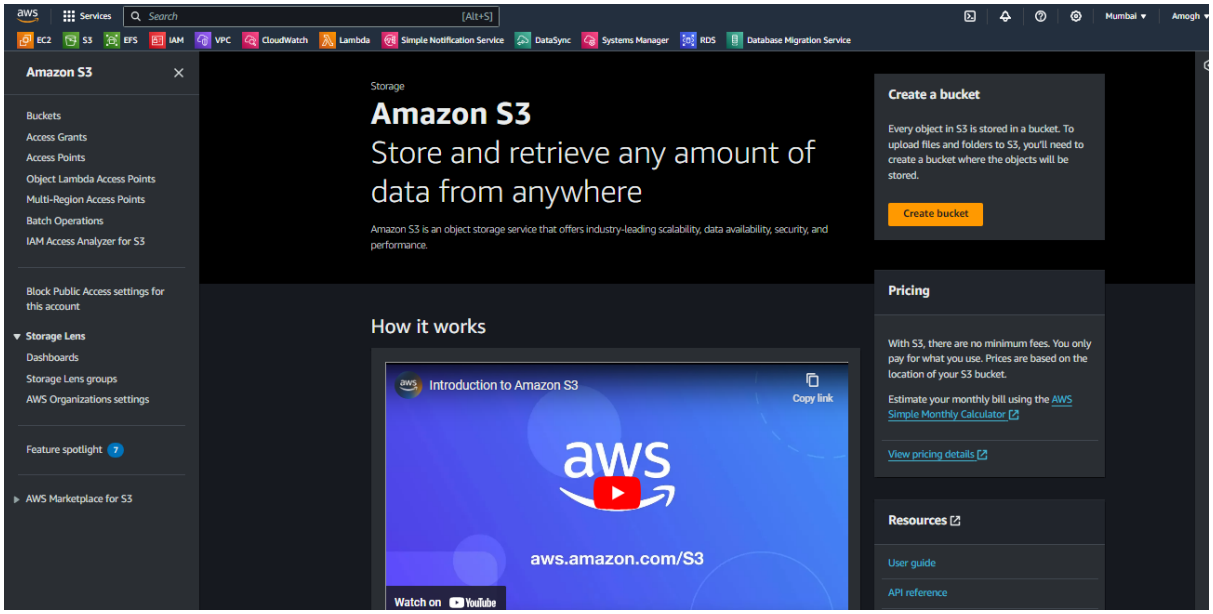
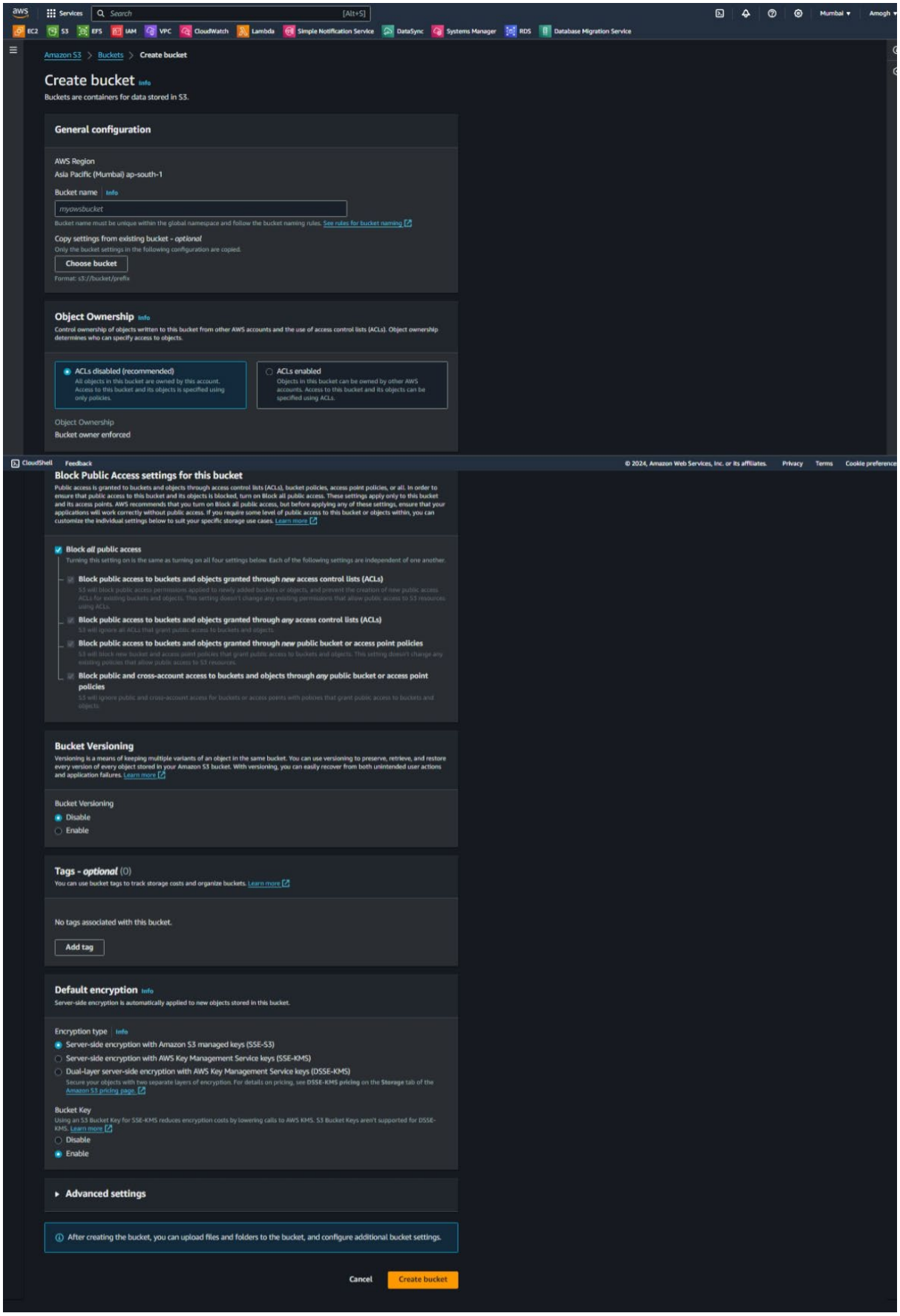
TASK

Create 2 S3 buckets and 2 IAM Users Give policy to both the IAM user in which one of the IAM user have full access of s3 service and the other IAM user having only read-only access to bucket 2(Single bucket).

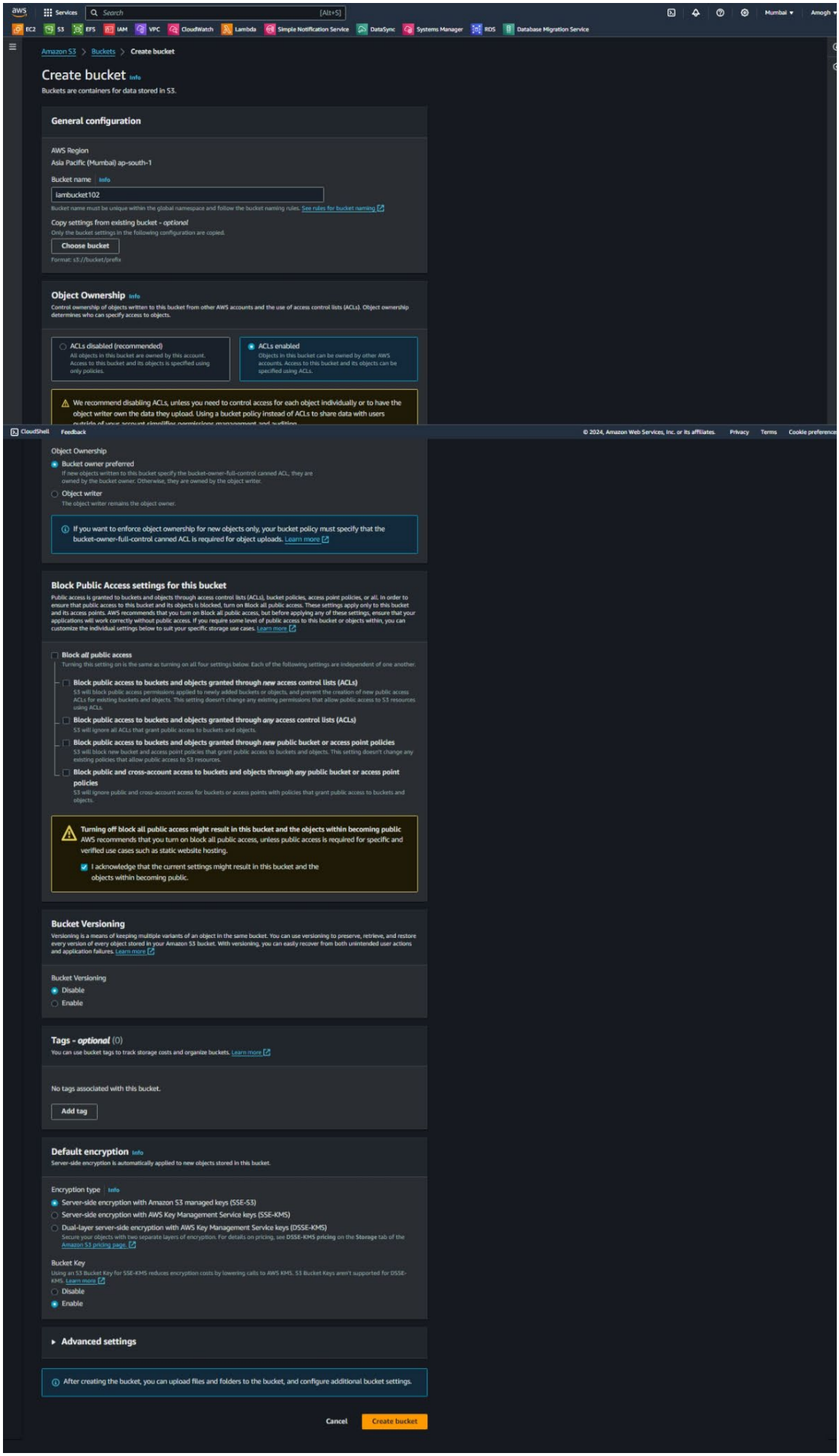
Step 1: Create 2 s3 buckets in AWS console using root user authentication



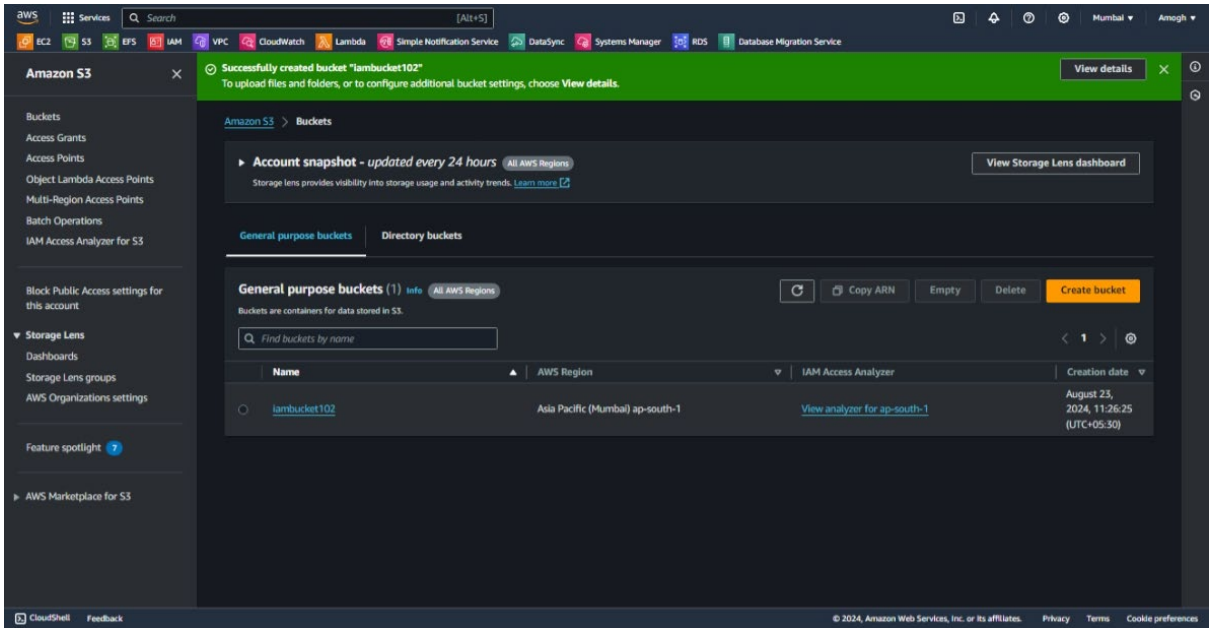
- Initial display page of creating s3 bucket.



