

Lab -279 Introduction to IAM

Supplementary Training Material to AWS Restart



June 13, 2023

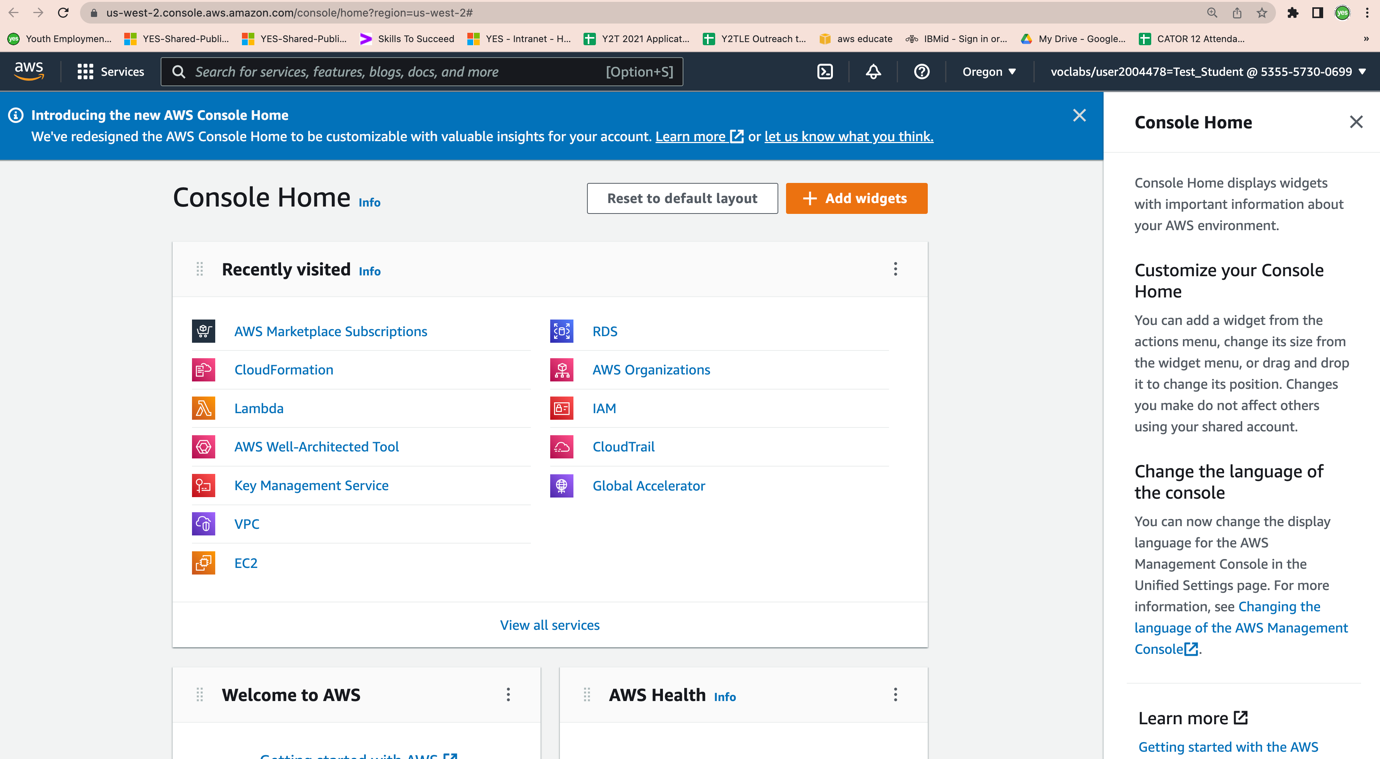
# Introduction

AWS Identity and Access Management (IAM) is **a web service that helps you securely control access to AWS resources**. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

