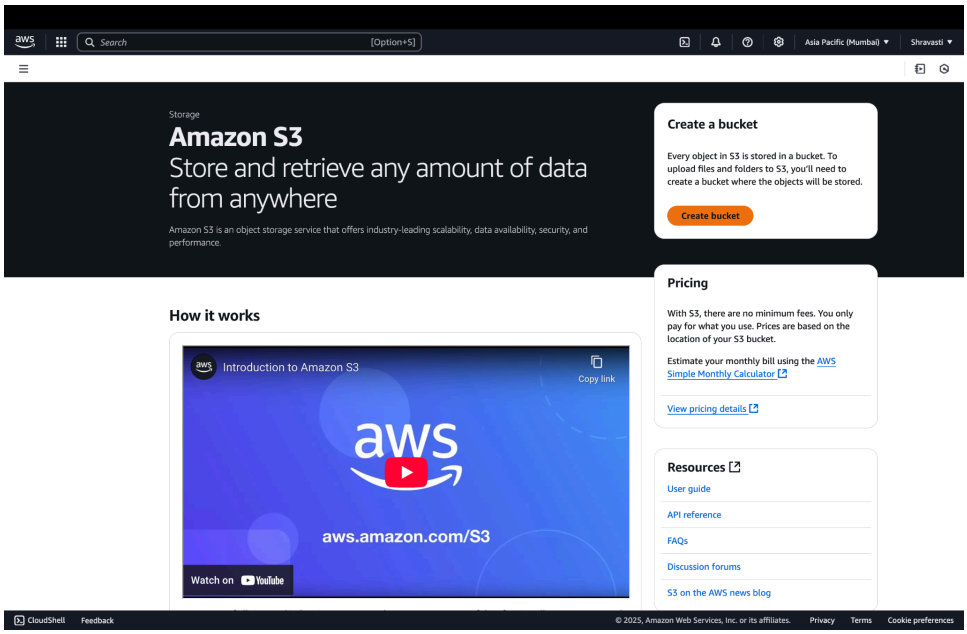
CBE 321 Cloud Computing & Security

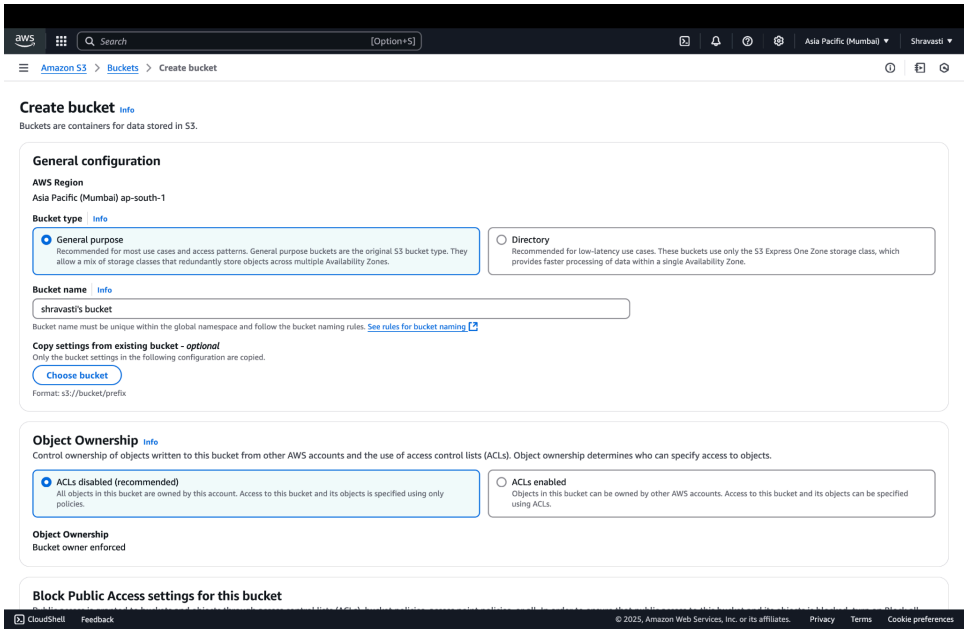
SHRAVASTI OHOL 2022BCY0012

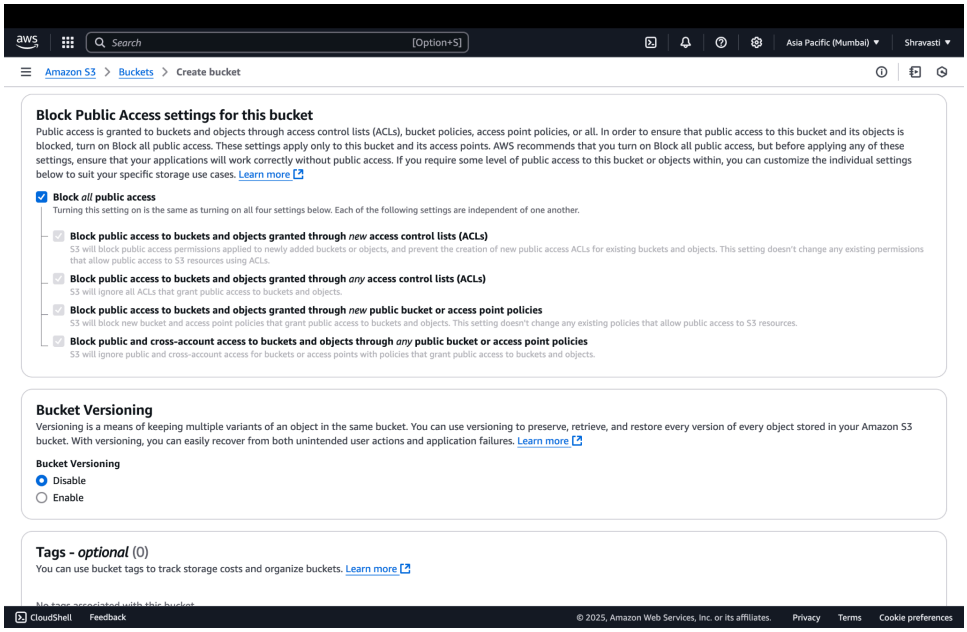
AWS - Simple Storage Service (S3)

