**AWS DOCUMENTATION..!**

**IDENTIFY ACCESS MANAGEMENT AND MANAGEMENT DOCUMENTATION:-**

* **IAM USER:---** IAM is the service that can be used for the create the user, group, roles,policies (group of permission). IAM is used for resource management of AWS cloud. IAM is free of cost service.
* IAM is global service
* Major four resources as follow

1. User

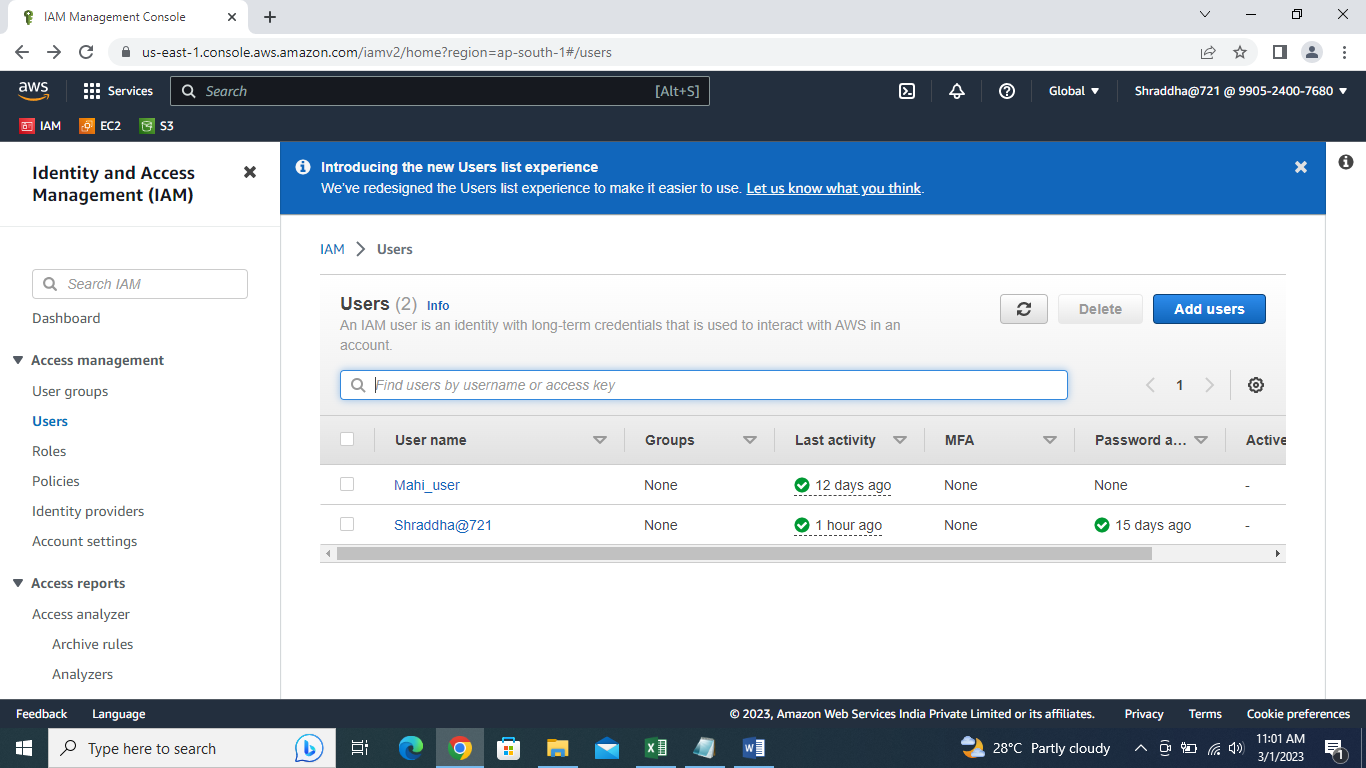
2. Group

3. Role

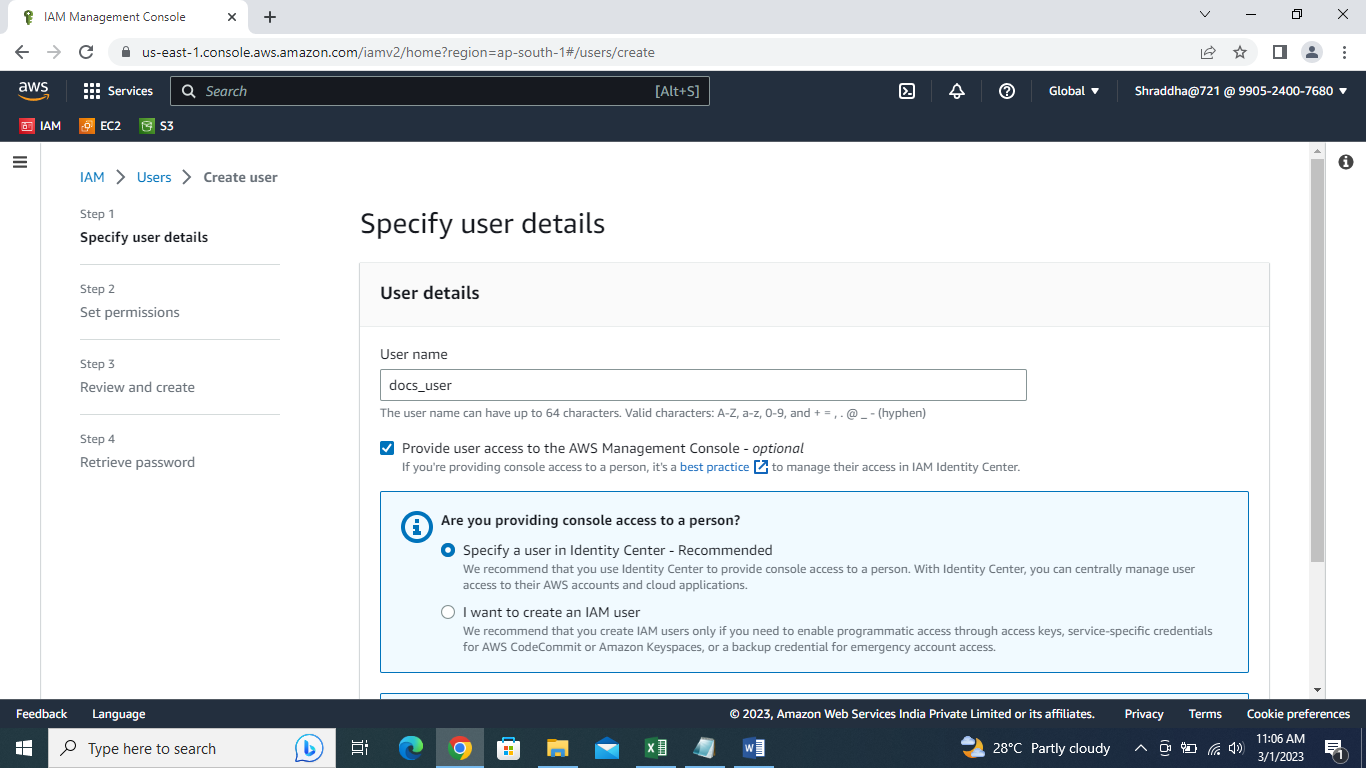
4. Policies

1. ACCESS MANAGEMENT:--
2. **Users:-** Create User.

Step 1- Go to IAM user and Select ADD USERS.

