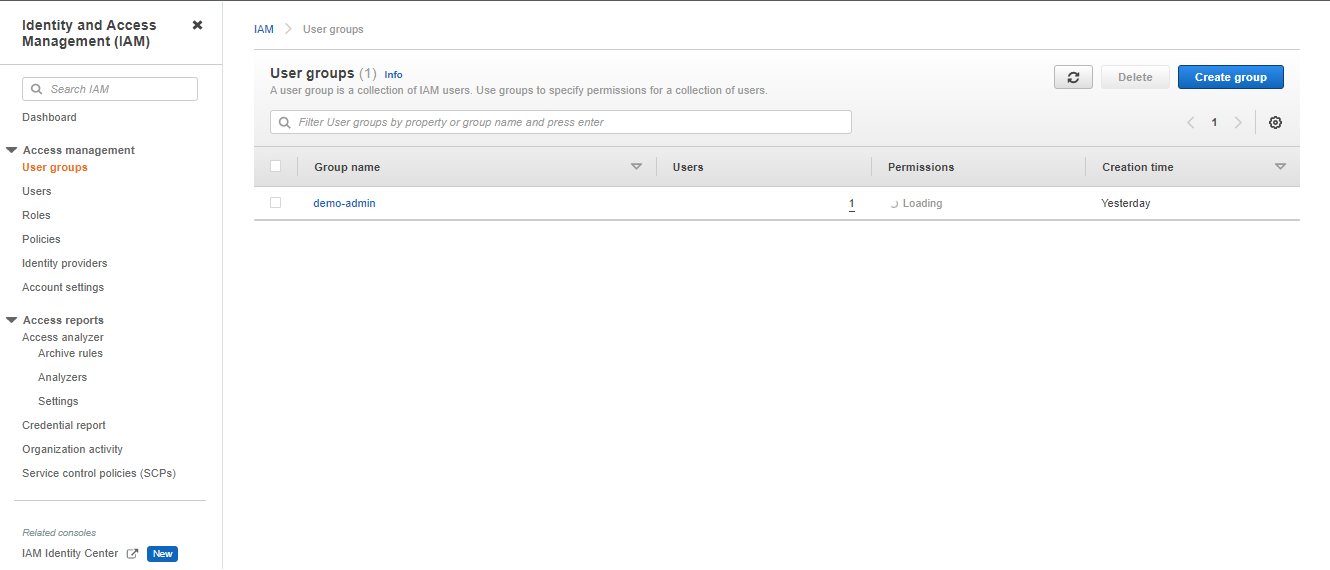
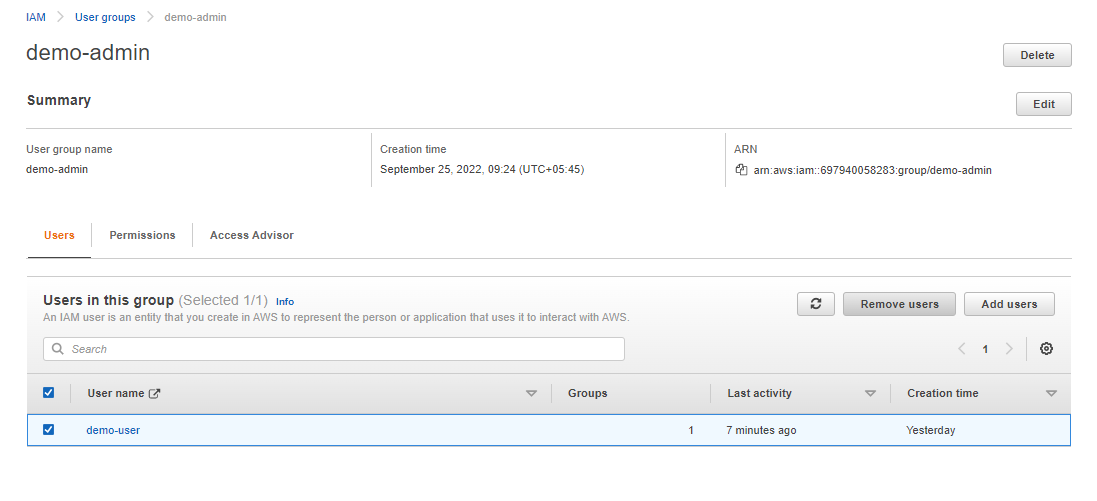
Go to IAM user group

