

**Project in AWS  
Practice Lab**

# **Introduction to AWS Identity and Access Management (IAM)**

**Andra-Diana Popescu**

**2023**

## **ABOUT THIS LAB**

AWS Identity and Access Management (IAM) is a service that allows AWS customers to manage user access and permissions for the accounts and available APIs/services within AWS. IAM can manage users, security credentials (such as API access keys), and allow users to access AWS resources.

In this lab, we will walk through the foundations of IAM. We'll focus on user and group management, as well as how to assign access to specific resources using IAM-managed policies. We'll learn how to find the login URL, where AWS users can log in to their account, and explore this from a real-world use case perspective.

## **LEARNING OBJECTIVES**

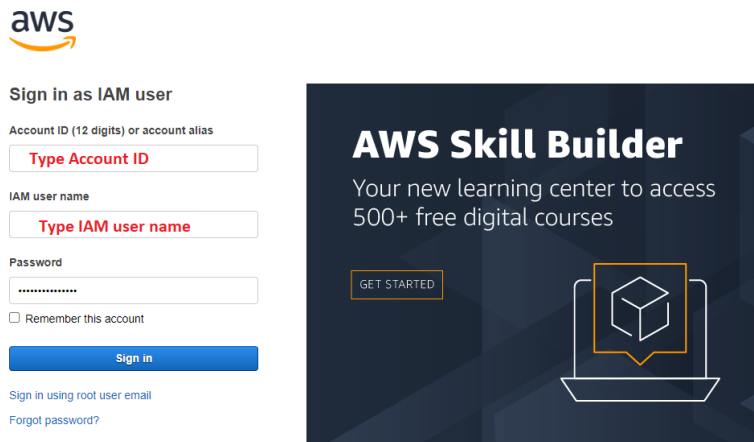
- Add the Users to the Proper Groups
- Use the IAM Sign-In Link to Sign-In as a User

**Source:** <https://learn.acloud.guru/course/certified-solutions-architect-associate/>

## Table of Contents

Log in to your AWS account .....	4
1. Explore Users and Groups .....	4
1.1. Explore the Users .....	4
1.2. Explore the Groups .....	7
2. Add the Users to the Proper Groups .....	10
3. Use the IAM Sign-In Link to Sign-In as Each User .....	13
3.1. Sign-In as user-1 .....	13
3.2. Sign-In as user-2 .....	16
3.3. Sign-In as user-3 .....	18

## Log in to your AWS account

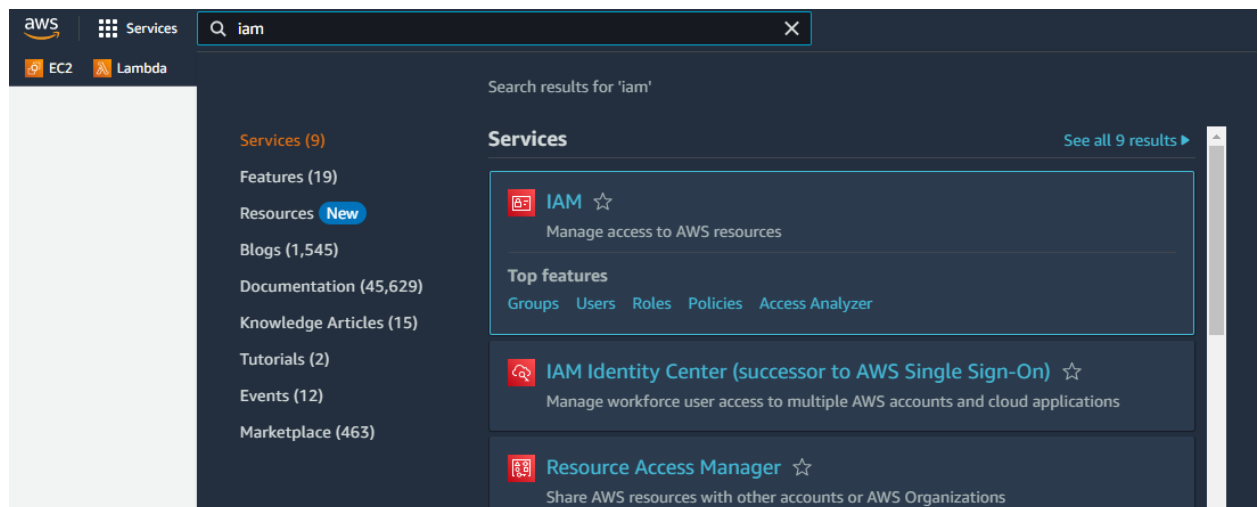


The image shows the AWS sign-in page. On the left, there is a form titled "Sign in as IAM user". It includes fields for "Account ID (12 digits) or account alias" with a placeholder "Type Account ID", "IAM user name" with a placeholder "Type IAM user name", and a "Password" field. Below the password field is a checkbox for "Remember this account" and a blue "Sign in" button. At the bottom of the form, there are links for "Sign in using root user email" and "Forgot password?". To the right of the form is a promotional banner for "AWS Skill Builder" with the text "Your new learning center to access 500+ free digital courses" and a "GET STARTED" button. The banner also features an icon of a laptop with a cube on the screen.

## 1. Explore Users and Groups

### 1.1. Explore the Users

1. Once you are logged in to the AWS Management Console, navigate to IAM.



2. From the left-side menu, click **Users**.
3. Select the **user-1** user name

**Identity and Access Management (IAM)**

Search IAM

Dashboard

Access management

- User groups
- Users 1**
- Roles
- Policies
- Identity providers
- Account settings

**Users (4)** Info

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

Find users by username or access key

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	cloud_user	None	3 minutes ago	None	1 hour ago	-
<input type="checkbox"/>	<b>user-1 2</b>	None	Never	None	1 hour ago	-
<input type="checkbox"/>	user-2	None	Never	None	1 hour ago	-
<input type="checkbox"/>	user-3	None	Never	None	1 hour ago	-

#### 4. Review the resources associated with **user-1**:

- Select the **Permissions** and **Groups** tabs, where you'll see **user-1** does not have any permissions assigned and does not belong to any groups.

**Identity and Access Management (IAM)**

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

**Access reports**

- Access analyzer
- Archive rules
- Analysers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related console

- IAM Identity Center
- AWS Organizations

**user-1**

**Summary**

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

Created: May 01, 2023, 10:59 (UTC+05:00)

Console access: Enabled without MFA

Last console sign-in: Never

Access key 1: Not enabled

Access key 2: Not enabled

**Permissions** Groups Tags (1) Security credentials Access Advisor

**Permissions policies (0)**

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

Find policies

No policies

**Permissions boundary (not set)**

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

**You need permissions**

You do not have the permission required to perform this operation. Ask your administrator to add permissions.

User: arn:aws:iam:: user/cloud\_user is not authorized to perform: access-analyzer:ListPolicyGenerations on resource: arn:aws:access-analyzer::east- \* with an explicit deny

**Identity and Access Management (IAM)**

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

**Access reports**

- Access analyzer
- Archive rules
- Analysers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related console

- IAM Identity Center
- AWS Organizations

**user-1**

**Summary**

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

Created: May 01, 2023, 10:59 (UTC+05:00)

Console access: Enabled without MFA

Last console sign-in: Never

Access key 1: Not enabled

Access key 2: Not enabled

**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.

- Select the **Security credentials** tab, where you would see user access keys, SSH public keys, and HTTPS Git credentials for AWS CodeCommit.

