**IAM - Identity and access management.**

**(It is a one type of webservice that helps you securely control access to aws resources).**

**Two types: 1) Identity-based policy.**

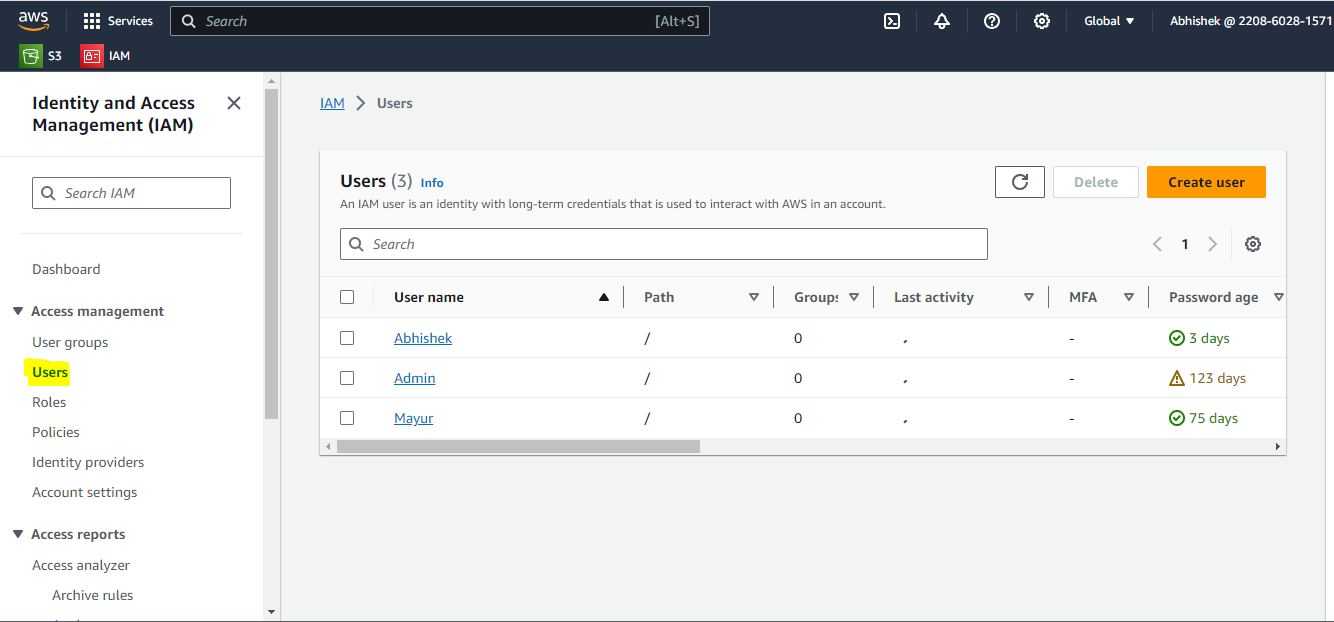
**2) Password-based authentication**

Step 1:

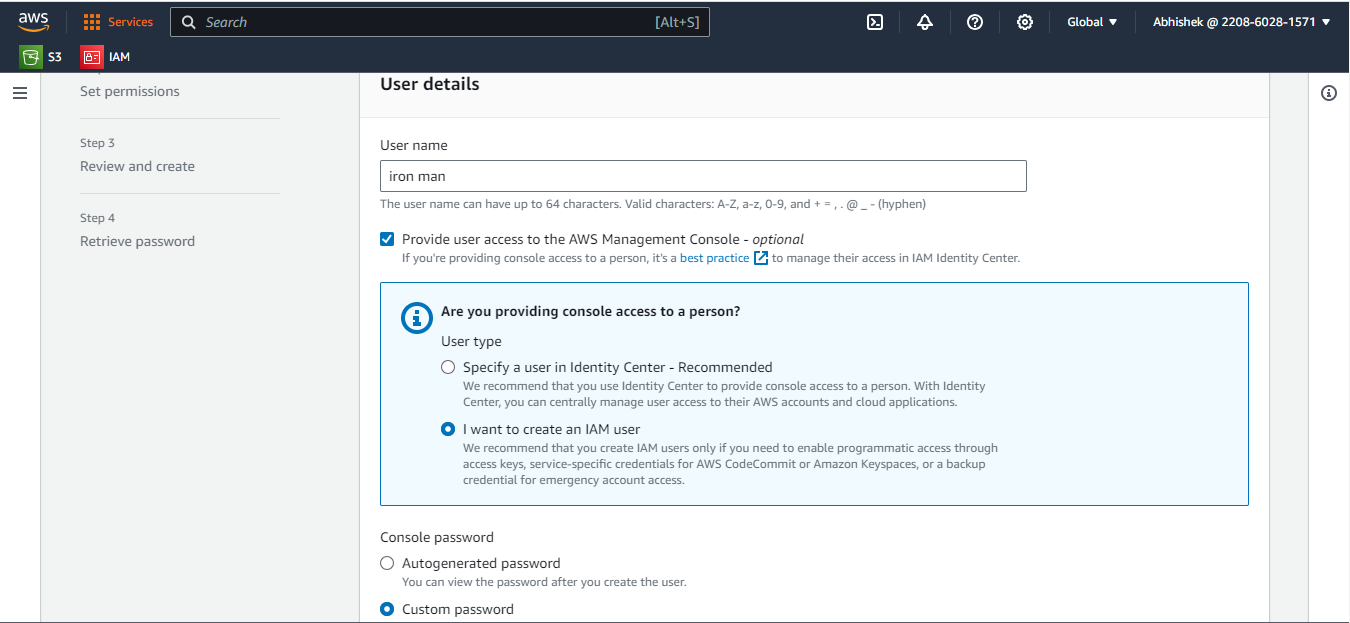
Open aws console → Search IAM service

Step 2: for user add.

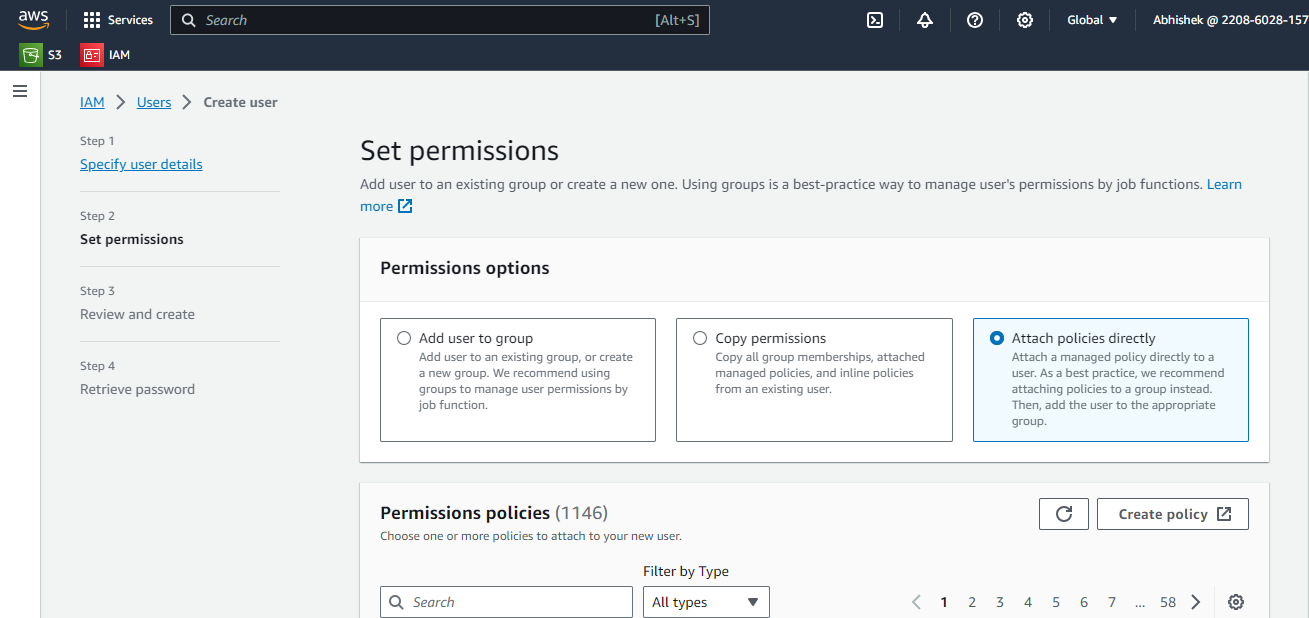
Users → create user



Step 3: Fills user details.

