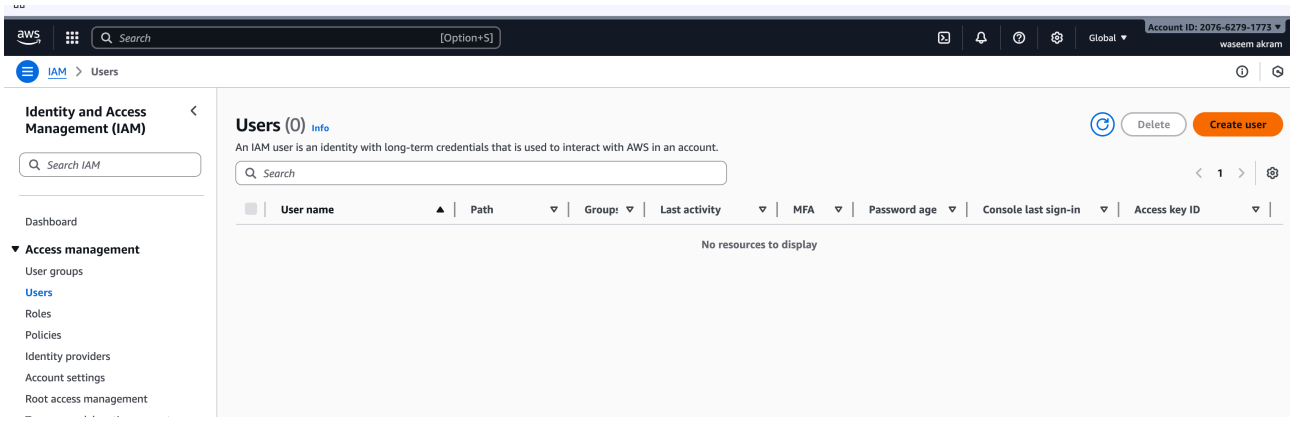
IAM TASK

1)Create one IAM user and assign EC2 and S3 full access roles.

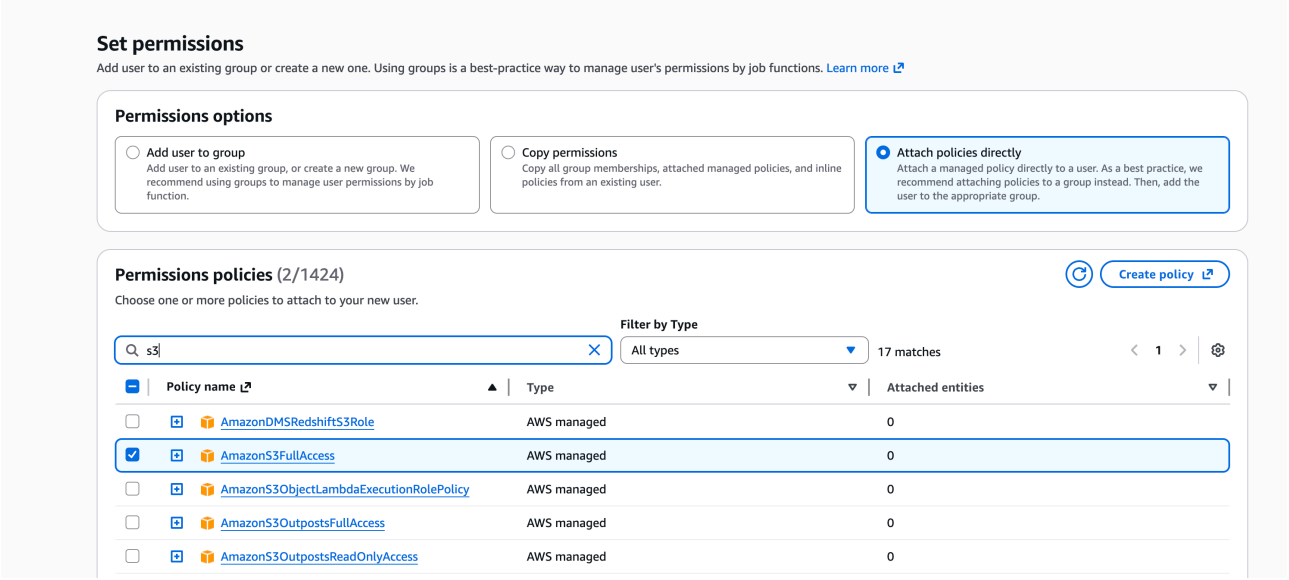
—> go to IAM and —> users —> create user—> give user name as myuser—> click next

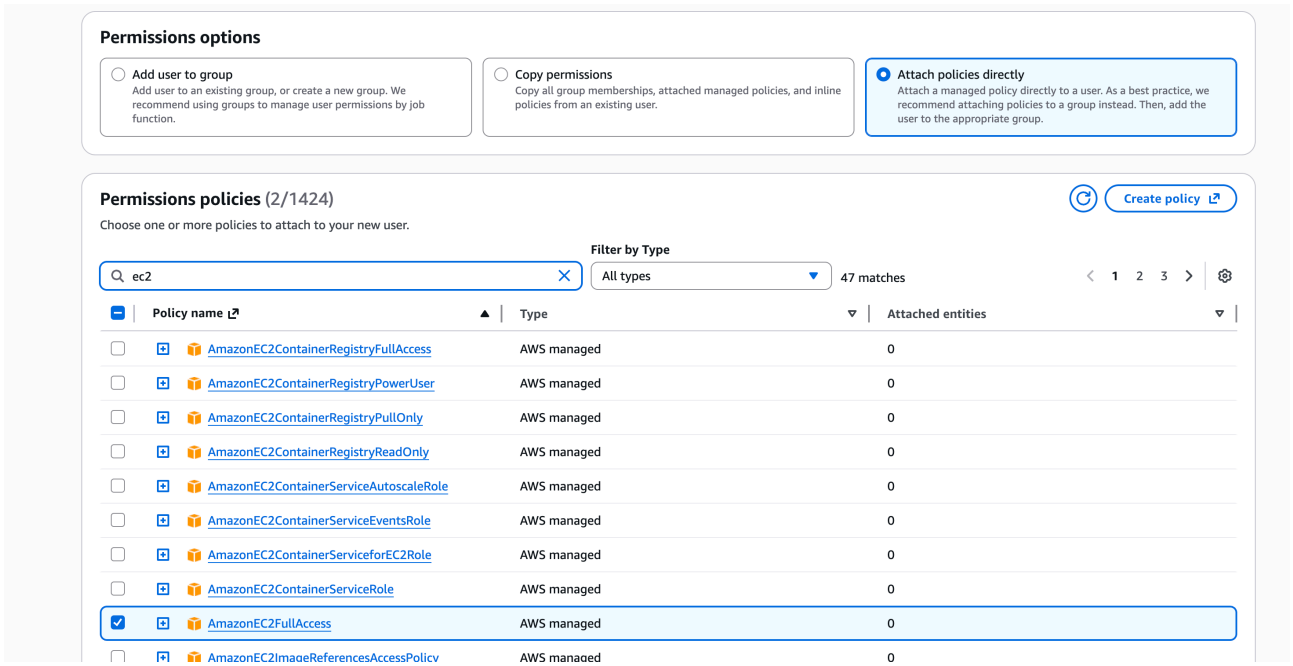


—> 2) Assign Permissions

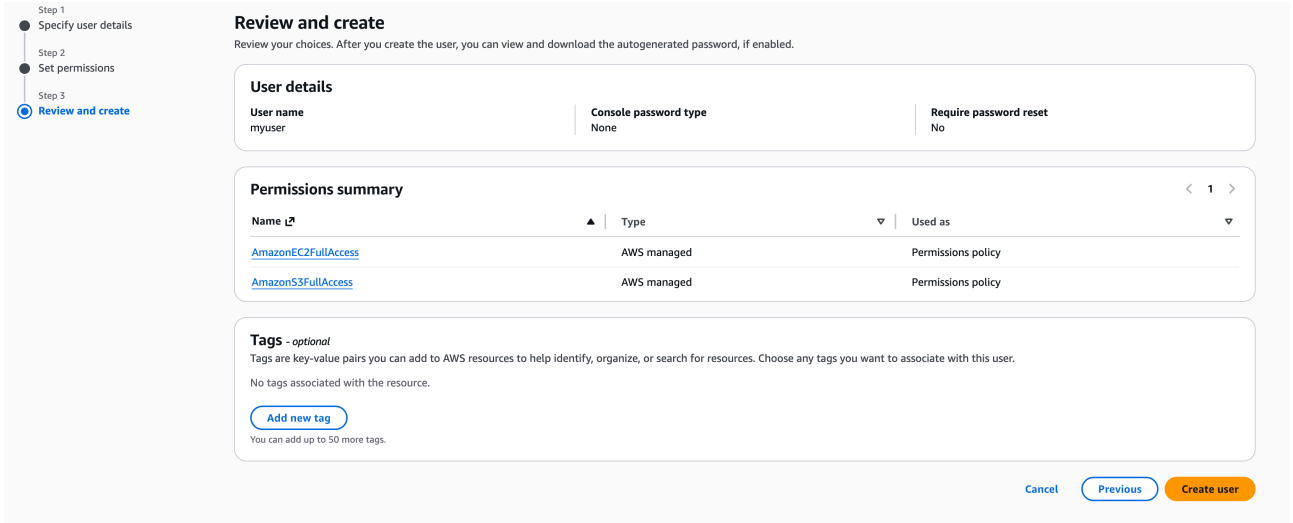
On the "Permissions" page:

1. Select **Attach existing policies directly**
2. Search for:
   - **AmazonEC2FullAccess**
   - **AmazonS3FullAccess**
3. Tick both checkboxes.

