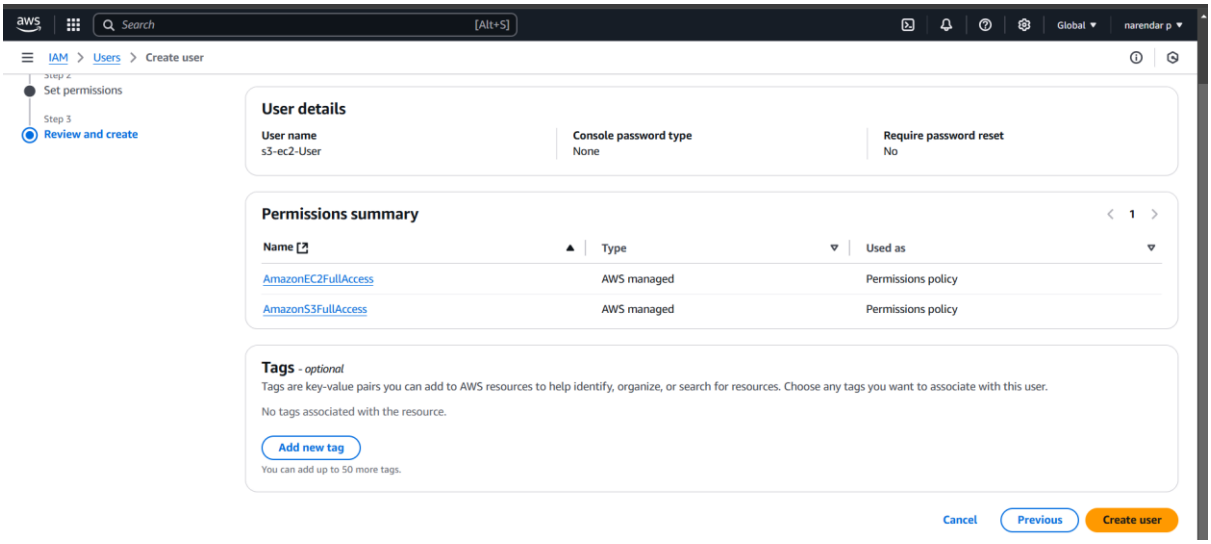
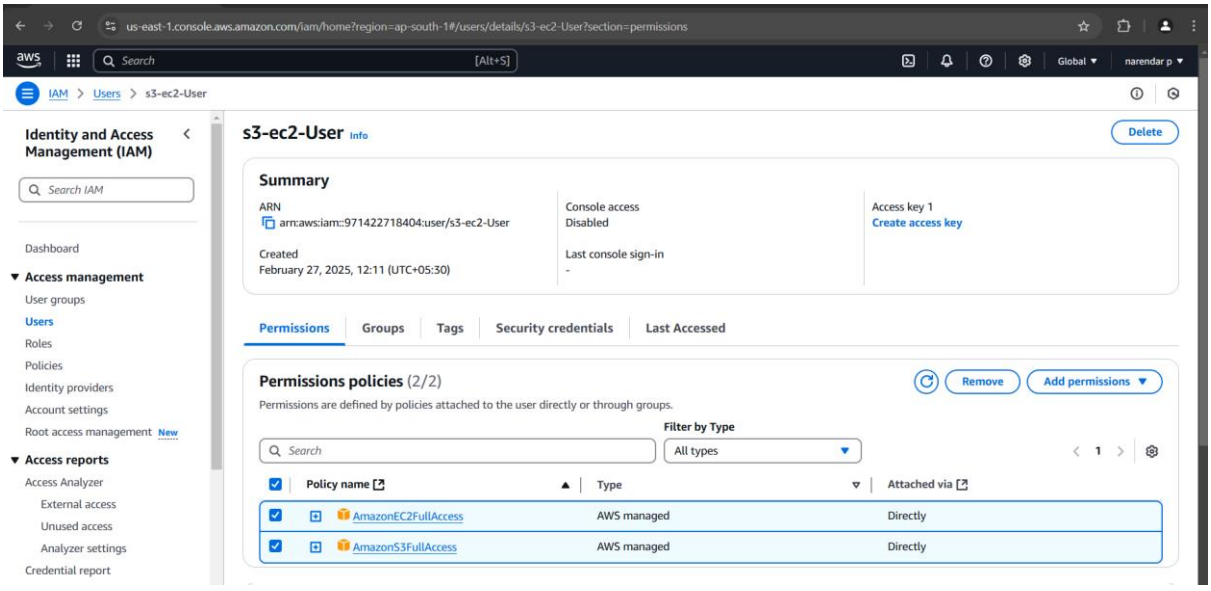
26-02-2025

