Terna Engineering College
Computer Engineering Department
Program: Sem VIII

Course: Cloud Computing Lab (CSL803)

Faculty: Reshma Koli

Experiment No. 4

A.1 Aim: To demonstrate and implement Storage as a service using AWS S3 Service.

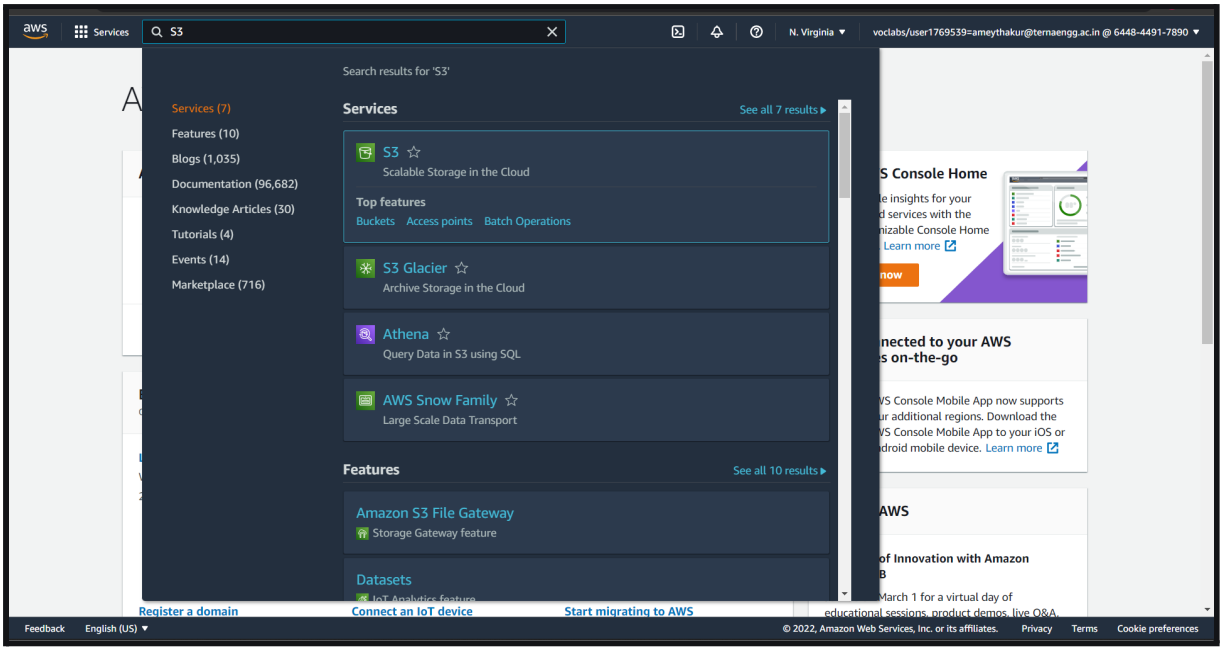
PART B
(PART B: TO BE COMPLETED BY STUDENTS)

Roll No. 50	**Name:** AMEY MAHENDRA THAKUR
Class: BE COMPS B 50	**Batch:** B3
Date of Experiment: 14-02-2022	**Date of Submission:** 14-02-2022
Grade:	

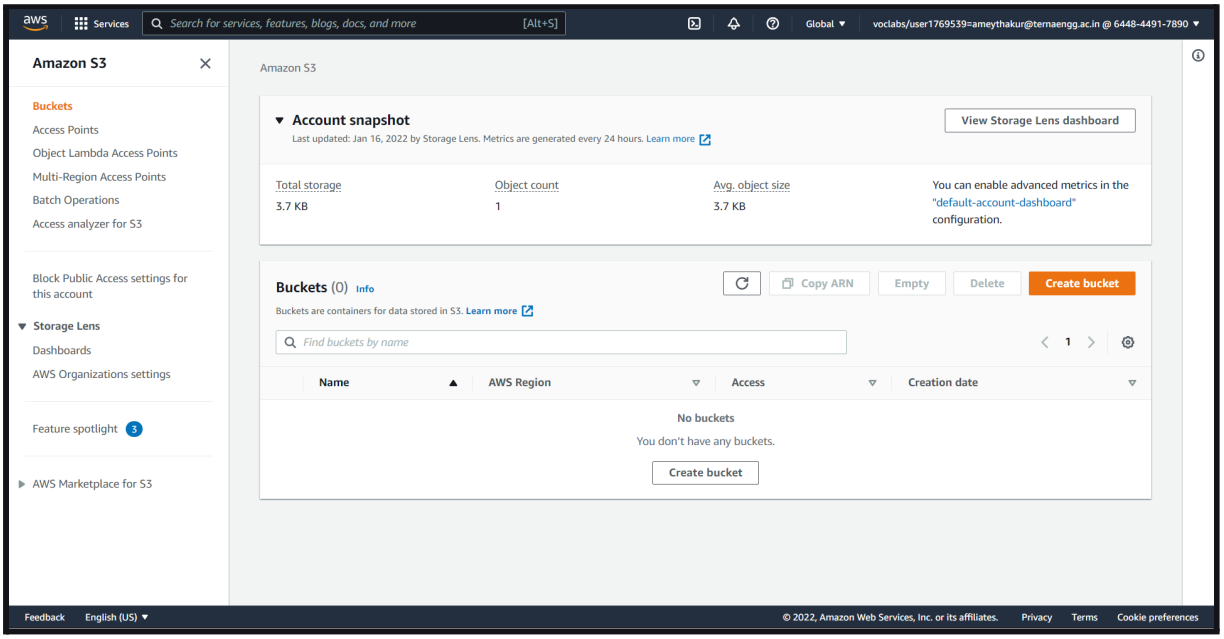
B.1 Question of Curiosity:
Q1: Create Bucket using AWS S3 service (Add stepwise screenshots of the same).
ANS:

Practical Video (AWS S3 Service): https://youtu.be/CnM07Vg7pW8

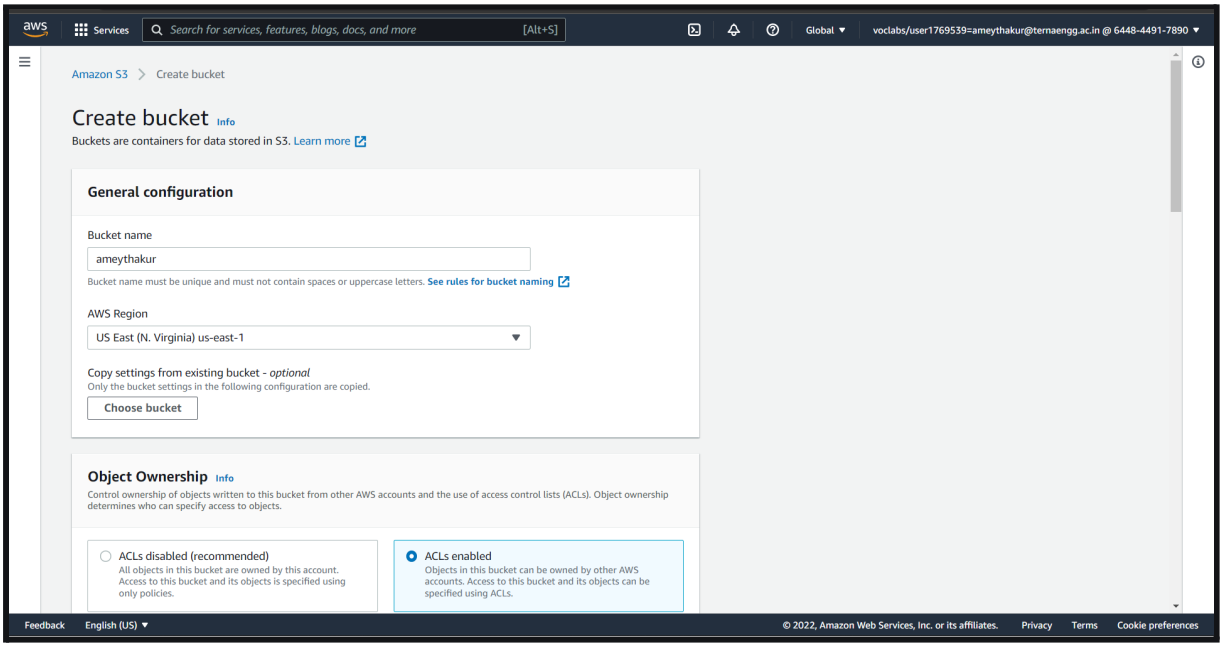
Step 1:



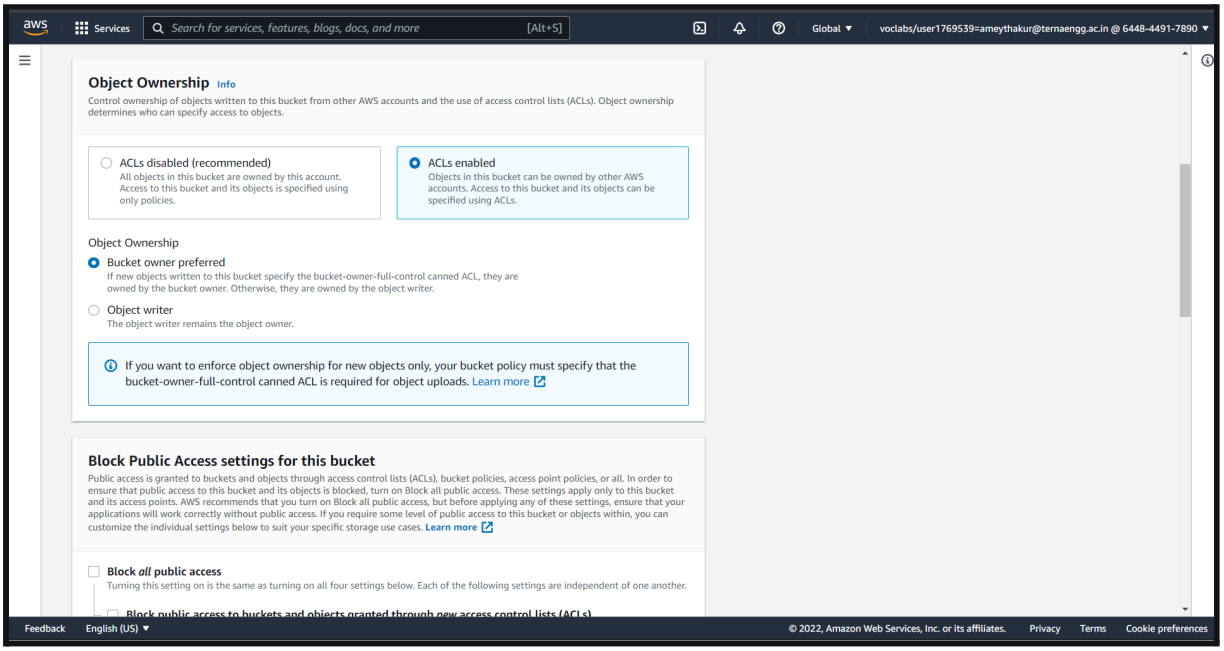
Step 2:


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Account snapshot
View Storage Lens dashboard
Total storage
3.7 KB
Object count
1
Avg. object size
3.7 KB
Buckets (0) Info
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
No buckets
You don't have any buckets.
Create bucket
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

