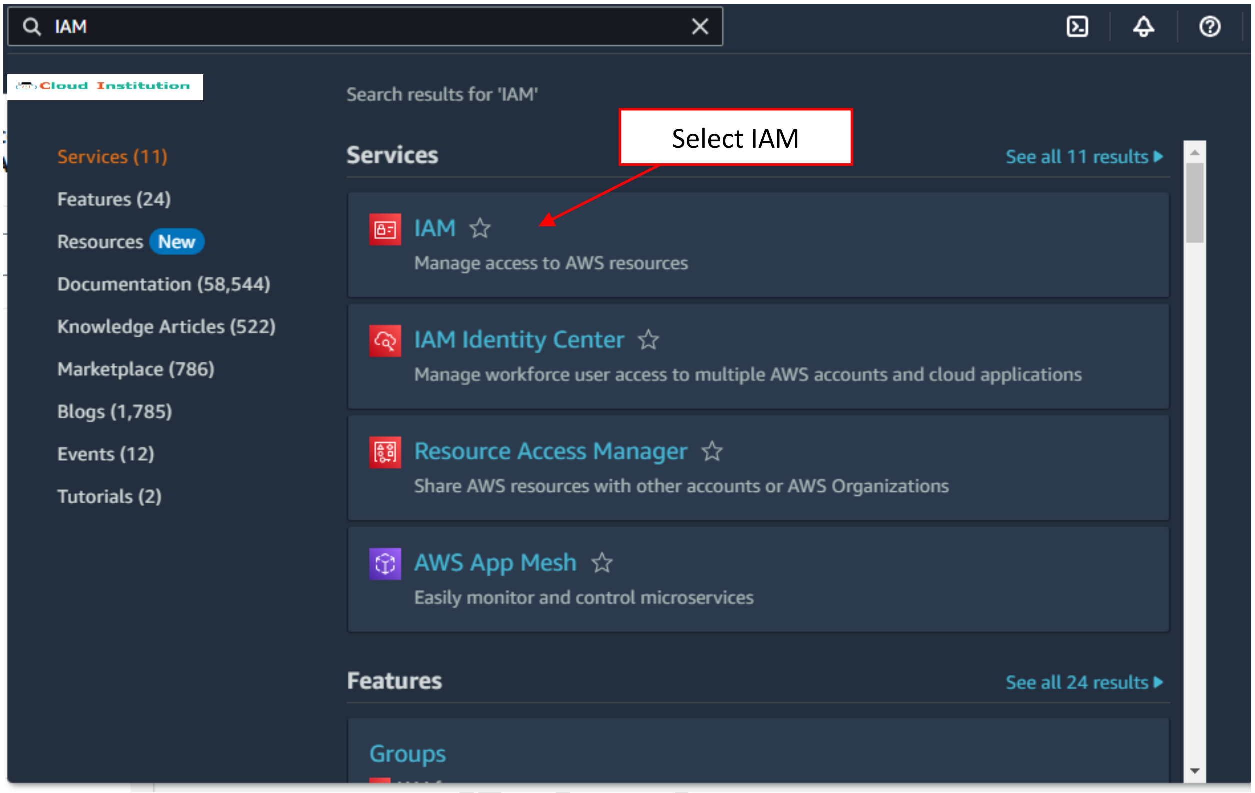
# *Creating a user group*



Select IAM

IAM

Cloud Institution

Search results for 'IAM'

Services (11)
Features (24)
Resources New
Documentation (58,544)
Knowledge Articles (522)
Marketplace (786)
Blogs (1,785)
Events (12)
Tutorials (2)

Services — See all 11 results ▸

IAM ☆
Manage access to AWS resources

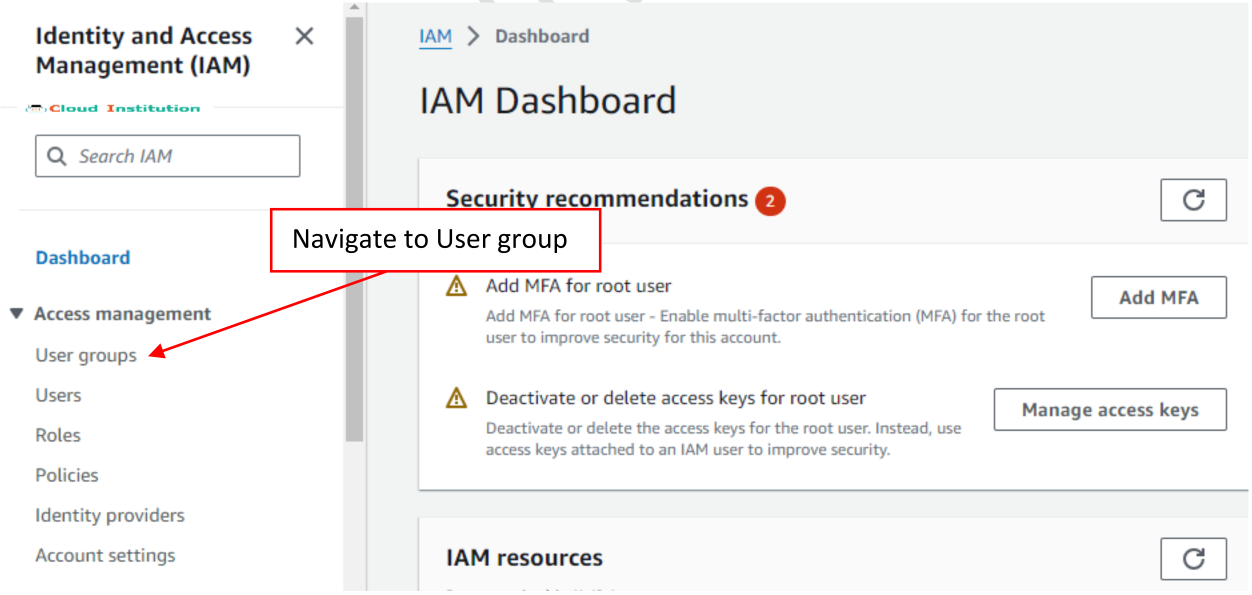
IAM Identity Center ☆
Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager ☆
Share AWS resources with other accounts or AWS Organizations

AWS App Mesh ☆
Easily monitor and control microservices

Features — See all 24 results ▸

Groups



Navigate to User group

Identity and Access Management (IAM) ✕

Cloud Institution

Search IAM

Dashboard

▼ Access management
User groups
Users
Roles
Policies
Identity providers
Account settings

IAM > Dashboard

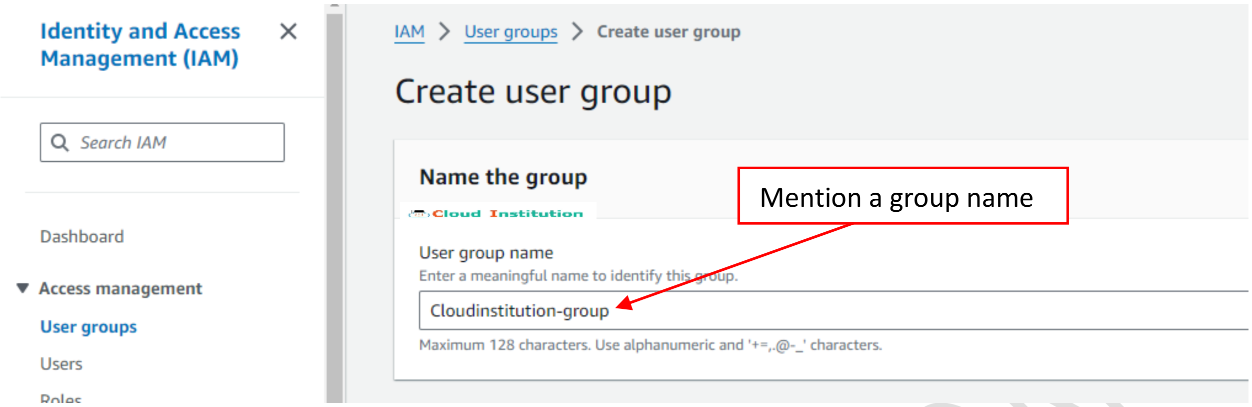
IAM Dashboard

Security recommendations 2

⚠ Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.
Add MFA

⚠ Deactivate or delete access keys for root user
Deactivate or delete the access keys for the root user. Instead, use access keys attached to an IAM user to improve security.
Manage access keys

IAM resources



Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

IAM > User groups > Create user group

Create user group

Name the group

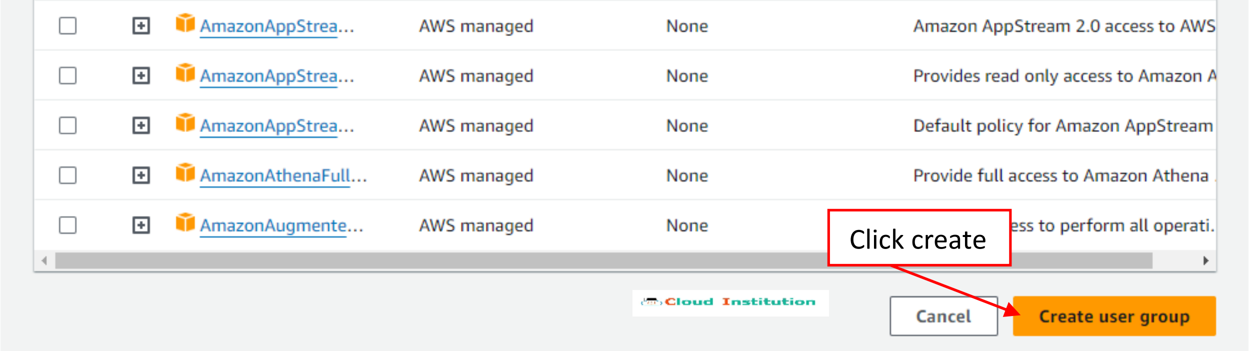
User group name

Enter a meaningful name to identify this group.

Cloudinstitution-group

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

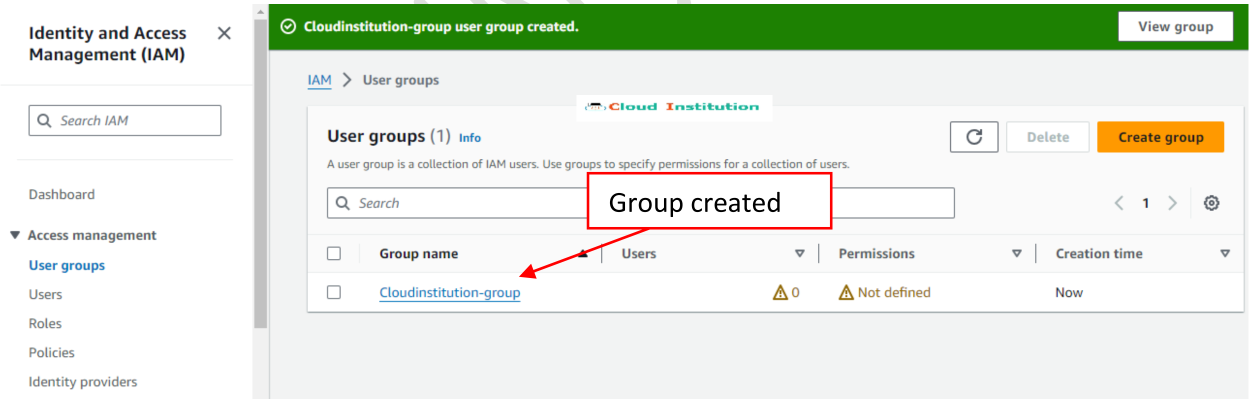
Mention a group name



| | | | | | |
|---|---|---|---|---|---|
| □ | ⊞ | AmazonAppStrea... | AWS managed | None | Amazon AppStream 2.0 access to AWS |
| □ | ⊞ | AmazonAppStrea... | AWS managed | None | Provides read only access to Amazon A |
| □ | ⊞ | AmazonAppStrea... | AWS managed | None | Default policy for Amazon AppStream |
| □ | ⊞ | AmazonAthenaFull... | AWS managed | None | Provide full access to Amazon Athena |
| □ | ⊞ | AmazonAugmente... | AWS managed | None | ess to perform all operati. |

