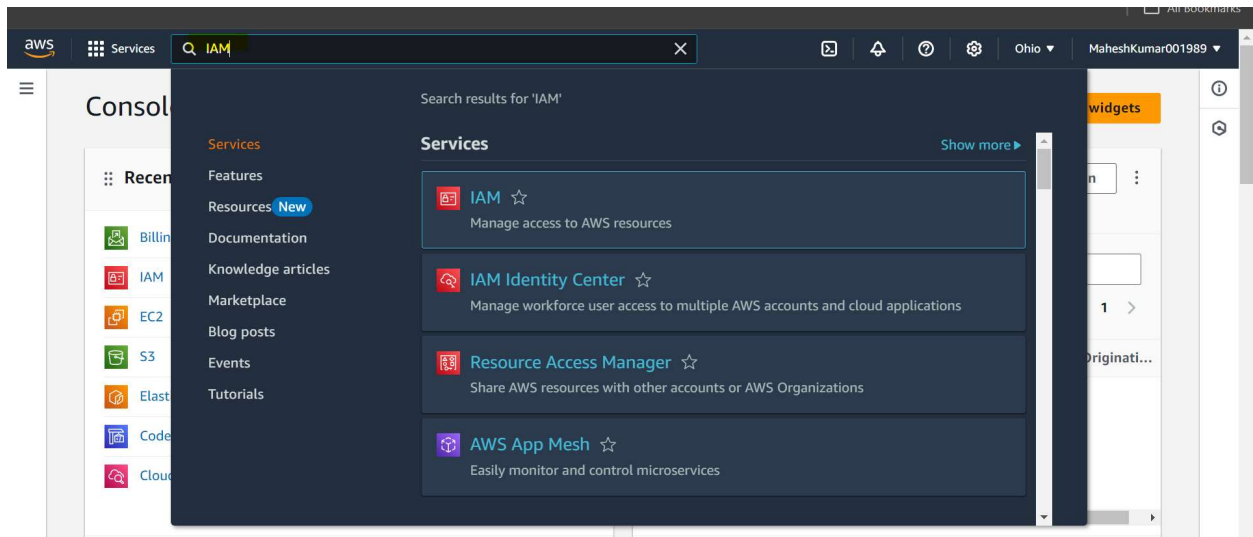
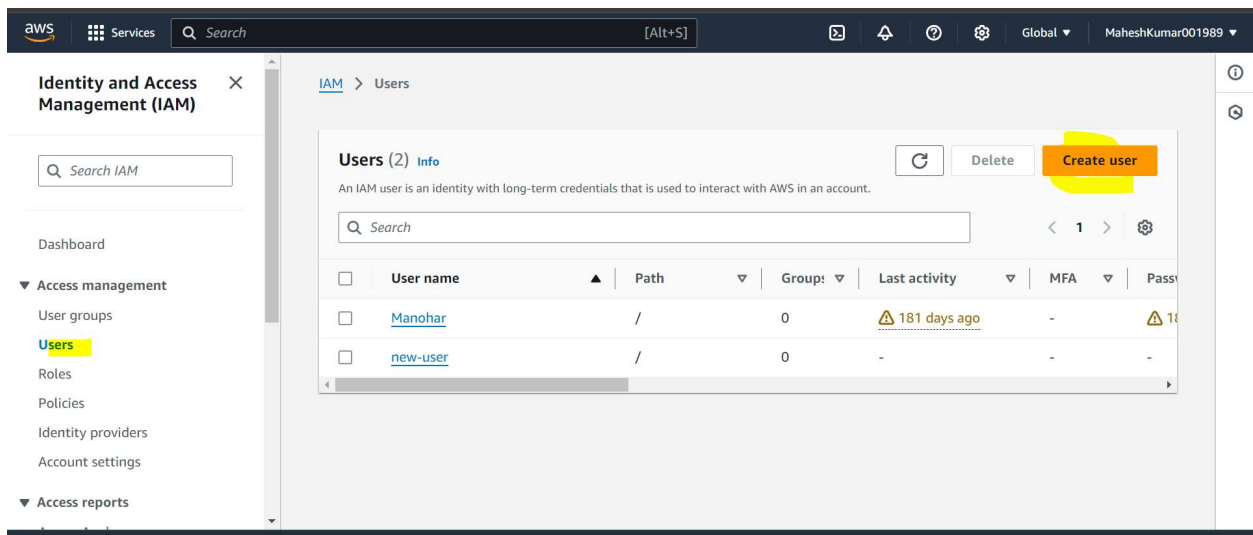


Create a IAM User

Login to aws console and search for IAM



Click on users and click on create a user



Give a name to your IAM user, check the box “provide user access to the aws management console” and select option I want to create an IAM user.

Specify user details

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

User details

User name
manohar
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, =, @, _ - (hyphen)

☒ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

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

We have option to create password so either you can create a custom password for your IAM user or choose option autogenerated password but for this time I choose option autogenerated password and click on next.

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.

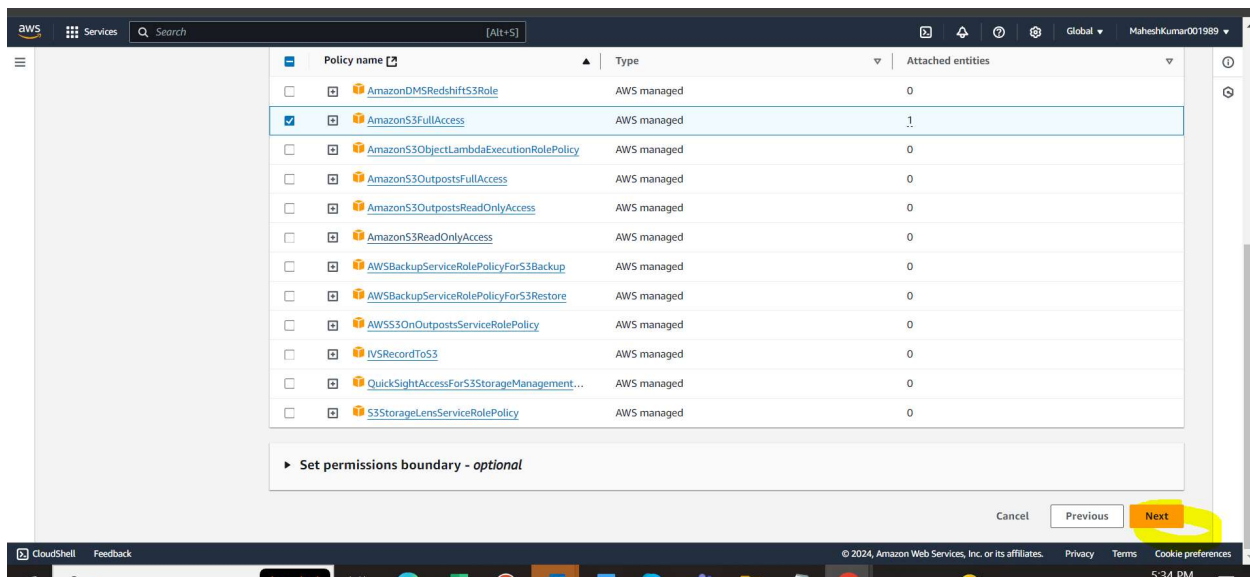
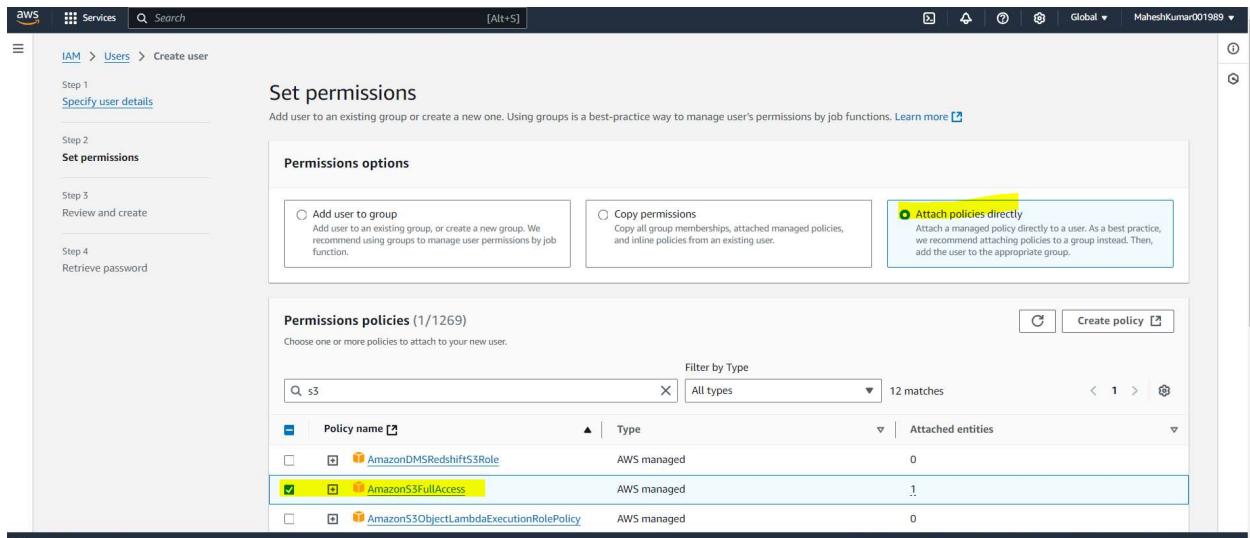
☐ Show password

☒ 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.

