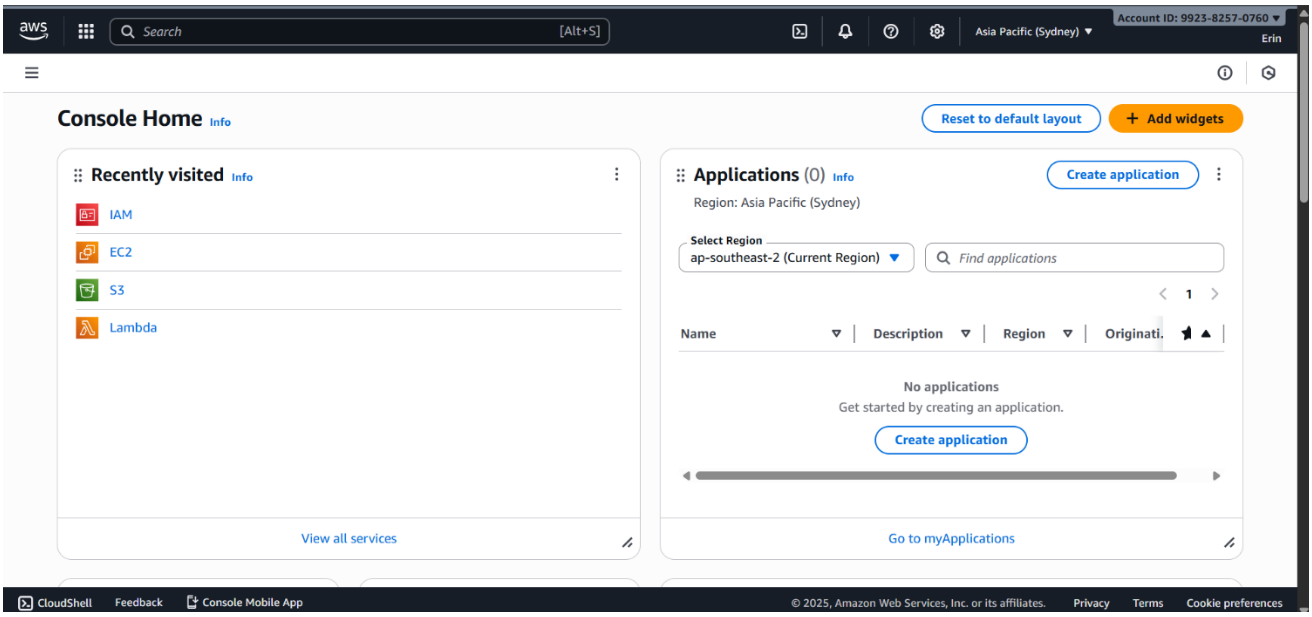
Practical:-5

Objective:- Creating **an** IAM (Identity and Access Management) user in AWS is to provide secure and controlled access to AWS resources for individuals or applications without using the root account.

Step 1: Sign in to AWS Console

Log in to your **AWS Management Console** using your **root account** or an **IAM user** who has **Administrator privileges**.



Region: Asia Pacific (Sydney)

Select Region: ap-southeast-2 (Current Region)

Find applications

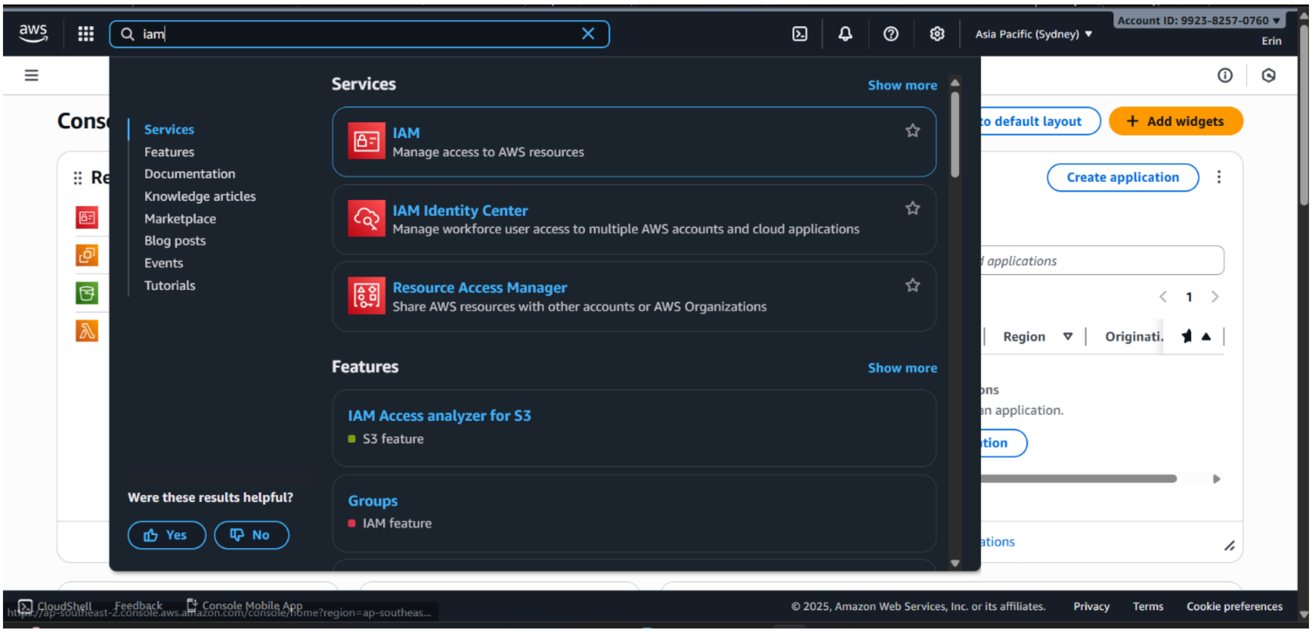
Name	Description	Region	Originati...

No applications

Get started by creating an application.

Step 2: Open IAM Service

In the search bar at the top, type **IAM**. Select **IAM (Identity and Access Management)**.



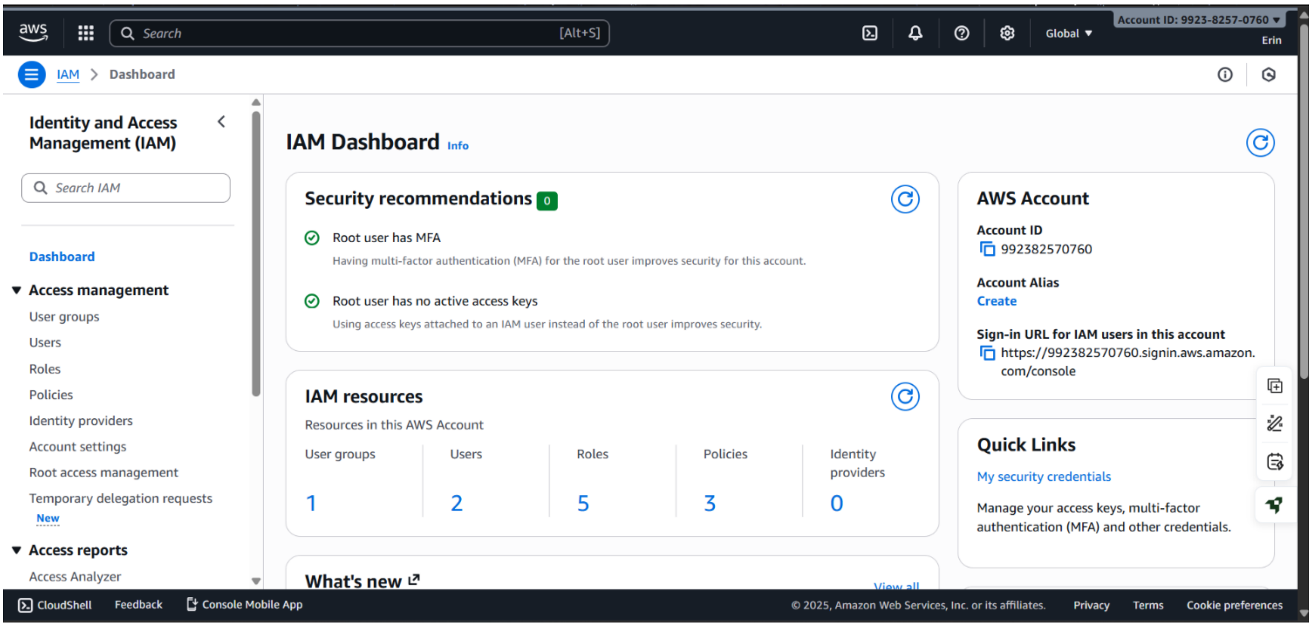
IAM
Manage access to AWS resources

IAM Identity Center
Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager
Share AWS resources with other accounts or AWS Organizations

IAM Access analyzer for S3
S3 feature

Groups
IAM feature



Security recommendations 0

✓ Root user has MFA
Having multi-factor authentication (MFA) for the root user improves 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
1	2	5	3	0

