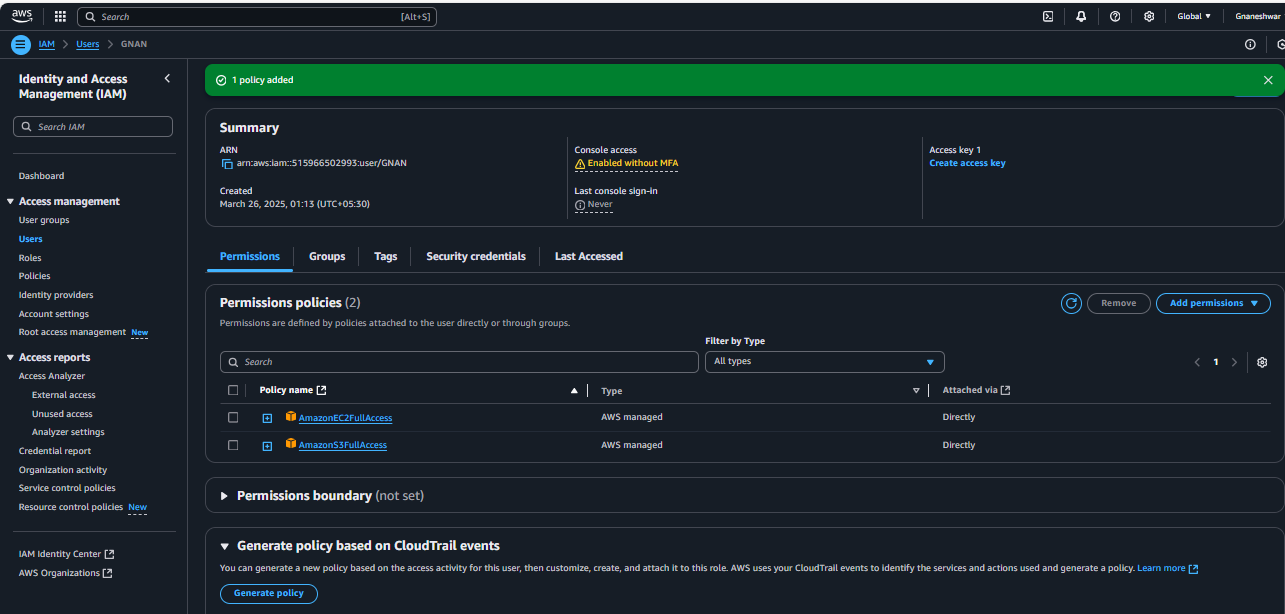
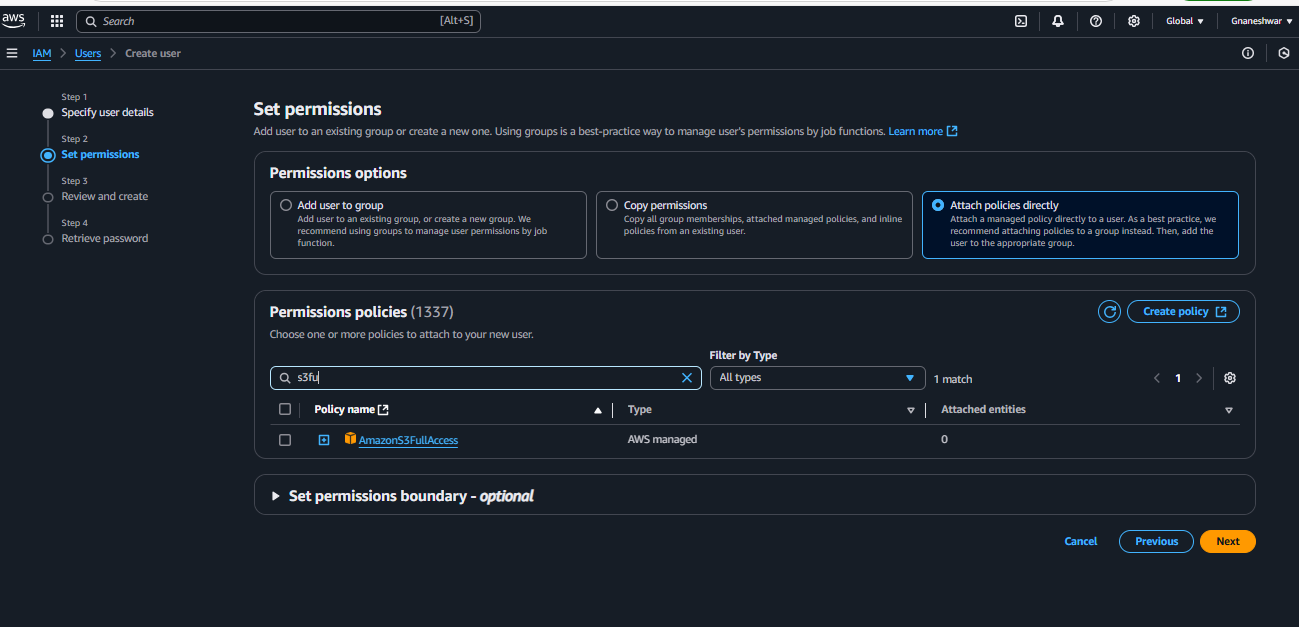
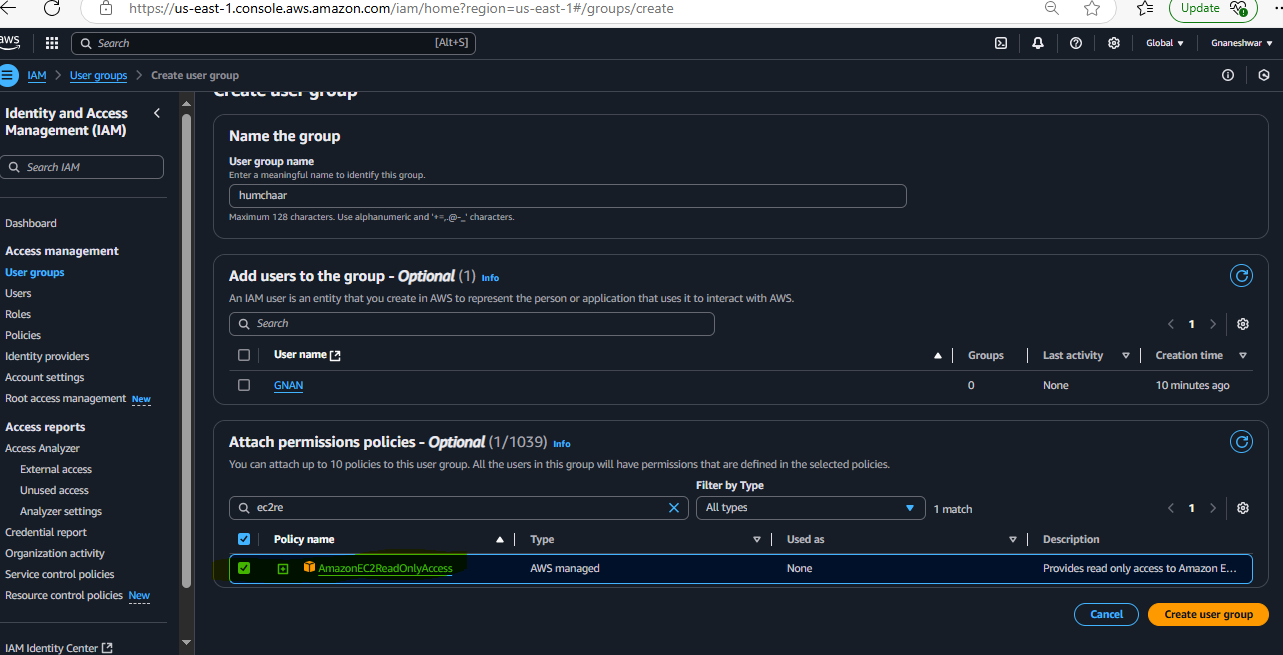
1. Create one IAM user and assign ec2,s3 full access role.

