Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) is a service provided by Amazon Web Services that allows you to securely manage access to AWS services and resources. IAM provides fine-grained control over who can access what resources, ensuring secure and organized access management.

Key Features of IAM

1. **Secure Access**:
   - Manage **who** (users, groups, roles) can perform actions on AWS resources and **how** they access them.
   - Support for **multi-factor authentication (MFA)** for additional security.
2. **Granular Permissions**:
   - Control access at a detailed level using JSON-based **IAM policies**.
   - Restrict access by specific actions (e.g., read, write), resources, and conditions.
3. **Temporary Credentials**:
   - Use **IAM roles** to provide applications, services, or users temporary access to AWS resources without sharing credentials.
4. **Federation**:
   - Integrate with corporate directories like Microsoft Active Directory or external identity providers using **AWS Single Sign-On (SSO)** or **SAML**.
5. **Auditing and Monitoring**:
   - Track IAM activity through AWS CloudTrail logs for compliance and auditing.

Key Components of IAM

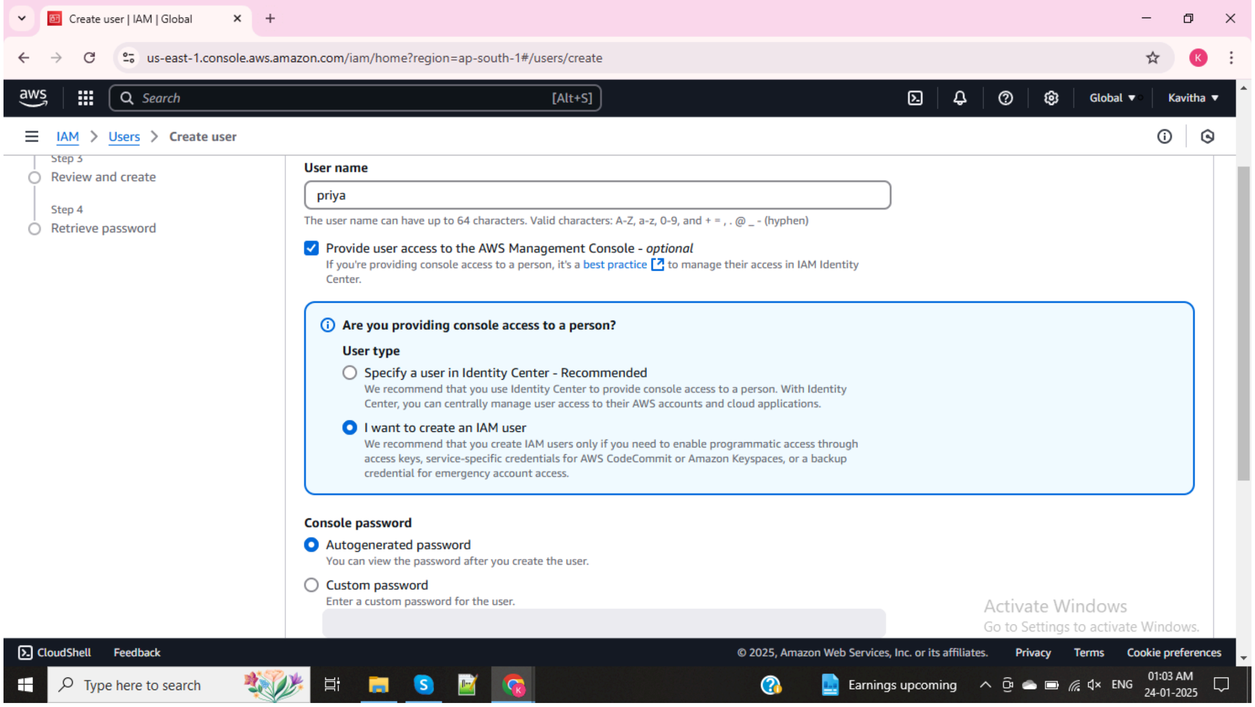
Component	Description
Users	Represent individual users with access credentials for AWS management console or API access.
Groups	Logical grouping of users to assign permissions collectively.
Roles	Provide temporary access permissions for AWS resources to applications, services, or users.
Policies	JSON documents specifying permissions, defining who can access what resources.

How IAM Works

1. **Authentication**:
   - Users, roles, or services authenticate using credentials or temporary security tokens.
2. **Authorization**:
   - IAM evaluates attached policies to determine if a requested action is allowed or denied.
3. **Resource-Based Policies**:
   - Add extra control by attaching policies directly to AWS resources like S3 or DynamoDB.

