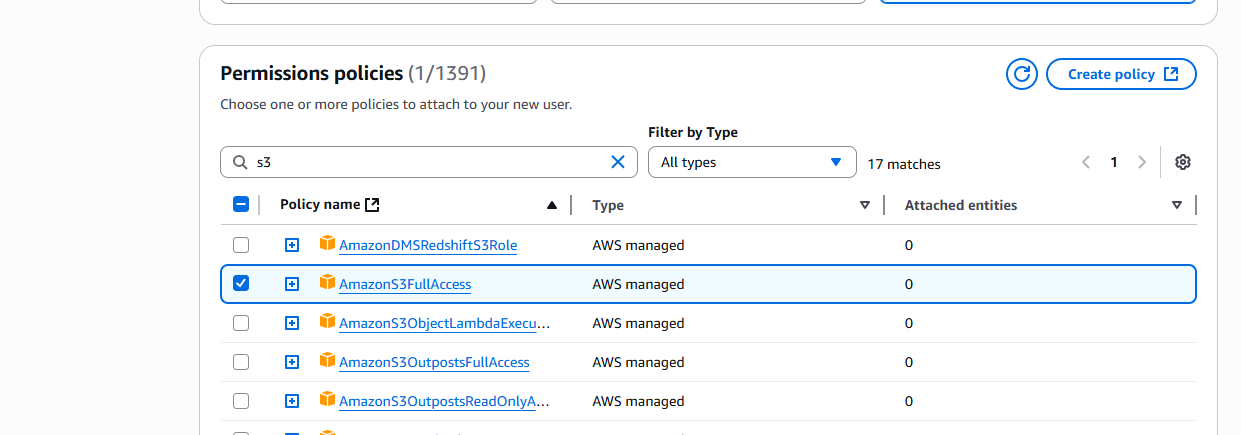
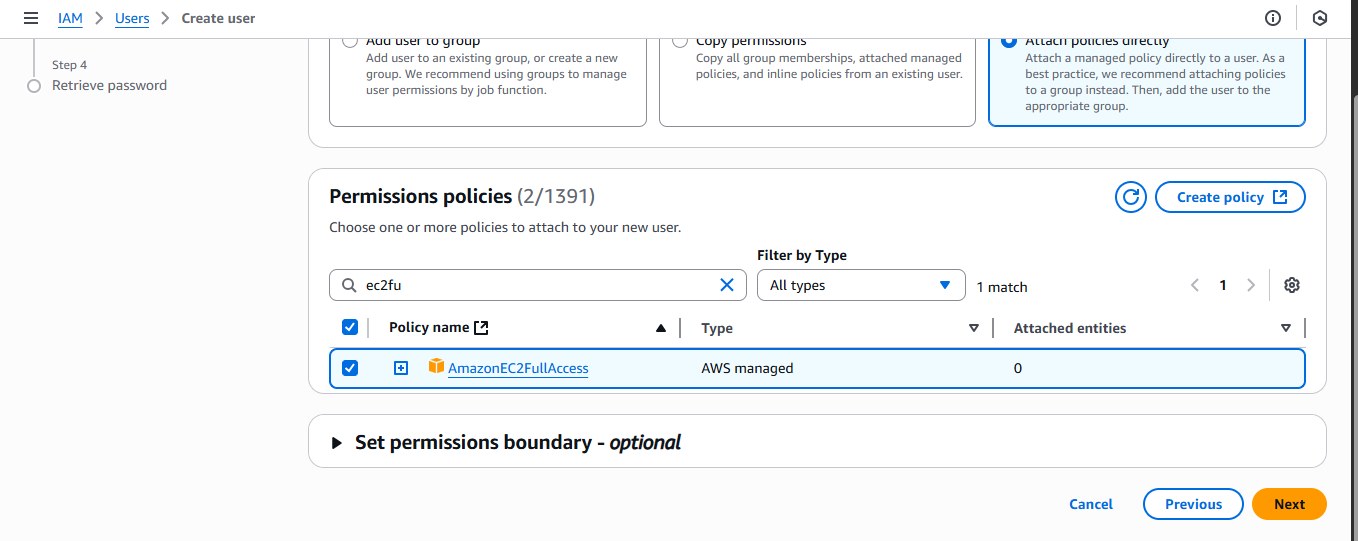
# IAM Daily task 1

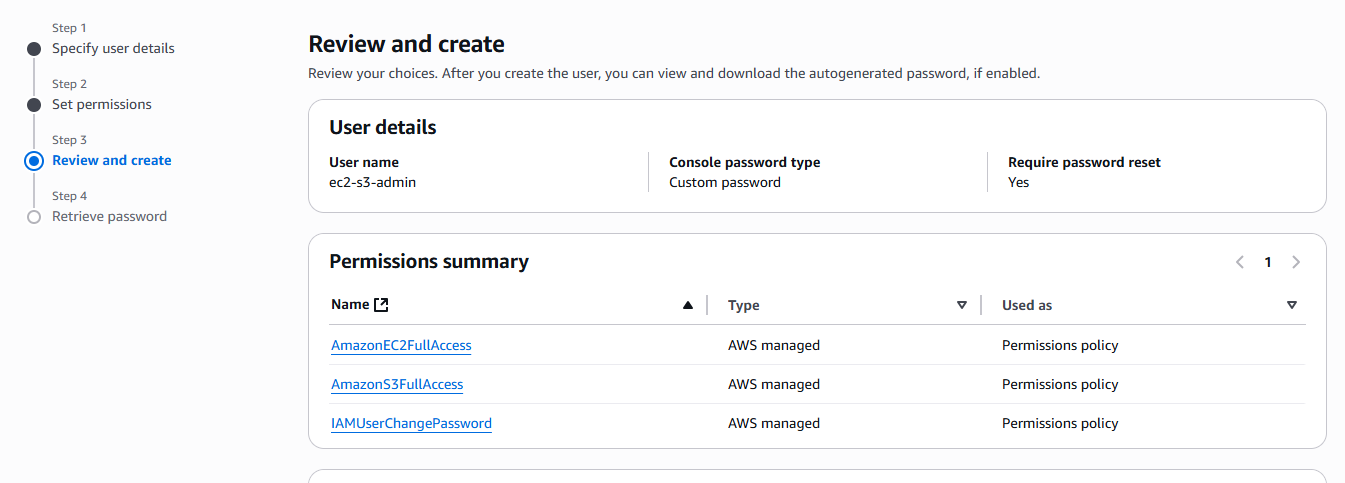
1. Create one IAM user and assign EC2 and S3 full access roles.