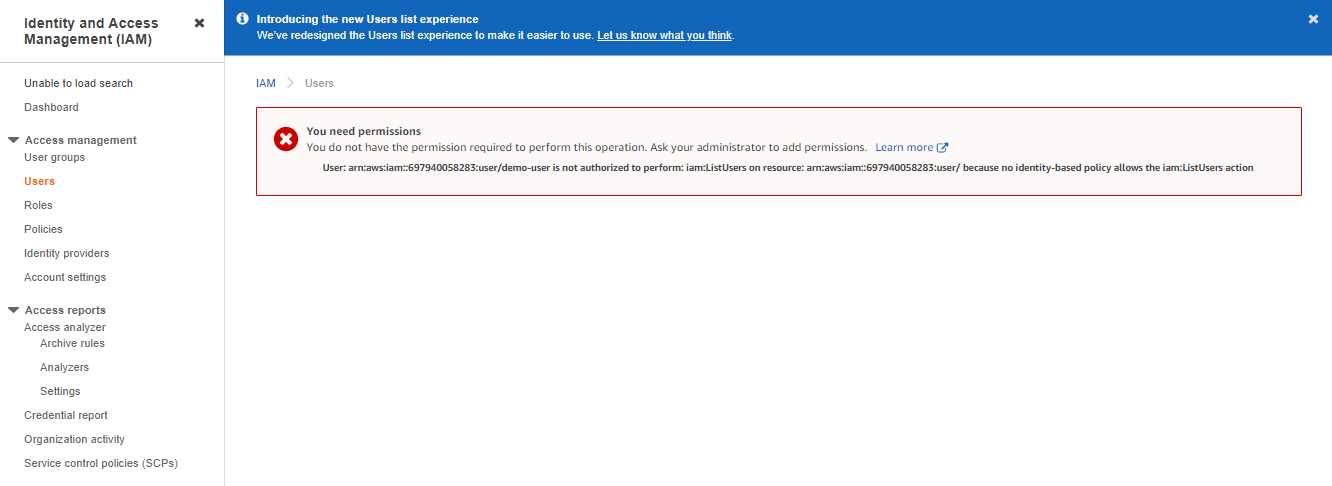


Open group name

* Click on **Remove users.**

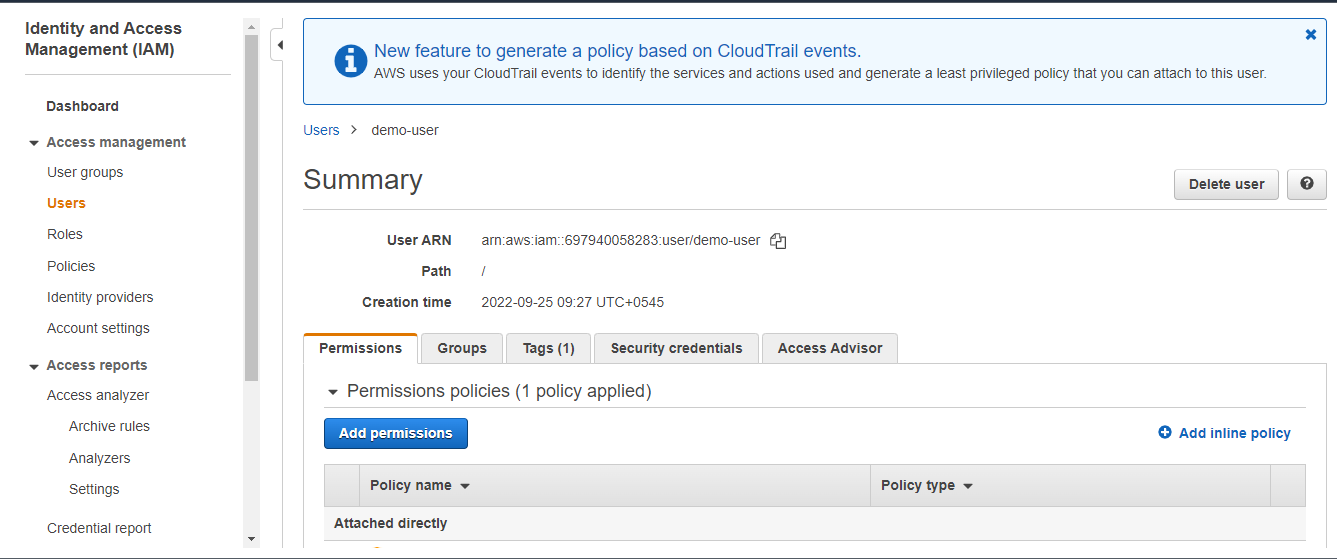


Now you will see following changes

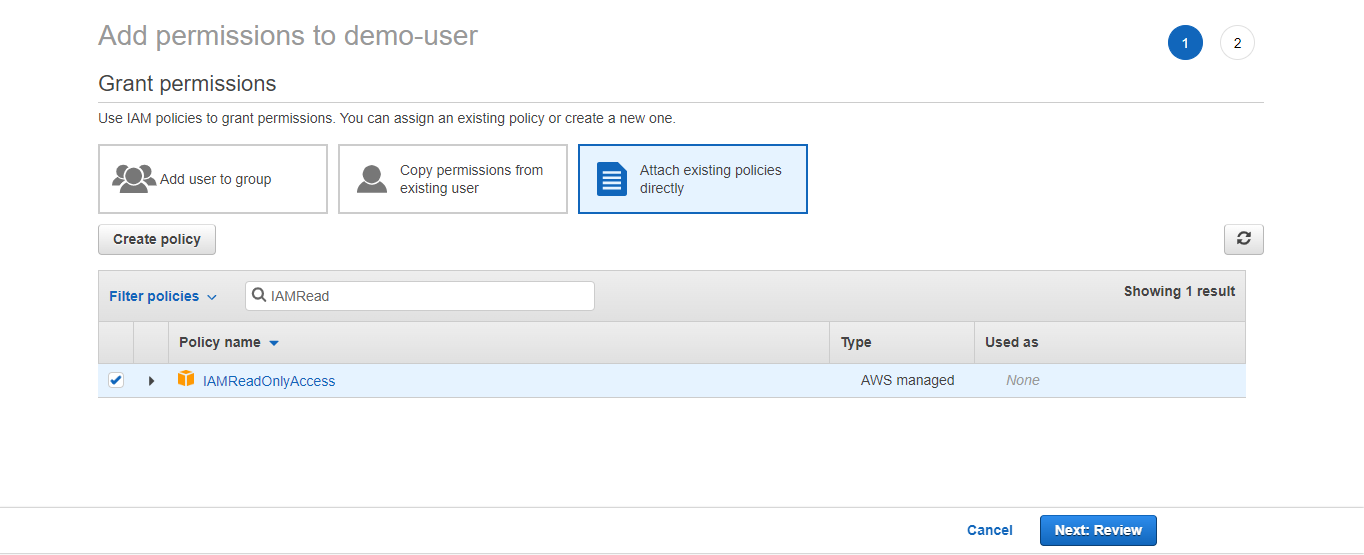


Again Go to Users and own user name demo-user on IAM using your root aws account.

