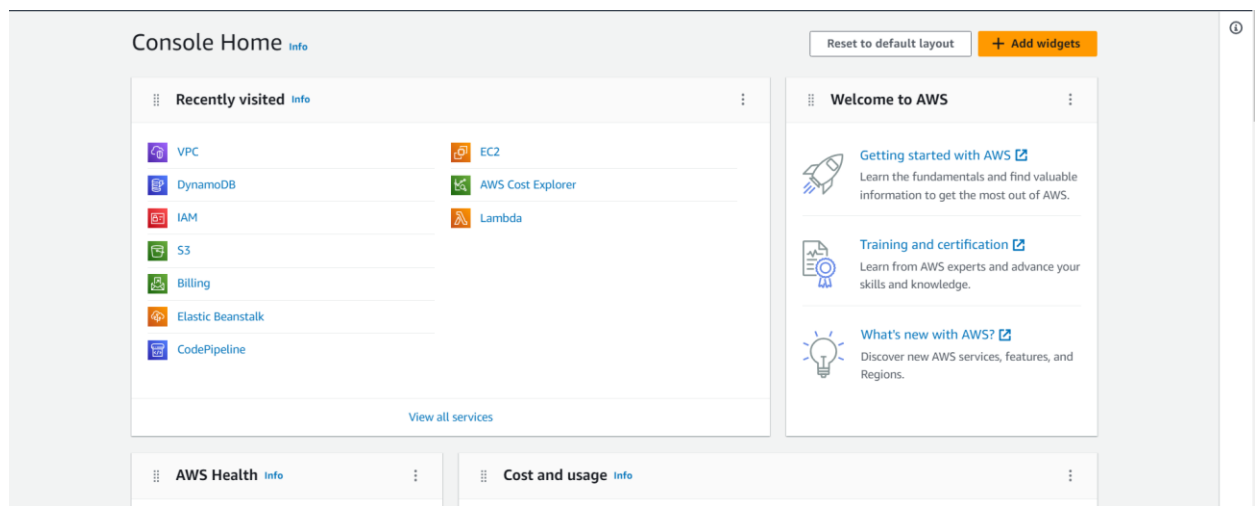
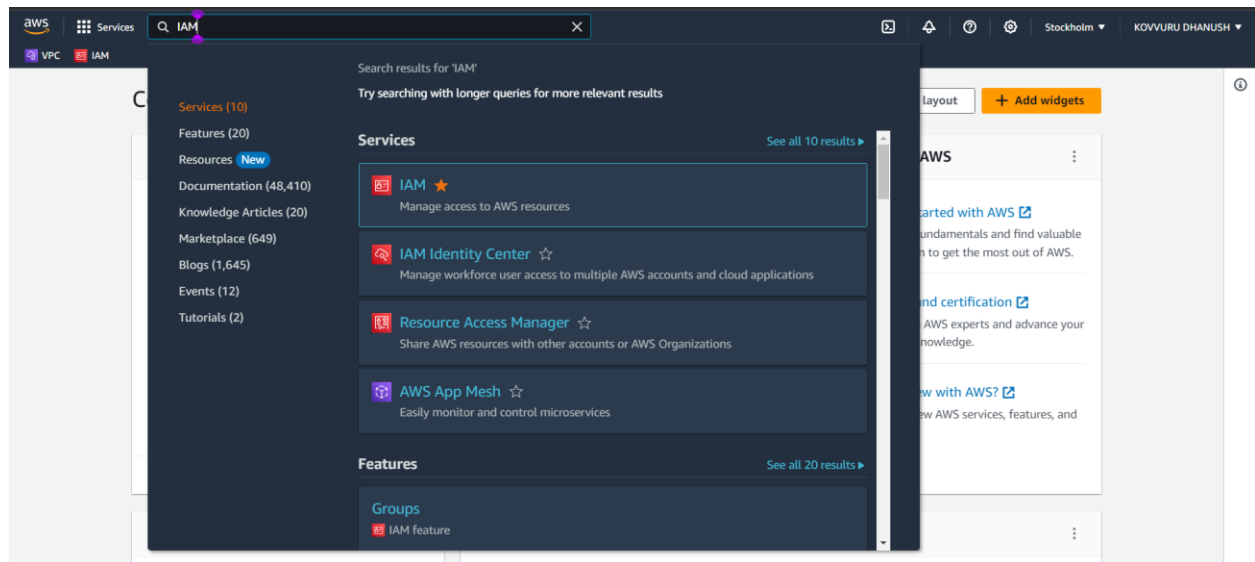


