Name :- Anjali punsl
Class:- D20B
Roll no - 57
Experiment no 7

Aim :- To study and Implement Storage as a Service using Own Cloud/ AWS, Glaciers

Theory :-

Storage as a Service (STaaS) is a cloud computing model that provides scalable and on-demand storage to users over the internet. It allows users to access and manage their data without the need for owning or maintaining physical storage infrastructure. Implementing STaaS involves managing storage resources, including provisioning, allocation, and monitoring of storage capacity, ensuring data availability, integrity, and security. Data lifecycle management, security, scalability, cost management, and integration are key aspects of implementing STaaS using OwnCloud or AWS Glacier. It's important to carefully plan and design your STaaS implementation to meet your specific storage requirements and business needs.Storage as a Service (STaaS) is a cloud computing model that provides scalable and on-demand storage to users over the internet. It allows users to access and manage their data without the need for owning or maintaining physical storage infrastructure.

There are several key concepts and technologies involved in implementing STaaS using OwnCloud or AWS Glacier:

OwnCloud: OwnCloud is an open-source software suite that provides a cloud storage solution similar to Dropbox or Google Drive. It allows you to create a private cloud storage platform that you can host and manage yourself.

AWS Glacier: AWS Glacier is a low-cost storage service provided by Amazon Web Services (AWS) designed for data archiving and long-term backup. It is optimized for infrequently accessed data that requires long-term retention.

Storage Management: Implementing STaaS involves managing storage resources, including provisioning, allocation, and monitoring of storage capacity. This includes ensuring data availability, integrity, and security.

Data Lifecycle Management: STaaS solutions often include features for managing the lifecycle of data, including automated data archiving, retention policies, and data expiration.

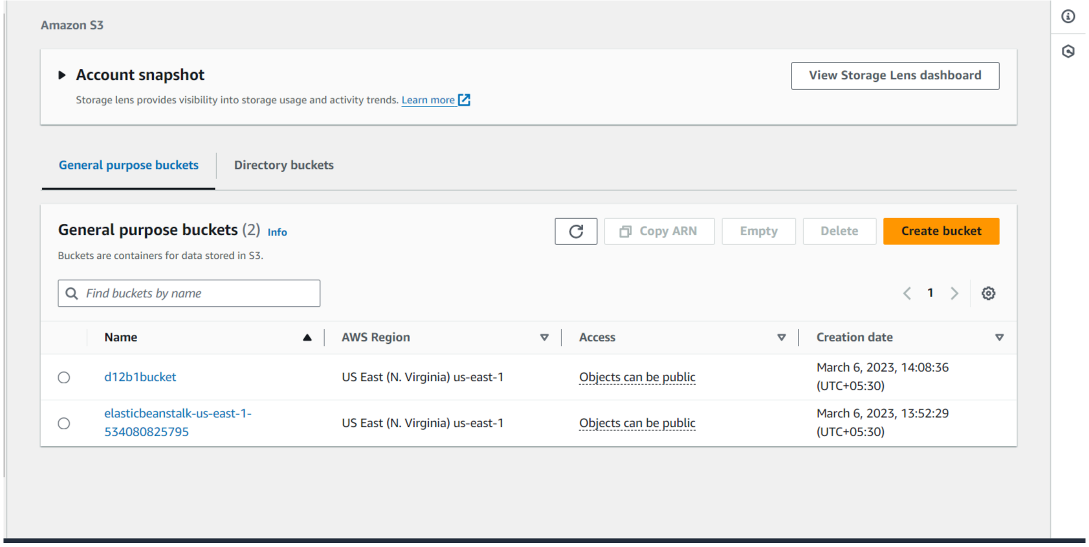
Security: Security is a critical aspect of STaaS, including data encryption, access control, and compliance with data protection regulations.

Scalability: STaaS solutions should be scalable to accommodate growing storage needs, allowing users to easily expand storage capacity as needed.

Implementing STaaS using OwnCloud or AWS Glacier requires a solid understanding of these concepts and technologies, as well as hands-on experience with cloud storage solutions. It's important to carefully plan and design your STaaS implementation to meet your specific storage requirements and business needs.

Steps :-

Step 1 :- In aws click S3 Then click on create bucket



Amazon S3

Account snapshot

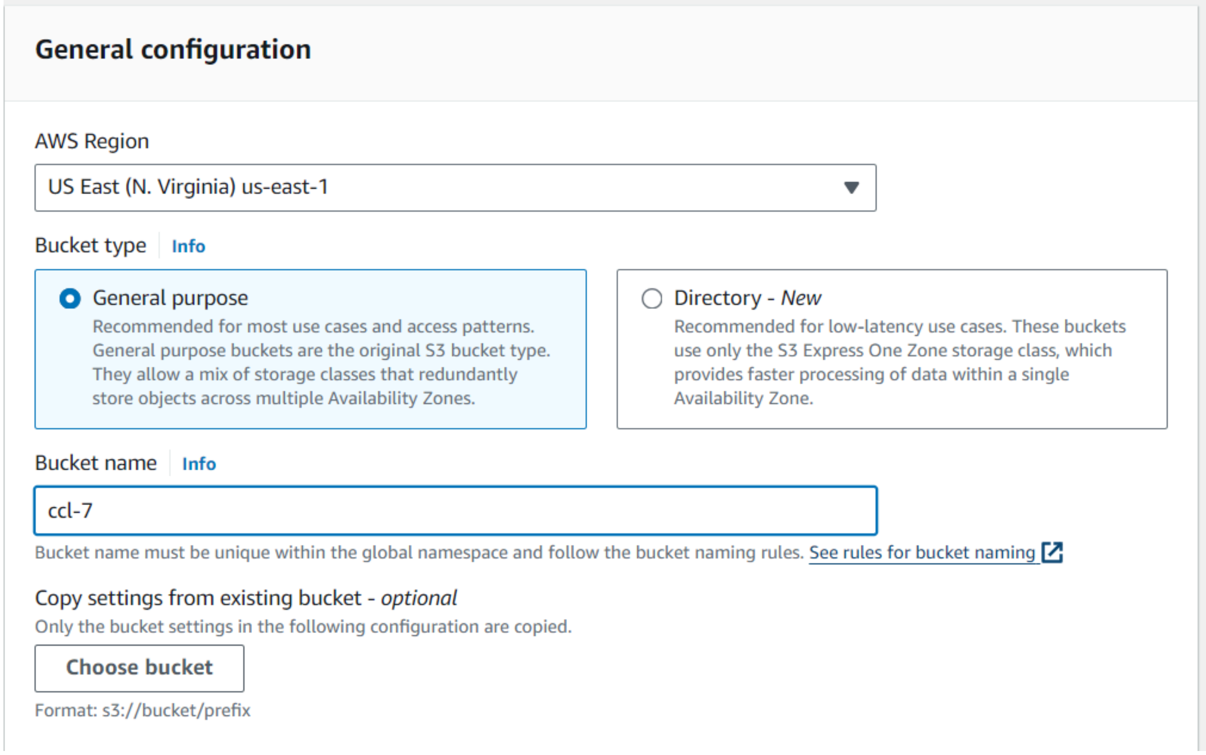
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (2) Info

Buckets are containers for data stored in S3.

