

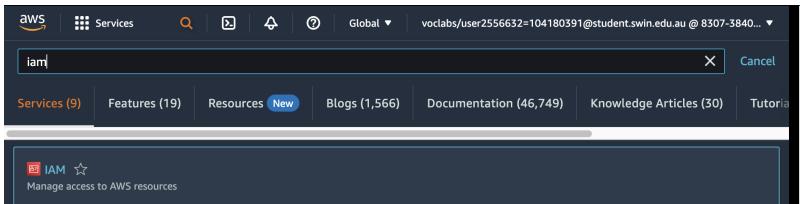
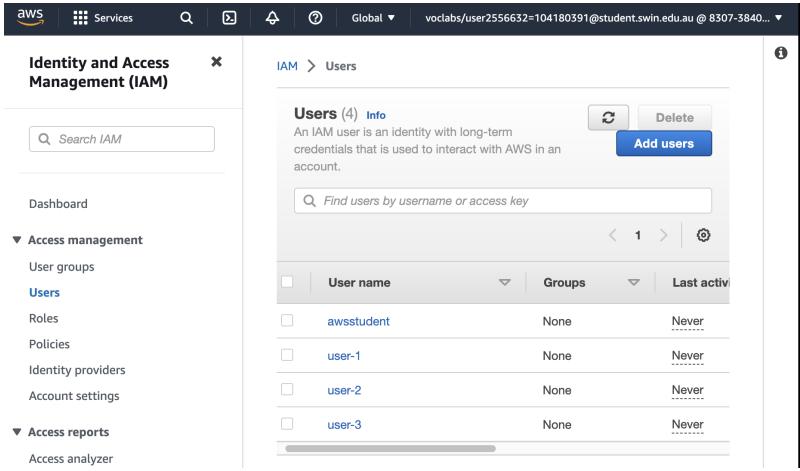
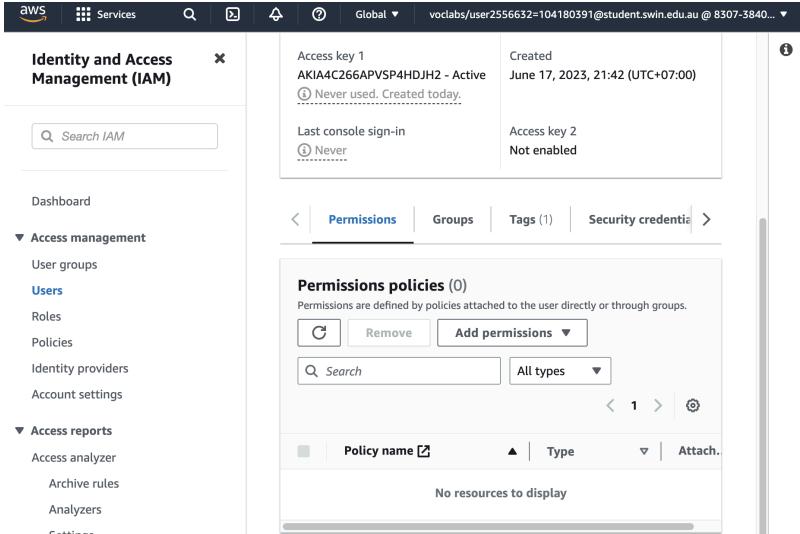


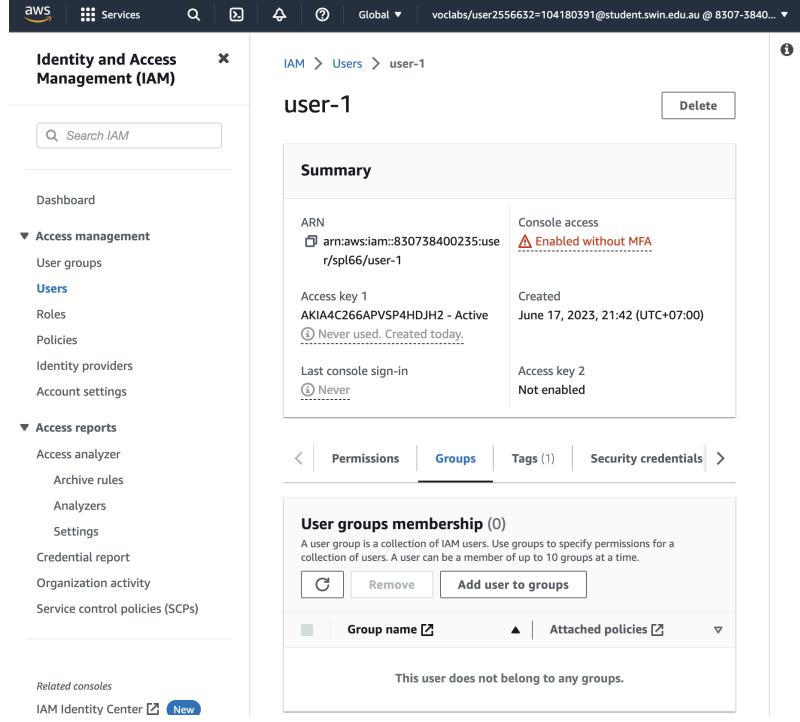
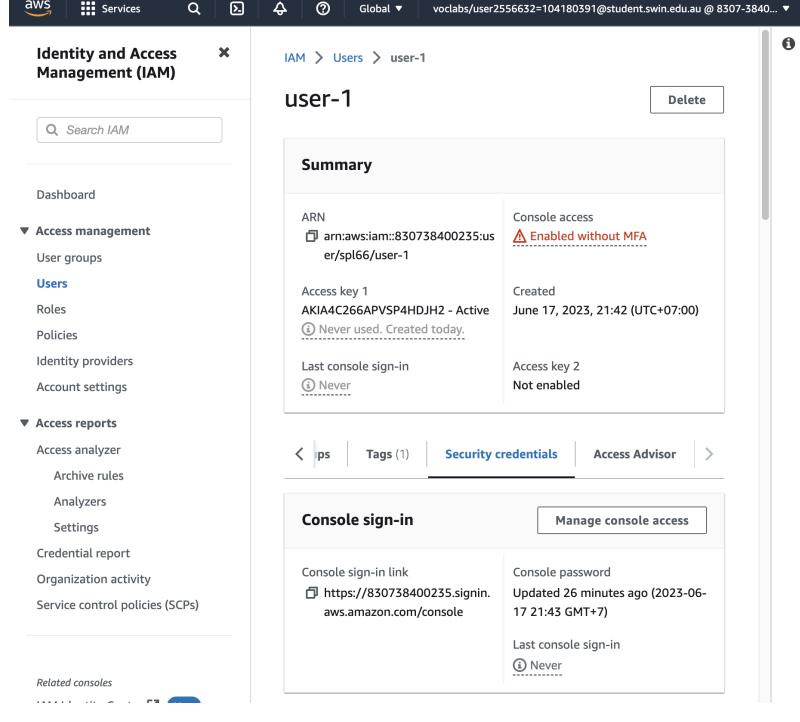
ACF Lab 1: Intro to AWS IAM