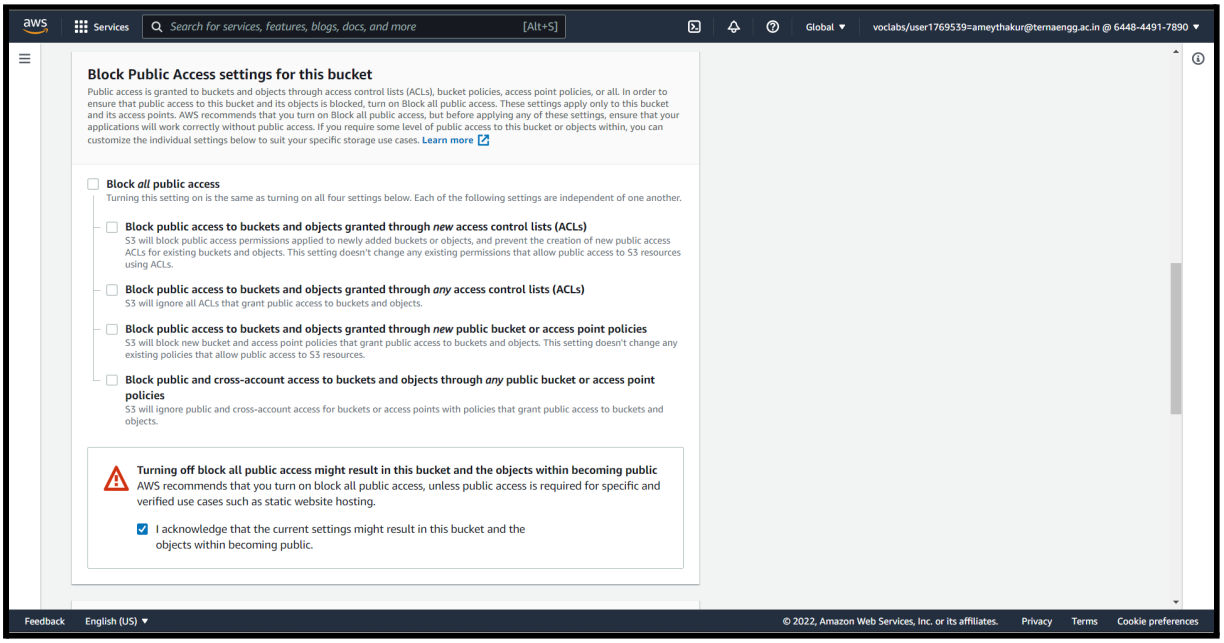
Step 3:


Amazon S3 > Create bucket
Create bucket Info
Buckets are containers for data stored in S3. Learn more
General configuration
Bucket name
ameythakur
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
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.
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

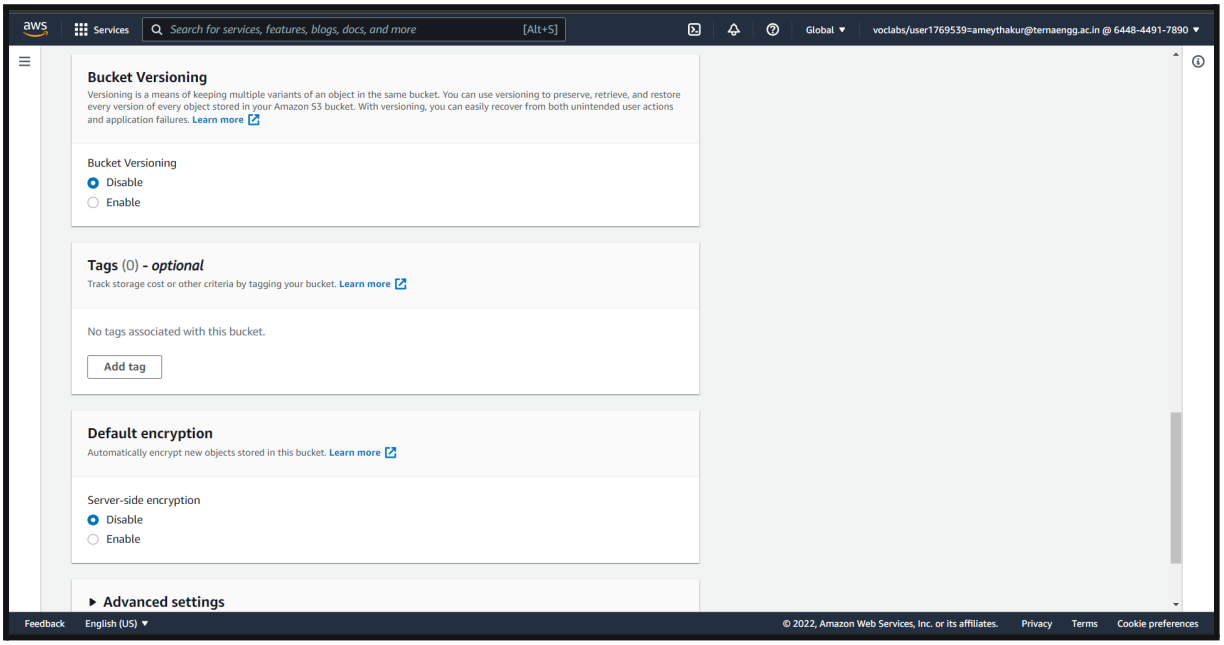
Step 4:


Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
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 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.
If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more
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.
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

