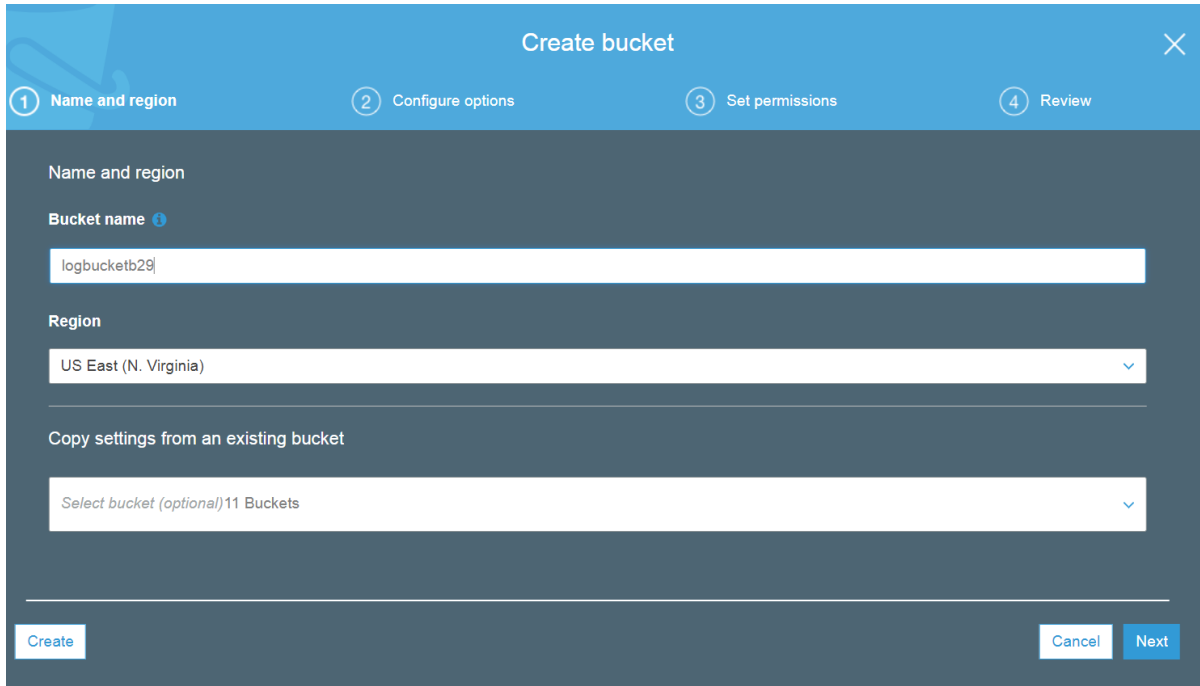


Lab manual – S3 – Simple Storage Service

Steps

1. Create log bucket
2. Create data bucket
3. Upload the File

1. Create log bucket

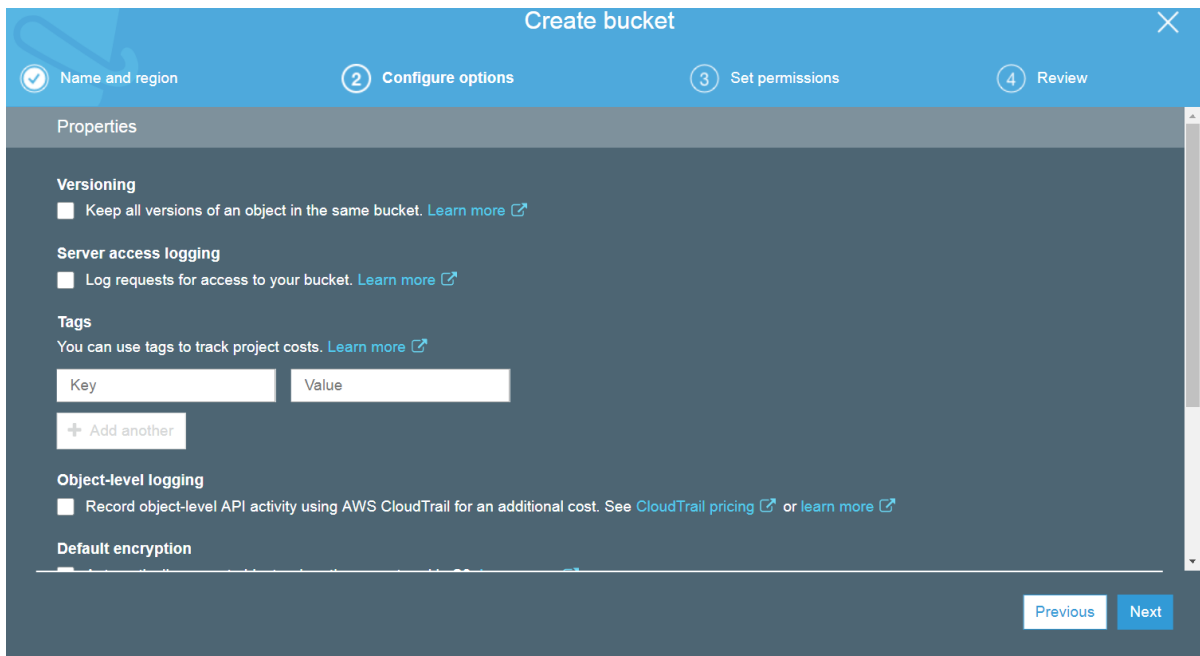


The screenshot shows the 'Create bucket' wizard in the AWS S3 console. The title bar is blue with a close button (X) on the right. Below the title bar is a progress bar with four steps: 1. Name and region (active), 2. Configure options, 3. Set permissions, and 4. Review. The main content area is dark blue and contains the following fields:

- Name and region**
 - Bucket name**: A text input field containing 'logbucketb29'.
 - Region**: A dropdown menu showing 'US East (N. Virginia)'.
 - Copy settings from an existing bucket**: A dropdown menu showing 'Select bucket (optional) 11 Buckets'.

At the bottom of the form are three buttons: 'Create' (disabled), 'Cancel', and 'Next' (active).

Click "NEXT".



The screenshot shows the 'Create bucket' wizard in the AWS S3 console, Step 2: Configure options. The title bar is blue with a close button (X) on the right. Below the title bar is a progress bar with four steps: 1. Name and region (completed), 2. Configure options (active), 3. Set permissions, and 4. Review. The main content area is dark blue and contains the following sections:

- Properties**
 - Versioning**: A checkbox labeled 'Keep all versions of an object in the same bucket. Learn more' is unchecked.
 - Server access logging**: A checkbox labeled 'Log requests for access to your bucket. Learn more' is unchecked.
 - Tags**: A section with the text 'You can use tags to track project costs. Learn more'. It contains two input fields labeled 'Key' and 'Value', and a button labeled '+ Add another'.
 - Object-level logging**: A checkbox labeled 'Record object-level API activity using AWS CloudTrail for an additional cost. See CloudTrail pricing or learn more' is unchecked.
 - Default encryption**: A section with a progress bar and a button labeled 'Learn more'.

At the bottom of the form are two buttons: 'Previous' and 'Next' (active).

Click "NEXT"

Create bucket

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

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)

Manage system permissions

Do not grant Amazon S3 Log Delivery group write access to this bucket

Do not grant Amazon S3 Log Delivery group write access to this bucket

Grant Amazon S3 Log Delivery group write access to this bucket

Previous Next

Select "Grant Amazon S3 log" for this bucket.

Create bucket

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

Options Edit

Versioning	Disabled
Server access logging	Disabled
Tagging	0 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled
Object lock	Disabled

