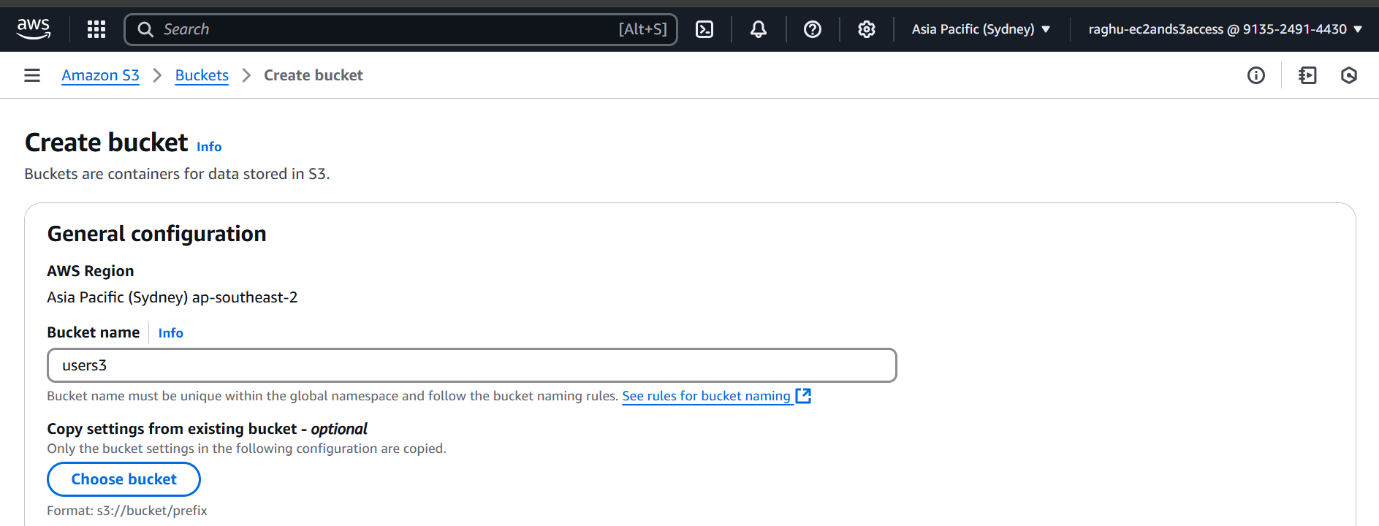
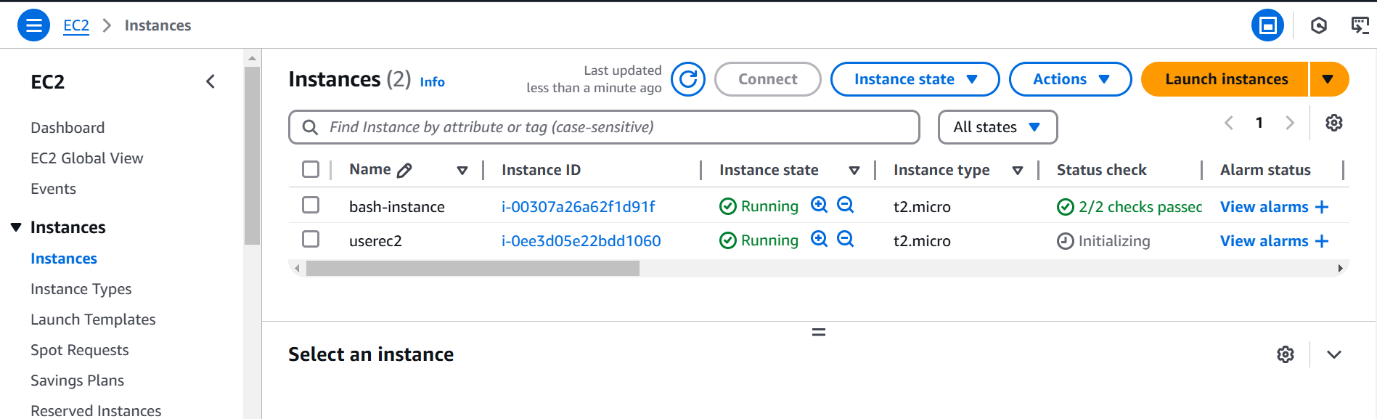
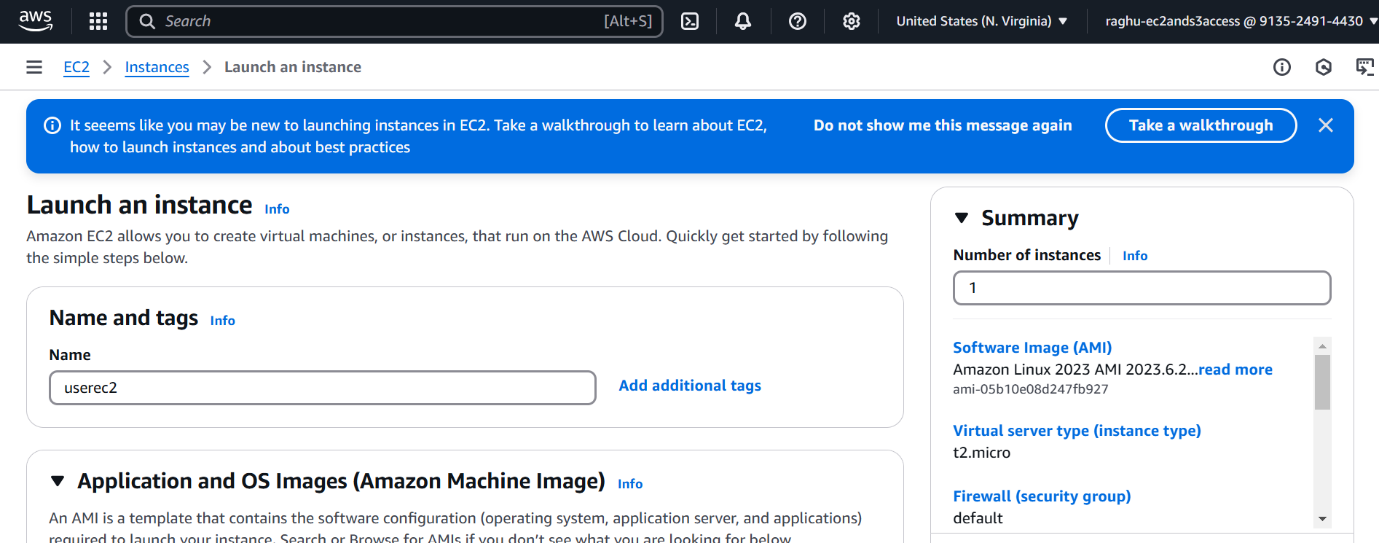
