Secure Cloud Storage & Backup Management System

Introduction

This project demonstrates a secure cloud-based storage and backup solution. It ensures data availability, controlled access, and recovery from failures using cloud storage services.

Problem Statement

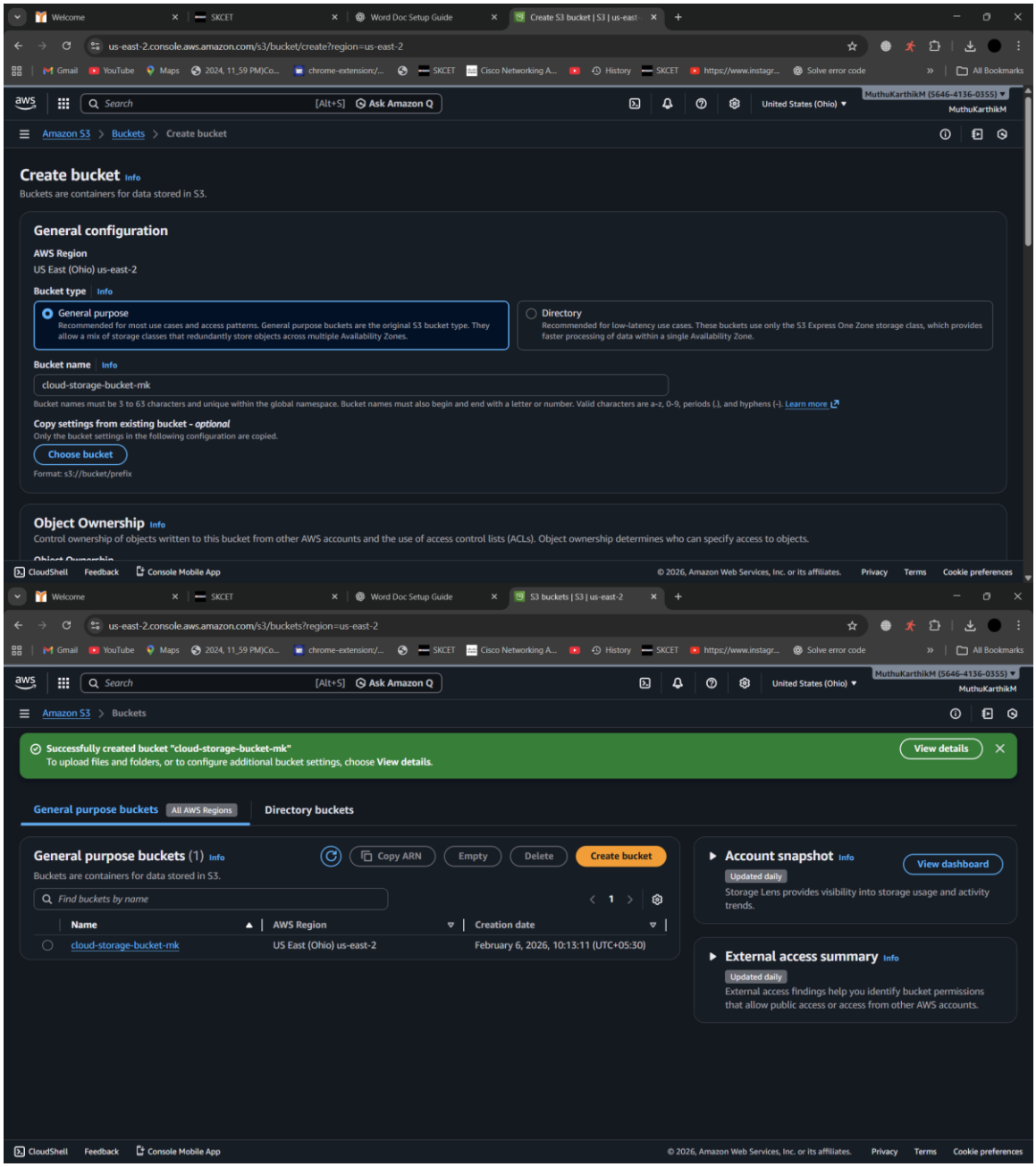
An organization has lost critical internal documents due to accidental deletion and disk failures. There is no backup policy, no retention strategy, and no centralized access control. Management demands a secure cloud-based storage and backup solution that ensures data availability and controlled access.