IAM is fundamental to securely managing AWS environments and enabling precise control over resources, making it an essential tool in any AWS deployment.

Creating IAM user by using root user



IAM > Users > Create user

Step 3
○ Review and create

Step 4
○ Retrieve password

User name

priya

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.

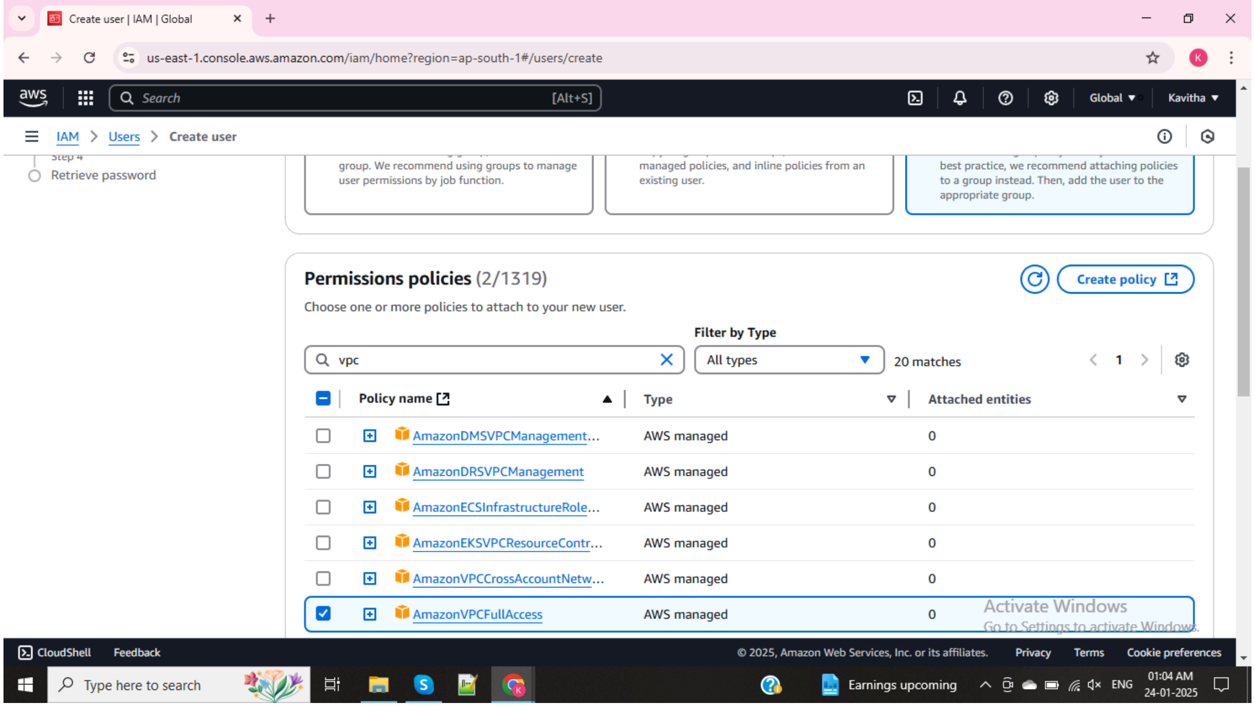
Console password

● 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
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Search [Alt+S]
Global
Kavitha
Activate Windows
Go to Settings to activate Windows.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
Earnings upcoming
ENG
01:03 AM
24-01-2025

Attach policy for that IAM user - Amazon VPC full access



IAM > Users > Create user

Step 4
○ Retrieve password

group. We recommend using groups to manage user permissions by job function.

managed policies, and inline policies from an existing user.

best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (2/1319)

