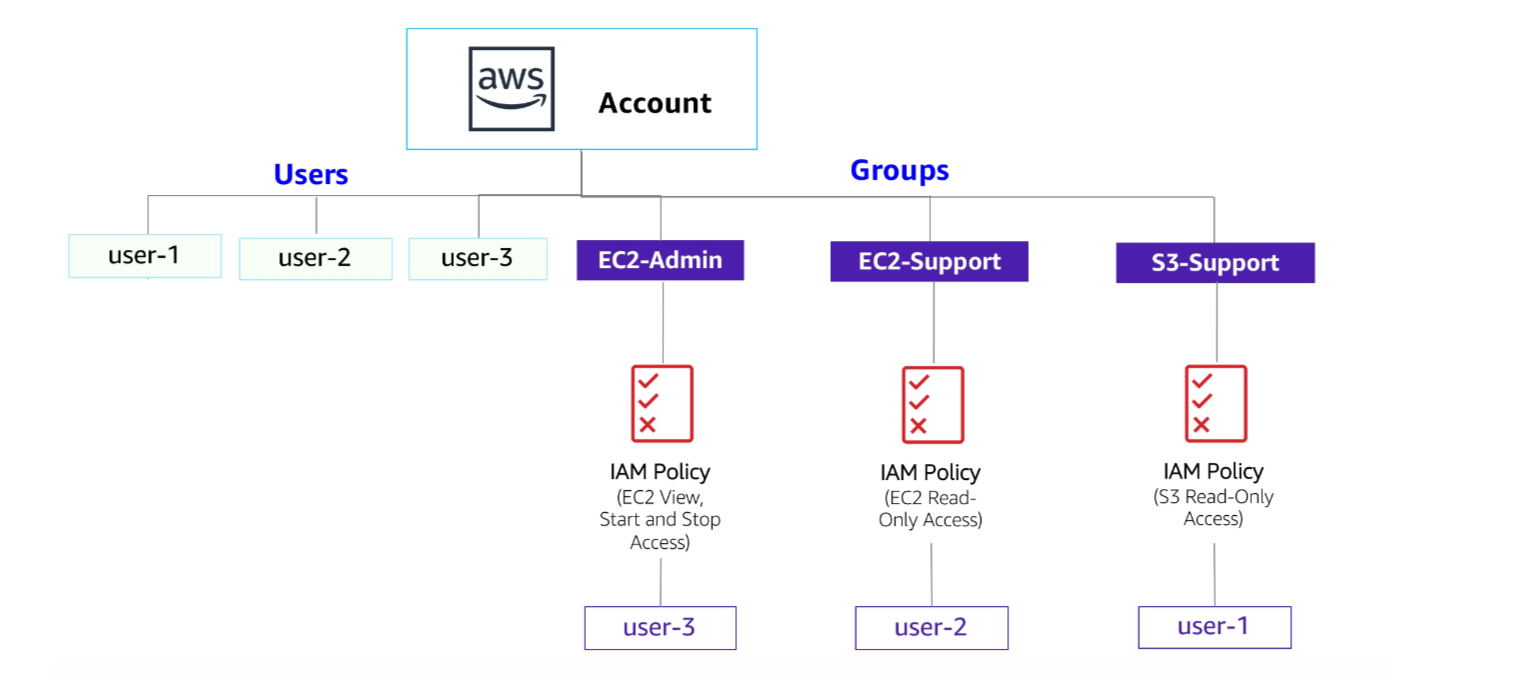
**Aim : Introduction to AWS Identity and Access Management(IAM)**

**AWS Identity and Access Management (IAM)** is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. With IAM, you can centrally manage **users**, **security credentials** such as access keys, and **permissions** that control which AWS resources users can access



