AWS IAM - Identity Access Management and Top 20 Interview Question

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources.

With IAM, you can centrally manage permissions that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

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

AWS strongly recommend that you don't use the root user for your everyday tasks.

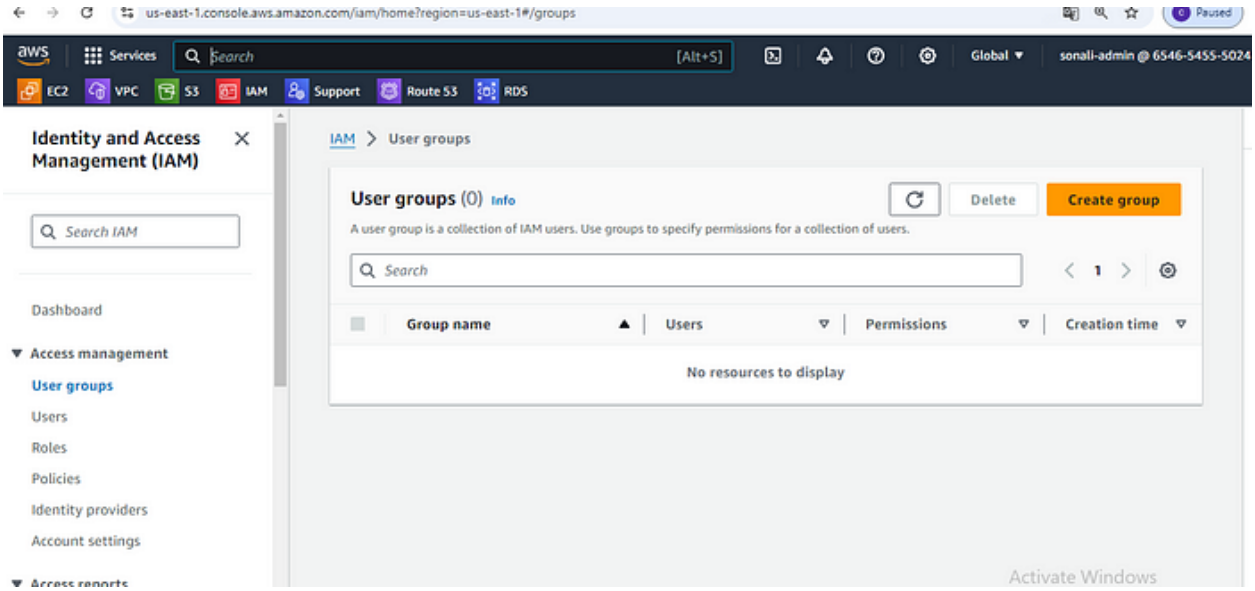
Safeguard your root user credentials and use them to perform the tasks that only the root user can perform.
User are people within your organization and it can be group.

Groups only contain users not other group.

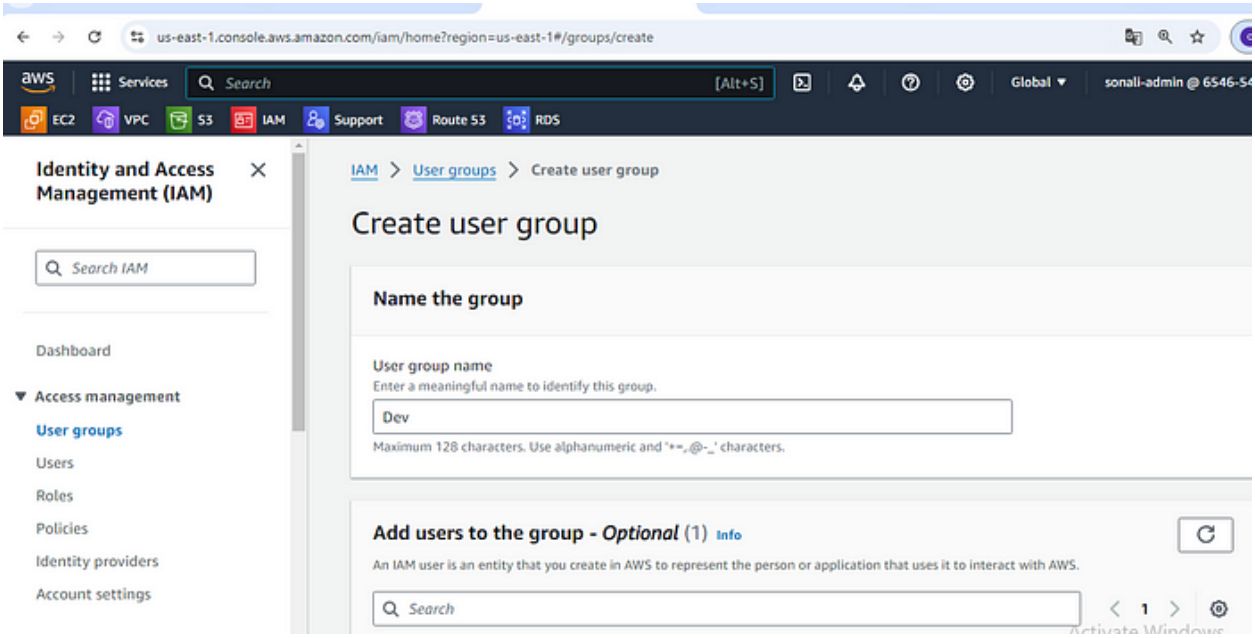
Users don’t belongs to the one group it can belongs to multiple group