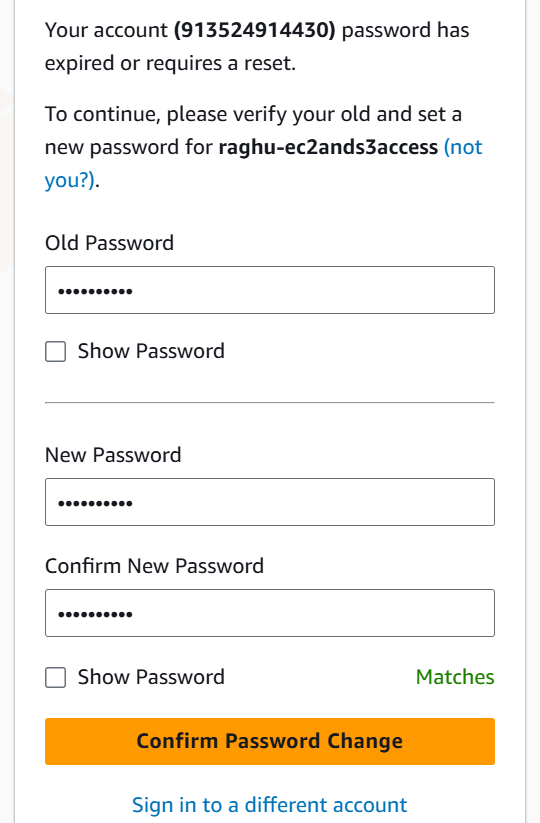
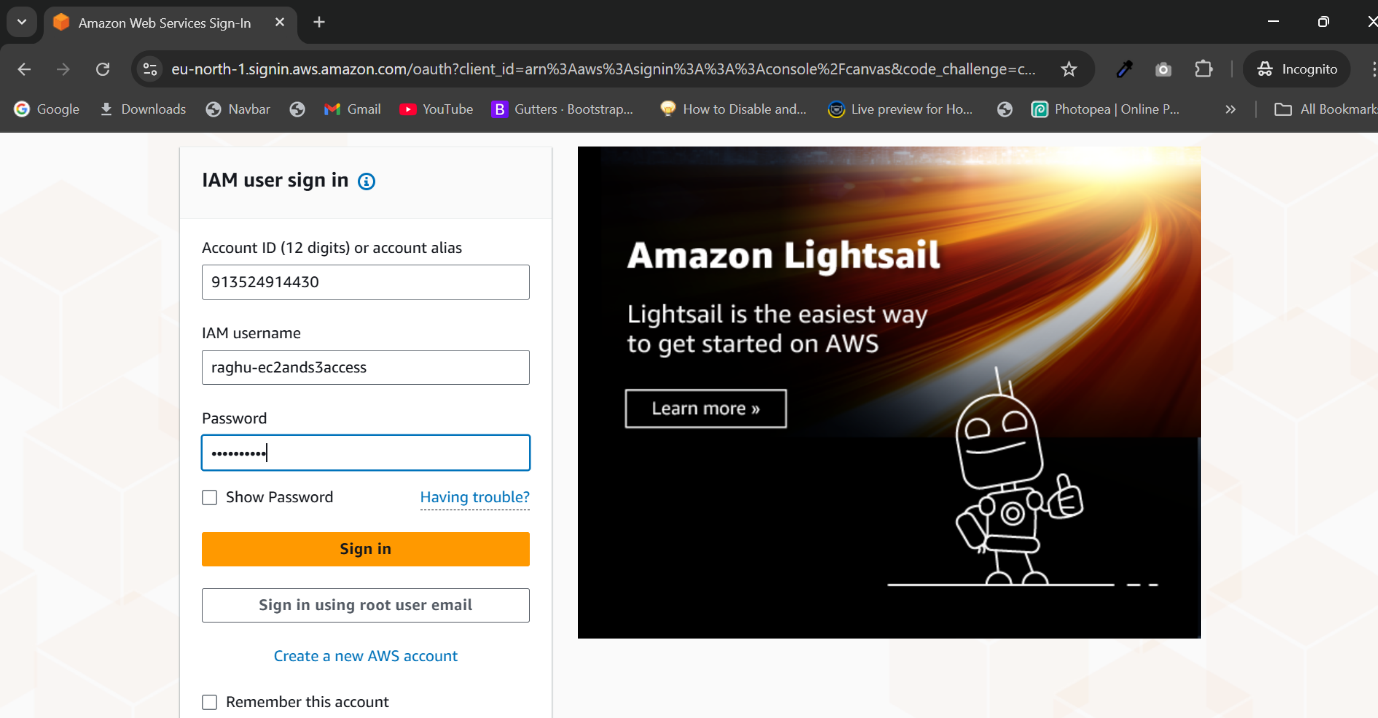
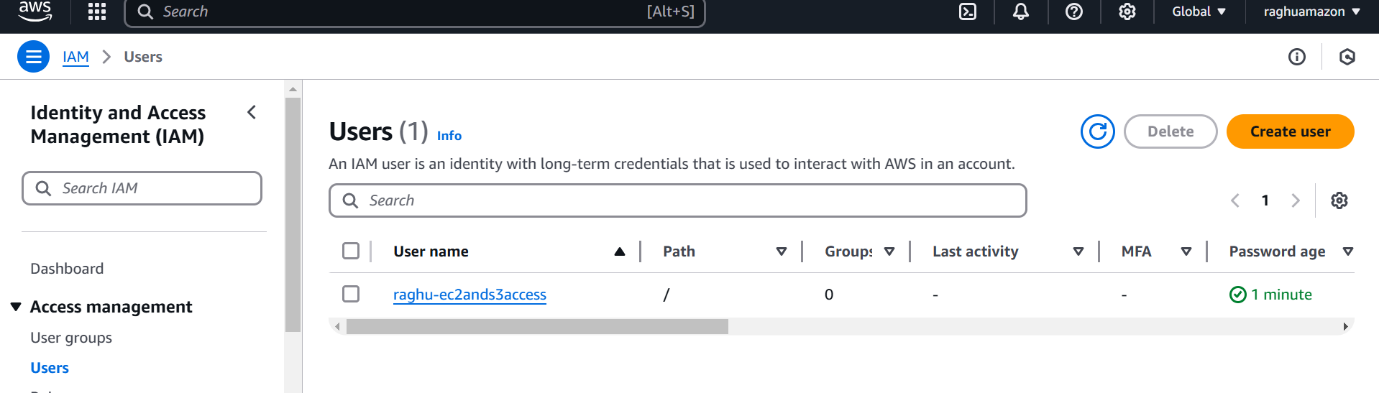
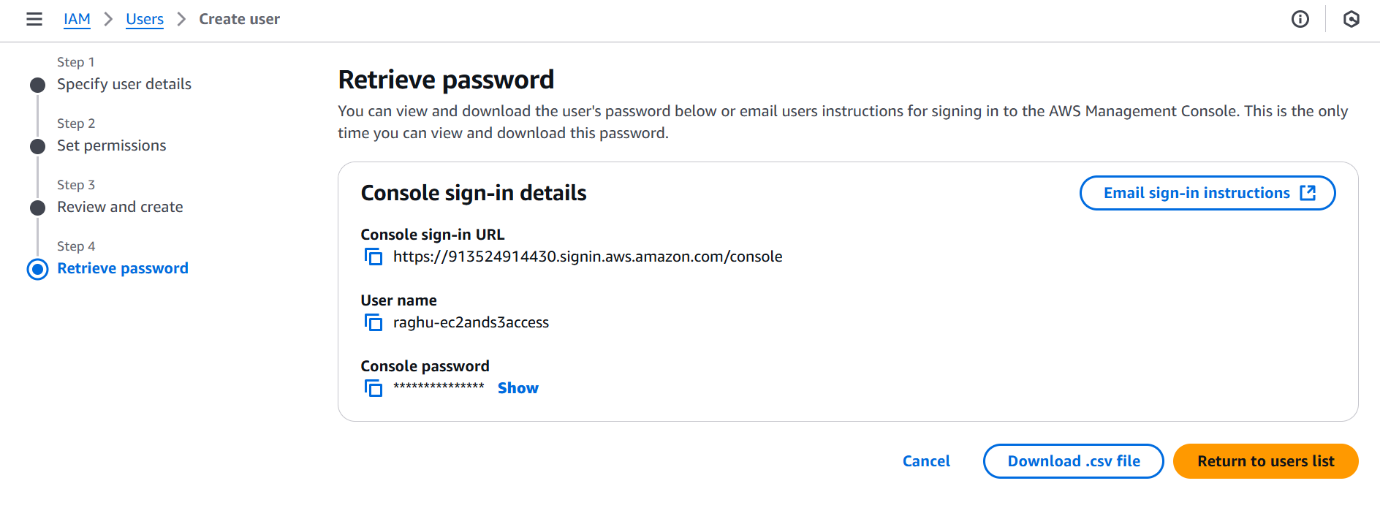
