

CI/CD IN-SEM LAB EXAM

2310030088
M.V.Sita Rama Raju

To create an IAM user with EC2 access through a directly attached policy and S3 access through an IAM group

The screenshot shows the IAM Dashboard. On the left, the navigation pane includes 'Identity and Access Management (IAM)', 'Access management' (with 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Root access management'), and 'Access reports' (with 'Access Analyzer', 'Resource analysis', 'Unused access', and 'Analyzer settings'). A central panel displays 'Security recommendations' with two items: 'Root user has MFA' and 'Root user has no active access keys'. Below this is the 'IAM resources' section, which shows 1 User group, 2 Users, 2 Roles, 0 Policies, and 0 Identity providers. To the right, there's an 'AWS Account' summary with the account ID (849681699618), account alias ('Create'), and sign-in URL (<https://849681699618.signin.aws.amazon.com/>). A 'Quick Links' section provides links to 'My security credentials' and other management options.

1. Create the IAM User:

- Navigate to the IAM service in the AWS Management Console.
- Choose Users in the navigation pane, then click Create user.
- Provide a User name.

The screenshot shows the 'Specify user details' step of the IAM User creation wizard. On the left, a sidebar lists steps: Step 1 (selected), Step 2, Step 3, Step 4, and Retrieve password. The main area is titled 'Specify user details' and contains a 'User details' section with a 'User name' field set to 'exam_user'. Below it is a note about character restrictions and a checked checkbox for 'Provide user access to the AWS Management Console - optional'. A large blue-bordered box highlights the 'Are you providing console access to a person?' section, which contains two radio button options: 'Specify a user in Identity Center - Recommended' (unchecked) and 'I want to create an IAM user' (checked). The 'I want to create an IAM user' option includes a note about creating IAM users for programmatic access. At the bottom, there's a 'Console password' section with an 'Autogenerated password' radio button and a note about viewing the password after creation.

2. Attach the EC2 Policy Directly to the User:

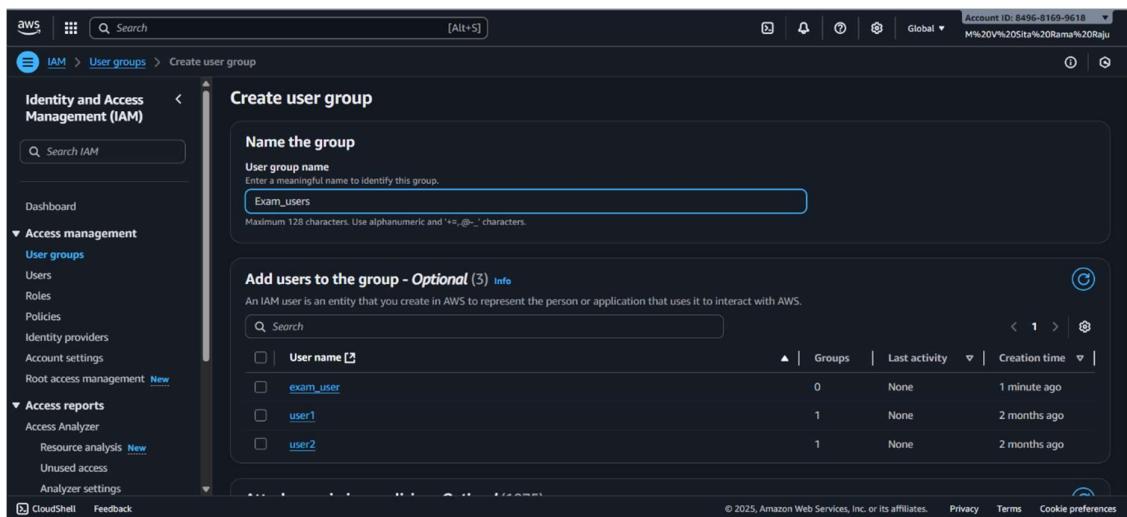
- On the "Set permissions" page, choose Attach policies directly.
- Search for and select a suitable AWS managed policy for EC2 access, such as AmazonEC2FullAccess
- create the user.