User group:-

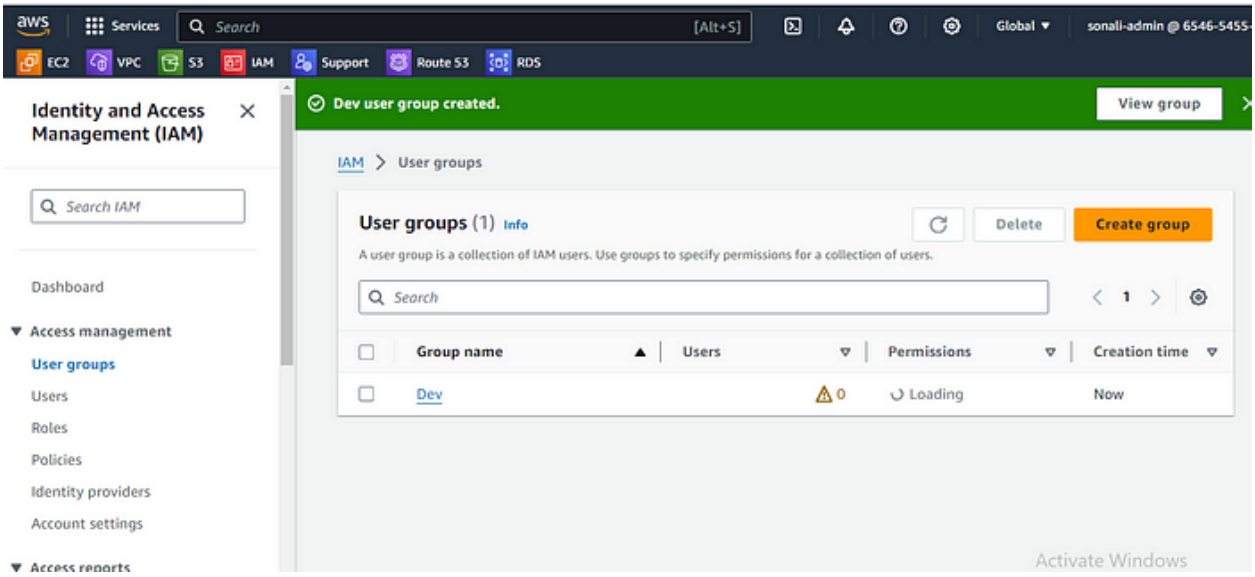
IAM group help you to give similar permission to set of users. suppose you have 100 Employee in your Company and you have to give similar set of permission to that 100 Employee. At that time you can all 100 Employee in single group and give the permission to that group. To create group follow the below step.



Step 1: Click on User group and then create group



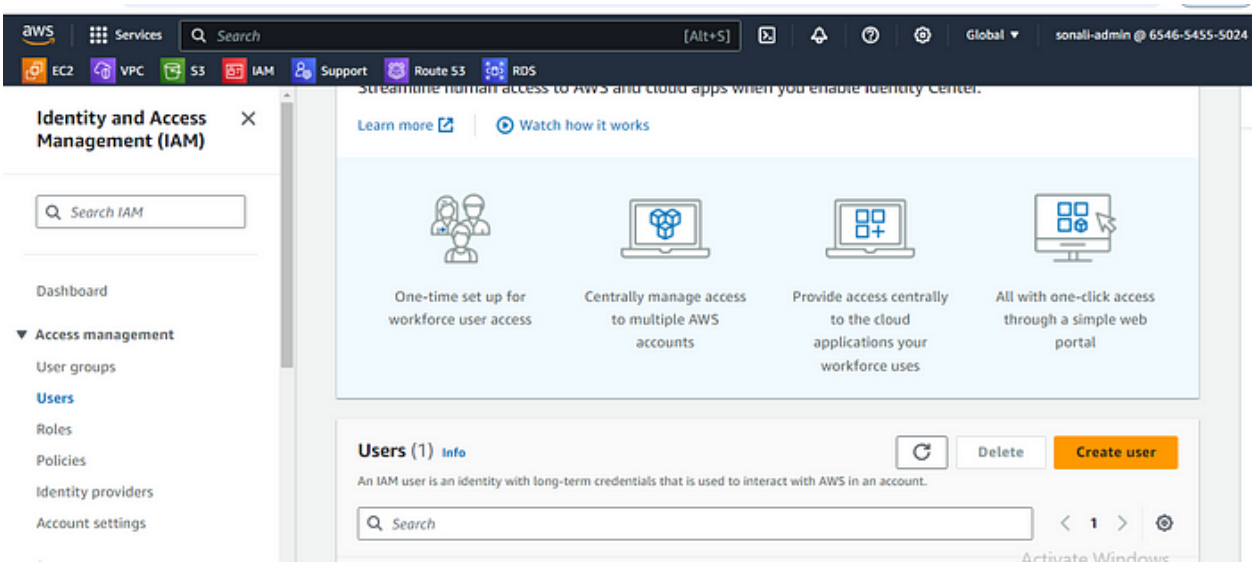
Step 2: Give the name to that group. If your user is already created then you can add directly. otherwise assign the policies to group while creating the group. And click on create user group.



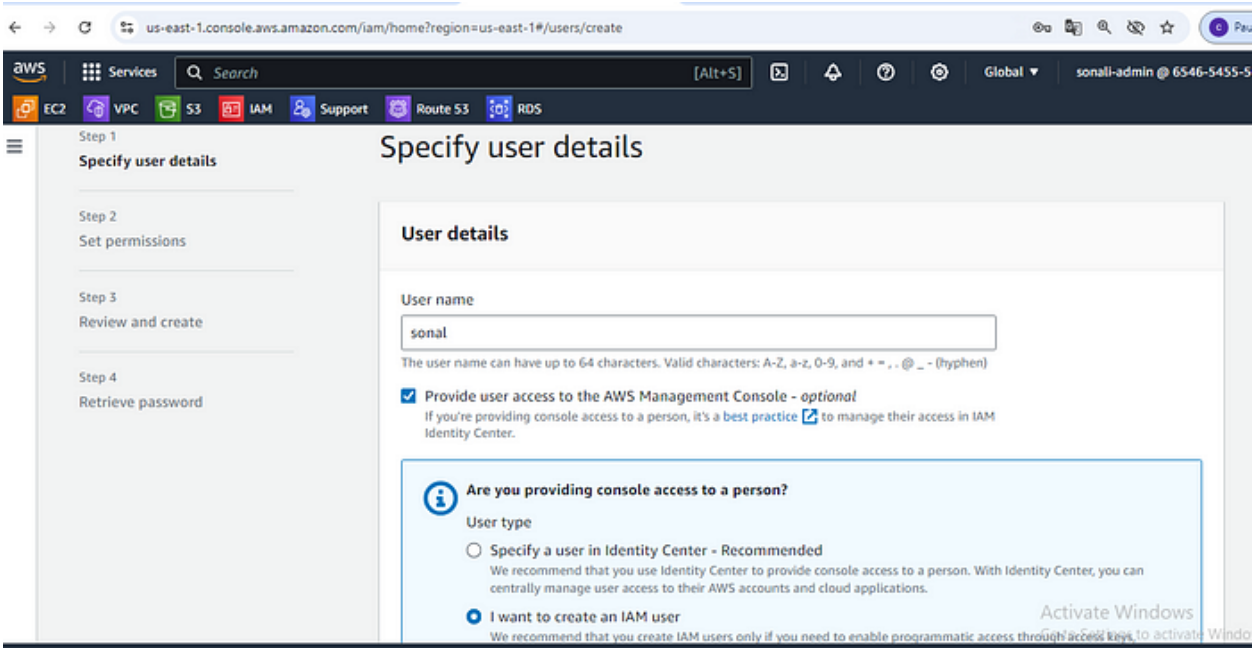
IAM User:-

An IAM user is an entity that you create in AWS. The IAM user represents the person or service who uses the IAM user to interact with AWS. To create IAM user follow the below steps.