* Go to AWS ec2 then open a serach bar and enter **IAM.**
* Then create a user.
* Gave a name to the user **ec2-s3-admin.**
* Then gave provide access console aws.
* Then auto generate the password. This will help uh for the accesskey and secreat key.
* Then gave permisson step.
* Choose **Attaching existing polices.**
* Open a serach bar and >>
* **ec2 full access**
* **S3 full access**

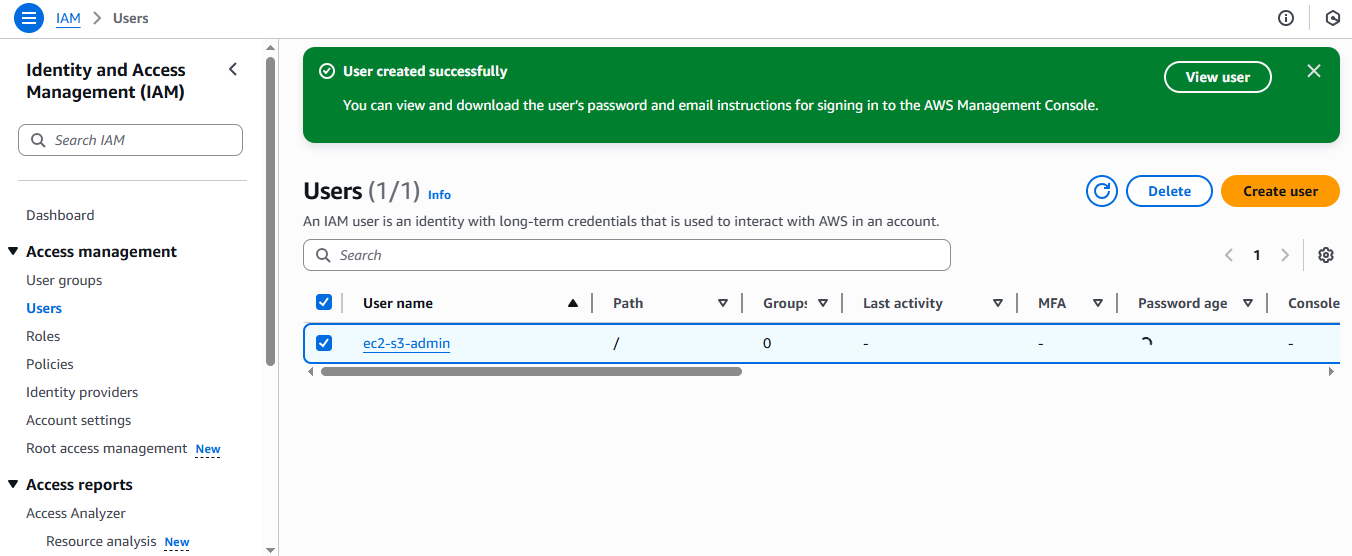




Review:

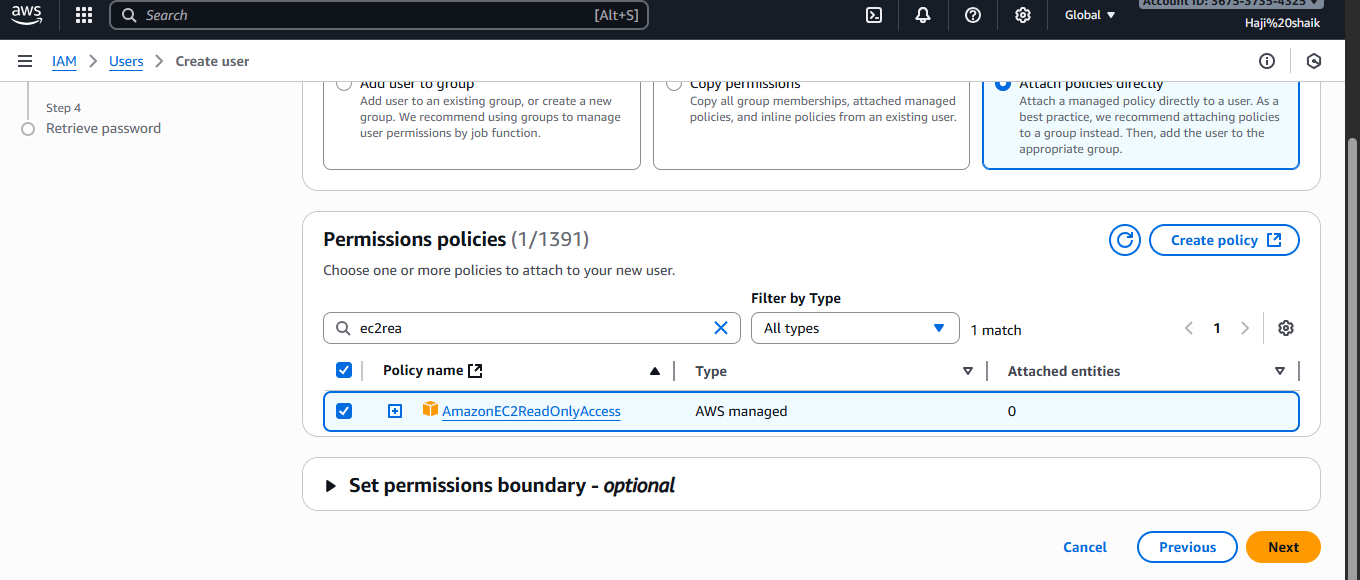


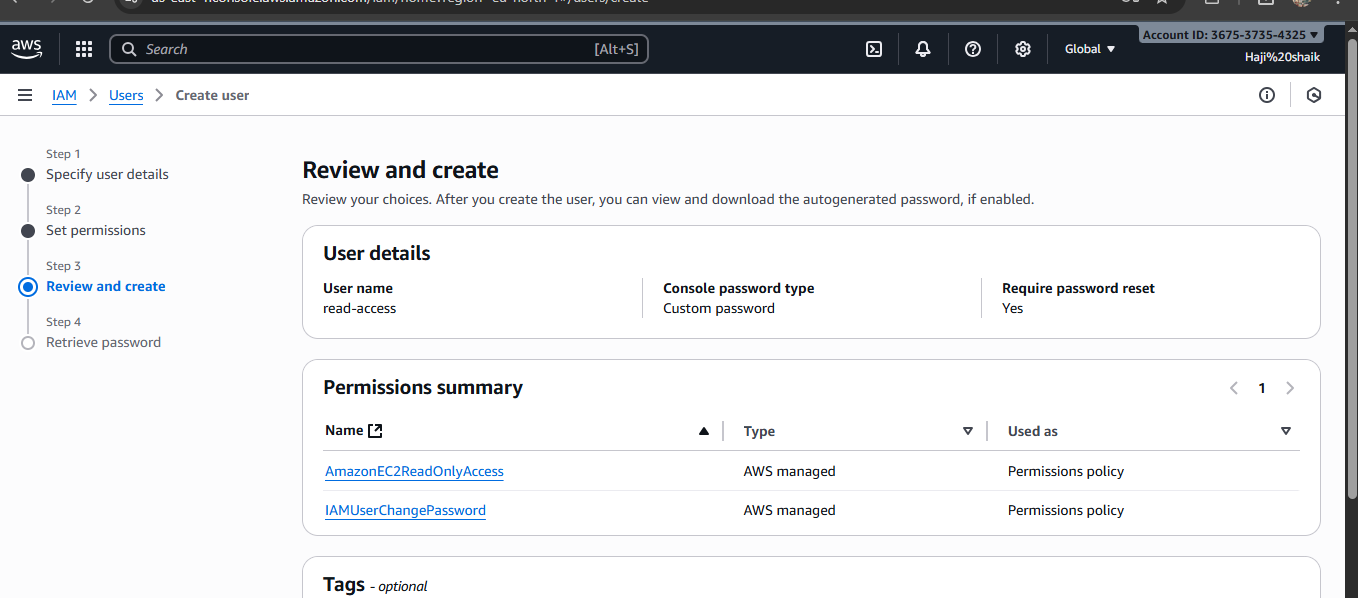
User created successfully:

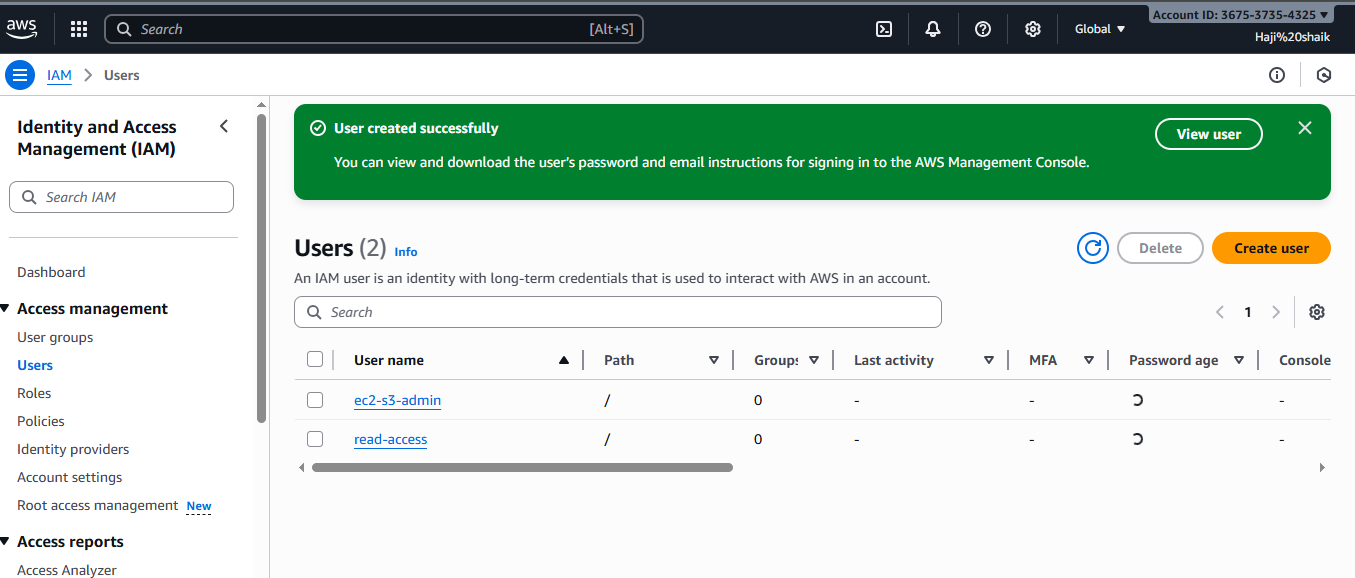


1. Create one group in IAM and assign read access for EC2.

* Go to AWS ec2 then open a serach bar and enter **IAM.**
* Then create a user.
* Gave a name to the user **read access.**
* Then gave provide access console aws.
* Then create password.
* Click the next page.
* Then existing permissons.
* Then **ec2read acess only.**
* Review
* And create user successfully:
* Here the results are:

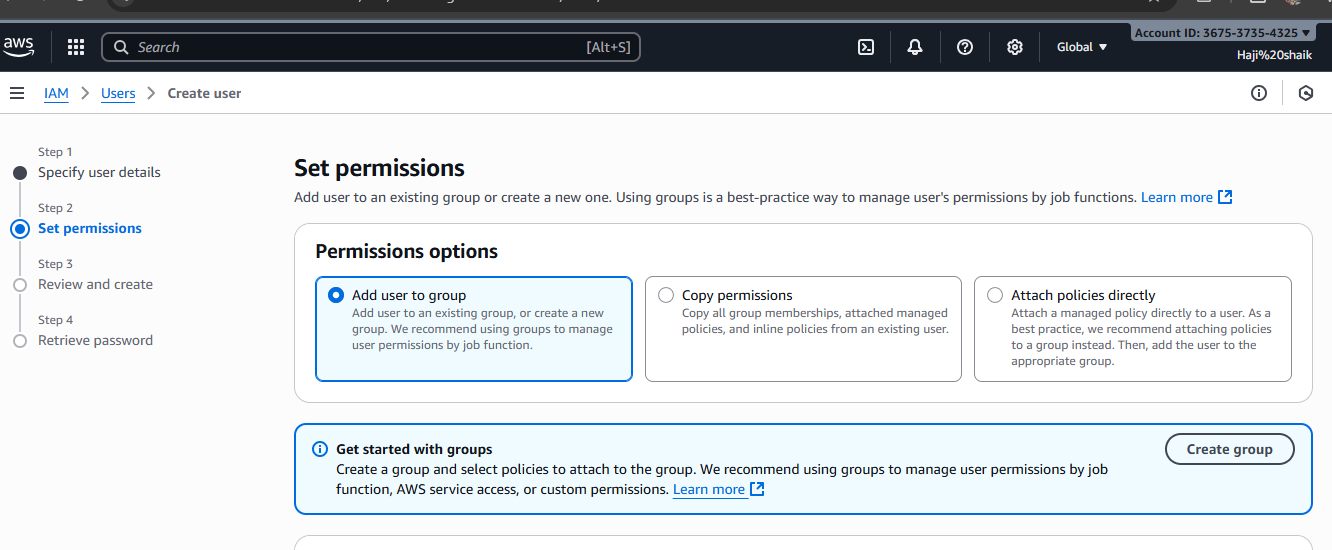


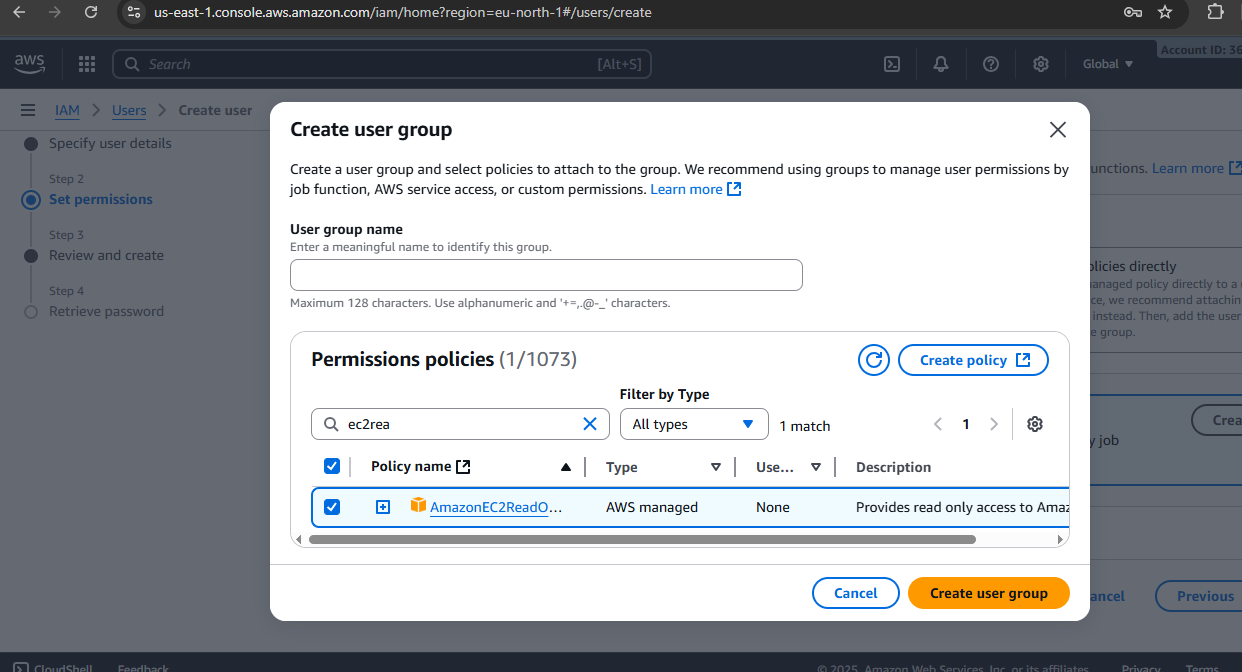


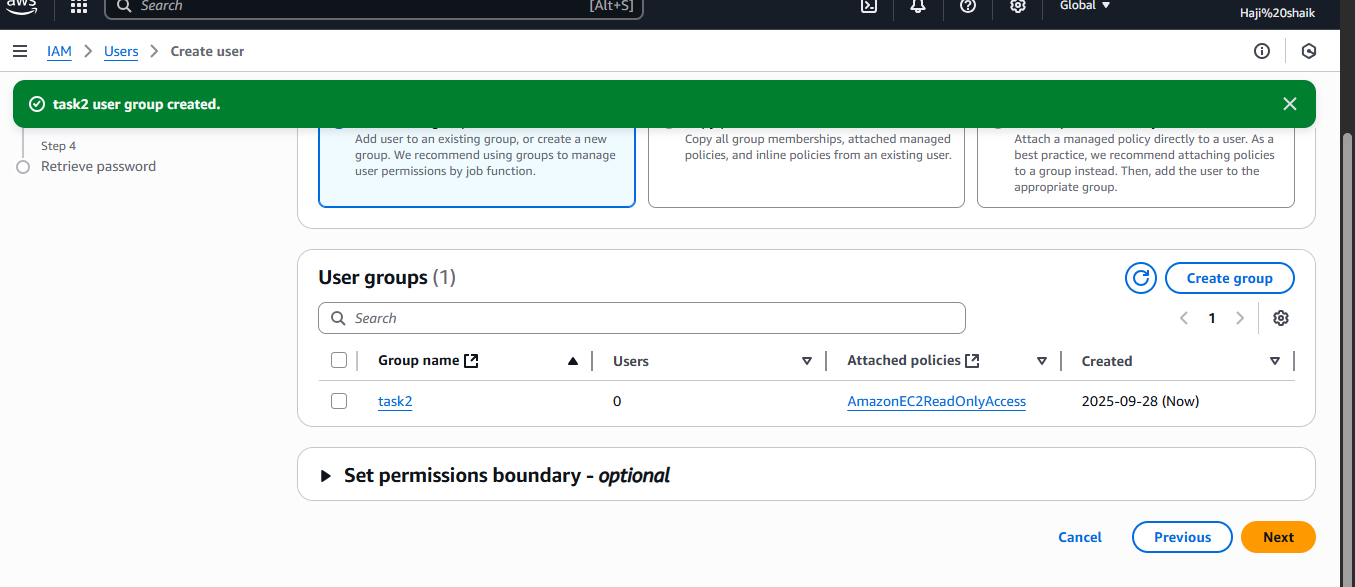


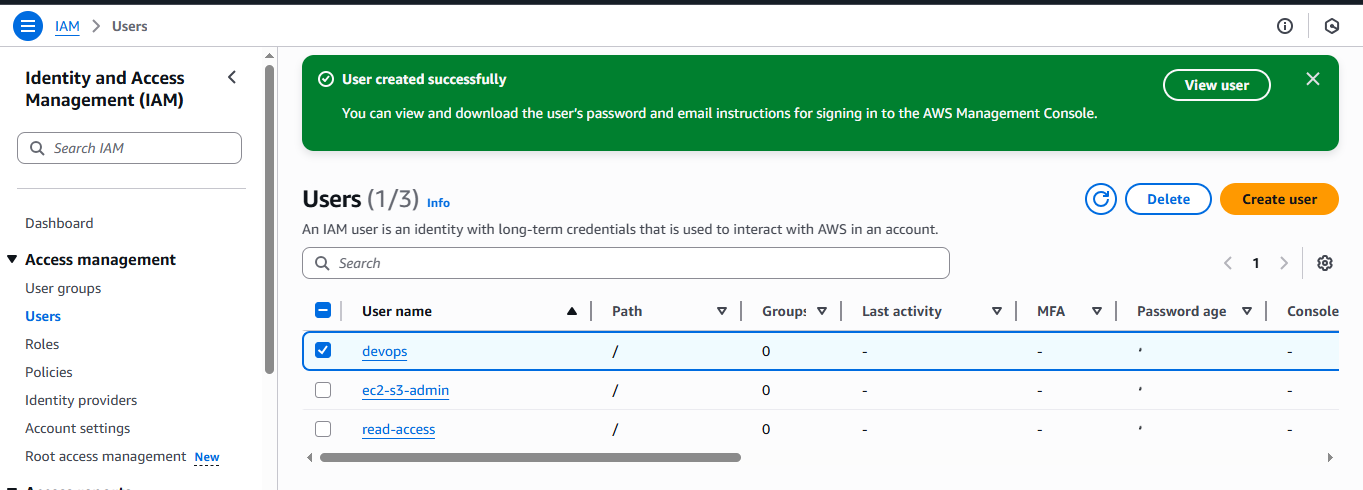
1. Create a new user named "Devops" and add to the group created in task 2.

