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

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

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

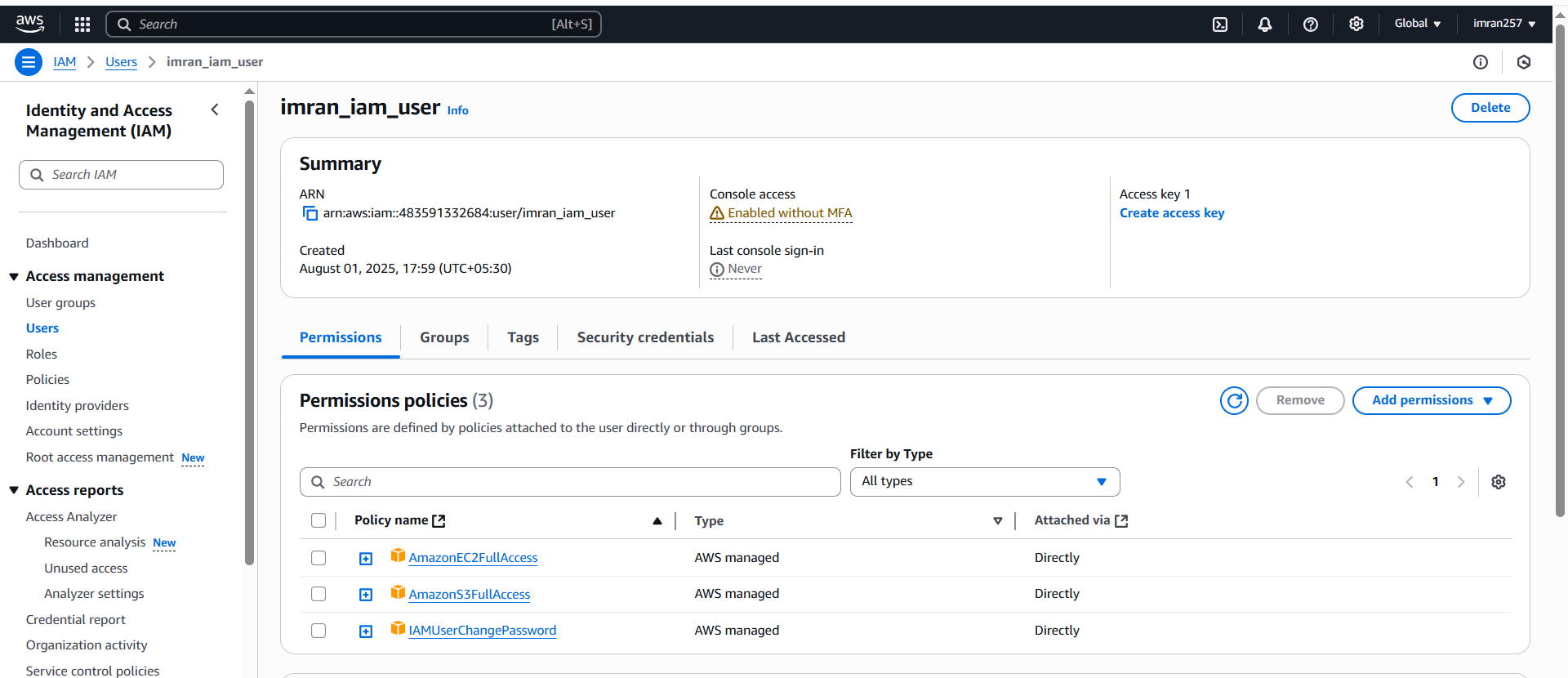
4) Write a bash script to create a IAM user with VPC full access.