The screenshot displays the AWS IAM console interface. On the left is a navigation sidebar with sections for 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Related console' links. The main content area is titled 'IAM > Users > user-1' and shows the 'Security credentials' tab for 'user-1'. The 'Summary' section at the top provides details about the user's ARN, creation date, and console access status. Below this, the 'Console sign-in' section shows the sign-in link and password. The 'Multi-factor authentication (MFA)' section indicates that MFA is not currently enabled. The 'Access keys' section shows no keys are present. The 'SSH public keys for AWS CodeCommit' and 'HTTPS Git credentials for AWS CodeCommit' sections also show no credentials. The 'Credentials for Amazon Keyspaces (for Apache Cassandra)' section shows no credentials. Finally, the 'Signing certificates (X.509)' section shows no certificates. Each section includes a 'Create' or 'Generate' button and a 'Learn more' link.

**Identity and Access Management (IAM)**

Search IAM

Dashboard

**Access management**

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

**Access reports**

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related console

- IAM Identity Center
- AWS Organizations

**user-1** [Delete]

**Summary**

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

Created: May 01, 2023, 10:59 (UTC+03:00)

Console access: Enabled without MFA

Last console sign-in: Never

Access key 1: Not enabled

Access key 2: Not enabled

Permissions Groups Tags [1] **Security credentials** Access Advisor

**Console sign-in** [Manage console access]

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

Console password: Updated 1 hour ago (2023-05-01 11:00 GMT+3)

Last console sign-in: Never

**Multi-factor authentication (MFA)**

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]

[Remove] [Resync] [Assign MFA device]

Device type Identifier Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment

[Assign MFA device]

**Access keys**

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more]

[Create access key]

No access keys

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more]

[Create access key]

**SSH public keys for AWS CodeCommit**

Use SSH public keys to authenticate access to AWS CodeCommit repositories. You can have a maximum of five SSH public keys (active or inactive) at a time. [Learn more]

Actions [Upload SSH public key]

SSH Key ID Uploaded Status

No SSH public keys

[Upload SSH public key]

**HTTPS Git credentials for AWS CodeCommit**

Generate a user name and password you can use to authenticate HTTPS connections to AWS CodeCommit repositories. You can have a maximum of 2 sets of credentials (active or inactive) at a time. [Learn more]

Actions [Generate credentials]

User name Created Status

No credentials

[Generate credentials]

**HTTPS Git credentials for AWS CodeCommit**

Generate a user name and password you can use to authenticate HTTPS connections to AWS CodeCommit repositories. You can have a maximum of 2 sets of credentials (active or inactive) at a time. [Learn more]

Actions [Generate credentials]

User name Created Status

No credentials

[Generate credentials]

**Credentials for Amazon Keyspaces (for Apache Cassandra)**

Generate a user name and password you can use to authenticate to Amazon Keyspaces. You can have a maximum of two sets of credentials (active or inactive) at a time. [Learn more]

Actions [Generate credentials]

User name Created Status

No credentials

[Generate credentials]

**Signing certificates (X.509)**

Use X.509 certificates to make secure SOAP protocol requests to some AWS services. You can have a maximum of two X.509 certificates (active or inactive) at a time. [Learn more]

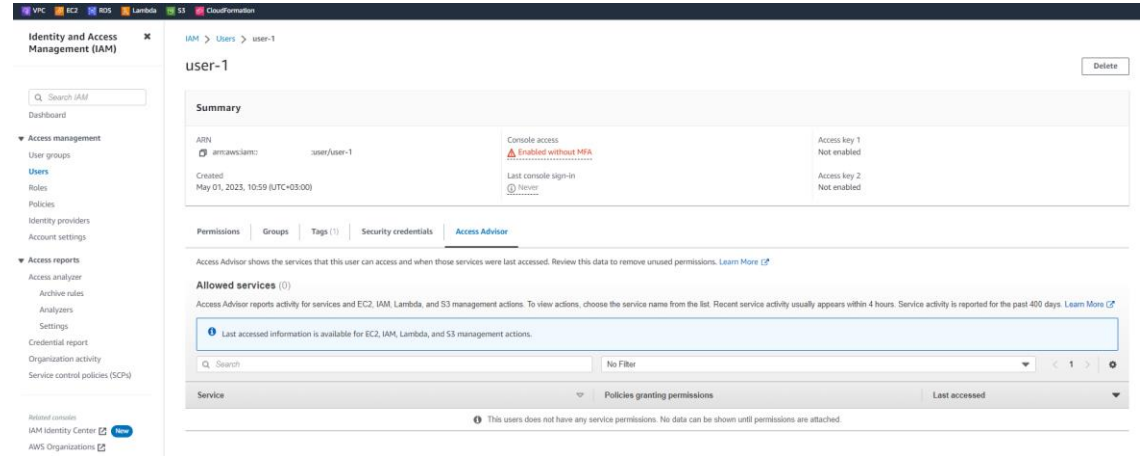
Actions [Upload] [Create X.509 certificate]

Creation time Thumbprint Status

No X.509 certificates

[Create X.509 certificate]

- Select the **Access Advisor** tab to see which services the user has accessed and when.



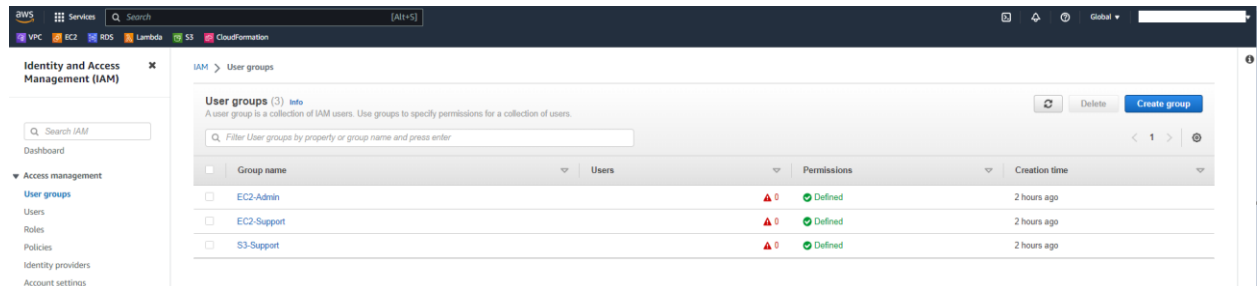
5. At the top of the page, under **Summary**, observe the user's **ARN (Amazon Resource Name)**, path, and creation time.

## 1.2. Explore the Groups

1. In the IAM sidebar menu, select **User groups**.

You should see three provided user groups for this lab:

- **EC2-Admin:** Provides permissions to view, start, and stop EC2 instances
- **EC2-Support:** Provides read-only access to EC2
- **S3-Support:** Provides read-only access to S3



2. Select the **EC2-Admin** group name.
3. Review the resources associated with **EC2-Admin**:
  - Select the **Permissions** tab, where you can see that there is an inline policy associated with the group.

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with sections like 'Access management', 'Access reports', and 'Access analyzer'. The main content area displays the 'EC2-Admin' user group details. Under the 'Permissions' tab, there is a table of 'Permissions policies (1)'. The policy 'ec2-admin' is listed with a plus-sign icon to its left.

