

What is IAM ?

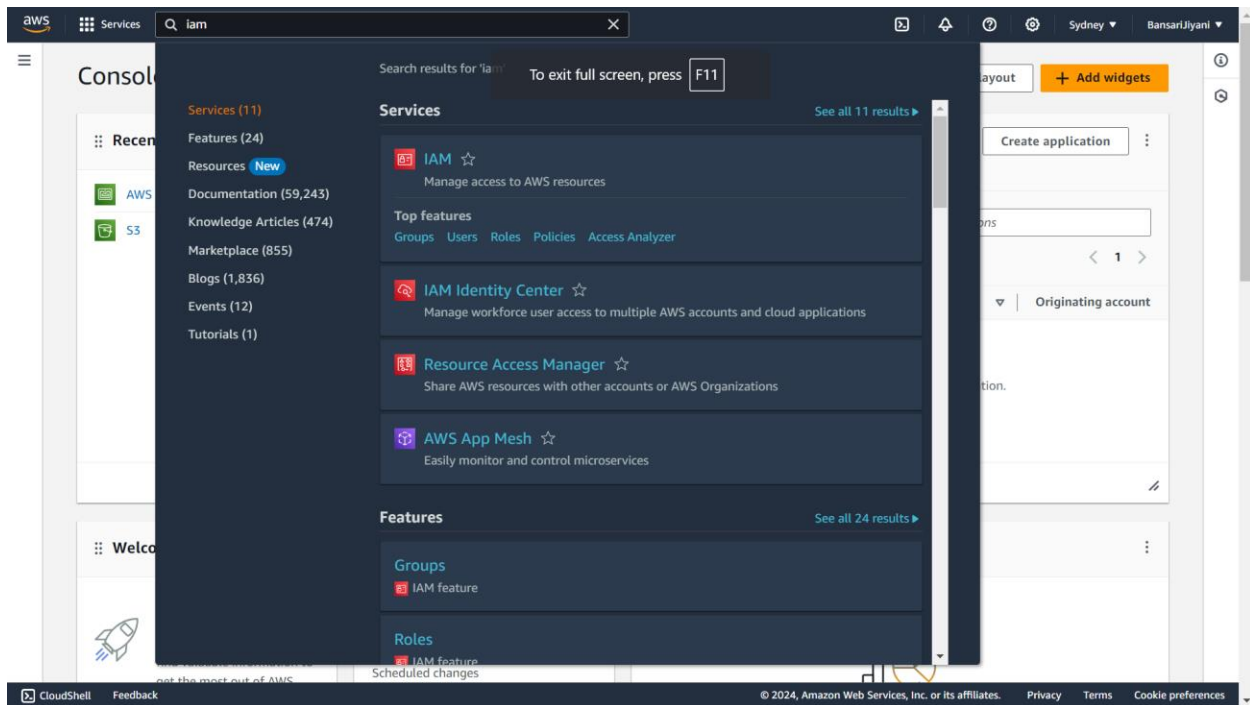
Identity and Access Management

AWS IAM (Identity and Access Management) is a service that helps you securely control access to AWS resources.

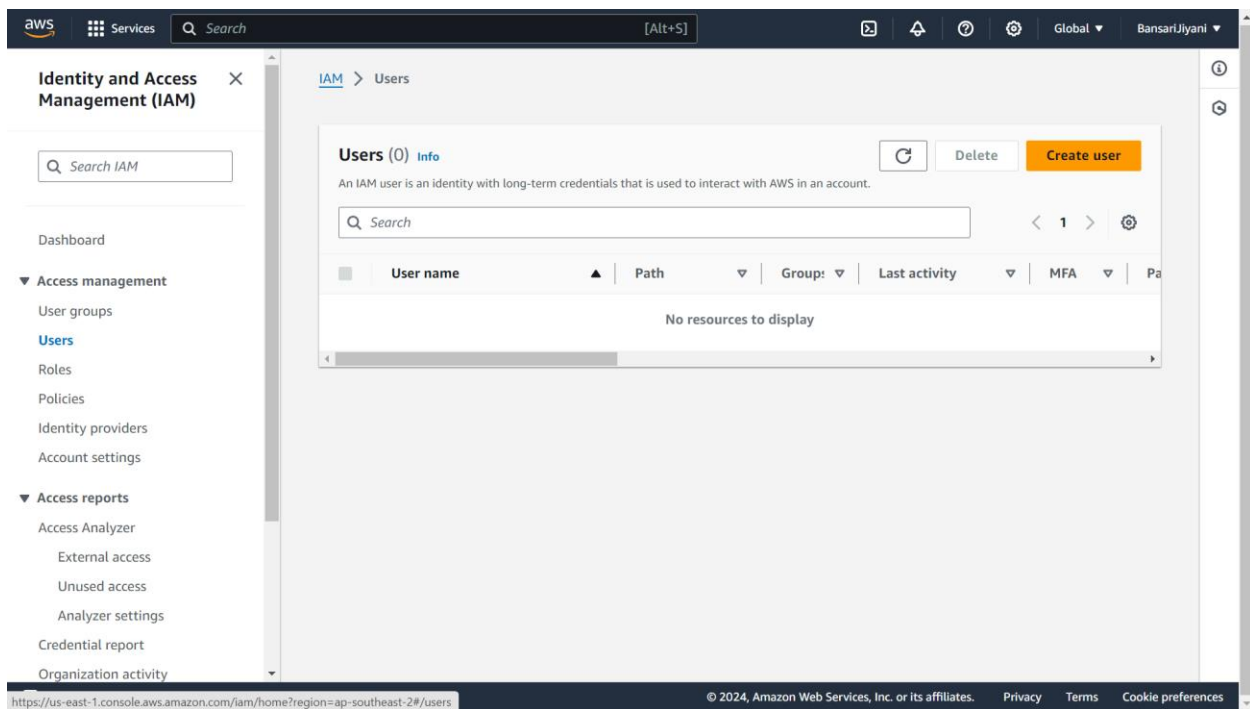
- **Users:** You can create individual users (like employees) who can log in to AWS. Each user can have their own permissions based on what they need to do.
- **Groups:** Users can be grouped together, and permissions can be assigned to the whole group, making it easier to manage access for multiple users at once.
- **Roles:** Roles are used to give permissions to AWS services or applications, allowing them to perform actions on your behalf. For example, a role might allow an application to access data in an S3 bucket.
- **Policies:** These are rules that define what actions are allowed or denied. You attach policies to users, groups, or roles to control their permissions.

PRACTICAL :

1. Search IAM and open it.



2. Go to the users in left side. And click on Create user for create new user .



3. Add name for create user.

User details

User name
bansirijyani

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.

☐ 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

4. Select I want to create an IAM user. And add password. And uncheck the users must create new password at next sign-in.

☐ 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.