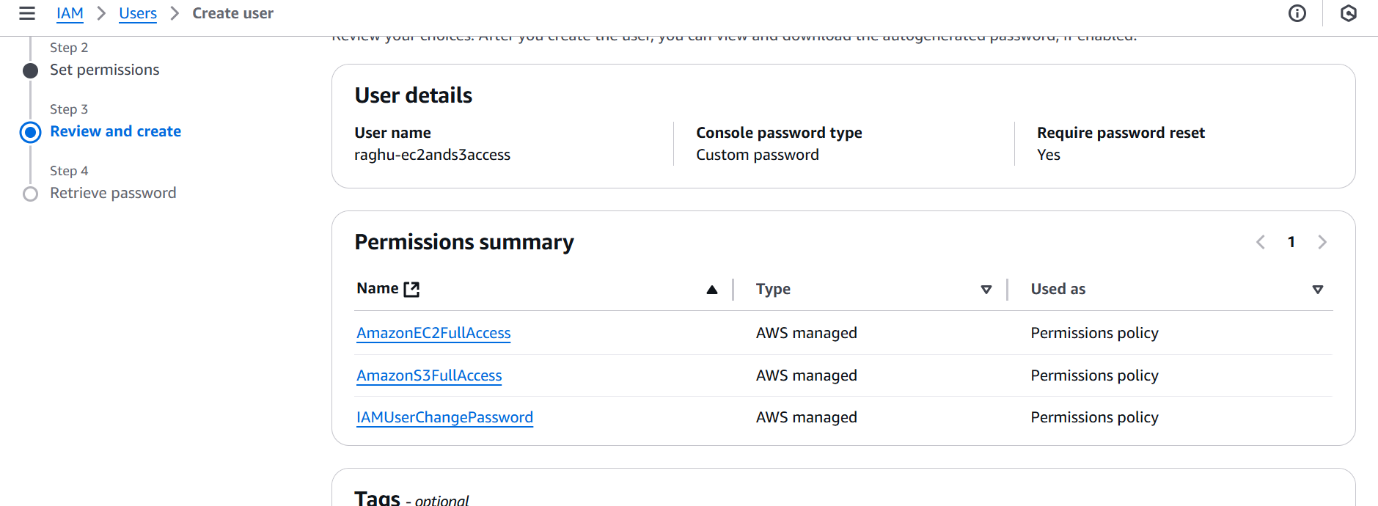
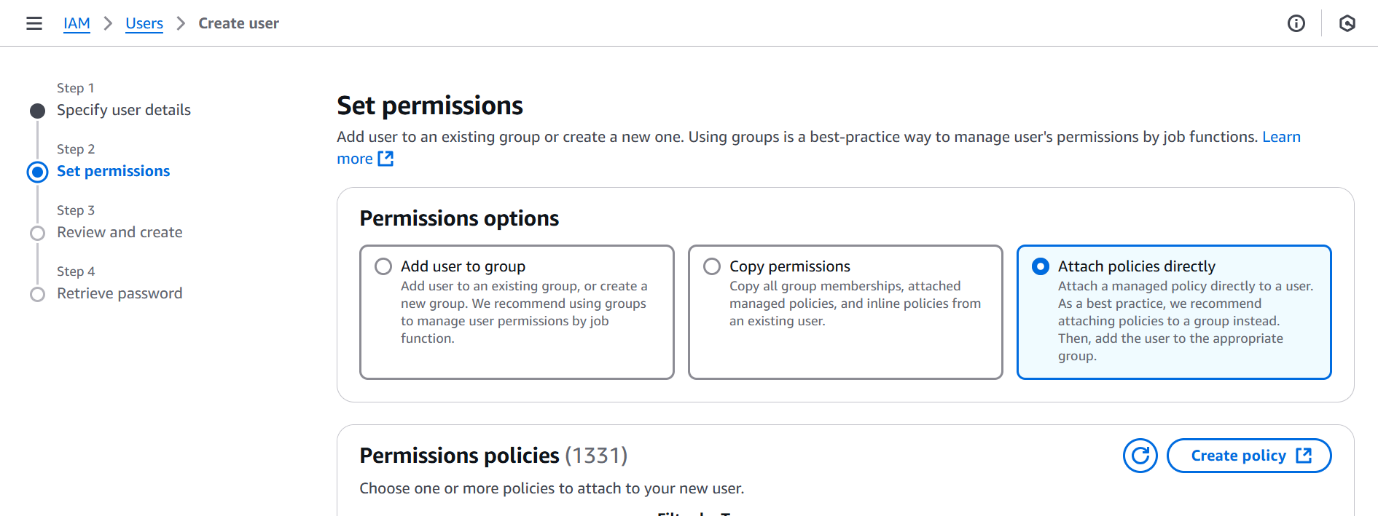
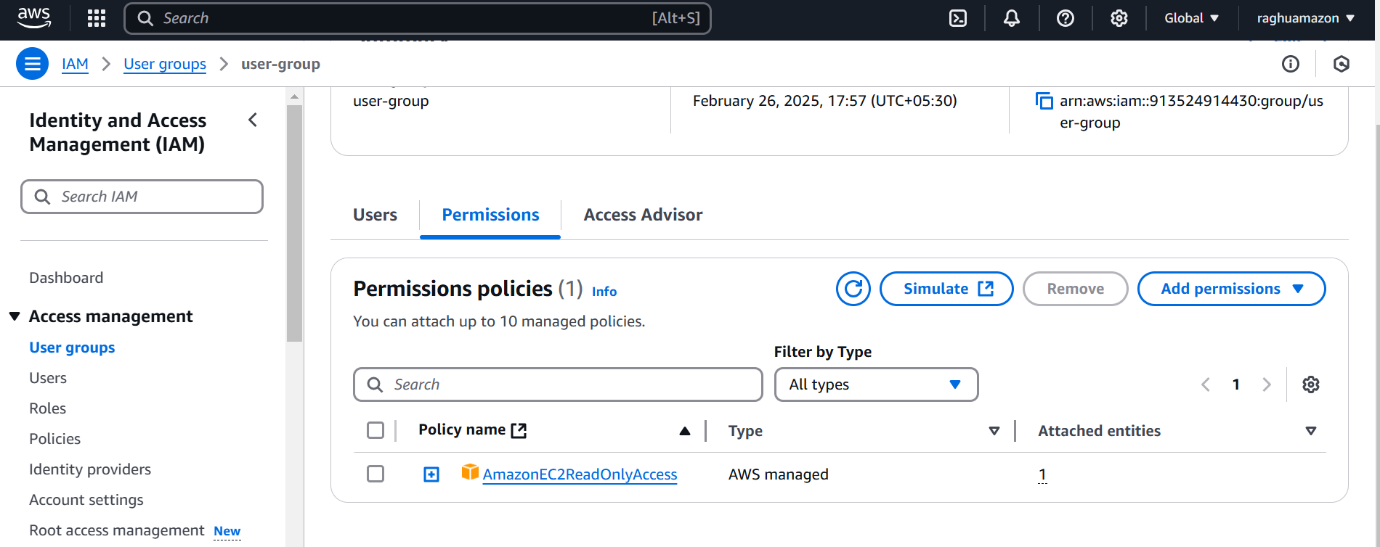
