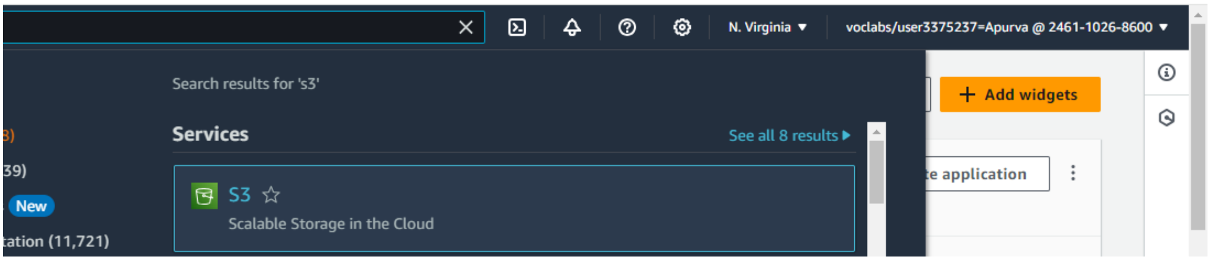
ASSIGNMENT 7

Practical Implementation of Storage as a Service Create an S3 Bucket, Upload a file to S3 Bucket, Retrieve a File from S3 Bucket, Delete a File From S3 Bucket using AWS.

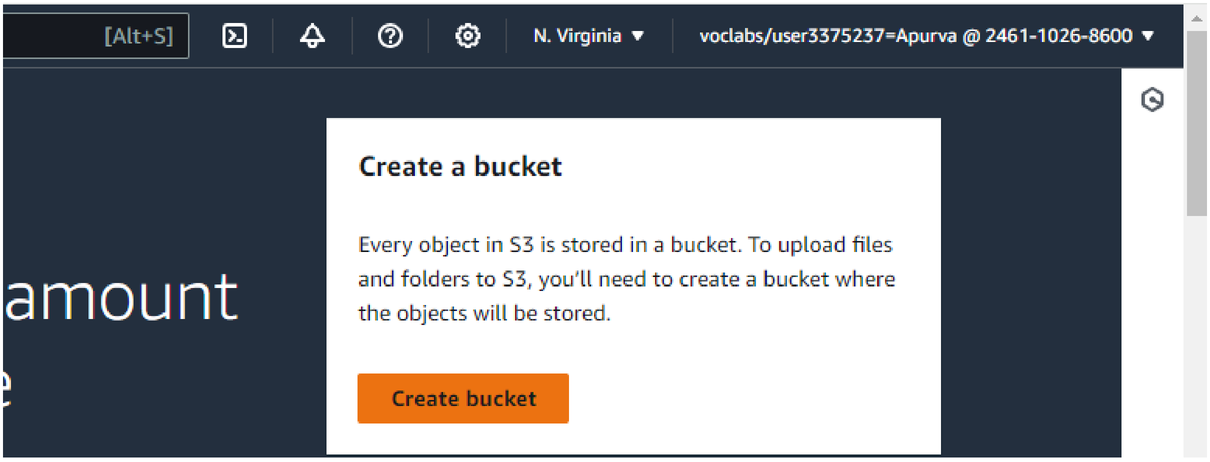
1. Create an S3 Bucket

   1. Log in to AWS Management Console

   2. Navigate to S3 from the Services menu.



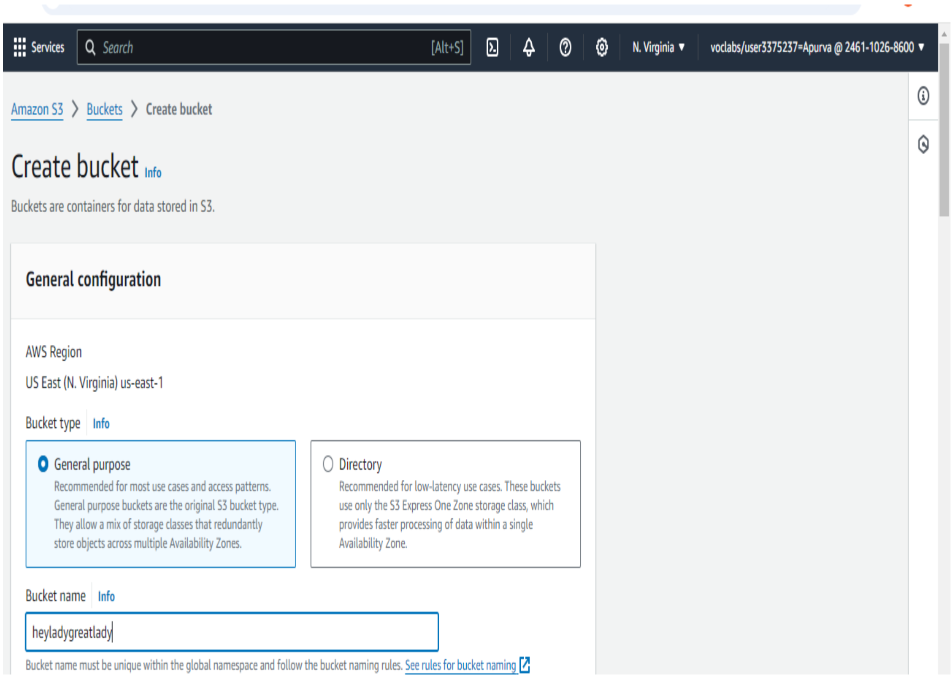
   3. Click on Create Bucket.



Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

4. Enter a Bucket Name (it must be unique globally).



Amazon S3 › Buckets › Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

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

Bucket type Info

● General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

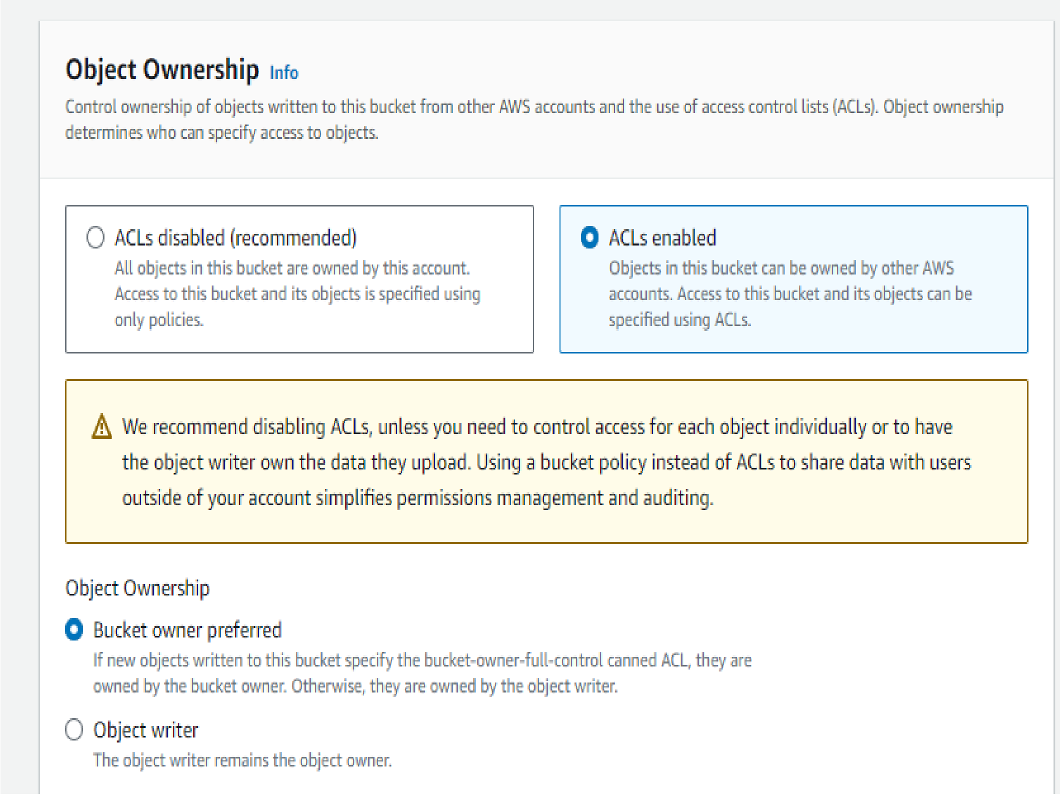
○ Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info

heyladygreatlady

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

5. In Object Ownership,Enabled 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.

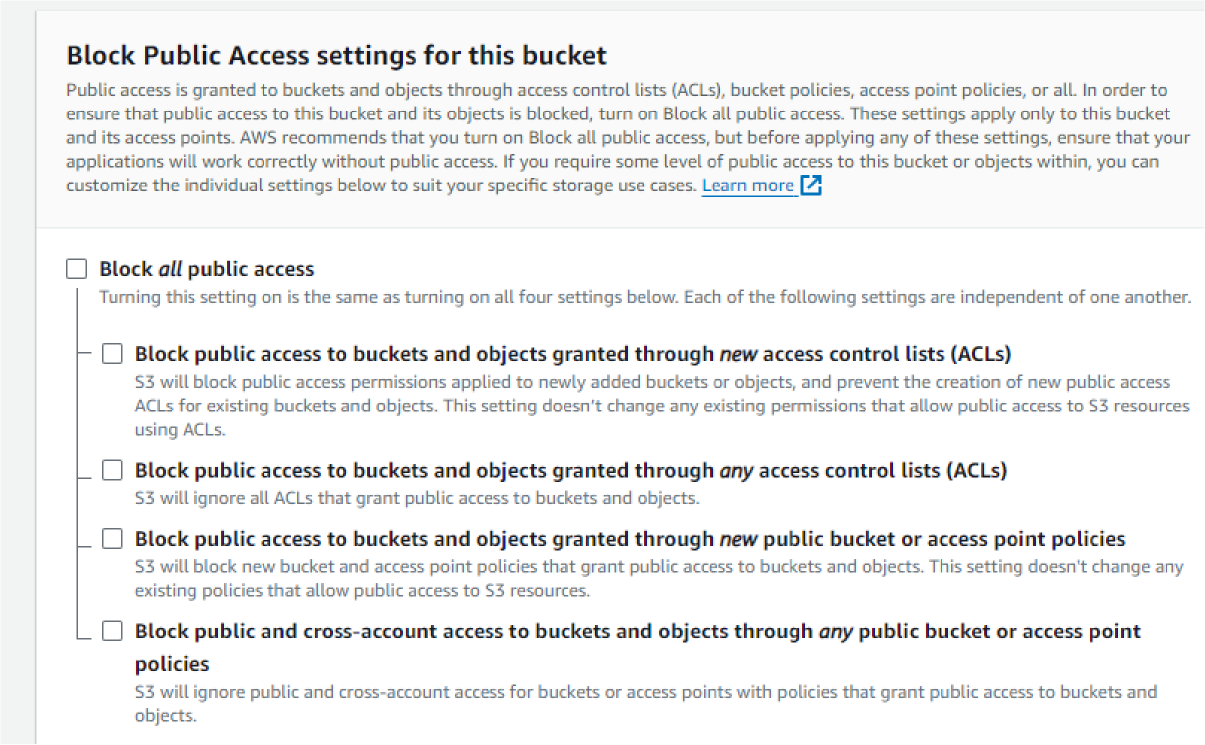
⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

● Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

○ Object writer
The object writer remains the object owner.

6.In block Public Access settings for this bucket untick all ther block.



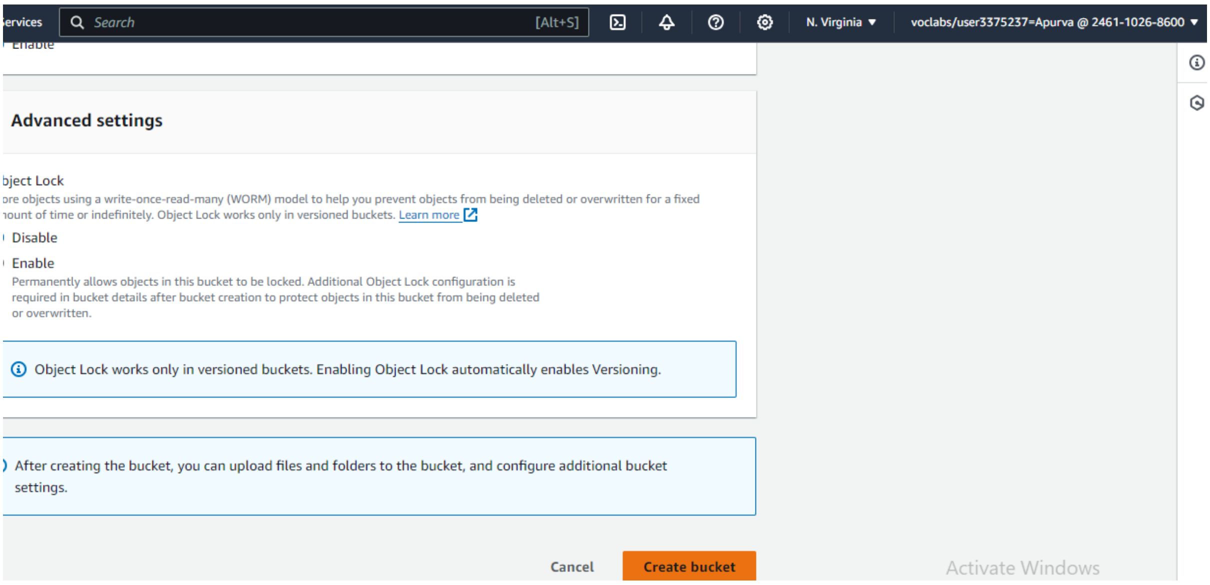
Block Public Access settings for this bucket

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.

