Week-2 Identity and Access Management (IAM)

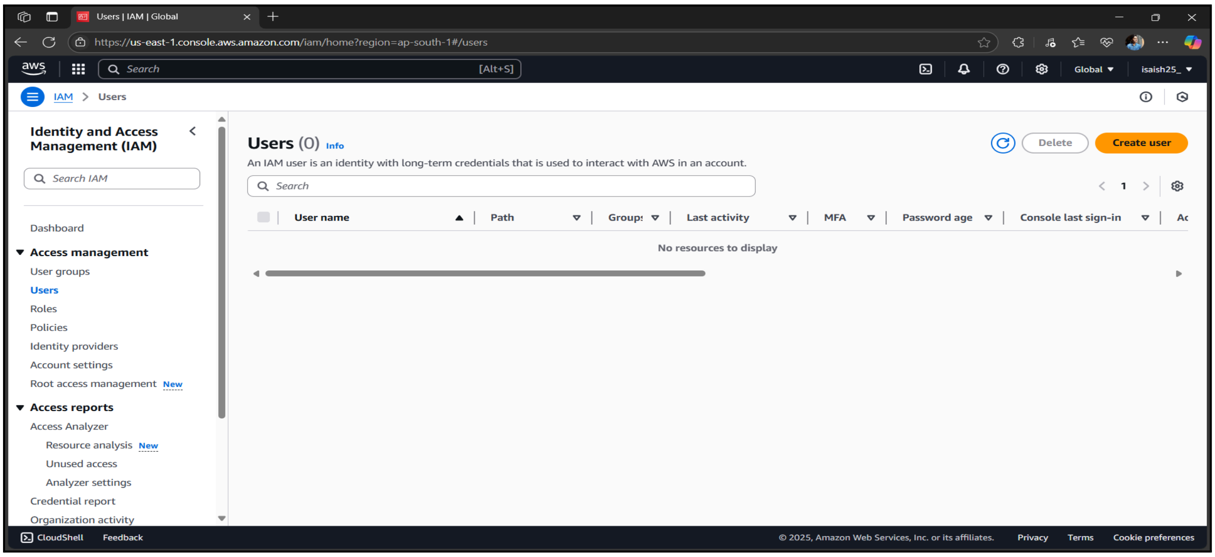
Name- Saish Dhiwar
PRN- 2124UCSM2011
Email- saish.dhiwar_24ucs@sanjivani.edu.in

Task- 1) Create IAM users, groups, and roles.
2) Apply the least privilege principle.
3) Document policies and screenshots.

Steps to Create IAM Users, Groups, Roles-

1) Sign in to AWS Console, go to: https://aws.amazon.com/, sign in using your root user or IAM user.

2) Create IAM User, Go to IAM→ Users→ Click on Create user.



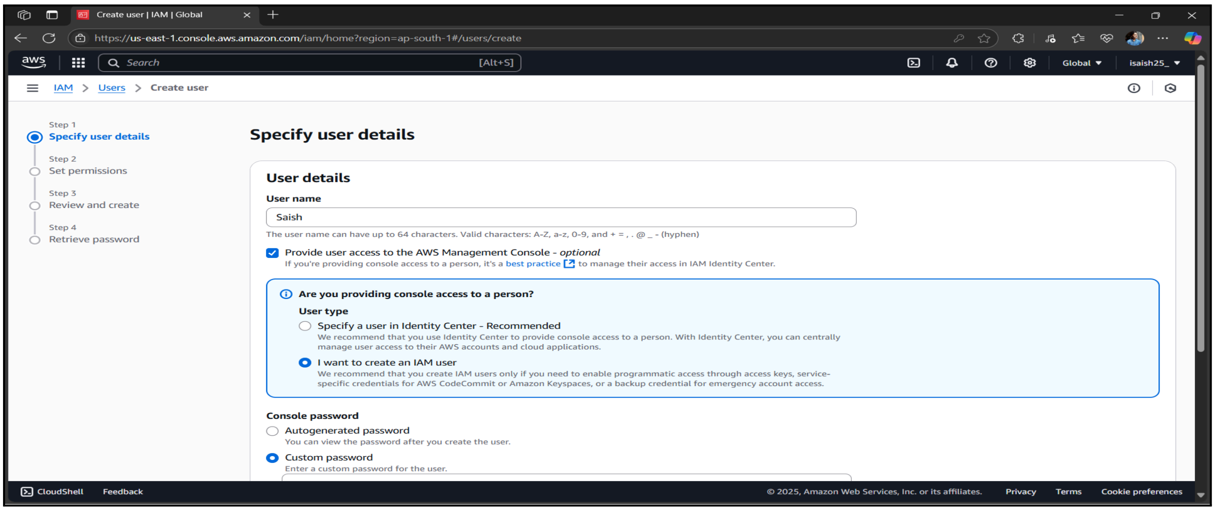
Users (0) Info

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

User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Ac

No resources to display

3) Enter the User name, Select AWS Management Console access, then check the custom password and reset the password and click Next Button.