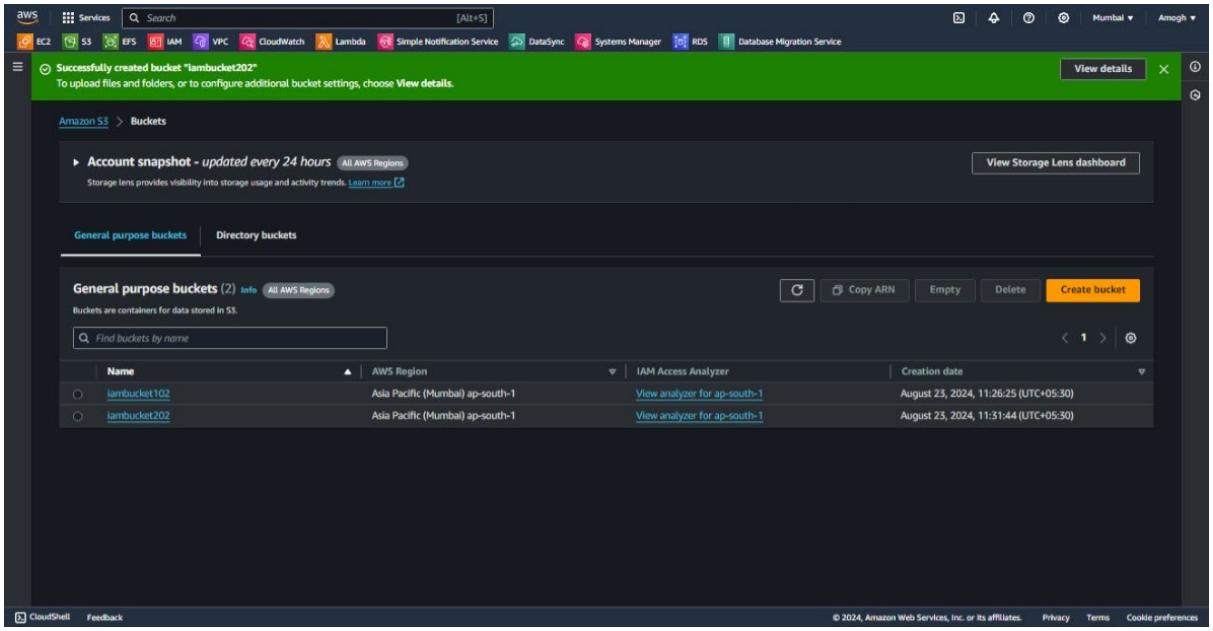
- So, we have created a bucket with the name “iambucket102”.



- Now 1 s3 bucket is created

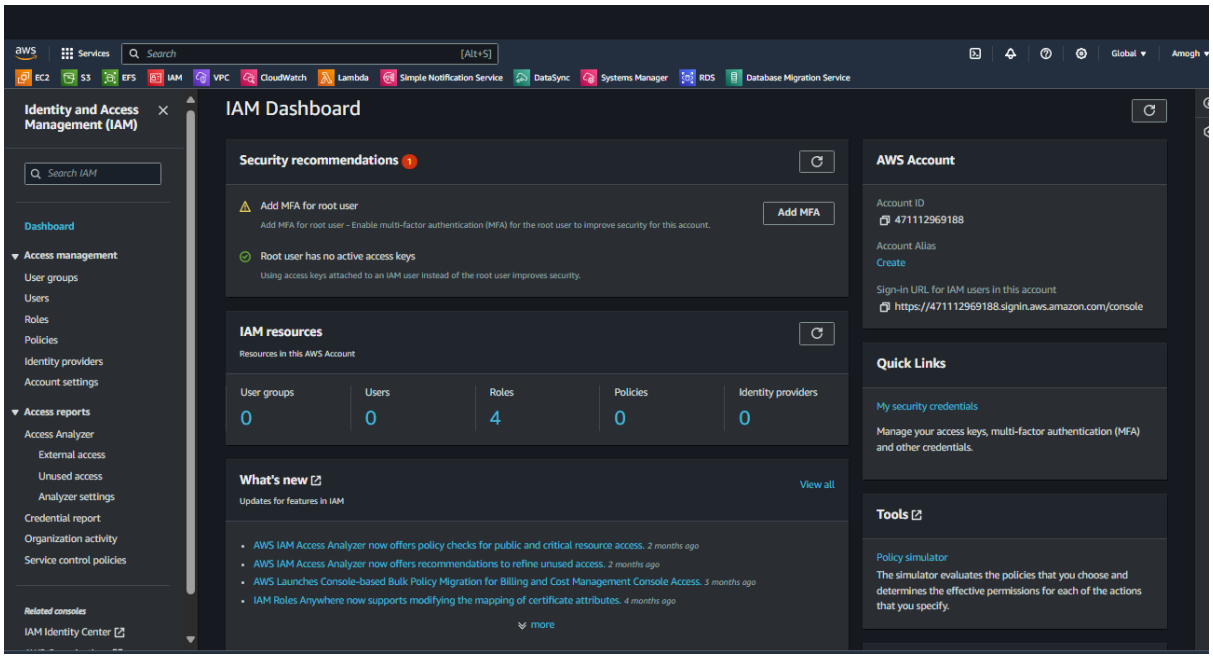


Similarly, we have to create 2nd bucket.

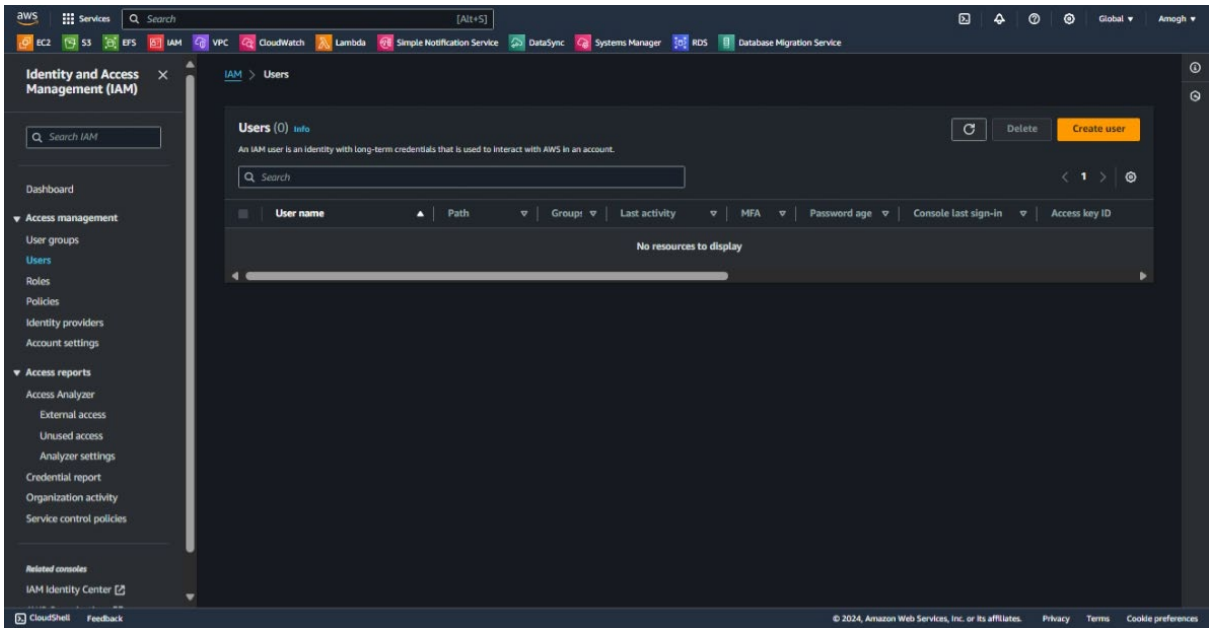


- We have successfully created the 2nd bucket as well.

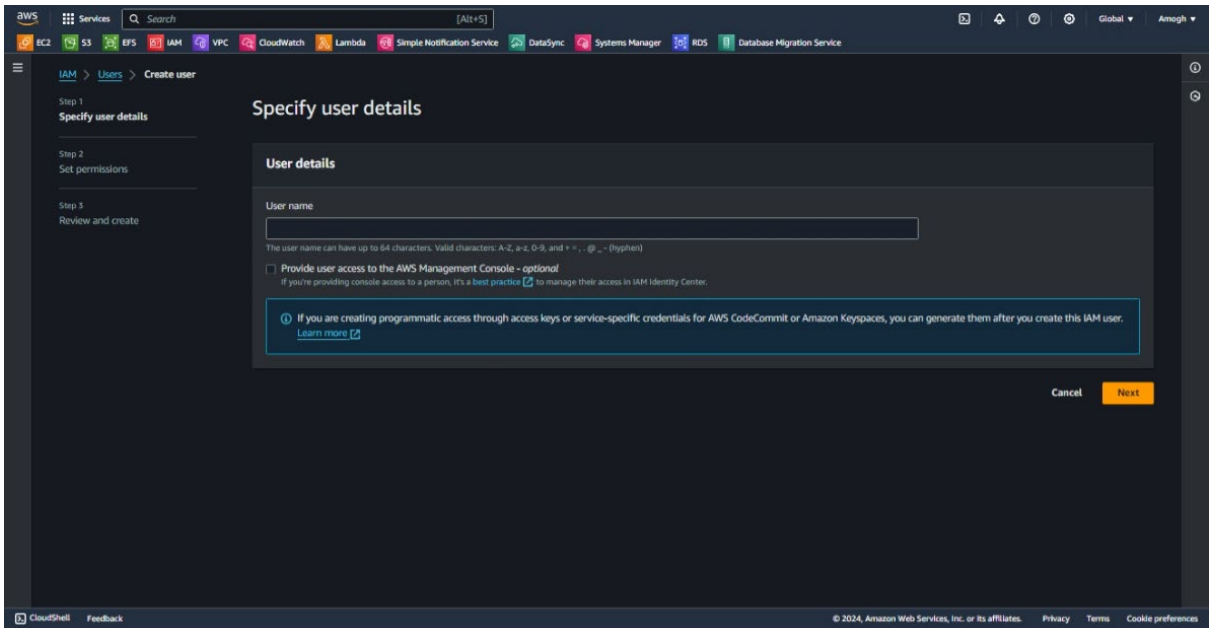
Step 2: Now after successfully creating 2 buckets, we have to search "**IAM**" in the Service desk and click on the service.



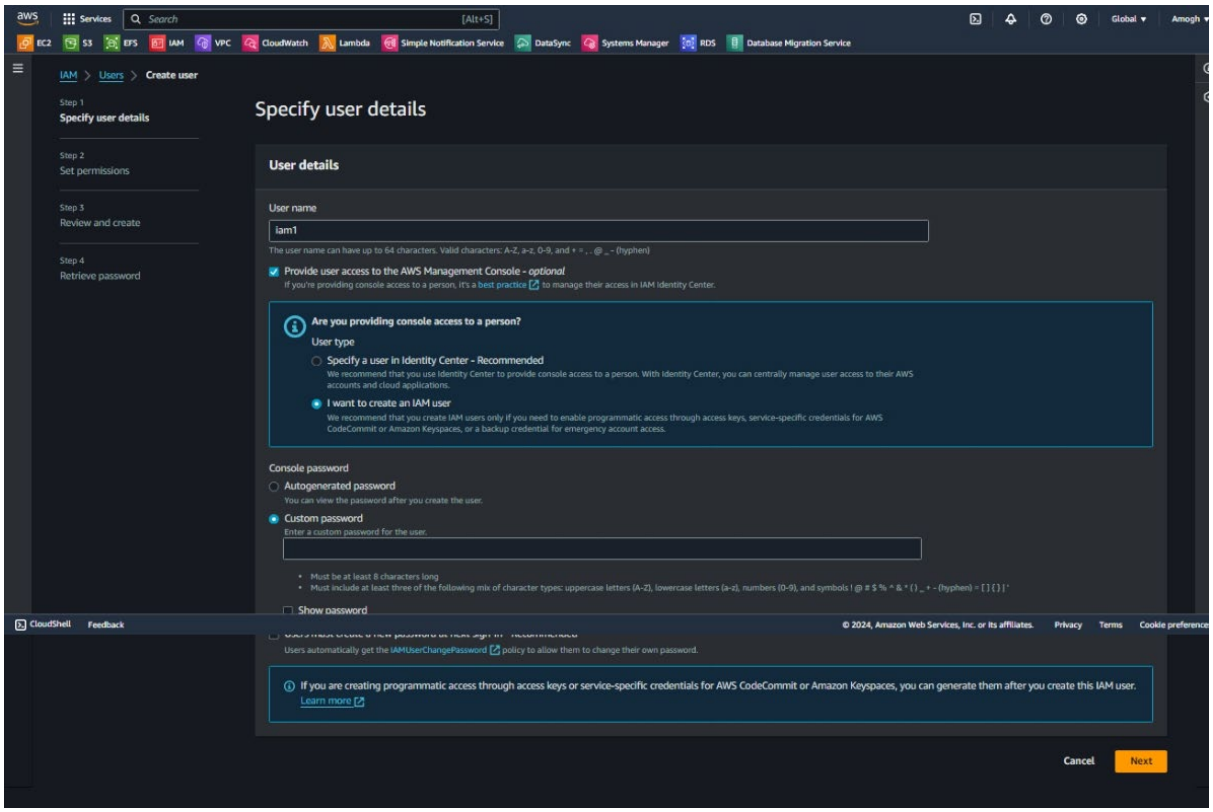
- Here click on the option "Users" and choose the option and click on "**Create user**".