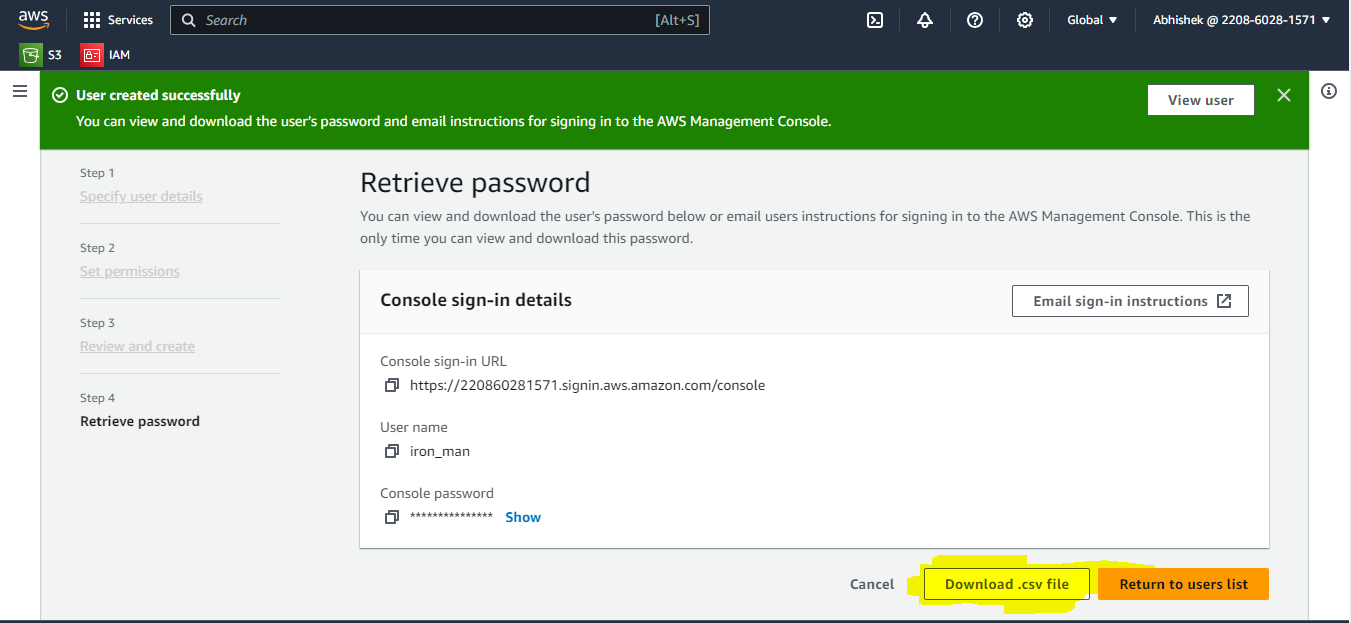


Step 4: You can give permission for user like (s3 read)



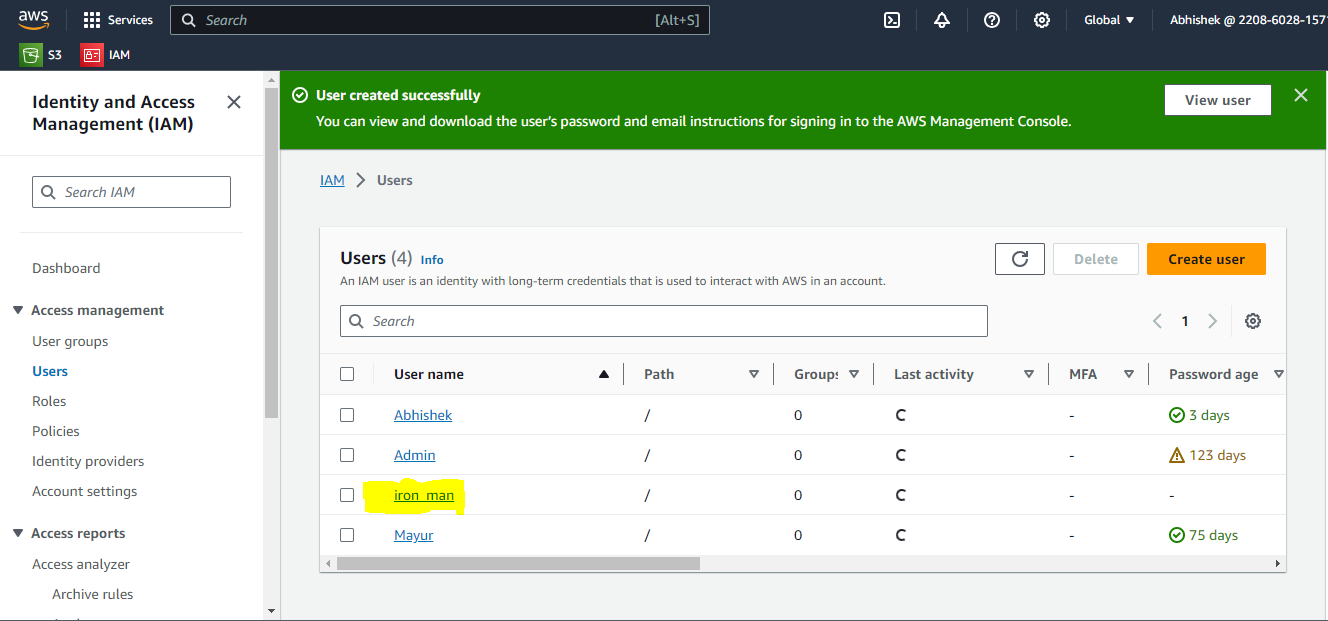
Step 4 :

User created successfully.



Step 5 : To check user created or not.

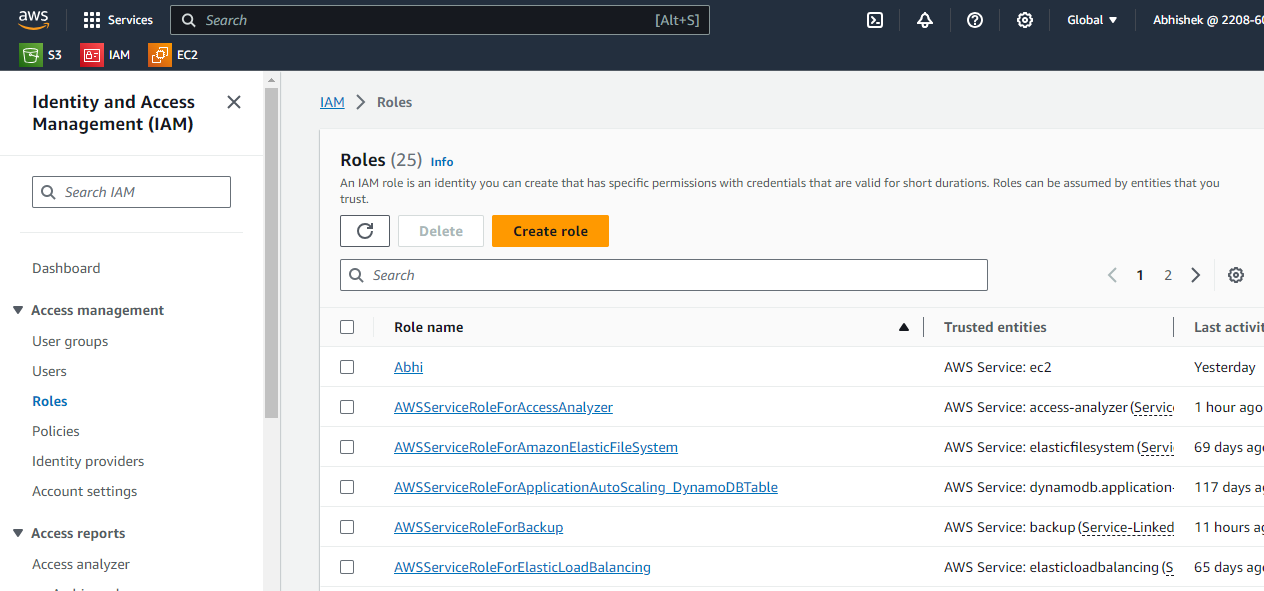
IAM → Users → you will list of users.