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

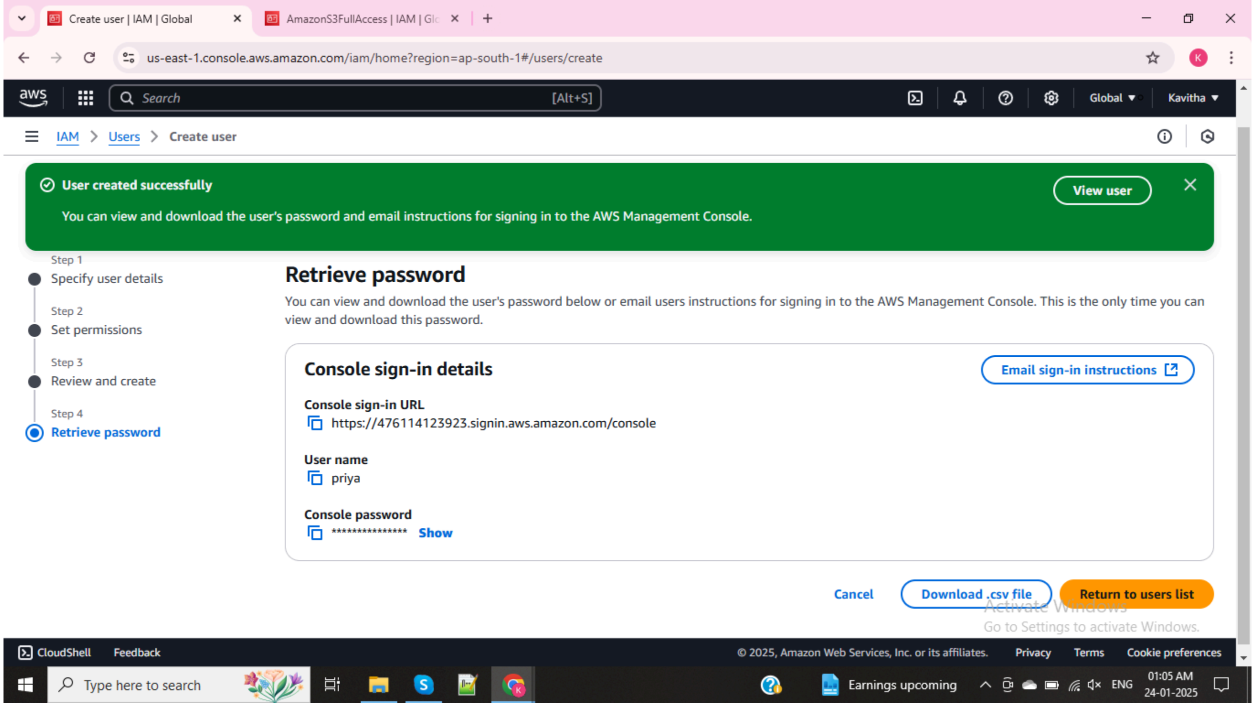
Filter by Type

vpc | All types | 20 matches

	Policy name	Type	Attached entities
□	AmazonDMSVPCManagement…	AWS managed	0
□	AmazonDRSVPCManagement	AWS managed	0
□	AmazonECSInfrastructureRole…	AWS managed	0
□	AmazonEKSVPCResourceContr…	AWS managed	0
□	AmazonVPCCrossAccountNetw…	AWS managed	0
☑	AmazonVPCFullAccess	AWS managed	0

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Search [Alt+S]
Global
Kavitha
Create policy
1
Activate Windows
Go to Settings to activate Windows.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
Earnings upcoming
ENG
01:04 AM
24-01-2025

Successfully created IAM user



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.