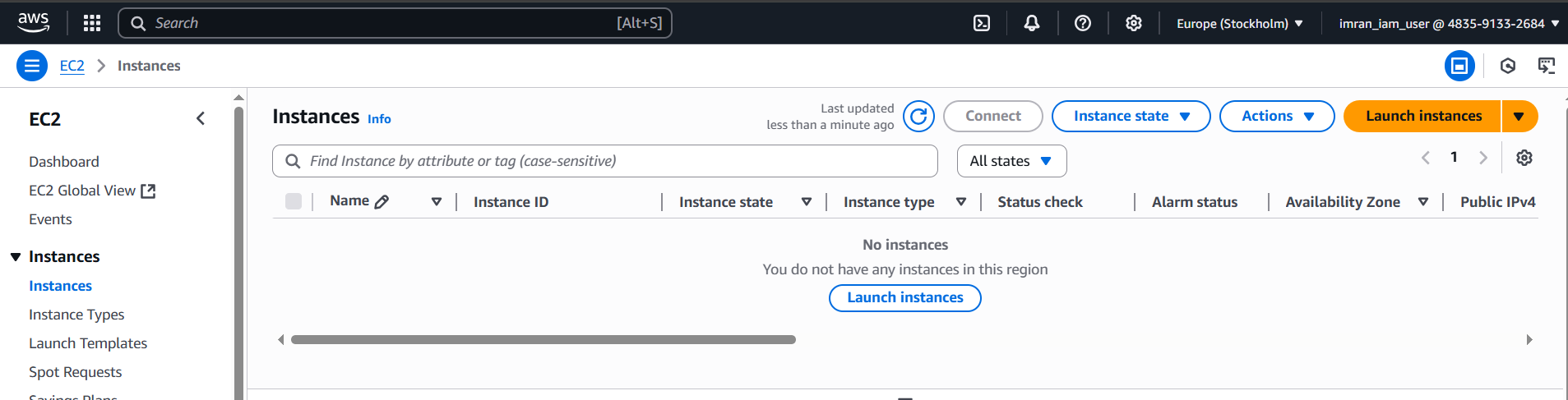
5) Create a IAM policy to access ec2 for a specific user in specific regions only.

6) We have two accounts Account A and Account B, Account A user should access s3 bucket in Account B.

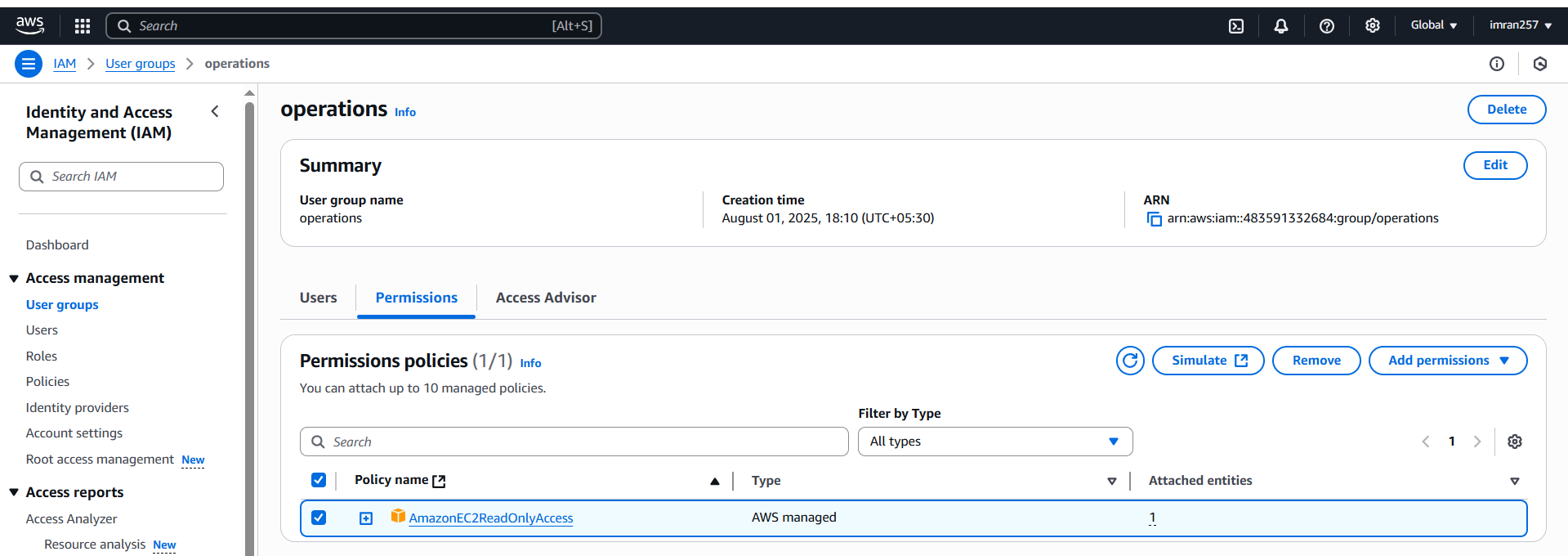
(Collaborate with team member and execute this.Mostly asked in every interview)

