SECURE CLOUD STORAGE AND BACKUP MANAGEMENT SYSTEM

Introduction :

Cloud computing provides scalable and secure data storage solutions for organizations. Data loss due to hardware failure or human error can cause serious business impact. This project implements a secure cloud storage and backup management system using Amazon Web Services (AWS). Amazon S3 is used for storing business files, and AWS Identity and Access Management (IAM) is used for controlling access. The system ensures that data is protected, backed up, and easily recoverable in case of failure.

Problem Statement :

An organization has lost important internal documents due to accidental deletion and disk failures. There is no centralized storage, no backup strategy, and no defined access control policy. As a result, data security and availability are compromised. The organization needs a secure cloud-based storage system that provides backup, controlled access, and quick recovery in case of failures.

Objectives :

The objectives of this project are:

- To store organizational data securely in cloud storage
- To implement backup using Amazon S3 versioning
- To restore files in case of accidental deletion
- To provide role-based access control using IAM

- To ensure data security using encryption
- To study storage performance and reliability

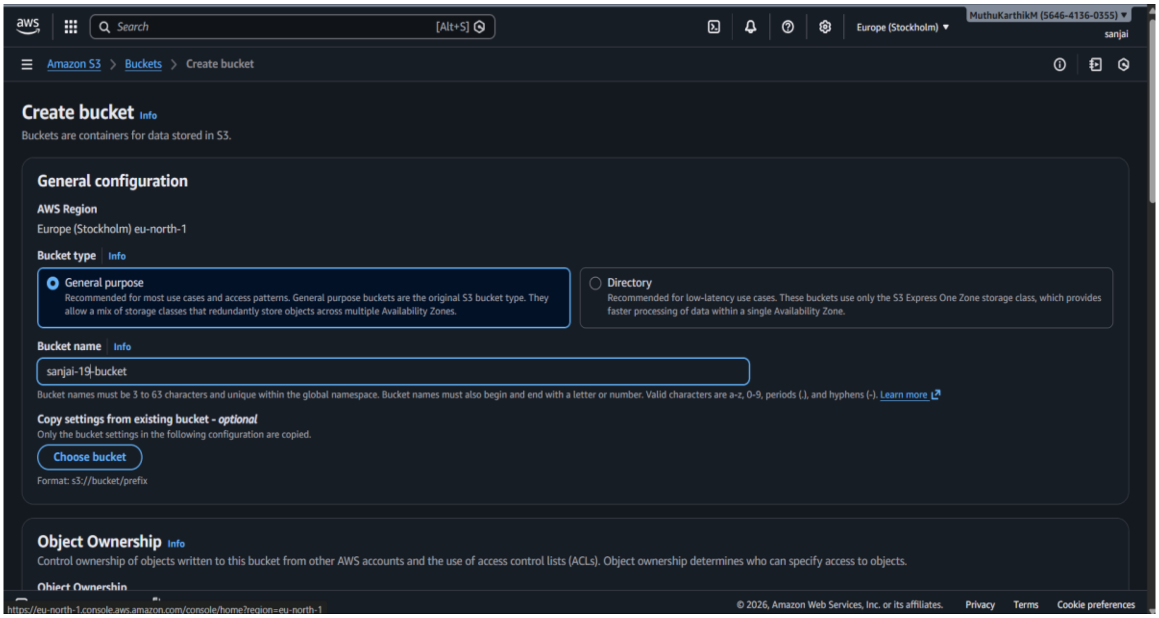
Architecture :

The system architecture uses Amazon S3 as the main storage service. Business files are uploaded into an S3 bucket created for the organization. IAM users and policies are created to manage access permissions. Versioning is enabled on the bucket to maintain multiple versions of files, which acts as a backup solution. Encryption is enabled to protect data at rest, and HTTPS is used to protect data during transfer.

