Practical 3

IAM user groups.

— An IAM user group is a collection of IAM user. User groups let you specify permissions for multiple users which can make it easier to make & manage the permissions for those users. For ex, you have a user group called 'Admins' & give that user group typical administrator permissions. Any users in that user group automatically has 'Admins' group permission. If a new user joins your organization & needs administrator privileges you can assign the appropriate permissions by addition of the user to the 'admins' user groups. If a person changes jobs in your organization, instead of editing that user's permissions you can remove them.

— You can attach an identity-based policy to a user group so that all of the users in the user group receive the policy's permission. You cannot identify a user group as a principal in a policy (such as resource based policy) because groups relate to permissions, not authentication.

Some important characteristics of user group are

→ A user group can contain many users and a user belong to multiple user groups.

2] Users groups can be nested, they can contain only users not other user groups

3] There is no default user groups that automatically include all users in the AWS account. If you want to have a user group like that, you must ~~the~~ create it & assign each new user to it.

4] The number & size of IAM resources in an AWS account, such as the no. of groups & the no. of groups that a user can be no. of are limited.

* USERS :

1] Root user :

The account owner with complete access to all AWS services & resources. You are the root user if you created the AWS account & you sign in using your root user email & password.

ii] IAM identity center user.

A user whose AWS account is a part of AWS organization who signs in through the AWS access portal with a unique URL. These users can either be created directly in IAM identity center.

11] IAM user -

An identity within your AWS account that's granted specific custom permissions. You're an IAM user if you didn't create the AWS account & your administrator or help desk employee provided you your sign-in credentials that include an AWS account.

Q2] IAM

AWS identity & access management (IAM) is a web-service that helps you securely control access to AWS & resources with IAM, you can manage permission that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) & authorized (has permissions) to use resources.

— Identities.

When you create an AWS account, you begin with one sign in identity that has complete access to all AWS services & resources in the account. This identity is called the AWS account root user & is accessed by signing in with email ID & password.

Access Management.

After a user is setup in IAM, they use their sign up credentials to authenticate & with AWS. Authentication provided by matching the sign in credentials to a principal (an IAM user, federated user, IAM role) trusted by the AWS account. Next, a request is made to grant the principal access to resources.
For eg. when you first sign in to the console & on the console homepage, you aren't accessing a specific service. When you select a service, the request for authorization is sent to that service & it looks to see if your identity is on the list of authorized users, what policies are being enforced to control the level of access.

Q3 IAM Roles.

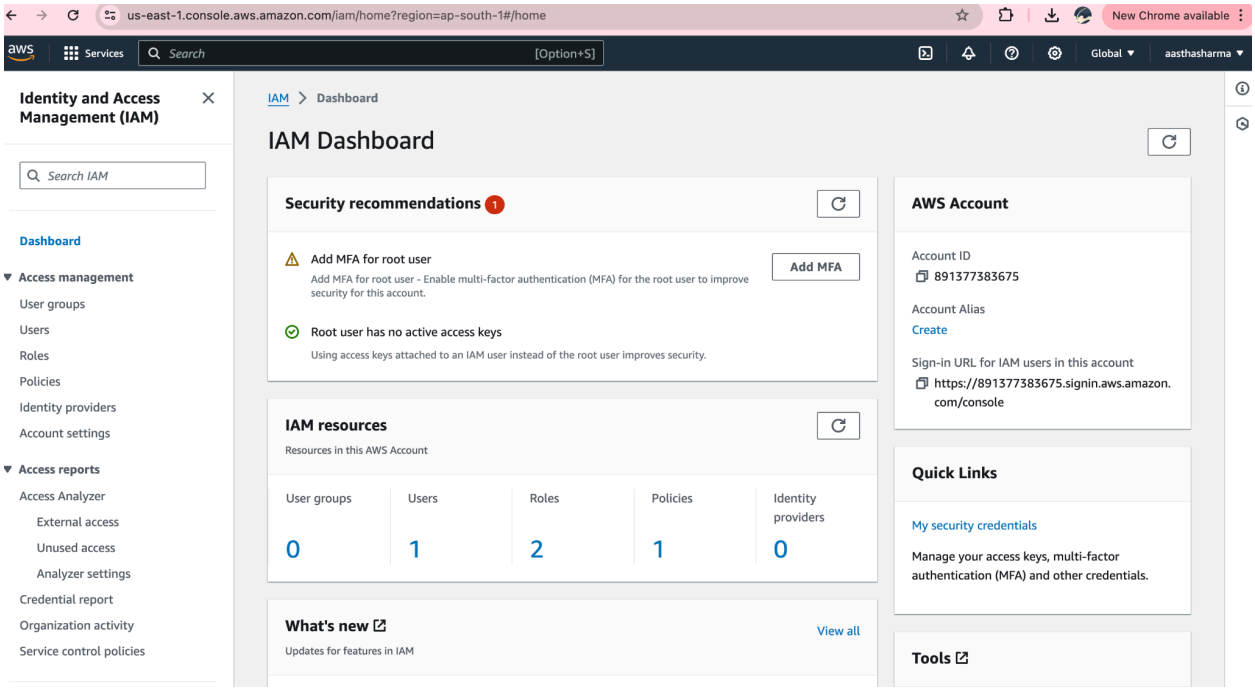
An IAM role is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can & cannot do in AWS. However, instead of being uniquely associated with one person, a role credentials such as a password or access key associated with it.

