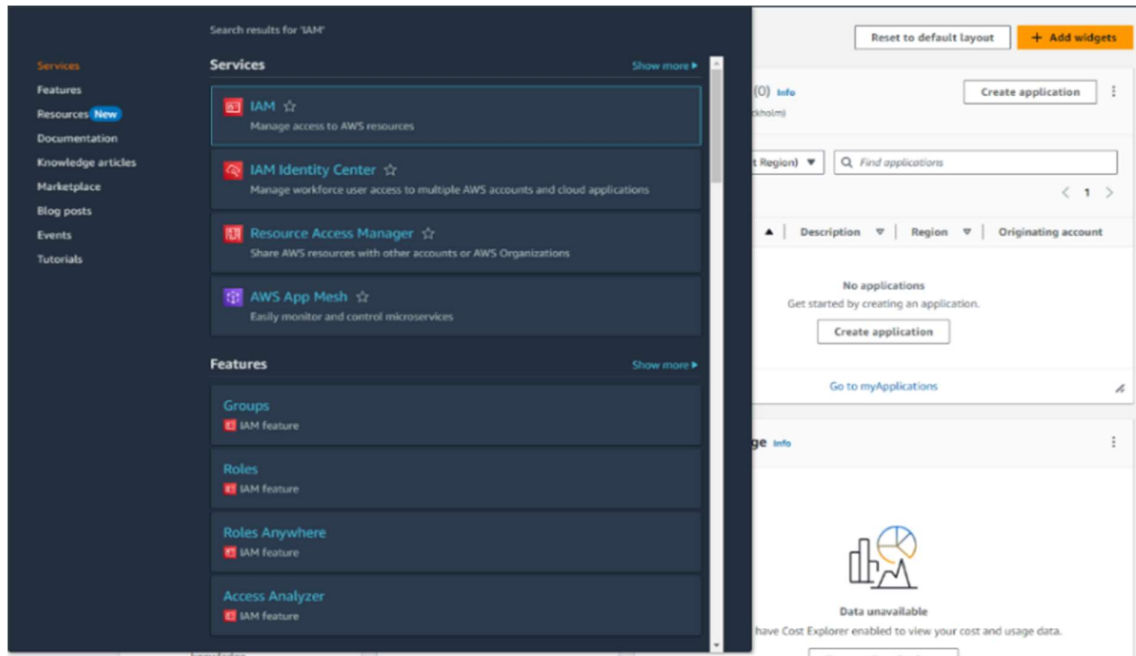
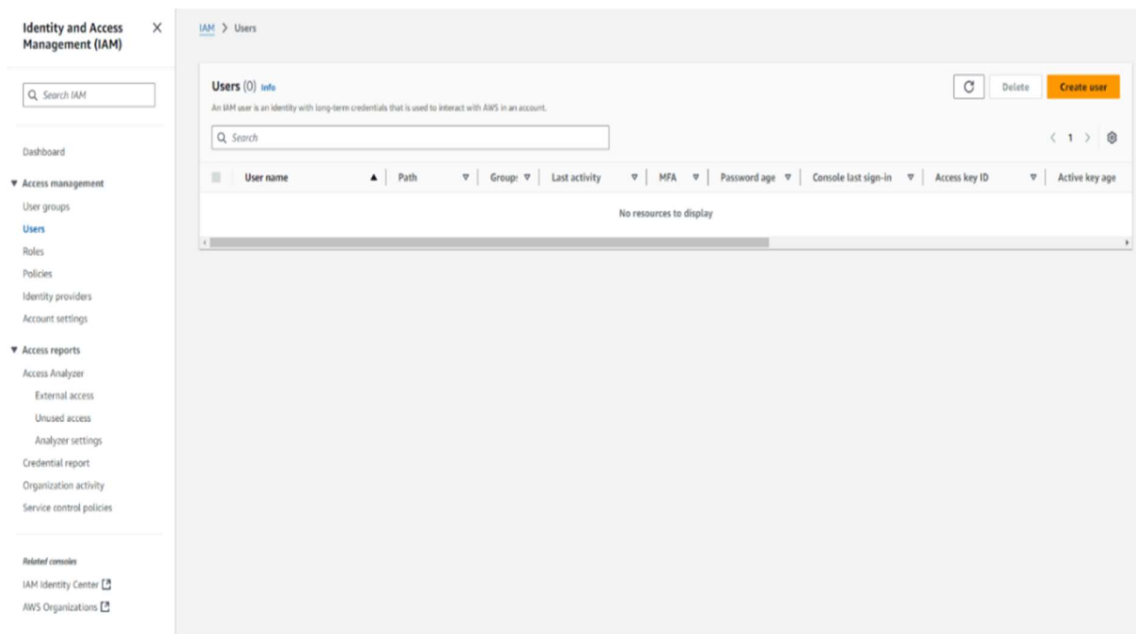


IAM - IDENTITY ACCESS MANAGEMENT

Step-1: Search IAM in the root user account and select.



Step-2: Once we select it shows the page like this and there is no user by default.



