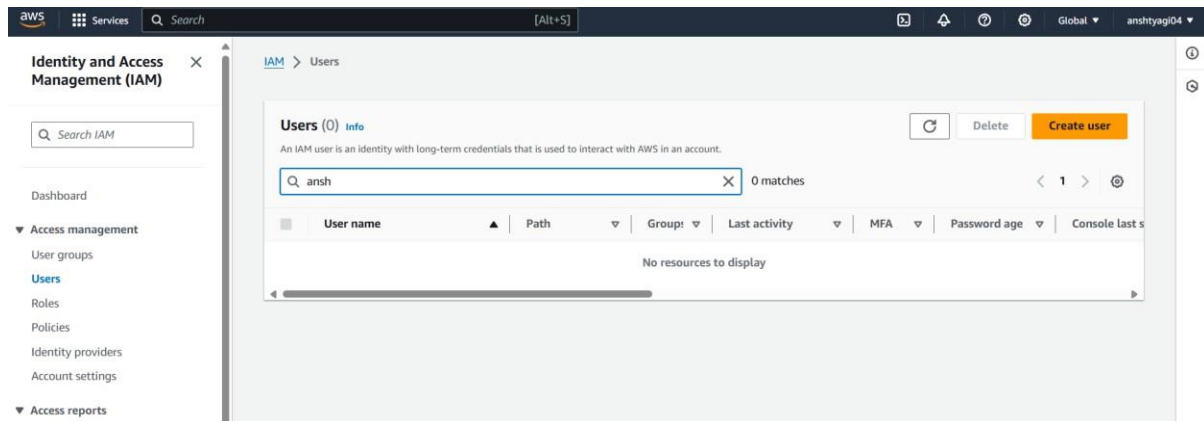


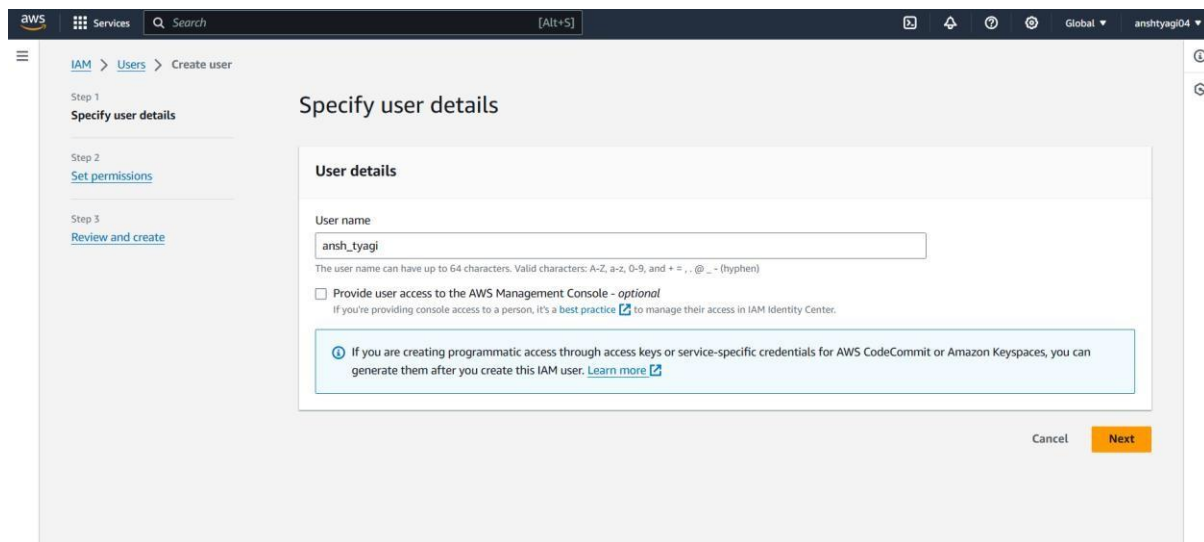
Himanshu Pal
A045
86062300021

IAM - Identity and Access Mangement

Step 1: Search for IAM. Click on it

