**Cloud Security with AWS IAM Using AWS**

**Project Summary**:

In this project, We will demonstrate How to use AWS IAM to Control access and permission settings in our AWS Account.

**What is EC2 Instance:**

Amazon EC2 is a service that lets you rent and use virtual computers in the cloud. It’s like your personal computers, but they exist on the internet instead of being physically in front of you. You can create, customize, and use these computers for all different reasons, from running applications to hosting websites.

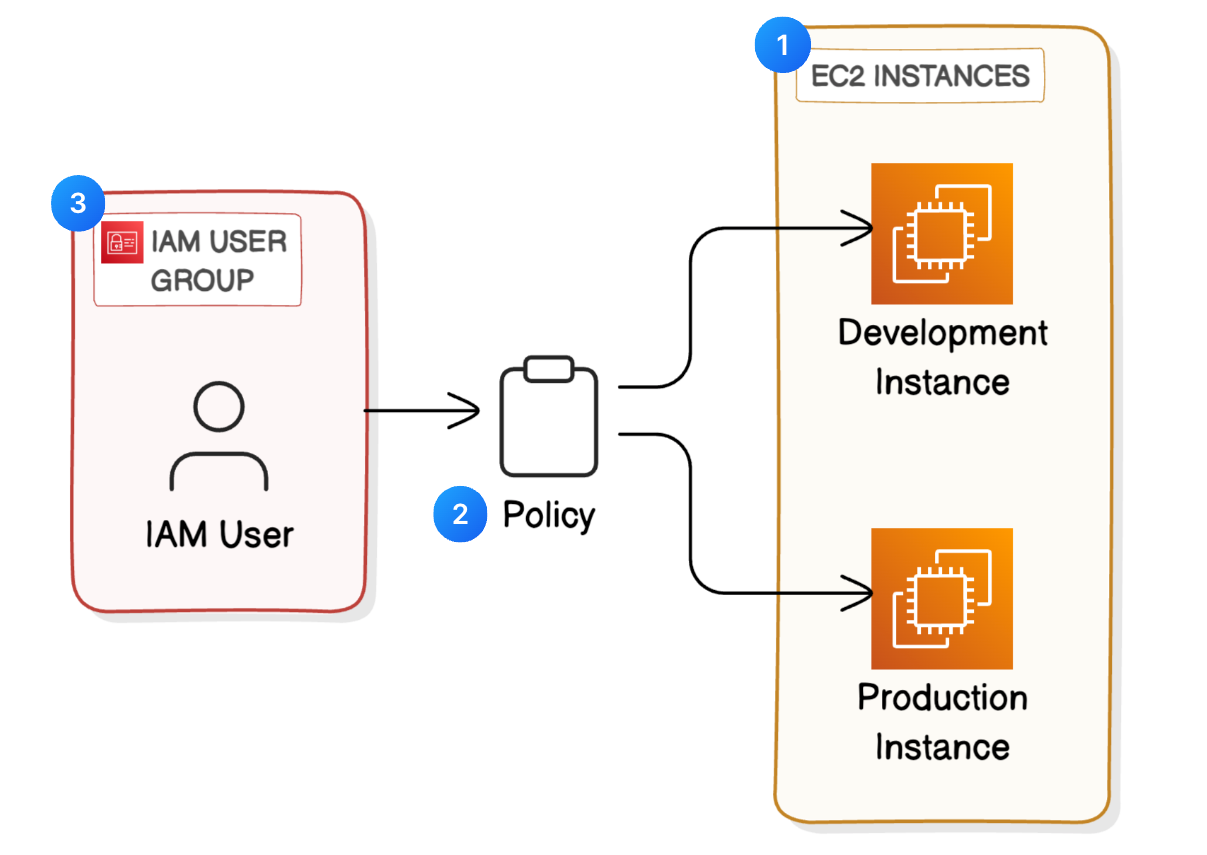
**What is IAM Service:**

**AWS Identity and Access Management (IAM)** service to control who is authenticated (signed in) and authorized (has permissions) in your AWS account.

**AWS Services Used to Create in this Projects:**

* EC2 Instances
* IAM Policies
* IAM Users & groups
* AWS Account Alias

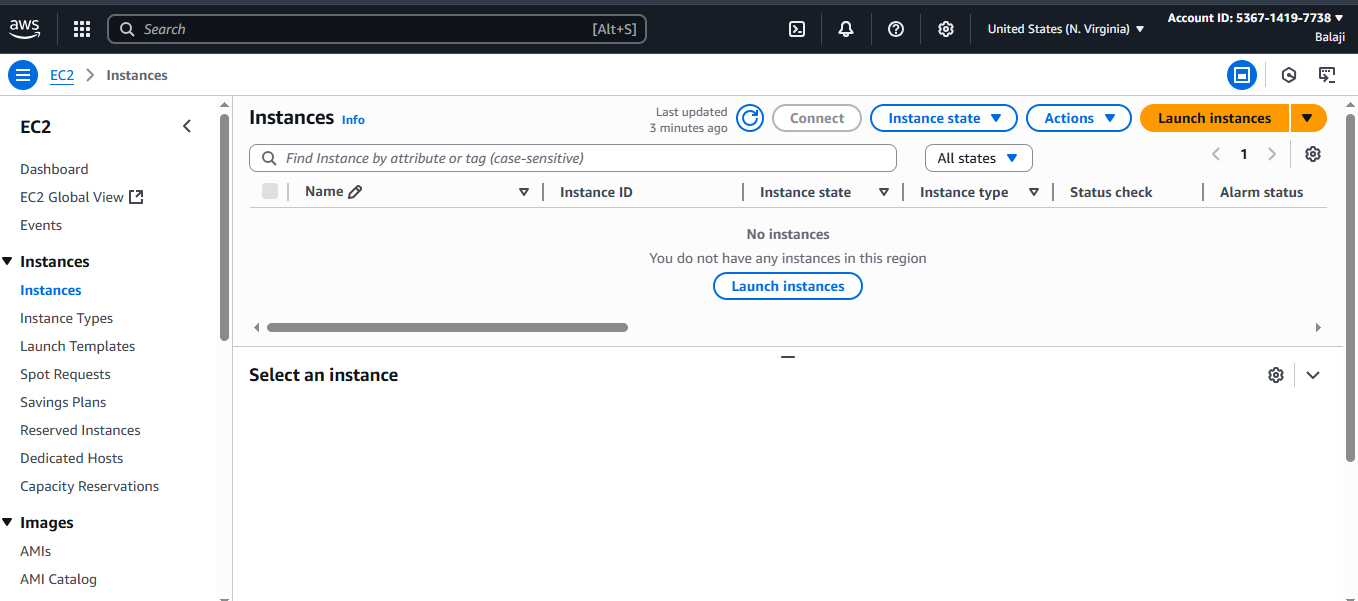
**Architecture Diagram:**



**Steps:**

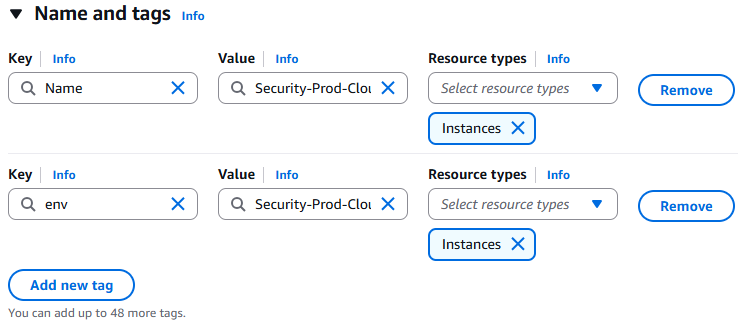
**Step 1:** Login to AWS Management console.

**Step 2:** Launch an EC2 Instances for (Production Environment)

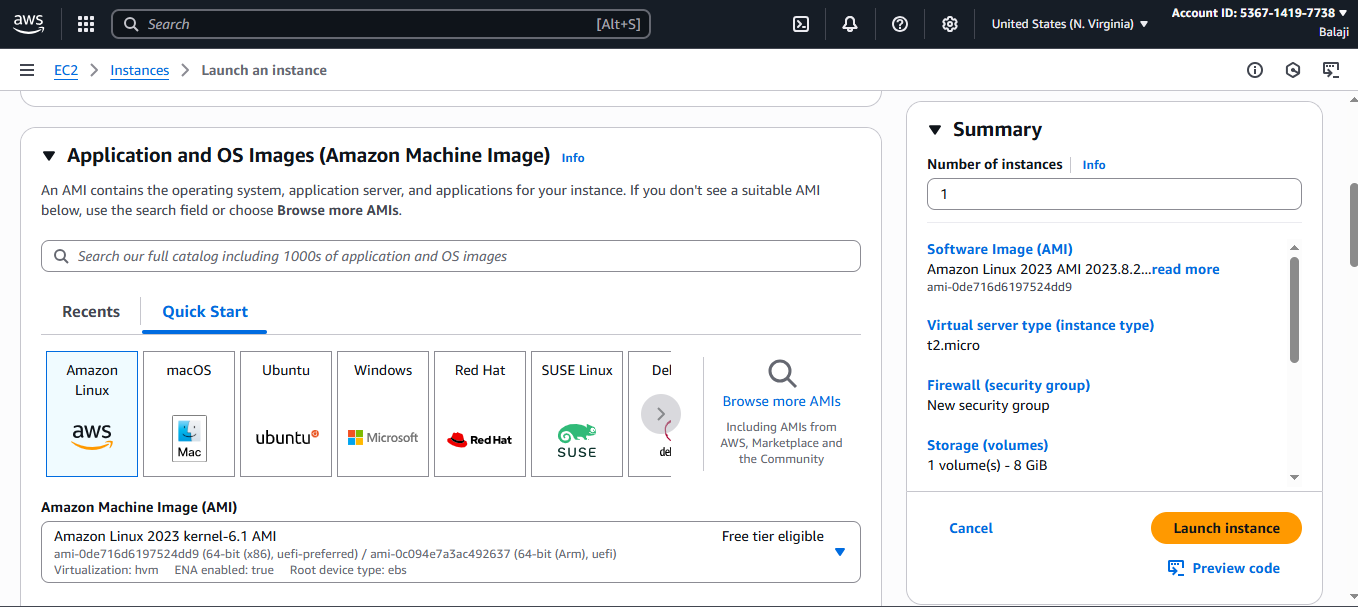


**Step 3:** Enter the Name & Tags of the EC2 instance.

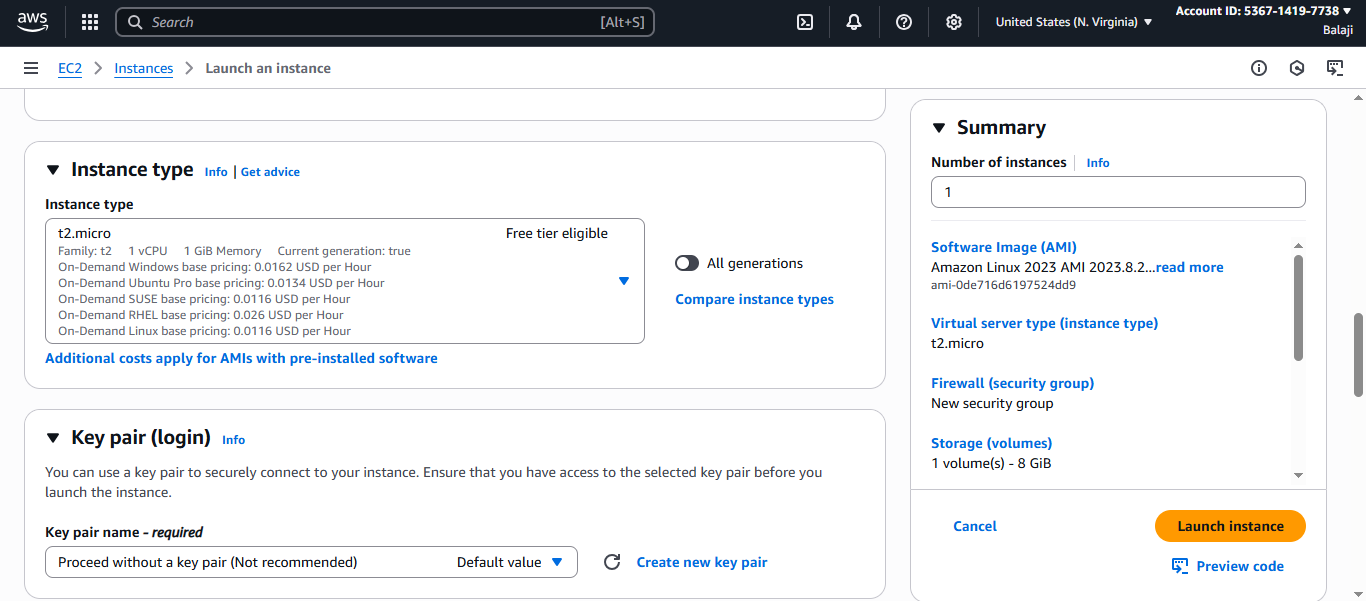
**EC2 Instance name**: Security-Prod-Cloud



