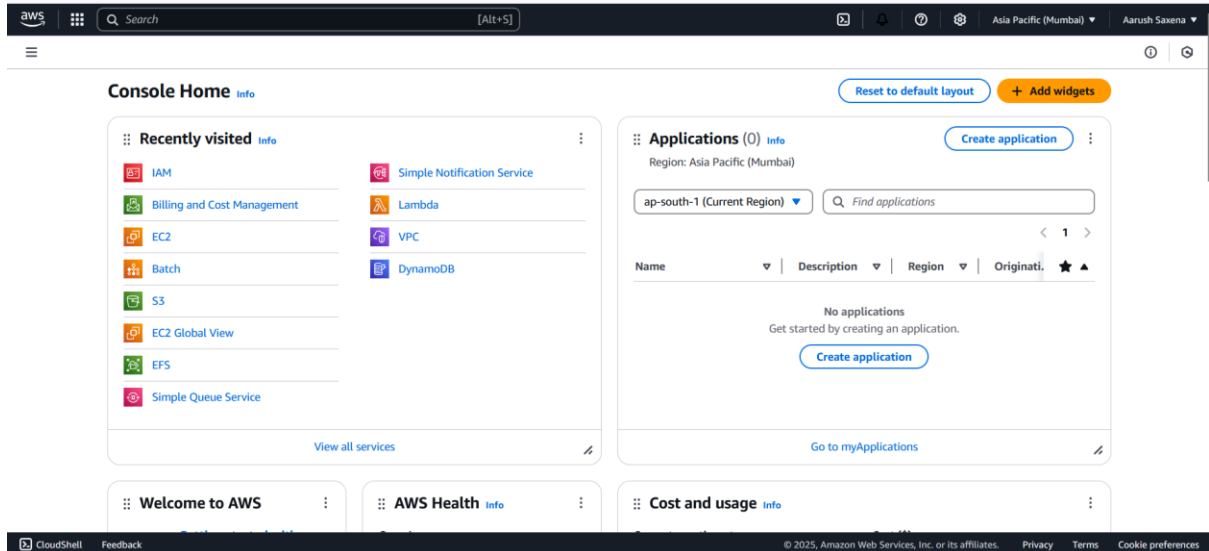
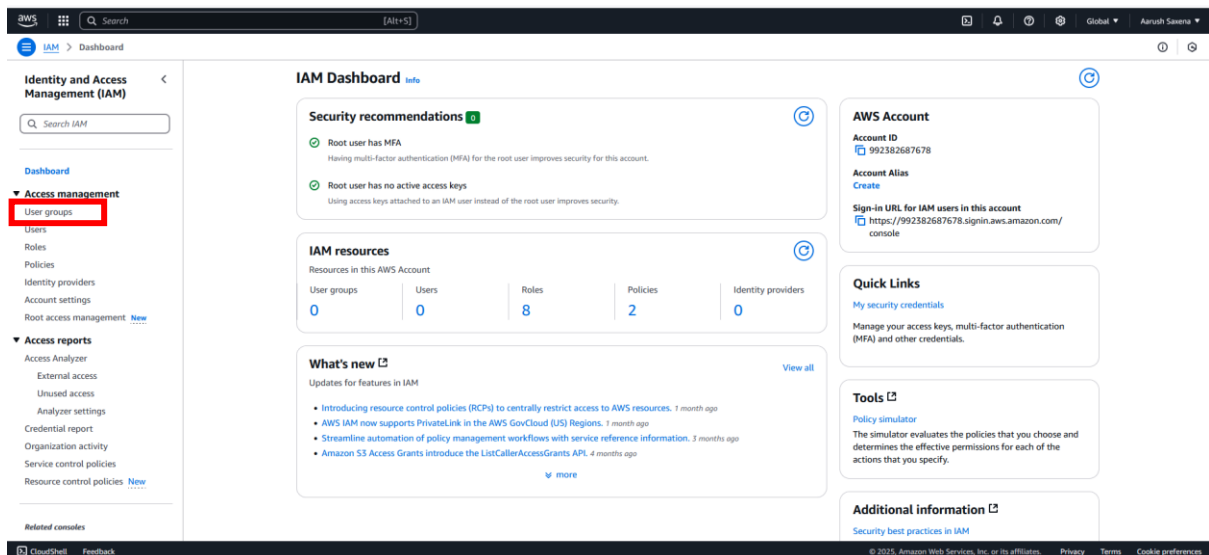


