



COS20019

Cloud Computing Architecture

Week 6 – ACF Lab 1:  
Intro to AWS IAM

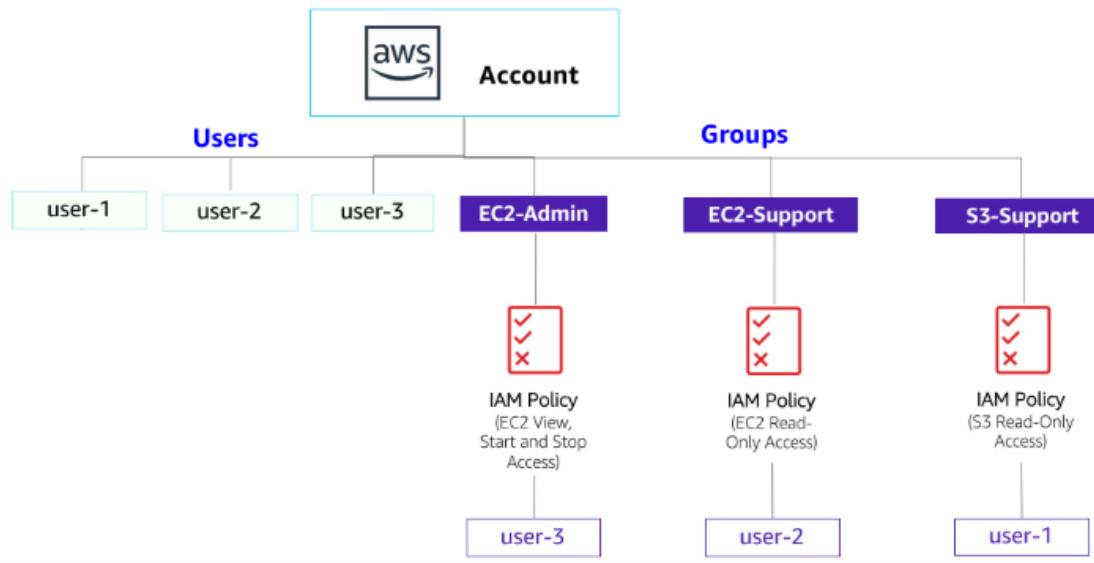
Truong Ngoc Gia Hieu  
105565520

# Lab 1: Introduction to AWS 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.

## A. Lab overview and objectives

This lab will demonstrate:



- Exploring pre-created **IAM Users and Groups**
- Inspecting **IAM policies** as applied to the pre-created groups
- Following a **real-world scenario**, adding users to groups with specific capabilities enabled
- Locating and using the **IAM sign-in URL**
- Experimenting with the effects of policies on service access

## AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that are needed to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that are described in this lab.

## 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.

## Duration

This lab takes approximately **40 minutes** to complete.

## B. Accessing the AWS Management Console

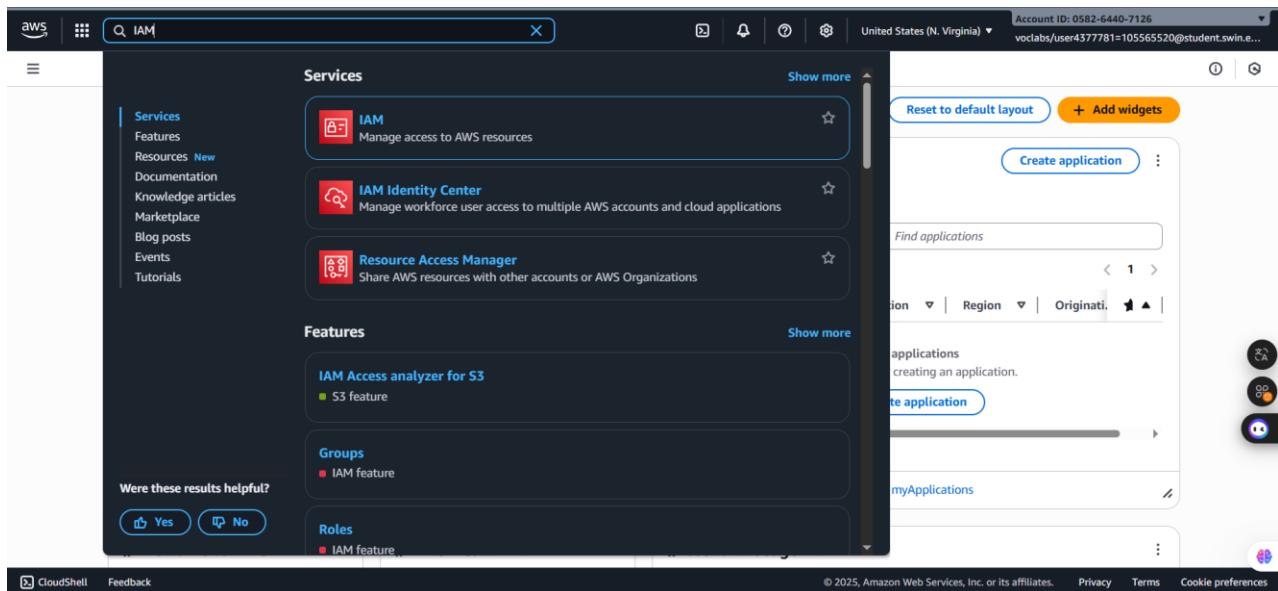
At the top of the lab, click the  **Start Lab** button to start lab and wait until the button next to the AWS turns from red to green.



*Figure 1: AWS Management Console Activated*

## C. Task 1: Explore the Users and Groups

**Step 1.1:** After opening the AWS Management Console, search IAM in the box which next to the service icon and select the first one.

**Figure 2: Search and select the IAM**

**Step 1.2:** In the IAM Homepage, choose Users in the left navigation which already contains three following created IAM users:

- user-1
- user-2
- user-3

Users (4) <small>Info</small>							
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.							
	User name	Path	Groups	Last activity	MFA	Password age	Console last s
	awsstudent	/	Access denied	Access denied	Access denied	Access denied	-
	user-1	/spl66/	0	-	-	9 minutes	-
	user-2	/spl66/	0	-	-	9 minutes	-
	user-3	/spl66/	0	-	-	9 minutes	-

**Figure 3: Users**

**Step 1.4:** Select the user-1 itself to confirm these following instructions:

- Permissions** tab: for user-1 does not have any permissions
- Groups** tab: user-1 also is not a member of any groups.
- Security Credentials**: user-1 is assigned a **Console password**.

**Permissions policies (0)**

Permissions are defined by policies attached to the user directly or through groups.

**Filter by Type**  
All types

**Policy name** ▲ | Type ▼ | Attached via ▾

No resources to display

**▼ Permissions boundary (not set)**  
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more about permission boundaries](#)

[Set permissions boundary](#)

**▼ Generate policy based on CloudTrail events**  
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

[Generate policy](#)

No requests to generate a policy in the past 7 days.

*Figure 4: Permissions tab*

**Identity and Access Management (IAM)**

**Summary**

ARN: arn:aws:iam::058264407126:user/spl66/user-1

Console access: Enabled without MFA

Access key 1: AKIAQ3EGUJRL2PV5DVP - Active  
Never used. Created today.

Access key 2: Create access key

**Permissions** | **Groups** (selected) | **Tags (1)** | **Security credentials** | **Last Accessed**

**User groups membership**

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.

**Groups** | **Attached policies** ▾

No resources  
This user does not belong to any groups.

*Figure 5: Groups tab*

**Identity and Access Management (IAM)**

**Created**: September 24, 2025, 17:38 (UTC+07:00)

**Last console sign-in**: Never

**ACCESS KEY 2**: Create access key

**Permissions** | **Groups** | **Tags (1)** | **Security credentials** (selected) | **Last Accessed**

**Console sign-in**

Console sign-in link: <https://058264407126.signin.aws.amazon.com/console>

Console password: Updated 20 minutes ago (2025-09-24 17:39 GMT+7)

Last console sign-in: Never

**Multi-factor authentication (MFA) (0)**

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

**Type** | **Identifier** | **Certifications** | **Created on**

No MFA devices. Assign an MFA device to improve the security of your AWS environment

[Assign MFA device](#)

*Figure 6: Security Credentials tab*

**Step 1.5:** Select the **User groups** in the left navigation to see following already user groups:

- EC2-Admin
- EC2-Support
- S3-Support

The screenshot shows the AWS IAM User groups page. On the left, there's a navigation pane with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'User groups' is also selected. The main area displays a table titled 'User groups (3)'. The table has columns for 'Group name', 'Users', 'Permissions', and 'Creation time'. Three groups are listed: EC2-Admin, EC2-Support, and S3-Support, all created 22 minutes ago. Each group has 0 users and 0 permissions defined.

