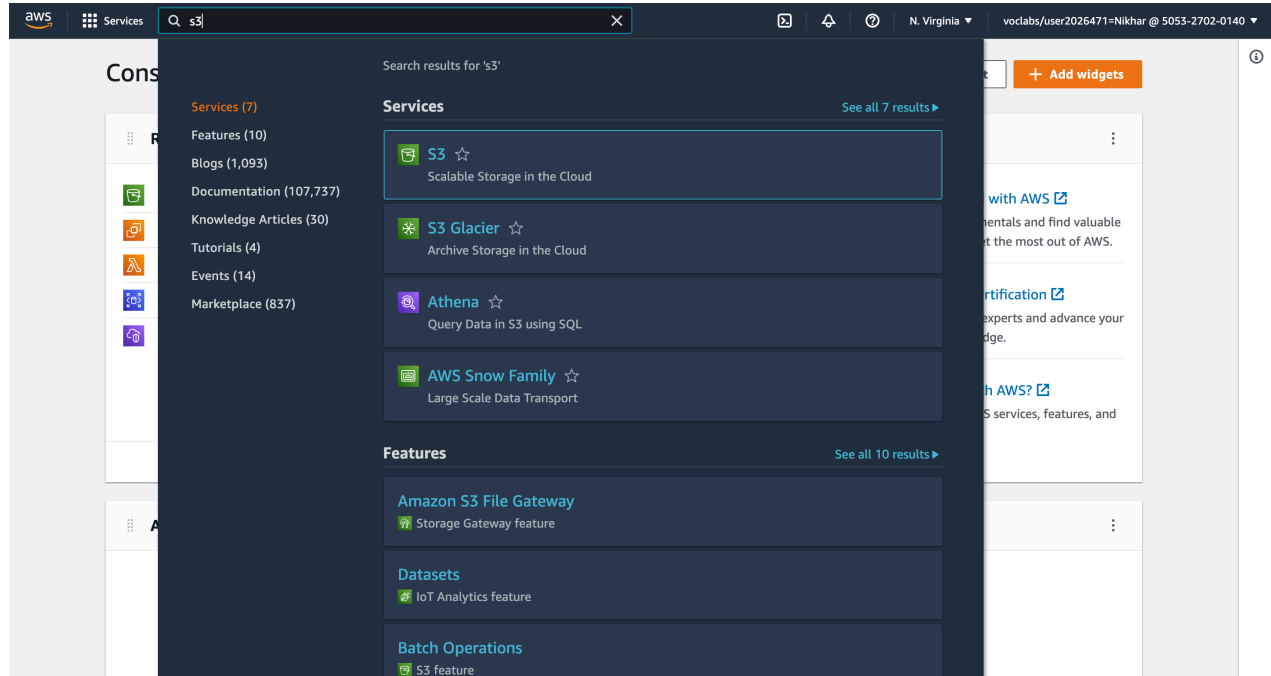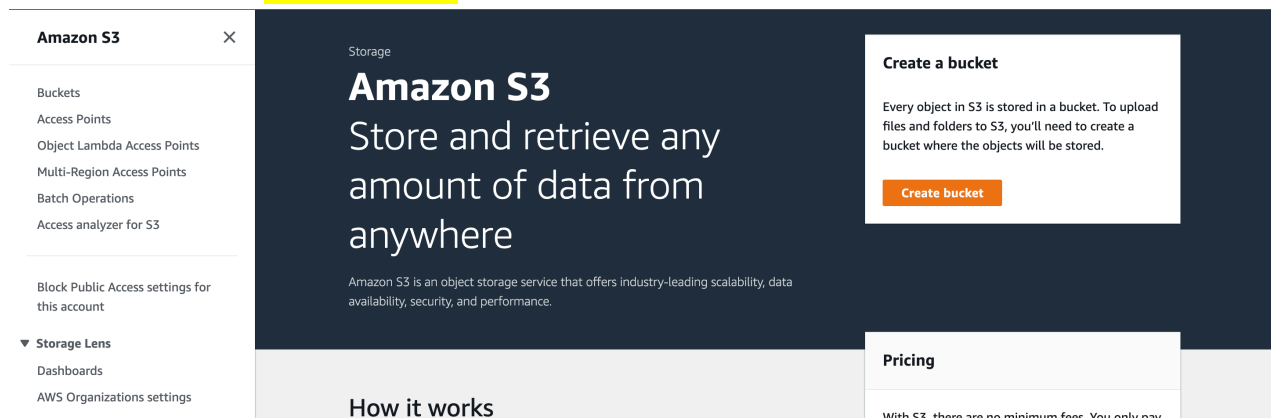# Create an S3 bucket

Prerequisites: Region should be selected as N. Virginia.

1. Open AWS dashboard and type <mark>S3</mark> in the search field

2. Click on the <mark>Create bucket</mark> button

3. Bucket names should be unique. Next, select the region - <mark>N. Virginia</mark>. Scroll down to the bottom of the page and click on the <mark>Create bucket</mark> 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 ▼

4. **Disable ACLs**

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

5. Toggle off 'Block Public Access', and acknowledge below.

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.

