Swinburne University of Technology

COS20019 Cloud Computing Architecture

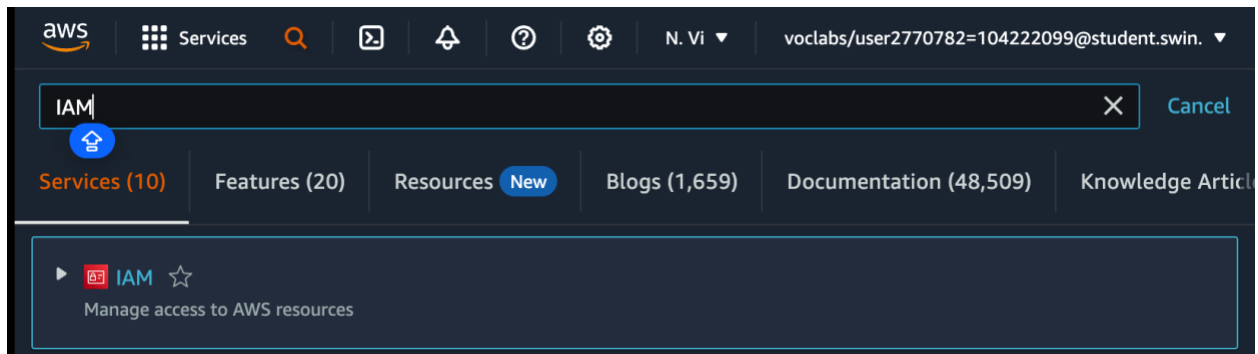# Week 6: ACF Lab 1: Intro to AWS IAM

Saturday 14th October, 2023

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**.
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.

Create access key

< **Permissions** | **Groups** | **Tags** (1) | **Sec** >

Permissions policies (0)

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

| C | Remove | Add permissions ▼ |

Filter by Type

Q Search   All ty... ▼

< 1 >   ⚙

☐	Policy name ☐	▲	Type

No resources to display

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-Admin
- EC2-Support
- S3-Support
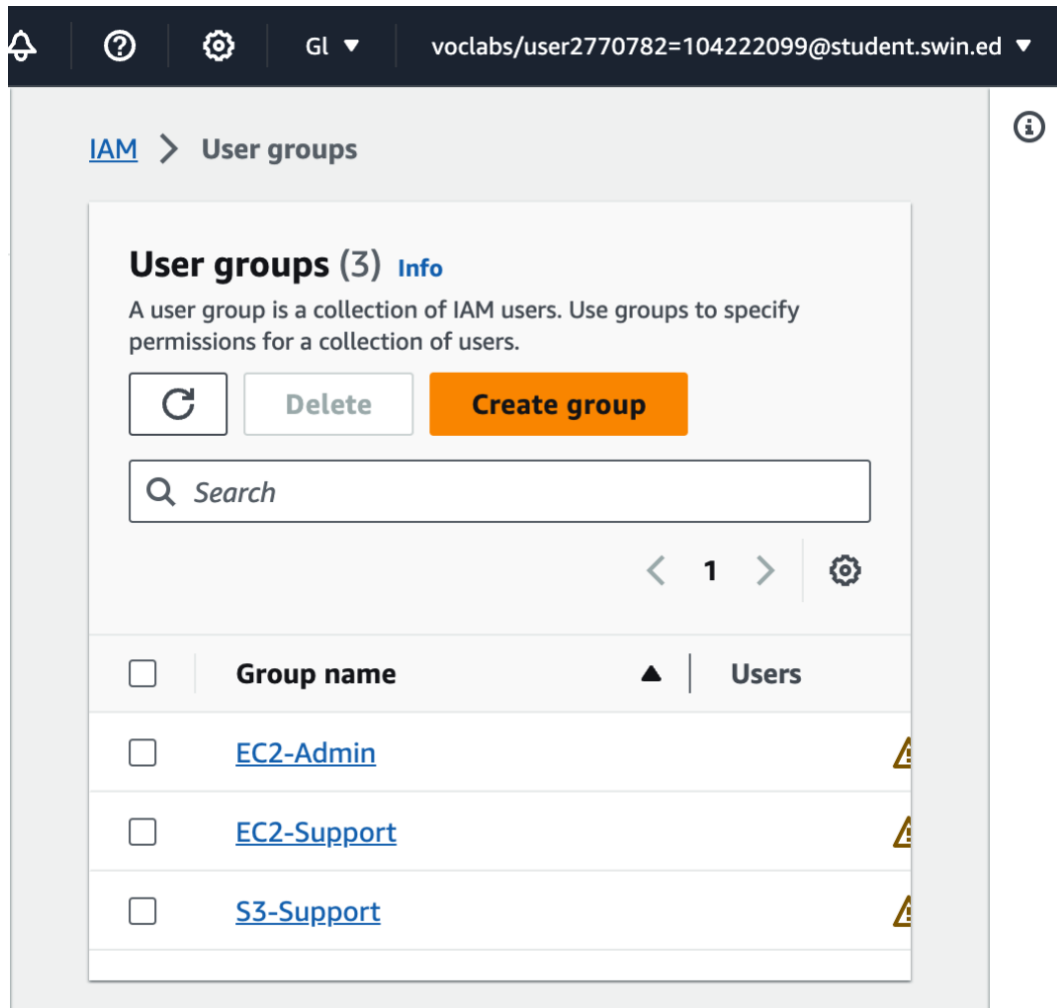
Choose the **EC2-Support** group.
This will bring you to the summary page for the **EC2-Support** group.

