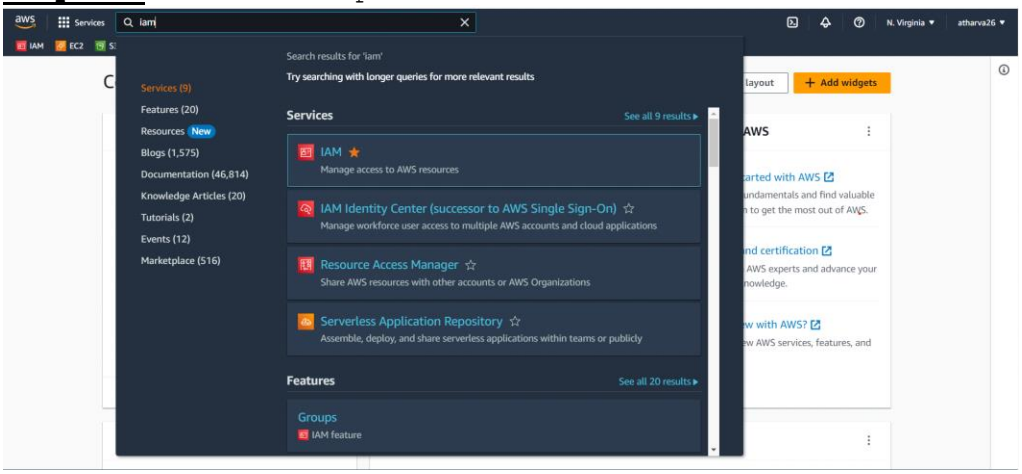
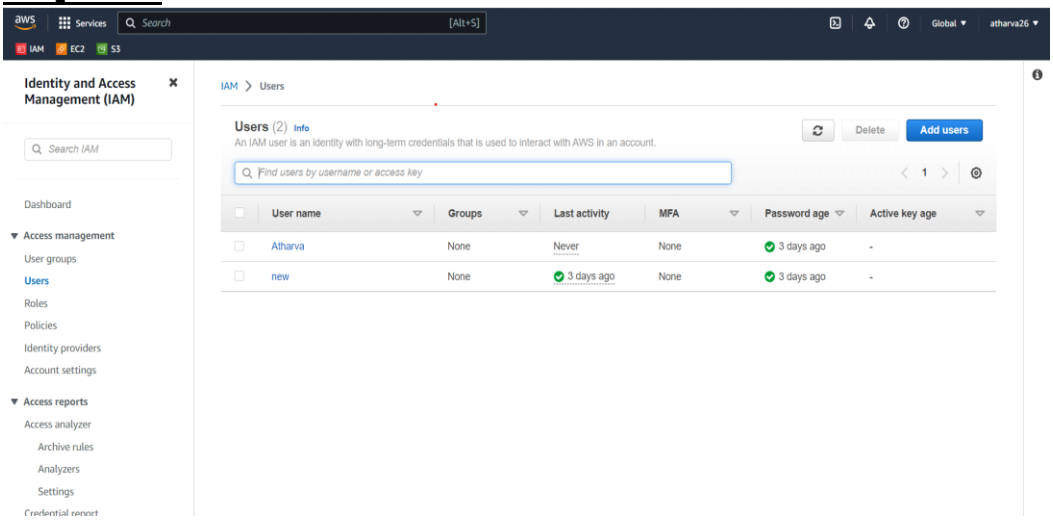
1. Create a New IAM User:

Create a new IAM user with programmatic access.
Assign appropriate permissions to the user based on their role or responsibilities.
Generate and securely provide the user's access key and secret access key.
-->> creating i am user:-

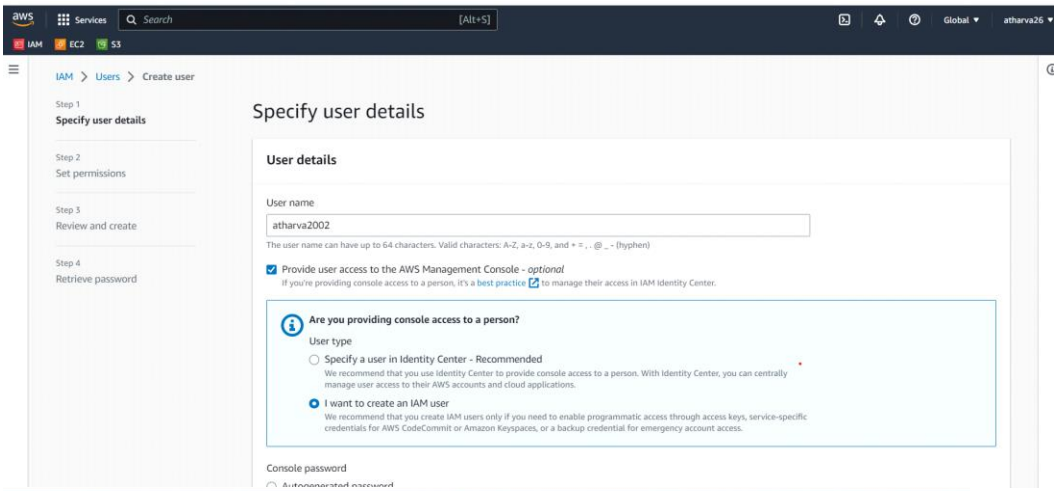
step 1:-search and open iam service on aws