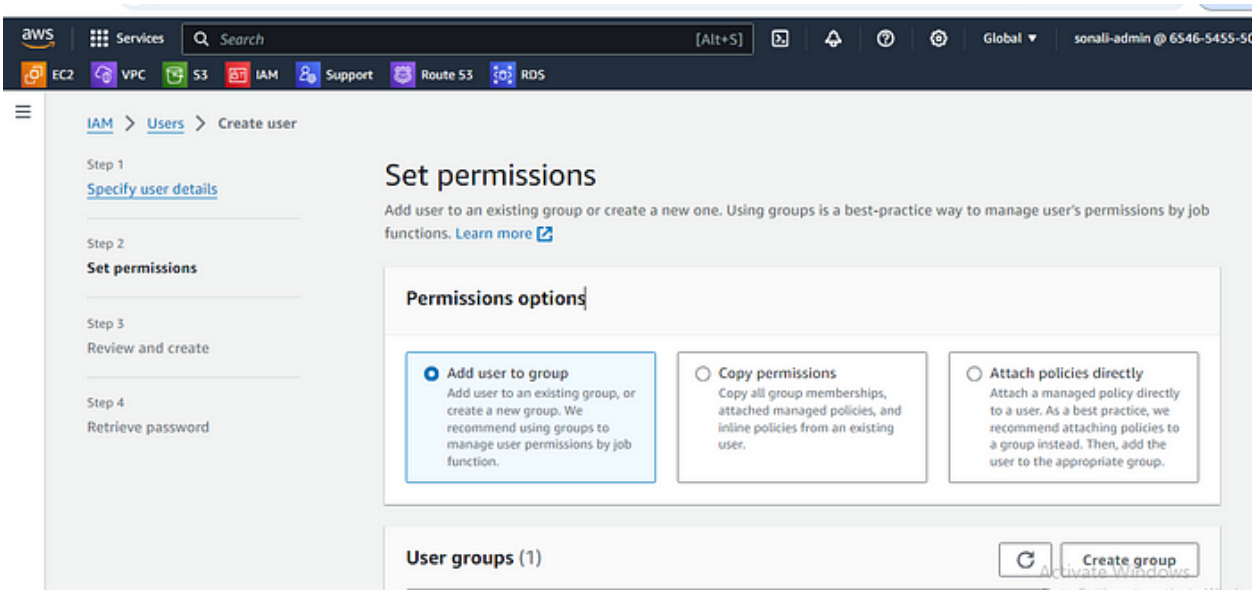
Step 1: Go to the IAM service. Access management tab is there. Click on users and the create user



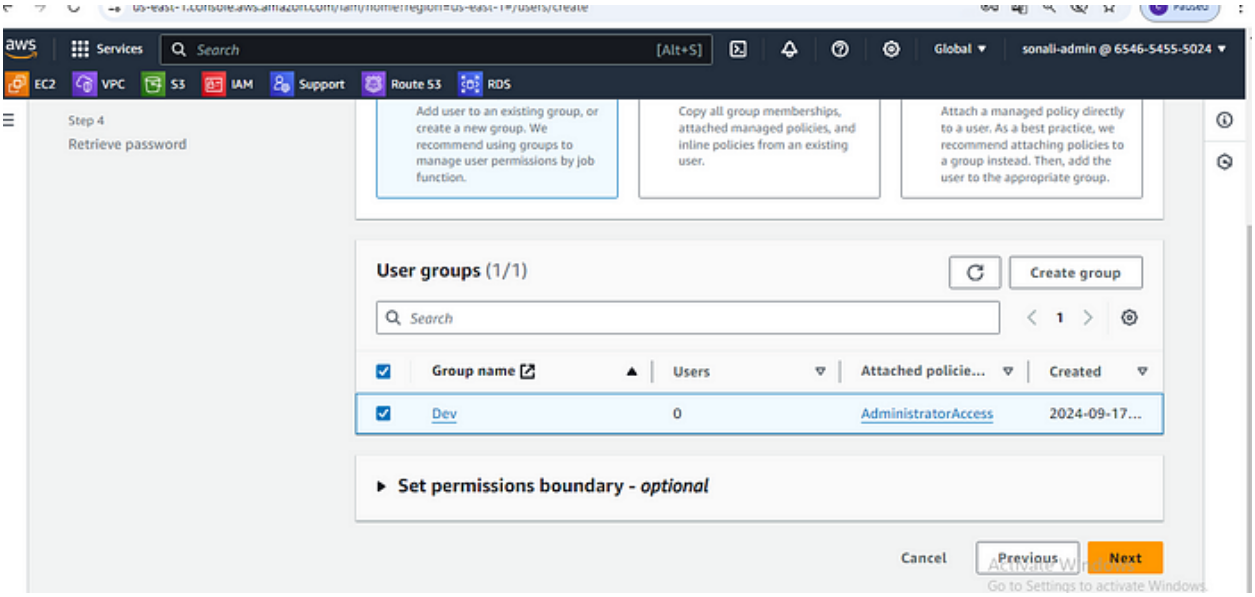
Step 2: Give User name. And Provide user access to the AWS Management Console. Click on option ‘I want to create an IAM user’ And then click on custom password and give the password. Click on next.