Click create

Cancel | Create user group



Cloudinstitution-group user group created. | View group

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

IAM > User groups

User groups (1) Info

Delete | Create group

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

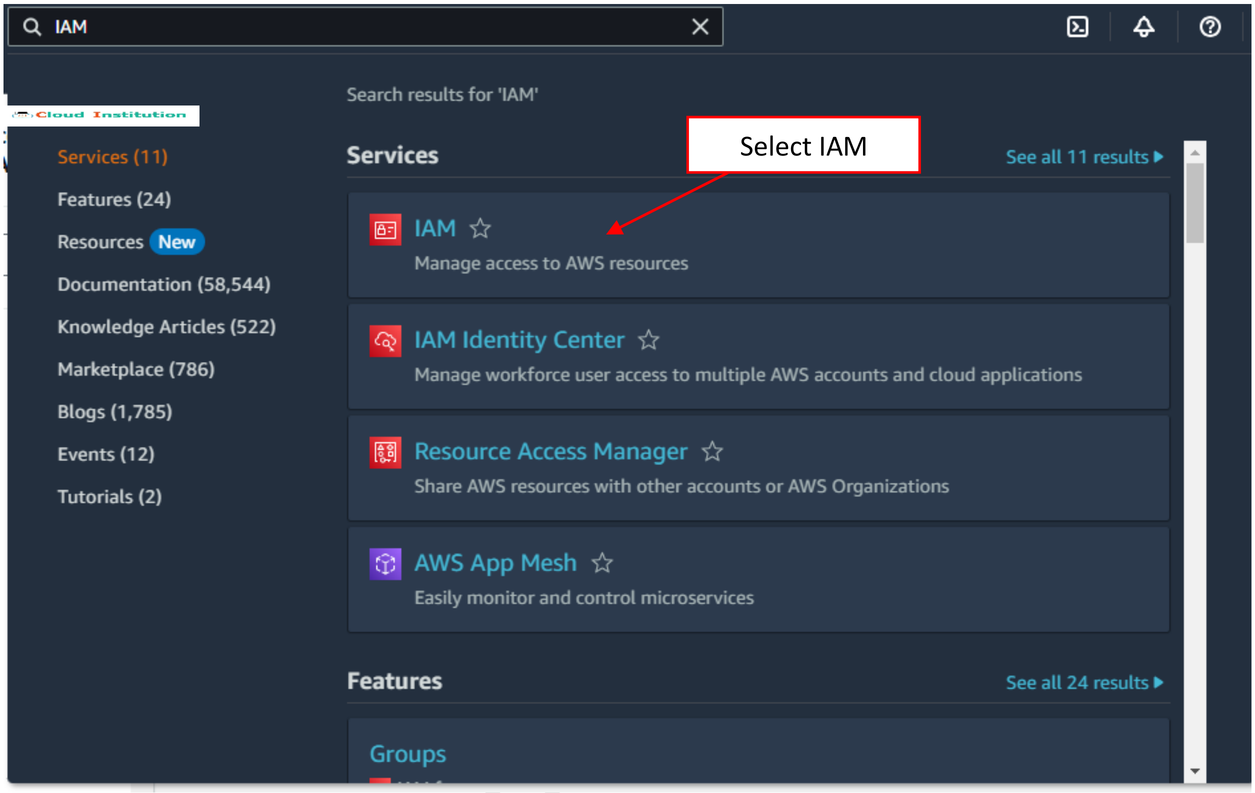
Search

Group created

| □ | Group name | Users | Permissions | Creation time |
|---|---|---|---|---|
| □ | Cloudinstitution-group | ⚠ 0 | ⚠ Not defined | Now |

# *Creating an IAM User*

Step 1 : Create an IAM user



IAM

Search results for 'IAM'

Services (11)
Features (24)
Resources New
Documentation (58,544)
Knowledge Articles (522)
Marketplace (786)
Blogs (1,785)
Events (12)
Tutorials (2)

Services — See all 11 results

IAM ☆
Manage access to AWS resources

IAM Identity Center ☆
Manage workforce user access to multiple AWS accounts and cloud applications

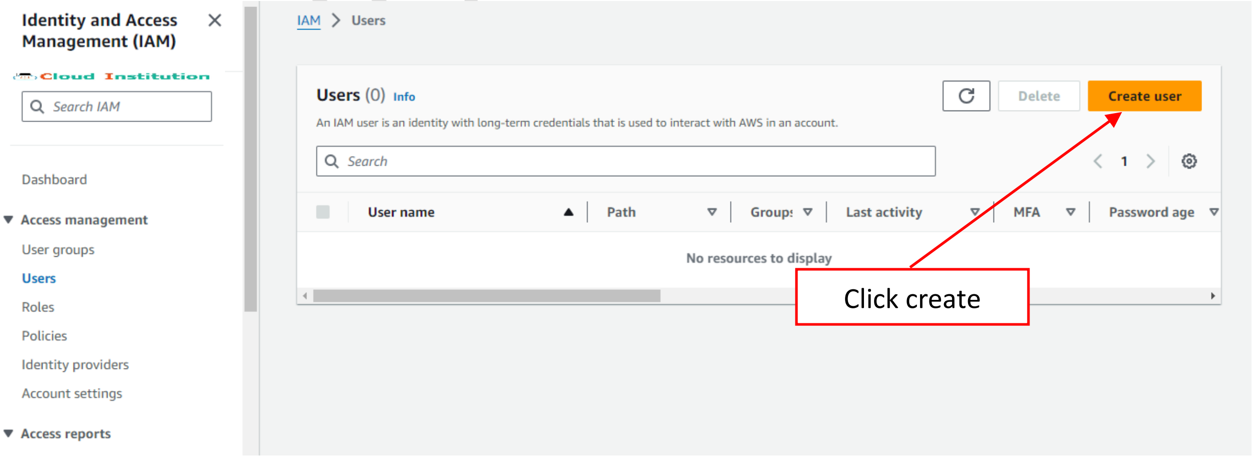
Resource Access Manager ☆
Share AWS resources with other accounts or AWS Organizations

AWS App Mesh ☆
Easily monitor and control microservices

Features — See all 24 results

Groups

Select IAM



Identity and Access Management (IAM)

Search IAM

Dashboard
▼ Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
▼ Access reports

IAM > Users

Users (0) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

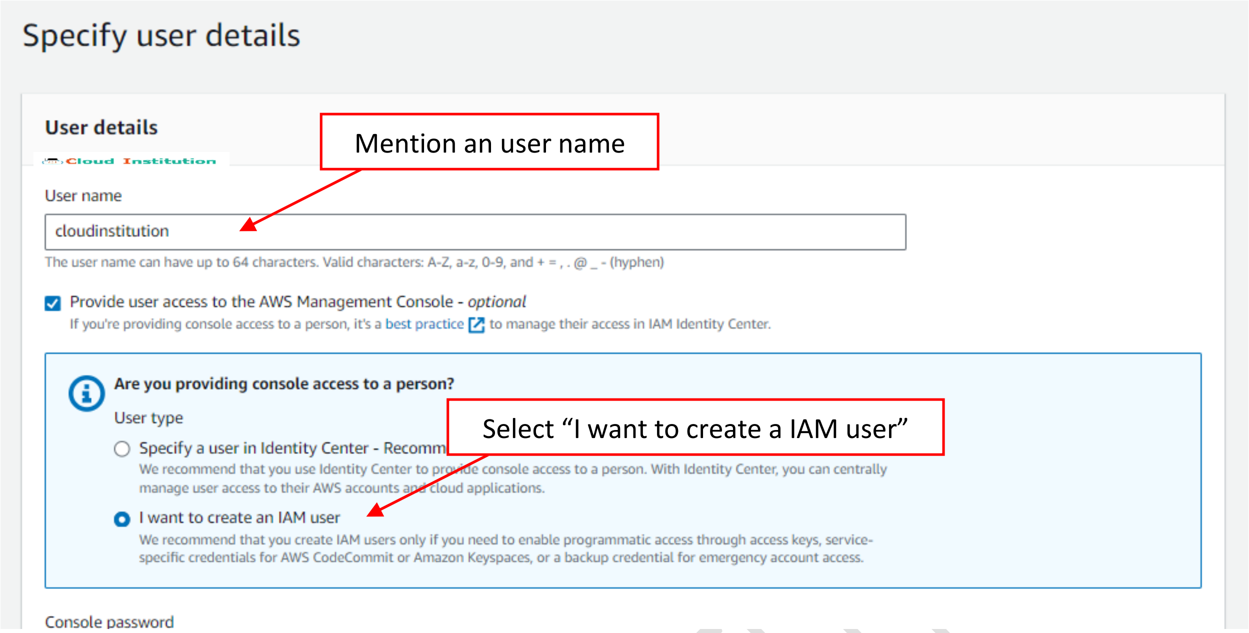
Delete | Create user

Search

| ☐ | User name ▲ | Path | Groups | Last activity | MFA | Password age |
|---|---|---|---|---|---|---|

No resources to display

Click create



Specify user details

**User details**

User name

cloudinstitution

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.

**Are you providing console access to a person?**

User type

○ Specify a user in Identity Center - Recomm

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

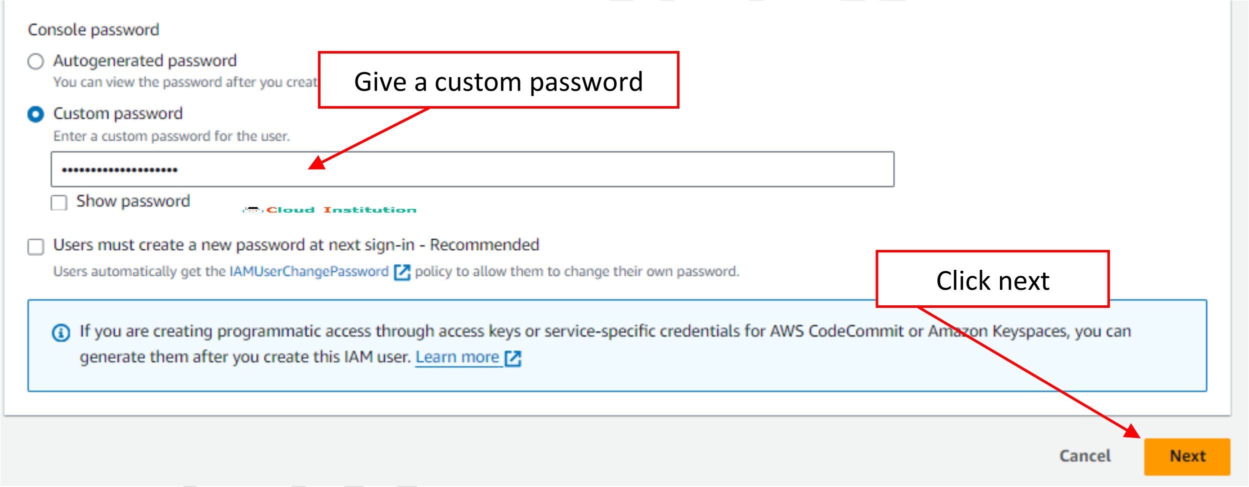
● I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

Mention an user name

Select "I want to create a IAM user"



Console password

○ Autogenerated password

You can view the password after you creat

● Custom password

Enter a custom password for the user.