You can use roles to delegate access to users apps, or services that don't normally have access to your AWS resources. For eg. you might want to grant users in your AWS account access to resources they don't usually have or grant users in one AWS account access to resources in another account. Or you sometimes you want to give AWS access to users who already have identities defined outside of AWS such as in your corporate directory. Or you access to your account to 3rd party so they can perform an audit on your resources.

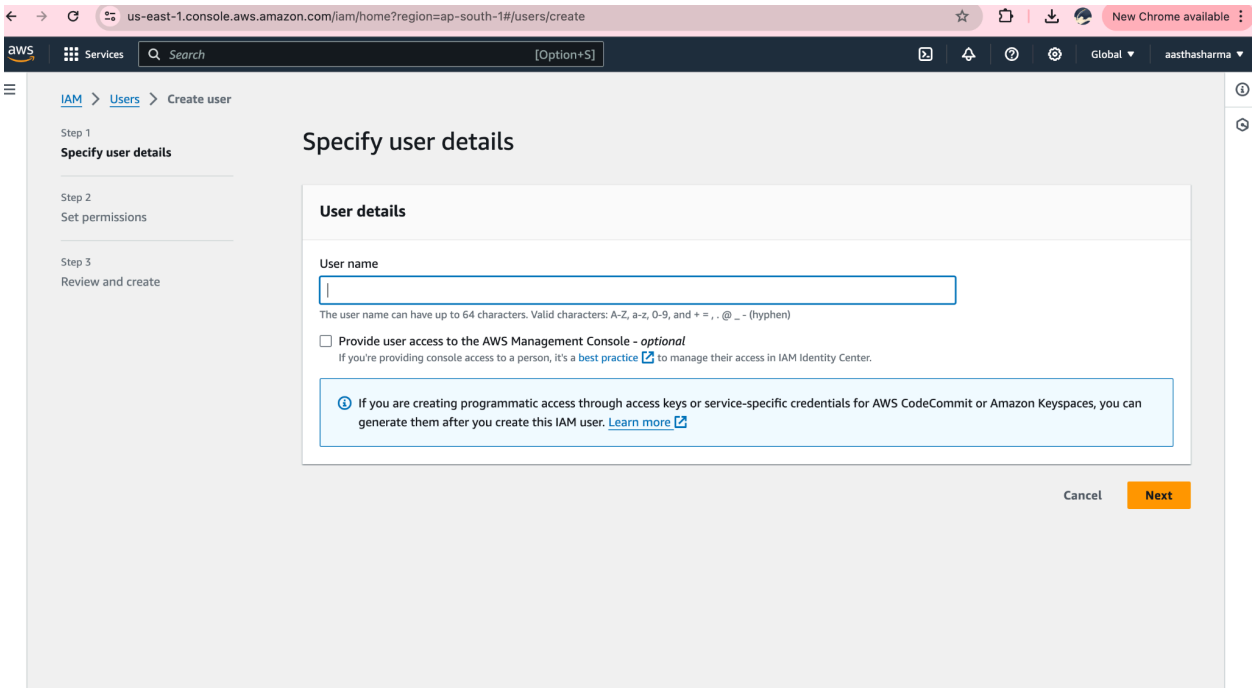
Practical-3
IAM

Steps

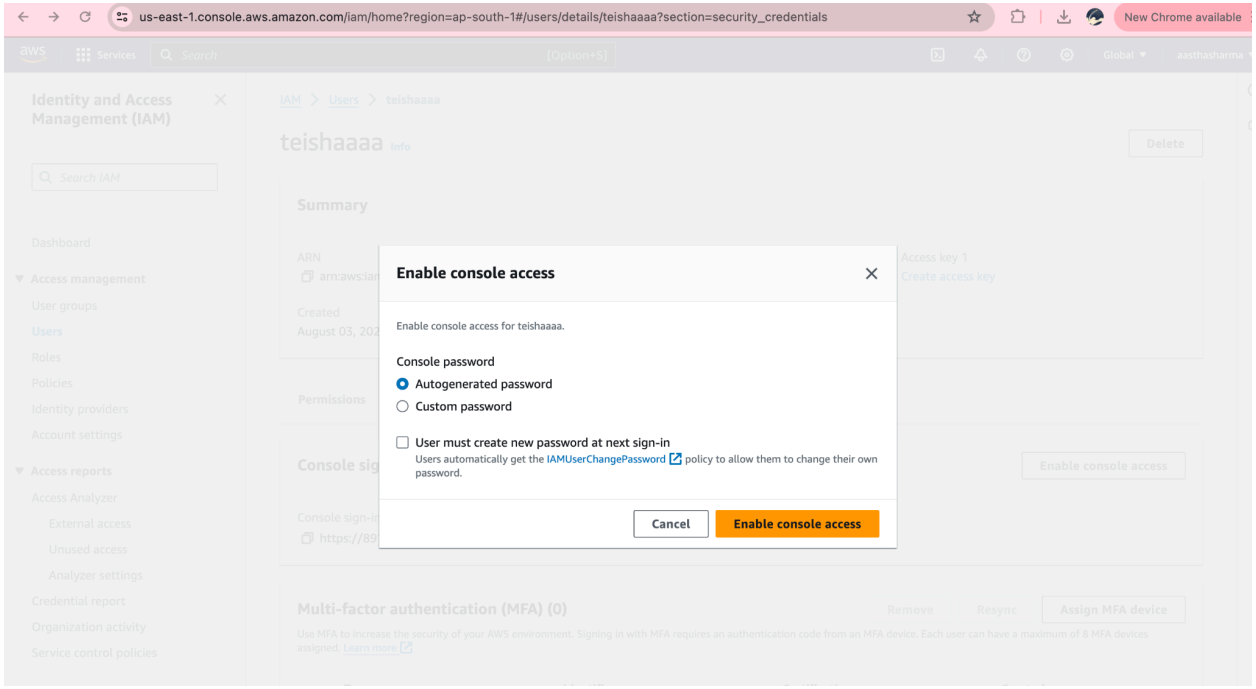
1. Go to IAM



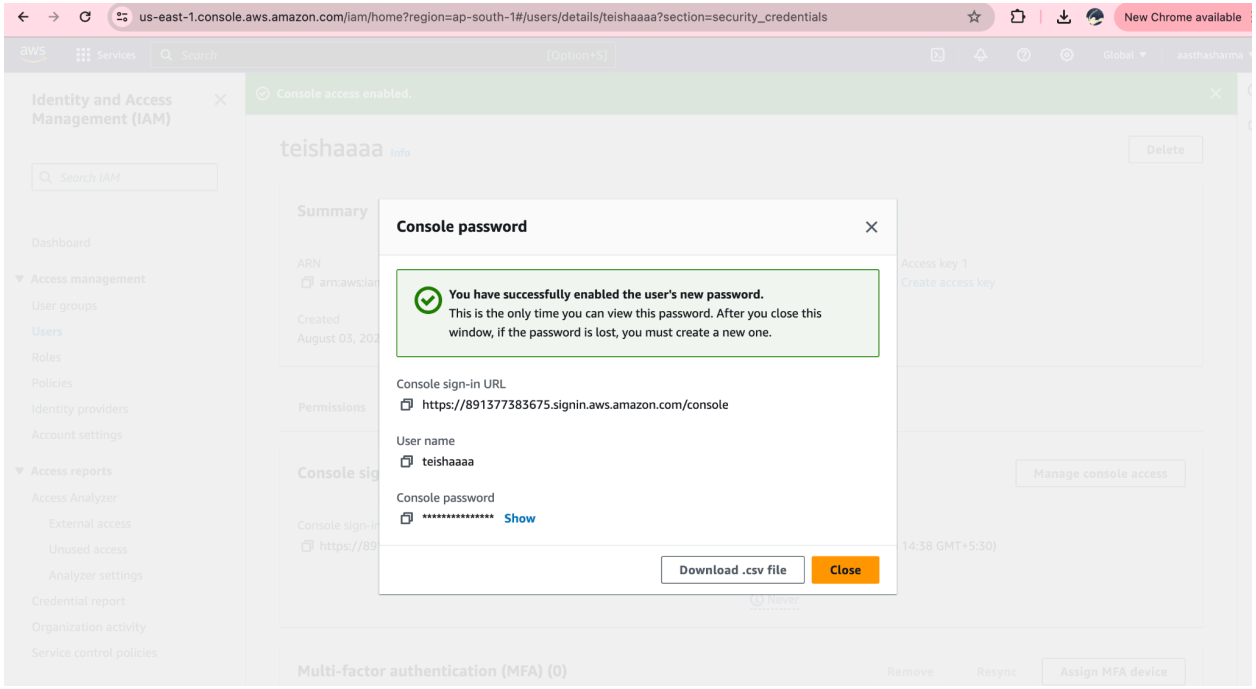
2. Go to users and add a user



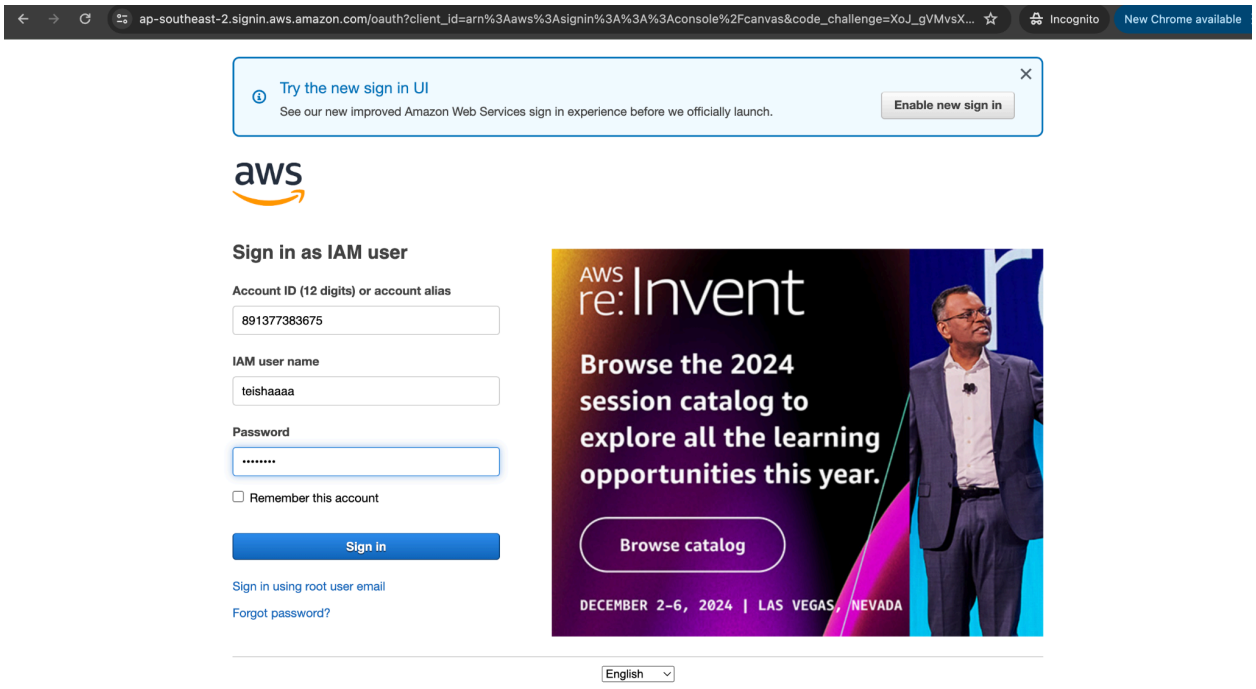
3. Either auto generate the password or create custom password