How to create user groups and attach it to IAM users

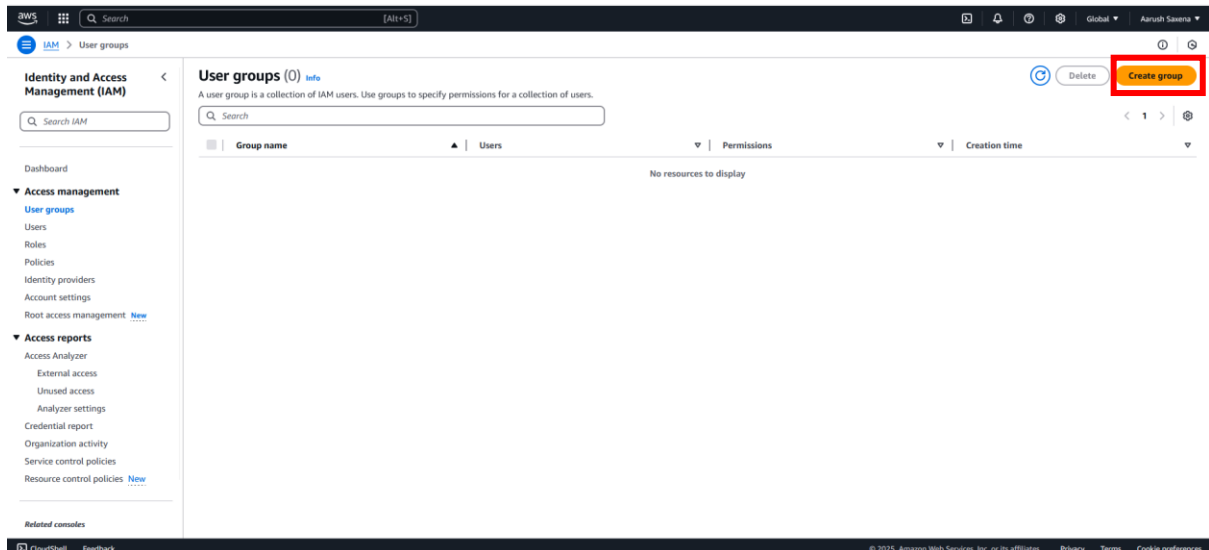
Step1: Log-in to your aws console, search for IAM or click on IAM from the dashboard as shown in image given below.



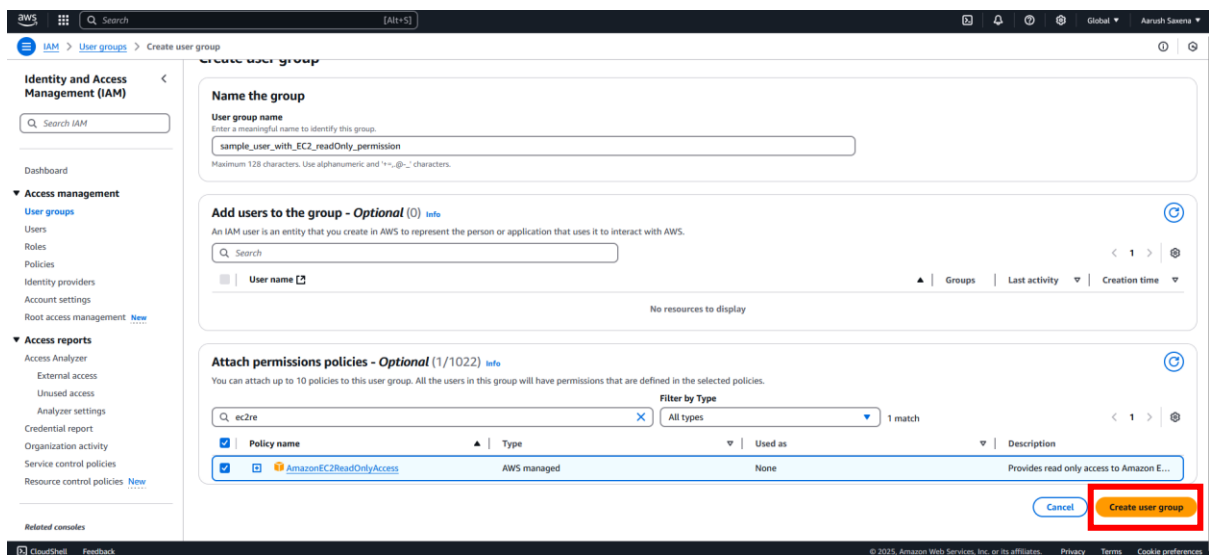
After clicking on it you can see IAM Dashboard from there click on user groups to create groups you can attach one group to multiple users and vice versa.



