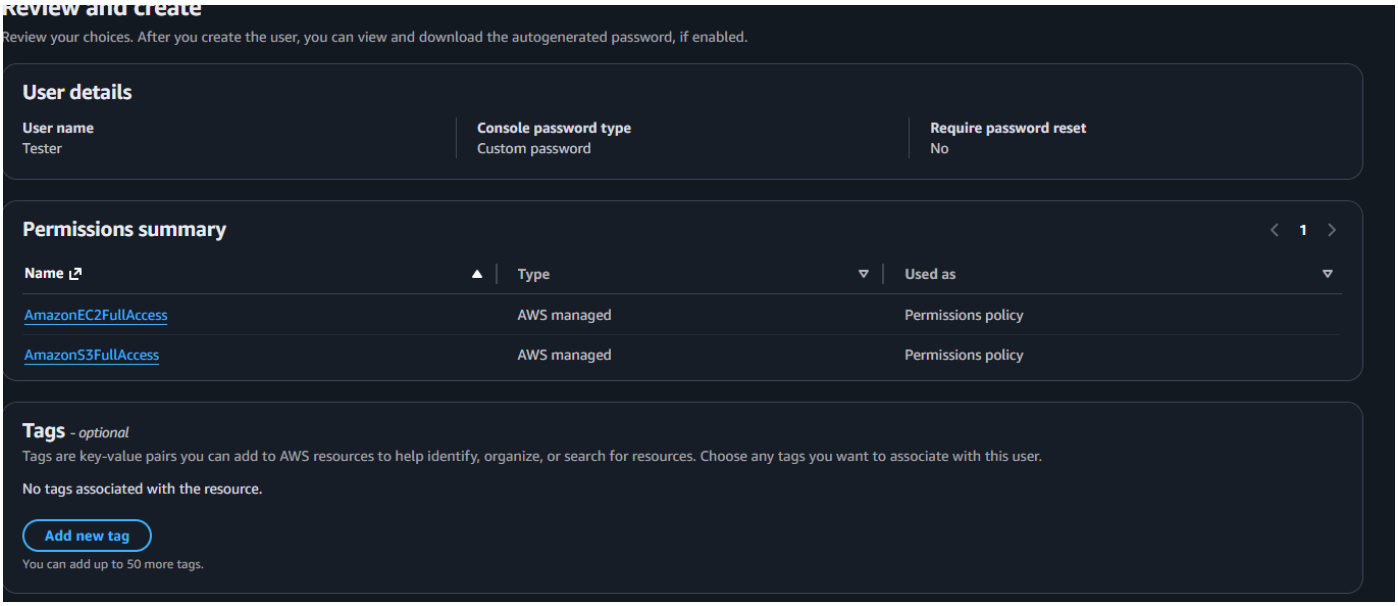
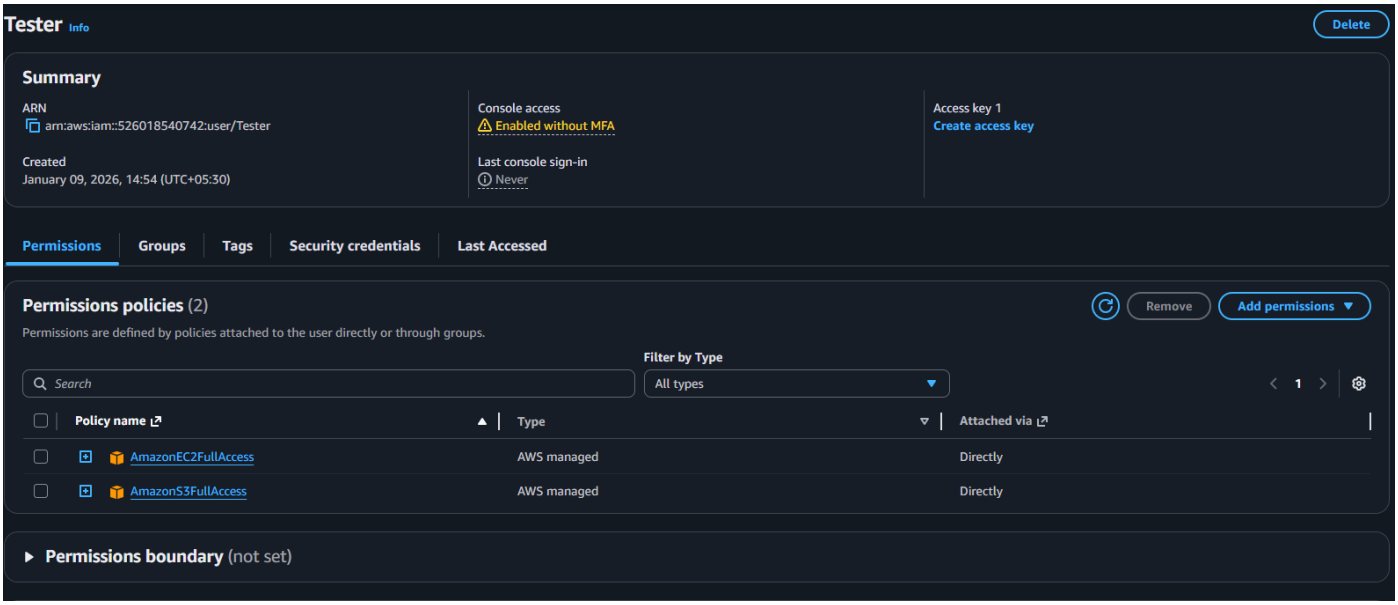
IAM Tasks-01