	Name	AWS Region	Access	Creation date
○	d12b1bucket	US East (N. Virginia) us-east-1	Objects can be public	March 6, 2023, 14:08:36 (UTC+05:30)
○	elasticbeanstalk-us-east-1-534080825795	US East (N. Virginia) us-east-1	Objects can be public	March 6, 2023, 13:52:29 (UTC+05:30)

Step-2: Give Bucket name & select region for storage



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 - *New*
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

ccl-7

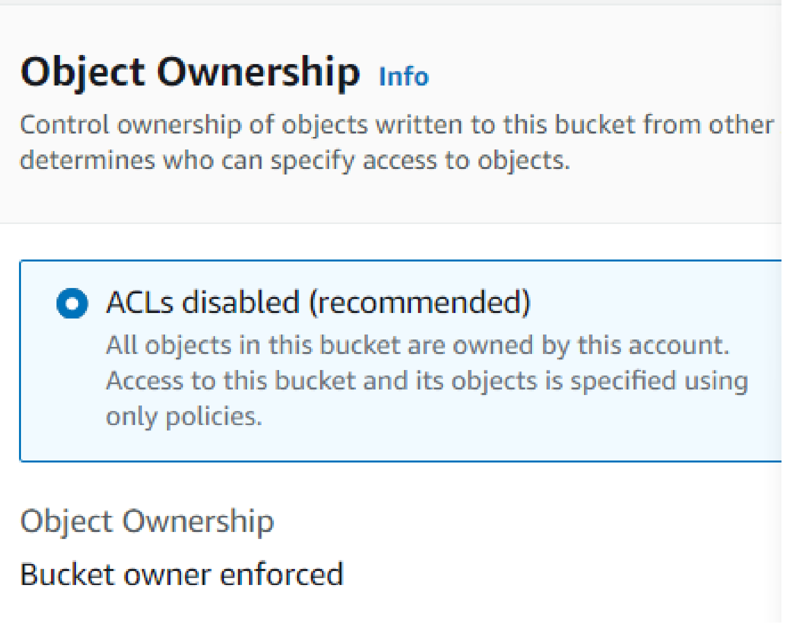
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Step-3: Keep object ownership setting as ACLs Disabled as by-default



Object Ownership Info

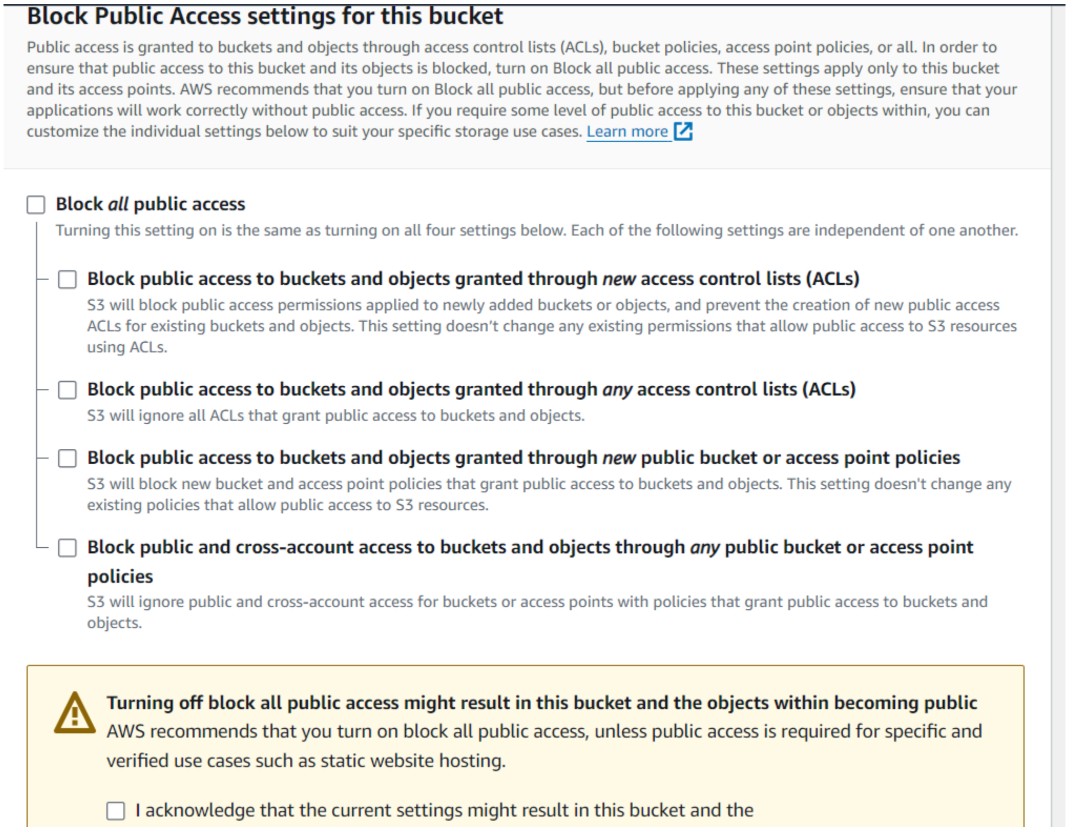
Control ownership of objects written to this bucket from other
determines who can specify access to objects.

● 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.

Object Ownership

Bucket owner enforced

Step-4: Disable block all public access checkbox but click on i acknowledge



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.

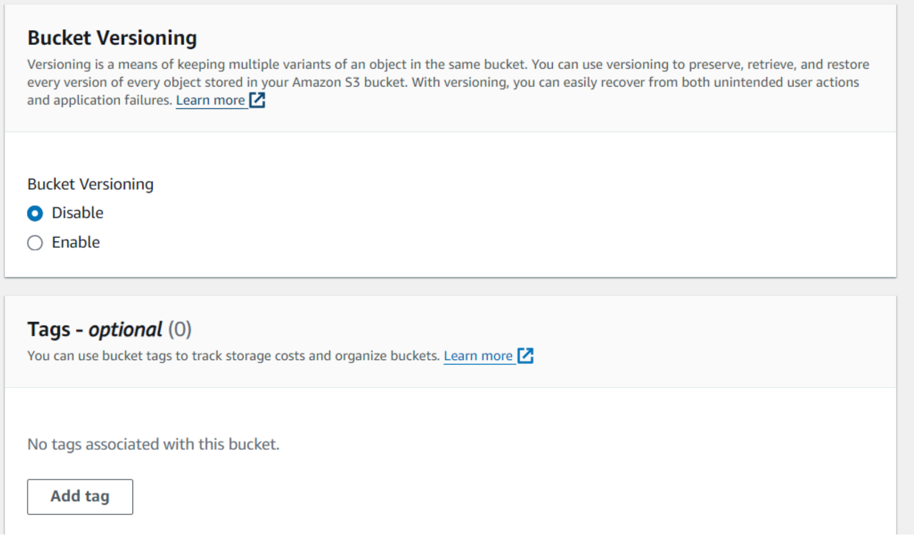
- □ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any 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

Step-5: Select the checkbox for Turning off block all public access might result in this bucket and the objects within becoming public

Step-6: Keep bucket versioning as disabled and add tags if required.



