Identity and Access Management (IAM)

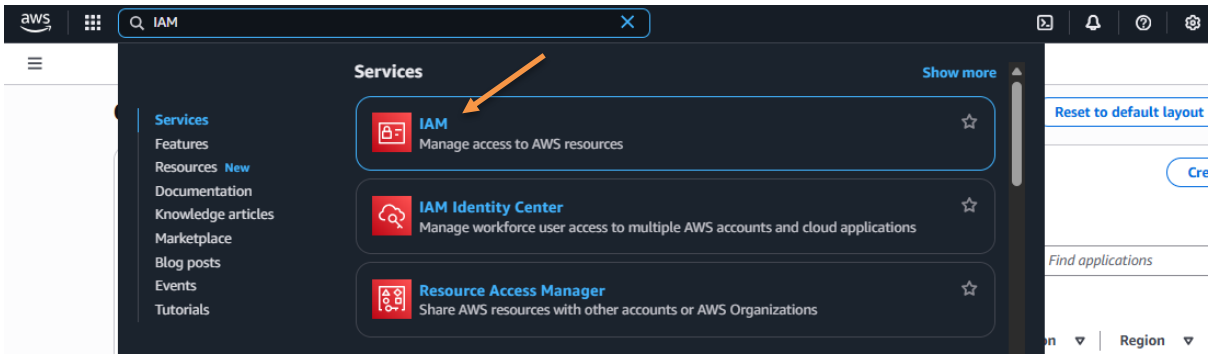
Introduction:

- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources.
- With IAM, you can manage permissions that control which AWS resources users can access.
- You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
- IAM provides the infrastructure necessary to control authentication and authorization for your AWS accounts.

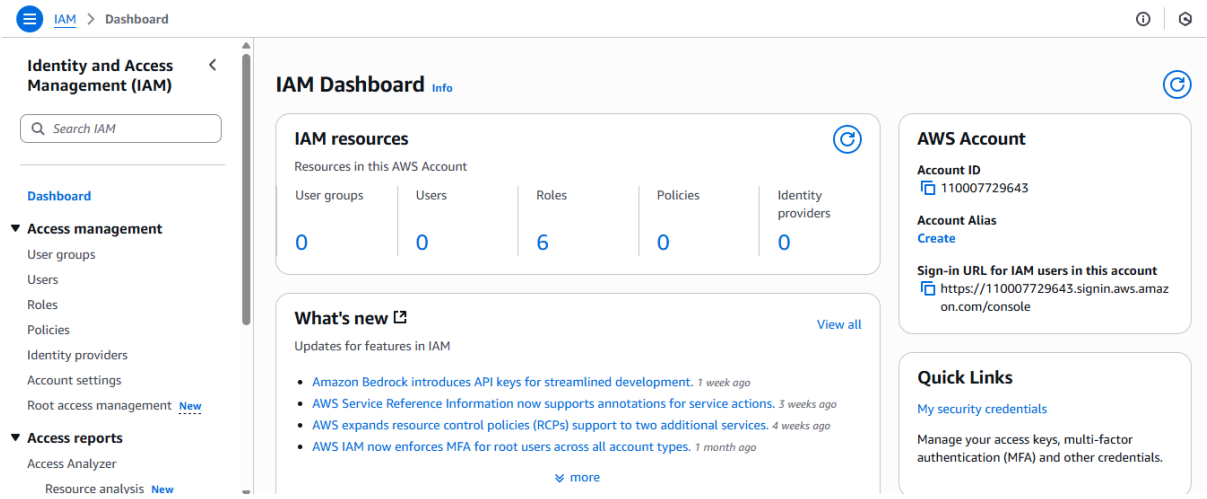
Step by Step Instructions:

Step 1:

- Go to “AWS Management Console” and search “IAM”.



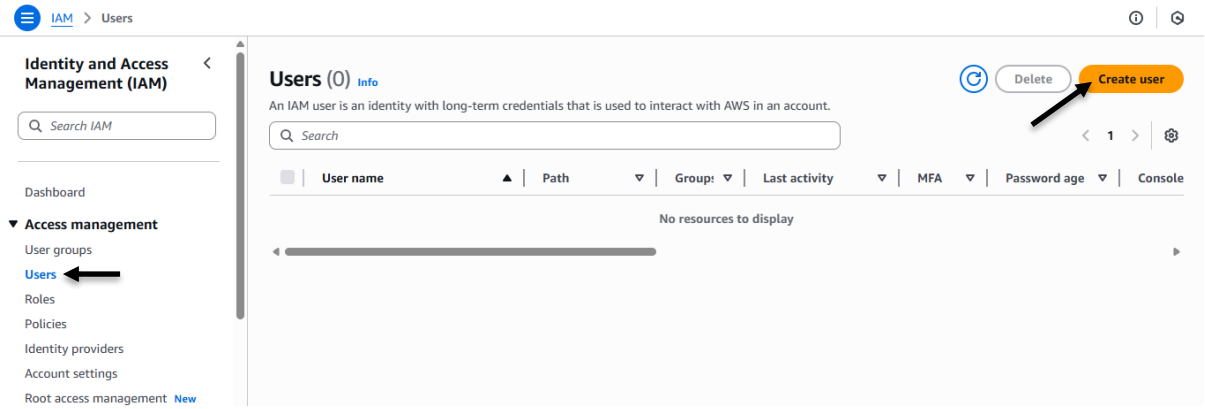
- The “IAM Dashboard” will open.



Creating users with the help of IAM:

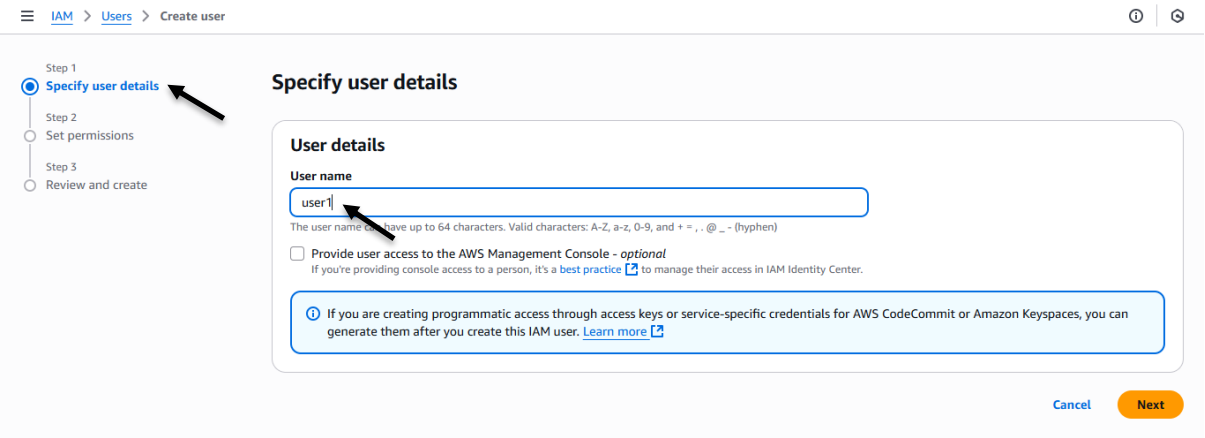
Step 2:

- On the left side under “Access management”, click on “Users”.
- Click on “Create user”.

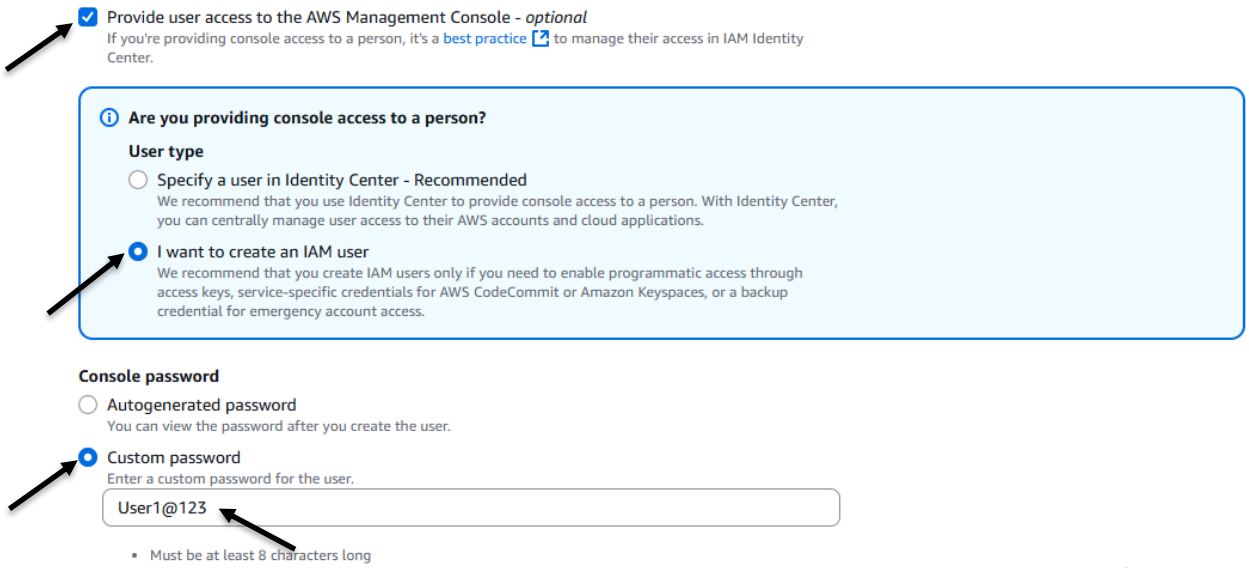


Step 3:

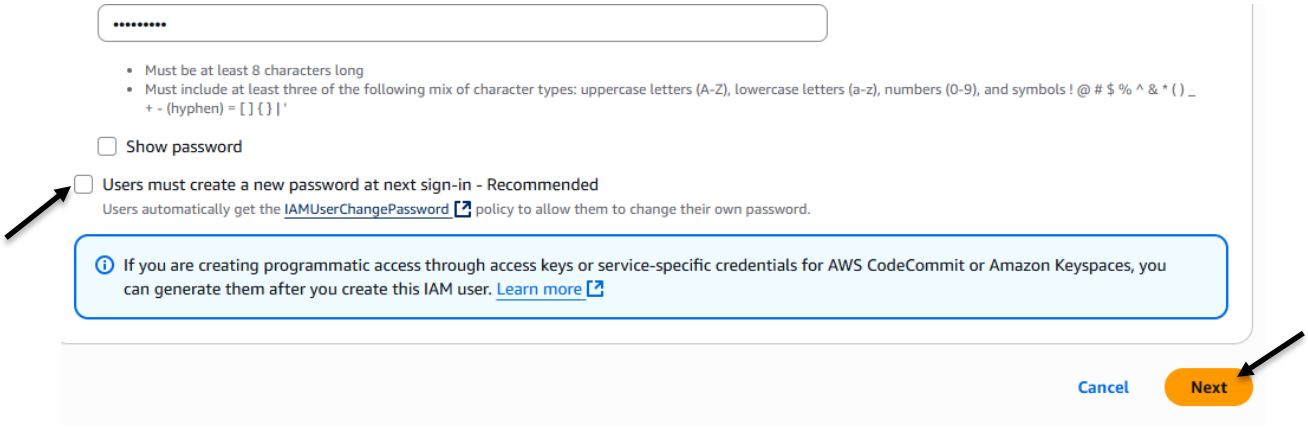
- In “Specify user details”, write the name of the user.



- Check the “Provide user access to the AWS Management Console” option.
- In “User type”, select “I want to create an IAM user”.
- In “Console password”, select “Custom password” and write a password for user1 (e.g. “User1@123”).

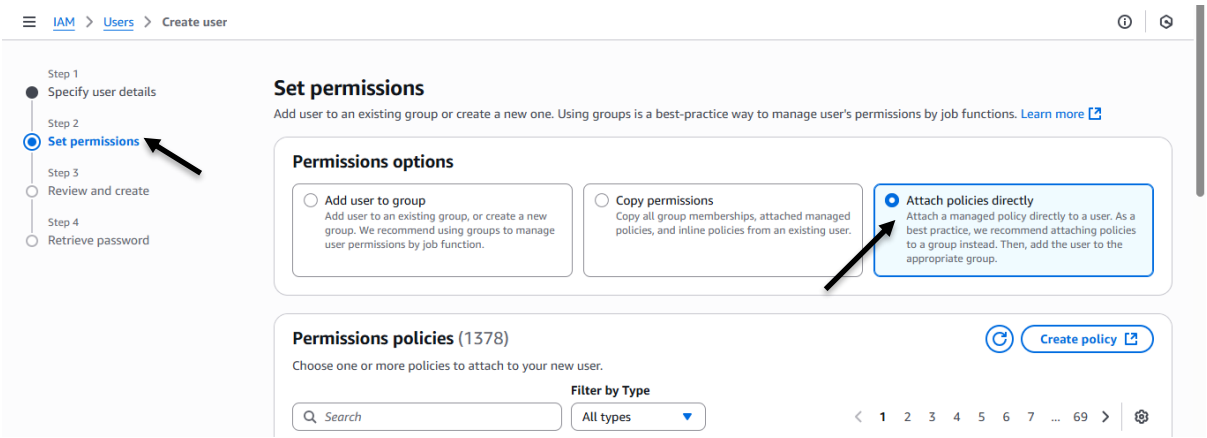


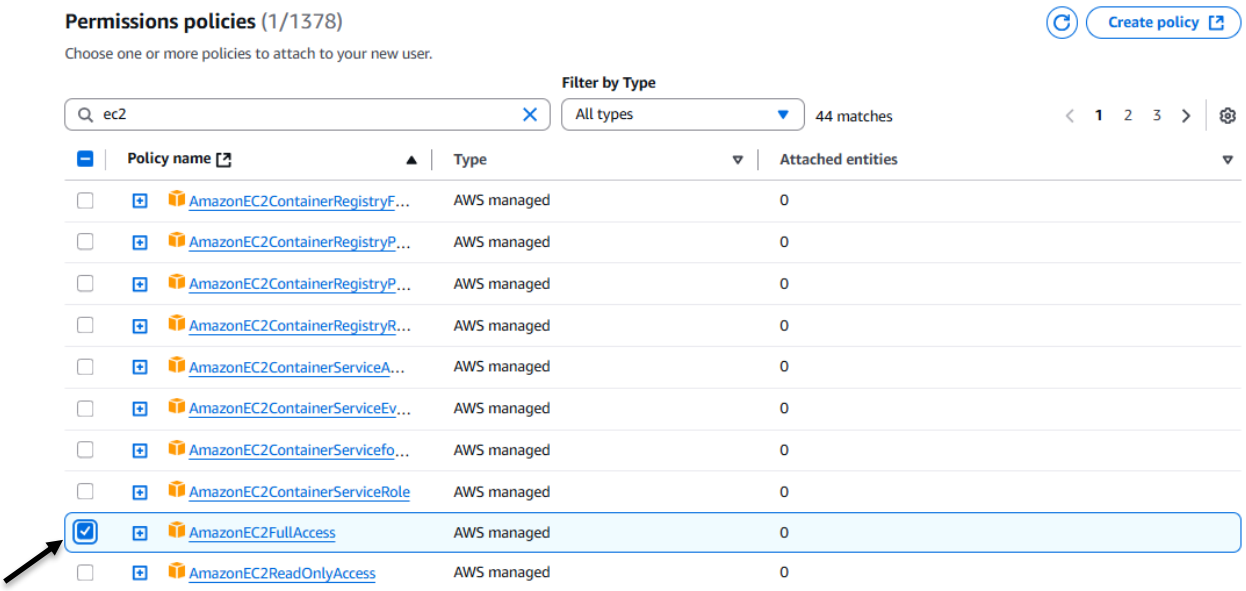
- Uncheck the option “Users must create a new password at next sign-in”.
- Click on “Next”.



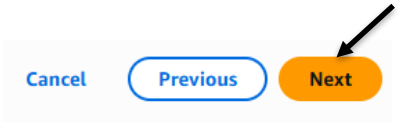
Step 4:

- In “Set permissions”, select “Attach policies directly” as “Permissions options”.
- Now select the “Permissions policies” that you want to add.



