**Module-3: Case Study**

**Problem Statement**

You work for XYZ Corporation that uses on premise solutions and a limited number of systems. With the increase in requests in their application, the load also increases. So, to handle the load the corporation had to buy more systems almost on a regular basis. Realizing the need to cut down the expense on systems, they decided to move their infrastructure to AWS.

**You now been asked for:**

1. **(a) –** Create a user account that can login to the console.

**(b) –** Create a group and make sure that the group can only launch and stop EC2 instances using that previously created account.

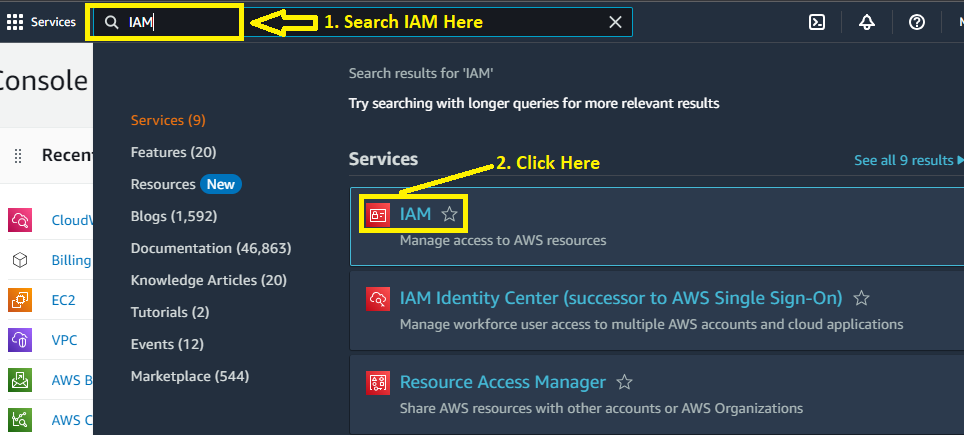
**2. (a) –** Provide permission to let the user of a previously created account to create VPC’s, Subnet, NACL & security groups.

**(b) –** Further add the permission so that the user can create a RDS instance.

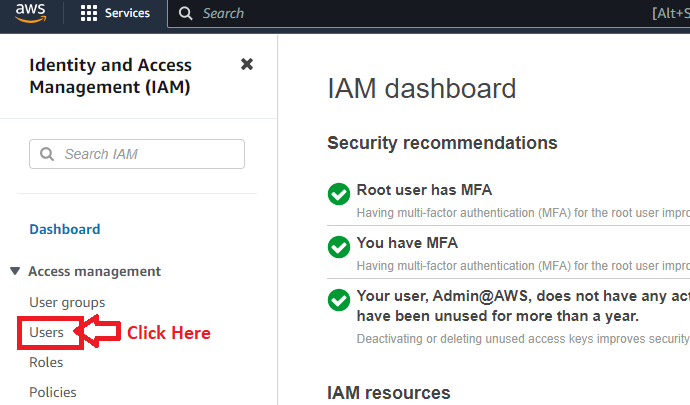
**(c) -** Explore security options to protect the AWS Resources and secure the permission provided to the group.

**Problem 1 (a) Solution:** Create a user account that can login to the console.

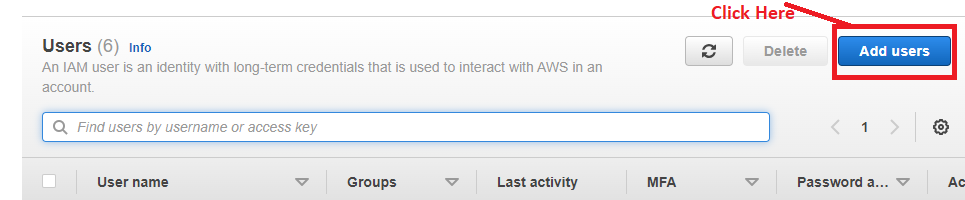
**a. Go** tothe **“Services>Search IAM>IAM”.**

****

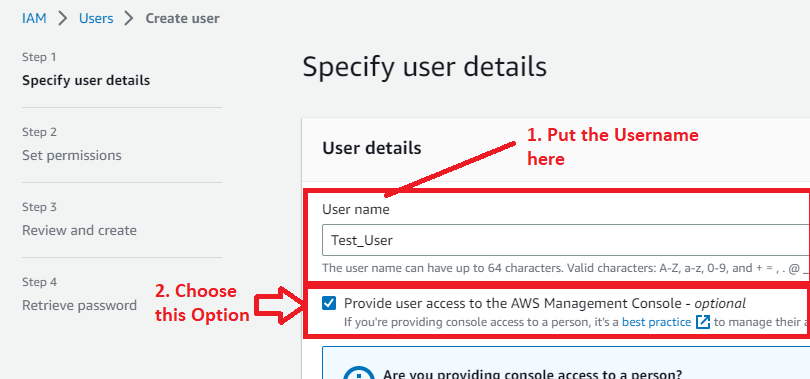
**b. Click** on the “**Users”**.



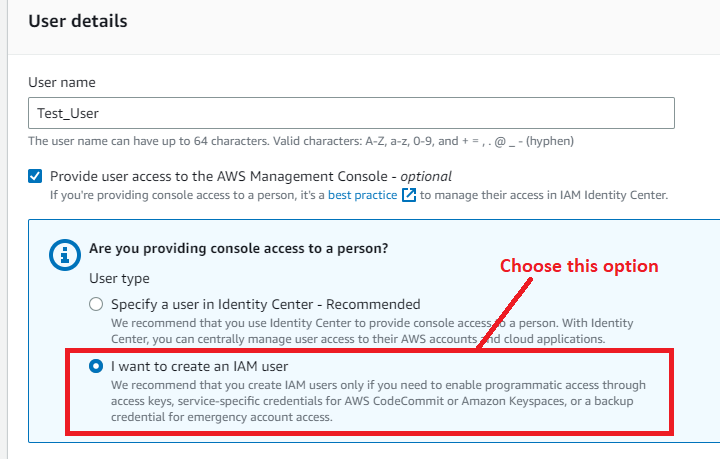
**c. Click** on the “**Add Users”**.



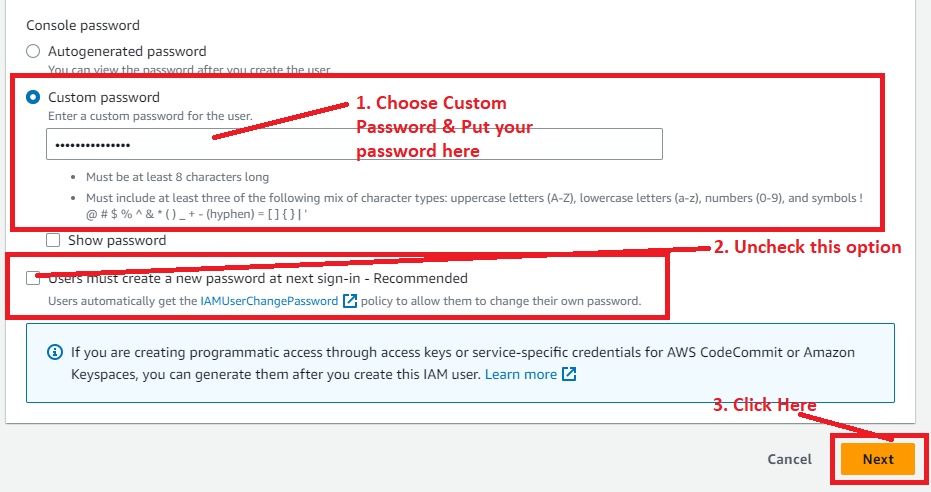
**d. Put** the **name** of the **user (Test\_User)** in **the “Username”** & **choose** the **“Provide User Access to the AWS Management Console- Optional”** option.

****

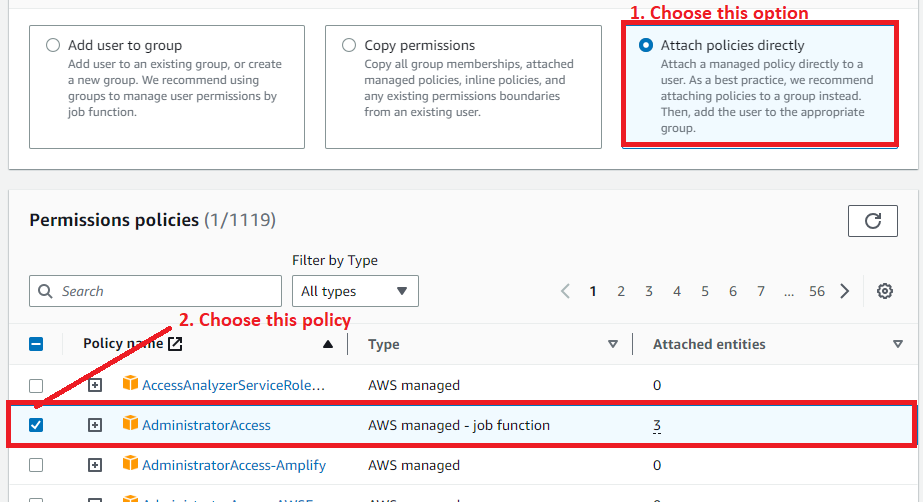
**e. Choose** the **“I want to create an IAM User”** option.

****

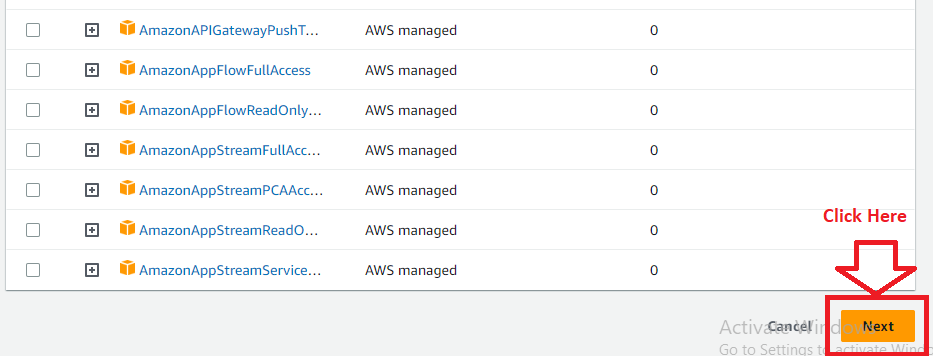
**f. Choose** the **“Console Password”** as **“Custom password”** & **Put** your **password** here**. Uncheck** or **disable** the **“Users must create a new password at next sign-in-Recommended”. Click** on the **“Next”.**

****

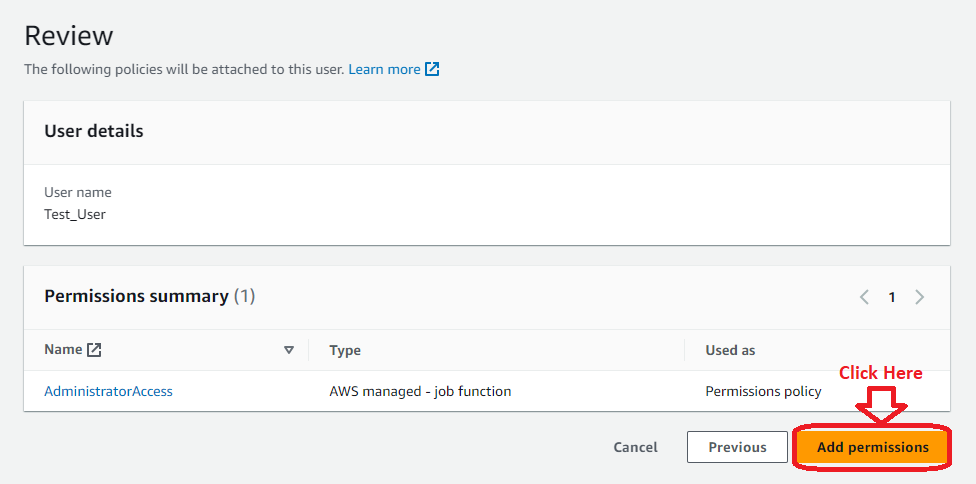
**g. In** the **“Add Permissions”, Choose** the **“Attach policies directly”** &the **“AdministratorAccess”.**

****

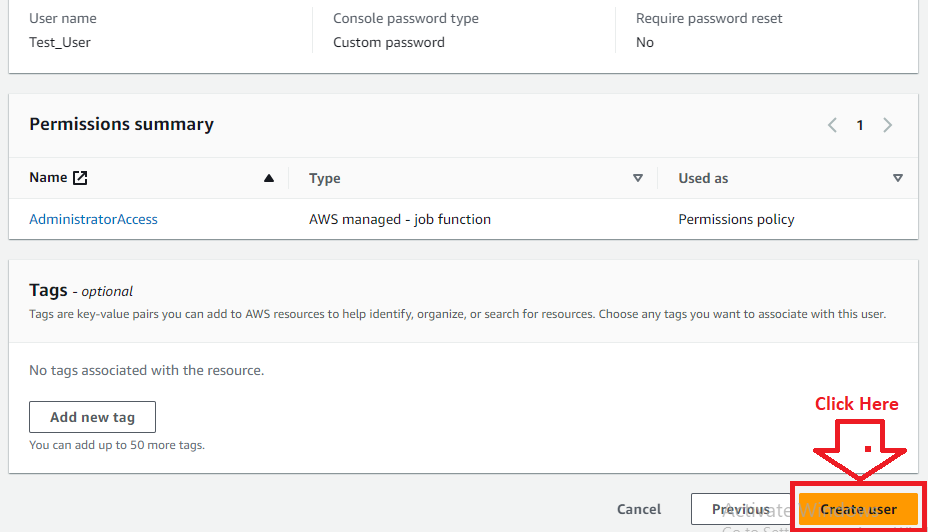
**h. Click** on the **“Next”** inthe **“Set permissions”.**

****

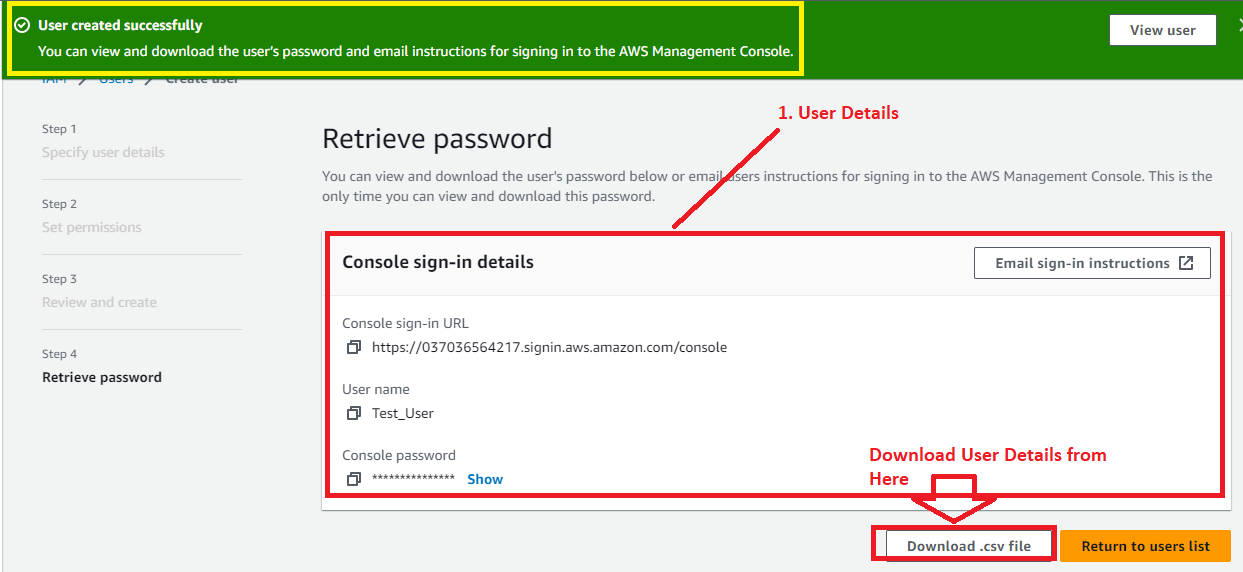
**h. Click** onthe **“Add Permissions”.**

