COS20019 - Cloud Computing Architecture

Week 6: ACF Lab 1: Intro to AWS IAM

Author: Trac Duc Anh Luong - ID: 103488117

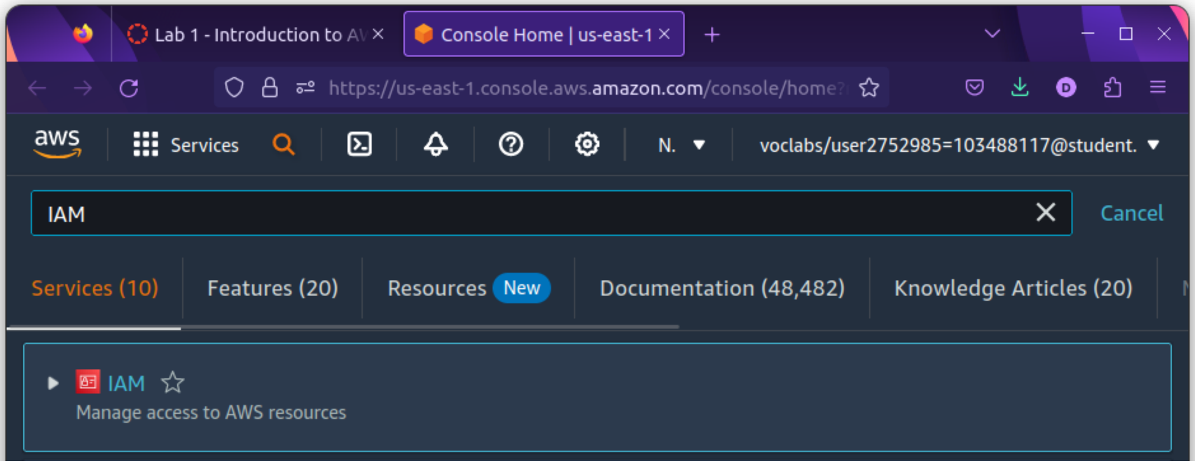
Due Date: 15/10/2023

Name: Trac Duc Anh Luong - ID: 103488117

Task 1: Explore the Users and Groups

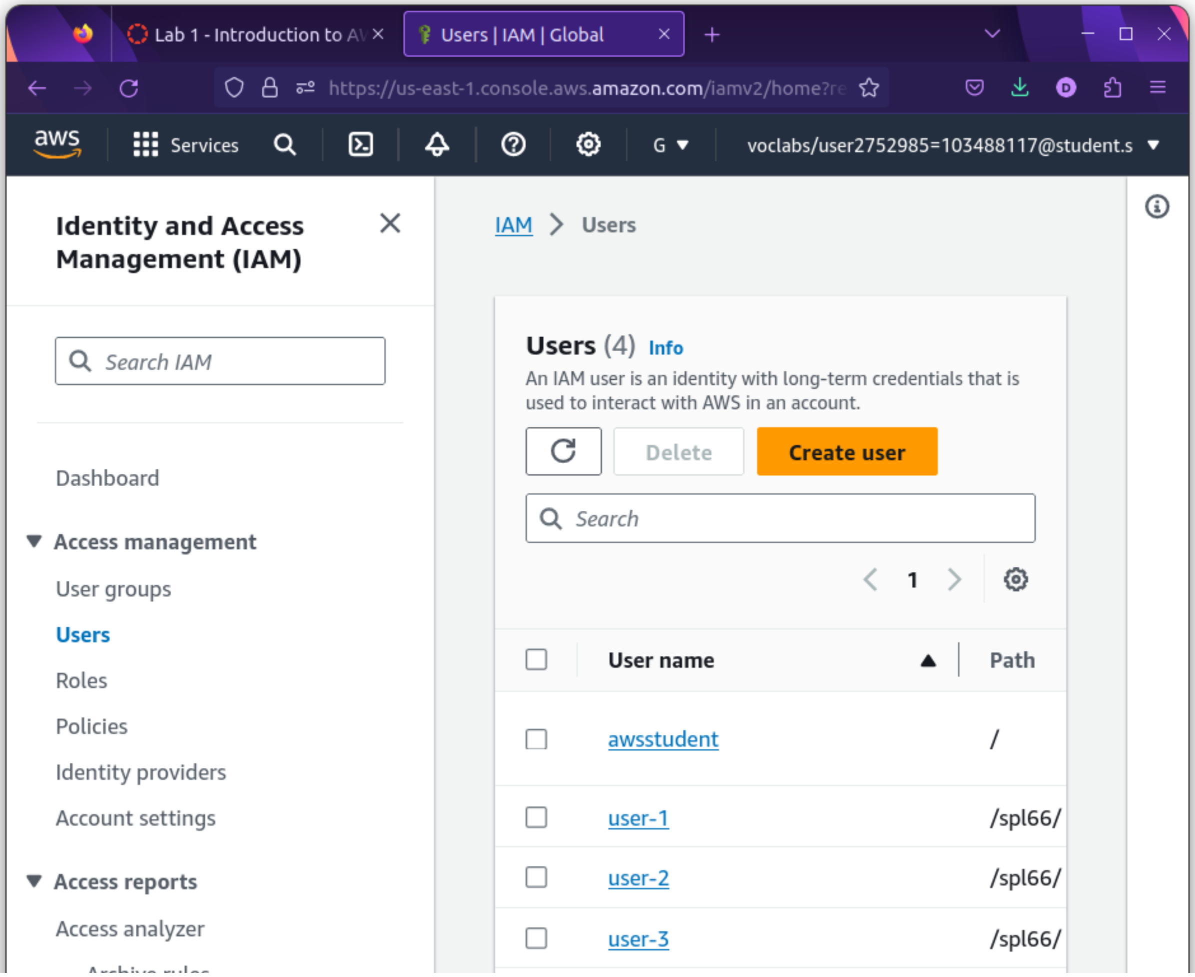
In this task, you will explore the Users and Groups that have already been created for you in IAM.

5. In the **AWS Management Console**, on the **Services** menu, select **IAM**.


Lab 1 - Introduction to A
Console Home | us-east-1
https://us-east-1.console.aws.amazon.com/console/home?
aws
Services
N.
voclabs/user2752985=103488117@student.
IAM
Cancel
Services (10)
Features (20)
Resources New
Documentation (48,482)
Knowledge Articles (20)
IAM
Manage access to AWS resources

6. In the navigation pane on the left, choose **Users**.
   The following IAM Users have been created for you:
   - user-1
   - user-2
   - user-3

Name: Trac Duc Anh Luong - ID: 103488117



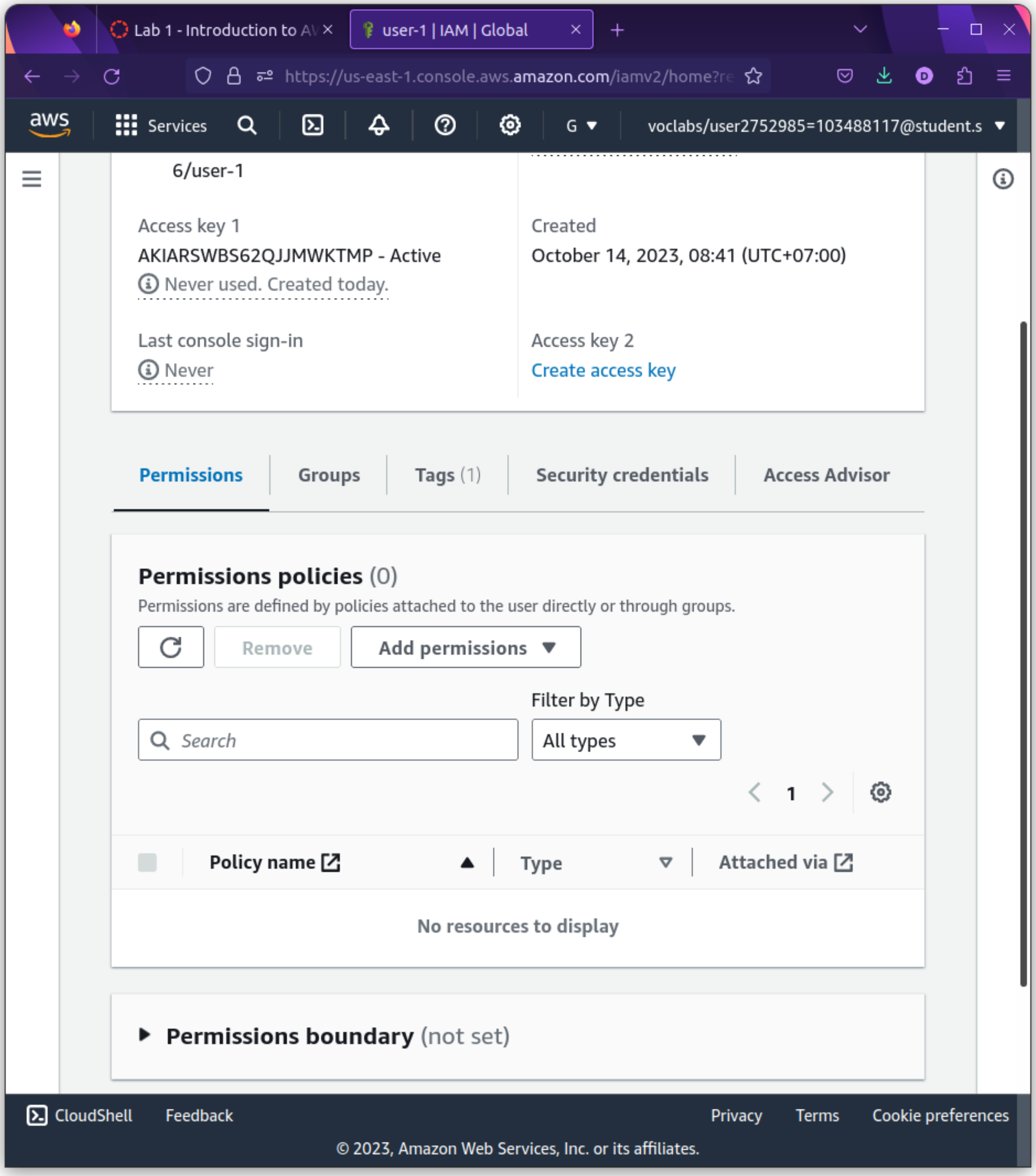
Users (4)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

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

Name: Trac Duc Anh Luong - ID: 103488117

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



Lab 1 - Introduction to A\
user-1 | IAM | Global
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s

6/user-1

Access key 1
AKIARSWBS62QJJMWKTMP - Active
Never used. Created today.

Created
October 14, 2023, 08:41 (UTC+07:00)

Last console sign-in
Never

Access key 2
Create access key

Permissions policies (0)

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

Policy name	Type	Attached via
No resources to display		

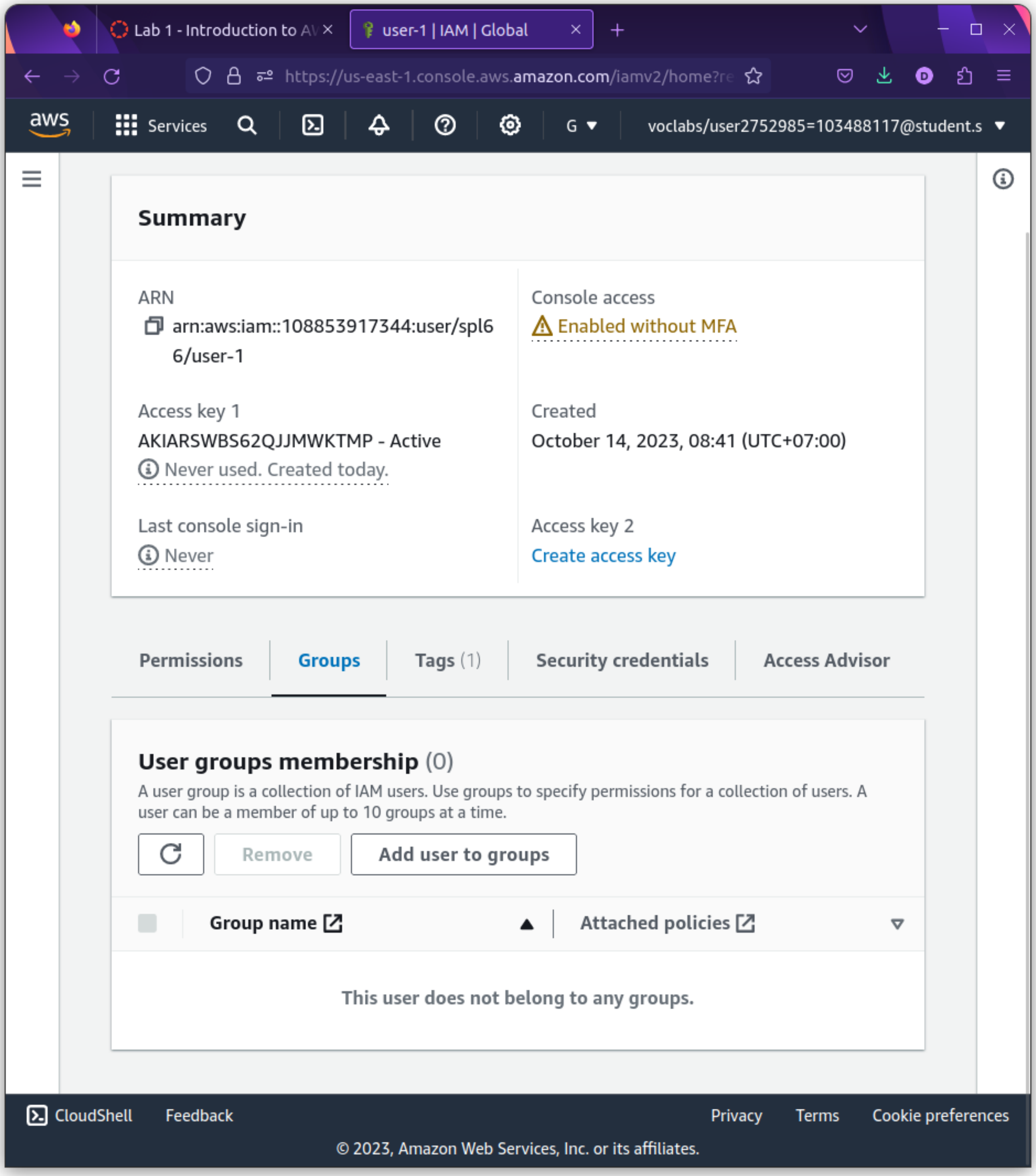
Permissions boundary (not set)

© 2023, Amazon Web Services, Inc. or its affiliates.

