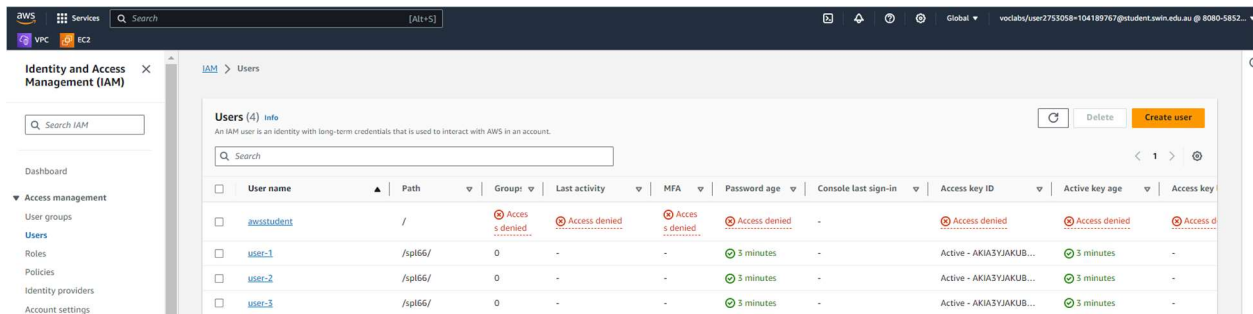


Lab 1: Introduction to AWS IAM

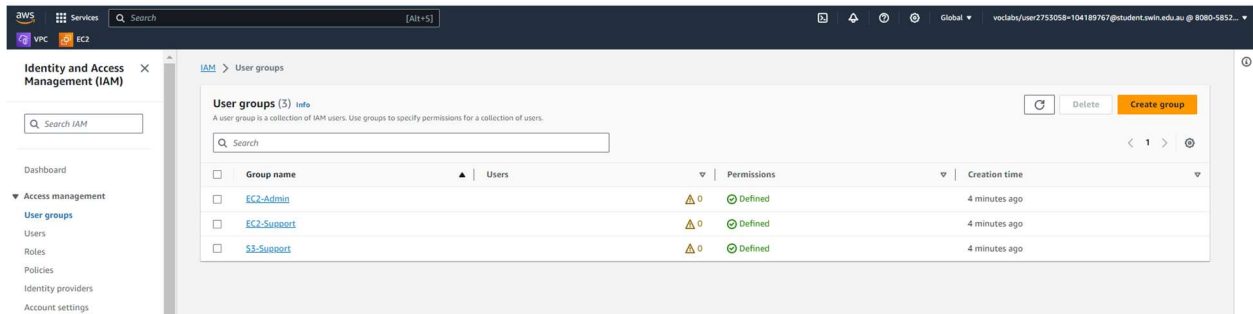
Name: Pham Do Tien Phong

Student ID: 104189767

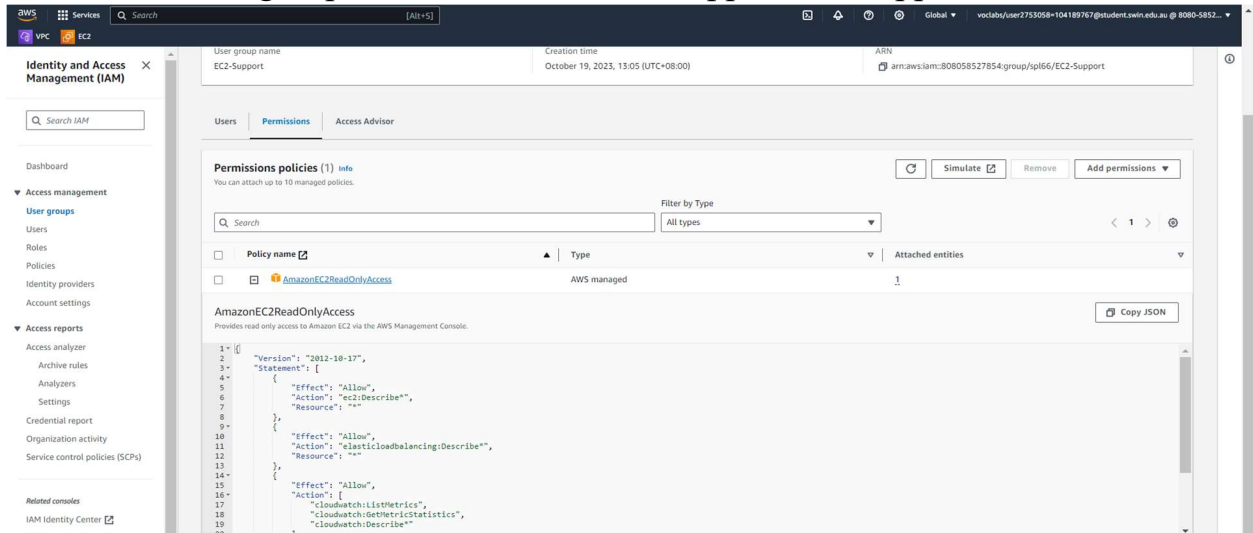
Task 1: Explore the Users and Groups



There are 3 users : user-1 , user-2, user-3



There are 3 user groups : EC2-Admin, EC2-Support, S3-Support



Permission policy of EC2-Support

The screenshot displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'Users' selected under 'Access management'. The main content area shows the 'Summary' tab for the 'S3-Support' user group. The summary includes the user group name, creation time (October 19, 2023, 13:05 UTC+08:00), and ARN (arn:aws:iam::808058527854:group/spi66/S3-Support). Below the summary, the 'Permissions policies' section shows one attached policy: 'AmazonS3ReadOnlyAccess'. The policy details section displays the JSON policy document for 'AmazonS3ReadOnlyAccess', which grants read-only access to all buckets via the AWS Management Console.