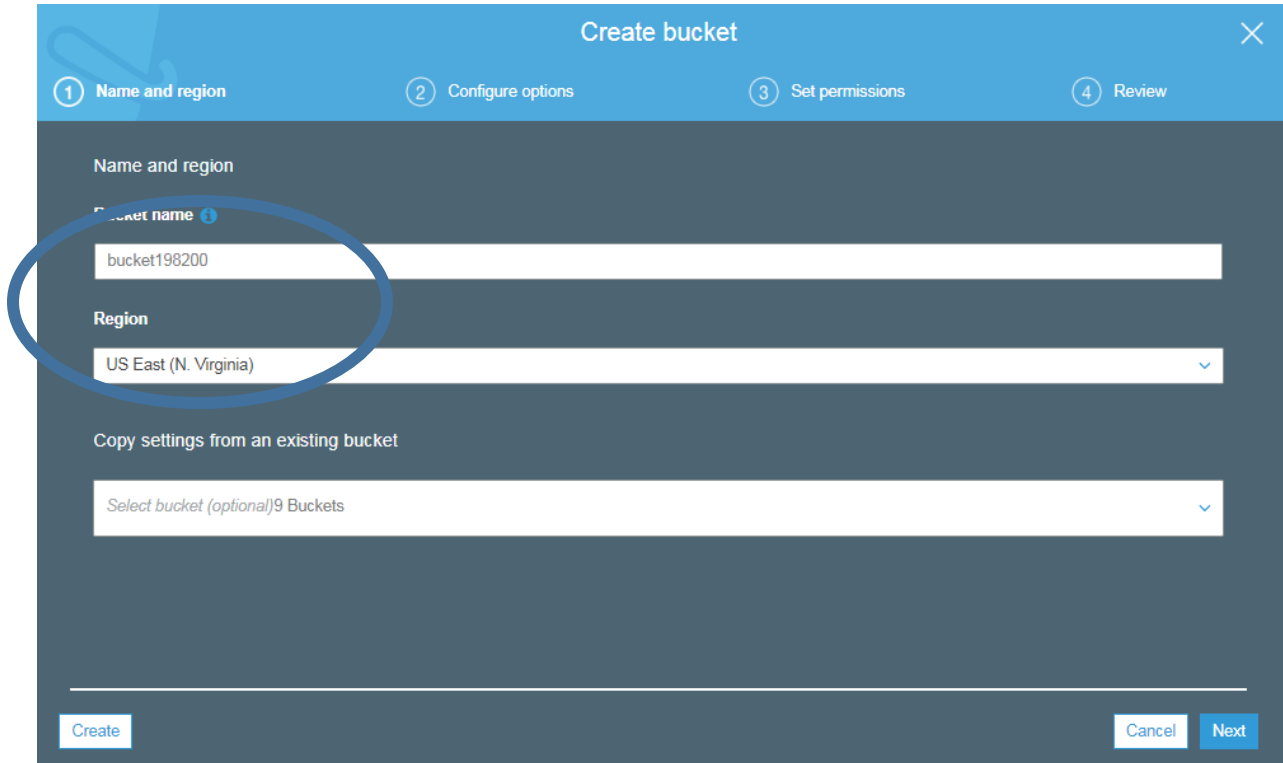
Permissions Edit

Block new public ACLs and uploading public objects	False
Remove public access granted through public ACLs	False
Block new public bucket policies	True

Previous Create bucket

Click on 'create Bucket.

2. Create data bucket



Create bucket

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

Name and region

Bucket name *i*

bucket198200

Region

US East (N. Virginia)