- **Objective:** To implement and manage AWS IAM users, groups, and policies by applying least-privilege access, automating user creation, restricting permissions by region, and enabling secure cross-account S3 access between AWS accounts.

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

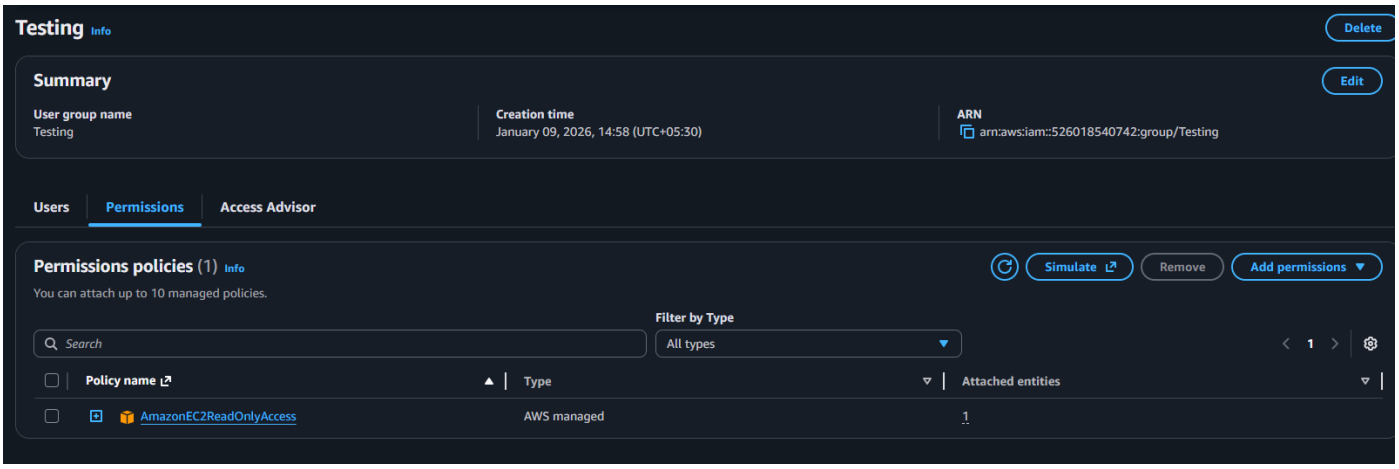


The user “Tester” has been created with both permissions.