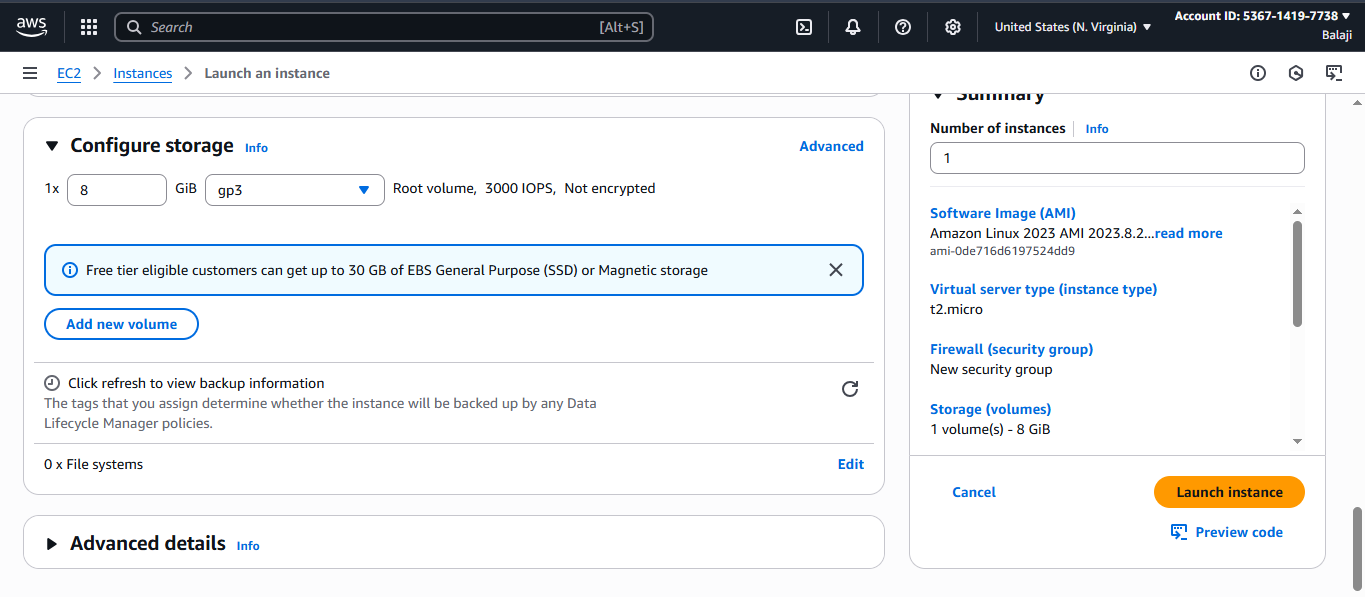
**Step 4:** Select the Linux AMI (Amazon Machine Image) & It is a Free Tier.



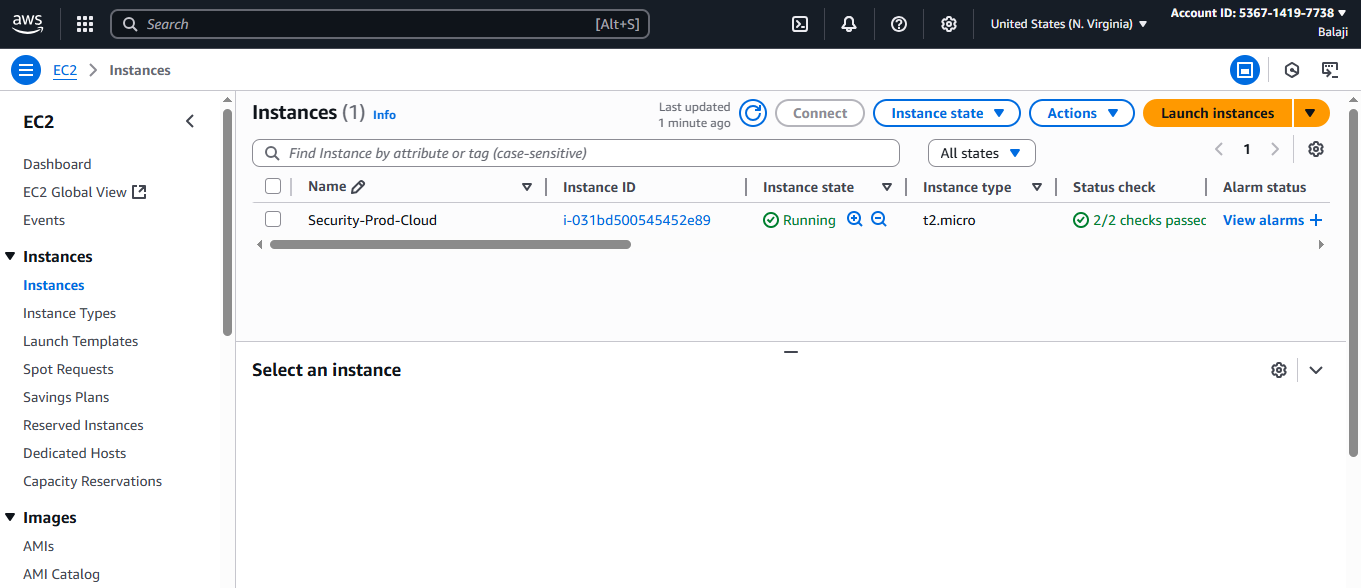
**Step 5:** Select the Instance type as t2.micro, Because it is a Free Tier & Proceed without key pair we do not require key pair for this project.