Objectives

- Store business files in cloud storage
- Take periodic backups
- Restore snapshots in case of failure
- Restrict access based on roles (admin/user)
- Understand storage performance (IOPS, throughput)

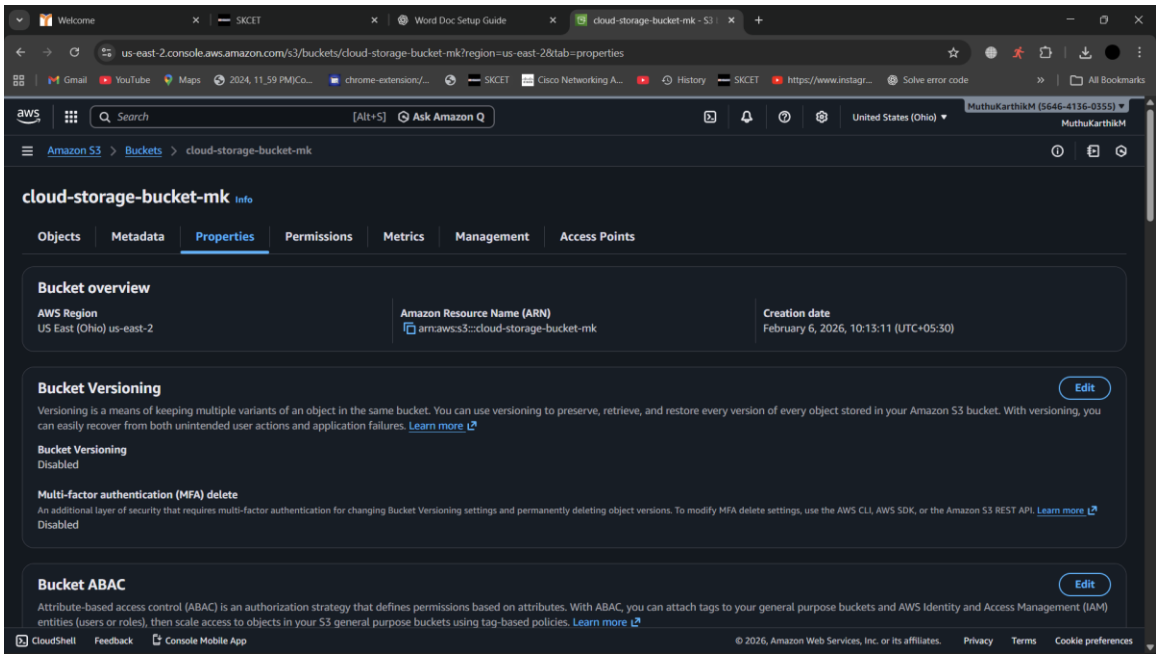
