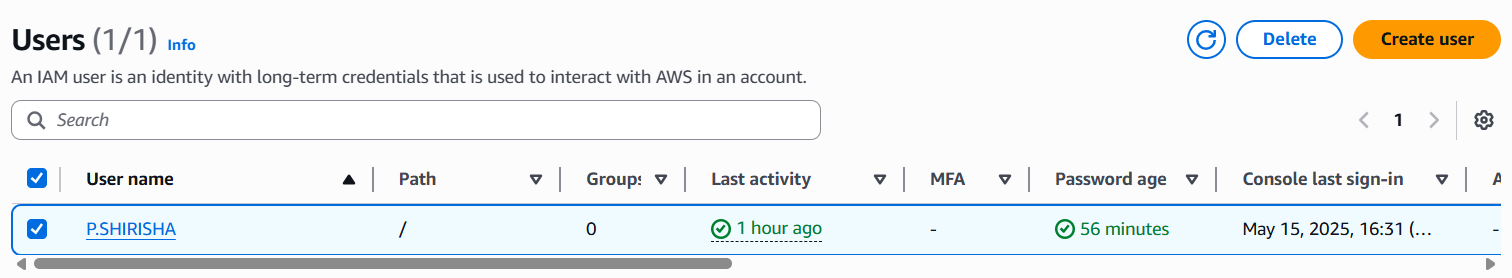
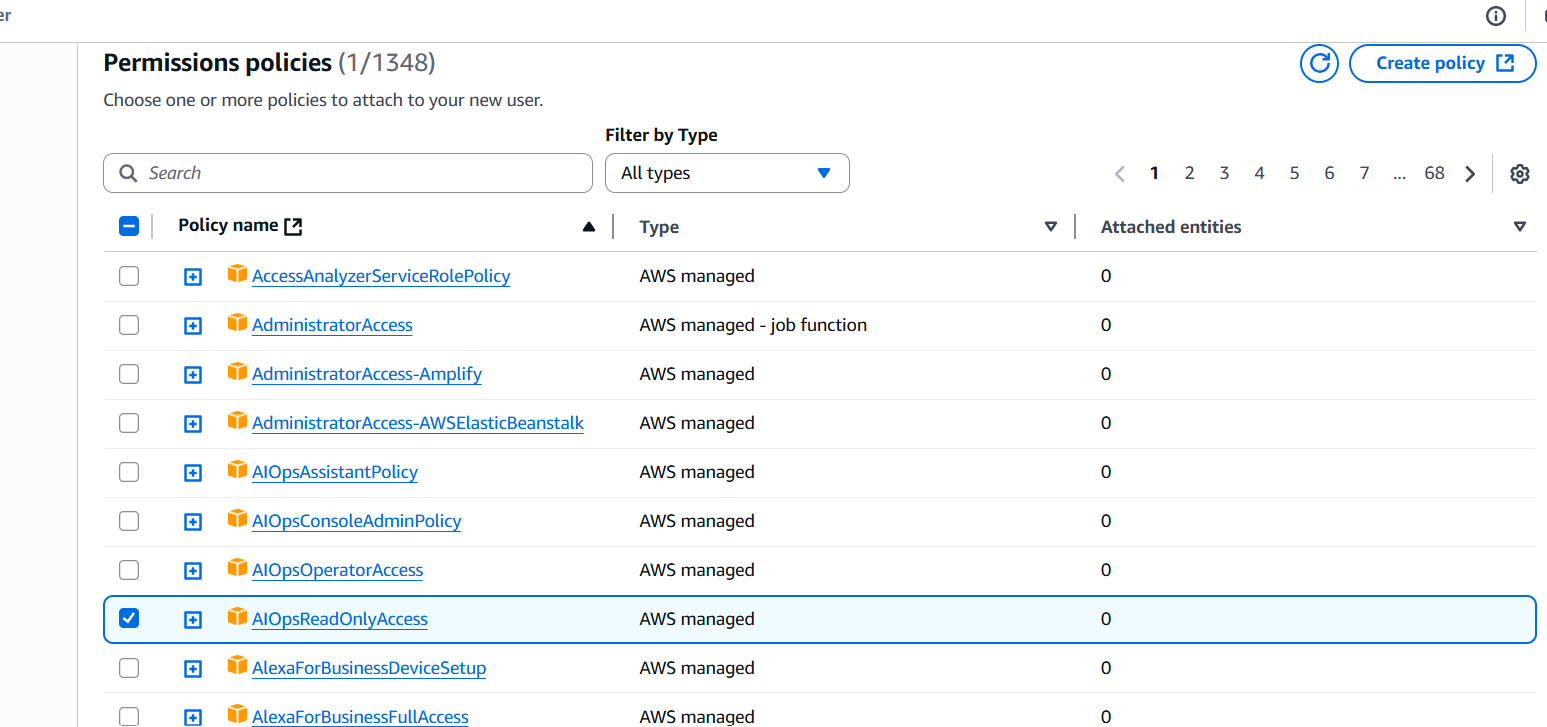
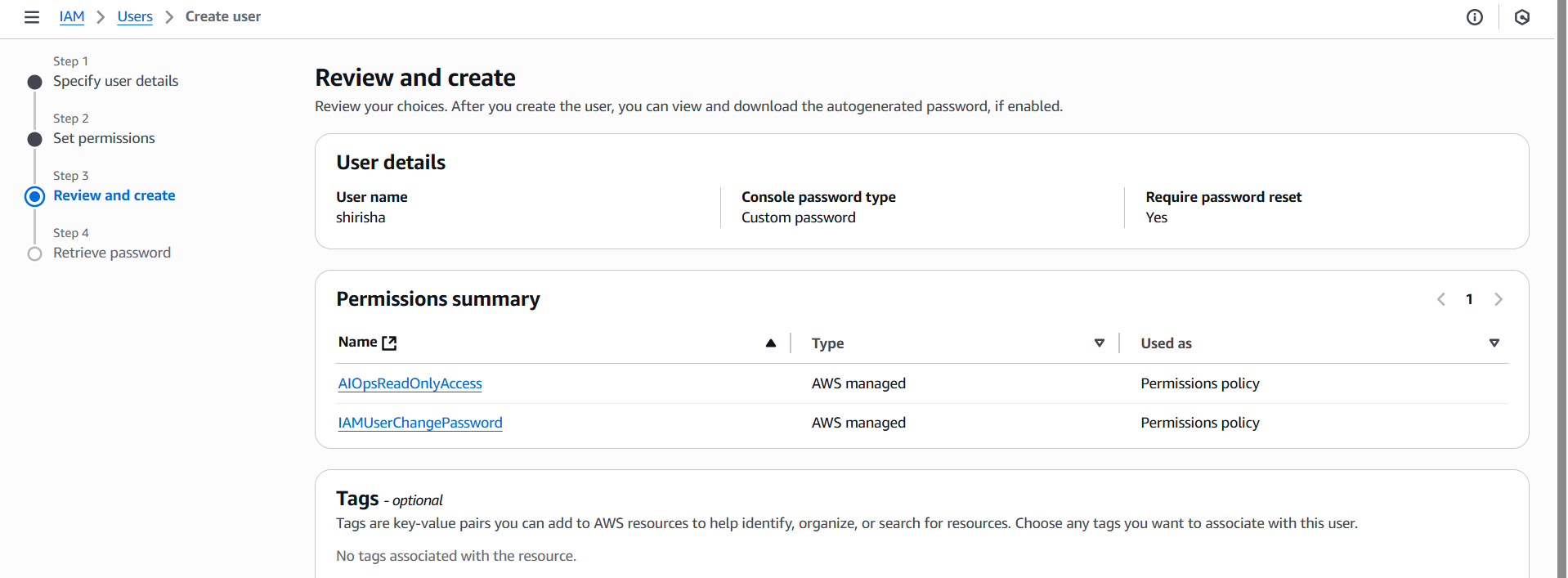
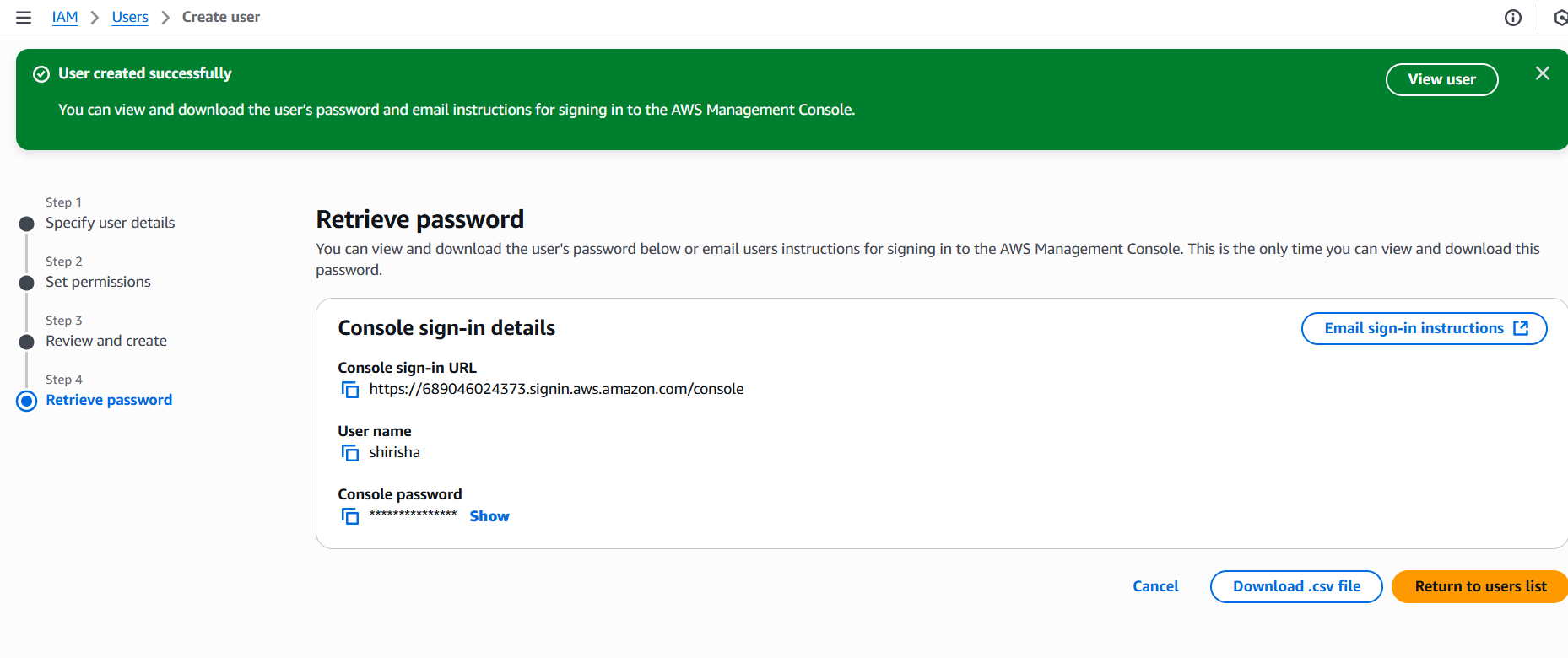
1. Create one IAM user and assign ec2, S3 full access role.