**B. To create a role**

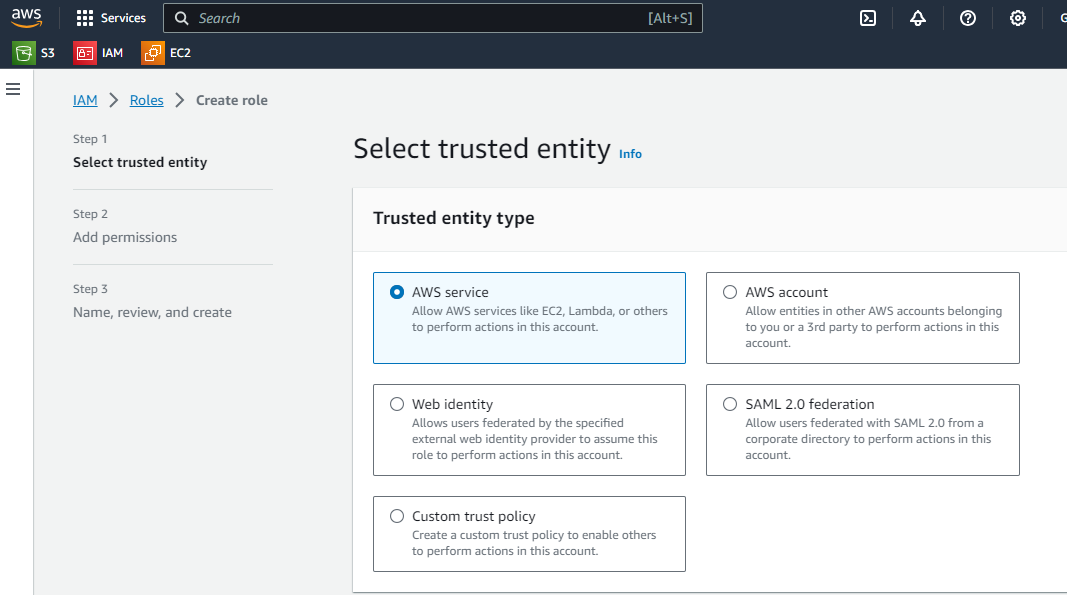
Step 1:

IAM → select role(left side) →click on create a role.

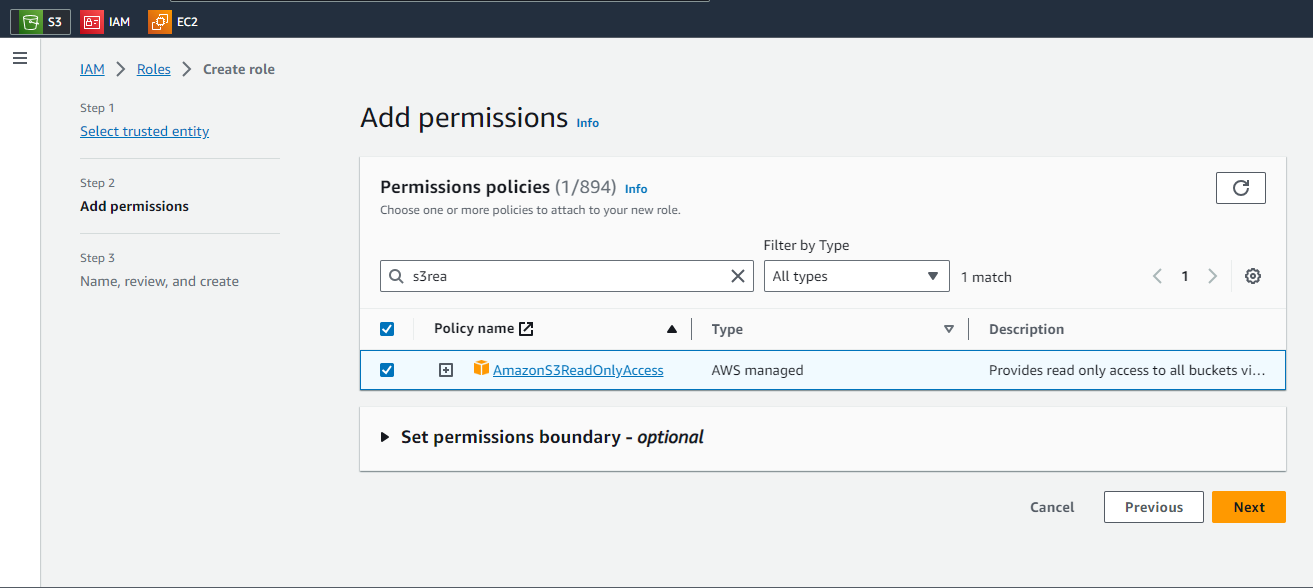


Step 2:

Roles → create a role → select trusted entity type(Aws) → select use case(service name)

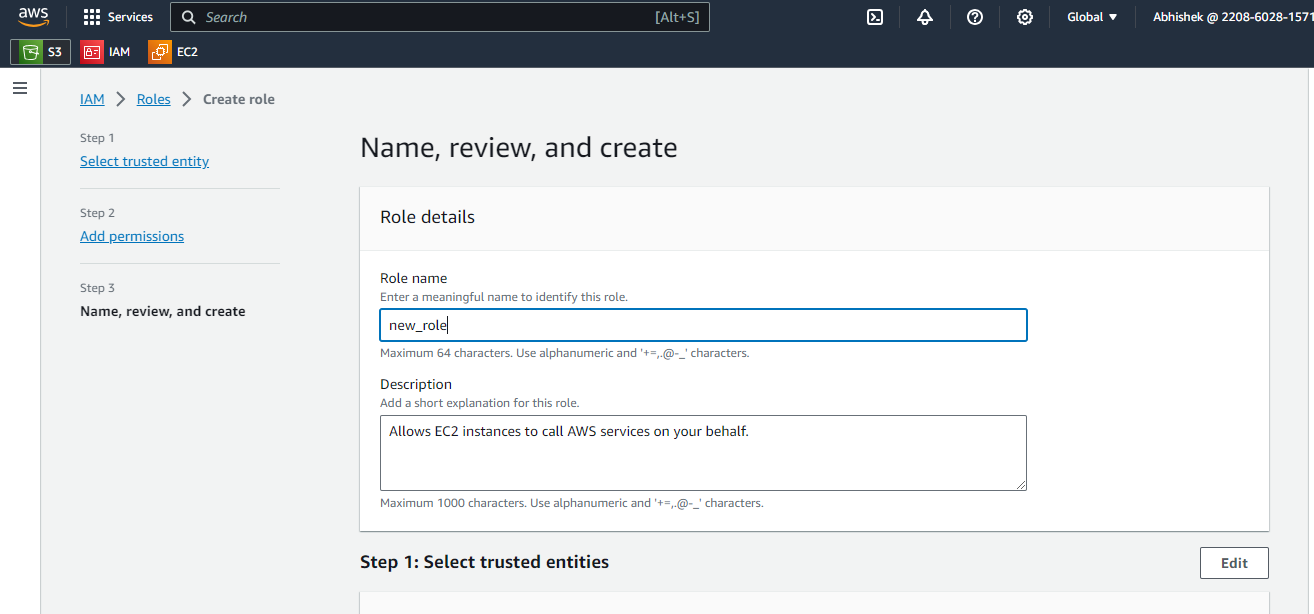


Step 3: set permission(like s3 read only)



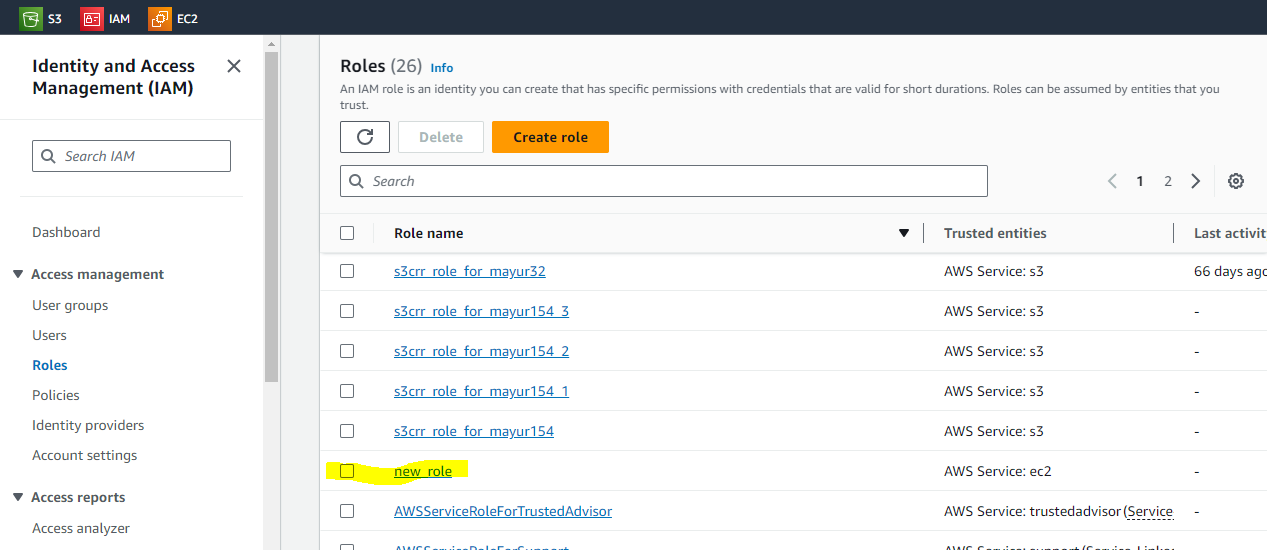
Step 4:

Give role name and save.



