

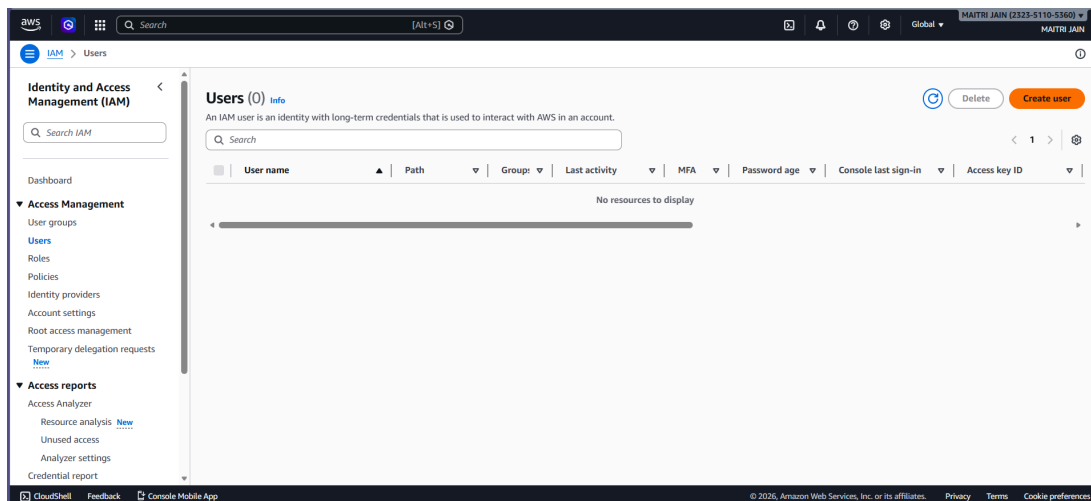
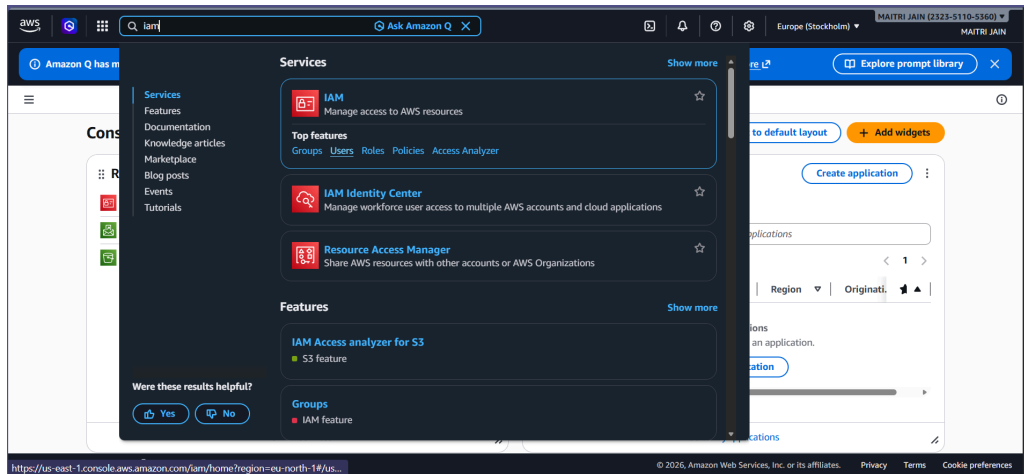
Experiment 3 — Create IAM User with S3 Access

Aim:

To create an IAM user and grant S3 full access.