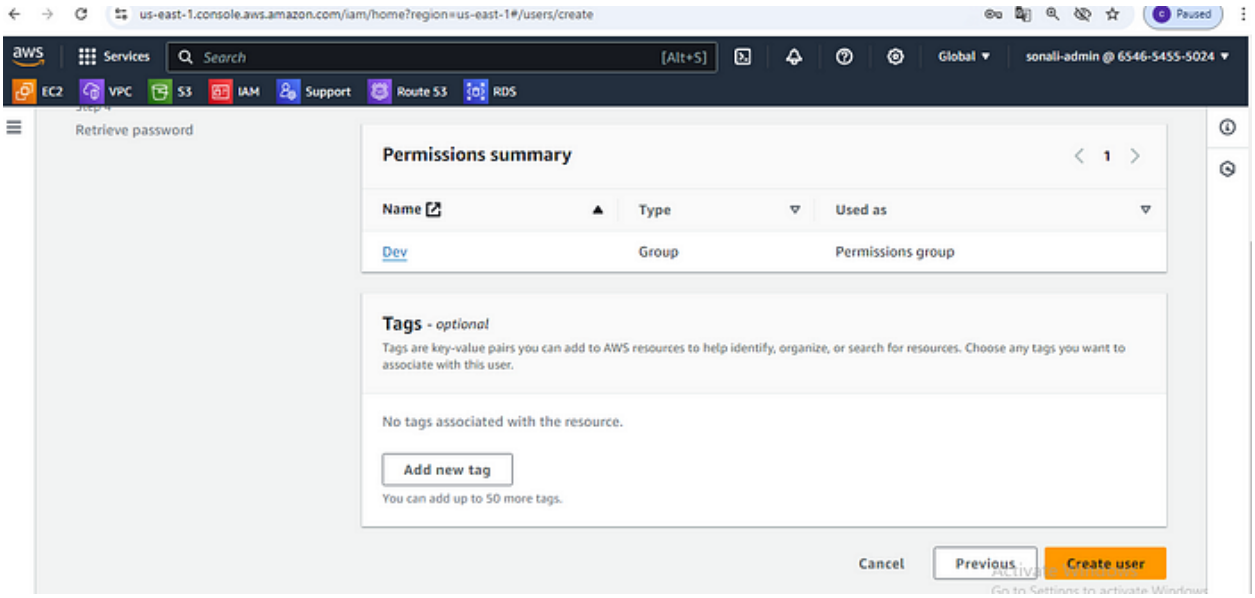
Step 3: Select permission option.



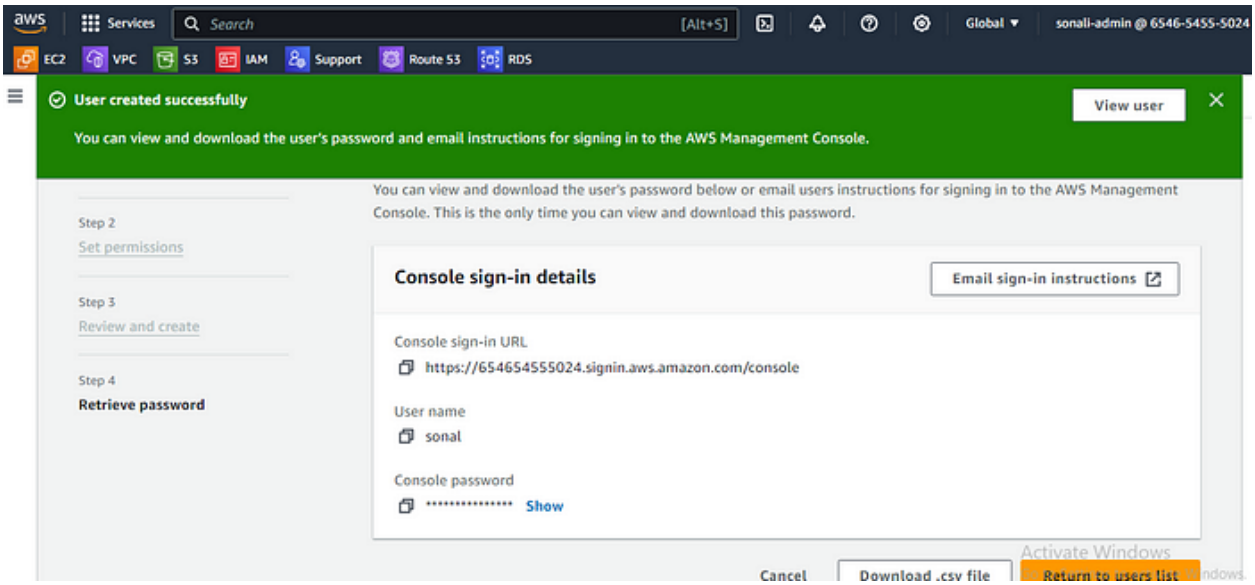
Step 4: If you want to add that user in group then you select group and click on next.



Step 5: Click on create user



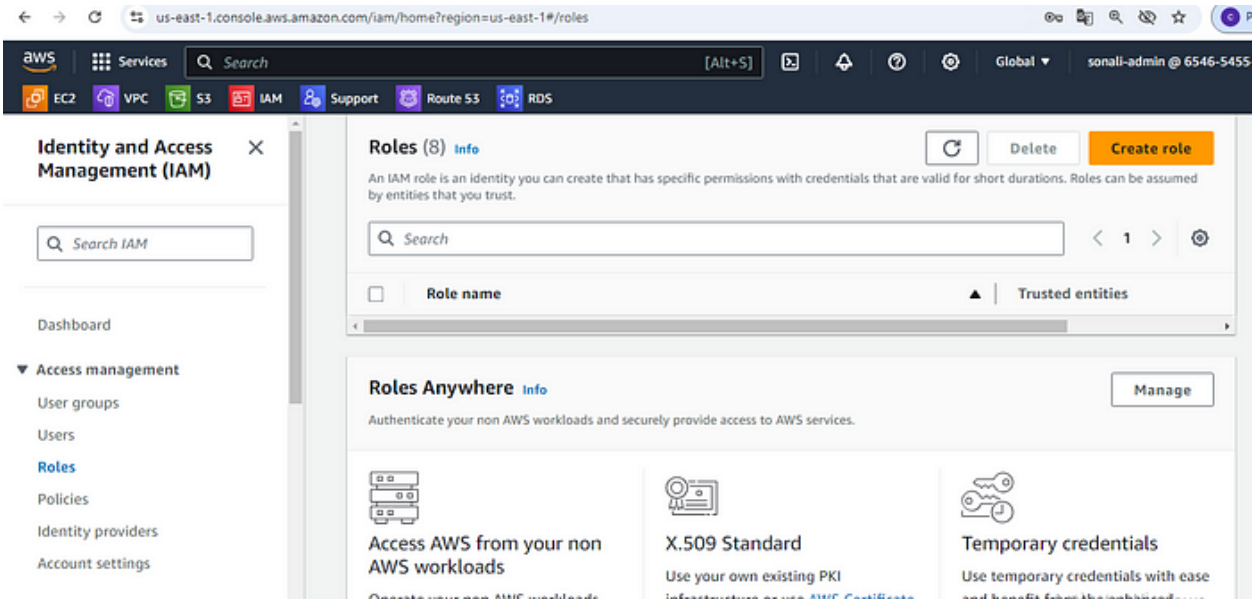
Step 6: user created Successfully. Download the .csv file.