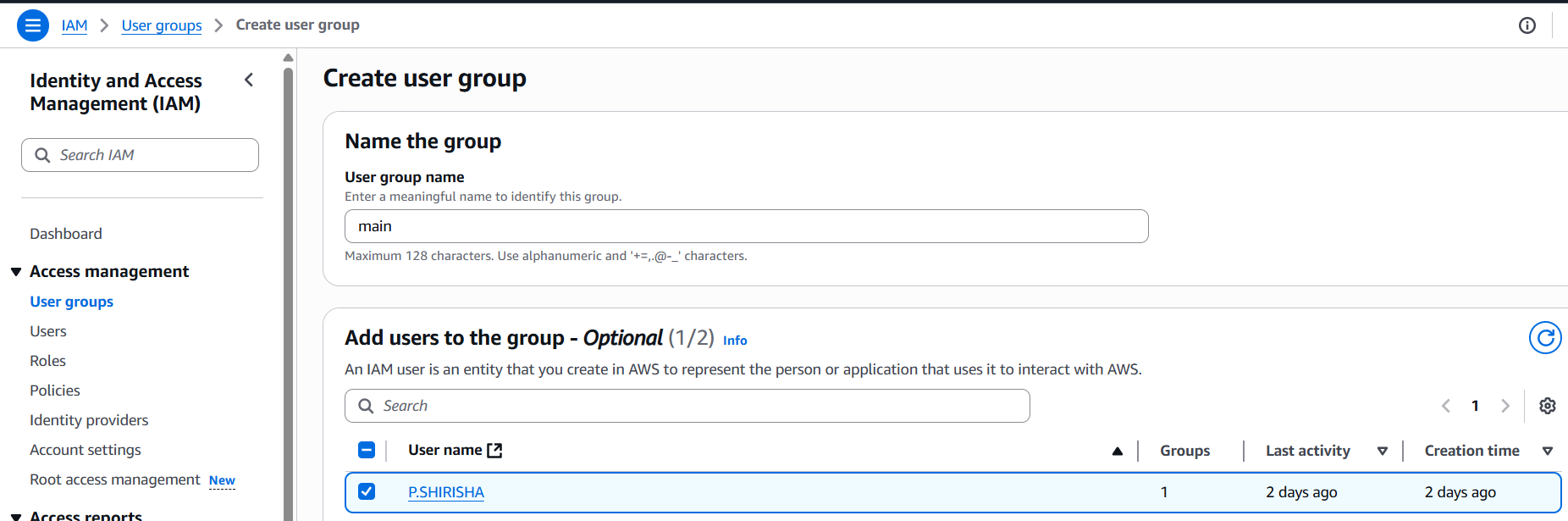


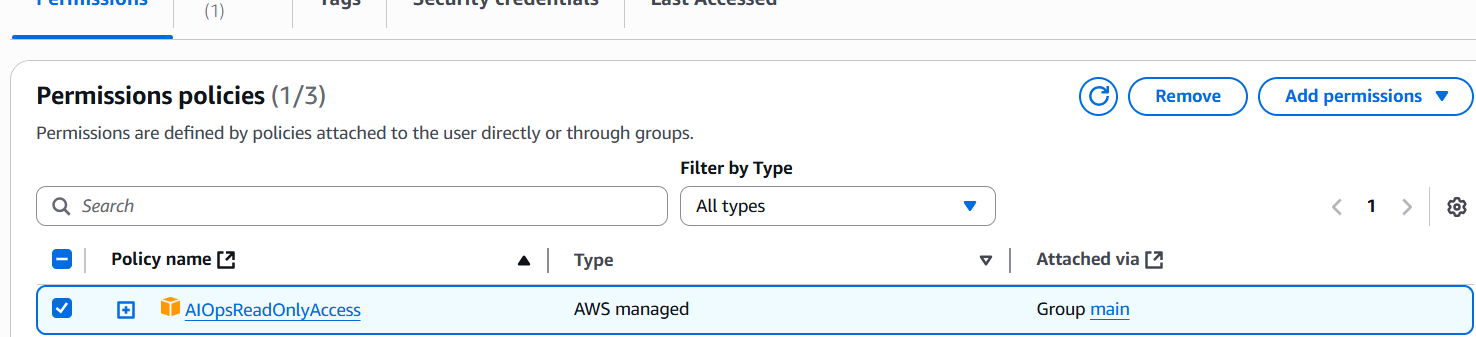




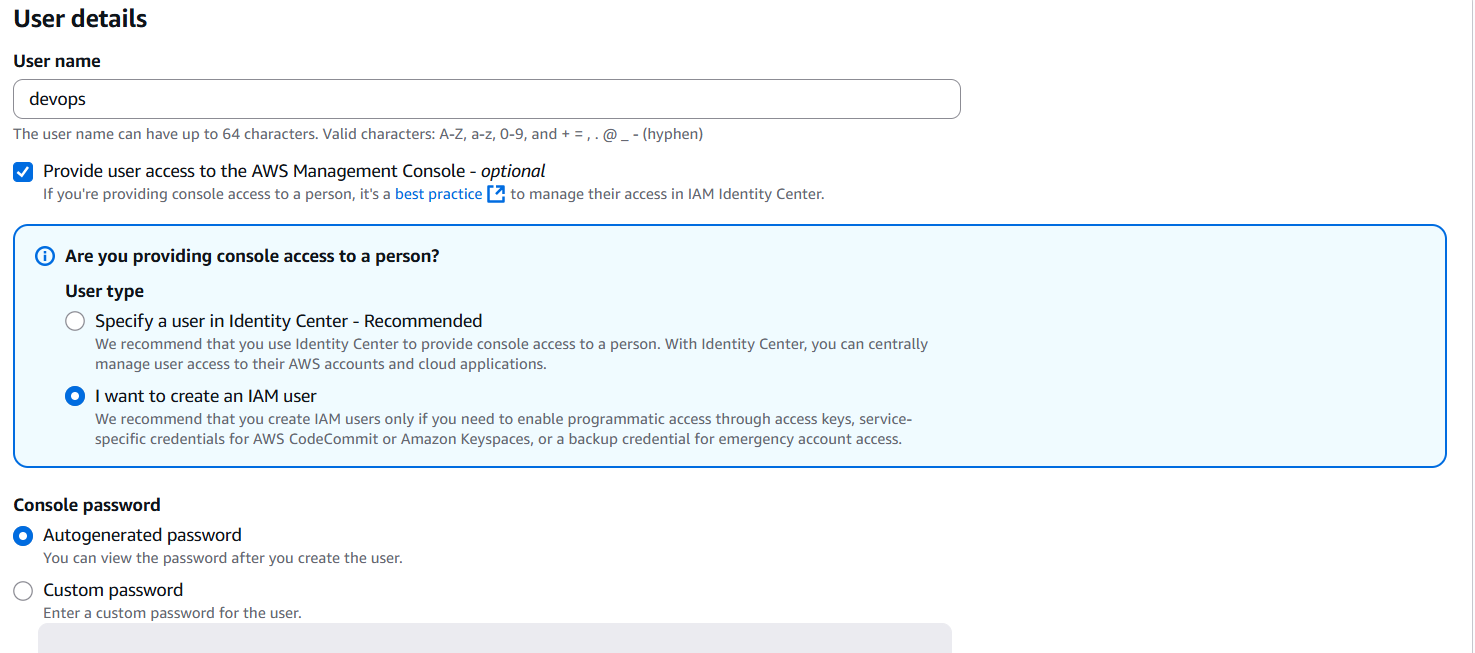
1. Create one Group in IAM and Assign Read access for ec2.

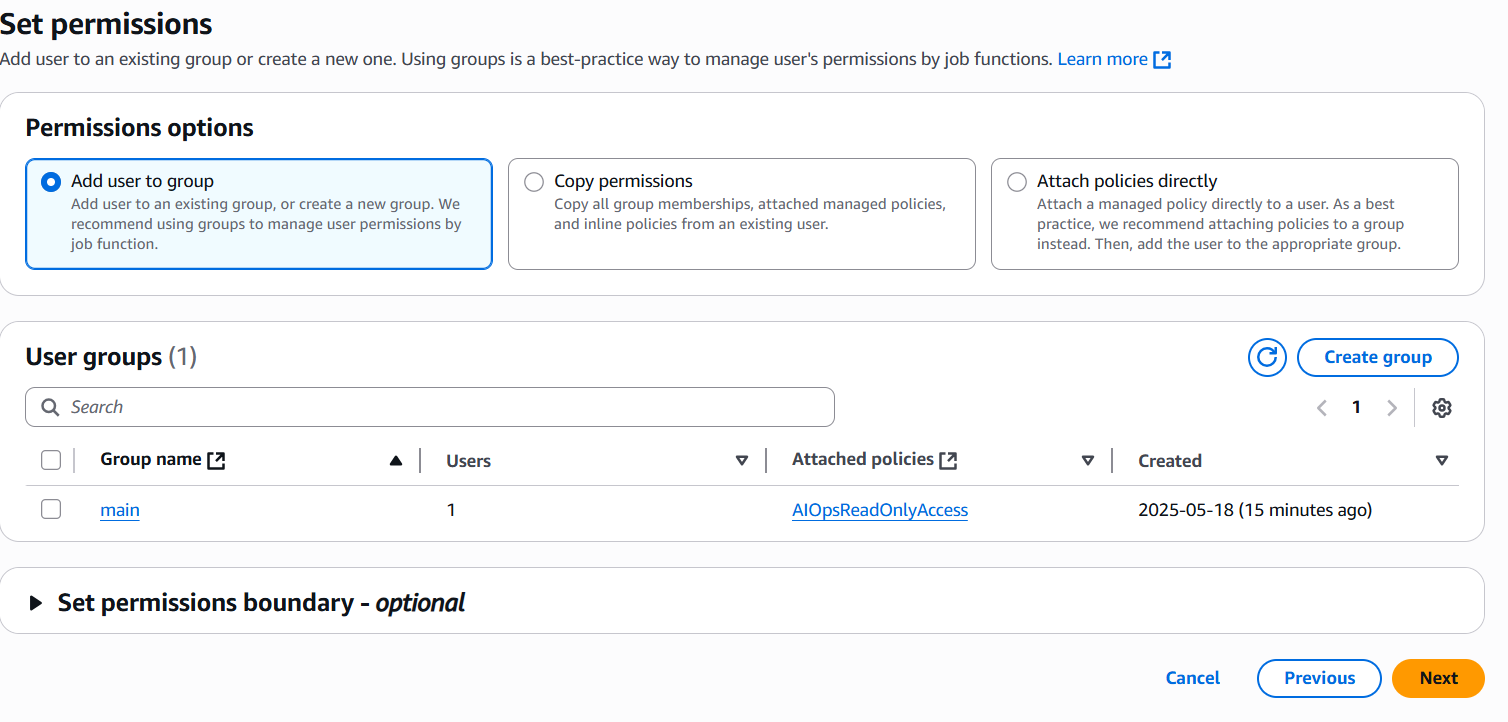
* first you need to create user group
* after creating user group then attach the user
* in the user group go permissions and click on add policy
* then select amazonec2readonly policy and then create the group
* verify that the ec2 is access or not in the mainuser