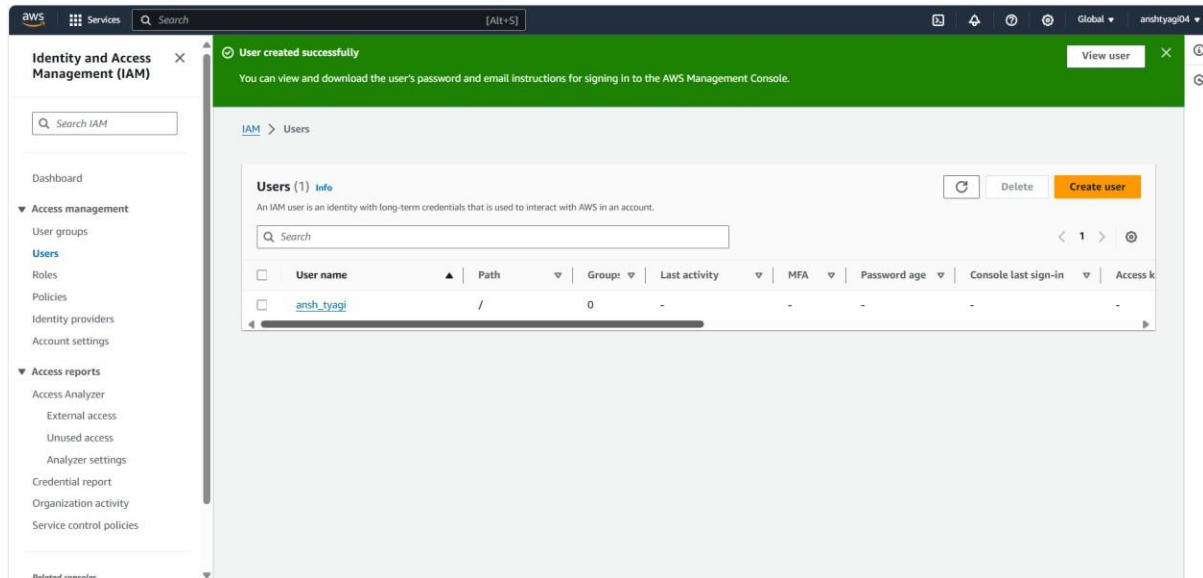


Step 2: Click on Users and Specify user details. Then Click on Create user.

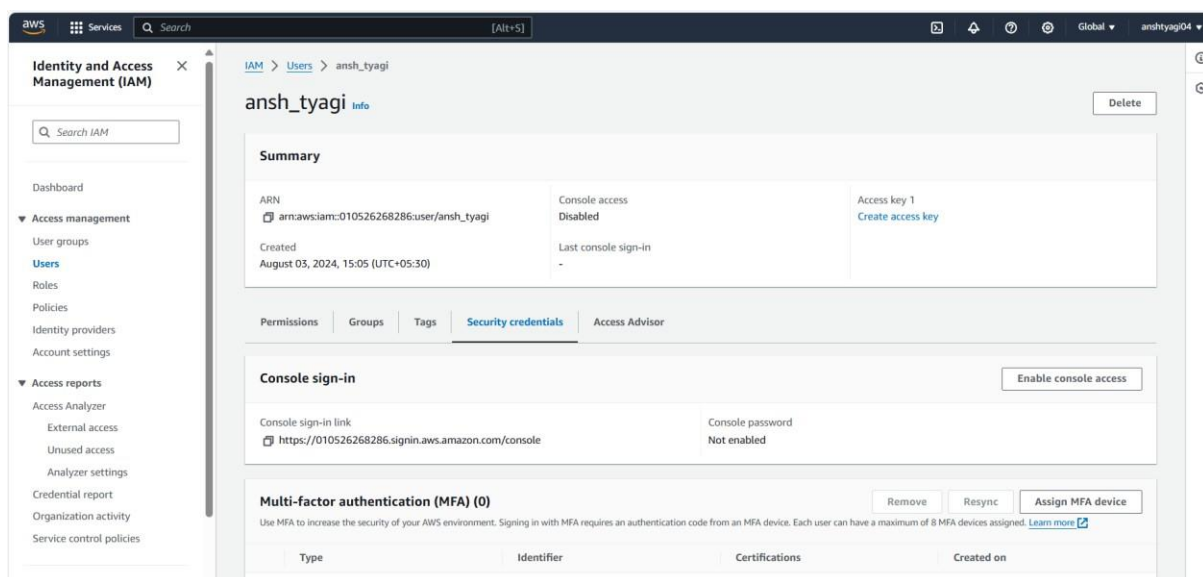


Step 3: Select Add user to group in Permission options.