**Step 6:**  Keep rest all settings as default & Click on Launch Instance.

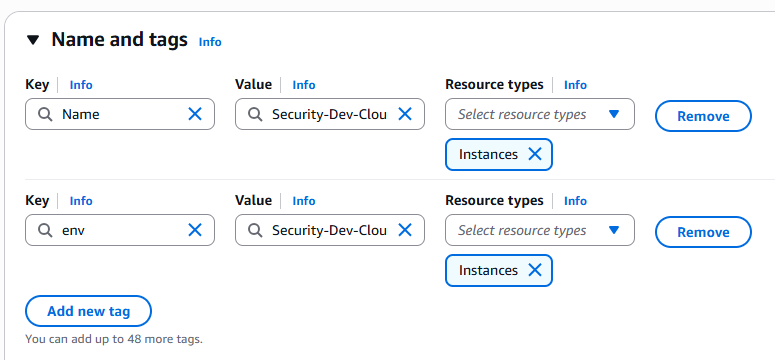


**Step 7:** Production Environment instance is created.

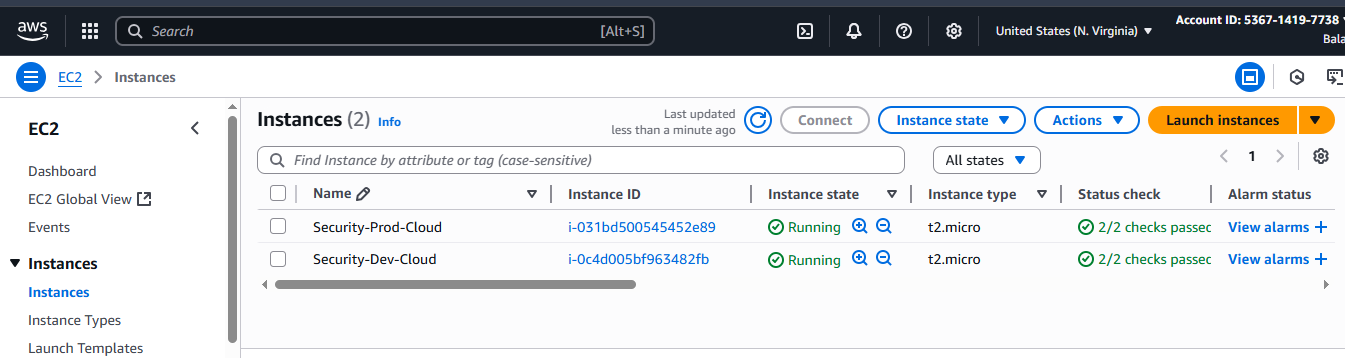


**Step 8:** Another EC2 instance for development Environment instance & Same settings which we did for prod env.

**EC2 Instance name**: Security-Dev-Cloud

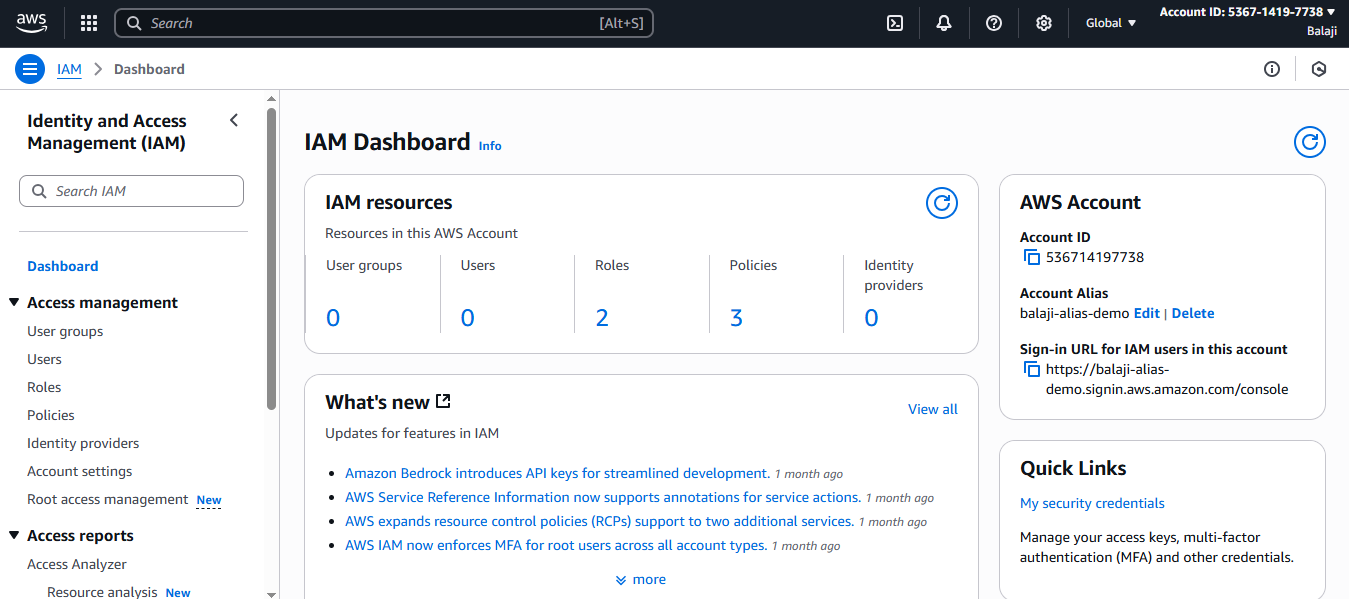


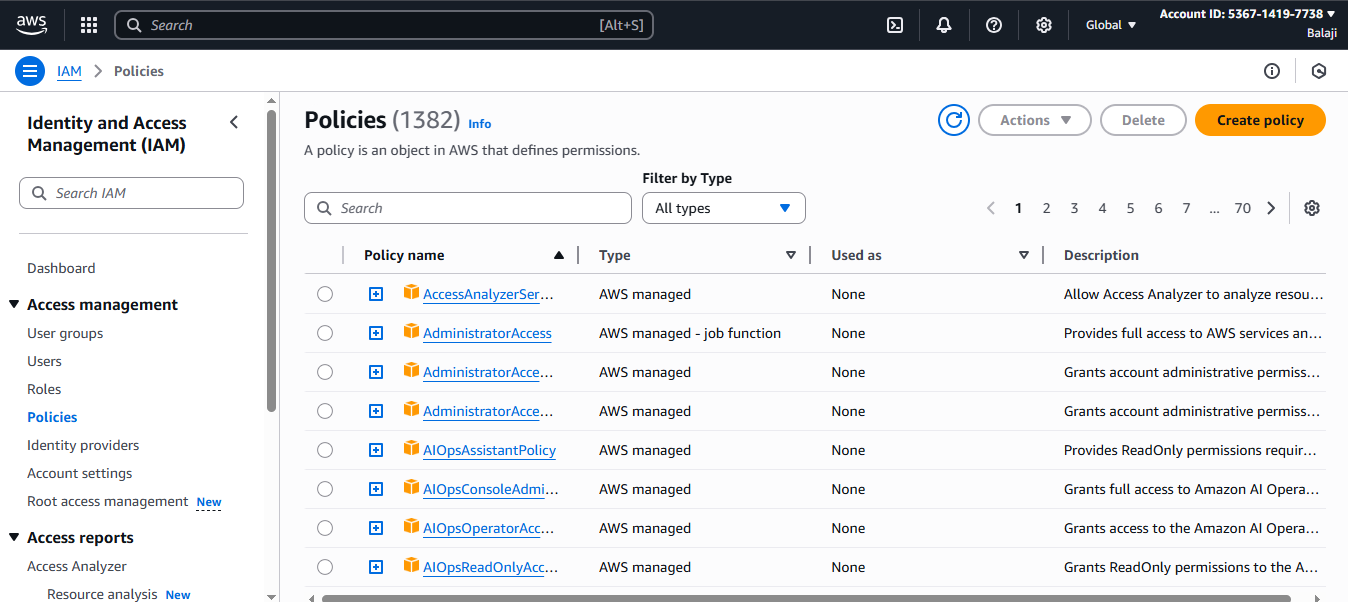
**Step 9:** Development Environment instance is created.

****

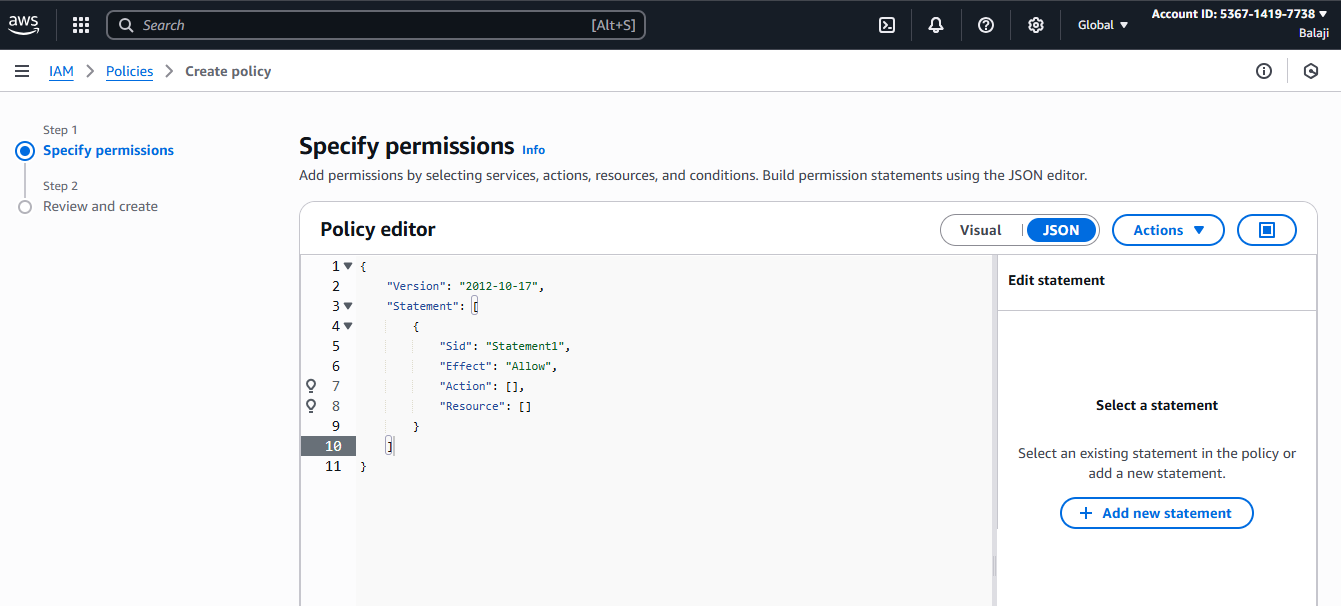
**Step 10:** We have created both Prod Env & Dev Env & Next we will be creating IAM Policies to give access to only development environment EC2 instance but not for production environment EC2 instance.

**Step 11:** Click on Policies & Click on Create Policies.

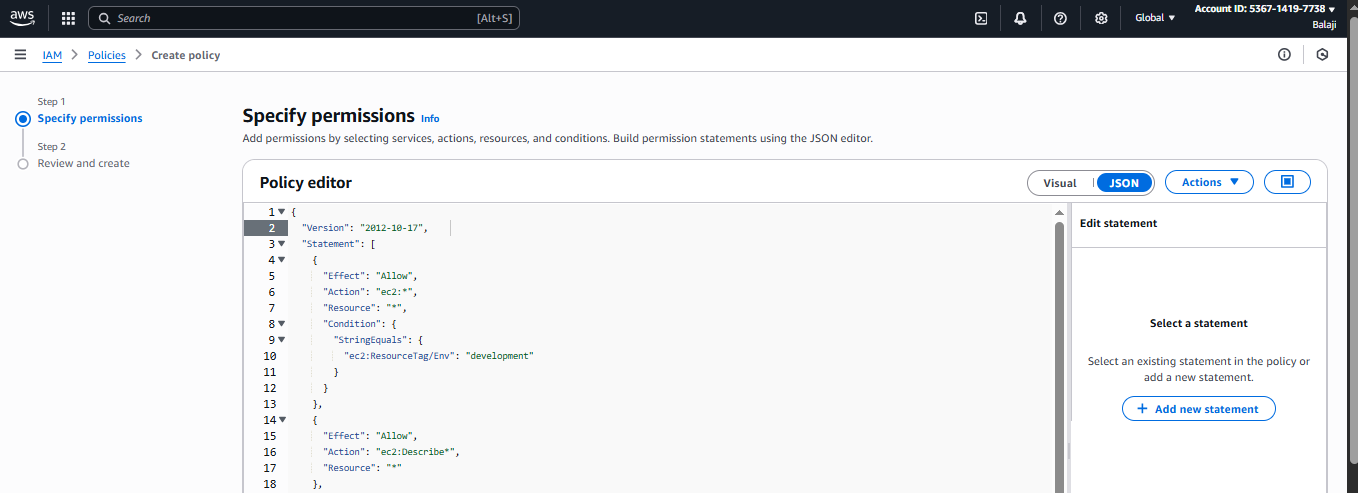


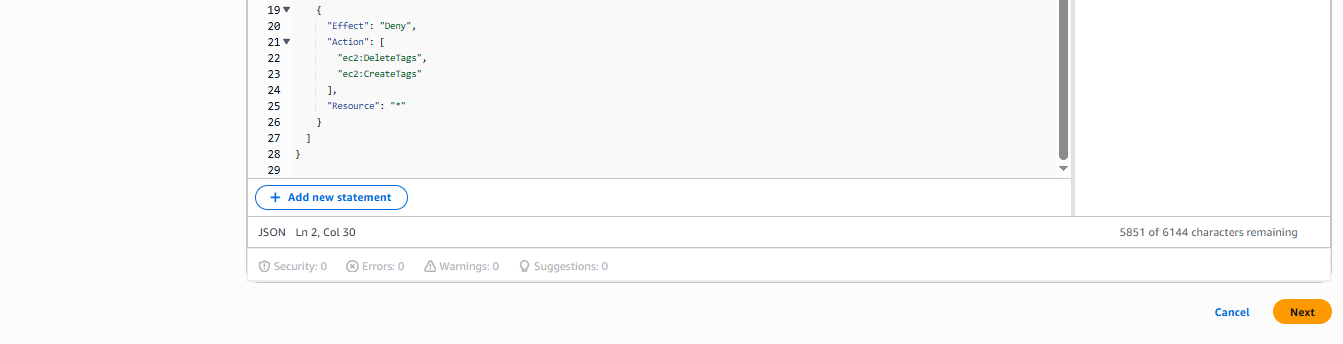


**Step 12:** Click on JSON policy code.

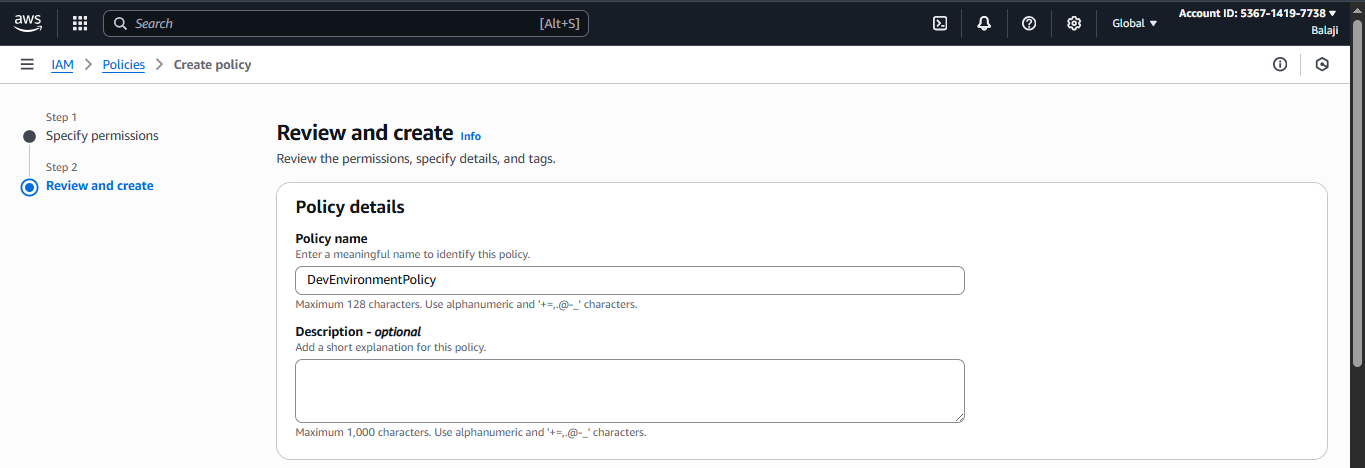


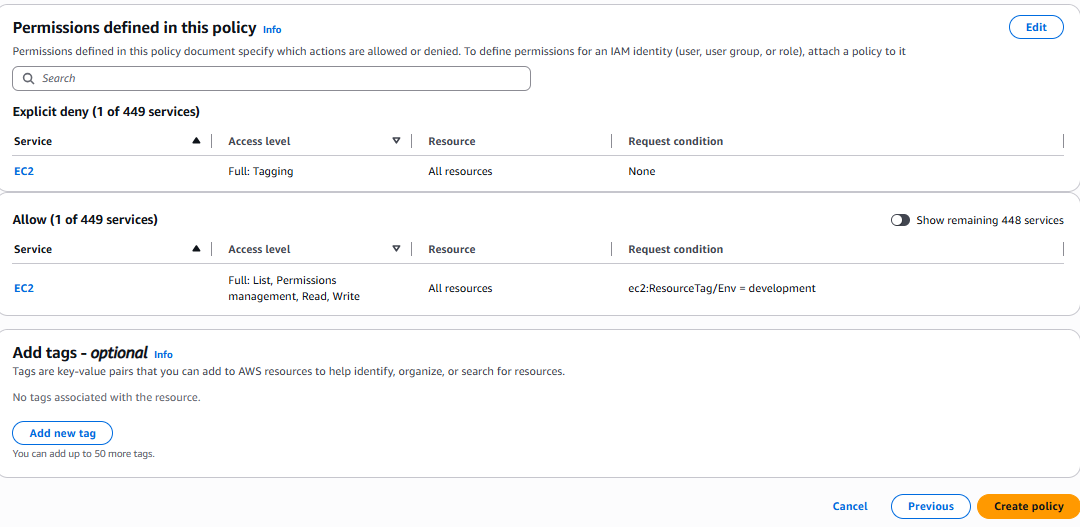
**Step 13:**Enter the JSON Code & Then Click on next.



