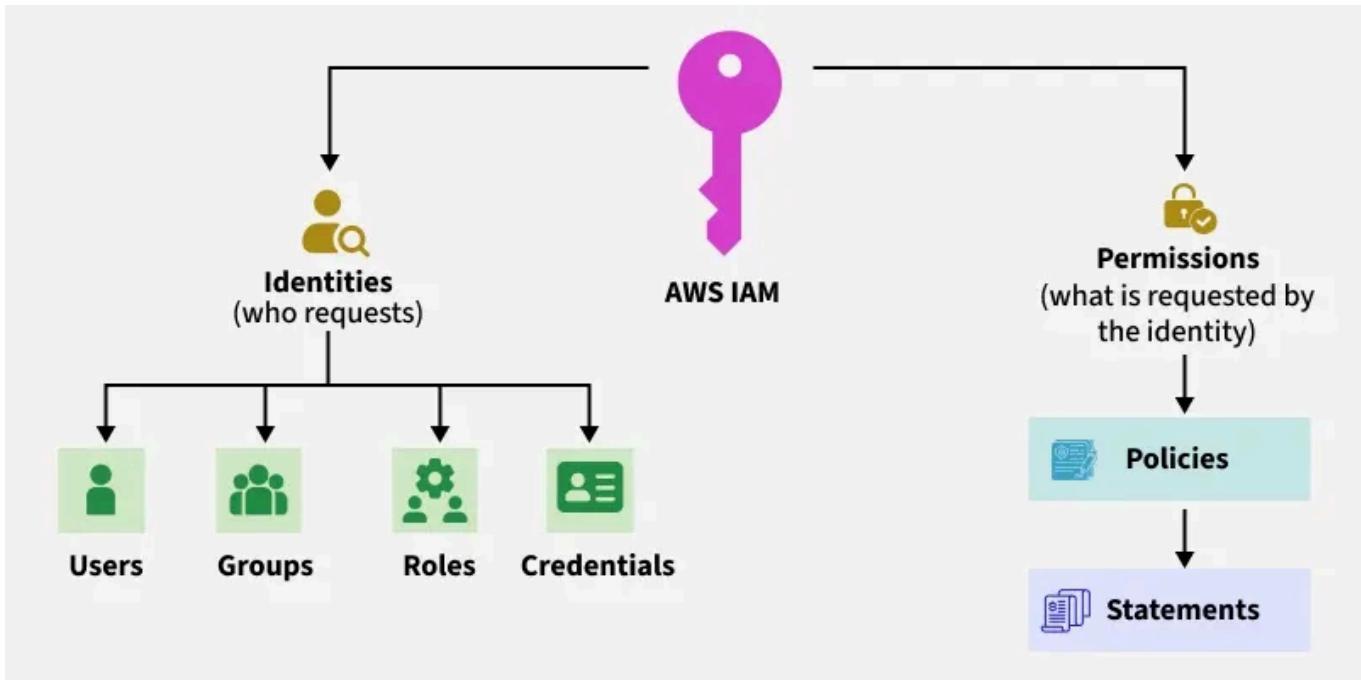


# IAM(Identity Access Management)

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can manage permissions that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources. IAM provides the infrastructure necessary to control authentication and authorization for your AWS accounts.



- > For owner account have a full permission
- > for IAM user have zero permission

**how to create a IAM :**

go to user and create user

The screenshot shows the 'Specify user details' step of the 'Create user' wizard. On the left, a sidebar lists steps: Step 1 (selected), Step 2, Step 3, Step 4, and Retrieve password. The main area is titled 'User details' and contains fields for 'User name' (with validation notes) and 'Console password' (radio buttons for 'Autogenerated password' or 'Custom password'). It also includes optional checkboxes for 'Provide user access to the AWS Management Console - optional' and 'Users must create a new password at next sign-in - Recommended'. A note at the bottom explains that users can generate programmatic access keys after creation.

set permission

The screenshot shows the 'Set permissions' step of the 'Create user' wizard. The sidebar shows 'Step 1' is selected. The main area has three options: 'Add user to group', 'Copy permissions', and 'Attach policies directly' (which is highlighted with a blue border). Below this is a table titled 'Permissions policies (1440)' showing a list of AWS managed policies. The table includes columns for 'Policy name', 'Type', and 'Attached entities'. Policies listed include 'AccessAnalyzerServiceRolePolicy', 'AccountManagementFromVercel', 'AdministratorAccess', etc.

