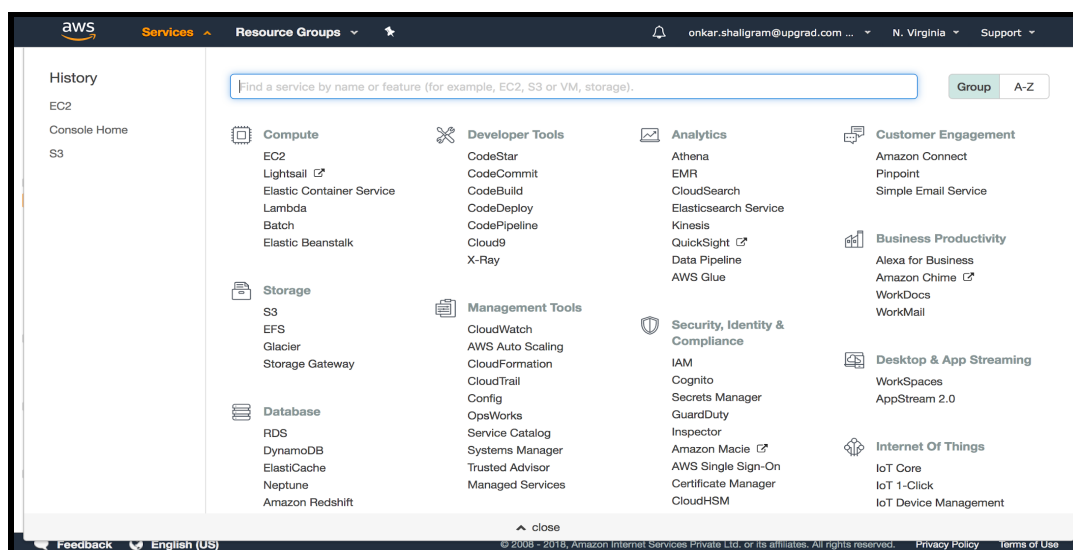


Creating an S3 Bucket

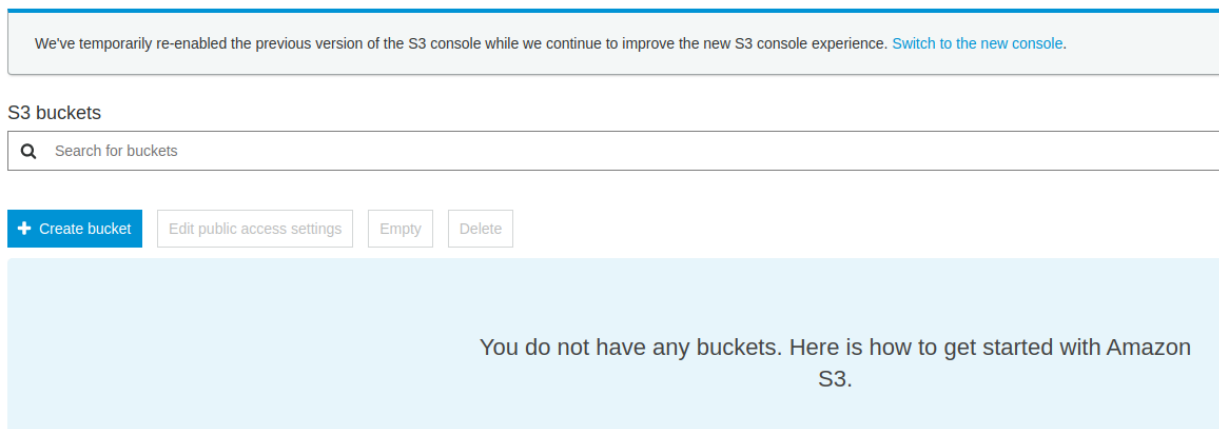
During the course, you will be making use of Amazon S3 to read and write data while running your queries on the Redshift cluster. For this purpose, you will need to create buckets on Amazon S3. The detailed steps for the same are given below.

Note: To avoid unnecessary costs, Please delete your buckets once you have gone through the module. If you want to practice the concepts later on you can create the buckets again.