Figure 7: User groups

**Step 1.6:** Select each group and see **Permissions** tab to see the policy name inside of each group.

The screenshot shows the AWS IAM EC2-Support group page. The left navigation pane shows 'User groups' selected. The main area shows the 'EC2-Support' group details. Under the 'Permissions' tab, it shows one policy attached: 'AmazonEC2ReadOnlyAccess'. This policy is of type 'AWS managed' and has 1 attached entity.

Figure 8: EC2-Support group

The screenshot shows the AWS IAM User Groups page for the 'EC2-Admin' group. The 'Permissions' tab is selected. Under 'Permissions policies (1)', there is one policy named 'EC2-Admin-Policy'. The ARN of the policy is listed as 'arn:aws:iam:058264407126:group/spl66/EC2-Admin'.

**Figure 9: EC2-Admin group**

The screenshot shows the AWS IAM User Groups page for the 'S3-Support' group. The 'Permissions' tab is selected. Under 'Permissions policies (1)', there is one policy named 'AmazonS3ReadOnlyAccess'. The ARN of the policy is listed as 'arn:aws:iam:058264407126:group/spl66/S3-Support'.

**Figure 10: S3-Support group**

## 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

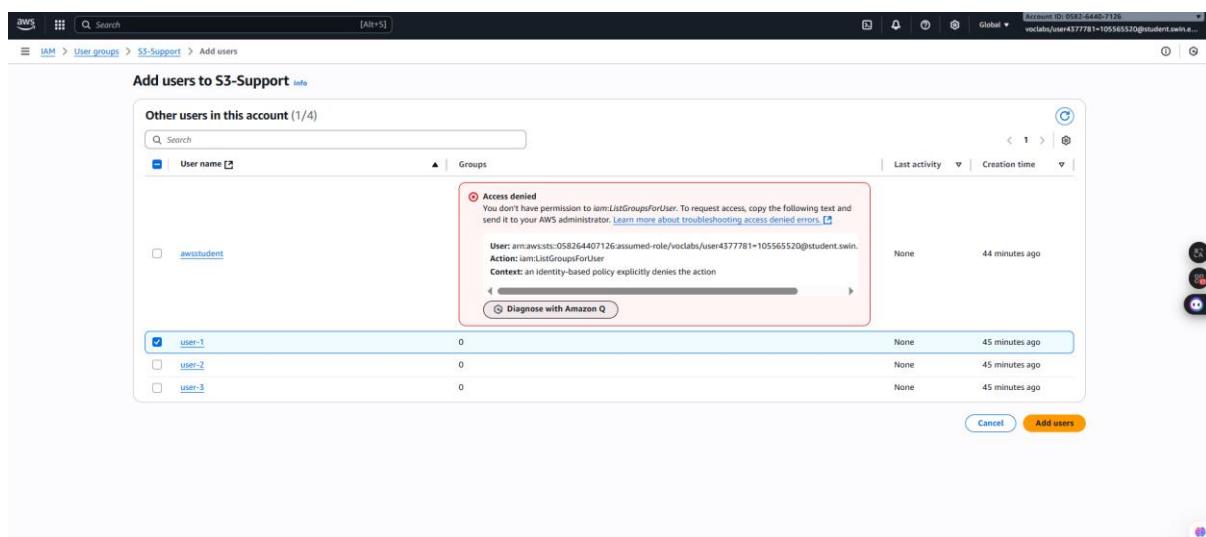
## D. Task 2: Add Users to Groups

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.

 You can ignore any "not authorized" errors that appear during this task. They are caused by your lab account having limited permissions and will not impact your ability to complete the lab.

### Step 2.1: Add user-1 to the S3-Support Group

- First and foremost, choose the User groups in the left navigation pane and select the **S3-Support** group link. After that, Choose the Users tab. Then, In the **Users** tab, choose **Add users**.
- In the **Add users to S3-Support** configuration window, select the **user-1** and choose at the bottom of the screen.



*Figure 11: Add user-1 to S3-Support configuration window*

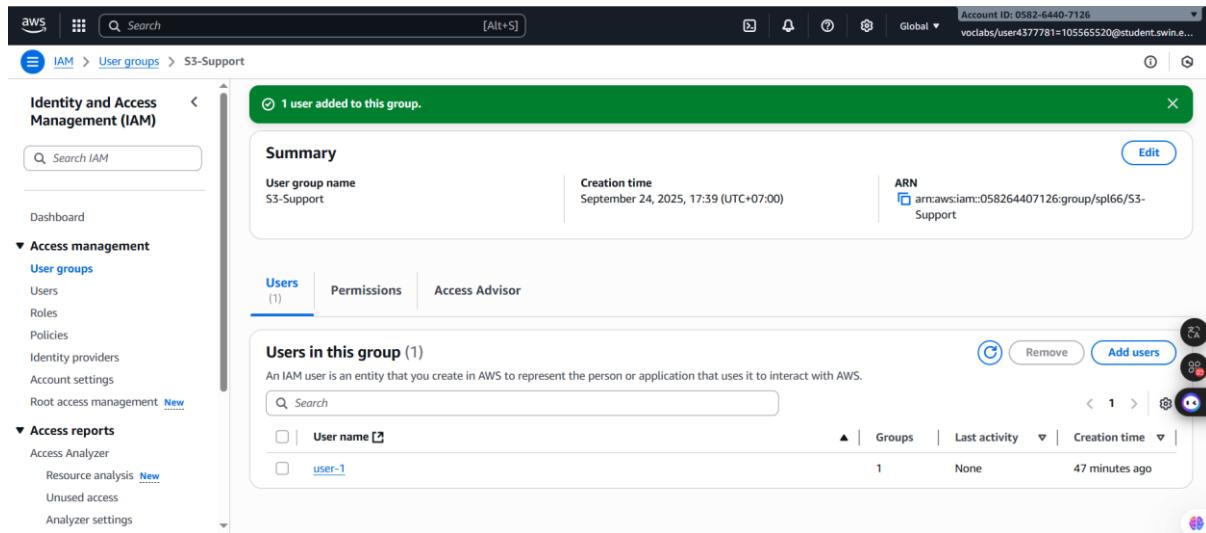


Figure 12: Add user-1 to S3-Support successfully

### Step 2.2: Add user-2 to the EC2-Support Group

- Second, choose the User groups in the left navigation pane and select the EC2-Support group link. After that, Choose the Users tab. Then, In the **Users** tab, choose **Add users**.
- In the **Add users to EC2-Support** configuration window, select the **user-1** and choose **Add users** at the bottom of the screen

