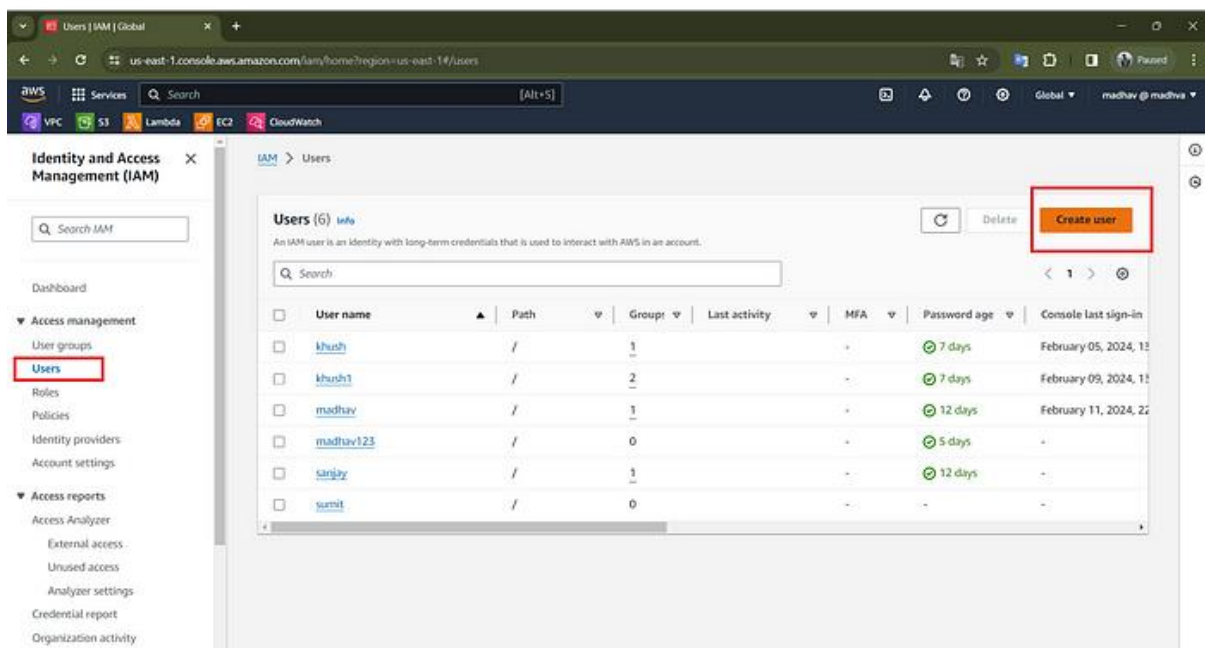


IAM Service

1. On the **Console Home** page, select the IAM service.
2. In the navigation pane, select **Users** and then select **Add Users**.

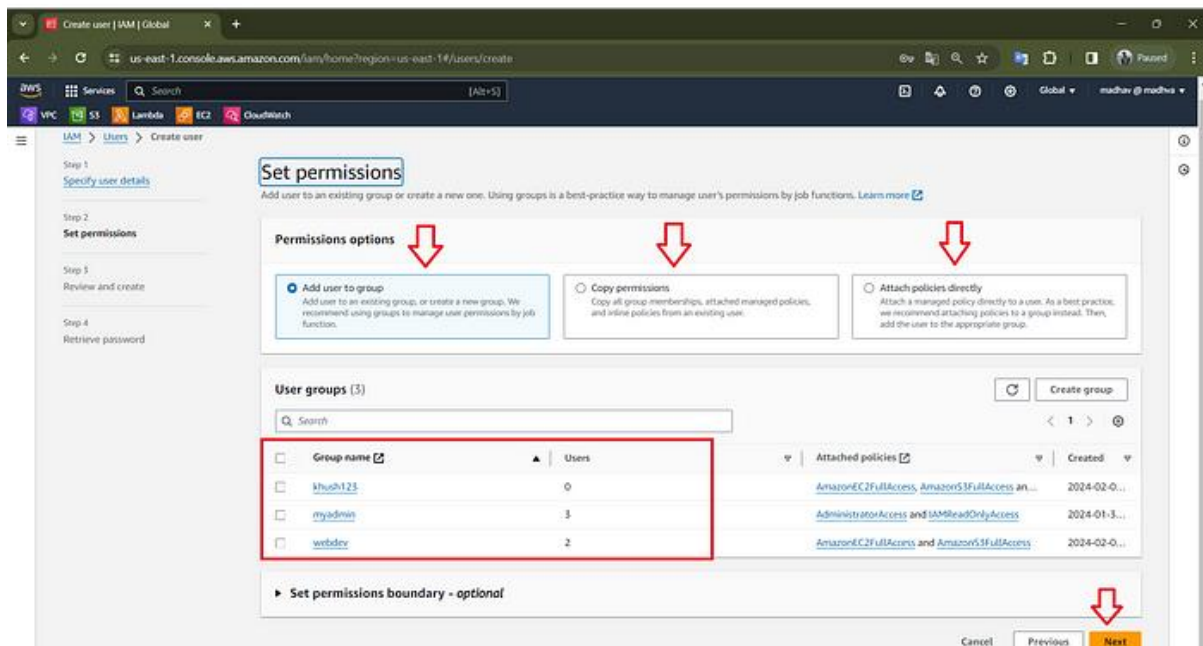


1. For the **User name**, enter **TestUser**. Names cannot contain spaces.
2. Select the check box next to **Provide user access to the AWS Management Console– optional** and then choose **I want to create an IAM user**.
3. Under **Console password**, select **Custom password**.
4. Clear the check box next to the **User must create a new password at the next sign-in (recommended)**.

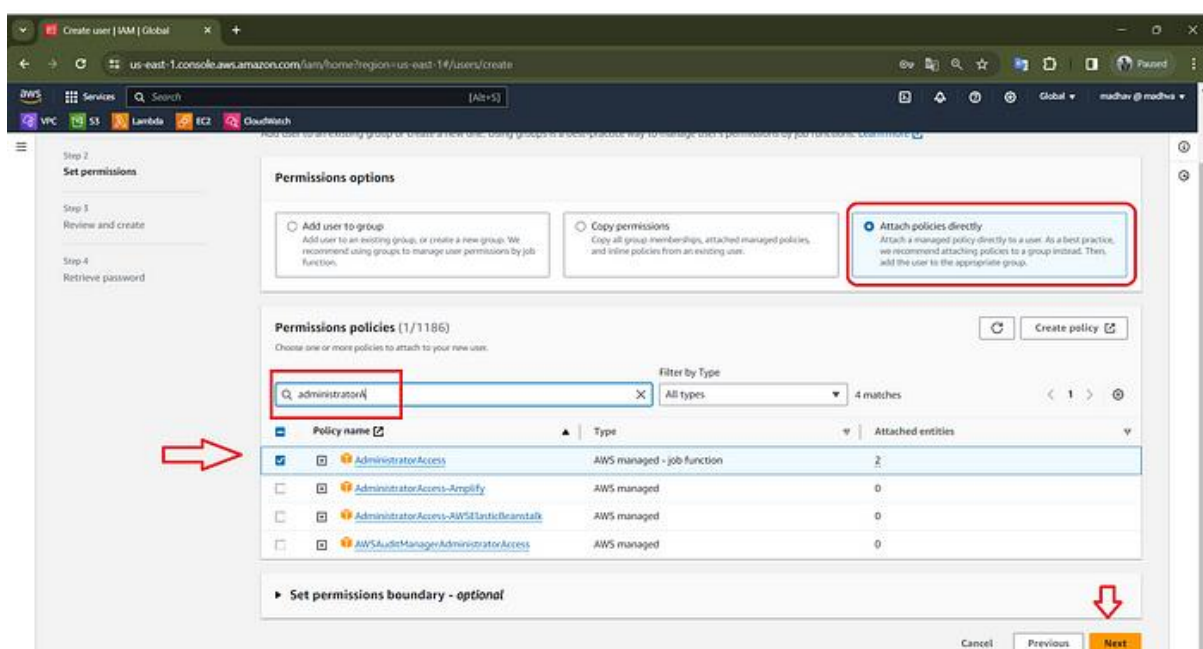
Because this IAM user is for emergency access, a trusted administrator retains the password and only provides it when needed.

The screenshot shows the 'Create user' page in the AWS IAM console, specifically the 'User details' section. The 'User name' field is highlighted with a red box and contains the text 'TestUser'. Below this, there is a checkbox for 'Provide user access to the AWS Management Console - optional', which is checked. A blue information box titled 'Are you providing console access to a person?' is visible. Under 'Console password', the 'Custom password' option is selected and highlighted with a red box. A red arrow points to the 'Next' button at the bottom right of the page.

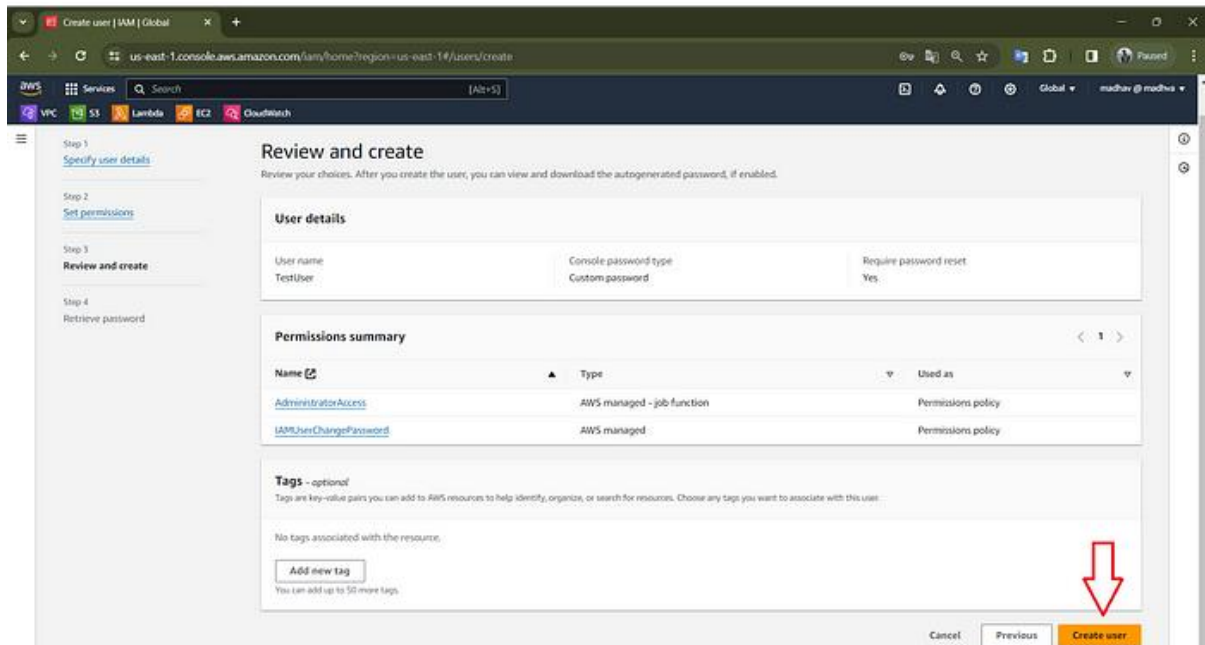
1. On the **Set permissions** page, under **Permissions options**, select **Add user to group**. so user Group you can add that particular user to the particular group and in one group have multiple users with the same permission



