Intro to Cloud Computing

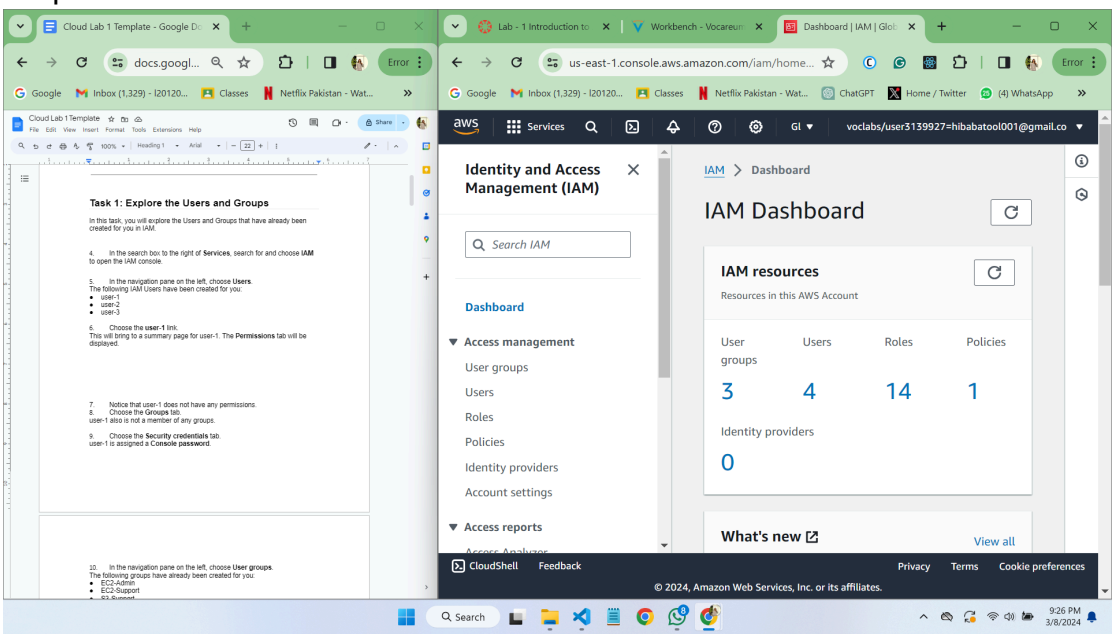
Lab - 1 Introduction to AWS IAM

Hiba Batool
20L-1205, Section 8-A

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.

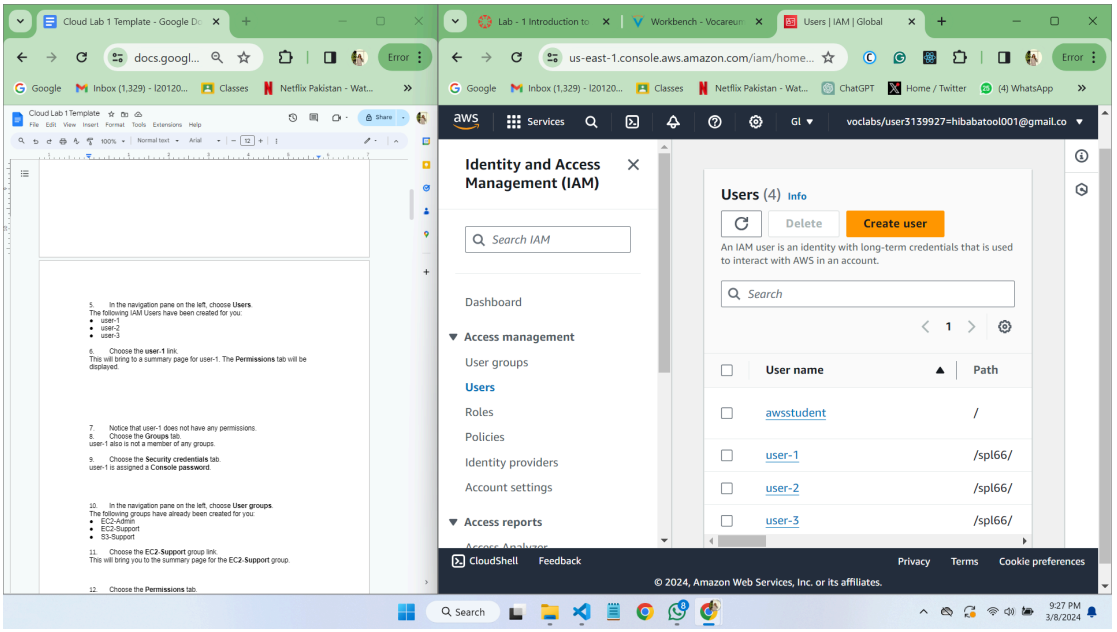
4. In the search box to the right of **Services**, search for and choose **IAM** to open the IAM console.



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

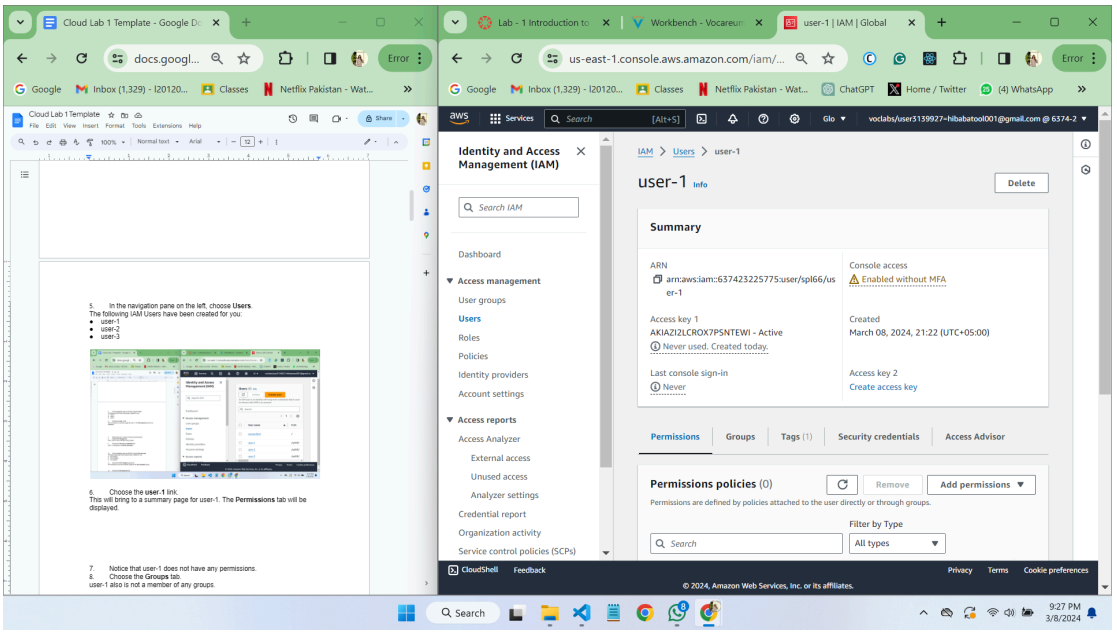
The following IAM Users have been created for you:

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



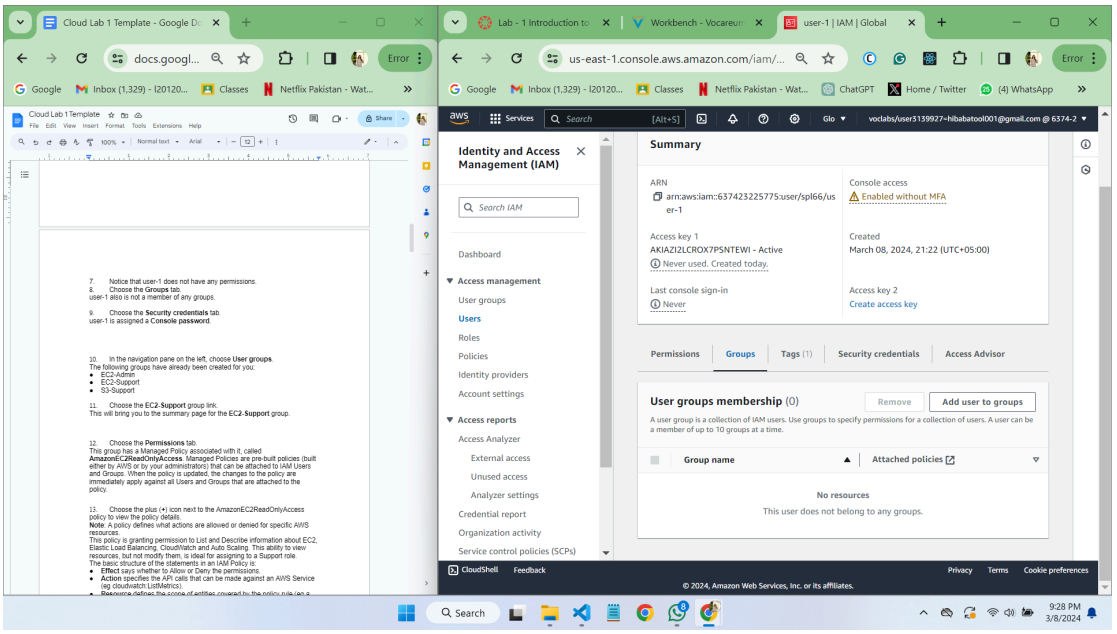
6. Choose the **user-1** link.