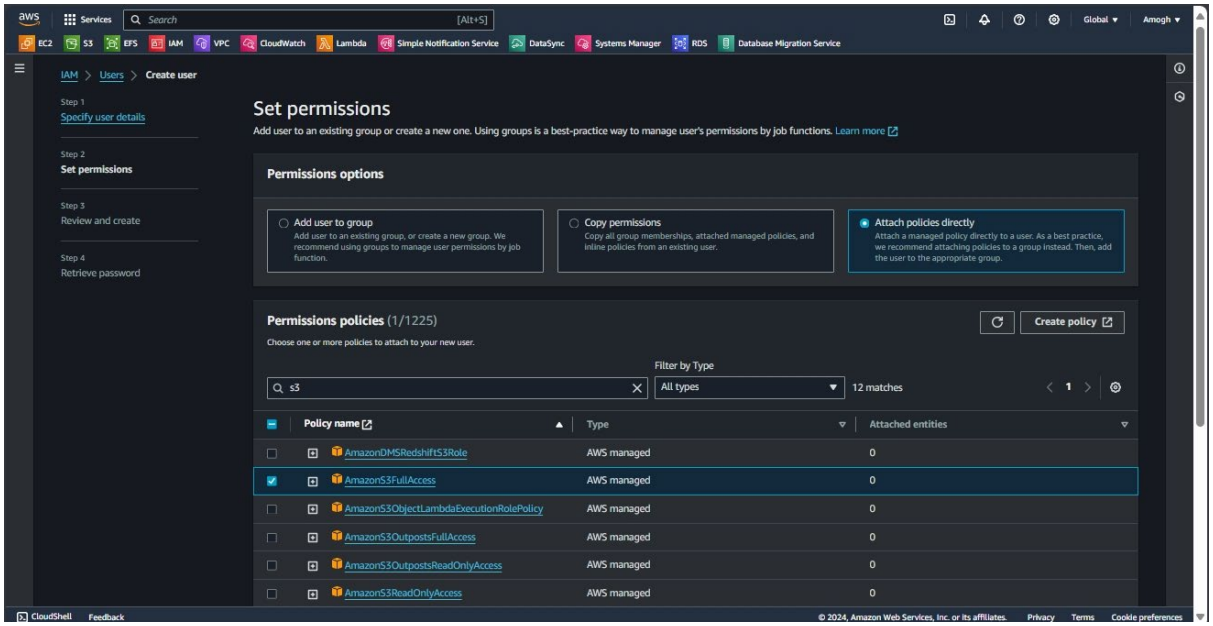
- After going inside “**Create user**” page, name the username and click on the checkbox below to “**Provide user access to the AWS Management Console**” so that password can be created by us for the IAM user.

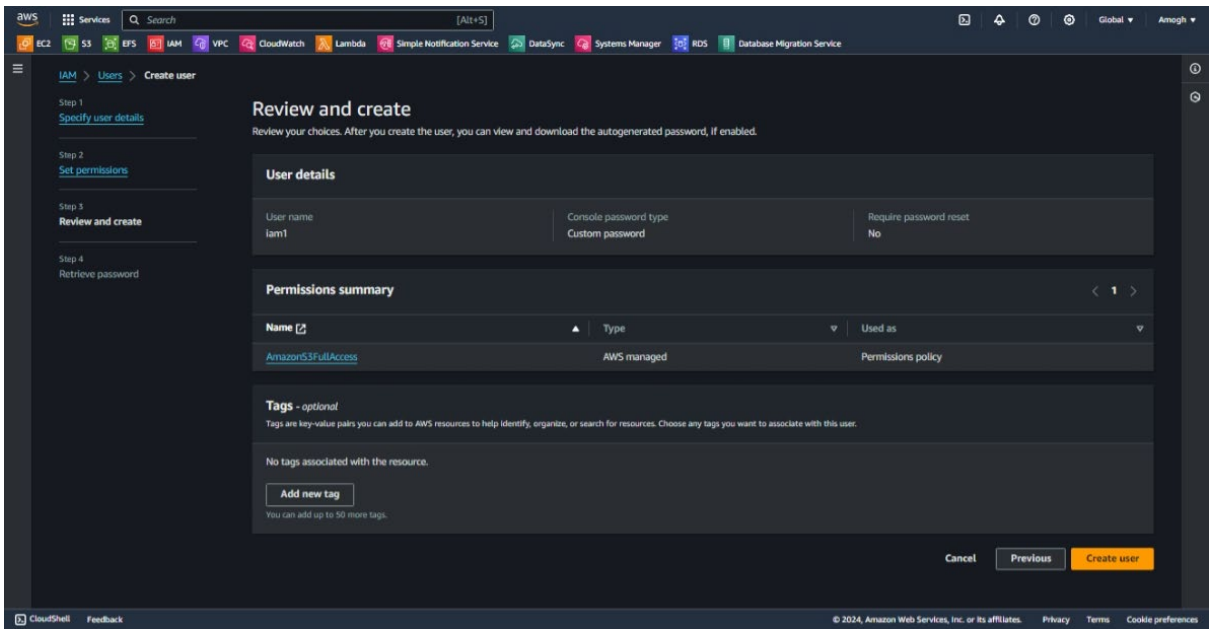


- We are disabling the “**User must create a new password at next sign-in**” option.

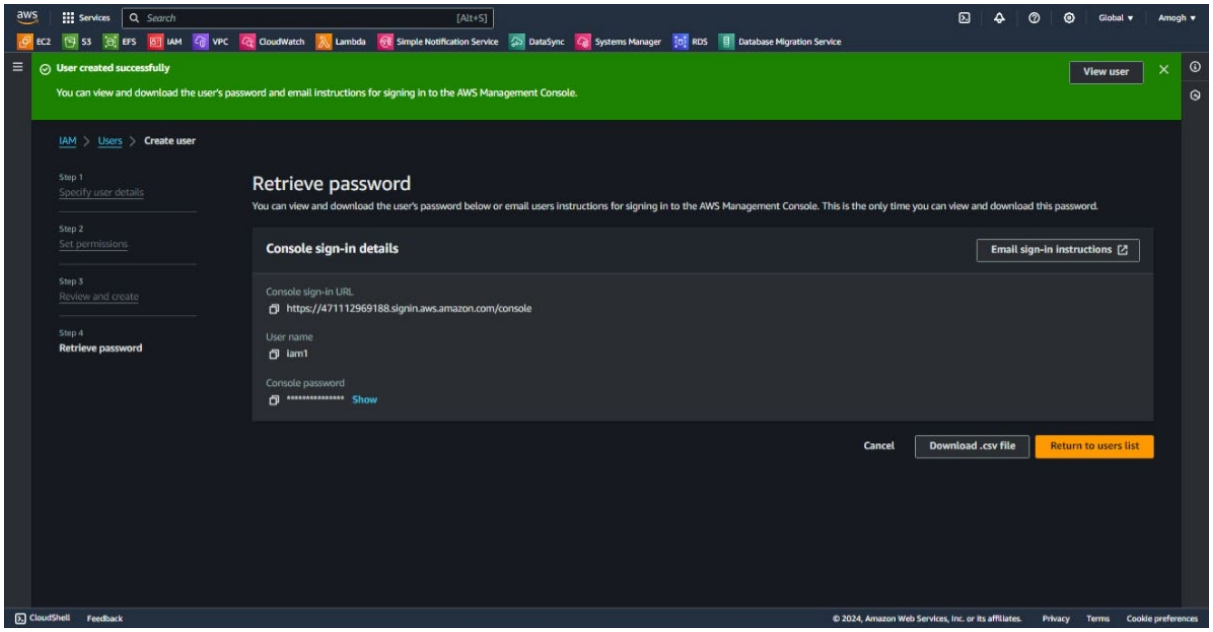


- We need to attach policy for an IAM user. Here we should give s3FullAccess policy for 1st IAM user.

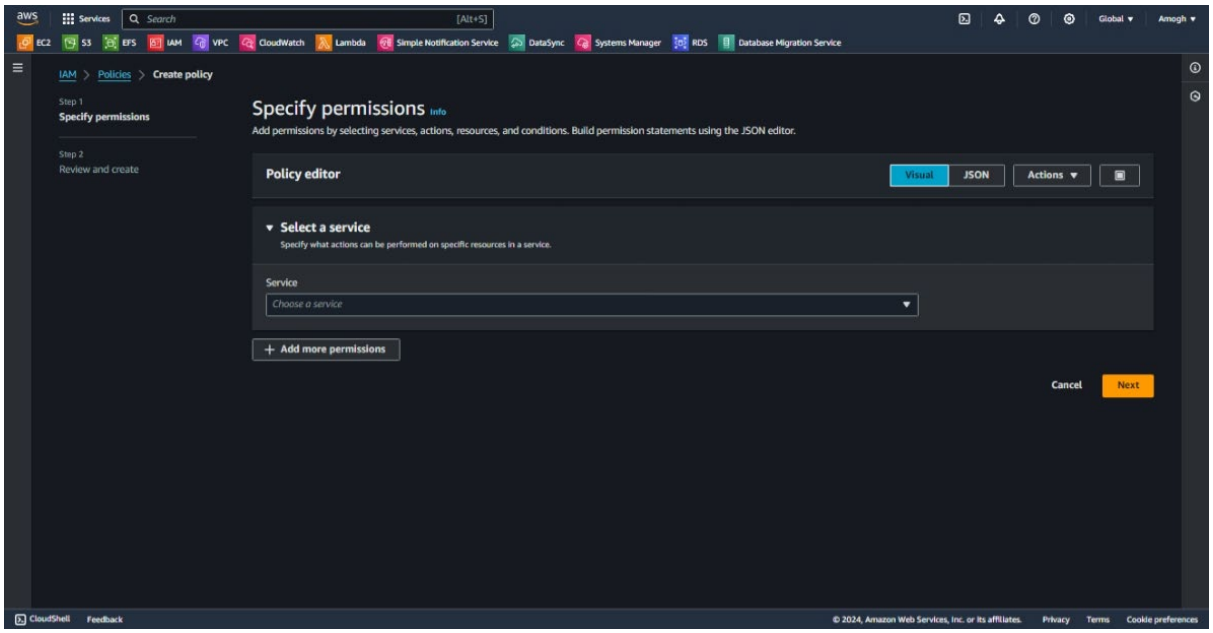




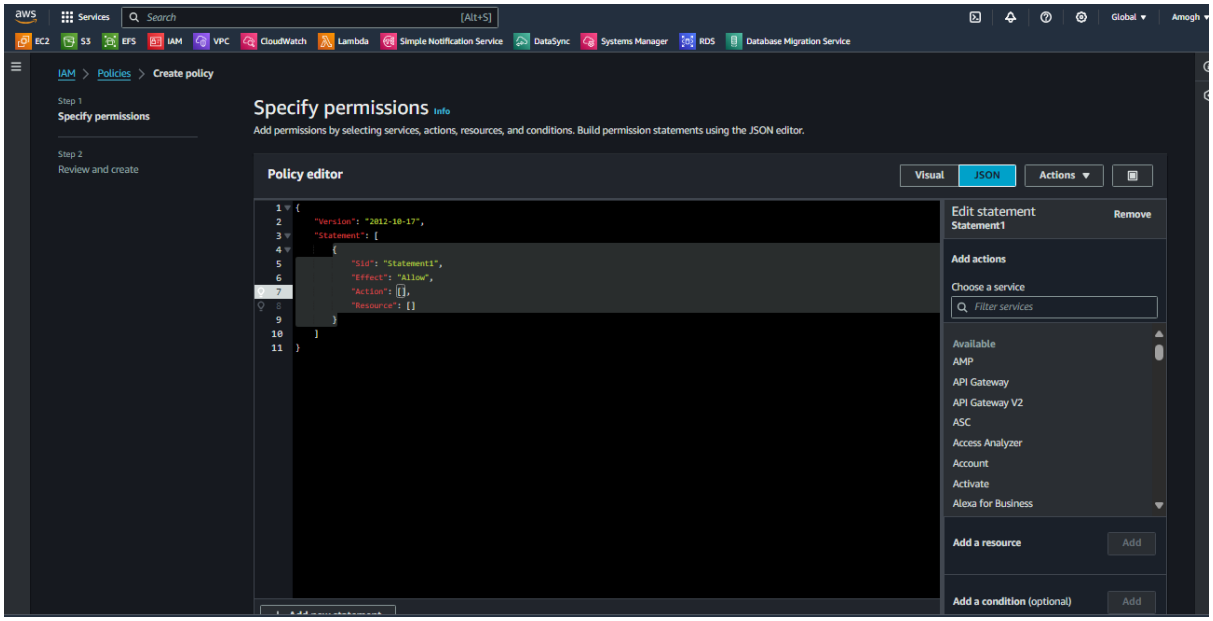
- 1st User is created. Now we should save the console sign-in details.



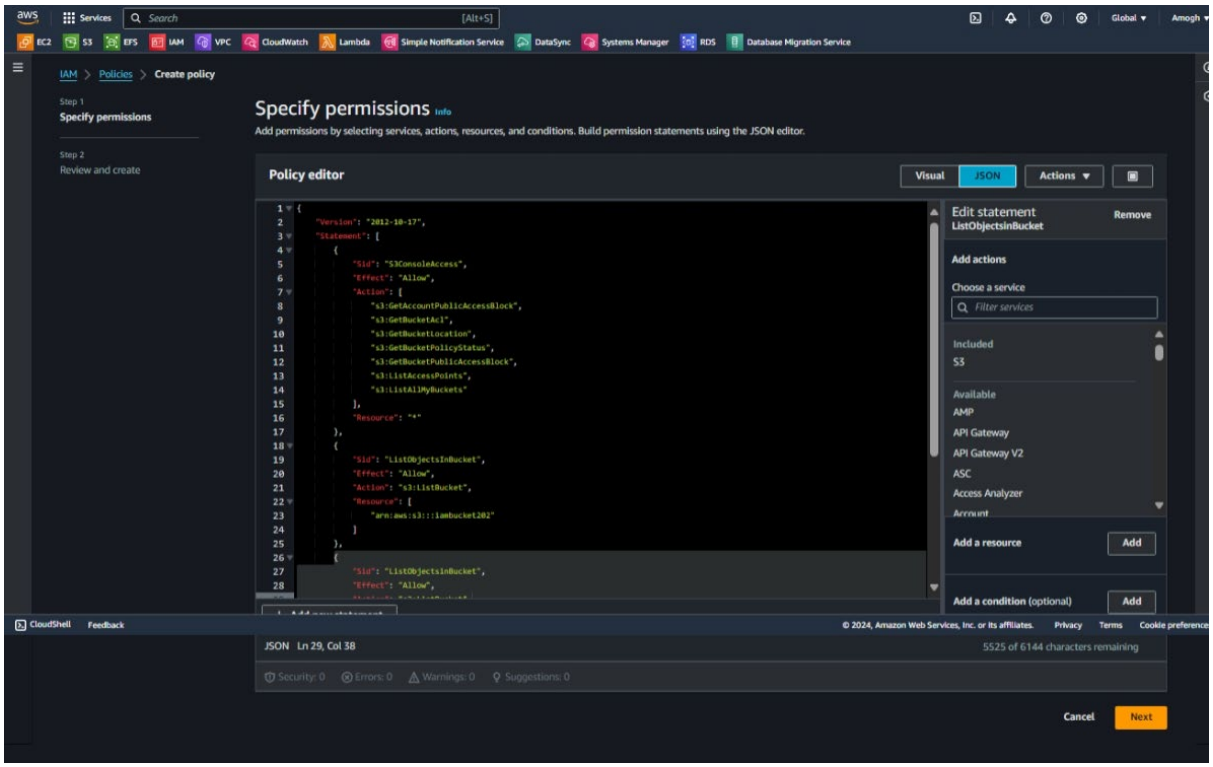
Step 3: After creating 1st IAM user with S3FullAccess policy, we should create a policy by clicking on "**Create policy**" option.