6.then click on the “create Bucket”.



Advanced settings

bject Lock
ore objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed
nount of time or indefinitely. Object Lock works only in versioned buckets. Learn more

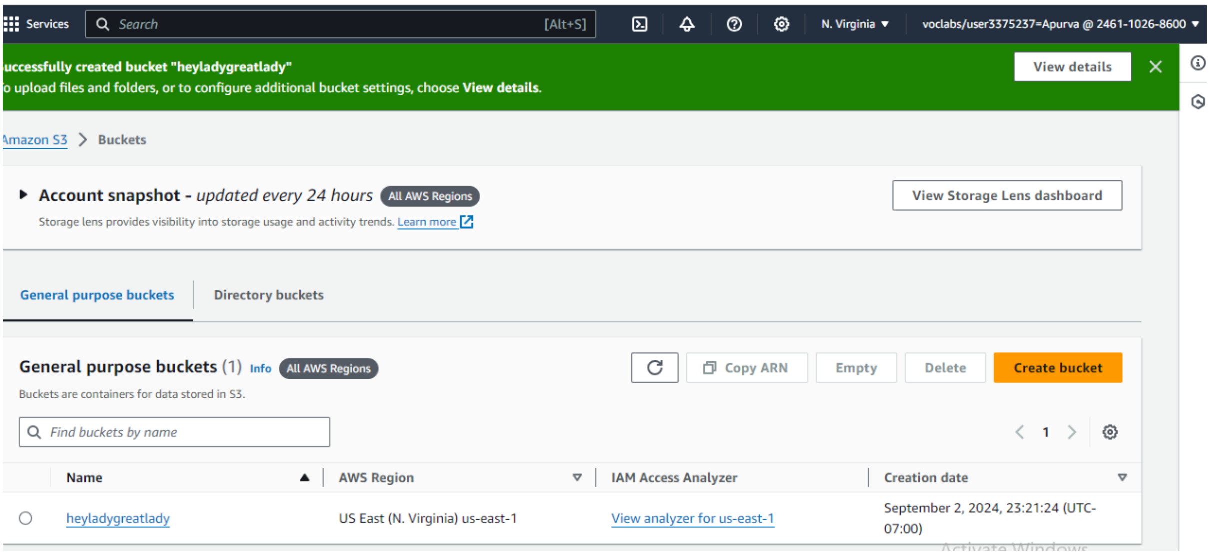
Disable

Enable
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

7.See here, Bucket is Created Successfully.



uccessfully created bucket "heyladygreatlady"
o upload files and folders, or to configure additional bucket settings, choose **View details**.

Account snapshot - *updated every 24 hours* All AWS Regions

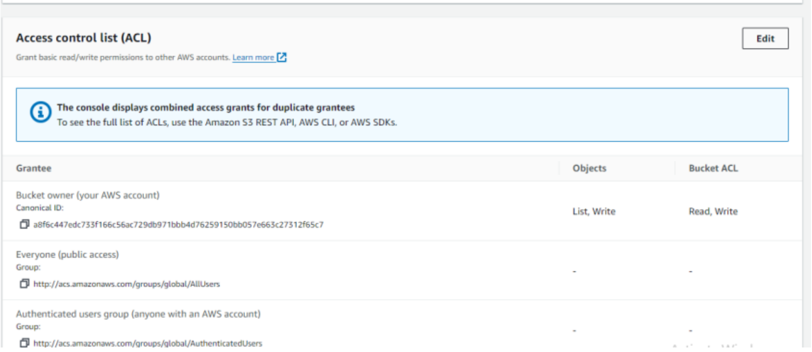
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	heyladygreatlady	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 2, 2024, 23:21:24 (UTC-07:00)

8.In bucket,Permissions edit the ACL and give list and read permission for public access.

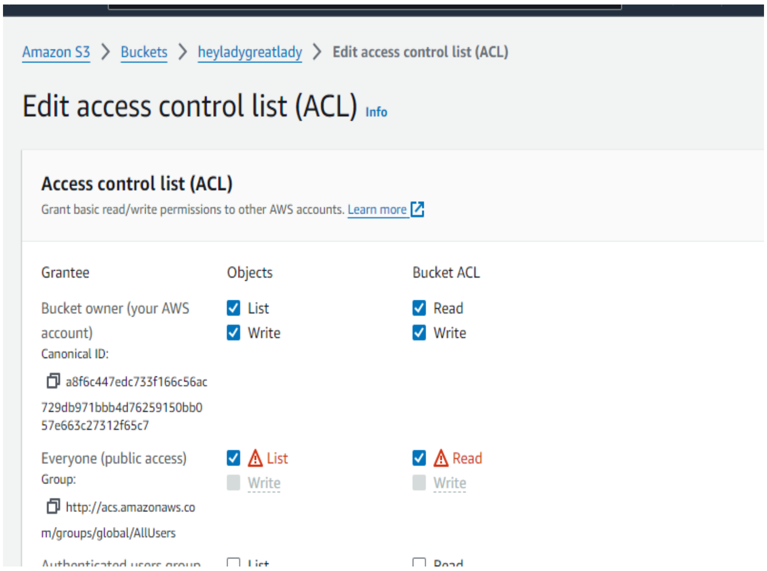


Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: a8f6c447edc733f166c56ac729db971bbb4d76259150bb057e663c27312f65c7	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-



Amazon S3 > Buckets > heyladygreatlady > Edit access control list (ACL)