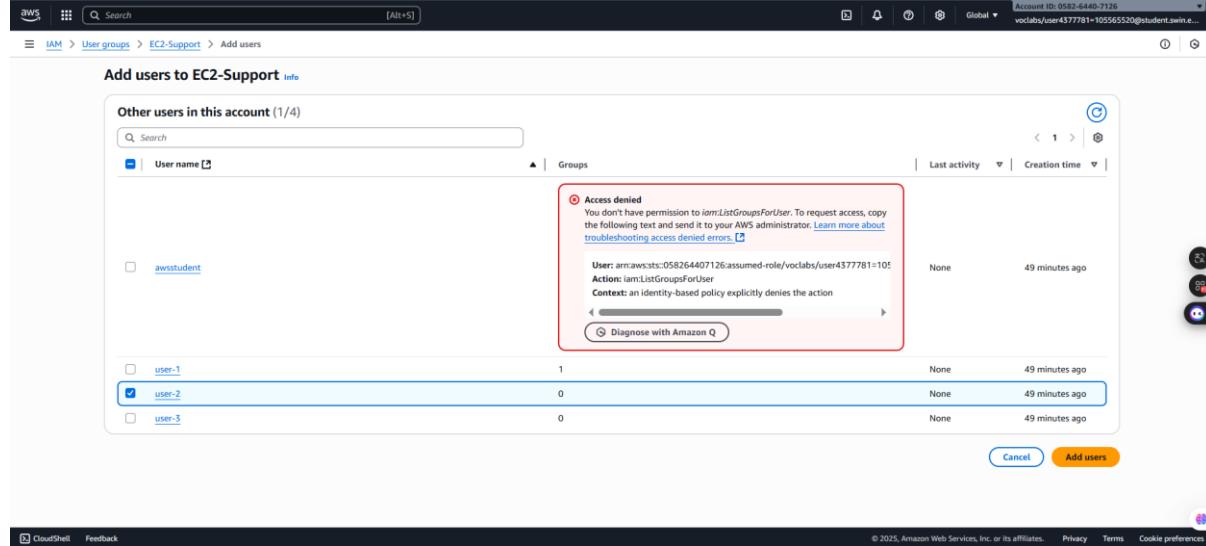
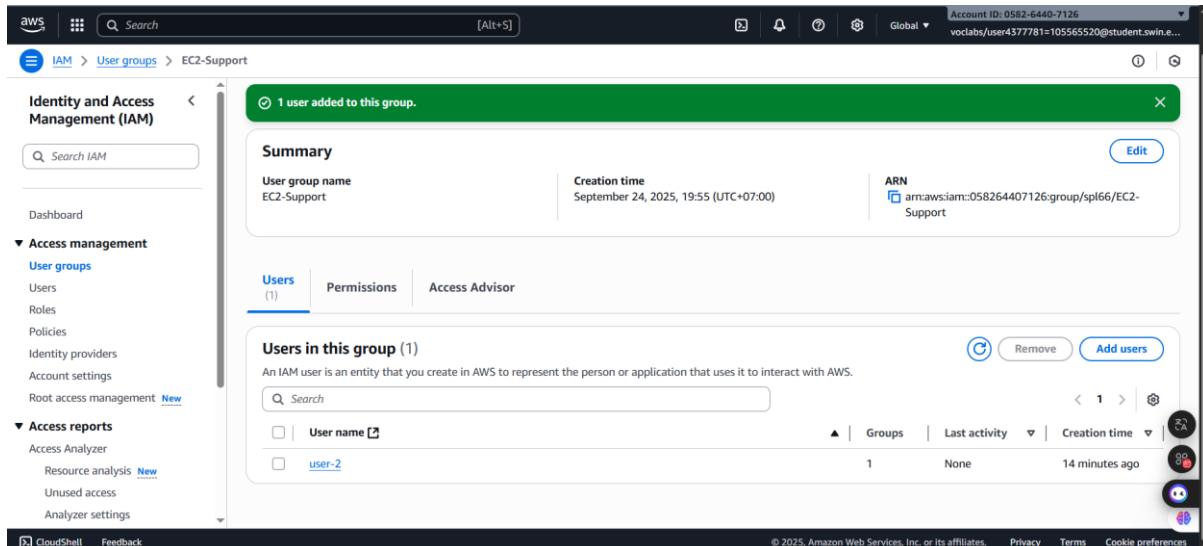


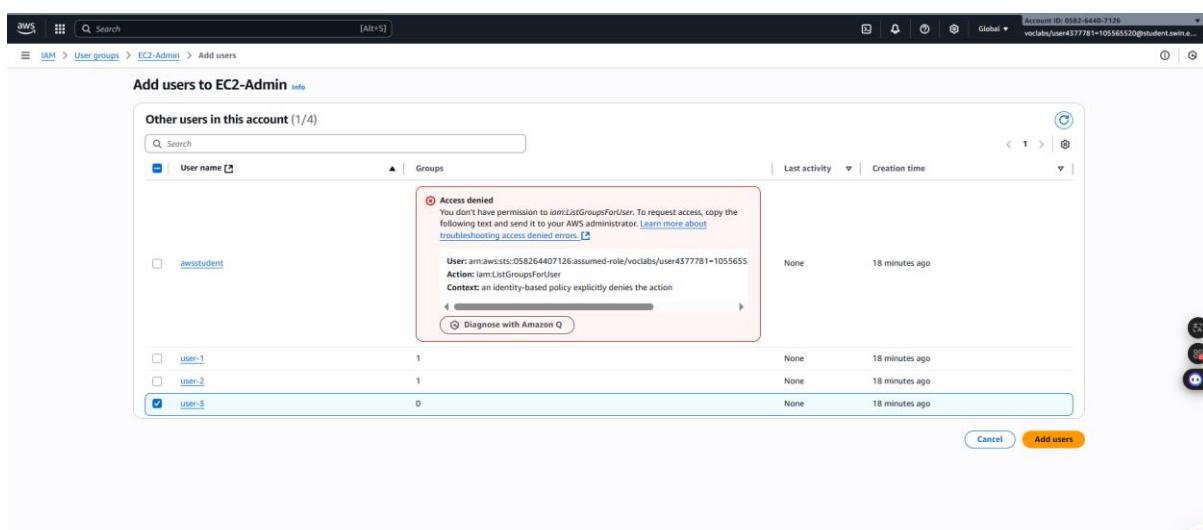
Figure 13: Add user-2 to EC2-Support configuration window



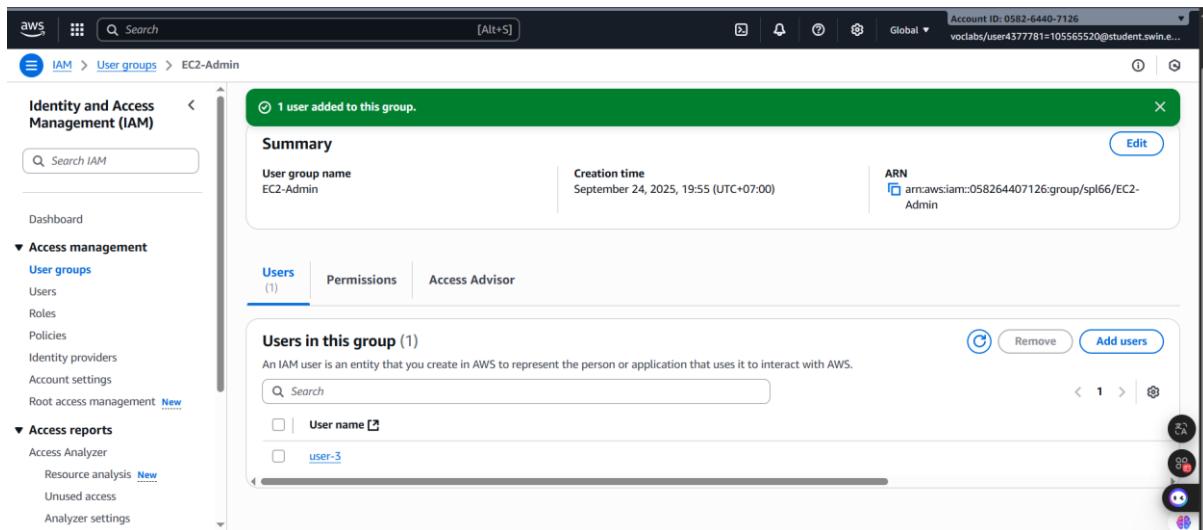
**Figure 14: Add user-2 to EC2-Support successfully**

### Step 2.3: Add user-3 to the EC2-Admin Group

- Third. choose the User groups in the left navigation pane and select the **EC2-Admin** group link. After that, Choose the Users tab. Then, In the **Users** tab, choose **Add users**.
- In the **Add users to EC2-Admin** configuration window, select the **user-3** and choose **Add users** at the bottom of the screen