AWS Account

Account ID
992382570760

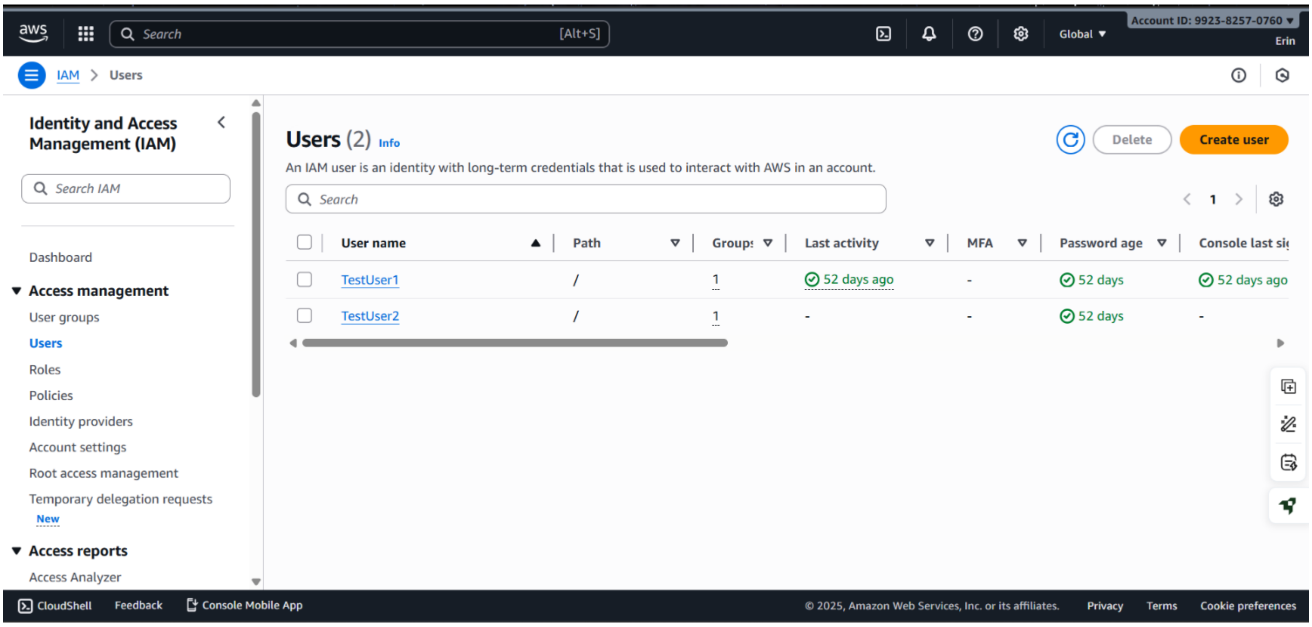
Account Alias
Create

Sign-in URL for IAM users in this account
https://992382570760.signin.aws.amazon.com/console

Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Step 3: Go to Users Section

In the left sidebar, click on **Users**. You will see a list of all existing users. Click **“Create user”** to add a new one.



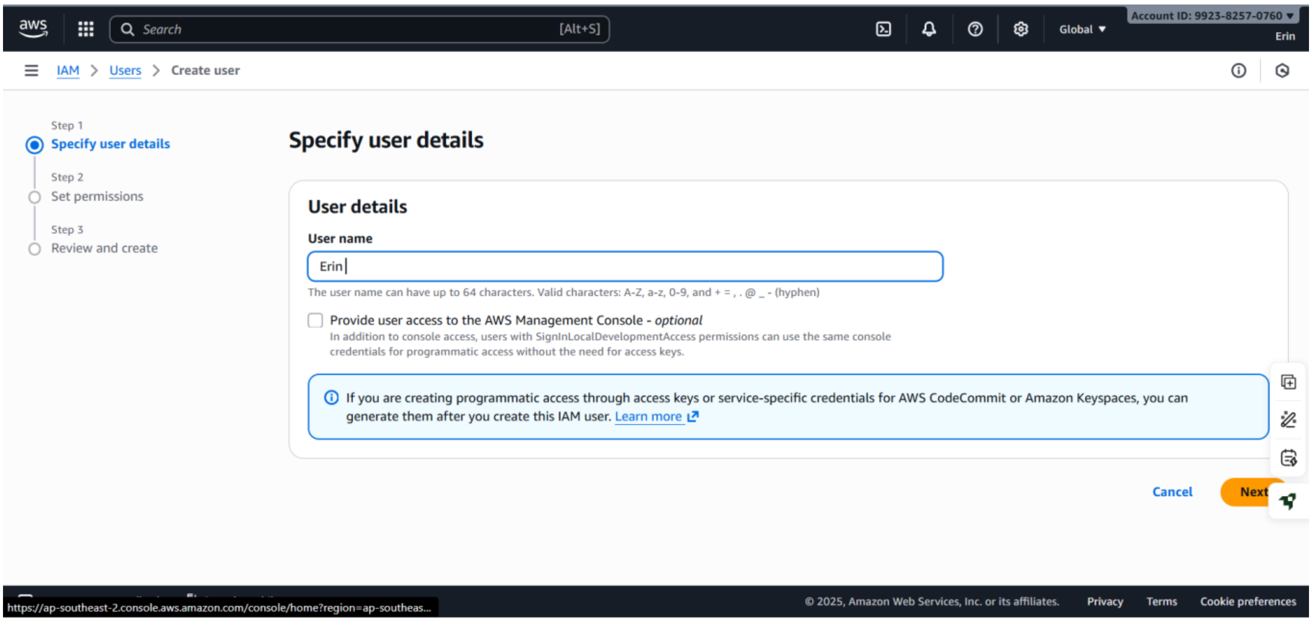
Users (2) Info

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 si
□	TestUser1	/	1	52 days ago	-	52 days	52 days ago
□	TestUser2	/	1	-	-	52 days	-

Step 4: Enter User Details

Enter a **User name** . Choose the type of access: **Password access** → if the user needs to log in to the AWS Console. Click **Next**.


aws
Search [Alt+S]
Global ▾
Account ID: 9923-8257-0760 ▾
Erin
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Cancel
Next
https://ap-southeast-2.console.aws.amazon.com/console/home?region=ap-southeas...
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Specify user details

User details

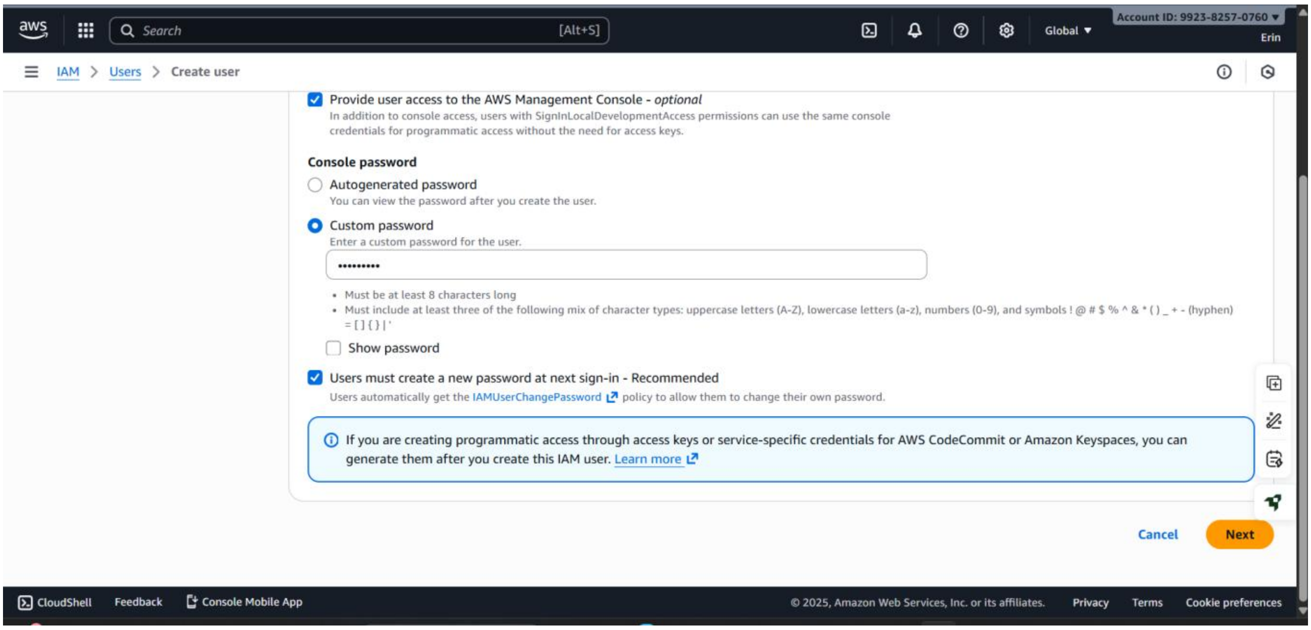
User name

Erin

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*
In addition to console access, users with SignInLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.

ⓘ 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



☑ Provide user access to the AWS Management Console - *optional*
In addition to console access, users with SignInLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.