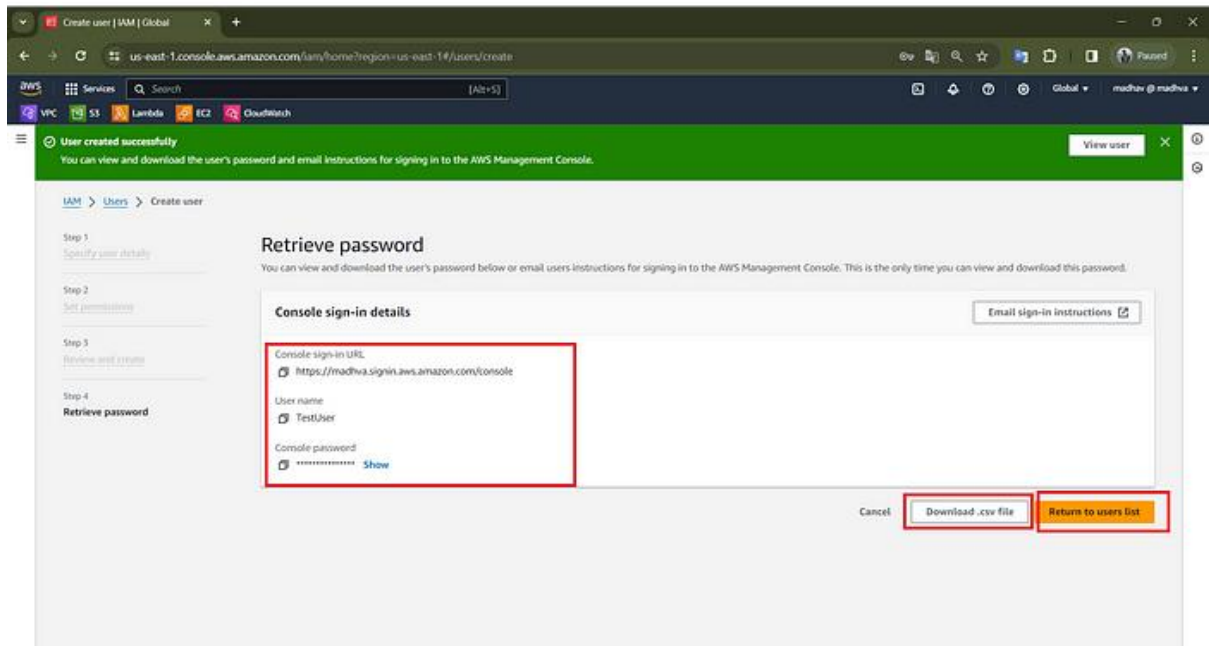
- But in my case, I am using **Attach Policies Directly**.
- under **Permissions Policies**, select the permission that you want to give to the user, Here I am using Administrator Access “best practice do go with admin access”
- Select **Next** to proceed to the **Review and Create** page.



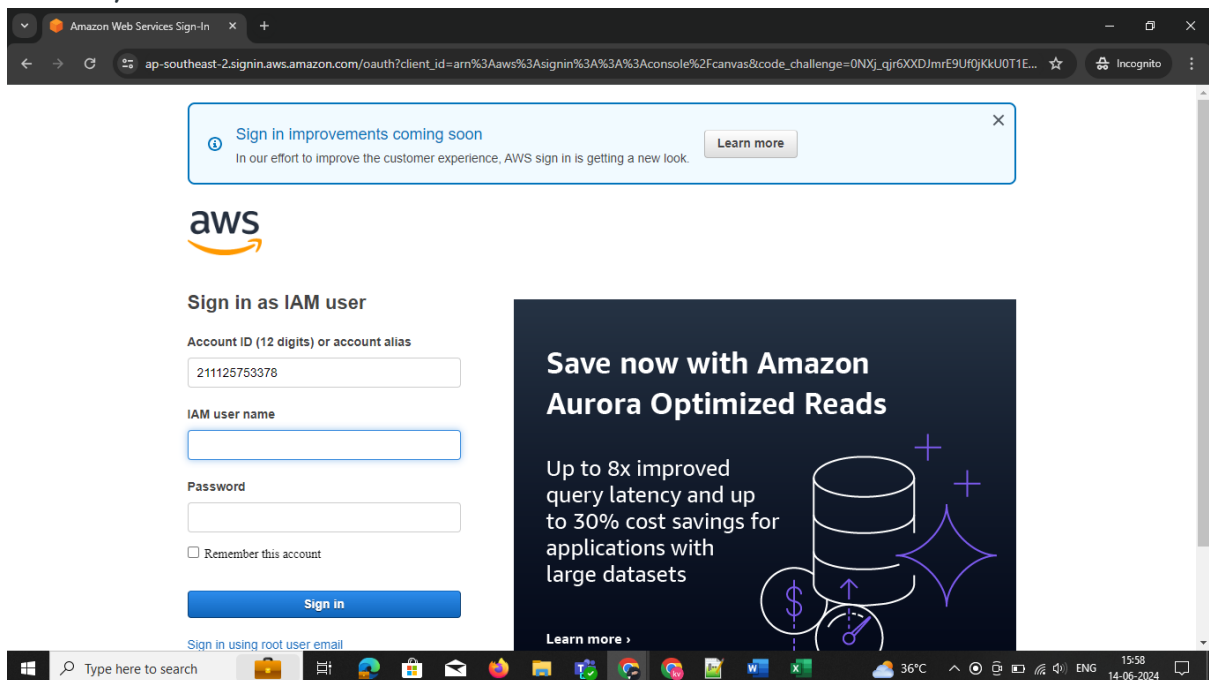
- On the **Review and Create** page, review the list of user group memberships to be added to the new user. When you are ready to proceed, select **Create User**.



- On the **Retrieve password** page, select **Download .csv file** to save a .csv file with the user credential information (Connection URL, user name, and password).
- Save this file to use if you need to sign-in to IAM and do not have access to your federated identity provider



How to login the IAM USER ones get the one how to in above url share the any one



Once giving the u-named and password now it shows this generate custom password

Amazon Web Services Sign-In

ap-southeast-2.signin.aws.amazon.com/clm?action=changepassword&userType=iam&redirect_uri=https%3A%2F%2Fconsole.aws.amazon.com%2Fconsole%2Fho...

aws

You must change your password to continue

AWS account 211125753378

IAM user name saidevopsteam

Old password

New password

Retype new password

Confirm password change

[Sign in using root user email](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2024, Amazon Web Services, Inc. or its affiliates.

Windows taskbar: Type here to search, 36°C, 16:01, 14-06-2024

Once you giving this passwords and now we need to login in to aws now we need to give the permission to AWS access key security to user IAM

Go to IAM > select user > security credentials click > create access key

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/devq?section=security_credentials

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

Console sign-in [Manage console access](#)

Console sign-in link
<https://211125753378.signin.aws.amazon.com/console>

Console password
Updated 8 days ago (2024-06-05 18:45 GMT+5:30)

Last console sign-in
8 days ago (2024-06-05 18:48 GMT+5:30)

Multi-factor authentication (MFA) (0) [Remove](#) [Resync](#) [Assign MFA device](#)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			

[Assign MFA device](#)

Access keys (1) [Create access key](#)

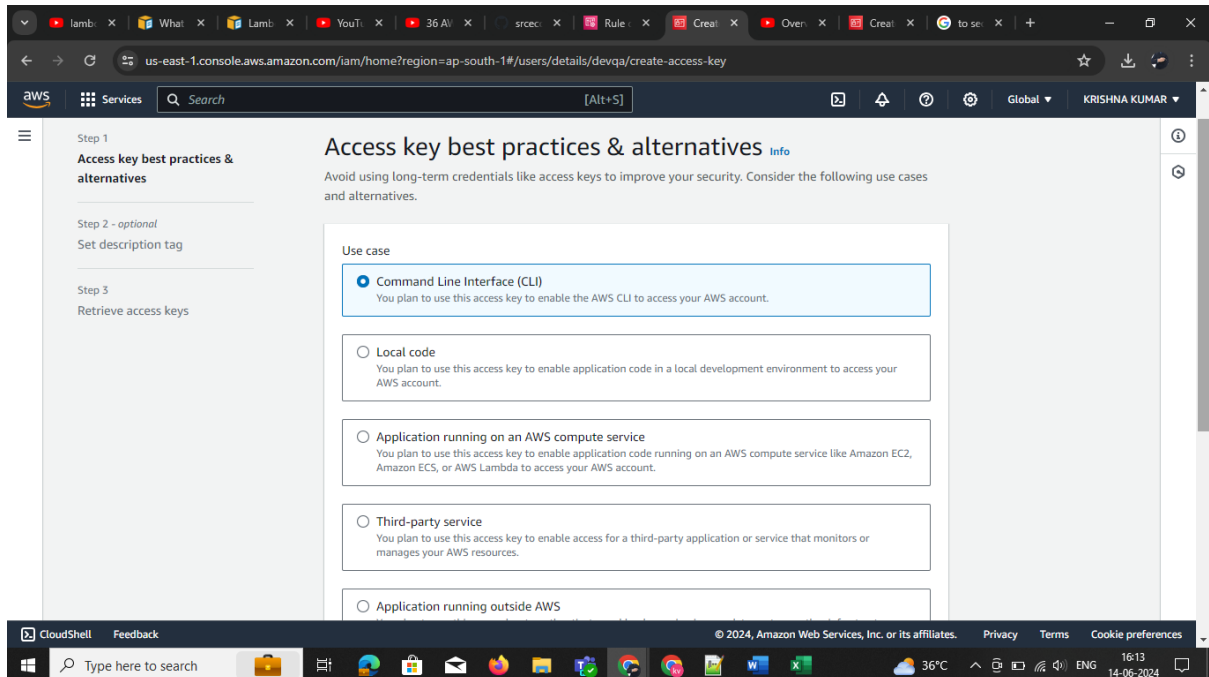
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two