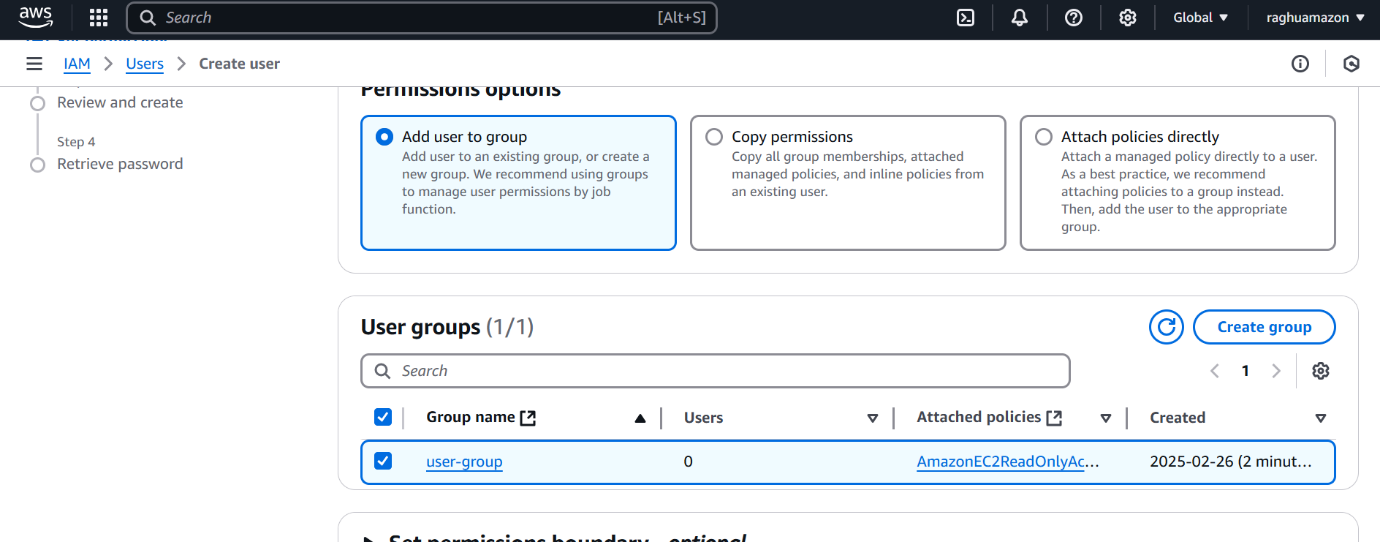
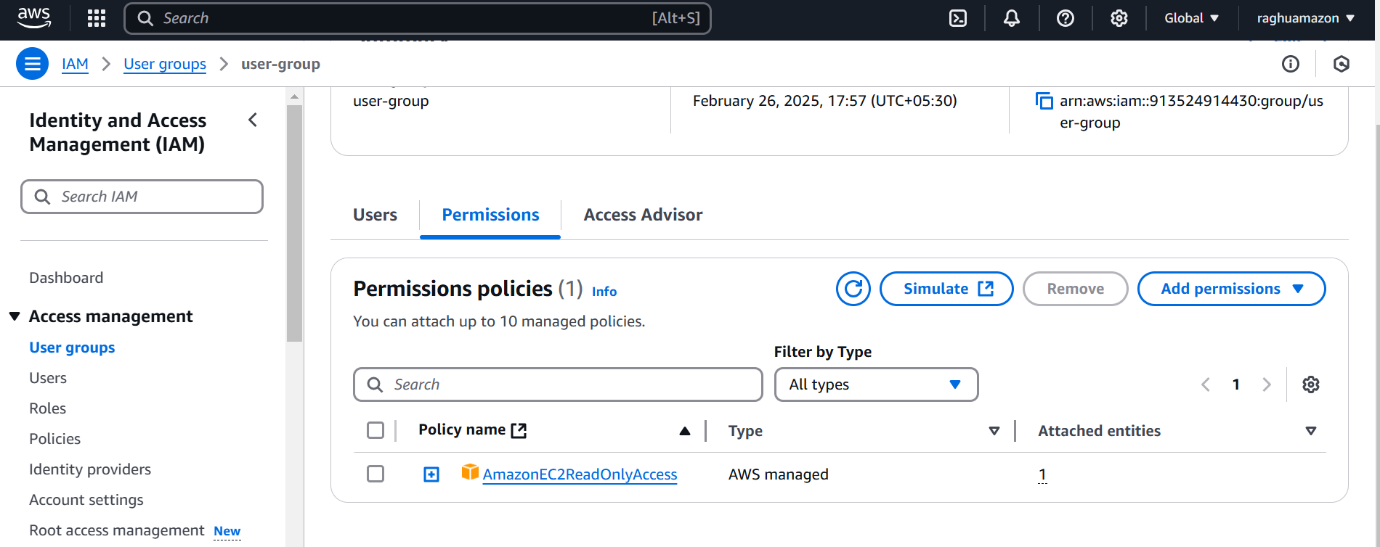
1. Create one IAM user and assign ec2,s3 full access role.