Create user | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Search [Alt+S]
Global
isaish25_
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Specify user details

User details

User name: Saish

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

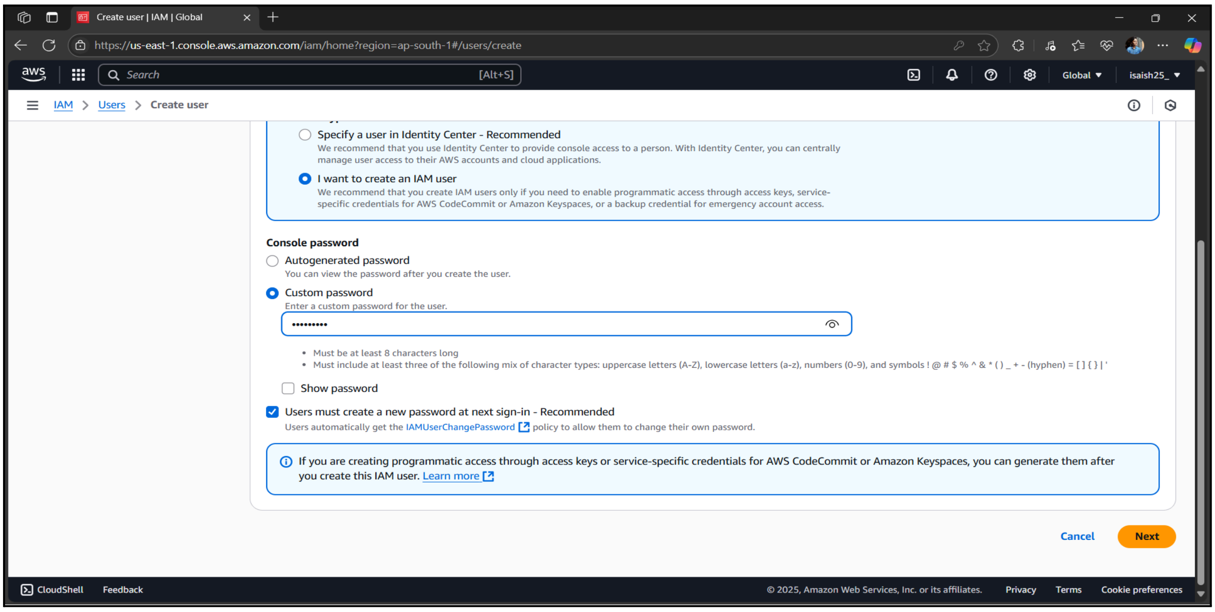
○ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● 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
You can view the password after you create the user.

● Custom password
Enter a custom password for the user.


Create user | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Search [Alt+S]
Global
isaish25_
IAM > Users > Create user
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

○ 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.
•••••••••

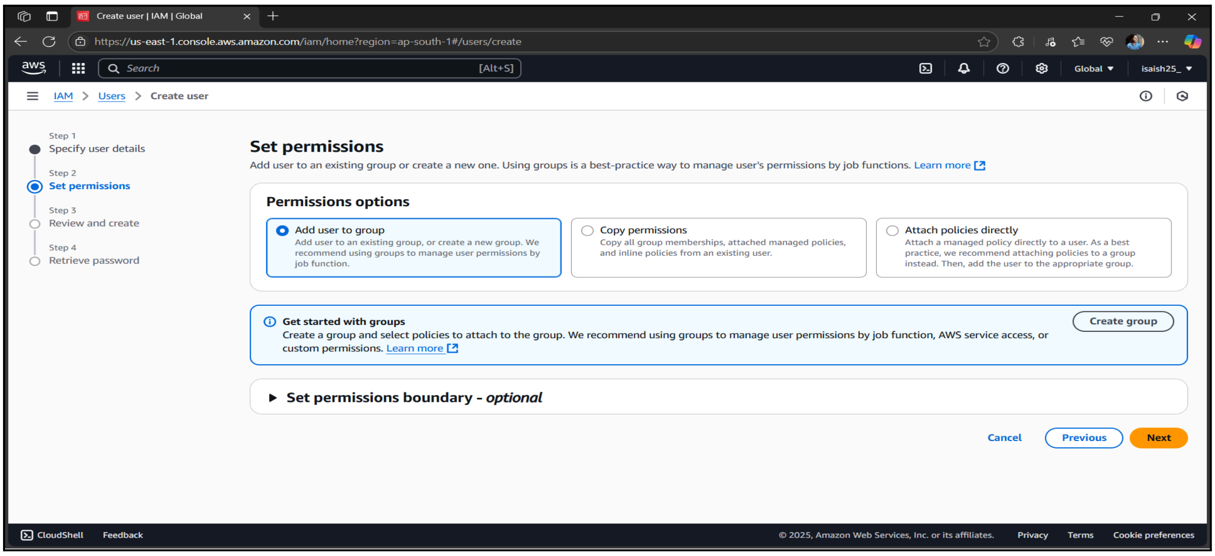
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ 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

4) Set the permission and then click Create 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.

