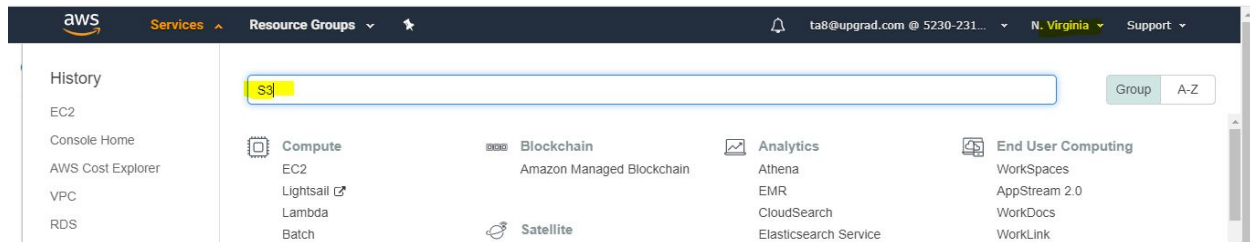




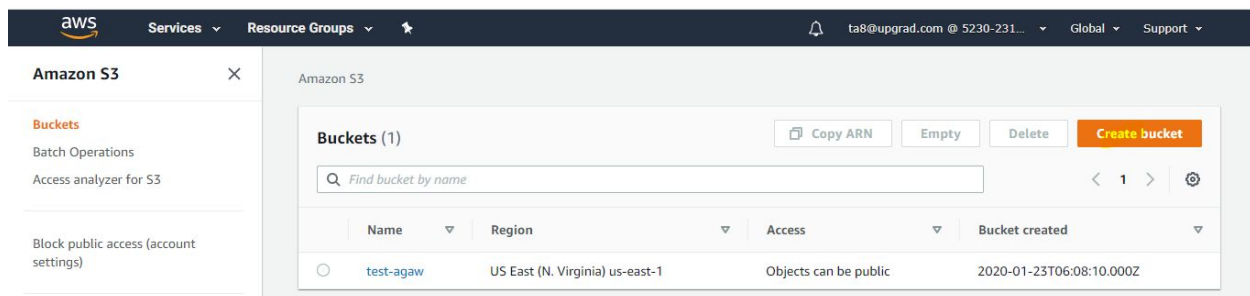
Create an S3 bucket

Prerequisites: Region should be selected as N. Virginia.

1. Open AWS dashboard and type **S3** in the search field



2. Click on the **Create bucket** button



3. Bucket names should be unique. Next, select the region - **N. Virginia**. Scroll down to the bottom of the page and click on the **Create bucket** button.

General configuration

Bucket name

upgrad-123

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

Region

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

► Advanced settings

Cancel Create bucket



Amazon S3

Buckets

Batch Operations

Access analyzer for S3

Block public access (account settings)

Feature spotlight

Successfully created bucket upgrad-123

To upload files and folders, or to configure additional bucket settings such as Bucket Versioning, tags, and default encryption, choose [Go to bucket details](#).

Amazon S3

Buckets (2)

Copy ARN Empty Delete Create bucket

Find bucket by name

	Name	Region	Access	Bucket created
<input type="radio"/>	test-agaw	US East (N. Virginia) us-east-1	Objects can be public	2020-01-23T06:08:10.000Z
<input type="radio"/>	upgrad-123	US East (N. Virginia) us-east-1	Not Public	2020-04-08T06:00:58.000Z

Upload an object on S3 bucket

1. Click on bucket name and click on **upload**.

Amazon S3 > upgrad-123

upgrad-123

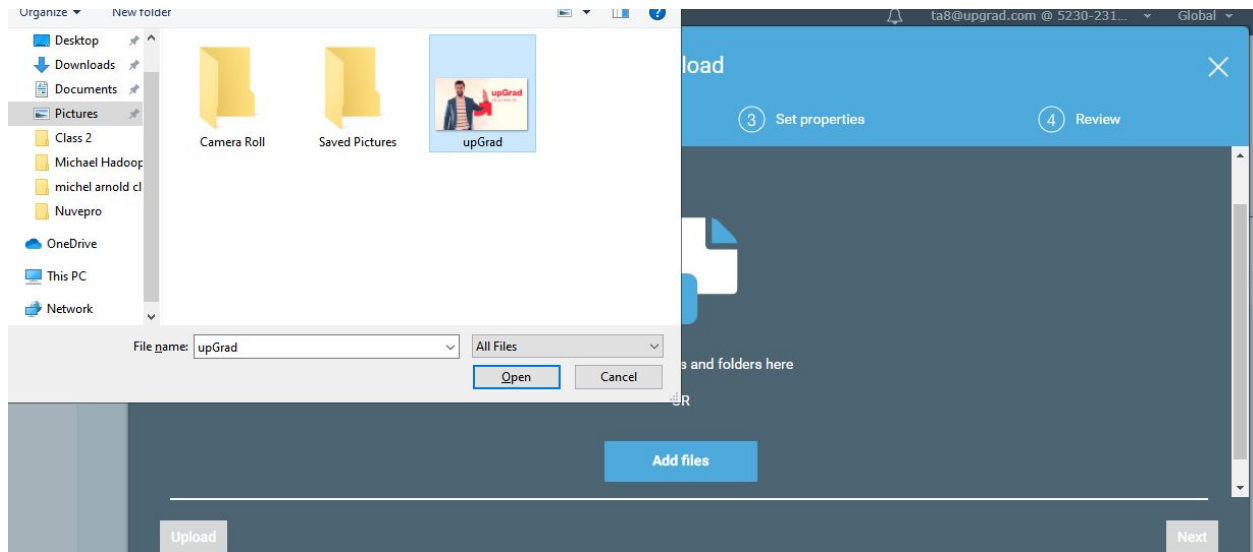
Overview Properties Permissions Management Access points