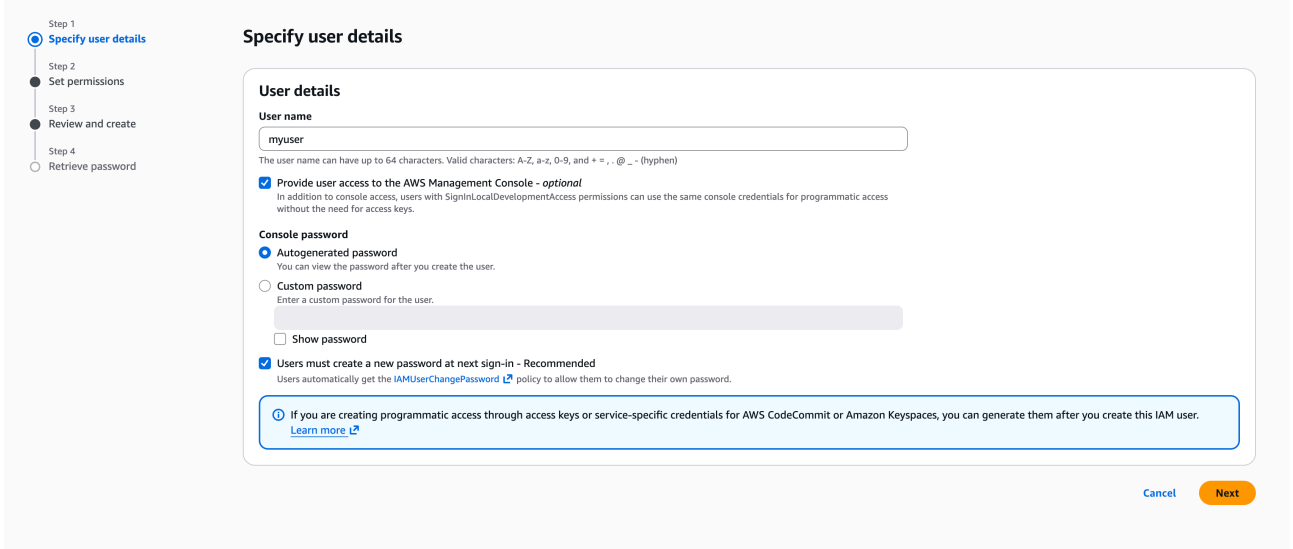




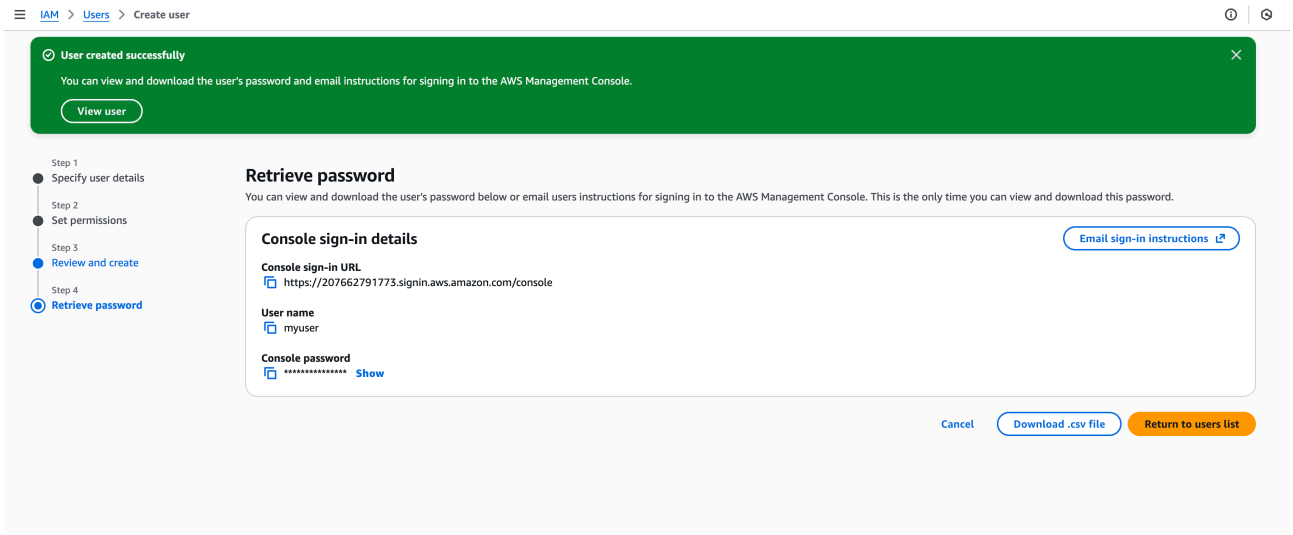
—> we have given s3 all access and ec2 all access to the user as permission



