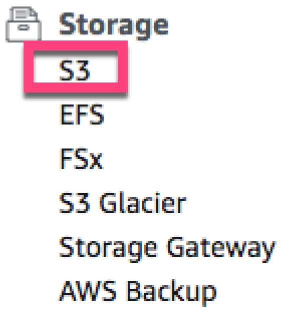
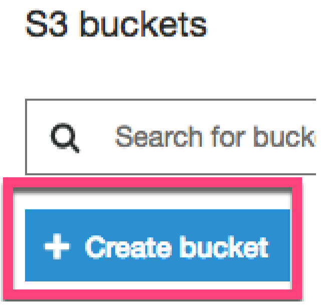
Cloud Storage on S3

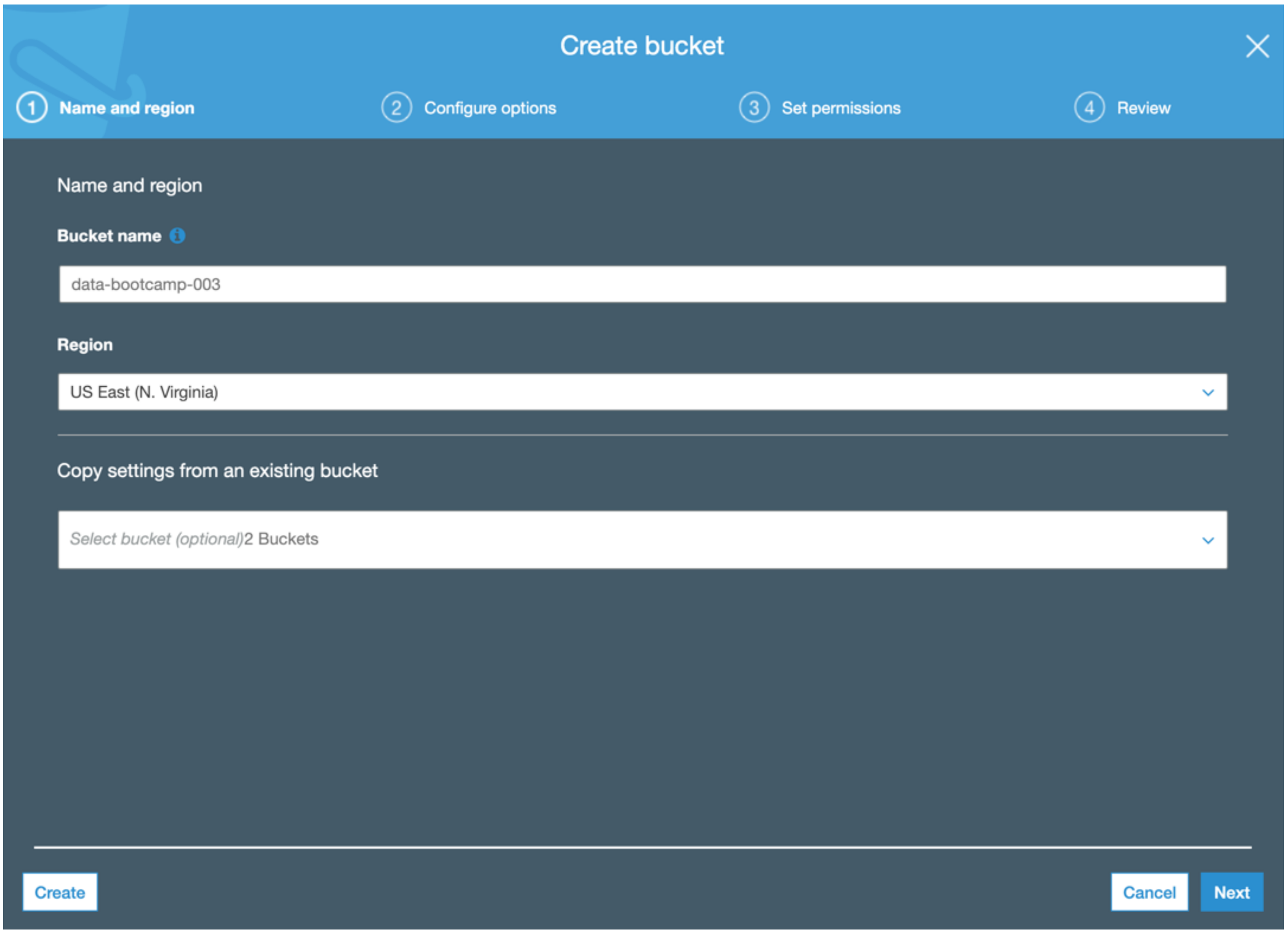
- Go to console.aws.amazon.com and then select S3 under Storage.



- Click "Create bucket".



- 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 `US East (N. Virginia)`. Changing the region will change the object URL used in all examples today.



