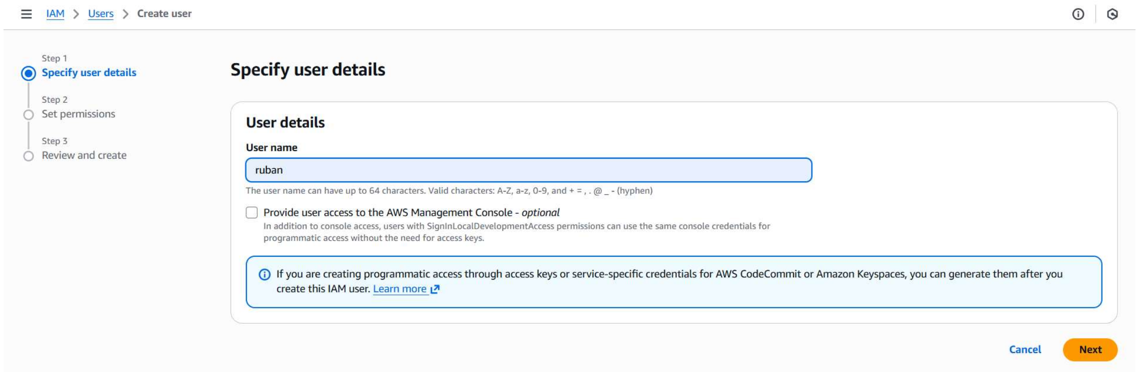
AWS IAM Users and User Groups Creation.

What is IAM?

IAM lets you:

- Create **Users** (individual identities)
- Create **Groups** (collection of users)
- Assign **Policies** (permissions)
- Control access to AWS services securely

Step 1: specify the user details.



Specify user details

User details

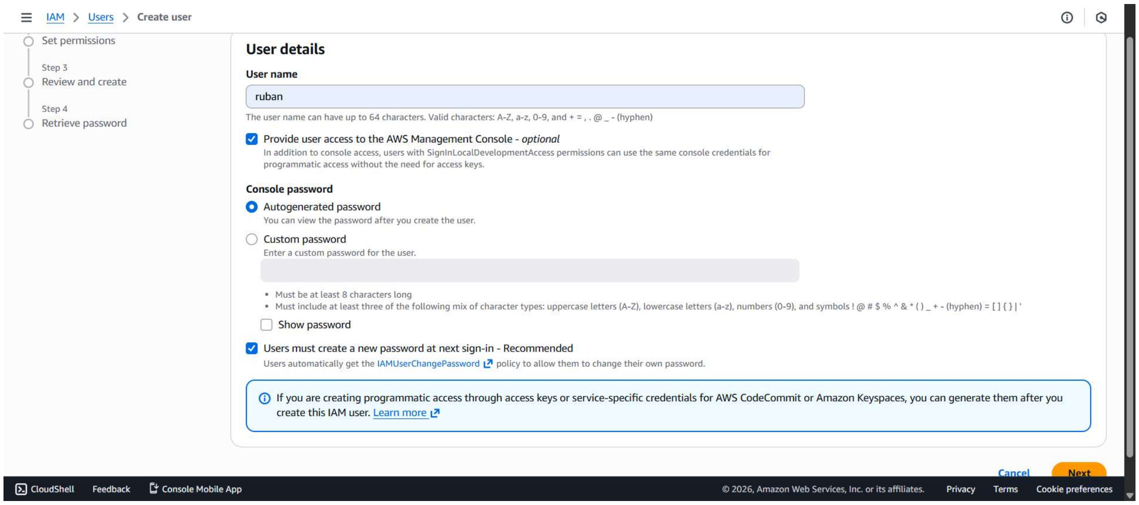
User name

ruban

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*
In addition to console access, users with SignInLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.

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



User details

User name

ruban

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*
In addition to console access, users with SignInLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.

Console password

● Autogenerated password
You can view the password after you create the user.

○ Custom password
Enter a custom password for the user.

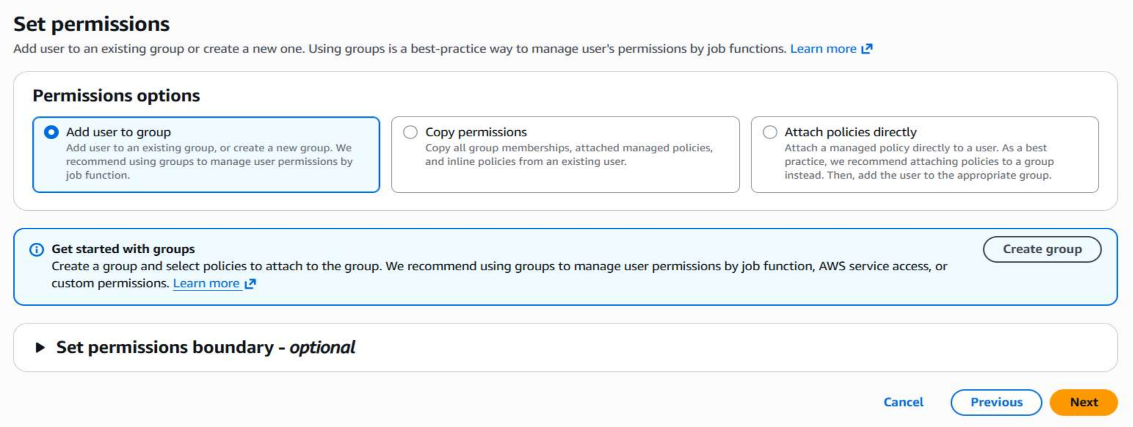
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ 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

Step 2 : if you want you have to set permission.