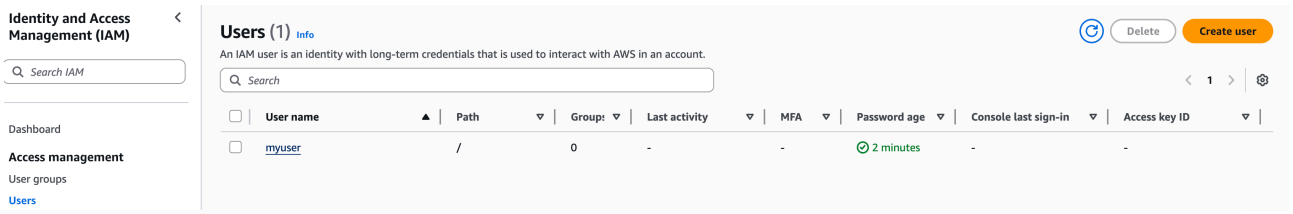
—>for consol password

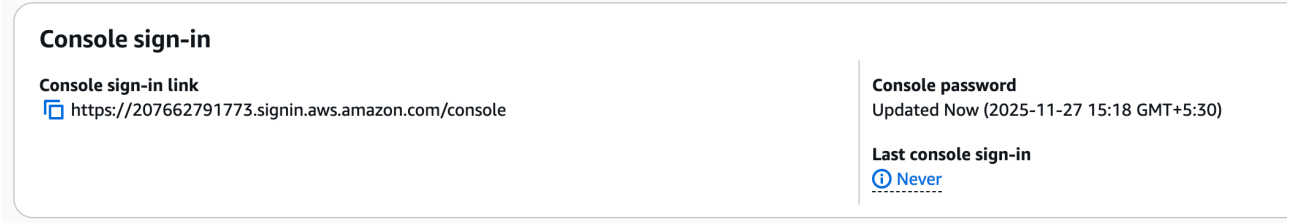


—> copy the console url and past in browser and add the details

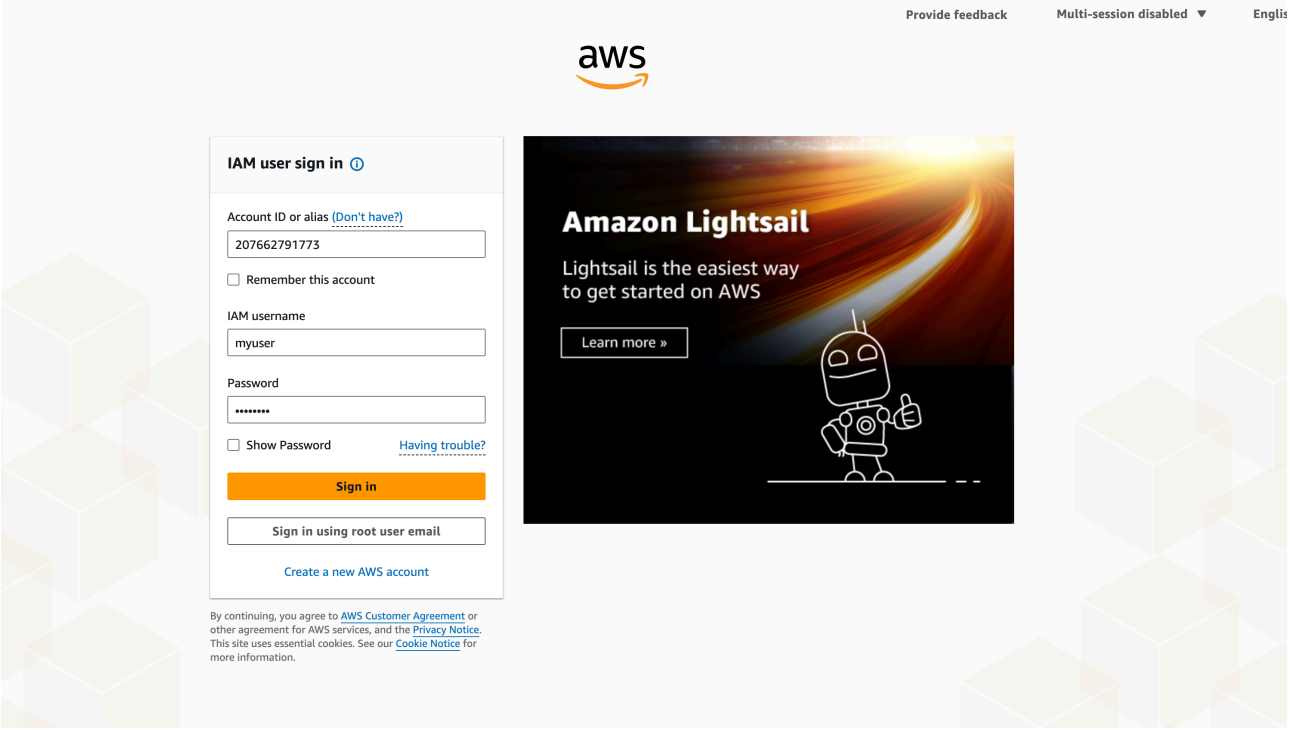


—> user created successfully

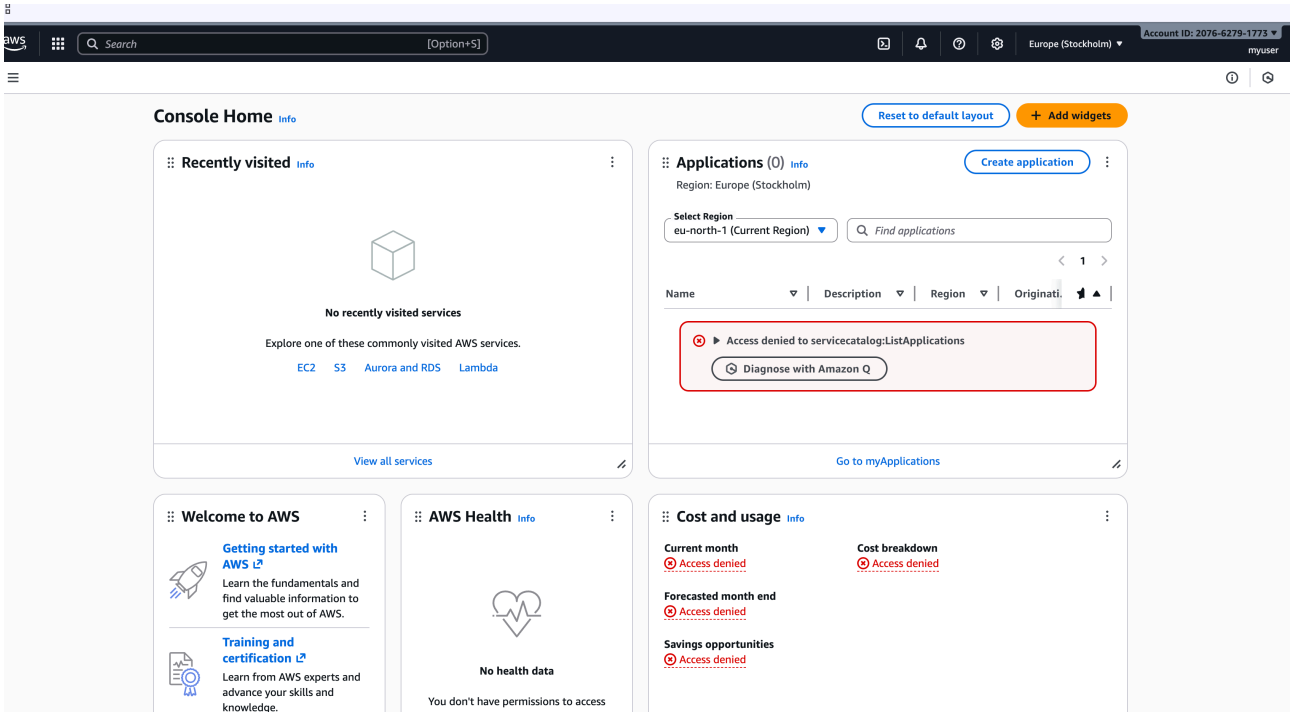




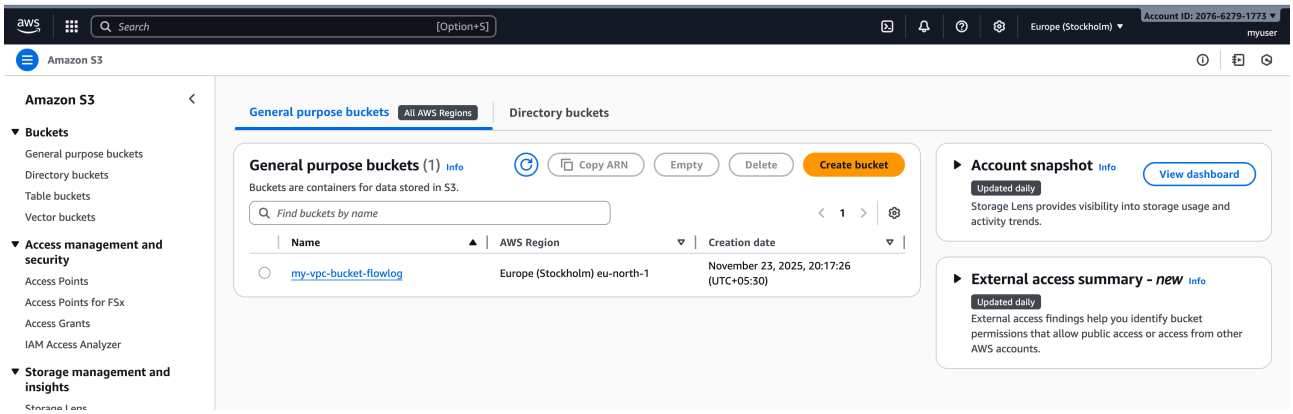
—> account number is given with url number



