

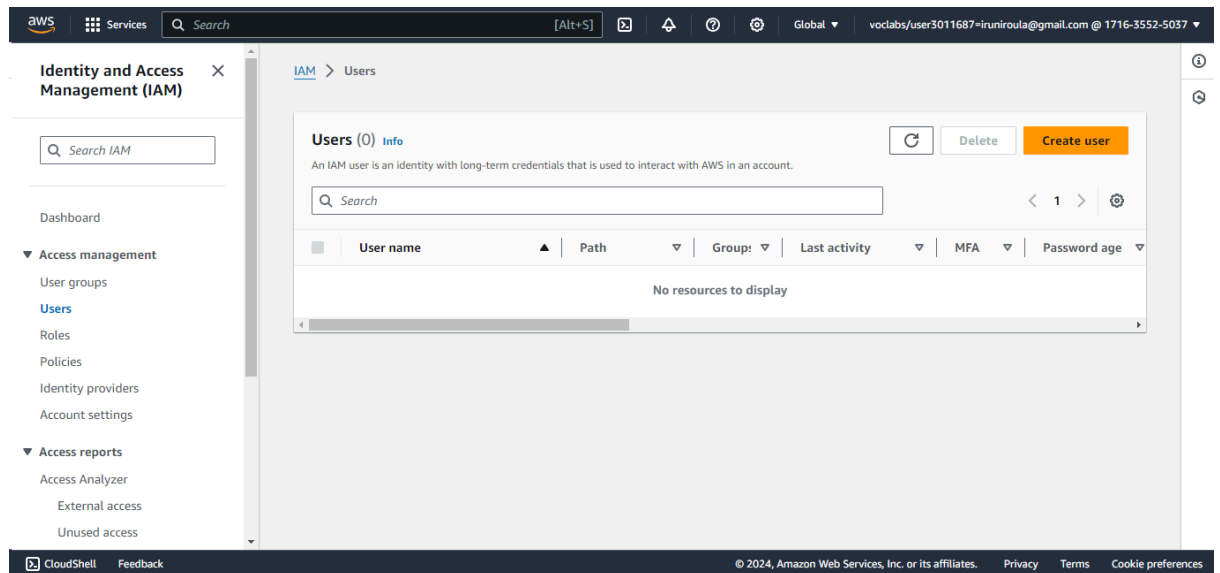
IAM Users and Roles Lab

Objective: To understand AWS Identity and Access Management (IAM) by creating and managing users, groups, and roles.

Approach: Students will create new IAM users, assign them to groups, and apply policies to manage permissions. The lab will also involve creating roles for AWS services and understanding the use of IAM roles for cross-service access.

Goal: Students will learn about user and permission management in AWS, the importance of roles for security and best practices for IAM.

Create a new IAM User Group



Inserting user details

The screenshot shows the 'Specify user details' page in the AWS IAM console. The left sidebar indicates the current step is 'Specify user details' (Step 2), with other steps being 'Set permissions', 'Review and create', and 'Retrieve password'. The main content area is titled 'User details' and contains the following fields and options:

- User name:** A text input field containing 'iru'. Below it, a note states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , _ @ - (hyphen)'.
- Provide user access to the AWS Management Console - optional:** A checked checkbox with a note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.'
- Console password:** A section with two options:
 - Autogenerated password:** An unselected radio button with the note: 'You can view the password after you create the user.'
 - Custom password:** A selected radio button. Below it is a text input field containing 'this@2024'. A note states: 'Enter a custom password for the user.'
- Custom password requirements:** A list of requirements:
 - Must be at least 8 characters long
 - Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + = , - (hyphen) [] { } ' "
- Show password:** A checked checkbox.
- Users must create a new password at next sign-in - Recommended:** A checked checkbox with a note: 'Users automatically get the IAMUserChangePassword policy to allow them to change their own password.'

At the bottom of the main content area, there is an information box: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)'.