# Accessing the Management Console

Login to AWS using the AWS Restart Vocareum Labs Link

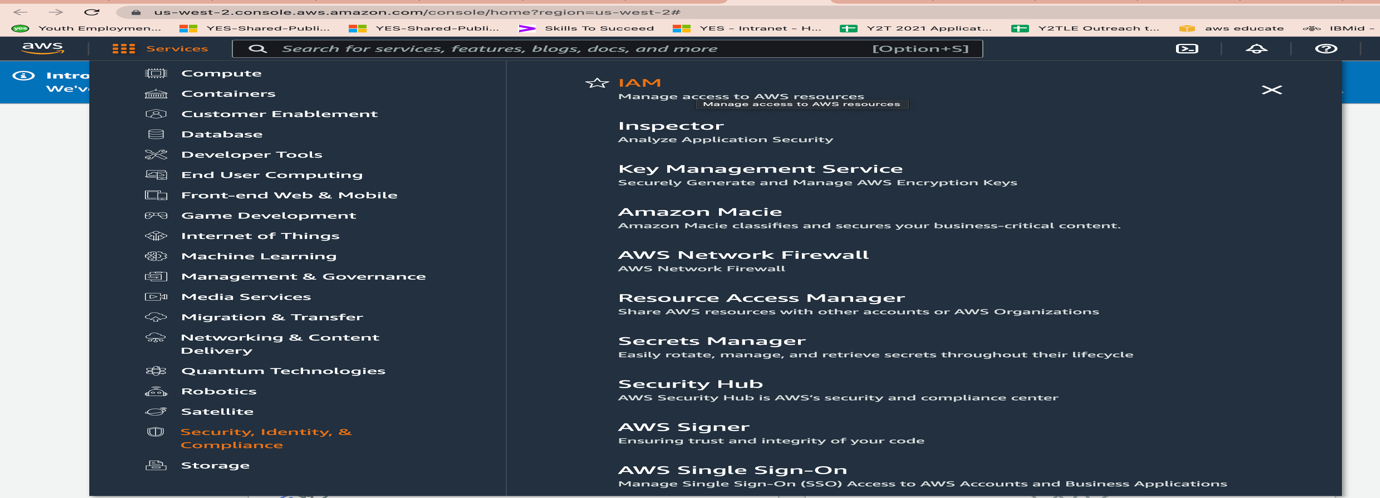
# Explore the AWS Management Console



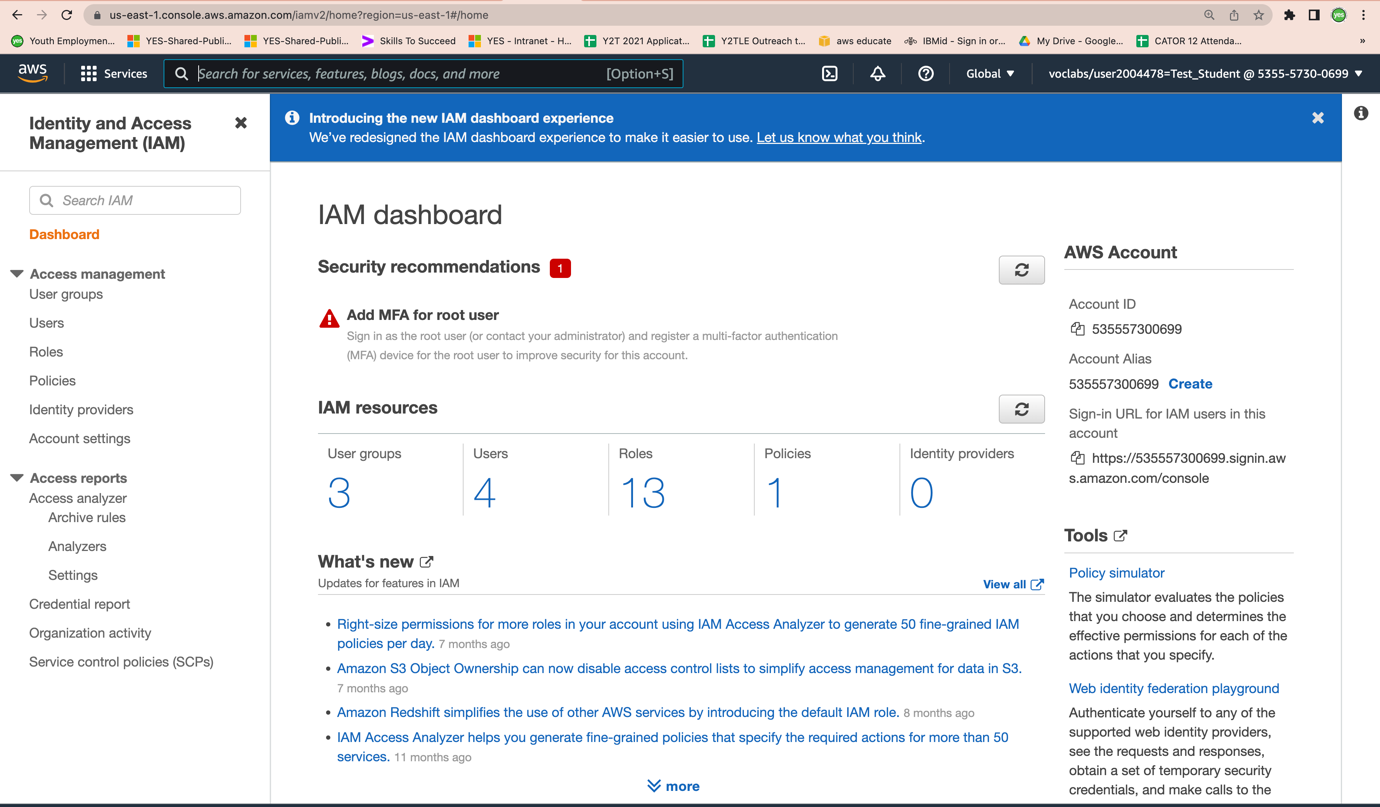
## Task 1: Explore the Users and Groups

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

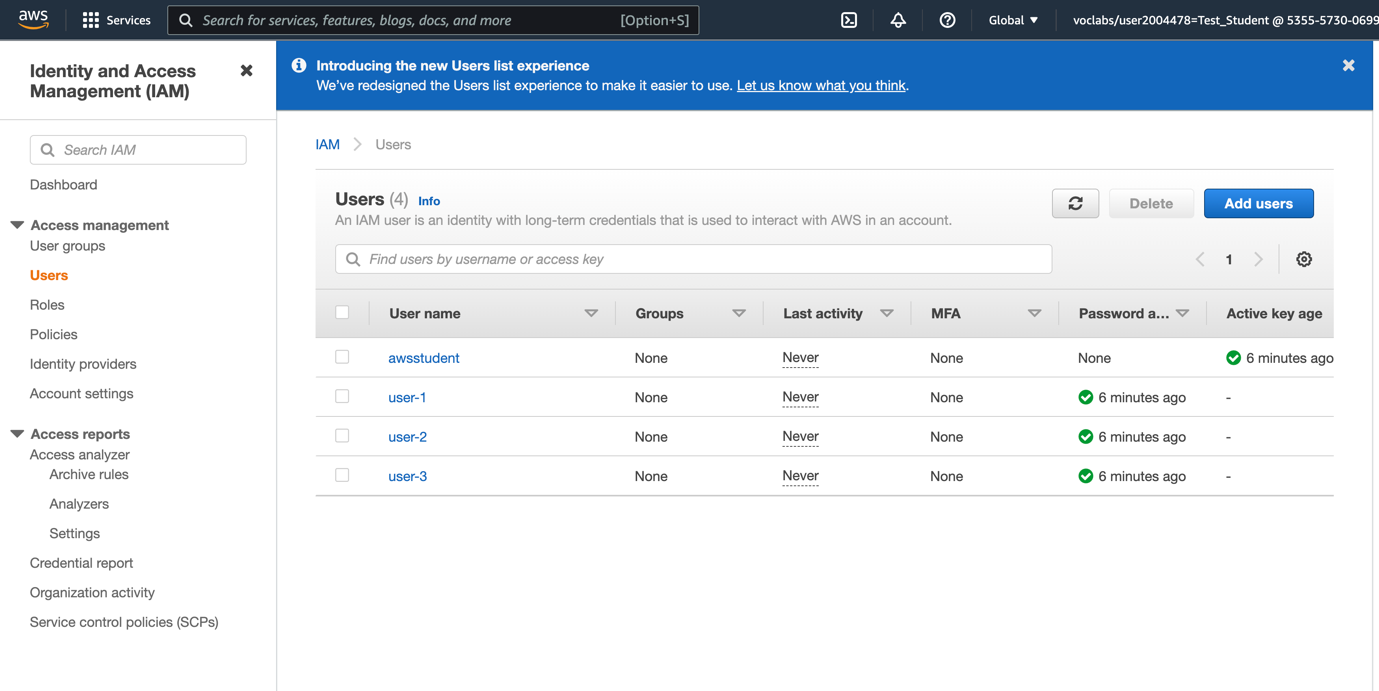
In the **AWS Management Console**, on the **Services** menu, under **Security, Identity, & Compliance** choose **IAM**.



## The IAM Dashboard Opens up



# On the Left Navigation Pane Select Users



# Note that the following IAM Users have been created for you:

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

# Choose User -1

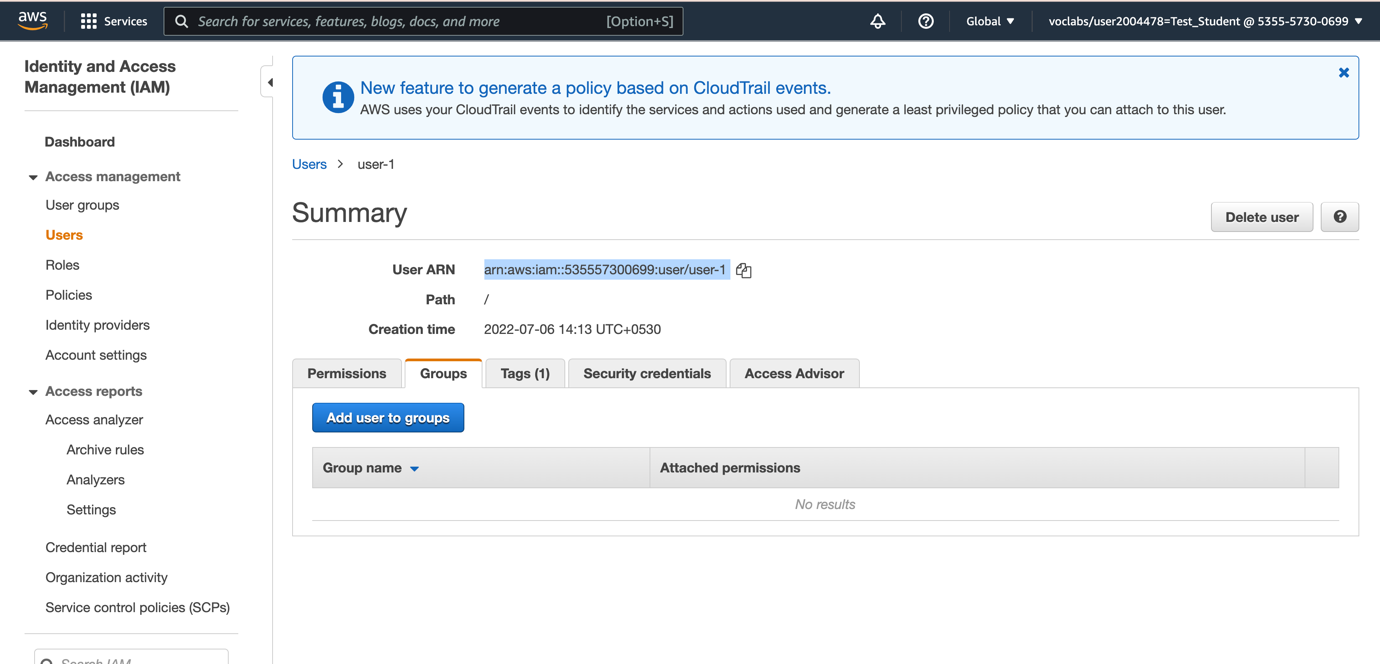
This will bring to a summary page for user-1. The **Permissions** tab will be displayed.



Observe that user-1 does not have any permissions.

# Click the Groups Tab

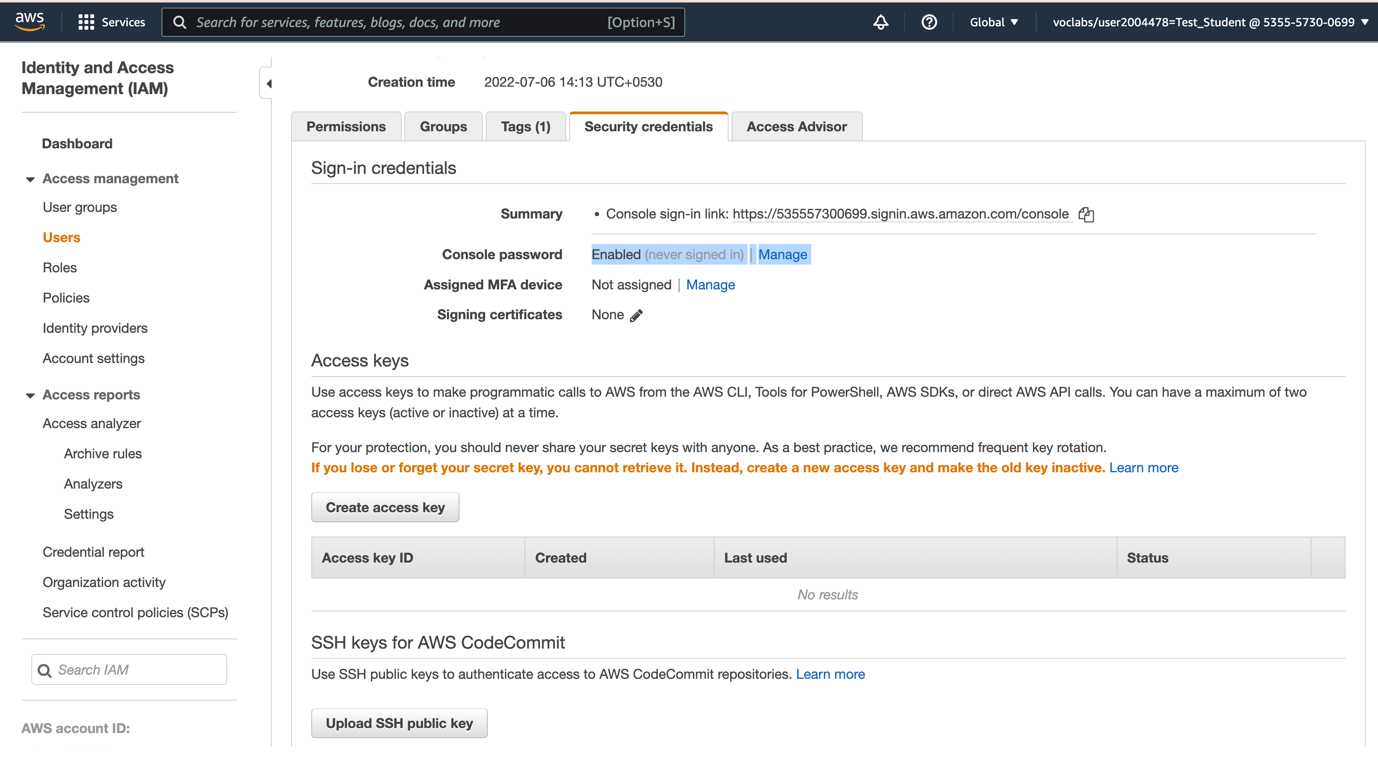
Note that User -1 is not Part of any group



# Choose the Security credentials tab.

Note that User 1 is not provided specific password and the console credentials can be used to sign in .User -1 is given the console password .

