

MODULE 1

Submitted by – KINJARAPU RAJASEKHAR

Date Of Submission-21/08/2024

Date of Resubmission-

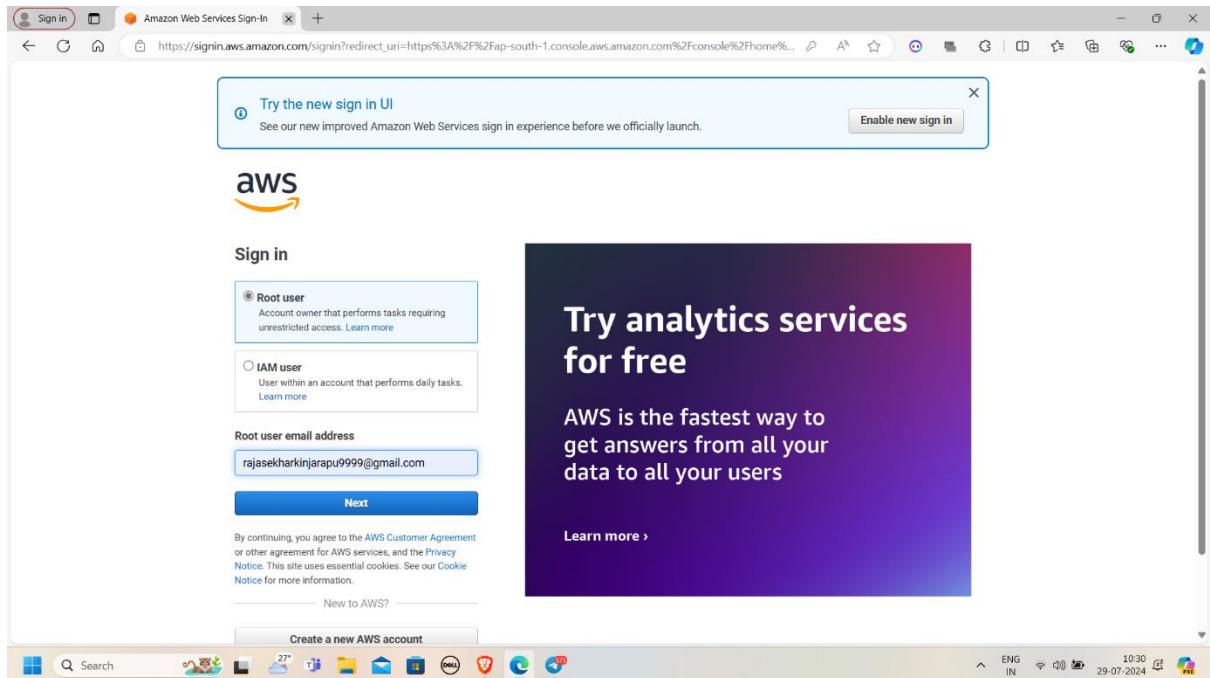
Batch no-SA246007

Submitted to- Vikul Mentor

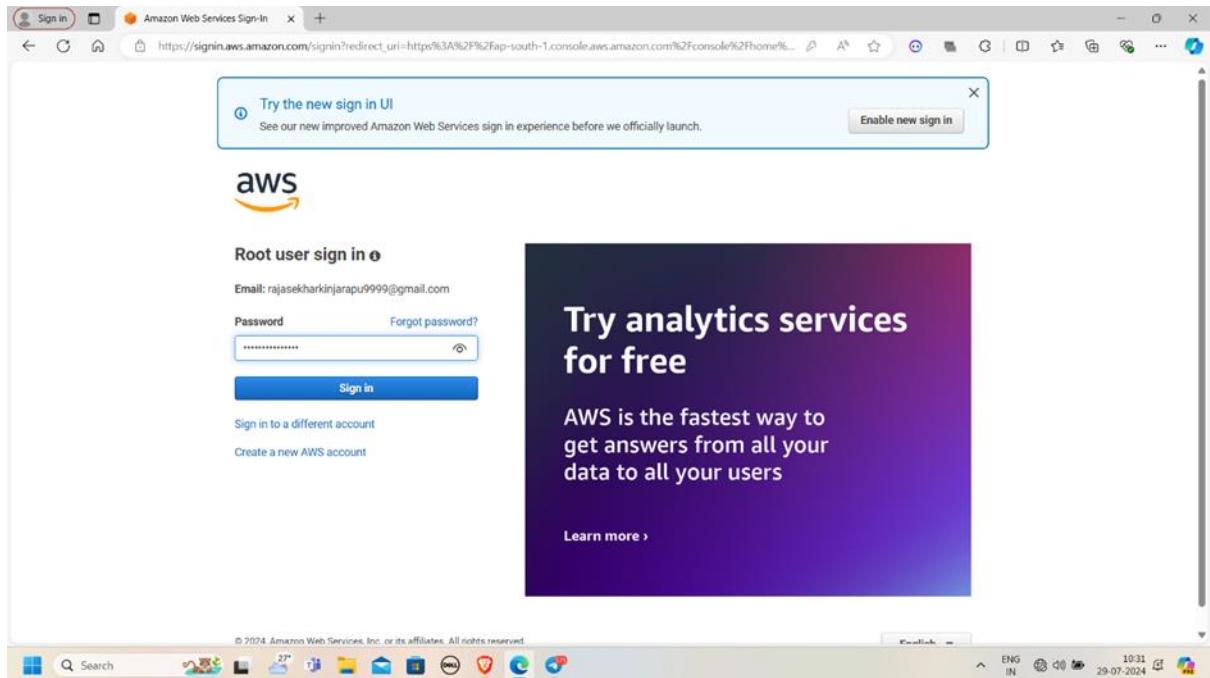
2. L2 - Login to AWS Console and Create IAM User Role, and Group

TO CREATE IAM USER

Step 1: login to aws console with root user



Step 2 : Enter the password of your root account ,then click on signin.



Step 3 : go to IAM service

The screenshot shows the AWS Cloud Services dashboard. On the left sidebar, under 'Recently visited', the 'IAM' icon is highlighted with a red box. Other services listed include Billing and Cost Management, EC2, Service Quotas, CloudShell, AWS Health Dashboard, AWS Organizations, DynamoDB, S3, and Lightsail. The main content area displays sections for Applications (0), AWS Health (Info), and Cost and usage. The IAM section is not explicitly visible in this view.

Step 4: go to IAM dashboard and click on users to create user .

The screenshot shows the IAM dashboard. The left sidebar has 'Identity and Access Management (IAM)' selected. Under 'Access management', the 'Users' icon is highlighted with a red box. Other options include User groups, Roles, Policies, Identity providers, and Account settings. The main content area shows 'Root user has no active access keys' and 'IAM resources' (0 users, 6 roles, 0 policies, 0 identity providers). A 'What's new' section lists recent updates. To the right, there are 'Quick Links' for 'My security credentials' and 'Tools' for 'Policy simulator'. The URL in the address bar is https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#users.

Step5 : click on create user