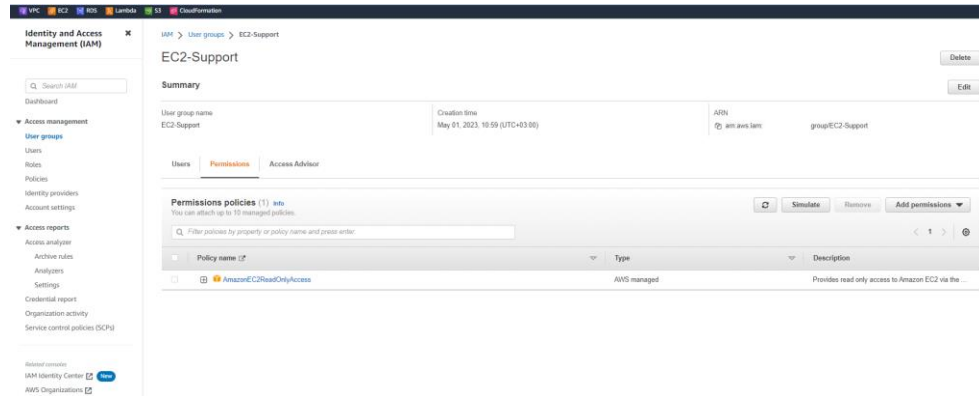
- Click the plus-sign icon to the left of the policy name to view the associated inline policy.

This screenshot shows the 'ec2-admin' inline policy expanded. The policy content is displayed in a code editor, showing a JSON structure with actions like 'ec2:Describe\*', 'ec2:StartInstances', 'ec2:StopInstances', 'elasticloadbalancing:Describe\*', 'cloudwatch:Describe\*', and 'cloudwatch:Delete\*', all with 'Effect': 'Allow'. The breadcrumb at the top of the page reads 'User groups > EC2-Admin'.

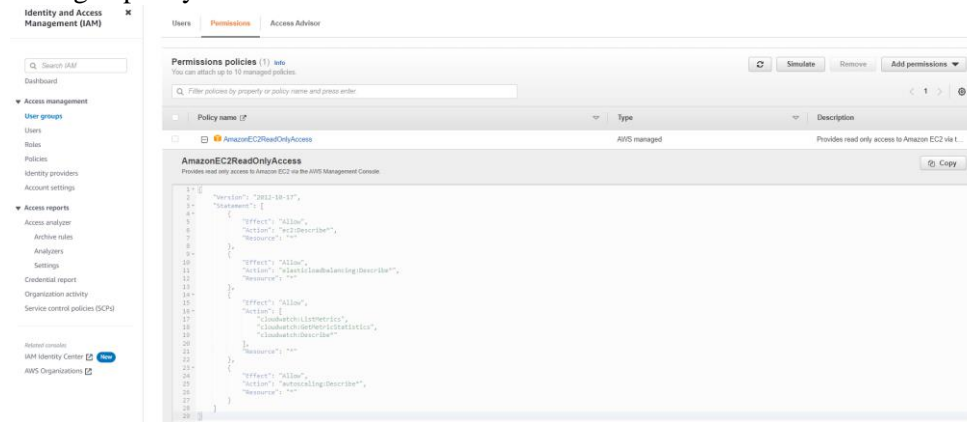
- Use the breadcrumb along the top of the page to select **User groups**.
- Select the **EC2-Support** group name.
- Review the resources associated with **EC2-Support**:

- Select the **Permissions** tab, where you'll see that the group has an AWS managed policy.



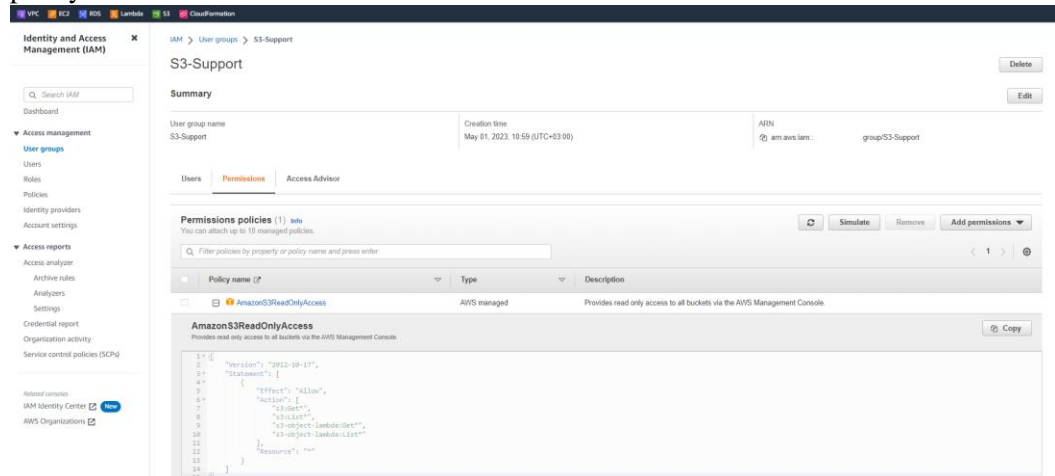


- Click the plus-sign icon to the left of the policy name to view the associated AWS managed policy.



7. Use the breadcrumb along the top of the page to select **User groups**.
8. Select the **S3-Support** group name.
9. Review the resources associated with **S3-Support**:

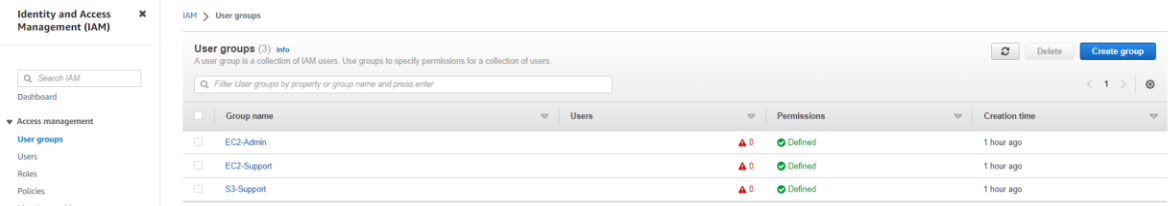
- Select the **Permissions** tab, where you'll see that the group is only allowed read-only access.
- Click the plus-sign icon to the left of the policy name to view the associated read-only policy.



## 2. Add the Users to the Proper Groups

1. Navigate to **IAM**.
2. In the IAM sidebar menu, select **User groups**.
3. Add **user-1** to the **S3-Support** group:

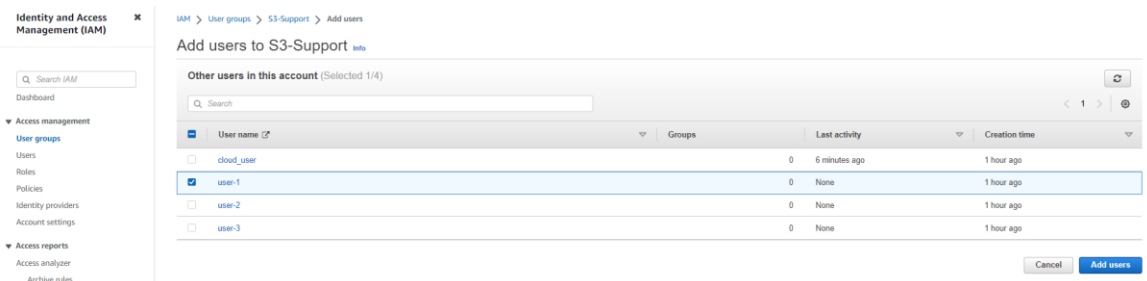
- Select the **S3-Support** group name.



