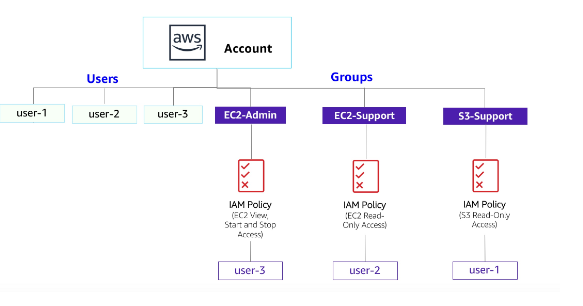
**EXPERIMENT :6**

# AIM: 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.



* 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

  Other AWS Services

During this lab, you may receive error messages when performing actions beyond the steps in this lab guide. These messages will not impact your ability to complete the lab.

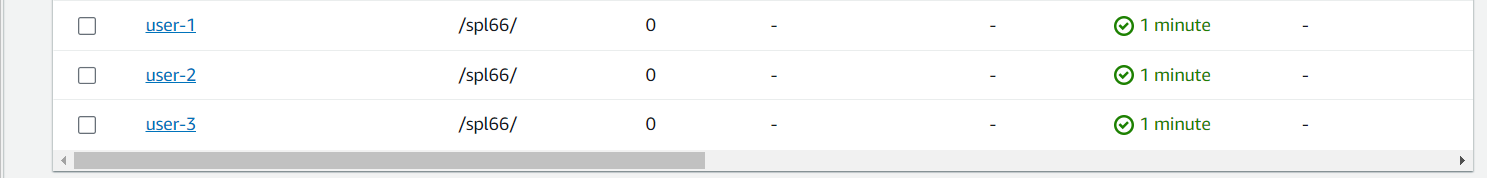
  AWS Identity and Access Management

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

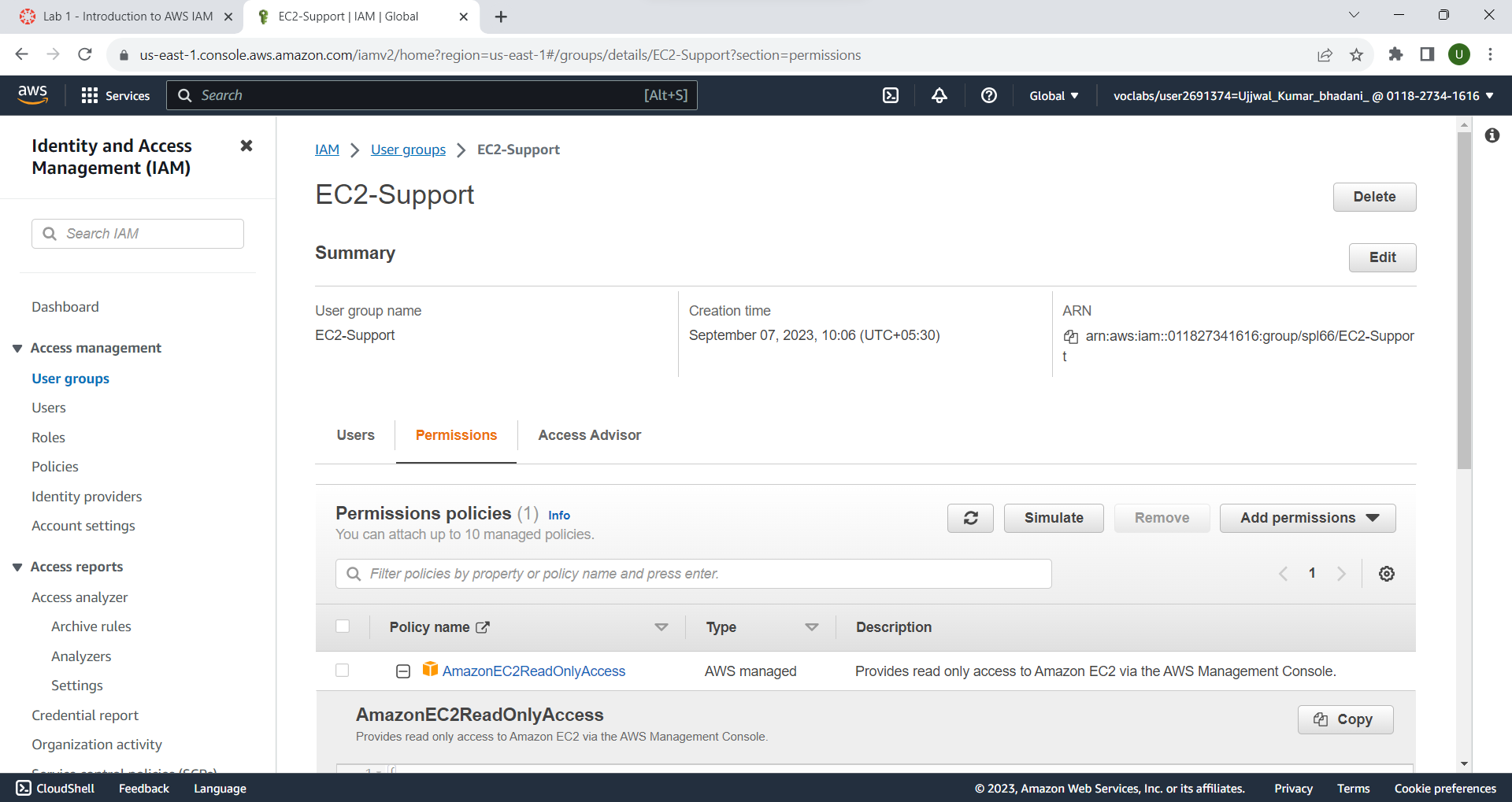
* Manage IAM Users and their access: You can create Users and assign them individual security credentials (access keys, passwords, and multi-factor authentication devices). You can manage permissions to control which operations a User can perform.
* Manage IAM Roles and their permissions: An IAM Role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

