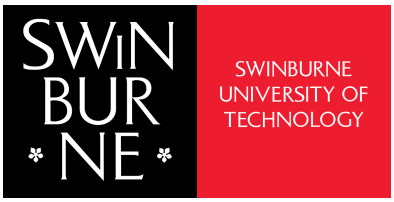
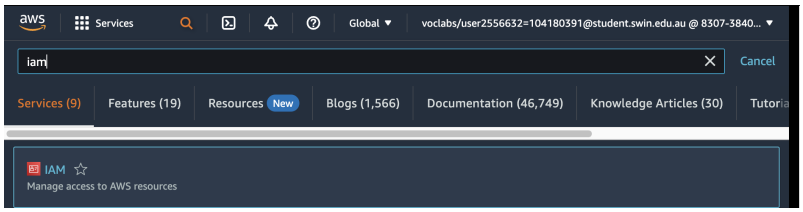
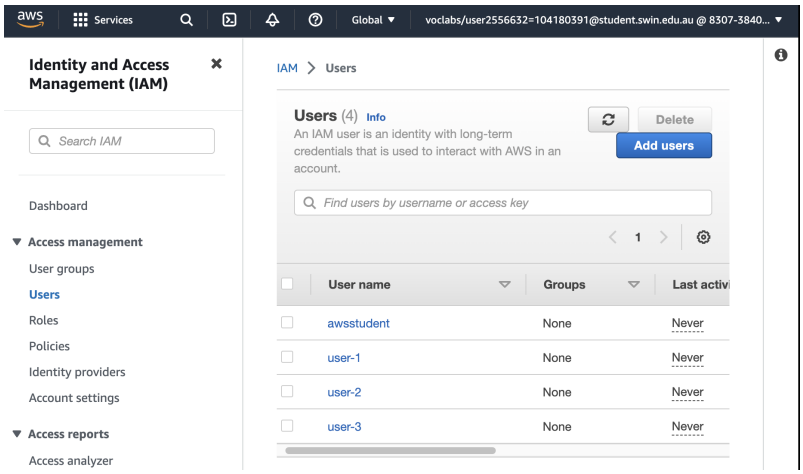
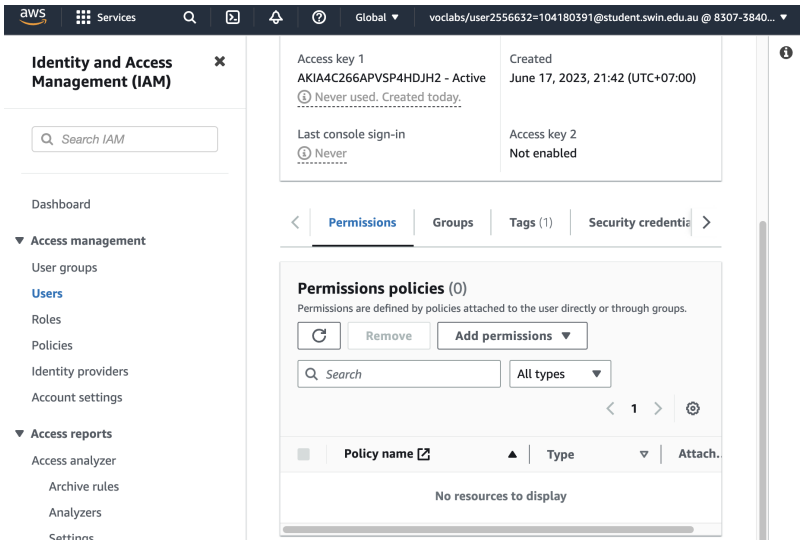
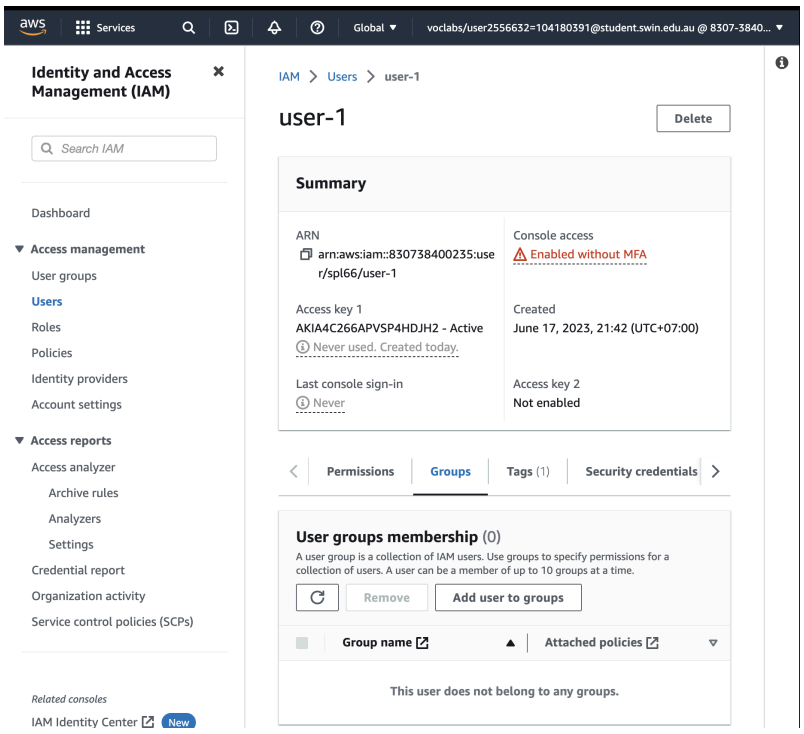
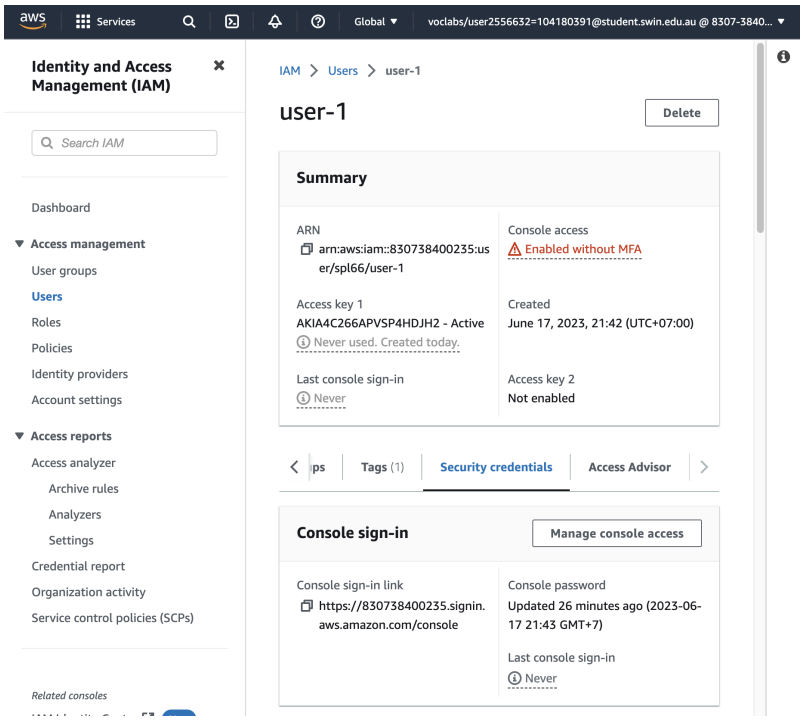


