

# Intro to Cloud Computing

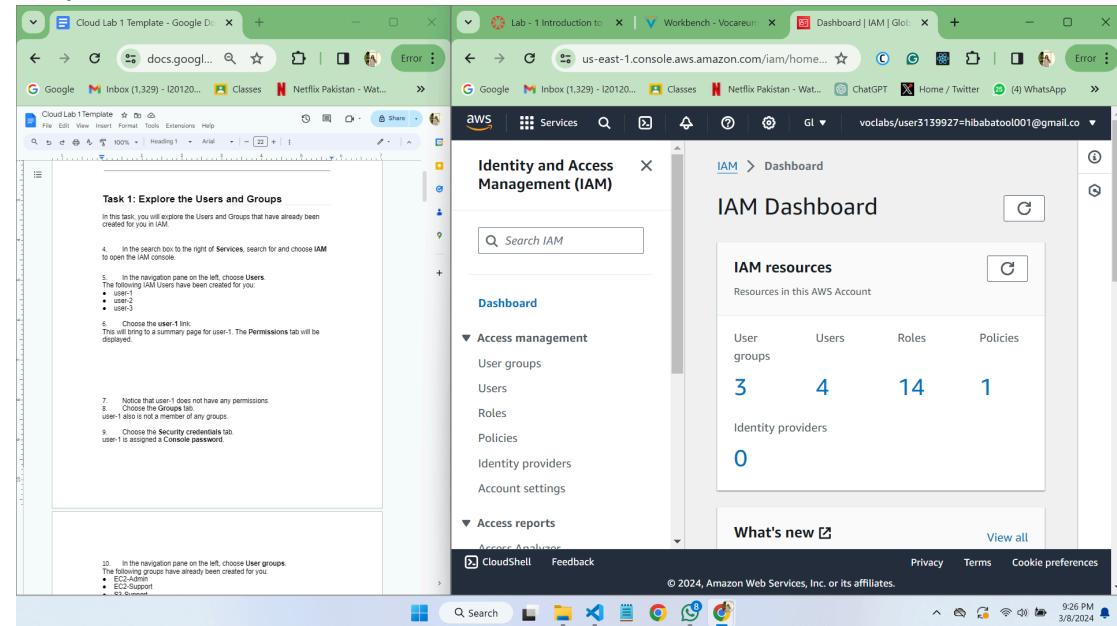
## Lab - 1 Introduction to AWS IAM

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

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

Notice that user-1 does not have any permissions.  
Choose the Groups tab.  
user-1 also is not a member of any groups.  
Choose the Security credentials tab.  
user-1 is assigned a Console password.

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

- EC2-Support
- EC2-Support
- EC2-Support

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

Choose the Permissions tab.

**Identity and Access Management (IAM)**

**Users (4) Info**

User name	Path
awsstudent	/
user-1	/spl66/
user-2	/spl66/
user-3	/spl66/

© 2024, Amazon Web Services, Inc. or its affiliates.

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

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

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 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.  
Choose the Groups tab.  
user-1 also is not a member of any groups.

**Identity and Access Management (IAM)**

**user-1 Info**

**Summary**

ARN	arn:aws:iam::637423225775:user/spl66/user-1
Access key 1	AKIAZI2LRCRX7PSNTEWI - Active
Last console sign-in	Never
Created	March 08, 2024, 21:22 (UTC+05:00)
Access key 2	Create access key

**Permissions** | Groups | Tags (1) | Security credentials | Access Advisor

**Permissions policies (0)**

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

Filter by Type

© 2024, Amazon Web Services, Inc. or its affiliates.

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.

The screenshot displays two browser windows side-by-side. The left window is a Google Doc titled 'Cloud Lab 1 Template' containing the following steps:

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 by AWS that define what actions are allowed or denied for specific AWS resources. This policy is granting permission to List and Describe information about EC2 Instances, Volumes, Snapshots, and Networks. It is also allowing users to attach policies to other AWS resources, but not modify them, is ideal for assigning to a Support role. This policy does not grant any permissions to CloudWatch Metrics.
  - Effect says whether to Allow or Deny the permissions.
  - AmazonEC2ReadOnlyAccess is the policy that can be made against an AWS Service (eg cloudwatchMetrics).
- Bookmarks (1) Define the scope of entities covered by the policy rule (a)

The right window is the AWS Identity and Access Management (IAM) service, specifically the 'Groups' tab for the user 'user-1'. The 'User groups membership (0)' section shows 'No resources'. The 'Console access' section indicates 'Enabled without MFA'.

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

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

The screenshot displays two browser windows side-by-side. The left window is a Google Doc titled 'Cloud Lab 1 Template' containing the following steps:

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**.

The right window is the AWS Identity and Access Management (IAM) service, specifically the 'Security credentials' tab for the user 'user-1'. The 'Console sign-in' section shows a single entry for 'Console sign-in link' with the URL <https://65742525775.sigin.aws.amazon.com/console> and a 'Console password' updated 4 minutes ago (2024-03-08 21:23 GMT+5). The 'Multi-factor authentication (MFA)' section is empty.

**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

The screenshot shows a dual-monitor setup. The left monitor displays a Google Docs document titled "Cloud Lab 1 Template". The right monitor displays the AWS Identity and Access Management (IAM) console, specifically the "User groups" page. The IAM page lists three user groups: EC2-Admin, EC2-Support, and S3-Support, each with 0 users and defined permissions, all created 5 minutes ago. The navigation pane on the left of the IAM console shows "User groups" is selected under "Access management".

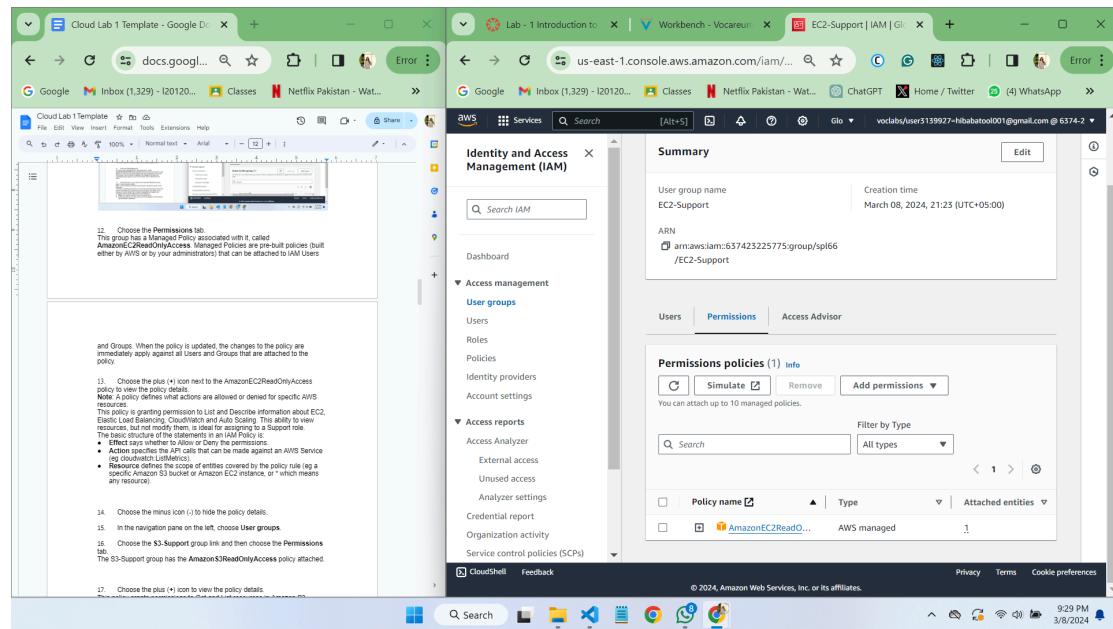
**11. Choose the **EC2-Support** group link.**