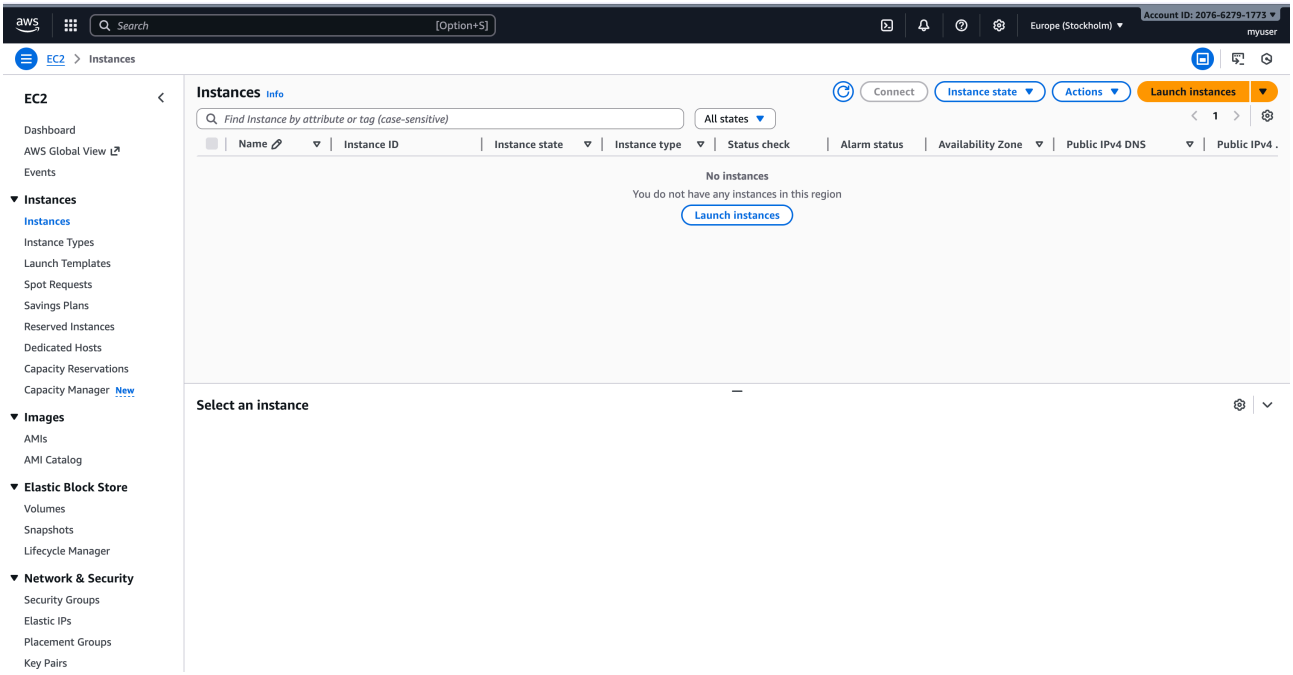
—> login to the IAM USER



—> given s3full access



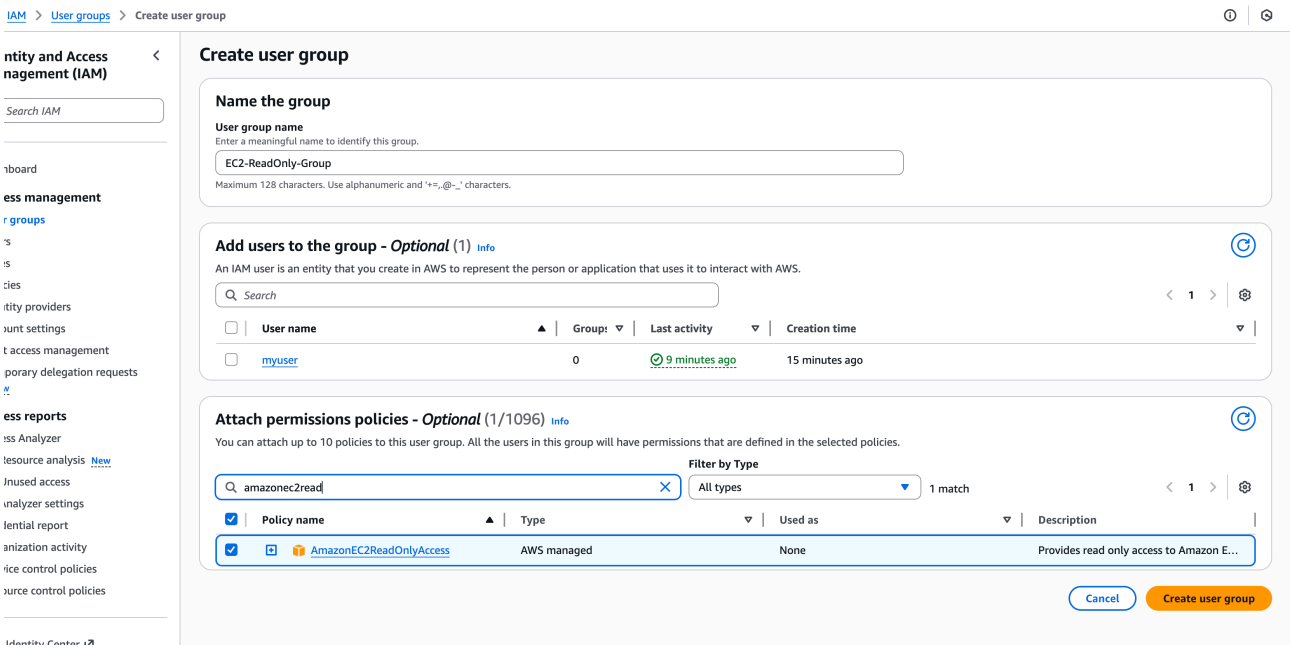
—> given ec2 full access



2)Create one group in IAM and assign read access for EC2.

Go to IAM Groups

1. Open AWS Console
2. Go to **IAM**
3. On the left menu → click **User groups**
4. Click **Create group**



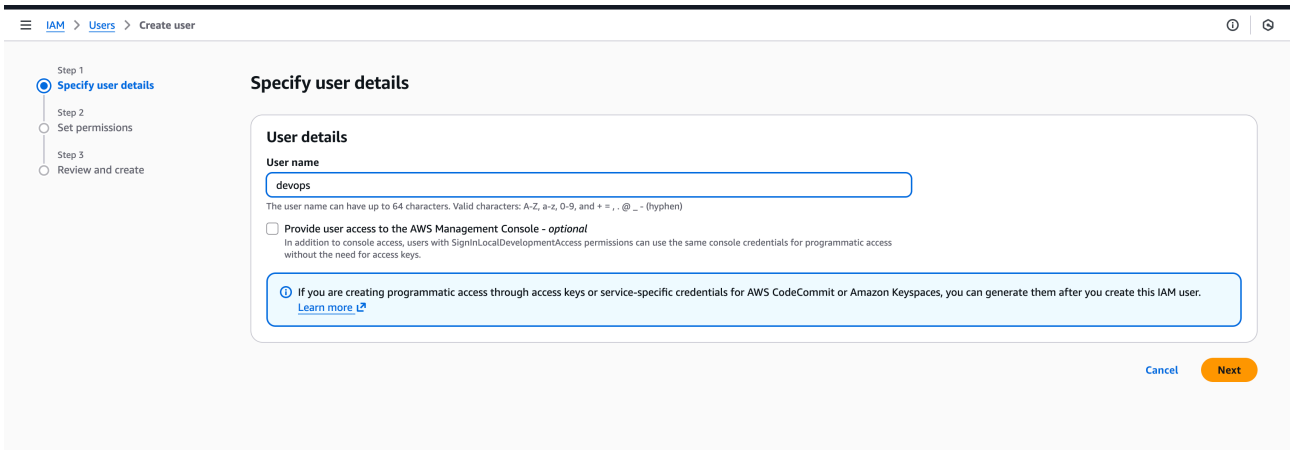
—> give the group name as EC2-readonly-group
—> attach the permission

Attach Policy

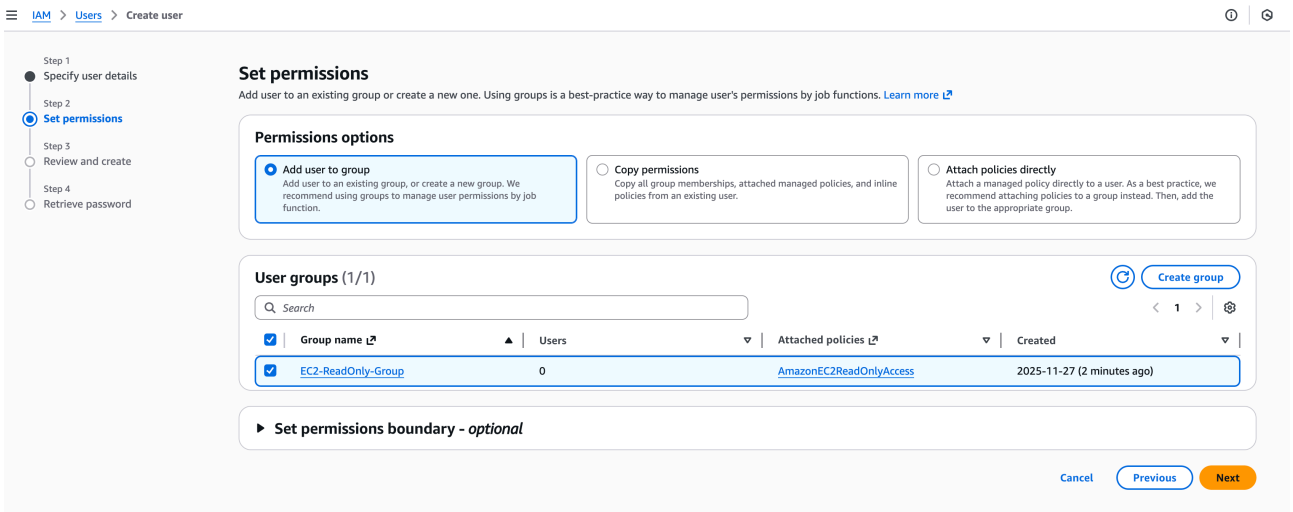
—> In the permissions list, search:

`AmazonEC2ReadOnlyAccess`
—> and then click create

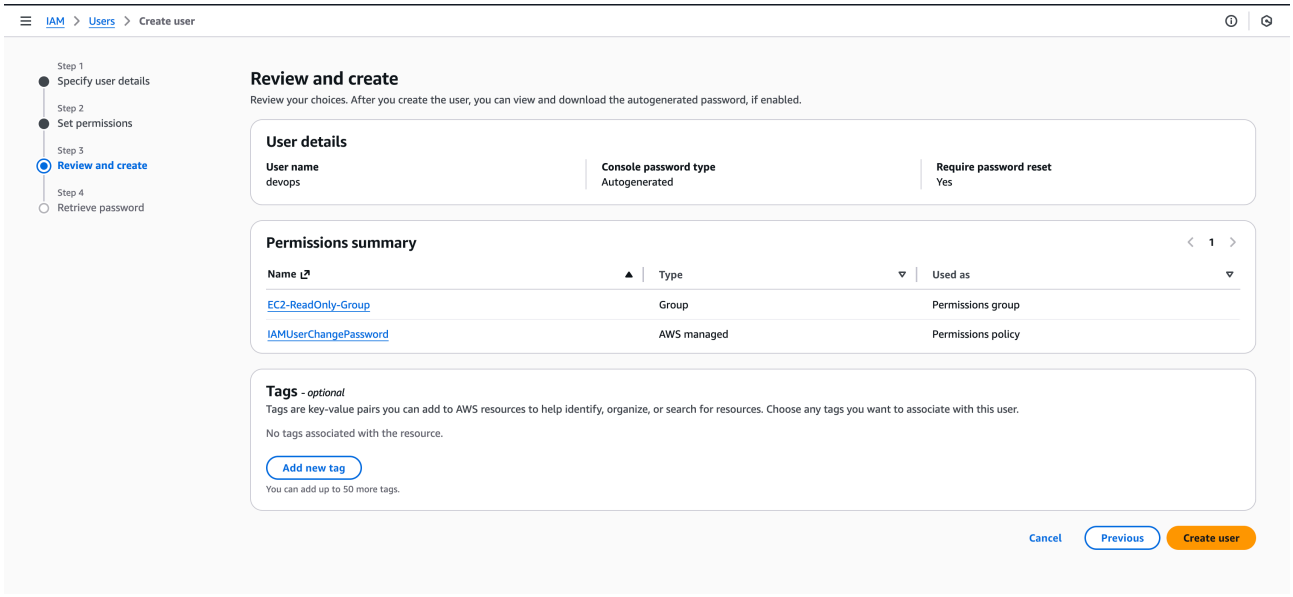
3)Create a new user named "Devops" and add to the group created in task 2.



—> give name devops while creating another user

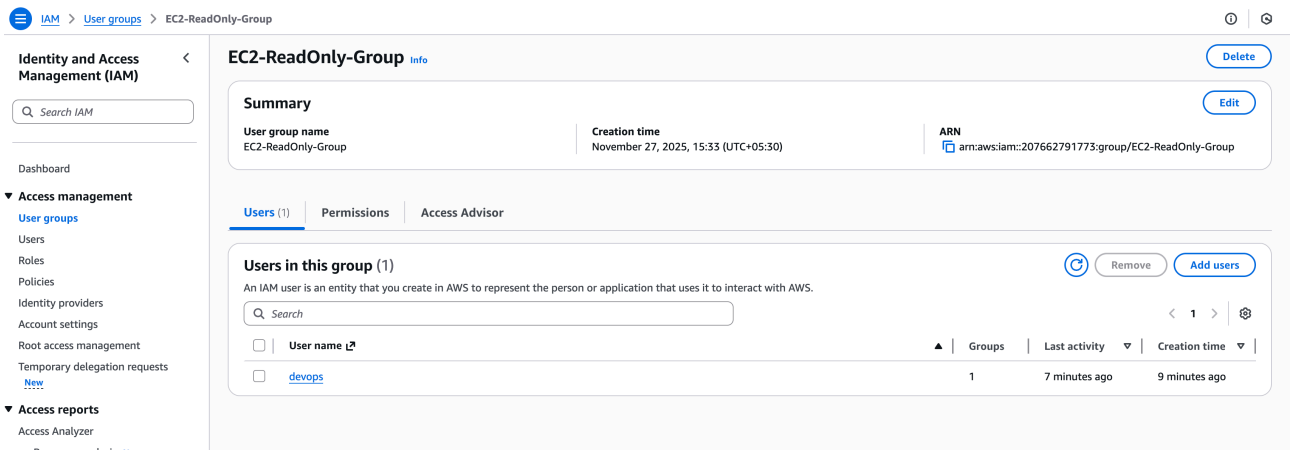


—> add user to group



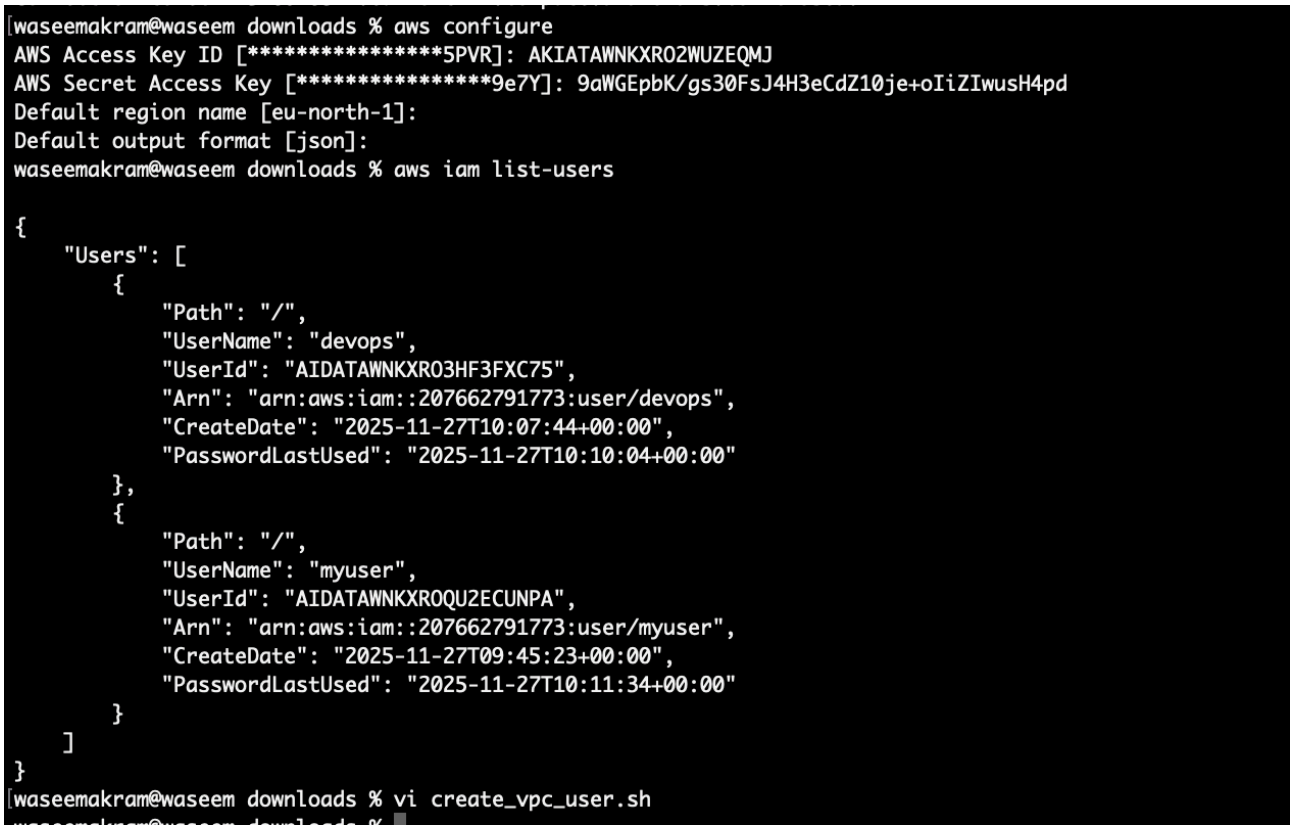
After creating the devops user go and check the user in that group Which we created in task2

