

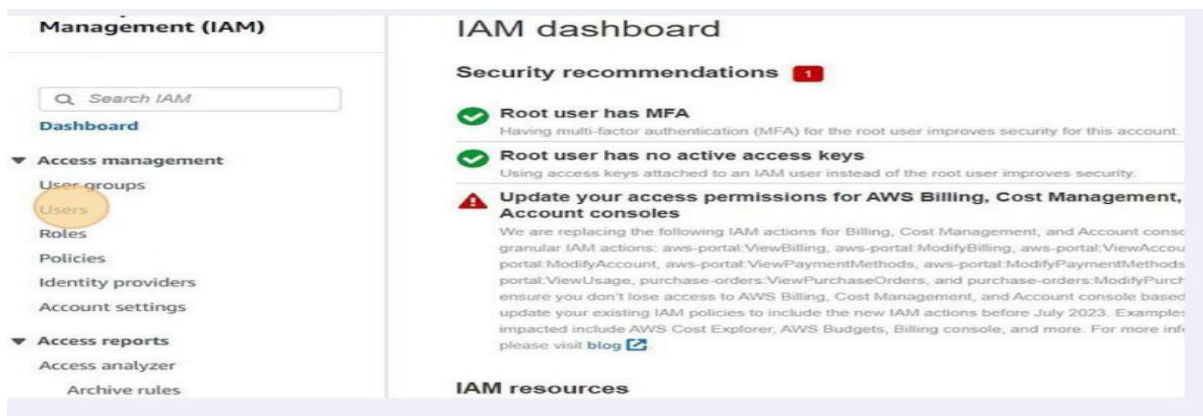
AWS-3

Create IAM resource giving full access of S3(storage).

1. Sign in to your console (as root user).
2. On the top side of the page go to the Search bar and type "IAM".
3. Click on the first result showing "IAM"



4. Then click on users.



5. Then click on Add users.



6. After that you have to create a user and specify the details.
 - a. Specify the name of the user
 - b. Check the "Provide user access to the AWS Management Console" box
 - c. Select the option "I want to create an IAM user".
 - d. Select custom password and enter it.
 - e. Uncheck the "Users must create a new password at next sign-in" box.
 - f. Then click on next.

User details

User name

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?

☐ Specify a user in Identity Center - Recommended
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

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

☒ 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](#)

Cancel **Next**

7. Now under Permissions Options, select Add user to Group option.
8. Under User Groups click on Create Group button.

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)

Create group

<input type="checkbox"/>	Group name	Users	Attached policies	Created
<input type="checkbox"/>	Server_EC2	1	AmazonEC2FullAcce...	2023-02-13 (5 days ...)
<input type="checkbox"/>	Storage_S3	1	AmazonDMSRedshift...	2023-02-13 (5 days ...)