1. Navigate to S3 service. Click on Create Bucket.

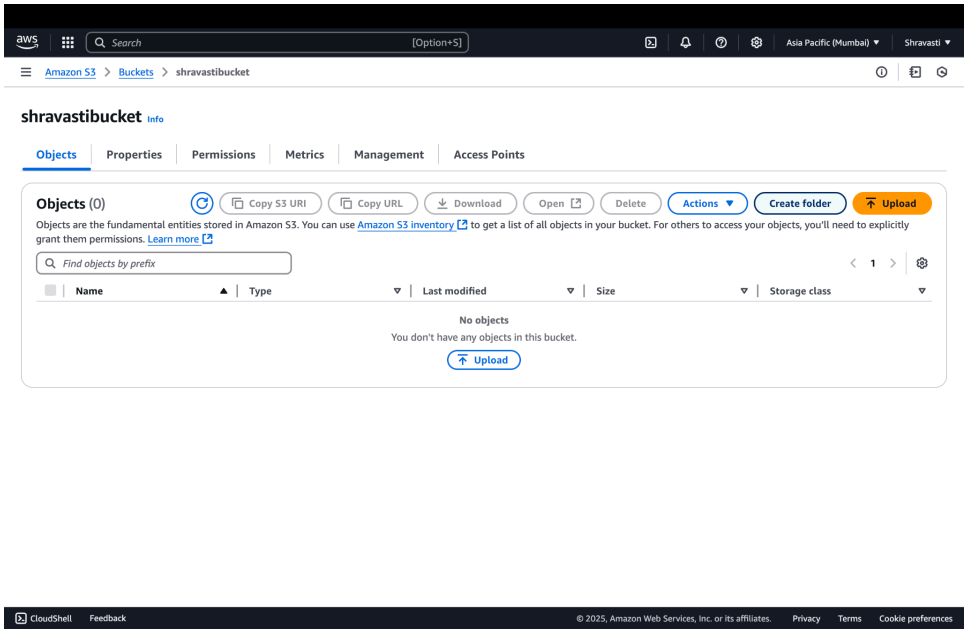


2. Configure settings accordingly

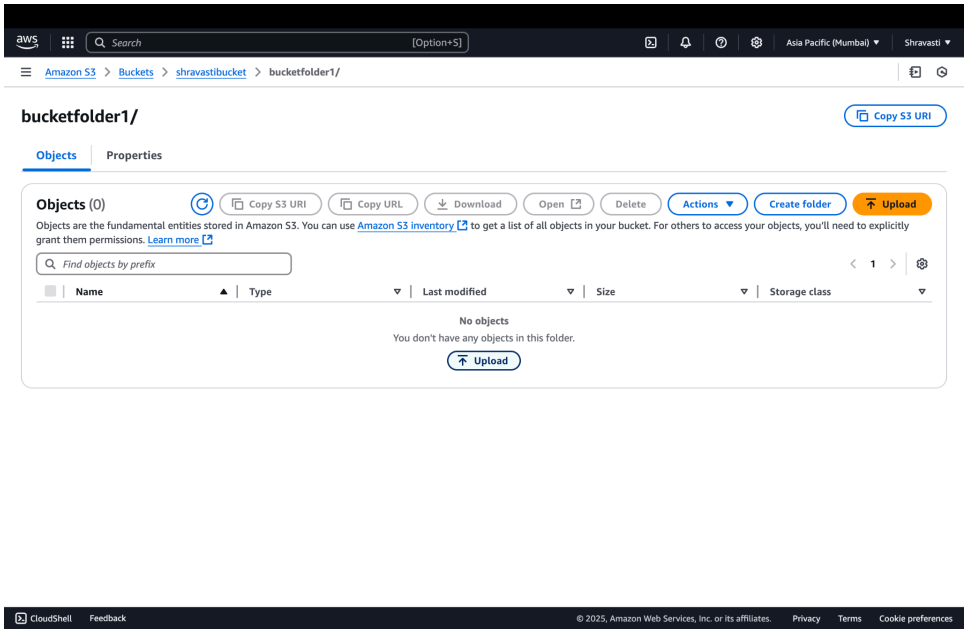


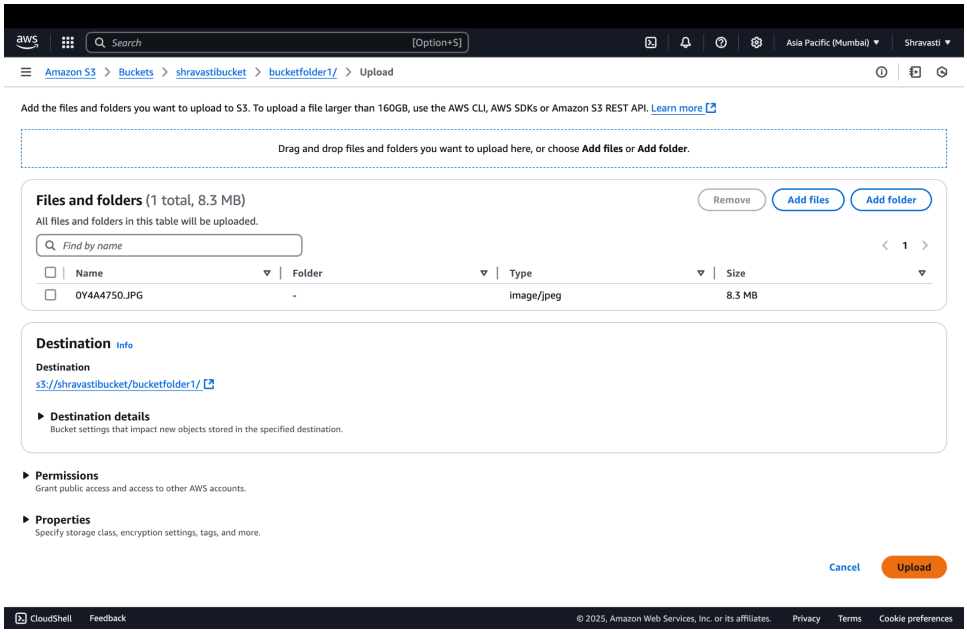


3. After the bucket is successfully created, create an object inside the bucket i.e. a folder

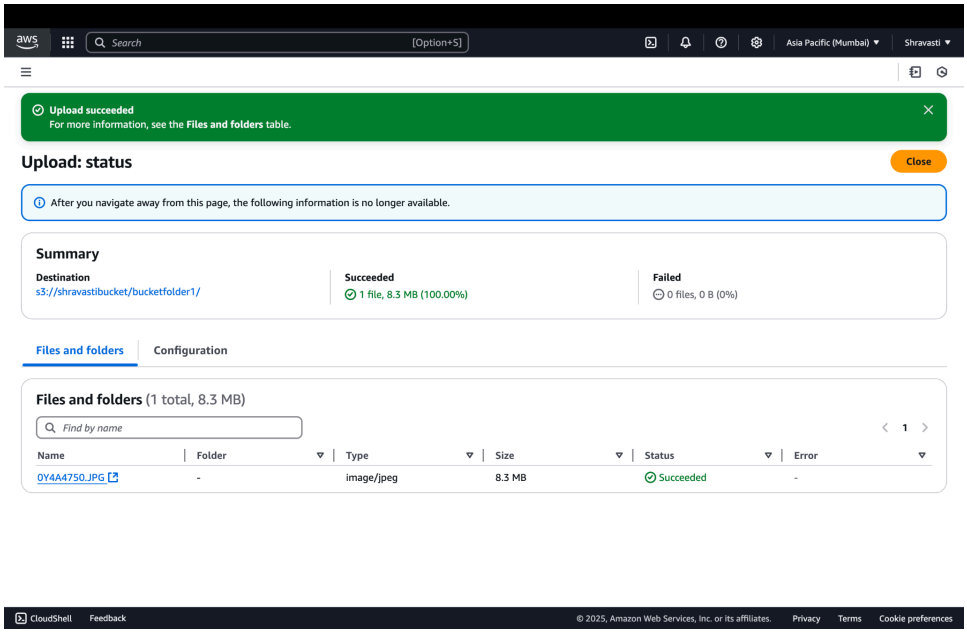


4. After creating a folder, upload a file in it.

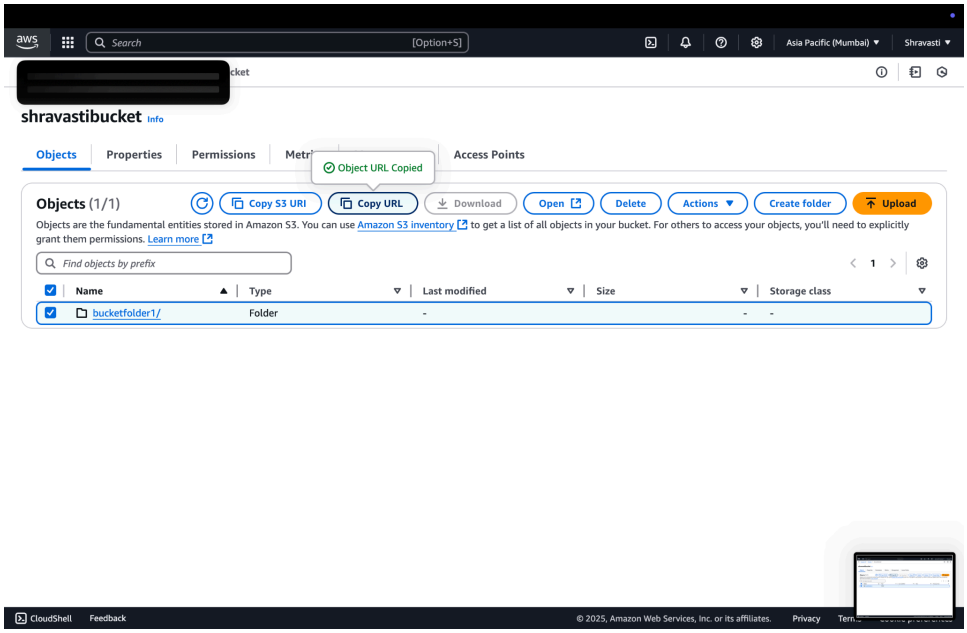




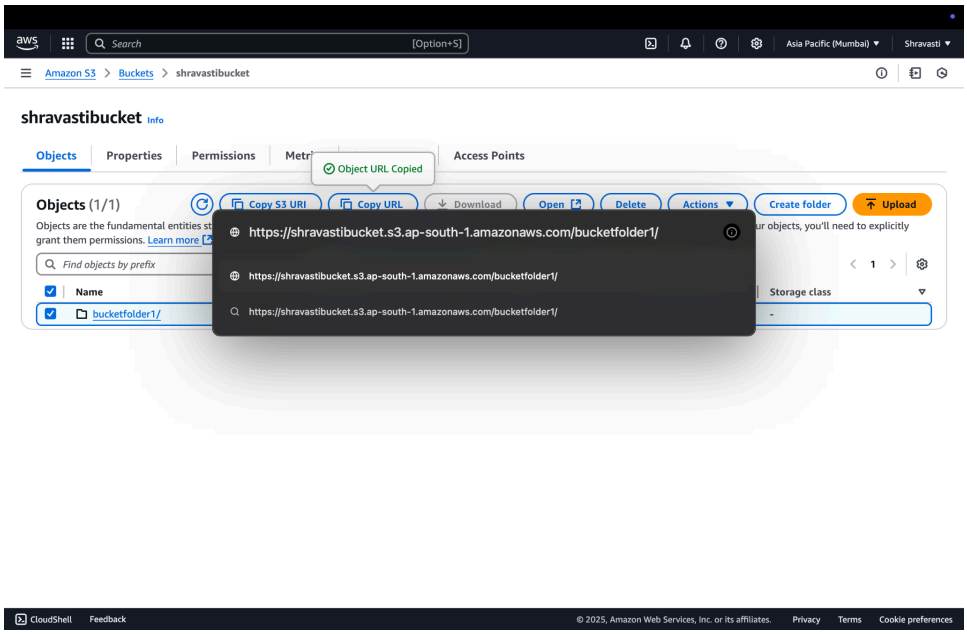
5. Once the upload is successful, you will get a notification.



