

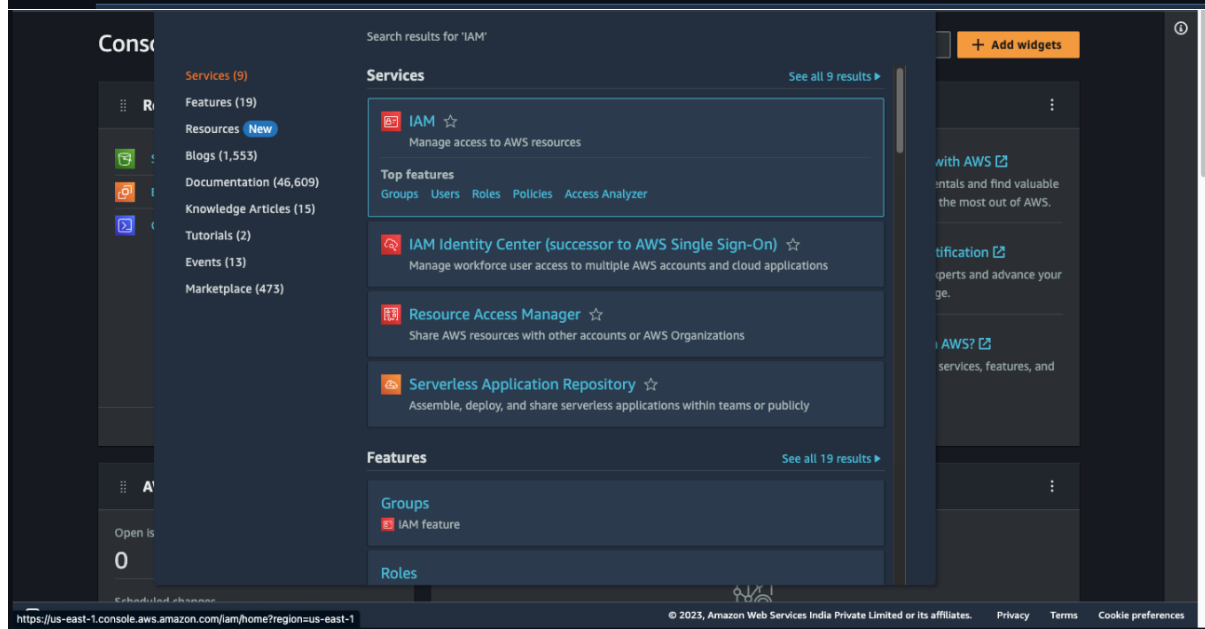
Creating IAM user & IAM admin user in AWS

Prerequisites

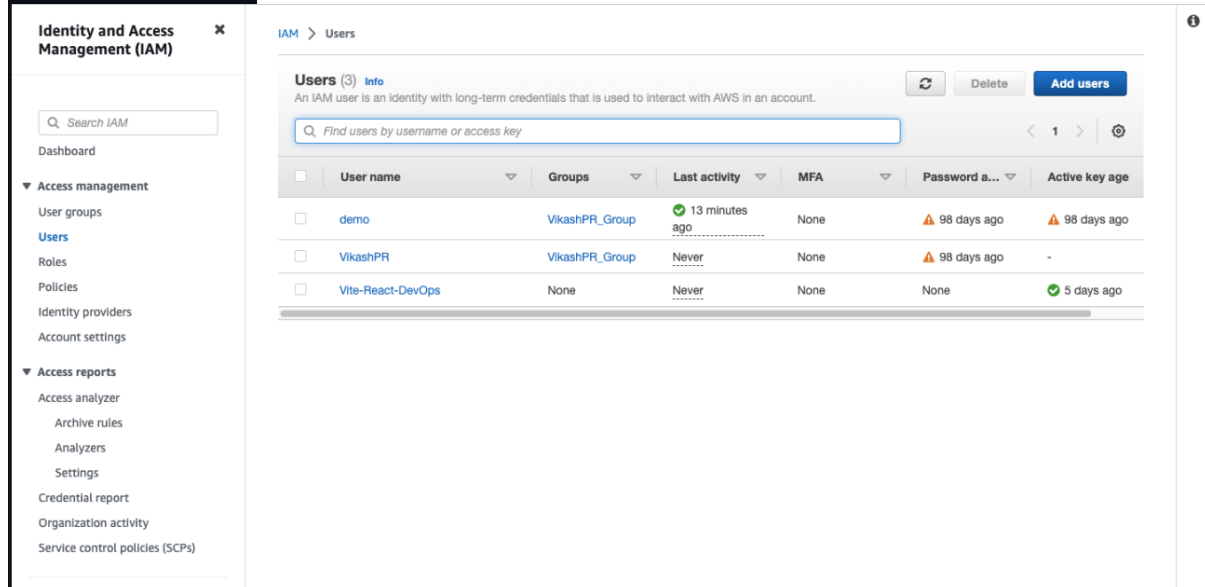
- AWS account

Procedure for Creating IAM user and IAM admin user in AWS

- Login to AWS account Link: <https://aws.amazon.com/>
- Go to IAM service



- Click on Users



- Click on Add user
- Enter user name
- Select AWS access type
- Click on attach existing policies directly
- Select AdministratorAccess policy from the list of policies

Step 1 Specify user details

Step 2 **Set permissions**

Step 3 Review and create

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.

Permissions policies (Selected 1/1089)
Choose one or more policies to attach to your new user.

Search: adm 36 matches

Policy name	Type	Attached entities
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	2
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	0
<input type="checkbox"/> AdministratorAccess-AWSElast...	AWS managed	0
<input type="checkbox"/> AmazonAPIGatewayAdministra...	AWS managed	0
<input type="checkbox"/> AmazonNimbleStudio-StudioA...	AWS managed	0
<input type="checkbox"/> AmazonSageMakerAdmin-Serv...	AWS managed	0

- Click on Next: Tags
- Click on Next: Review
- Click on Create user

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

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 (4) Info

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 age	Active key age
<input type="checkbox"/> demo	VikashPR_Group	24 minutes ago	None	98 days ago	98 days ago
<input type="checkbox"/> VikashPR	VikashPR_Group	Never	None	98 days ago	-
<input type="checkbox"/> VikashPR-Admin	None	Never	None	None	-
<input type="checkbox"/> Vite-React-DevOps	None	Never	None	None	5 days ago

- The user is created successfully with admin access

Q Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Summary

ARN
am:aws:iam::447193178734:user/VikashPR-Admin

Console access
Disabled

Access key 1
Not enabled

Created
May 18, 2023, 21:35 (UTC+05:30)

Last console sign-in
-

Access key 2
Not enabled

Permissions

Groups

Tags

Security credentials

Access Advisor

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Q Search

All types

< 1 > ⚙

☐

Policy name

▲

Type

▼

Attached via

☐

AdministratorAccess

AWS managed - job function

Directly