**Lab2: Working with AWS IAM**

**Objective:** Managing and securing access to AWS resources using IAM

**Architectural diagram:**

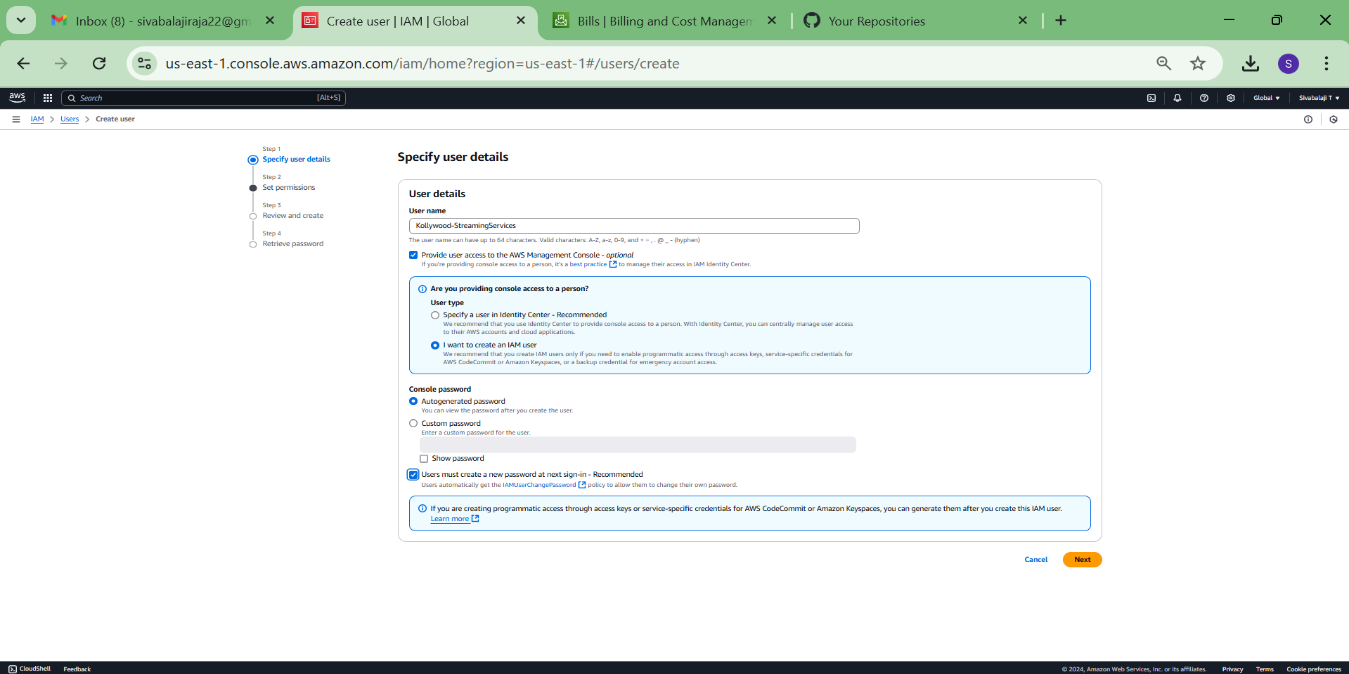


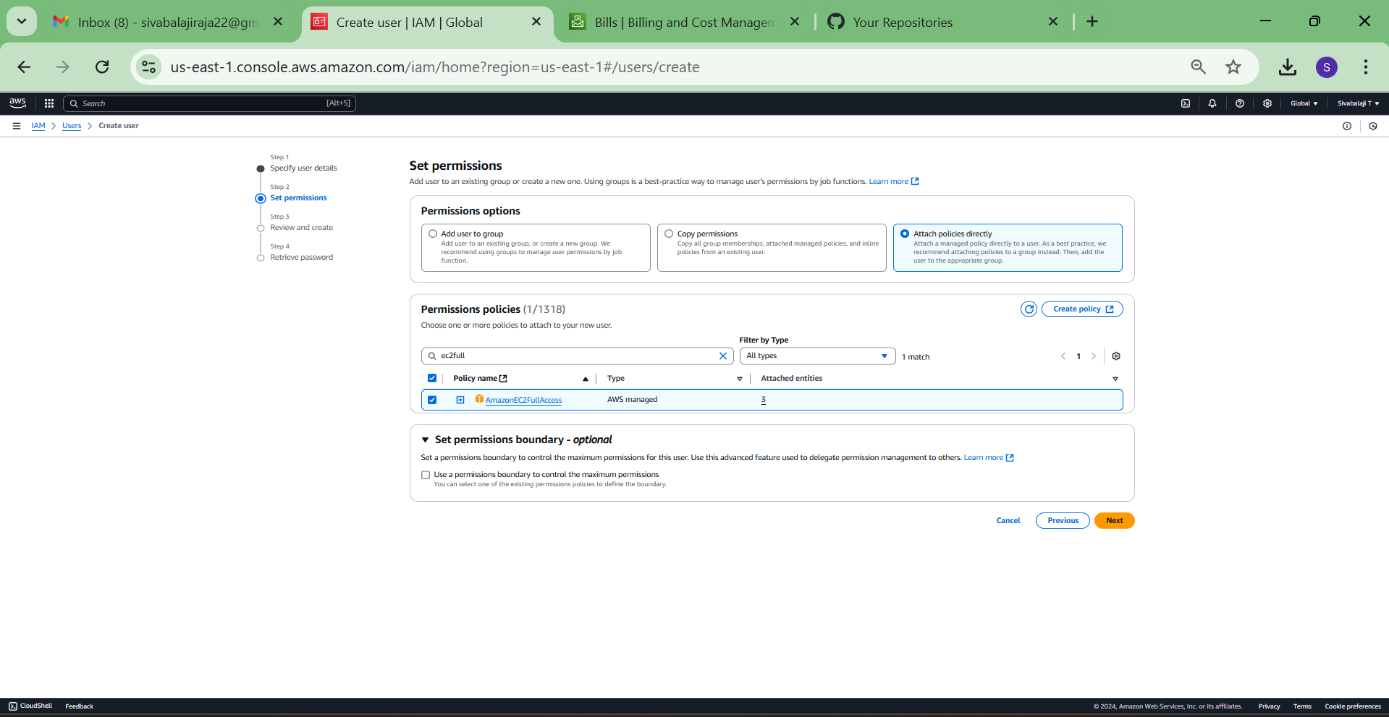
**Step-by-Step Instructions:**

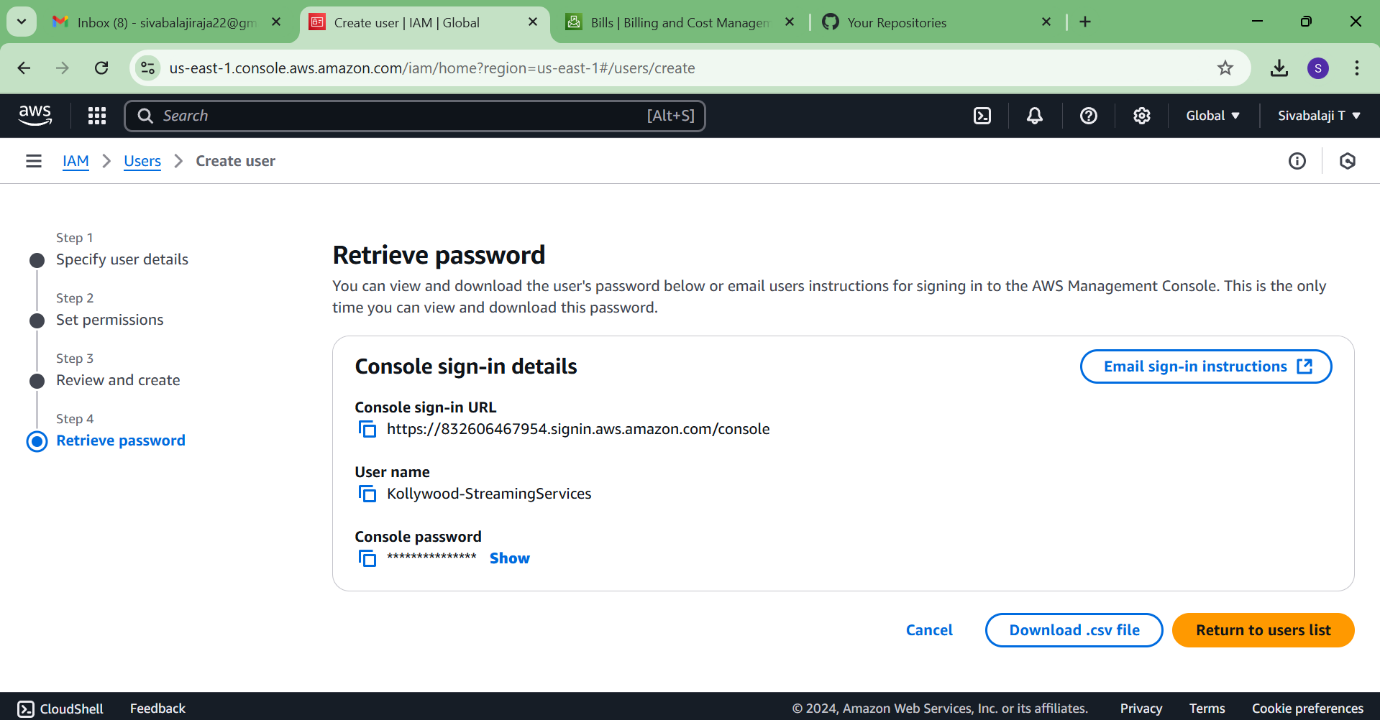
**Step 1: Access IAM**

1. Log in to the AWS Management Console.
