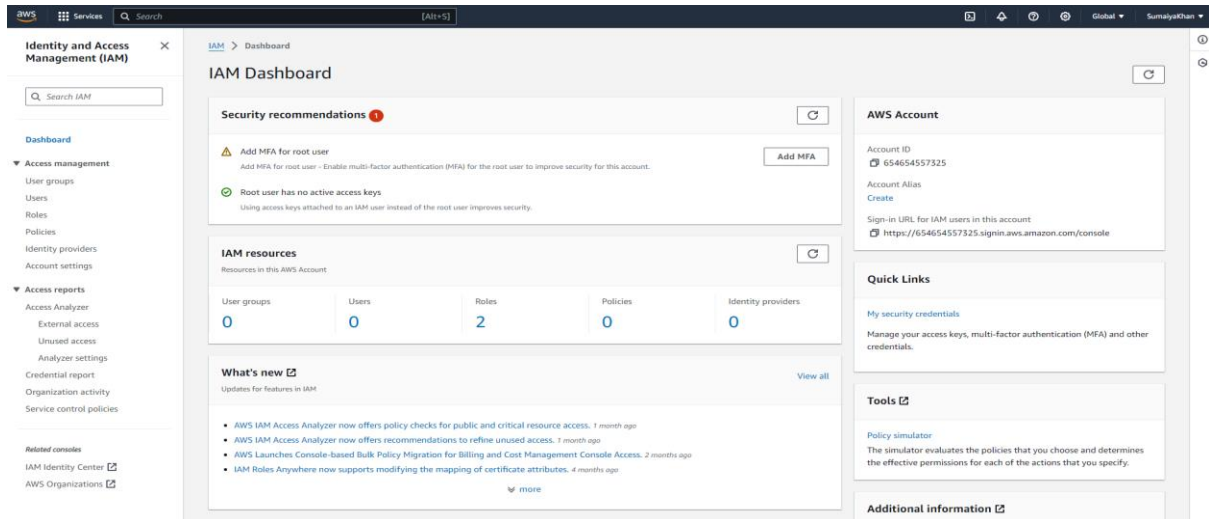


Practical 3 –

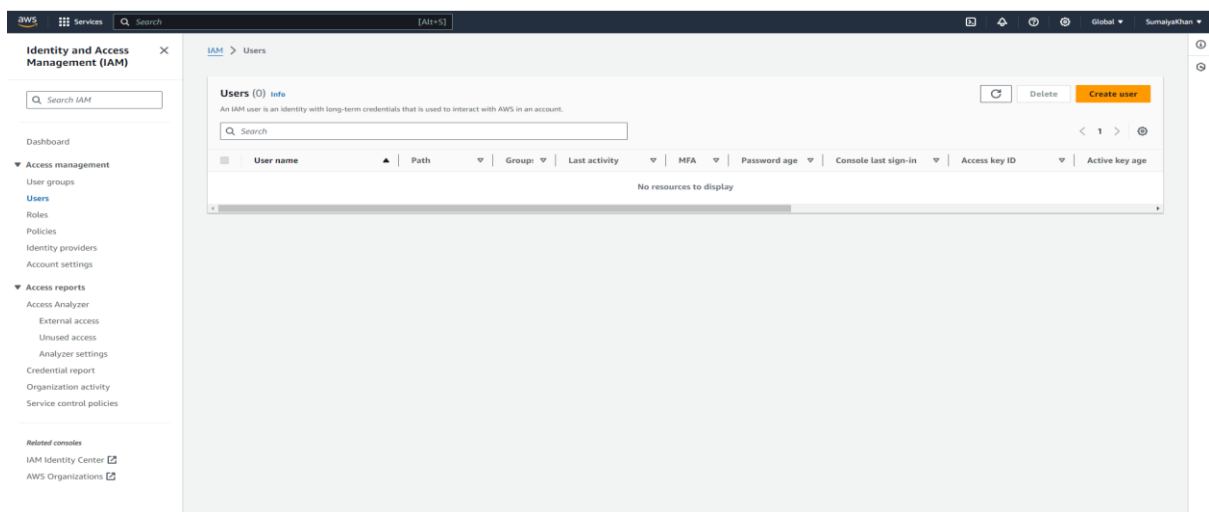
Name: Khan Sumaiya

Roll No: A031

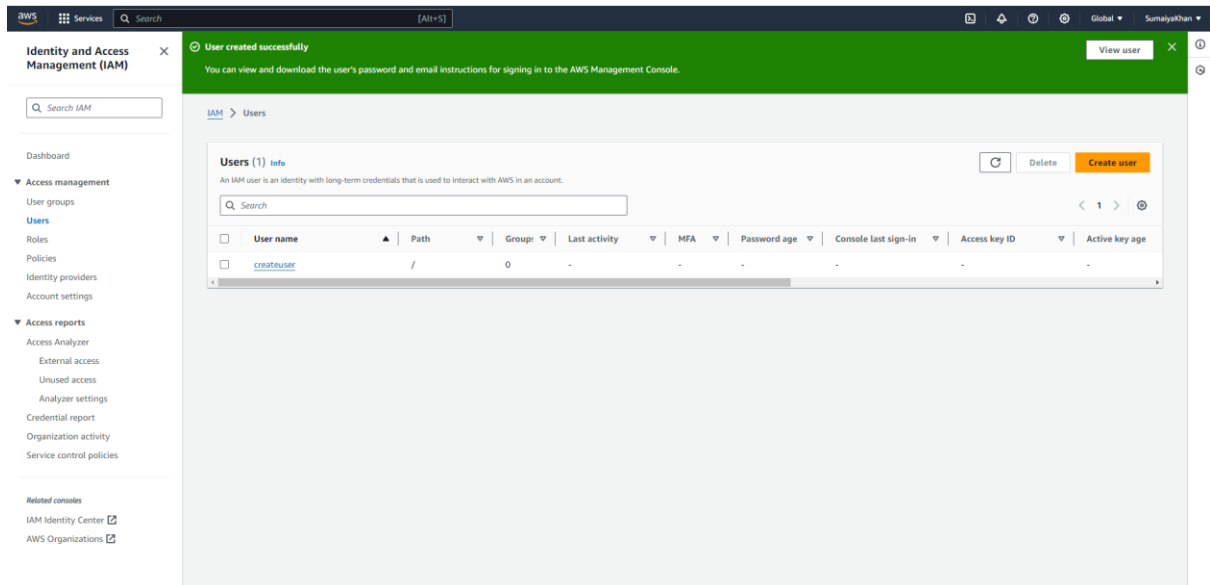
Select IAM from services



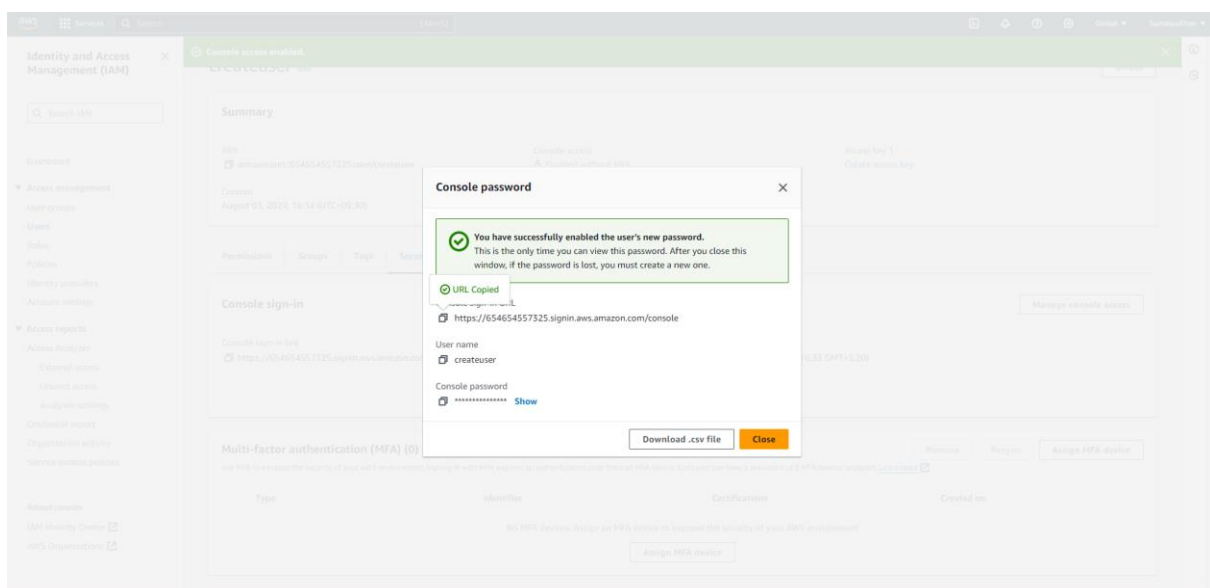
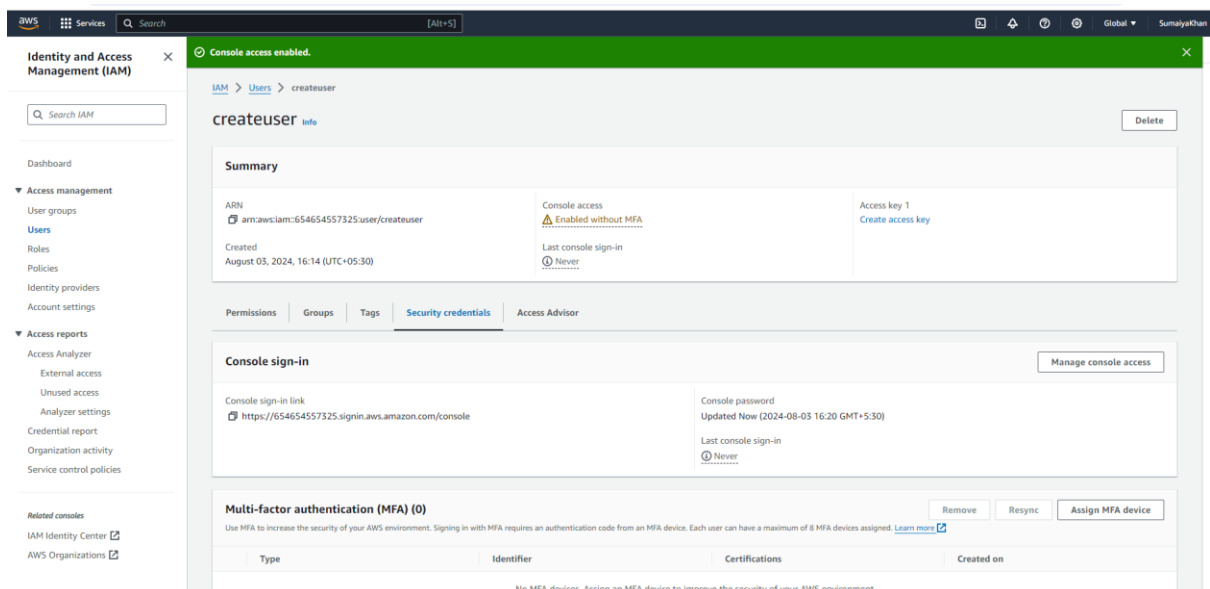
click on create user



User Created



Select myuser> enable access > password



On new incognito paste the copied url and then password and login

Try the new sign in UI
See our new improved Amazon Web Services sign in experience before we officially launch. [Enable new sign in](#)

aws

Sign in as IAM user

Account ID (12 digits) or account alias
654654557325

IAM user name
createuser

Password

☐ Remember this account

[Sign in](#)

[Sign in using root user email](#)
[Forgot password?](#)

Amazon Lightsail
Lightsail is the easiest way to get started on AWS
[Learn more »](#)

English

Terms of Use Privacy Policy © 1999-2024, Amazon Web Services, Inc. or its affiliates.

Services Search [Alt+S] Stockholm createuser @ 6546-5435

Console Home

[Reset to default layout](#) [+ Add widgets](#)

Recently visited Info

No recently visited services

Explore one of these commonly visited AWS services.

[EC2](#) [S3](#) [RDS](#) [Lambda](#)

[View all services](#)

Applications (0) Info

Region: Europe (Stockholm)

eu-north-1 (Current Region) Find applications

< 1 >

Name	Description	Region	Originating account
Access denied			

[Go to myApplications](#)

Welcome to AWS

[Getting started with AWS](#)
Learn the fundamentals and find valuable information to get the most out of AWS.

[Training and certification](#)
Learn from AWS experts and advance your skills and knowledge.

AWS Health Info

No health data
You don't have permissions to access AWS Health.