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

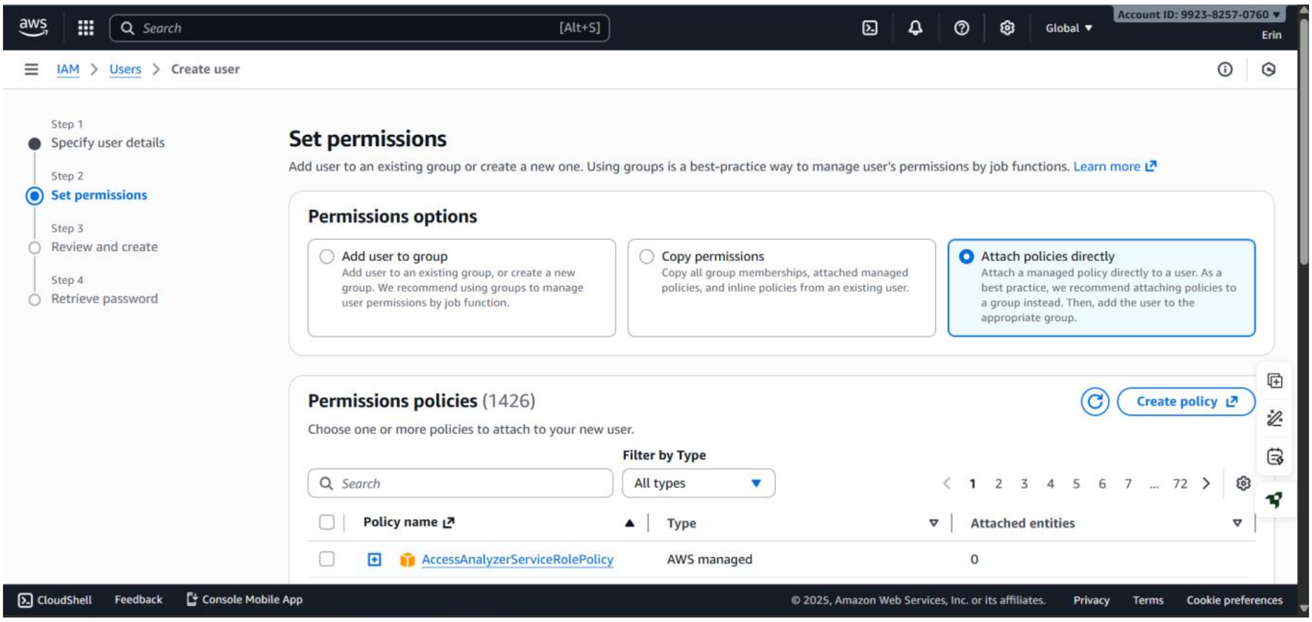
☑ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

ⓘ 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 5: Set Permissions

Choose **Attach policies directly** → assign permissions manually (e.g., `AmazonS3FullAccess`, `AdministratorAccess`, etc.).

Then click **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.

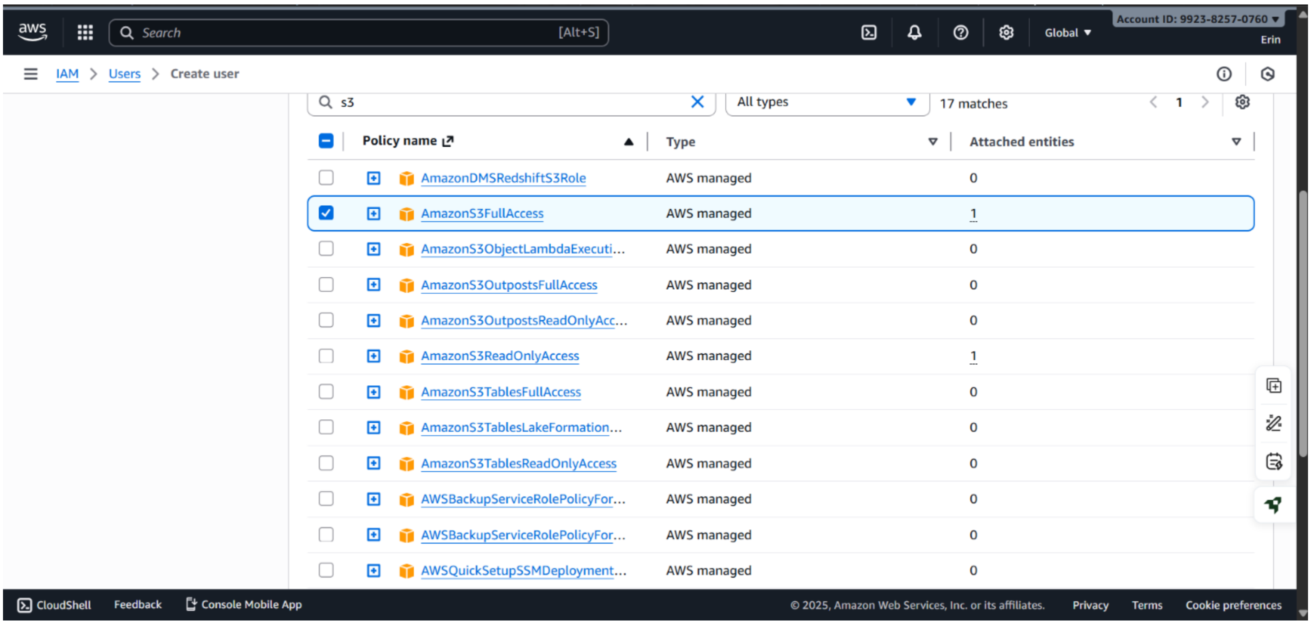
● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1426)

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

Filter by Type: All types

□	Policy name	Type	Attached entities
□	AccessAnalyzerServiceRolePolicy	AWS managed	0



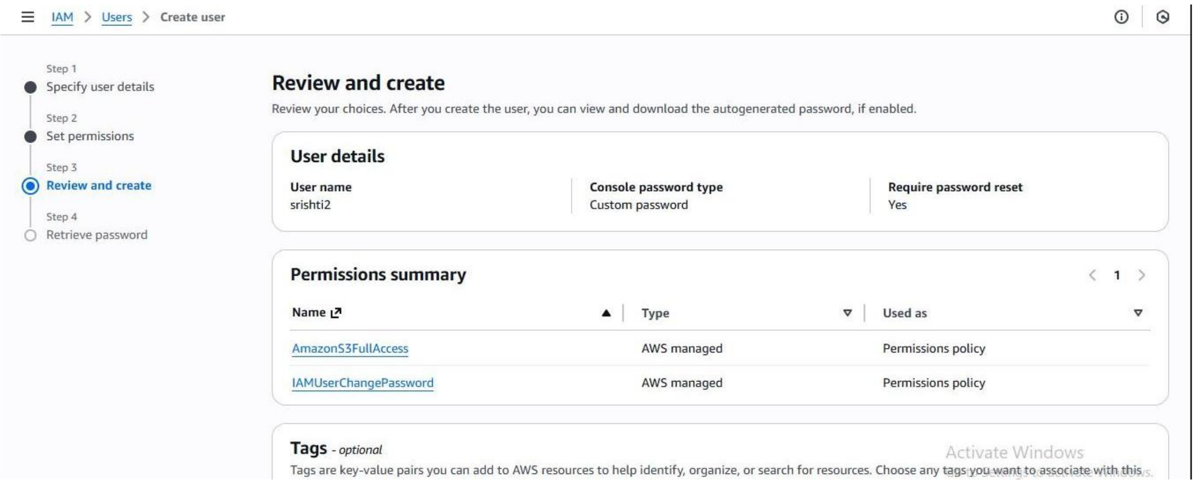
aws
Search [Alt+S]
Global ▾
Account ID: 9923-8257-0760 ▾
Erin
IAM > Users > Create user
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

s3 | All types | 17 matches | 1

	Policy name	Type	Attached entities
□	AmazonDMSRedshiftS3Role	AWS managed	0
☑	AmazonS3FullAccess	AWS managed	1
□	AmazonS3ObjectLambdaExecuti…	AWS managed	0
□	AmazonS3OutpostsFullAccess	AWS managed	0
□	AmazonS3OutpostsReadOnlyAcc…	AWS managed	0
□	AmazonS3ReadOnlyAccess	AWS managed	1
□	AmazonS3TablesFullAccess	AWS managed	0
□	AmazonS3TablesLakeFormation…	AWS managed	0
□	AmazonS3TablesReadOnlyAccess	AWS managed	0
□	AWSBackupServiceRolePolicyFor…	AWS managed	0
□	AWSBackupServiceRolePolicyFor…	AWS managed	0
□	AWSQuickSetupSSMDeployment…	AWS managed	0

Step 6: Review and Create

Review all details carefully. Click **Create user**.