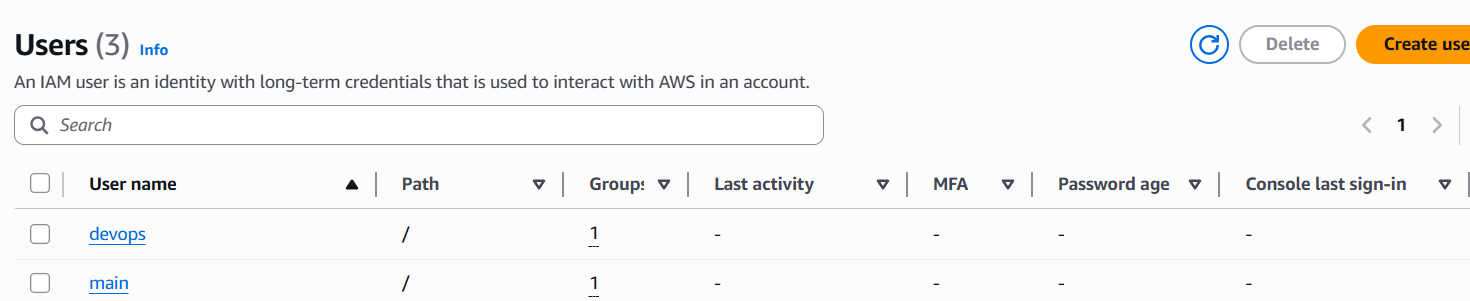




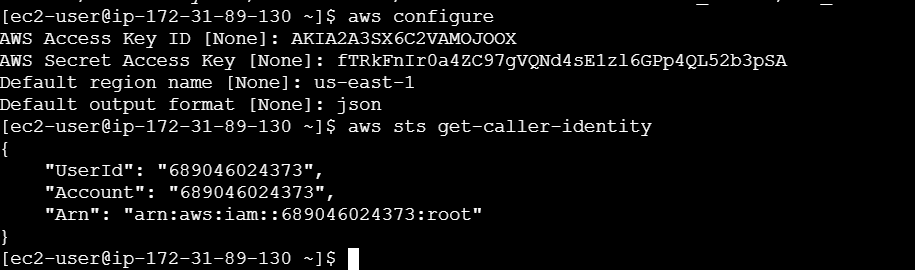
1. Create a new user with name Devops and add to the group created in task2

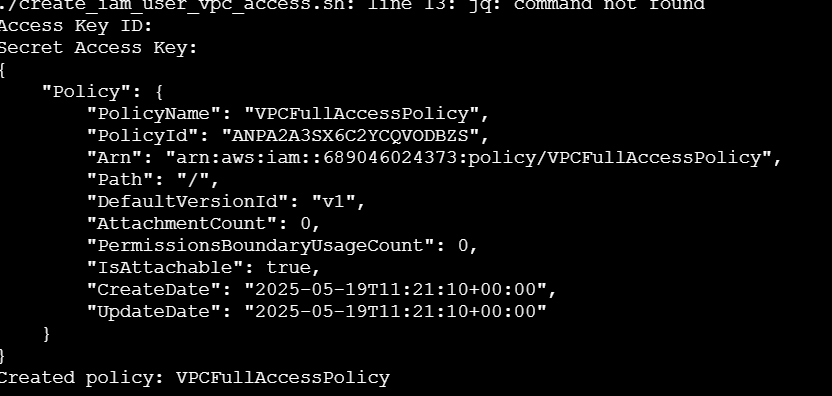






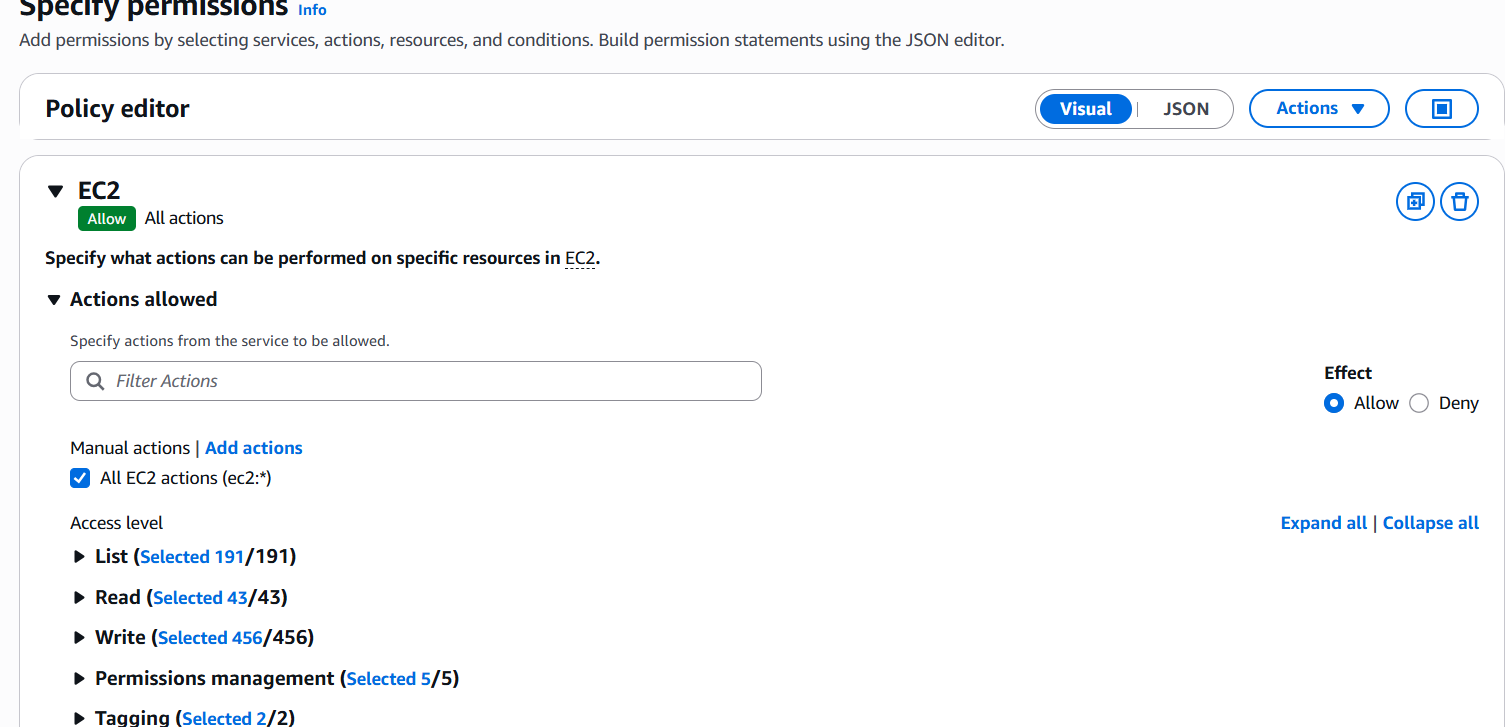
1. Write a bash script to create a IAM user with VPC full access.