- Ensure the **Users** tab is selected and then click **Add users** on the right.



- From the list of available users, check the checkbox next to **user-1**.
- Click **Add users**.



4. Use the breadcrumb along the top of the page to select **User groups**.
5. Add **user-2** to the **EC2-Support** group:
  - Select the **EC2-Support** group name.
  - Ensure the **Users** tab is selected and then click **Add users** on the right.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysts

Settings

Credential report

Organization activity

Service control policies (SCPs)

EC2-Support

Summary

User group name: EC2-Support

Creation time: May 01, 2023, 13:59 (UTC+03:00)

ARN: arn:aws:iam::group:EC2-Support

Users

Permissions

Access Advisor

Users in this group (0)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

User name

Groups

Last activity

Creation time

No resources to display

Remove users

Add users

- From the list of available users, check the checkbox next to **user-2**.
- Click **Add users**.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysts

Settings

Add users to EC2-Support

Other users in this account (Selected 1/4)

Search

User name

Groups

Last activity

Creation time

cloud\_user

0

12 minutes ago

1 hour ago

user-1

1

None

1 hour ago

user-2

0

None

1 hour ago

user-3

0

None

1 hour ago

Cancel

Add users

6. Use the breadcrumb along the top of the page to select **User groups**.
7. Add **user-3** to the **EC2-Admin** group:
  - Select the **EC2-Admin** group name.
  - Ensure the **Users** tab is selected and then click **Add users** on the right.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysts

Settings

EC2-Admin

Summary

User group name: EC2-Admin

Creation time: May 01, 2023, 13:59 (UTC+03:00)

ARN: arn:aws:iam::group:EC2-Admin

Users

Permissions

Access Advisor

Users in this group (0)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

User name

Groups

Last activity

Creation time

No resources to display

Remove users

Add users

- From the list of available users, check the checkbox next to **user-3**.
- Click **Add users**.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysts

Settings

Add users to EC2-Admin

Other users in this account (Selected 1/4)

Search

User name

Groups

Last activity

Creation time

cloud\_user

0

21 minutes ago

1 hour ago

user-1

1

None

1 hour ago

user-2

1

None

1 hour ago

user-3

0

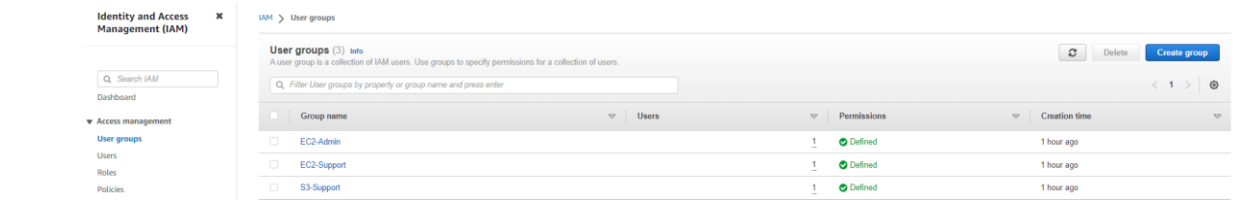
None

1 hour ago

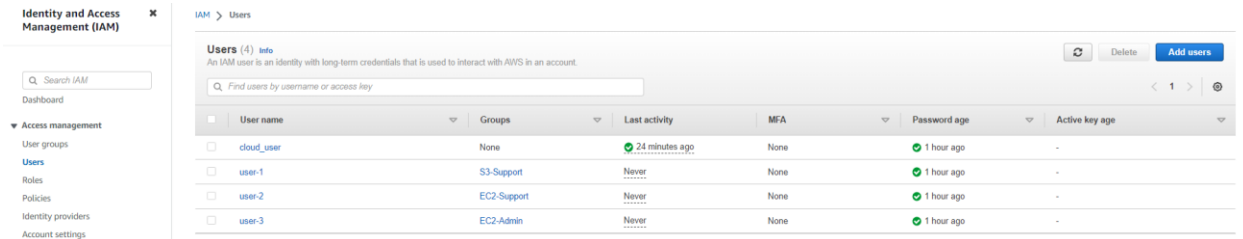
Cancel

Add users

Now we have one user for each of these groups.