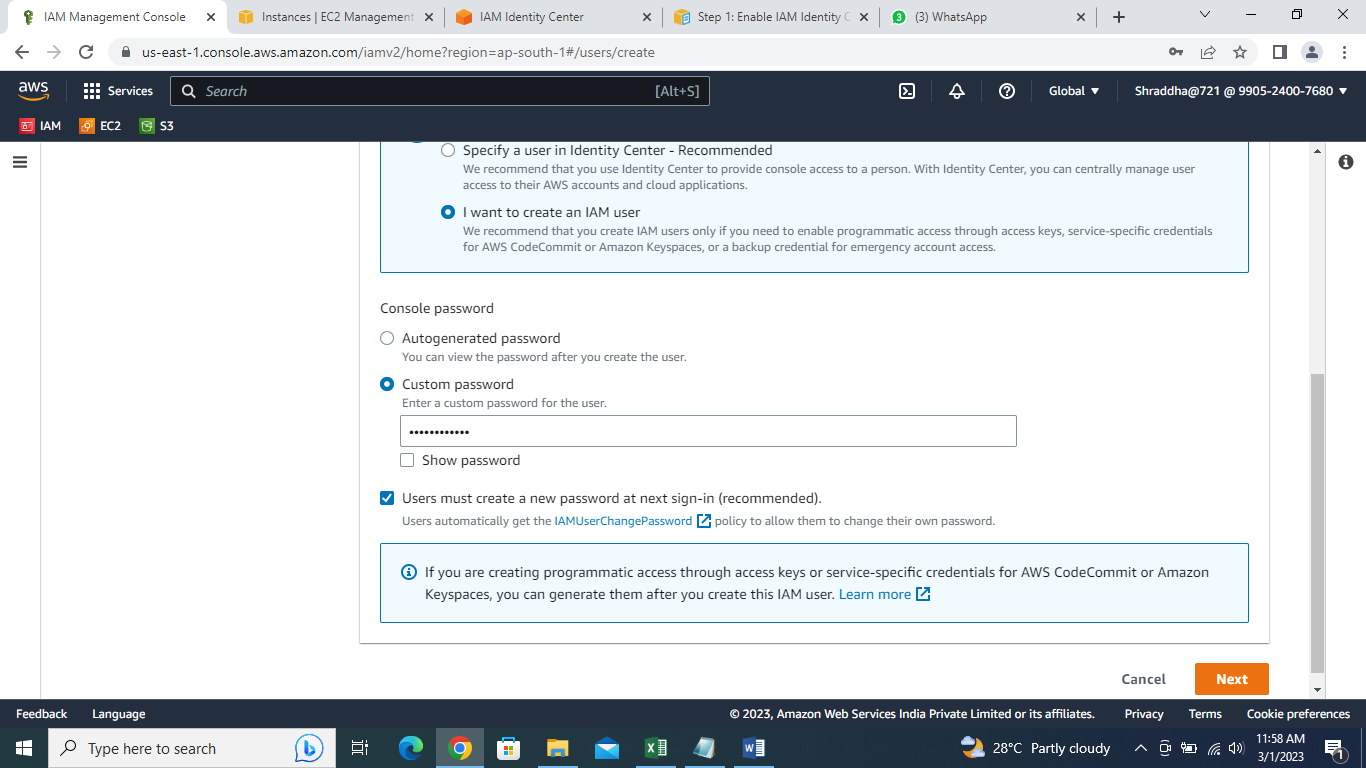


Step 2 -Specify user details. Fill all the details. Add user name.



Step 3- There are two types for creating the users.

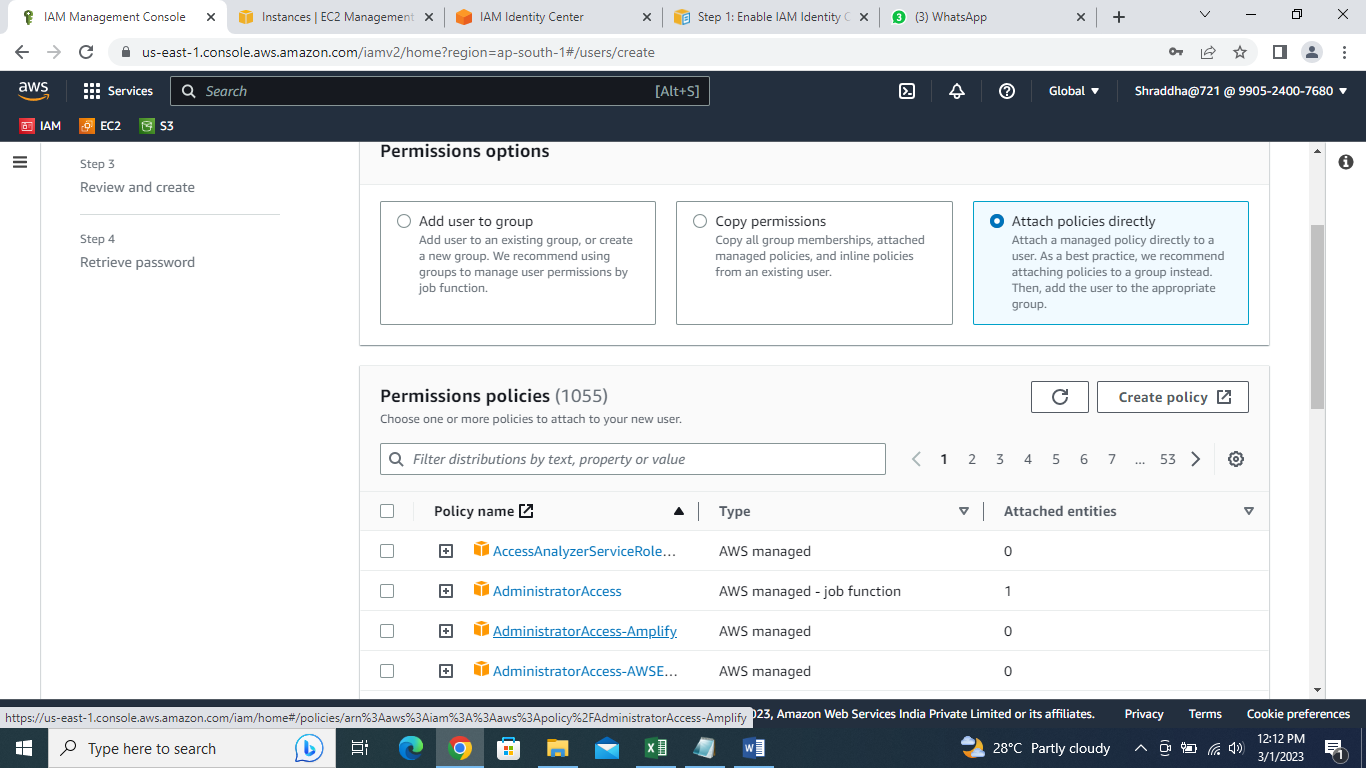
1. Consol Base :- Console base user is type of graphical base.
2. Programatic Access :- It is command line base user.
3. Console Base :- Choose console base and I want to create an IAM user after that choose custom password. ( reset password – If you select then when you log-in if you need to change password)



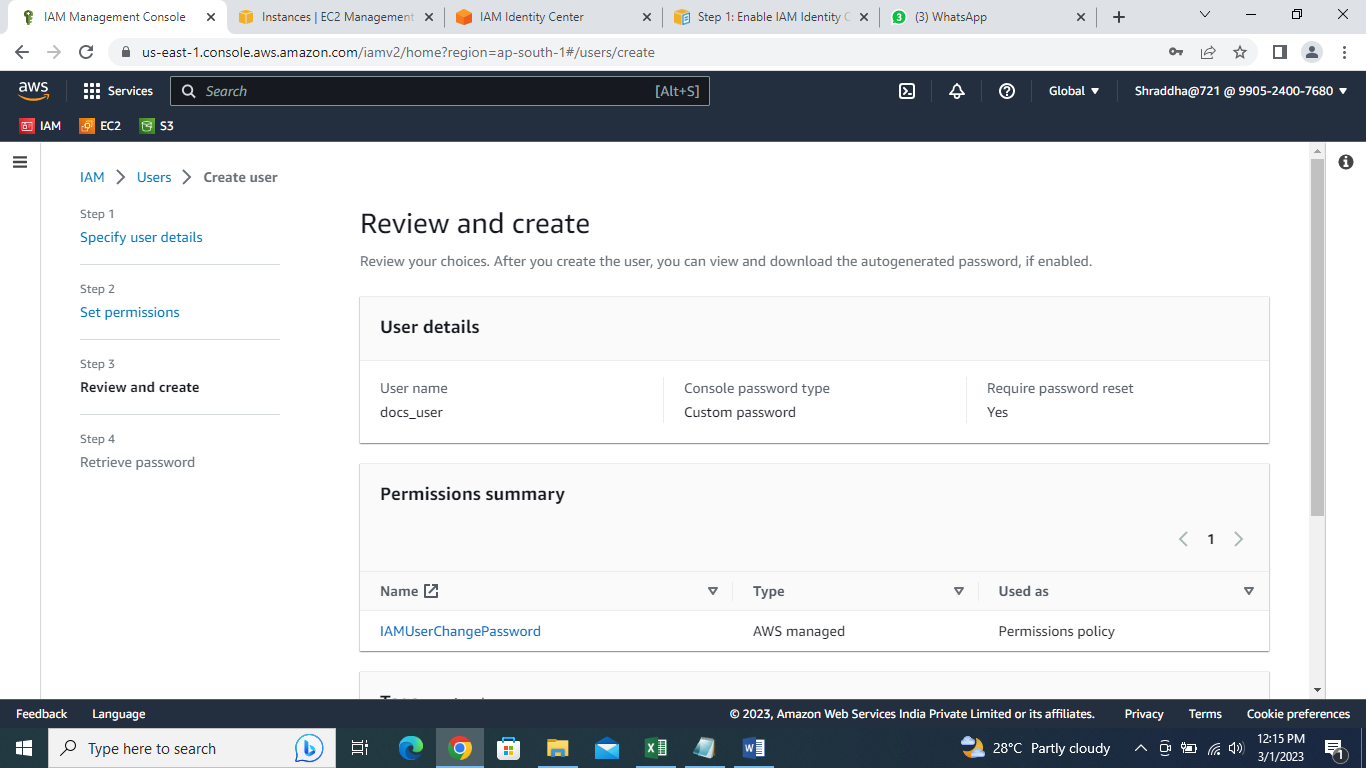
Step 4- Set Permissions **;- Policy:-** Policy is Bunch of permissions. This is types of Permissions Options.