The screenshot shows the AWS IAM Users page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' and sections for 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings), 'Access reports' (Access Analyzer, External access, Unused access, Analyzer settings, Credential report), and 'CloudShell' and 'Feedback' buttons. The main area has a heading 'Ready to streamline human access to AWS and cloud apps?' with a 'Dismiss' button and a 'Manage workforce users' link. Below it, a message says 'Identity Center is enabled. We recommend managing workforce users' access to AWS accounts and cloud applications in Identity Center.' with 'Learn more' and 'Watch how it works' links. The 'Users' section shows two entries: 'durga' (Last activity: 12 days ago, MFA: -, Password age: 25 days, Created: July 31, 2024, 17:42) and 'rajasekhar' (Last activity: 3 days ago, MFA: -, Password age: 167 days, Created: August 08, 2024, 17:42). There are 'Search', 'Delete', and 'Create user' buttons at the top of the user list. The bottom of the page includes copyright information (© 2024, Amazon Web Services, Inc. or its affiliates.) and links for Privacy, Terms, and Cookie preferences. The system status bar at the bottom shows ENG IN, 18:09, 12-08-2024, and a battery icon.

Step 6: give the user name

The screenshot shows the 'Specify user details' step in the AWS IAM User creation wizard. The left sidebar shows 'Step 1 Specify user details', 'Step 2 Set permissions', and 'Step 3 Review and create'. The main area has a heading 'Specify user details' and a 'User details' section. It contains a 'User name' input field with 'demouser' typed in, a note about valid characters (A-Z, a-z, 0-9, + = . @ _ - (hyphen)), and a checkbox for 'Provide user access to the AWS Management Console - optional'. A note below the checkbox states: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keypairs, you can generate them after you create this IAM user.' There are 'Cancel' and 'Next' buttons at the bottom right. The bottom of the page includes copyright information (© 2024, Amazon Web Services, Inc. or its affiliates.) and links for Privacy, Terms, and Cookie preferences. The system status bar at the bottom shows ENG IN, 18:09, 12-08-2024, and a battery icon.