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

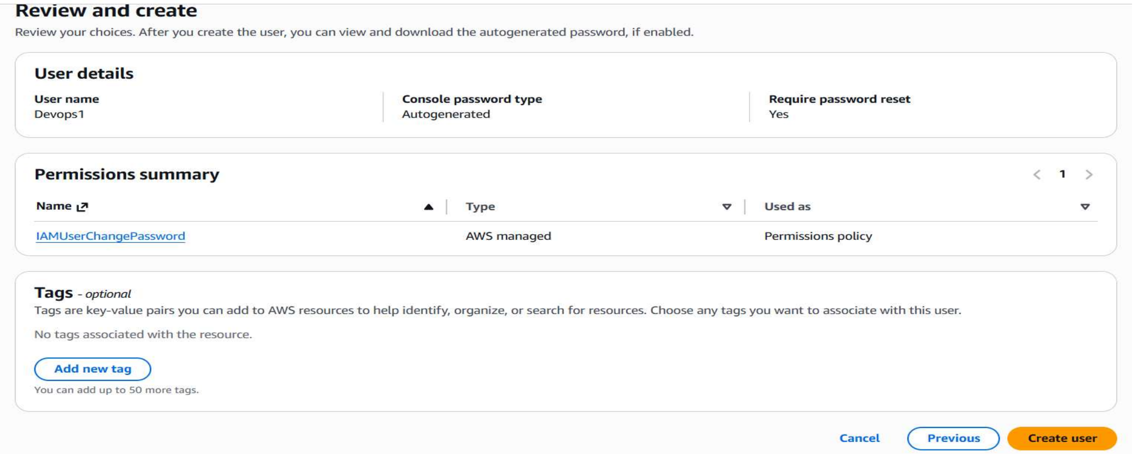
Permissions options

- ● 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.

Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more

▶ **Set permissions boundary - *optional***

Step 3 : You can see the details of the permission and review the details.



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	Console password type	Require password reset
Devops1	Autogenerated	Yes

Permissions summary

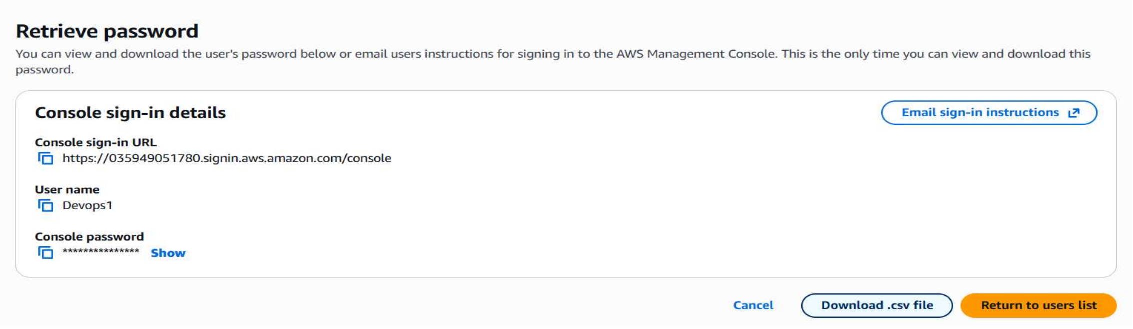
Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

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.

Step 4 : you have to download the csv file and you have to mail it to the personnel.



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.

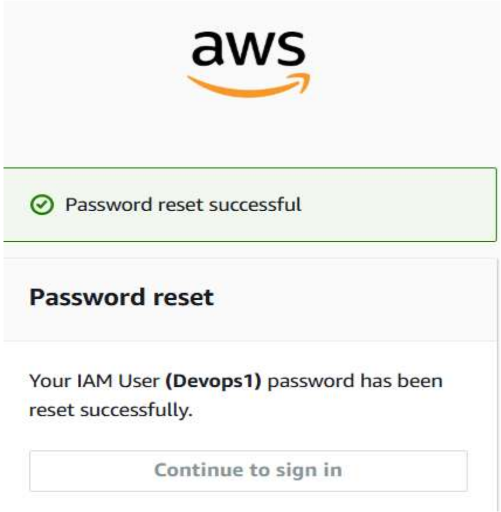
Console sign-in details

Console sign-in URL
https://035949051780.signin.aws.amazon.com/console

User name
Devops1

Console password
*************** Show

Step 5 : then we have to create an new password for the personnel.



Password reset successful

Password reset

Your IAM User **(Devops1)** password has been reset successfully.