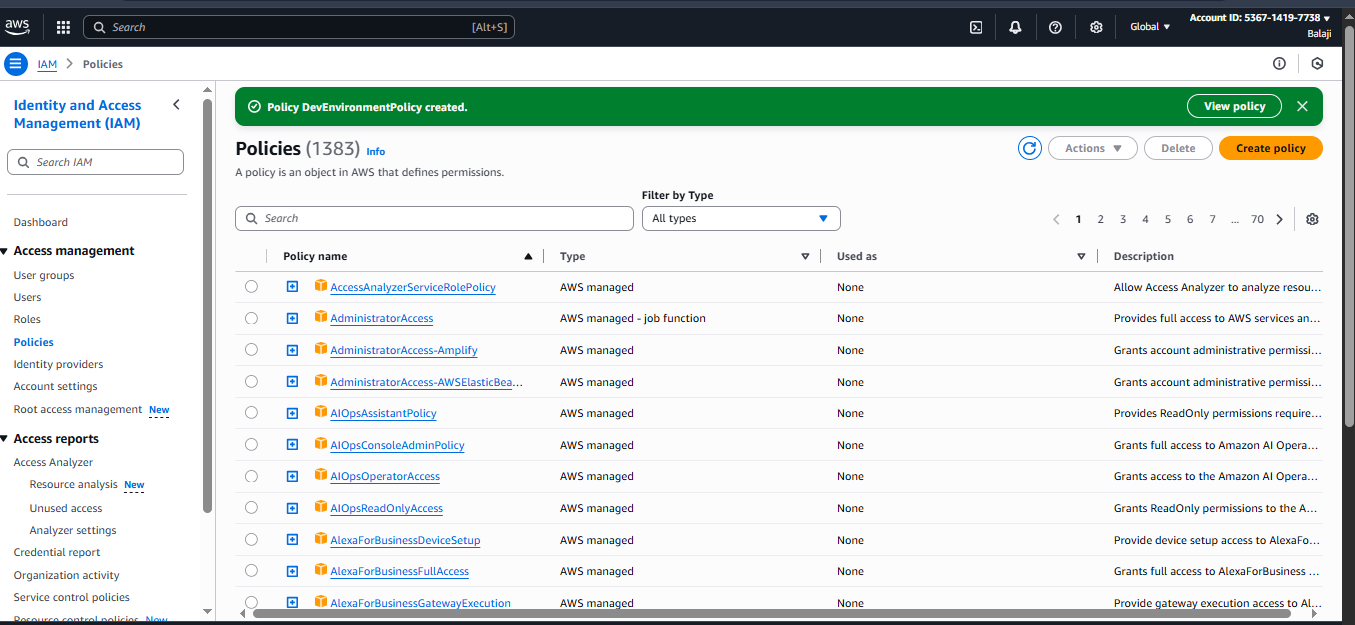


**Step 14:** Enter the name of the policy & Click on create Policy.





**Step 15:** Successfully IAM-Policy Has created.

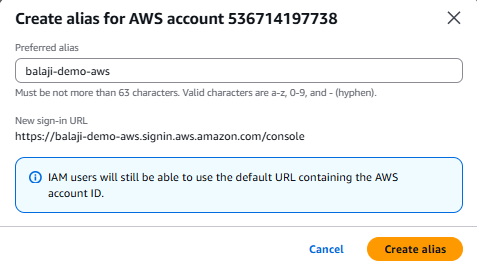


Step 16: Go to IAM Dashboard & Click on Create Account Alias

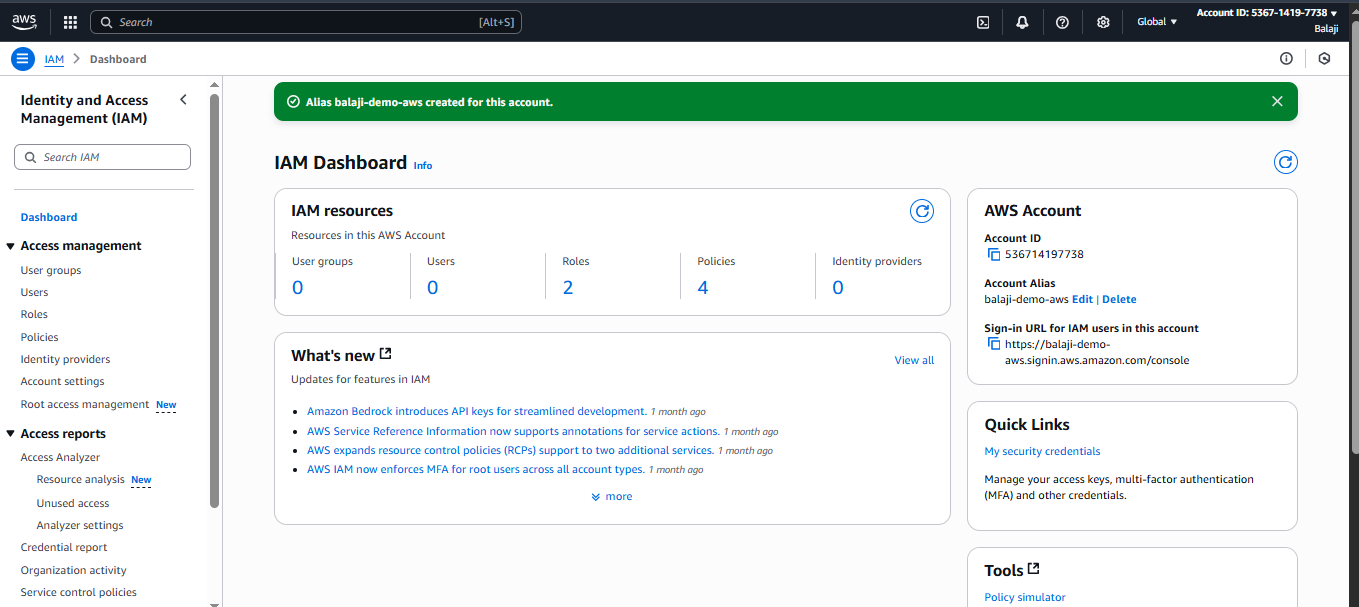
Account Alias is simply a nickname for our AWS Account instead of a using long Account ID we can have Account Alias.



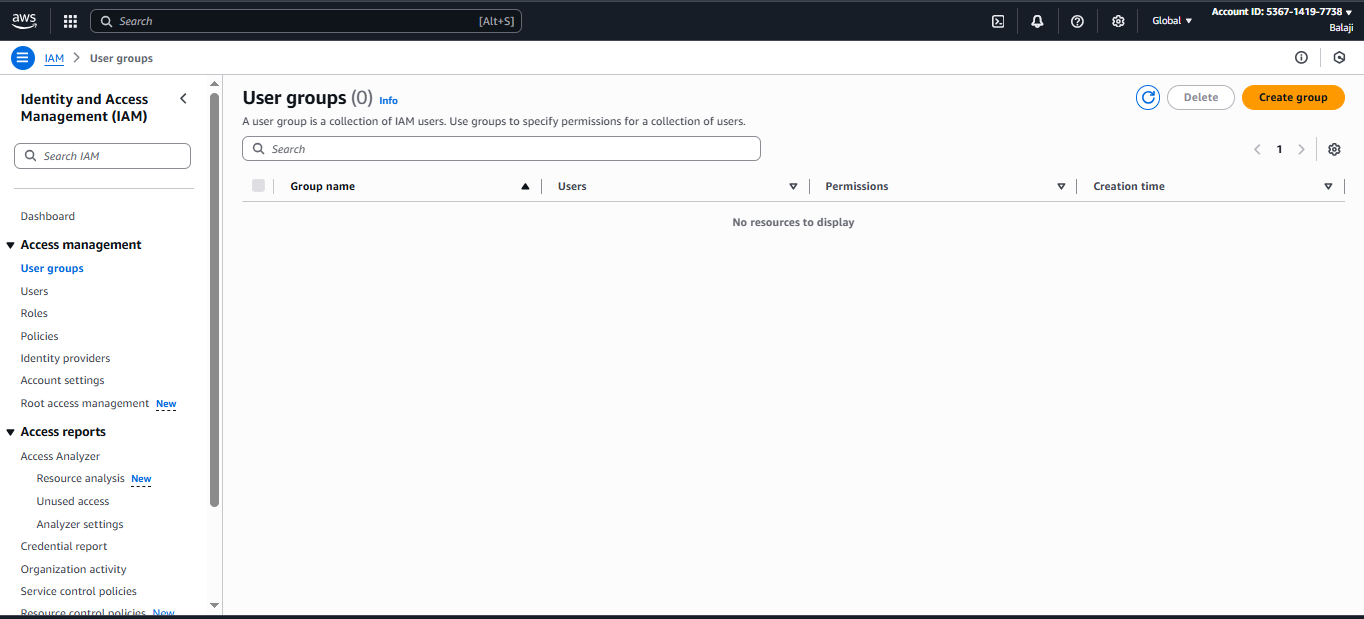
Step 17: Enter the alias name & Click on create Alias.