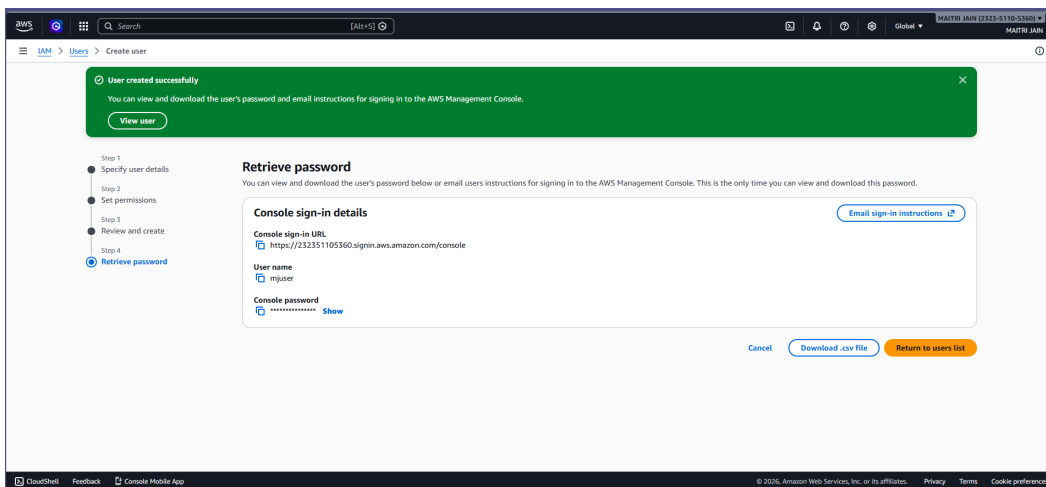
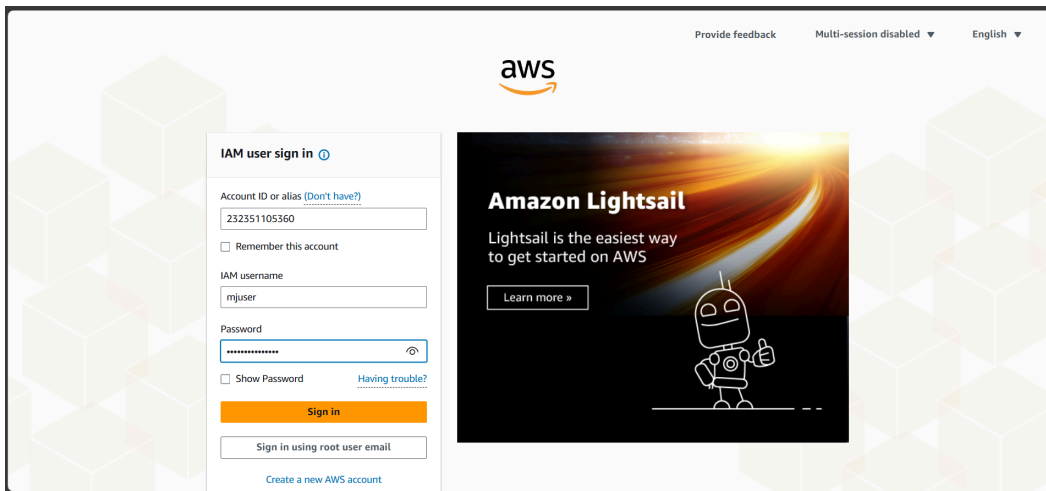
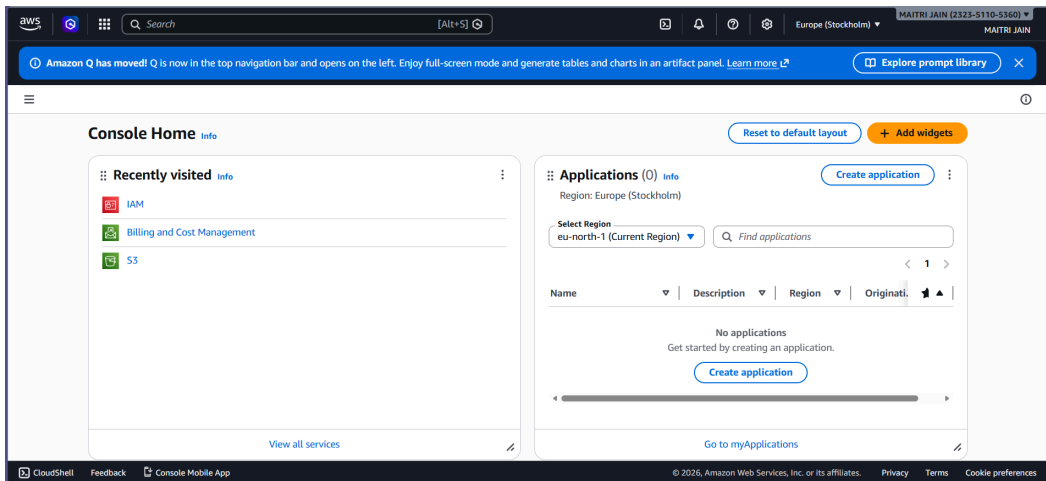
Procedure:

1. IAM → Users → Create User.



2. Enter username.
3. Enable console access.

5. Create user.

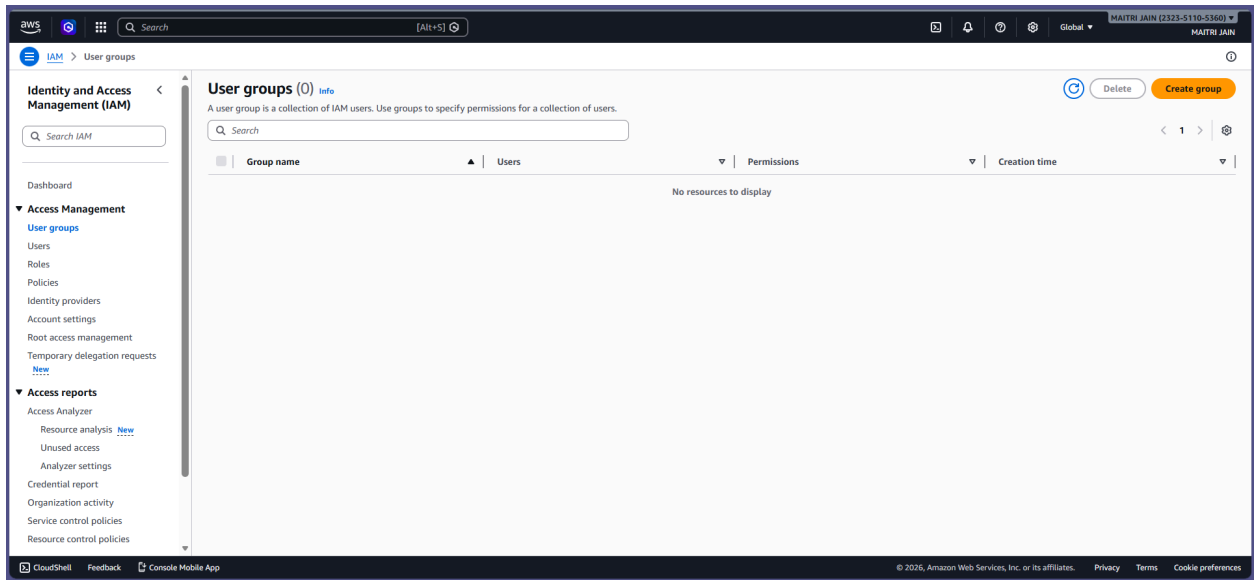


Result:

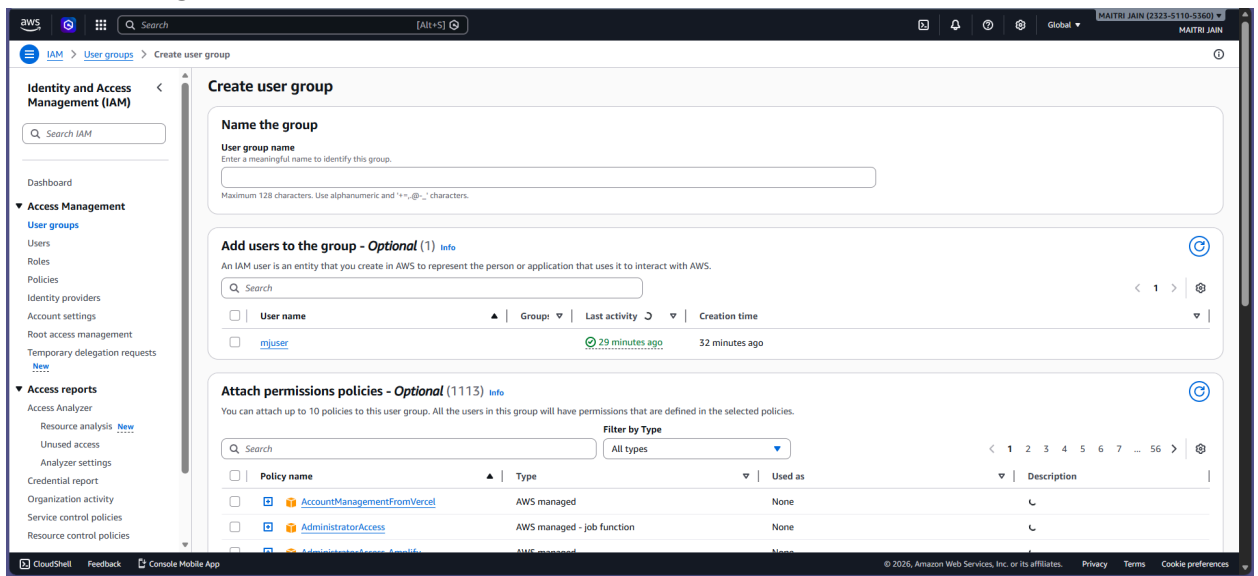
IAM user created with S3 permissions.