**AWS Identity and Access Management**

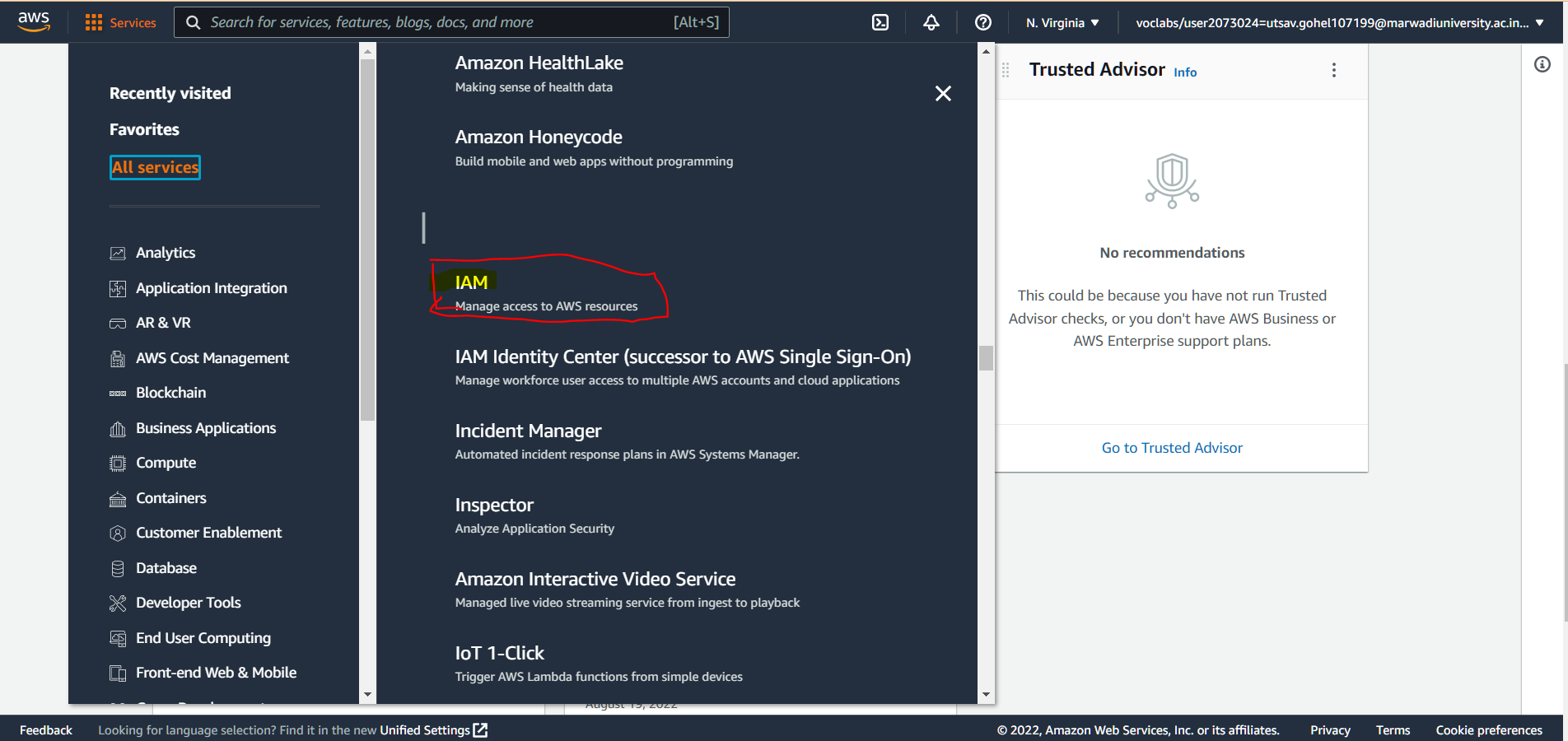
AWS Identity and Access Management (IAM) can be used to:

* **Manage IAM Users and their access:** You can create Users and assign them individual security credentials (access keys, passwords, and multi-factor authentication devices). You can manage permissions to control which operations a User can perform.
* **Manage IAM Roles and their permissions:** An IAM Role is similar to a User, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a Role is intended to be *assumable* by anyone who needs it.
* **Manage federated users and their permissions:** You can enable *identity federation* to allow existing users in your enterprise to access the AWS Management Console, to call AWS APIs and to access resources, without the need to create an IAM User for each identity.