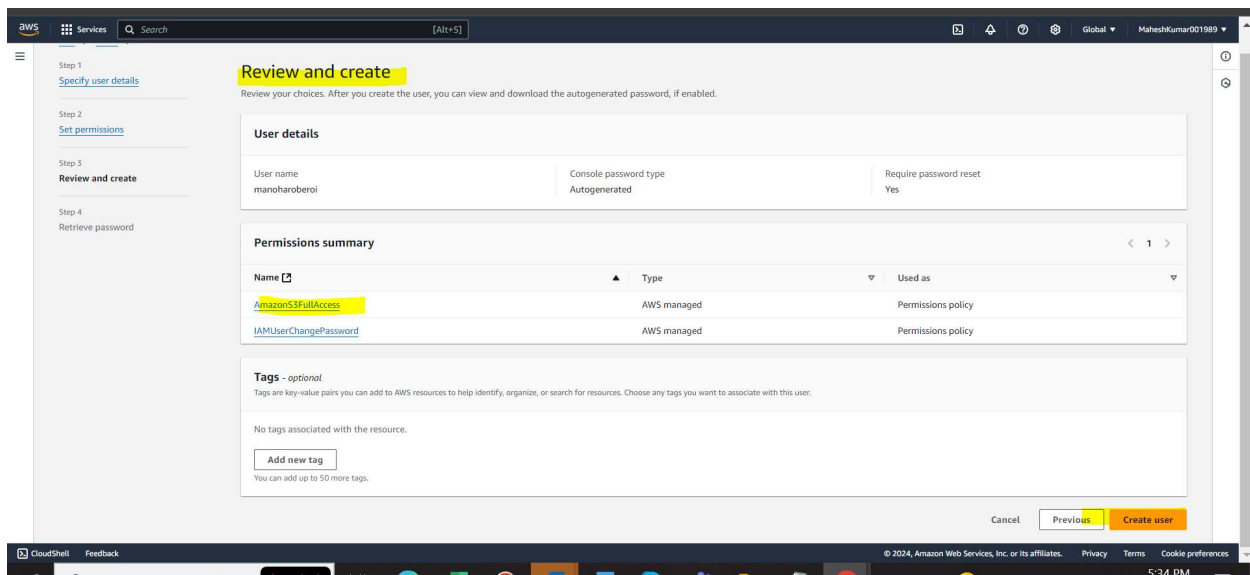
Next

In set permission we can give IAM user full access to the S3

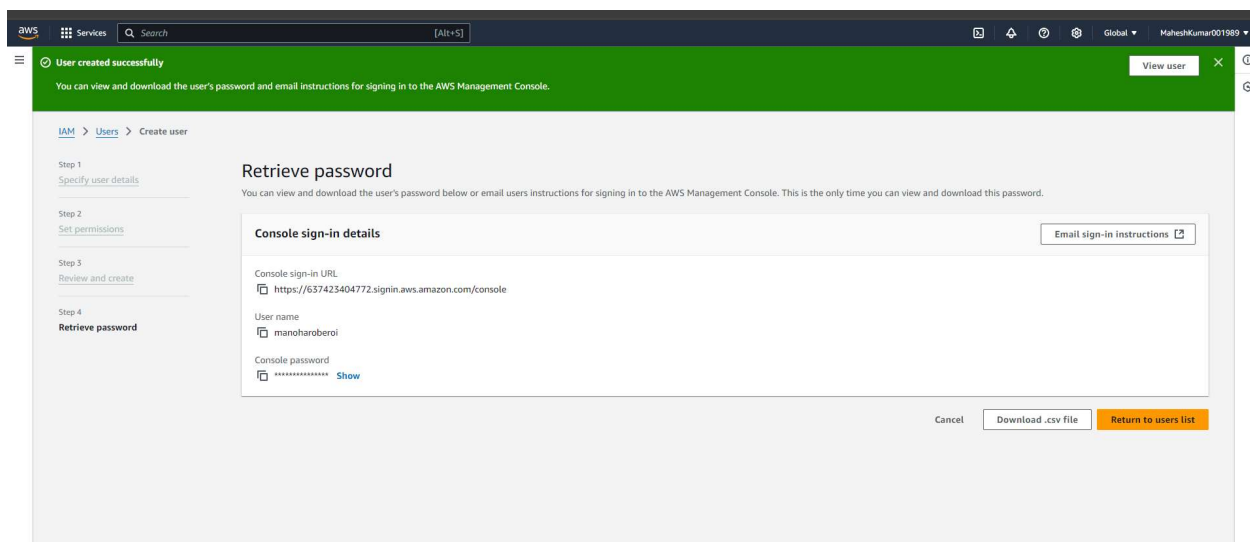
Note: S3 is simple storage.



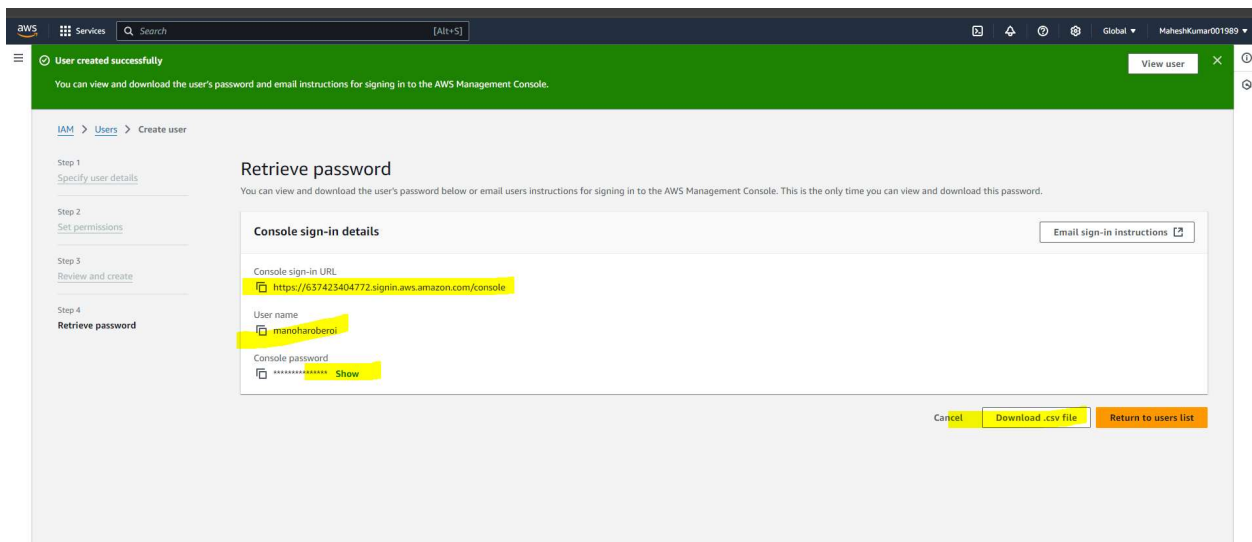
Click on create IAM user



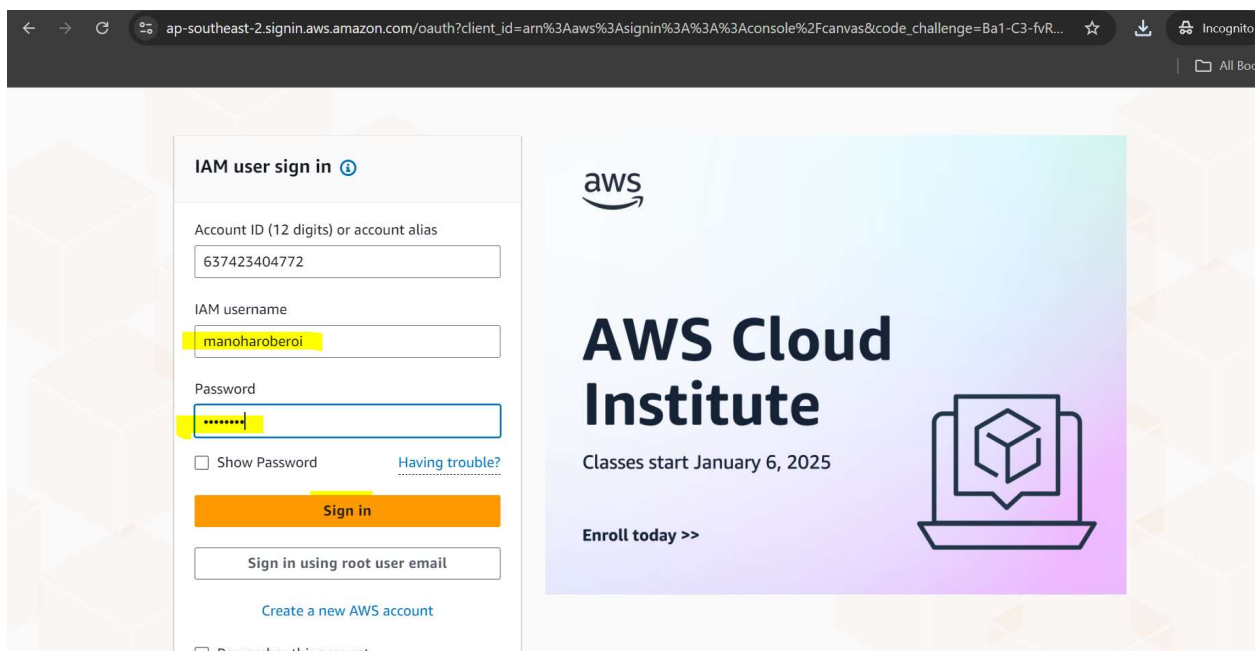
IAM user has been created successfully.