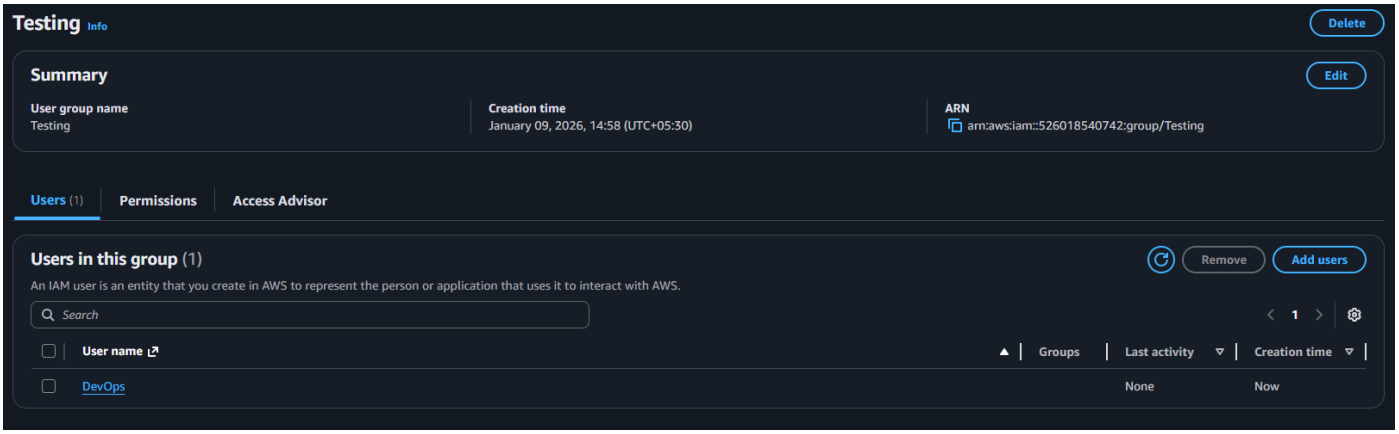
IAM Tasks-01

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



A group named “Testing” has been created with the given permissions.

- **Create a new user named "DevOps" and add to the group created in task 2.**



A user named “DevOps” was created and added to the group “Testing”.

IAM Tasks-01

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

```
$ cat IAM.bash
#!/bin/bash

# Exit immediately if any command fails
set -e

# Prompt for IAM username
read -p "Enter IAM username: " user

# Validate input
if [ -z "$user" ]; then
  echo "Error: Username cannot be empty"
  exit 1
fi

policy="arn:aws:iam::aws:policy/AmazonVPCFullAccess"

# Create IAM user
echo "Creating IAM user: $user"
aws iam create-user --user-name "$user"

# Attach VPC Full Access policy
echo "Attaching VPC Full Access policy"
aws iam attach-user-policy \
  --user-name "$user" \
  --policy-arn "$policy"

echo "User '$user' created with VPC Full Access"
```

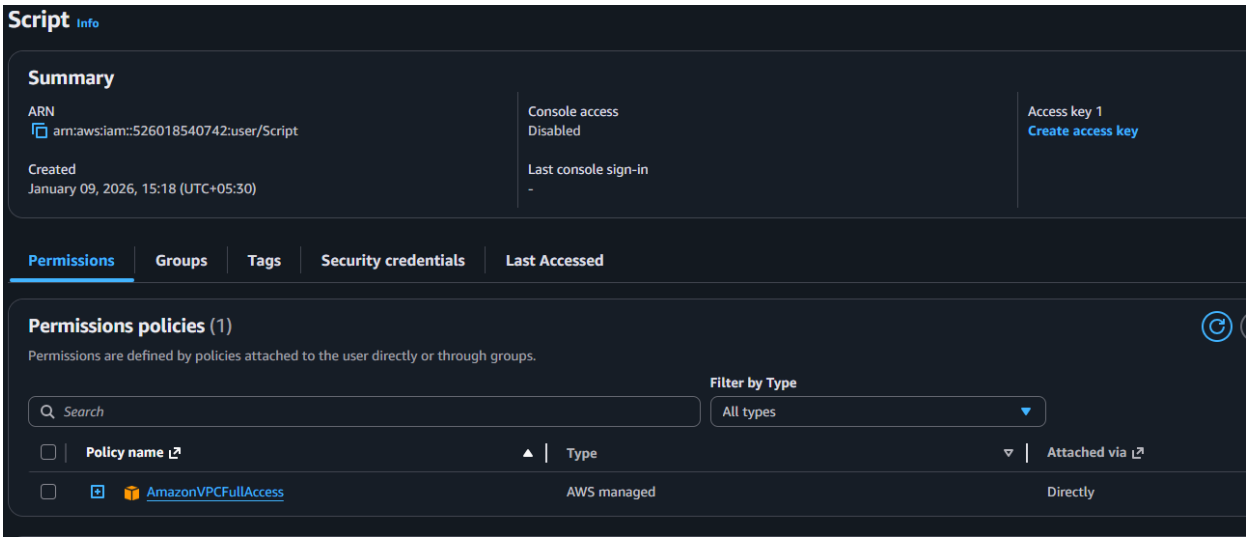
The script was written so that the user can input any username and create a user with VPC full access. The arn of the existing VPC full access was used in the policy variable.

```
Viqaas@LAPTOP-VGO25G9U MINGW64 /d/DevOps/Me/DevOps-Learning/Scripts (main)
$ bash IAM.bash
Enter IAM username: Script
Creating IAM user: Script
{
    "User": {
        "Path": "/",
        "UserName": "Script",
        "UserId": "AIDAXU6JF6TDDXVQVMQD6",
        "Arn": "arn:aws:iam::526018540742:user/Script",
        "CreateDate": "2026-01-09T09:48:22+00:00"
    }
}
Attaching VPC Full Access policy
User 'Script' created with VPC Full Access
```