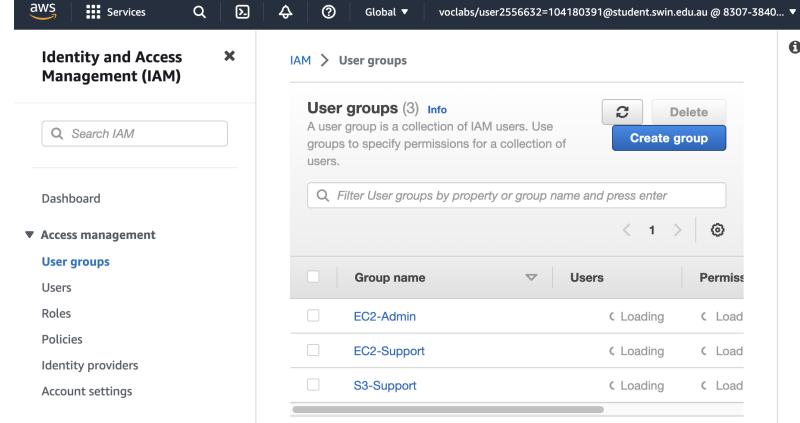
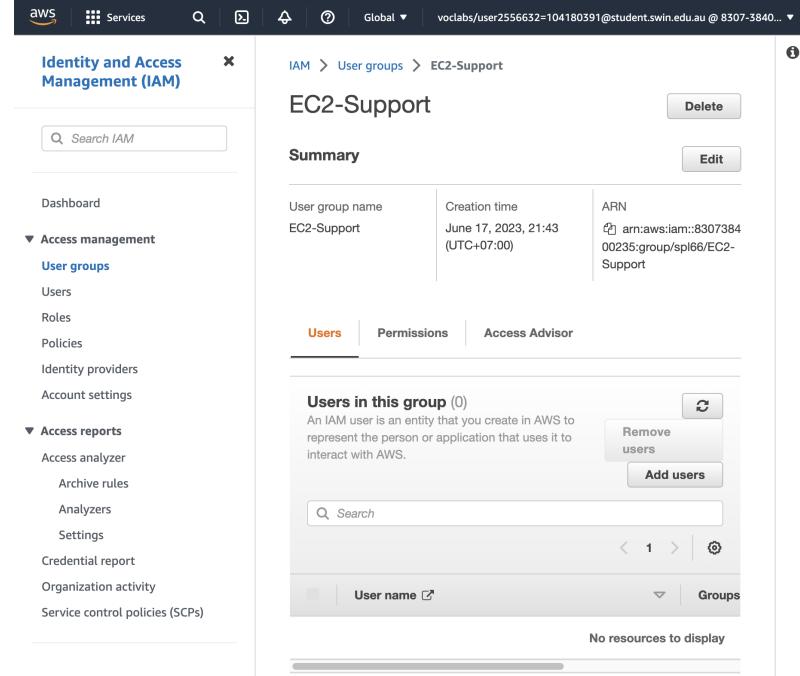
June 17, 2023