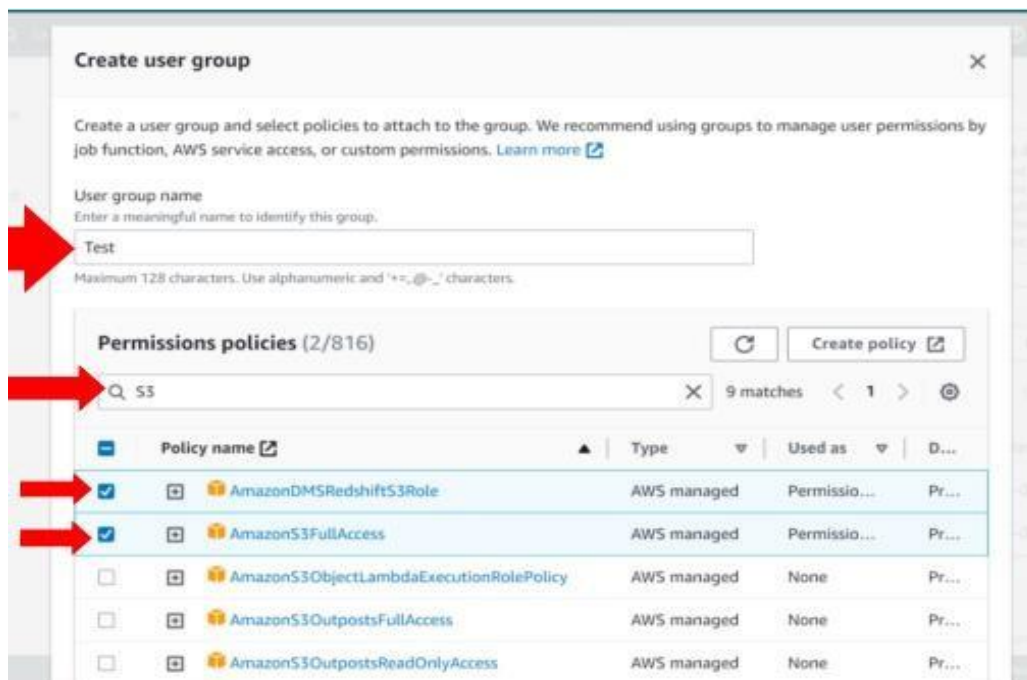
9. A pop-up will appear where you have to specify the new group name and edit the policies/permissions associated with it

a. Enter the User Group Name

b. Next in the find policies search bar type S3 as we have to give permission only for S3.