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



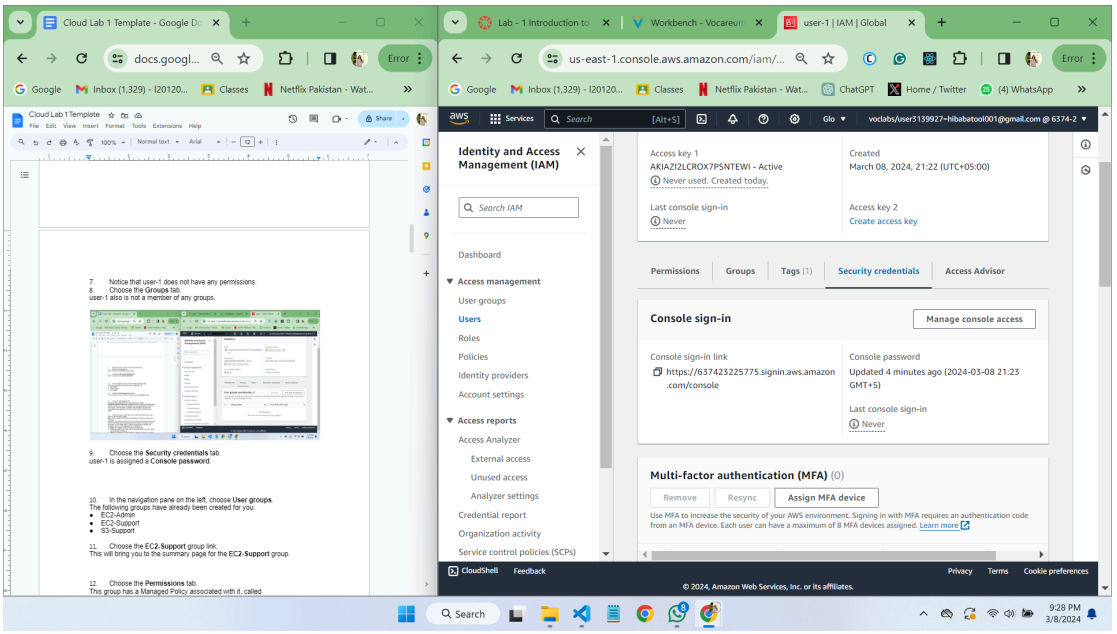
7. Notice that user-1 does not have any permissions.
8. Choose the **Groups** tab.

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



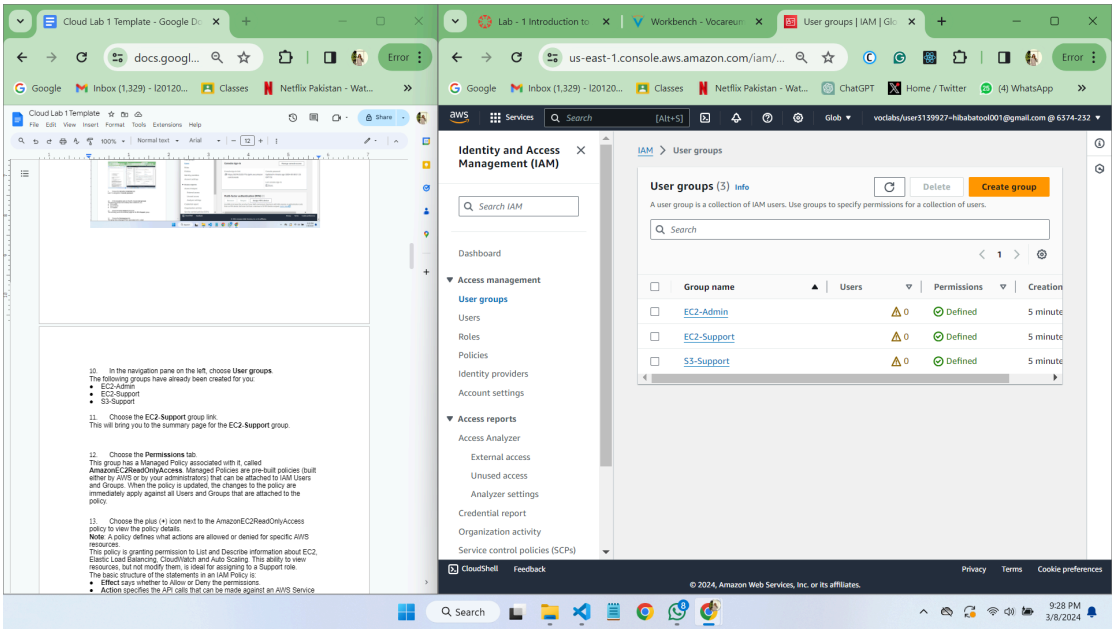
9. Choose the **Security credentials** tab.

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

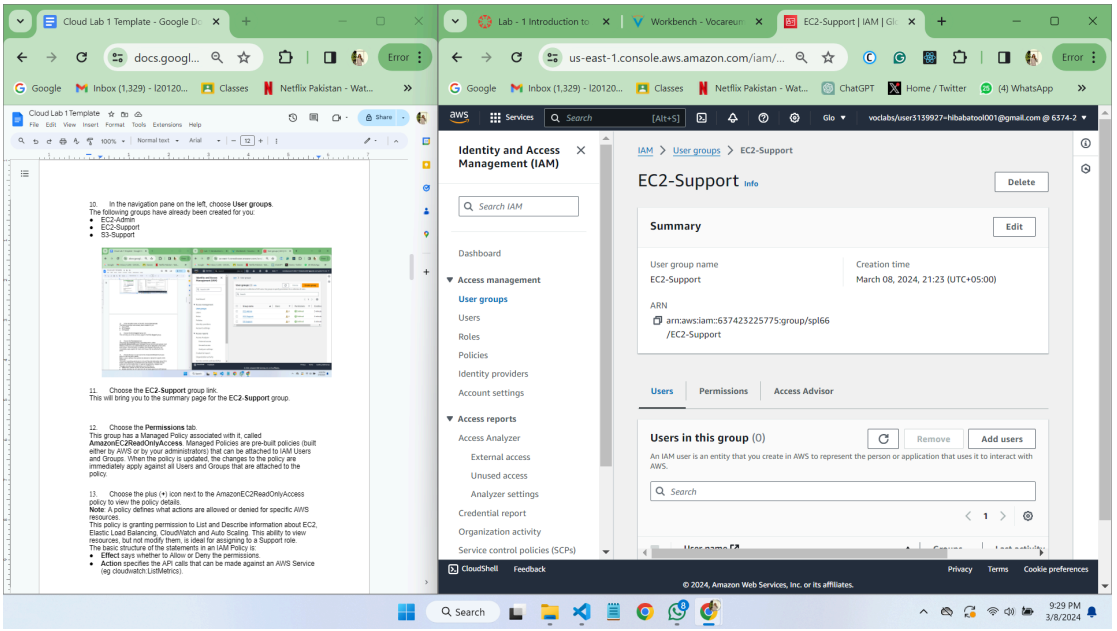


10. In the navigation pane on the left, choose **User groups**.
The following groups have already been created for you:

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

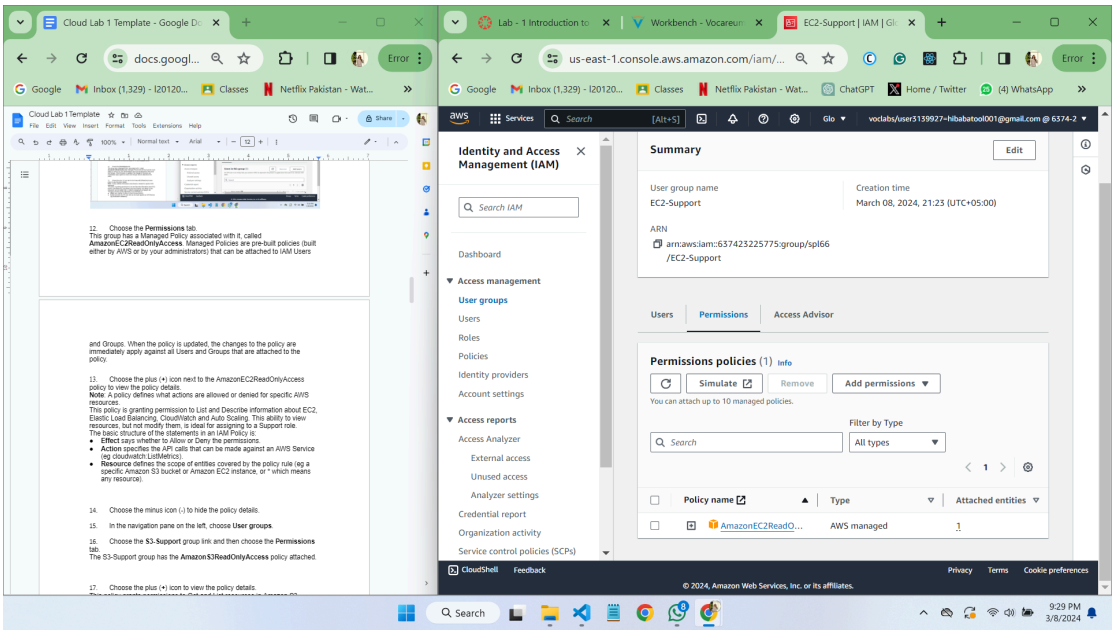


11. Choose the **EC2-Support** group link.
This will bring you to the summary page for the **EC2-Support** group.



12. 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.



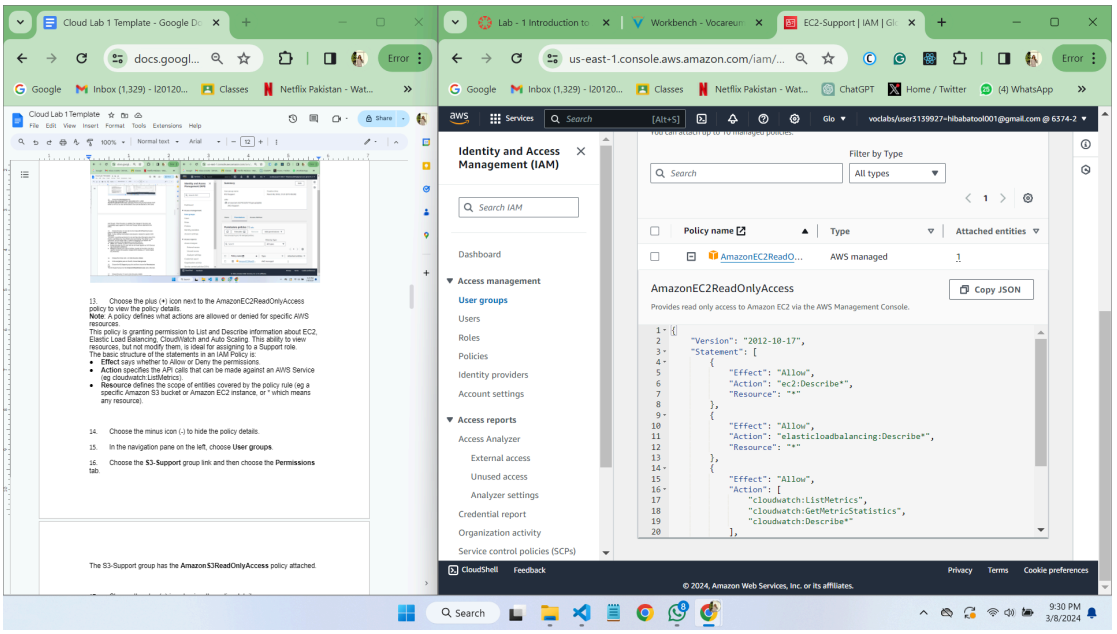
13. Choose the plus (**+**) icon next to the AmazonEC2ReadOnlyAccess policy to view the policy details.