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": [
7-         "s3:Get*",
8-         "s3:List*",
9-         "s3:Describe*",
10-        "s3-object-lambda:Get*",
11-        "s3-object-lambda:List*"
12-       ],
13-       "Resource": "*"
14-     }
15-   ]
16- }
```

Permission policy of S3-Support

The screenshot displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'Users' selected under 'Access management'. The main content area shows the 'Summary' tab for the 'EC2-Admin' user group. The summary includes the user group name, creation time (October 19, 2023, 13:05 UTC+08:00), and ARN (arn:aws:iam::808058527854:group/spi66/EC2-Admin). Below the summary, the 'Permissions policies' section shows one attached policy: 'EC2-Admin-Policy'. The policy details section displays the JSON policy document for 'EC2-Admin-Policy', which grants permissions to describe, start, and stop EC2 instances.

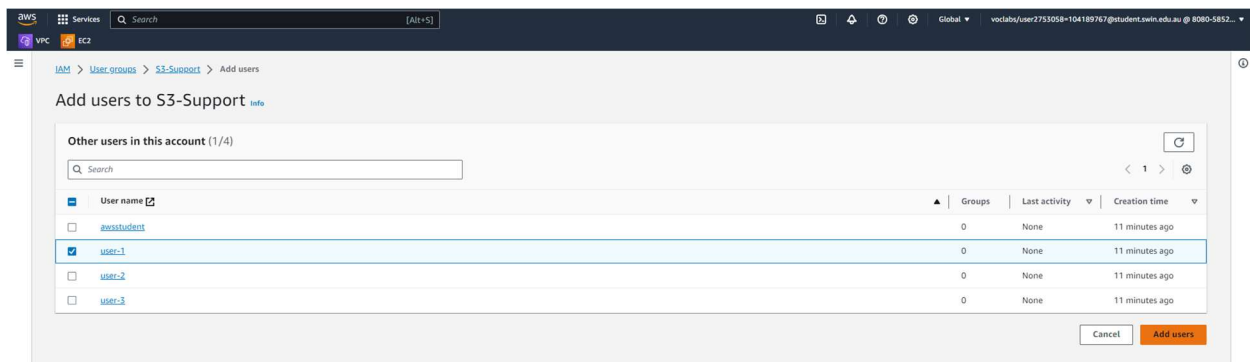
```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Action": [
6-         "ec2:Describe*",
7-         "ec2:StartInstances",
8-         "ec2:StopInstances"
9-       ],
10-      "Resource": [
11-        "*"
12-      ],
13-      "Effect": "Allow"
14-     }
15-   ]
16- }
```

Permission policy of EC2-Admin

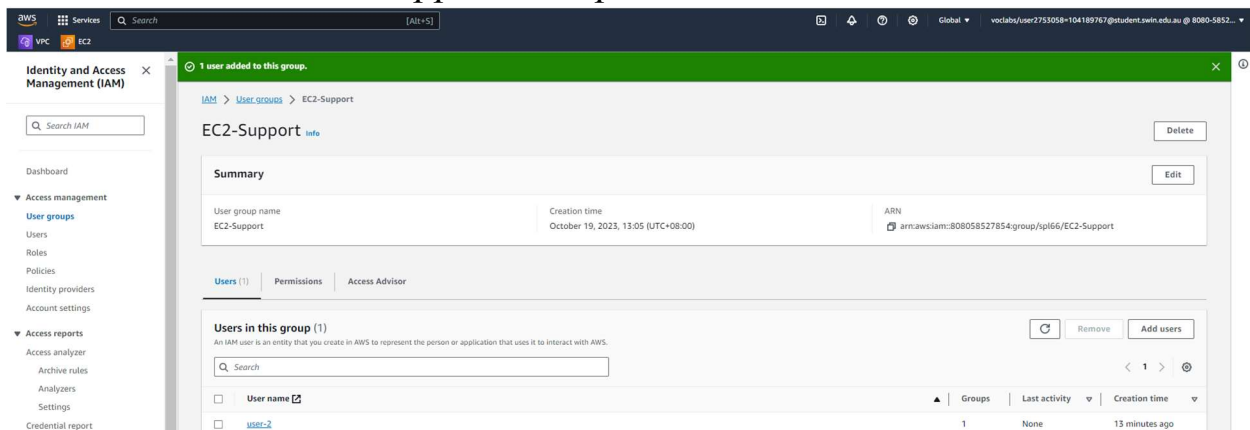
Business Scenario

Task 2: Add Users to Groups

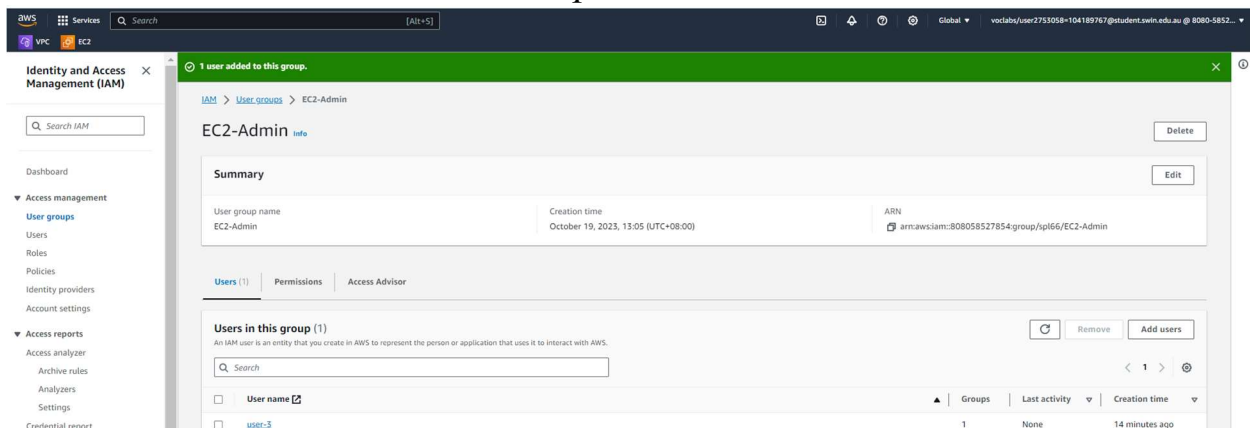
Add user-1 to the S3-Support Group



I add user-1 to S3-Support
Add user-2 to the EC2-Support Group

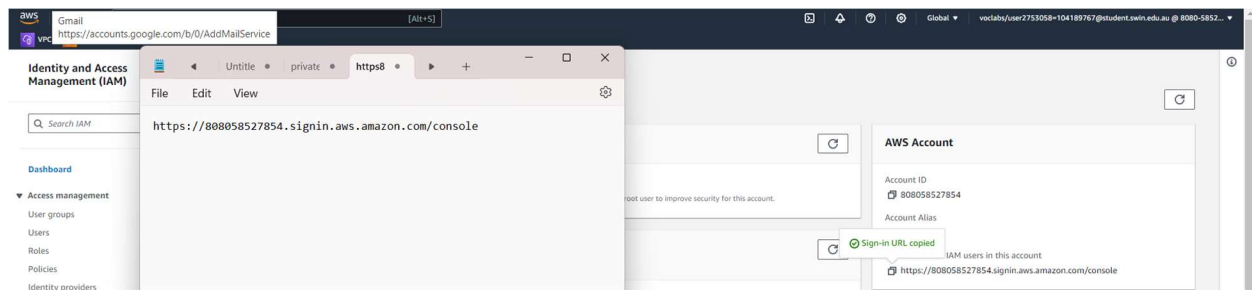