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

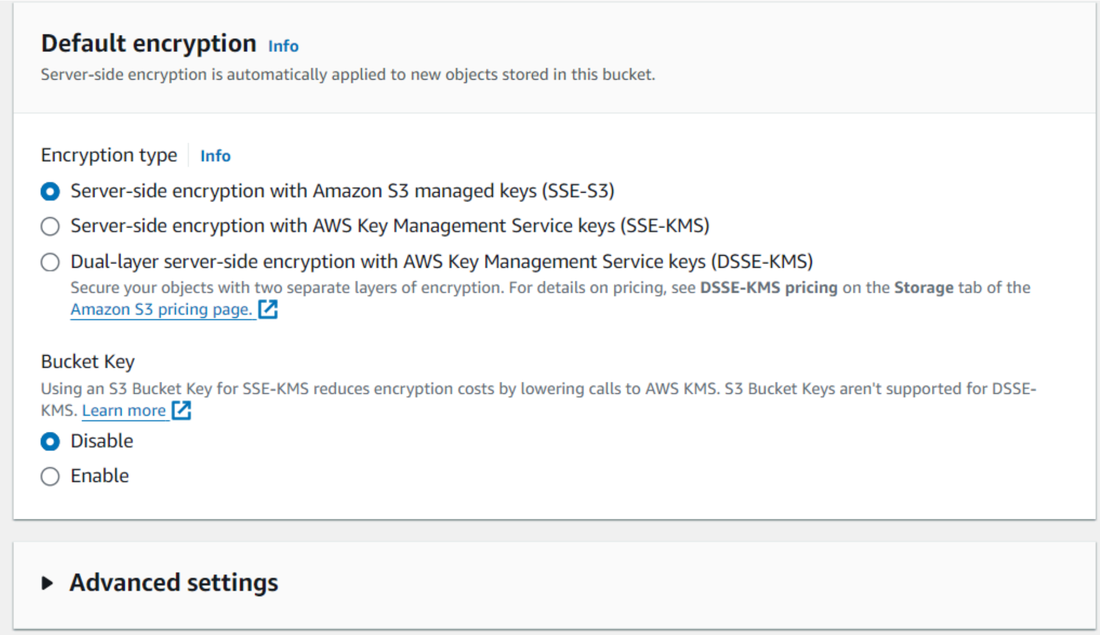
○ Enable

Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.

Step-7: Keep default encryption disabled and click on create bucket button



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type | Info

● Server-side encryption with Amazon S3 managed keys (SSE-S3)

○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

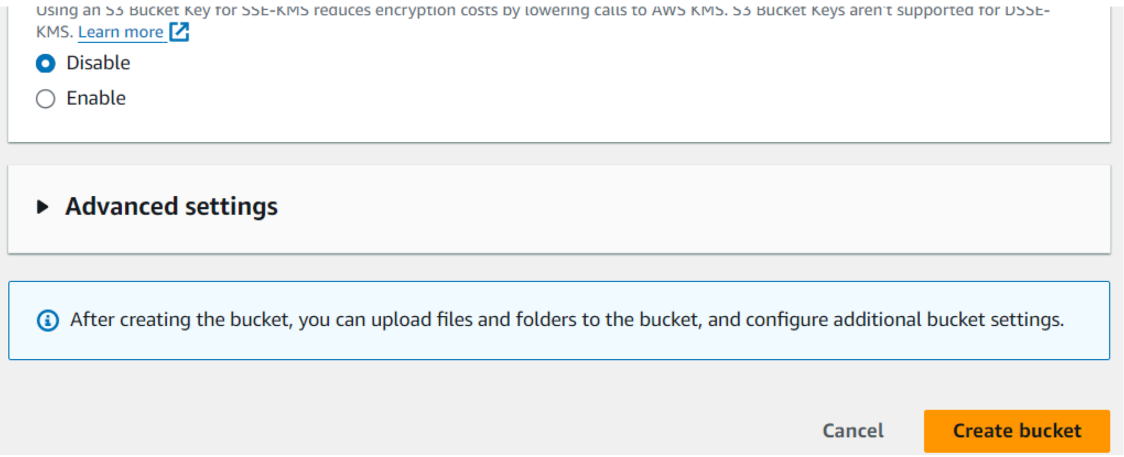
Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

● Disable

○ Enable

Click on create bucket



Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

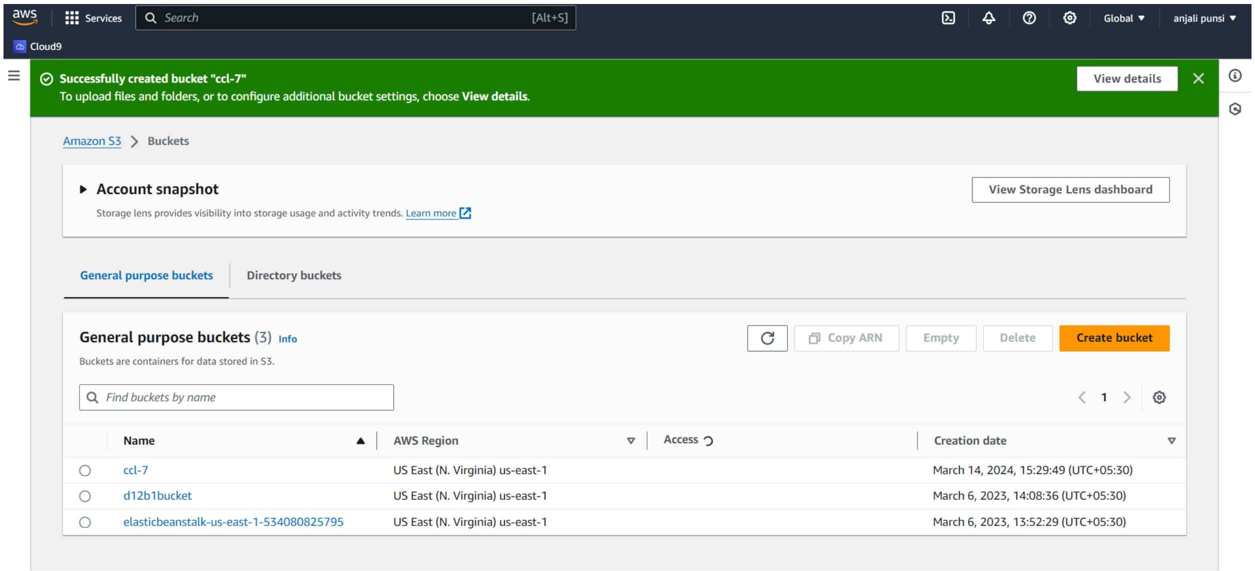
● Disable

○ Enable

▸ Advanced settings

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

You can now see the successful creation of your bucket



Successfully created bucket "ccl-7"

To upload files and folders, or to configure additional bucket settings, choose **View details**.