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).

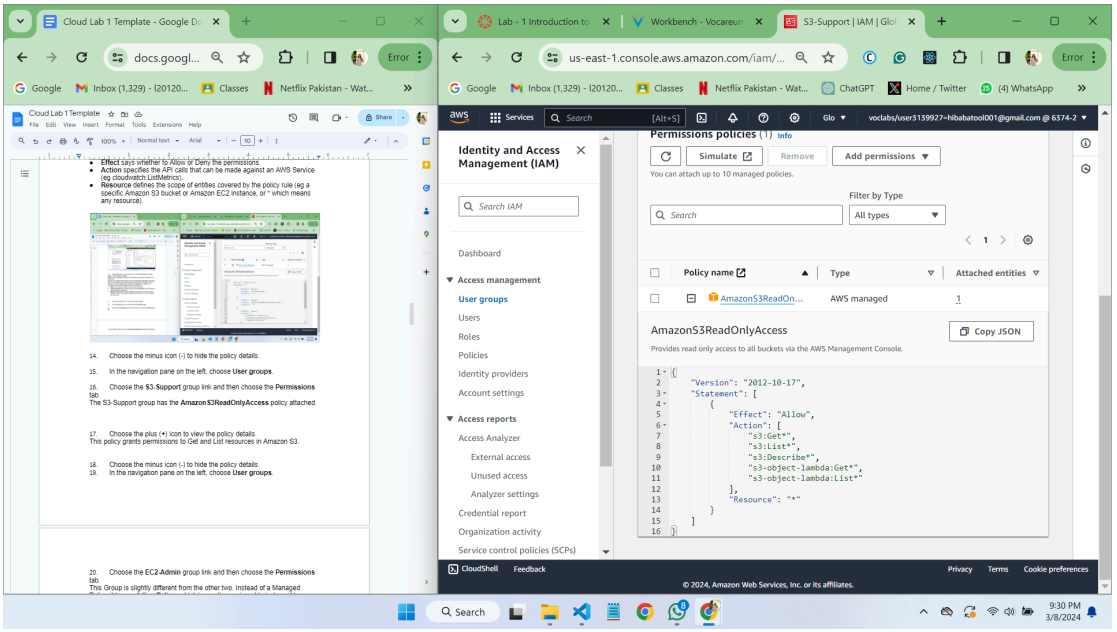


14. Choose the minus icon (-) to hide the policy details.

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

16. Choose the **S3-Support** group link and then choose the **Permissions** tab.
The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.

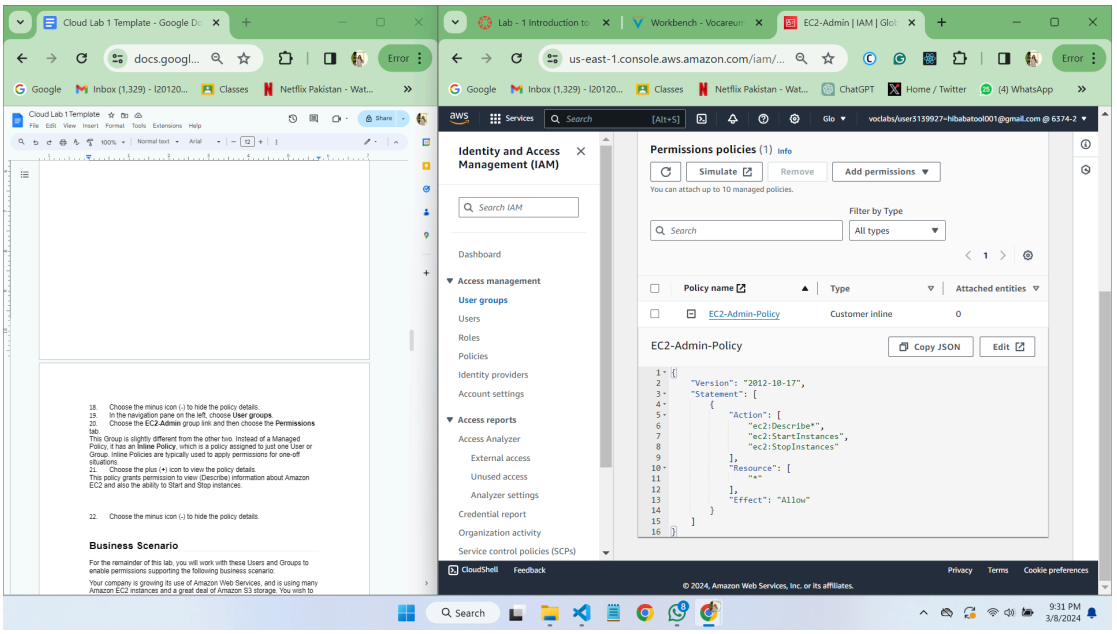
17. Choose the plus (**+**) icon to view the policy details.
This policy grants permissions to Get and List resources in Amazon S3.



18. Choose the minus icon (**-**) to hide the policy details.
19. In the navigation pane on the left, choose **User groups**.
20. 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.

21. 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.

22. Choose the minus icon (**-**) to hide the policy details.

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.

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.

Add user-1 to the S3-Support Group

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

24. Choose the **S3-Support** group link.

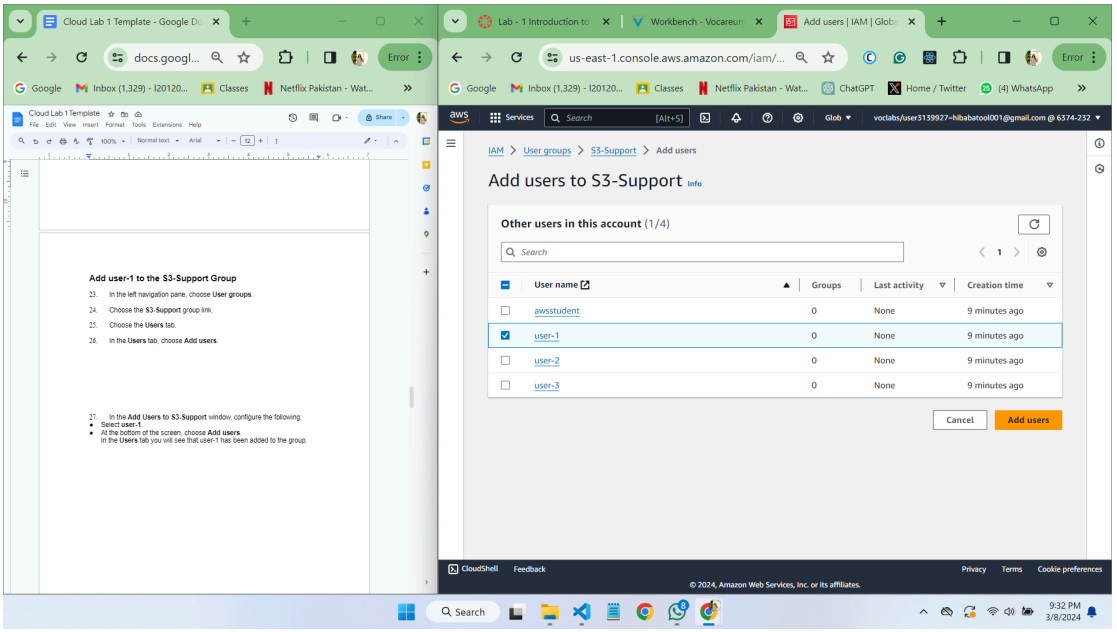
25. Choose the **Users** tab.

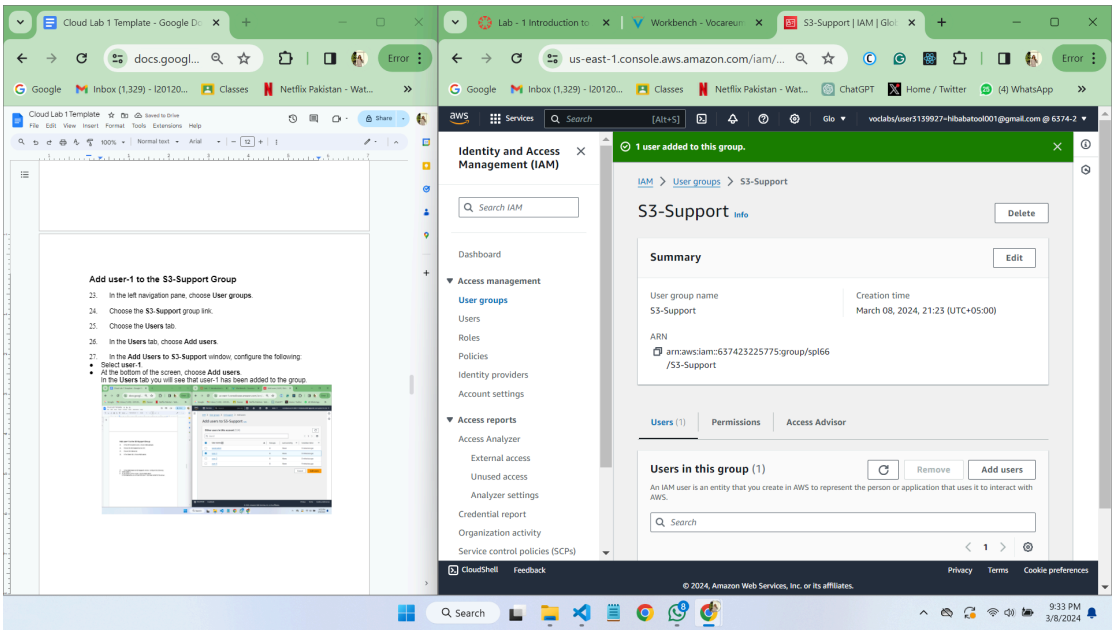
26. In the **Users** tab, choose **Add users**.