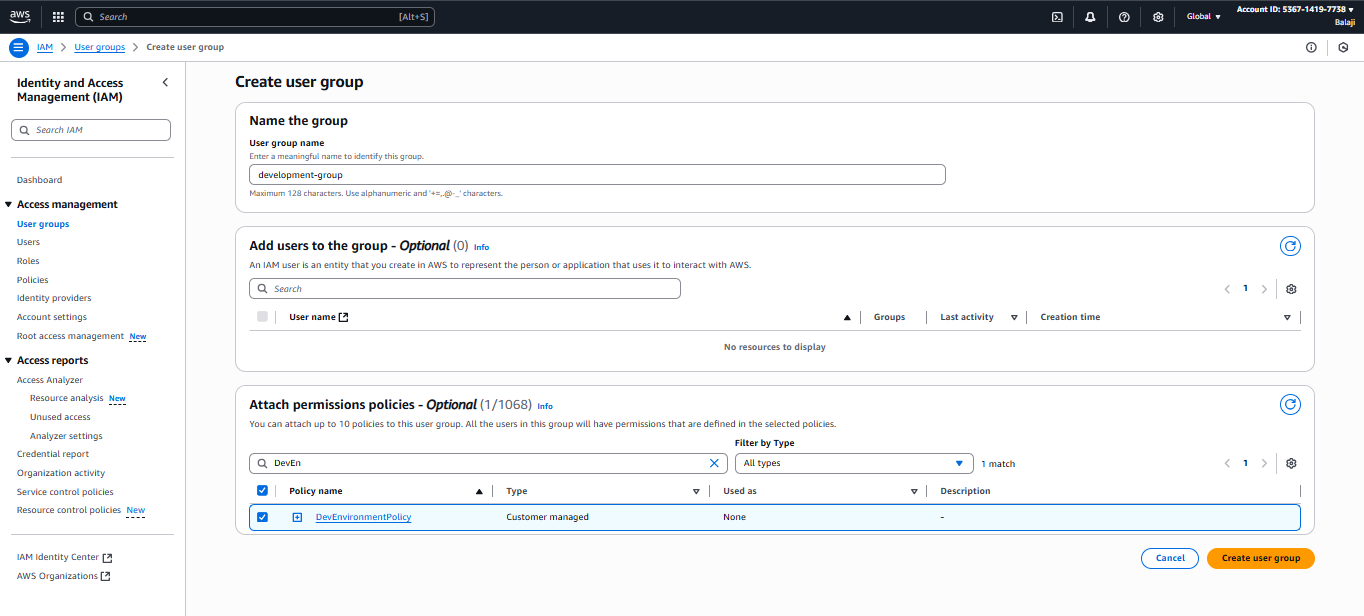
Step 18: Successfully Account alias is created.



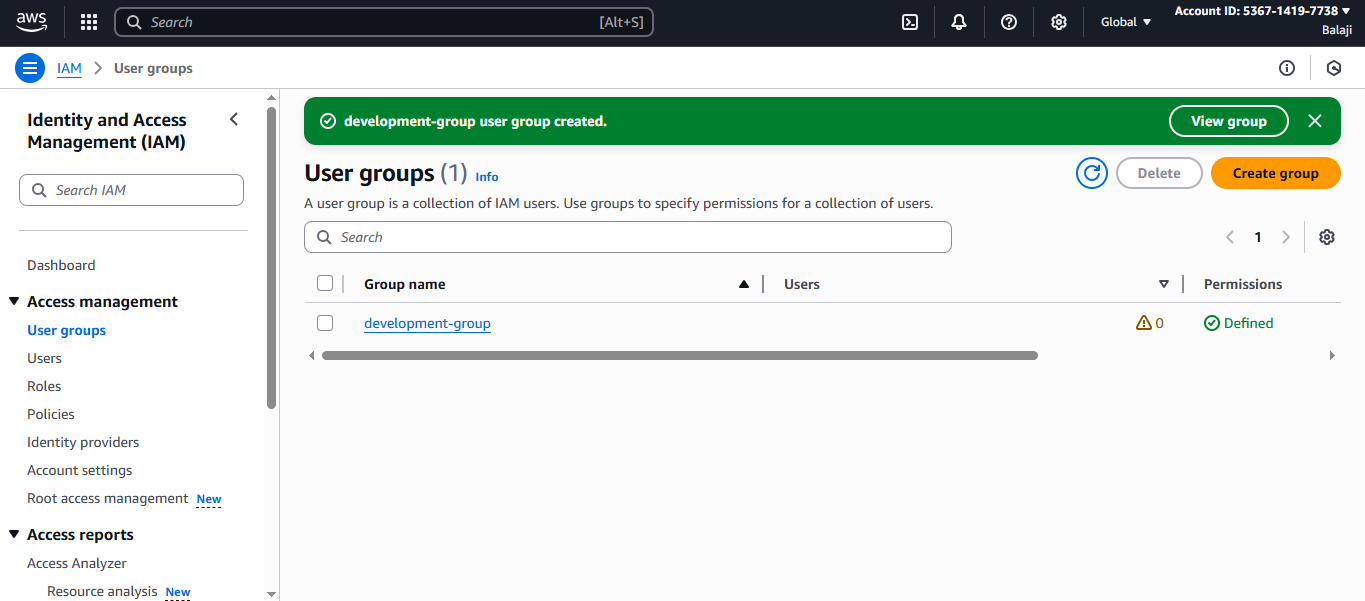
**Step 19:** Go to User groups in IAM & Click on create group tab.



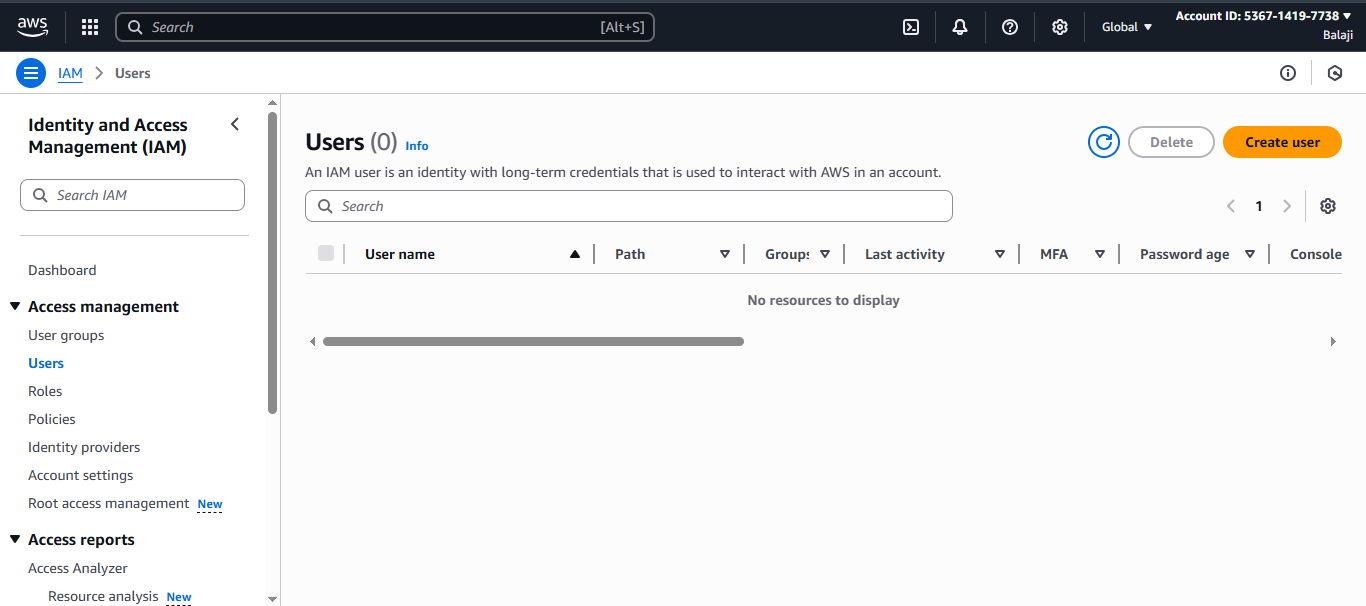
**Step 20:** Enter the name of the Group, Attach permission policy which we created earlier & Click on create Group.



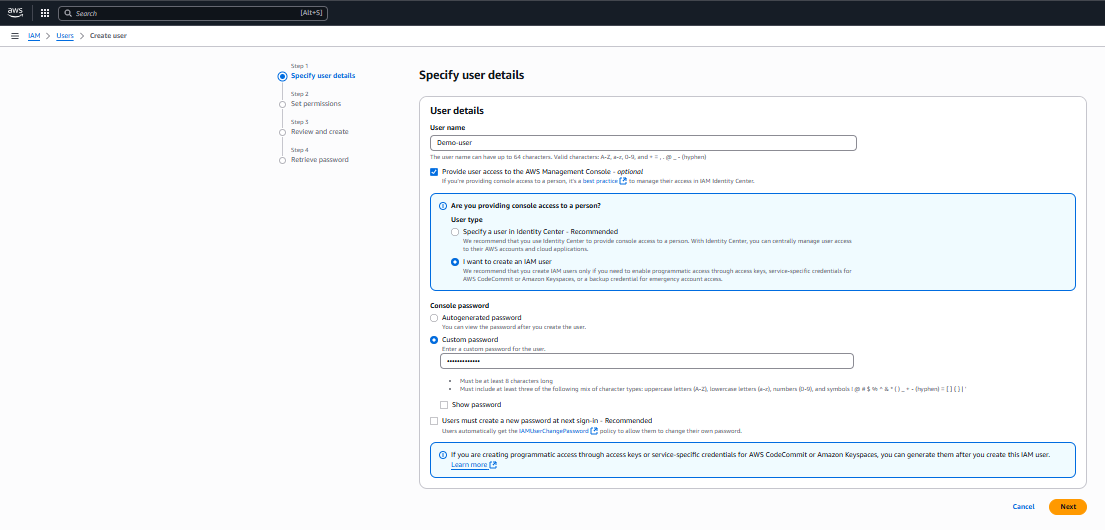
**Step 21:** User group is successfully Created.



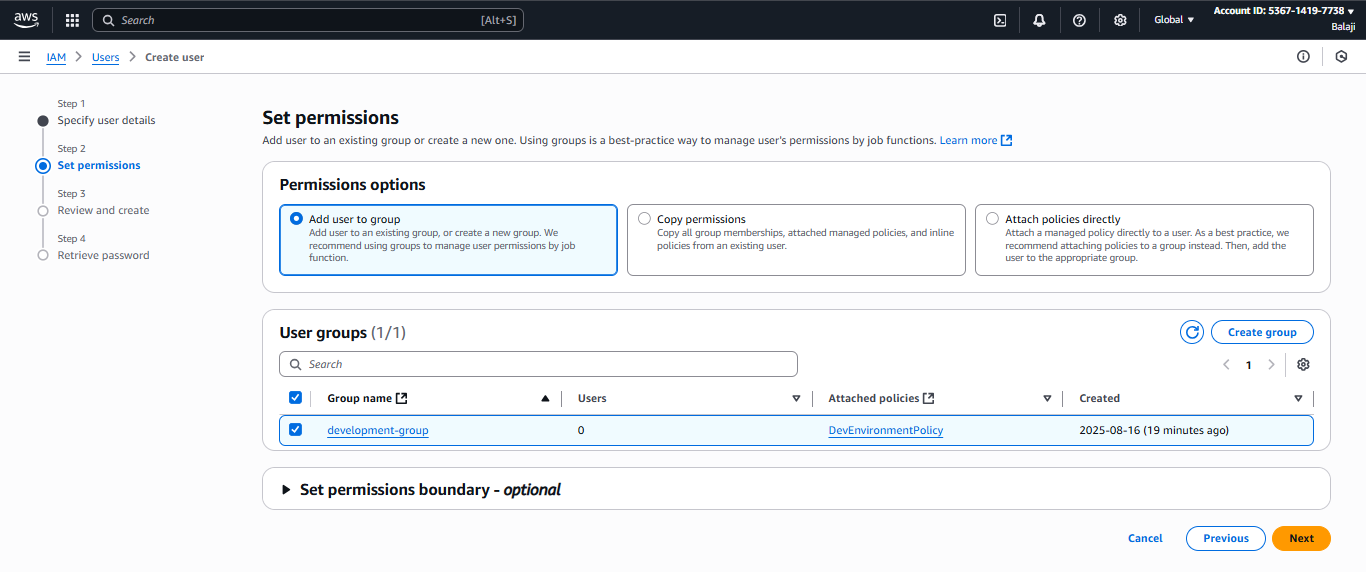
**Step 22:** Go to Users & Click on Create User.



