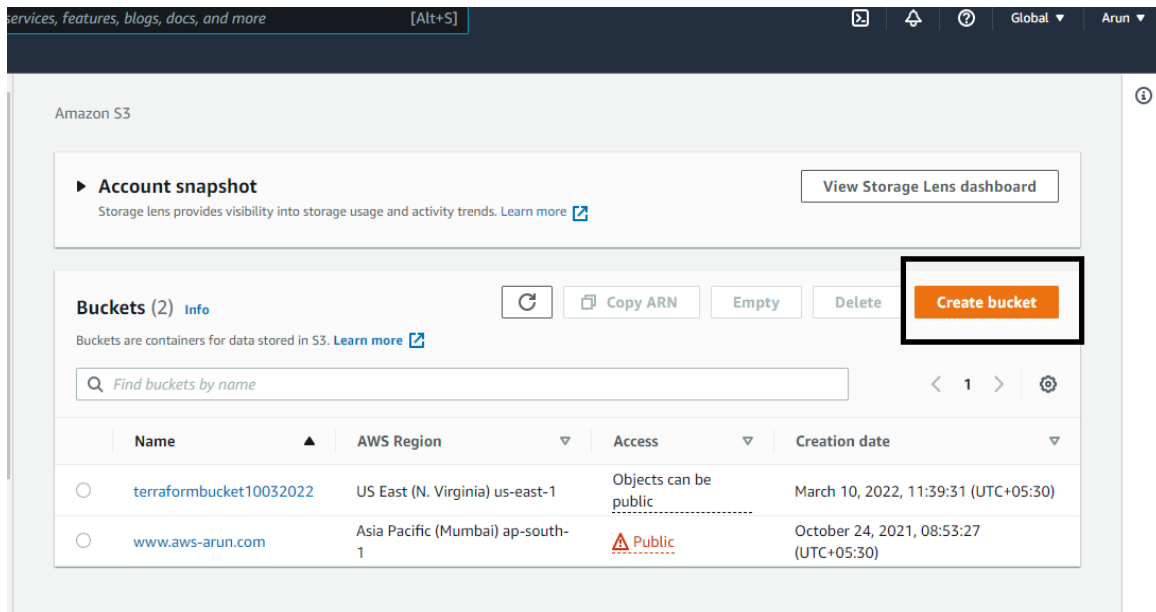


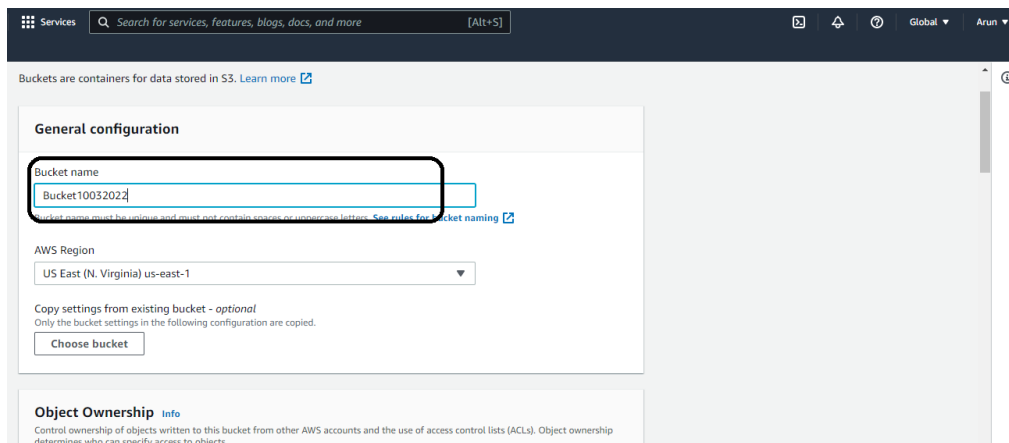
# Simple Storage Service

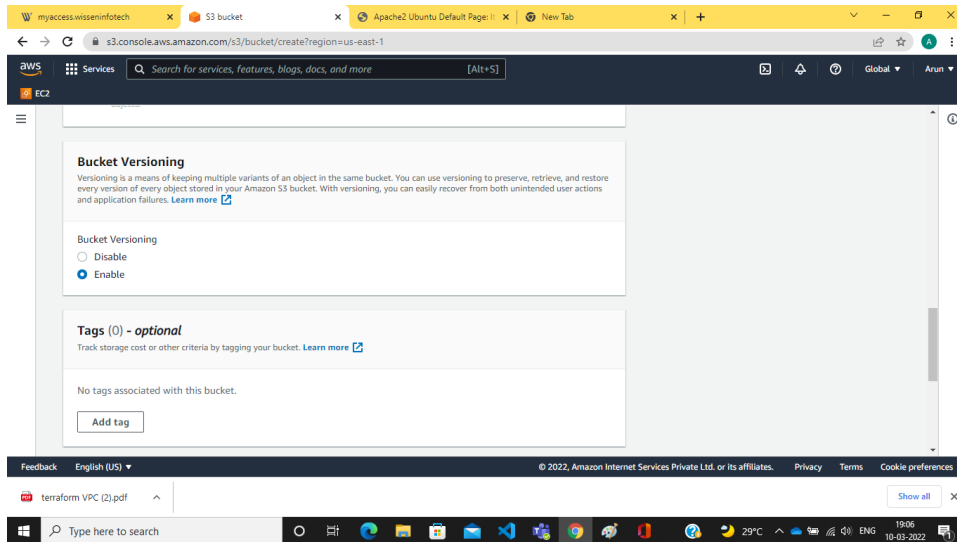
step 1 : Goto Management Console Create Bucket >> search for S3 service >> click create Bucket