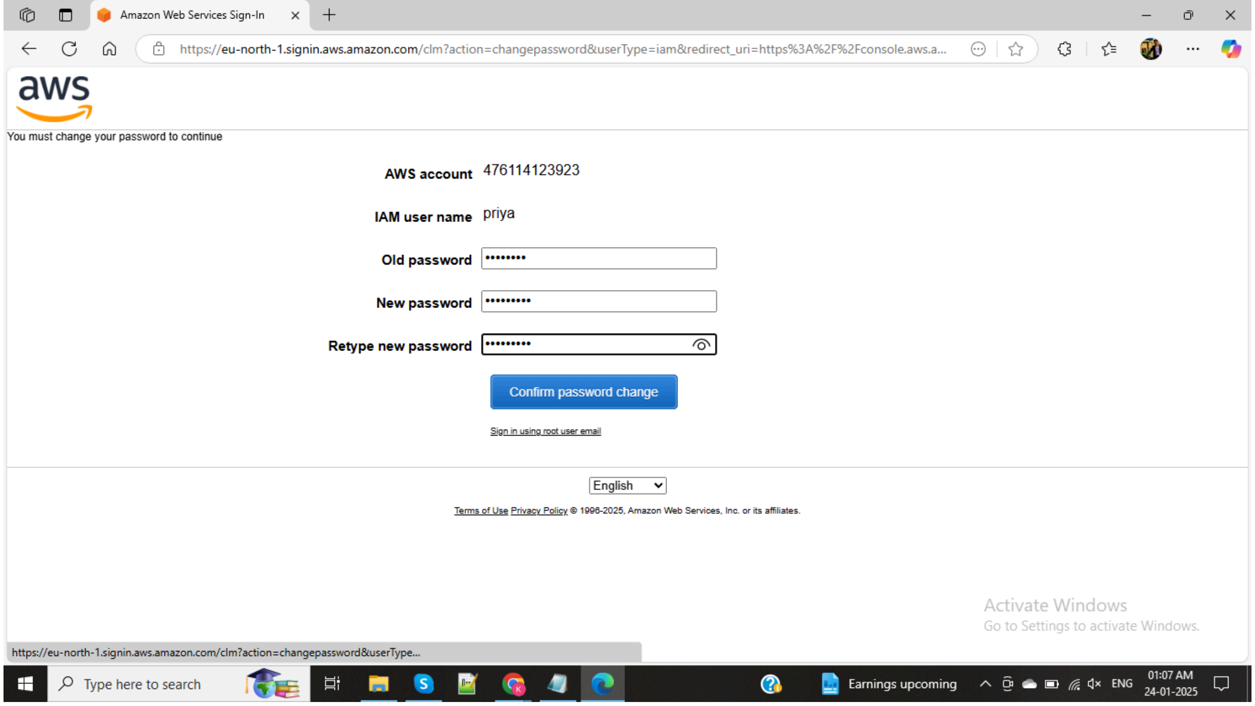
Console sign-in details

Console sign-in URL
https://476114123923.signin.aws.amazon.com/console

User name
priya

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

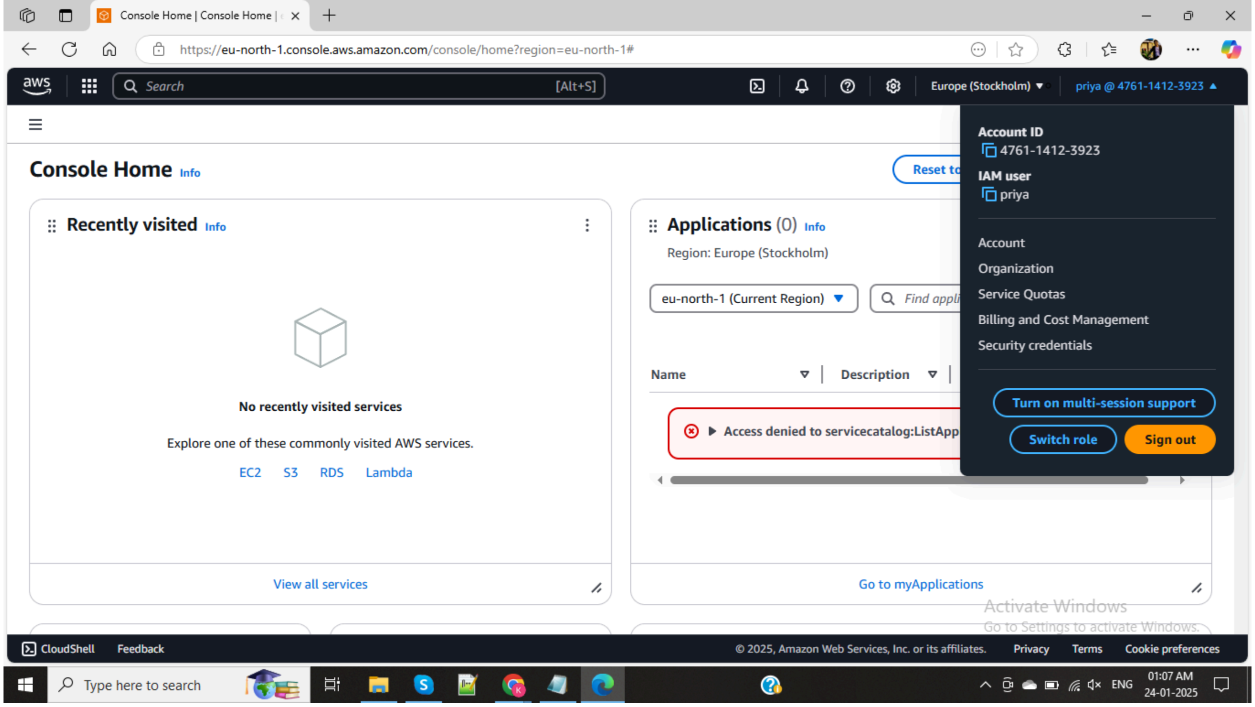
Checking IAM user logging and it automatically sign into new password created page