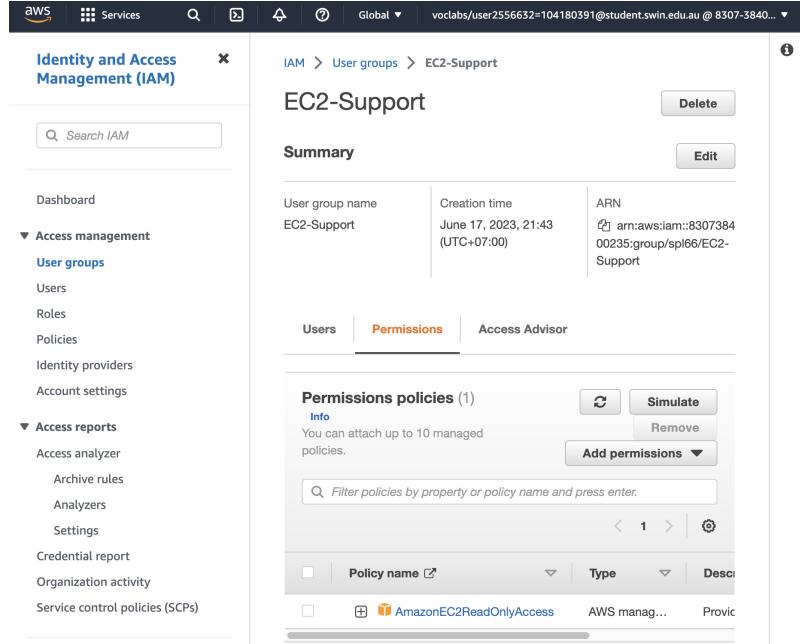
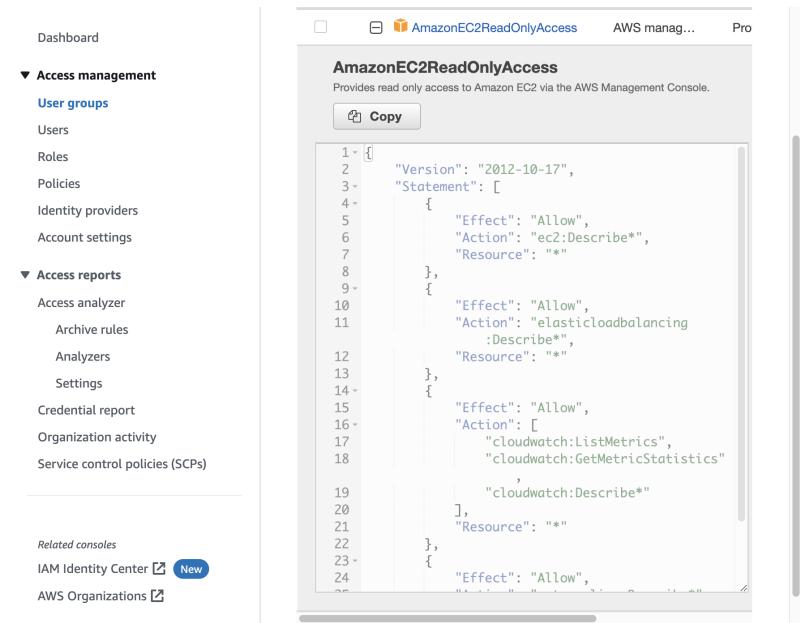
Luu Tuan Hoang
Student ID: 104180391

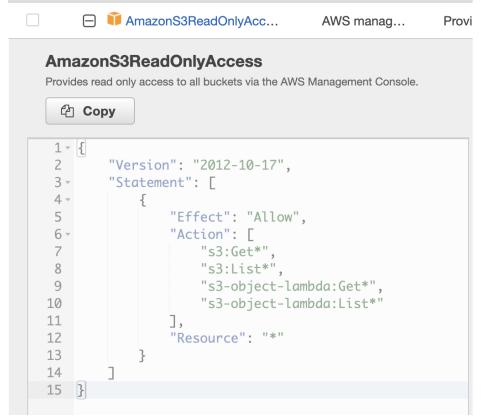
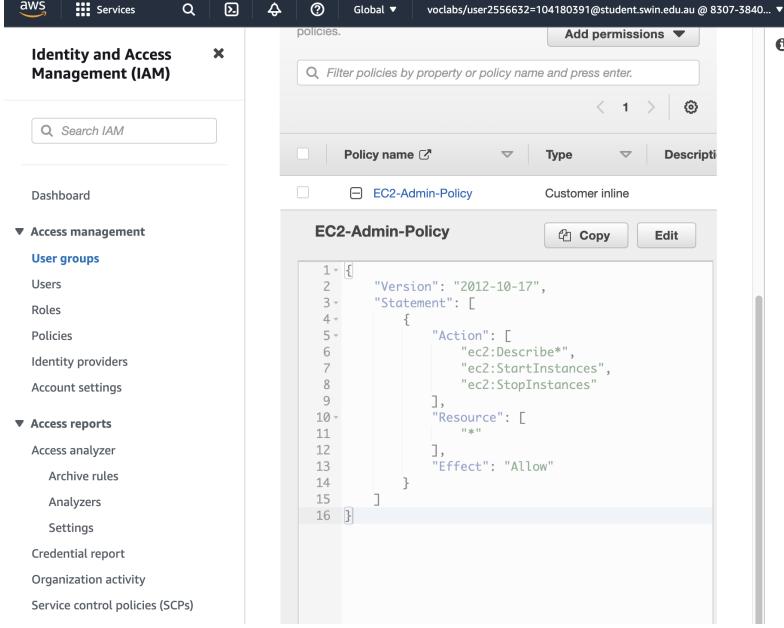
Task 1: Explore the Users and Groups

Step	Description	Screenshot
1	In the AWS Management Console, on the Services menu, select IAM .	
2	In the navigation pane on the left, choose Users . The following IAM Users have been created: <ul style="list-style-type: none">- user-1- user-2- user-3	
3	Choose user-1 . 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.	