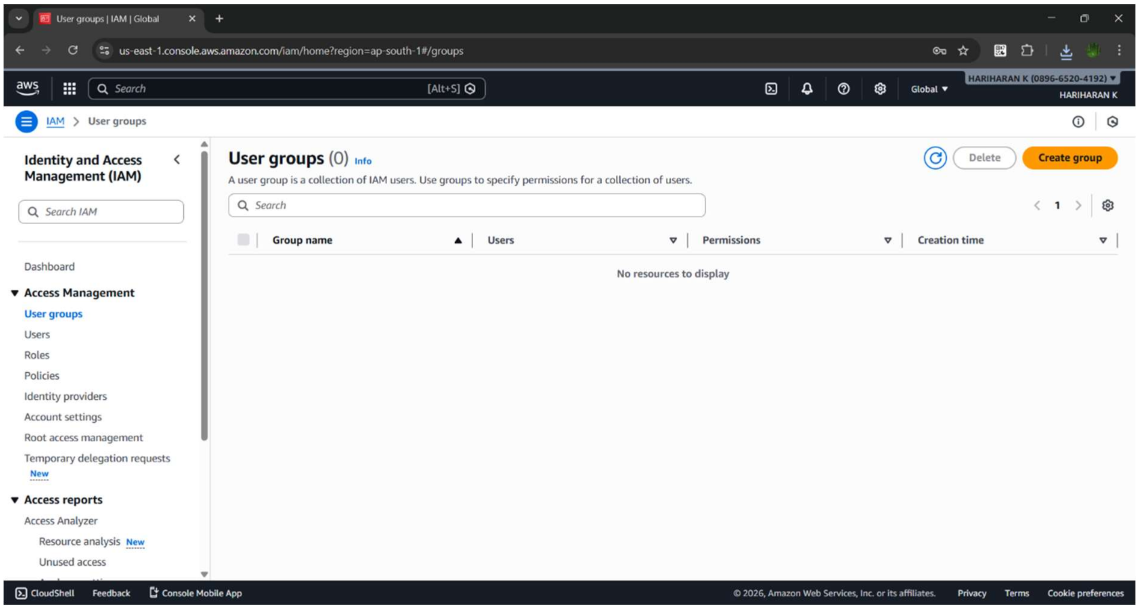
Creating an IAM Group

Groups are smart.
You don't assign permissions to users individually — you assign to groups.

Example:

- Dev group → EC2 + S3 access
- Admin group → Full access
- ReadOnly group → View only

Step 1 : creating the user groups.



us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups

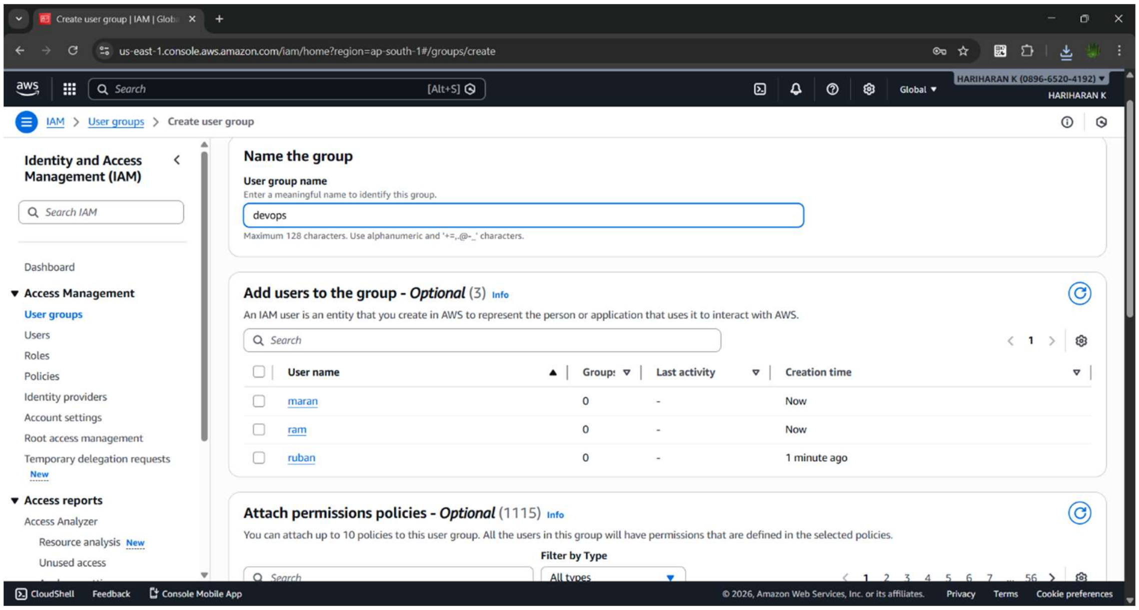
User groups (0)

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

No resources to display

© 2026, Amazon Web Services, Inc. or its affiliates.



us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/create

IAM > User groups > Create user group

Name the group

User group name
Enter a meaningful name to identify this group.
devops
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (3) 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.

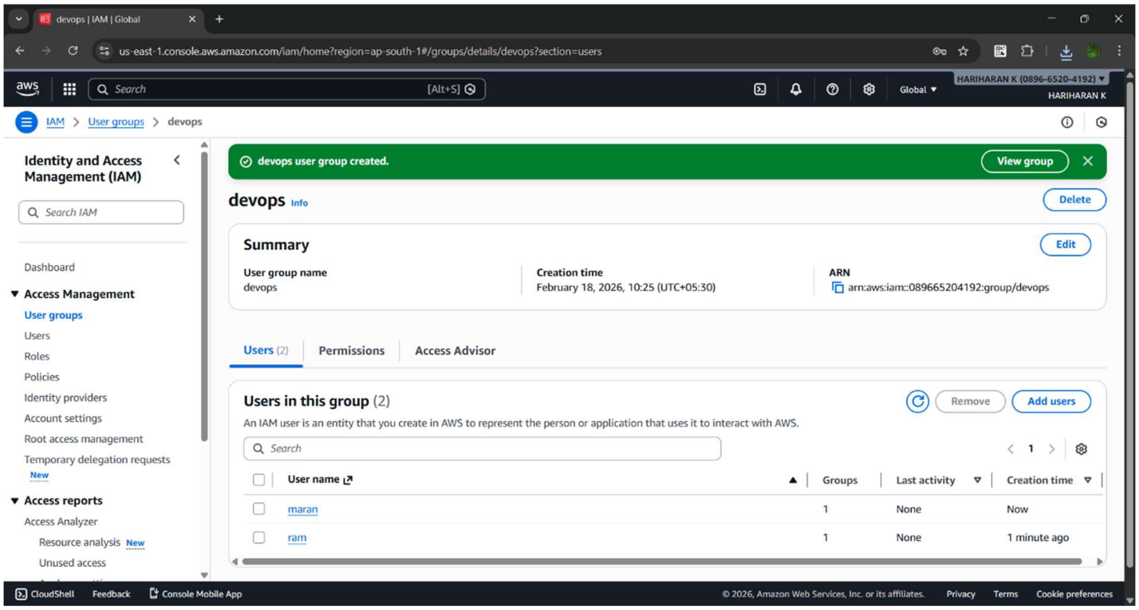
□	User name	Groups	Last activity	Creation time
□	maran	0	-	Now
□	ram	0	-	Now
□	ruban	0	-	1 minute ago