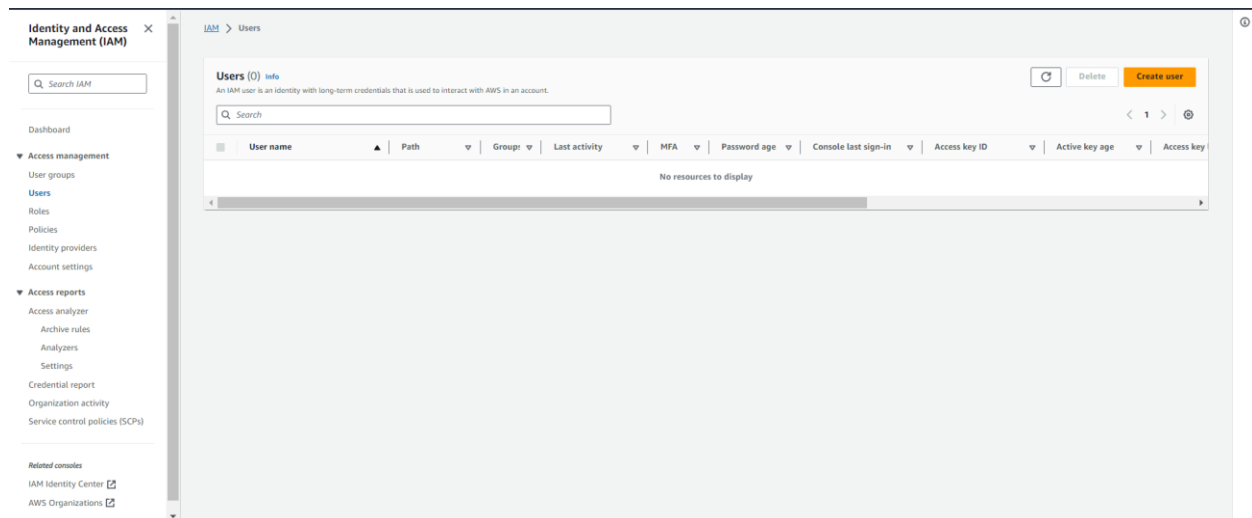
## IAM Users and Groups Hands ON



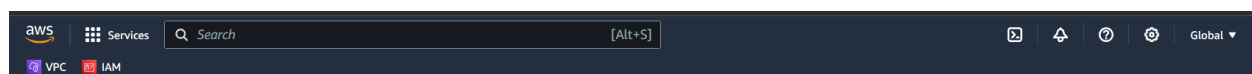
Open the Console.