Amazon S3 ✕

Buckets

Batch Operations

Access analyzer for S3

Block public access (account settings)

Feature spotlight 2️⃣

✓ **Successfully created bucket upgrad-123**   **Go to bucket details** ✕
To upload files and folders, or to configure additional bucket settings such as Bucket Versioning, tags, and default encryption, choose **Go to bucket details**.
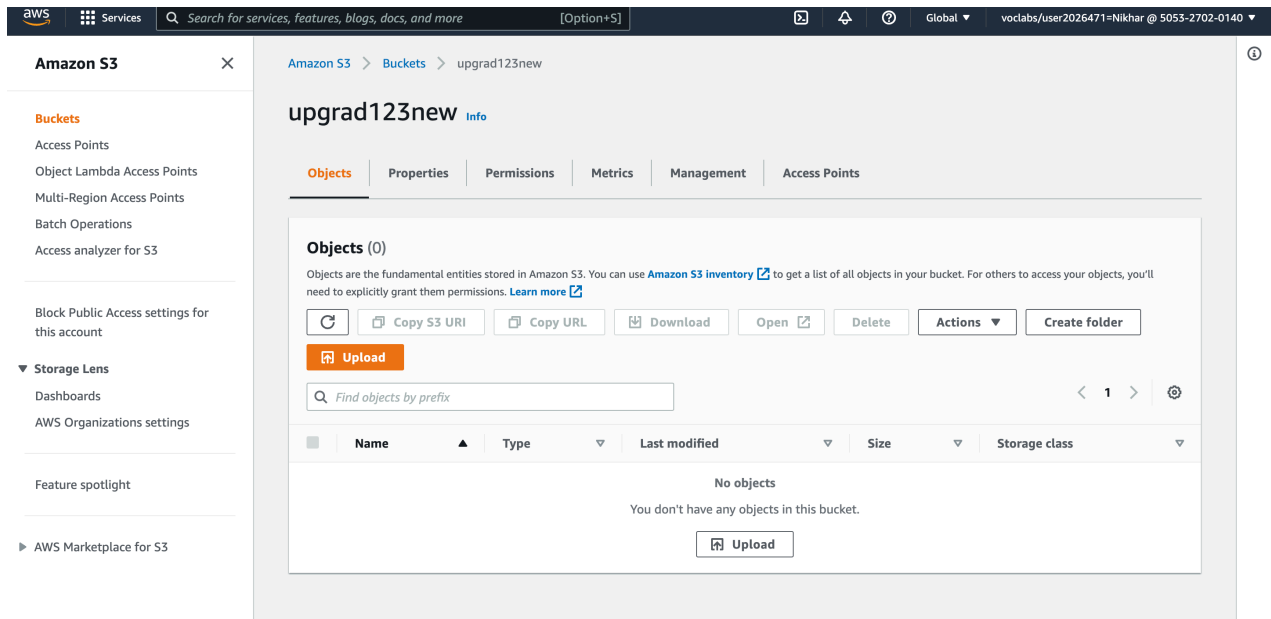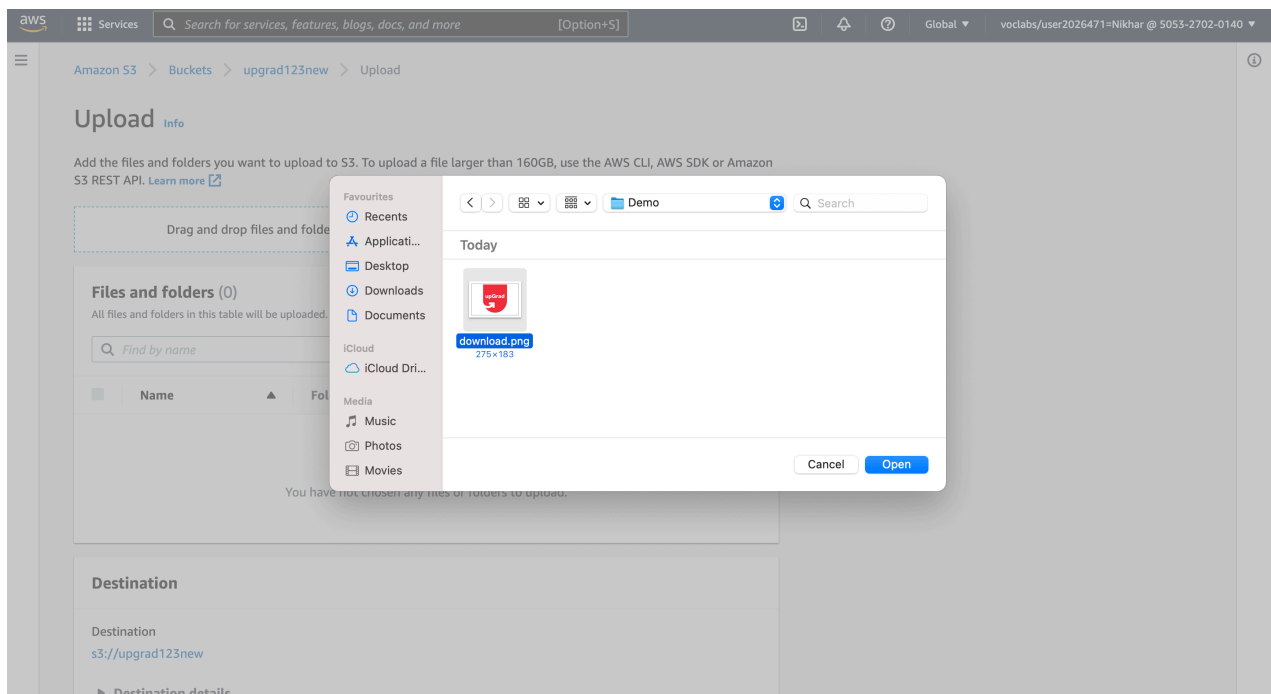
Amazon S3