Attach permissions policies - *Optional* (1115) 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

Step 2 : we can see the users in the group.



us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/devops?section=users

IAM > User groups > devops

devops user group created.

devops Info

Summary

User group name	Creation time	ARN
devops	February 18, 2026, 10:25 (UTC+05:30)	arn:aws:iam::089665204192:group/devops

Users (2) | Permissions | Access Advisor

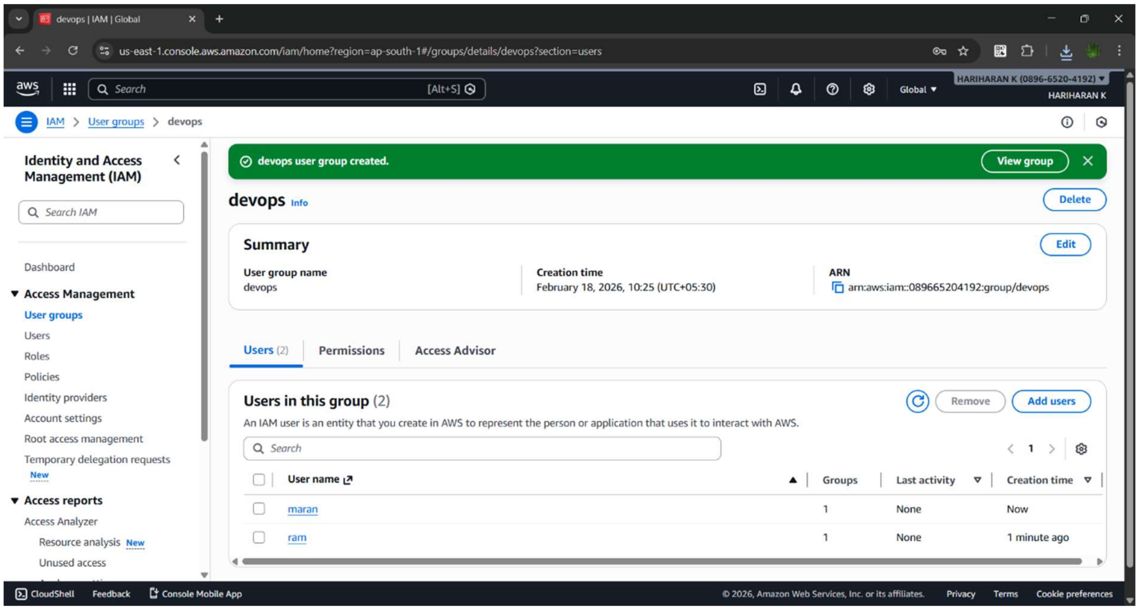
Users in this group (2)

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
□	maran	1	None	Now
□	ram	1	None	1 minute ago

Add Users to Group

- Go to:
  Users → Select user → Add to group → Select group → Save.



devops | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/devops?section=users

HARIHARAN K (0896-6520-4192) · HARIHARAN K · Global

IAM > User groups > devops

Identity and Access Management (IAM)

- Dashboard
- Access Management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
  - Root access management
  - Temporary delegation requests New
- Access reports
  - Access Analyzer
    - Resource analysis New
    - Unused access

devops user group created.

devops

Summary

User group name	Creation time	ARN
devops	February 18, 2026, 10:25 (UTC+05:30)	arn:aws:iam::089665204192:group/devops

Users (2) | Permissions | Access Advisor

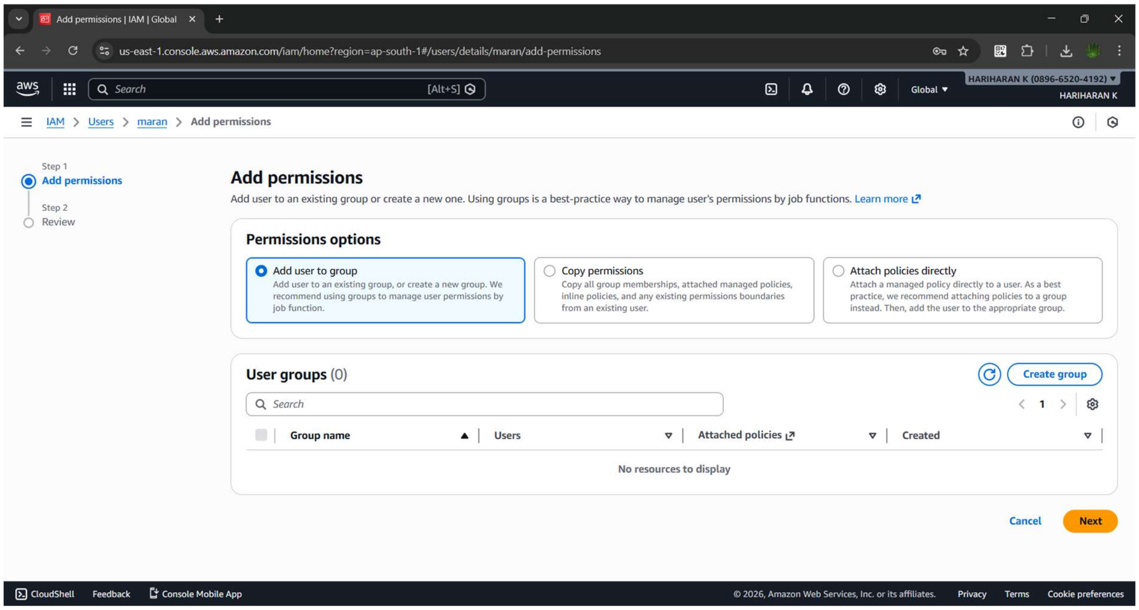
Users in this group (2)

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
maran	1	None	Now
ram	1	None	1 minute ago

© 2026, Amazon Web Services, Inc. or its affiliates.