Architecture

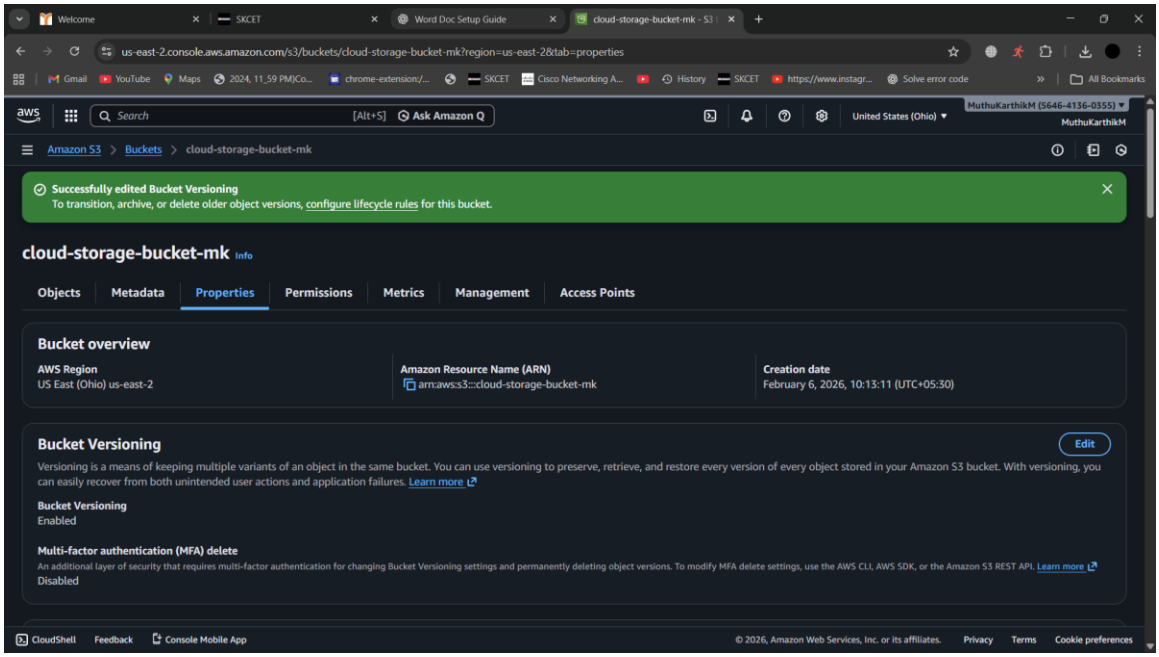
The system uses cloud object or block storage. Files are uploaded to cloud storage, snapshots are taken periodically, and access is controlled using IAM roles.