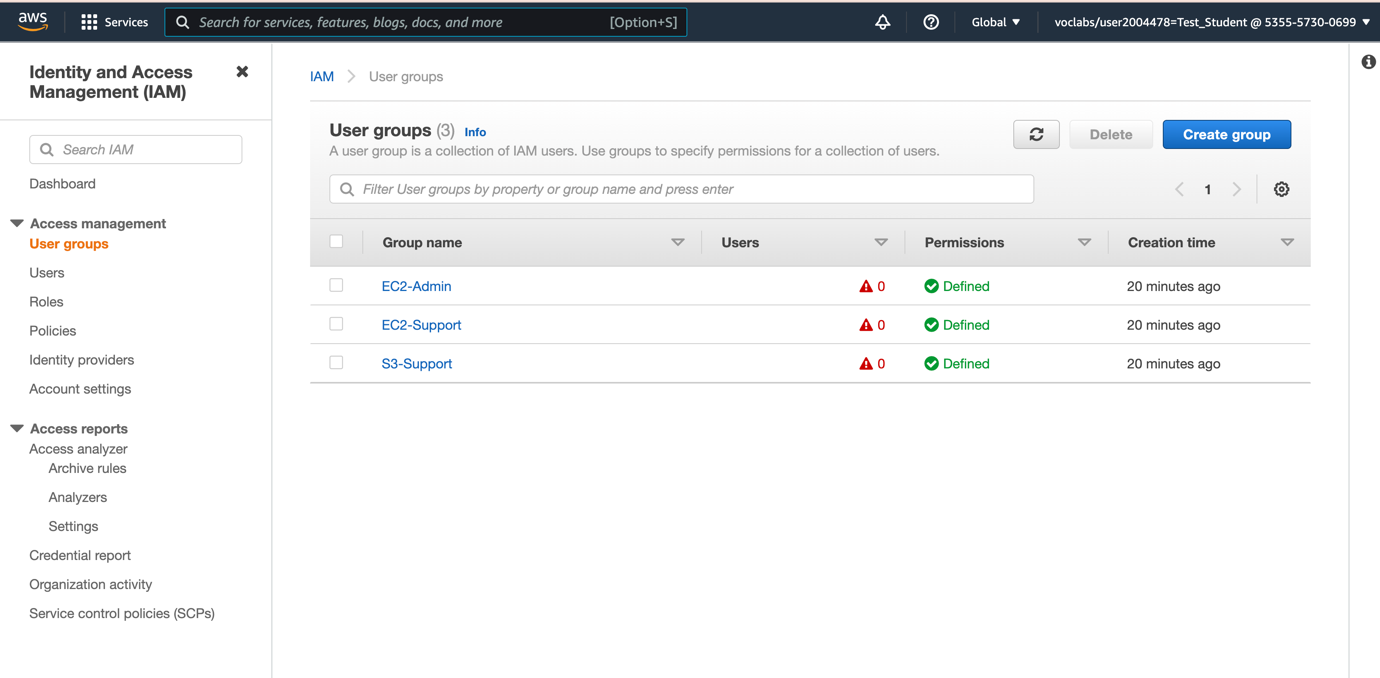
In this lab the console password is not known as we sign in using the Access Key and Secret Key.



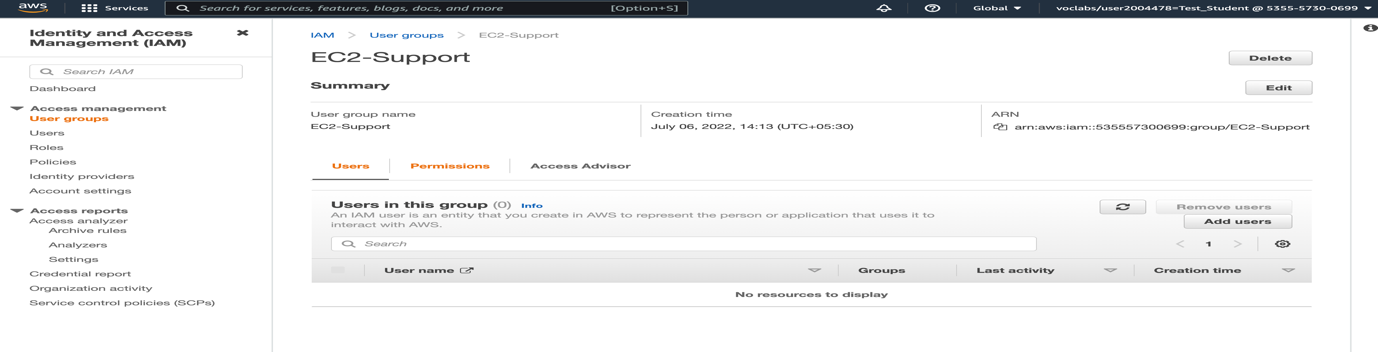
# In the navigation pane on the left, choose **User groups**.

Note that the following groups have already been created for you:

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

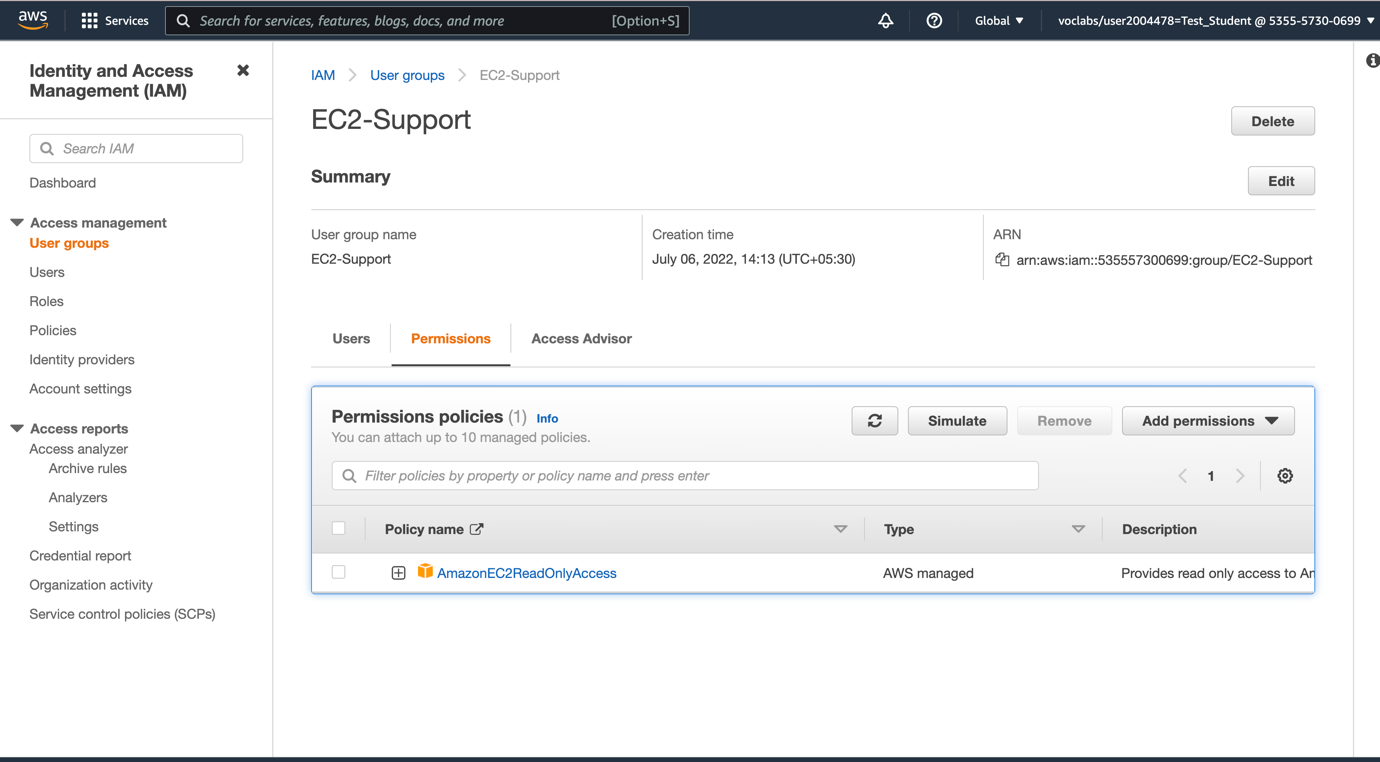


# Choose the **EC2-Support** group.

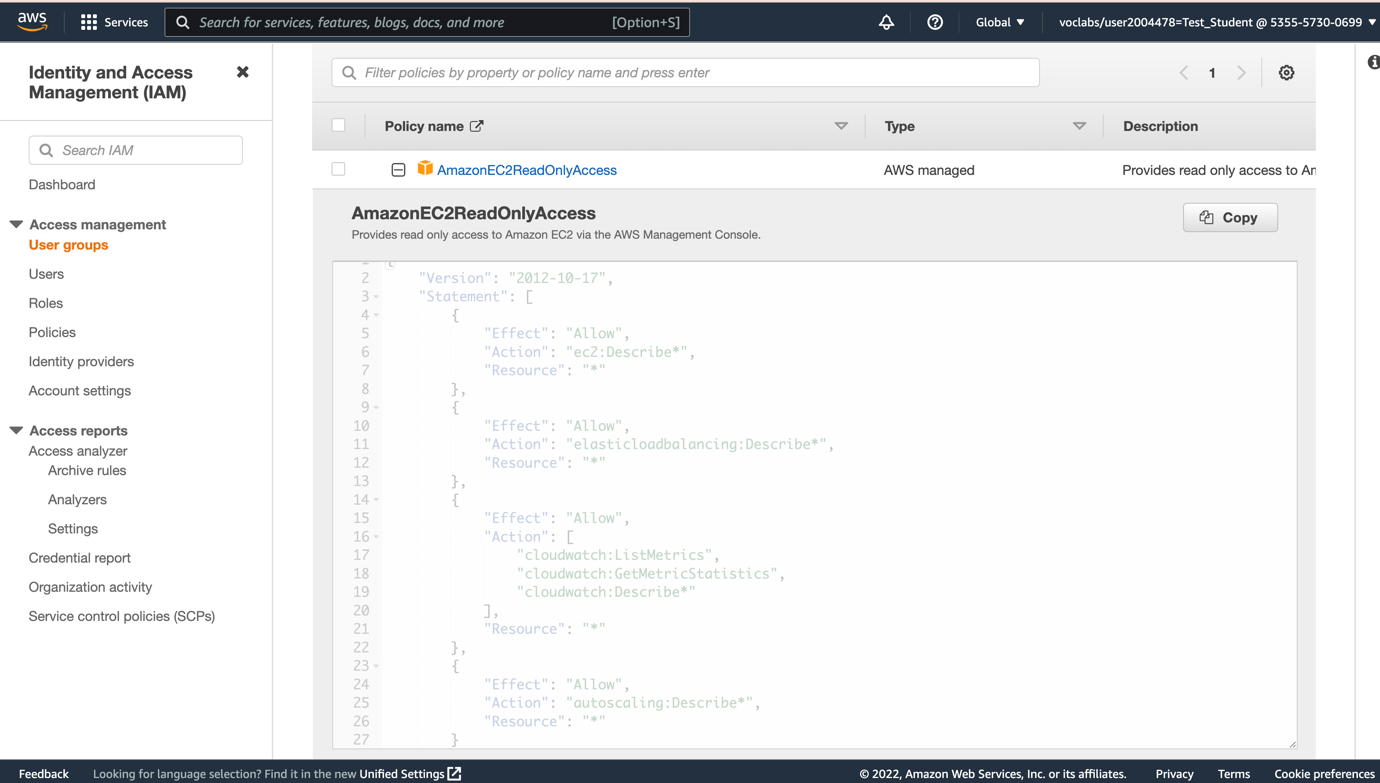


# Choose the Permissions Tab

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.