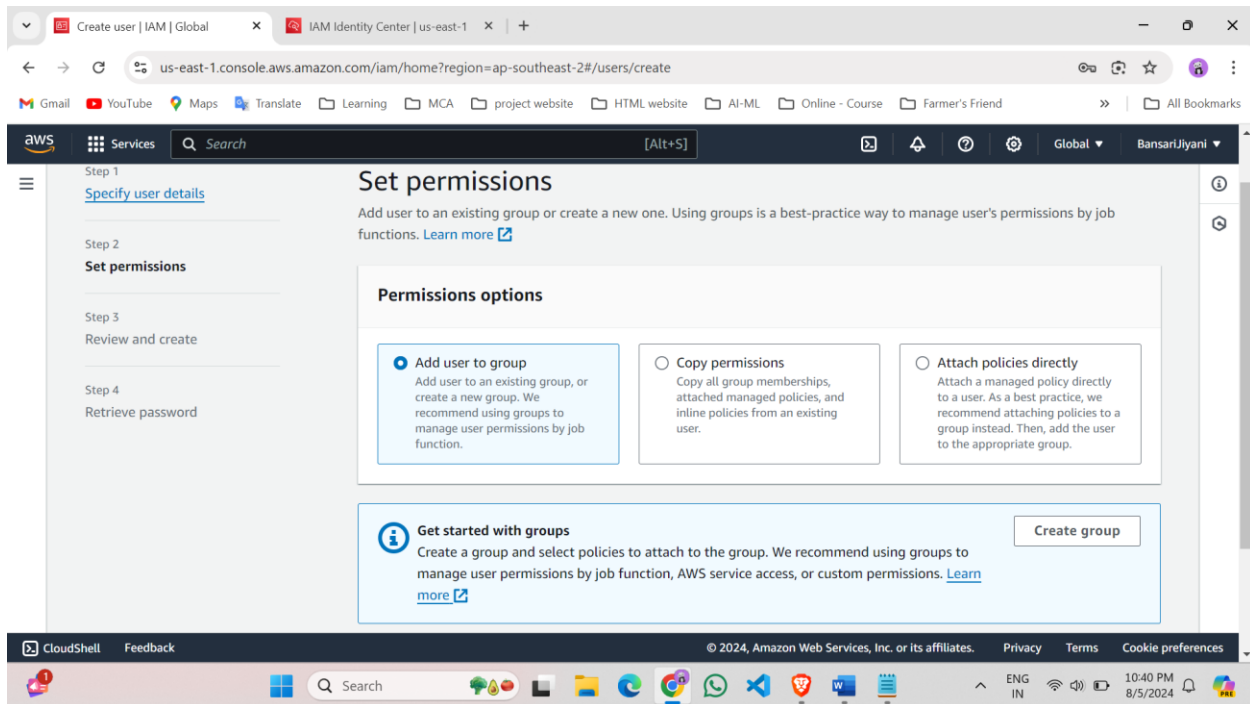
☒ Custom password
Enter a custom password for the user.

- 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) = [] { } ' "

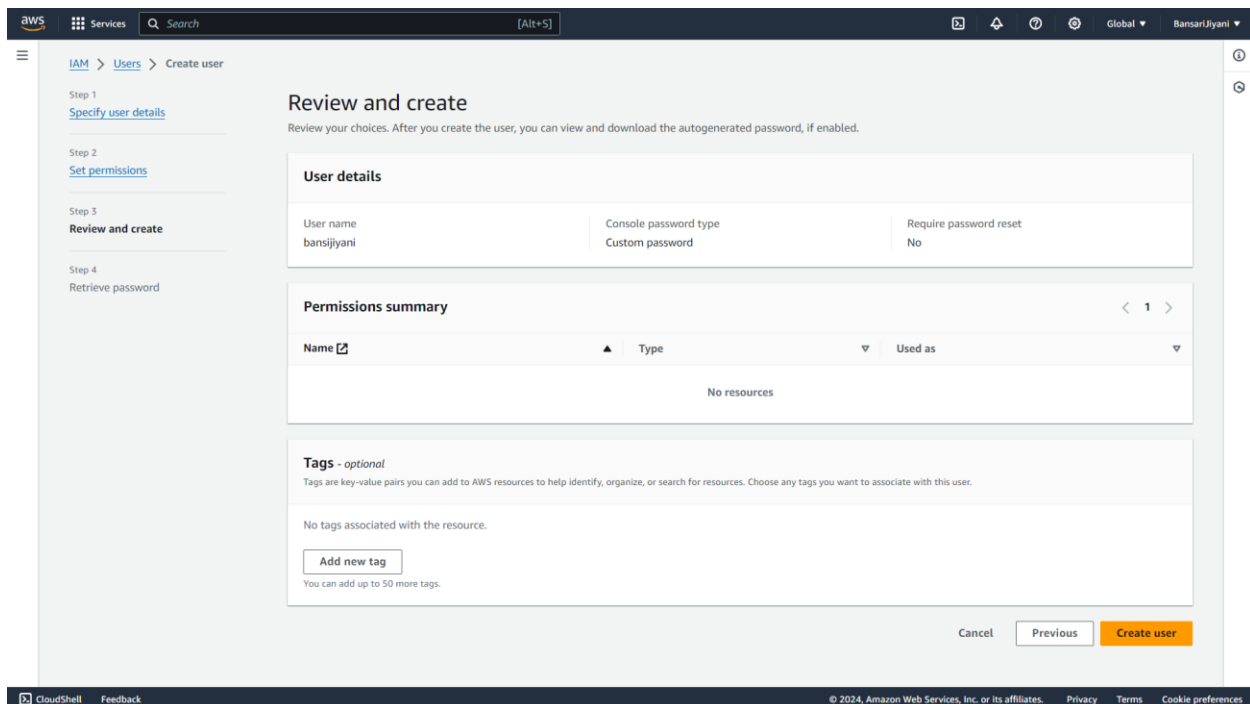
☐ Show password

☐ Users must create a new password at next sign-in - Recommended
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own

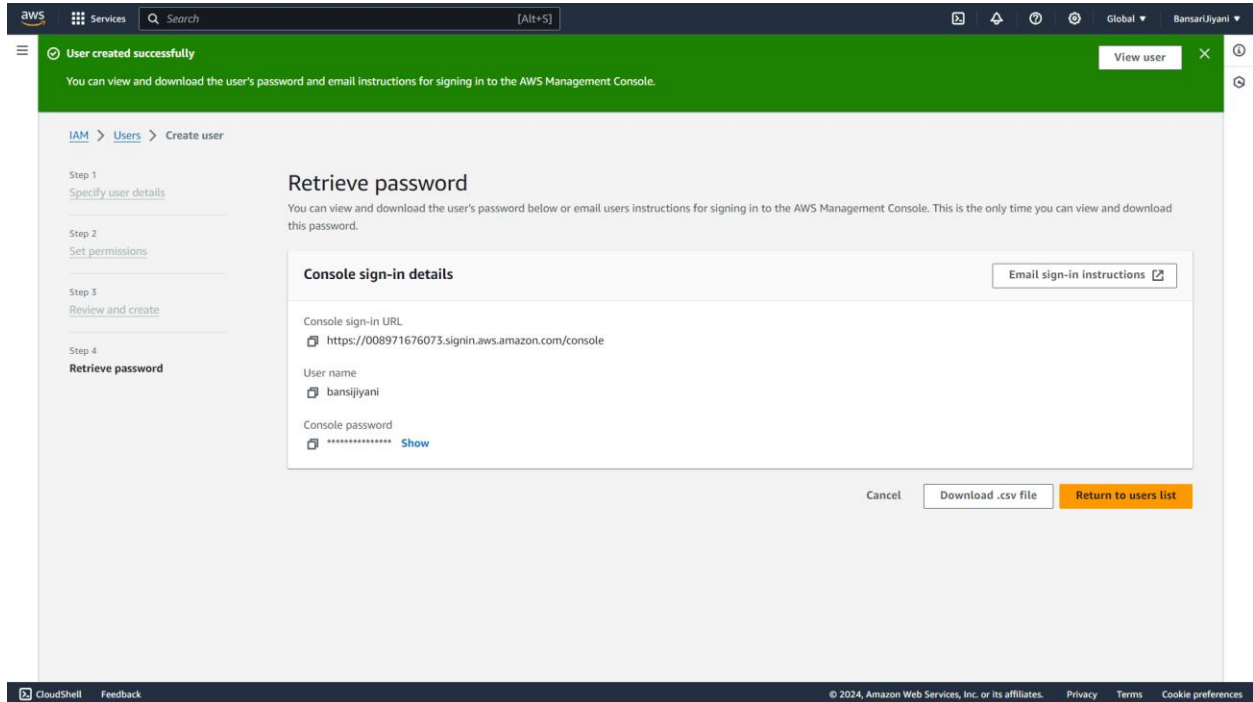
5. Go to the Set permission and in my case I am not giving any permission because after we know that which permission is given by default.