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

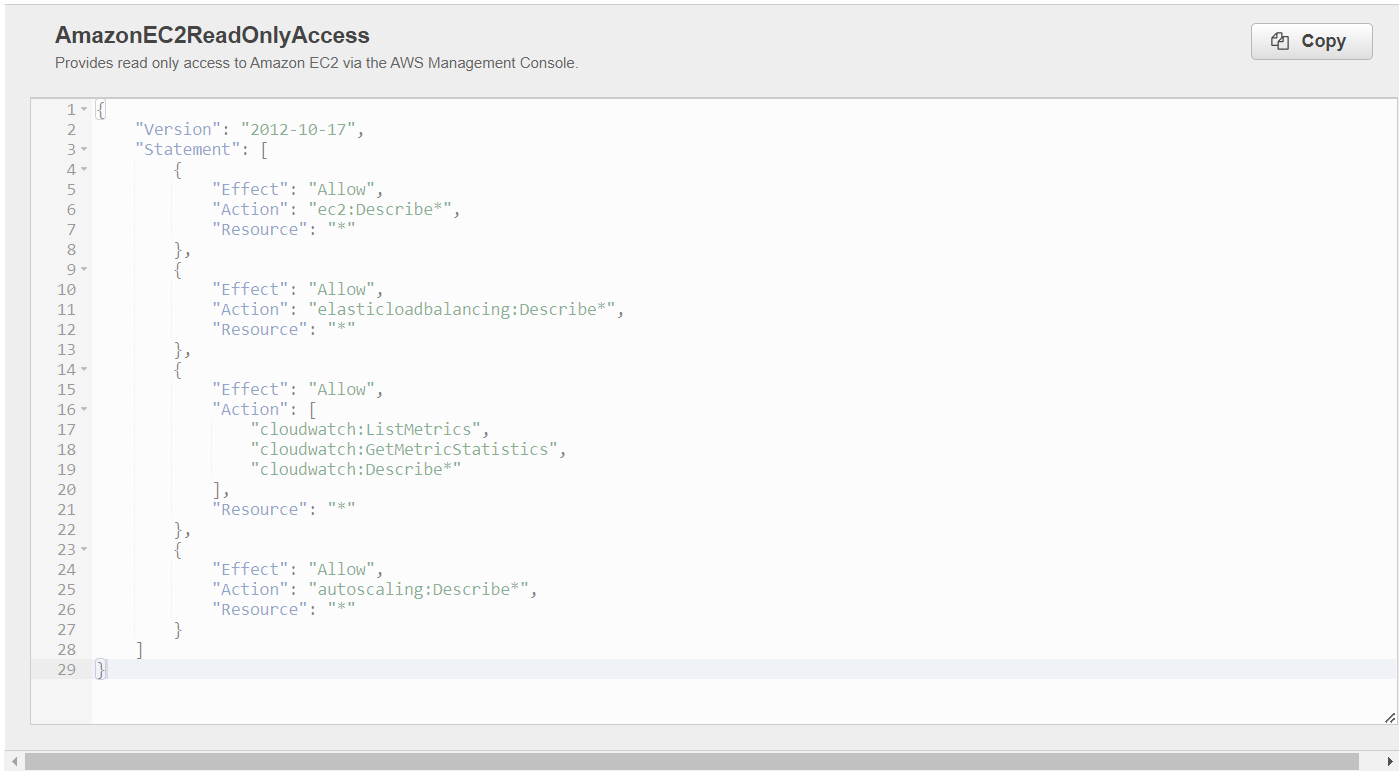
* In the **AWS Management Console**, on the **Services** menu, select **IAM**.
* In the navigation pane on the left, choose **Users**.
  + The following IAM Users have been created for you:
  + user-1
  + user-2
  + user-3



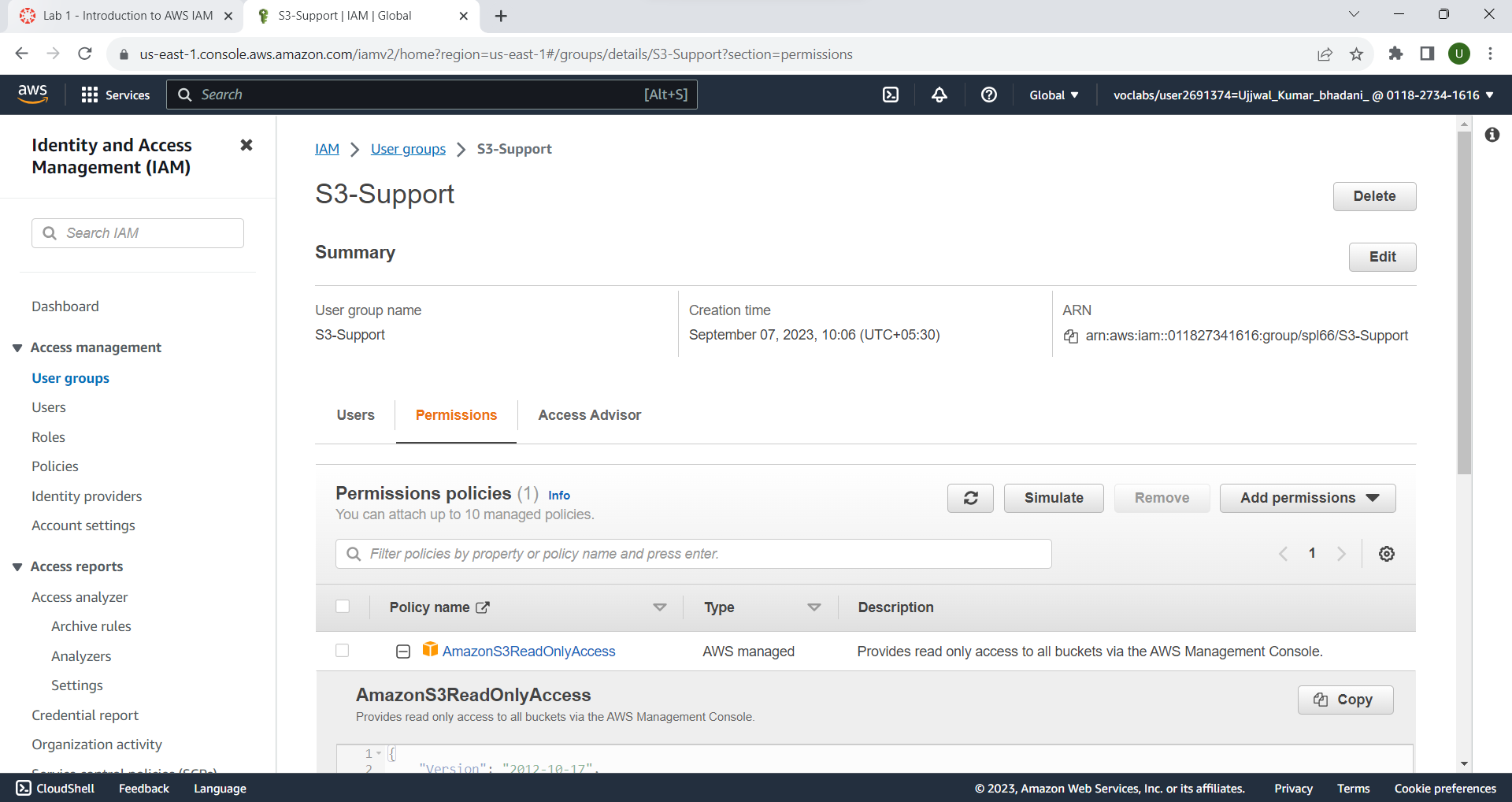
* Choose **user-1**.
* Notice that user-1 does not have any permissions.
* Choose the **Groups** tab.
* Choose the **Security credentials** tab.
* In the navigation pane on the left, choose **User groups**.
  + EC2-Admin
  + EC2-Support
  + S3-Support
* Choose the **EC2-Support** group.
* Choose the **Permissions** tab.