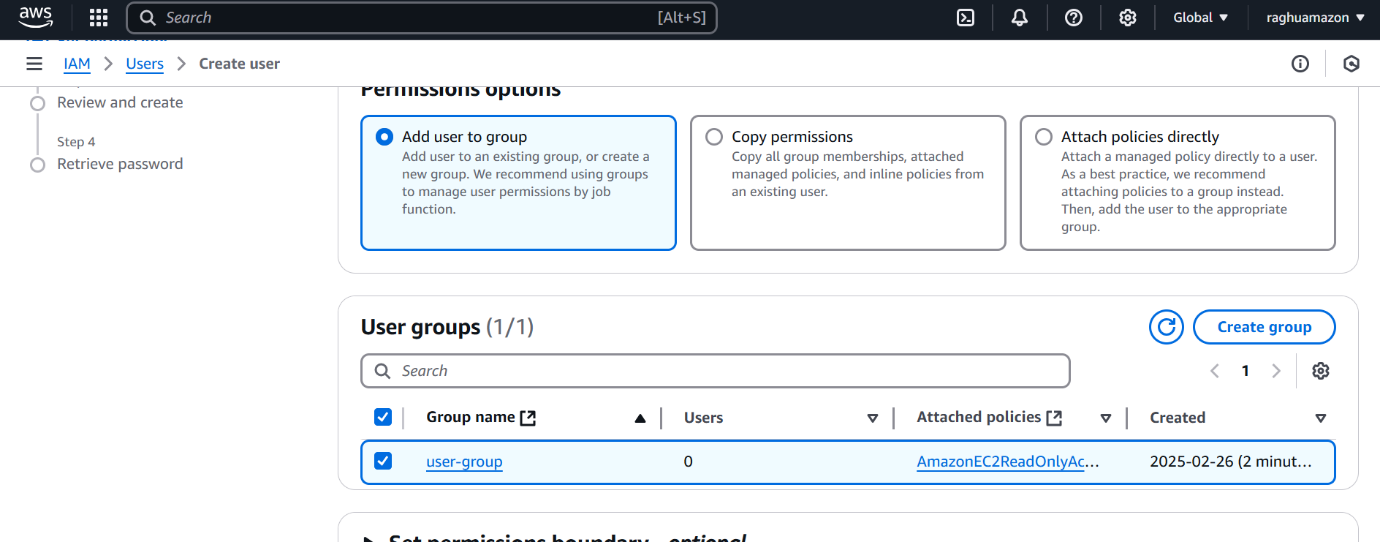


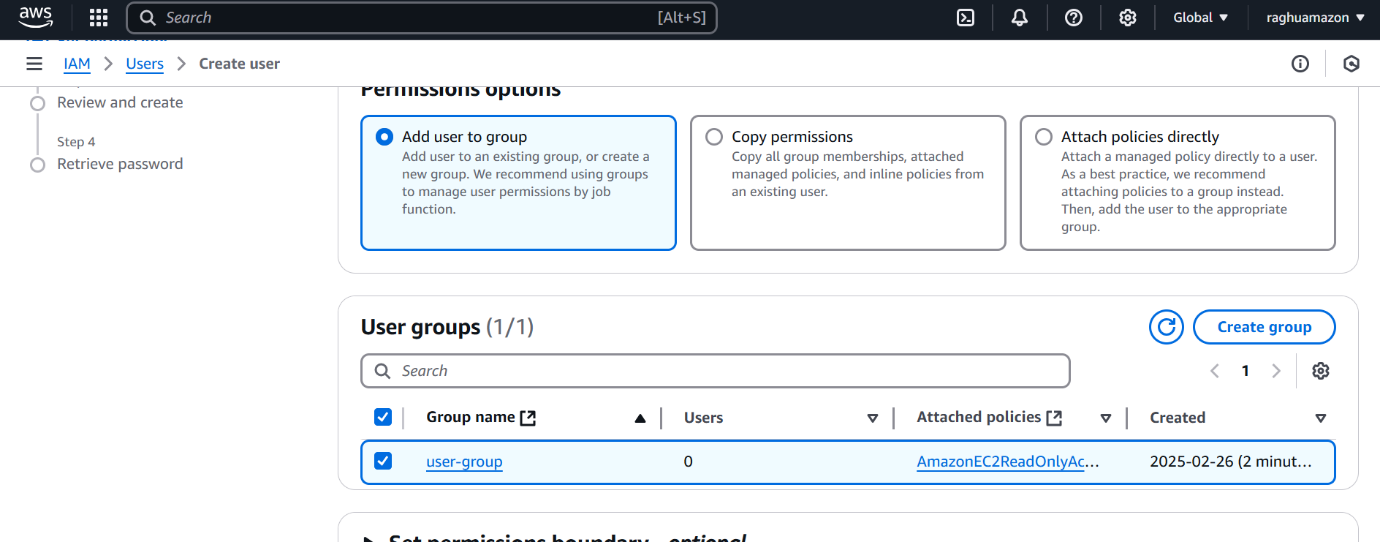
1. Create one Group in IAM and Assign Read access for ec2.