Cost and usage Info

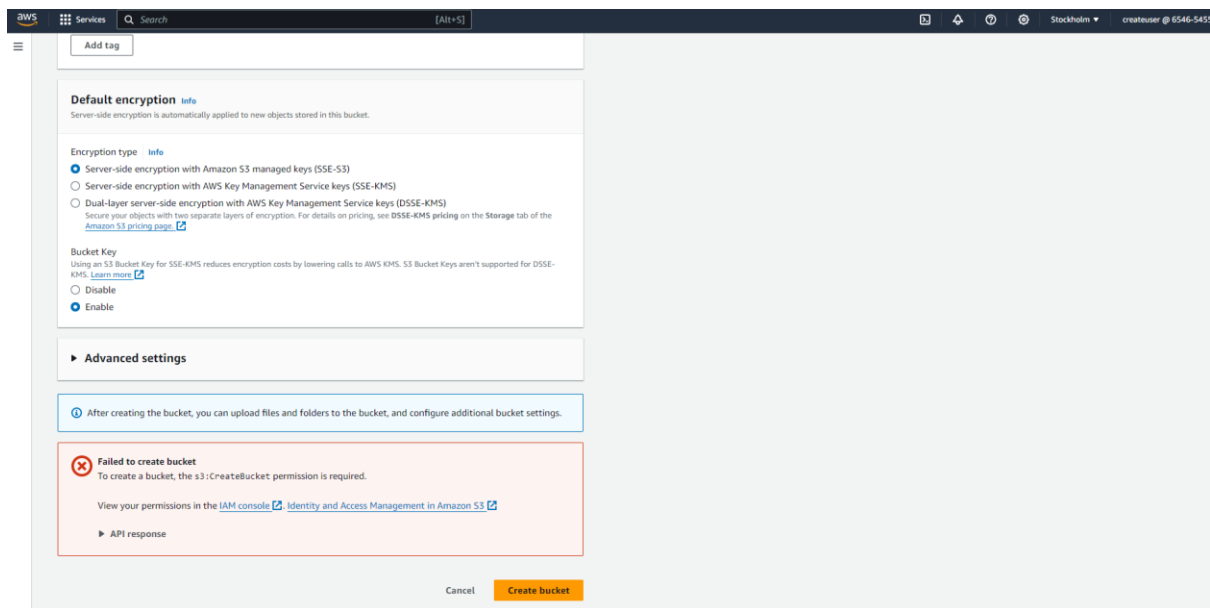
Current month costs
Access denied

Cost breakdown
Access denied

Forecasted month end costs
Access denied

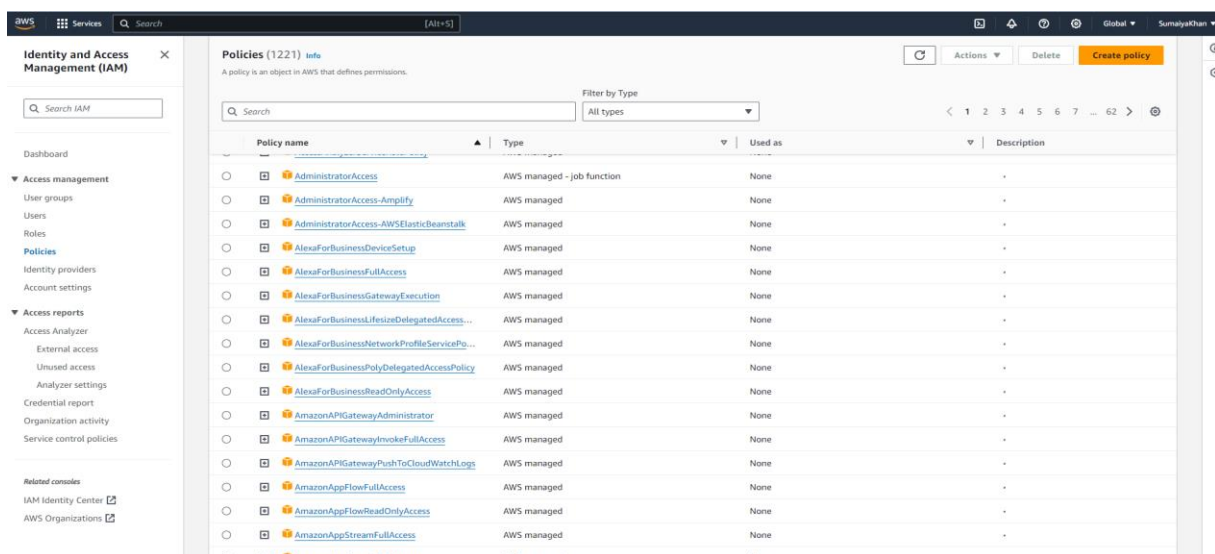
Savings opportunities
Access denied

Now lets create a bucket using S3, but bucket cannot be made because we haven't rootuser has not given access to admin(create user) so lets check

