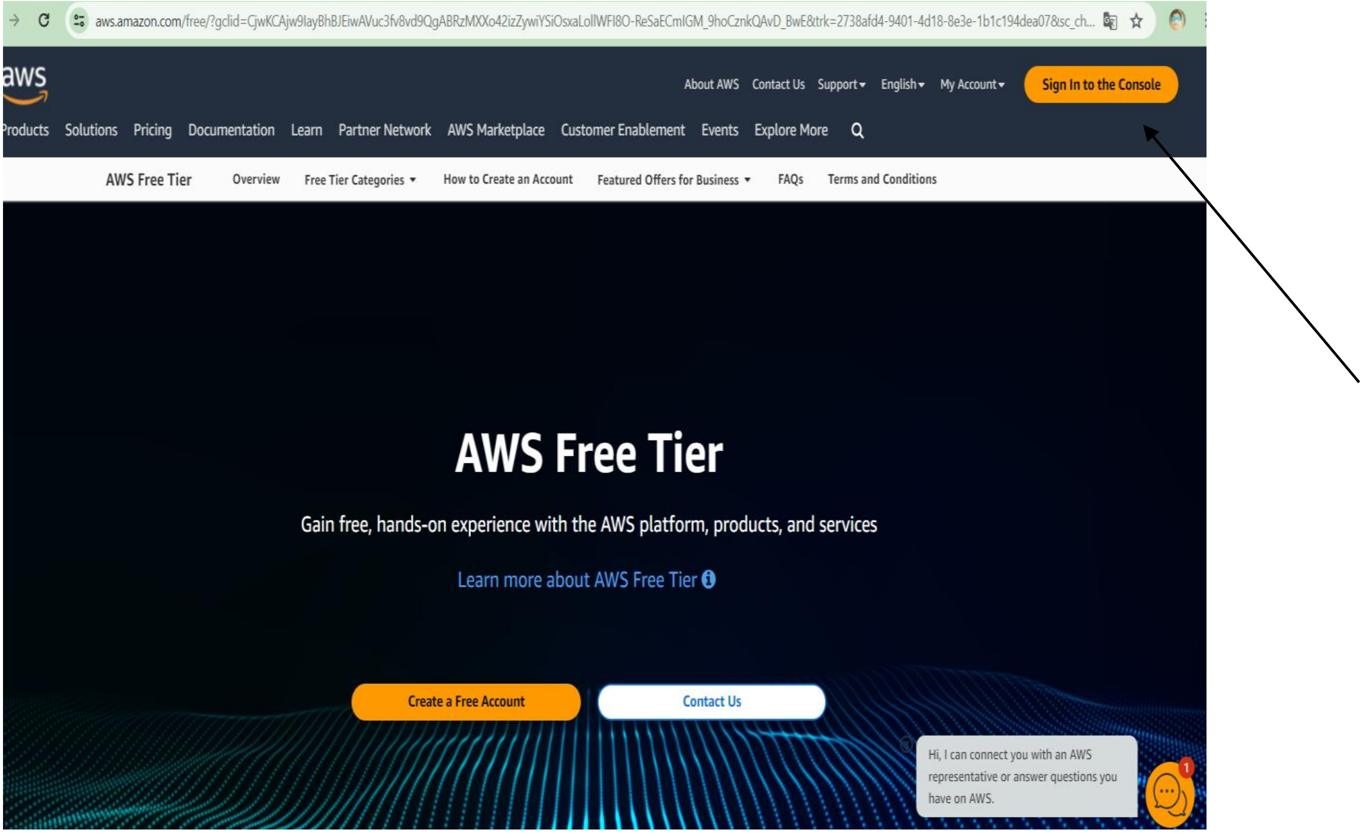
L2 - Login to AWS Console and Create IAM User, Role, and Group

STEP-1 : Login to AWS console using **Root account credentials.**



AWS Free Tier

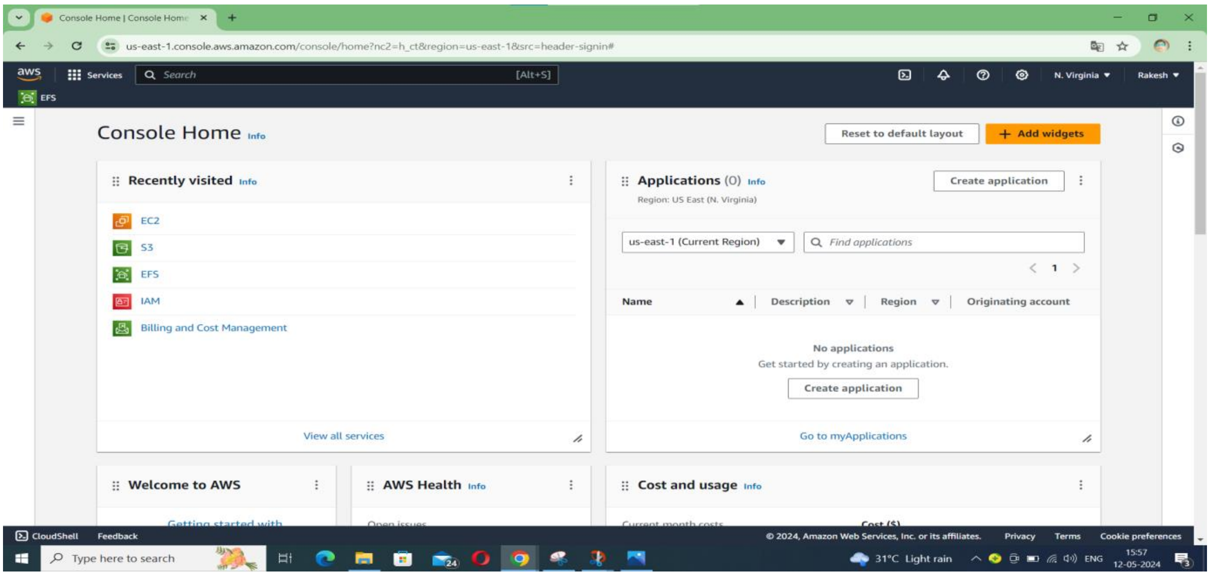
Gain free, hands-on experience with the AWS platform, products, and services

Learn more about AWS Free Tier

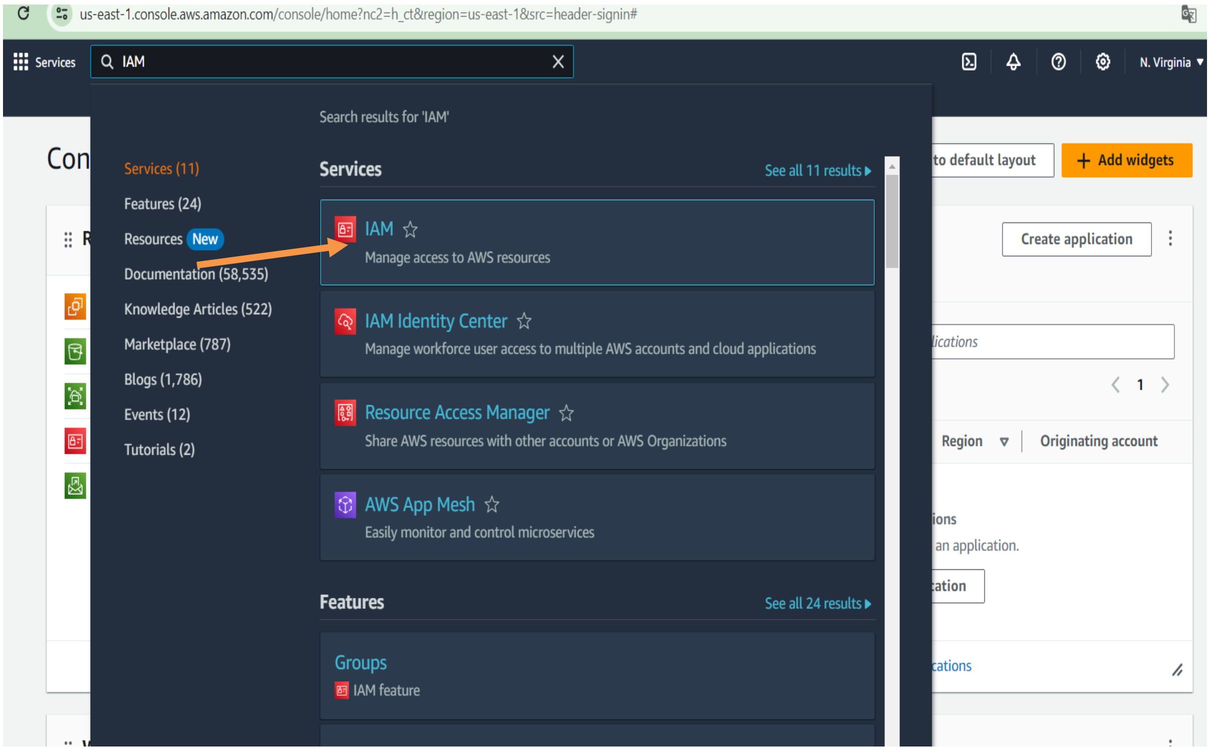
Hi, I can connect you with an AWS representative or answer questions you have on AWS.

.

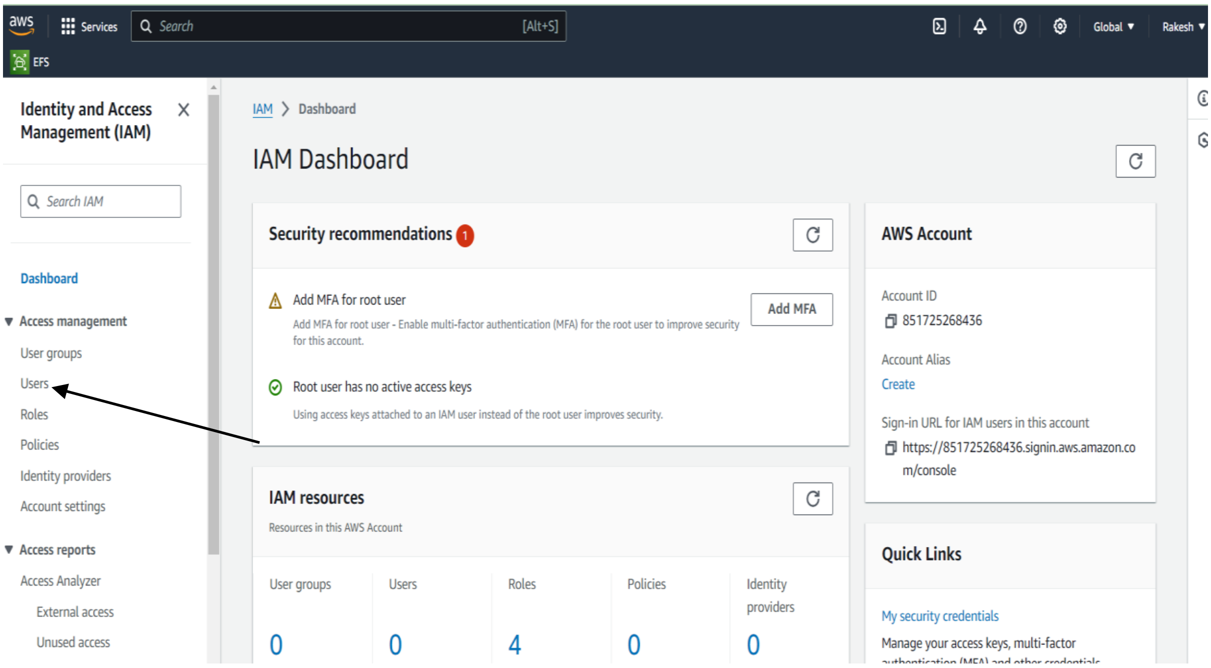
STEP 2: Then you will see **console home page** as shown in below picture.