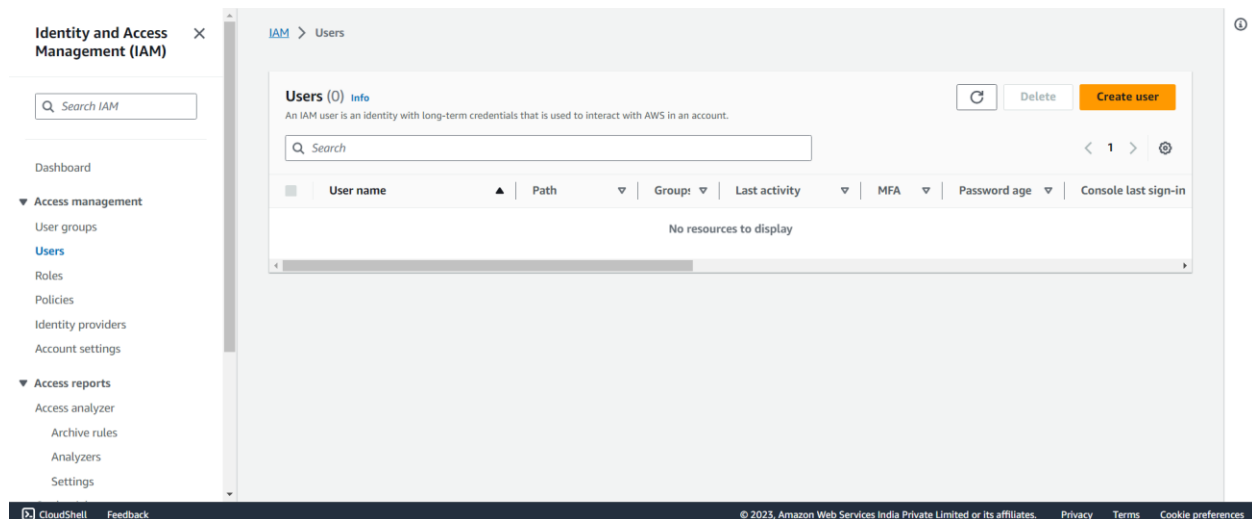
In Search Bar type IAM.



Come to the users section.



Here I would like to mention IAM is a Global Service.



Now Click on Create User.

User name

Kovvuru\_Dhansuh

Enter Username and here it's Kovvuru\_Dhansuh

- ☒ 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.



#### 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.

And click on that I want to Create IAM User.

☒ 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.

**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.

- 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  
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel **Next**

And click on create Custom Password.

And Remember the Password it's Important.

Here Uncheck Users must create a new password at the next sign-in .


And click on next.

# 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

Click on Create a group.

Create user group

Create a user 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](#)

User group name

Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+=, @-\_' characters.

Permissions policies (888)








Create policy

Filter by Type

Search

All ty... ▼

< 1 2 3 4 5 6 7 ... 45 > ⚙

<input type="checkbox"/>	Policy name	Type	Use...	Description
<input type="checkbox"/>	<input type="checkbox"/>  <a href="#">AdministratorAccess</a>	AWS managed ...	None	Provides full access to AWS service
<input type="checkbox"/>	<input type="checkbox"/>  <a href="#">AdministratorAcce...</a>	AWS managed	None	Grants account administrative per
<input type="checkbox"/>	<input type="checkbox"/>  <a href="#">AdministratorAcce...</a>	AWS managed	None	Grants account administrative per
<input type="checkbox"/>	<input type="checkbox"/>  <a href="#">AlexaForBusinessD...</a>	AWS managed	None	Provide device setup access to Alex
<input type="checkbox"/>	<input type="checkbox"/>  <a href="#">AlexaForBusinessF...</a>	AWS managed	None	Grants full access to AlexaForBusin
<input type="checkbox"/>	<input type="checkbox"/>  <a href="#">AlexaForBusinessG...</a>	AWS managed	None	Provide gateway execution access t
<input type="checkbox"/>	<input type="checkbox"/>  <a href="#">AlexaForBusinessLi...</a>	AWS managed	None	Provide access to Lifesize AVS devi

Cancel

Create user group

Here you will be landing on this page.

Create user group

×

Create a user 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](#)

User group name

Enter a meaningful name to identify this group.

Administrato\_Group

Maximum 128 characters. Use alphanumeric and '+=, @-\_' characters.

Permissions policies (1/888)