# Expand **AmazonEC2ReadOnlyAccess** to view the policy.



# What is a Policy

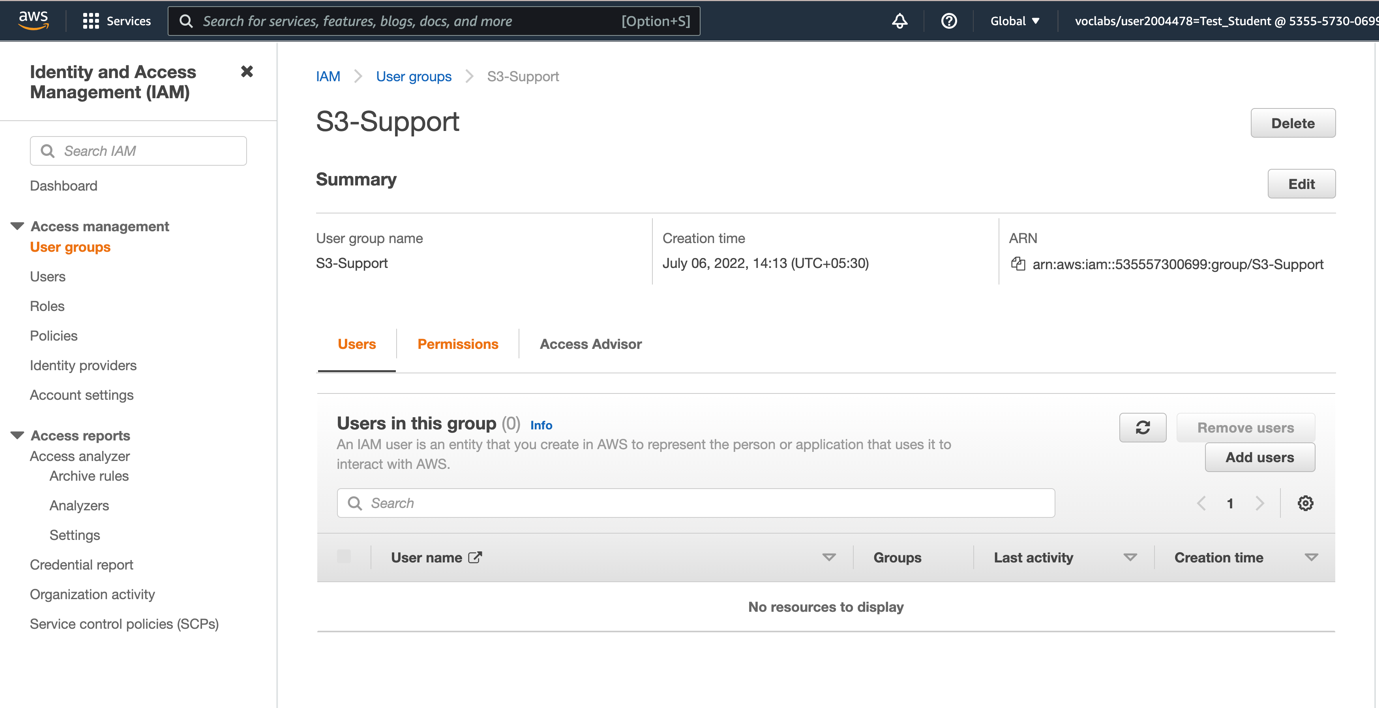
A policy defines what actions are allowed or denied for specific AWS resources. This policy is granting permission to List and Describe information about EC2, Elastic Load Balancing, CloudWatch and Auto Scaling. This ability to view resources, but not modify them, is ideal for assigning to a Support role.

The basic structure of the statements in an IAM Policy is:

* + **Effect** says whether to *Allow* or *Deny* the permissions.
  + **Action** specifies the API calls that can be made against an AWS Service (eg *cloudwatch:ListMetrics*).
  + **Resource** defines the scope of entities covered by the policy rule (eg a specific Amazon S3 bucket or Amazon EC2 instance, or \* which means *any resource*).

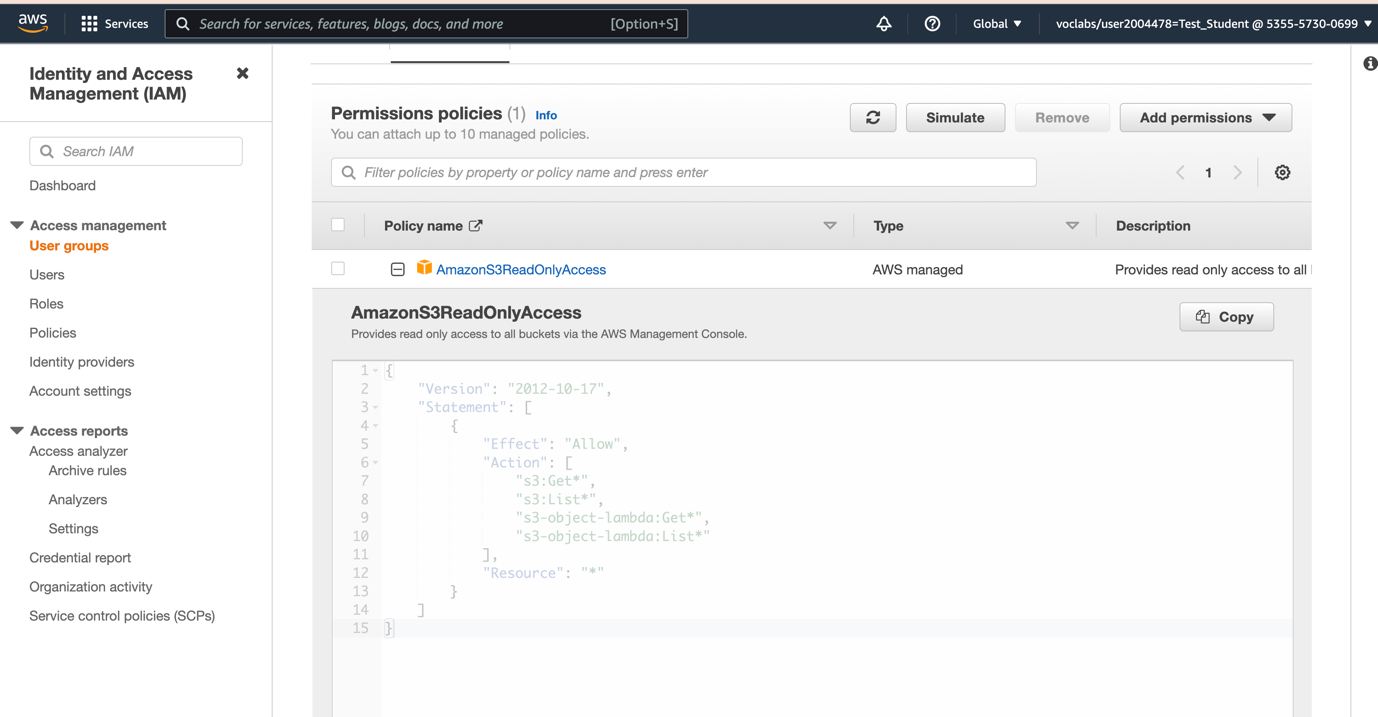
# In the navigation pane on the left, choose **User groups**.

## Choose the **S3-Support** group followed by the **Permissions** tab

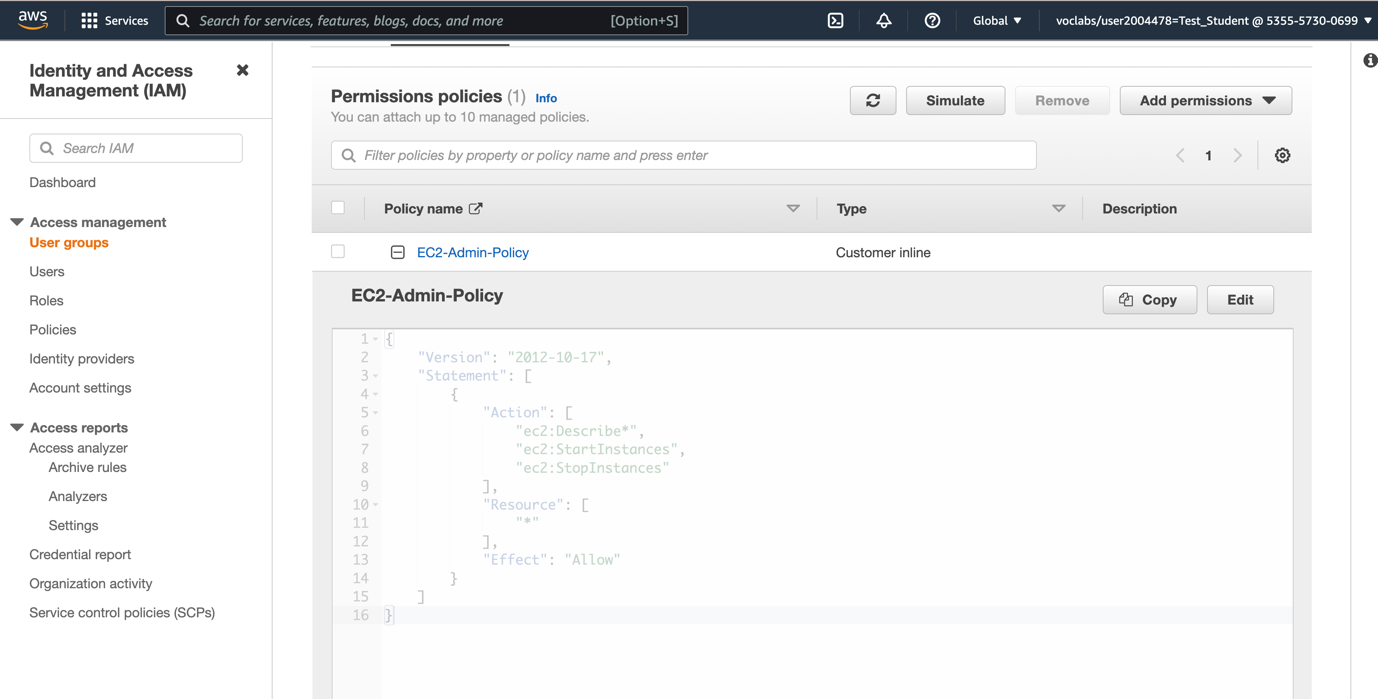




# Expand **AmazonS3ReadOnlyAccess** to view the attached policy.



# In the navigation pane on the left, choose **User groups**. Choose the **EC2-Admin** group followed by the **Permissions** tab



# Business Scenario

For the remainder of this lab, you will work with these Users and Groups to enable permissions supporting the following business scenario:

Your company is growing its use of Amazon Web Services, and is using many Amazon EC2 instances and a great deal of Amazon S3 storage. You wish to give access to new staff depending upon their job function:

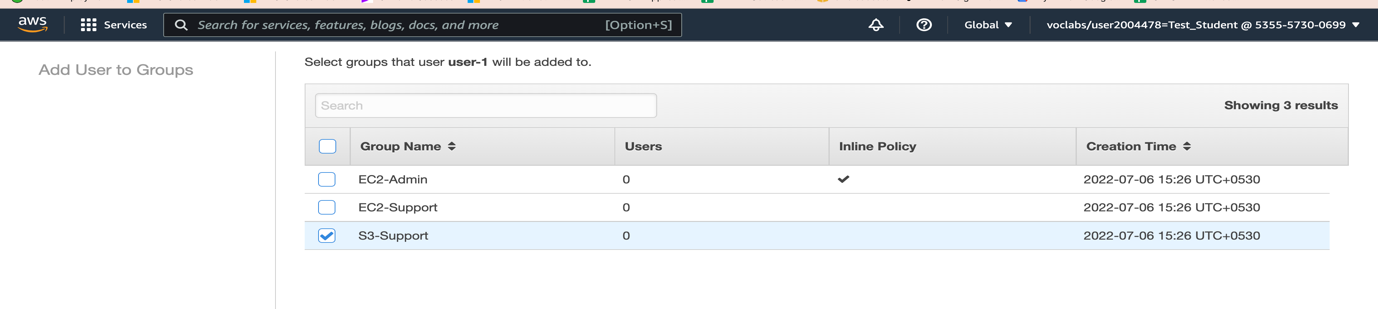
| **User** | **In Group** | **Permissions** |
| --- | --- | --- |
| user-1 | S3-Support | Read-Only access to Amazon S3 |
| user-2 | EC2-Support | Read-Only access to Amazon EC2 |
| user-3 | EC2-Admin | View, Start and Stop Amazon EC2 instances |

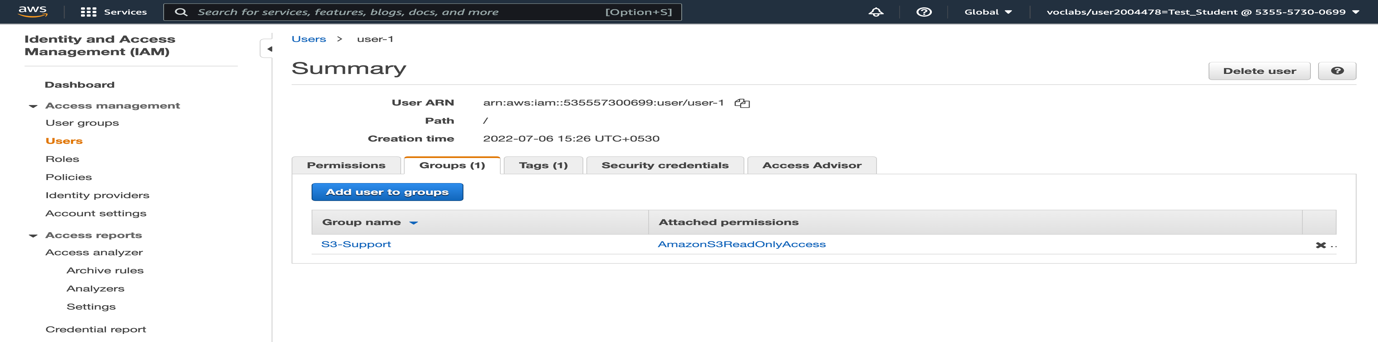
# Task 2: Add Users to Groups

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.

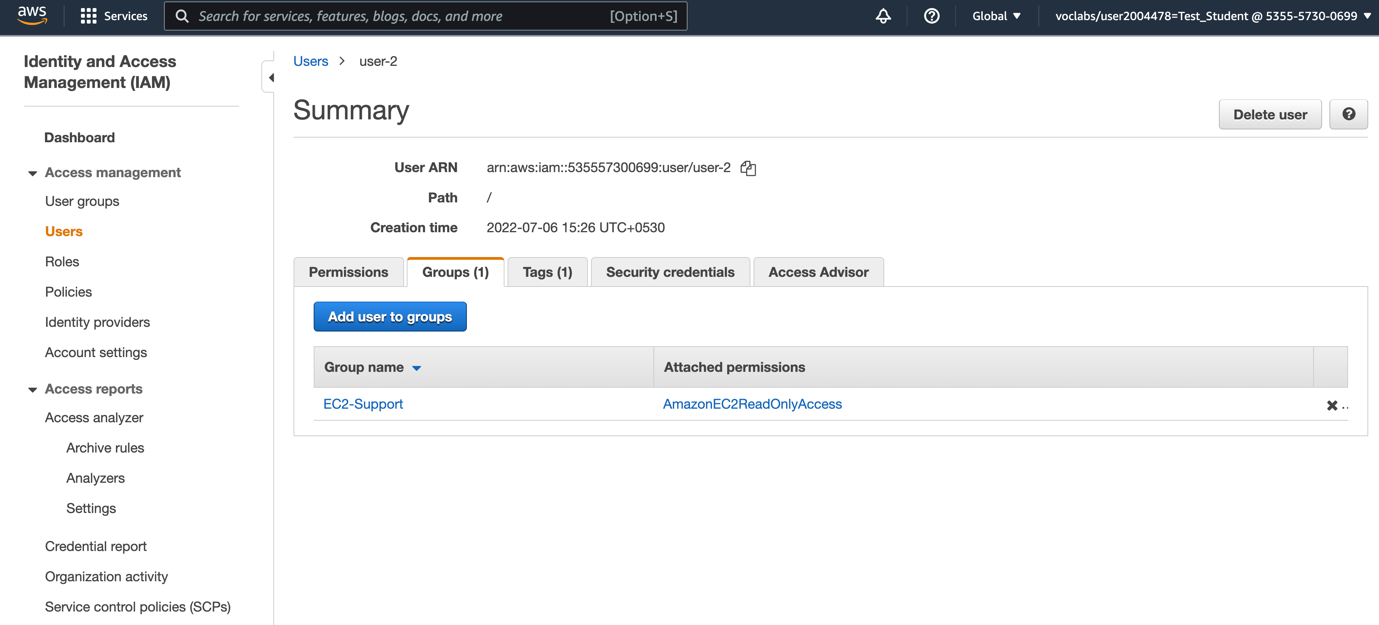
## Step -1 Add user-1 to the S3-Support Group

*Click On User -1 and in the groups icon add user -1 to S3-Support Group*

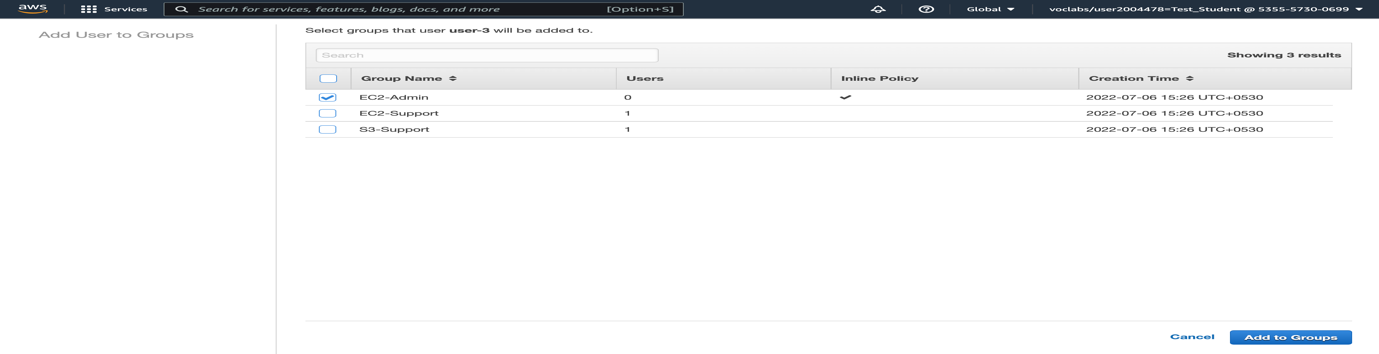
**

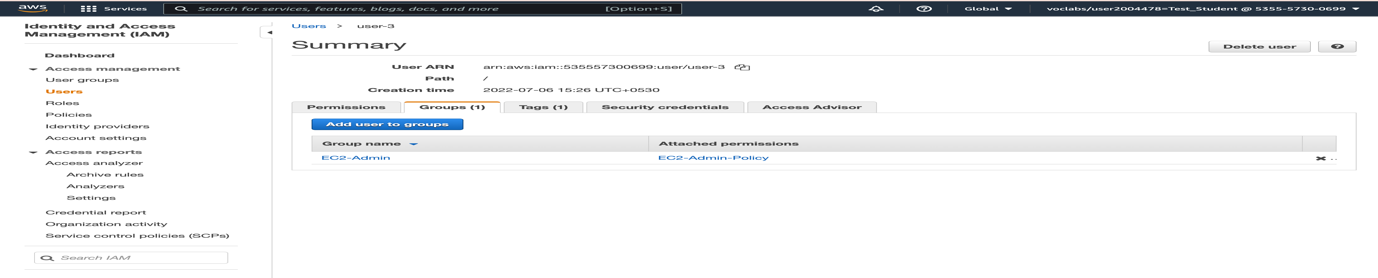
**

## Step -2 Add user-2 to the EC2-Support Group



# Step-3 Add User -3 to the EC2-Admin Group





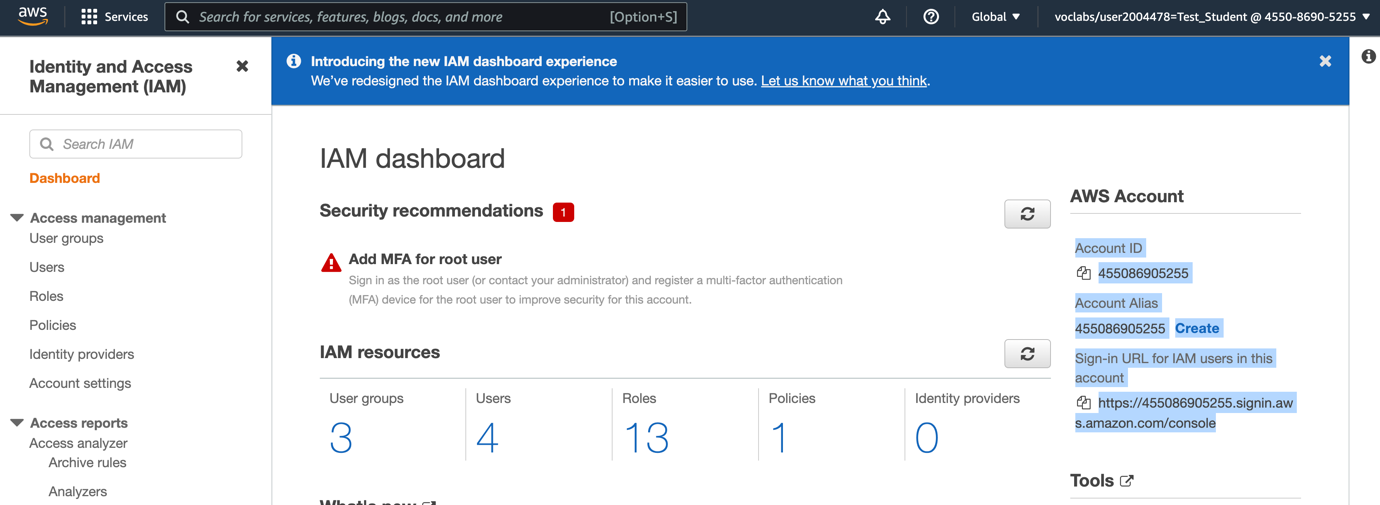
# Sign in and Test Users added to Groups

## Task 3: Sign-In and Test Users

In this task, you will test the permissions of each IAM User.

