**IAM TASKS**

**1.Create one IAM user and assign EC2 and S3 full access roles.**

**Step 1: Sign in to AWS Console**

* Log in to the **AWS Management Console** with an account that has **IAM Admin privileges**.
* Go to **IAM (Identity and Access Management)** service.

**Step 2: Create IAM User**

1. In IAM, click **Users → Add users**.
2. Enter a **username** (example: test-user).
3. Select **Access type**:
   * **Password** (if the user needs to log in to AWS Console).
   * **Access key** (if the user needs CLI/SDK access). You can select both.
4. Click **Next**.

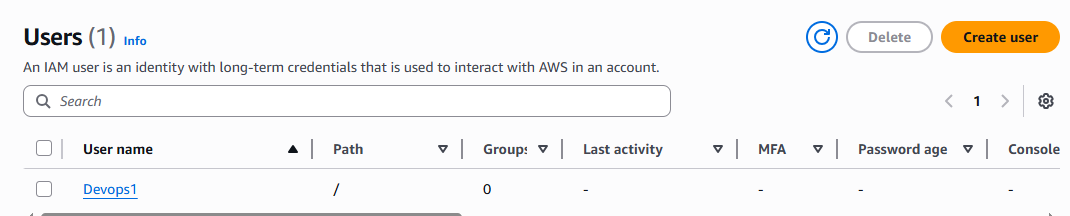
**Step 3: Attach Policies**

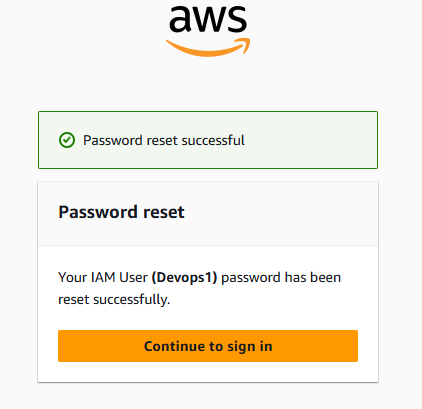
1. On the permissions page, choose **Attach policies directly**.
2. Search and select these two AWS Managed Policies:
   * AmazonEC2FullAccess
   * AmazonS3FullAccess
3. Click **Next → Create User**.