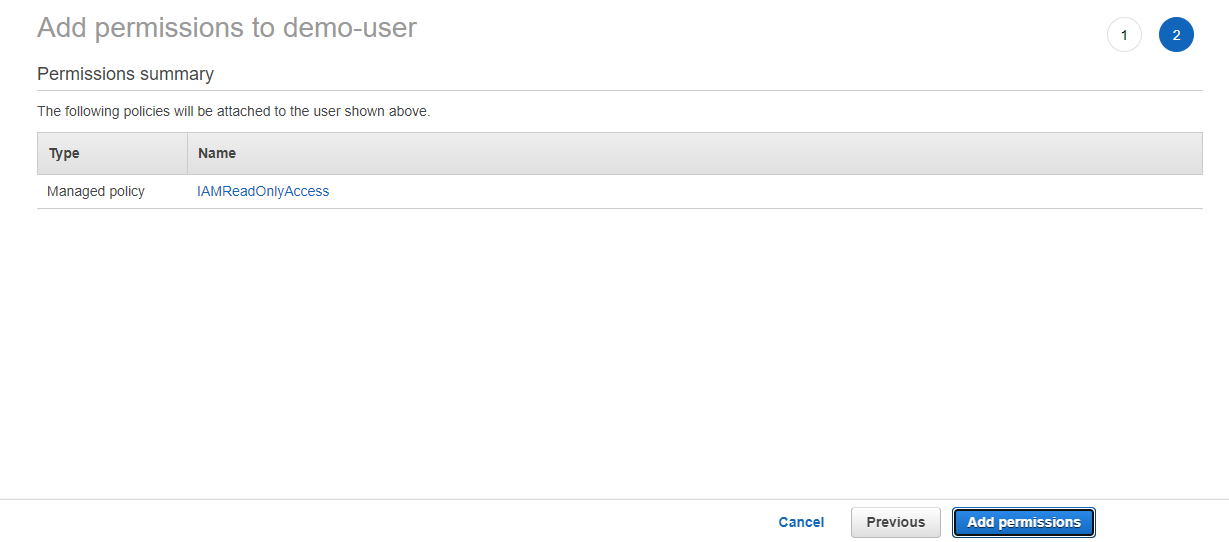
Click on **Add permissions.**



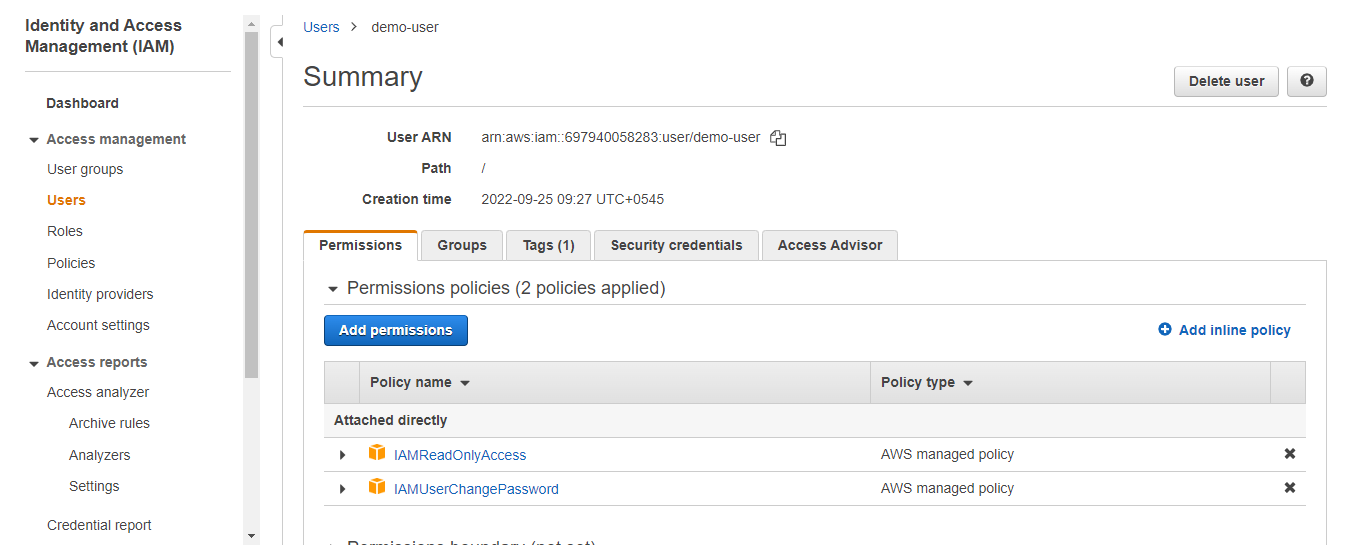
* Click on **Attach existing policies directly**
* Select **IAMReadOnlyAccess**.
* Once completed **Click on Review**.



Click Add permission.

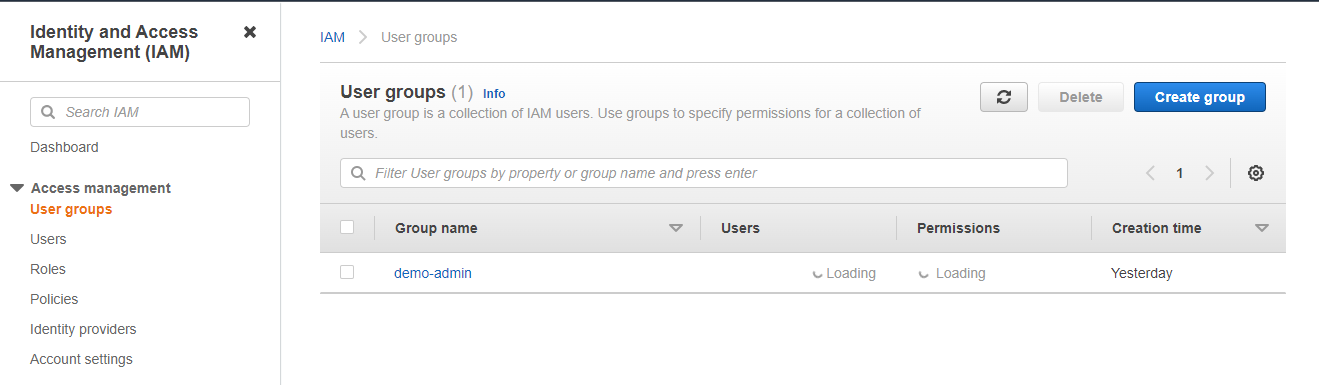


Now, Alias account has IAMReadOnlyAccess.