Step 7: click on block then it shows to create console password and then click on next.

The screenshot shows the 'User details' section of the IAM user creation wizard. The 'User name' field contains 'demouser'. A checked checkbox says 'Provide user access to the AWS Management Console - optional'. Below it, an 'Autogenerated password' radio button is selected, with a note that the password can be viewed after creation. An unselected 'Custom password' radio button has a placeholder for entering a custom password. A note below the password fields specifies password requirements: at least 8 characters, including uppercase letters, lowercase letters, numbers, and symbols. A checked checkbox says 'Users must create a new password at next sign-in - Recommended'. A callout box at the bottom right provides information about generating programmatic access keys.

Step 8 : after it goes permissions options click on attach policies directly or other option based on your requirement

The screenshot shows the 'Permissions options' section of the IAM user creation wizard. It includes three options: 'Add user to group', 'Copy permissions', and 'Attach policies directly'. The 'Attach policies directly' option is selected. Below this, the 'Permissions policies' section lists 1224 policies, with a search bar and a 'Create policy' button. The policies listed include 'AccessAnalyzerServiceRolePolicy', 'AdministratorAccess', 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSElasticBe...', 'AlexaForBusinessDeviceSetup', and 'AlexaForBusinessFullAccess'. The table also includes columns for 'Type' (AWS managed or AWS managed - job function) and 'Attached entities'.

Step 9: give access to the user based on requirement. Here I am giving administrative full access.

The screenshot shows the AWS IAM 'Create user' wizard at Step 9. The 'Permissions policies' section is displayed, listing various AWS managed policies. A search bar at the top left shows 'ad'. A table below lists policies under 'Policy name' and 'Type'. One policy, 'AdministratorAccess', is selected and highlighted with a blue border. The table includes columns for 'Policy name', 'Type', and 'Attached entities'. The 'Attached entities' column shows values ranging from 0 to 2. The bottom right of the table area contains copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.' and links for 'Privacy', 'Terms', and 'Cookie preferences'.

Step 10: then click on next

The screenshot shows the AWS IAM 'Create user' wizard at Step 10. The 'Set permissions boundary - optional' section is visible, containing a list of AWS managed policies. The policies listed are: AmazonChimeReadOnly, AmazonCloudDirectoryReadOnlyAccess, AmazonCloudWatchEvidentlyReadOnly, AmazonCloudWatchRUMReadOnly, AmazonCodeCatalystReadOnlyAccess, AmazonCodeGuruProfilerReadOnly, AmazonCodeGuruReviewerReadOnly, AmazonCognitoReadOnly, AmazonConnectReadOnlyAccess, AmazonDevOpsGuruReadOnlyAccess, AmazonDocDBElasticReadOnlyAccess, and AmazonDocDBReadOnlyAccess. Below this list is a note: '▶ Set permissions boundary - optional'. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons. The bottom right corner of the screen shows system status: ENG IN 18:10 12-08-2024.

Step 11 : then click on create user

User details

User name demouser	Console password type Autogenerated	Require password reset Yes
-----------------------	--	-------------------------------

Permissions summary

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Create user

Step 12: Here the user created successfully

User created successfully

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

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Retrieve password

Console sign-in details

Console sign-in URL https://21112555582.sigin.aws.amazon.com/console	Email sign-in instructions
User name demouser	
Console password ***** Show	

Cancel Download .csv file Return to users list

Step 13: here the credentials of user

The screenshot shows the 'Create user' process in the AWS Management Console. The user has successfully created a new user named 'demouser'. The 'Console sign-in details' section displays the following information:

- Console sign-in URL: <https://21112555582.sigin.aws.amazon.com/console>
- User name: demouser
- Console password: a5rzE1@# (with a 'Hide' link)

At the bottom right of the page are buttons for 'Cancel', 'Download .csv file', and 'Return to users list'.

