

# 02 Assignment - AWS Cloud

Name: Pooja Prakash Belgaumkar

## 2. L2 - Login to AWS Console and Create IAM User, Role, and Group

### a) User Group

- Creating the Developers named User Group with **AmazonEC2FullAccess** permission

The screenshot shows the AWS IAM console interface for creating a new user group. The top navigation bar includes the AWS logo, a search bar, and account information (Account ID: 7871-6932-0097, PoojaPrakash). The breadcrumb trail indicates the path: IAM > User groups > Create user group.

**Add users to the group - Optional (0)** Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search:

< 1 > | Settings

<input type="checkbox"/>	User name	▲	Group: ▼	Last activity	▼	Creation time	▼
No resources to display							

**Attach permissions policies - Optional (1/1109)** Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type

Search:  X All types ▼ 1 match < 1 > | Settings

<input checked="" type="checkbox"/>	Policy name	▲	Type	▼	Use...	▼	Description
<input checked="" type="checkbox"/>	AmazonEC2FullAccess		AWS managed		None		Provides full access to Amazon EC2 via...

Cancel Create user group

aws Account ID: 7871-6932-0097 PoojaPrakash


IAM > User groups > Developers

## Developers Info

[Delete](#)

### Summary

[Edit](#)

<b>User group name</b> Developers	<b>Creation time</b> January 02, 2026, 00:09 (UTC+05:30)	<b>ARN</b>  arn:aws:iam::787169320097:group/Developers
--------------------------------------	---	--

[Users](#) | [Permissions](#) | [Access Advisor](#)

### Users in this group (0)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

[Refresh](#) [Remove](#) [Add users](#)

< 1 > [Settings](#)

<input type="checkbox"/>	User name <a href="#">↗</a>	Groups	Last activity	Creation time
No resources to display				

## b) IAM User

- Creating IAM user dev-user with custom password and adding to the Developers group

IAM > Users > Create user

Step 1: Specify user details  
Step 2: Set permissions  
**Step 3: Review and create**  
Step 4: Retrieve password

## Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

### User details

<b>User name</b> dev-user	<b>Console password type</b> Custom password	<b>Require password reset</b> Yes
------------------------------	---	--------------------------------------

### Permissions summary

< 1 >

Name <a href="#">↗</a>	Type	Used as
<a href="#">Developers</a>	Group	Permissions group
<a href="#">IAMUserChangePassword</a>	AWS managed	Permissions policy

### Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create user](#)

- Logged in as dev-user IAM user

The screenshot displays the AWS Management Console interface. At the top, the header includes the AWS logo, a search bar, and navigation icons. The top right corner shows the account ID '7871-6932-0097' and the user 'dev-user'. The main content area is titled 'Console Home' and features a 'Recently visited' section with a message 'No recently visited services' and links to EC2, S3, Aurora and RDS, and Lambda. To the right, the 'Applications' section shows a region of 'Europe (Stockholm)' and a 'Select Region' dropdown. Below this, a red box highlights an 'Access denied' error for 'servicecatalog'. A user menu is open on the right side, displaying options such as 'Account ID', 'Account color', 'IAM user', 'Account', 'Organization', 'Service Quotas', 'Billing and Cost Management', 'Security credentials', and 'Console Mobile App'. At the bottom of the menu are buttons for 'Turn on multi-session support', 'Switch role', and 'Sign out'. The bottom of the console shows a 'Welcome to' section and a 'Cost and usage' section.

## c) Role

- Creating IAM Role with EC2-S3-ReadRole permission.

### Role details

**Role name**  
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+=, @-\_' characters.

**Description**  
Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: \_+=, @-/\[\]{}#%&^\*()~:~'"`

### Step 1: Select trusted entities

Edit

#### Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "sts:AssumeRole"  
8       ],  
9       "Principal": {  
10        "Service": [  
11          "ec2.amazonaws.com"  
12        ]  
13      }  
14    }  
15  ]  
16 }
```

### Step 2: Add permissions

Edit

#### Permissions policy summary

Policy name <a href="#">↗</a>	Type	Attached as
<a href="#">AmazonS3ReadOnlyAccess</a>	AWS managed	Permissions policy

### Step 3: Add tags

#### Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create role