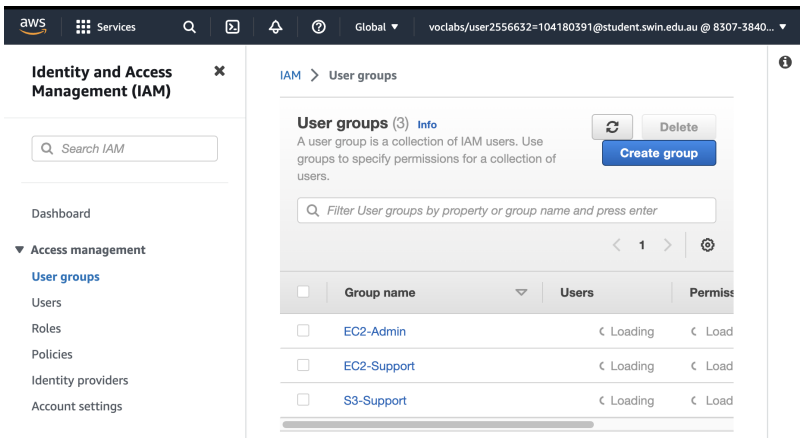
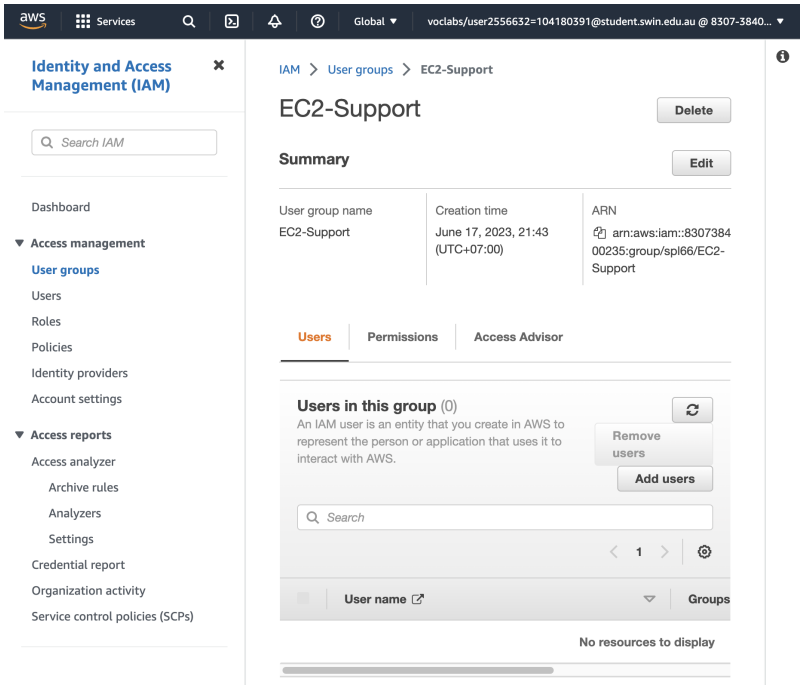
ACF Lab 1: Intro to AWS IAM