Review and create

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

User details

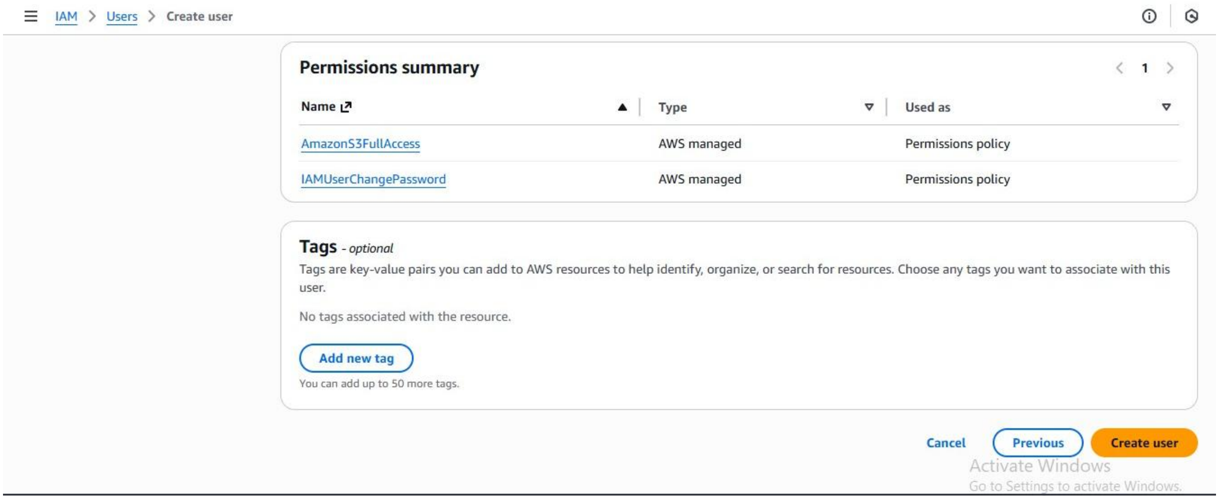
User name	Console password type	Require password reset
srishti2	Custom password	Yes

Permissions summary

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy
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



Permissions summary

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

Tags - *optional*

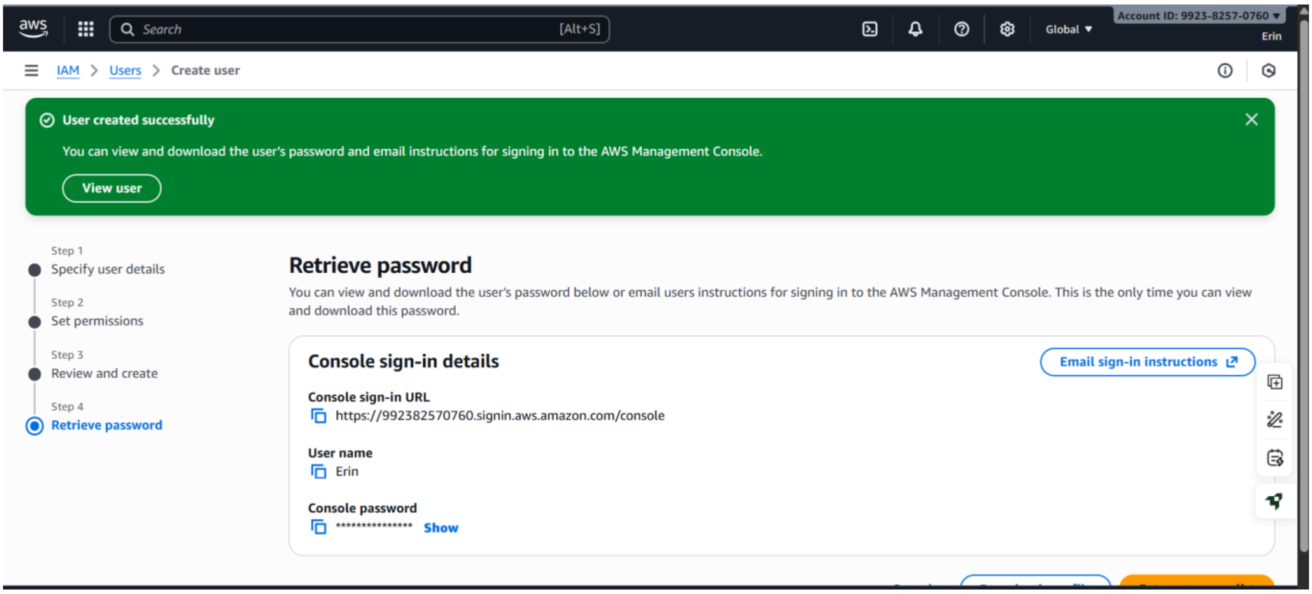
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

You can add up to 50 more tags.

Step 7: Save Login Details

- Once the user is created, AWS will show:
  - **User ARN (Amazon Resource Name)**
  - **Console login link**
  - **Password or Access key/Secret key** (Download the `.csv` file — it won't be shown again).



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

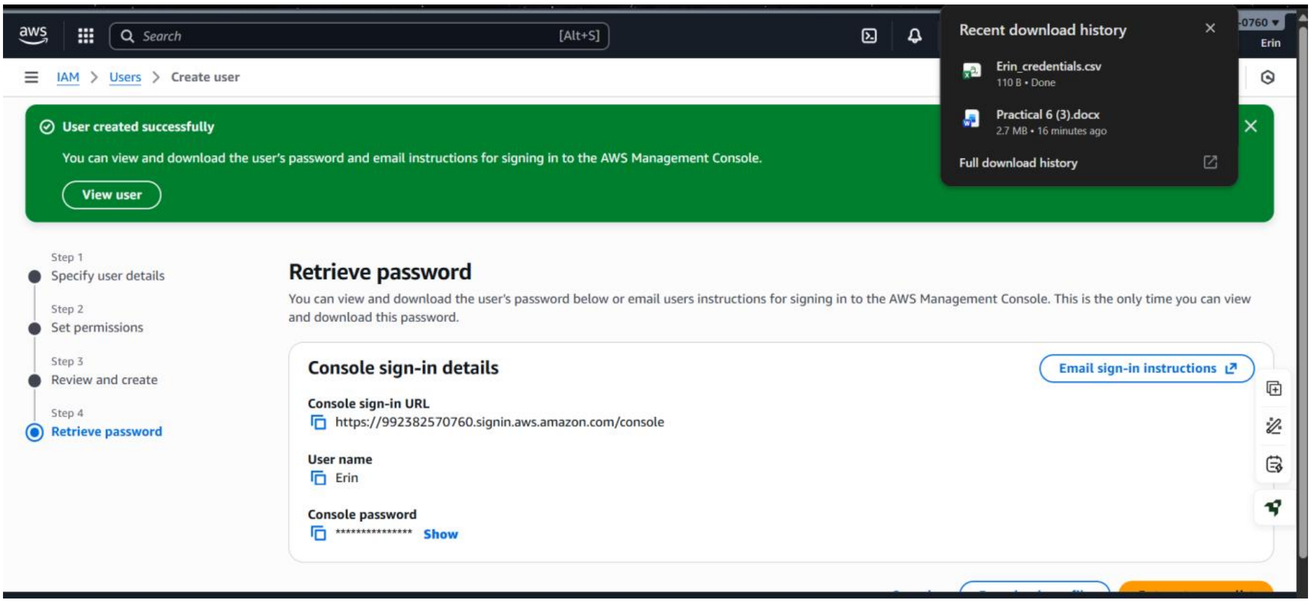
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL
https://992382570760.signin.aws.amazon.com/console

User name
Erin

Console password
*************** Show



Recent download history

Erin_credentials.csv
110 B • Done

Practical 6 (3).docx
2.7 MB • 16 minutes ago

Full download history

User created successfully

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

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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://992382570760.signin.aws.amazon.com/console

User name
Erin

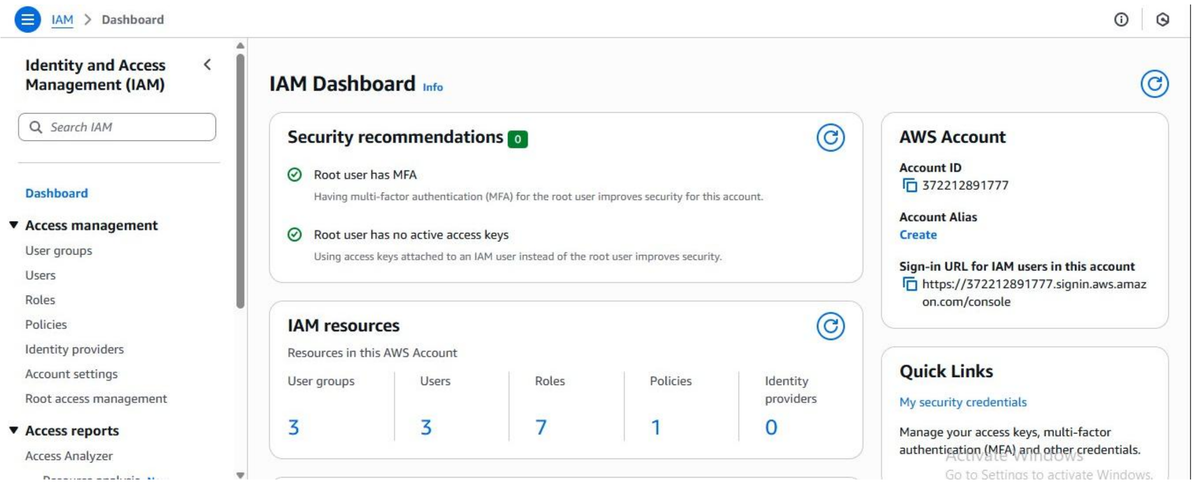
Console password
****

Practical:-7

Objective: To create a user group in AWS IAM in order to manage permissions collectively for multiple users having similar roles or responsibilities.