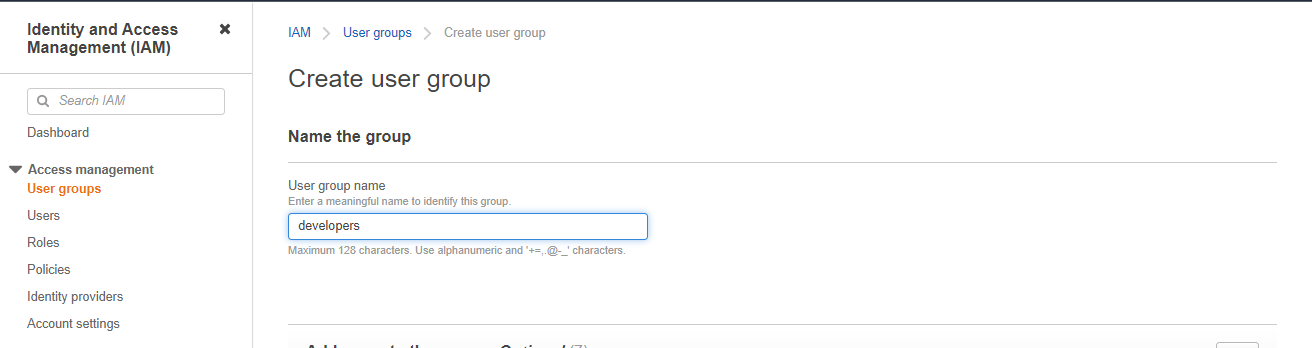


Now Go to your alias account

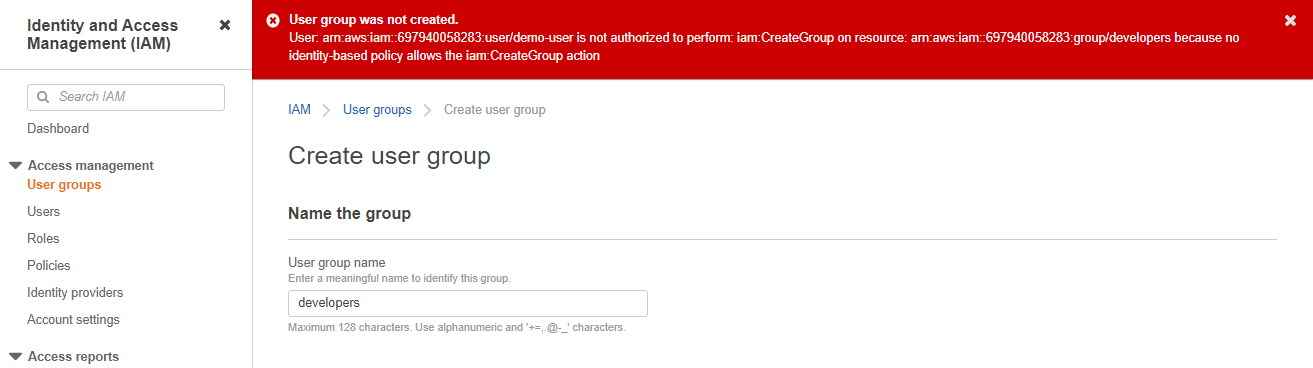
Go to User Group on IAM console



Create Group name

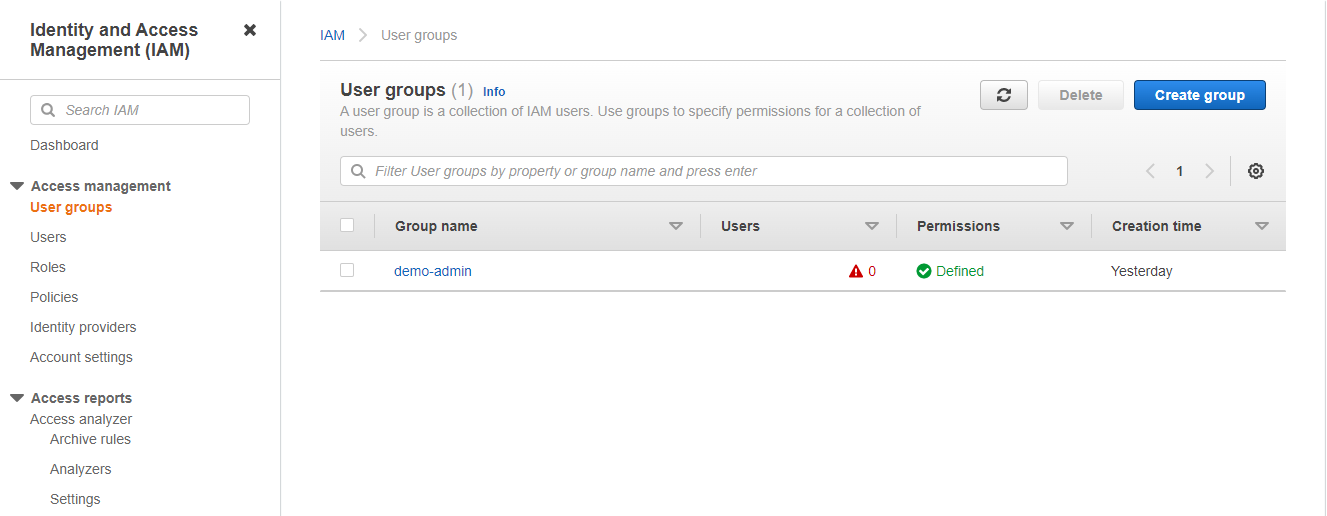


You arenot authorized to create a group.You have read only access.