Upload Create folder Download Actions

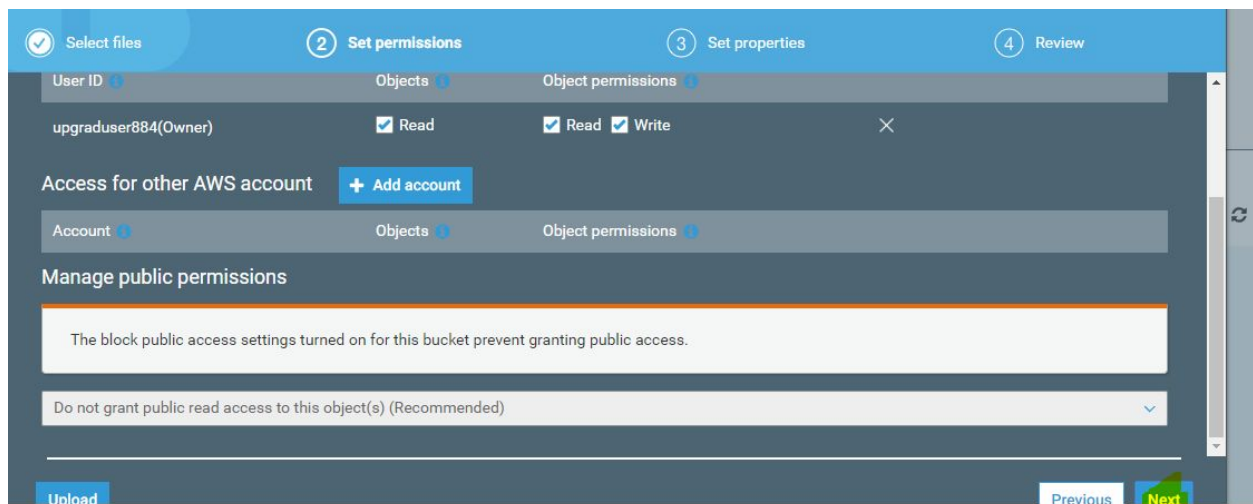
US East (N. Virginia)

This bucket is empty. Upload new objects to get started.

2. You can directly **drag and drop** the object or scroll down and click on **Add files**.



3. Once the objects have been added, click on **Next**



4. Select the default option as is highlighted in the image below. Click on **Next**



Upload

1 Select files

2 Set permissions

3 Set properties

4 Review

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 checked="" 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
<input type="radio"/> Glacier	Archive data with retrieval times ranging from minutes to hours	≥ 3	90 days	40KB	-	Per-GB fees apply
<input type="radio"/> Glacier Deep Archive	Archive data that rarely, if ever, needs to be accessed	≥ 3	180 days	40KB	-	Per-GB fees apply

Upload

Previous

Next

5. Navigate to the below screen and click on the **Upload** button

upgrad-123

Overview

Properties

Permissions

Management

Access points

Q

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

Upload

Create folder

Download

Actions

US East (N. Virginia)

Name	Last modified	Size	Storage class
<input type="checkbox"/> upGrad.jpg	Apr 8, 2020 11:47:16 AM GMT+0530	92.5 KB	Standard

