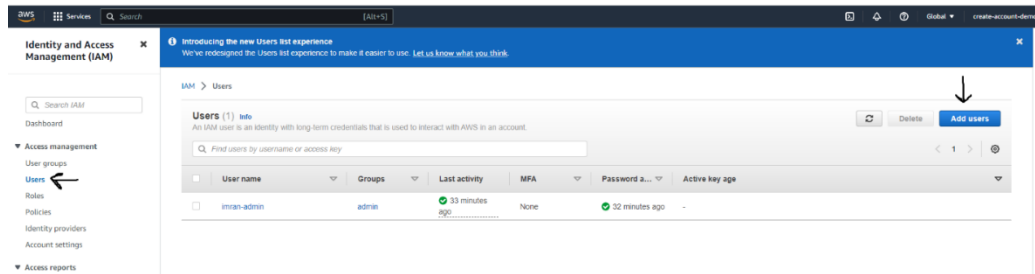


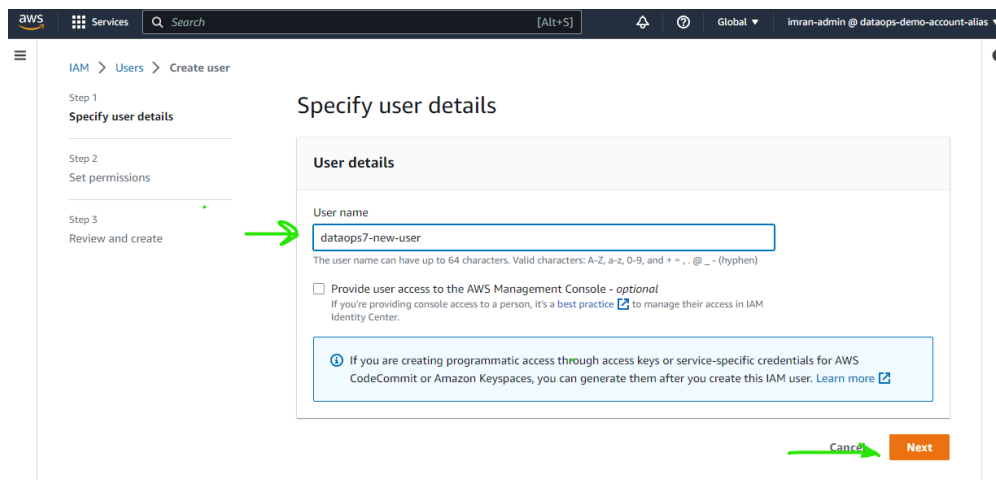
Create User -Give Access to S3-Create Access Key

1- Open IAM User Service

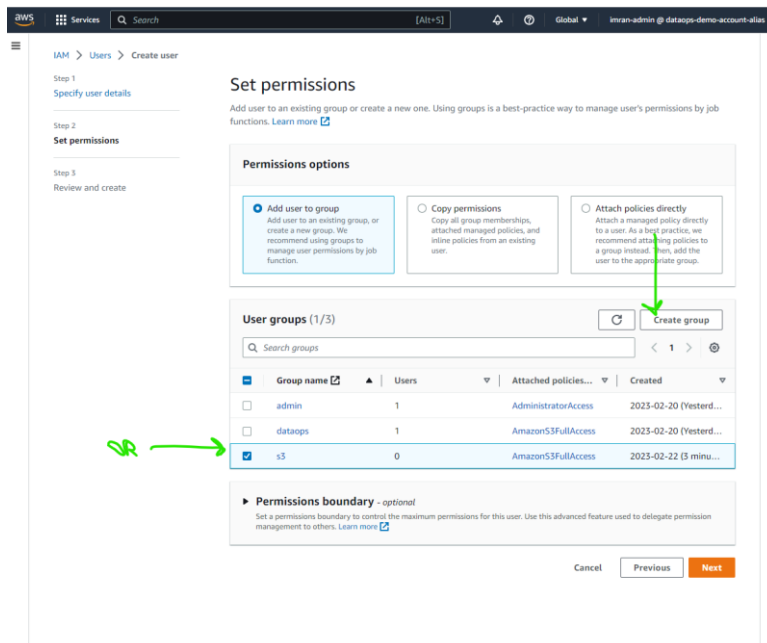
Click User and Add User



2- Give name



3- Create group or add it to existing group or you can select attach policies directly



4- Create new group

Give name → select permission

Create user group

Create a user 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](#)

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

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

Permissions policies (1/816)

1 match < 1 >

<input checked="" type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	Permissions policy (2)	Provides full access ...