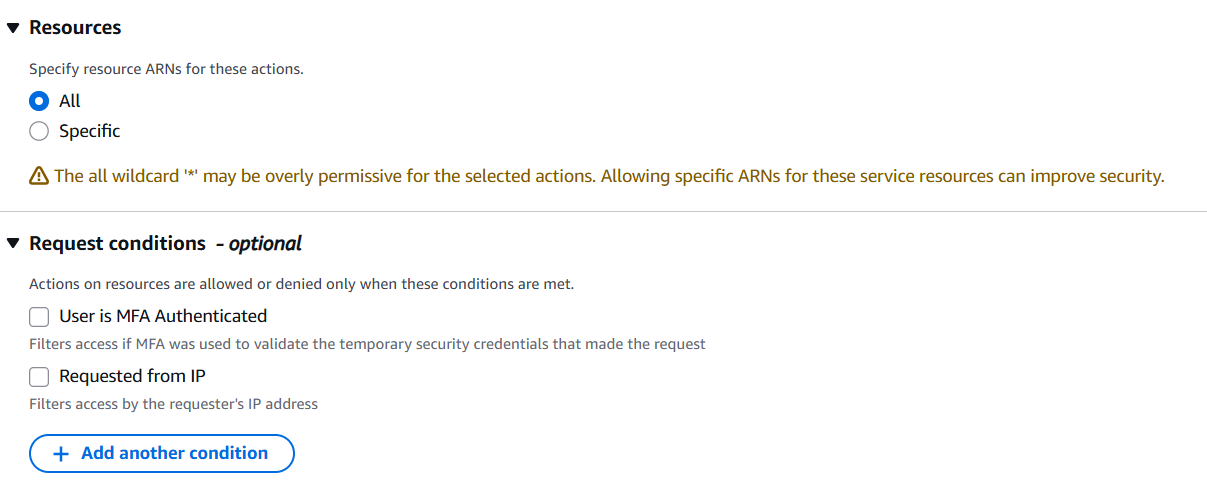


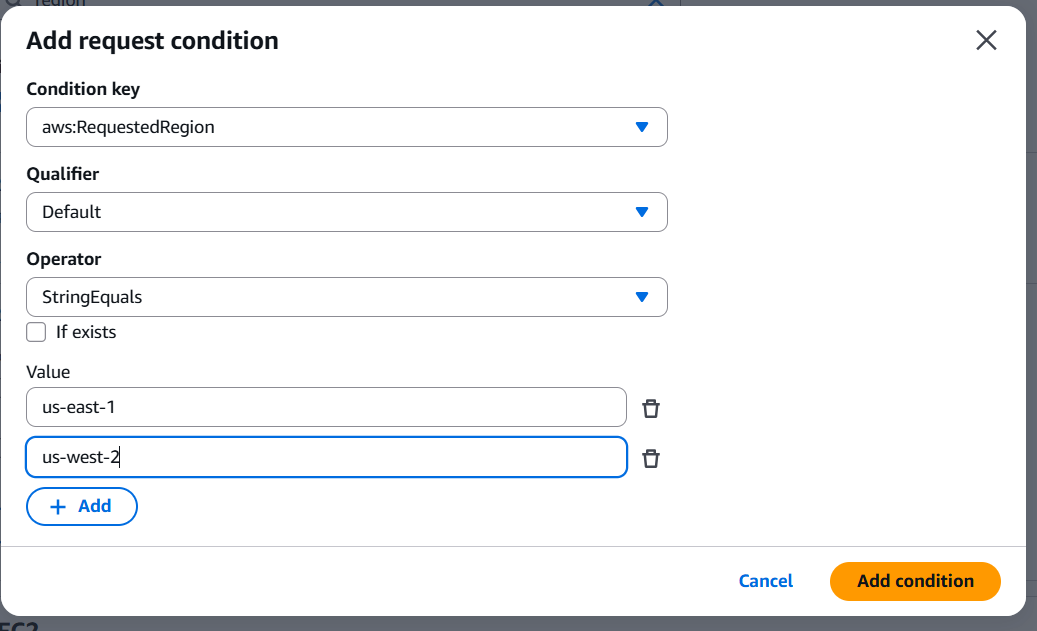
 

1. Create a IAM policy to access ec2 for a specific user in specific regions only.

* go to the policies and select EC2 and select Describe regions
* then in the request conditions give the regions and click on create policy
* then attach that policy to the user and then verify it is working or not