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.

Add permissions ▼

Filter by Type

🔍 Search

All ty... ▼

‹ 1 › ⚙

	Policy name ⬀ ▲	Type ▽
☐	⊟ 📦 AmazonEC2ReadO...	AWS managed

AmazonEC2ReadOnlyAccess

Provides read only access to Amazon EC2 via the AWS Management Cons

⎙ **Copy JSON**

```
 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:
12              "Resource": "*"
13          },
14 ▾        {
15              "Effect": "Allow",
16 ▾            "Action": [
17                  "cloudwatch:ListMetrics",
18                  "cloudwatch:GetMetricStatist
19                  "cloudwatch:Describe*"
20              ],
21              "Resource": "*"
```

Choose the **EC2-Admin** group 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**,

| Users | **Permissions** | Access Advisor |

Permissions policies (1) Info

You can attach up to 10 managed policies.

[⟳]

[**Simulate** ↗] [Remove]

[**Add permissions** ▼]

Filter by Type

[🔍 Search] [All ty... ▼]

< **1** >   ⚙

☐	**Policy name** ↗ ▲	**Type**
☐	⊞ EC2-Admin-Policy	Customer inline

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

	Policy name ↗	▲	Type
☐	⊟ EC2-Admin-Policy		Customer inline

EC2-Admin-Policy   📋 Copy JSON

```
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 }
```

Task 2: Add Users to Groups

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.
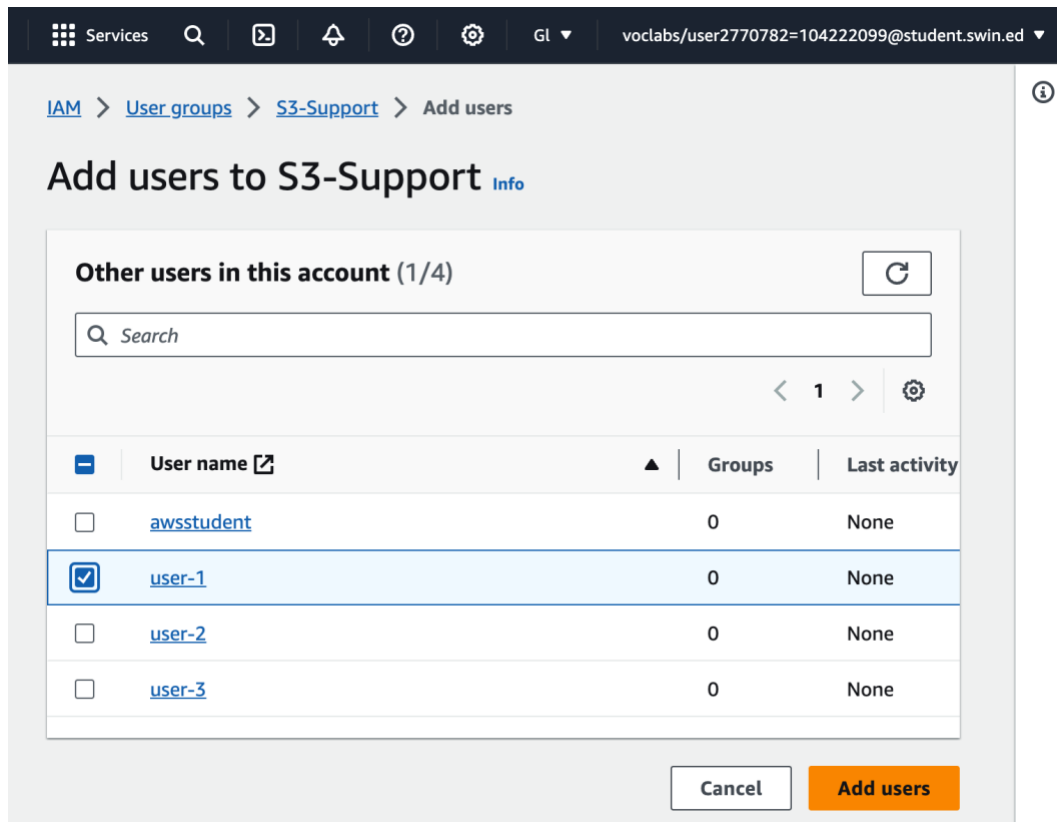
Add user-2 to the EC2-Support Group