Click on user groups as shown in image given below then you can see a window click on create group button to create group and add permissions or policies to it.

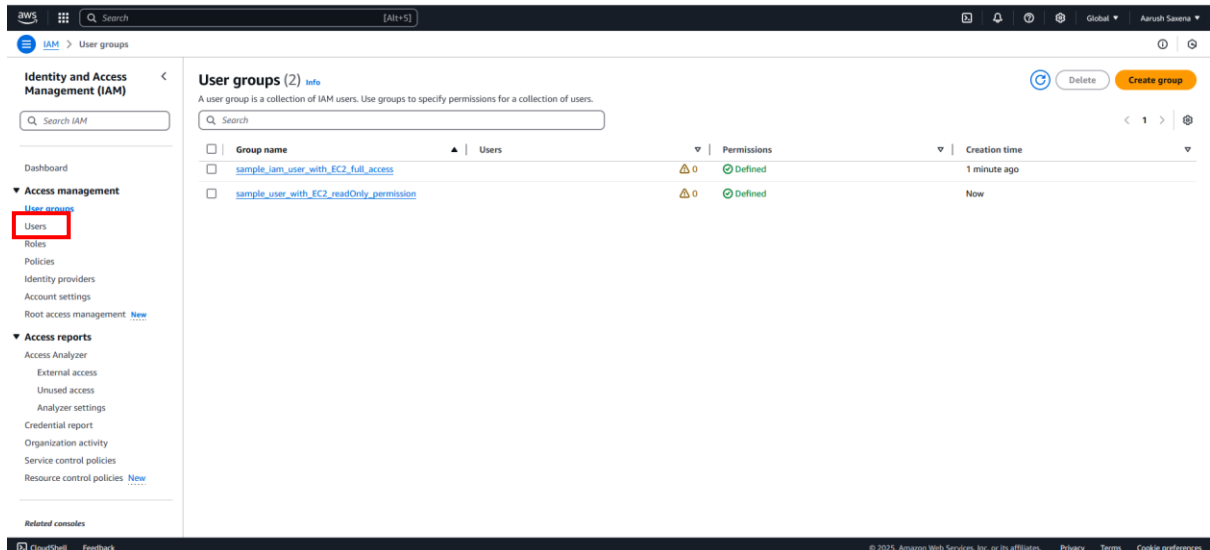


Then provide name to your group and click on create user group.