8. Notice that user-1 does not have any permissions.

Name: Trac Duc Anh Luong - ID: 103488117

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



Lab 1 - Introduction to A
user-1 | IAM | Global
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s

Summary

ARN
arn:aws:iam::108853917344:user/spl66/user-1

Console access
Enabled without MFA

Access key 1
AKIARSWBS62QJJMWKTMP - Active
Never used. Created today.

Created
October 14, 2023, 08:41 (UTC+07:00)

Last console sign-in
Never

Access key 2
Create access key

Permissions
Groups
Tags (1)
Security credentials
Access Advisor

User groups membership (0)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.

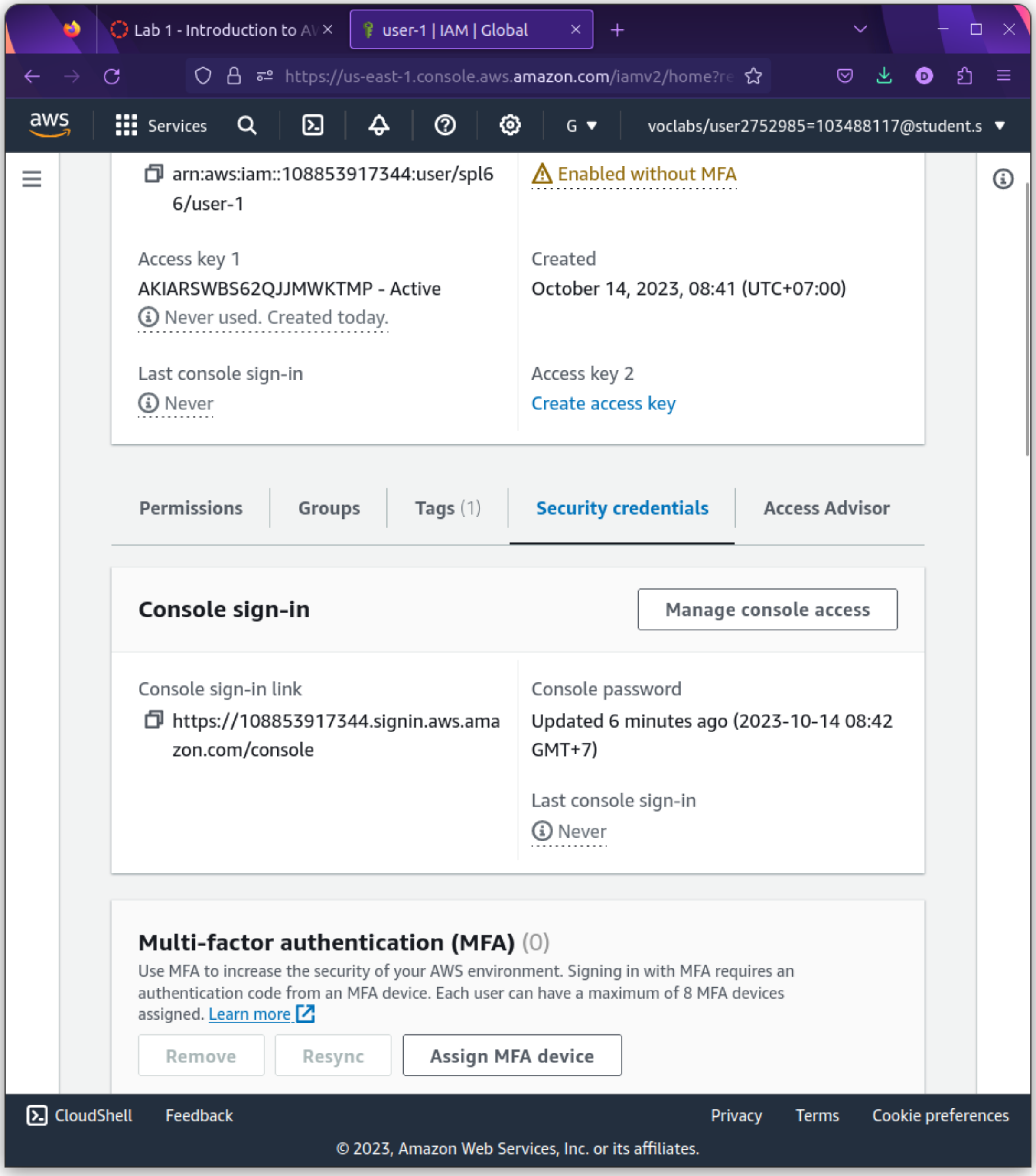
□	Group name	Attached policies

This user does not belong to any groups.

© 2023, Amazon Web Services, Inc. or its affiliates.

Name: Trac Duc Anh Luong - ID: 103488117

10. Choose the **Security credentials** tab.
    user-1 is assigned a **Console password**



Lab 1 - Introduction to A\
user-1 | IAM | Global
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s

arn:aws:iam::108853917344:user/spl66/user-1

⚠ Enabled without MFA

Access key 1
AKIARSWBS62QJJMWKTMP - Active
Never used. Created today.

Created
October 14, 2023, 08:41 (UTC+07:00)

Last console sign-in
Never

Access key 2
Create access key

Permissions
Groups
Tags (1)
Security credentials
Access Advisor

Console sign-in

Console sign-in link
https://108853917344.signin.aws.amazon.com/console

Console password
Updated 6 minutes ago (2023-10-14 08:42 GMT+7)

Last console sign-in
Never

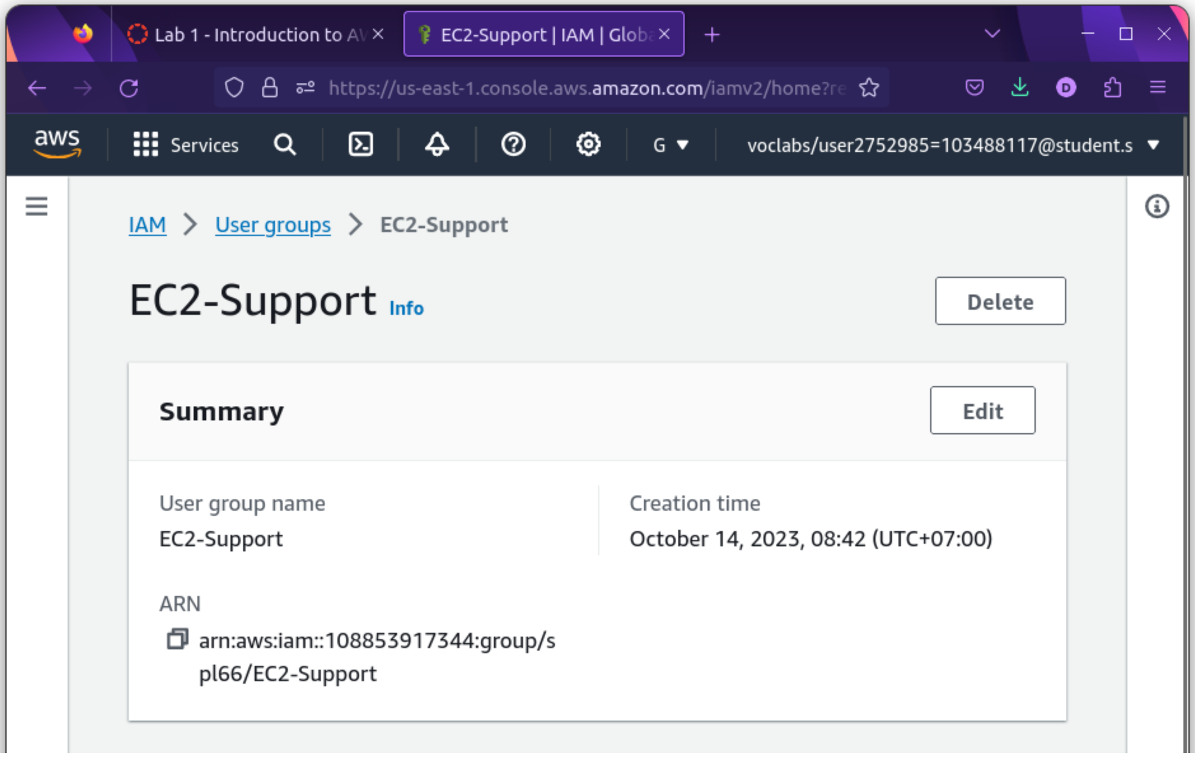
Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

© 2023, Amazon Web Services, Inc. or its affiliates.

11. 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

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


Lab 1 - Introduction to A
EC2-Support | IAM | Glob
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s

IAM > User groups > EC2-Support

EC2-Support Info

Delete

Summary

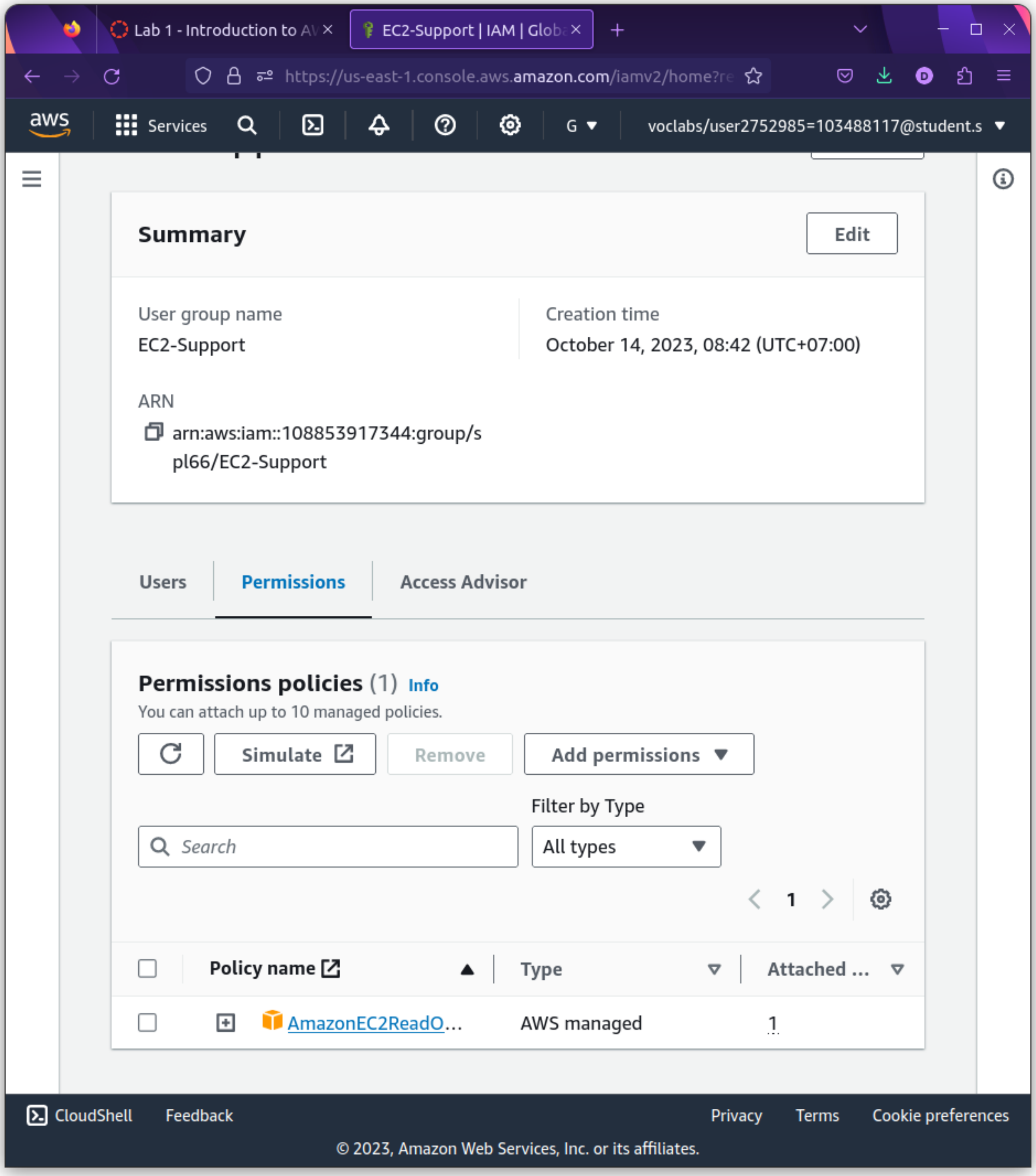
Edit

User group name
EC2-Support

Creation time
October 14, 2023, 08:42 (UTC+07:00)

ARN
arn:aws:iam::108853917344:group/spl66/EC2-Support

13. 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.