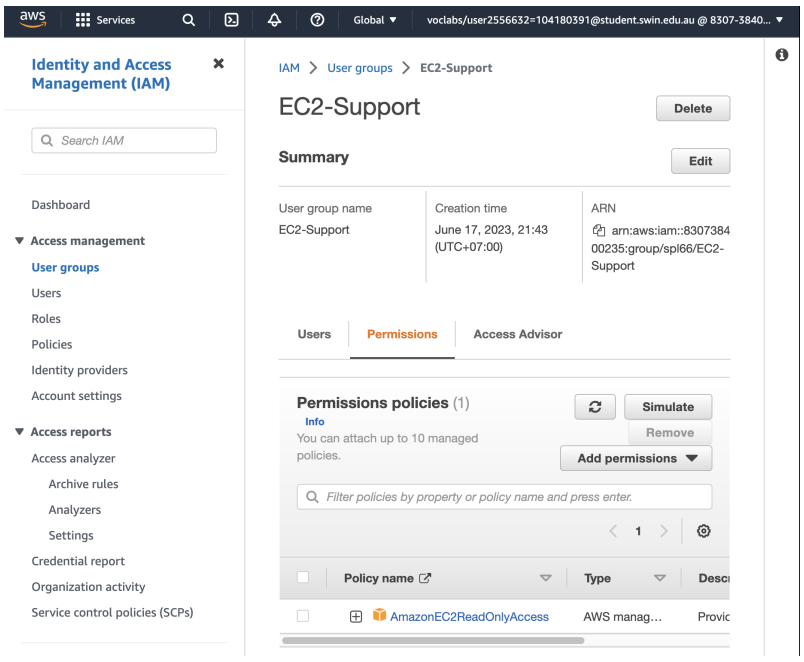
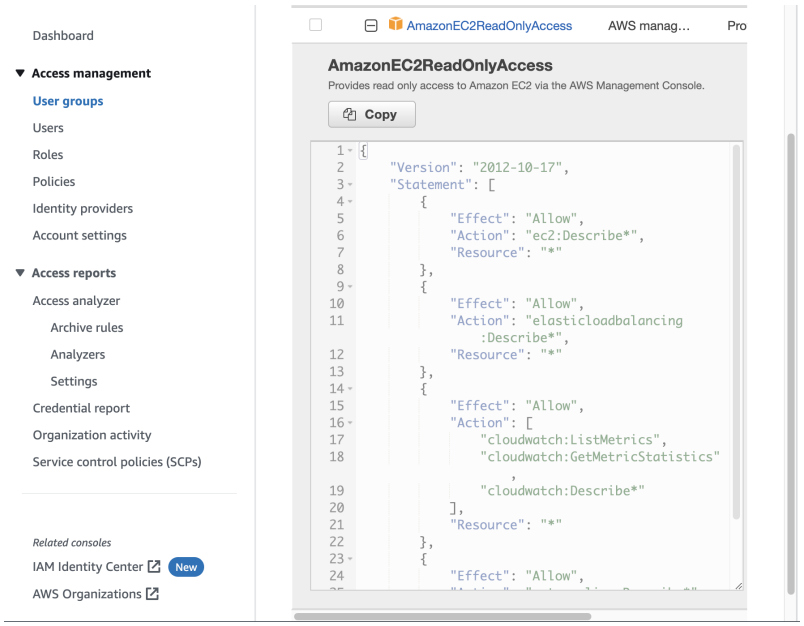
June 17, 2023