STEP -3: In console home page in search box search for **IAM Service** And **click** on IAM sevice as shown below.



STEP 4: In IAM Dashboard under **Access management** click on **Users.**



IAM Dashboard

Security recommendations 1

Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	4	0	0

AWS Account

Account ID
851725268436

Account Alias
Create

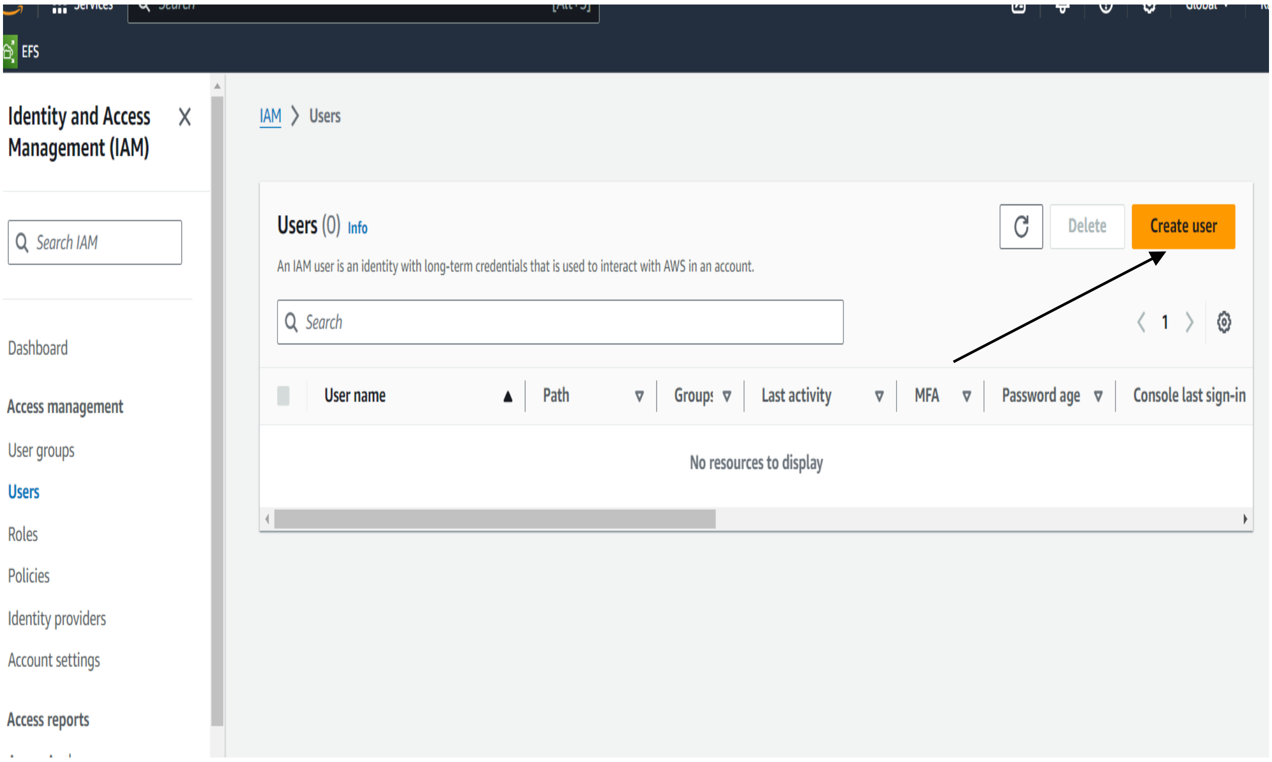
Sign-in URL for IAM users in this account
https://851725268436.signin.aws.amazon.com/console

Quick Links

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials

STEP 5: In Right side of the picture **click** on **Create user**



Users (0)

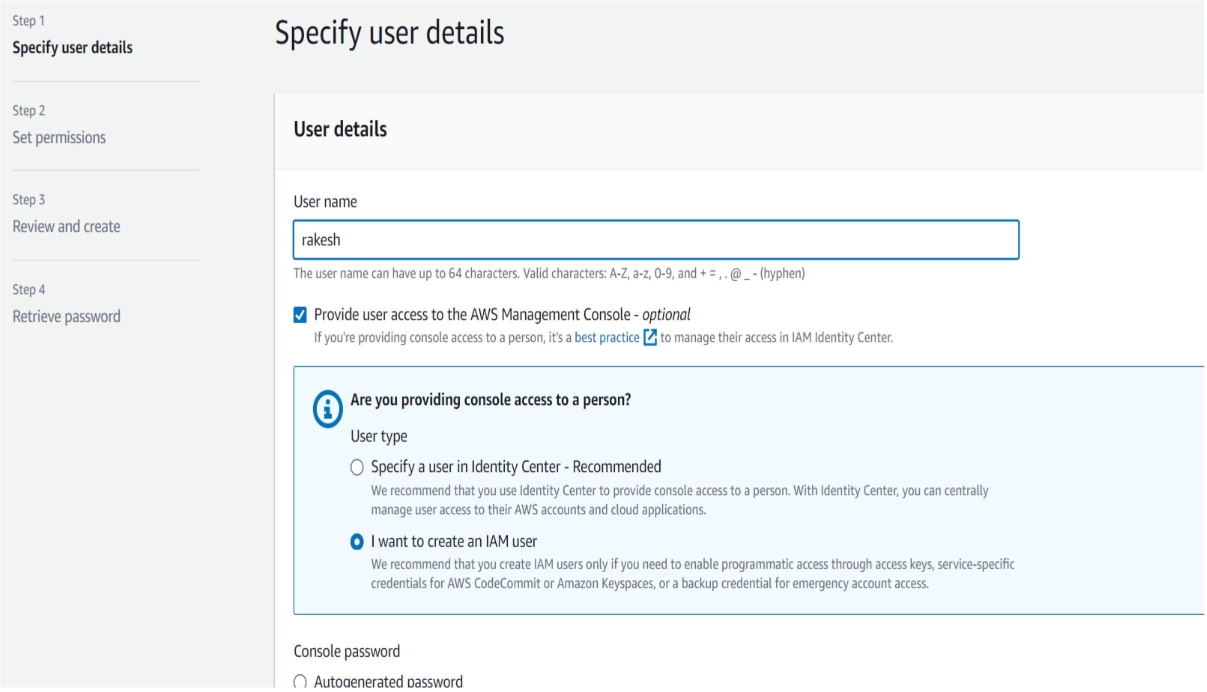
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name ▲	Path	Groups	Last activity	MFA	Password age	Console last sign-in
No resources to display						

STEP 6: In user details fill **User name** .

Enable AWS management console.

In **User type** enable 2nd box as shown in picture.



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

rakesh

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.

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.

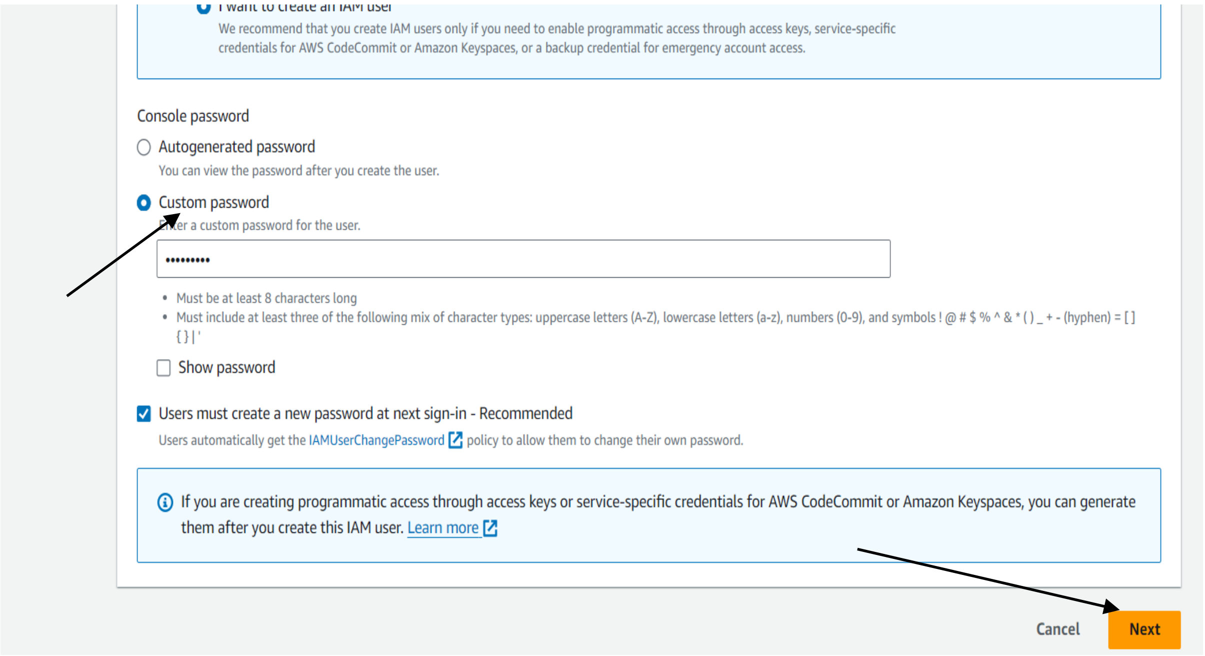
Console password

○ Autogenerated password

STEP 7 : In same page in **console password** .

Click on custom password and create password .

Then **Click** on Next.