Viewing 1 to 1

6. You won't be able to open this image. Click on the image to get the **URL** (as highlighted below)



upGrad

Open

Download

Download as

Make public

Copy path

Owner

upgraduser884

Last modified

Apr 8, 2020 11:47:16 AM GMT+0530

Etag

3745e767d293937e57830df615447916

Storage class

Standard

Server-side encryption

None

Size

92.5 KB

Key

upGrad.jpg

Object URL

<https://upgrad-123.s3.amazonaws.com/upGrad.jpg>

7. Open URL to different tab

← → ↻ upgrad-123.s3.amazonaws.com/upGrad.jpg

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

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>C94DAFF0A4D1AAE6</RequestId>
  <HostId>
    W9gO2H014ZyPlsPfrQYnEb2MN0tvKCRemudFrTu4cOUHPnTVMADXnzx5YfSmDse4XeSxoJ4ZM9k=
  </HostId>
</Error>
```

8. Navigate back to the bucket click on the bucket name.



Amazon S3 > upgrad-123 > upGrad.jpg

upGrad.jpg Latest version ▾

Overview Properties Permissions Select from

Open Download Download as Make public Copy path

Owner
upgraduser884

Last modified
Apr 8, 2020 11:47:16 AM GMT+0530

Etag
3745e767d293937e57830df615447916

Storage class

9. Next, click on **Permissions**.

upgrad-123

Overview Properties Permissions Management Access points

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

Upload Create folder Download Actions ▾

US East (N. Virginia) ↻

Viewing 1 to 1

<input type="checkbox"/> Name ▾	Last modified ▾	Size ▾	Storage class ▾
<input type="checkbox"/> upGrad.jpg	Apr 8, 2020 11:47:16 AM GMT+0530	92.5 KB	Standard

Viewing 1 to 1

10. Click on the **Edit** button to edit the bucket public access.

Overview Properties Permissions Management Access points

Block public access Access Control List Bucket Policy CORS configuration

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
On

Edit

11. **Uncheck** block all public access and click on **Save**.



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.

[Cancel](#) [Save](#)

12. Click on **Confirm**.

13. You will get a confirmation message stating that **Public access settings updated successfully**

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](#)

☒ **Public access settings updated successfully**

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 or access point policies**
Off

[Edit](#)



14. Click on Amazon S3.

Amazon S3 > upgrad-123

upgrad-123

Overview Properties Permissions Management Access points

Block public access Access Control List Bucket Policy CORS configuration

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](#)

✓ Public access settings updated successfully

15. Click on bucket and click on object name. And click on **Make public**.

Overview Properties Permissions Select from

Open Download Download as **Make public** Copy path

Owner
upgraduser884

Last modified
Apr 8, 2020 11:47:16 AM GMT+0530

Etag
3745e767d293937e57830df615447916

Storage class
Standard

Server-side encryption
None

Size
92.5 KB

Key
upGrad.jpg

Object URL
<https://upgrad-123.s3.amazonaws.com/upGrad.jpg>

16. Now open the object URL in a different tab.



upGrad

[Open](#) [Download](#) [Download as](#) [Make public](#) [Copy path](#)

Owner
upgraduser884

Last modified
Apr 8, 2020 11:47:16 AM GMT+0530

Etag
3745e767d293937e57830df615447916

Storage class
Standard

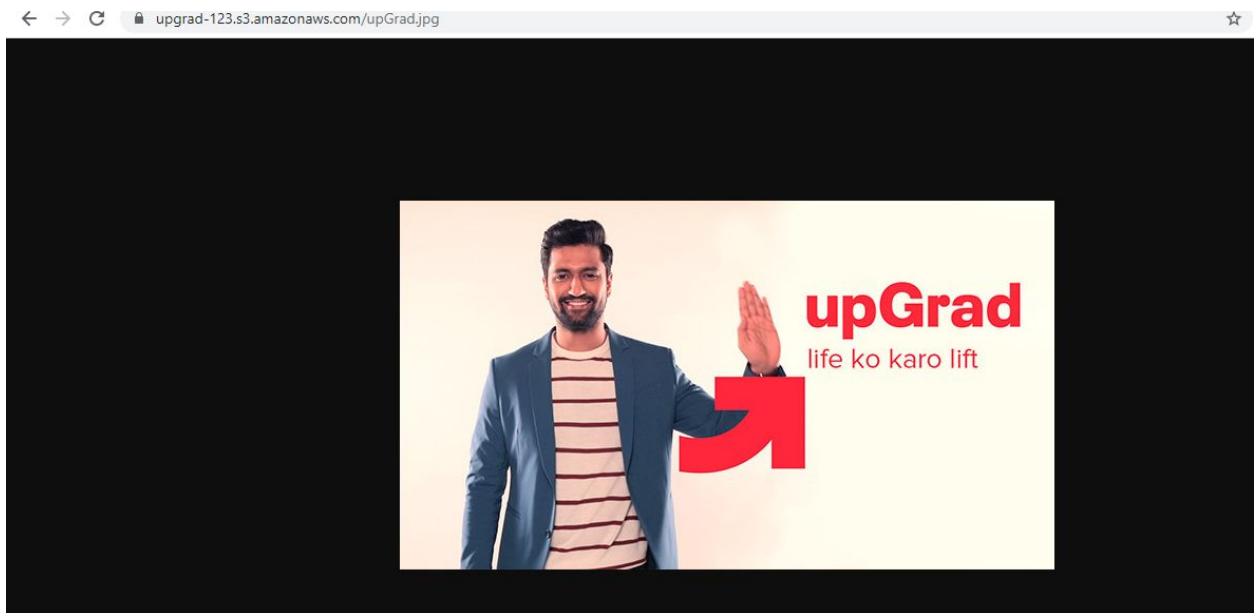
Server-side encryption
None

Size
92.5 KB

Key
upGrad.jpg

Object URL
<https://upgrad-123.s3.amazonaws.com/upGrad.jpg>

17. You should now be able to view the image.



18.