Implementation Steps :

Step 1: Create S3 Bucket

An S3 bucket is created in AWS to store organizational files. The bucket acts as centralized cloud storage. A suitable name and region are selected while creating the bucket.



aws
Search [Alt+S]
Europe (Stockholm) ▾
MuthuKarthikM (5646-4136-0355) ▾
sanjai
Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

Europe (Stockholm) eu-north-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

sanjai-19-bucket

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn more

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

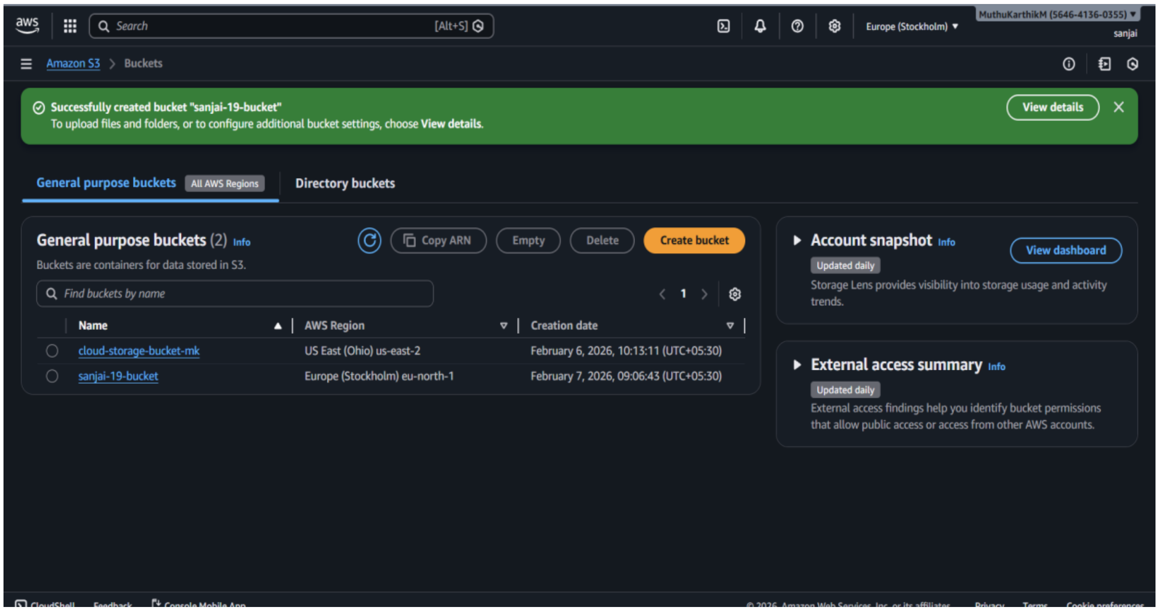
Format: s3://bucket/prefix

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.

Object Ownership

https://eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Successfully created bucket "sanjai-19-bucket"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

General purpose buckets (2)

Buckets are containers for data stored in S3.

	Name	AWS Region	Creation date
○	cloud-storage-bucket-mk	US East (Ohio) us-east-2	February 6, 2026, 10:13:11 (UTC+05:30)
○	sanjai-19-bucket	Europe (Stockholm) eu-north-1	February 7, 2026, 09:06:43 (UTC+05:30)