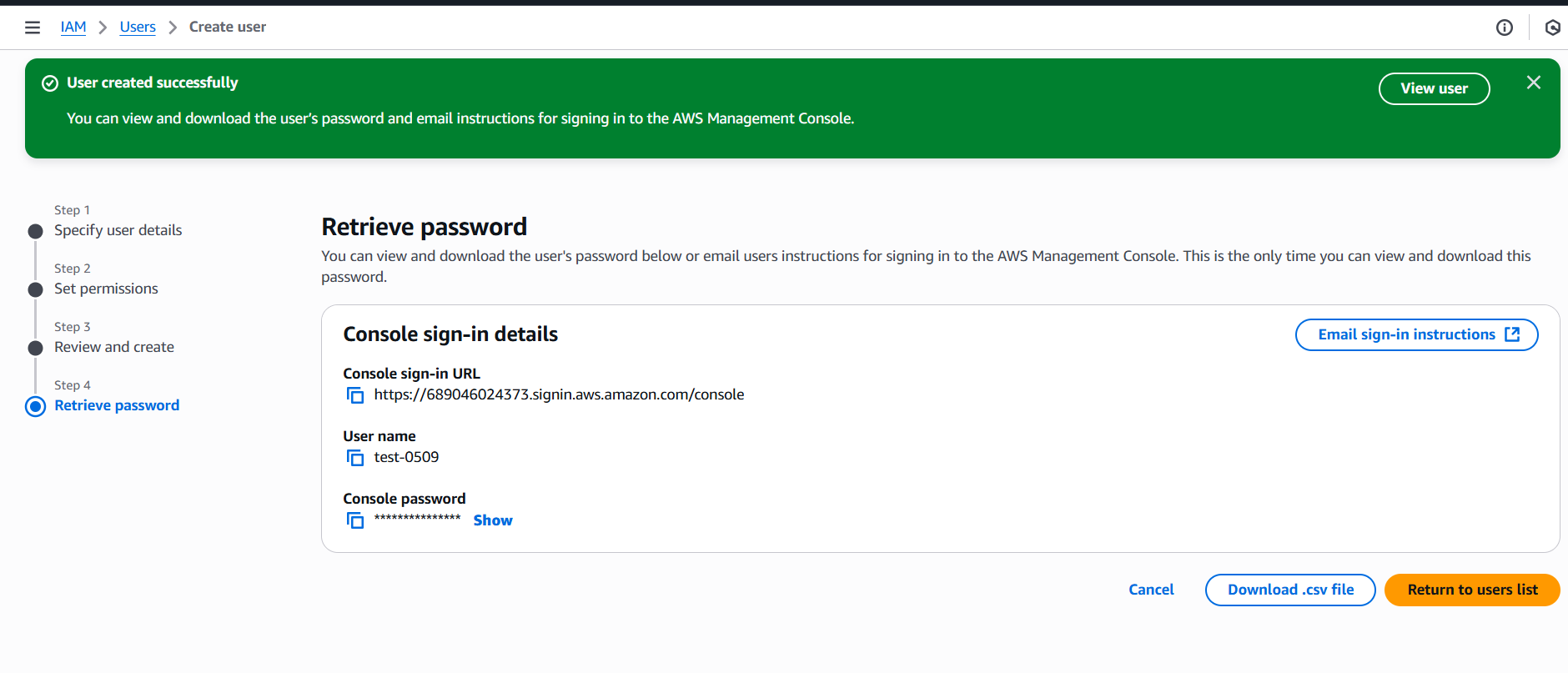


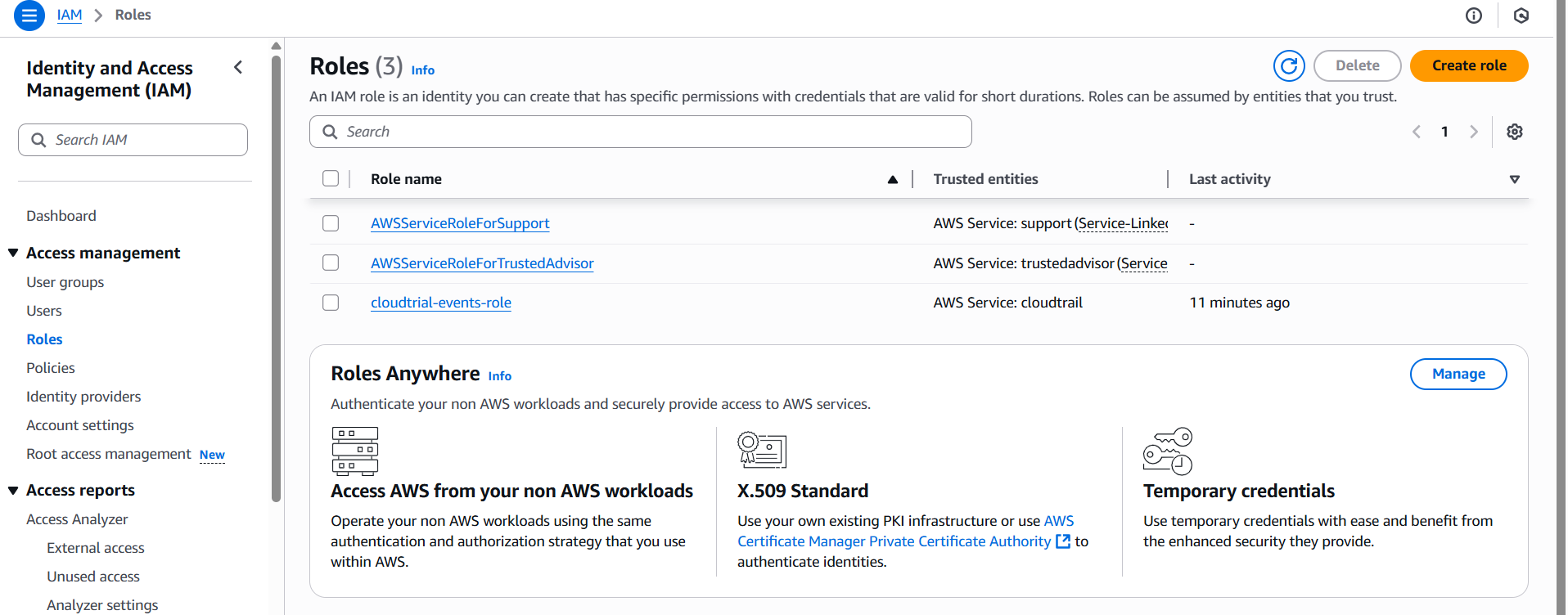


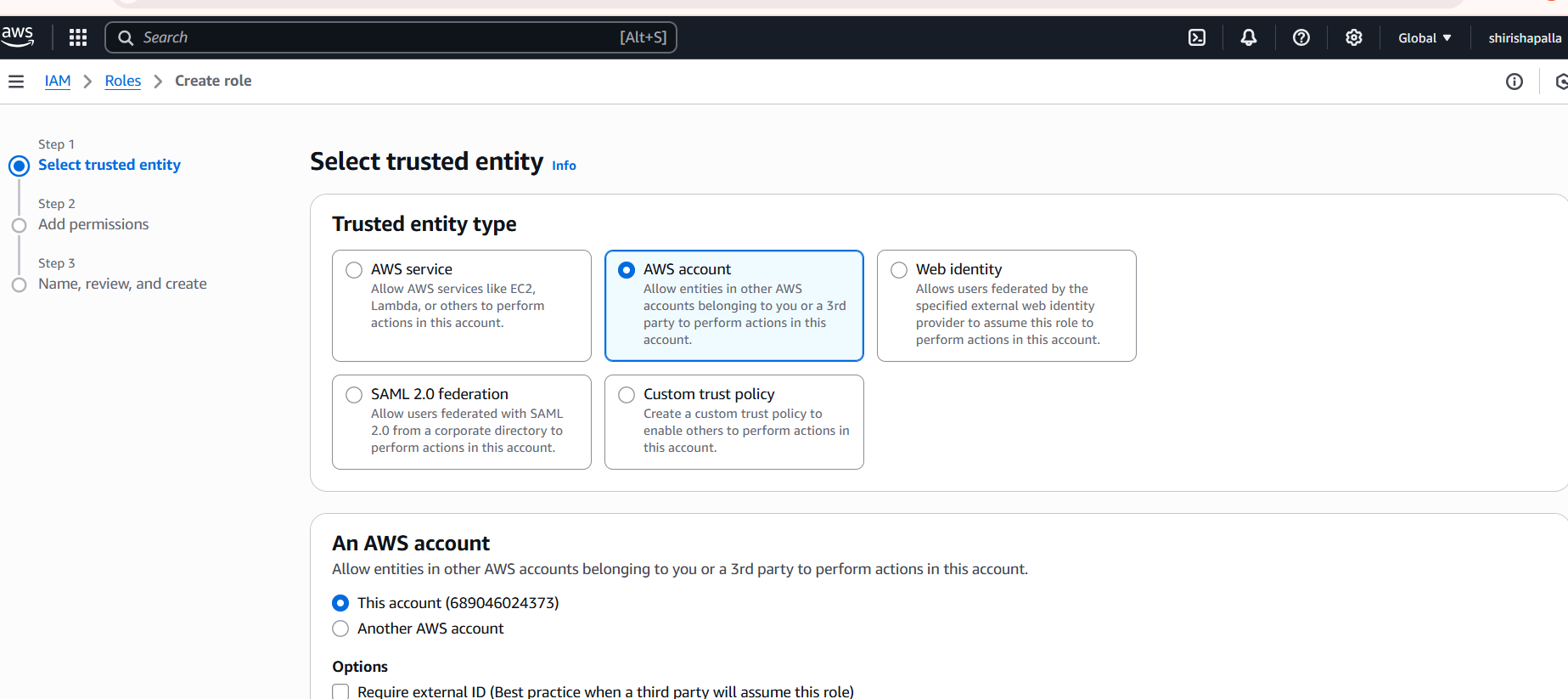
6) We have two accounts Account A and Account B, Account A user should access