Step 2 : Enter Bucket name : **Bucket name must be unique globally and must not contain spaces or uppercase letters**

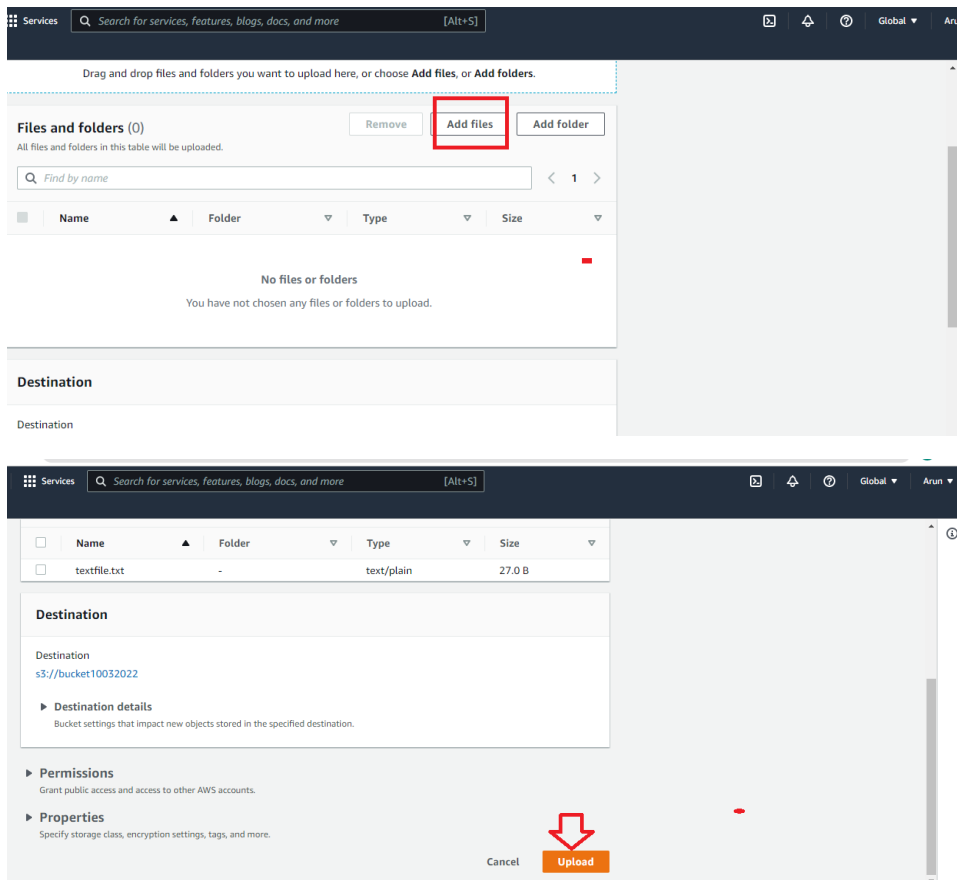
Enable bucket versioning Enter Create Bucket