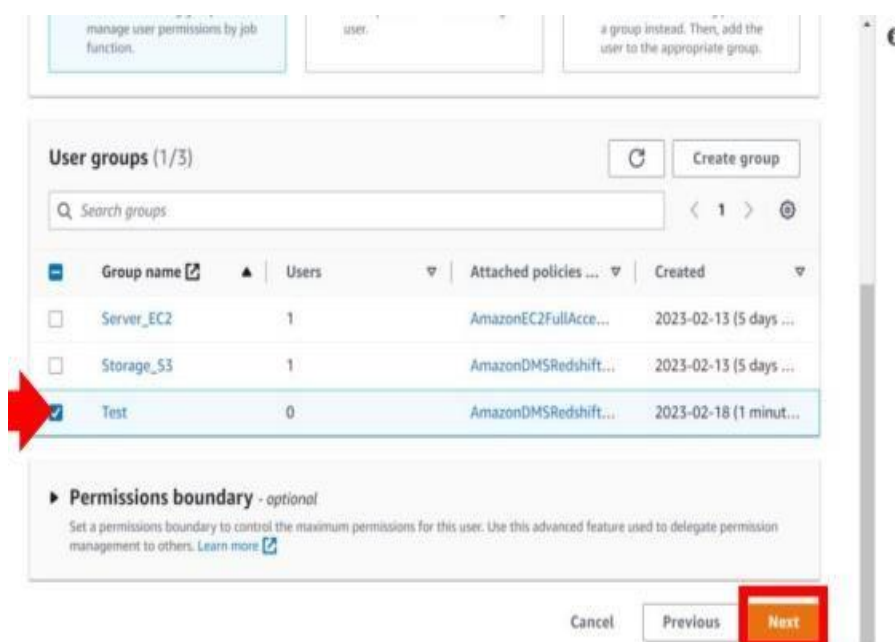
c. Select the first two options

d. Then click on Create User Group

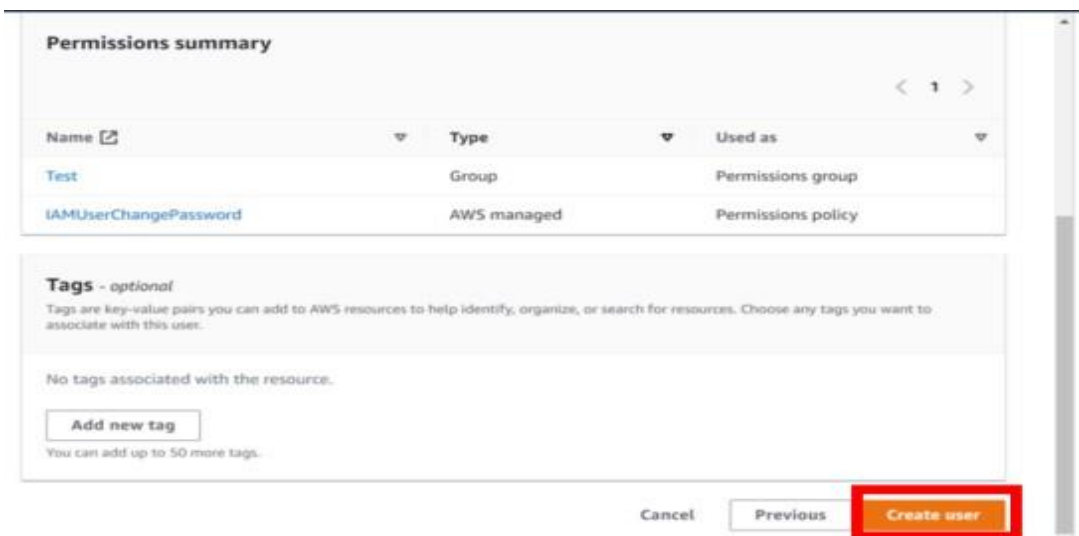


10. Now the pop-up closes and under the User Groups section our newly created group is visible in a table format. Select the group.

11. Then click on Next.



12. We arrive at the Review and Create page. After reviewing click on the Create User button.



Permissions summary

Name	Type	Used as
Test	Group	Permissions group
IAMUserChangePassword	AWS managed	Permissions policy

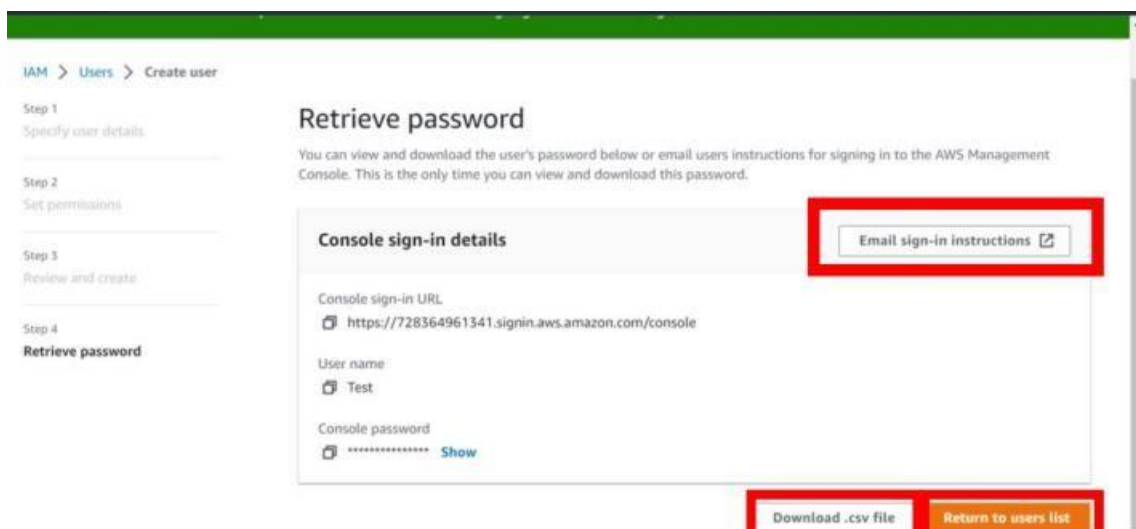
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)
You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create user](#)

13. Next, we arrive at the Retrieve Password page where we can download a .csv file or email the sign-in details of the newly created IAM user.