- Below is the default JSON policy



- Click on JSON to choose the JSON option and give the command for limited access to s3 bucket where the IAM user have only read-only Access to bucket 2

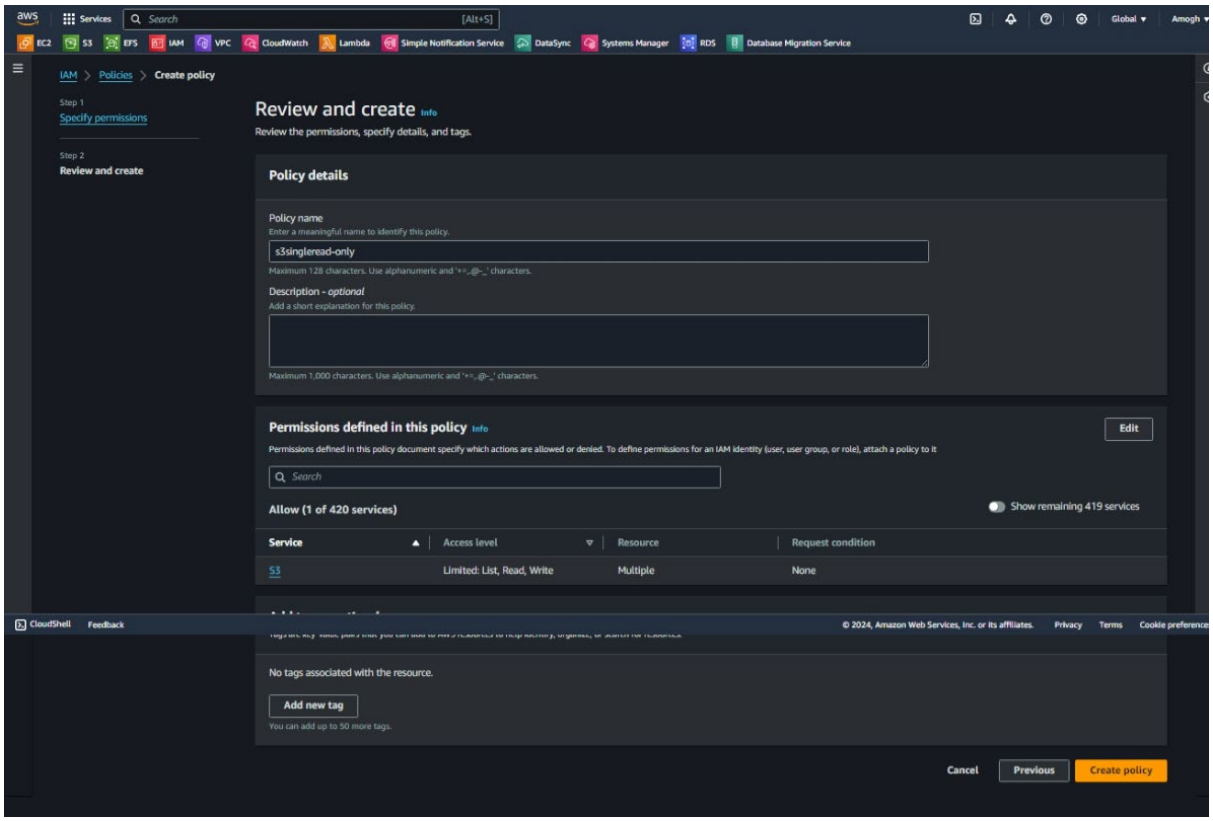


- The above policy code is mentioned below: (Note: Replace bucket names)

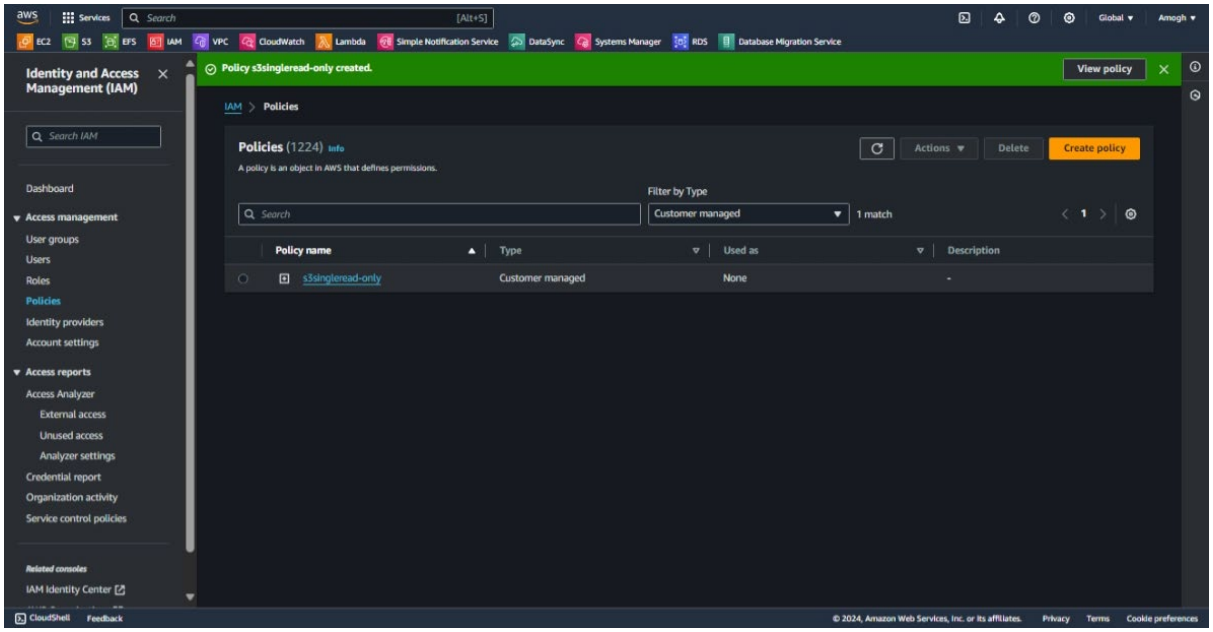
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3ConsoleAccess",
      "Effect": "Allow",
      "Action": [
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ListObjectsInBucket",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": [
        "arn:aws:s3:::iambucket202"
      ]
    },
    {
      "Sid": "ListObjectsinBucket",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
```