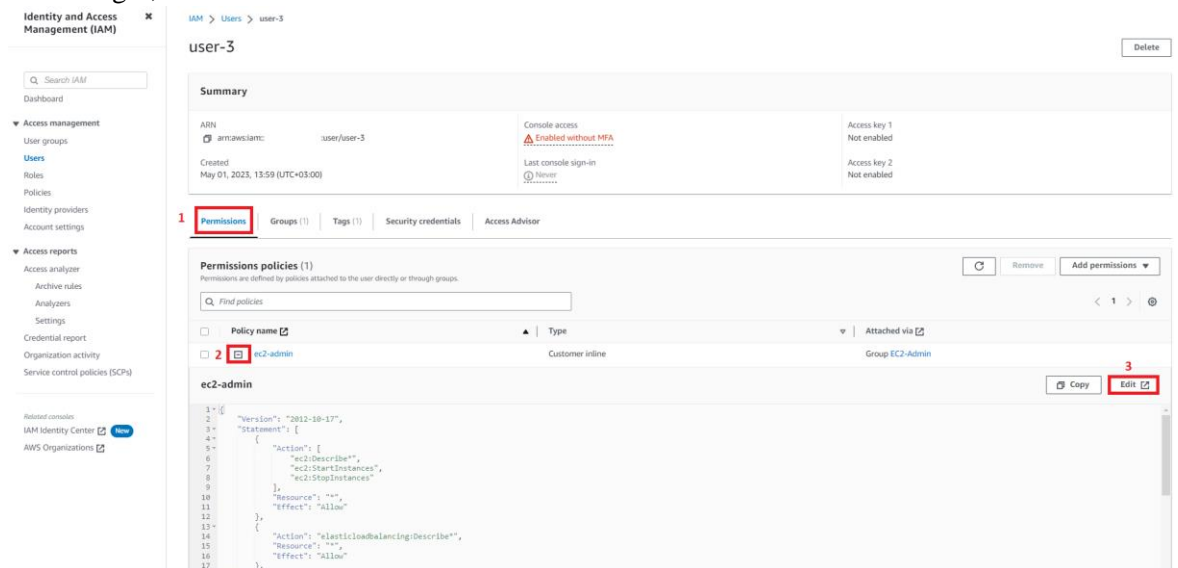


8. In the IAM sidebar menu, select **Users**.

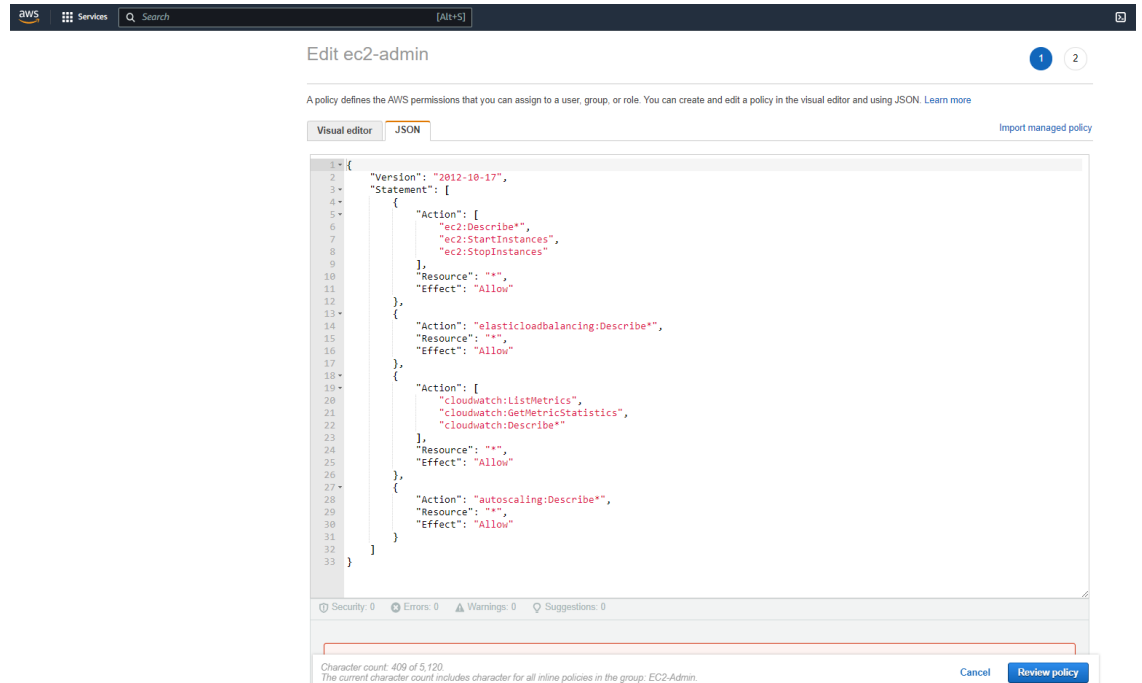


9. Review the permissions for **user-3**:

- Select the **user-3** user name.
- Select the **Permissions** tab and then click the plus-sign icon to expand the customer inline policy associated with **user-3**.
- On the right, click **Edit**.



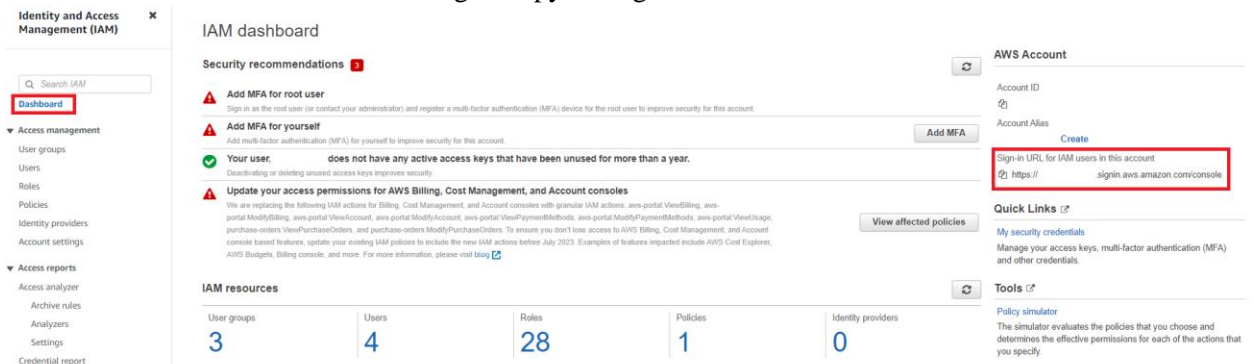
- Select the **JSON** tab and review the policy permissions, but do not make any changes.
- Click **Cancel**.



### 3. Use the IAM Sign-In Link to Sign-In as Each User

#### 3.1. Sign-In as user-1

1. In the IAM sidebar menu, select **Dashboard**.
2. In the **AWS Account** section on the right, copy the sign-in URL.



3. In a new browser tab, navigate to the URL.
4. Log in to the AWS Management Console as **user-1** using the password provided in the lab's resources. Remember that this user only has read-only access to S3.



### Sign in as IAM user

Account ID (12 digits) or account alias

IAM user name

Password

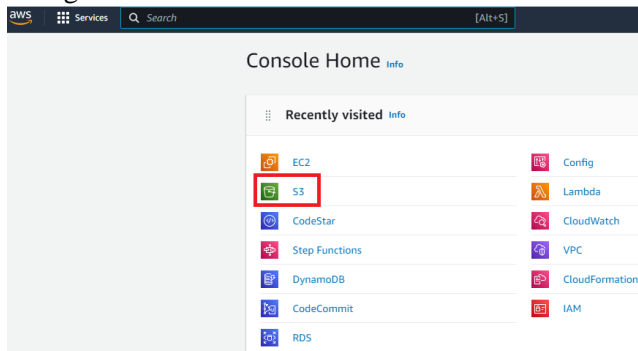
☐ Remember this account

[Sign in using root user email](#)

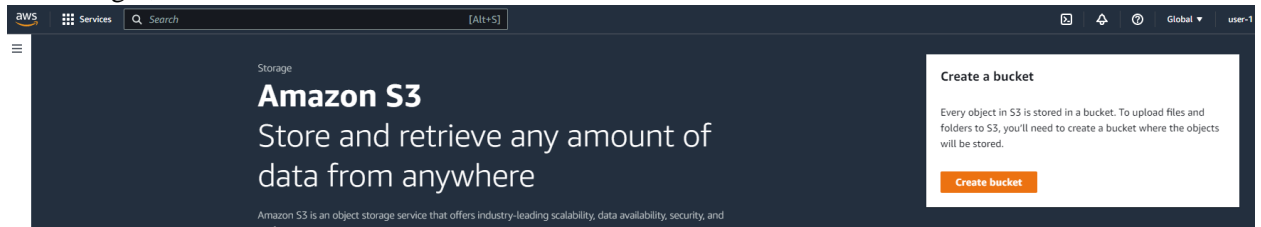
[Forgot password?](#)



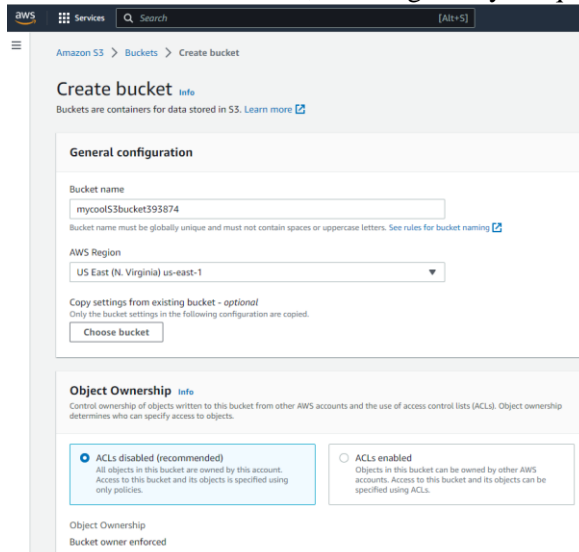
### 5. Navigate to S3.



### 6. On the right, click **Create bucket**.



### 7. In the **Bucket name** field, enter a globally unique bucket name (e.g., mycools3bucket393874).



8. Leave all other default settings and click **Create bucket**. You should receive an Access Denied error, indicating that your group policy is in effect.