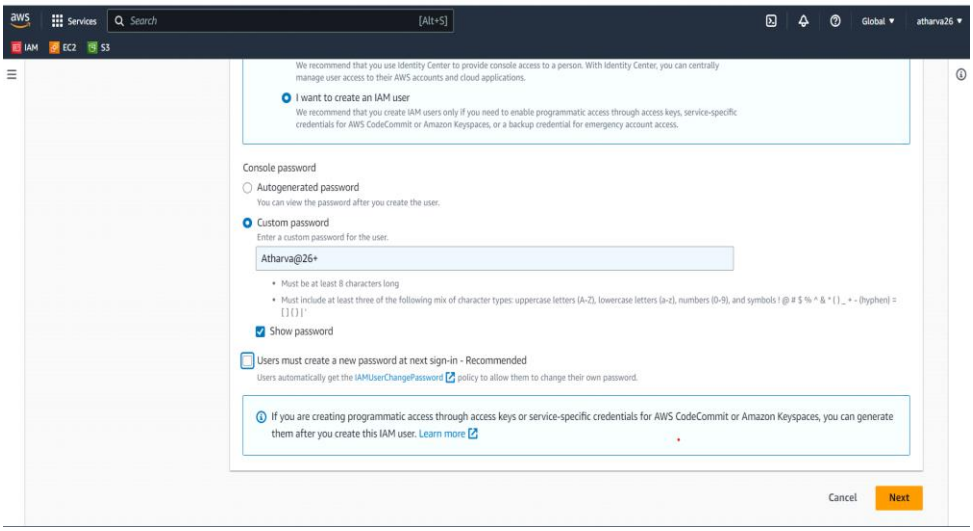


step 2:- Next click on users and next click on add user



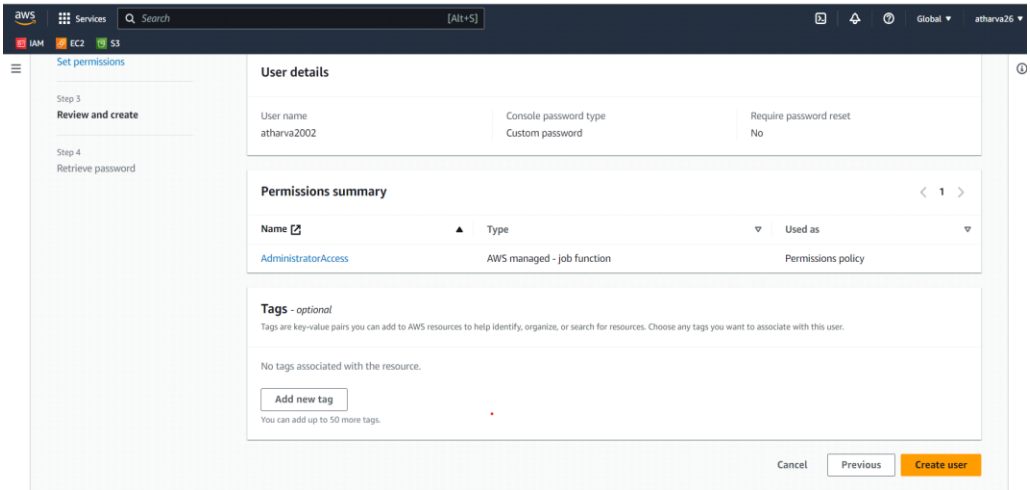
step 3 :-Then gave user name then click on provides users access to the aws management console and in it select i want to create an iam user Gave a password to user by click on custom password
password ex.:- Atharva@26+

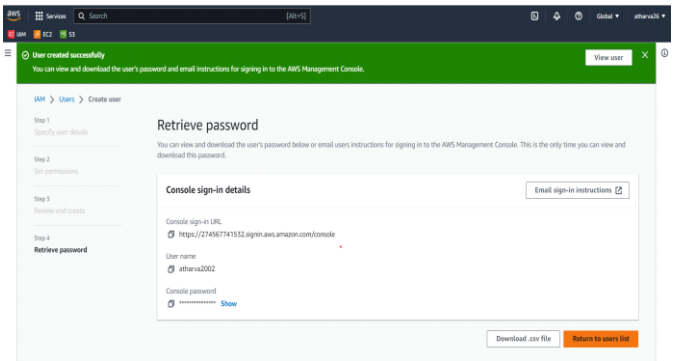




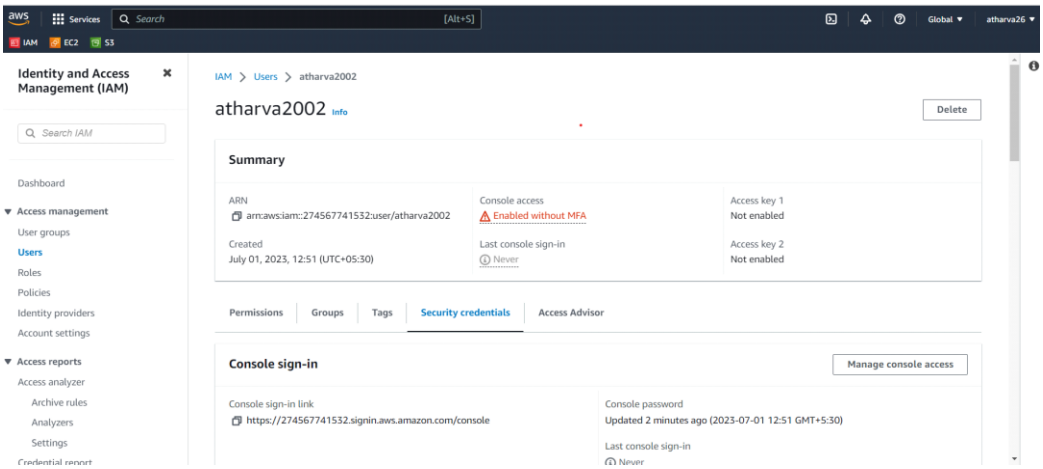
step 4:- Then deselect if u don't want to rechange password when you loged in next time and click on next

step 5:- Then check details you entered and if you want to add tags then you can add it. and click to create user.

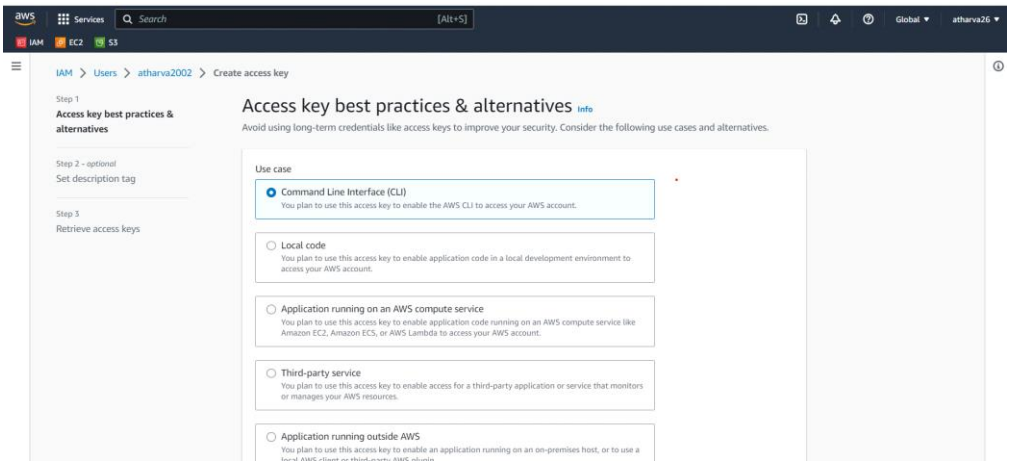


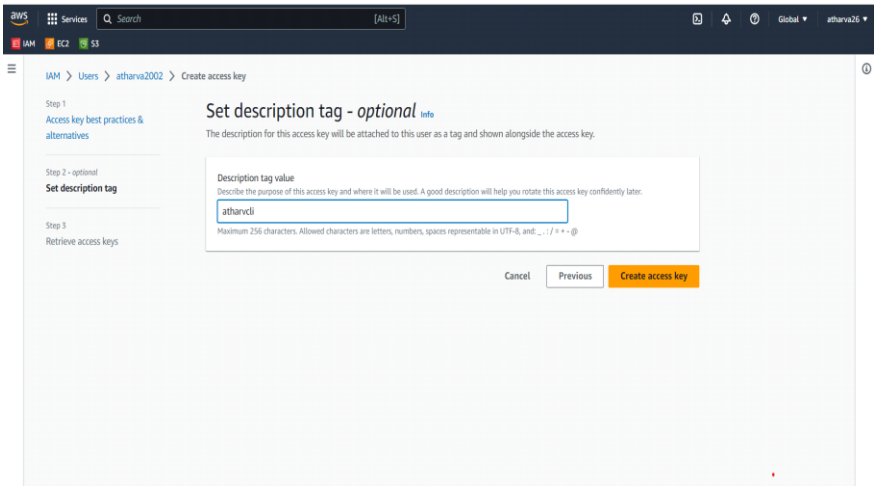


step 6:- Then go to user and go to security credentials go to access key click on create access key.