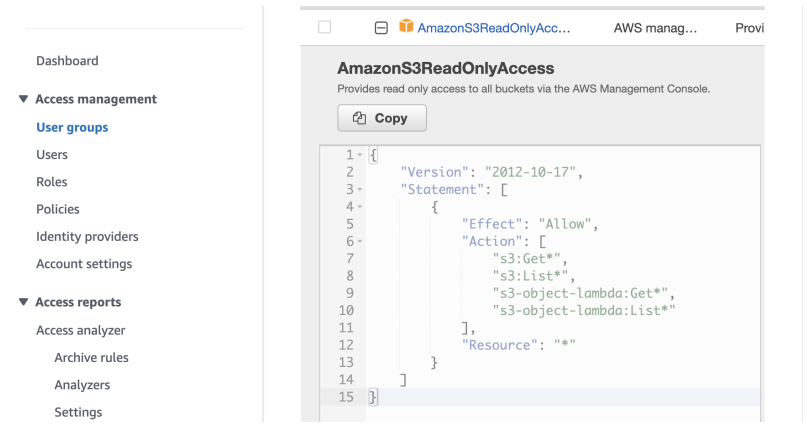
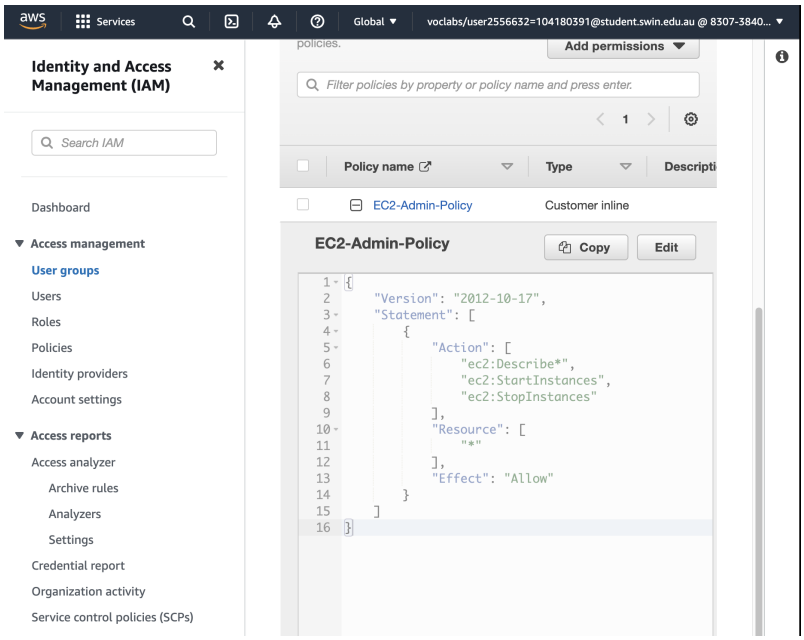
Luu Tuan Hoang
Student ID: 104180391

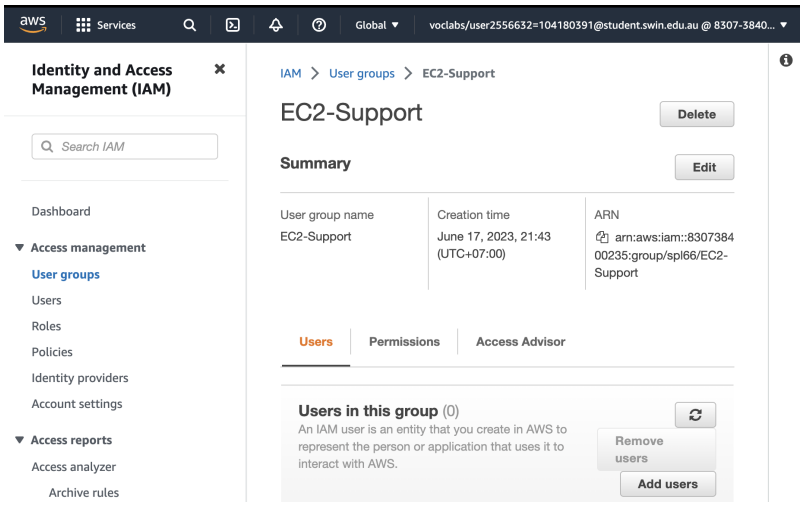
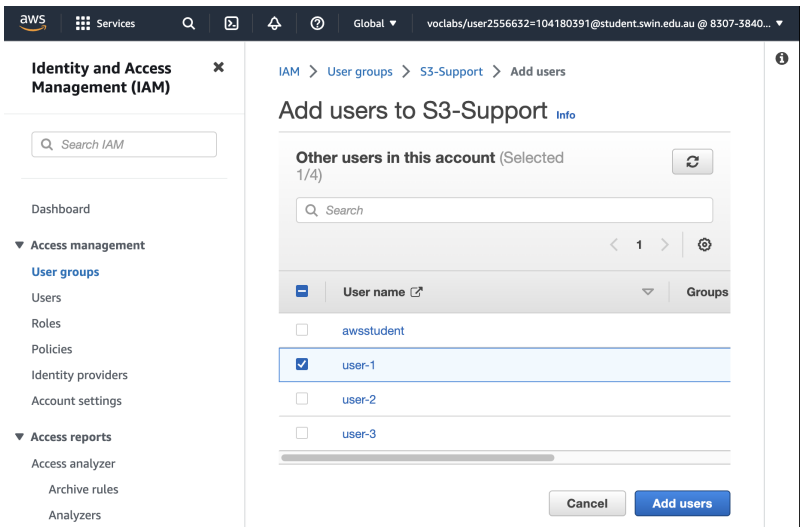
Task 1: Explore the Users and Groups		
Step	**Description**	**Screenshot**
1	In the AWS Management Console, on the **Services** menu, select **IAM**.	
2	In the navigation pane on the left, choose **Users**. The following IAM Users have been created: - user-1 - user-2 - user-3	
3	Choose **user-1**. This will bring to a summary page for **user-1**. The **Permissions** tab will be displayed. Notice that **user-1** does not have any permissions.	