In a notepad you can copy the console URL, username and password or you can download the .csv file



Now we can copy the console URL and paste on the browser and sign in to aws console with a IAM user



Its asking to change the password so I will create a new password for my IAM user

← → ↻ ap-southeast-2.signin.aws.amazon.com/clm?action=changepassword&userType=iam&redirect_uri=https%3A%2F%2Fconsole.aws.amazon.co... ☆ ⬇ Incognito ⋮

aws

You must change your password to continue

AWS account 637423404772

IAM user name manoharoberoi

Old password

New password

Retype new password

Confirm password change

[Sign in using root user email](#)

← → ↻ ap-southeast-2.signin.aws.amazon.com/clm?action=changepassword&userType=iam&redirect_uri=https%3A%2F%2Fconsole.aws.amazon.co... ☆ ⬇ Incognito ⋮

aws

You must change your password to continue

AWS account 637423404772

IAM user name manoharoberoi

Old password

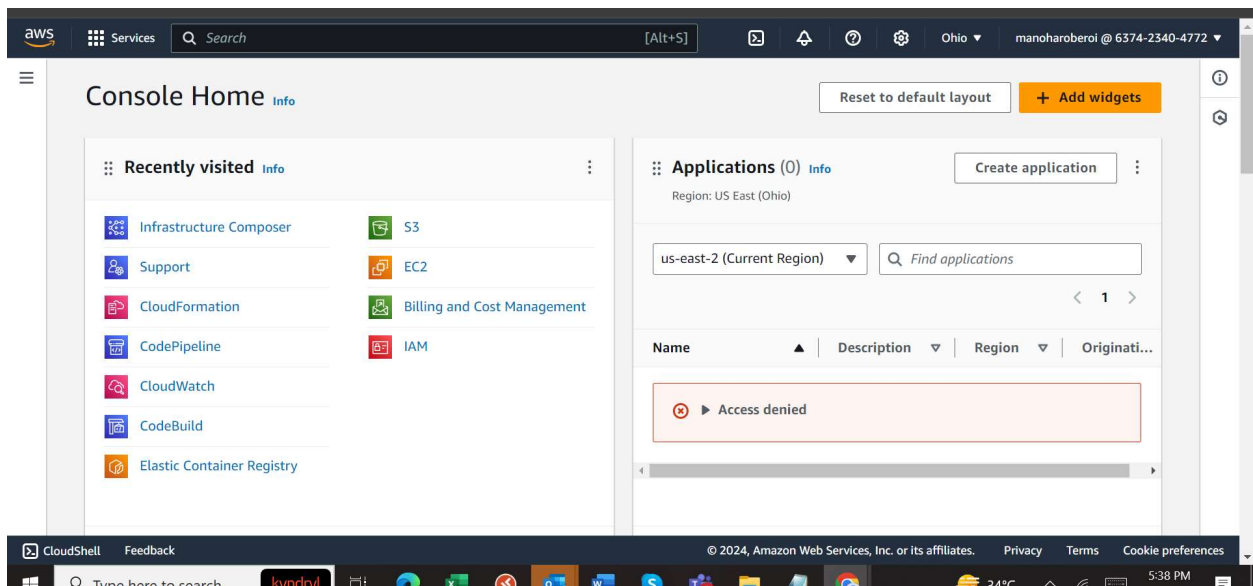
New password

Retype new password

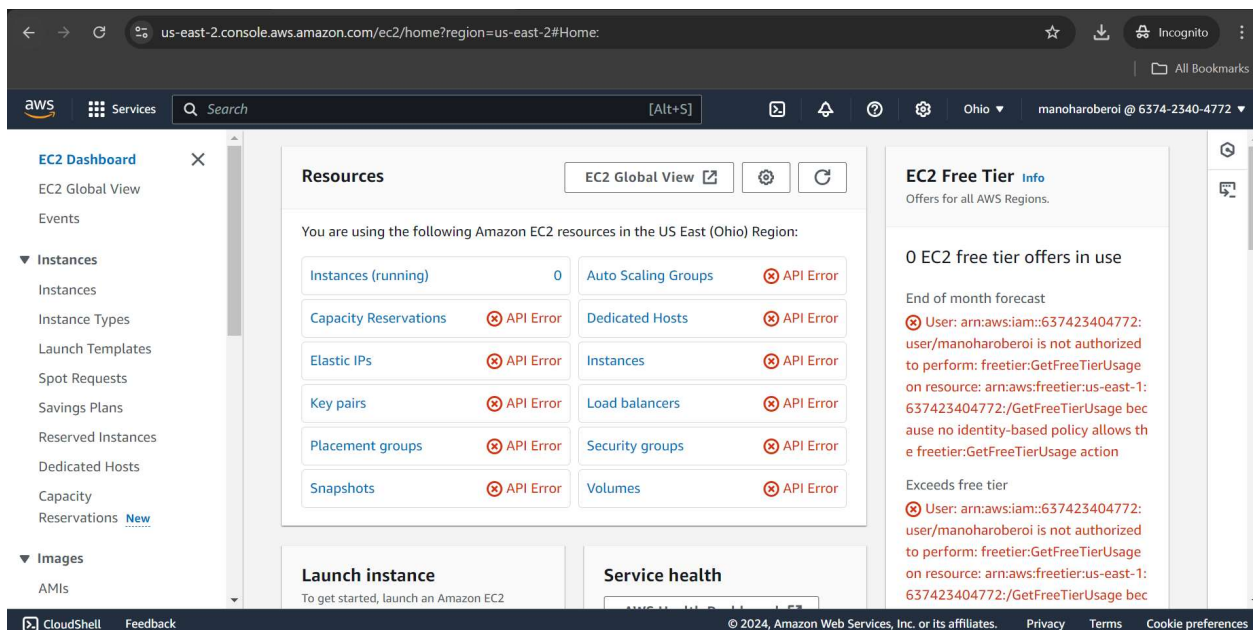
Confirm password change

[Sign in using root user email](#)

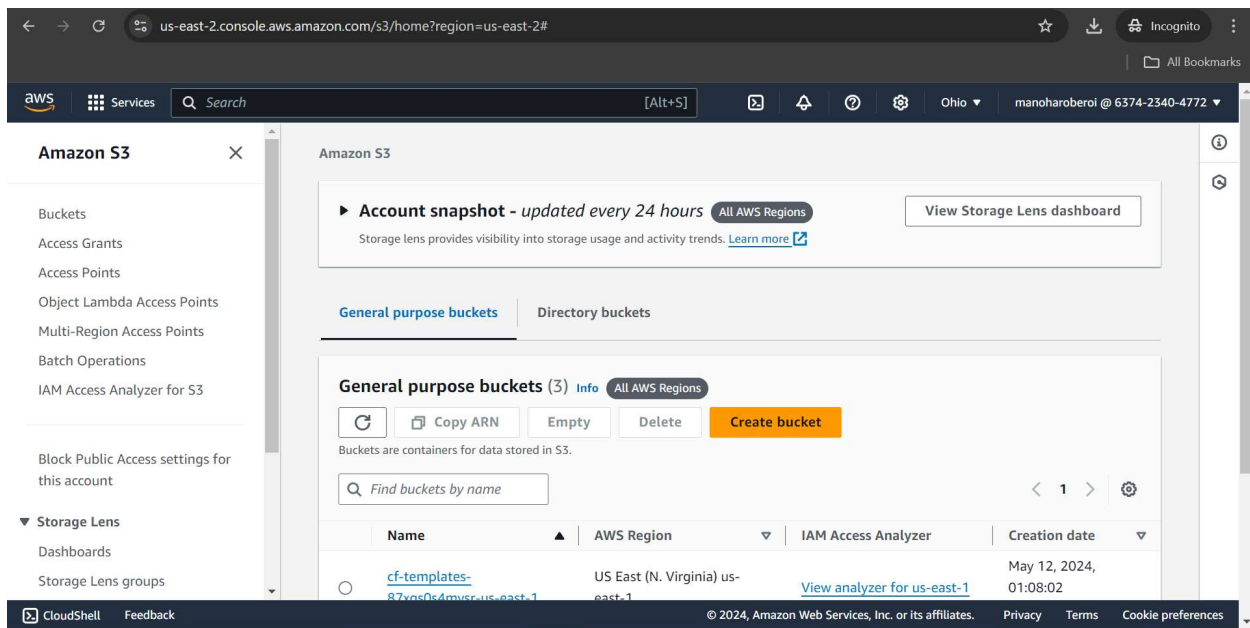
Successfully logged in to aws console with a IAM user