↺












Create policy

Filter by Type

Search

All ty... ▼

< 1 2 3 4 5 6 7 ... 45 > ⚙

	Policy name	Type	Use...	Description
<input checked="" type="checkbox"/>	 <a href="#">AdministratorAccess</a>	AWS managed ...	None	Provides full access to AWS service...
<input type="checkbox"/>	 <a href="#">AdministratorAcce...</a>	AWS managed	None	Grants account administrative perm...
<input type="checkbox"/>	 <a href="#">AdministratorAcce...</a>	AWS managed	None	Grants account administrative perm...
<input type="checkbox"/>	 <a href="#">AlexaForBusinessD...</a>	AWS managed	None	Provide device setup access to Alex...
<input type="checkbox"/>	 <a href="#">AlexaForBusinessF...</a>	AWS managed	None	Grants full access to AlexaForBusin...
<input type="checkbox"/>	 <a href="#">AlexaForBusinessG...</a>	AWS managed	None	Provide gateway execution access t...
<input type="checkbox"/>	 <a href="#">AlexaForBusinessLi...</a>	AWS managed	None	Provide access to Lifesize AVS devic...
<input type="checkbox"/>	 <a href="#">AlexaForBusinessP...</a>	AWS managed	None	Provide access to Poly AVS devices
<input type="checkbox"/>	 <a href="#">AlexaForBusinessR...</a>	AWS managed	None	Provide read only access to AlexaFc...
<input type="checkbox"/>	 <a href="#">AmazonAPIGatewa...</a>	AWS managed	None	Provides full access to create/edit/c...
<input type="checkbox"/>	 <a href="#">AmazonAPIGatewa...</a>	AWS managed	None	Provides full access to invoke APIs i...

Cancel

Create user group

Here enter a group name.

And add permission AdministratorAccess.

## Create user group

Then click in create user group.

### 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.

#### User groups (1)

Search



Create group

< 1 > ⚙

<input type="checkbox"/>	Group name	Users	Attached policies	Created
<input type="checkbox"/>	<a href="#">Administrato_Group</a>	0	<a href="#">AdministratorAccess</a>	2023-10-01 (Now)

#### ► Set permissions boundary - optional

Cancel

Previous

Next

Now the group what we have created It will be visible here check once then only we can say that our group is created successfully.

z

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.

#### User groups (1/1)

Search

Create group

< 1 > ⚙

<input checked="" type="checkbox"/>	Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/>	<a href="#">Administrato_Group</a>	0	<a href="#">AdministratorAccess</a>	2023-10-01 (1 minute ago)

#### ► Set permissions boundary - optional

Cancel Previous Next

And click on next.

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

Step 1  
[Specify user details](#)

Step 2  
[Set permissions](#)

Step 3  
**Review and create**

Step 4  
Retrieve password

## Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

### User details

User name Kovvuru_Dhanush	Console password type Custom password	Require password reset No
------------------------------	--	------------------------------

### Permissions summary

< 1 >

Name	Type	Used as
<a href="#">Administrato_Group</a>	Group	Permissions group

### Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

CancelPreviousCreate user

Then you will be landing on this page.

### Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

If you're on a thought to add tags, then you can .

## Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

### User details

User name Kovvuru_Dhanush	Console password type Custom password	Require password reset No
------------------------------	--	------------------------------