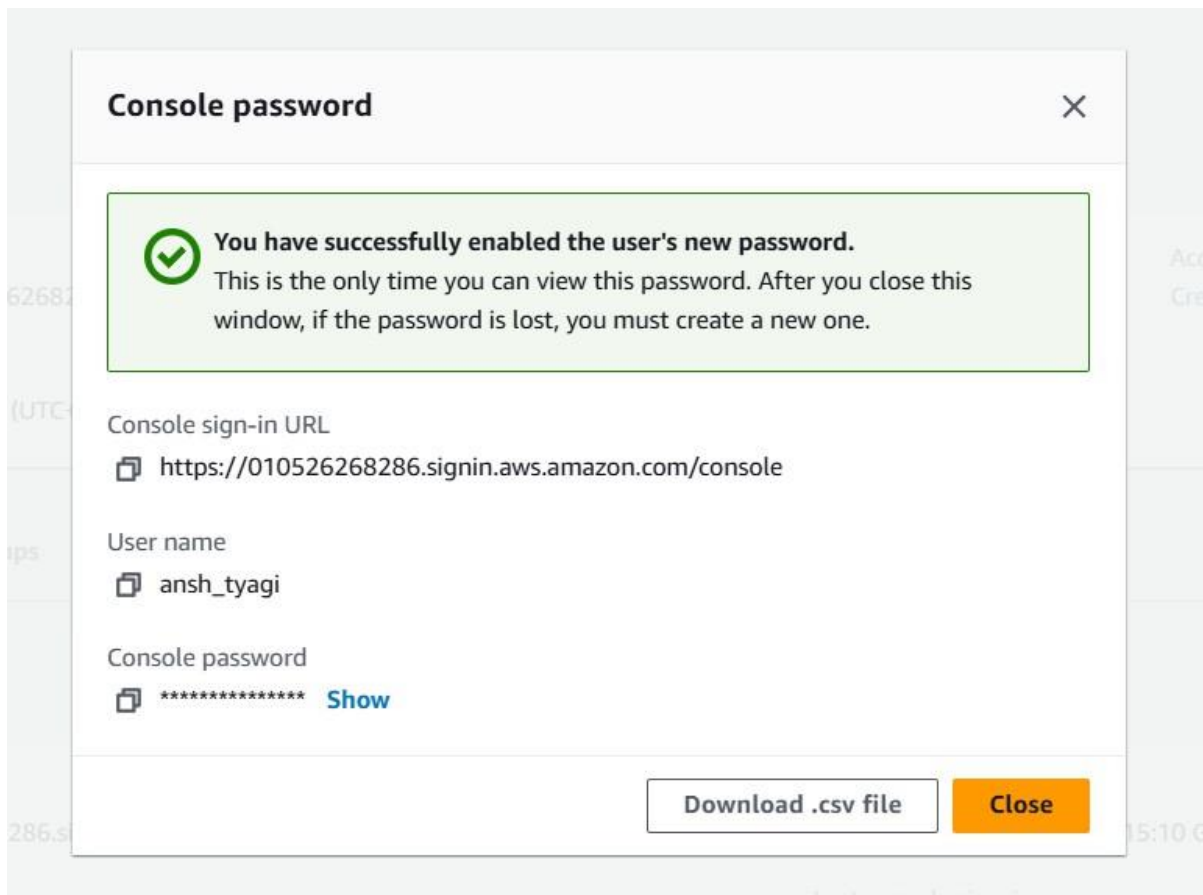
Step 5: User is created successfully.