27. 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.



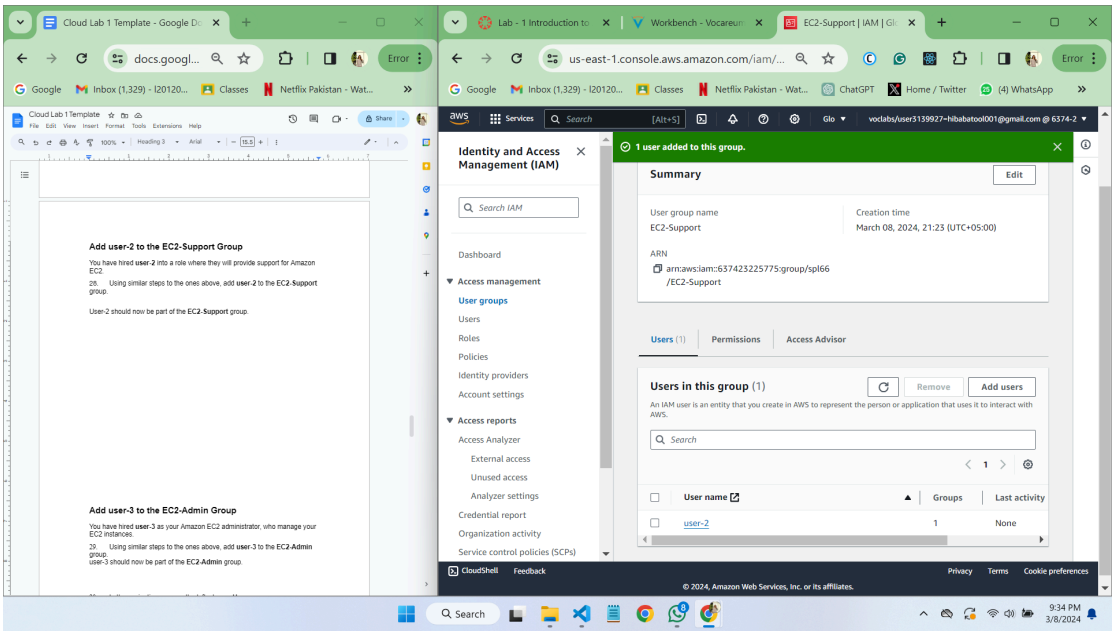


Add user-2 to the EC2-Support Group

You have hired **user-2** into a role where they will provide support for Amazon EC2.

28. Using similar steps to the ones above, add **user-2** to the **EC2-Support** group.

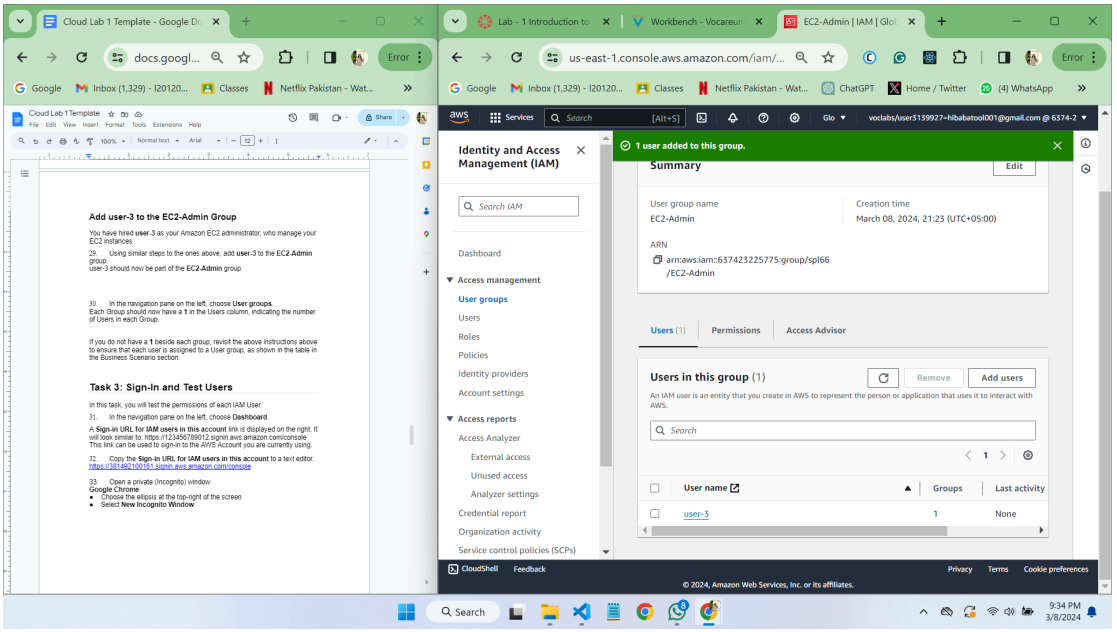
User-2 should now be part of the **EC2-Support** group.



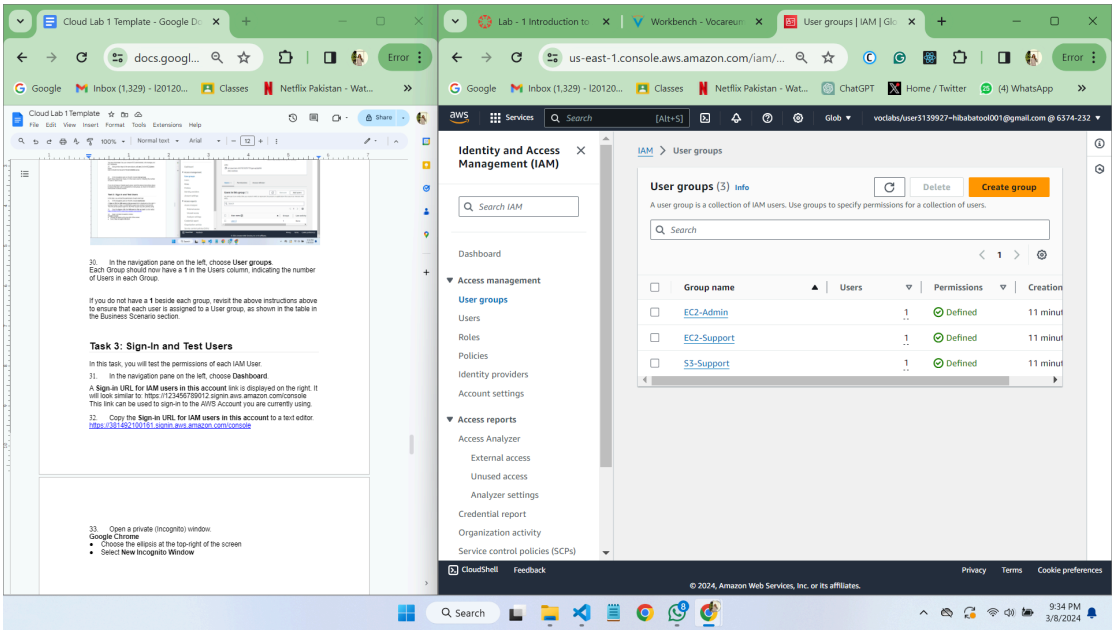
Add user-3 to the EC2-Admin Group

You have hired **user-3** as your Amazon EC2 administrator, who manage your EC2 instances.

29. 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.



30. In the navigation pane on the left, choose **User groups**.
Each Group should now have a **1** in the Users column, indicating the number of Users in each Group.



If you do not have a **1** beside each group, revisit the above instructions above to ensure that each user is assigned to a User group, as shown in the table in the Business Scenario section.

Task 3: Sign-In and Test Users

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

31. 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.

32. Copy the **Sign-in URL for IAM users in this account** to a text editor.

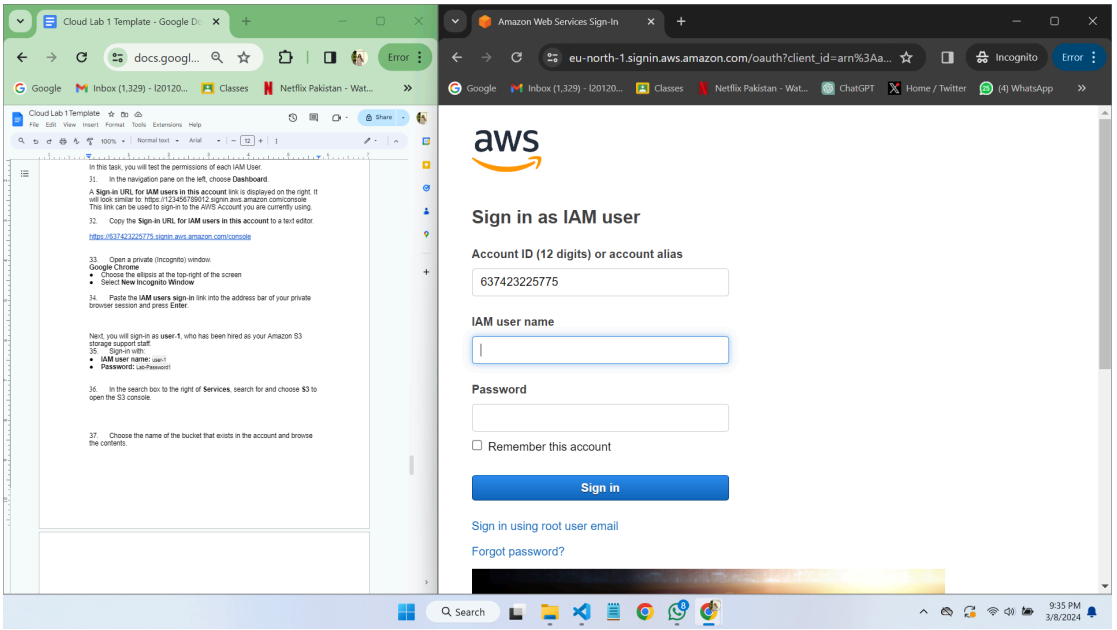
https://637423225775.signin.aws.amazon.com/console