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

The screenshot shows a dual-monitor setup. The left monitor displays the same Google Docs document as before. The right monitor displays the AWS IAM console, specifically the summary page for the EC2-Support user group. The summary page shows the group name is EC2-Support, it was created on March 08, 2024, at 21:23 (UTC+05:00), and its ARN is arn:aws:iam::657423225775:group/spl66/EC2-Support. The "Users" tab is selected, showing 0 users in this group. The "Permissions" tab is also visible. The navigation pane on the left of the IAM console shows "User groups" is selected under "Access management".

## 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).

The screenshot shows a dual-monitor setup. The left monitor displays a Google Doc titled "Cloud Lab 1 Template - Google Docs" with the following content:

```

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.

```

The right monitor displays the AWS Management Console, specifically the Identity and Access Management (IAM) service. The "AmazonEC2ReadOnlyAccess" policy is selected. The JSON code for the policy is shown below:

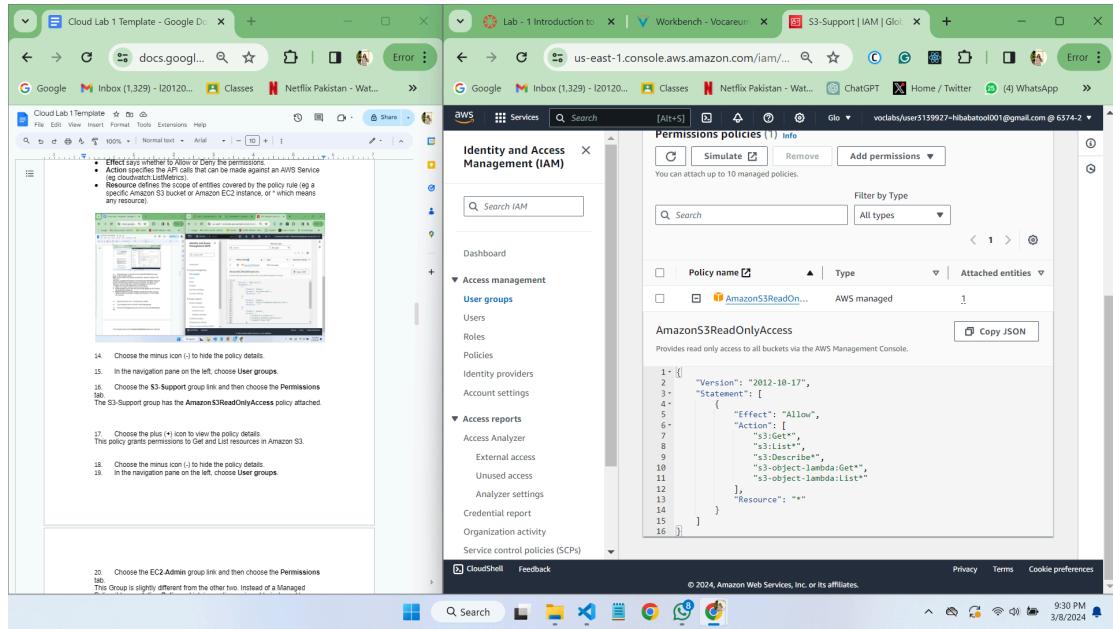
```

1+ {
  2   "Version": "2012-10-17",
  3   "Statement": [
  4     {
  5       "Effect": "Allow",
  6       "Action": "ec2:Describe",
  7       "Resource": "*"
  8     },
  9     {
  10      "Effect": "Allow",
  11      "Action": "elasticloadbalancing:Describe",
  12      "Resource": "*"
  13    },
  14    {
  15      "Effect": "Allow",
  16      "Action": [
  17        "cloudwatch:ListMetrics",
  18        "cloudwatch:GetMetricStatistics",
  19        "cloudwatch:Describe"
  20      ],
  21    }
  22  ]
}

```

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.

The screenshot shows a dual-monitor setup. The left monitor displays a Google Docs document titled "Cloud Lab 1 Template - Google Docs" containing step-by-step instructions for navigating the AWS IAM console. The right monitor displays the AWS Identity and Access Management (IAM) service. In the left sidebar, under "Access management", "User groups" is selected, showing the "EC2-Admin" group. The main content area shows the "Permissions policies (1) info" section for the "EC2-Admin-Policy". Below the table, the JSON code for the policy is displayed:

```

1+ [{
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Action": [
6-         "ec2:Describe",
7-         "ec2:StartInstances",
8-         "ec2:StopInstances"
9-       ],
10-      "Resource": [
11-        "*"
12-      ],
13-      "Effect": "Allow"
14-    }
15-  ]
16-]