Account snapshot

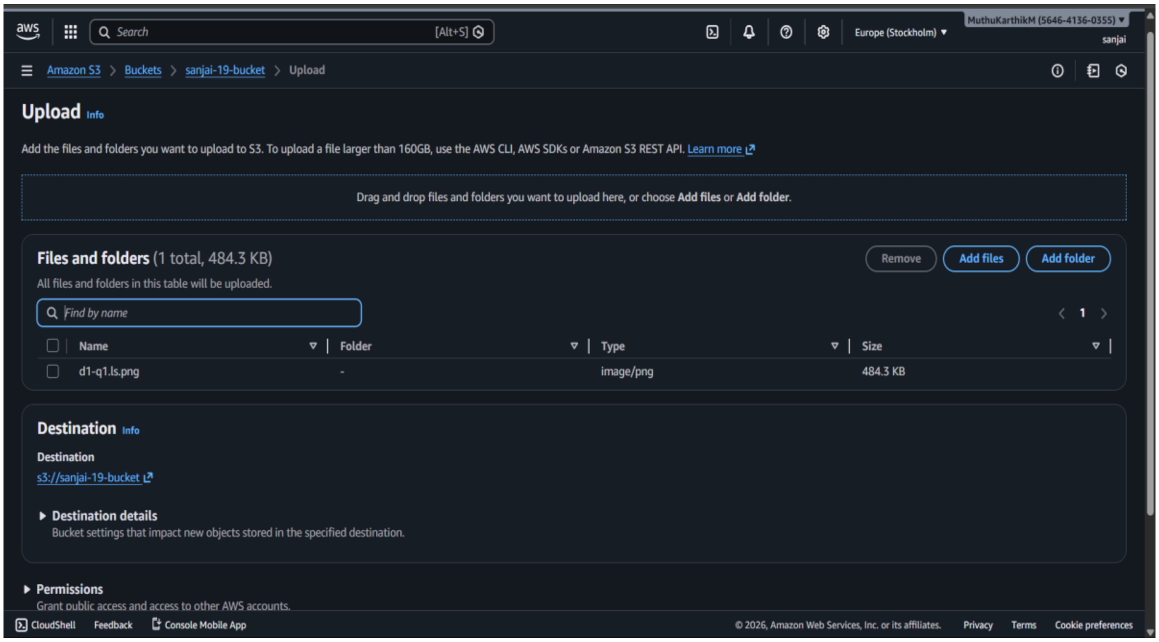
Storage Lens provides visibility into storage usage and activity trends.

External access summary

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Step 2: Upload Files

Business documents such as reports and text files are uploaded to the S3 bucket. These files represent organizational data.



Upload

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs 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, 484.3 KB)

All files and folders in this table will be uploaded.

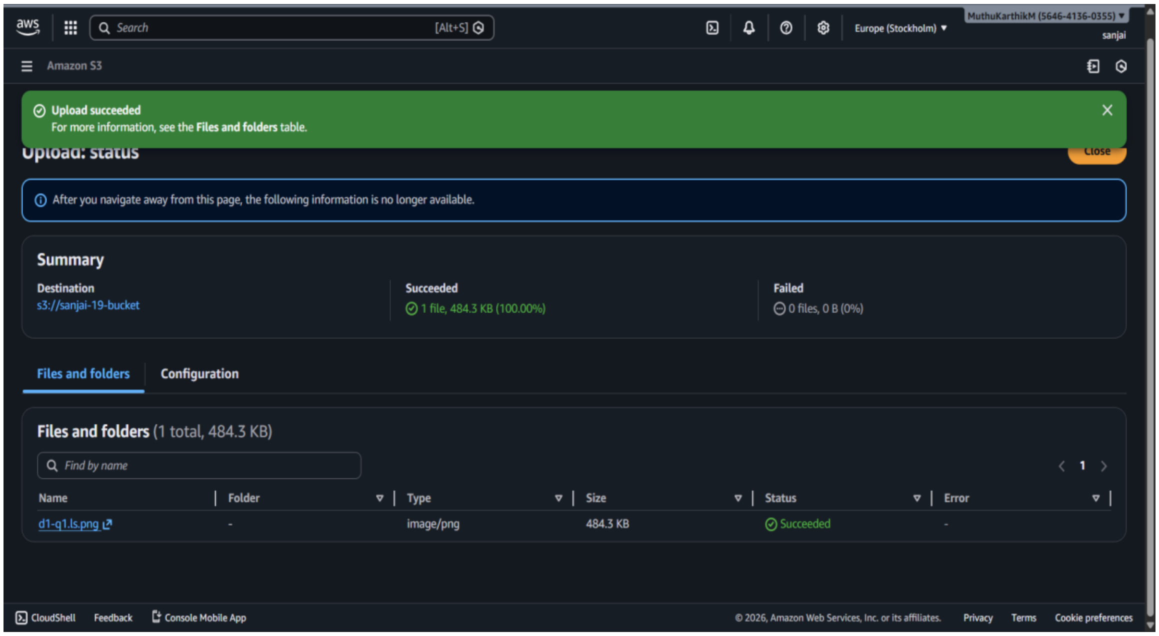
□	Name	Folder	Type	Size
□	d1-q1.ls.png	-	image/png	484.3 KB

Destination

Destination
s3://sanjai-19-bucket

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

▸ Permissions
Grant public access and access to other AWS accounts.