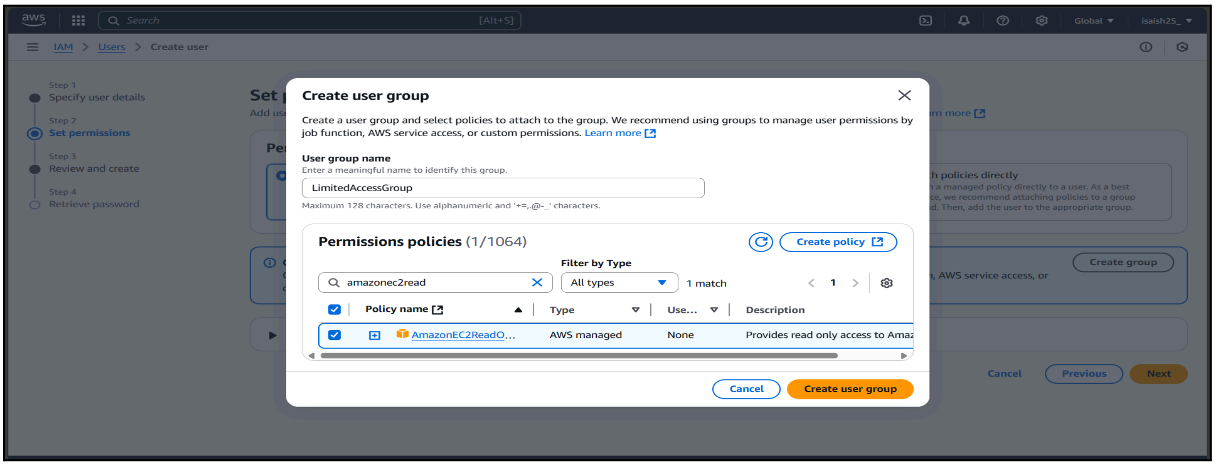
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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.

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***

5) Enter the User group name, select the Permissions policies, and then click the Create User 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

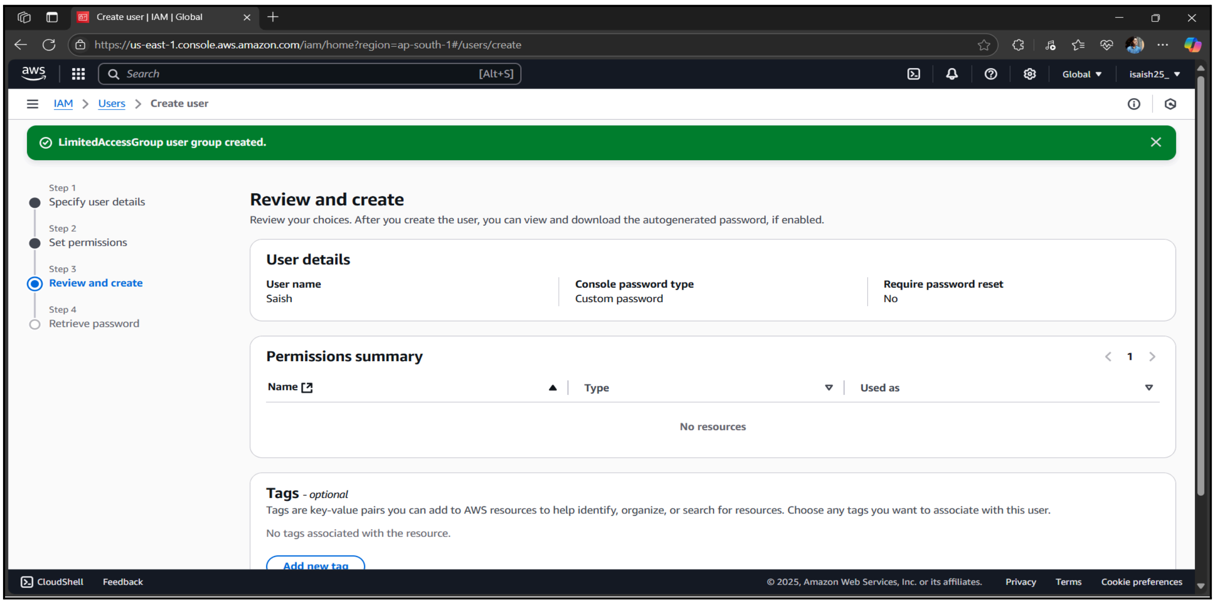
User group name
Enter a meaningful name to identify this group.
LimitedAccessGroup
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions policies (1/1064)

Filter by Type: All types
amazonec2read
1 match

☑	Policy name	Type	Use...	Description
☑	AmazonEC2ReadO...	AWS managed	None	Provides read only access to Amaz

6) Click the Create user button.



Create user | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Search [Alt+S]
Global
isaish25_
IAM > Users > Create user

LimitedAccessGroup user group created.