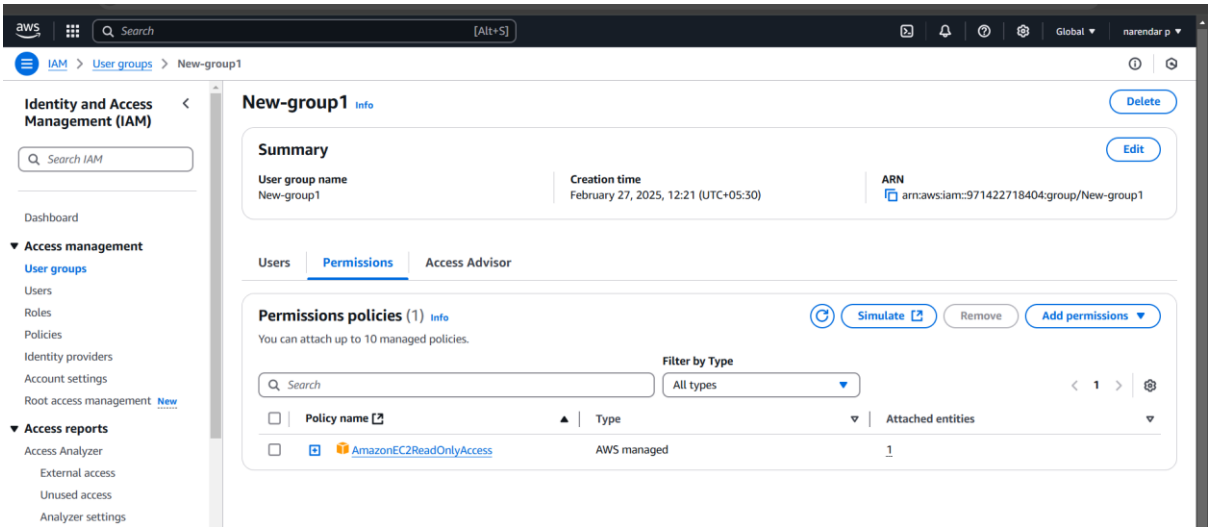
TASK ON IAM

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

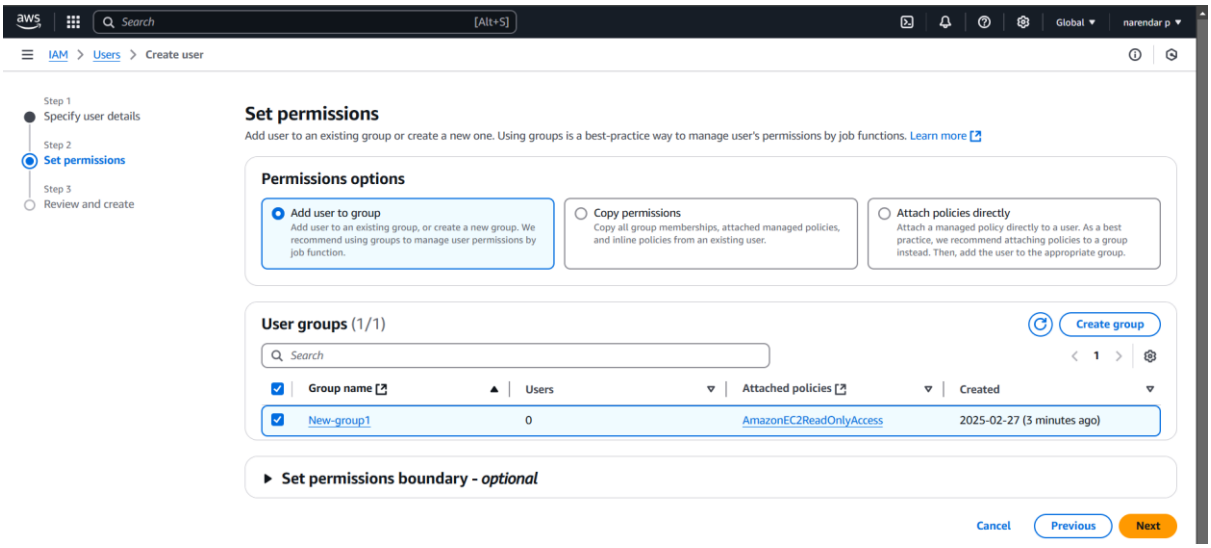


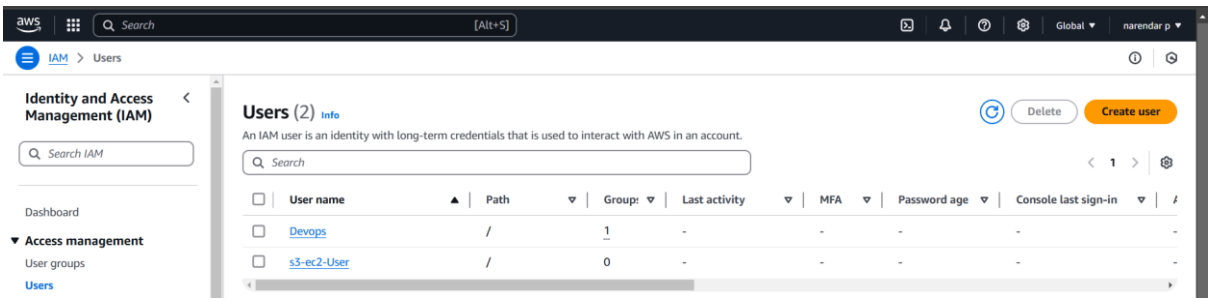


