Create a New IAM User

1.Create a new IAM user with programmatic access.

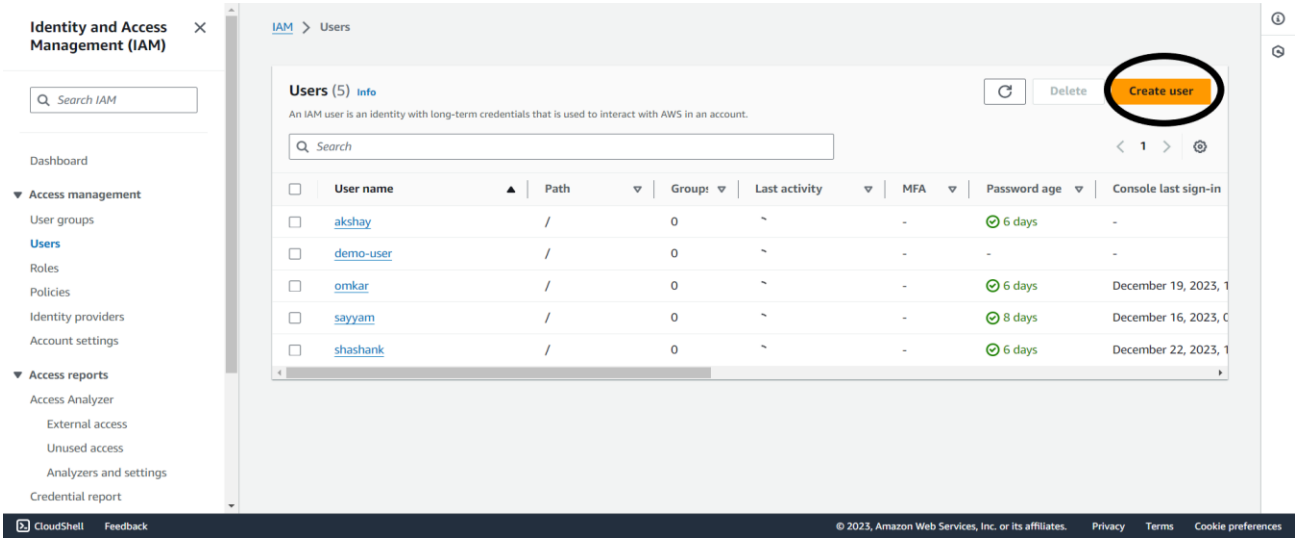
Assign appropriate permissions to the user based on their role or responsibilities.

Generate and securely provide the user's access key and secret access key.

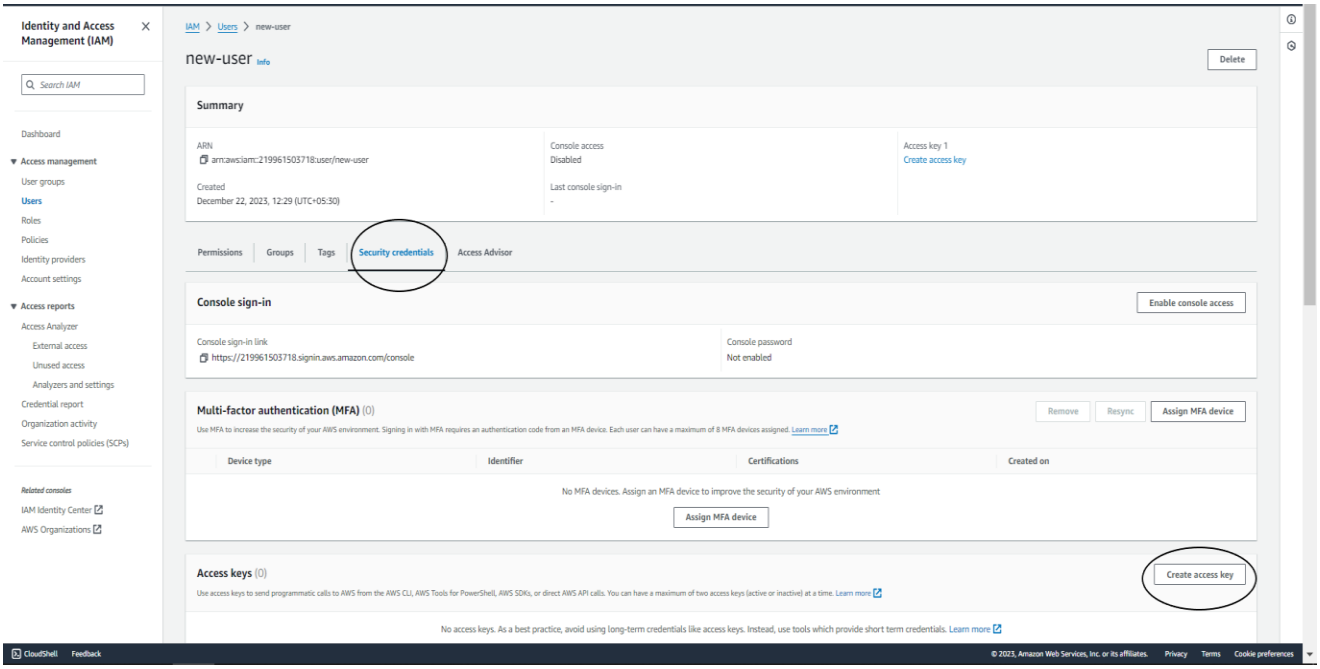
Configure IAM Roles:

Create a IAM user-:

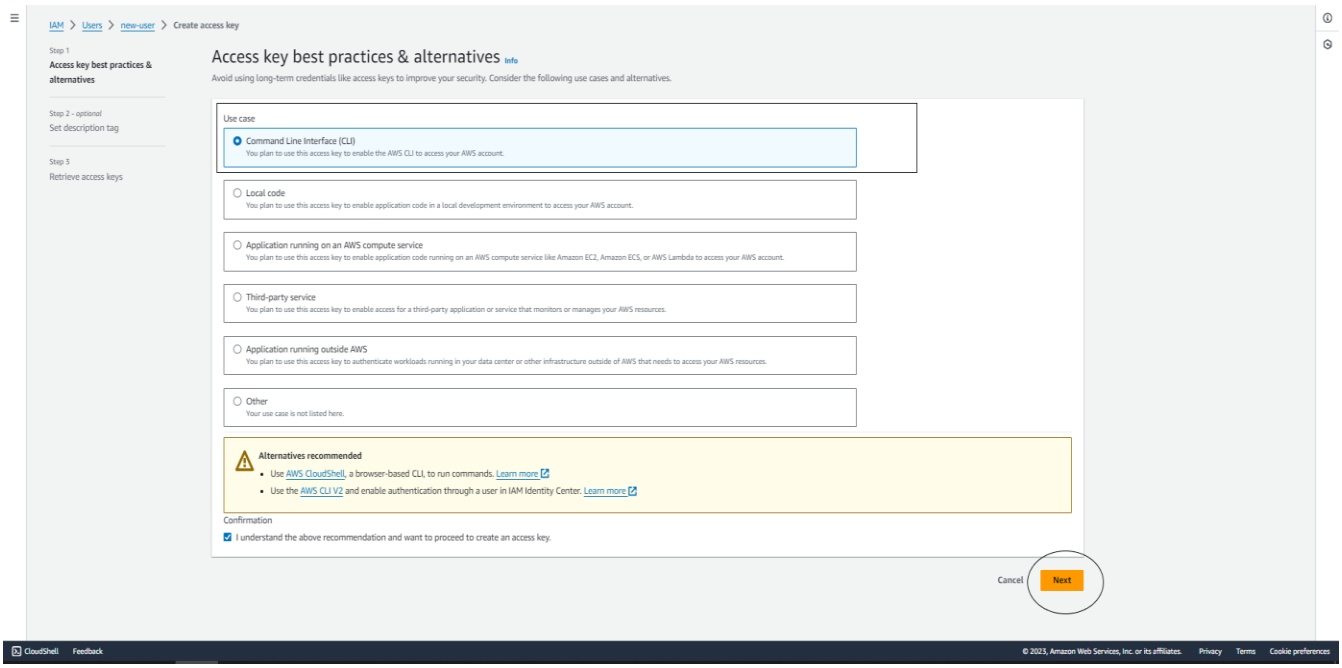
Step 1- Go to IAM services and create user.



Step 2- Go to the security credentials to create access key and secret key.

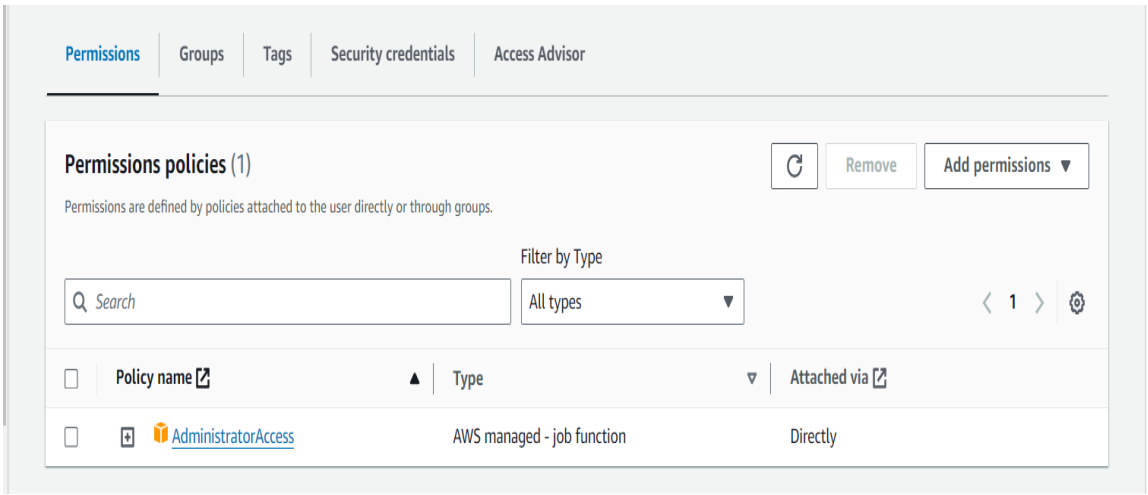


Step 3- Select the use case. (Select Cli)



Step 4- Then search cloud shell in search bar of the console and log in the console.

Step 5- Attach or remove policy.

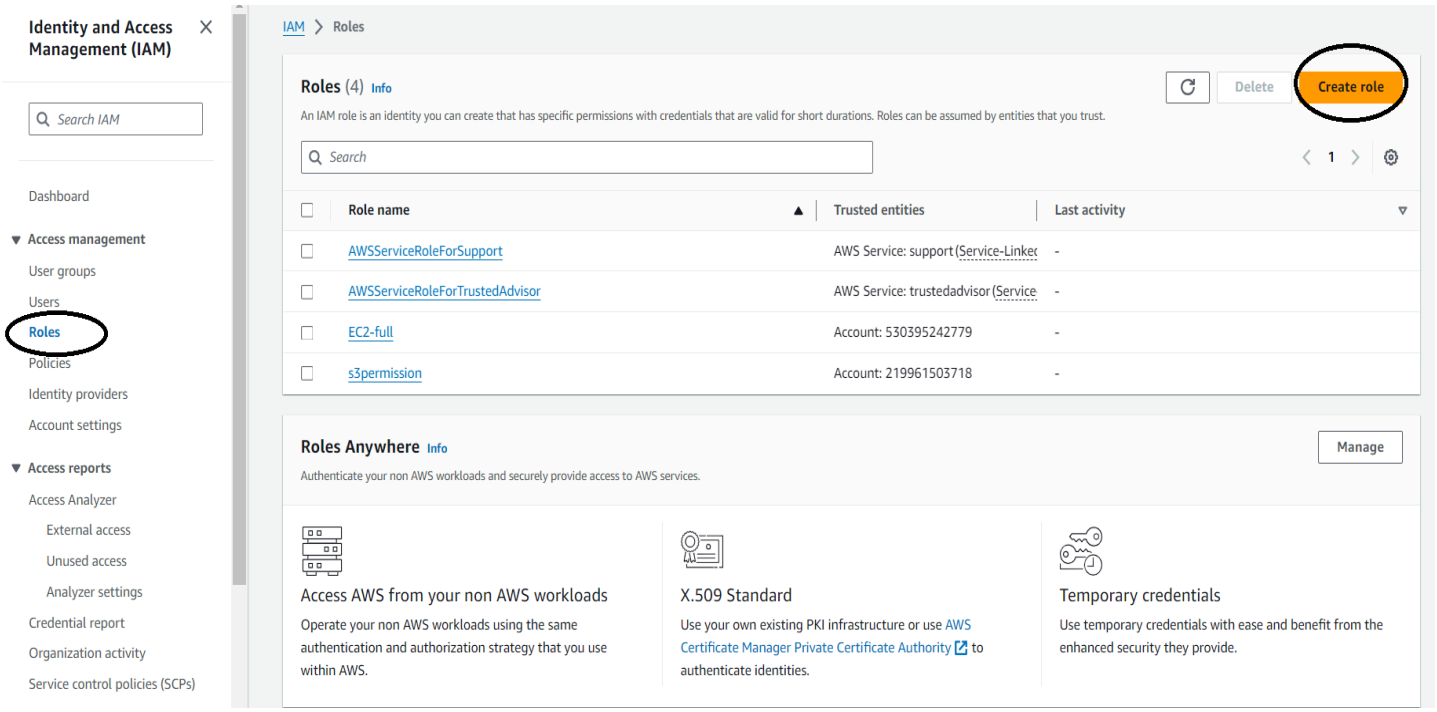


2.Create an IAM role for EC2 instances or Lambda functions with specific permissions.

