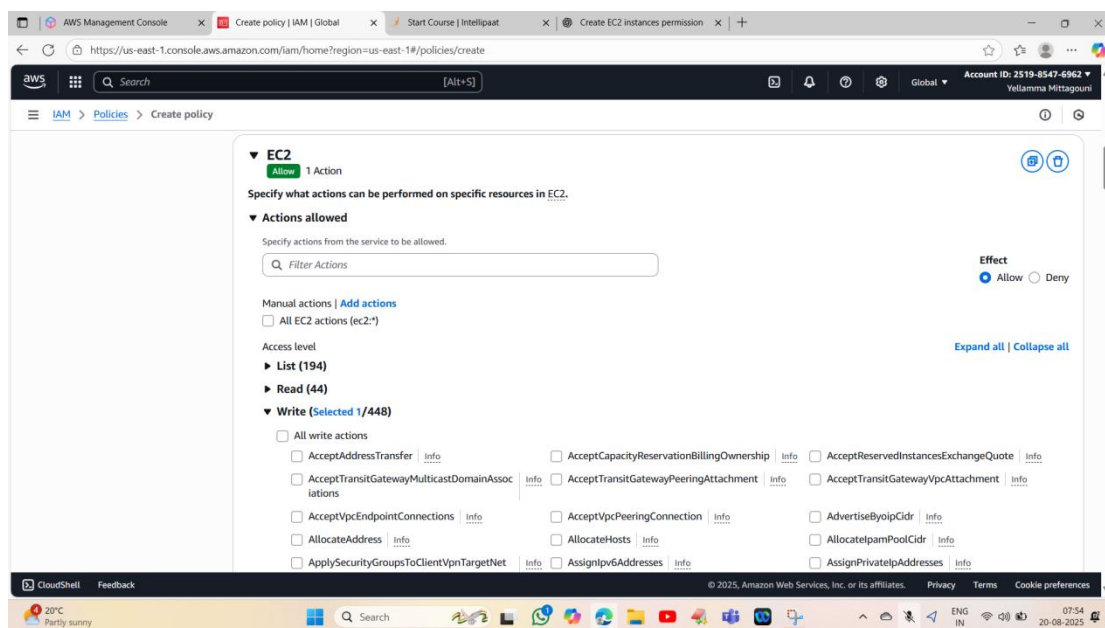
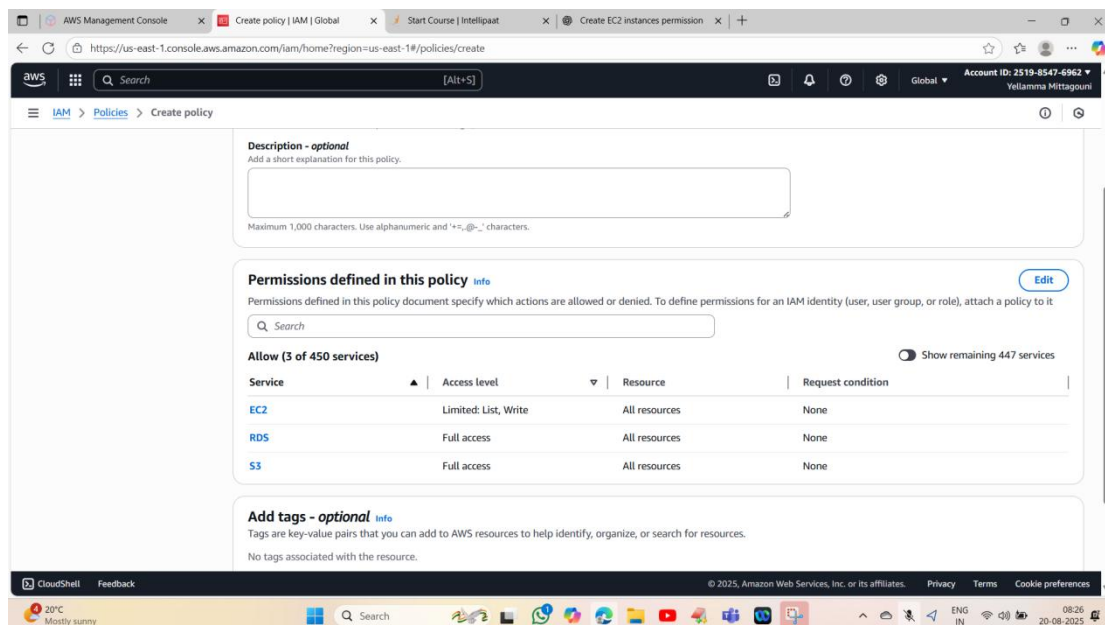
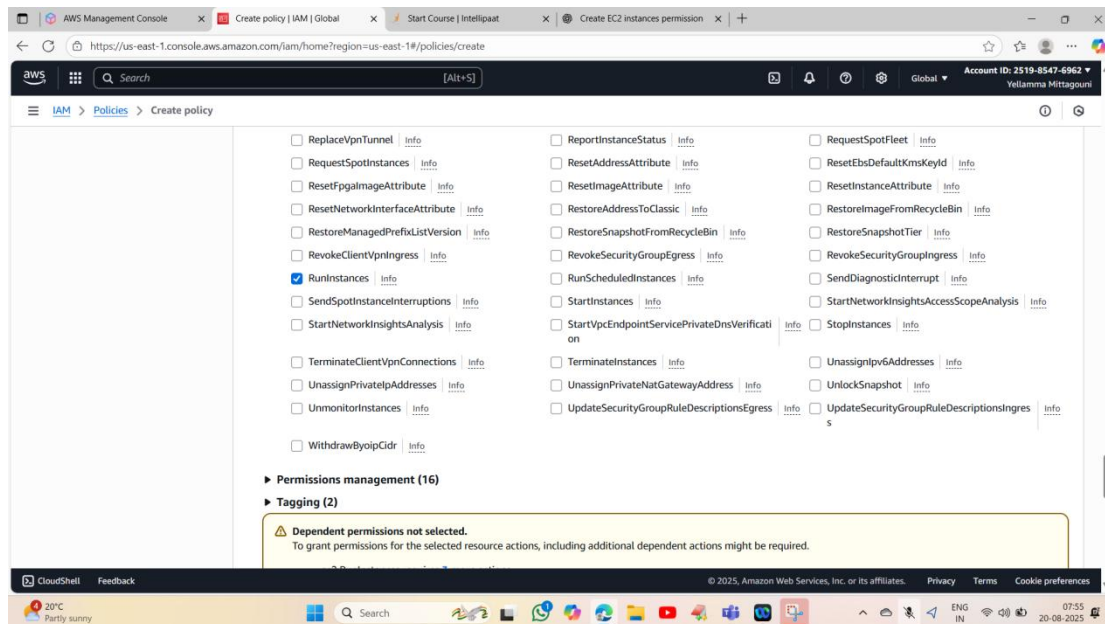