••••••••••••••••••••

□ Show password

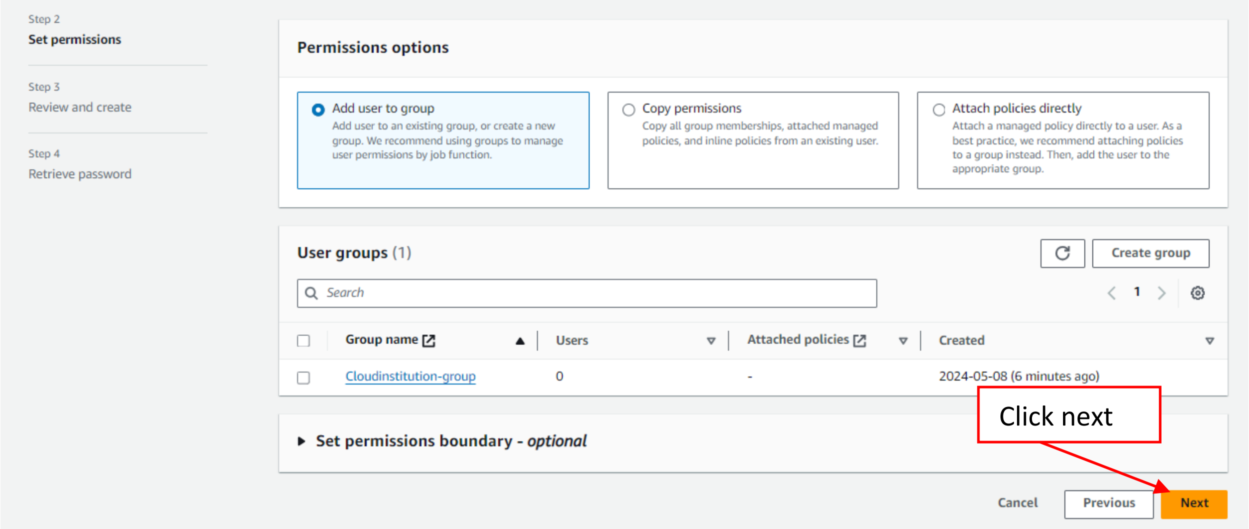
□ Users must create a new password at next sign-in - Recommended

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

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

Give a custom password

Click next



Step 2
**Set permissions**

Step 3
Review and create

Step 4
Retrieve password

**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.

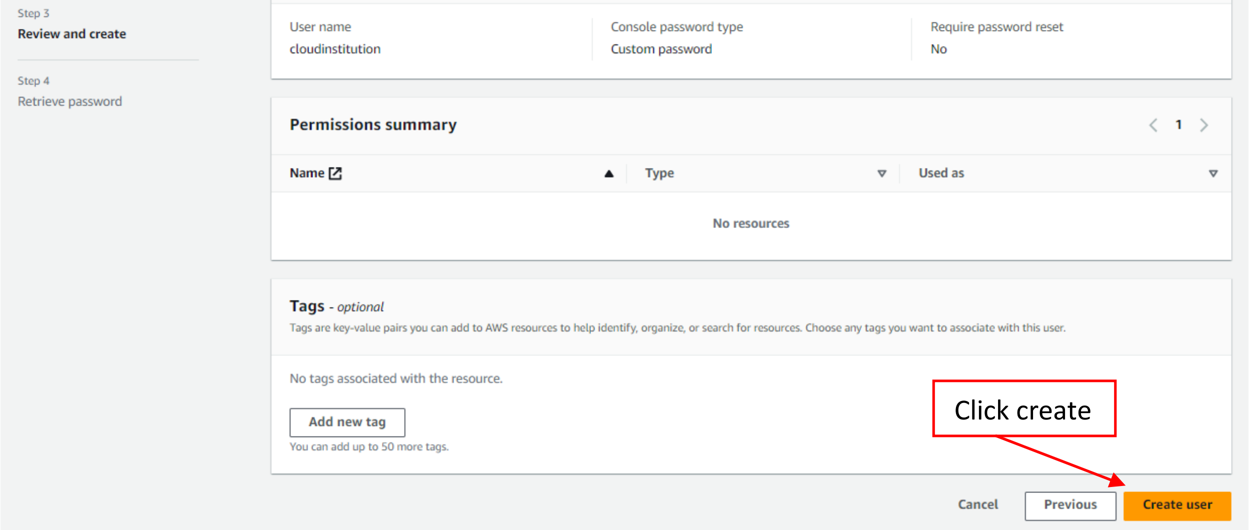
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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.

**User groups** (1)

| □ | Group name | Users | Attached policies | Created |
|---|---|---|---|---|
| □ | Cloudinstitution-group | 0 | - | 2024-05-08 (6 minutes ago) |

▸ **Set permissions boundary - *optional***



Step 3
**Review and create**

Step 4
Retrieve password

| User name | Console password type | Require password reset |
|---|---|---|
| cloudinstitution | Custom password | No |

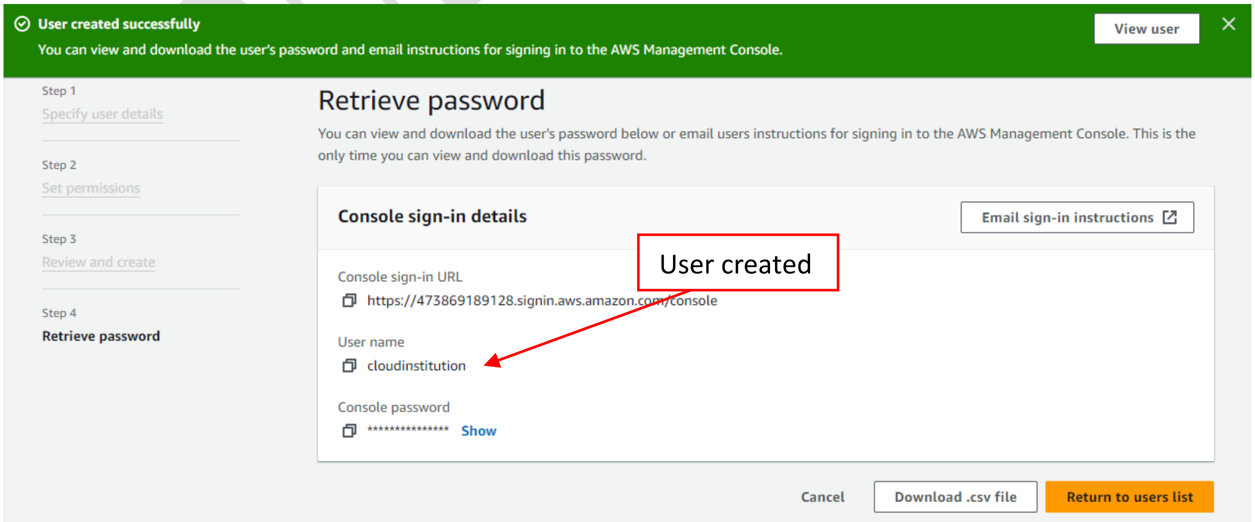
**Permissions summary**

| 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.

You can add up to 50 more tags.



**User created successfully**
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
**Retrieve password**

## Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

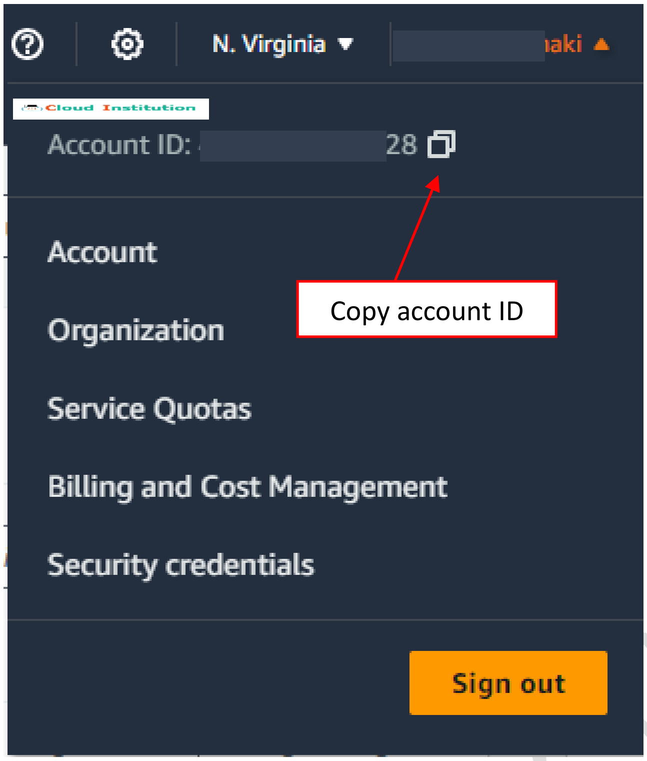
**Console sign-in details**

Console sign-in URL
https://473869189128.signin.aws.amazon.com/console

User name
cloudinstitution

Console password
***************

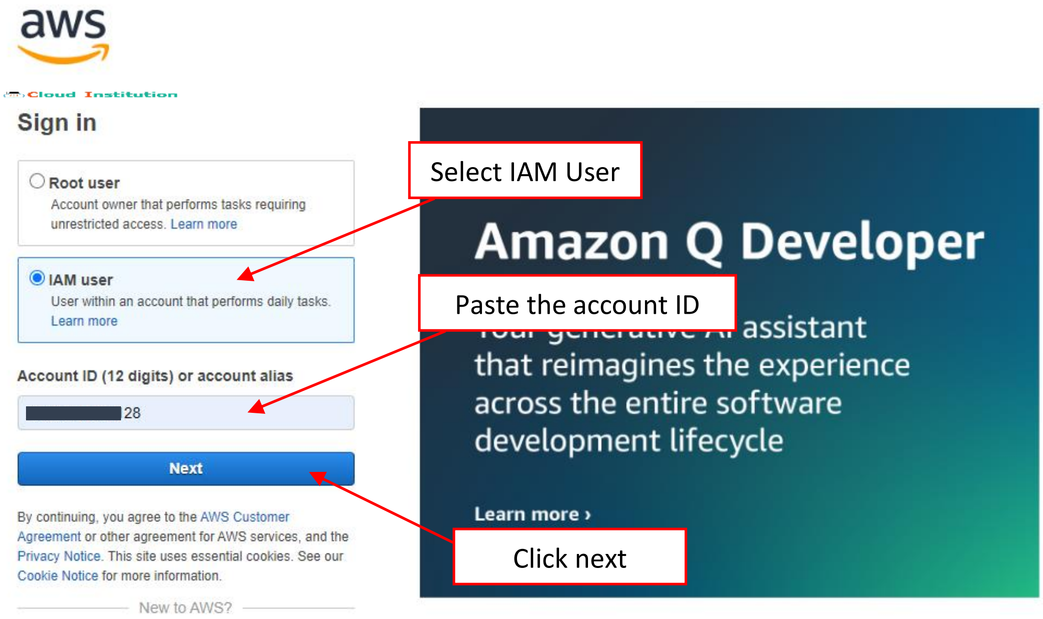
Step 2 : Login to the created IAM User



Account ID: [redacted]28

Copy account ID

Open a new tab and go to sign in console



Sign in

○ Root user
Account owner that performs tasks requiring unrestricted access. Learn more

● IAM user
User within an account that performs daily tasks. Learn more

Account ID (12 digits) or account alias

[redacted]28

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

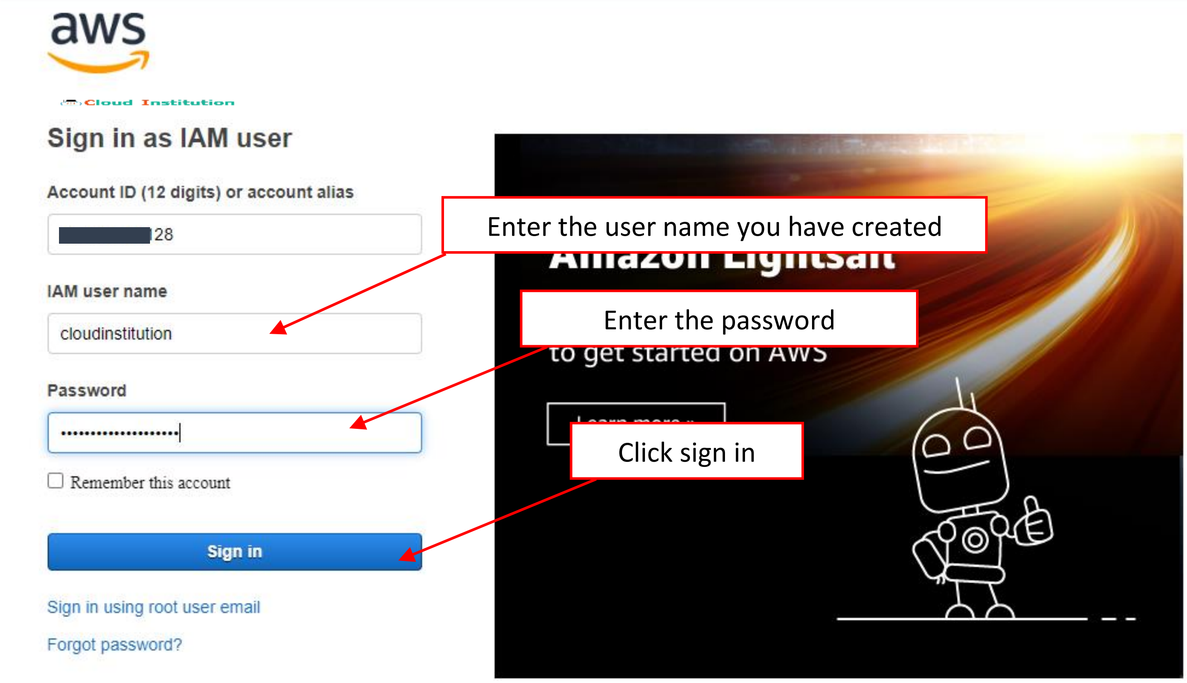
Amazon Q Developer

Your generative AI assistant that reimagines the experience across the entire software development lifecycle

Select IAM User

Paste the account ID

Click next



Sign in as IAM user

Account ID (12 digits) or account alias

[redacted]28

IAM user name

cloudinstitution

Password

••••••••••••••••••••

□ Remember this account

Sign in

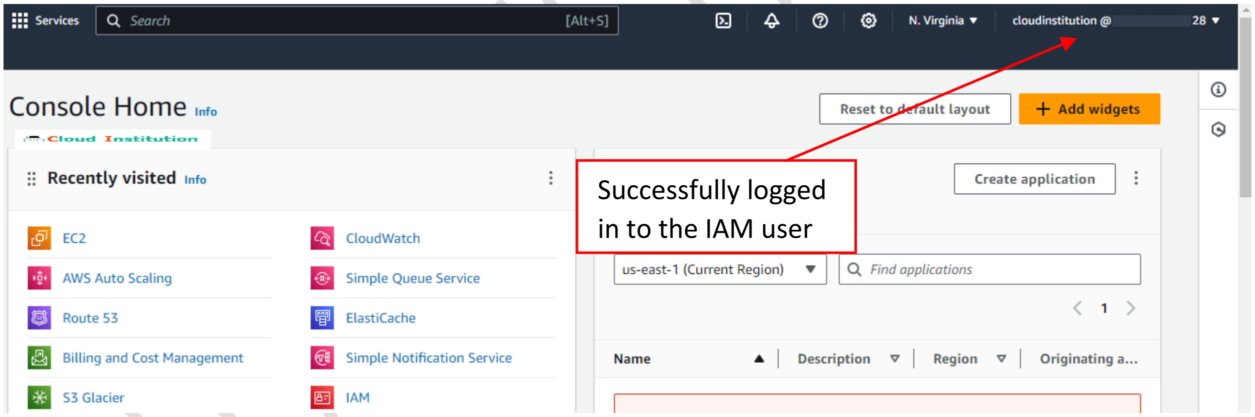
Sign in using root user email

Forgot password?