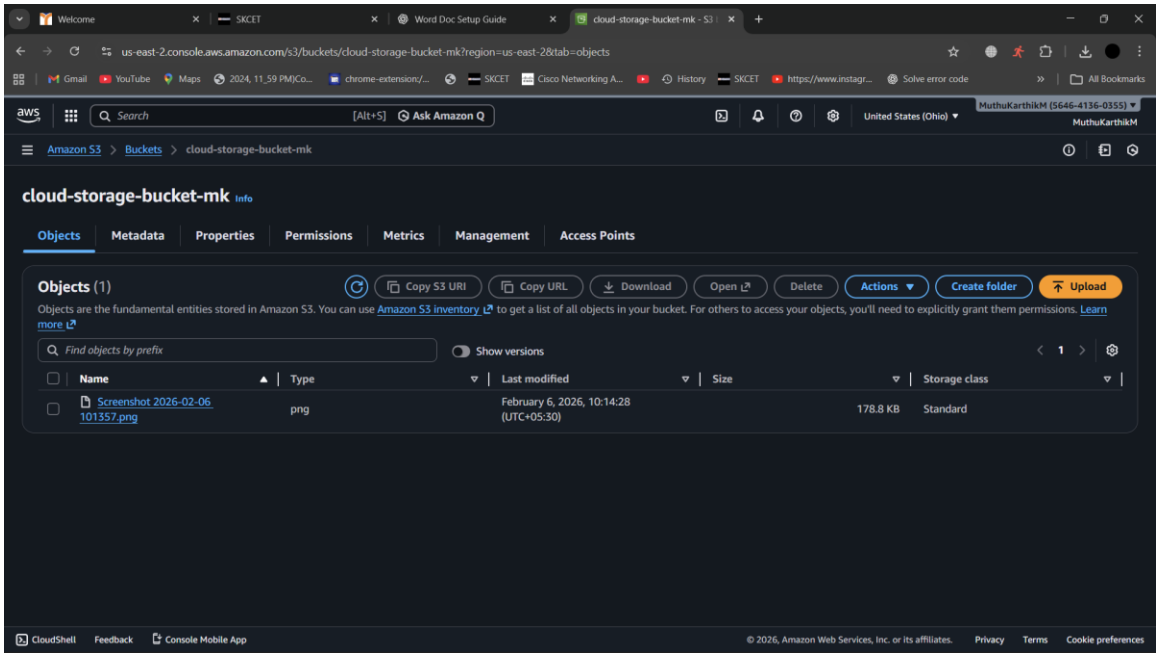
Implementation Steps

Step 1: Enable