● 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) = [ ] { } | '

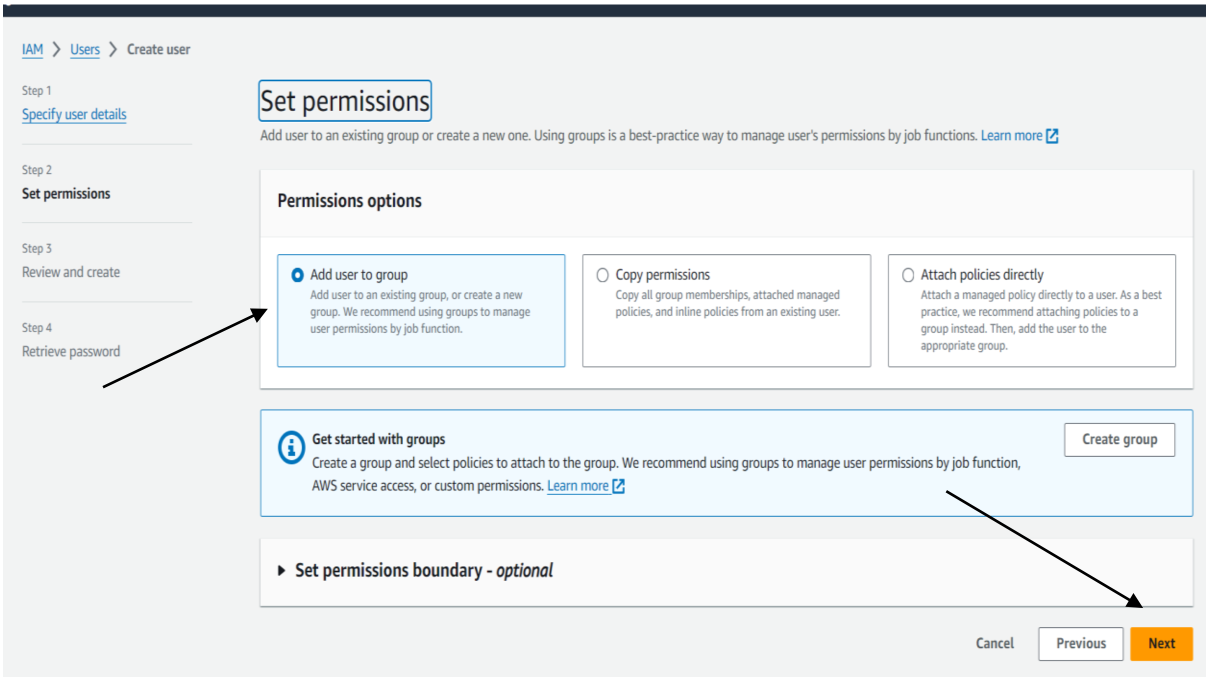
□ Show password

☑ 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

STEP 8: In Set Permission Option Select 1st one 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

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.

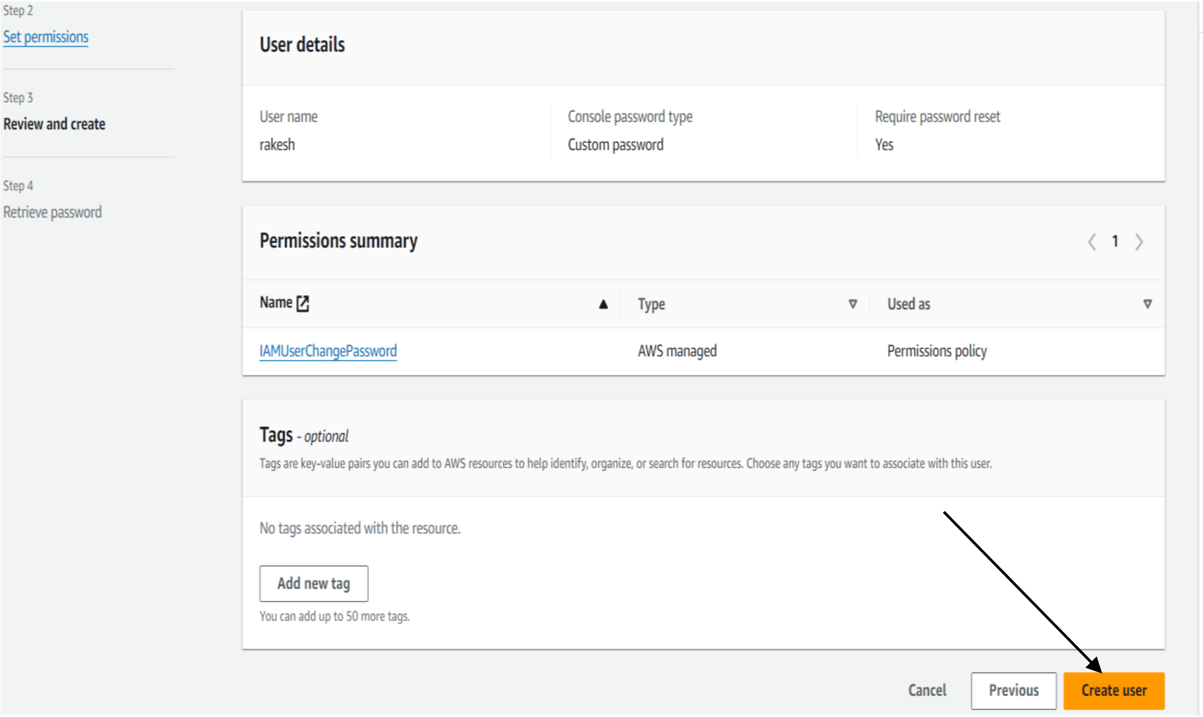
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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

▸ Set permissions boundary - *optional*

STEP 9: Here **click** on Create user.



Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

User details

User name	Console password type	Require password reset
rakesh	Custom password	Yes

Permissions summary

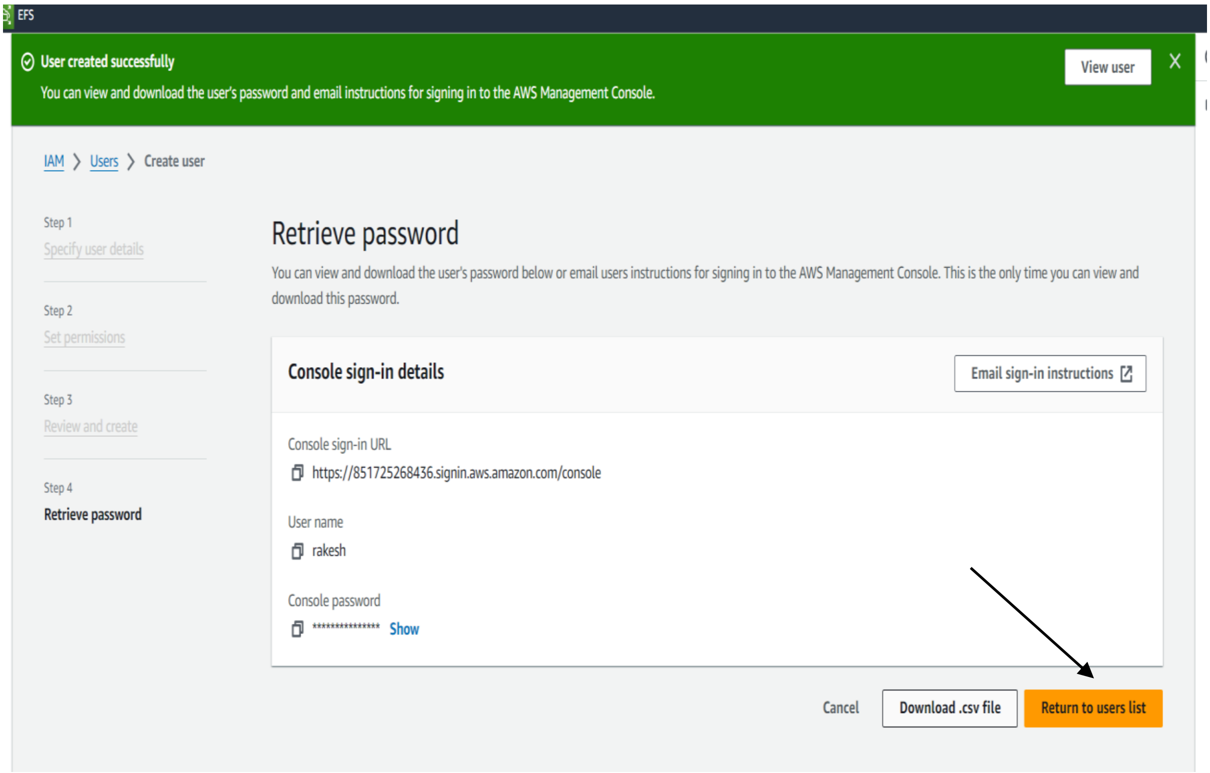
Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

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.

You can add up to 50 more tags.

STEP 10: In below picture you will see **User created successefully.** To view user **click** on **Return to user list**.



User created successfully

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

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

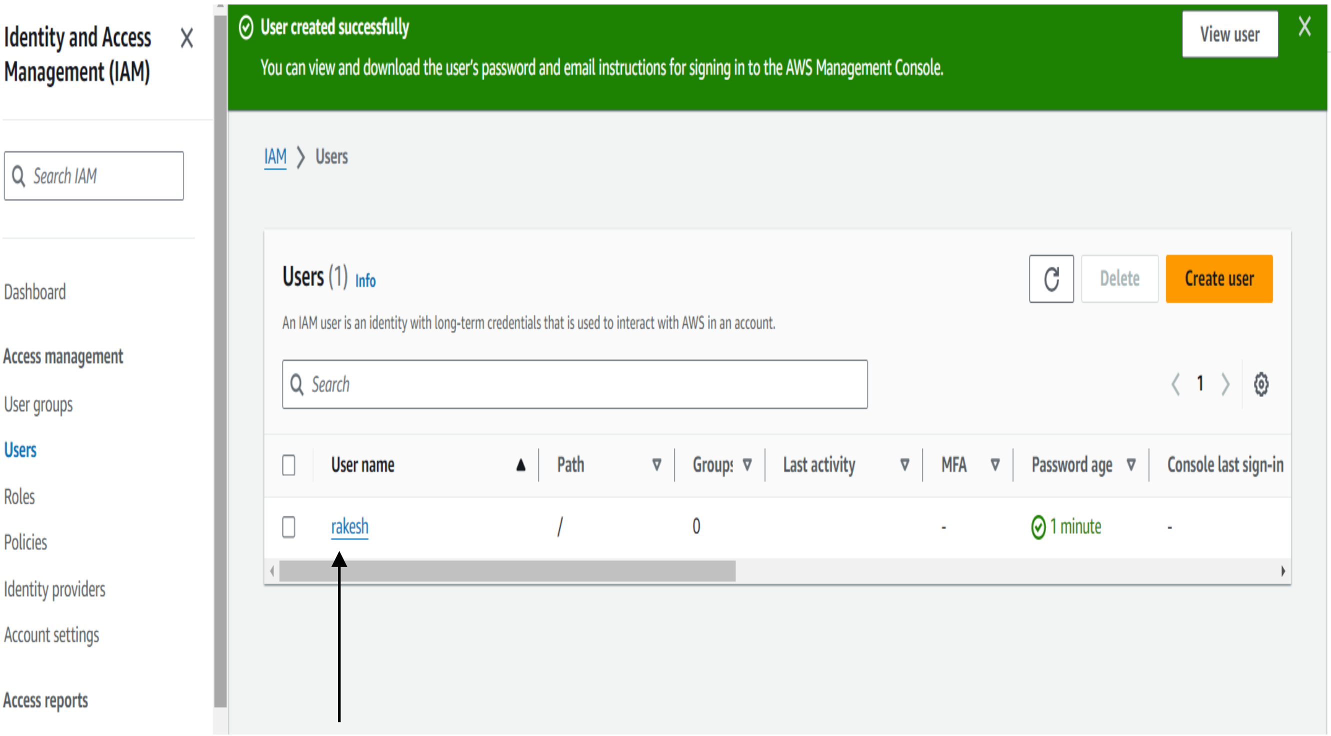
Console sign-in details

Console sign-in URL
https://851725268436.signin.aws.amazon.com/console

User name
rakesh

Console password
****

STEP 11: In below pictre you will find User **rakesh** got created in the **User List.**