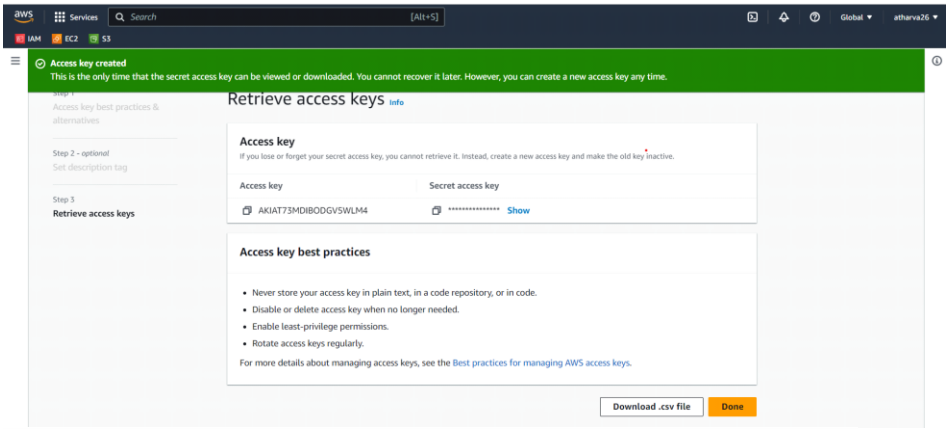


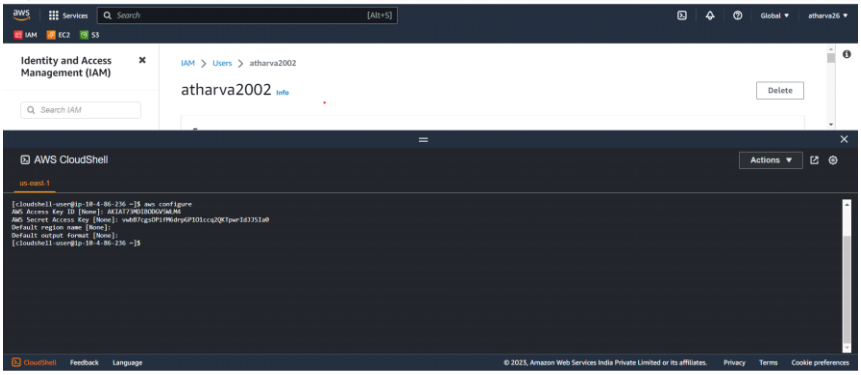
step 7:- Then choose option cammand line interface add description tag if you want and then click on create access key.





step 8:- here please download that both keys because it will not be reatined after that open cli cloudshell and type cammand aws configure after that it will ask for both keys just enter both keys and then enter enter and you will get acess of that user on cli.



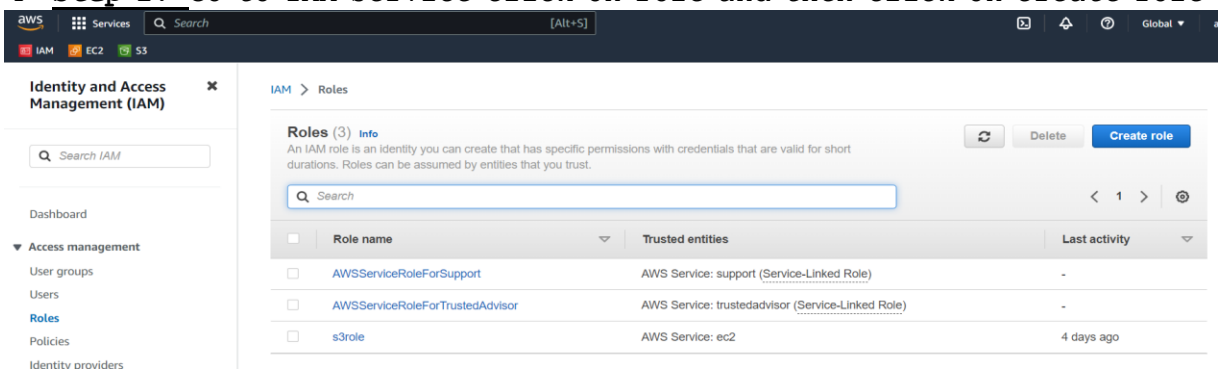


2. Configure IAM Roles:

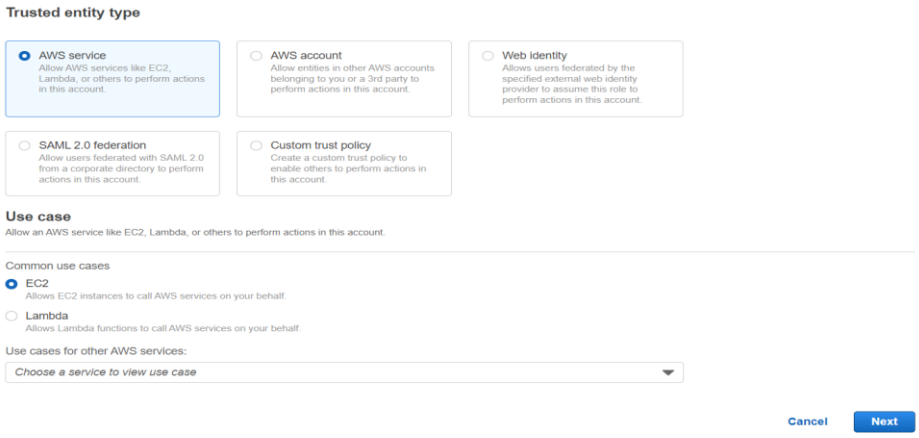
Create an IAM role for EC2 instances or Lambda functions with specific

permissions.
Attach policies to the role that grant necessary permissions to access AWS resources.
Assign the role to EC2 instances or Lambda functions.

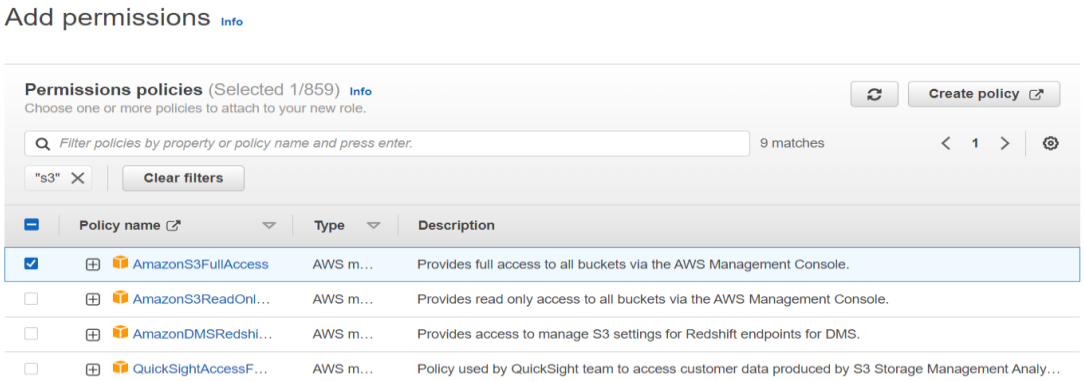
➔ **Step 1:-**Go to IAM service click on role and then click on create role