Backup/Snapshot Feature

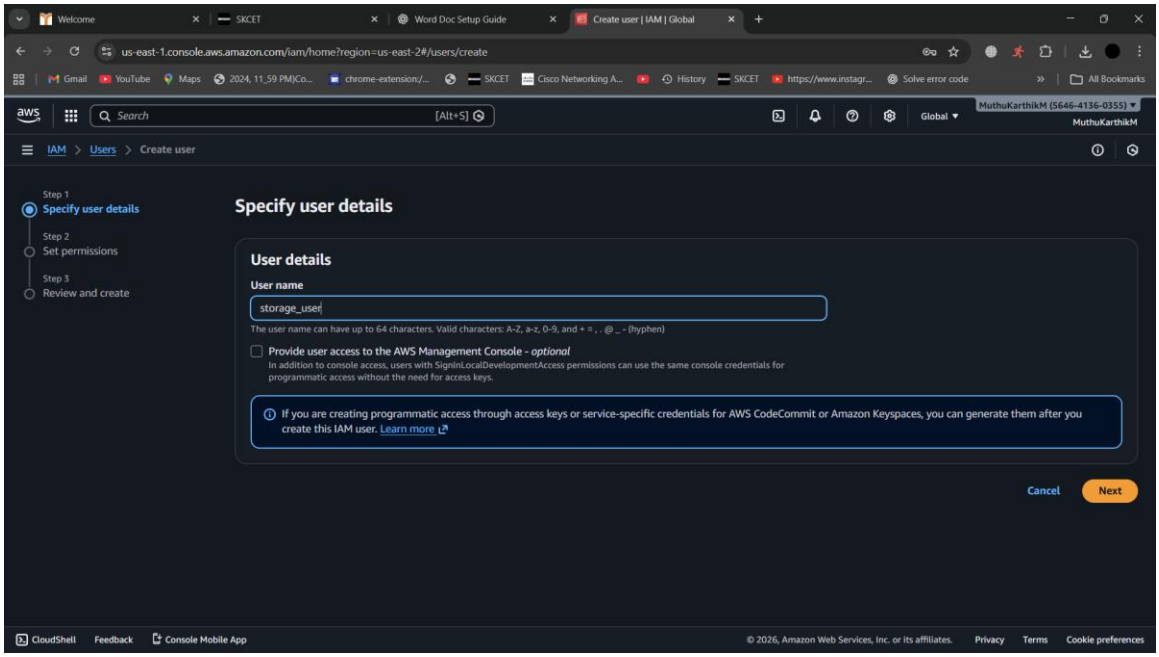


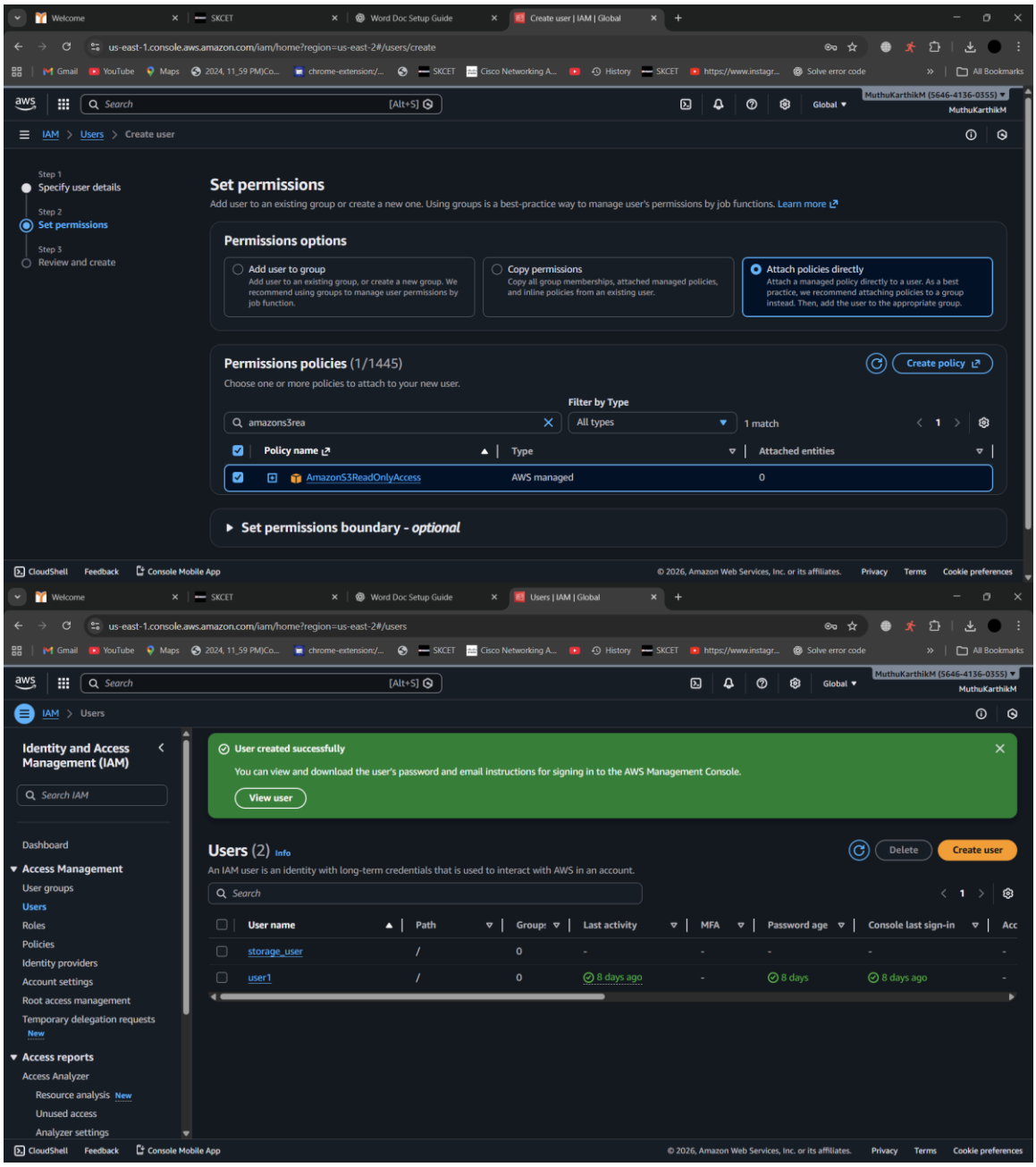