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	Console password type	Require password reset
Saish	Custom password	No

Permissions summary

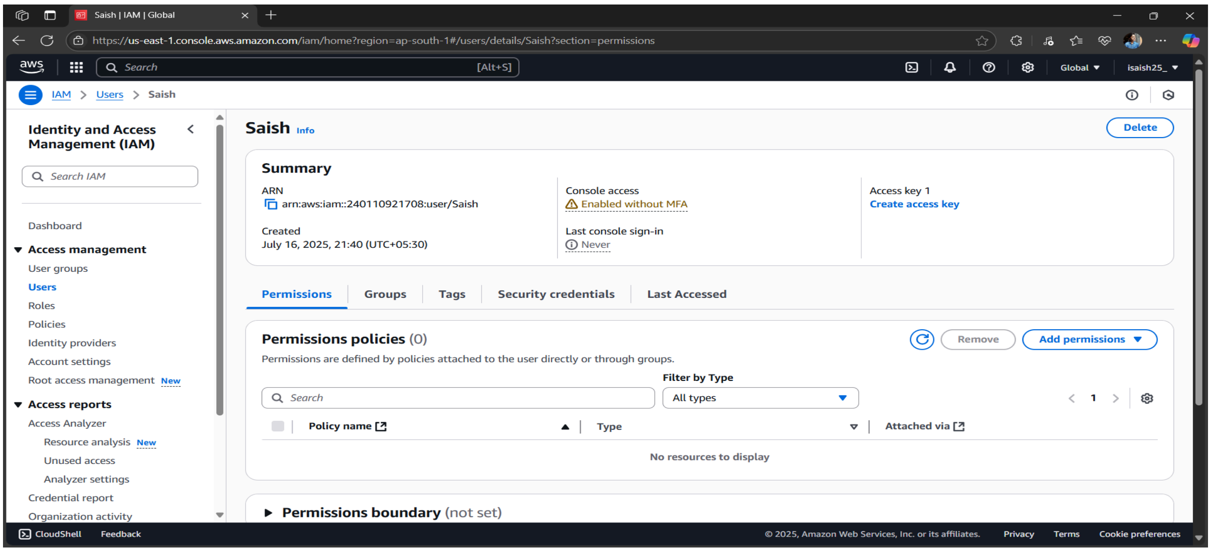
Name	Type	Used as
No resources		

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.

7) User Created Successfully.



Summary

ARN
arn:aws:iam::240110921708:user/Saish

Created
July 16, 2025, 21:40 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

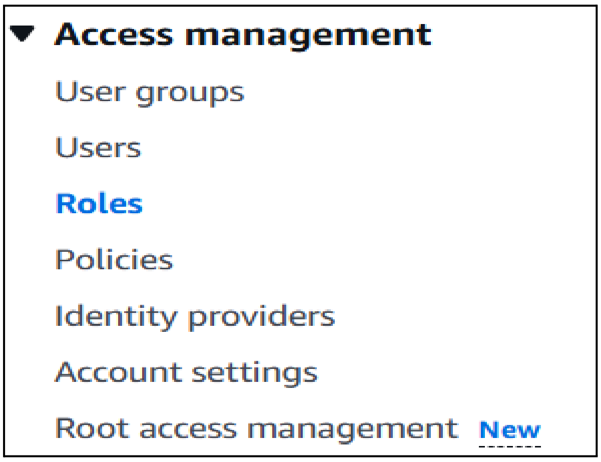
Permissions policies (0)

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

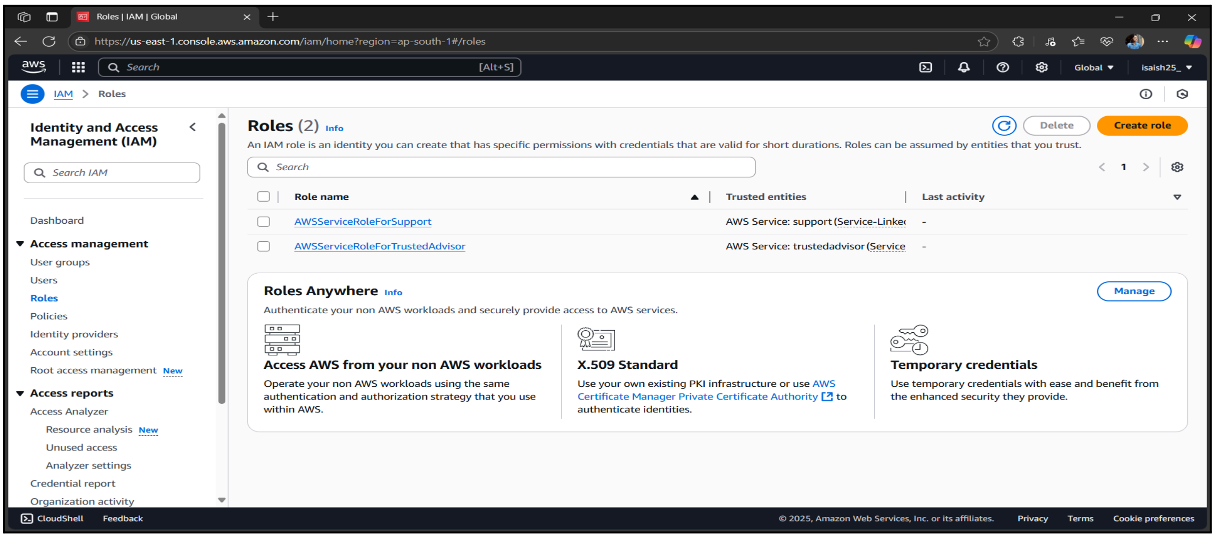
Policy name	Type	Attached via
No resources to display		

Permissions boundary (not set)

8) Create Role, click Role Option.