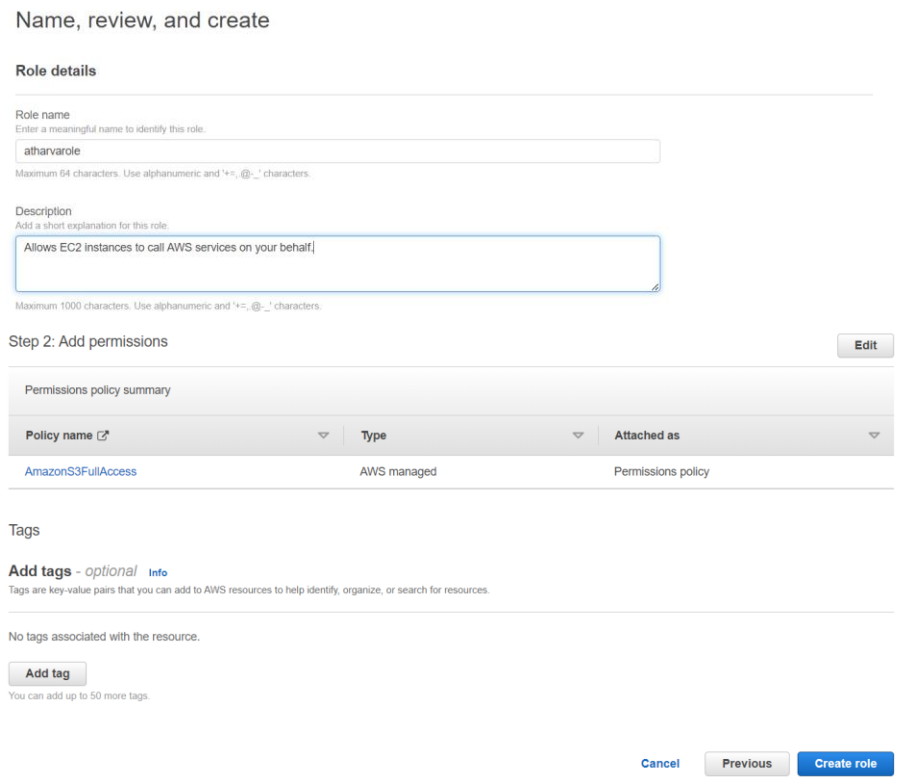
Step 2:-Select aws service and select which service do you want ec2 or lambda and then click on next



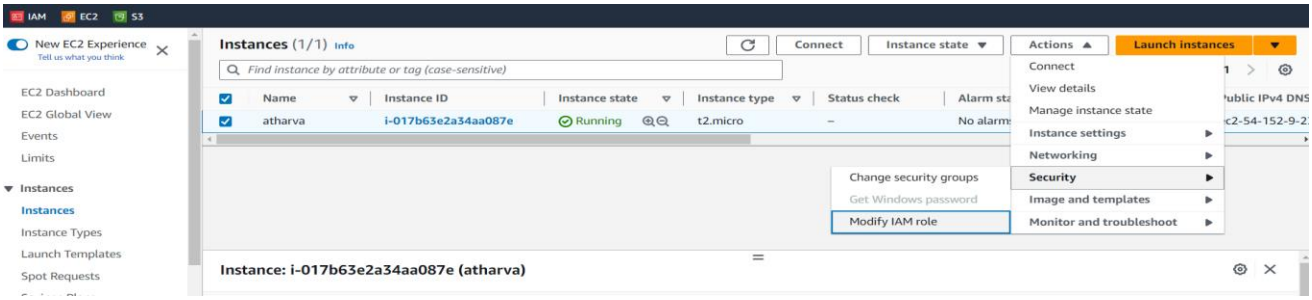
Step 3:-Then attach policy to that role. And click on next.



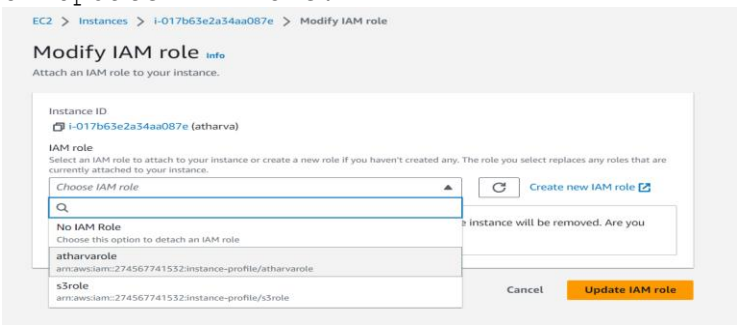
Step 4:-Then give name to the role and add tag if you want then click on create role.



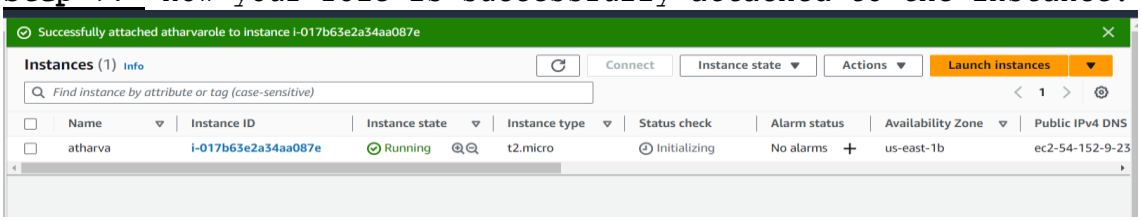
Step 5:- After that go to ec2 instance on which you want to apply role select that instance click on actions then security then select option Modify IAM role



Step 6:- Then select IAM role that we create in previous step and then click on Update IAM role.

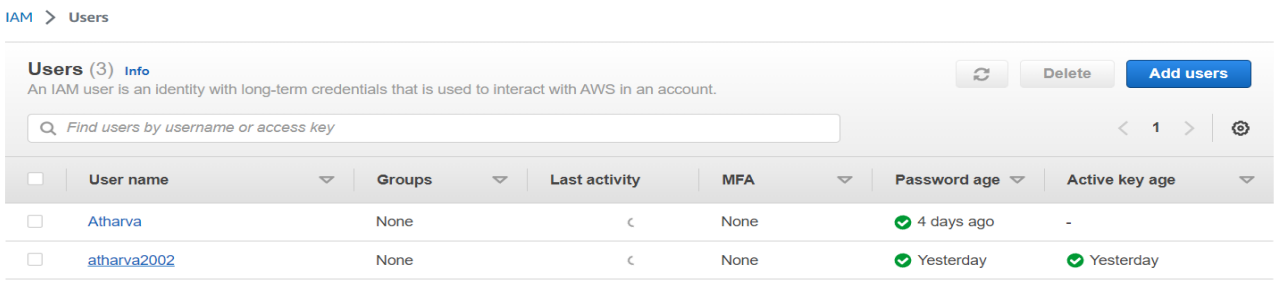


Step 7:- now your role is successfully attached to the instance.