CloudShell Feedback

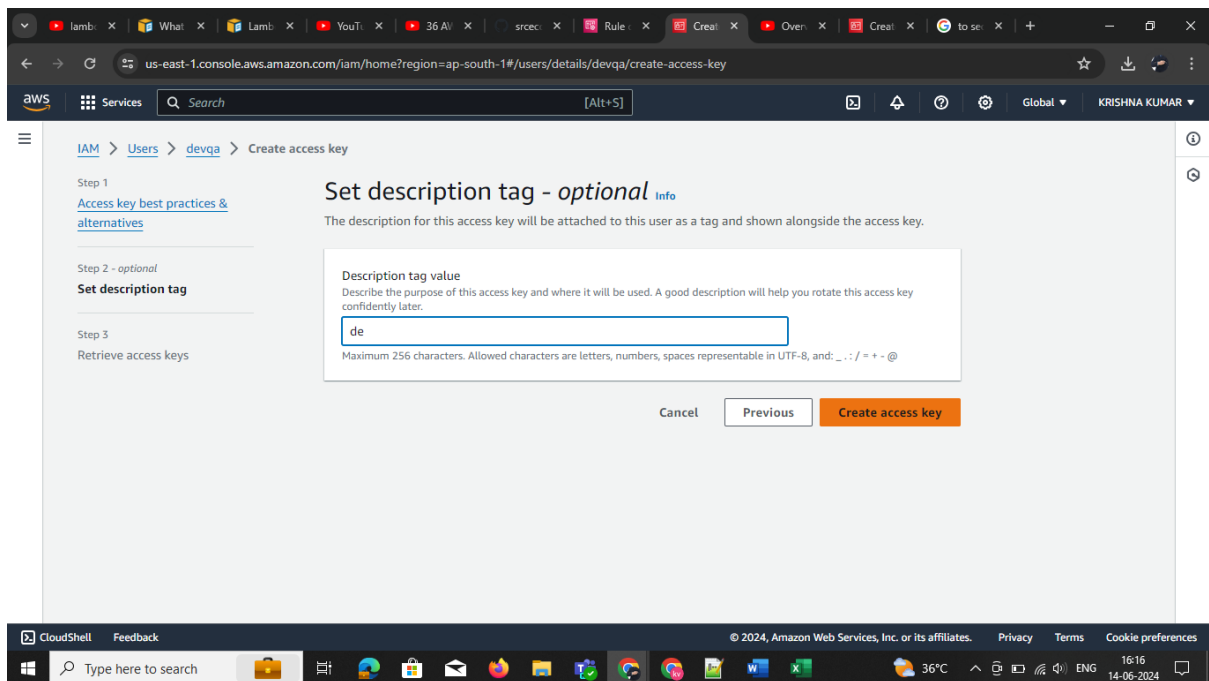
© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

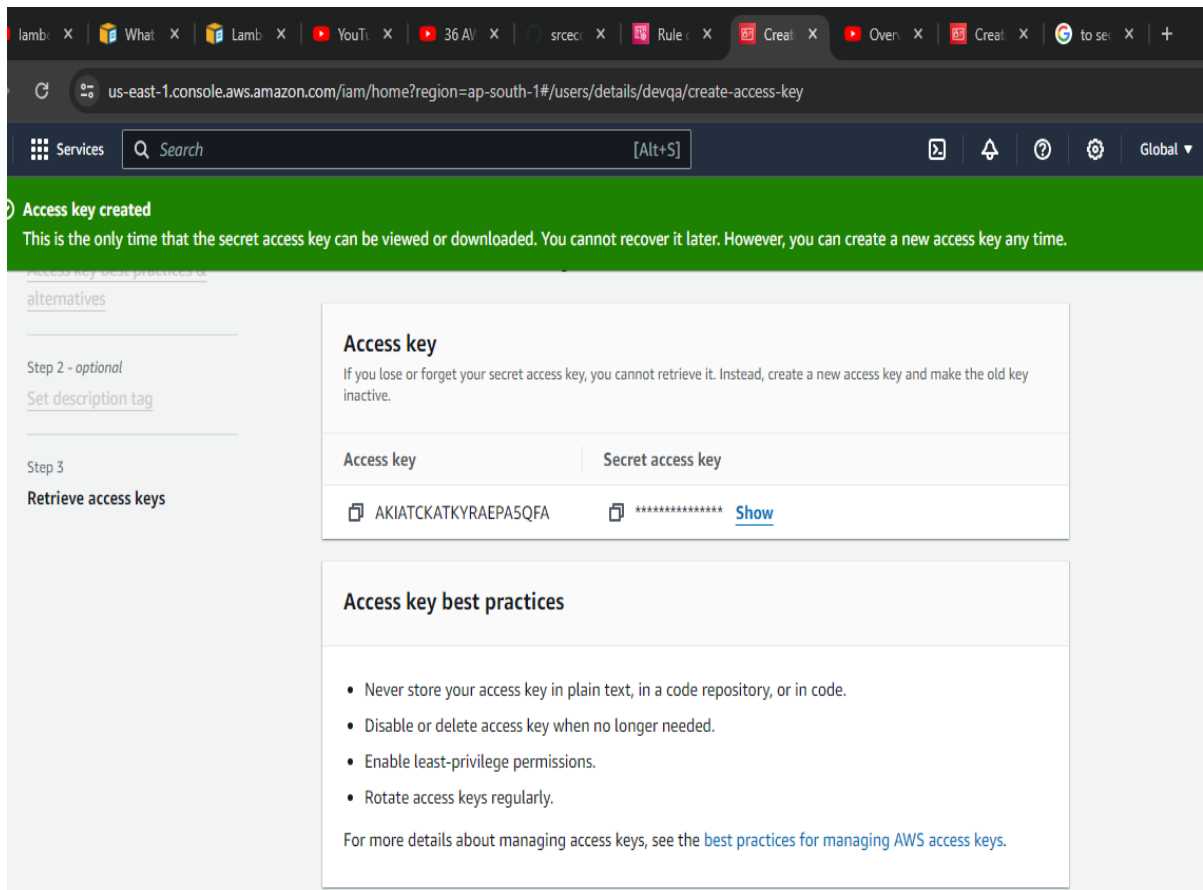
Windows taskbar: Type here to search, 36°C, 16:11, 14-06-2024

Select the > create access key



Selects one of the options go NEXT give the tag name click NEXT



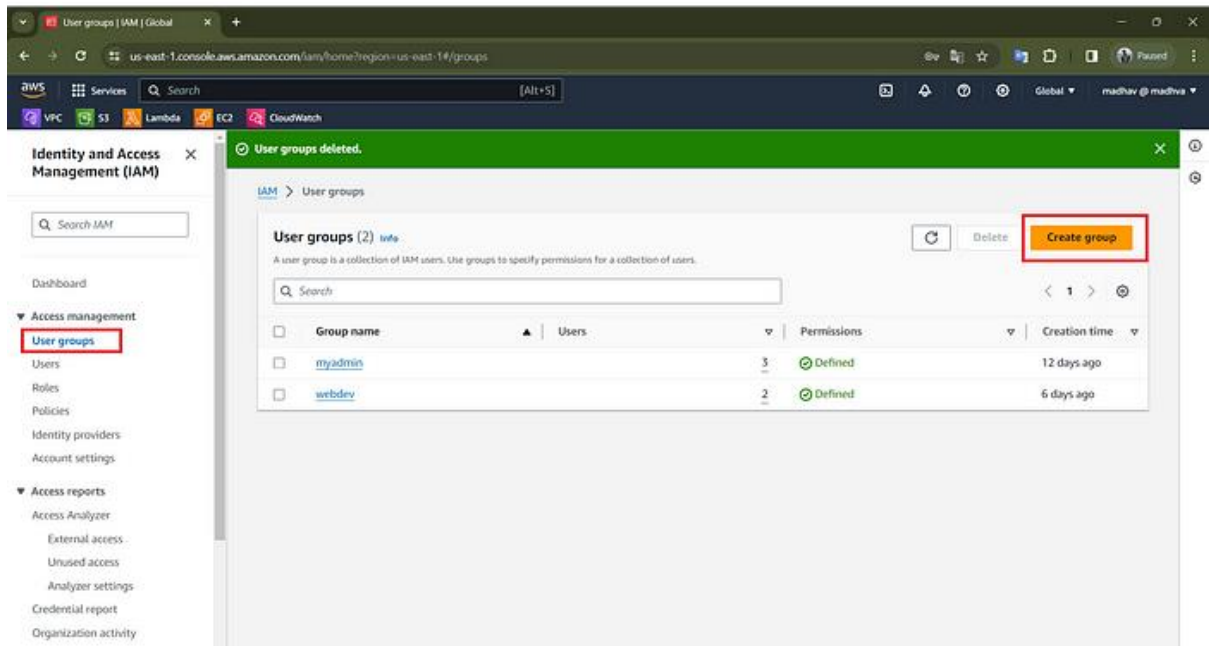


Note: don't share this key

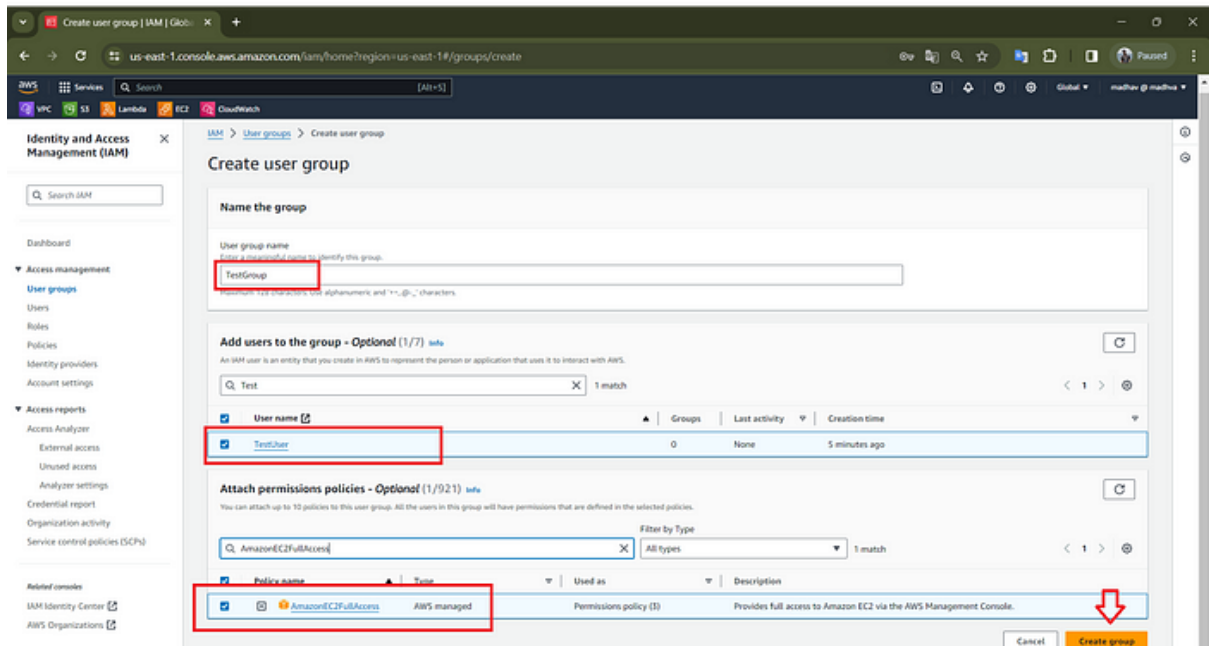
Create your first IAM user Group:

Groups make it easy to manage permissions for lots of users at once. You can put users into groups and give the whole group certain permissions. It's like giving everyone in a club the same access to club stuff.