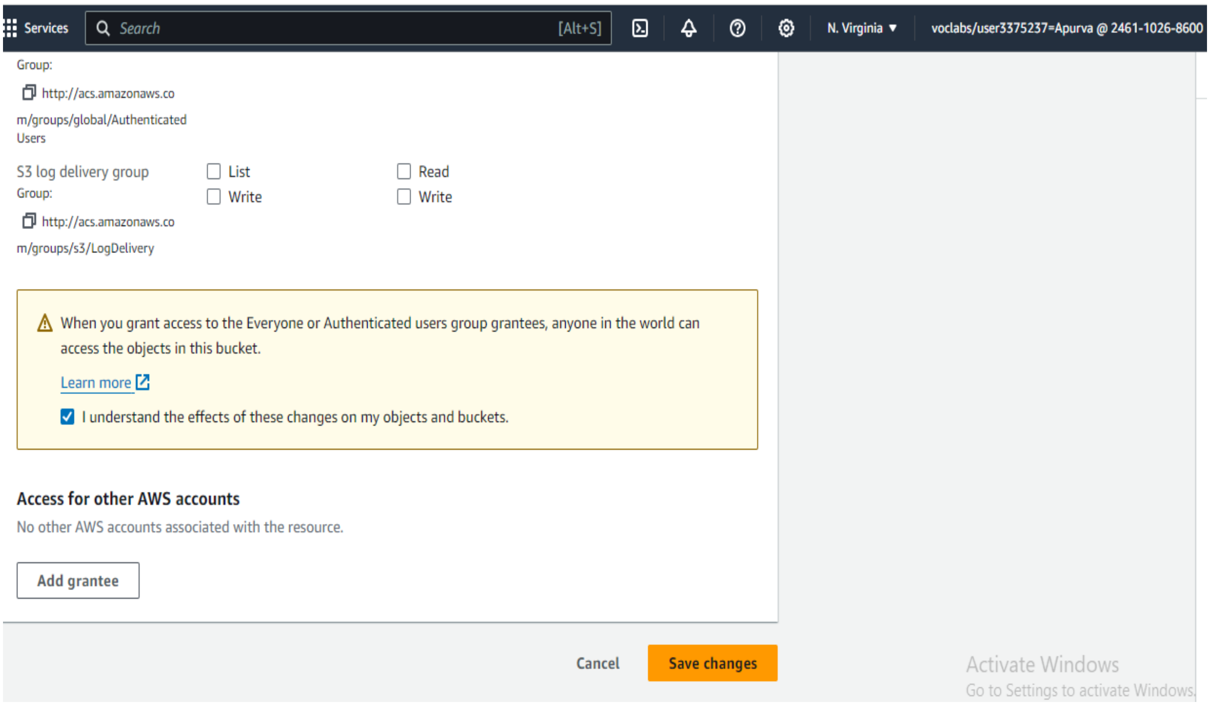
Edit access control list (ACL) Info

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: a8f6c447edc733f166c56ac729db971bbb4d76259150bb057e663c27312f65c7	☑ List ☑ Write	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	☑ ⚠ List □ Write	☑ ⚠ Read □ Write
Authenticated users group	□ List	□ Read

9.and then click on Save changes.



Group:

http://acs.amazonaws.com/groups/global/AuthenticatedUsers

S3 log delivery group

Group:

http://acs.amazonaws.com/groups/s3/LogDelivery

□ List □ Write □ Read □ Write

When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.

Learn more

☑ I understand the effects of these changes on my objects and buckets.

Access for other AWS accounts

No other AWS accounts associated with the resource.

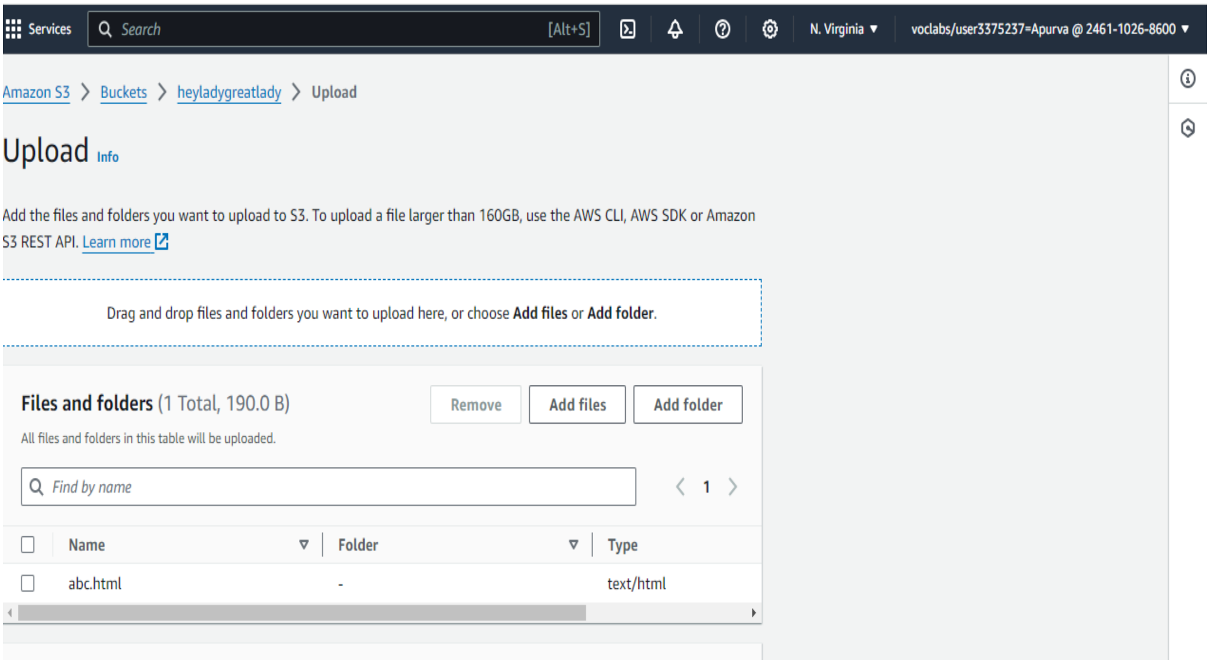
Add grantee

Cancel Save changes

Services
Search [Alt+S]
N. Virginia
voclabs/user3375237=Apurva @ 2461-1026-8600
Activate Windows
Go to Settings to activate Windows.

2. Upload a File to S3 Bucket.

10.then click on add files in upload section and add the abc.html file and upload it.