1. Add user to group. 2) Copy permissions

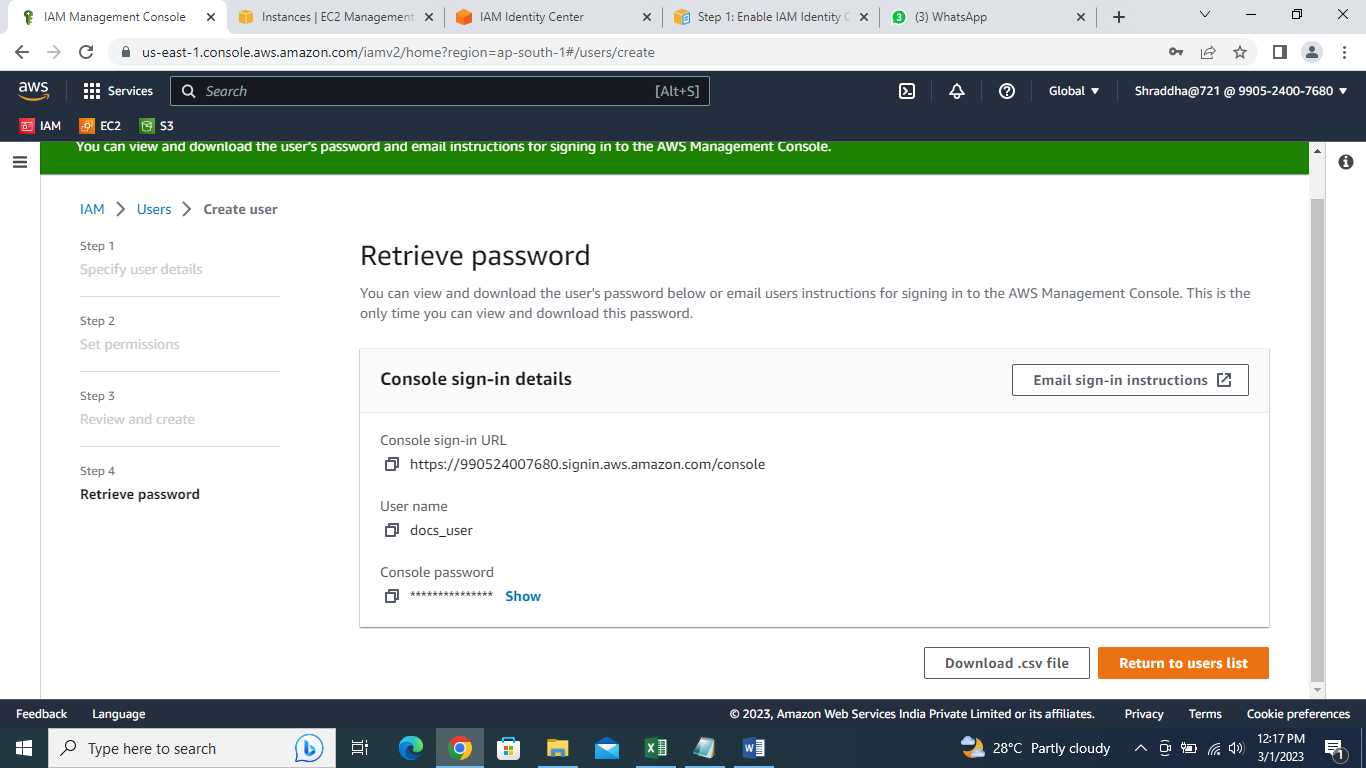
3)Attach policies directly. :- Choose any policy Which we need.