IAM users allow controlled access instead of root login.

6. Go to **IAM** → **User groups**.



7. Click **Create group**.



8. Enter group name **S3FullAccessGroup**.

9. Attach **AmazonS3FullAccess** policy.

The screenshot shows the AWS IAM console's 'Create user group' page. On the left, the 'Identity and Access Management (IAM)' sidebar is visible. The main content area displays a list of policies filtered by 's3', showing 14 matches. The 'AmazonS3FullAccess' policy is selected, highlighted in blue. The table lists the following policies:

Policy name	Type	Used as	Description
<input type="checkbox"/> AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to manage S3 settings...
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	Permissions policy (1)	Provides full access to all buckets via t...
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	None	Provides AWS Lambda functions perm...
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	None	Provides full access to Amazon S3 on ...
<input type="checkbox"/> AmazonS3OutpostsReadOnlyAccess	AWS managed	None	Provides read only access to Amazon S...
<input type="checkbox"/> AmazonS3ReadOnlyAccess	AWS managed	None	Provides read only access to all bucket...
<input type="checkbox"/> AmazonS3TablesFullAccess	AWS managed	None	Provides full access to all S3 table buc...
<input type="checkbox"/> AmazonS3TablesLakeFormationServiceRole	AWS managed	None	This managed policy grants AWS Lake ...
<input type="checkbox"/> AmazonS3TablesReadOnlyAccess	AWS managed	None	Provides read only access to all S3 tabl...
<input type="checkbox"/> AWSBackupServiceRolePolicyForS3Backup	AWS managed	None	Policy containing permissions necessar...
<input type="checkbox"/> AWSBackupServiceRolePolicyForS3Restore	AWS managed	None	Policy containing permissions necessar...
<input type="checkbox"/> AWSQuickSetupSSMDeploymentS3BucketR...	AWS managed	None	This policy grants permissions for listi...
<input type="checkbox"/> QuickSightAccessForS3StorageManagemen...	AWS managed	None	Policy used by QuickSight team to acc...
<input type="checkbox"/> S3UnlockBucketPolicy	AWS managed	None	Provides access required to unlock a S...

Buttons at the bottom right: 'Cancel' and 'Create user group'.

The screenshot shows the 'Create user group' page in the AWS IAM console. The 'Name the group' section has 'S3FullAccessGroup' entered as the 'User group name'. The 'Add users to the group - Optional (1/1)' section shows a search for 'mjuser' and a table with one user added:

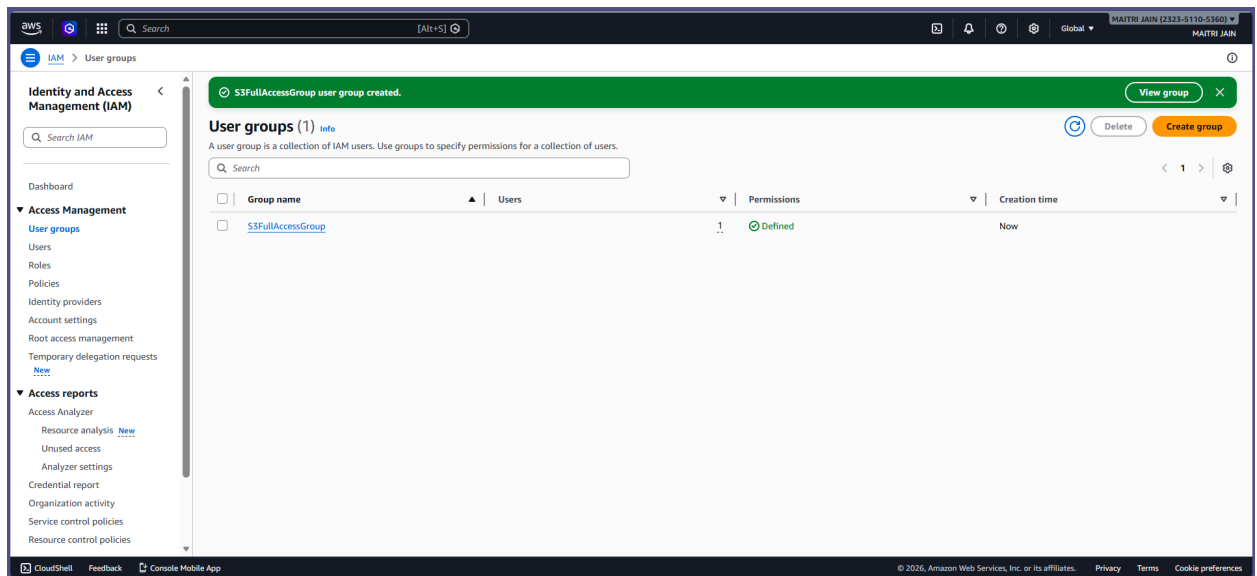
User name	Group	Last activity	Creation time
<input checked="" type="checkbox"/> mjuser	0	30 minutes ago	33 minutes ago

