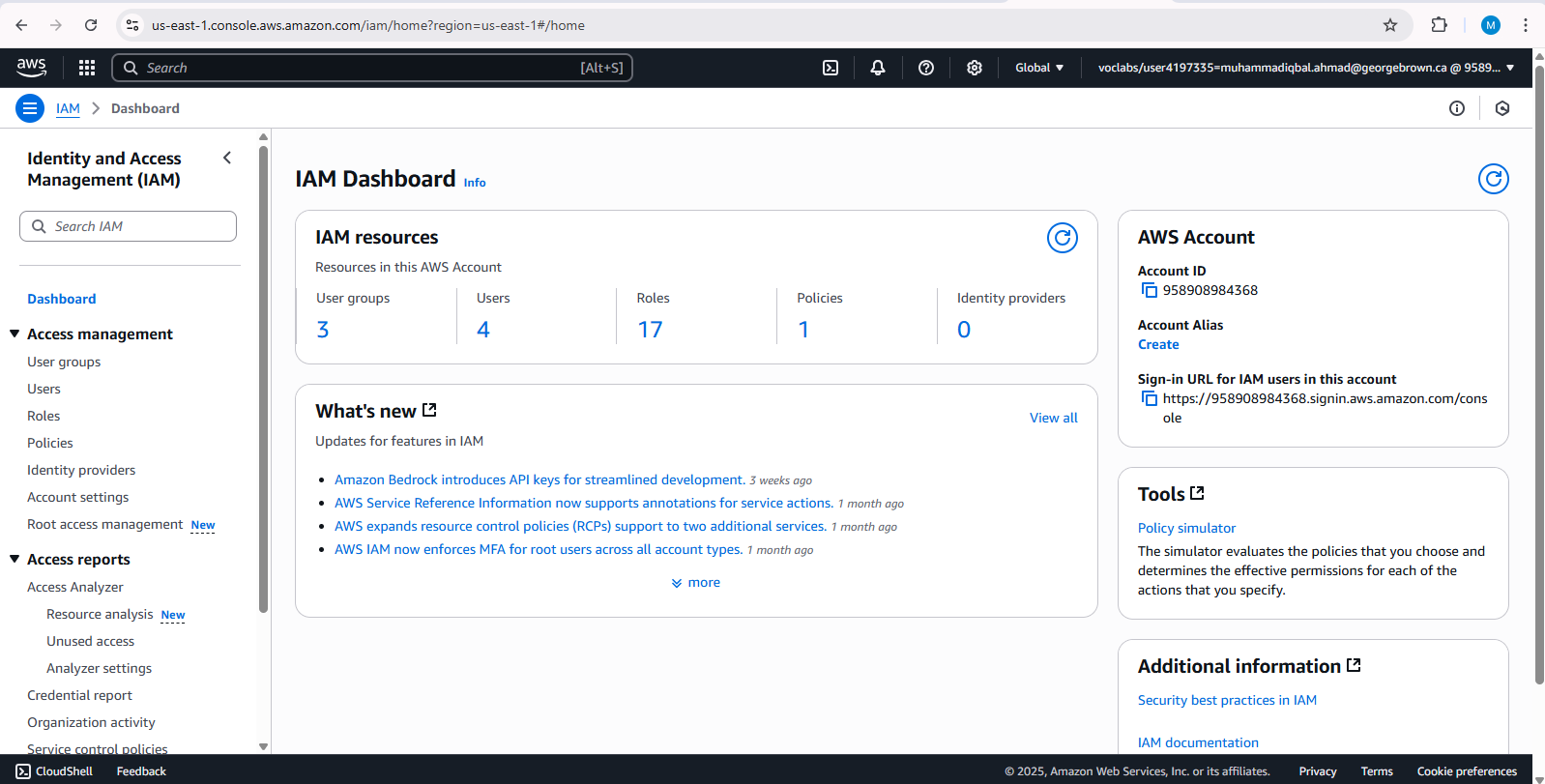
**AWS Identity and Access Management**

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

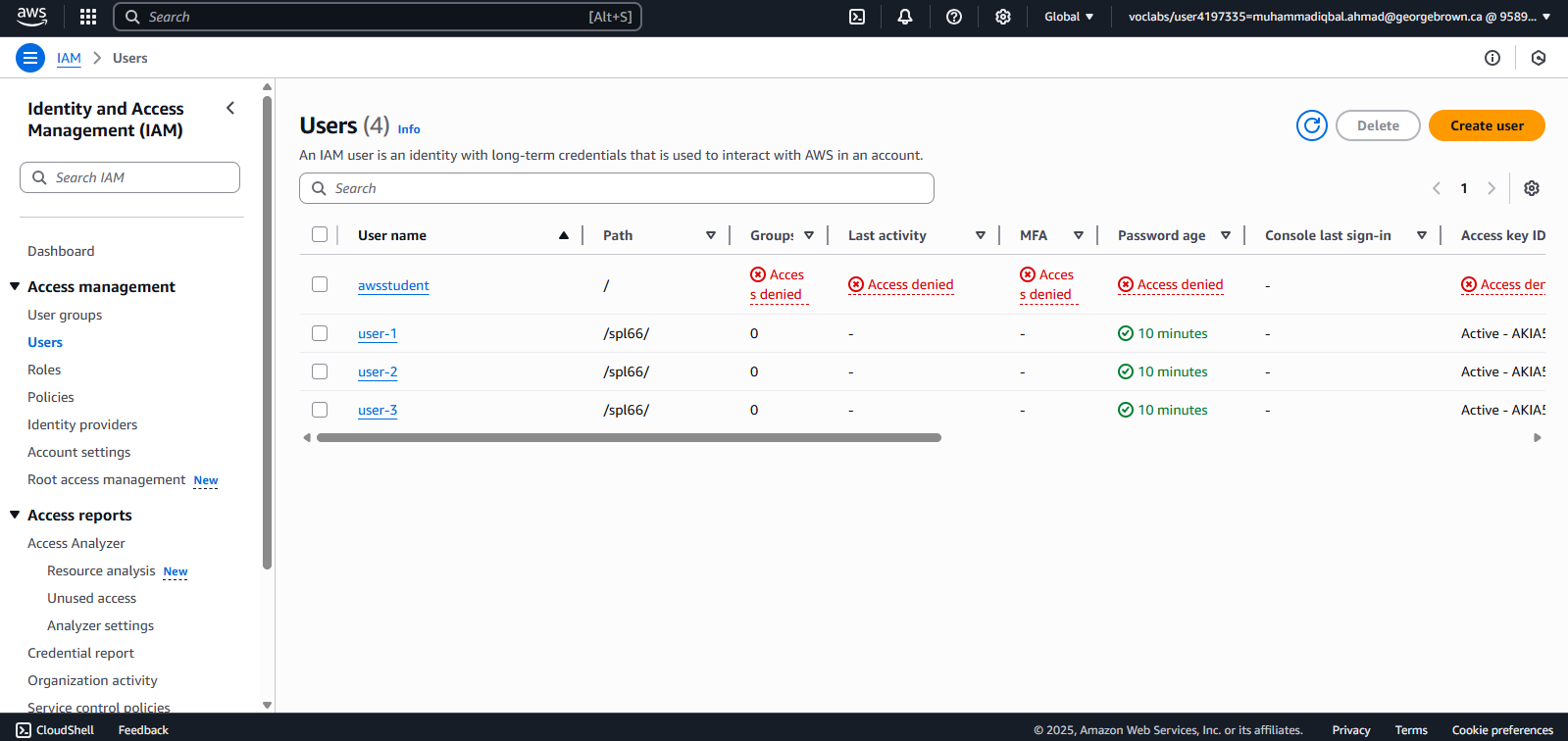
* **Manage IAM Users and their access:** You can create Users and assign them individual security credentials (access keys, passwords, and multi-factor authentication devices). You can manage permissions to control which operations a User can perform.
* **Manage IAM Roles and their permissions:** An 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.