Buckets (2)   🗗 Copy ARN | Empty | Delete | **Create bucket**

🔍 Find bucket by name   ‹ 1 ›   ⚙️

	Name ▽	Region ▽	Access ▽	Bucket created ▽
○	test-agaw	US East (N. Virginia) us-east-1	Objects can be public	2020-01-23T06:08:10.000Z
○	upgrad-123	US East (N. Virginia) us-east-1	Not Public	2020-04-08T06:00:58.000Z

<u>Upload an object on S3 bucket</u>

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

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

3. Navigate to the below screen and clock on the **Upload** button

The object will get successfully uploaded.

Versioning an S3 bucket

1. Create a bucket.

General configuration

Bucket name

versioningdemobucket

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

2. Follow all the steps mentioned above for object ownership and block public access settings for this bucket.

3. **Enable bucket versioning.**

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. **Learn more** ⧉
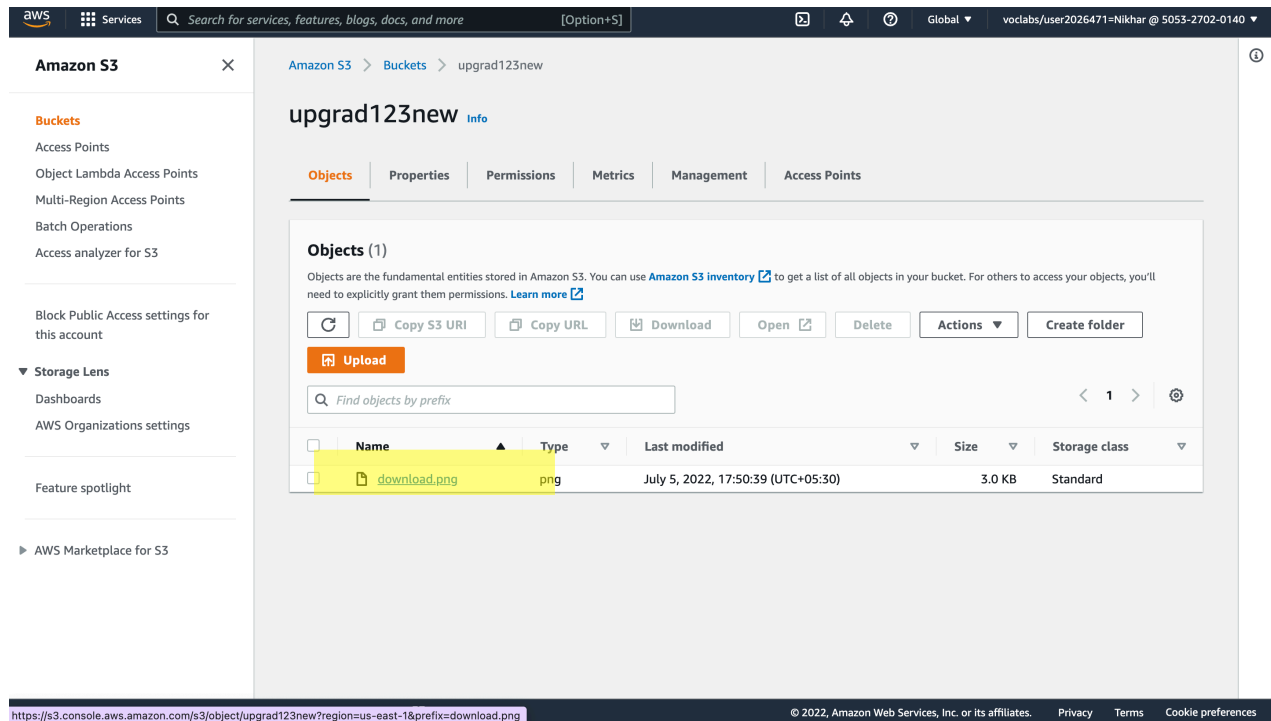
Bucket Versioning
○ Disable
◉ Enable

4. Click on create bucket.

5. For uploading an object into this bucket, follow the steps mentioned in the previous section.

Downloading a file from S3 bucket

1. Click on the object you want to download.

2. Click on the **download** button at the top. The file will get downloaded in your local machine.