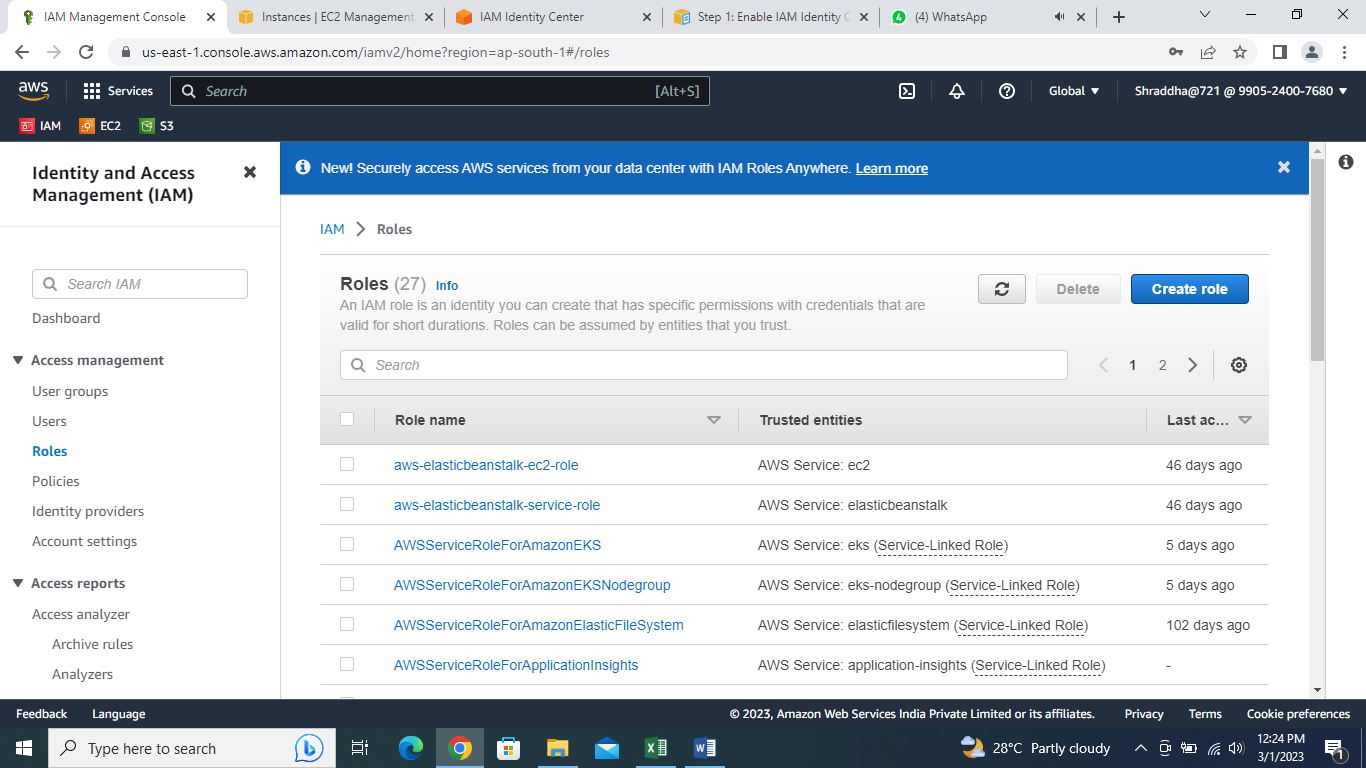
Step 5- Review and create :-

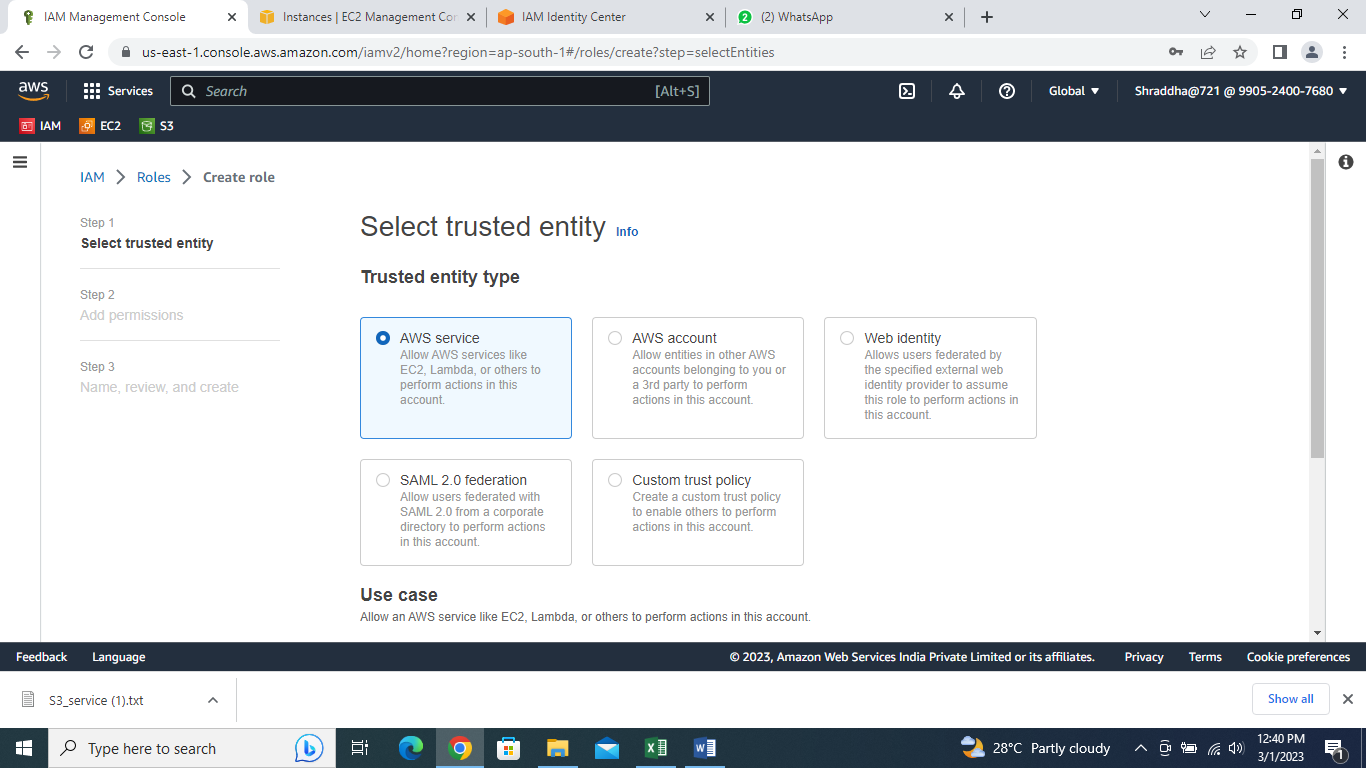


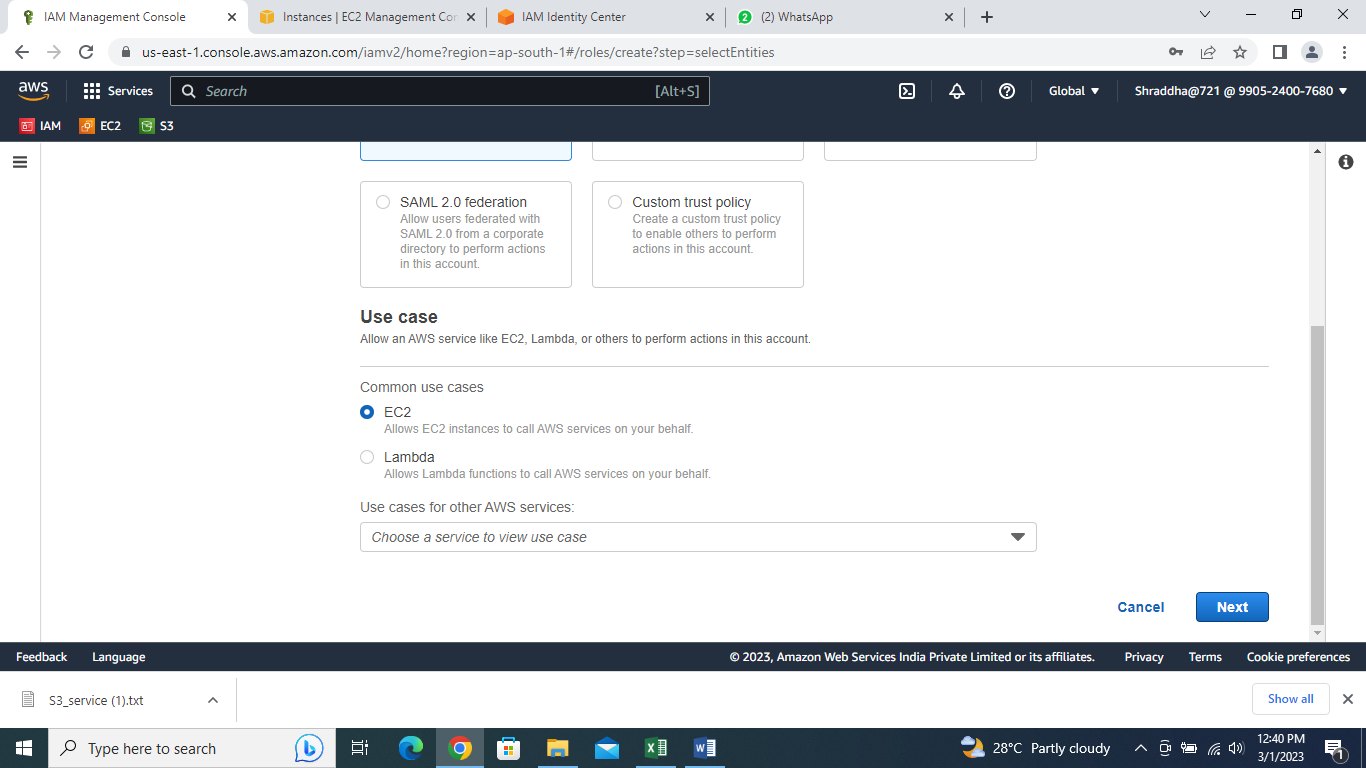
Step 6- Retreive Password:- download.csv file. And return to users list.