**Explore the Users and Groups**

1. In the search box to the right of **Services**, search for and choose **IAM** to open the IAM console.

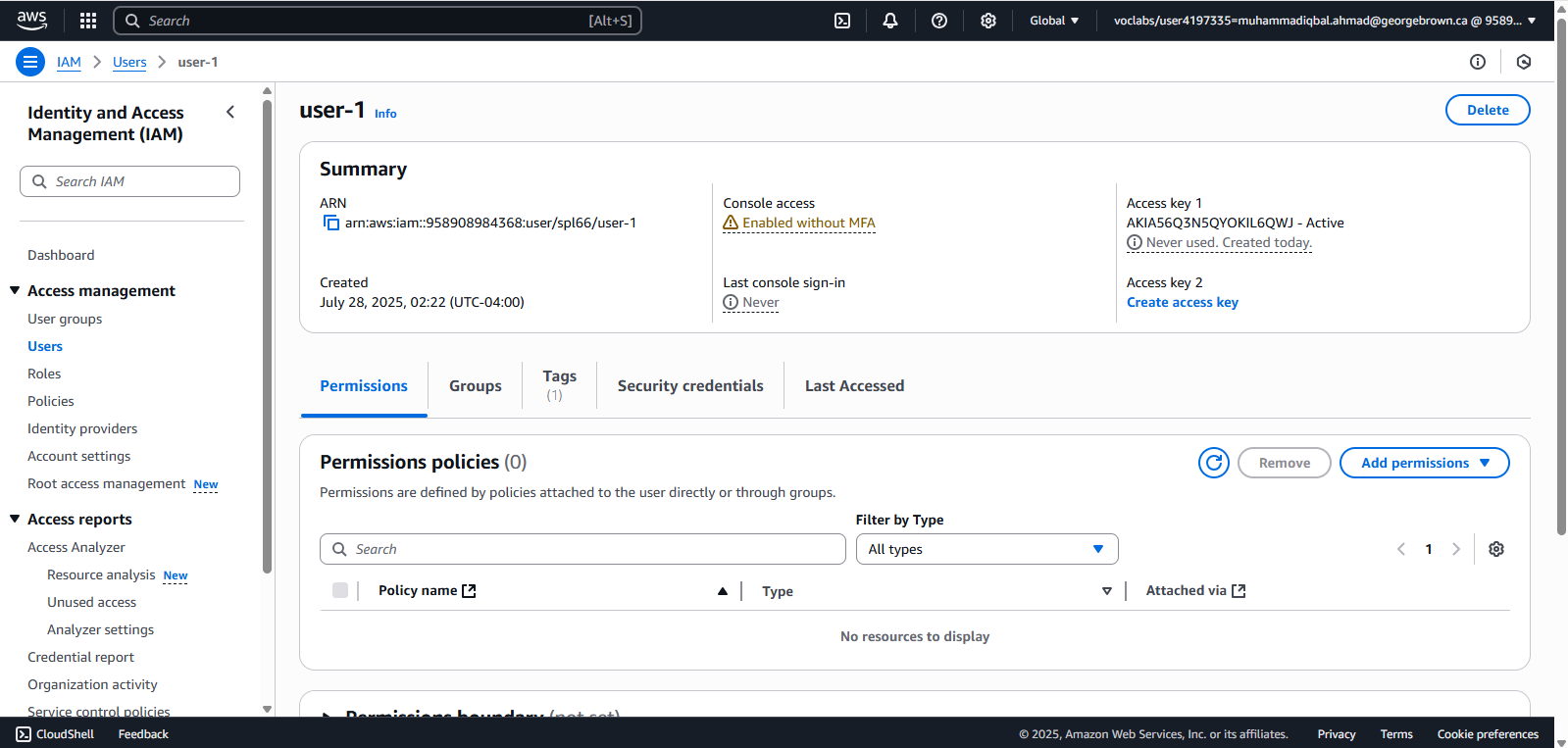


1. In the navigation pane on the left, choose **Users**.



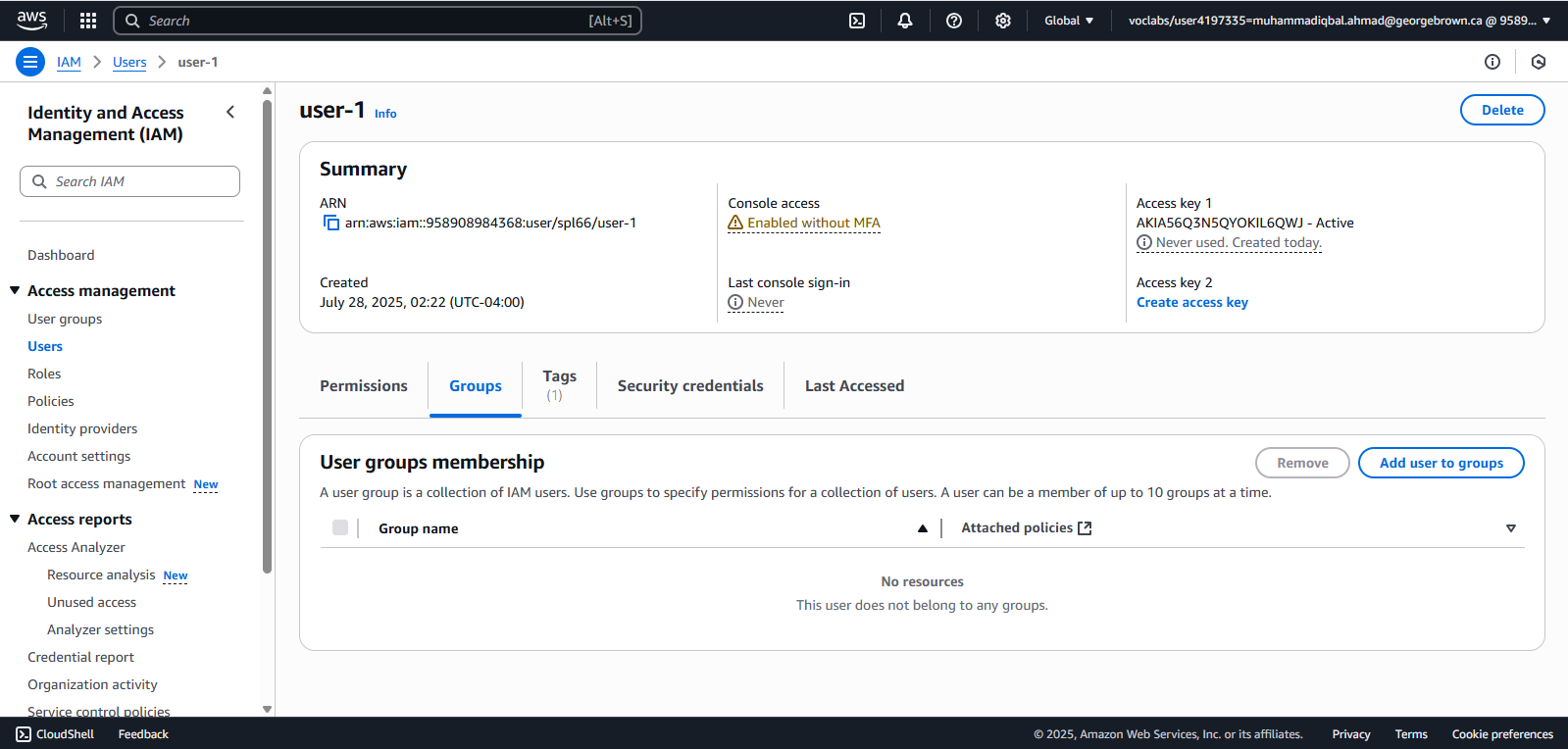
1. Choose the **user-1** link.

This will bring to a summary page for user-1. The **Permissions** tab will be displayed. Notice that user-1 does not have any permissions.



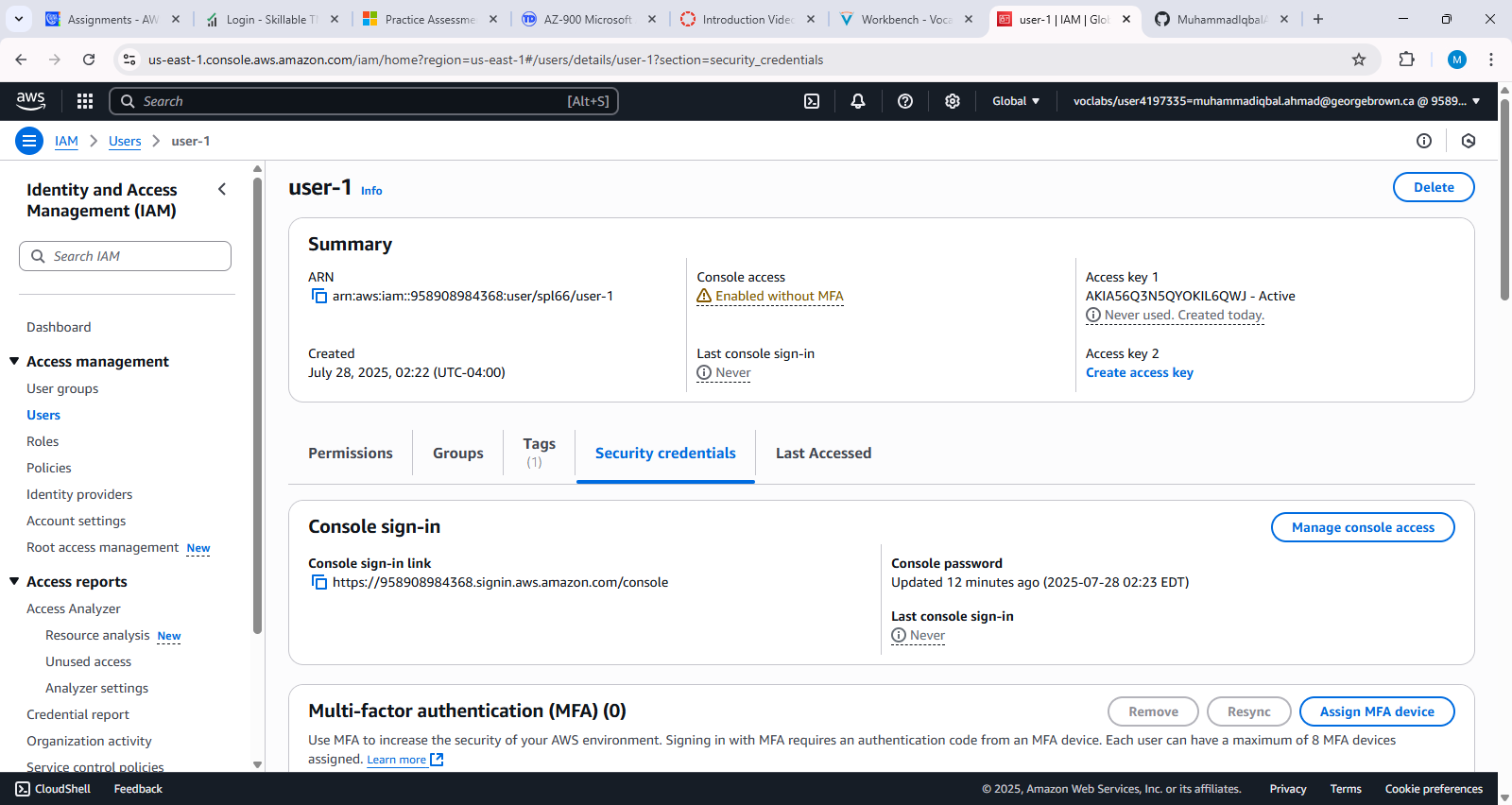
1. Choose the **Groups** tab.