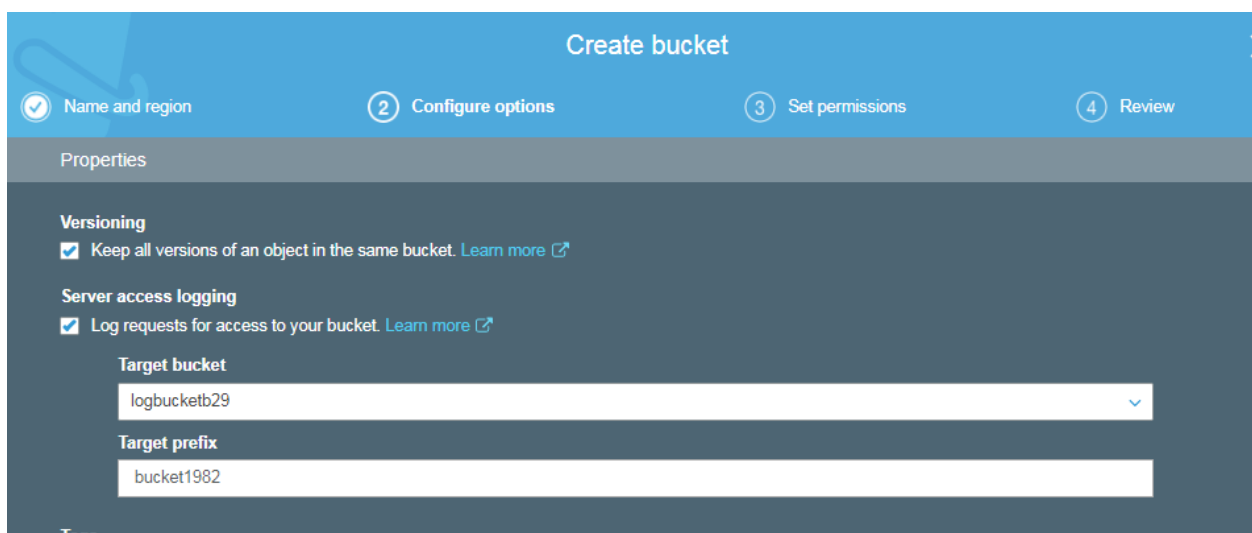
Copy settings from an existing bucket

Select bucket (optional) 9 Buckets

Create Cancel Next

Note:- The Data Bucket and Log Bucket should be in the same Region

Click **“NEXT”**



Create bucket

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

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](#)

Target bucket

logbucketb29

Target prefix

bucket1982

Create bucket

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

Tags

You can use tags to track project costs. [Learn more](#)

Key Value

+ Add another

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](#)

► Advanced settings

Management

CloudWatch request metrics

☐ Monitor requests in your bucket for an additional cost. See [CloudWatch pricing](#) or [learn more](#)

Previous Next

Click “NEXT”

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)**
- ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**

– ☒ **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.

– ☒ **Block public and cross-account access to buckets and objects through *any* public bucket policies**
S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.

Manage system permissions

Do not grant Amazon S3 Log Delivery group write access to this bucket

Previous Next

Click **“NEXT”**

Create bucket

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

Tagging 0 Tags

Object-level logging Disabled

Default encryption None

CloudWatch request metrics Disabled

Object lock Disabled

Permissions Edit

Block *all* public access Off

– Block public access to buckets and objects granted through *new* access control lists (ACLs) Off

– Block public access to buckets and objects granted through *any* access control lists (ACLs) Off

– Block public access to buckets and objects granted through *new* public bucket policies On

– Block public and cross-account access to buckets and objects through *any* public bucket policies On

Previous Create bucket

Click **“Create bucket”**

Output:

Q

Search for buckets

All access types



+ Create bucket

Edit public access settings

Empty

Delete

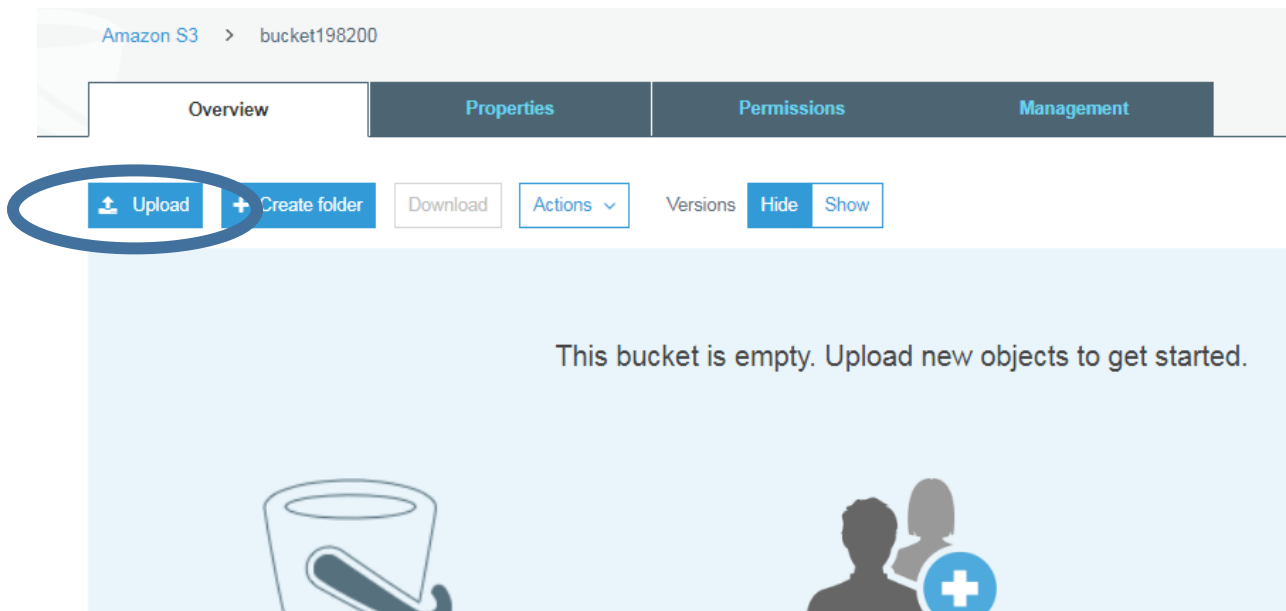
10 Buckets2 Regions

<input type="checkbox"/> Bucket name	Access	Region	Date created
<input type="checkbox"/>  bucket198200	Objects can be public	US East (N. Virginia)	May 28, 2019 9:30:00 PM GMT+0530
<input type="checkbox"/>  cf-templates-1d9xwztox18ty-us-east-1	Objects can be public	US East (N. Virginia)	May 25, 2019 10:00:42