I add user-2 to EC2-Support with the same steps.
Add user-3 to the EC2-Admin Group

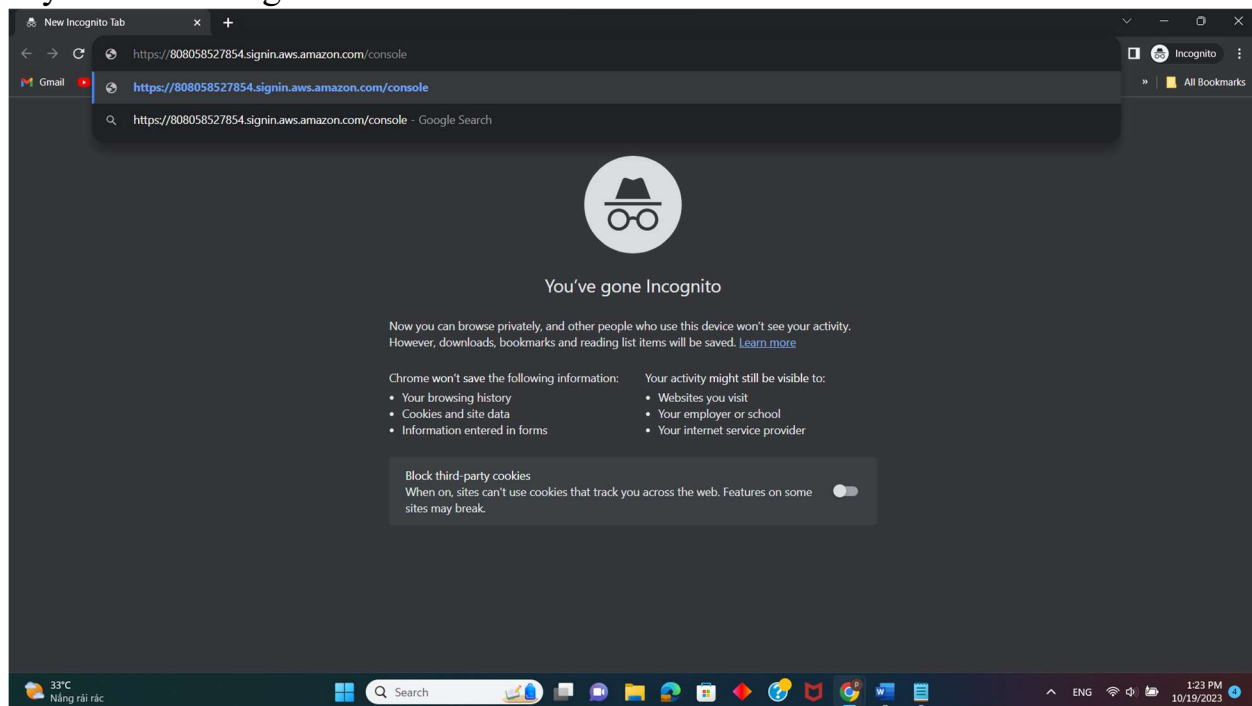


I add user-3 to EC2-Admin with the same steps.

Task 3: Sign-In and Test Users



My IAM users sign-in link



Open an Incognito Window and paste IAM users sign-in link



Sign in as IAM user

Account ID (12 digits) or account alias

808058527854

IAM user name

user-1

Password

.....

☐ Remember this account

Sign-in with the user name is user-1 and Password is Lab-Password1

The screenshot shows the Amazon S3 console interface. On the left is a navigation sidebar with options like Buckets, Access Points, and IAM Access Analyzer for S3. The main content area displays an 'Account snapshot' section with a 'View Storage Lens dashboard' button. Below this is a 'Buckets (1)' section with a search bar and a table of buckets. The table has columns for Name, AWS Region, Access, and Creation date. One bucket is listed: 'samplebucket-ff541e20' in 'US East (N. Virginia) us-east-1' with 'Bucket and objects not public' access, created on 'October 19, 2023, 13:04:40 (UTC+08:00)'. Action buttons like 'Copy ARN', 'Empty', 'Delete', and 'Create bucket' are visible.

Name	AWS Region	Access	Creation date
samplebucket-ff541e20	US East (N. Virginia) us-east-1	Bucket and objects not public	October 19, 2023, 13:04:40 (UTC+08:00)

S3 bucket in the user1 account.