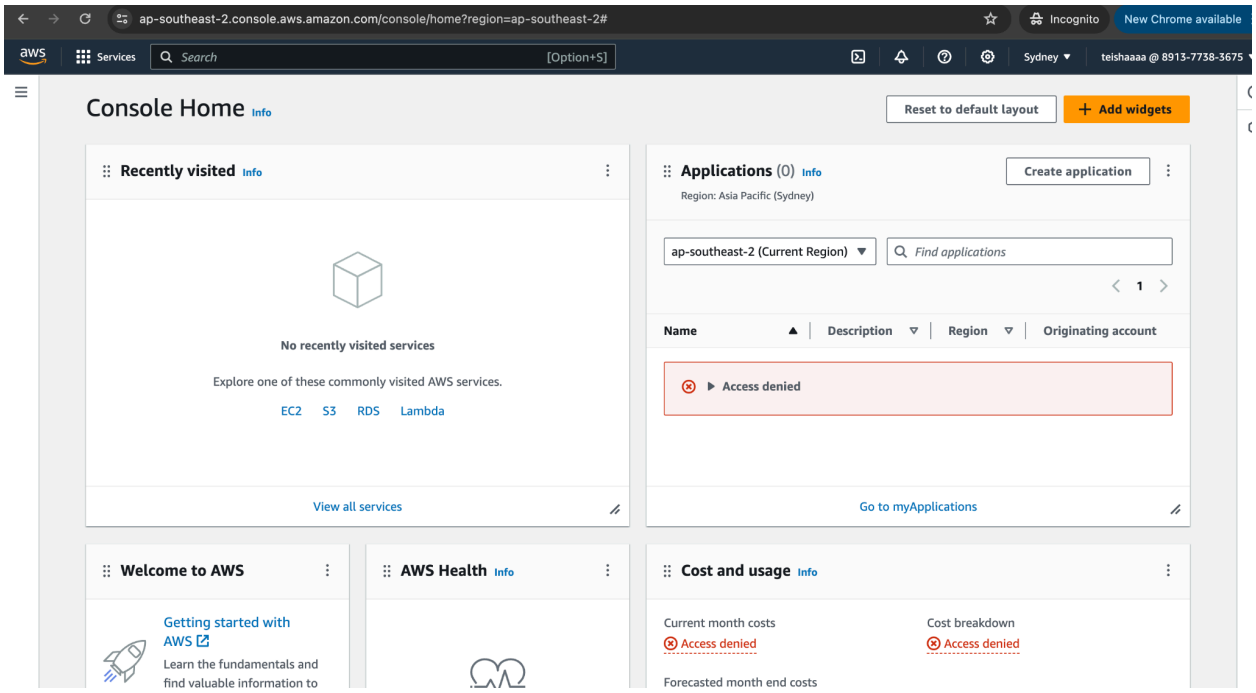
4. Use the gen URL and password

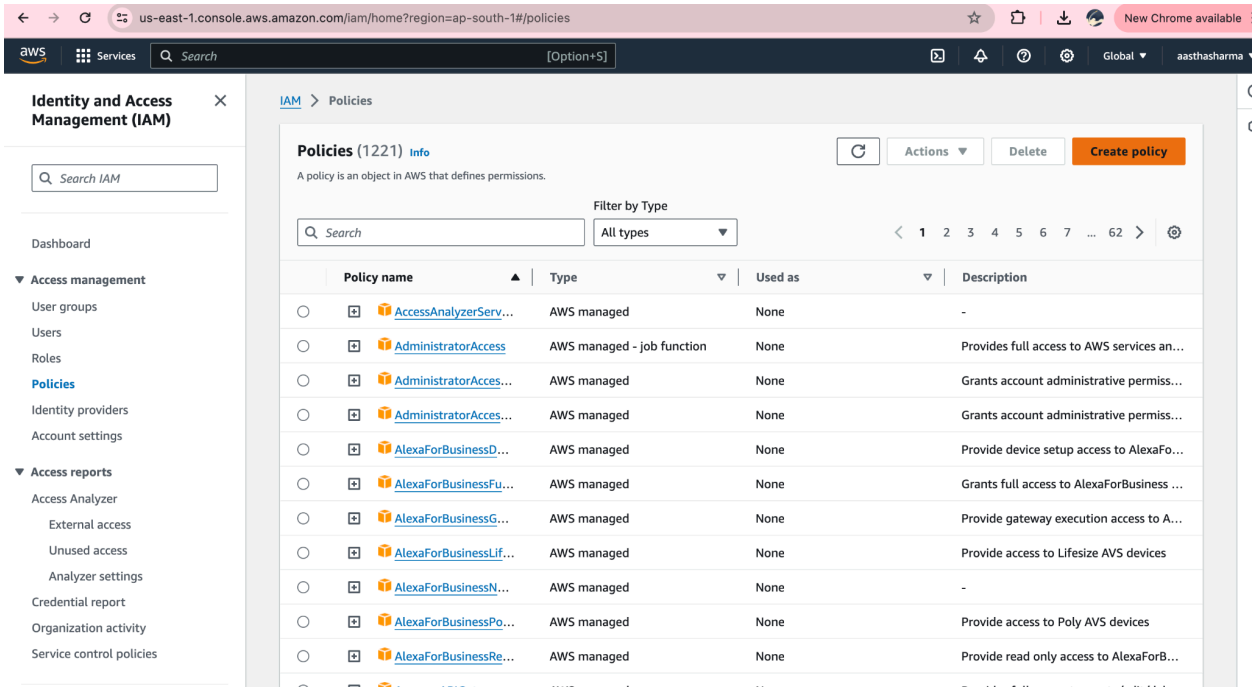


5.open a new window and use the