```

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

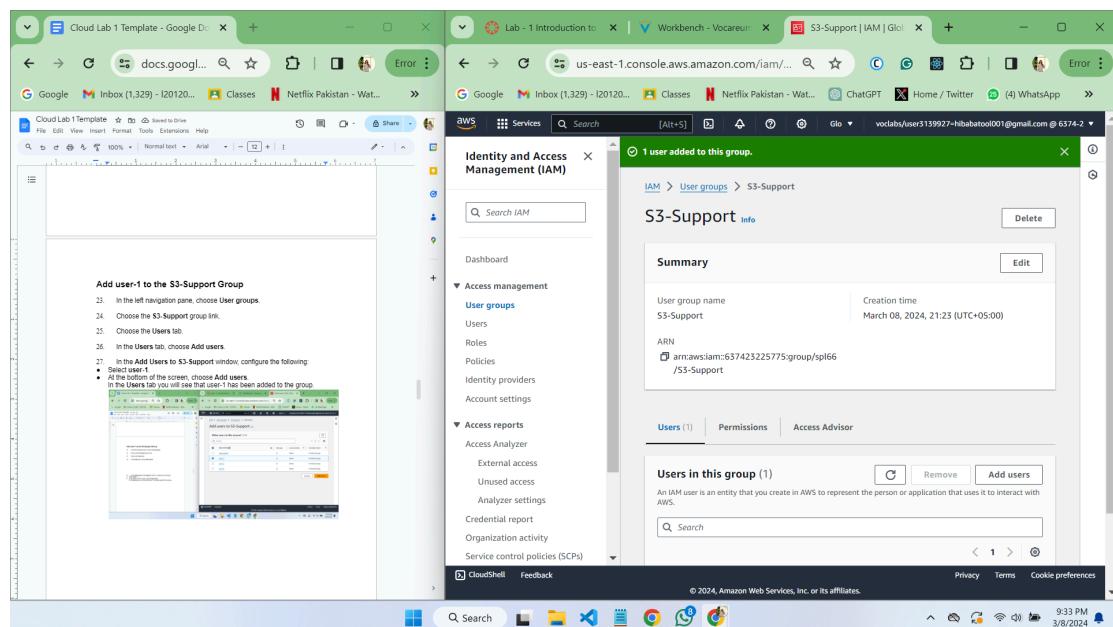
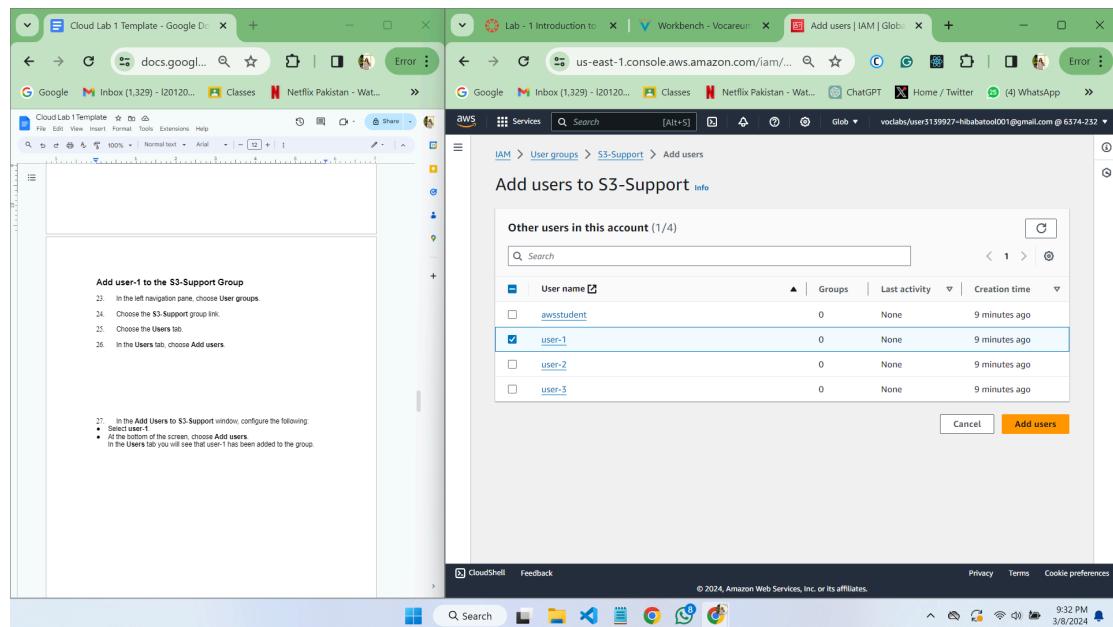
---

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.

The screenshot shows a dual-monitor setup. The left monitor displays a Google Docs document titled "Cloud Lab 1 Template - Google Docs". It contains two sections: "Add user-2 to the EC2-Support Group" and "Add user-3 to the EC2-Admin Group". Both sections instruct the user to hire the respective user into a role for managing EC2 instances. The right monitor displays the AWS Identity and Access Management (IAM) console at <https://us-east-1.console.aws.amazon.com/iam/>. A modal window titled "1 user added to this group." is open, showing a summary of the addition. The user group name is "EC2-Support" and the ARN is "arn:aws:iam::657423225775:group/spl66/EC2-Support". The "Users" tab is selected, showing a table with one row for "user-2". The table includes columns for User name, Groups, and Last activity. The status for "user-2" is "None". The bottom right corner of the screen shows the Windows taskbar with various pinned icons and the system clock indicating 9:34 PM on 3/8/2024.

# 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.

The screenshot shows a dual-monitor setup. The left monitor displays a Google Docs document titled "Cloud Lab 1 Template - Google Docs" with instructions for adding a user to the EC2-Admin group. The right monitor displays the AWS Cloud Console, specifically the IAM service. A modal window titled "1 user added to this group." is open, showing the "Summary" tab for the "EC2-Admin" user group. It lists one user, "user-3", under "Users in this group". The ARN of the group is also displayed as `arn:aws:iam::657423225775:group/spl66`.

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.

The screenshot shows a dual-monitor setup. The left monitor displays a Google Docs document titled "Cloud Lab 1 Template - Google Docs" with instructions for adding a user to the EC2-Admin group. The right monitor displays the AWS Cloud Console, specifically the IAM service. A modal window titled "User groups (3) info" is open, showing the "User groups" table. It lists three groups: "EC2-Admin", "EC2-Support", and "S3-Support", each with one user assigned. The table includes columns for "Group name", "Users", "Permissions", and "Creation". All groups have "Defined" permissions and were created 11 minutes ago.

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.

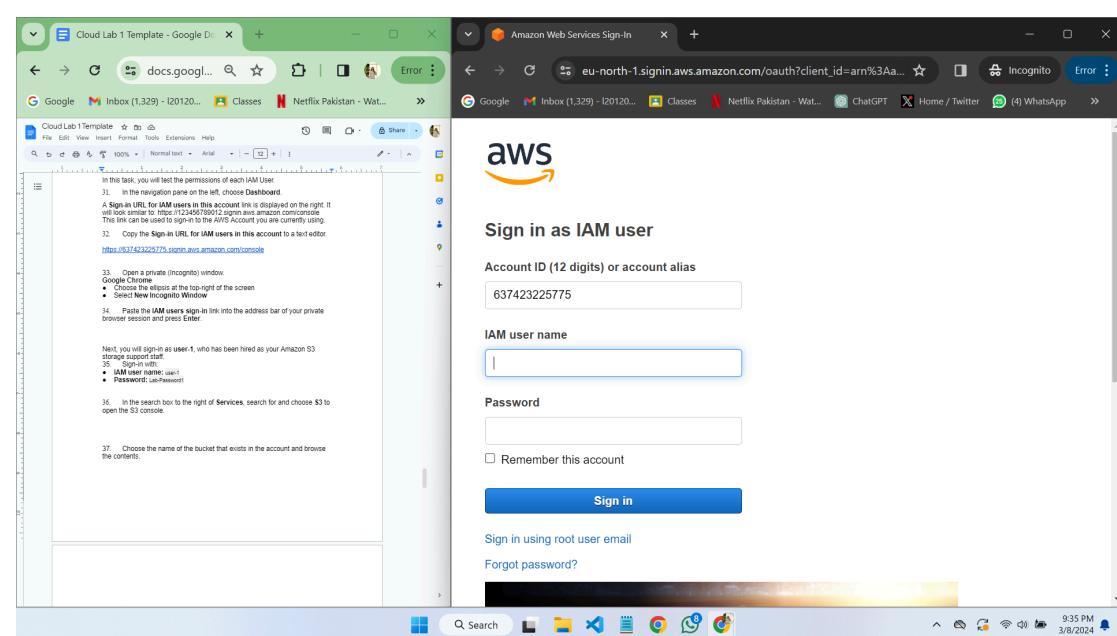
<https://637423225775.signin.aws.amazon.com/console>

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**.