5- 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.

User groups (1/4)

< 1 >

<input type="checkbox"/>	Group name	Users	Attached policies...	Created
<input type="checkbox"/>	admin	1	AdministratorAccess	2023-02-20 (Yesterd...
<input type="checkbox"/>	dataops	1	AmazonS3FullAccess	2023-02-20 (Yesterd...
<input type="checkbox"/>	s3	0	AmazonS3FullAccess	2023-02-22 (8 minu...
<input checked="" type="checkbox"/>	S3-Access	0	AmazonS3FullAccess	2023-02-22 (Now)

Permissions boundary - optional
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

6- Create User

The screenshot shows the 'Review and create' step in the AWS IAM console. A green notification banner at the top states 'S3-Access user group created.' The left sidebar shows the navigation path: IAM > Users > Create user, with steps 1 (Specify user details), 2 (Set permissions), and 3 (Review and create). The main content area is titled 'Review and create' and includes a sub-header '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
dataops7-new-user	None	No

Permissions summary

< 1 >

Name	Type	Used as
S3-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.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Create user'. A green arrow points to the 'Previous' button.

7- Select user to create Access Key

The screenshot shows the AWS IAM console 'Users' page. A blue notification banner at the top states 'Introducing the new Users list experience'. A green notification banner below it states 'User created successfully'. The left sidebar shows the navigation path: Identity and Access Management (IAM) > Users. The main content area is titled 'Users (Selected 1/4)' and includes a sub-header 'Ready to streamline human access to AWS and cloud apps?'. Below this, there is a table of users. The user 'dataops7-new-user' is selected, indicated by a blue checkmark in the first column. A green arrow points to the 'dataops7-new-user' row in the table.

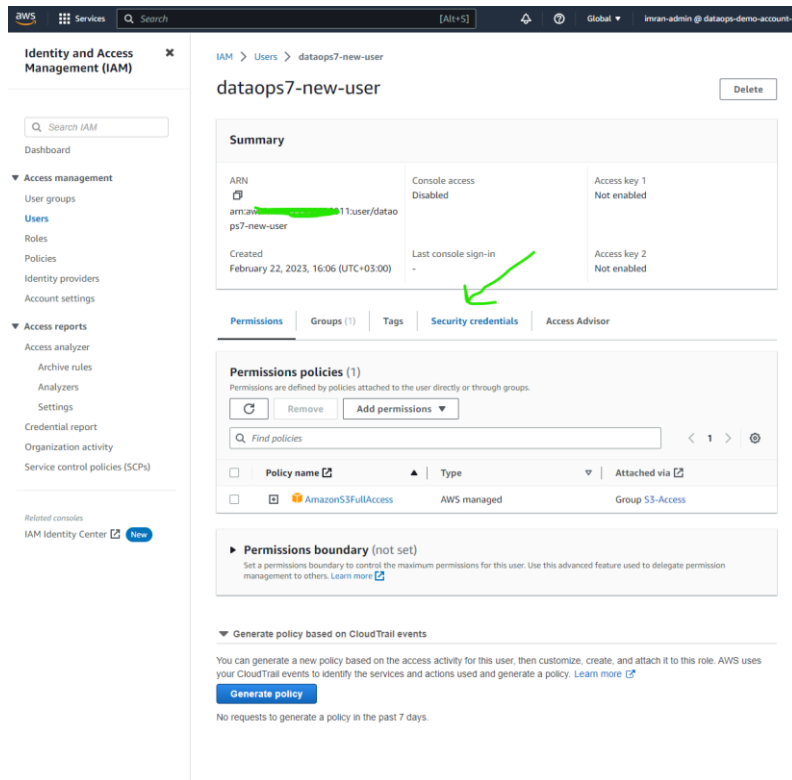
Users (Selected 1/4)

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](#)