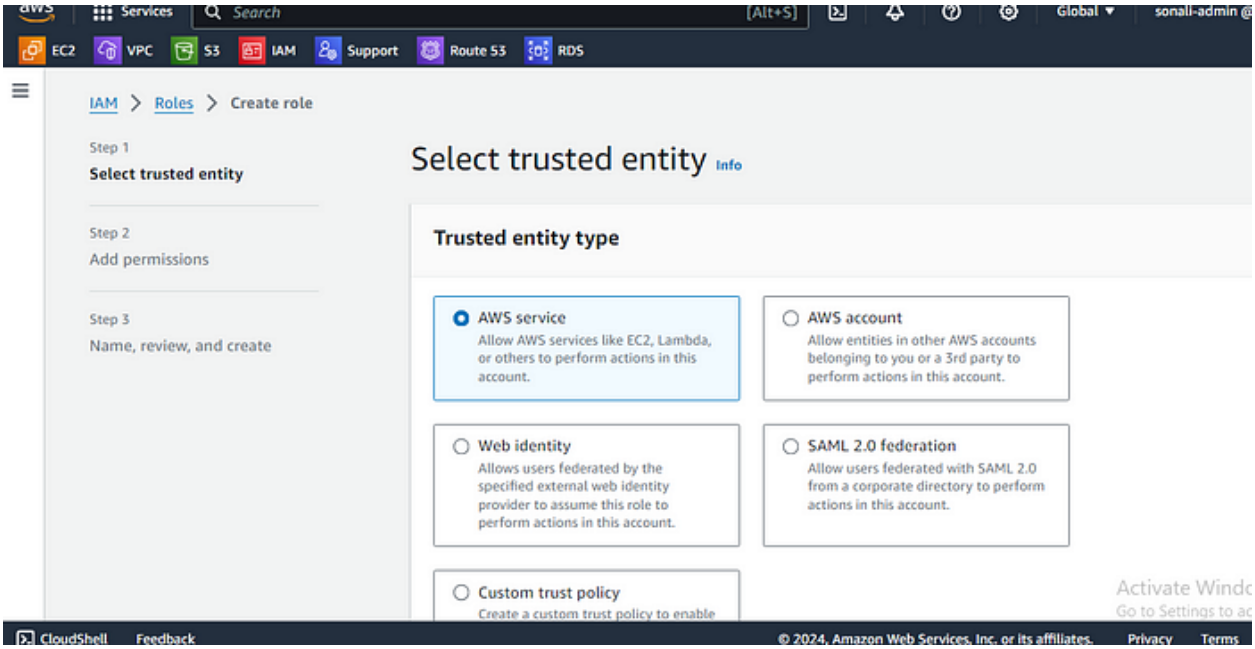
IAM Role :-

To Access the Resource of another service in AWS we can use IAM Role. Suppose you want to show the s3 bucket using EC2 Service. Follow the below step to Create role.

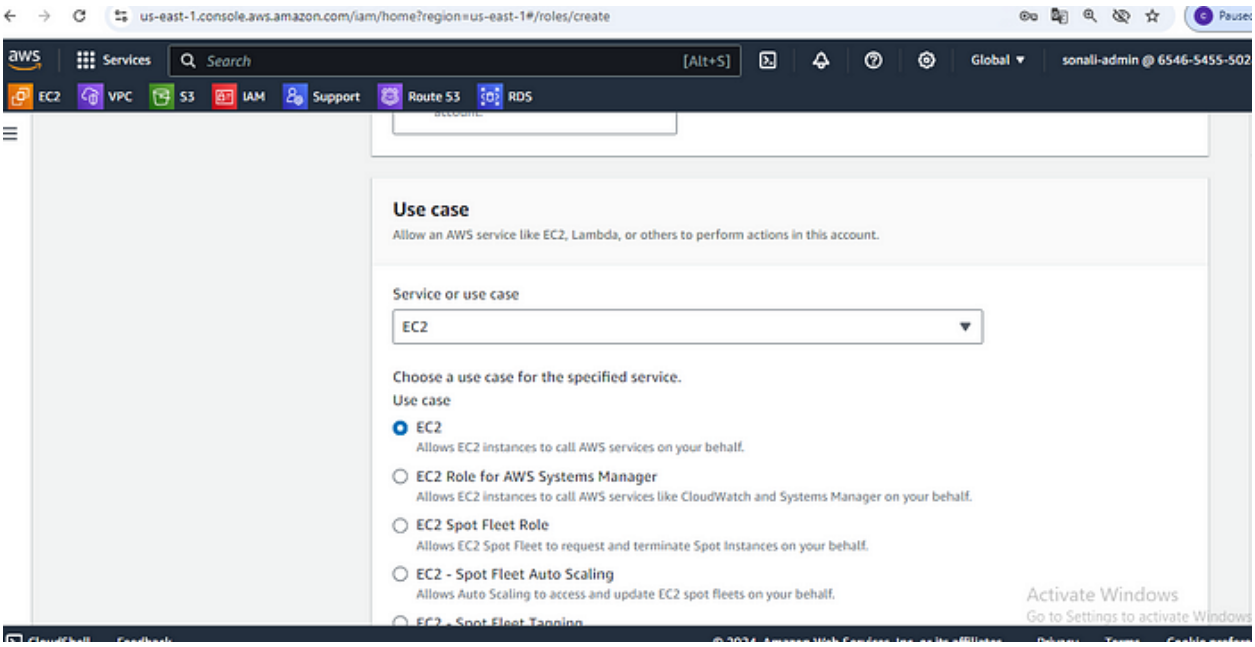
Step 1: Go to roles and click on create role