You must change your password to continue

AWS account	476114123923
IAM user name	priya
Old password	••••••••
New password	•••••••••
Retype new password	•••••••••

IAM user login page



https://eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1#

Europe (Stockholm) ▾ priya @ 4761-1412-3923 ▴

Console Home Info

Recently visited Info

No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 RDS Lambda

View all services

Applications (0) Info

Region: Europe (Stockholm)

eu-north-1 (Current Region) ▾

Name	Description

Access denied to servicecatalog:ListApp

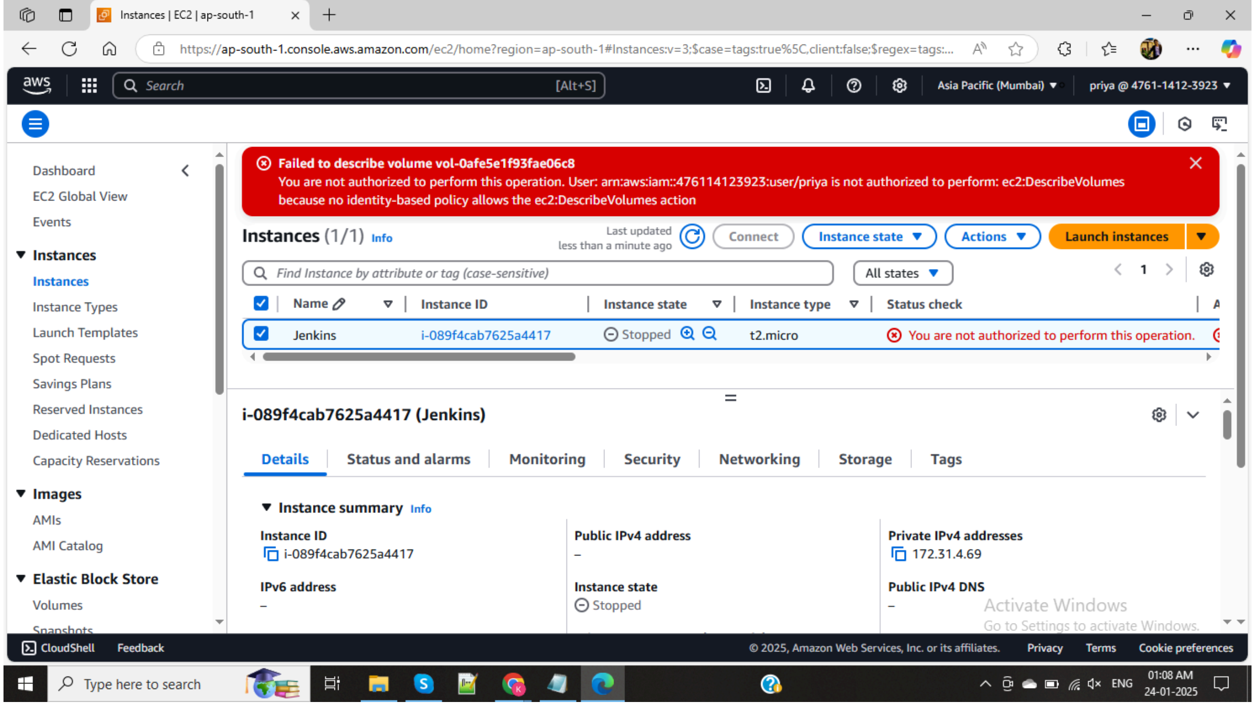
Go to myApplications

Account ID
4761-1412-3923

IAM user
priya

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

We give access to VPC but checking whether any other resources working or not - Unable to access EC2 instance



https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:...

Asia Pacific (Mumbai) ▾ priya @ 4761-1412-3923 ▾

Failed to describe volume vol-0afe5e1f93fae06c8
You are not authorized to perform this operation. User: arn:aws:iam::476114123923:user/priya is not authorized to perform: ec2:DescribeVolumes because no identity-based policy allows the ec2:DescribeVolumes action

Instances (1/1) Info

Last updated less than a minute ago

☑	Name	Instance ID	Instance state	Instance type	Status check
☑	Jenkins	i-089f4cab7625a4417	Stopped	t2.micro	You are not authorized to perform this operation.