****

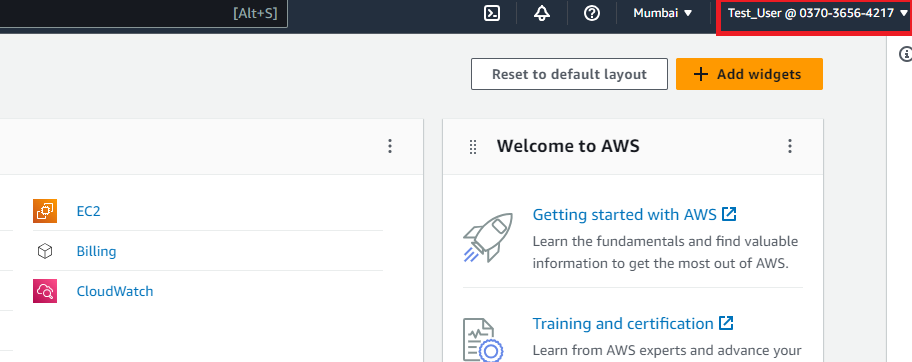
**i. Click** onthe **“Create User”** in the **“Review and create”.**

****

**j. The user** will be **created successfully. You** can **download** your **IAM User Sign-in URL, Username & Password** ina **.csv file** fromthe **“Download .csv file”.**

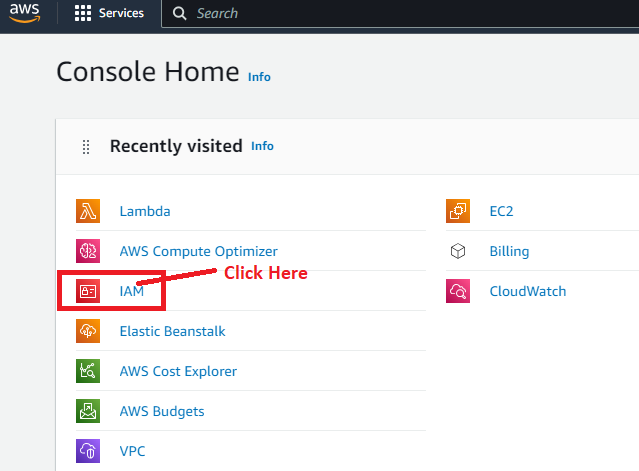
****

**k. Now, other user account (Test\_User)** has been **created successfully** & **Now, you** can **login** intoyour **Test\_User account** with **your** **username** & **password.**

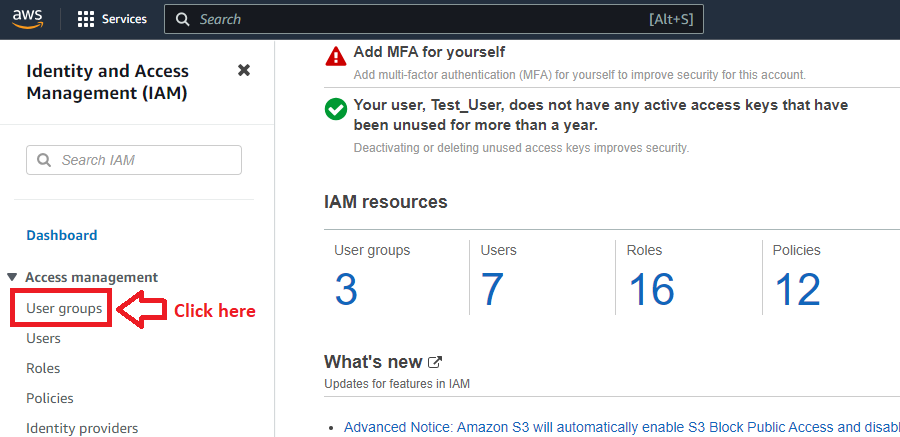
**You** can now **perform** any **activity** with this **user account** because **we** have **given** this **account** asthe **“Administrator access”.**

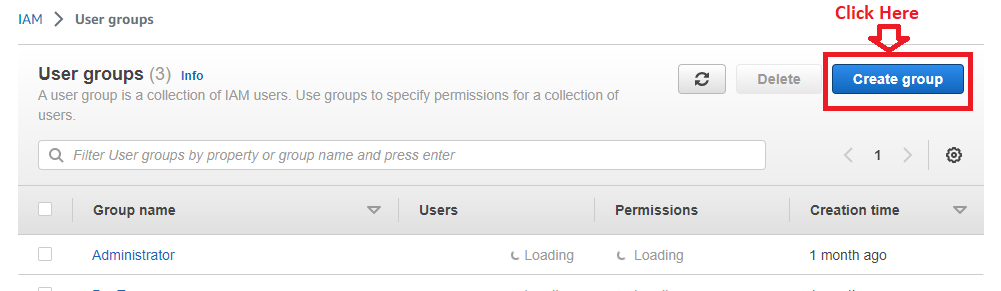
**Problem 1 (b) Solution:** Create a group and make sure that the group can only launch and stop EC2 instances using that previously created account.

**Step 1: Click** onthe **“IAM”** inthe **“Console Home”.**

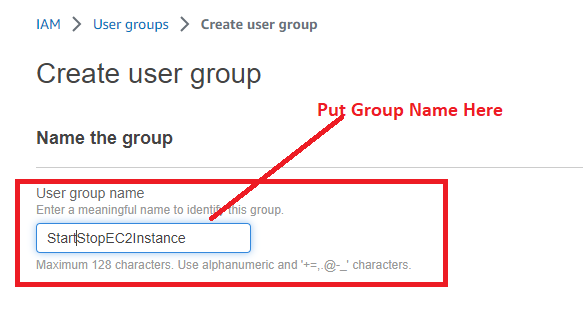
****

**Step 2: Go** tothe **“User groups”.**

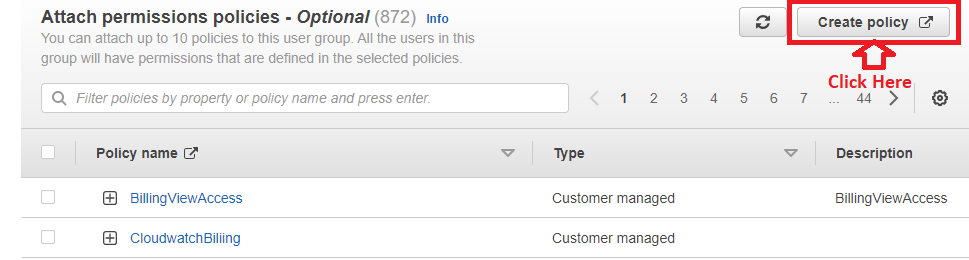
****

**Step 3: Click** onthe **“Create Group”.”**

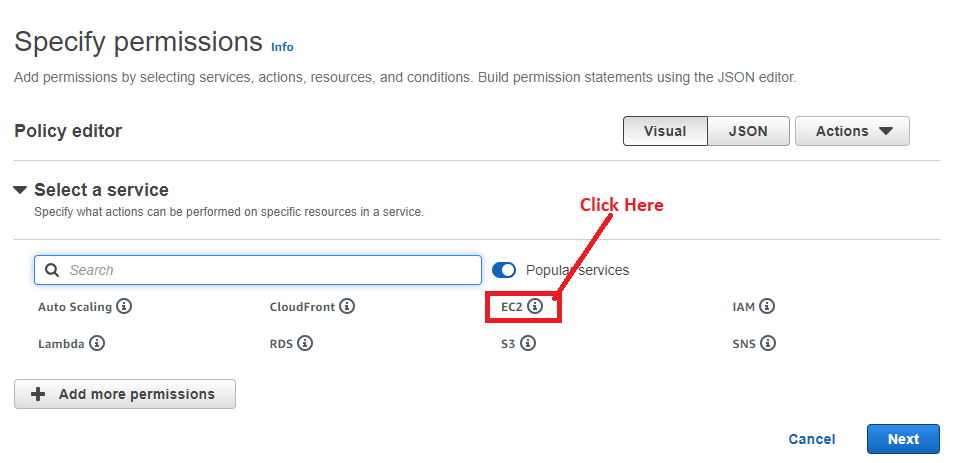
**Step 4: Put** the **“User group name”** as the **“StartStopEC2Instance”.**

****

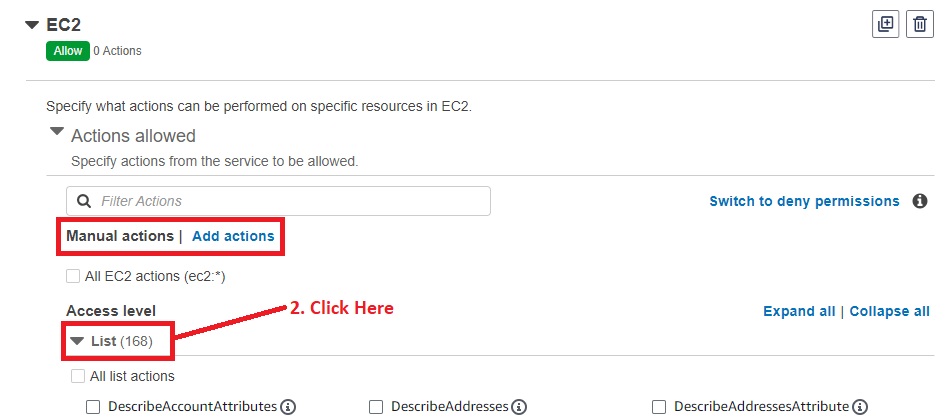
**Step 5: In** the **“Attach Permission Policies-Optional”, Click** on the **“Create Policy”.**

****

**Step 6: A separate tab** will be **opened** for **creating the policy. It** will **ask you** to **select a service** for **“creating the policy”. Click** on the **“EC2”.**

****

**Step 7: In** the **“Manual Actions”, click** on the **“List (168)”.**

****

**Choose** these **responsibilities** here;

1. DescribeAccountAttributes
2. DescribeAddresses
3. DescribeAddressesAttributes
4. DescribeImages
5. DescribeImageAttributes
6. DescribeAvailabilityZones
7. DescribeHosts
8. DescribeImages
9. DescribeInstances
10. DescribeInstanceAttribute
11. DescribeInstanceTypes
12. DescribeInstanceStatus
13. DescribeInstanceEventWindows
14. DescribeInternetGateways
15. DescribeLaunchTemplates
16. DescribeLaunchTemplateVersions
17. DescribeRouteTables
18. DescribeInstanceStatus
19. DescribeKeyPairs
20. DescribeSecurityGroups
21. DescribeSecurityGroupRules
22. DescribeVpc
23. Describe Subnets
24. DescribeVolumes
25. DescribeRegions
26. DescribeTags

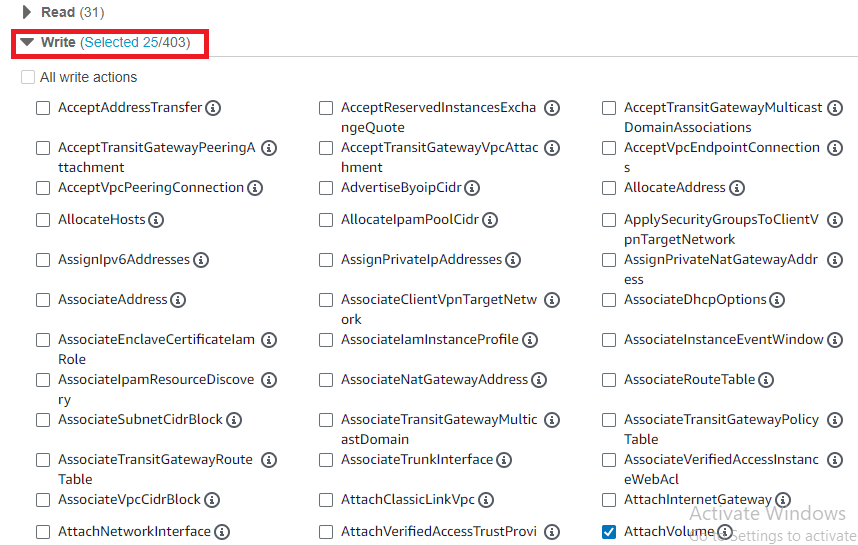
DescribeVolumeAttribute

DescribeVolumeStatus

DescribeVpcAttributes

DescribeVpcConnections

**Step 8: Go** to the **“Write (403)” & choose** the **write actions;**

****

1. CreateImage
2. CreateKeyPair
3. DeleteKeyPair
4. StartInstances
5. StopInstances
6. Run Instances
7. DeleteSnapshot
8. AttachVolume
9. CreateVolume
10. DeleteVolume
11. Detach Volume
12. CreateVpc
13. DeleteVpc
14. AuthorizeSecurityGroupEgress
15. AuthorizeSecurityGroupIngress
16. CreateDefaultVpc
17. CreateDefaultSubnet
18. CreateSecurityGroup
19. CreateSubnet
20. DeleteSecurityGroup
21. DeleteSubnet
22. AssociateRouteTables
23. CreateRouteTable
24. DeleteRouteTable
25. CreateRoute
26. DeleteRoute

RevokeSecurityGroupEgress

RevokeSecurityGroupIngress

AllocateHosts

Allocate Addresses

Copy Image

CreateSnapshots

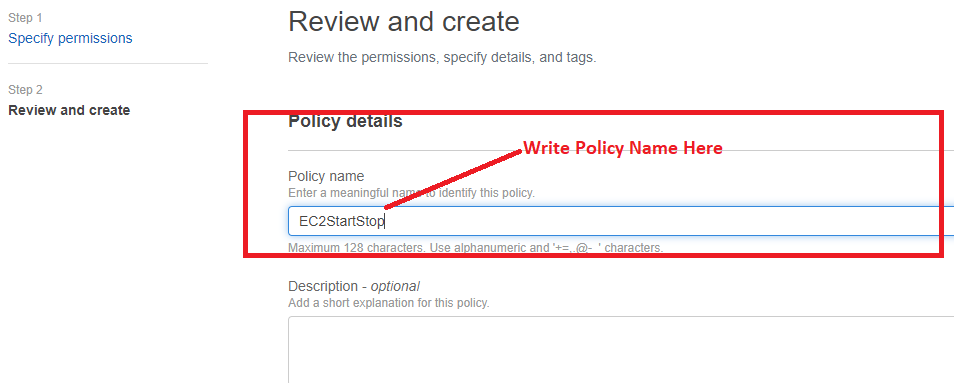
CreateSnapshot

**Step 9:** In the “**Tagging”**, choose the **“All Tagging Actions”.**

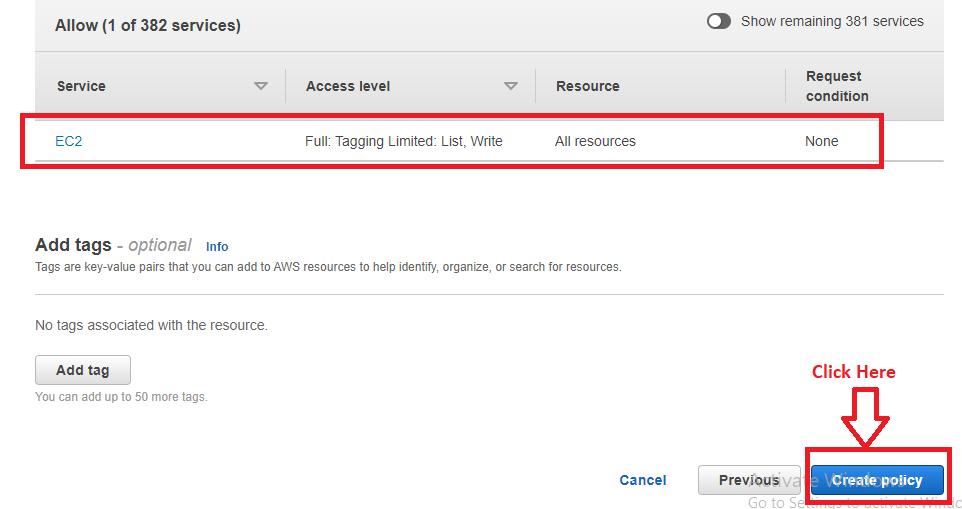


**Click** on the **“Next”.**

**Step 10: Choose** the **“Policy Name”** as **“EC2StartStop”.**

****

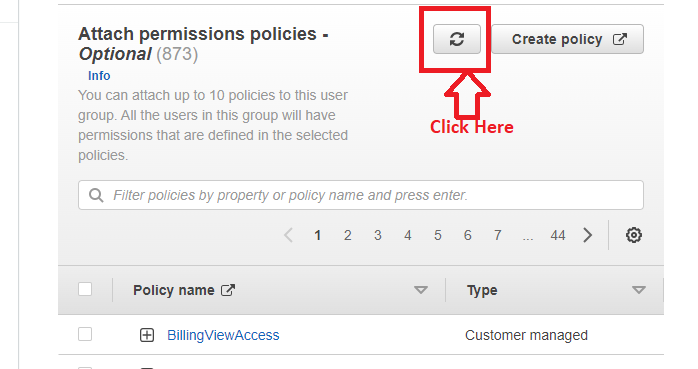
**Step 11: Click** onthe **“Create Policy”.**

