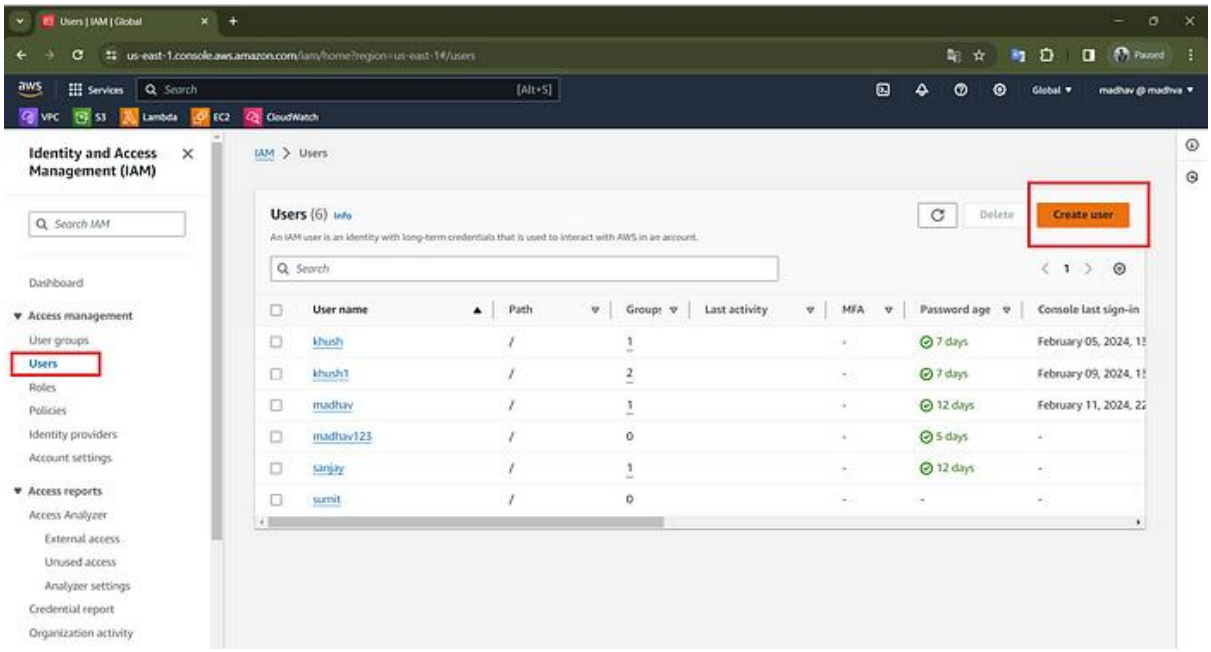
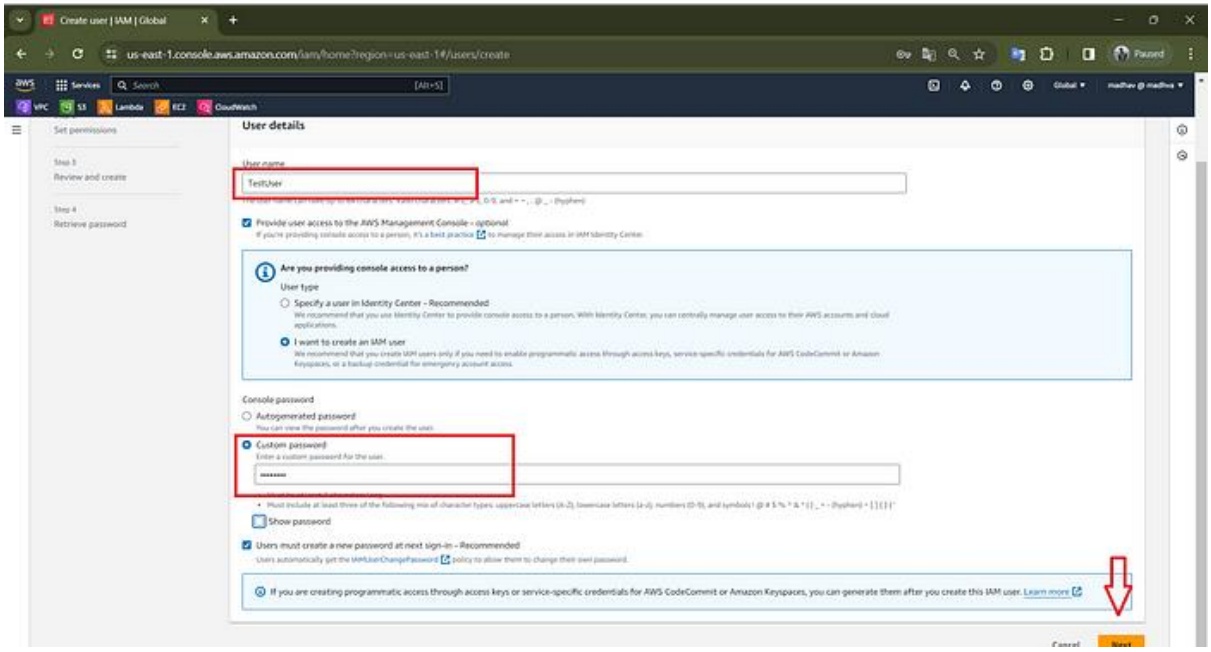
IAM Service

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

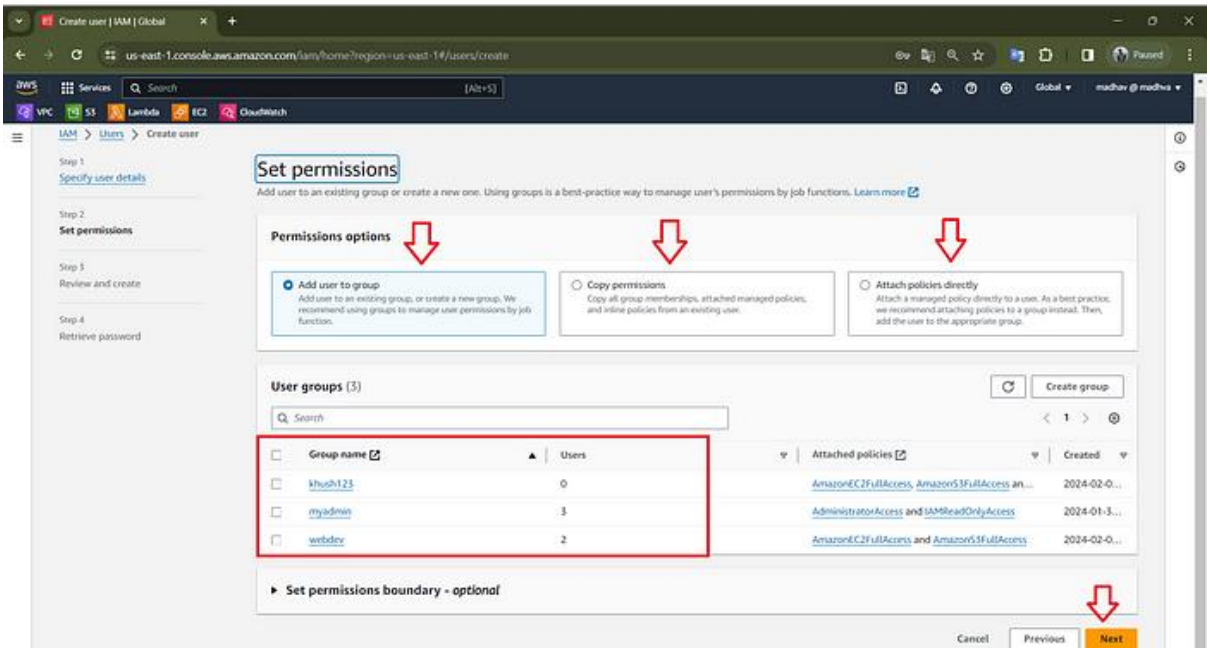


1. For the **User name**, enter **TestUser**. Names cannot contain spaces.
2. Select the check box next to **Provide user access to the AWS Management Console– *optional*** and then choose **I want to create an IAM user**.
3. Under **Console password**, select **Custom password**.
4. Clear the check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

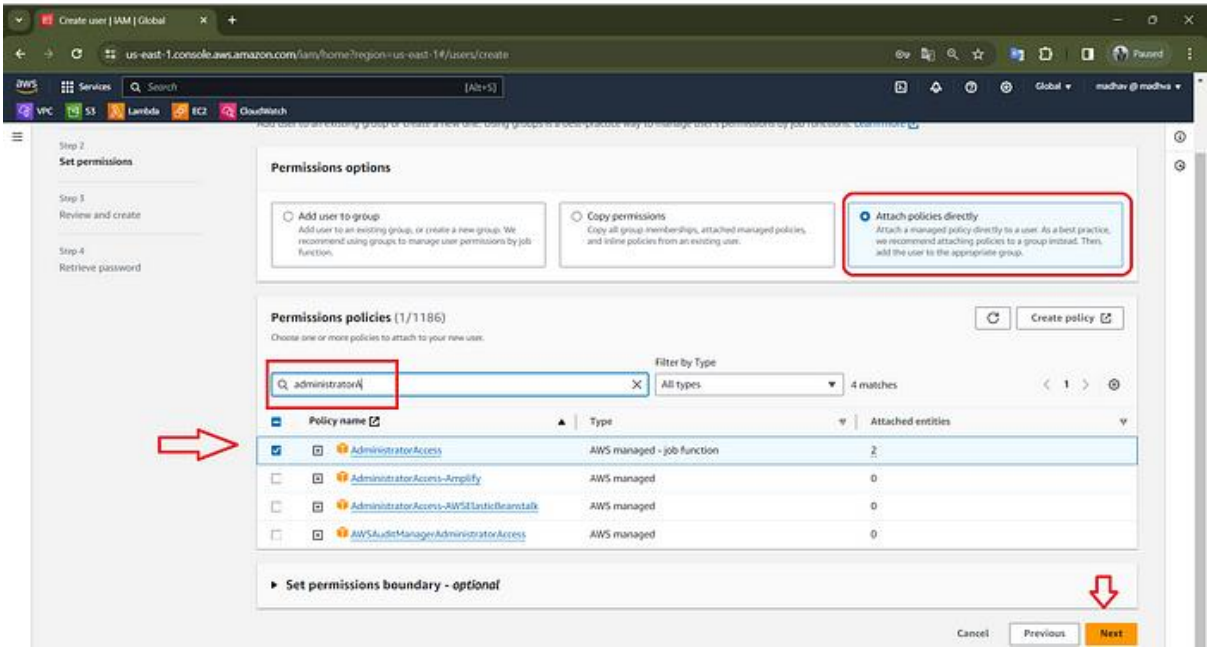
Because this IAM user is for emergency access, a trusted administrator retains the password and only provides it when needed.



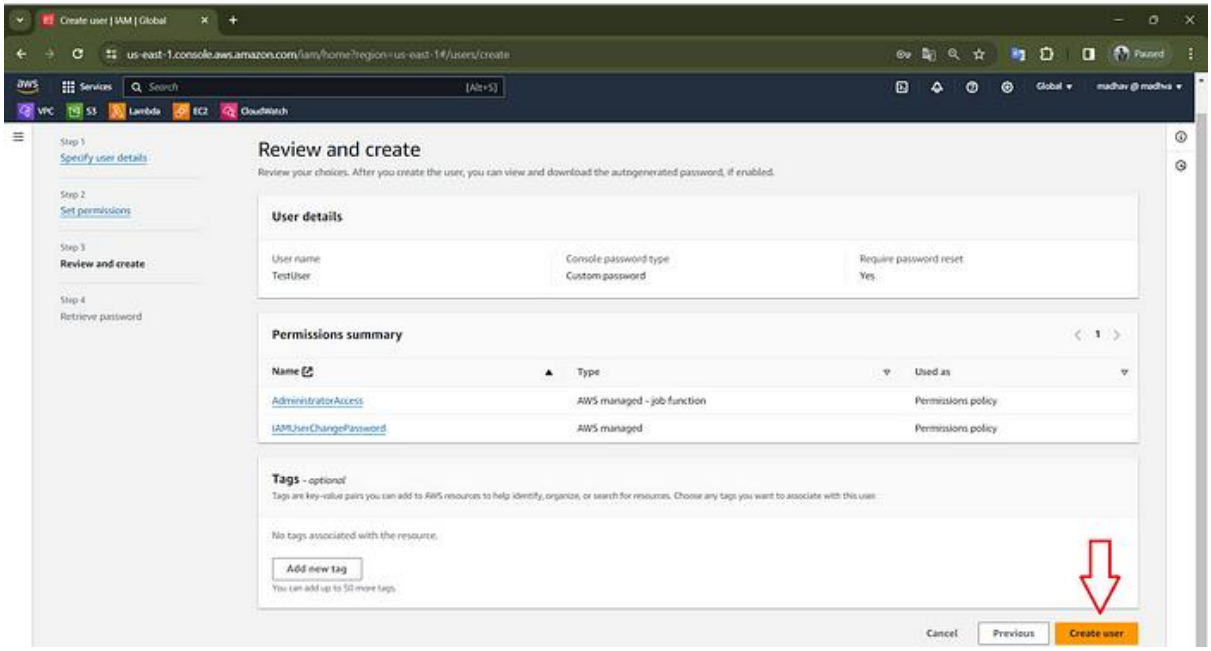
1. On the **Set permissions** page, under **Permissions options**, select **Add user to group**. so user Group you can add that particular user to the particular group and in one group have multiple users with the same permission