2. Search for and open the **IAM Dashboard**.

**Step 2: Create an IAM User**

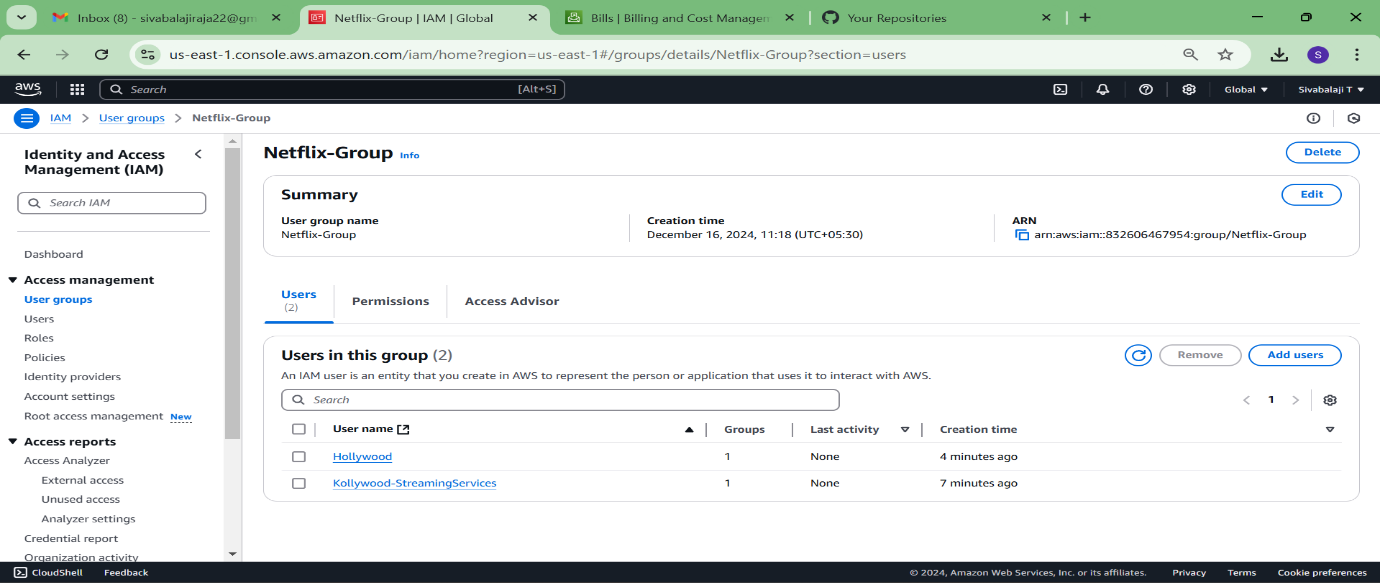
1. Go to **Users** in the IAM dashboard.
2. Click **Add Users**.
3. Configure the user:
   * **User Name**: Provide a name for the user.
   * **Access Type**:
     + Select **AWS Management Console access** for GUI-based access.
     + Select **Programmatic access** for API/CLI/SDK access (generates access keys).
4. Click **Next: Permissions**.
5. Assign permissions:
   * **Add user to group**: Create or add to a group with the required policies (e.g., AdministratorAccess or ReadOnlyAccess).
   * **Attach policies directly**: Attach pre-defined or custom policies.
6. Download or note down the **Access Key ID** and **Secret Access Key**