1. Create policy number 1 which lets the users to:
 - a. Access S3 completely
 - b. Only create EC2 instances
 - c. Full access to RDS





2. Create a policy number 2 which allows the users to:
 - a. Access CloudWatch and billing completely
 - b. Can only list EC2 and S3 resources

AWS Management Console | Create policy | IAM | Global | Start Course | Intellipaat | Create EC2 instances permission

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create

Search [Alt+S]

Global Account ID: 2519-8547-6962 Yellamma Mittagouni

Step 1: Review and create

Policy editor

Visual JSON Actions

CloudWatch

Allow All actions

Specify what actions can be performed on specific resources in CloudWatch.

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Manual actions | Add actions

☒ All CloudWatch actions (cloudwatch:*)

Access level

- List (Selected 7/7)
- Read (Selected 21/21)
- Write (Selected 25/25)
- Tagging (Selected 2/2)

Effect: ☒ Allow ☐ Deny

Expand all | Collapse all

Resources

Specify resource ARNs for these actions.

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

20°C Mostly sunny

AWS Management Console | Create policy | IAM | Global | Start Course | Intellipaat | Create EC2 instances permission

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create

Search [Alt+S]

Global Account ID: 2519-8547-6962 Yellamma Mittagouni

Step 1: Specify permissions

Specify permissions

Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual JSON Actions

Billing

Allow All actions

Specify what actions can be performed on specific resources in Billing.

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Manual actions | Add actions

☒ All Billing actions (billing:*)

Access level

- List (Selected 1/1)
- Read (Selected 12/12)
- Write (Selected 7/7)
- Permissions management (Selected 3/3)
- Tagging (Selected 2/2)

Effect: ☒ Allow ☐ Deny

Expand all | Collapse all

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Nifty bank -0.29%

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Watchlist

Ideas

Search

ENG IN

10:49

20-08-2025

AWS Management Console

Create policy | IAM | Global

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create

Search

[Alt+S]

IAM

Policies

Create 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

Search

Allow (2 of 450 services)

Show remaining 448 services

Service	Access level	Resource	Request condition
Billing	Full access	All resources	None
CloudWatch	Full access	All resources	None

Add tags - optional

Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create policy

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Watchlist

Ideas

Search

ENG IN

11:43

20-08-2025

AWS Management Console

Create policy | IAM | Global

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create

Search

[Alt+S]

IAM

Policies

Create 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

Search

Allow (2 of 450 services)

Show remaining 448 services

Service	Access level	Resource	Request condition
EC2	Limited: List	All resources	None
S3	Limited: List	All resources	None