**Figure 15: Add user-3 to EC2-Admin configuration window**



**Figure 16: Add user-3 to EC2-Admin successfully**

#### Step 2.4: Confirm that each User Group has 1 Users

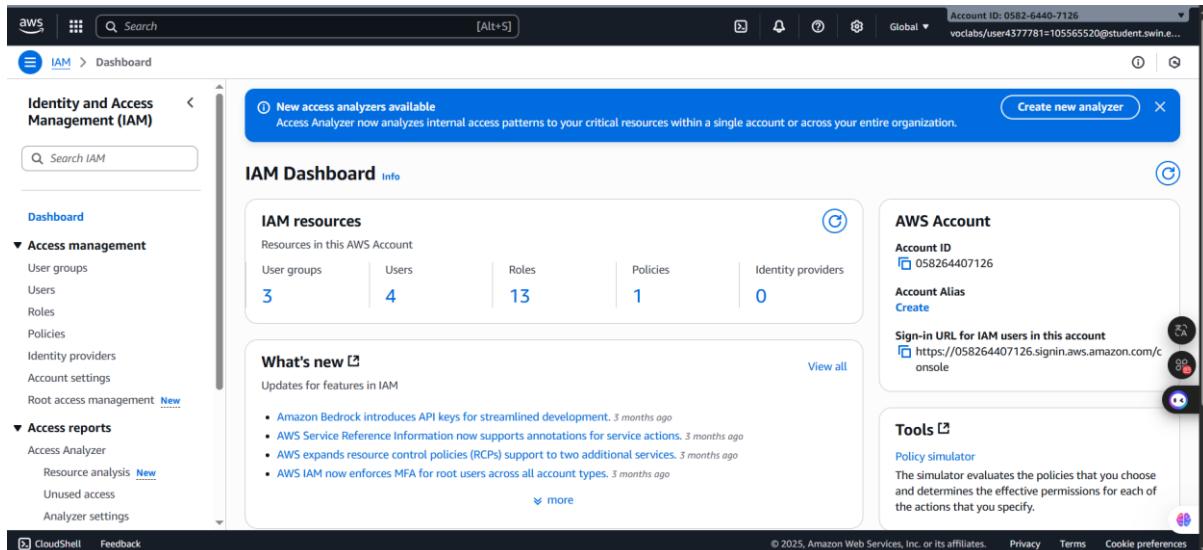
User groups (3) Info																					
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.																					
<table border="1"> <thead> <tr> <th>Group name</th><th>Users</th><th>Permissions</th><th>Creation time</th></tr> </thead> <tbody> <tr> <td>EC2-Admin</td><td>1</td><td>Defined</td><td>21 minutes ago</td></tr> <tr> <td>EC2-Support</td><td>1</td><td>Defined</td><td>21 minutes ago</td></tr> <tr> <td>S3-Support</td><td>1</td><td>Defined</td><td>21 minutes ago</td></tr> </tbody> </table>						Group name	Users	Permissions	Creation time	EC2-Admin	1	Defined	21 minutes ago	EC2-Support	1	Defined	21 minutes ago	S3-Support	1	Defined	21 minutes ago
Group name	Users	Permissions	Creation time																		
EC2-Admin	1	Defined	21 minutes ago																		
EC2-Support	1	Defined	21 minutes ago																		
S3-Support	1	Defined	21 minutes ago																		
Group name	Users	Permissions	Creation time																		
EC2-Admin	1	Defined	21 minutes ago																		
EC2-Support	1	Defined	21 minutes ago																		
S3-Support	1	Defined	21 minutes ago																		

**Figure 17: User Groups Confirmation**

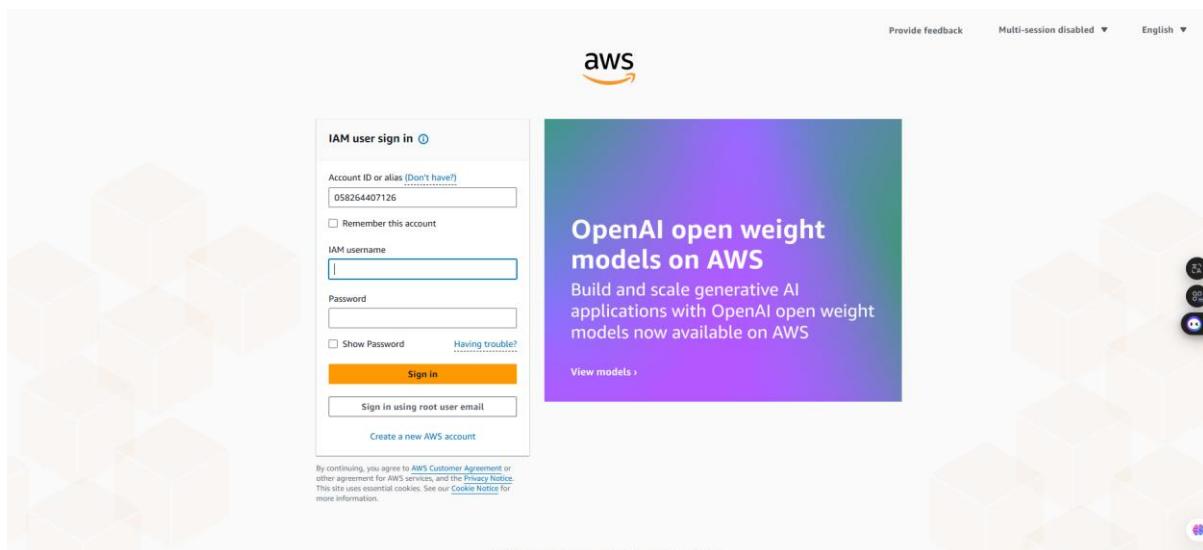
## E. Task 3: Sign-In and Test Users

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

**Step 3.1:** In the left navigation bar, choose the **Dashboard**

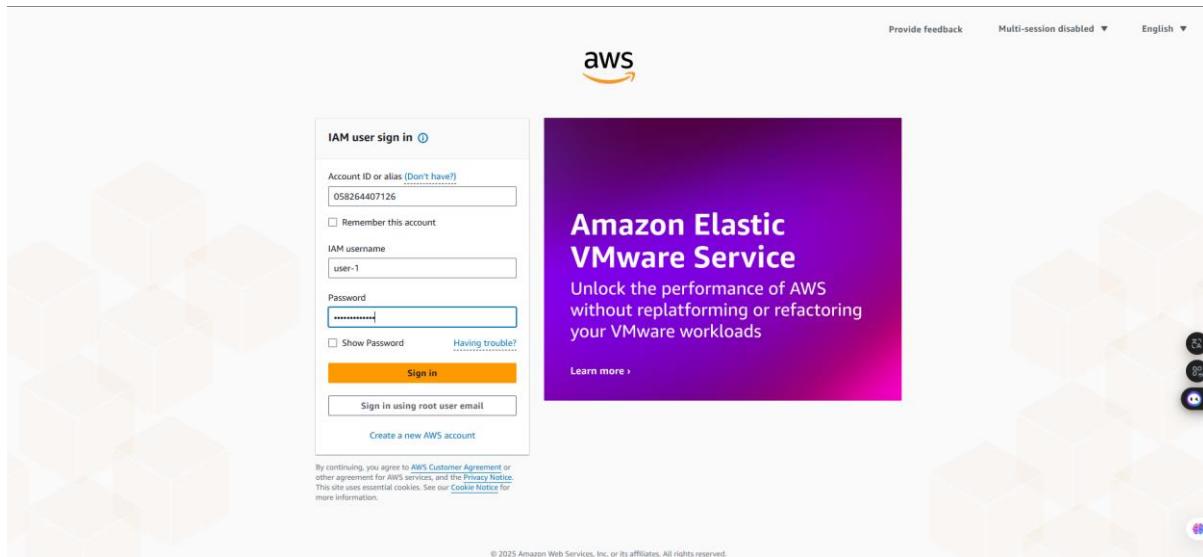
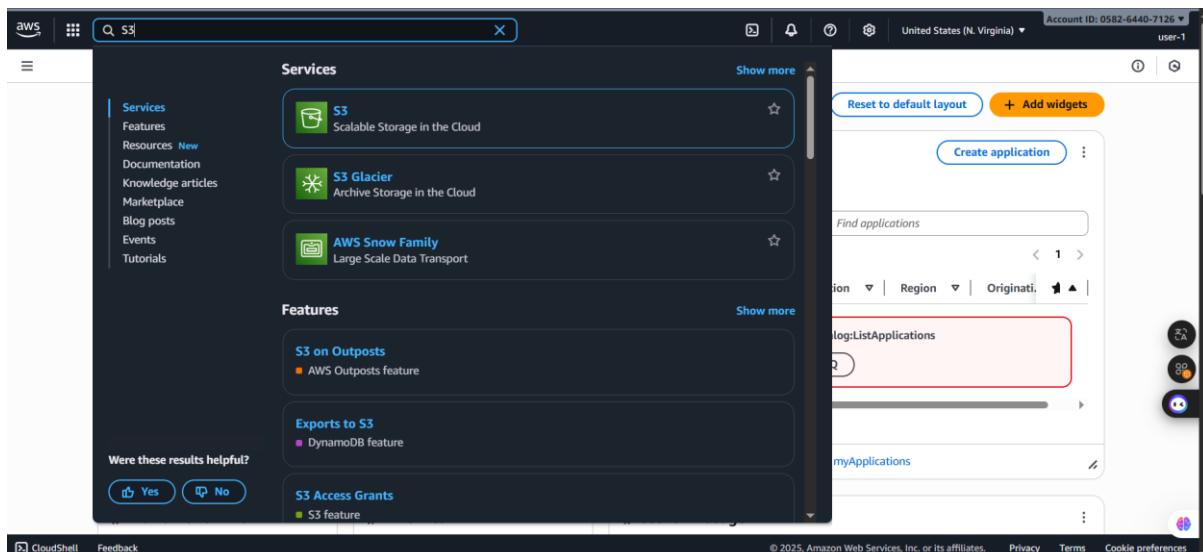
**Figure 18: IAM Dashboard**