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

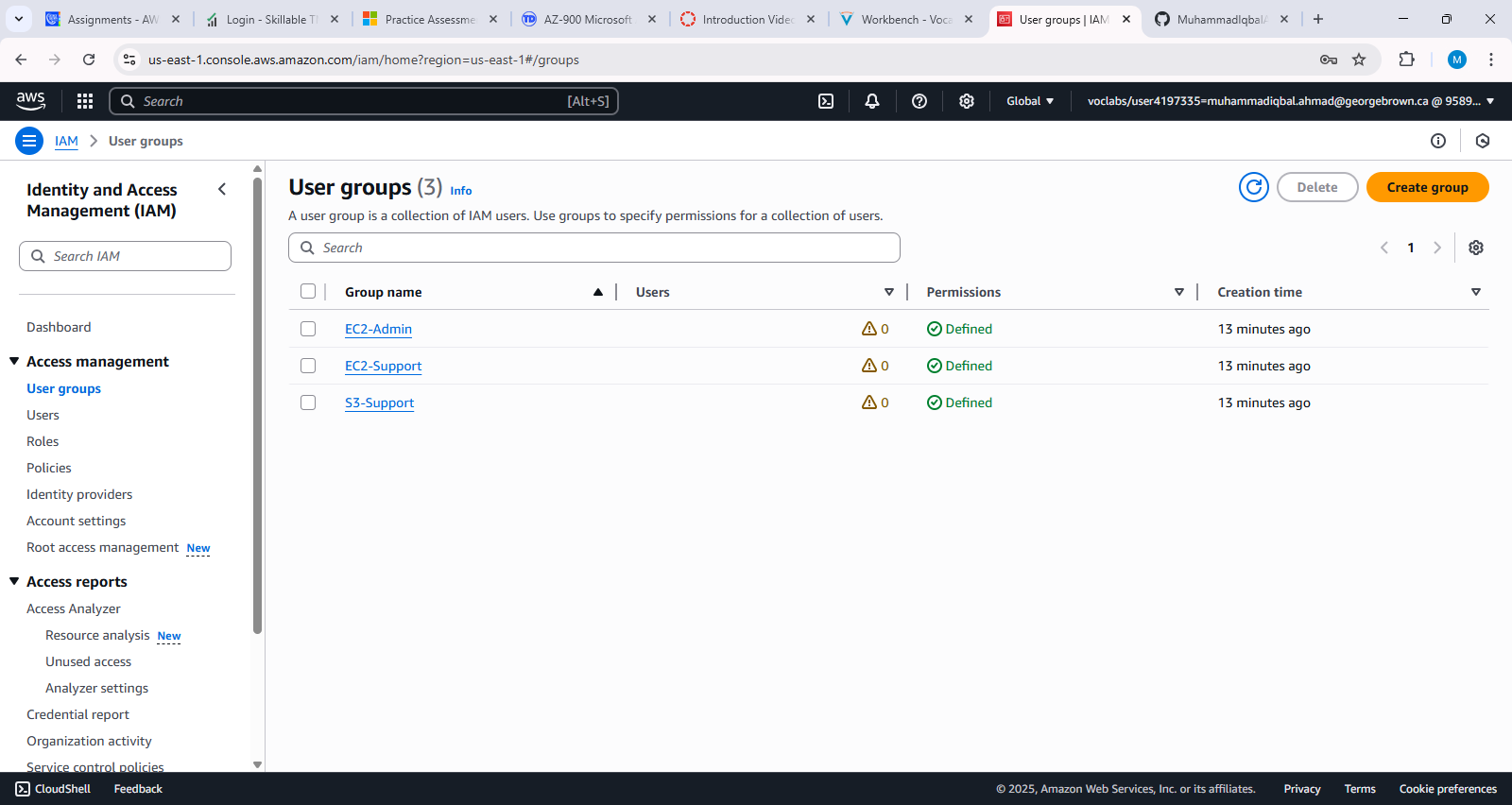


1. Choose the **Security credentials** tab.

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



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



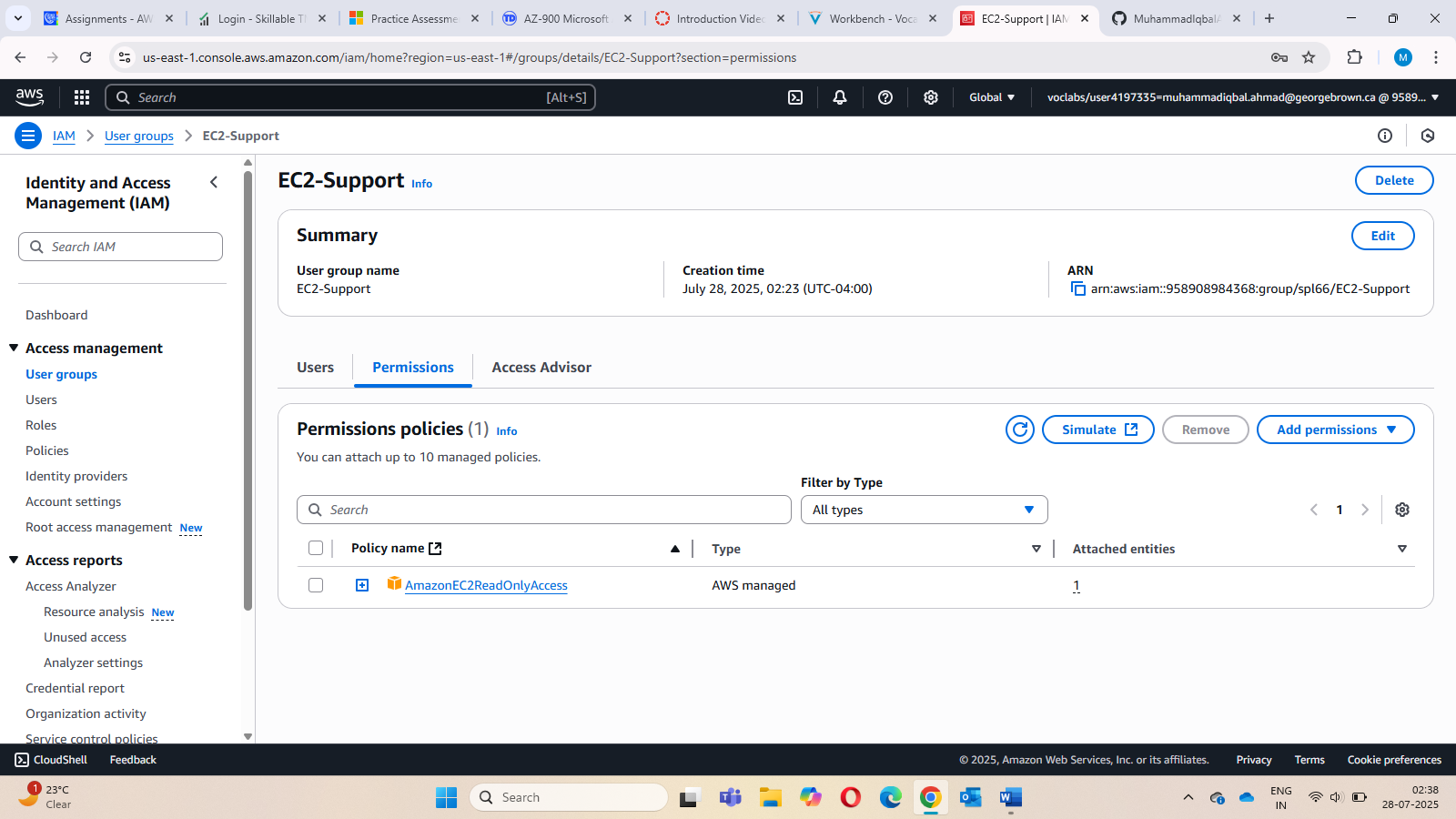
1. Choose the **EC2-Support** group link.

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.



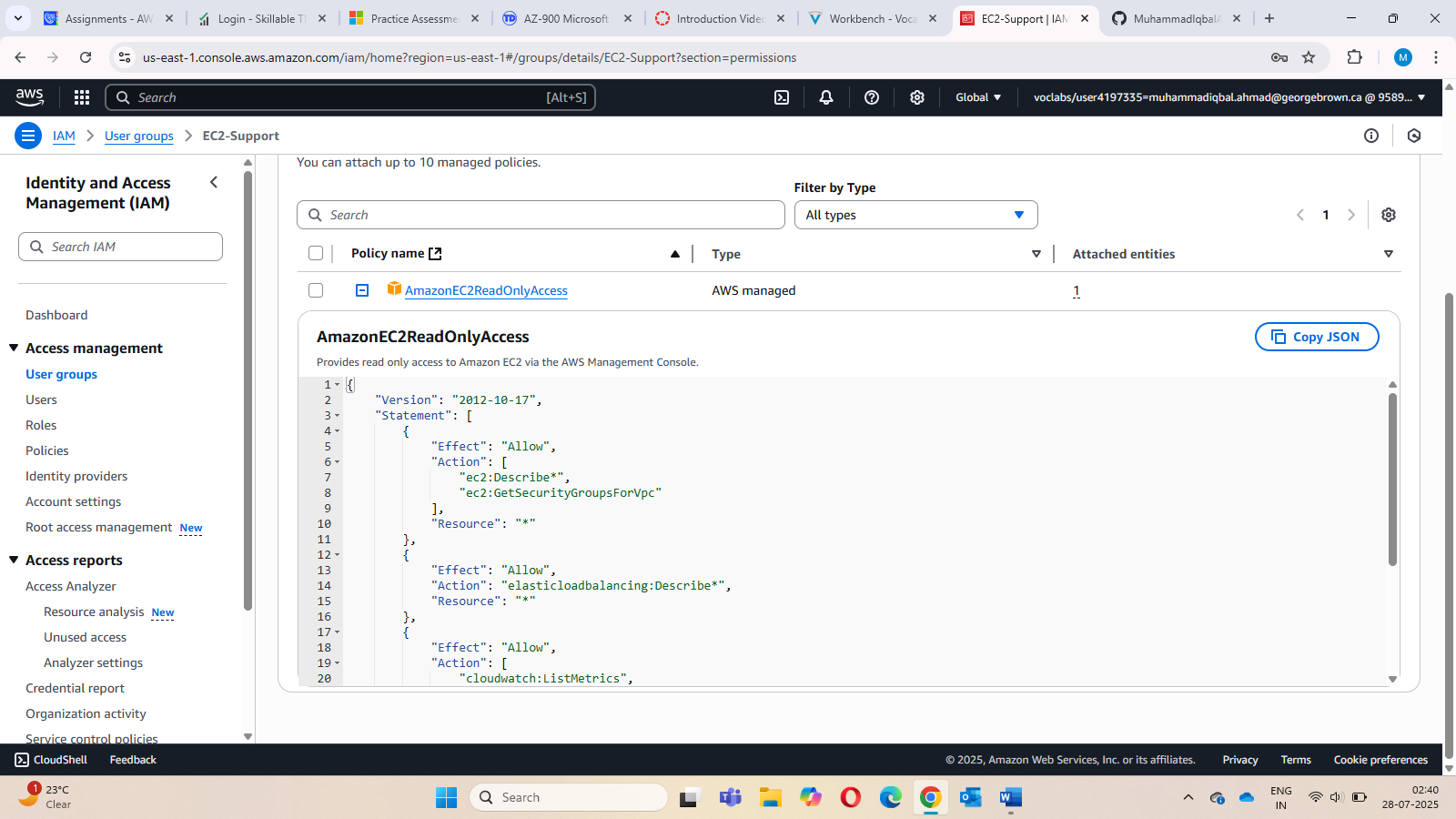
1. Choose the plus (**+**) icon next to the AmazonEC2ReadOnlyAccess policy to view the policy details.