```
        "Resource": [
            "arn:aws:s3:::iambucket102"
        ]
    },
    {
        "Sid": "AllObjectActions",
        "Effect": "Allow",
        "Action": "s3:*Object",
        "Resource": [
            "arn:aws:s3:::iambucket102/*"
        ]
    }
  ]
}
```

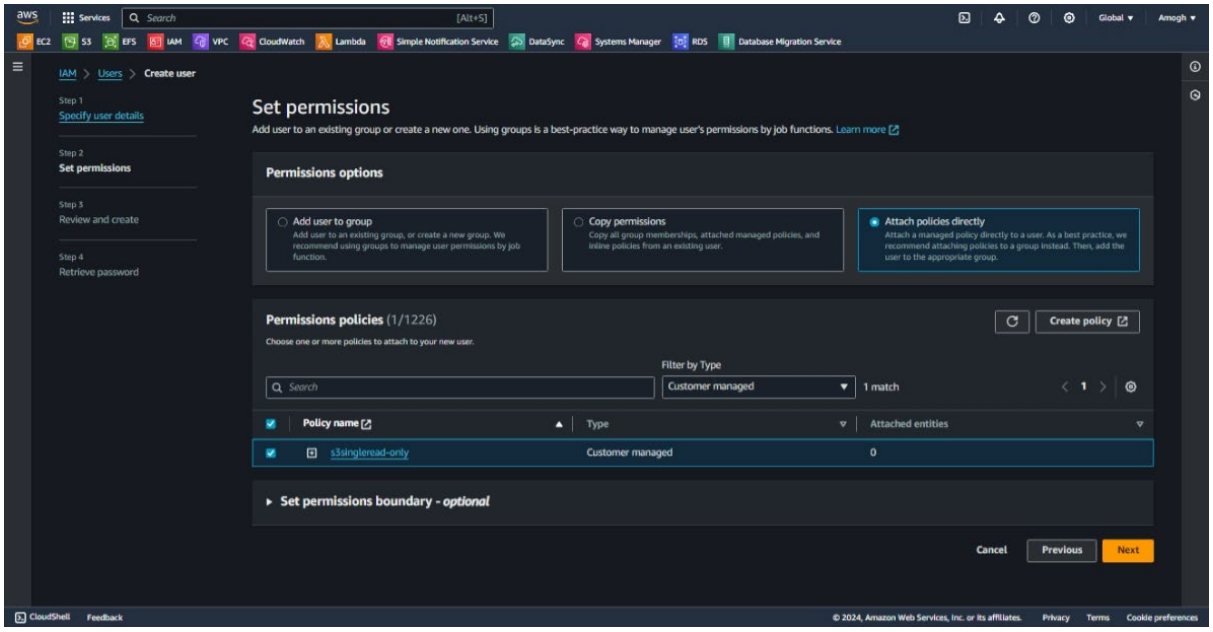
- Clicking Next takes us to naming the policy page

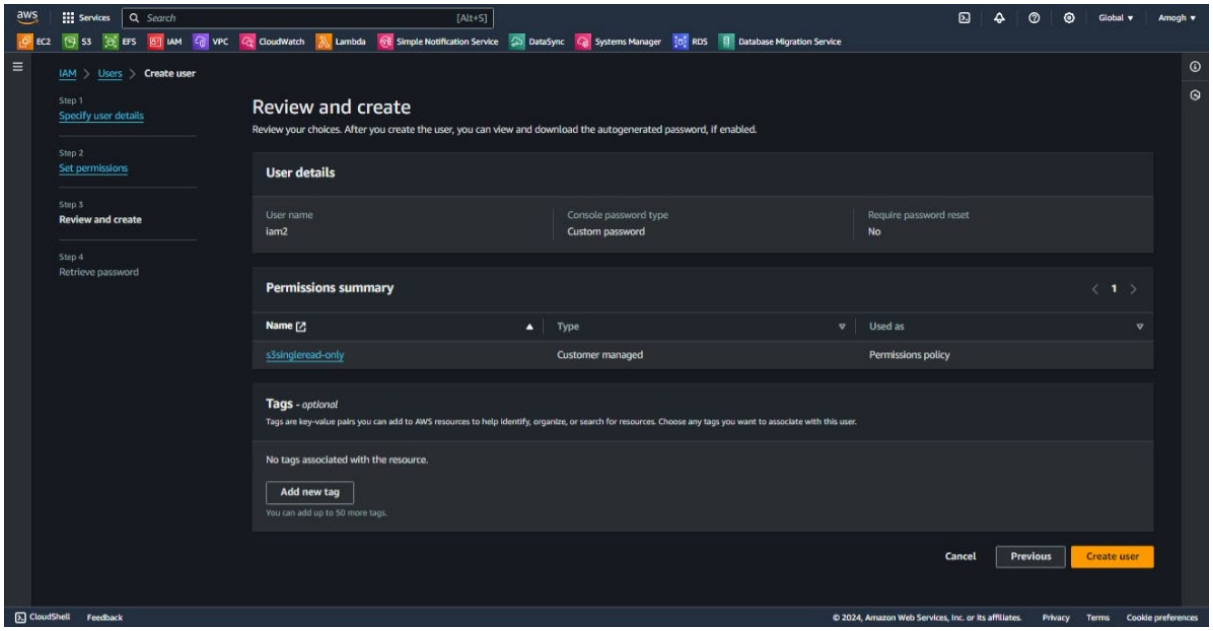


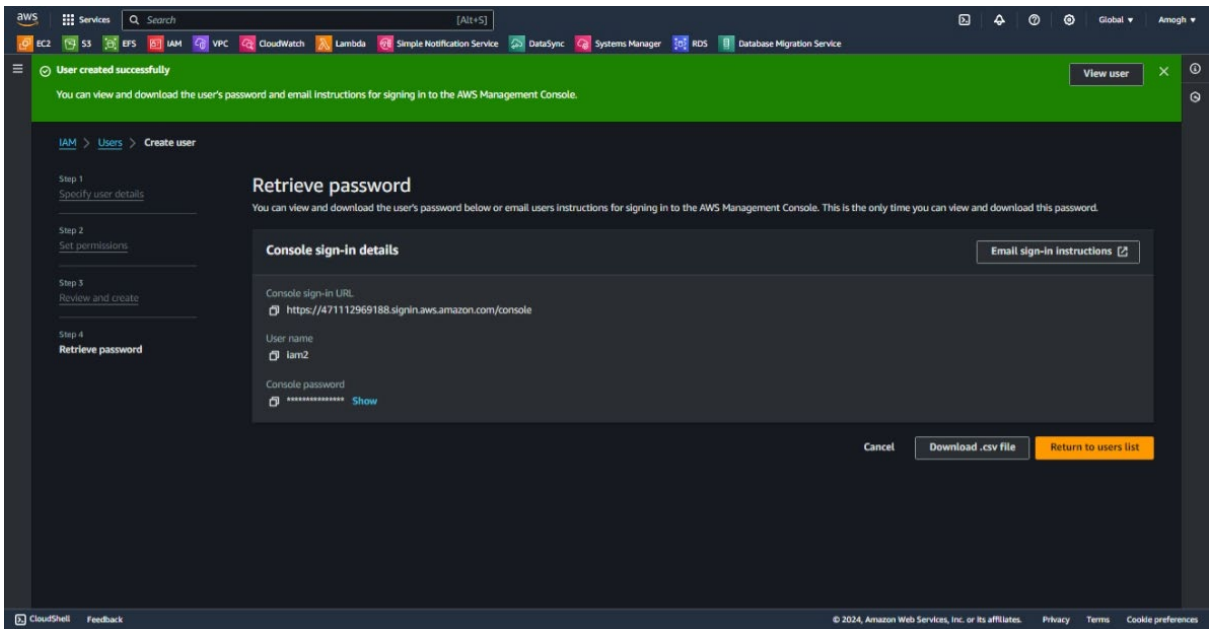
- Customer policy is created

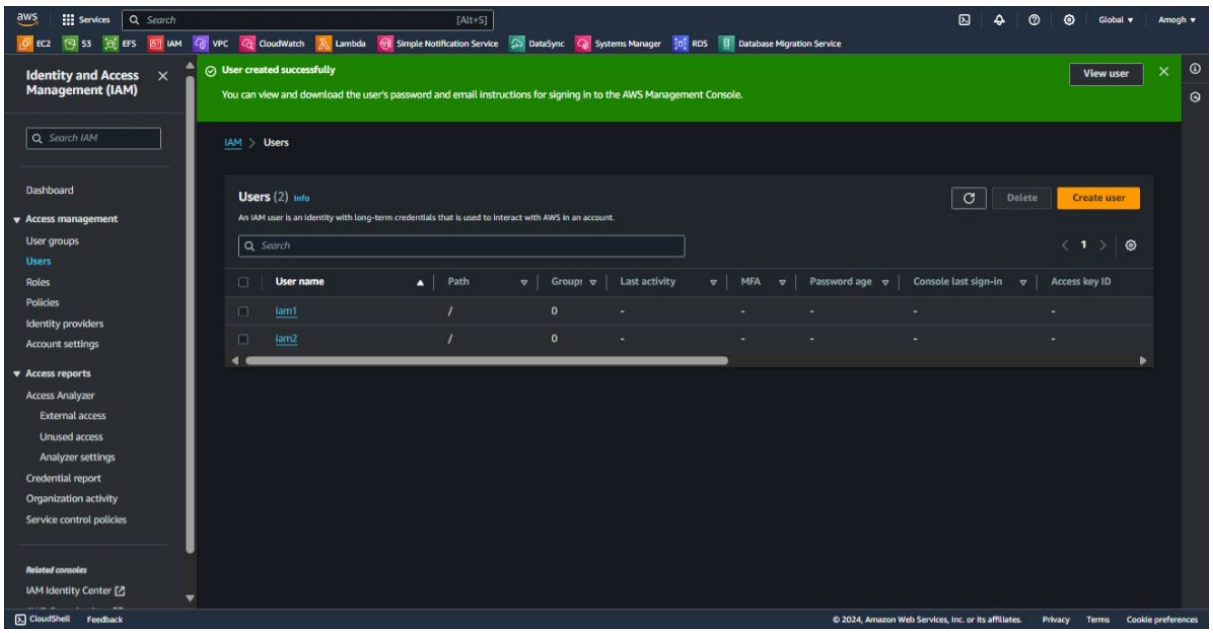


- Now we need to create 2nd IAM user with the same procedure as we used in creating 1st IAM user but the only difference is in policy selection section. For 2nd IAM user, we should choose the customer managed policy that we have created with the name "s3singleread-only". So, we should attach "**s3singleread-only**" to 2nd IAM user.




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
iam2
Console password type
Custom password
Require password reset
No
Permissions summary
Name
Type
Used as
s3singleread-only
Customer 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

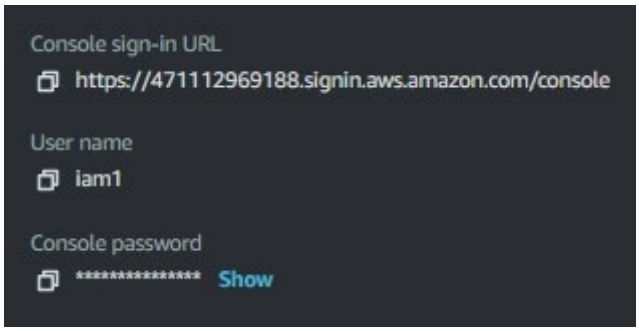

User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Retrieve password
You can 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://471112969188.signin.aws.amazon.com/console