****

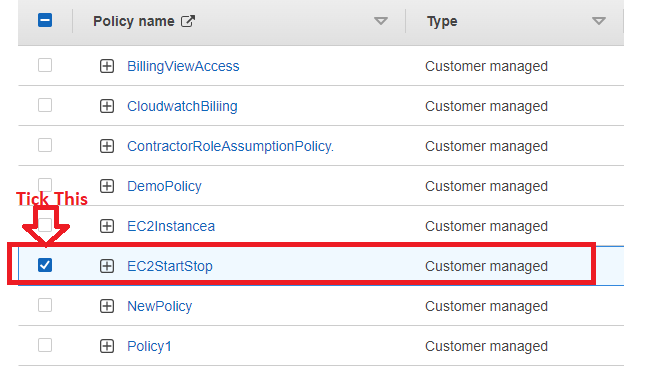
**Step 12: The policy (EC2StartStop)** will be **successfully created.**

****

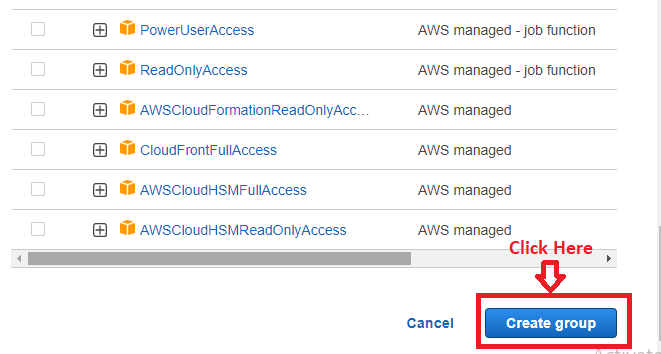
**Step 13: Now, go** tothe **“User Groups”** & **Click** on the **“Refresh”** in the **“Attach permission policies – Optional”.**

****

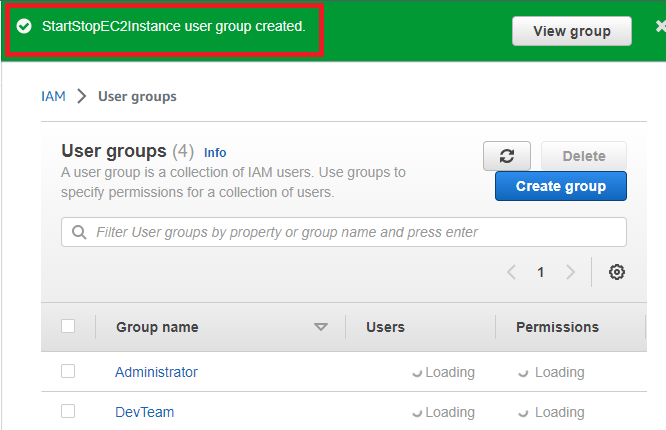
**Step 14: Choose** the **“EC2StartStop”** inthe **“Policy name”.**

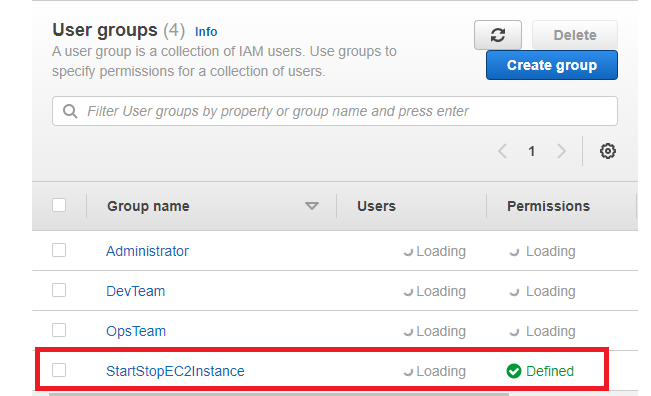
****

**Step 15: Click** on the **“Create group”.**

****

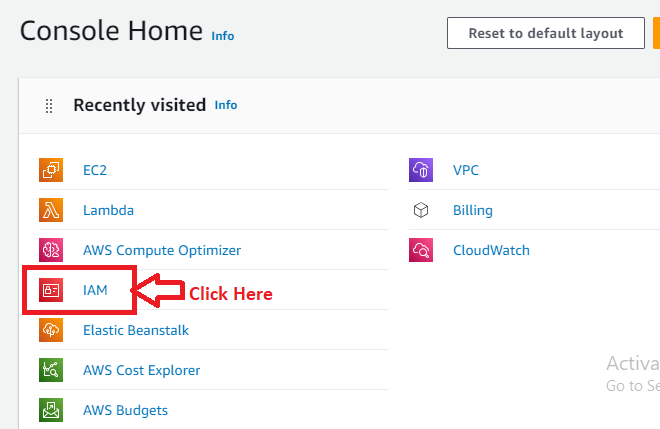
**Step 16: The “group (StartStopEC2Instance)”** will be **created successfully.**

****

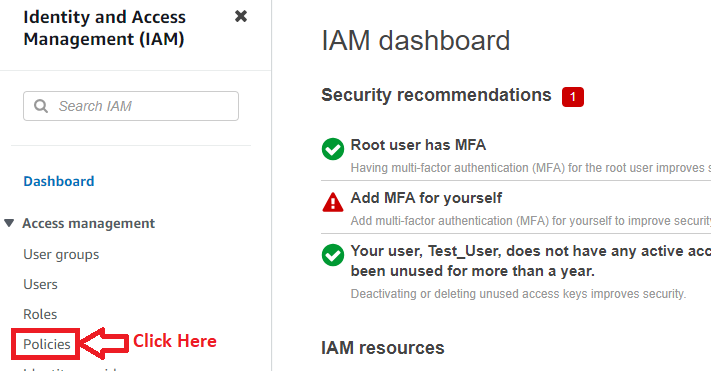
****

**Problem Solution 2 (a) -** Provide permission to let the user of a previously created account to create VPC’s, Subnet, NACL & security groups.

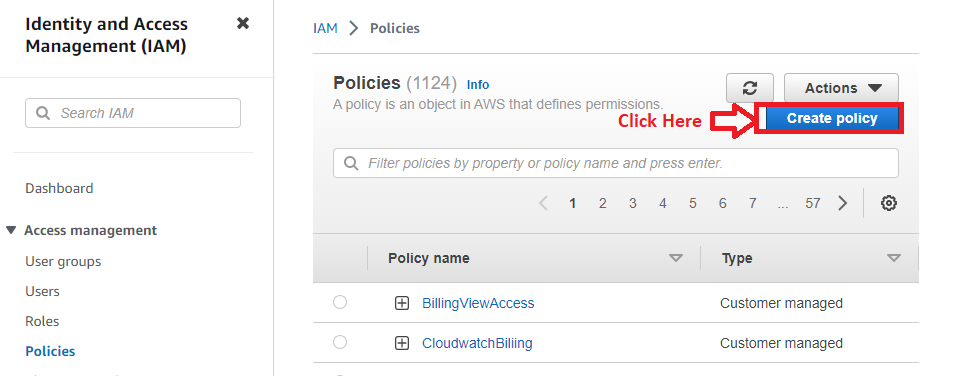
**Step 1: Go** tothe **“IAM”.**

****

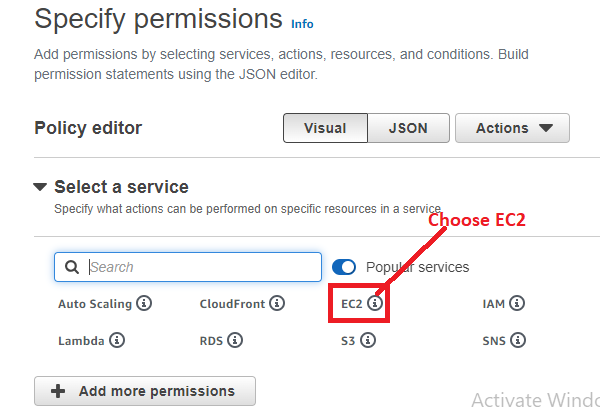
**Step 2: Go** to the **“Policies”.**

****

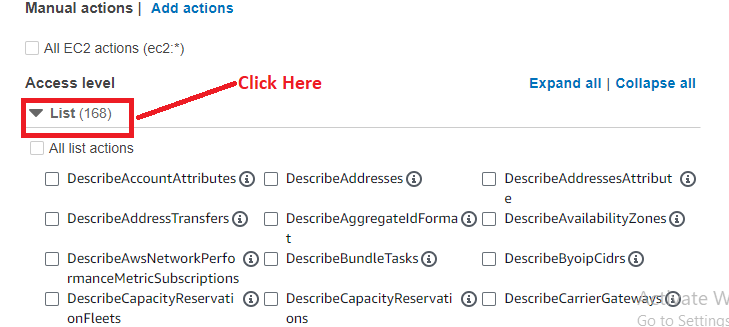
**Step 3: Click** on the **“Create Policy”.**

****

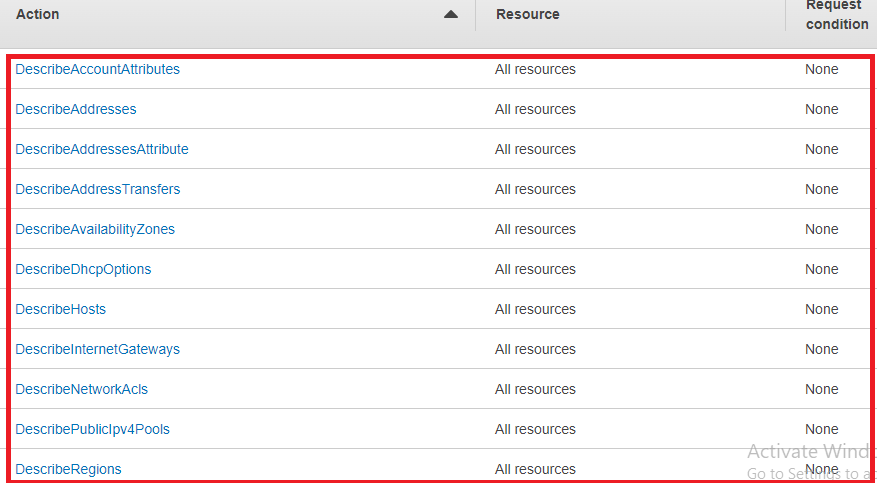
**Step 4: Choose** the **“EC2”.**

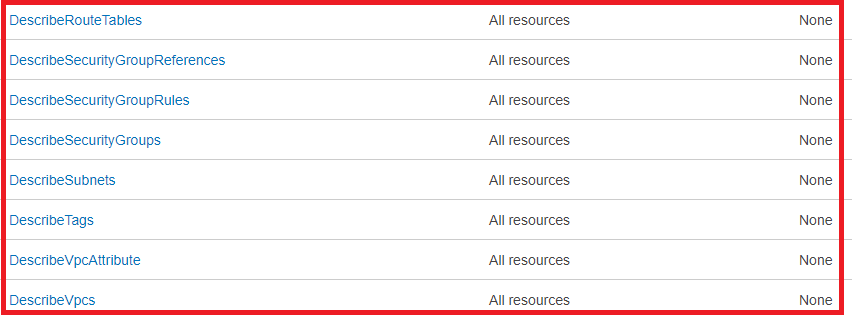
****

**Step 5: Click** to the **“List”.**

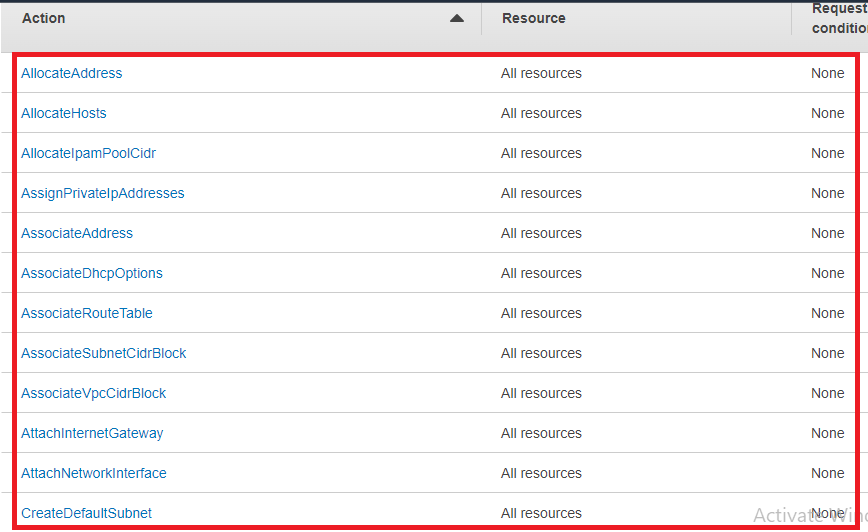
****

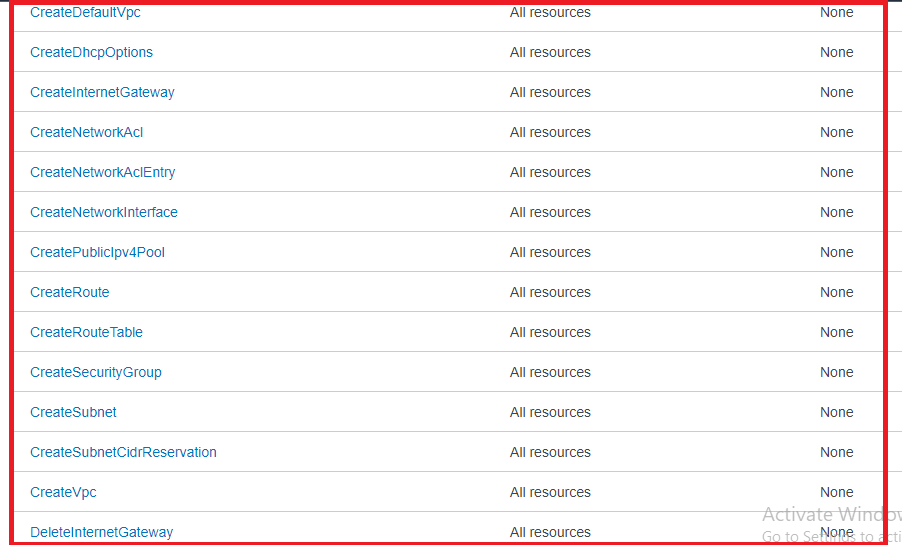
**Step 6: Choose** the **following actions** in the **“list” section:**

****

****

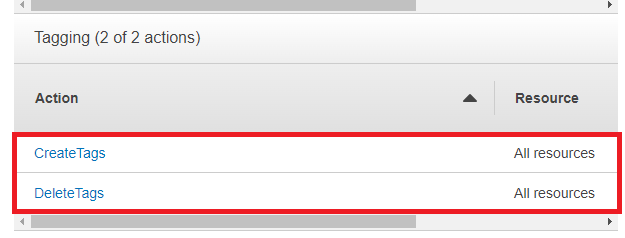
**Step 7: Choose** the **following actions** in the **“write” section:**