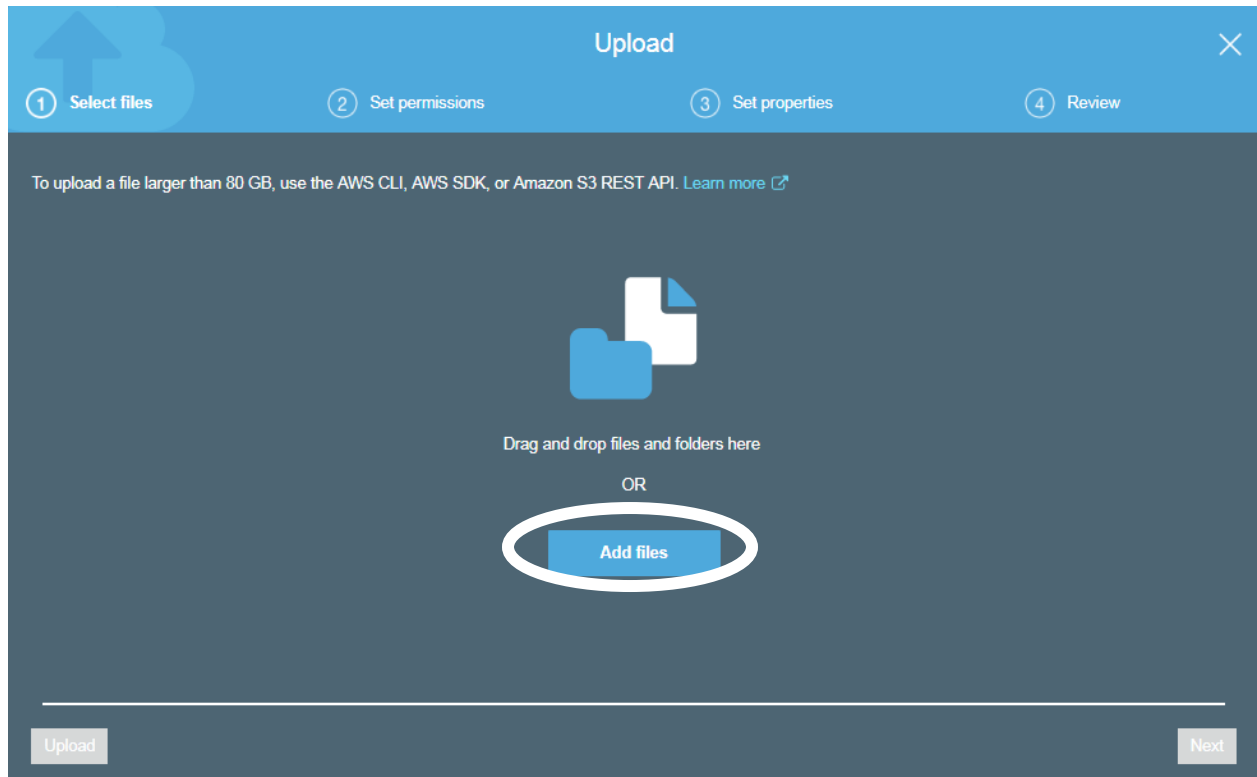
3. Upload the File

Click on the Bucket name

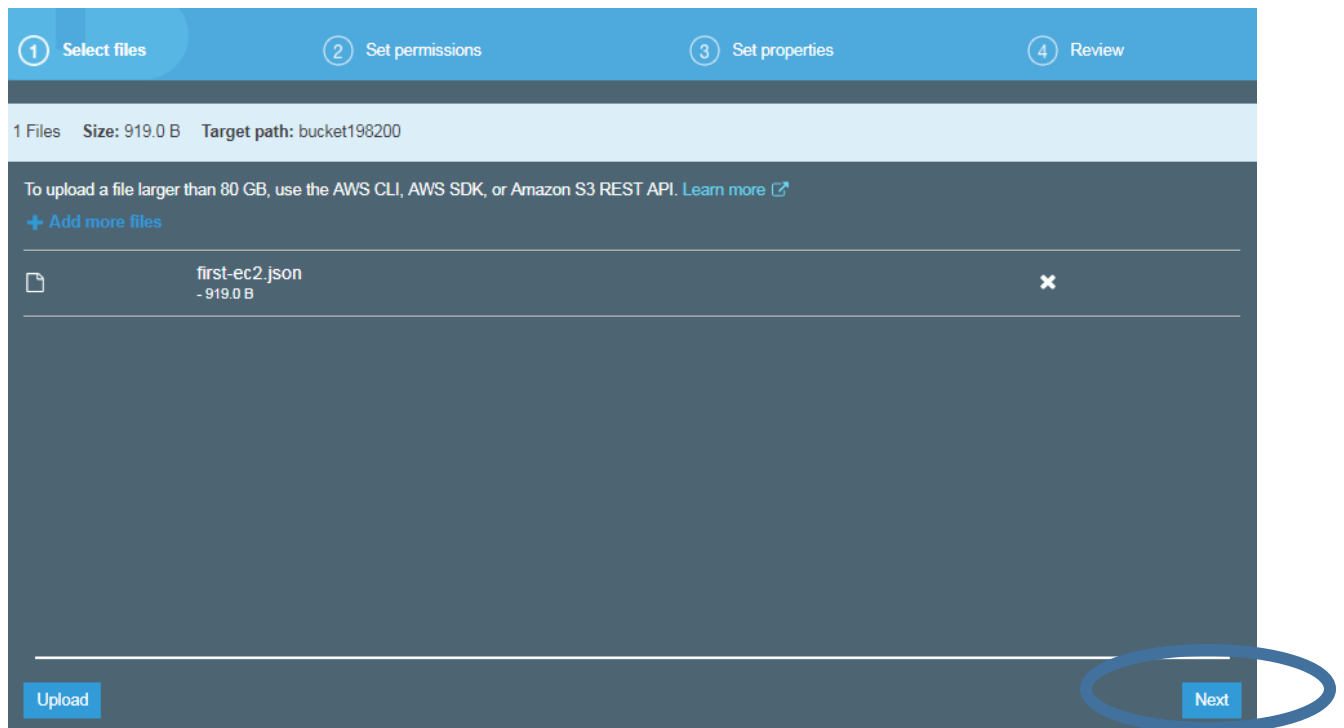
You should be able to see the below screen