9) Click Create Role


Roles | IAM | Global

https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles

IAM > Roles

Identity and Access Management (IAM)

Search IAM

Dashboard

- Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
  - Root access management New
- Access reports
  - Access Analyzer
    - Resource analysis New
    - Unused access
    - Analyzer settings
  - Credential report
  - Organization activity

Roles (2) Info

Delete | Create role

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
AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-

Roles Anywhere Info

Manage

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

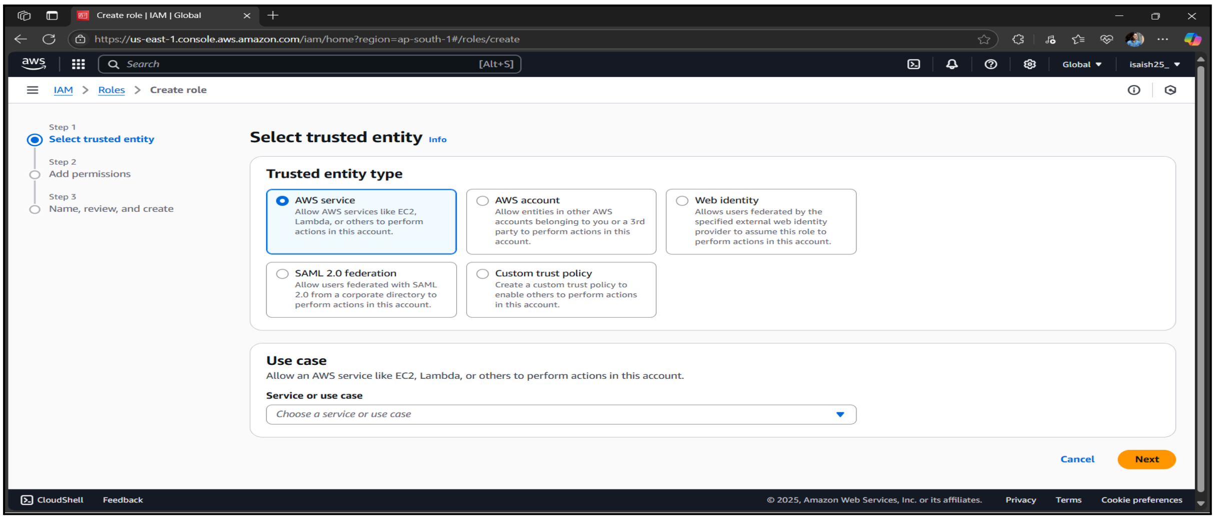
Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials
Use temporary credentials with ease and benefit from the enhanced security they provide.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

10) Then select Trusted Entity.


Create role | IAM | Global

https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create

IAM > Roles > Create role

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.

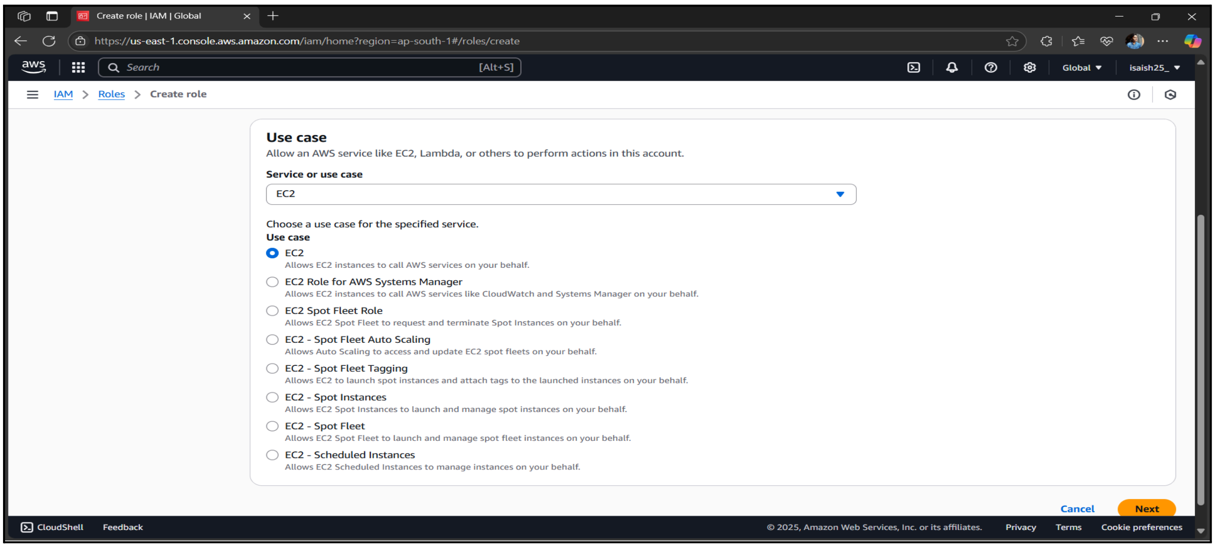
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
Choose a service or use case

Cancel | Next

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

11) Select the use case EC2, and then click Next.