**Note**: 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.

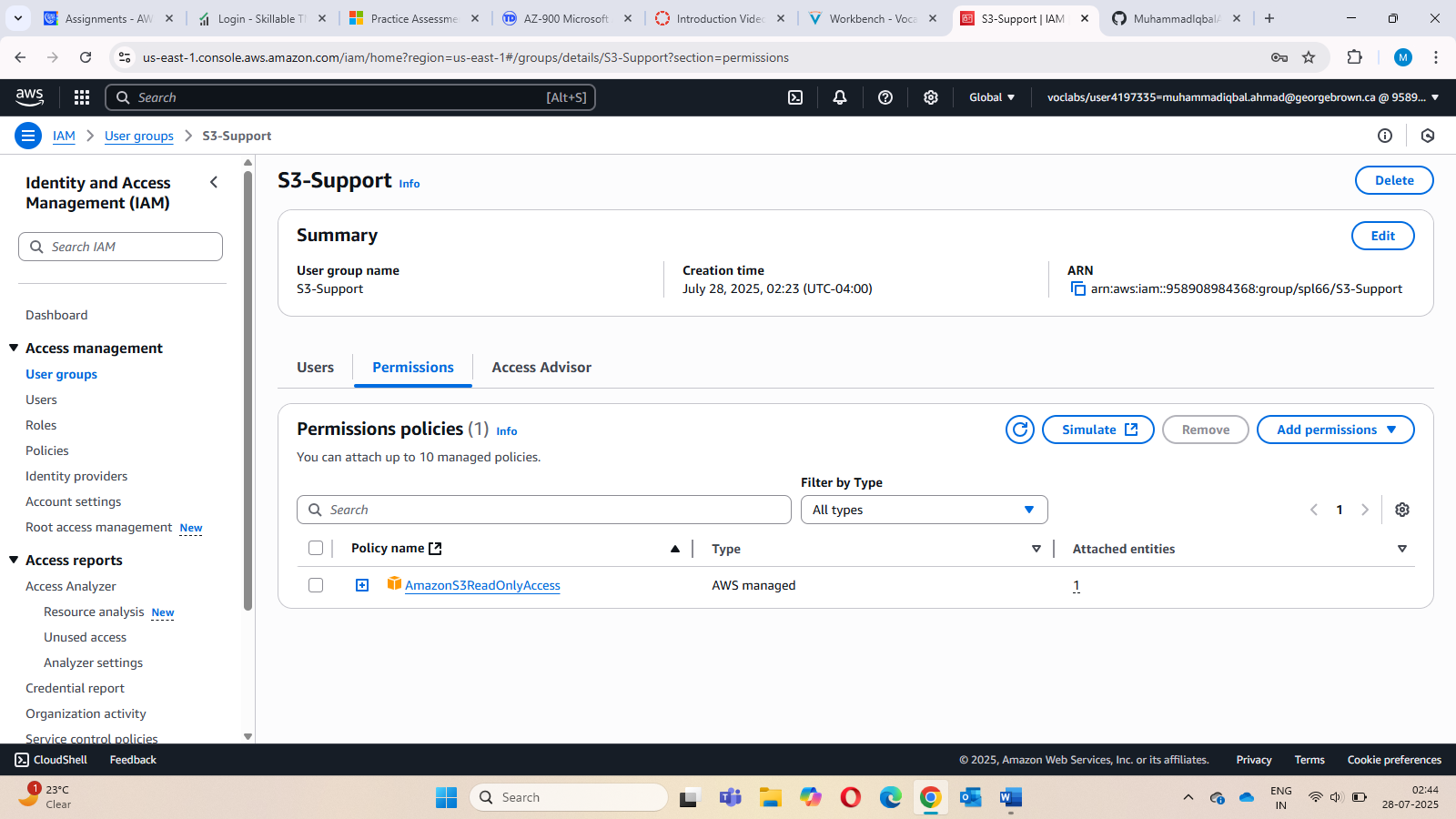
The basic structure of the statements in an IAM Policy is:

* + **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*).



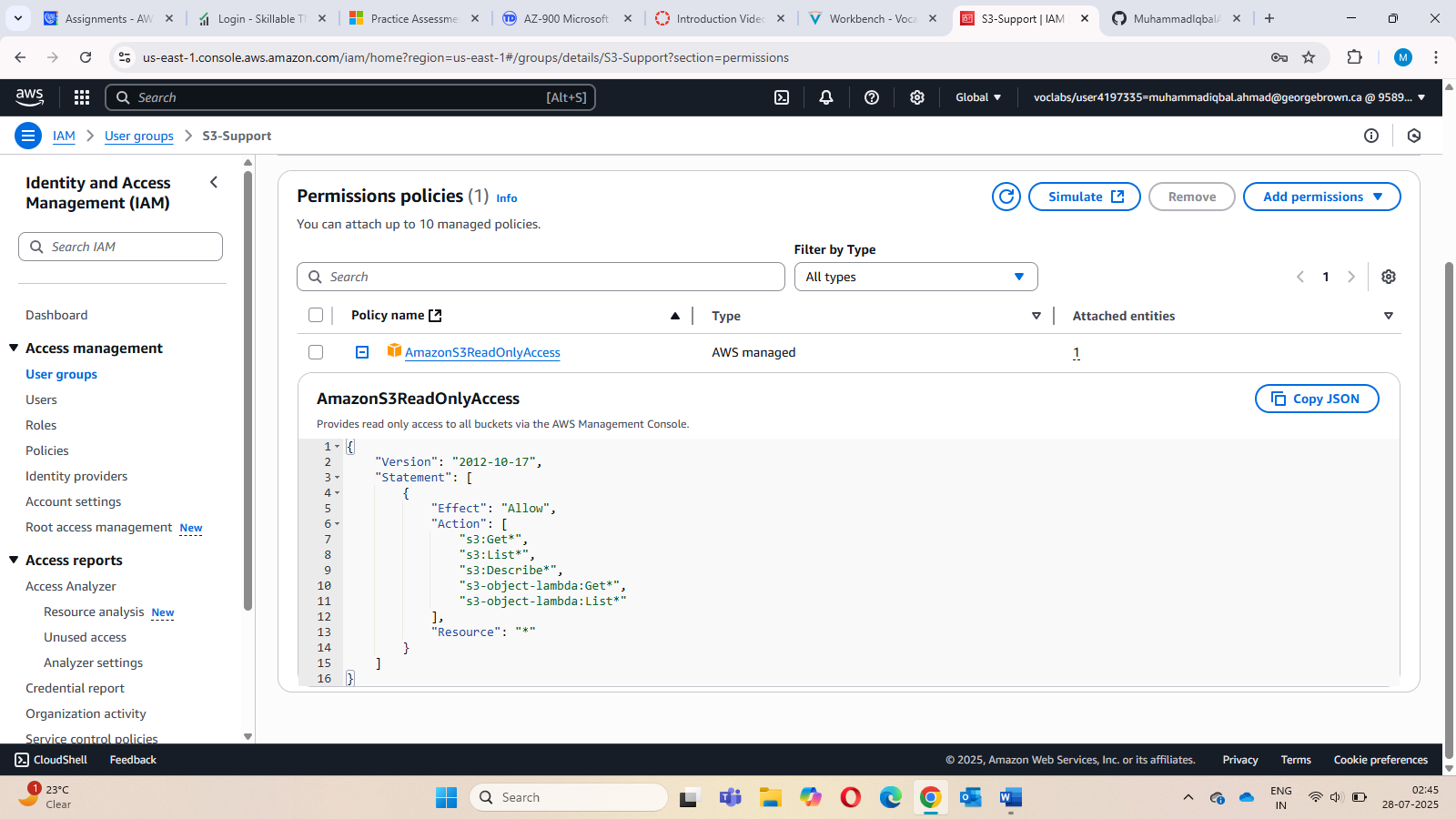
1. In the navigation pane on the left, choose **User groups**. Choose the **S3-Support** group link and then choose the **Permissions** tab.

The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.