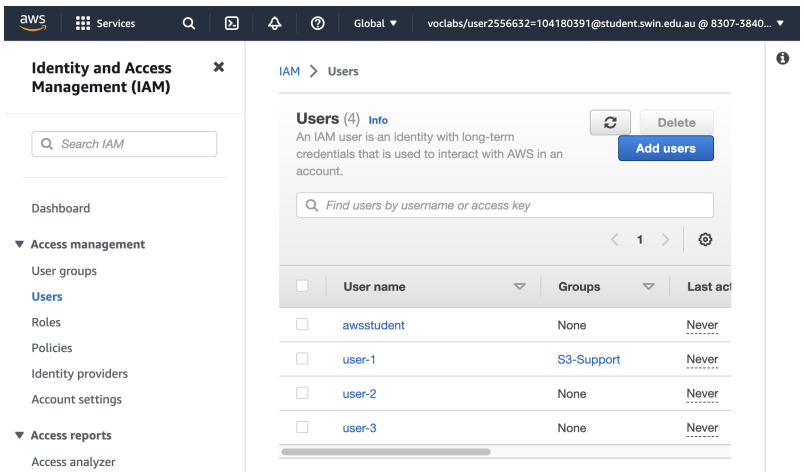
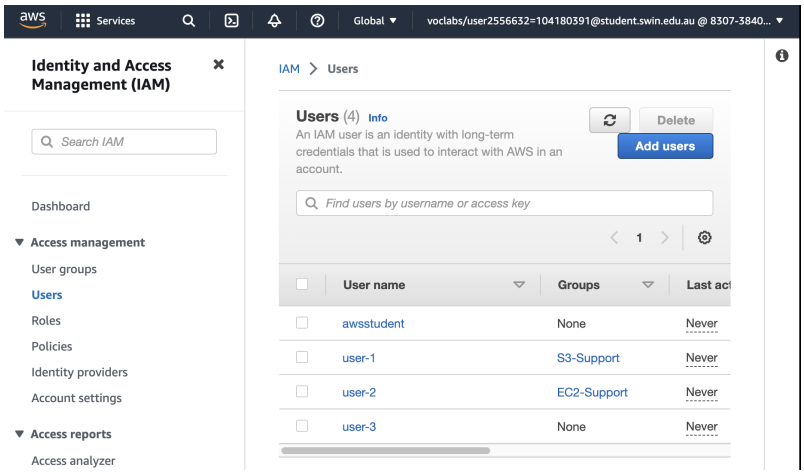
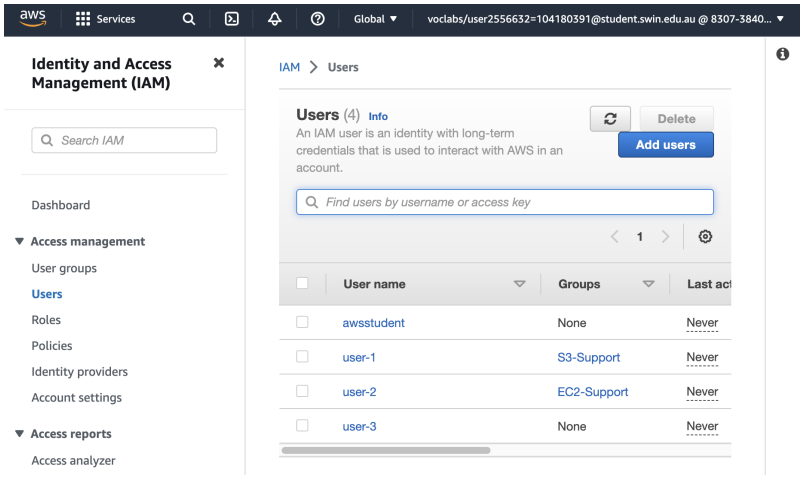
4	Choose the **Groups** tab. **user-1** also is not a member of any groups.	
5	Choose the **Security** credentials tab. **user-1** is assigned a Console password	