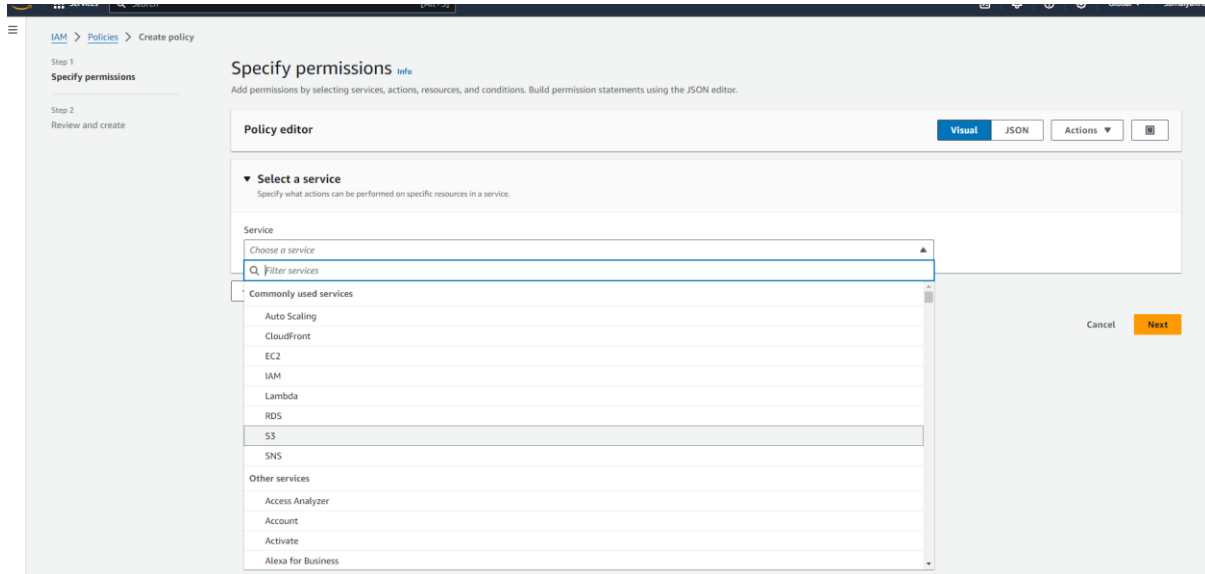


lets create policies from our original account

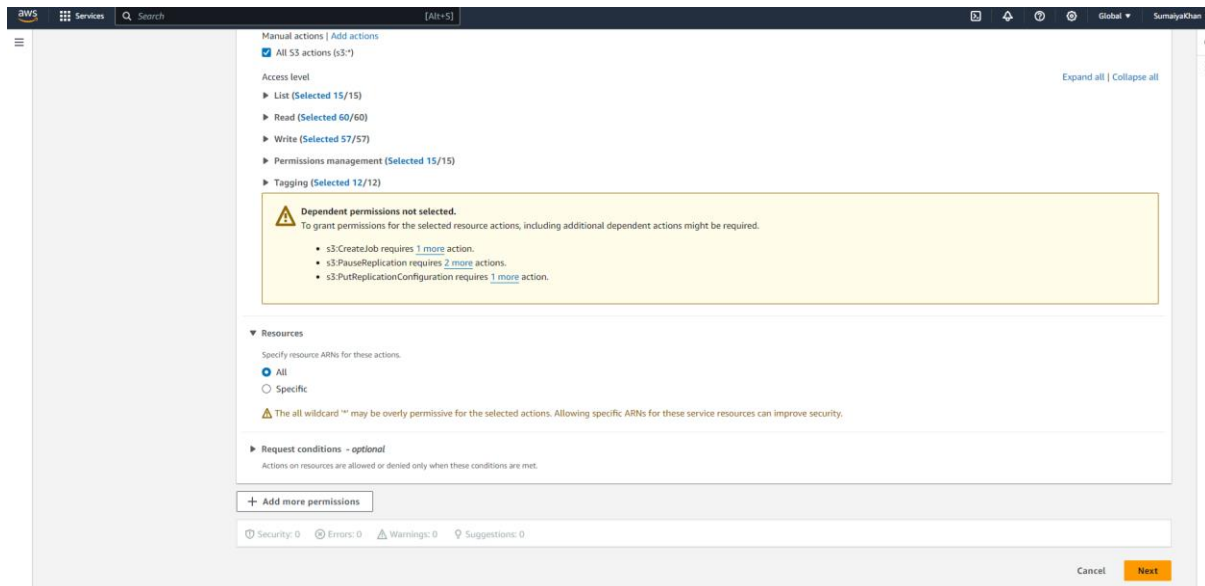
Create policies> click on policy



We get the above page. IN the “Visual” Section in “select a service”. Click on S3 to give access



Select checkbox for “All S3 actions”



In the JSON section, change the name to the user name

Review and create [info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and ""-@_>-<- characters.