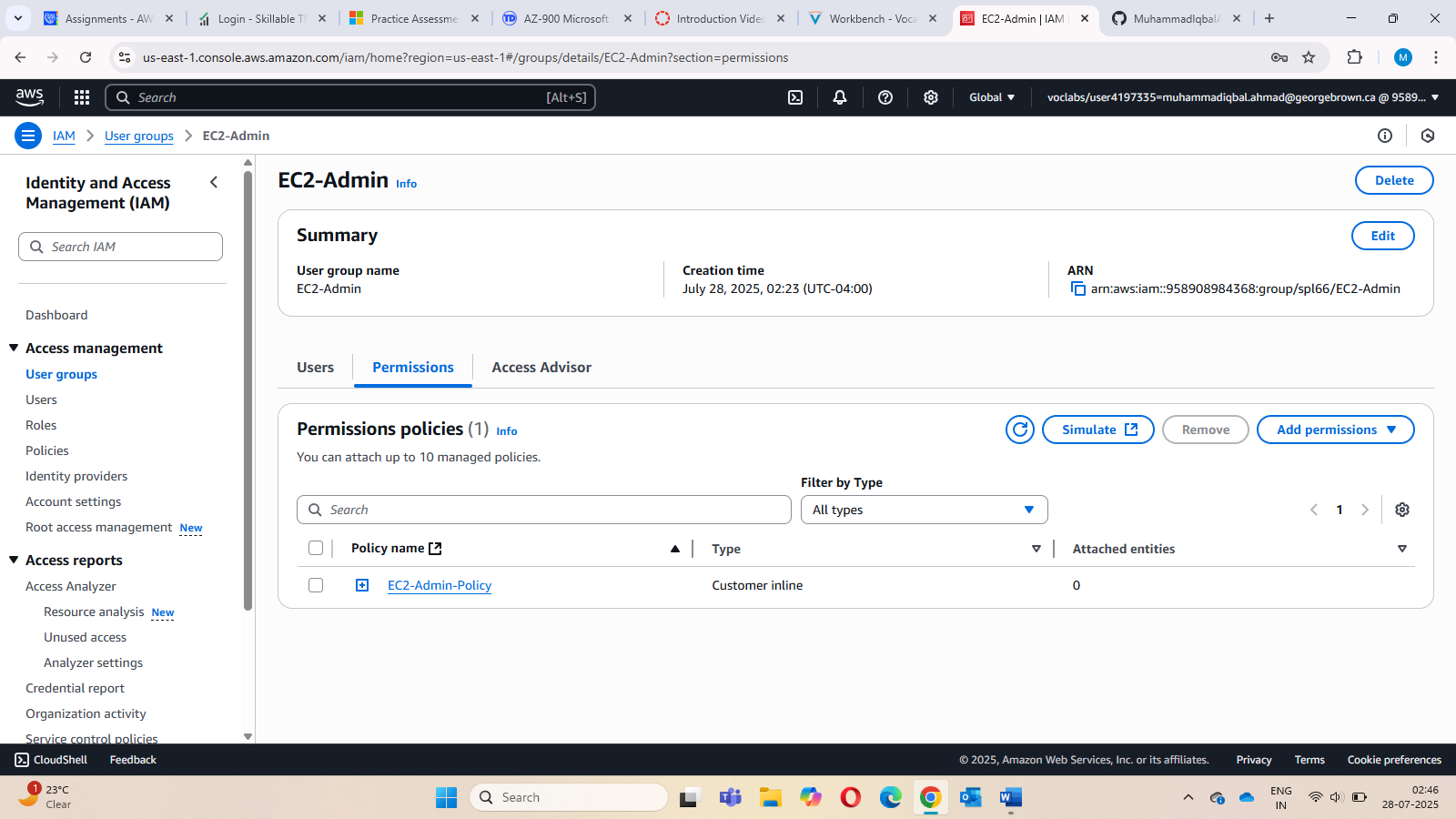
1. Choose the plus (**+**) icon to view the policy details.

This policy grants permissions to Get and List resources in Amazon S3.



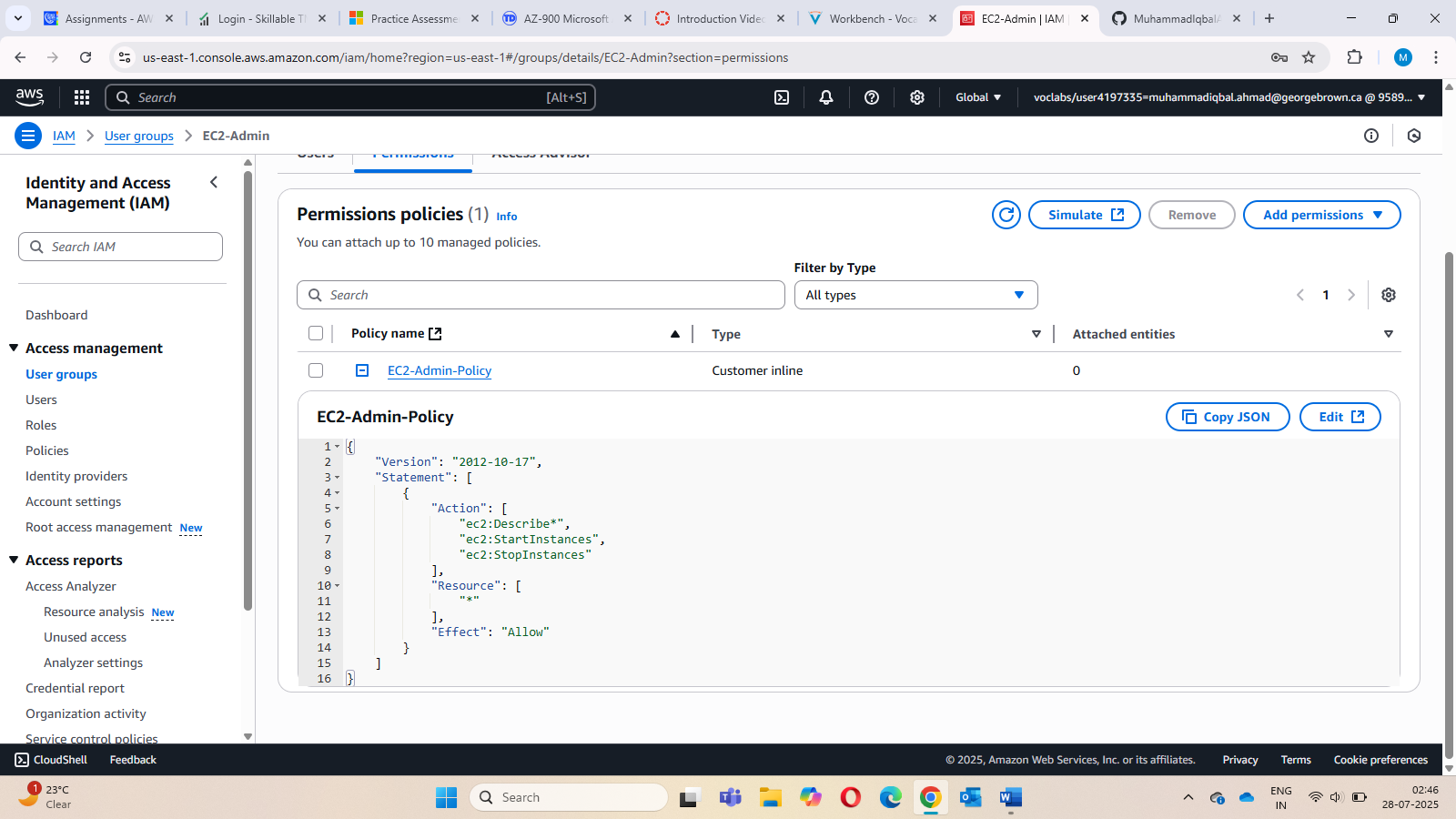
16. Choose the minus icon (**-**) to hide the policy details. In the navigation pane on the left, choose **User groups**. Choose the **EC2-Admin** group link and then choose the **Permissions** tab.

This Group is slightly different from the other two. Instead of a *Managed Policy*, it has an **Inline Policy**, which is a policy assigned to just one User or Group. Inline Policies are typically used to apply permissions for one-off situations.



* 1. Choose the plus (**+**) icon to view the policy details.

This policy grants permission to view (Describe) information about Amazon EC2 and also the ability to Start and Stop instances.



**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 have hired user-2 into a role where they will provide support for Amazon EC2. You have hired user-3 as your Amazon EC2 administrator, who manage your EC2 instances. You will add them to the S3-Support group so that they inherit the necessary permissions via the attached *AmazonS3ReadOnlyAccess* policy.**