Giving permission to the user.



Add permissions | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/maran/add-permissions

HARIHARAN K (0896-6520-4192) · HARIHARAN K · Global

IAM > Users > maran > Add permissions

Step 1 ● Add permissions

Step 2 ○ Review

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

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, inline policies, and any existing permissions boundaries from an existing user.

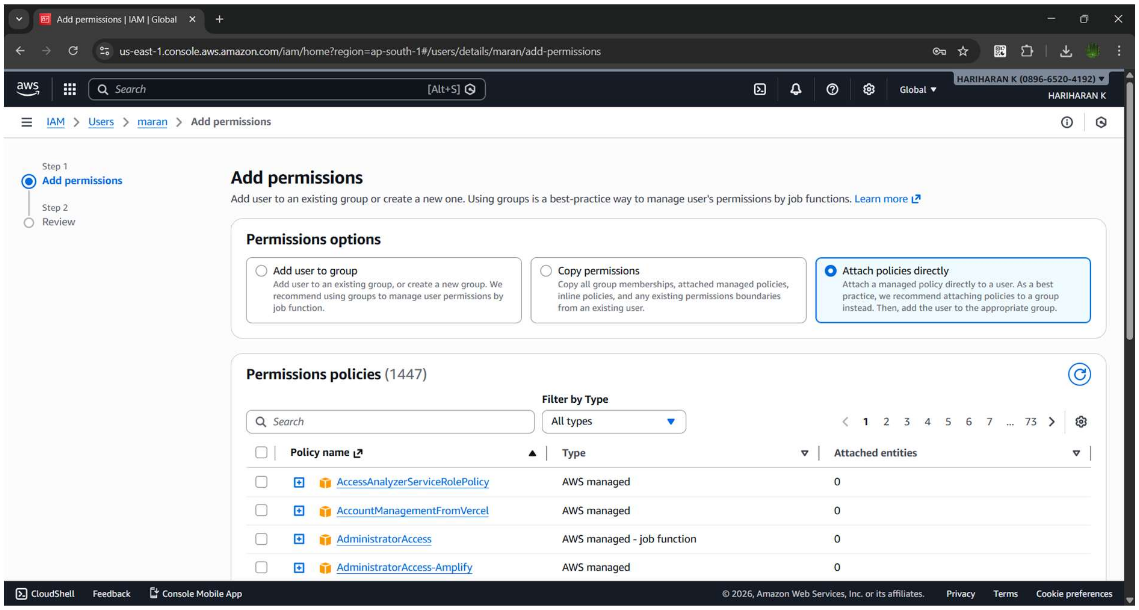
○ Attach policies directly — Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (0)

Group name	Users	Attached policies	Created
No resources to display			

Cancel | Next

© 2026, Amazon Web Services, Inc. or its affiliates.



Add permissions | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/maran/add-permissions
Search [Alt+S]
Global
HARIHARAN K (0896-6520-4192)
HARIHARAN K
IAM > Users > maran > Add permissions
Step 1
Add permissions
Step 2
Review

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

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, inline policies, and any existing permissions boundaries 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.

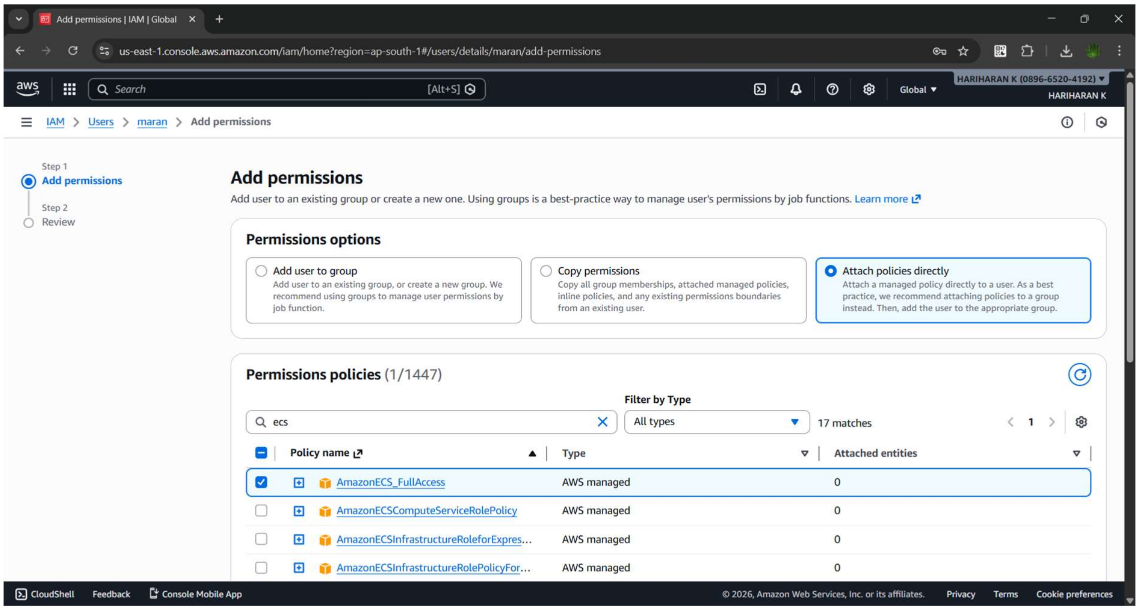
Permissions policies (1447)

Filter by Type: All types

< 1 2 3 4 5 6 7 ... 73 >

□	Policy name	Type	Attached entities
□	AccessAnalyzerServiceRolePolicy	AWS managed	0
□	AccountManagementFromVercel	AWS managed	0
□	AdministratorAccess	AWS managed - job function	0
□	AdministratorAccess-Amplify	AWS managed	0

CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Add permissions | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/maran/add-permissions
Search [Alt+S]
Global
HARIHARAN K (0896-6520-4192)
HARIHARAN K
IAM > Users > maran > Add permissions
Step 1
Add permissions
Step 2
Review

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

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, inline policies, and any existing permissions boundaries 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.