—> devops named user is available in EC2-ReadOnly-Group



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

—> go to your terminal
—> aws configure (for configuring the aws account in your terminal)
—> give the details and enter
—> aws iam list-users (will lists the users in iam)
—> we have already created two iam users one myuser from task1 and devops user from task3



—> now we have to write a script for creating the iam user

—> after aws configure
—> create a file for bashscripting for creating a new iam user
—> we created a file name create_vpc_user.sh as file name
—> added script Inside it

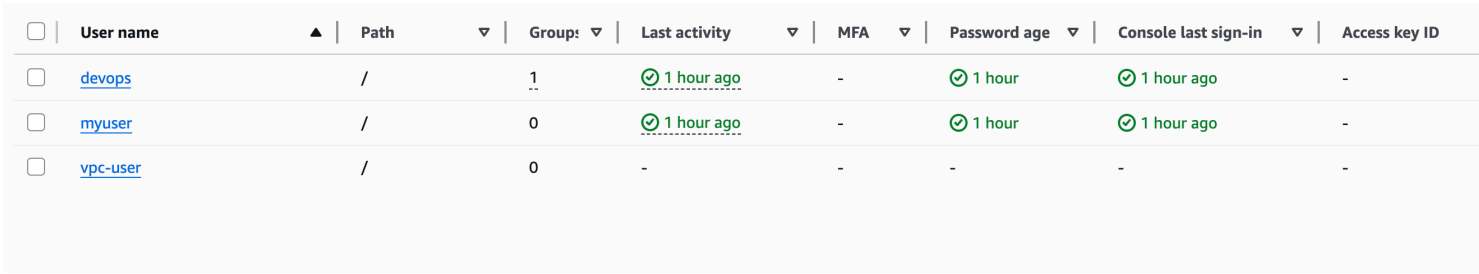
```
}
[waseemakram@waseem downloads % vi create_vpc_user.sh
[waseemakram@waseem downloads % chmod 755 create_vpc_user.sh
[waseemakram@waseem downloads % ./create_vpc_user.sh
Creating IAM user: vpc-user
{
    "User": {
        "Path": "/",
        "UserName": "vpc-user",
        "UserId": "AIDATAWNKXRO4MXHN4TXR",
        "Arn": "arn:aws:iam::207662791773:user/vpc-user",
        "CreateDate": "2025-11-27T11:41:31+00:00"
    }
}
User 'vpc-user' created and VPC Full Access policy attached.
waseemakram@waseem downloads %
```

—> this the script we used to create a iam user

```
#!/bin/bash

USERNAME="vpc-user"

echo "Creating IAM user: $USERNAME"

aws iam create-user --user-name $USERNAME

aws iam attach-user-policy \
  --user-name $USERNAME \
  --policy-arn arn:aws:iam::aws:policy/AmazonVPCFullAccess

echo "User '$USERNAME' created and VPC Full Access policy attached."
```

—> now go and check in IAM —> USERS
—> we will find the created user inside the users

—> we created vpc-user inside our terminal and we can find that user in side IAM



User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID
devops	/	1	1 hour ago	-	1 hour	1 hour ago	-
myuser	/	0	1 hour ago	-	1 hour	1 hour ago	-
vpc-user	/	0	-	-	-	-	-

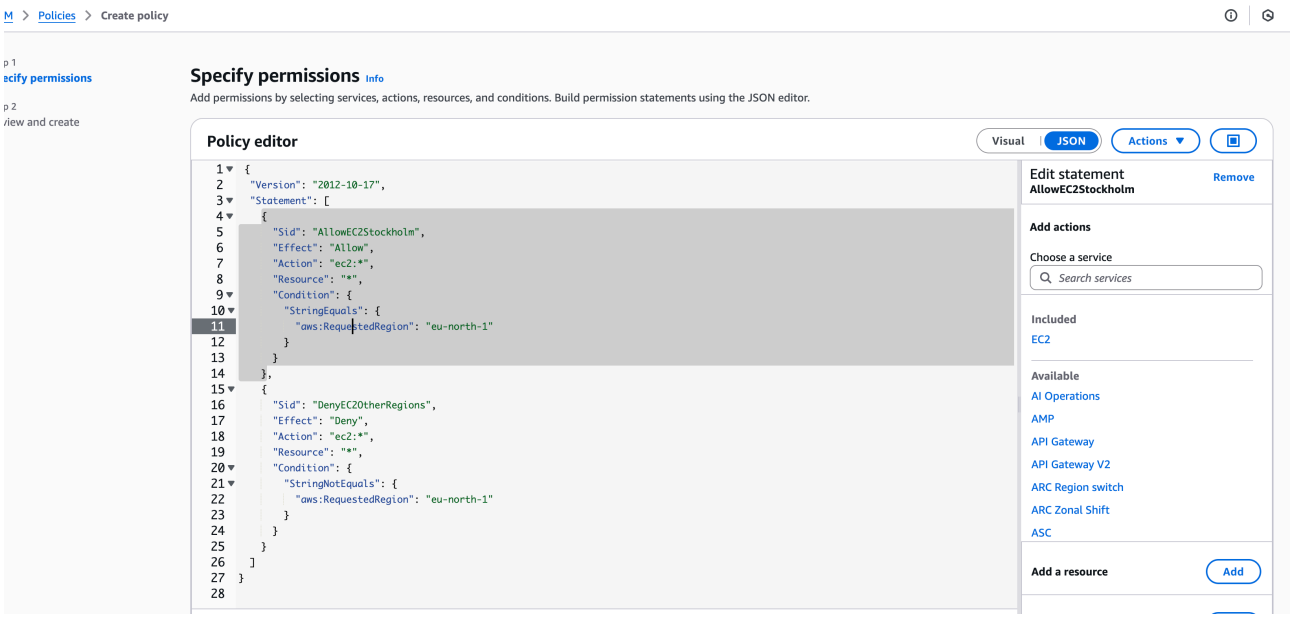
—> aws iam list-users will display all our iam users inside our aws

```
waseemakram@waseem downloads % aws iam list-users

{
    "Users": [
        {
            "Path": "/",
            "UserName": "devops",
            "UserId": "AIDATAWNKXRO3HF3FXC75",
            "Arn": "arn:aws:iam::207662791773:user/devops",
            "CreateDate": "2025-11-27T10:07:44+00:00",
            "PasswordLastUsed": "2025-11-27T10:10:04+00:00"
        },
        {
            "Path": "/",
            "UserName": "myuser",
            "UserId": "AIDATAWNKXROQU2ECUNPA",
            "Arn": "arn:aws:iam::207662791773:user/myuser",
            "CreateDate": "2025-11-27T09:45:23+00:00",
            "PasswordLastUsed": "2025-11-27T10:11:34+00:00"
        },
        {
            "Path": "/",
            "UserName": "vpc-user",
            "UserId": "AIDATAWNKXRO4MXHN4TXR",
            "Arn": "arn:aws:iam::207662791773:user/vpc-user",
            "CreateDate": "2025-11-27T11:41:31+00:00"
        }
    ]
}
waseemakram@waseem downloads %
```