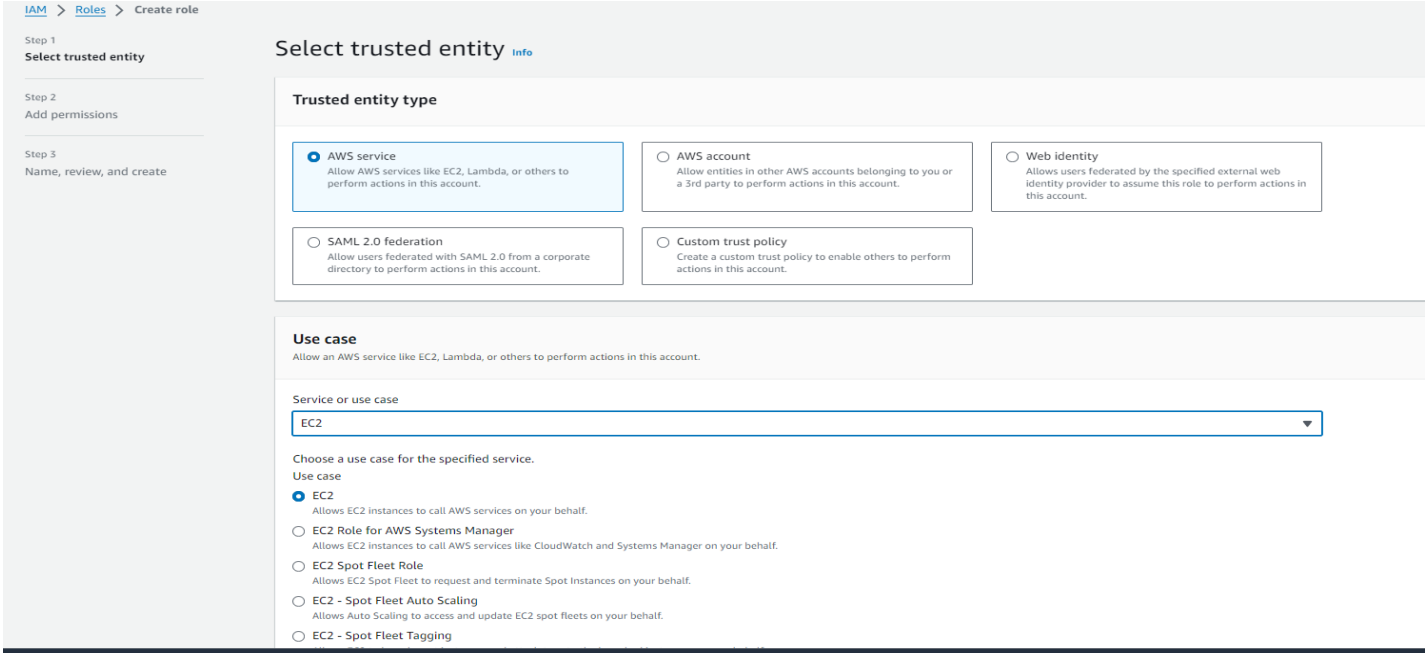
Attach policies to the role that grant necessary permissions to access AWS resources.

Assign the role to EC2 instances or Lambda functions.

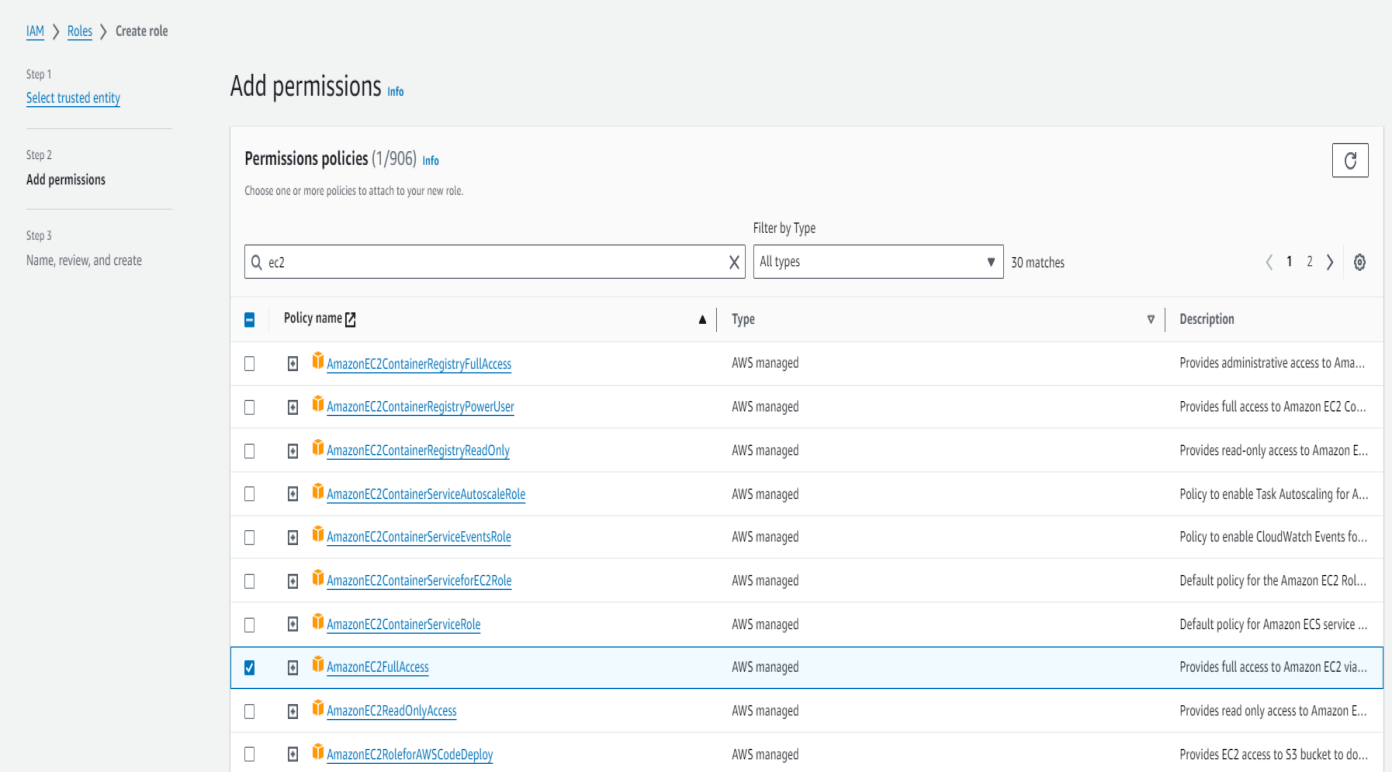
Step 1- Go to the IAM services inside the IAM services click on the role for creating the role.



Step 2- Select AWS service which is in present in trusted entity and after that select use case as EC2

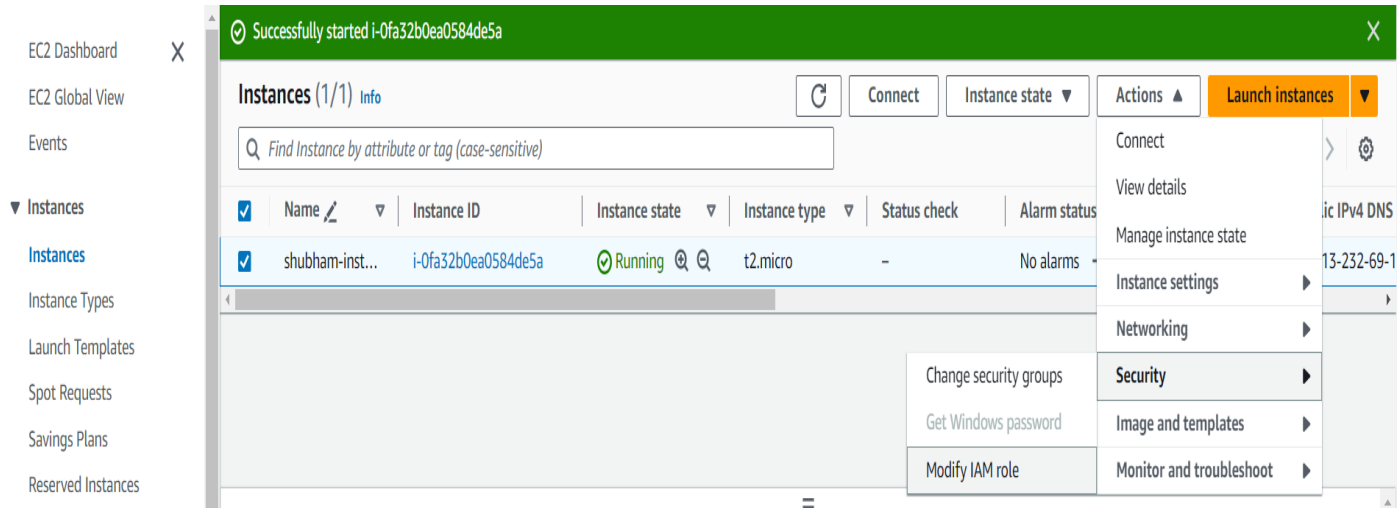


Step 3- After this select the permission that you have to apply (EC2 full access in this case)

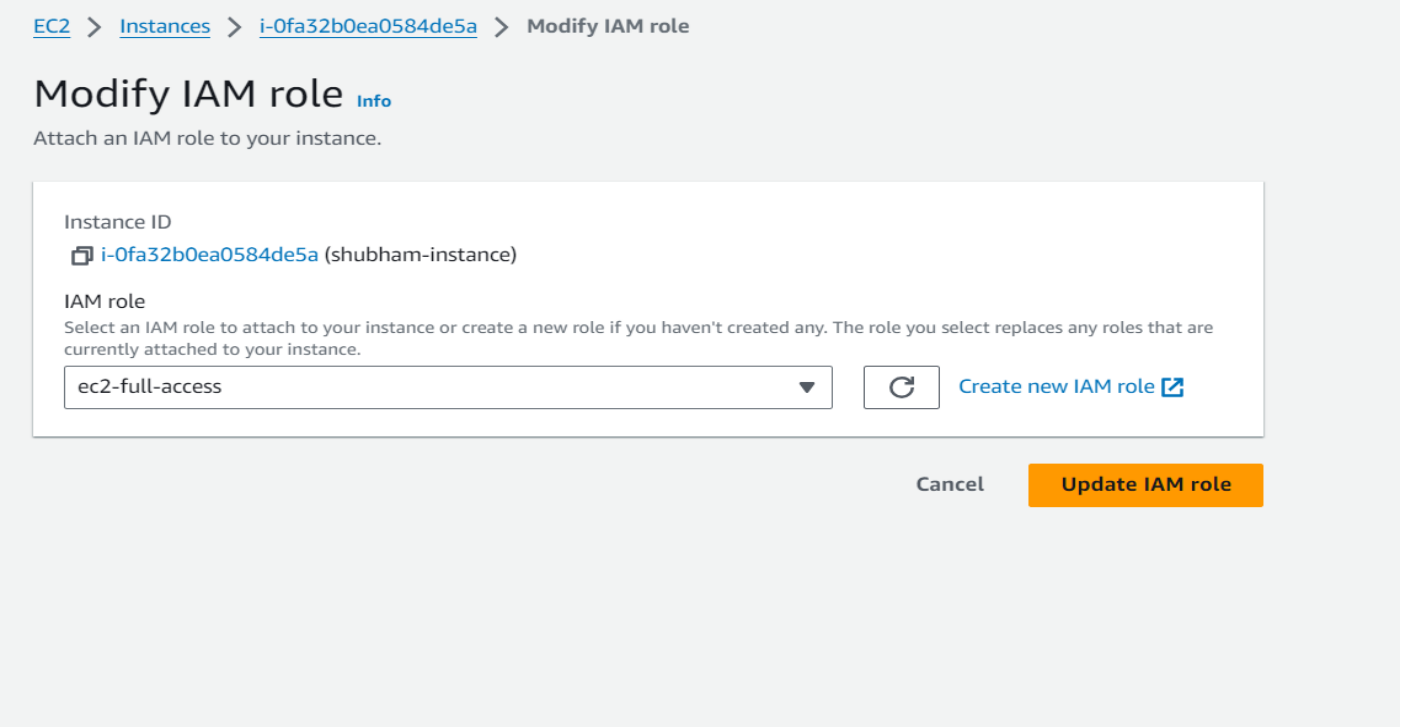


Step 4- Click next permission after this go to the EC2 services select instance select instance then start it. When the instance start running go to

action->security->modify role



Step 5- Select the role and click update IAM role



3.Implement Multi-Factor Authentication (MFA):

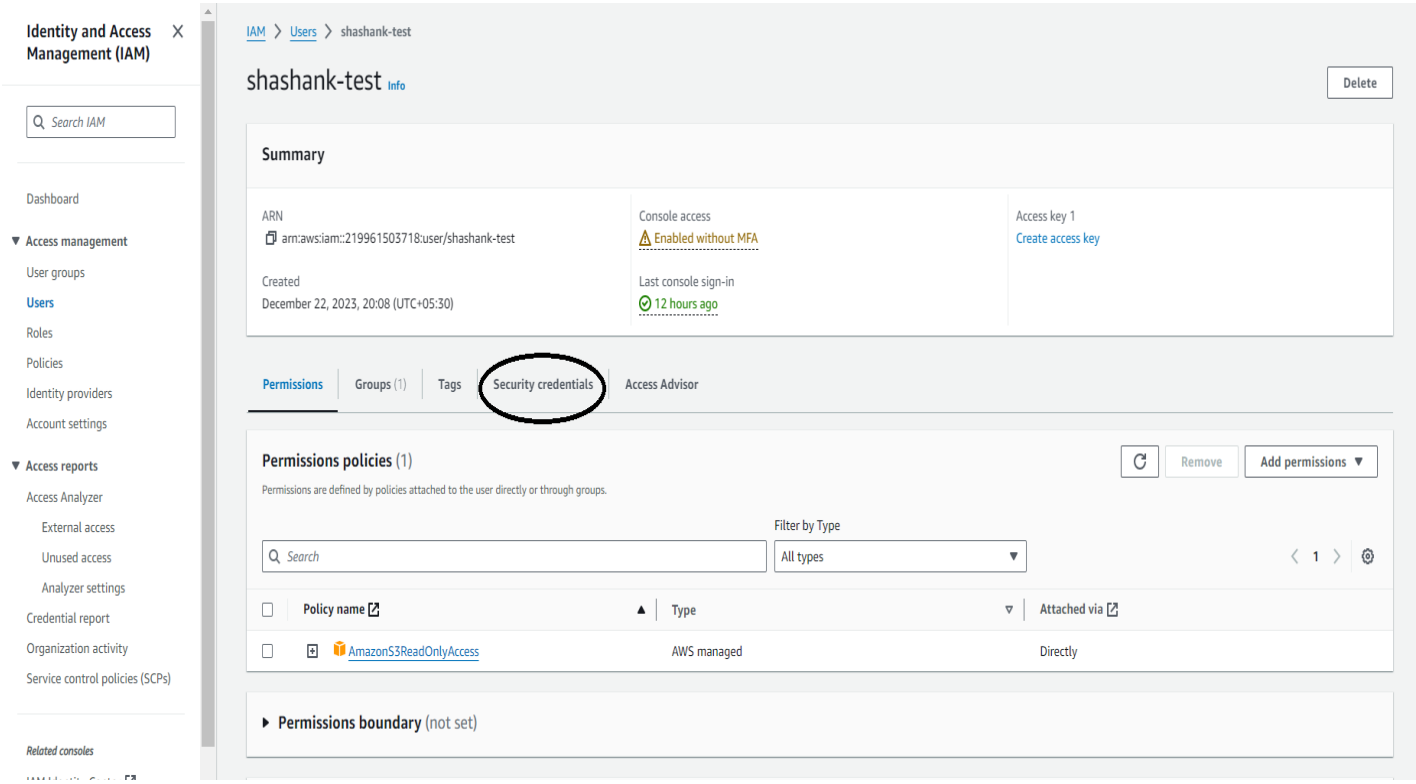
Enable MFA for IAM users to provide an additional layer of security.

Guide users on how to set up MFA devices (such as virtual MFA apps or hardware tokens).