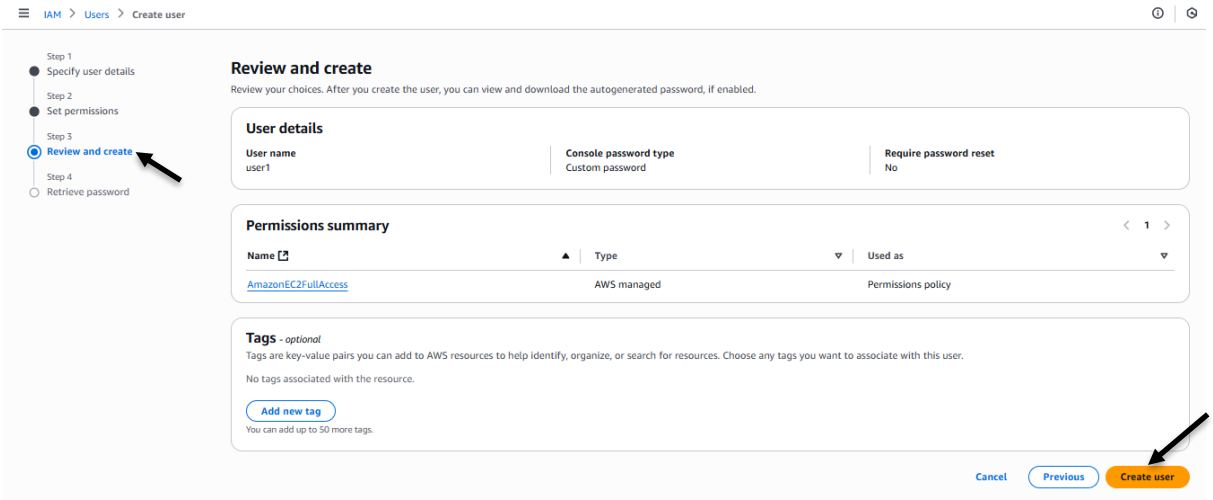


- Suppose I want to give EC2 full access to user1 so, I checked the option "AmazonEC2FullAccess".
- Similarly, you can give other permissions also.
- Click on "Next".

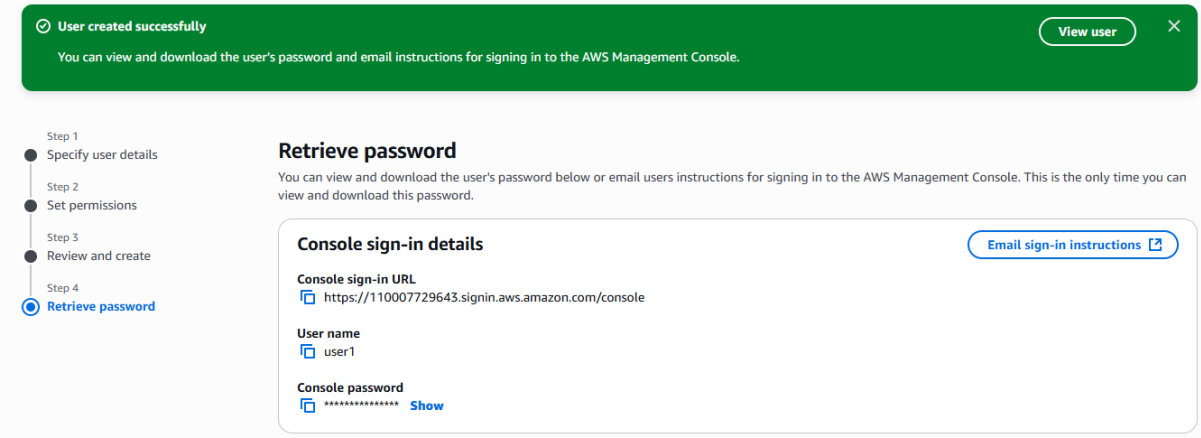


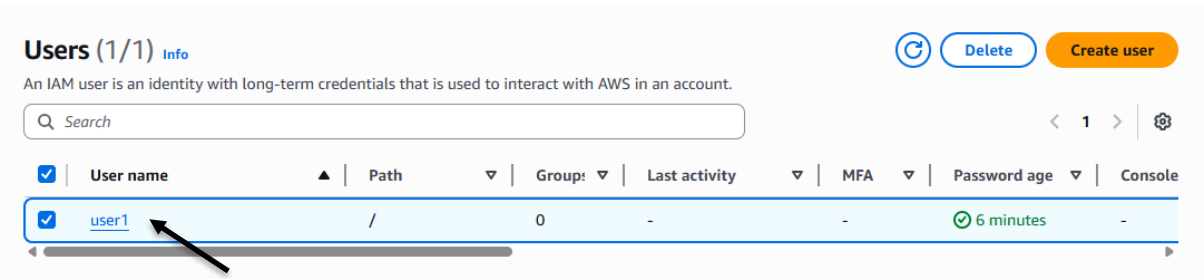
Step 5:

- Now review all the options and click on "Create user".



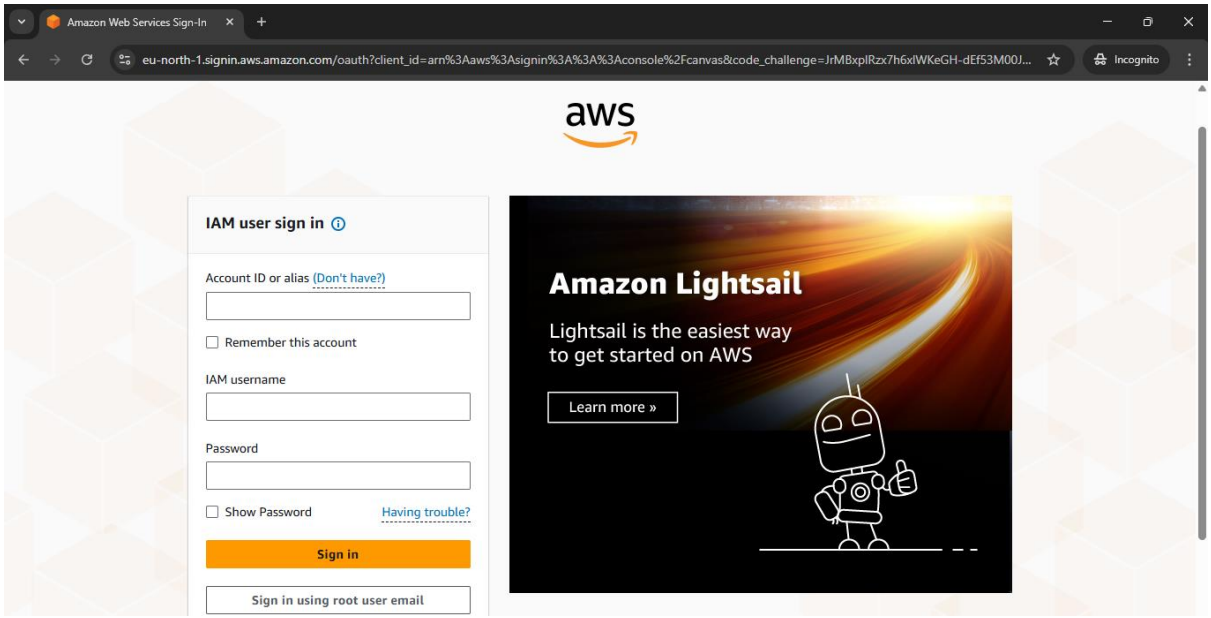
- User is created.
- You can retrieve the password.



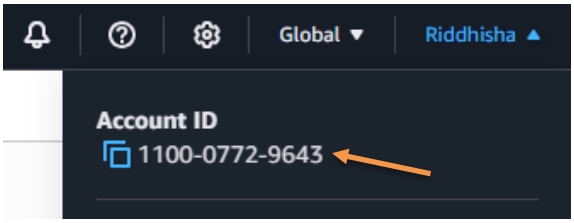


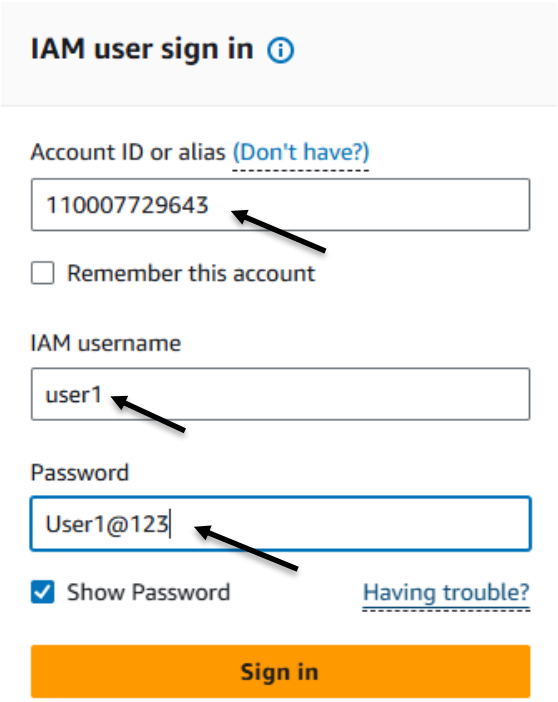
Step 6:

- Now go to another browser or incognito tab and open “AWS Management Console”.