****

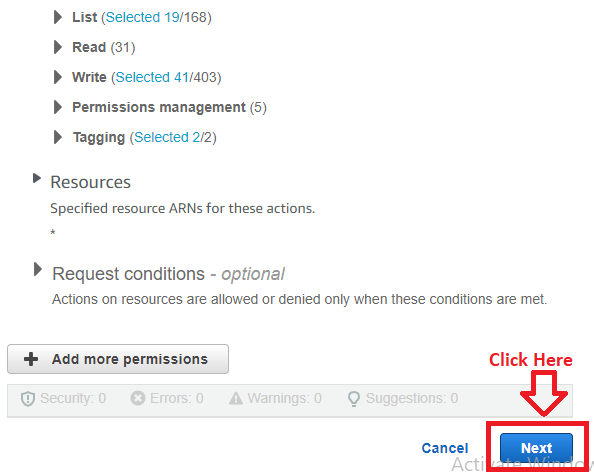
****

****

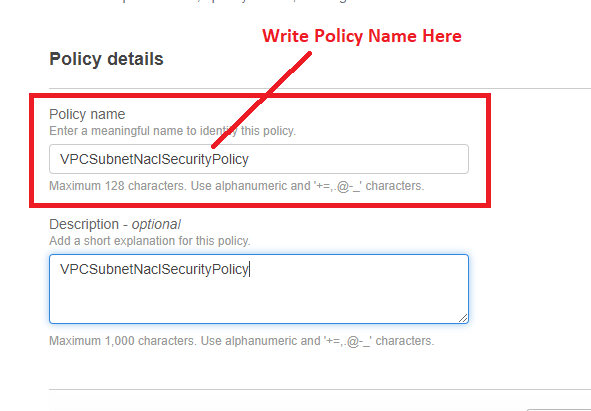
**Step 8: Choose** the **following actions** inthe **“Tagging”.**

****

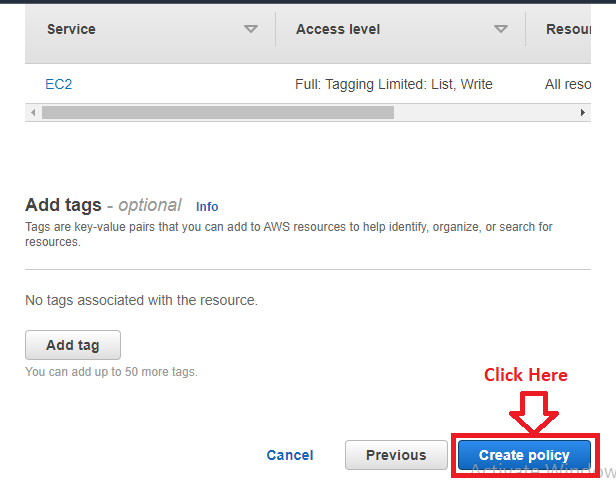
**Step 9: Click** on the **“Next”.**

****

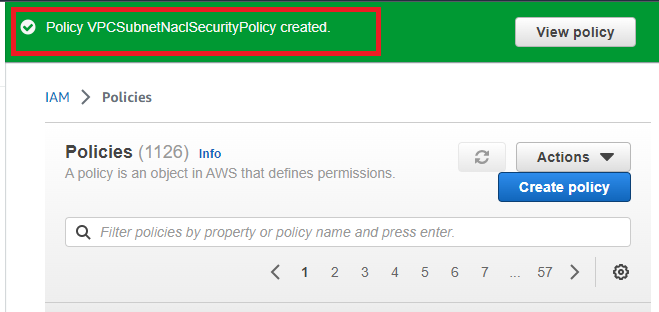
**Step 10: In** the **“Policy Details”, Choose** the **“Policy Name”** asthe **“*VPCSubnetNaclSecurityPolicy*”.**

****

**Step 11: Click** onthe **“Create Policy”.**

****

**Step 12: The policy (VPCSubnetNaclSecurityPolicy)** will be **successfully created.**

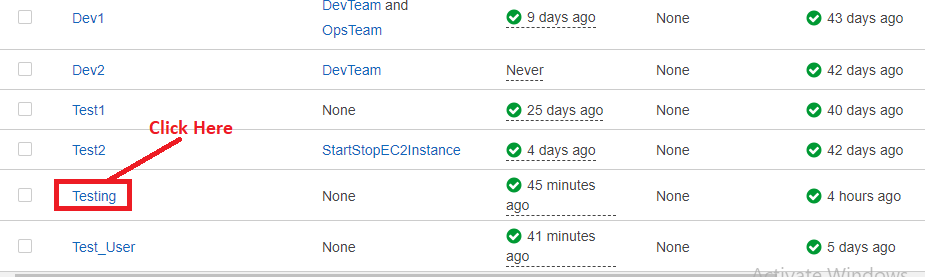
****

****

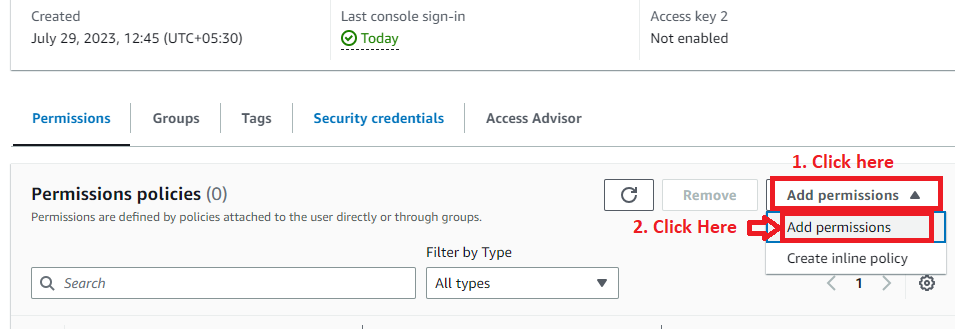
**Step 13: Go** tothe **“Users”.**

****

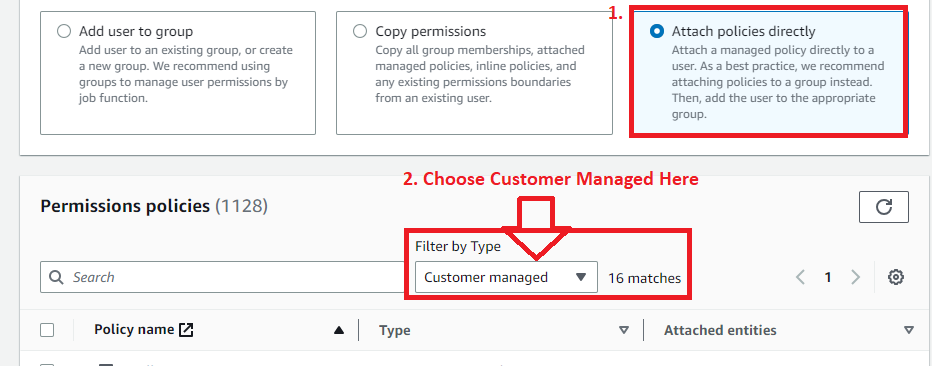
**Step 14: We** have **created** the **“Testing”** User**. Now, we** will **attach** this **policy** to the “**Testing user”. Click** on the **“Testing”.**

****

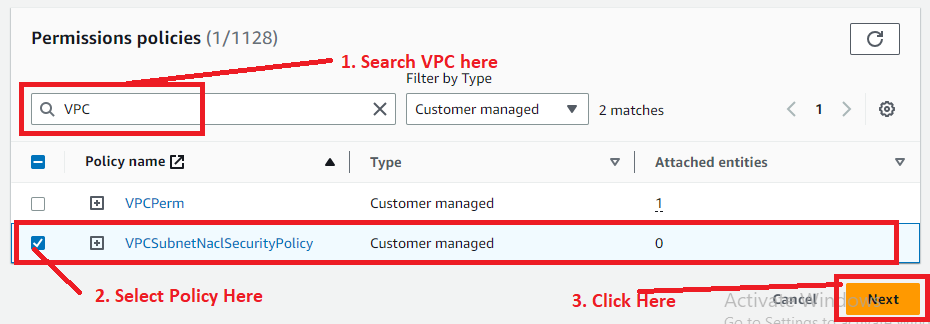
**Step 15: Click** on the **“Add Permissions>Add Permissions”.**

****

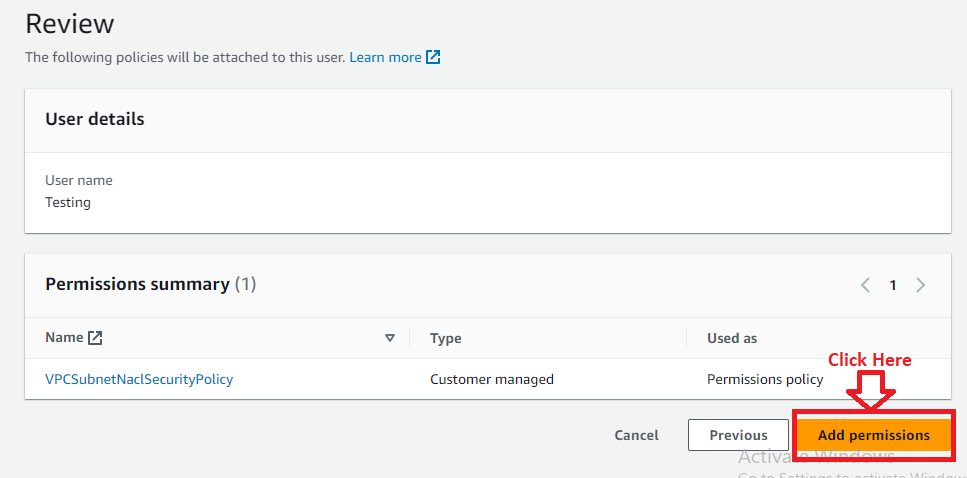
**Step 16: Click** onthe **“Attach policies directly”** & **In** the **“Filter by Type”, choose** the **“Customer Managed”.**

****

**Step 17: Search** the **“VPC”** in **the “Policy”** section **& choose** the **“*VPCSubnetNaclSecurityPolicy*”. Click** on **“Next”.**

****

**Step 18: In** the **“Review”, click** onthe **“Add Permissions”.**

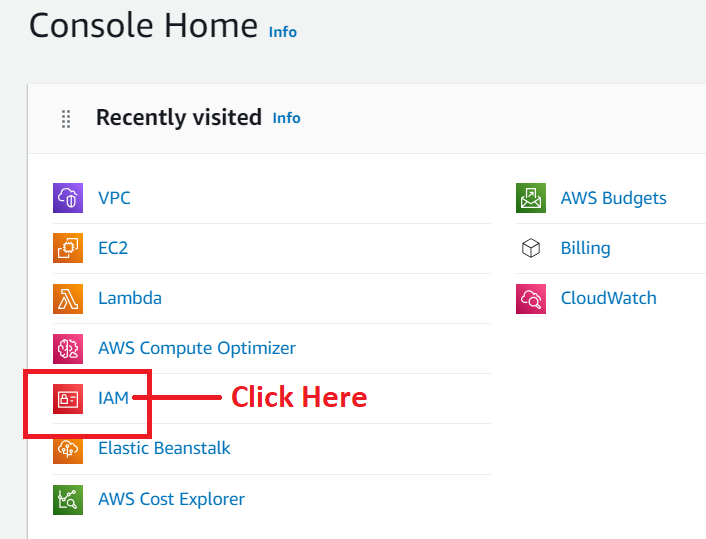
****

**Step 19: Now, the policy** will be **successfully added** to the **“Testing” user. You** can **create VPC, Subnet, NACL & Security Groups** through this **“Testing” User only.**

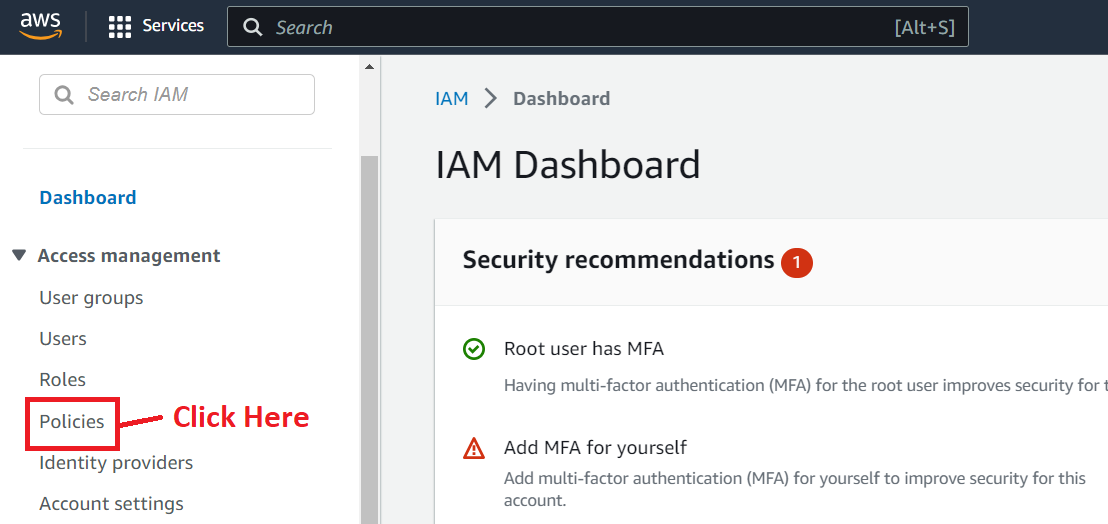
****

**Problem Solution 2 (b):** Further add the permission so that the user can create a RDS instance.

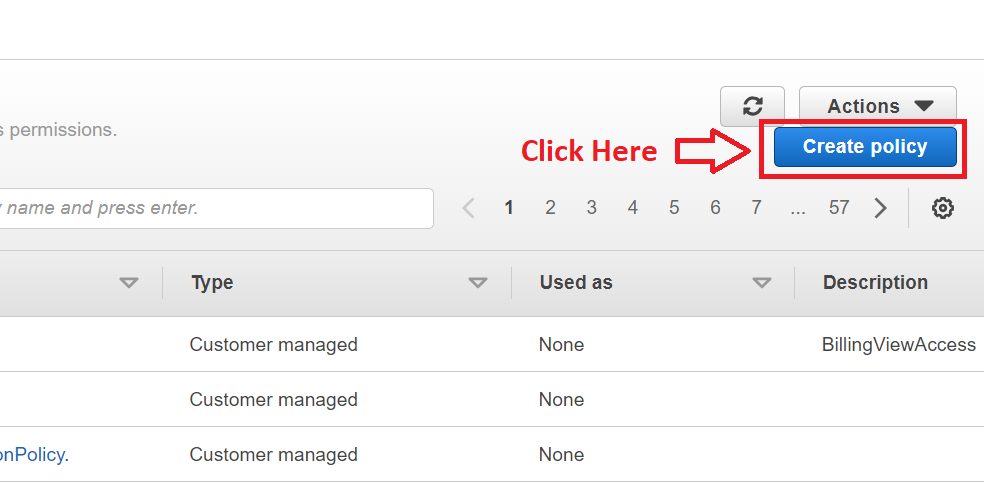
**Step 1: Click** onthe **“IAM”** inthe **“Console Home”.**

