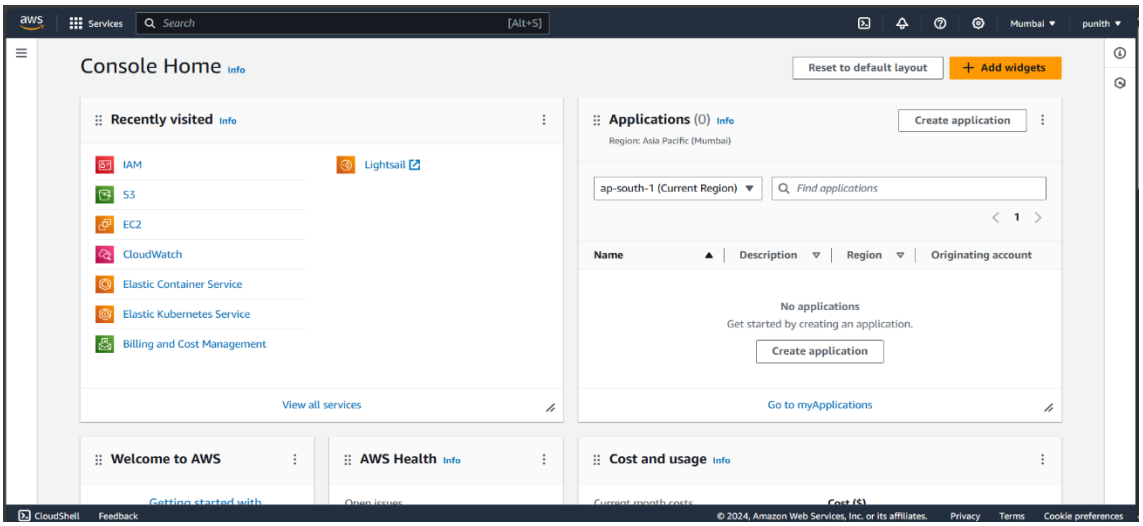
AWS IAM (Identify Access Management)

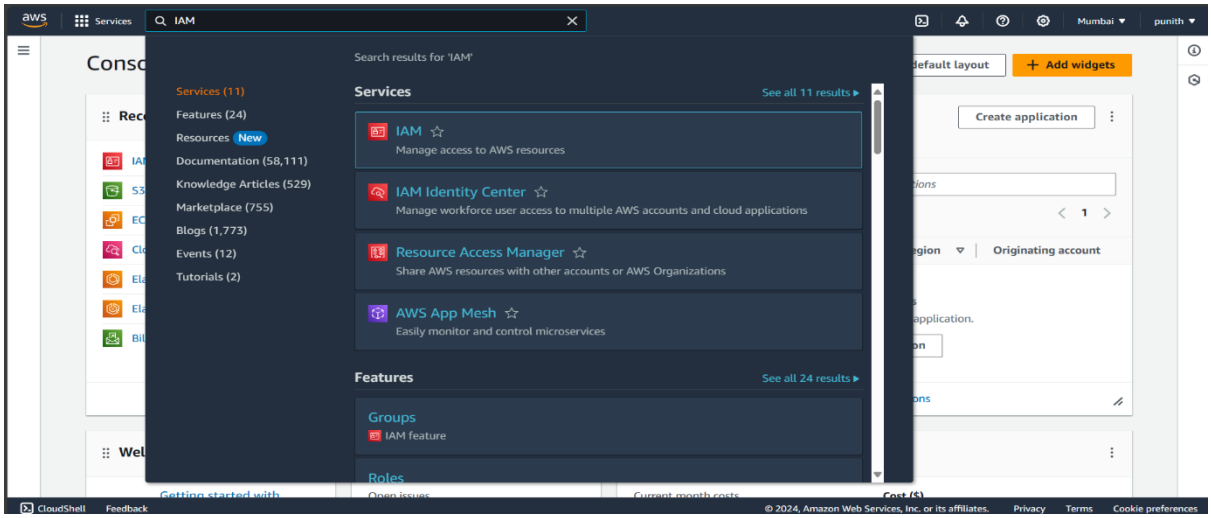
- IAM(Identify Access Management) is a service in AWS(Amazon Web Services) that provides user-level configurations for the user from root account.It is actually all about Authentication and Authorization and it also provides four set of actions to perform in the AWS cloud platform. They are: 1) Users
  2) Policies
  3) Groups
  4) Roles
- Users: Users are those who can access the services for some extent with few set of permissions and policies that are made by admin i.e root user. For example, if a user wants to access the EC2 services , then the root user provides the permissions to access the the EC2 and perform few set of actions like creating instances, launching instances.
- Policies: Policies are the set of permissions that are given to user account in IAM. They let the users to perform any action in the entire AWS account.
- Groups: In IAM , Groups are combined of multiple users that can perform the actions in AWS and the permisssions are given easily to users. For example, if a organization has the three teams i.e Dev, QA, Production then we have different groups for each team and it makes easier to add users to respective groups.
- Roles: Roles are way similar to the users and it also helps to create user with specific permissions for temporary uses. It also can be created outside the AWS account and can access another AWS account i.e Cross-Account Access.