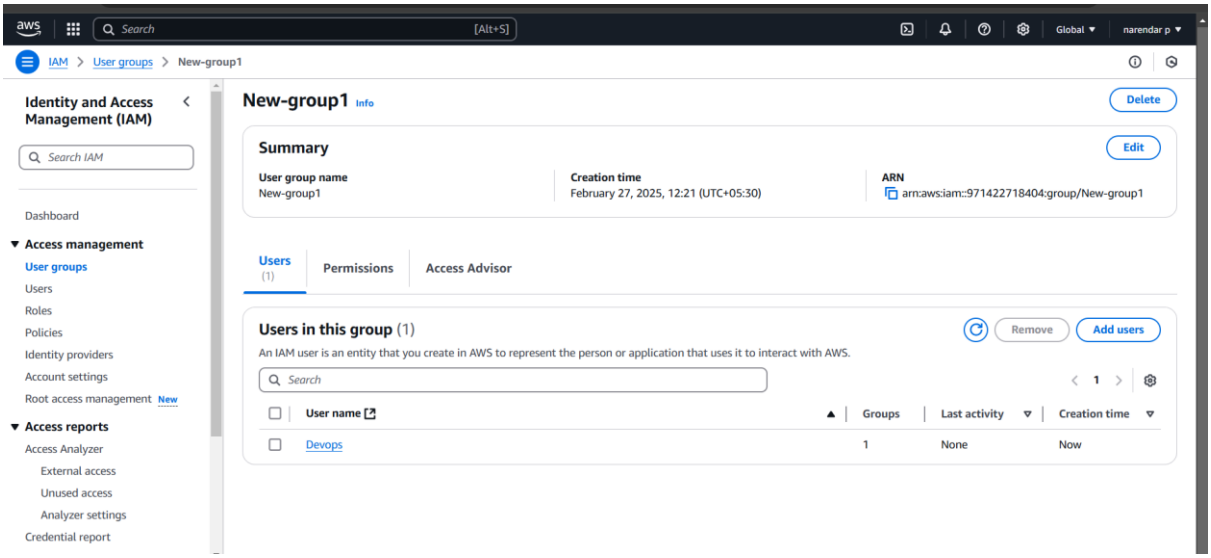
2) Create one Group in IAM and Assign Read access for ec2:



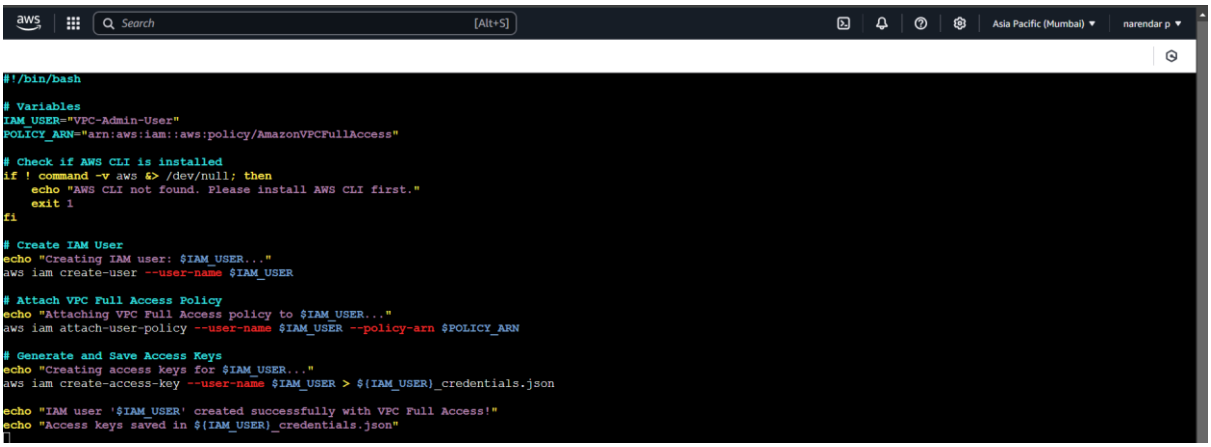
3) Create a new user with name DevOps and add to the group created in task2:

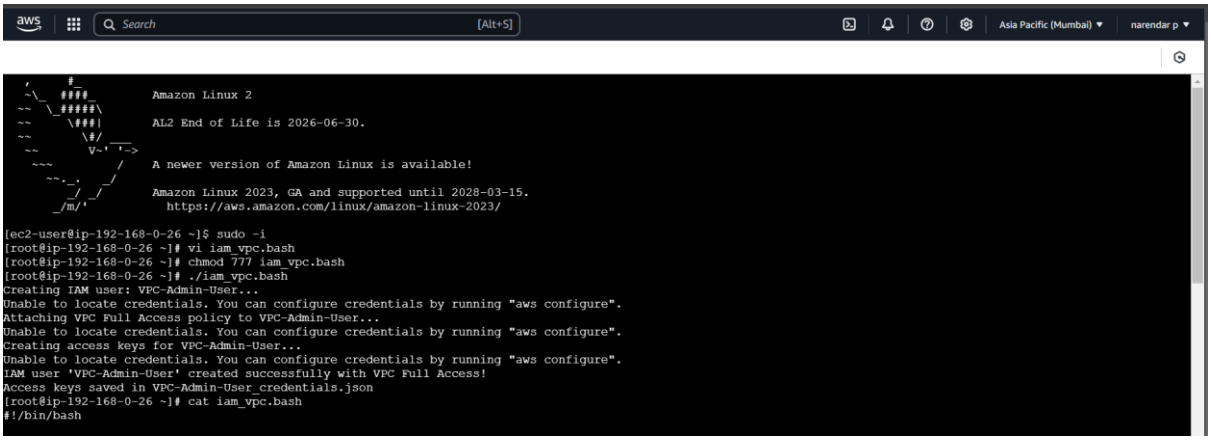




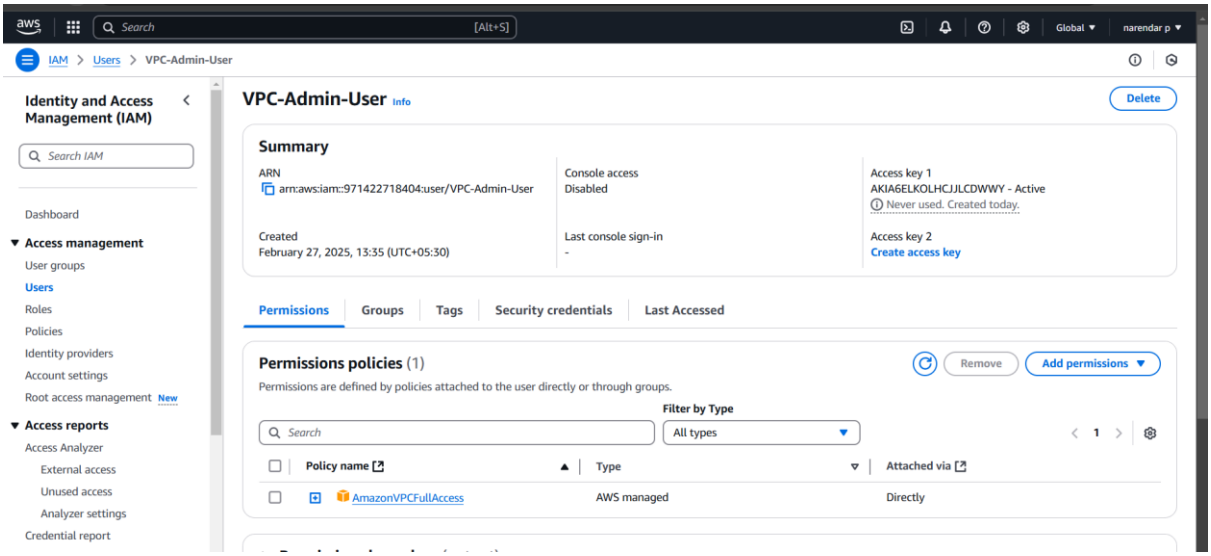


4) Write a bash script to create a IAM user with VPC full access:



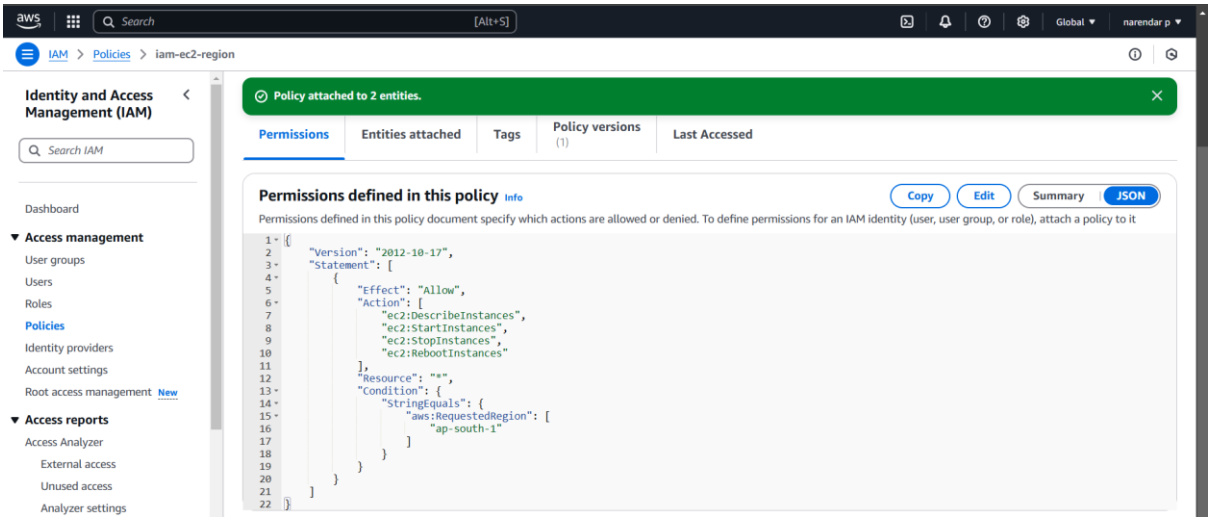


```
[root@ip-192-168-0-26 ~]# aws configure
AWS Access Key ID [None]: AKIA6ELKOLHCFDRJTV7W
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: json
[root@ip-192-168-0-26 ~]# ./iam_vpc.bash
Creating IAM user: VPC-Admin-User...
{
    "User": {
        "UserName": "VPC-Admin-User",
        "Path": "/",
        "CreateDate": "2025-02-27T08:05:45Z",
        "UserId": "AIDA6ELKOLHCFY7DTXTOL",
        "Arn": "arn:aws:iam::971422718404:user/VPC-Admin-User"
    }
}
Attaching VPC Full Access policy to VPC-Admin-User...
Creating access keys for VPC-Admin-User...
IAM user 'VPC-Admin-User' created successfully with VPC Full Access!
Access keys saved in VPC-Admin-User_credentials.json
```

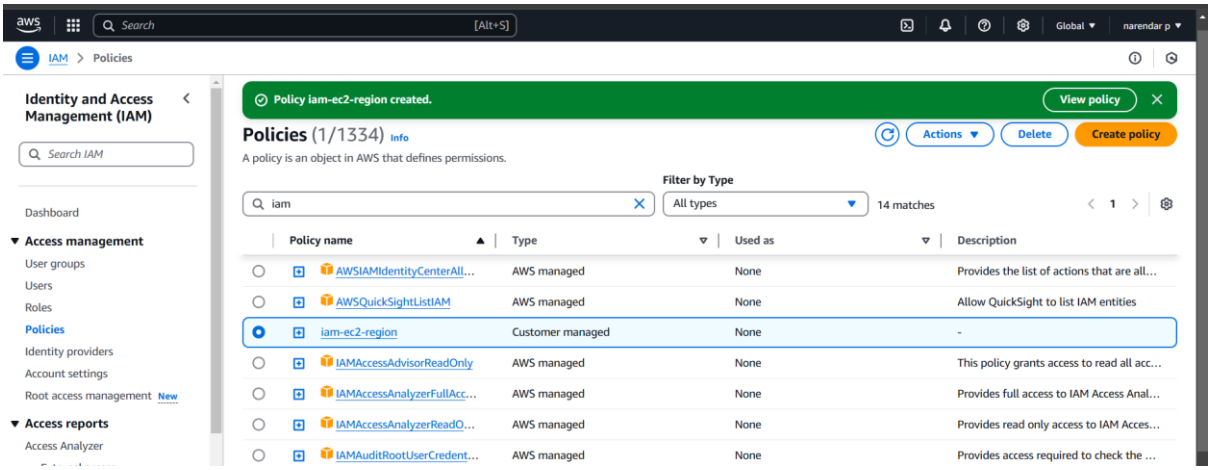


5) Create a IAM policy to access ec2 for a specific user in specific regions only:

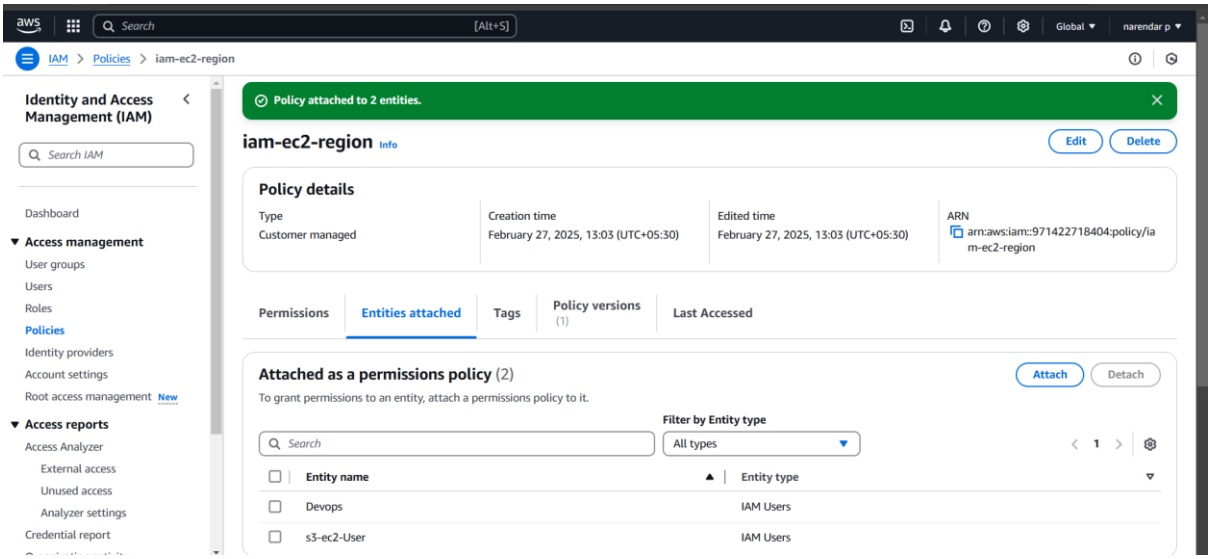
Json entry: To create IAM policy to access ec2 in specific region:



Created Policy:

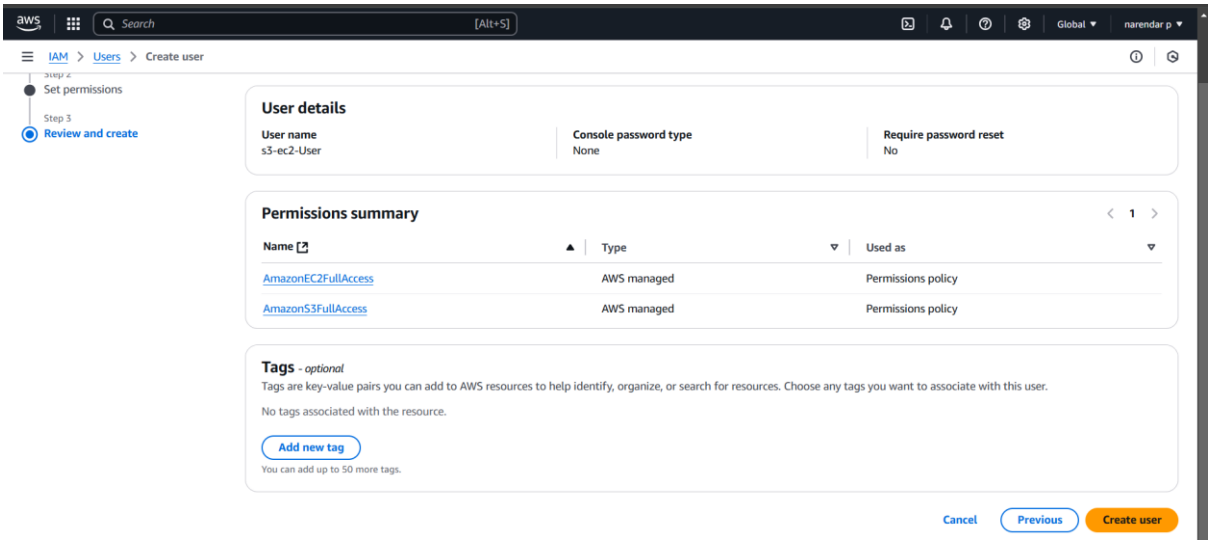


Attached users to the Policy:

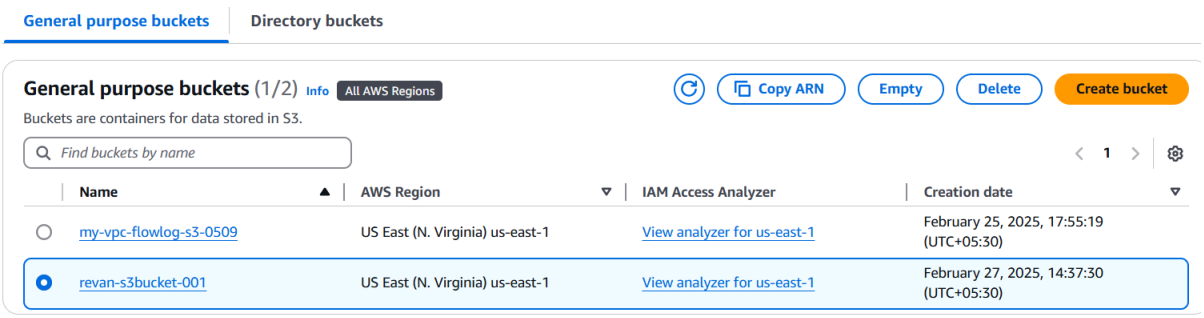


6) We have two accounts Account A and Account B, Account A user should access s3 bucket in Account B.