User name
iam2
Console password
Show
Cancel
Download .csv file
Return to users list


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
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
IAM > Users
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
Access key ID
iam1
/
0
iam2
/
0

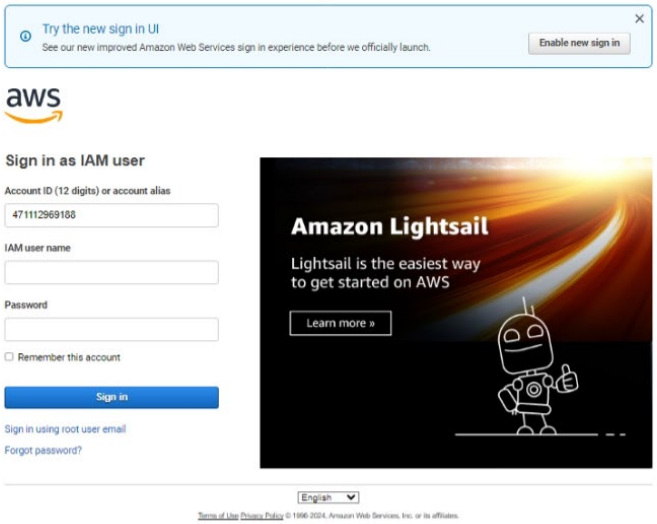
- After successfully creating 2 users and attaching the required policy and saving the credentials of IAM users' sign-in for both users, we should logout from root user and go to console login and sign-in to 1st IAM user

OR

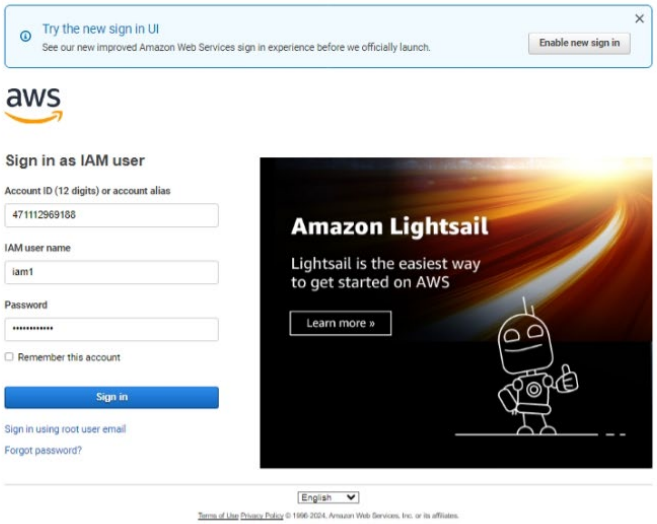
Paste the link of the IAM user



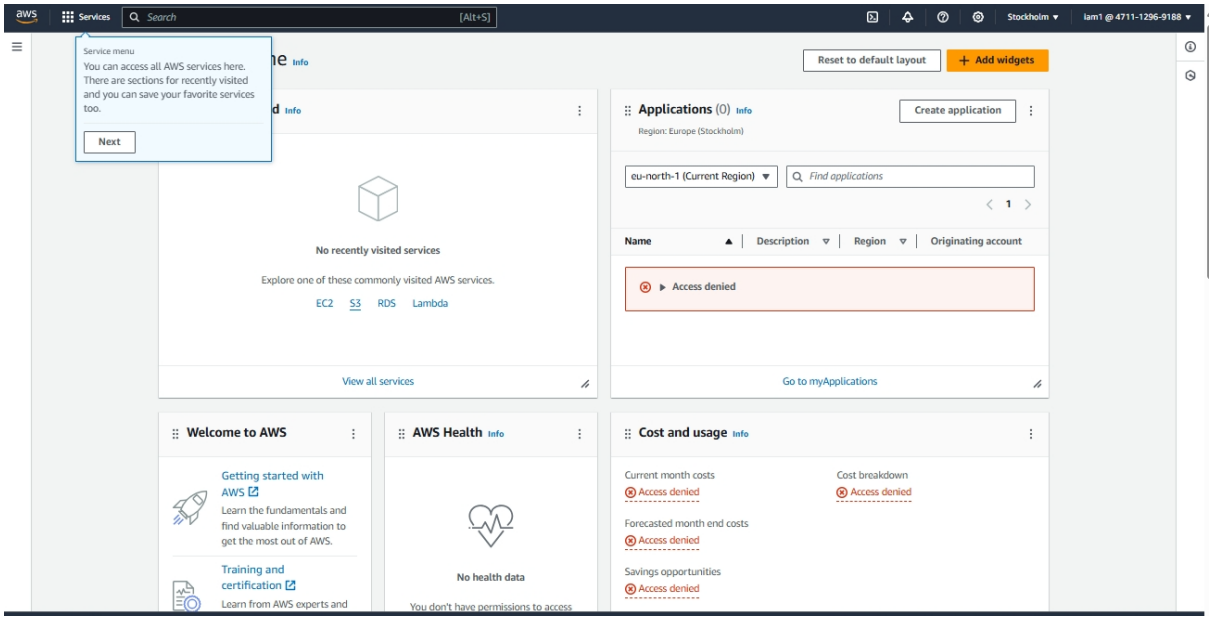
- Now, we should paste (or) type the username and password for signing-in. Here I have pasted the given link and signing in.



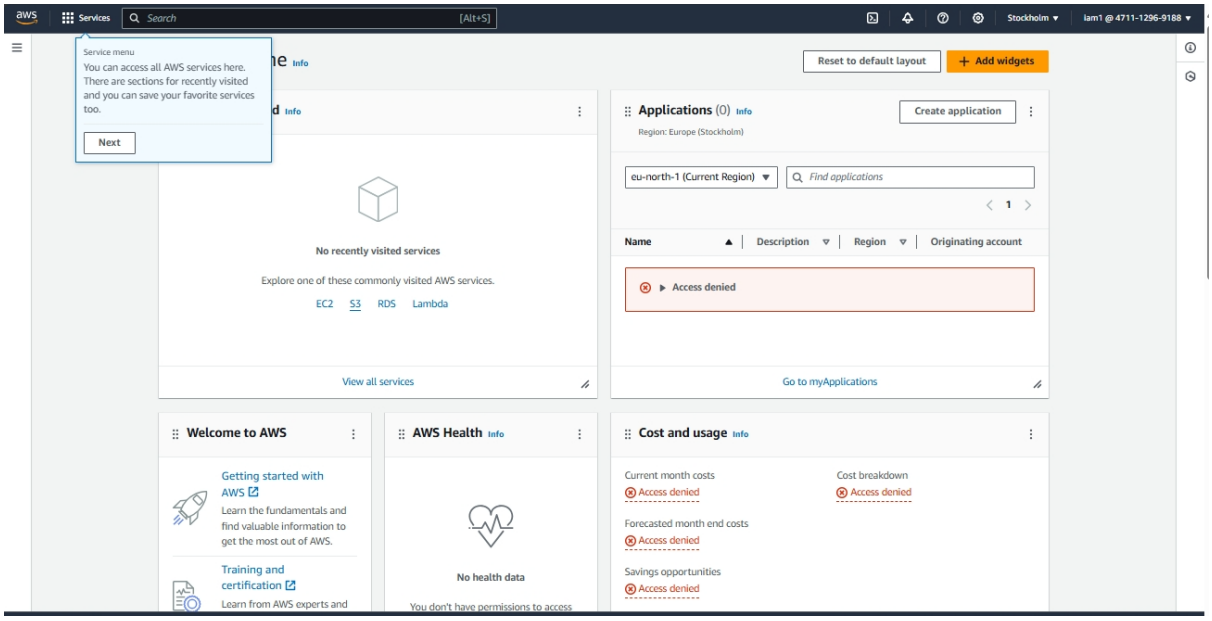
- Since, we pasted the link the "**Account ID**" will automatically get entered, if we to try sign-in directly from console we should type the Account ID manually.



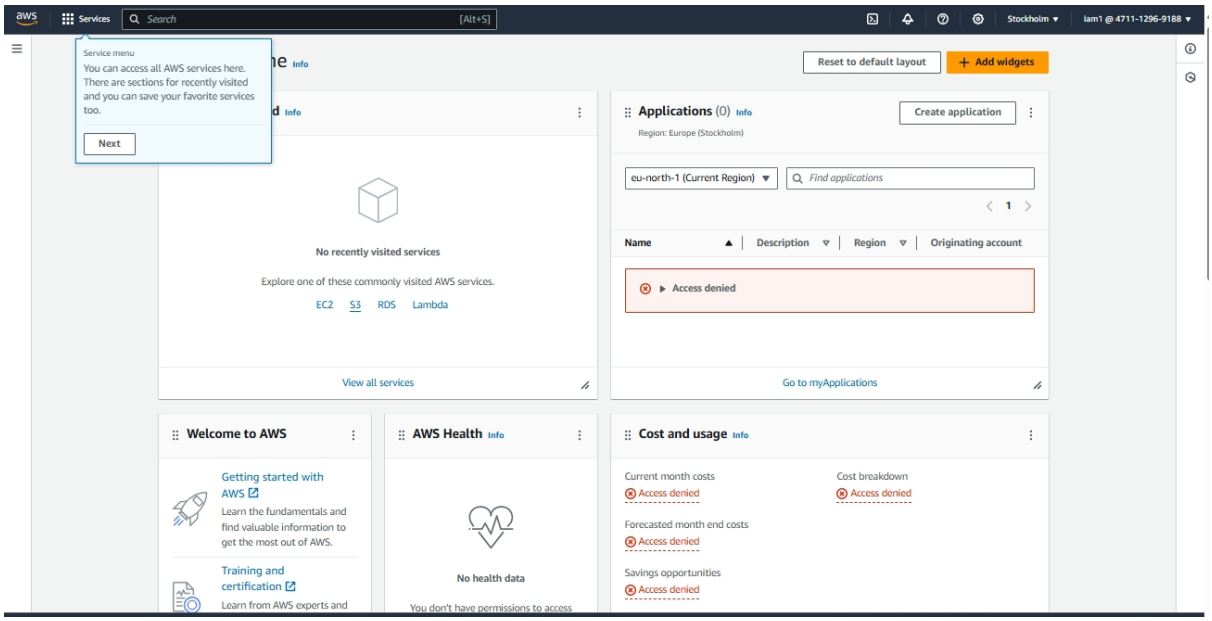
- After signing into the 1st IAM user account, this is the display page.



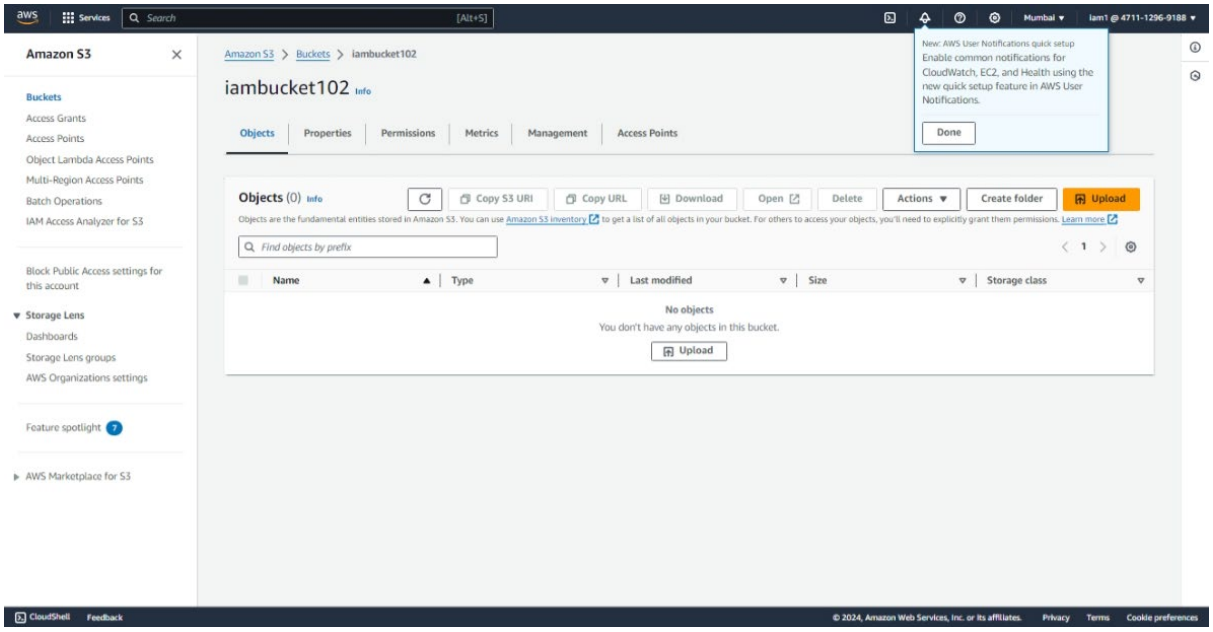
- It’s better and safe to change the region to our default “Asia Pacific (Mumbai)ap-south-1” Region.