Name and region

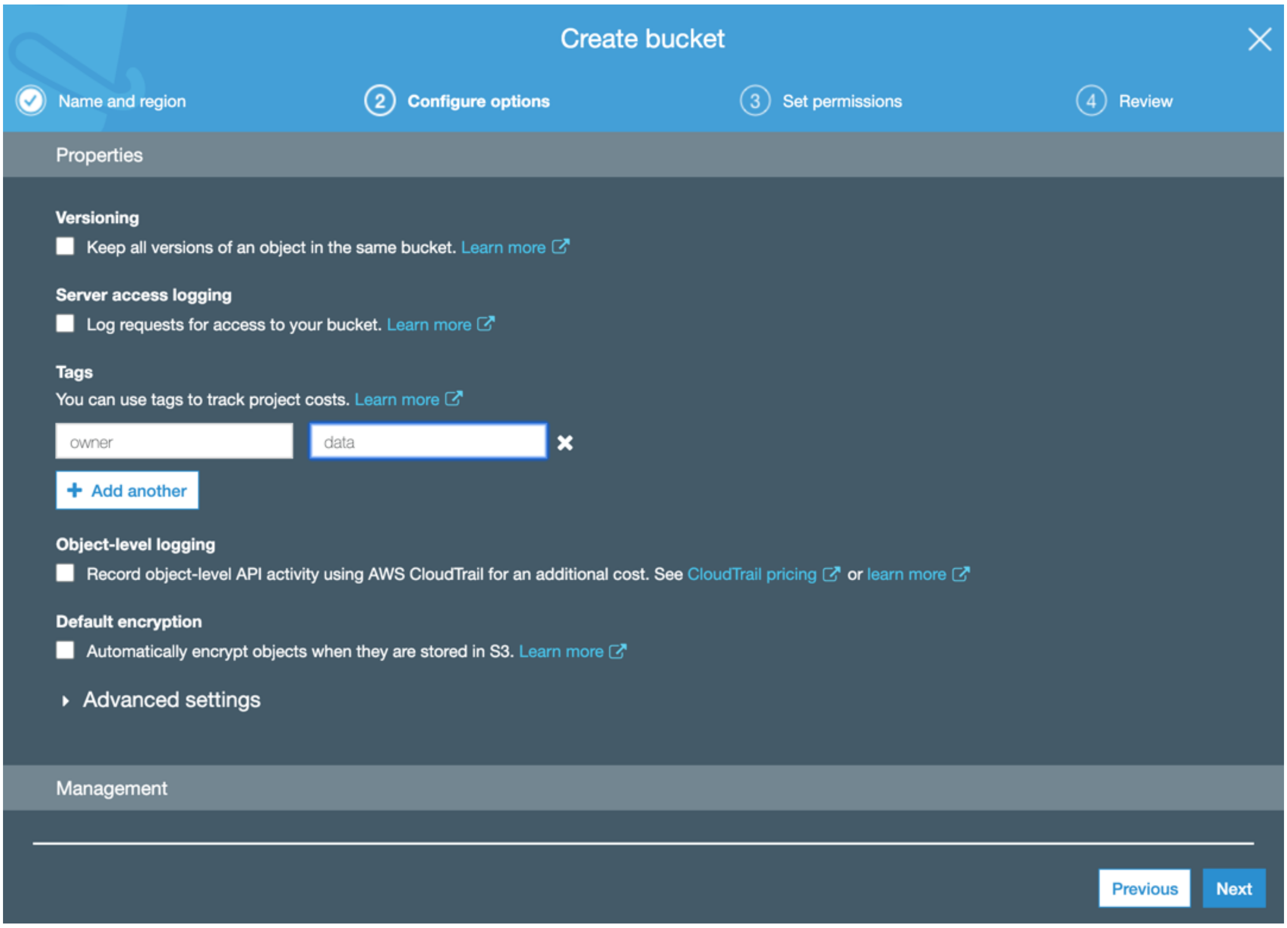
Bucket name: data-bootcamp-003

Region: US East (N. Virginia)

Copy settings from an existing bucket

*Select bucket (optional)*2 Buckets

- Most of the options on the Configure Options tab can stay as the default values.
- Tags are user-defined key-value pairs of information that can help keep track of buckets.
- Click Next.



Properties

Versioning

□ Keep all versions of an object in the same bucket. Learn more

Server access logging

□ Log requests for access to your bucket. Learn more

Tags

You can use tags to track project costs. Learn more

owner	data

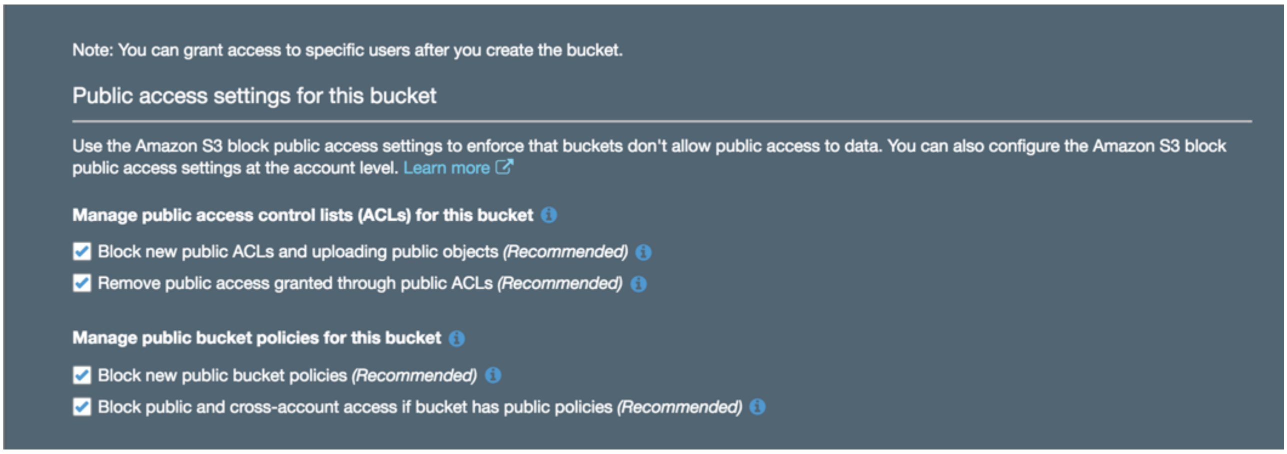
Object-level logging

□ Record object-level API activity using AWS CloudTrail for an additional cost. See CloudTrail pricing or learn more

Default encryption

□ Automatically encrypt objects when they are stored in S3. Learn more

- The Set Permissions page allows us to grant permissions for accessing buckets.
- Many security breaches have been the result of unsecured S3 buckets.
- Public access is denied by default.
  - Leave the boxes checked and click Next.