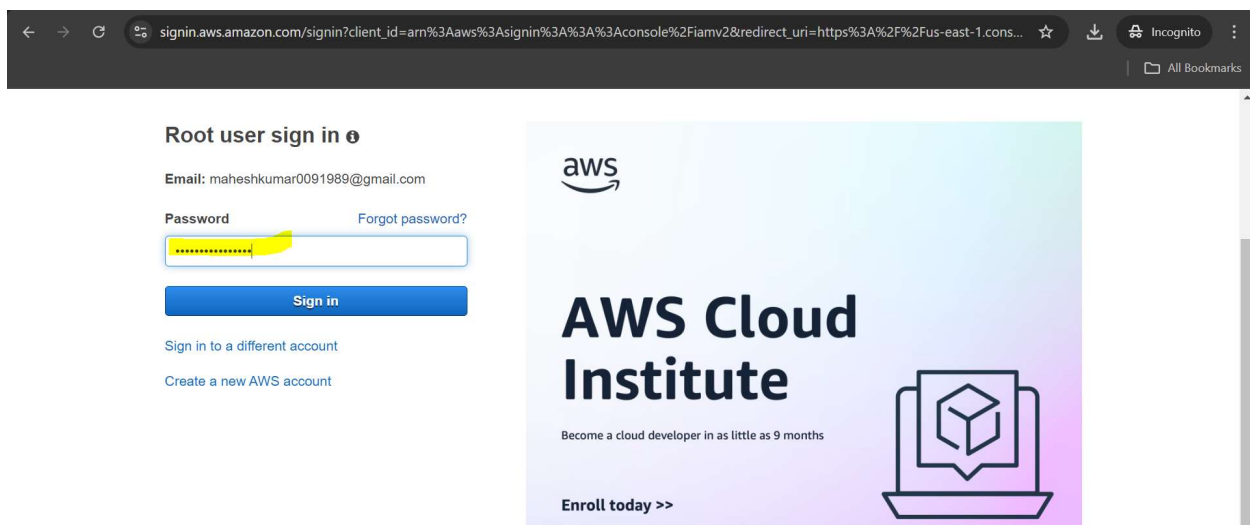
Search for EC2 but I am getting API error becoz to this IAM user I have only given the s3 full access but not the EC2 full access so I am getting this error.



I will search for s3 and I am not getting any api error.



If I want I can give my IAM user ec2 full access. So I will logout from the IAM user and I will login to aws console with my root user account and add ec2 full access permissions to my IAM user



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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 > Users

Users (3) Info

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

Search

Refresh

Delete

Create user

< 1 >

⚙

<input type="checkbox"/>	User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age
<input type="checkbox"/>	Manohar	/	0	181 days ago	-	181 days	-	Active - AKIAZ1ZLF35...	181 days
<input type="checkbox"/>	manoharoberoi	/	0	5 minutes ago	-	4 minutes	October 20, 2024, 17:...	-	-
<input type="checkbox"/>	new-user	/	0	-	-	-	-	-	-

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

5:13 PM

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

manoharoberoi Info

Delete

Summary

ARN

arn:aws:iam::637423404772:user/manoharoberoi

Console access

Enabled without MFA

Access key 1

Create access key

Created

October 20, 2024, 17:34 (UTC+05:30)

Last console sign-in

Today

Permissions

Groups

Tags

Security credentials

Last Accessed

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

Refresh

Remove

Add permissions

Search

Filter by Type

All types

< 1 >

⚙

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	AmazonSSFullAccess	AWS managed	Directly
<input type="checkbox"/>	IAMUserChangePassword	AWS managed	Directly

▶ Permissions boundary (not set)

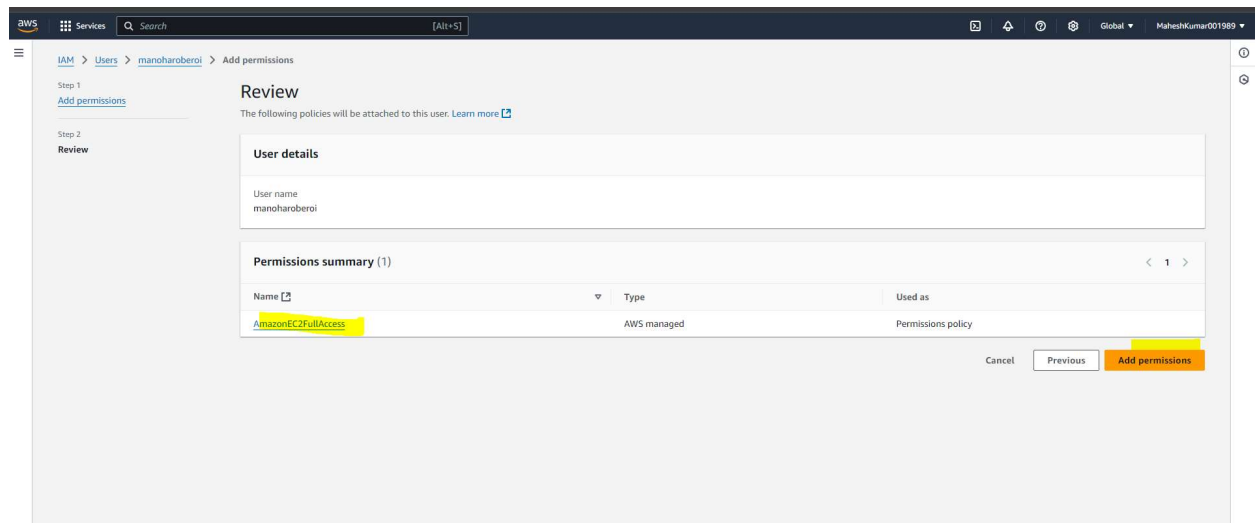
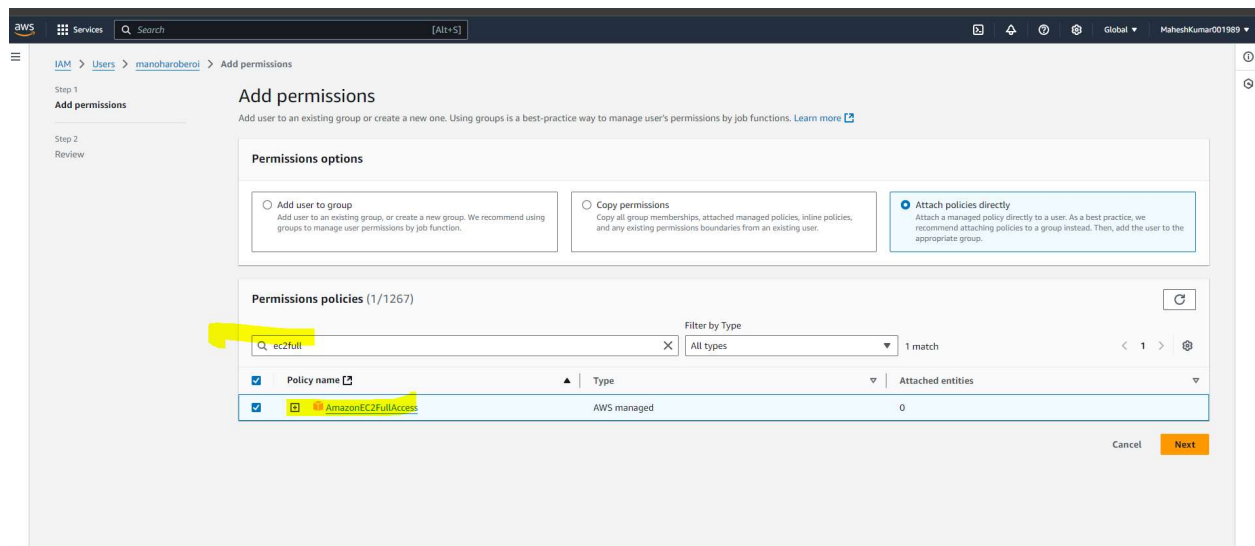
CloudShell

Feedback

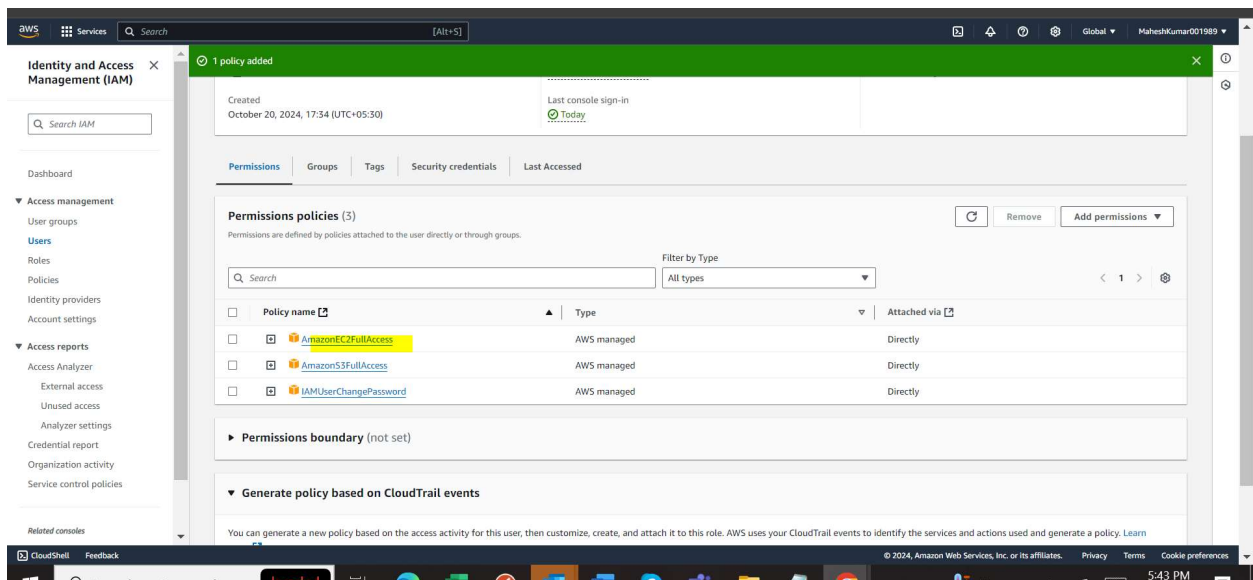
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