Permissions policies (1/1447)

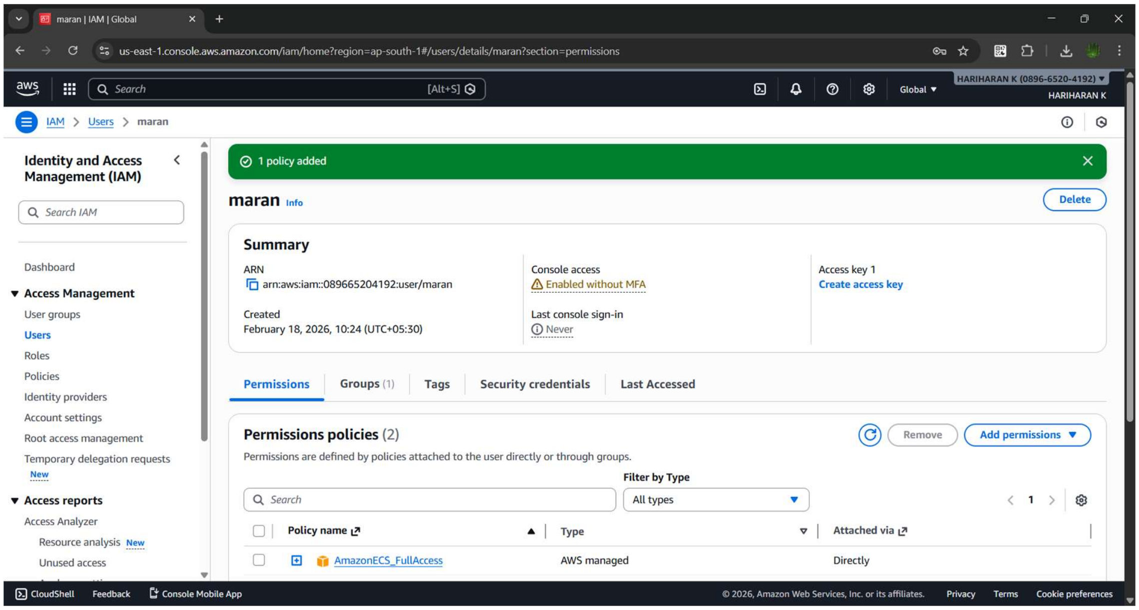
Search: ecs

Filter by Type: All types

17 matches

< 1 >

▣	Policy name	Type	Attached entities
☑	AmazonECS_FullAccess	AWS managed	0
□	AmazonECSComputeServiceRolePolicy	AWS managed	0
□	AmazonECSInfrastructureRoleforExpres...	AWS managed	0
□	AmazonECSInfrastructureRolePolicyFor...	AWS managed	0



1 policy added

maran Info

Summary

ARN
arn:aws:iam::089665204192:user/maran

Created
February 18, 2026, 10:24 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Never

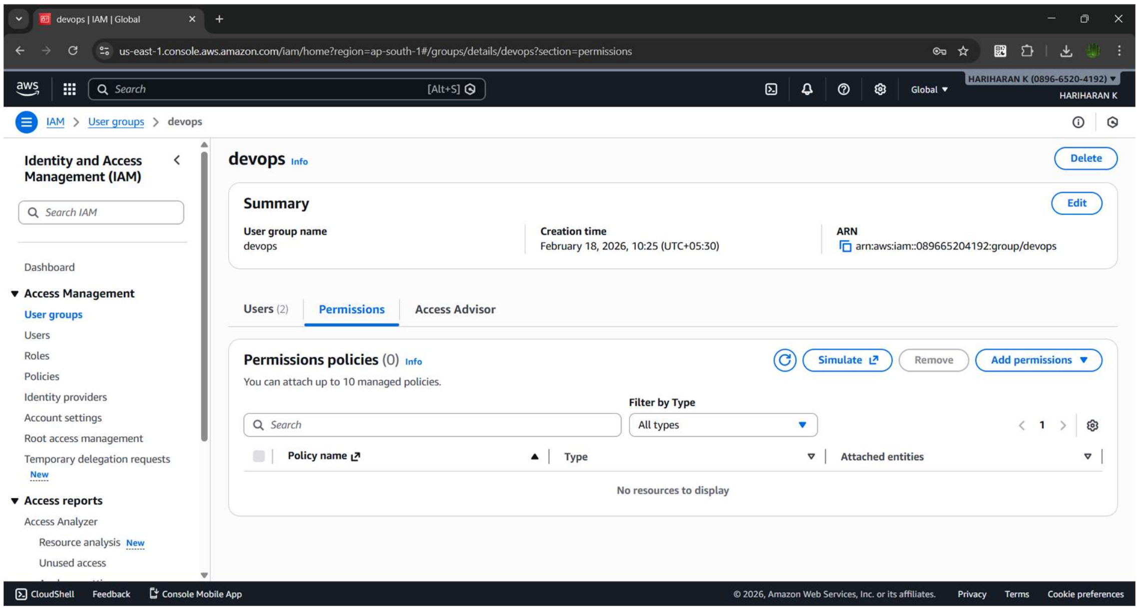
Access key 1
Create access key

Permissions policies (2)

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

Policy name	Type	Attached via
AmazonECS_FullAccess	AWS managed	Directly

Giving permission to the group.



devops Info

Summary

User group name
devops

Creation time
February 18, 2026, 10:25 (UTC+05:30)