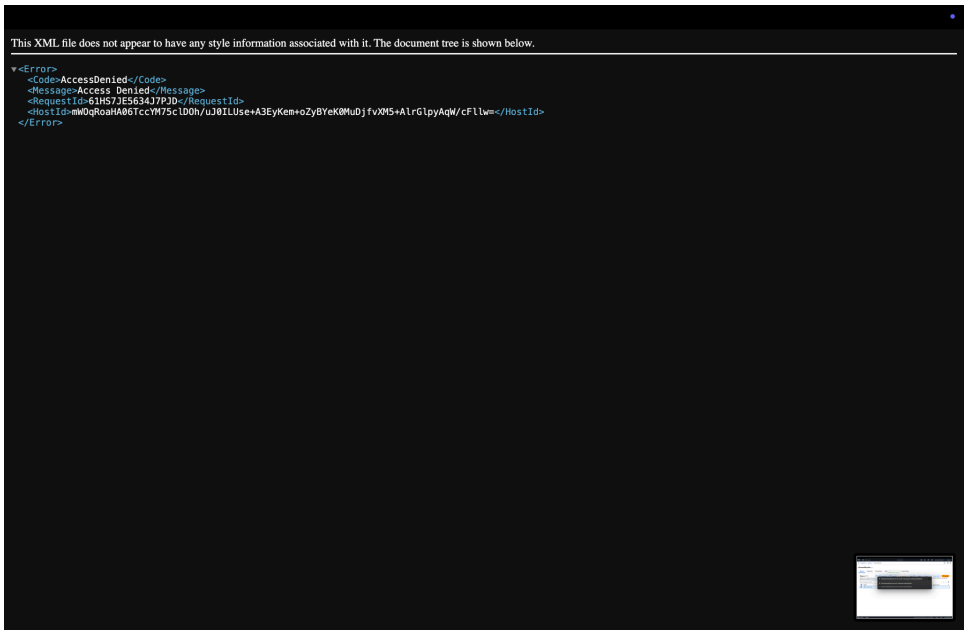
6. Select the bucket created and copy its URL



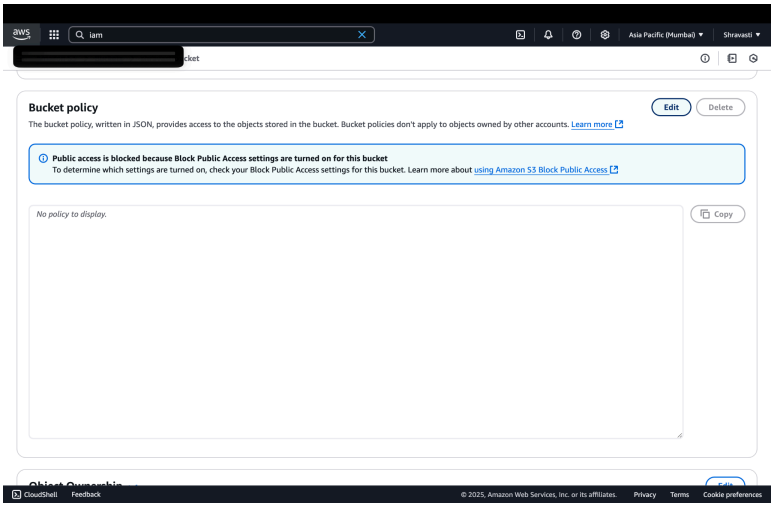
7. Paste it in a new tab



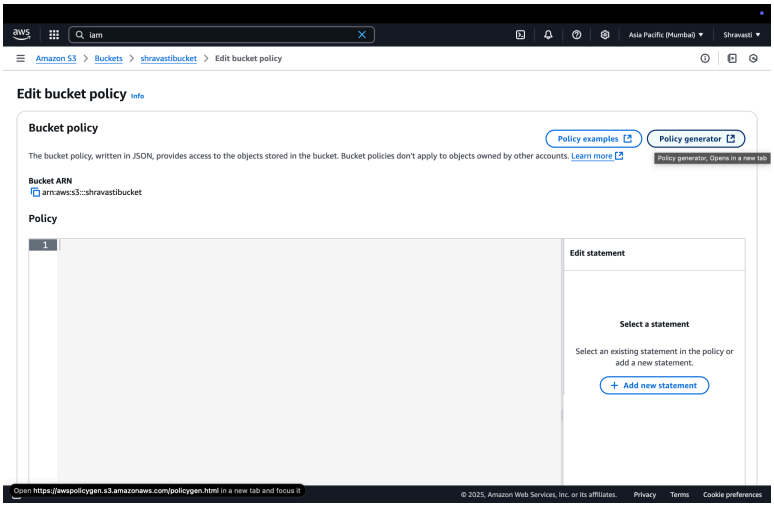
8. Access to the resource will be denied. This is because public access to the bucket and its contents was restricted while creating the bucket.



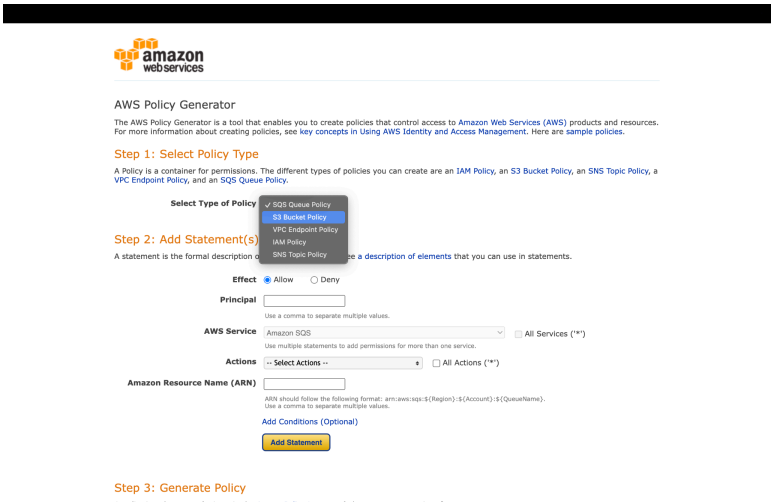
9. Two ways to do this
    a. Changing bucket policies
        i. Under the bucket, go to the Permissions tab



