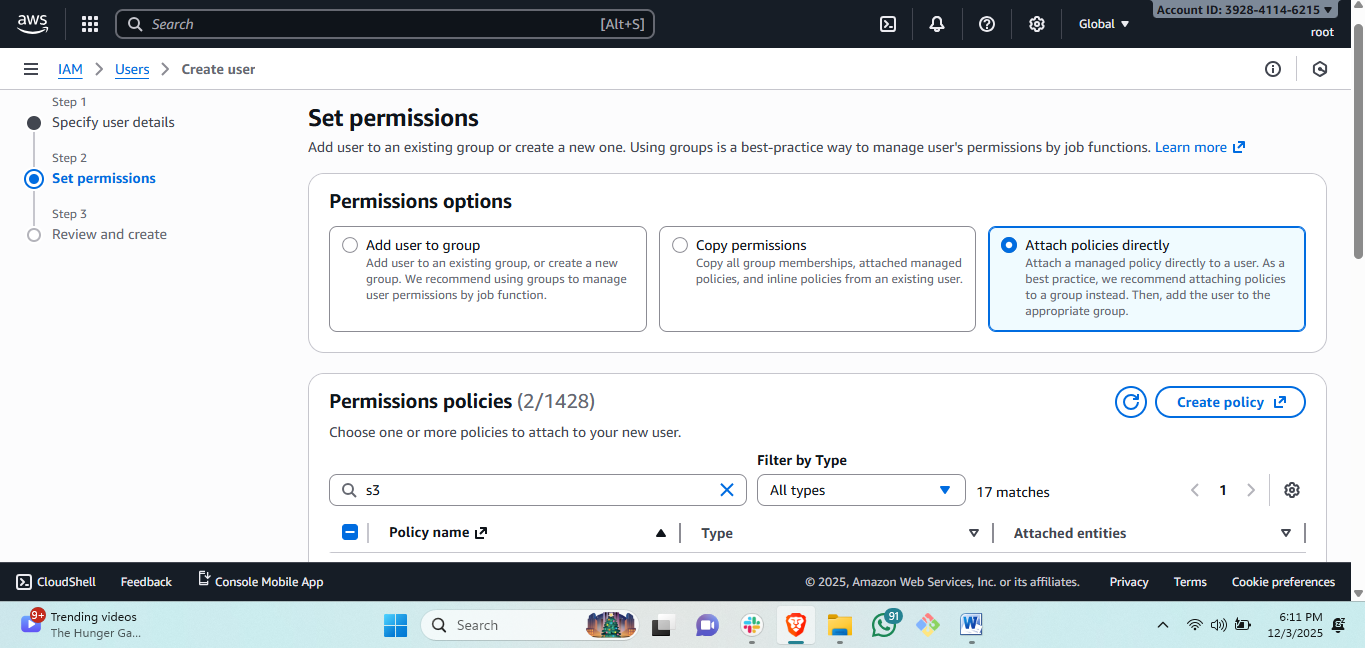
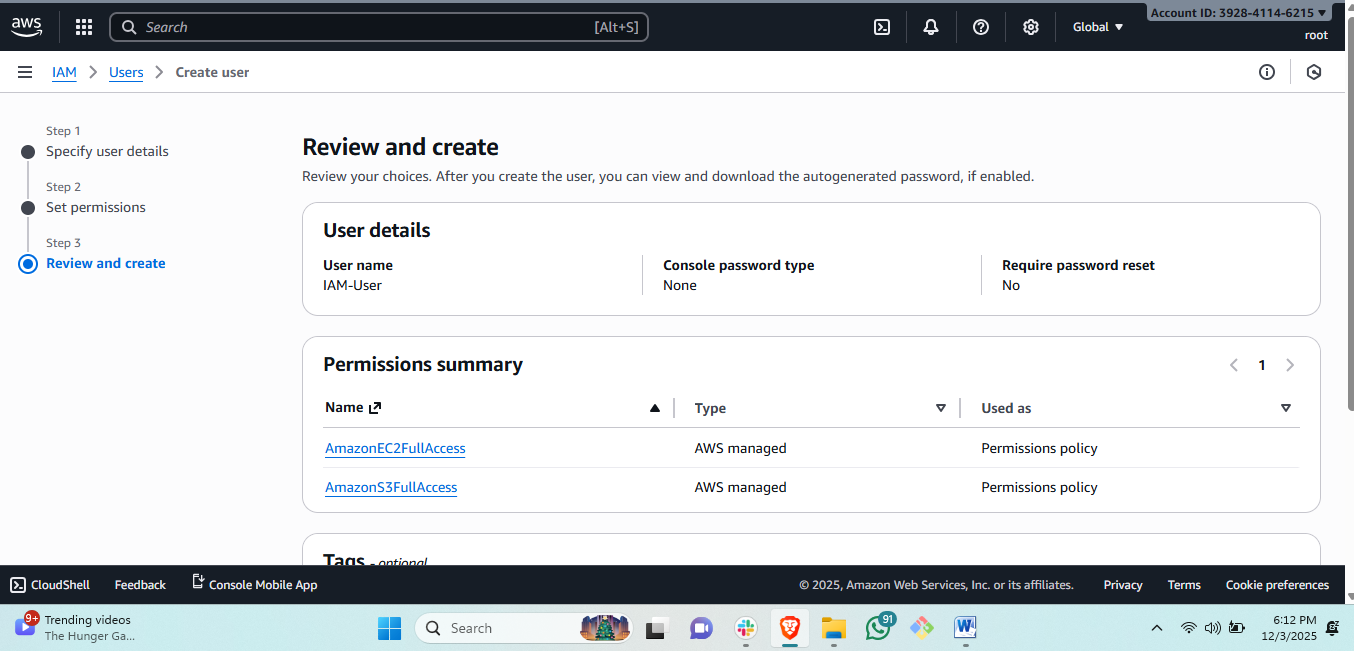