User created successfully

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

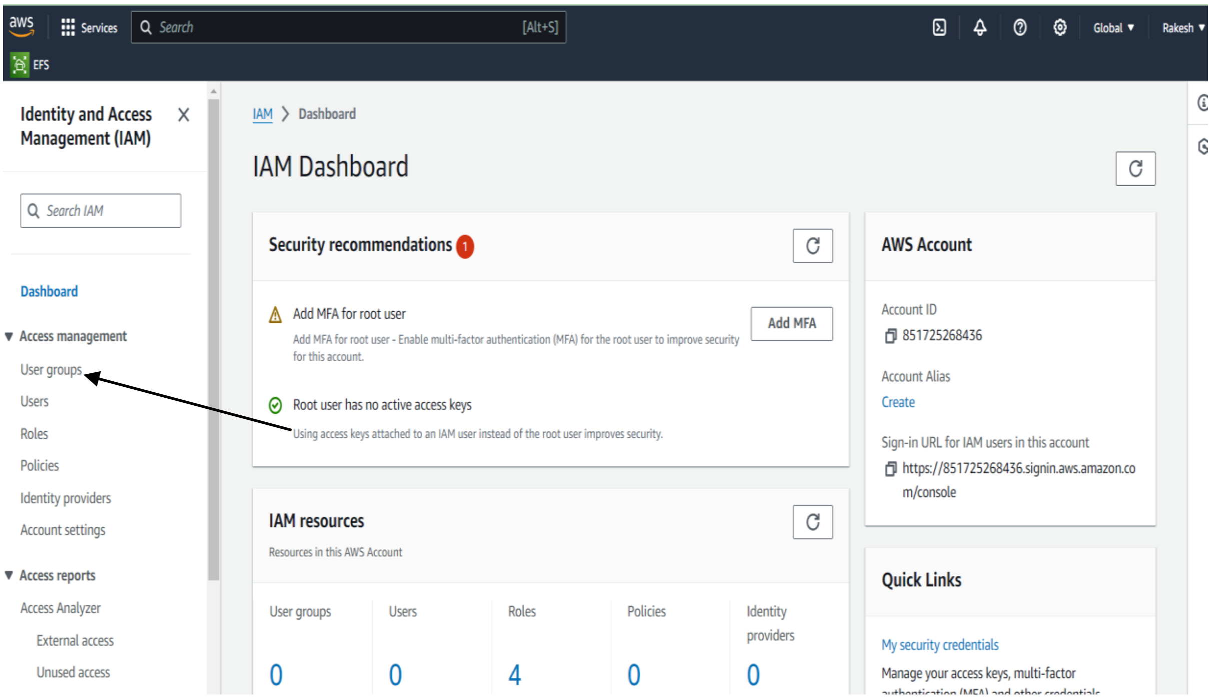
Users (1)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name ▲	Path	Groups	Last activity	MFA	Password age	Console last sign-in
□	rakesh	/	0		-	✓ 1 minute	-

CREATION OF IAM GROUP

STEP 1: In IAM Dashboard under **Access management** click on **User Group.**



Identity and Access Management (IAM)

Search IAM

Dashboard

▾ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▾ Access reports

Access Analyzer

External access

Unused access

IAM > Dashboard

IAM Dashboard

Security recommendations 1

Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Add MFA

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	4	0	0

AWS Account

Account ID

851725268436

Account Alias

Create

Sign-in URL for IAM users in this account

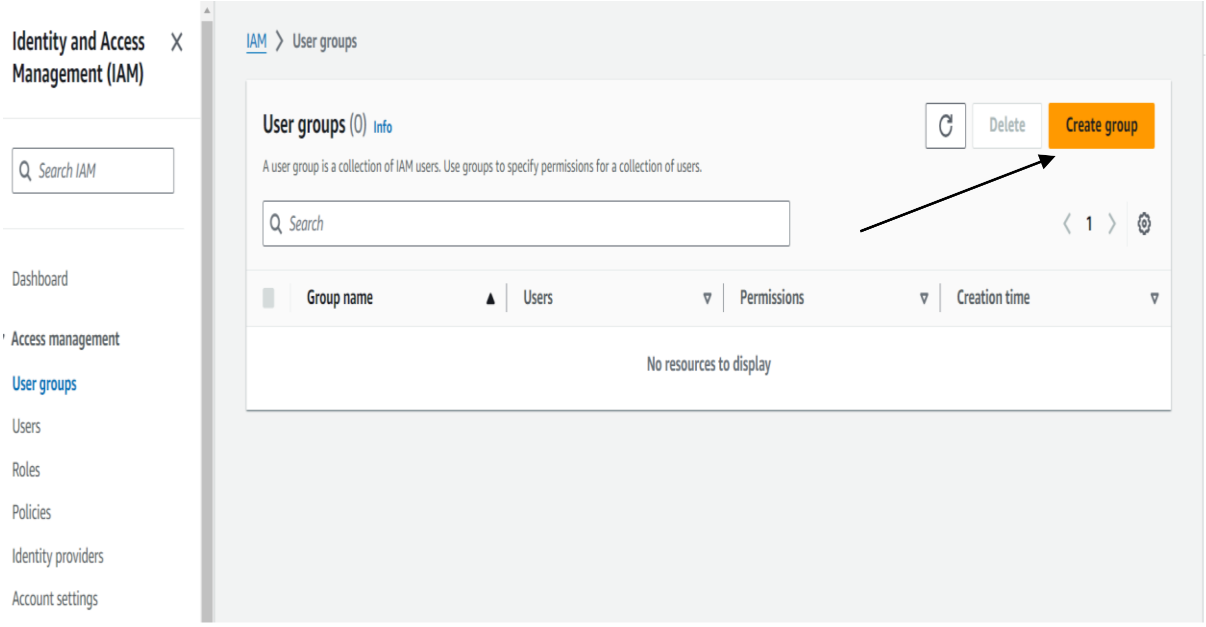
https://851725268436.signin.aws.amazon.com/console

Quick Links

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials

STEP 2: Click on **Create group.**



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

IAM > User groups

User groups (0) Info

Delete

Create group

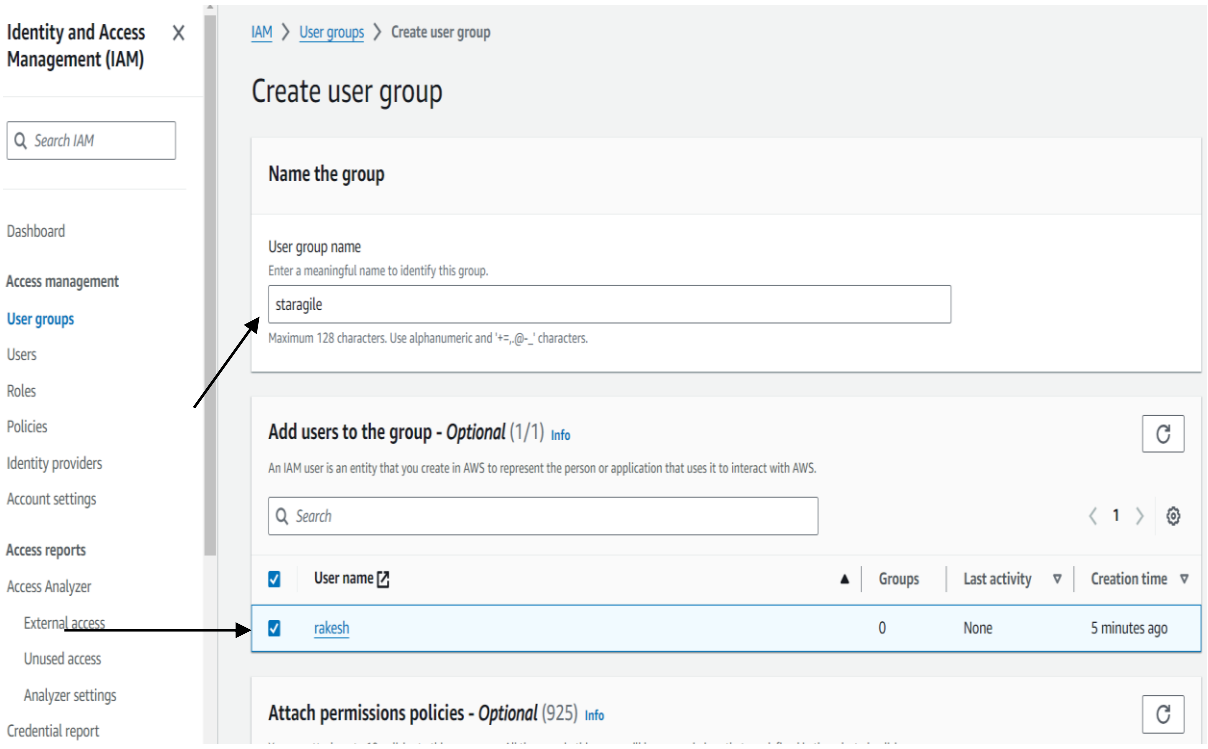
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

Group name	Users	Permissions	Creation time
No resources to display			

STEP 3: 1st **Give Group name** { staragile}.

And **add User** {rakesh} as shown as below.