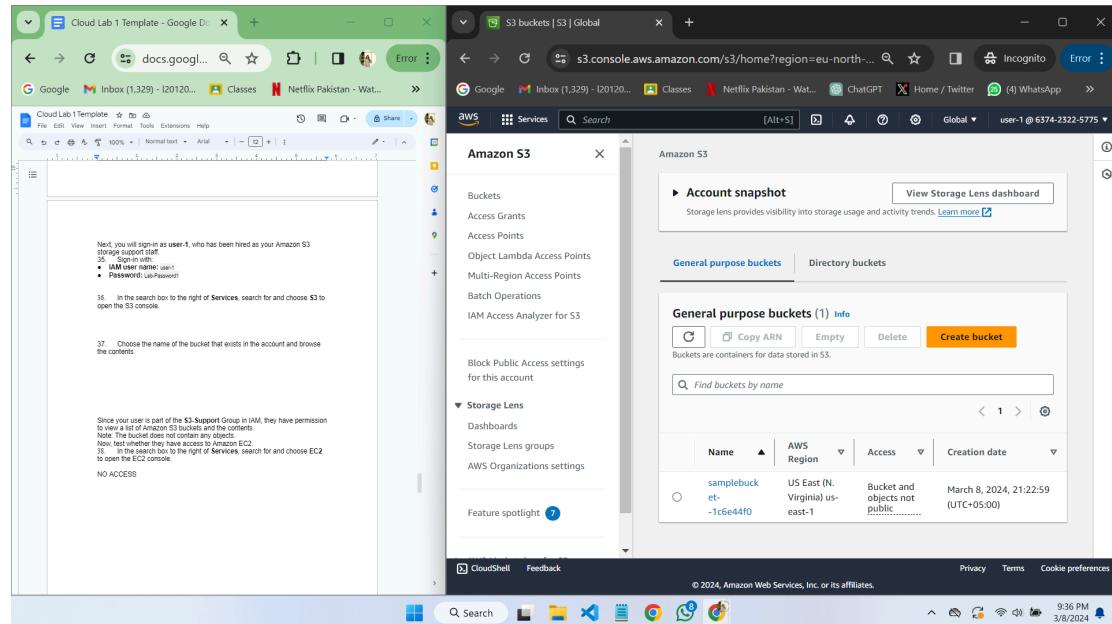


Next, you will sign-in as **user-1**, who has been hired as your Amazon S3 storage support staff.

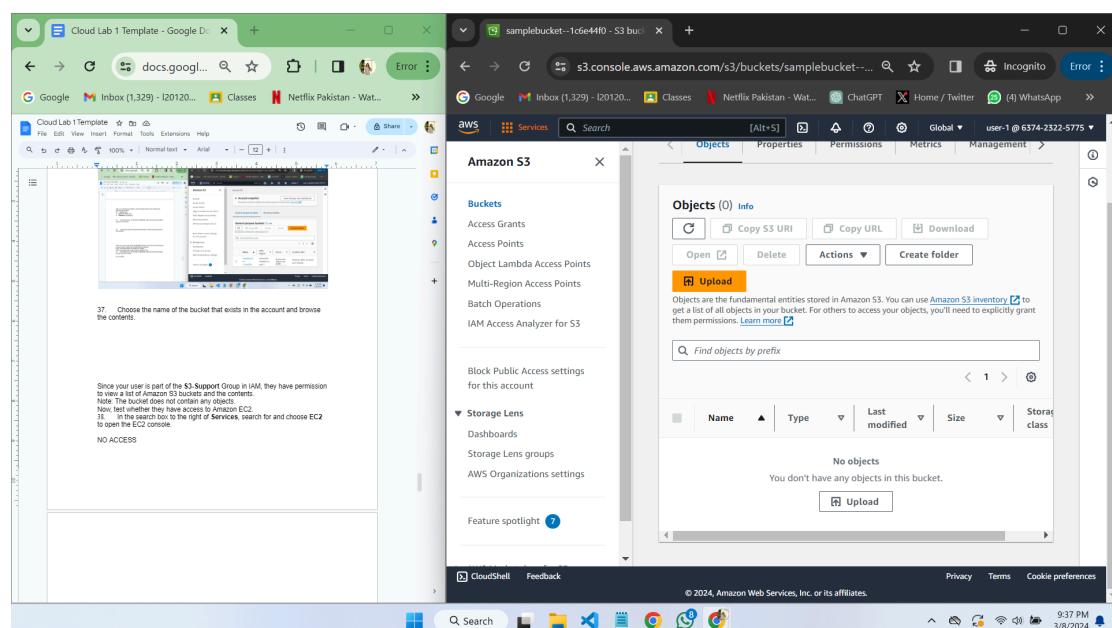
35. Sign-in with:

- **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

The screenshot displays two browser windows. The left window is a Google Docs document titled 'Cloud Lab 1 Template'. It contains instructions for testing EC2 access, mentioning the 'S3-Support' group and providing steps to sign in as user-2 and complete the AWS Management Console setup. The right window is the AWS EC2 Dashboard. The navigation pane on the left shows various services like Launch Templates, Spot Requests, and Instances. The main content area displays an 'Access denied' message: 'You are using the following Amazon EC2 resources in the Europe (Stockholm) Region: Instances (running) 0 Auto Scaling Groups 0 API Error Dedicated Hosts 0 API Error Elastic IPs 0 API Error Instances 0 API Error Key pairs 0 API Error Load balancers 0 API Error Placement groups 0 API Error Security groups 0 API Error Snapshots 0 API Error Volumes 0 API Error'. Below this, there's a 'Launch instance' button and a 'Service health' section with an error message: 'An error occurred An error occurred retrieving service health information'. The bottom of the dashboard shows the AWS footer with copyright information and links.