- Now , we see the hands-on with IAM and the photos has been attached below:

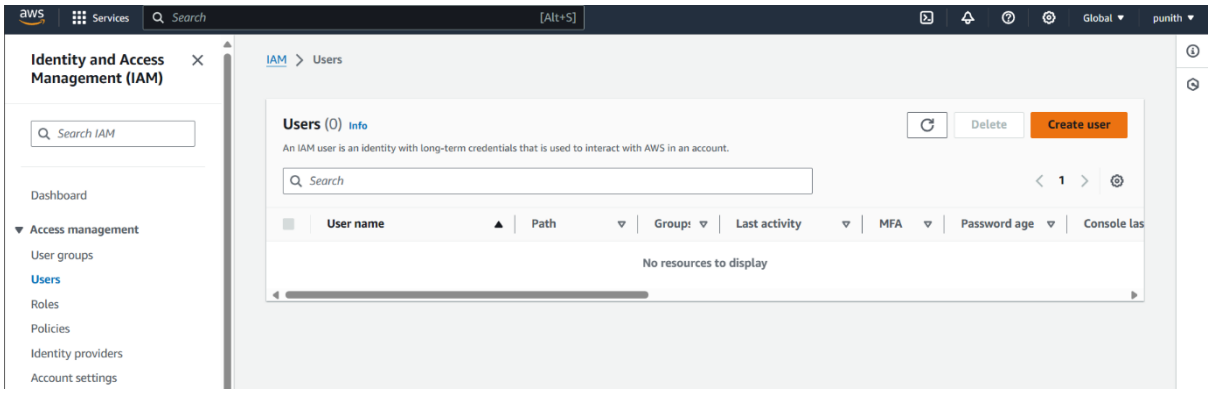
Login to AWS console.



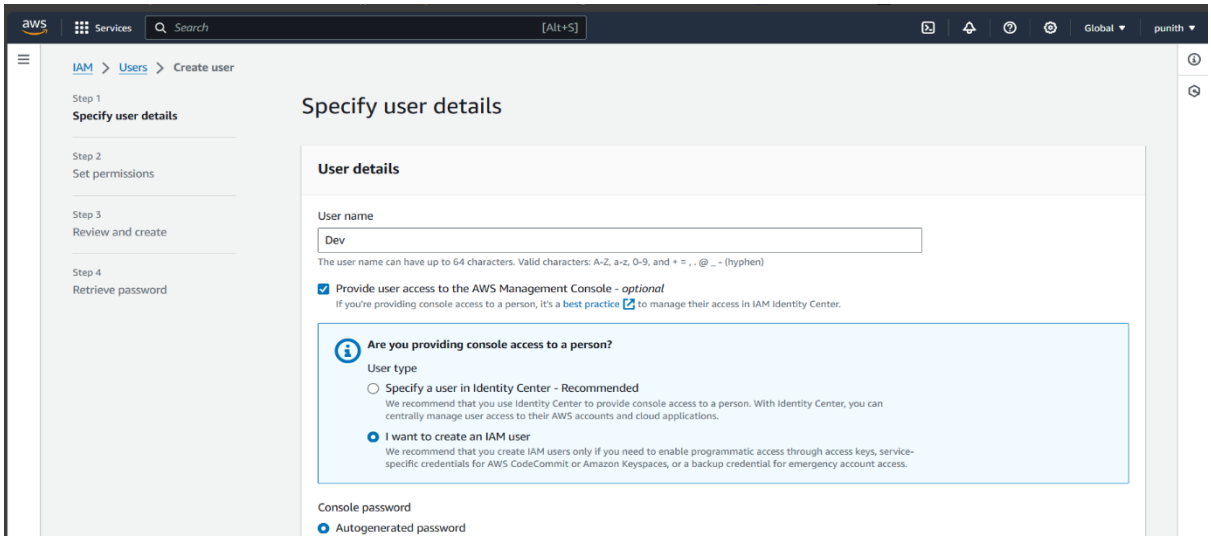
Search for IAM service.



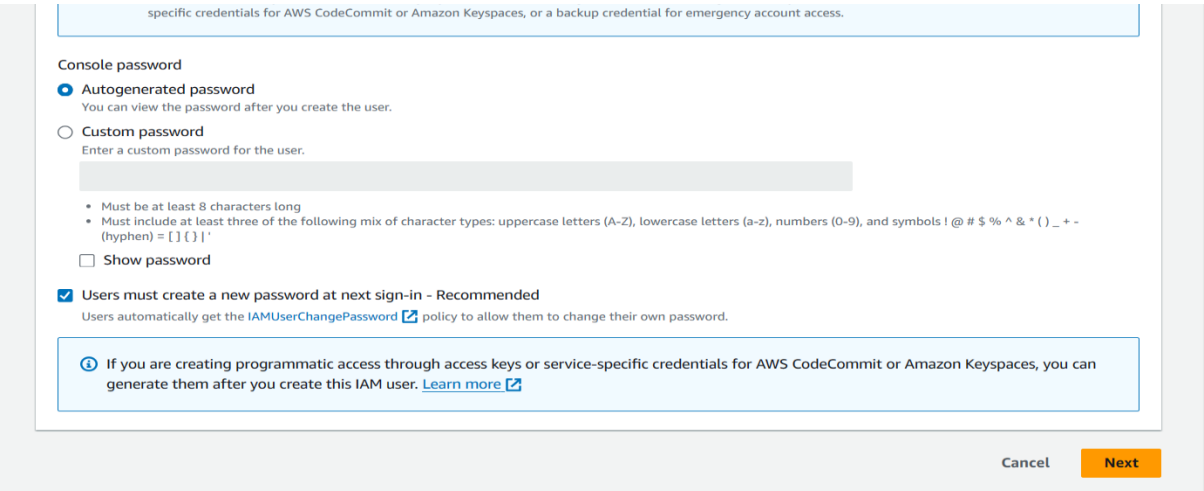
This is IAM interface and Now click on Create User to create a user .