**Add users to respective groups using the following steps.**

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

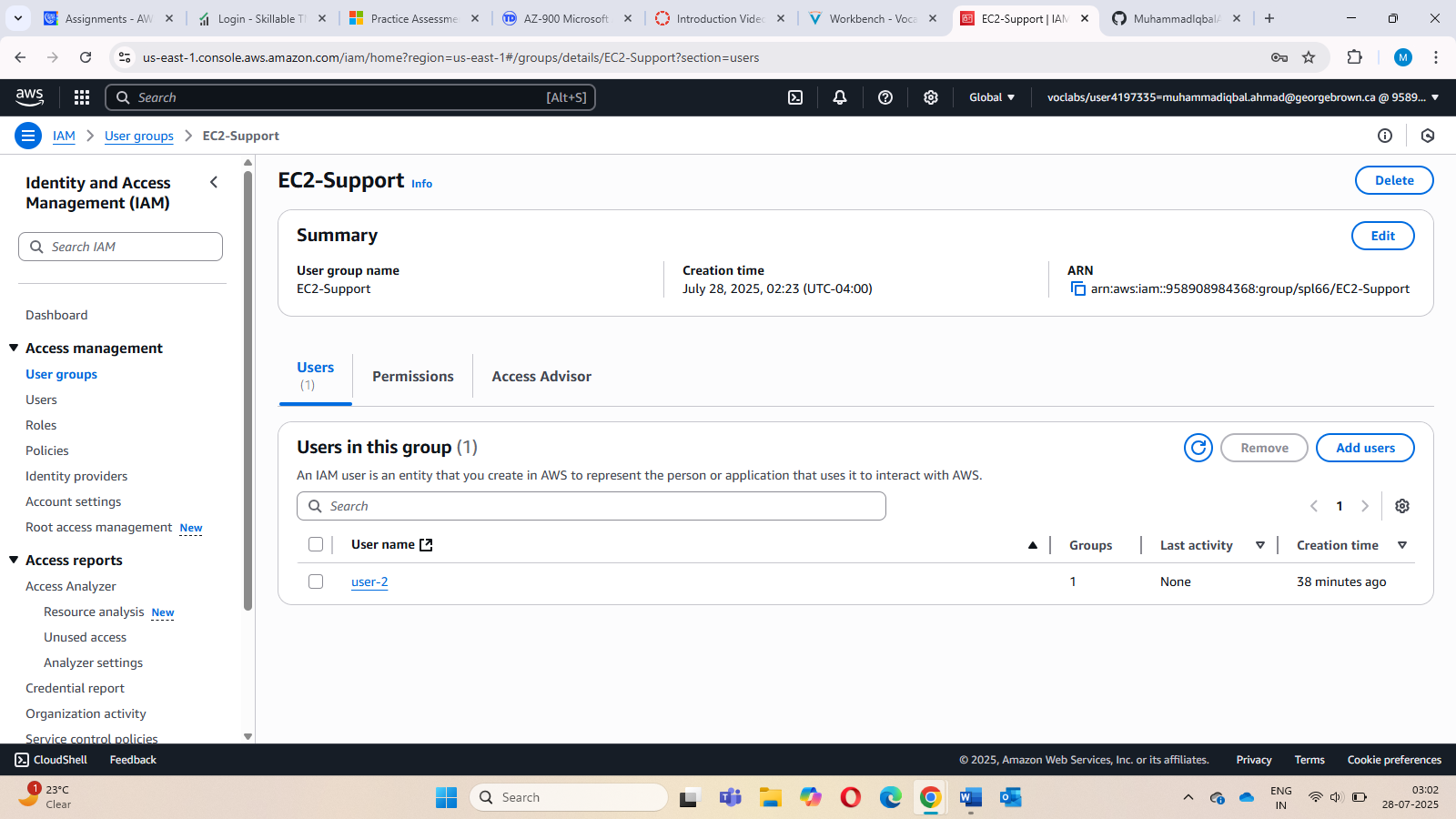
* **Choose the group link.**

* **Choose the Users tab.**

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

* **In the Add Users to group window, configure the following:**
  + **Select user.**
  + **At the bottom of the screen, choose Add users.**