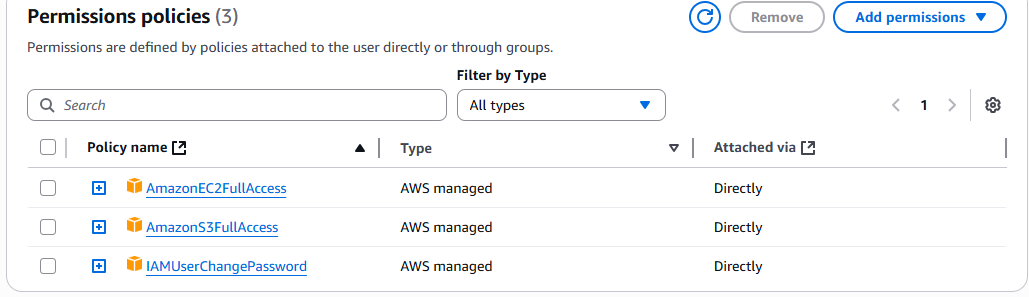
**Step 4: Save Credentials**

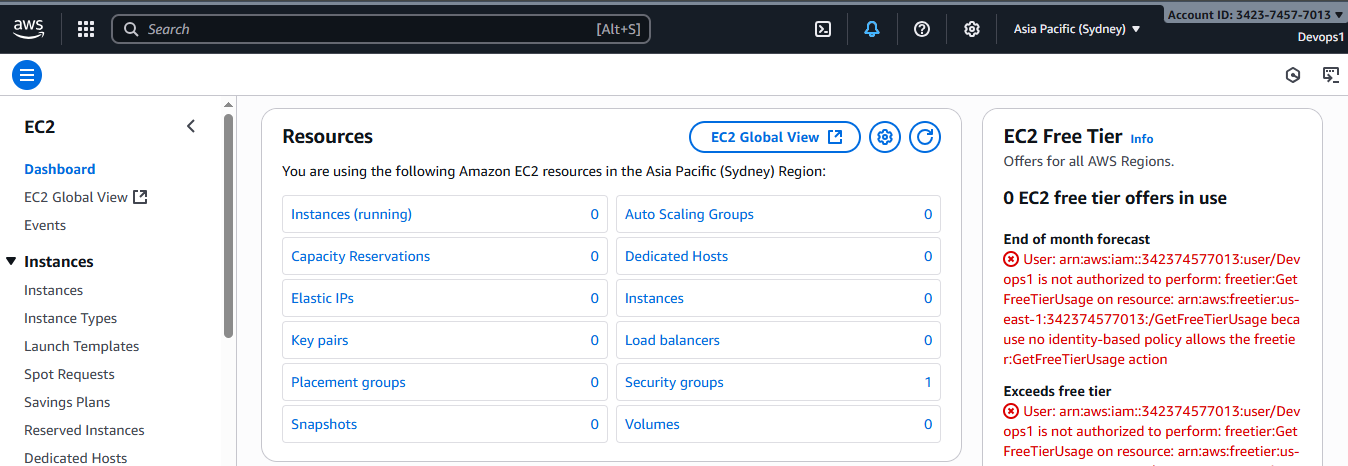
* If you selected **Access Key**, AWS will generate an **Access key ID** and **Secret access key**.
* Download the .csv file or copy them securely. (You won’t be able to see the secret again.)

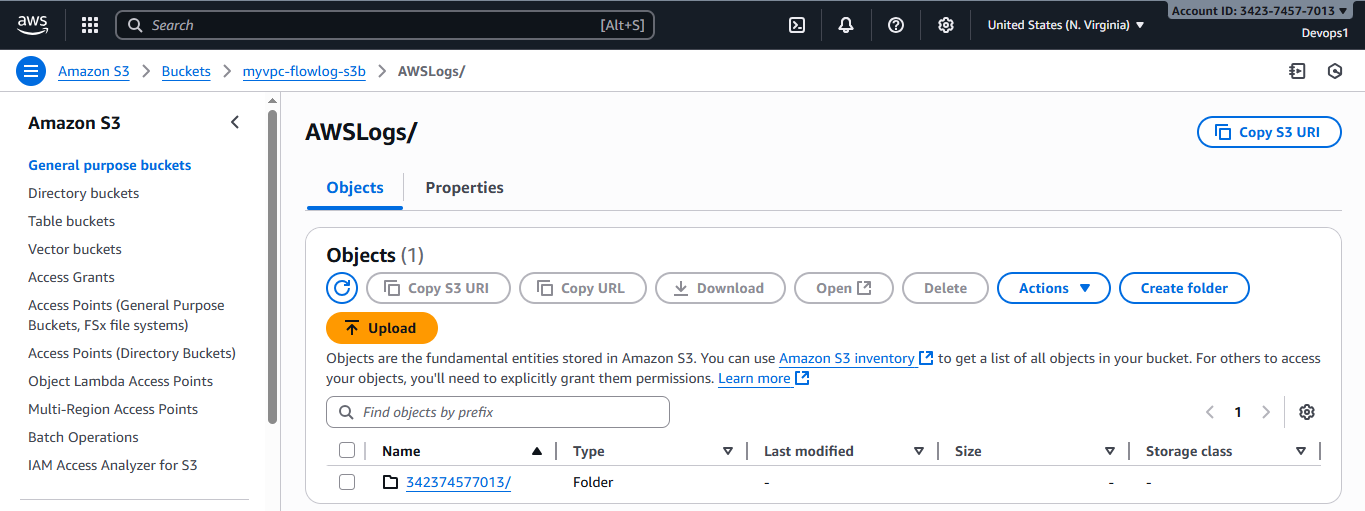
✅ Now your IAM user has **full EC2 and S3 access**.











**2.Create one group in IAM and assign read access for EC2.**

### ****Steps in AWS Console****

#### **Step 1: Open IAM**

* Log in to **AWS Management Console** → Go to **IAM** service.