33. Open a private (Incognito) window.

Google Chrome

- Choose the ellipsis at the top-right of the screen
- Select **New Incognito Window**

34. Paste the **IAM users sign-in** link into the address bar of your private browser session and press **Enter**.

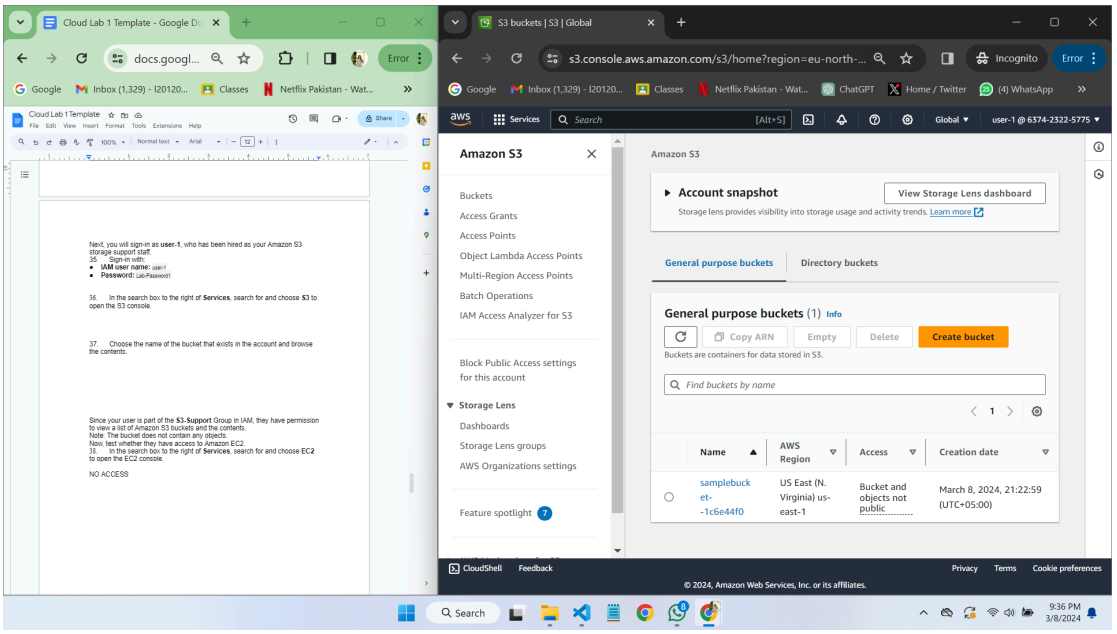


Next, you will sign-in as **user-1**, who has been hired as your Amazon S3 storage support staff.

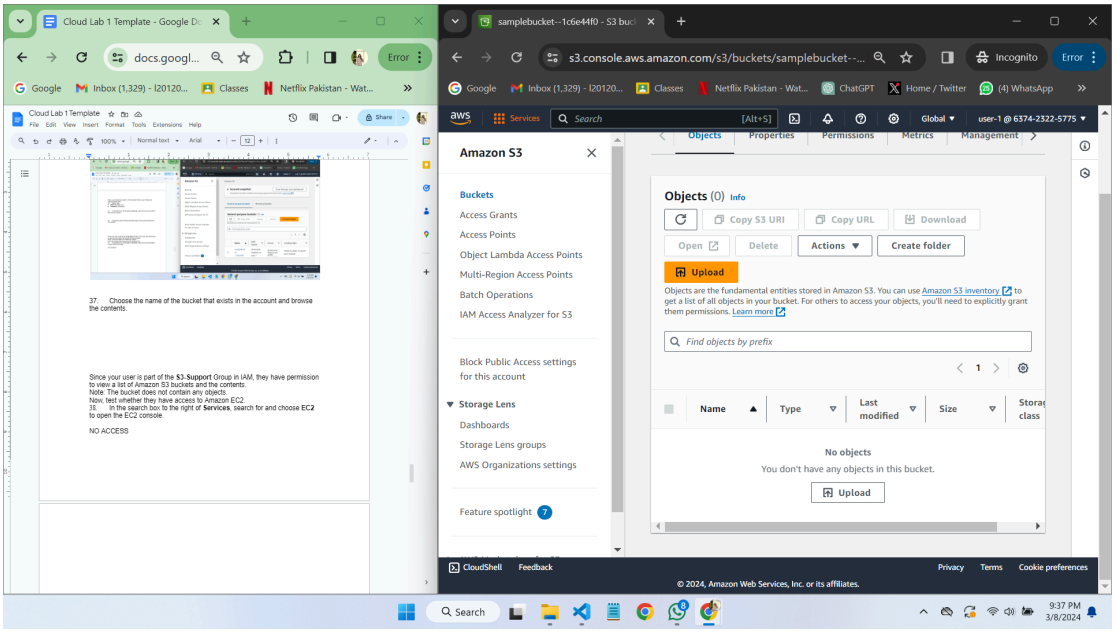
35. Sign-in with:

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

36. In the search box to the right of **Services**, search for and choose **S3** to open the S3 console.

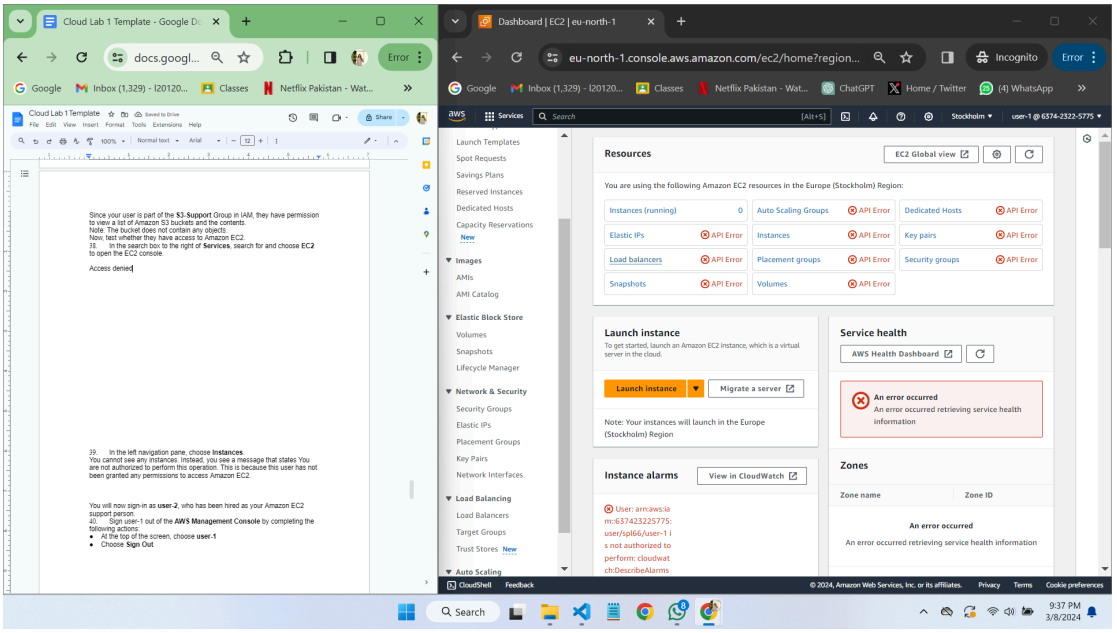


37. Choose the name of the bucket that exists in the account and browse the contents.

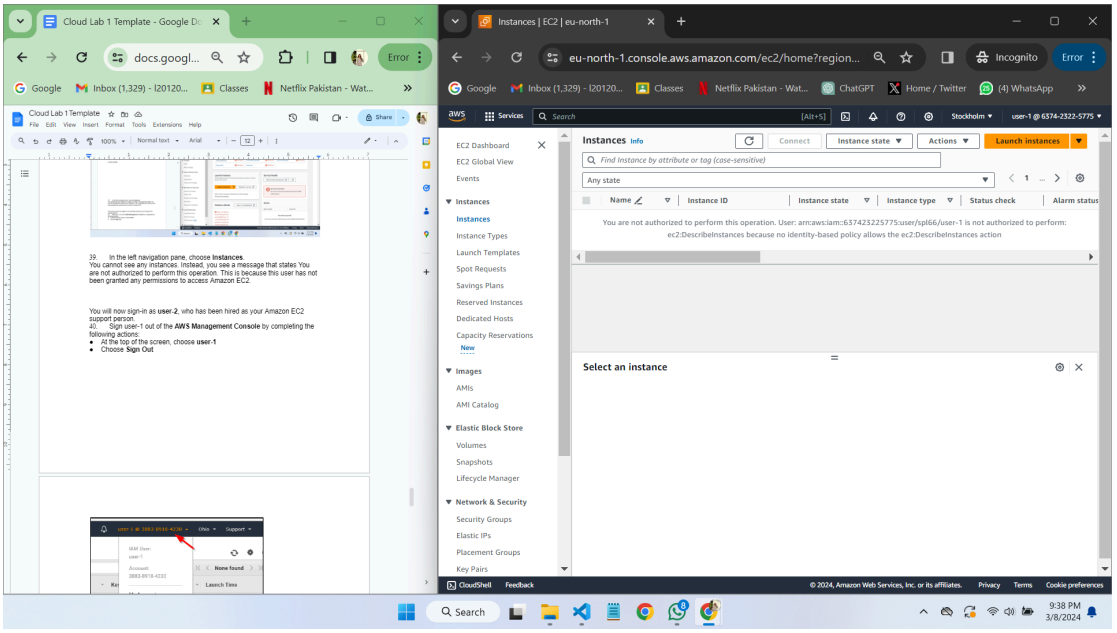


Since your user is part of the **S3-Support** Group in IAM, they have permission to view a list of Amazon S3 buckets and the contents.
Note: The bucket does not contain any objects.
Now, test whether they have access to Amazon EC2.
38. In the search box to the right of **Services**, search for and choose **EC2** to open the EC2 console.