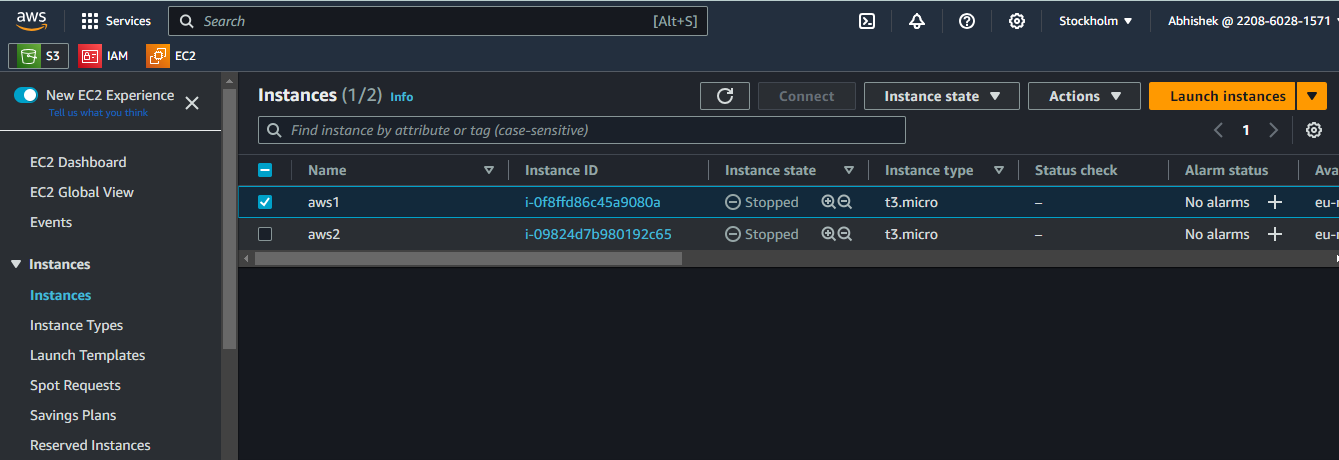
Step 5:

New role is created.



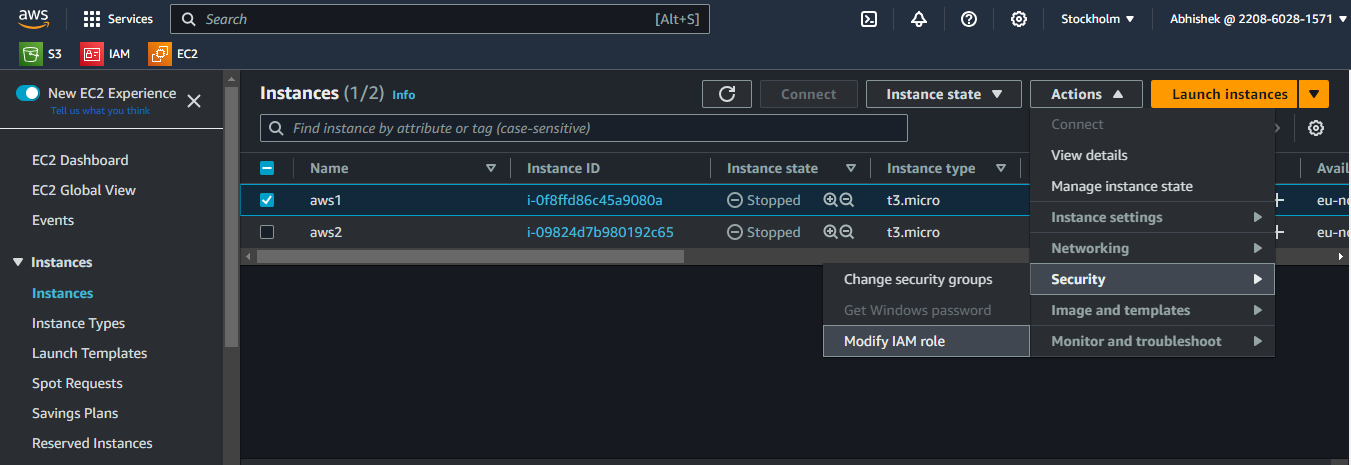
Step 6: Now we can attach this role to services.

Open EC2 → create one instance → select that instance



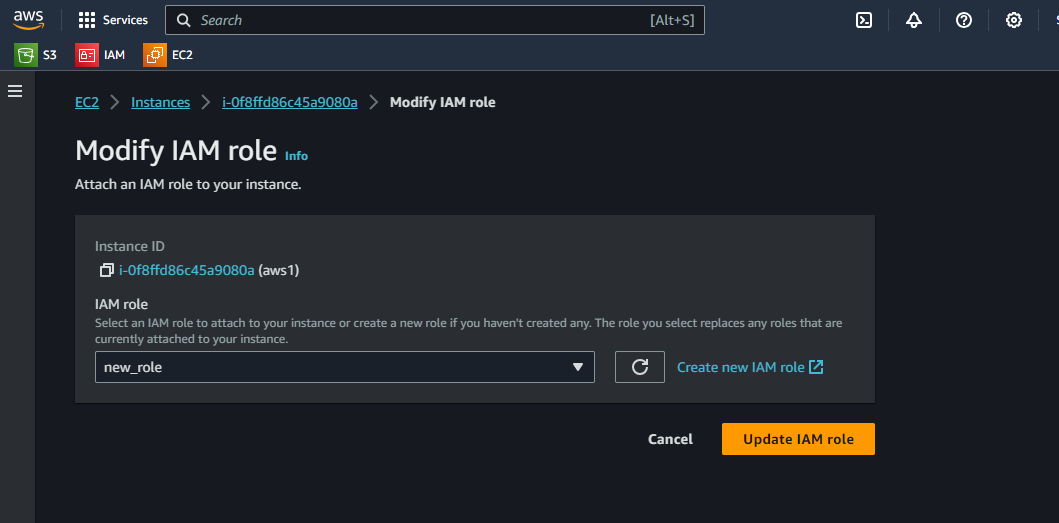
Step 7 : for attaching that role.

Select instance → click on action →security → modify IAM role.



Step 8:

Select IAM role → update IAM role.

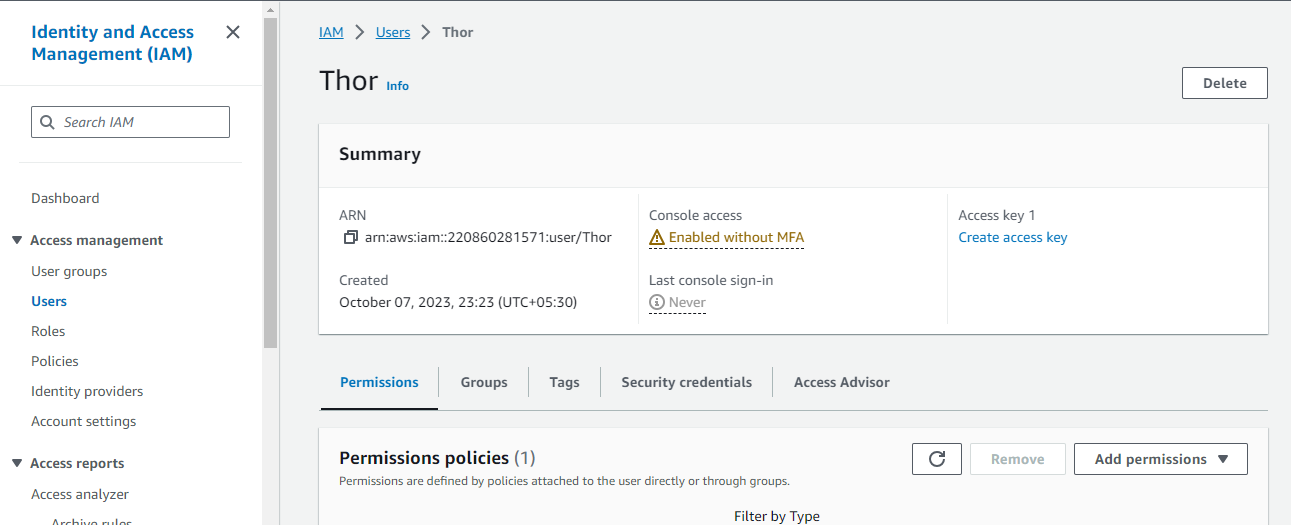


**B) Programmatic access control(Access key)**

Task: create one user, and with the help of programmatic access control allow user to access s3 bucket in windows command prompt.