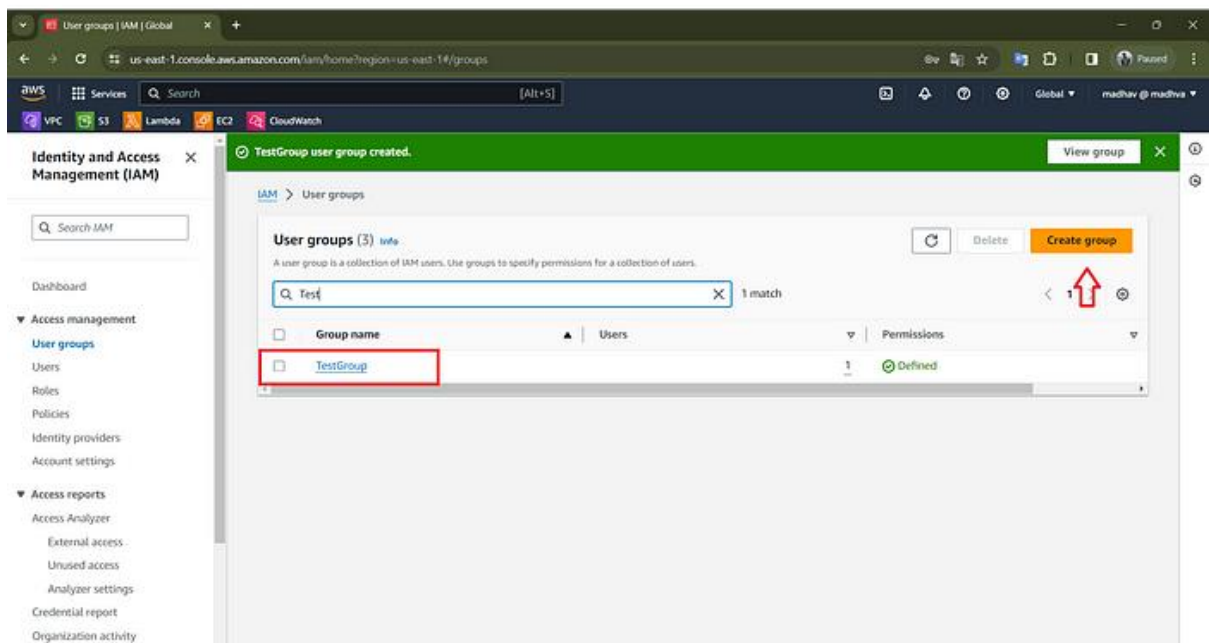
- In the navigation pane, choose **User Groups** and then choose **Create group**.



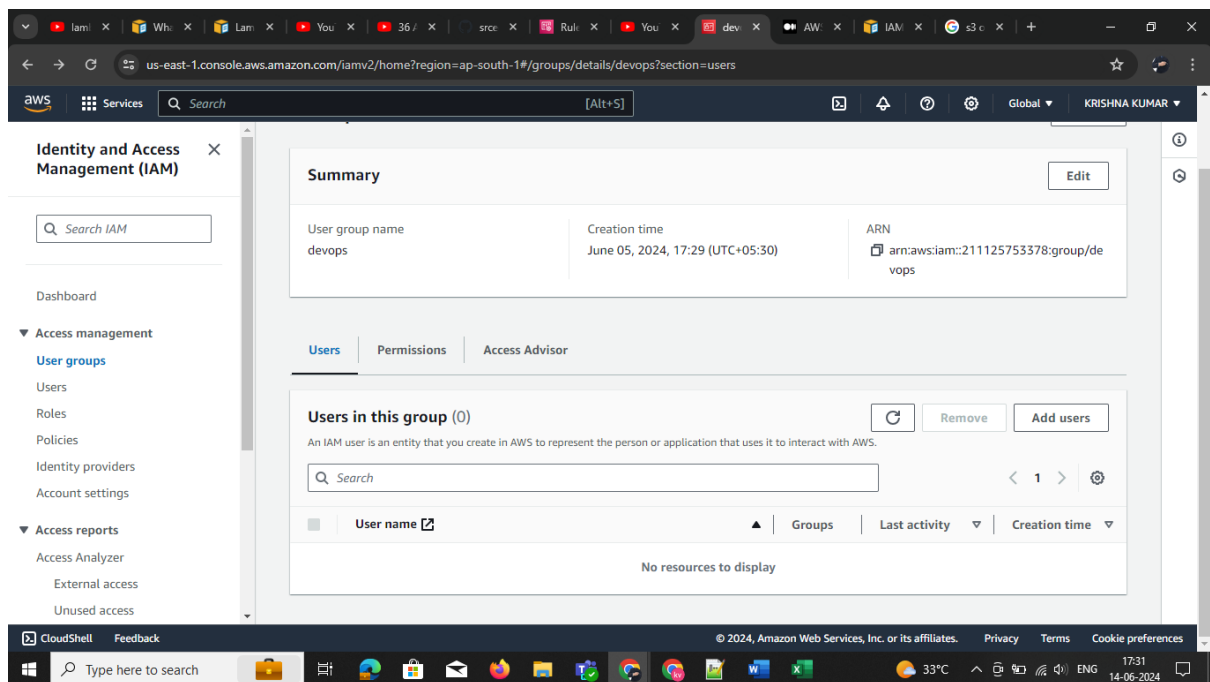
- For the **User group name**, type the name of the group.
- In the list of users, select the check box for each user that you want to add to the group, Like **Test User**.
- In the list of policies, select the check box for each policy that you want to apply to all members of the group like **AdministratorAccess**. “ Practices only”
- Choose **Create group**.



Here you can see the Group that we created, With the name of **TestGroup**



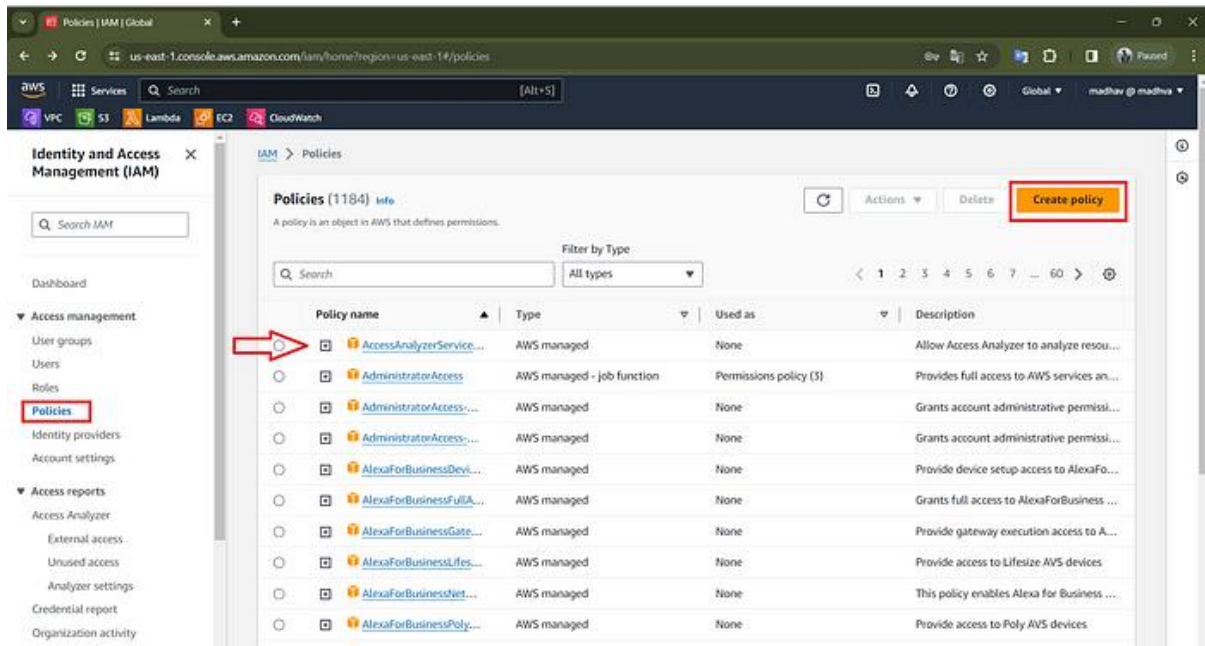
To add the use in the group > select the group add user



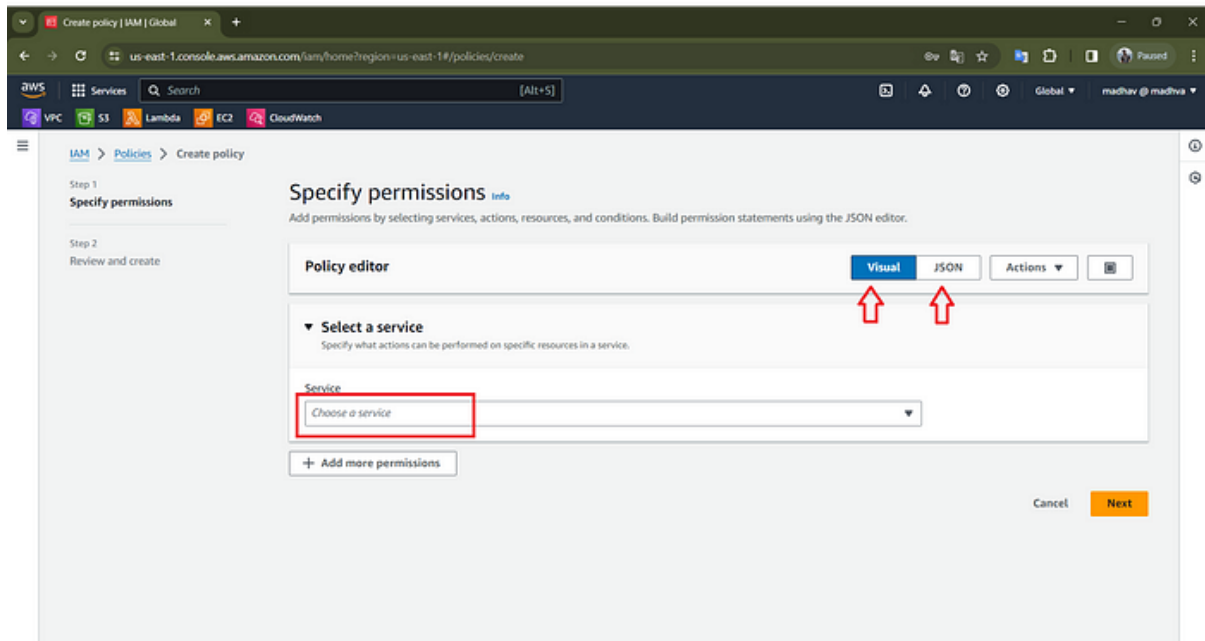
create your first IAM policy

Policies are rules that say what users and groups can or can't do in AWS. They're written in a special way called JSON. Policies make sure everyone only does what they're supposed to, which keeps everything safer.