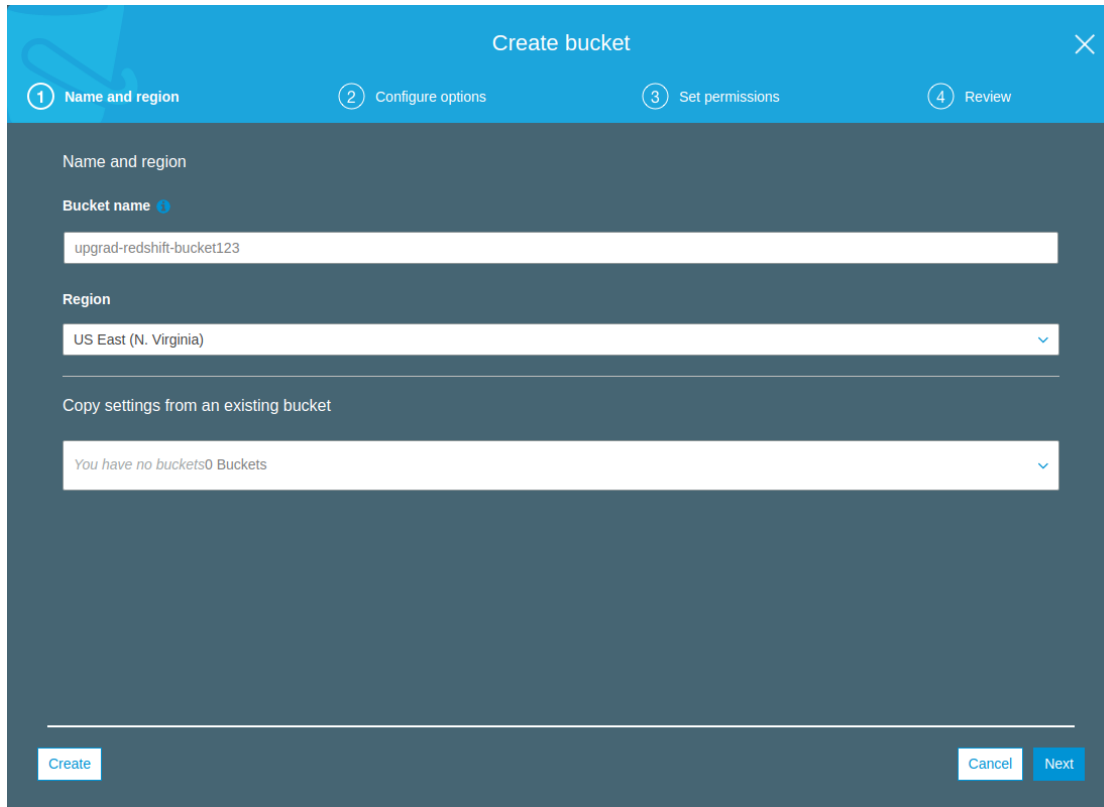
1. Choose the S3 option from your Amazon dashboard



2. You will then be redirected to the S3 management console



3. Click on the “**Create Bucket**” button to get the below pop-up



To create a new bucket you will need to enter the following details:

- **Bucket Name:** Enter the name of the bucket that you want to create. **The bucket name has to be unique across the entire S3 system.**
- **Region:** Please ensure you **select the same region as that of your instance.** If the bucket is in a separate region from the instance you will not be able to read/write the data to the bucket. In this case, as your instance is in the **US East (N. Virginia)** region, please select the same region for your S3 bucket.
- You can skip the third option “Copy settings from an existing bucket” and click on the Next button.

4. After clicking the Next button you should see the following screen. You **do not need to make any changes on this screen** and can move ahead by clicking **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](#)

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](#)