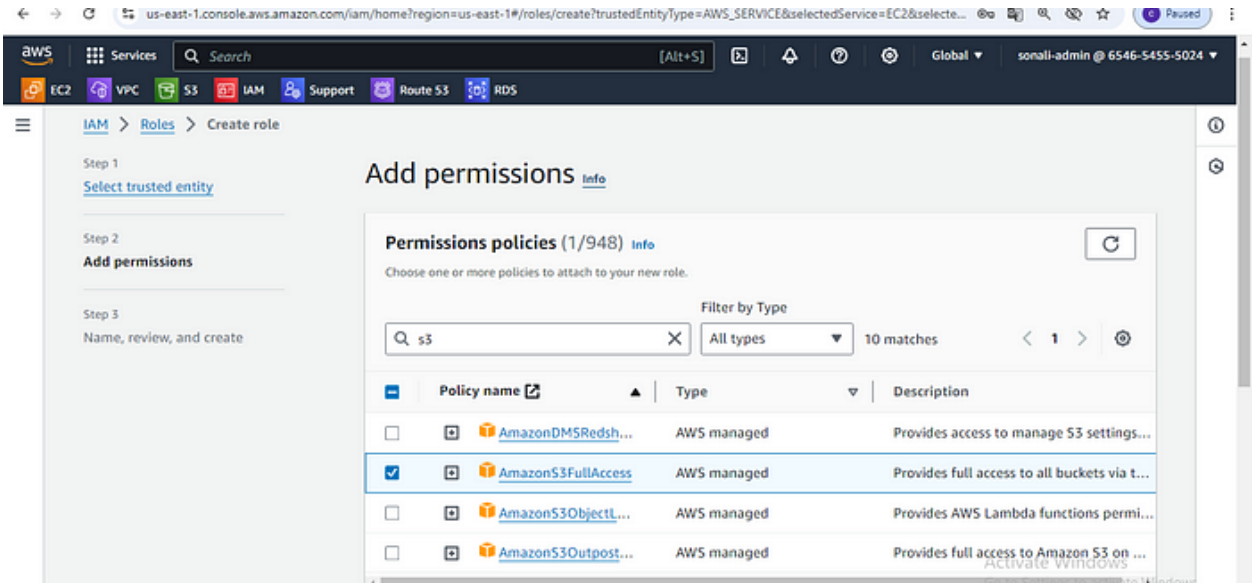
Step 2: Select AWS Service



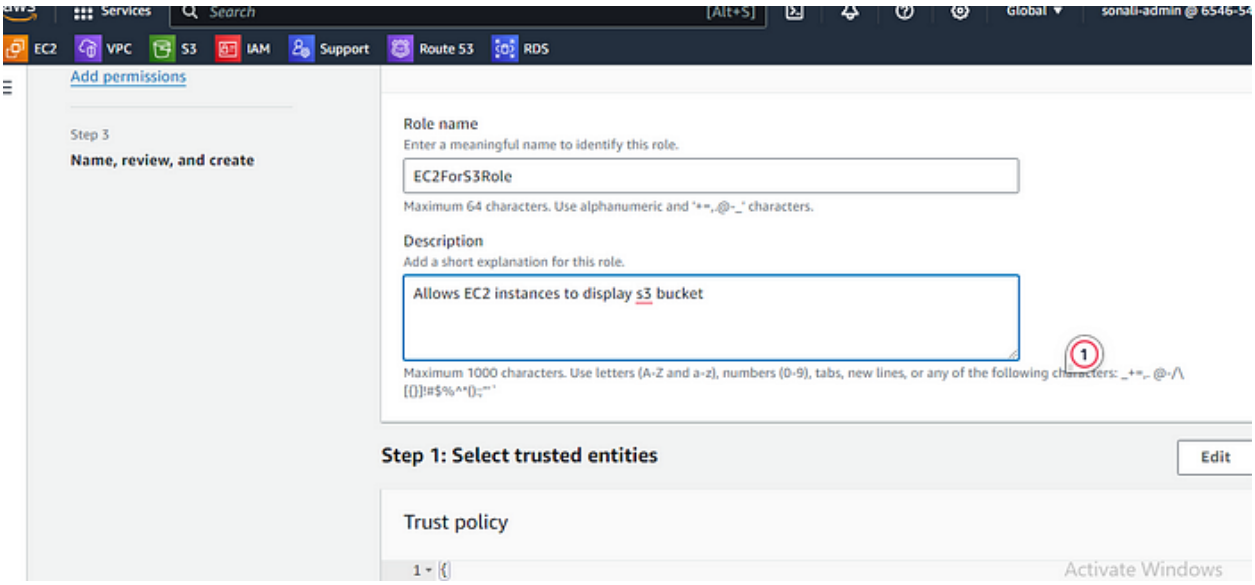
Step 3: Select Use case EC2 and click on next.



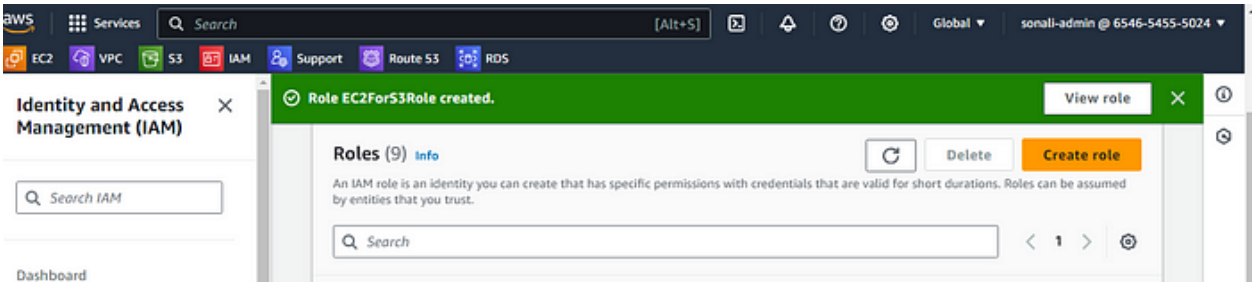
Step 4: Give the s3 permission and click on next.