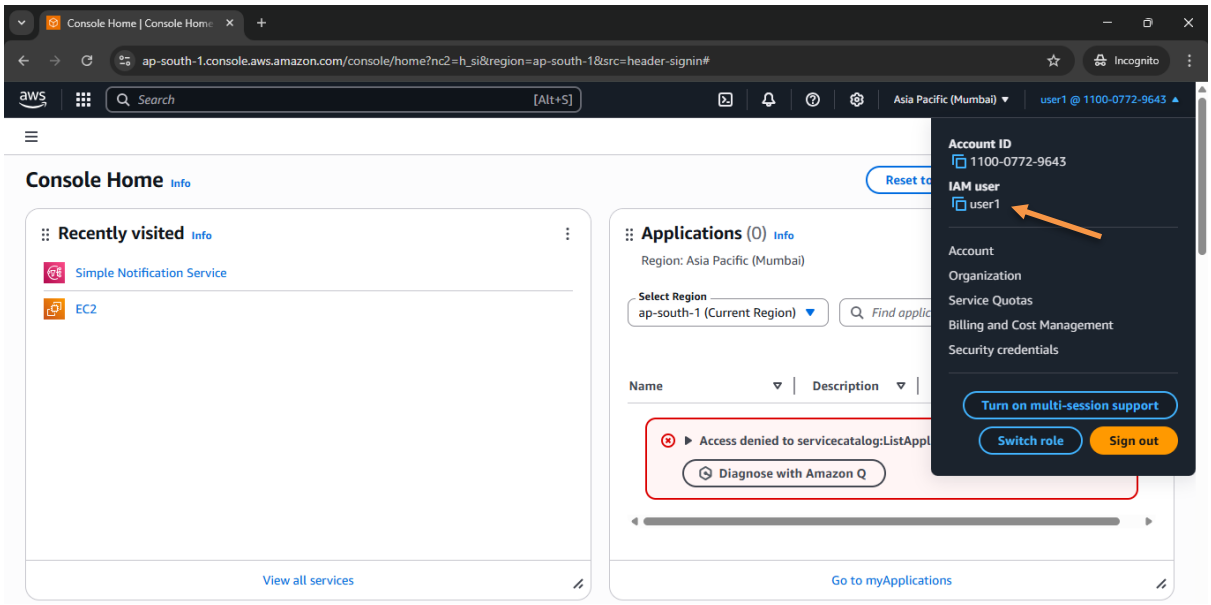


- Enter your root account ID in “Account ID or alias” box.



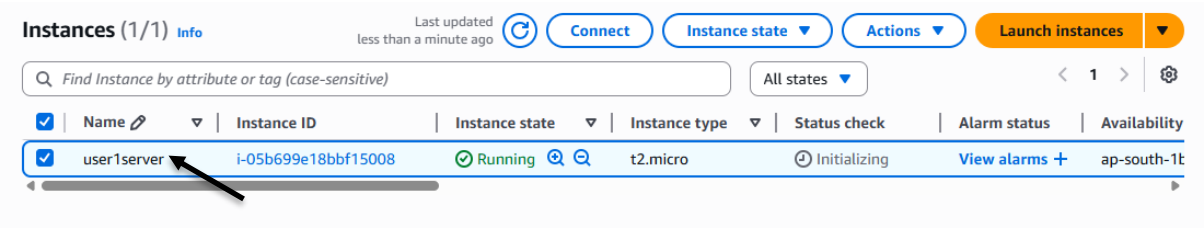


- Enter the “IAM username” that you have created i.e. “user1”.
- Enter the password and click on “Sign in”.
- Now “user1” is signed in to the root user account.

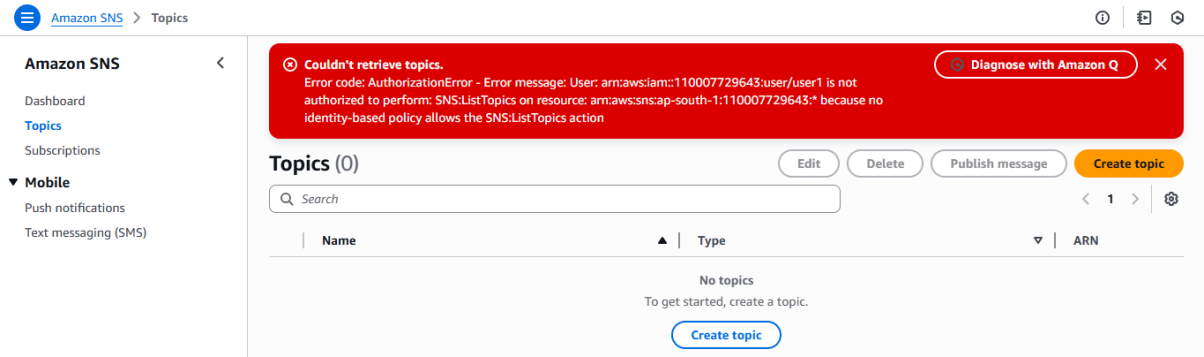


Step 7:

- “user1” can easily access all the properties of EC2.
- But it cannot access other options.
- For example, “user1” can easily launch an instance, create a volume, snapshots, and all other things that comes under EC2.



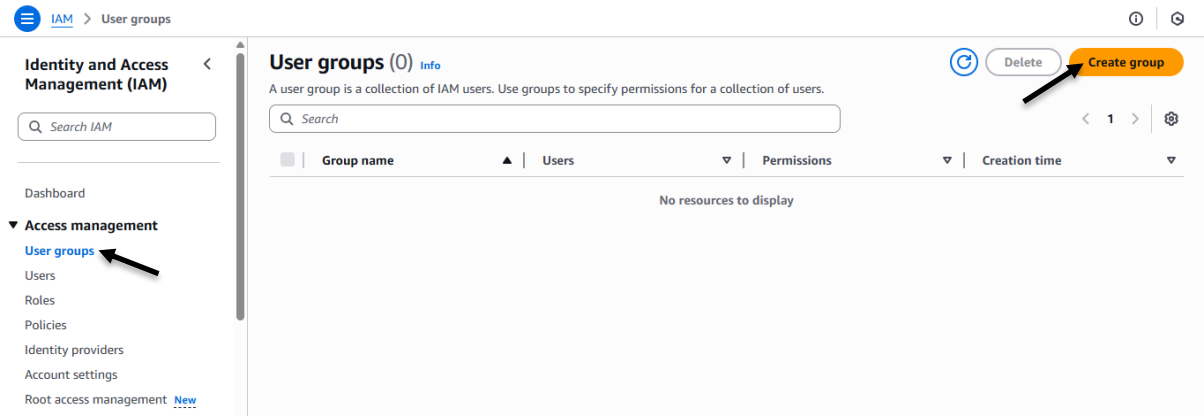
- But if “user1” tries to create a topic in SNS, he/she will be unable to do so.



Creating user groups:

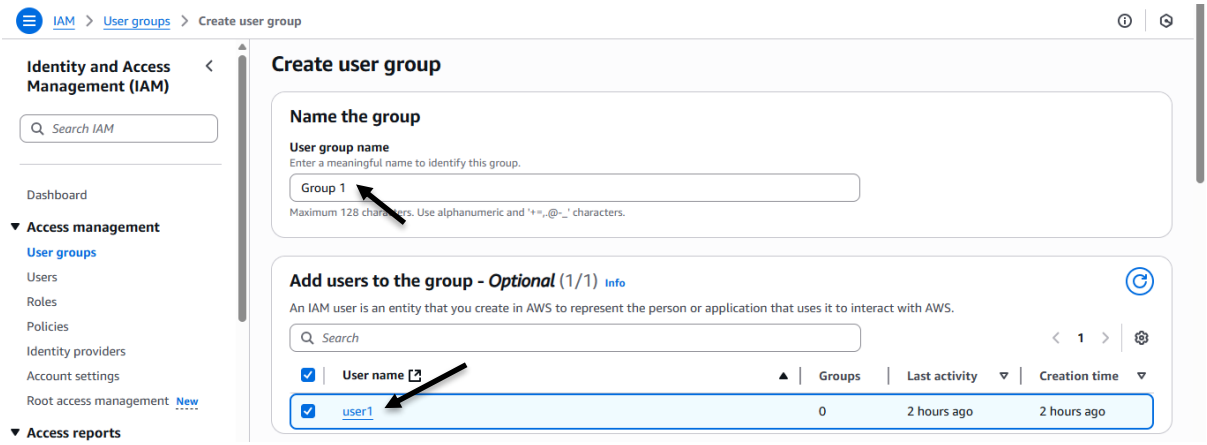
Step 8:

- In “Access management”, go to “User groups” and click on “Create group”.