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

Public access settings for this bucket

Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the account level. Learn more

Manage public access control lists (ACLs) for this bucket

☑ Block new public ACLs and uploading public objects *(Recommended)*

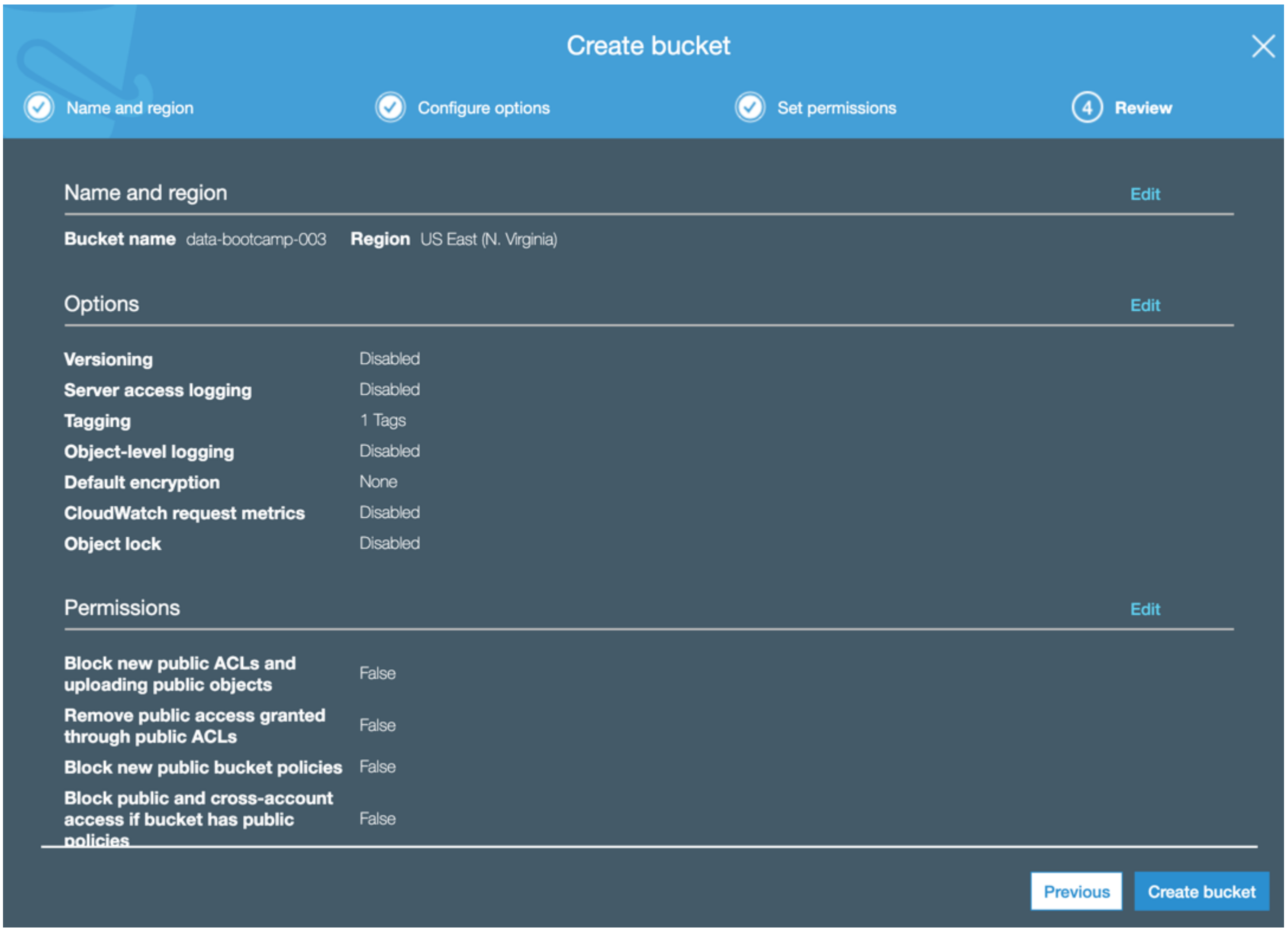
☑ Remove public access granted through public ACLs *(Recommended)*

Manage public bucket policies for this bucket

☑ Block new public bucket policies *(Recommended)*

☑ Block public and cross-account access if bucket has public policies *(Recommended)*

- The Review page is a summary of the bucket configurations. Click "Create bucket." The bucket name now appears in the S3 console.



Name and region

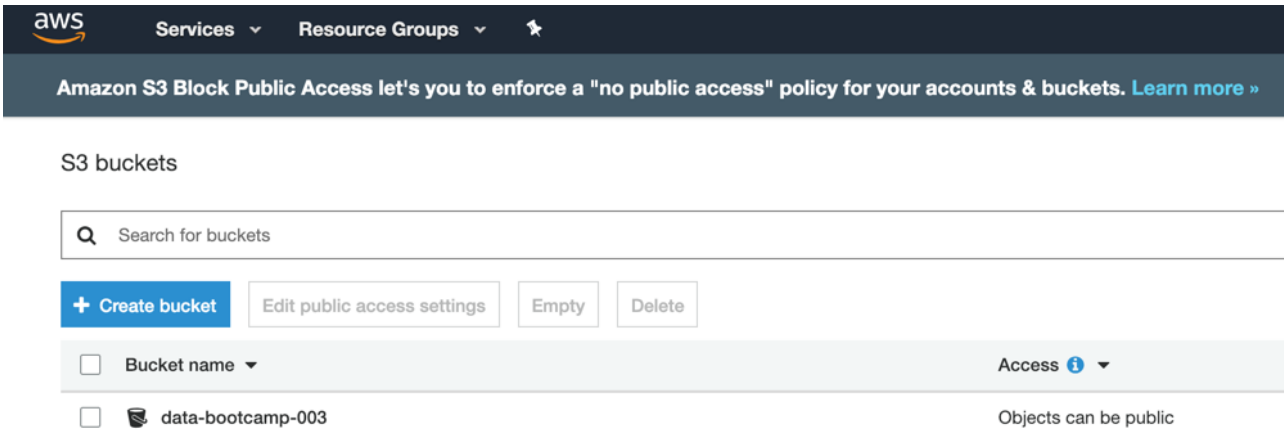
Bucket name data-bootcamp-003 **Region** US East (N. Virginia)

Options

Versioning	Disabled
Server access logging	Disabled
Tagging	1 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled
Object lock	Disabled

Permissions

Block new public ACLs and uploading public objects	False
Remove public access granted through public ACLs	False
Block new public bucket policies	False
Block public and cross-account access if bucket has public policies	False