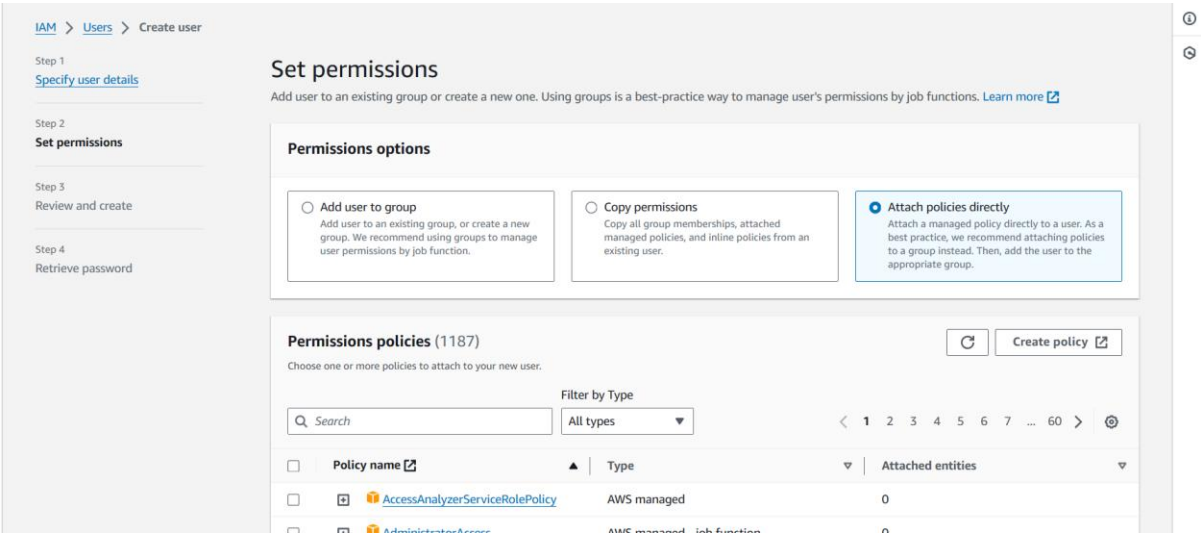
Name the User and Check the box to create a IAM user.



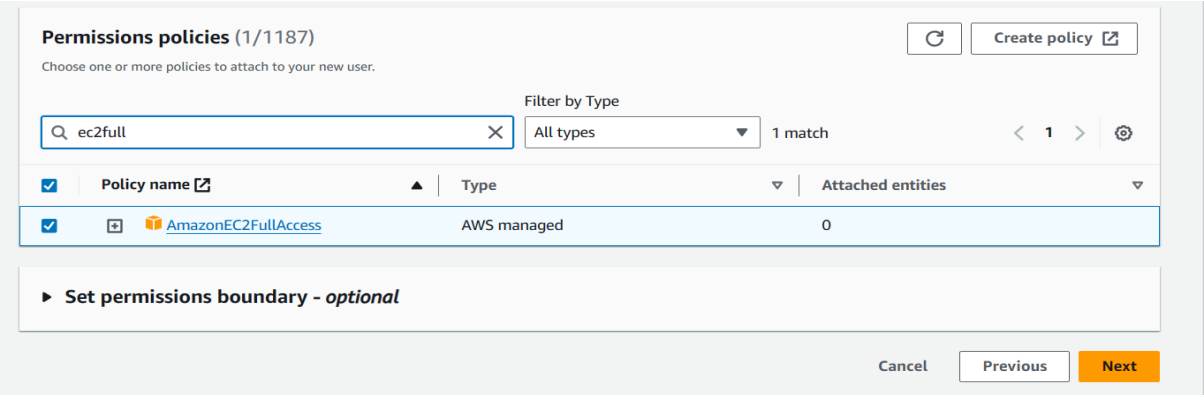
Make it autogenerated password for the first time and click on Next.