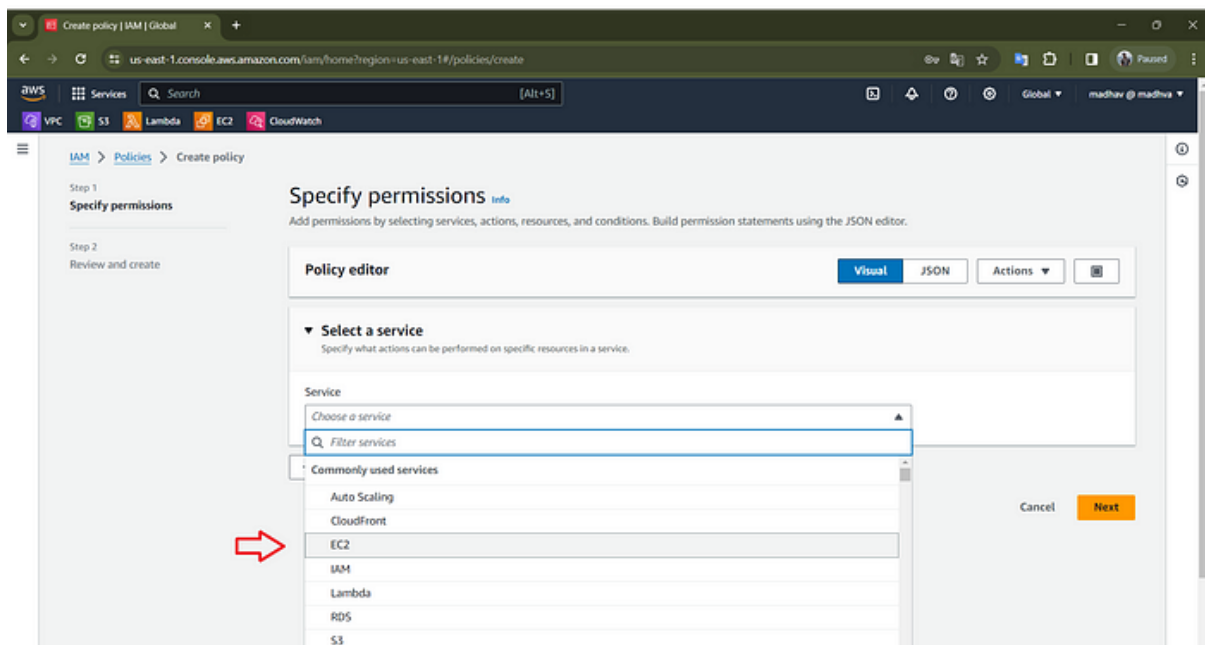
- In the navigation pane, choose **Policies**.
- If this is your first-time choosing **Policies**, the **Welcome to Managed Policies** page appears. Choose **Get Started**.
- Choose **Create policy**.



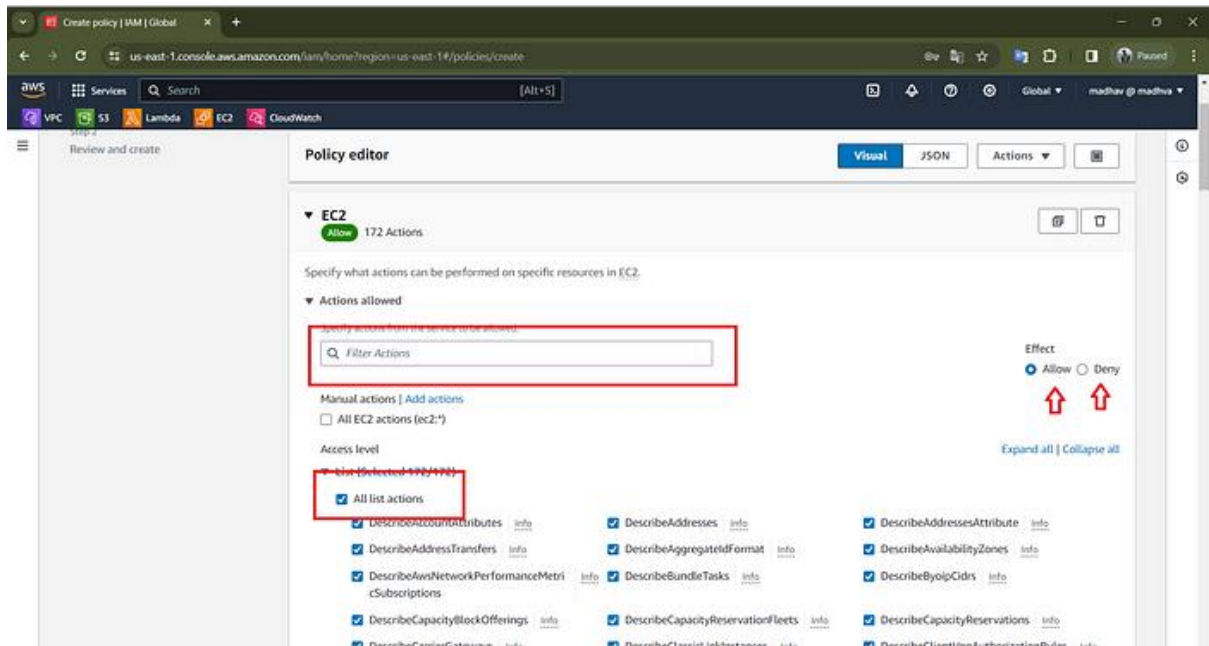
- On the **Create policy** page,
- There are two options **Visual** and **Json**
- In Visual, we can create policies manually, by using GUI



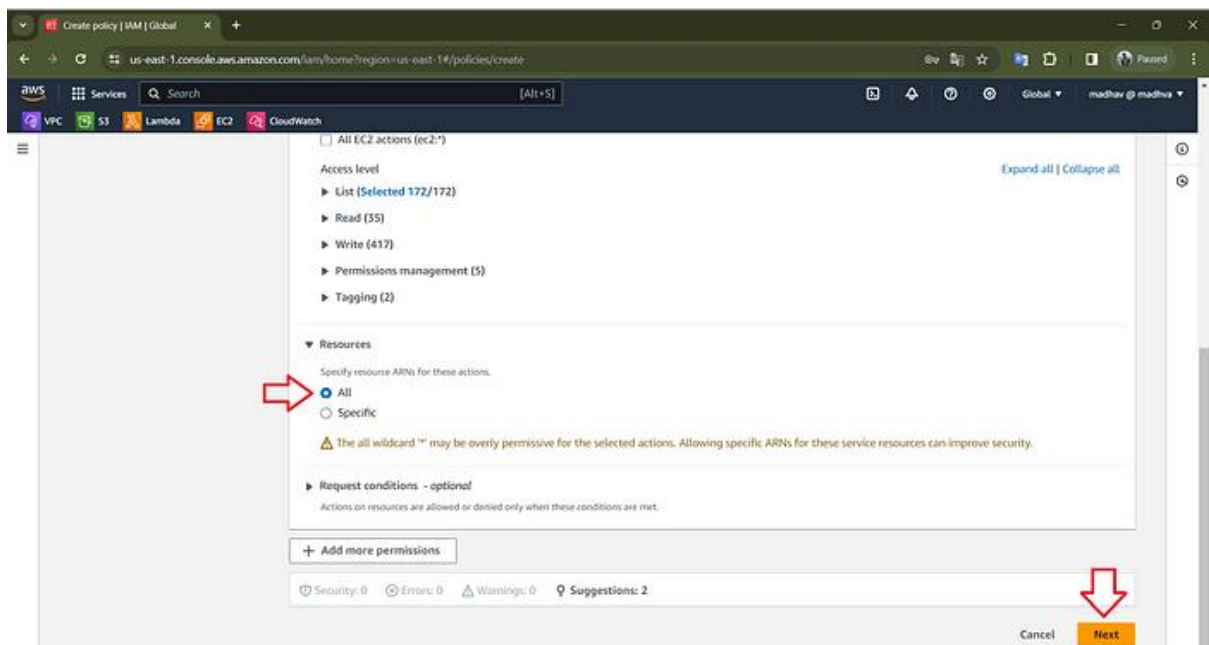
- In Json we use Json Language to create Policies, In my case I go to import policy Json
- Choose **Next**.
- In this **visual**, Under **Select a service**, We want to choose the service, for creating policies, Here I am using **EC2**
- Then Click, **Next**



Here you can choose **effect**, **Allow** and **Deny** for service, now you can select the action that you want to allow or deny



- In the **resource**, Select **All**,
- Then click **Next**,



- On the **Review and Create** page, for the **Policy name**, type **ec2ReadPloicy**. For **Description**, You can describe the Policy type.

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

Step 1
Specify permissions

Step 2
Review and create

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and "+, @, _" characters.

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and "+, @, _" characters.

Permissions defined in this policy

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Allow (1 of 404 services) Show remaining 403 services

- Then choose **Create policy** to save the policy.

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

Step 1
Specify permissions

Step 2
Review and create

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and "+, @, _" characters.

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and "+, @, _" characters.