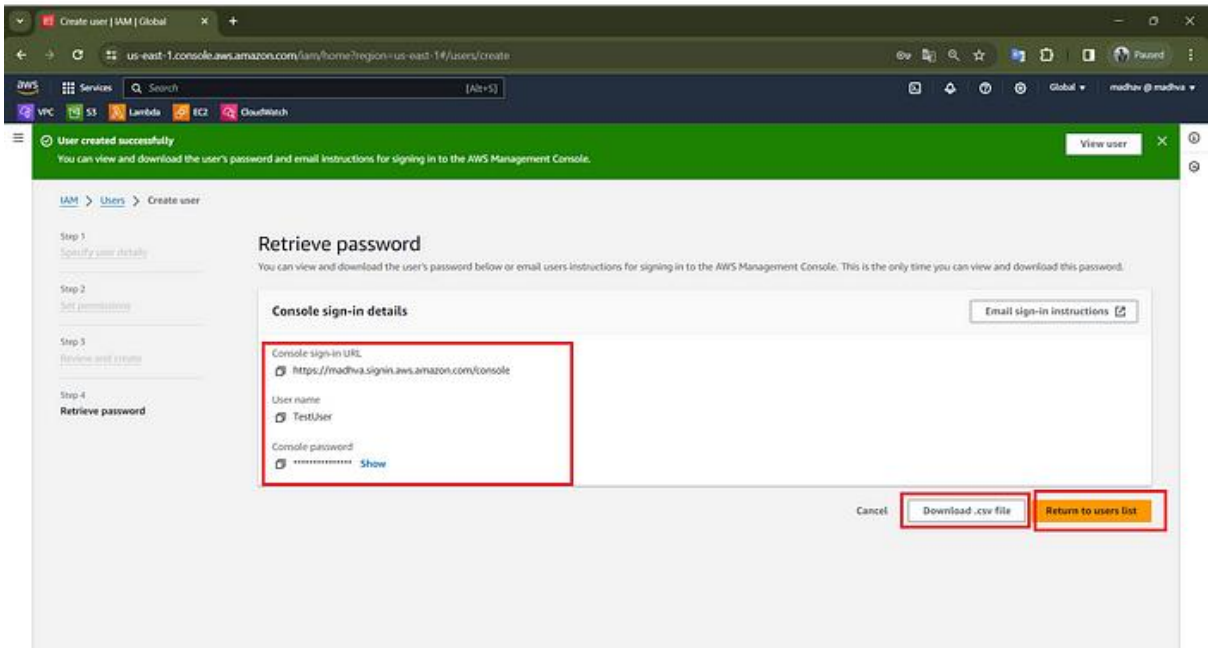
- But in my case, I am using **Attach Policies Directly.**
- under **Permissions Policies,** select the permission that you want to give to the user, Here I am using Administrator Access " best practice do go with admin access "
- Select **Next** to proceed to the **Review and Create** page.



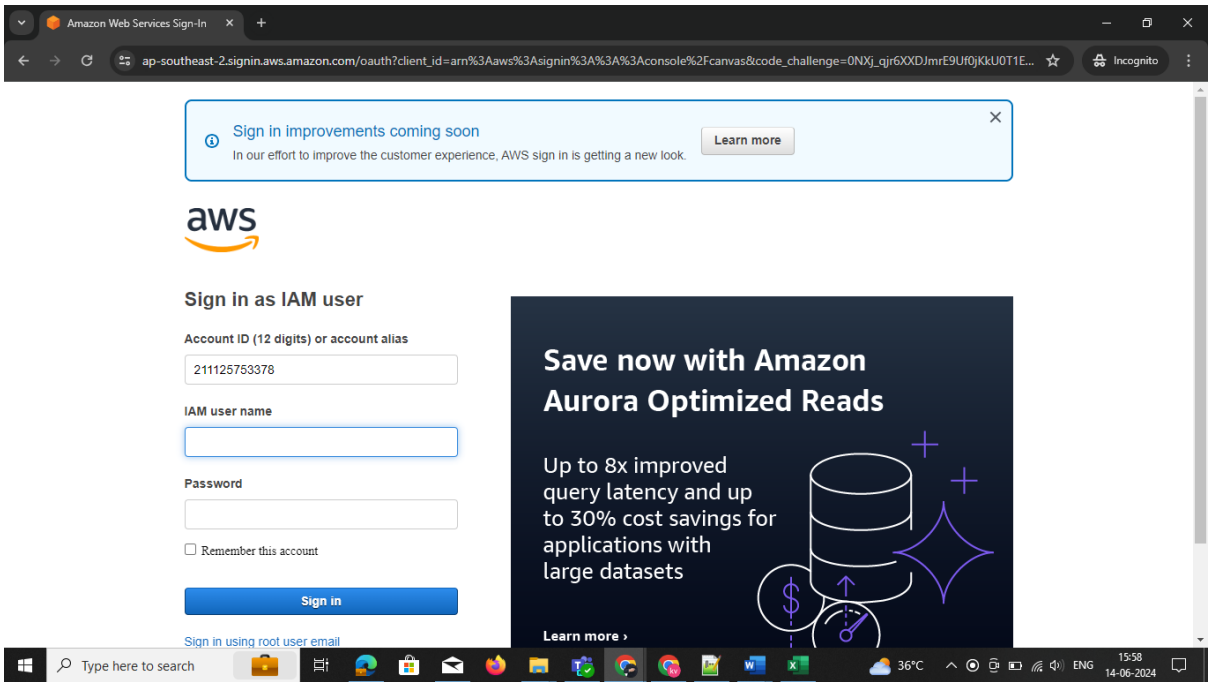
- On the **Review and Create** page, review the list of user group memberships to be added to the new user. When you are ready to proceed, select **Create User**.



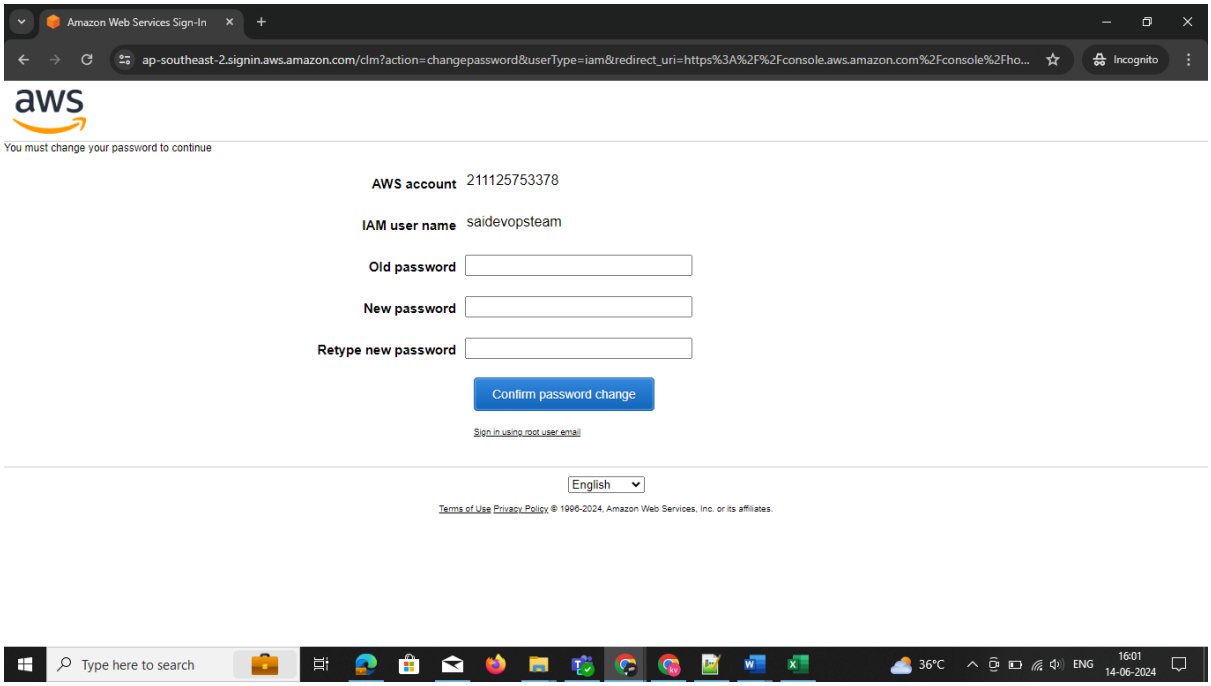
- On the **Retrieve password** page, select **Download .csv file** to save a .csv file with the user credential information (Connection URL, user name, and password).
- Save this file to use if you need to sign-in to IAM and do not have access to your federated identity provider



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

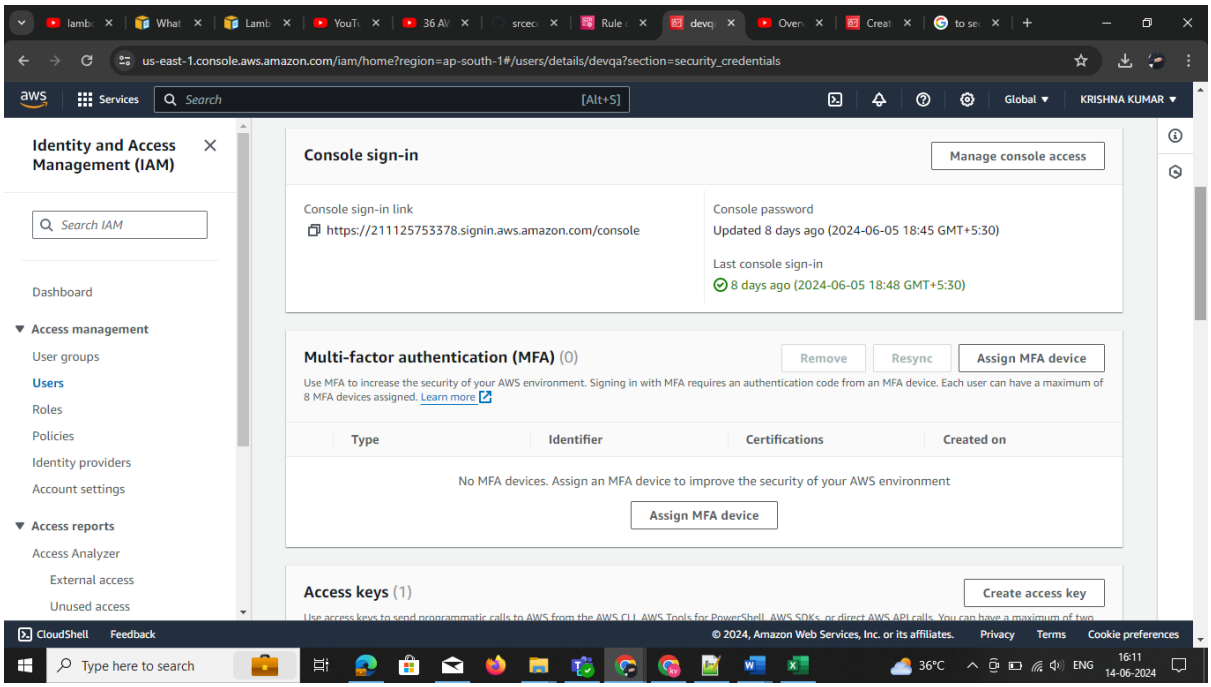


Once giving the u-named and password now it shows this generate custom password

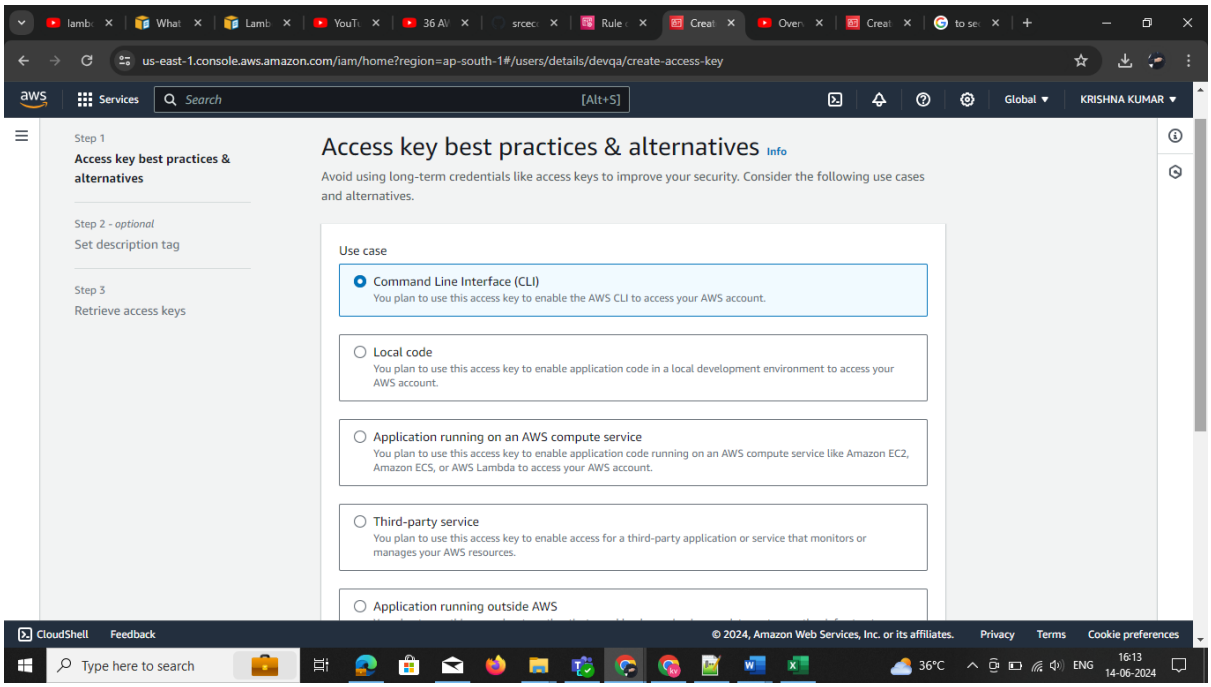


Once you giving this passwords and now we need to login in to aws now we need to give the permission to AWS access key security to user IAM