The screenshot shows the AWS IAM console 'Instances' page. The top navigation bar includes the AWS logo, Services menu, Search bar, and user information 'user-1 @ 8080-5852-7854'. The left sidebar shows navigation options like EC2 Dashboard, EC2 Global View, and Instances. The main content area has a search bar and a table with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. A message states 'You are not authorized to perform this operation.' Below the table is a horizontal scrollbar.

I can't see any instance in this account.



Sign in as IAM user

Account ID (12 digits) or account alias

808058527854

IAM user name

user-2

Password

.....

☐ Remember this account

Sign in

Sign out user-1 account and sign-in user-2 account with username: user-2 and Password:Lab-Password2

The screenshot shows the AWS Management Console interface for the user-2 account. The 'Instances' page is active, displaying a table with two instances: 'LabHost' and 'Bastion Host'. Both instances are in the 'Running' state. The 'LabHost' instance has an ID of 'i-0fe3a6077a9e7a19b' and is of type 't2.micro'. The 'Bastion Host' instance has an ID of 'i-0066f0a8e64b5be72' and is also of type 't2.micro'. The table includes columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4 address, Elastic IP, and IPv6 IPs.

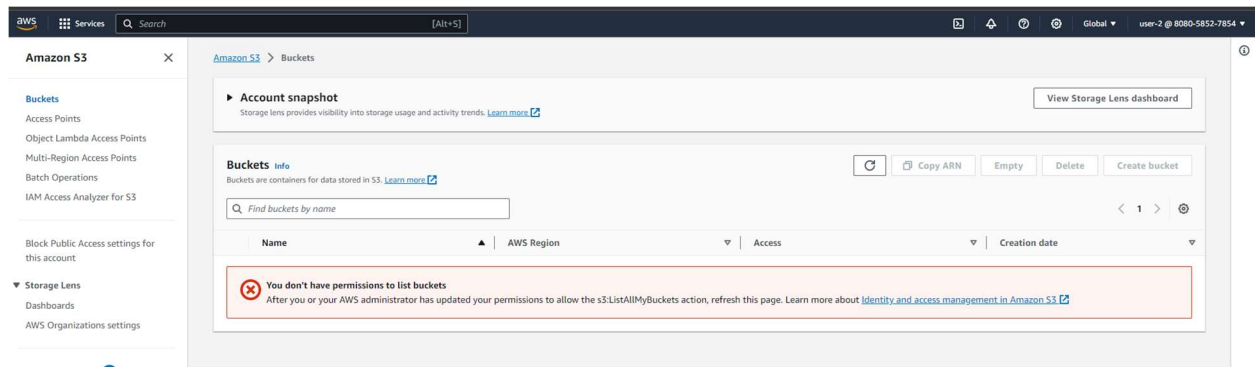
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
LabHost	i-0fe3a6077a9e7a19b	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-3-238-3-209.comp...	3.238.3.209	-	-
Bastion Host	i-0066f0a8e64b5be72	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-18-207-183-179.co...	18.207.183.179	-	-

There are 2 instances in the user-2 account.