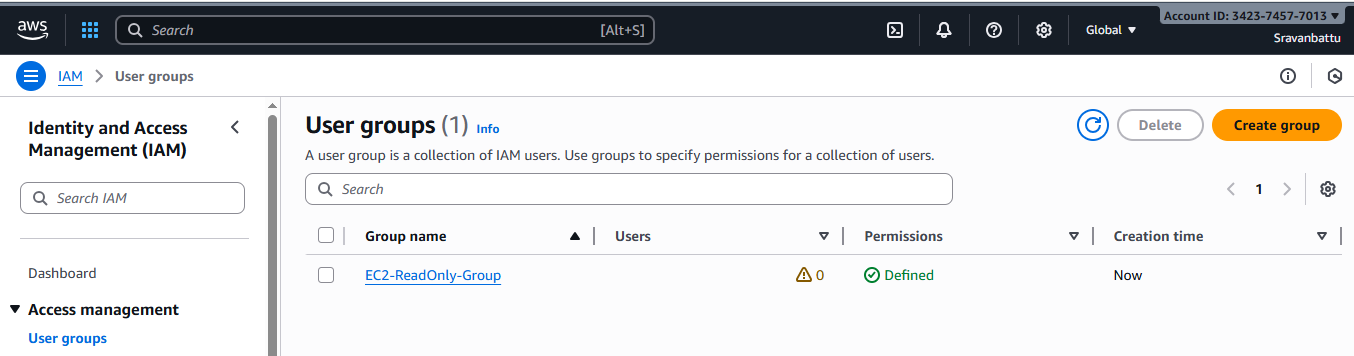
#### **Step 2: Create Group**

1. In the left panel, click **User groups → Create group**.
2. Enter a **Group name** (example: EC2-ReadOnly-Group).
3. In the **Attach permissions policies** section:
   * Search for **AmazonEC2ReadOnlyAccess**.
   * Check the box.
4. Click **Create group**.

#### **Step 3: Add Users**

* Once the group is created, you can click **Add users to group** and select existing IAM users.

✅ Now, all users in this group will only have **read-only access to EC2** (can describe instances, volumes, etc., but cannot start/stop/terminate).



**3.Create a new user named "Devops" and add to the group created in task 2.**

### ****Step 1: Create User****

1. Go to **IAM → Users → Add users**.
2. Enter **User name** = Devops.
3. Select **Access type**:
   * **Password** → for AWS Console login.
   * **Access key** → for CLI/SDK access.  
     (You can enable both if needed).
4. Click **Next**.