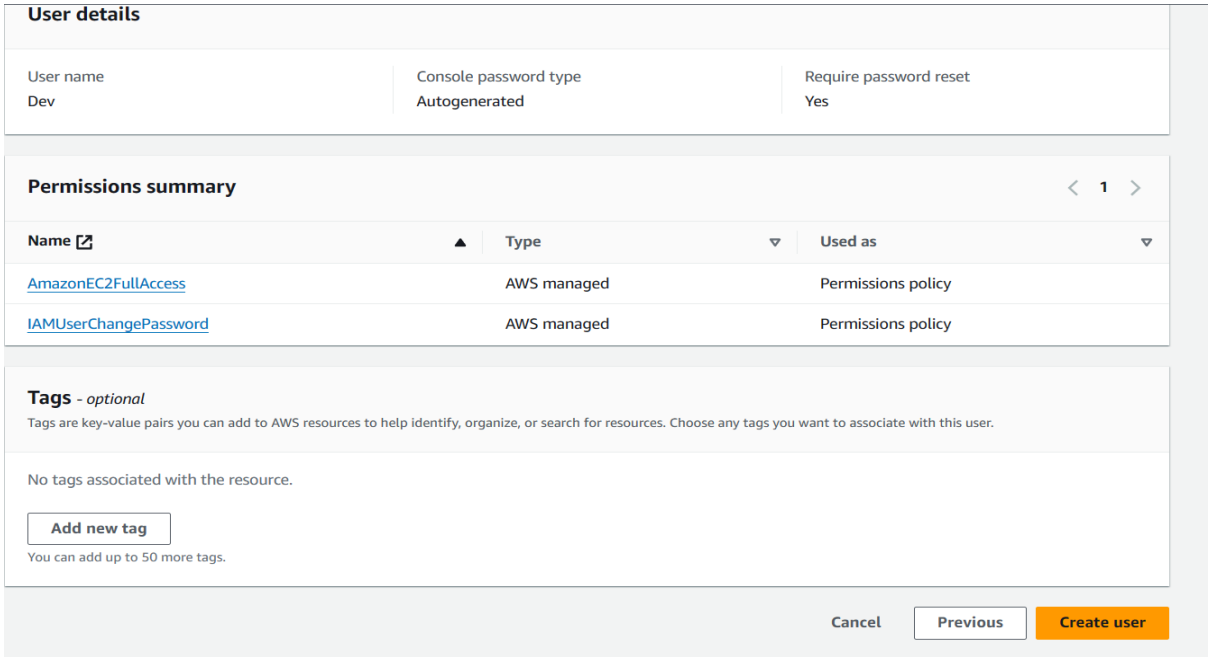
Set permission and select the policies that are to be given to user.



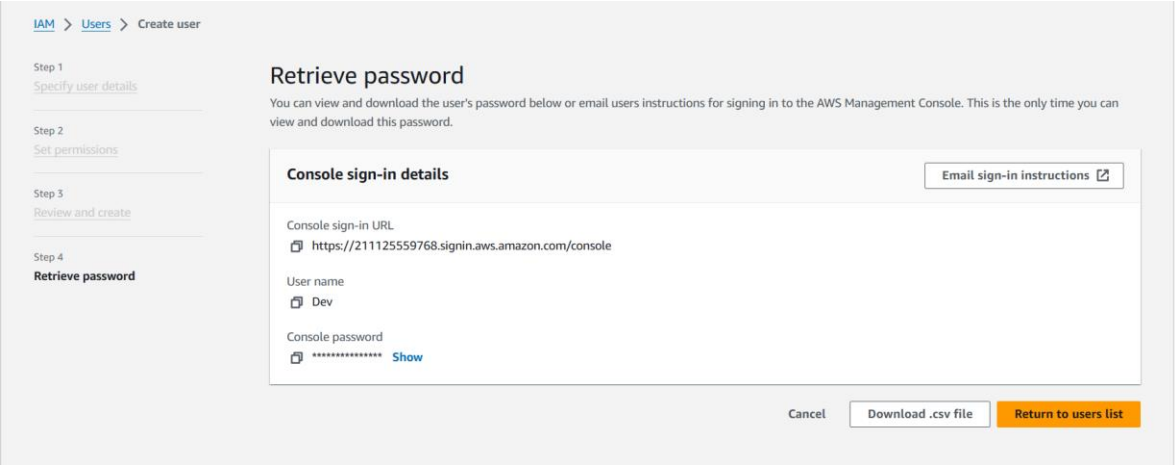
Search for EC2 and Check on to the policy and click on Next.



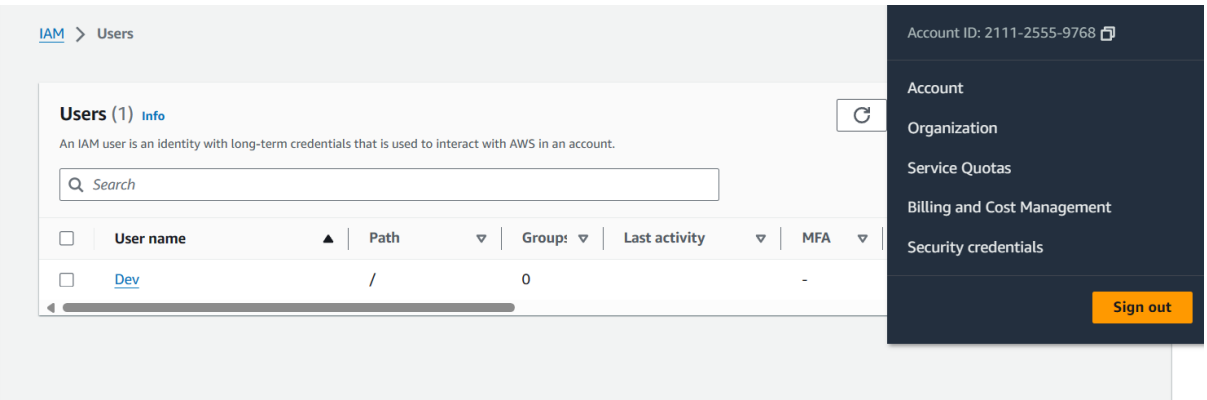
Review the details and click on Create User.