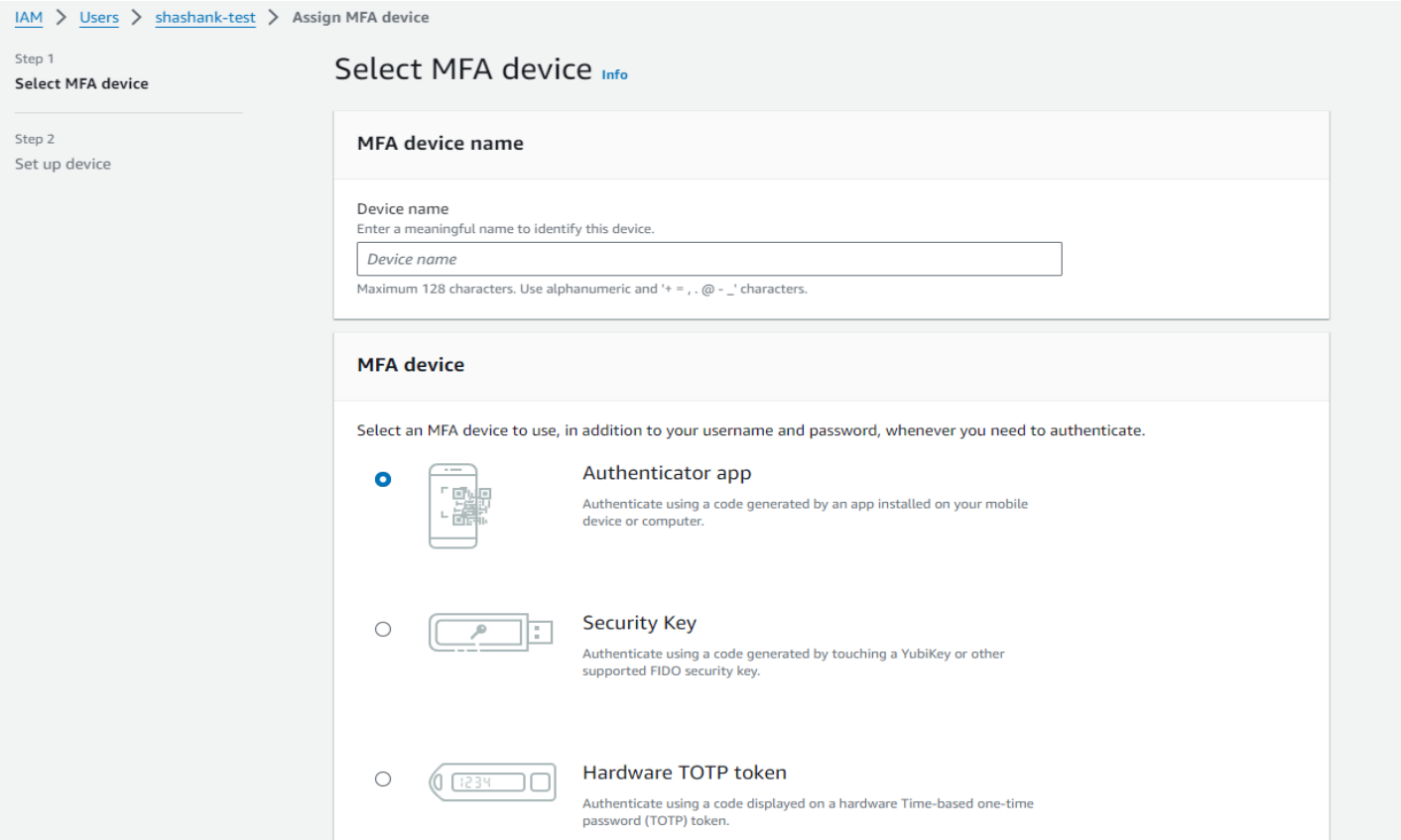
Test the MFA configuration to ensure it functions correctly.

Create IAM Policies:

Step 1- To enable MFA go IAM services->user->security credentials->assign MFA device



Step 2- Select MFA device



Set up device-

1. Install authenticator app

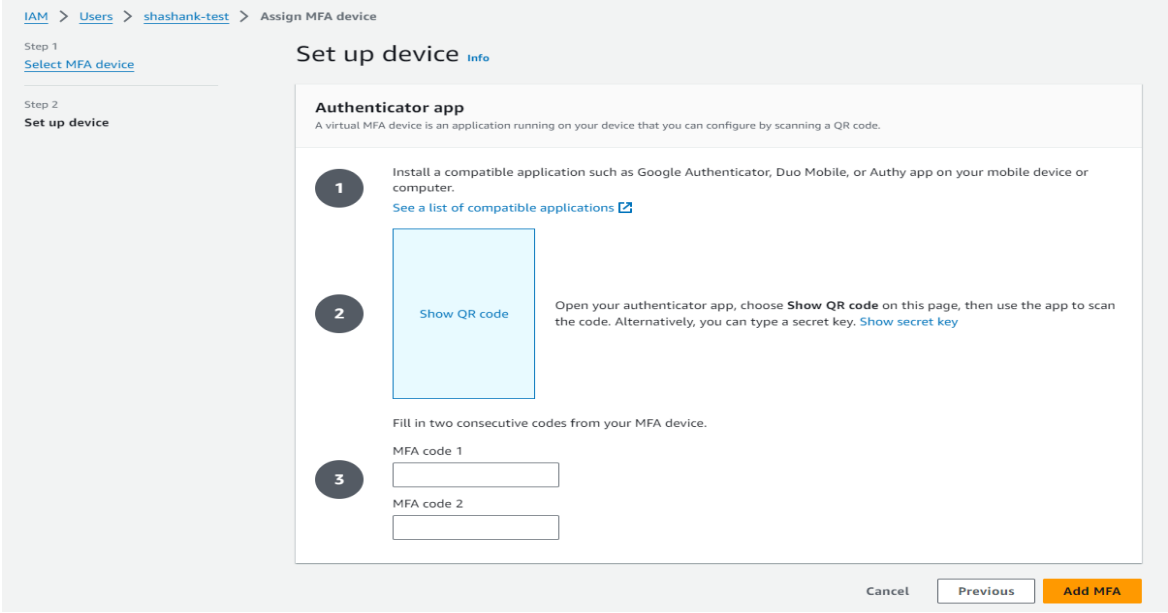
Download and install an authenticator app on your mobile device.

2. Scan QR code or enter key

Us app to scan the QR code display in IAM console or manually enter the secret configuration key.

3. Enter verification code

The app will generate a time-based verification code. Enter this code in IAM console to confirm activation.



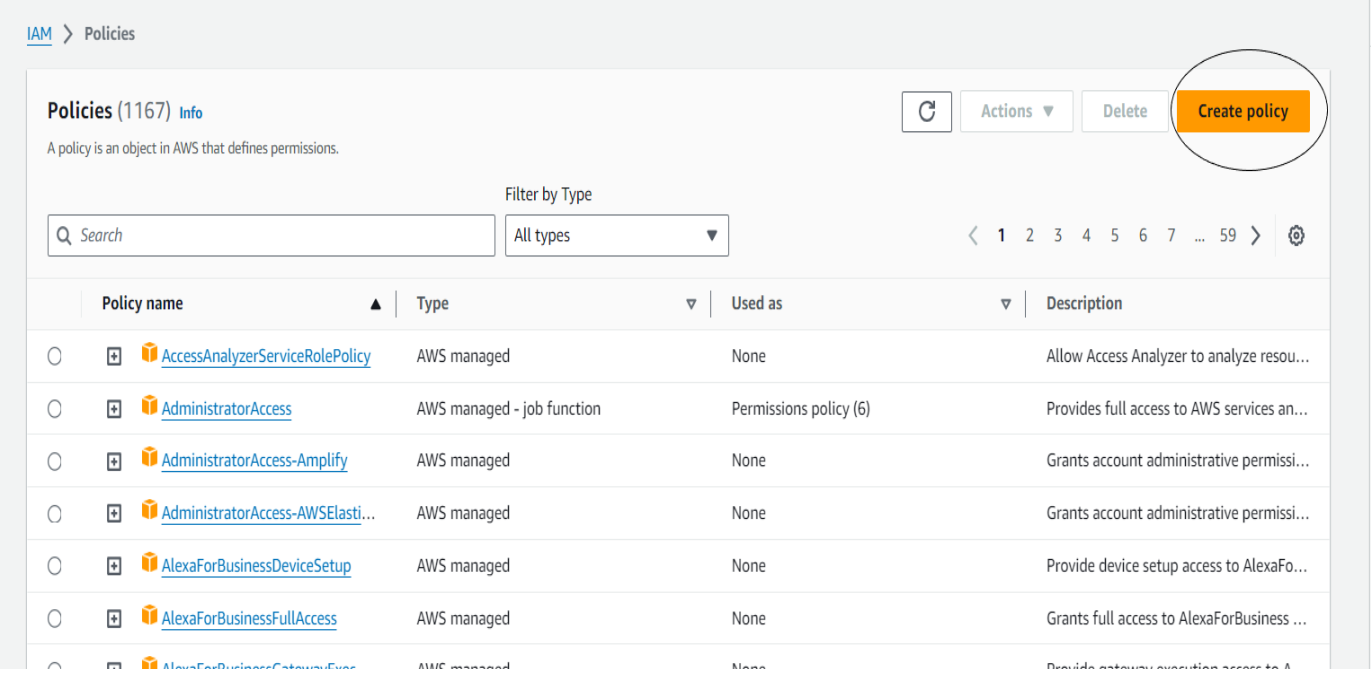
4.Write a custom IAM policy that allows or denies specific actions on AWS resources.

Associate the policy with the appropriate IAM users, groups, or roles.

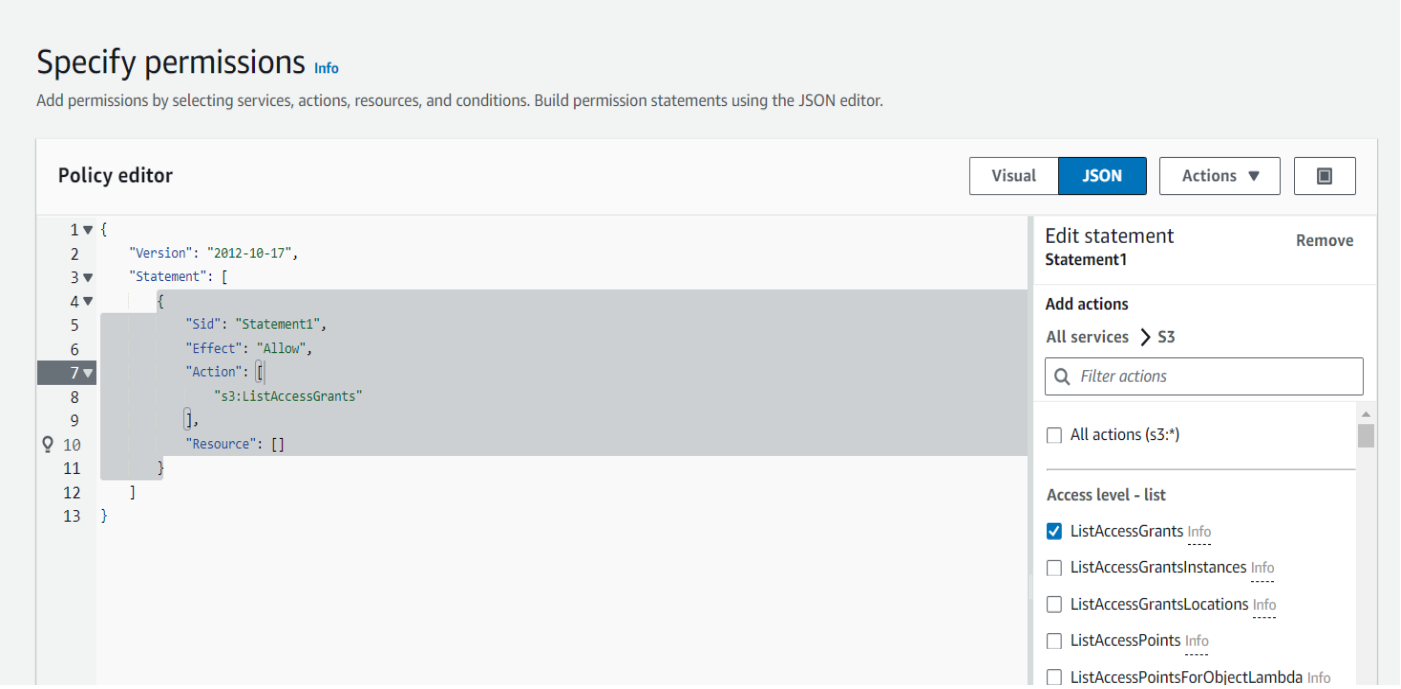
Test the policy to verify that the desired access control is enforced.