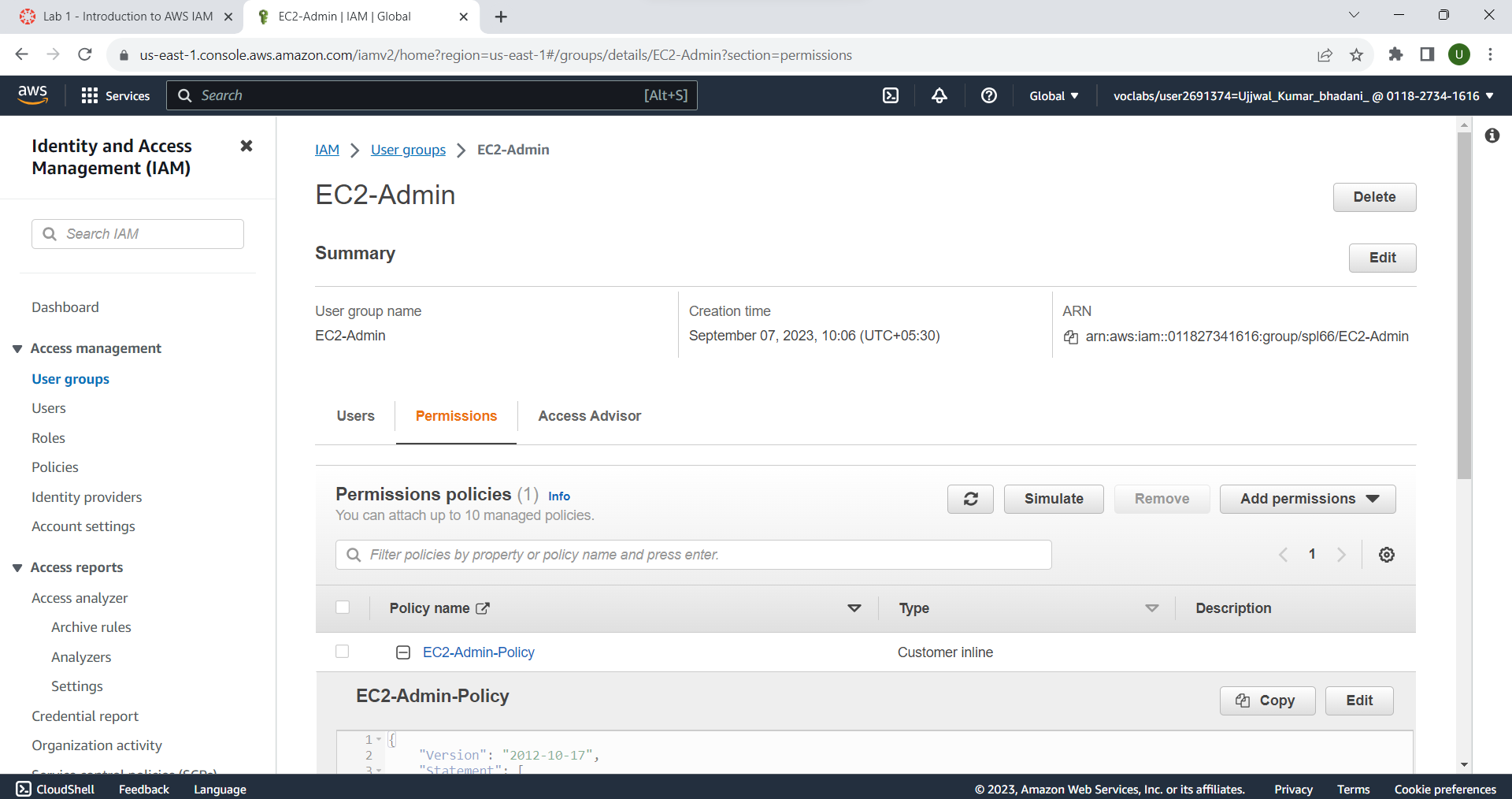
* Choose the plus (**+**) icon next to the AmazonEC2ReadOnlyAccess policy to view the policy details.

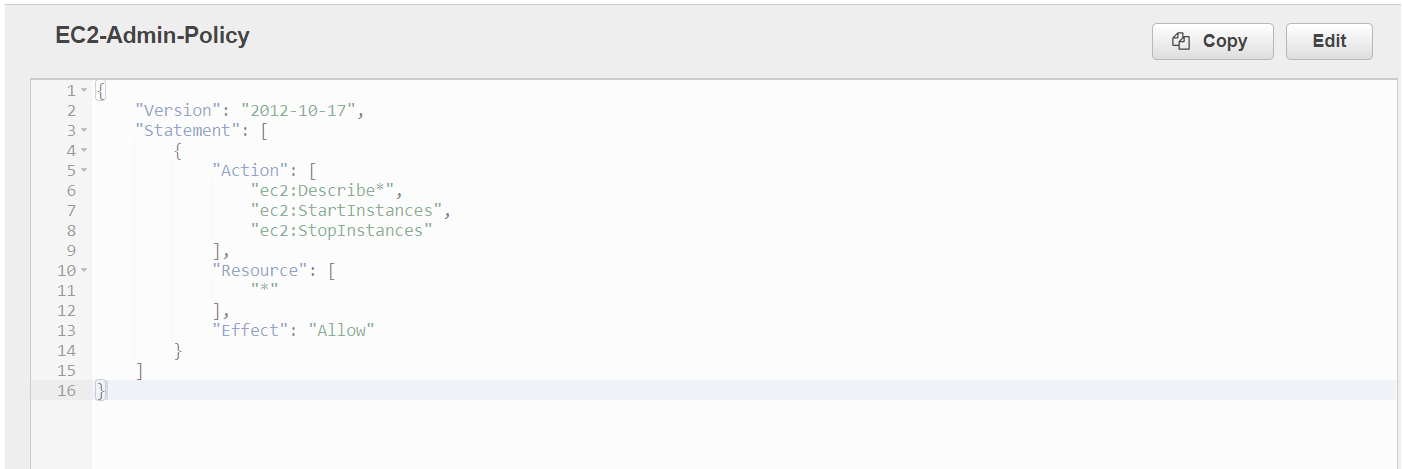


* Choose the minus icon (**-**) to hide the policy details.
* In the navigation pane on the left, choose **User groups**.
* Choose the **S3-Support** group and then choose the **Permissions** tab.
* Choose the plus (**+**) icon to view the policy details.
* Choose the minus icon (**-**) to hide the policy details.