In the navigation pane on the left, choose **Dashboard**.

An **IAM users sign-in link** is displayed in the right side of the window. It will look similar to: <https://123456789012.signin.aws.amazon.com/console>

**

This link can be used to sign-in to the AWS Account you are currently using.

Copy the **IAM users sign-in link** to a text editor.

Open a private window.

**Mozilla Firefox**

* + Choose the menu bars at the top-right of the screen
  + Select **New Private Window**

**Google Chrome**

* + Choose the ellipsis at the top-right of the screen
  + Choose **New incognito window**

**Microsoft Edge**

* + Choose the ellipsis at the top-right of the screen
  + Choose **New InPrivate window**

**Microsoft Internet Explorer**

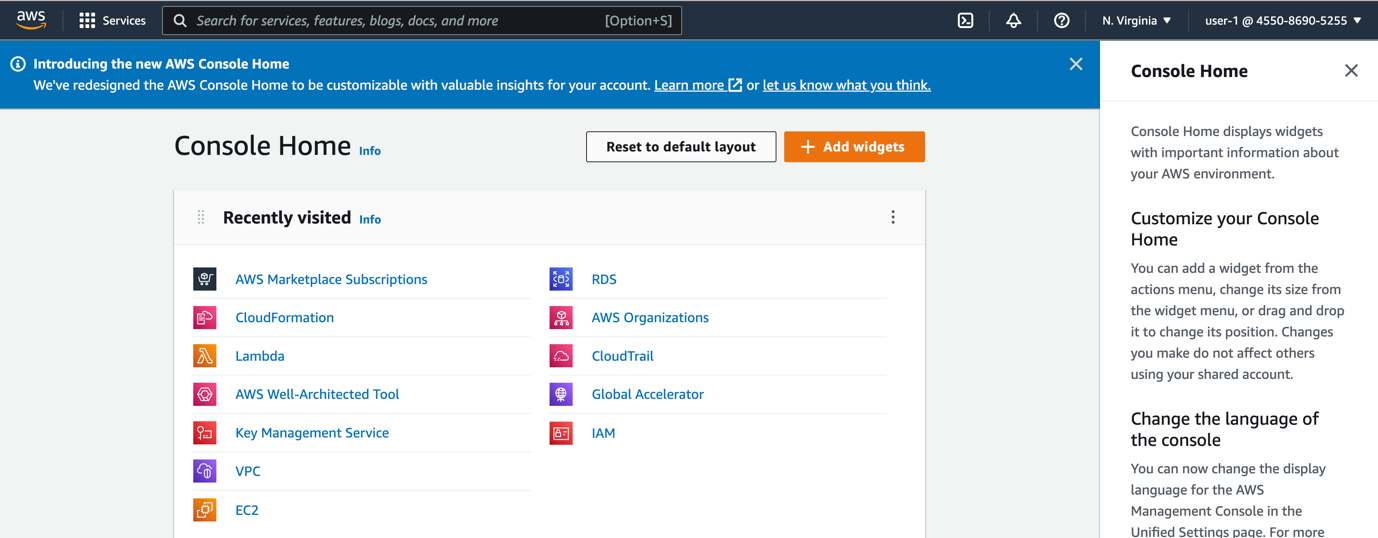
* + Choose the **Tools** menu option
  + Choose **InPrivate Browsing**

Paste the **IAM users sign-in** link into your private window and press **Enter**.

You will now sign-in as **user-1**, who has been hired as your Amazon S3 storage support staff.

Sign-in with:

* + **IAM user name:** user-1
  + **Password:** Lab-Password1



In the **Services** menu, choose **S3**.

Choose the name of one of your buckets and browse the contents.

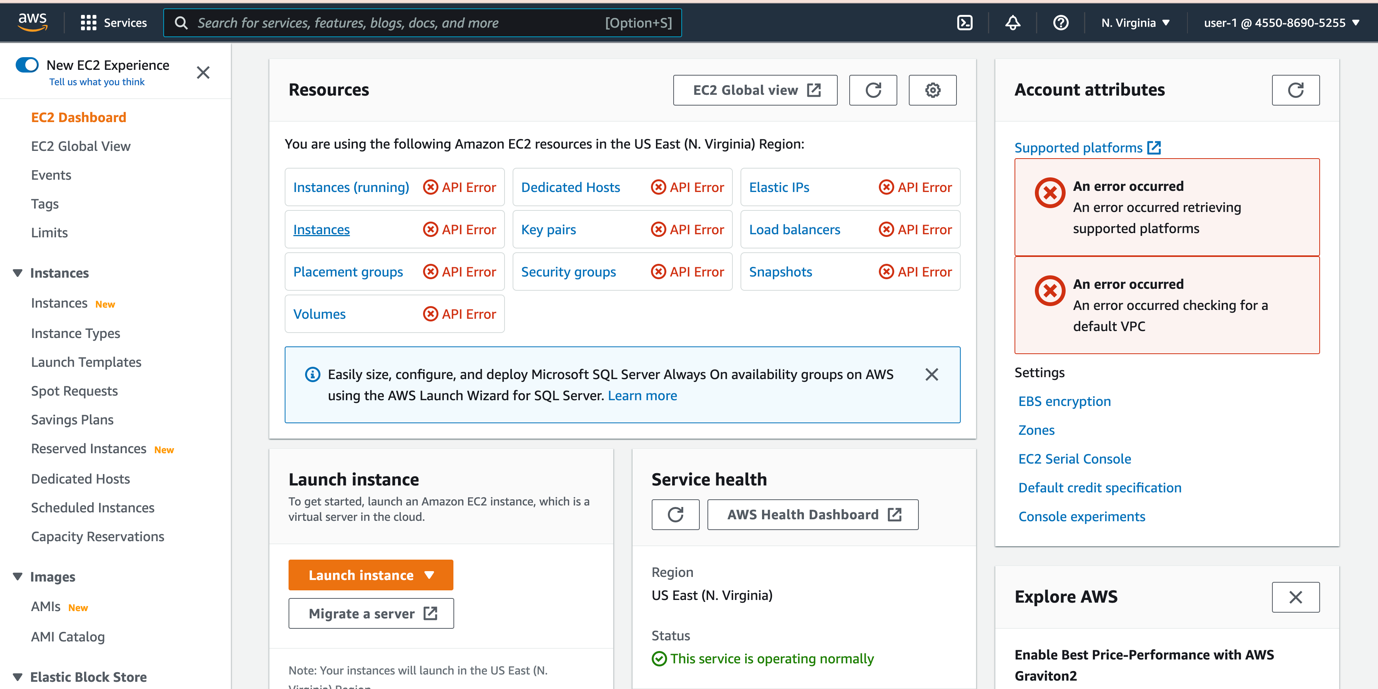
Since your user is part of the **S3-Support** Group in IAM, they have permission to view a list of Amazon S3 buckets and their contents.

Now, test whether they have access to Amazon EC2.

In the **Services** menu, choose **EC2**.

In the left navigation pane, choose **Instances**.

You cannot see any instances! Instead, it states You are not authorized to perform this operation. This is because your user has not been assigned any permissions to use Amazon EC2.



