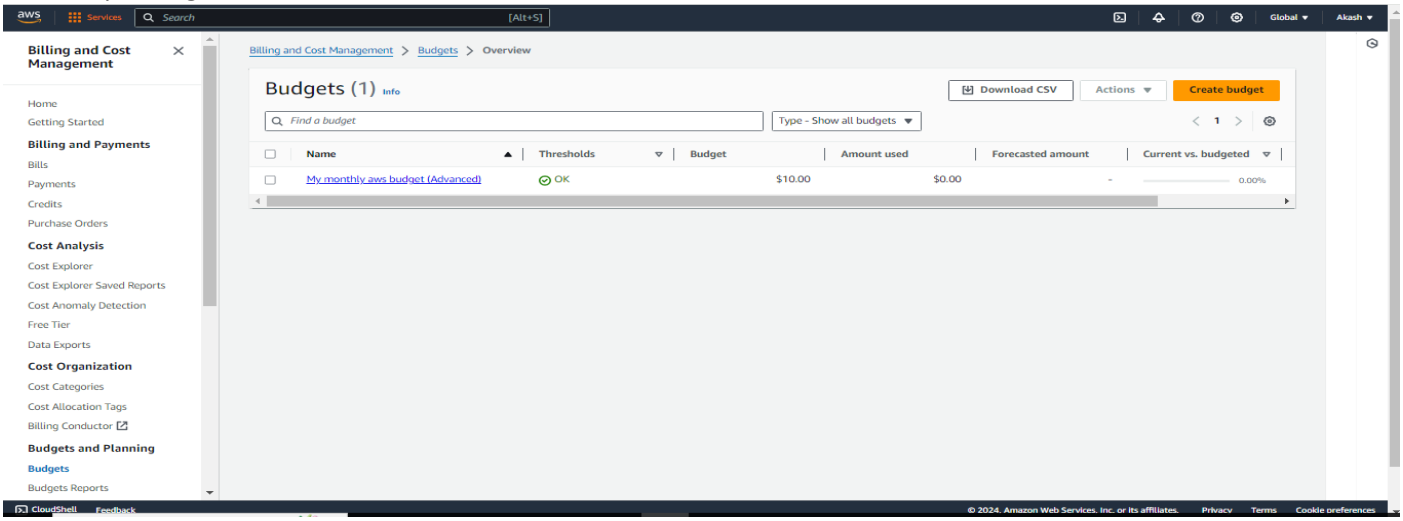
Practical:2 - IAM (Identity Access Management)

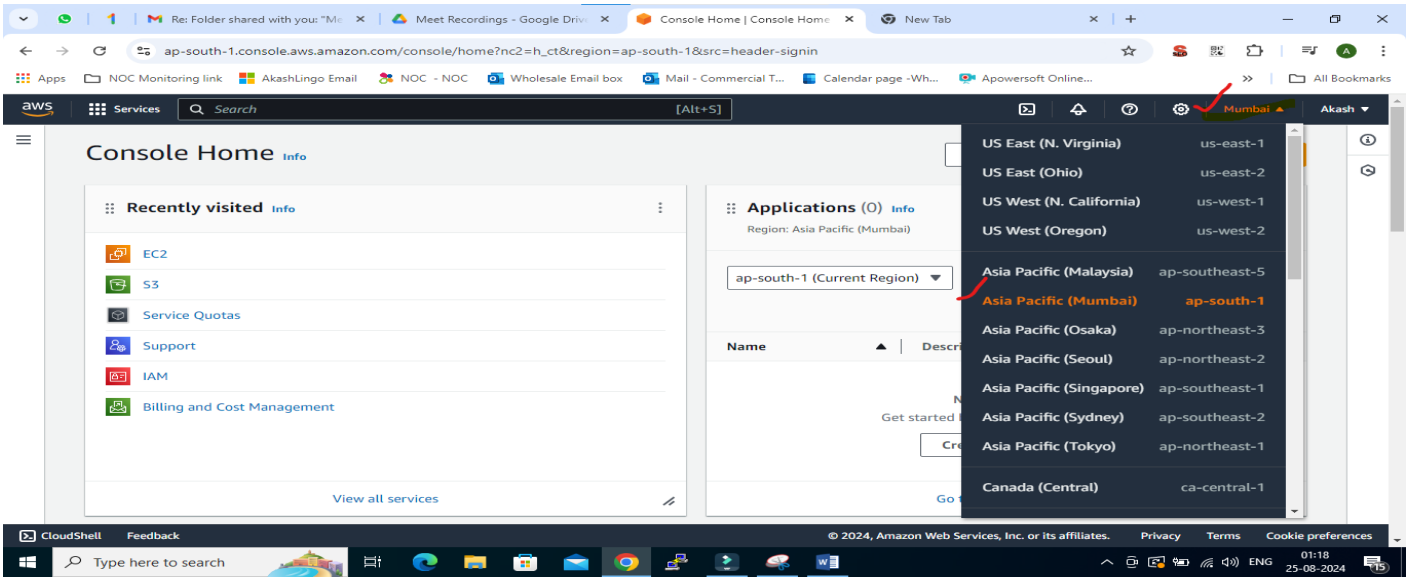
14th Aug 2024 (L-2) | Akash Ghuge

---

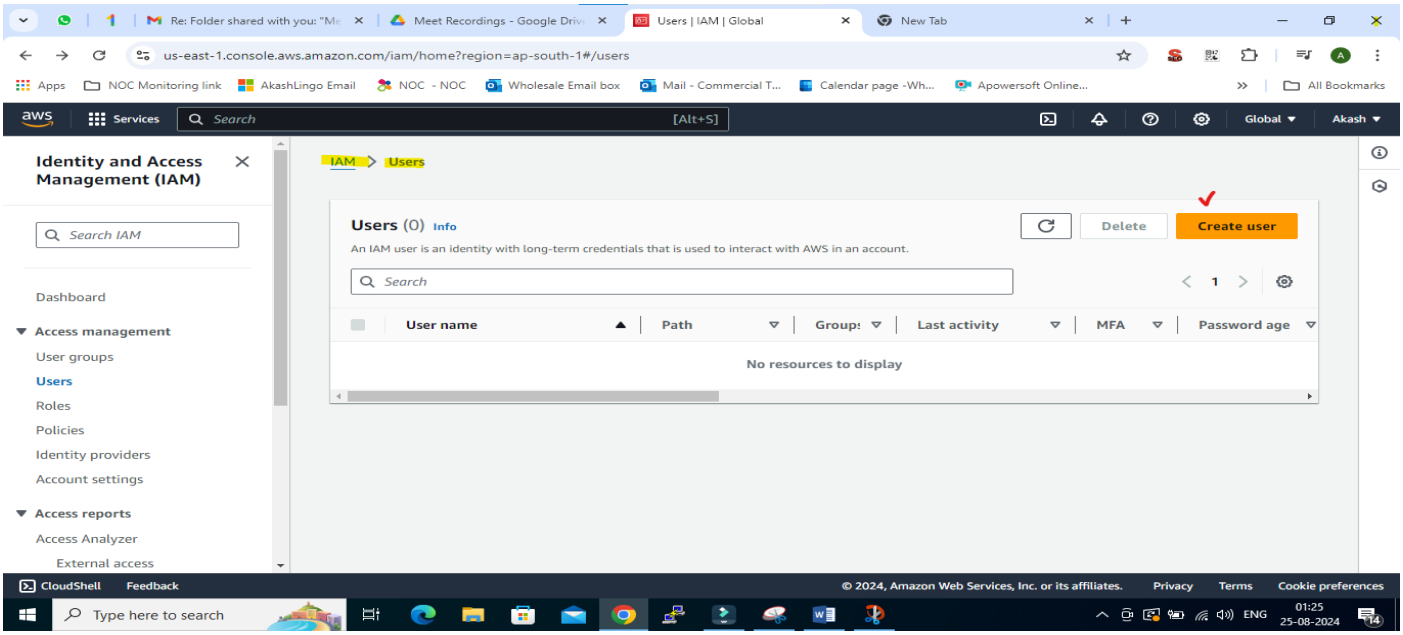
1. Setup billing alarm.

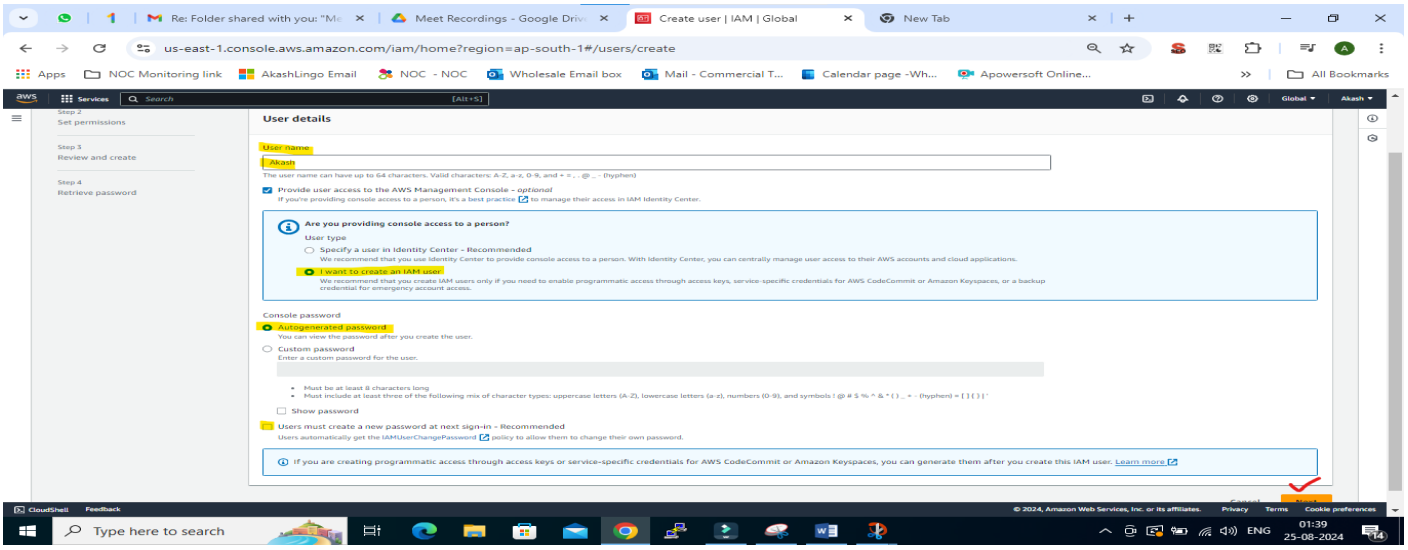


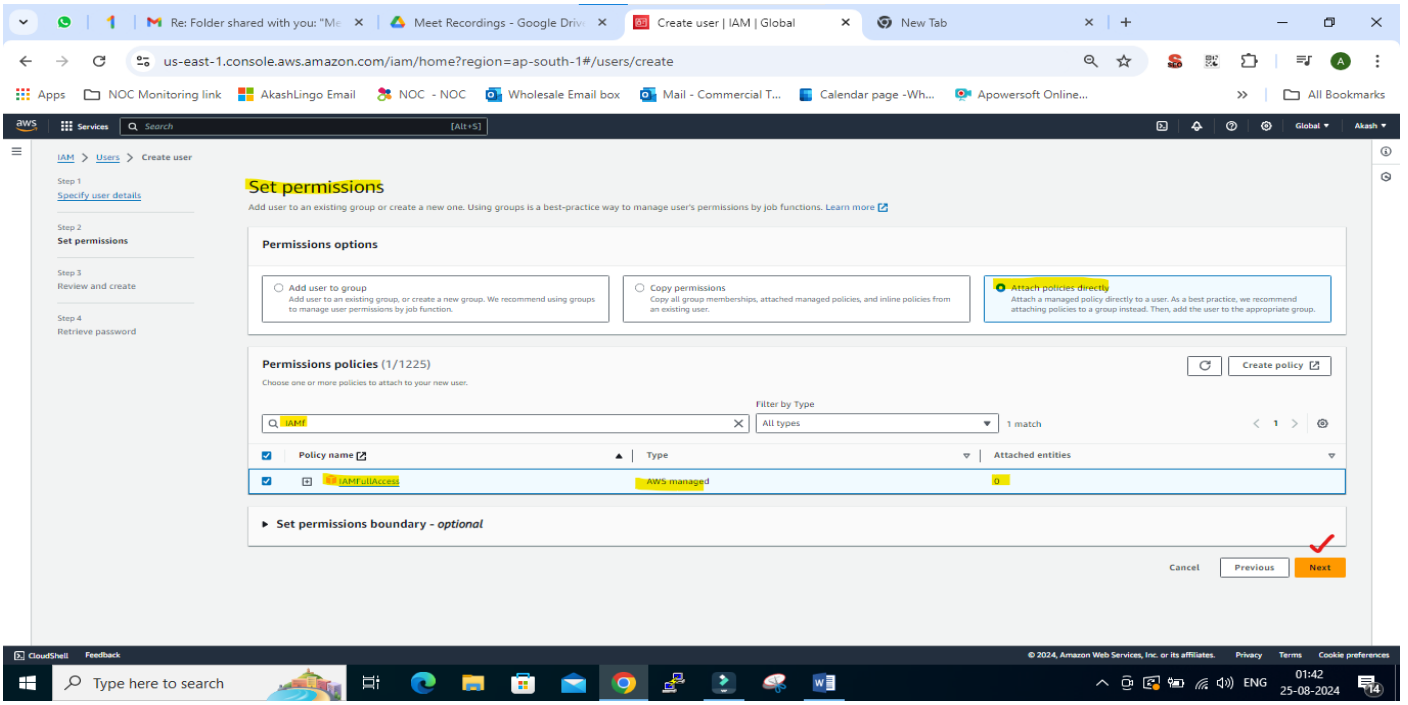
2. Set the Mumbai Regions:

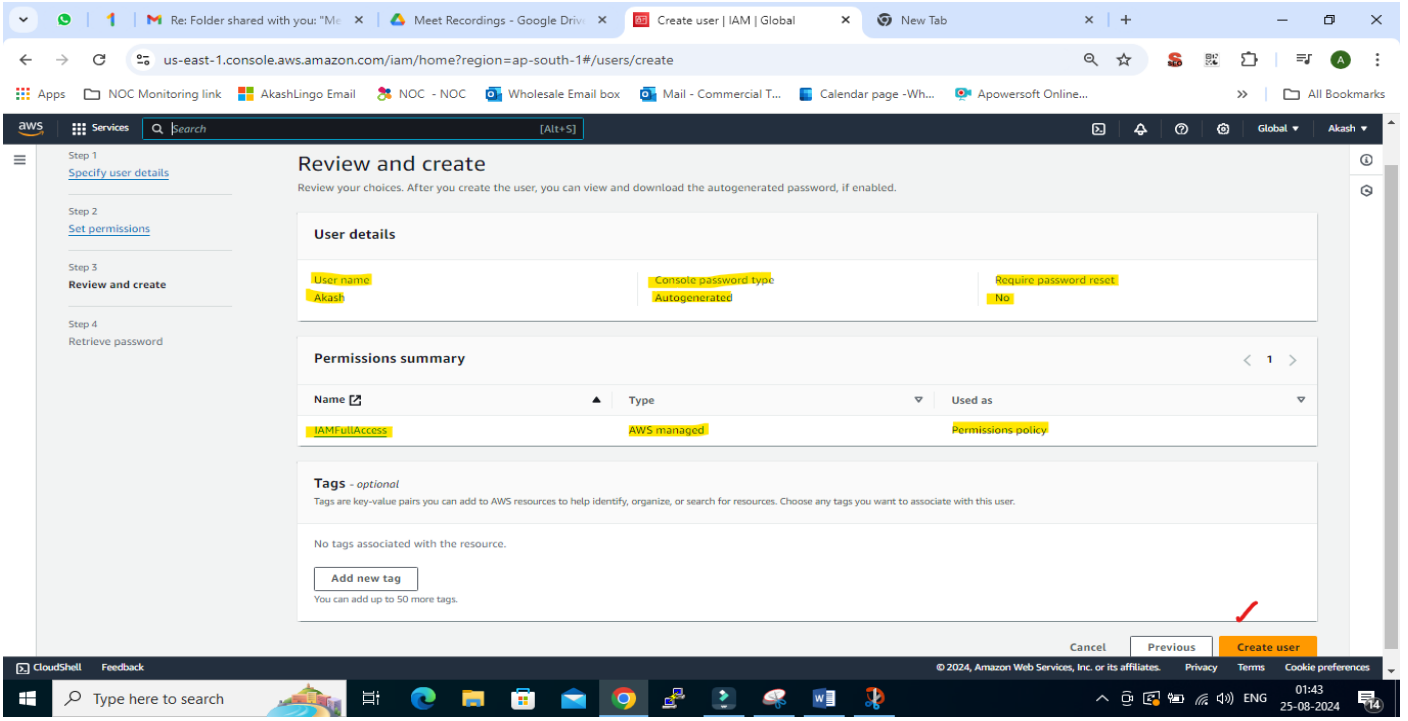


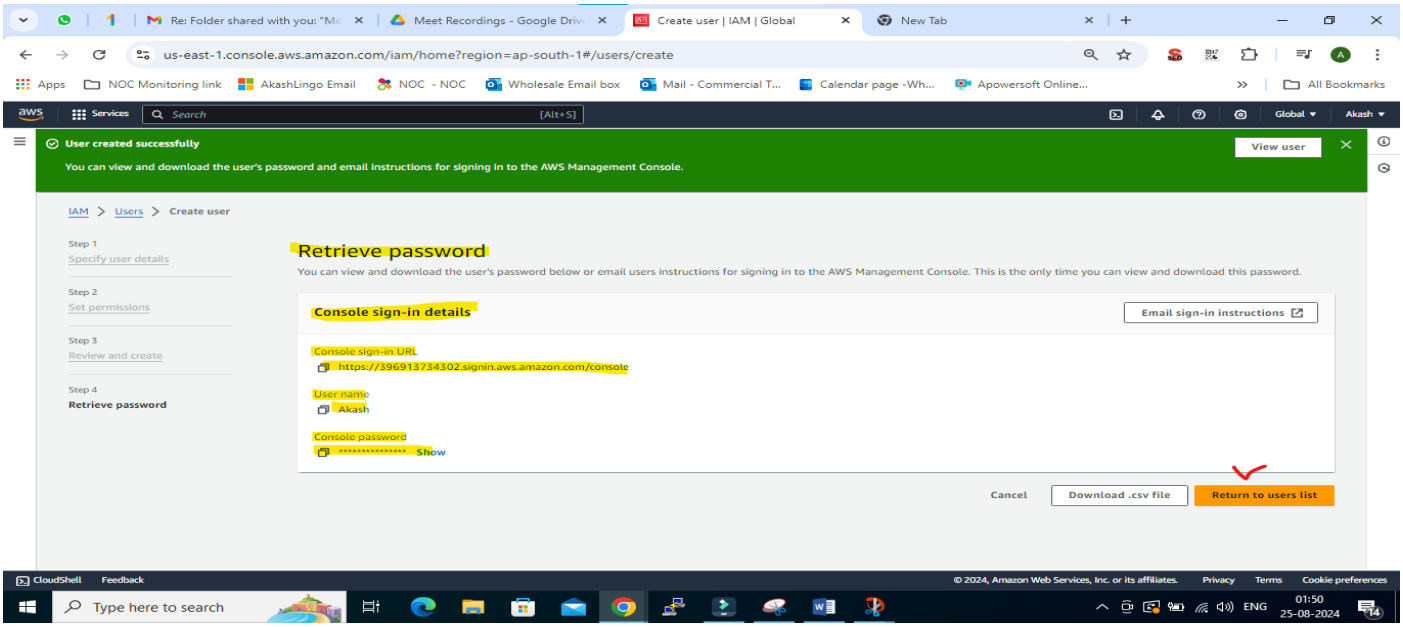
3. Create User



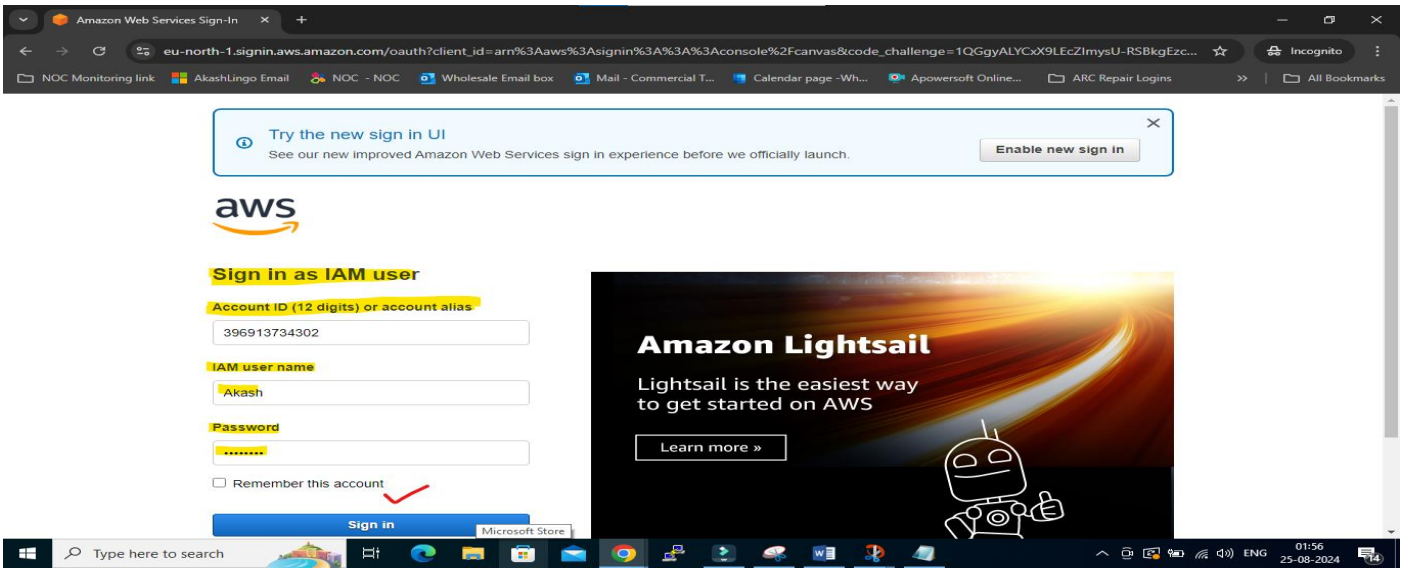

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
User details
User name
Akash
Provide user access to the AWS Management Console - optional
Are you providing console access to a person?
I want to create an IAM user
Console password
Autogenerated password
Custom password
Show password
Users must create a new password at next sign-in - Recommended
Type here to search
01:39
25-08-2024

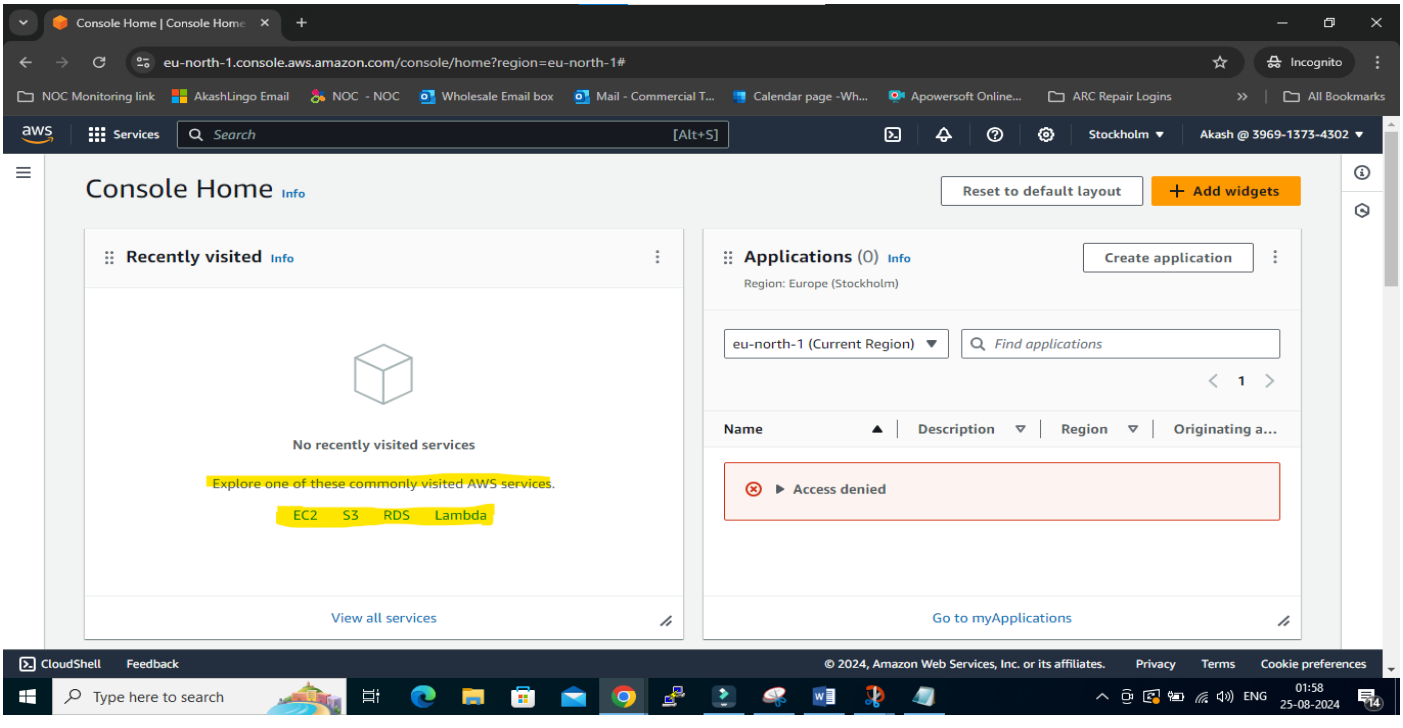

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Copy permissions
Attach policies directly
Permissions policies (1/1225)
Choose one or more policies to attach to your new user.
Create policy
Filter by Type
IAMF
All types
1 match
Policy name
Type
Attached entities
IAMFullAccess
AWS managed
0
Set permissions boundary - optional
Cancel
Previous
Next
Type here to search
01:42
25-08-2024