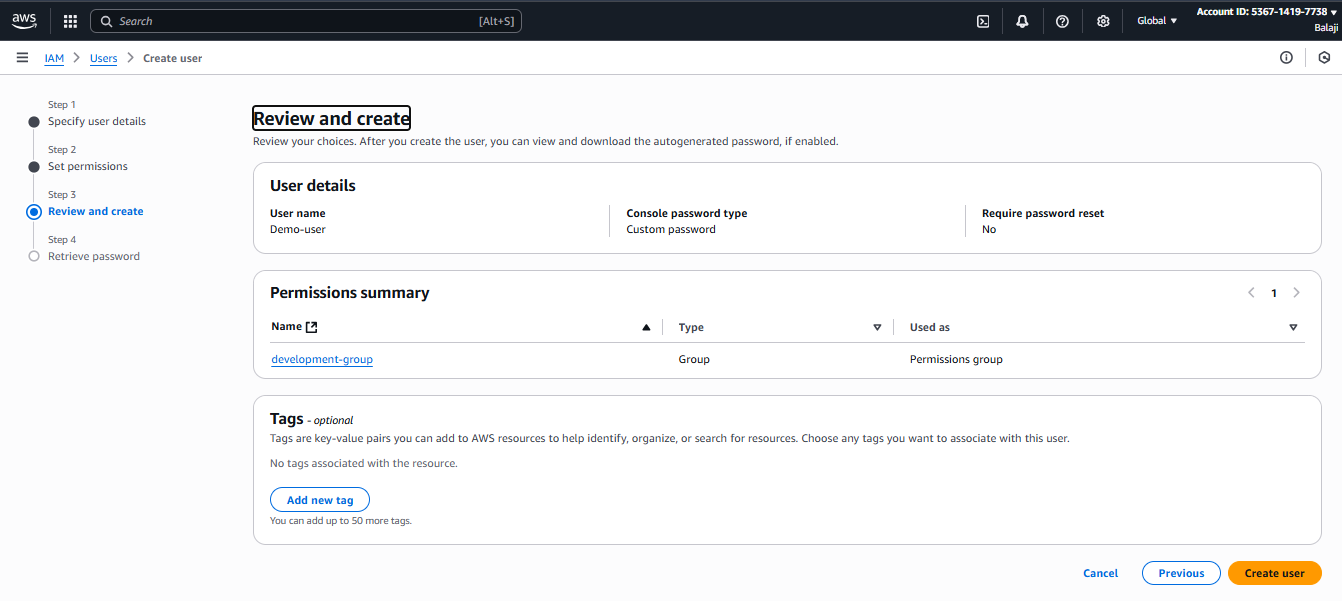
**Step 23:** Enter the name of the user & set the own custom password, Then Click on next.



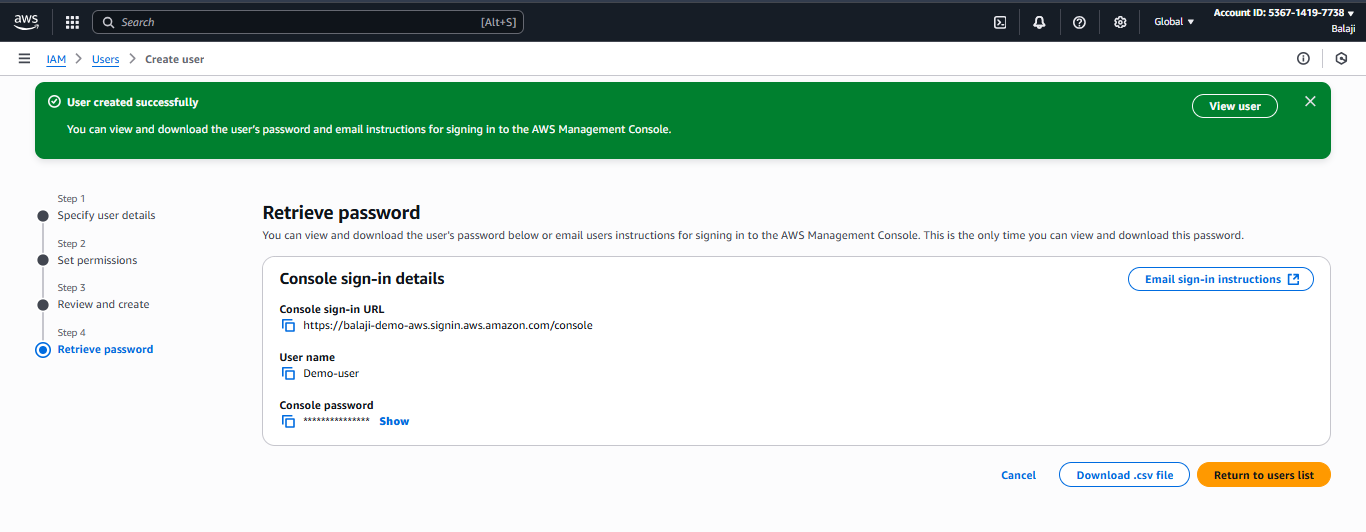
**Step 24:** Add the User group & click on Next.



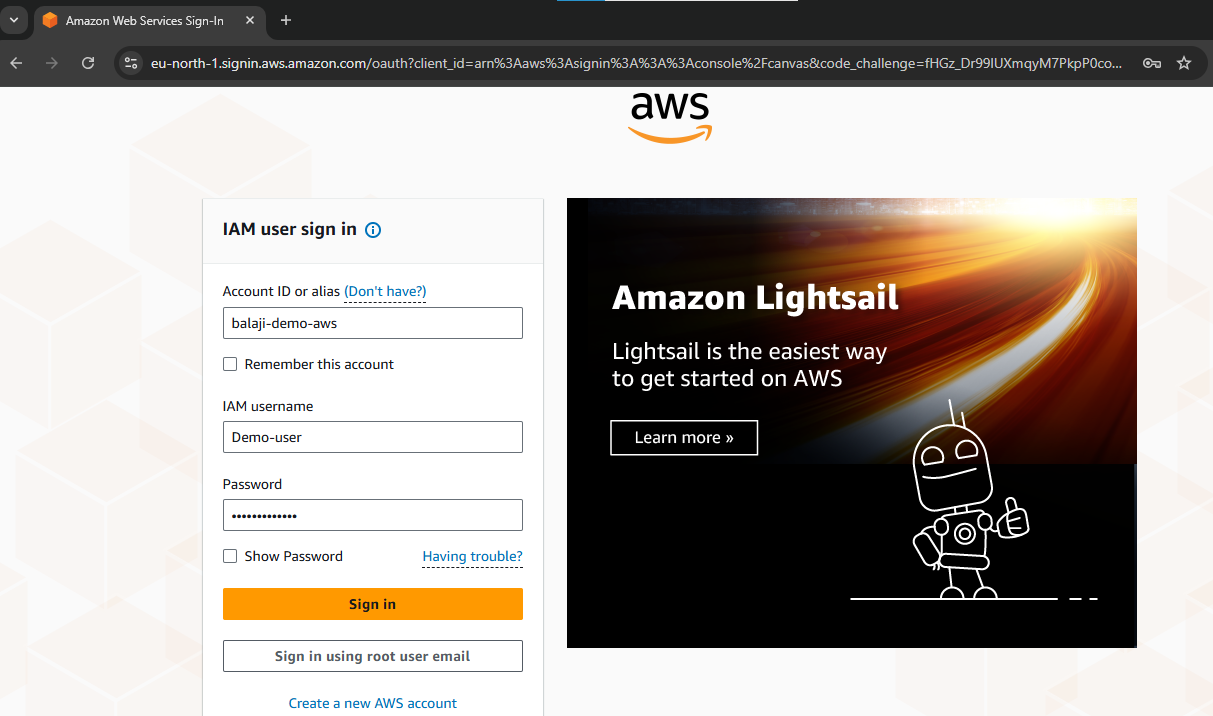
**Step 25:** Click on Create User.



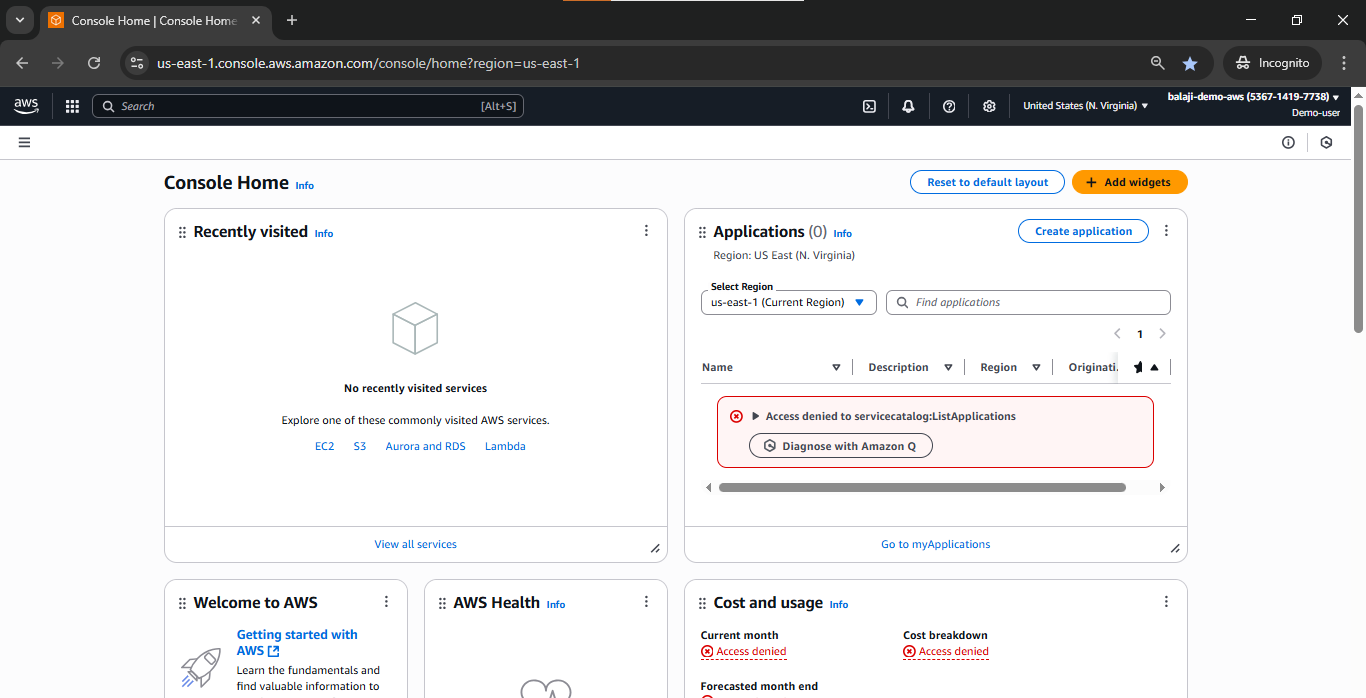
**Step 26:** Successfully created the user, Download the CSV File & Copy the Console sign-in URL.



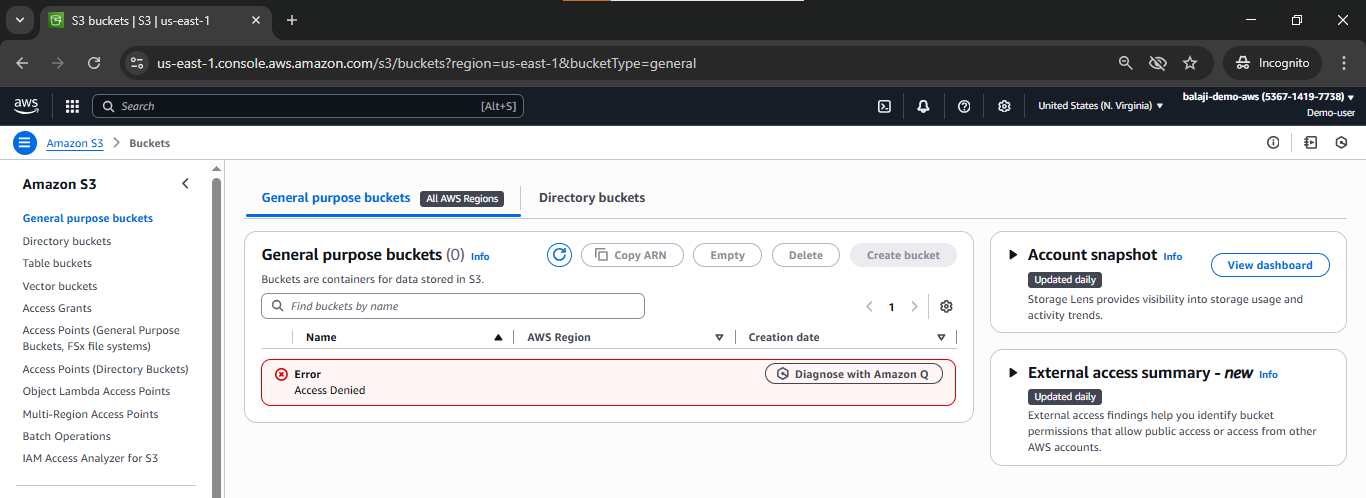
**Step 27:** Paste the URL in the new tab & Enter the IAM Username & Password and click on sign in.