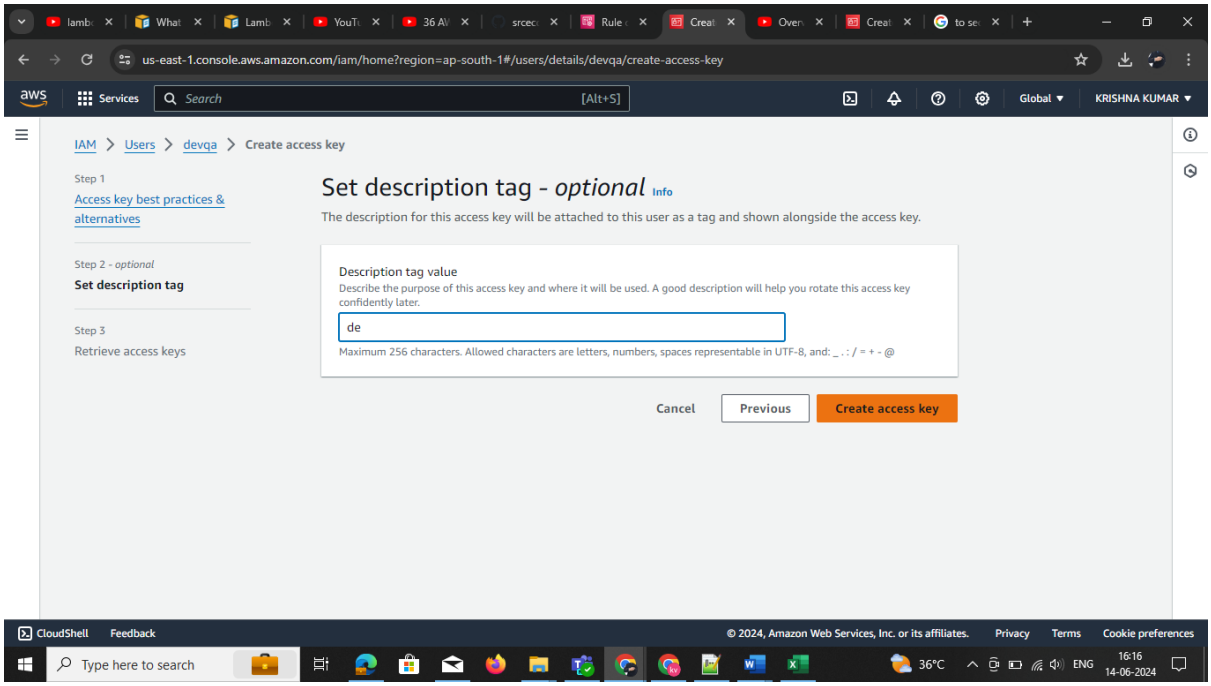
Go to IAM > select user > security credentials click > create access key

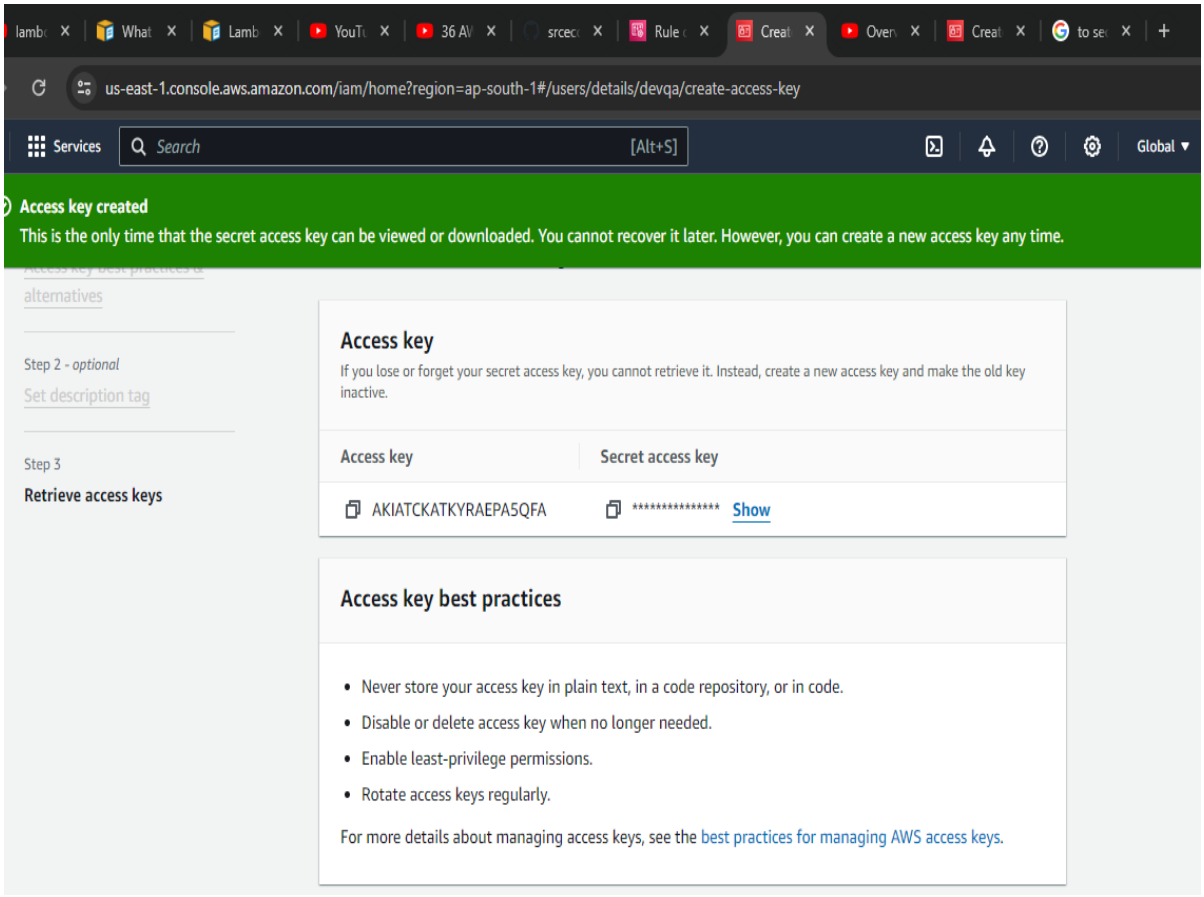


Select the > create access key



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



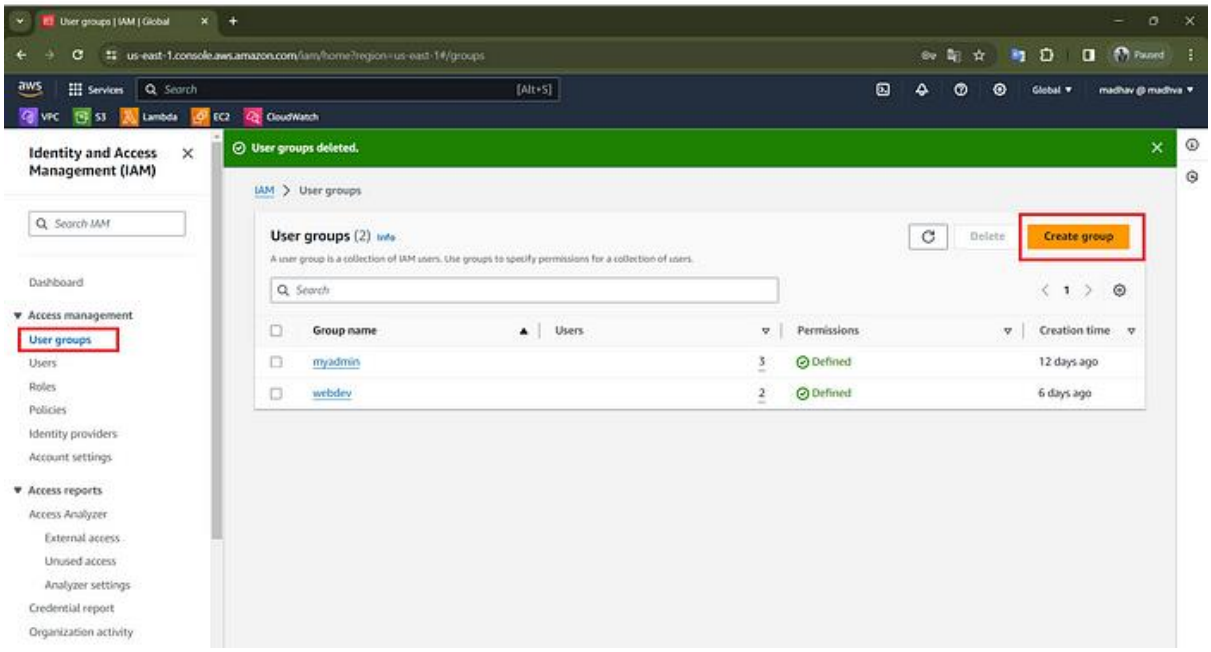


Note: don't share this key

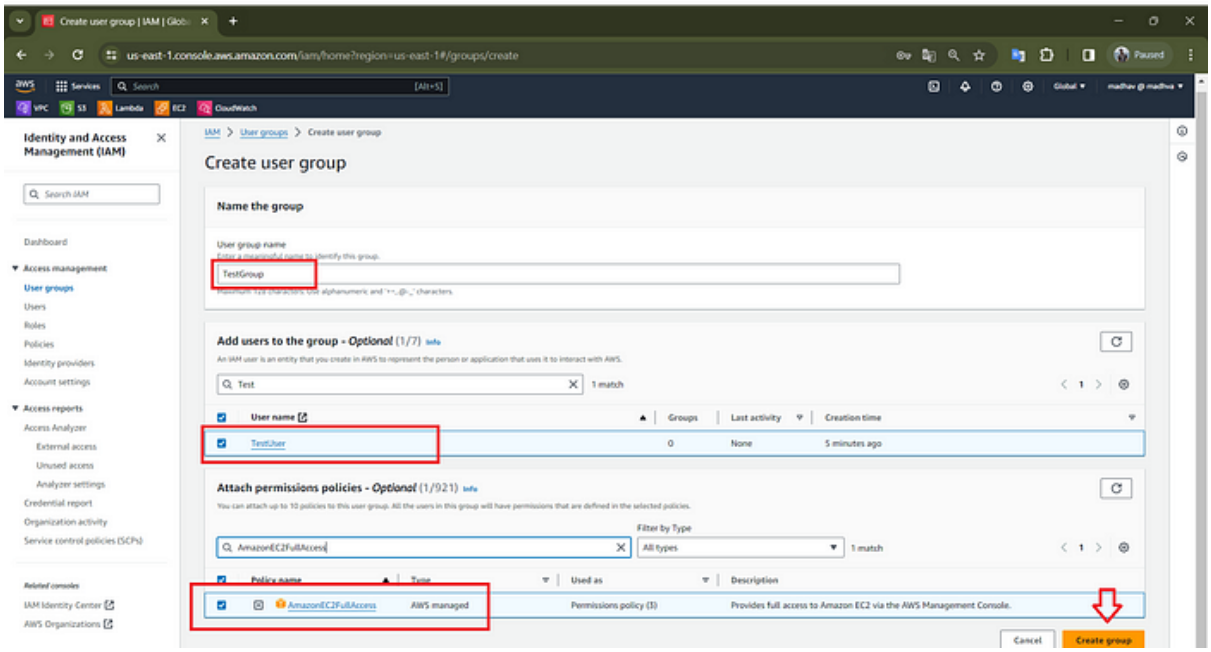
Create your first IAM user Group:

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.