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

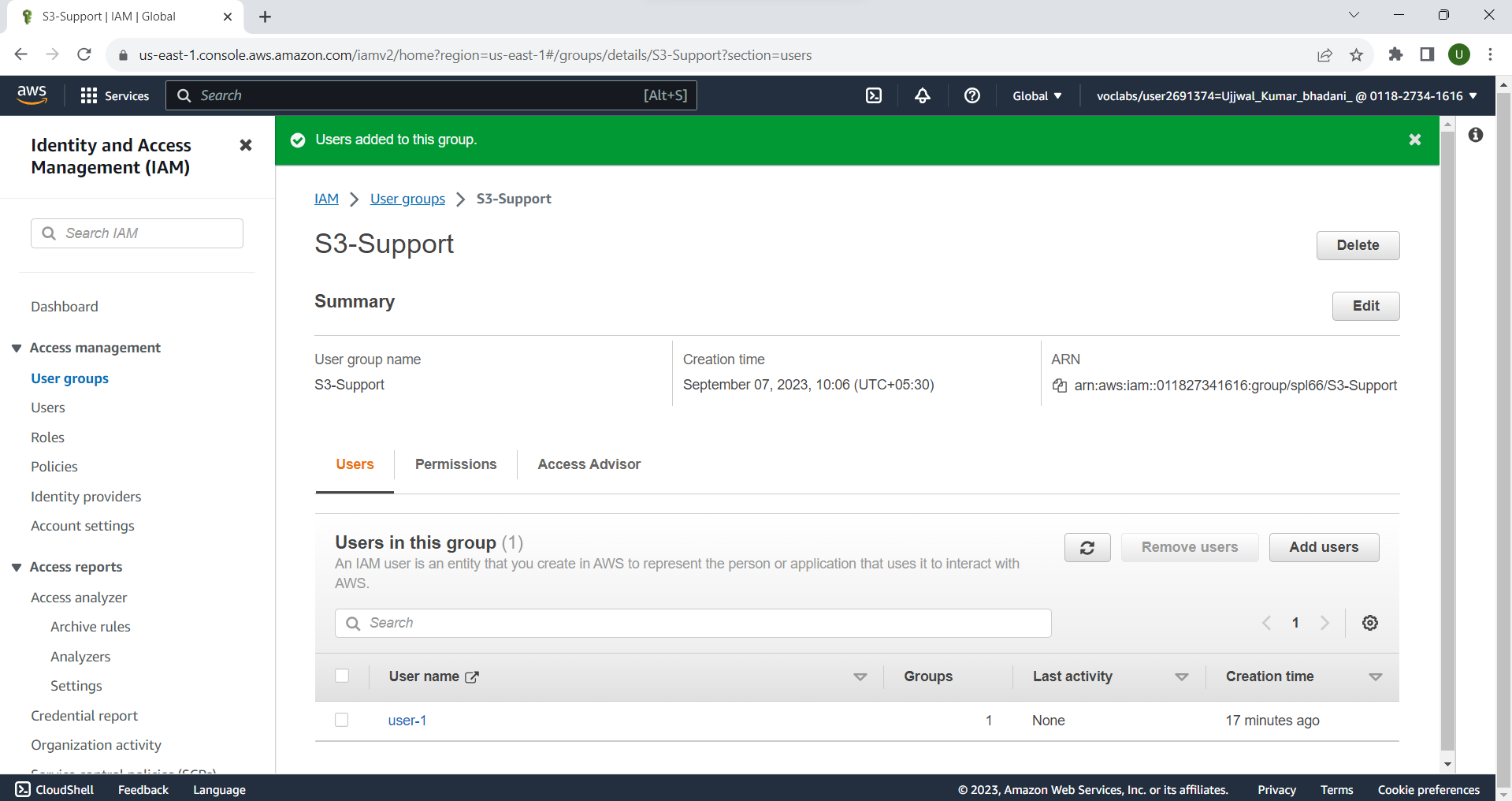




## **Task 2: Add Users to Groups**

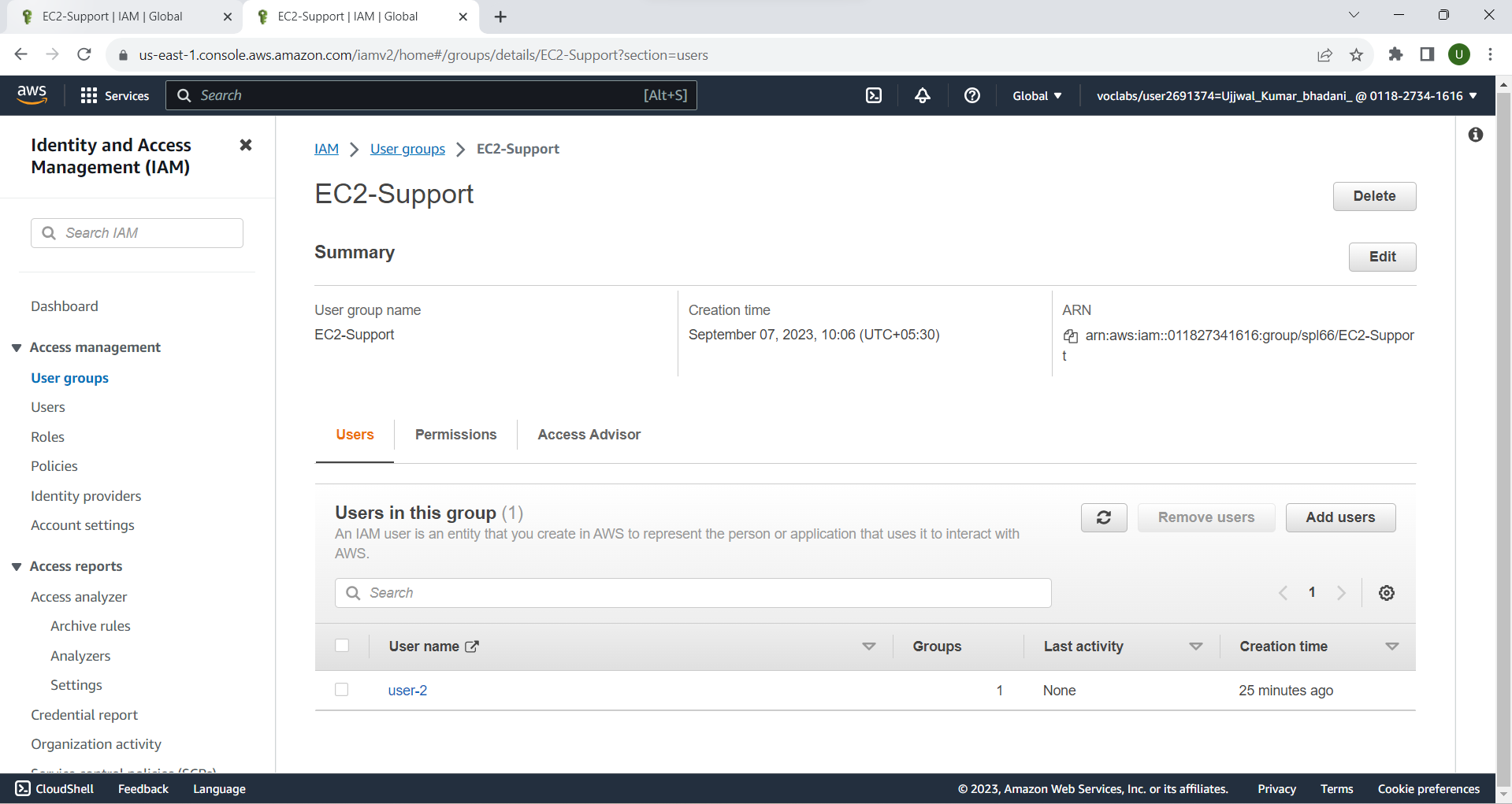
### Add user-1 to the S3-Support Group

* In the left navigation pane, choose **User groups**.
* Choose the **S3-Support** group.
* Choose the **Users** tab.
* In the **Users** tab, choose **Add users**.
* 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.