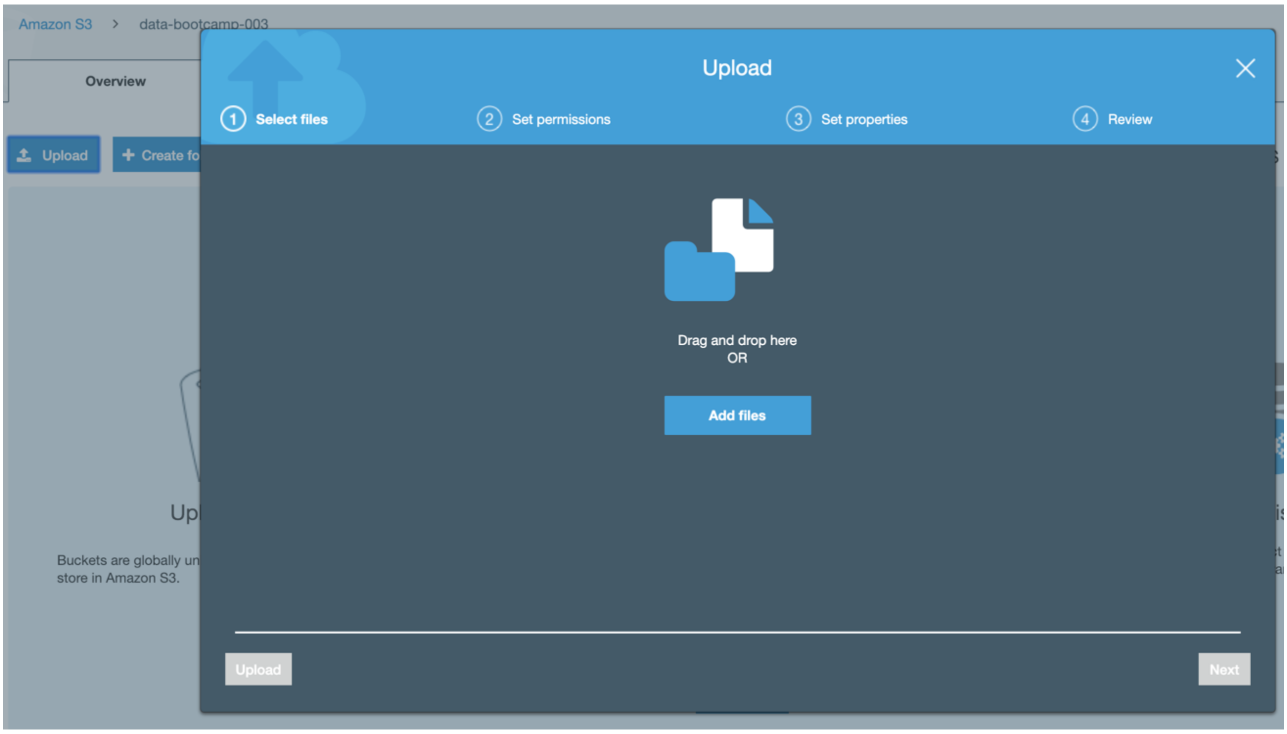


Amazon S3 Block Public Access let's you to enforce a "no public access" policy for your accounts & buckets. Learn more »

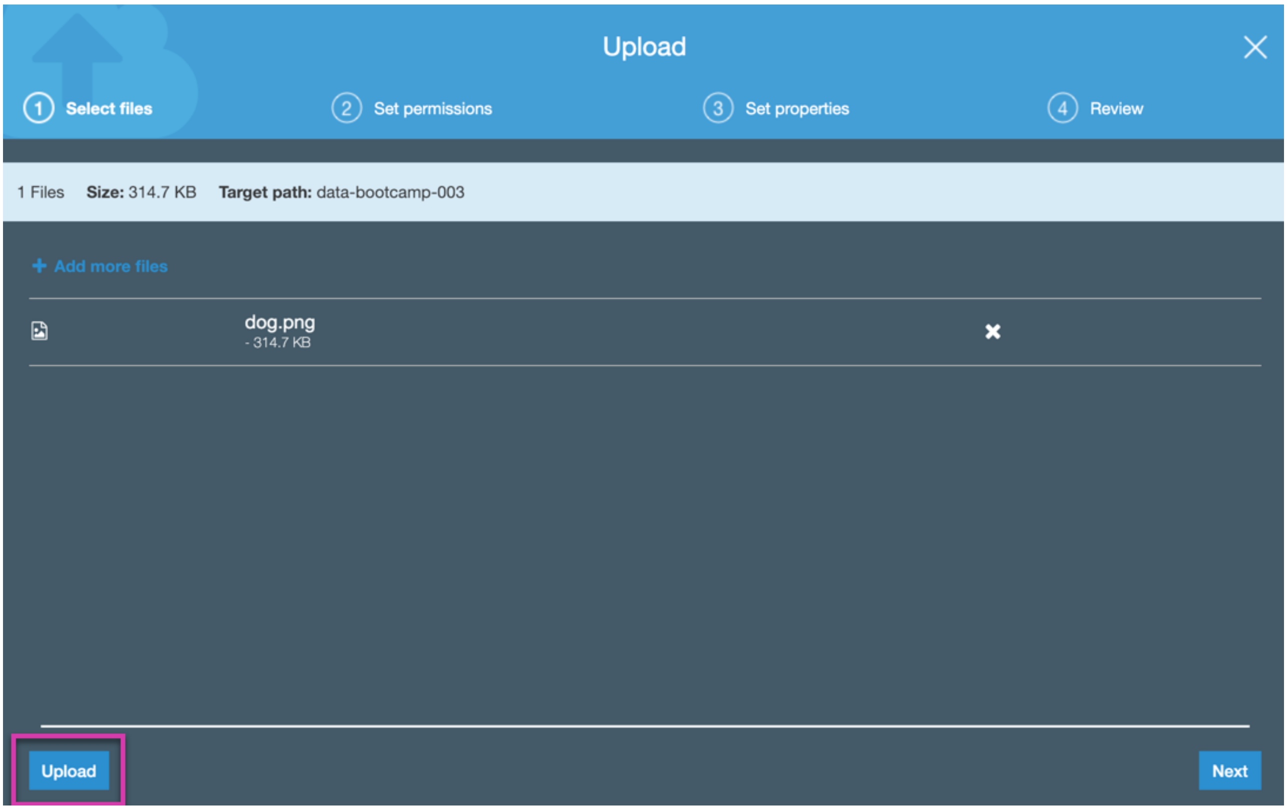
S3 buckets

Bucket name	Access
data-bootcamp-003	Objects can be public

- We'll now upload an image file to the newly created bucket. Click the bucket name and then click Upload.
  - You can drag a file to the screen to upload it..
- Click Upload.