****

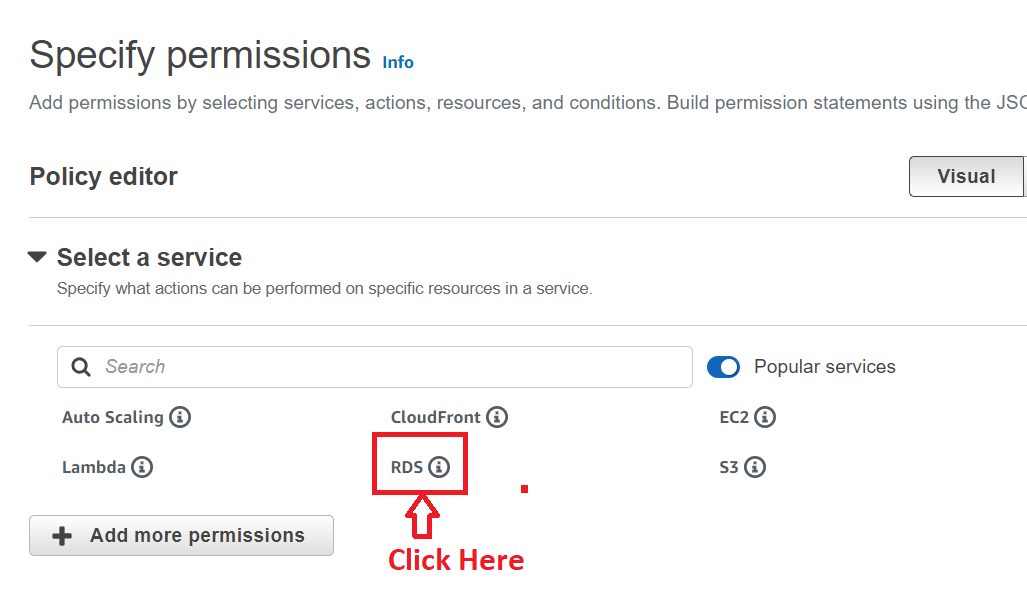
**Step 2: Click** on the **“Policies”.**

****

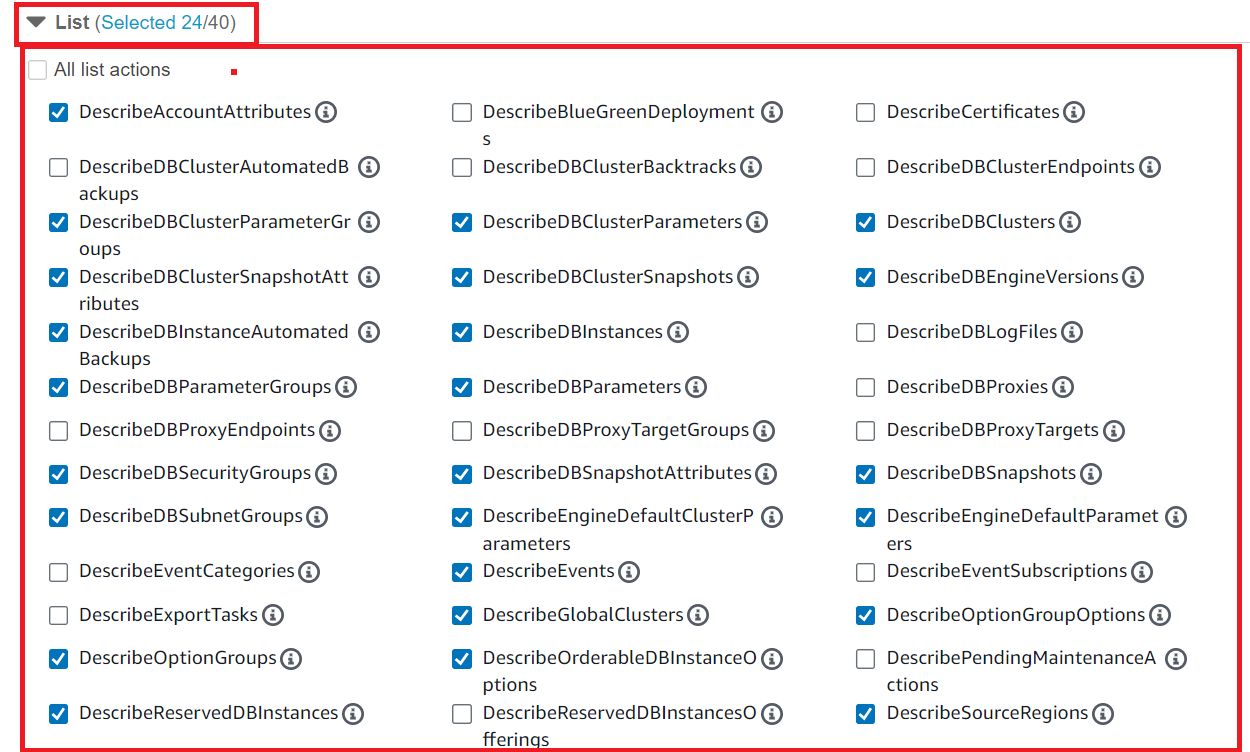
**Step 3: Click** onthe **“Create Policy”.**

****

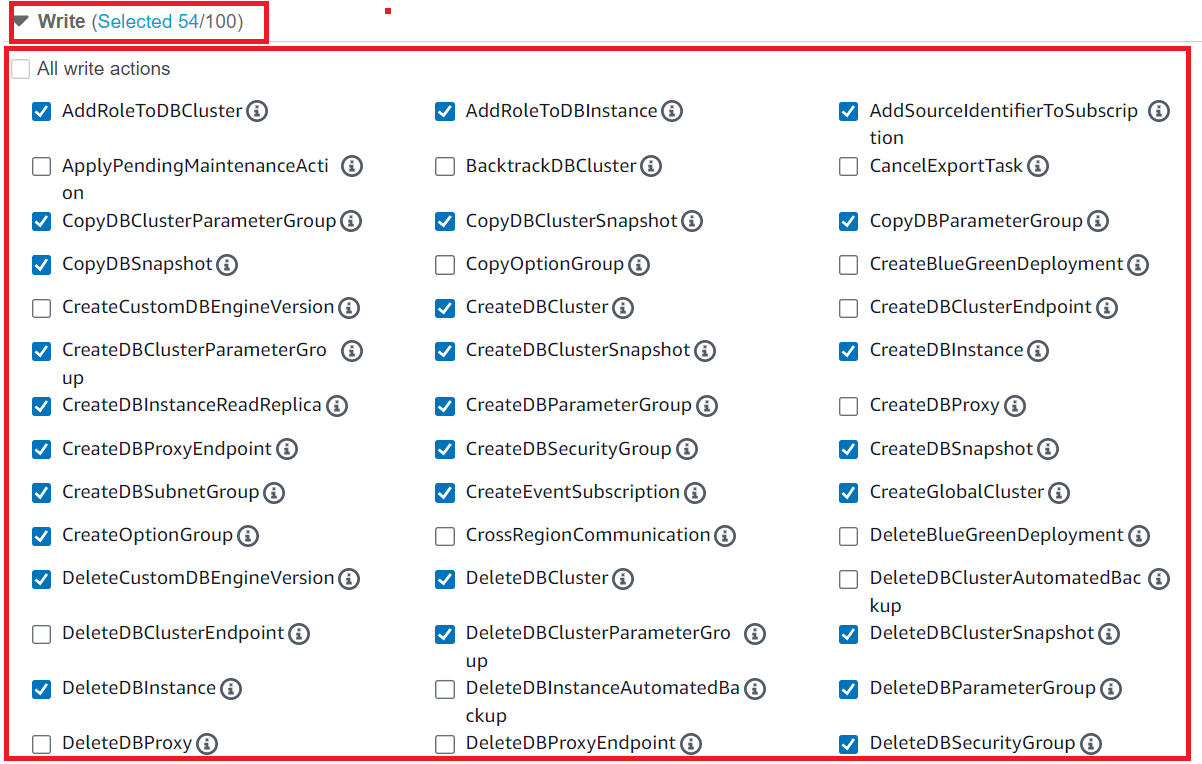
**Step 4: In** the **“Select a Service”, Choose** the **“RDS”.**

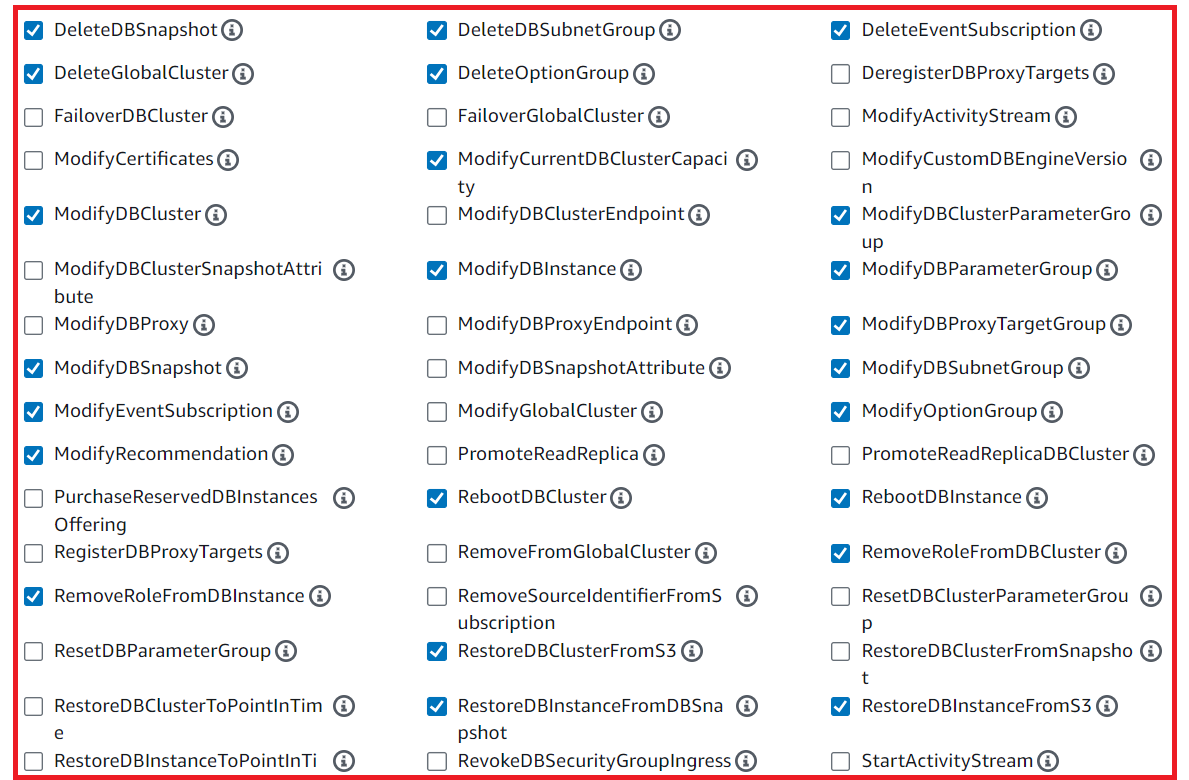
****

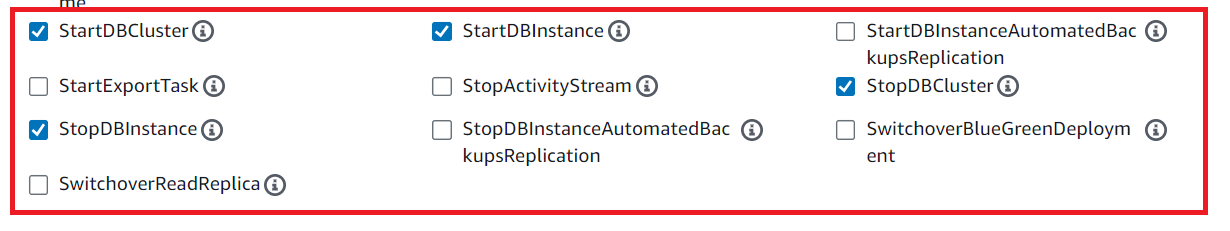
**Step 5: In** the **“List”, choose** these **actions:**

****

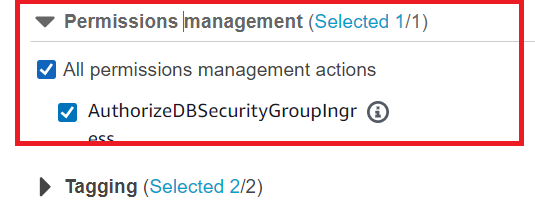
**Step 6: In** the **“Write”, choose** the **following actions;**

****

****

****

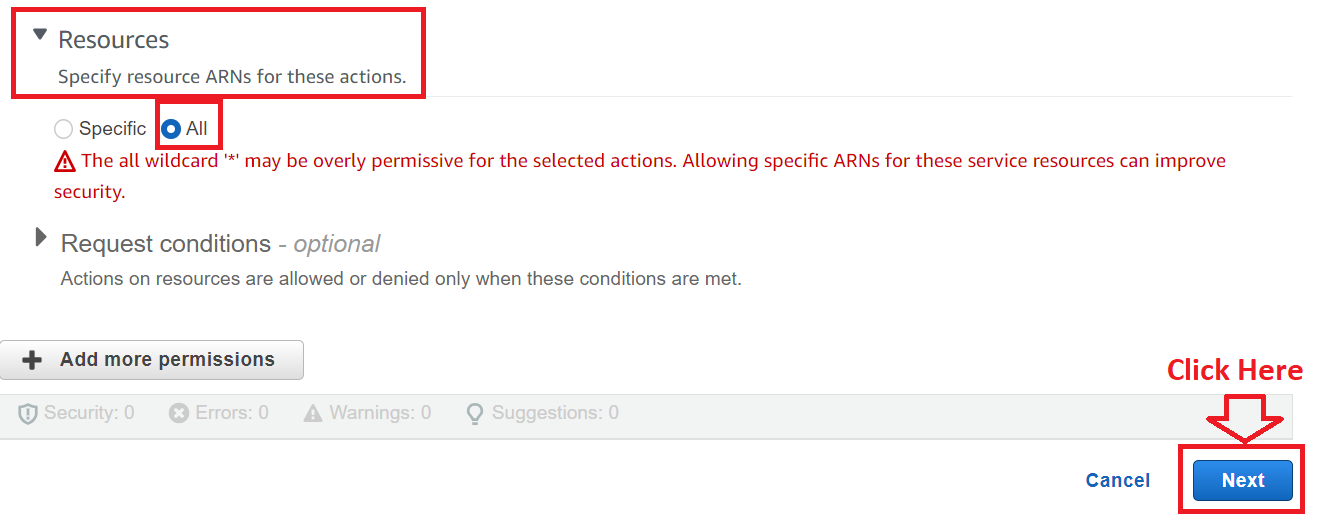
**Step 7: In** the **“Permission Management”, choose** the **“AuthorizeDBSecurity GroupIngress”.**

****

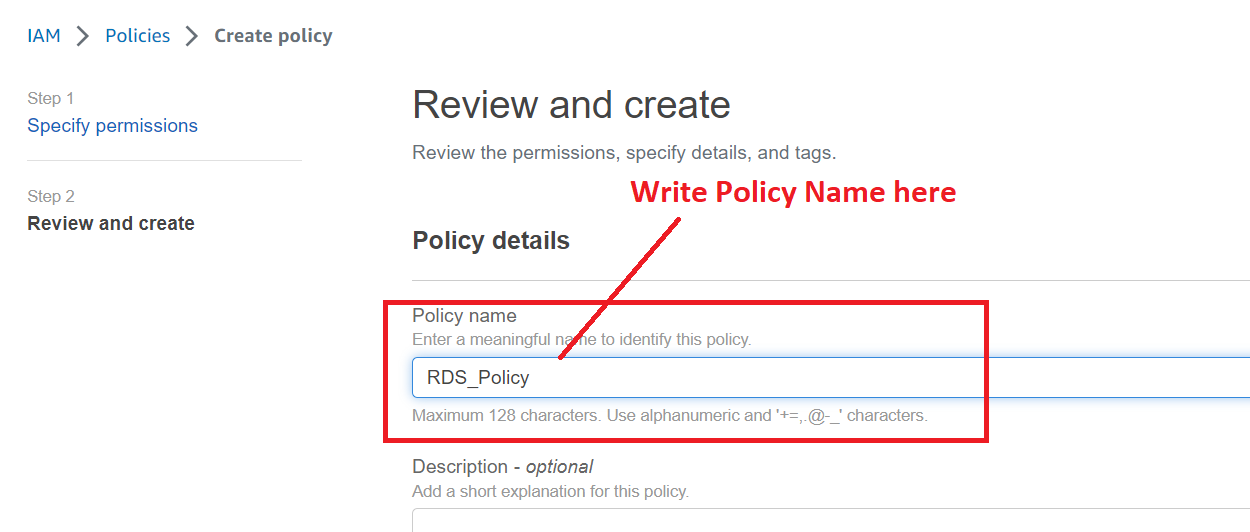
**Step 8: In** the **“Tagging”, choose** the **“All Tagging Actions”.**