Upload succeeded
For more information, see the **Files and folders** table.

Upload: status

After you navigate away from this page, the following information is no longer available.

Summary

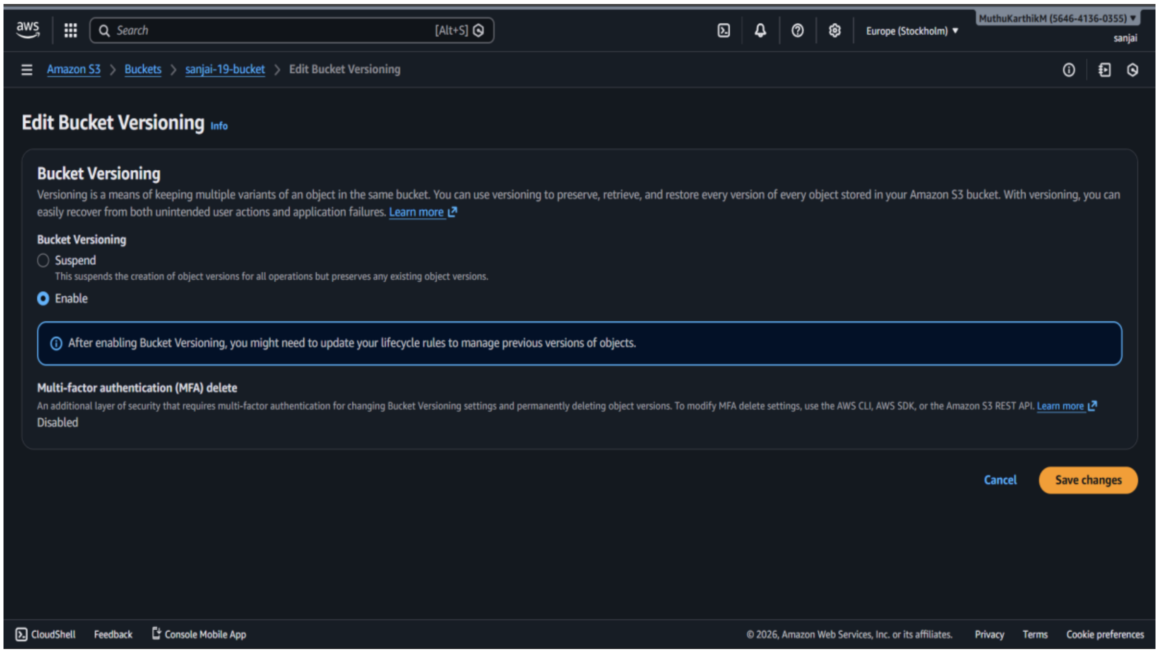
Destination	Succeeded	Failed
s3://sanjai-19-bucket	1 file, 484.3 KB (100.00%)	0 files, 0 B (0%)

Files and folders (1 total, 484.3 KB)

Name	Folder	Type	Size	Status	Error
d1-q1.ls.png	-	image/png	484.3 KB	Succeeded	-

Step 3: Enable Versioning

Versioning is enabled to maintain multiple versions of the same file. This helps recover files if they are deleted or overwritten.


aws
Search
[Alt+S]
Europe (Stockholm) ▾
MuthuKarthikM (5646-4136-0355) ▾
sanjai
Amazon S3 > Buckets > sanjai-19-bucket > Edit Bucket Versioning

Edit Bucket Versioning Info

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

○ Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.