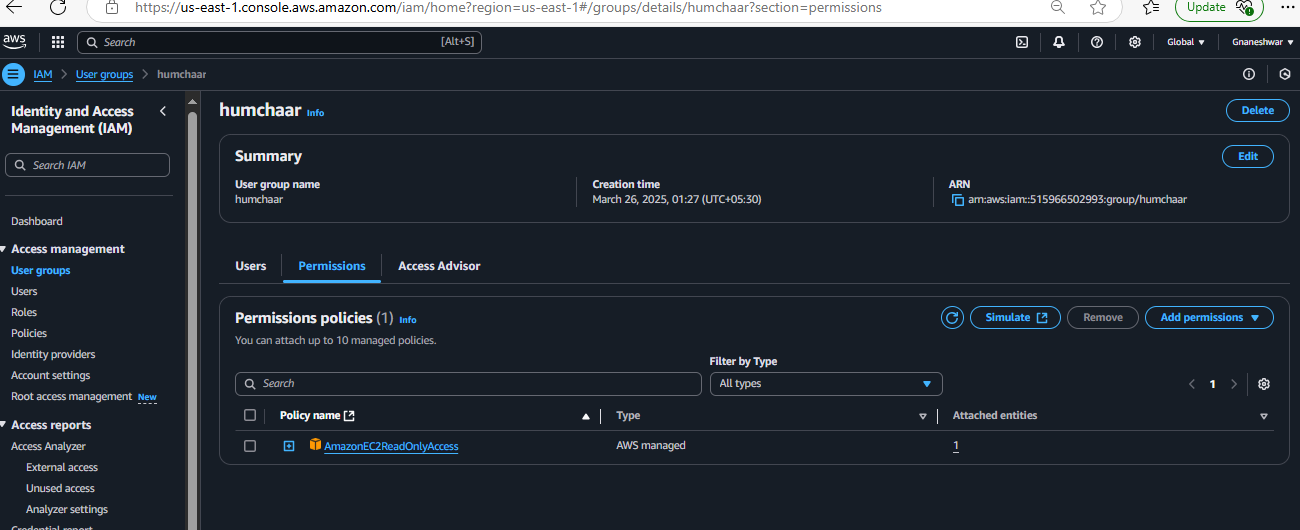
Goto IAM--🡪 Select Users from Dashboard--🡪Create User and then next under Attach policies directly select S3 fullaccess and ec2fullacess