****

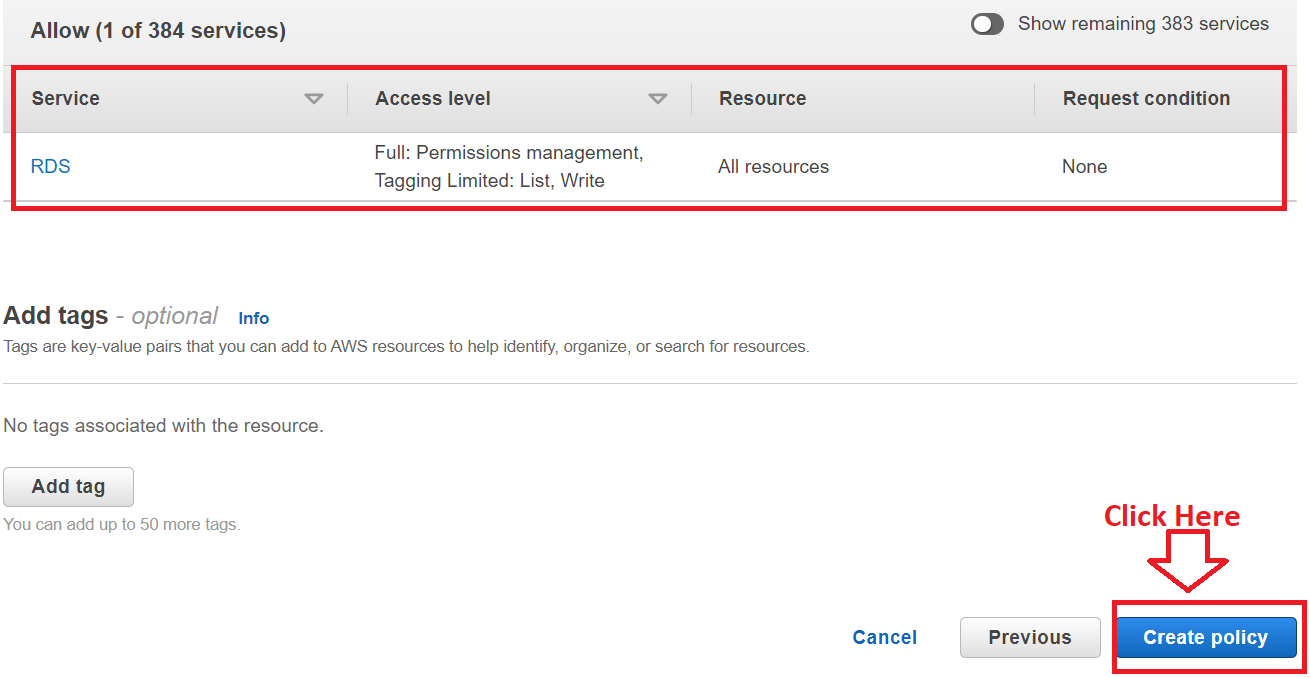
**Step 9: Choose** the **“Resources”** as **“All”** & **click** onthe **“Next”.**

****

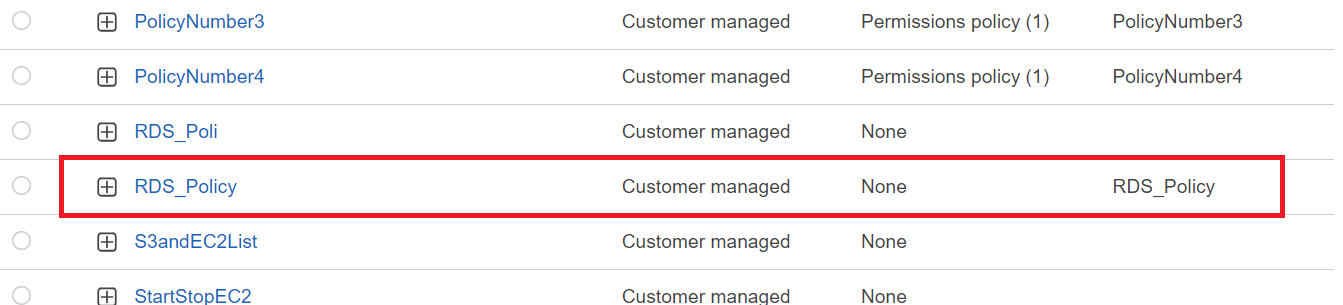
**Step 10: Write** the **“Policy Name”** as the **“RDS\_Policy”.**

****

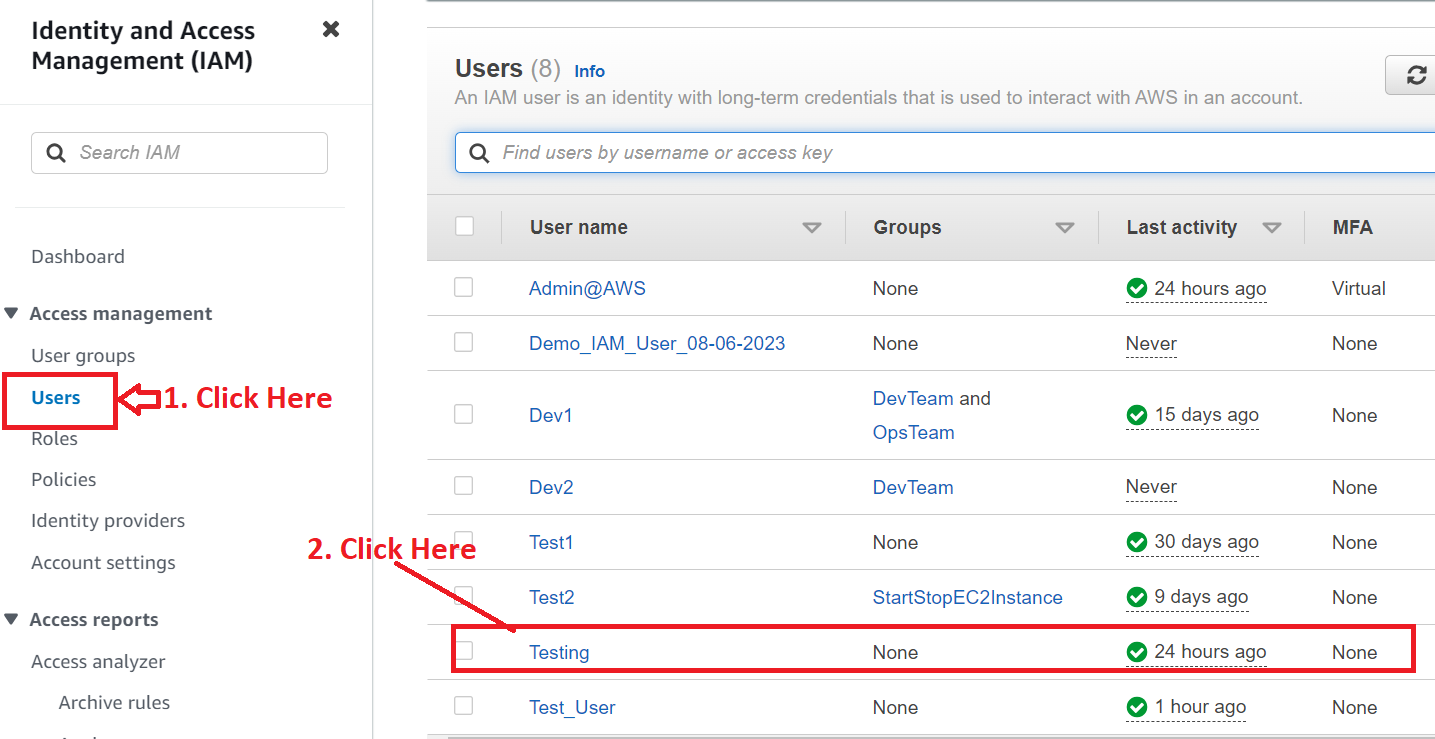
**Step 11: Click** on the **“Create Policy”.**

****

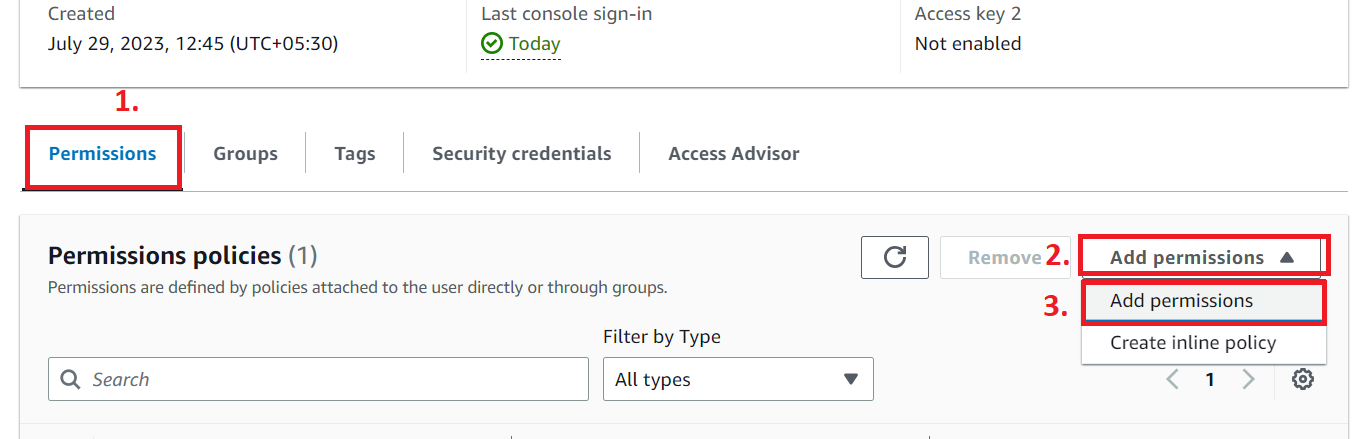
**Step 12: The Policy (RDS\_Policy)** will be **successfully created.**



**Step 13: Go** to the **“Users” & click** onthe **“Testing” user.**

****

**Step 14: Go** to the **“Permissions>Add Permissions>Add Permissions”.**

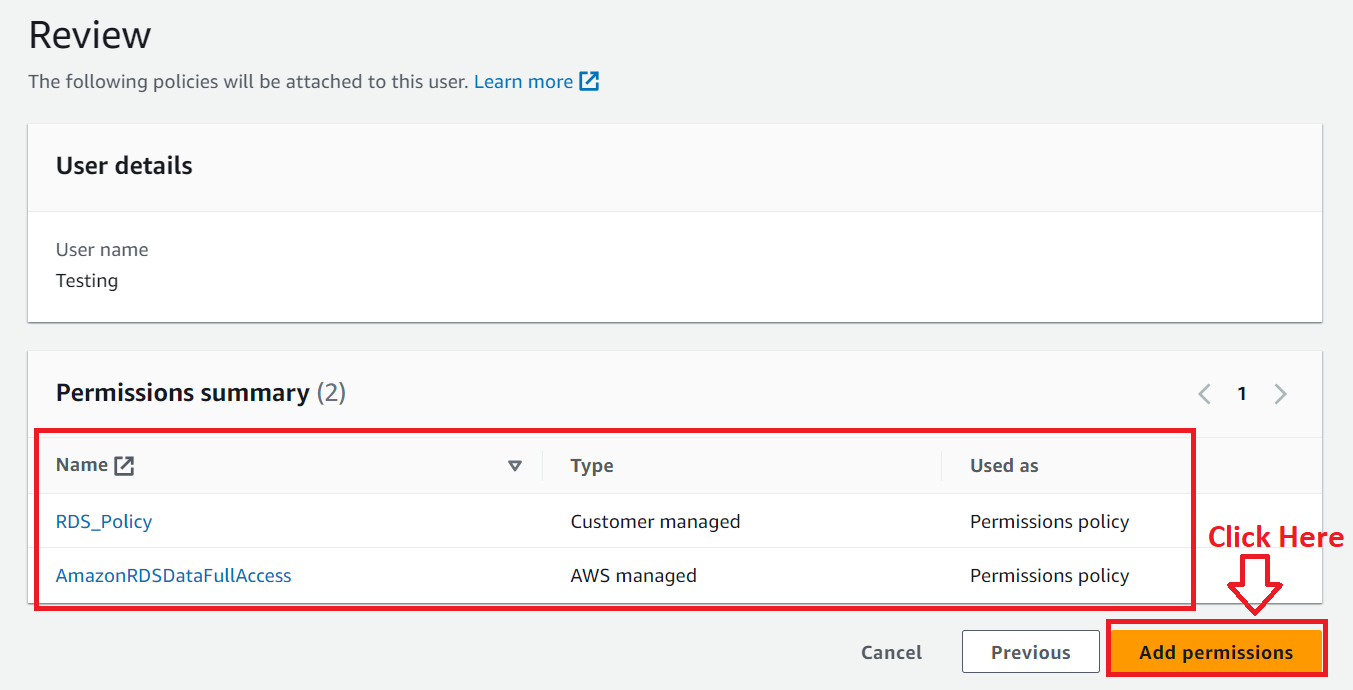
****

**Step 15: Choose** the **“Attach policies directly”** & **choose** the **“Created & AWS Managed policy”** here.

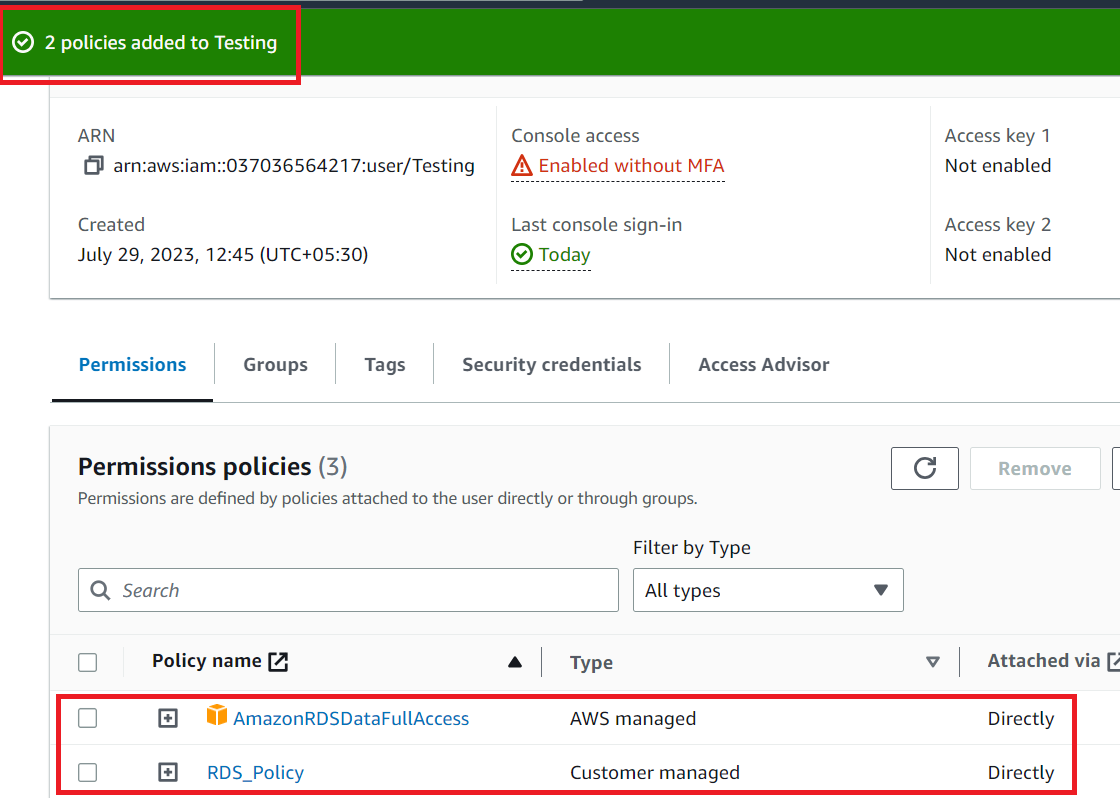
**Customer Managed –** RDS\_Policy (Created by us)

**AmazonRDSDataFullAccess –** AWS Managed

**Click** on the **“Add permissions”.**

****

**Step 16: Now, you** can **successfully create** the **database** through the **“Testing” user** using this **policy.**

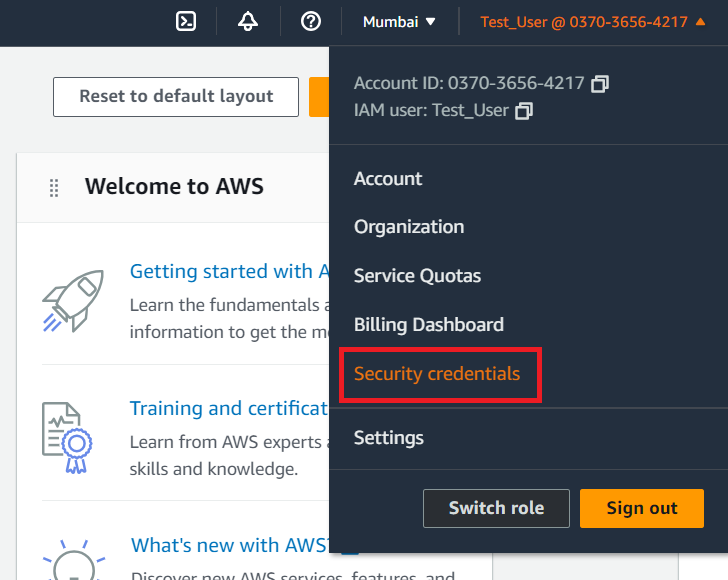
****

**Problem 2 (c) Solution):** Explore security options to protect the AWS Resources and secure the permission provided to the group.