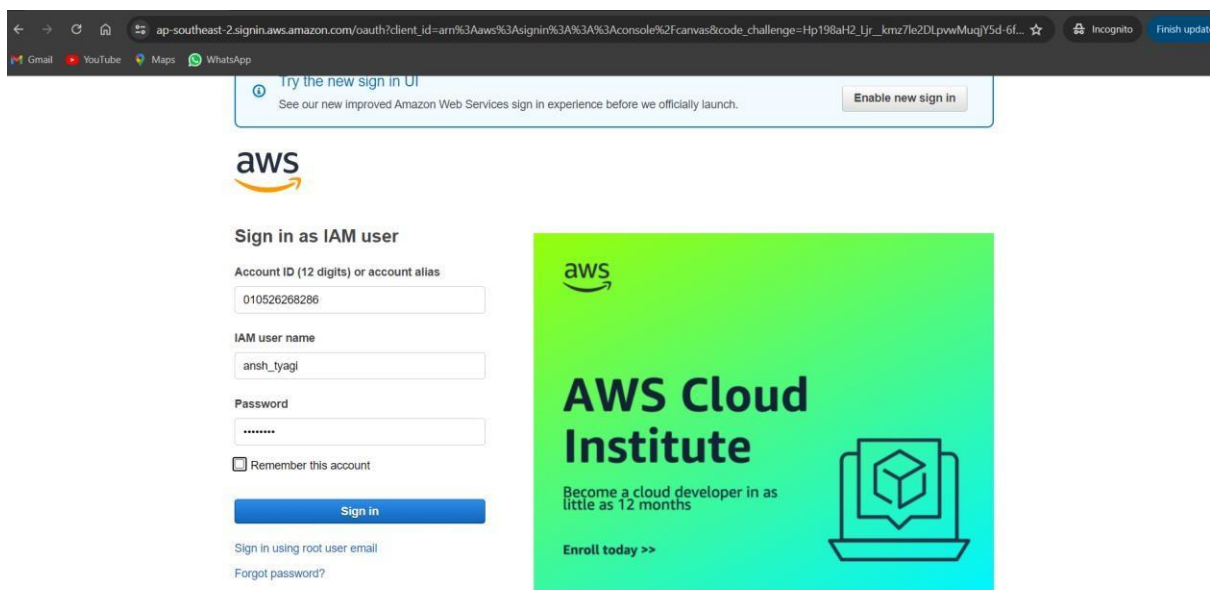
Step 6: Click on a user “ansh_tyagi” and go to Security Credentials C Select enable control access.

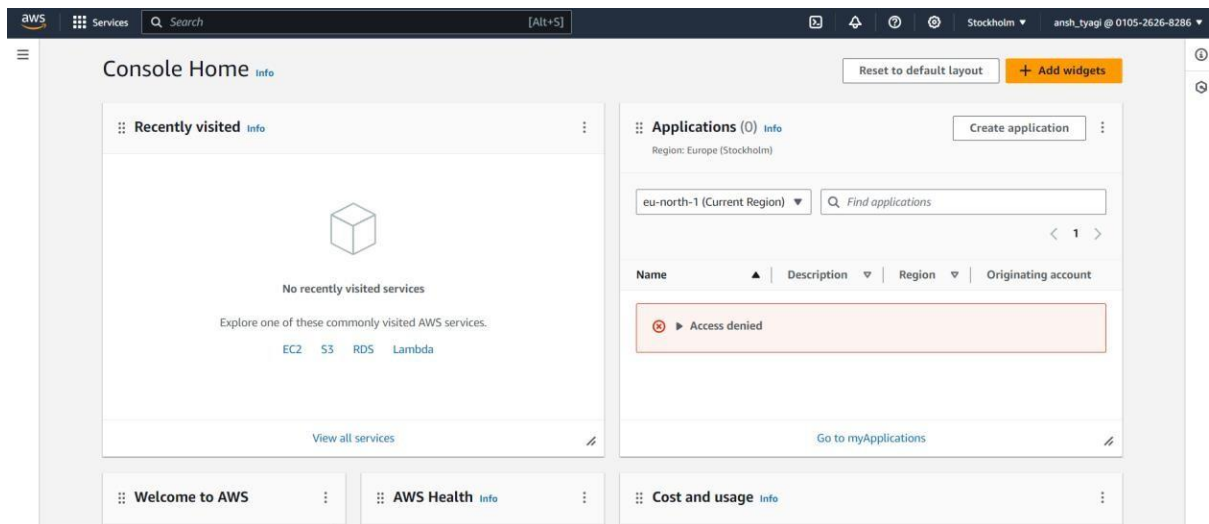


Step 7: Go for autogenerated password and it shows Console credentials. Then Download the .csv file which contains the credentials of the console.