Step 2: Upload Files

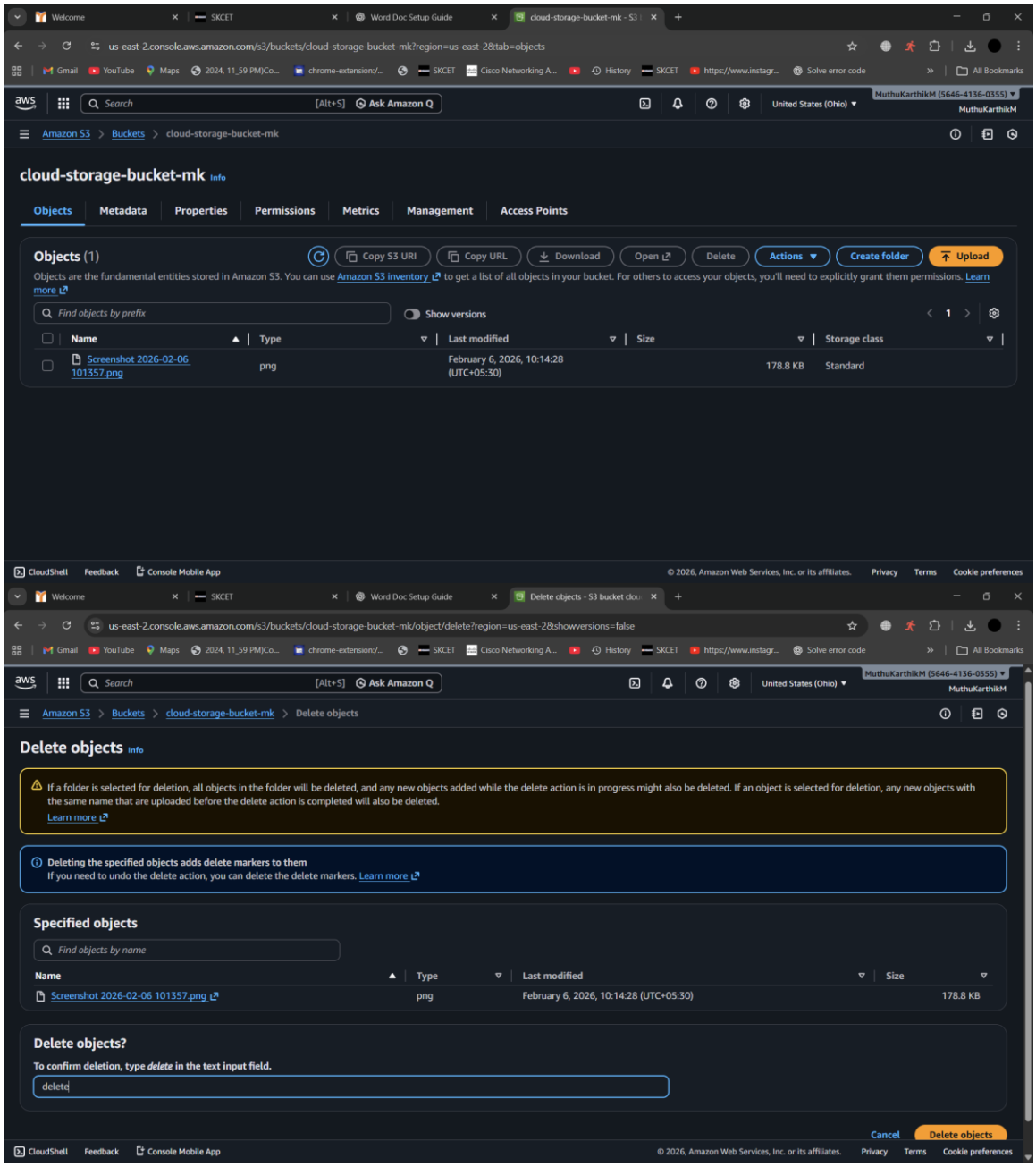


