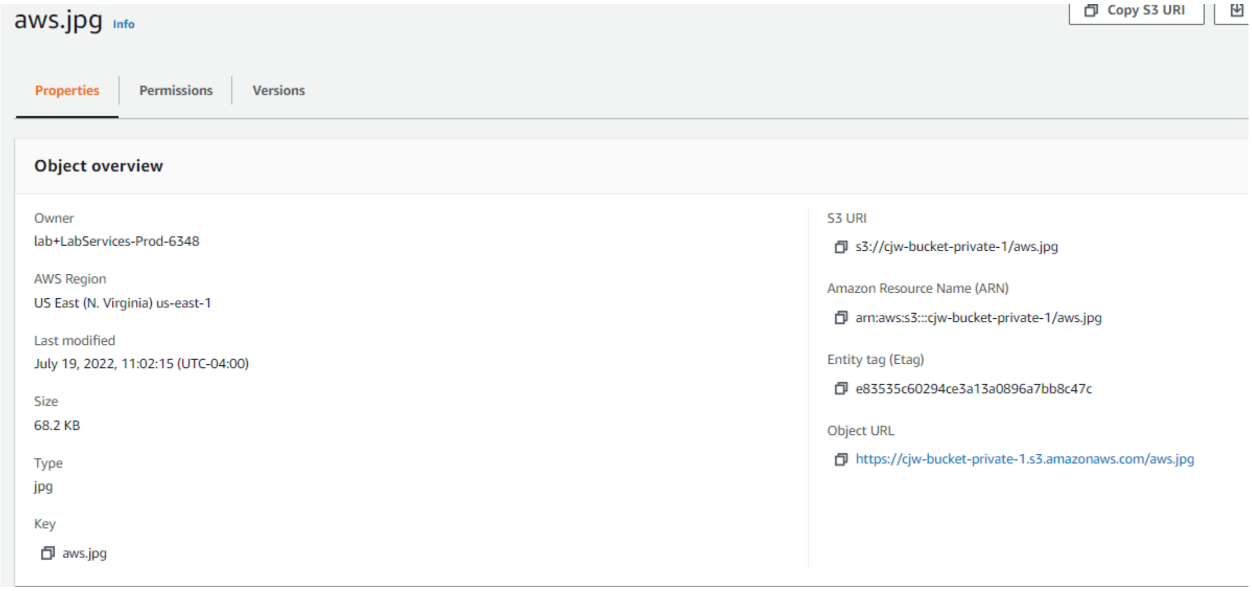
Destination	Succeeded	Failed
s3://cjw-bucket-private-1	✓ 1 file, 68.2 KB (100.00%)	⊖ 0 files, 0 B (0%)

Files and folders (1 Total, 68.2 KB)

Find by name

Name ▲	Folder ▽	Type ▽	Size ▽	Status
aws.jpg	-	image/jpeg	68.2 KB	✓ Succeeded

4. Here you would want to select the hyperlink on the very bottom shown in the picture above. Here it will show you the overview of the object/image you have uploaded.



aws.jpg

Object overview

Owner
lab+LabServices-Prod-6348

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

Last modified
July 19, 2022, 11:02:15 (UTC-04:00)