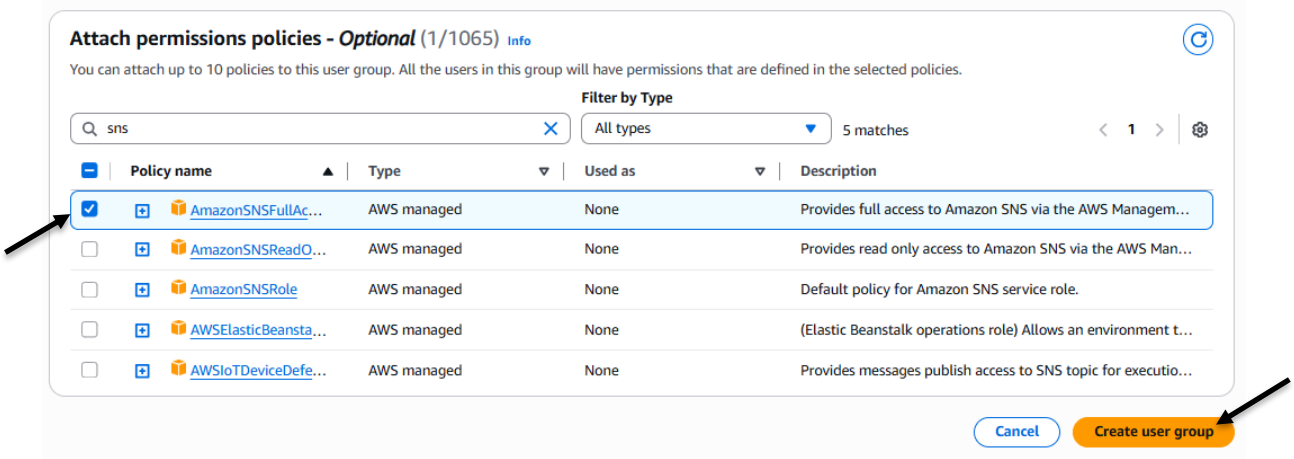


Step 9:

- Write the “User group name”.
- Select the users whom you want to add to the group.
- For now, we will add user1 to “Group 1”.

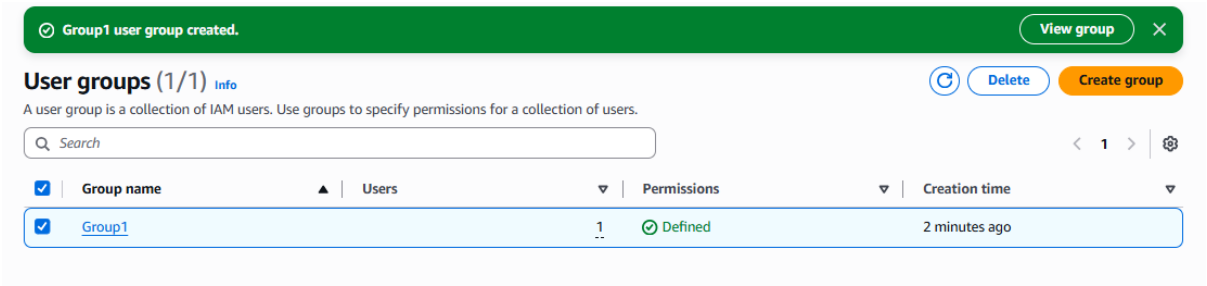


- Attach permission policies to the group as per your choice.
- For example, I have added “AmazonSNSFullAccess”.
- Click on “Create user group”.



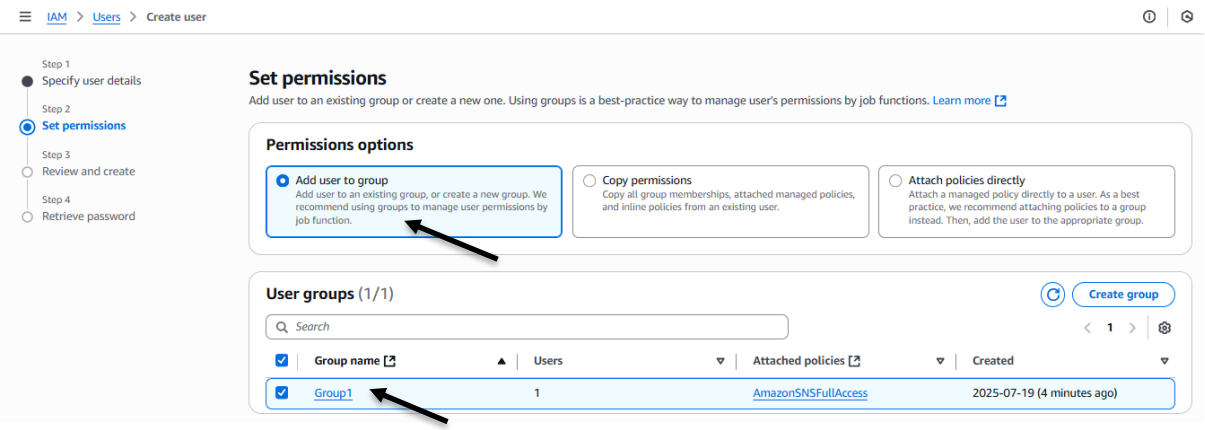
Step 10:

- User group “Group1” is created successfully.

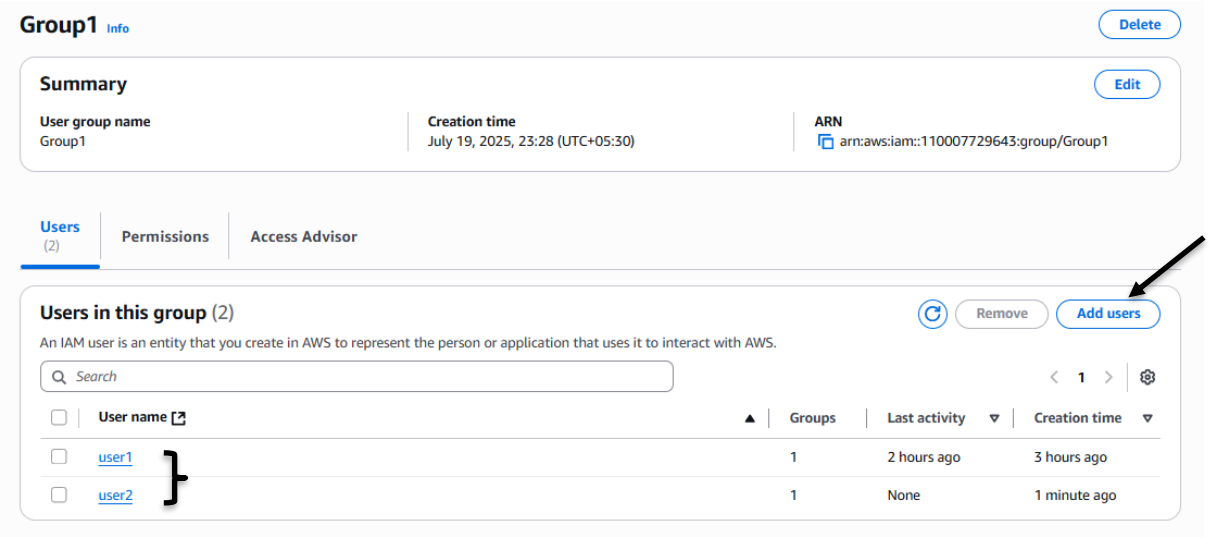


Step 11:

- Similarly, if we create another user (e.g. “user2”), under “Set permissions”, we can directly add the user to the group we just created.
- Select “Add user to group”.
- Select “Group1”.



- Now we can see that “Group1” has two users.
- We can add more users by clicking on “Add users”.

