

Task-1

User Name:

User details

User name

EC2User1

User Group: (Adding the user to the group)

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

SuperAdmin

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

Add users to the group - *Optional* (4) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Q EC2User1



0 matches



1



Attaching Permissions:

Attach permissions policies - *Optional* (1023) [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Q EC2Super Admin



Filter by Type

All types

0 matches



1



Defining 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



▼ EC2

Allow All actions

Specify what actions can be performed on specific resources in EC2.

▼ Actions allowed

Specify actions from the service to be allowed.

Q Filter Actions

Effect

☒ Allow ☐ Deny

Manual actions | [Add actions](#)

☒ All EC2 actions (ec2:*)

Access level

► List (Selected 186/186)

► Read (Selected 40/40)

▼ Write (Selected 440/440)

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

Task-2

User Name:

User details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

User Group: (Adding the user to the group)

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

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

Add users to the group - *Optional* (4) [Info](#)


An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

0 matches

Attaching Permissions:

Attach permissions policies - *Optional* (1/1023) [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type					1 match	
<input type="text" value="EC2ReadOnly"/>						
<input checked="" type="checkbox"/>	Policy name	Type	Used as	Description		
<input checked="" type="checkbox"/>	 AmazonEC2ReadOnlyAccess	AWS managed	None	Provides read only access to Amazon E...		

Defining Permissions:

Specify permissions [Info](#)

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

Policy editor

VisualJSONActions

▼ EC2

Allow40 Actions

Specify what actions can be performed on specific resources in EC2.

▼ Actions allowed

Specify actions from the service to be allowed.

Effect

☒ Allow ☐ Deny

Manual actions | [Add actions](#)

☐ All EC2 actions (ec2:*)

Access level

☒ List (186)

☒ Read (Selected 40/40)

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

Task-3

User Name:

User details

User name

User Group: (Adding the user to the group)

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

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

Add users to the group - *Optional* (4) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.



0 matches



1



Attaching Permissions:

Attach permissions policies - *Optional* (1/1023) [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.



Filter by Type

All types

0 matches



1



Defining 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 ▼



▼ Cost Explorer Service

Allow 27 Actions

Specify what actions can be performed on specific resources in Cost Explorer Service.

▼ Actions allowed

Specify actions from the service to be allowed.

Effect

☒ Allow ☐ Deny

Manual actions | [Add actions](#)

☐ All Cost Explorer Service actions (ce:*)

Access level

► List (5)

► Read (Selected 27/27)

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

Task-4

User Name:

User details

User name

User Group: (Adding the user to the group)

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

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

Add users to the group - *Optional* (4) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.



0 matches

< 1 >

Attaching Permissions:

Attach permissions policies - *Optional* (1/1023) [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.



Filter by Type

All types

0 matches

< 1 >

Defining Permissions:

Step 1

Step 2

Specify permissions

Review and create

Specify permissions

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

Policy editor

VisualJSONActions

▼ Cost Explorer Service

Allow27 Actions

Specify what actions can be performed on specific resources in Cost Explorer Service.

▼ Actions allowed

Specify actions from the service to be allowed.

QFilter Actions

Effect

Allow

Deny

Manual actions | Add actions

☐ All Cost Explorer Service actions (bcm*)

Access level

► List (5)

► Read (selected 27/27)

► Write (22)

► Tagging (2)

Expand all | Collapse all

► Resources

Specify resource ARNs for these actions.

► Request conditions - optional

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

▼ BillingAndCostManagementDataExports

Allow4 Actions

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

▼ Actions allowed

Specify actions from the service to be allowed.

QFilter Actions

Effect

Allow

Deny

Manual actions | Add actions

☐ All BillingAndCostManagementDataExports actions (bcm-data-exports*)

Access level

► List (3)

► Read (selected 4/4)

► Write (3)

► Tagging (2)

Expand all | Collapse all

▼ Resources

Specify resource ARNs for these actions.

☐ All

☒ Specific

export | info

Specified export resource ARN for the DeleteExport and 7 more actions. Add ARNs to restrict access.

☐ Any in this account

table | info

Specified table resource ARN for the CreateExport and 2 more actions. Add ARNs to restrict access.

☐ Any in this account

► Request conditions - optional

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

▼ Cost and Usage Report

Allow6 Actions

Specify what actions can be performed on specific resources in Cost and Usage Report.

▼ Actions allowed

Specify actions from the service to be allowed.

QFilter Actions

Effect

Allow

Deny

Manual actions | Add actions

☐ All Cost and Usage Report actions (cur*)

Access level

► Read (selected 6/6)

► Write (4)

► Tagging (2)

Expand all | Collapse all

▼ Resources

Specify resource ARNs for these actions.

☐ All

☒ Specific

cur | info

Specified cur resource ARN for the DeleteReportDefinition and 5 more actions. Add ARNs to restrict access.

☐ Any in this account

► Request conditions - optional

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

+

Add more permissions

Security: 0Errors: 0Warnings: 0Suggestions: 0

▼ Access denied to access-analyzer:ValidatePolicy

You don't have permission to access-analyzer:ValidatePolicy. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: arn:aws:iam::165278525958:user/student

Action: access-analyzer:ValidatePolicy

On resource(s): arn:aws:access-analyzer:us-east-1:165278525958:*

Cancel

Next