6. Click next and review and create the user.

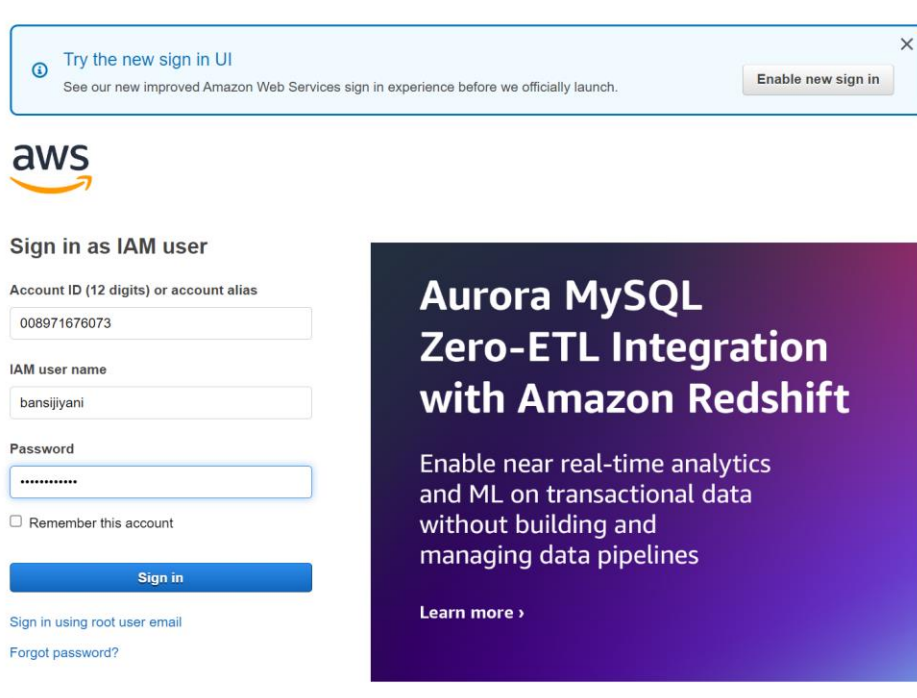


7. Now you get the UserID , user name and password.



8. Now open AWS console for log in user and select IAM user and write Account ID from above Console sign-in URL in retrieve password page and sign-in.

URL : <https://008971676073.signin.aws.amazon.com/console>



9. By default it is not given any access.

The screenshot shows the AWS Management Console home page. The top navigation bar includes the AWS logo, 'Services', a search bar, and the user's profile 'bansijiyani @ 0089-7167-6073'. The main content area is divided into several sections:

- No recently visited services:** A message stating 'Explore one of these commonly visited AWS services.' with links for EC2, S3, RDS, and Lambda. A 'View all services' link is at the bottom.
- Welcome to AWS:** A section with links for 'Getting started with AWS' and 'Training and certification'.
- AWS Health:** A section with a heart icon and a message: 'No health data. You don't have permissions to access AWS Health.'
- Cost and usage:** A section with links for 'Current month costs', 'Forecasted month end costs', and 'Savings opportunities'. All these links are marked with a red 'X' and 'Access denied'.

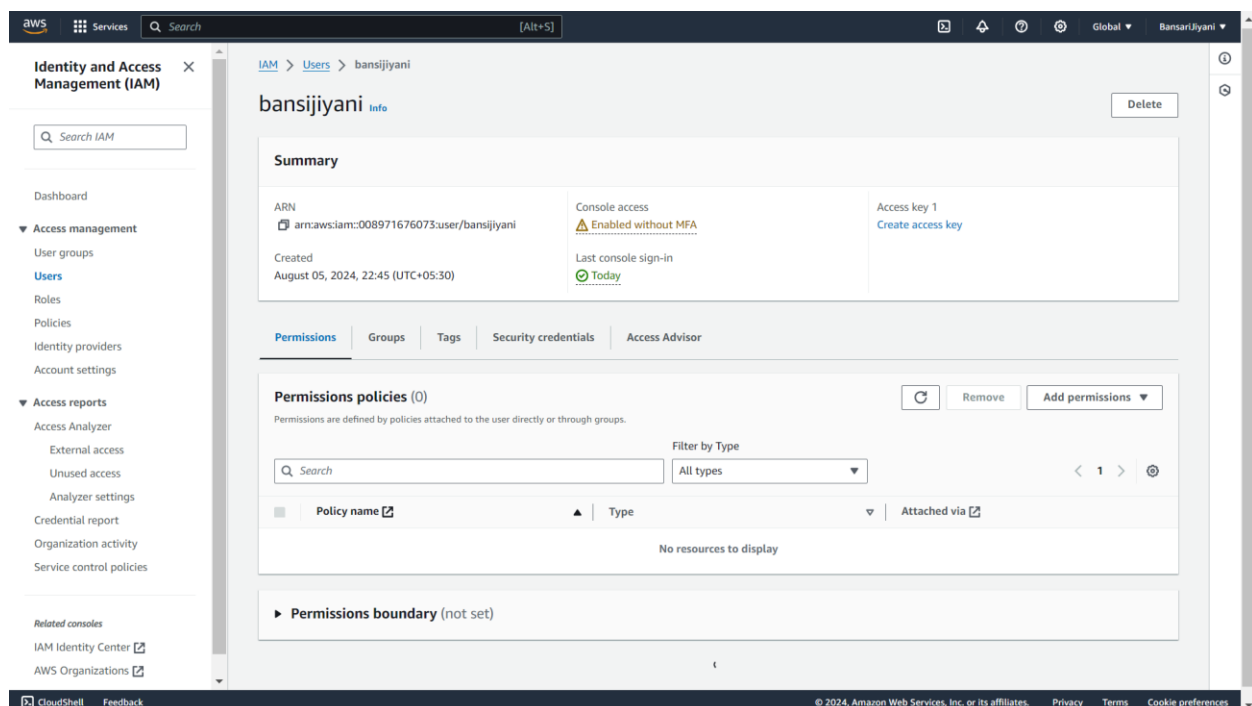
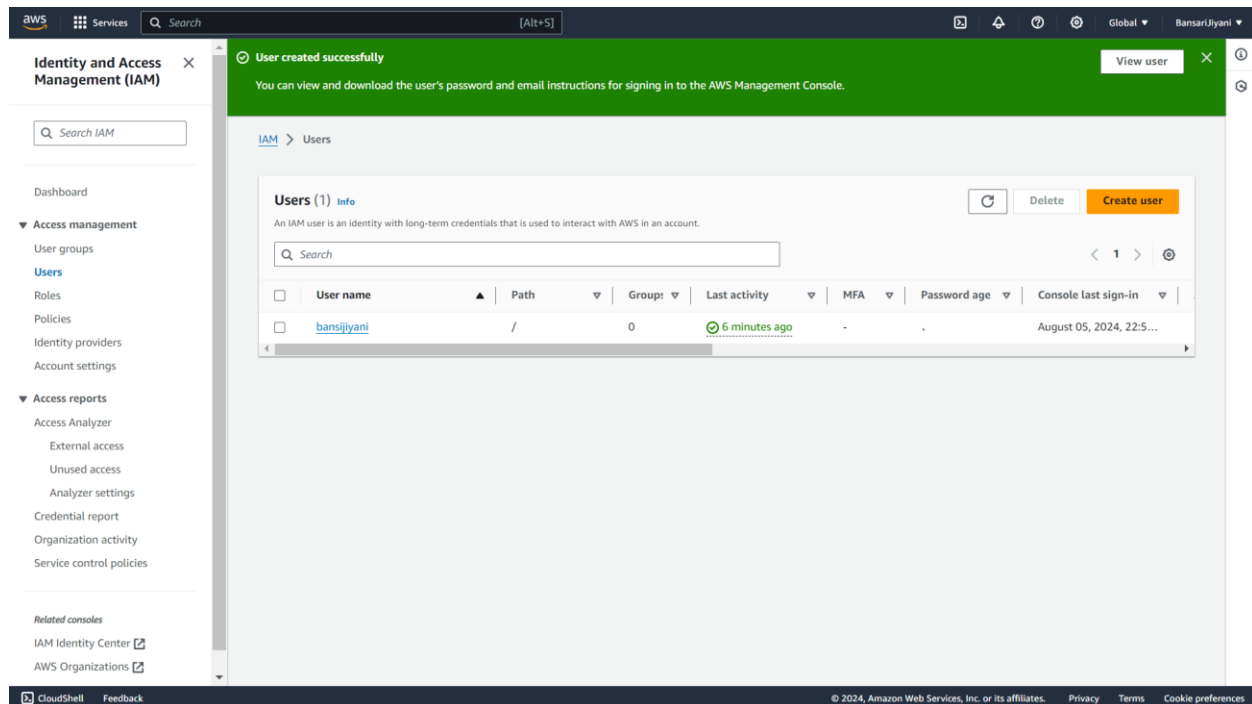
The bottom of the page features a footer with 'CloudShell', 'Feedback', and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