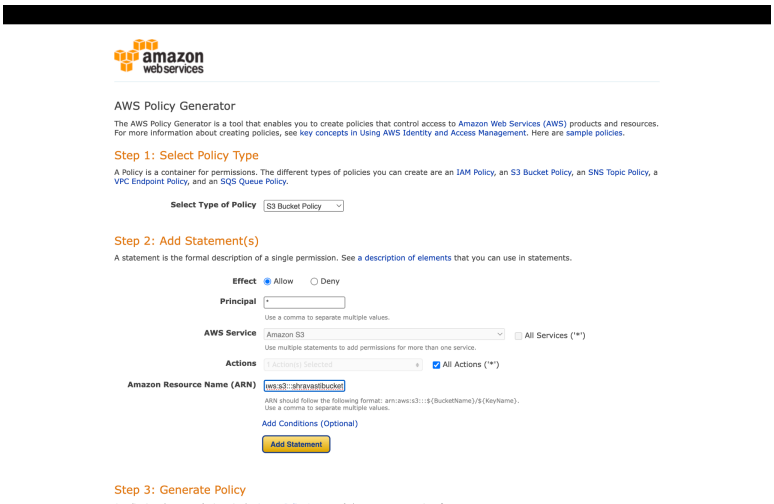
        ii. Click on Policy generator



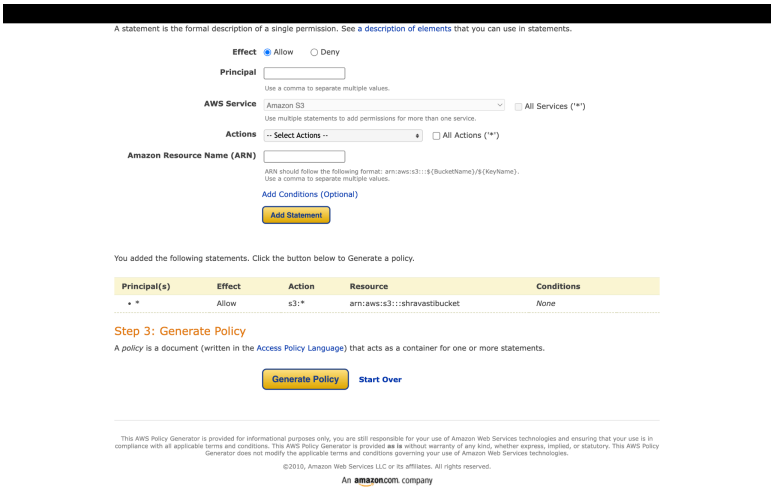
        iii. Select policy type as ‘S3 Bucket Policy’



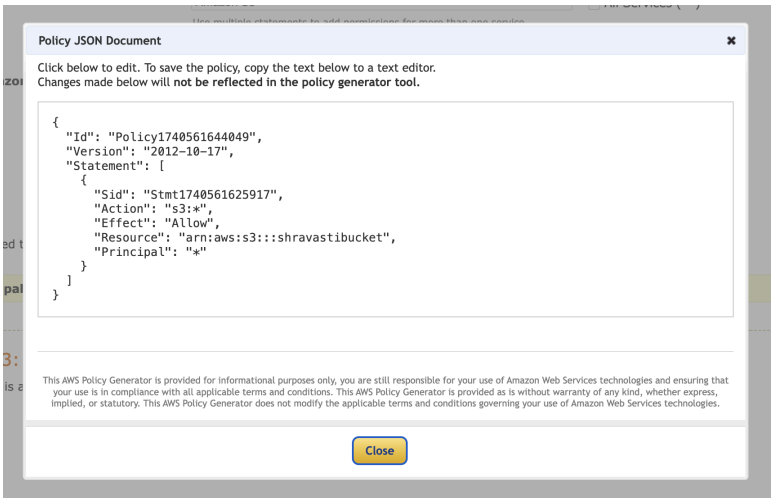
iv. Paste the ARN for the bucket



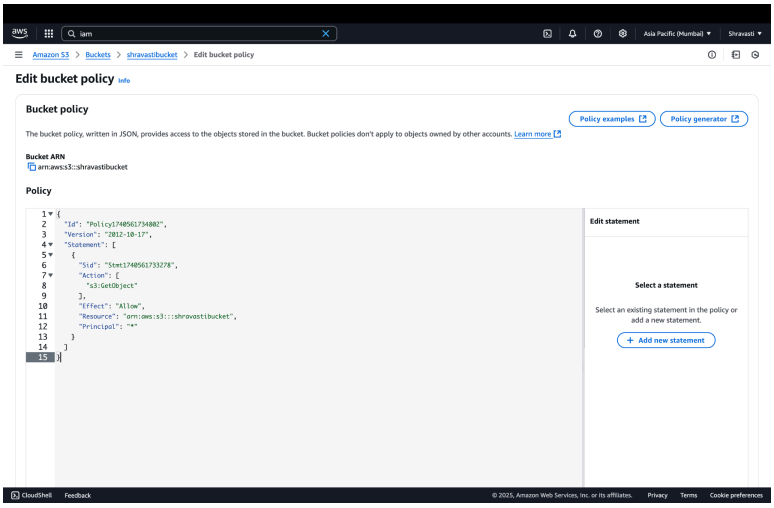
v. Click on generate policy



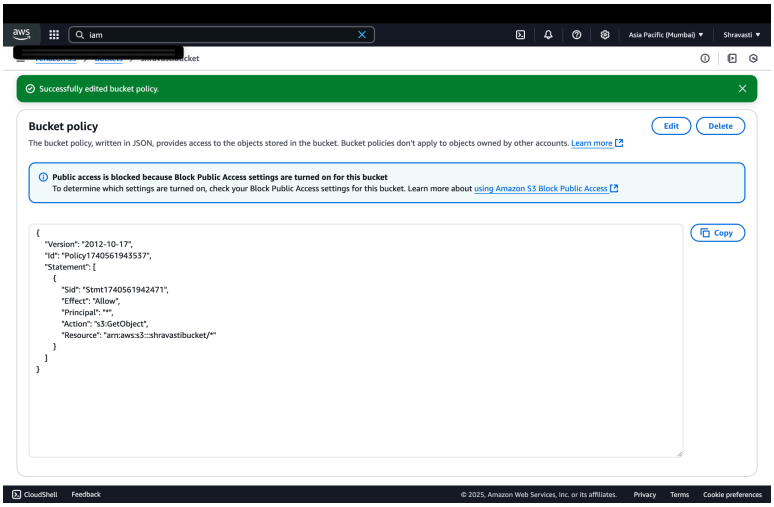
vi. Copy the generated policy



vii. Paste the policy in the bucket policy section



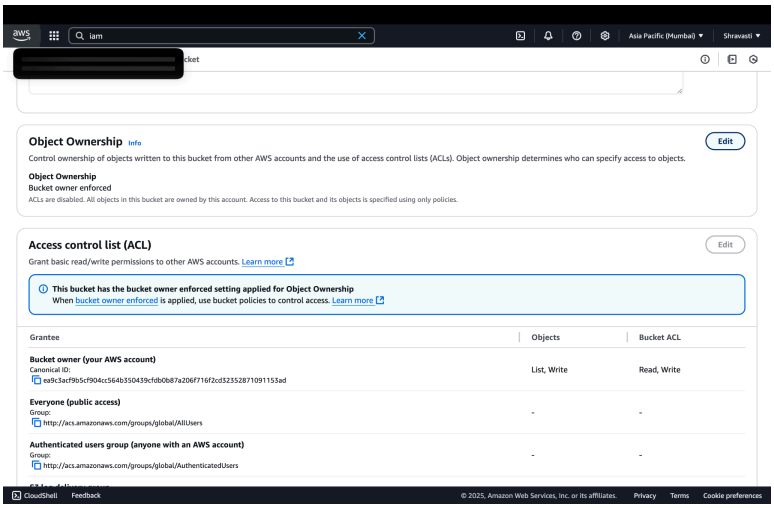
viii. Create the policy



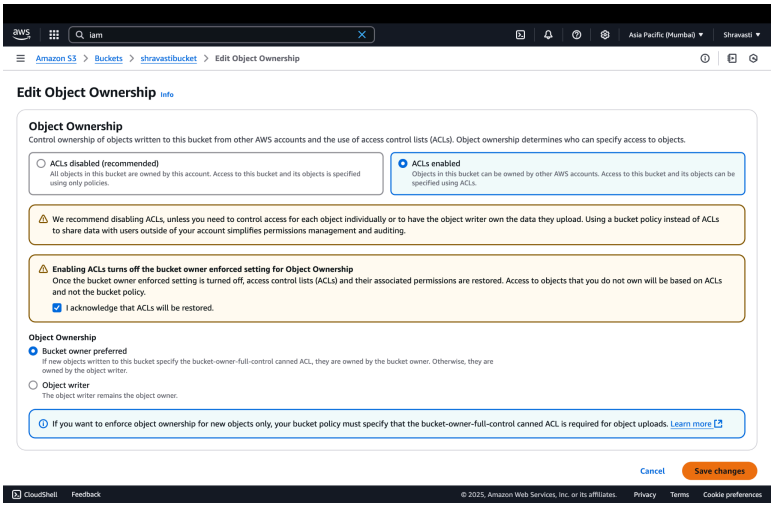
ix. The resource will be publicly accessible through the URL