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



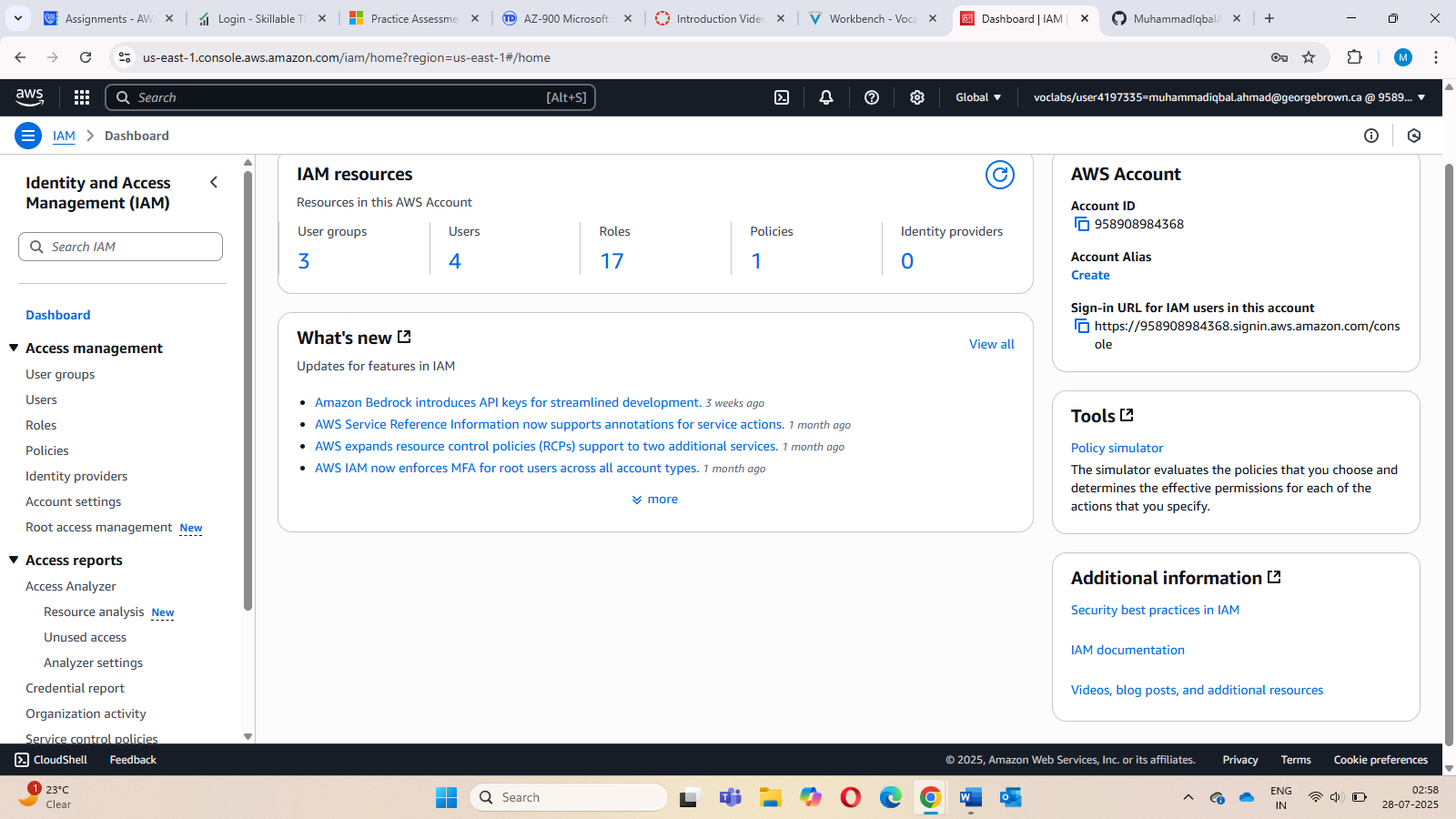
**Task 3: Sign-In and Test Users**

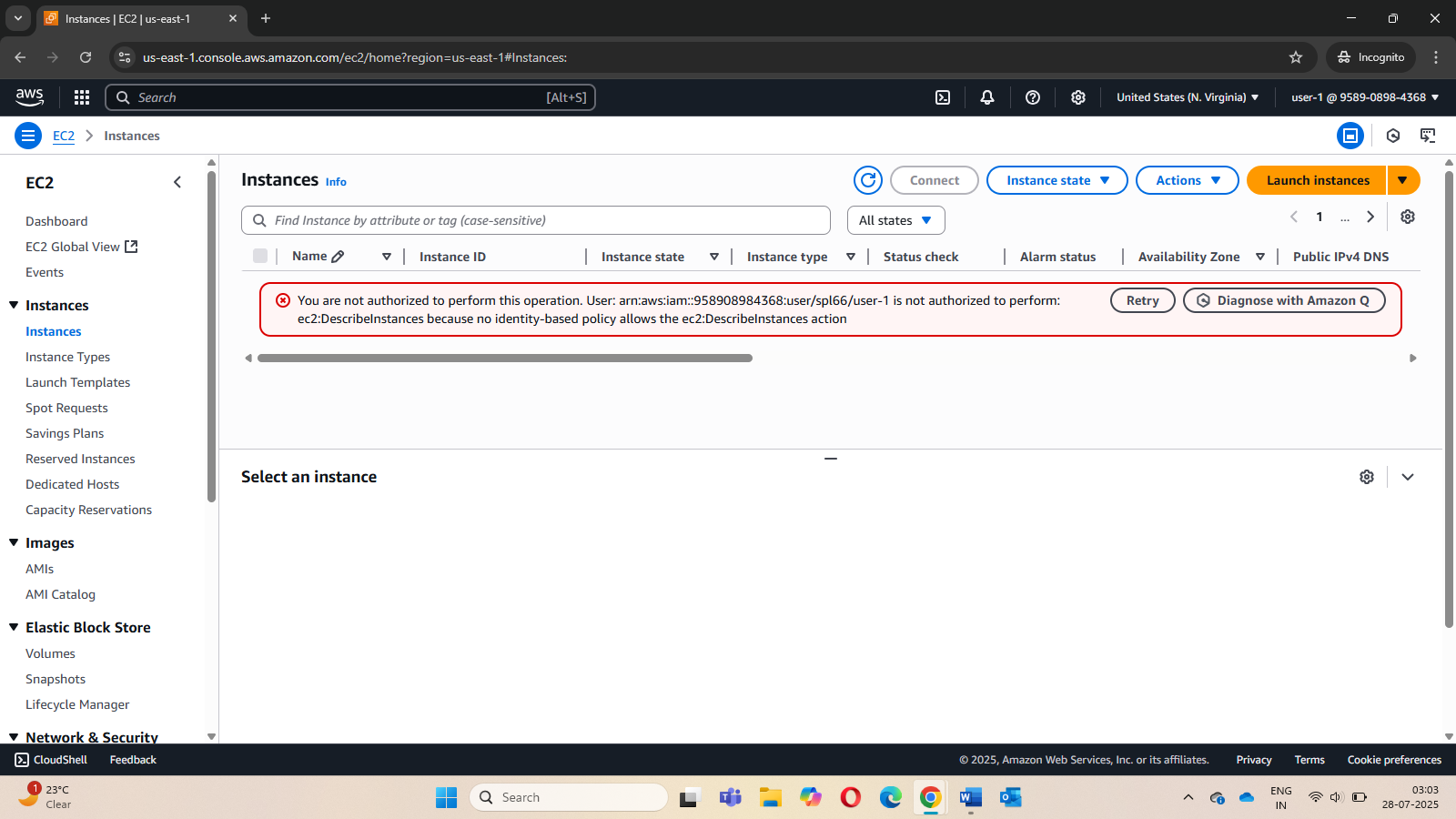
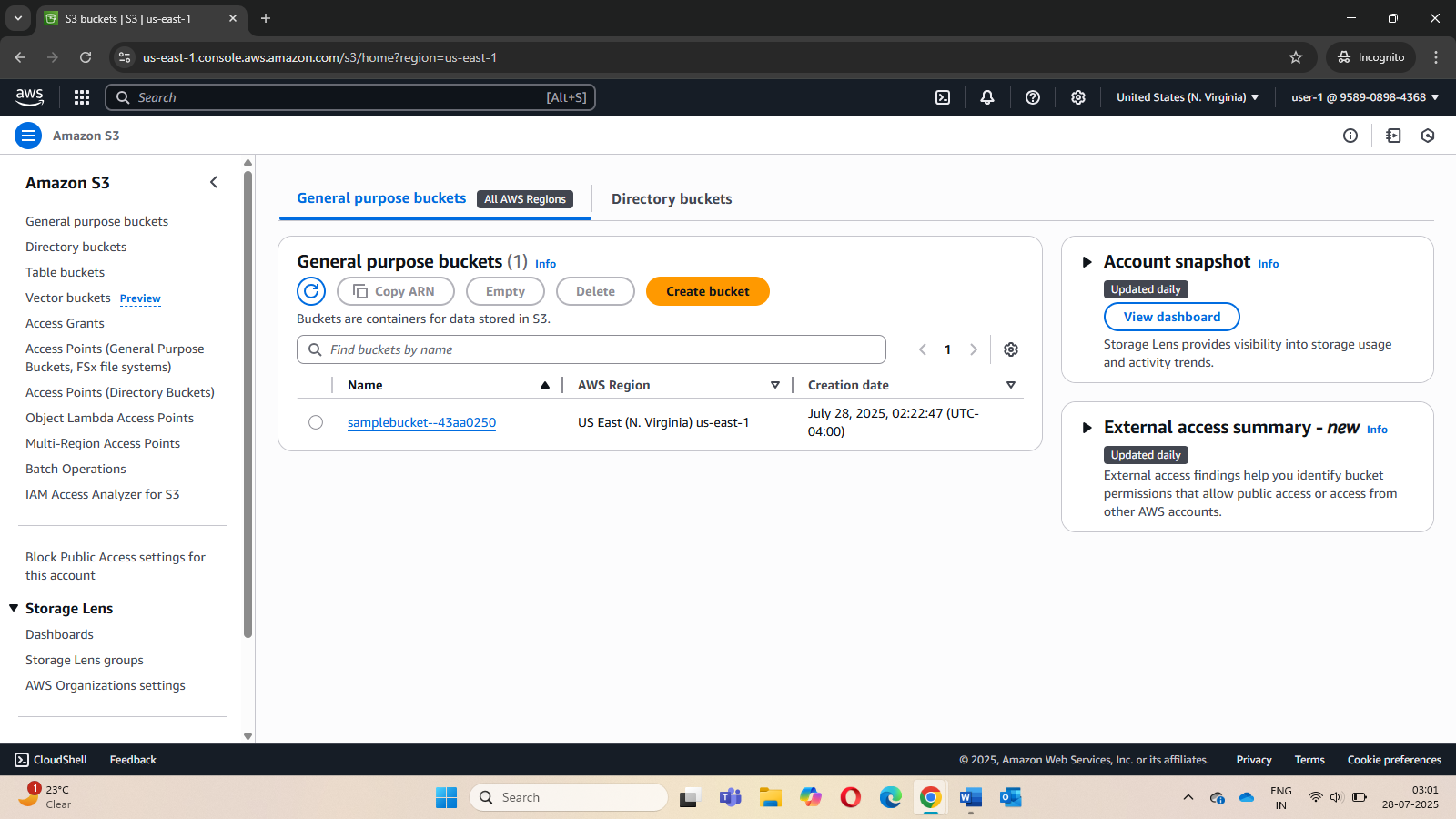
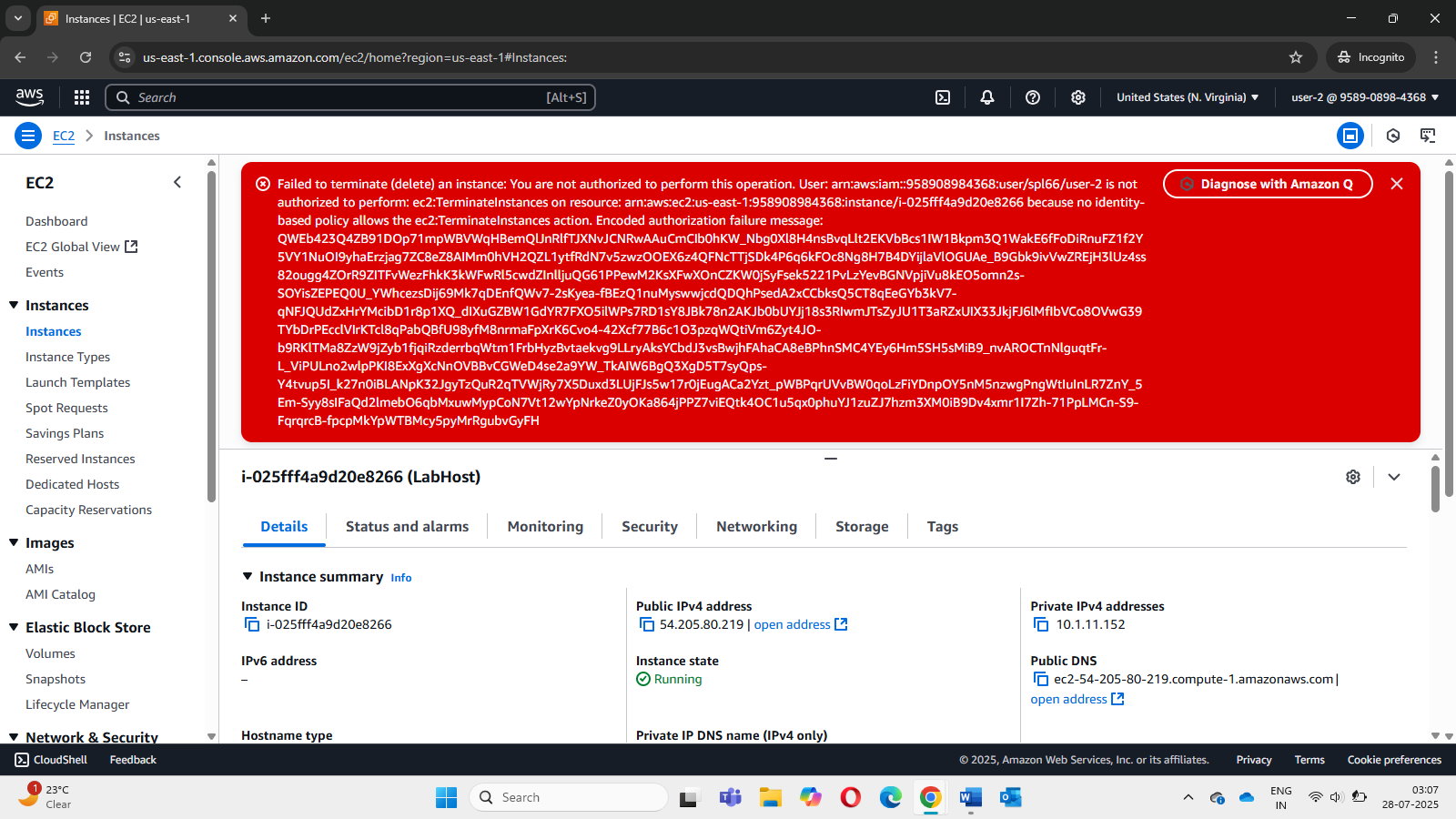
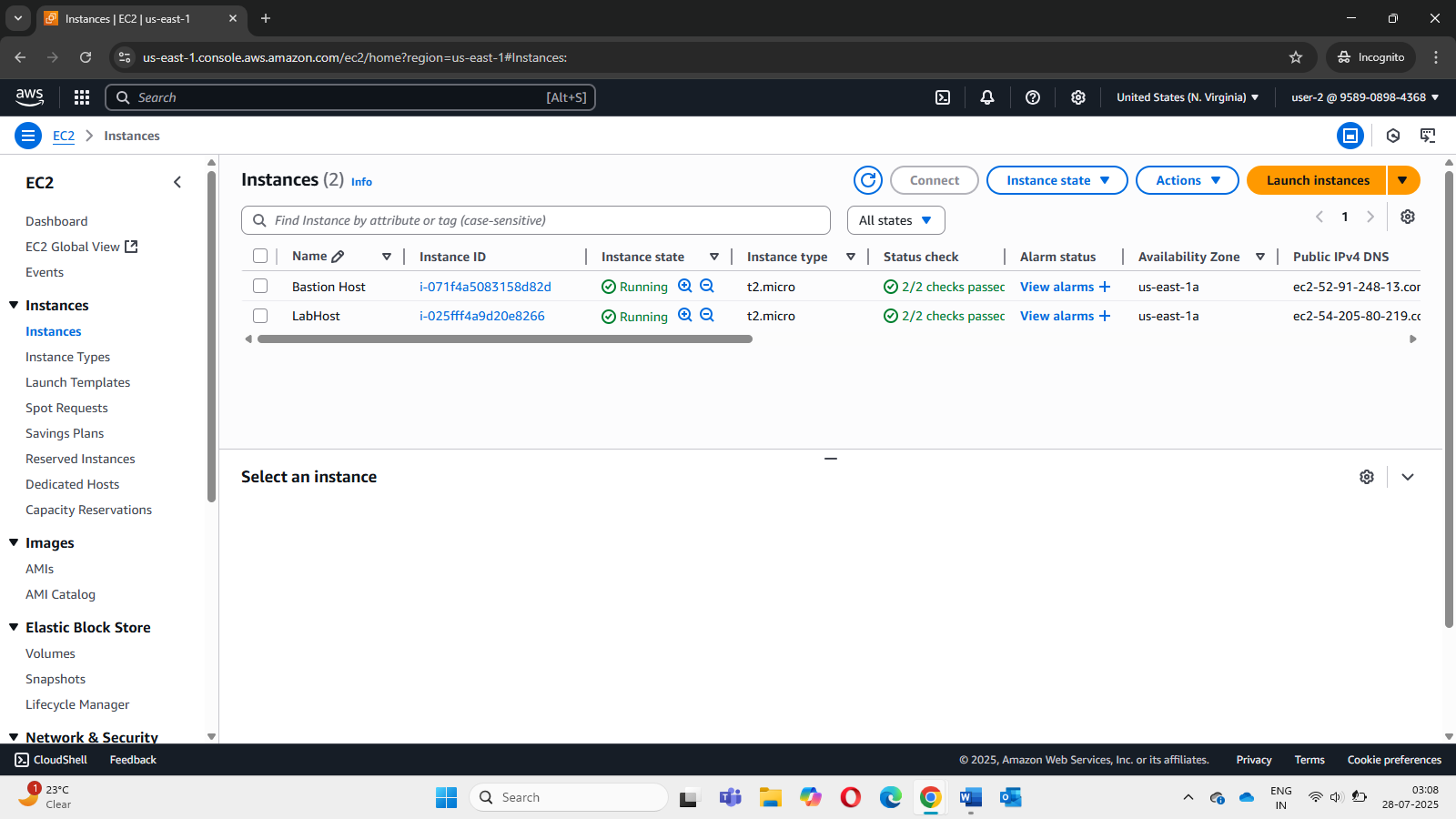
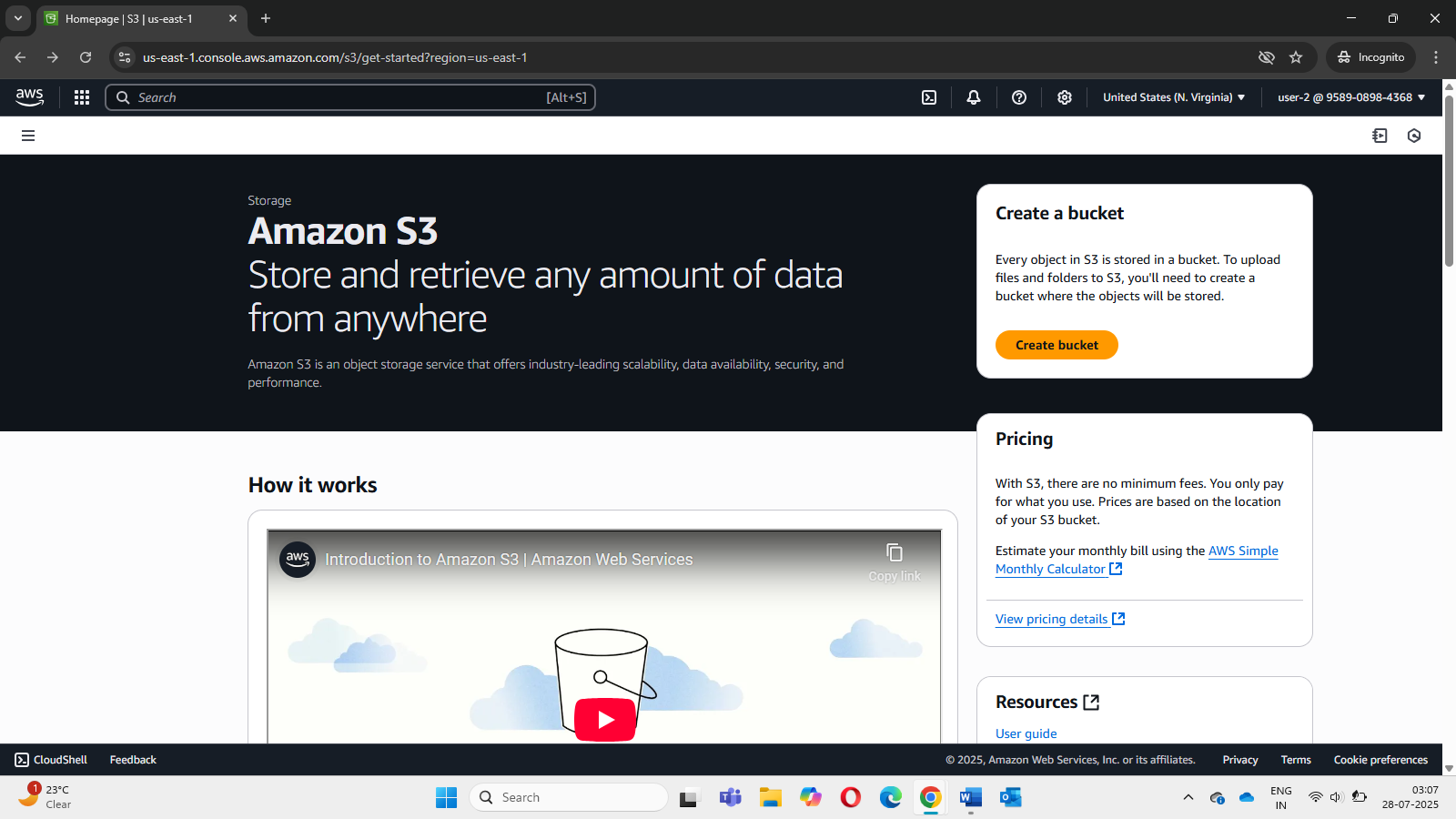
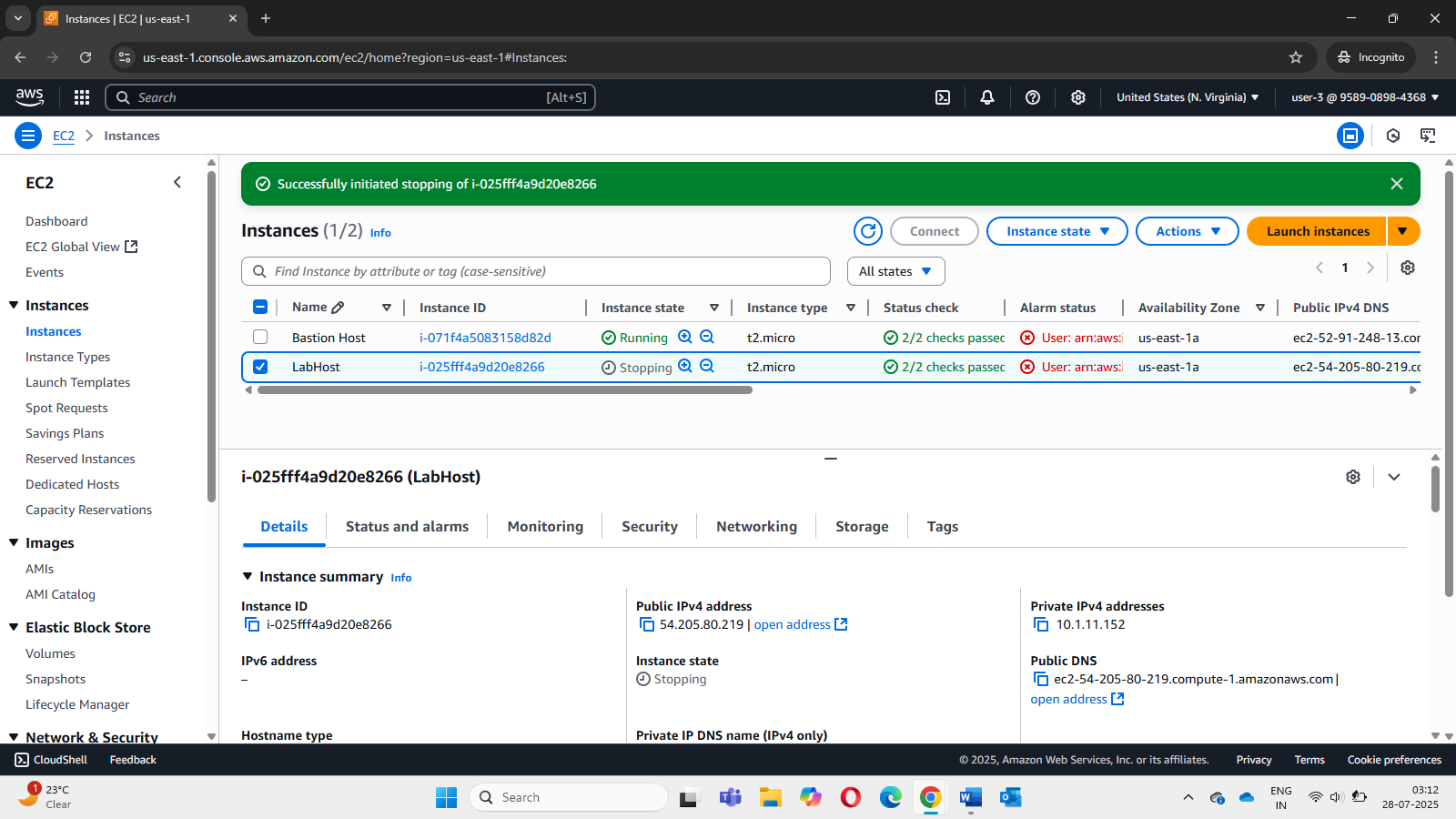
**In this task, you will test the permissions of each IAM User.**

* + 1. **In the navigation pane on the left, choose Dashboard.**

**A Sign-in URL for IAM users in this account link is displayed on the right. 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.**



* + 1. **Sign in with user-1 and Lab-Password1. Verify that S3 can be accessed while EC2 cannot be accessed by this user.**
    2. **Sign out of user-1’s account and sign in using user-2 credentials. Now you will see that user 2 does not have permissions to view S3 buckets. Also, this user has permission to view EC2 instances but cannot terminate them.**
    3. **Sign out and sign in using user-3 credentials. You will be able to stop instances now, since this user is part of the EC2 admin group which has permissions that allow this action.**

Conclusion

* Explored pre-created IAM users and groups
* Inspected IAM policies as applied to the pre-created groups
* Followed a real-world scenario, adding users to groups with specific capabilities enabled
* Located and used the IAM sign-in URL
* Experimented with the effects of policies on service access