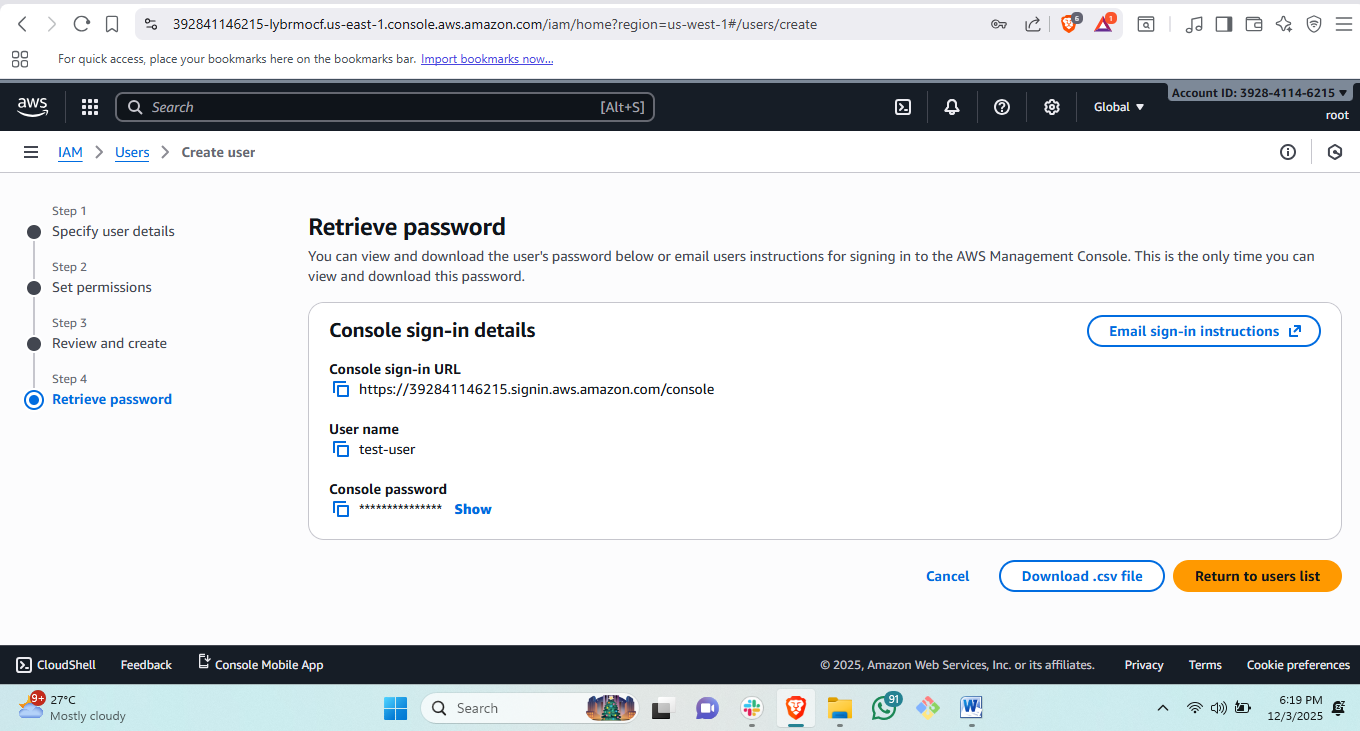
Mohammed Mujahed Batch-16 IAM-Tasks