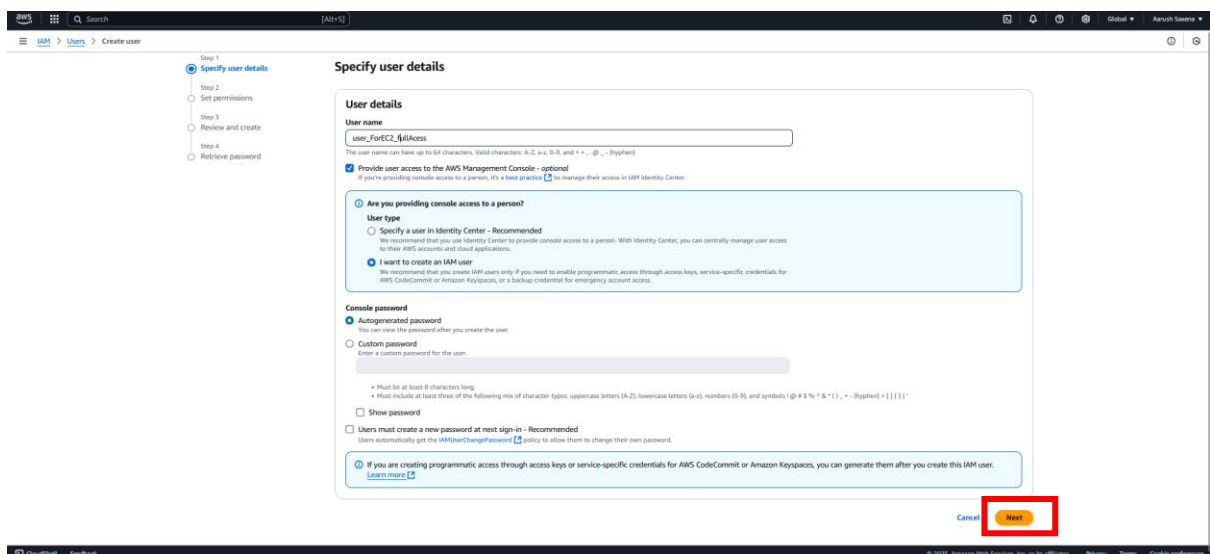
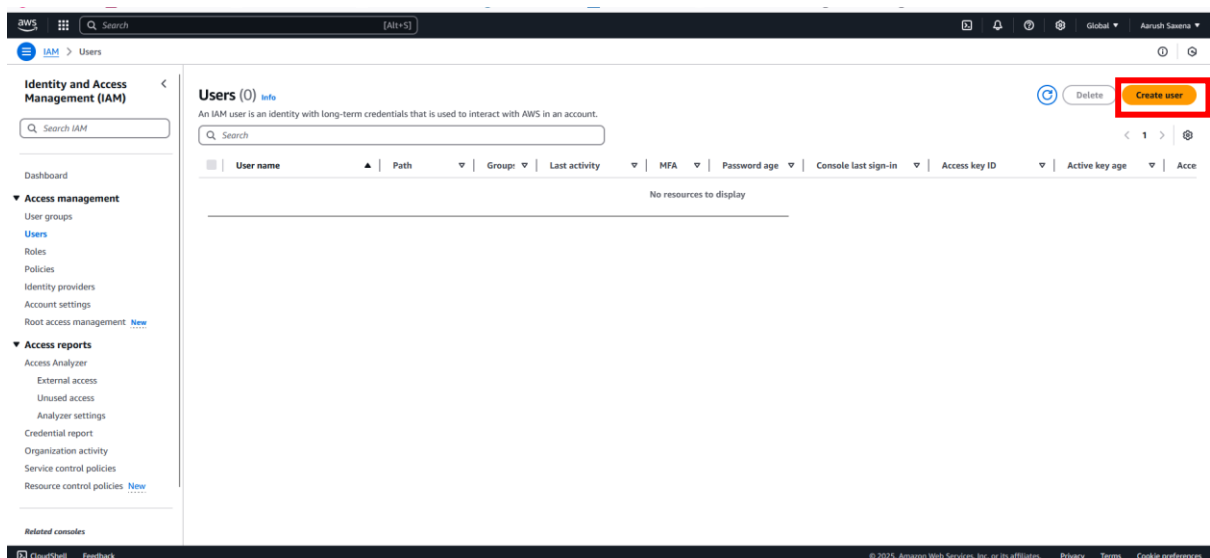


Create another group with same process but in above image we provide read only permission and in another group we attach EC2 full access policies.

Go back to users and create users.



Create users and attach these user groups to it we are going to create two users and attach groups to it.



Attach user groups according to there skills or as per requirements of it and click on next.

The screenshot shows the 'Set permissions' step of the AWS IAM 'Create user' wizard. The left sidebar indicates the current step is 'Set permissions'. The main content area has a heading 'Set permissions' and a subtext '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](#)'. Below this is a 'Permissions options' section with three radio buttons: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. The 'Add user to group' option has a description: 'Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.' Below this is a 'User groups (2)' section with a search bar and a table of existing groups. The table has columns for 'Group name', 'Users', 'Attached policies', and 'Created'. Two groups are listed: 'sample_iam_user_with_EC2_full_access' and 'sample_user_with_EC2_readOnly_permi...'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons, with the 'Next' button highlighted by a red box.