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

—> to create a iam policy to a user
—> iam —>policys—>create policy

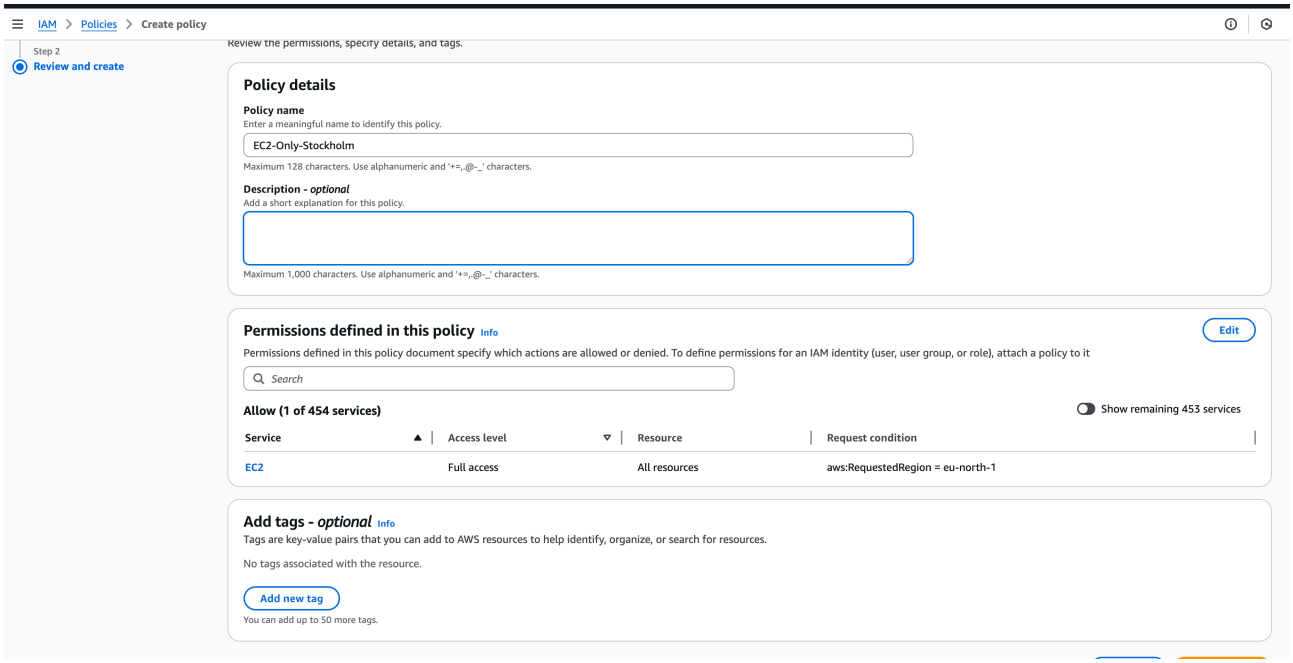
1. Go to **IAM → Policies → Create policy**
2. Select **JSON —->give the policy to allow ec2 access for user in**
3. Click **Next → Create policy**



This policy will:

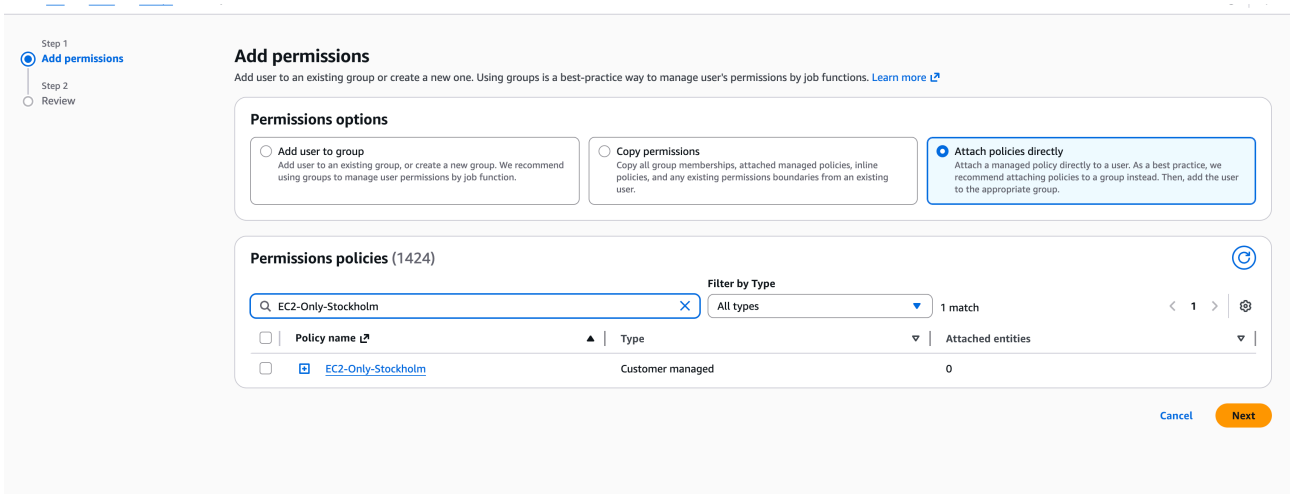
- **Allow** EC2 full access in **Stockholm (eu-north-1)**
- **Deny** EC2 access in **every other region**
- Apply to **a specific IAM user**

—> next we have to give the policy name which we are creating



—> Attach this policy to specific user

—> iam —> users —>devops



—>Go to **IAM → Users**

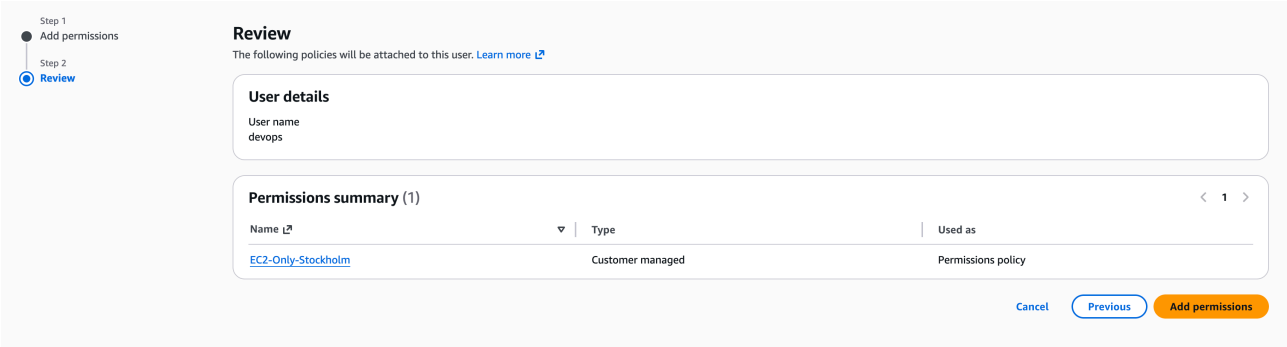
—>Click the user you want (example:we are having user `devops`)