The screenshot shows the AWS Management Console interface with an error message displayed. The error message states: 'Failed to stop the instance i-0fe3a6077a9e7a19b. You are not authorized to perform this operation. Encoded authorization failure message: ...'. Below the error message, the 'Instances' table is visible, showing the 'LabHost' instance in the 'Running' state. The 'Bastion Host' instance is also in the 'Running' state.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
LabHost	i-0fe3a6077a9e7a19b	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-3-238-3-209.comp...	3.238.3.209	-	-
Bastion Host	i-0066f0a8e64b5be72	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-18-207-183-179.co...	18.207.183.179	-	-

I fail to stop LabHost instance



I don't have permission in list buckets.



Sign in as IAM user

Account ID (12 digits) or account alias

808058527854

IAM user name

user-3

Password

.....

☐ Remember this account

Sign in

I sign-out user-2 account and sign-in user-3 account.

Successfully stopped i-0fe3a6077a9e7a19b

Instances (1/2) info

Find Instance by attribute or tag (case-sensitive)

Connect Instance state Actions Launch instances Refresh instances

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
<input checked="" type="checkbox"/>	LabHost	i-0fe3a6077a9e7a19b	Stopped	t2.micro	-	User: amawesl	us-east-1a	-	-	-	-
<input type="checkbox"/>	Bastion Host	i-0066f0a8e64b5be72	Running	t2.micro	2/2 checks passed	User: amawesl	us-east-1a	ec2-18-207-183-179.co...	18.207.183.179	-	-

I can stop LabHost instance in user-3 account.