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

Set 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, 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 (2)

Search

<input type="checkbox"/>	Group name	Users	Attached policies	Created
<input type="checkbox"/>	sample_iam_user_with_EC2_full_access	0	AmazonEC2FullAccess	2025-01-05 (5 minutes ago)
<input type="checkbox"/>	sample_user_with_EC2_readOnly_permi...	0	AmazonEC2ReadOnlyAccess	2025-01-05 (1 minute ago)

► Set permissions boundary - optional

Cancel Previous **Next**

The screenshot shows the 'Review and create' step of the AWS IAM 'Create user' wizard. The left sidebar indicates the current step is 'Review and create'. The main content area has a heading 'Review and create' and a subtext 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.' Below this is a 'User details' section with three columns: 'User name' (user_forEC2_fullAccess), 'Console password type' (Autogenerated), and 'Require password reset' (No). Below this is a 'Permissions summary' section with a table showing the group 'sample_iam_user_with_EC2_full_access' as a 'Permissions group'. Below this is a 'Tags - optional' section with a search bar and a list of tags. One tag is shown: 'userWithFullAccess'. At the bottom right, there are 'Cancel', 'Previous', and 'Create user' buttons.

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name user_forEC2_fullAccess	Console password type Autogenerated	Require password reset No
-------------------------------------	--	------------------------------

Permissions summary

Name	Type	Used as
sample_iam_user_with_EC2_full_access	Group	Permissions group

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.

Key: name Value: optional

userWithFullAccess

Remove

Use "userWithFullAccess"

Add new tag

You can add up to 49 more tags.

Cancel Previous **Create user**

The screenshot shows the 'Retrieve password' step of the AWS IAM 'Create user' wizard. The left sidebar indicates the current step is 'Retrieve password'. The main content area has a heading 'Retrieve password' and a subtext '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.' Below this is a 'Console sign-in details' section with a table showing the console sign-in URL, user name, and console password. At the bottom right, there are 'Cancel', 'Download .csv file', and 'Return to users list' buttons.

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

Retrieve password

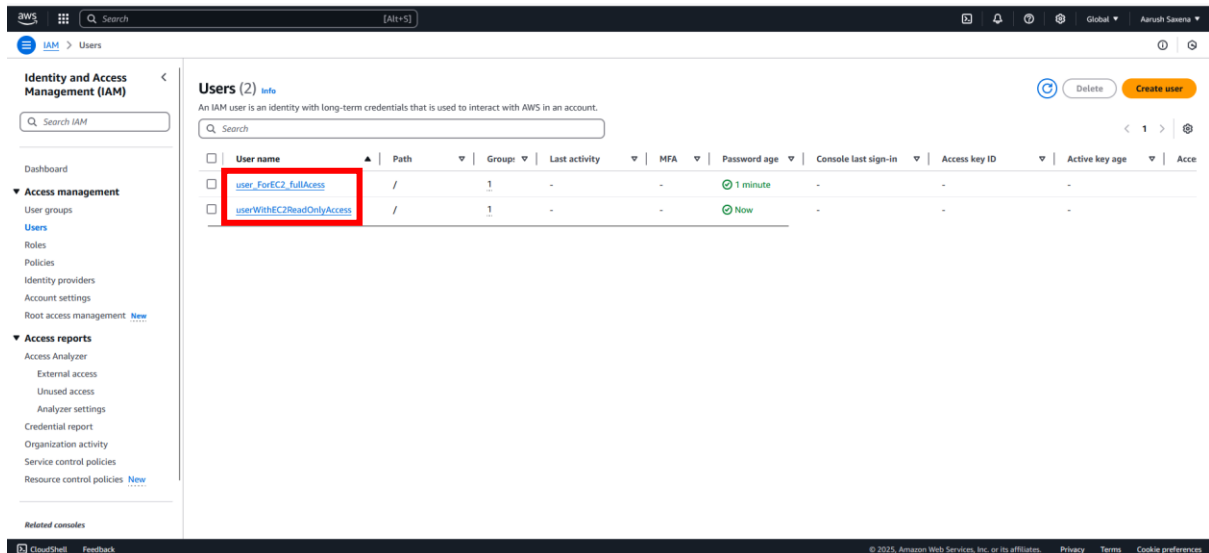
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL https://992382687678.signin.aws.amazon.com/console	Email sign-in instructions
User name user_forEC2_fullAccess	
Console password Show	