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and ""-@_>-<- characters.

Permissions defined in this policy [info](#) Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity base, user group, or role, attach a policy to it.

Allow (1 of 420 services) Show remaining 419 services

Service	Access level	Resource	Request condition
S3	Full access	All resources	None

Add tags - optional [info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag
You can add up to 50 more tags.

Cancel Previous Create policy

Give the policy a name and give a short description of the policy. Check the permissions defined for the policy. Then Click on create policy

Identity and Access Management (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

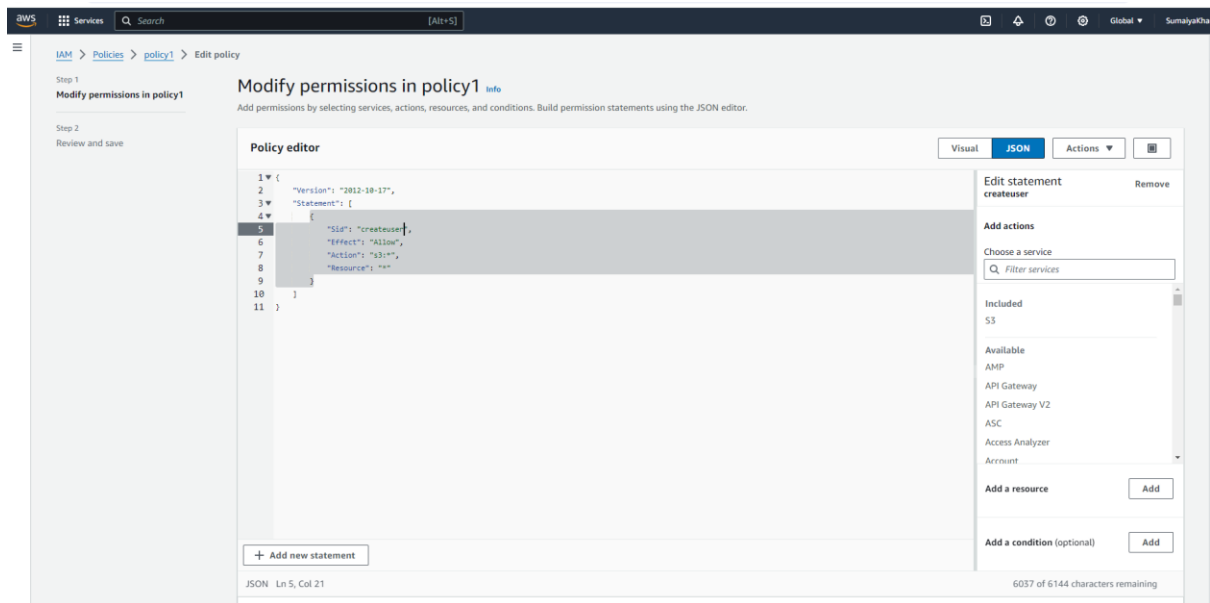
- [IAM Identity Center](#)
- [AWS Organizations](#)