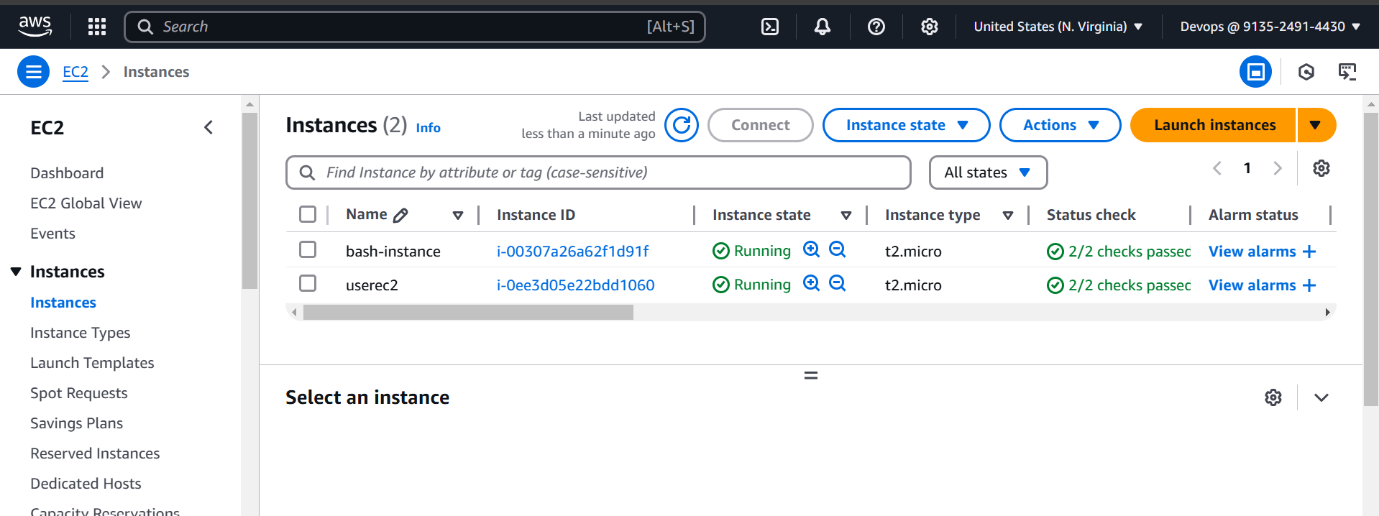


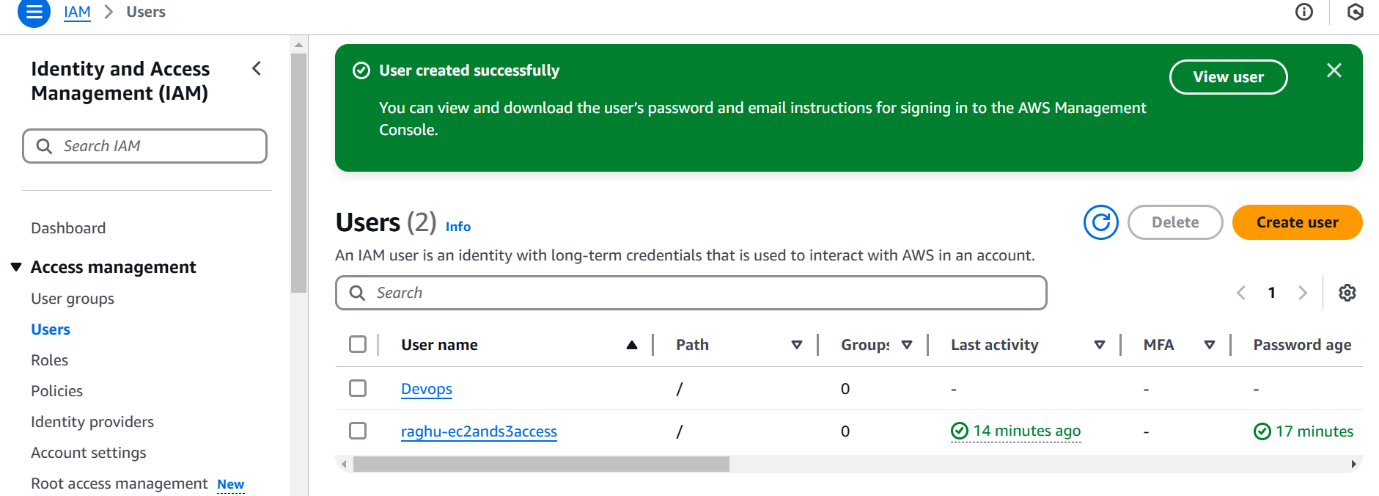


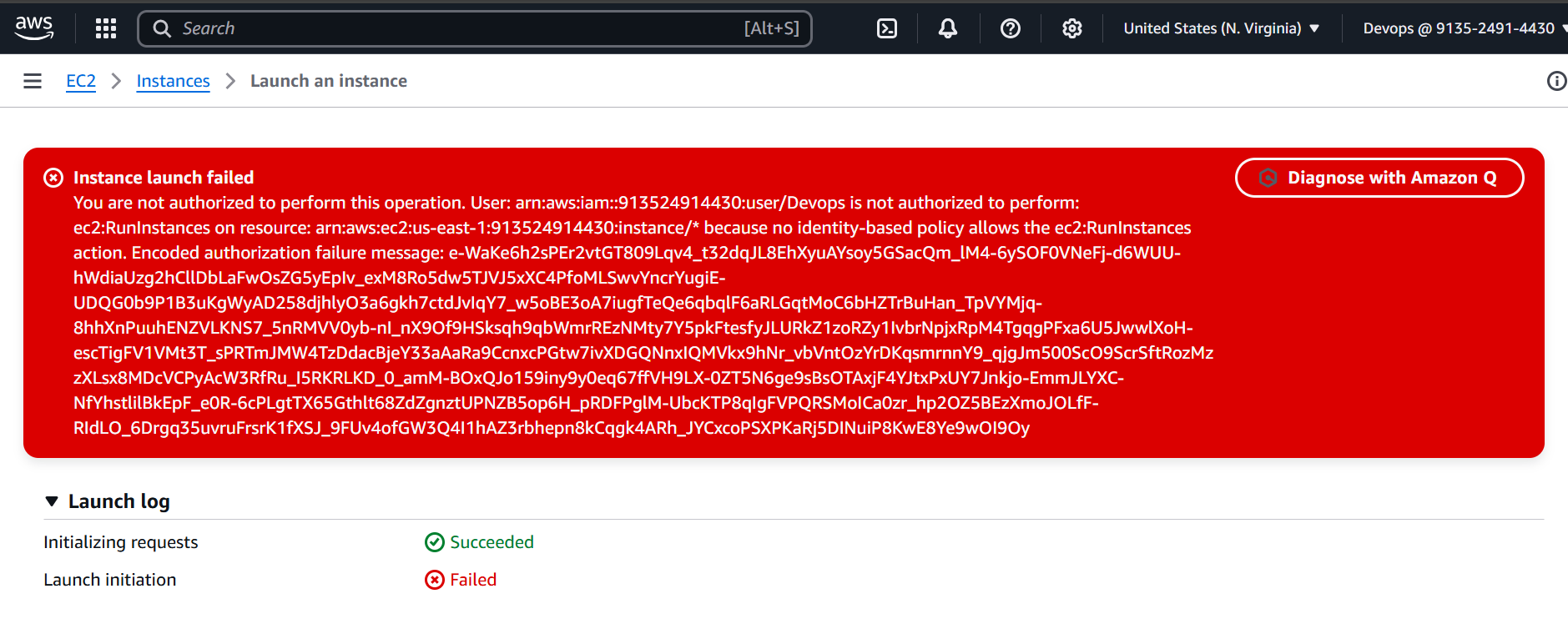
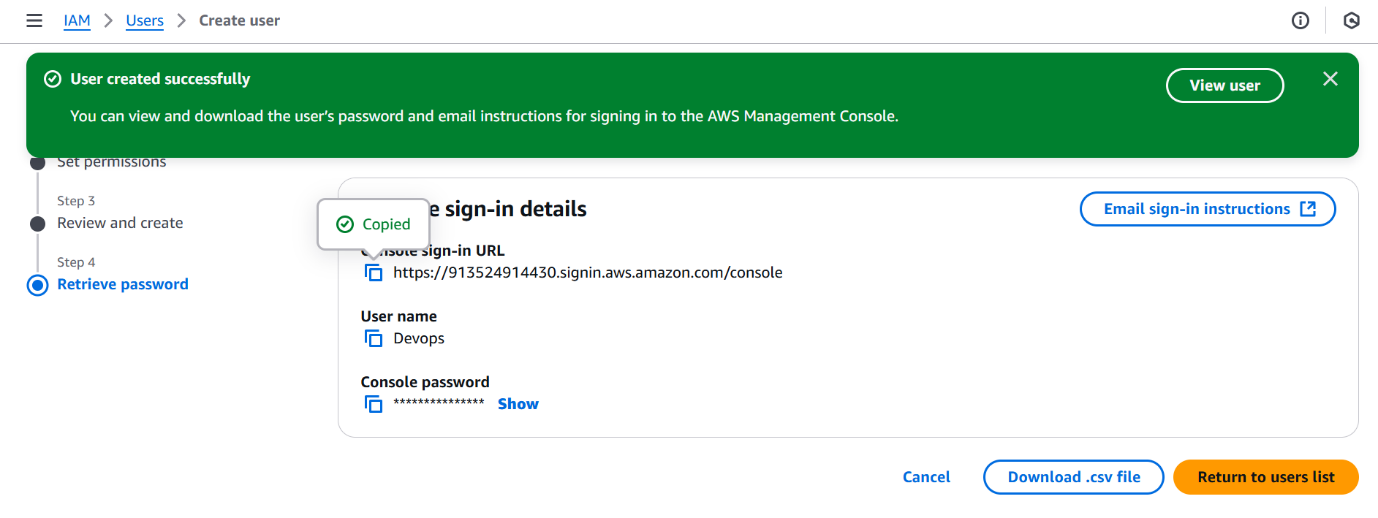