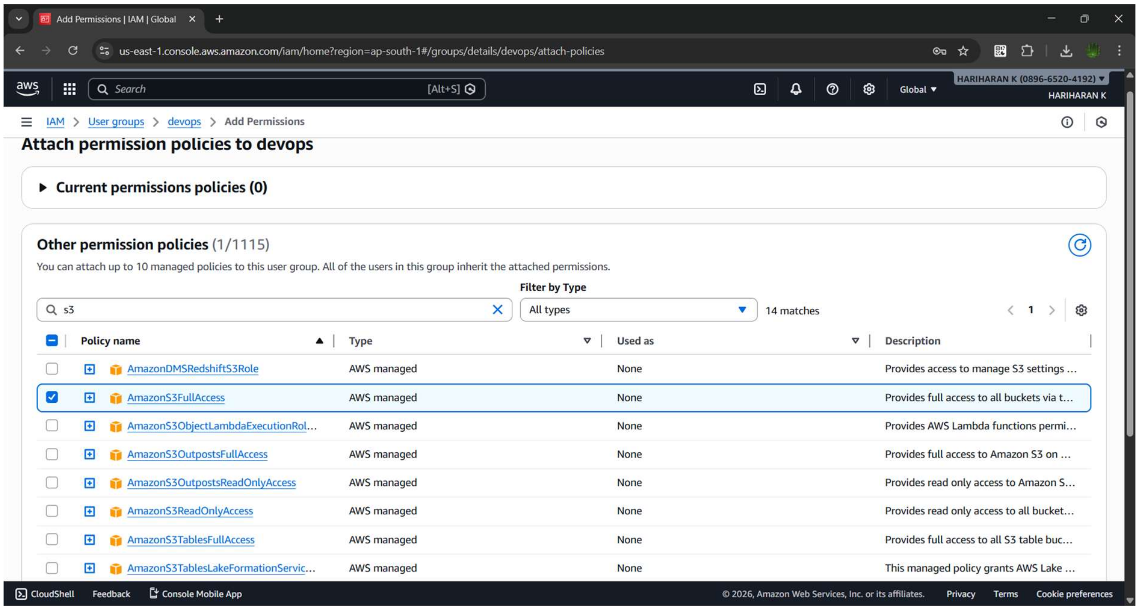
ARN
arn:aws:iam::089665204192:group/devops

Permissions policies (0) Info

You can attach up to 10 managed policies.

Policy name	Type	Attached entities

No resources to display


Add Permissions | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/devops/attach-policies
Search [Alt+S]
Global ▼
HARIHARAN K (0896-6520-4192) ▼
HARIHARAN K
IAM > User groups > devops > Add Permissions

Attach permission policies to devops

▸ Current permissions policies (0)

Other permission policies (1/1115)

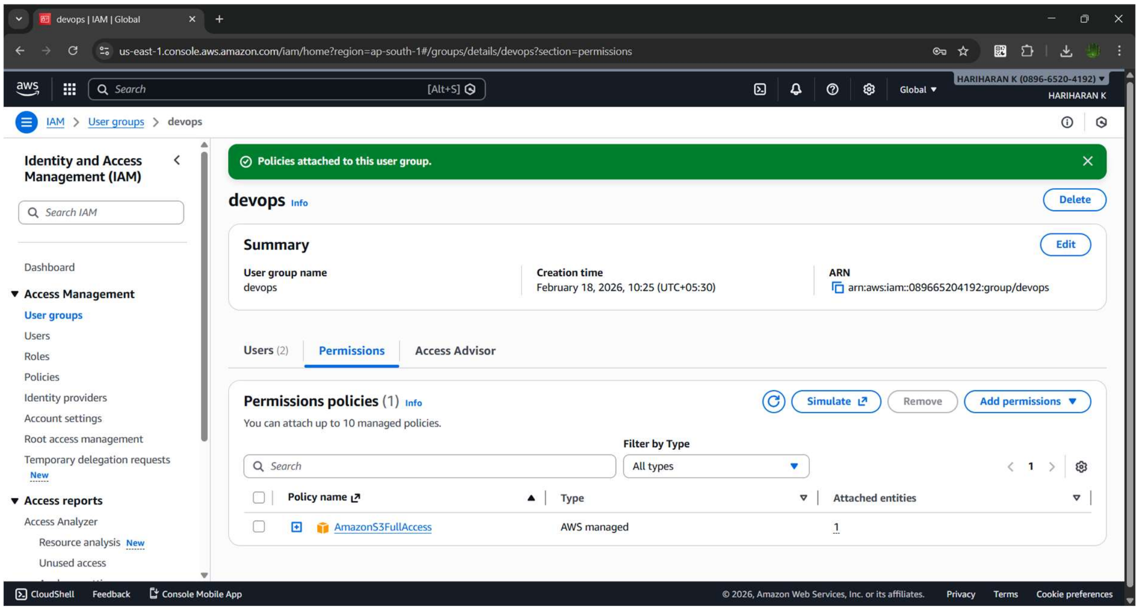
You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Search: s3

Filter by Type: All types

14 matches

	Policy name	Type	Used as	Description
□	AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to manage S3 settings …
☑	AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets via t…
□	AmazonS3ObjectLambdaExecutionRol…	AWS managed	None	Provides AWS Lambda functions permi…
□	AmazonS3OutpostsFullAccess	AWS managed	None	Provides full access to Amazon S3 on …
□	AmazonS3OutpostsReadOnlyAccess	AWS managed	None	Provides read only access to Amazon S…
□	AmazonS3ReadOnlyAccess	AWS managed	None	Provides read only access to all bucket…
□	AmazonS3TablesFullAccess	AWS managed	None	Provides full access to all S3 table buc…
□	AmazonS3TablesLakeFormationServic…	AWS managed	None	This managed policy grants AWS Lake …