Policies (1222) [info](#) Refresh Actions Delete Create policy

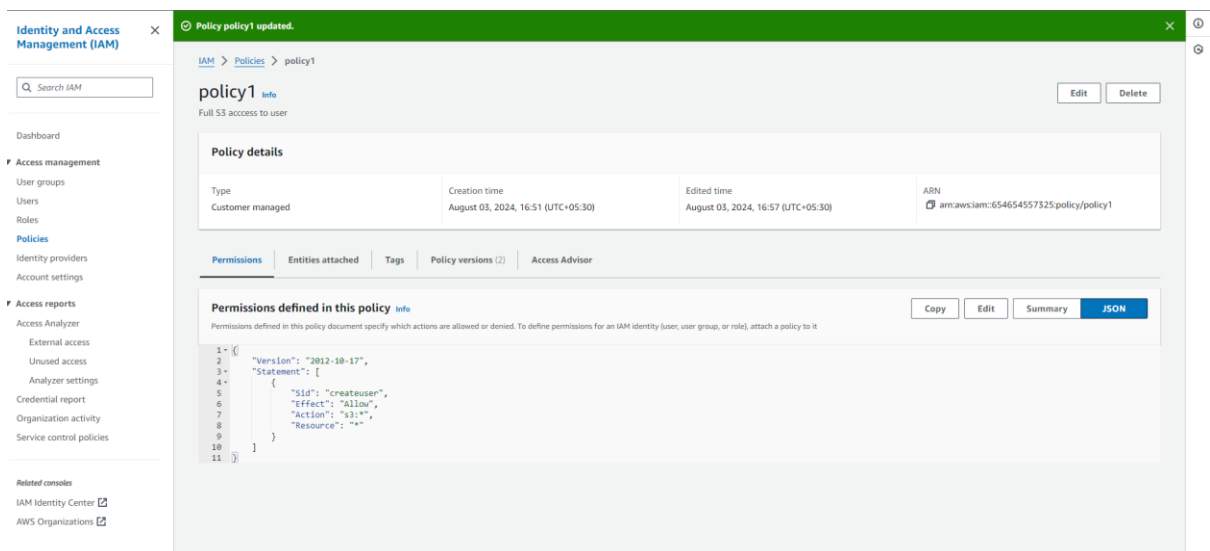
A policy is an object in AWS that defines permissions.