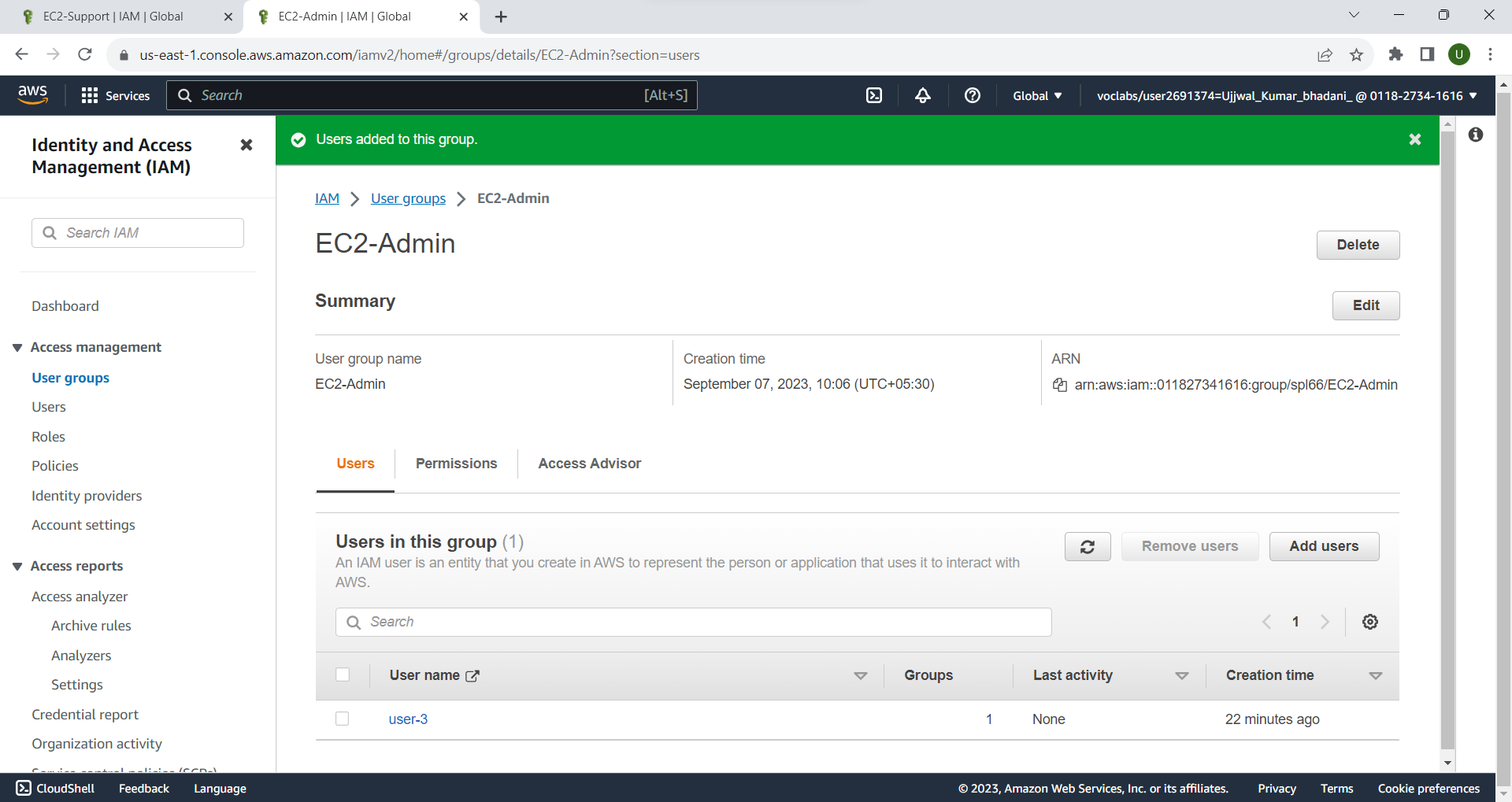
### Add user-2 to the EC2-Support Group

* You have hired **user-2** into a role where they will provide support for Amazon EC2.
* Using similar steps to the ones above, add **user-2** to the **EC2-Support** group.
* user-2 should now be part of the **EC2-Support** group.



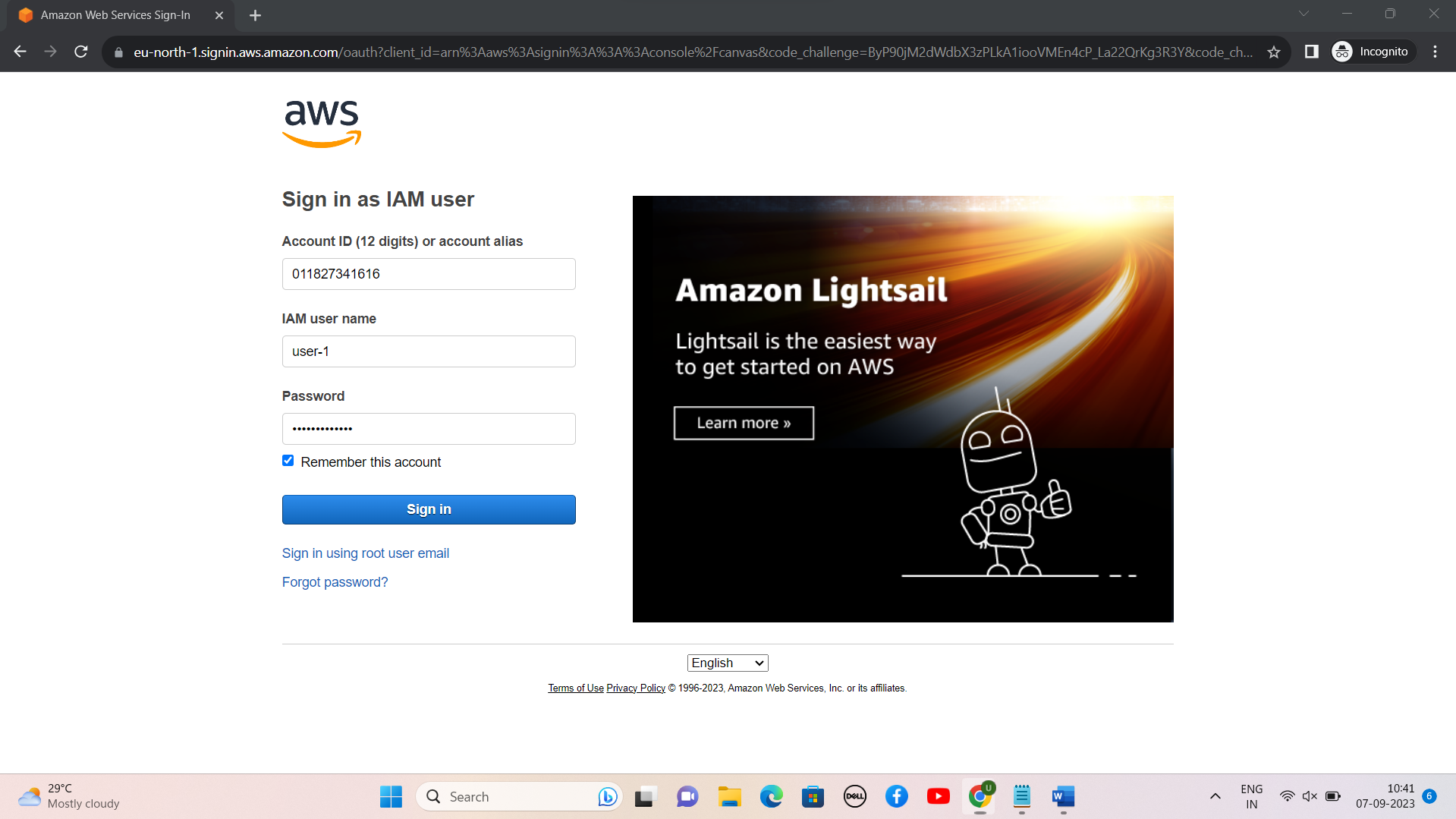
### Add user-3 to the EC2-Admin Group. You have hired **user-3** as your Amazon EC2 administrator, who manage your EC2 instances.

* Using similar steps to the ones above, add **user-3** to the **EC2-Admin** group.user-3 should now be part of the **EC2-Admin** group.