● Enable

After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

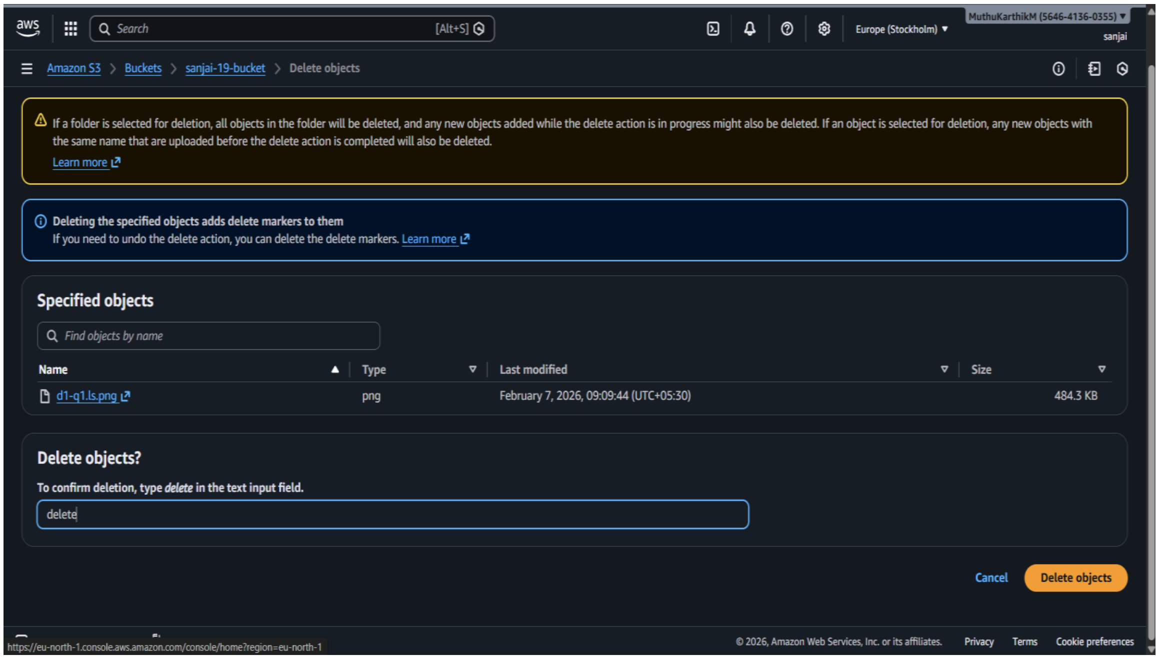
Multi-factor authentication (MFA) delete

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

Disabled

Step 4: Simulate Failure

A file is deleted from the bucket to simulate accidental deletion.


aws
Search
[Alt+S]
Europe (Stockholm) ▾
MuthuKarthikM (5646-4136-0355) ▾
sanjai
Amazon S3 > Buckets > sanjai-19-bucket > Delete objects
Cancel
Delete objects
https://eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

⚠ 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.
Learn more

ⓘ Deleting the specified objects adds delete markers to them
If you need to undo the delete action, you can delete the delete markers. Learn more