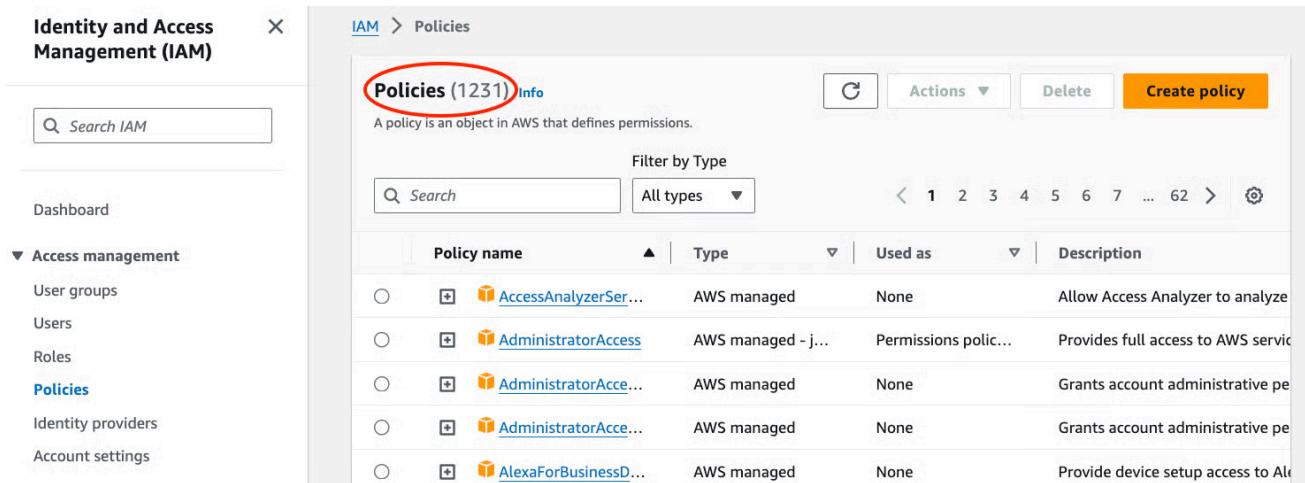
using this create the user.

## Creating and attaching policies to users, groups, and roles:

Creating and attaching policies to users, groups, and roles in AWS is pretty straightforward.

### Creating a policy:

- To create a policy, click “Policies” in the IAM console left-hand menu and click “Create Policy.”
- You can define your policy using the visual editor or the JSON tab. The visual editor is easier if you’re not familiar with JSON. For example, to create a policy that allows read-only access to S3, you can select the “S3 service” and then choose the “read-only” actions.
- Once you’ve defined the policy, click “Review policy.” Then, give your policy a name and description and click “Create policy.” At this point, your custom policy should be created.



The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, there's a sidebar with a search bar and a list of access management options: Dashboard, User groups, Users, Roles, Policies (which is selected and highlighted in blue), Identity providers, and Account settings. The main area is titled "Policies (1231)" and contains a table of existing policies. The table has columns for Policy name, Type, Used as, and Description. The first few rows show managed policies like "AccessAnalyzerServiceRole", "AdministratorAccess", and "AdministratorAccess". A red circle highlights the "Policies (1231)" link at the top left of the main content area.

Policy name	Type	Used as	Description
<a href="#">AccessAnalyzerServiceRole</a>	AWS managed	None	Allow Access Analyzer to analyze
<a href="#">AdministratorAccess</a>	AWS managed - j...	Permissions polic...	Provides full access to AWS services
<a href="#">AdministratorAccess</a>	AWS managed	None	Grants account administrative pe...
<a href="#">AdministratorAccess</a>	AWS managed	None	Grants account administrative pe...
<a href="#">AlexaForBusinessDeviceSetup</a>	AWS managed	None	Provide device setup access to Al...

## Attaching policies to users

- If you want to attach a policy to a user, go to “Users” in the IAM console and select the user to whom you want to attach the policy.
- Click on the “Permissions” tab and then click “Add permissions.”

Select “Attach policies directly,” find the policy you created (or any existing policy you want to attach) and choose it.

Step 1

**Add permissions**

Step 2

Review

## Add 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, inline policies, and any existing permissions boundaries 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 (1234)

Filter by Type

 s3

All types

21 matches

<input type="checkbox"/>	Policy name	Type	Att...
<input type="checkbox"/>	 <a href="#">AmazonDMSRedshiftS3Role</a>	AWS managed	0
<input type="checkbox"/>	 <a href="#">AmazonS3FullAccess</a>	AWS managed	8

- Go to “Roles” in the IAM console and select the role to which you want to attach a policy.
- Click on the “Permissions” tab and then click ”Add permissions.” This step is slightly different from what we’ve encountered previously. You’re shown the current permission policies and the complete list of other policies you can attach.