Step1:- Open the IAM Service:

In the search bar at the top of the console, type **IAM**, then select **Identity and Access Management** from the results.



IAM > Dashboard

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

▼ Access reports

Access Analyzer

IAM Dashboard Info

Security recommendations 0

✓ Root user has MFA

Having multi-factor authentication (MFA) for the root user improves 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
3	3	7	1	0

AWS Account

Account ID

372212891777

Account Alias

Create

Sign-in URL for IAM users in this account

https://372212891777.signin.aws.amazon.com/console

Quick Links

My security credentials

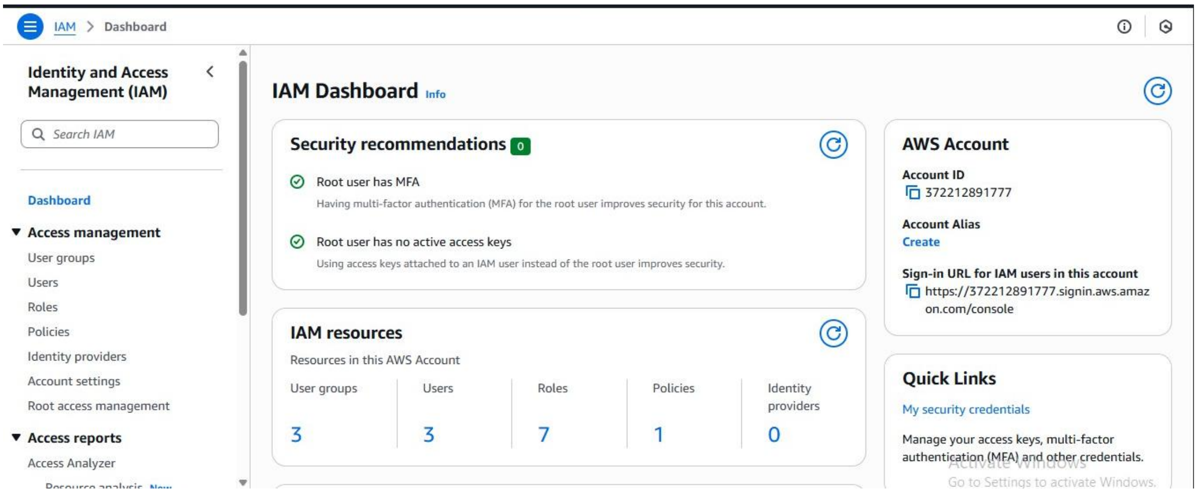
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Activate Windows

Go to Settings to activate Windows.

Step 2:- Go to User Groups Section:

In the left-hand sidebar, click on **User groups**.



IAM > Dashboard

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

▼ Access reports

Access Analyzer

Resource analysis New

IAM Dashboard Info

Security recommendations 0

✓ Root user has MFA

Having multi-factor authentication (MFA) for the root user improves 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
3	3	7	1	0

AWS Account

Account ID

372212891777

Account Alias

Create

Sign-in URL for IAM users in this account

https://372212891777.signin.aws.amazon.com/console

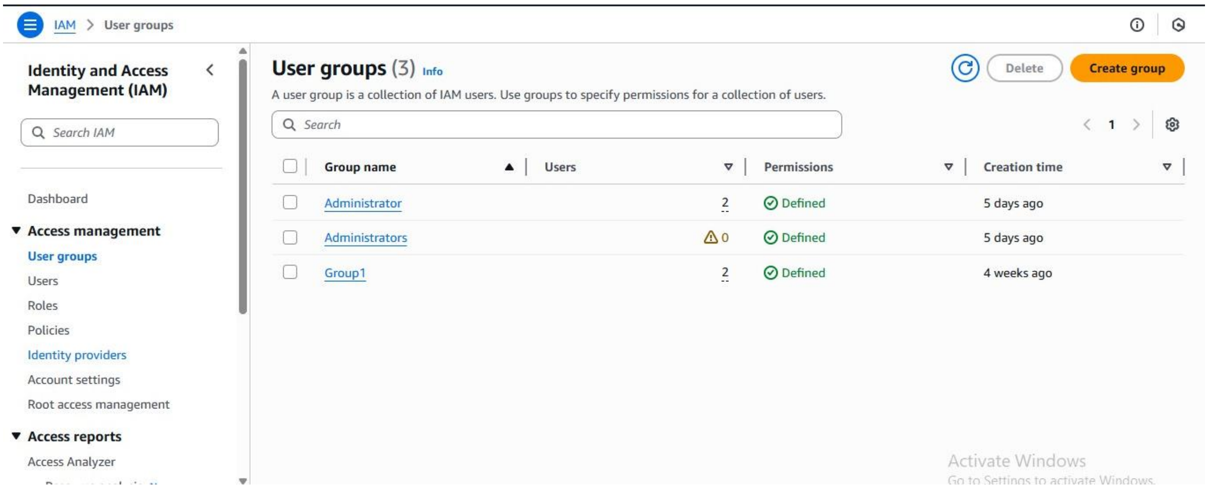
Quick Links

My security credentials

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

Activate Windows

Go to Settings to activate Windows.



User groups (3) 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
□	Administrator	2	✓ Defined	5 days ago
□	Administrators	⚠ 0	✓ Defined	5 days ago
□	Group1	2	✓ Defined	4 weeks ago

Step 3:- Click on “Create group”:

On the User Groups page, click the **“Create group”** button to start creating a new group

Step 4:- Enter Group Name:

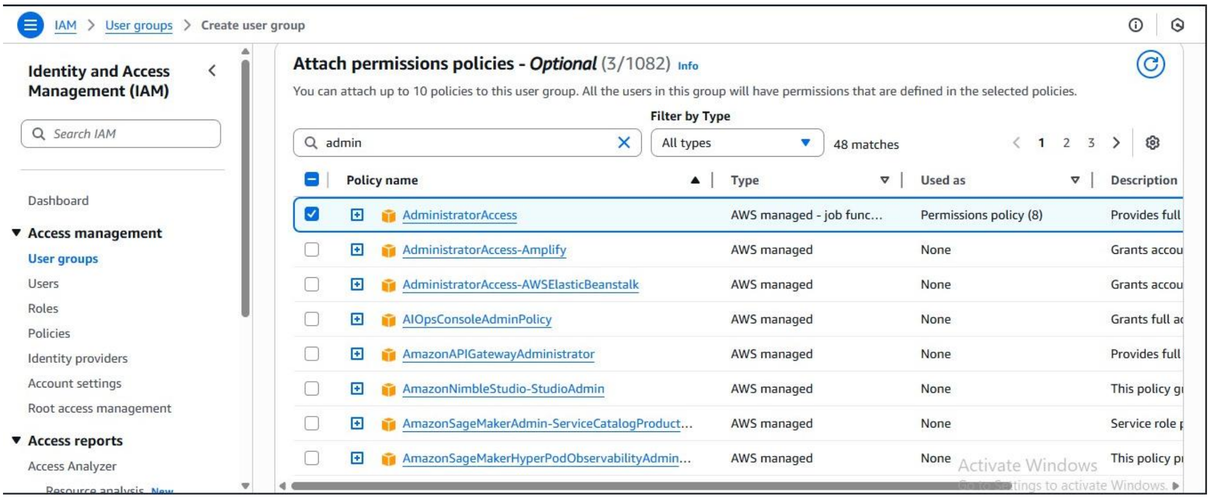
Type a **unique name** for your group (for example, *Developers*, *Admins*, or *ReadOnlyUsers*).

Step 5:- Attach Permissions Policies (Optional):

You can choose policies to attach to this group, such as:

- `AmazonS3FullAccess`
- `AmazonEC2ReadOnlyAccess`
- `AdministratorAccess`

If you want to add permissions later, you can **skip this step** and click **Next**.