The screenshot shows the AWS Management Console EC2 Dashboard. The left sidebar contains a navigation menu with 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Instances', 'Images', and 'Elastic Block Store'. The main content area is divided into several sections:

- Resources:** A section titled 'You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:'. It lists various resources with their counts and status: 'Instances (running)' (0), 'Dedicated Hosts' (API Error), 'Instances' (API Error), 'Load balancers' (API Error), 'Security groups' (API Error), 'Volumes' (API Error), 'Auto Scaling Groups' (API Error), 'Elastic IPs' (API Error), 'Key pairs' (API Error), 'Placement groups' (API Error), and 'Snapshots' (API Error).
- Launch instance:** A section with a 'Launch instance' button and a 'Migrate a server' link.
- Service health:** A section with a 'AWS Health Dashboard' link and a message: 'An error occurred. An error occurred'.
- EC2 Free Tier:** A section titled 'Offers for all AWS Regions.' showing '0 EC2 free tier offers in use'. It includes an 'End of month forecast' and a detailed error message: 'User: arn:aws:iam::008971676073:user/bansijiyani is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:008971676073:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action'. It also mentions 'Exceeds free tier' and 'User: arn:aws:iam::008971676073:user/bansijiyani is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:008971676073:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action'.

The bottom of the page features a footer with '© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

10. Now we give access to this user for the EC2. So go to the user create page



Click to the Add permission and select attach policy directly.

Step 2
Review

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, inline policies, and any existing permissions boundaries 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 (1225)

Search Filter by Type All types

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AccessAnalyzerServiceRolePolicy	AWS managed	0
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	0
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	0
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanst...	AWS managed	0
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	0
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	0
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	0
<input type="checkbox"/>	AlexaForBusinessLifsizeDelegatedAcc...	AWS managed	0
<input type="checkbox"/>	AlexaForBusinessNetworkProfileServic...	AWS managed	0
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccess...	AWS managed	0
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	AWS managed	0

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Here you can see different type of access.

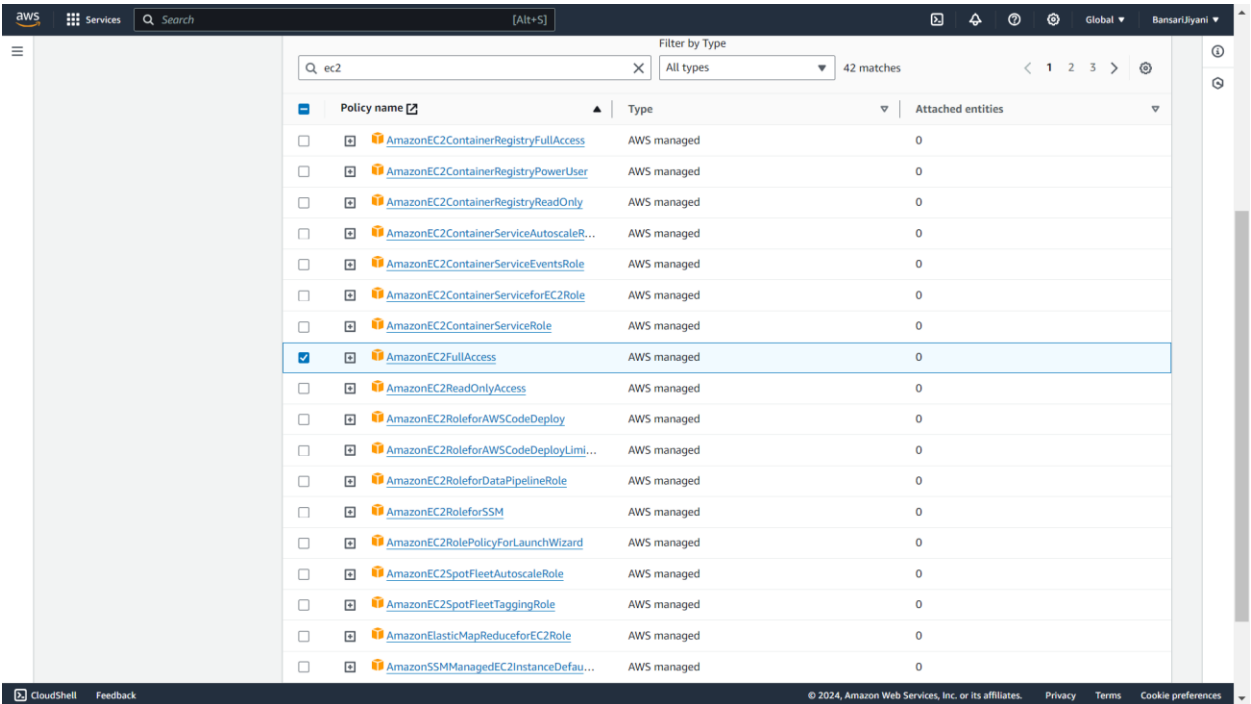
Permissions policies (1225)