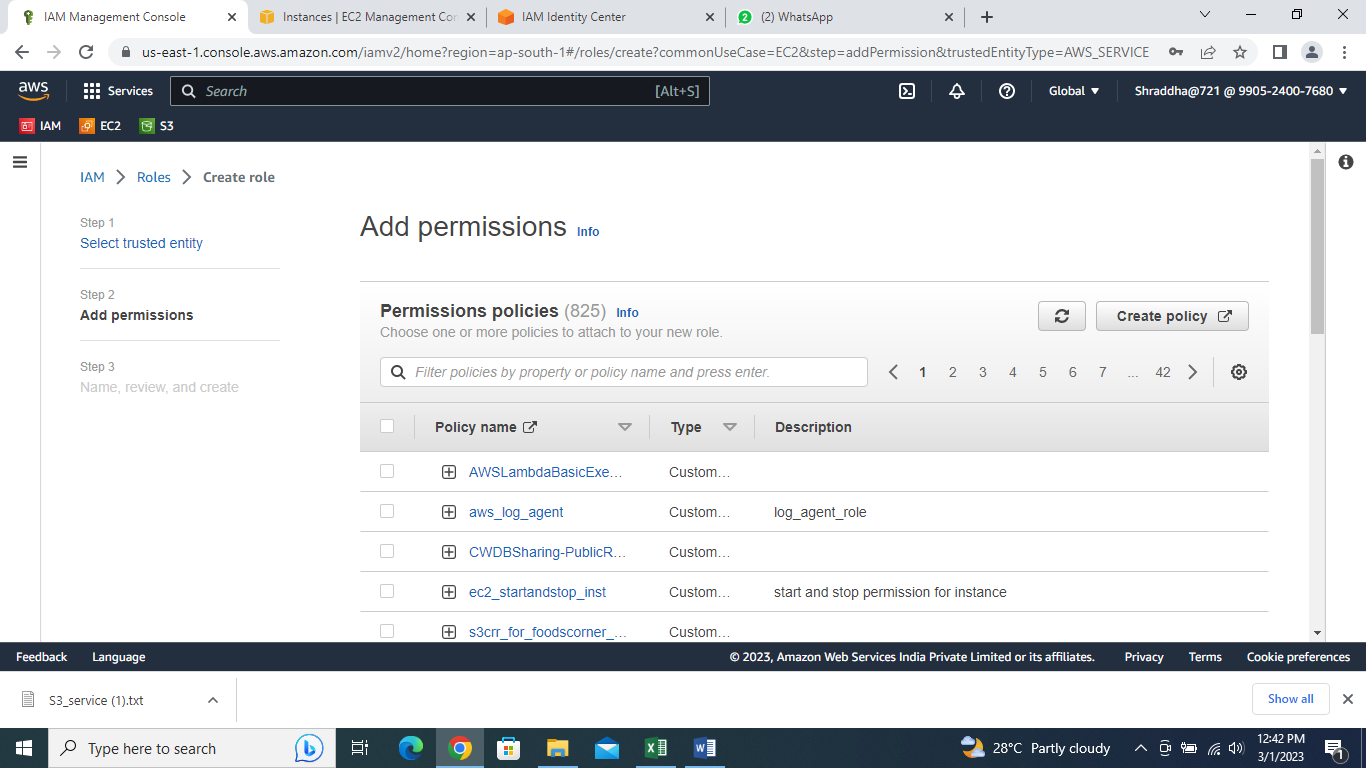


1. **ROLES** :- Roles is used for to give the permission to other services or the resources. It is not applied to the user. If You applied roles to the service you can access the other services or resource of applied service.

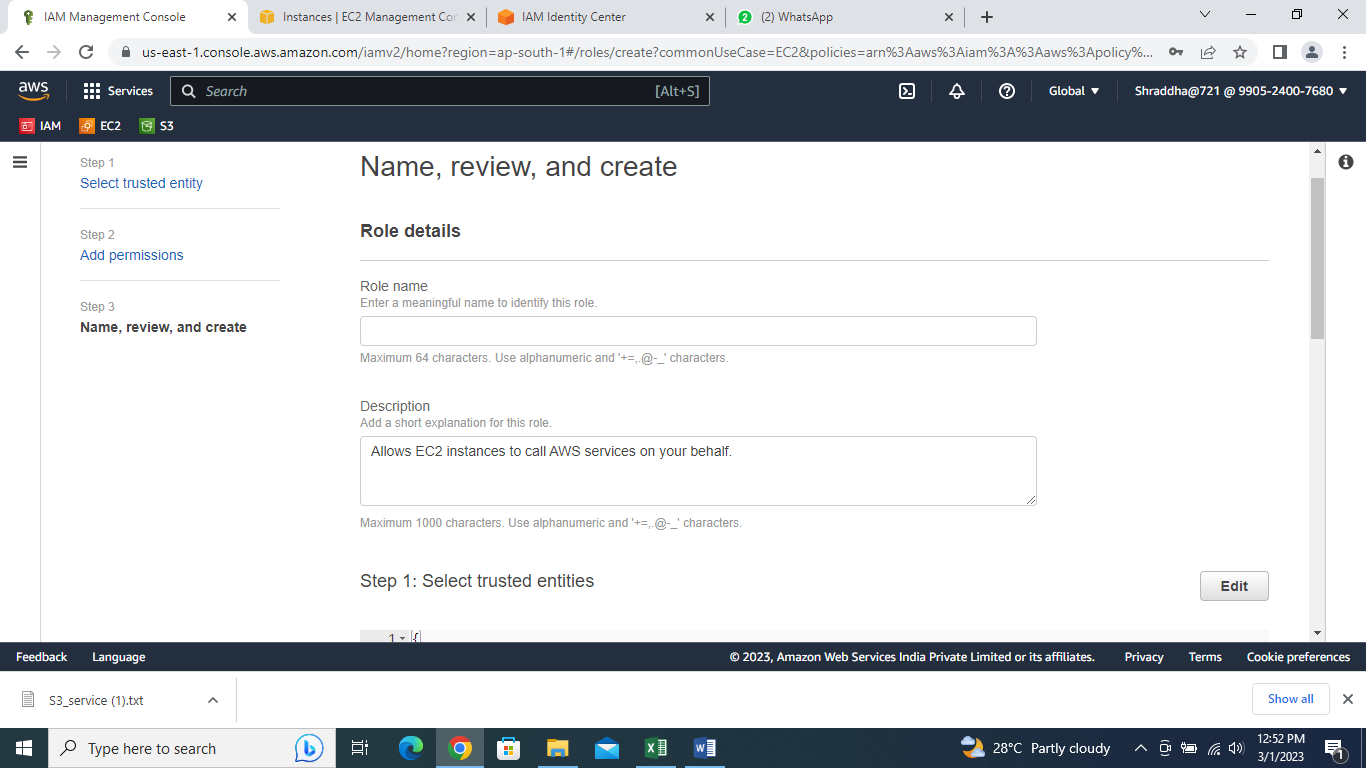
Step 1- **Create Role** :- Select Create role.

Step 2- Select trusted entity. After That use EC2.  




Step 3- Add Permissions :- Choose one or more policies to attach to your new role. 

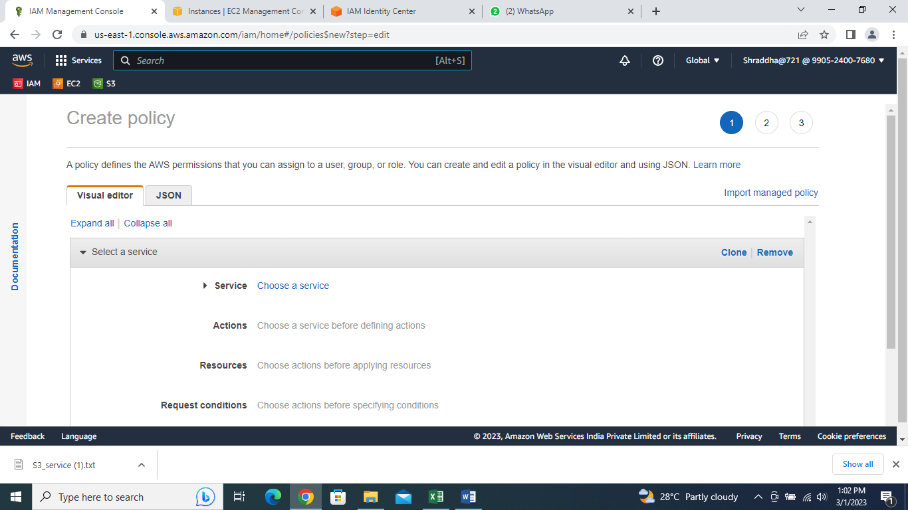
Step 4- Role Details:- Give name to the role. And create role.



1. POLICIES :- Policies is the group of permissions give to userto access the service (without policies user cannot allow to access the service).

Select Create Policy. Then creating policies have two types; 1) visual editor. 2) json (by the use of coding).