Identity and Access Management (IAM)

IAM > User groups > Create user group

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

staragile

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

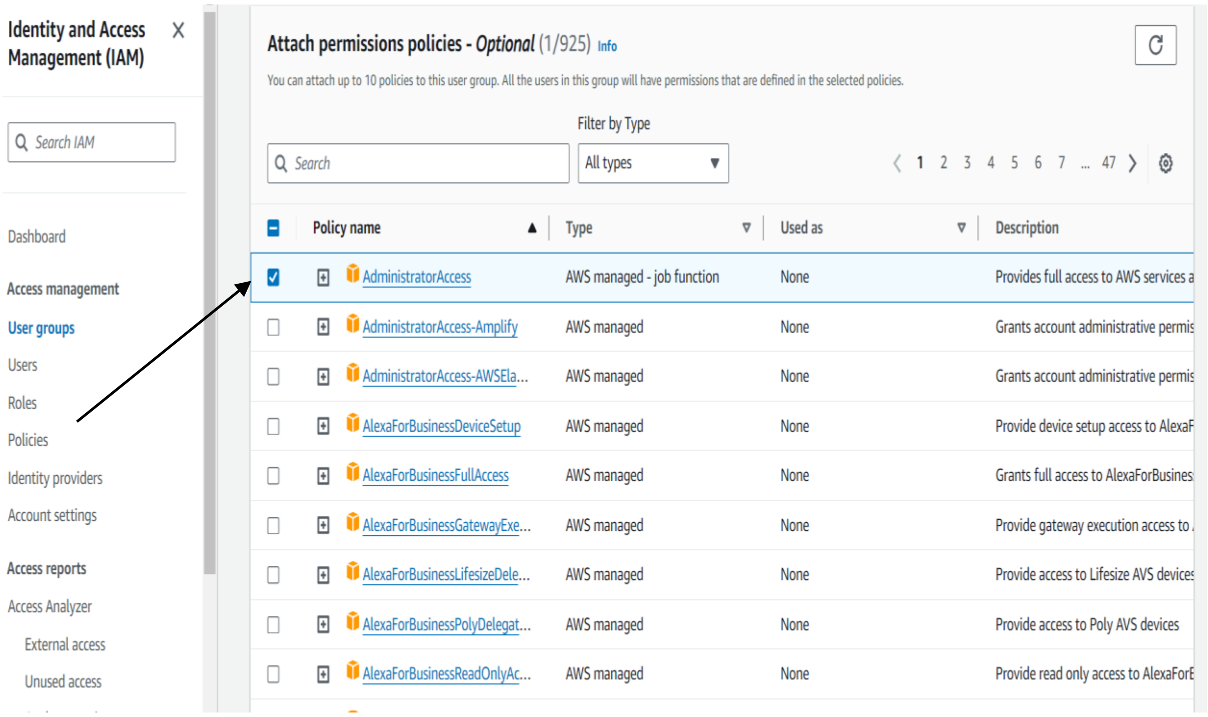
Add users to the group - *Optional* (1/1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

☑	User name	Groups	Last activity	Creation time
☑	rakesh	0	None	5 minutes ago

Attach permissions policies - *Optional* (925) Info

STEP 4: In same page **Attach** any Permissions Policies [optional].



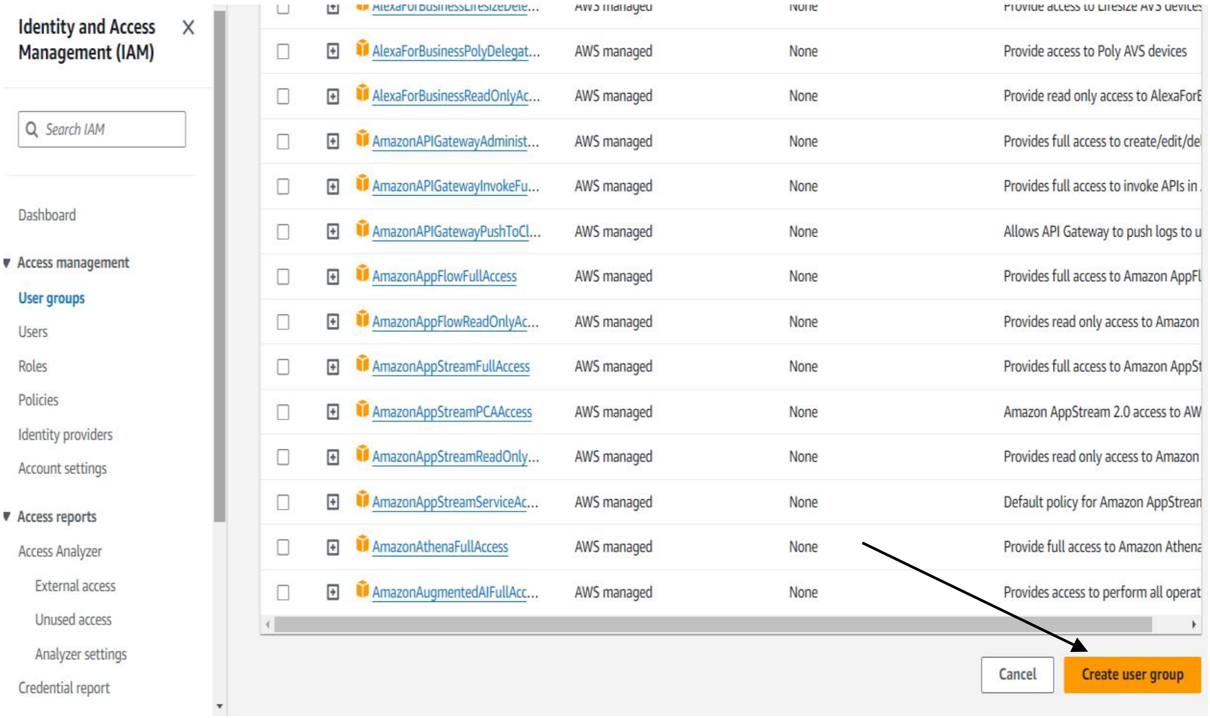
Attach permissions policies - *Optional* (1/925) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type: All types

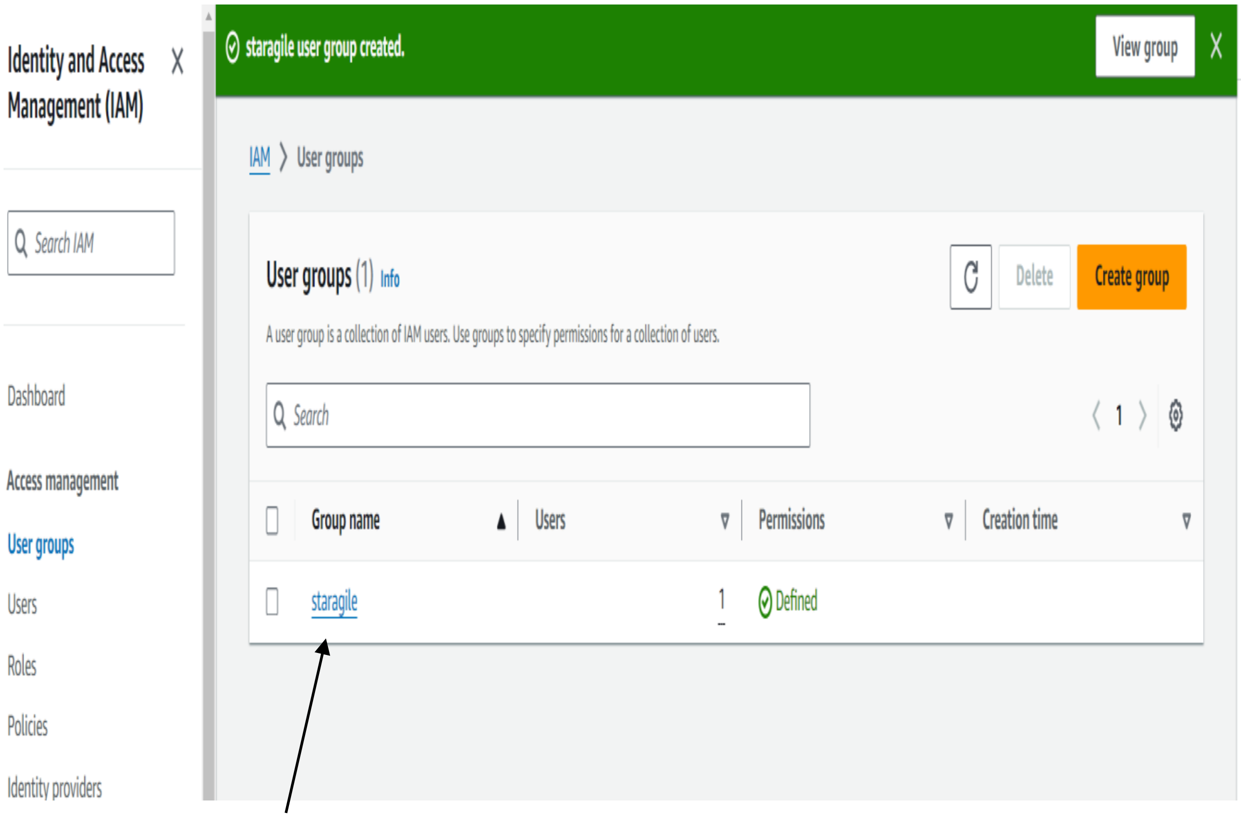
	Policy name	Type	Used as	Description
☑	AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services a
□	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permis
□	AdministratorAccess-AWSEla...	AWS managed	None	Grants account administrative permis
□	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaF
□	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusines
□	AlexaForBusinessGatewayExe...	AWS managed	None	Provide gateway execution access to
□	AlexaForBusinessLifesizeDele...	AWS managed	None	Provide access to Lifesize AVS device
□	AlexaForBusinessPolyDelegat...	AWS managed	None	Provide access to Poly AVS devices
□	AlexaForBusinessReadOnlyAc...	AWS managed	None	Provide read only access to AlexaForE

STEP 5: After attaching policies **Click** on create Group.



□	⊞	AlexaForBusinessLifesizeDele...	AWS managed	None	Provide access to Lifesize AVS devices
□	⊞	AlexaForBusinessPolyDelegat...	AWS managed	None	Provide access to Poly AVS devices
□	⊞	AlexaForBusinessReadOnlyAc...	AWS managed	None	Provide read only access to AlexaForE
□	⊞	AmazonAPIGatewayAdminist...	AWS managed	None	Provides full access to create/edit/de
□	⊞	AmazonAPIGatewayInvokeFu...	AWS managed	None	Provides full access to invoke APIs in
□	⊞	AmazonAPIGatewayPushToCl...	AWS managed	None	Allows API Gateway to push logs to u
□	⊞	AmazonAppFlowFullAccess	AWS managed	None	Provides full access to Amazon AppFl
□	⊞	AmazonAppFlowReadOnlyAc...	AWS managed	None	Provides read only access to Amazon
□	⊞	AmazonAppStreamFullAccess	AWS managed	None	Provides full access to Amazon AppSt
□	⊞	AmazonAppStreamPCAAccess	AWS managed	None	Amazon AppStream 2.0 access to AW
□	⊞	AmazonAppStreamReadOnly...	AWS managed	None	Provides read only access to Amazon
□	⊞	AmazonAppStreamServiceAc...	AWS managed	None	Default policy for Amazon AppStrean
□	⊞	AmazonAthenaFullAccess	AWS managed	None	Provide full access to Amazon Athena
□	⊞	AmazonAugmentedAIFullAcc...	AWS managed	None	Provides access to perform all operat

STEP 6: **Group** [staragile] got **Created.**



staragile user group created.