1. Create one IAM user and assign EC2 and S3 full access roles.

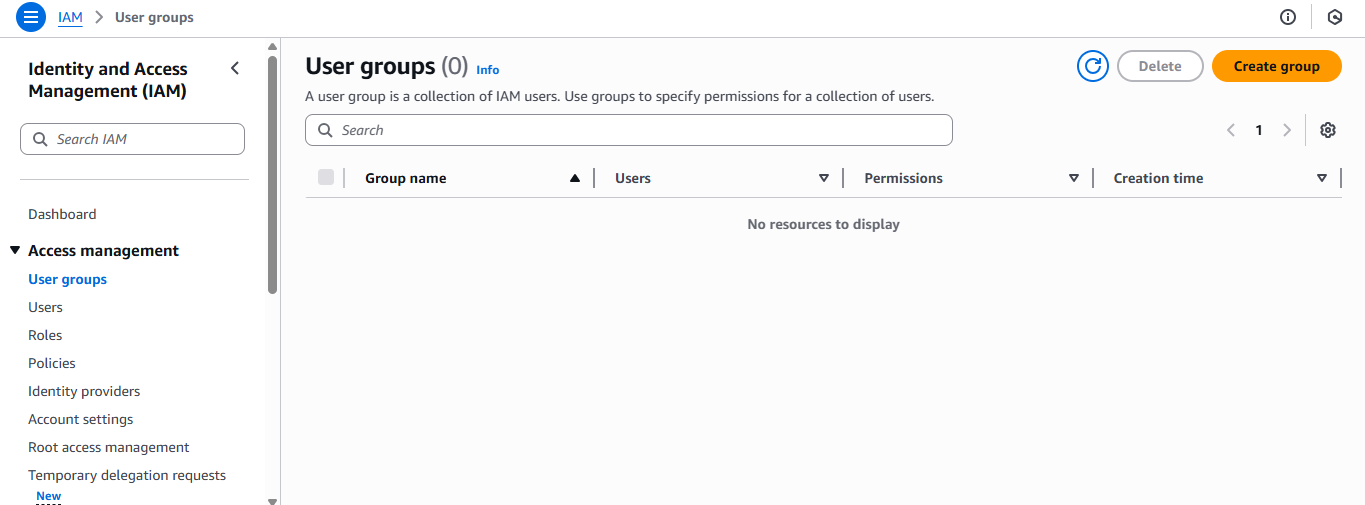


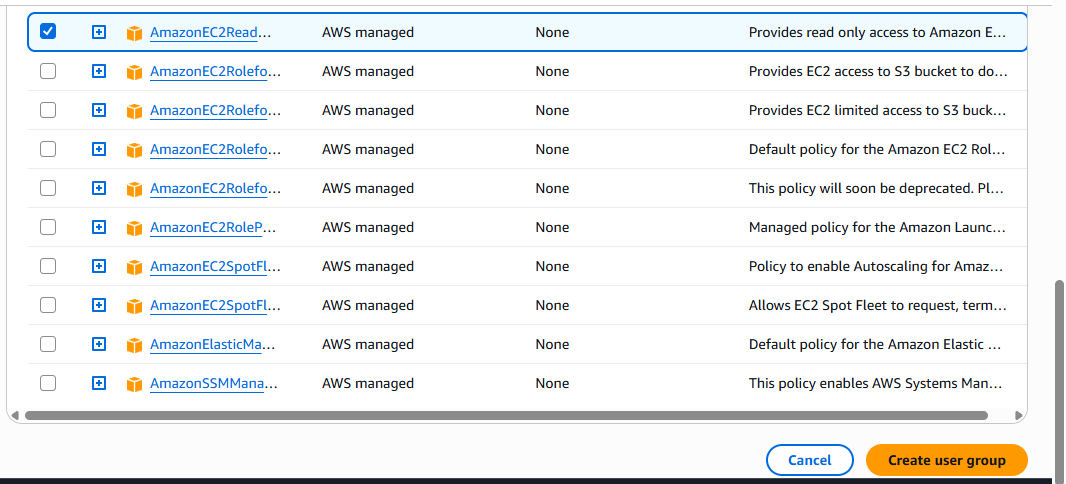
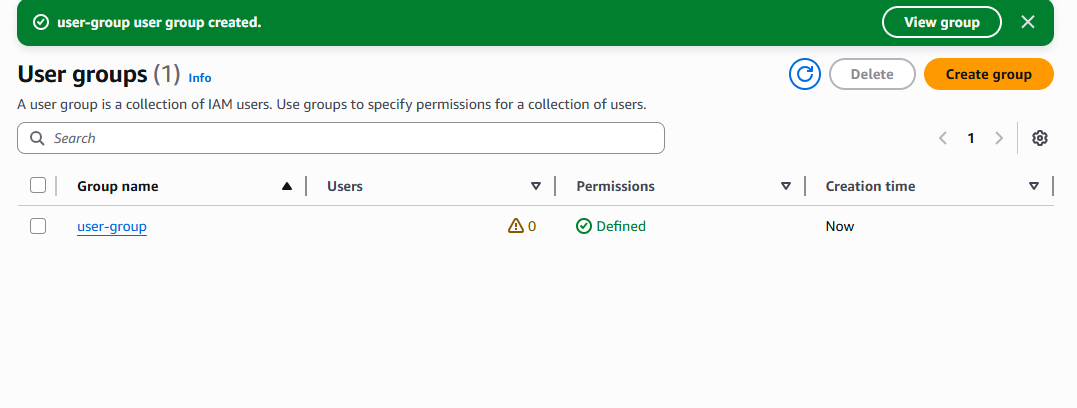