b. Using Object Ownership

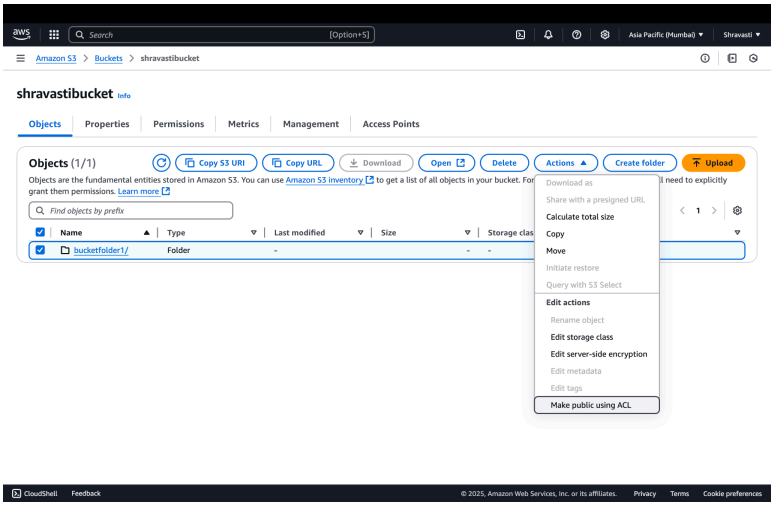
i. Under Object ownership, click on edit



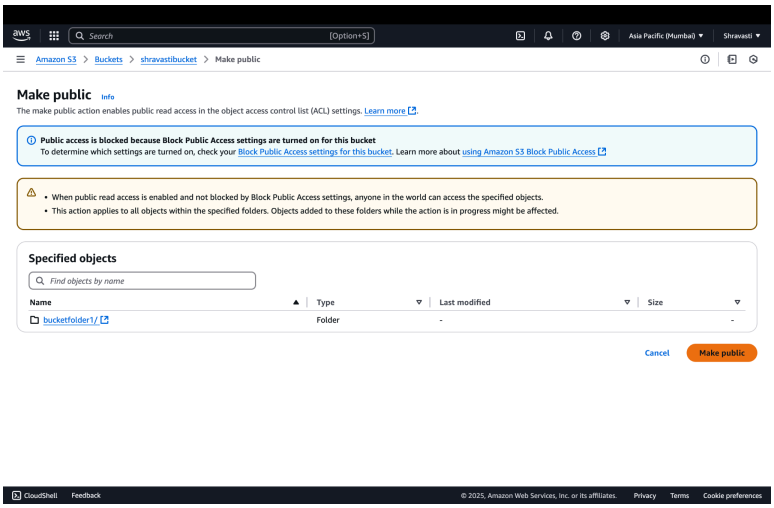
ii. Select ACL enabled → bucket owner preferred



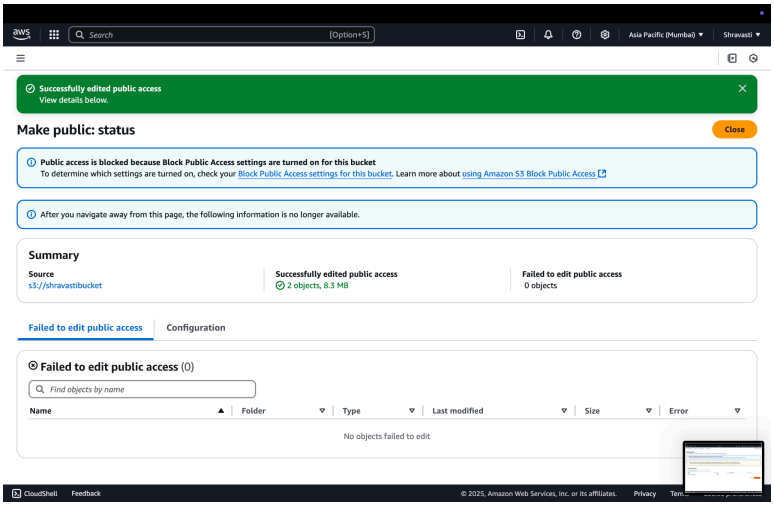
iii. Go to the bucket and select it. Under Actions, select ‘make public using ACL’



iv. Click on make public

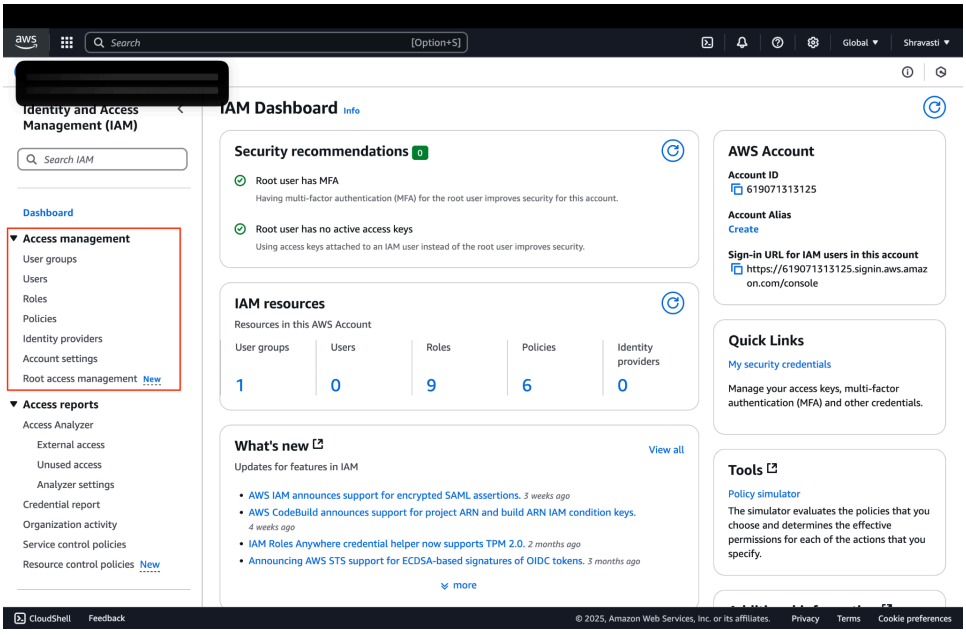


v. Public access will be successfully enabled and objects will be visible publicly.