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

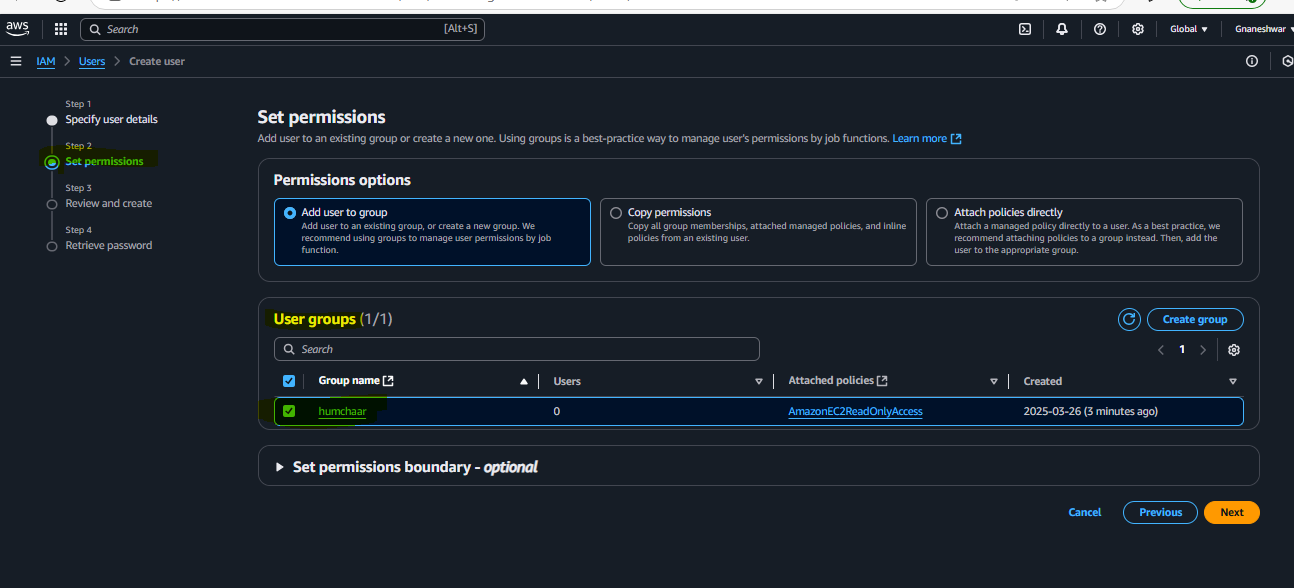
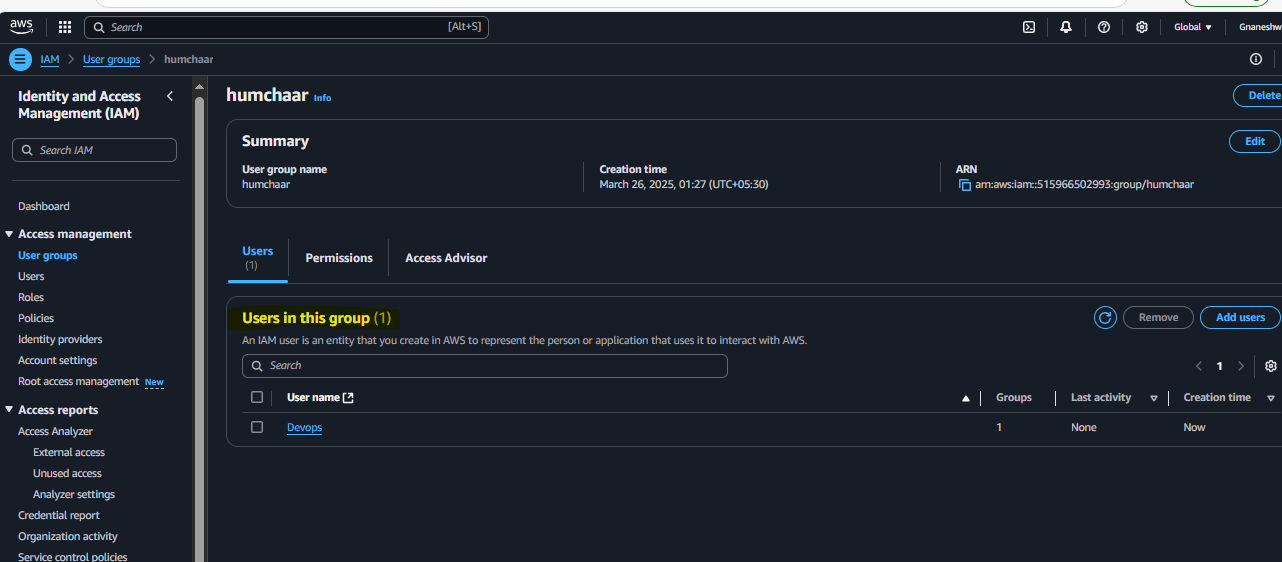
Goto IAM--🡪 Select User groups from Dashboard--🡪Create User group and then next under *Attach policies directly* select *ec2 readonlyaccess*





