Identity and Access Management (IAM)

IAM allows us to manage users and manage their permissions to the AWS console and services. It acts like a central place to manage and control our AWS account.

Common terms used:

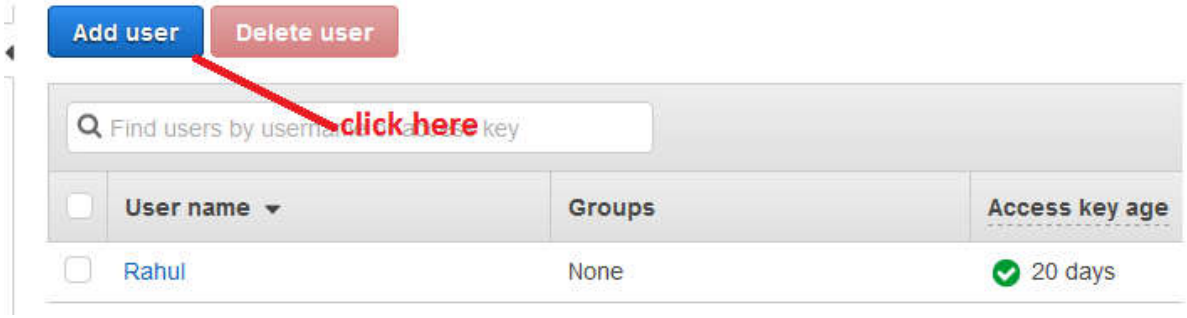
- User - person
- Group - is set of permissions to be made available to users. For e.g. "Admin", "Manager". User are assigned to group(s)
- Roles - are assigned to AWS resources to access other resources
- Policy - JSON document having the access related information

IAM is global and users, groups are same across all the regions for a given account.

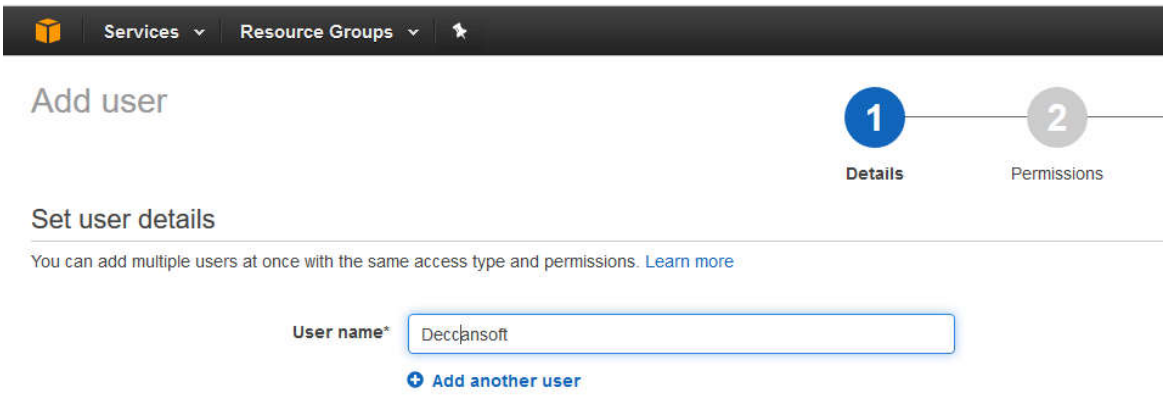
To create a user, we need to follow the steps as mentioned below:

Step 1 - To perform any task in AWS, we need to create IAM user, which will provide a key.

Let us see how we can create a role for user by using the given permission.