**Step 28:** User is successfully Logged-in.

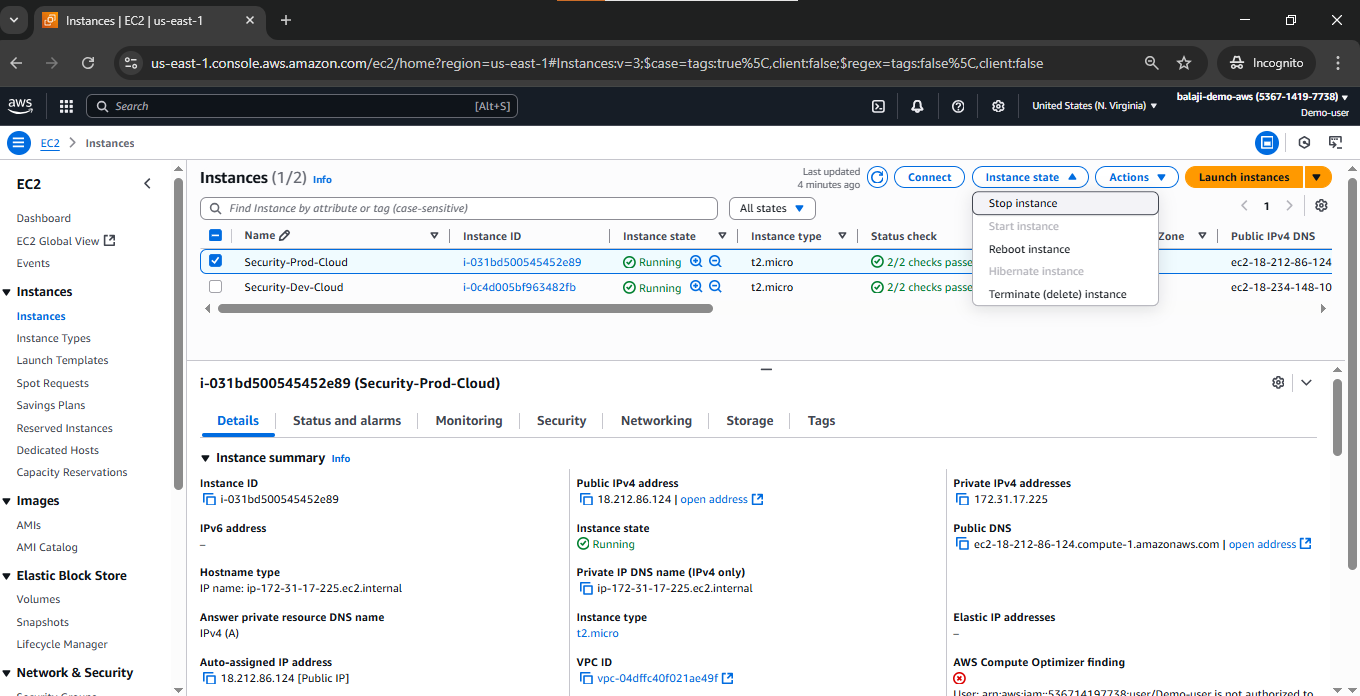


**Step 29:** User can Test if User can access s3.

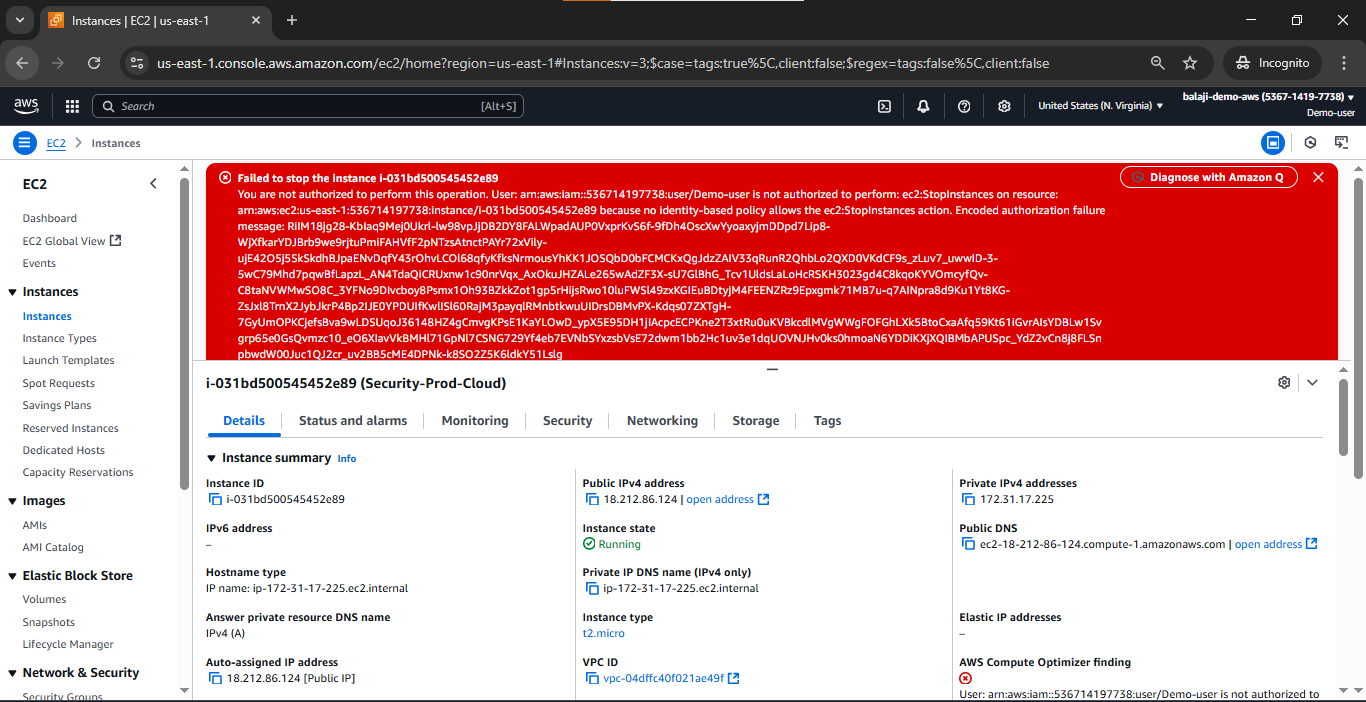


**Step 30:** Tested successfully s3 is showing access denied error because user has only access to EC2 instance based on the created IAM policy and attached in the user group

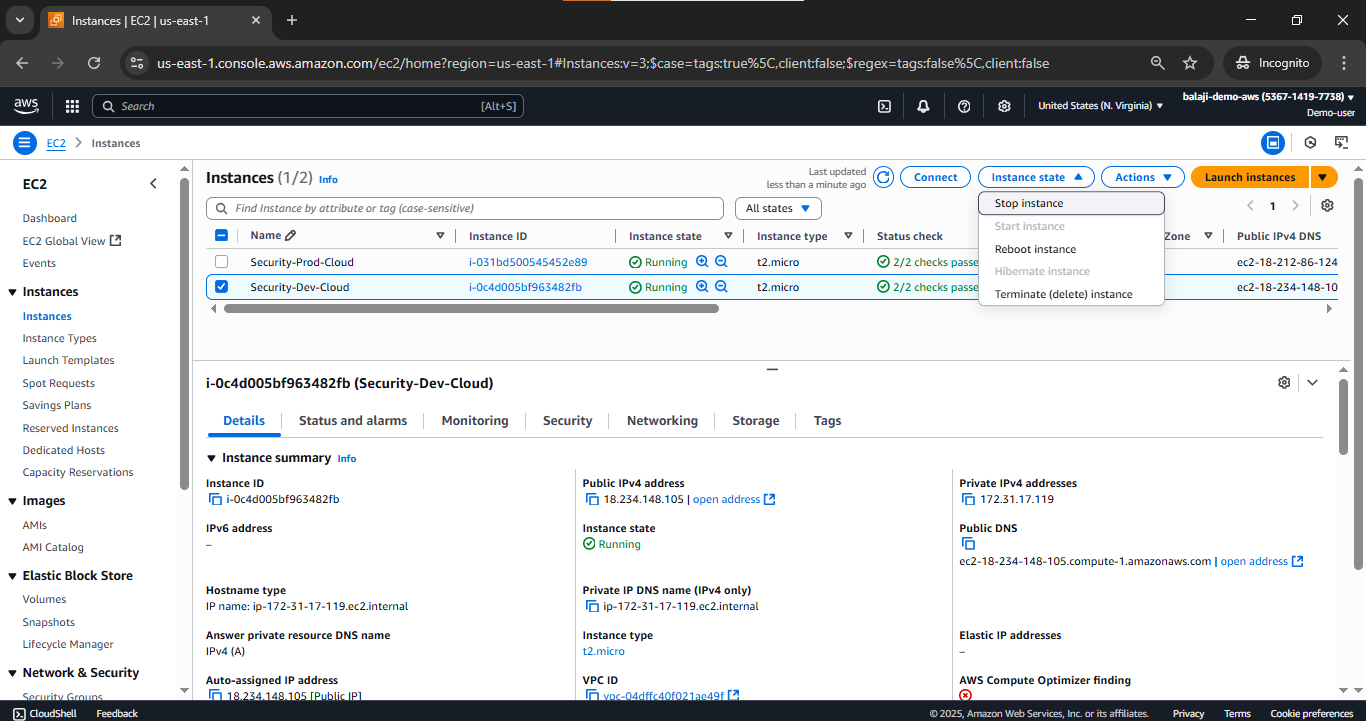
**Step 31:** Go to EC2 instance & Try to stop the instance.