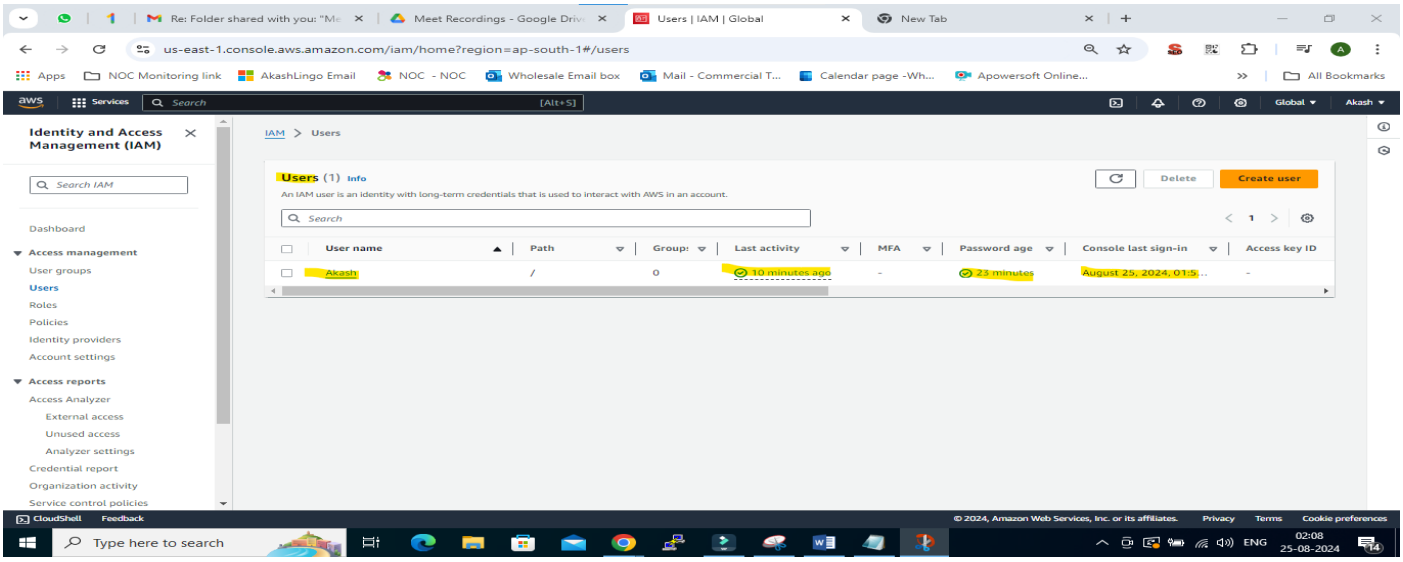

Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
Akash
Console password type
Autogenerated
Require password reset
No
Permissions summary
Name
Type
Used as
IAMFullAccess
AWS managed
Permissions policy
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create user
Type here to search
01:43
25-08-2024



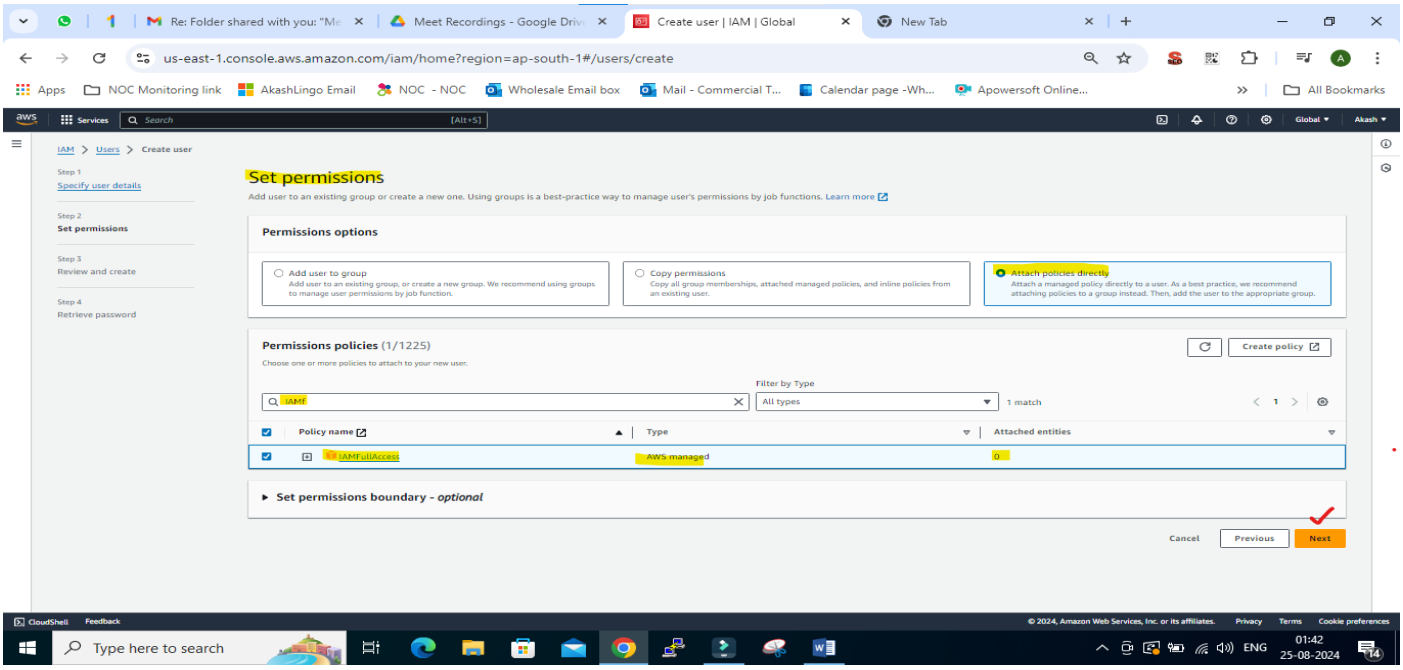
4. Used Different Browser to access IAM user with URL, ID & Password