Add tags - optional

Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

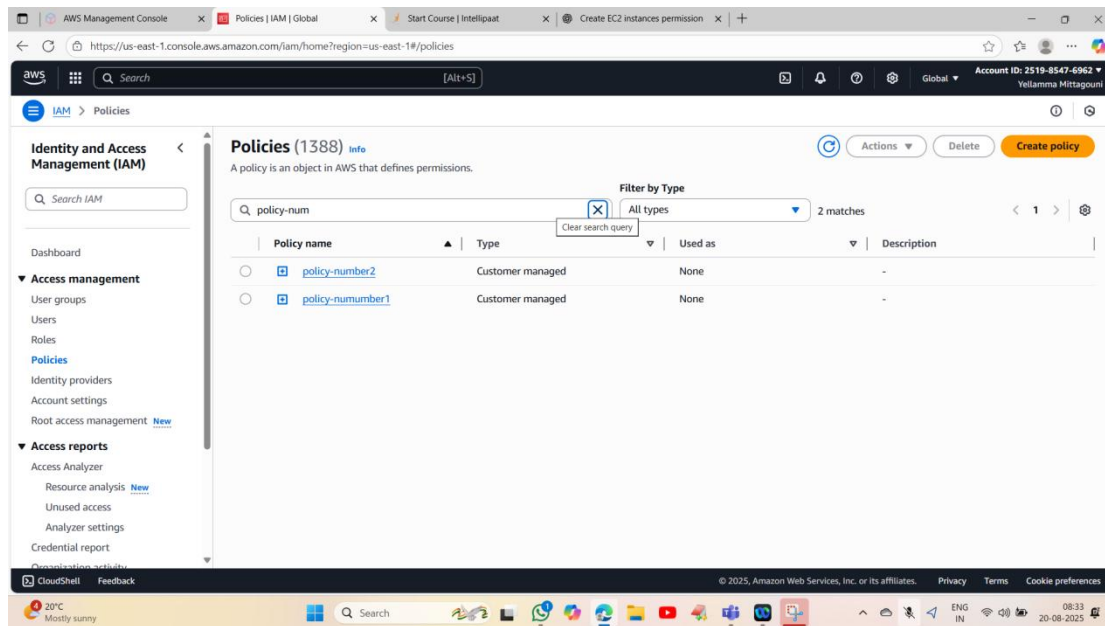
Add new tag

You can add up to 50 more tags.

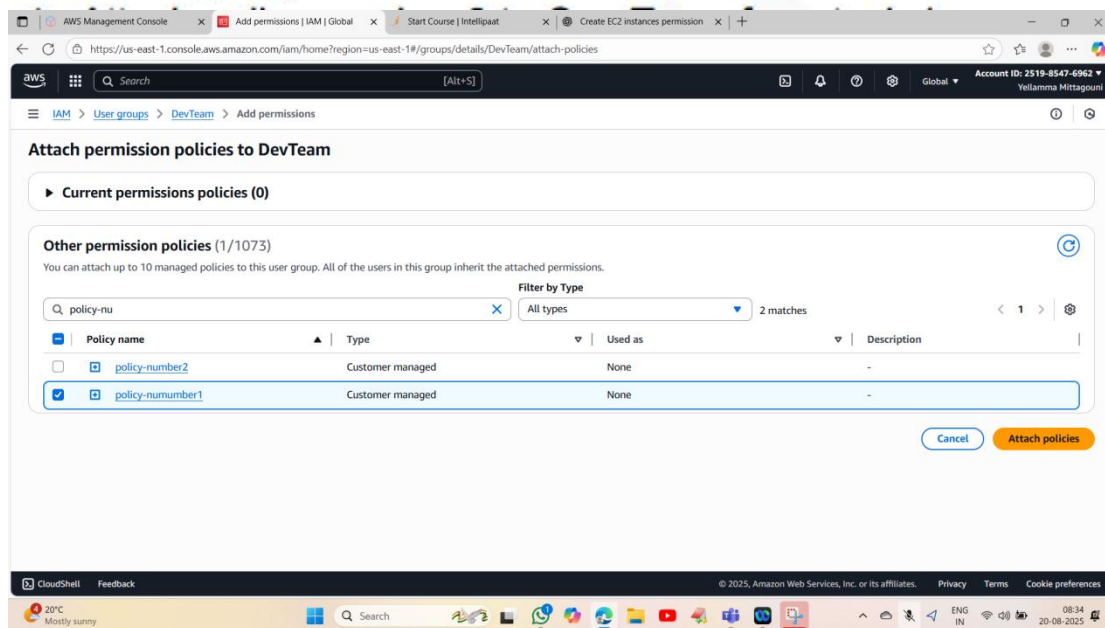
Cancel

Previous

Create policy



3. Attach policy number 1 to the Dev Team from task 1



4. Attach policy number 2 to Ops Team from task 1

The screenshot shows the AWS IAM console interface for attaching permissions policies to the 'OpsTeam' group. The breadcrumb navigation is 'IAM > User groups > OpsTeam > Add permissions'. The page title is 'Attach permission policies to OpsTeam'. Below this, there are two sections: 'Current permissions policies (0)' and 'Other permission policies (1/1073)'. The 'Other permission policies' section includes a search bar with the text 'policy-nu' and a dropdown menu set to 'All types', showing '2 matches'. A table lists the policies:

<input type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	policy-number2	Customer managed	None	-
<input type="checkbox"/>	policy-number1	Customer managed	Permissions policy (1)	-

At the bottom right of the table, there are two buttons: 'Cancel' and 'Attach policies' (highlighted in orange). The footer of the console shows '© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'. The Windows taskbar at the bottom indicates a temperature of 21°C, 'Mostly sunny' weather, and the time 08:35 on 20-08-2025.