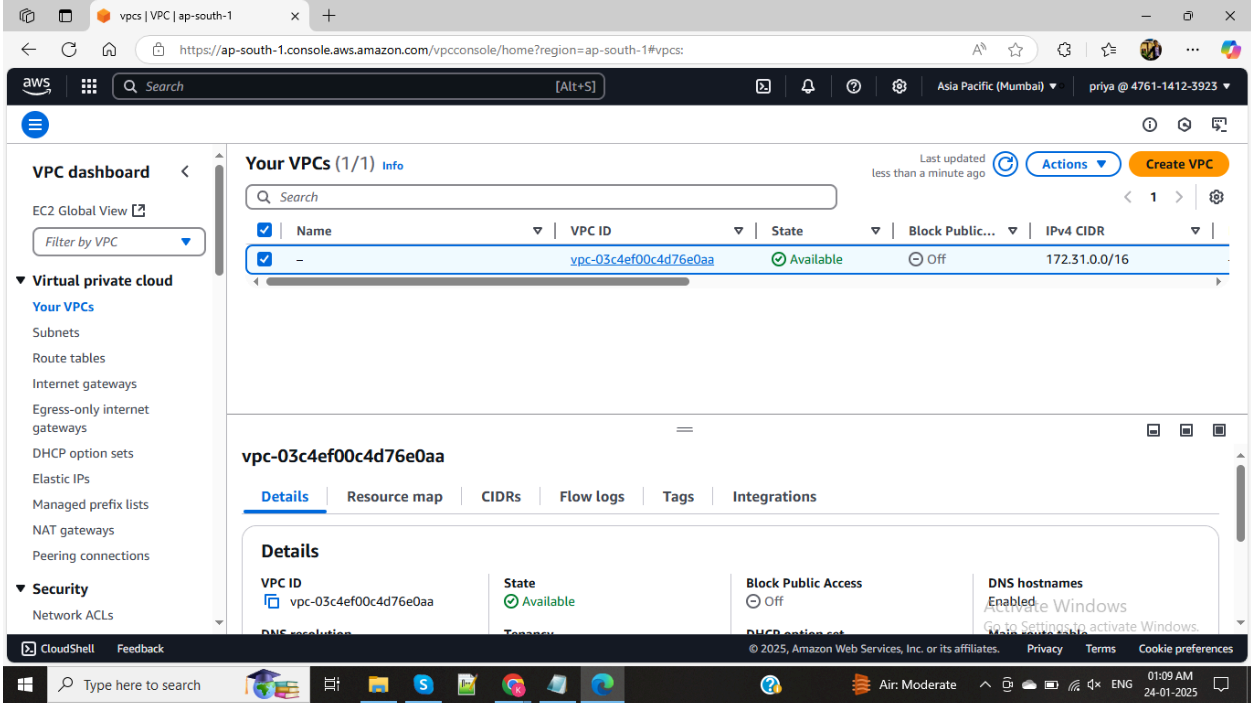
i-089f4cab7625a4417 (Jenkins)

Instance summary Info

Instance ID i-089f4cab7625a4417	Public IPv4 address –	Private IPv4 addresses 172.31.4.69
IPv6 address –	Instance state Stopped	Public IPv4 DNS –

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

VPC accessible as per our policy attach



https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#vpcs:

Asia Pacific (Mumbai) | priya @ 4761-1412-3923

Your VPCs (1/1)