Enter the user name you have created

Enter the password

Click sign in



cloudinstitution @ [redacted] 28 ▼

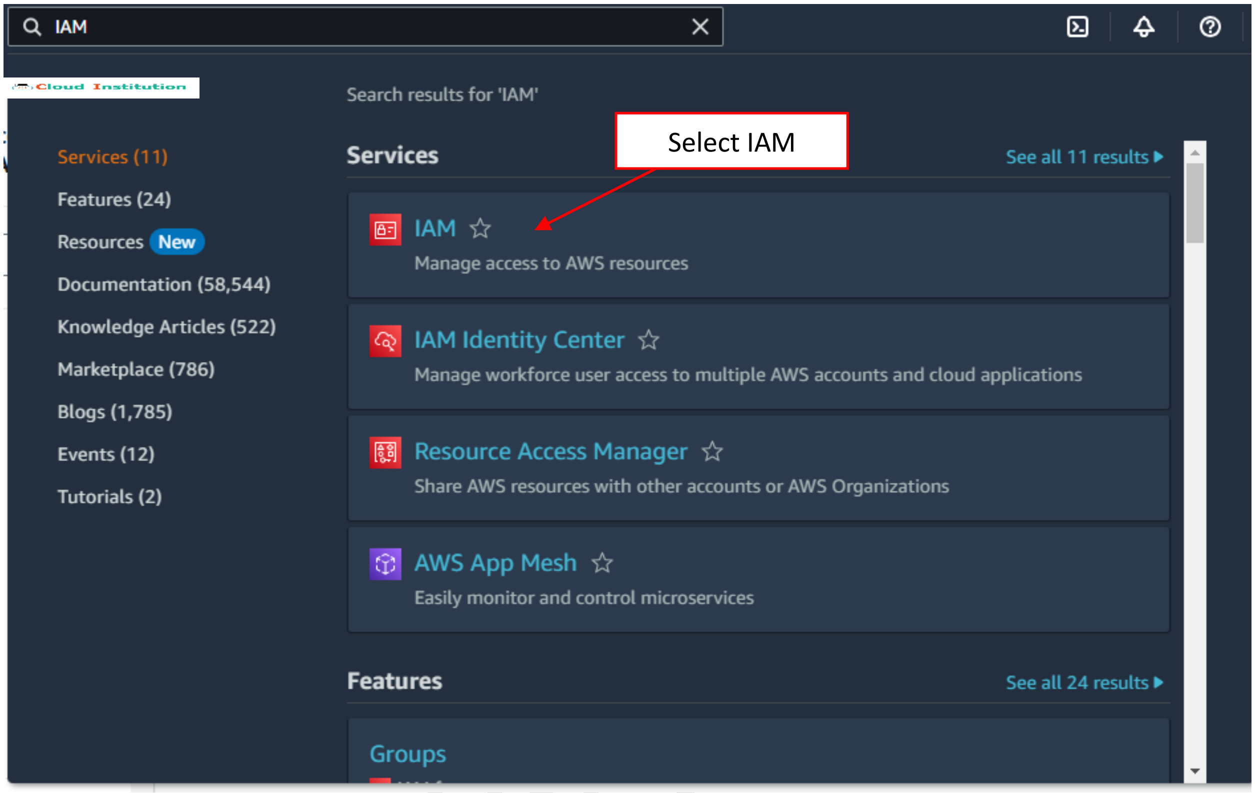
Console Home Info

Recently visited Info

| | |
|---|---|
| EC2 | CloudWatch |
| AWS Auto Scaling | Simple Queue Service |
| Route 53 | ElastiCache |
| Billing and Cost Management | Simple Notification Service |
| S3 Glacier | IAM |

Successfully logged in to the IAM user

# *Creating an IAM Role*



Search results for 'IAM'

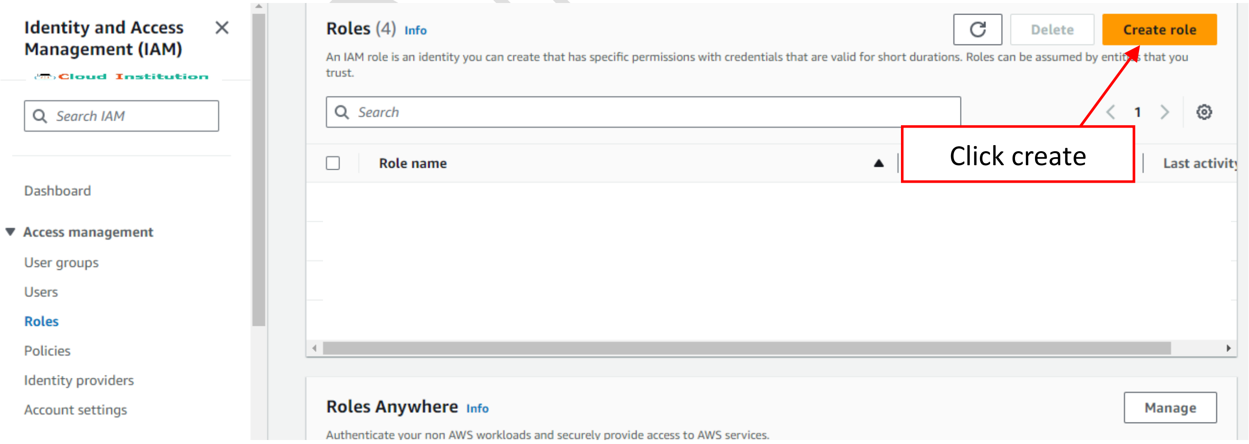
Select IAM

IAM — Manage access to AWS resources

IAM Identity Center — Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager — Share AWS resources with other accounts or AWS Organizations

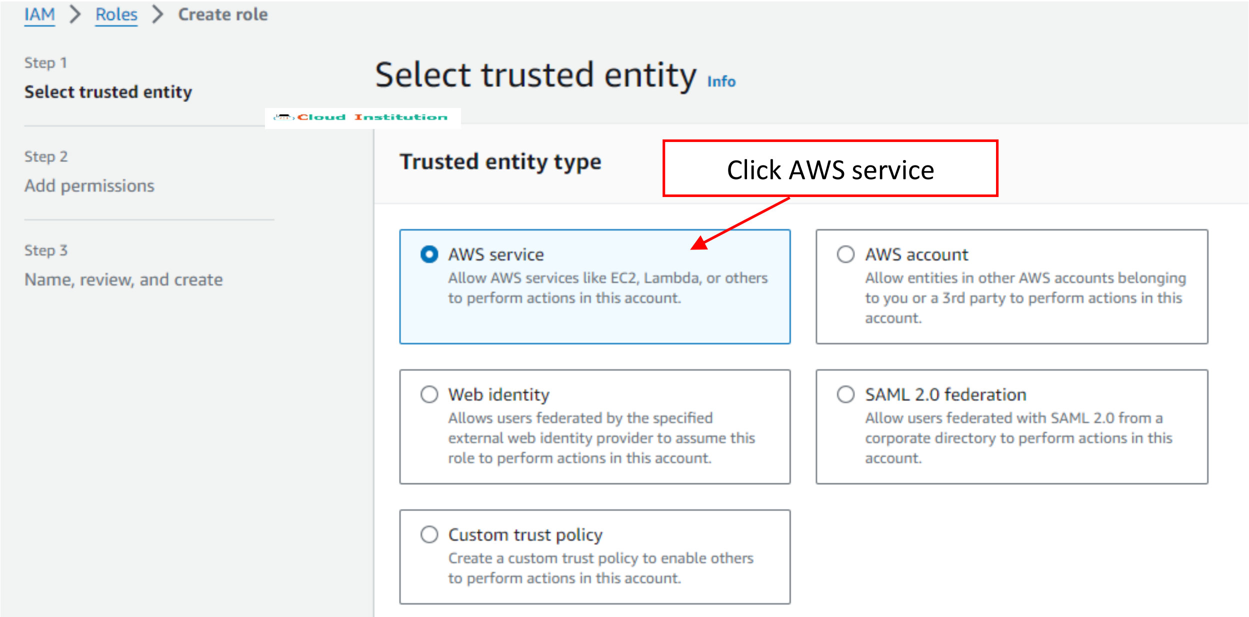
AWS App Mesh — Easily monitor and control microservices



An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Click create

Authenticate your non AWS workloads and securely provide access to AWS services.



IAM > Roles > Create role

Step 1

**Select trusted entity**

Step 2

Add permissions

Step 3

Name, review, and create

## Select trusted entity Info

**Trusted entity type**

Click AWS service

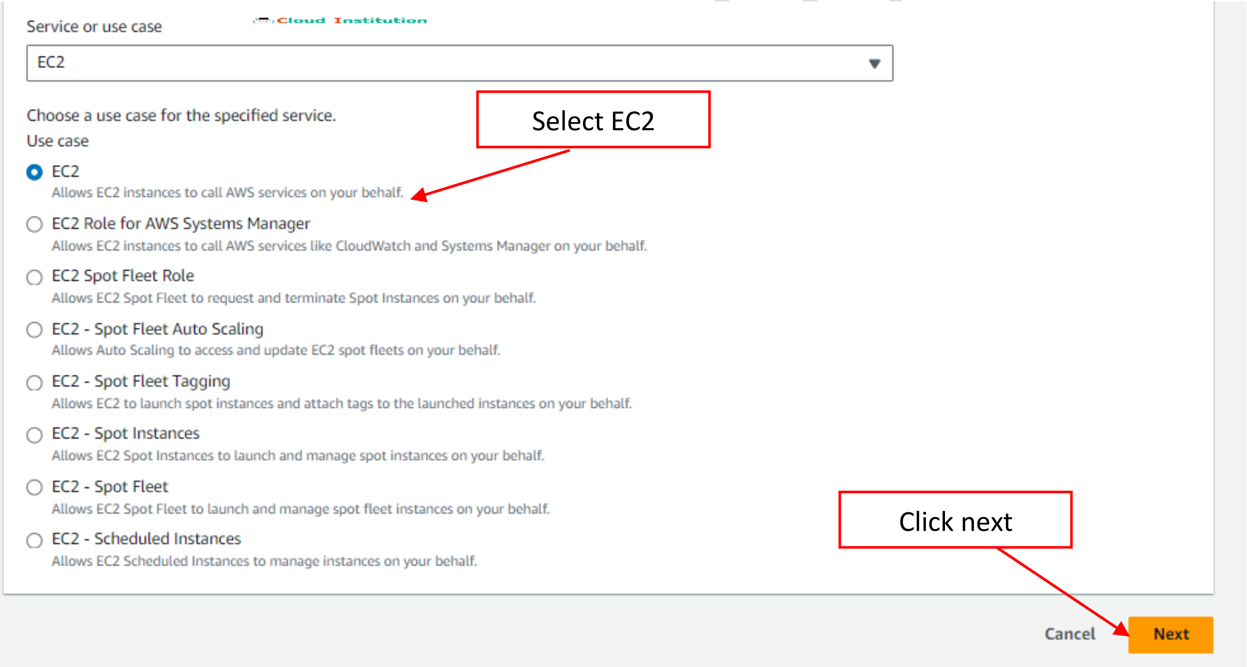
● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.



Service or use case

EC2 ▾

Choose a use case for the specified service.