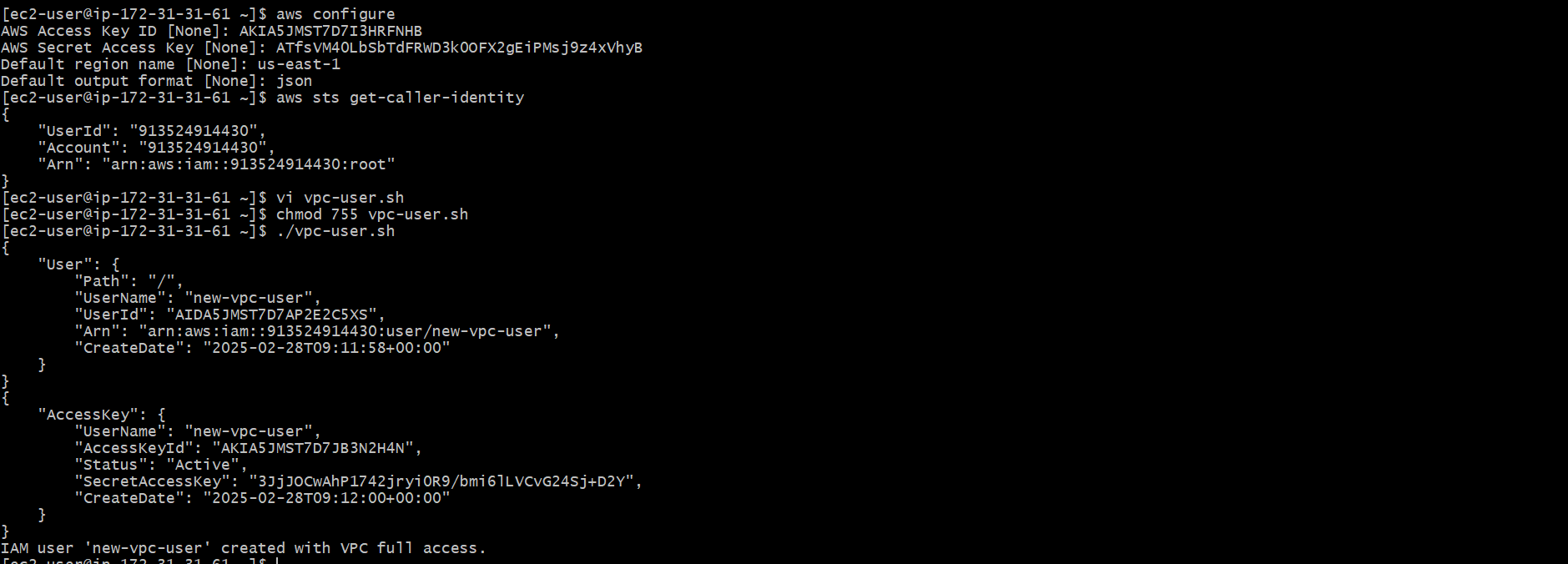
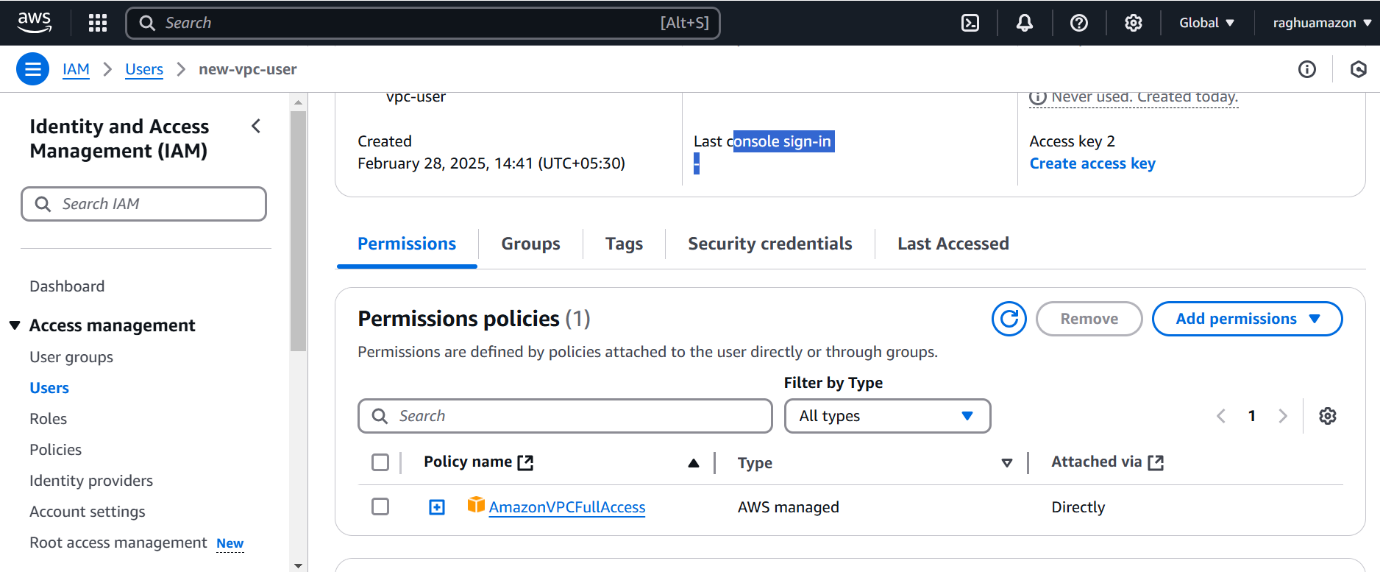
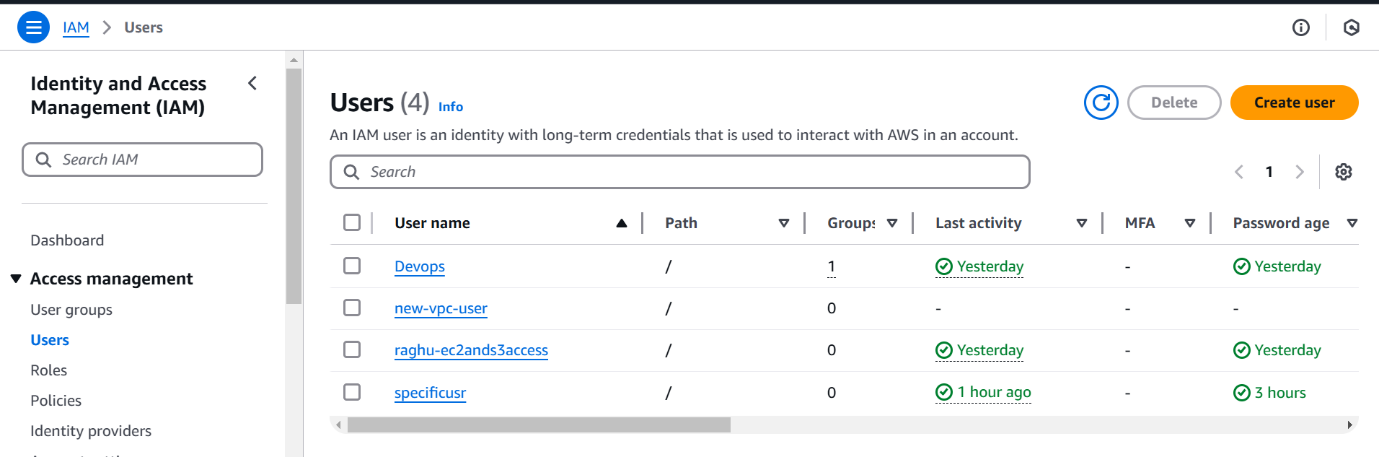
1. Create a new user with name Devops and add to the group created in task2.