**Task 1: Explore the Users and Groups**

In this task, you will explore the Users and Groups that have already been created for you in IAM.

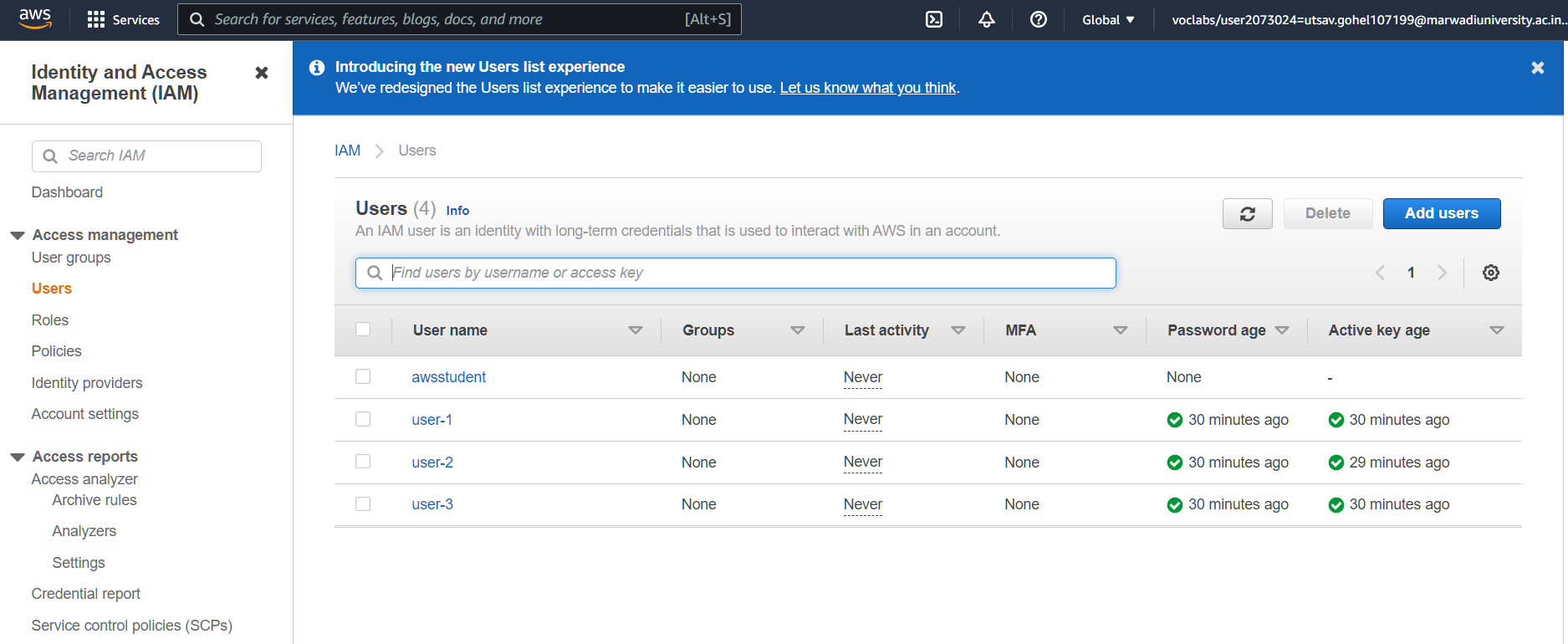
1. In the **AWS Management Console**, on the **Services** menu, select **IAM**.