Use IAM Groups:

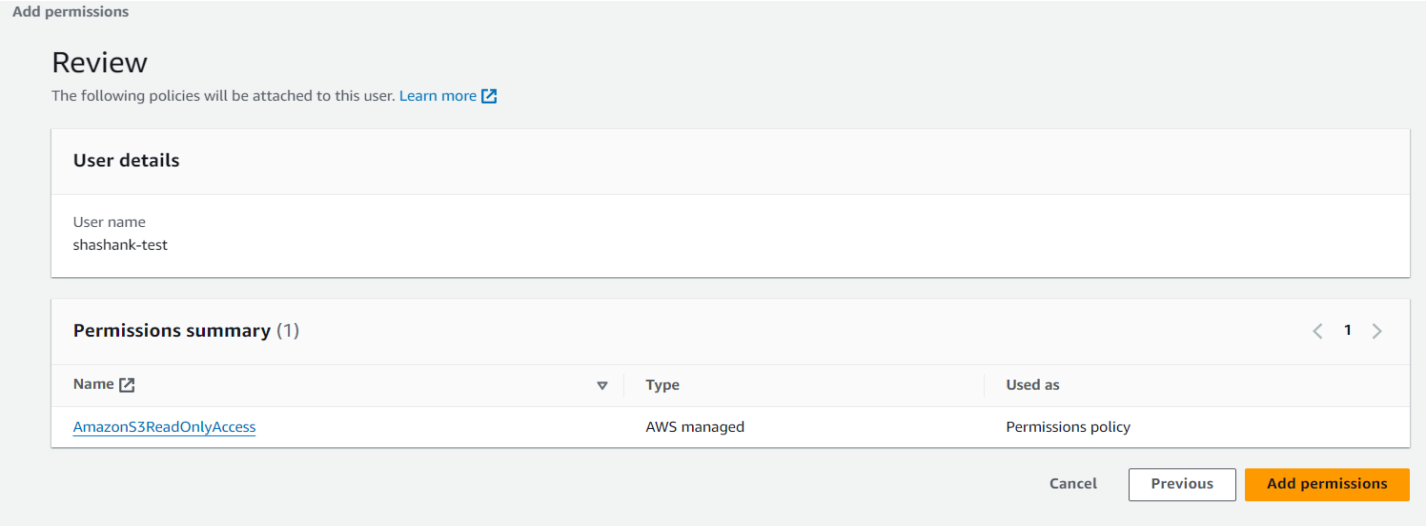
Step 1- Go to IAM policies to create policy -> Create policy



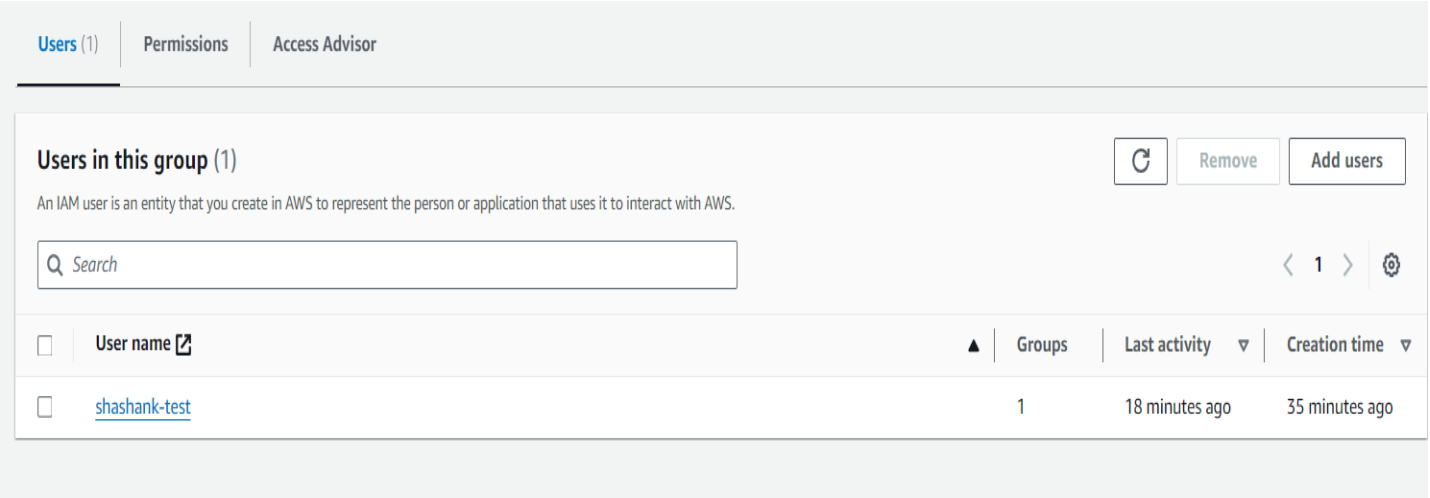
Step 2- Write JESON code for policy (S3 list access grand)



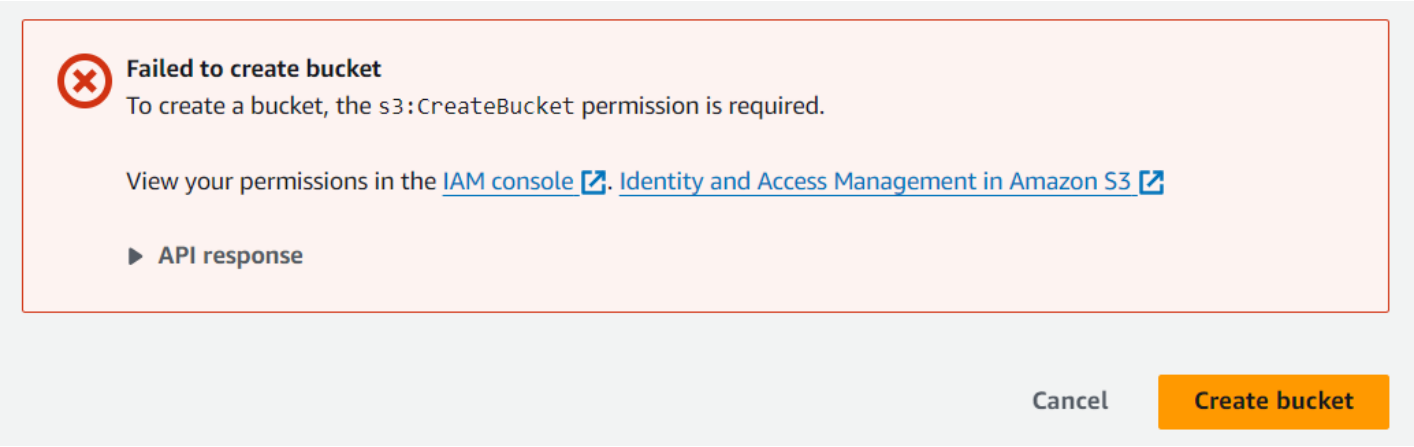
Step 3- Attach policy to the user



Step 4- After attaching the policy user added into the group



Step 5- After adding into the group check the policy the error occurs due to incomplete access of S3



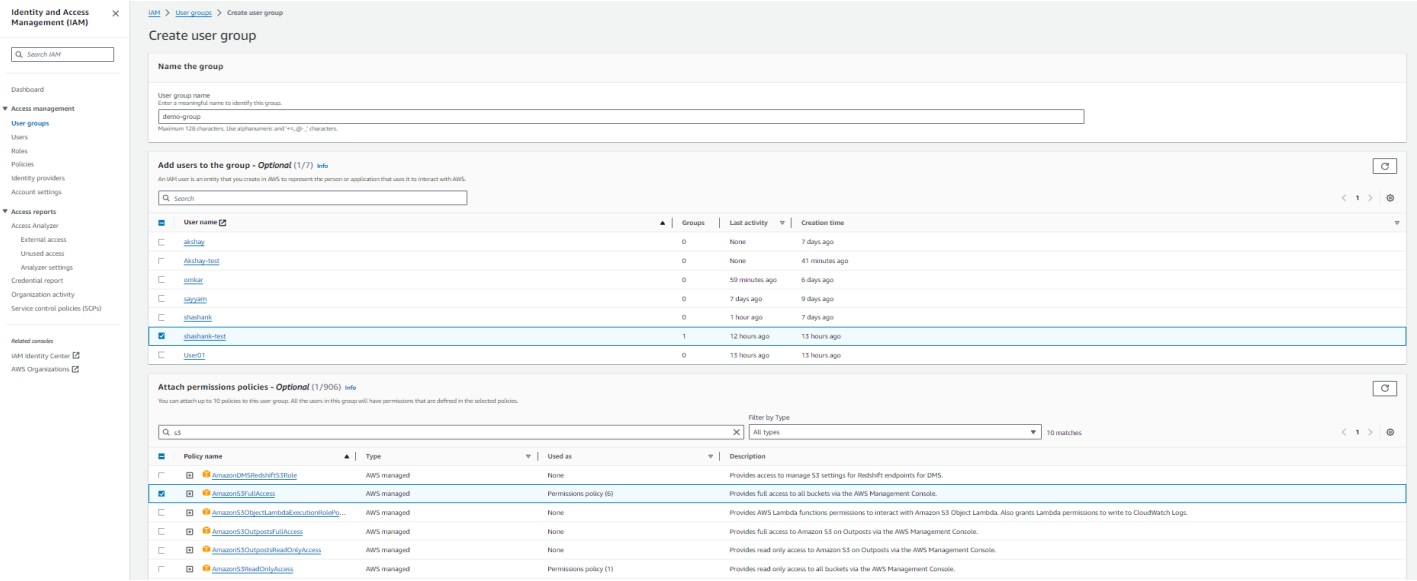
5.Create an IAM group and assign permissions to it.

Add IAM users to the group to manage their access collectively.

Remove users from the group when their access requirements change.

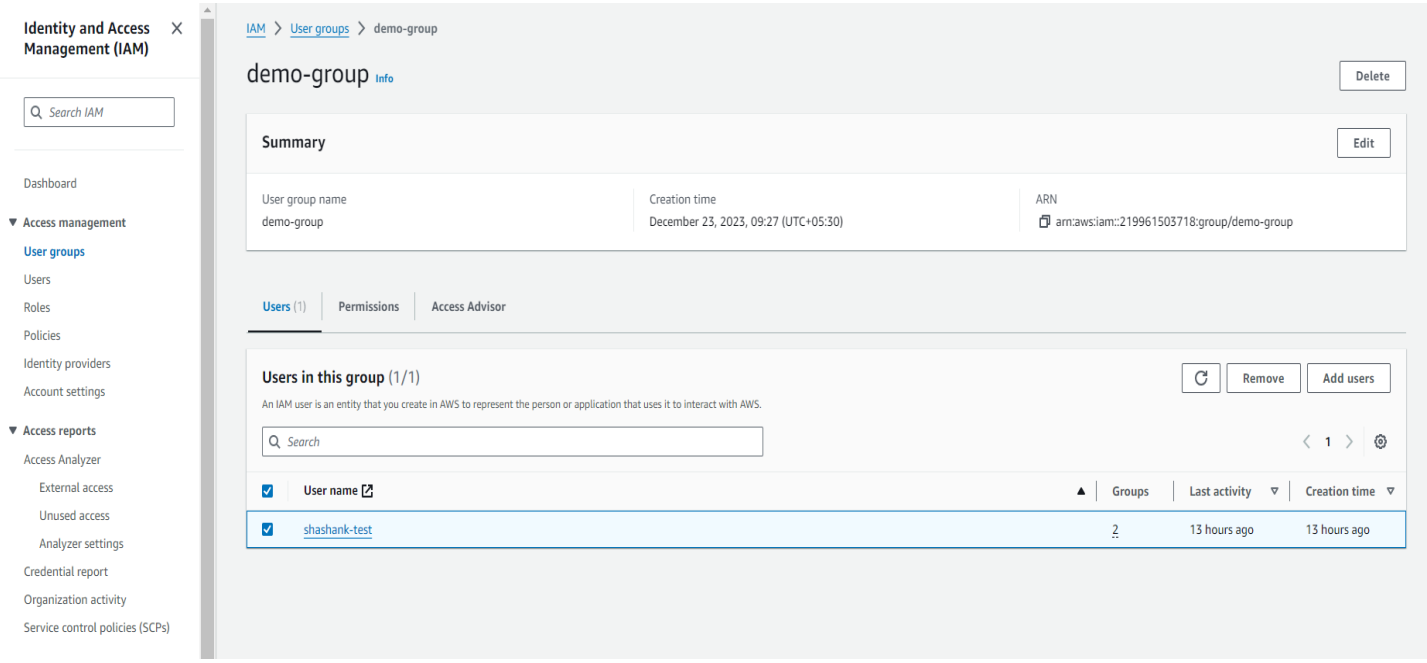
Implement IAM Access Analyzer:

Step 1- Create an IAM group go to the IAM console->user group->create user group->name the group (demo group)->add users to the groups->attach permission policies



Step 2- Removing users from the group

Go to -Access group members->select user->remove users



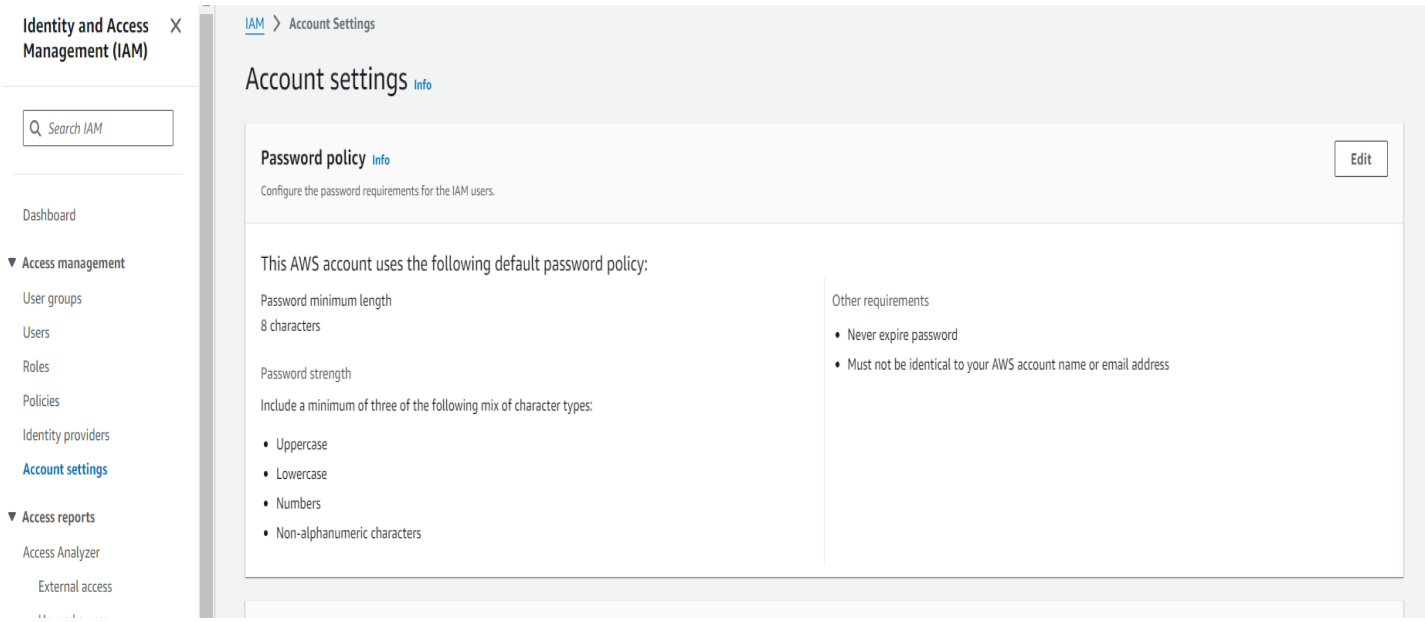
6.Define and enforce password policies for IAM users.

Set requirements such as minimum password length, complexity, and expiration.