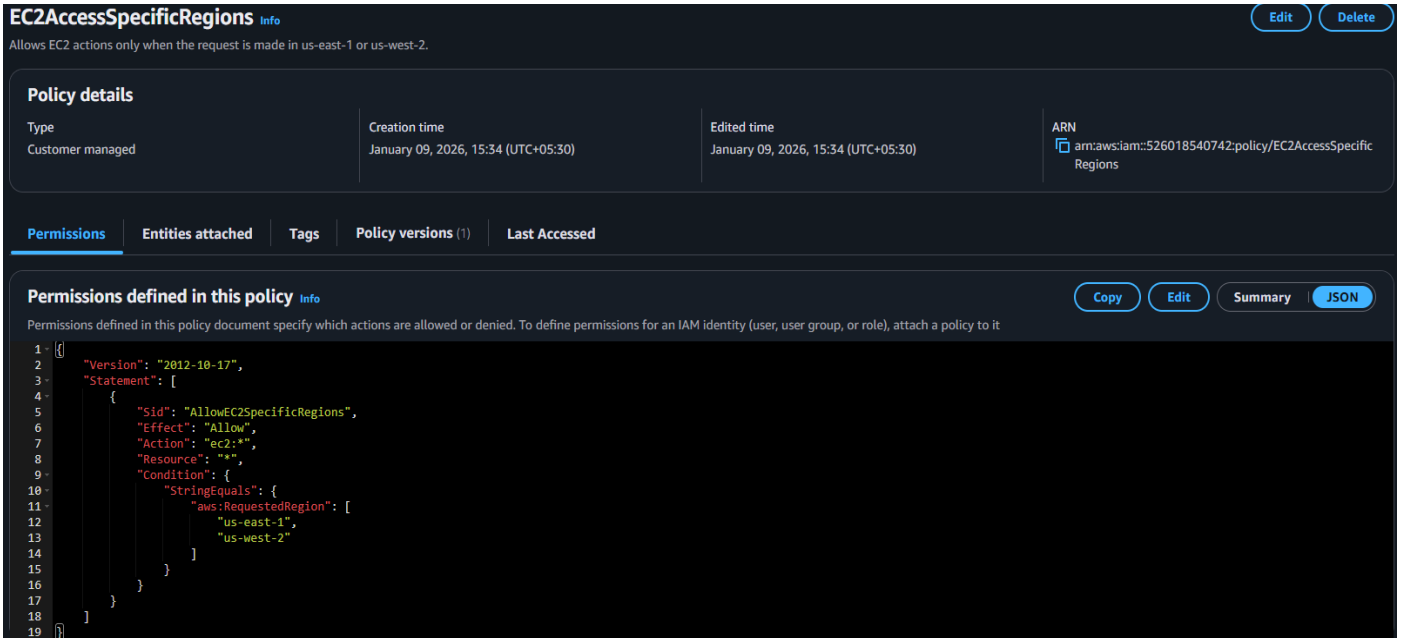
The user was successfully created.

IAM Tasks-01

The user will have to configure AWS CLI with root permissions first before executing the above script.