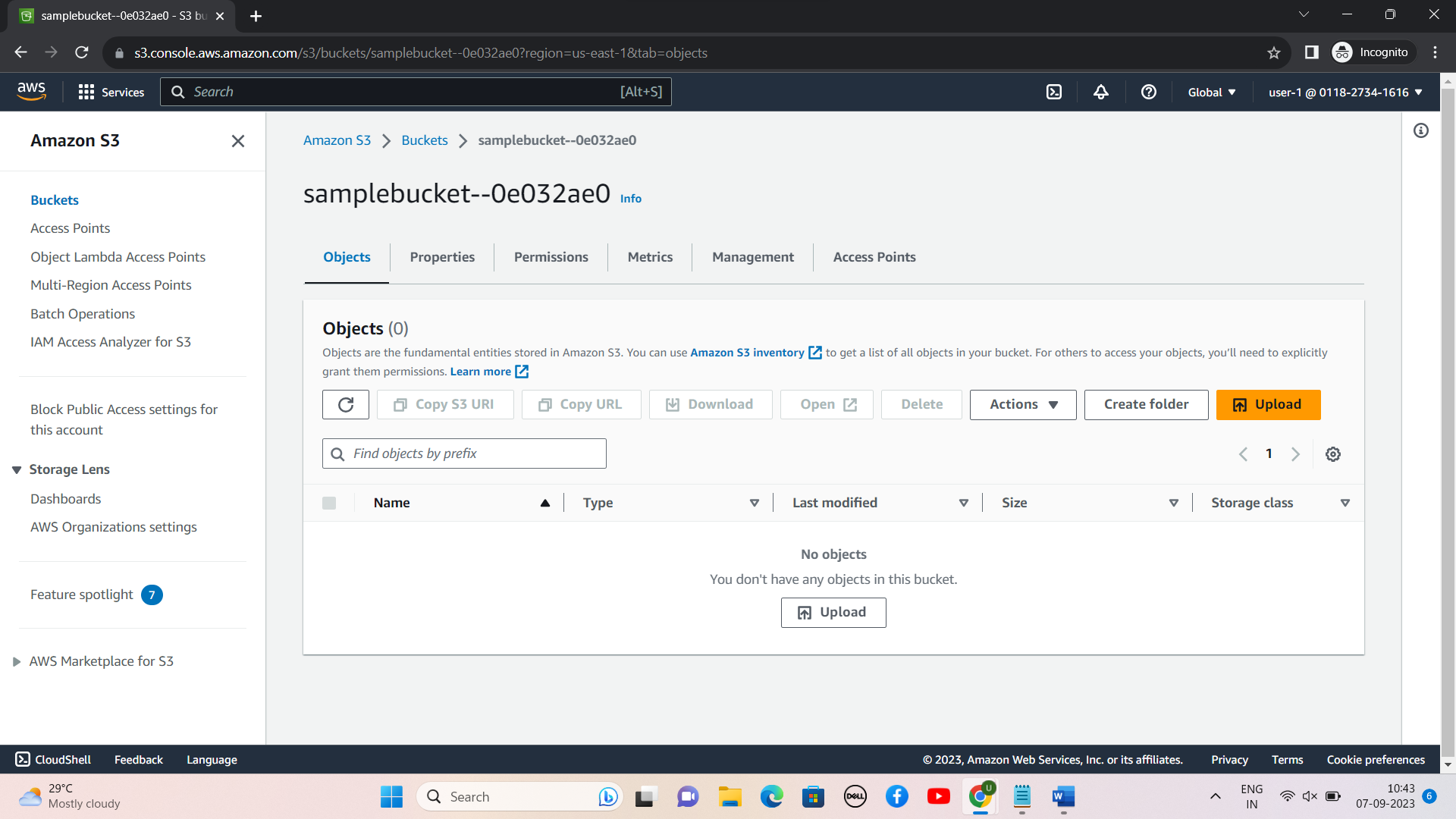


## **Task 3: Sign-In and Test Users**

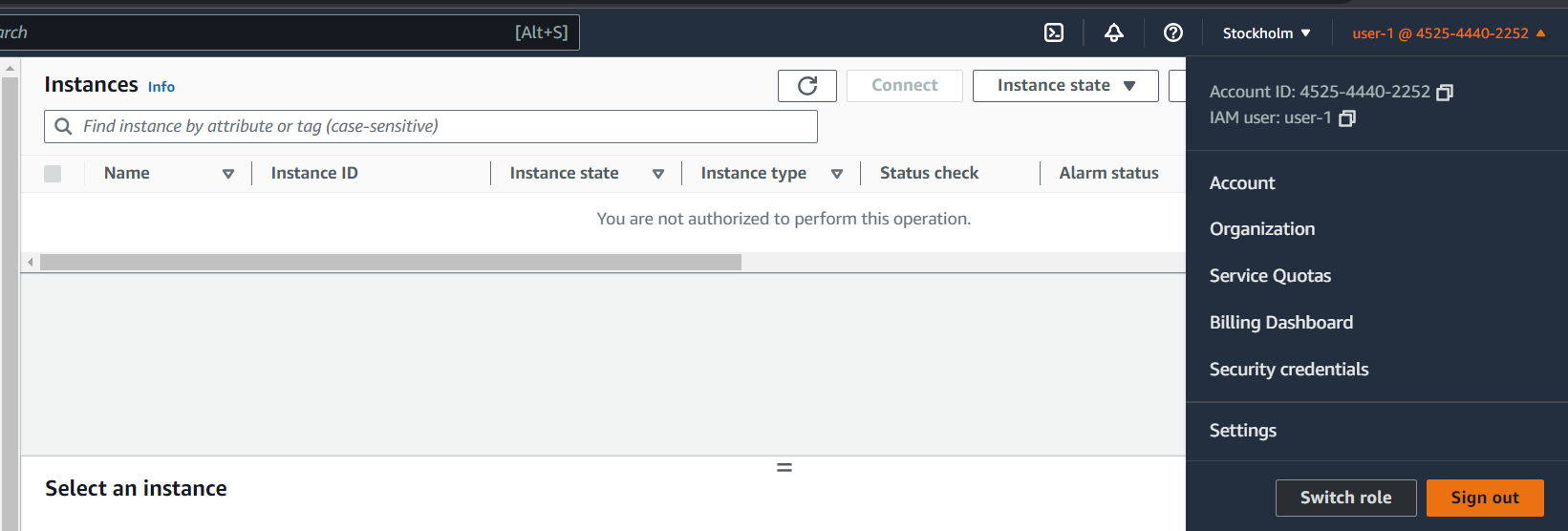
* In the navigation pane on the left, choose **Dashboard**.
* Copy the **Sign-in URL for IAM users in this account** to a text editor.
* Open a private (Incognito) window.
* Paste the **IAM users sign-in** link into the address bar of your private browser session and press **Enter**.
* Sign-in with:
  + **IAM user name:** user-1
  + **Password:** Lab-Password1



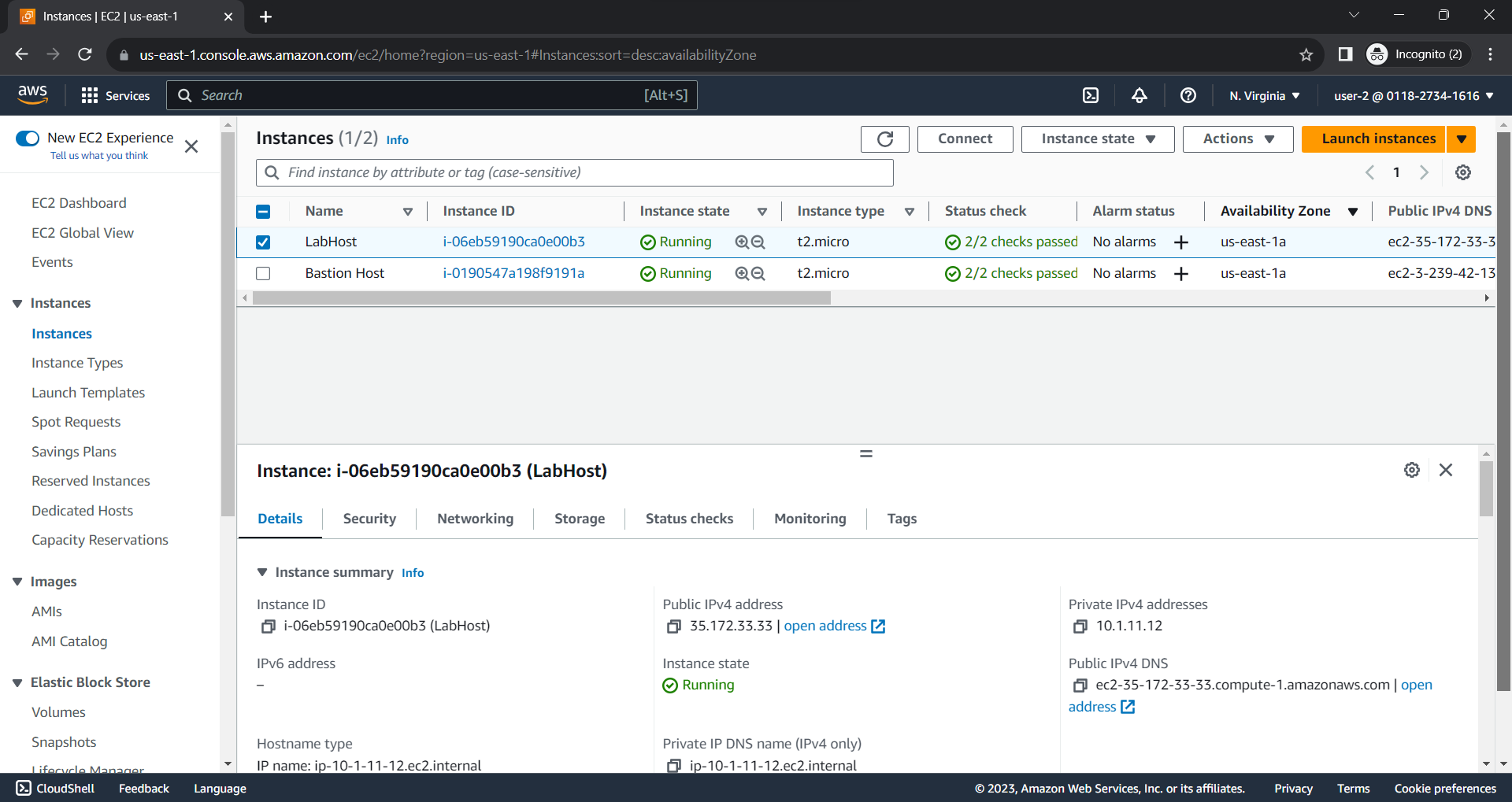
* In the **Services** menu, choose **S3**.
* Choose the name of the bucket that exists in the account and browse the contents.