Step 14: click on users you can see the users list

The screenshot shows the 'Users' page in the AWS Management Console under the 'Identity and Access Management (IAM)' service. The page displays three IAM users: 'demouser', 'durga', and 'rajasekhar'. The table includes columns for User name, Path, Group, Last activity, MFA, Password age, and Console last sign-in.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
demouser	/	0	-	-	-	-
durga	/	0	12 days ago	-	25 days	July 31, 2024, 17:45
rajasekhar	/	0	3 days ago	-	167 days	August 08, 2024, 17:45

TO CREATE IAM ROLE:

Step 1: go to iam dashboard click on roles and then click on create role

The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. The main area displays a table titled 'Roles (6) Info' with columns for 'Role name', 'Trusted entities', and 'Last activity'. The roles listed are: aws_s3_instance (AWS Service: ec2), AWSServiceRoleForElasticLoadBalancing (AWS Service: elasticloadbalancing), AWSServiceRoleForOrganizations (AWS Service: organizations), AWSServiceRoleForRDS (AWS Service: rds), AWSServiceRoleForSupport (AWS Service: support), and AWSServiceRoleForTrustedAdvisor (AWS Service: trustedadvisor). Below the table, there's a section titled 'Roles Anywhere' with a 'Manage' button.

Step 2: it shows selected trusted entity then click on aws service

The screenshot shows the 'Select trusted entity' step in the IAM Role creation wizard. The left sidebar shows 'Step 1 Select trusted entity' and 'Step 2 Add permissions'. The main area has a 'Trusted entity type' section with four options: 'AWS service' (selected), 'AWS account', 'SAML 2.0 federation', and 'Custom trust policy'. Below this is a 'Use case' section with a note about allowing actions in EC2, Lambda, or others. A 'Service or use case' dropdown is present. At the bottom right are 'Cancel' and 'Next' buttons.

Step 3: give usecase ,here I am giving ec2 and click on next

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

EC2
Allows EC2 instances to call AWS services on your behalf.

EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.

Cancel Next

Step 4:then set the permissions ,here I am giving s3 full acess.

Create role | IAM | Global AWS Cloud (1).pdf https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntityType=AWS_SERVICE&select... Gmail YouTube Dell ContentKeeper Aut... WhatsApp Best Free Websites... Revolutionizing the... Watch Anaconda F... CC - Google Drive (19) YouTube www.jiocinema.com Prime Video: Ranga... Services Search [Alt+S] Global KINJARAPU%20RAJASEKHAR

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 18:11 12-08-2024

Step 2 Add permissions Step 3 Name, review, and create

Permissions policies (1/946) Info

Choose one or more policies to attach to your new role.

Filter by Type

s3 All types 9 matches

Policy name	Type	Description
AmazonDMSRedshiftS3Role	AWS managed	Provides access to manage S3 settings...
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...
AmazonS3ObjectLambdaExecutionRole	AWS managed	Provides AWS Lambda functions permis...
AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on ...
AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S...
AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all bucket...
AWSBackupServiceRolePolicyForS3Bar...	AWS managed	Policy containing permissions necessar...
AWSBackupServiceRolePolicyForS3Res...	AWS managed	Policy containing permissions necessar...
QuickSightAccessForS3StorageManag...	AWS managed	Policy used by QuickSight team to acc...

Set permissions boundary - optional

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 18:12 12-08-2024

Step 5: click on next

Filter by Type
All types 9 matches

Policy name	Type	Description
AmazonDMSRedshiftS3Role	AWS managed	Provides access to manage S3 settings...
AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...
AmazonS3ObjectLambdaExecutionRole	AWS managed	Provides AWS Lambda functions permis...
AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on ...
AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S...
AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all bucket...
AWSBackupServiceRolePolicyForS3Backup	AWS managed	Policy containing permissions necessar...
AWSBackupServiceRolePolicyForS3Restore	AWS managed	Policy containing permissions necessar...
QuickSightAccessForS3StorageManager	AWS managed	Policy used by QuickSight team to acc...

▶ Set permissions boundary - *optional*

Cancel Previous Next

Step 6: give the rolename

Role name
Enter a meaningful name to identify this role.
s3role

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.

Step 1: Select trusted entities

Trust policy

```
1- [ { "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "sts:AssumeRole" ], "Principal": [ "Service": [ "ec2.amazonaws.com" ] ] } ] }
```

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 18:12 12-08-2024

Step 7: then click on create role

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

Step 3: Add tags

Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create role

Step8: here the role successfully created .