Lab 1 - Introduction to A\
EC2-Support | IAM | Glob
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s
Edit
Users
Permissions
Access Advisor
Info
Simulate
Remove
Add permissions
Search
1
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

Summary

User group name
EC2-Support

Creation time
October 14, 2023, 08:42 (UTC+07:00)

ARN
arn:aws:iam::108853917344:group/spl66/EC2-Support

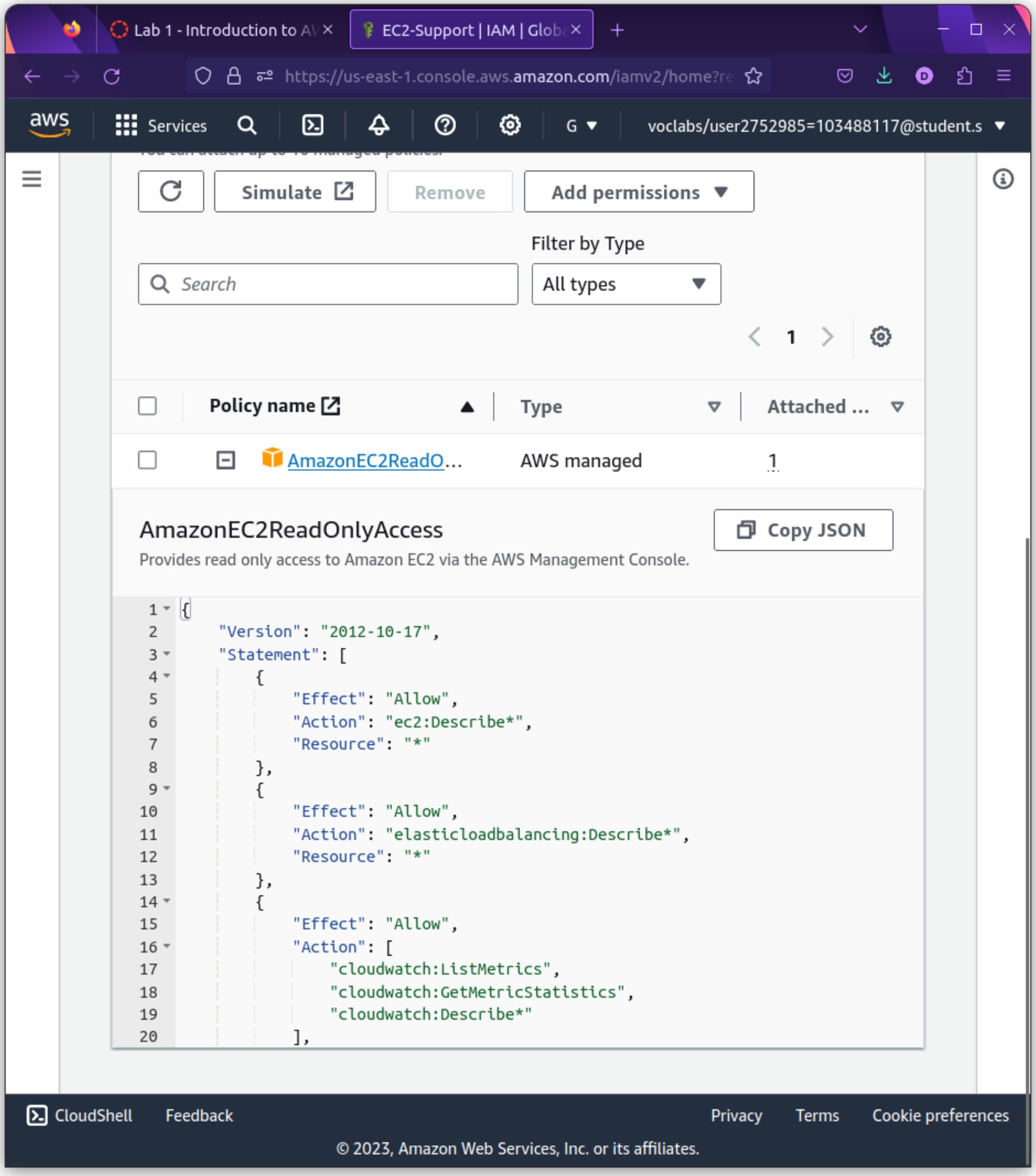
Permissions policies (1)

You can attach up to 10 managed policies.

Filter by Type
All types

□	Policy name	Type	Attached ...
□	AmazonEC2ReadO...	AWS managed	1

14. 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*).


Lab 1 - Introduction to A
EC2-Support | IAM | Glob
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s
Simulate
Remove
Add permissions
Filter by Type
Search
All types
1
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

□	Policy name	Type	Attached ...
□	AmazonEC2ReadO…	AWS managed	1

AmazonEC2ReadOnlyAccess

Provides read only access to Amazon EC2 via the AWS Management Console.