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

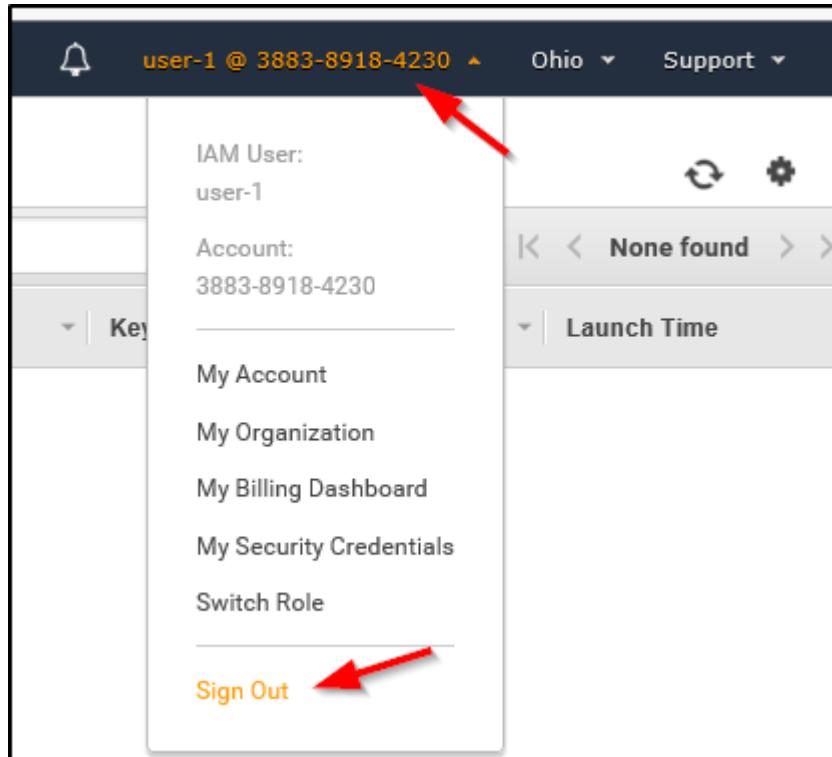
You cannot see any instances. Instead, you see a message that states You are not authorized to perform this operation. This is because this user has not been granted any permissions to access Amazon EC2.

The screenshot displays two browser windows. The left window is a Google Docs document titled 'Cloud Lab 1 Template'. It contains instructions for testing EC2 access, mentioning the 'S3-Support' group and providing steps to sign in as user-2 and complete the AWS Management Console setup. The right window is the AWS EC2 Instances page. The navigation pane on the left shows various services like EC2 Dashboard, Events, Instances, and Auto Scaling. The main content area displays an 'Access denied' message: 'You are not authorized to perform this operation. User: arn:aws:iam::637423225775:user:sp166/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action'. A modal dialog box titled 'Select an instance' is visible at the bottom. The bottom of the dashboard shows the AWS footer with copyright information and links.

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**



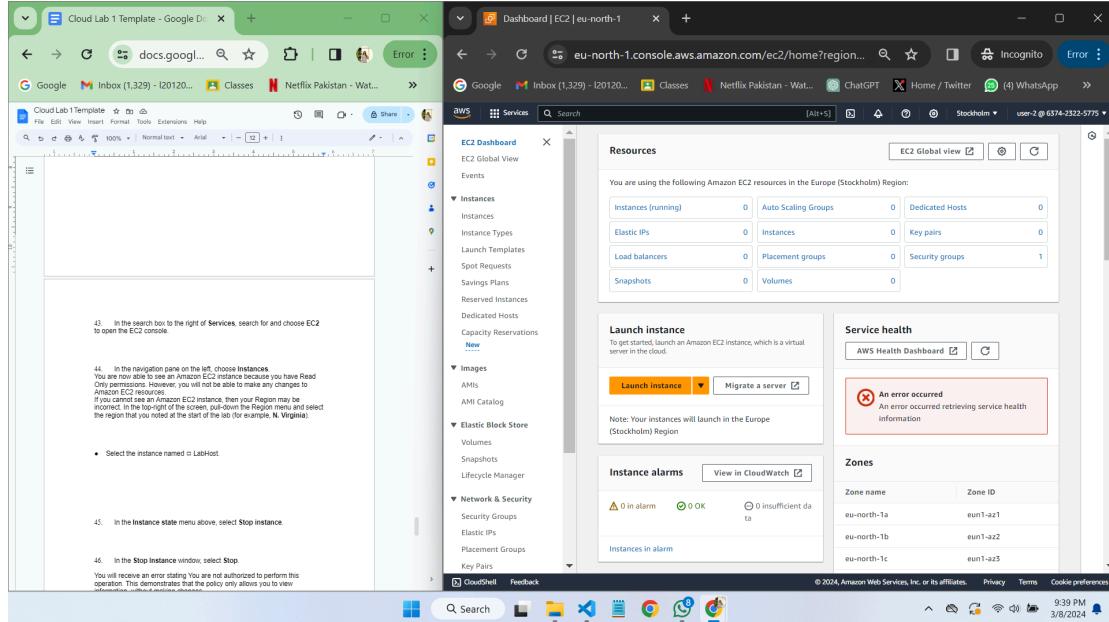
41. Paste the **IAM users sign-in** link into your private browser tab's address bar and press **Enter**.

Note: This link should be in your text editor.

42. Sign-in with:

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

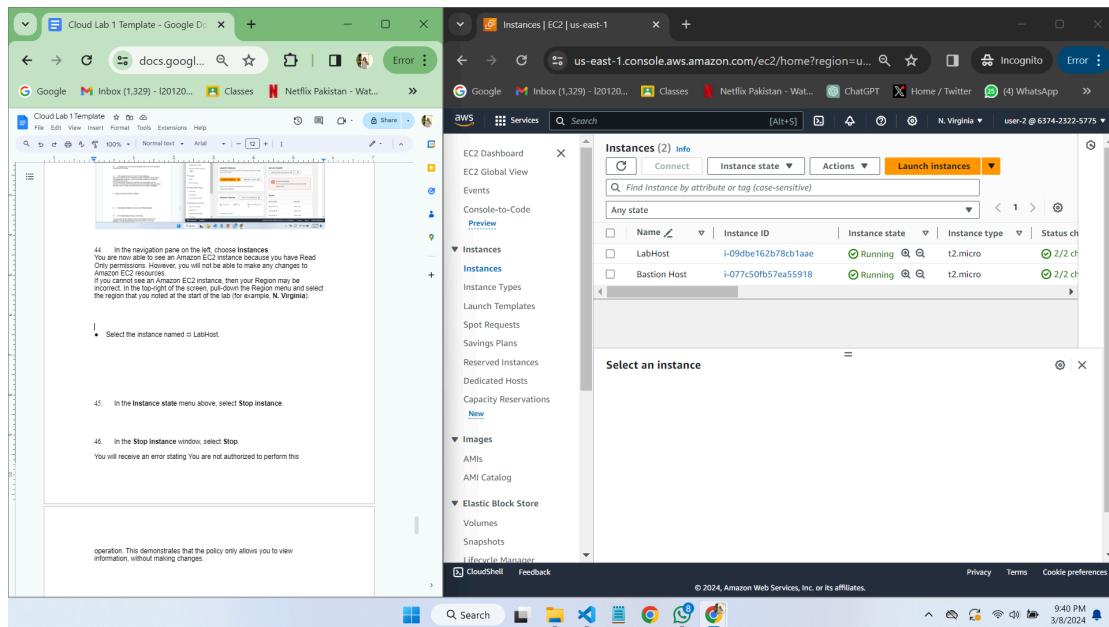
43. In the search box to the right of **Services**, search for and choose **EC2** to open the EC2 console.