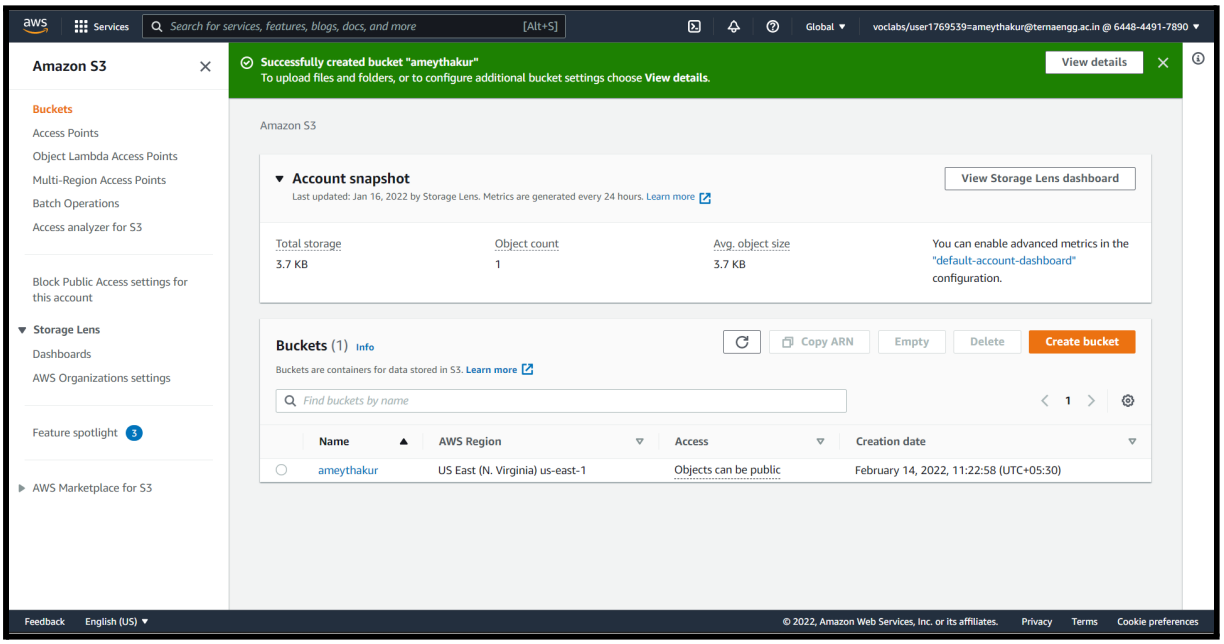
Step 5:


Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
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.
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

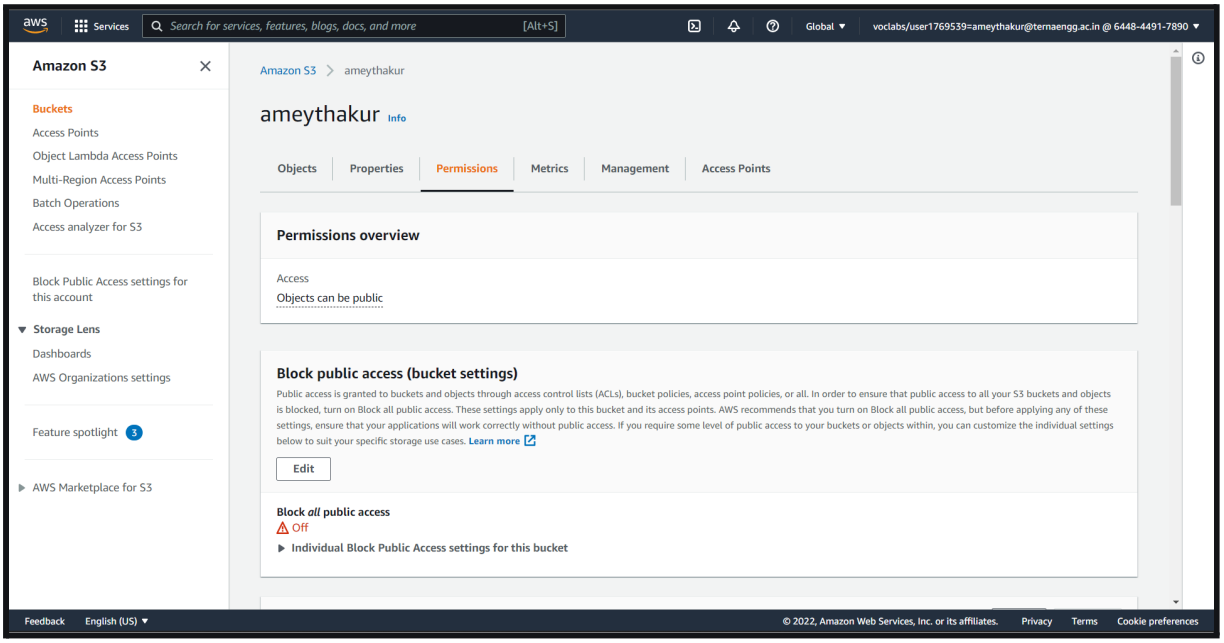
Step 6:


Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
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
Tags (0) - optional
Track storage cost or other criteria by tagging your bucket. Learn more
No tags associated with this bucket.
Add tag
Default encryption
Automatically encrypt new objects stored in this bucket. Learn more
Server-side encryption
Disable
Enable
Advanced settings
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