Size
68.2 KB

Type
jpg

Key
aws.jpg

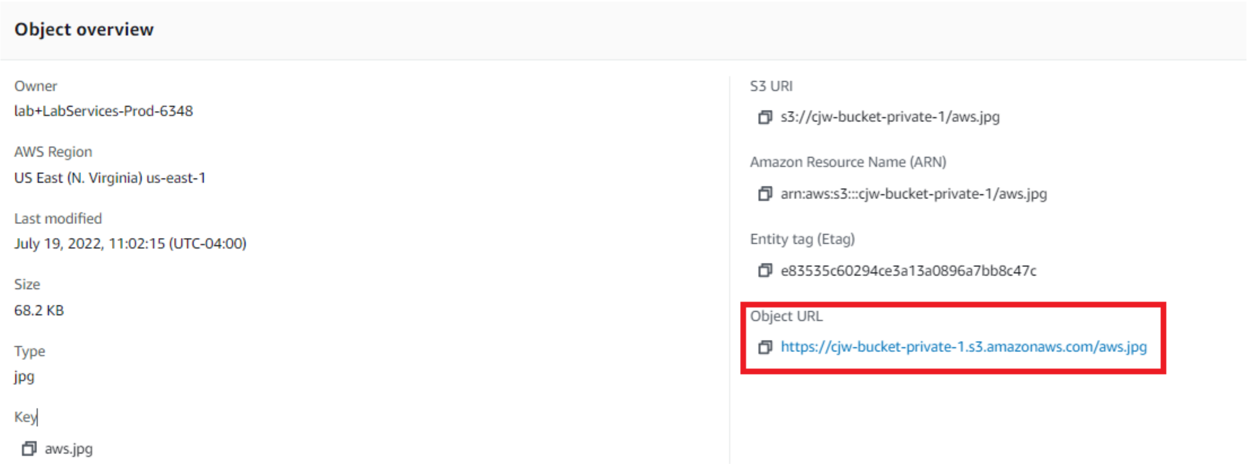
S3 URI
s3://cjw-bucket-private-1/aws.jpg

Amazon Resource Name (ARN)
arn:aws:s3:::cjw-bucket-private-1/aws.jpg

Entity tag (Etag)
e83535c60294ce3a13a0896a7bb8c47c

Object URL
https://cjw-bucket-private-1.s3.amazonaws.com/aws.jpg

5. Down below you see the object URL, click on it.



Object overview

Owner
lab+LabServices-Prod-6348

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

Last modified
July 19, 2022, 11:02:15 (UTC-04:00)

Size
68.2 KB

Type
jpg

Key
aws.jpg

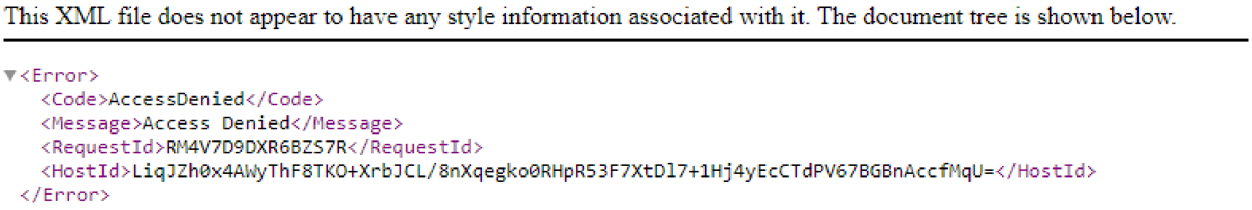
S3 URI
s3://cjw-bucket-private-1/aws.jpg