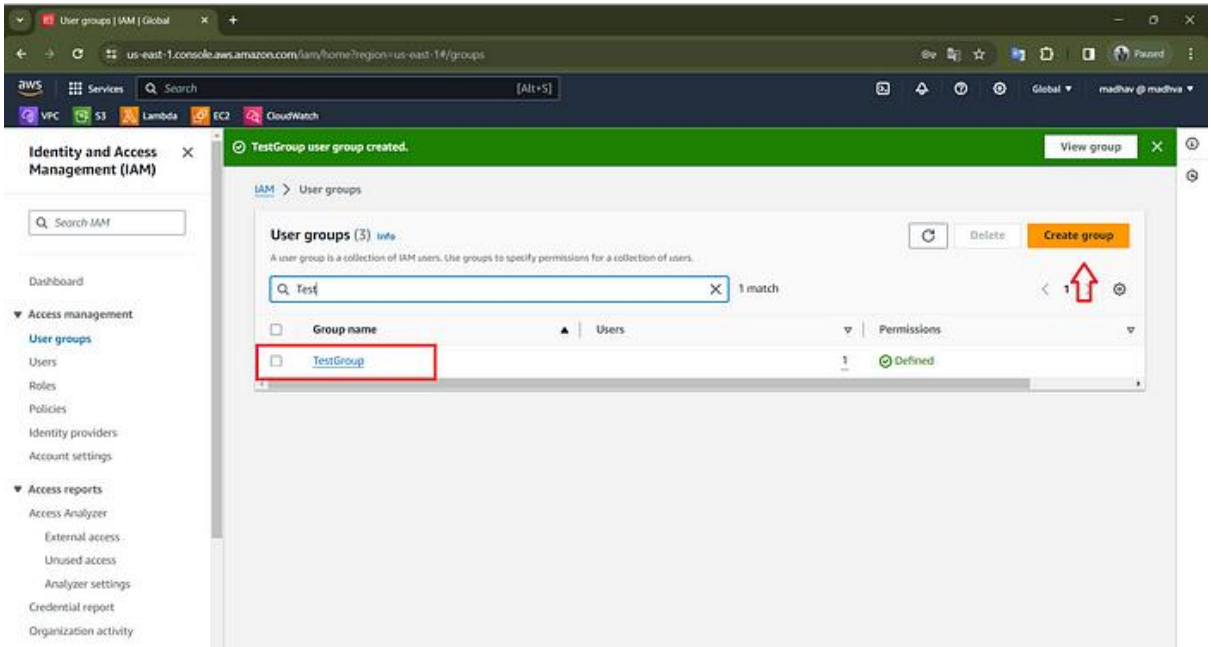
- In the navigation pane, choose **User Groups** and then choose **Create group**.



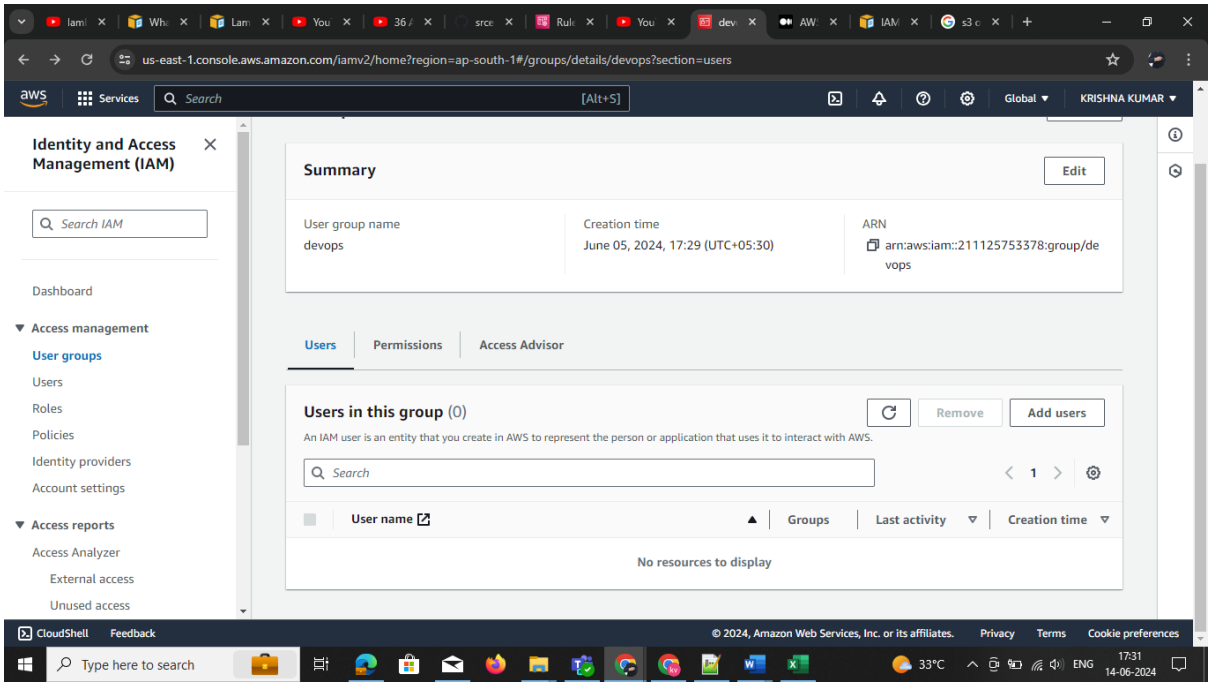
- For the **User group name**, type the name of the group.
- In the list of users, select the check box for each user that you want to add to the group, Like **Test User**.
- In the list of policies, select the check box for each policy that you want to apply to all members of the group like **AdminstratorAccess**.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



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



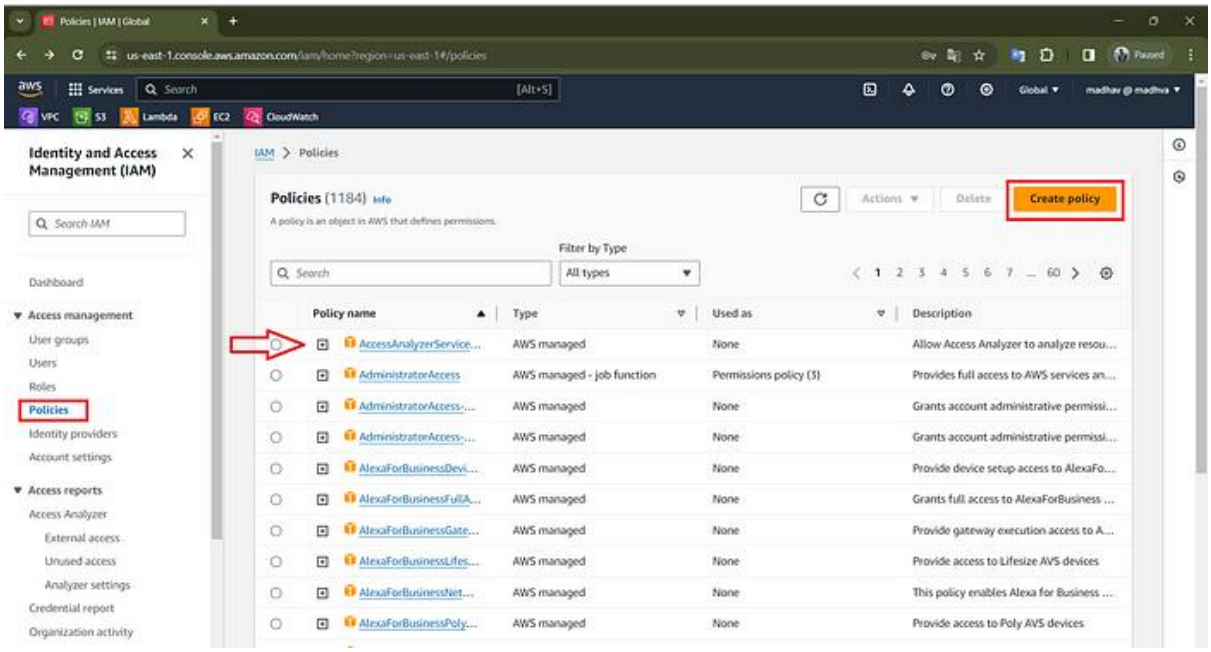
To add the use in the group > select the group add user



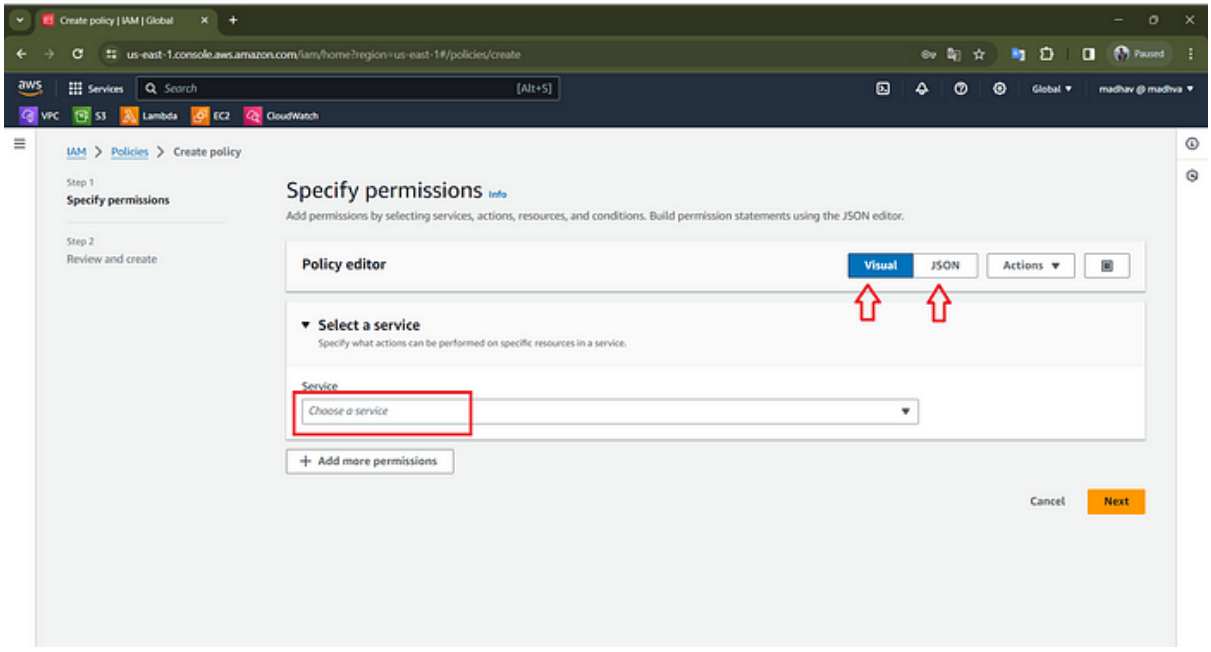
create your first IAM policy

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**.

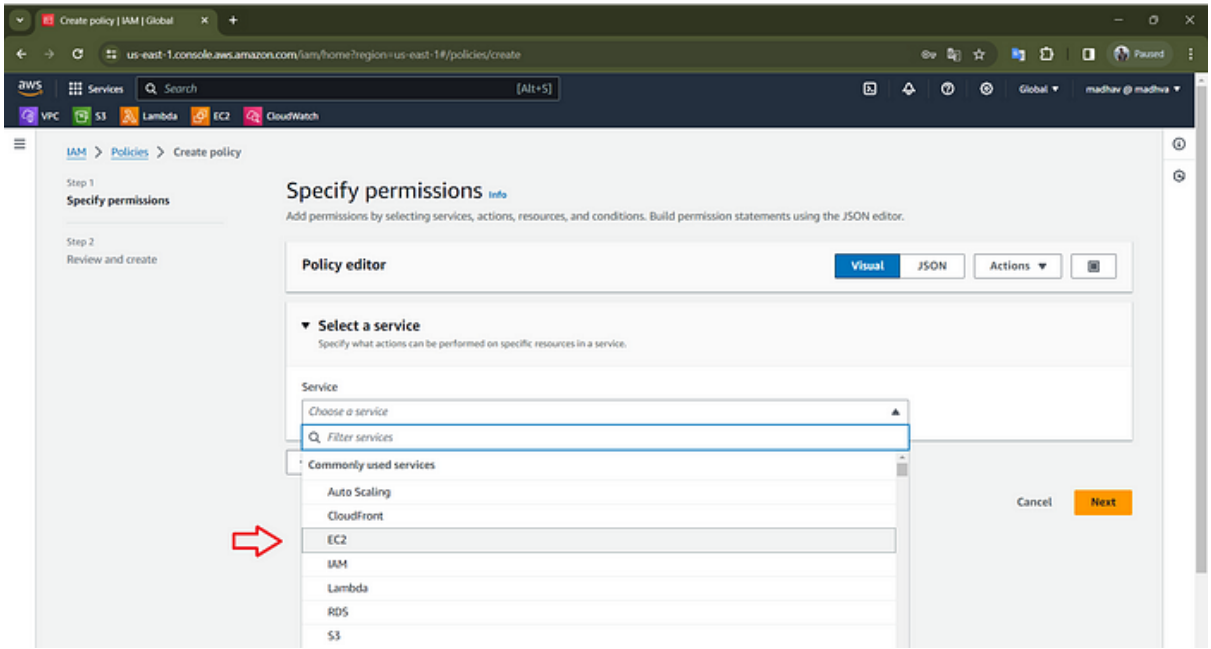


- On the **Create policy** page,
- There are two options **Visual** and **Json**
- In Visual, we can create policies manually, by using GUI