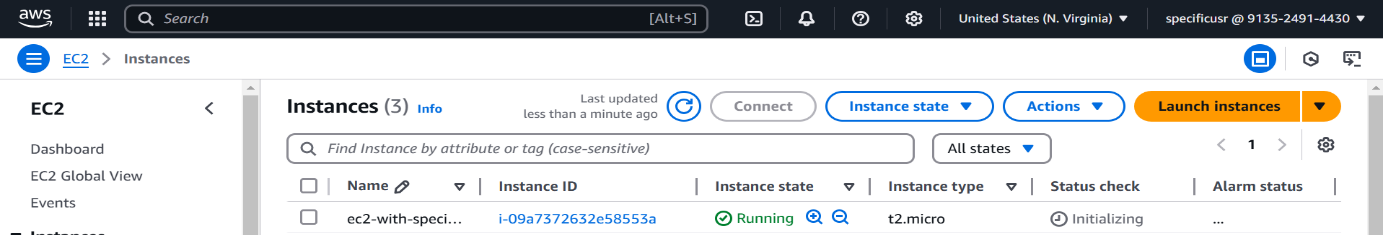


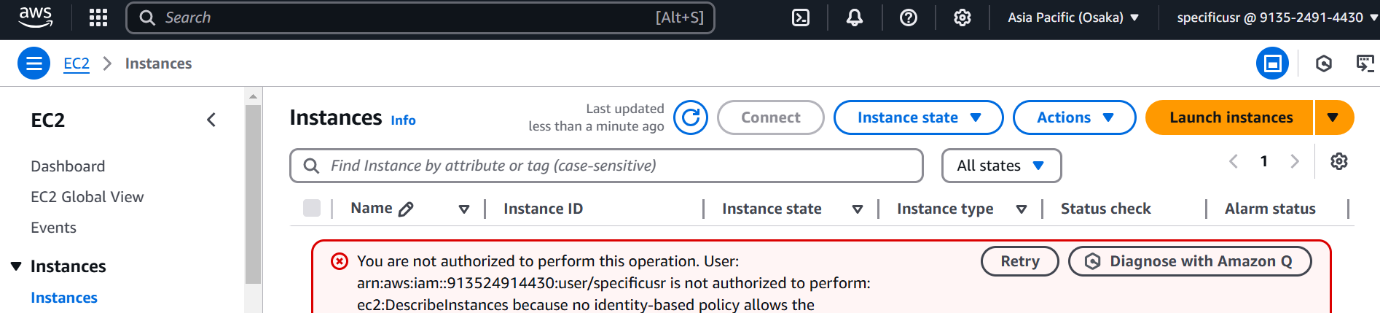


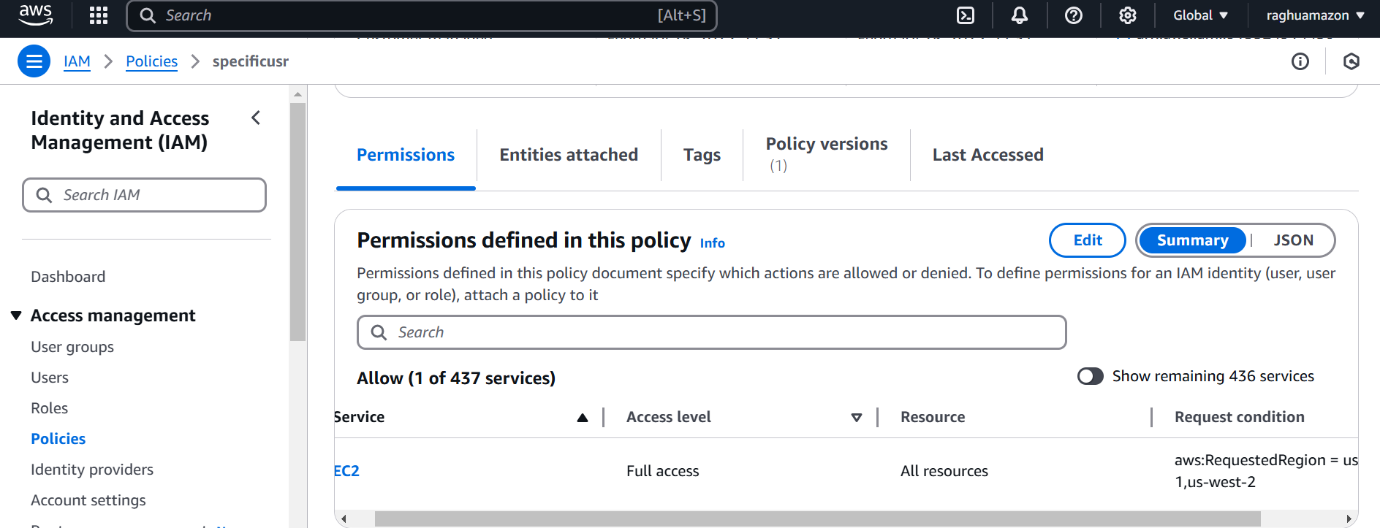
1. Write a bash script to create a IAM user with VPC full access.

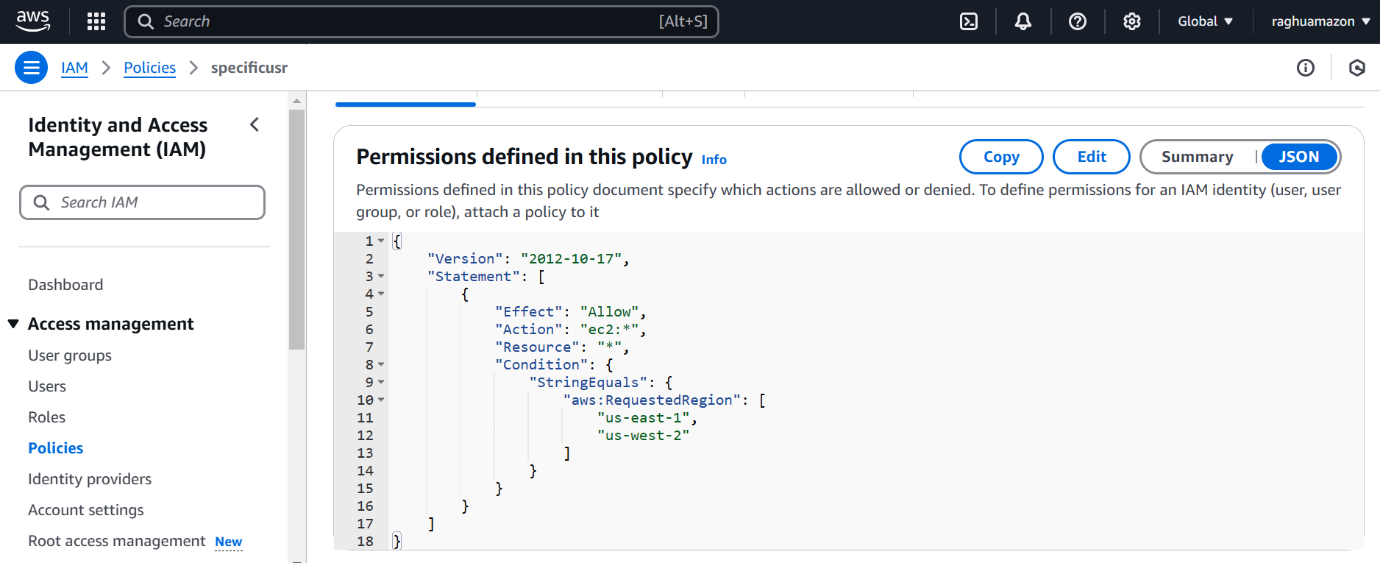


1. Create a IAM policy to access ec2 for a specific user in specific regions only.



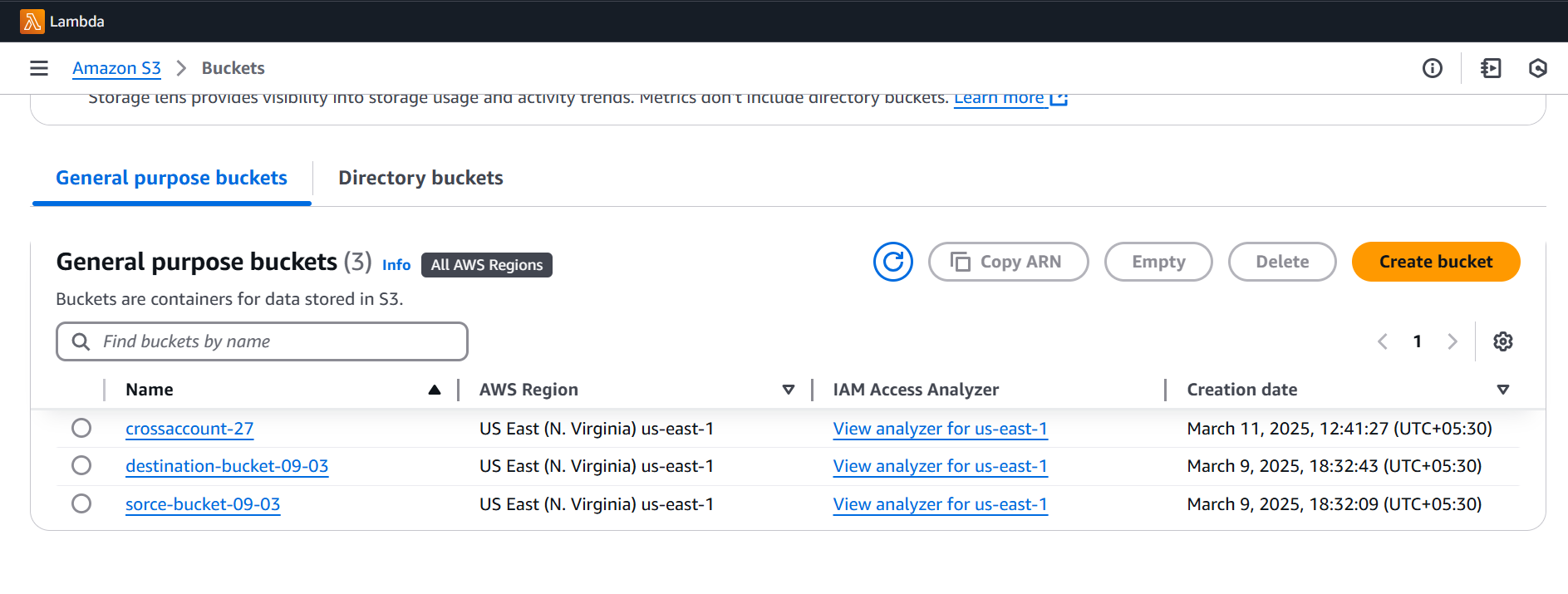






1. We have two accounts Account A and Account B, Account A user should access s3 bucket in Account B. (Collaborate with team member and execute this.Mostly asked in every interview)

First I have create one bucket in s3 and create a bucket policy and inserted Account ID of another user



{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::203918872713:root"

},

"Action": [

"s3:GetObject",

"s3:ListBucket",

"s3:PutObject"

],

"Resource": [

"arn:aws:s3:::crossaccount-27",

"arn:aws:s3:::crossaccount-27/\*"

]

}

]

}

Now we can access the another account of s3 bucket of other user