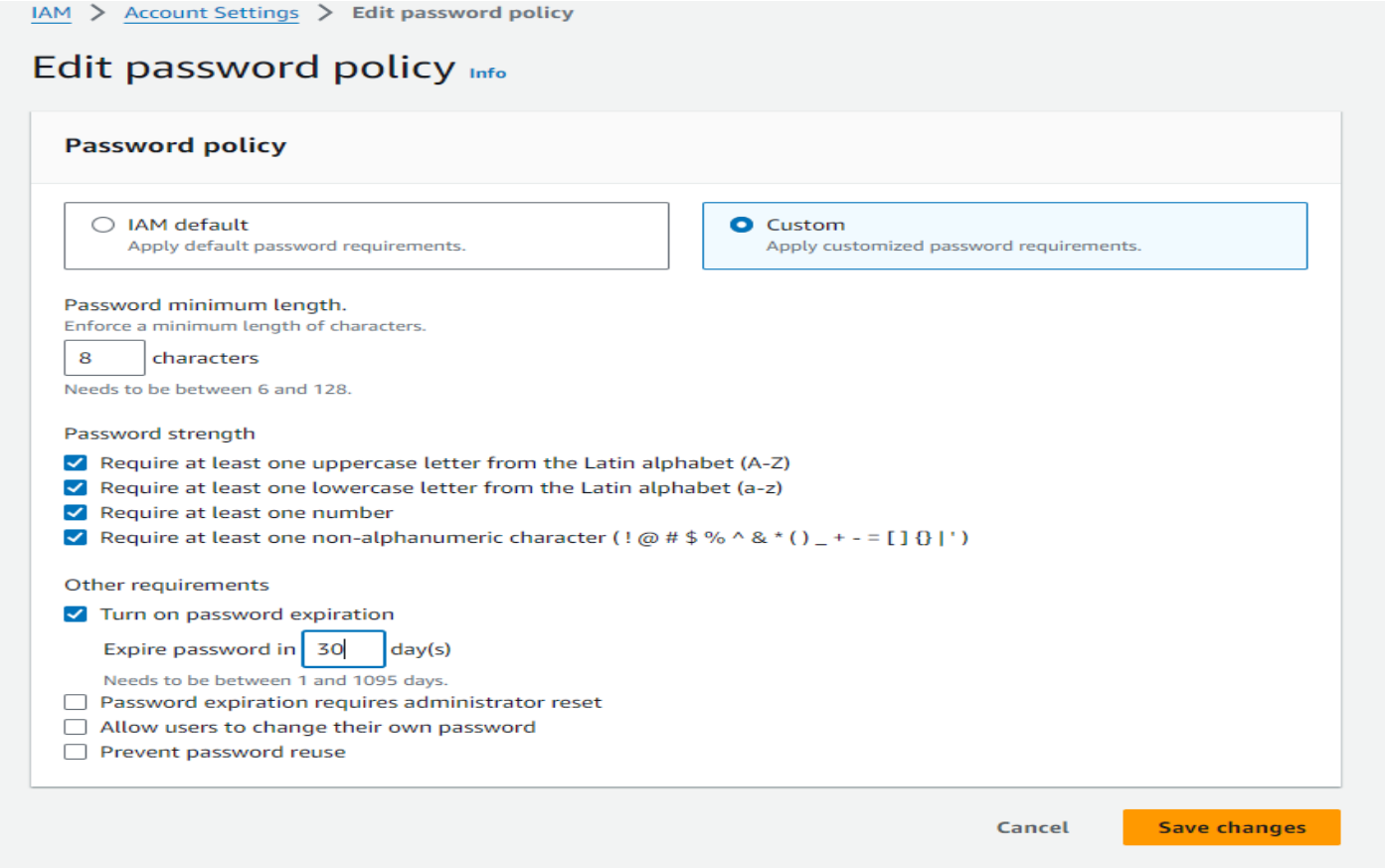
Regularly remind users to update their passwords according to the policy.

Step 1- To set policy for the password go to the

–IAM console-> account setting->password policy->edit



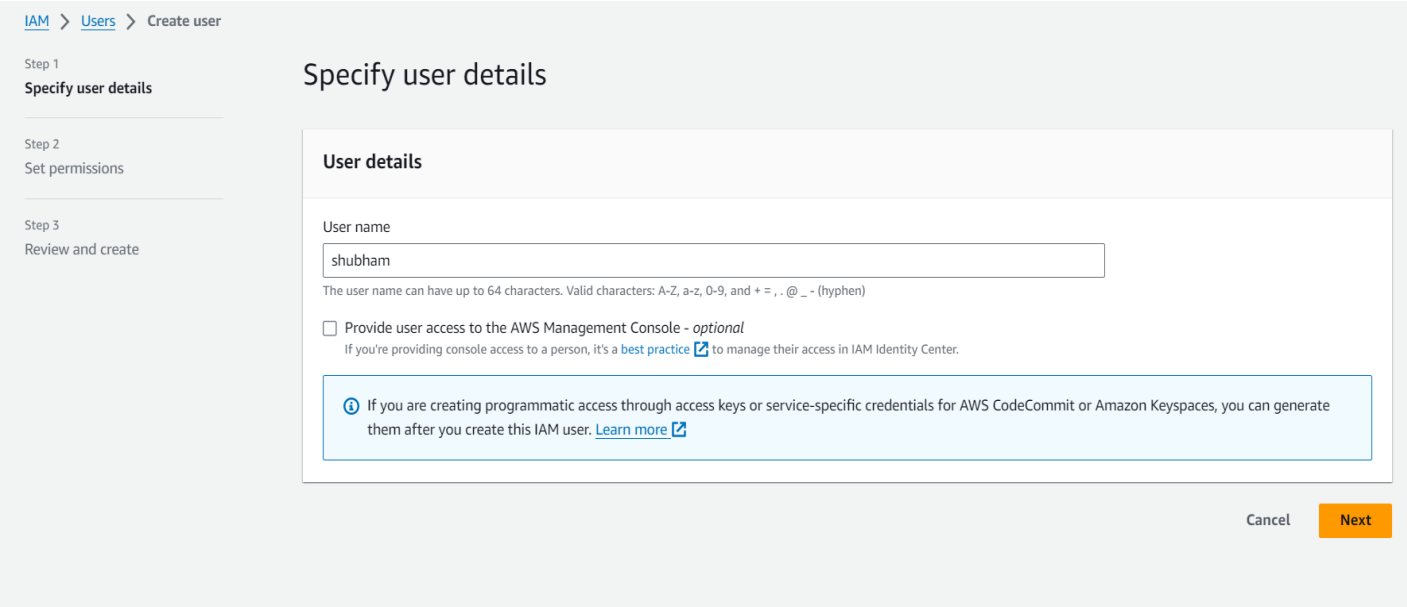
Step 2- After entering the edit option click on ->custom (configure as per requirement) click on save changes. To apply new password policy.



7.Create user Shubham.shubham can only launch ec2 instance in Mumbai

Region

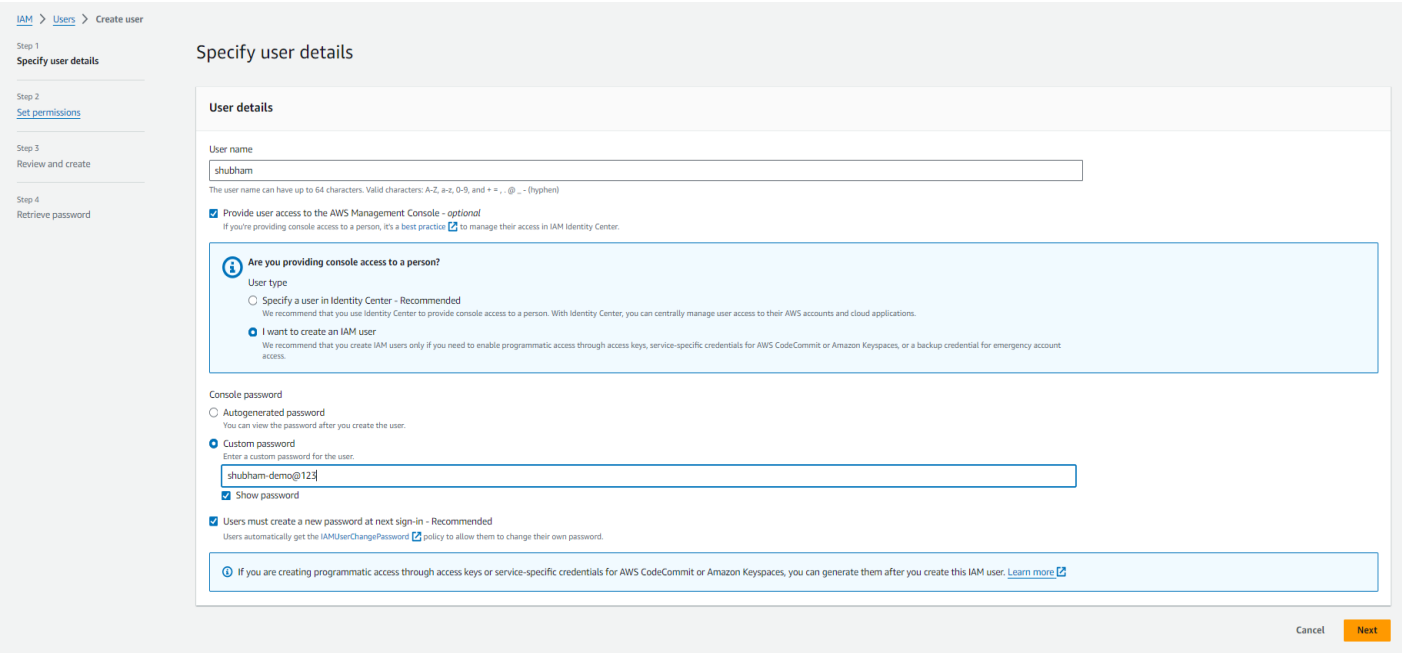
Step 1- For creating the new user go to the IAM console ->user-> create user ->specify user details->user name(in our case user name is shubham)



Step 2- select – provide user access to AWS management console

Select- i want to create an IAM user

Go to console password->Select custom password->next



Step 3- Attach the policy

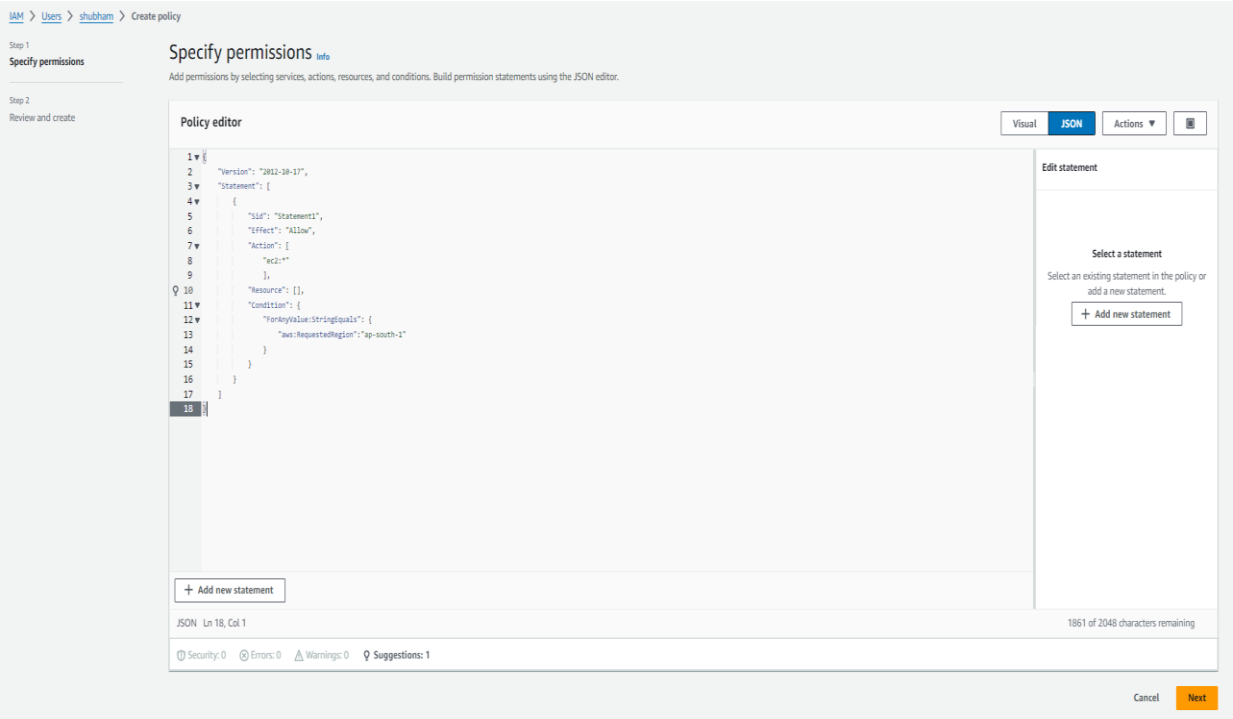
Click on user which is present in IAM console

Select the user(in our case shubham)

Go to permission policy and click on add permission then click on create inline policy

Click next and

Add policy to it



8.Scenario: You are a DevOps engineer responsible for managing AWS resources for your company's e-commerce application. Your company uses S3 to store

product images, and you need to grant specific permissions to different teams within your organization.

Task: Your task is to set up IAM users and policies to manage access to the S3 buckets containing product images. Here are the steps you need to follow:

Create IAM Groups:

Create two IAM groups: "Marketing" and "Developers."

Create IAM Policies:

Create an IAM policy called "MarketingAccess" that allows read-only access to the S3 bucket containing product images. Attach this policy to the "Marketing" group.

Create an IAM policy called "DevAccess" that allows both read and write access to the same S3 bucket. Attach this policy to the "Developers" group.

Create IAM Users:

Create two IAM users: "Shubham" and "Deepak"

Add "Shubham" to the "Marketing" group and "Deepak" to the "Developers" group.

Configure S3 Bucket Permissions:

Configure the S3 bucket containing product images with a bucket policy that allows read-only access for the "Marketing" group and read/write access for the "Developers" group.

Testing:

Log in to the AWS Management Console as "Shubham" (Marketing team) and verify that he can only read the product images from the S3 bucket.

Log in to the AWS Management Console as "Deepak" (Developers team) and verify that he can both read and write product images to the S3 bucket.