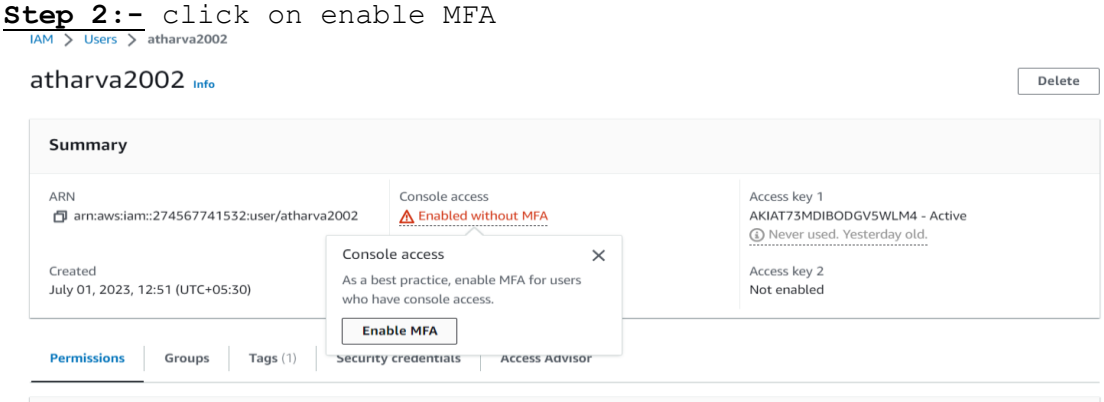


3. Implement Multi-Factor Authentication (MFA):

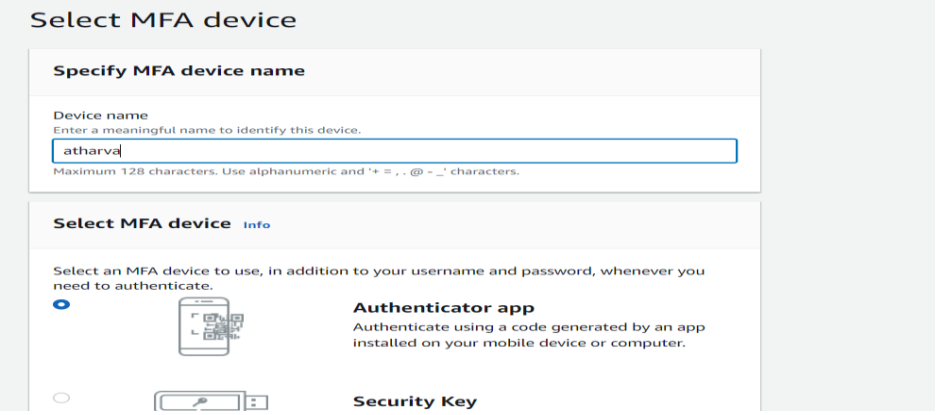
Enable MFA for IAM users to provide an additional layer of security.
Guide users on how to set up MFA devices (such as virtual MFA apps or hardware tokens).
Test the MFA configuration to ensure it functions correctly.
→ **Step 1:-** select user from IAM service on which you want apply MFA click on that user.



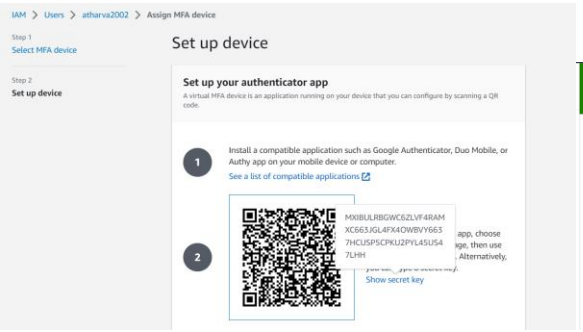
Step 2:- click on enable MFA

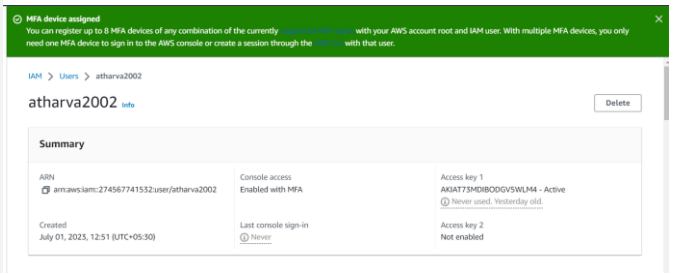


Step 3:- then enter one meaningful name and select option like authenticator app or security key or hardware totp token and click on next I choose app



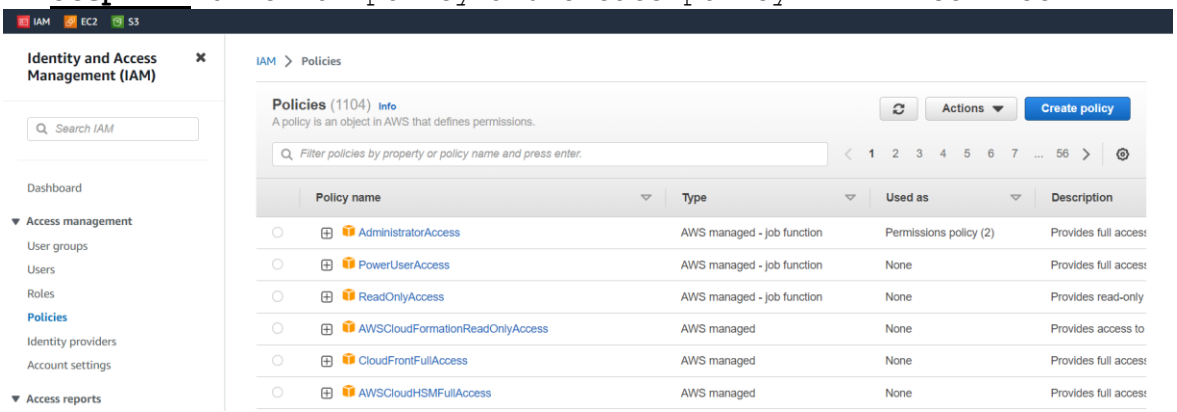
Step 4:- then open app and scan QR or enter that secret key which is shown in below picture and after that enter 2 MFA codes then click on next. MFA is enabled.



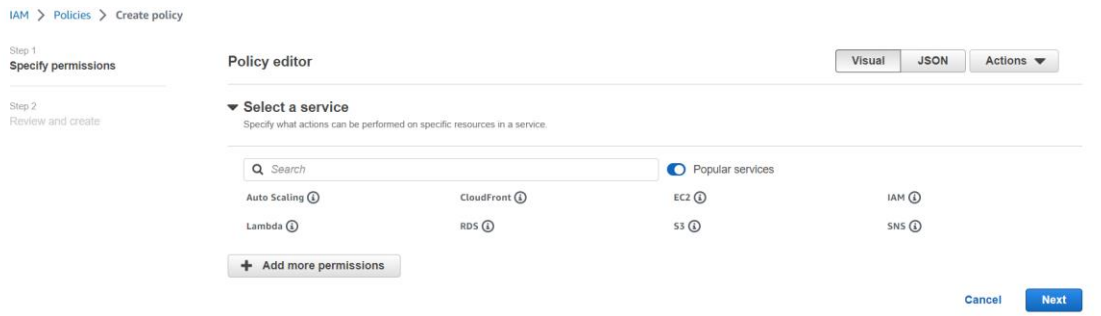


4. Create IAM Policies:

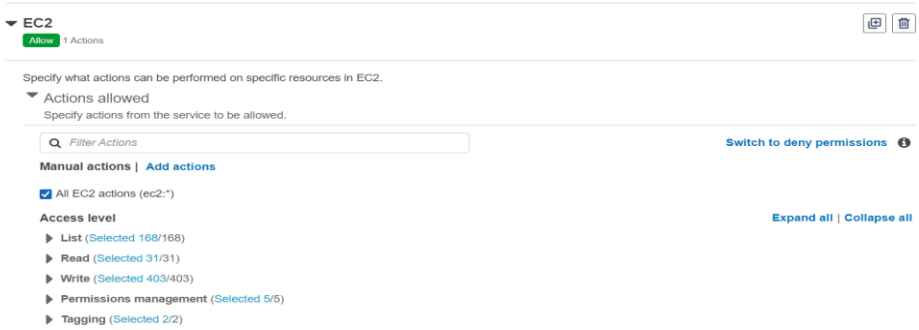
Write a custom IAM policy that allows or denies specific actions on AWS resources.
Associate the policy with the appropriate IAM users, groups, or roles.
Test the policy to verify that the desired access control is enforced.
→ **Step 1:-** Click on policy and create policy in IAM service