* Go to AWS ec2 then open a serach bar and enter **IAM.**
* Then create a user.
* Gave a name to the user **read access.**
* Then gave provide access console aws.
* Then create password.
* Click the next page.
* Then set a permisson for add user group and craete a group and gave a permisson of **ec2readaccess only.**
* **Create** a group name task2.
* And review the page.
* Group and user will create:
* Here the results are;



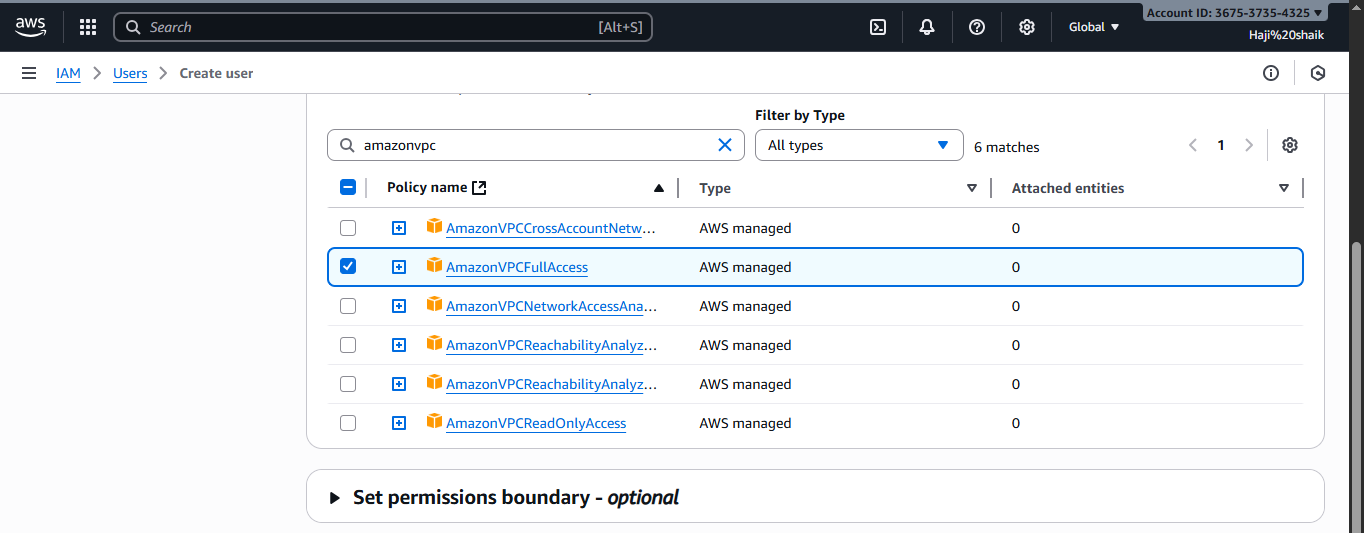




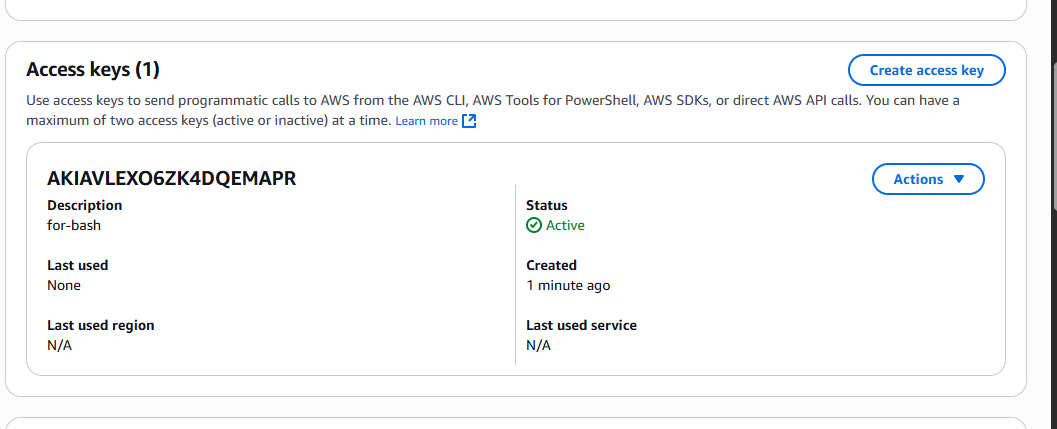


1. Write a bash script to create an IAM user with VPC full access.

* Go to AWS ec2 then open a serach bar and enter **IAM.**
* Then create a user.
* Gave a name to the user **read access.**
* Then gave provide access console aws.
* Then create password.
* Click the next page.
* Then set a permisson for add user group and craete a group and gave a permisson of **amazonvpcfullaccess.**
* Then for running this CLI access key.