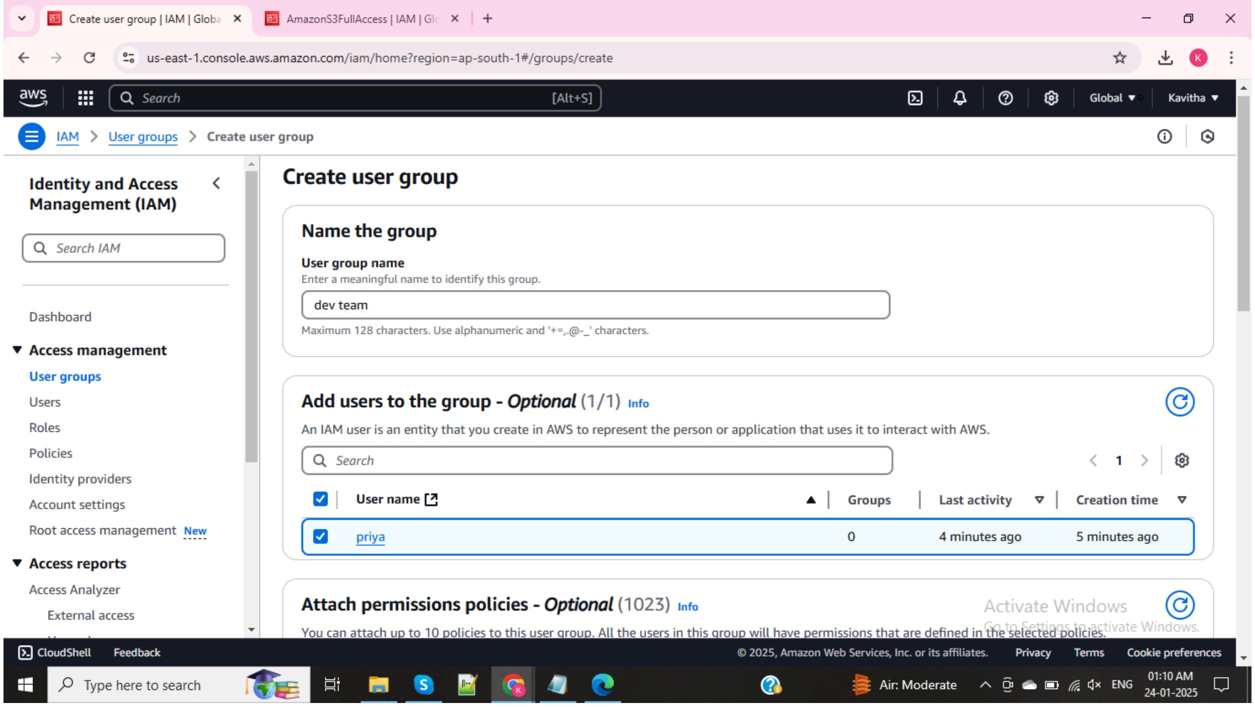
	Name	VPC ID	State	Block Public...	IPv4 CIDR
☑	–	vpc-03c4ef00c4d76e0aa	Available	Off	172.31.0.0/16

vpc-03c4ef00c4d76e0aa

Details

VPC ID	State	Block Public Access	DNS hostnames
vpc-03c4ef00c4d76e0aa	Available	Off	Enabled

Creating GROUP and attach EC2 full access policy for that group



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

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

dev team

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

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

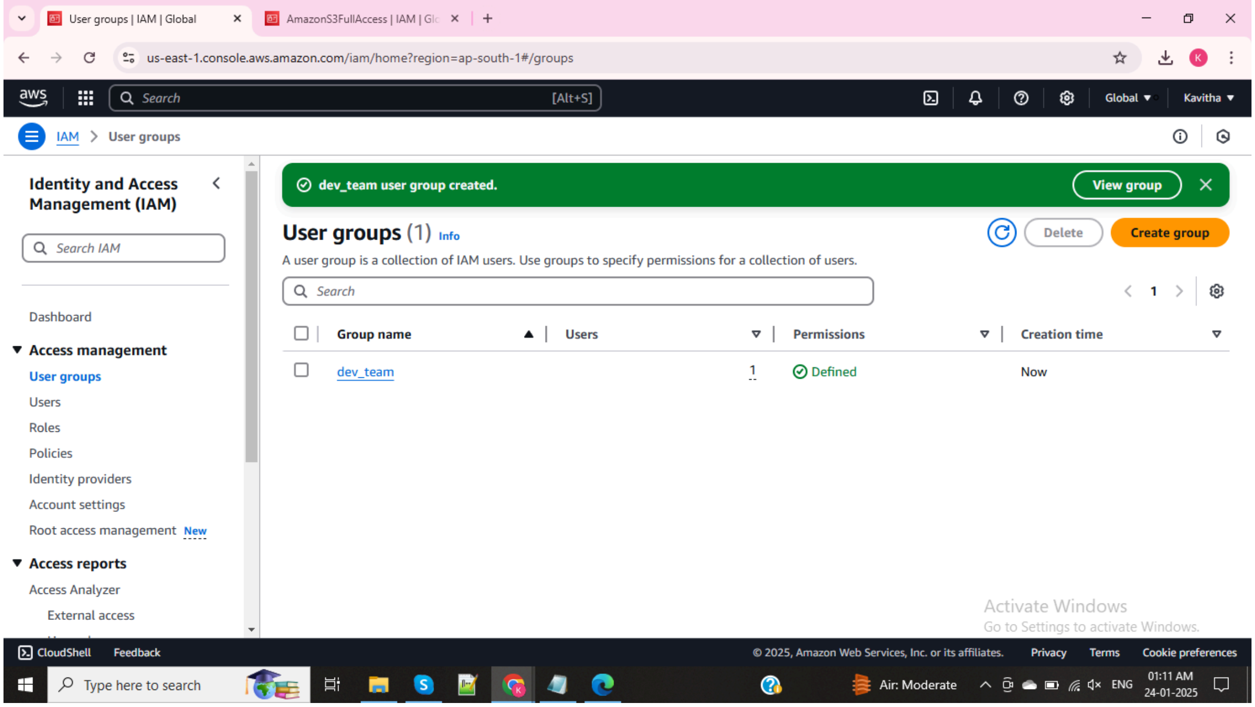
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