### Permissions summary

< 1 >

Name	Type	Used as
<a href="#">Administrato_Group</a>	Group	Permissions group

### Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

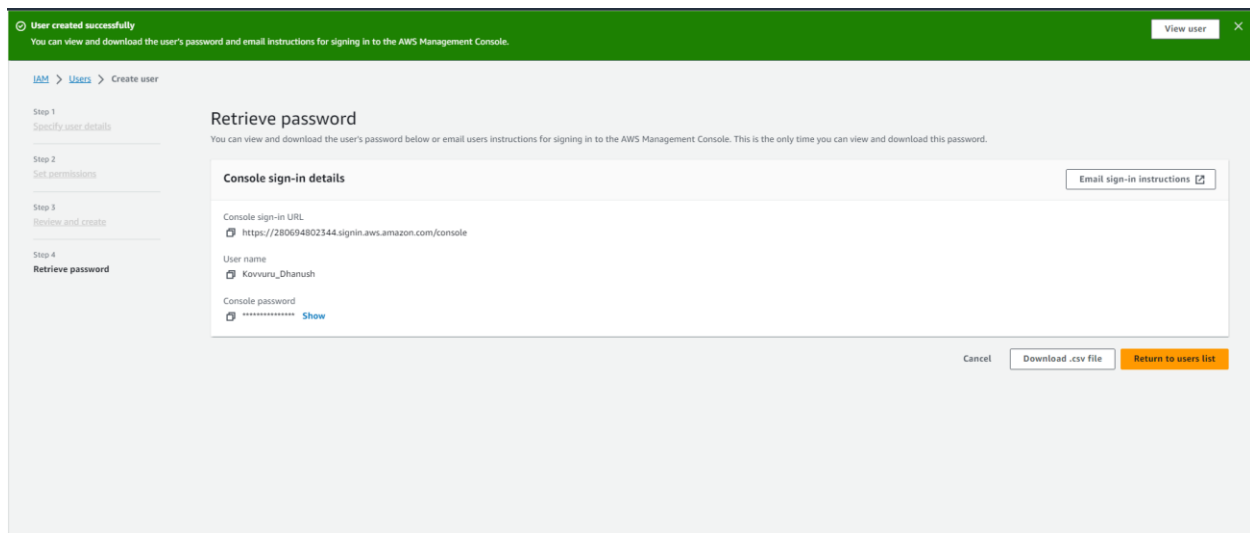
Add new tag

You can add up to 50 more tags.

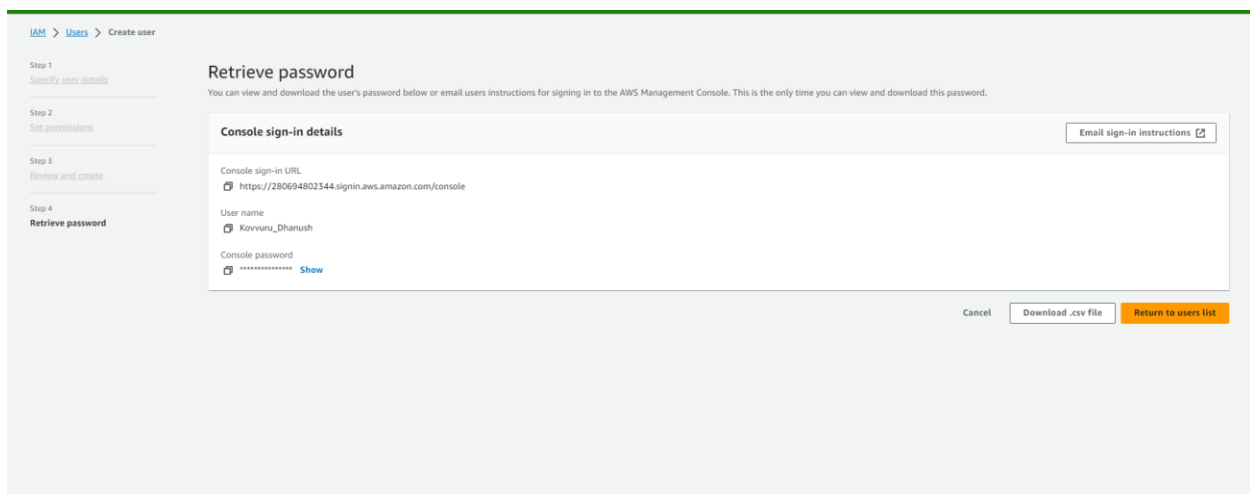
CancelPreviousCreate user

Now click on create user.