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

[Email sign-in instructions](#)

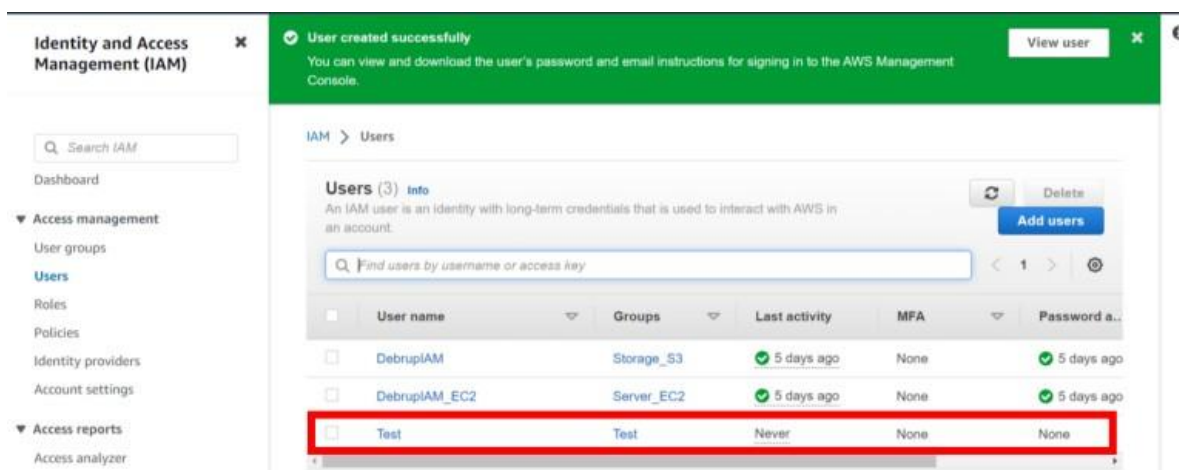
Console sign-in URL
<https://728364961341.signin.aws.amazon.com/console>

User name
Test

Console password
***** [Show](#)

[Download .csv file](#) [Return to users list](#)

14. After that we can return to users list and see that our new user has been added to the users' table.



Identity and Access Management (IAM)

[Search IAM](#)

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer

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

[View user](#)

Users (3)

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

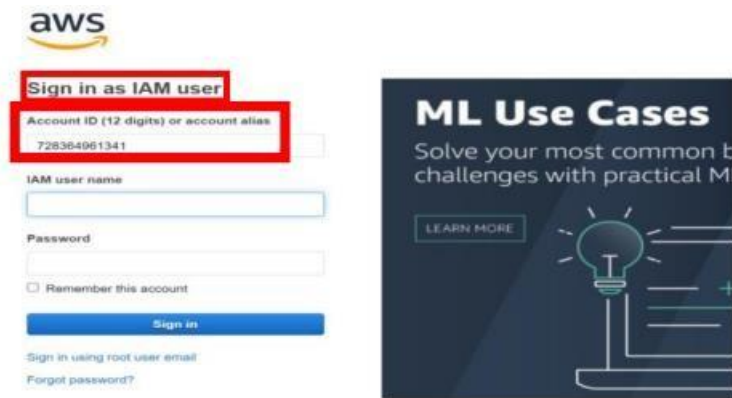
[Find users by username or access key](#)

User name	Groups	Last activity	MFA	Password a...
DebrupIAM	Storage_S3	5 days ago	None	5 days ago
DebrupIAM_EC2	Server_EC2	5 days ago	None	5 days ago
Test	Test	Never	None	None

15. Now we logout of our console.

16. Next, we again try to login to the console. But now we select IAM user login.

17. Here we have to enter Account ID of the root user. We can get that in the drop-down menu after logging in our root user account. Alternatively, we can use the link in our downloaded .csv file or our email which if used in our browser will redirect use to the login page with the Account ID already entered!



18. Enter the credentials.

19. Note the username in the top right corner. Also, you cannot access your account page as it is controlled only by your root user.

20. Next you can type S3 in the search box and select the first option.

21. Hence we have full access of S3.