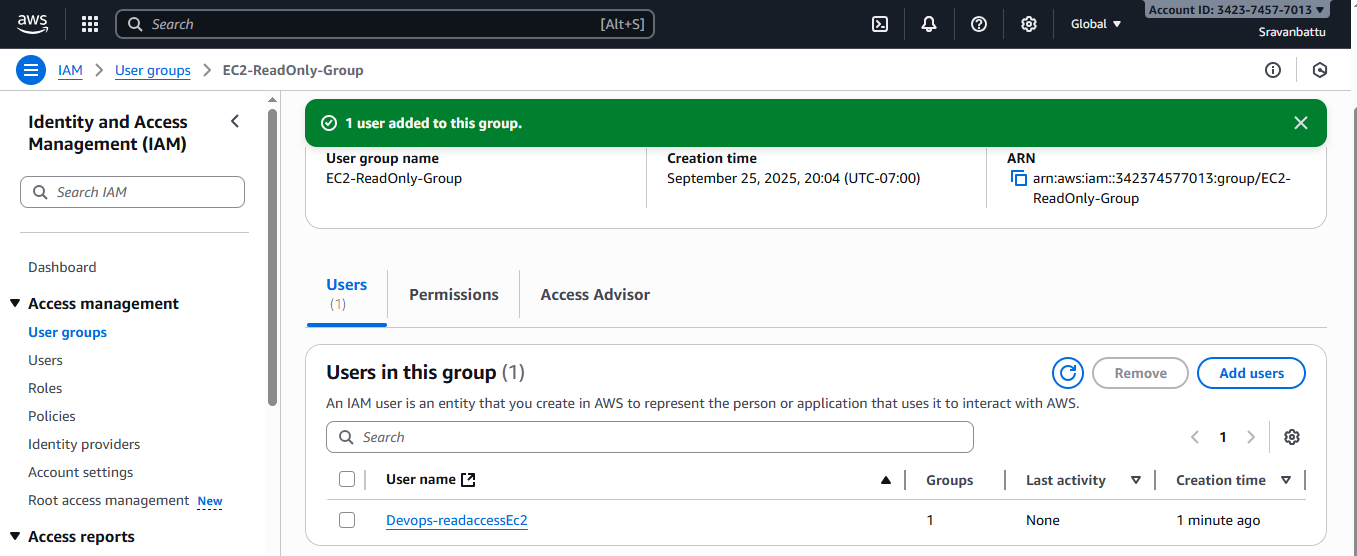
### ****Step 2: Add User to Group****

1. On the permissions page, select **Add user to group**.
2. Choose the group you created earlier: **EC2-ReadOnly-Group**.
3. Click **Next → Create user**.

### ****Step 3: Save Credentials****

* If you enabled **Access key**, download the .csv file or copy the keys.
* If you enabled **Password**, note down the login details.

Now, user **Devops** is part of **EC2-ReadOnly-Group** ✅ and will have **read-only EC2 permissions**.



**4.Write a bash script to create an IAM user with VPC full access.**

### ****Step 1: Create an IAM Role for EC2****

1. Go to **AWS Console → IAM → Roles → Create role**
2. **Trusted entity type** → Select **AWS service**
3. Choose **EC2**
4. **Permissions** → Attach a policy that has full IAM access, such as:
   * AdministratorAccess (for testing)
   * or at least a custom policy with:
     + iam:CreateUser
     + iam:CreateLoginProfile
     + iam:AttachUserPolicy
     + iam:GetUser
5. Give the role a name, e.g. EC2-IAM-Admin-Role
6. Create role ✅

### ****Step 2: Attach Role to Your EC2 Instance****

1. Go to **EC2 Console → Instances**
2. Select your instance (ip-172-31-0-10)
3. From the **Actions** menu → **Security → Modify IAM role**
4. Select the role you created (EC2-IAM-Admin-Role)
5. Save

Now your EC2 will automatically use **temporary credentials** via the role. No need for aws configure.

### ****Step 3: Verify Role Access****

Run this command in your EC2:

aws sts get-caller-identity

You should see an ARN like:

{

"UserId": "AROAxxxxxx:instance-profile",

"Account": "123456789012",

"Arn": "arn:aws:sts::123456789012:assumed-role/EC2-IAM-Admin-Role/i-0abcd1234efgh5678"

}

## Bash Script

#!/bin/bash

# Variables

IAM\_USER\_NAME="vpc-user"

POLICY\_ARN="arn:aws:iam::aws:policy/AmazonVPCFullAccess"

PASSWORD="MySecurePassword@123" # Change this to a strong password

# Step 1: Create IAM user

echo "Creating IAM user: $IAM\_USER\_NAME ..."

aws iam create-user --user-name $IAM\_USER\_NAME

# Step 2: Create login profile (for AWS Console access with password)

echo "Creating login profile..."

aws iam create-login-profile \

--user-name $IAM\_USER\_NAME \

--password "$PASSWORD" \

--password-reset-required

# Step 3: Attach VPC Full Access policy

echo "Attaching AmazonVPCFullAccess policy..."

aws iam attach-user-policy \

--user-name $IAM\_USER\_NAME \

--policy-arn $POLICY\_ARN

echo "✅ IAM user '$IAM\_USER\_NAME' created successfully."

echo "👉 Console login username: $IAM\_USER\_NAME"

echo "👉 Temporary password: $PASSWORD"

## 🔹 How to Run

1. Save script:
2. nano create-vpc-console-user.sh

Paste the script.

1. Make it executable:
2. chmod +x create-vpc-console-user.sh
3. Run it:

./create-vpc-console-user.sh

It should successfully create:

* IAM user vpc-user
* Login password
* Attach AmazonVPCFullAccess policy
* 