Create role | IAM | Global

https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create

IAM > Roles > Create role

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.

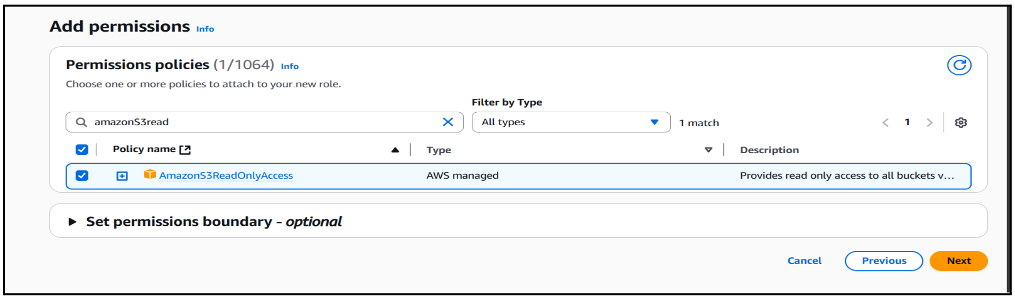
○ EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

○ EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.

Cancel | Next

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

12) Attach the policies AmazonS3ReadOnlyAccess and CloudWatchAgentServer Policy and click the Next button.



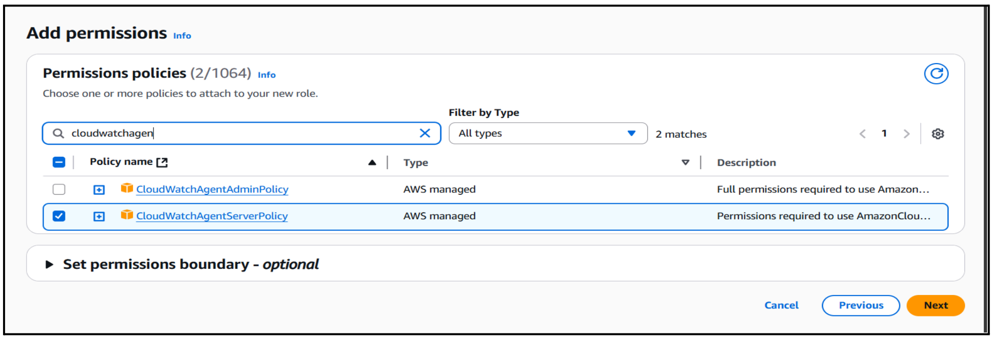
Add permissions Info

Permissions policies (1/1064) Info

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

Search: amazonS3read — Filter by Type: All types — 1 match

	Policy name	Type	Description
☑	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all buckets v…



Add permissions Info

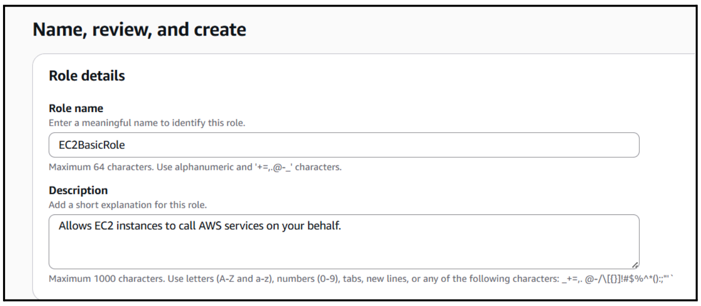
Permissions policies (2/1064) Info

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

Search: cloudwatchagen — Filter by Type: All types — 2 matches

	Policy name	Type	Description
□	CloudWatchAgentAdminPolicy	AWS managed	Full permissions required to use Amazon…
☑	CloudWatchAgentServerPolicy	AWS managed	Permissions required to use AmazonClou…

13) Give the Role details like name and description.



Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

EC2BasicRole

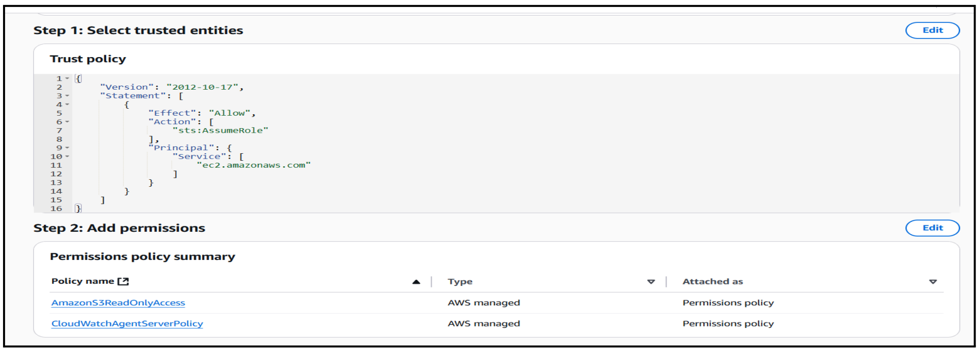
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

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: _+=,. @-/\[{}]!#$%^();:"'`

14) Select Trusted Entities and check the permission.



Step 1: Select trusted entities

Trust policy

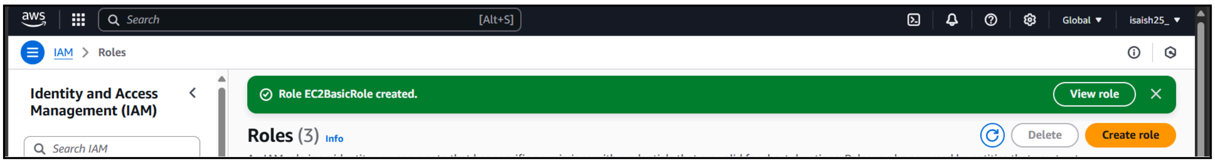
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonS3ReadOnlyAccess	AWS managed	Permissions policy
CloudWatchAgentServerPolicy	AWS managed	Permissions policy

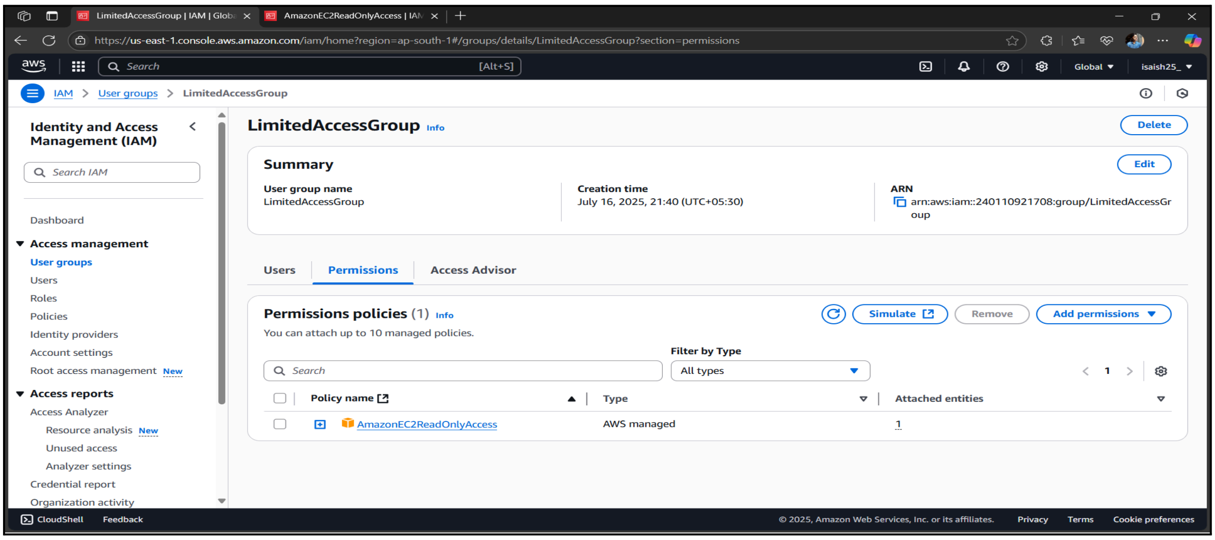
15) The role is successfully created.



Role EC2BasicRole created.

Roles (3) Info

Apply the least privilege principle.



https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/LimitedAccessGroup?section=permissions