IAM > User groups > Create user group

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

▼ Access reports

Access Analyzer

Resource analysis New

Attach permissions policies - *Optional* (3/1082) 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

admin | All types | 48 matches | < 1 2 3 >

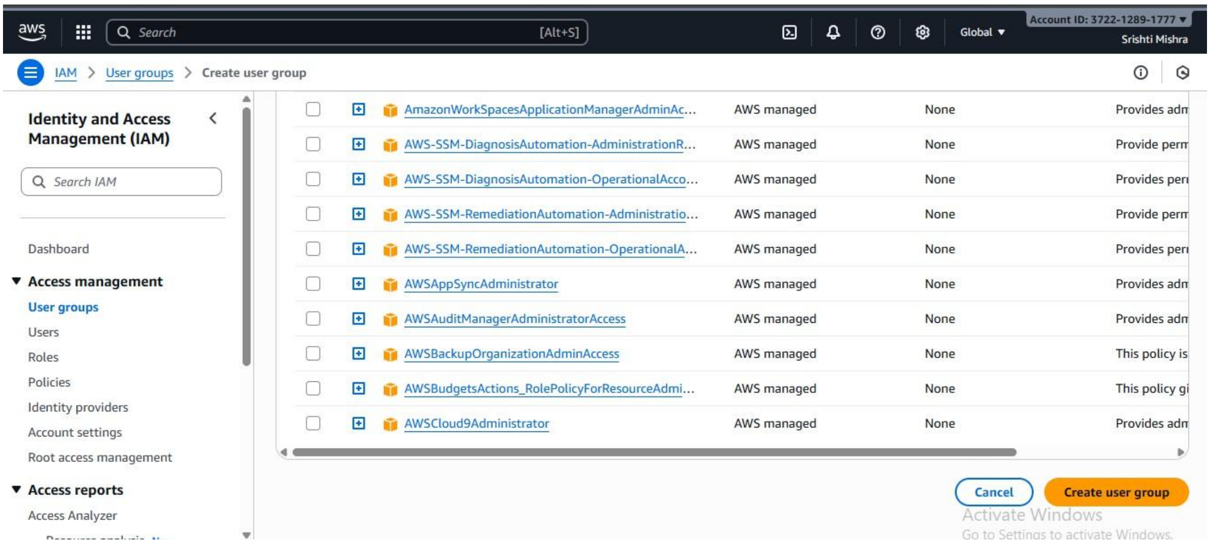
☐	Policy name	Type	Used as	Description
☑	AdministratorAccess	AWS managed - job func...	Permissions policy (8)	Provides full
☐	AdministratorAccess-Amplify	AWS managed	None	Grants accou
☐	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants accou
☐	AIOpsConsoleAdminPolicy	AWS managed	None	Grants full ac
☐	AmazonAPIGatewayAdministrator	AWS managed	None	Provides full
☐	AmazonNimbleStudio-StudioAdmin	AWS managed	None	This policy gi
☐	AmazonSageMakerAdmin-ServiceCatalogProduct...	AWS managed	None	Service role f
☐	AmazonSageMakerHyperPodObservabilityAdmin...	AWS managed	None	This policy pi

Step 6:- Add Users to the Group (Optional):

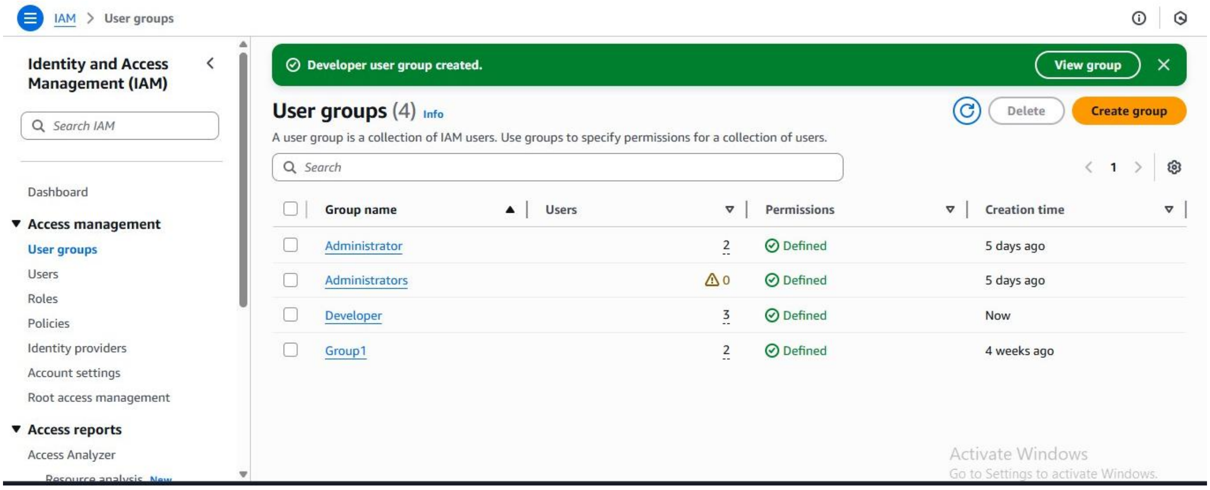
You can select existing IAM users to include in this group now, or you can add users later after creating the group.

Step 7:- Review and Create Group:

Review the group details and attached policies, then click **Create group**.



□	AmazonWorkSpacesApplicationManagerAdminAc…	AWS managed	None	Provides adm
□	AWS-SSM-DiagnosisAutomation-AdministrationR…	AWS managed	None	Provide perm
□	AWS-SSM-DiagnosisAutomation-OperationalAcco…	AWS managed	None	Provides per
□	AWS-SSM-RemediationAutomation-Administratio…	AWS managed	None	Provide perm
□	AWS-SSM-RemediationAutomation-OperationalA…	AWS managed	None	Provides per
□	AWSAppSyncAdministrator	AWS managed	None	Provides adm
□	AWSAuditManagerAdministratorAccess	AWS managed	None	Provides adm
□	AWSBackupOrganizationAdminAccess	AWS managed	None	This policy is
□	AWSBudgetsActions_RolePolicyForResourceAdmi…	AWS managed	None	This policy gi
□	AWSCloud9Administrator	AWS managed	None	Provides adm



✓ Developer user group created.

User groups (4) Info

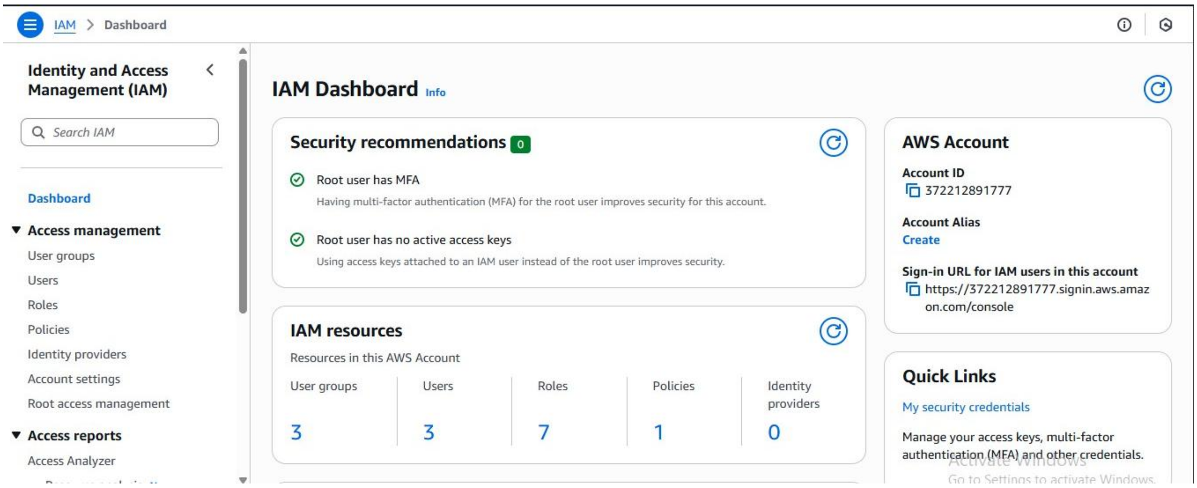
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name	Users	Permissions	Creation time
□	Administrator	2	✓ Defined	5 days ago
□	Administrators	⚠ 0	✓ Defined	5 days ago
□	Developer	3	✓ Defined	Now
□	Group1	2	✓ Defined	4 weeks ago

Practical:-8

Objective:-To create a security role in AWS IAM that allows AWS services or users to securely access specific AWS resources with defined permissions, ensuring controlled and temporary access without sharing long-term credentials.

Step 1:- Open the IAM Service:
In the search bar at the top of the console, type **IAM**, then select **Identity and Access Management** from the results.



IAM Dashboard Info

Security recommendations 0

Root user has MFA
Having multi-factor authentication (MFA) for the root user improves 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.

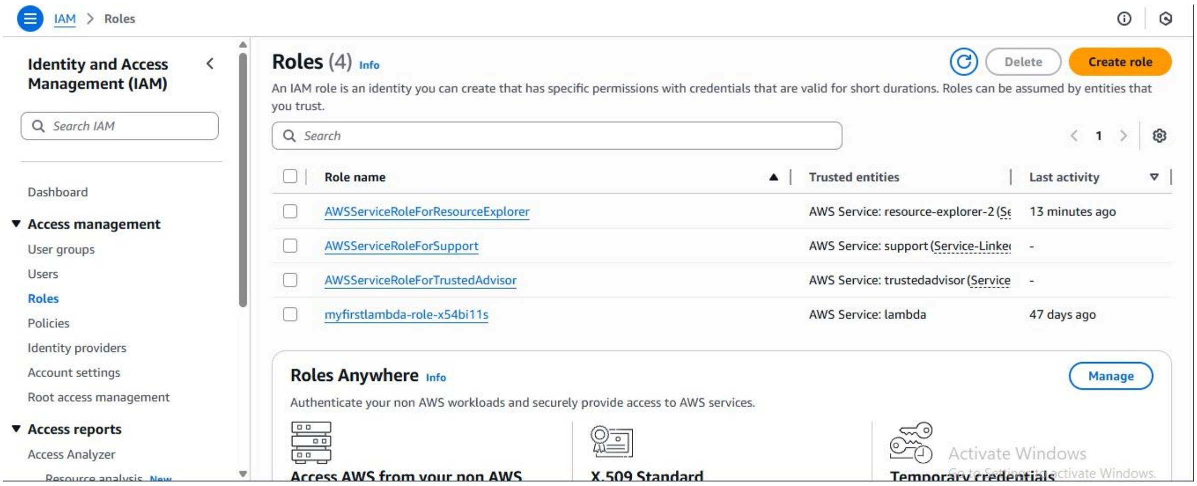
IAM resources
Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
3	3	7	1	0

AWS Account
Account ID
372212891777
Account Alias
Create
Sign-in URL for IAM users in this account
https://372212891777.signin.aws.amazon.com/console

Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Step 2:- Go to Roles Section:
In the left-hand navigation pane, click on **Roles**.