Search ec2 Filter by Type All types 42 matches

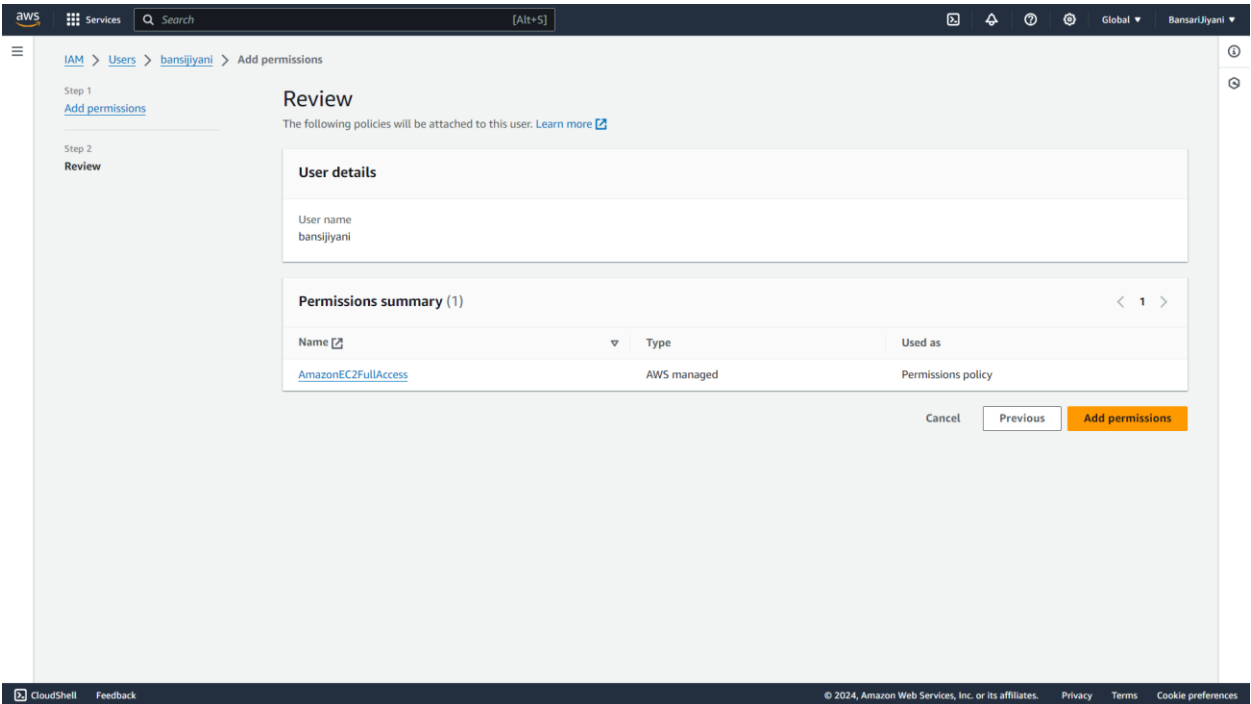
<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonEC2ContainerRegistryFullAccess	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerRegistryPowerUser	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerRegistryReadOnly	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerServiceAutoscale...	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerServiceEventsRole	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerServiceforEC2Role	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerServiceRole	AWS managed	0
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	0
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS managed	0
<input type="checkbox"/>	AmazonEC2RoleforAWSCodeDeploy	AWS managed	0
<input type="checkbox"/>	AmazonEC2RoleforAWSCodeDeployLI...	AWS managed	0
<input type="checkbox"/>	AmazonEC2RoleforDataPipelineRole	AWS managed	0
<input type="checkbox"/>	AmazonEC2RoleforSSM	AWS managed	0
<input type="checkbox"/>	AmazonEC2RolePolicyForLaunchWizard	AWS managed	0
<input type="checkbox"/>	AmazonEC2SpotFleetAutoscaleRole	AWS managed	0
<input type="checkbox"/>	AmazonEC2SpotFleetTaggingRole	AWS managed	0
<input type="checkbox"/>	AmazonElasticMapReduceforEC2Role	AWS managed	0

https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-1... © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

I want to give full access so that it can be read or write both and user get full permission for create any service/machine.



Add this permission.



Now you can see here your permission which you gave to the user in permission policies.

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
 - Analyzer settings
- Credential report
- Organization activity
- Service control policies

Related consoles

- IAM Identity Center
- AWS Organizations

1 policy added

bansijiyani Info Delete

Summary

ARN: `arn:aws:iam::008971676073:user/bansijiyani`

Console access: Enabled without MFA

Access key 1: Create access key

Created: August 05, 2024, 22:45 (UTC+05:30)

Last console sign-in: Today

Permissions Groups Tags Security credentials Access Advisor

Permissions policies (1) Remove Add permissions

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

Search Filter by Type: All types

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	Directly

Permissions boundary (not set)

Also add IAM read only access and check the permission.

1 policy added

☐ 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.

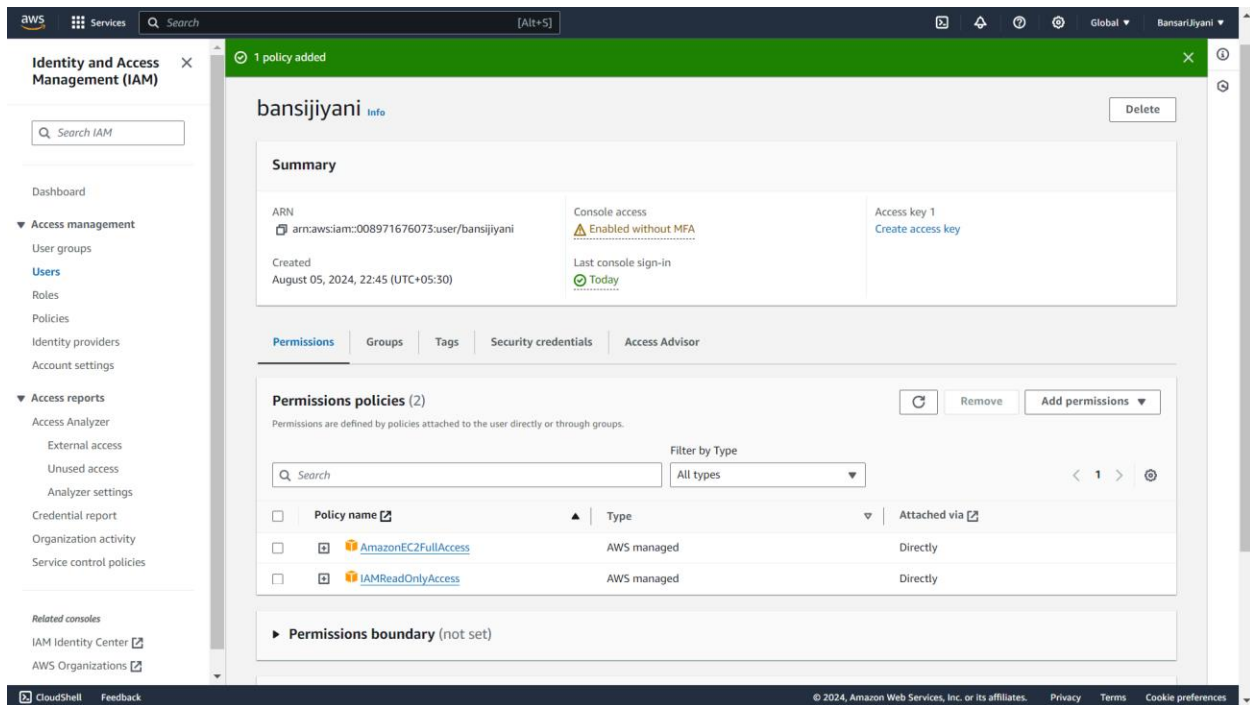
☐ Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.

☒ **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.