	User name	Groups	Last activity	Creation time
☑	priya	0	4 minutes ago	5 minutes ago

Attach permissions policies - *Optional* (1023)

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.

USER GROUPS created successfully



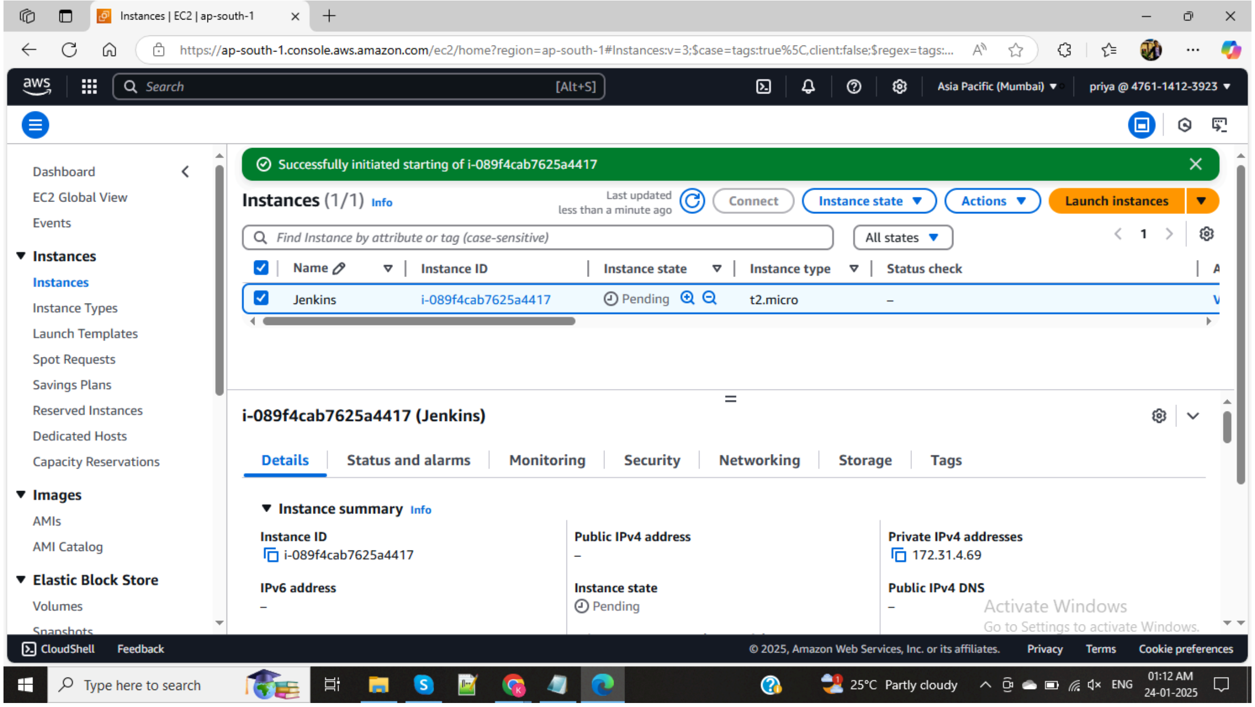
dev_team user group created.

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
☐	dev_team	1	✓ Defined	Now

IAM user added to that group, Now user can access EC2 instance



Successfully initiated starting of i-089f4cab7625a4417

Instances (1/1) Info

☑	Name	Instance ID	Instance state	Instance type	Status check
☑	Jenkins	i-089f4cab7625a4417	Pending	t2.micro	–

i-089f4cab7625a4417 (Jenkins)

Instance summary Info

Instance ID i-089f4cab7625a4417	Public IPv4 address –	Private IPv4 addresses 172.31.4.69
IPv6 address –	Instance state Pending	Public IPv4 DNS –