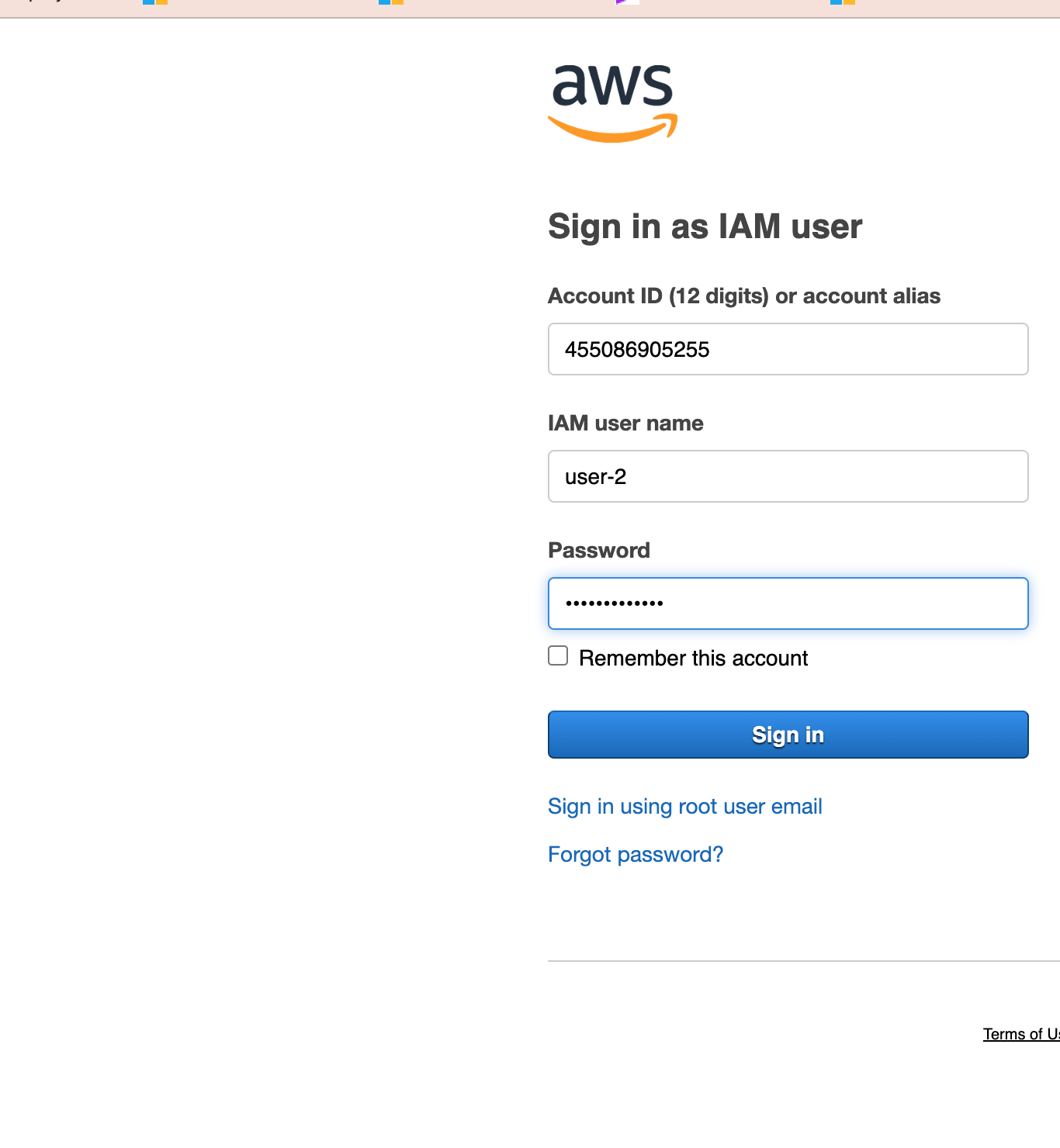
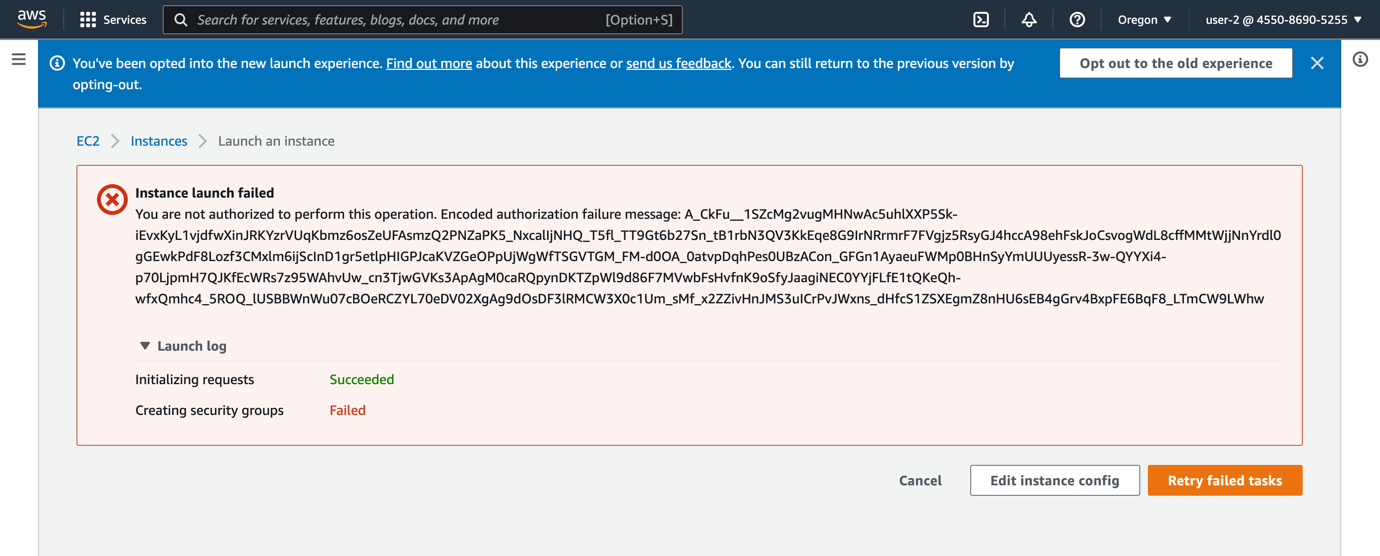
Sign-in with:

**IAM user name:** user-2

**Password:** Lab-Password2

In the **Services** menu, choose **EC2**.

In the navigation pane on the left, choose **Instances**.

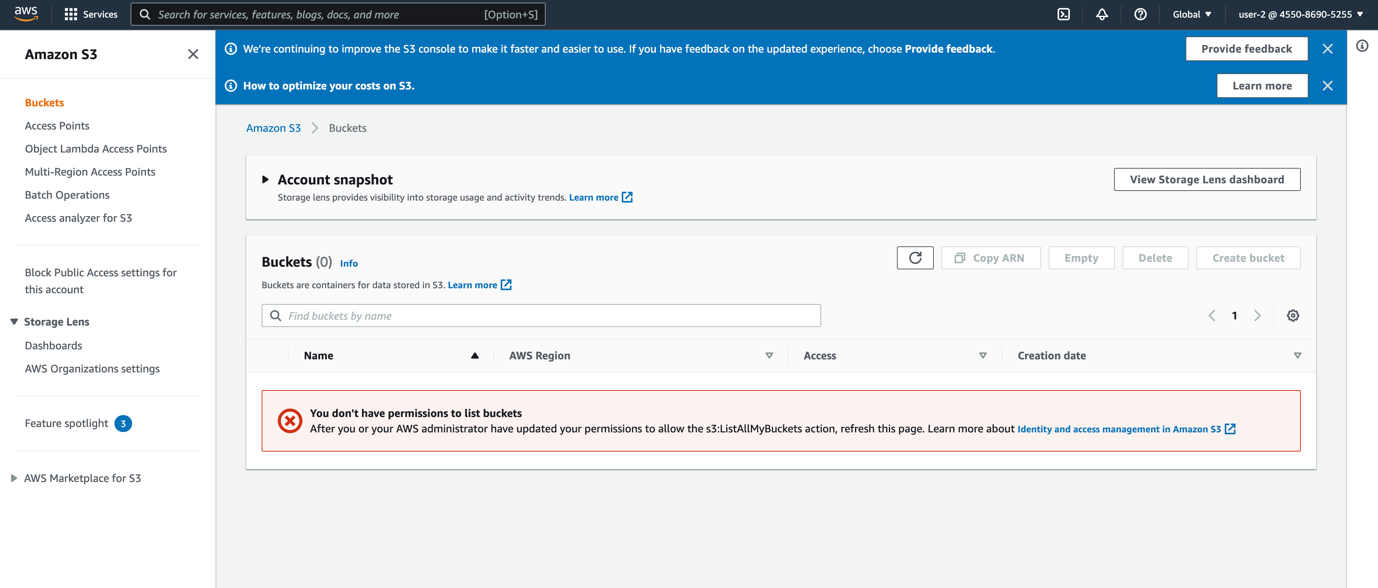
You are now able to see an Amazon EC2 instance because you have Read Only permissions. However, you will not be able to make changes in EC-2

Close the **Failed to stop the instance ..** window.

Next, check if user-2 can access Amazon S3.

In the **Services**, choose **S3**.

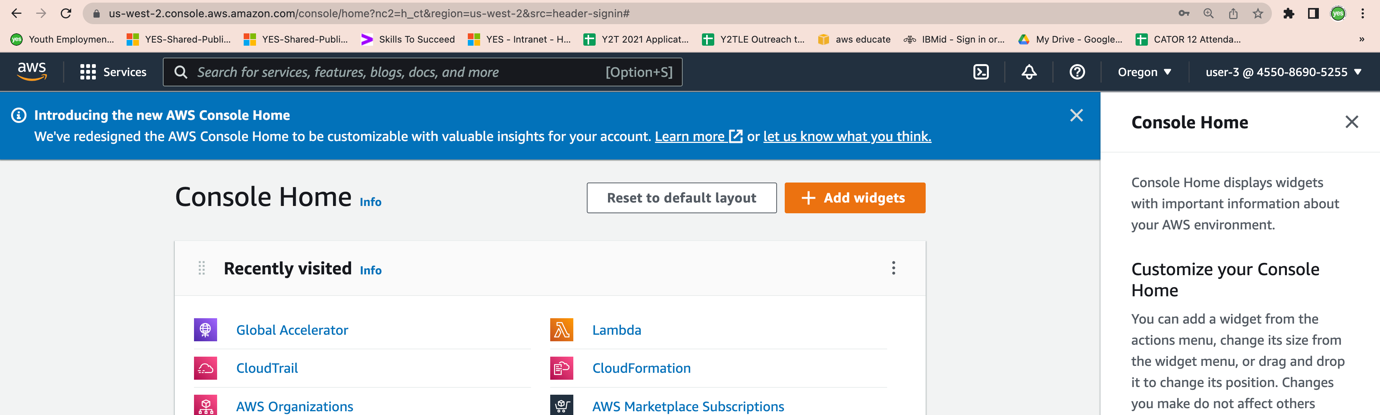
You will receive an **You don't have permissions to list buckets** error because user-2 does not permission to use Amazon S3.