4	<p>Choose the Groups tab. user-1 also is not a member of any groups.</p>	 <p>The screenshot shows the AWS IAM User Details page for a user named "user-1". The "Groups" tab is selected. The summary section shows the ARN of the user and two access keys. The "User groups" section indicates that the user is not a member of any groups, with a message stating "This user does not belong to any groups."</p>
5	<p>Choose the Security credentials tab. user-1 is assigned a Console password</p>	 <p>The screenshot shows the AWS IAM User Details page for a user named "user-1". The "Security credentials" tab is selected. The summary section shows the ARN of the user and two access keys. The "Console sign-in" section displays a console sign-in link and a recent update timestamp. The "Console password" section shows the password was updated 26 minutes ago.</p>

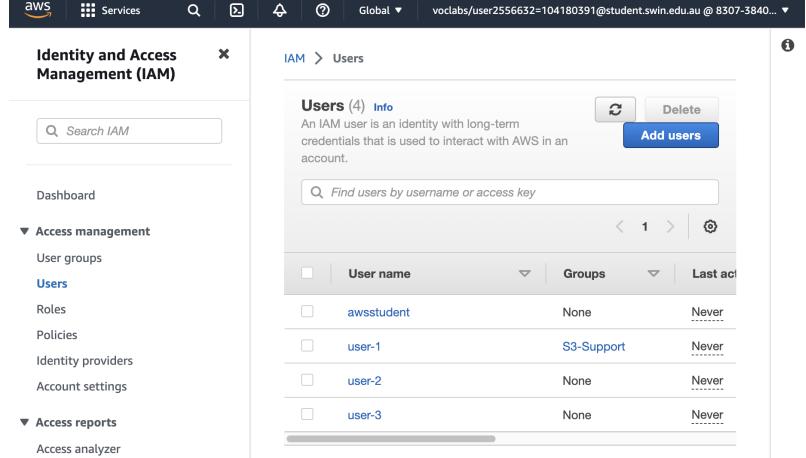
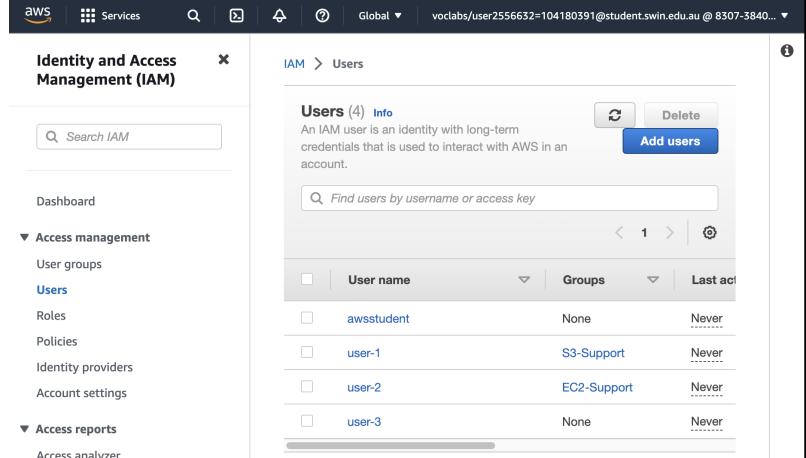
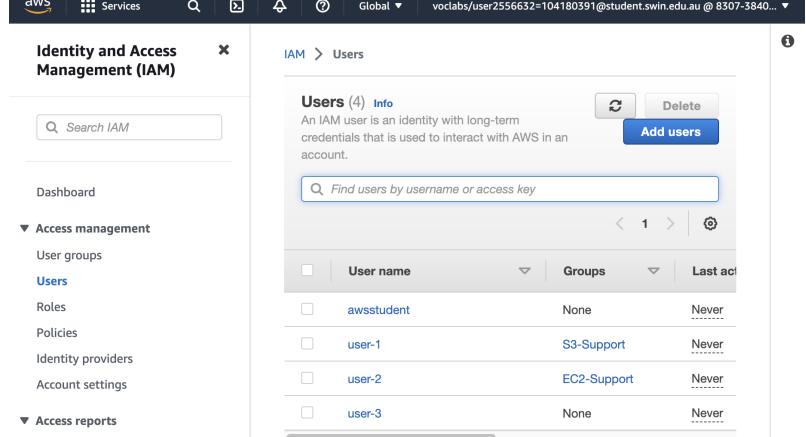
6	<p>In the navigation pane on the left, choose User groups. The following groups have already been created:</p> <ul style="list-style-type: none"> - EC2-Admin - EC2-Support - S3-Support 	 <p>The screenshot shows the AWS Identity and Access Management (IAM) service. In the top navigation bar, 'User groups' is selected. Below it, there's a search bar and a table listing three user groups. The columns in the table are 'Group name', 'Users', and 'Permissions'. The groups listed are EC2-Admin, EC2-Support, and S3-Support, each with a status of 'Loading' under 'Users' and 'Permissions'.</p>
7	<p>Choose the EC2-Support group. This will bring to the summary page for the EC2-Support group.</p>	 <p>The screenshot shows the AWS Identity and Access Management (IAM) service. The URL in the address bar indicates we're on the 'EC2-Support' group's summary page. The left sidebar shows the 'Access management' section with 'User groups' selected. The main content area displays the group's summary information: User group name (EC2-Support), Creation time (June 17, 2023, 21:43 (UTC+07:00)), and ARN (arn:aws:iam::8307384:00235:group/spl66/EC2-Support). Below this, tabs for 'Users', 'Permissions', and 'Access Advisor' are visible. A section titled 'Users in this group (0)' explains what an IAM user is and includes buttons for 'Remove users' and 'Add users'. A search bar and a table for managing users are also present.</p>