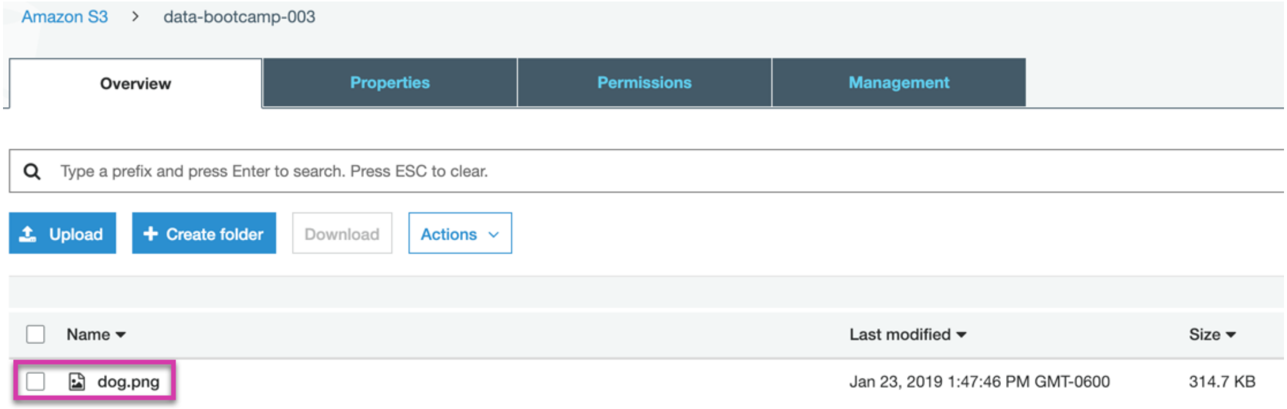
Buckets are globally un
store in Amazon S3.



1 Files **Size:** 314.7 KB **Target path:** data-bootcamp-003

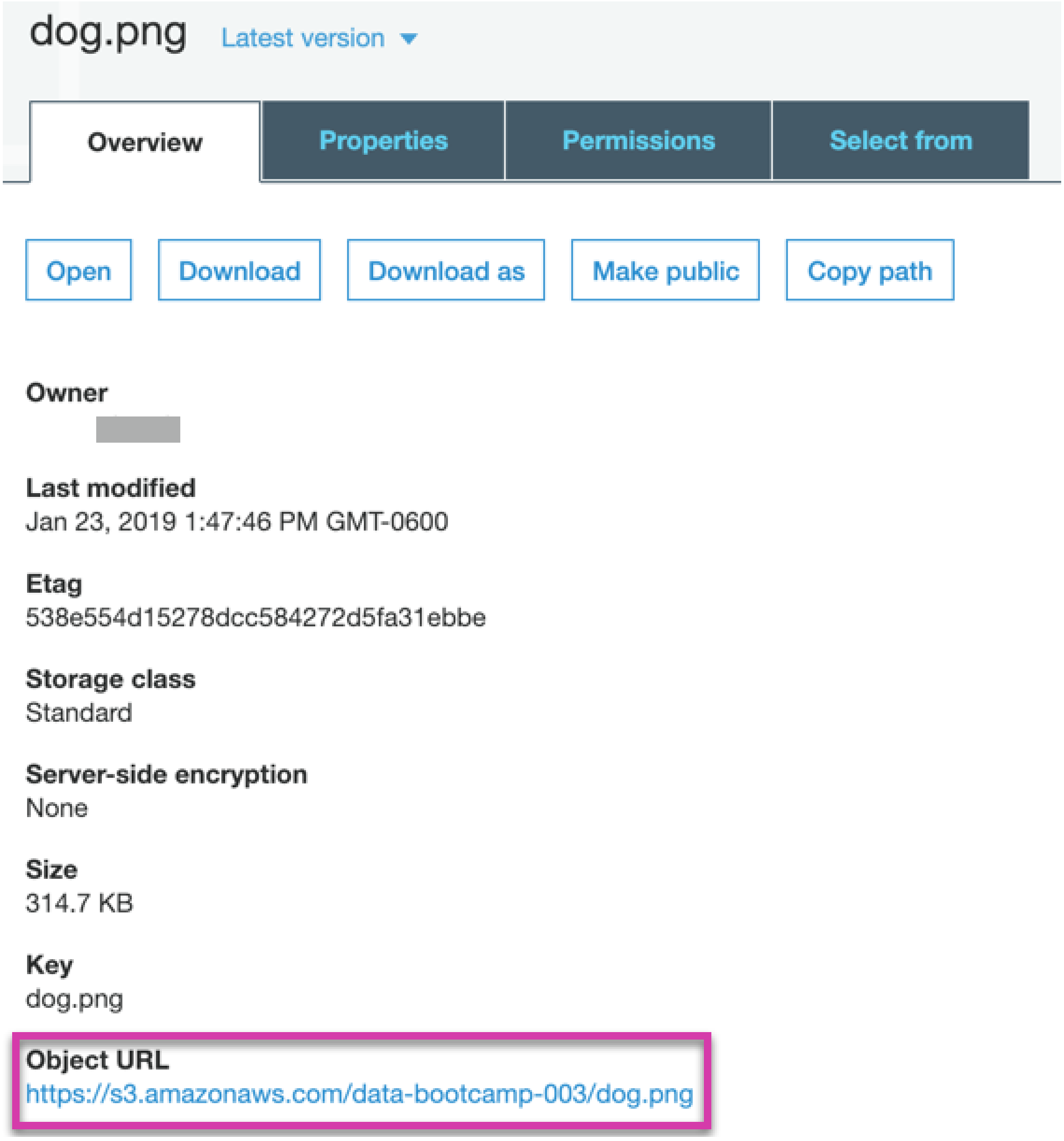
dog.png
- 314.7 KB

- Click the filename.