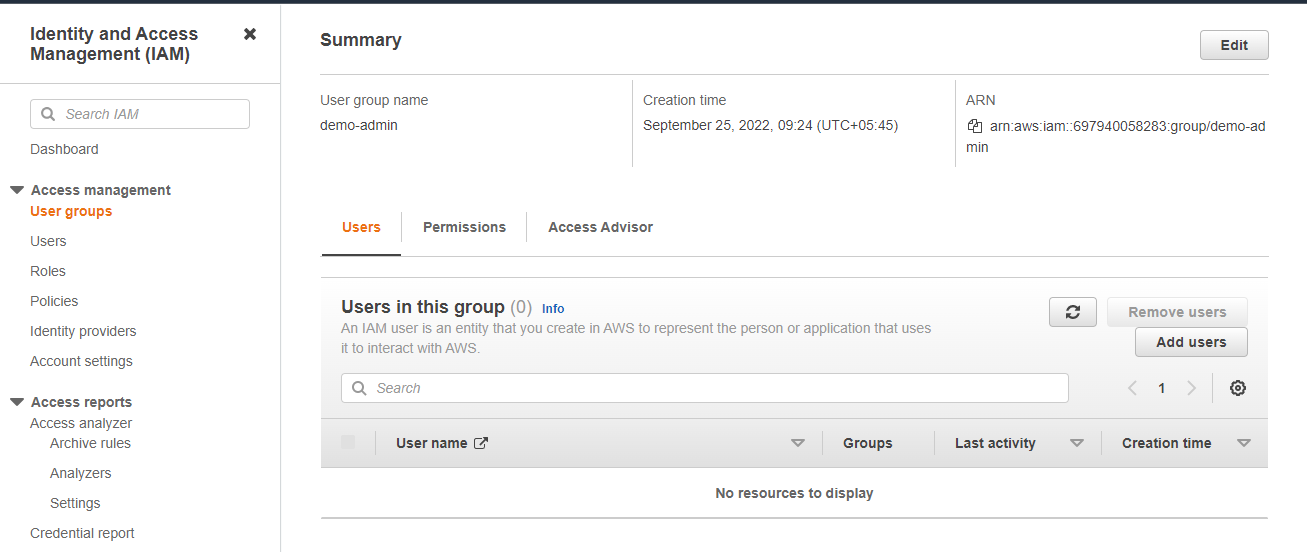


Again go to root account

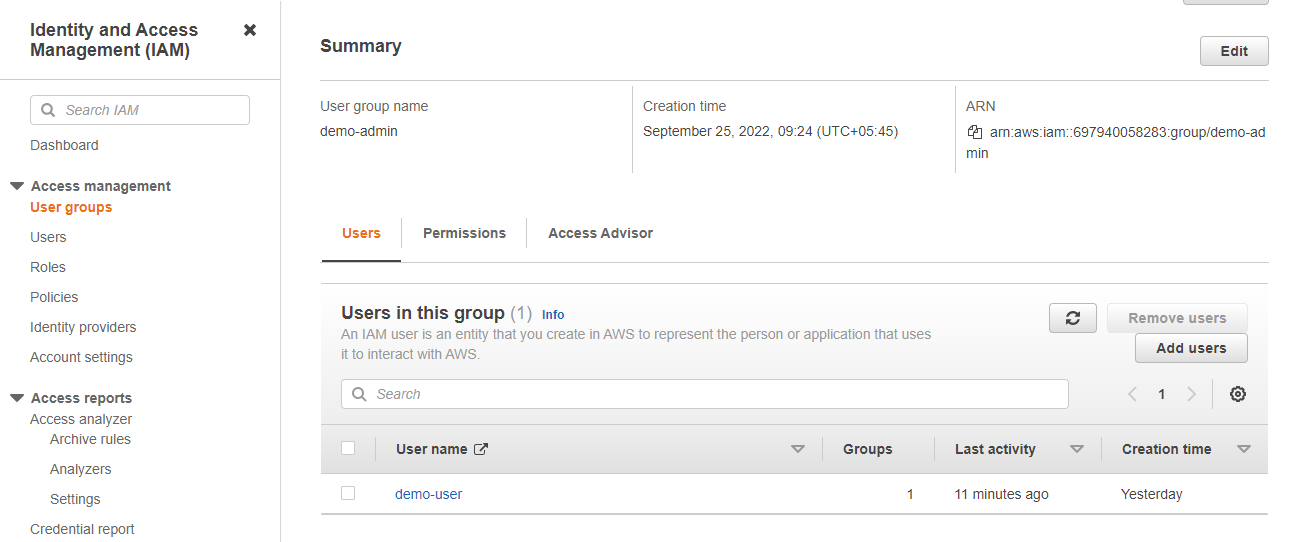
* Go to **User Groups**
* Click on **Create group**



