

Lab 2- IAM policy

- Go to IAM and click on Policies -> Create Policy

The screenshot shows the AWS IAM console 'Policies' page. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, User groups, Users, Roles, Policies (selected), Identity providers, Account settings, and Root access management. The main content area is titled 'Policies (1329)' and includes a search bar, a 'Filter by Type' dropdown set to 'All types', and a table of policies. The table has columns for Policy name, Type, Used as, and Description. Policies listed include AccessAnalyzerSer..., AdministratorAccess, and AI Ops Assistant Policy.

Policy name	Type	Used as	Description
AccessAnalyzerSer...	AWS managed	None	-
AdministratorAccess	AWS managed - job fu...	Permissions policy (2)	Provides full access to AWS services an
AdministratorAcce...	AWS managed	None	Grants account administrative permis
AdministratorAcce...	AWS managed	None	Grants account administrative permis
AI Ops Assistant Policy	AWS managed	None	Provides ReadOnly permissions requir.
AI Ops ConsoleAdmi...	AWS managed	None	Grants full access to Amazon AI Opera

In visual

The screenshot shows the 'Policy editor' in 'Visual' mode. It is configured for the 'S3' service with 'All actions' allowed. The 'Actions allowed' section shows 'All S3 actions (s3:*)' selected. The 'Effect' is set to 'Allow'. The 'Resources' section is set to 'All'. A warning message states: 'The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.' There are also links for 'Expand all' and 'Collapse all'.

Policy editor [Visual] [JSON] [Actions] [Icon]

▼ **S3** [Allow] All actions

Specify what actions can be performed on specific resources in **S3**.

▼ **Actions allowed**

Specify actions from the service to be allowed.

[Filter Actions]

Manual actions | [Add actions](#)

☒ All S3 actions (s3:*)

Access level

► **List (Selected 16/16)**

Effect

☒ Allow ☐ Deny

[Expand all](#) | [Collapse all](#)

▼ **Resources**

Specify resource ARNs for these actions.

☒ All ☐ Specific

⚠ The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

► **Request conditions - optional**

Actions on resources are allowed or denied only when these conditions are met.

Check json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Provide policy a name and create policy

Policy details

Policy name

Enter a meaningful name to identify this policy.

mys3policy

Maximum 128 characters. Use alphanumeric and '+=,._@-_' characters.

Description - optional

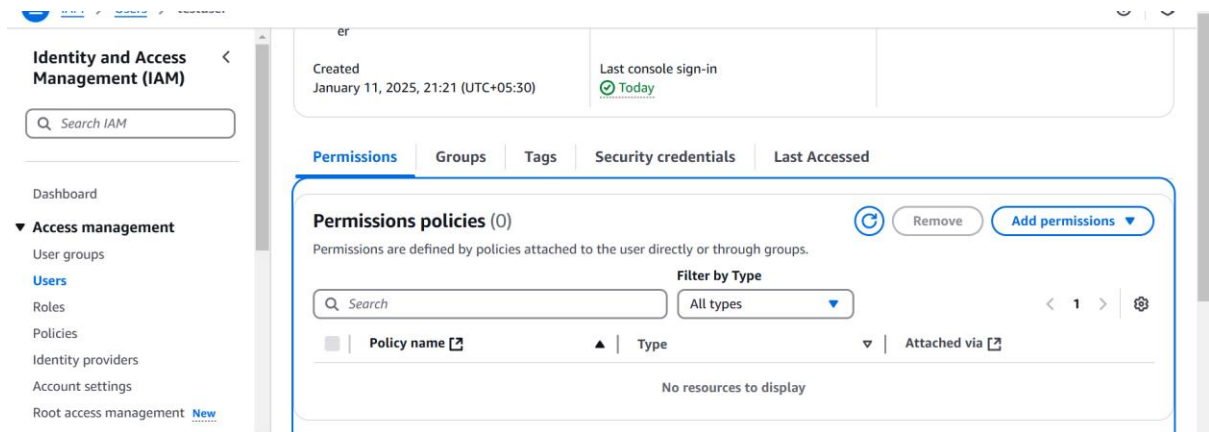
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,._@-_' characters.