Specified objects

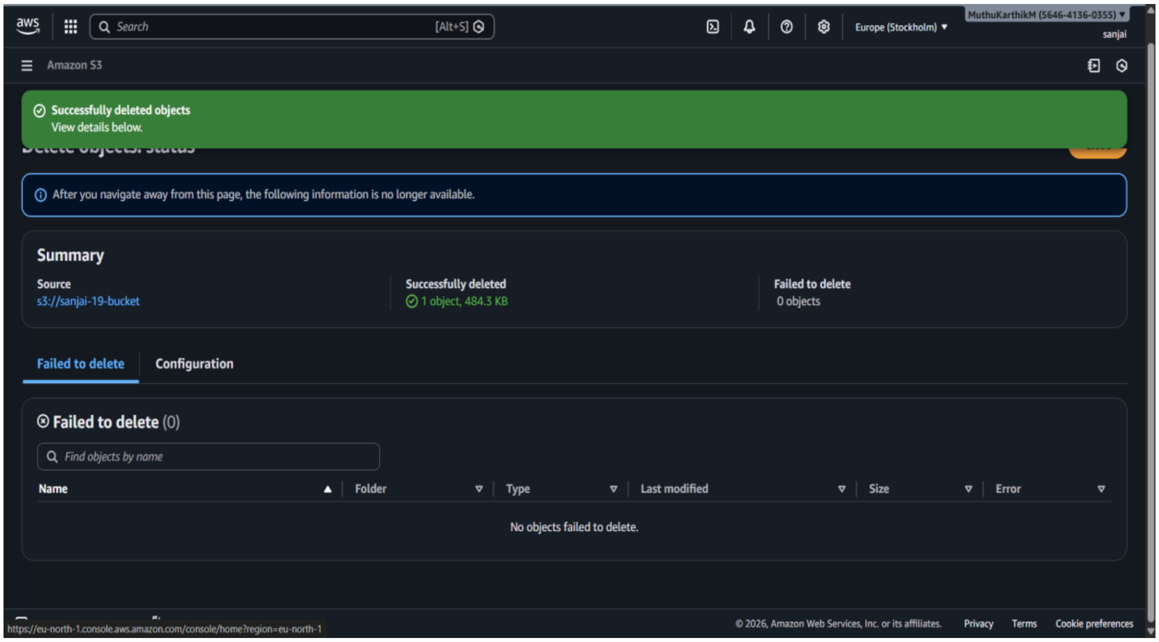
Find objects by name

Name	Type	Last modified	Size
d1-q1.ls.png	png	February 7, 2026, 09:09:44 (UTC+05:30)	484.3 KB

Delete objects?

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

delete


aws
Search
[Alt+S]
Europe (Stockholm) ▾
MuthuKarthikM (5646-4136-0355) ▾
sanjai
Amazon S3
Failed to delete
Configuration
https://eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

✓ Successfully deleted objects
View details below.

ⓘ After you navigate away from this page, the following information is no longer available.

Summary

Source	Successfully deleted	Failed to delete
s3://sanjai-19-bucket	✓ 1 object, 484.3 KB	0 objects

Failed to delete (0)