Amazon S3 > data-bootcamp-003
Overview
Properties
Permissions
Management
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
Download
Actions

□	Name	Last modified	Size
□	dog.png	Jan 23, 2019 1:47:46 PM GMT-0600	314.7 KB

- Explain why clicking the link generates an error message.



Owner
[redacted]

Last modified
Jan 23, 2019 1:47:46 PM GMT-0600

Etag
538e554d15278dcc584272d5fa31ebbe

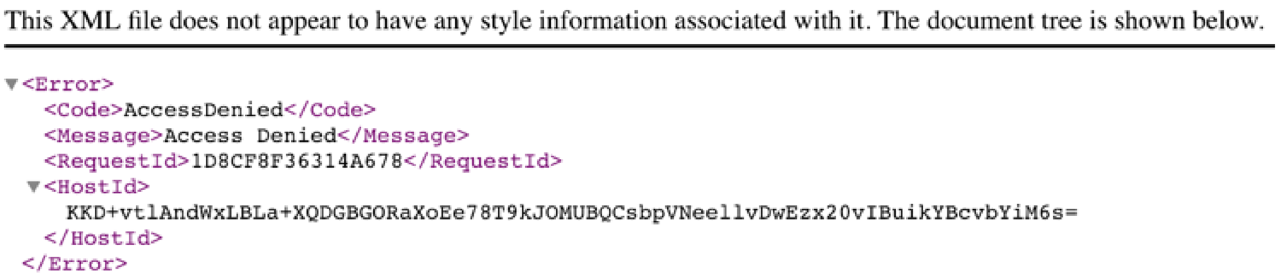
Storage class
Standard

Server-side encryption
None

Size
314.7 KB

Key
dog.png

Object URL
https://s3.amazonaws.com/data-bootcamp-003/dog.png

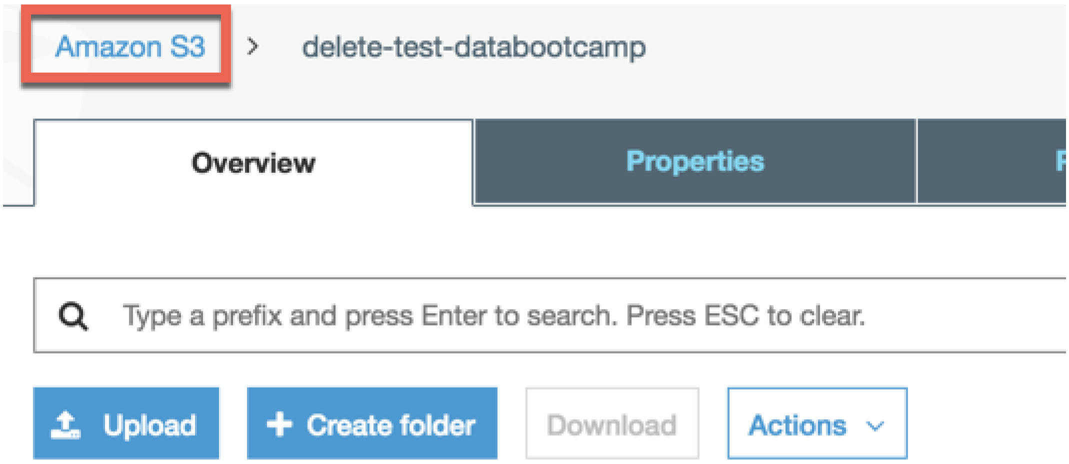


This XML file does not appear to have any style information associated with it. The document tree is shown below.

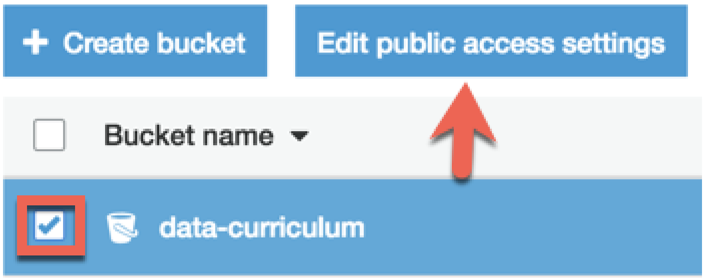
```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>1D8CF8F36314A678</RequestId>
 ▼<HostId>
     KKD+vtlAndWxLBLa+XQDGBGORaXoEe78T9kJOMUBQCsbpVNeellvDwEzx20vIBuikYBcvbYiM6s=
   </HostId>
 </Error>
```

- By default, the permission for the file denies access to everyone, so you need to change it.