Amazon Resource Name (ARN)
arn:aws:s3:::cjw-bucket-private-1/aws.jpg

Entity tag (Etag)
e83535c60294ce3a13a0896a7bb8c47c

Object URL
https://cjw-bucket-private-1.s3.amazonaws.com/aws.jpg

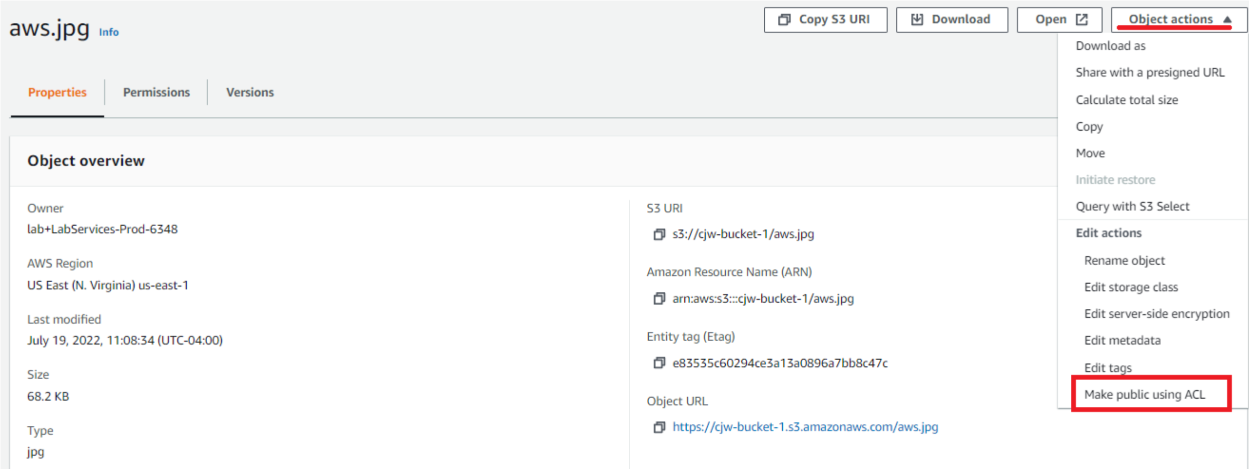
6. Once you click on it, you will notice that you have access denied because it is a private bucket