**CLI acess key:**



* Then after a create a instance name bash.
* Then enter the instance with ssh key
* Then create a file name with create\_vpc\_user.sh
* Then use the bash script for “**Google refrence”**
* then gave permisson chmod600 filr name.
* nd ./filename
* **Here the results are :**
* **Bash script:**

#!/bin/bash

# Variables

USER\_NAME="VpcAdminUser"

POLICY\_ARN="arn:aws:iam::aws:policy/AmazonVPCFullAccess"

echo "🔹 Creating IAM user: $USER\_NAME"

# 1. Create IAM user

aws iam create-user --user-name $USER\_NAME

# 2. Attach AmazonVPCFullAccess policy

aws iam attach-user-policy \

--user-name $USER\_NAME \

--policy-arn $POLICY\_ARN

# 3. Create access keys (programmatic access)

ACCESS\_KEYS=$(aws iam create-access-key --user-name $USER\_NAME)

# Extract and display AccessKeyId and SecretAccessKey

ACCESS\_KEY\_ID=$(echo $ACCESS\_KEYS | jq -r '.AccessKey.AccessKeyId')

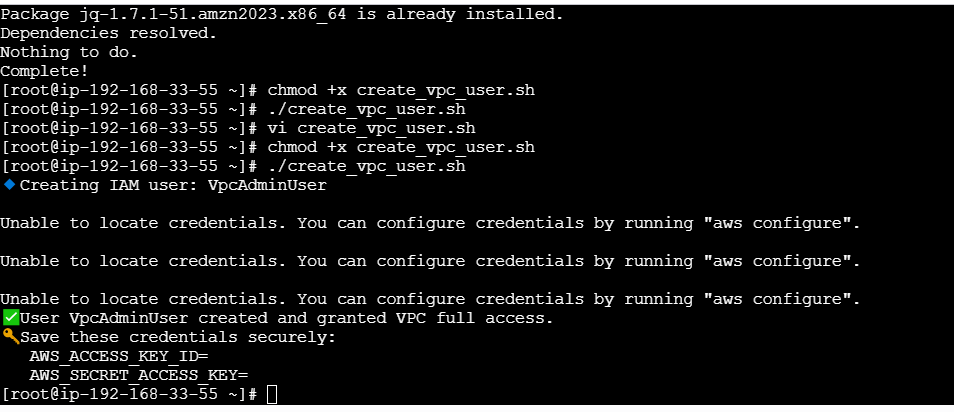
SECRET\_ACCESS\_KEY=$(echo $ACCESS\_KEYS | jq -r '.AccessKey.SecretAccessKey')

echo "✅ User $USER\_NAME created and granted VPC full access."

echo "🔑 Save these credentials securely:"

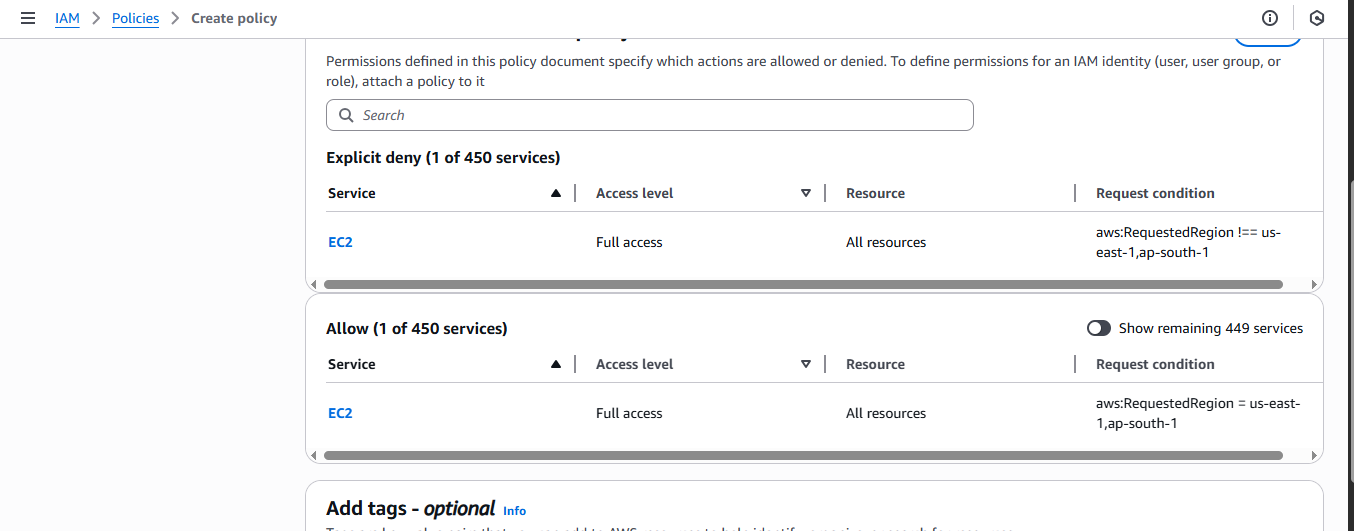
echo " AWS\_ACCESS\_KEY\_ID=$ACCESS\_KEY\_ID"

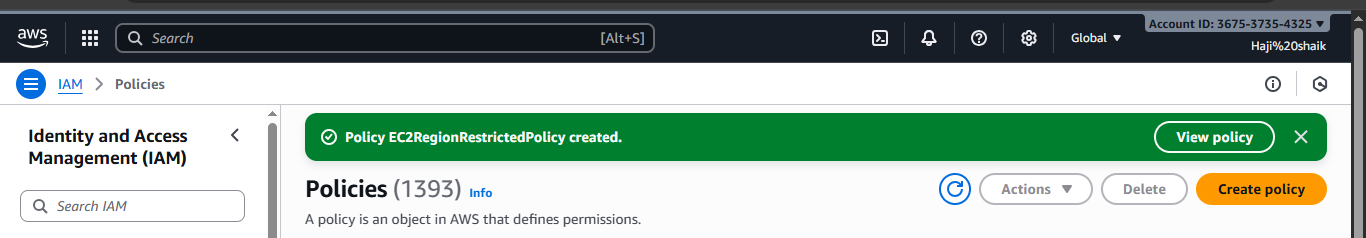
echo " AWS\_SECRET\_ACCESS\_KEY=$SECRET\_ACCESS\_KEY"