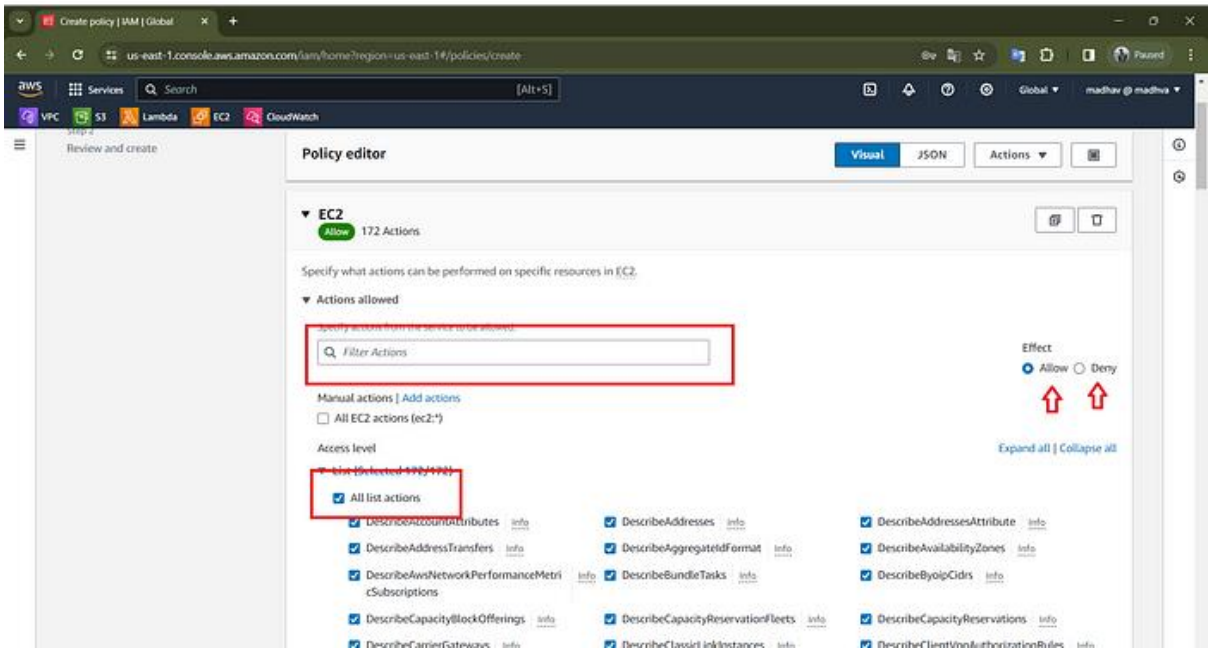


- In Json we use Json Language to create Policies, In my case I go to import policy Json
- Choose **Next**.

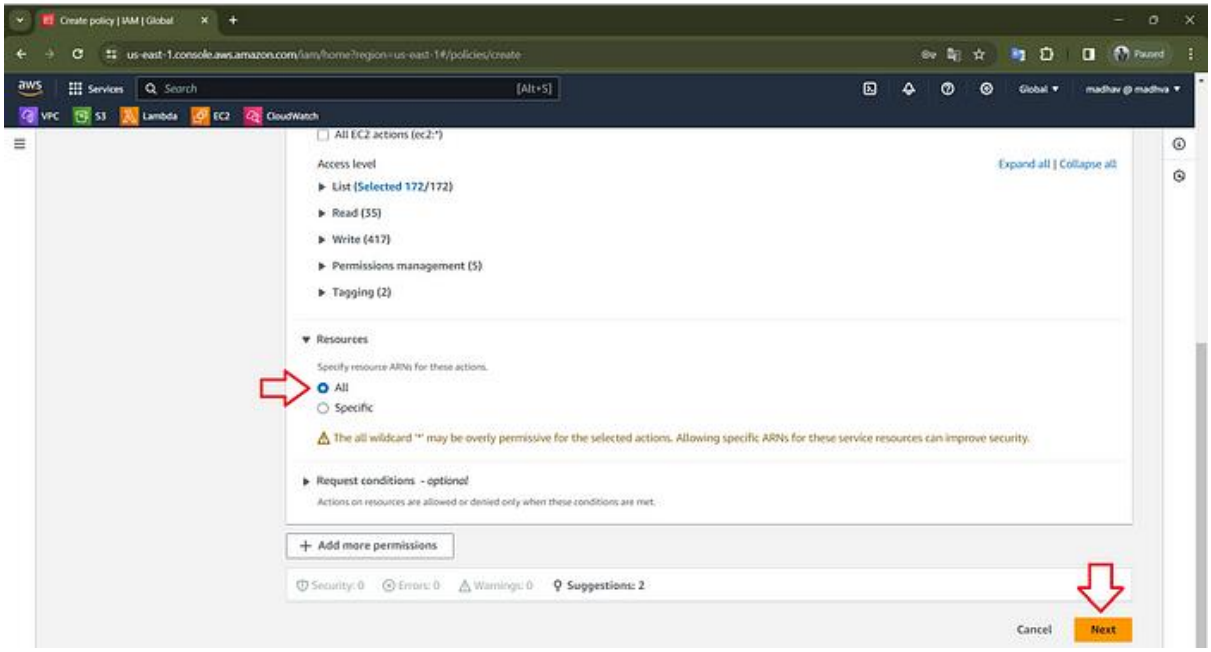
- In this **visual**, Under **Select a service**, We want to choose the service, for creating policies, Here I am using **EC2**
- Then Click, **Next**



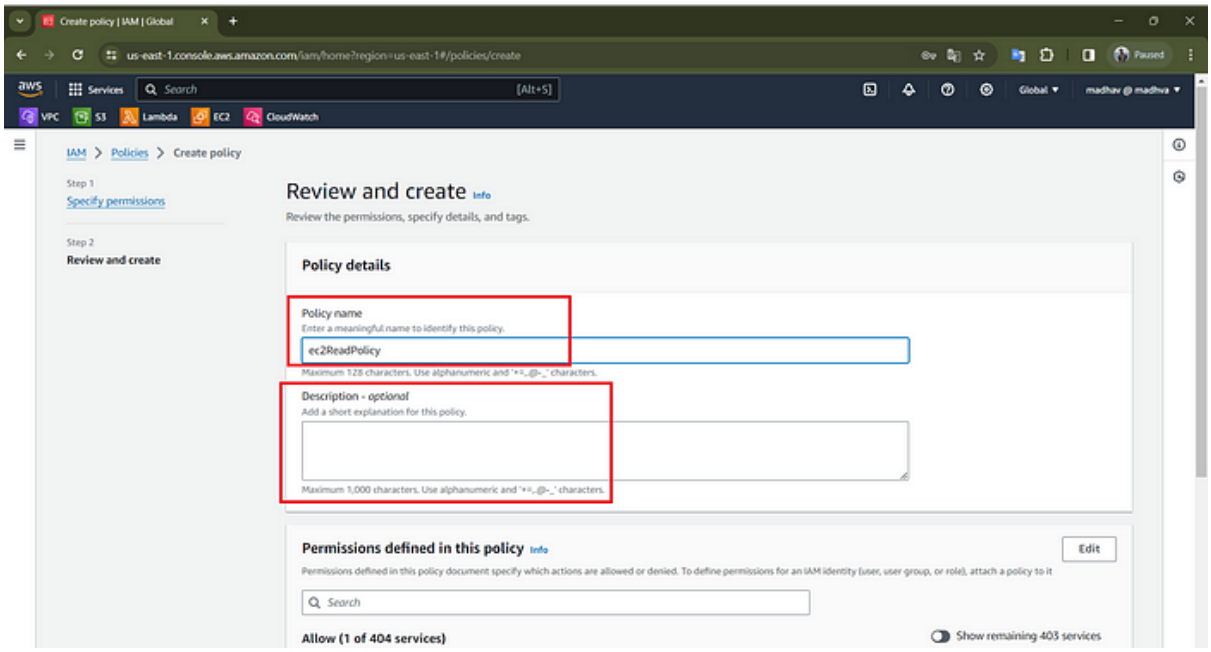
Here you can choose **effect**, **Allow** and **Deny** for service, now you can select the action that you want to allow or deny



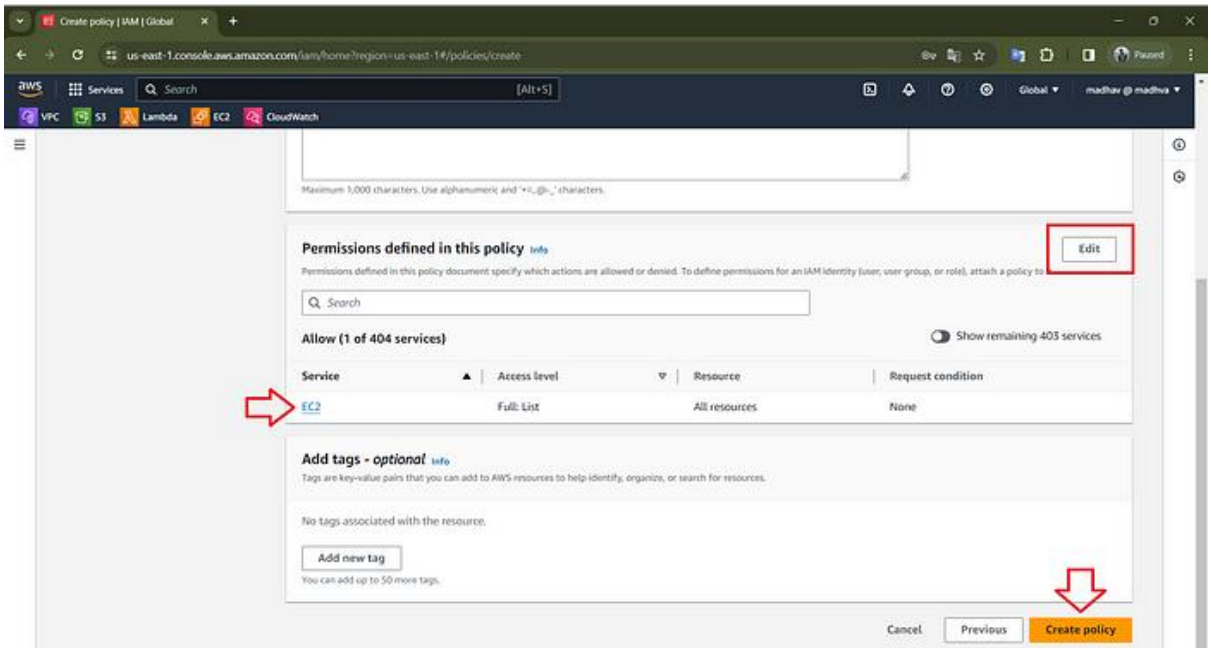
- In the **resource**, Select **All,**
- Then click **Next,**



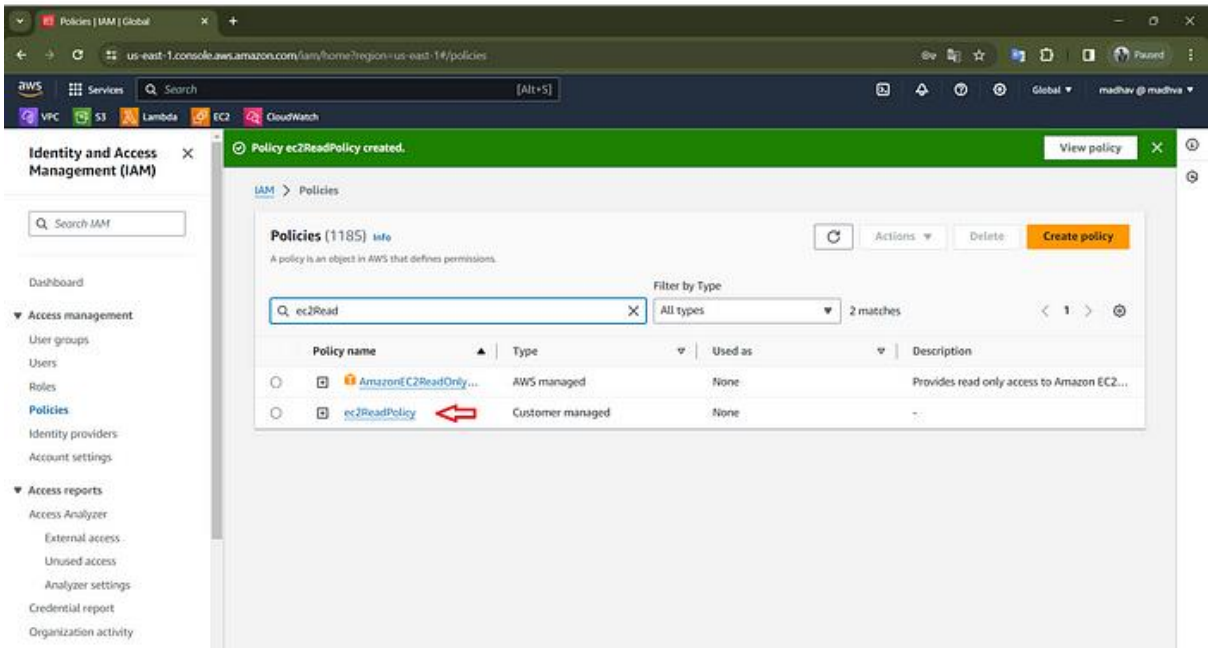
- On the **Review and Create** page, for the **Policy name**, type **ec2ReadPloicy**. For **Description**, You can describe the Policy type.