—>Click **Add permissions**

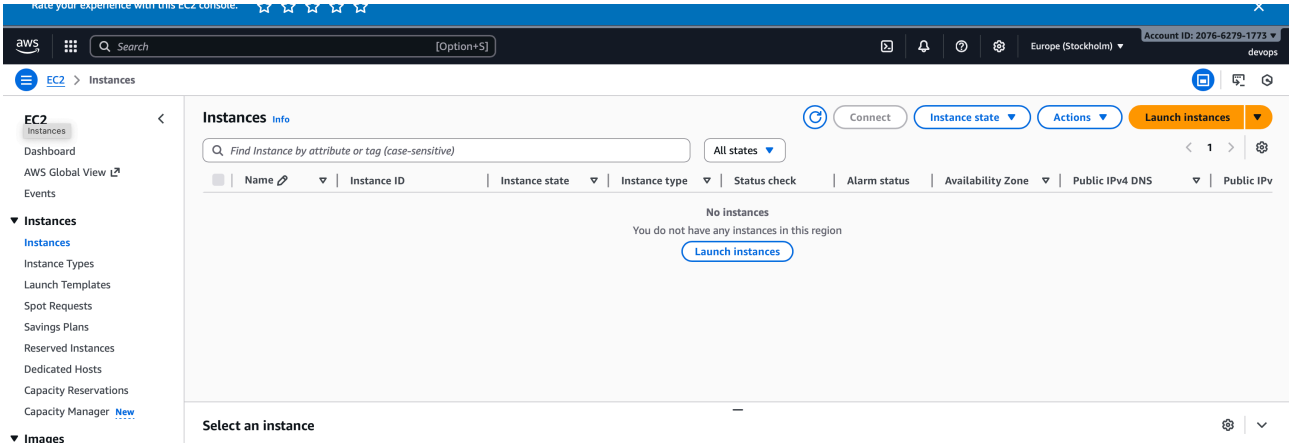
—>Choose **Attach policies directly**

—>Select the policy you created

—>Click **Add permissions**

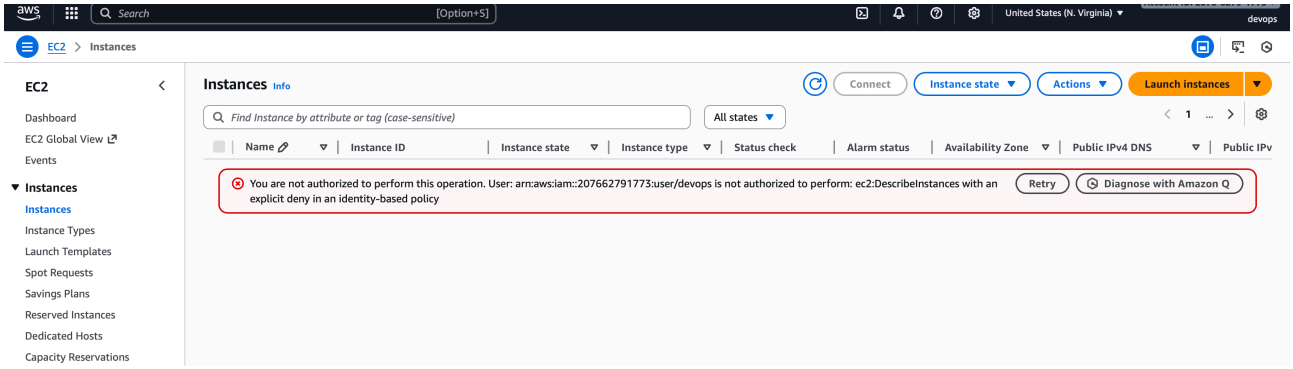


—>verification
—> as we have given only eu-north-1 (stockholm)



—> we are able to have access to that region

—>as I changed to other regions like Virginia we are getting access denied



They will get **AccessDenied**.

6)We have two accounts: Account A and Account B. Account A user should access an S3 bucket in Account B.

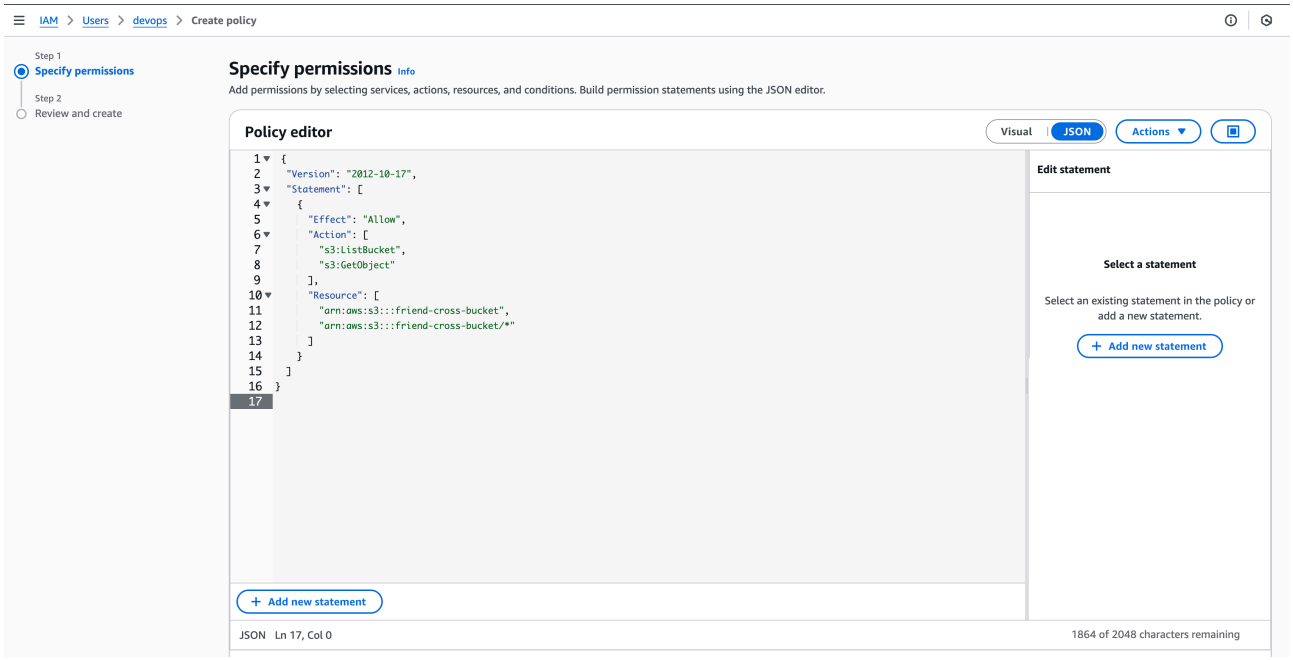
—> so I have accessed the bucket of my friend

—> so the account A is me and my friend is account B

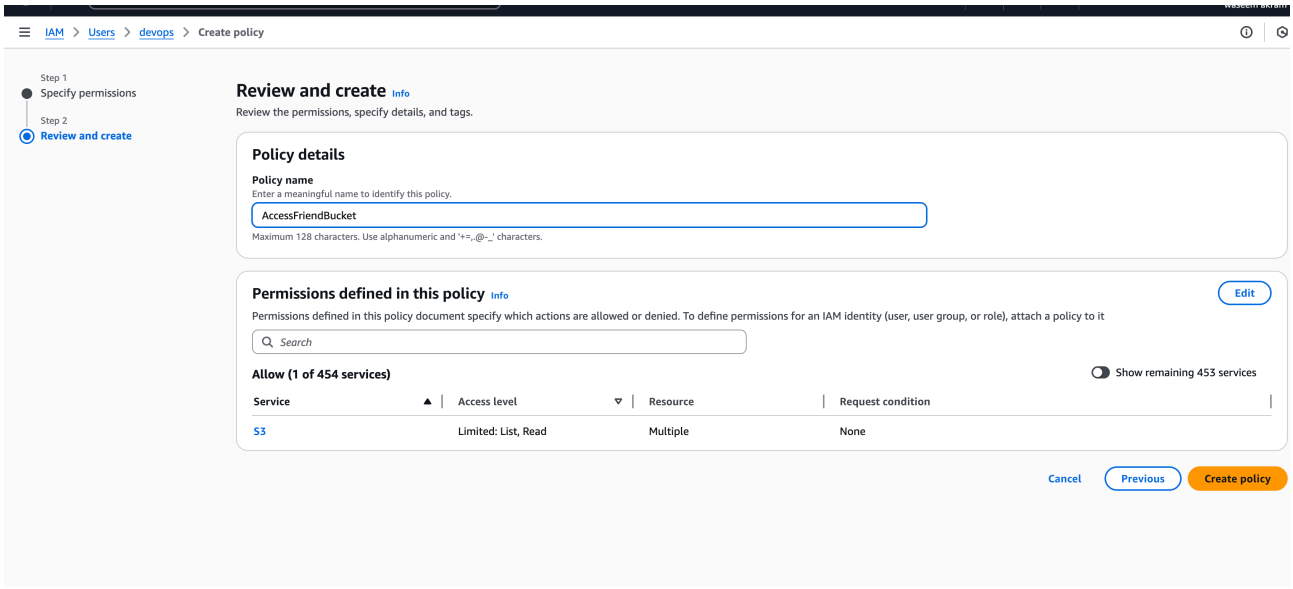
So from his side he has created a bucket policy for me to have access To his bucket

—> so the bucket name is friend-cross-bucket
We have attached the bucket and added my aws account id with user to send there access
—> so after creating the bucket policy I have to go to the IAM

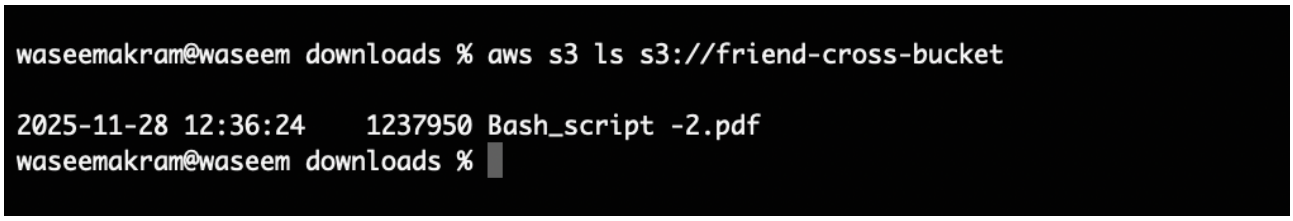
—>users —> devops—>create policy and add the policy of bucket of friend



—> we have added the bucket name and allow the access of that bucket



And for configuring we have to go to terminal were our aws access is there



—> aws s3 ls://friend-cross-bucket as we can see we are able to have access of my friend bucket which he has