Policies attached to this user group.

devops Info

Delete

Summary Edit

User group name	Creation time	ARN
devops	February 18, 2026, 10:25 (UTC+05:30)	arn:aws:iam::089665204192:group/devops

Users (2) | **Permissions** | Access Advisor

Permissions policies (1) Info

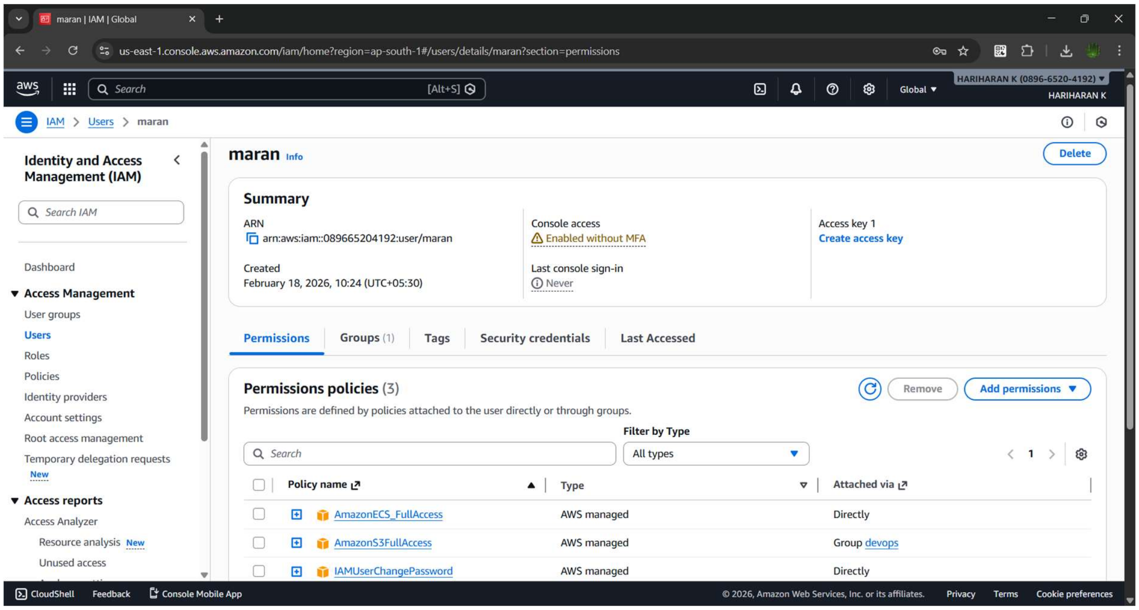
Simulate | Remove | Add permissions ▼

You can attach up to 10 managed policies.

Filter by Type: All types

	Policy name	Type	Attached entities
□	AmazonS3FullAccess	AWS managed	1

The permission given to the user and by group



maran Info

Summary

ARN
arn:aws:iam::089665204192:user/maran

Created
February 18, 2026, 10:24 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

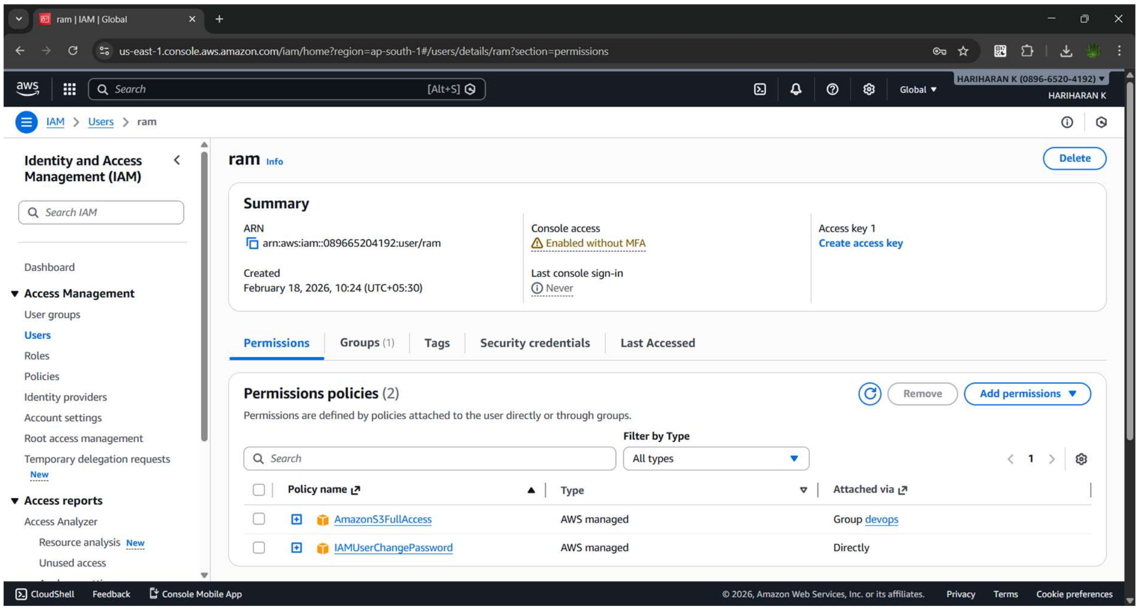
Permissions policies (3)

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

Filter by Type: All types

Policy name	Type	Attached via
AmazonECS_FullAccess	AWS managed	Directly
AmazonS3FullAccess	AWS managed	Group devops
IAMUserChangePassword	AWS managed	Directly

The permission given to the user by group



ram Info

Summary

ARN
arn:aws:iam::089665204192:user/ram

Created
February 18, 2026, 10:24 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

Permissions policies (2)

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

Filter by Type: All types

Policy name	Type	Attached via
AmazonS3FullAccess	AWS managed	Group devops
IAMUserChangePassword	AWS managed	Directly