Amazon S3 > Buckets > heyladygreatlady > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

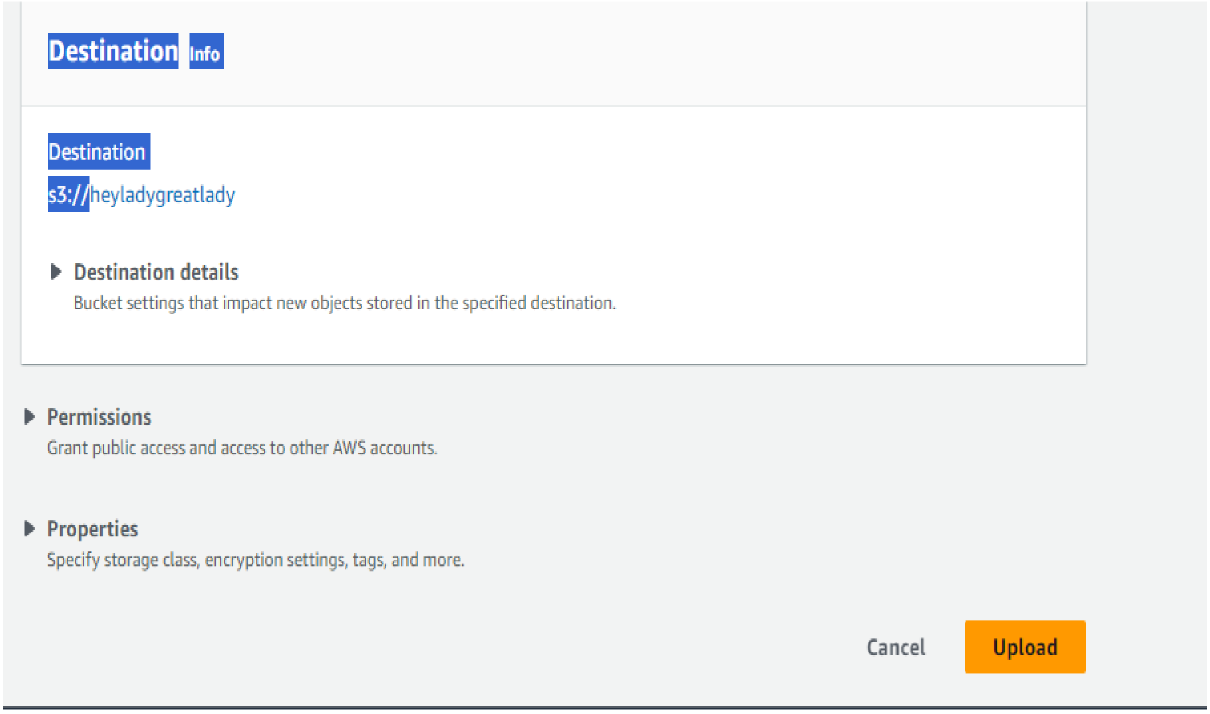
Files and folders (1 Total, 190.0 B)

All files and folders in this table will be uploaded.

Remove Add files Add folder

Find by name

□	Name	Folder	Type
□	abc.html	-	text/html



Destination Info

Destination

s3://heyladygreatlady

Destination details

Bucket settings that impact new objects stored in the specified destination.

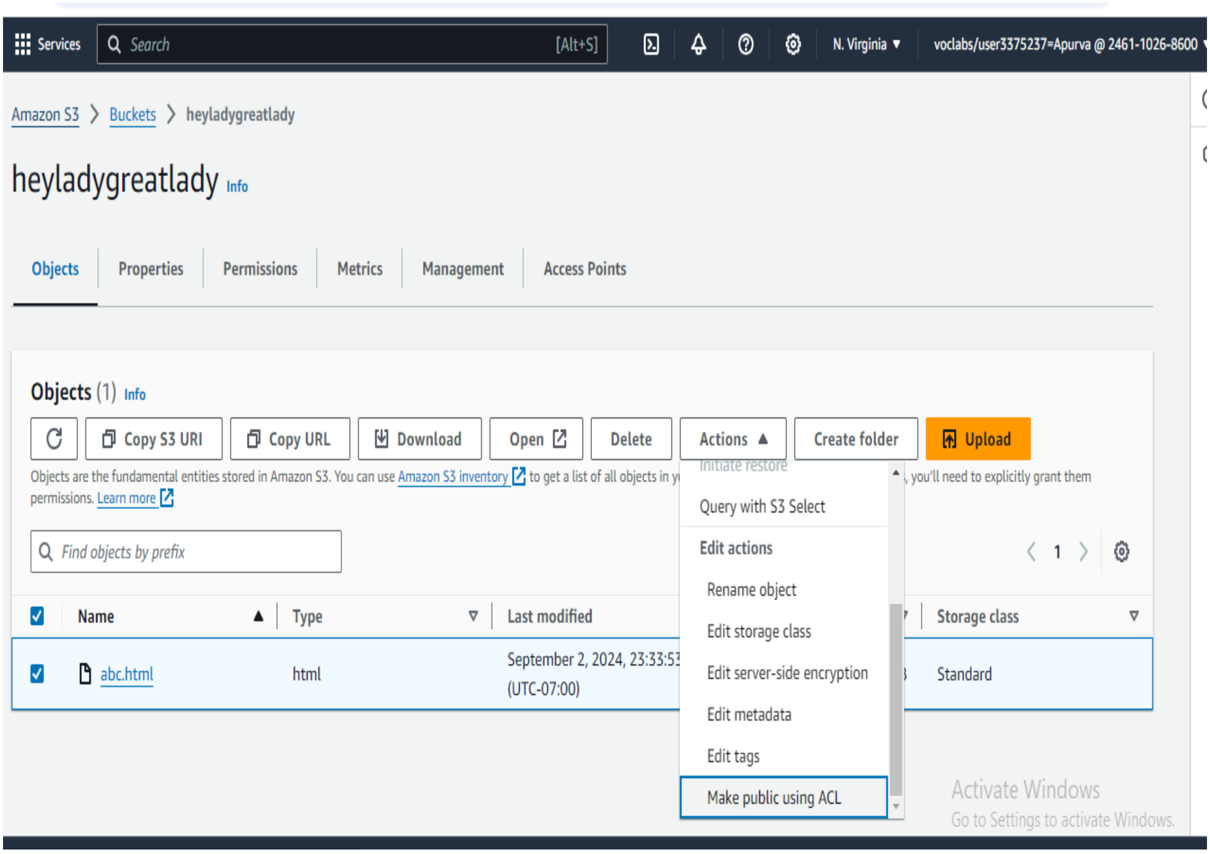
Permissions

Grant public access and access to other AWS accounts.

Properties

Specify storage class, encryption settings, tags, and more.