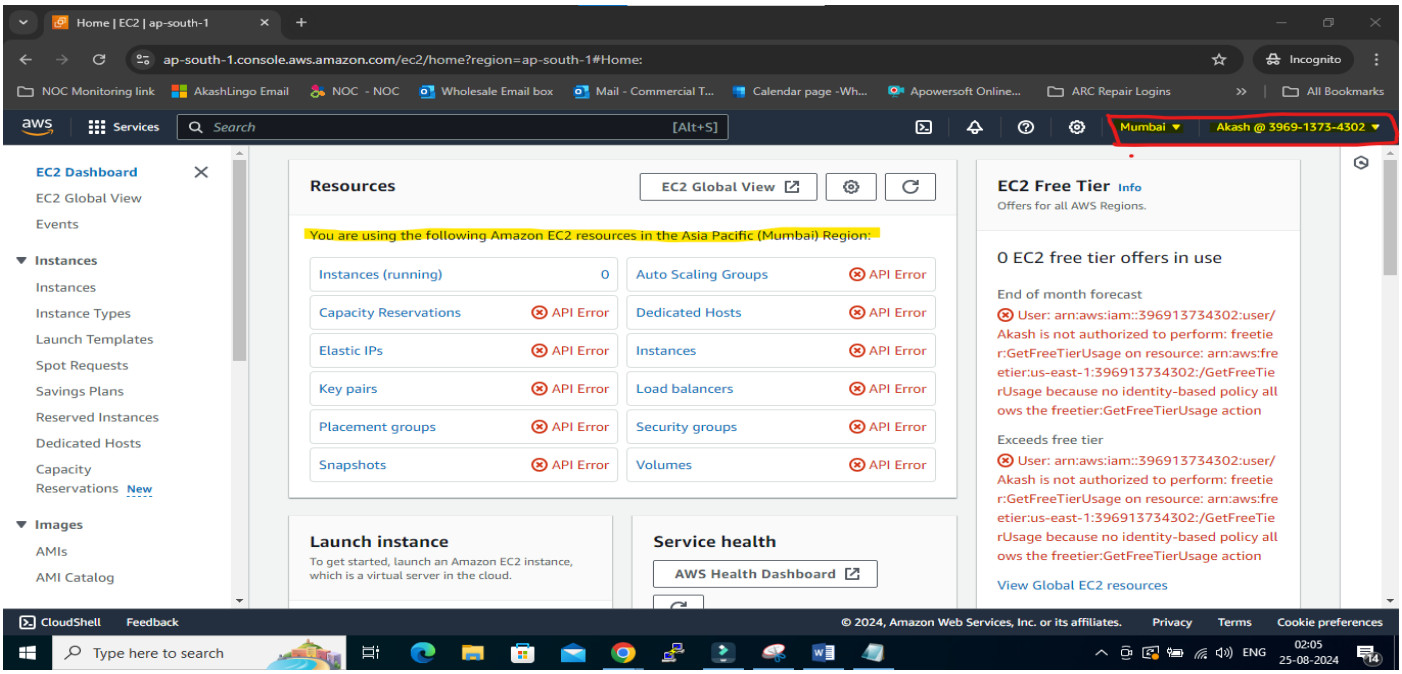




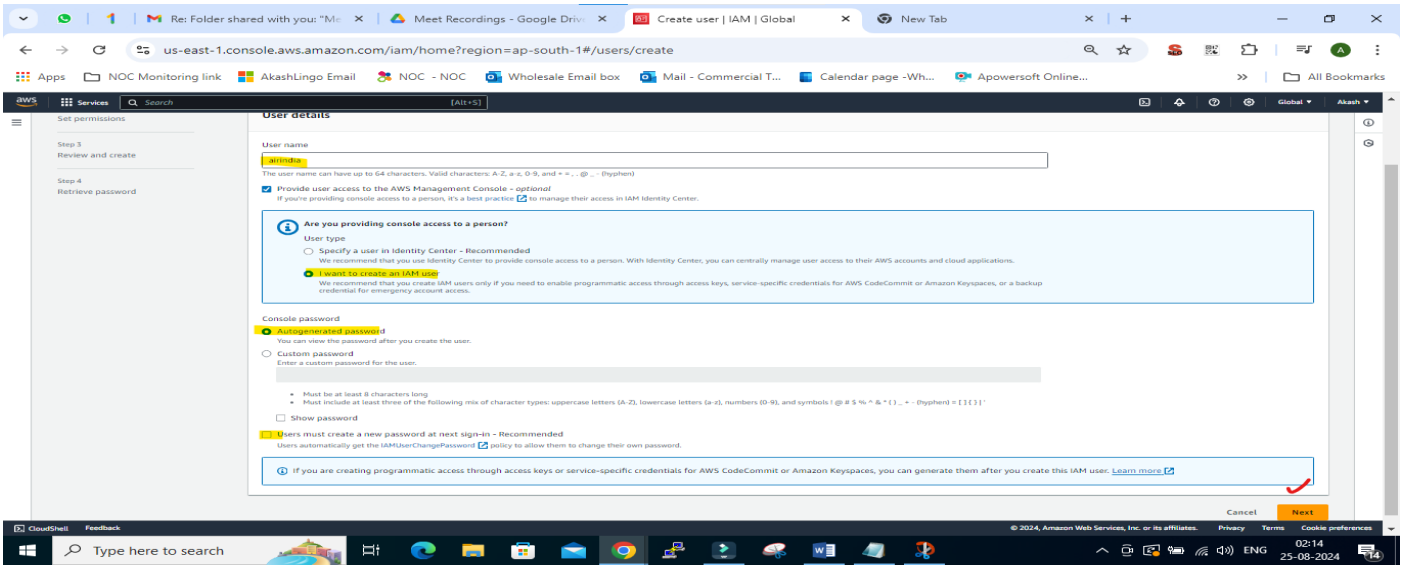


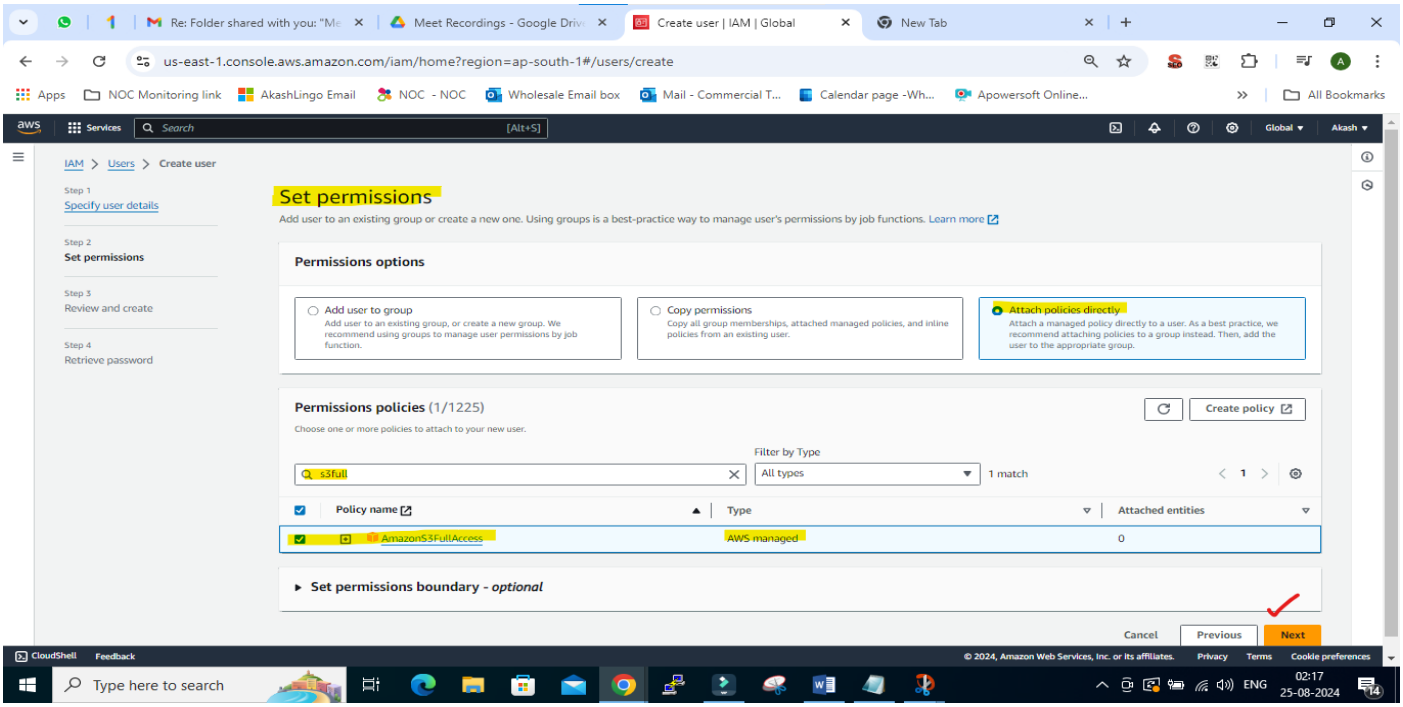
5. IAM User are able to access all the services such as S3 & EC2 etc.

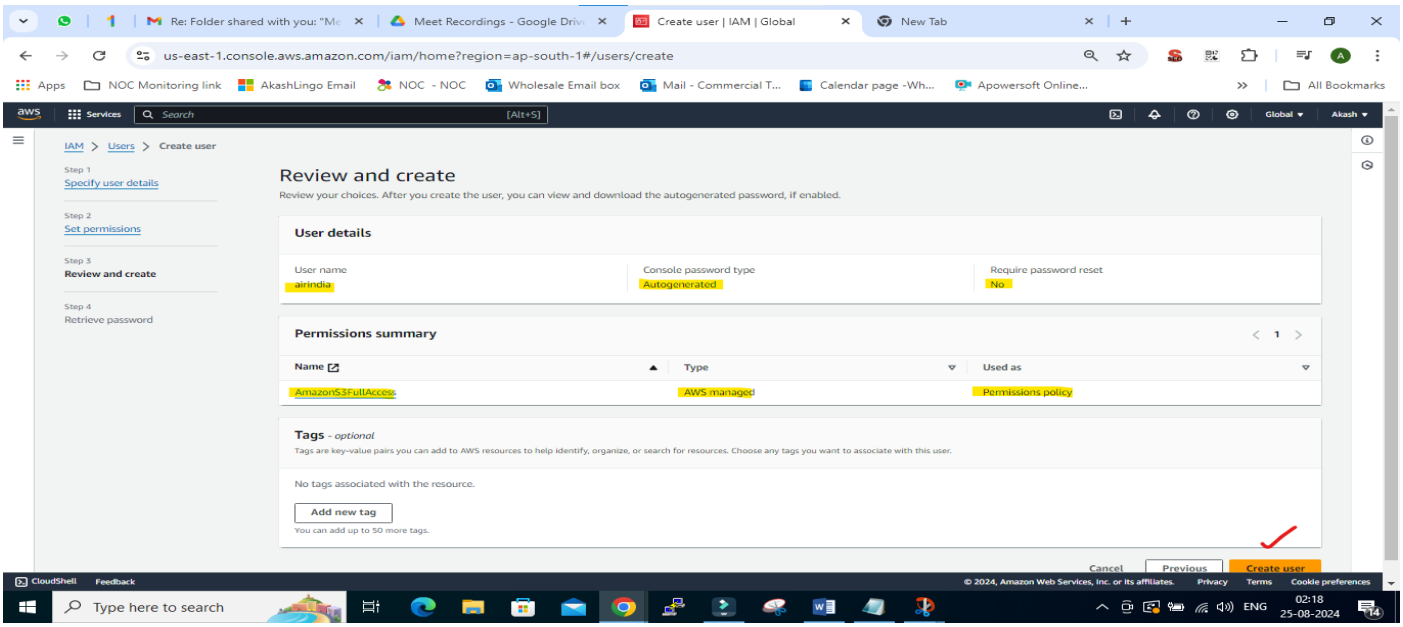


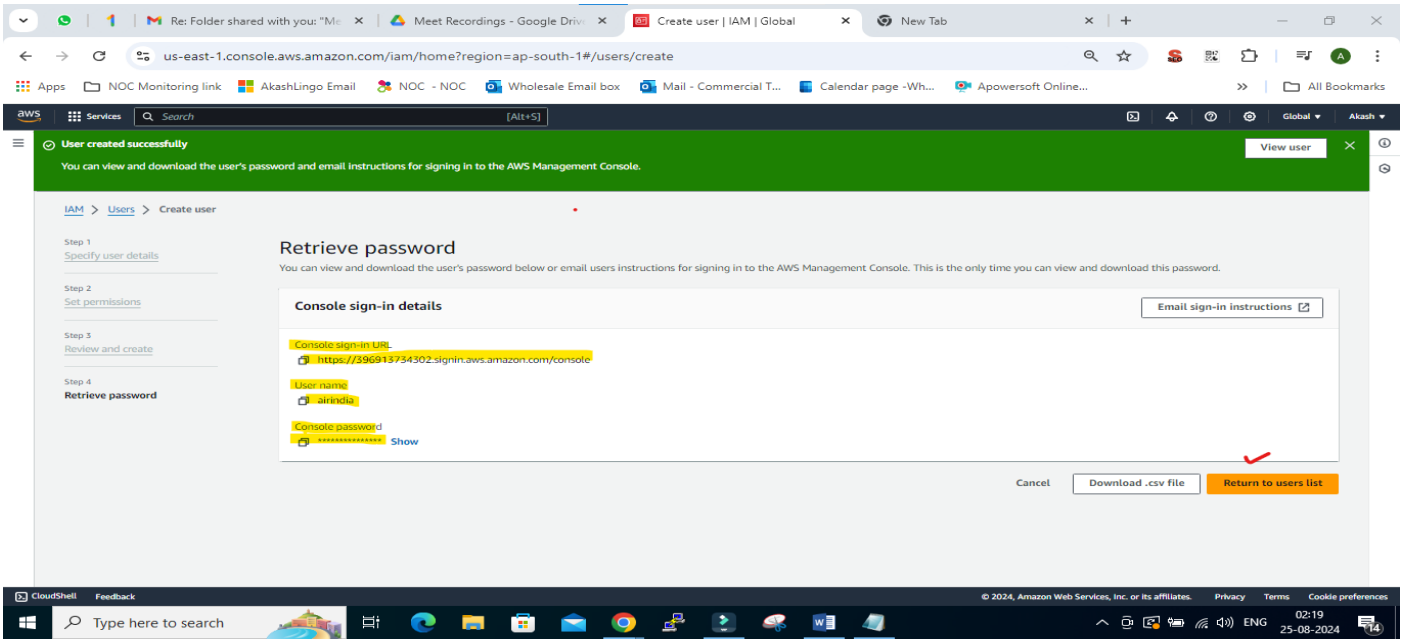


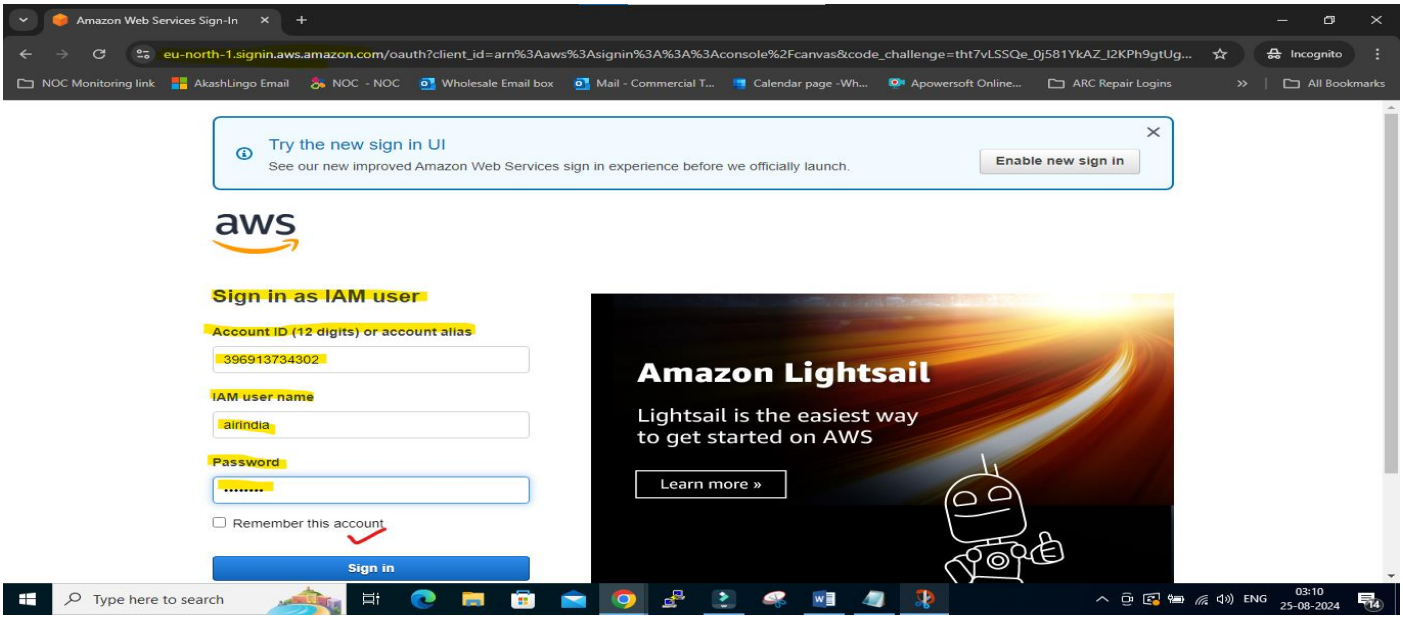
1. User: Airindia >> Policy S3 Full Access:



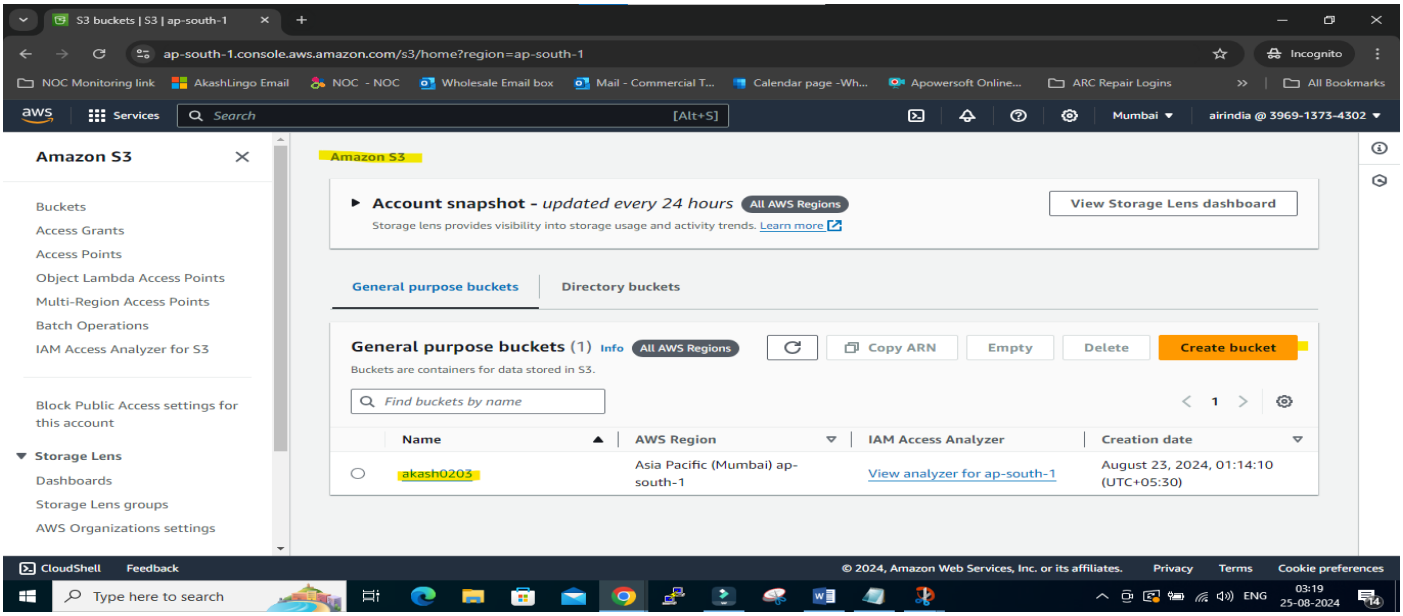


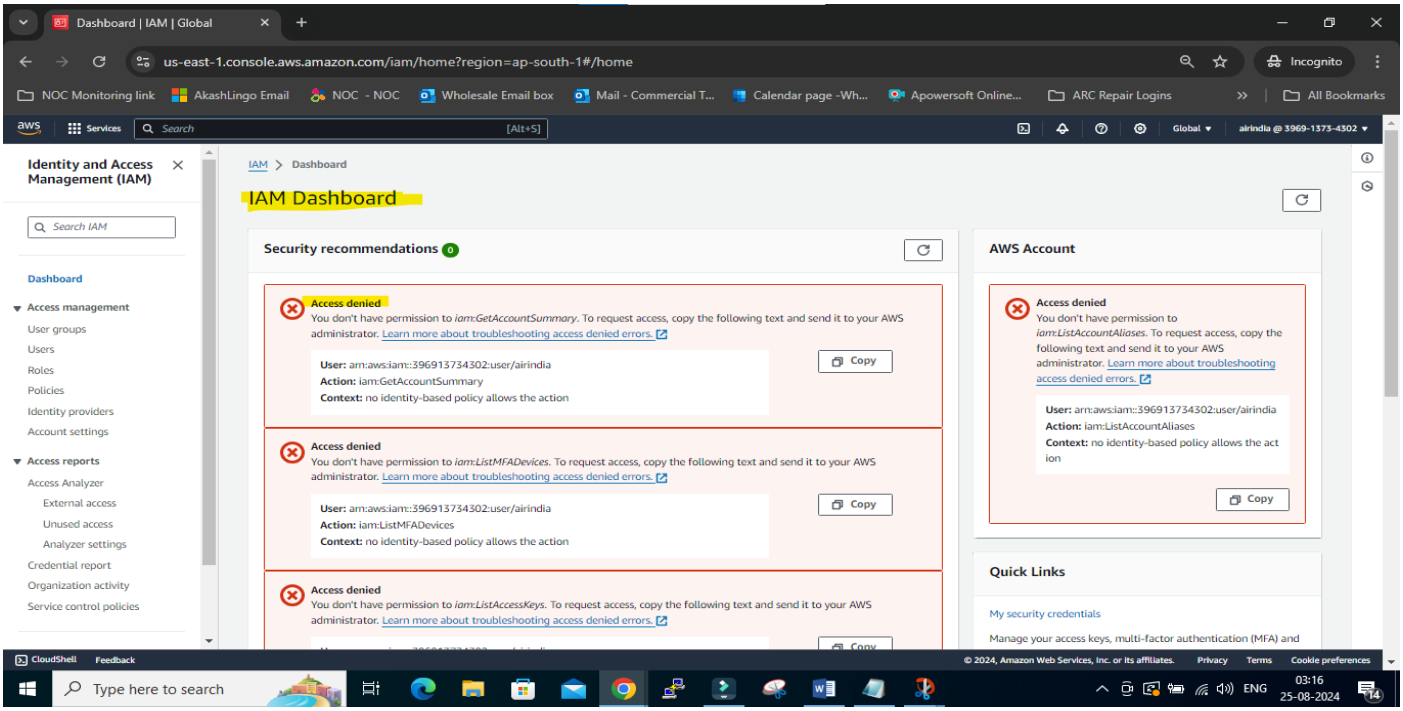






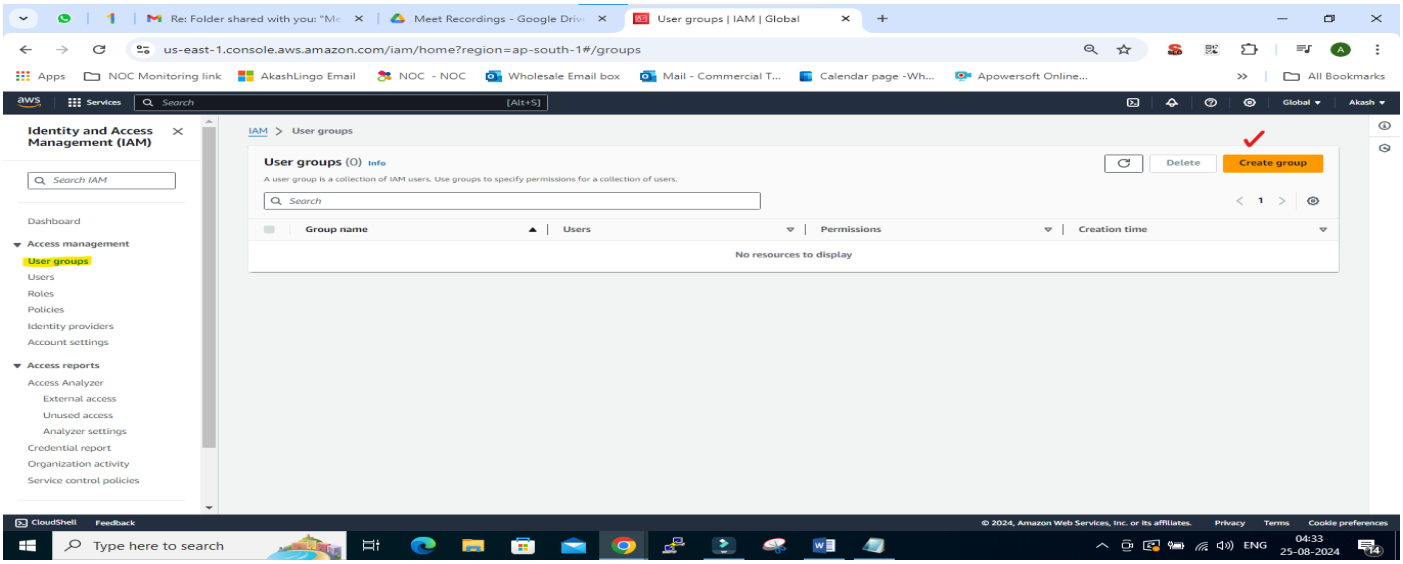
2. AirIndia user is only allow to access S3 not for IAM:

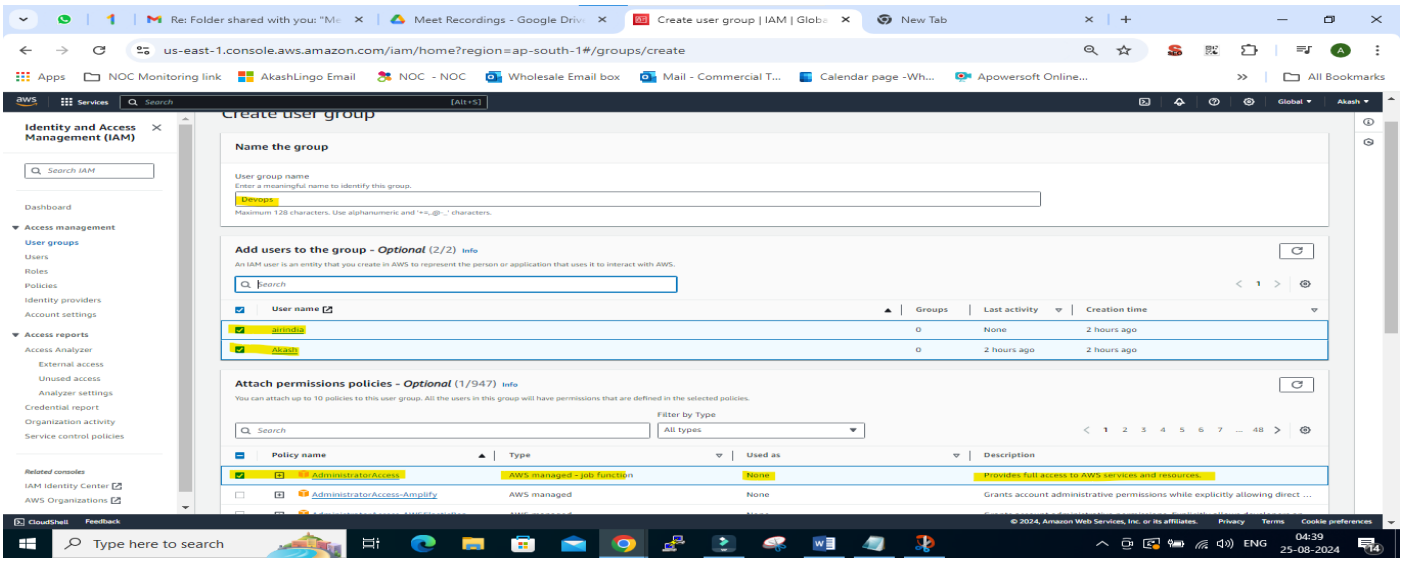


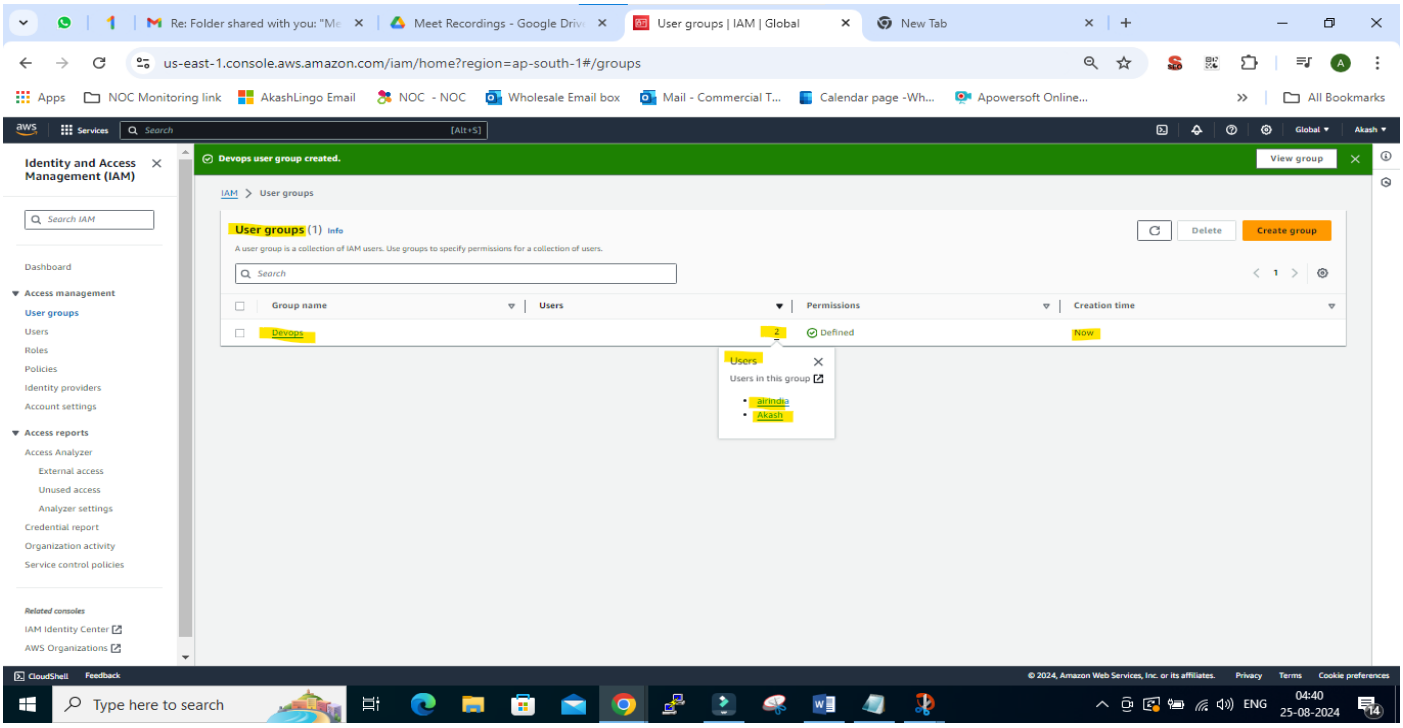


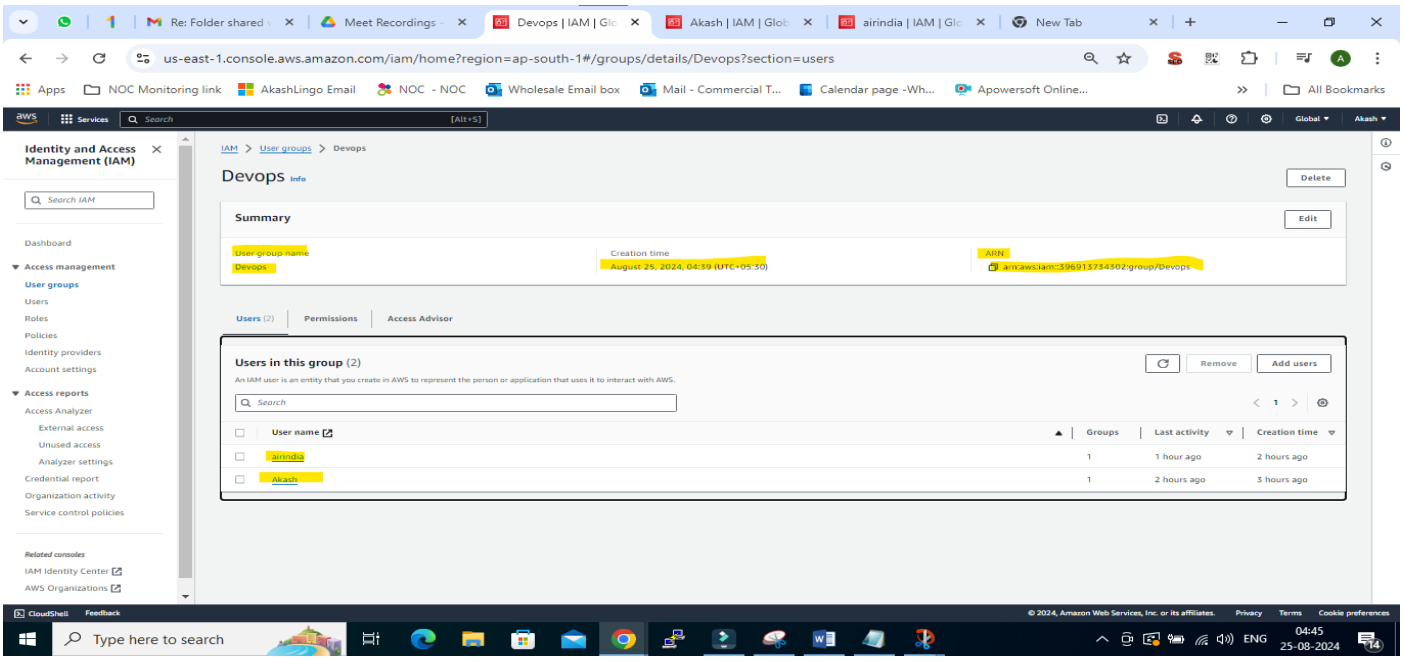
---

1. Create Groups:

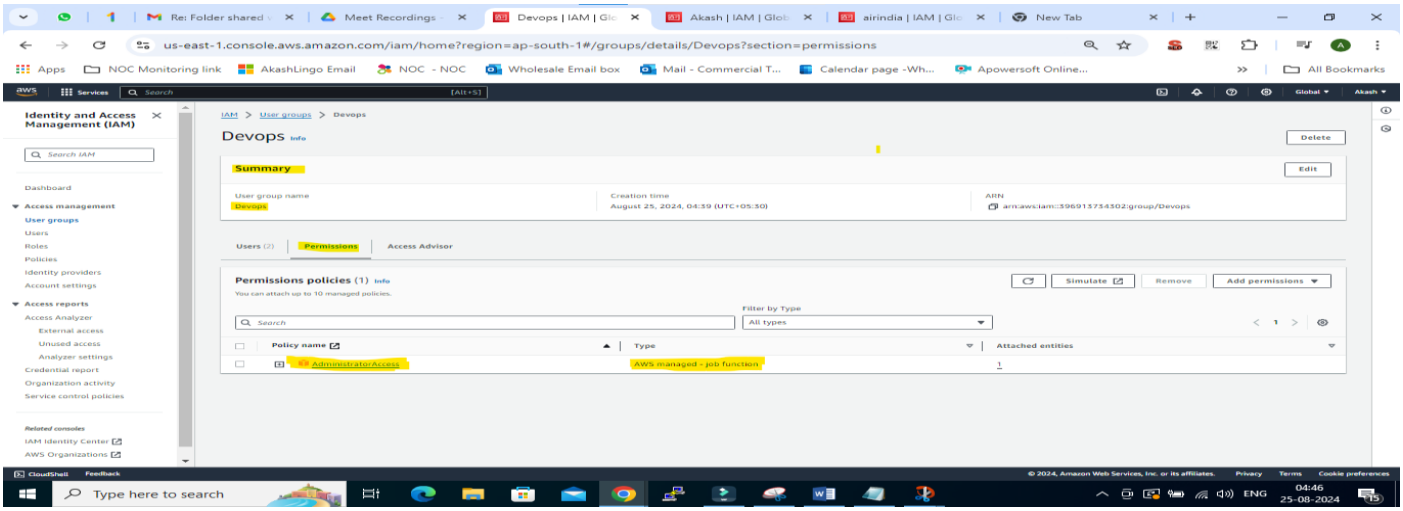