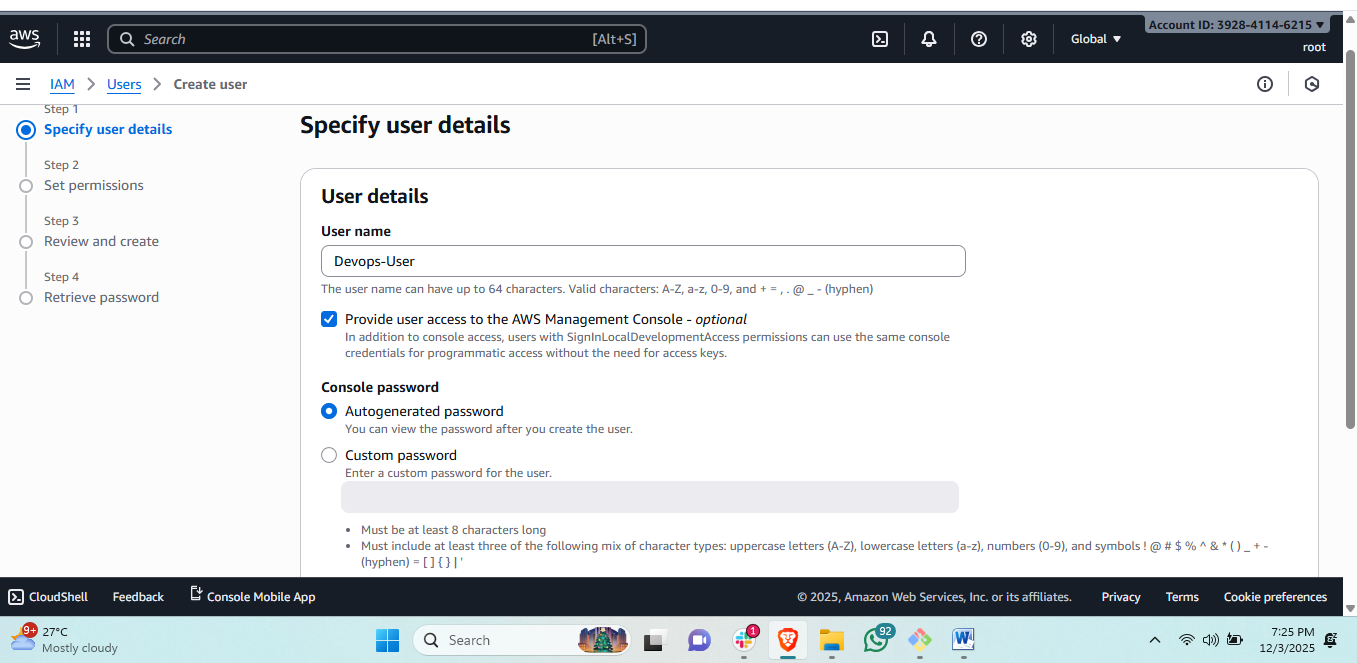
Steps to create user:   
# first go to IAM by searching then click on click on users and create user.  
#give name of user and attach policy and create user and it will create a user.  
# copy the console sign in URL to the team member and console password he can login.