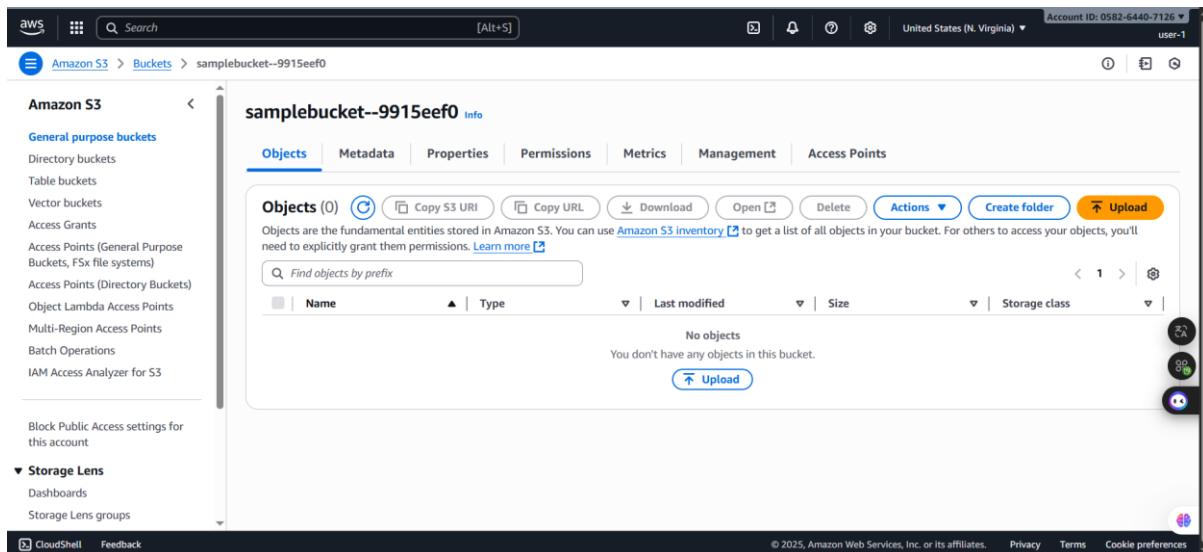
**Step 3.2:** In the AWS Accoun box on the right side, copy the **Sign-in URL for IAM users in this account** and paste it into a new browser tab

**Figure 19: Sign-in AWS Interface**

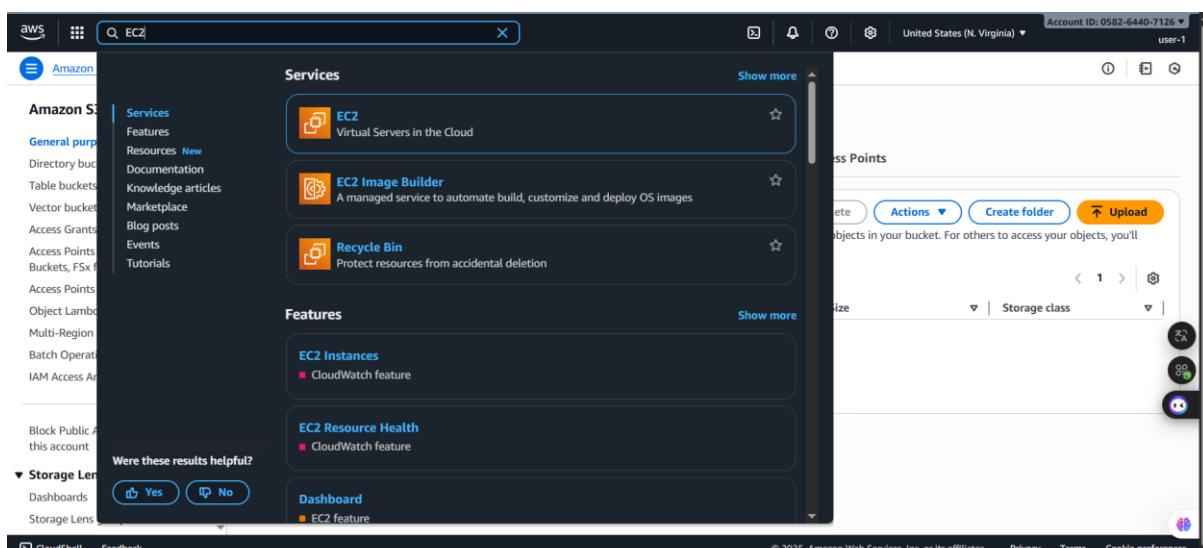
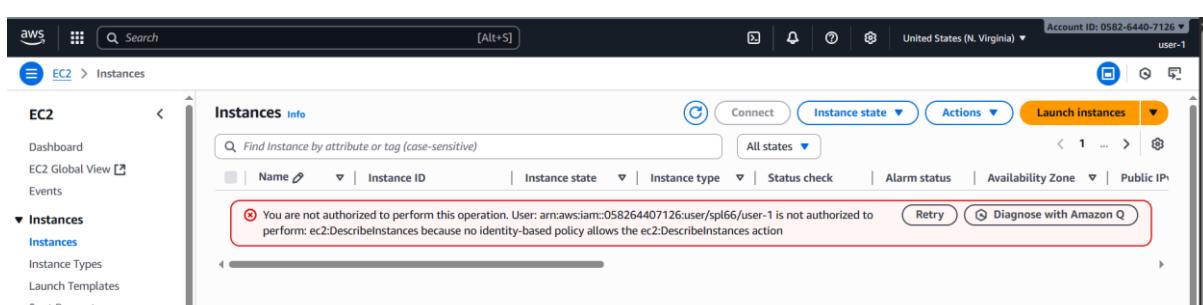
**Step 3.3:** Sign in the AWS Interface with following requirements:

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

**Figure 20: Sign-in AWS with user-1 account****Step 3.4:** Then, search and choose Amazon S3**Figure 21: Searching Amazon S3****Step 3.4:** Next, choose the sample bucket in the Amazon S3

*Figure 22: Choosing the sample bucket*

### Step 3.5: In the next step, search the EC2 and choose Instances

*Figure 23: Searching the EC2**Figure 24: EC2 homepage*

**Step 3.6:** Sign out the **user-1** in the AWS Management Console by clicking on the account name which is located in the top right corner of the screen.