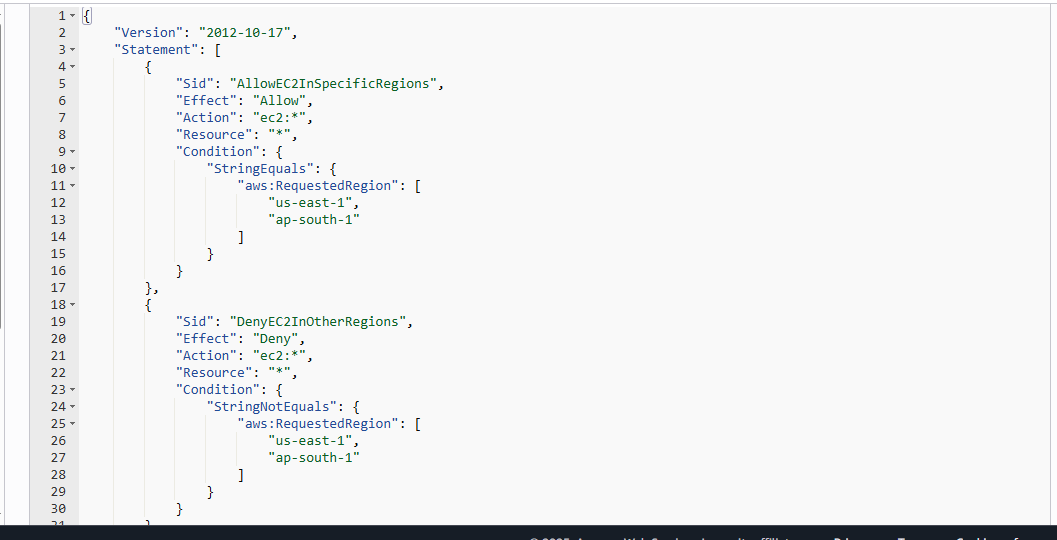


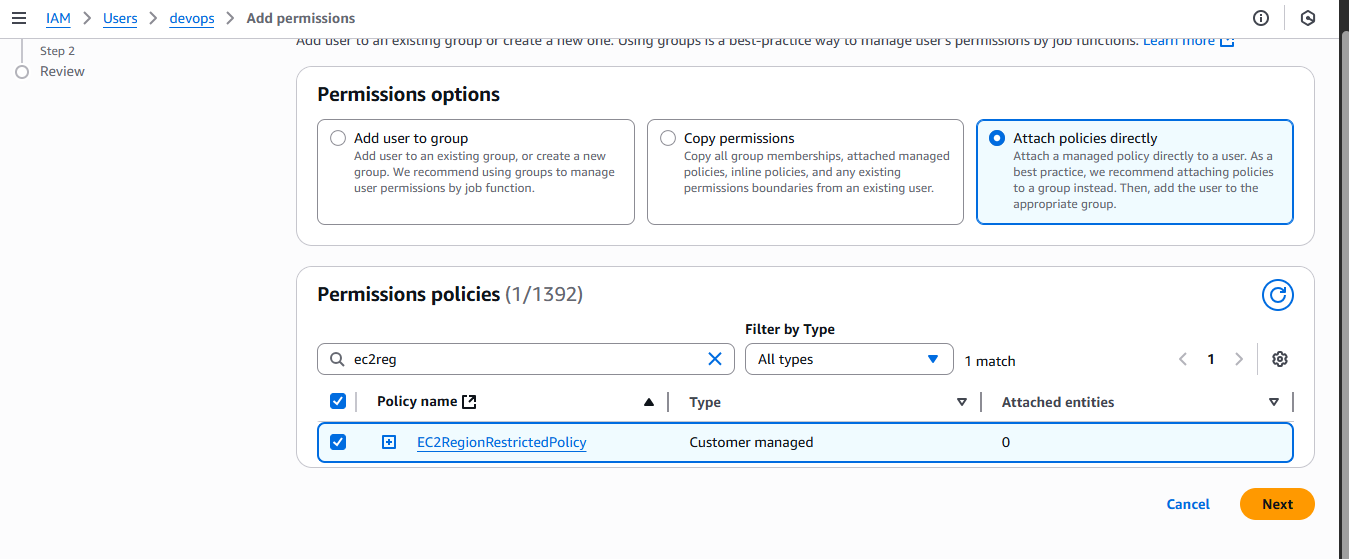
1. Create an IAM policy to allow EC2 access for a specific user in specific regions only.

* Go to aws then search for iam.
* Create a policy ec2 full access.
* Choose json tab and paste script refrence from google.
* Then save the script with the name of **ec2 region restricted policy.**
* Then attach the policy for specific user.
* I choose devops user.
* Then the results here:









1. We have two accounts: Account A and Account B. Account A user should access an S3 bucket in Account B.(Collaborate with a team member and execute this. This is mostly asked in every interview.)