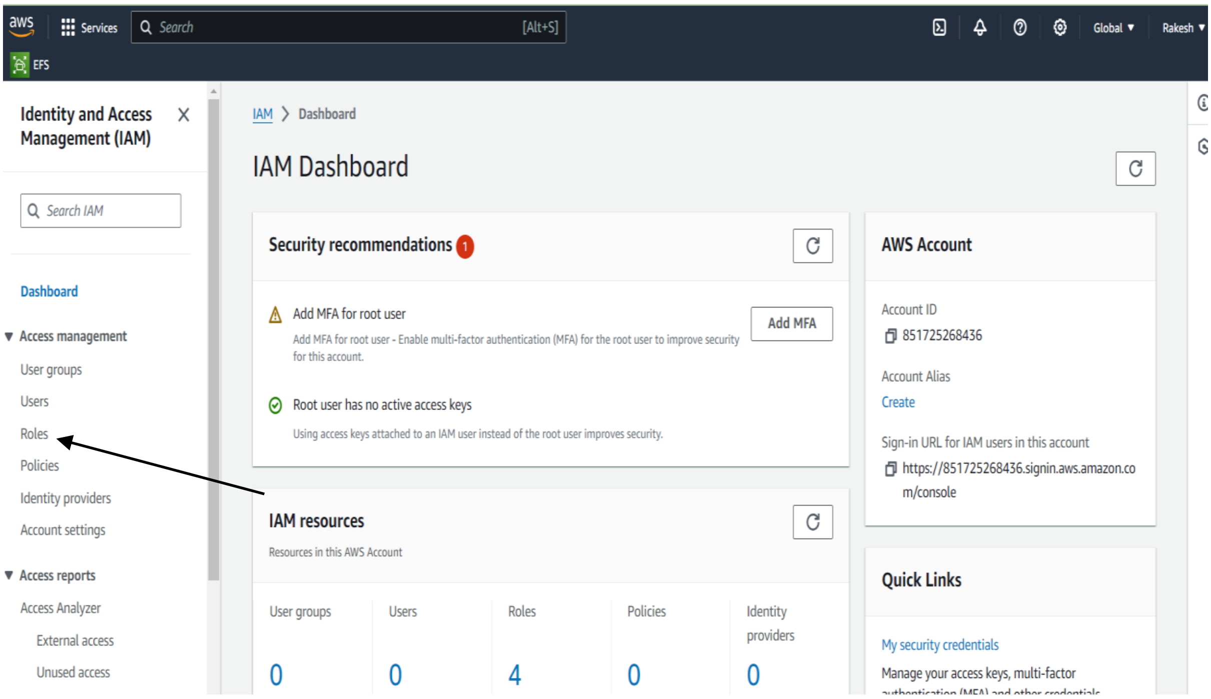
User groups (1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name ▲	Users ▿	Permissions ▿	Creation time ▿
□	staragile	1	✓ Defined	

CREATION OF IAM ROLE

STEP 1: In IAM Dashboard under **Access management** click on **ROLES.**



IAM Dashboard

Security recommendations 1

Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Add MFA

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	4	0	0

AWS Account

Account ID
851725268436

Account Alias
Create

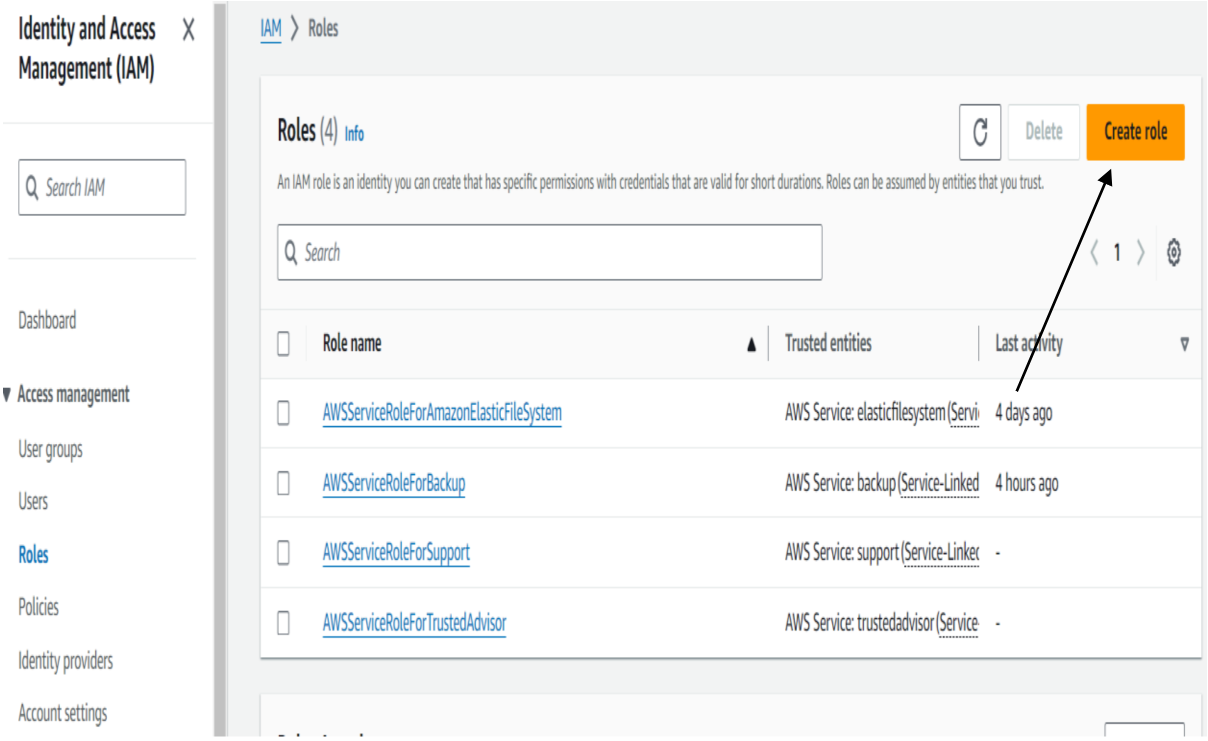
Sign-in URL for IAM users in this account
https://851725268436.signin.aws.amazon.com/console

Quick Links

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials

STEP 2: Click on **Create Role.**

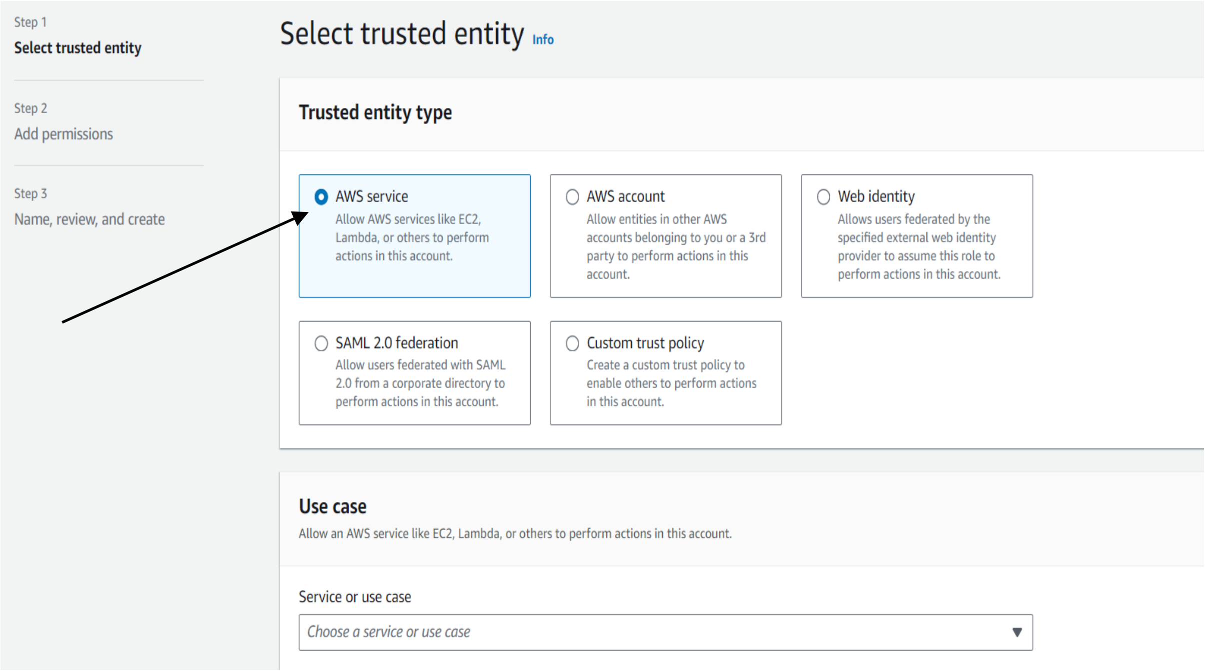


Roles (4) Info

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
□	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Servi	4 days ago
□	AWSServiceRoleForBackup	AWS Service: backup (Service-Linked	4 hours ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linkec	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-

STEP 3: In **Trusted entity type** Select **AWS service** as shown below.



Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

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

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

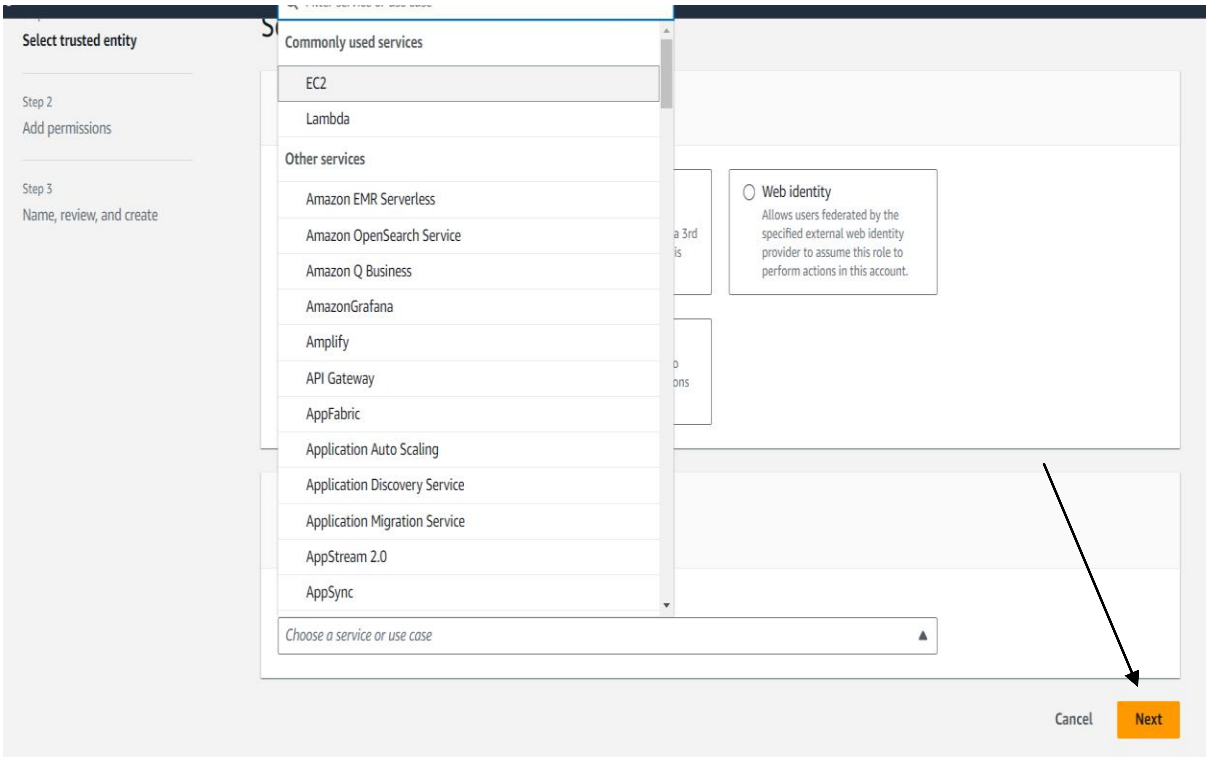
○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

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

Service or use case
Choose a service or use case ▼

STEP 4: In **use case** search any AWS sevice [EC2] and select.
And **click** on Next.



Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Commonly used services
EC2
Lambda
Other services
Amazon EMR Serverless
Amazon OpenSearch Service
Amazon Q Business
AmazonGrafana
Amplify
API Gateway
AppFabric
Application Auto Scaling
Application Discovery Service
Application Migration Service
AppStream 2.0
AppSync

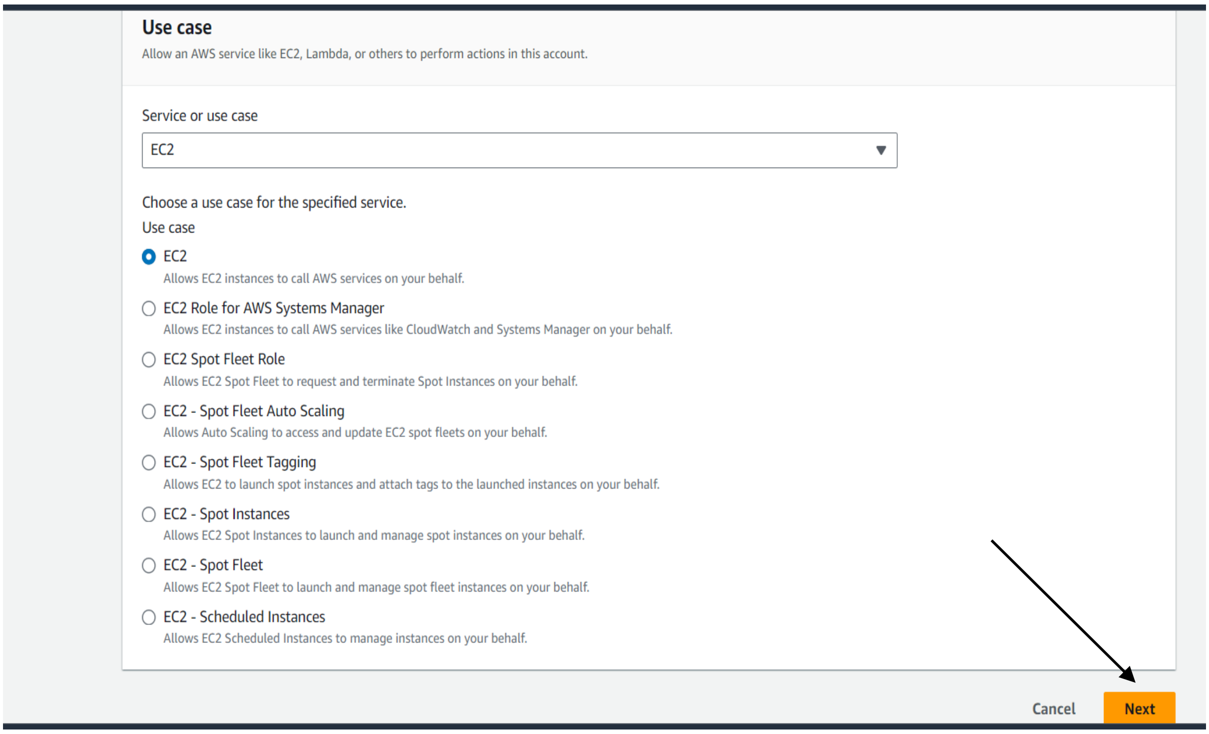
○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

Choose a service or use case ▲

Cancel Next

STEP 5: **Choose** for specified service as shown below .

And **Click** on Next.



Use case

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.

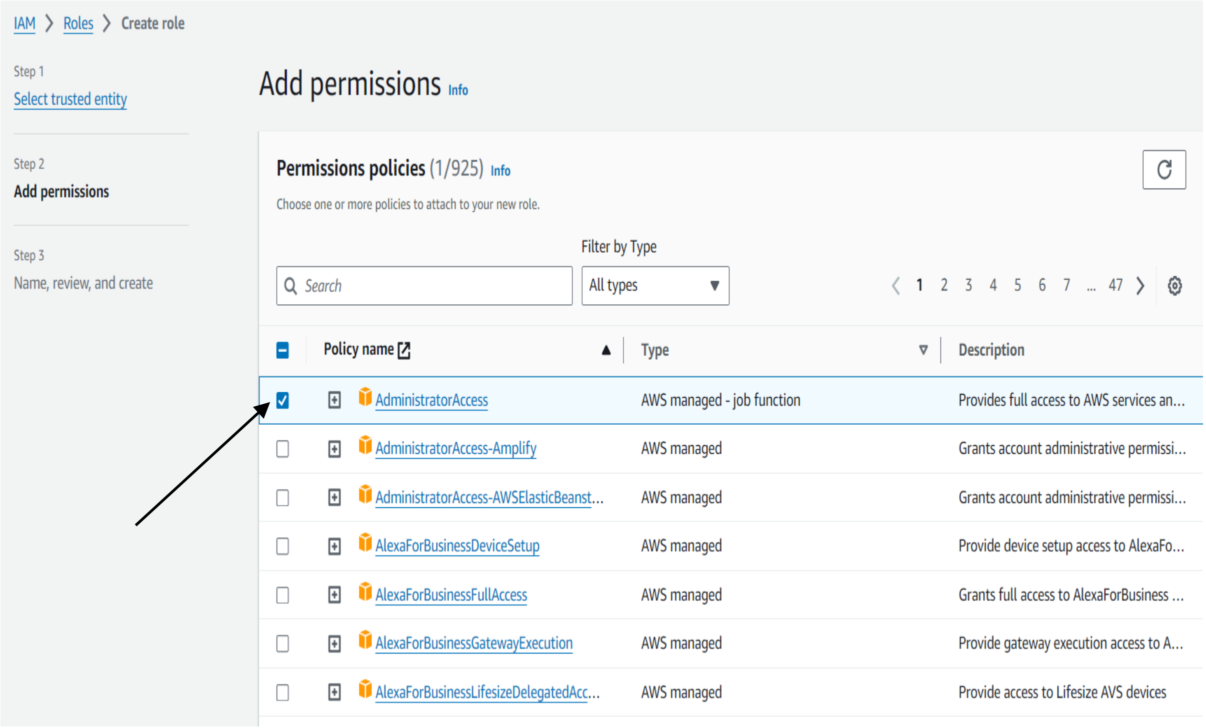
○ EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

○ 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.

STEP 6: In Add Permission attach any policies.



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

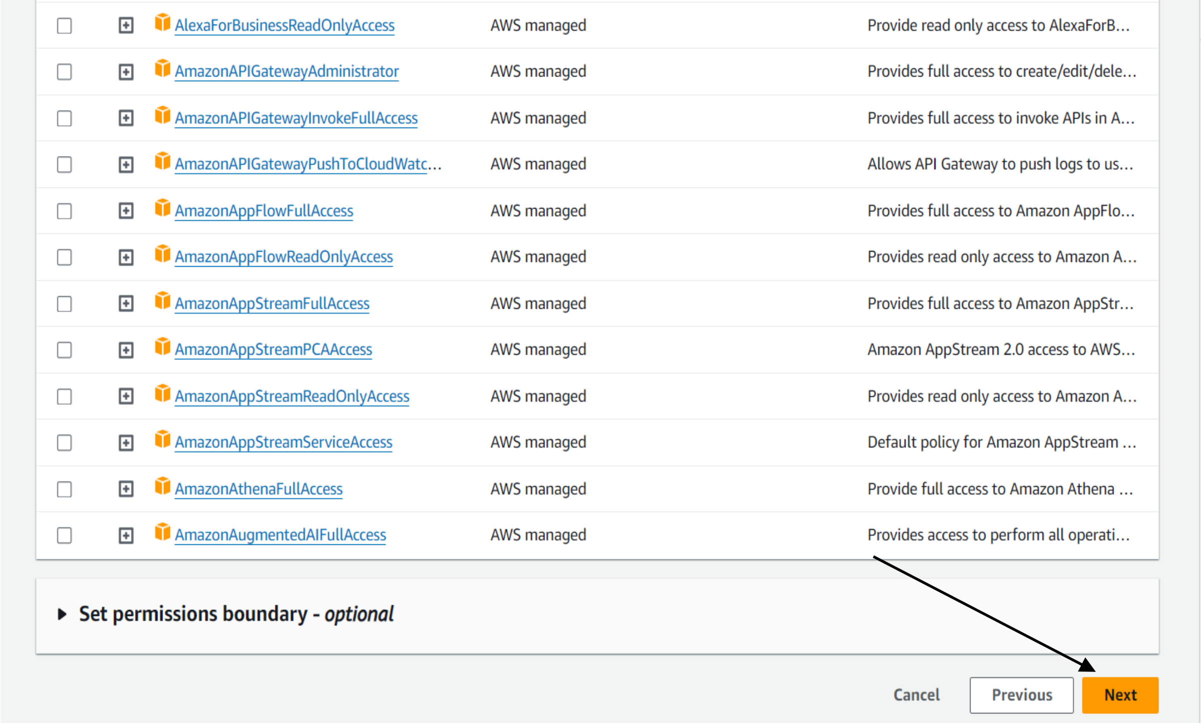
Permissions policies (1/925) Info

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

Filter by Type

☐	Policy name	Type	Description
☑	AdministratorAccess	AWS managed - job function	Provides full access to AWS services an...
☐	AdministratorAccess-Amplify	AWS managed	Grants account administrative permissi...
☐	AdministratorAccess-AWSElasticBeanst...	AWS managed	Grants account administrative permissi...
☐	AlexaForBusinessDeviceSetup	AWS managed	Provide device setup access to AlexaFo...
☐	AlexaForBusinessFullAccess	AWS managed	Grants full access to AlexaForBusiness ...
☐	AlexaForBusinessGatewayExecution	AWS managed	Provide gateway execution access to A...
☐	AlexaForBusinessLifesizeDelegatedAcc...	AWS managed	Provide access to Lifesize AVS devices