Use case

Select EC2

● EC2
Allows EC2 instances to call AWS services on your behalf.

○ EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

○ EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

○ EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

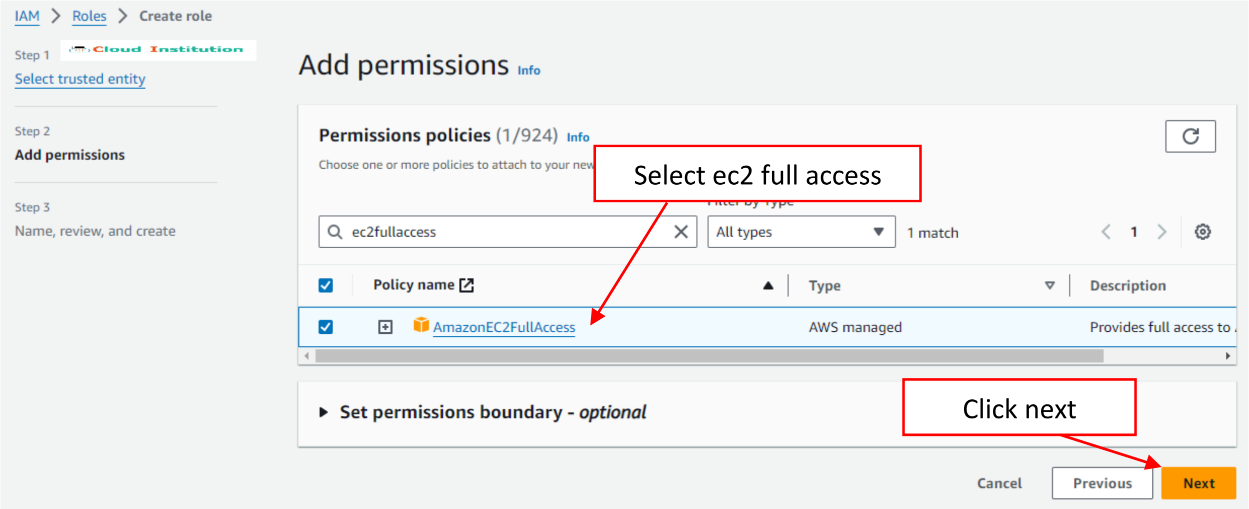
○ EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

○ EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

○ EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

○ EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.

Click next



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

Permissions policies (1/924) Info

Choose one or more policies to attach to your new

Filter by Type

ec2fullaccess | All types | 1 match

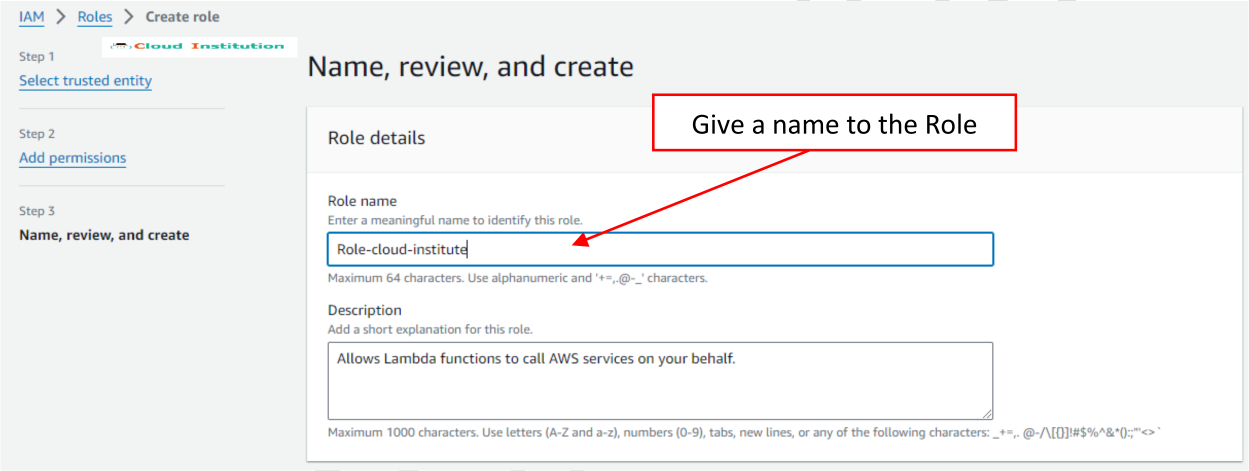
| ☑ | Policy name | Type | Description |
|---|---|---|---|
| ☑ | AmazonEC2FullAccess | AWS managed | Provides full access to |

▸ Set permissions boundary - *optional*

Cancel | Previous | Next

Select ec2 full access

Click next



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

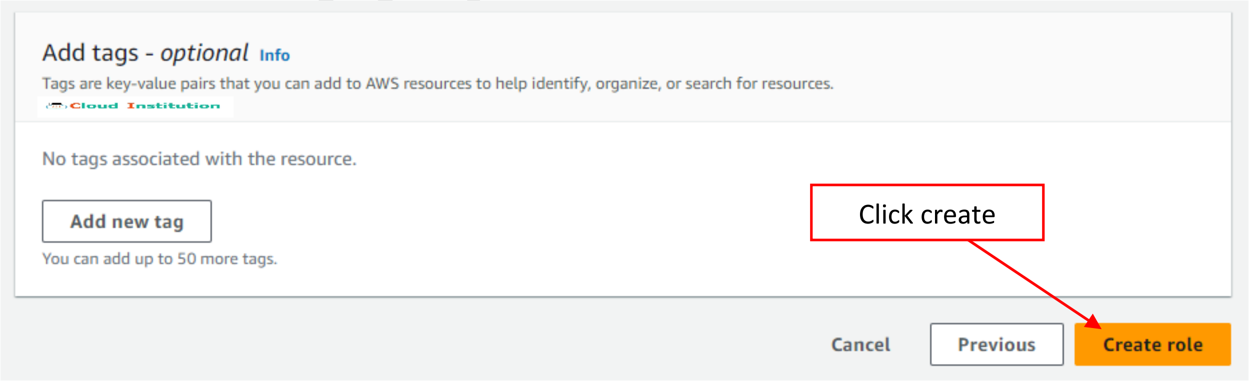
Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
Role-cloud-institute
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.
Allows Lambda functions to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^&*();:"'<> `

Give a name to the Role



Add tags - *optional* Info

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

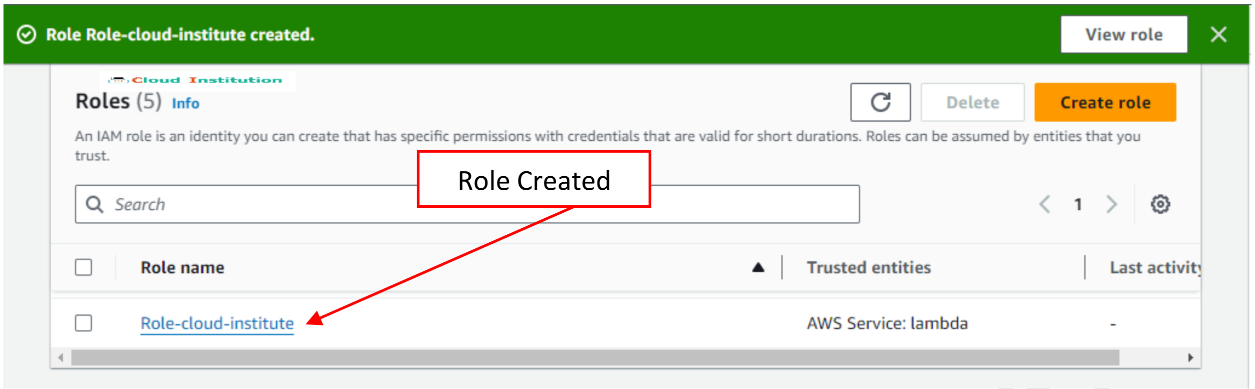
No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel | Previous | Create role

Click create



Role Role-cloud-institute created.

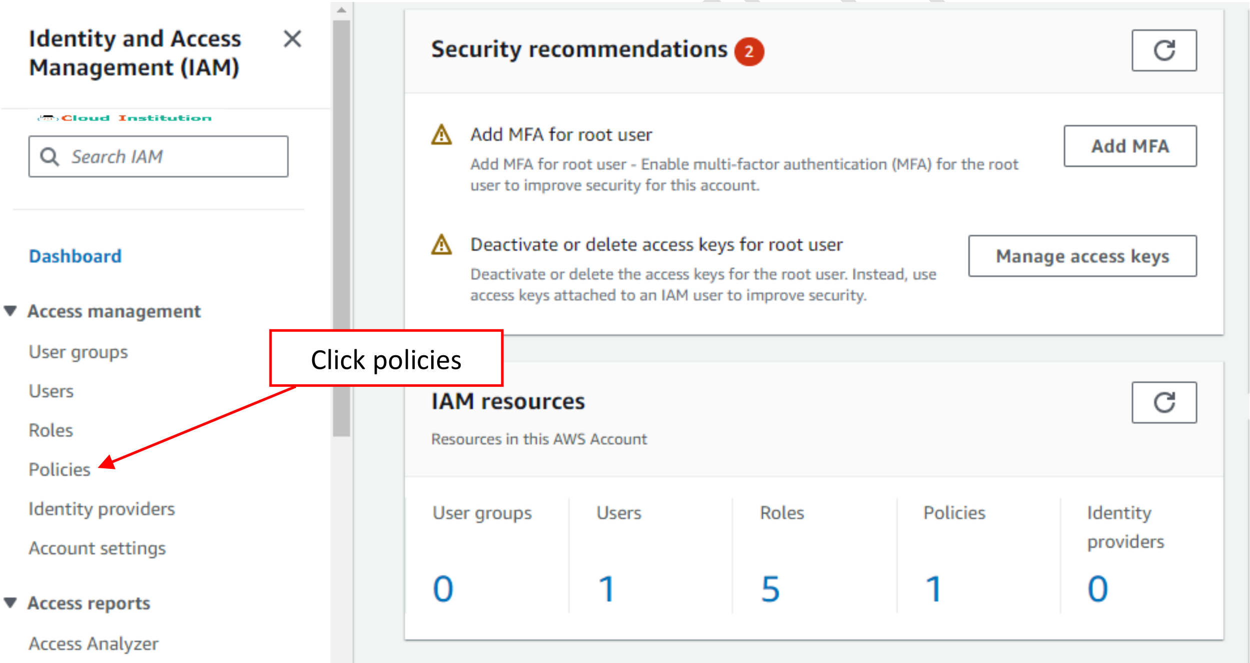
Roles (5) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

| □ | Role name | Trusted entities | Last activity |
|---|---|---|---|
| □ | Role-cloud-institute | AWS Service: lambda | - |

## *Create a policy in IAM*

Go to IAM Dashboard



Security recommendations 2

Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

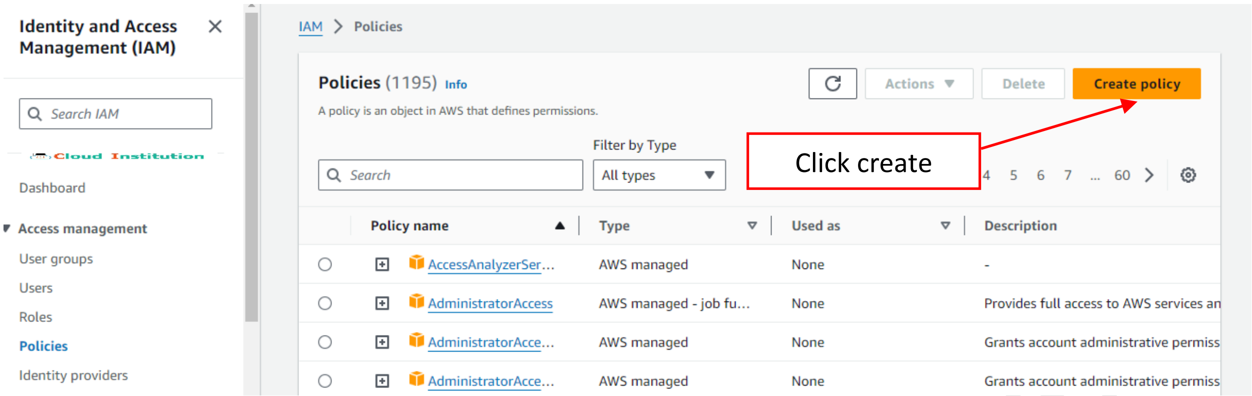
Deactivate or delete access keys for root user

Deactivate or delete the access keys for the root user. Instead, use access keys attached to an IAM user to improve security.