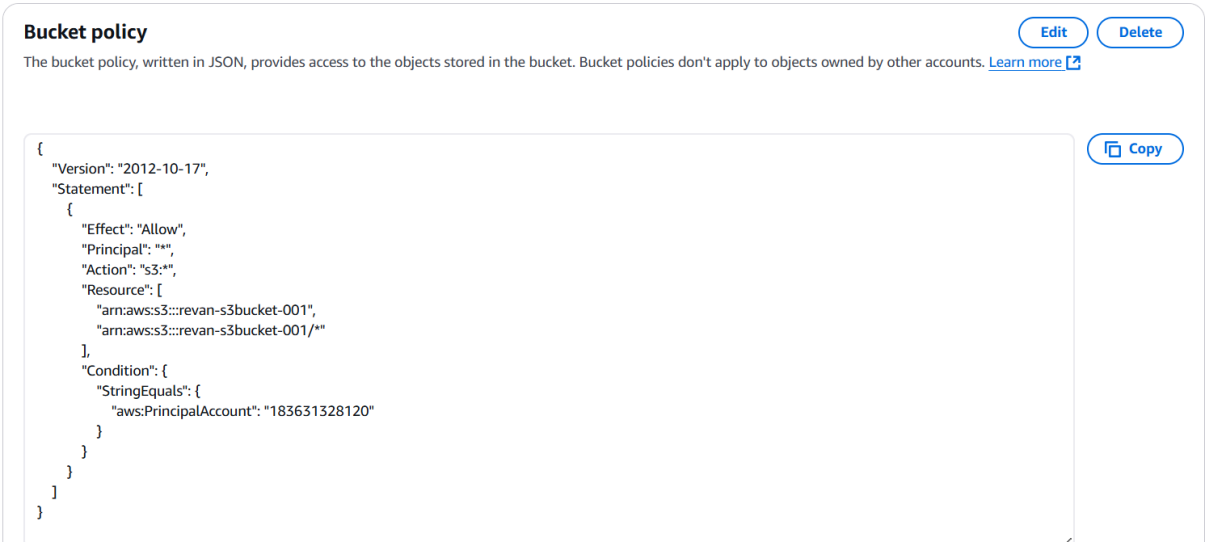
(Collaborate with team member and execute this. Mostly asked in every interview):



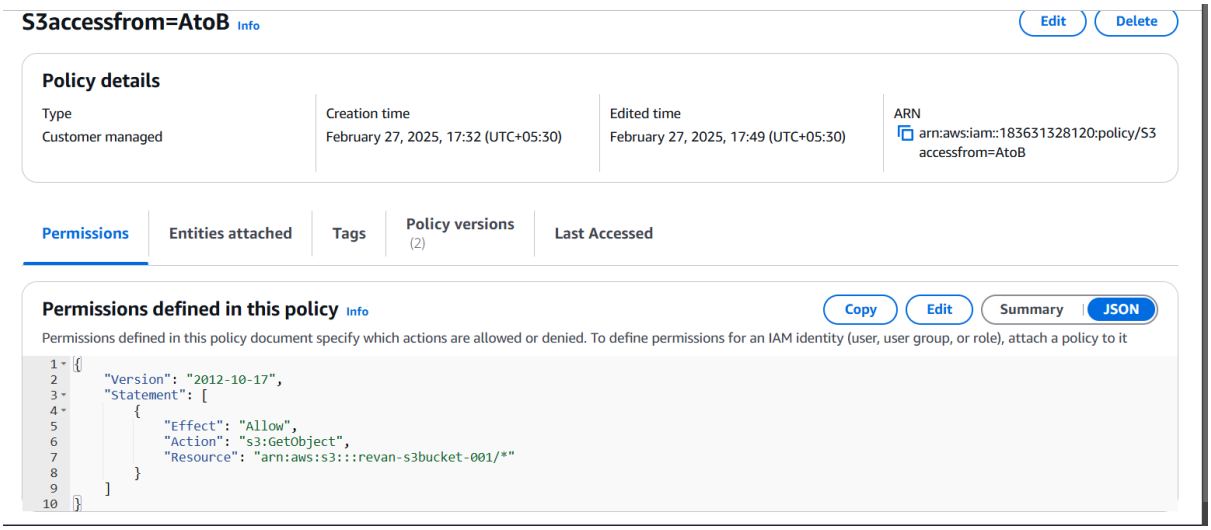
➔ Created a s3 bucket from my account (Account B)