LimitedAccessGroup Info

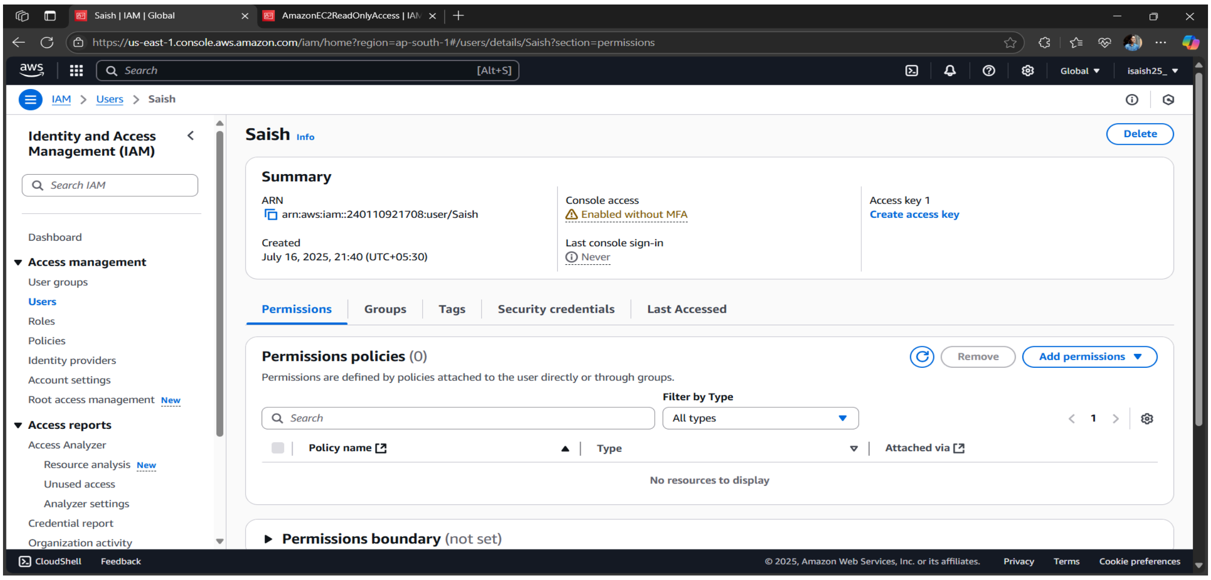
Summary

User group name: LimitedAccessGroup
Creation time: July 16, 2025, 21:40 (UTC+05:30)
ARN: arn:aws:iam::240110921708:group/LimitedAccessGroup

Permissions policies (1) Info

You can attach up to 10 managed policies.

Policy name	Type	Attached entities
AmazonEC2ReadOnlyAccess	AWS managed	1



https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/Saish?section=permissions

Saish Info

Summary

ARN: arn:aws:iam::240110921708:user/Saish
Created: July 16, 2025, 21:40 (UTC+05:30)
Console access: Enabled without MFA
Last console sign-in: Never
Access key 1: Create access key

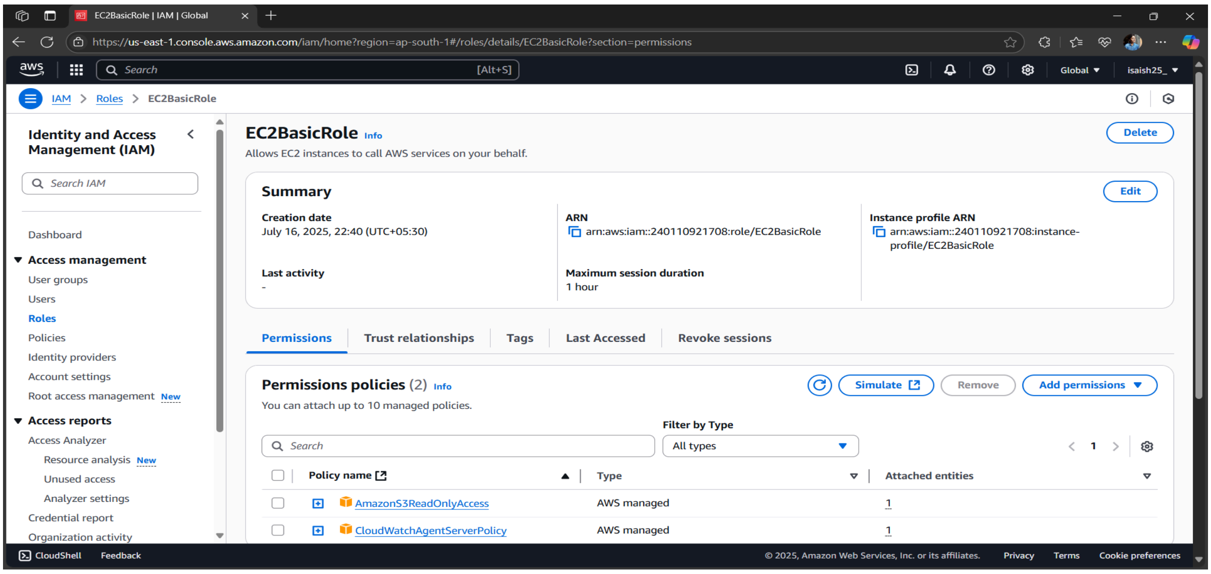
Permissions policies (0)

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

Policy name	Type	Attached via

No resources to display

Permissions boundary (not set)



https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/EC2BasicRole?section=permissions

EC2BasicRole Info

Allows EC2 instances to call AWS services on your behalf.

Summary

Creation date: July 16, 2025, 22:40 (UTC+05:30)
ARN: arn:aws:iam::240110921708:role/EC2BasicRole
Instance profile ARN: arn:aws:iam::240110921708:instance-profile/EC2BasicRole
Last activity: -
Maximum session duration: 1 hour

Permissions policies (2) Info

You can attach up to 10 managed policies.

Policy name	Type	Attached entities
AmazonS3ReadOnlyAccess	AWS managed	1
CloudWatchAgentServerPolicy	AWS managed	1