Step 3 : to upload object in the bucket >> select the bucket

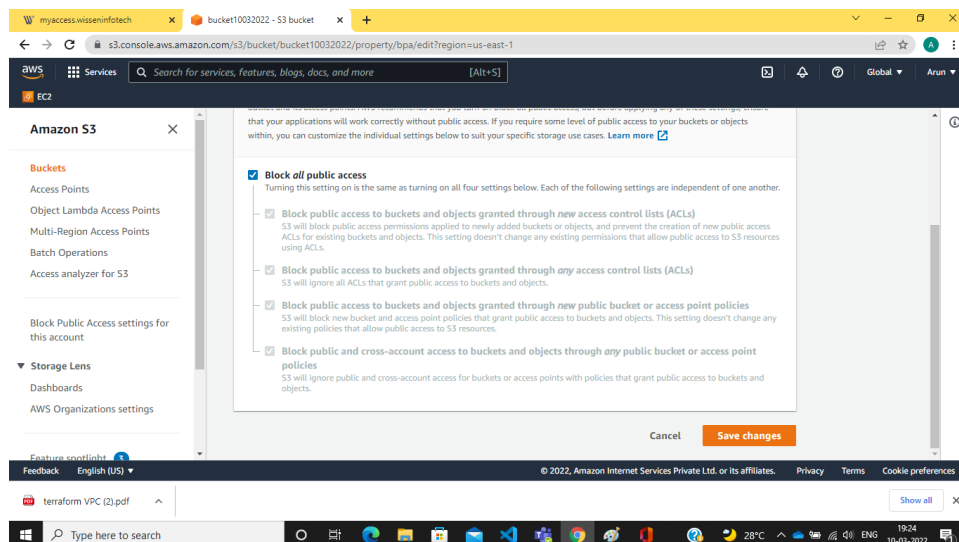
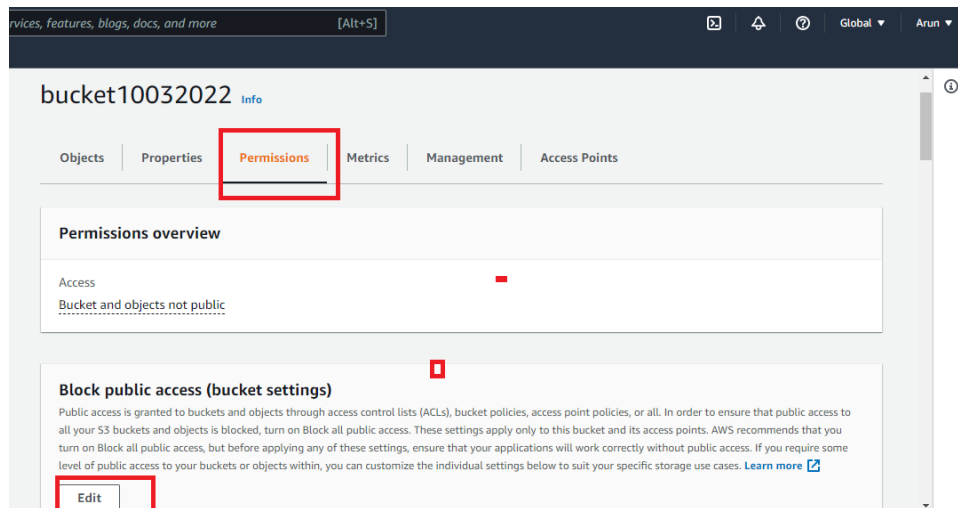
>> click upload >> add files >> upload files from local device



Step 4 : By default buckets are Private.

To make bucket accessible to public

Select the bucket >> goto permissions >> click edit bucket public access >> remove tick mark >> save changes >> and confirm



Before enabling access points, AWS recommends that you turn on block all public access, edit 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.

Cancel **Save changes**

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

**Edit Block public access (bucket settings)** ✕

**⚠** Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

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

Cancel **Confirm**