Access denied



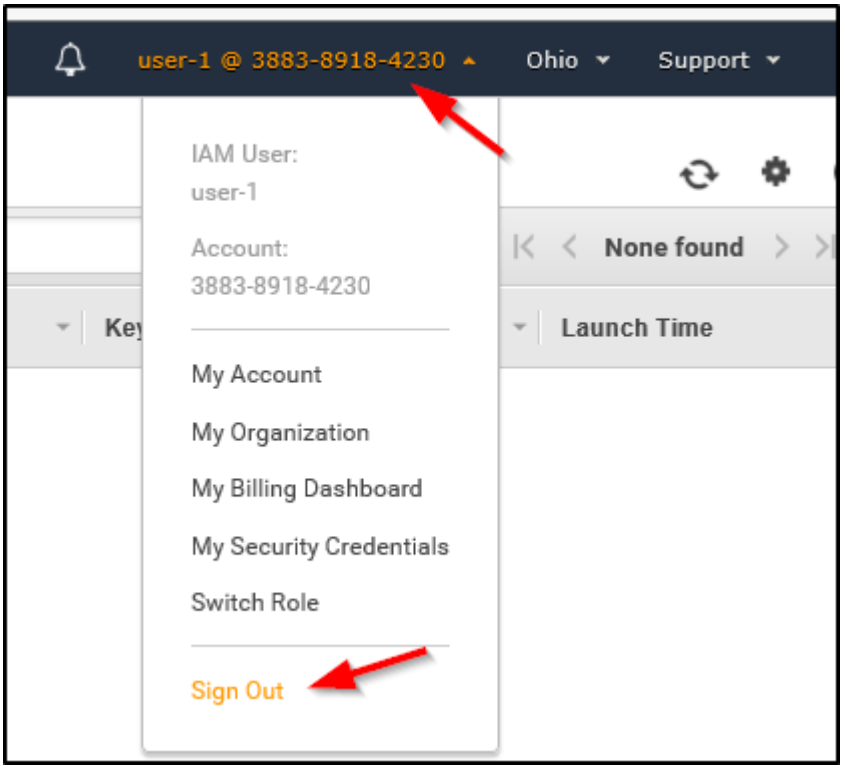
39. In the left navigation pane, choose **Instances**.
You cannot see any instances. Instead, you see a message that states You are not authorized to perform this operation. This is because this user has not been granted any permissions to access Amazon EC2.



You will now sign-in as **user-2**, who has been hired as your Amazon EC2 support person.

40. 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**

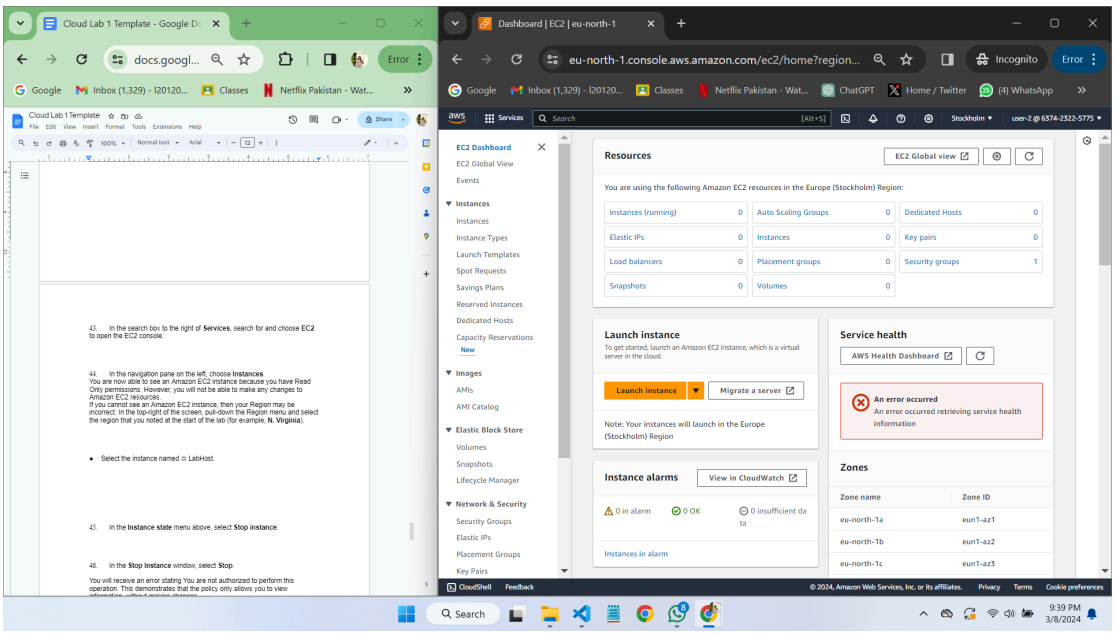


41. Paste the **IAM users sign-in** link into your private browser tab's address bar and press **Enter**.
Note: This link should be in your text editor.

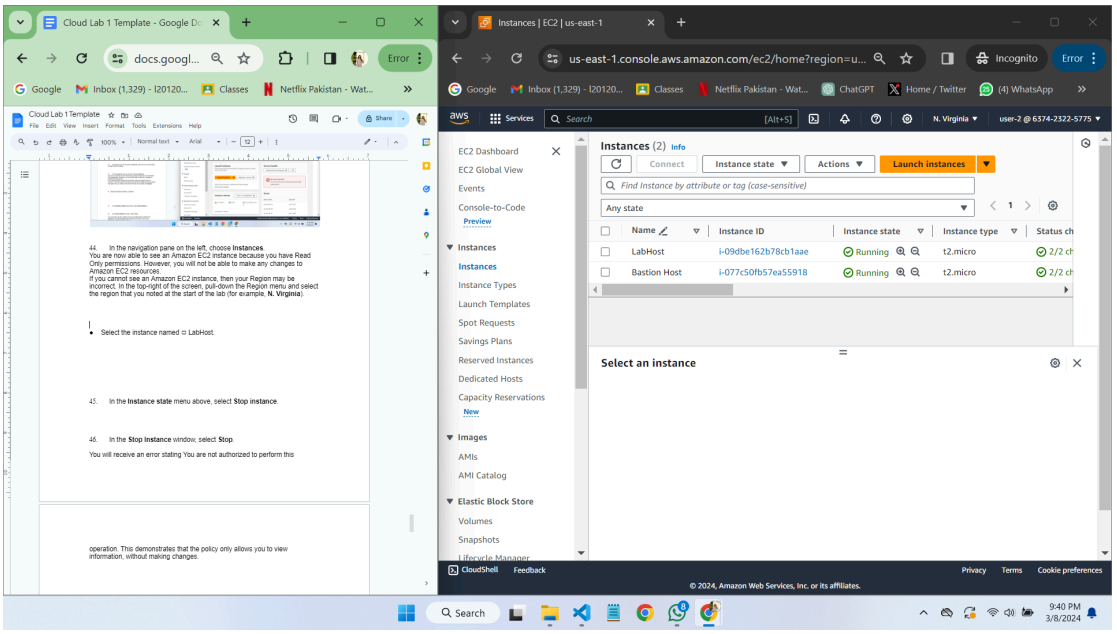
42. Sign-in with:

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

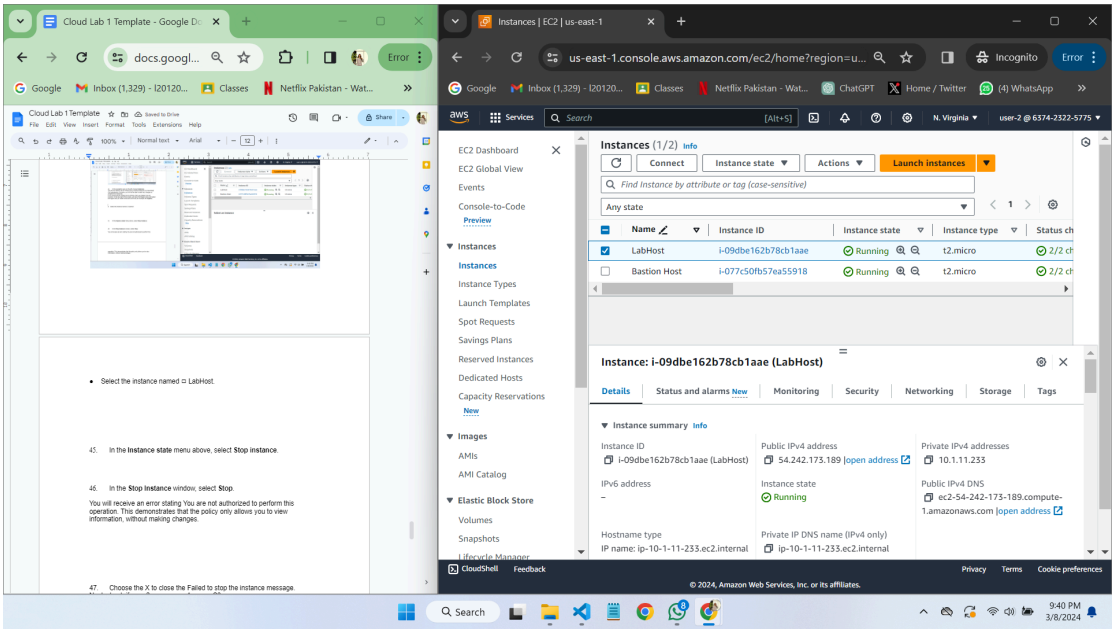
43. In the search box to the right of **Services**, search for and choose **EC2** to open the EC2 console.