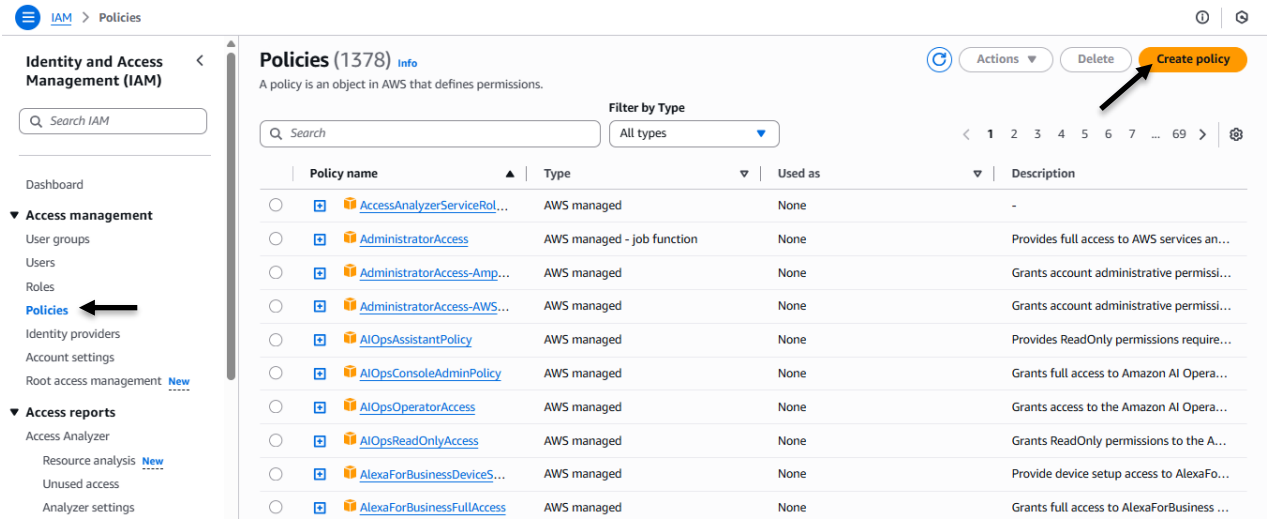


- The users in Group1 have only one permission – “AmazonSNSFullAccess”.
- They cannot access other features except SNS.

Creating policies:

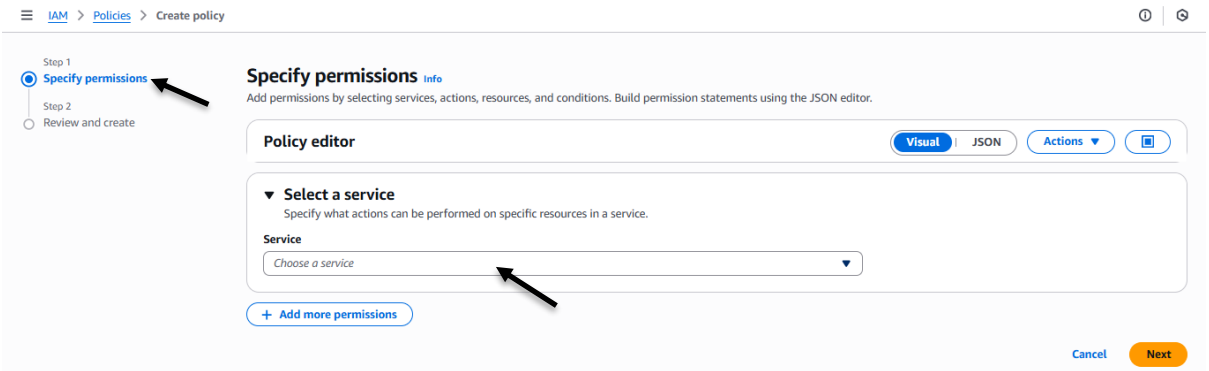
Step 12:

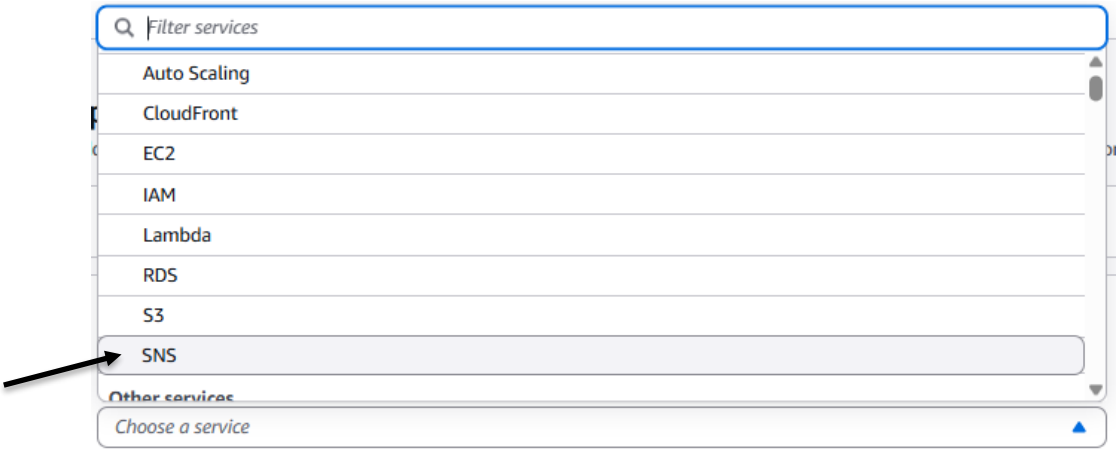
- In “Access management”, go to “Policies”.
- There are already 1378 policies present.
- We can create and add more policies as per our choice.
- Click on “Create policy”.



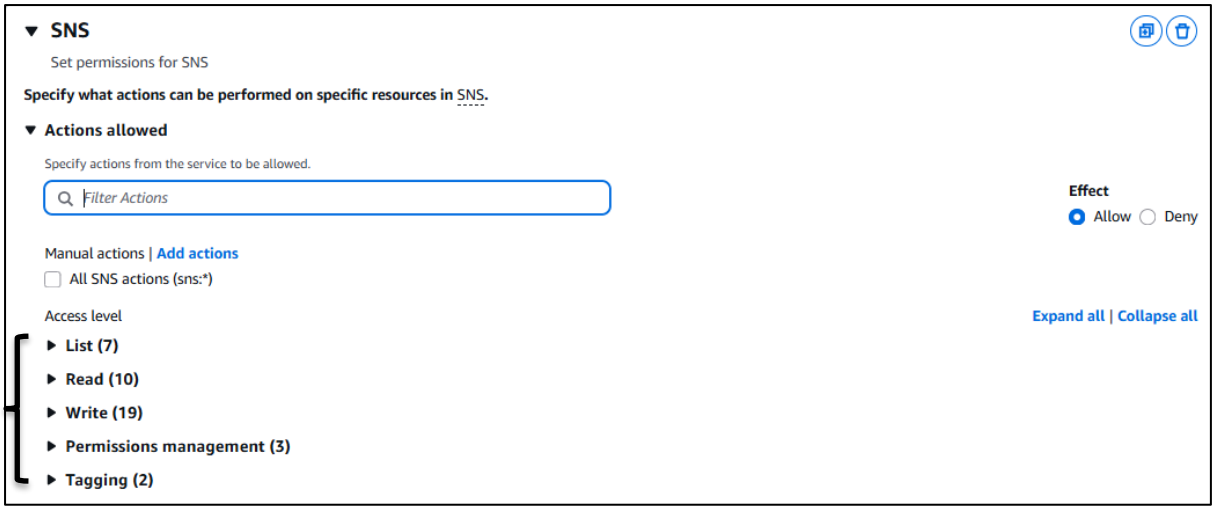
Step 13:

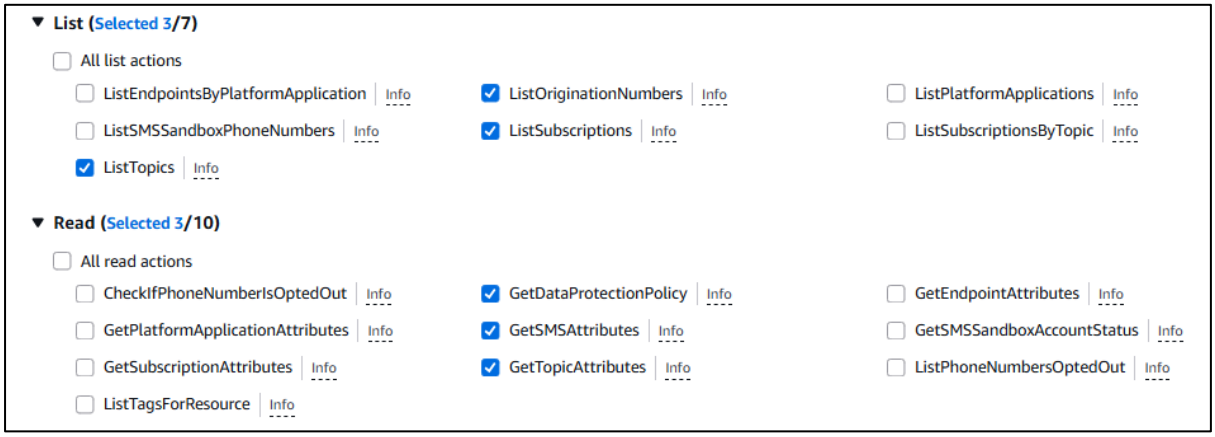
- Now select a service under “Specify permissions”.
- Select “SNS”.