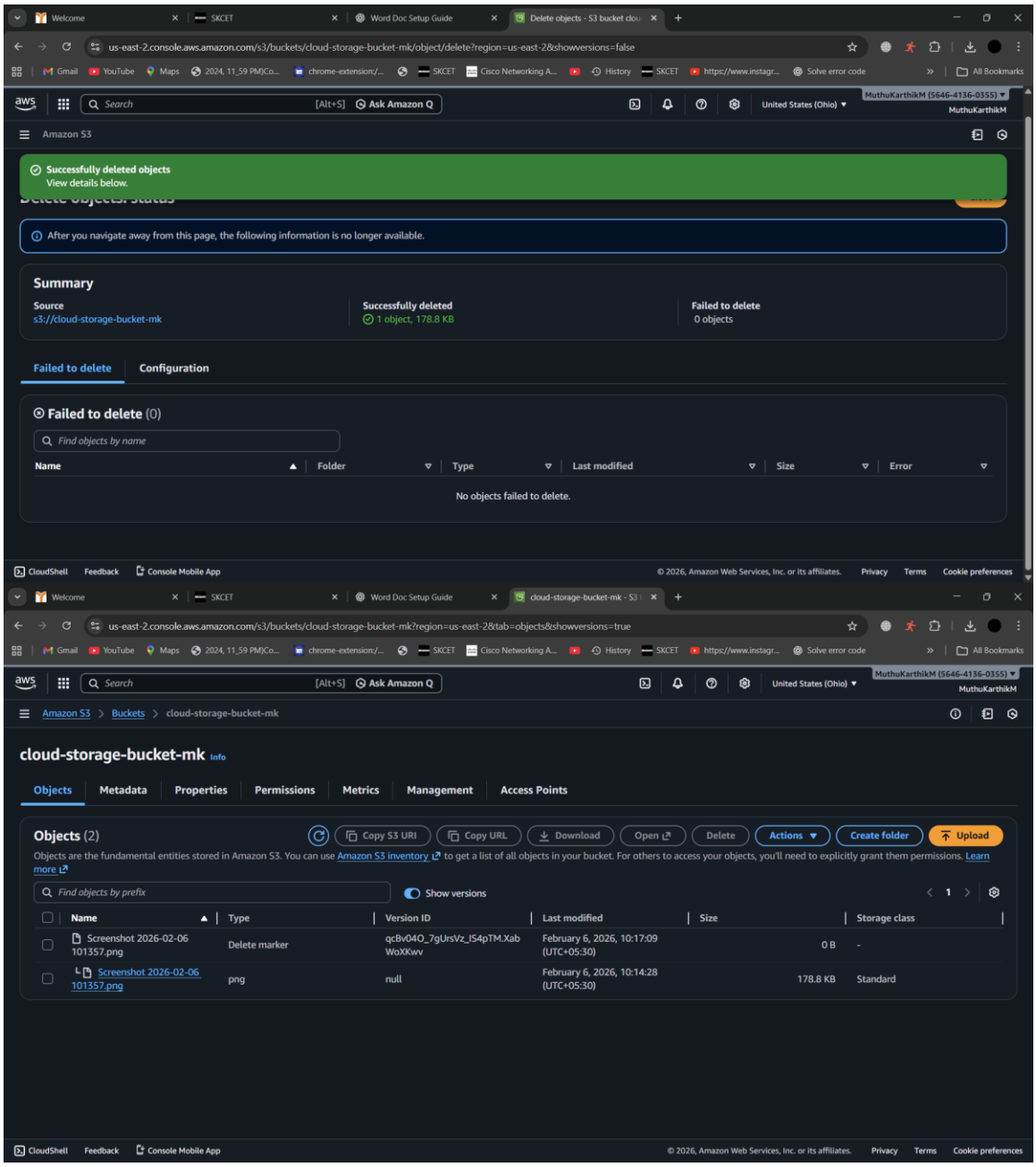
Step 3: Configure Access Control (Admin/User)