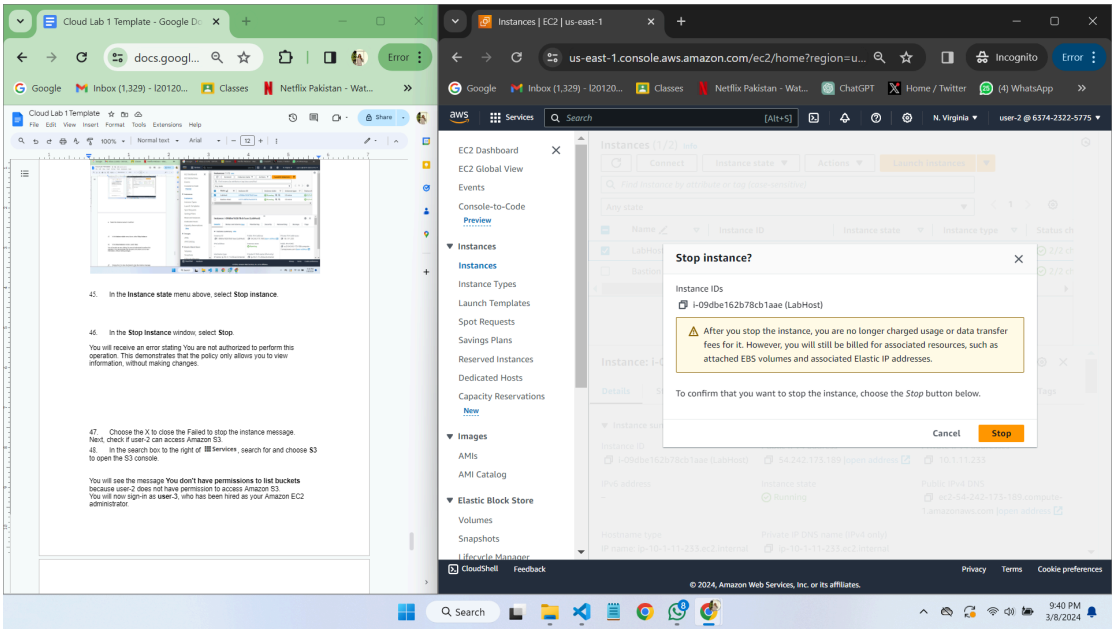
44. In the navigation pane on the left, choose **Instances**.
You are now able to see an Amazon EC2 instance because you have Read Only permissions. However, you will not be able to make any changes to Amazon EC2 resources.
If you cannot see an Amazon EC2 instance, then your Region may be incorrect. In the top-right of the screen, pull-down the Region menu and select the region that you noted at the start of the lab (for example, **N. Virginia**).



- Select the instance named □ LabHost.

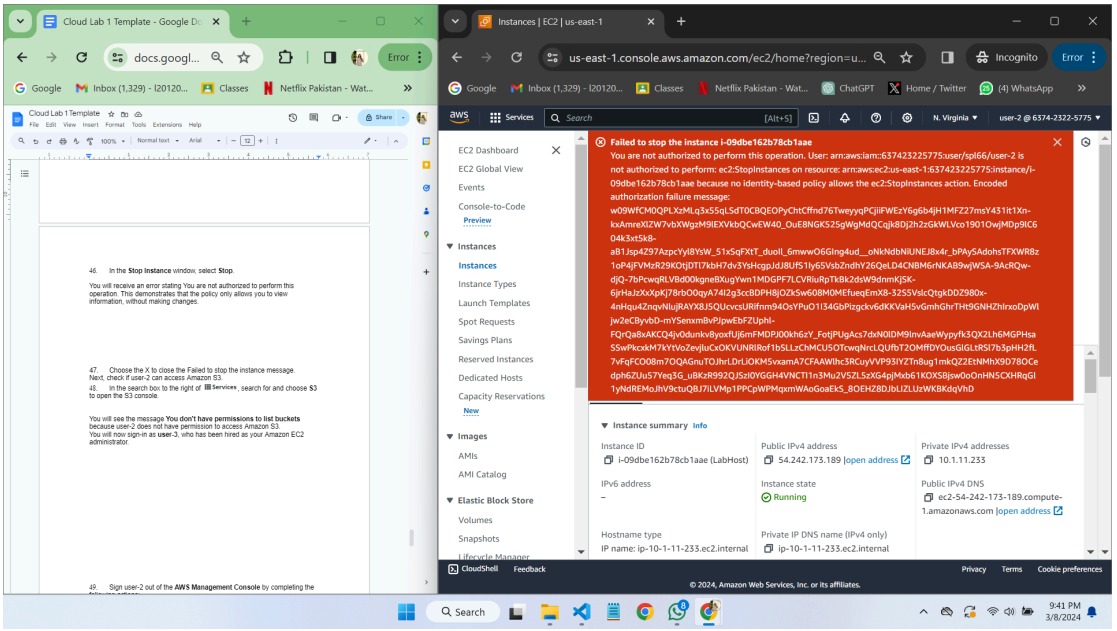


45. In the **Instance state** menu above, select **Stop instance**.

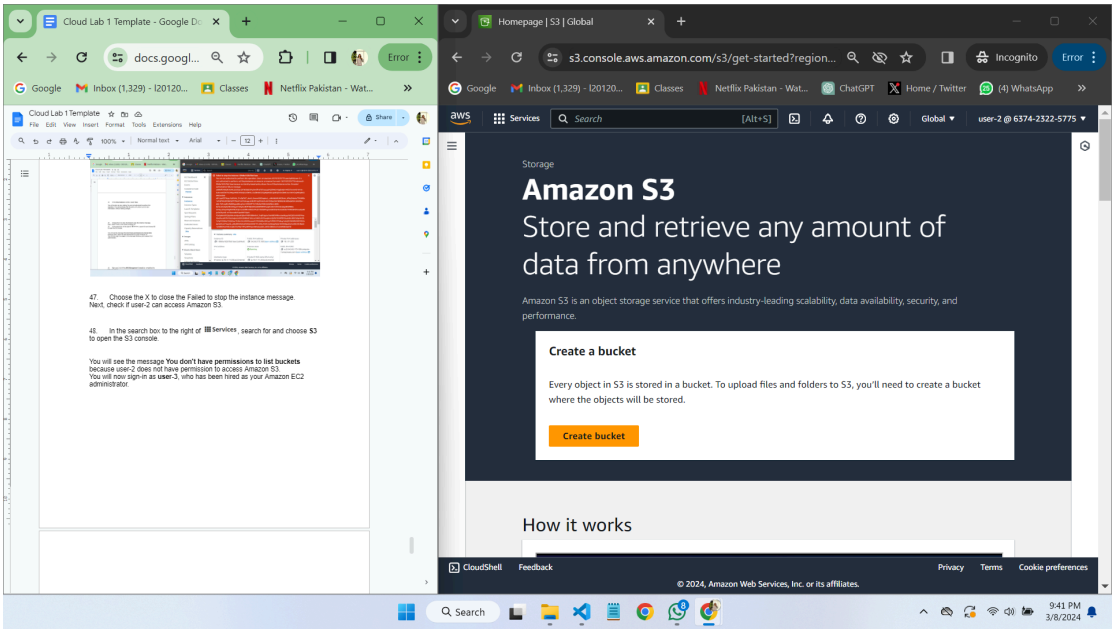


46. In the **Stop Instance** window, select **Stop**.

You will receive an error stating You are not authorized to perform this operation. This demonstrates that the policy only allows you to view information, without making changes.



47. Choose the X to close the Failed to stop the instance message. Next, check if user-2 can access Amazon S3.



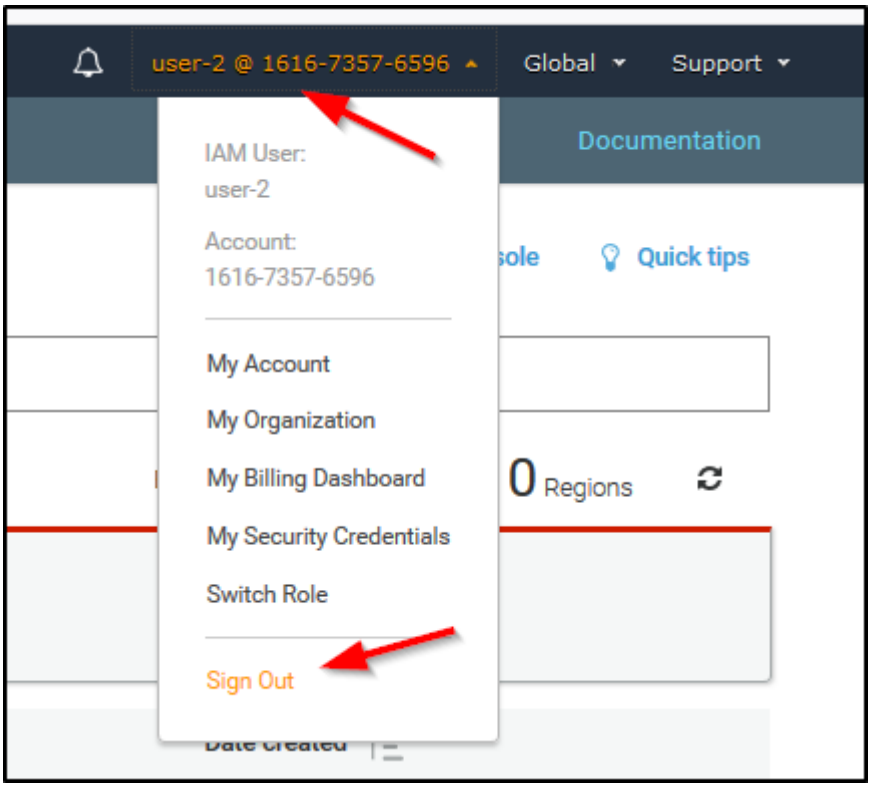
48. In the search box to the right of services, search for and choose **S3** to open the S3 console.