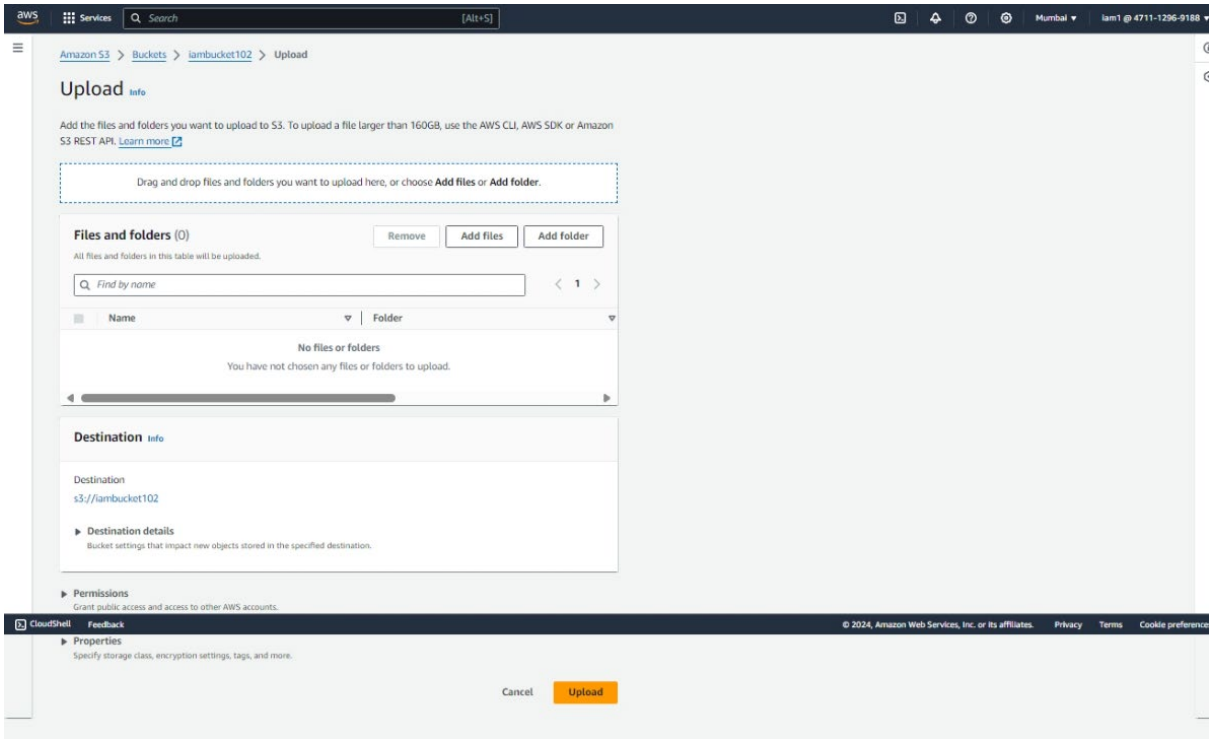
- Both buckets are visible from IAM user 1.

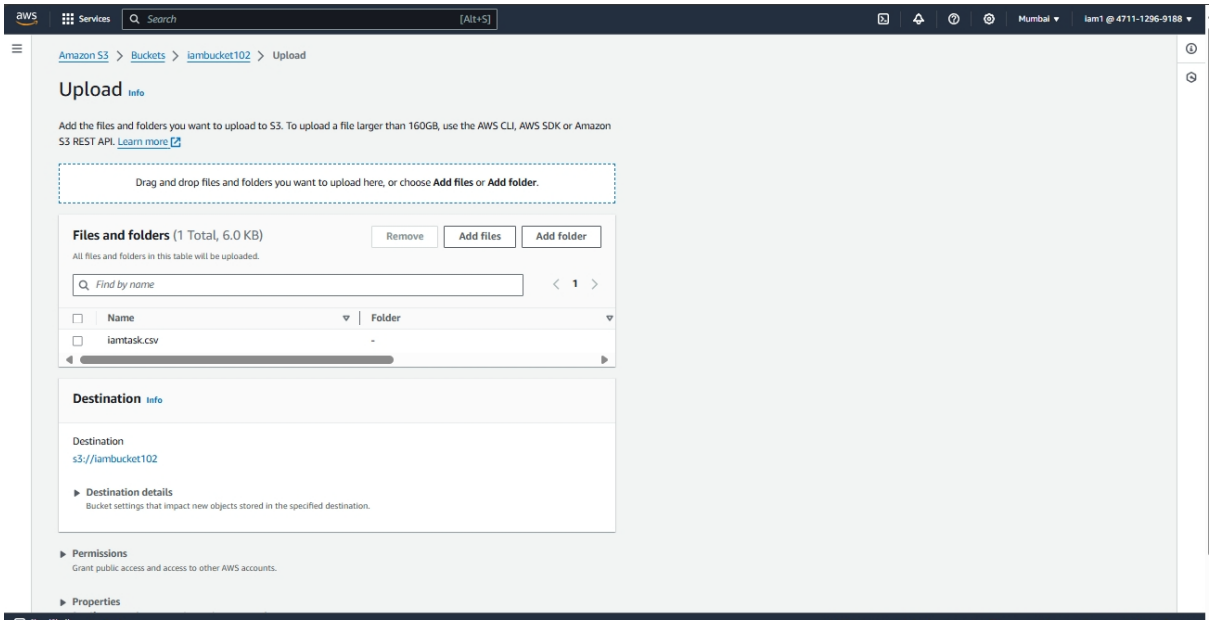


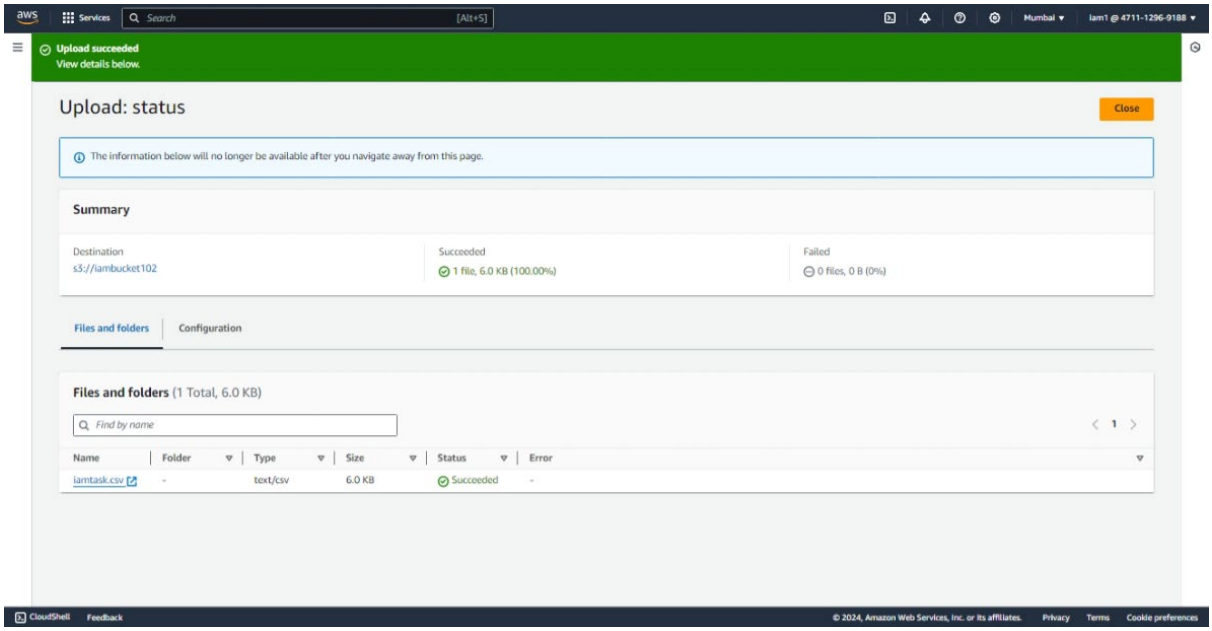
- Now let us upload a file into 1st bucket(iambucket102) from IAM user 1 and view it from IAM user 2.

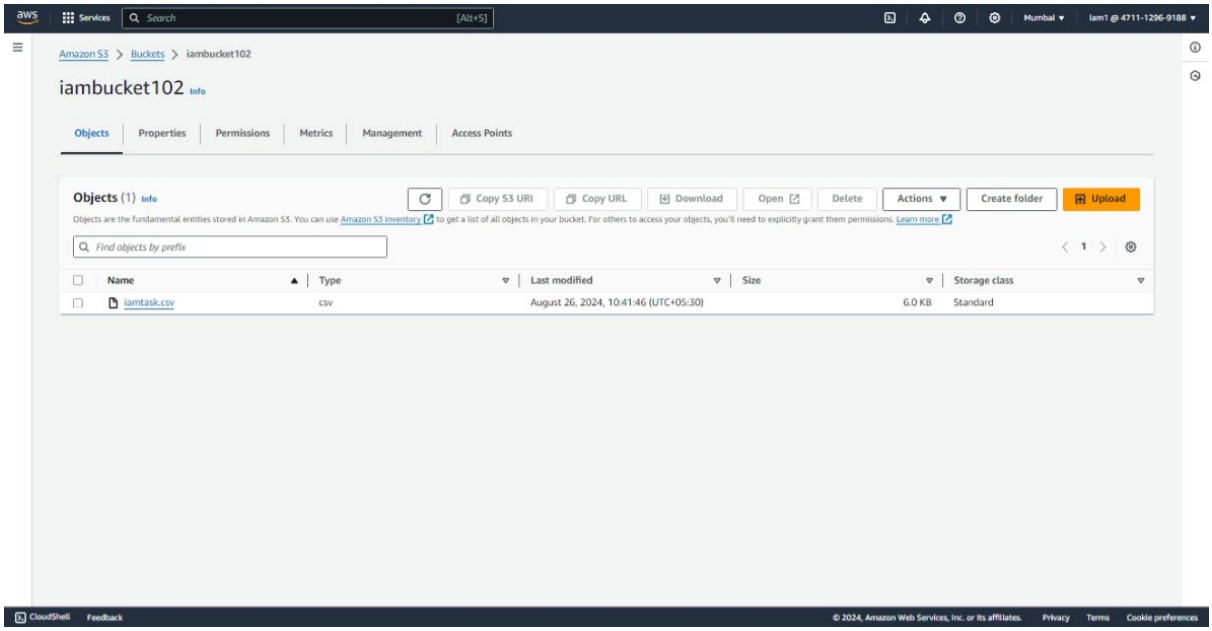


- After clicking Upload button, it is redirected to the below page:

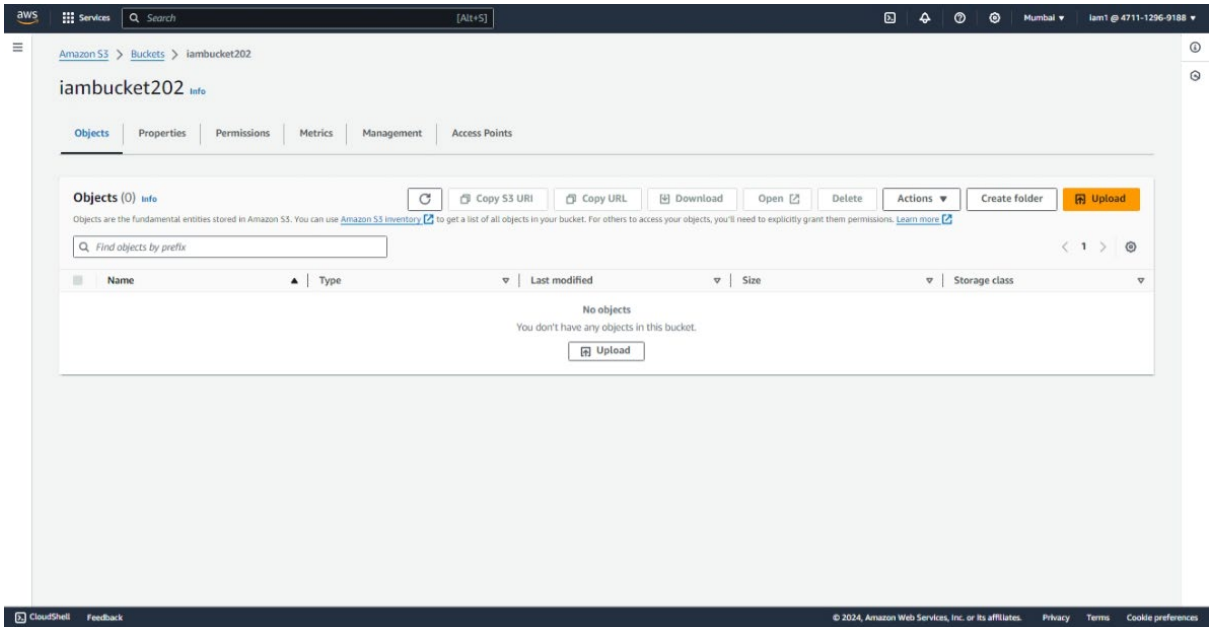


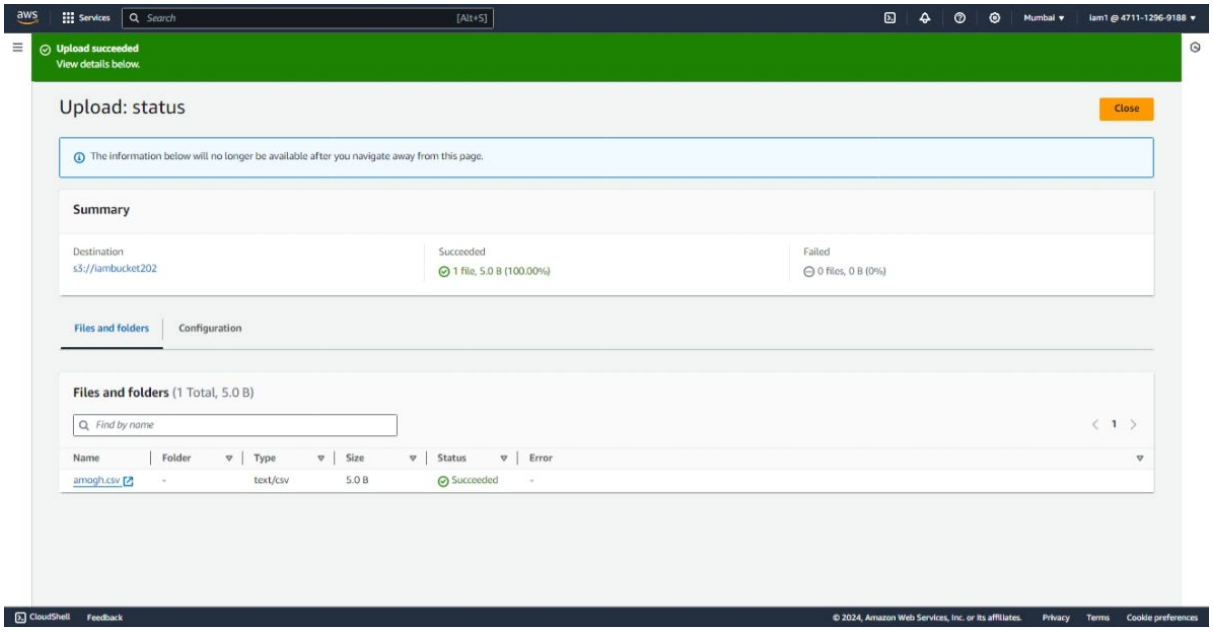

Services
Search
[Alt+S]
Mumbai
iam1 @ 4711-1296-9188
Amazon S3 > Buckets > iambucket102 > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 Total, 6.0 KB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
Name
Folder
iamtask.csv
-
Destination Info
Destination
s3://iambucket102
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Properties


Services
Search
[Alt+S]
Mumbai
iam1 @ 4711-1296-9188
Upload succeeded
View details below.
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://iambucket102
Succeeded
1 file, 6.0 KB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 Total, 6.0 KB)
Find by name
Name
Folder
Type
Size
Status
Error
iamtask.csv
-
text/csv
6.0 KB
Succeeded
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

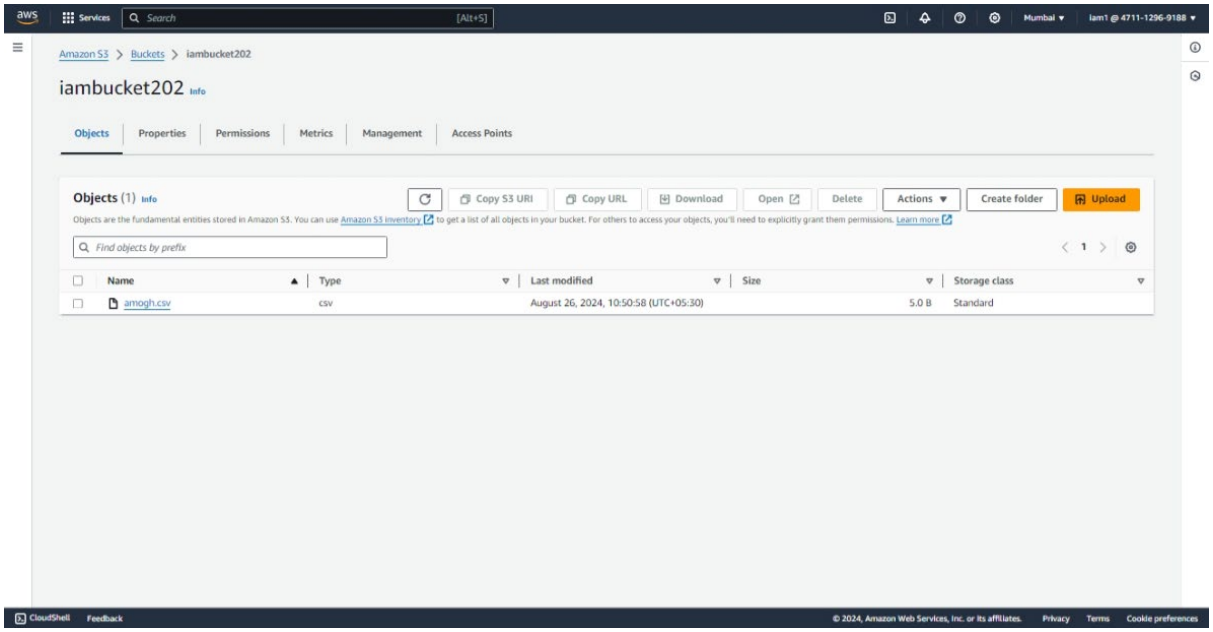

Services
Search
[Alt+S]
Mumbai