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

**Create user as mentioned in the Task 1 and while creating choose option under “User groups” for attaching the user to the group**

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

**\*Create an ec2 instance and connect through Git bash by using ssh**

**\*Configure aws by using command “aws configure”**

**Give your AWS account secret credentials “access key ID” and “secret key”**

**Create a bash script file with .sh extentension and give execute permissions to run the script**

**And enter the below given script**

#!/bin/bash

# Define variables

USER\_NAME="gnaneshwarvpc"

POLICY\_ARN="arn:aws:iam::aws:policy/AmazonVPCFullAccess" # VPC full access policy

PROFILE\_NAME="default" # AWS CLI profile name

# Create the IAM user

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

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

# Attach the AmazonVPCFullAccess policy to the user

echo "Attaching policy: AmazonVPCFullAccess to $USER\_NAME..."

aws iam attach-user-policy --user-name $USER\_NAME --policy-arn $POLICY\_ARN --profile $PROFILE\_NAME

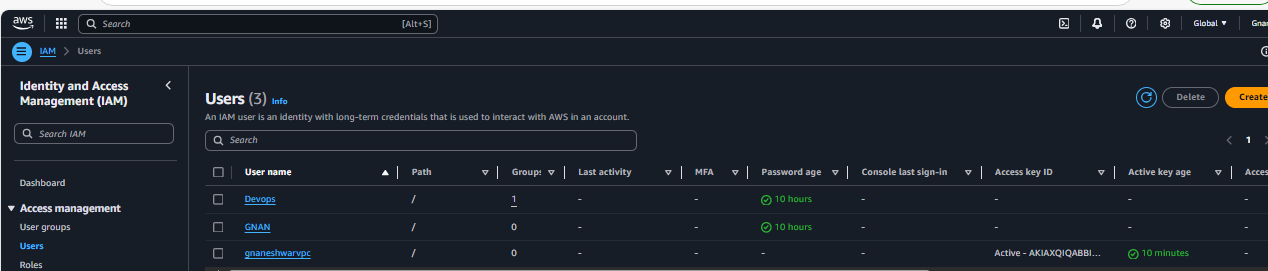
# Generate access keys for the IAM user

echo "Creating access keys for $USER\_NAME..."

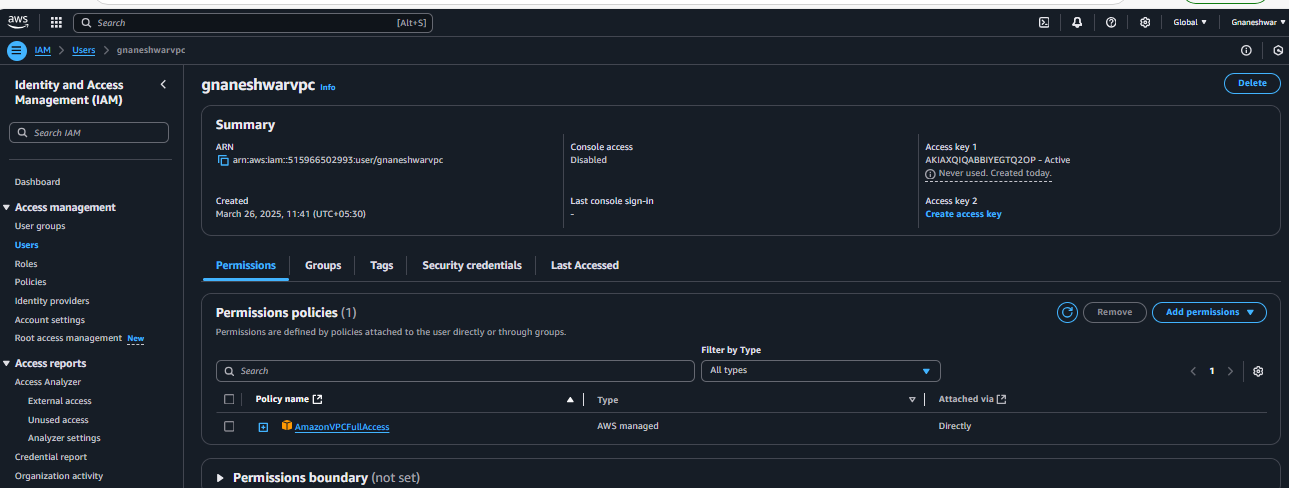
aws iam create-access-key --user-name $USER\_NAME --profile $PROFILE\_NAME