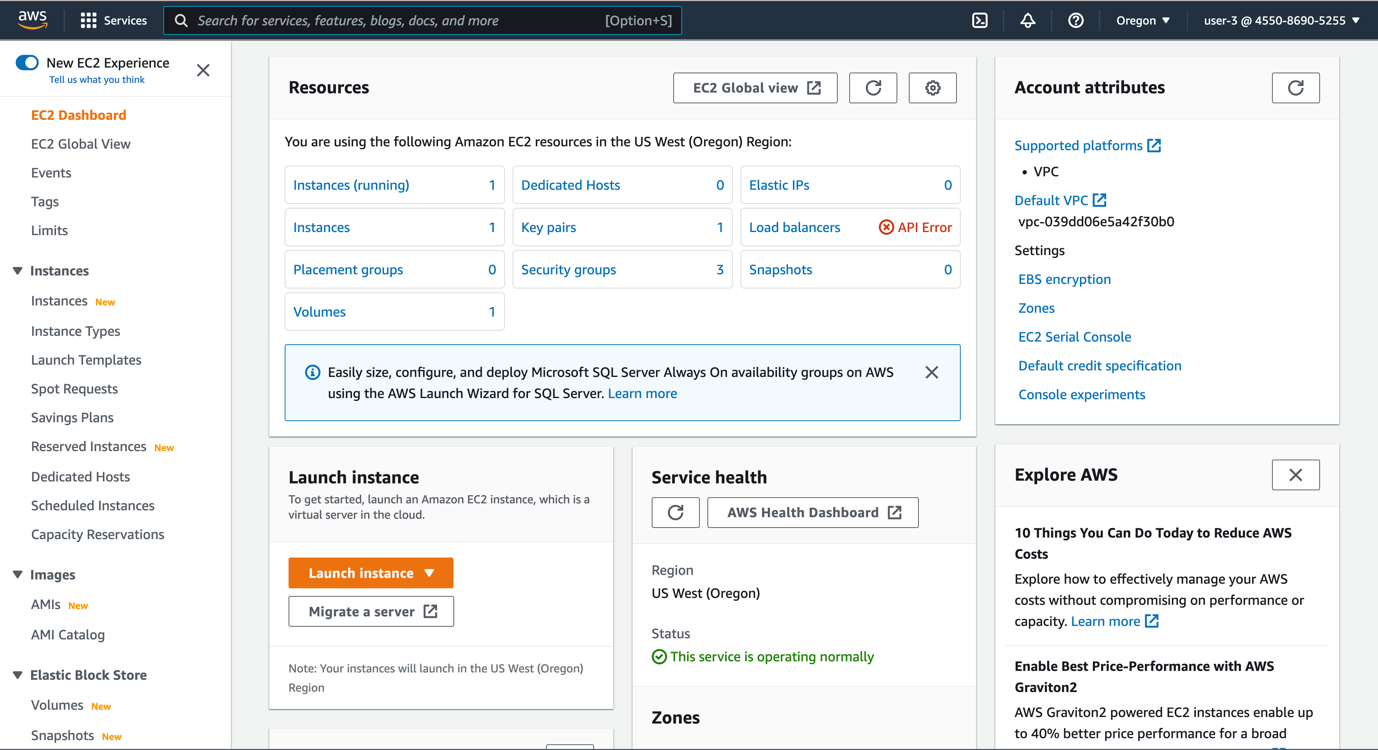
Paste the sign-in link into your web browser address bar again. If it is not in your clipboard, retrieve it from the text editor where you stored it earlier.

Sign-in with:

* + **IAM user name:** user-3
  + **Password:** Lab-Password3



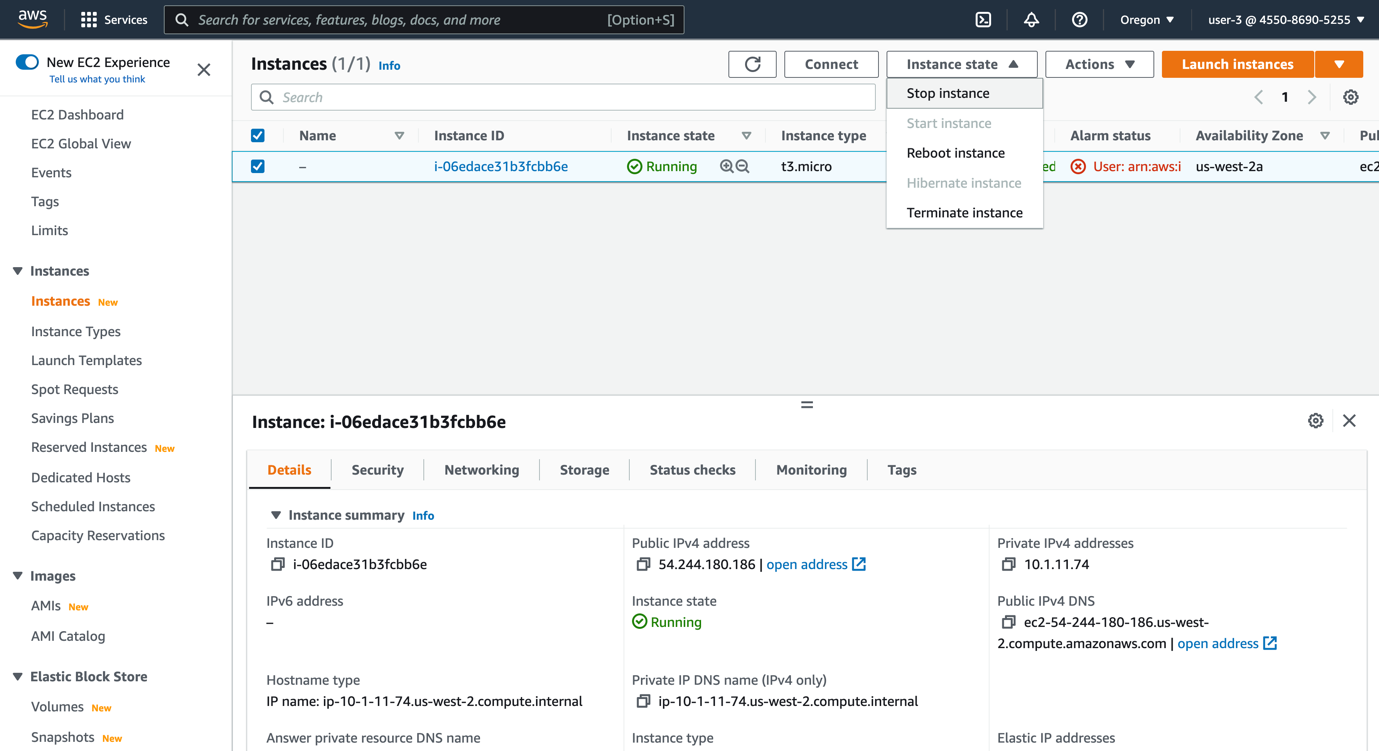
In the **Services** menu, choose **EC2**.



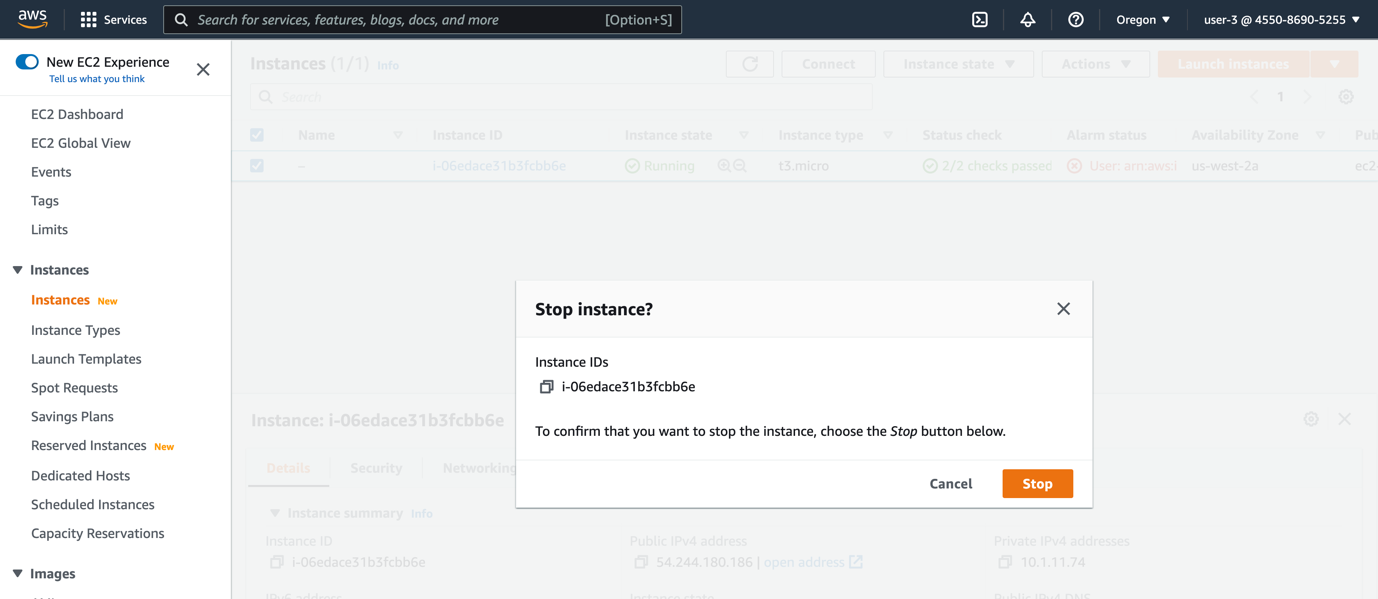
In the navigation pane on the left, choose **Instances**.



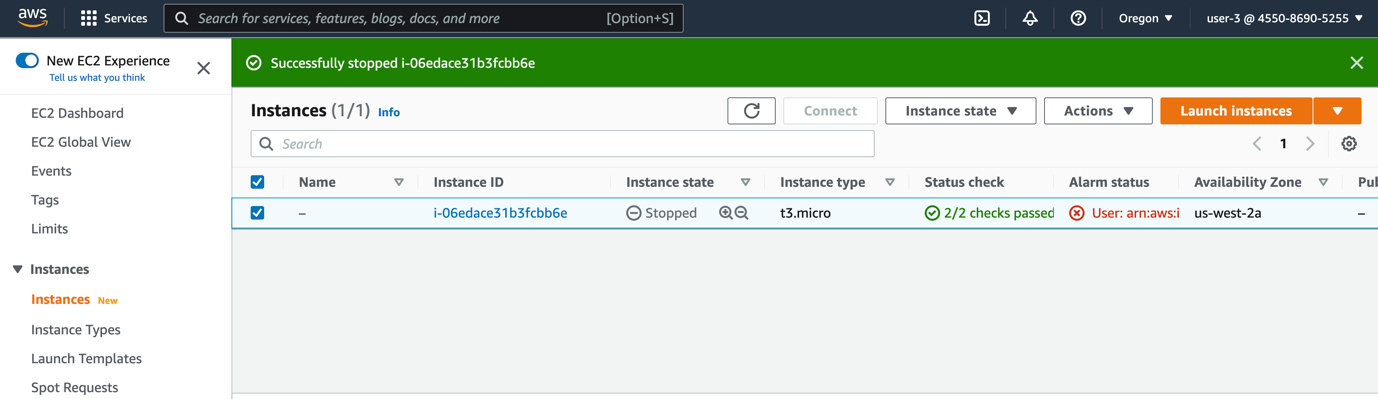
As an EC2 Administrator, you should now have permissions to Stop the Amazon EC2 instance.



Your EC2 instance should be selected . If it is not, please select it.



Wait for a couple of minutes to check if the lab is stopped



# Conclusion

In this lab we added users to groups which had policies attached to the groups and verified that users added to groups were constrained by the principle of least privilege to access aws services as mandated by the Policies.

# LAB Complete