5:43 PM

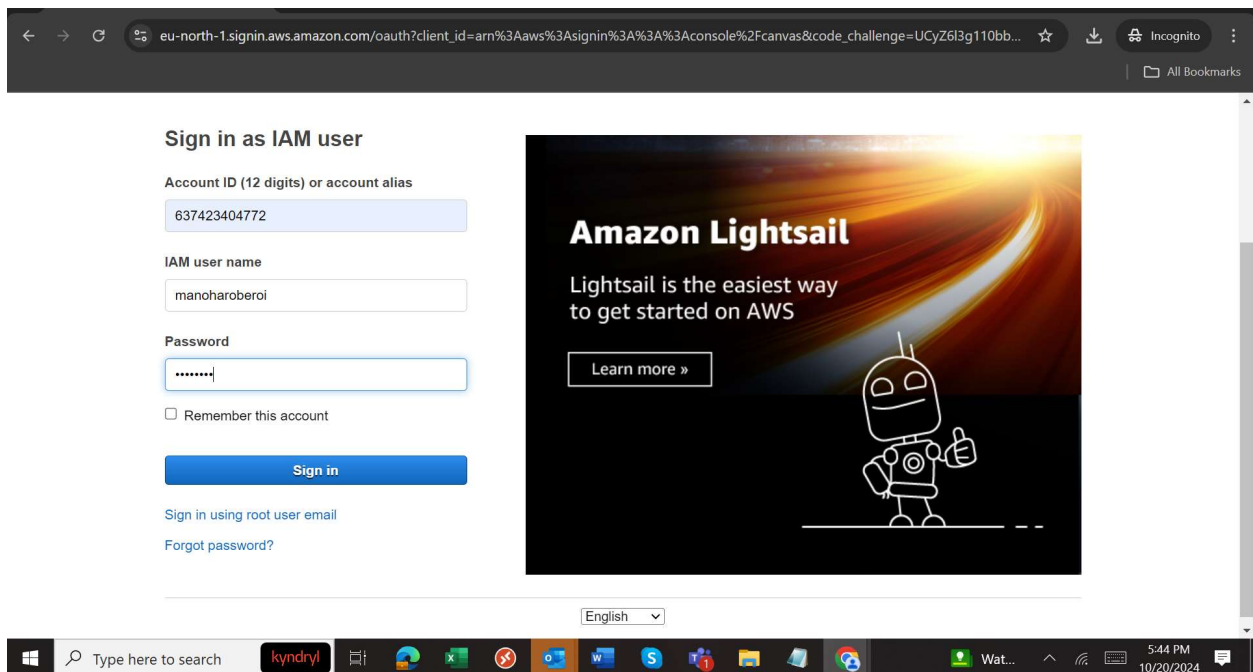
10/20/2024



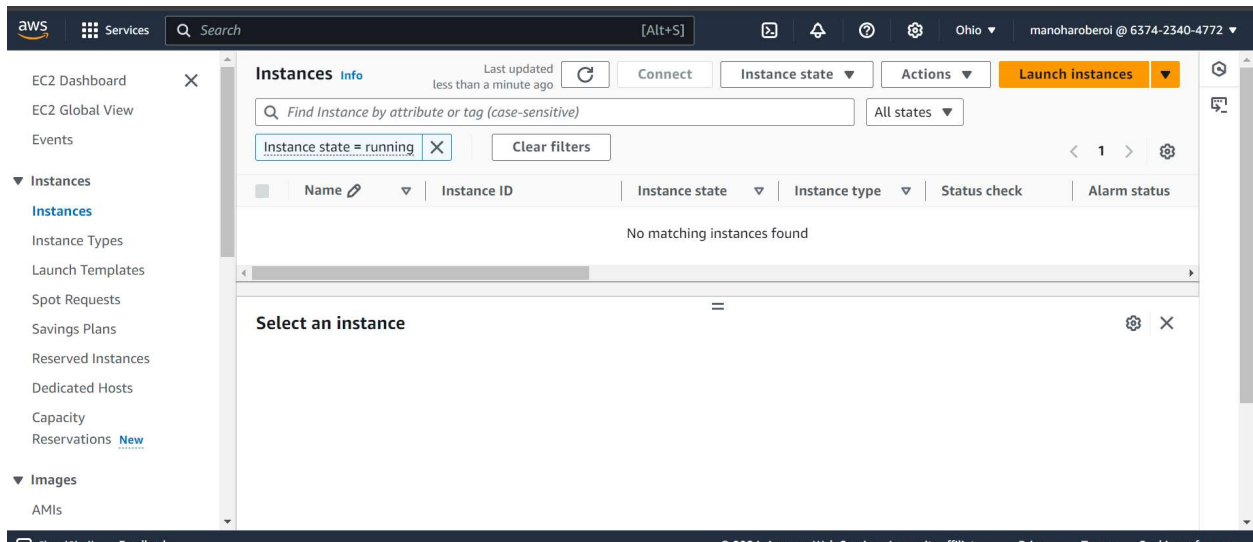
Successfully added ec2 full access permission to my IAM user



I will again login to aws console with my IAM user.



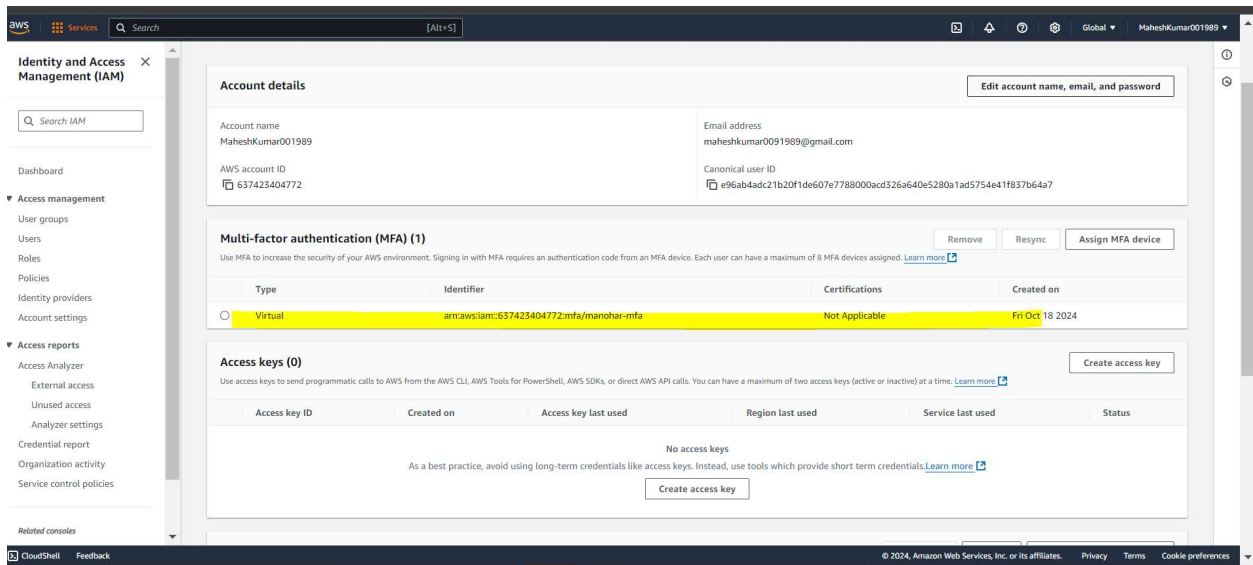
This time when I search for ec2 I am not seeing the API error.



Note: In cloud trial we can check which user has done which changes.

Note: IAM Role we can also create suppose if we want to integrate jenkins with s3 so for s3 we can create a role and give full ec2 permission to our s3 bucket so for that we need to create a role.

MFA already enabled for the root user account.



Create a S3 bucket- search for s3 and click on create a bucket

Amazon S3

Account snapshot - updated every 24 hours [View Storage Lens dashboard](#)

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets | Directory buckets

General purpose buckets (3) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

[Find buckets by name](#)

[Create bucket](#)

Name	AWS Region	IAM Access Analyzer	Creation date
cf-templates-87xgs0s4myar-us-east-1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	May 12, 2024, 01:08:02 (UTC+05:30)
elasticbeanstalk-ap-southeast-1-637423404772	Asia Pacific (Singapore) ap-southeast-1	View analyzer for ap-southeast-1	March 31, 2024, 15:09:41 (UTC+05:30)
elasticbeanstalk-us-east-1-637423404772	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 13, 2024, 18:31:48 (UTC+05:30)

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3.