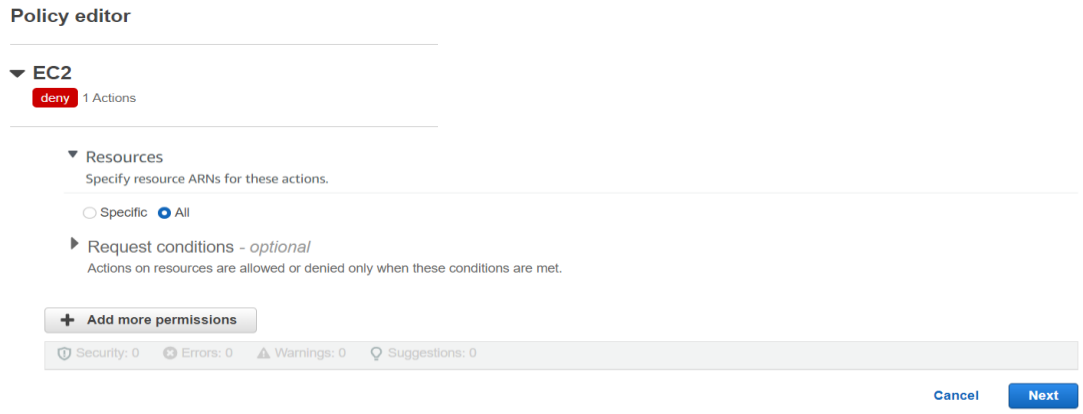
Step 2:- Select which permission you want to add or deny.



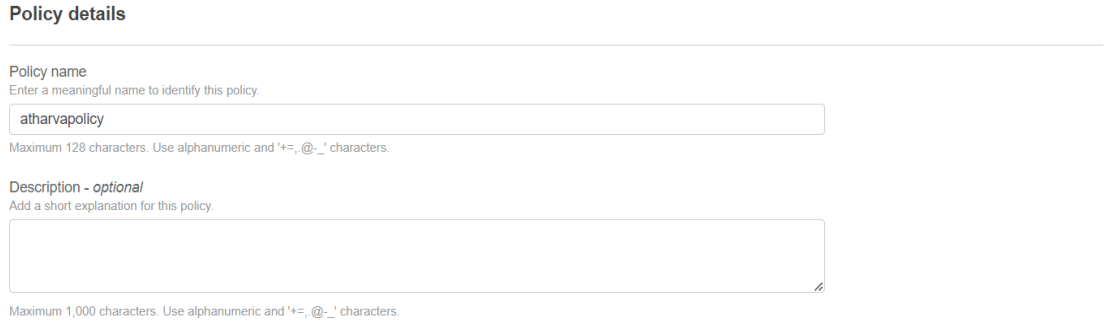
Step 3:- I chose ec2 policy and I want to deny it for all ec2 service that's why I clicked on all service and then click on switch to deny.

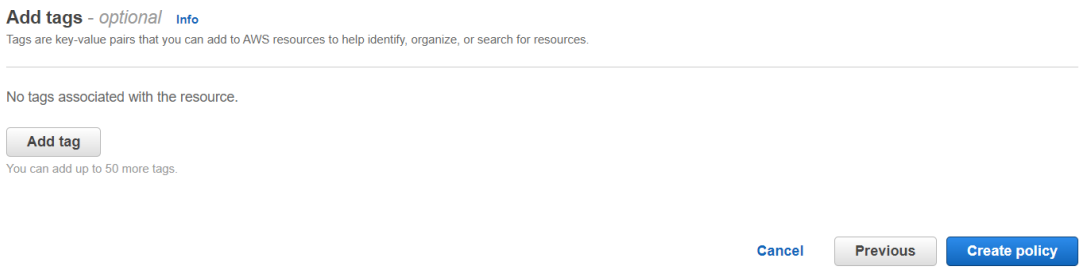


Step 4:- after click to switch to deny scroll down and there you can select it for all or for specific resources I want apply it on all resources so I select all and then click on next.

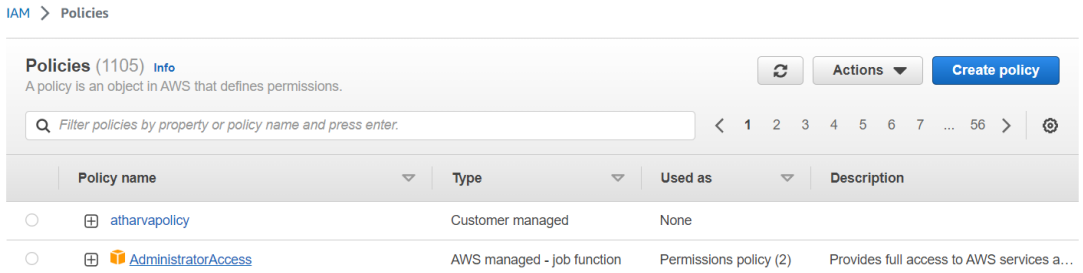


Step 5:- give the name to that policy and add tag if you want to add and then click on create policy.

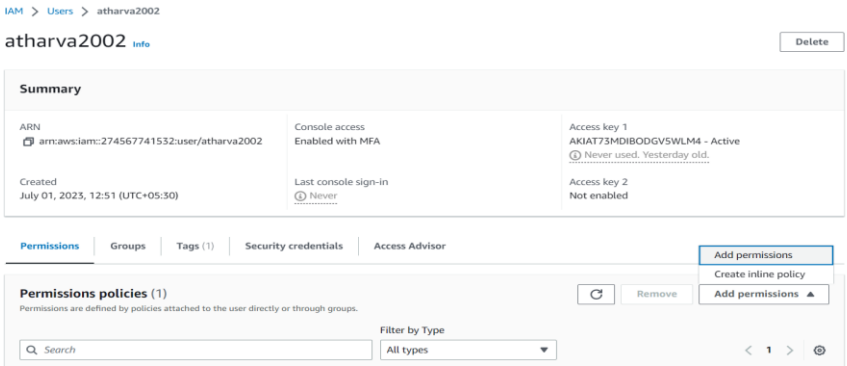




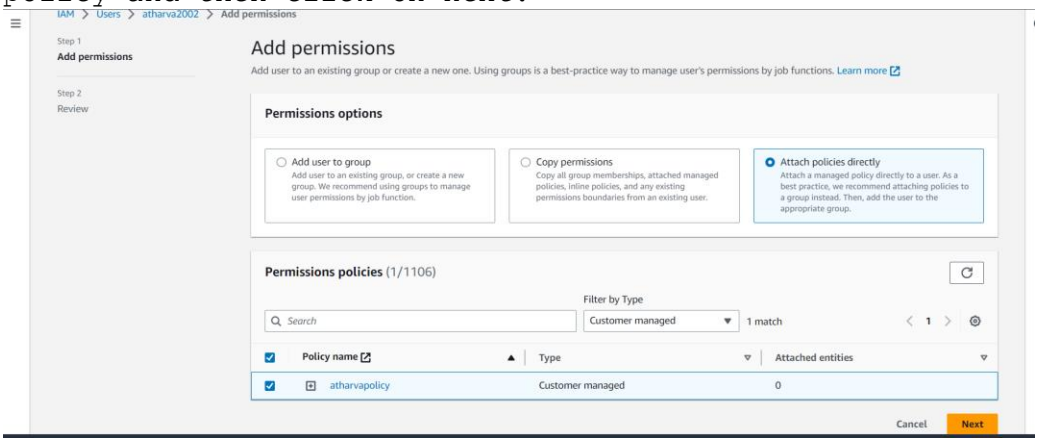
Step 6:- policy is created and created policy is shown in policy section as mentioned in the below pictures.