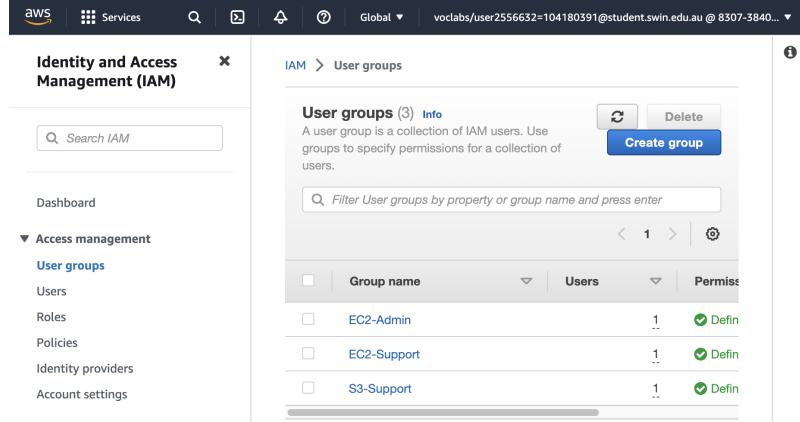
8	<p>Choose the Permissions tab.</p> <p>This group has a Managed Policy associated with it, called AmazonEC2ReadOnlyAccess.</p> <p>Choose the plus (+) icon next to the AmazonEC2ReadOnlyAccess policy to view the policy details.</p>	 <p>The screenshot shows the AWS Identity and Access Management (IAM) console. In the left sidebar, under 'Access management', 'User groups' is selected. The main area displays the 'EC2-Support' user group. The 'Permissions' tab is active, showing a table of policies attached to the group. One policy, 'AmazonEC2ReadOnlyAccess', is highlighted with a blue border. At the bottom of the table, there is a 'Copy' button.</p>
9	<p>A policy defines what actions are allowed or denied for specific AWS resources.</p>	 <p>The screenshot shows the AWS IAM Policies page. A policy named 'AmazonEC2ReadOnlyAccess' is displayed. The policy document is shown in JSON format, detailing the actions and resources it allows. The 'Copy' button is visible at the top of the policy content area.</p> <pre> 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], 20 "Resource": "*" 21 }, 22 { 23 "Effect": "Allow", 24 "Action": "cloudwatch:Describe*", 25 "Resource": "*" 26 } 27] </pre>

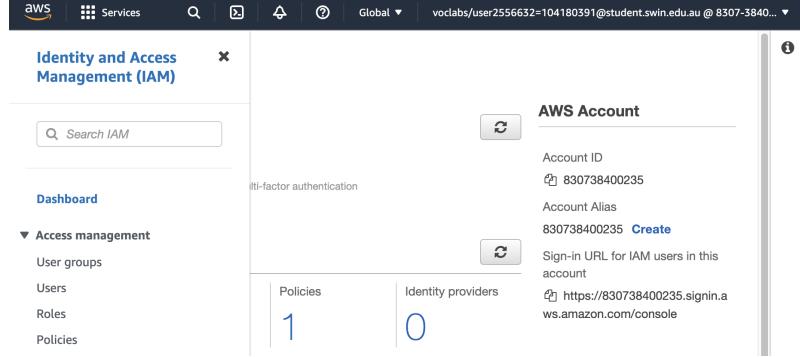
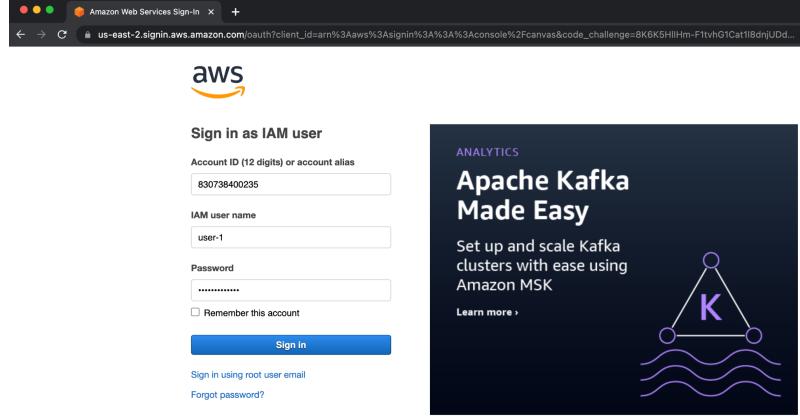
10	<p>Choose the S3-Support group and then choose the Permissions tab.</p> <p>The S3-Support group has the AmazonS3ReadOnlyAccess policy attached.</p> <p>Choose the plus (+) icon to view the policy details.</p> <p>This policy grants permissions to Get and List resources in Amazon S3.</p>	 <pre> 1 "Version": "2012-10-17", 2 "Statement": [3 { 4 "Effect": "Allow", 5 "Action": [6 "s3:Get*", 7 "s3>List*", 8 "s3-object-lambda:Get*", 9 "s3-object-lambda>List*" 10], 11 "Resource": "*" 12 } 13] 14] 15] </pre>
11	<p>Choose the EC2-Admin group and then choose the Permissions tab.</p> <p>The EC2-Admin group has the AmazonS3ReadOnlyAccess policy attached.</p> <p>Choose the plus (+) icon to view the policy details.</p> <p>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.</p>	 <pre> 1 "Version": "2012-10-17", 2 "Statement": [3 { 4 "Action": [5 "ec2:Describe*", 6 "ec2:StartInstances", 7 "ec2:StopInstances" 8], 9 "Resource": "*", 10 "Effect": "Allow" 11 } 12] 13] 14] 15] 16] </pre>