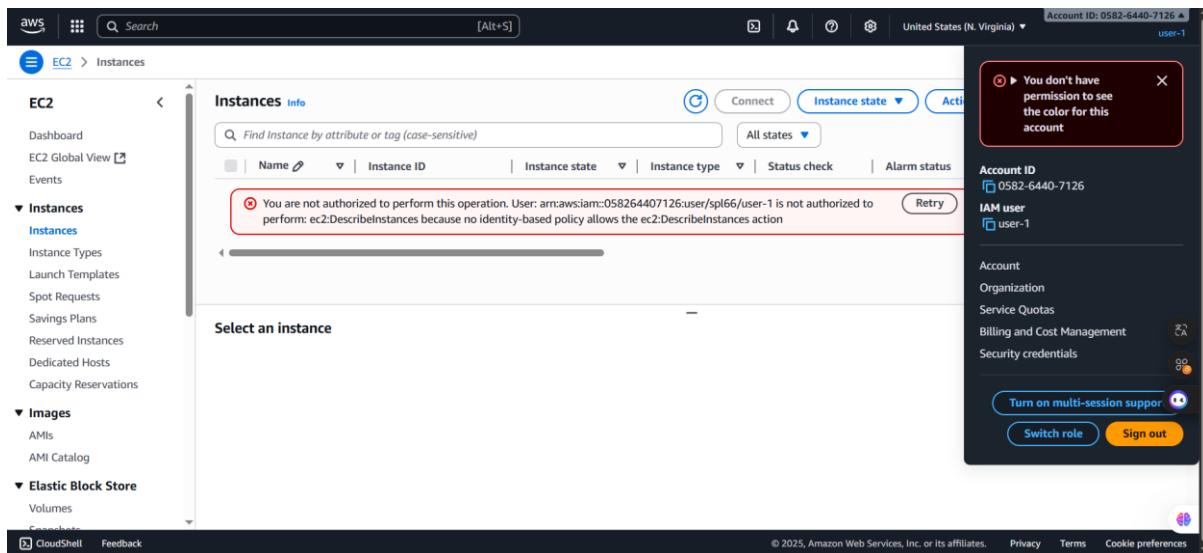


Figure 24: Sign out

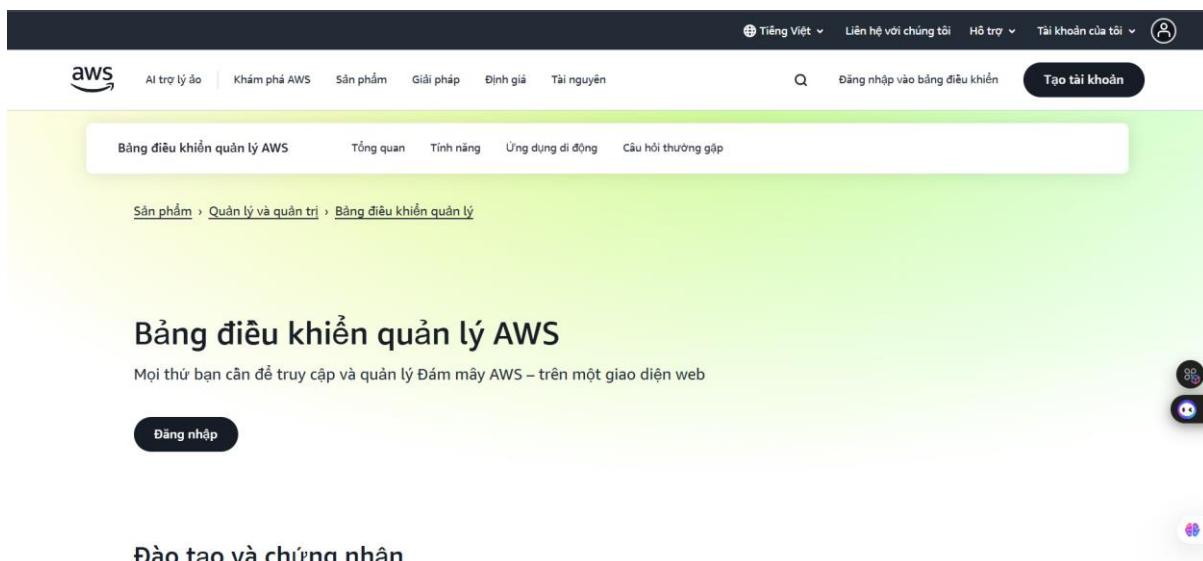
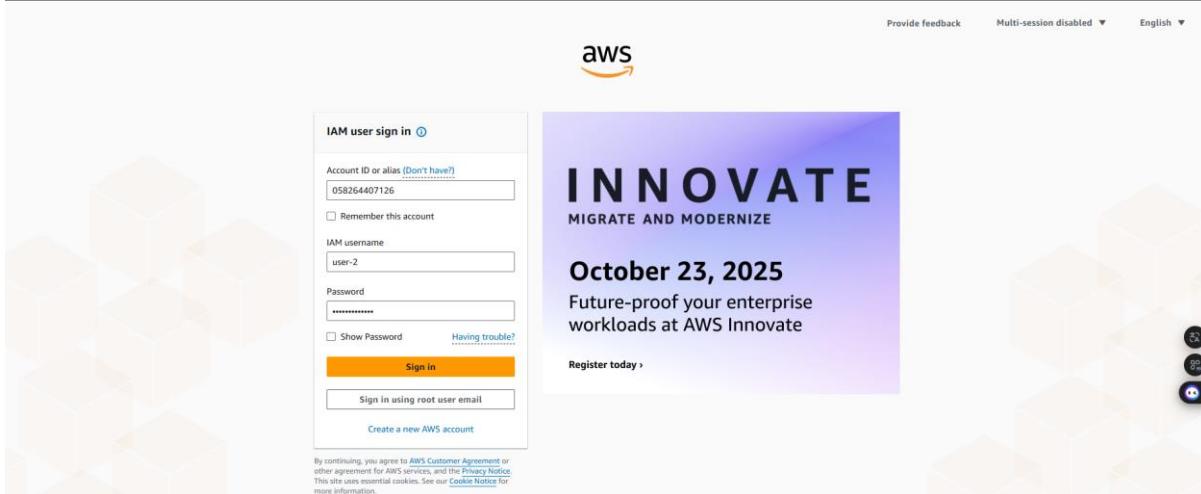


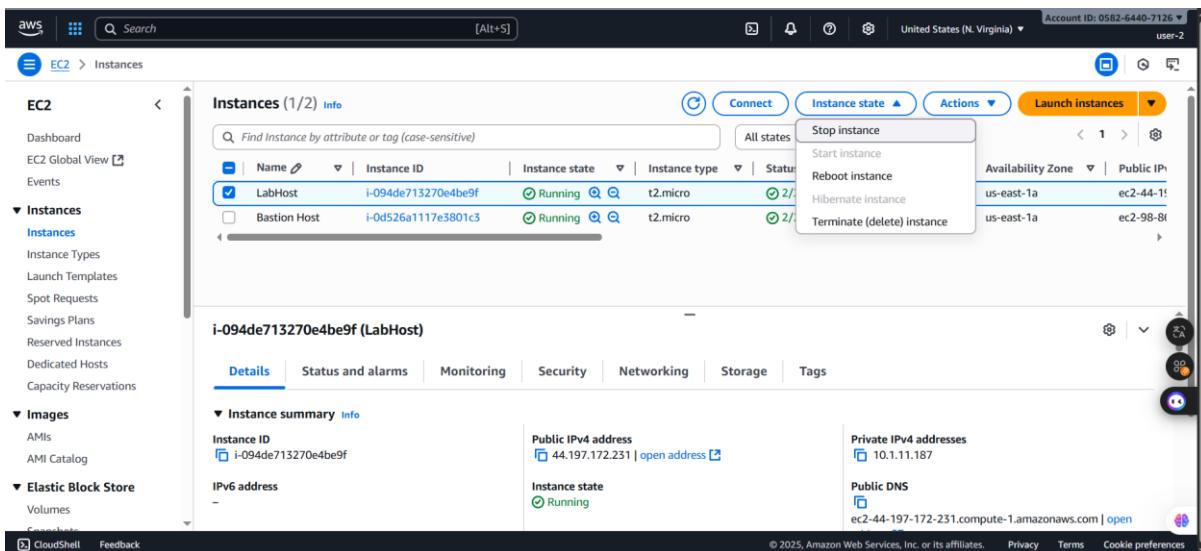
Figure 25: Sign out successfully interface

**Step 3.7:** Sign in the AWS Interface again with:

- **IAM user name:** user-2
- **Password:** Lab-Password2

*Figure 26: Sign-in AWS with user-2 account*

**Step 3.8:** After signing in successfully into the AWS with user-2 account, select the Instances in the left side panel and select the **LabHost**. In the **Instance state** menu above, select **Stop instance**.