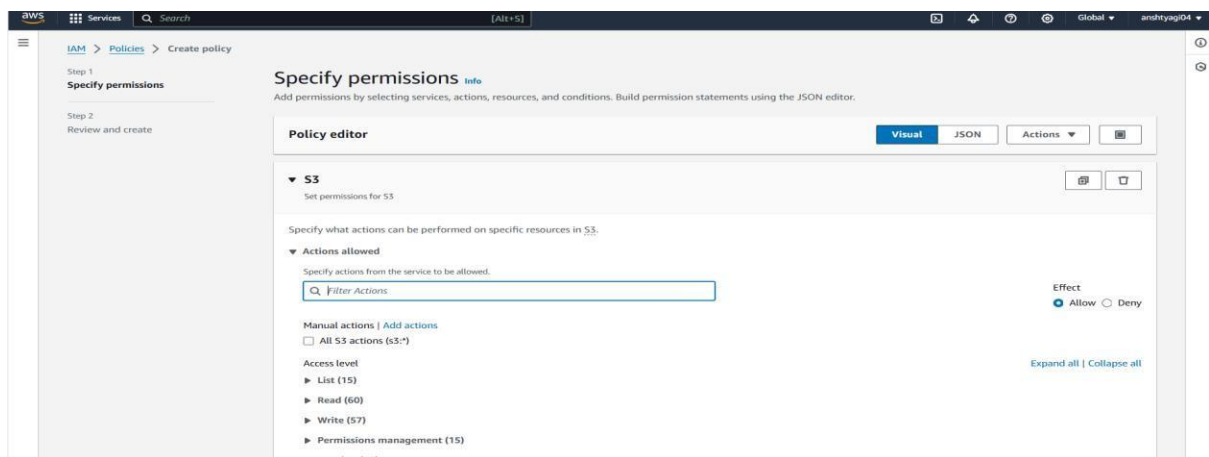
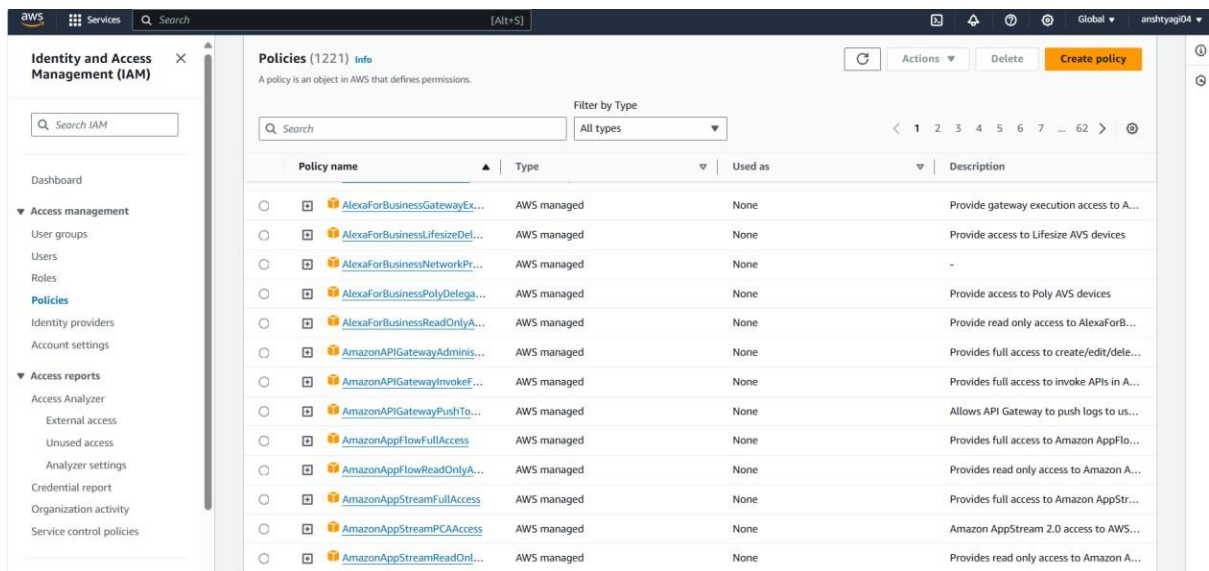


Step 8: Copy the Console sign-in URL, open the incognito window, and paste it on it. Sign in with your username and password and we are signed in.





Step 9: Now Click on Policies and then select Create Policy.