11.then select the file and go to Actions and Make public using ACL.



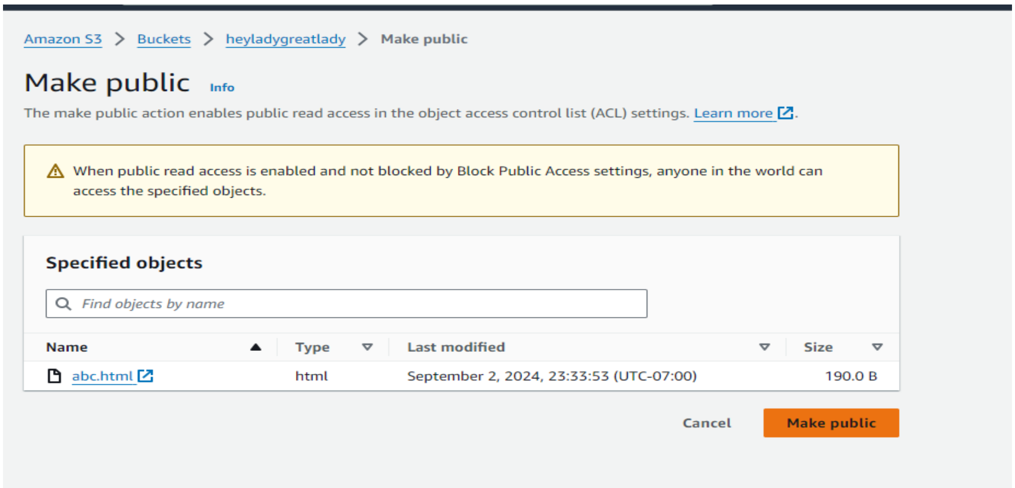
heyladygreatlady Info

Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in y… , you'll need to explicitly grant them permissions. Learn more

	Name	Type	Last modified	Storage class
☑	abc.html	html	September 2, 2024, 23:33:53 (UTC-07:00)	Standard

12.and click on Make public.



Amazon S3 > Buckets > heyladygreatlady > Make public

Make public Info

The make public action enables public read access in the object access control list (ACL) settings. Learn more

⚠ When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

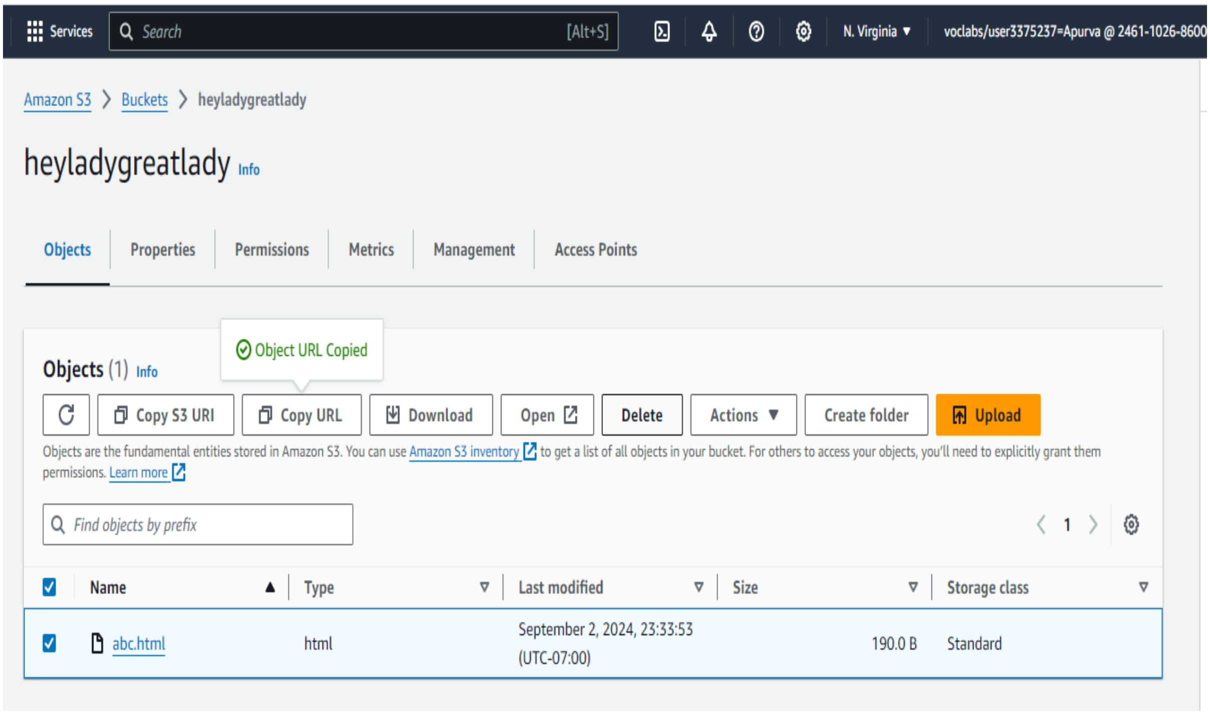
Specified objects

Find objects by name

Name	Type	Last modified	Size
abc.html	html	September 2, 2024, 23:33:53 (UTC-07:00)	190.0 B

3. Retrieve a File from S3 Bucket

1. In the S3 console, navigate to the bucket and find the file you uploaded
2. Click on the file name.
3. You can copy the URL to access the file.



Amazon S3 > Buckets > heyladygreatlady

heyladygreatlady Info

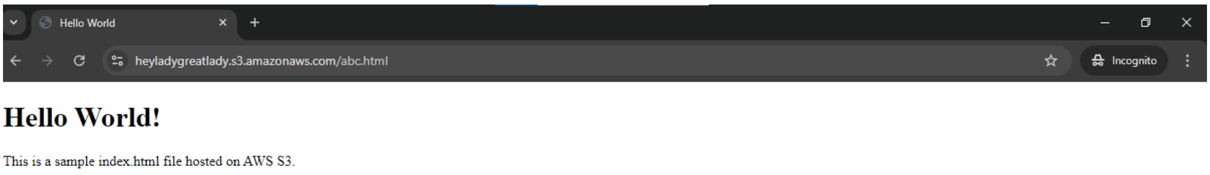
Objects (1) Info

✓ Object URL Copied

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

☑	Name	Type	Last modified	Size	Storage class
☑	abc.html	html	September 2, 2024, 23:33:53 (UTC-07:00)	190.0 B	Standard



Hello World!