1. Create one group in IAM and assign read access for EC2.

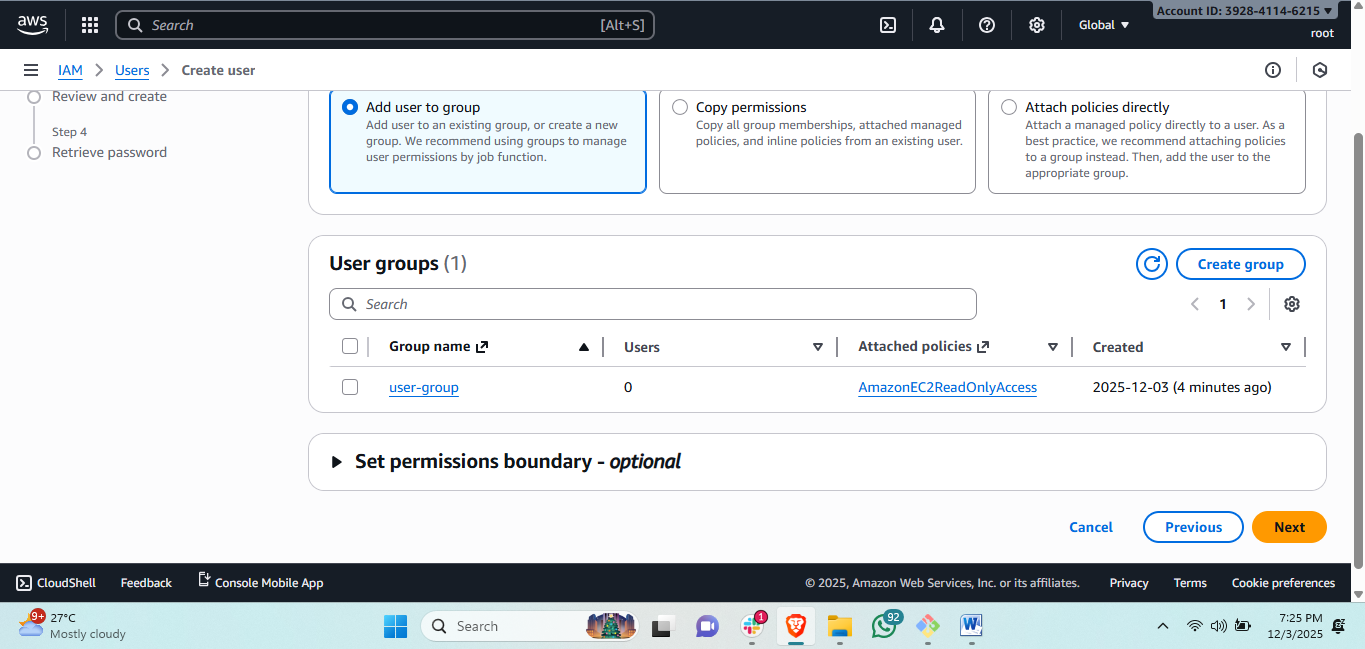
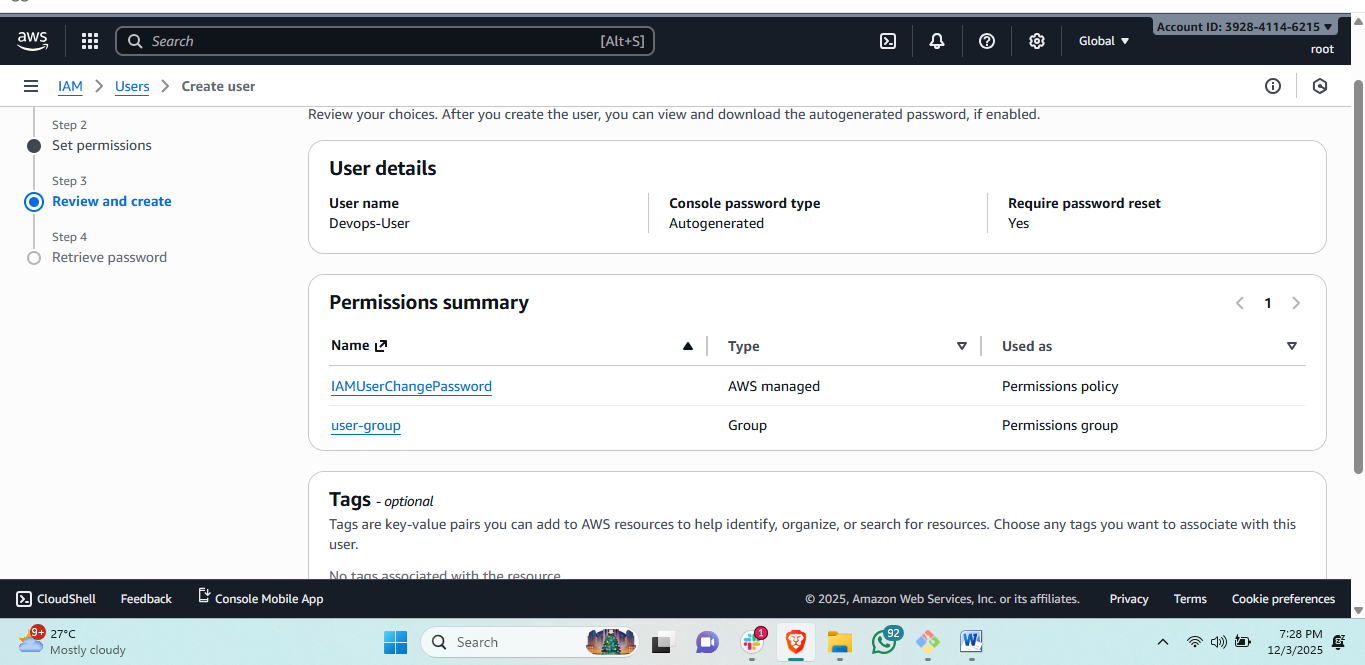
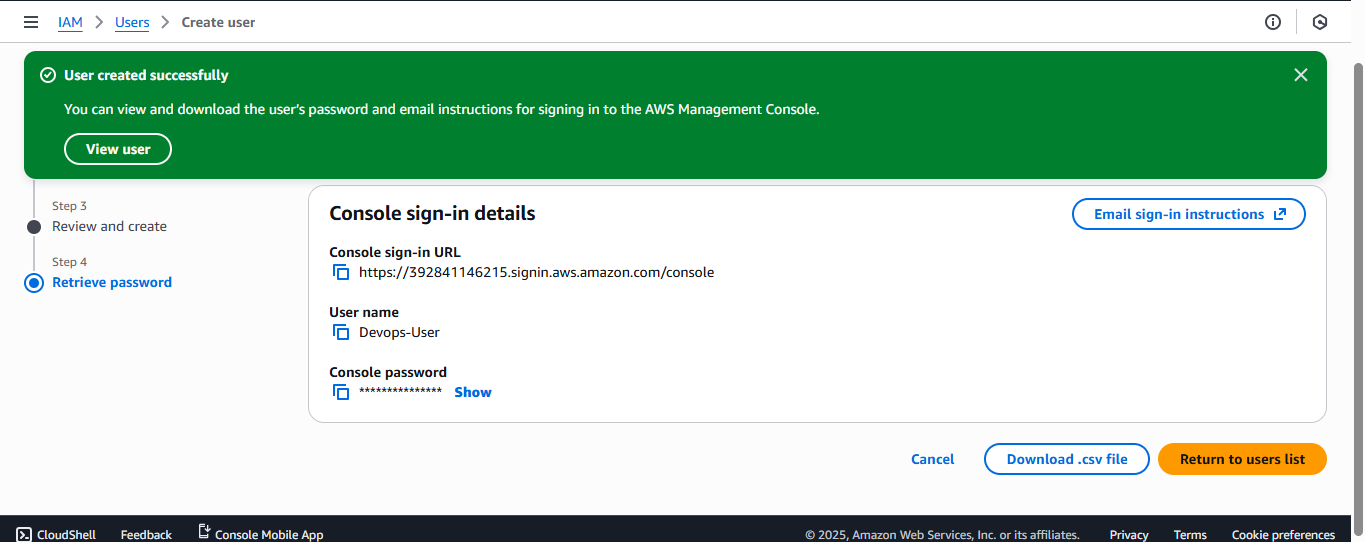