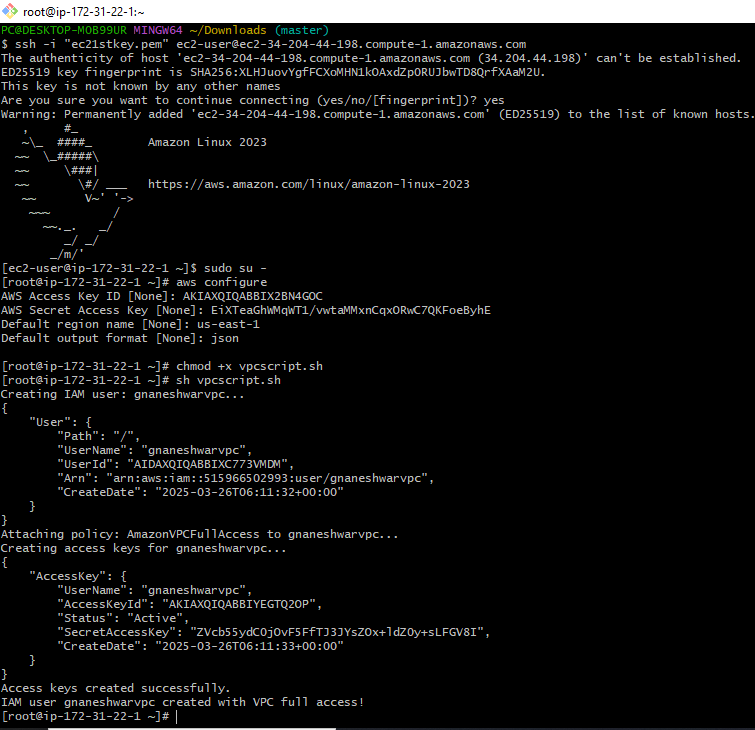
echo "Access keys created successfully."

echo "IAM user $USER\_NAME created with VPC full access!"