**Default encryption** [Info](#)  
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type [Info](#)  
☒ Amazon S3 managed keys (SSE-S3)  
☐ AWS Key Management Service key (SSE-KMS)

**Bucket Key**  
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)  
☐ Disable  
☒ Enable

► **Advanced settings**

ⓘ After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

❌ **Failed to create bucket**  
To create a bucket, s3:CreateBucket permissions are required.  
  
View your permissions in the IAM console [IAM console](#). Identity and Access Management in Amazon S3 [IAM console](#)  
  
► API response

Cancel **Create bucket**

9. Navigate to **EC2**. You should see a number of API errors, indicating that you do not have access to EC2.

**EC2 Dashboard**  
EC2 Global View

Events  
Limits

▼ **Instances**  
Instances  
Instance Types  
Launch Templates  
Spot Requests  
Savings Plans  
Reserved Instances  
Dedicated Hosts  
Scheduled Instances  
Capacity Reservations

▼ **Images**  
AMIs  
AMI Catalog

▼ **Elastic Block Store**  
Volumes  
Snapshots  
Lifecycle Manager

▼ **Network & Security**  
Security Groups  
Elastic IPs

**Resources**  
You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running) 0	Auto Scaling Groups API Error	Dedicated Hosts API Error
Elastic IPs API Error	Instances API Error	Key pairs API Error
Load balancers API Error	Placement groups API Error	Security groups API Error
Snapshots API Error	Volumes API Error	

ⓘ Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. [Learn more](#)

**Launch instance**  
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.  
  
**Launch instance** ▼ [Migrate a server](#)  
  
Note: Your instances will launch in the US East (N. Virginia) Region

**Scheduled events**  
  
US East (N. Virginia)  
  
❌ **An error occurred**  
There was an error while checking for scheduled events

**Service health**  
Region: US East (N. Virginia) Status: This service is operating normally  
  
**Zones**  
Zone name Zone ID  
  
An error occurred  
An error occurred retrieving service health information  
  
[Enable additional Zones](#)

**Account attributes**  
[Supported platforms](#)  
  
❌ **An error occurred**  
An error occurred retrieving supported platforms  
  
❌ **An error occurred**  
An error occurred checking for a default VPC  
  
**Settings**  
EBS encryption  
Zones  
EC2 Serial Console  
Default credit specification  
Console experiments

**Explore AWS**  
  
**Save up to 90% on EC2 with Spot Instances**  
Optimize price-performance by combining EC2 purchase options single EC2 ASG. [Learn more](#)  
  
**Amazon GuardDuty Malware Protection**  
GuardDuty now provides agentless malware detection in Amazon EC2 container workloads. [Learn more](#)  
  
**Get Up to 40% Better Price Performance**  
T4g instances deliver the best price performance for burstable ge purpose workloads in Amazon EC2. [Learn more](#)

10. In the top right corner of the page, expand the **user-1** dropdown menu.
11. Copy the **Account ID** and then click **Sign out**.

**EC2 Dashboard**  
EC2 Global View

Events  
Limits

▼ **Instances**  
Instances  
Instance Types  
Launch Templates  
Spot Requests  
Savings Plans  
Reserved Instances  
Dedicated Hosts  
Scheduled Instances  
Capacity Reservations

▼ **Images**  
AMIs  
AMI Catalog

▼ **Elastic Block Store**  
Volumes  
Snapshots  
Lifecycle Manager

▼ **Network & Security**  
Security Groups  
Elastic IPs

**Resources**  
You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running) 0	Auto Scaling Groups API Error	Dedicated Hosts API Error
Elastic IPs API Error	Instances API Error	Key pairs API Error
Load balancers API Error	Placement groups API Error	Security groups API Error
Snapshots API Error	Volumes API Error	

ⓘ Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. [Learn more](#)

**Launch instance**  
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.  
  
**Launch instance** ▼ [Migrate a server](#)  
  
Note: Your instances will launch in the US East (N. Virginia) Region

**Scheduled events**  
  
US East (N. Virginia)  
  
❌ **An error occurred**  
There was an error while checking for scheduled events

**Service health**  
Region: US East (N. Virginia) Status: This service is operating normally  
  
**Zones**  
Zone name Zone ID  
  
An error occurred  
An error occurred retrieving service health information  
  
[Enable additional Zones](#)

**Account attributes**  
[Supported platforms](#)  
  
❌ **An error occurred**  
An error occurred retrieving supported platforms  
  
❌ **An error occurred**  
An error occurred checking for a default VPC  
  
**Settings**  
EBS encryption  
Zones  
EC2 Serial Console  
Default credit specification  
Console experiments

**Explore AWS**  
  
**Save up to 90% on EC2 with Spot Instances**  
Optimize price-performance by combining EC2 purchase options single EC2 ASG. [Learn more](#)  
  
**Amazon GuardDuty Malware Protection**  
GuardDuty now provides agentless malware detection in Amazon EC2 container workloads. [Learn more](#)  
  
**Get Up to 40% Better Price Performance**  
T4g instances deliver the best price performance for burstable ge purpose workloads in Amazon EC2. [Learn more](#)

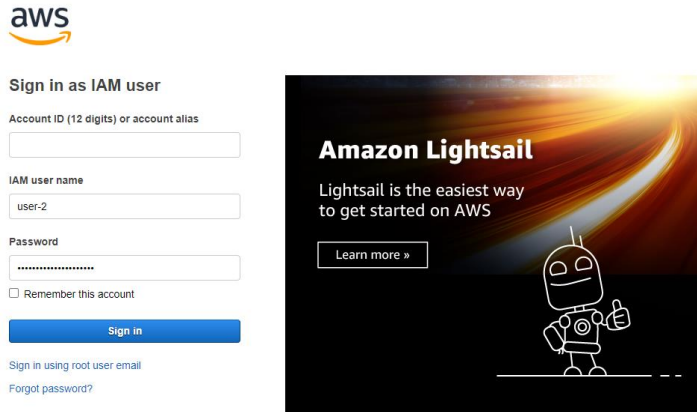
**Account ID**  
IAM user: user-1

**Account**  
Organization  
Service Quotas  
Billing Dashboard  
Security credentials

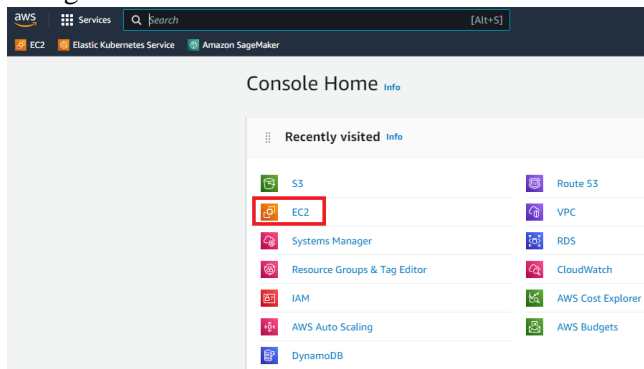
**Settings**  
[Redacted]  
  
[Switch role](#) **Sign out**

### 3.2. Sign-In as user-2

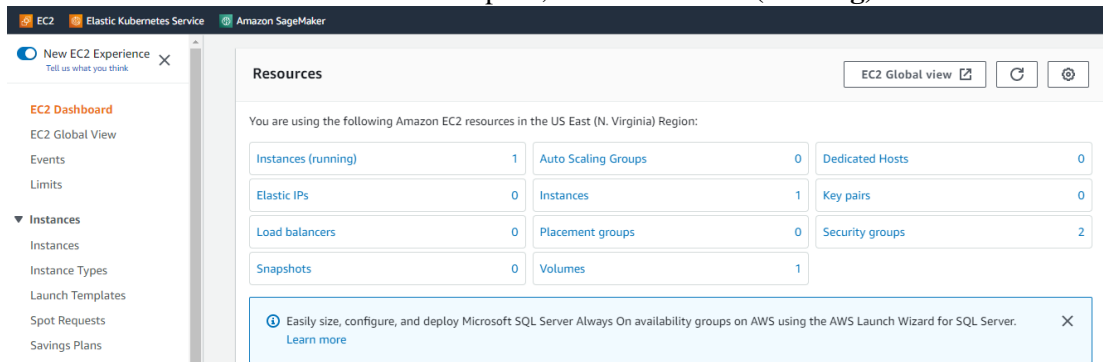
1. Click **Log back in** and then paste your copied account ID in the **Account ID** field.
2. Log in to the AWS Management Console as **user-2** using the password provided in the lab's resources. Remember that this user only has read-only access to EC2.