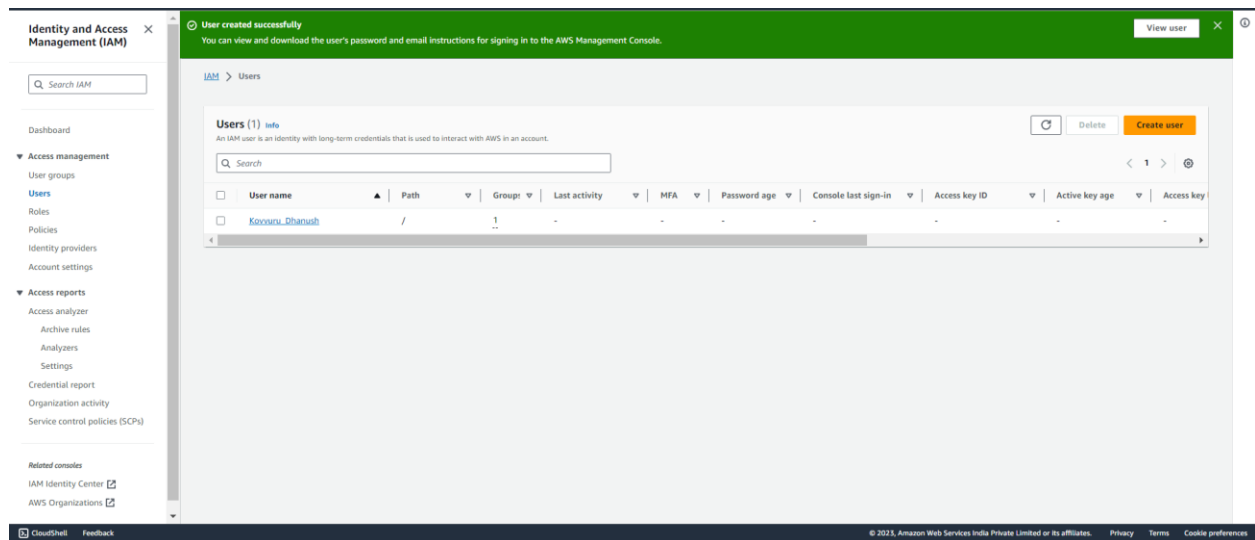
Now the user and the Group have been created successfully.



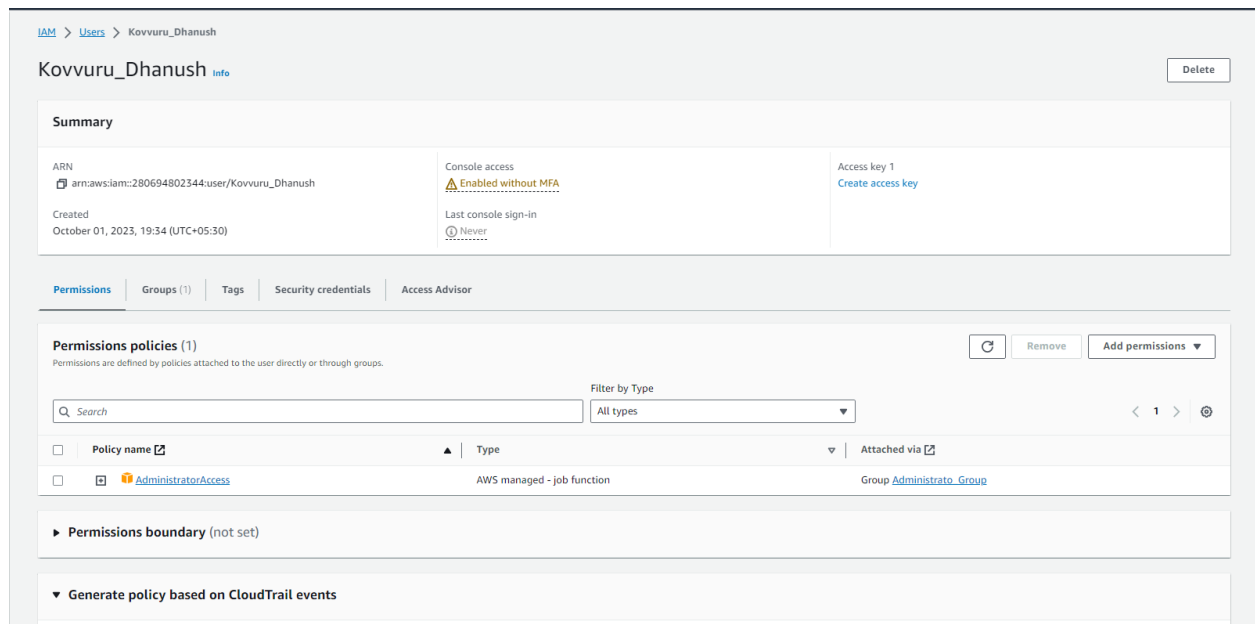
Here you can share this credentials who need them.

You share this credentials to Via Email.