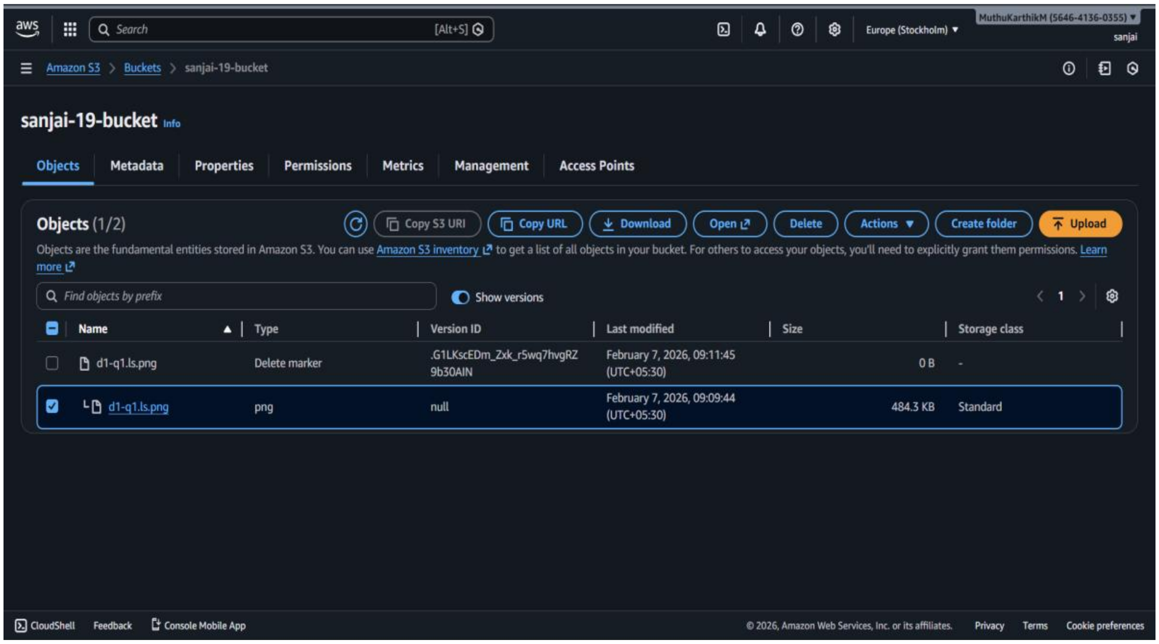
Find objects by name

Name	Folder	Type	Last modified	Size	Error

No objects failed to delete.

Step 5: Restore File

The deleted file is restored using the previous version maintained by S3.



sanjai-19-bucket Info

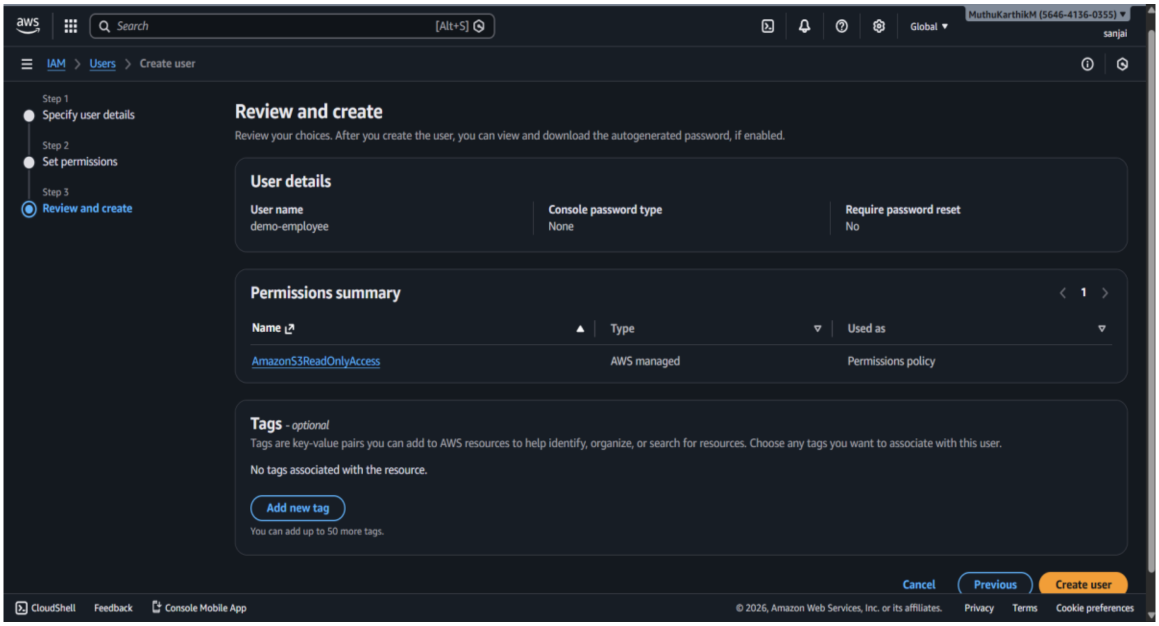
Objects (1/2)

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	Version ID	Last modified	Size	Storage class
□	d1-q1.ls.png	Delete marker	.G1LKscEDm_Zxk_r5wq7hvgRZ 9b30AIN	February 7, 2026, 09:11:45 (UTC+05:30)	0 B	-
☑	d1-q1.ls.png	png	null	February 7, 2026, 09:09:44 (UTC+05:30)	484.3 KB	Standard

Step 6: Configure IAM

An IAM user is created and assigned limited permissions such as read-only access to the bucket.



Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
demo-employee	None	No

Permissions summary

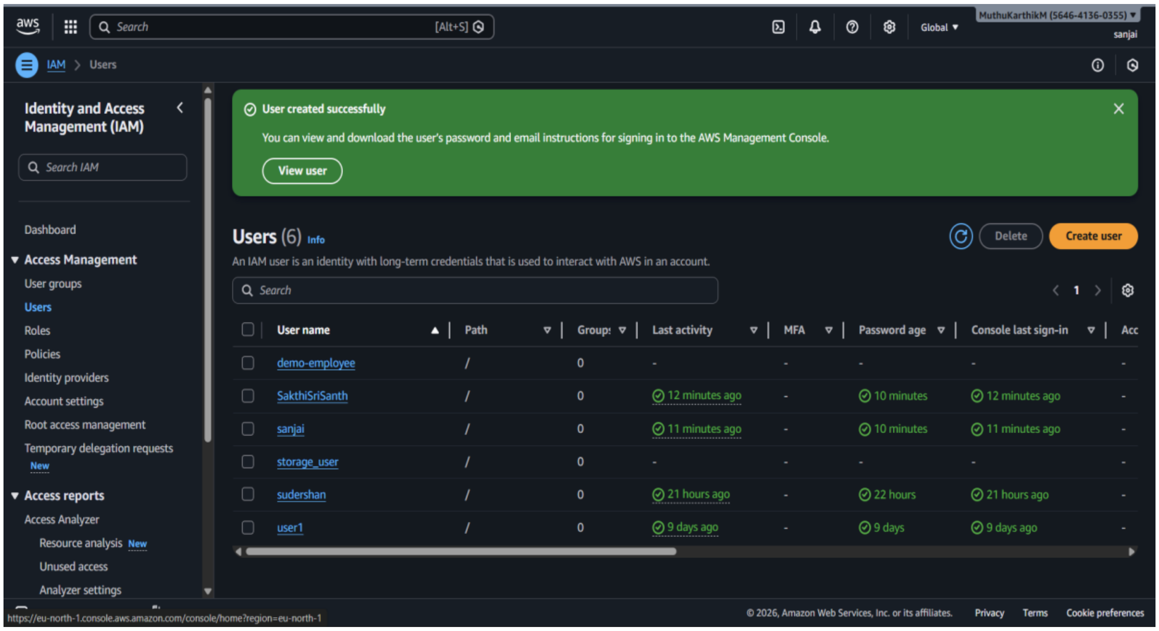
Name	Type	Used as
AmazonS3ReadOnlyAccess	AWS managed	Permissions policy

Tags - *optional*

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

You can add up to 50 more tags.



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Users (6) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Acc
□	demo-employee	/	0	-	-	-	-	-
□	SakthiSriSanth	/	0	✓ 12 minutes ago	-	✓ 10 minutes	✓ 12 minutes ago	-
□	sanjai	/	0	✓ 11 minutes ago	-	✓ 10 minutes	✓ 11 minutes ago	-
□	storage_user	/	0	-	-	-	-	-
□	sudershan	/	0	✓ 21 hours ago	-	✓ 22 hours	✓ 21 hours ago	-
□	user1	/	0	✓ 9 days ago	-	✓ 9 days	✓ 9 days ago	-

https://eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1

© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Security Features :

Amazon S3 provides server-side encryption to protect data stored in the bucket. Data in transit is protected using HTTPS. IAM policies ensure that only authorized users can access the data. These measures provide confidentiality, integrity, and availability of data.

Recovery Process :

When data is deleted or corrupted, the administrator uses S3 versioning to restore the previous version of the file. This ensures that important data is not permanently lost and business operations can continue without interruption.

Performance Considerations :

Amazon S3 provides high durability and availability. It supports high throughput for file transfers and is suitable for storing large volumes of data. Performance depends on network bandwidth and object size.

Conclusion :

This project demonstrates a secure and reliable cloud storage and backup management system using AWS. By using S3 for storage and IAM for access control, the system ensures data security, availability, and recovery from failures. This solution is suitable for protecting organizational data in a cloud environment.

- SANJAI J
  727723EUCY047
  BE CSE (CYBER) III