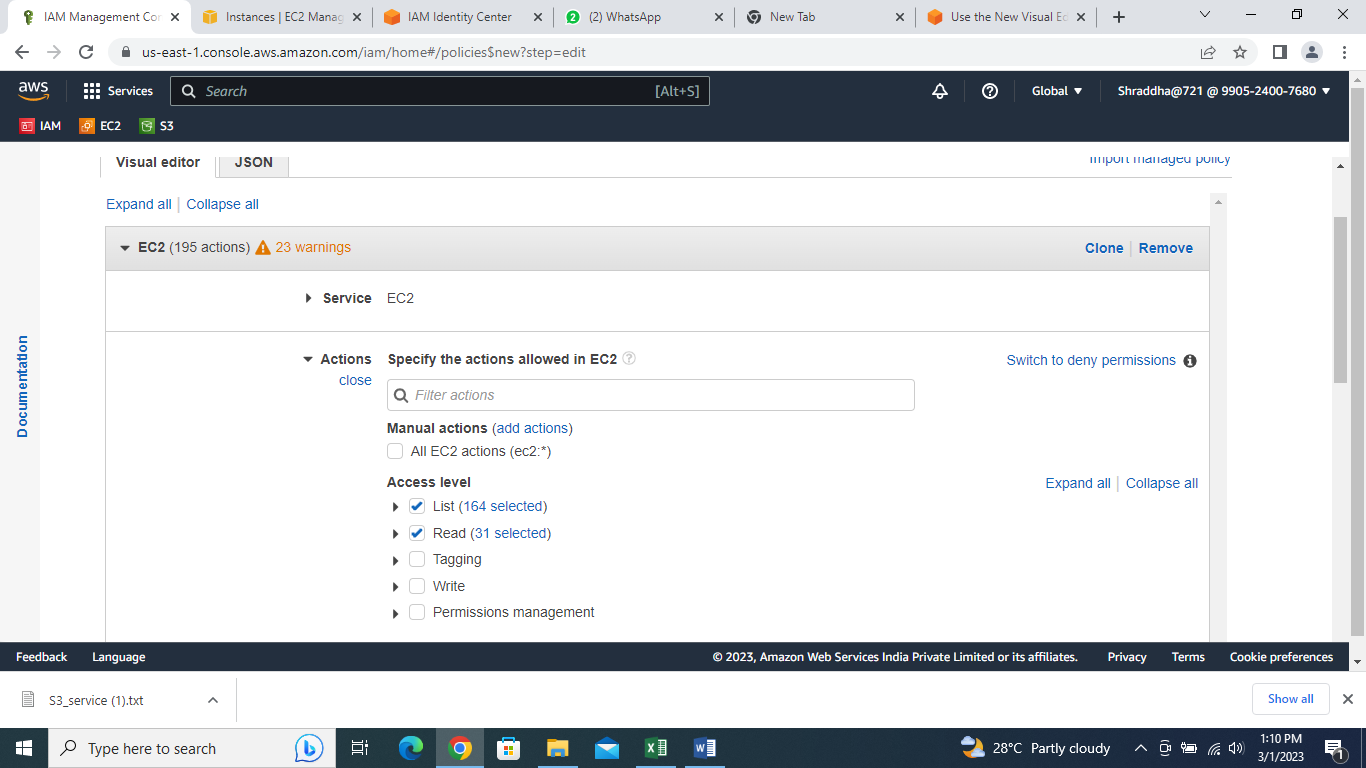
# Visual Editor:-  Create and Modify Your AWS IAM Policies

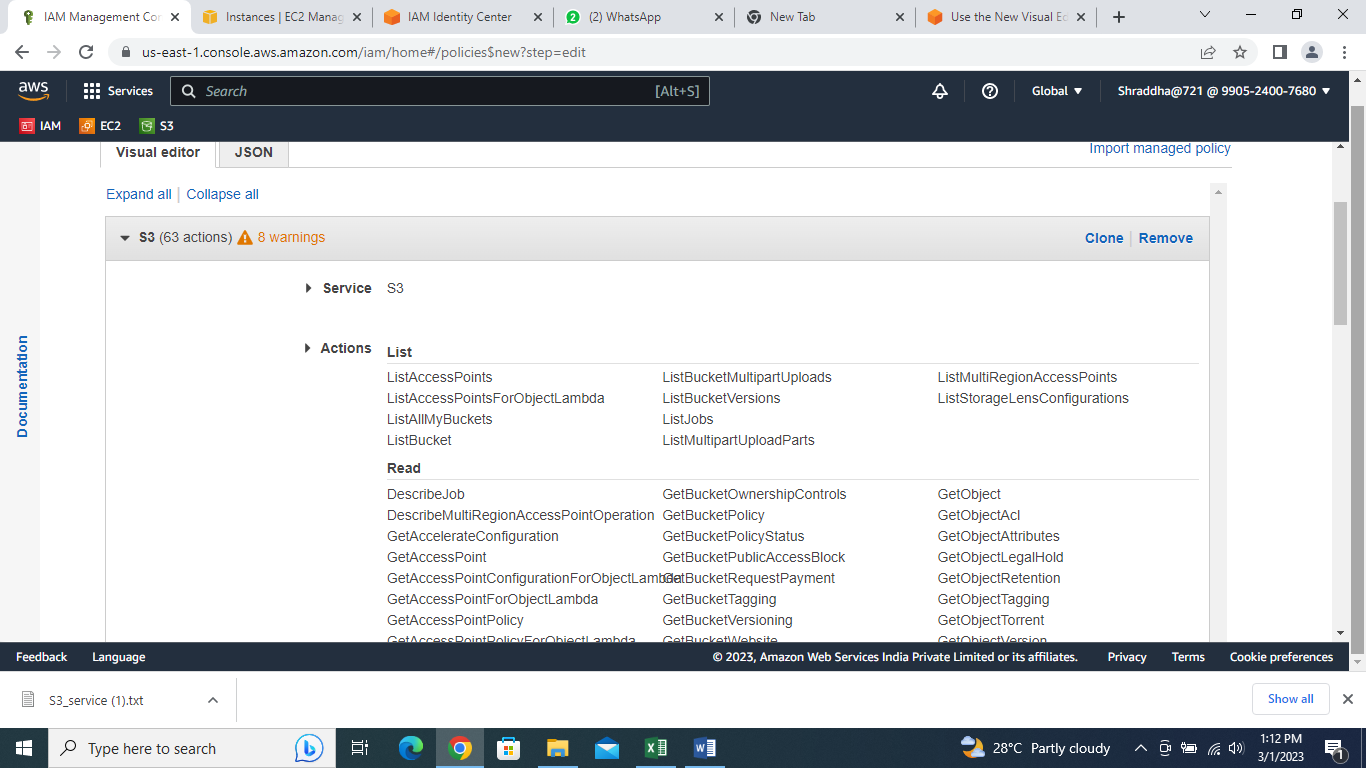


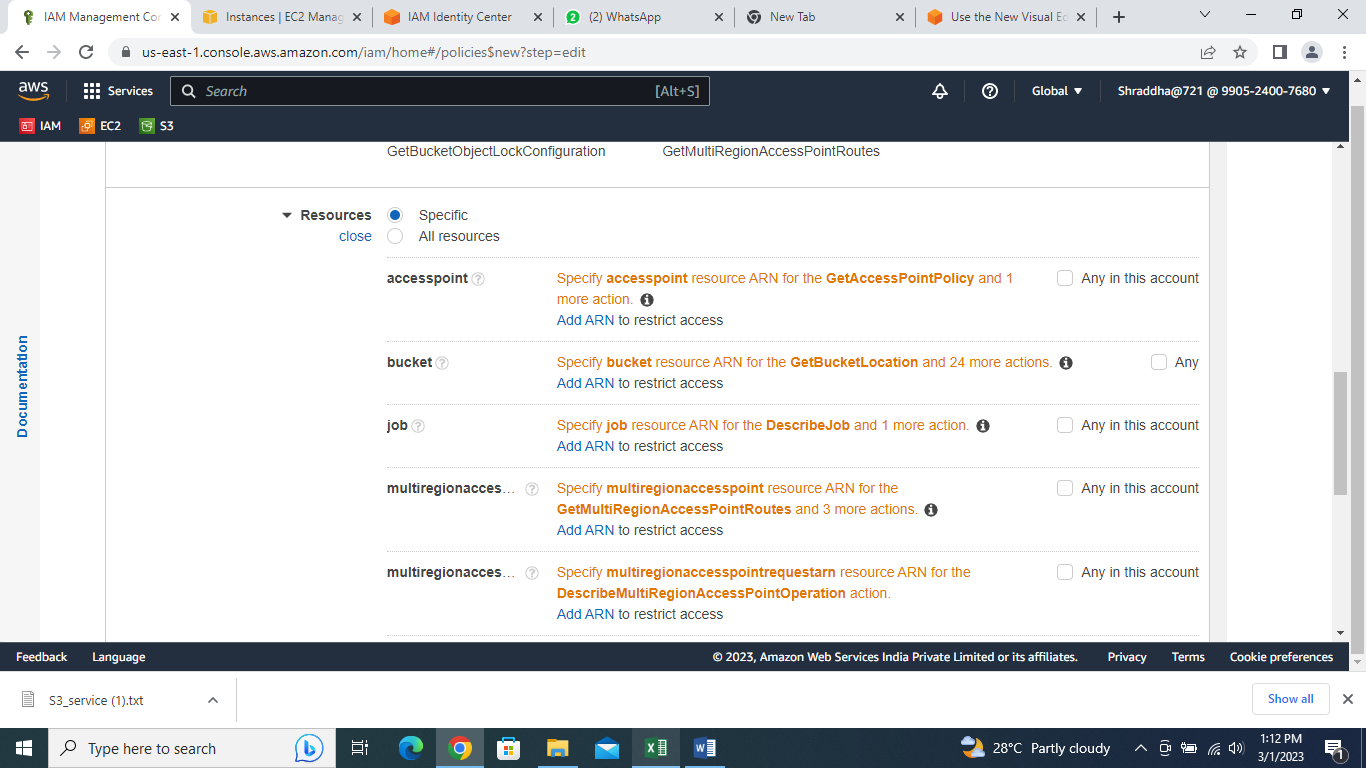
Step 1- Services :- Select the type of policy as per requirement.