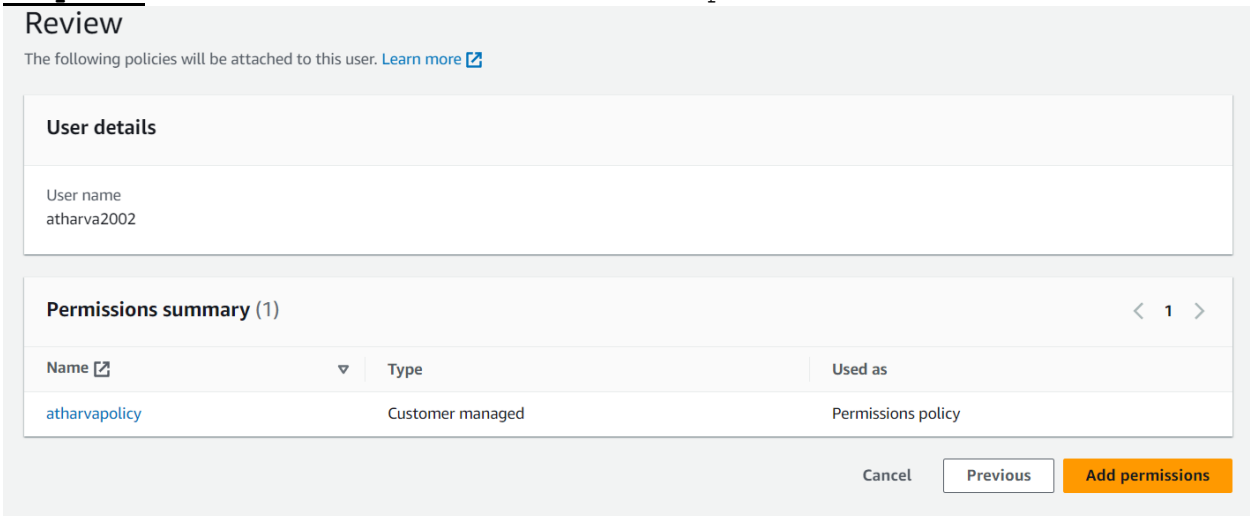
Step 7:- then go to user on which you want to apply the policy. Then click on add permission.



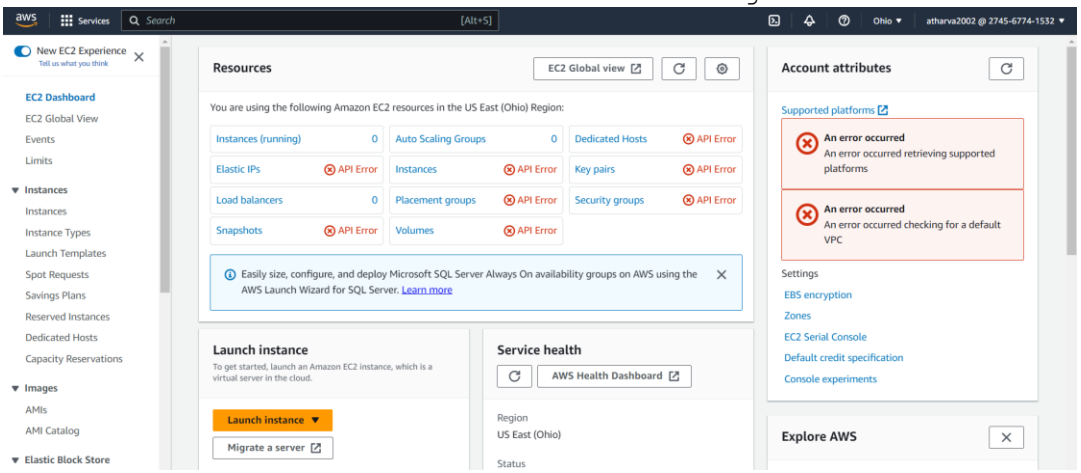
Step 8:- then click on attached policy directly then search your created policy and then click on next.



Step 9:- check details and click on add permission.

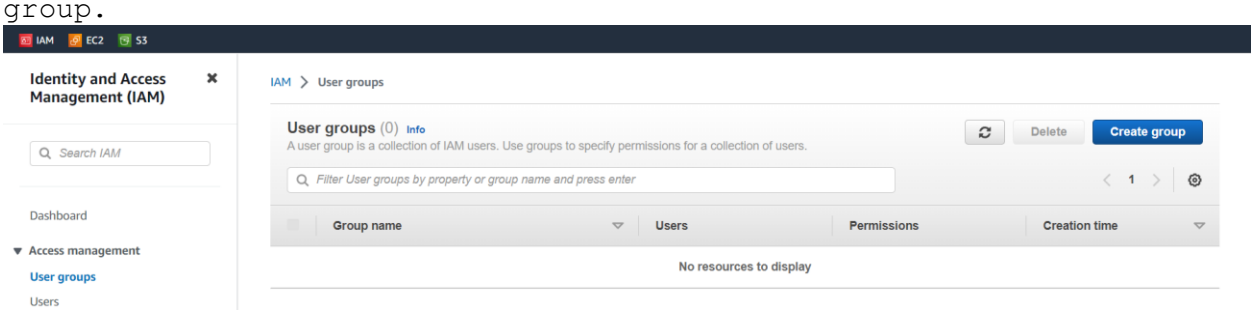


Step 10 :- check that applied policy works or not so loged into the user atharva2002 and check that this user will get EC2 access or not.