Identity and Access Management (IAM)

Roles (7) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
aws_s3_instance	AWS Service: ec2	4 days ago
AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing	126 days ago
AWSServiceRoleForOrganizations	AWS Service: organizations	-
AWSServiceRoleForRDS	AWS Service: rds	1 hour ago
AWSServiceRoleForSupport	AWS Service: support	57 days ago
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor	-
s3role	AWS Service: ec2	-

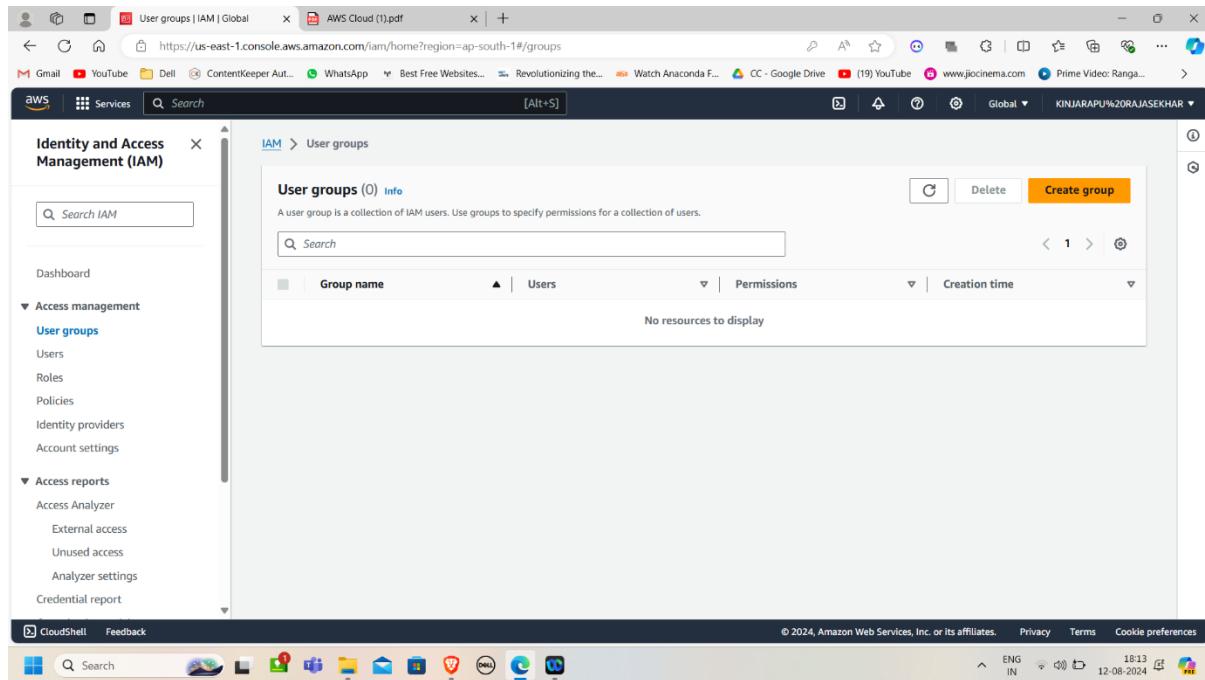
Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