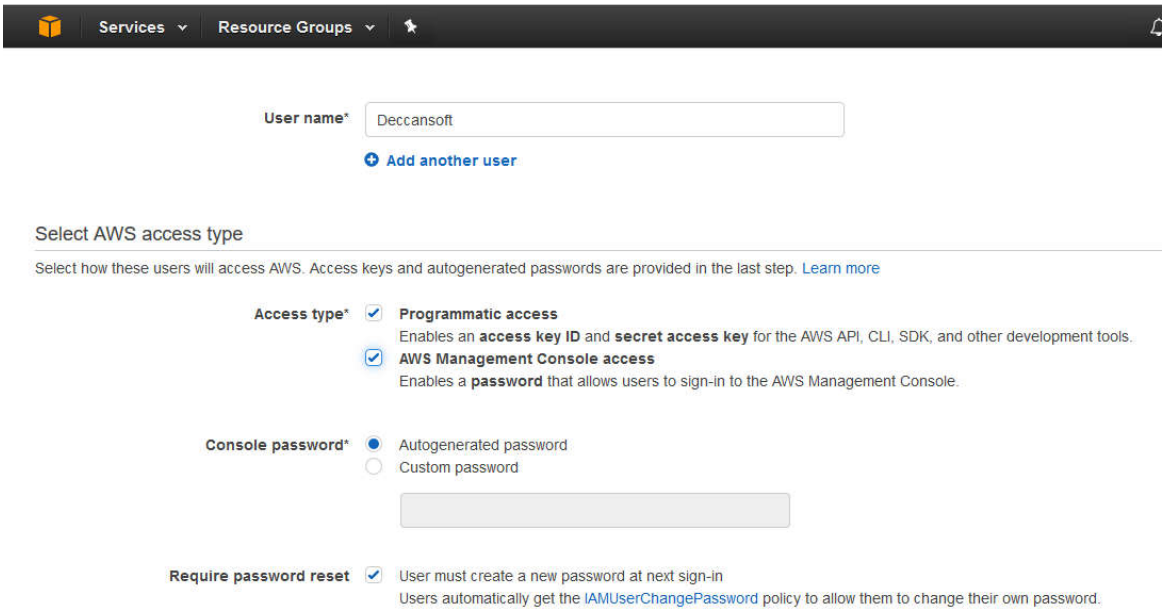


Step 2 - To add new user, we need to click at new user after it will pop-up new fields like given below.

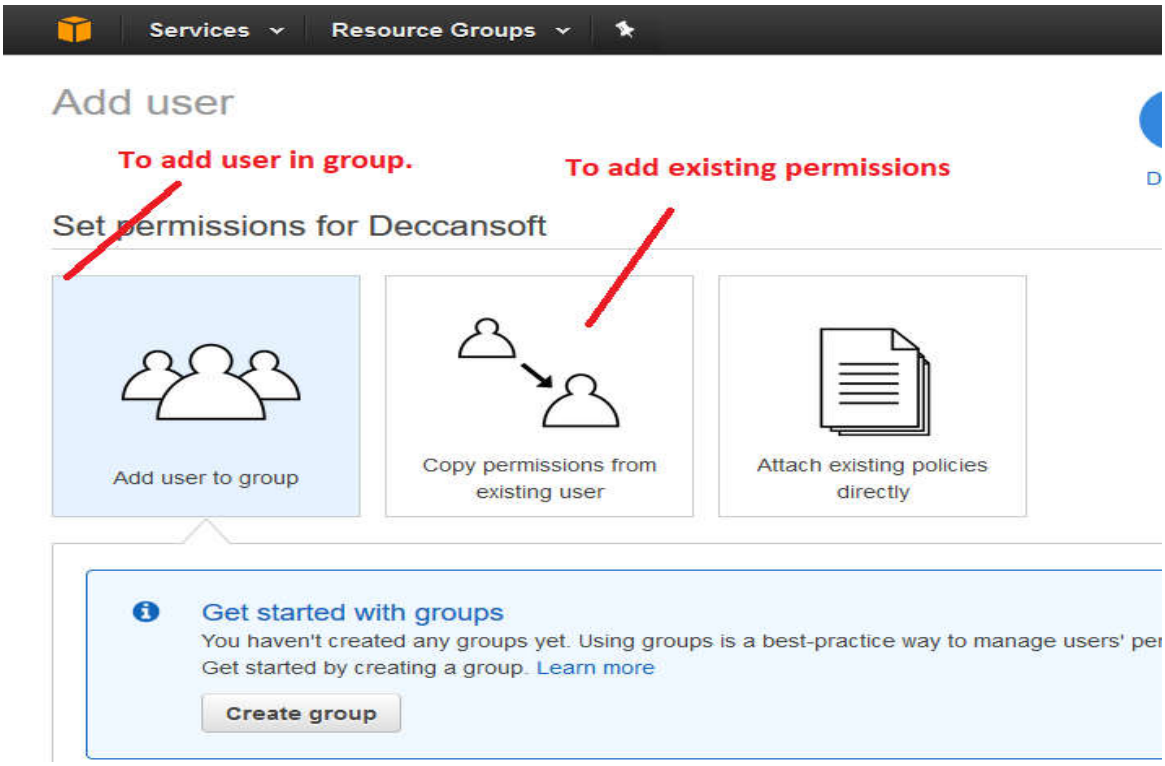


After specifying a username, we need to move for next step which is to provide permissions.