The screenshot shows the AWS IAM 'Create user' wizard at the 'Set permissions' step. On the left, a vertical navigation bar lists steps: Step 1 (Specify user details), Step 2 (Set permissions - highlighted in blue), Step 3 (Review and create), and Step 4 (Retrieve password). The main area is titled 'Set permissions' and contains three options: 'Add user to group', 'Copy permissions', and 'Attach policies directly'. The 'Attach policies directly' option is selected and highlighted with a blue border. Below this is a list of 'Permissions policies (1/1393)' with a search bar and filter. The 'AmazonEC2FullAccess' policy is selected and highlighted with a blue border. At the bottom, there are buttons for 'Create policy' and 'Next Step'.

The screenshot shows the AWS IAM 'Create user' wizard at the 'Retrieve password' step. The vertical navigation bar on the left shows steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password - highlighted in blue). The main area is titled 'Retrieve password' and contains a 'Console sign-in details' section. It shows a 'Console sign-in URL' (https://849681699618.signin.aws.amazon.com/console) and fields for 'User name' (exam_user) and 'Console password' (a masked password). There is also a 'Email sign-in instructions' button. At the bottom, there are buttons for 'Cancel', 'Download .csv file', and 'Return to users list'.

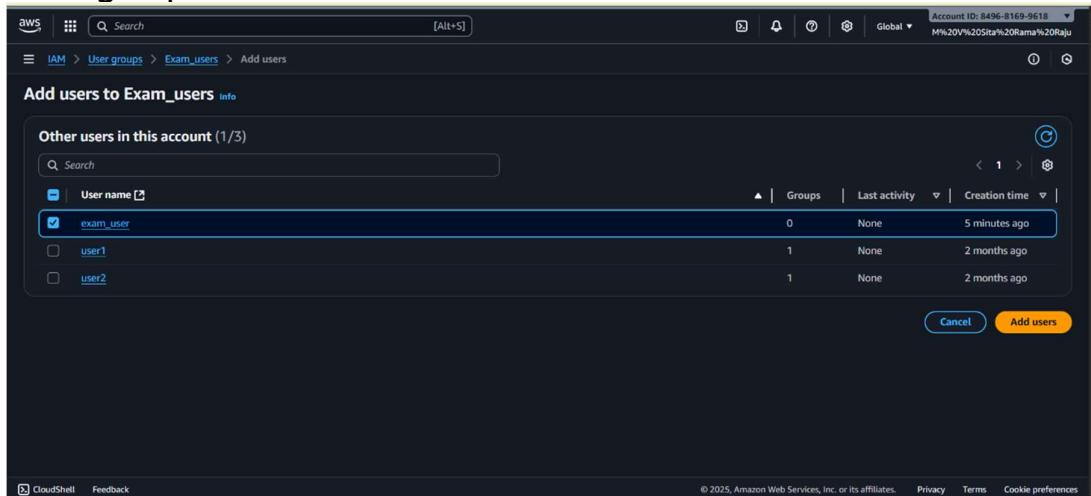
3. Create the IAM Group for S3 Access:

- After creating the user, navigate back to the IAM service.
- Choose User groups in the navigation pane, then click Create group.
- Provide a User group name
- Search for and select a suitable AWS managed policy for S3 access, such as AmazonS3FullAccess
- Review the group details and create the group.



4. Add the User to the S3 Access Group:

- Navigate back to the created IAM group (S3-Access-Group).
- Under the Users tab, click Add users.
- Select the ec2-s3-user you created earlier and add them to this group.



The screenshot shows the AWS IAM User Groups page. The left sidebar is titled "Identity and Access Management (IAM)" and includes sections for "Access management" (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management), "Access reports" (Access Analyzer, Resource analysis, Unused access, Analyzer settings), and "CloudShell" and "Feedback". The main content area is titled "Exam_users" and shows a summary: "1 user added to this group." The user group name is "Exam_users", creation time is "October 09, 2025, 13:00 (UTC+05:30)", and the ARN is "arn:aws:iam::849681699618:group/Exam_users". Below the summary, there are tabs for "Users" (selected), "Permissions", and "Access Advisor". The "Users in this group" section shows one user named "exam_user".

Now, the ec2-s3-user has:

- EC2 permissions directly attached through the chosen EC2 policy.
- S3 permissions inherited from the S3-Access-Group they are a member of.