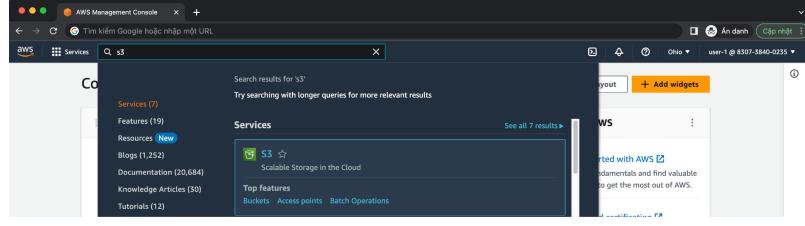
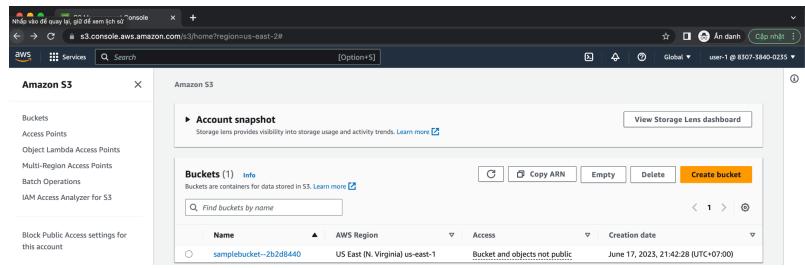
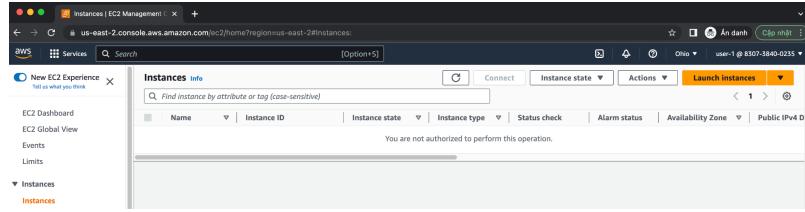
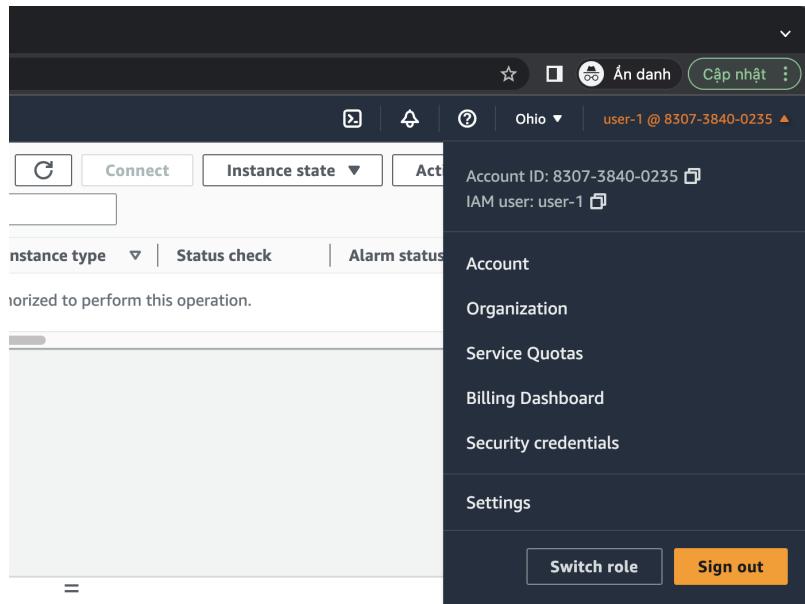
Task 2: Add Users to Groups