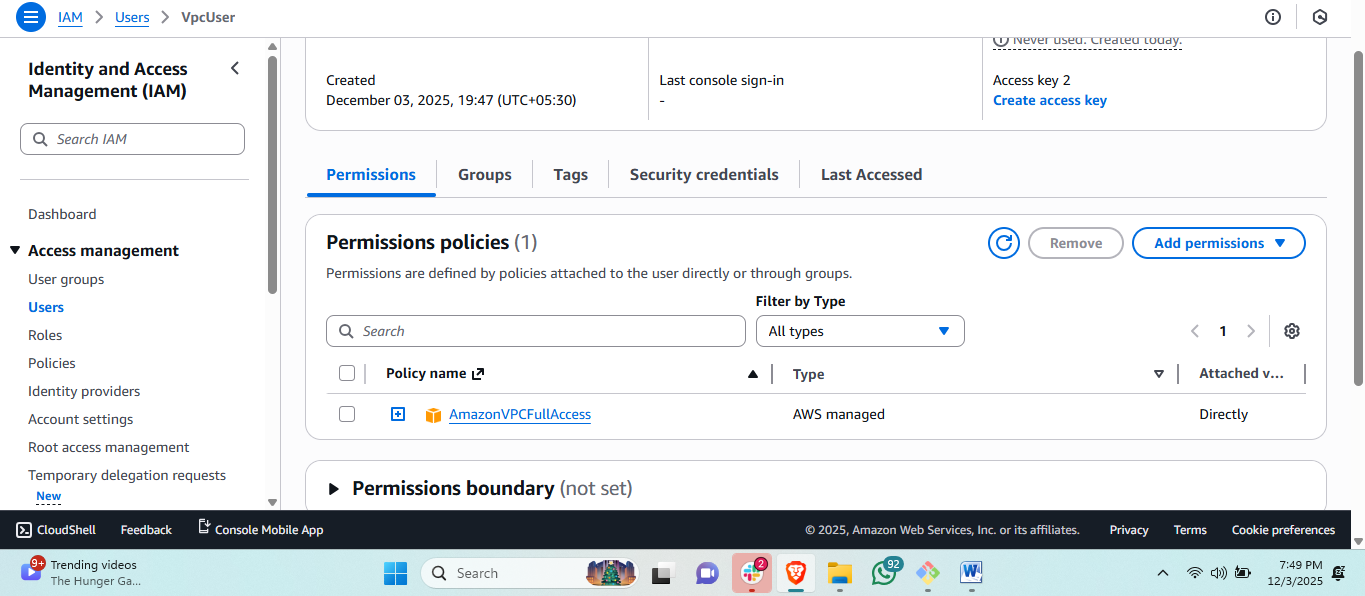
  
  
steps: to create a group need to search IAM and the click on create group.  
#then give a desired name and select the particular policy you want to add.  
#then scroll down and click on create group.