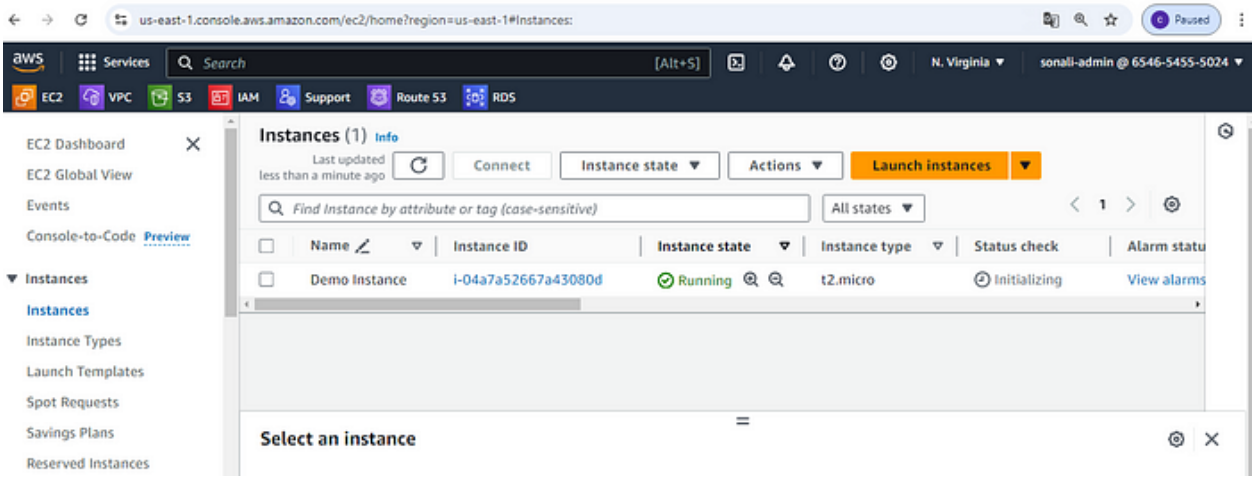
Step 5: Give the role name and description and click on next



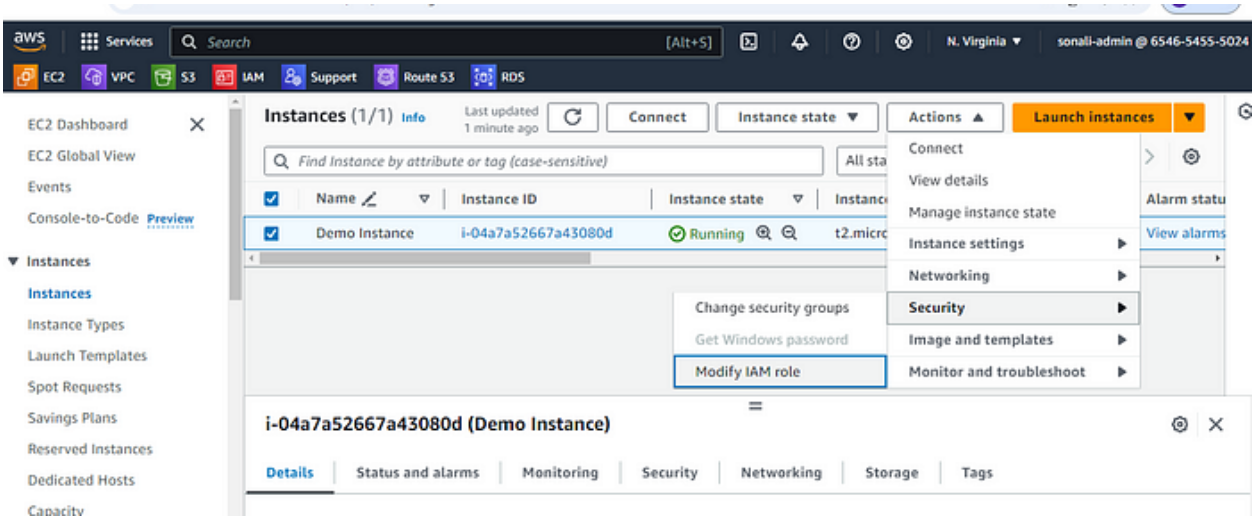
Step 6: Role has been created successfully.



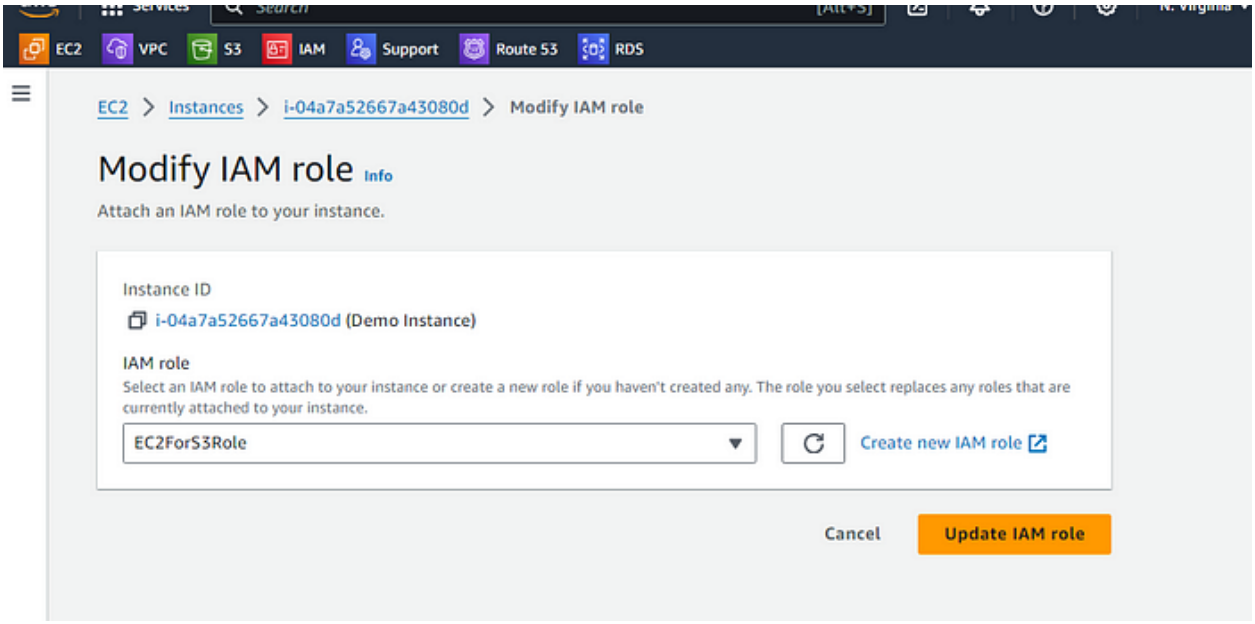
Step 7 : Create EC2 Instance.