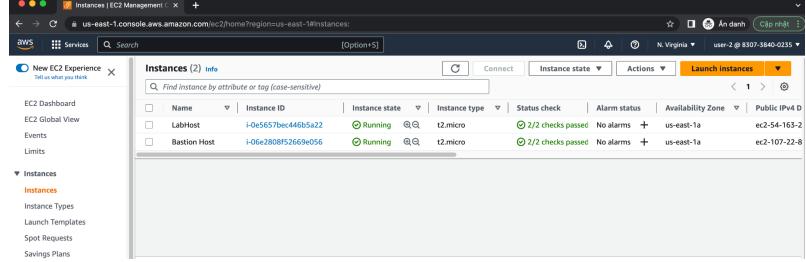
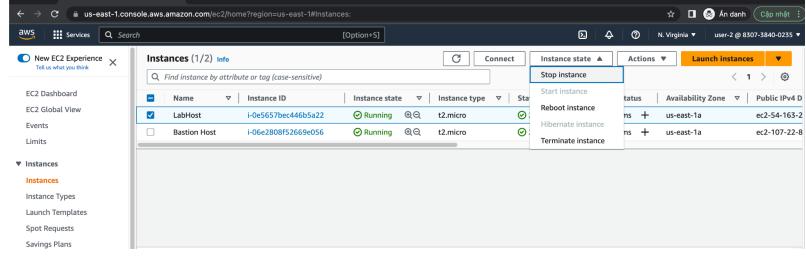
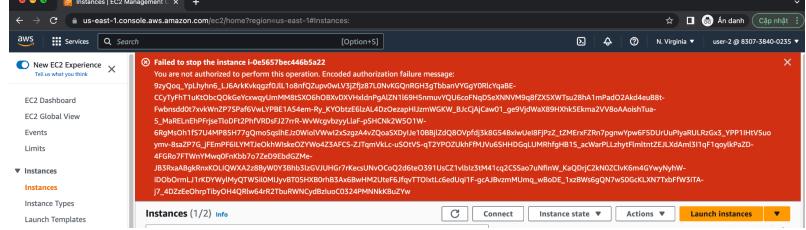
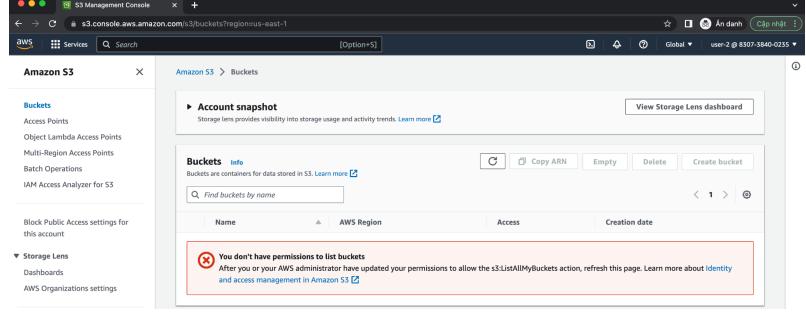
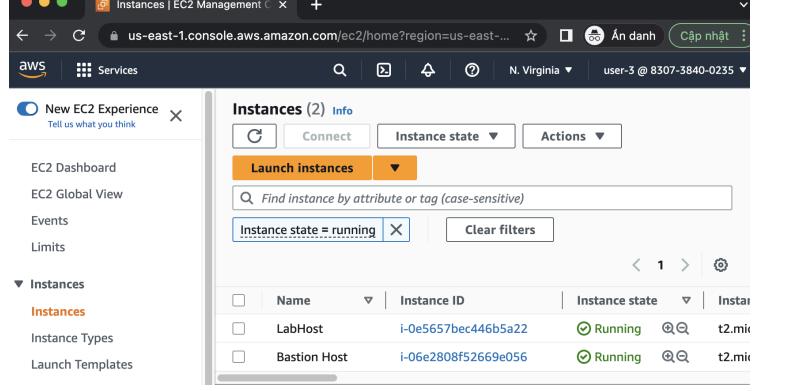
Step	Description	Screenshot
1	<p>In the left navigation pane, choose User groups.</p> <p>Choose the S3-Support group.</p> <p>Choose the Users tab.</p> <p>In the Users tab, choose Add users.</p>	
2	<p>In the Add Users to S3-Support window, configure the following:</p> <ul style="list-style-type: none"> - Select user-1. - At the bottom of the screen, choose Add Users. 	