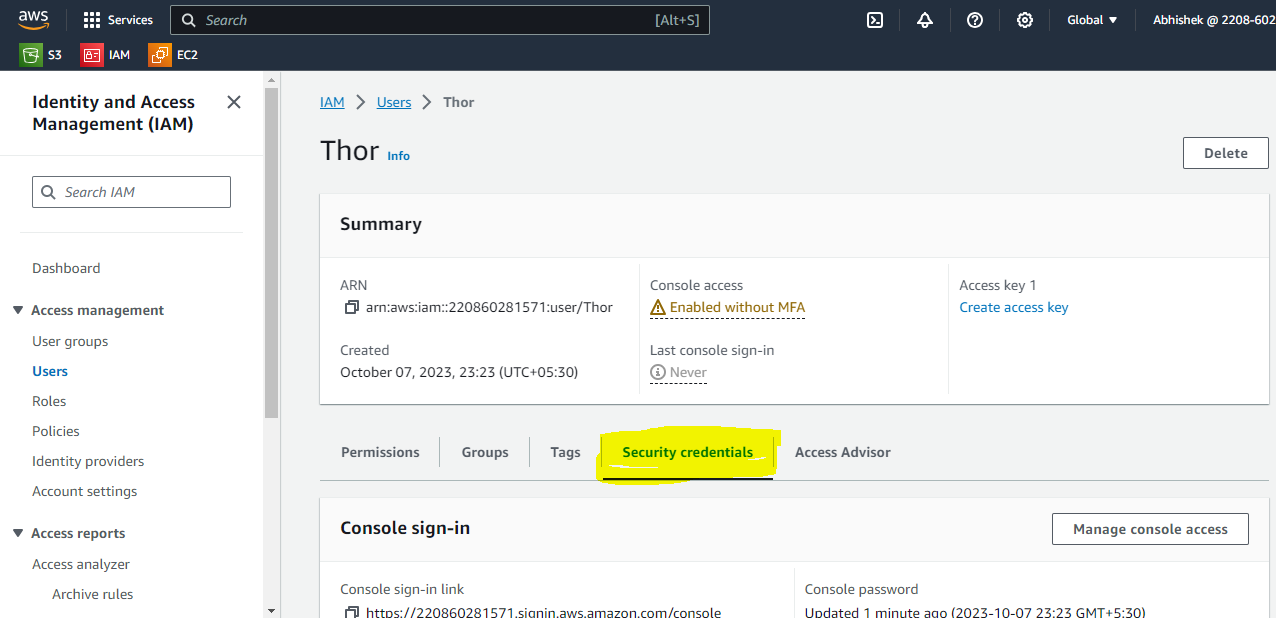
Step 1: create user

IAM → users → create user → Thor → set permissions as usual



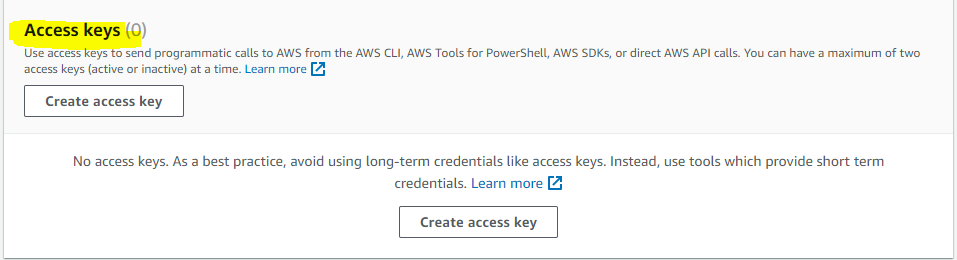
Step 2: Then go to security credentials.

IAM → users → Thor → select security credentials(Below to user details)



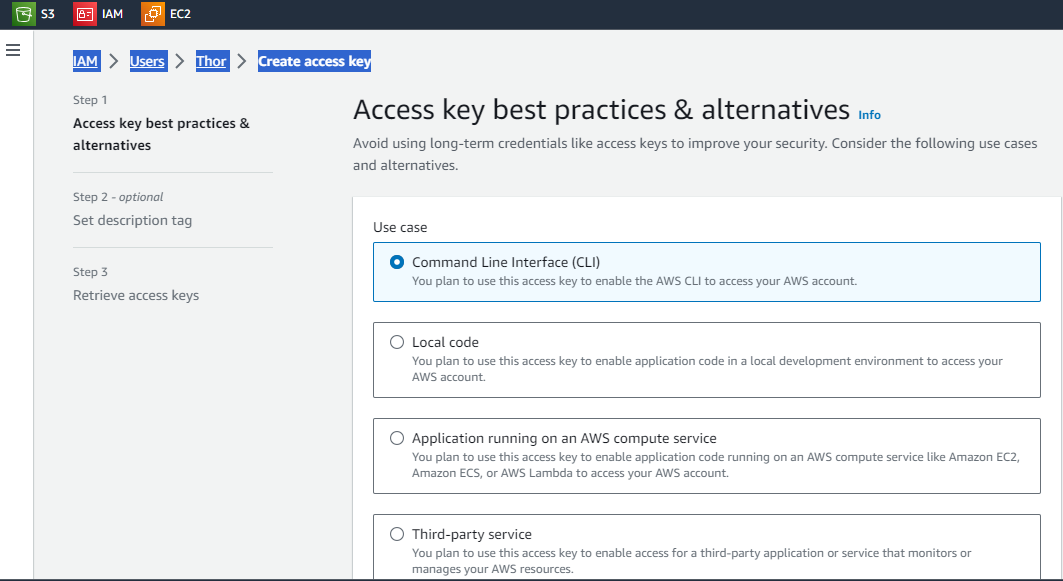
Step 3:

In Security credential → select create access key →

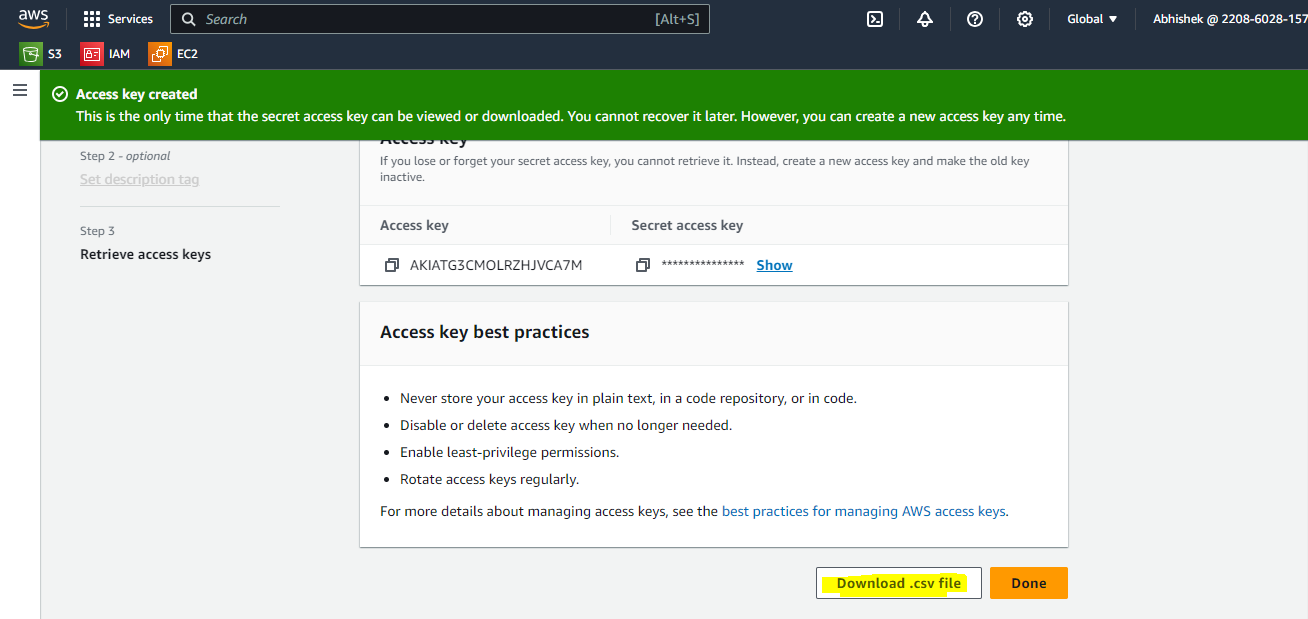


Step 4:

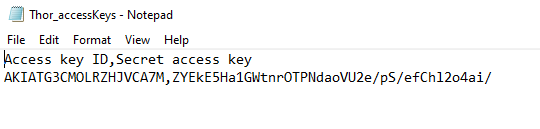
[IAM](https://us-east-1.console.aws.amazon.com/iamv2/home?region=eu-north-1#/home) → [Users](https://us-east-1.console.aws.amazon.com/iamv2/home?region=eu-north-1#/users) → [Thor](https://us-east-1.console.aws.amazon.com/iamv2/home?region=eu-north-1#/users/details/Thor) → Create access key → CLI



Step 5 : key is created now download .csv file in your system and save it.



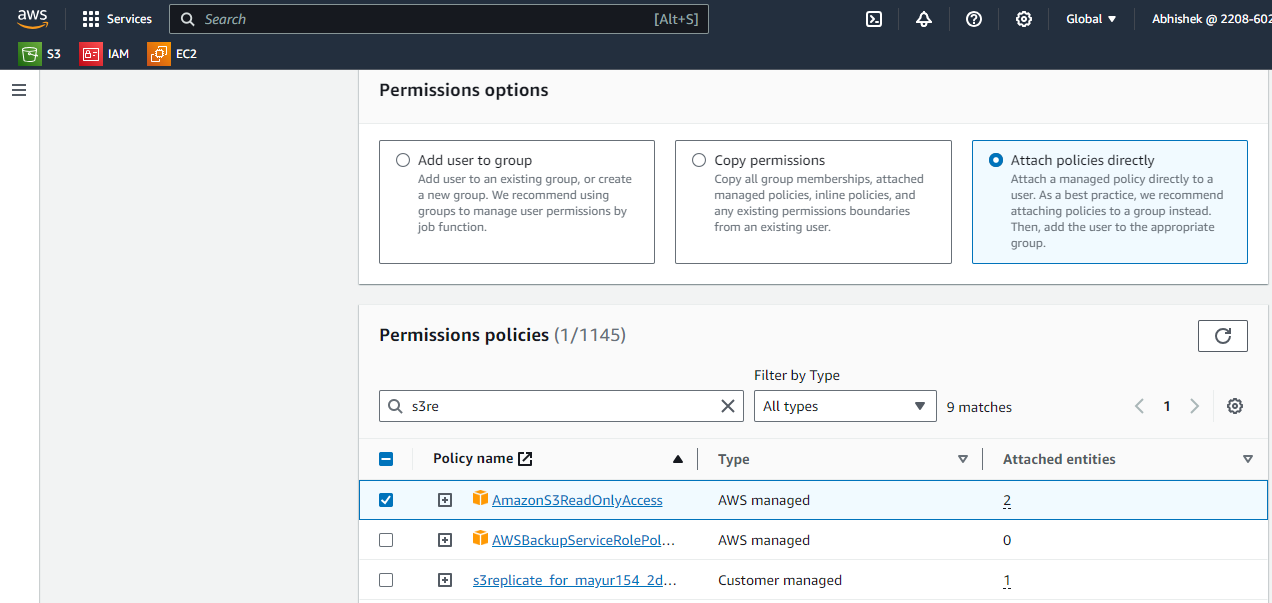
Step 6 : secret and access key is downloaded in your system.



Step 7 :

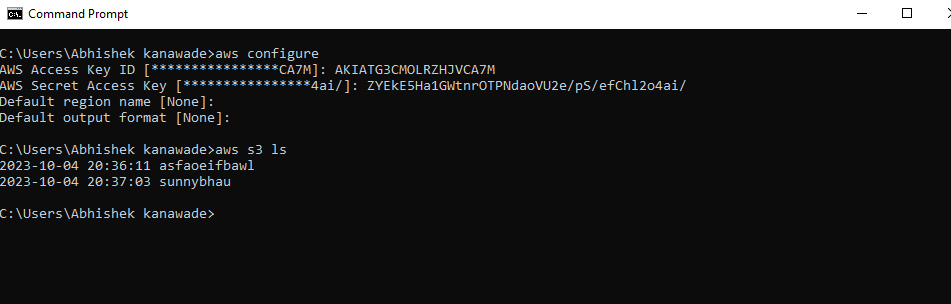
Also we need to add permissions for user to access s3 bucket.

IAM → user →Thor → permission → Add permission → attach policies directly → search s3read only access → add permission.



Step 8:

Now open cmd in your windows machine → download aws cli for windows from google(link to download aws cli - [**https://awscli.amazonaws.com/AWSCLIV2.msi**](https://awscli.amazonaws.com/AWSCLIV2.msi)) → after downloading open cmd in windows → type aws configure → It will ask access key, open notepad file(we have downloaded .csv file use access key from there) → after entering key access key it will ask secret key(Gain use downloaded .csv file) → Default region name(none) → Default output format (None) → now user can access services.



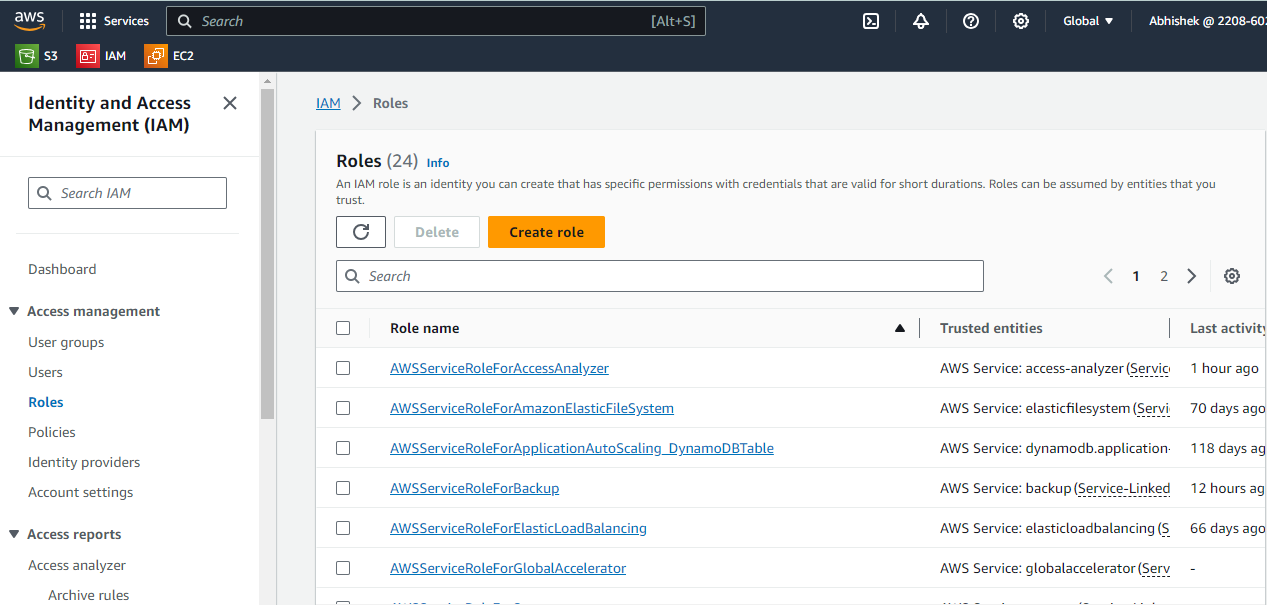
You can see bucket now.

**C) Role**

Task : create one role, give s3 read only access to EC2 service and attach that role to instance. (Actually the role is attached to resources or services and policies are attached to users.)