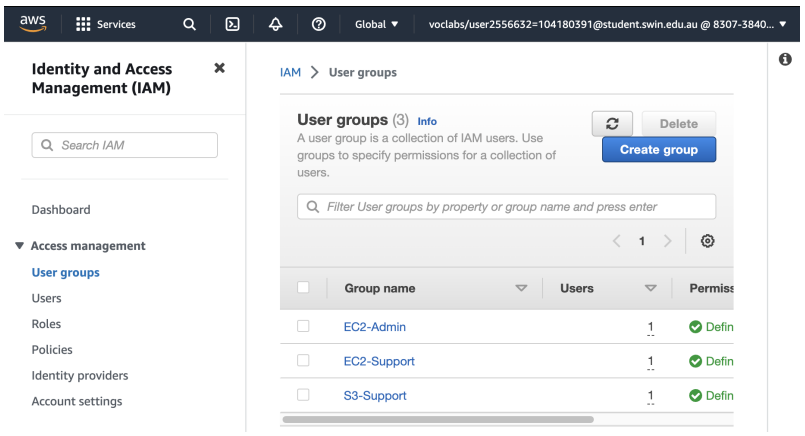
6	In the navigation pane on the left, choose **User groups**. The following groups have already been created: - EC2-Admin - EC2-Support - S3-Support	
7	Choose the **EC2-Support** group. This will bring to the summary page for the **EC2-Support** group.	

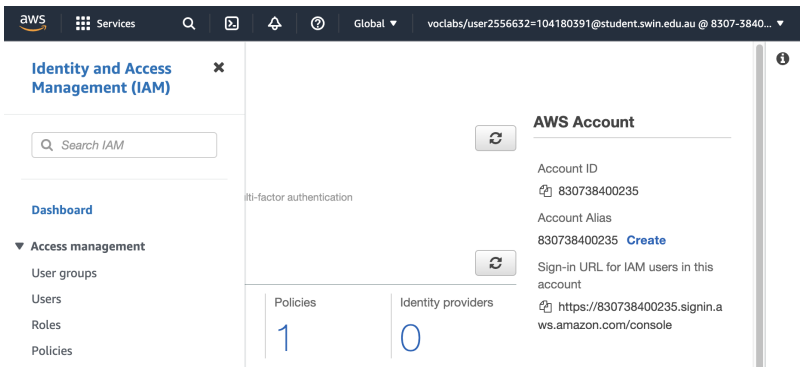
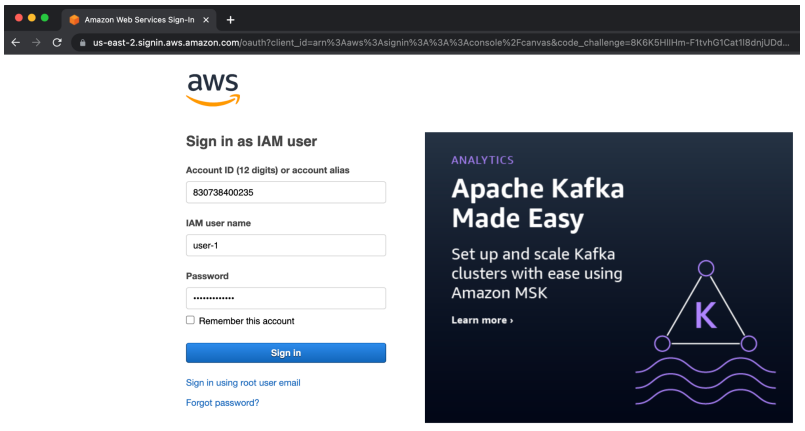
8	Choose the **Permissions** tab. This group has a **Managed Policy** associated with it, called **AmazonEC2ReadOnlyAccess**. Choose the plus **(+)** icon next to the **AmazonEC2ReadOnlyAccess** policy to view the policy details.	
9	A policy defines what actions are allowed or denied for specific AWS resources.	