Documentation:

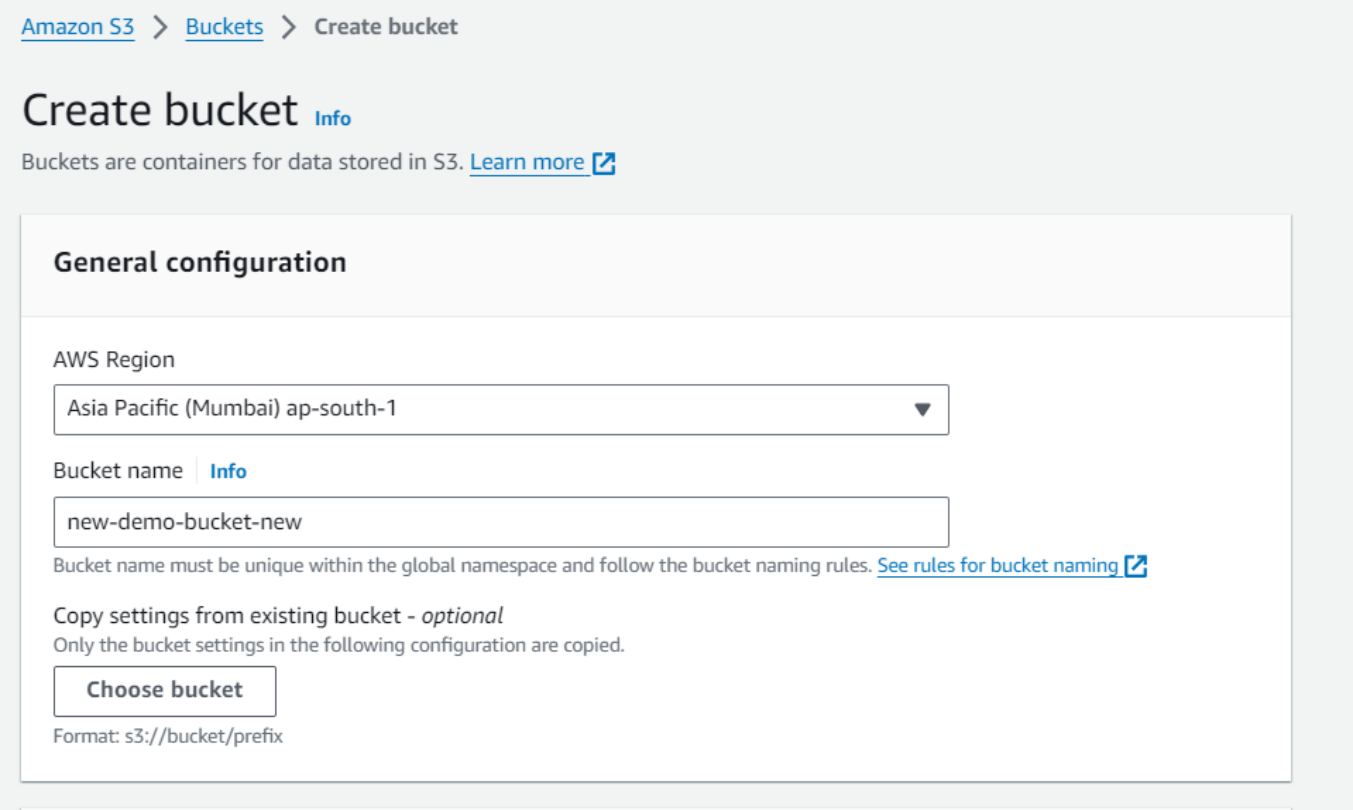
Step 1- create S3 bucket

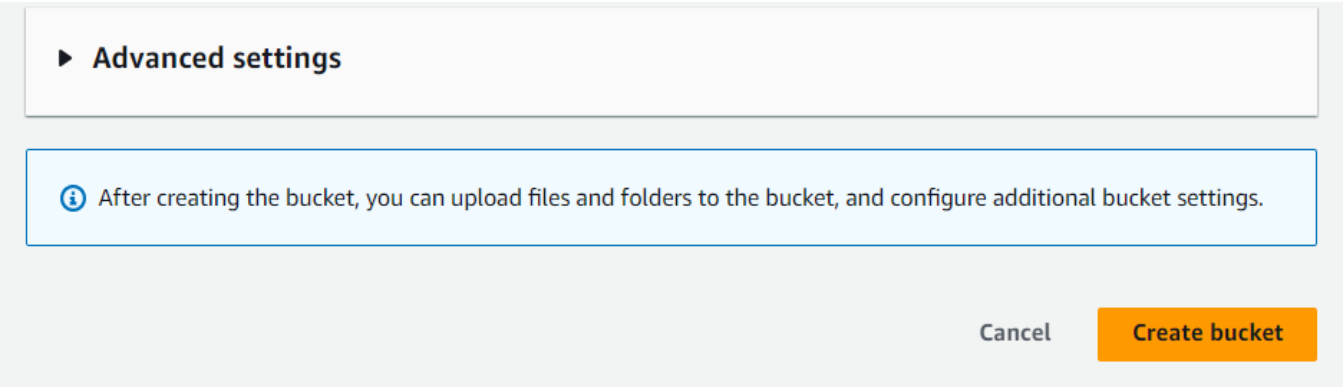
Go to S3 console

click on ->Create bucket

Select->AWS Region

Click on ->create bucket





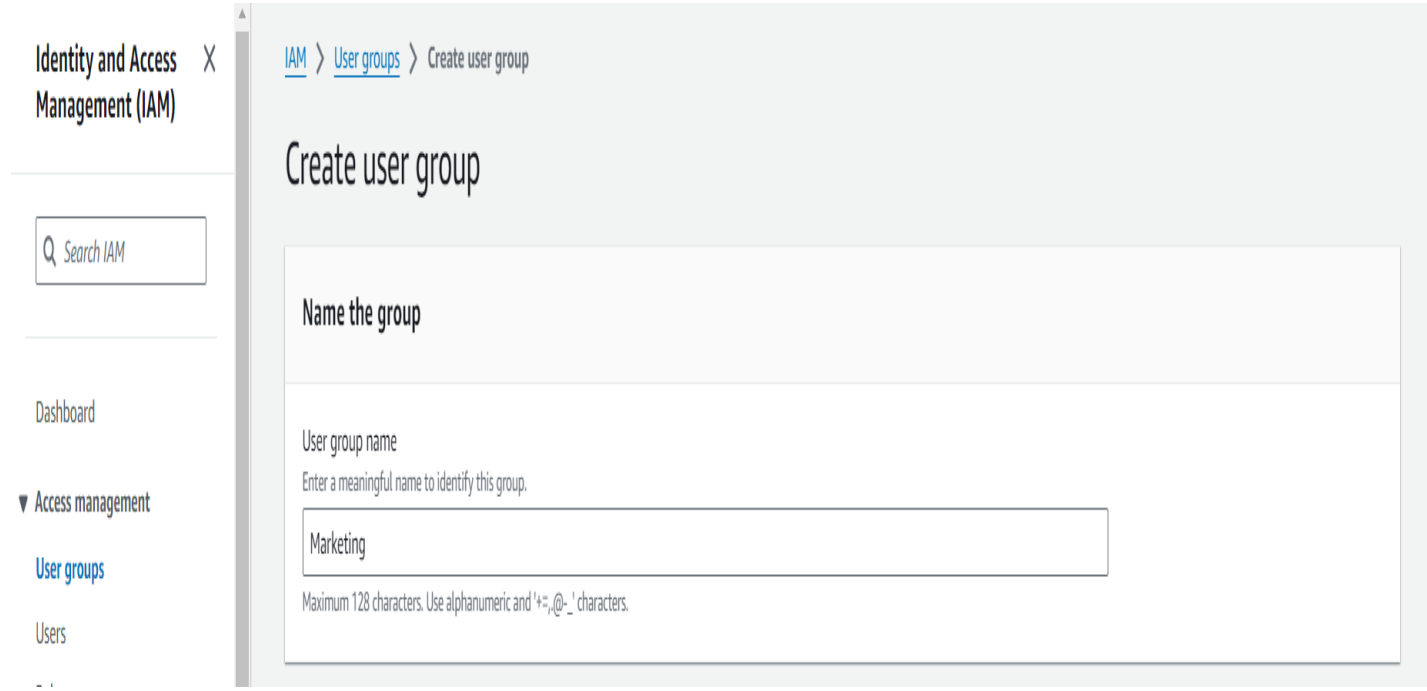
Step 2- Creating an IAM group for marking

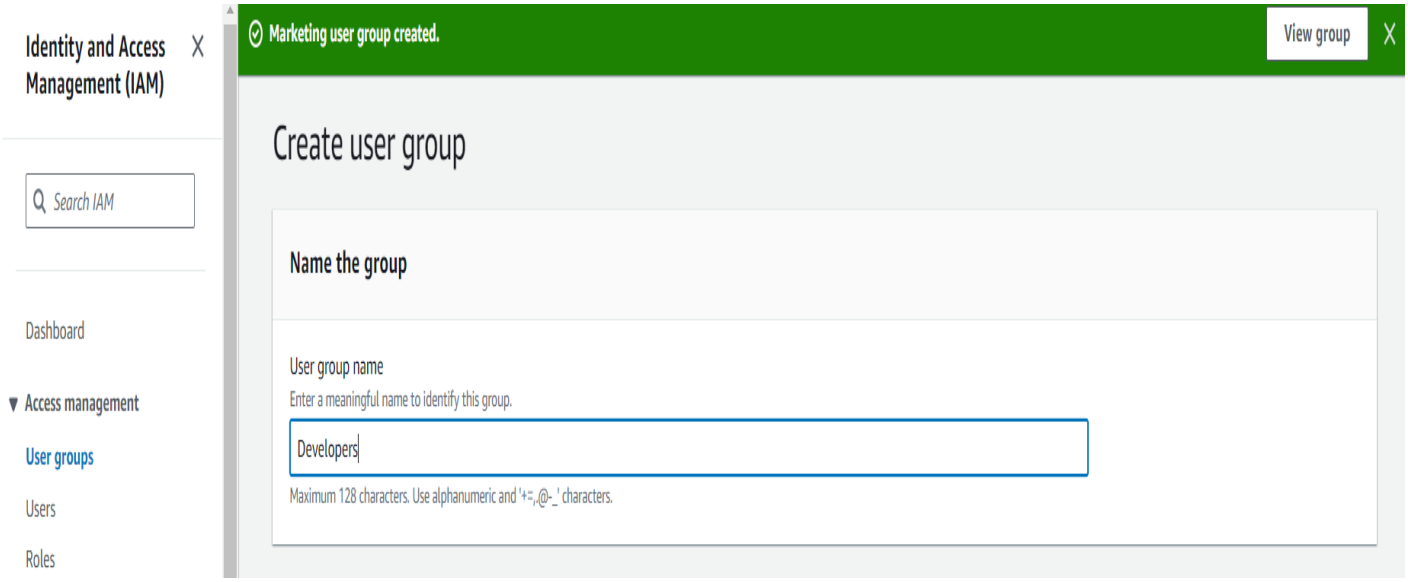
Go to the IAM console

Click on user group

Click on create group for marketing and developers

Name the group(marketing and for second group developers)