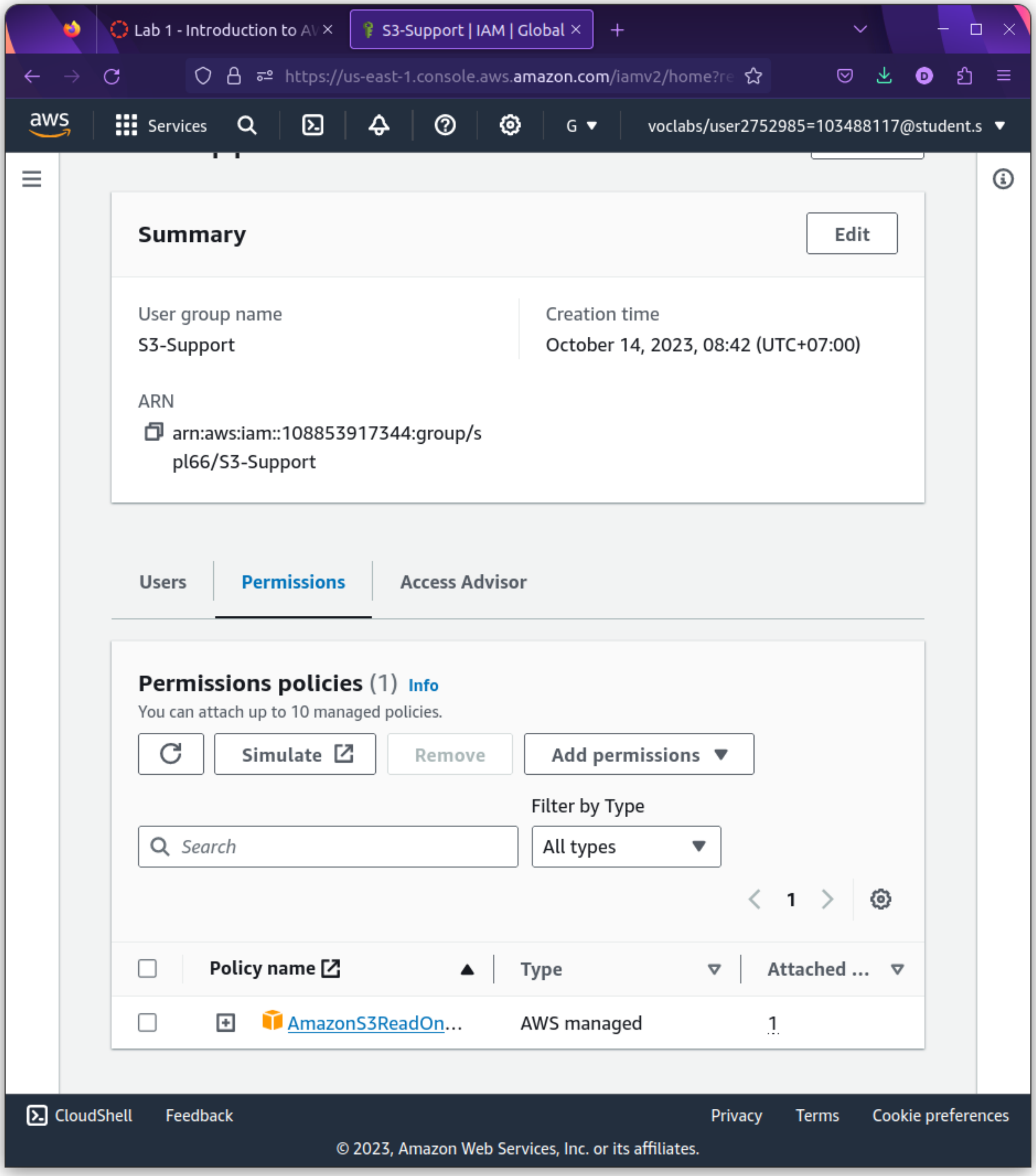
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:Describe*"
            ],
```

15. Choose the minus icon (-) to hide the policy details.

16. In the navigation pane on the left, choose **User groups**.

Name: Trac Duc Anh Luong - ID: 103488117

17. Choose the **S3-Support** group and then choose the **Permissions** tab.
    The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.



Lab 1 - Introduction to A
S3-Support | IAM | Global
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s

Summary Edit

User group name
S3-Support

Creation time
October 14, 2023, 08:42 (UTC+07:00)

ARN
arn:aws:iam::108853917344:group/spl66/S3-Support

Permissions policies (1) Info

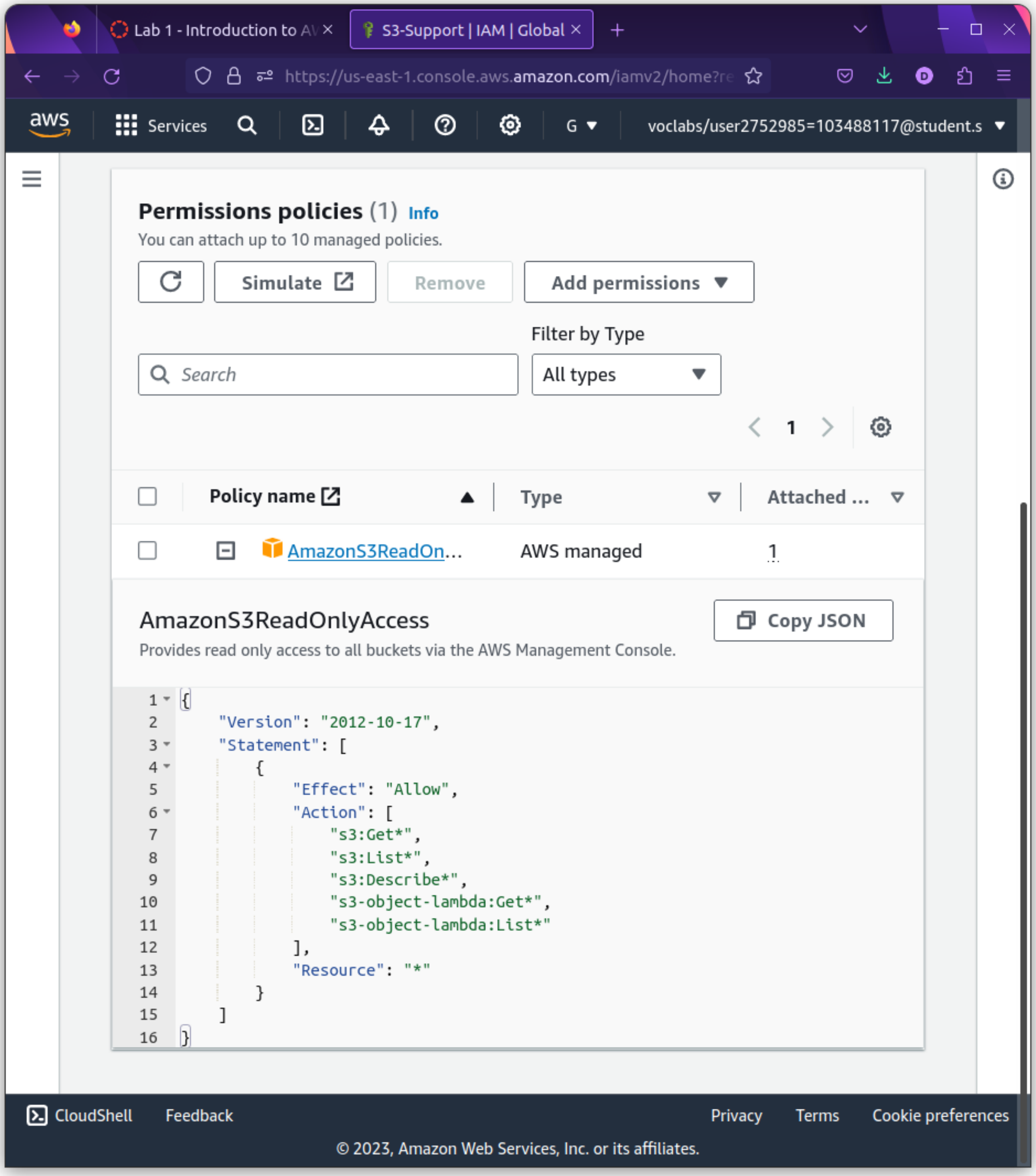
You can attach up to 10 managed policies.

□	Policy name	Type	Attached ...
□	AmazonS3ReadOn...	AWS managed	1

© 2023, Amazon Web Services, Inc. or its affiliates.

Name: Trac Duc Anh Luong - ID: 103488117

18. Choose the plus (+) icon to view the policy details.
    This policy grants permissions to Get and List resources in Amazon S3.


Lab 1 - Introduction to A
S3-Support | IAM | Global
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s
Simulate
Remove
Add permissions
Search
Filter by Type
All types
1
Copy JSON
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

Permissions policies (1) Info

You can attach up to 10 managed policies.

□	Policy name	Type	Attached ...
□	AmazonS3ReadOn...	AWS managed	1

AmazonS3ReadOnlyAccess

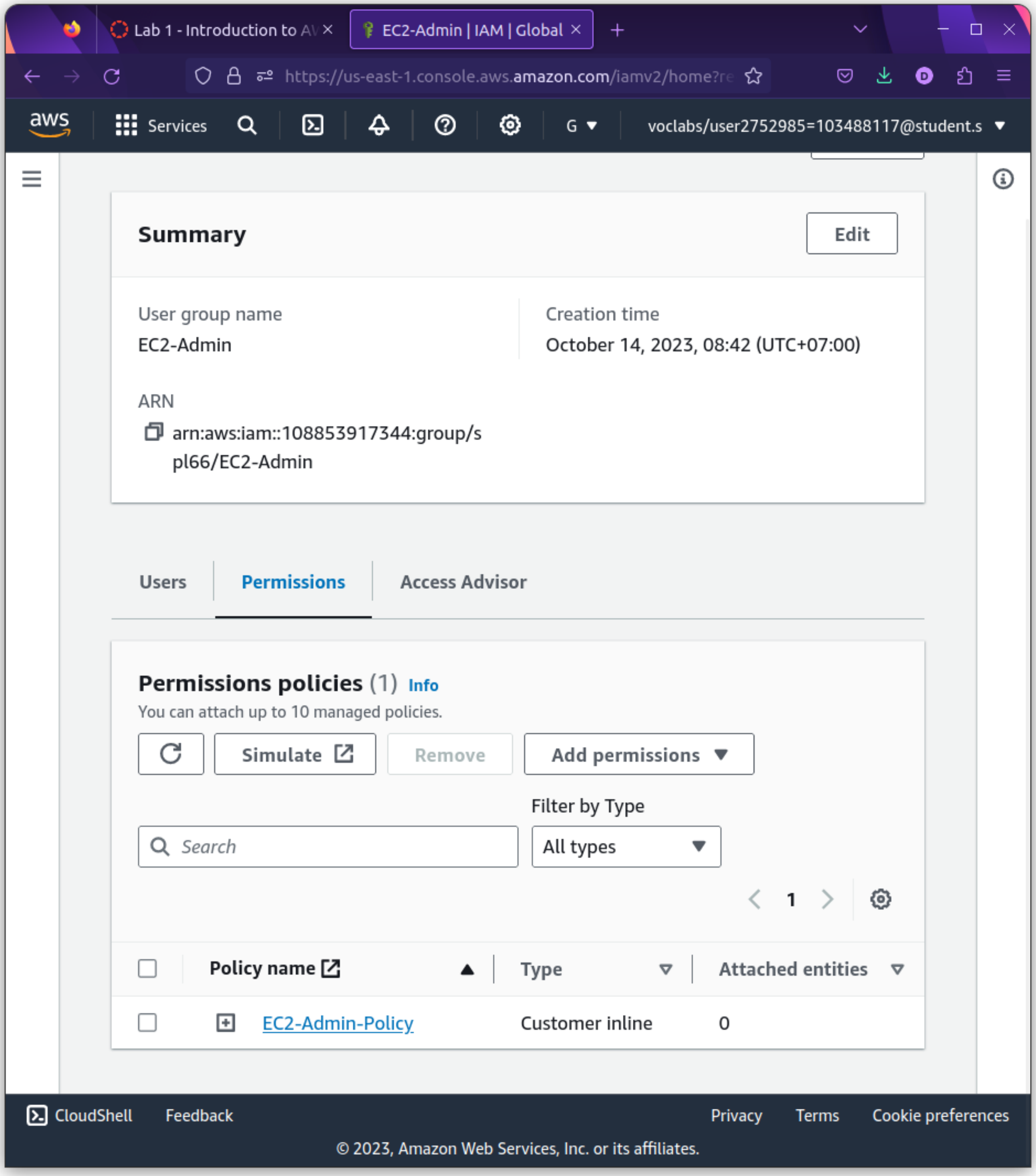
Provides read only access to all buckets via the AWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*",
                "s3:Describe*",
                "s3-object-lambda:Get*",
                "s3-object-lambda:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

19. Choose the minus icon (-) to hide the policy details.

20. In the navigation pane on the left, choose **User groups**.

21. 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**, which is a policy assigned to just one User or Group. Inline Policies are typically used to apply permissions for one-off situations.


Lab 1 - Introduction to A
EC2-Admin | IAM | Global
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s
Edit
Users
Permissions
Access Advisor
Info
Simulate
Remove
Add permissions
Search
1
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

Summary

User group name
EC2-Admin

Creation time
October 14, 2023, 08:42 (UTC+07:00)

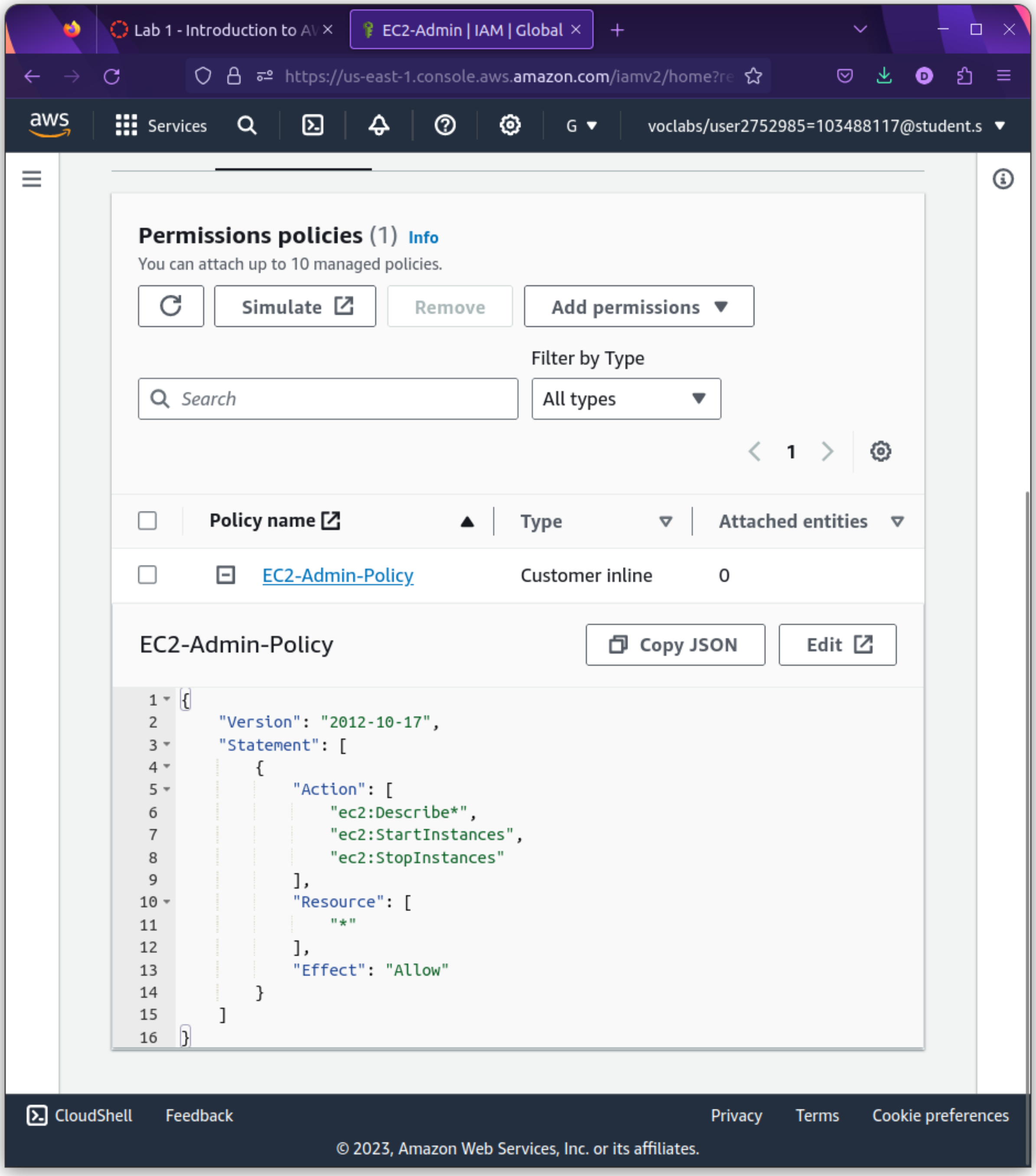
ARN
arn:aws:iam::108853917344:group/spl66/EC2-Admin

Permissions policies (1)
You can attach up to 10 managed policies.

Filter by Type: All types

	Policy name	Type	Attached entities
□	EC2-Admin-Policy	Customer inline	0

22. Choose the plus (+) icon to view the policy details.
    This policy grants permission to view (Describe) information about Amazon EC2 and also the ability to Start and Stop instances.


Lab 1 - Introduction to A
EC2-Admin | IAM | Global
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type

All types ▼

□	Policy name ▲	Type	Attached entities
□	⊟ EC2-Admin-Policy	Customer inline	0

EC2-Admin-Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:Describe*",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

© 2023, Amazon Web Services, Inc. or its affiliates.

23. Choose the minus icon (-) to hide the policy details.

Name: Trac Duc Anh Luong - ID: 103488117

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