Step 10: Create policy and named as “policy12”

The screenshot shows the 'Review and create' step in the AWS IAM console. The policy name is 'policy12'. The permissions section shows 'Full access' for 'All resources' with 'None' request conditions. The 'Add tags' section is empty.

Policy details

Policy name:

Description - optional:

Permissions defined in this policy

Search:

Allow (1 of 420 services)

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

Add tags - optional

No tags associated with the resource.

Step 11: Policy is created Successfully.

The screenshot shows the 'Policy policy12 created' notification. The 'Policies' list shows 'policy12' with 'Full access' permissions.

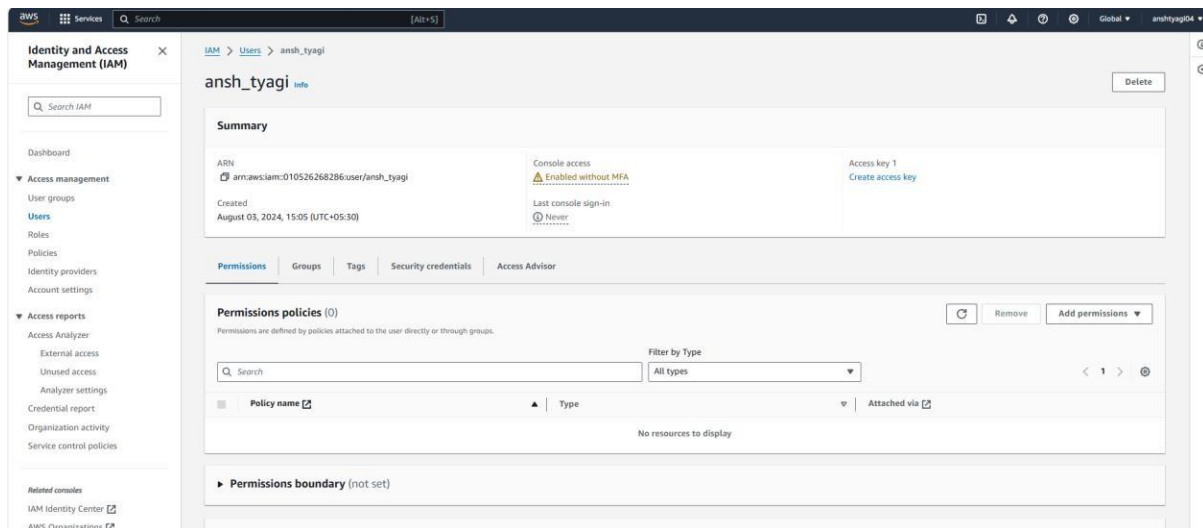
Policy policy12 created.

Policies (1222)