View role Create role

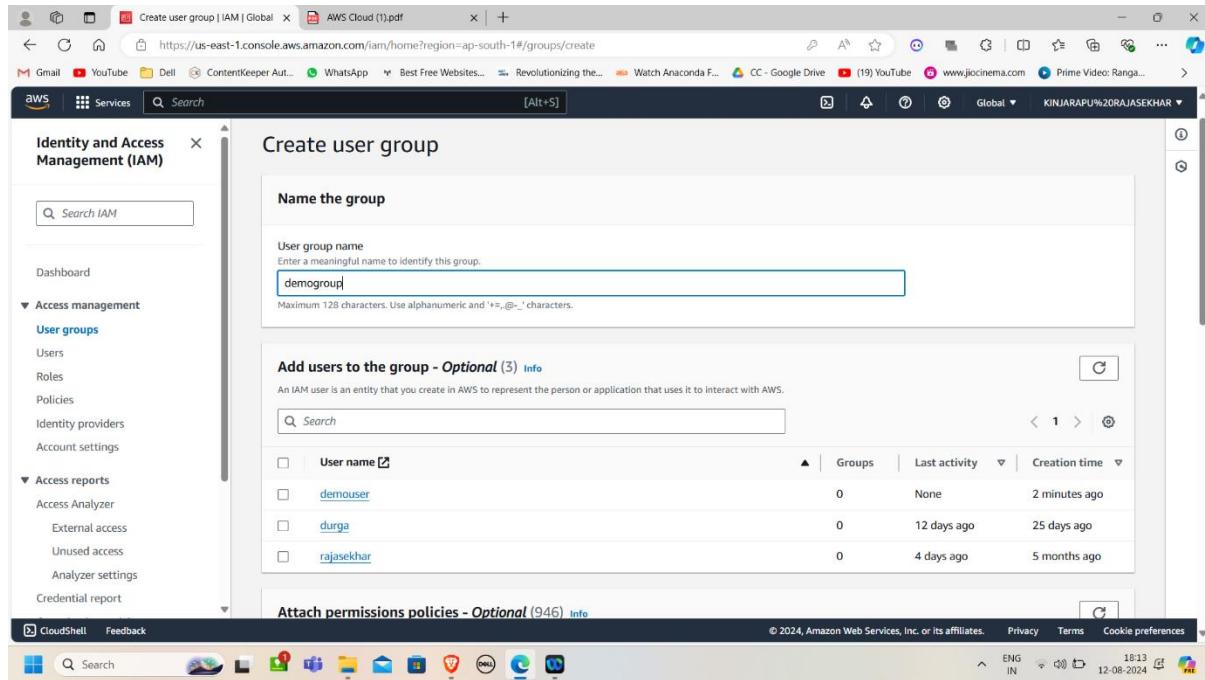
TO CREATE GROUP:

Step 1: click on groups and then click on create group



The screenshot shows the AWS IAM console with the URL <https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups>. The left sidebar is open, showing the 'User groups' section under 'Access management'. The main area displays a table titled 'User groups (0) Info' with a single row 'No resources to display'. A prominent orange 'Create group' button is located at the top right of the table area.

Step 2: give the group name



The screenshot shows the 'Create user group' page with the URL <https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/create>. The left sidebar is open, showing the 'User groups' section under 'Access management'. The main area has three sections: 'Name the group' (with 'User group name' field containing 'demogroup'), 'Add users to the group - Optional (3) Info' (listing users 'demouser', 'durga', and 'rajasekhar' with their respective activity details), and 'Attach permissions policies - Optional (946) Info' (button). The 'User group name' field has a placeholder 'Enter a meaningful name to identify this group.' and a note 'Maximum 128 characters. Use alphanumeric and '-' characters.'

Step 3: click the on user names whom you want in that group and attach policies and click on create group.

The screenshot shows the AWS IAM User Groups page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'User groups' is also selected. A search bar at the top right says 'Search [Alt+S]'. Below it, a table lists three users: 'demouser' (checked), 'durga' (unchecked), and 'rajasekhar' (checked). To the right, a section titled 'Attach permissions policies - Optional (1/946) Info' shows a table of policies. One policy, 'AmazonS3FullAccess', is checked and highlighted in blue. Other policies listed include 'AmazonDMSRedshift...', 'AmazonS3ObjectLambda...', 'AmazonS3Outposts...', and 'AmazonS3OutpostsR...'. The bottom right corner shows the date and time as '12-08-2024 18:14'.

Step 4: here the group successfully created

The screenshot shows the AWS IAM User Groups page after a group has been created. A green banner at the top says 'demogroup user group created.' Below it, the 'User groups (1) info' section shows a table with one entry: 'demogroup'. The table includes columns for 'Group name', 'Users', 'Permissions', and 'Creation time'. The 'demogroup' entry shows '2' users, 'Defined' permissions, and was created 'Now'. The bottom right corner shows the date and time as '12-08-2024 18:14'.

Step 5:click on the group name ,you can see the users in the group name

The screenshot shows the AWS IAM Groups page. On the left, a sidebar menu includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (with 'User groups' selected), 'Policies', 'Identity providers', 'Account settings', 'Access reports' (with 'Access Analyzer' selected), 'Unused access', 'Analyzer settings', and 'Credential report'. The main content area shows the 'demogroup' details. Under 'Summary', it lists 'User group name: demogroup', 'Creation time: August 12, 2024, 18:14 (UTC+05:30)', and 'ARN: arn:aws:iam::21112555582:group/demogroup'. Below this, the 'Users' tab is selected, showing two users: 'demouser' (last activity: None, 3 minutes ago) and 'rajasekhar' (last activity: 4 days ago, 5 months ago). A search bar and pagination controls are also present.