24. In the left navigation pane, choose **User groups**.

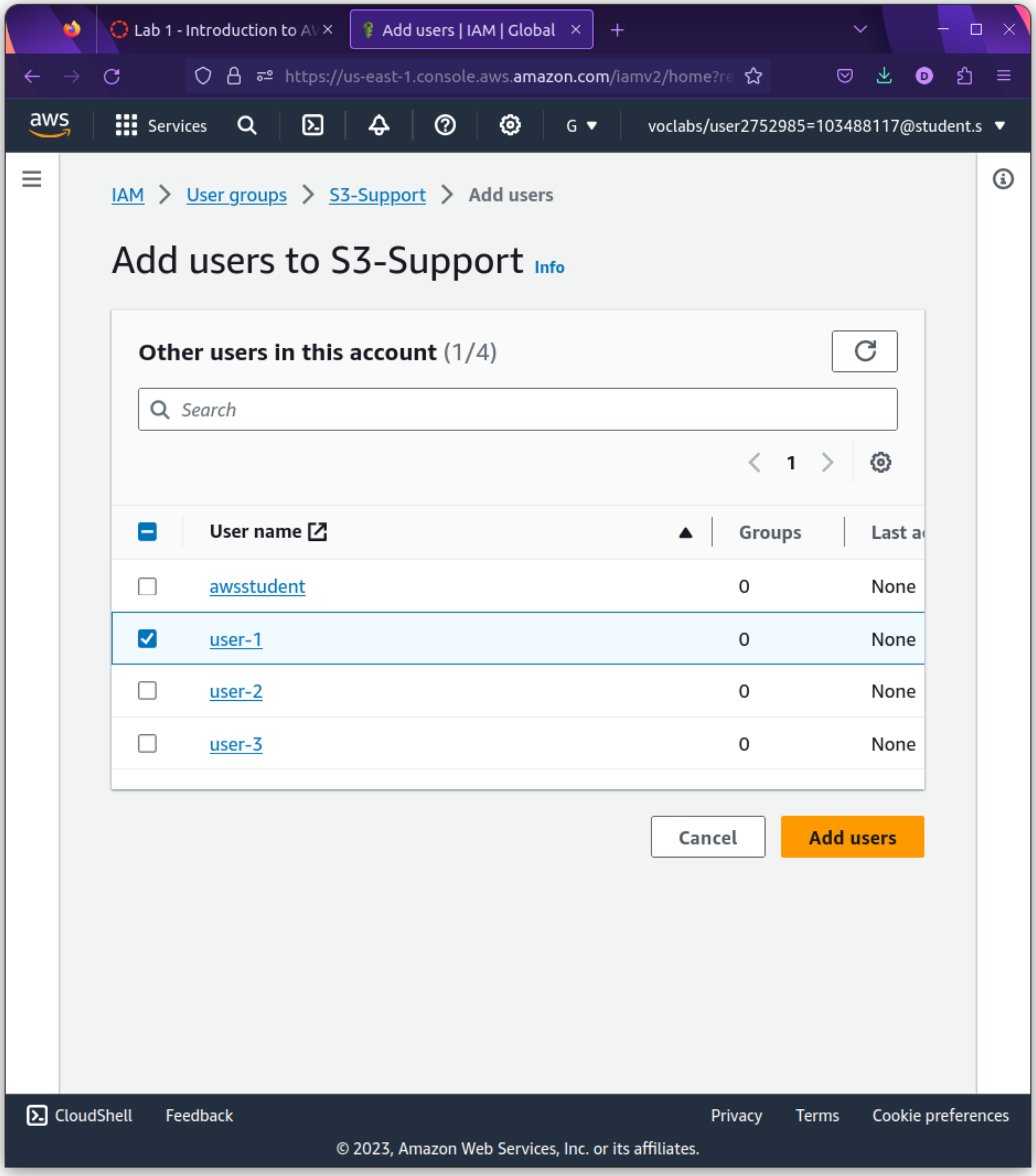
25. Choose the **S3-Support** group.

26. Choose the **Users** tab.

27. In the **Users** tab, choose **Add users**.

28. In the **Add Users to S3-Support** window, configure the following:
    - Select **user-1**.
    - At the bottom of the screen, choose **Add Users**.

Name: Trac Duc Anh Luong - ID: 103488117


Lab 1 - Introduction to A
Add users | IAM | Global
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

IAM > User groups > S3-Support > Add users

Add users to S3-Support Info

Other users in this account (1/4)

Search

< 1 >

	User name	Groups	Last a
□	awsstudent	0	None
☑	user-1	0	None
□	user-2	0	None
□	user-3	0	None

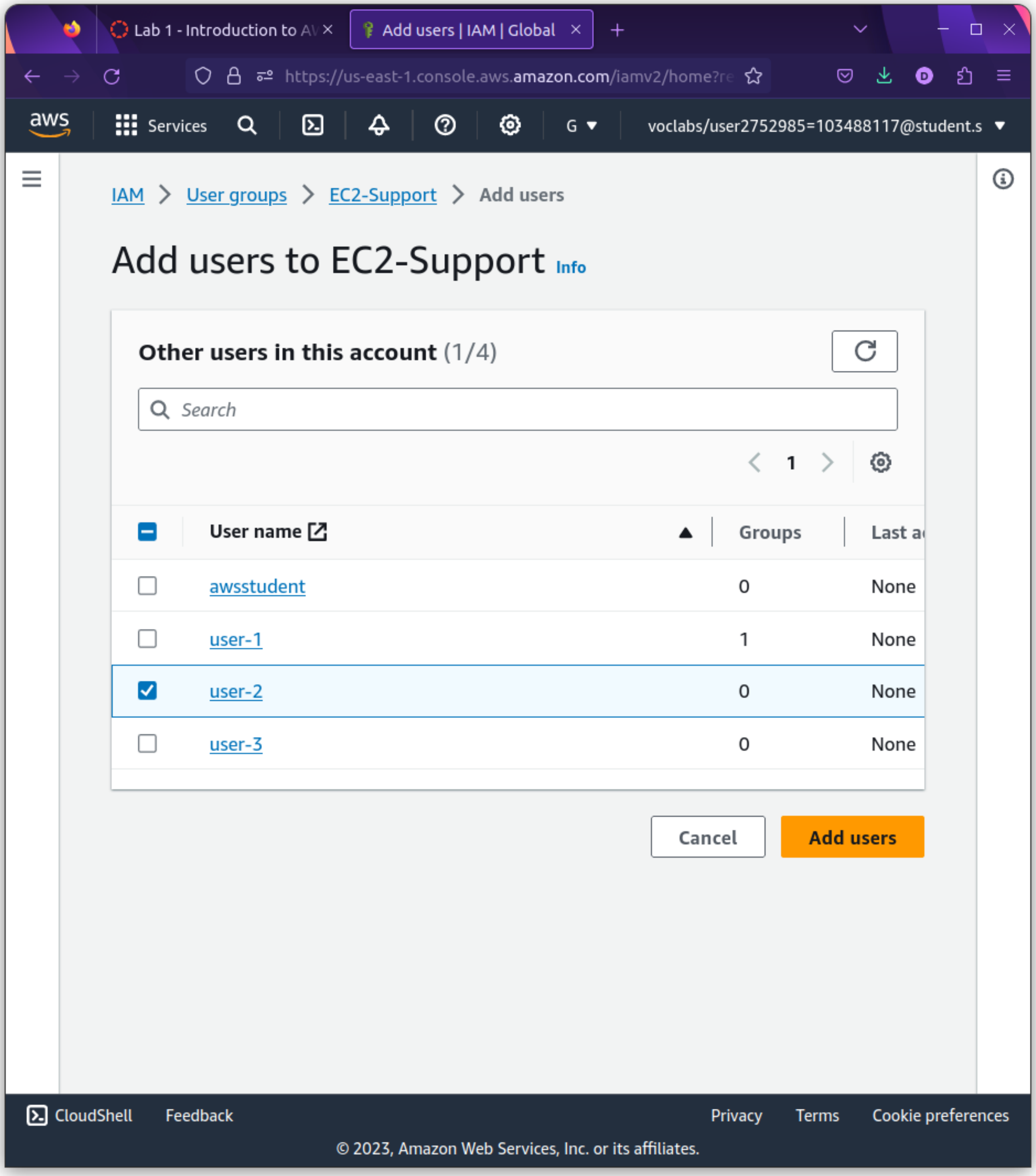
Cancel | Add users

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.

29. 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.


Lab 1 - Introduction to A
Add users | IAM | Global
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s
IAM > User groups > EC2-Support > Add users

Add users to EC2-Support Info

Other users in this account (1/4)

Search

☐	User name	Groups	Last a
☐	awsstudent	0	None
☐	user-1	1	None
☑	user-2	0	None
☐	user-3	0	None

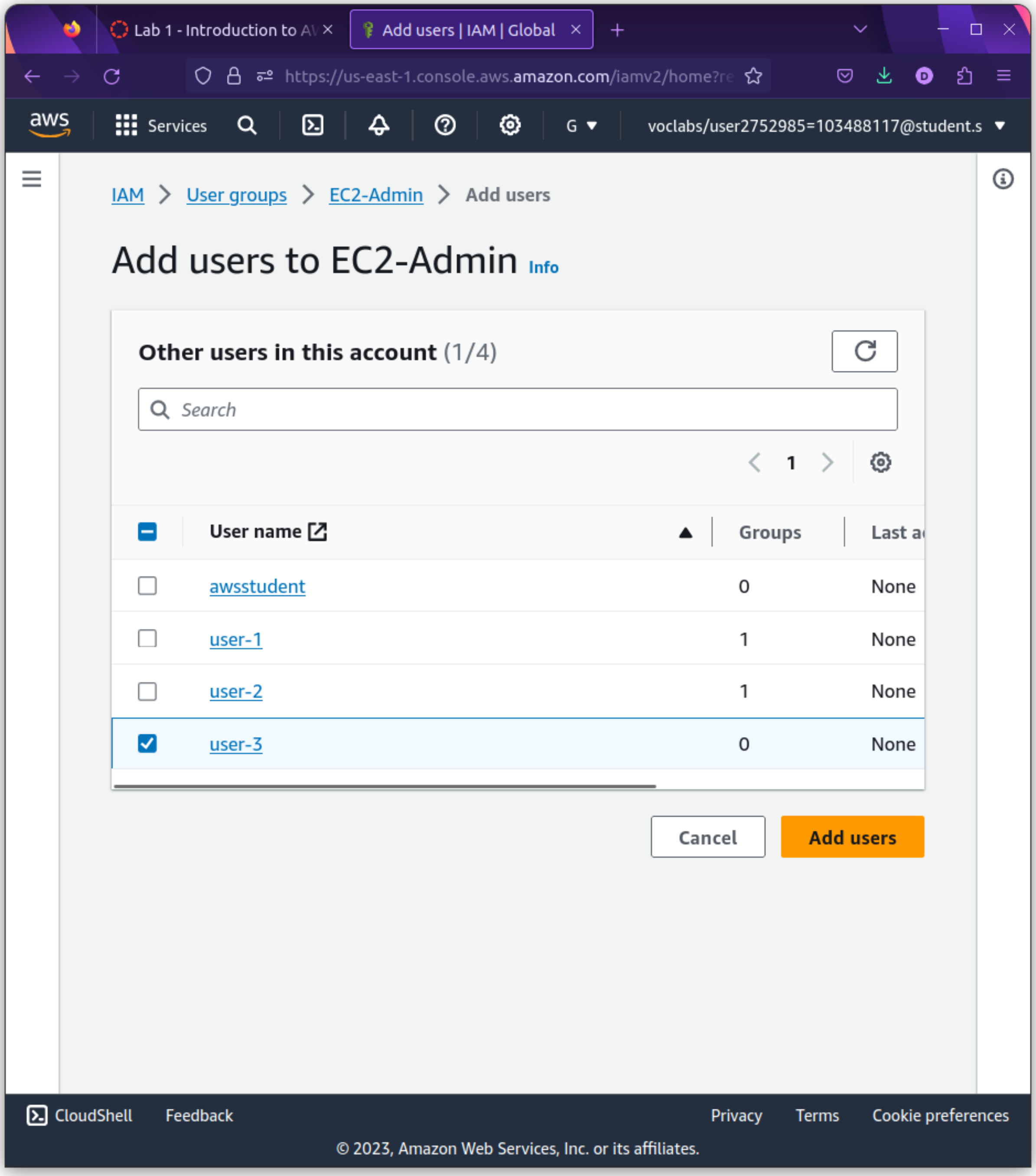
Cancel
Add users
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

Name: Trac Duc Anh Luong - ID: 103488117

Add user-3 to the EC2-Admin Group

You have hired **user-3** as your Amazon EC2 administrator, who manage your EC2 instances.

30. 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.


Lab 1 - Introduction to A
Add users | IAM | Global
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s
IAM > User groups > EC2-Admin > Add users
Info
Search
1
Cancel
Add users
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

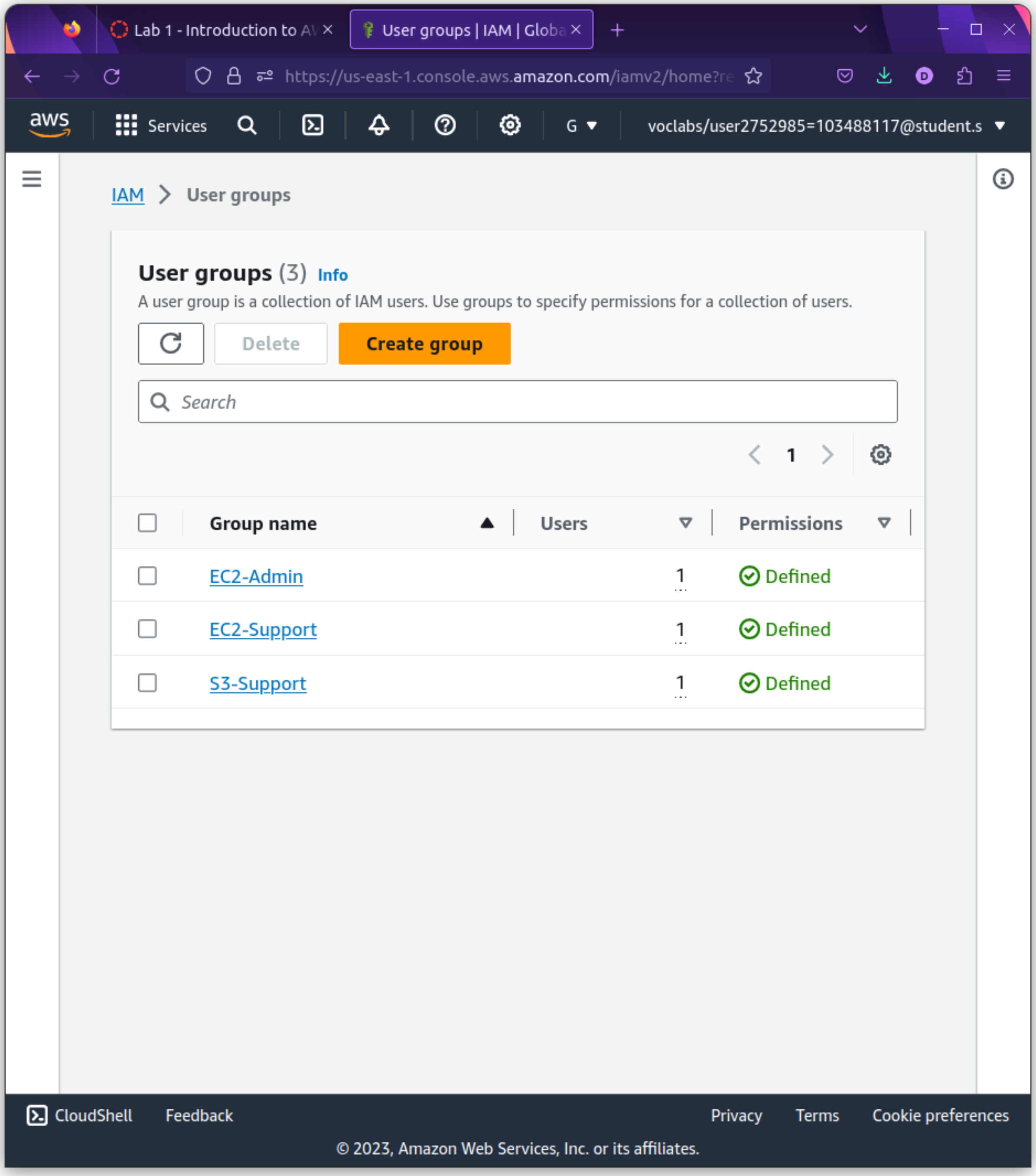
Add users to EC2-Admin

Other users in this account (1/4)

	User name	Groups	Last a
□	awsstudent	0	None
□	user-1	1	None
□	user-2	1	None
☑	user-3	0	None

Name: Trac Duc Anh Luong - ID: 103488117

31. In the navigation pane on the left, choose **User groups**.
Each Group should now have a **1** in the Users column for the number of Users in each Group. 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.



Lab 1 - Introduction to A
User groups | IAM | Globa
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s
IAM
User groups

User groups (3) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Delete
Create group
Search
1

□	Group name	Users	Permissions
□	EC2-Admin	1	✓ Defined
□	EC2-Support	1	✓ Defined
□	S3-Support	1	✓ Defined

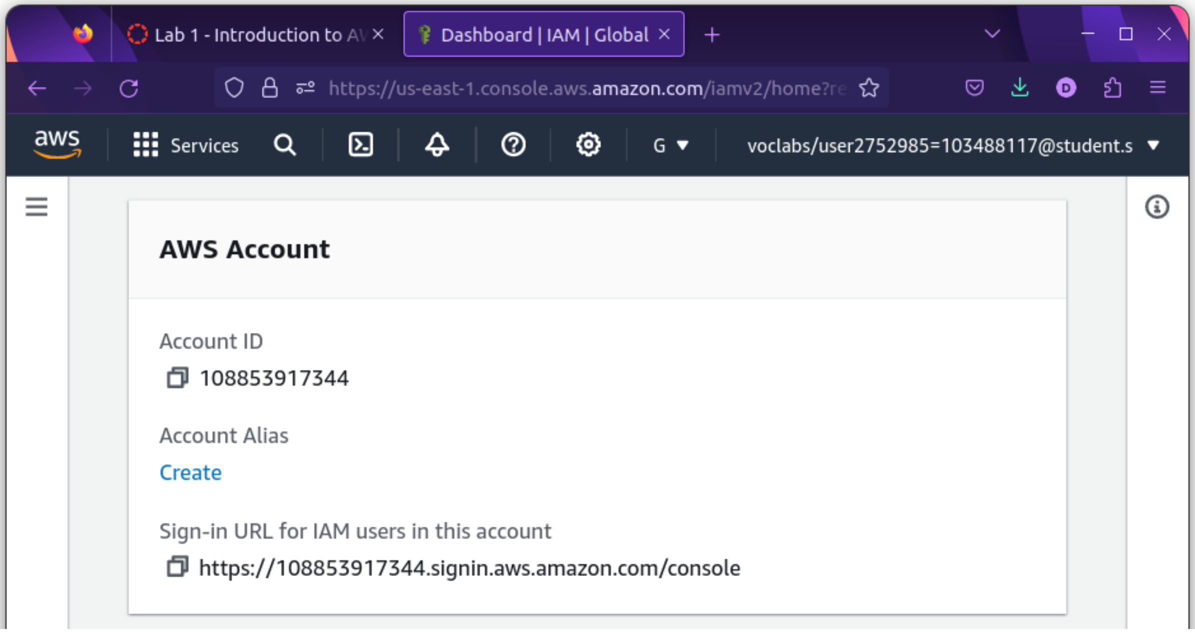
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

Name: Trac Duc Anh Luong - ID: 103488117

Task 3: Sign-In and Test Users

In this task, you will test the permissions of each IAM User.

32. In the navigation pane on the left, choose **Dashboard**.
    An **IAM users sign-in 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.


Lab 1 - Introduction to A
Dashboard | IAM | Global
https://us-east-1.console.aws.amazon.com/iamv2/home?re
aws
Services
G
voclabs/user2752985=103488117@student.s

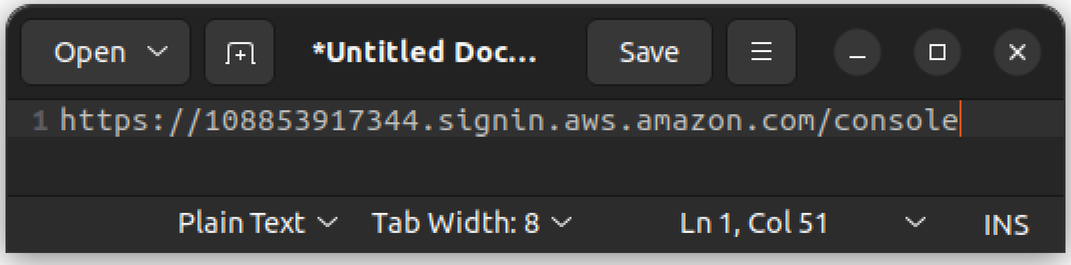
AWS Account

Account ID
108853917344

Account Alias
Create

Sign-in URL for IAM users in this account
https://108853917344.signin.aws.amazon.com/console

33. Copy the **Sign-in URL for IAM users in this account** to a text editor.