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.
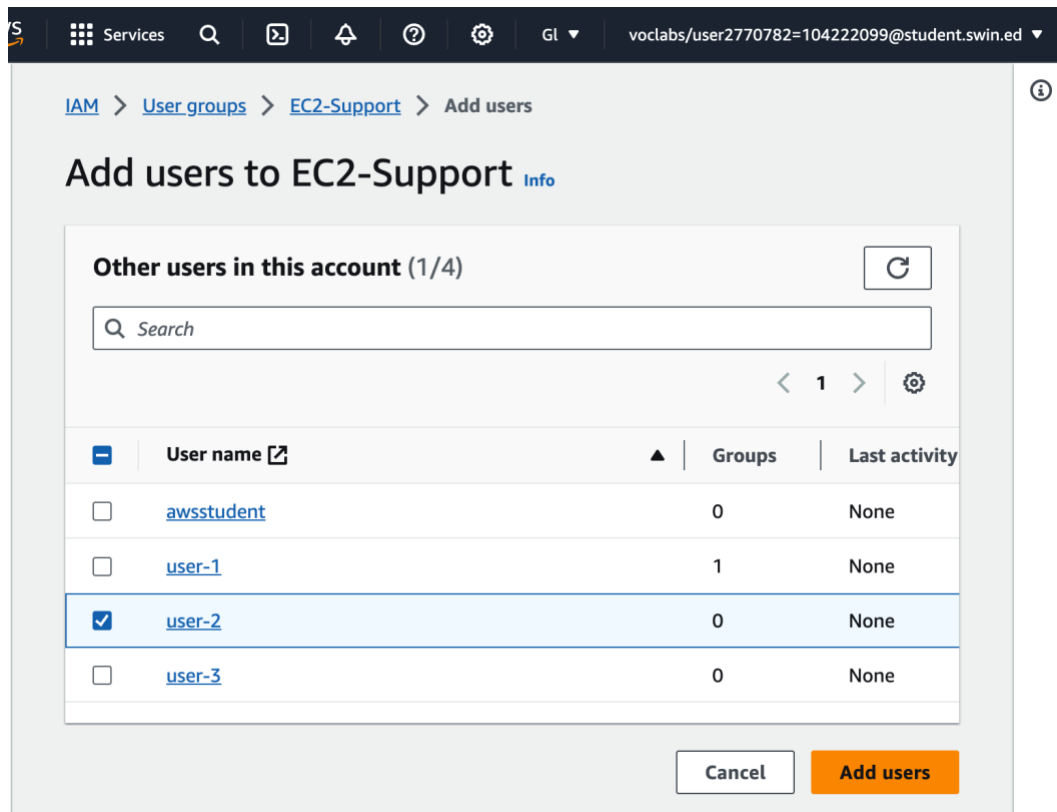
Add user-3 to the EC2-Admin Group