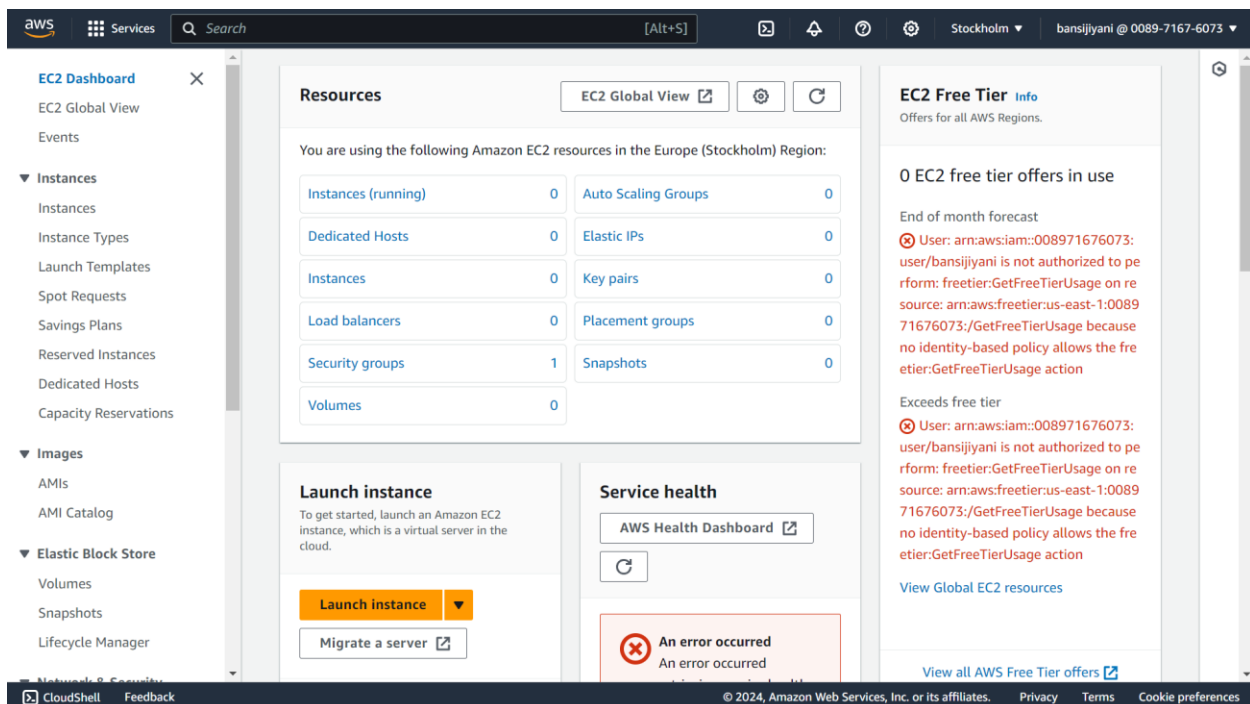
Permissions policies (1/1224) Filter by Type: All types 10 matches

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AWSIAMIdentityCenterAllowListForDe...	AWS managed	0
<input type="checkbox"/>	AWSQuickSightListIAM	AWS managed	0
<input type="checkbox"/>	IAMAccessAdvisorReadOnly	AWS managed	0
<input type="checkbox"/>	IAMAccessAnalyzerFullAccess	AWS managed	0
<input type="checkbox"/>	IAMAccessAnalyzerReadOnlyAccess	AWS managed	0
<input type="checkbox"/>	IAMFullAccess	AWS managed	0
<input checked="" type="checkbox"/>	IAMReadOnlyAccess	AWS managed	0
<input type="checkbox"/>	IAMSetManagedServiceSpecificCredenti...	AWS managed	0
<input type="checkbox"/>	IAMUserChangePassword	AWS managed	0
<input type="checkbox"/>	IAMUserSSHKeys	AWS managed	0