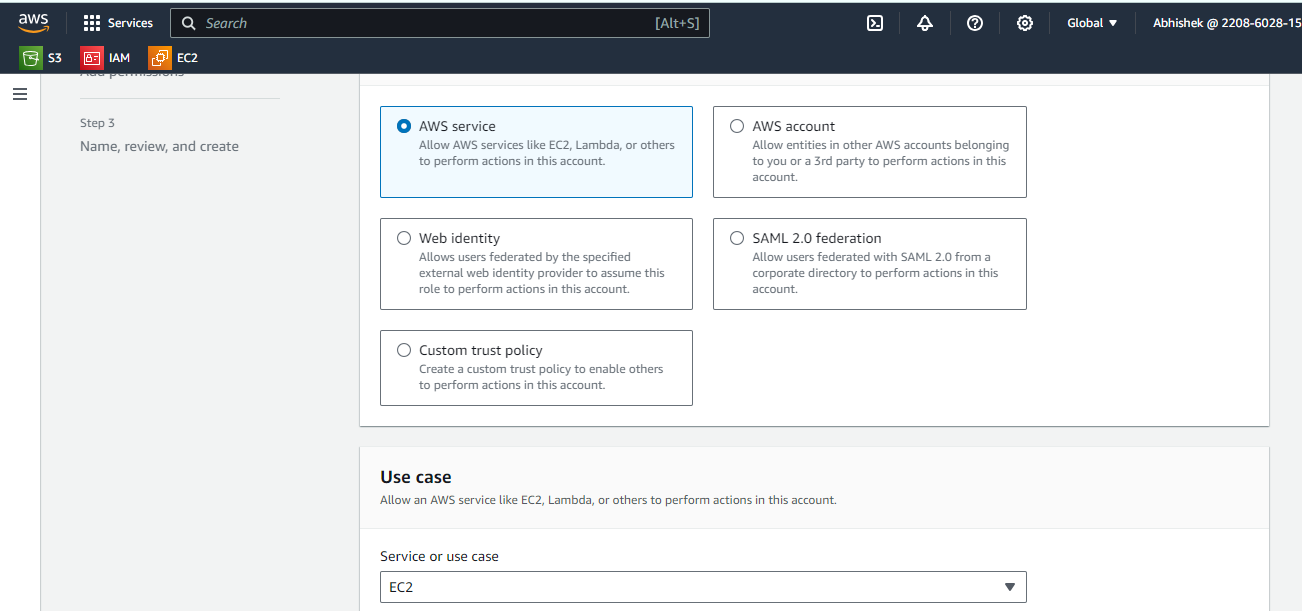
Step 1: For creating role.

IAM → roles → create role →



Step 2:

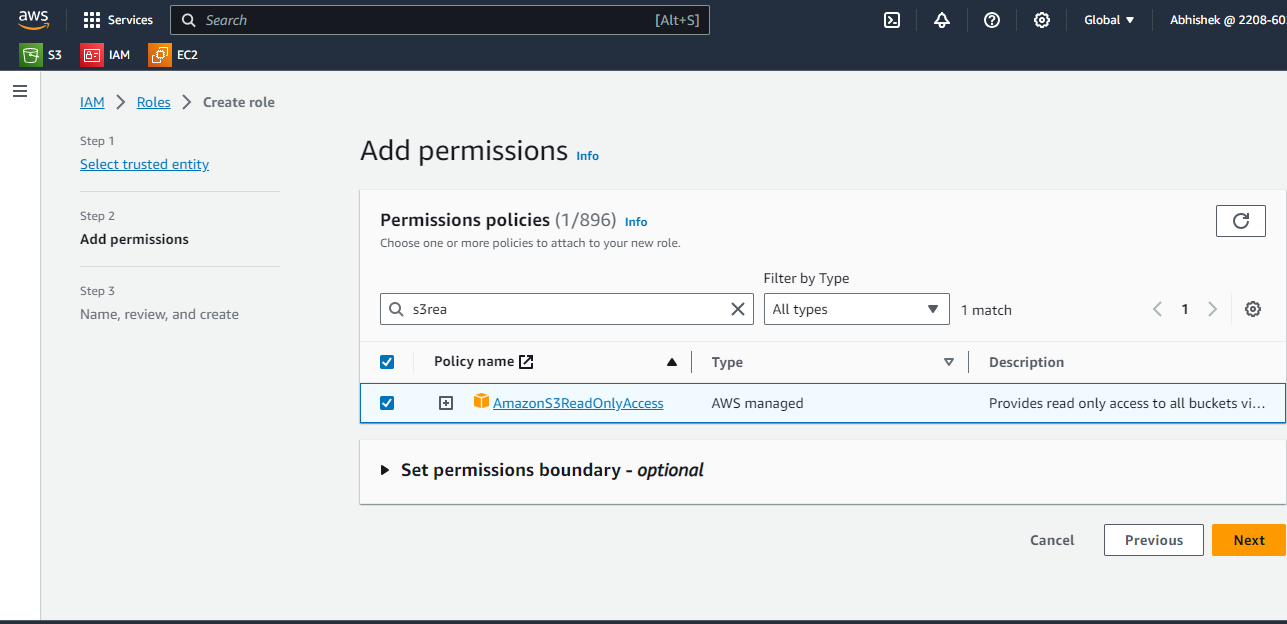
Roles → create role → select aws service → select use case(EC2 –we are applying on EC2)



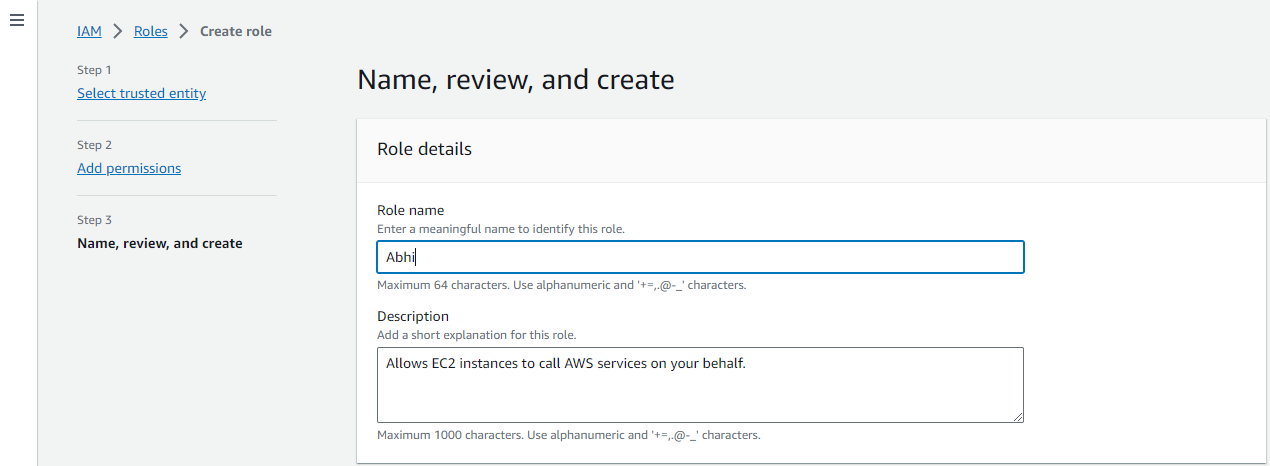
Step 3:

add permissions

Then add permission which permission you have give to service.



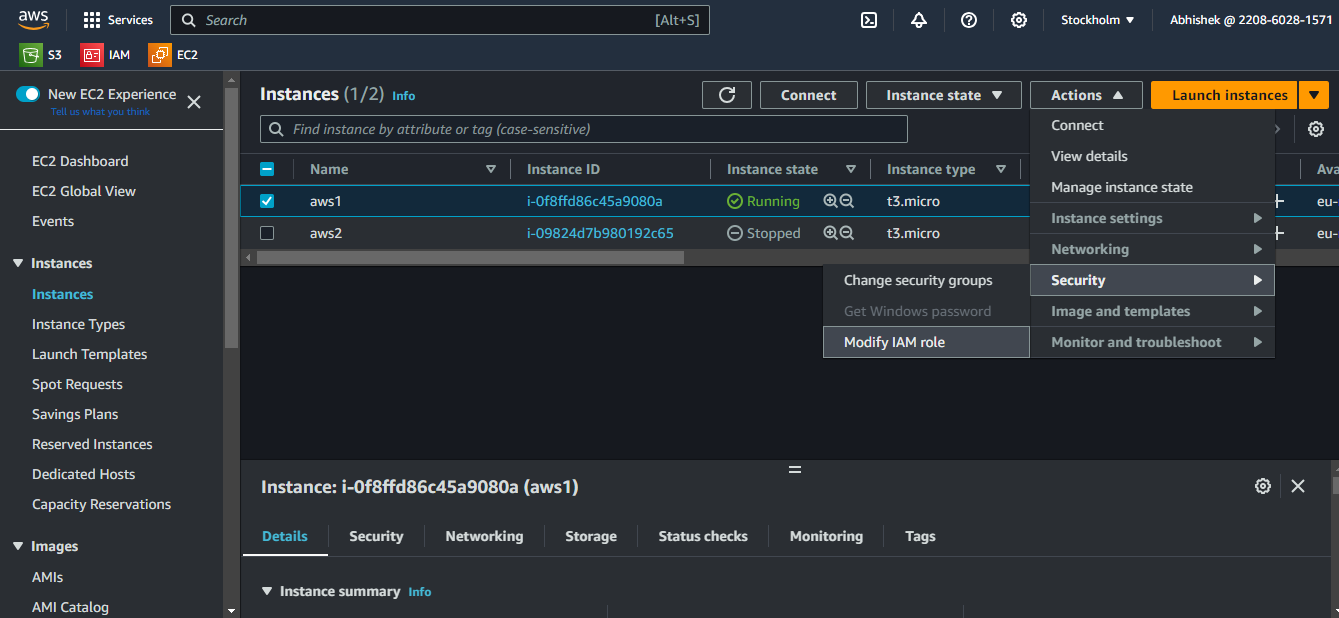
Step 4: give role name.