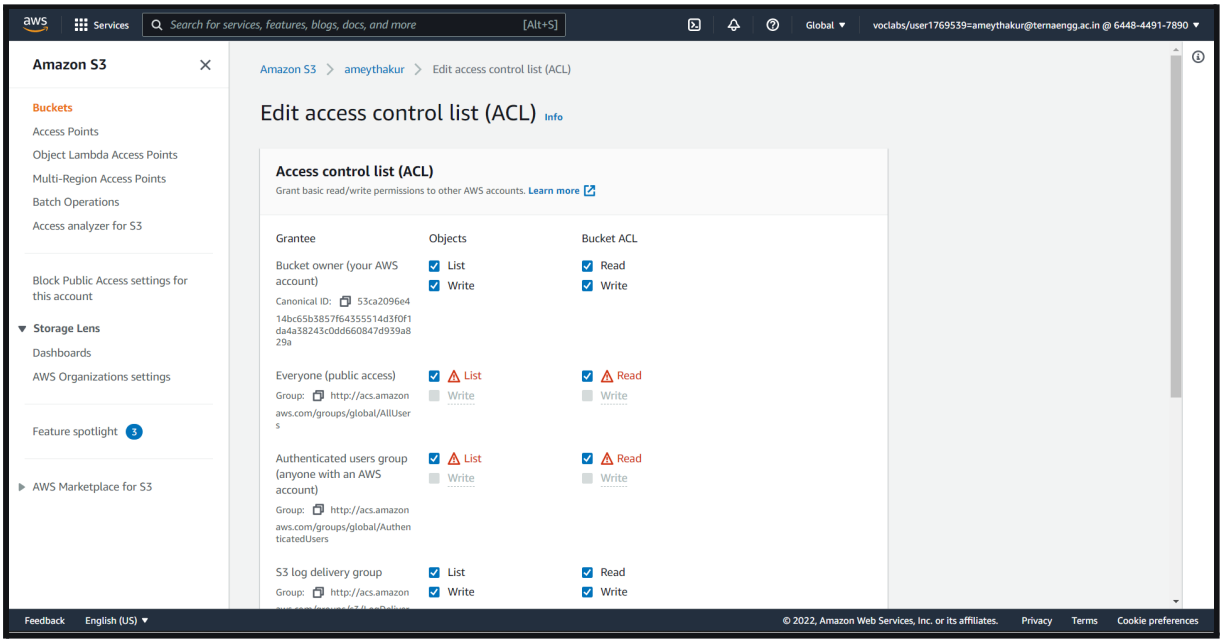
Step 7:


Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Successfully created bucket "ameythakur"
To upload files and folders, or to configure additional bucket settings choose View details.
View details
Amazon S3
Account snapshot
Last updated: Jan 16, 2022 by Storage Lens. Metrics are generated every 24 hours. Learn more
View Storage Lens dashboard
Total storage
3.7 KB
Object count
1
Avg. object size
3.7 KB
You can enable advanced metrics in the "default-account-dashboard" configuration.
Buckets (1) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
ameythakur
US East (N. Virginia) us-east-1
Objects can be public
February 14, 2022, 11:22:58 (UTC+05:30)
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

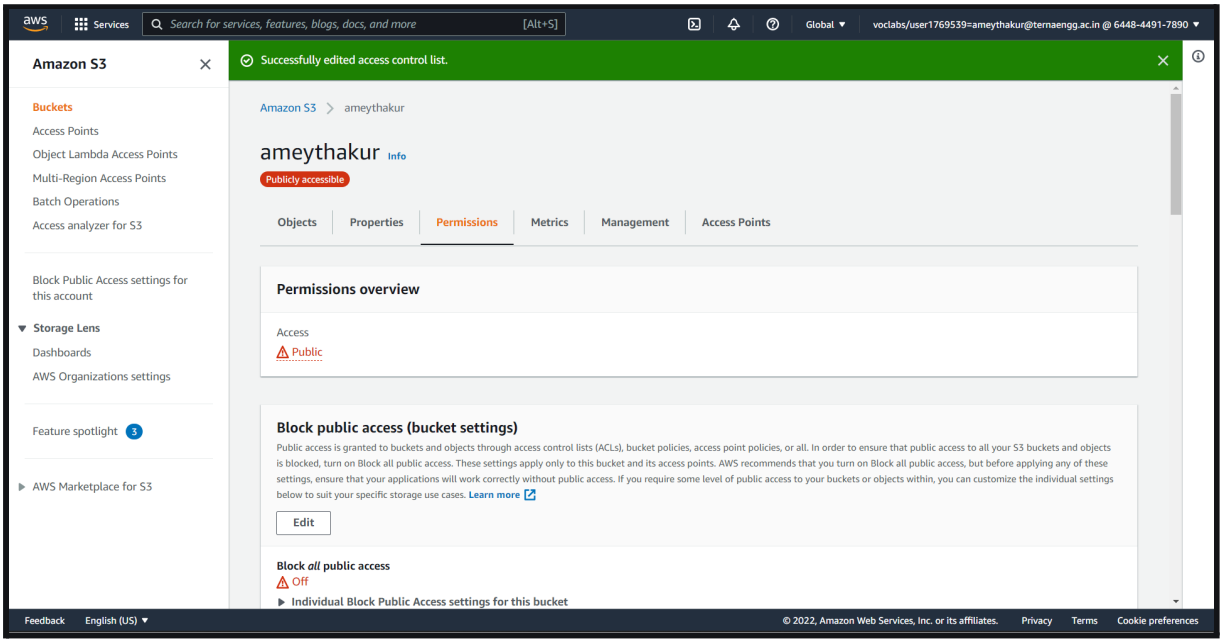
Step 8:


Amazon S3
ameythakur
Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Objects can be public
Block public access (bucket settings)
Edit
Block all public access
Off
Individual Block Public Access settings for this bucket