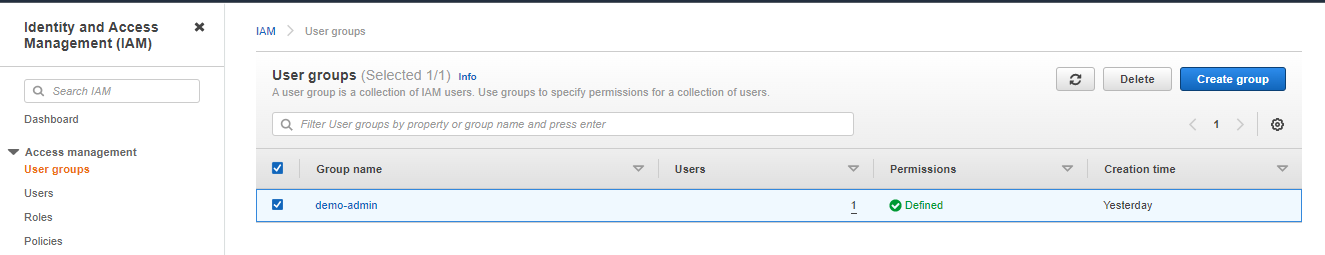
* Click on **Add users.**



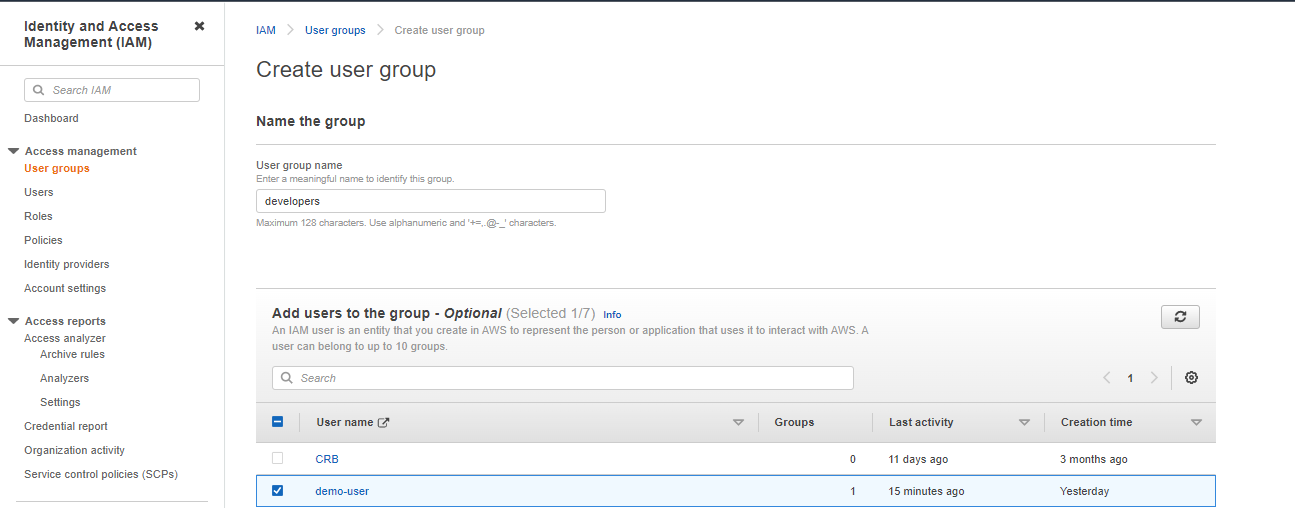
* Select your user name demo-user
* Click on Add user



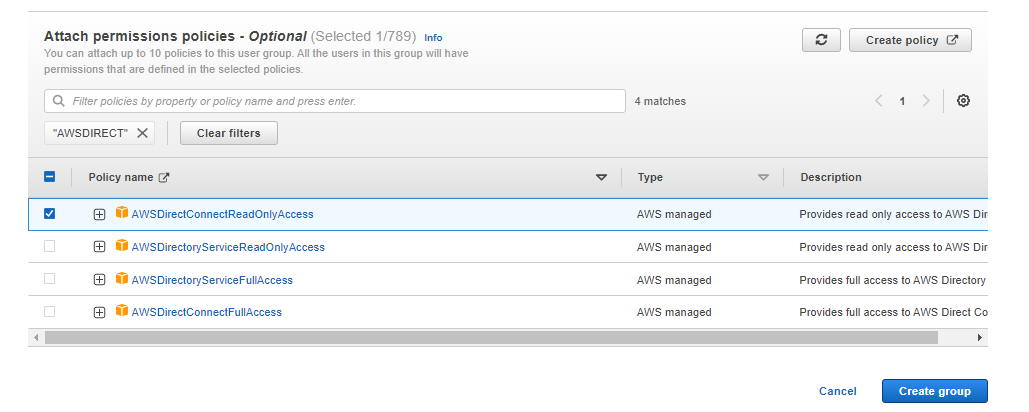
Go to user group and Create group



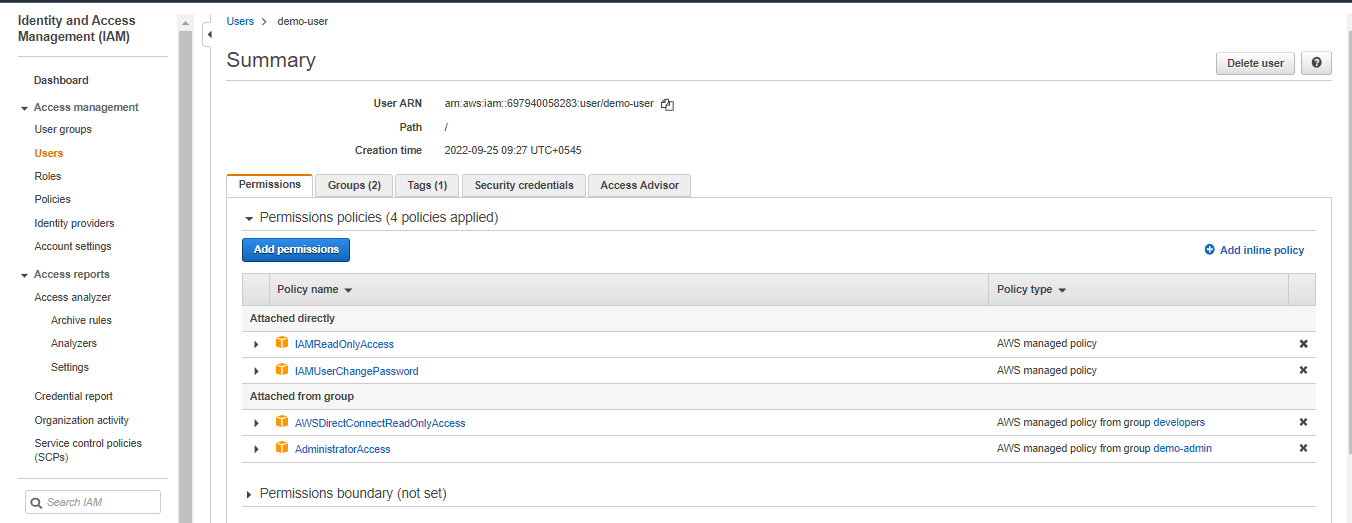
Name Group with attach user name and attach policies.