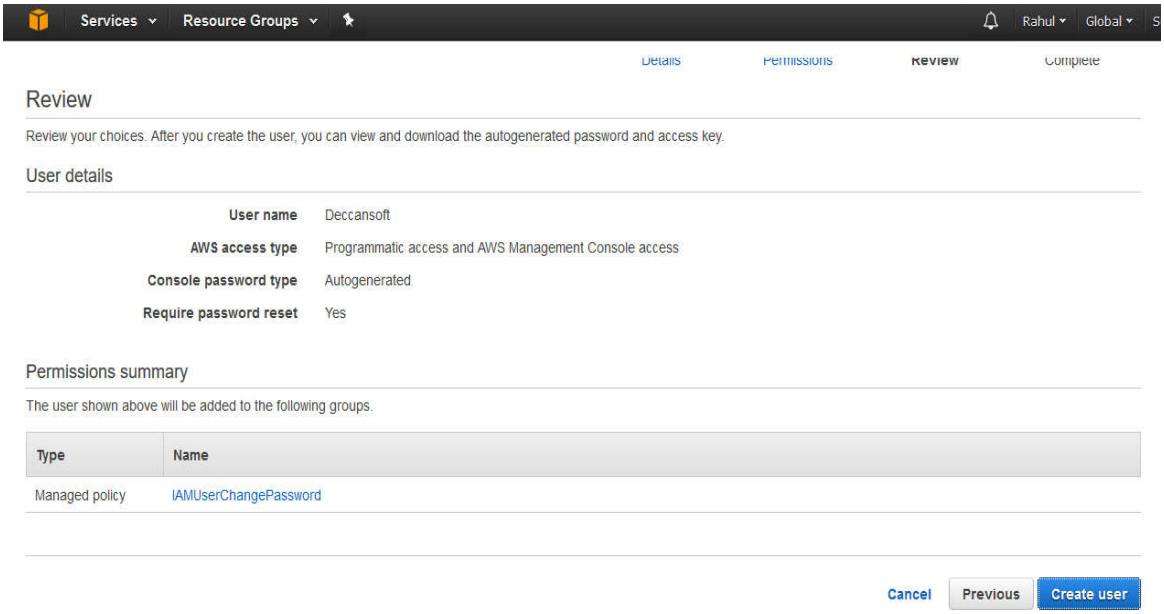
Step 3: Adding permissions.



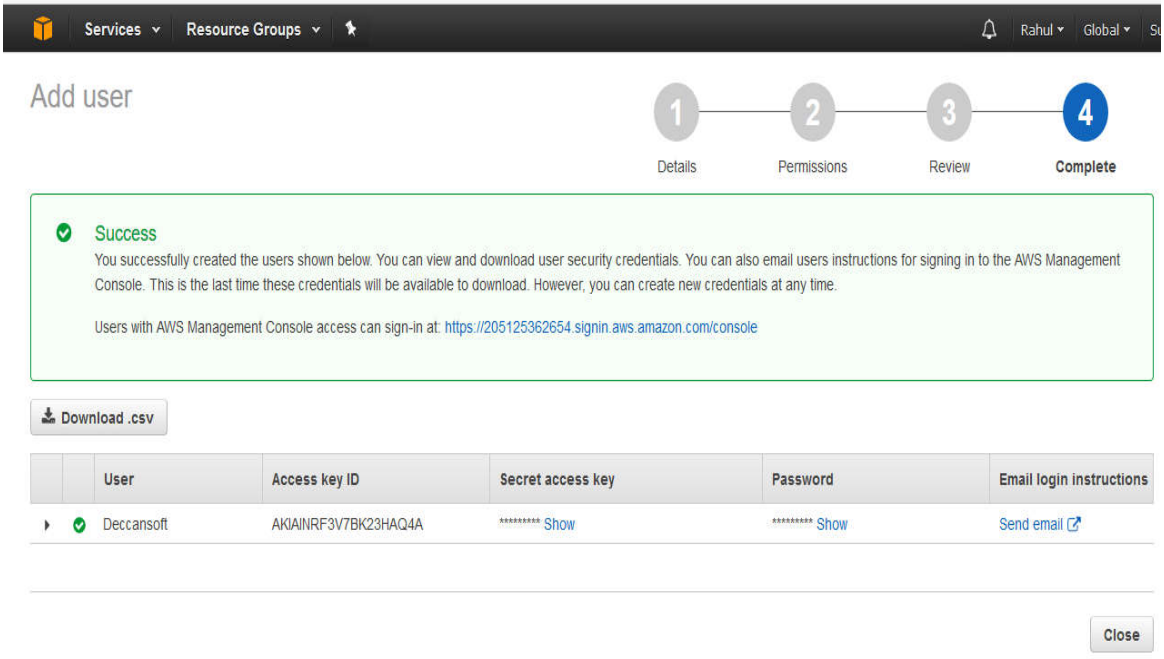
Step 4 - To add extra permissions we need to follow the suggestions as specified



Step 5 - After adding all required permissions we will see the descriptions as below.



Step 6: after confirming all information, we can move forward for create user operations.



Step 7 - After creating user we can add more permissions as per our requirements.