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.

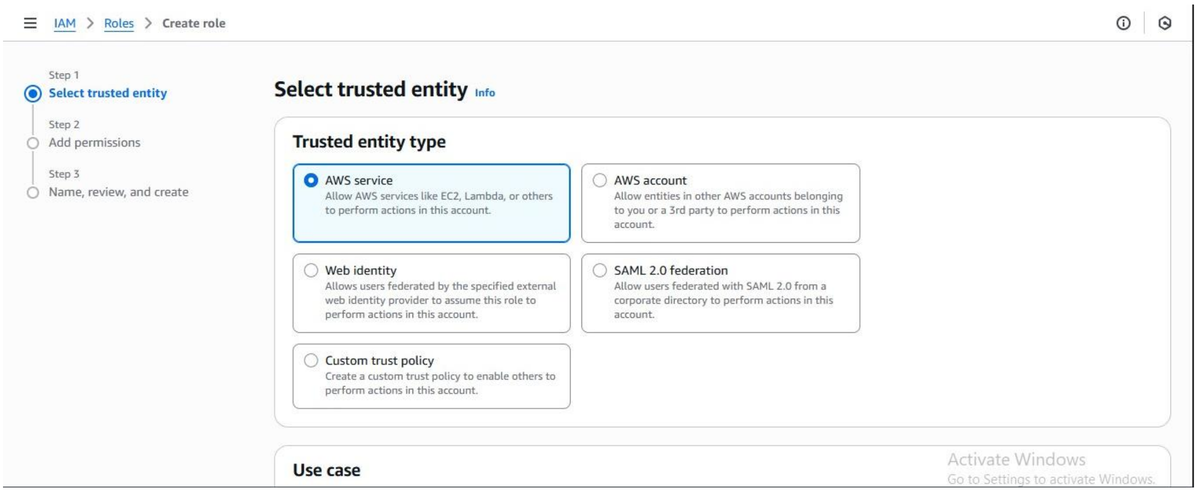
□	Role name	Trusted entities	Last activity
□	AWSServiceRoleForResourceExplorer	AWS Service: resource-explorer-2 (Se	13 minutes ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
□	myfirstlambda-role-x54bi11s	AWS Service: lambda	47 days ago

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

Access AWS from your non AWS
X.509 Standard
Temporary credentials

Step 3:- Click on "Create role":

On the Roles page, click the **"Create role"** button to start the process.


IAM > Roles > Create role
Activate Windows
Go to Settings to activate Windows.

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.

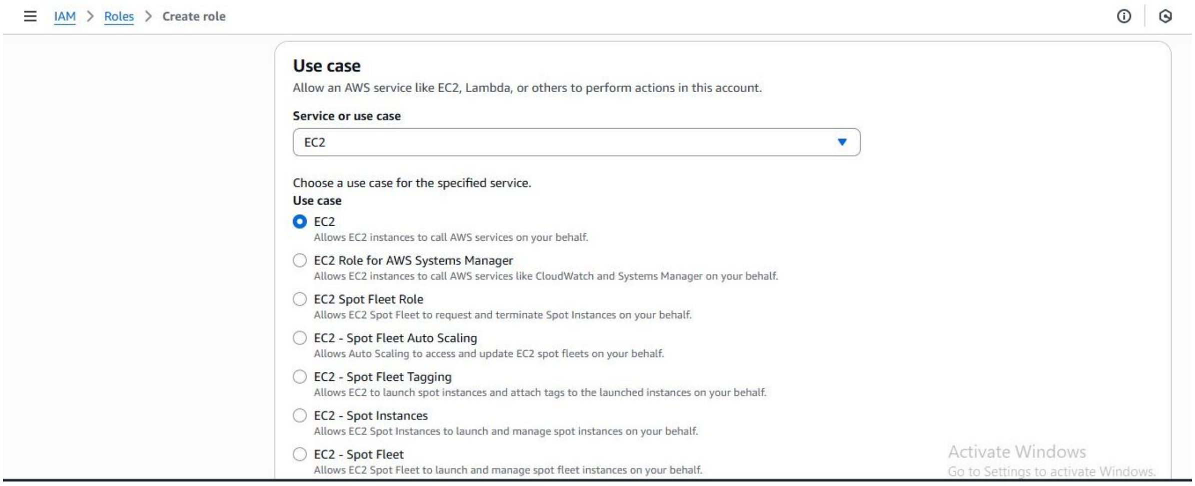
Use case

Step 4:- Select Trusted Entity Type:

Choose who will use the role, such as:

- **AWS Service** (e.g., EC2, Lambda)
- **Another AWS Account**
- **Web Identity** or **SAML 2.0 Federation**

Click **Next** after selecting the appropriate option.


IAM > Roles > Create role
Activate Windows
Go to Settings to activate Windows.

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.

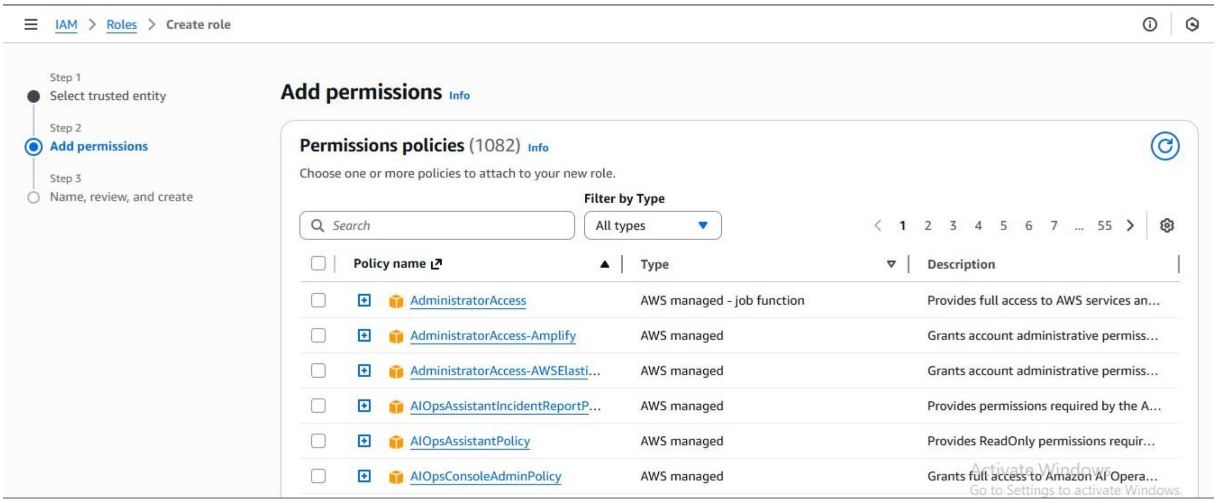
○ EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

○ 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.

Step 5:-Attach Permissions Policies:

Select the **permissions policies** that define what actions the role can perform (for example, `AmazonS3FullAccess` or `AmazonEC2FullAccess`).