*Figure 27: Select the instance to stop*

**Step 3.9:** In the **Stop Instance** window, select **Stop**.

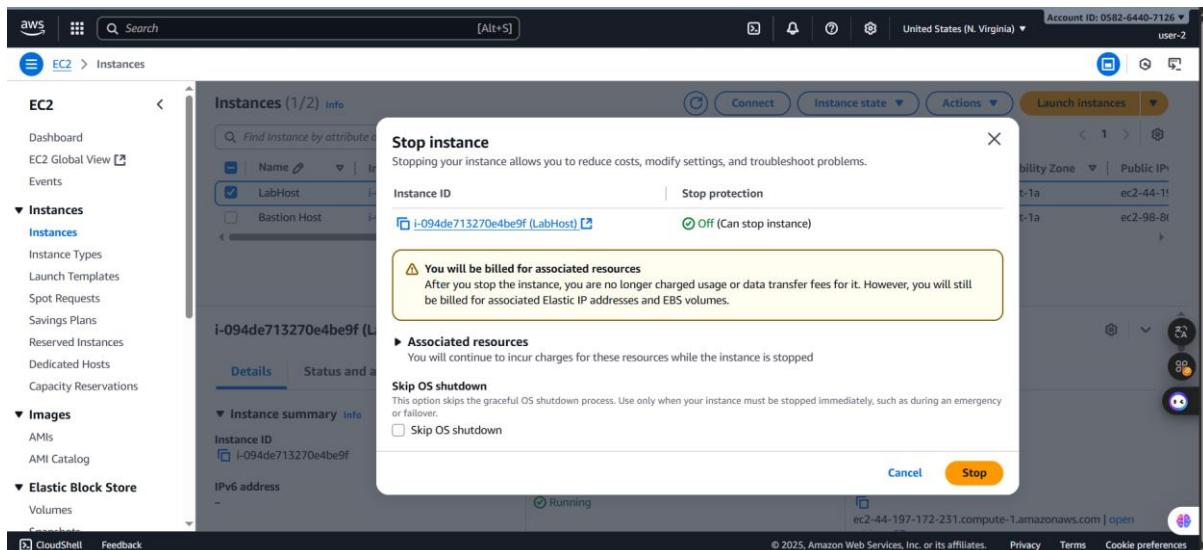


Figure 28: Stop announcement

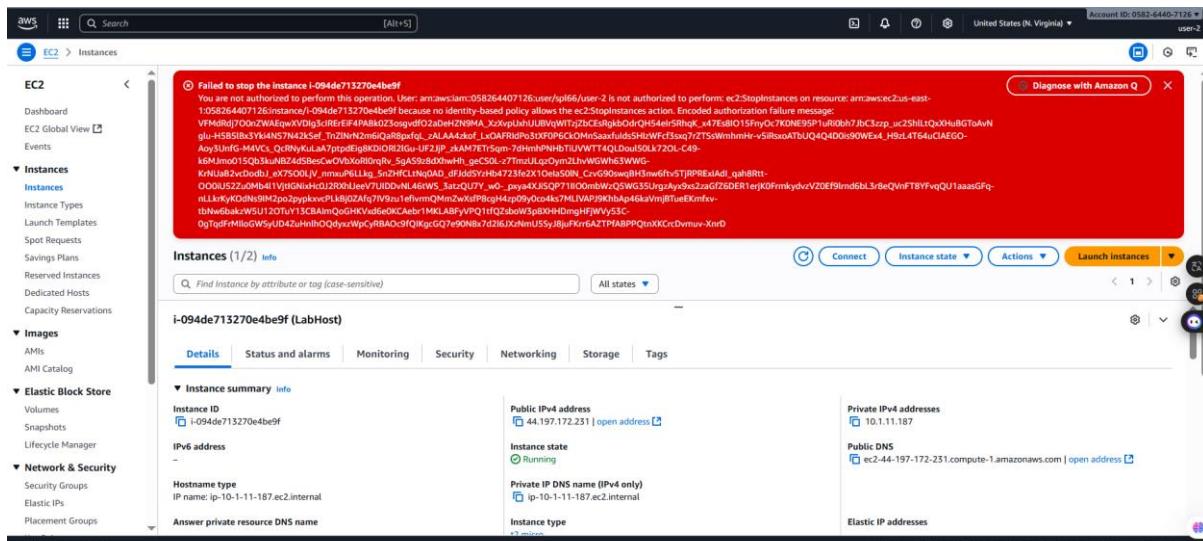
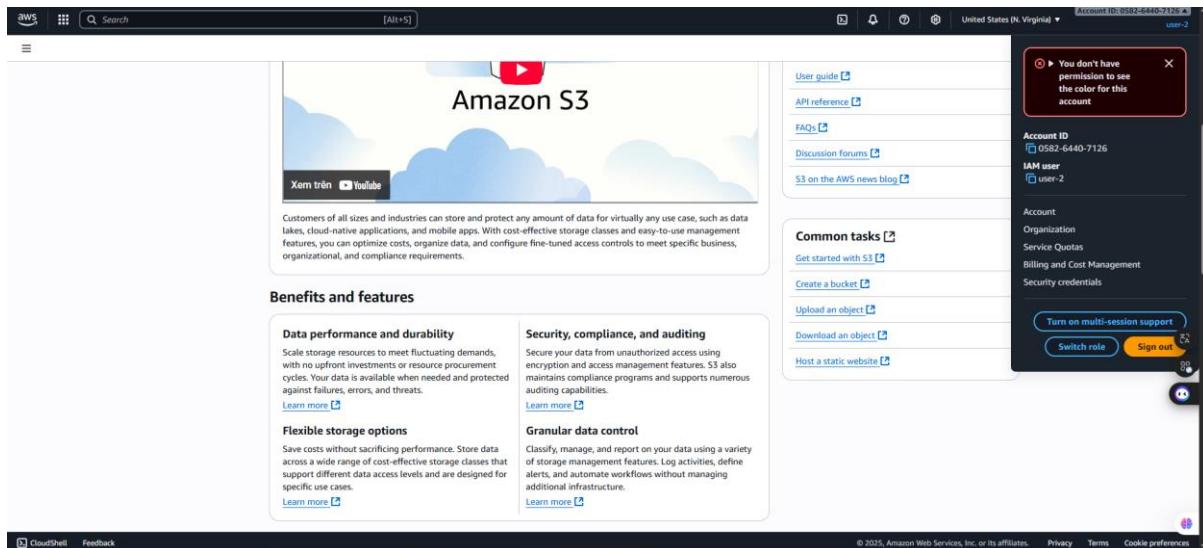
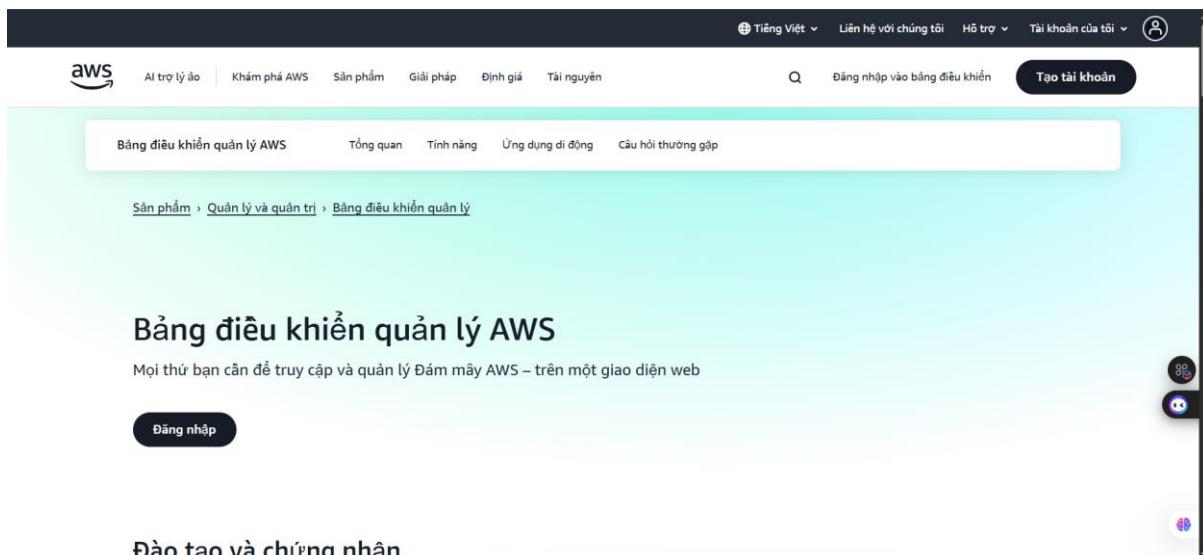


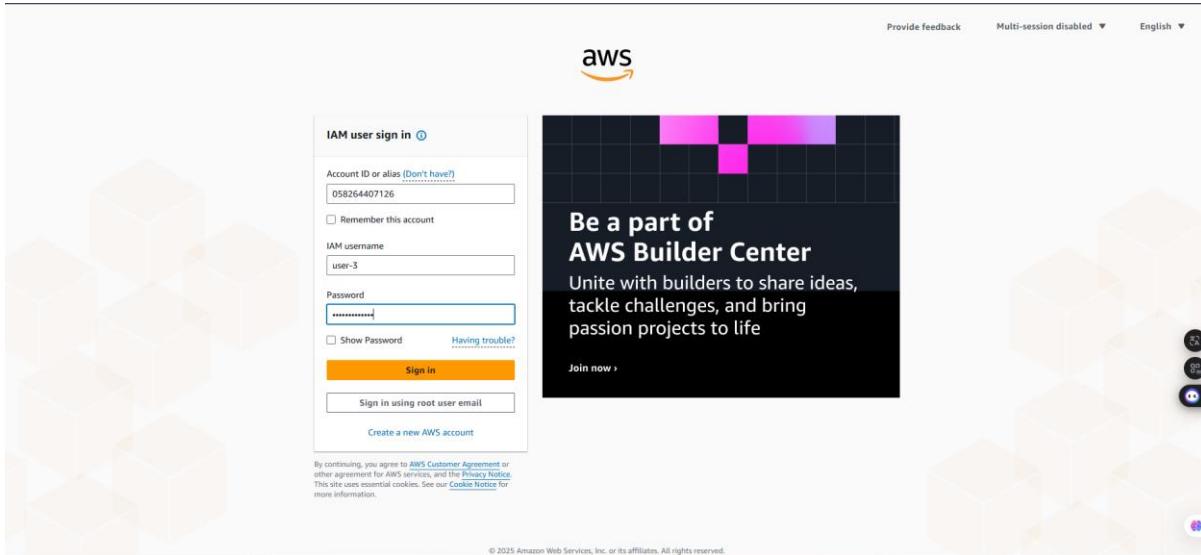
Figure 29: Failed to stop

**Step 3.10:** In the searching bar, search **Amazon S3** to see the announce “**You don't have permissions to list buckets**”. After that, similarly to **user-1**, sign out and move to **user-3**