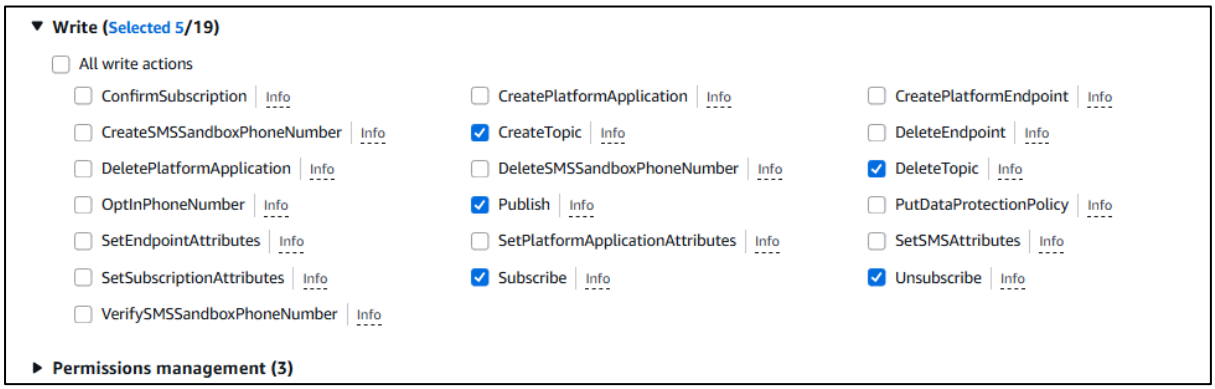




- Under “Actions allowed”, select all the permissions that you want to add to your policy.
- Select from “List (7)”, “Read (10)”, “Write (19)”, “Permissions management (3)” and “Tagging (2)”.



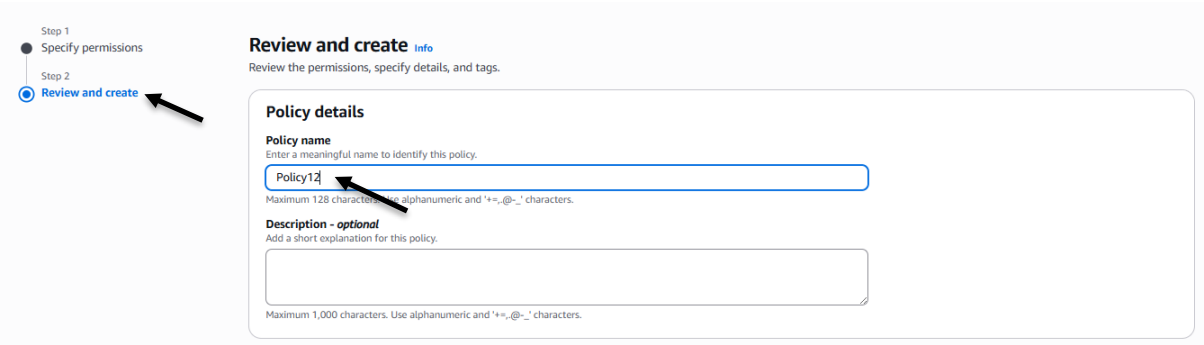


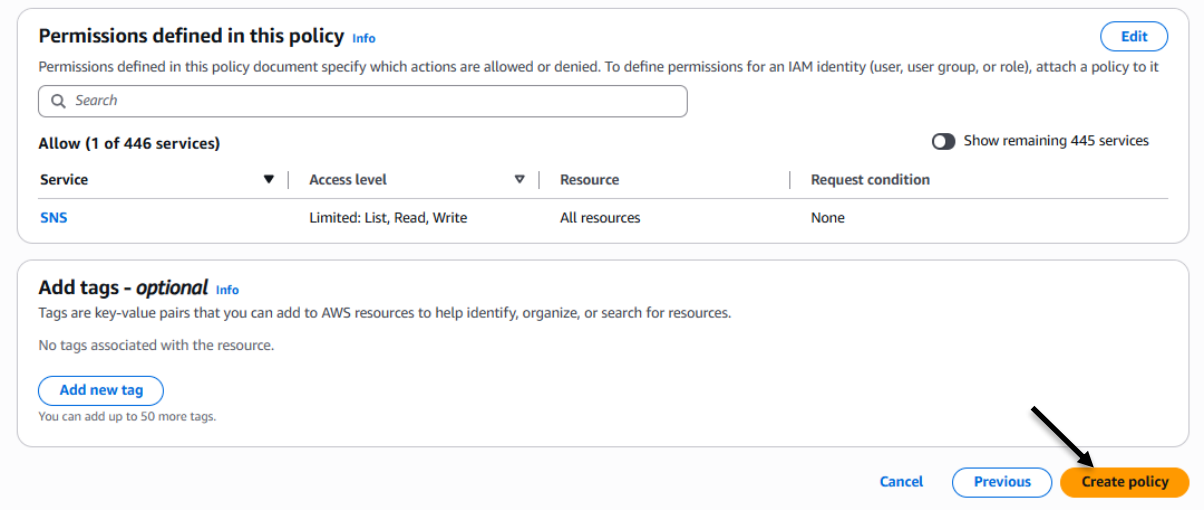


- Click on “Next”.

Step 14:

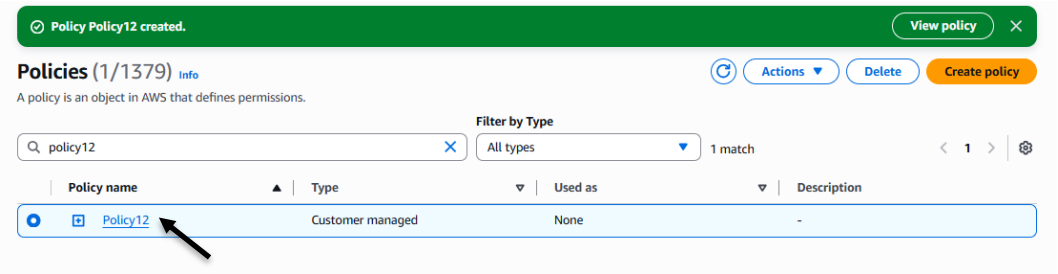
- In “Review and create”, give a unique name to your policy (e.g. “Policy12”).
- Leave rest other options as it is.
- Click on “Create policy”.



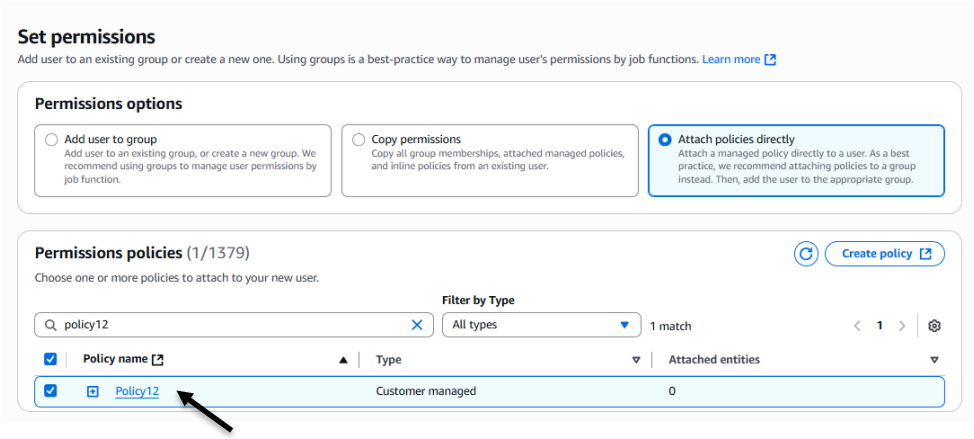


Step 15:

- The policy is created.



- Now we can use this policy the next time we create a new user.

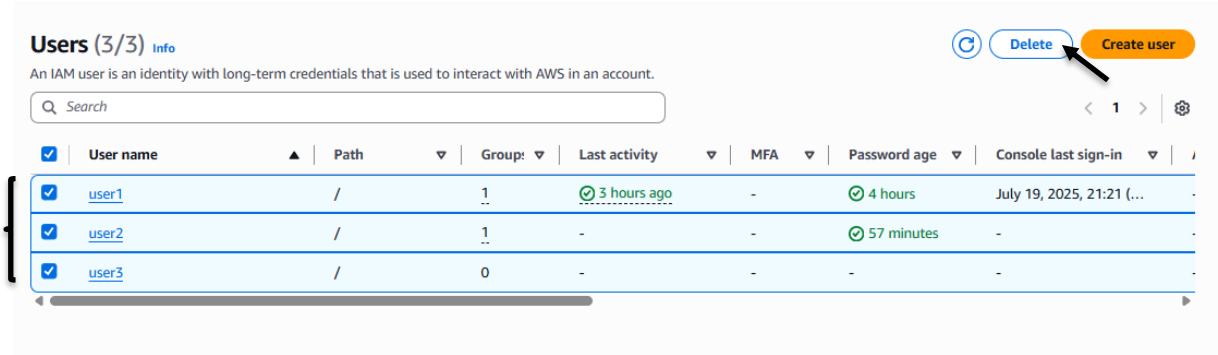


- These policies define what permissions a user have and what actions they can perform.