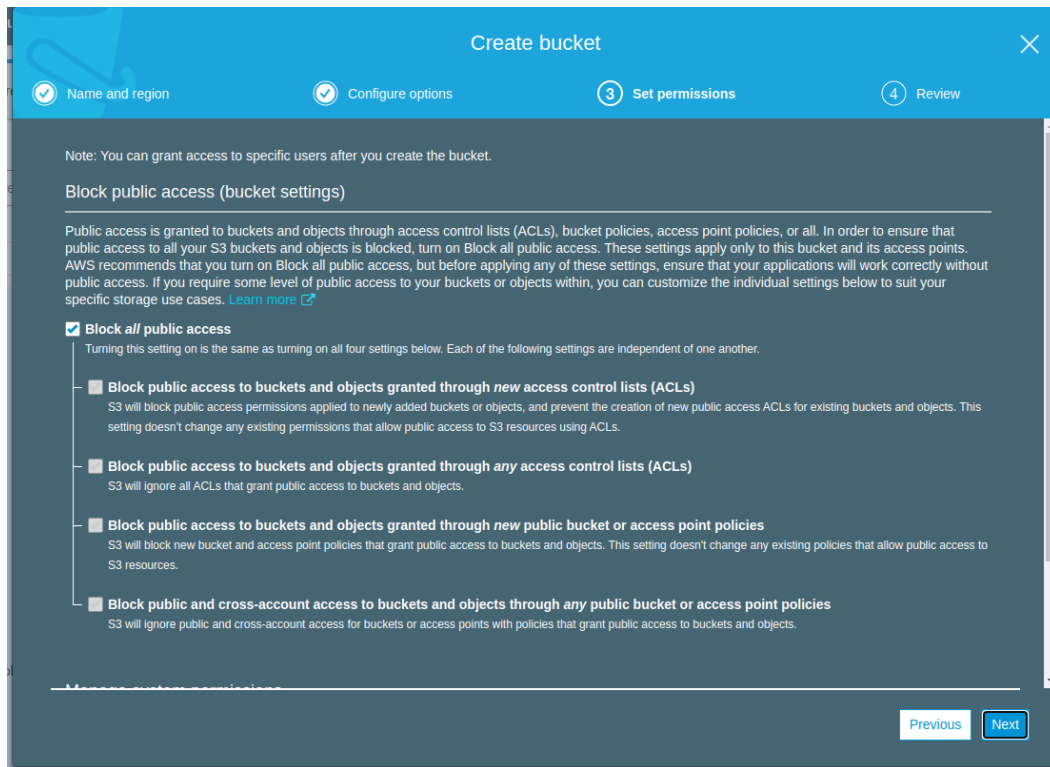
Advanced settings

Management

Previous

Next

- The next screen deals with the read and writes permissions of your bucket. **Uncheck** the checkbox labeled as **Block all public access**. then...



Create bucket

1 Name and region 2 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, access point policies, or all. 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 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 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 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.

[Manage custom permissions](#)

[Previous](#) [Next](#)

Please check the checkbox with the text - **I acknowledge that the current settings may result in this bucket and the objects within becoming public.**

See the below image for reference, Click on the next button.

Create bucket

✓

Name and region

✓

Configure options

3

Set permissions

4

Review

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

⚠

Disabling Block all public access may result in this bucket and the objects within becoming public

AWS recommends that you block all public access to your bucket, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings may result in this bucket and the objects within becoming public

■

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.

Previous

Next

© Copyright. upGrad Education Pvt. Ltd. All rights reserved

- The next screen shows a preview of the settings that you have selected for the bucket. Please **ensure that the region selected as US East (N. Virginia)** and the **public read permission is enabled**. You can then click on the “**Create Bucket**” button.

Create bucket

✓ Name and region

✓ Configure options

✓ Set permissions

4 Review

Name and region

Bucket name upgrad-redshift-bucket123

Region US East (N. Virginia)

Options

Versioning Disabled

Server access logging Disabled

Tagging 0 Tags

Object-level logging Disabled

Default encryption None

CloudWatch request metrics Disabled

Object lock Disabled

Permissions

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

Previous

Create bucket

© Copyright. upGrad Education Pvt. Ltd. All rights reserved

7. You will now be able to see your bucket on the S3 management screen.

How to optimize your costs on S3. [Learn more »](#)

Documentation

We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. [Switch to the new console.](#)

S3 buckets

Discover the console

Search for buckets

All access types

Create bucket

Edit public access settings

Empty

Delete

1 Buckets

1 Regions

<input type="checkbox"/> Bucket name	Access	Region	Date created
<input type="checkbox"/> upgrad-redshift-bucket123	Objects can be public	US East (N. Virginia)	Sep 7, 2020 7:49:21 PM GMT+0530

- You can create subfolders inside your S3 bucket using the intuitive UI.