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

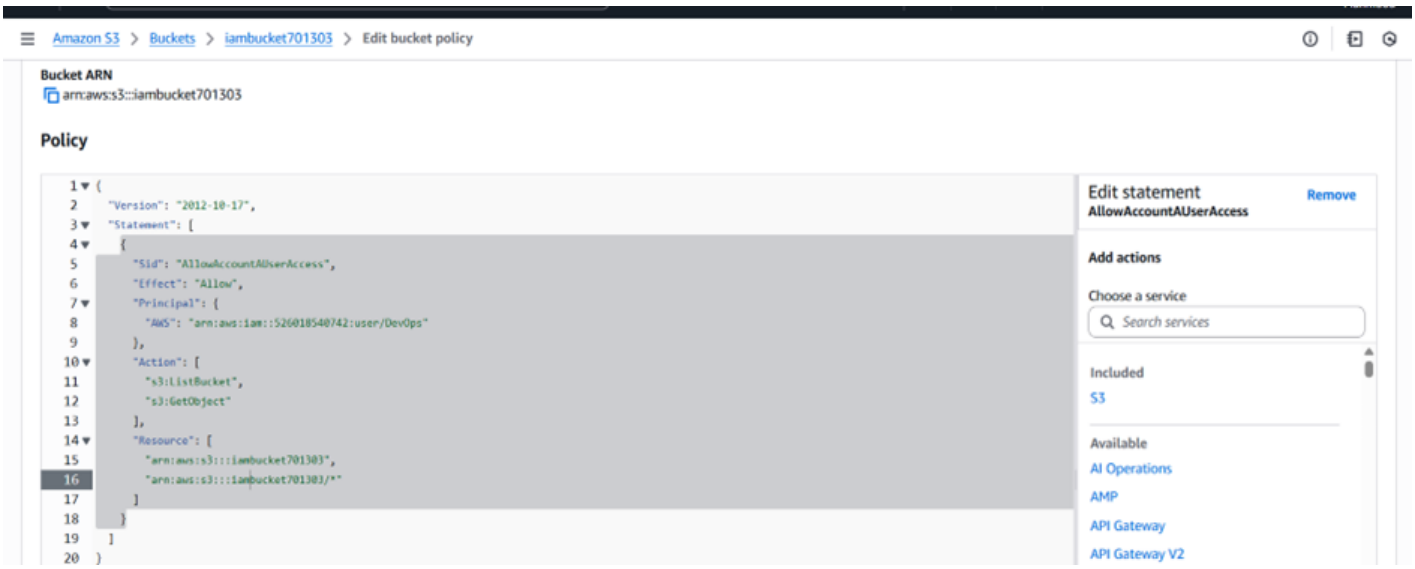


The policy above allows EC2 actions only when the request is made in ‘‘us-east-1" or “us-west-2".

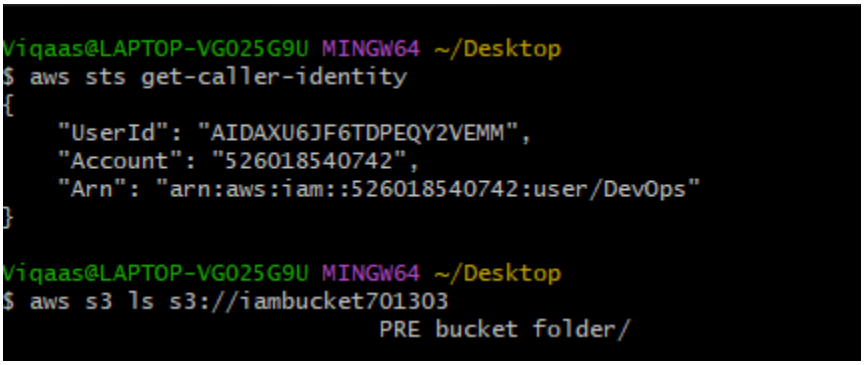
- The regions can be changed as per requirement.
- The policy was created in json format with the name “EC2AccessSpecificRegions’’.
- We can attach this policy to a specific user or a group.

IAM Tasks-01

- We have two accounts: Account A and Account B. Account A user should access an S3 bucket in Account B.
- First, Account A user needs S3 full access to access the bucket in Account B.
- Then Account B needs to create a bucket policy which gives access to Account A.



- Then Account A can use AWS CLI to access the bucket.



- **Successfully completed all assigned AWS IAM tasks, including user, group, policy management, automation, and secure cross-account S3 access.**