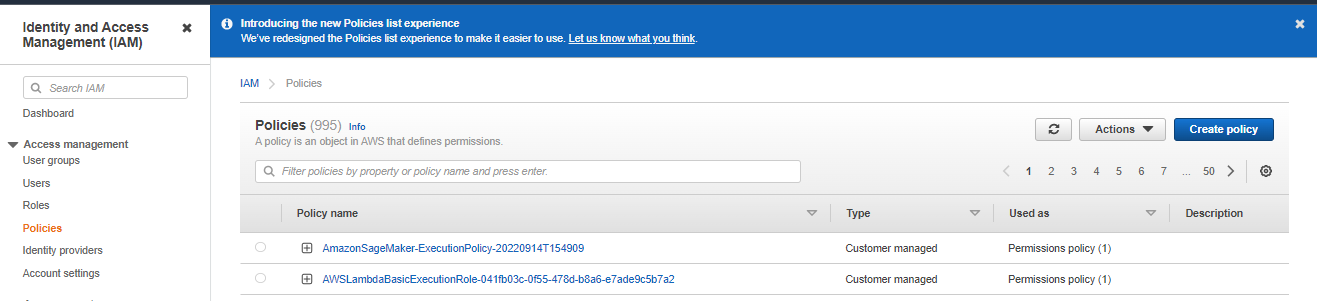
Then create group



One Users you can see two attach policy from two groups.

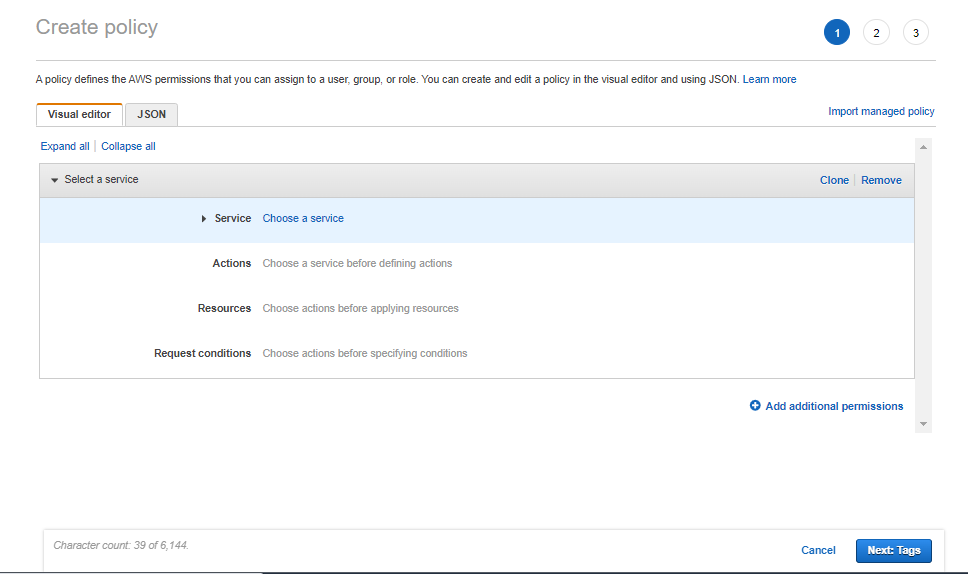


* Go to policies using root account on IAM console.
* Click on Create policy.

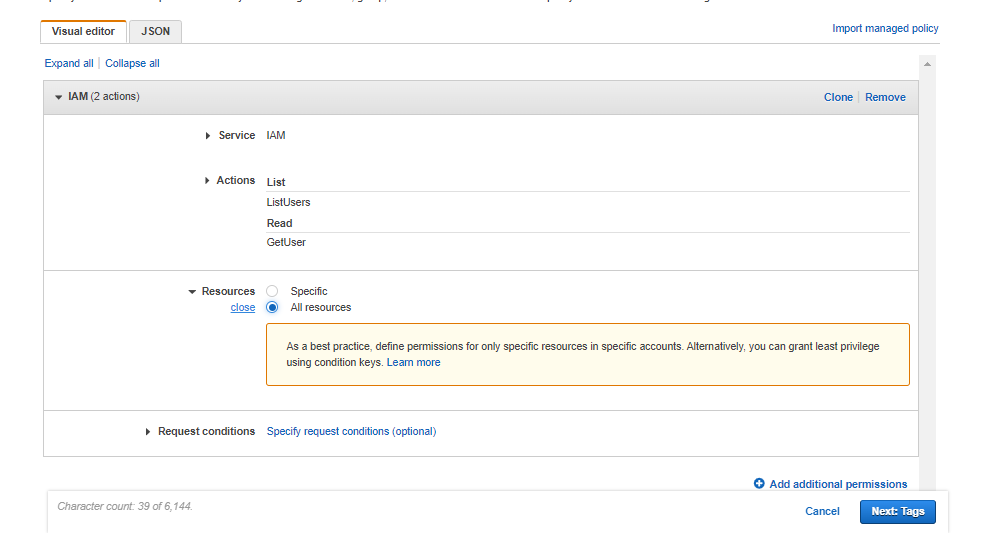


You have two options visual editor or JSON

* Click on visual editor.



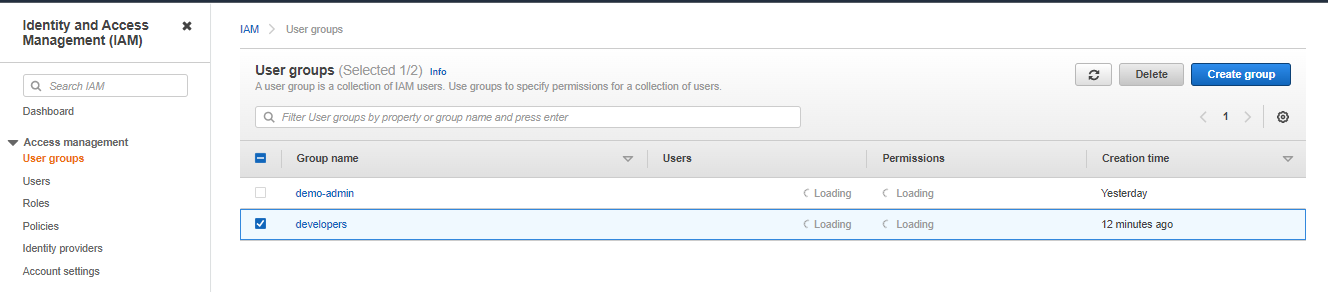
* Choose IAM service
* Choose ListUsers,GetUsers,