generated credentials

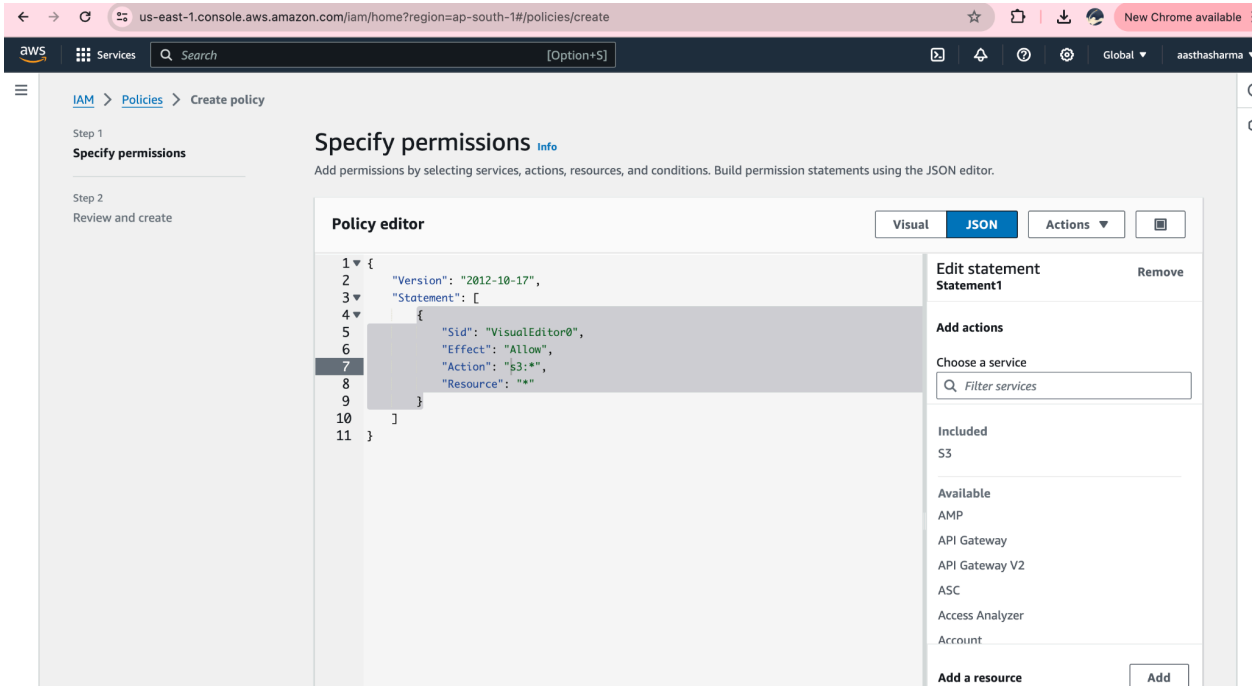


6. As of now, permissions are denied even though console is visible.