Amazon S3 > Buckets

▸ Account snapshot

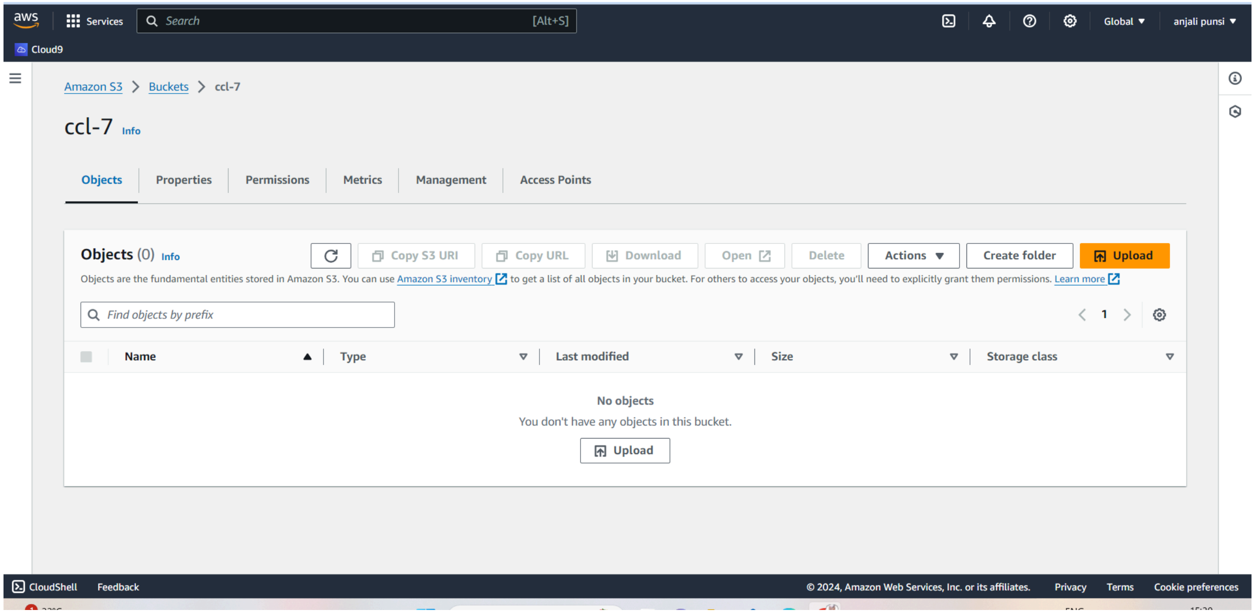
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (3) Info

Buckets are containers for data stored in S3.

	Name	AWS Region	Access	Creation date
○	ccl-7	US East (N. Virginia) us-east-1		March 14, 2024, 15:29:49 (UTC+05:30)
○	d12b1bucket	US East (N. Virginia) us-east-1		March 6, 2023, 14:08:36 (UTC+05:30)
○	elasticbeanstalk-us-east-1-534080825795	US East (N. Virginia) us-east-1		March 6, 2023, 13:52:29 (UTC+05:30)

Step-8: now click on the bucket that you have created and You can either create a folder here or upload an existing file in the bucket now click on upload button and click on add files button browse your local machine and select which file you need to upload on S3 next click on upload button at bottom right end



ccl-7 Info

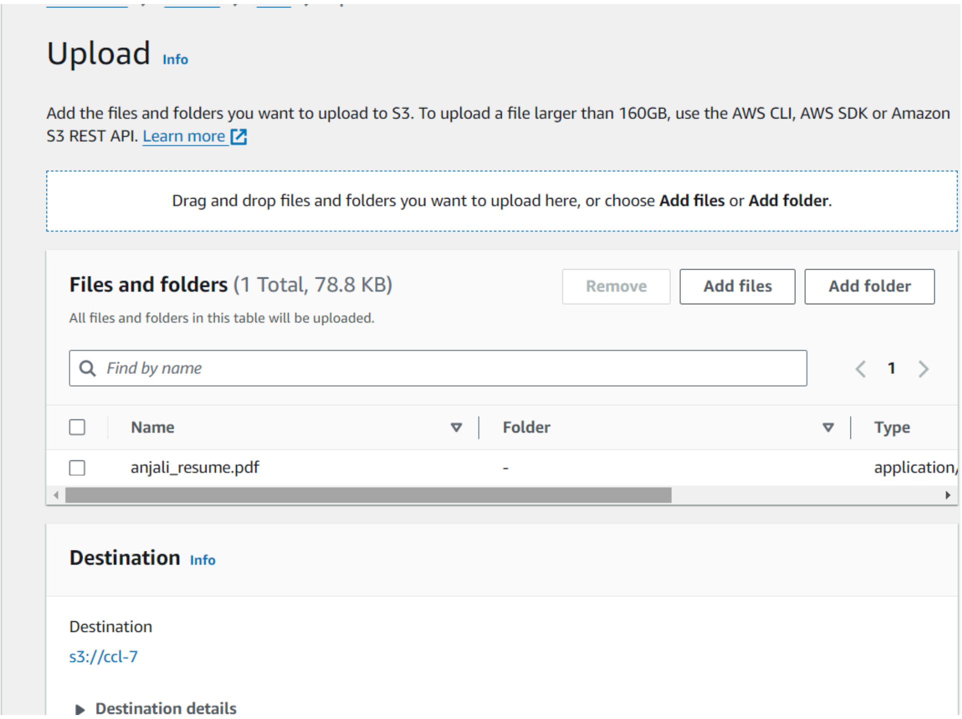
Objects (0) Info

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

No objects

You don't have any objects in this bucket.

© 2024, Amazon Web Services, Inc. or its affiliates.



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, 78.8 KB)

All files and folders in this table will be uploaded.

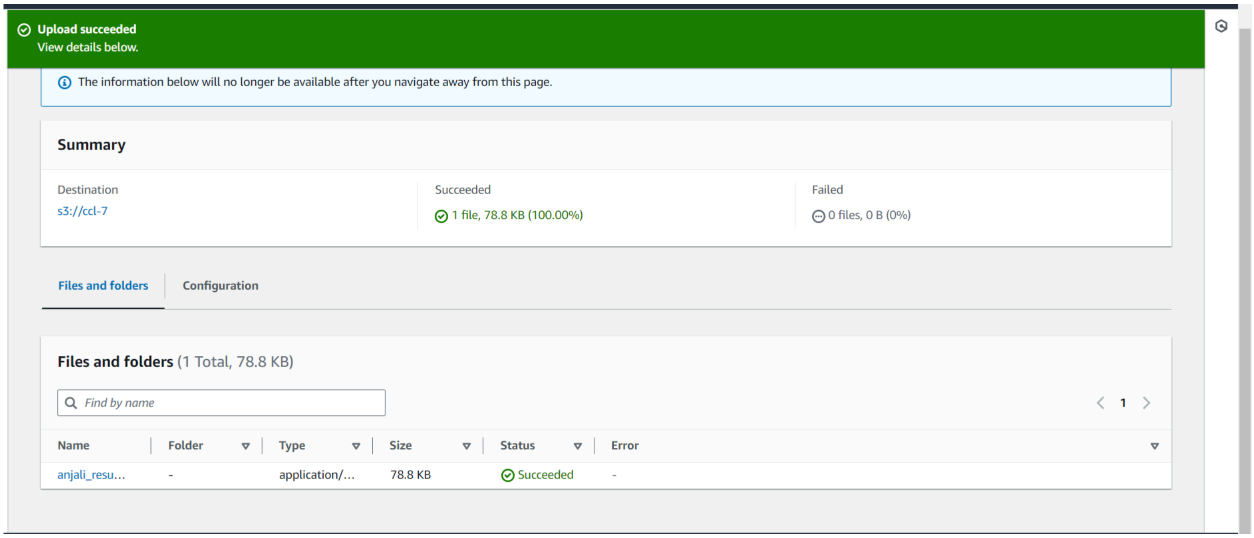
Name	Folder	Type
anjali_resume.pdf	-	application,

Destination Info

Destination

s3://ccl-7

Now you can check the upload status screen so mine is success yeahhhh!!!!!!!