Create user

Users

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Specify user details

User details

User name

Sakshi-123

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, -, @, _ - (hyphen)

☒ Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a best practice [to manage their access in IAM Identity Center](#).

i Are you providing console access to a person?

User type

- ☐ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
- ☒ I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☐ Autogenerated password

You can view the password after you create the user.

☒ Custom password

Enter a custom password for the user.

Welcome@123

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters [A-Z], lowercase letters [a-z], numbers [0-9], and symbols ! @ # \$ % ^ & * () _ - = { } | ~ ' " , . ; : ' (hyphen) [] [] '

☒ Show password

Users must create a new password at next sign-in - Recommended

[IAM](#) > [Users](#) > Create user

Step 1
[Specify user details](#)

Step 2
Set permissions

Step 3
[Review and create](#)

Step 4
[Retrieve password](#)

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.

 **Get started with groups**
Create a 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](#)

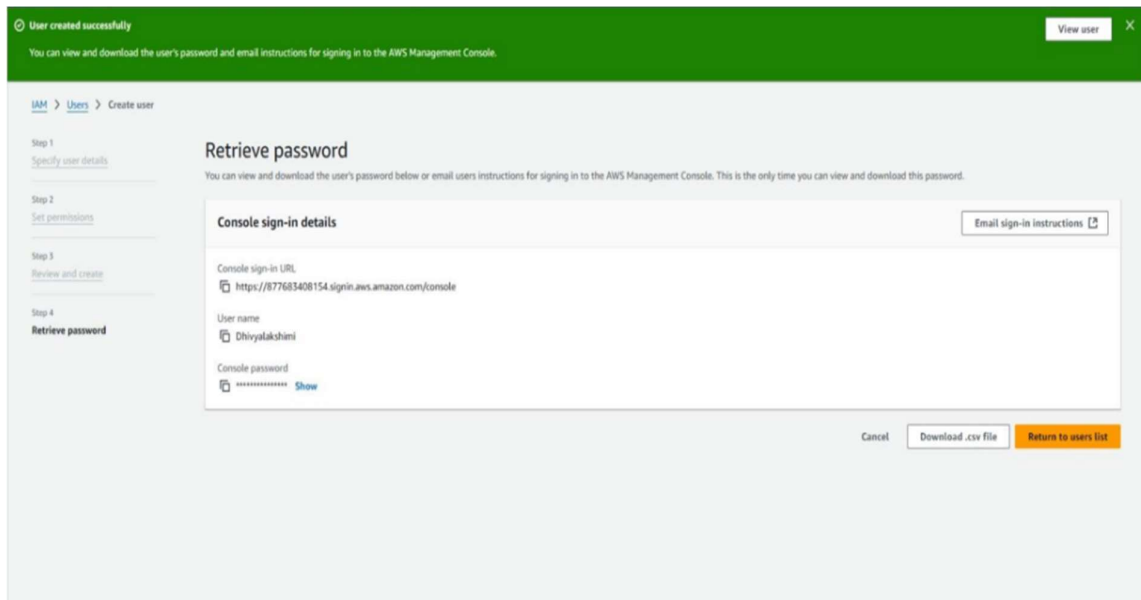
Create group

► **Set permissions boundary - optional**