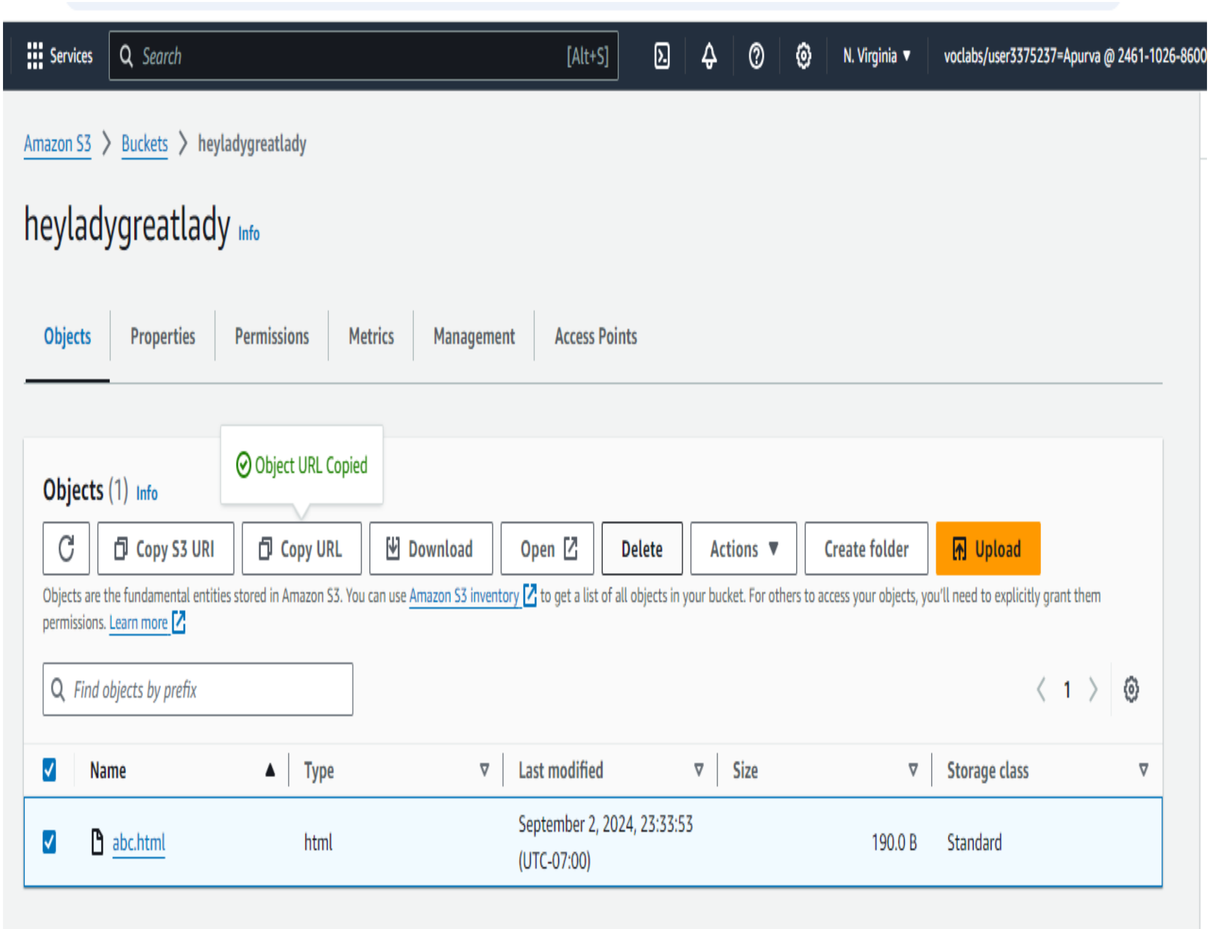
This is a sample index.html file hosted on AWS S3.

4. Delete a File from S3 Bucket

1. In the S3 console, go to the bucket and locate the file you want to delete.

2. Select the file by clicking the checkbox next to it.

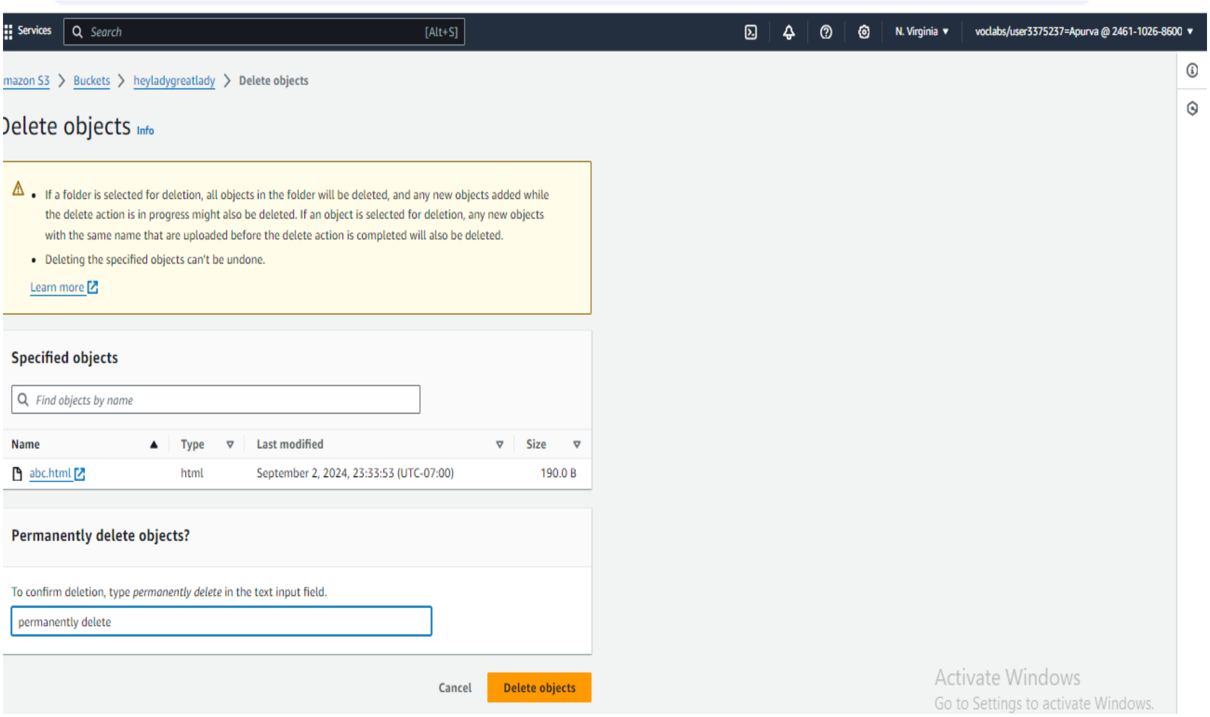
3. Click on Delete



Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

☑	Name ▲	Type	Last modified	Size	Storage class
☑	abc.html	html	September 2, 2024, 23:33:53 (UTC-07:00)	190.0 B	Standard

3. Confirm the deletion by clicking on Delete object.


Services
Search
[Alt+S]
N. Virginia ▾
voclabs/user3375237=Apurva @ 2461-1026-8600 ▾
mazon S3 > Buckets > heyladygreatlady > Delete objects
Info
Learn more
Cancel
Delete objects
Activate Windows
Go to Settings to activate Windows.