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**
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](#)
manoharbucket209

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

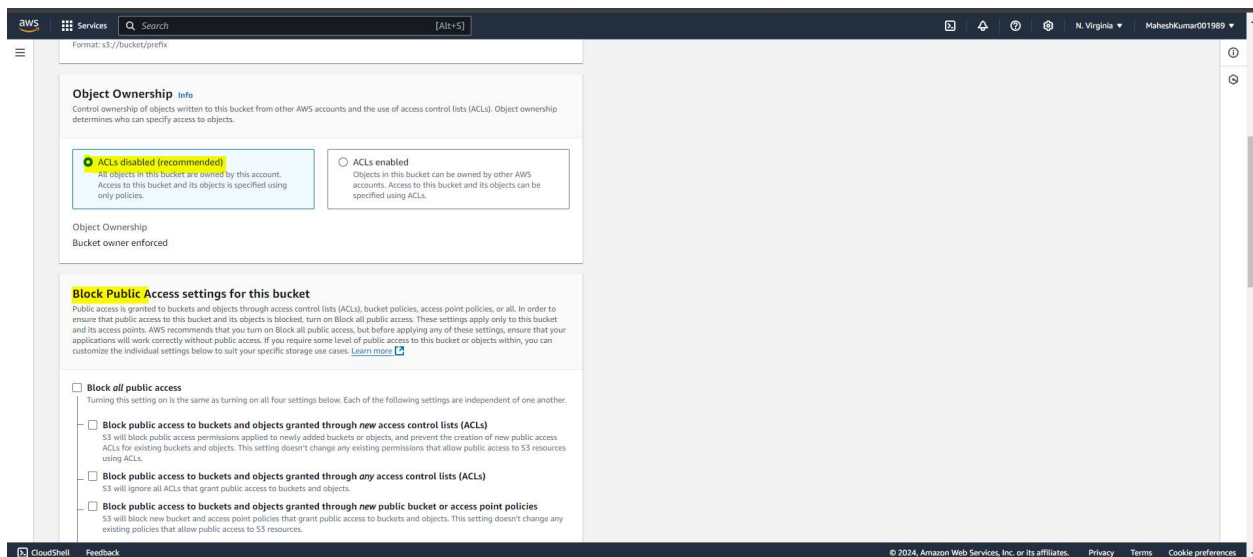
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

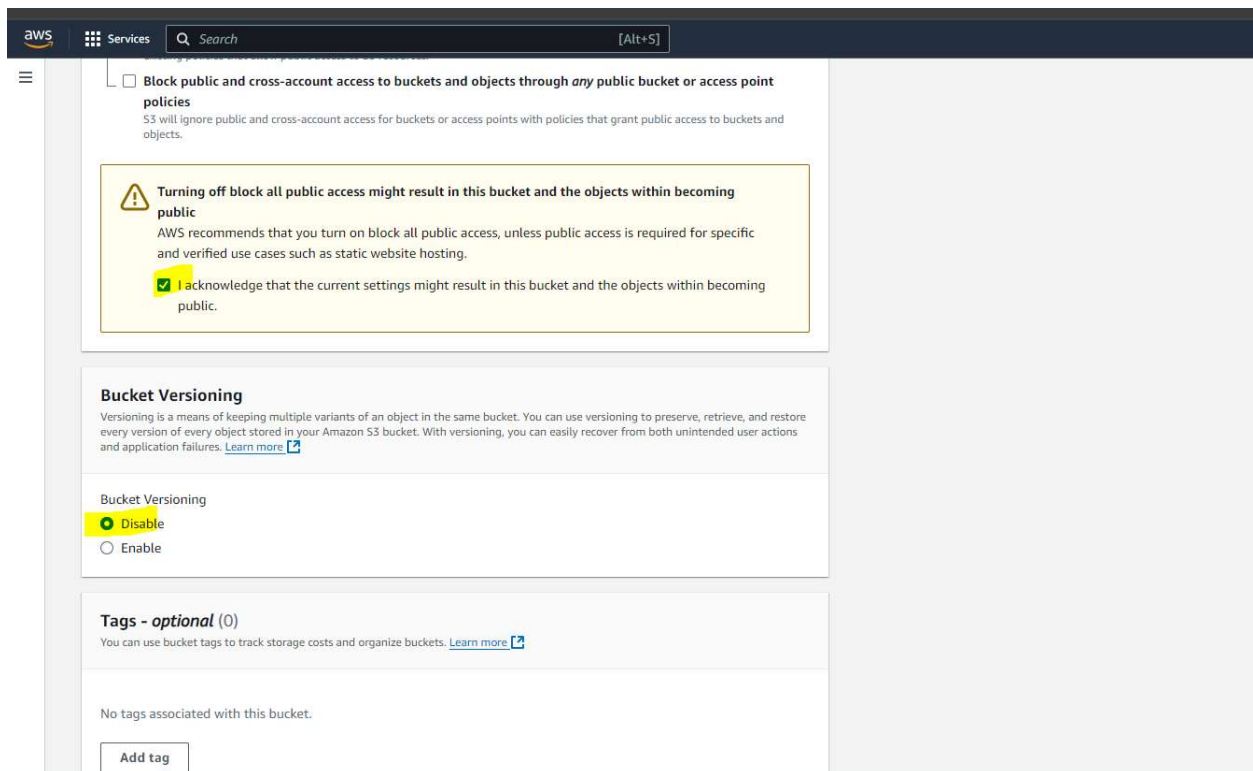
Format: s3://bucket/prefix

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.

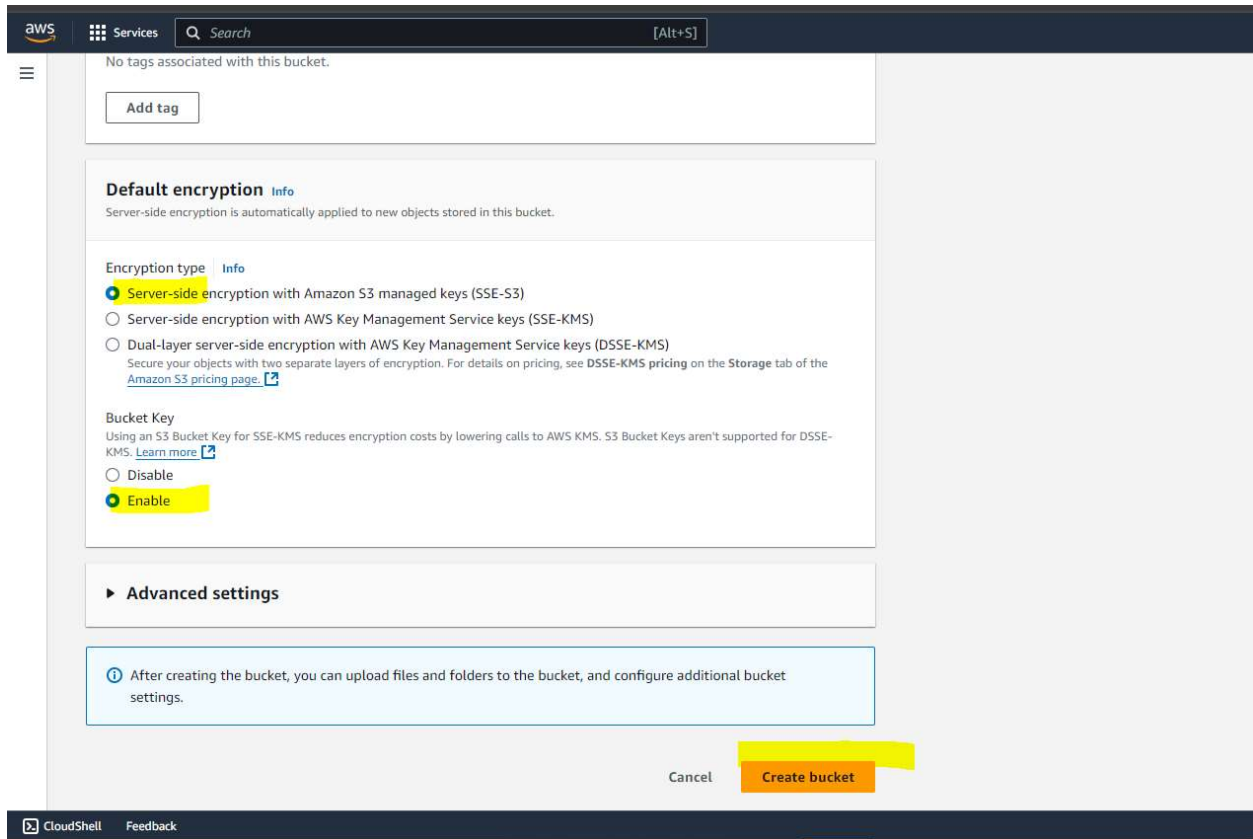
ACL disabled (recommended) an enable public access