After creating user, you receive the password and account ID of the user.

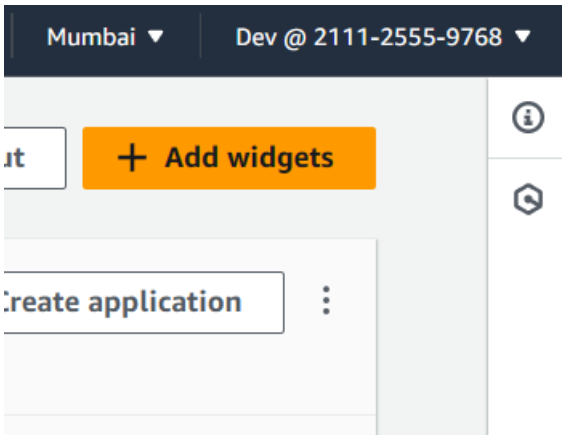


Sign out from the Root account and try logging with the user created now from IAM console.

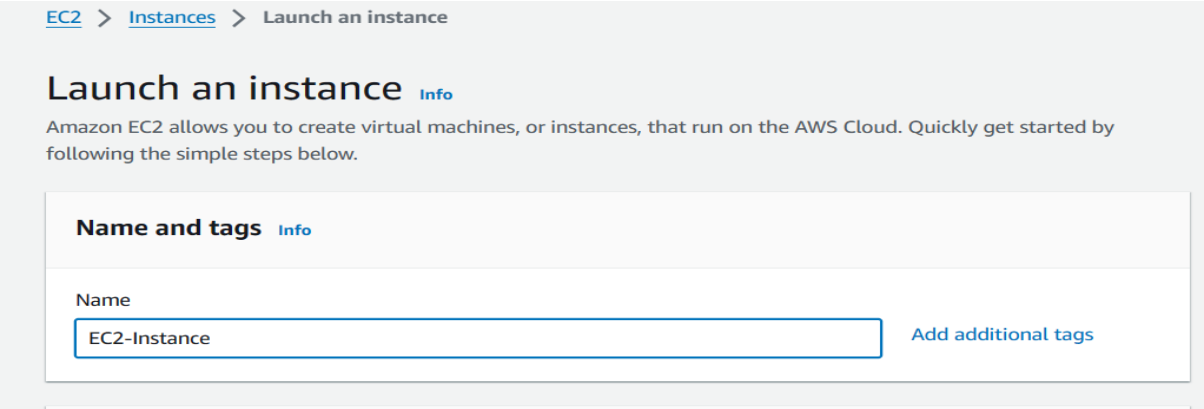


Enter the details and sign in into IAM console.

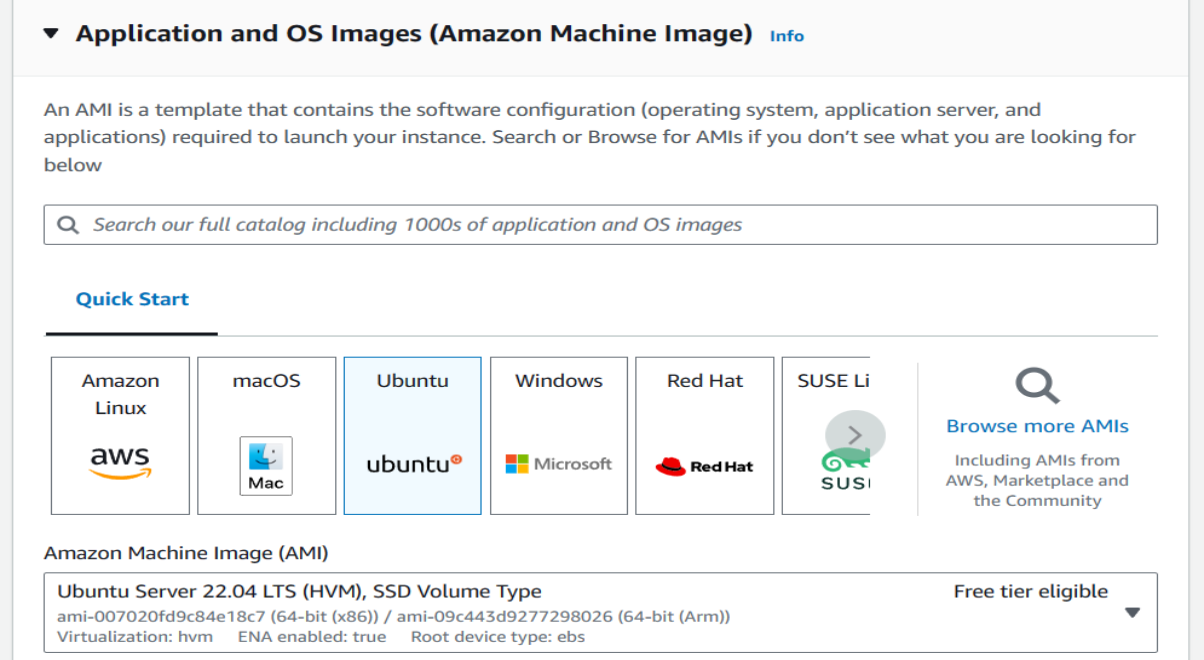
You can see , The user Dev is successfully logged into the IAM console.