3. Navigate to **EC2**.

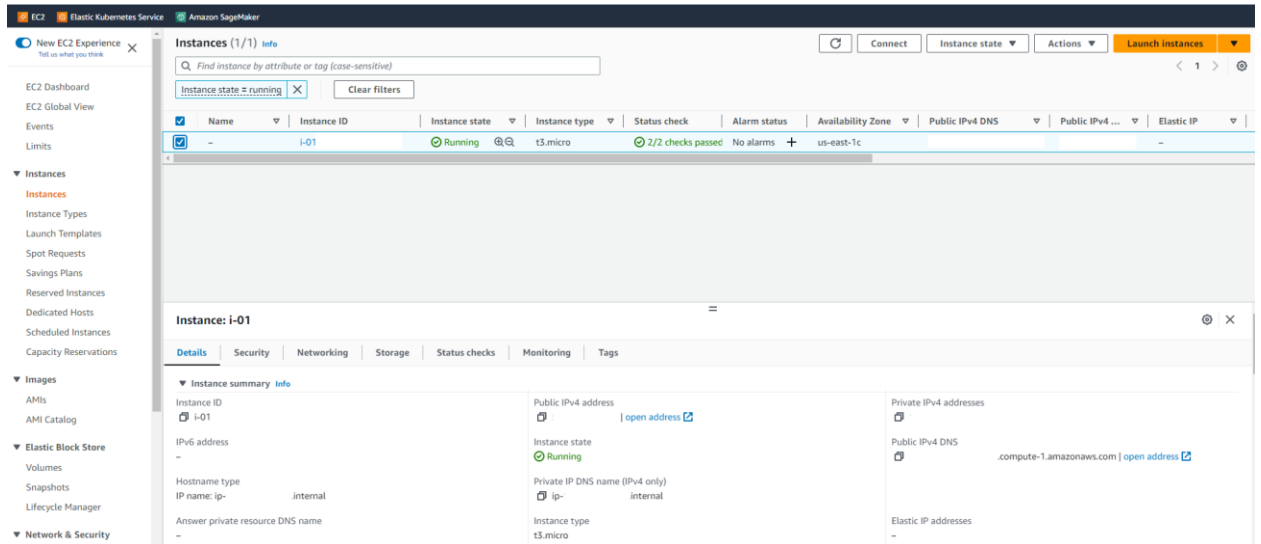


4. From the **Resources** section in the main pane, select **Instances (running)**.

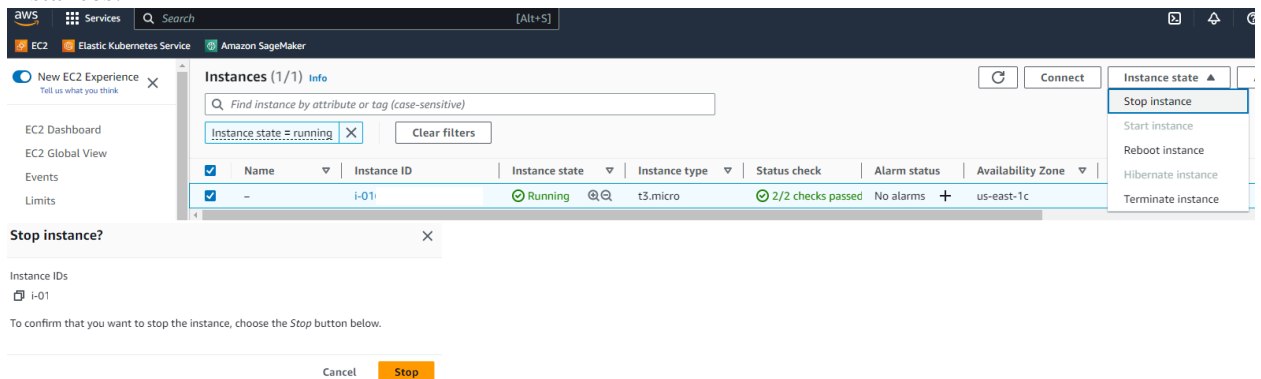


5. Check the checkbox to the left of the running instance and review the instance details.

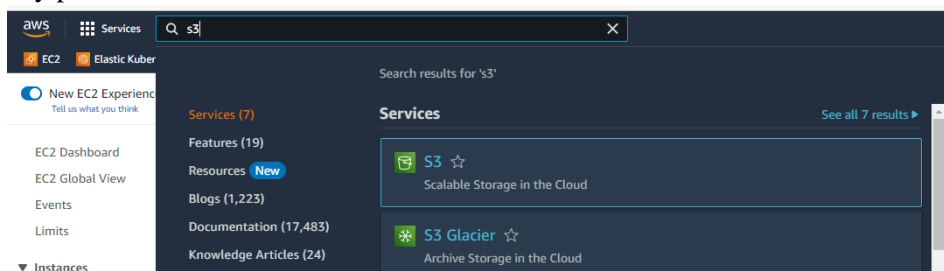


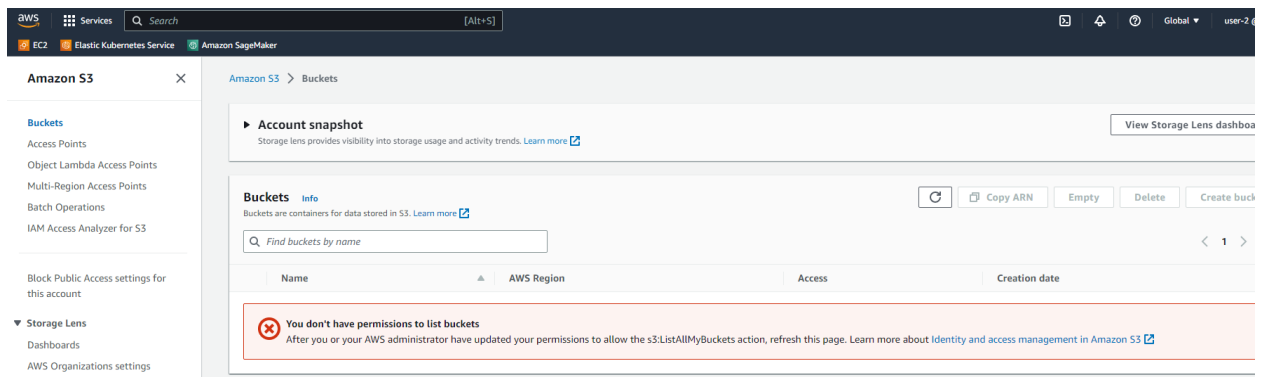


- Along the top of the page, use the **Instance state** dropdown to select **Stop instance**, and then click **Stop**. You should see an error message, since this user doesn't have the permissions to stop instances.