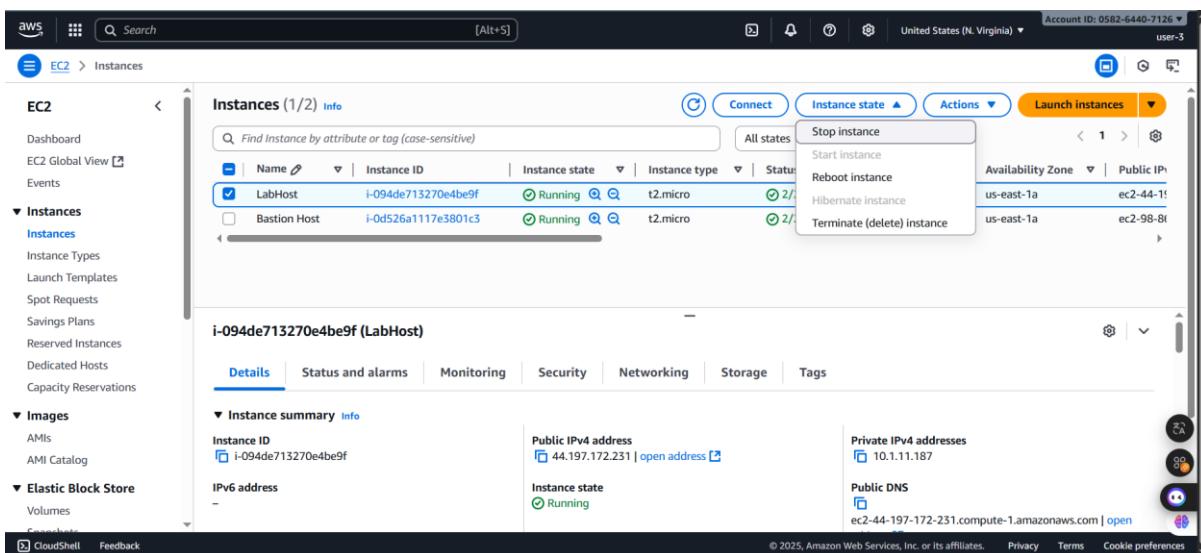
*Figure 30: Sign out preparation**Figure 31: Sign out successfully*

**Step 3.11:** Paste the **IAM users sign-in link** into a new browser tab and press **Enter**. Then, sign in with:

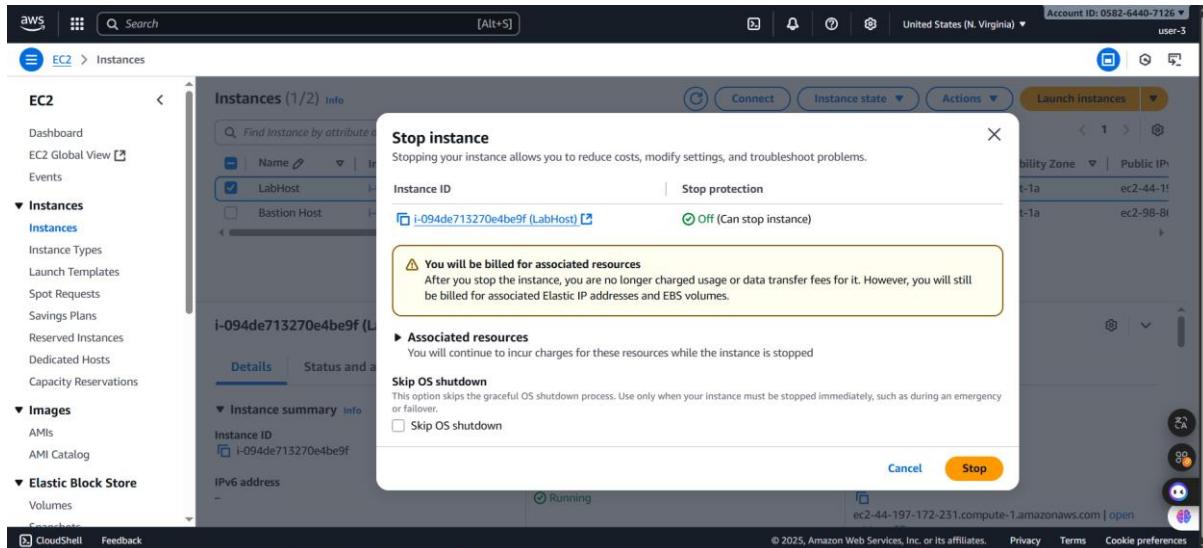
- **IAM user name:** user-3
- **Password:** Lab-Password3

**Figure 32: Sign in with user-3 account**

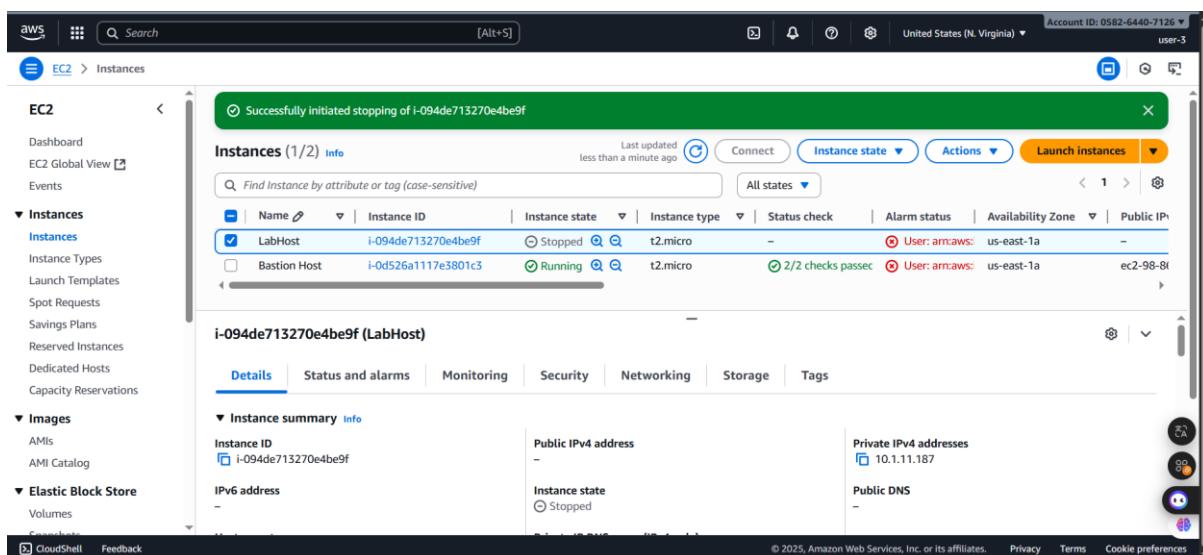
**Step 3.12:** When logging successfully, search in the search box EC2 and select the instance **LabHost**, then in the **Instance state** menu, choose **Stop instance**.

**Figure 33: Stop instance selection**

- As I expected, the instance displays the warning before stopping the instance

**Figure 34: Stop instance announcement**

- After clicking the **Stop** button and waiting for moment, the instance finally **stopped**



## F. Completed Task

Total score	40/40
TASK 2a - Added user-1 to S3-Support group	5/5
TASK 2b - Added user-2 to EC2-Support group	5/5
TASK 2c - Added user-3 to EC2-Admin group	5/5
TASK 3a - user-1 logged in	5/5
TASK 3b - user-2 logged in	5/5
TASK 3c - user-2 ec2 stop instance attempt	5/5
TASK 3d - user-3 logged in	5/5
TASK 3e - user-3 EC2 stop instance attempt	5/5

## G. Conclusion

- In this lab, I learned how to use AWS Identity and Access Management (IAM) to manage users, groups, and permissions. I explored the existing IAM users and groups, examined the policies attached to them, and practiced adding users to the appropriate groups based on their roles. I also tested the permissions by signing in as different users and observing how their access was restricted or allowed depending on their assigned policies.
- Through this experience, I understood the importance of IAM in controlling access to AWS resources and ensuring security by applying the principle of least privilege. I realized how user and group configurations directly impact what actions can be performed in the

AWS environment. Overall, this lab helped me build confidence in managing identities and permissions securely in AWS.