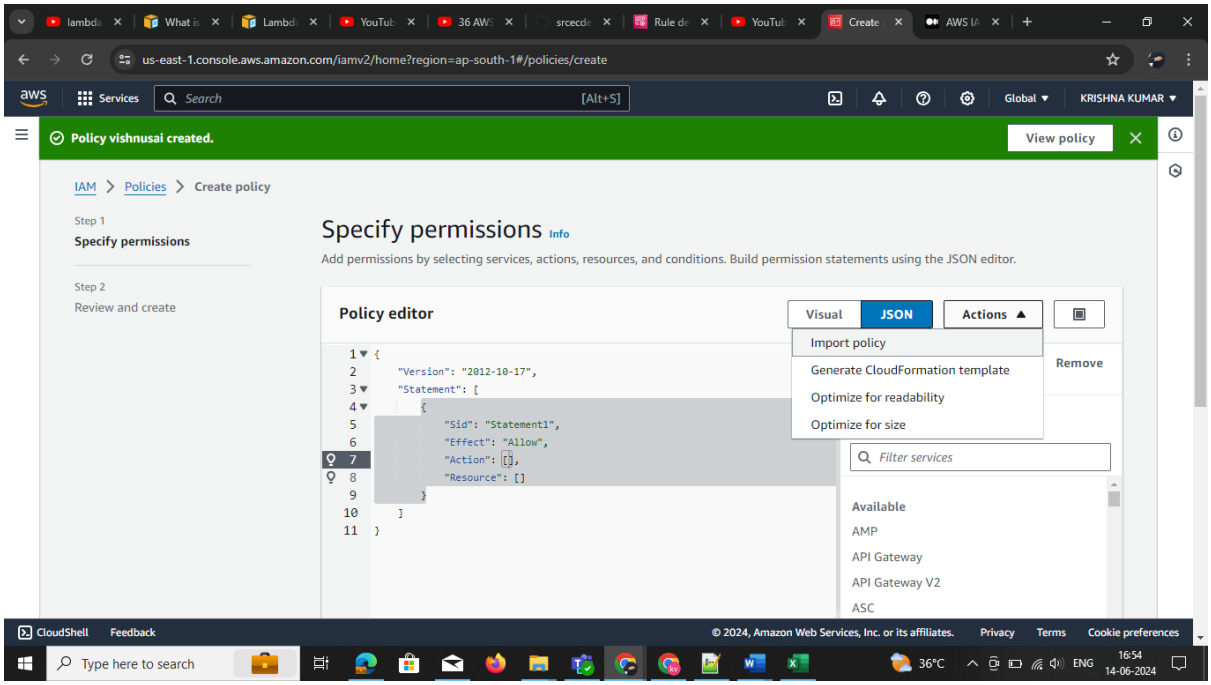
- Then choose **Create policy** to save the policy.



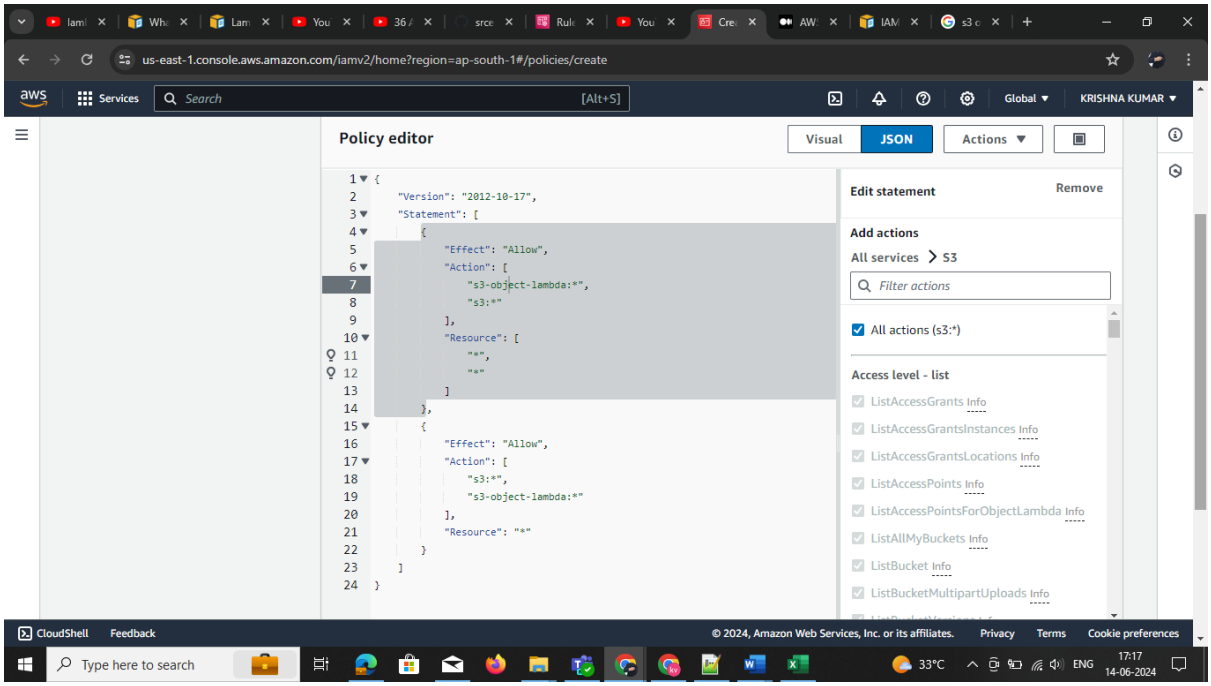
Here you can see the Policy that we created, With the name that you gave, Here You need to search for the Policy Because in AWS there Are many policies exist.

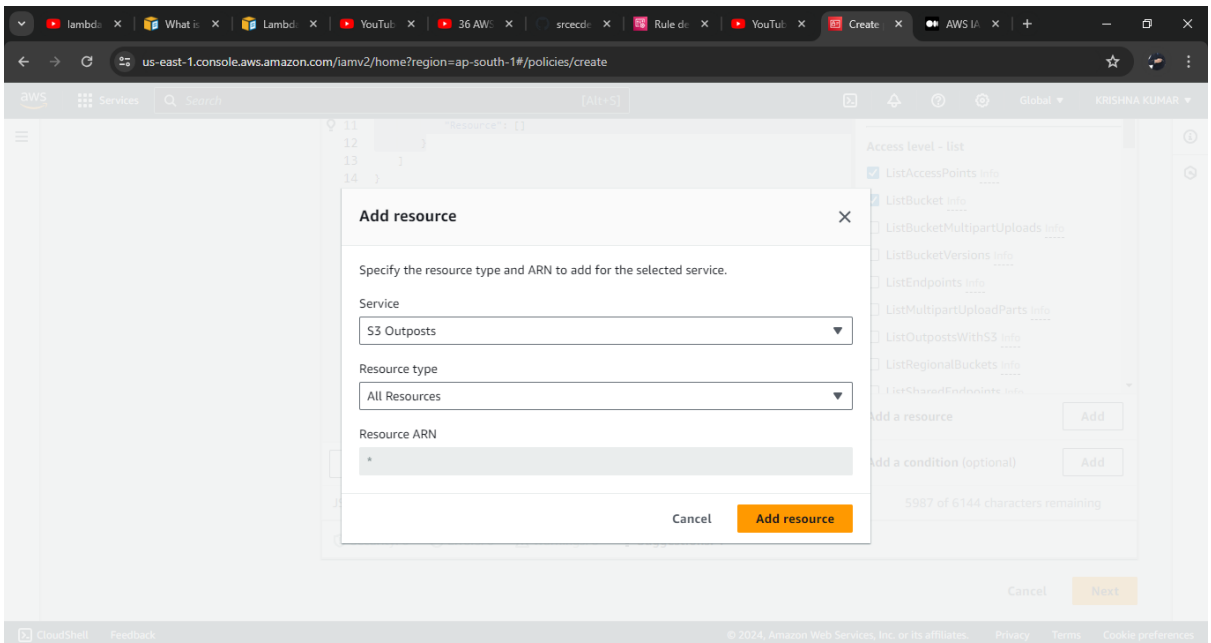


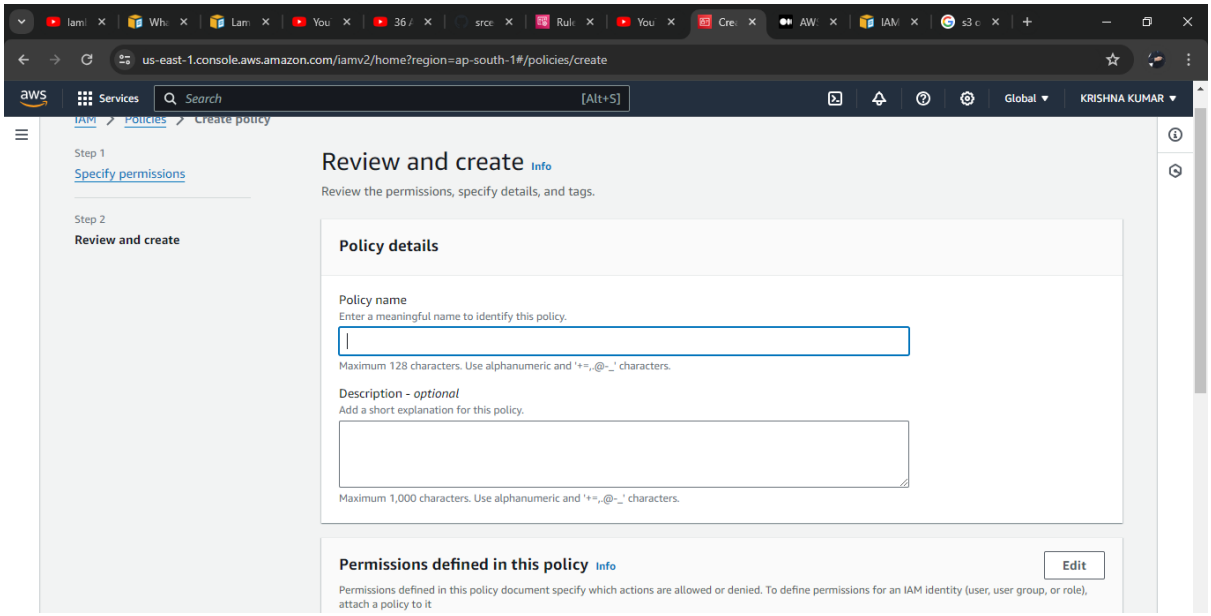
In JSON FORMAT



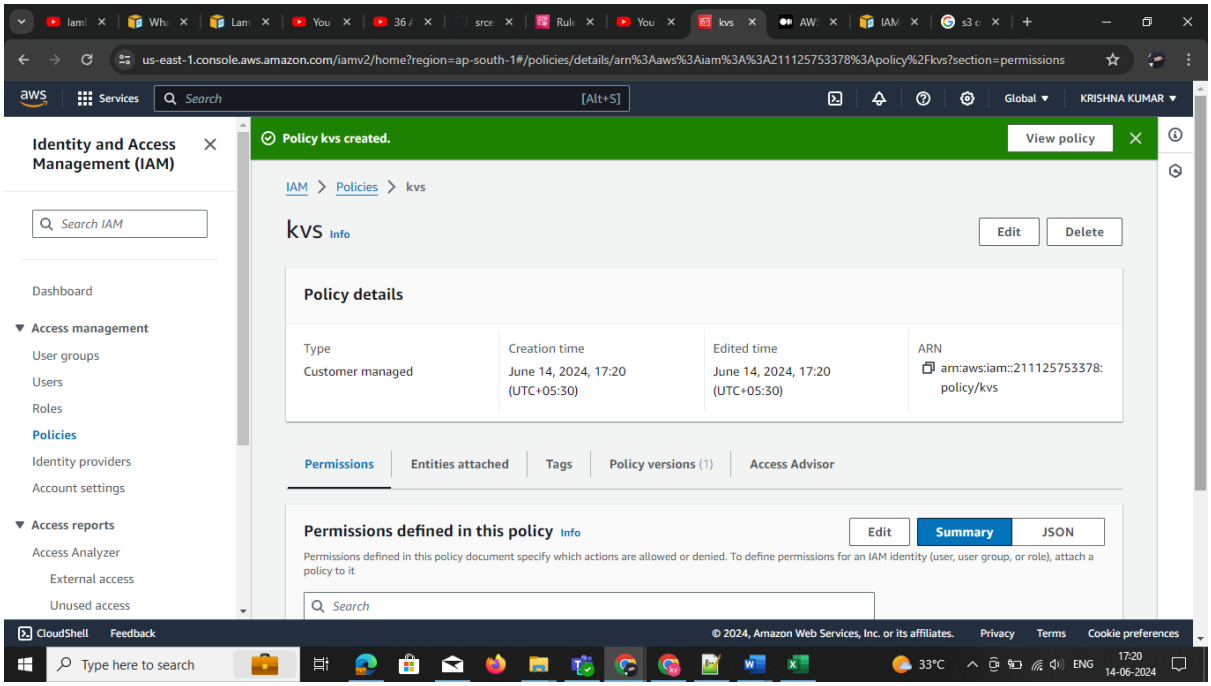
copy your Owen script are import policy type SELECT THE ACTIONS


us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/policies/create
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"s3-object-lambda:*",
"s3:*"
],
"Resource": [
"*",
"*"
]
},
{
"Effect": "Allow",
"Action": [
"s3:*",
"s3-object-lambda:*"
],
"Resource": "*"
}
]
}
Edit statement
Remove
Add actions
All services > S3
Filter actions
All actions (s3:*)
Access level - list
ListAccessGrants Info
ListAccessGrantsInstances Info
ListAccessGrantsLocations Info
ListAccessPoints Info
ListAccessPointsForObjectLambda Info
ListAllMyBuckets Info
ListBucket Info
ListBucketMultipartUploads Info
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
33°C
ENG
17:17
14-06-2024


us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/policies/create
Add resource
Specify the resource type and ARN to add for the selected service.
Service
S3 Outposts
Resource type
All Resources
Resource ARN
*
Cancel
Add resource