1. In the navigation pane on the left, choose **Users**.

The following IAM Users have been created for you:

* + user-1
  + user-2
  + user-3



1. Choose **user-1**.

This will bring to a summary page for user-1. The **Permissions** tab will be displayed.

1. Notice that user-1 does not have any permissions.
2. Choose the **Groups** tab.

user-1 also is not a member of any groups.

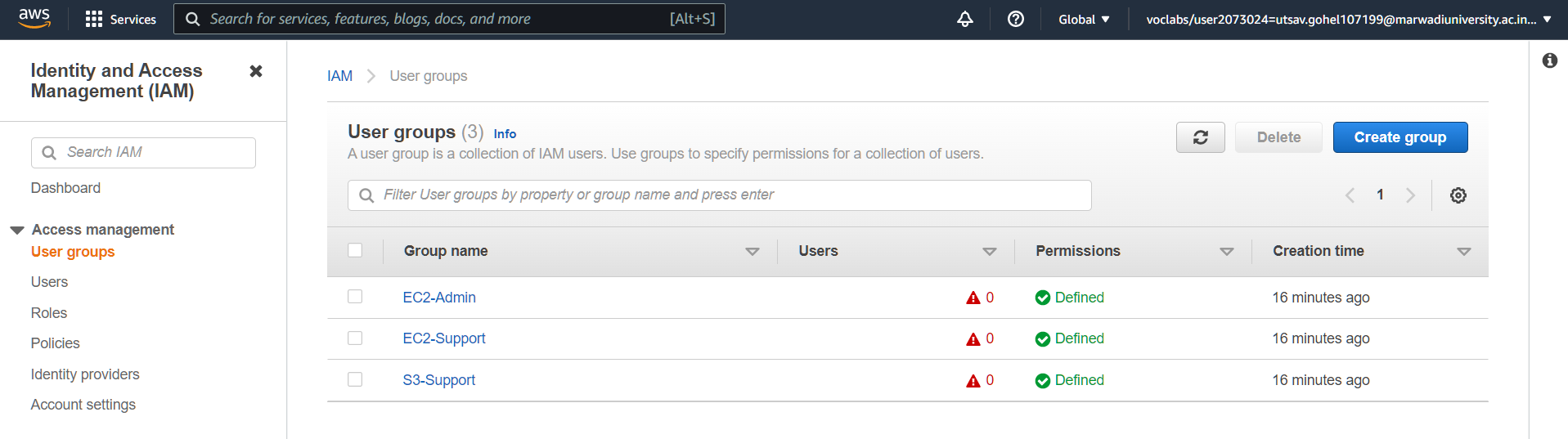
1. Choose the **Security credentials** tab.

user-1 is assigned a **Console password**

1. In the navigation pane on the left, choose **User groups**.

The following groups have already been created for you:

* + EC2-Admin
  + EC2-Support
  + S3-Support



1. Choose the **EC2-Support** group.

This will bring you to the summary page for the **EC2-Support** group.

1. Choose the **Permissions** tab.

This group has a Managed Policy associated with it, called **AmazonEC2ReadOnlyAccess**. Managed Policies are pre-built policies (built either by AWS or by your administrators) that can be attached to IAM Users and Groups. When the policy is updated, the changes to the policy are immediately apply against all Users and Groups that are attached to the policy.

## Task 2: Add Users to Groups

You have recently hired **user-1** into a role where they will provide support for Amazon S3. You will add them to the **S3-Support** group so that they inherit the necessary permissions via the attached AmazonS3ReadOnlyAccess policy.

### Add user-1 to the S3-Support Group

1. In the left navigation pane, choose **User groups**.

1. Choose the **S3-Support** group.

1. Choose the **Users** tab.

1. In the **Users** tab, choose **Add users**.

1. In the **Add Users to S3-Support** window, configure the following:
   * Select  **user-1**.
   * At the bottom of the screen, choose **Add Users**.

In the **Users** tab you will see that user-1 has been added to the group.

Step 1) Login to Your AWS account