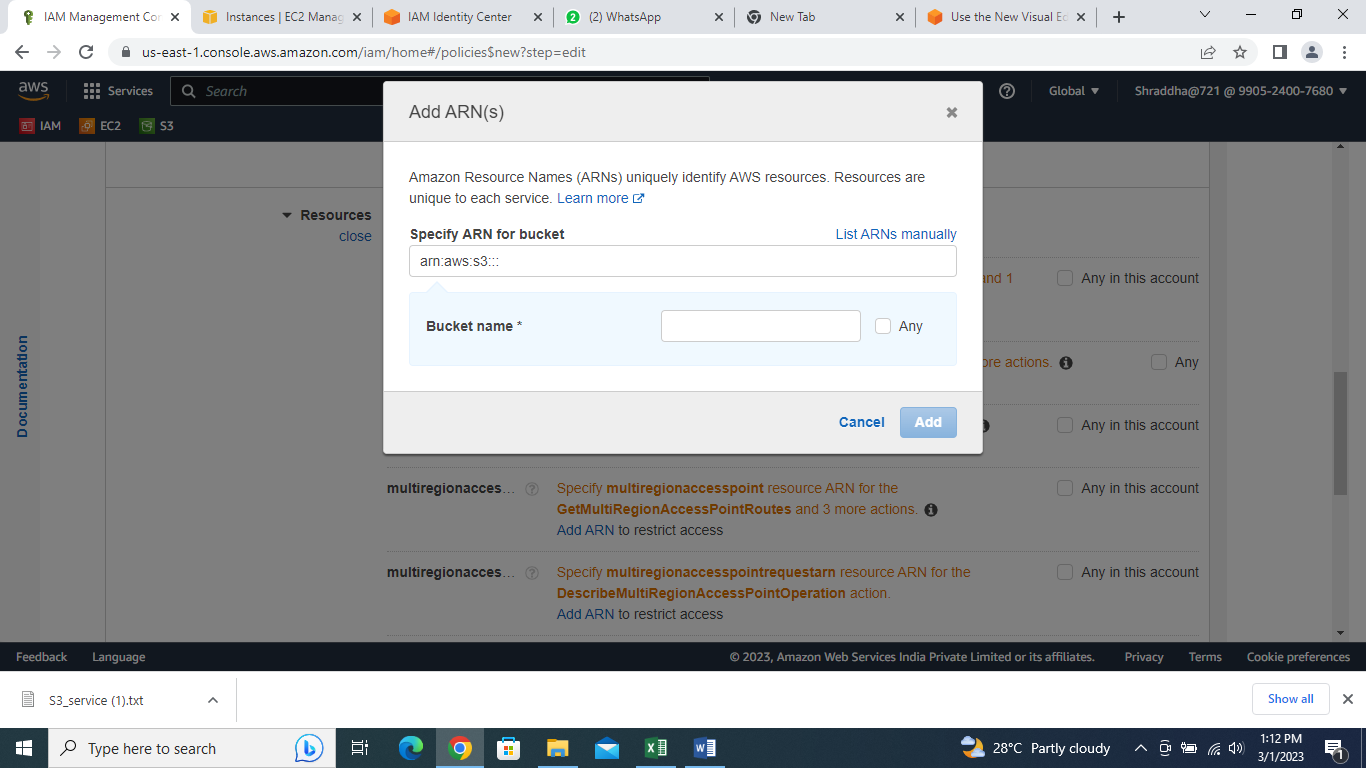
Actions:- Choose Access level.

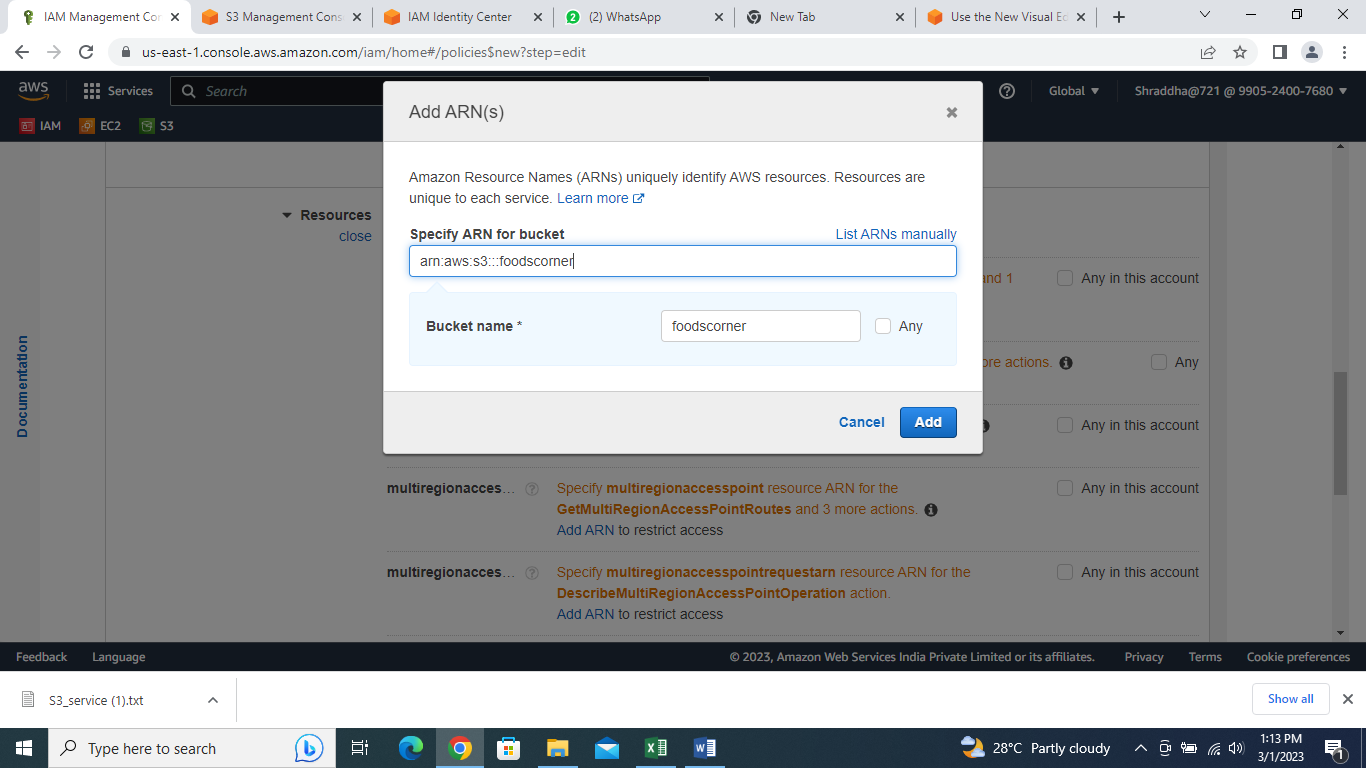
Resources:- Choose Bucket—ARN ( Copy Bucket ARN).