iam1 @ 4711-1296-9188
Amazon S3 > Buckets > iambucket102
iambucket102 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored 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
Name
Type
Last modified
Size
Storage class
iamtask.csv
csv
August 26, 2024, 10:41:46 (UTC+05:30)
6.0 KB
Standard
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

- Now let's upload another file to 2nd bucket using same procedure from 1st IAM user (iam1) only.

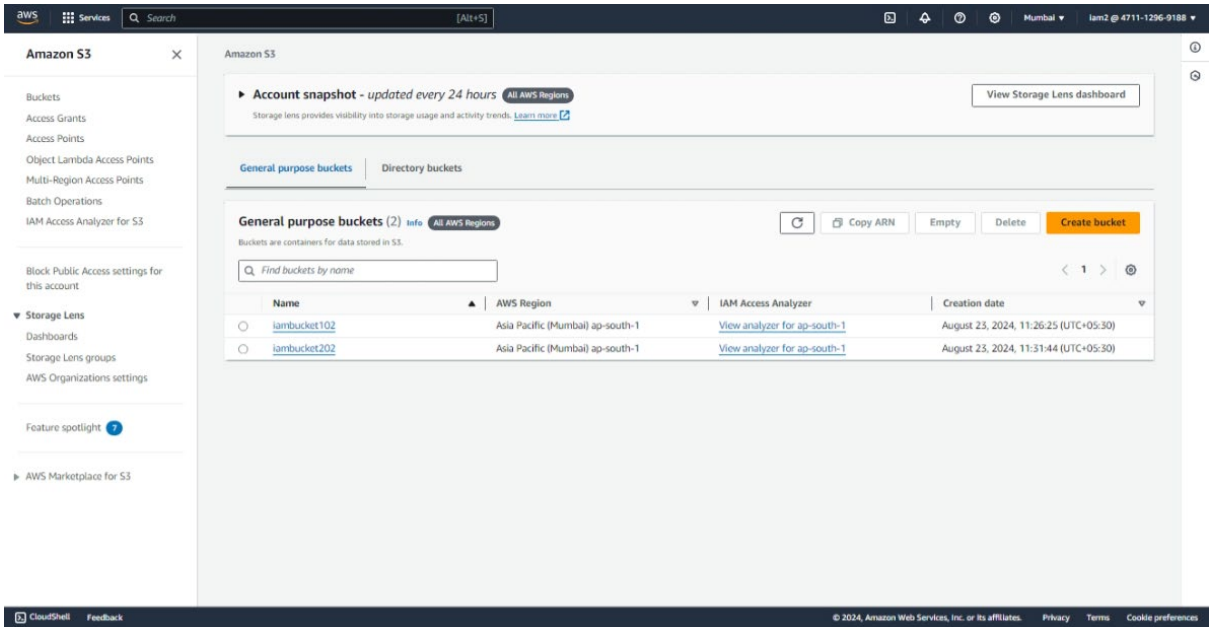




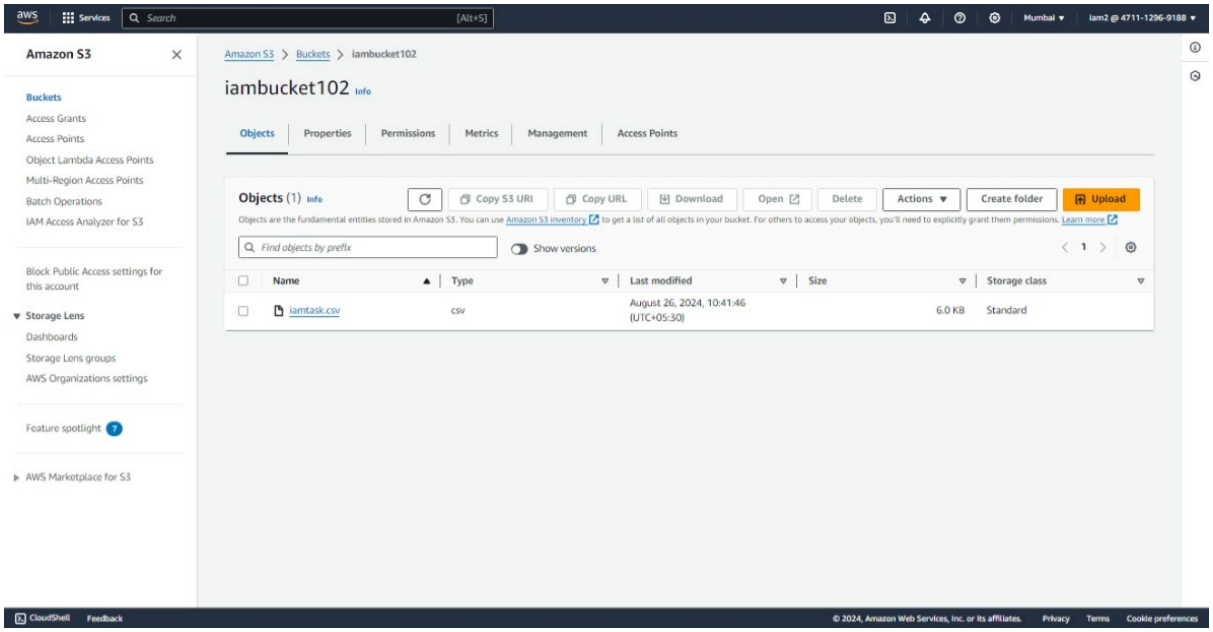
- Now we uploaded a different file into 2nd bucket (iambucket202).



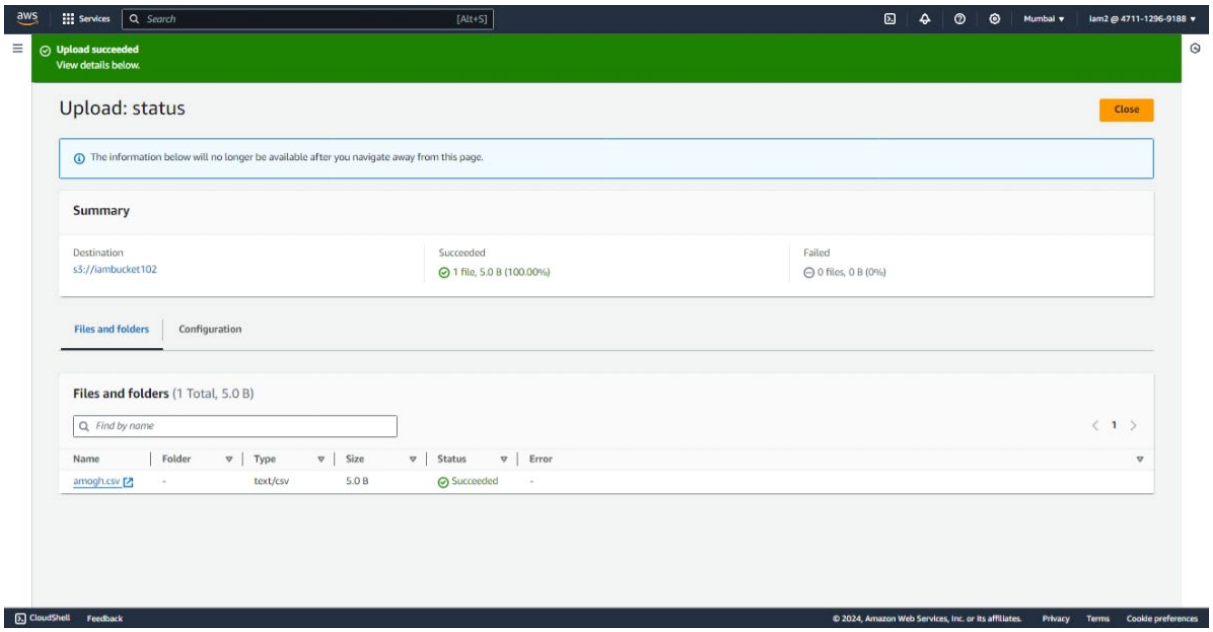
- We signed-in as iam2(IAM user 2) and we can see both buckets visible in S3 tab.



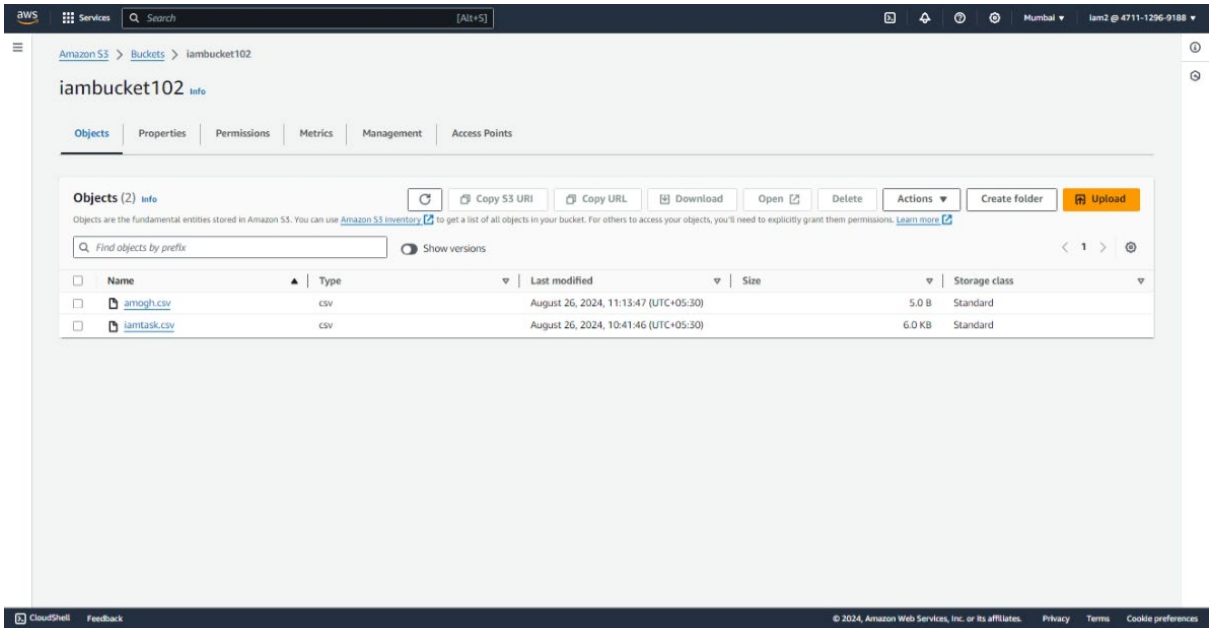
- We can view the file uploaded in 1st bucket too



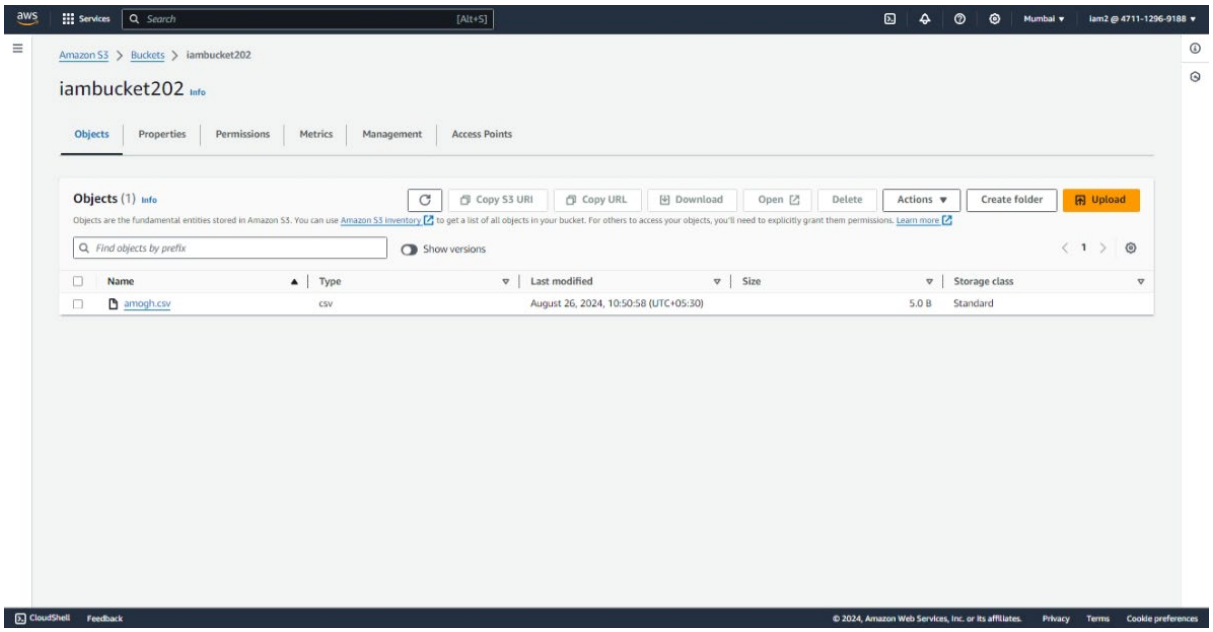
- Now let's upload a file into 1st bucket



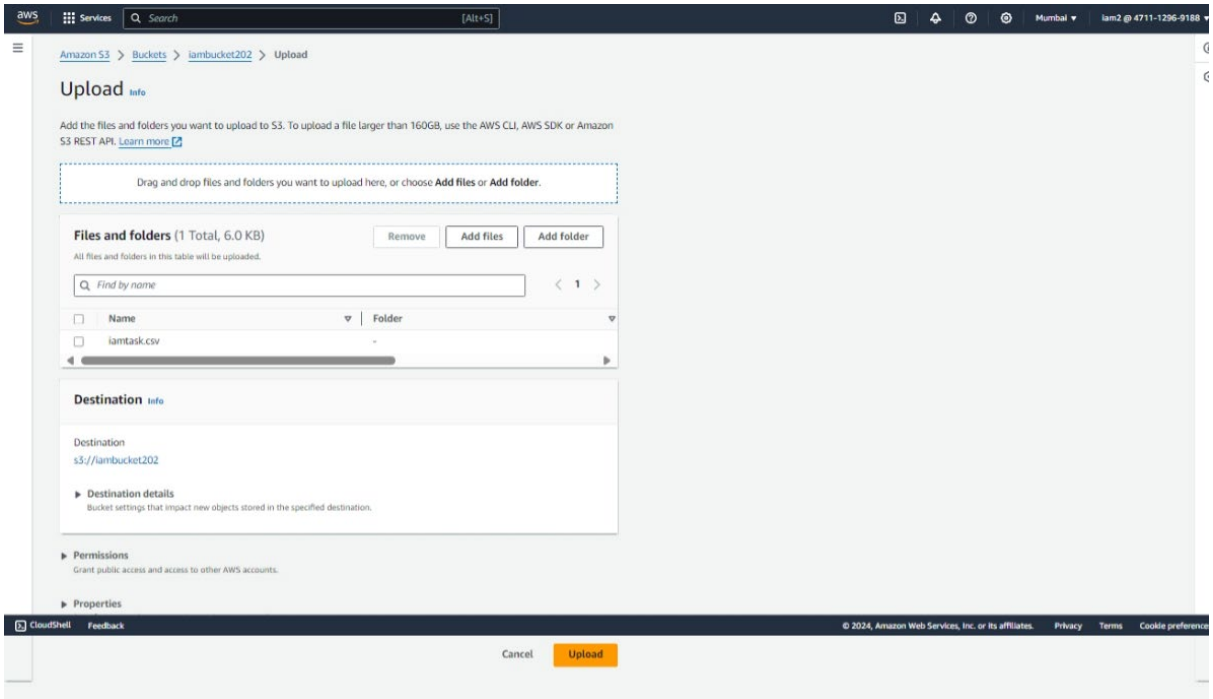
- File upload is successful.



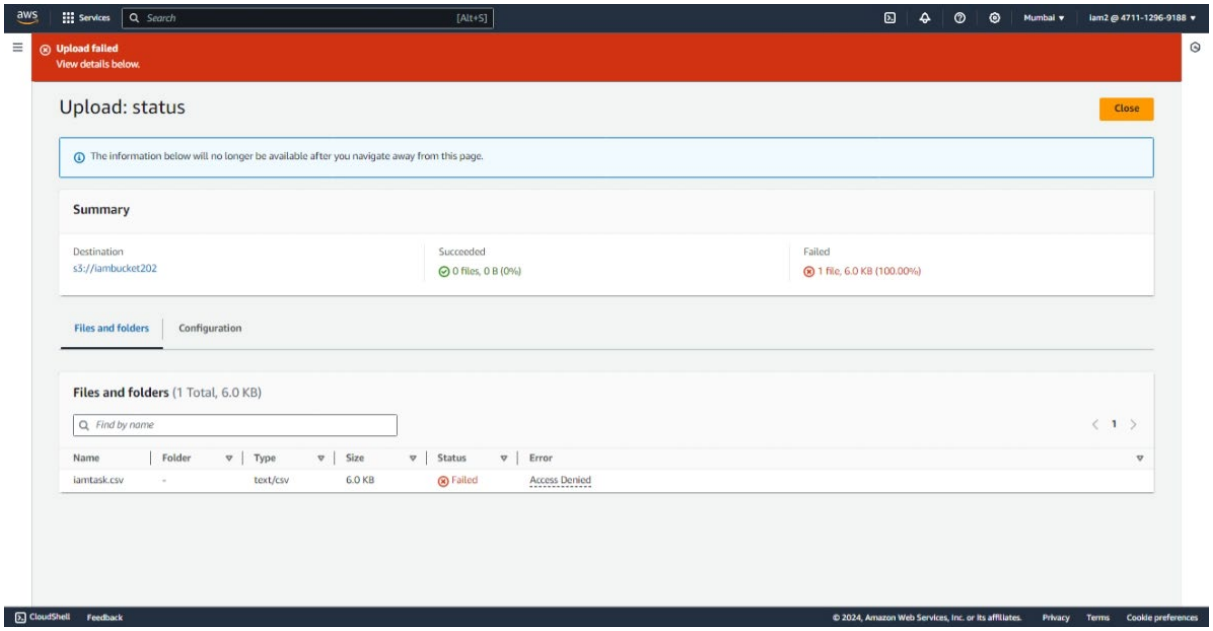
- Now we'll go to 2nd bucket



- In 2nd bucket, all objects are visible. Now we'll try to upload an object



- Hence, when an object is uploaded into iambucket202(2nd bucket) from IAM user 2(iam2), it is giving error.



- Object is not uploaded in 2nd bucket from iam2(2nd IAM user)