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

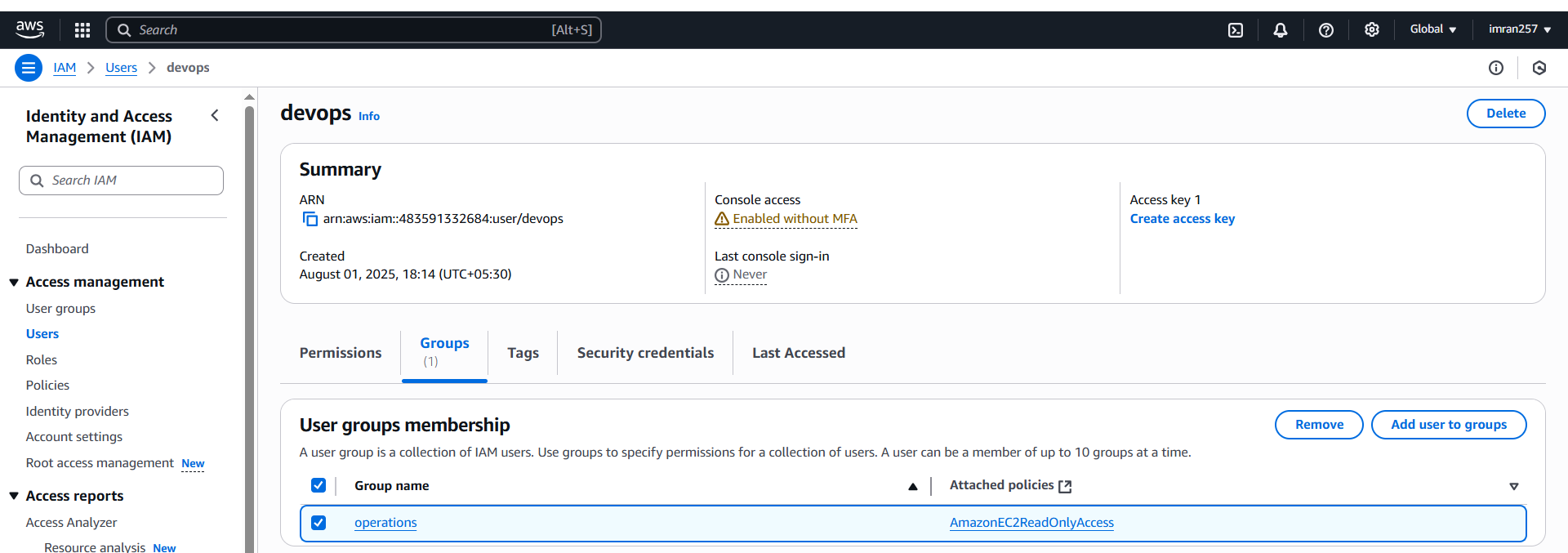
****

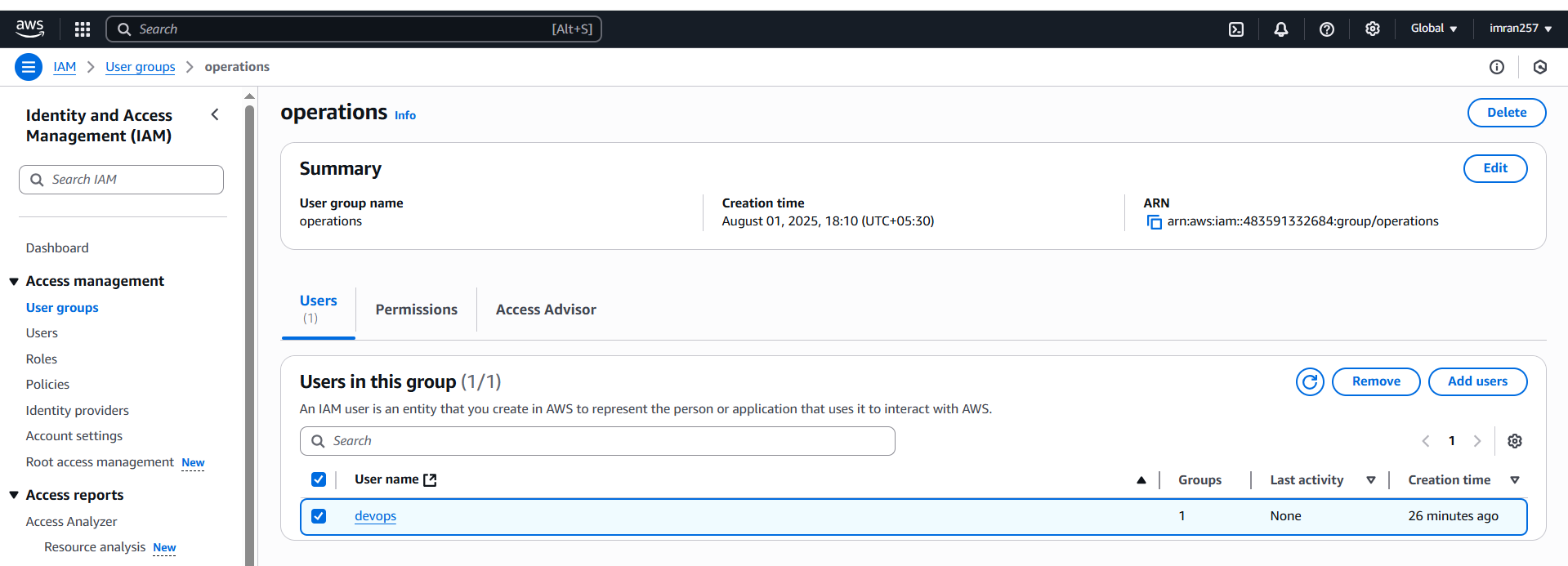
****

**2) Create one Group in IAM and Assign Read access for ec2.**

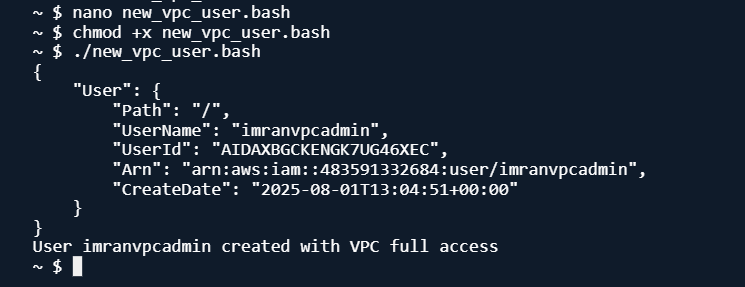