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.
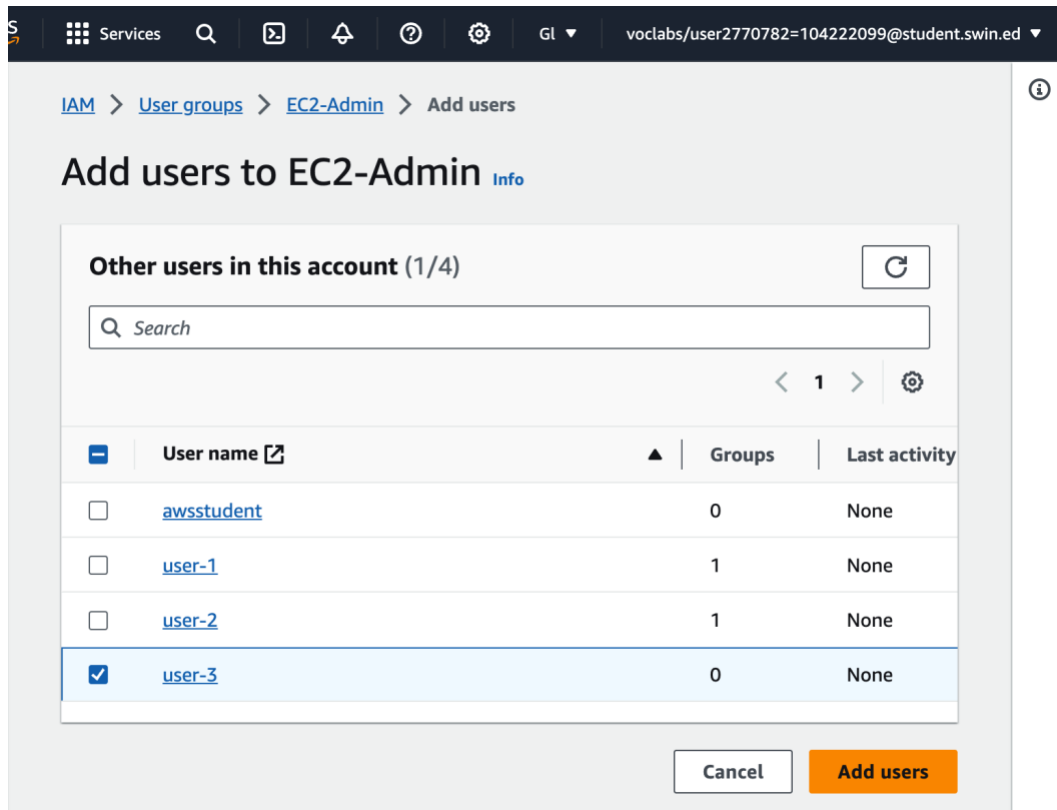
Each Group should now have a **1** in the Users column for the number of Users in each Group.

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.
Sign-in with:

- **IAM user name:** user-1
- **Password:** Lab-Password1
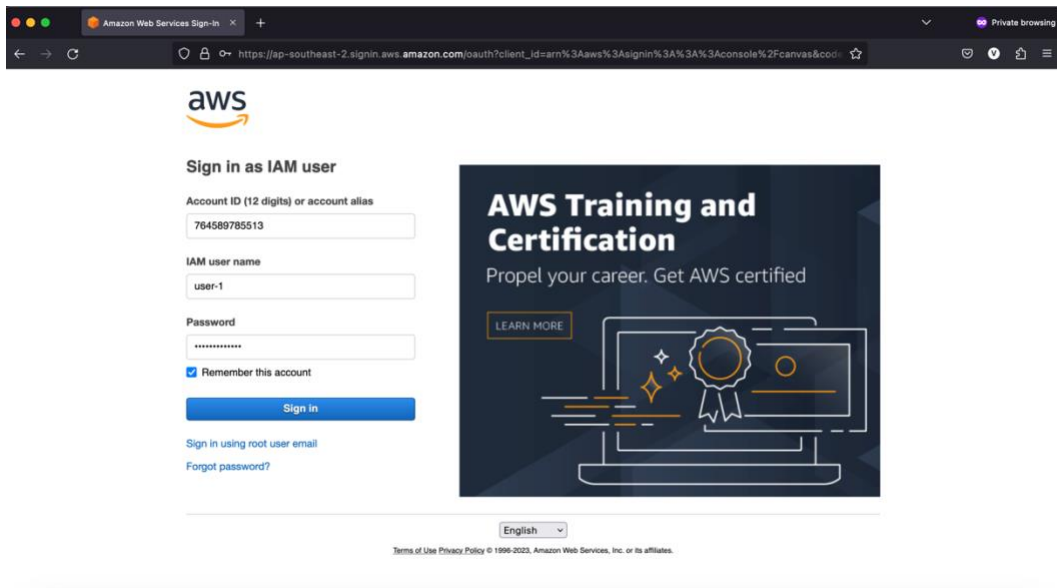
In the **Services** menu, choose **S3**.
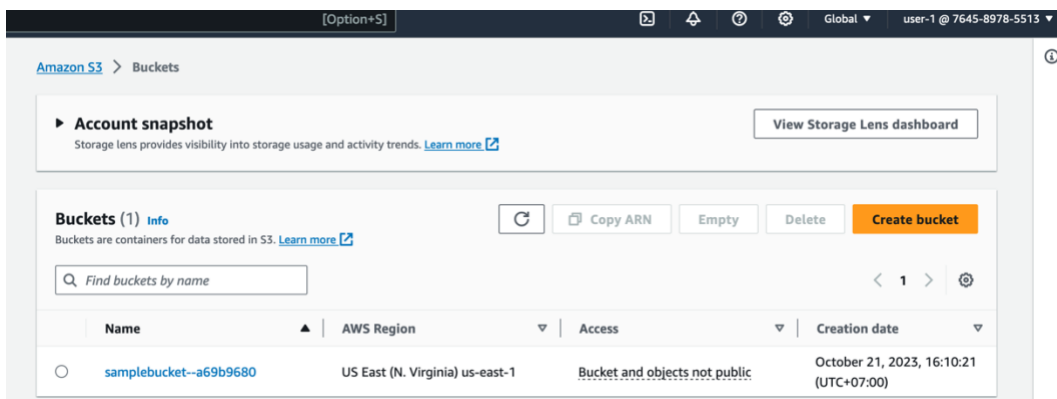
In the **Services** menu, choose **EC2**.
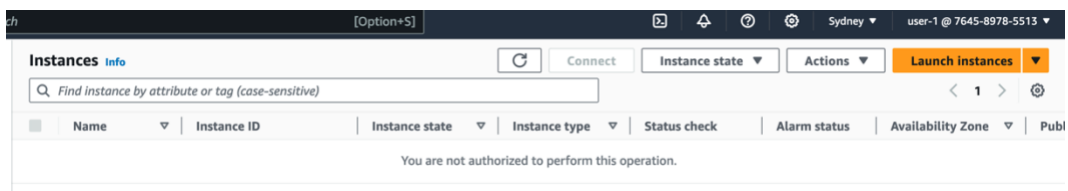
Sign user-1 out of the **AWS Management Console** by completing the following actions:
- At the top of the screen, choose **user-1**
- Choose **Sign Out**

Sign-in with:
- **IAM user name:** user-2
- **Password:** Lab-Password2

In the **Services** menu, choose **EC2**.
- Select the instance named *LabHost*.