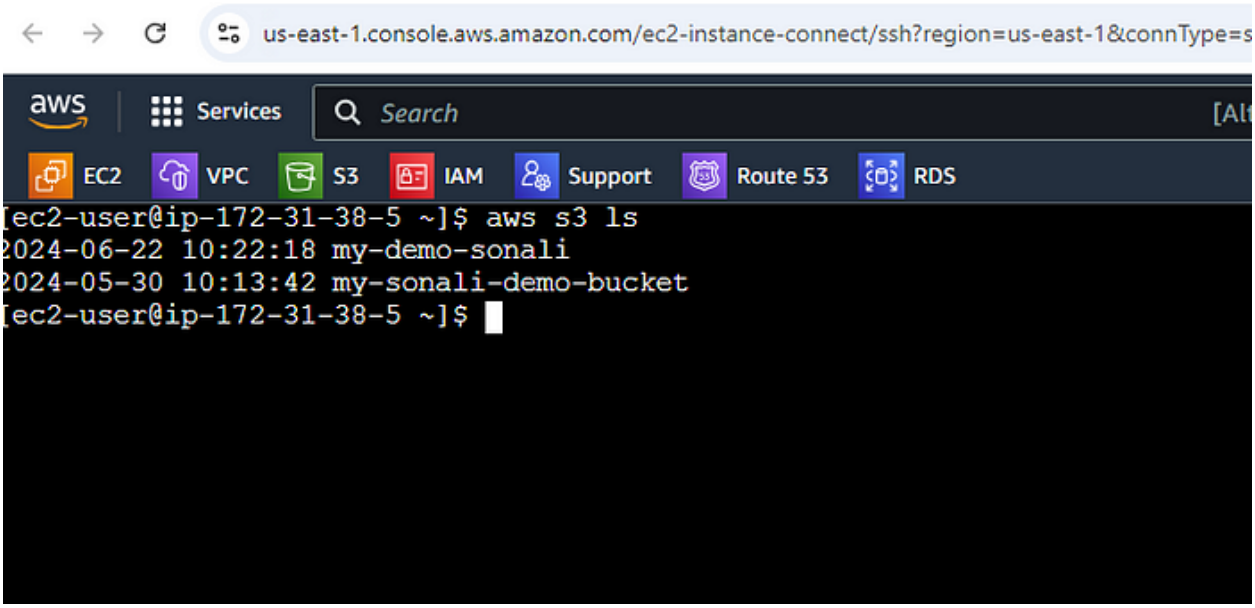
Step 8: Select instance. Click on Action tab and Select Security and Click on Modify IAM Role.



Step 9: Select IAM role which we have created previously. and update the IAM Role.



Step 10 : Connect the instance. Check the AWS CLI is installed or not . And configure your AWS security credential like access key and secrete key using “aws configure” utility. And Write the command to display s3 bucket “ aws s3 ls” you will get the list of all the bucket.



IAM Policies :- IAM policies is used to give permission to the user ,group or role. IAM Policies is a JSON document with set of rule.

Types of IAM Policies

1. **AWS Managed Policies**: Predefined policies by AWS that you can attach to users, groups, or roles.

Example: `AmazonS3ReadOnlyAccess`, `AdministratorAccess`

2. Customer Managed Policies: Custom policies that you create and manage yourself. These offer more fine-grained control over permissions.

3. Inline Policies: Embedded directly into a user, group, or role rather than being a standalone entity like managed policies. These are tightly coupled with the principal they are associated with.

Interview Question

1. What is AWS Identity and Access Management (IAM)?

IAM is Identity and Access Management Service, provided by AWS . It is Global Service. It helps you securely control access to AWS resources**.**

AWS IAM is a service that allows you to manage users, groups, and permissions for accessing AWS resources. It provides centralized control over authentication and authorization.

2. What are the key components of AWS IAM?

Key components of AWS IAM include users, groups, roles, policies, permissions, and identity providers.

3. What is the difference between authentication and authorization in AWS IAM?

Authentication is the process of verifying the identity of users or entities, while authorization is the process of granting or denying access to resources based on policies and permissions.

4. How can you secure your AWS account using IAM?

You can secure your AWS account by enforcing the principle of least privilege, creating strong password policies, enabling multi-factor authentication (MFA), and regularly reviewing permissions.

5. How do IAM users differ from IAM roles?

IAM users are individuals or entities that have a fixed set of permissions associated with them. IAM roles are temporary credentials that can be assumed by users or AWS services to access resources.

we can use IAM role for give access resource **permission** of one service to another service.

6. What is an IAM policy?

An IAM policy is a JSON document that defines permissions. It specifies what actions are allowed or denied on which AWS resources for whom (users, groups, or roles).

7. What is the purpose of IAM groups?

IAM groups allow you to group users and apply policies to them collectively, simplifying permission management by granting the same set of permissions to multiple users.

8. How can you grant permissions to an IAM user?

You can grant permissions to an IAM user by attaching policies to the user directly or by adding the user to groups with associated policies.

9. What is the difference between IAM policies and resource-based policies?

IAM policies are attached to identities (users, groups, roles), while resource-based policies are attached to AWS resources (e.g., S3 buckets, Lambda functions) to control access from different identities.

10. **What are managed policies and inline policies in AWS IAM?**

Answer:
— Managed Policies: Managed policies are standalone policies that you can attach to multiple users, groups, or roles. They are created and managed independently and can be shared across AWS accounts.
— Inline Policies: Inline policies are policies that are embedded directly into a single user, group, or role. They are defined within the entity they are attached to and cannot be shared or reused outside of that entity.

11. Scenario: Your team wants to ensure secure access to AWS resources for different team members. How could you implement this?

Answer: I would use AWS Identity and Access Management (IAM) to create fine-grained policies for each team member. IAM roles and groups can be assigned permissions based on least privilege principles.