Get to polices and search with name

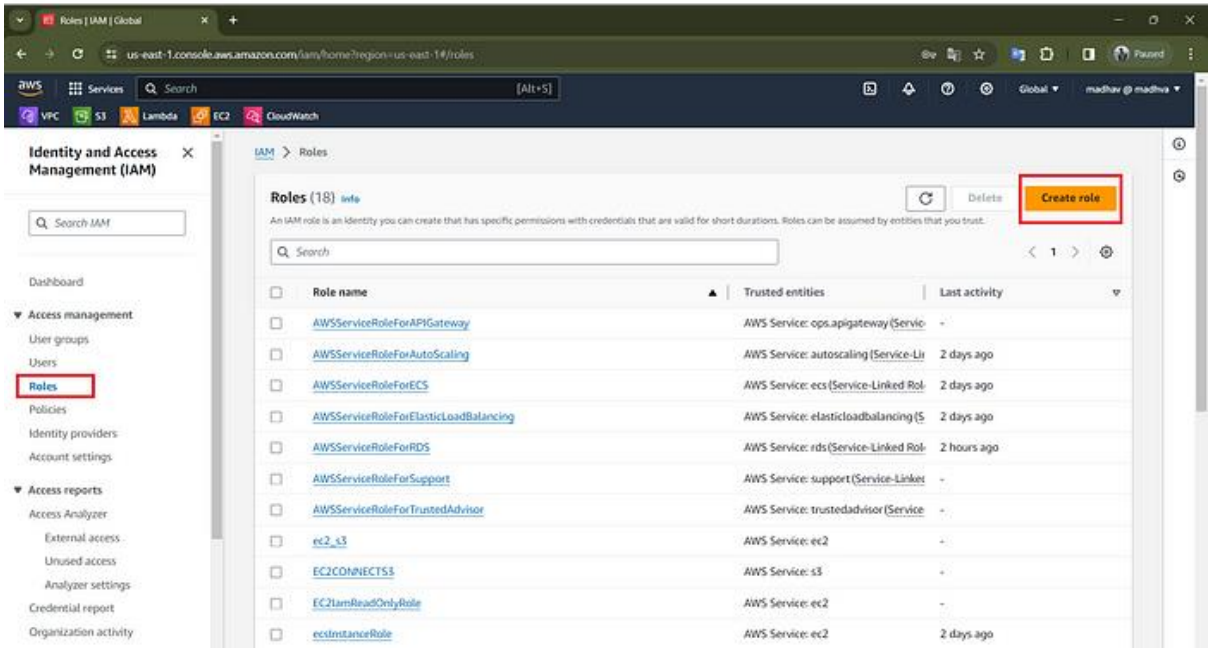


Create your first role:

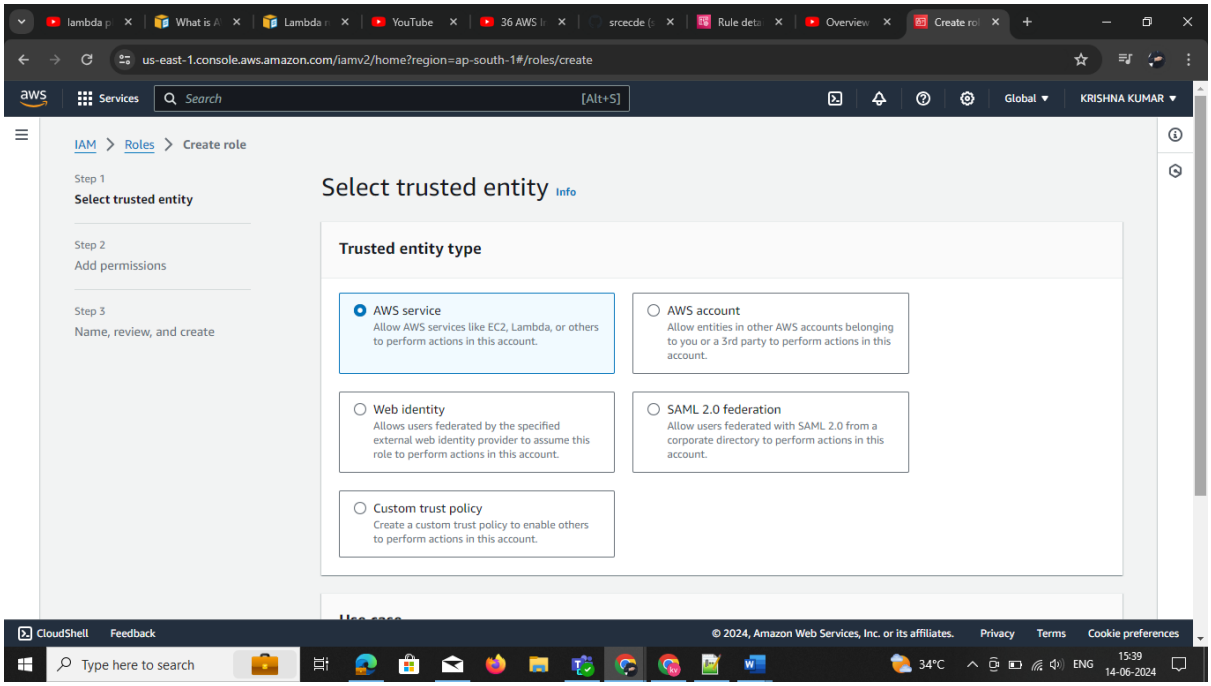
In AWS IAM, a role is a set of permissions that define what actions can be performed on AWS resources. Roles are assigned to entities like users, applications, or services, granting temporary access as needed. Roles help ensure security by allowing users or services to

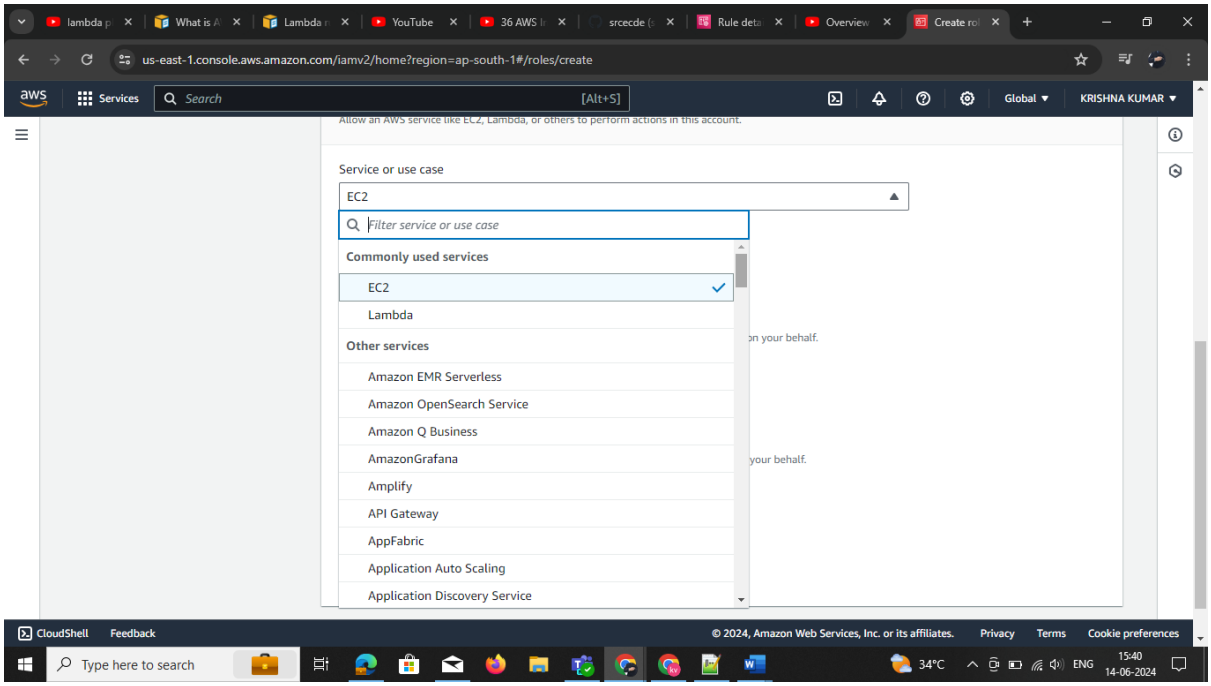
access resources only, when necessary, without needing permanent credentials.

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

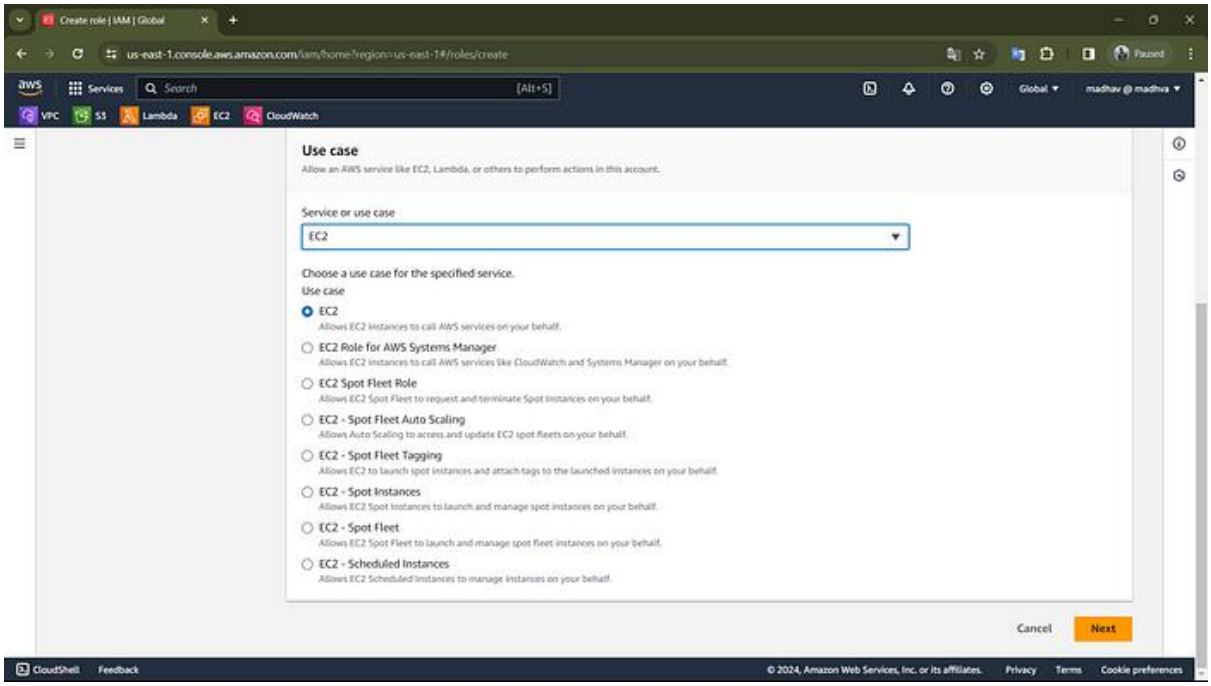


- Choose **AWS account** role type and select **AWS Services**.