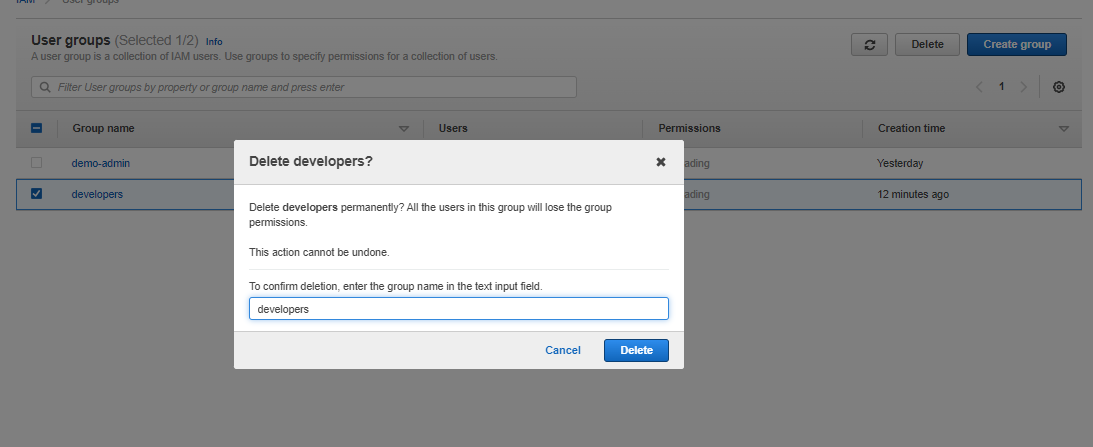


In json format.



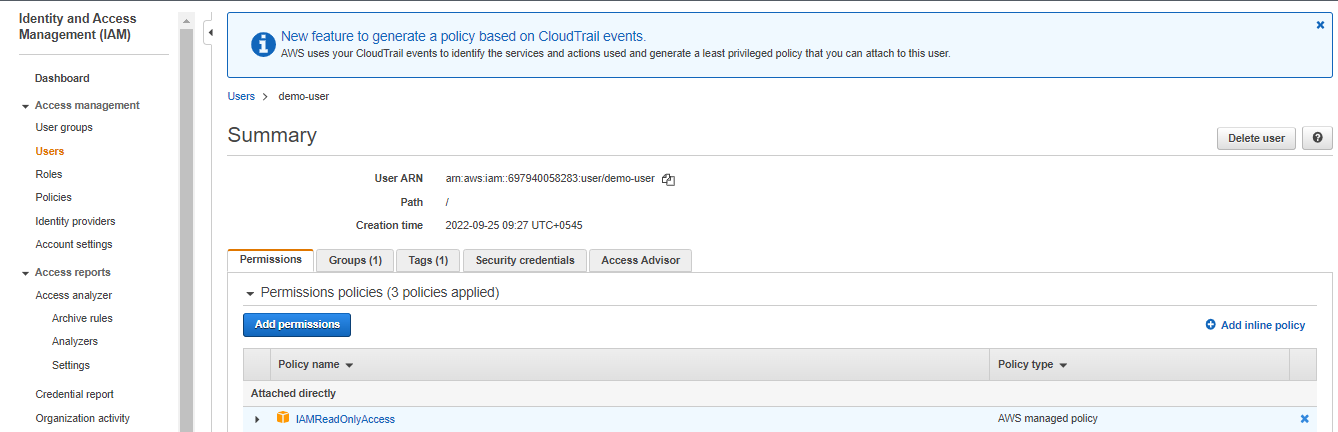
* Go to user group and delete developers user group.



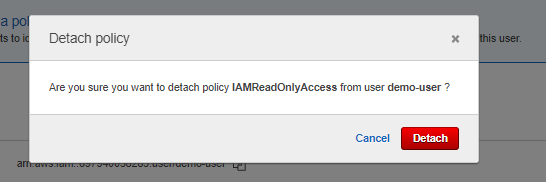


Go to users and click on your Users.

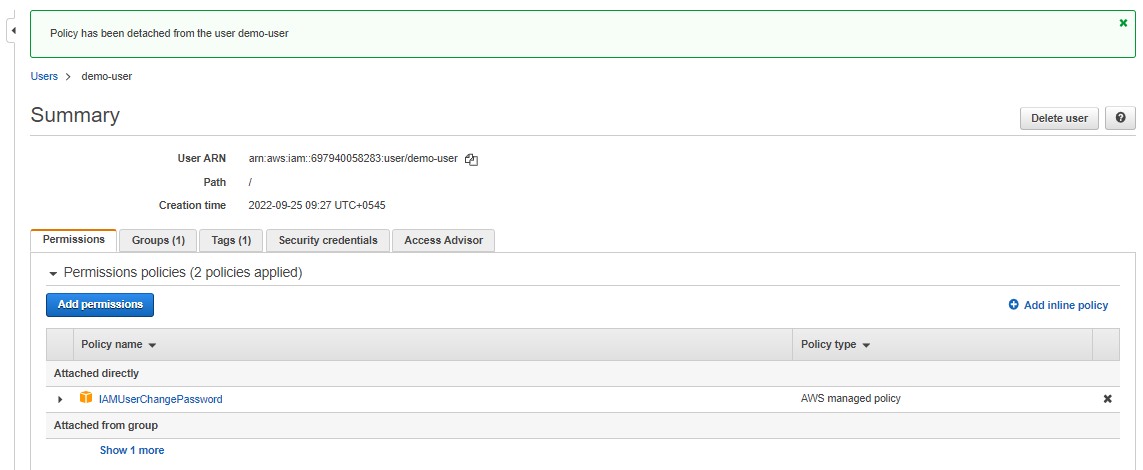
Click close bar.



Click Detach.



* Policy has been removed.



Go to alias account