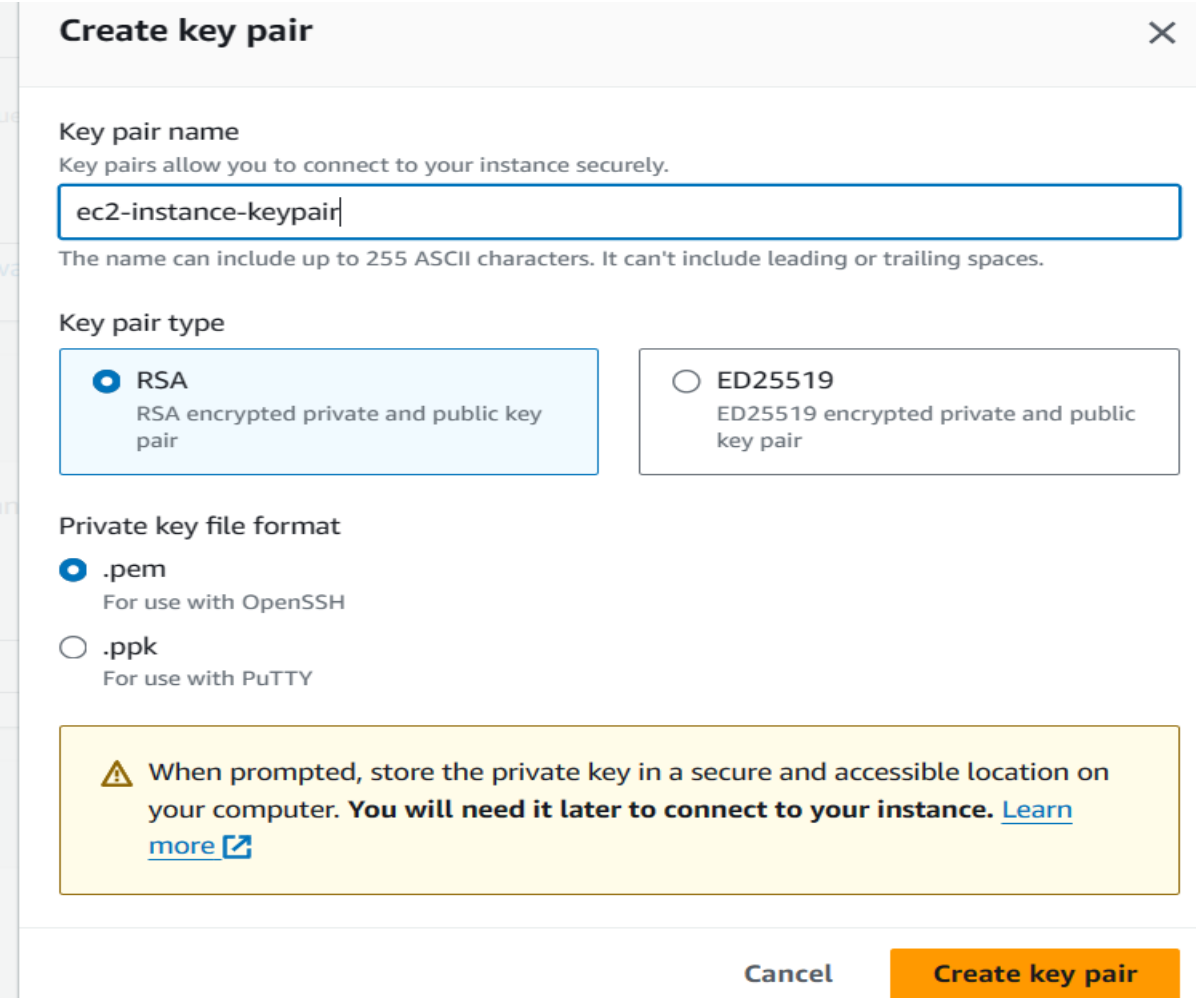
Go to EC2 and Launch an instance. Name the instance.