Step 3- Create IAM policies Marketing Access

Go to IAM console

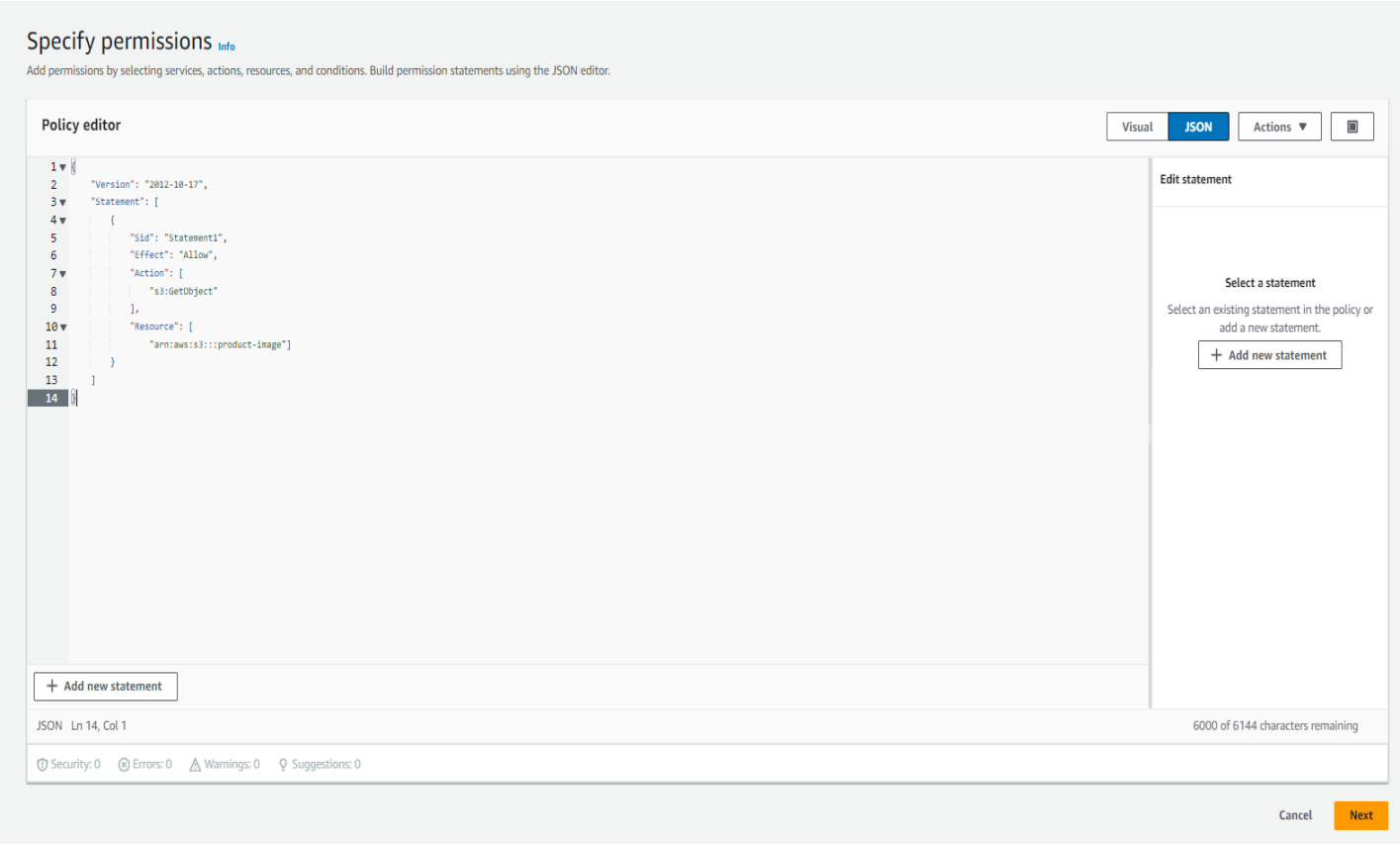
Click on policies

Click on create policy

Choose JSON type for the creation of policy

Enter the name as marketing access

Click on create



Step 4- Create IAM policies Developer Access

Go to IAM console

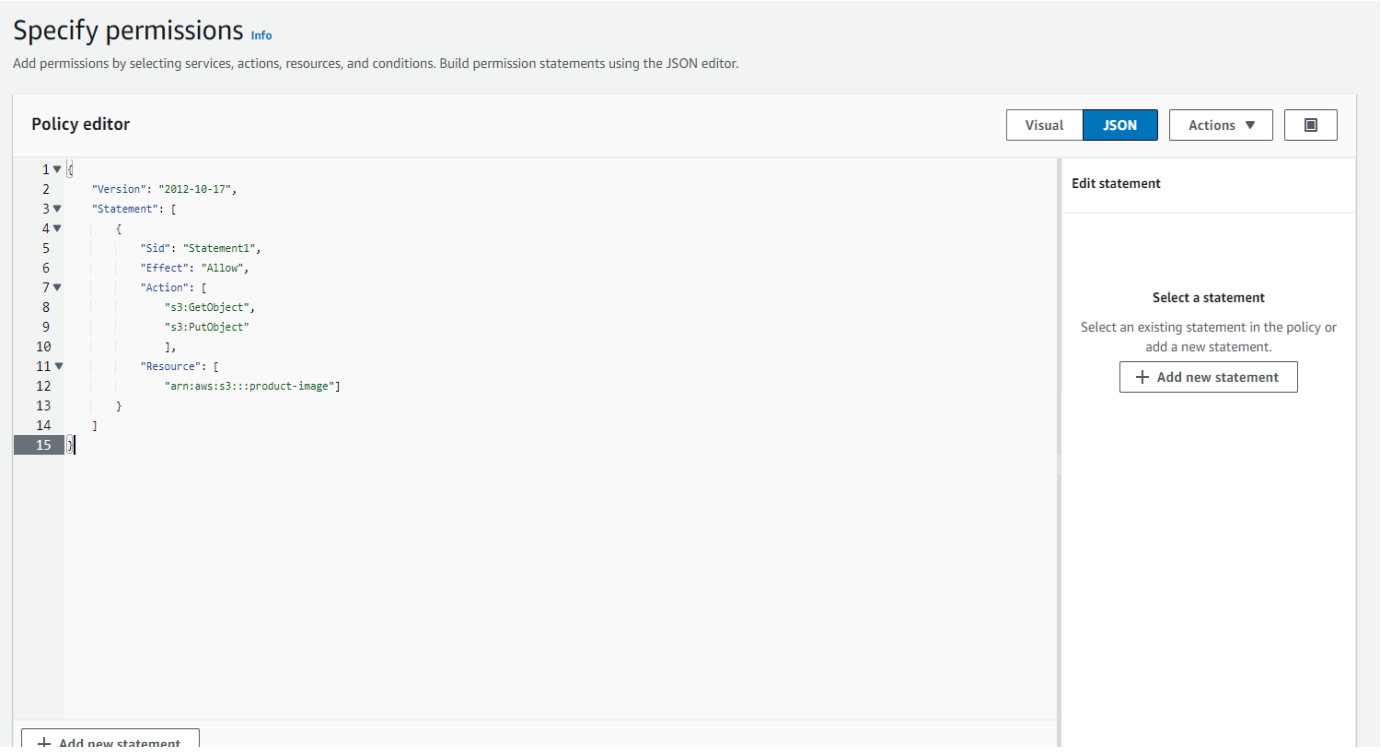
Click on policies

Click on create policy

Choose JSON type for the creation of policy

Enter the name as Developer access

Click on create



Step 5- Attach the policies to groups

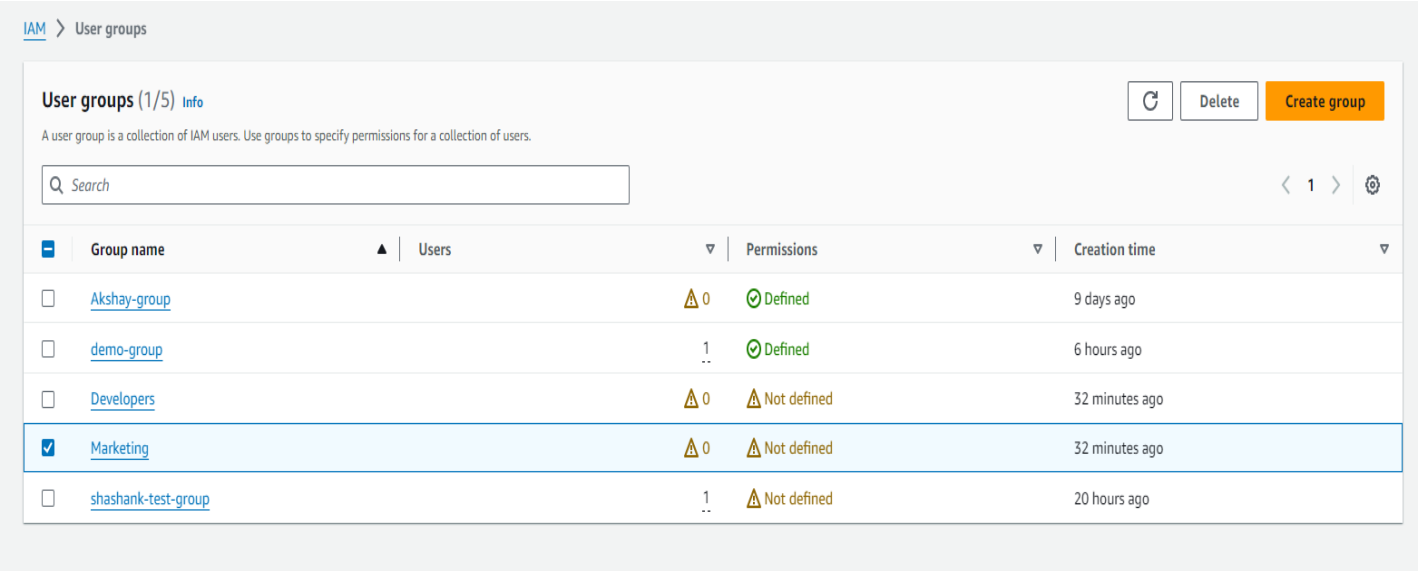
Click on IAM console

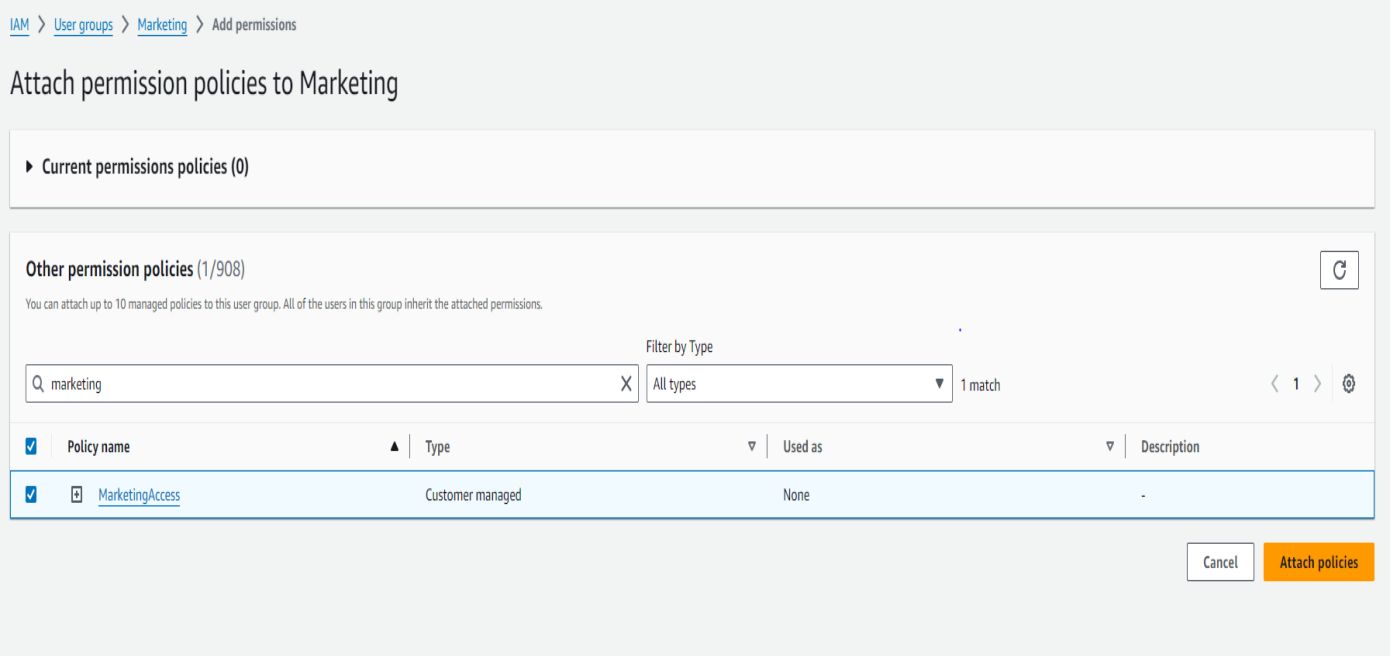
Click on user group

Select marketing

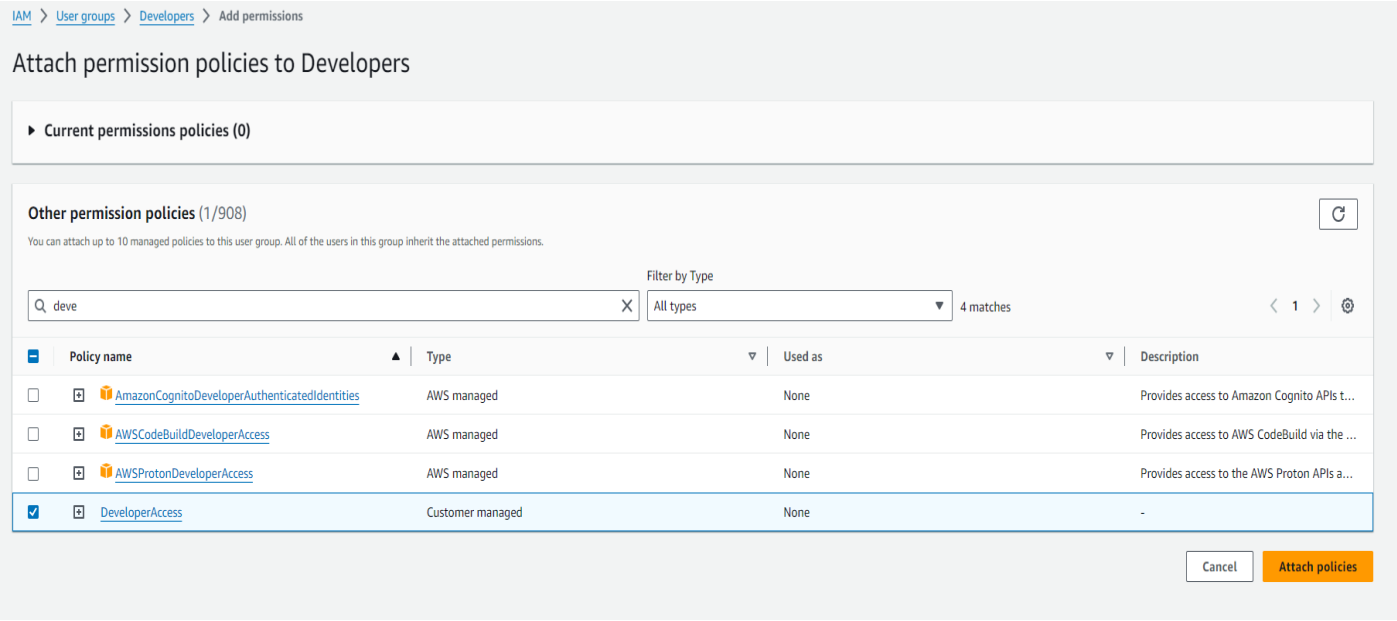
Go to permission add permission

Attach policy





Step 6- Same for the Developer



Step 7- Create IAM user