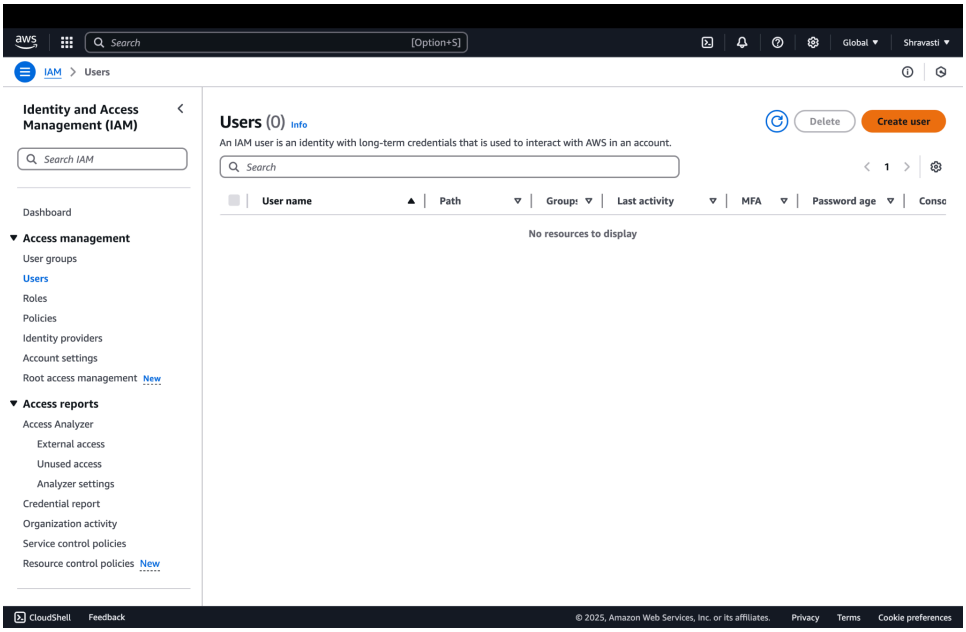


10. Creating an IAM user and giving that user access to the bucket and its contents

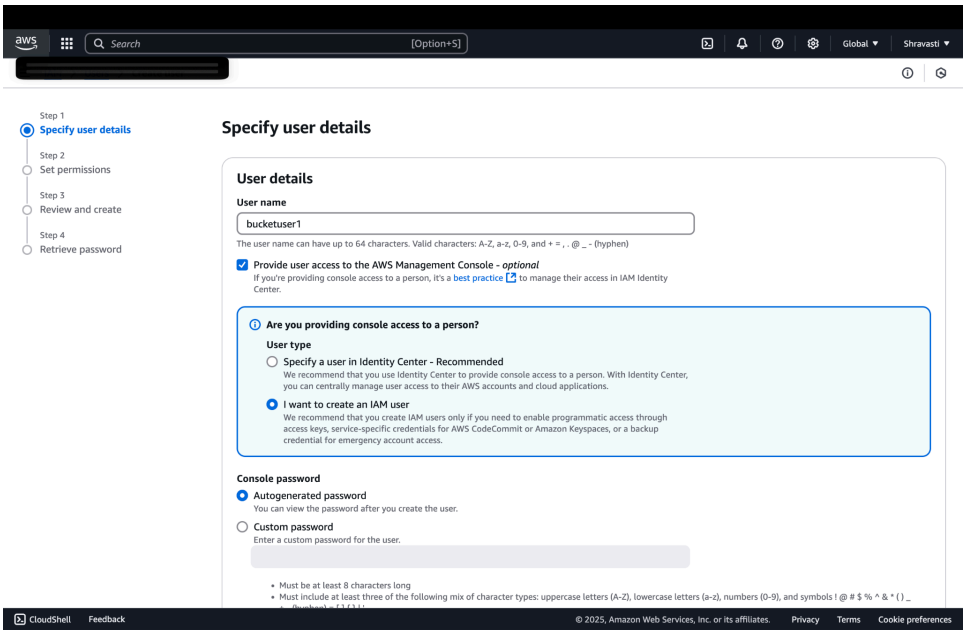
a. Navigate to the IAM service

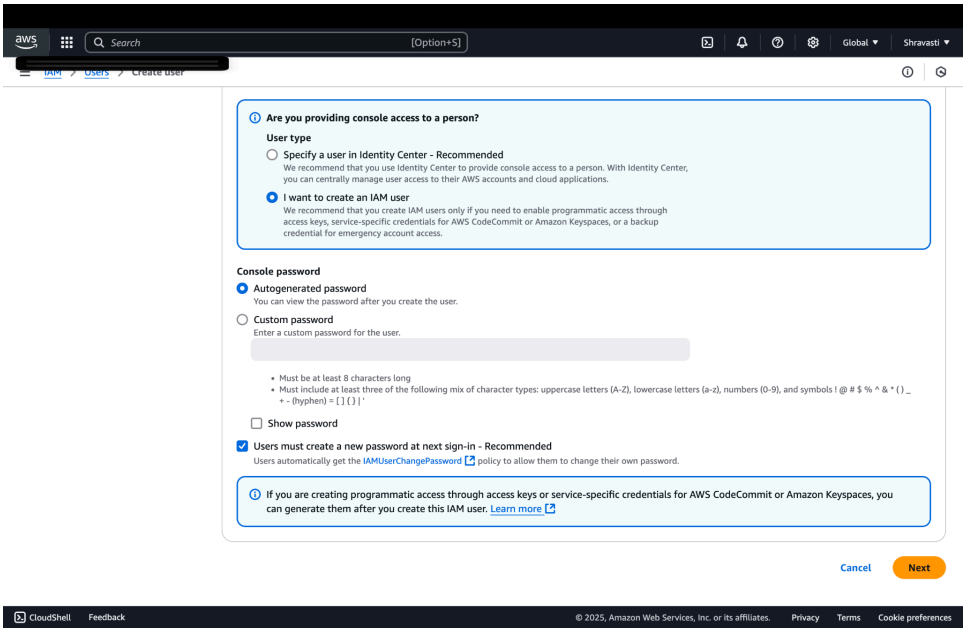


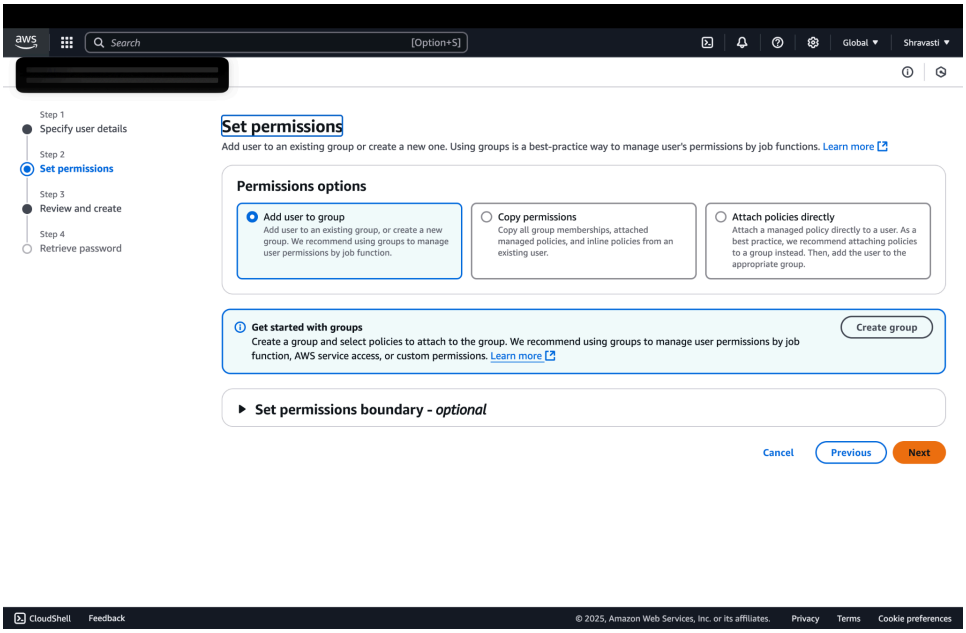
b. Click on create user

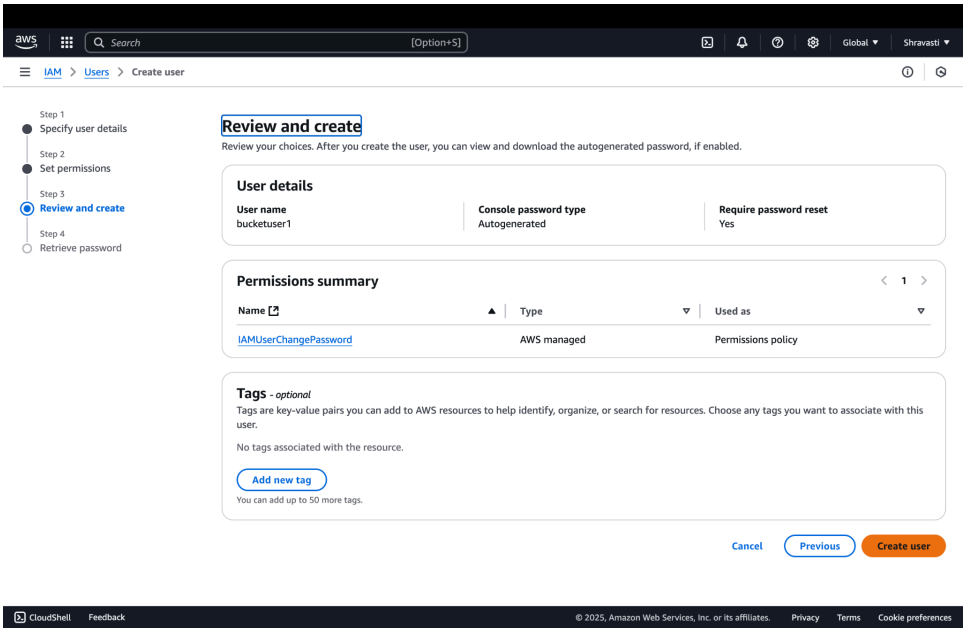


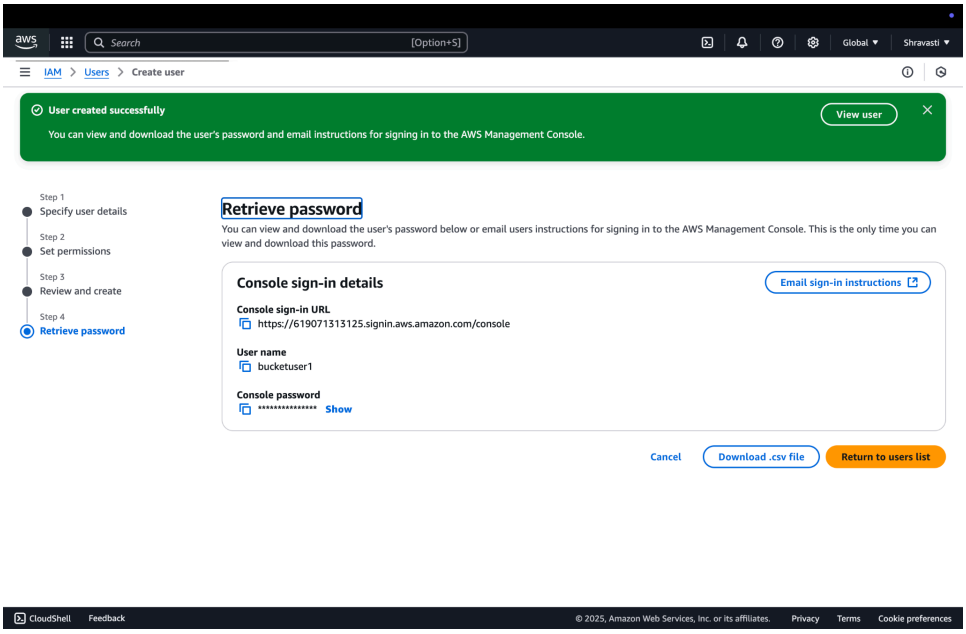
c. Configure the settings to provide access to the console



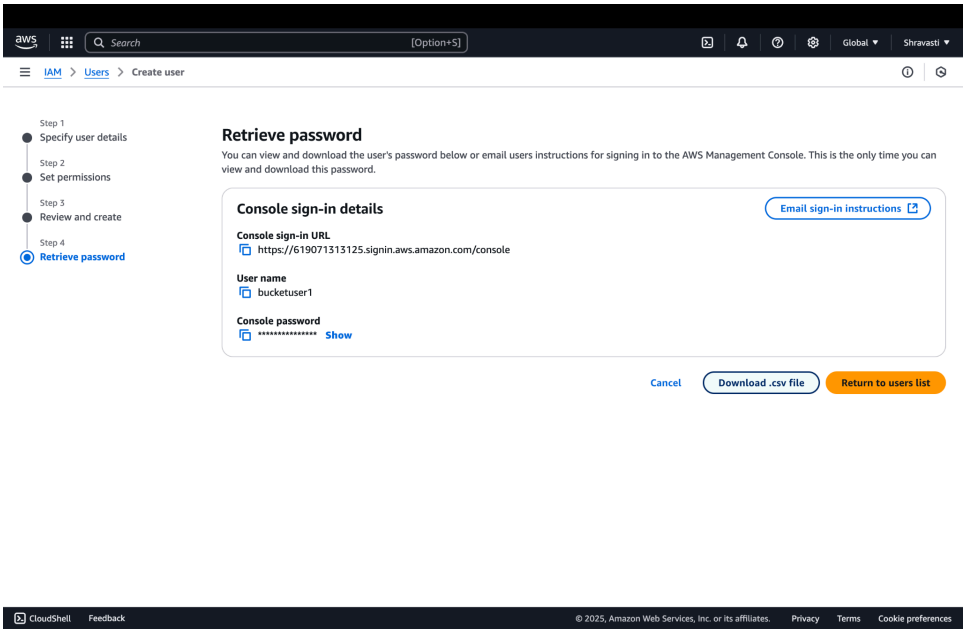

aws
Search
[Option+S]
Global
Shravasti
IAM > Users > Create user
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
Console password
Autogenerated password
You can view the password after you create the user.
Custom password
Enter a custom password for the user.
• Must be at least 8 characters long
• Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '
Show password
Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Search
[Option+S]
Global
Shravasti
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
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.
Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
Create group
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

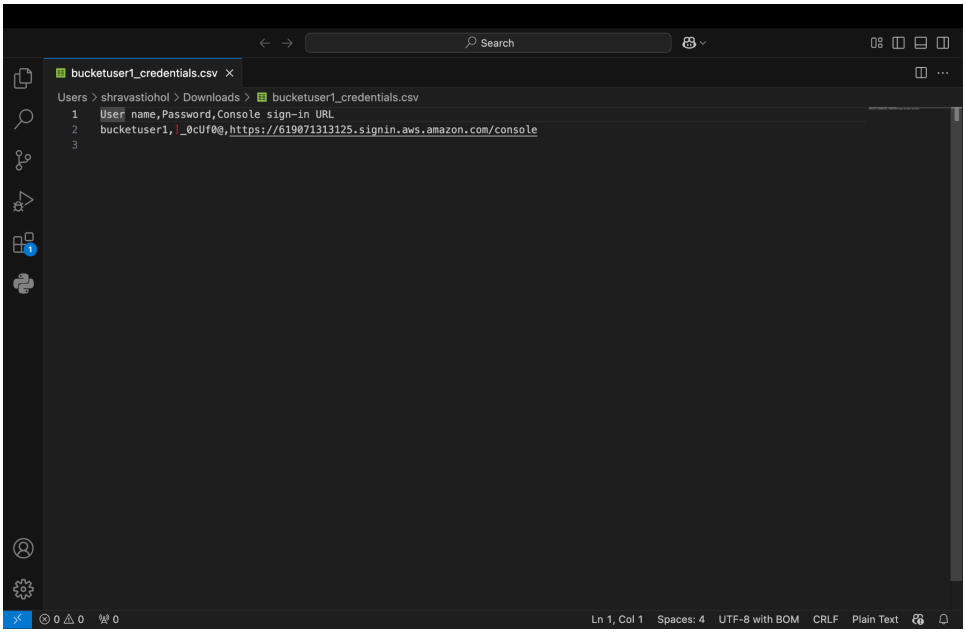

Search
[Option+S]
Global
Shravasti
IAM
Users
Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
bucketuser1
Console password type
Autogenerated
Require password reset
Yes
Permissions summary
Name
Type
Used as
IAMUserChangePassword
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.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create user
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Option+S]
Global
Shravasti
IAM
Users
Create user
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
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.
Console sign-in details
Email sign-in instructions
Console sign-in URL
https://619071313125.signin.aws.amazon.com/console
User name
bucketuser1
Console password
********** Show
Cancel
Download .csv file
Return to users list
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

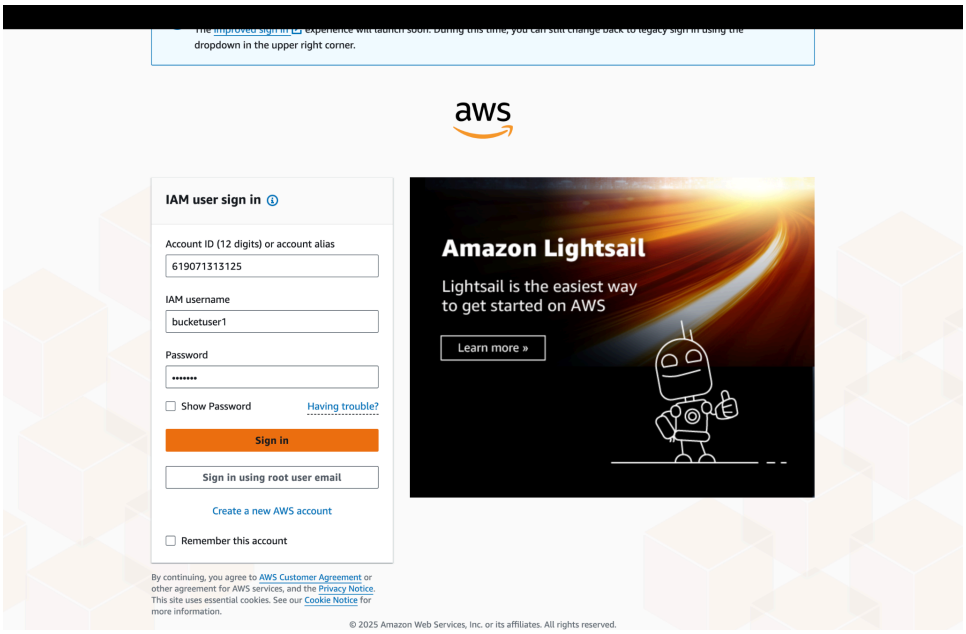
d. Download the .csv file. Navigate to Console Sign-in