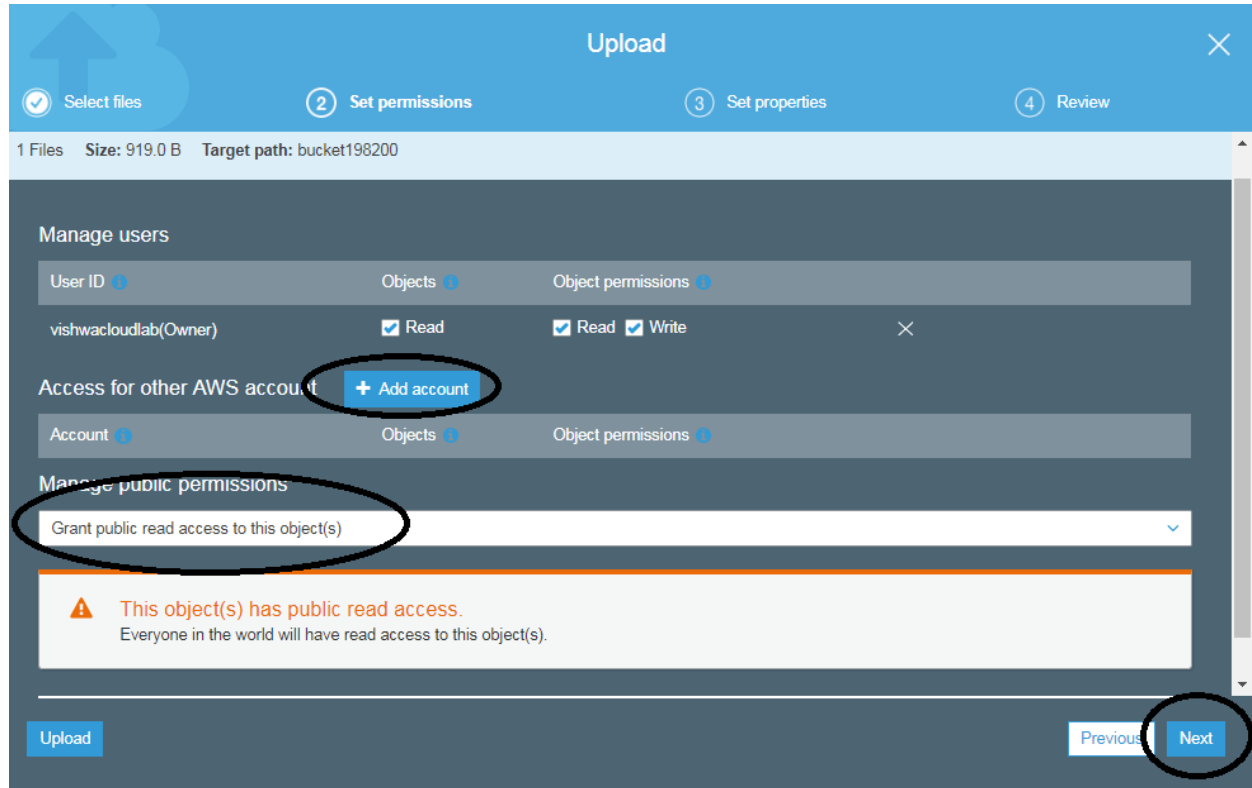
Click “upload”



Click on **“Add Files”**



Click on **“NEXT”**



Select **“Grant public read access to this object”**

Then Click **“NEXT”**

Storage class

Choose a storage class based on your use case and access requirements. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
<input type="radio"/> Standard	Frequently accessed data	≥ 3	-	-	-	-
<input type="radio"/> Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
<input type="radio"/> Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply

Encryption
Protect data at rest by using Amazon S3 master-key or by using AWS KMS master-key.

☒ None ☐ Amazon S3 master-key ☐ AWS KMS master-key

Metadata
Metadata is a set of name-value pairs. You cannot modify object metadata after it is uploaded.

Header	Value
Select a key	

Tag
Add tags to search, organize and manage access

Key	Value
Key	Value

Upload Previous **Next**

Note:-- If required we can enable “Encryption” on file/object level

Click on **“NEXT”**

Upload

✓ Select files ✓ Set permissions ✓ Set properties 4 Review

Files Edit

1 Files Size: 919.0 B

Permissions Edit

2 grantees

Properties Edit

Encryption
No

Storage class
Standard

Metadata

Tag

Previous **Upload**

Click on **“UPLOAD”**

OUTPUT:

Amazon S3 > bucket198200

Overview Properties Permissions Management

🔍 Type a prefix and press Enter to search. Press ESC to clear.

📁 Upload + Create folder Download Actions ▾ Versions Hide Show US East (N. Virg)

	Name ▾	Last modified ▾	Size ▾	Storage class ▾
<input type="checkbox"/>	📄 first-ec2.json	May 28, 2019 9:40:39 PM GMT+0530	919.0 B	Standard

Viewing