Go to IAM console

Click to users

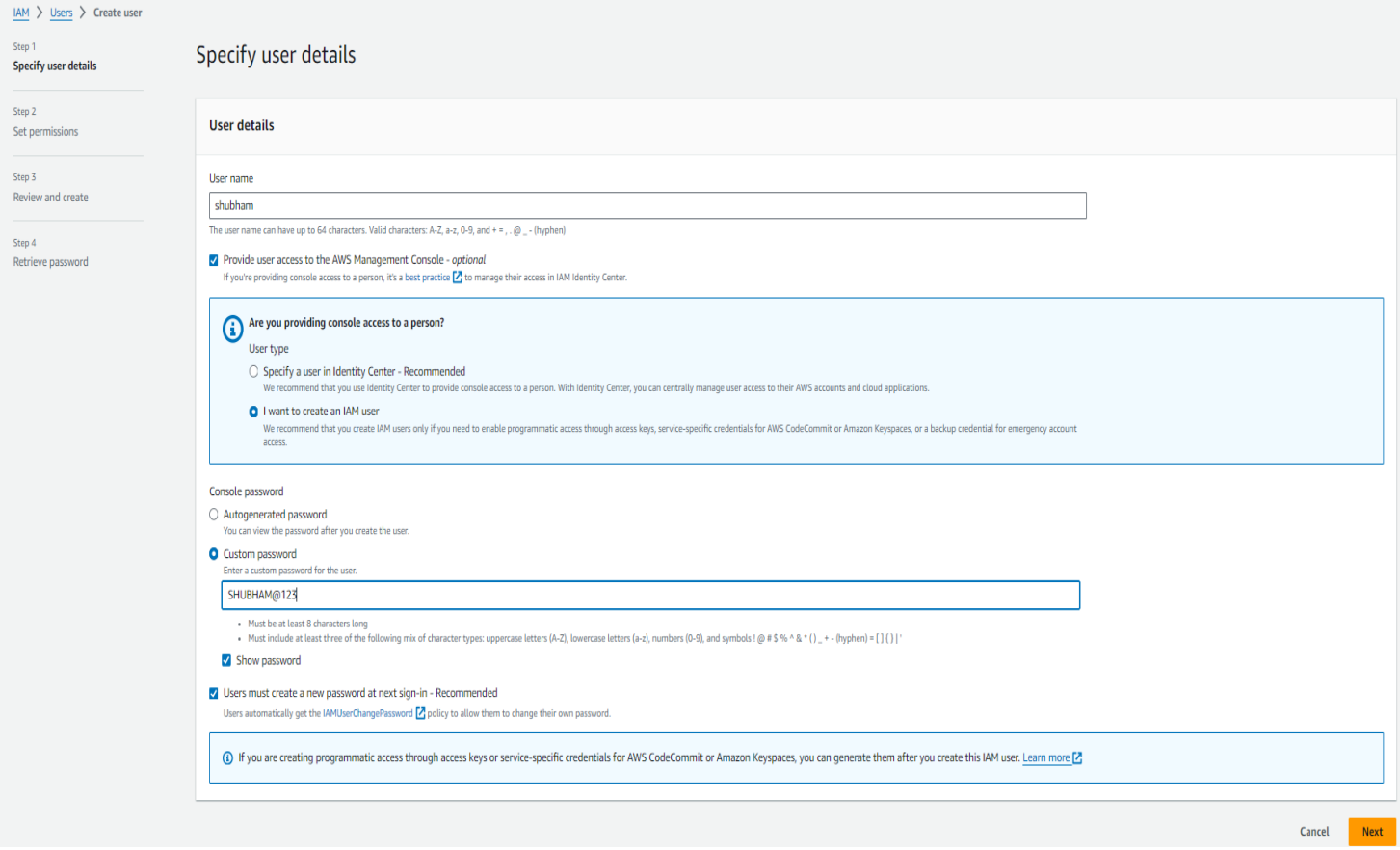
Create shubham user

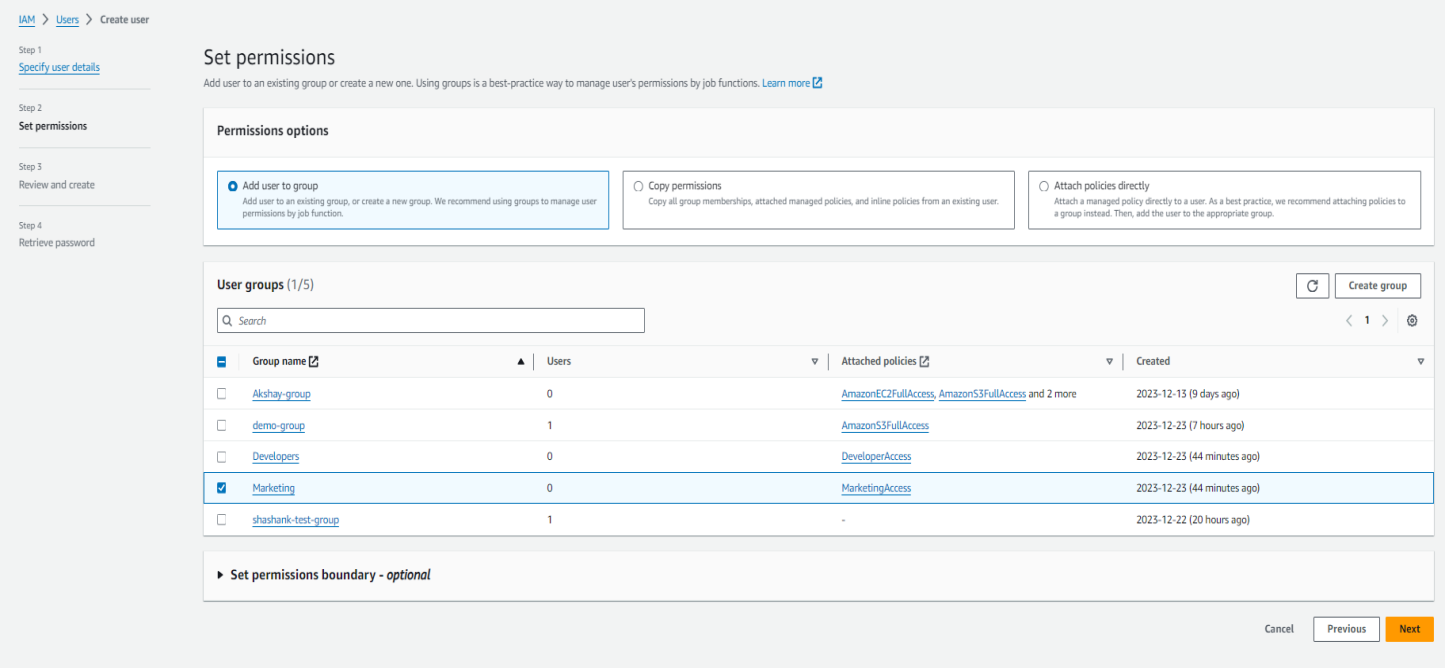
Click next

Add permission select marketing

Click next

Click create user





Step 8- Create IAM user for developer

Go to IAM console

Click to users

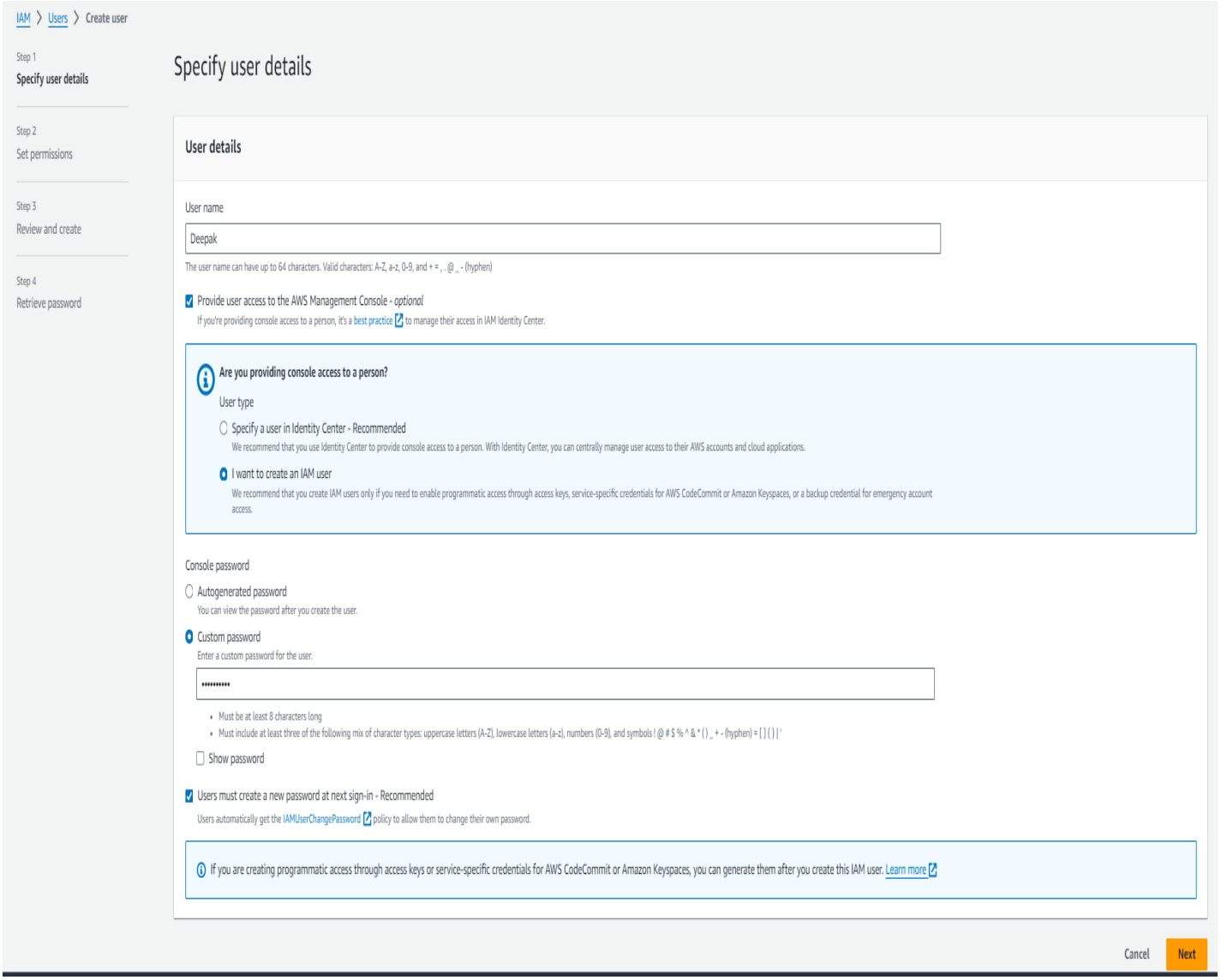
Create deepak user

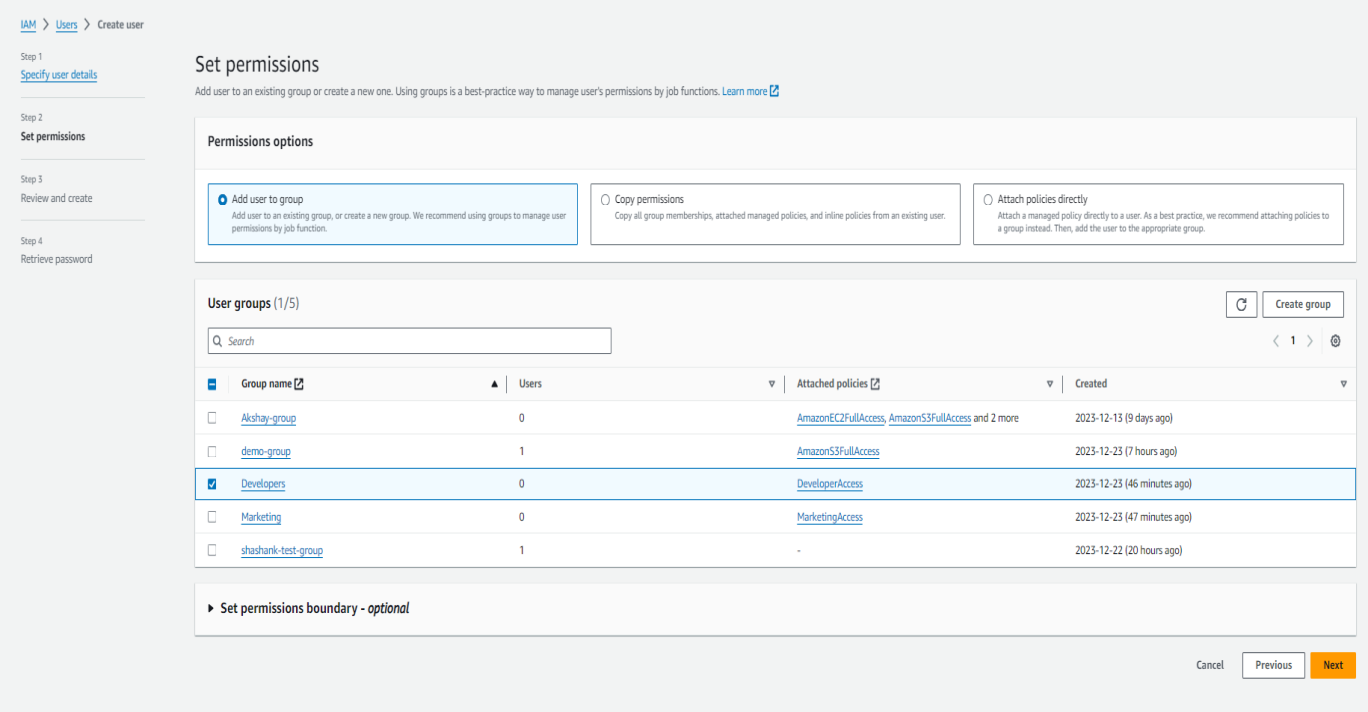
Click next

Add permission select marketing

Click next

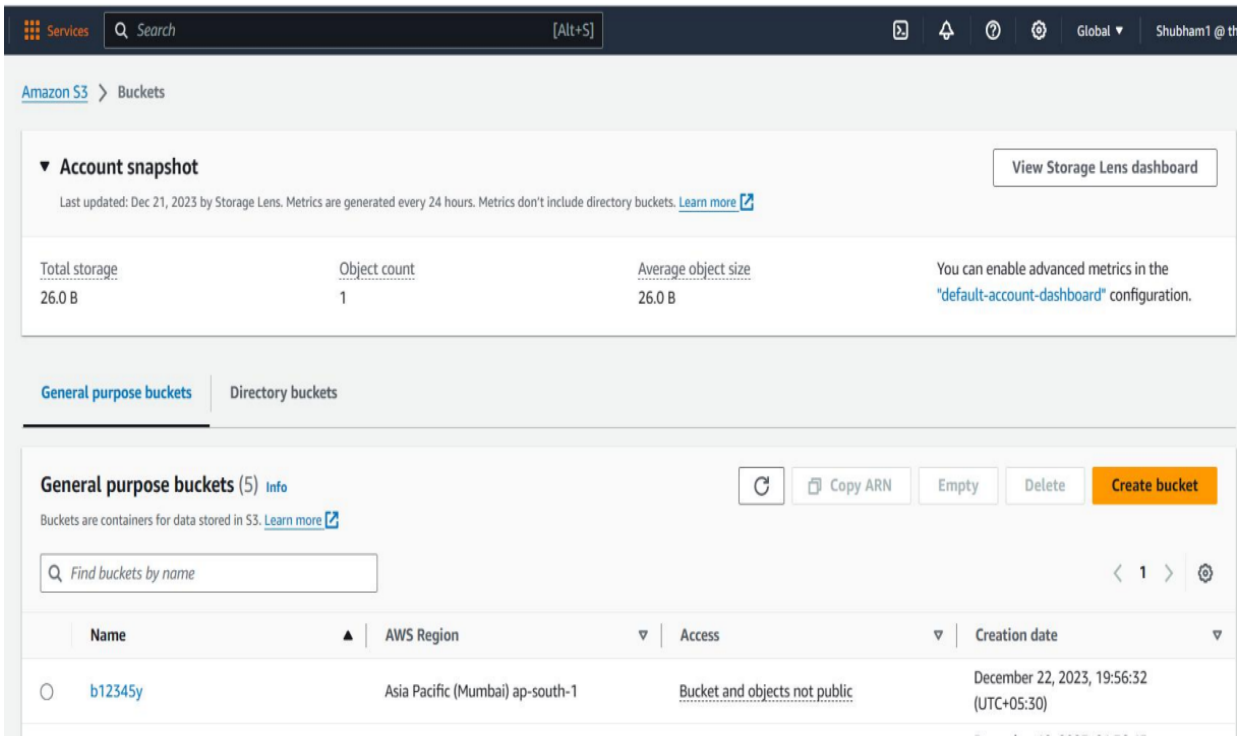
Click create user

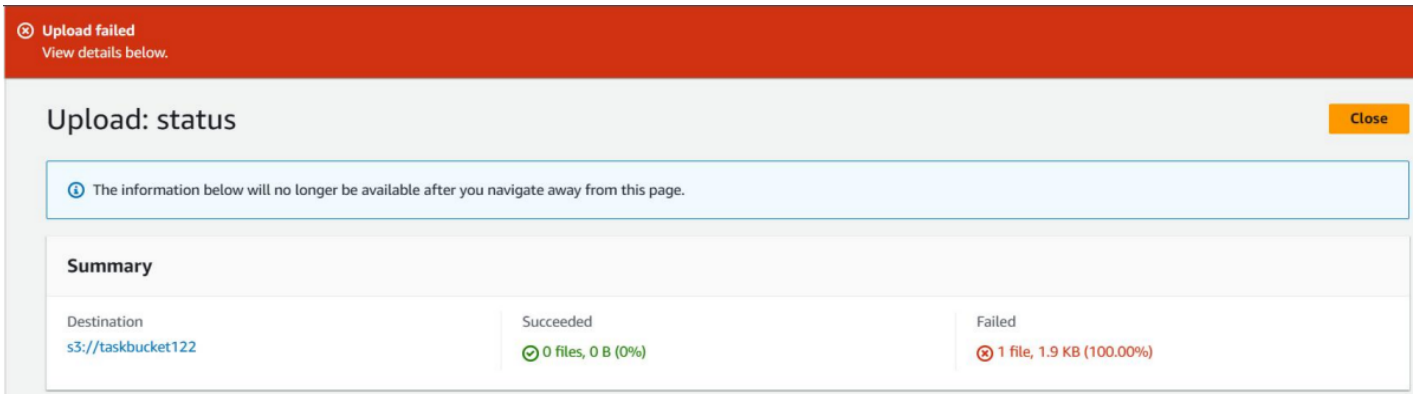




Step 9- Testing for shubham user

Shubham (marketing team) and he only have read only permission so it fail to create bucket and upload the files





In case of Deepak(Developer team) and he have read and write permission

So he create bucket and uplaod the files