s3 bucket in Account B. (Collaborate with team member and execute this. Mostly asked in every interview)

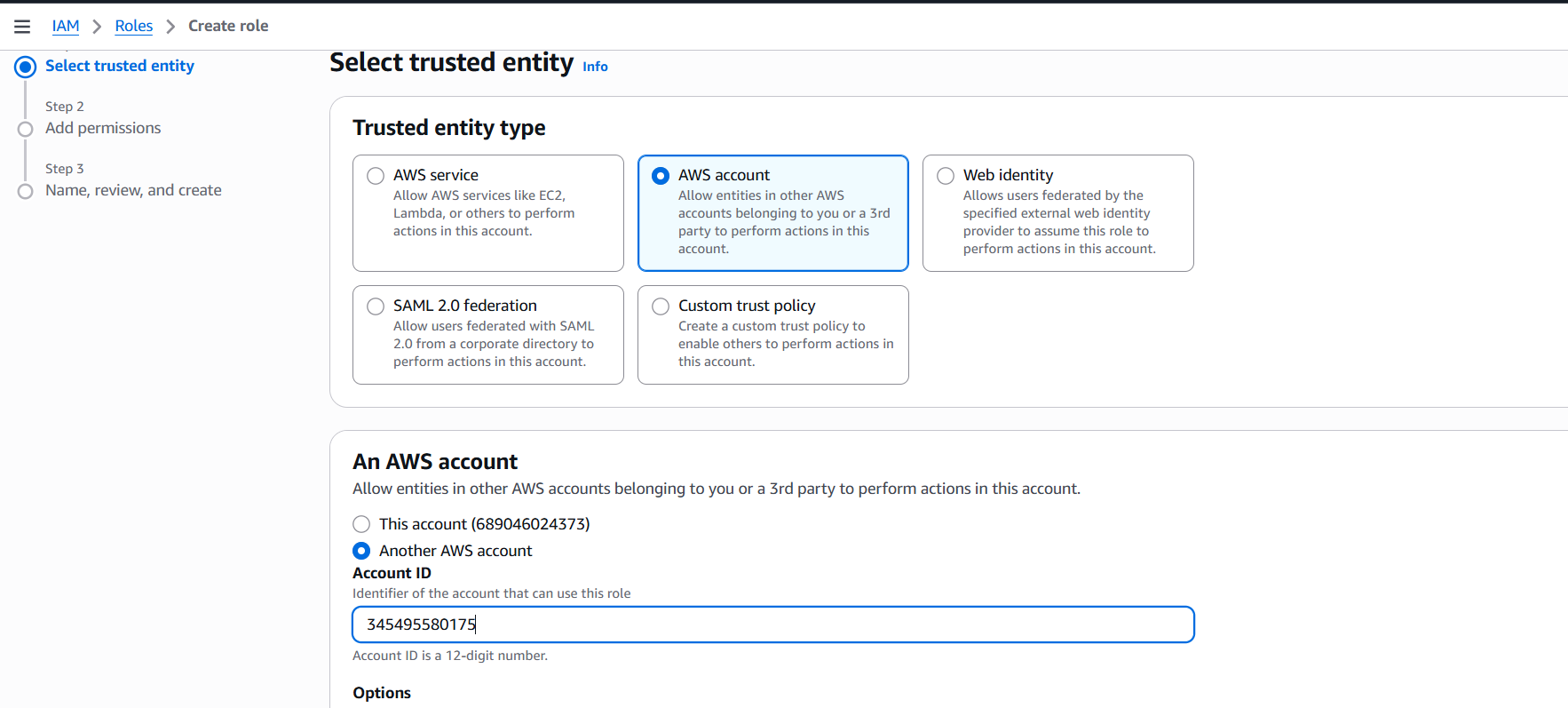
<https://689046024373.signin.aws.amazon.com/console>