****

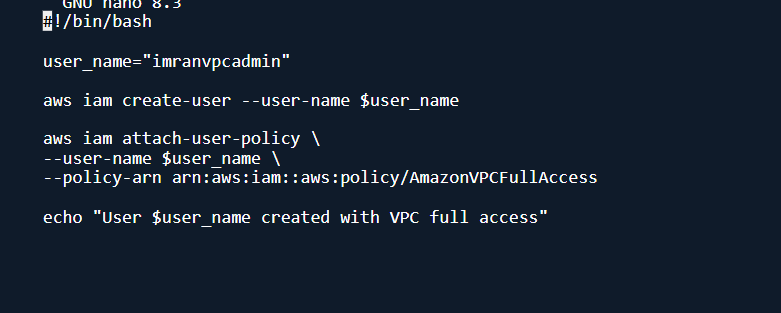
**3) Create a new user with name Devops and add to the group created in task2.**

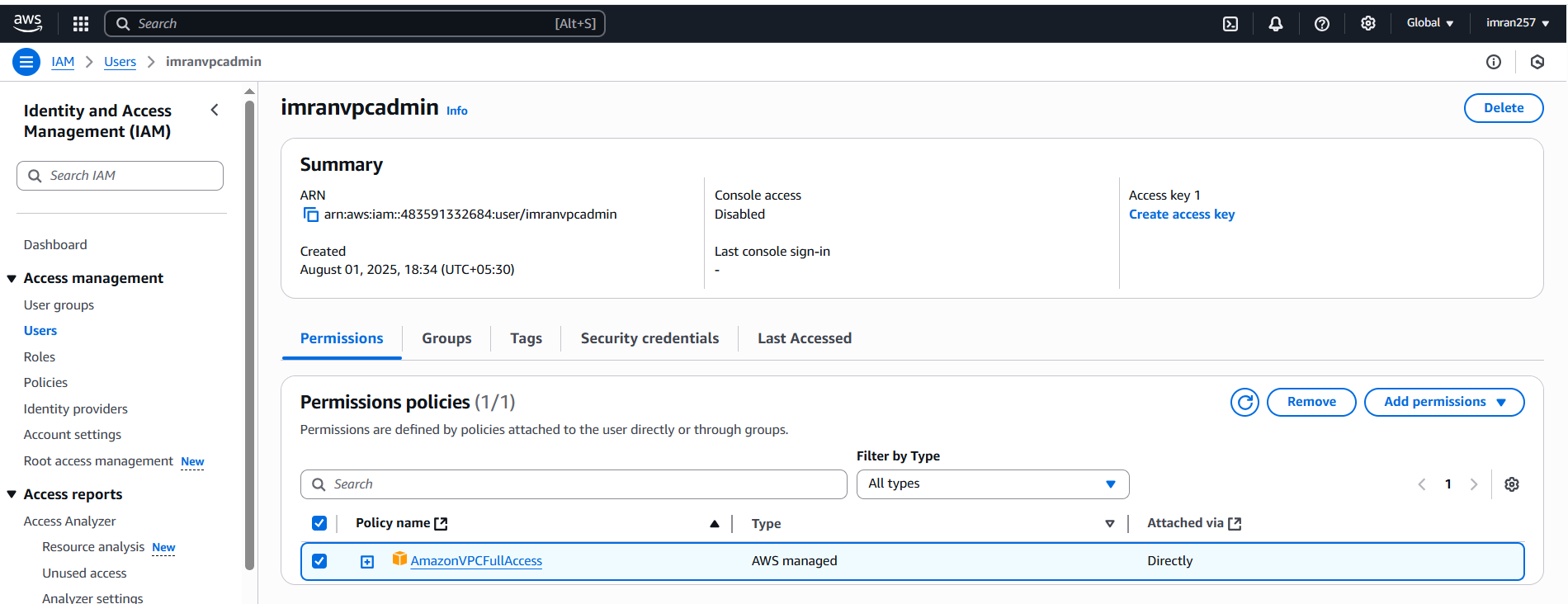
****

****

**4) Write a bash script to create a IAM user with VPC full access.**

****

****

****

**5) Create a IAM policy to access ec2 for a specific user in specific regions only.**

1. **Go to IAM → Policies → create policy → json**
2. **Enter below script and create and assign to user**