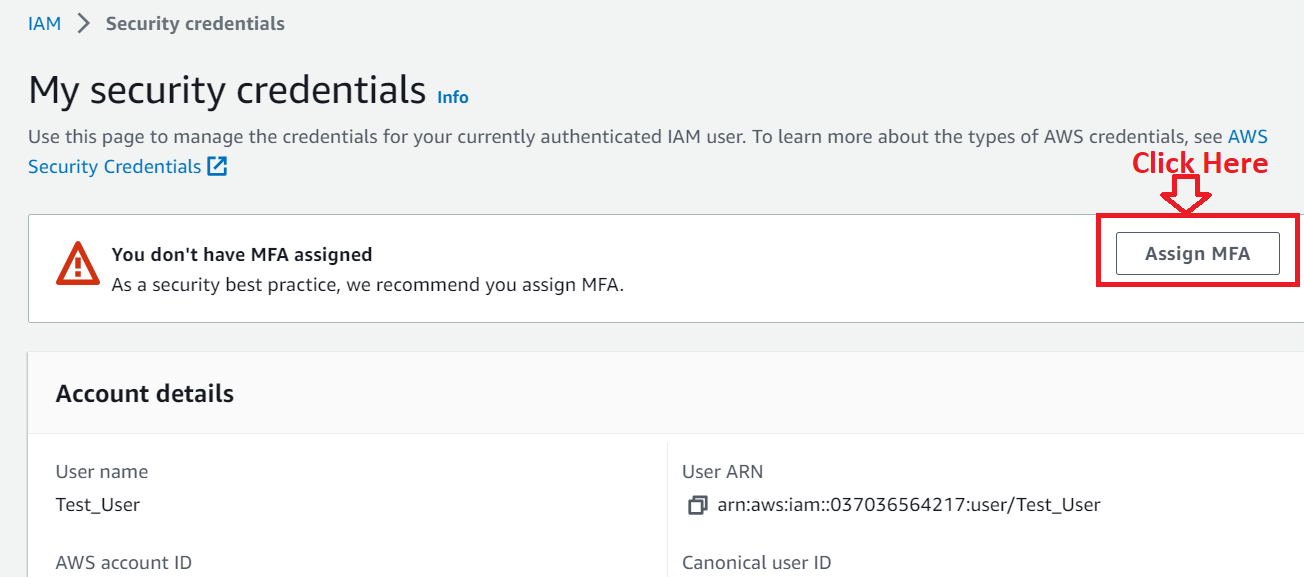
**1. Securing the AWS User Account Resources**

**For securing** the **AWS resources, you** should **use Administrator level account** & **enable MFA** to **secure** the **administrator account. You** can **also provide** the **limited access to user’s** & **its groups** also.

**Step 1: Go** to the **“Security credentials”.**

****

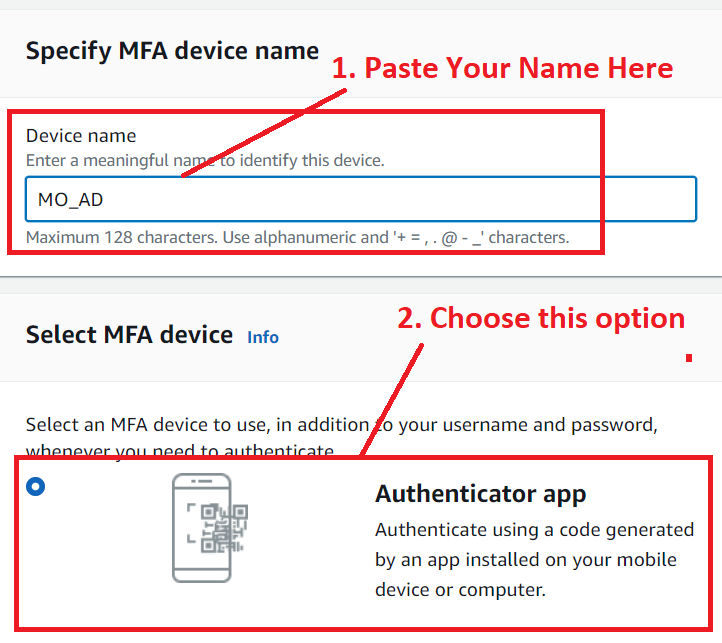
**Step 2: Click** on the **“Assign MFA”.**

****

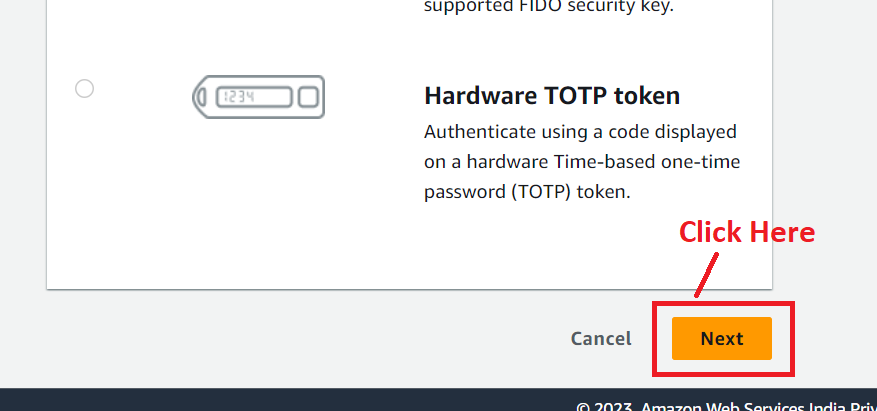
**Step 3: Choose** the **following options** here:

**Device Name:** MO\_AD

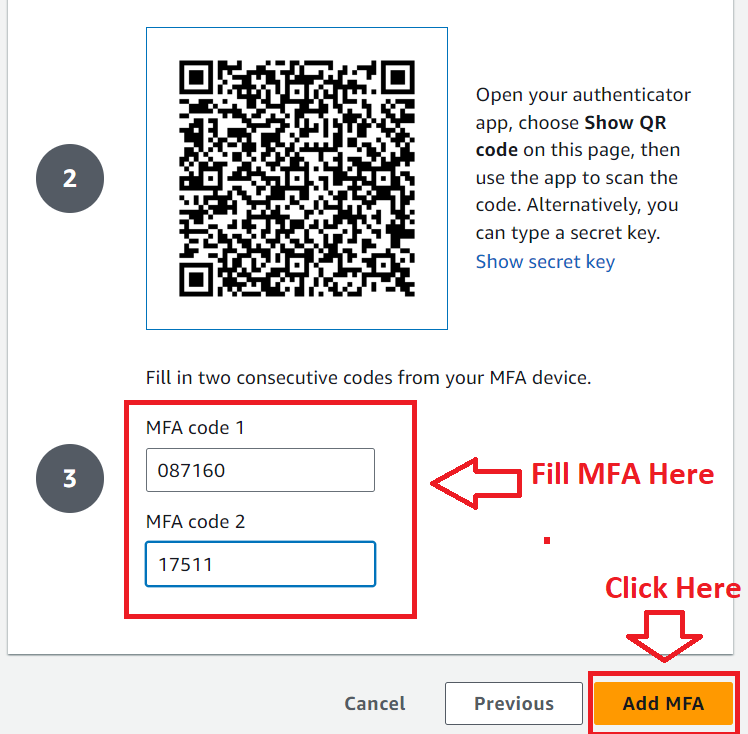
**Select MFA Device:** Authenticator app

****

**Click on Next.**

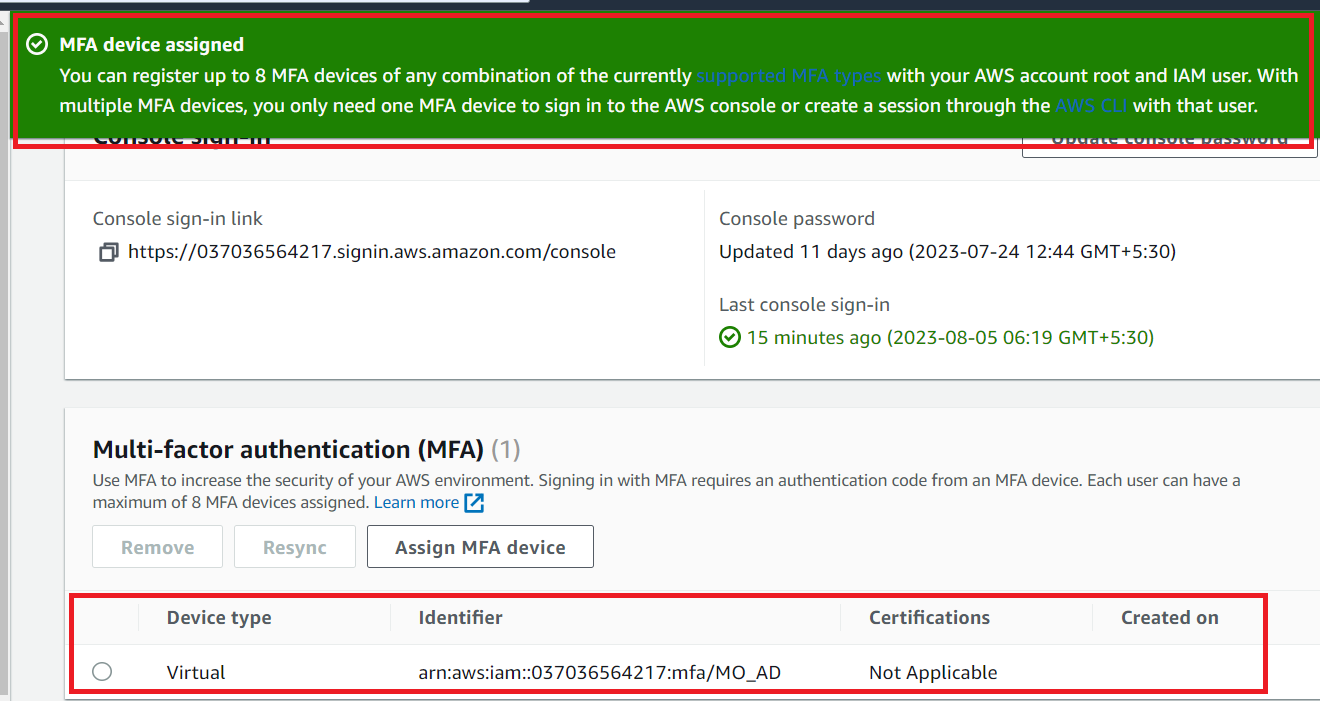
****

**Step 4: Now, install** the **Google Authenticator App** on your **mobile** & **Scan** this **QR Code. We** have **installed Google Authenticator** & **now we** will **scan** the **QR code.**

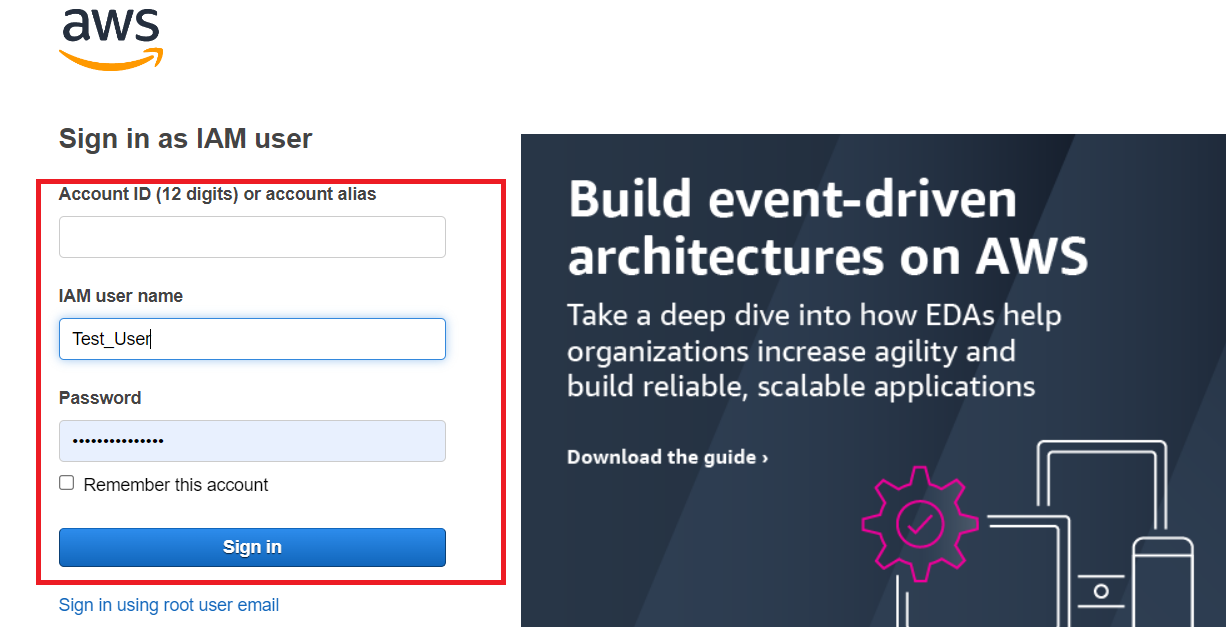
****

**Fill** the **MFA Codes, click** on **“Add MFA”.**

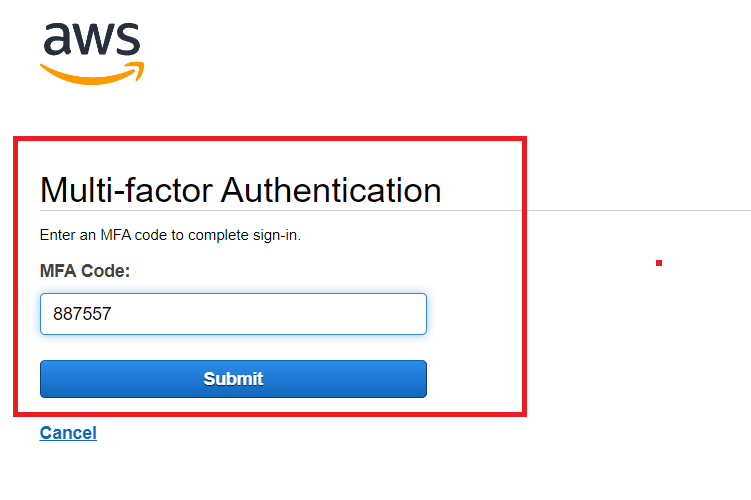
**Step 5: Now, your MFA** is **assigned** & **when you login** into your **administrator level account, you** must **fill MFA code** to **login in it.**