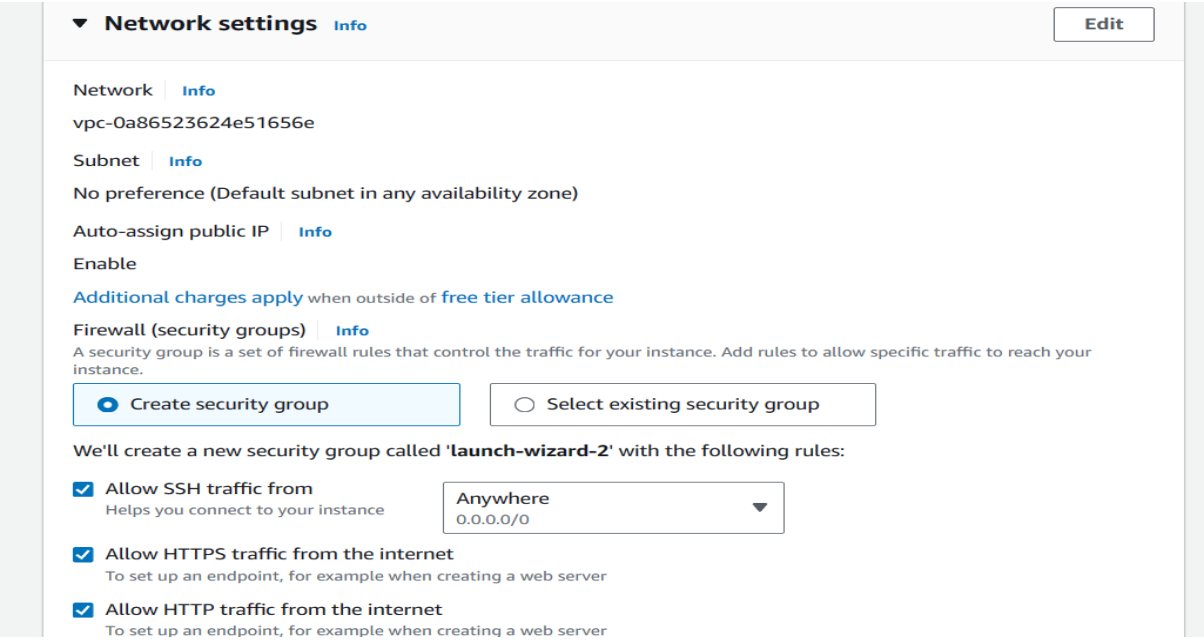
Select the OS images and version of the OS.



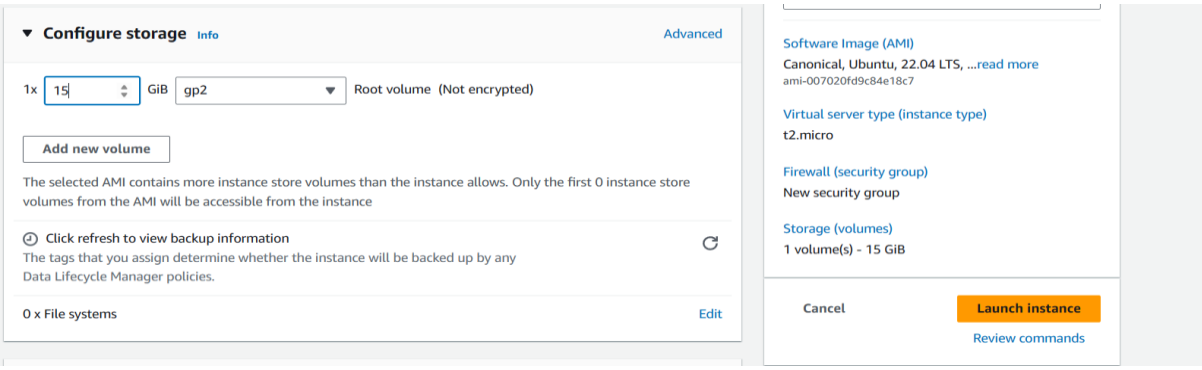
Create a key-pair for the instance. We will discuss deeply about OS instance type and key-pairs in the session of EC2.



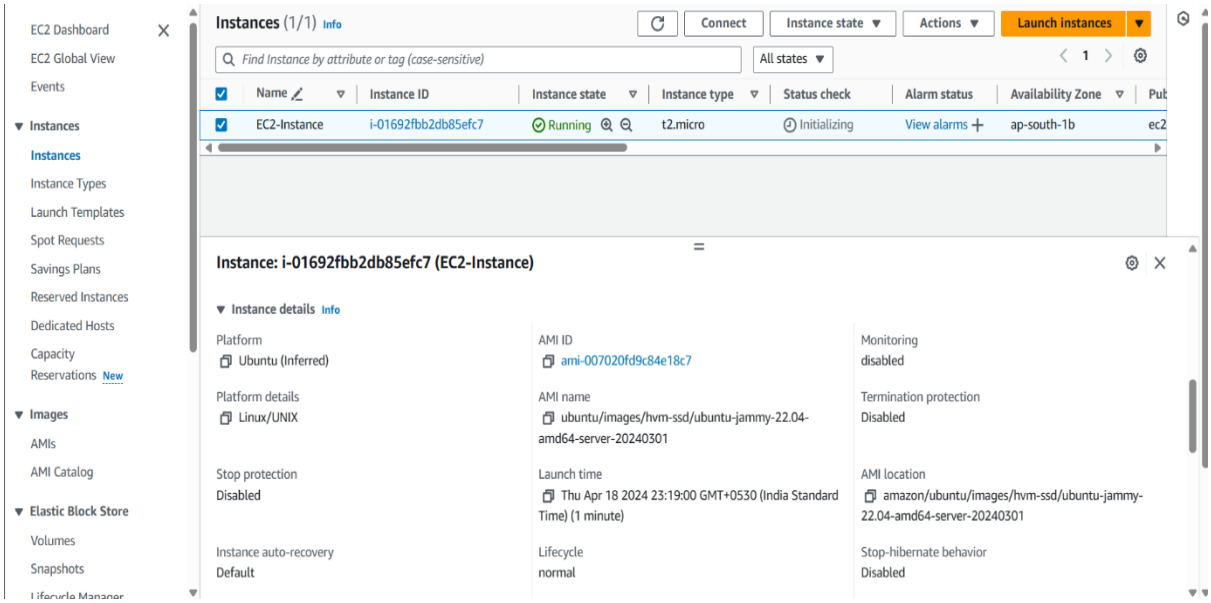
Create a security group and allow all protocols.