You will see the message **You don't have permissions to list buckets** because user-2 does not have permission to access Amazon S3.
You will now sign-in as **user-3**, who has been hired as your Amazon EC2 administrator.

49. 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**

1.



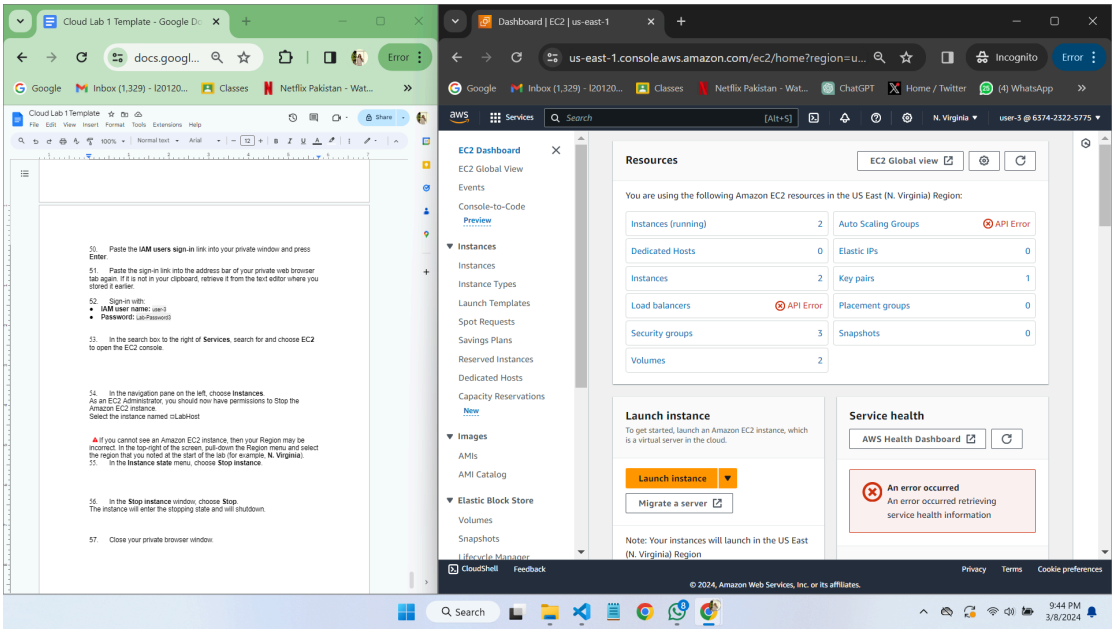
50. Paste the **IAM users sign-in** link into your private window and press **Enter**.

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

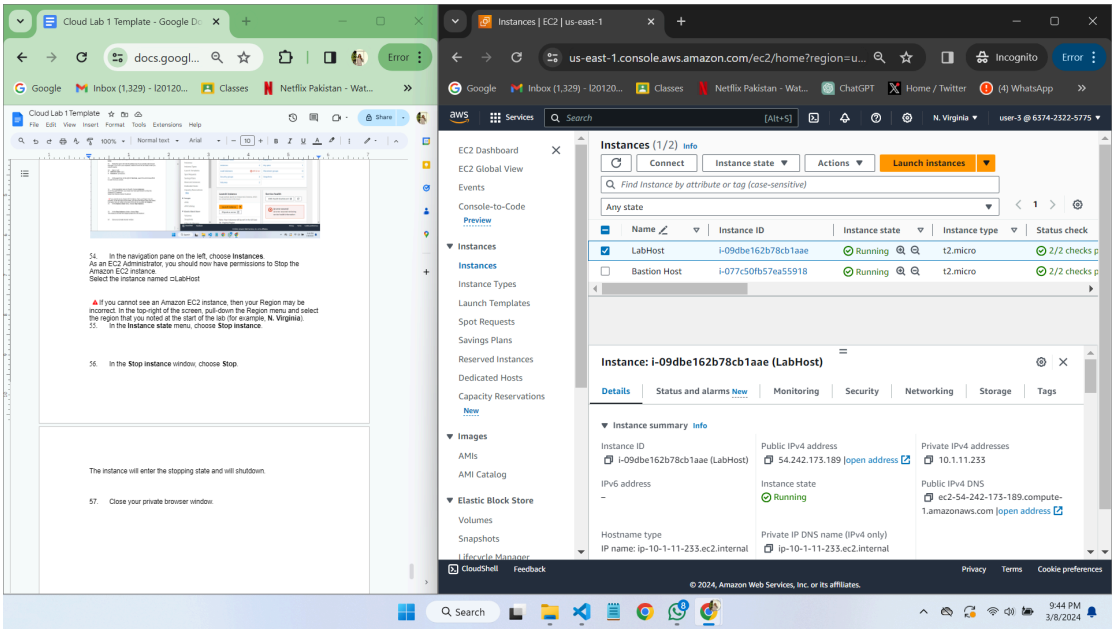
52. Sign-in with:

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

53. In the search box to the right of **Services**, search for and choose **EC2** to open the EC2 console.

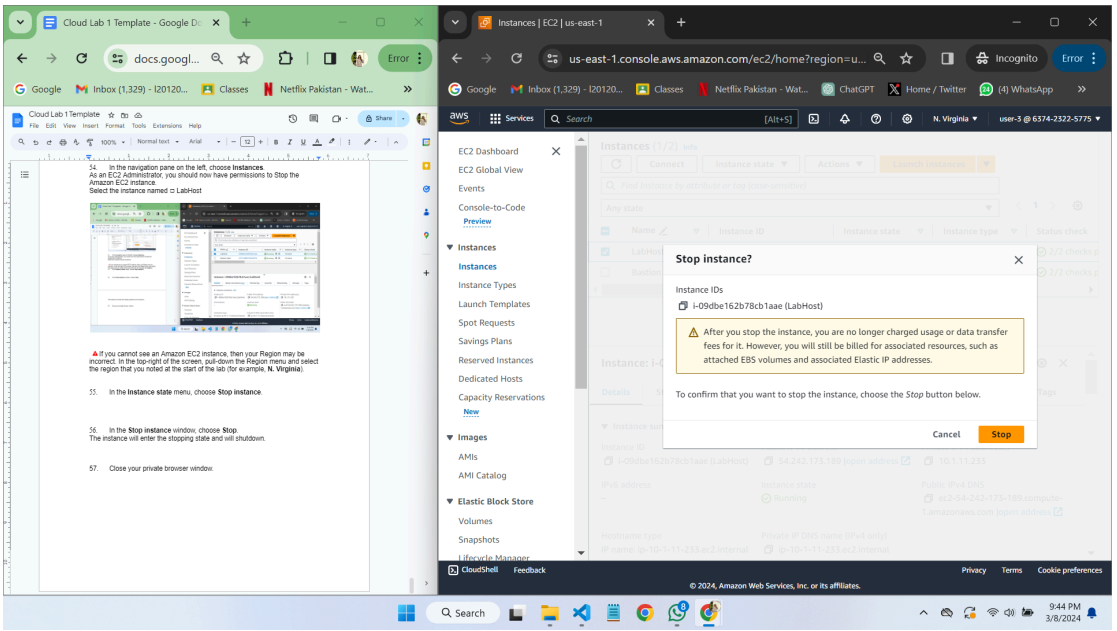


54. In the navigation pane on the left, choose **Instances**.
As an EC2 Administrator, you should now have permissions to Stop the Amazon EC2 instance.
Select the instance named □ LabHost

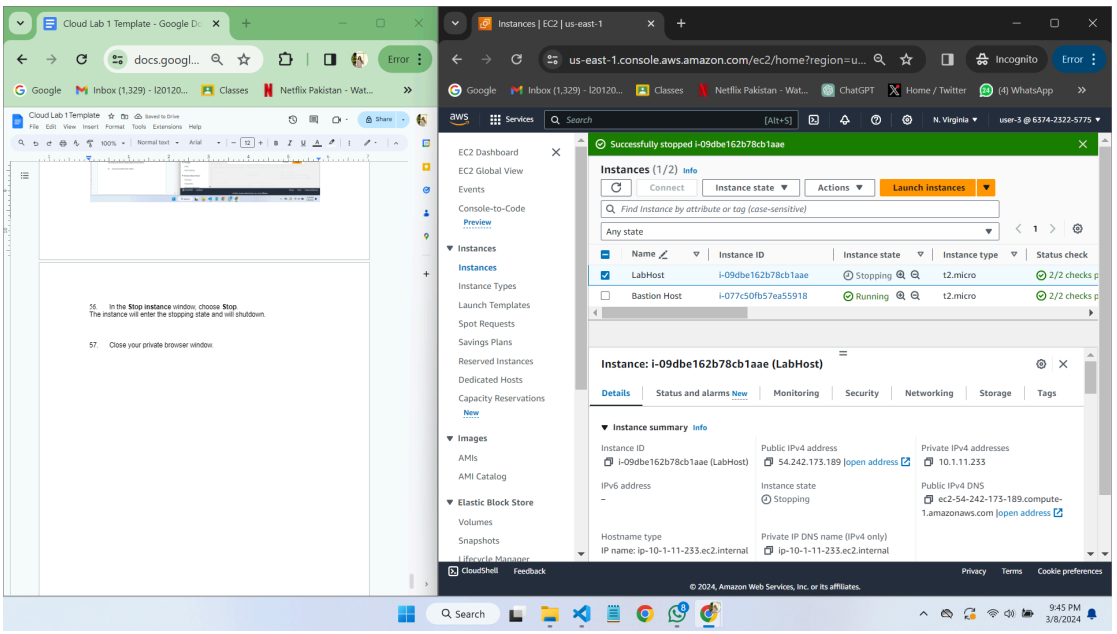


⚠ If you cannot see an Amazon EC2 instance, then your Region may be incorrect. In the top-right of the screen, pull-down the Region menu and select the region that you noted at the start of the lab (for example, **N. Virginia**).

55. In the **Instance state** menu, choose **Stop instance**.



56. In the **Stop instance** window, choose **Stop**.
The instance will enter the stopping state and will shutdown.



57. Close your private browser window.