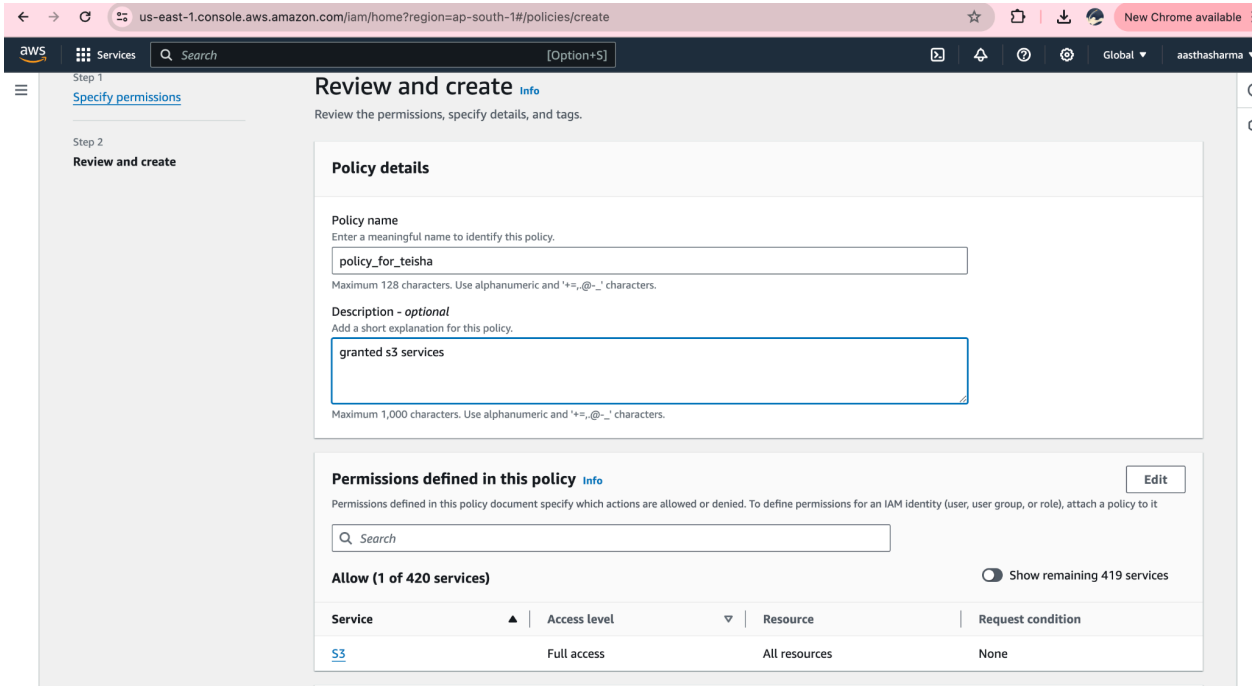




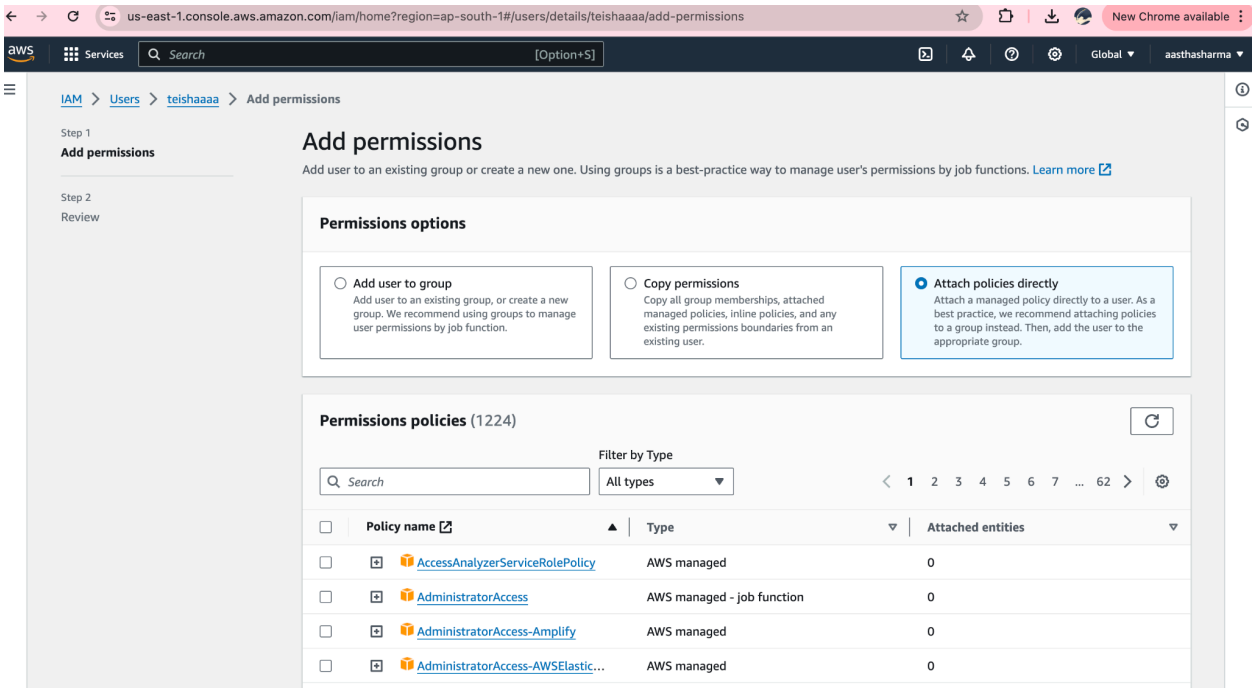
7. ^ go to policy and create policy, change SID to your created user