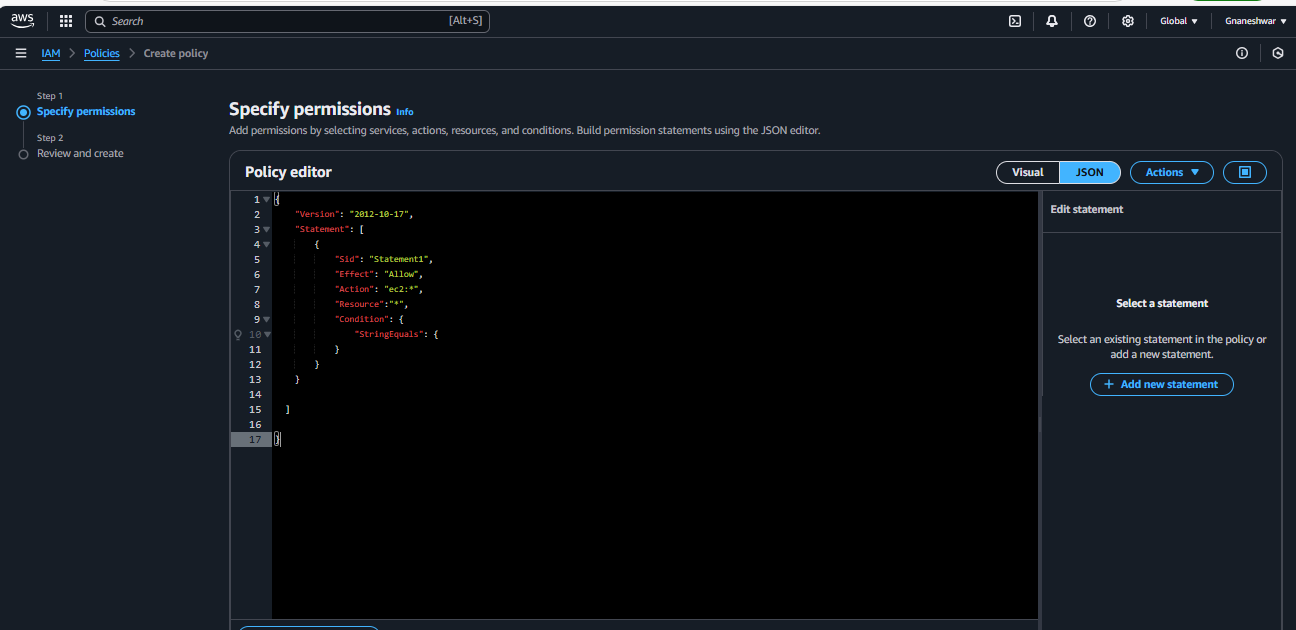
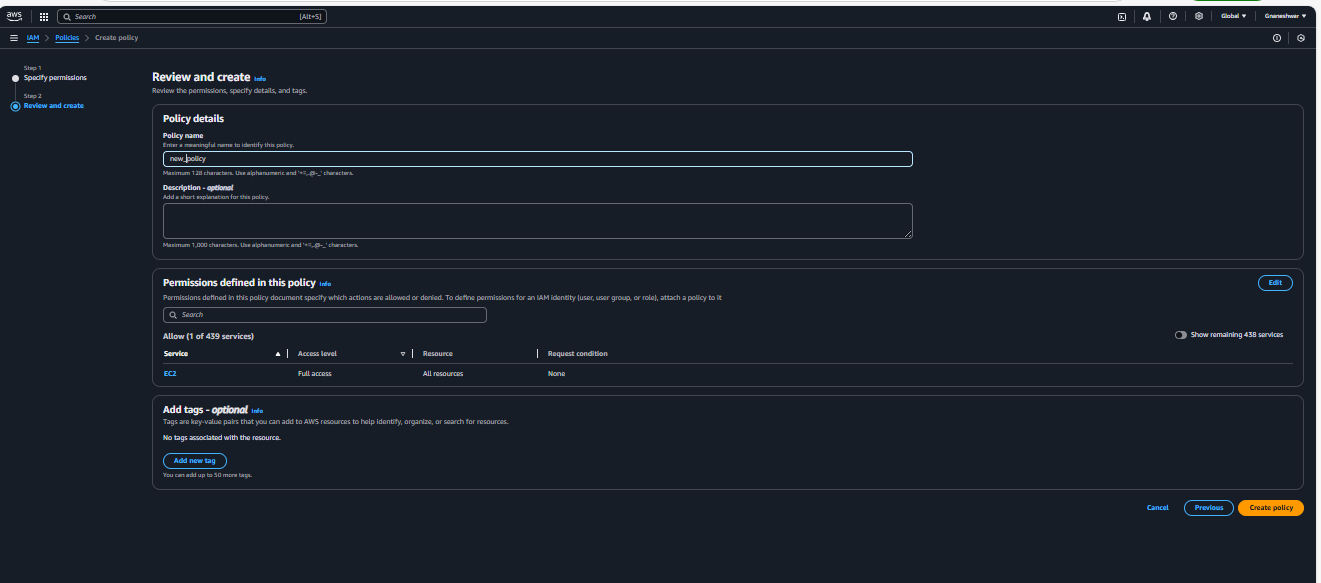
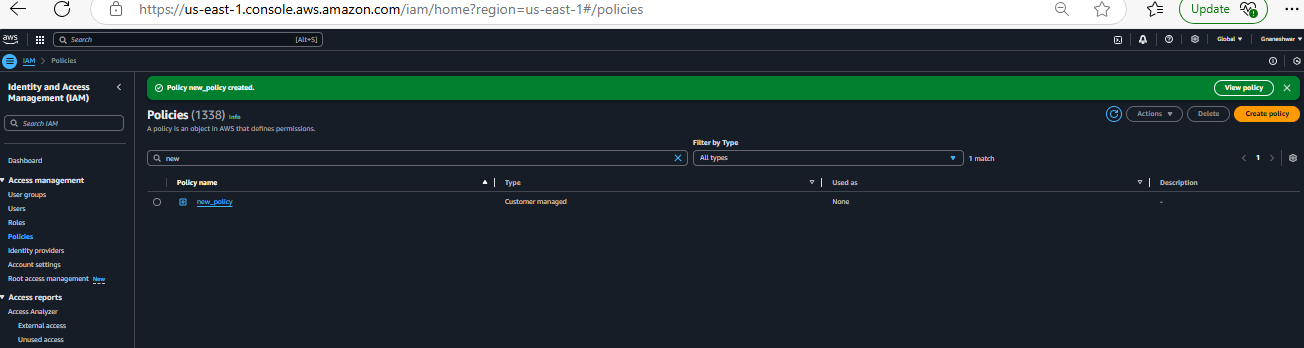


If you check in the Users new user added with VPC fullaccess



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

Goto IAM--🡪 Select Policies from Dashboard--🡪Create policy

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)

**Create a S3 bucket with bucke policy** with other acoount ID ARN

{

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

"Statement": [

{

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::418272767210:root"

},

"Action": [

"s3:GetObject",

"s3:ListBucket",

"s3:PutObject"