**{**

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

**"Statement": [**

**{**

**"Sid": "AllowEC2SpecificRegions",**

**"Effect": "Allow",**

**"Action": "ec2:\*",**

**"Resource": "\*",**

**"Condition": {**

**"StringEquals": {**

**"aws:RequestedRegion": ["us-east-1", "us-west-2"]**

**}**

**}**

**},**

**{**

**"Sid": "DenyEC2OtherRegions",**

**"Effect": "Deny",**

**"Action": "ec2:\*",**

**"Resource": "\*",**

**"Condition": {**

**"StringNotEquals": {**

**"aws:RequestedRegion": ["us-east-1", "us-west-2"]**

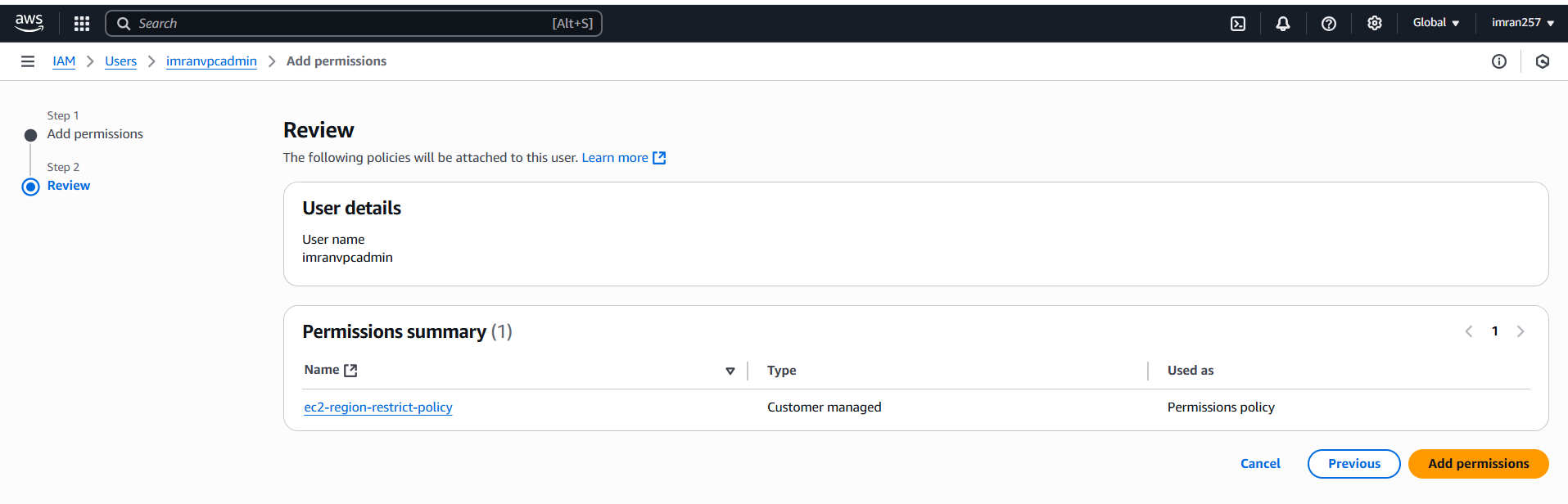
**}**

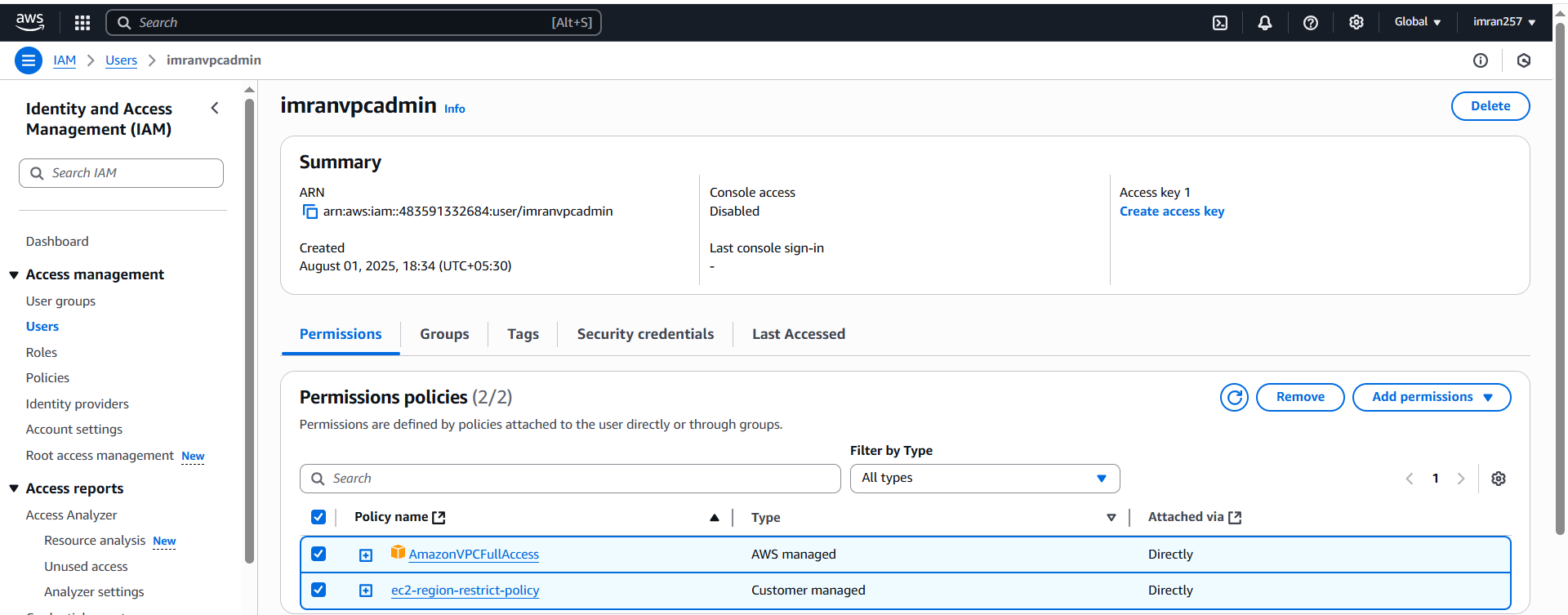
**}**

**}**

**]**

**}**

****

****

**6) 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)**

**Imran account A.**

1. **From here open IAM and create user imran and provide inline policy.**

**{**

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

**"Statement": [**

**{**

**"Sid": "Example",**

**"Effect": "Allow",**

**"Action": [**

**"s3:ListBucket"**

**],**

**"Resource": [**

**"arn:aws:s3:::cross-account-s3-imran;"**

**]**

**}**

**]**

**}**

1. **Account B need to Create s3 bucket and give bucket policy.**

**{**

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

**"Statement": [**

**{**

**"Sid": "Example permissions",**

**"Effect": "Allow",**

**"Principal": {**

**"AWS": "arn:aws:iam::483591332684:root"**

**},**

**"Action": [**

**"s3:GetLifecycleConfiguration",**

**"s3:ListBucket"**

**],**

**"Resource": [**

**"arn:aws:s3:::vaseem.shop"**

**]**

**}**

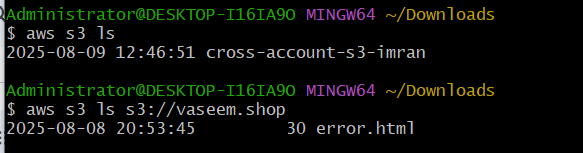
**]**

**}**

**Now open bash window and configure aws with imran access key,**

**Now check**

**aws s3 ls s3://vaseem.shop**

****