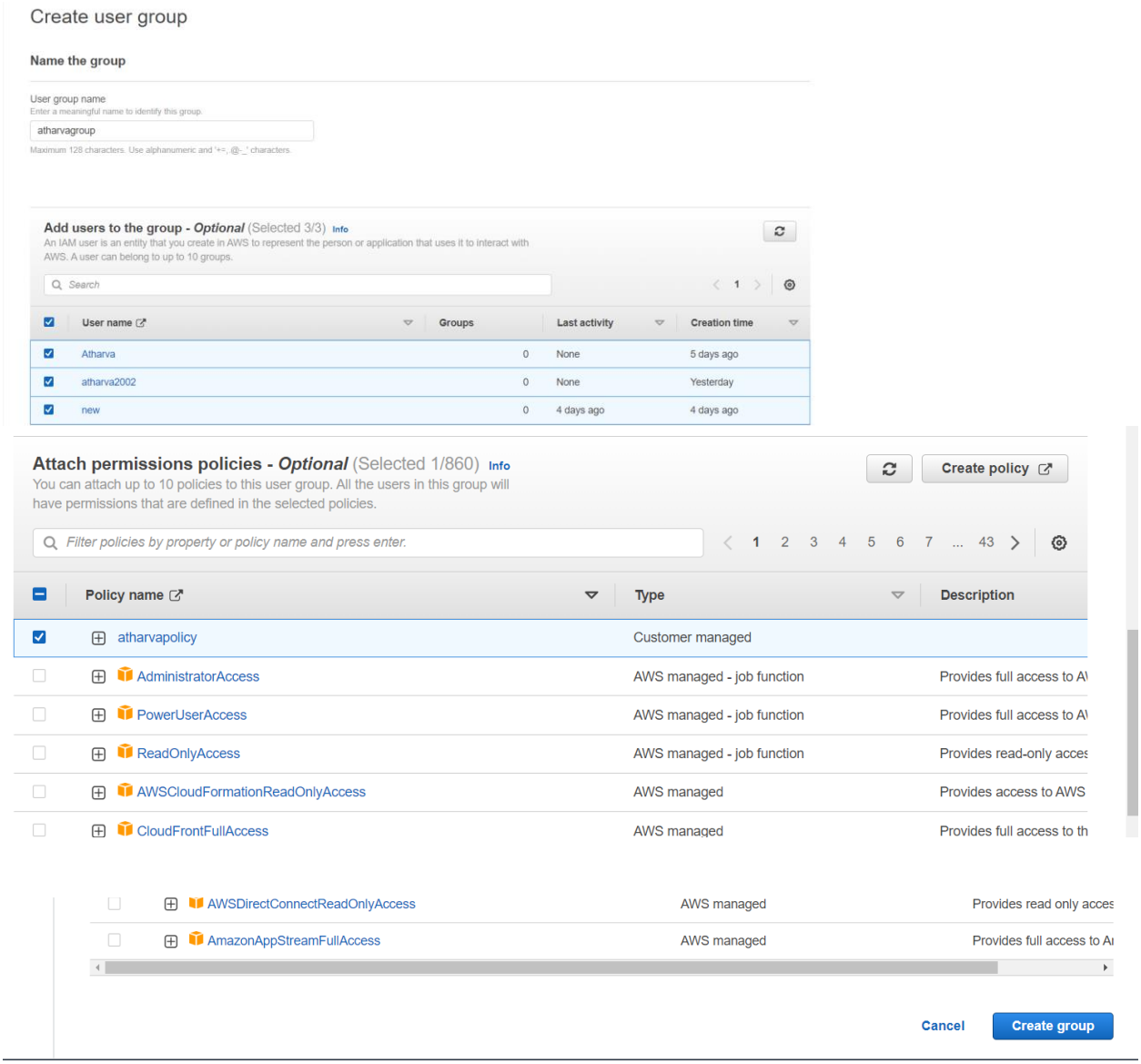


5. Use IAM Groups:

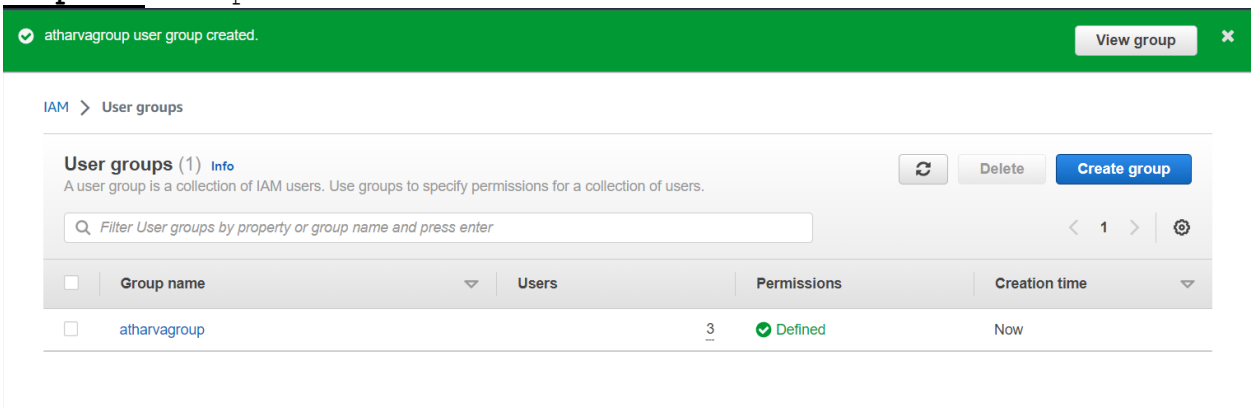
Create an IAM group and assign permissions to it.
Add IAM users to the group to manage their access collectively.
Remove users from the group when their access requirements change.
→ **Step 1:-** Go to IAM service click on user group and the click on crate group.



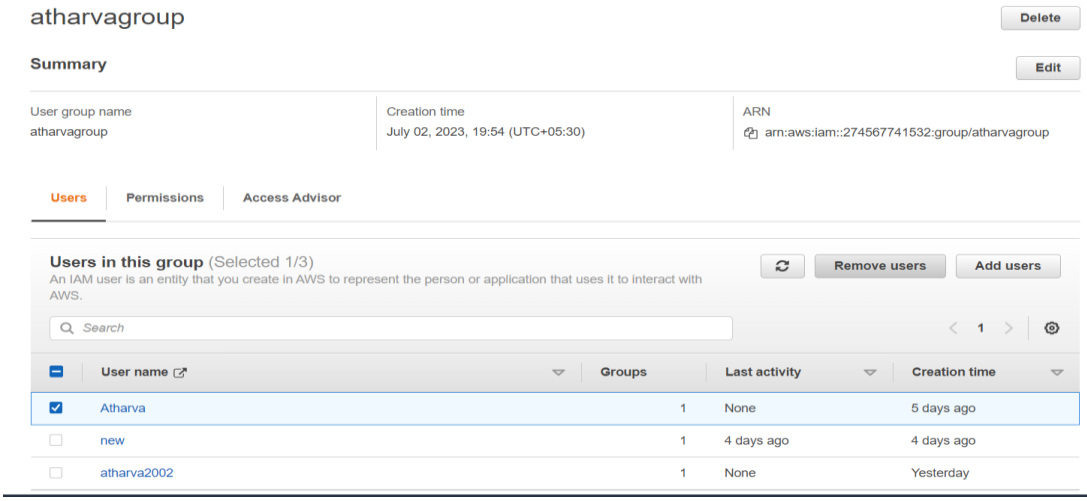
Step 2:- Then give the name to the group and select users you want to add in that group. Then add the policy to the group. Then click on the create group



Step 3:- Group is created.



Step 4:- to remove user from group then click on group select user you want to remove and click on remove.

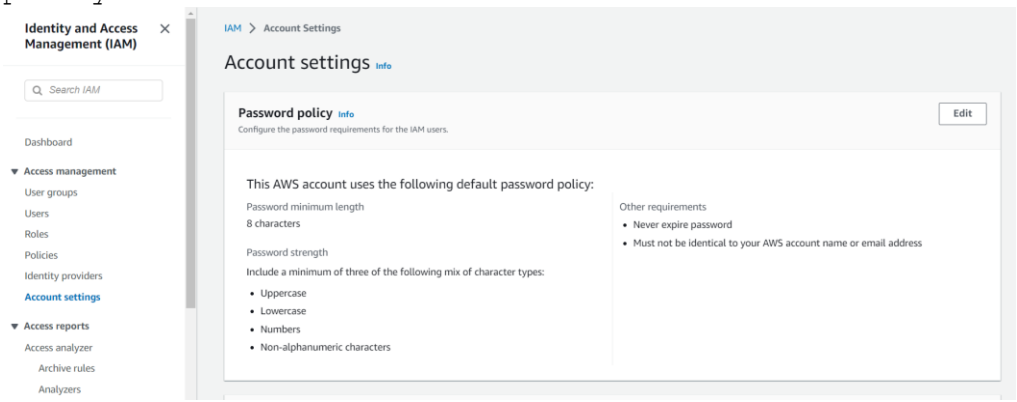


6. Implement IAM Access Analyzer:

Enable IAM Access Analyzer to identify unintended access to your AWS resources.
Review and resolve findings generated by IAM Access Analyzer.
Continuously monitor and remediate any potential security risks.

Enable AWS CloudTrail for IAM:
Enable CloudTrail to capture API activity related to IAM.
Configure CloudTrail to store logs in an S3 bucket.
Review and analyze CloudTrail logs for any suspicious or unauthorized activities.

Implement IAM Password Policies:
Define and enforce password policies for IAM users.
Set requirements such as minimum password length, complexity, and expiration.
Regularly remind users to update their passwords according to the policy.
→ **Step 1:-** click on Account settings and click on edit option in password policy.



Step 2:- and then click on coustom and do the changes whatever you want

and click on save change.