Permissions defined in this policy

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Allow (1 of 404 services) Show remaining 403 services

Service	Access level	Resource	Request condition
EC2	Full: List	All resources	None

Add tags - optional

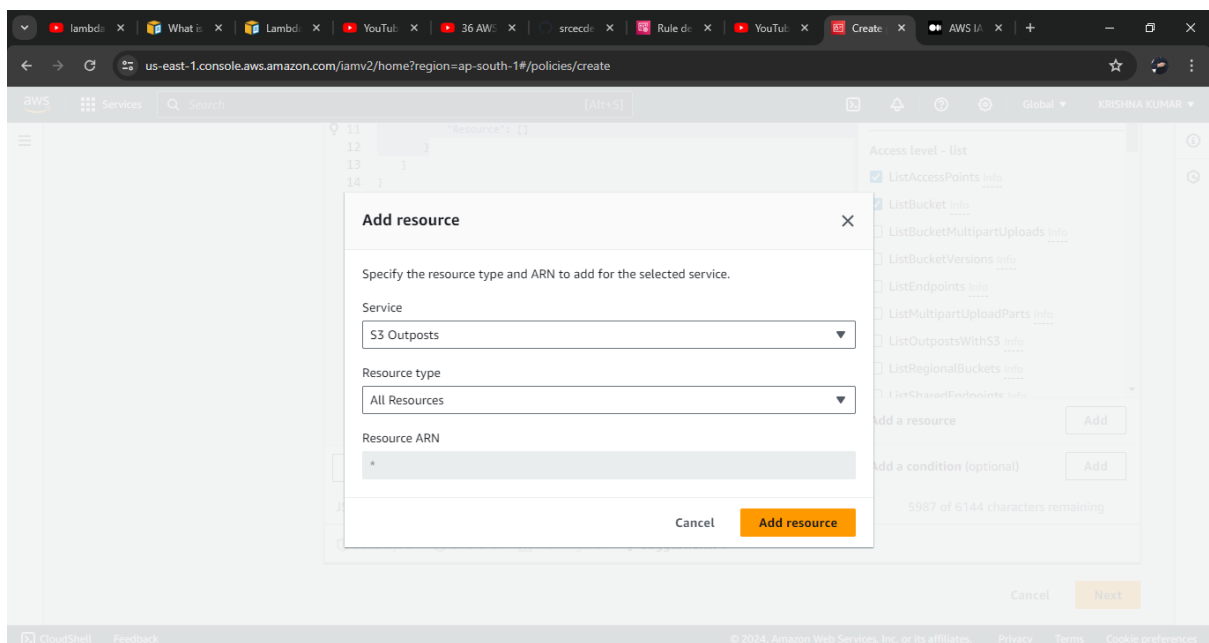
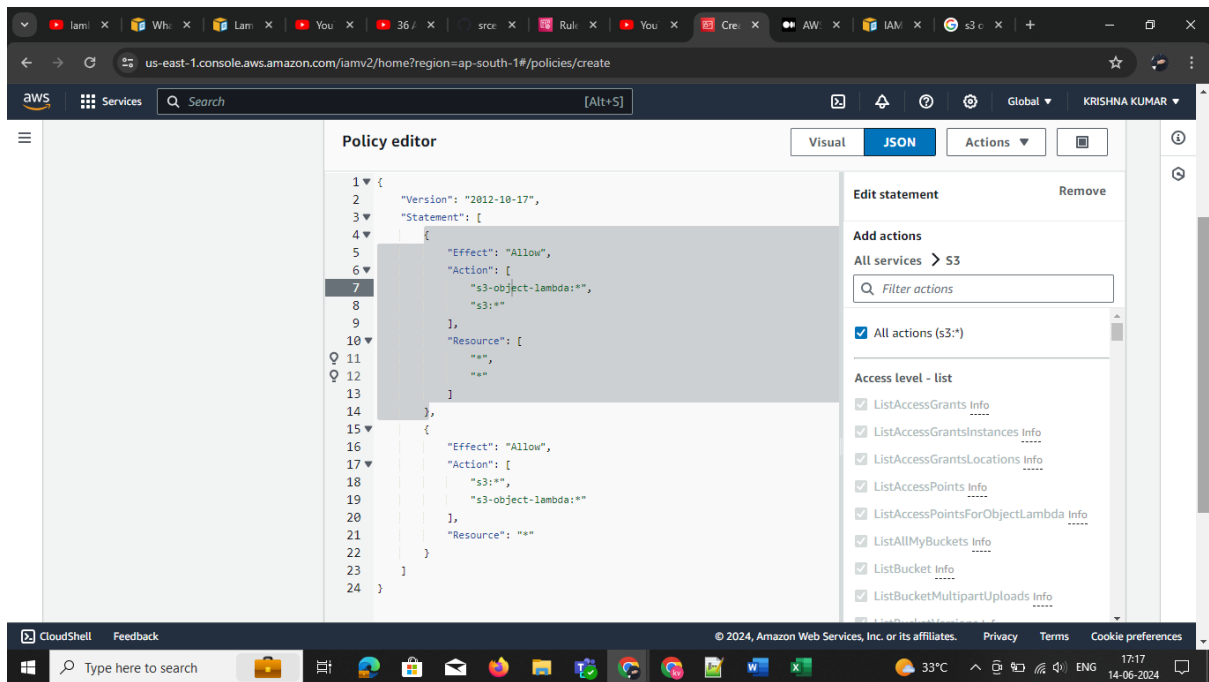
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

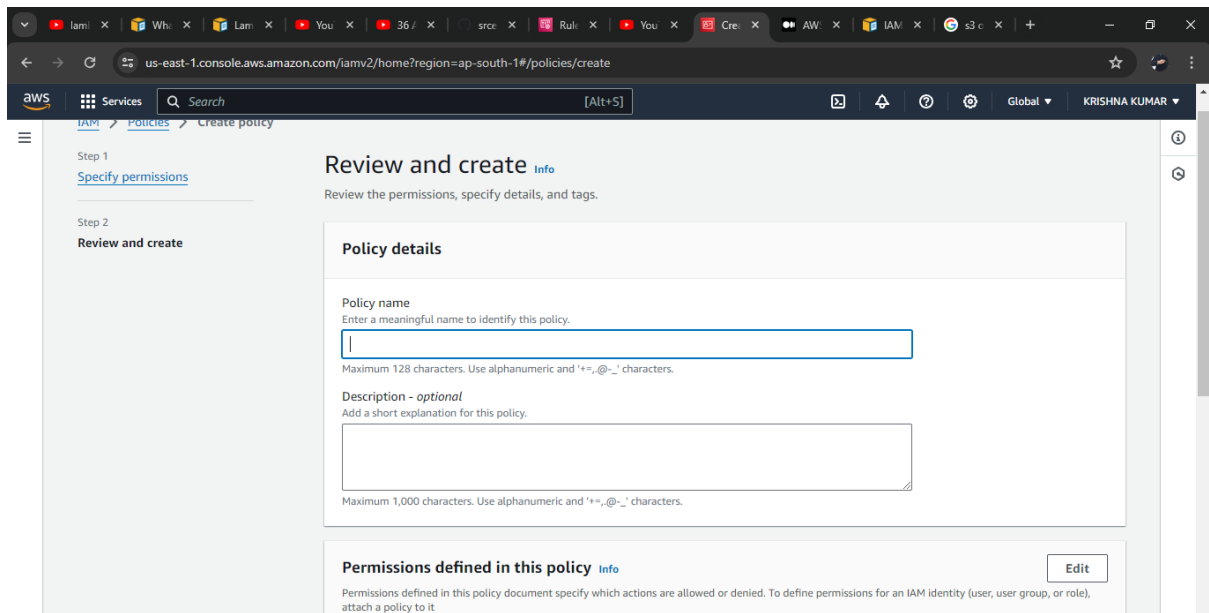
No tags associated with the resource.

You can add up to 50 more tags.

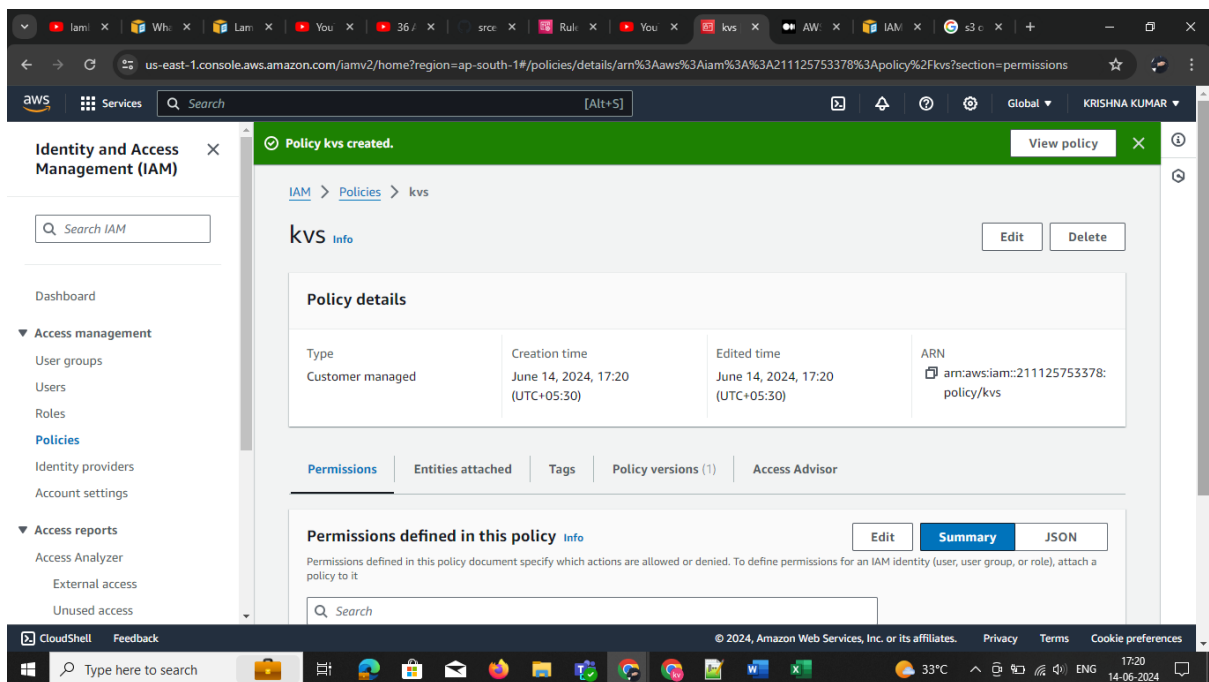
Cancel

Here you can see the Policy that we created, With the name that you gave, Here You need to search for the Policy Because in AWS there Are many policies exist.