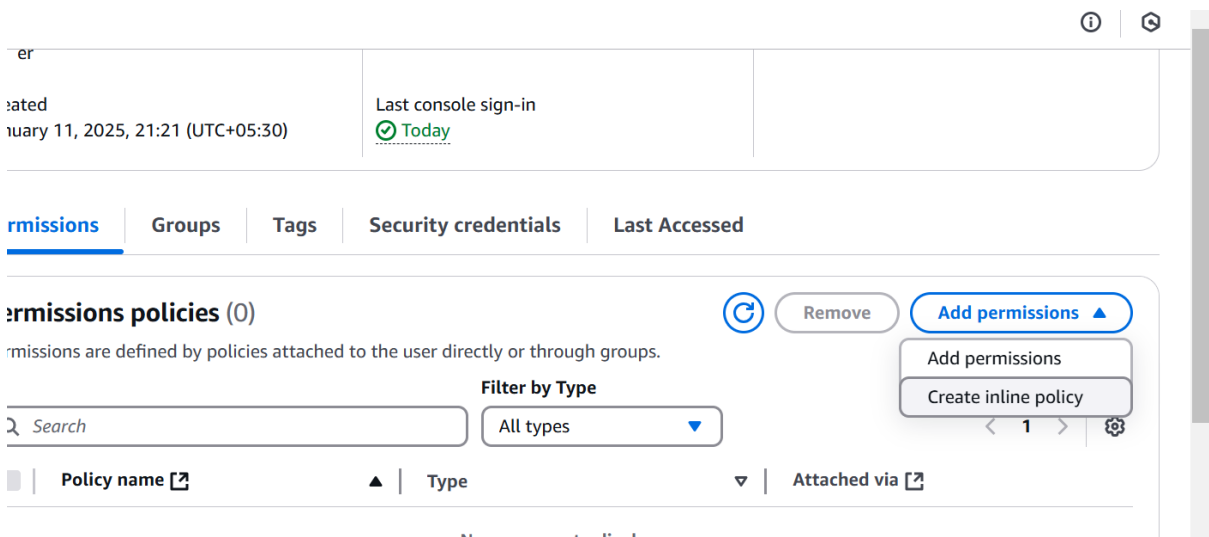
Permissions defined in this policy [Info](#) [Edit](#)

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

Click on user and click on your user and add permission



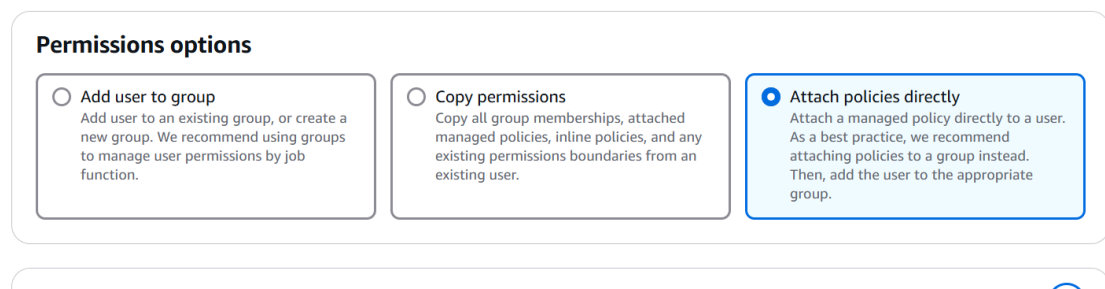
Add Permission



Attach policy directly

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](#)



Attach policy

Permissions policies (1/1332)

Filter by Type

Q my

X

All types

▼

6 matches

< 1 >

<div><div>[-]</div></div>	Policy name ↗	Type	Attached entities
<input type="checkbox"/>	<div><div>+</div> mypolicy</div>	Customer managed	1
<input checked="" type="checkbox"/>	<div><div>+</div> mys3policy</div>	Customer managed	0
<input type="checkbox"/>	<div><div>+</div> s3crr_for_myamit23bucket_4...</div>	Customer managed	1
<input type="checkbox"/>	<div><div>+</div> s3crr_for_myamit23bucket_5...</div>	Customer managed	1
<input type="checkbox"/>	<div><div>+</div> s3crr_for_myamit23bucket_c...</div>	Customer managed	1
<input type="checkbox"/>	<div><div>+</div> s3replicate_for_myamit23buc...</div>	Customer managed	1

Cancel

Next

Add permission

Review

The following policies will be attached to this user. [Learn more](#) [↗](#)

User details

User name
testuser

Permissions summary (1)

Name [↗](#)

▼

Type

Used as

[mys3policy](#)

Customer managed

Permissions policy

Cancel

Previous

Add permissions

Now go to testuser portal, and check s3 resource