```
https://108853917344.signin.aws.amazon.com/console
```

34. Open a private (Incognito) window.
    Mozilla Firefox
    - Choose the menu bars at the top-right of the screen
    - Select **New private window**

Google Chrome

- ○ Choose the ellipsis at the top-right of the screen
- ○ Select **New Incognito Window**

Microsoft Edge

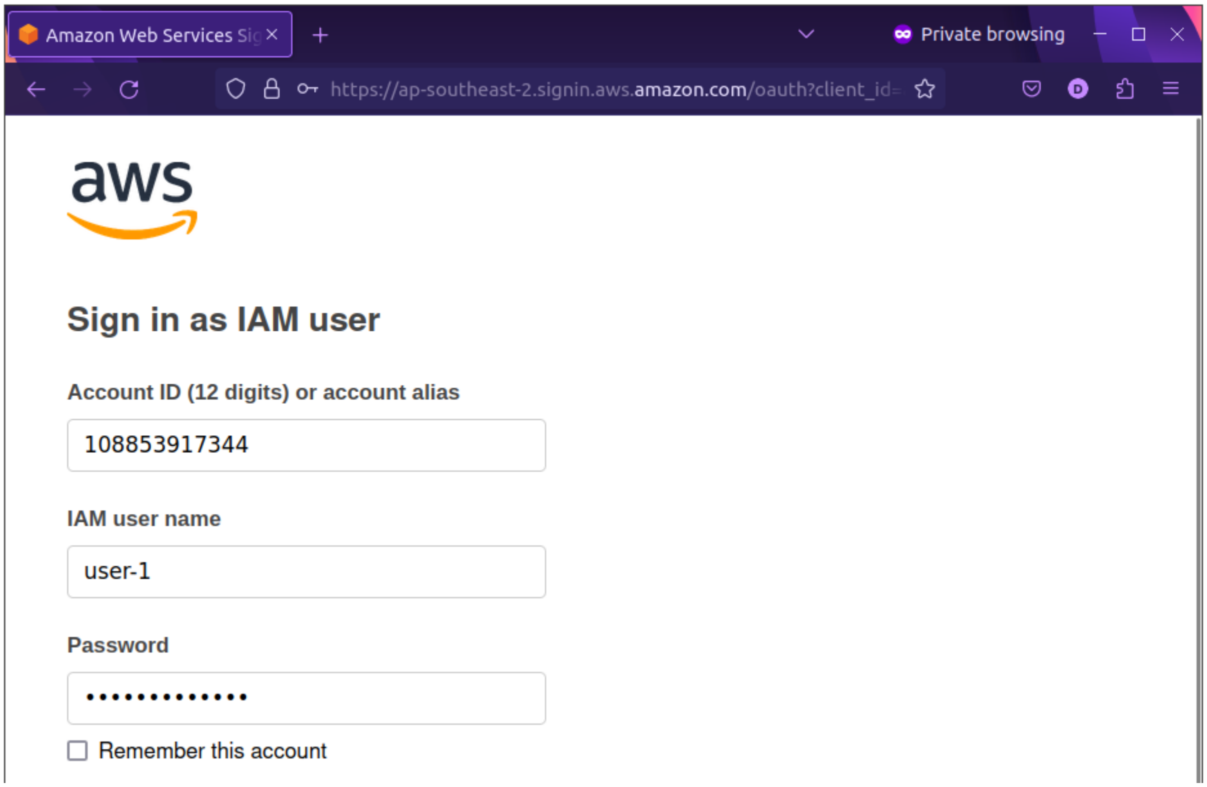
- ○ Choose the ellipsis at the top-right of the screen
- ○ Choose **New InPrivate window**

Microsoft Internet Explorer

- ○ Choose the **Tools** menu option
- ○ Choose **InPrivate Browsing**

35. 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.

36. Sign-in with:
   - ○ **IAM user name:** `user-1`
   - ○ **Password:** `Lab-Password1`


Amazon Web Services Sig
Private browsing
https://ap-southeast-2.signin.aws.amazon.com/oauth?client_id=
aws

Sign in as IAM user

Account ID (12 digits) or account alias

108853917344

IAM user name

user-1

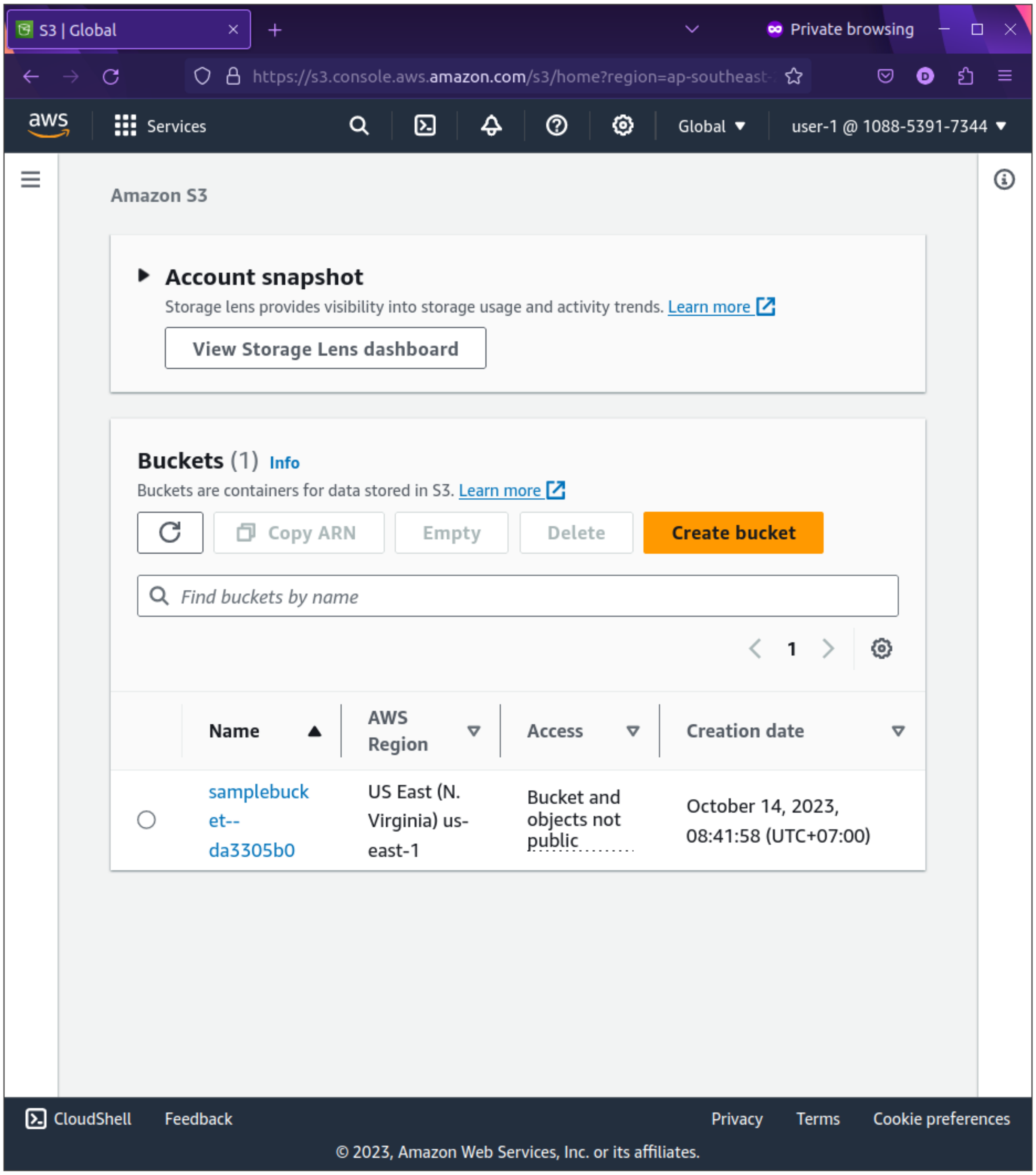
Password

•••••••••••••

□ Remember this account

Name: Trac Duc Anh Luong - ID: 103488117

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


S3 | Global
Private browsing
https://s3.console.aws.amazon.com/s3/home?region=ap-southeast-
aws
Services
Global ▼
user-1 @ 1088-5391-7344 ▼

Amazon S3

▶ **Account snapshot**

Storage lens provides visibility into storage usage and activity trends. Learn more

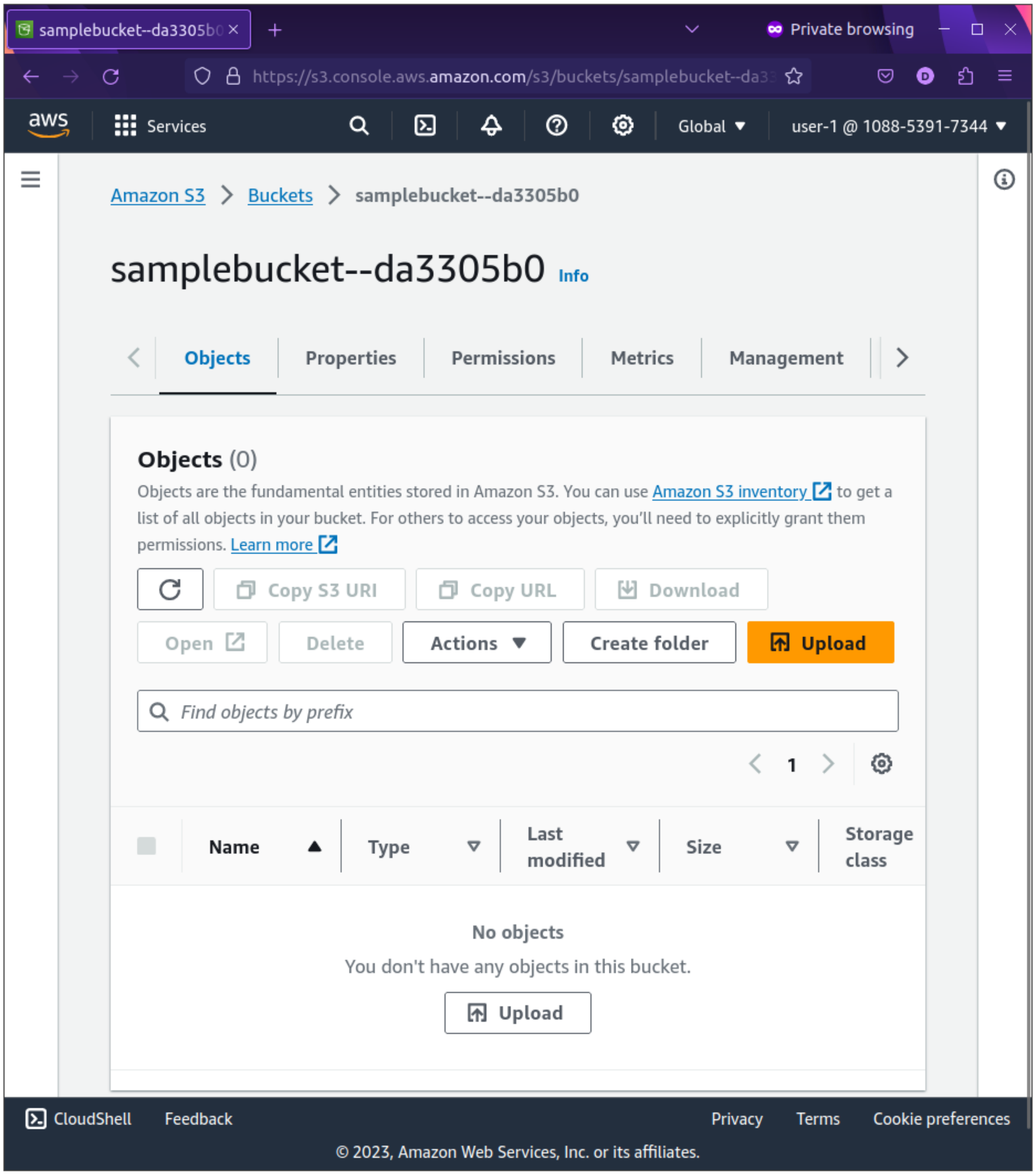
View Storage Lens dashboard

Buckets (1) Info

Buckets are containers for data stored in S3. Learn more

	Name ▲	AWS Region	Access	Creation date
○	samplebucket--da3305b0	US East (N. Virginia) us-east-1	Bucket and objects not public	October 14, 2023, 08:41:58 (UTC+07:00)

38. 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.



https://s3.console.aws.amazon.com/s3/buckets/samplebucket--da33

Amazon S3 > Buckets > samplebucket--da3305b0

samplebucket--da3305b0 Info

Objects (0)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

No objects

You don't have any objects in this bucket.

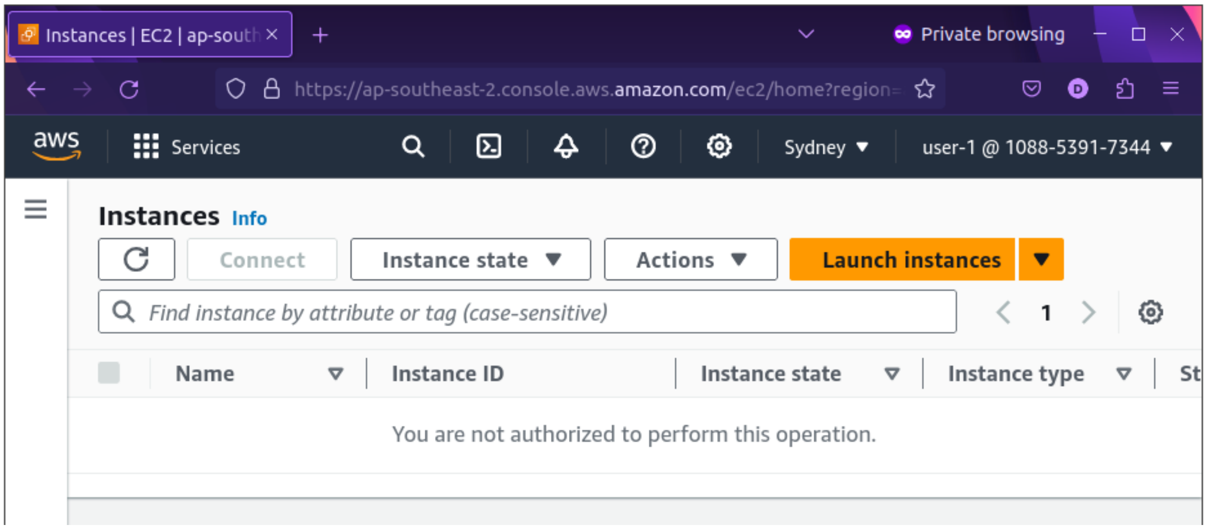
© 2023, Amazon Web Services, Inc. or its affiliates.

Now, test whether they have access to Amazon EC2.

Name: Trac Duc Anh Luong - ID: 103488117

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