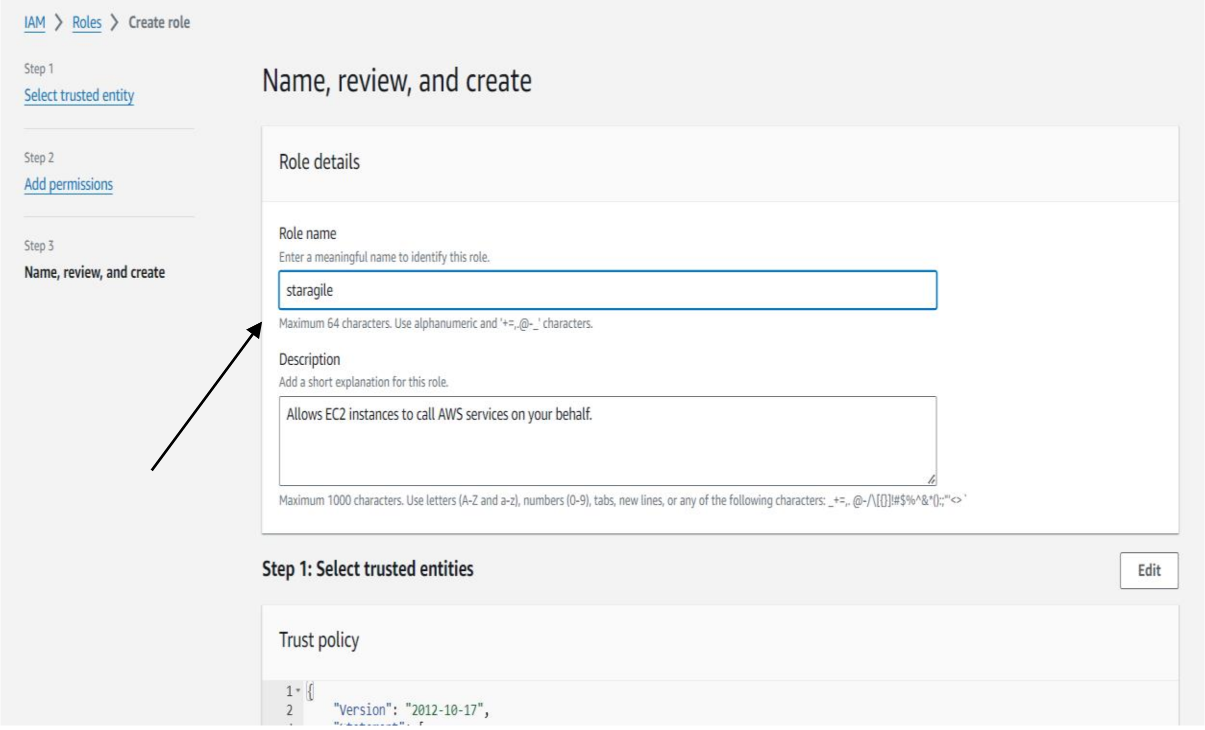
STEP 7: **Click** on Next.



□	⊞	AlexaForBusinessReadOnlyAccess	AWS managed	Provide read only access to AlexaForB...
□	⊞	AmazonAPIGatewayAdministrator	AWS managed	Provides full access to create/edit/dele...
□	⊞	AmazonAPIGatewayInvokeFullAccess	AWS managed	Provides full access to invoke APIs in A...
□	⊞	AmazonAPIGatewayPushToCloudWatc...	AWS managed	Allows API Gateway to push logs to us...
□	⊞	AmazonAppFlowFullAccess	AWS managed	Provides full access to Amazon AppFlo...
□	⊞	AmazonAppFlowReadOnlyAccess	AWS managed	Provides read only access to Amazon A...
□	⊞	AmazonAppStreamFullAccess	AWS managed	Provides full access to Amazon AppStr...
□	⊞	AmazonAppStreamPCAAccess	AWS managed	Amazon AppStream 2.0 access to AWS...
□	⊞	AmazonAppStreamReadOnlyAccess	AWS managed	Provides read only access to Amazon A...
□	⊞	AmazonAppStreamServiceAccess	AWS managed	Default policy for Amazon AppStream ...
□	⊞	AmazonAthenaFullAccess	AWS managed	Provide full access to Amazon Athena ...
□	⊞	AmazonAugmentedAIFullAccess	AWS managed	Provides access to perform all operati...

▸ Set permissions boundary - *optional*

STEP 8: In **Role details** type Role name [staragile].



Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
staragile
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

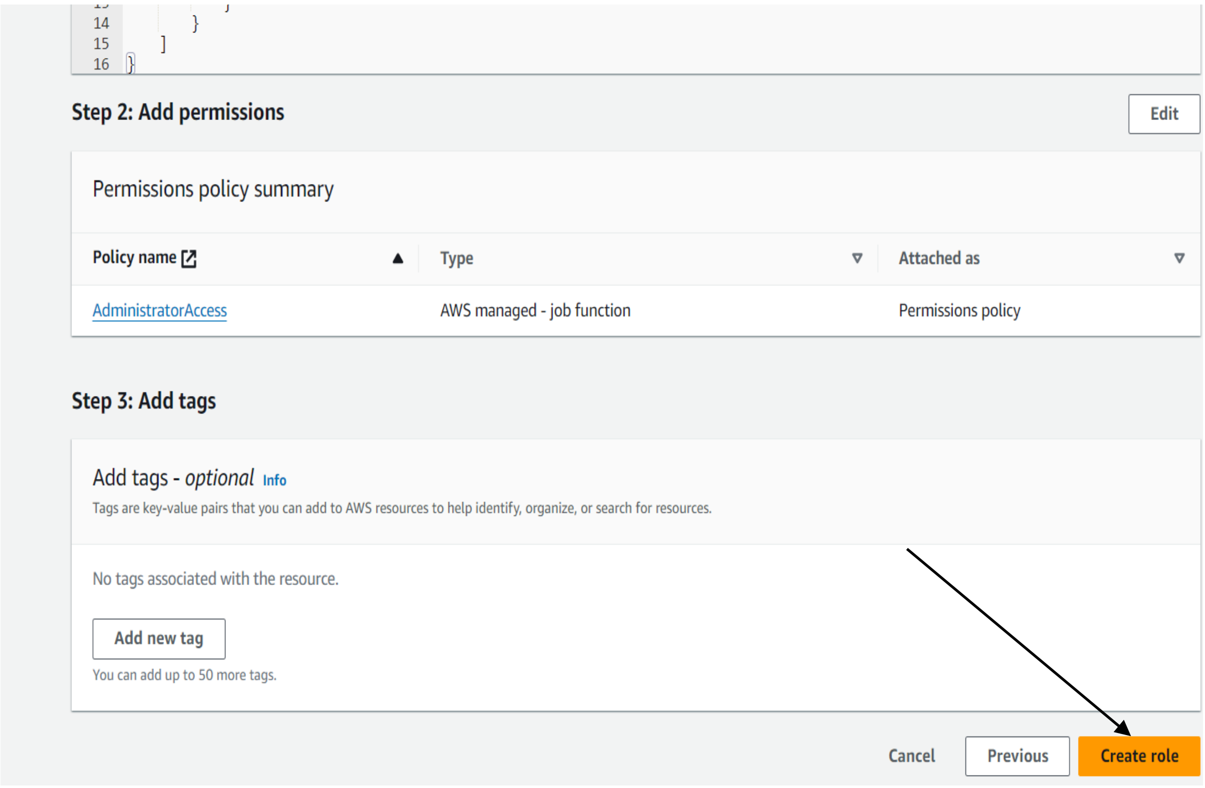
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^&*();:"'<>`

Step 1: Select trusted entities

Trust policy

```
{
    "Version": "2012-10-17",
```

STEP 9: **Click** on Create Role.



```
            }
        ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name ▲	Type	Attached as
AdministratorAccess	AWS managed - job function	Permissions policy

Step 3: Add tags

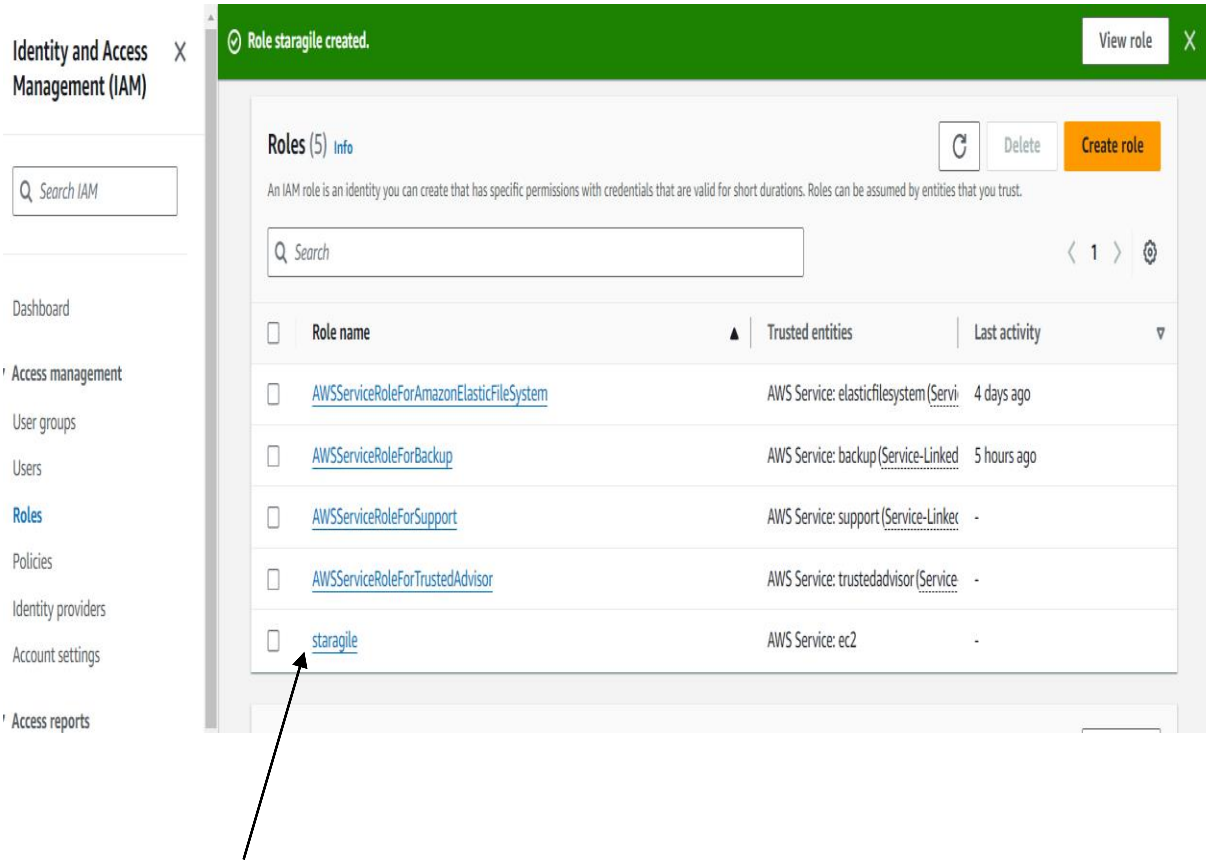
Add tags - *optional* Info

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.

You can add up to 50 more tags.

STEP 10: Role [staragile] got created.



Role staragile created.

Roles (5) 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
□	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Servi	4 days ago
□	AWSServiceRoleForBackup	AWS Service: backup (Service-Linked	5 hours ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linkec	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
□	staragile	AWS Service: ec2	-