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

⊗ Failed to stop the instance i-03adab0781ac33e56

You are not authorized to perform this operation. User: arn:aws:iam::764589785513:user/spl66/user-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:764589785513:instance/i-03adab0781ac33e56 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: dbFcBvtZO6ElFDD3WGviE_c-u2yMRwlkLnKu90TiVKh3NXN9GZ0OGIGScHg5l4mE54LIG1oeGxBkZykERNv_2lvVEEi0wULbpsWCfRzOOZb45xqsPN3UruWdtkWuiPzMv8ArVkigJW9NwP6j0Lz_FqO1JOmyGCqz uR4pnFe8Wlb-qPHOln4g_O8pQRWY6Vauyp0GF7--avltTKSgSHGkhrUJZRtpmDVnMYFqhXr8yvmdVPrY4BeJk8f0uzUEXxPCjjxt3CL8o3Y7NTVYO8B7DIibVk9lQAXxOZxnjag_Dt9cYKAHBnBphh8 CS1lOiuX08by01mzNmzyOiJEwtD23SbsPS2Me5_OojQM139iRxpllxj3IdJF5RI7BmIo4rFnAf3nOAQsyBy40XHwkT3JUplU5UawYTKleZLP6WdPx89KdeoFQZJ9gZIFD0GRwhAGJ8yj 2l_VXXEDc46GCcms1dfTB7HIiP6YJgsRDwf_bTDyn2G9gt4lOGn4267mWM4qdFNrLvdsaZBICaYY9oRn-XYz7YomDIg5xc-w94LW67vCeApZ2iFZnhhzJYV50gIH8hj97ahSQfQxrNwfseQdlhblOrGAZHVhQ2xyxr-_8vf0dq753Jq658nsqJPB-mEl1uXDxaQr-vv0nv443yYr3ytaeQYykVnn8eeJ2eP9L5yP7FIXNkbxQ0DhV5cW8QLwqKl3BlCyyizmbRCri3ev4nLw6Iv45vwICw3m662e04d2blTDZXXzxoUKU2c273HLag1UTDzmgiYT65f9YDzY Ppkbux-UJzphM_SNgdhwCq3wy32g4JtyAGdtbtjou7dnkasmLMP2FEs8VgsdAmE6KXV1-xb1XcAIplGYIaSkwhFsL1MtpXlhdTDhmLN5uj1pAf3KT3k9JzfSkx-dzOKx0JecJFRVOS8RP8O1wQaDVc6uezs2KUfW5uPZiDuL8BA_h-R7x-nWAdQDSUK1Szj0cpLGBiEJWwu2-t7OWv1gctoY

In the **Services**, choose **S3**.

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

Buckets Info

Buckets are containers for data stored in S3. Learn more ⧉

⊗ **You don't have permissions to list buckets**

After you or your AWS administrator has updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3 ⧉

You will now sign-in as **user-3**, who has been hired as your Amazon EC2 administrator.

Sign-in with:

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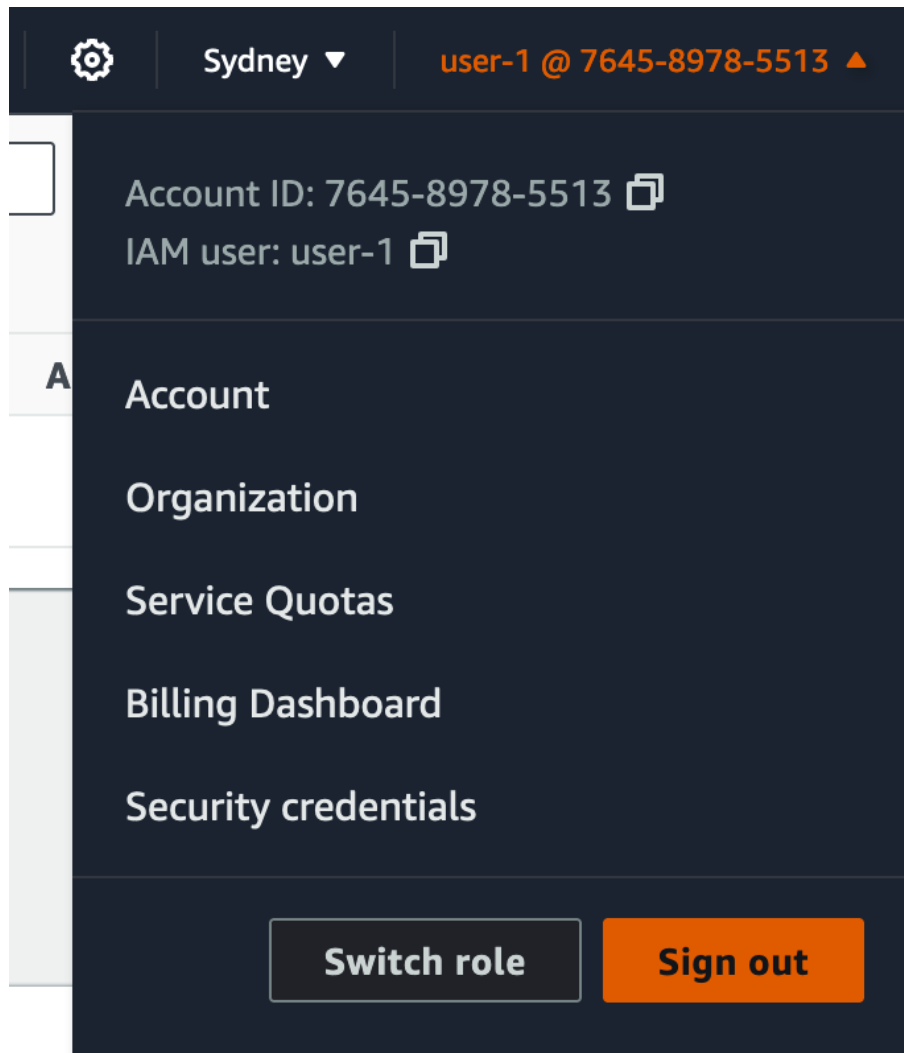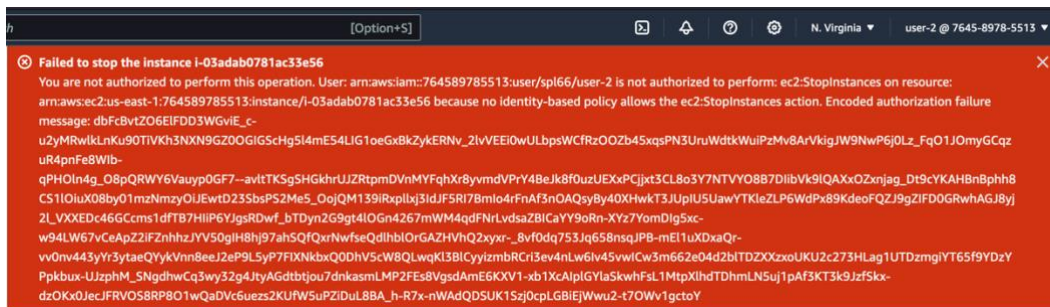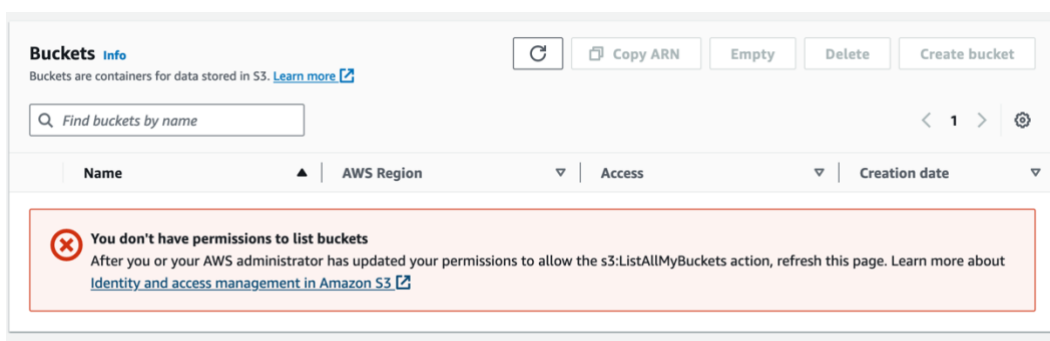- **Password:** Lab-Password3

In the **Services** menu, choose **EC2**.

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

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Publ
Bastion Host	i-020049b293dec1990	⊘ Running	t2.micro	⊘ 2/2 checks passed	⊗ User: arn:aws:i	us-east-1a	ec2-5
LabHost	i-03adab0781ac33e56	⊘ Running	t2.micro	⊘ 2/2 checks passed	⊗ User: arn:aws:i	us-east-1a	ec2-5
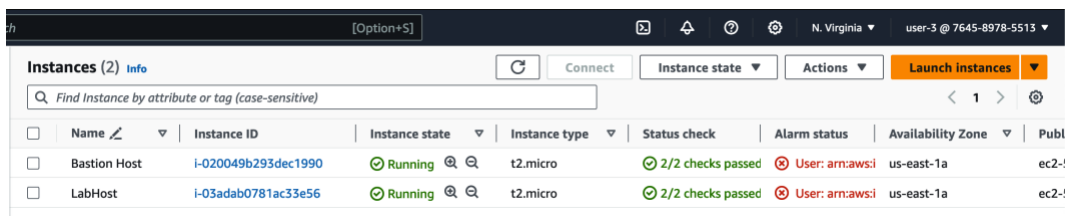
In the **Instance state** menu, choose **Stop instance**.

In the **Stop instance** window, choose **Stop**.

ENDLAB.