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>RM4V7D9DXR6BZS7R</RequestId>
   <HostId>LiqJZh0x4AWyThF8TKO+XrbJCL/8nXqegko0RHpR53F7XtDl7+1Hj4yEcCTdPV67BGBnAccfMqU=</HostId>
 </Error>
```

7. We can't make this public using the ACL because of the settings we implied to our bucket
8. Repeat sets 1-5 above for the public bucket
9. But you would see when clicking on the Object URL… It still gives us the access denied error.
   a. We haven't allowed access to this particular file yet
10. To make this object public, click on object actions on the far right > Make public using ACL



Object overview

Owner
lab+LabServices-Prod-6348

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

Last modified
July 19, 2022, 11:08:34 (UTC-04:00)

Size
68.2 KB

Type
jpg

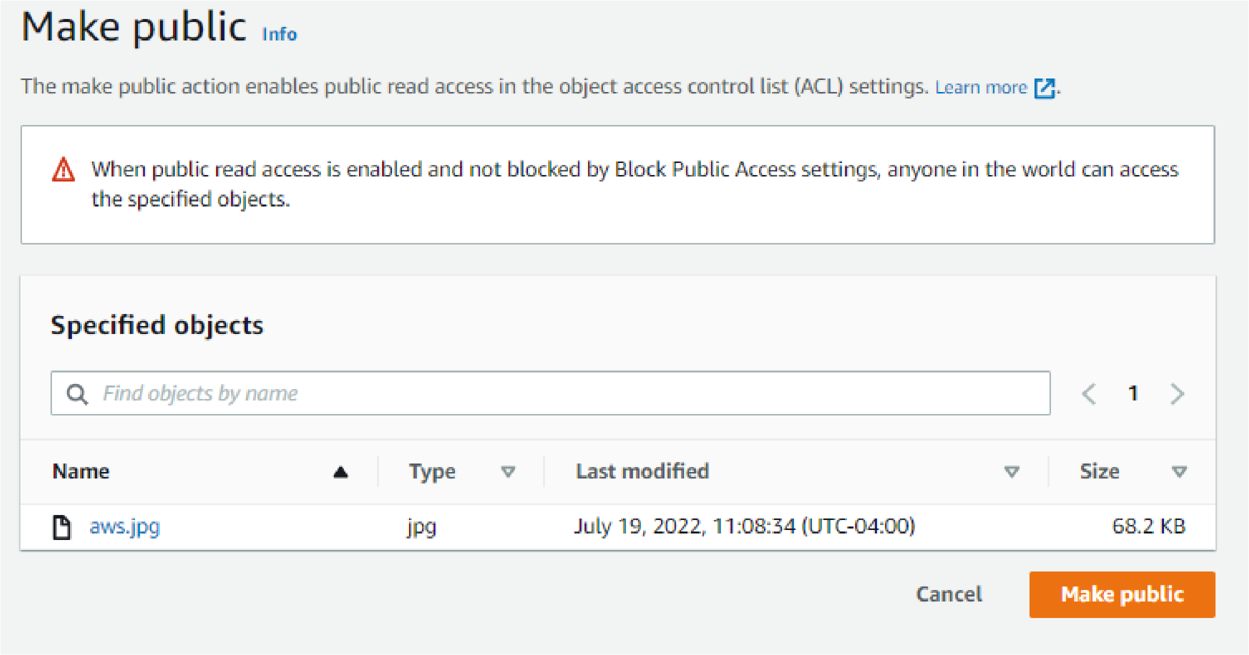
S3 URI
s3://cjw-bucket-1/aws.jpg

Amazon Resource Name (ARN)
arn:aws:s3:::cjw-bucket-1/aws.jpg

Entity tag (Etag)
e83535c60294ce3a13a0896a7bb8c47c

Object URL
https://cjw-bucket-1.s3.amazonaws.com/aws.jpg

11. Once in there click on the orange "Make Public"



Make public Info

The make public action enables public read access in the object access control list (ACL) settings. Learn more.

⚠ When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

Specified objects

Name	Type	Last modified	Size
aws.jpg	jpg	July 19, 2022, 11:08:34 (UTC-04:00)	68.2 KB

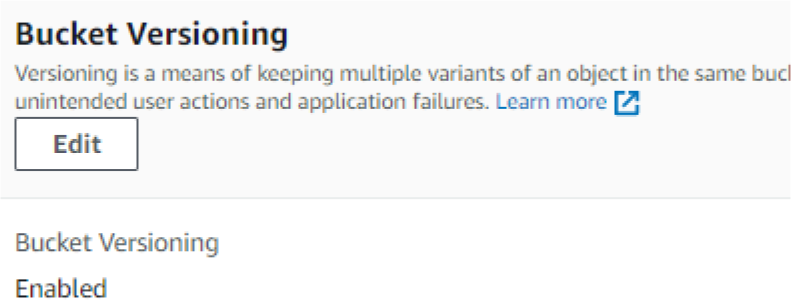
12. Once completed, go back into the object overview on the image we uploaded.
13. Once there, click on the Object URL again and you can see the image loads without any issues

Enable Object Versioning

Versioning-enabled buckets can help you recover objects from accidental deletion or overwrite. For example, if you delete an object, Amazon S3 inserts a delete marker instead of removing the object permanently.

1. First step would be going into the desired bucket
2. From here, on the 6 tabs below the bucket name. Click on "Properties"

3. From there you would click on “Edit” under bucket versioning > And then enable
4. After completing that, you will see the bucket versioning is enabled.



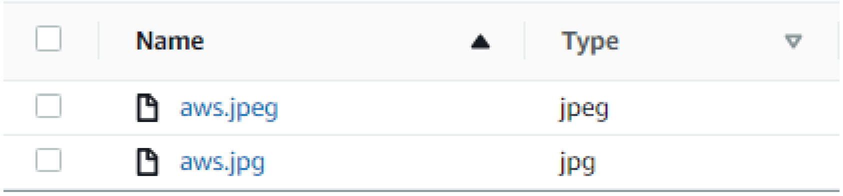
Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucl
unintended user actions and application failures. Learn more

Bucket Versioning

Enabled

5. Now once we upload files with the same name of an existing file, it will just add a new version to that existing file.
6. Repeat steps 1-5 on “Uploading A file to a bucket” (This will only work if it is the same format)



□	Name ▲	Type ▽
□	aws.jpeg	jpeg
□	aws.jpg	jpg

7. Above is an example that will not work for versioning. Once that same file with the same file name is uploaded repeat steps 9-12 on “Uploading A file to a bucket”
8. Once reviewing the objects you would then see there are different versions but in order to see the 2nd file you would have to make that public as well.