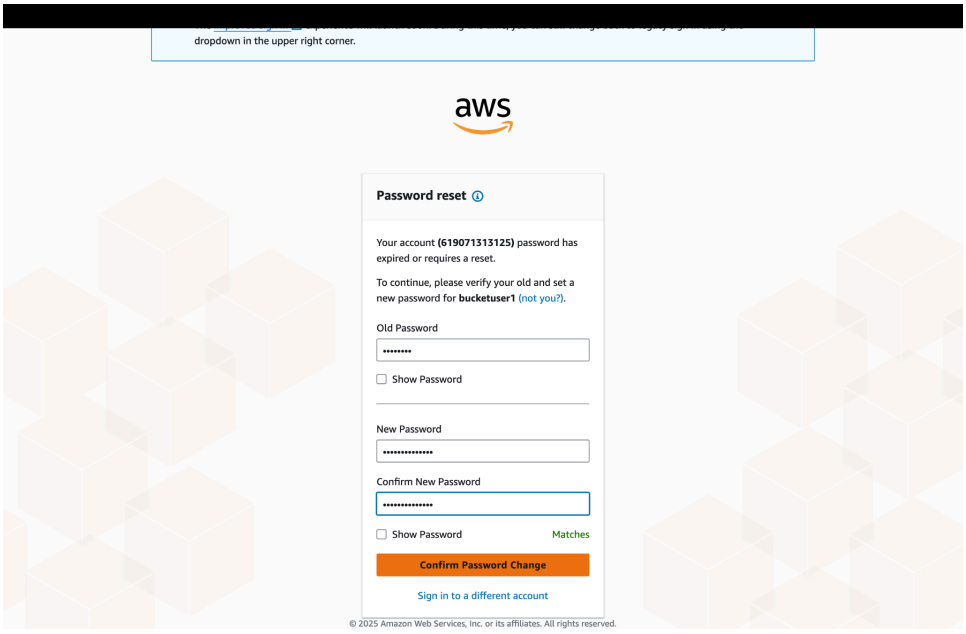
e. Downloaded .csv file contains IAM user credentials



f. Sign-in using the credentials provided



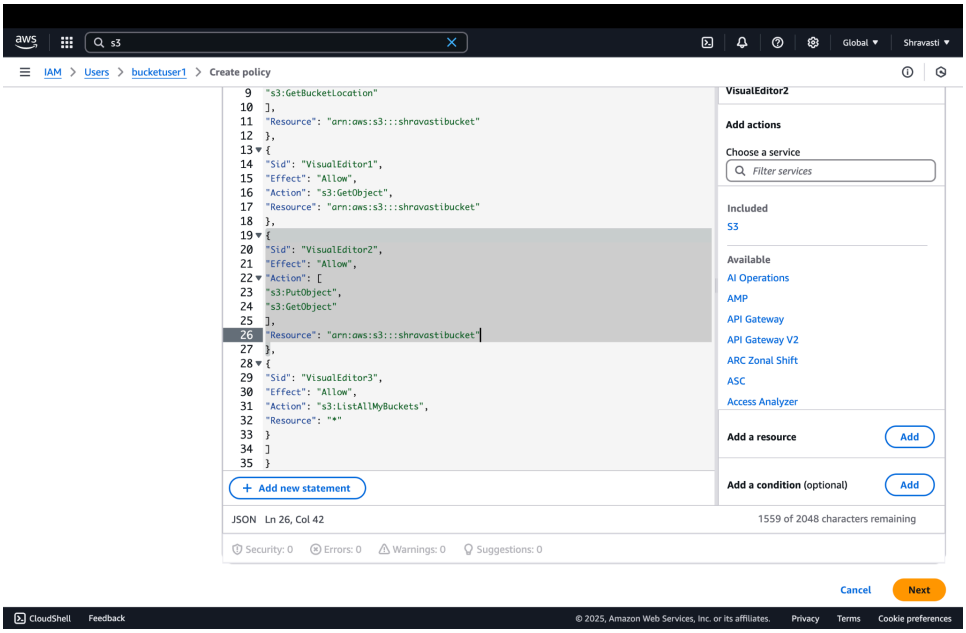
g. Reset the password



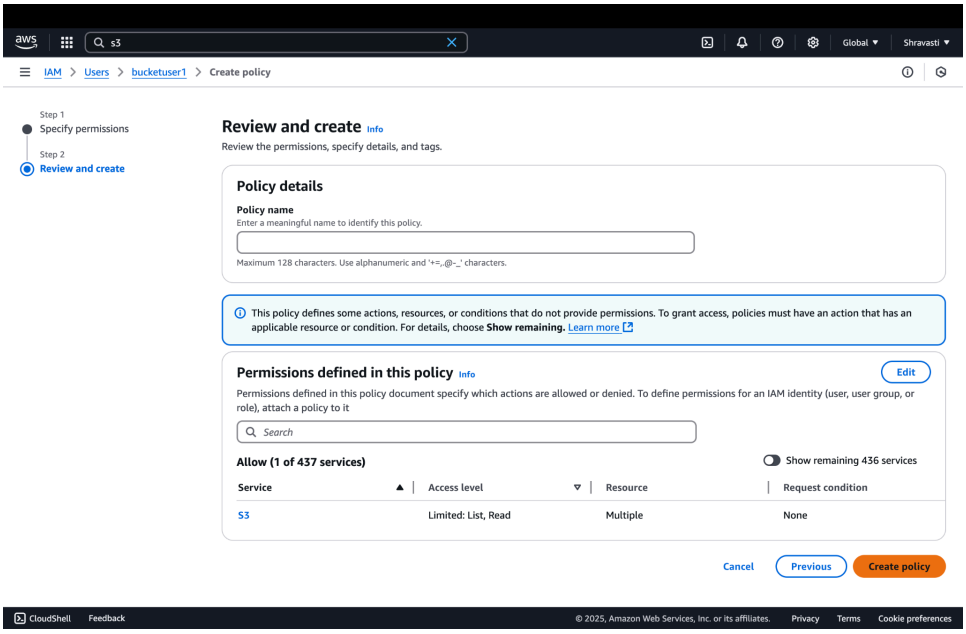
h. Access to the bucket and its contents will be denied.

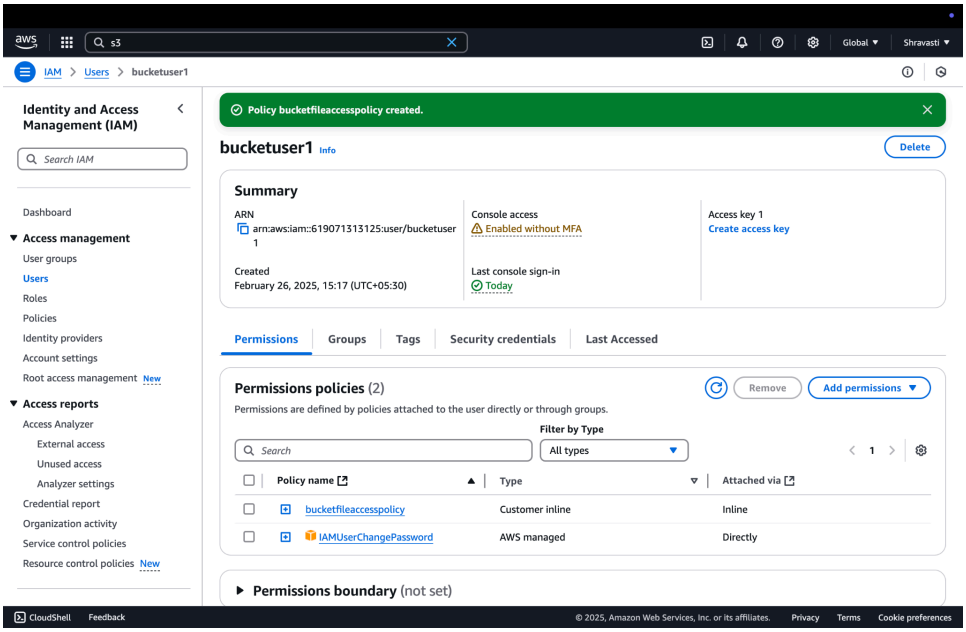
i. Configure inline permissions for the IAM user through the root user.

j. Write the inline policy



k. Name the policy and create it





l. Bucket and its contents will now be visible