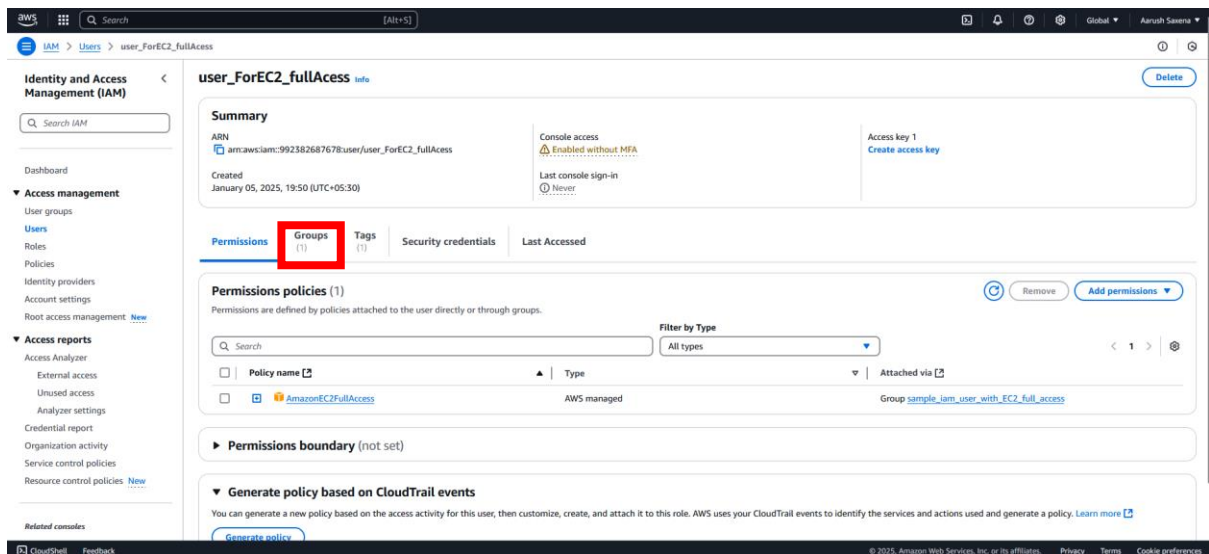
Cancel Download .csv file Return to users list

You can see our users has been created and groups attach to it you can also see it by clicking on user name and click on groups and it will show all groups attach to iam user.



The screenshot shows the AWS IAM console 'Users' page. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Related consoles. The main content area displays a table of users. The user 'user_ForEC2_fullAccess' is highlighted with a red box. The table columns include User name, Path, Groups, Last activity, MFA, Password age, Console last sign-in, Access key ID, Active key age, and Access key.

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Access key
user_ForEC2_fullAccess	/	1	-	-	1 minute	-	-	-	-
userWithEC2ReadOnlyAccess	/	1	-	-	Now	-	-	-	-



The screenshot shows the AWS IAM console 'user_ForEC2_fullAccess' details page. The left sidebar is the same as the previous screenshot. The main content area displays the user's summary, permissions, groups, tags, security credentials, and last accessed information. The 'Groups' tab is highlighted with a red box. The 'Permissions policies' section shows a list of policies attached to the user.

Summary

ARN: `arn:aws:iam::992382687678:user/user_ForEC2_fullAccess`
Created: January 05, 2025, 19:50 (UTC+05:30)
Console access: Enabled without MFA
Last console sign-in: Never

Permissions **Groups (1)** **Tags (1)** **Security credentials** **Last Accessed**

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
AmazonEC2FullAccess	AWS managed	Group sample_iam_user_with_EC2_full_access

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

Search

[Alt+S]

Global

Aarush Saxena

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

Related consoles

user_ForEC2_fullAccess

Delete

Summary

ARN

arn:aws:iam::992382687678:user/user_ForEC2_fullAccess

Console access

Enabled without MFA

Access key 1

Create access key

Created

January 05, 2025, 19:50 (UTC+05:30)

Last console sign-in

Never

Permissions

Groups

Tags

Security credentials

Last Accessed

User groups membership

Remove

Add user to groups

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.

Group name

sample_iam_user_with_EC2_full_access

Attached policies

AmazonEC2FullAccess

CloudShell

Feedback

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