3	<p>In the Users tab, user-1 has been added to the group.</p>	 <p>The screenshot shows the AWS IAM service's 'Users' page. The left sidebar has 'Identity and Access Management (IAM)' selected under 'Access management'. The main area displays a table of users:</p> <table border="1"> <thead> <tr> <th>User Name</th> <th>Groups</th> <th>Last Activity</th> </tr> </thead> <tbody> <tr> <td>awsstudent</td> <td>None</td> <td>Never</td> </tr> <tr> <td>user-1</td> <td>S3-Support</td> <td>Never</td> </tr> <tr> <td>user-2</td> <td>None</td> <td>Never</td> </tr> <tr> <td>user-3</td> <td>None</td> <td>Never</td> </tr> </tbody> </table>	User Name	Groups	Last Activity	awsstudent	None	Never	user-1	S3-Support	Never	user-2	None	Never	user-3	None	Never
User Name	Groups	Last Activity															
awsstudent	None	Never															
user-1	S3-Support	Never															
user-2	None	Never															
user-3	None	Never															
4	<p>Using similar steps to the ones above, add user-2 to the EC2-Support group.</p>	 <p>The screenshot shows the AWS IAM service's 'Users' page. The left sidebar has 'Identity and Access Management (IAM)' selected under 'Access management'. The main area displays a table of users:</p> <table border="1"> <thead> <tr> <th>User Name</th> <th>Groups</th> <th>Last Activity</th> </tr> </thead> <tbody> <tr> <td>awsstudent</td> <td>None</td> <td>Never</td> </tr> <tr> <td>user-1</td> <td>S3-Support</td> <td>Never</td> </tr> <tr> <td>user-2</td> <td>EC2-Support</td> <td>Never</td> </tr> <tr> <td>user-3</td> <td>None</td> <td>Never</td> </tr> </tbody> </table>	User Name	Groups	Last Activity	awsstudent	None	Never	user-1	S3-Support	Never	user-2	EC2-Support	Never	user-3	None	Never
User Name	Groups	Last Activity															
awsstudent	None	Never															
user-1	S3-Support	Never															
user-2	EC2-Support	Never															
user-3	None	Never															
5	<p>Using similar steps to the ones above, add user-3 to the EC2-Admin group.</p>	 <p>The screenshot shows the AWS IAM service's 'Users' page. The left sidebar has 'Identity and Access Management (IAM)' selected under 'Access management'. The main area displays a table of users:</p> <table border="1"> <thead> <tr> <th>User Name</th> <th>Groups</th> <th>Last Activity</th> </tr> </thead> <tbody> <tr> <td>awsstudent</td> <td>None</td> <td>Never</td> </tr> <tr> <td>user-1</td> <td>S3-Support</td> <td>Never</td> </tr> <tr> <td>user-2</td> <td>EC2-Support</td> <td>Never</td> </tr> <tr> <td>user-3</td> <td>None</td> <td>Never</td> </tr> </tbody> </table>	User Name	Groups	Last Activity	awsstudent	None	Never	user-1	S3-Support	Never	user-2	EC2-Support	Never	user-3	None	Never
User Name	Groups	Last Activity															
awsstudent	None	Never															
user-1	S3-Support	Never															
user-2	EC2-Support	Never															
user-3	None	Never															

6	<p>In the navigation pane on the left, choose User groups.</p> <p>Each Group should now have a 1 in the Users column.</p>	 <p>The screenshot shows the AWS Identity and Access Management (IAM) console. In the left navigation pane, under 'Access management', 'User groups' is selected. On the right, the 'User groups' page displays three entries: 'EC2-Admin' (1 user), 'EC2-Support' (1 user), and 'S3-Support' (1 user). Each entry has a 'Defin' button next to it.</p>
---	--	---

Task 3: Sign-In and Test Users		
Step	Description	Screenshot
7	<p>In the navigation pane on the left, choose Dashboard.</p> <p>An IAM user's sign-in link is displayed on the right.</p>	 <p>The screenshot shows the AWS Identity and Access Management (IAM) console. In the left navigation pane, under 'Access management', 'User groups' is selected. On the right, the 'AWS Account' section displays the account ID (830738400235), account alias (830738400235), and a 'Create' button. Below this, the 'Sign-in URL for IAM users in this account' is shown as https://830738400235.signin.amazonaws.com/console.</p>
8	<p>Paste the IAM users sign-in link into the address bar of the private browser session.</p> <p>Sign-in with:</p> <ul style="list-style-type: none"> - IAM username: user-1 - Password: Lab-Password1 	 <p>The screenshot shows a browser window with the AWS Sign-in page. The URL is us-east-2.sigin.aws.amazon.com/oauth?client_id=arn%3aws%3asignin%3A%3Aconsole%2Fcanvas&code_challenge=8K6K5HlHm-FtvhG1Cat18dnjUdd... The page asks for a sign-in user name (user-1) and password. To the right, there is an advertisement for 'Apache Kafka Made Easy' with a purple 'K' logo.</p>

9	<p>In the Services menu, choose S3.</p>	
10	<p>Choose the name of the bucket that exists in the account and browse the contents. Since the user is part of the S3-Support Group in IAM, they have permission to view a list of Amazon S3 buckets and the contents.</p>	
11	<p>In the Services menu, choose EC2. In the left navigation pane, choose Instances. The user cannot see any instances. Instead, the user sees 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.</p>	
12	<p>Sign-out from the current user. Sign-in again with:<ul style="list-style-type: none">• IAM user name: user-2• Password: Lab-Password2</p>	

13	<p>In the Services menu, choose EC2.</p> <p>In the left navigation pane, choose Instances. The user is now able to see an Amazon EC2 instance because the user has Read Only permissions. However, the user will not be able to make any changes to Amazon EC2 resources.</p>	
14	<p>Select the instance named LabHost. In the Instance state menu above, select Stop instance.</p>	
15	<p>The user will receive an error stating You are not authorized to perform this operation. This demonstrates that the policy only allows the user to view information, without making changes.</p>	
16	<p>In the Services, choose S3. The user will see the message You don't have permissions to list buckets because user-2 does not have permission to access Amazon S3</p>	
17	<p>Sign-out from the current user.</p> <p>Sign-in again with:</p> <ul style="list-style-type: none"> • IAM user name: user-3 • Password: Lab-Password3 <p>In the Services menu, choose EC2.</p> <p>In the left navigation pane, choose Instances.</p>	

18

Select the instance named **LabHost**. In the **Instance state** menu above, select **Stop instance**.

The instance will enter the stopping state and will shut down.

Screenshot of the AWS EC2 Management console showing the Instances page. A success message at the top says "Successfully stopped i-0e5657bec446b5a22". The table lists two instances:

Name	Instance ID	Instance State	Instance Type
LabHost	i-0e5657bec446b5a22	Stopping	t2.micro
Bastion Host	i-06e2808f52669e056	Running	t2.micro