IAM resources

Resources in this AWS Account

| User groups | Users | Roles | Policies | Identity providers |
|---|---|---|---|---|
| 0 | 1 | 5 | 1 | 0 |

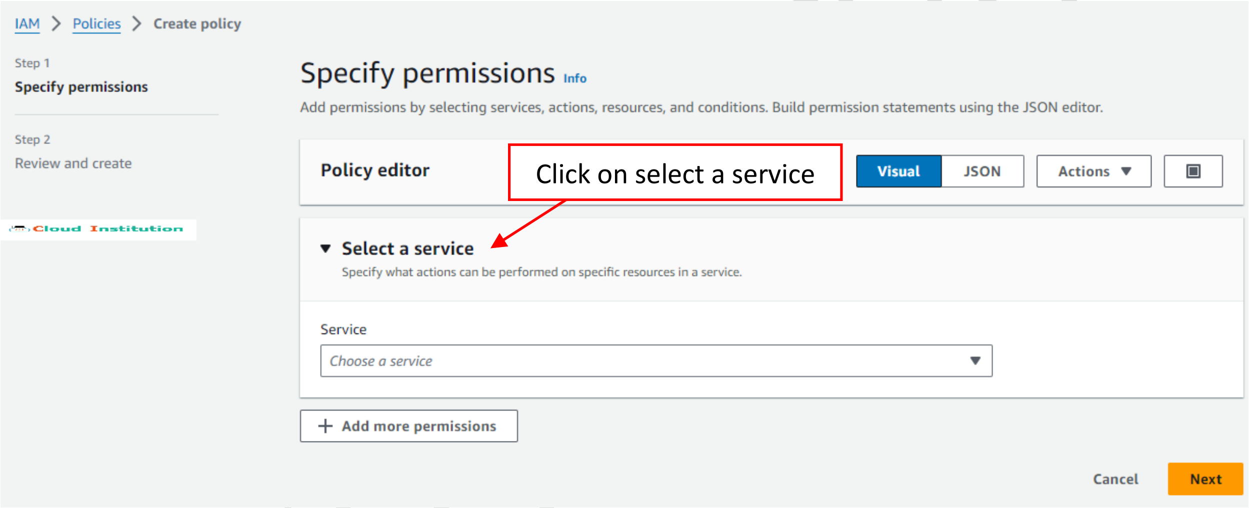


Policies (1195) Info

A policy is an object in AWS that defines permissions.

Click create

| Policy name | Type | Used as | Description |
|---|---|---|---|
| AccessAnalyzerSer... | AWS managed | None | - |
| AdministratorAccess | AWS managed - job fu... | None | Provides full access to AWS services an |
| AdministratorAcce... | AWS managed | None | Grants account administrative permiss |
| AdministratorAcce... | AWS managed | None | Grants account administrative permiss |



Specify permissions Info

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

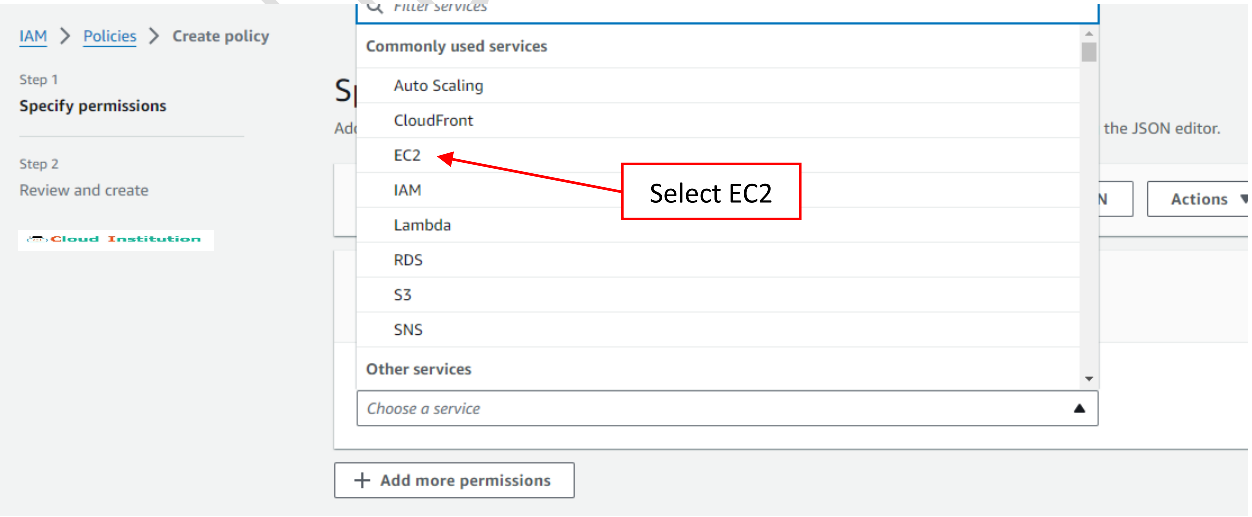
Policy editor

Click on select a service

Select a service

Specify what actions can be performed on specific resources in a service.

Service: Choose a service



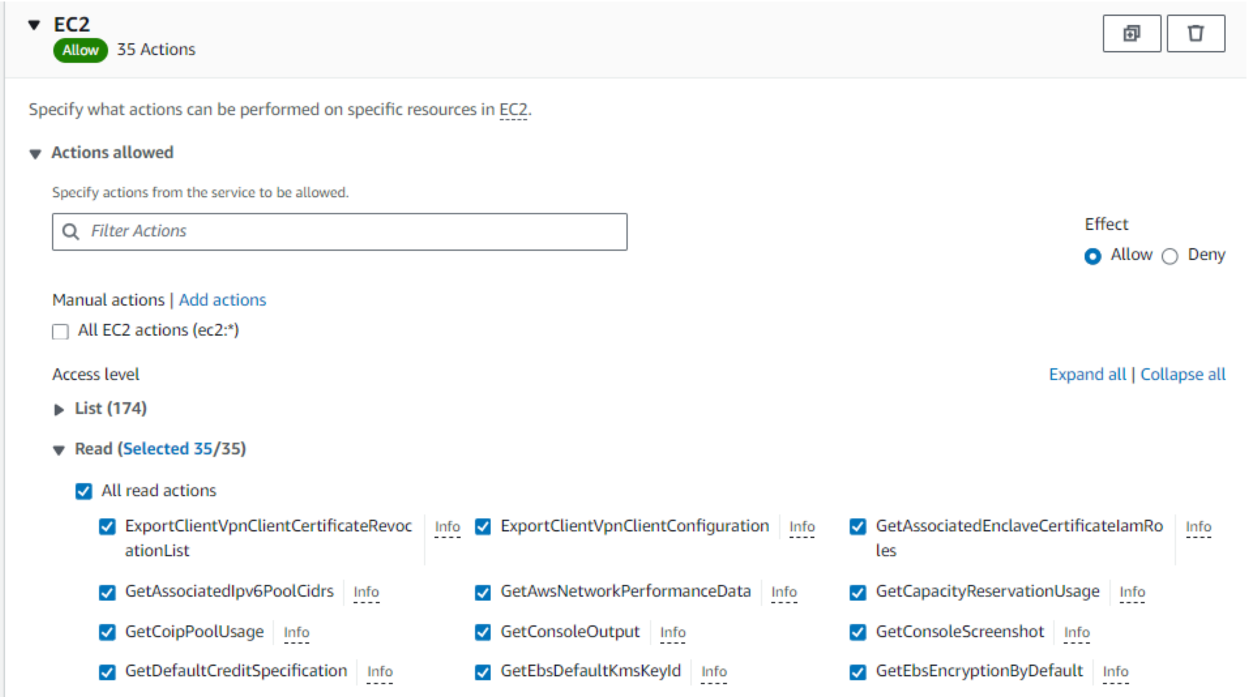
Commonly used services

- Auto Scaling
- CloudFront
- EC2
- IAM
- Lambda
- RDS
- S3
- SNS

Other services

Choose a service

Select EC2



▼ EC2
Allow 35 Actions

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

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect
● Allow ○ Deny

Manual actions | Add actions
□ All EC2 actions (ec2:*)

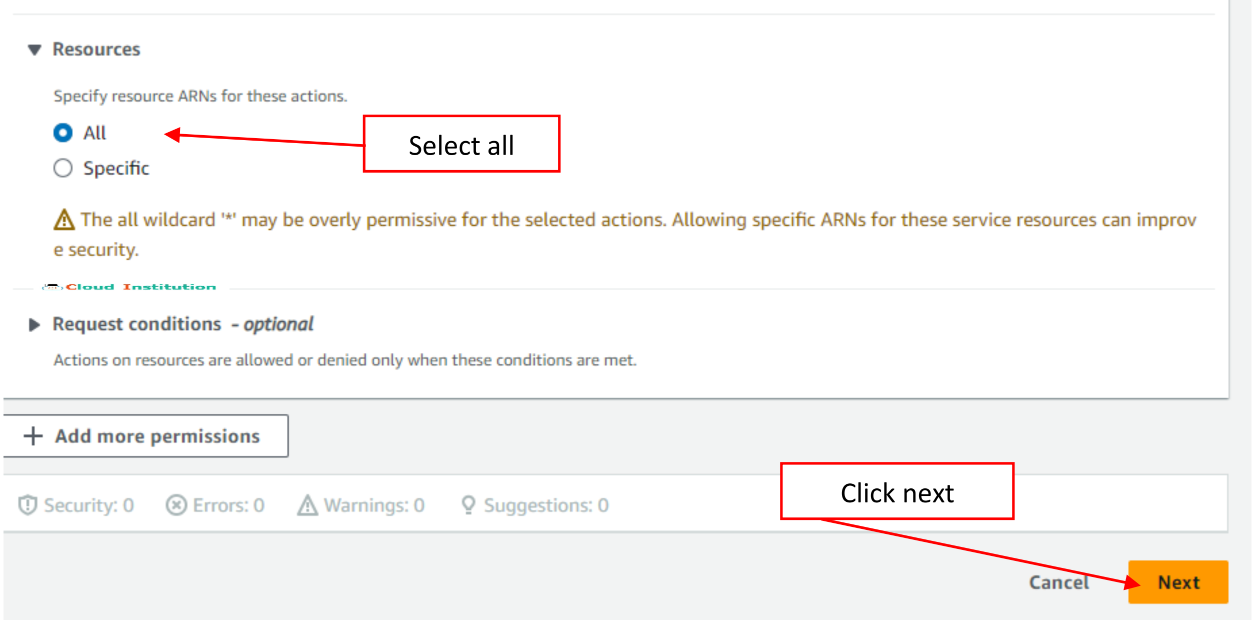
Access level | Expand all | Collapse all

▶ List (174)

▼ Read (Selected 35/35)

☑ All read actions

| | | |
|---|---|---|
| ☑ ExportClientVpnClientCertificateRevocationList Info | ☑ ExportClientVpnClientConfiguration Info | ☑ GetAssociatedEnclaveCertificateIamRoles Info |
| ☑ GetAssociatedIpv6PoolCidrs Info | ☑ GetAwsNetworkPerformanceData Info | ☑ GetCapacityReservationUsage Info |
| ☑ GetCoipPoolUsage Info | ☑ GetConsoleOutput Info | ☑ GetConsoleScreenshot Info |
| ☑ GetDefaultCreditSpecification Info | ☑ GetEbsDefaultKmsKeyId Info | ☑ GetEbsEncryptionByDefault Info |



▼ Resources

Specify resource ARNs for these actions.

● All
○ Specific

Select all

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

▶ Request conditions - *optional*

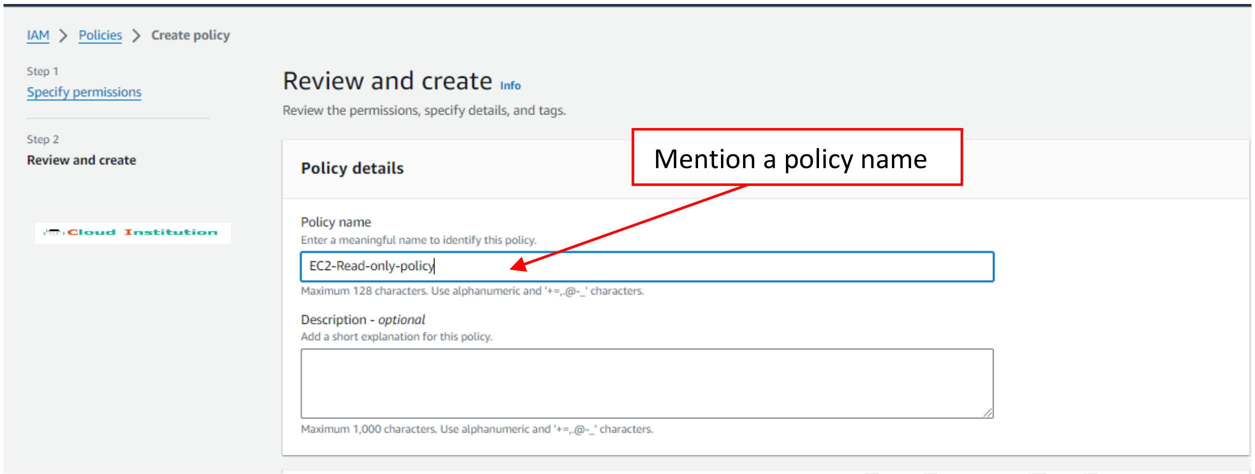
Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

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

Click next

Cancel Next



IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

## Review and create Info

Review the permissions, specify details, and tags.