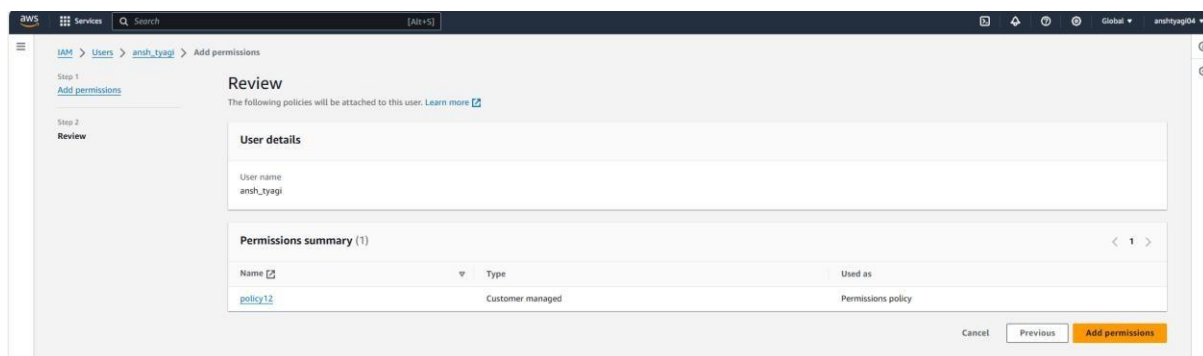
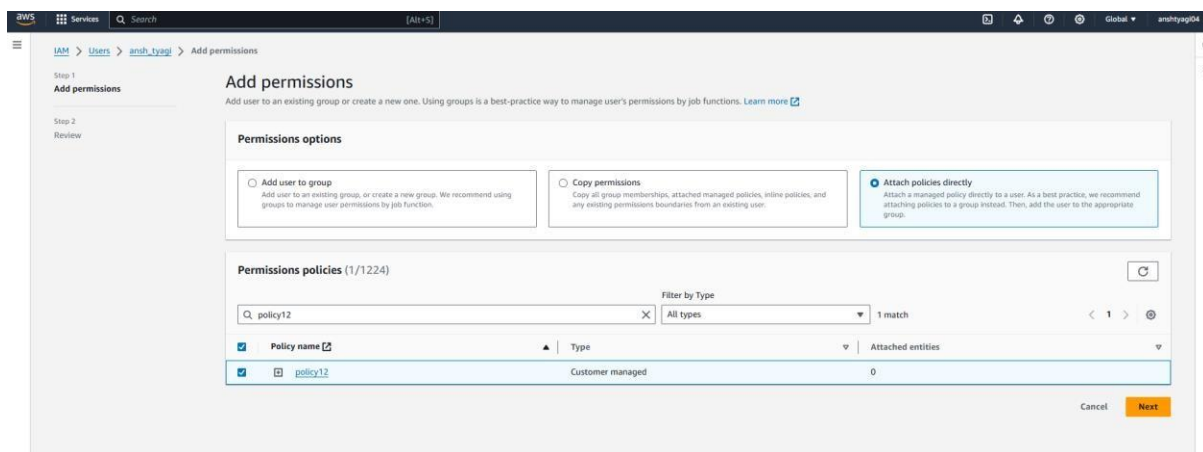
Filter by Type: All types | 1 match

Policy name	Type	Used as	Description
policy12	Customer managed	None	

Step 12: Click on Users again and then select Add Permissions option



Step 13: Find “policy12” in the add permissions tab and click on next > Add Permissions



Step 14: “Policy12” is added successfully

The screenshot shows the AWS IAM console interface. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Related consoles. The main content area displays the 'ansh_tyagi' user profile. A green banner at the top indicates '1 policy added'. The 'Summary' section shows the user's ARN, creation date, and console access status. The 'Permissions' tab is active, showing a table of permissions policies. The table lists 'policy12' as a customer-managed policy attached directly to the user. The 'Permissions boundary' is set to '(not set)'. A button 'Generate policy based on CloudTrail events' is visible at the bottom.

Policy name	Type	Attached via
policy12	Customer managed	Directly

Step 15: Go to the Amazon S3 dashboard and Click Create Bucket.

The screenshot shows the Amazon S3 console interface. The left sidebar contains navigation links for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings, Storage Lens, and Feature spotlight. The main content area displays the 'General purpose buckets' section. A table lists the existing bucket 'mybucketprac2'. A 'Create bucket' button is visible in the top right corner of the bucket list.

Name	AWS Region	IAM Access Analyzer	Creation date
mybucketprac2	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	August 2, 2024, 12:12:09 (UTC+05:30)

Step 16: Create bucket as “mybucketsec”

aws

Services

Search

[Alt+S]

Stockholm

ansh_tyagi @ 0105-2626-8286

Amazon S3 > Buckets > Create bucket

Create bucket info

Buckets are containers for data stored in S3.

General configuration

AWS Region

Europe (Stockholm) eu-north-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 - New

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

mybucketsec

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

Step 17: Bucket is Created Successfully using S3.

aws

Services

Search

[Alt+S]

Stockholm

ansh_tyagi @ 0105-2626-8286

Successfully created bucket "mybucketsec"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Amazon S3 > Buckets

Account snapshot - updated every 24 hours All AWS Regions

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

[View Storage Lens dashboard](#)

General purpose buckets

Directory buckets

General purpose buckets (2) info All AWS Regions

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Buckets are containers for data stored in S3.

☐

mybucketprac2

Asia Pacific (Mumbai) ap-south-1

[View analyzer for ap-south-1](#)

August 2, 2024, 12:12:09 (UTC+05:30)

☐

mybucketsec

Europe (Stockholm) eu-north-1

[View analyzer for eu-north-1](#)

August 3, 2024, 15:35:40 (UTC+05:30)