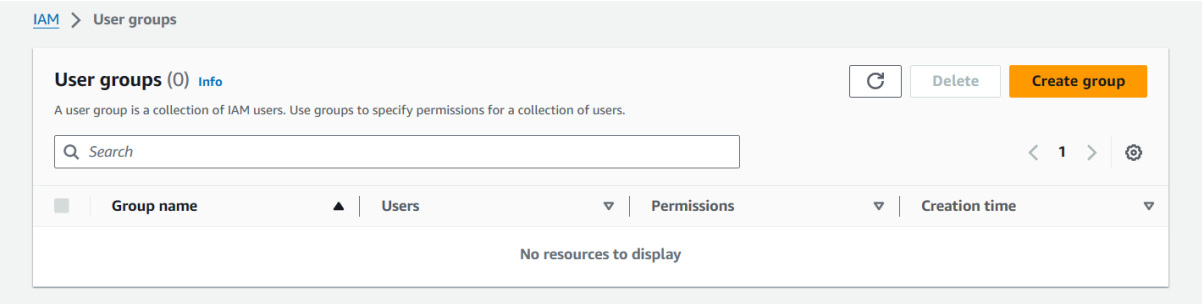
Select the size of the volume and Click on launch instance.



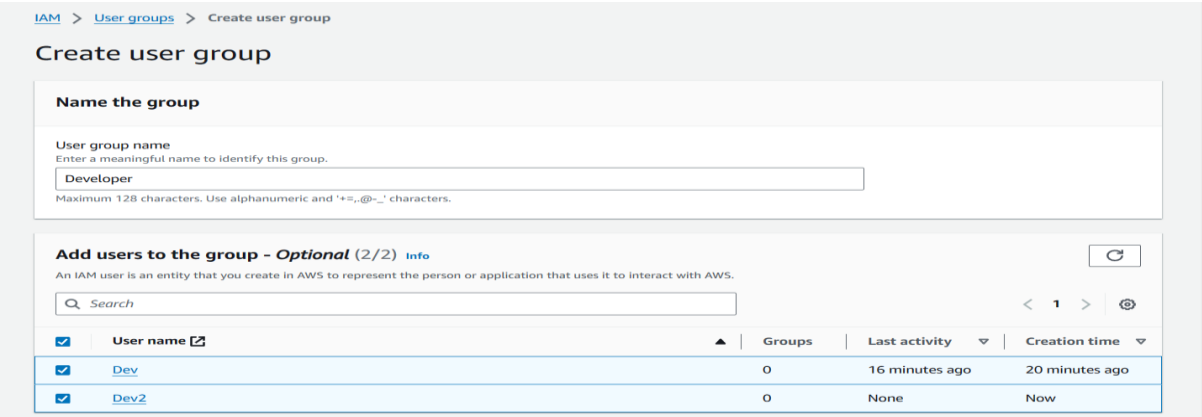
You can see, We have launched an instance but few permissions are disabled for the user Dev.



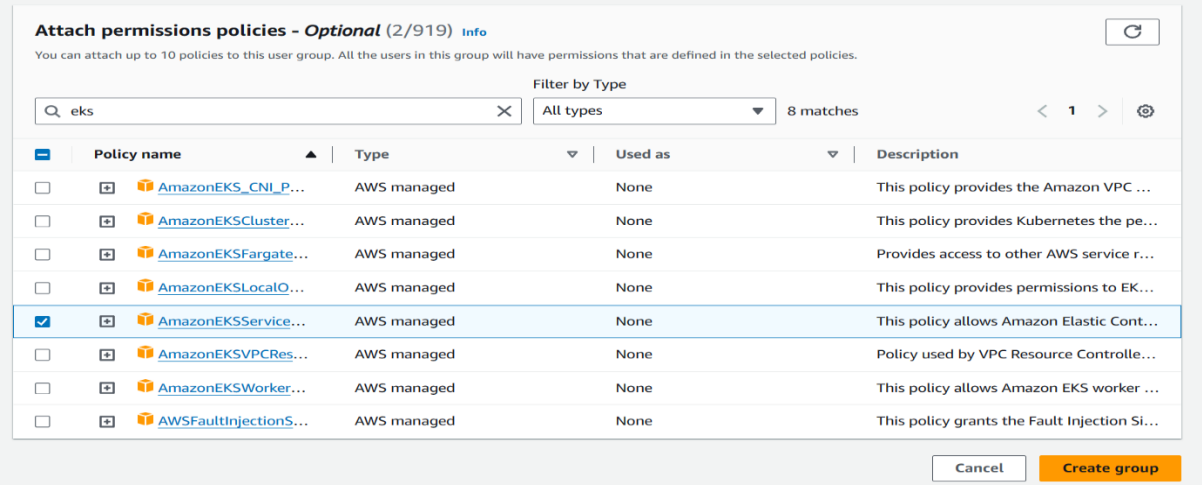
Now , sign out from user Dev and comeback to Root account and Open IAM to create Groups for Users.



Name the Group and select the users that you want to add in the group.Here, I have created two users and added them to Developer Group.



Attach the policy permissions to the group like EKS , EC2 permissions. Click on Create Group.



After creating, You can view the group and the Users, Permissions in the group