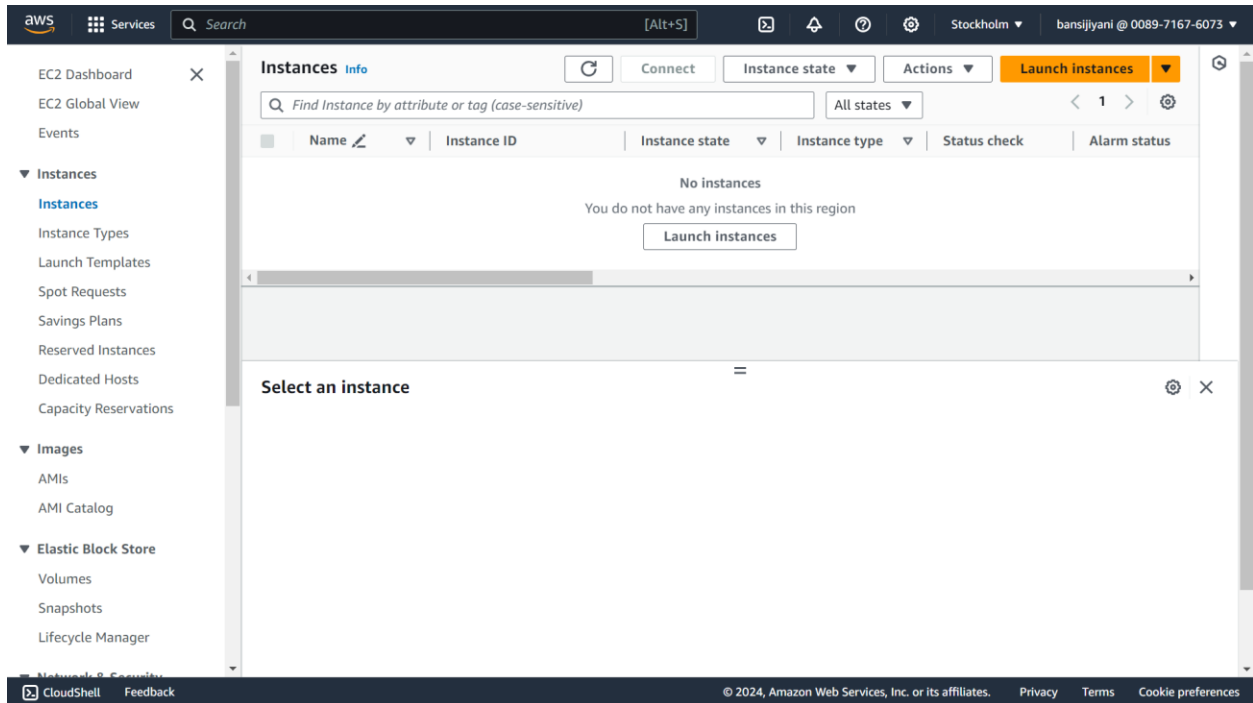
Cancel Next



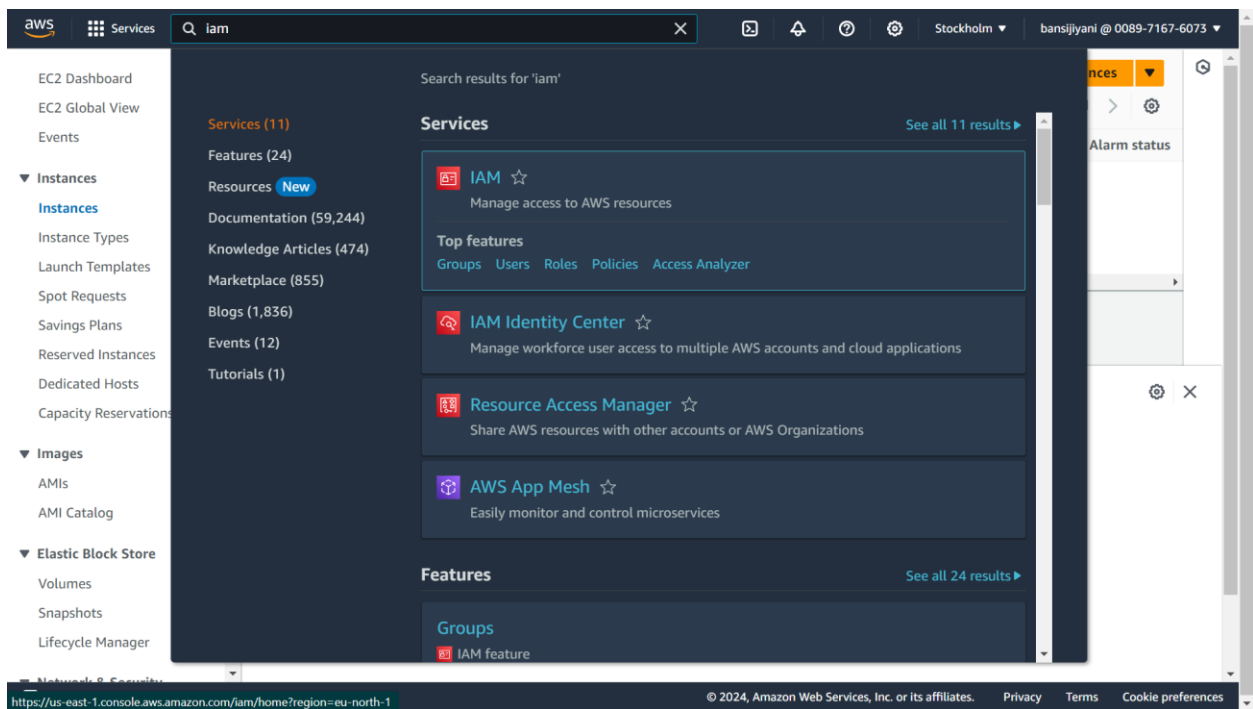
Now go to the user dashboard and check the permission.



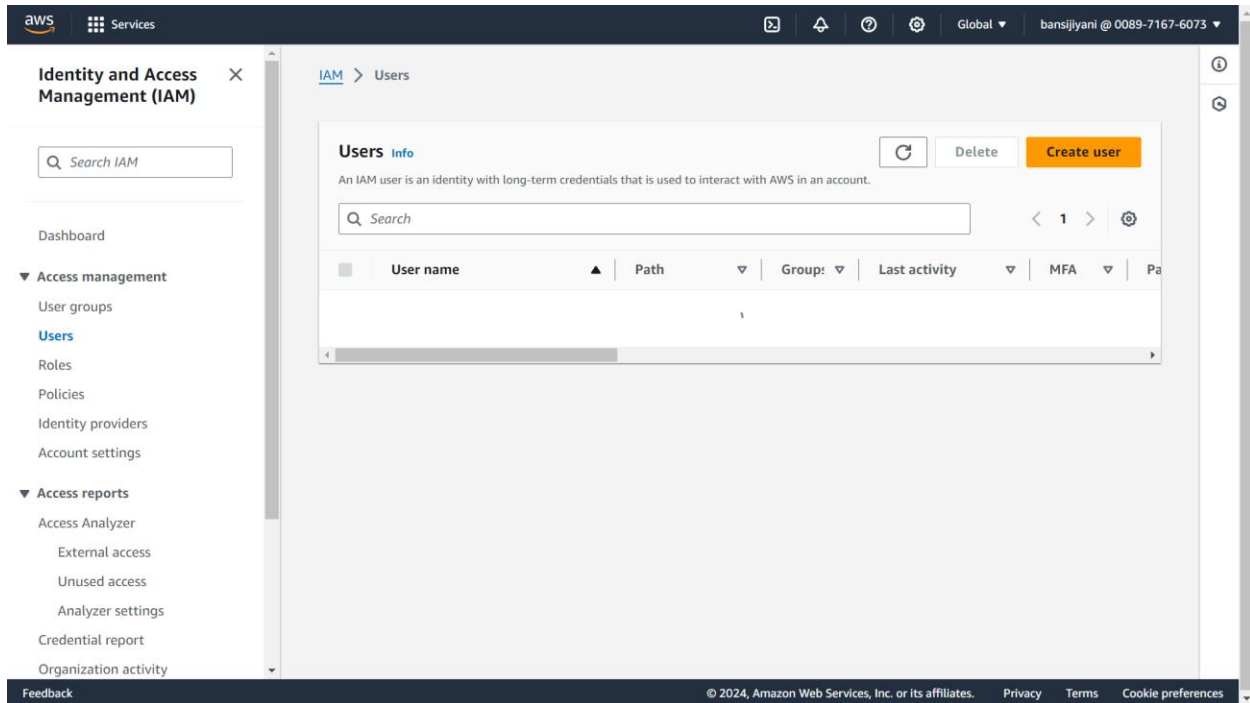
Now it is ready to create instance.



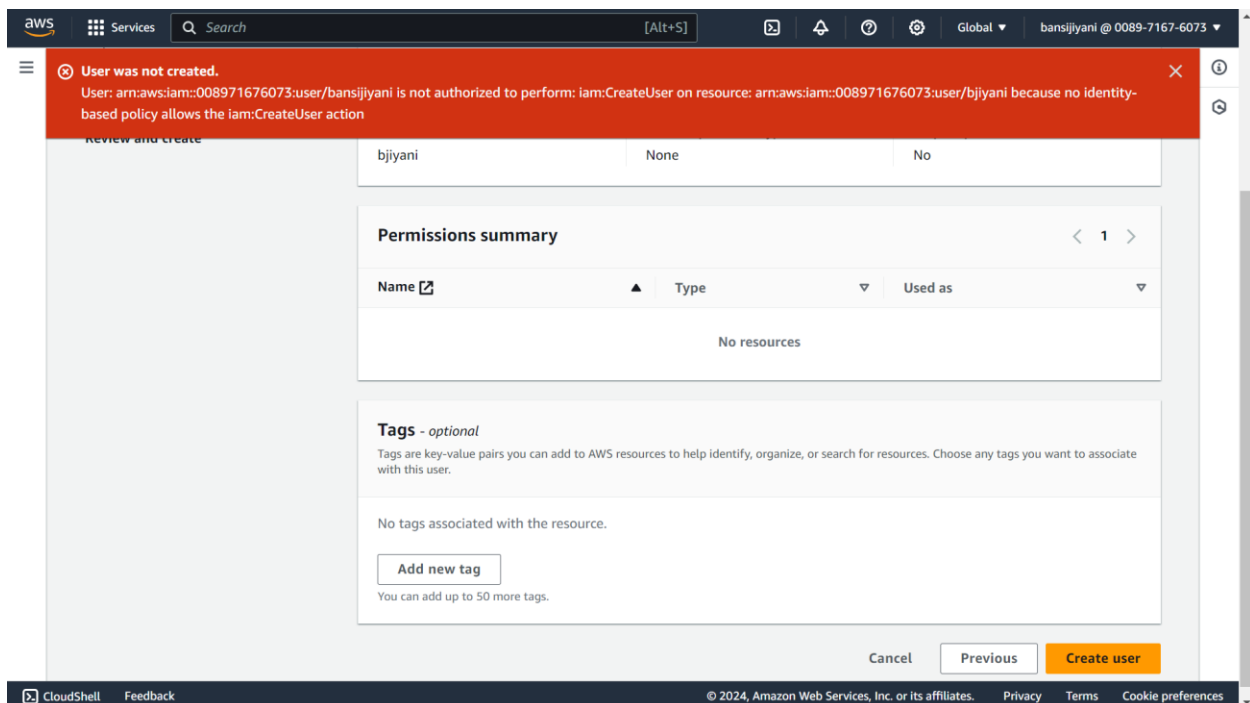
Now go to the IAM in user dashboard and create user.



Create a user in this service.