Upload succeeded
View details below.

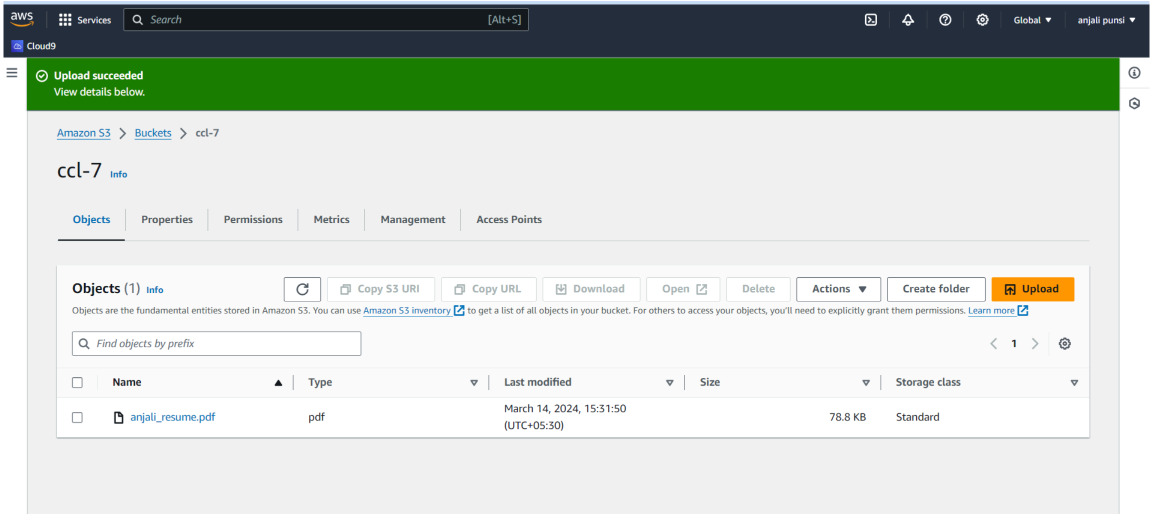
The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://ccl-7	1 file, 78.8 KB (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 78.8 KB)

Name	Folder	Type	Size	Status	Error
anjali_resu...	-	application/...	78.8 KB	Succeeded	-



Upload succeeded
View details below.

Amazon S3 > Buckets > ccl-7

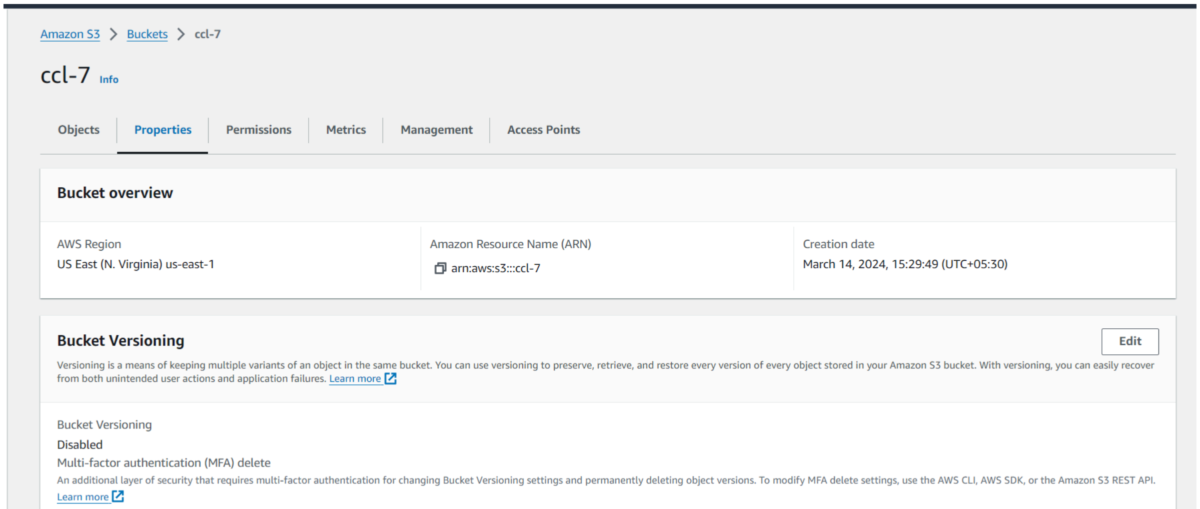
ccl-7 Info

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 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
□	anjali_resume.pdf	pdf	March 14, 2024, 15:31:50 (UTC+05:30)	78.8 KB	Standard

Step 9 :-Now click on close button The screen will appear as below



Amazon S3 > Buckets > ccl-7

ccl-7 Info

Bucket overview

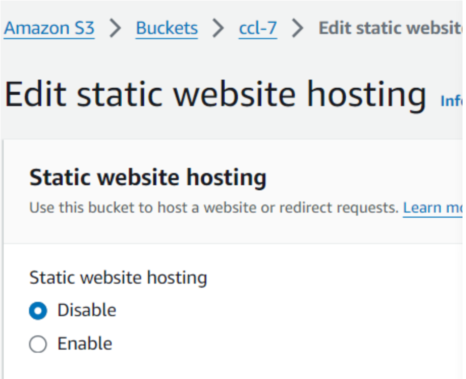
AWS Region	Amazon Resource Name (ARN)	Creation date
US East (N. Virginia) us-east-1	arn:aws:s3:::ccl-7	March 14, 2024, 15:29:49 (UTC+05:30)

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
Disabled
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more

Step-10: Select properties and scroll down to **Static website hosting** option which is disabled now click on Edit option on right side