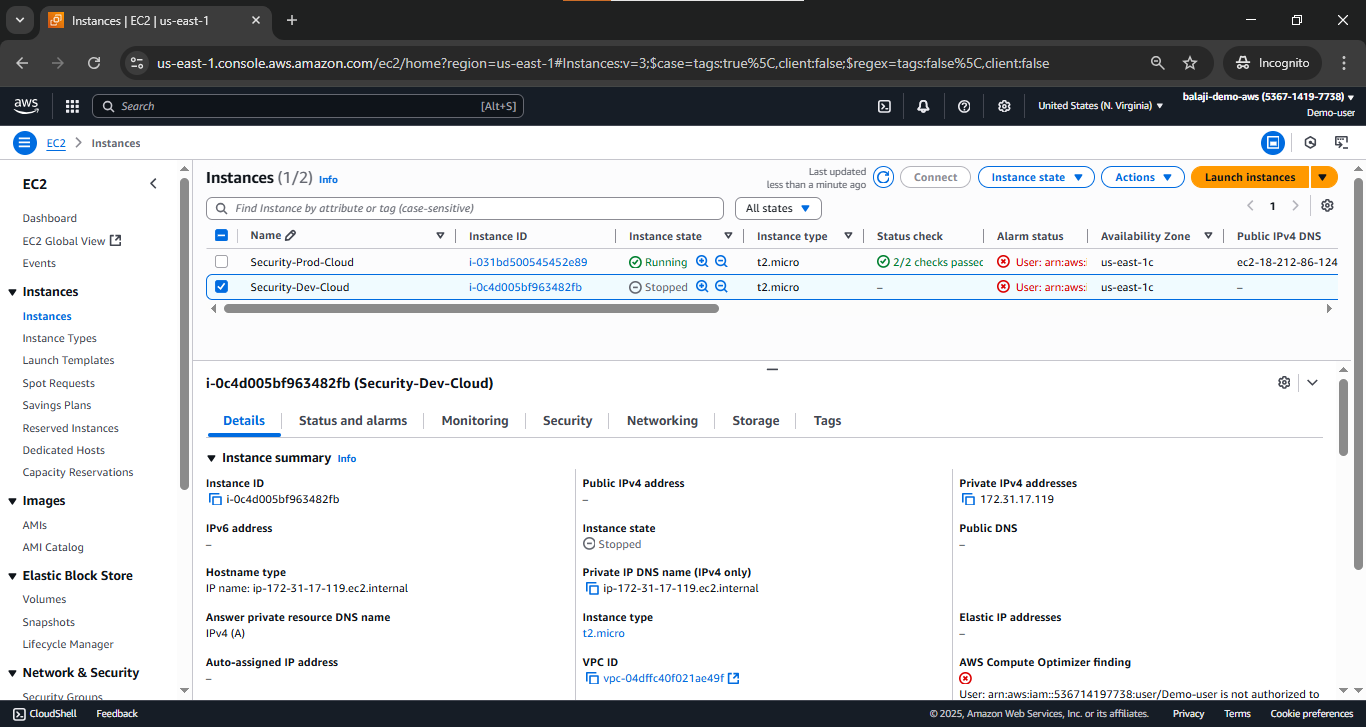
**Step 32:** Error while stopping the EC2 instance because user do not have the right Permission to stop the Production Environment(Instance).



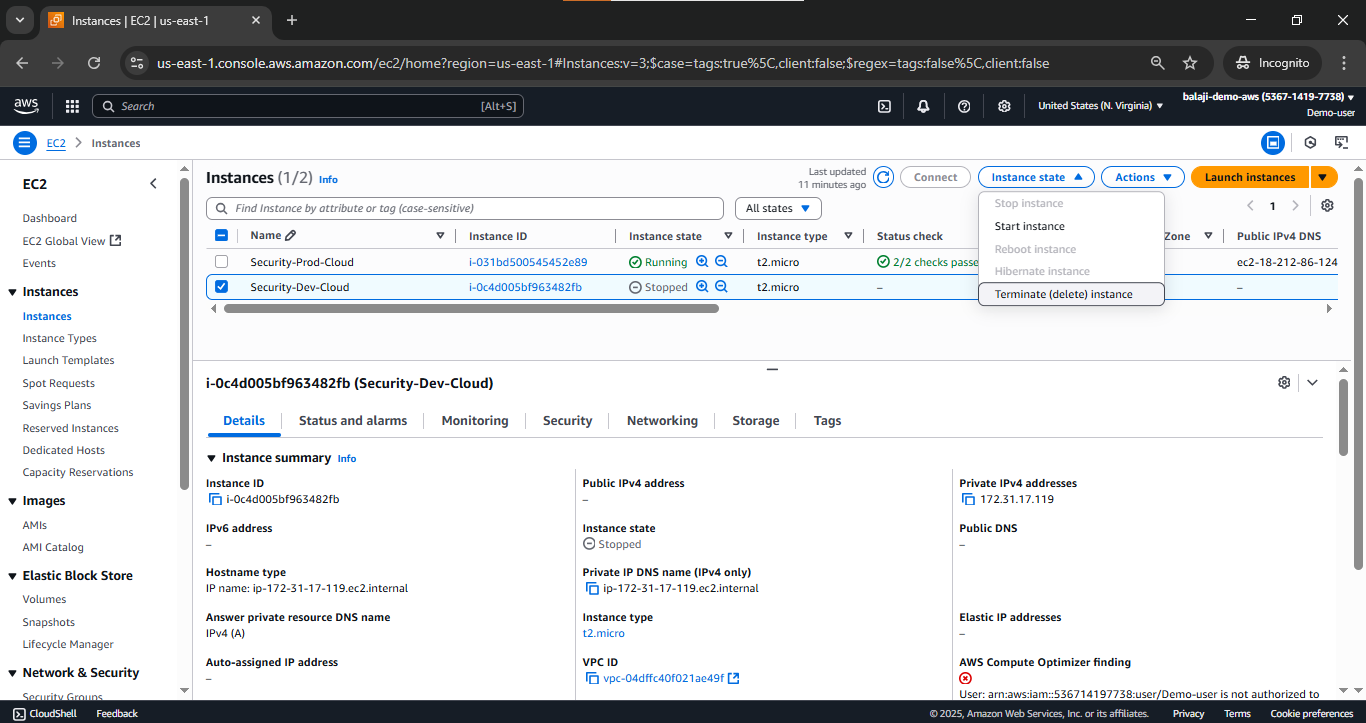
**Step 33:** User is trying to stop the development Environment (Instance)



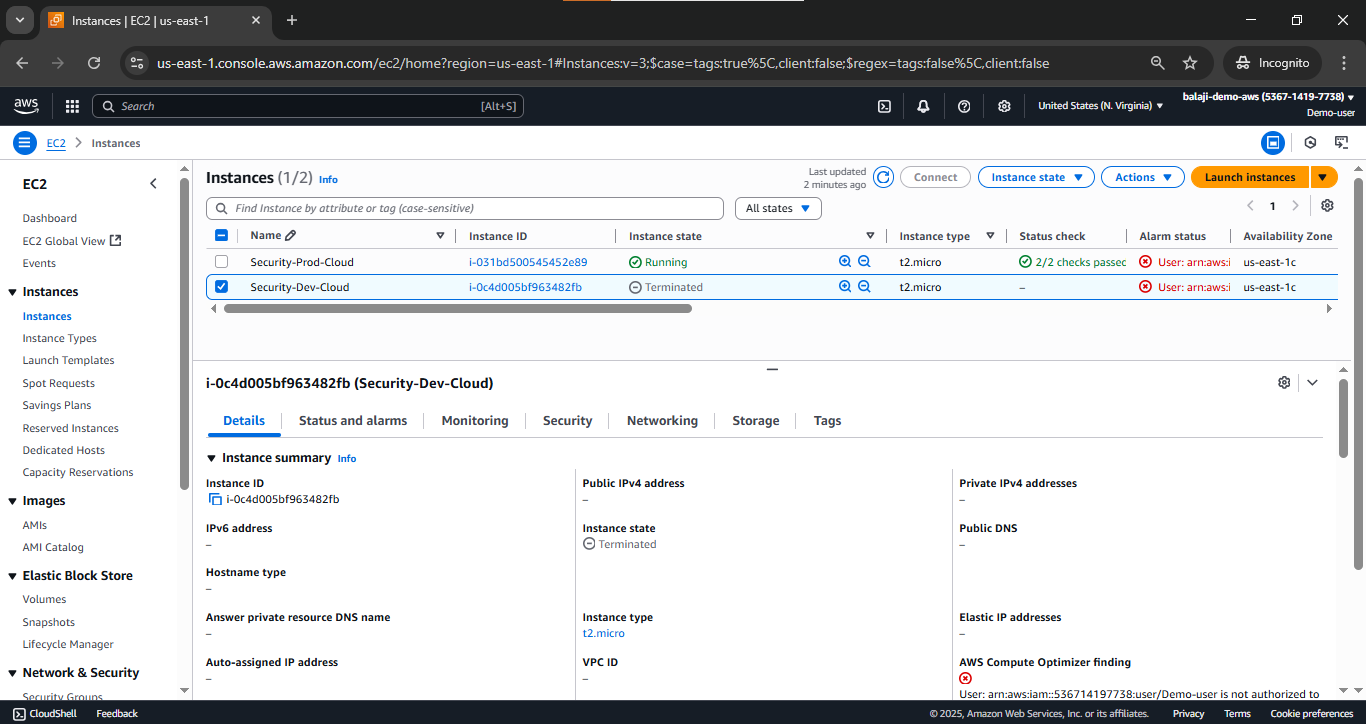
**Step 34:** Now, Development Environment (Instance) Has been Stopped



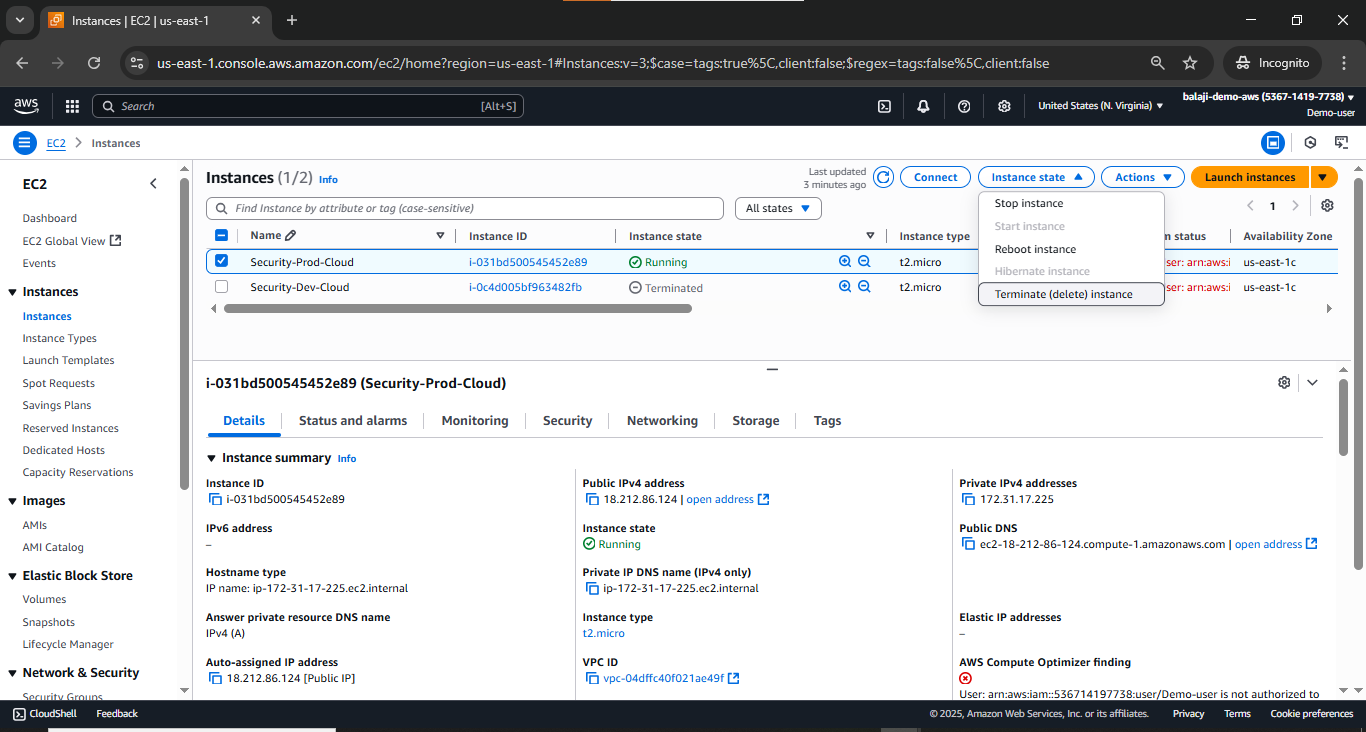
**Final Result – 1:** User is trying to Terminate(delete) Instance -Development Environment.



User has Successfully Terminated.



**Final Result – 2:** User is trying to Terminate(delete) Instance - Production Environment.



Access Denied because user do not have access on production Environment (Instance)