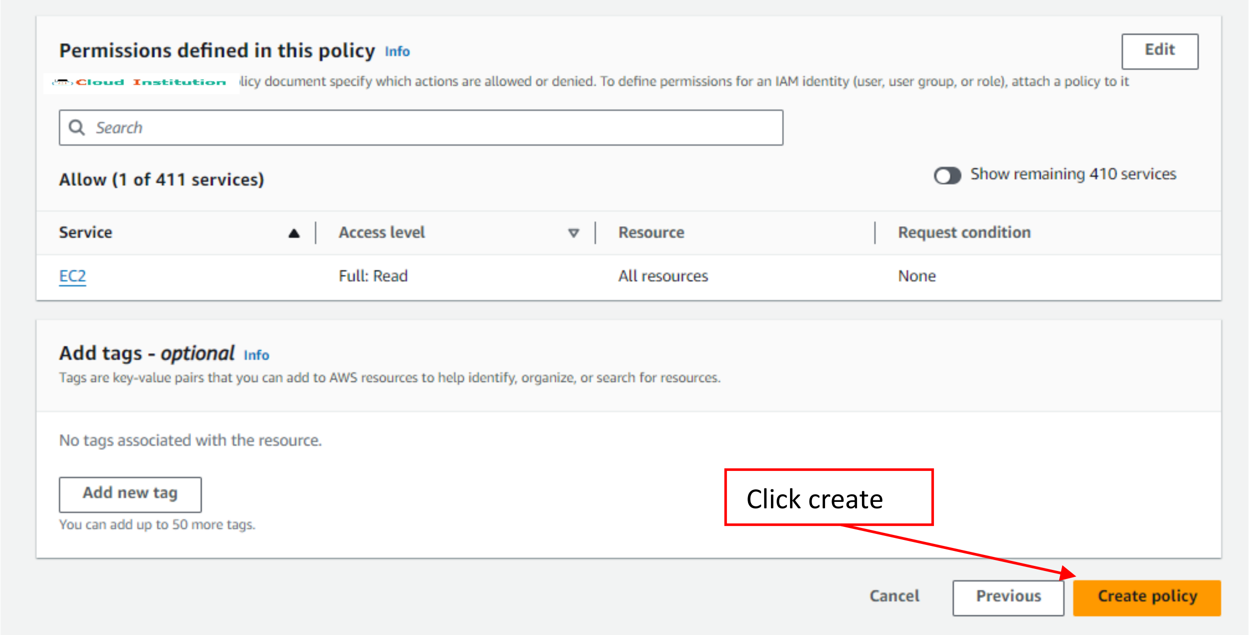
**Policy details**

Mention a policy name

Policy name
Enter a meaningful name to identify this policy.
EC2-Read-only-policy
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

licy 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

**Allow (1 of 411 services)**

Show remaining 410 services

| Service | Access level | Resource | Request condition |
|---|---|---|---|
| EC2 | Full: Read | All resources | None |

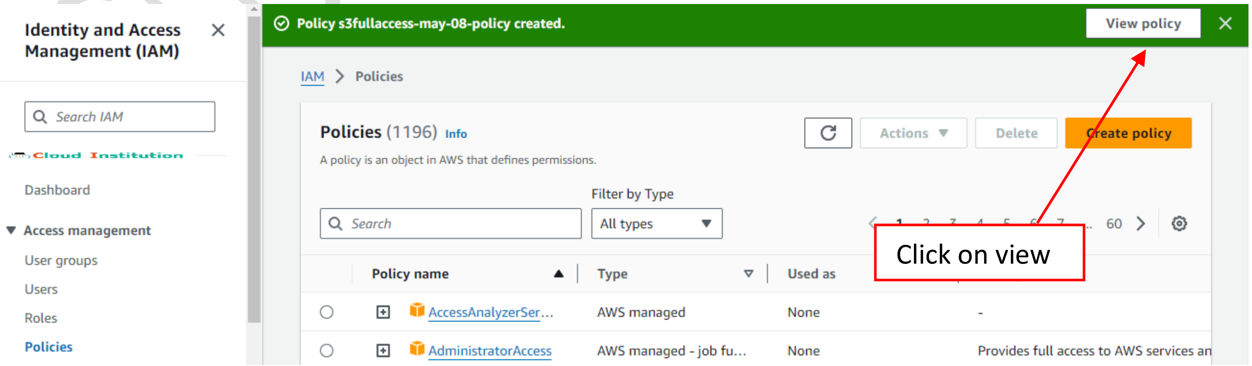
**Add tags - *optional*** Info

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.

You can add up to 50 more tags.

Click create



Policy s3fullaccess-may-08-policy created.

Identity and Access Management (IAM)

IAM > Policies

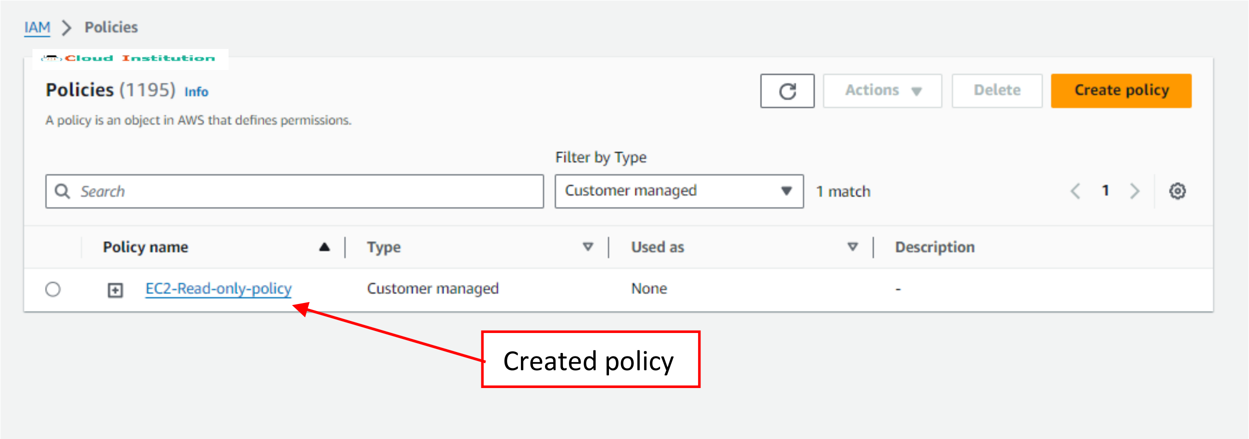
**Policies** (1196) Info

A policy is an object in AWS that defines permissions.

Filter by Type: All types

Click on view

| | | Policy name | Type | Used as | |
|---|---|---|---|---|---|
| ○ | ⊞ | AccessAnalyzerSer… | AWS managed | None | - |
| ○ | ⊞ | AdministratorAccess | AWS managed - job fu… | None | Provides full access to AWS services an |



**Policies** (1195) Info

A policy is an object in AWS that defines permissions.

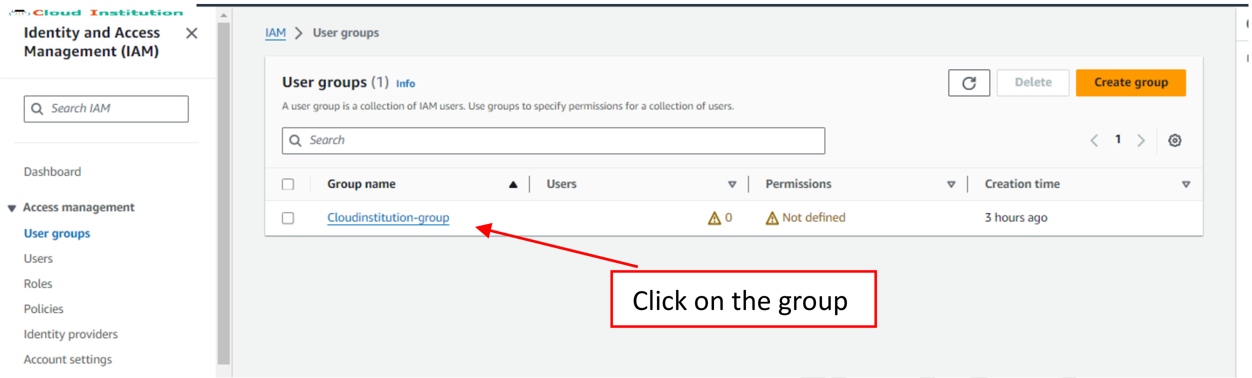
Filter by Type: Customer managed ▼   1 match

🔍 Search

| | | Policy name ▲ | Type | Used as | Description |
|---|---|---|---|---|---|
| ○ | ⊞ | EC2-Read-only-policy | Customer managed | None | - |

Created policy

# *Attach user and policy to the user group*

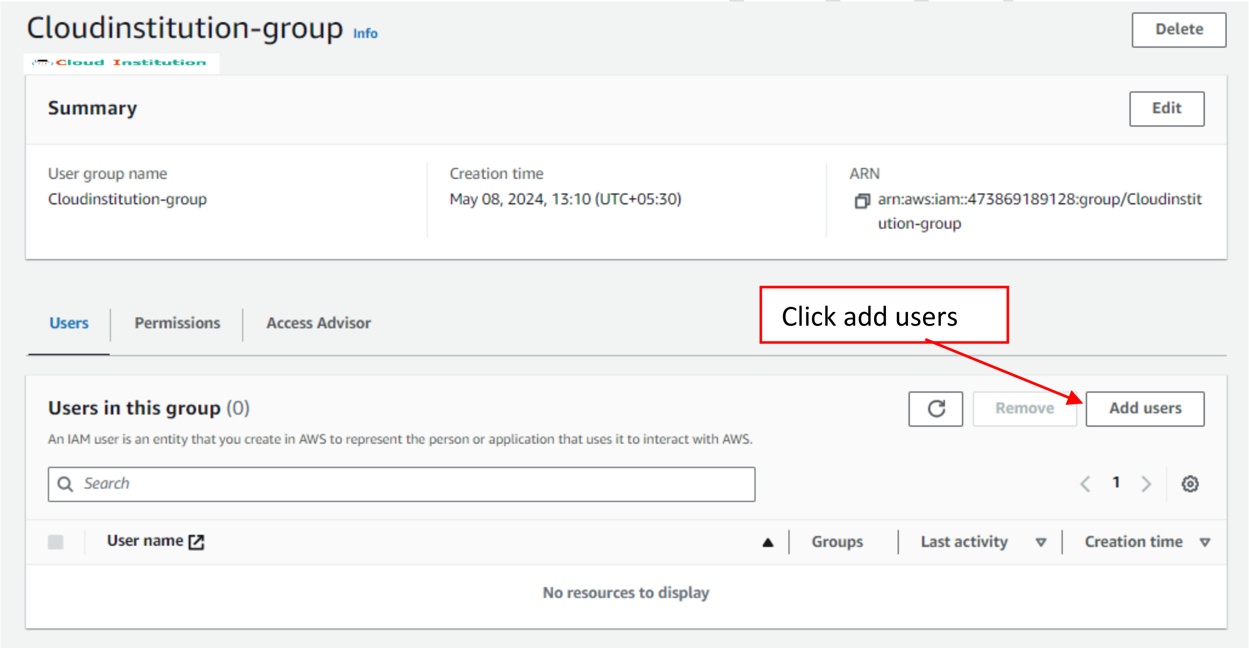


User groups (1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

| □ | Group name | Users | Permissions | Creation time |
|---|---|---|---|---|
| □ | Cloudinstitution-group | ⚠ 0 | ⚠ Not defined | 3 hours ago |

Click on the group



## Cloudinstitution-group Info

Summary

| User group name | Creation time | ARN |
|---|---|---|
| Cloudinstitution-group | May 08, 2024, 13:10 (UTC+05:30) | arn:aws:iam::473869189128:group/Cloudinstitution-group |