Amazon S3 > Buckets > ccl-7 > Edit static websit

Edit static website hosting Inf

Static website hosting

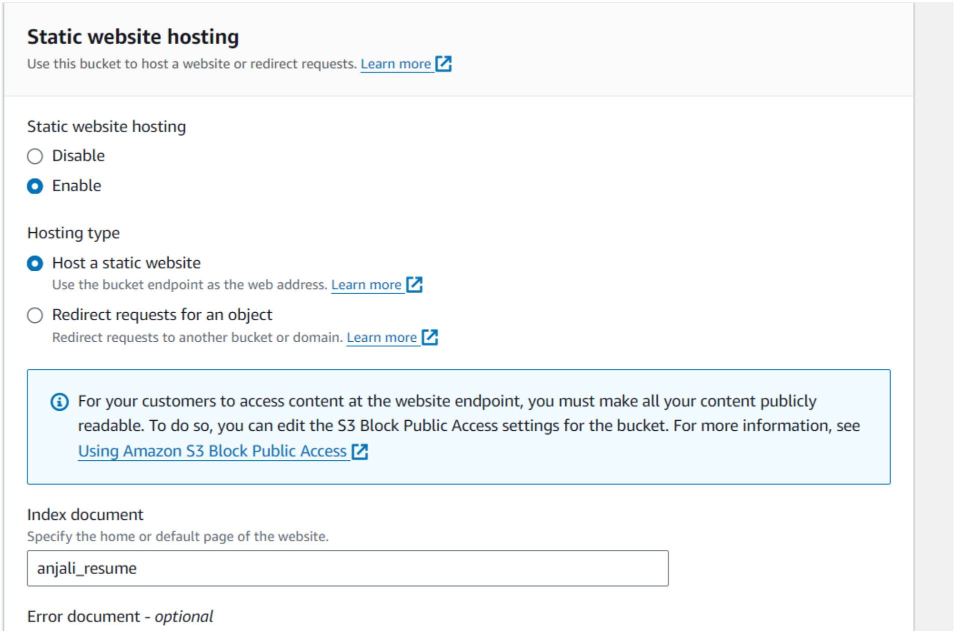
Use this bucket to host a website or redirect requests. Learn m

Static website hosting

● Disable

○ Enable

Step-11: Enable the radio button and specify the file name in **document** which you have added in S3



Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting

○ Disable

● Enable

Hosting type

● Host a static website

Use the bucket endpoint as the web address. Learn more

○ Redirect requests for an object

Redirect requests to another bucket or domain. Learn more

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access

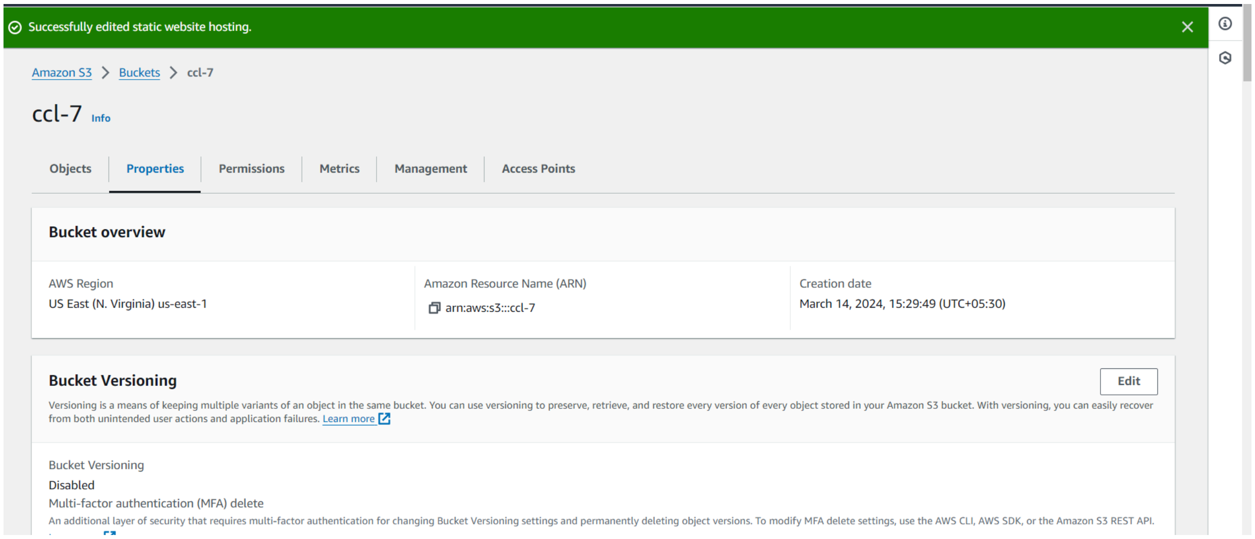
Index document

Specify the home or default page of the website.

anjali_resume

Error document - *optional*

Step 12:- Scroll down and save the changes at bottom right Following screen will appear



Successfully edited static website hosting.

Amazon S3 > Buckets > ccl-7

ccl-7 Info

Bucket overview

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

Amazon Resource Name (ARN)
arn:aws:s3:::ccl-7

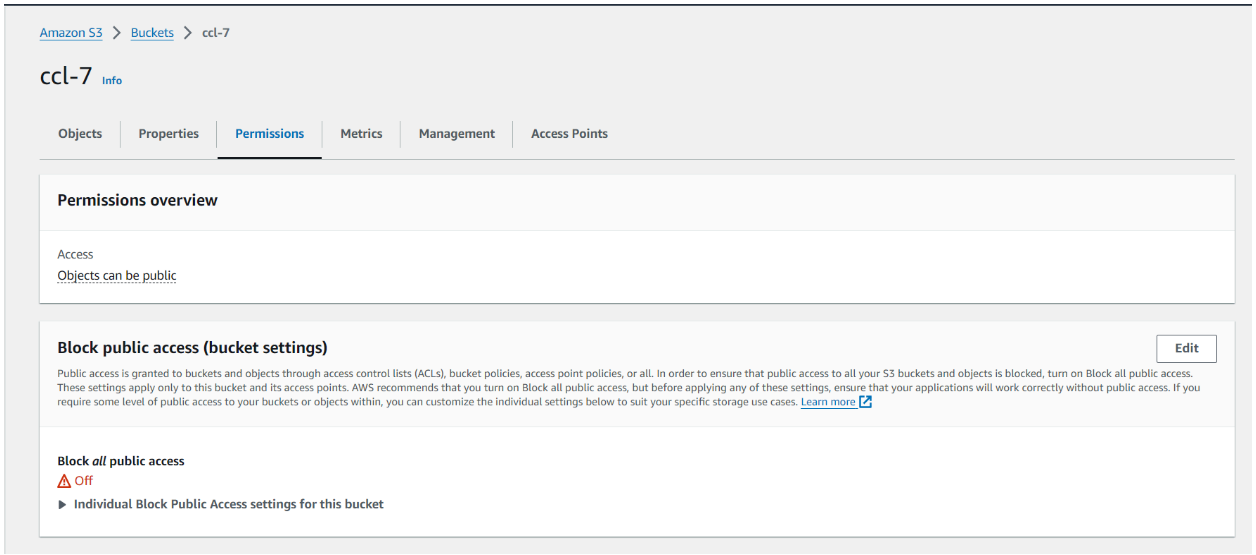
Creation date
March 14, 2024, 15:29:49 (UTC+05:30)

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
Disabled
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API.