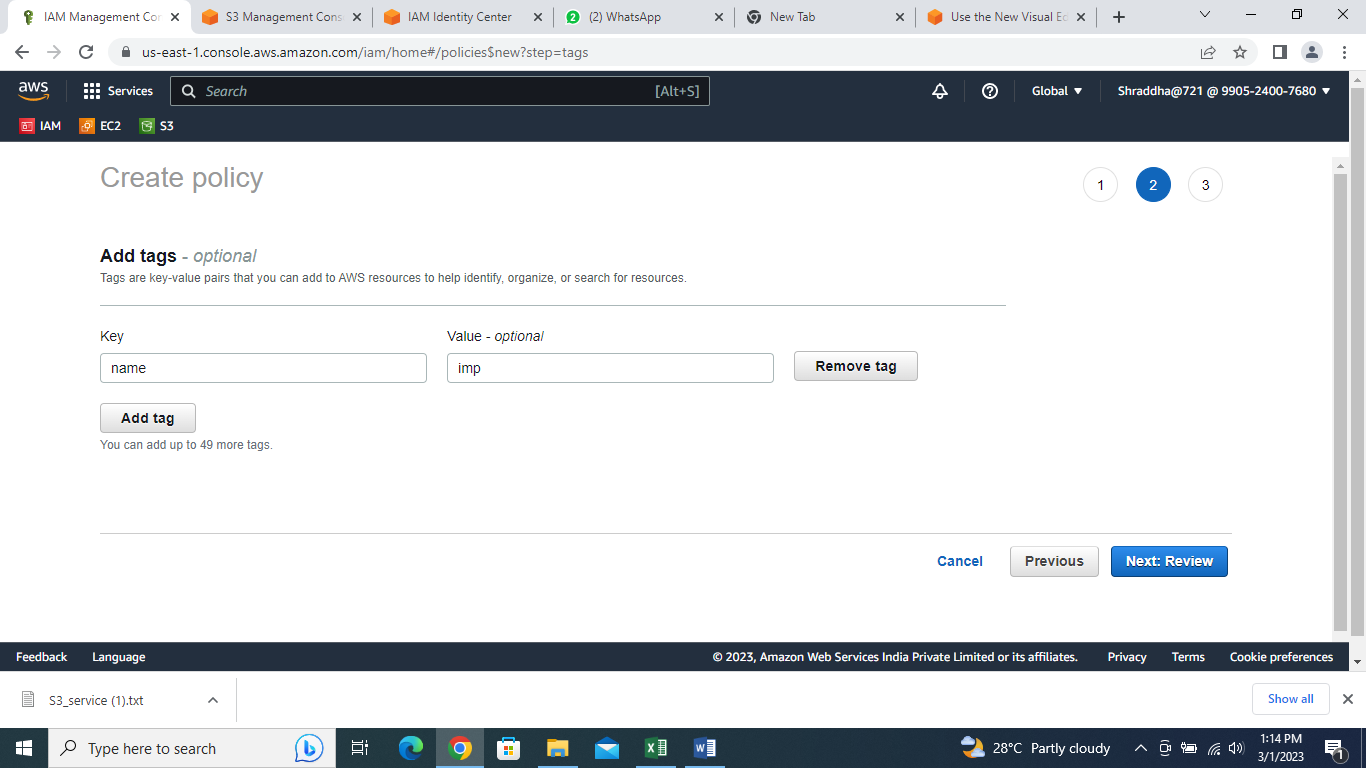


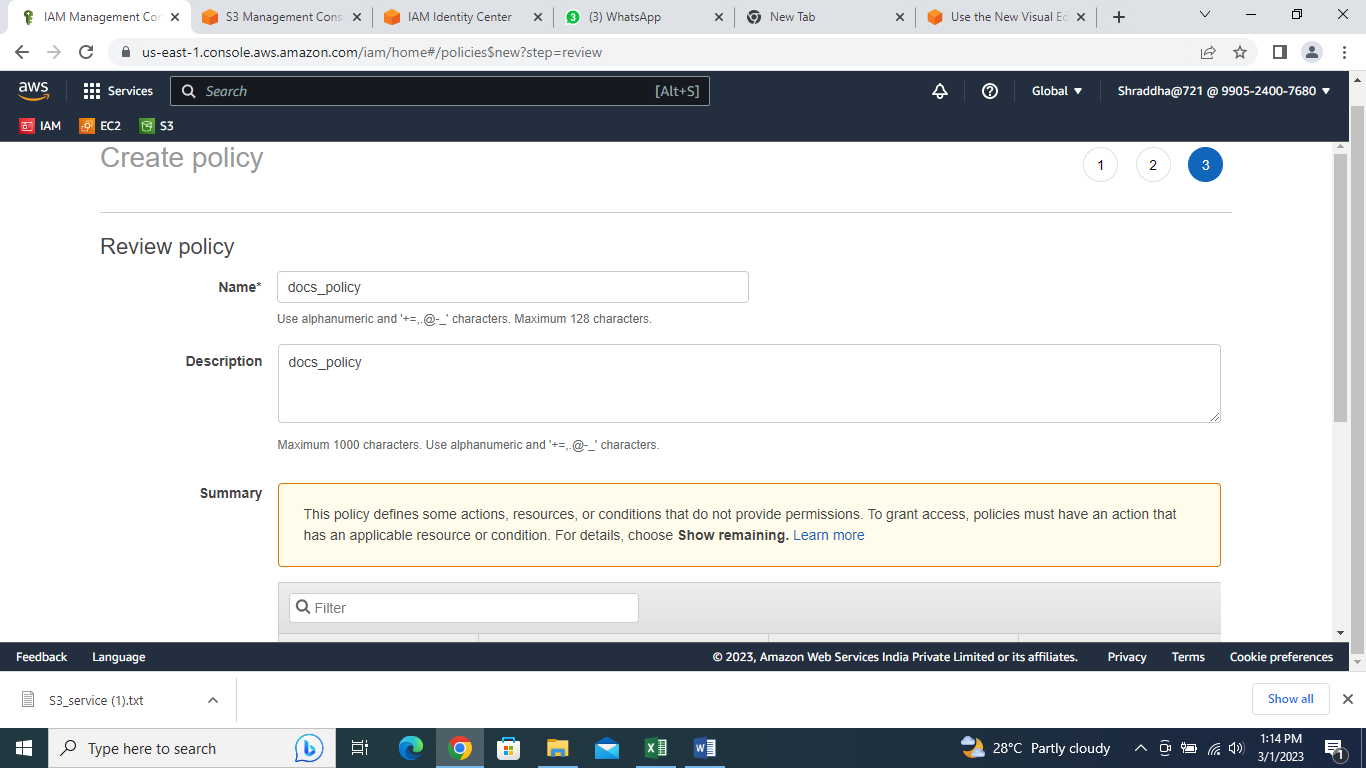




Step 2 – Create Policy :- Add tags.

Step 3- Create Policy:- Review policy. Give name to the policy. Policy is created.





**INTERVIEW QEUSTIONS OF AWS IAM :---**

Q) Which are the key features of AWS IAM?

Access control to AWS resources Multi-factor authentication (MFA) Federated access Analytics.

Q) Explain AWS IAM Policies.

IAM Policies are how you determine who has access to what resources in your account. For example, you could allow users access to all Amazon EC2 instances within your AWS account, or just a specified instance.

Q) What is the IAM Hierarchy of Privileges?

IAM user , Root user,User with temporary credentials.

What are the features of AWS IAM?

There are many features of AWS IAM few of them would be:

Q) Identity federation.

Secure Access to AWS resources for applications that run on Amazon EC2,

Granular permisions,

Multi-factor authentication (MFA),

Integrated with many AWS services,

Free to use.

Q) What is the importance of IAM?

With an increase in security threats and user privacy preferences turning more difficult to handle, IAM has started to play a crucial role for organizations, irrespective of the industry and size. IAM is vital at a time when passwords get hacked within seconds, data breaches turn a frequent occurrence and intruders infiltrate government as well as organizational agencies.

Q) What are the different identities provided by IAM?

IAM Users is a resource in IAM that has associated credentials and permissions.IAM Roles is an IAM identity that you can create in your account that has specific permissions.

Q) What are the key capabilities provided by AWS IAM?

Access control to AWS resources,

Multi-factor authentication (MFA),

Federated access,

Analytics.

Q) Why do we need MFA?

Answer:

Multi-factor authentication is an important security measure that adds an extra layer of protection to your account. By requiring more than one form of authentication, it makes it more difficult for someone to gain unauthorized access to your account. MFA can help protect your account from threats like phishing and password guessing, and can also help you comply with regulatory requirements.

Q) Why we use IAM ?

Identity and access management (IAM) ensures that the right people and job roles in your organization (identities) can access the tools they need to do their jobs. Identity management and access systems enable your organization to manage employee apps without logging into each app as an administrator.

Q) Why do we need IAM role in AWS?

You should use IAM roles to grant access to your AWS accounts by relying on short-term credentials, a security best practice. Authorized identities, which can be AWS services or users from your identity provider, can assume roles to make AWS requests.