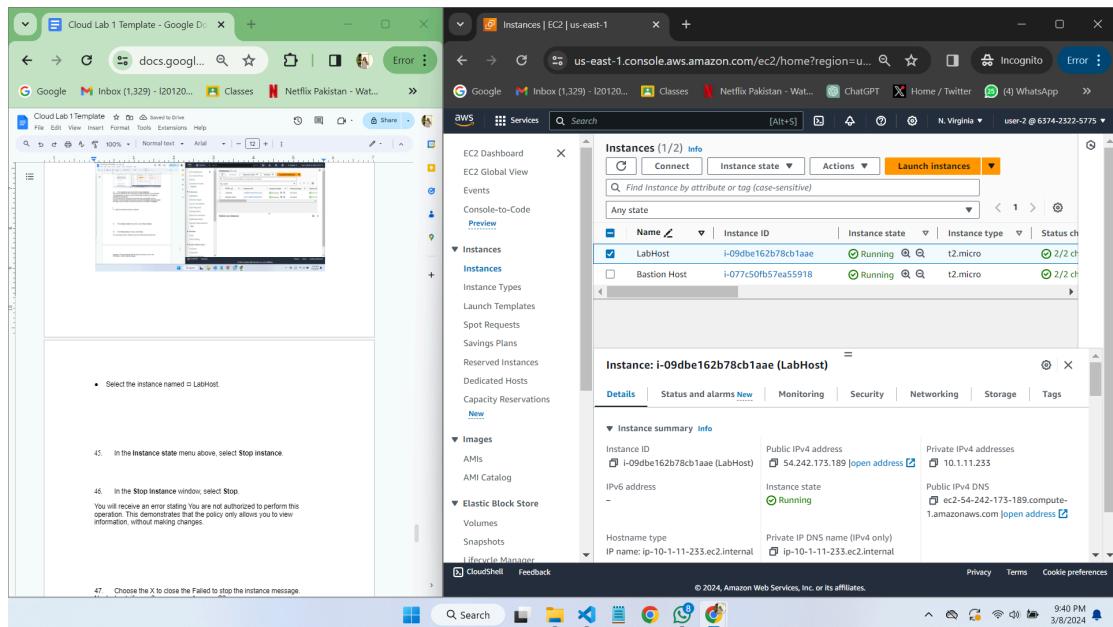
44. In the navigation pane on the left, choose **Instances**.

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.

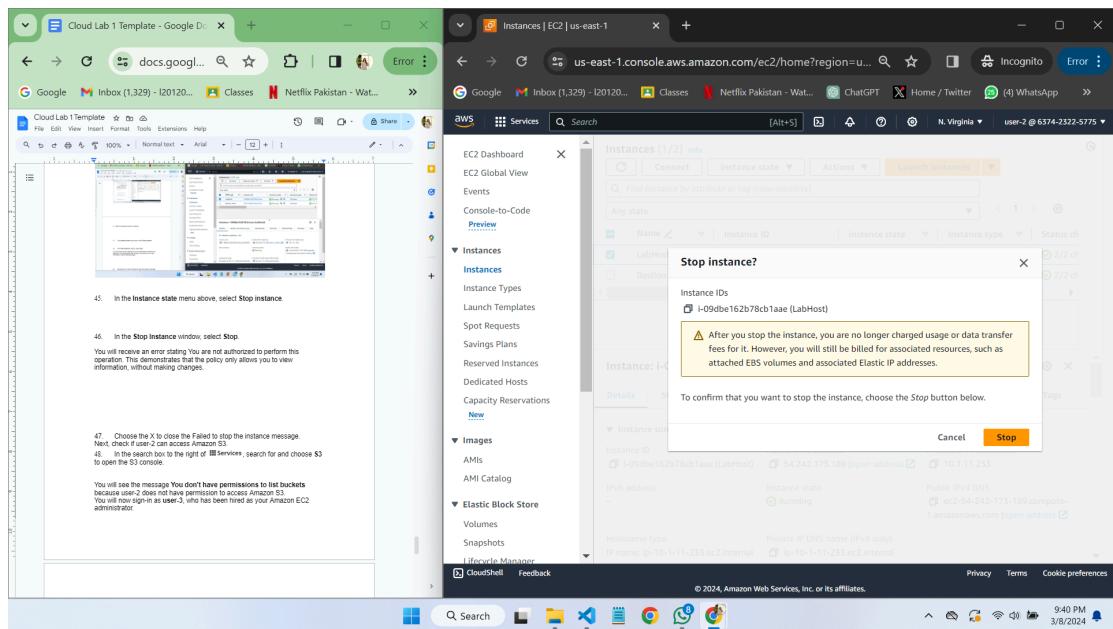
If you cannot see an Amazon EC2 instance, then your Region may be incorrect. In the top-right of the screen, pull-down the Region menu and select the region that you noted at the start of the lab (for example, N. Virginia).



- Select the instance named  LabHost.