The 'Attach permissions policies - Optional (1113)' section is also visible, showing a search bar and a table of policies to attach. The table lists the following policies:

Policy name	Type	Used as	Description
<input type="checkbox"/> AccountManagementFromVercel	AWS managed	None	For use with accounts created through...
<input type="checkbox"/> AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
<input type="checkbox"/> AdministratorAccessFromVercel	AWS managed	None	For use with accounts created through...

Buttons at the bottom right: 'Cancel' and 'Create user group'.

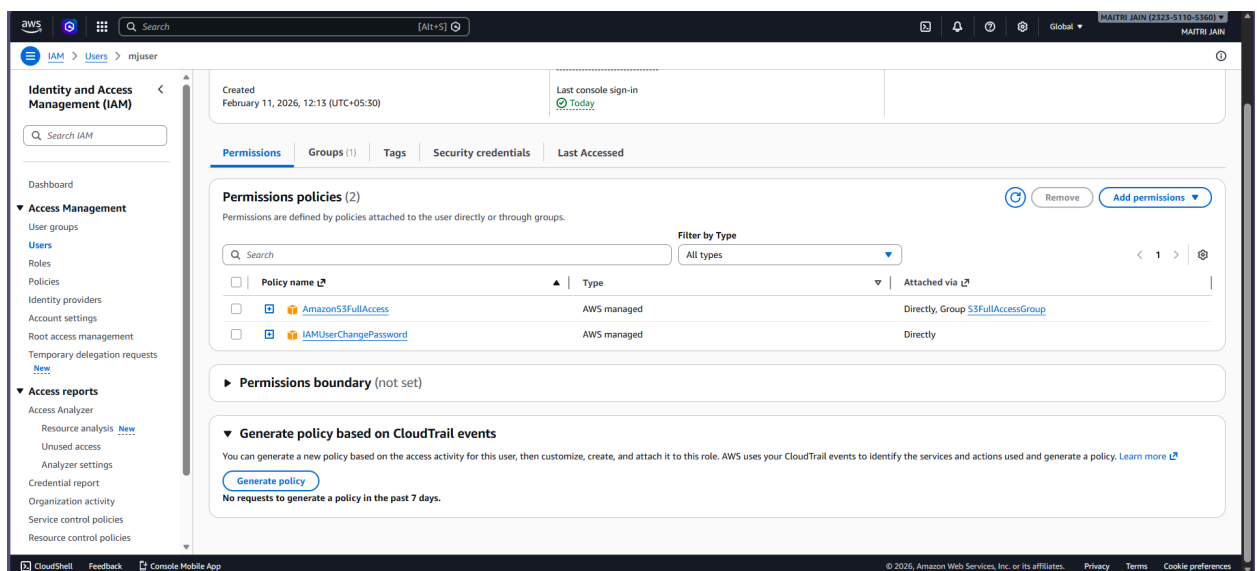
10. Create the group.



11. Open **IAM** → **Users** → (your username).

12. Click **Add user to group**.

13. Select **S3FullAccessGroup**.



14. Click **Add**.

Result: IAM user and user group were successfully created, and S3 Full Access permission was assigned to the user through the group.

Conclusion: IAM groups help manage permissions efficiently and securely by assigning policies to groups instead of individual users.