****

**Step 6: Now, we** will **check** the **account** & **see MFA** is **enabled or not.**

****

**Now, you** have to **fill the “MFA Code”** to **login** into your **account.**

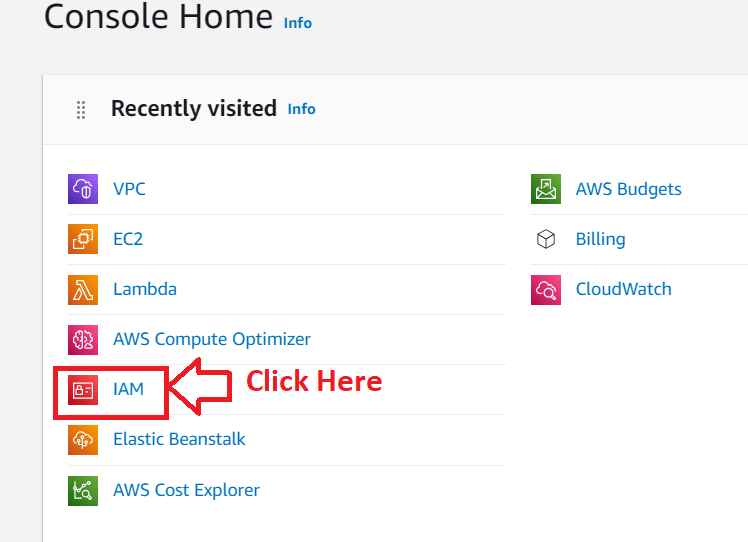
****

**To protect** your **account, you** can **change admin level account password** at the **regular intervals.**

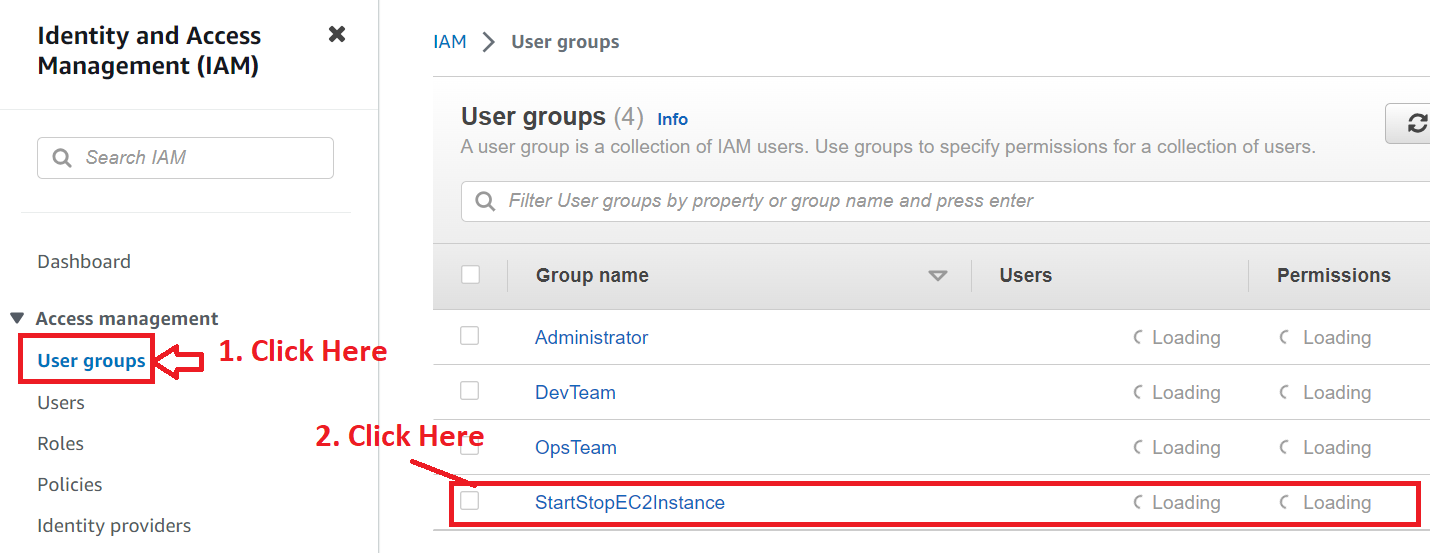
**2. Secure the group**

**For securing the group, you** can **add the Change Password policy** in the **group** for the **user. You** can **also provide limited accessibility** to the **groups** to **perform certain actions.**

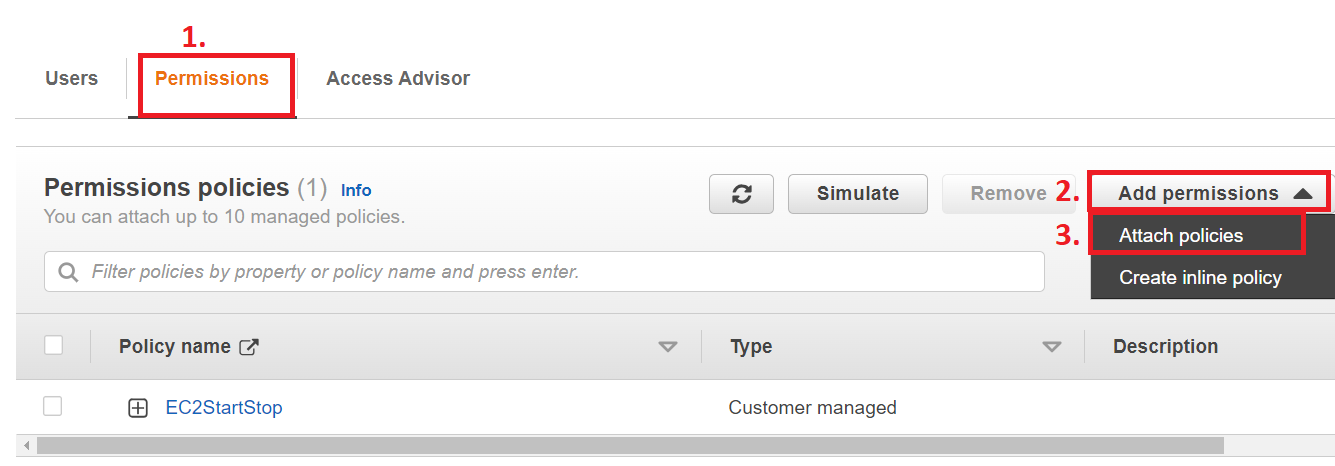
**Step 1: Go** tothe **“IAM”.**

****

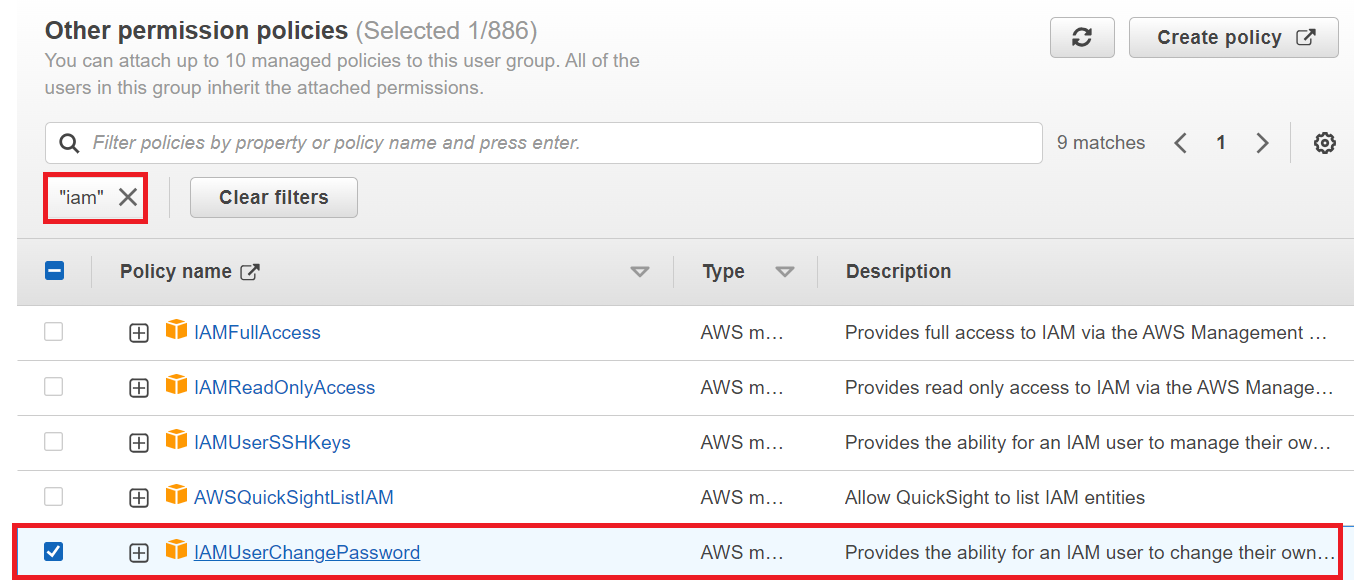
**Step 2: Go** to the “**User Groups”. Click** onthe **“StartStopEC2Instance”.**

****

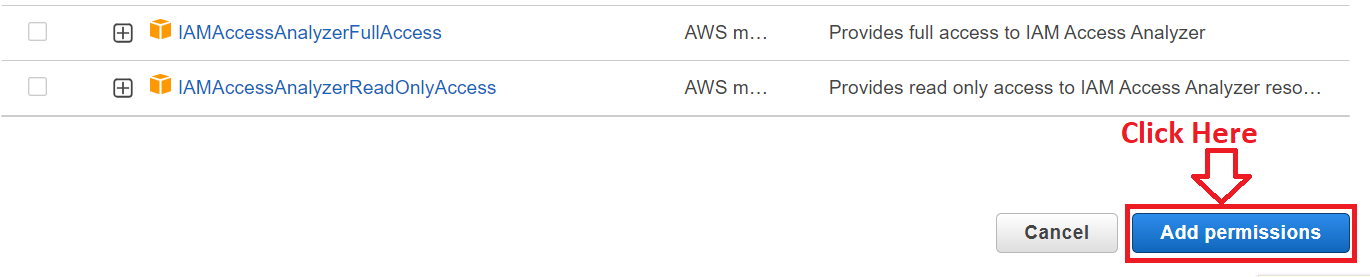
**Step 3: Go** tothe **“Permissions>Add Permissions>Attach policies”.**

****

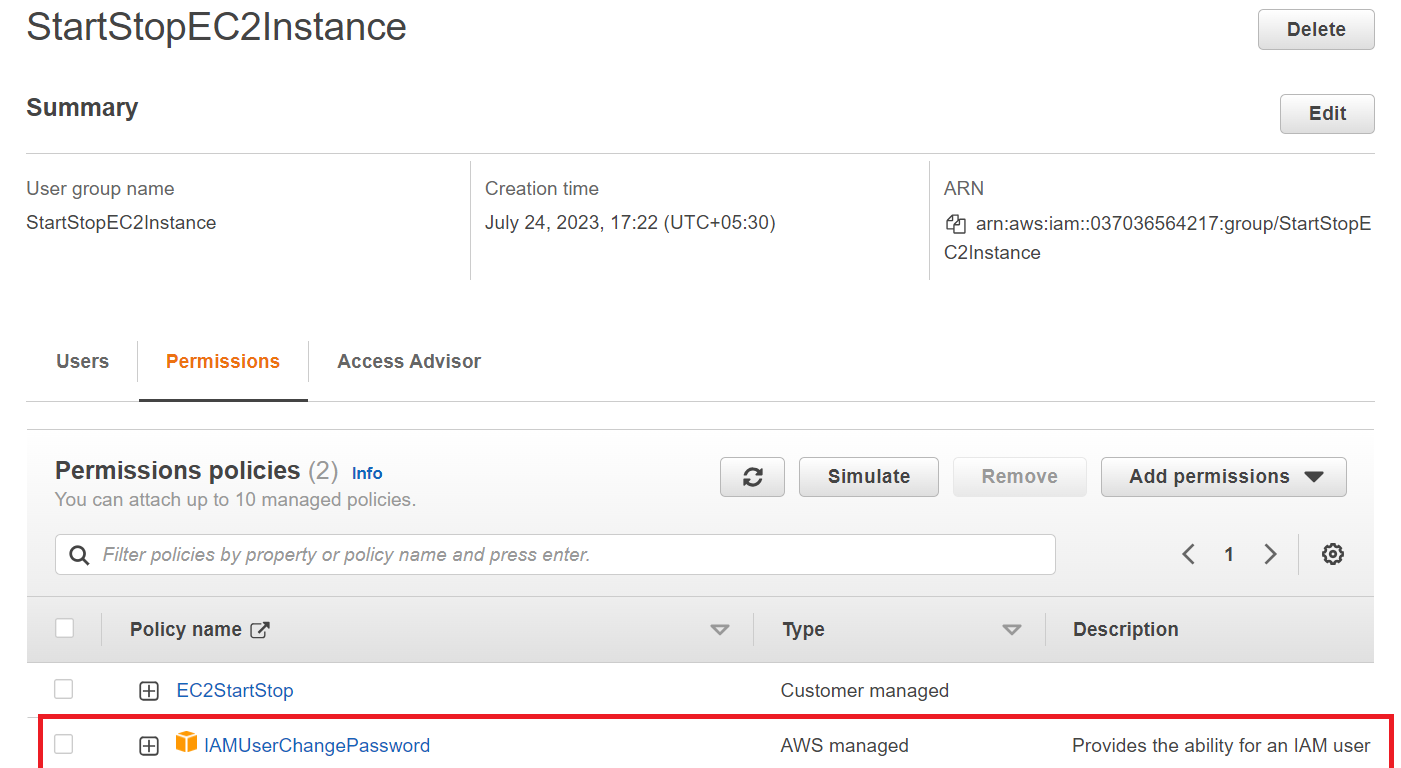
**Step 4: Type “iam” & choose** the **“IAMUserChangePassword”** policy.

****

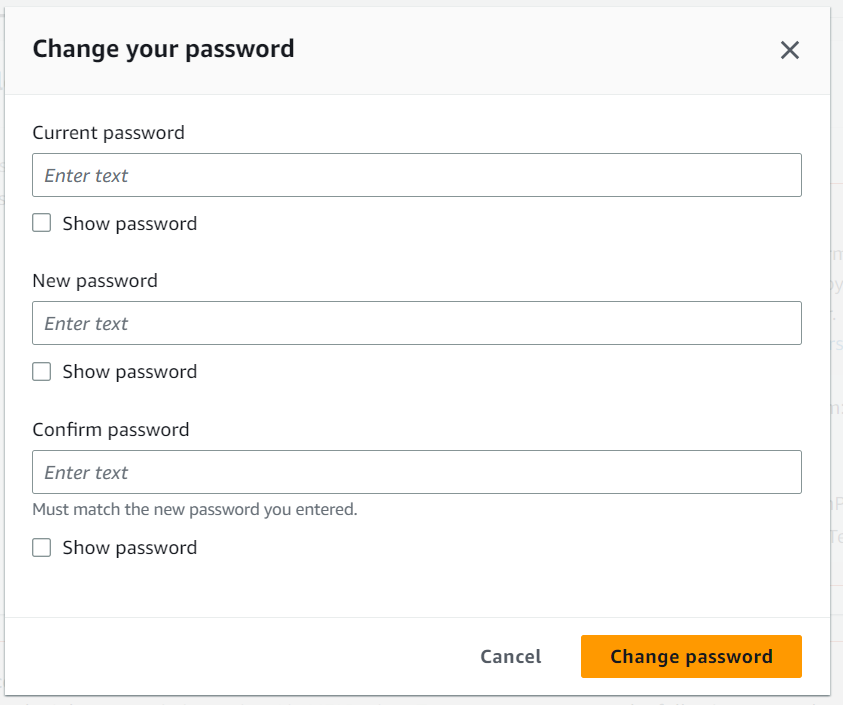
**Step 5: Click** on the **“Add Permissions”.**

****

**Step 6: The policy** will be **attached** & **you** can **change** your **password** on the **regular basis.**

****

**Now, you** can **change** your **password through** the **“Testing” User successfully.**

****

**You** can **also add other security layers** to **protect** your **account & users.**

**Task for You: You have to test** all the **manually created policies** on the **“Testing” user** & **they will be successfully working for you also. These all are working fine for us.**