Get to polices and search with name

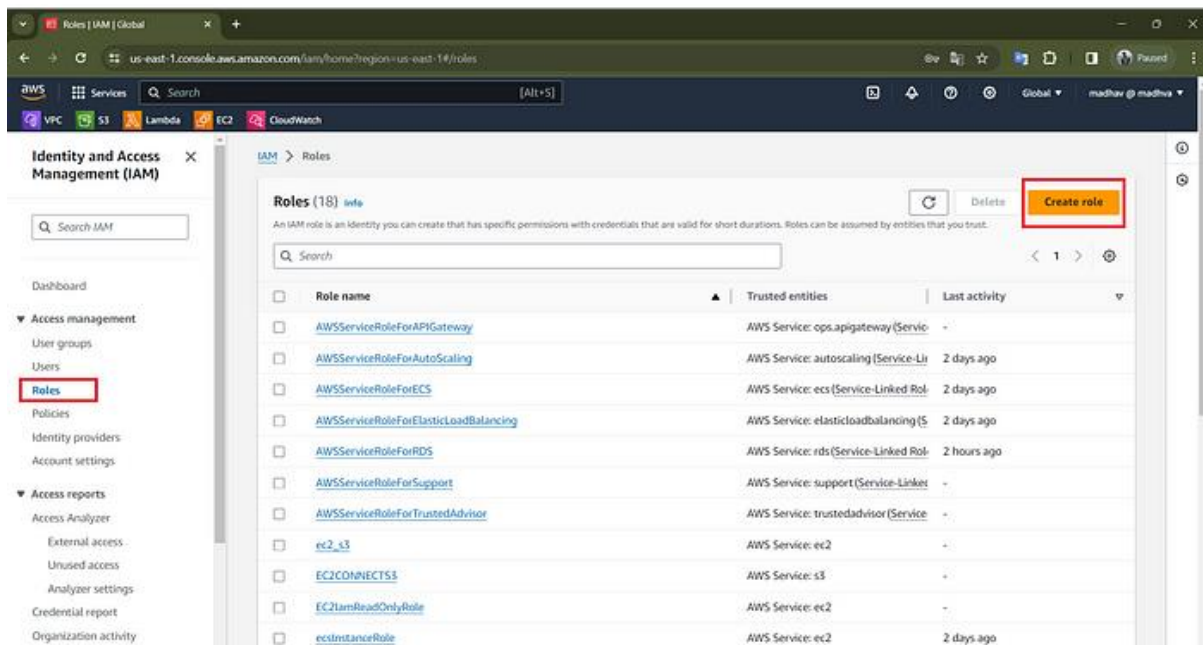


Create your first role:

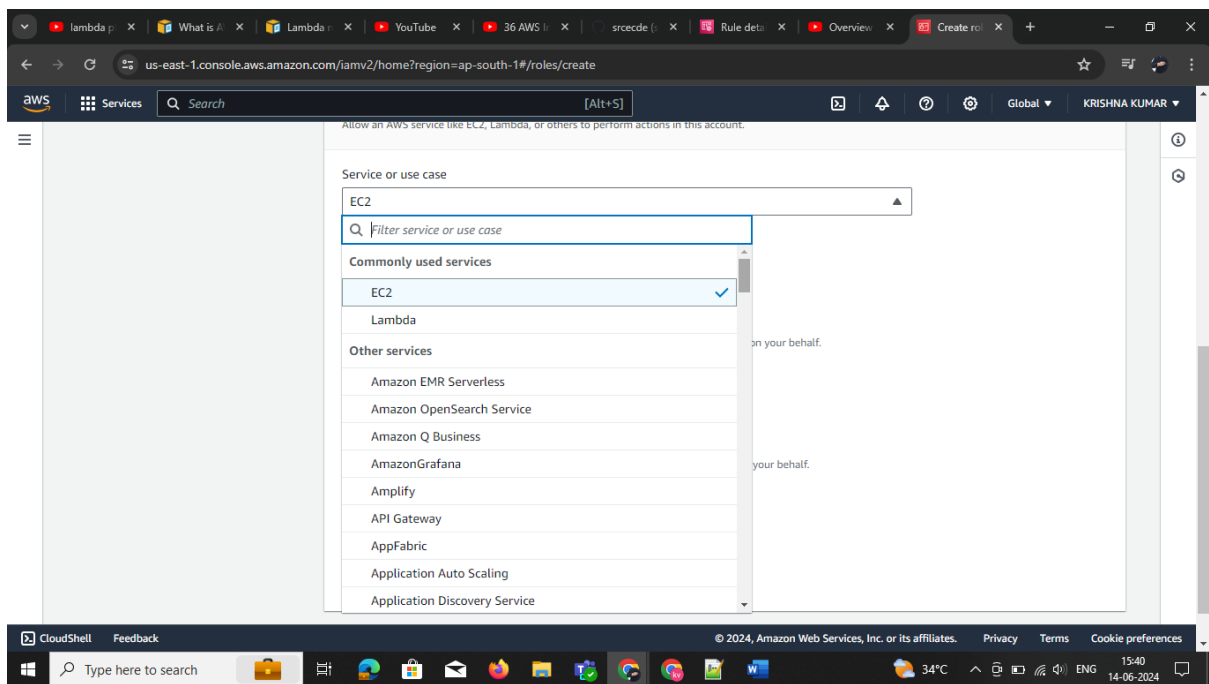
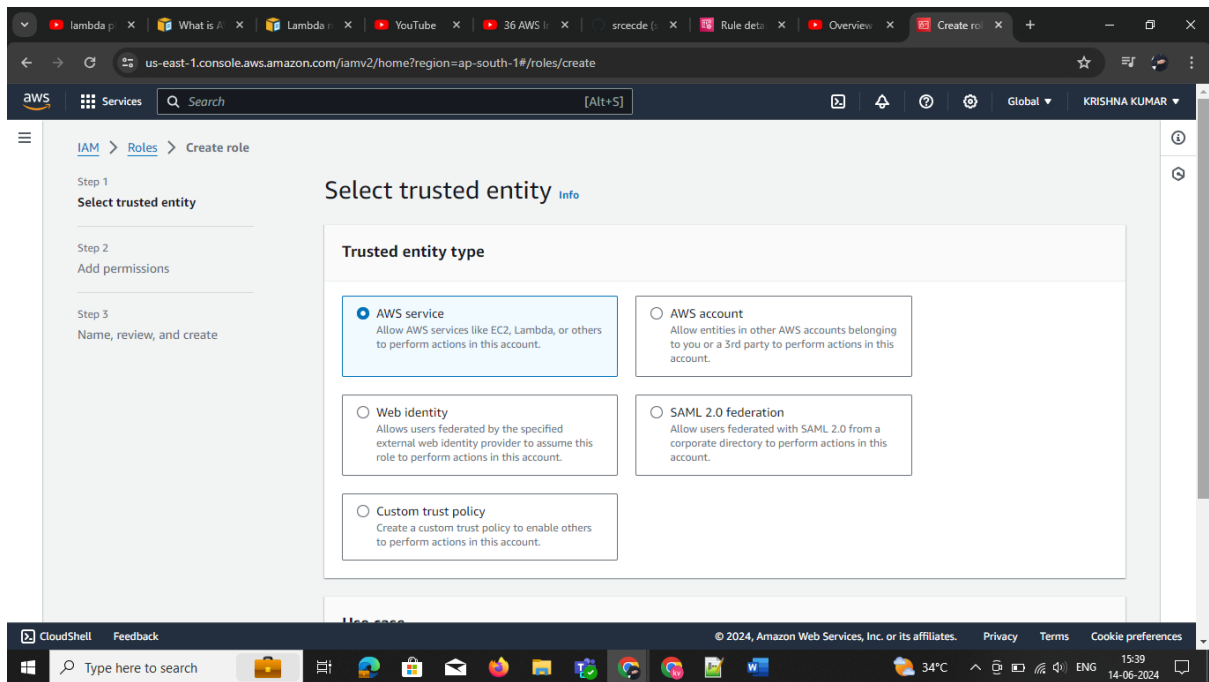
In AWS IAM, a role is a set of permissions that define what actions can be performed on AWS resources. Roles are assigned to entities like users, applications, or services, granting temporary access as needed. Roles help ensure security by allowing users or services to

access resources only, when necessary, without needing permanent credentials.

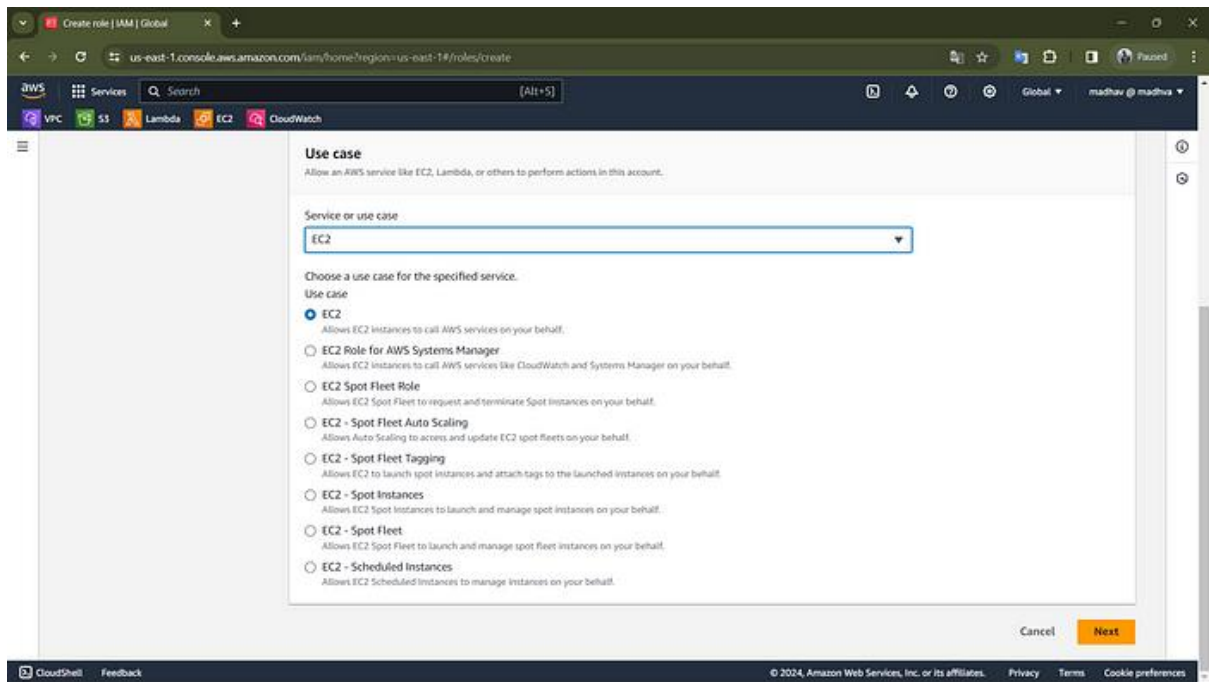
- In the navigation pane of the IAM console, choose **Roles** and then choose **Create role**.