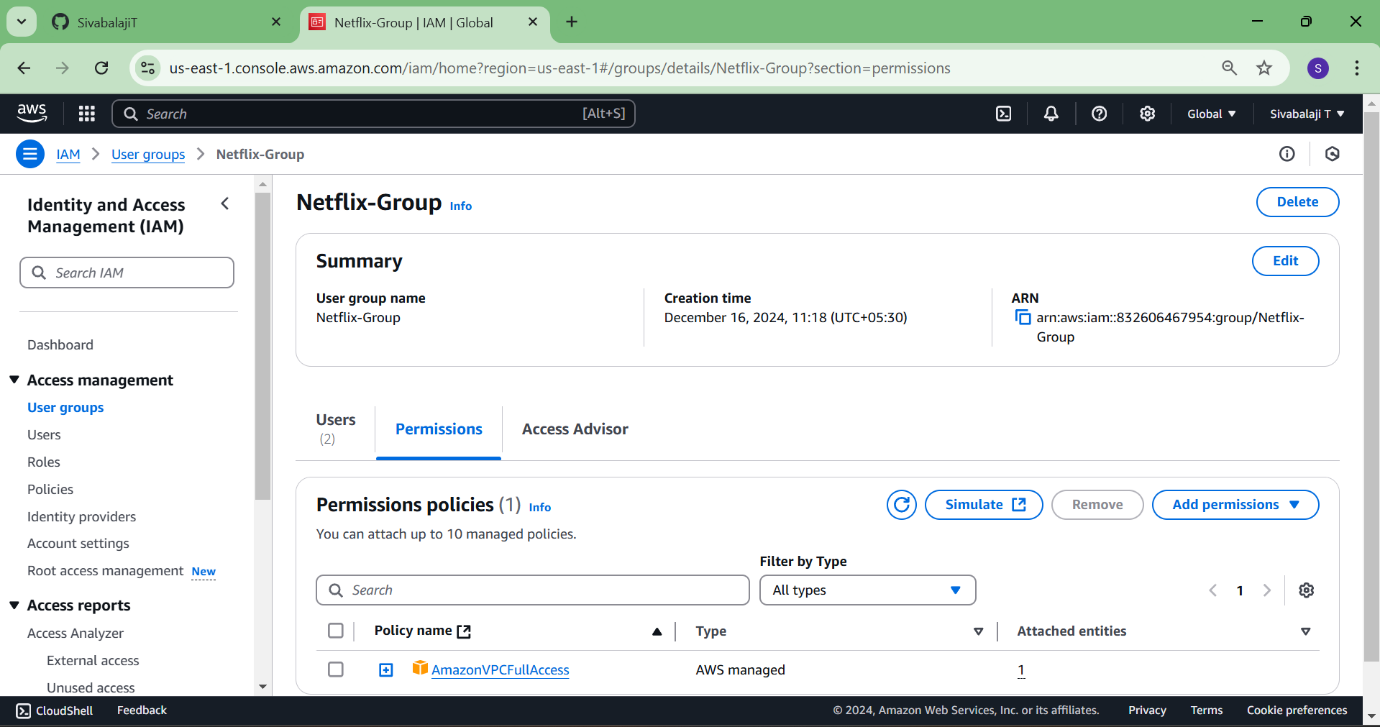




**Step 3: Create an IAM Group**

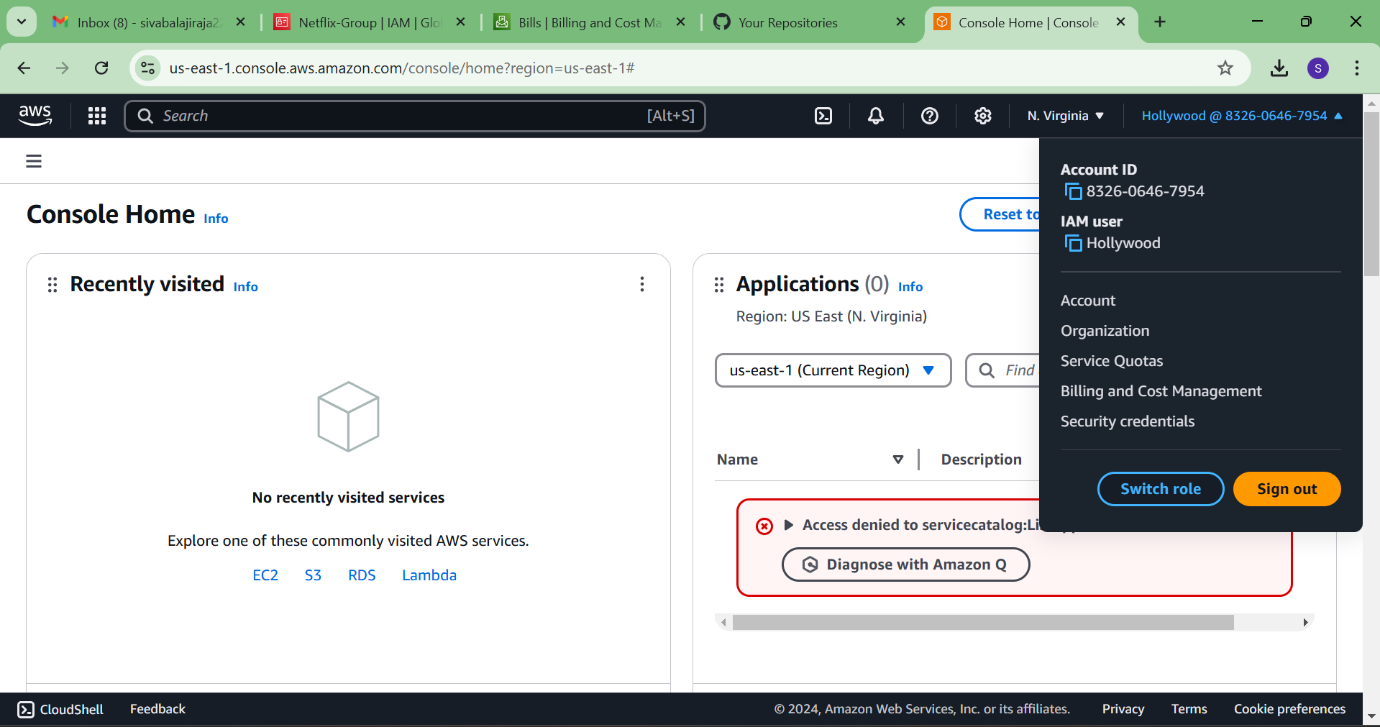
1. Go to **Groups** in the IAM dashboard.
2. Click **Create Group**.
3. Provide a group name.
4. Attach policies:
   * Select pre-defined policies or create a custom policy.
5. Click **Create Group**.
6. Add users to the group by editing the group’s user settings.