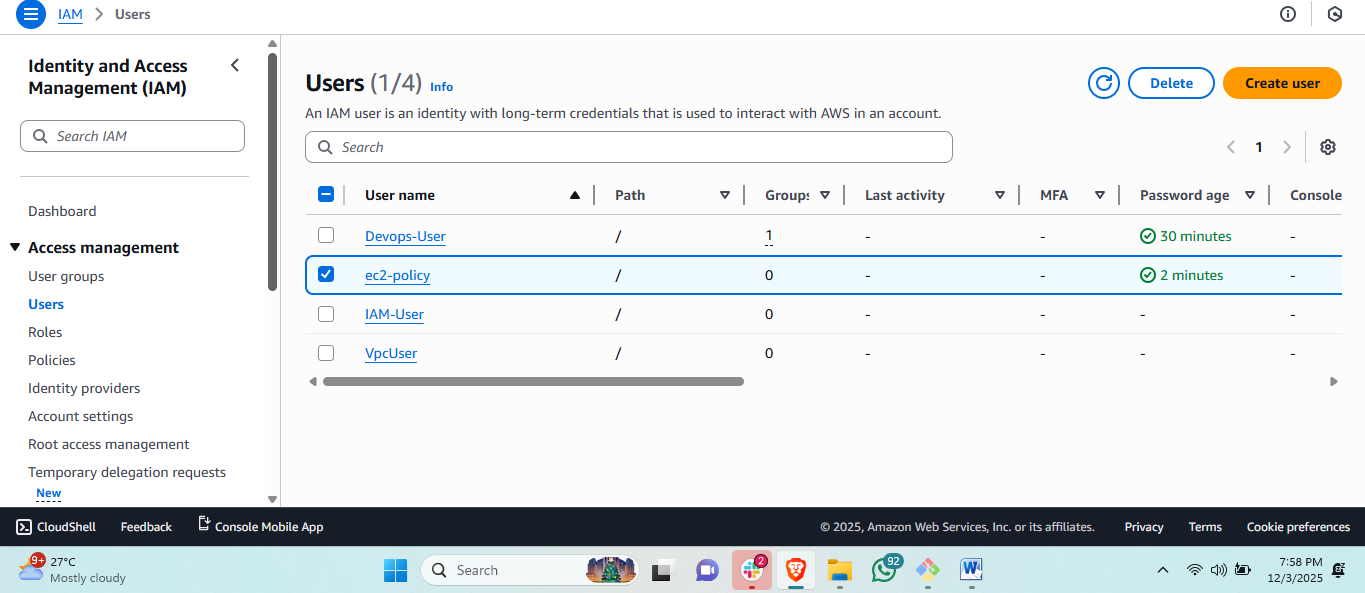
1. Create a new user named "Devops" and add to the group created in task 2.