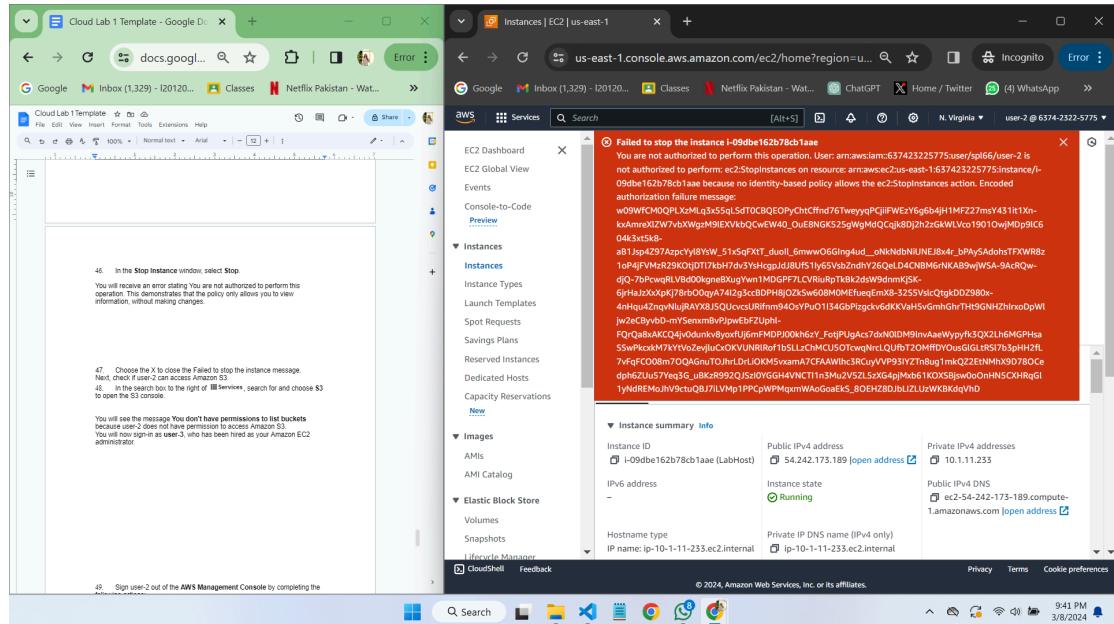


**45. In the Instance state menu above, select Stop instance.**

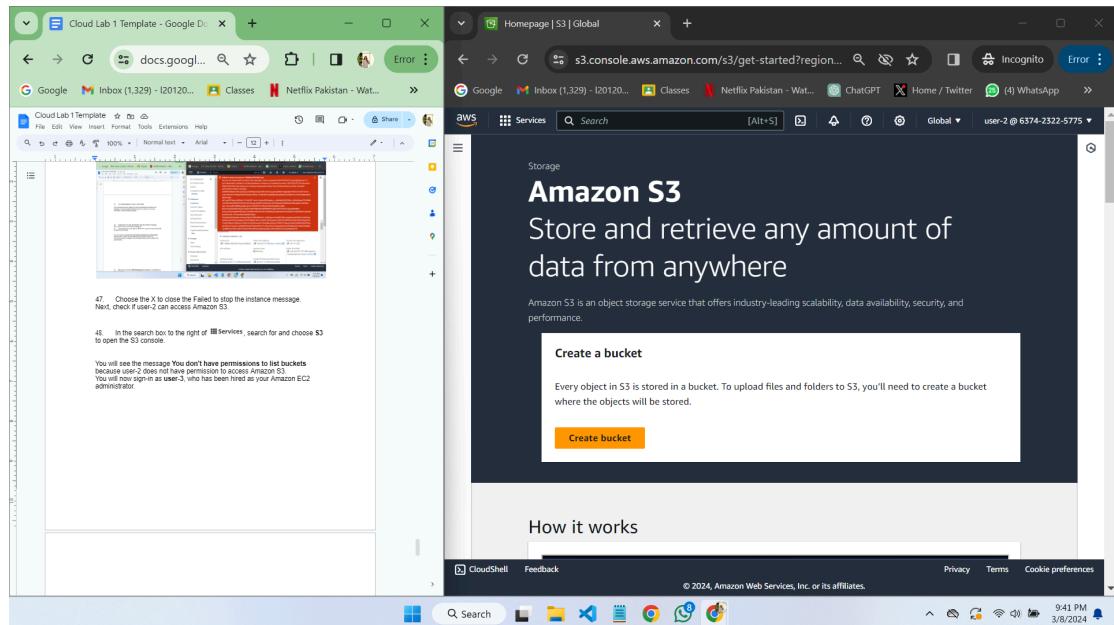


## 46. In the Stop Instance window, select Stop.

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.

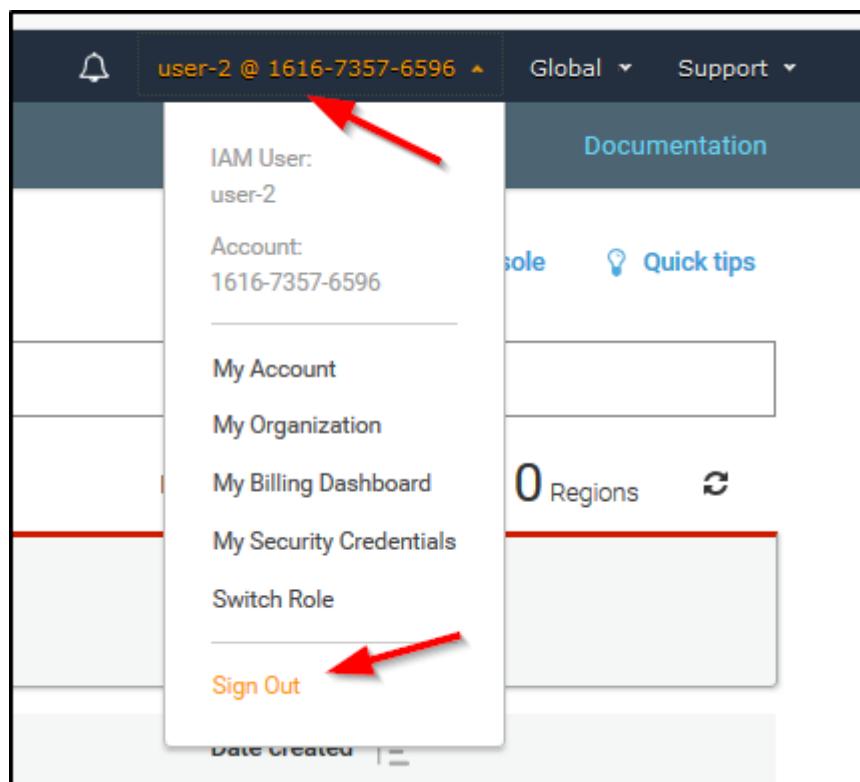
You will see the message **You don't have permissions to list buckets** because user-2 does not have permission to access Amazon S3.

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.



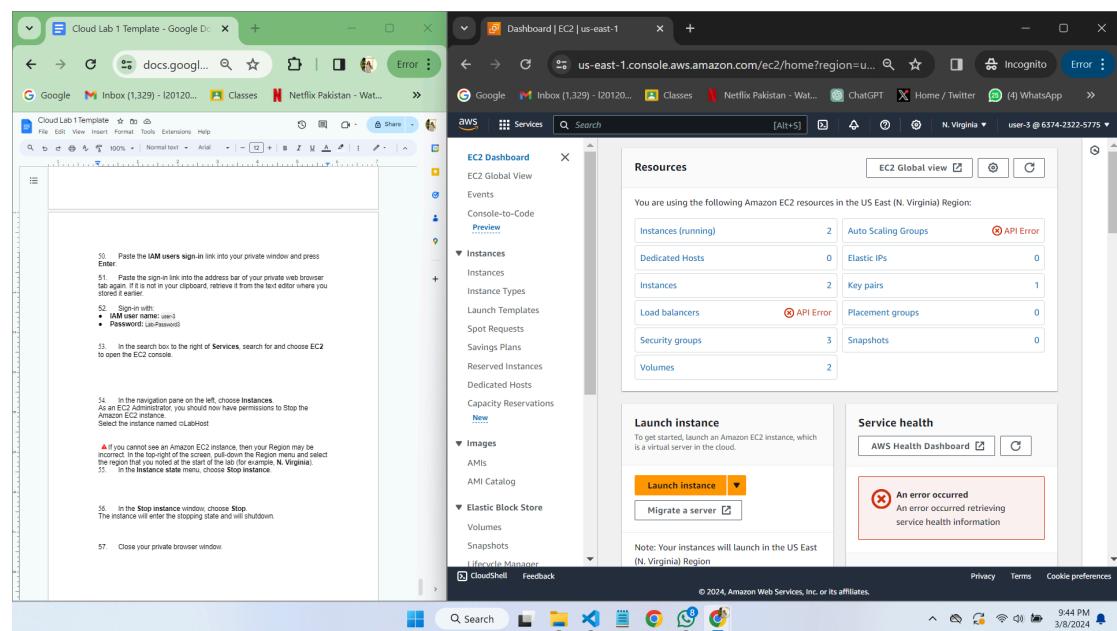
50. Paste the **IAM users sign-in** link into your private window and press **Enter**.

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.