Step 5:

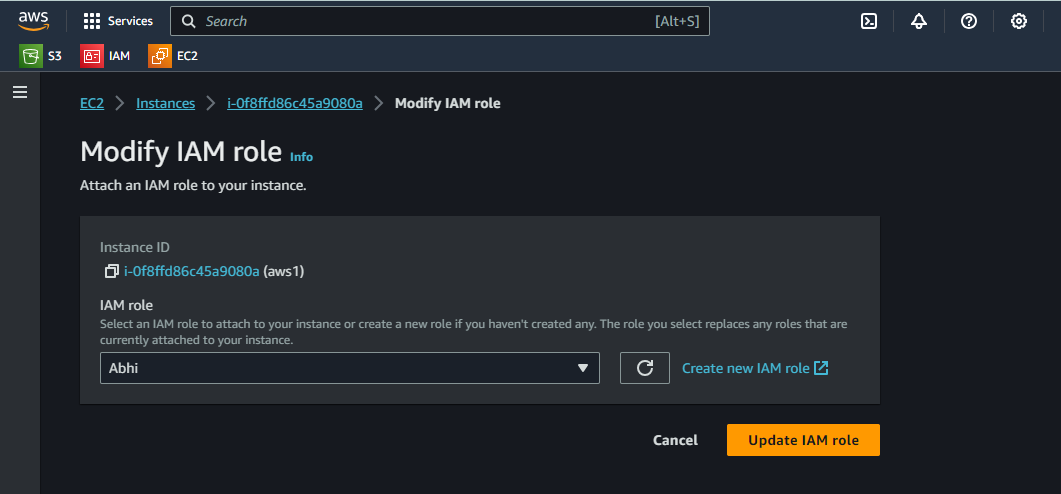
Attach role to instance.

EC2 → Instance → select instance → Action → security → Modify IAM role



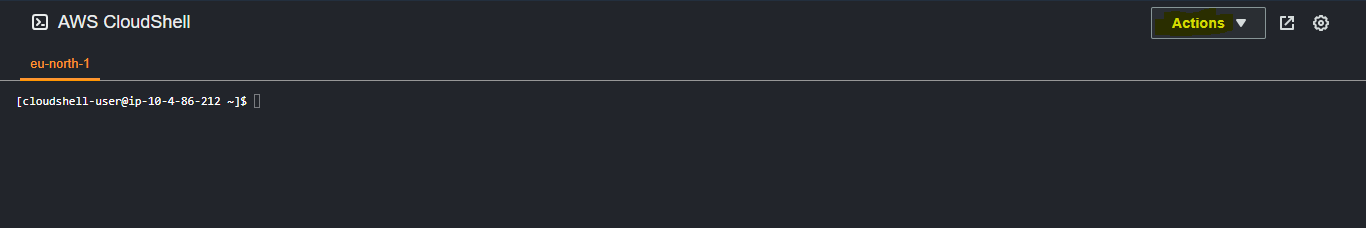
Step 6 :

attach created role.



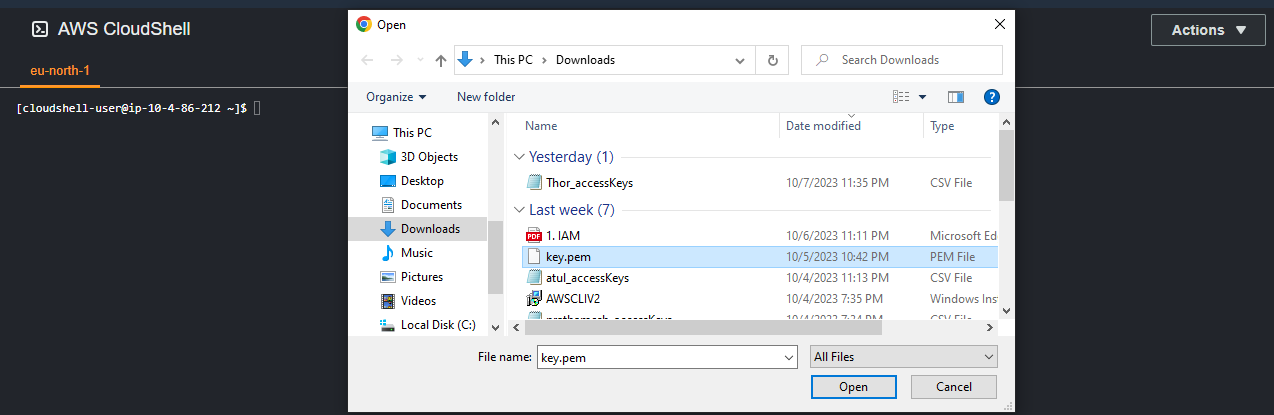
Step 6:

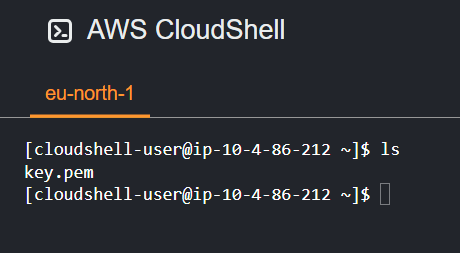
Now open cloudshell terminal → and we have one key file(while creating instance we have created one key for using ssh service) → upload that key in cloudshell console → go to action → upload file → select location where you save key→ upload



Step 7:

Action → upload file → select file

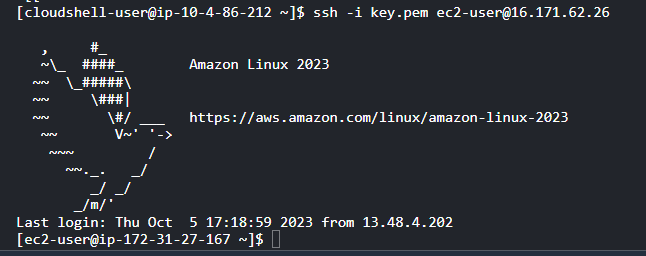




Step 8:

Take a access of created server. You will required instance public ip

ssh -i <key\_name> <macine\_name>@ipaddress



Step 9:

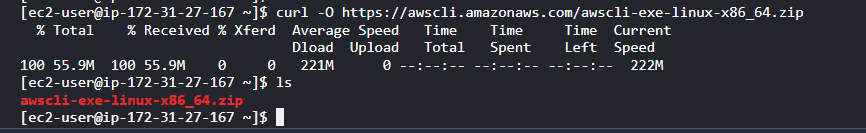
You need to download aws cli

Aws cli for linux download(search on google) → **curl -O**

[**https://awscli.amazonaws.com/awscli-exe-linux-x86\_64.zip**](https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip)

Step 10:

We have downloaded aws cli on the machine. Now we need to unzip this file, for that we need zip package install in a system.



Step 11:

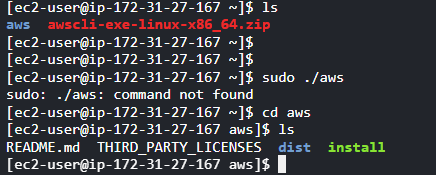
#sudo yum install zip -y

#unzip awsclii-exe



Now file is unzip.

Step 12:



Inside aws there is install script file we need to run that.

#sudo ./install

#aws s3 ls —---> you can check now you are able to see list of bucket or not.