],

"Resource": [

"arn:aws:s3:::gobucket9",

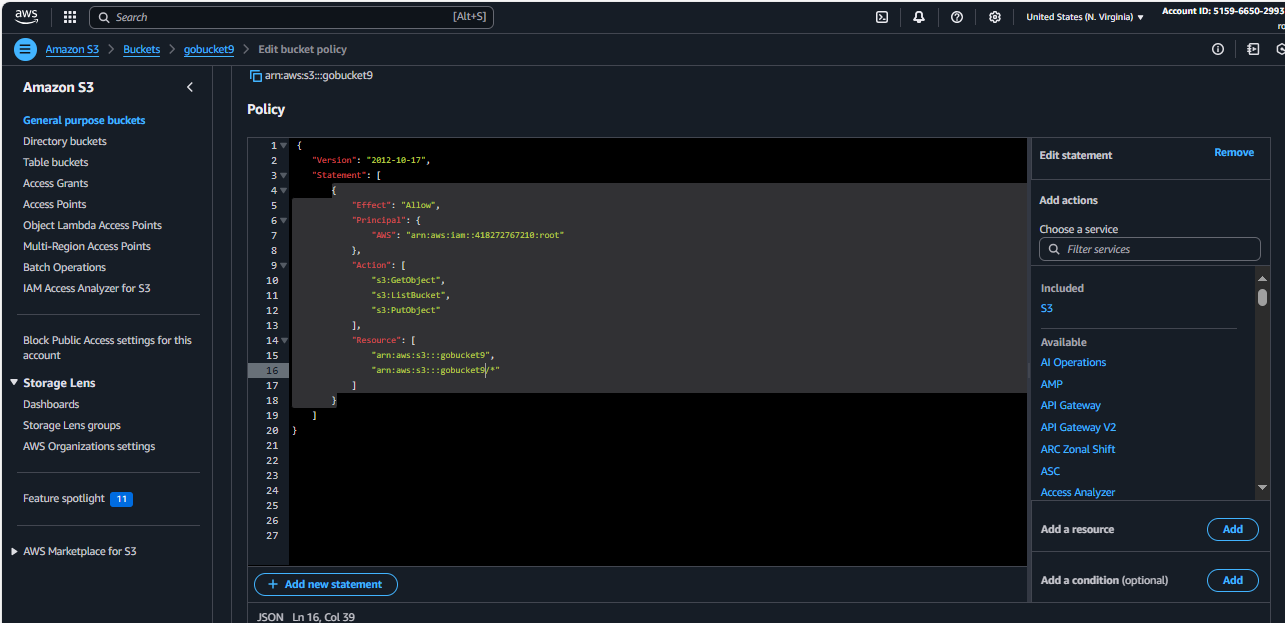
"arn:aws:s3:::gobucket9/\*"

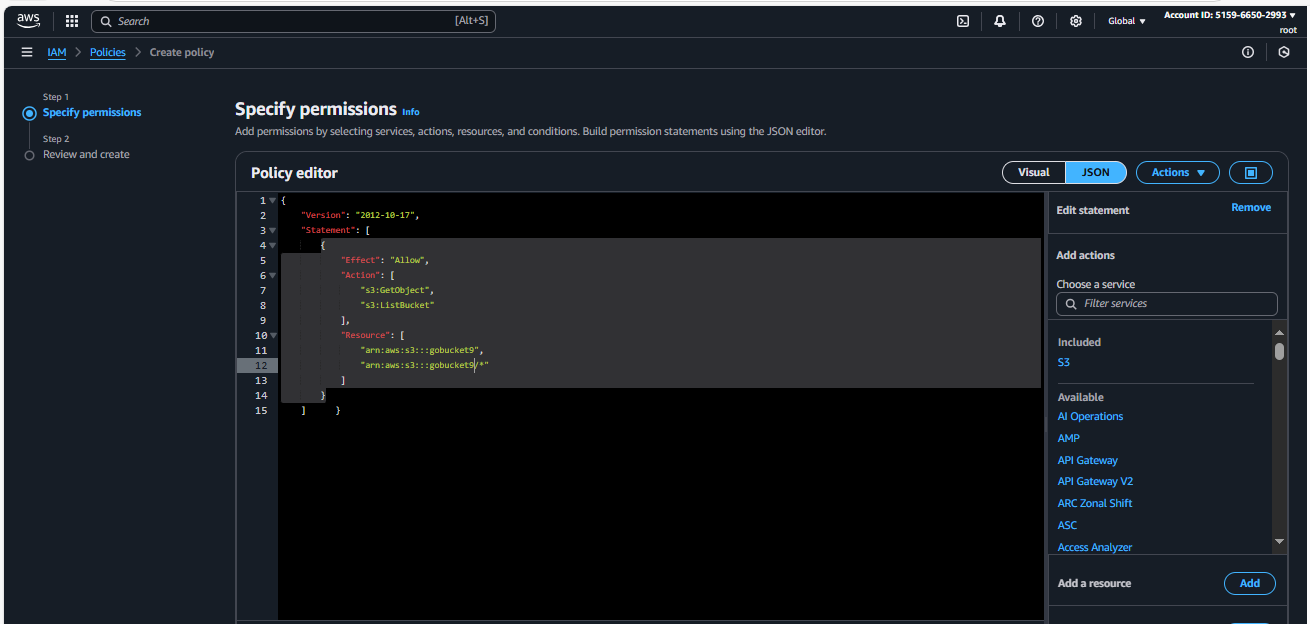
]

