

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.

Firstly create users in IAM. You can find IAM in aws Services.

[IAM](#) > [Users](#) > [Create user](#)

Step 1 of 3

Specify user details

User details

User name

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*
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

i 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](#)

Cancel **Next**

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☐ Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly

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.

Permissions policies (1182)

Choose one or more policies to attach to your new user.



Create policy

Filter by Type

Q Search


All types

< 1 2 3 4 5 6 7 ... 60 >

<input type="checkbox"/>	Policy name ↗	Type	Attached entities
<input type="checkbox"/>	<div><div>+</div><div> AccessAnalyzerSer...</div></div>	AWS managed	0
<input type="checkbox"/>	<div><div>+</div><div> AdministratorAccess</div></div>	AWS managed - jo...	1

Permissions summary

< 1 >

Name 



Type



Used as



No resources

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create user