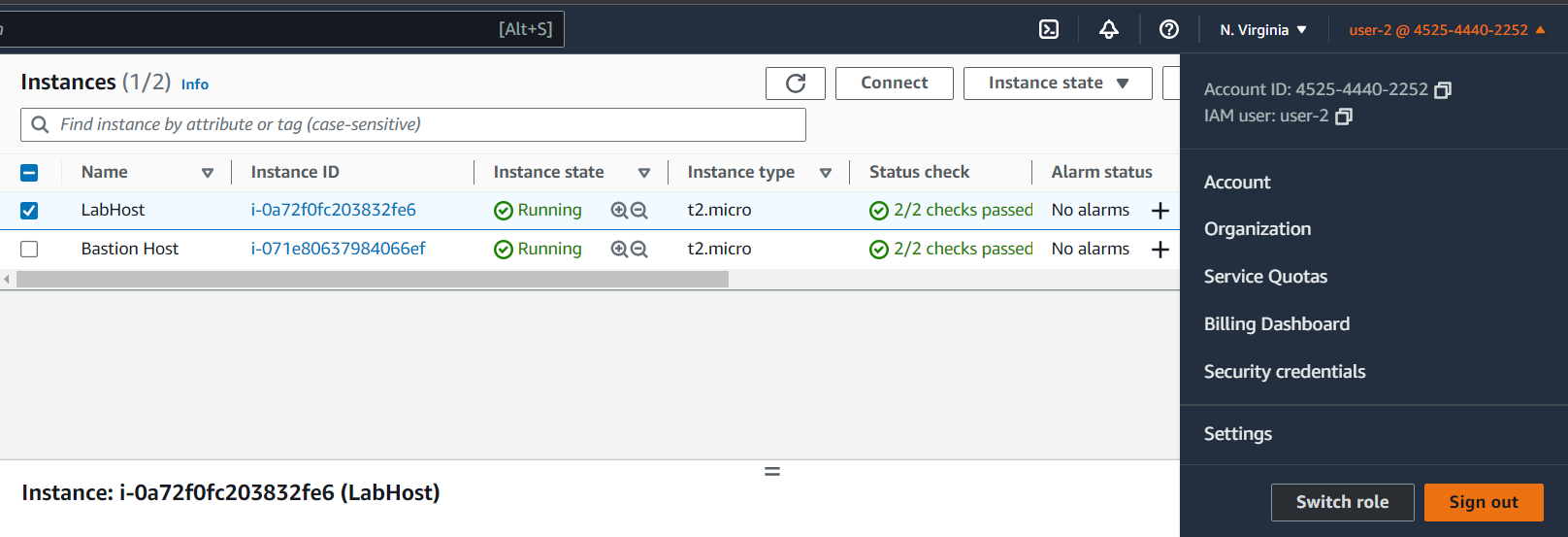
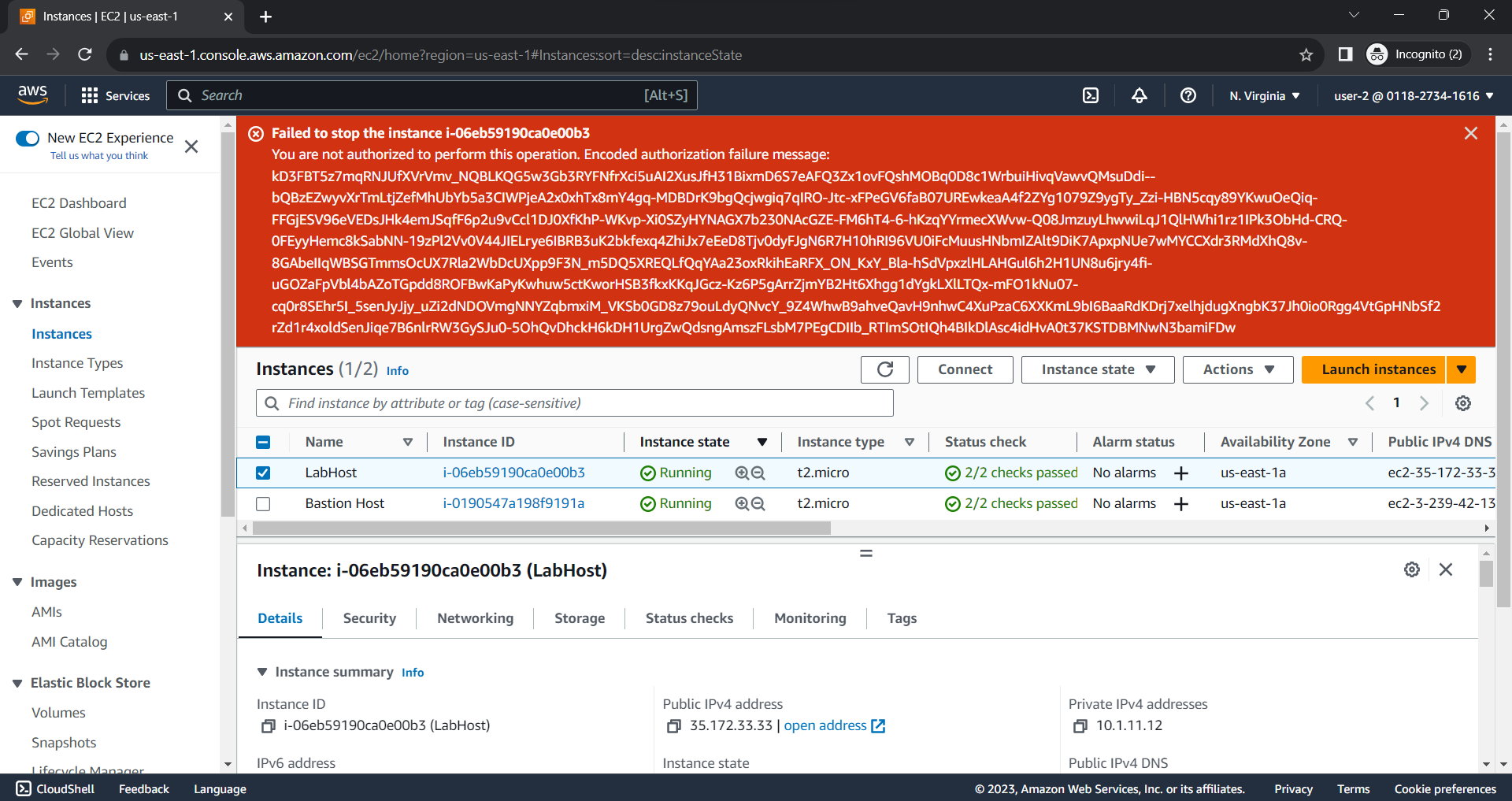
* In the **Services** menu, choose **EC2**.
* In the left navigation pane, choose **Instances**.
* Sign user-1 out of the **AWS Management Console** by completing the following actions:
  + At the top of the screen, choose **user-1**
  + Choose **Sign Out**