}

]

}





Create IAM policy

{

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

"Statement": [

{

"Effect": "Allow",

"Action": [

"s3:GetObject",

"s3:ListBucket"

],

"Resource": [

"arn:aws:s3:::gobucket9",

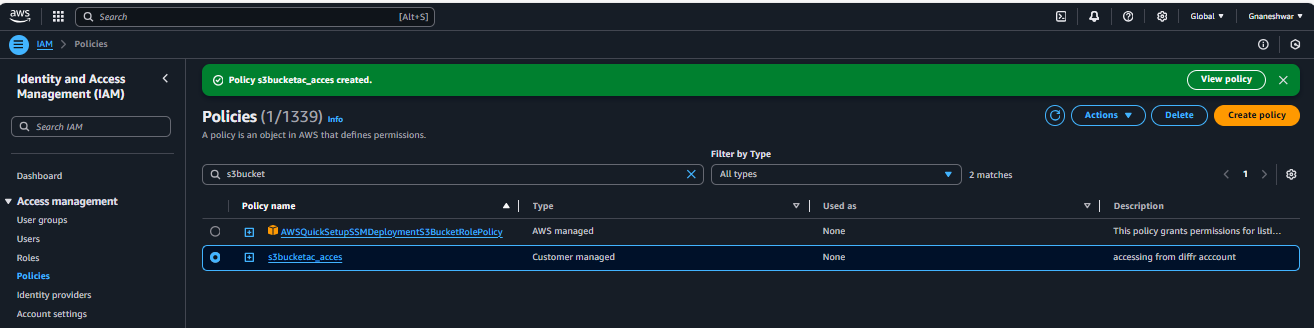
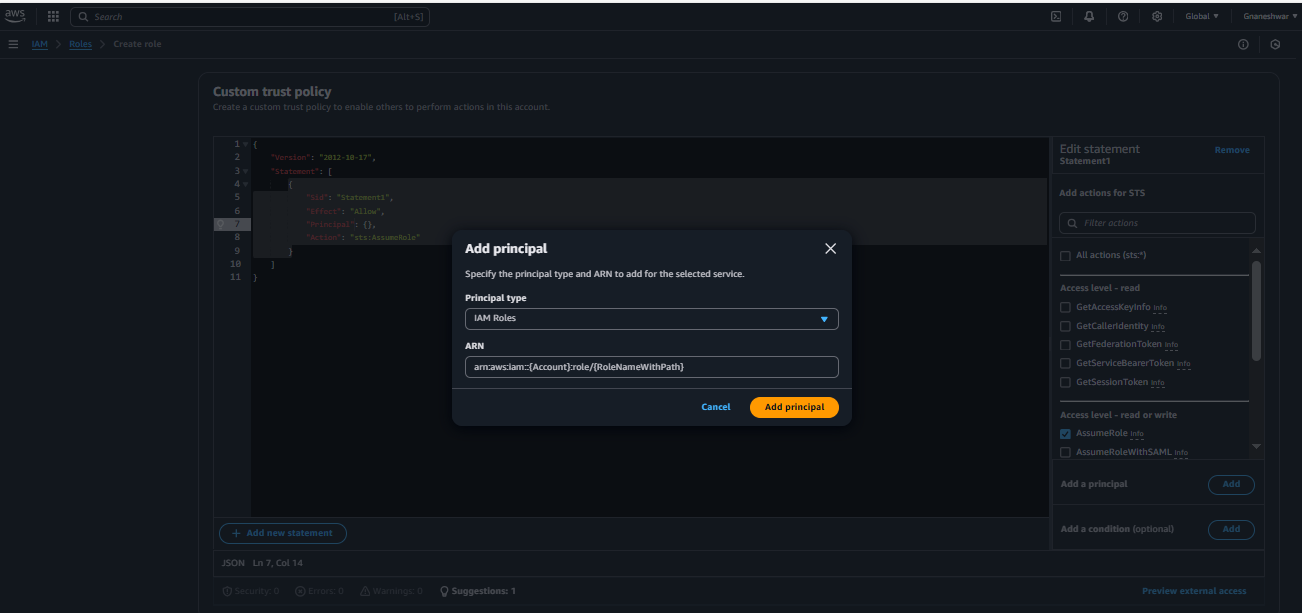
"arn:aws:s3:::gobucket9/\*"

]

}

]

}

IF you check the bucket list from other account ec2 instance using **aws s3 ls arn:aws:s3:::gobucket9**

It will show all the objects available in that bucket **gobucket9**