Step-13: Click on Permissions Tab



Amazon S3 > Buckets > ccl-7

ccl-7 Info

Permissions overview

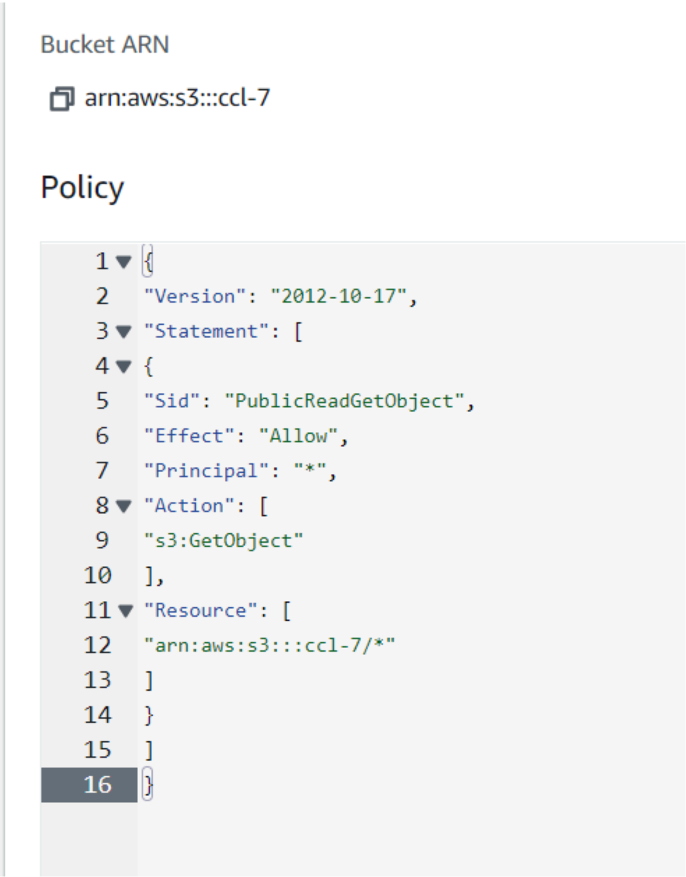
Access
Objects can be public

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
⚠ Off
▶ Individual Block Public Access settings for this bucket

Step-14:Step-14: In **bucket policy** click on Edit option and add this and change as per your bucket name