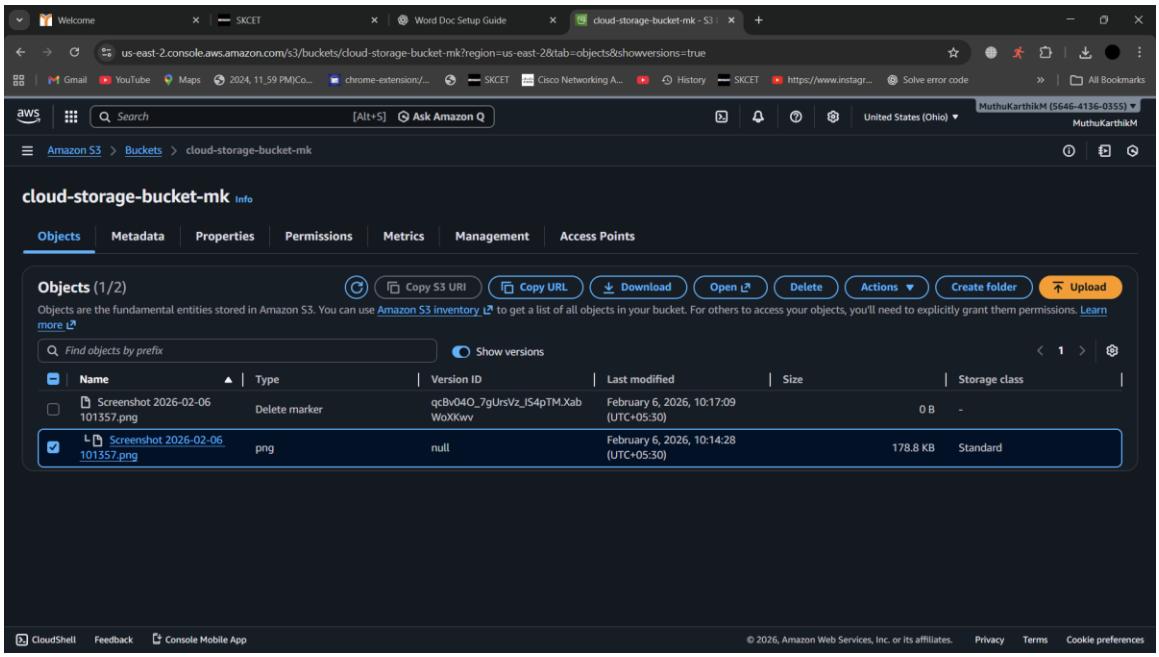

Welcome
SKCET
Word Doc Setup Guide
Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/users/create
Search
[Alt+S]
Global
MuthuKarthikM (5646-4136-0355)
MuthuKarthikM
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Permissions policies (1/1445)
Choose one or more policies to attach to your new user.
Create policy
Filter by Type
amazons3rea
All types
1 match
Policy name
Type
Attached entities
AmazonS3ReadOnlyAccess
AWS managed
0
Set permissions boundary - optional
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Users | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/users
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Users (2) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Groups
Last activity
MFA
Password age
Console last sign-in
storage_user
/
0
-
-
-
-
user1
/
0
8 days ago
-
8 days
8 days ago

Step 4: Simulate Failure and Restore Data




Successfully deleted objects
View details below.
After you navigate away from this page, the following information is no longer available.
Summary
Source
s3://cloud-storage-bucket-mk
Successfully deleted
1 object, 178.8 KB
Failed to delete
0 objects
Failed to delete
Configuration
Failed to delete (0)
Find objects by name
Name
Folder
Type
Last modified
Size
Error
No objects failed to delete.
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Amazon S3 > Buckets > cloud-storage-bucket-mk
cloud-storage-bucket-mk Info
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Objects (2)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
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
Show versions
Name
Type
Version ID
Last modified
Size
Storage class
Screenshot 2026-02-06 101357.png
Delete marker
qcBv04O_7gUrsVz_IS4pTM.XabWoXKwv
February 6, 2026, 10:17:09 (UTC+05:30)
0 B
-
Screenshot 2026-02-06 101357.png
png
null
February 6, 2026, 10:14:28 (UTC+05:30)
178.8 KB
Standard
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Security Features

- Encryption at rest
- Encryption in transit
- Role-based access control
- Backup retention policy

Recovery Process

In case of accidental deletion or disk failure, the admin restores data using snapshots or backups.

Conclusion

This project ensures reliable and secure cloud storage with proper backup and recovery mechanisms.