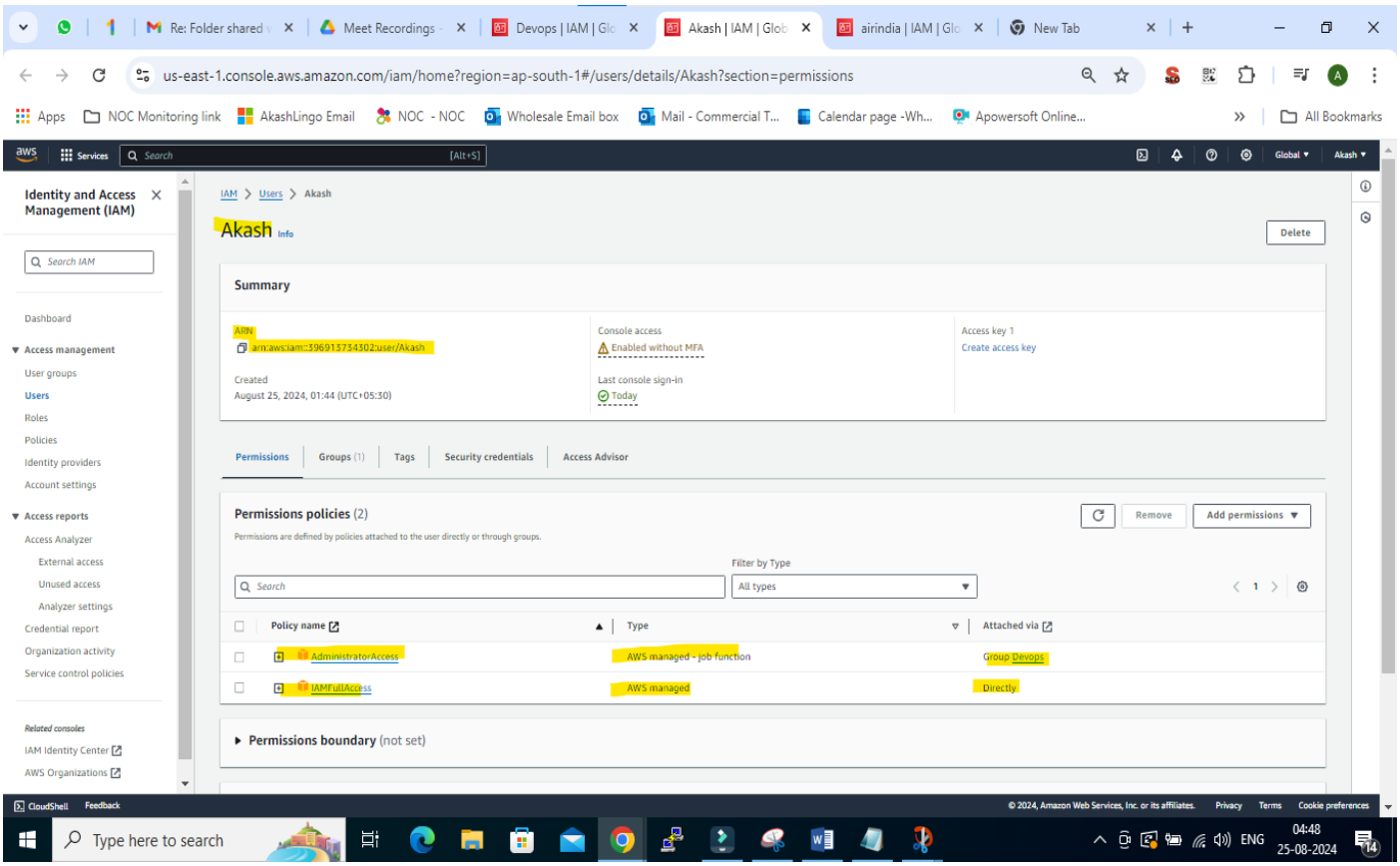


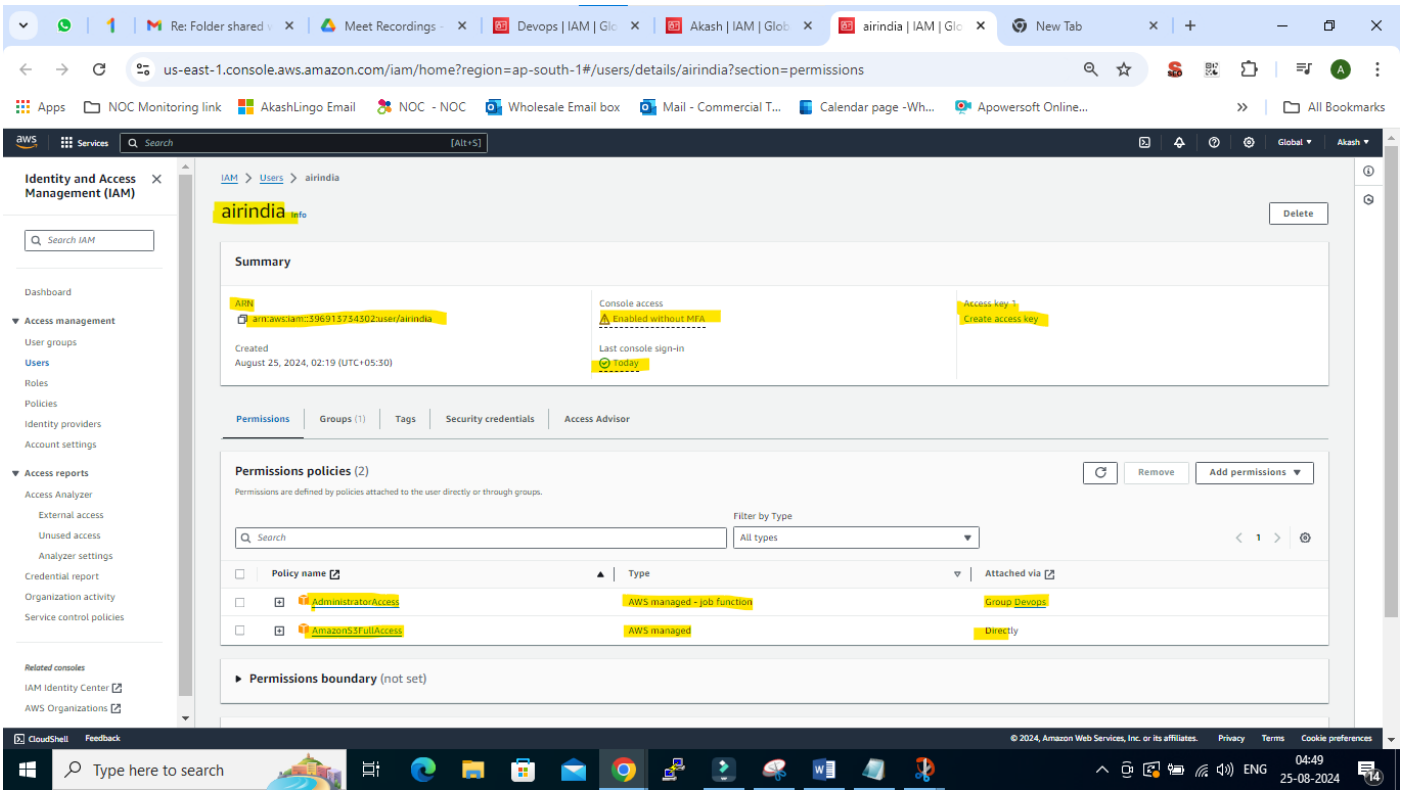
2. Group level permission:



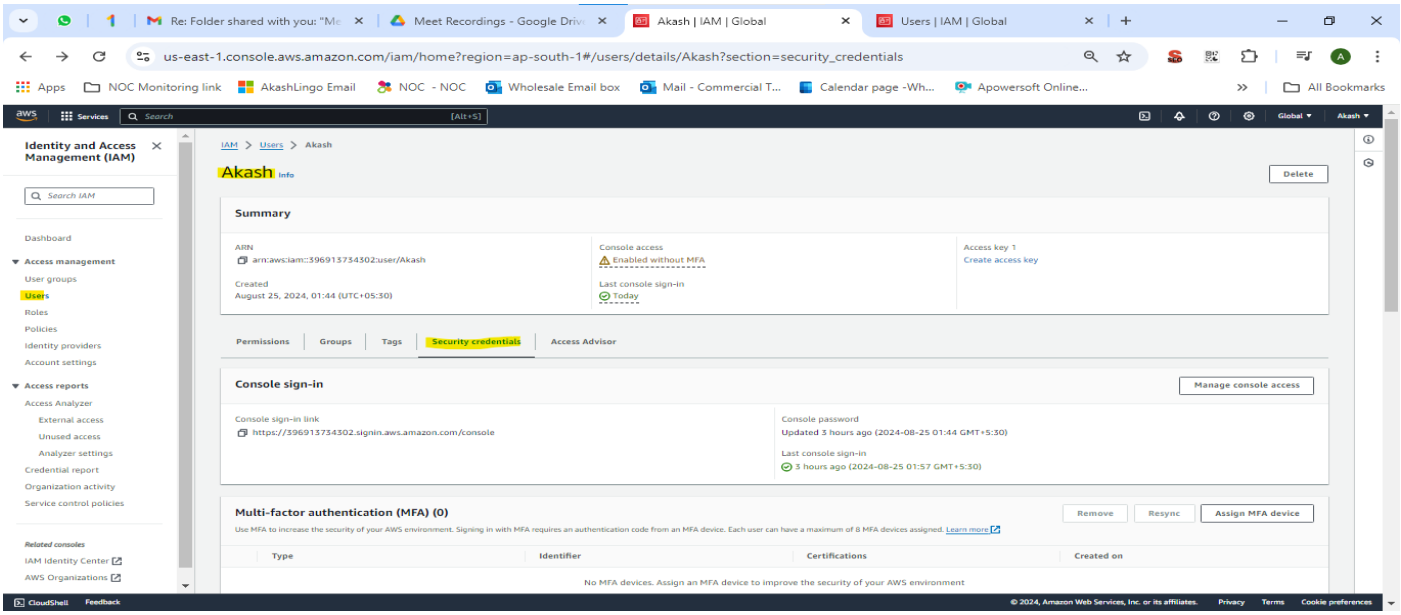
---

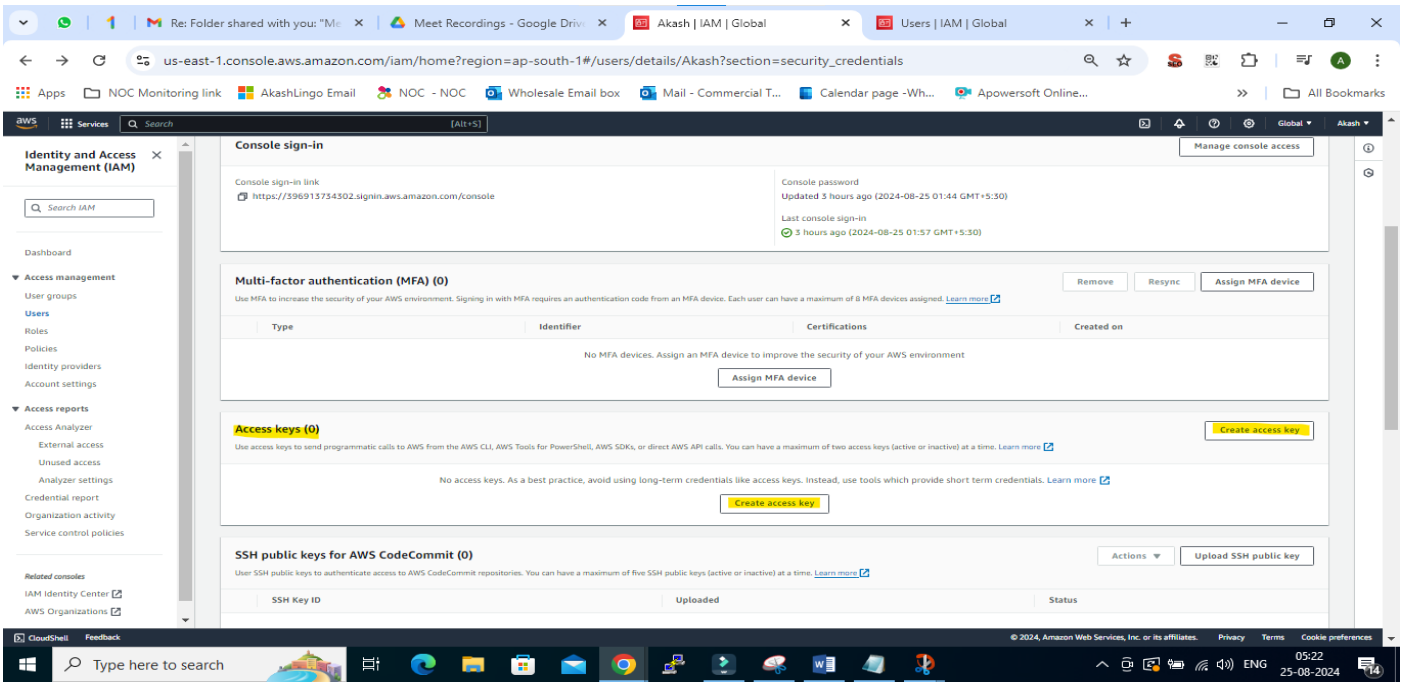
3. Individual permissions:

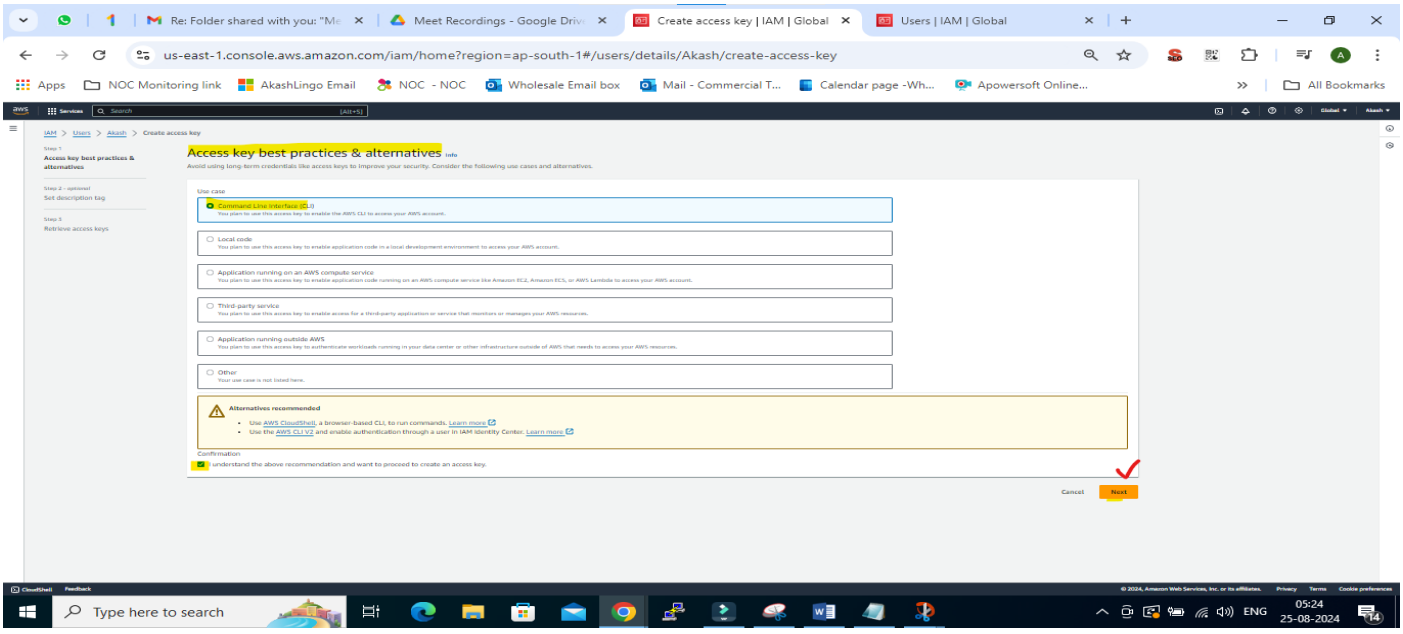


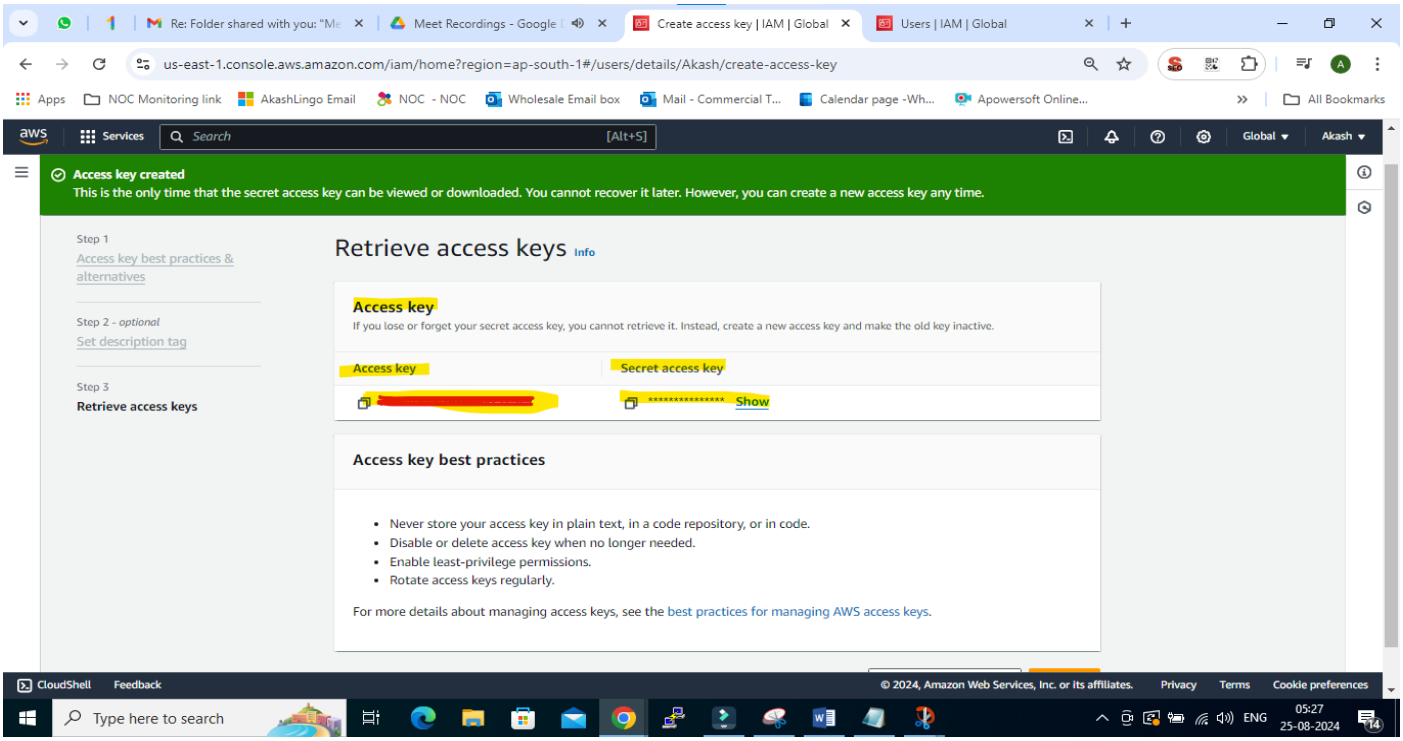


Access Key & Secret access Key:





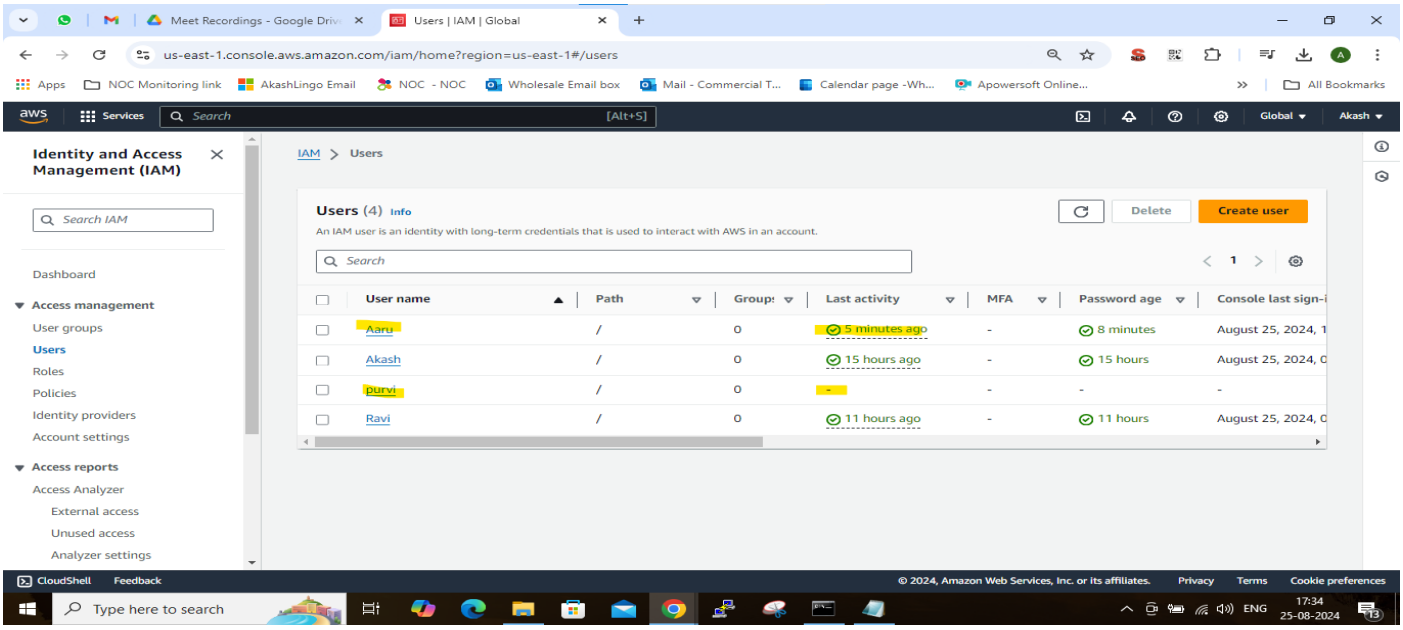




By using CLI:

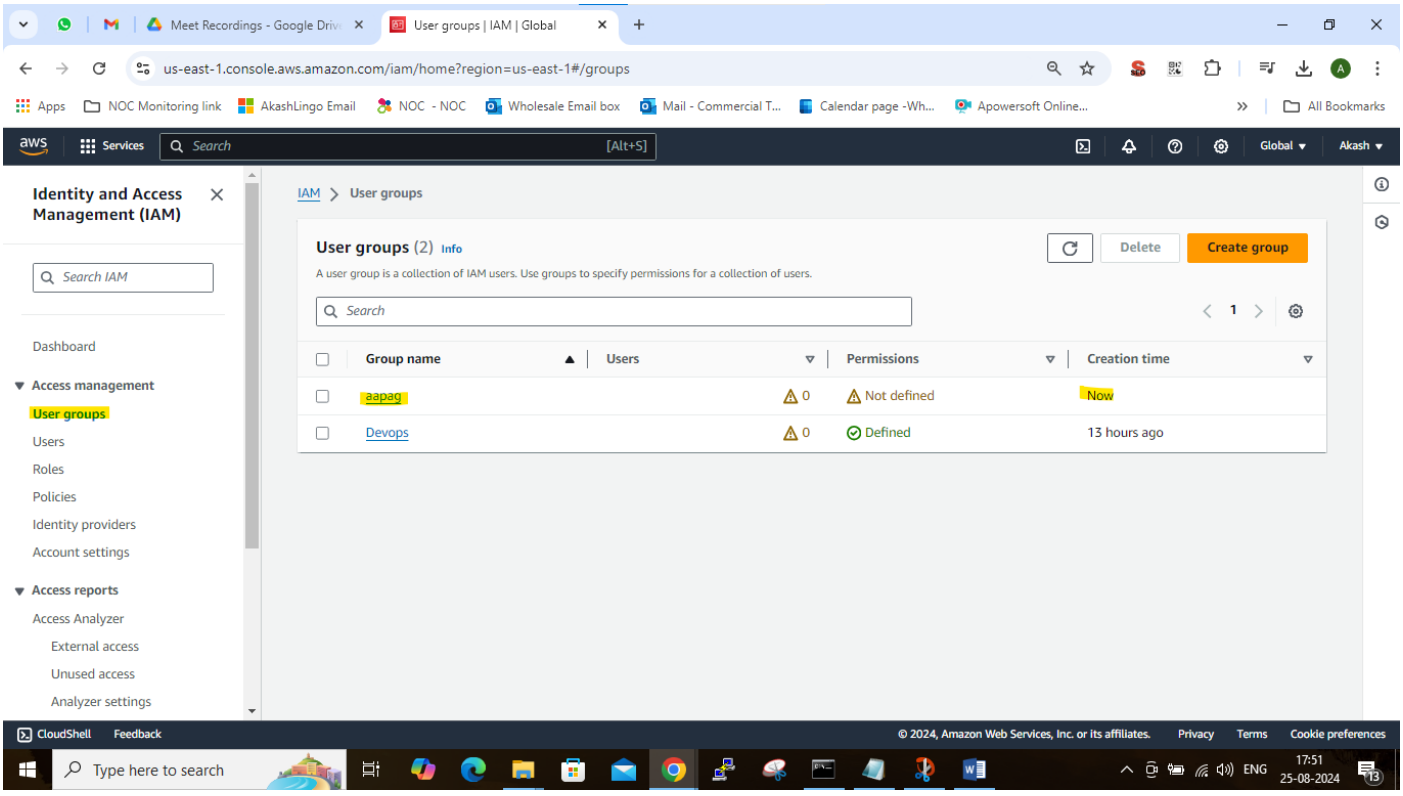
1. Create & Deleted User:

```
C:\Users\Admin>aws iam create-user --user-name purvi
{
    "User": {
        "Path": "/",
        "UserName": "purvi",
        "UserId": "AIDAVY2PG6KPPQSBKOO4Z",
        "Arn": "arn:aws:iam::396913734302:user/purvi",
        "CreateDate": "2024-08-25T12:02:50+00:00"
    }
}

C:\Users\Admin>aws iam create-user --user name purvi

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help

Unknown options: purvi

C:\Users\Admin>aws iam delete-user --user-name purvi
```



2. Create & Deleted Group:

```
Command Prompt
put-group-policy                    | put-role-permissions-boundary
put-role-policy                     | put-user-permissions-boundary
put-user-policy                     | remove-client-id-from-open-id-connect-provider
remove-role-from-instance-profile   | remove-user-from-group
reset-service-specific-credential   | resync-mfa-device
set-default-policy-version          | set-security-token-service-preferences
simulate-custom-policy              | simulate-principal-policy
tag-instance-profile                | tag-mfa-device
tag-open-id-connect-provider        | tag-policy
tag-role                            | tag-saml-provider
tag-server-certificate              | tag-user
untag-instance-profile              | untag-mfa-device
untag-open-id-connect-provider      | untag-policy
untag-role                          | untag-saml-provider
untag-server-certificate            | untag-user
update-access-key                   | update-account-password-policy
update-assume-role-policy           | update-group
update-login-profile                | update-open-id-connect-provider-thumbprint
update-role                         | update-role-description
update-saml-provider                | update-ssh-public-key
update-server-certificate           | update-service-specific-credential
update-signing-certificate          | update-user
upload-ssh-public-key               | upload-server-certificate
upload-signing-certificate          | wizard
wait                                | help


C:\Users\Admin>aws iam create-group --group-name aapag
{
    "Group": {
        "Path": "/",
        "GroupName": "aapag",
        "GroupId": "AGPAVY2PG6KPJOYAJHLZJ",
        "Arn": "arn:aws:iam::396913734302:group/aapag",
        "CreateDate": "2024-08-25T12:21:09+00:00"
    }
}


C:\Users\Admin>aws iam delete-group --group-name appag

An error occurred (NoSuchEntity) when calling the DeleteGroup operation: The group with name appag cannot be found.

C:\Users\Admin>
```



Theory – IAM (Identity Access Management)

IAM: Identity access management – User management

IMP: User, Group, Role, Policy Document

- **Login with 3 types**

1. **GUI** – URL, ID, Password
2. **CLI** – Access Key & Secret access key
3. **Terraform -**

1. Create user - Give permission to user – **Policy document** – Writhen in Jason (Java Script Object note- Key value pair) – EC2 Full access
2. Policy Document Type: 1. AWS Managed & 2. Inline Policy
3. While creating user we get ARL (Amazon Record Name) – Unique
4. Ex. **arn:aws:iam::396913734302:user/Akash**
5. Group - Give permission to Group – Policy document – Writhen in **Jason** – EC2 Full access
6. **Role**- assign Policy Document - attached with instance – a) While creating the instance b) Already created in instance

Q. Why should I learn IAM service?

IAM is used for the user management with the help of IAM we managed the entire **user management lifecycle**.

- User Management lifecycle

1. User ID Creation / User or Group Creation
2. Password creation
3. Email ID creation
4. Access Management / Policy Document