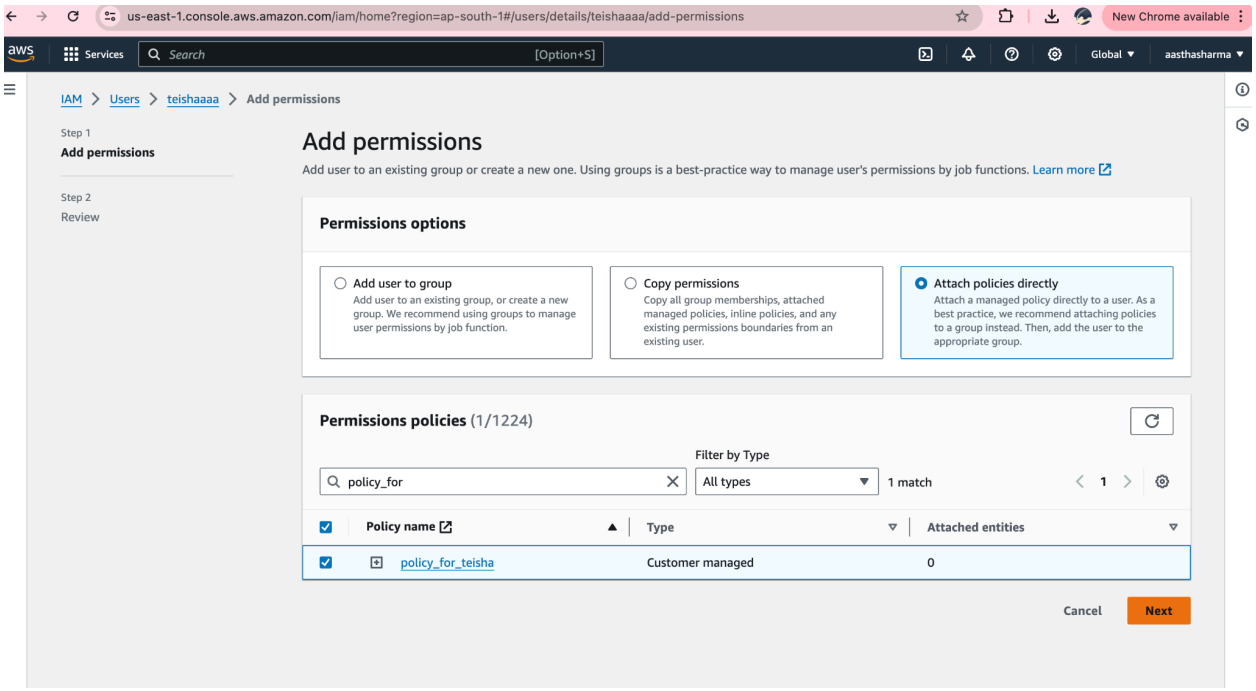
8. Name the policy and add description



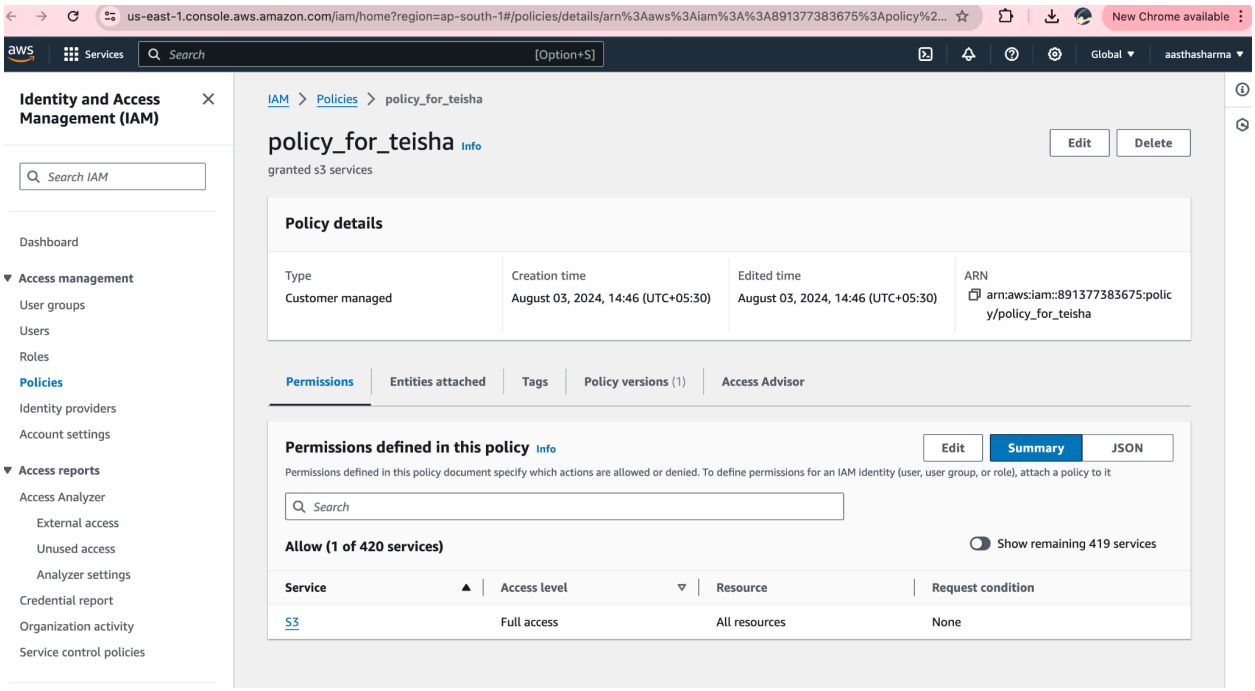
9. Attach the created policy



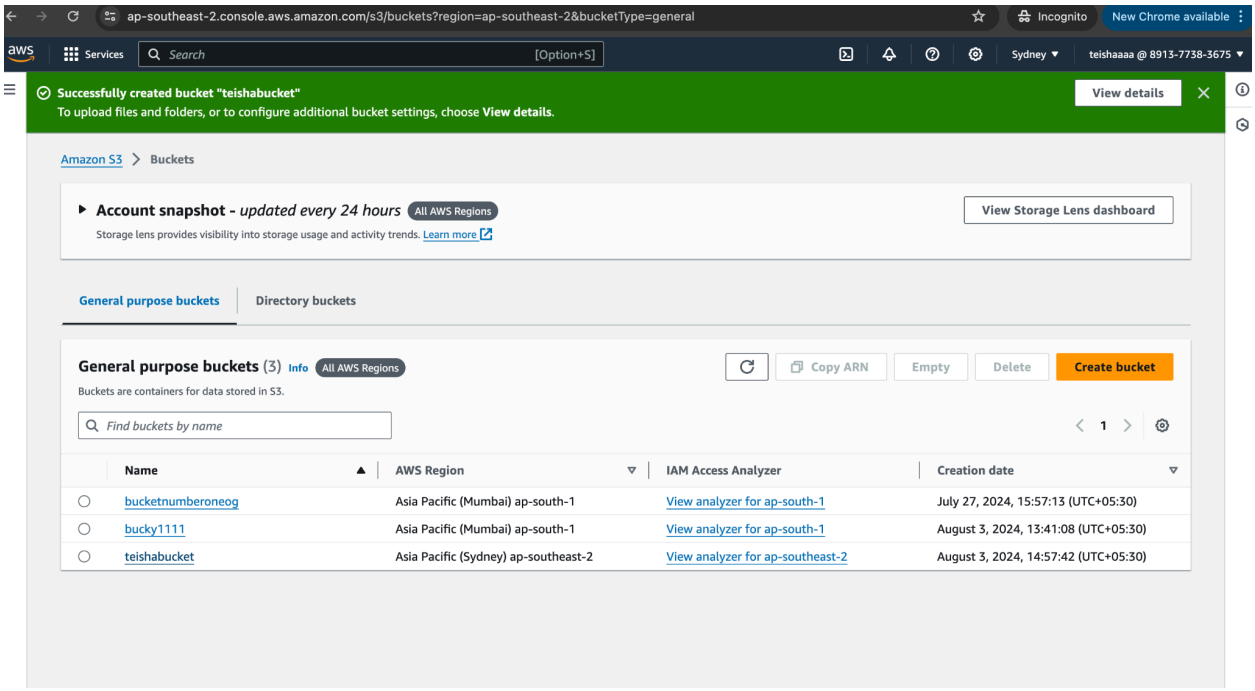
10. Attach the policy the user



S3 permission has been granted!



11. Open the account using user credentials again and we can see s3 permissions have been granted as a bucket is now created for user “teishaaa”



Create buckets and folders as required.