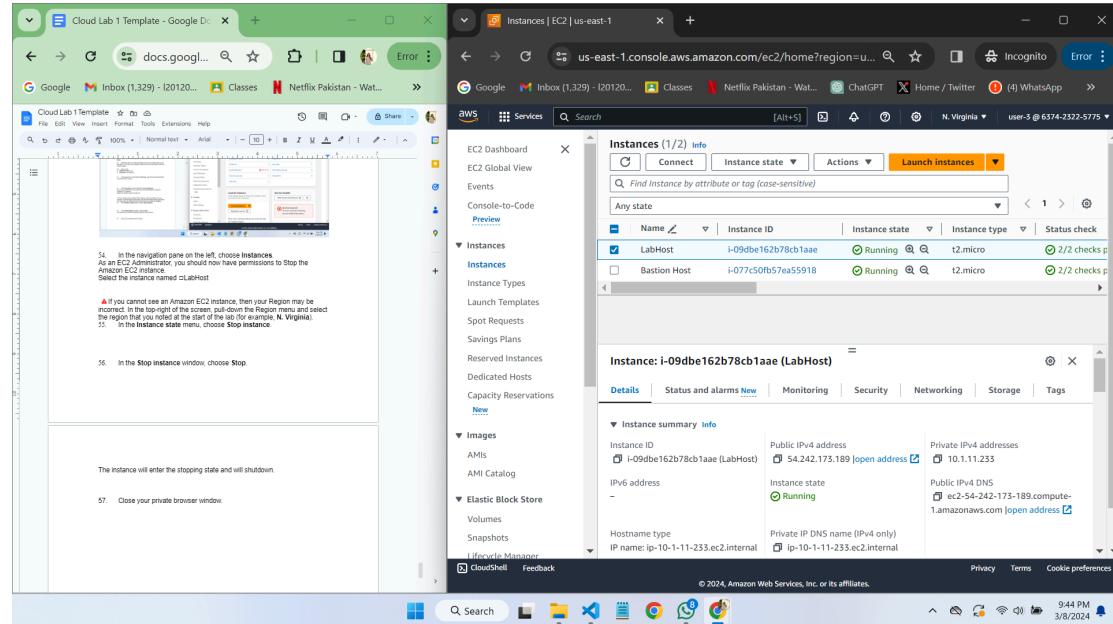
52. Sign-in with:

- **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.

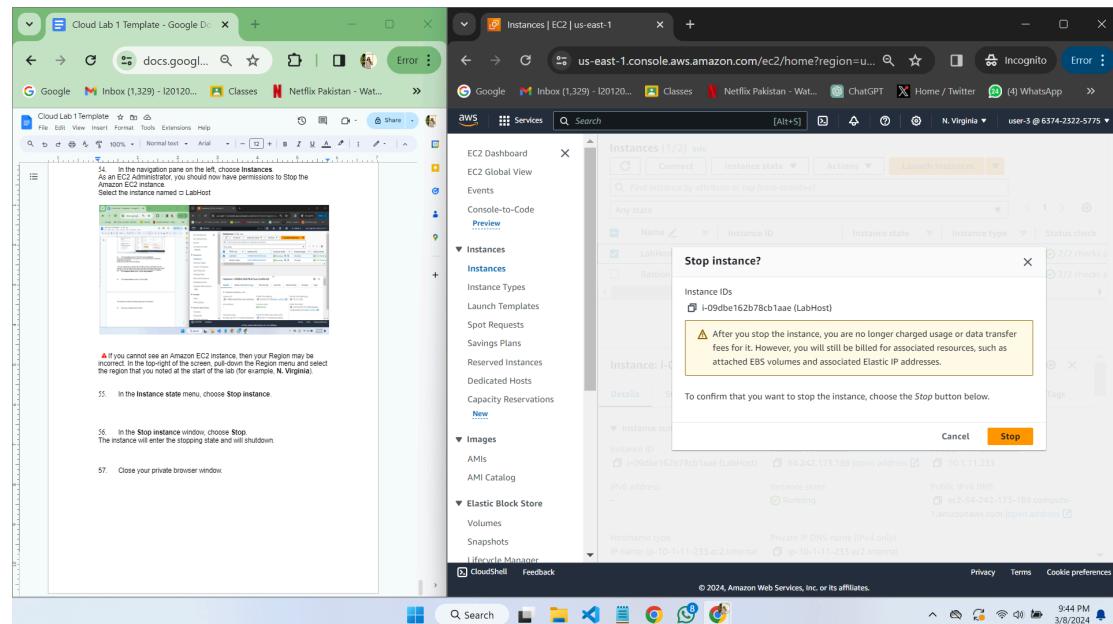


54. In the navigation pane on the left, choose **Instances**.  
As an EC2 Administrator, you should now have permissions to Stop the Amazon EC2 instance.  
Select the instance named  LabHost

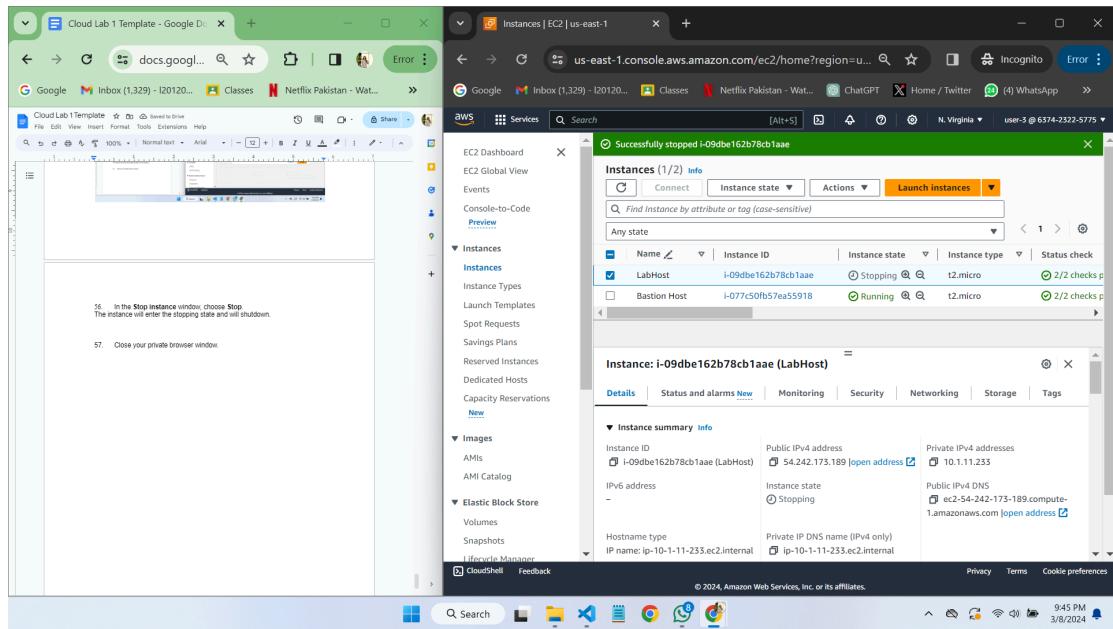


**⚠** If you cannot see an Amazon EC2 instance, then your Region may be incorrect. In the top-right of the screen, pull-down the Region menu and select the region that you noted at the start of the lab (for example, **N. Virginia**).

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.