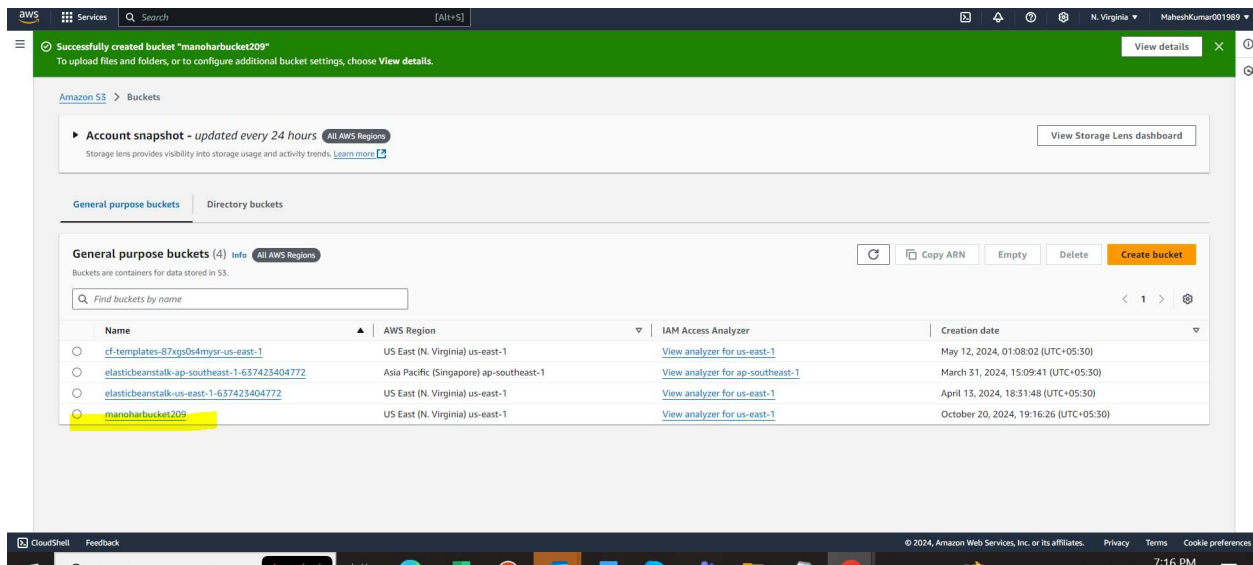
Versioning- disabled



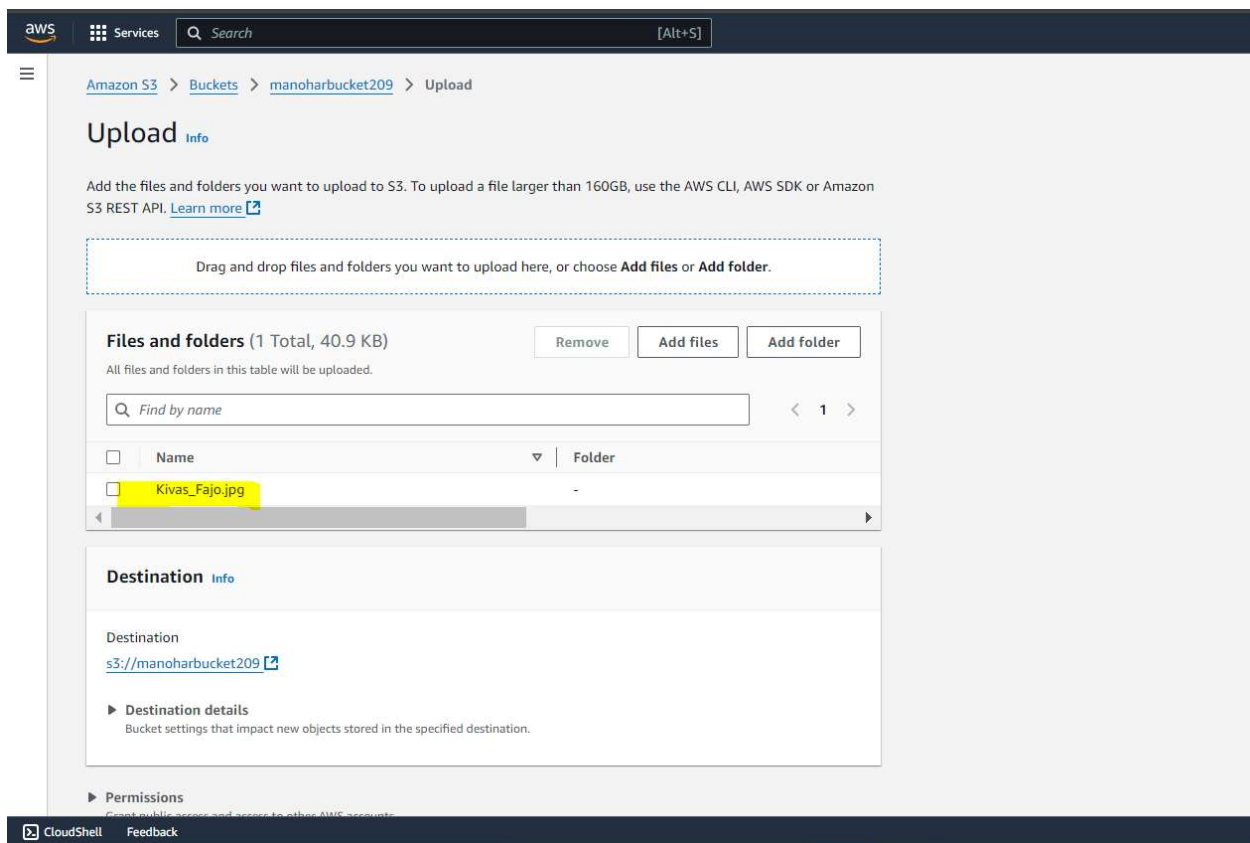
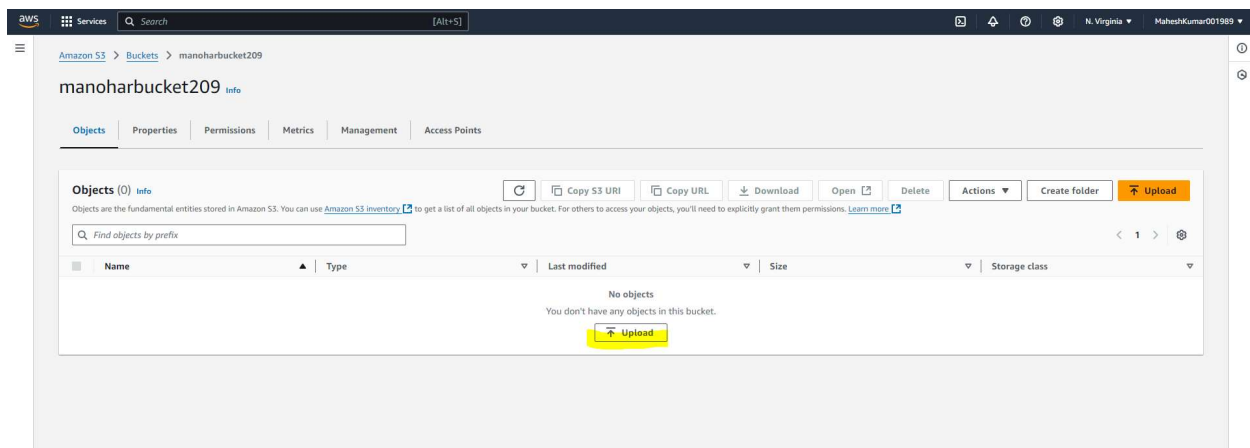
Server side encryption enabled and bucket key enabled and click on create bucket.



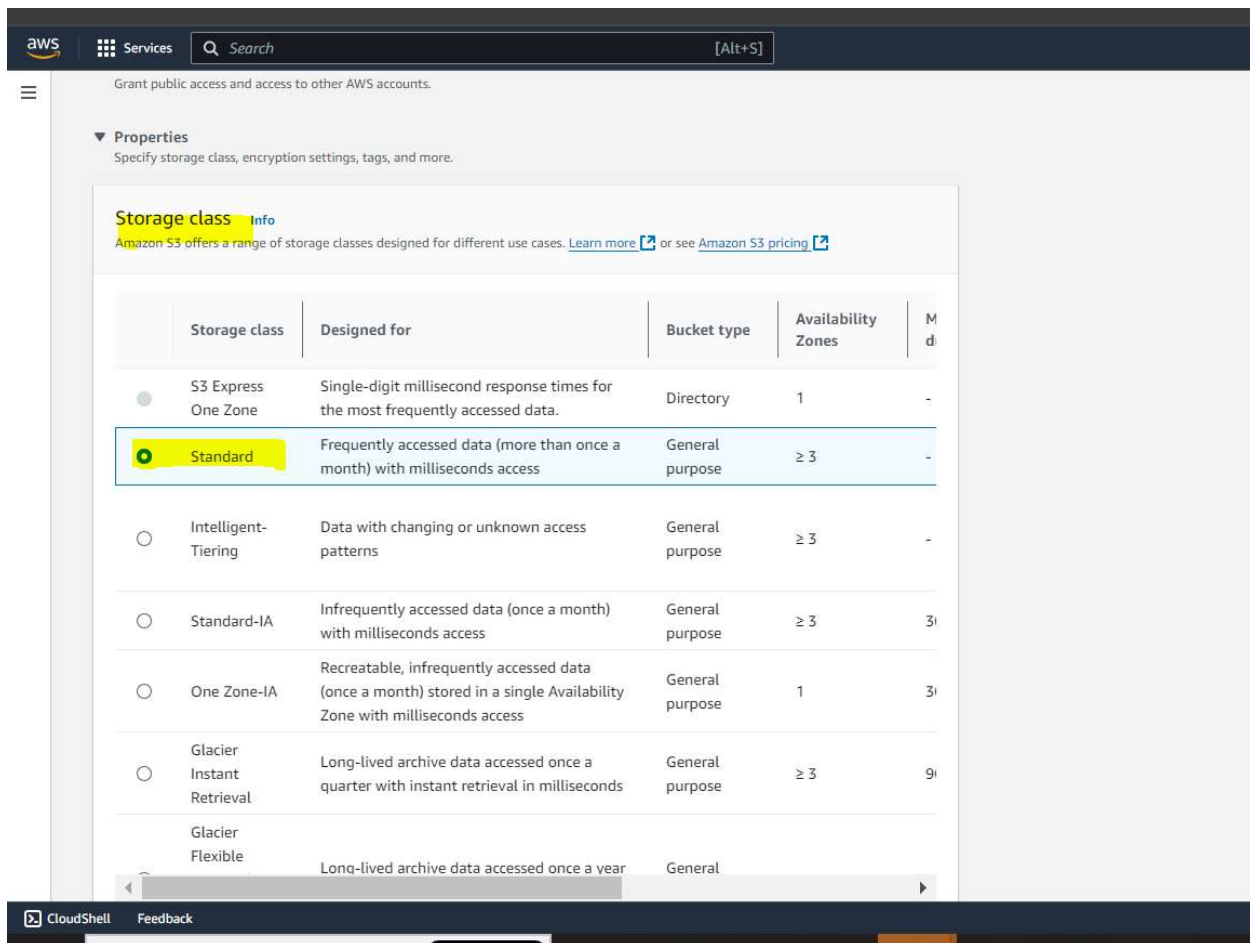
Bucket is created successfully.