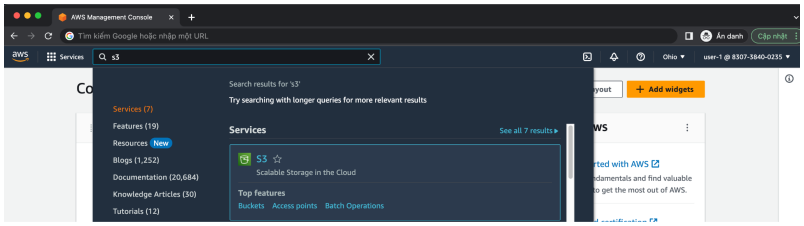
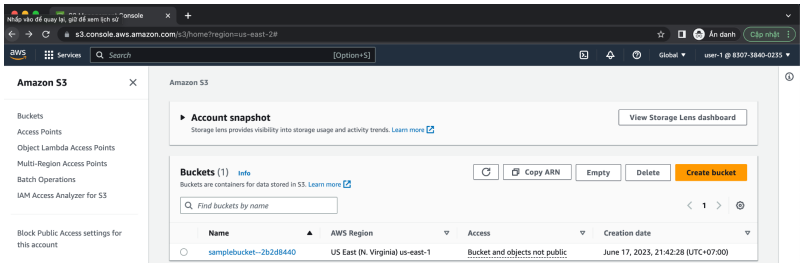
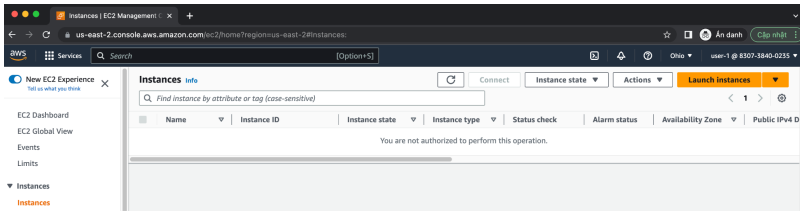
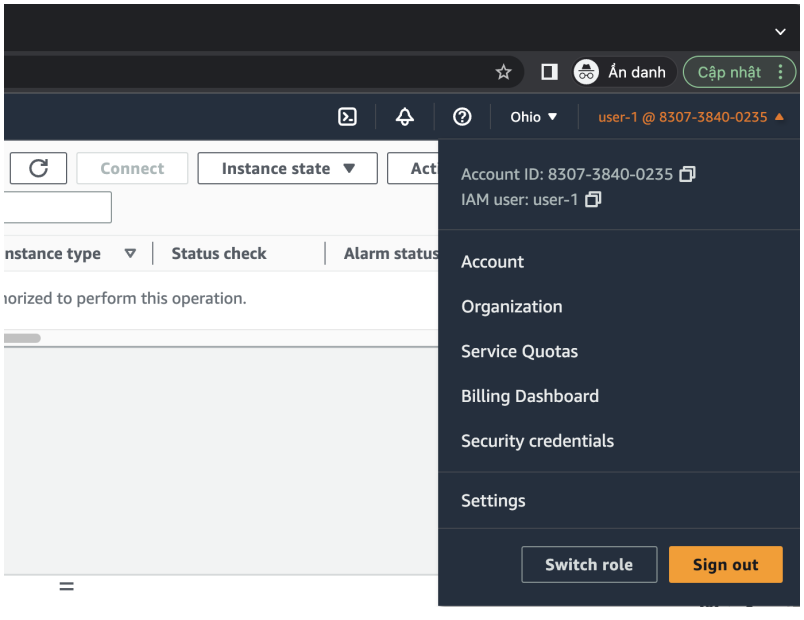
10	Choose the **S3-Support** group and then choose the Permissions tab. The **S3-Support** group has the **AmazonS3ReadOnlyAccess** policy attached. Choose the plus **(+)** icon to view the policy details. This policy grants permissions to Get and List resources in Amazon S3.	
11	Choose the **EC2-Admin** group and then choose the Permissions tab. The **EC2-Admin** group has the **AmazonS3ReadOnlyAccess** policy attached. Choose the plus **(+)** icon to view the policy details. 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.	