IAM > Roles > Create role

Step 1 Select trusted entity
Step 2 Add permissions
Step 3 Name, review, and create

Add permissions Info

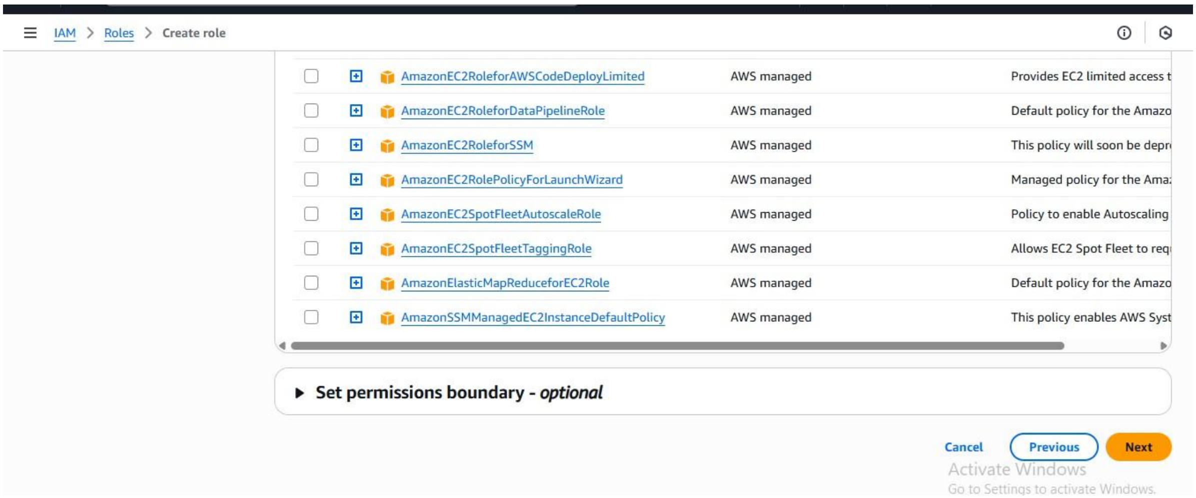
Permissions policies (1082) Info

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

Filter by Type: All types

< 1 2 3 4 5 6 7 ... 55 >

☐	Policy name	Type	Description
☐	AdministratorAccess	AWS managed - job function	Provides full access to AWS services an...
☐	AdministratorAccess-Amplify	AWS managed	Grants account administrative permiss...
☐	AdministratorAccess-AWSElasti...	AWS managed	Grants account administrative permiss...
☐	AIOpsAssistantIncidentReportP...	AWS managed	Provides permissions required by the A...
☐	AIOpsAssistantPolicy	AWS managed	Provides ReadOnly permissions requir...
☐	AIOpsConsoleAdminPolicy	AWS managed	Grants full access to Amazon AI Opera...



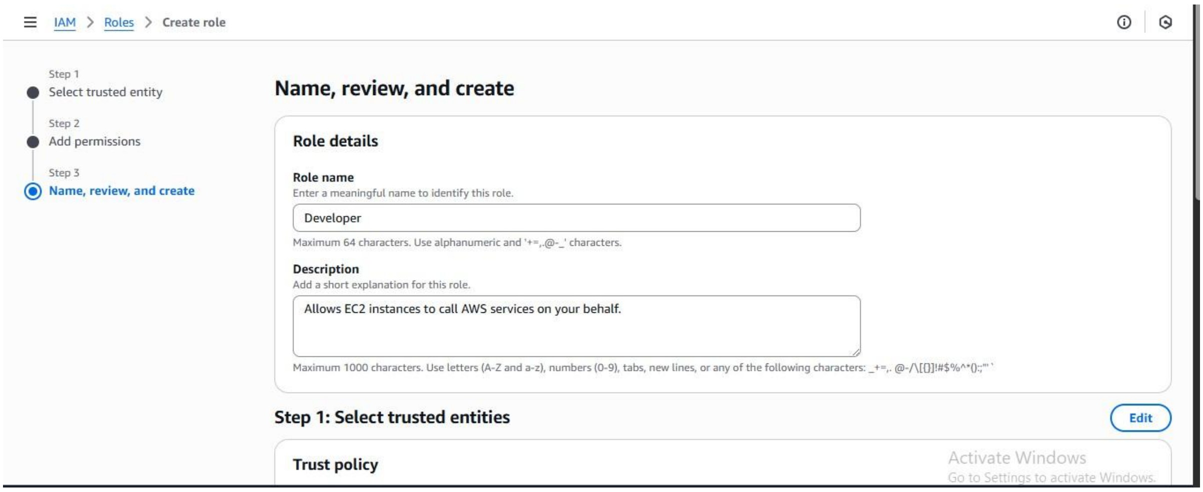
IAM > Roles > Create role

☐	Policy name	Type	Description
☐	AmazonEC2RoleforAWSCodeDeployLimited	AWS managed	Provides EC2 limited access t
☐	AmazonEC2RoleforDataPipelineRole	AWS managed	Default policy for the Amazo
☐	AmazonEC2RoleforSSM	AWS managed	This policy will soon be depr
☐	AmazonEC2RolePolicyForLaunchWizard	AWS managed	Managed policy for the Ama:
☐	AmazonEC2SpotFleetAutoscaleRole	AWS managed	Policy to enable Autoscaling
☐	AmazonEC2SpotFleetTaggingRole	AWS managed	Allows EC2 Spot Fleet to req
☐	AmazonElasticMapReduceforEC2Role	AWS managed	Default policy for the Amazo
☐	AmazonSSMManagedEC2InstanceDefaultPolicy	AWS managed	This policy enables AWS Syst

▸ Set permissions boundary - *optional*

Step 6:- Name and Review the Role:

Enter a **role name** (for example, *EC2SecurityRole* or *LambdaAccessRole*) and review all selected settings.



Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

Developer

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description

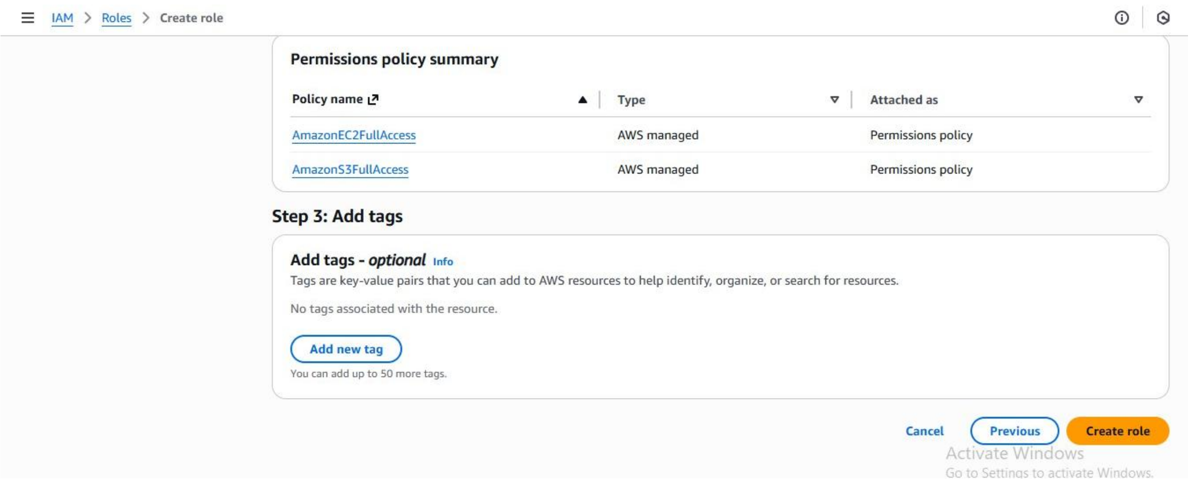
Add a short explanation for this role.

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



IAM > Roles > Create role
Add new tag
Cancel
Previous
Create role
Activate Windows
Go to Settings to activate Windows.

Permissions policy summary

Policy name	Type	Attached as
AmazonEC2FullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy

Step 3: Add tags

Add tags - *optional* Info

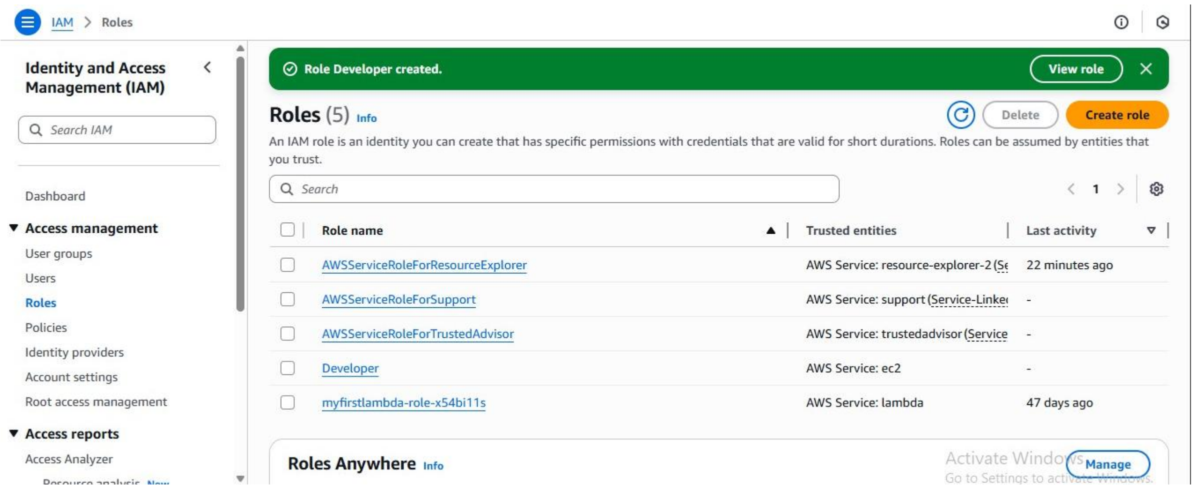
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.

Step7:- **Create the Role:**

Click **Create role** to finish.



Role Developer 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
□	AWSServiceRoleForResourceExplorer	AWS Service: resource-explorer-2 (Se	22 minutes ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
□	Developer	AWS Service: ec2	-
□	myfirstlambda-role-x54bi11s	AWS Service: lambda	47 days ago

Activate Windows
Go to Settings to activate Windows.