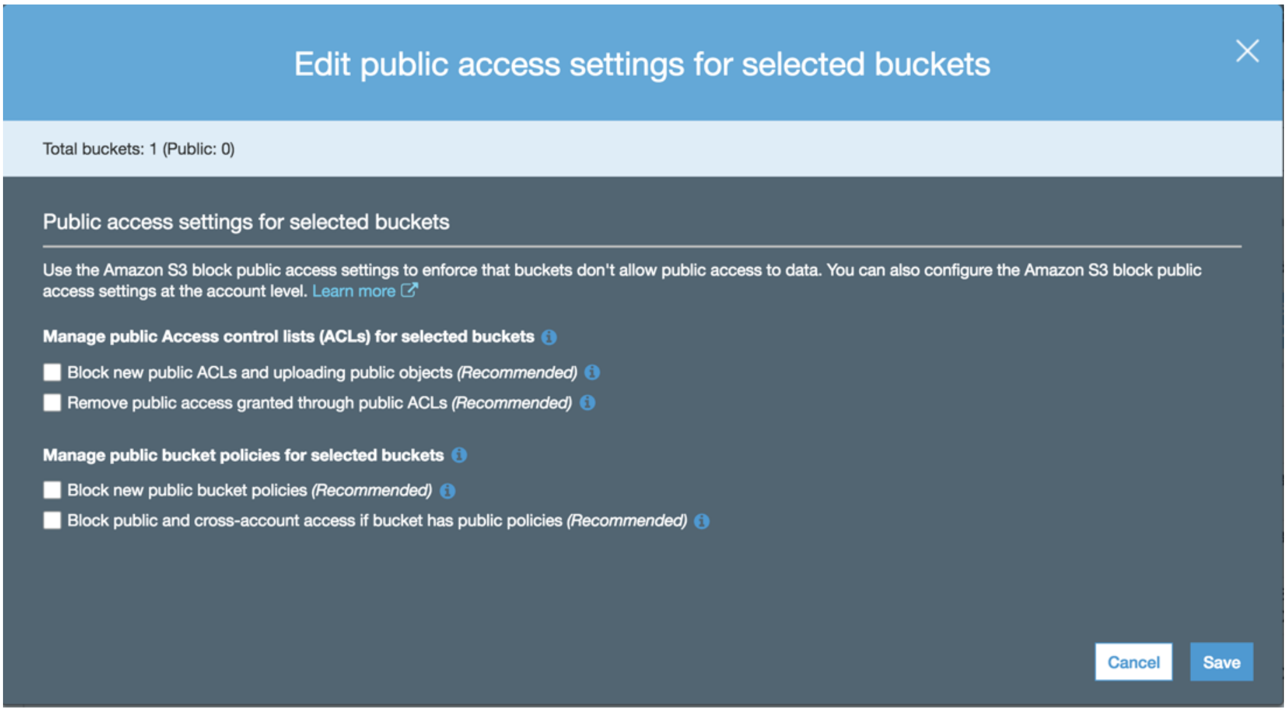
- Navigate back to the dashboard by clicking Amazon S3 on the top left.



- Check the box next to your bucket and click "Edit public access settings."



- Make sure all boxes are unchecked on the next screen. Even though these were checked in the initial setup, they should not be now.



Edit public access settings for selected buckets

Total buckets: 1 (Public: 0)

Public access settings for selected buckets

Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the account level. Learn more

Manage public Access control lists (ACLs) for selected buckets

□ Block new public ACLs and uploading public objects *(Recommended)*

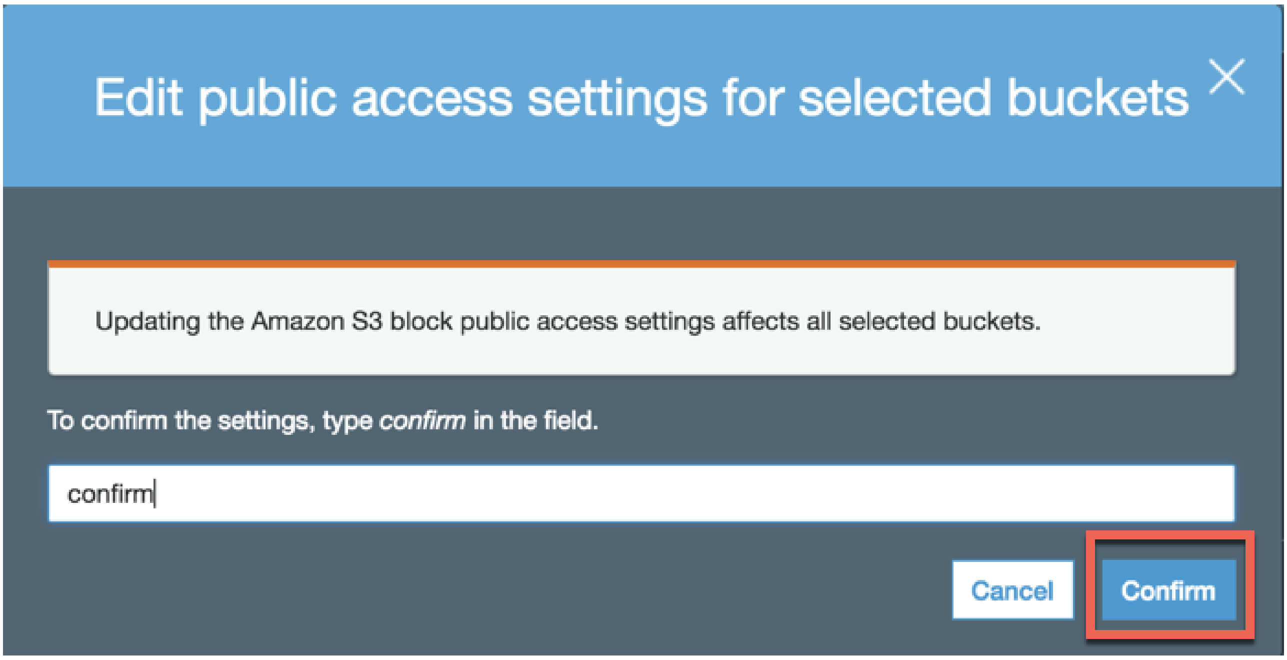
□ Remove public access granted through public ACLs *(Recommended)*

Manage public bucket policies for selected buckets

□ Block new public bucket policies *(Recommended)*

□ Block public and cross-account access if bucket has public policies *(Recommended)*

- Click Save, then type "confirm" and click the Confirm button.