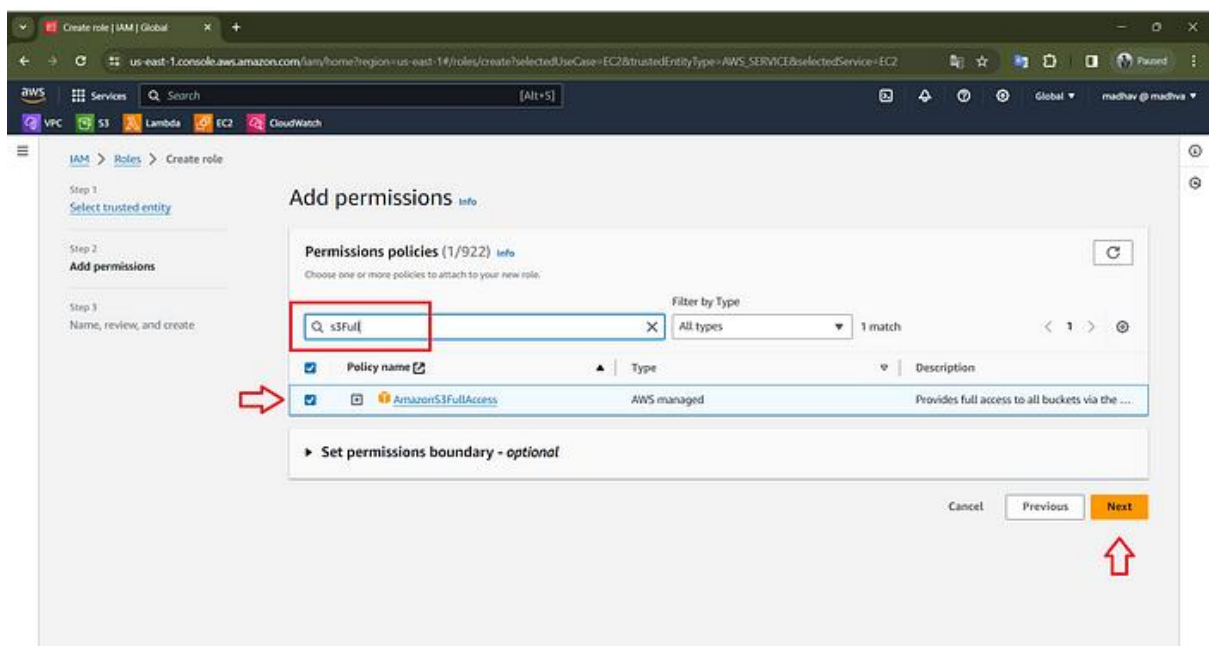
- Choose **AWS account** role type and select **AWS Services**.



- Under **Use case**, Select the service or Use case, Here I select **EC2** as the service. Select the based on the Requirement
- Then Click **Next**



- In **Add Permissions**, select the check box next to the permissions policy to apply. For this Article, we are going to select the **AmazonS3FullAccess** policy.
- Then Click, **Next**



- On the **Name Review and Create** page, for the **Role name**, type **EC2S3FullAccess**, **Role name**, enter a name that identifies this role For **Description**, You can describe the Role type.

The screenshot shows the AWS IAM console 'Create role' page. The browser address bar indicates the URL is `us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create?selectedUseCase=EC2&trustedEntityType=AWS_SERVICE&selectedService=EC2&policy=AmazonEC2FullAccess`. The page title is 'Create role | IAM | Global'. The left sidebar shows the navigation menu with 'IAM' selected. The main content area is titled 'Name, review, and create'. It includes a 'Role details' section with a 'Role name' field containing 'EC2S3FullAccess' and a 'Description' field containing 'Allows EC2 instances to call AWS services on your behalf.' Below this is a 'Step 1: Select trusted entities' section with an 'Edit' button. At the bottom is a 'Trust policy' section showing a JSON snippet.

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
EC2S3FullAccess

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and "+, -, @, _" characters.

Step 1: Select trusted entities Edit

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": "sts:AssumeRole",  
7       "Principal": {  
8         "Service": "ec2.amazonaws.com"  
9       }  
10    }  
11  ]  
12 }  
13  
14  
15  
16
```

Select **Create role**.

The screenshot shows the AWS IAM console 'Create role' page, Step 2: Add permissions. The browser address bar is the same as the previous screenshot. The page title is 'Create role | IAM | Global'. The left sidebar shows the navigation menu with 'IAM' selected. The main content area is titled 'Step 2: Add permissions'. It includes a 'Permissions policy summary' section with a table showing the policy 'AmazonS3FullAccess' attached as a 'Permissions policy'. Below this is a 'Step 3: Add tags' section with an 'Add new tag' button. At the bottom right, a red arrow points to the 'Create role' button.

Step 1: Select trusted entities Edit

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": "sts:AssumeRole",  
7       "Principal": {  
8         "Service": "ec2.amazonaws.com"  
9       }  
10    }  
11  ]  
12 }  
13  
14  
15  
16
```

Step 2: Add permissions Edit

Permissions policy summary

Policy name	Type	Attached as
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.

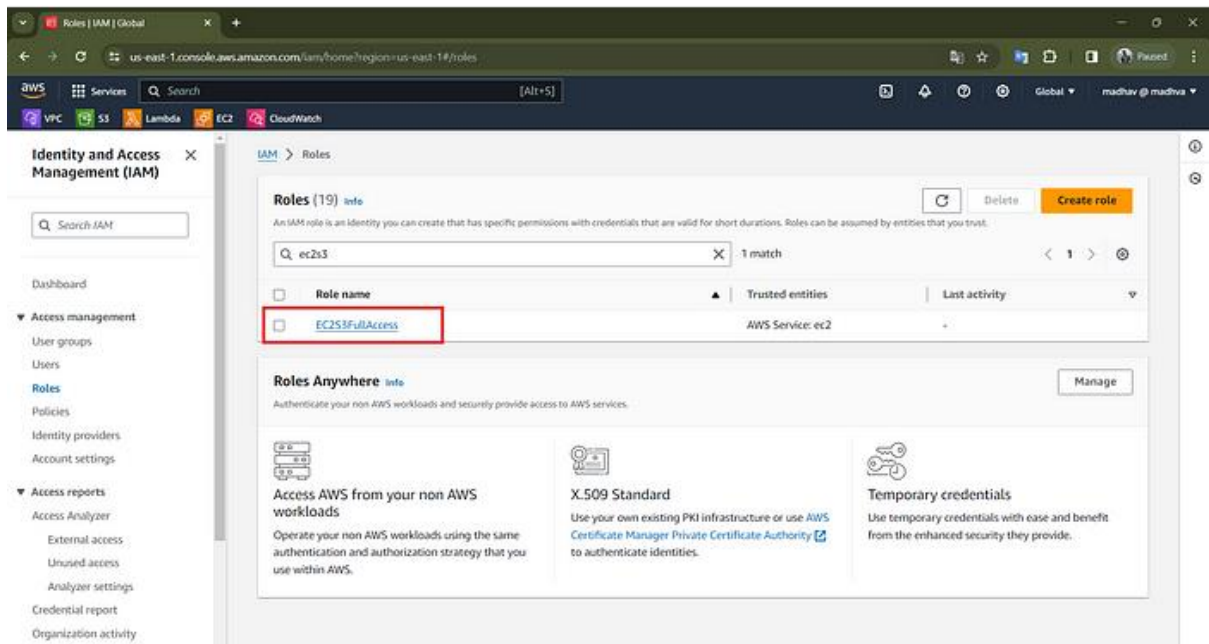
No tags associated with the resource.

Add new tag

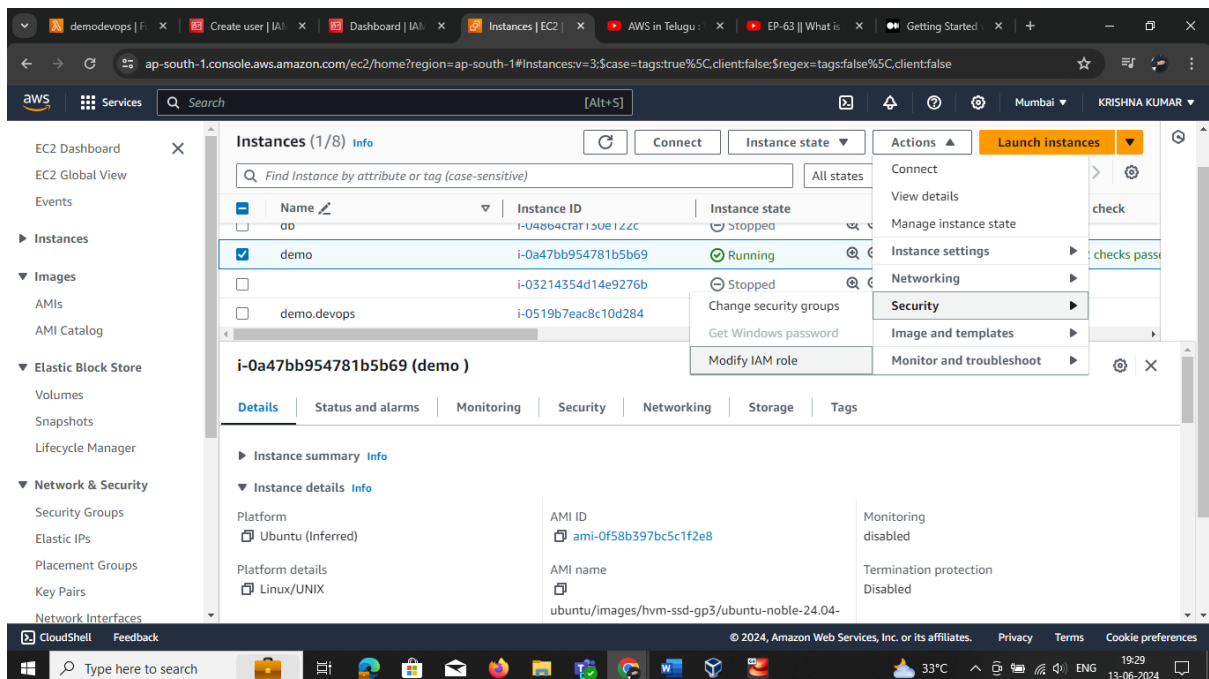
You can add up to 50 more tags.

Cancel Previous Create role

Here you can see the Role that we created, With the name that you gave, Here You need to search for the Role.



Attach the roles in ec2 instance



Select the IAM role and click update it