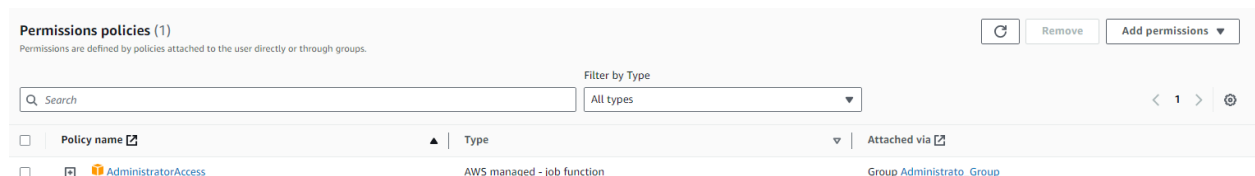
Here you can download .csv file and it will be downloaded in download sections.



Now come to the user's section.



Check the permissions that we gave earlier and it's reflecting here see it.



Now click on Groups the group which you created earlier, and you added the user right you can check here it is reflecting and it is stating that Kovvuru\_Dhanush is added to a group Administrator\_Group.

IAM > Users > Kovvuru\_Dhanush

Kovvuru\_Dhanush [Info](#) [Delete](#)

### Summary

ARN arn:aws:iam::280694802344:user/Kovvuru_Dhanush	Console access <b>Enabled without MFA</b>	Access key 1 <a href="#">Create access key</a>
Created October 01, 2023, 19:34 (UTC+05:30)	Last console sign-in Never	

Permissions | Groups (1) | **Tags** | Security credentials | Access Advisor

### Tags (0)

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

Key	Value
No tags associated with the resource	

[Add new tag](#)  
You can add 50 more tags.

Here we didn't add any tag so it is not reflecting here.

IAM > Users > Kovvuru\_Dhanush

Kovvuru\_Dhanush [Info](#) [Delete](#)

### Summary

ARN arn:aws:iam::280694802344:user/Kovvuru_Dhanush	Console access <b>Enabled without MFA</b>	Access key 1 <a href="#">Create access key</a>
Created October 01, 2023, 19:34 (UTC+05:30)	Last console sign-in Never	

Permissions | Groups (1) | Tags | **Security credentials** | Access Advisor

### Console sign-in

[Manage console access](#)

Console sign-in link <a href="https://280694802344.signin.aws.amazon.com/console">https://280694802344.signin.aws.amazon.com/console</a>	Console password Updated 8 minutes ago (2023-10-01 19:34 GMT+5:30)
	Last console sign-in Never

By using the above link, the user can access to the console or when we are logging to the account at starting if you remember it ask us to login via root user or IAM User .



## Sign in

### ☒ Root user

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

### ☐ IAM user

User within an account that performs daily tasks. [Learn more](#)

Root user email address

username@example.com

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

— New to AWS? —

Create a new AWS account

## ANALYTICS

# Try Amazon OpenSearch Service for Free

Get 750 free hours per month of a single-AZ t2.small.search or t3.small.search instance

[Learn more >](#)



Check here I hope you got it.

### Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Remove

Resync

Assign MFA device

Device type

Identifier

Certifications

Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment.

Assign MFA device

### Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Create access key

No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

Create access key

In my further post I will tell you what the use of Access key and MFA(Multi Factor Authentication) is

This MFA Is Important and AWS Recommend us to use MFA.

### Console sign-in

Manage console access

Console sign-in link

<https://280694802344.signin.aws.amazon.com/console>

Console password

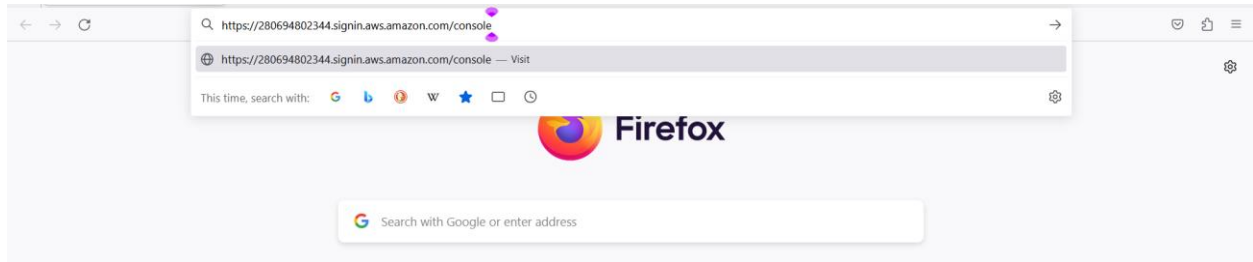
Updated 14 minutes ago (2023-10-01 19:34 GMT+5:30)

Last console sign-in

Never

Now copy the link.