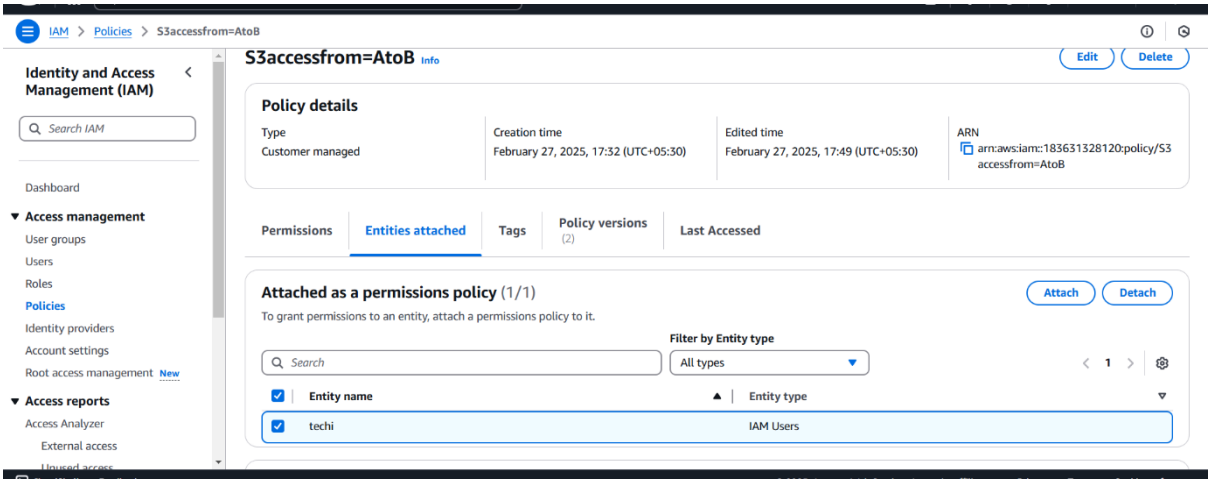
➔ Attached a json policy to the s3 bucket, adding account A id:



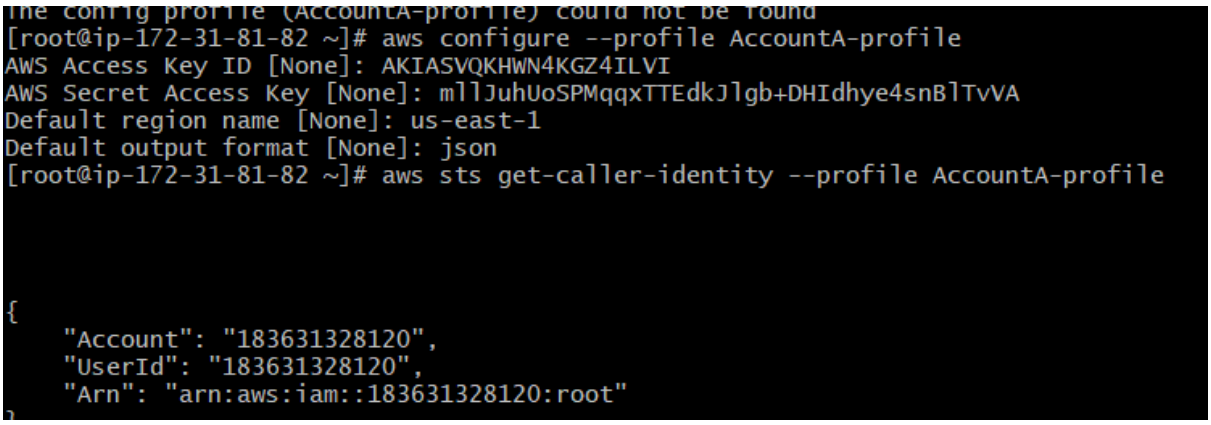
➔ Created a s3 bucket access policy from account A



➔ Attached an IAM user (techi) to this policy (from account A)



➔ Configured Account A account using aws cli



➔ s3 bucket objects in account B

revan-s3bucket-001 Info

Objects | Metadata | Properties | Permissions | Metrics | Management | Access Points

Objects (1/1) Copy S3 URI | Copy URL | Download | Open | Delete | Actions | Create folder | Upload

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

1

Name	Type	Last modified	Size	Storage class
challenge.bash	bash	February 27, 2025, 18:07:55 (UTC+05:30)	194.0 B	Standard

➔ Account A was able to access the s3 bucket objects of account B, using below command:

```
[root@ip-172-31-81-82 ~]#
[root@ip-172-31-81-82 ~]# aws s3 ls s3://revan-s3bucket-001 --profile AccountA-profile
[root@ip-172-31-81-82 ~]# aws s3 ls s3://revan-s3bucket-001 --profile AccountA-profile
2025-02-27 12:37:55        194 challenge.bash
[root@ip-172-31-81-82 ~]# aws s3 ls s3://bucket060918 --profile AccountA-profile
2025-02-27 12:57:26     221037 challenge-3.docx
[root@ip-172-31-81-82 ~]# exit
```