When we create the user it throws error because we are not giving the permission in main user for create another user in IAM.

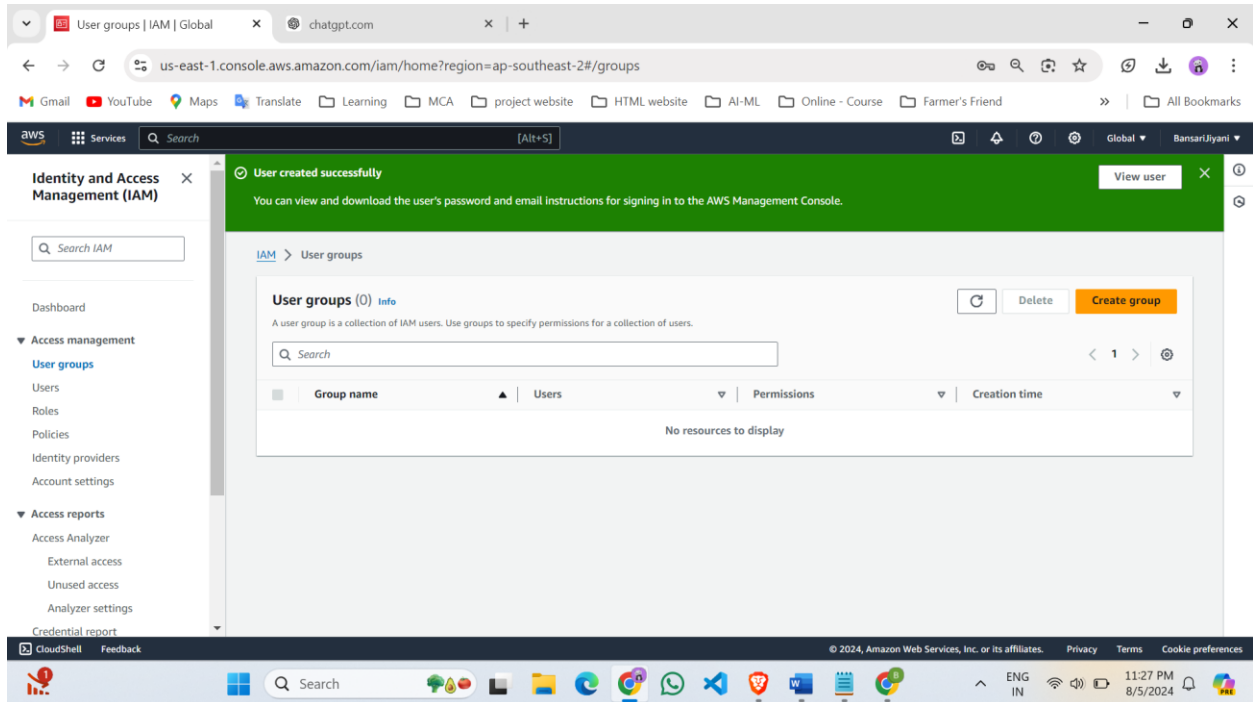


We have to give permission for any access.

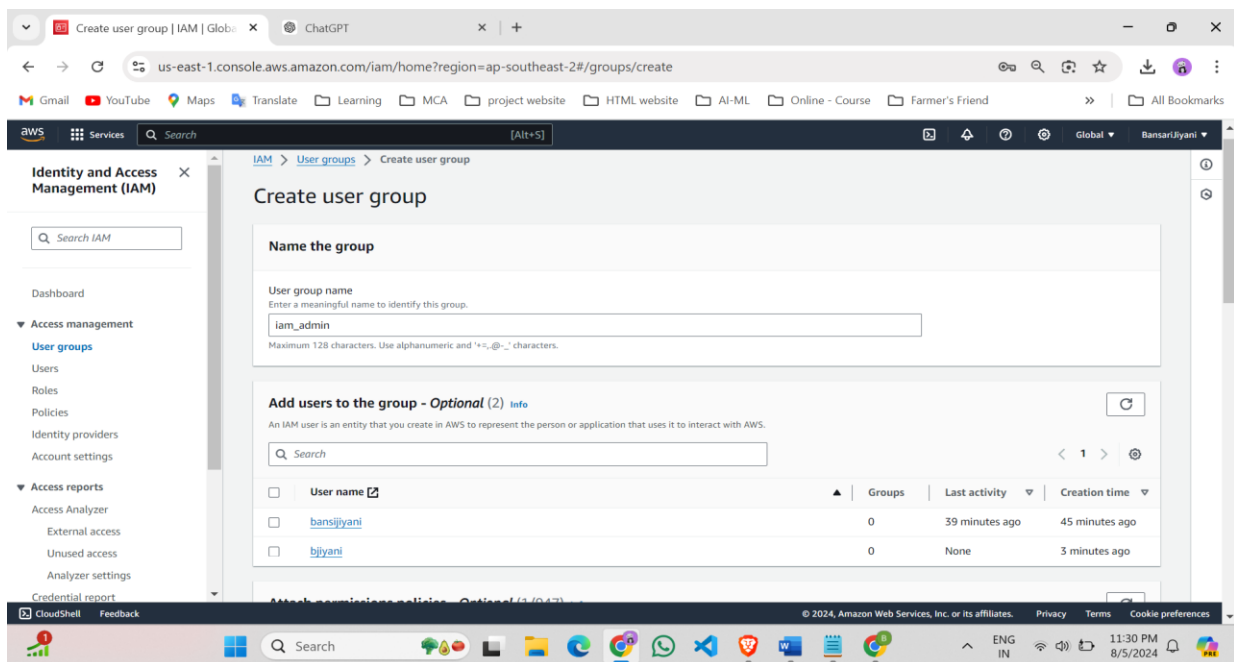
User Groups :

We can also create a Groups like user name.

1. Create group.



2. Give the group name.



3. Give this permission for full access.

The screenshot displays the AWS IAM console interface. The left sidebar shows the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access Analyzer, External access, Unused access, Analyzer settings, and Credential report. The main content area shows the 'AdministratorAccess' policy, which is an AWS managed job function policy that provides full access to AWS services and resources. The policy's JSON definition is displayed, showing a single statement with 'Effect': 'Allow' and 'Resource': '*'. Below the JSON, a table lists other AWS managed policies, including 'AdministratorAccess-Am...', 'AdministratorAccess-AW...', 'AlexaForBusinessDeviceS...', 'AlexaForBusinessFullAccess', 'AlexaForBusinessGatewa...', and 'AlexaForBusinessLifese...'. The bottom of the screen shows the Windows taskbar with various application icons and the system clock indicating 11:30 PM on 8/5/2024.

Policy name	Type	Used as	Description
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
AdministratorAccess Provides full access to AWS services and resources.			
<pre>1 { 2 "Version": "2012-10-17", 3 "Statement": [4 { 5 "Effect": "Allow", 6 "Action": "*", 7 "Resource": "*" } 8] 9 } 10</pre>			
<input type="checkbox"/> AdministratorAccess-Am...	AWS managed	None	Grants account administrative permissi...
<input type="checkbox"/> AdministratorAccess-AW...	AWS managed	None	Grants account administrative permissi...
<input type="checkbox"/> AlexaForBusinessDeviceS...	AWS managed	None	Provide device setup access to AlexaFo...
<input type="checkbox"/> AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
<input type="checkbox"/> AlexaForBusinessGatewa...	AWS managed	None	Provide gateway execution access to A...
<input type="checkbox"/> AlexaForBusinessLifese...	AWS managed	None	Provide access to Lifesize AVS devices

We can also create a user and groups as per our choice.