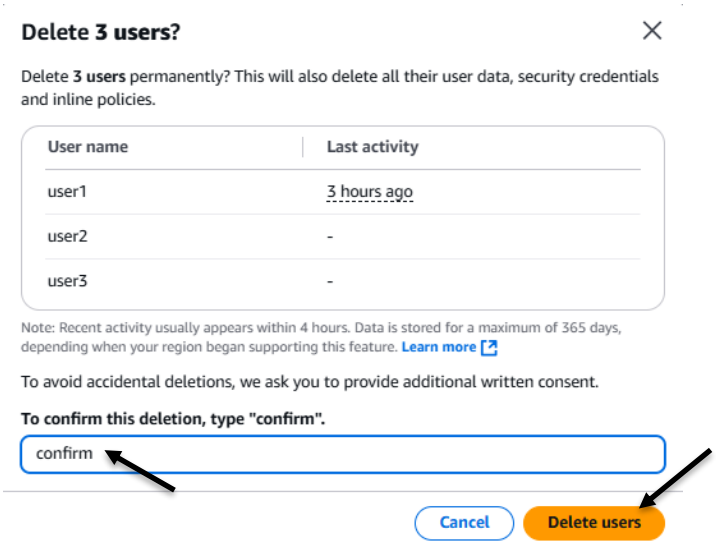
Delete a user:

Step 16:

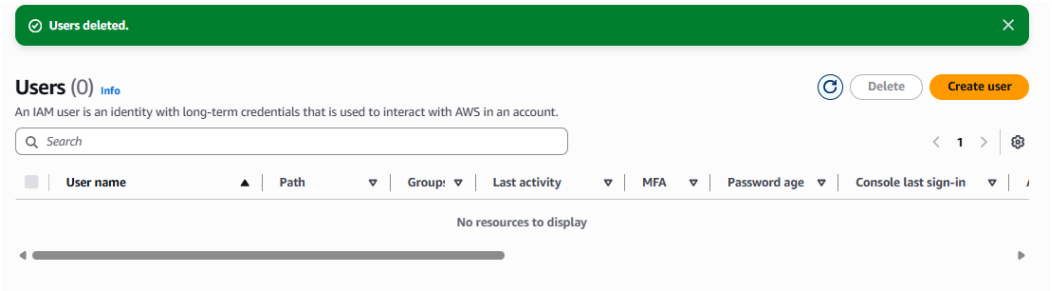
- In “Users”, select all the users that you want to delete.
- Click on “Delete”.



- Type “confirm” and click on “Delete users”.



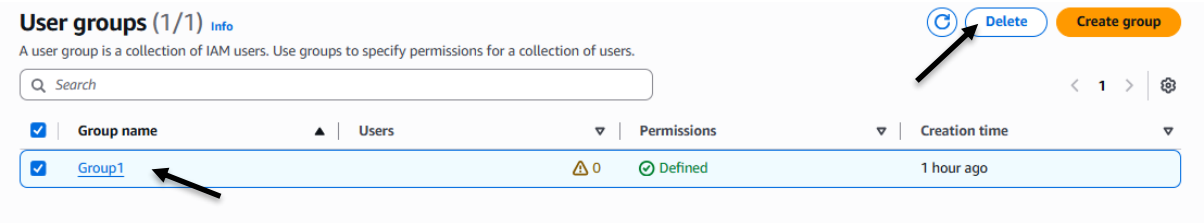
- The users are deleted.



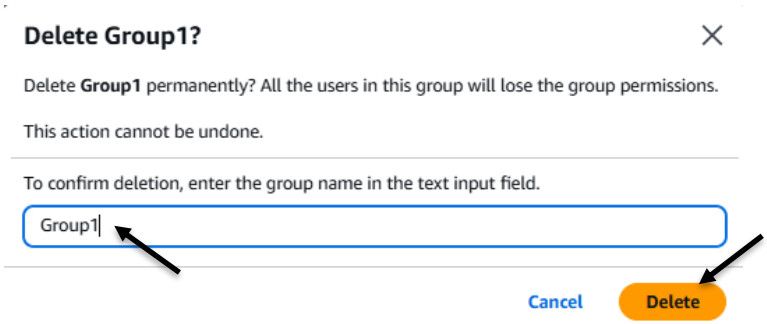
Delete user groups:

Step 17:

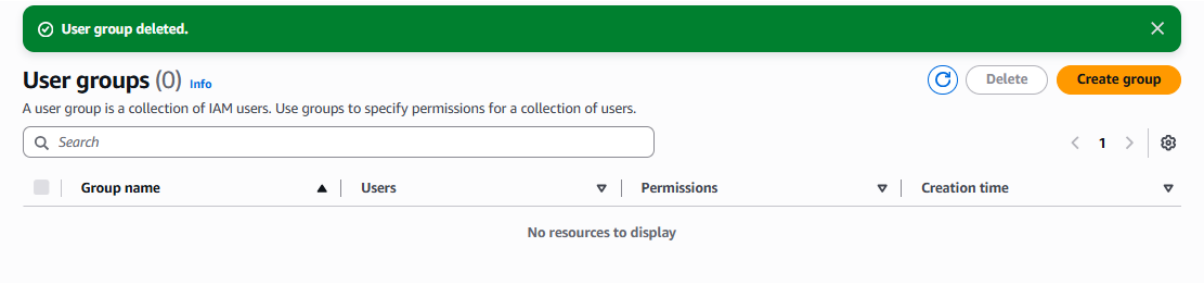
- In “User groups”, select the group that you want to delete.
- Click on “Delete”.



- Type “Group1” and click on “Delete”.



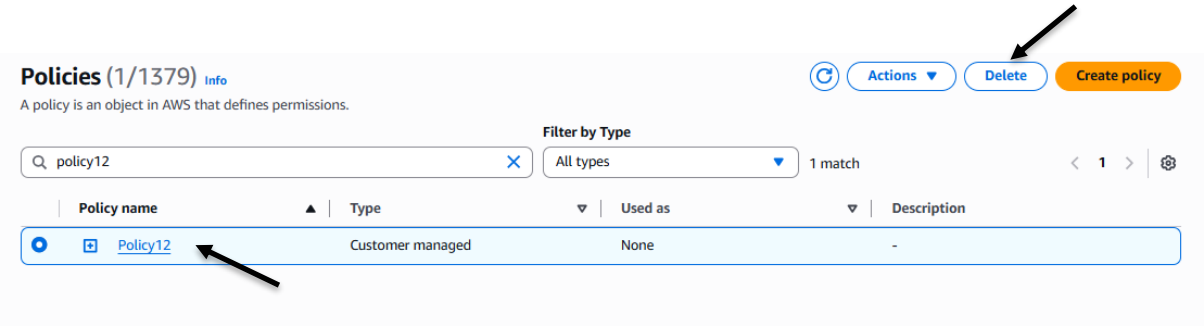
- The user group is also deleted.



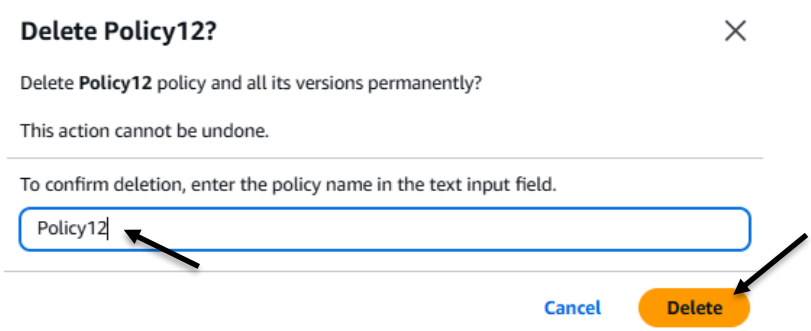
Delete a policy:

Step 18:

- Go to “Policies” and search the policy you created.
- Select your policy and click on “Delete”.
- It doesn’t matter even if your policy is not deleted.



- Type “Policy12” and click on “Delete”.



- The policy is deleted.