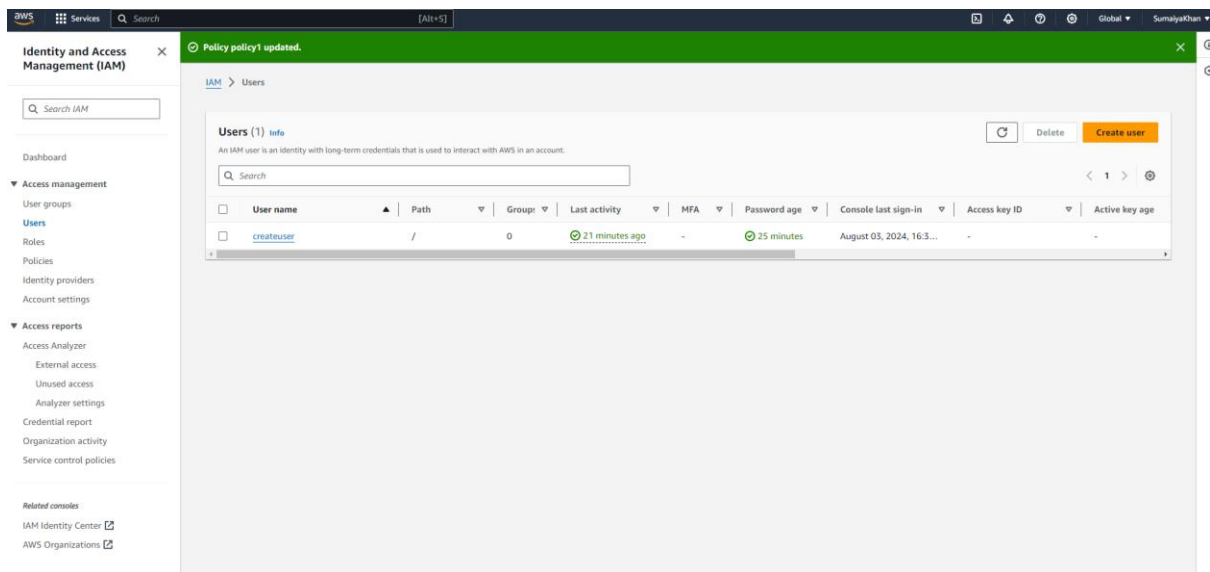
Filter by Type All types 1 match

Policy name	Type	Used as
<input type="radio"/> policy1	Customer managed	None

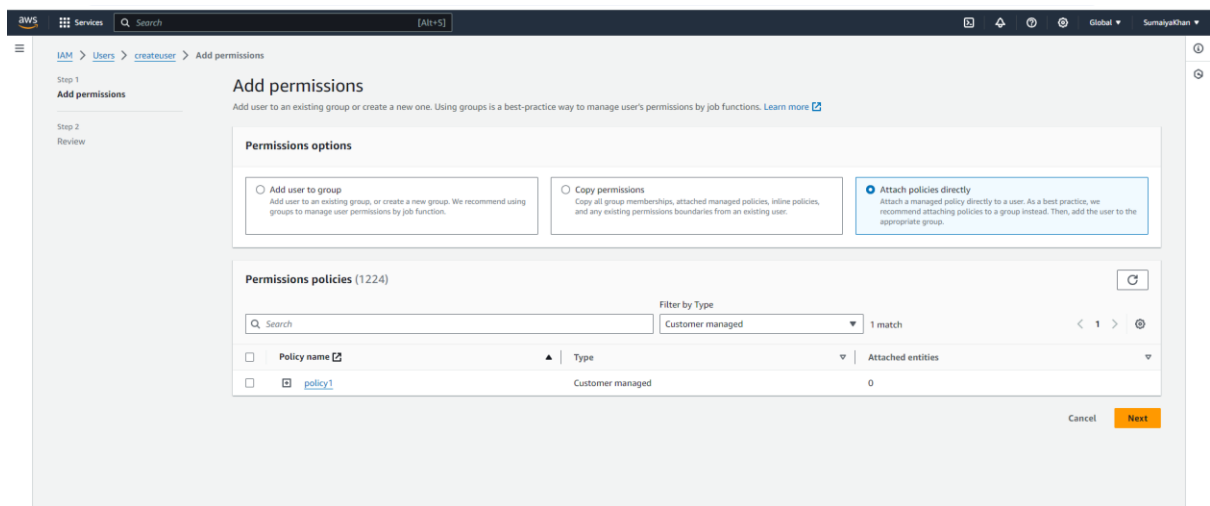


Can go and check JSON that user name is changed, in case policy need to be edited , select the policy, select edit, make the edits and update the policy.

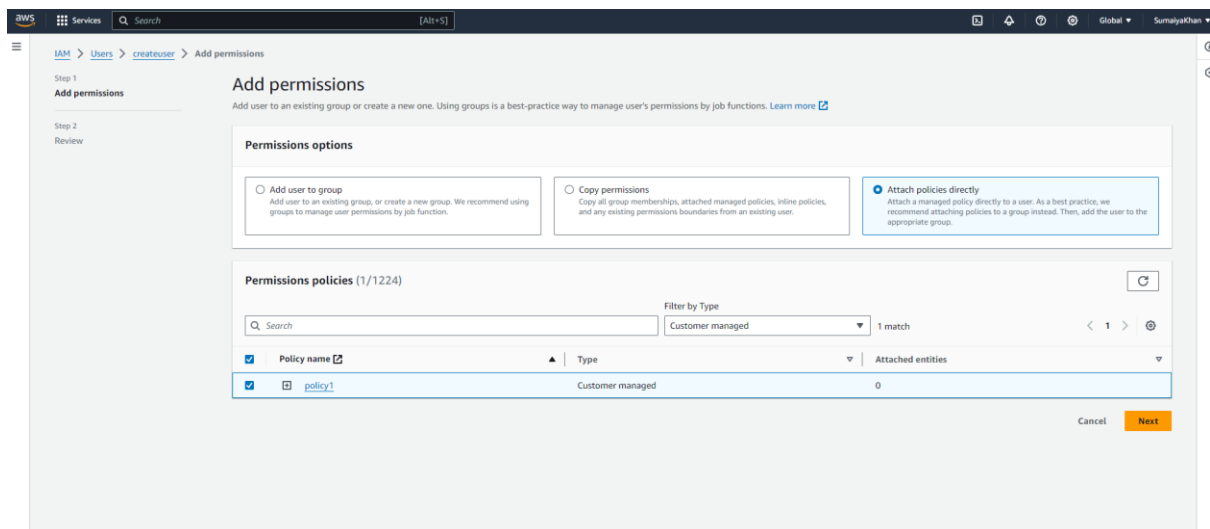




In the “Permission Policy”, select “add permissions” from drop down at right corner



Select policies created from above and attach policy directly



Check if the correct policy has been selected and then click on add permissions

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with sections like 'Access management' and 'Access reports'. The main content area is titled 'createuser' and has a green banner at the top stating '1 policy added'. Below this, the 'Permissions' tab is active, displaying a table of permissions policies. The table has columns for 'Policy name', 'Type', and 'Attached via'. One policy, 'policy1', is listed as 'Customer managed' and 'Attached via Directly'. There are buttons for 'Add permissions', 'Remove', and 'Filter by Type' at the top of the table. A 'Delete' button is also visible in the top right corner of the user details section.

Policy name	Type	Attached via
policy1	Customer managed	Directly

Then go back to incognito page click on create bucket this time the bucket will be created