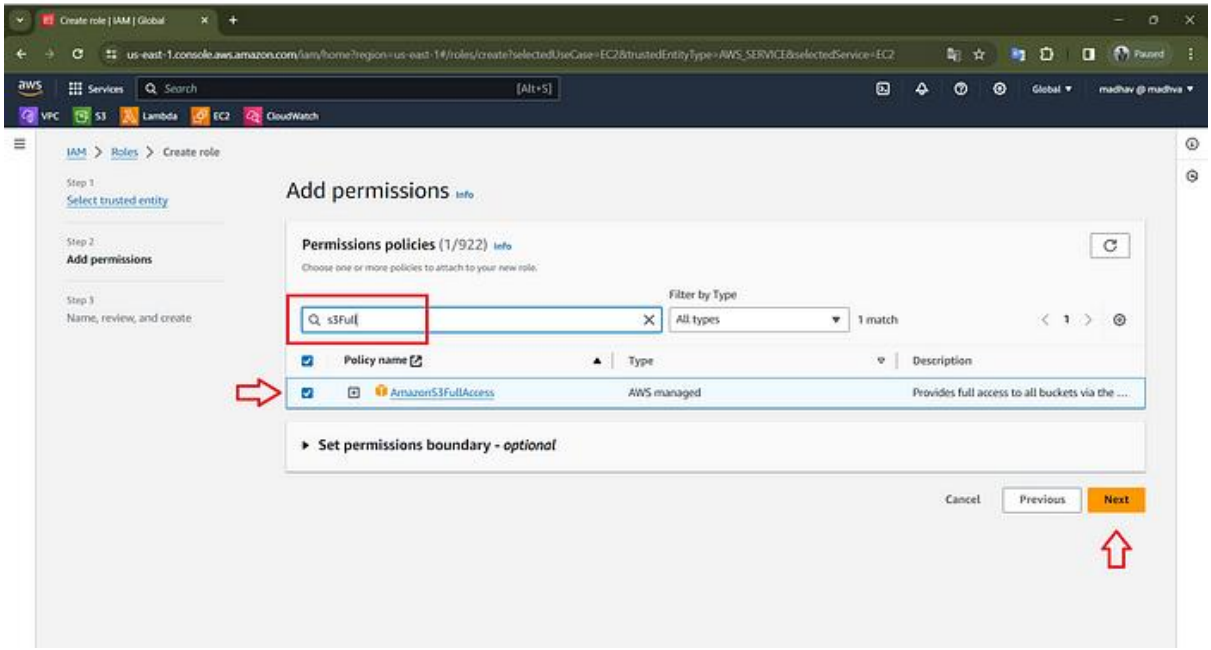




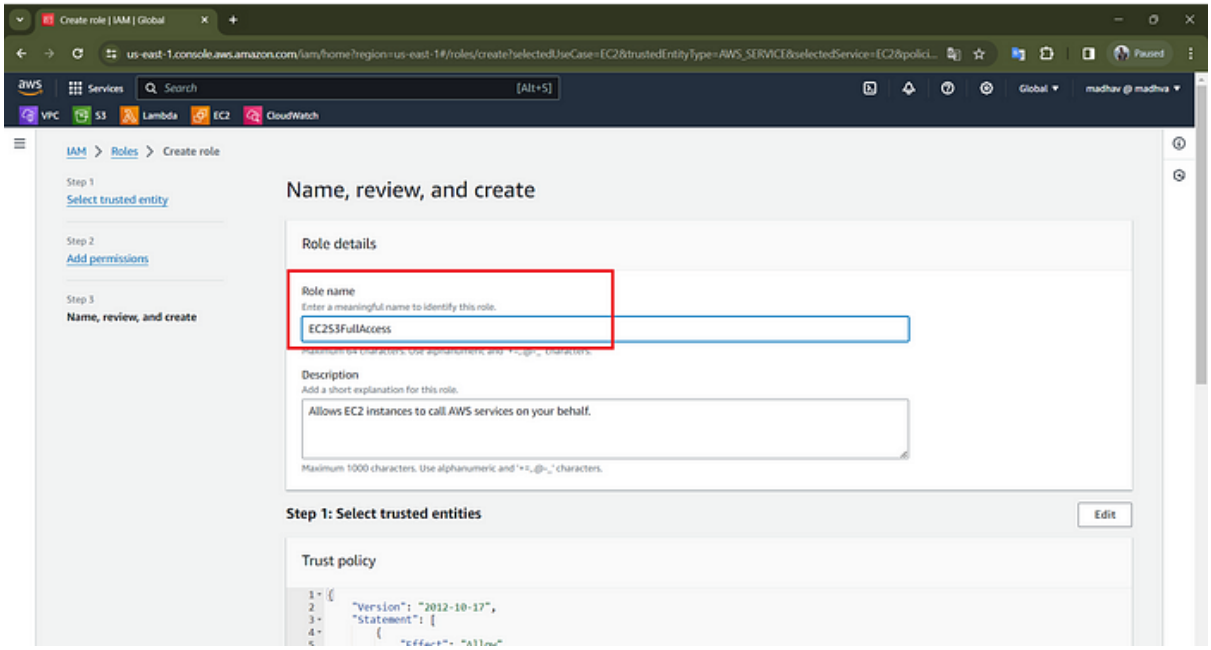
- Under **Use case**, Select the service or Use case, Here I select **EC2** as the service. Select the based on the Requirement
- Then Click **Next**



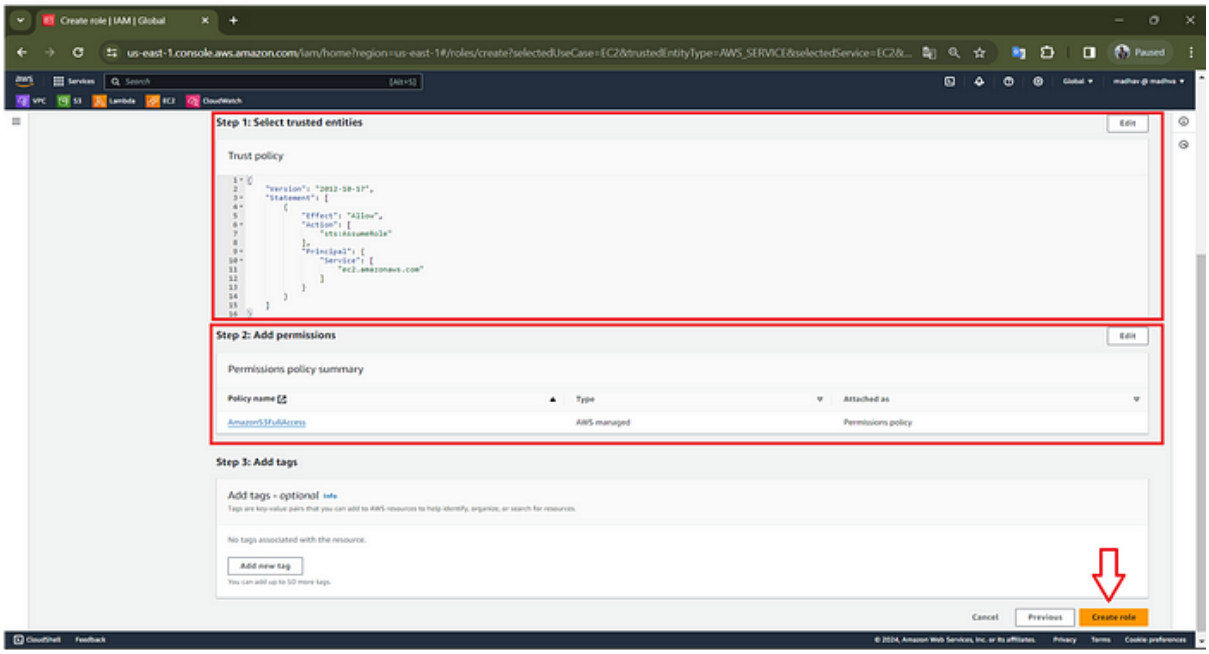
- In **Add Permissions**, select the check box next to the permissions policy to apply. For this Article, we are going to select the **AmazonS3FullAccess** policy.
- Then Click, **Next**



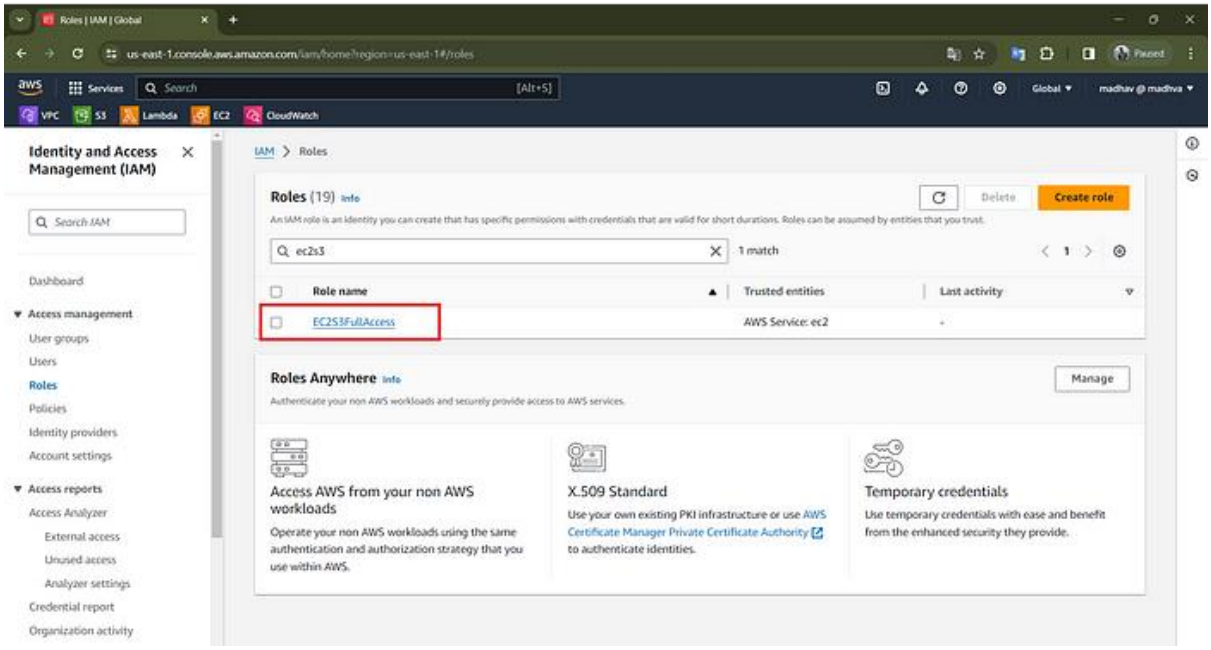
- On the **Name Review and Create** page, for the **Role name**, type **EC2S3FullAccess, Role name**, enter a name that identifies this role For **Description**, You can describe the Role type.



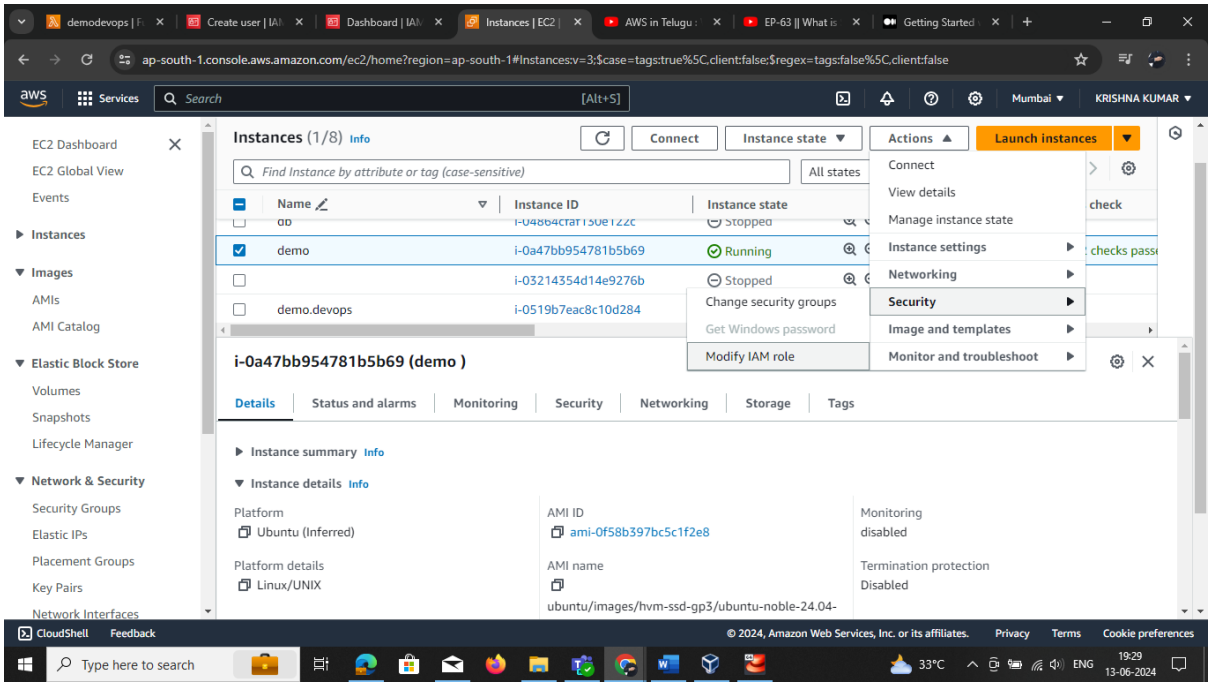
Select **Create role**.



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