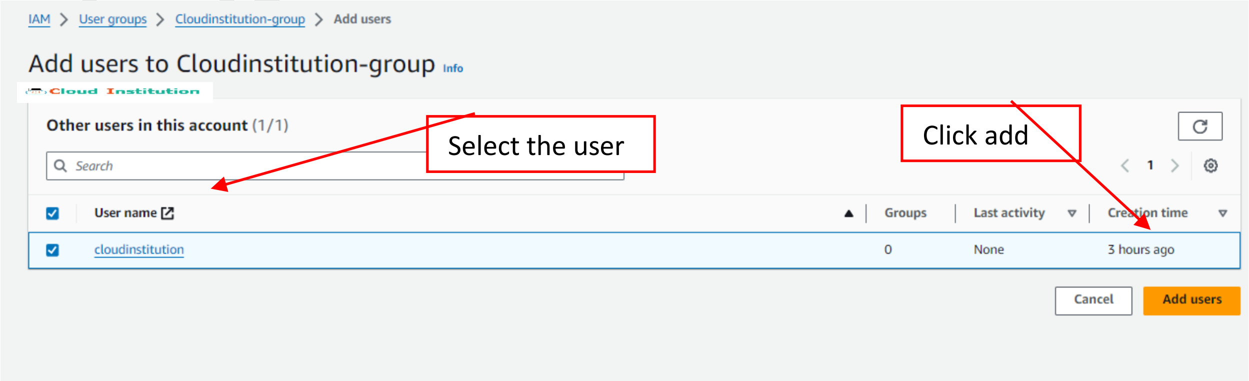
Users in this group (0)

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

| □ | User name | Groups | Last activity | Creation time |
|---|---|---|---|---|

No resources to display

Click add users



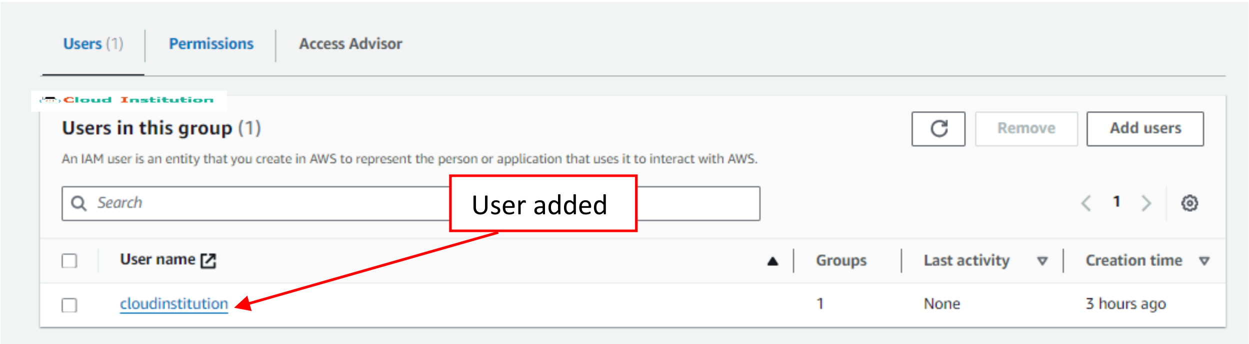
## Add users to Cloudinstitution-group Info

Other users in this account (1/1)

| ☑ | User name | Groups | Last activity | Creation time |
|---|---|---|---|---|
| ☑ | cloudinstitution | 0 | None | 3 hours ago |

Select the user

Click add



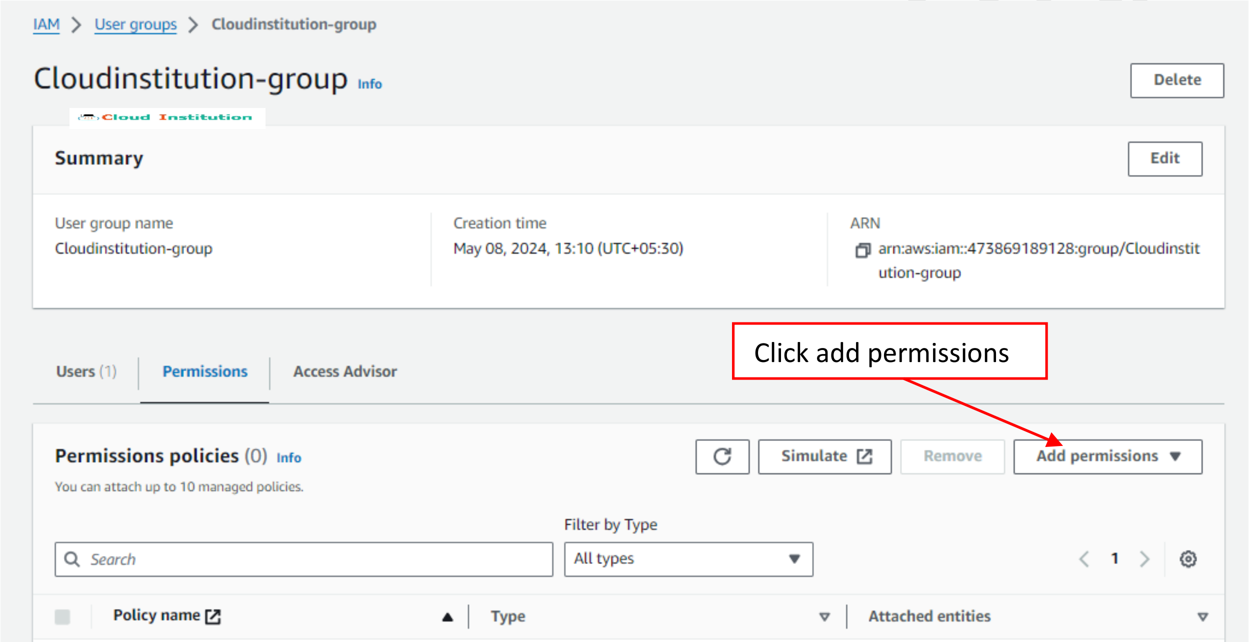
Users (1) | Permissions | Access Advisor

**Users in this group** (1)

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

| □ | User name | Groups | Last activity | Creation time |
|---|---|---|---|---|
| □ | cloudinstitution | 1 | None | 3 hours ago |

User added



IAM > User groups > Cloudinstitution-group

## Cloudinstitution-group Info

**Summary**

User group name
Cloudinstitution-group

Creation time
May 08, 2024, 13:10 (UTC+05:30)

ARN
arn:aws:iam::473869189128:group/Cloudinstitution-group

Users (1) | Permissions | Access Advisor

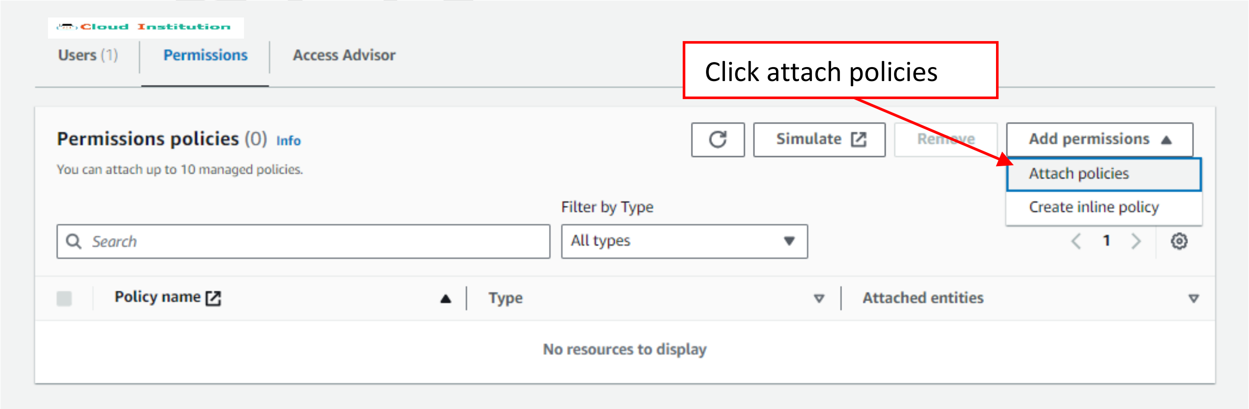
**Permissions policies** (0) Info

You can attach up to 10 managed policies.

Filter by Type: All types

| □ | Policy name | Type | Attached entities |
|---|---|---|---|

Click add permissions



Users (1) | Permissions | Access Advisor

**Permissions policies** (0) Info

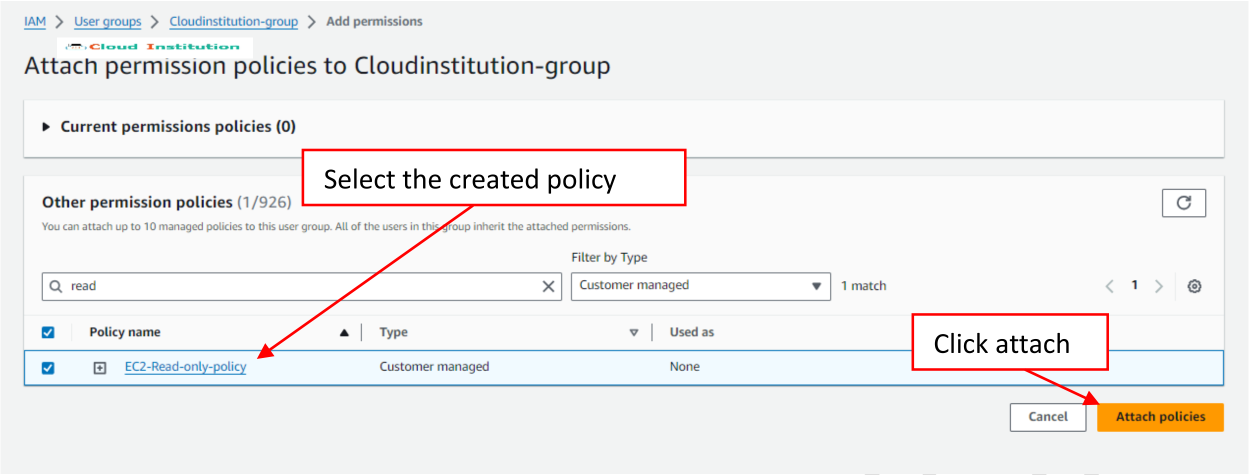
You can attach up to 10 managed policies.

Filter by Type: All types

| □ | Policy name | Type | Attached entities |
|---|---|---|---|

No resources to display

Click attach policies



IAM > User groups > Cloudinstitution-group > Add permissions

Attach permission policies to Cloudinstitution-group

▸ Current permissions policies (0)

Other permission policies (1/926)

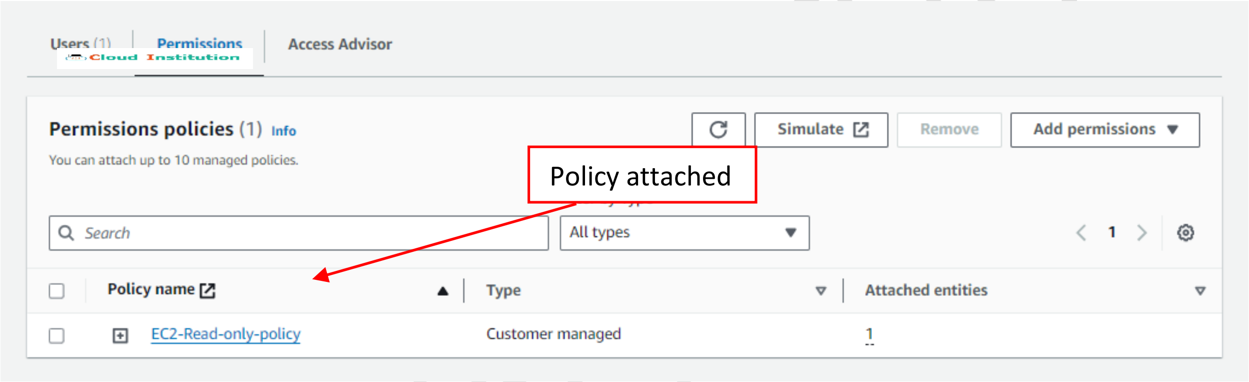
You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Filter by Type

| ☑ | Policy name ▲ | Type | Used as |
|---|---|---|---|
| ☑ | ⊞ EC2-Read-only-policy | Customer managed | None |

Select the created policy

Click attach



Permissions policies (1) Info

You can attach up to 10 managed policies.

| □ | Policy name | Type | Attached entities |
|---|---|---|---|
| □ | ⊞ EC2-Read-only-policy | Customer managed | 1 |

Policy attached