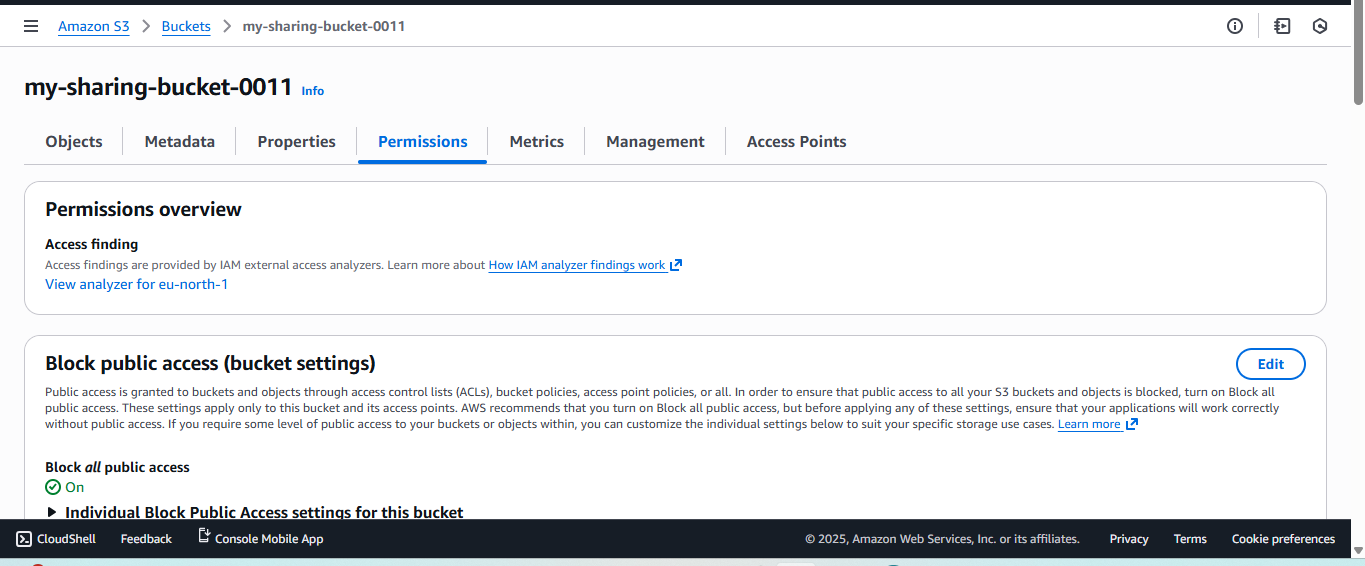
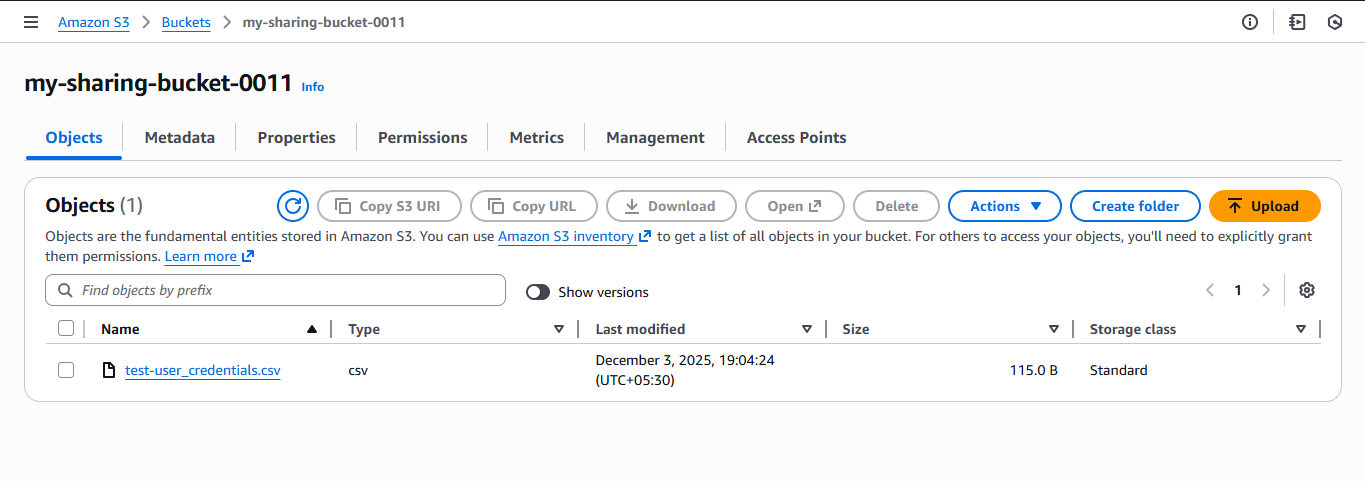
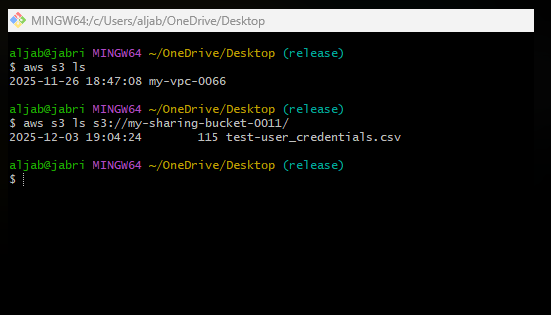


Steps: create a user called Devops-User

  
then add to the group as it shows in below and the polies which attach to the group.  
  
  
then create user then it willconnect with adding to the group and the group policy will attach to the user. 

1. Write a bash script to create an IAM user with VPC full access.  
   steps: first we need to connect to the instance and create a bash file and paste the script to create a vpcuser with VPC full access and configure aws cli in this server  
   #then run this script the user will create with VPC full access.  
     
     
     
     
     
   
2. Create an IAM policy to allow EC2 access for a specific user in specific regions only.

  
steps: first I created a user named with ec2-policy.  
#then go to user permission and add policy and inline policy and paste the script and click on attach policy and give name of policy.  
#then back to the users and click on user.  
  
here you can see the ec2-policy user having the ec2-access this policy is created by json inline policy.

1. We have two accounts: Account A and Account B. Account A user should access an S3 bucket in Account B.  
     
     
     
       
     
     
   first we create a bucket with the unique name then select this bucket and click on permissions then add policy for sharing the bucket to your team member.  
     
   add this policy in your policy and add the team member amazon id and your bucket name in it.  
     
     
   {
2. "Version":"2012-10-17",
3. "Statement":[
4. {
5. "Sid":"AllowAccountAUserAccess",
6. "Effect":"Allow",
7. "Principal": {
8. "AWS":"arn:aws:iam::ACCOUNT\_A\_ID:user/SomeUser"
9. },
10. "Action":[
11. "s3:GetObject",
12. "s3:PutObject",
13. "s3:ListBucket"
14. ],
15. "Resource":[
16. "arn:aws:s3:::bucket-in-account-b",
17. "arn:aws:s3:::bucket-in-account-b/\*"
18. ]
19. }
20. ]
21. }  
      
    then check in your team member in **aws cli**   
    then write this in your team member aws cli : command   
    # aws s3 ls s3://bucketname/  
    this command will show in your friend cli your bucket information.