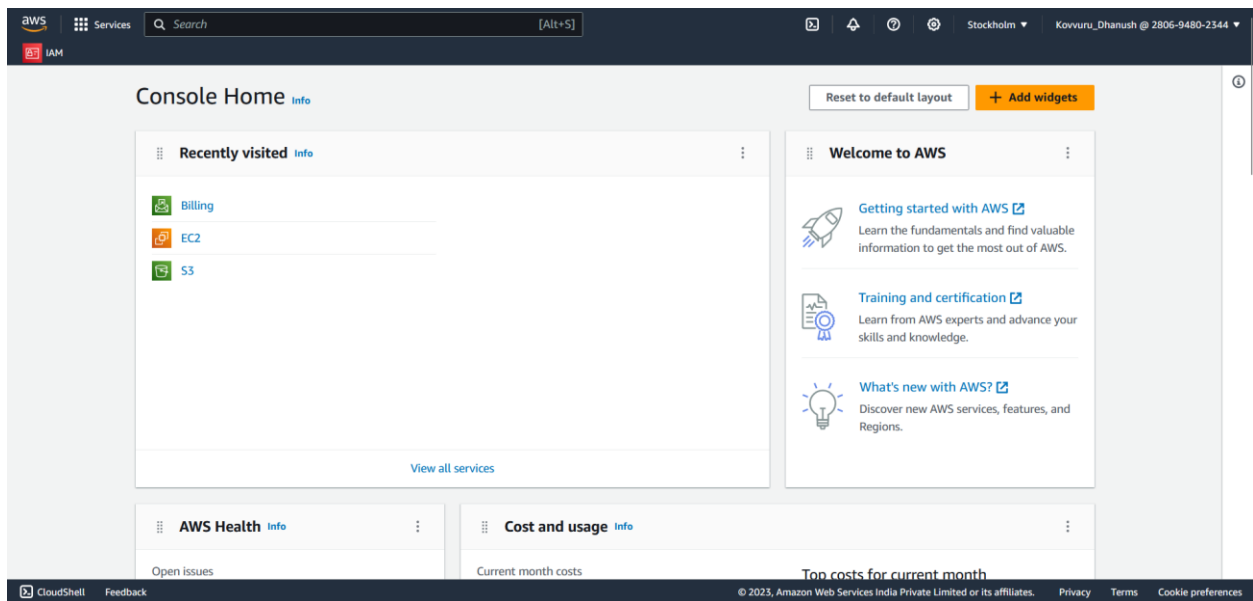
Open another web browser it is Important.



Paste the link.

A screenshot of the AWS IAM user sign-in page. The page features the AWS logo at the top left. Below it, the heading 'Sign in as IAM user' is followed by a form with three input fields: 'Account ID (12 digits) or account alias' (containing '280694802344'), 'IAM user name' (empty), and 'Password' (empty). There is a checkbox for 'Remember this account' and a blue 'Sign in' button. Below the button are links for 'Sign in using root user email' and 'Forgot password?'. On the right side, there is an advertisement for Amazon Lightsail with the text 'Amazon Lightsail' and 'Lightsail is the easiest way to get started on AWS', along with a 'Learn more »' button and a cartoon robot character. At the bottom, there is a language dropdown set to 'English' and a footer with 'Terms of Use Privacy Policy © 1996-2023, Amazon Web Services, Inc. or its affiliates'.

Enter your username and the password.



See now user can access the console the way you are accessing it as a root user but here this is a IAM User and please don't share this login credentials to anyone .

As AWS Recommend as to use IAM User not Root user in my further posts I will be using the IAM User .