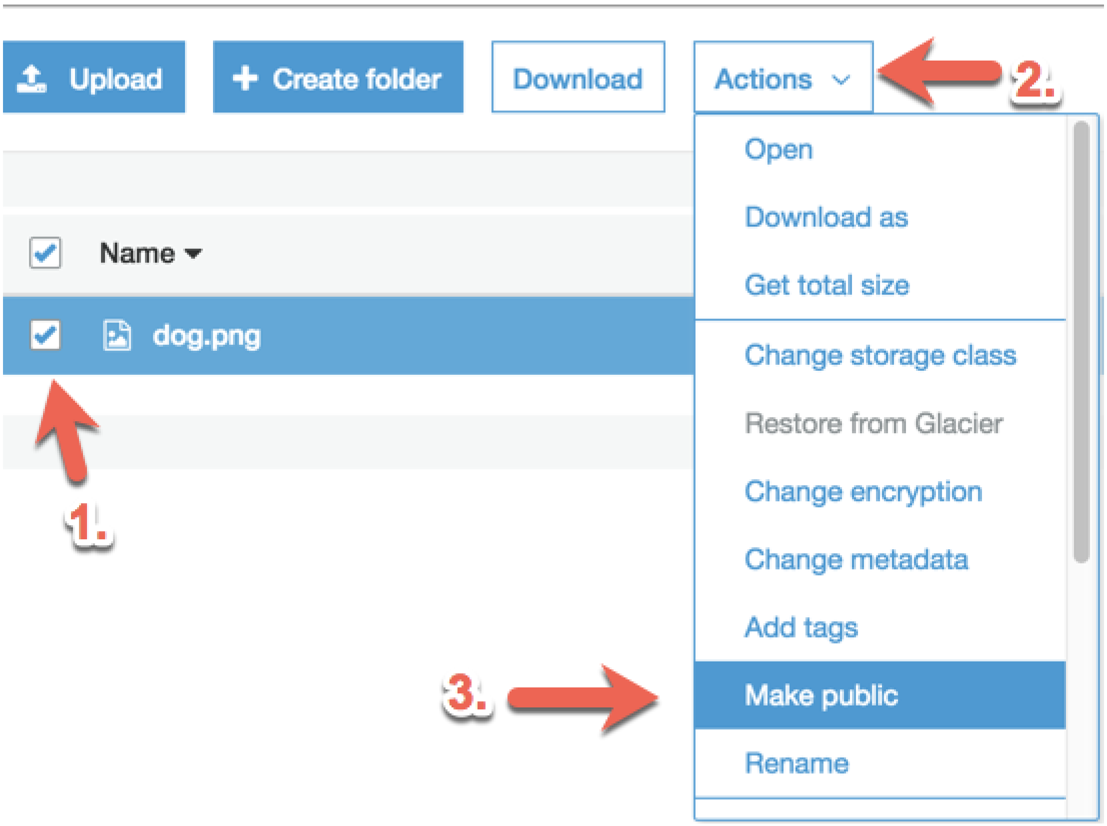
Edit public access settings for selected buckets

Updating the Amazon S3 block public access settings affects all selected buckets.

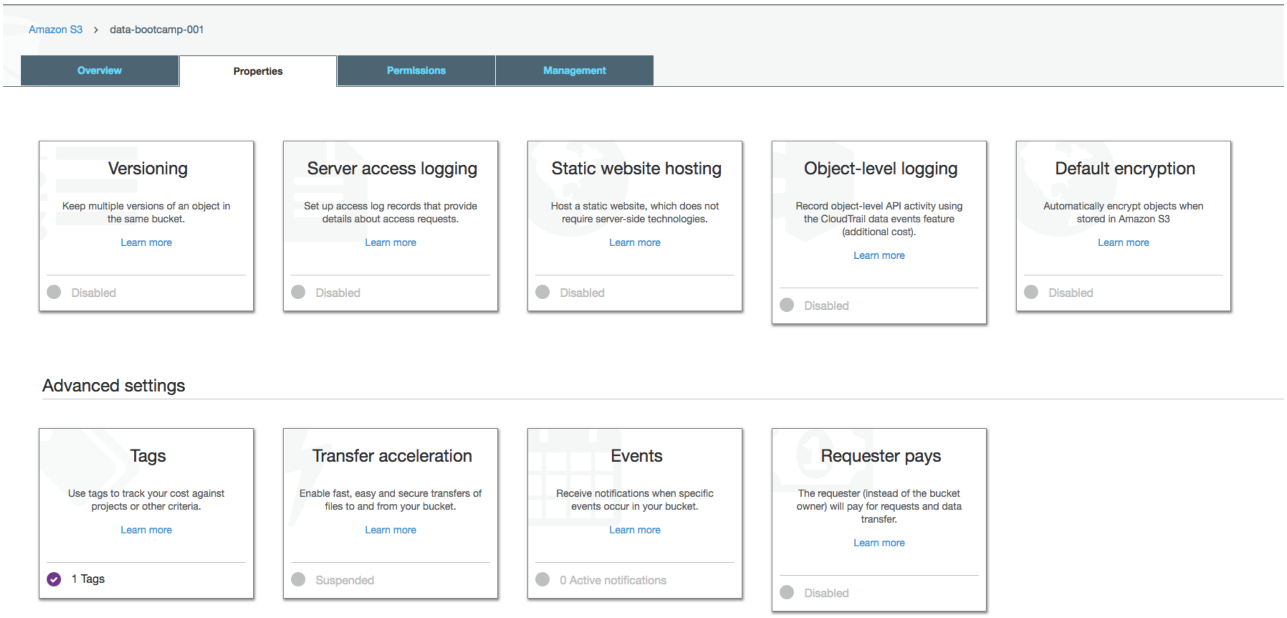
To confirm the settings, type *confirm* in the field.

confirm

- Next, navigate back into your bucket and check the box next to the image. Click the Actions box and select "Make public".



- Now the image will be displayed when you click on the link.
- You can explore various settings at the bucket level and the file level. Use the tabs at the bucket level to explore the available settings, such as tags:



Versioning
Keep multiple versions of an object in the same bucket.
Learn more
● Disabled

Server access logging
Set up access log records that provide details about access requests.
Learn more
● Disabled

Static website hosting
Host a static website, which does not require server-side technologies.
Learn more
● Disabled

Object-level logging
Record object-level API activity using the CloudTrail data events feature (additional cost).
Learn more
● Disabled

Default encryption
Automatically encrypt objects when stored in Amazon S3
Learn more
● Disabled

Advanced settings

Tags
Use tags to track your cost against projects or other criteria.
Learn more
✓ 1 Tags

Transfer acceleration
Enable fast, easy and secure transfers of files to and from your bucket.
Learn more
● Suspended

Events
Receive notifications when specific events occur in your bucket.
Learn more
● 0 Active notifications

Requester pays
The requester (instead of the bucket owner) will pay for requests and data transfer.
Learn more
● Disabled

- **Note:** You can remove public access at any time by repeating the preceding steps and checking all the boxes in Edit public access settings.