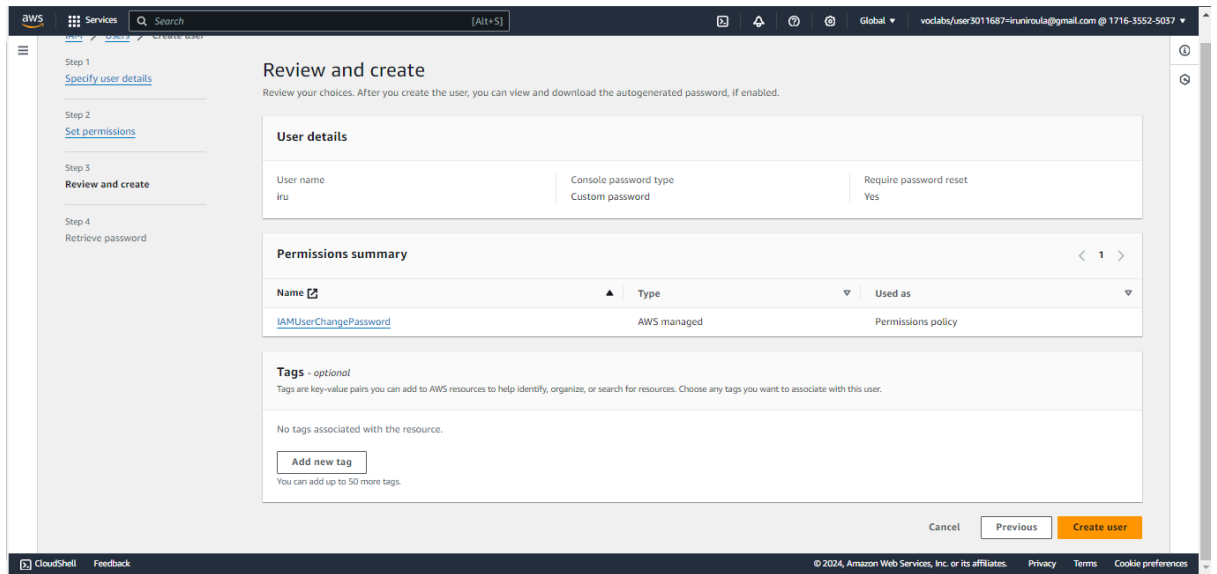
The bottom of the page features a 'Cancel' button and a 'Next' button.

Setting Permissions

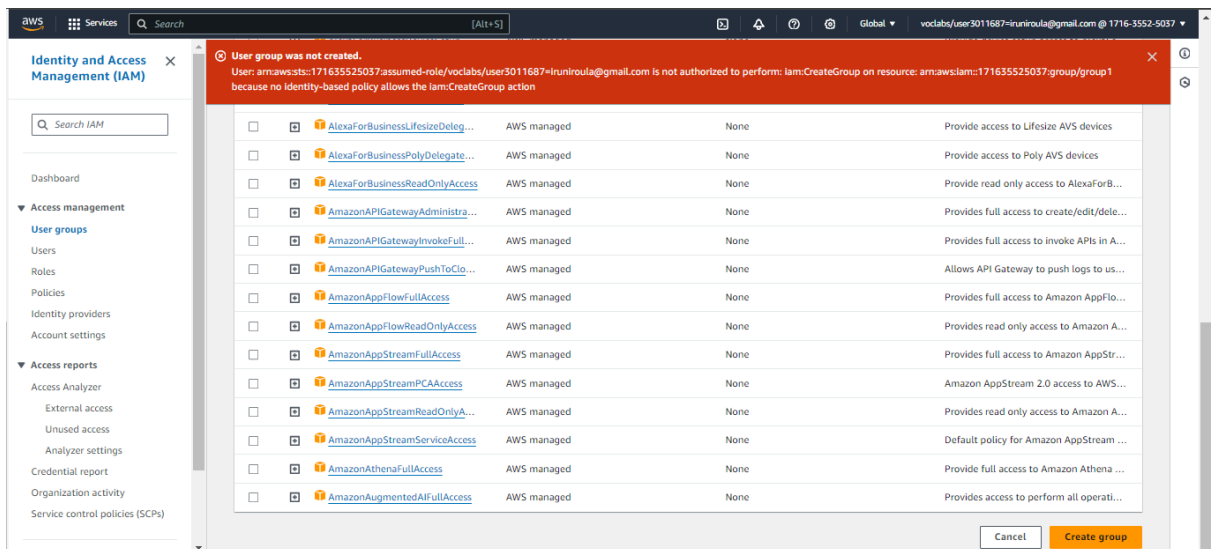
The screenshot shows the 'Set permissions' page in the AWS IAM console. The left sidebar indicates the current step is 'Set permissions' (Step 2), with other steps being 'Specify user details', 'Review and create', and 'Retrieve password'. The main content area is titled 'Set permissions' and contains the following sections:

- Permissions options:** A section with three radio button options:
 - Add user to group:** A selected radio button. Below it is a note: 'Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.'
 - Copy permissions:** An unselected radio button. Below it is a note: 'Copy all group memberships, attached managed policies, and inline policies from an existing user.'
 - Attach policies directly:** An unselected radio button. Below it is a note: 'Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.'
- Get started with groups:** A section with an information icon and a note: 'Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)'. To the right of this note is a 'Create group' button.
- Set permissions boundary - optional:** A section with a right-pointing arrow and the text 'Set permissions boundary - optional'.

At the bottom of the main content area, there are three buttons: 'Cancel', 'Previous', and 'Next'.



We are not authorized to create users or user groups. Therefore the rest of the actions are performed using AWS Cloud Foundations Lab



The following three users are created by default

<input type="checkbox"/>	user-1	/spl66/	0	-	-	✔ 8 minutes	-	Active - AKIAUGG
<input type="checkbox"/>	user-2	/spl66/	0	-	-	✔ 8 minutes	-	Active - AKIAUGG
<input type="checkbox"/>	user-3	/spl66/	0	-	-	✔ 8 minutes	-	Active - AKIAUGG

The following three user groups are created by default

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

IAM > User groups

User groups (3)

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

Search

< 1 >

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	EC2-Admin	0	✔ Defined	9 minutes ago
<input type="checkbox"/>	EC2-Support	0	✔ Defined	9 minutes ago
<input type="checkbox"/>	S3-Support	0	✔ Defined	9 minutes ago

Permission for EC2-Support Group

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > User groups > EC2-Support

EC2-Support

Summary

User group name

EC2-Support

Creation time

February 26, 2024, 14:12 (UTC+05:45)

ARN

arn:aws:iam::339712966097:group/spl66/EC2-Support

Users

Permissions

Access Advisor

Permissions policies (1)

You can attach up to 10 managed policies.

Search

Filter by Type

All types

< 1 >

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS managed	1

JSON Written Policy

PermissionsEntities attachedPolicy versions (2)Access Advisor

Permissions defined in this policy [Info](#)

CopySummaryJSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

1- [{
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:Describe*",
12- "Resource": "*" }
13- },
14- {
15- "Effect": "Allow",
16- "Action": [
17- "cloudwatch:ListMetrics",
18- "cloudwatch:GetMetricStatistics",
19- "cloudwatch:Describe*" }
20-] }
21-]

The following users need to be set to respective user groups

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

Adding users to the user group

aws

Services

Search

[Alt+S]

Global

vodafone/user3011687=iuniroula@gmail.com @ 3397-1296-6097

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > User groups > S3-Support

S3-Support [Info](#)

Delete

Edit

Summary

User group name

S3-Support

Creation time

February 26, 2024, 14:12 (UTC+05:45)

ARN

arn:aws:iam::339712966097:group/spl66/S3-Support

UsersPermissionsAccess 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

1

User name

Groups

Last activity

Creation time

No resources to display

Selecting user 1

<input checked="" type="checkbox"/>	user-1	0	None	25 minutes ago
<input type="checkbox"/>	user-2	0	None	25 minutes ago
<input type="checkbox"/>	user-3	0	None	25 minutes ago

Cancel

Add users

User added to the user group

1 user added to this group.

IAM > User groups > S3-Support

S3-Support

Info

Delete

Summary

Edit

User group name

S3-Support

Creation time

February 26, 2024, 14:12 (UTC+05:45)

ARN

arn:aws:iam::339712966097:group/spl66/S3-Support

Users (1)

PermissionsAccess Advisor

Users in this group (1)

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

< 1 > ⓘ

☐

User name🔍

▲

Groups

▼

Last activity

▼

Creation time

☐

[user-1](#)

1

None

26 minutes ago