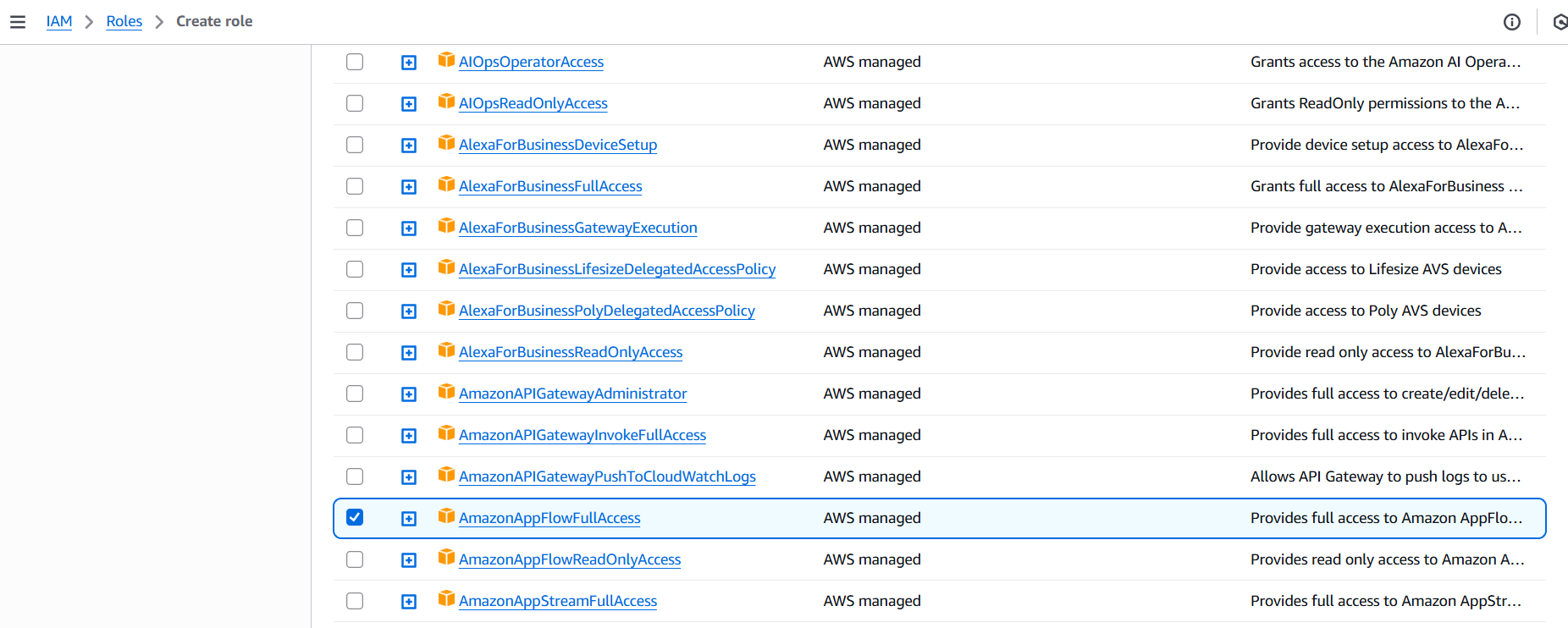
Step 1: Create user

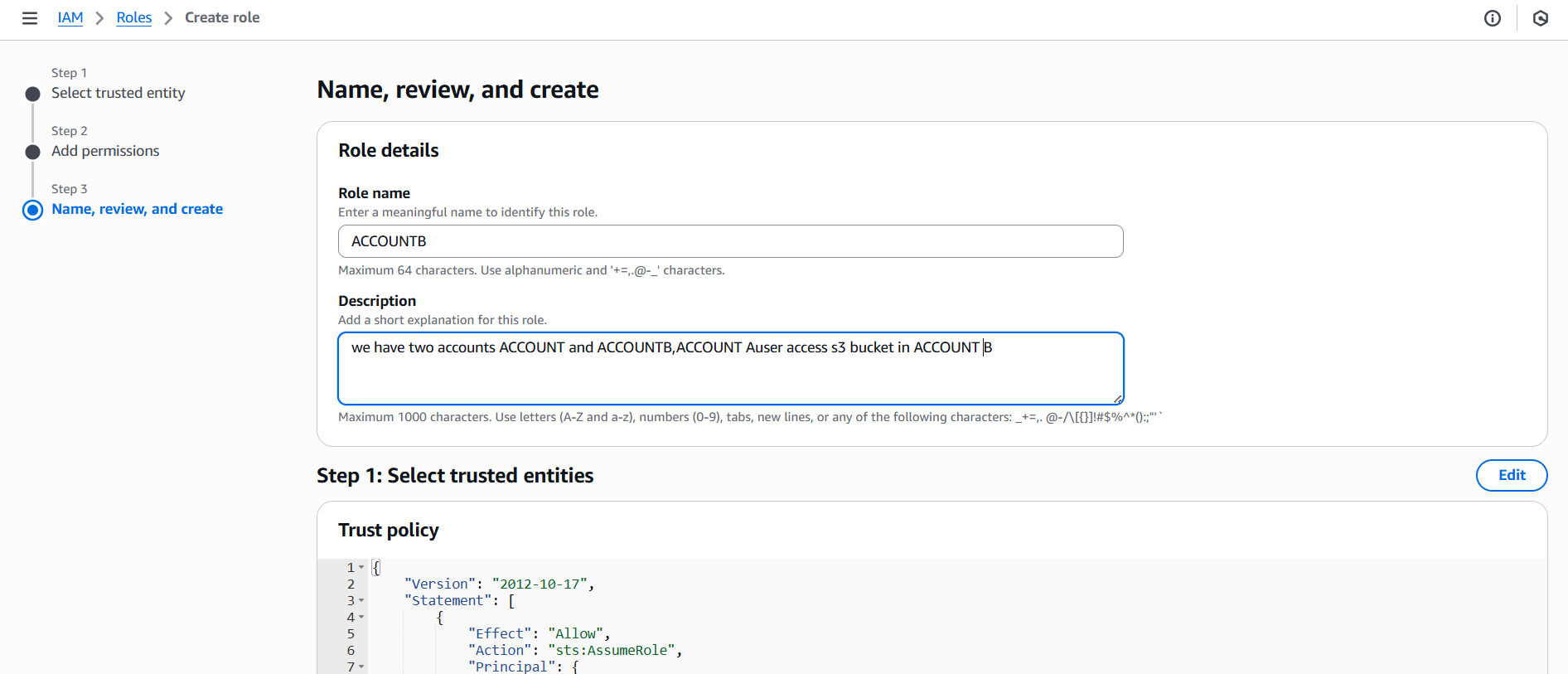


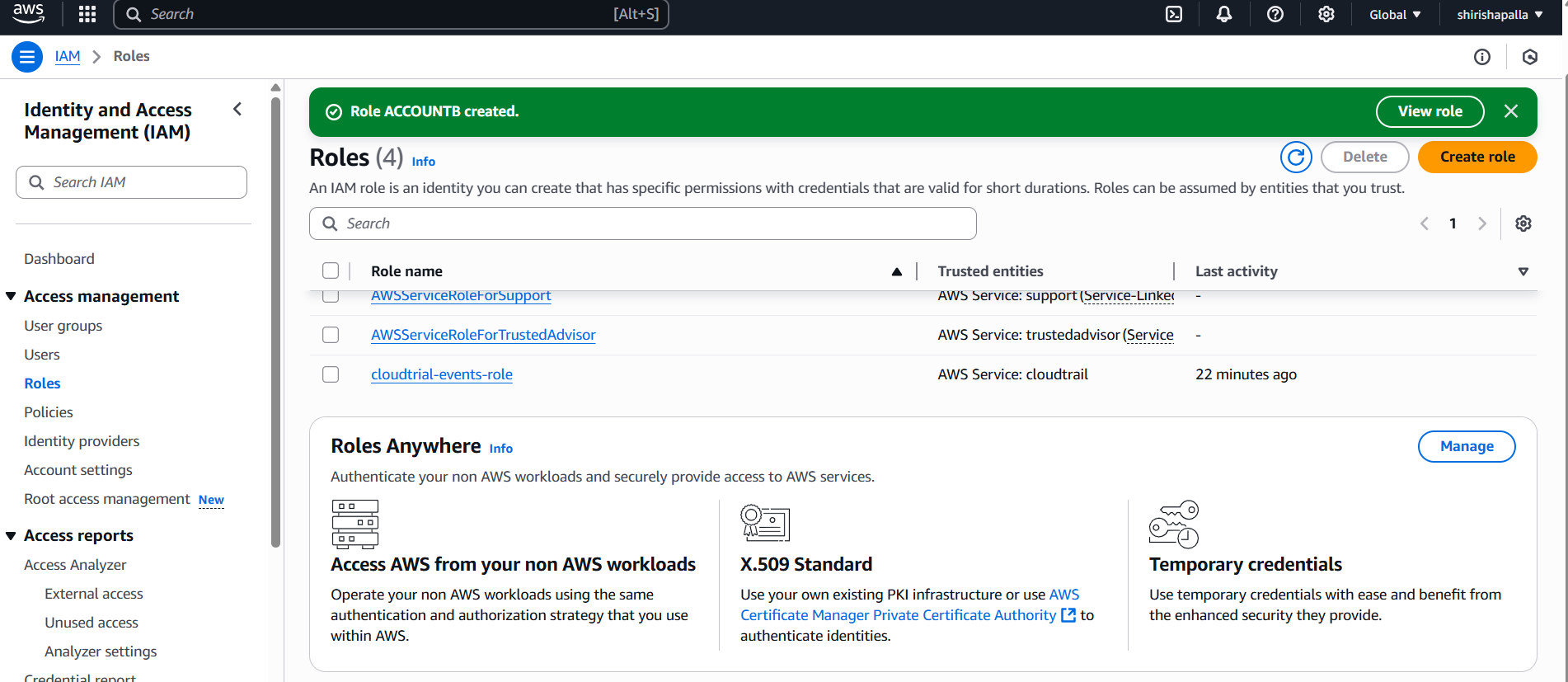


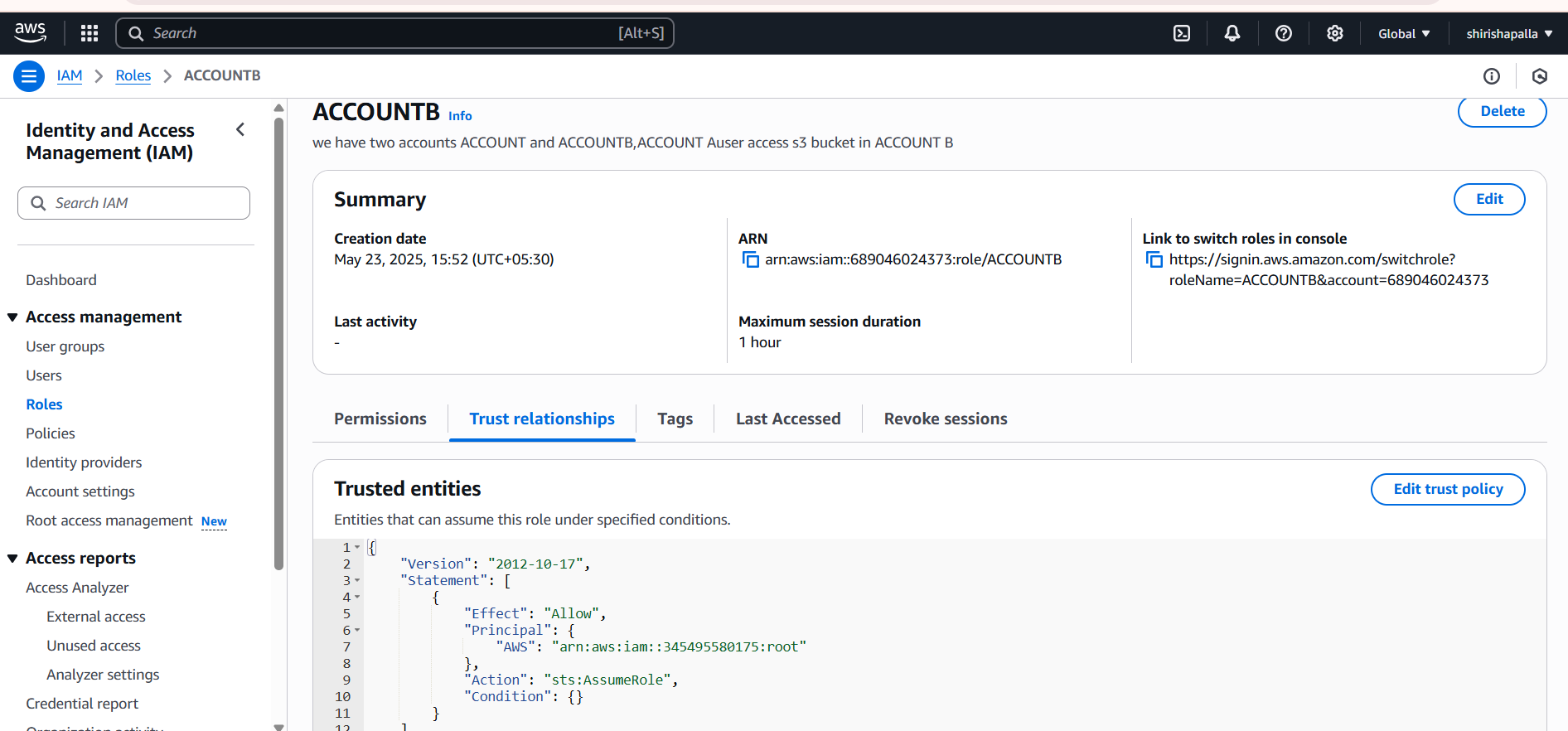










Step 2: Update the Trust Relationship  
1. Go to the role's Trust relationships tab.  
2. Click Edit trust relationship.  
3. Ensure Account A's ID is listed as a trusted entity.  


Step 3: Configure Account A's IAM User  
1. Log in to Account A.  
2. Go to IAM dashboard.  
3. Select the IAM user.  
4. Attach a policy allowing sts:AssumeRole for the role in Account B.  
Example policy:  
{  
 "Version": "2012-10-17",  
 "Statement": [

{  
 "Effect": "Allow",  
 "Action": "sts:AssumeRole",  
 "Resource": "arn:aws:iam::Account-B-ID:role/RoleName"  
 }  
 ]  
}  
Step 4: Access the S3 Bucket  
1. Use the IAM user's credentials in Account A.

2. Assume the role in Account B using the AWS SDK or CLI.

3. Access the S3 bucket in Account B.