Delete objects

- If a folder is selected for deletion, all objects in the folder will be deleted, and any new objects added while the delete action is in progress might also be deleted. If an object is selected for deletion, any new objects with the same name that are uploaded before the delete action is completed will also be deleted.
- Deleting the specified objects can't be undone.

Specified objects

Find objects by name

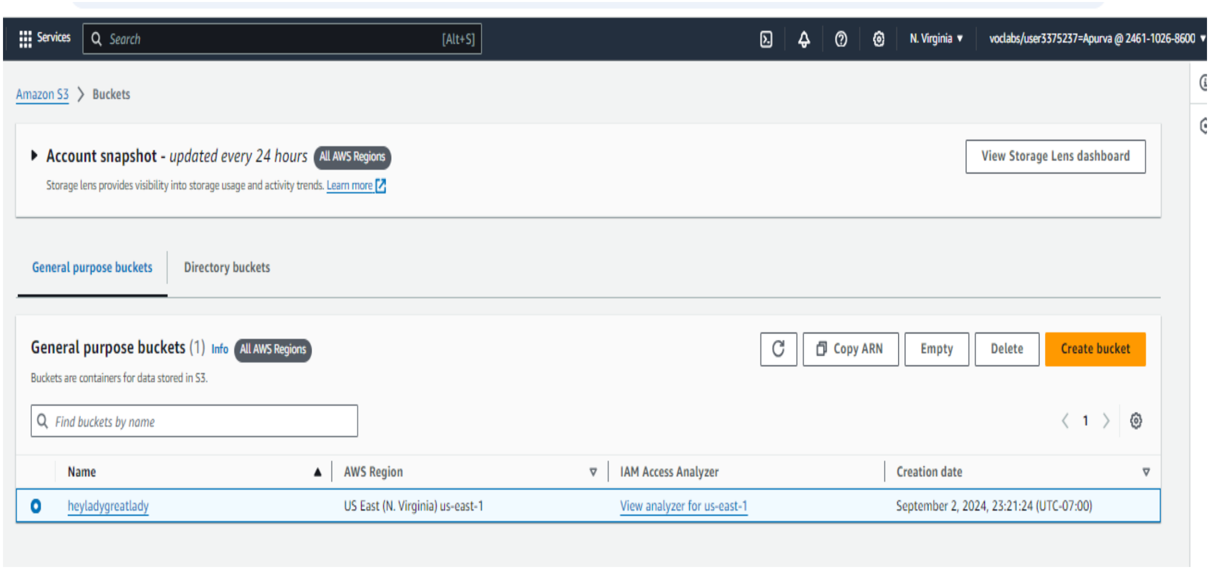
Name ▲	Type	Last modified	Size
abc.html	html	September 2, 2024, 23:33:53 (UTC-07:00)	190.0 B

Permanently delete objects?

To confirm deletion, type *permanently delete* in the text input field.

permanently delete

4.then select the Bucket and click on Delete.



Account snapshot - *updated every 24 hours*

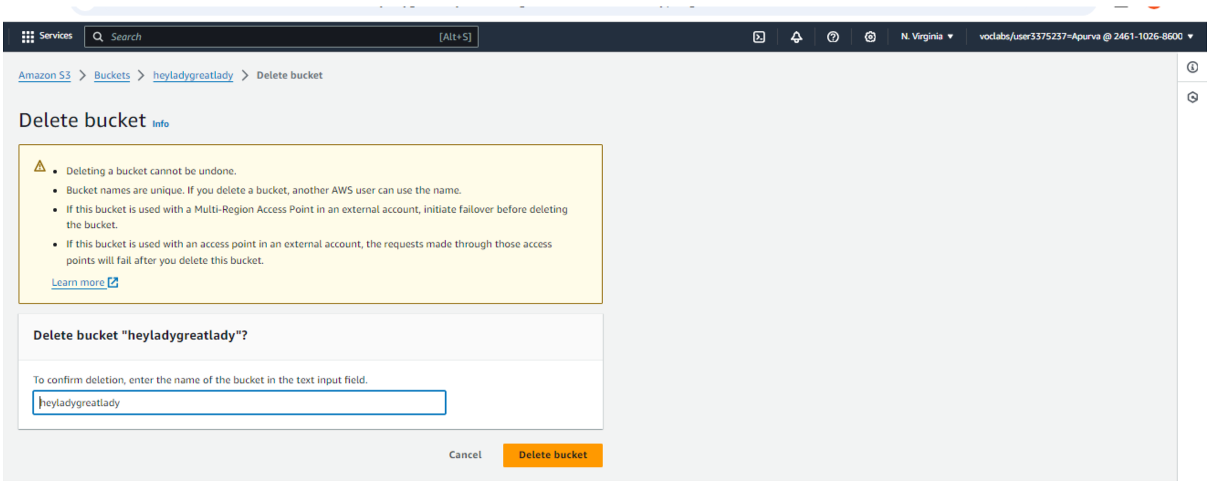
Storage lens provides visibility into storage usage and activity trends.

General purpose buckets (1)

Buckets are containers for data stored in S3.

	Name ▲	AWS Region	IAM Access Analyzer	Creation date
●	heyladygreatlady	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 2, 2024, 23:21:24 (UTC-07:00)

5. Confirm the deletion by clicking on Delete bucket.



Services
Search
[Alt+S]
N. Virginia
voclabs/user3375237=Apurva @ 2461-1026-8600
Amazon S3 > Buckets > heyladygreatlady > Delete bucket

Delete bucket Info

- Deleting a bucket cannot be undone.
- Bucket names are unique. If you delete a bucket, another AWS user can use the name.
- If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
- If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.

Learn more

Delete bucket "heyladygreatlady"?

To confirm deletion, enter the name of the bucket in the text input field.

heyladygreatlady