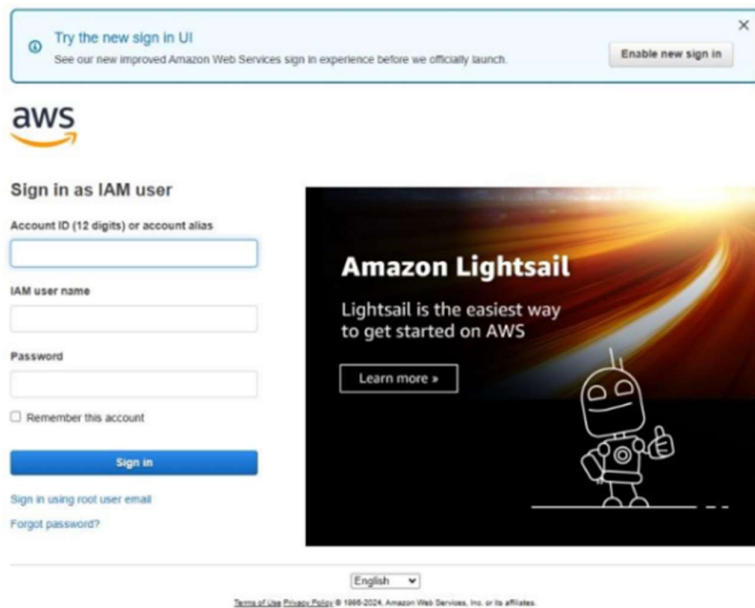
Cancel

Previous

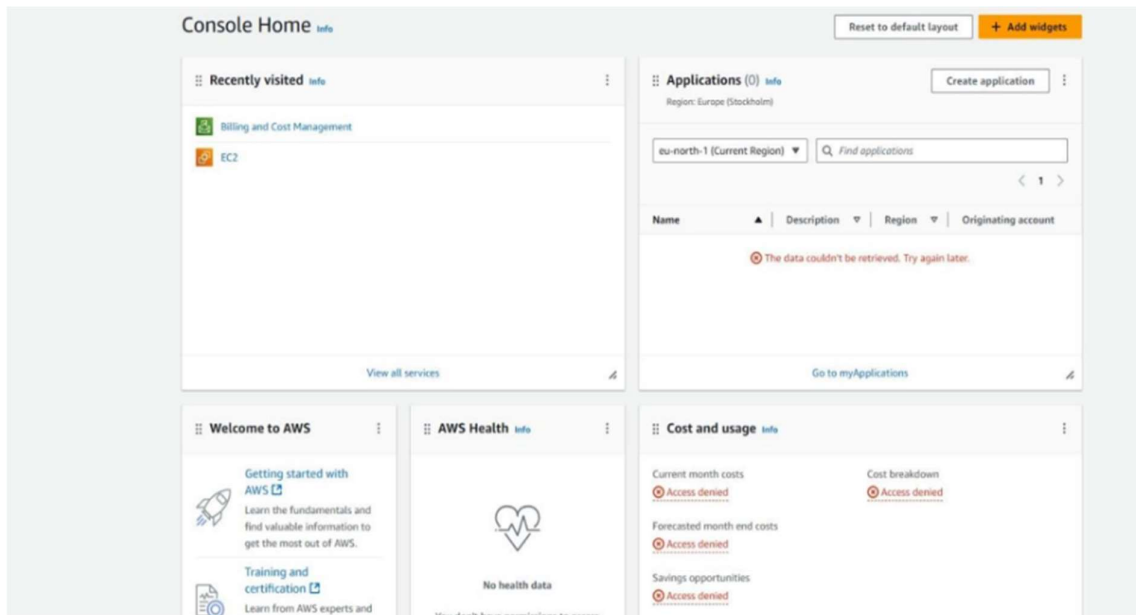
Next



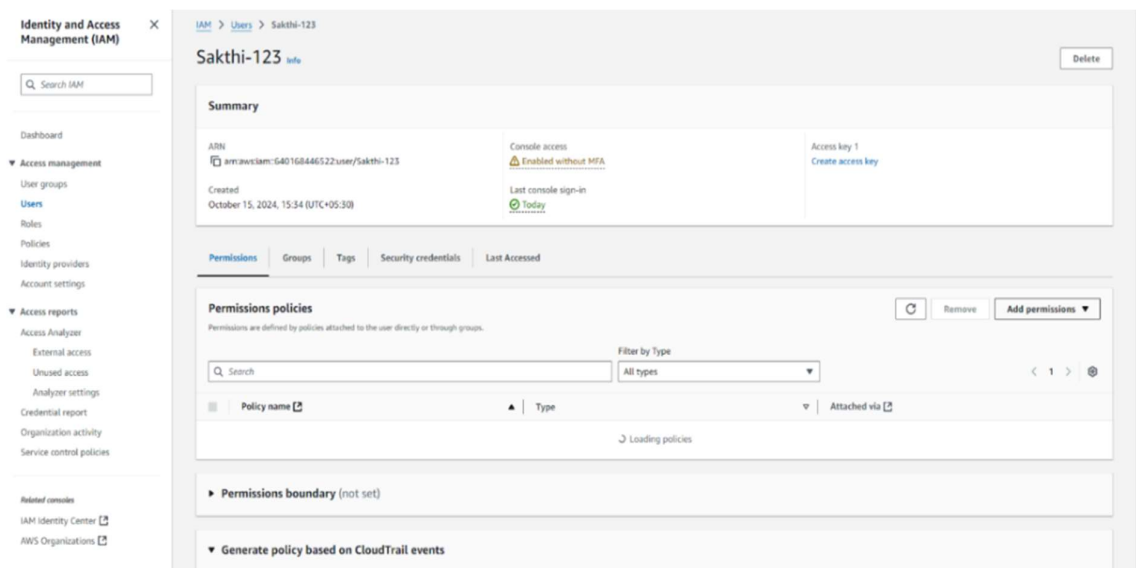
Step 6: Once the user is created, log in to AWS with the created user credentials.



Step-7: Once you log in, it shows the console page of the created user like this.



Step-8: Here we don't have permission to access the ec2 and the rest of the things.



Step-9: Go back to root user account > IAM Console > User > Select the created user > Permit by selecting add permission > select Amazons3fullAccess.

IAM > Users > Sakthi-123 > Add permissions

Step 1
Add permissions

Step 2
Review

Add 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, inline policies, and any existing permissions boundaries 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 (1239)

Filter by Type

All types 1 match

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	0

Cancel Next

Step-10: After selecting the permission give add permission.

1 policy added

IAM > Users > Sakthi-123 > Add permissions

Step 1
[Add permissions](#)

Step 2
Review

Review

The following policies will be attached to this user. [Learn more](#)

User details

User name
Sakthi-123

Permissions summary (1)

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy

Cancel Previous **Add permissions**