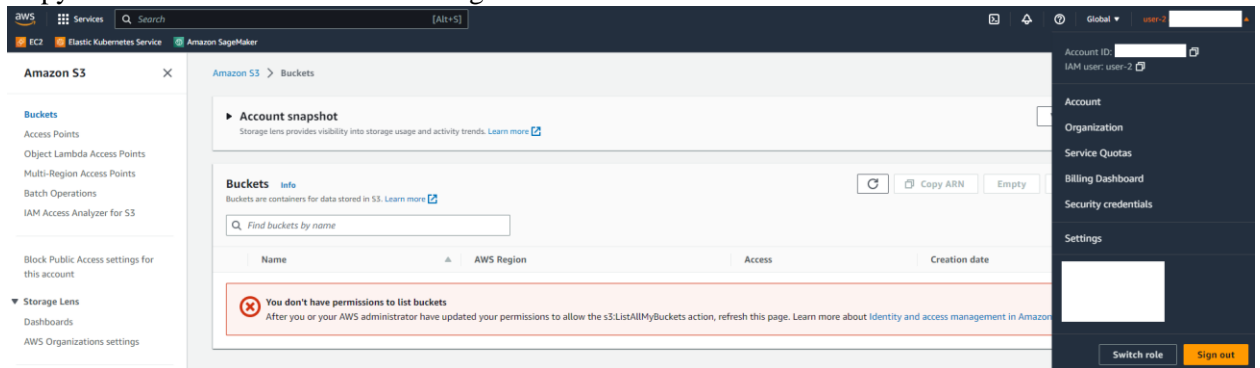


- Navigate to **S3**. You should see that S3 is unavailable for **user-2** because this user doesn't have any permissions outside of EC2.



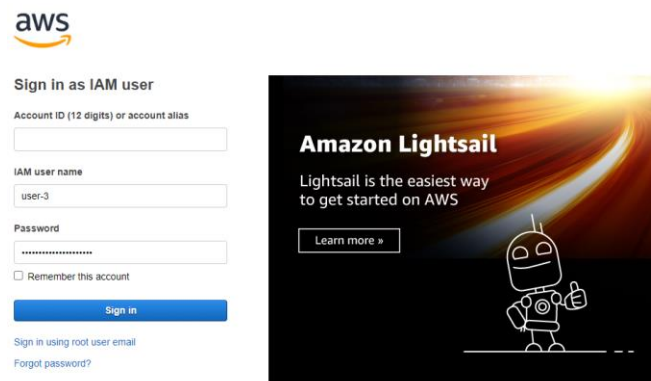


8. In the top right corner of the page, expand the **user-2** dropdown menu.
9. Copy the **Account ID** and then click Sign out.

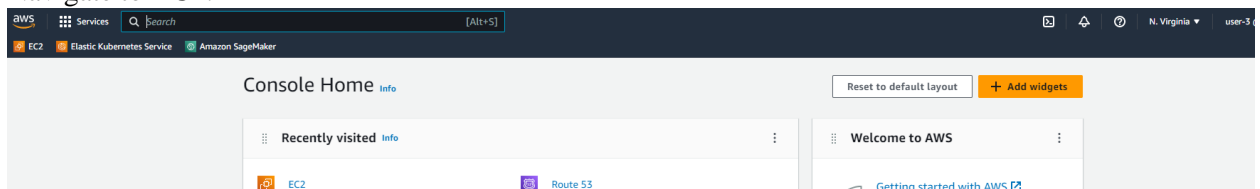


### 3.3. Sign-In as user-3

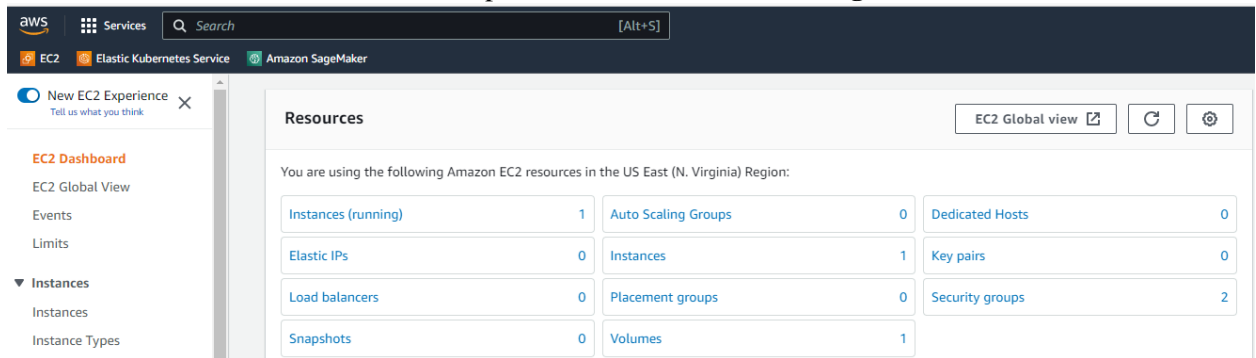
1. Click **Log back in** and then paste your copied account ID in the **Account ID** field.
2. Log in to the AWS Management Console as **user-3** using the password provided in the lab's resources. Remember that this user can view, start, and stop EC2 instances.



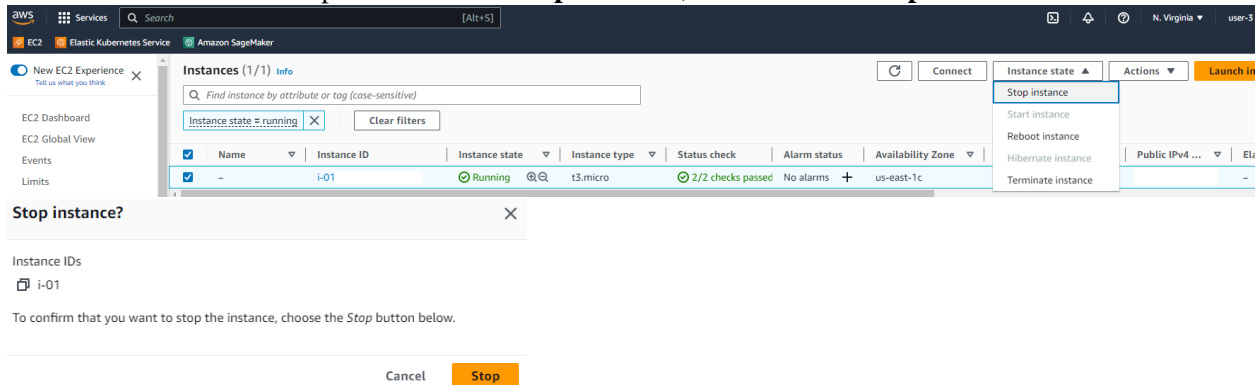
3. Navigate to **EC2**.



4. From the **Resources** section in the main pane, select **Instances (running)**.



5. Check the checkbox to the left of the running instance.
6. Use the **Instance state** dropdown to select **Stop instance**, and then click **Stop**.



7. After a minute, refresh the instances page to verify the instance is now in a **Stopped** state.