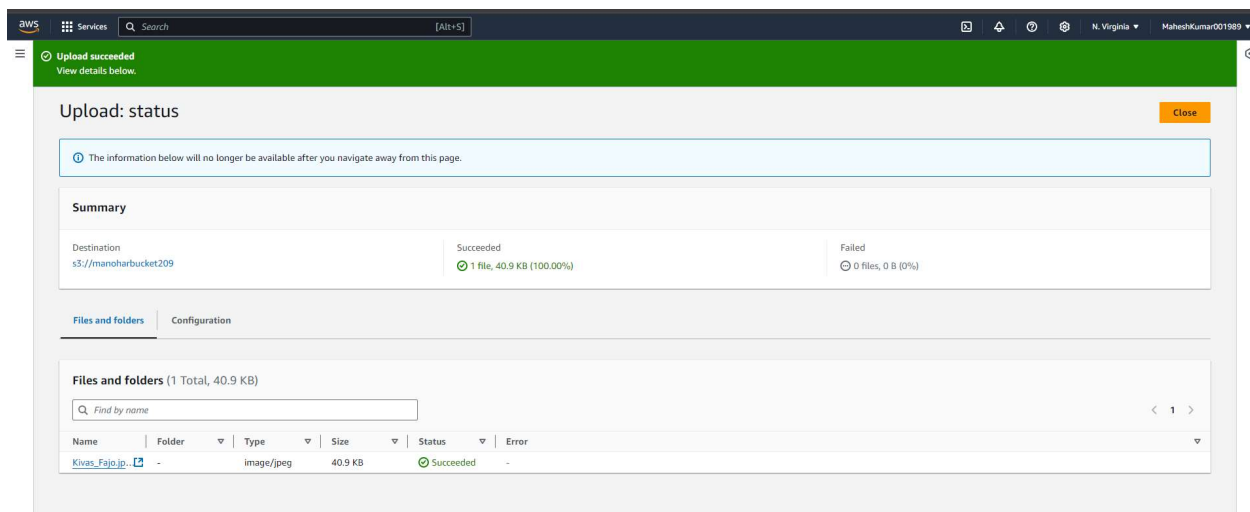
Upload a file in the bucket



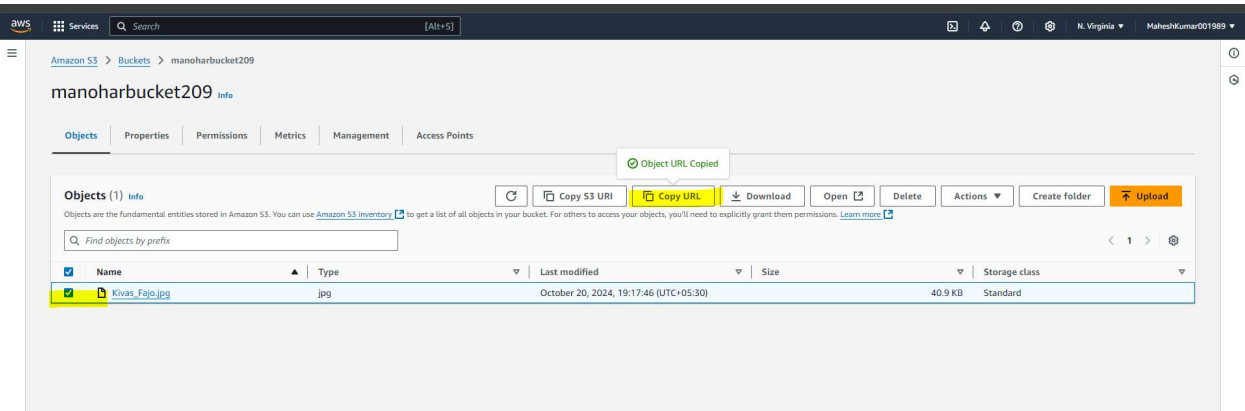
Storage class- standard



File uploaded successfully



Copy the URL and paste on the browser



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>SV4AYX9NSSDHN9X0</RequestId>
  <HostId>kV5VuybDey6ZrTdnWapsiNN+O36uamrY4Y05GxvbxU1lvRL/S10sgK6+X0B91C7nw66KKVdGVNtH=</HostId>
</Error>
```

aws

Services

Search

[Alt+S]

Amazon S3 > Buckets > manoharbucket209 > Edit Object Ownership

Edit Object Ownership Info

Object Ownership

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.

☐ 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.

☒ **ACLs enabled**

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

⚠ **Enabling ACLs turns off the bucket owner enforced setting for Object Ownership**

Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

☒ I acknowledge that ACLs will be restored.

Object Ownership

☒ **Bucket owner preferred**

If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☐ **Object writer**

The object writer remains the object owner.

CloudShell

Feedback

Amazon S3 > Buckets > manoharbucket209

manoharbucket209 Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1) Info

Copy

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

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size
<input checked="" type="checkbox"/>	Kivas_Fajo.jpg	jpg	October 20, 2024, 19:17:46 (UTC+05:30)	40

Download as

Share with a presigned URL

Calculate total size

Copy

Move

Initiate restore

Query with S3 Select

Edit actions

Rename object

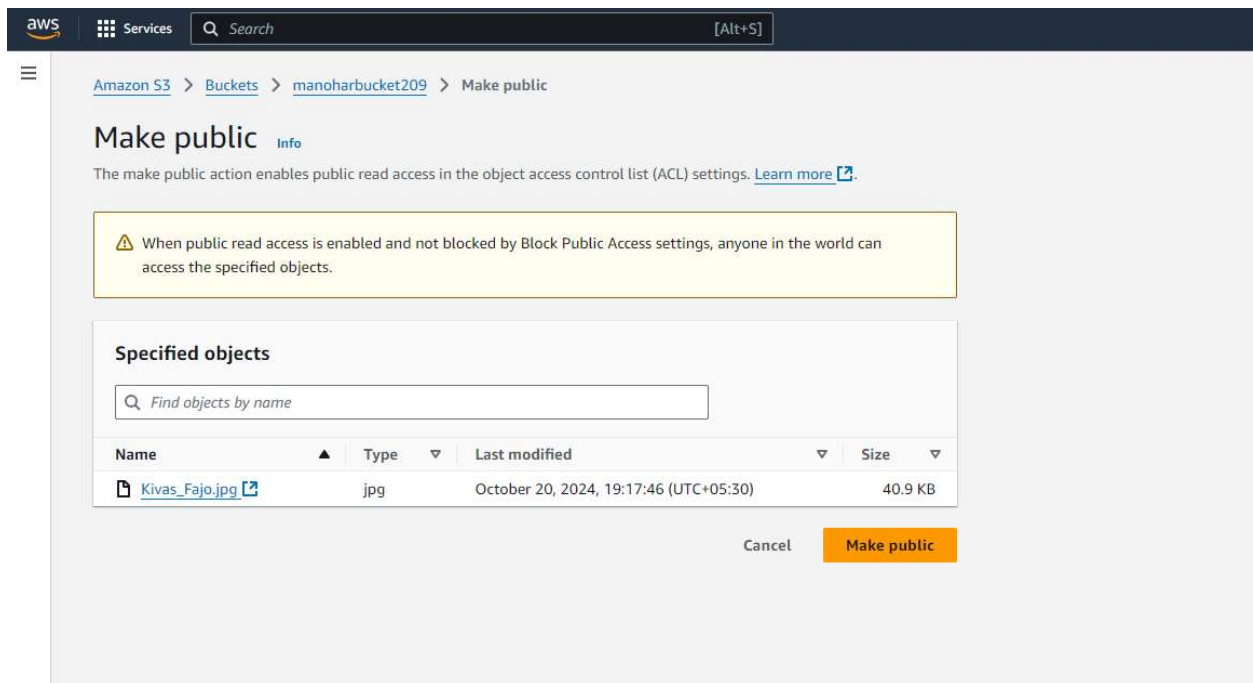
Edit storage class

Edit server-side encryption

Edit metadata

Edit tags

Make public using ACL



After enable the ACL and make it public I can access the image which I uploaded in S3 bucket using the S3 url