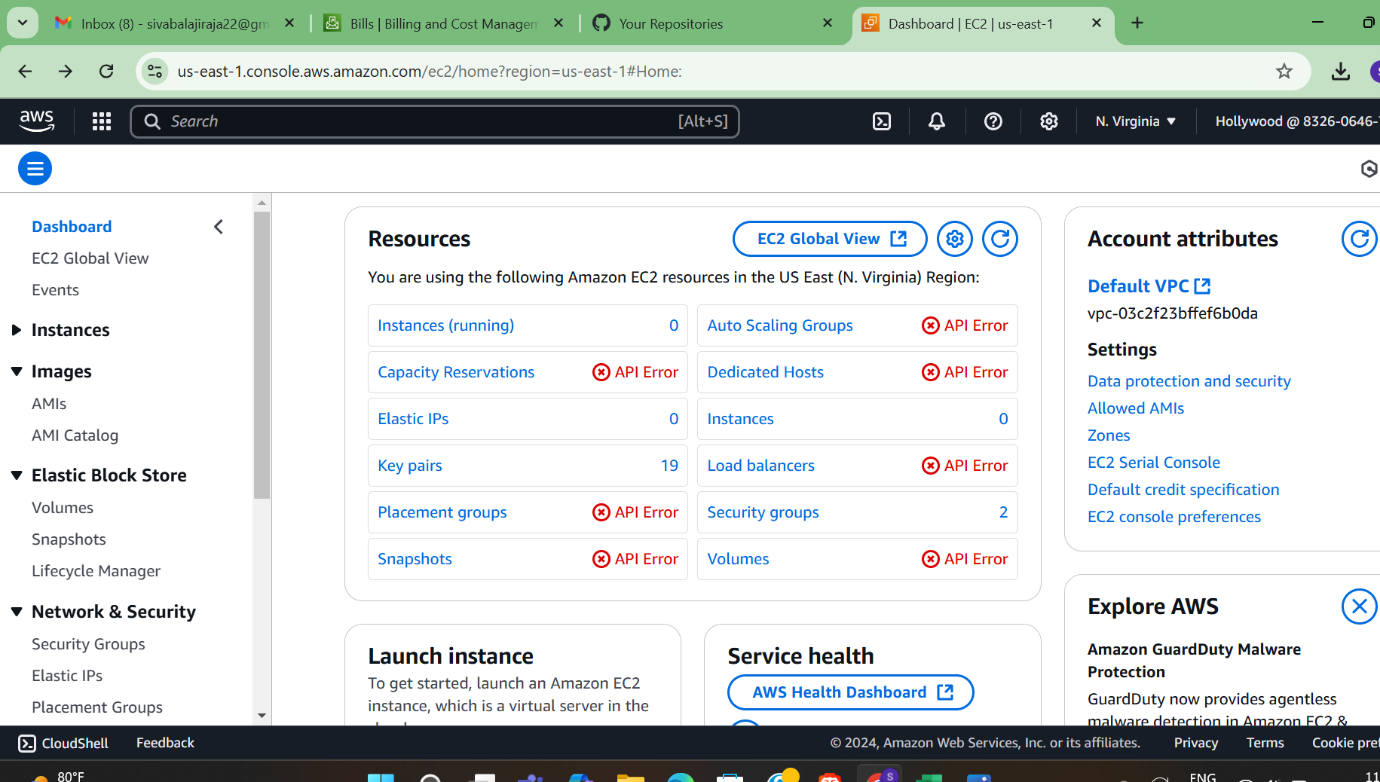




**Step 4: Try to login Aws console using IAM Access and Secret Key.**

1. Access the **permission** Services to use the aws services.
2. Without permission services won’t be using.

****

****