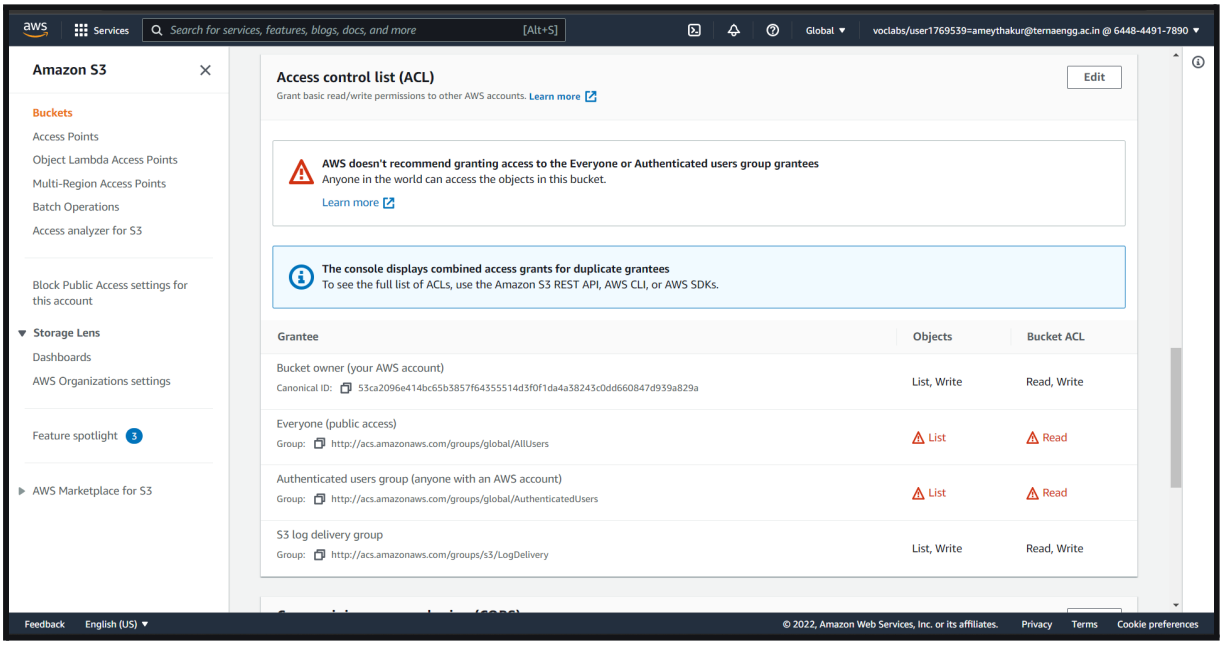
Step 9:


Amazon S3
ameythakur
Edit access control list (ACL)
Info
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts.
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
Everyone (public access)
Authenticated users group (anyone with an AWS account)
S3 log delivery group

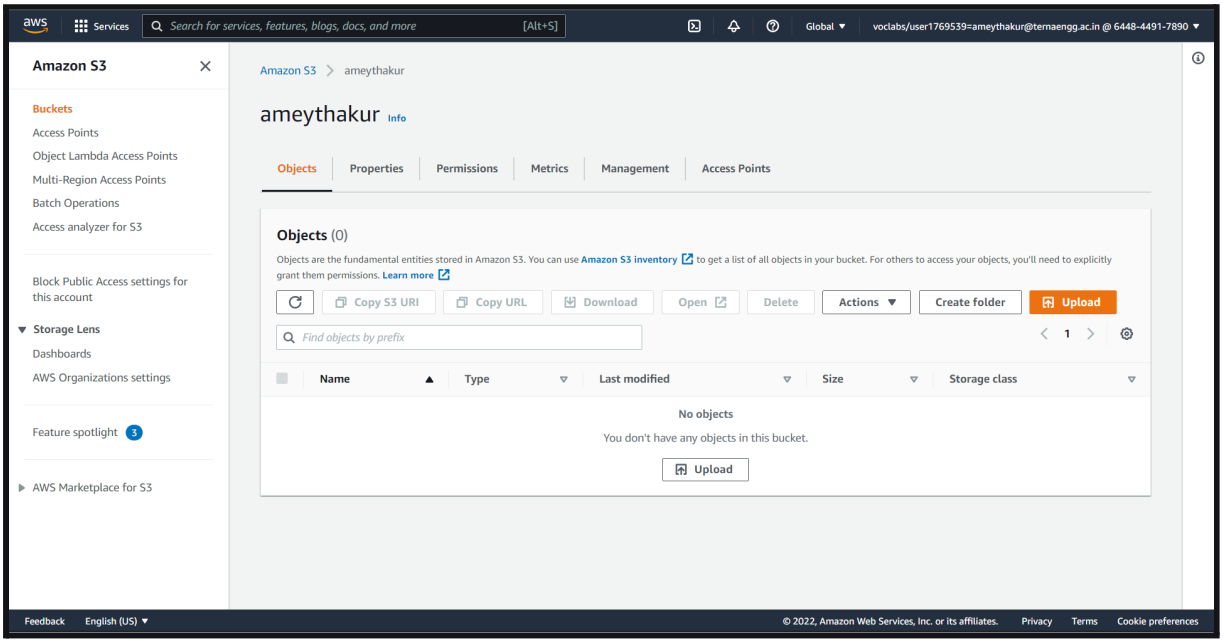
Step 10:



Step 11:

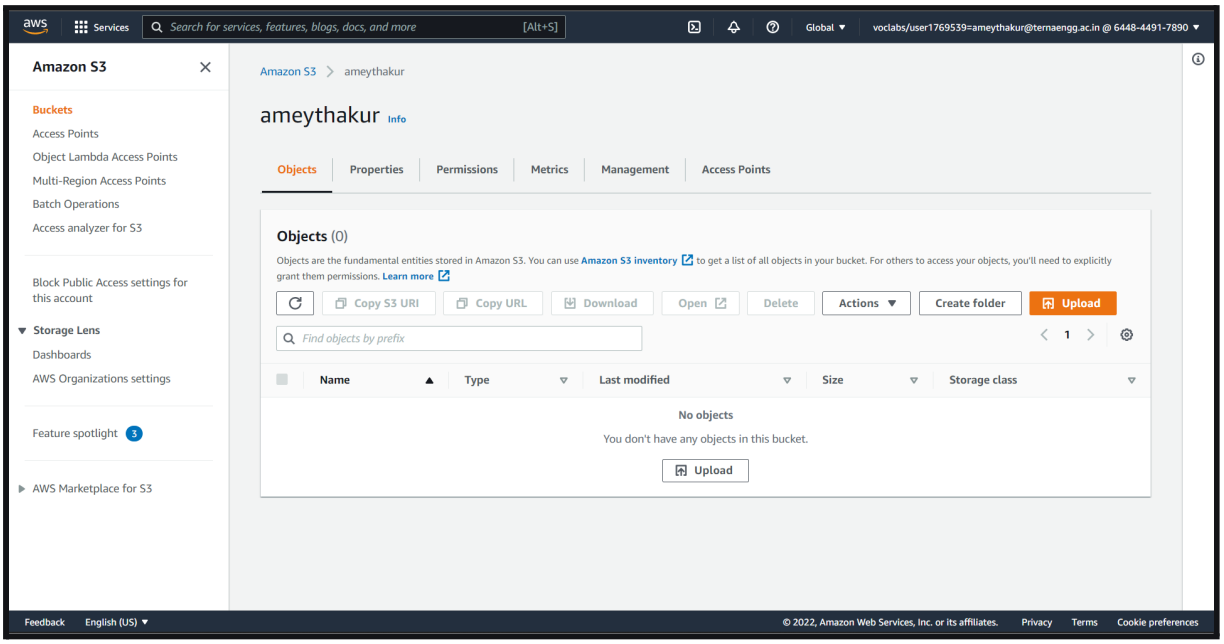


Step 12:

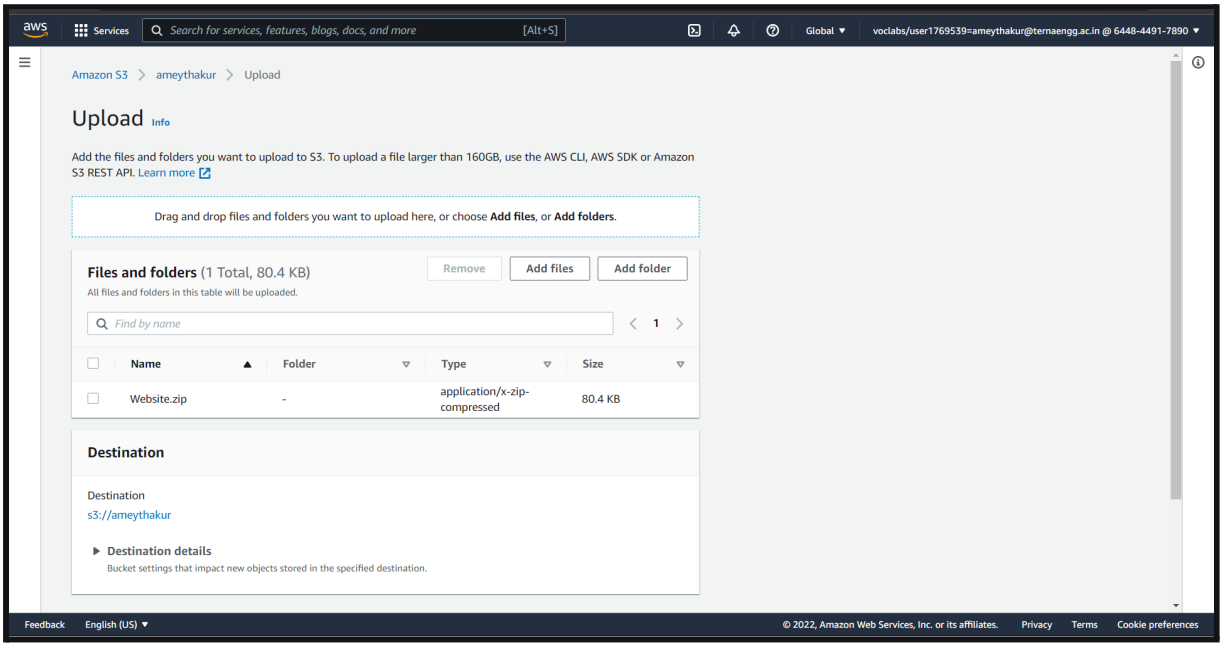


Q2: Add Objects to Bucket created (Add stepwise screenshots of the same).
ANS:

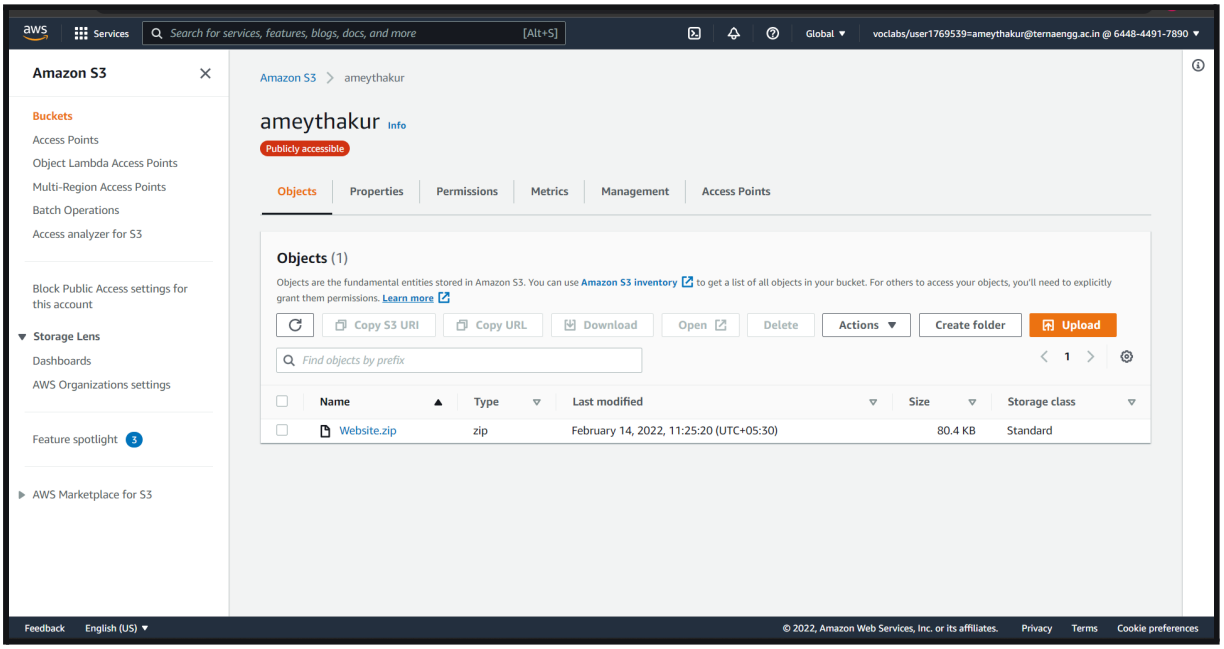
Step 1:



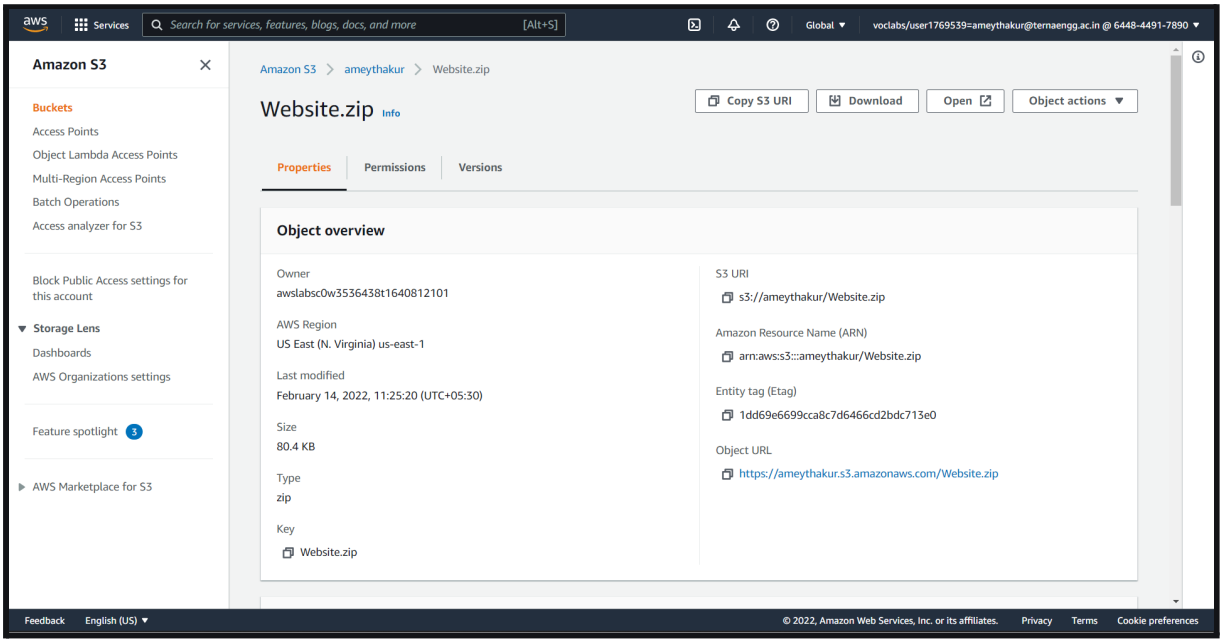
Step 2:


Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3 > ameythakur > 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 folders.
Files and folders (1 Total, 80.4 KB)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
1
Name
Folder
Type
Size
Website.zip
-
application/x-zip-compressed
80.4 KB
Destination
Destination
s3://ameythakur
Destination details
Bucket settings that impact new objects stored in the specified destination.
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 3:


Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
3
AWS Marketplace for S3
Amazon S3 > ameythakur
ameythakur Info
Publicly accessible
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1)
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
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
1
Name
Type
Last modified
Size
Storage class
Website.zip
zip
February 14, 2022, 11:25:20 (UTC+05:30)
80.4 KB
Standard
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 4:



Q3: Compare Google Drive with AWS S3.
ANS:

GOOGLE DRIVE	AMAZON S3
It is owned by Google LLC.	It is owned by Amazon.
It was launched in 2012.	It was launched in 2006.
It offers 15 GB of free storage space.	It does not offer free storage space.
It was developed by Google.	It was developed by Amazon Web Services (AWS).
The number of users using Google Drive is more.	The number of users using Amazon S3 is less.
It provides full security of data.	It also provides full security of data but comparatively less.

It has a maximum storage size of 30 TB.	It has an unlimited maximum storage size for paid users.
It does not support remote uploading.	Remote uploading is not supported here also.
The maximum file size in Google Drive is 5 TB.	Here the maximum file size is 5 GB.
It supports file versioning.	It also supports file versioning.
It does not require a credit card for free services.	It requires credit-card details for a free trial.

B.2 Conclusion:

Using an Amazon AWS Free Tier Account, we learned Storage as a Service and how to use the Amazon S3 Service. On AWS, we were able to successfully host a website by using S3 storage.