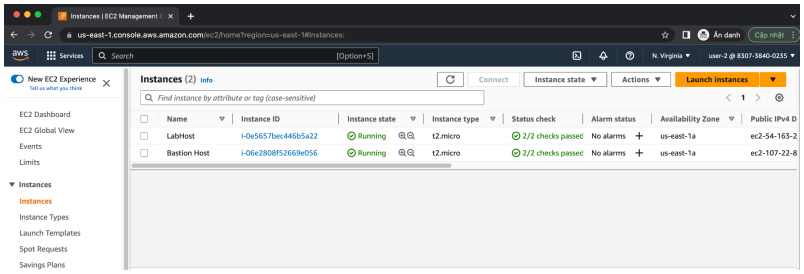
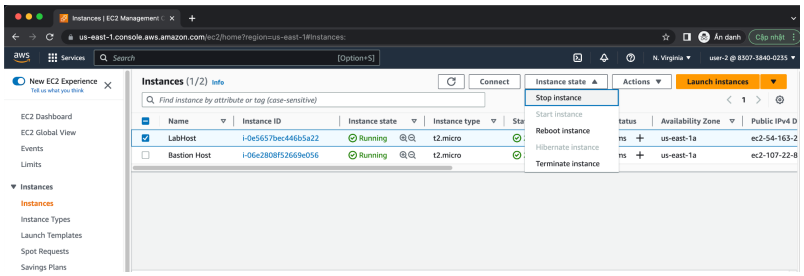
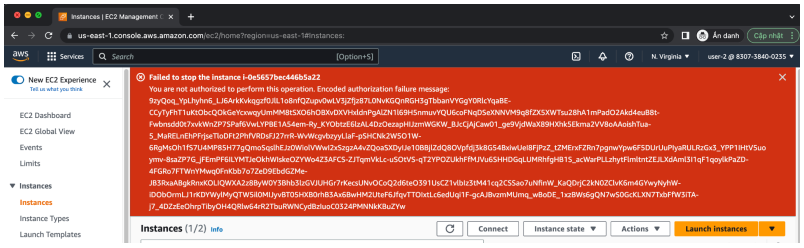
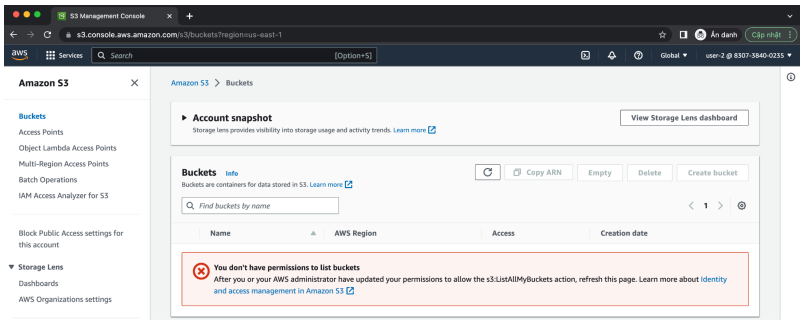
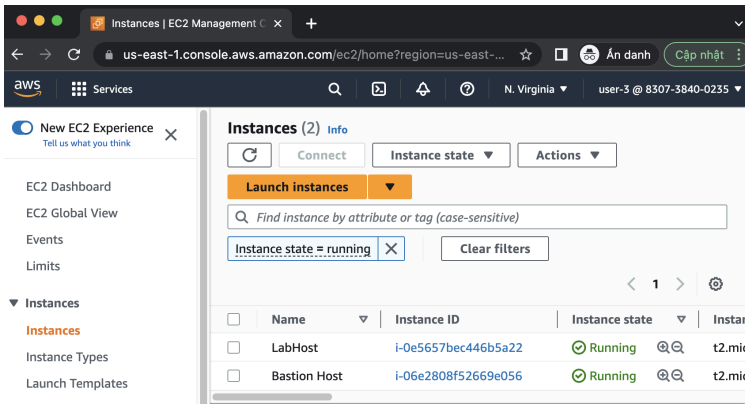
Task 2: Add Users to Groups		
Step	**Description**	**Screenshot**
1	In the left navigation pane, choose **User groups**. Choose the **S3-Support** group. Choose the **Users** tab. In the **Users** tab, choose **Add users**.	
2	In the **Add Users** to **S3-Support** window, configure the following: - Select **user-1**. - At the bottom of the screen, choose **Add Users**.	

3	In the **Users** tab, **user-1** has been added to the group.	
4	Using similar steps to the ones above, add **user-2** to the **EC2-Support** group.	
5	Using similar steps to the ones above, add **user-3** to the **EC2-Admin** group.	

6	In the navigation pane on the left, choose **User groups**. Each Group should now have a **1** in the **Users** column.	

Task 3: Sign-In and Test Users		
Step	**Description**	**Screenshot**
7	In the navigation pane on the left, choose **Dashboard**. An **IAM user's sign-in link** is displayed on the right.	
8	Paste the IAM users sign-in link into the address bar of the private browser session. Sign-in with: - **IAM username**: user-1 - **Password**: Lab-Password1	

9	In the **Services** menu, choose **S3**.	
10	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.	
11	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.	
12	Sign-out from the current user. Sign-in again with: • **IAM user name:** user-2 • **Password:** Lab-Password2	

13	In the **Services** menu, choose **EC2**. 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.	
14	Select the instance named **LabHost**. In the **Instance state** menu above, select **Stop instance**.	
15	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.	
16	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	
17	Sign-out from the current user. Sign-in again with: • **IAM user name:** user-3 • **Password:** Lab-Password3 In the **Services** menu, choose **EC2**. In the left navigation pane, choose **Instances**.	

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.