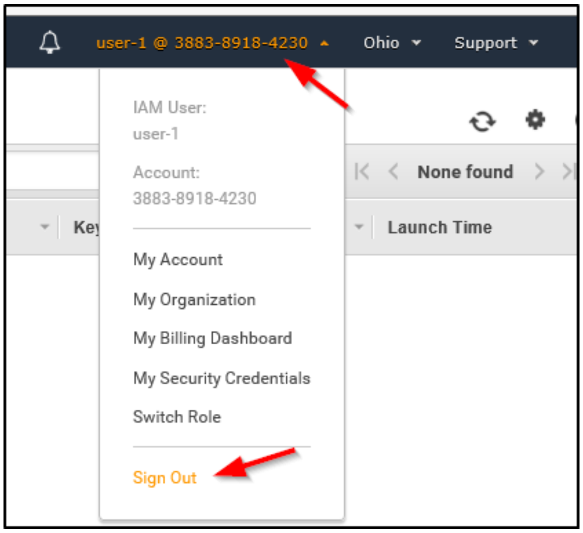
40. In the left navigation pane, choose **Instances**.
You cannot see any instances. Instead, you see a message that states *You are not authorized to perform this operation*. This is because this user has not been granted any permissions to access Amazon EC2.



You are not authorized to perform this operation.

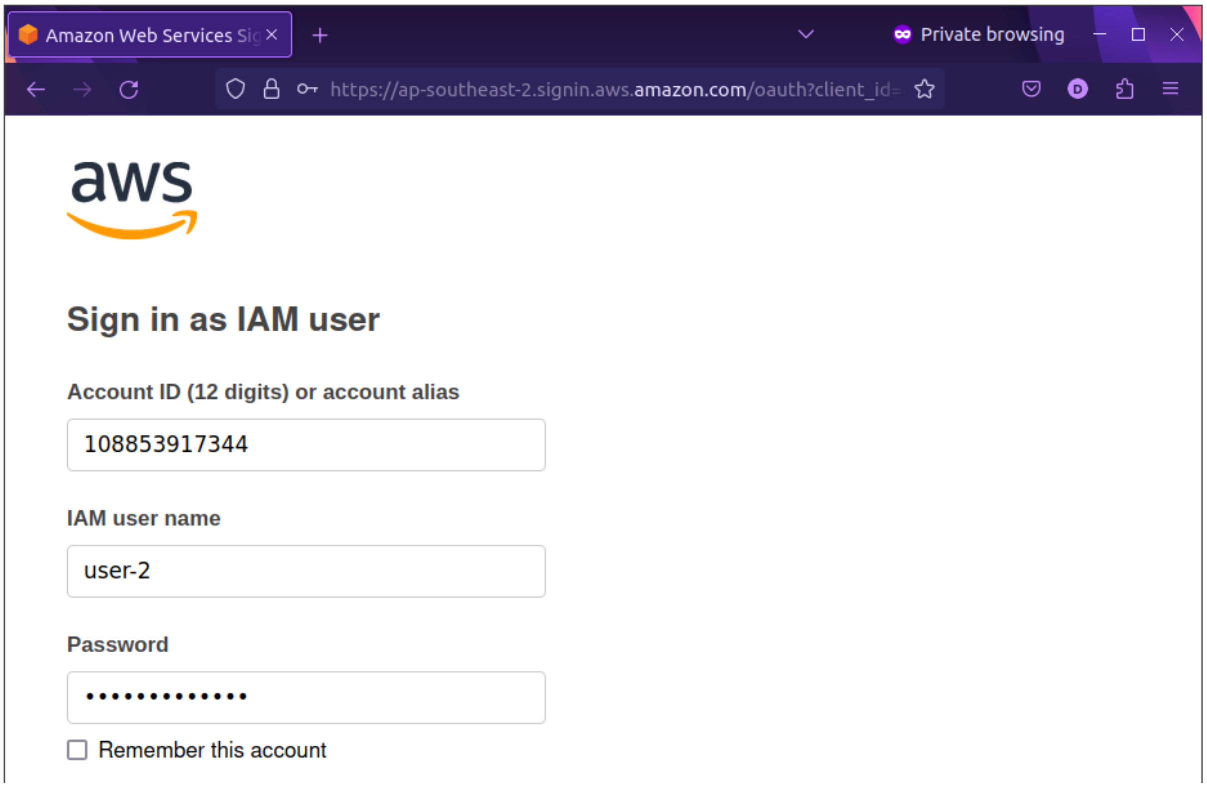
You will now sign-in as **user-2**, who has been hired as your Amazon EC2 support person.

41. 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**



42. 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.

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


Amazon Web Services Sig
Private browsing
https://ap-southeast-2.signin.aws.amazon.com/oauth?client_id=
aws

Sign in as IAM user

Account ID (12 digits) or account alias: 108853917344

IAM user name: user-2

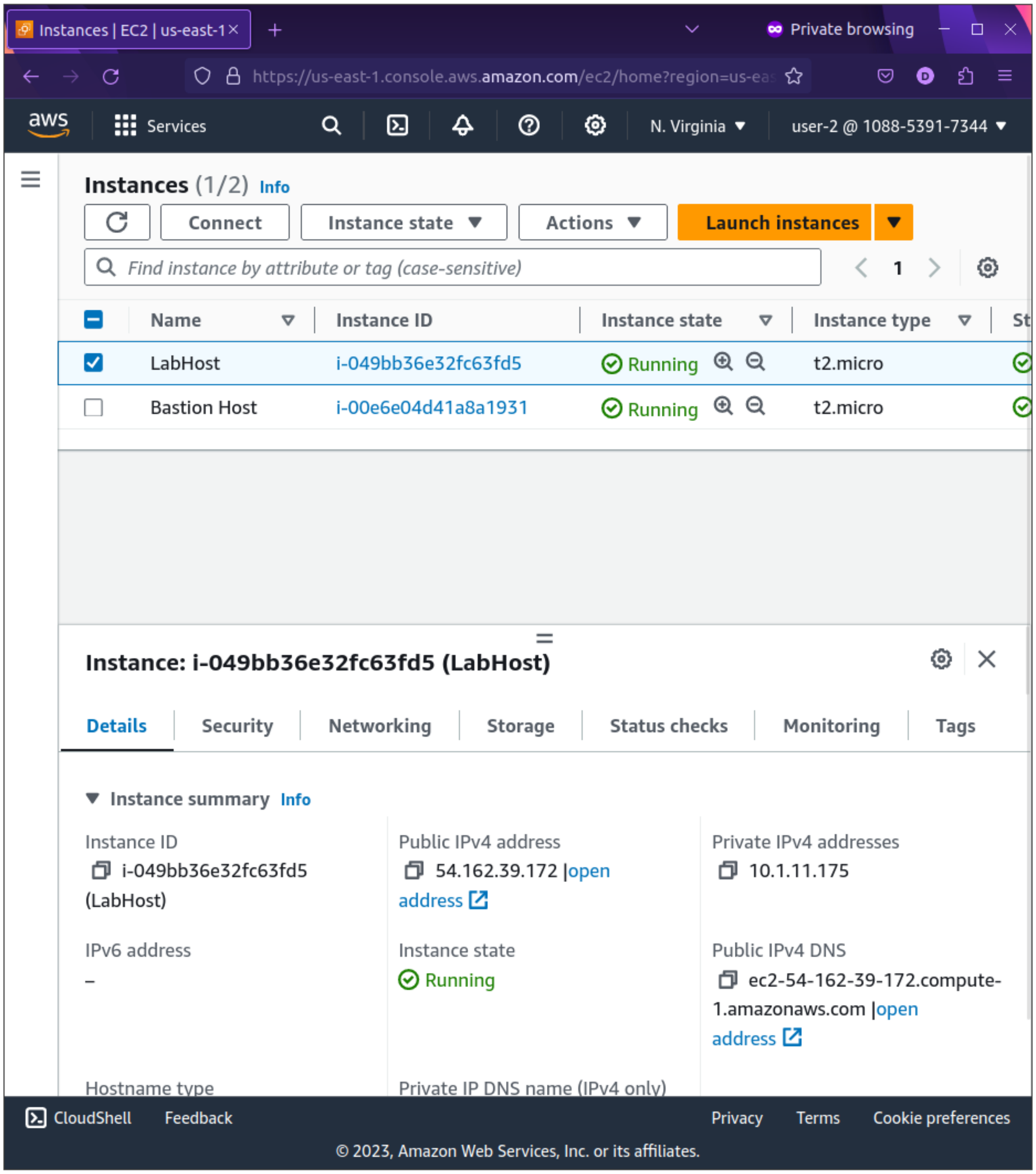
Password: ••••••••••••••

□ Remember this account

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

45. 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*.



Instances | EC2 | us-east-1
Private browsing
https://us-east-1.console.aws.amazon.com/ec2/home?region=us-eas
Services
N. Virginia
user-2 @ 1088-5391-7344
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

Instances (1/2) Info

	Name	Instance ID	Instance state	Instance type	St
☑	LabHost	i-049bb36e32fc63fd5	✓ Running	t2.micro	✓
□	Bastion Host	i-00e6e04d41a8a1931	✓ Running	t2.micro	✓

Instance: i-049bb36e32fc63fd5 (LabHost)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

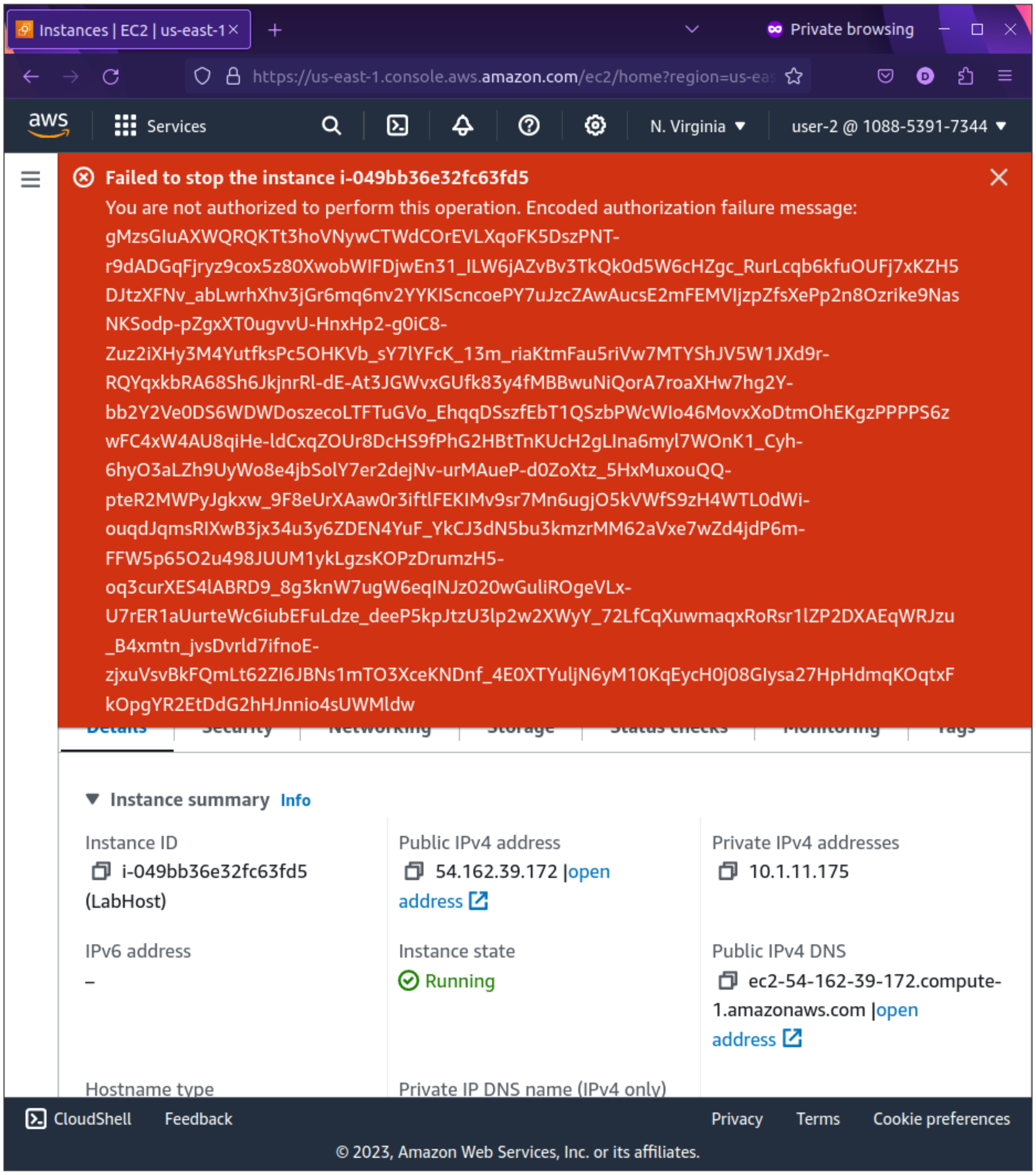
▼ Instance summary Info

Instance ID i-049bb36e32fc63fd5 (LabHost)	Public IPv4 address 54.162.39.172 |open address	Private IPv4 addresses 10.1.11.175
IPv6 address –	Instance state ✓ Running	Public IPv4 DNS ec2-54-162-39-172.compute-1.amazonaws.com |open address
Hostname type	Private IP DNS name (IPv4 only)	

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

Name: Trac Duc Anh Luong - ID: 103488117

47. 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.



Failed to stop the instance i-049bb36e32fc63fd5

You are not authorized to perform this operation. Encoded authorization failure message:

```
gMzsGIuAXWQRQKTt3hoVNywCTWdCOrEVLXqoFK5DszPNT-
r9dADGqFjryz9cox5z80XwobWIFDjwEn31_ILW6jAZvBv3TkQk0d5W6cHZgc_RurLcqb6kfuOUFj7xKZH5
DJtzXFNv_abLwrhXhv3jGr6mq6nv2YYKIScncoePY7uJzcZAwAucsE2mFEMVIjzpZfsXePp2n8Ozrike9Nas
NKSodp-pZgxXT0ugvvU-HnxHp2-g0iC8-
Zuz2iXHy3M4YutfksPc5OHKVb_sY7lYFcK_13m_riaKtmFau5riVw7MTYShJV5W1JXd9r-
RQYqxkbRA68Sh6JkjnrRl-dE-At3JGWvxGUfk83y4fMBBwuNiQorA7roaXHw7hg2Y-
bb2Y2Ve0DS6WDWDoszecoLTFTuGVo_EhqqDSszfEbT1QSzbPWcWIo46MovxXoDtmOhEKgzPPPPS6z
wFC4xW4AU8qiHe-ldCxqZOUr8DcHS9fPhG2HBtTnKUcH2gLIna6myl7WOnK1_Cyh-
6hyO3aLZh9UyWo8e4jbSolY7er2dejNv-urMAueP-d0ZoXtz_5HxMuxouQQ-
pteR2MWPyJgkxw_9F8eUrXAaw0r3iftlFEKIMv9sr7Mn6ugjO5kVWfS9zH4WTL0dWi-
ouqdJqmsRIXwB3jx34u3y6ZDEN4YuF_YkCJ3dN5bu3kmzrMM62aVxe7wZd4jdP6m-
FFW5p65O2u498JUUM1ykLgzsKOPzDrumzH5-
oq3curXES4lABRD9_8g3knW7ugW6eqINJz020wGuliROgeVLx-
U7rER1aUurteWc6iubEFuLdze_deeP5kpJtzU3lp2w2XWyY_72LfCqXuwmaqxRoRsr1lZP2DXAEqWRJzu
_B4xmtn_jvsDvrld7ifnoE-
zjxuVsvBkFQmLt62ZI6JBNs1mTO3XceKNDnf_4E0XTYuljN6yM10KqEycH0j08GIysa27HpHdmqKOqtxF
kOpgYR2EtDdG2hHJnnio4sUWMldw
```

▼ Instance summary Info

Instance ID
i-049bb36e32fc63fd5 (LabHost)

Public IPv4 address
54.162.39.172 |open address

Private IPv4 addresses
10.1.11.175

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-54-162-39-172.compute-1.amazonaws.com |open address

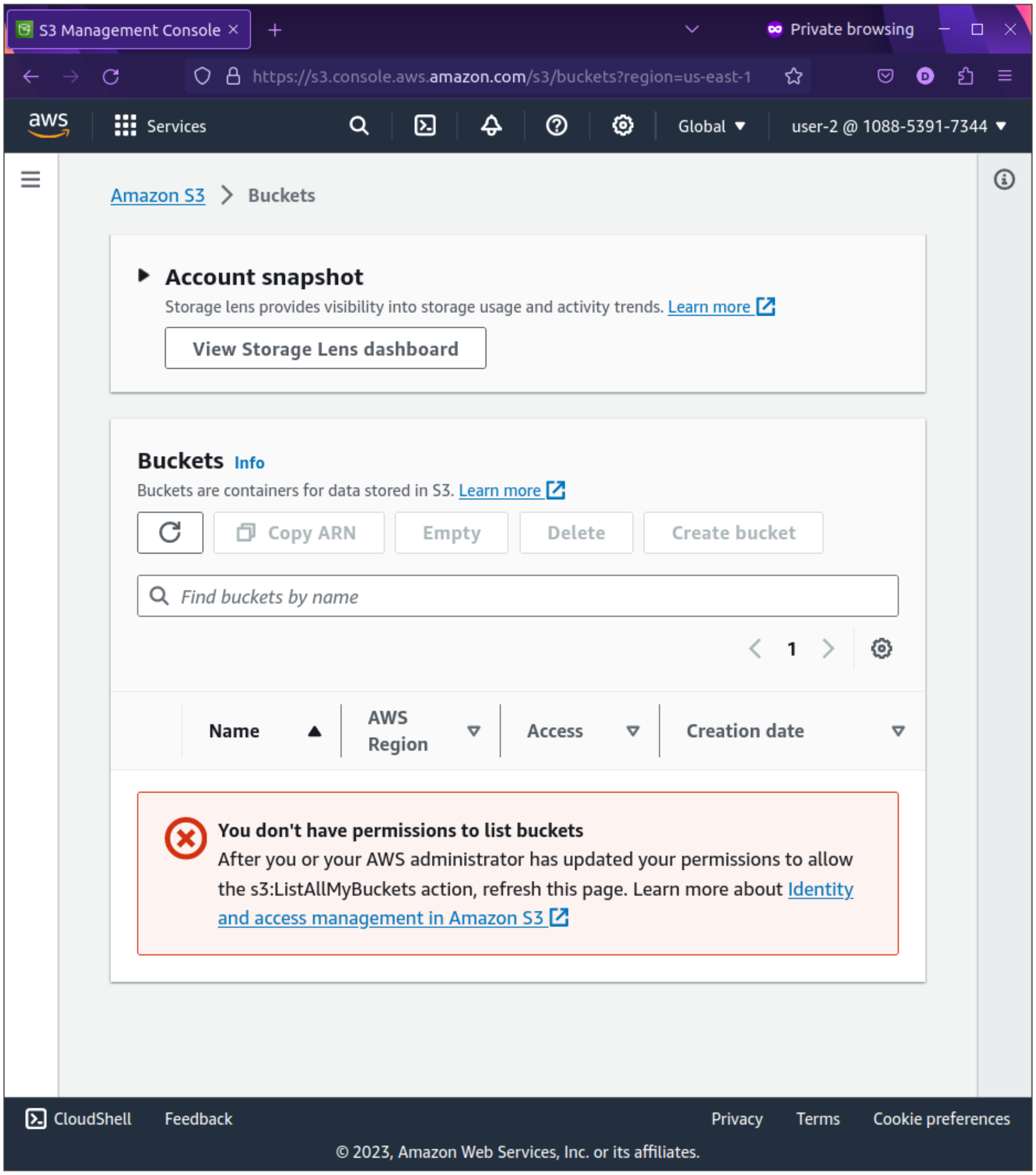
Hostname type

Private IP DNS name (IPv4 only)

© 2023, Amazon Web Services, Inc. or its affiliates.

48. Choose the X to close the *Failed to stop the instance* message.
    Next, check if user-2 can access Amazon S3.

49. 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.



Storage lens provides visibility into storage usage and activity trends. Learn more

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

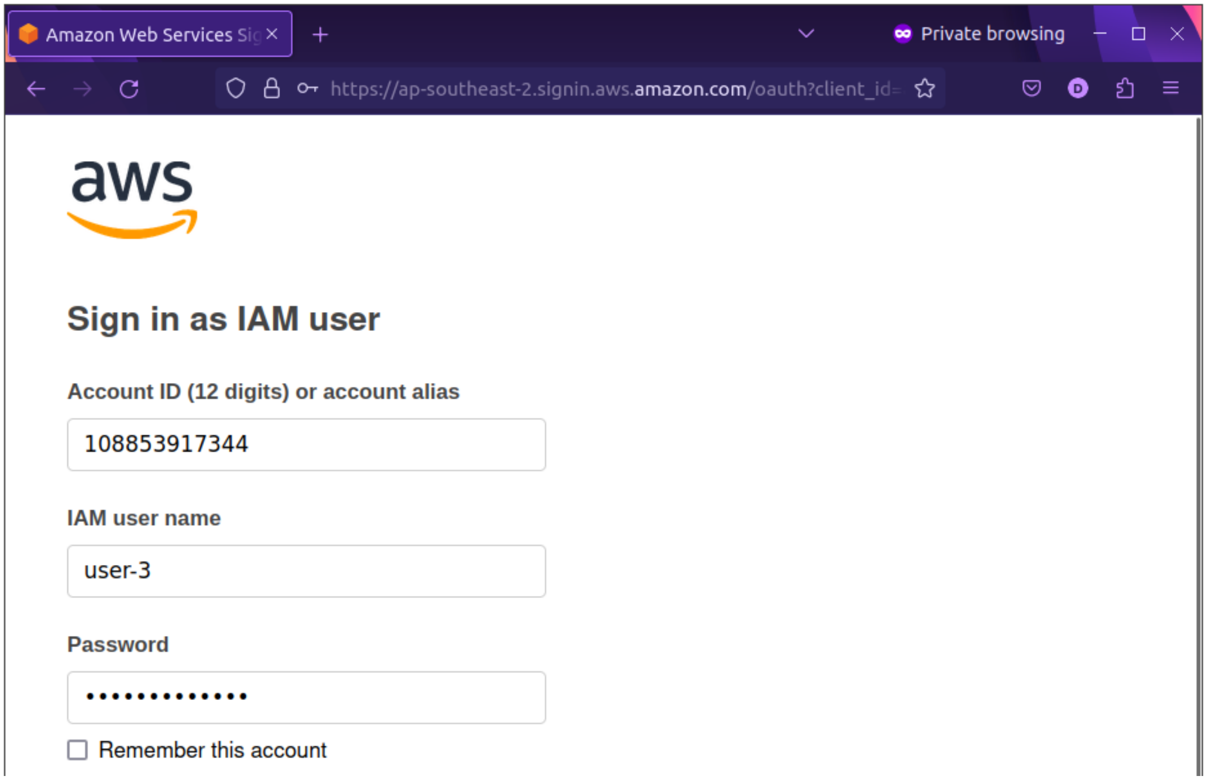
You will now sign-in as **user-3**, who has been hired as your Amazon EC2 administrator.

50. 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**

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

52. 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.

53. Sign-in with:
    - **IAM user name:** `user-3`
    - **Password:** `Lab-Password3`


Amazon Web Services Sig
Private browsing
https://ap-southeast-2.signin.aws.amazon.com/oauth?client_id=
aws

Sign in as IAM user

Account ID (12 digits) or account alias

108853917344

IAM user name

user-3

Password

•••••••••••••

□ Remember this account

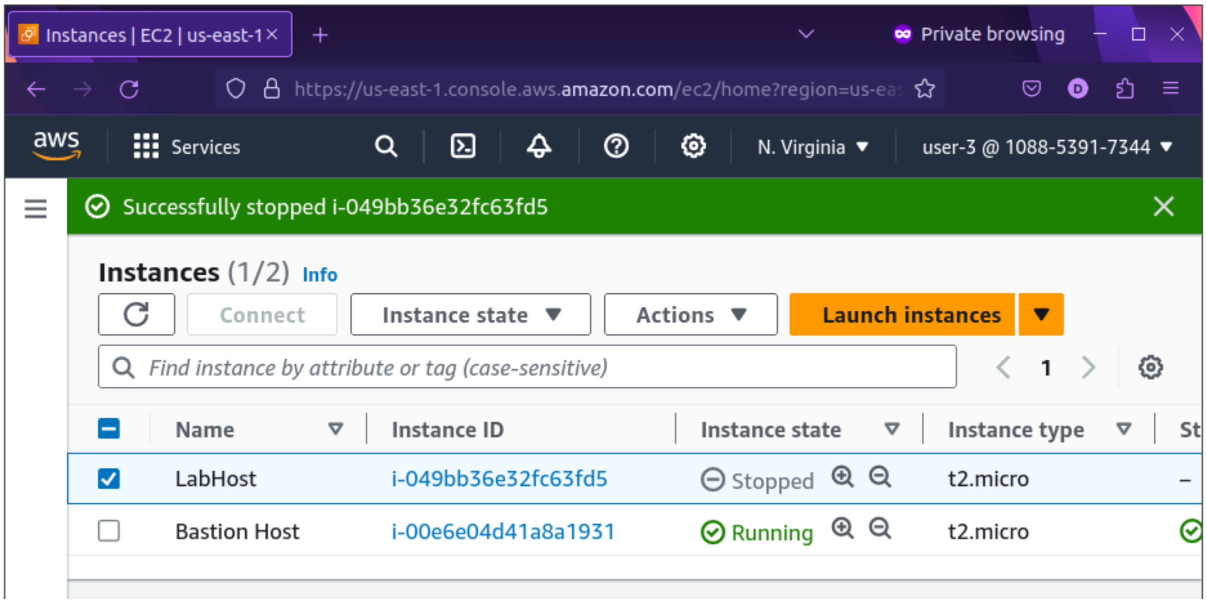
54. In the **Services** menu, choose **EC2**.

55. 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**).

56. In the **Instance state** menu, choose **Stop instance**.

57. In the **Stop instance** window, choose **Stop**.
    The instance will enter the *stopping* state and will shutdown.


Instances | EC2 | us-east-1
Private browsing
https://us-east-1.console.aws.amazon.com/ec2/home?region=us-eas
aws
Services
N. Virginia
user-3 @ 1088-5391-7344
Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
1

Successfully stopped i-049bb36e32fc63fd5

	Name	Instance ID	Instance state	Instance type	St
☑	LabHost	i-049bb36e32fc63fd5	⊖ Stopped	t2.micro	–
☐	Bastion Host	i-00e6e04d41a8a1931	✓ Running	t2.micro	✓

58. Close your private browser window.