****

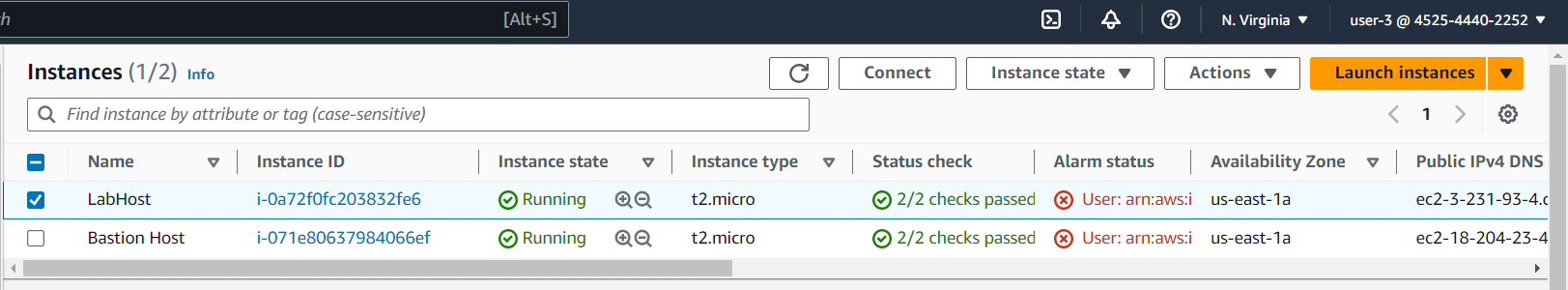
* Paste the IAM users sign-in link into your private browser tab's address bar and press Enter.
* Sign-in with:
  + IAM user name: user-2
  + Password: Lab-Password2
* In the Services menu, choose EC2.
* In the navigation pane on the left, choose Instances.
  + Select the instance named  *LabHost*.
* In the Instance state menu above, select Stop instance.
* In the Stop Instance window, select Stop.



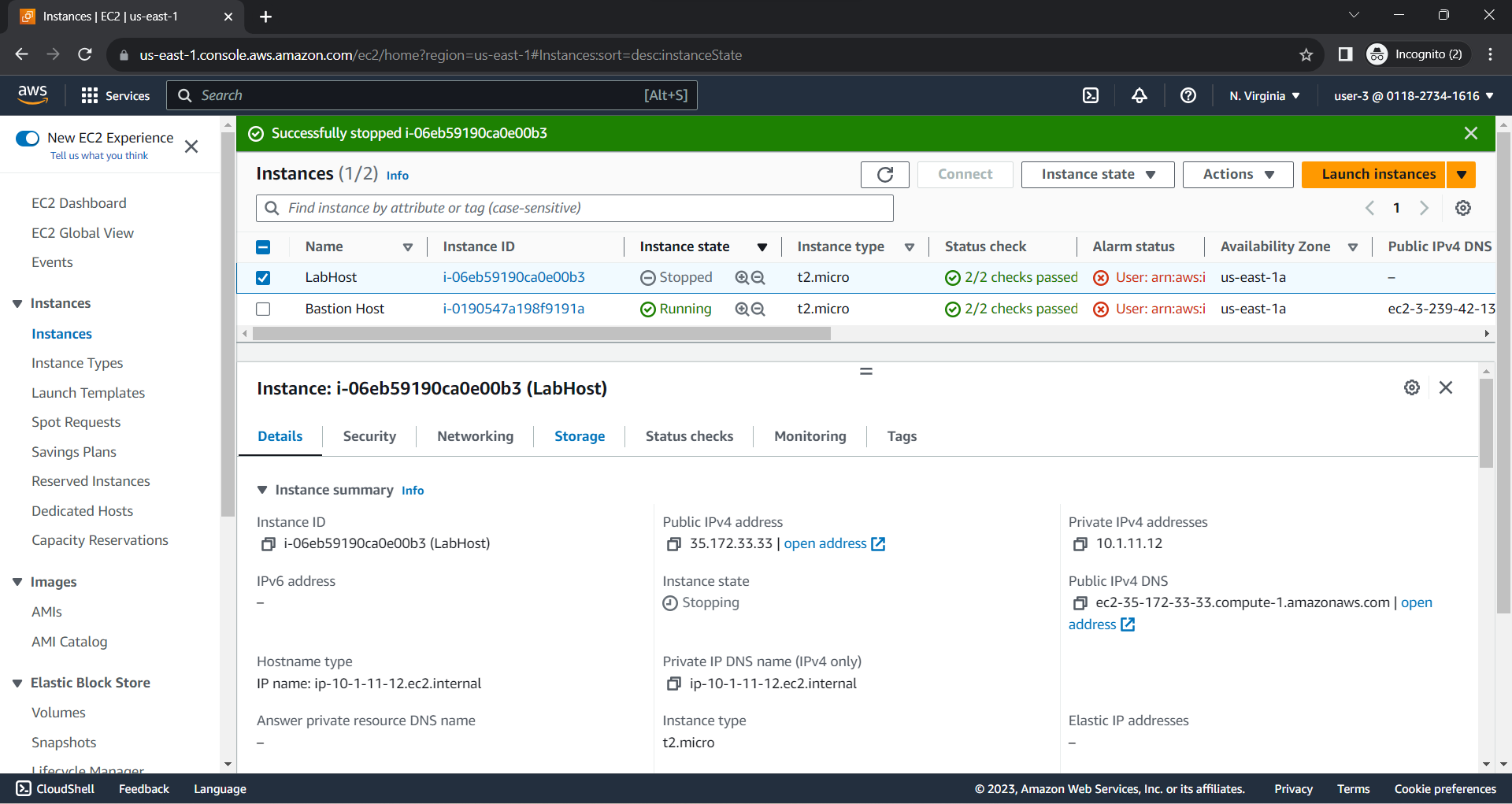
* Choose the X to close the *Failed to stop the instance* message.
* In the Services, choose S3.
* Sign user-2 out of the AWS Management Console by completing the following actions:
  + At the top of the screen, choose user-2
  + Choose Sign Out



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



* Select the instance named  LabHost .In the **Instance state** menu, choose **Stop instance**.
* In the **Stop instance** window, choose **Stop**.



|  |  |
| --- | --- |
| NAME : | Ujjwal Kumar Bhadani |
| ROLL NO: | CIT21046 |
| REG NO: | 2101020286 |
| GROUP: | 4 |
| SEMESTER: | 5th |

Submitted by