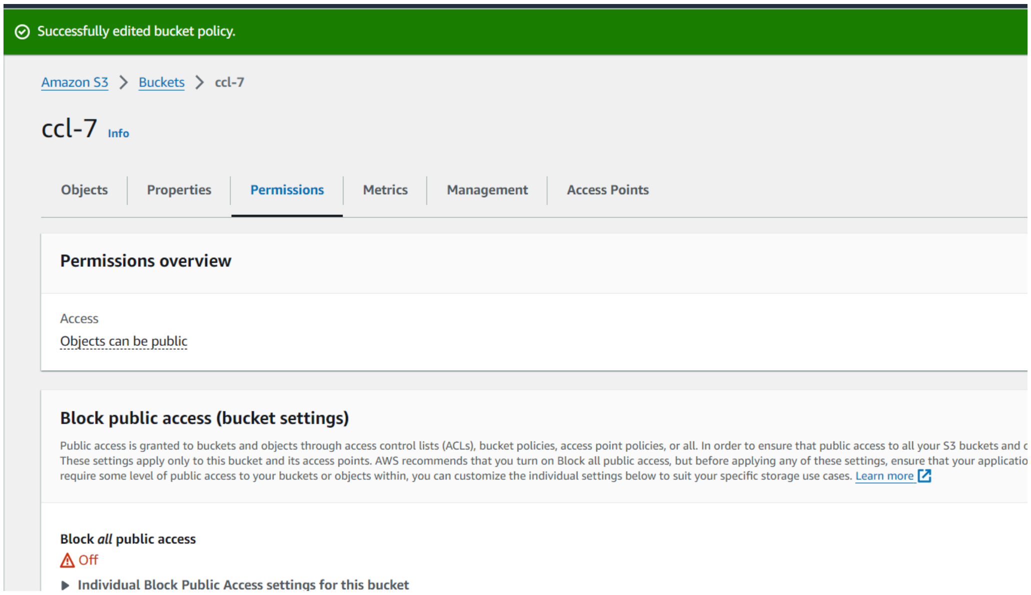
Bucket ARN

arn:aws:s3:::ccl-7

Policy

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "PublicReadGetObject",
"Effect": "Allow",
"Principal": "*",
"Action": [
"s3:GetObject"
],
"Resource": [
"arn:aws:s3:::ccl-7/*"
]
}
]
}
```

Step 15:- Scroll down and click on Save Changes button



Successfully edited bucket policy.

Amazon S3 > Buckets > ccl-7

ccl-7 Info

Permissions overview

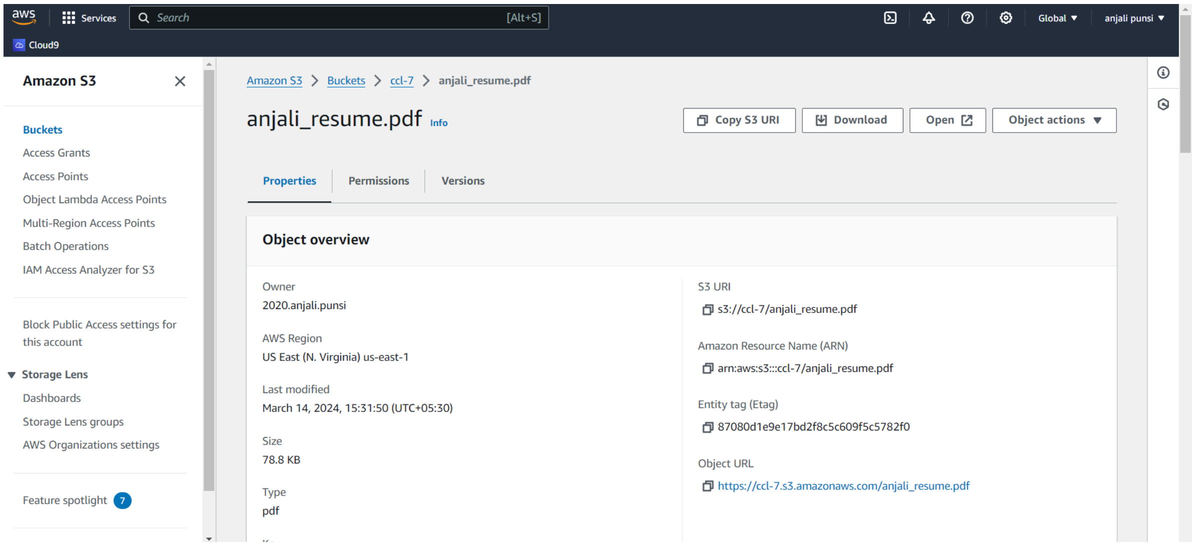
Access
Objects can be public

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 c
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 applicatio
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
⚠ Off
▸ Individual Block Public Access settings for this bucket

Step-16: after this this page will appear click on yourl file and click on Object URL



anjali_resume.pdf

Object overview

Owner
2020.anjali.punsi

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

Last modified
March 14, 2024, 15:31:50 (UTC+05:30)

Size
78.8 KB

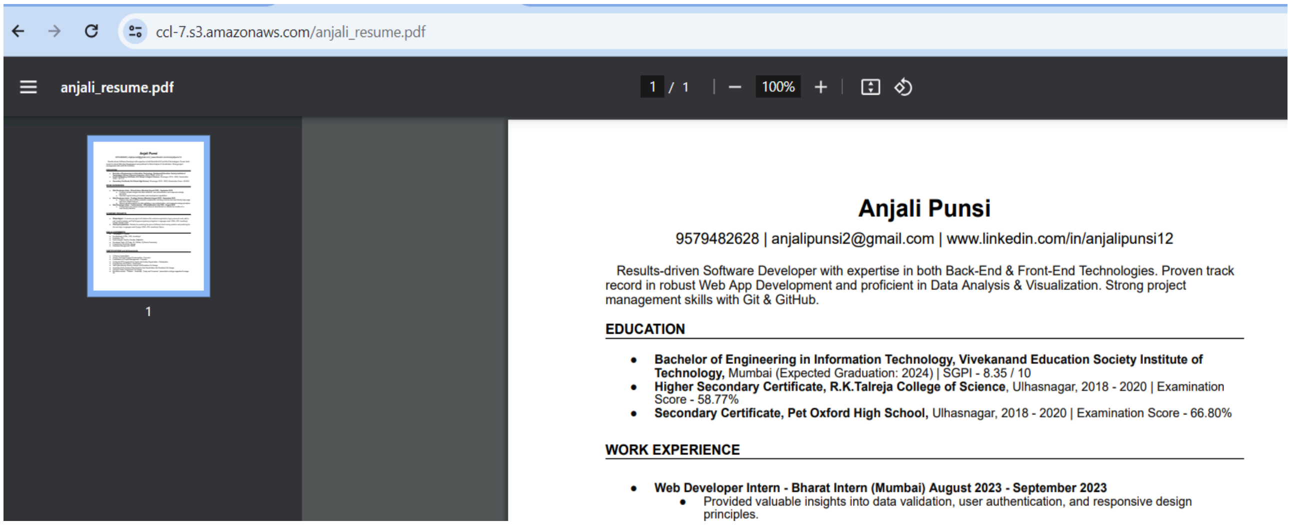
Type
pdf

S3 URI
s3://ccl-7/anjali_resume.pdf

Amazon Resource Name (ARN)
arn:aws:s3:::ccl-7/anjali_resume.pdf

Entity tag (Etag)
87080d1e9e17bd2f8c5c609f5c5782f0

Object URL
https://ccl-7.s3.amazonaws.com/anjali_resume.pdf



Anjali Punsi

9579482628 | anjalipunsi2@gmail.com | www.linkedin.com/in/anjalipunsi12

Results-driven Software Developer with expertise in both Back-End & Front-End Technologies. Proven track record in robust Web App Development and proficient in Data Analysis & Visualization. Strong project management skills with Git & GitHub.

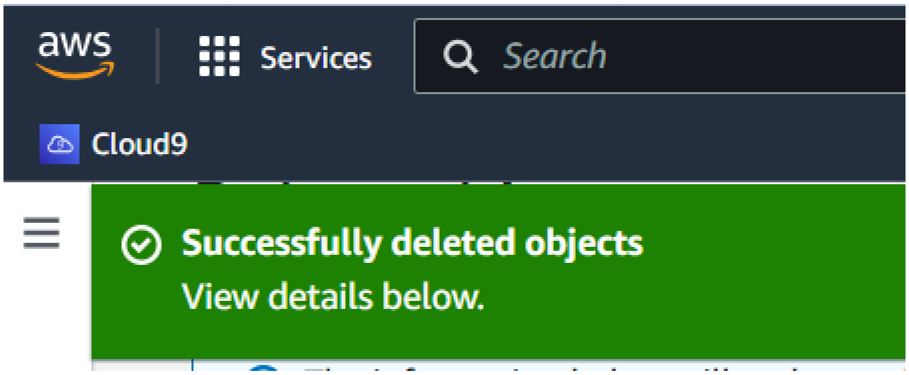
EDUCATION

- **Bachelor of Engineering in Information Technology, Vivekanand Education Society Institute of Technology,** Mumbai (Expected Graduation: 2024) | SGPI - 8.35 / 10
- **Higher Secondary Certificate, R.K.Talreja College of Science**, Ulhasnagar, 2018 - 2020 | Examination Score - 58.77%
- **Secondary Certificate, Pet Oxford High School,** Ulhasnagar, 2018 - 2020 | Examination Score - 66.80%

WORK EXPERIENCE

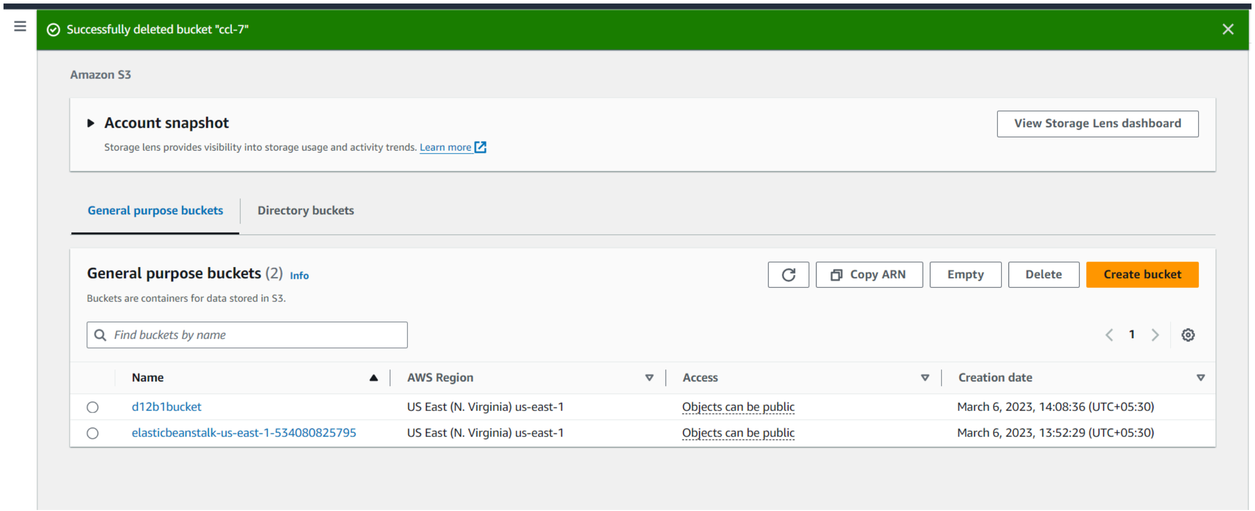
- **Web Developer Intern - Bharat Intern (Mumbai) August 2023 - September 2023**
  - Provided valuable insights into data validation, user authentication, and responsive design principles.

Step-17: Now for delete files click on checkbox of your file and then click on **Delete** Button
Write permanently delete and click on delete object button



Successfully deleted objects
View details below.

Step-18: now come to Amazon S3 tab and select your bucket and then click on delete button



Successfully deleted bucket "ccl-7"

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

General purpose buckets (2)

Buckets are containers for data stored in S3.

	Name	AWS Region	Access	Creation date
○	d12b1bucket	US East (N. Virginia) us-east-1	Objects can be public	March 6, 2023, 14:08:36 (UTC+05:30)
○	elasticbeanstalk-us-east-1-534080825795	US East (N. Virginia) us-east-1	Objects can be public	March 6, 2023, 13:52:29 (UTC+05:30)

Conclusion :-

Storage as a Service (STaaS) provides flexible, scalable storage solutions without the need for physical infrastructure. Implementing STaaS involves managing storage, ensuring data lifecycle management, implementing security measures, and optimizing costs. STaaS is a cost-effective, scalable option for businesses managing data storage needs.