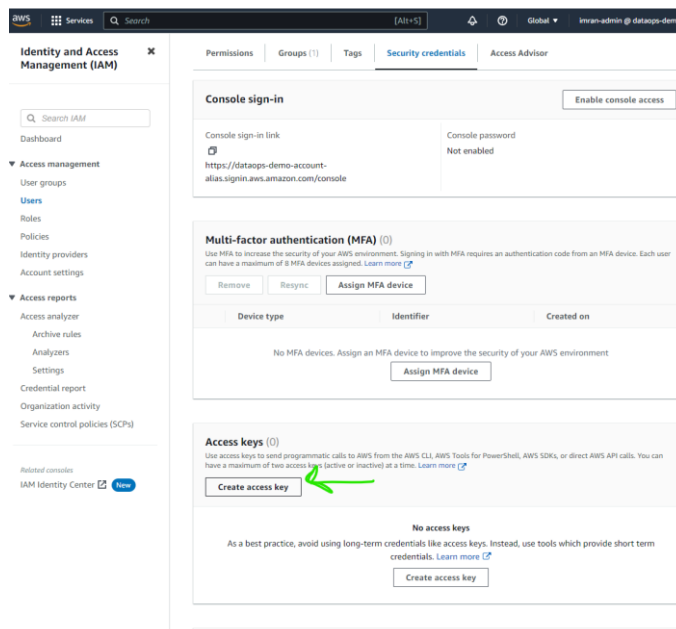
	User name	Groups	Last activity	MFA	Password
<input type="checkbox"/>	dataops-iam-user	dataops	Never	None	✓ Yesterd
<input checked="" type="checkbox"/>	dataops7-new-user	S3-Access	Never	None	None
<input type="checkbox"/>	imran-admin	admin	✓ 33 minutes ago	Virtual	✓ Yesterd
<input type="checkbox"/>	new-iam-user	s3	Never	None	None

8- Click Security Credentials



The screenshot shows the AWS IAM console interface. On the left is the navigation menu with sections for Identity and Access Management (IAM), Access management, Access reports, and Related consoles. The main content area is titled 'dataops7-new-user' and has a 'Delete' button. Below the title is a 'Summary' section with a table showing user details: ARN, Console access (Disabled), Access key 1 (Not enabled), Created date, and Last console sign-in (indicated by a dash and a green arrow). Below the summary are tabs for Permissions, Groups (1), Tags, Security credentials (selected), and Access Advisor. The 'Security credentials' tab shows 'Permissions policies (1)' with a table listing 'AmazonS3FullAccess' as an AWS managed policy. Below this is a 'Permissions boundary (not set)' section and a 'Generate policy based on CloudTrail events' section with a 'Generate policy' button.

9- Click Create Access Key



The screenshot shows the AWS IAM console interface, specifically the 'Security credentials' tab for the user 'dataops7-new-user'. The 'Console sign-in' section shows the console sign-in link and password status. The 'Multi-factor authentication (MFA)' section shows options to remove, resync, or assign an MFA device. The 'Access keys (0)' section, highlighted with a green arrow, shows a 'Create access key' button. Below this is a 'No access keys' section with a 'Create access key' button.

10- Select your use case

The screenshot shows the AWS IAM console interface. The breadcrumb trail is IAM > Users > dataops7-new-user > Create access key. On the left, a sidebar lists the steps: Step 1: Access key best practices & alternatives (selected), Step 2 - optional: Set description tag, and Step 3: Retrieve access keys. The main content area is titled 'Access key best practices & alternatives' and includes a warning: 'Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.' Below this, there are five radio button options: 'Command Line Interface (CLI)' (selected), 'Local code', 'Application running on an AWS compute service', 'Third-party service', and 'Application running outside AWS'. Each option has a brief description. At the bottom, there is a section for 'Alternatives recommended' with links to 'AWS CloudShell' and 'AWS CLI V2'. A checkbox at the bottom states 'I understand the above recommendation and want to proceed to create an access key.' The 'Next' button is highlighted in orange.

11- Click Create Access key and Done

Download your csv file and keep it safe file

The screenshot shows the 'Retrieve access keys' step of the 'Create access key' process. A green banner at the top states 'Access key created' and 'This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.' The breadcrumb trail is IAM > Users > dataops7-new-user > Create access key. The sidebar shows Step 3: Retrieve access keys as the active step. The main content area is titled 'Retrieve access keys' and contains a section for 'Access key' with a warning: 'If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.' Below this, there are two tabs: 'Access key' and 'Secret access key'. The 'Secret access key' tab is active, showing a text input field with a green highlight and a 'Show' button. Below the tabs, there is a section for 'Access key best practices' with a list of recommendations: 'Never store your access key in plain text, in a code repository, or in code.', 'Disable or delete access key when no longer needed.', 'Enable least-privilege permissions.', and 'Rotate access keys regularly.' A link to 'Best practices for managing AWS access keys' is provided. At the bottom, there are two buttons: 'Download .csv file' and 'Done' (highlighted in orange).