**AWS TASK**

**IAM:-**

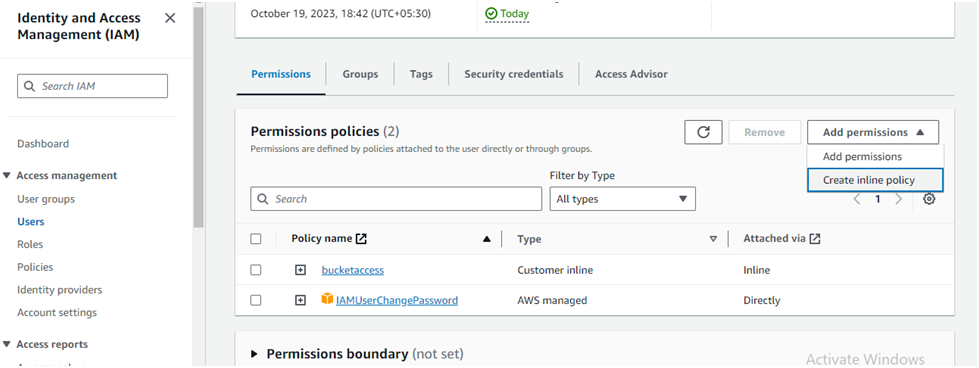
**Policy**

1. **Create a policy to access all objects in a specific bucket.**

**Ans:** Step 1: First to create user

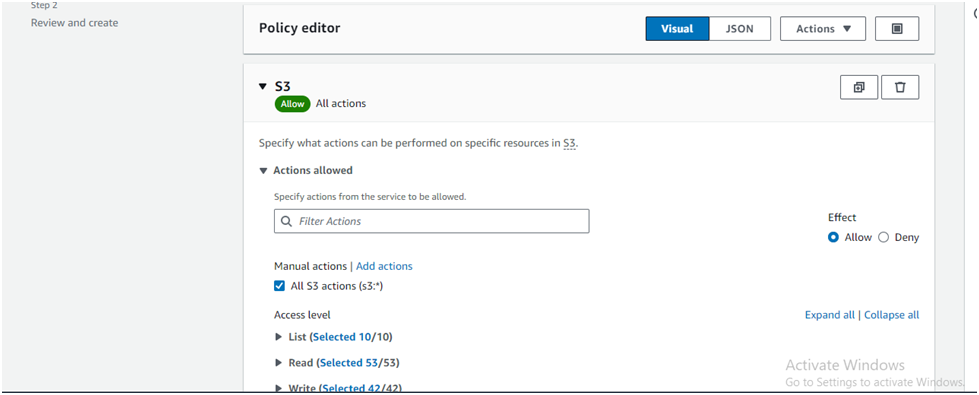
Step 2 : Choose a particular one user then click Add Permission.

Step 3 : choose Create inline policy.

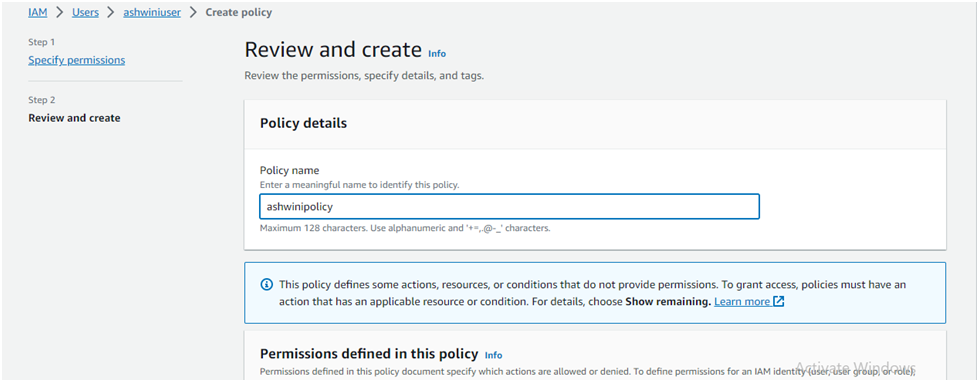


Step 4 : Select the service name >>> S3

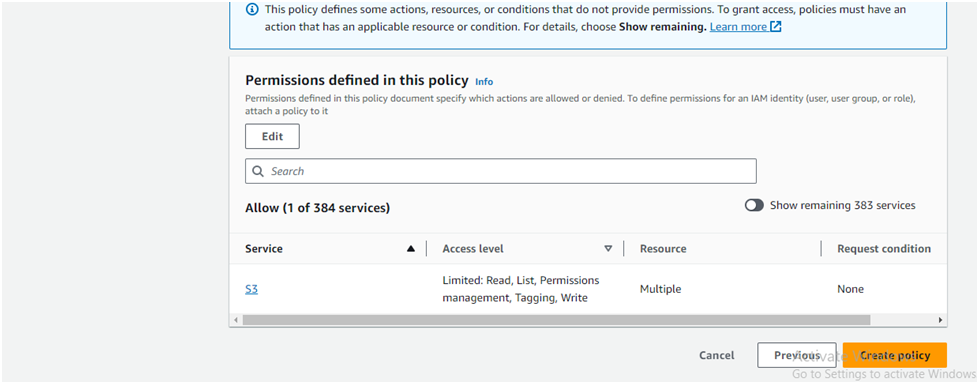
Step 5: Choose Action button and give all s3 bucket permission.



Step 6: Give Policy name



Step 7: Click on Create policy



**2.Create a policy to access only 2 objects in a specific bucket.**

**Ans:** Step 1: First to create user

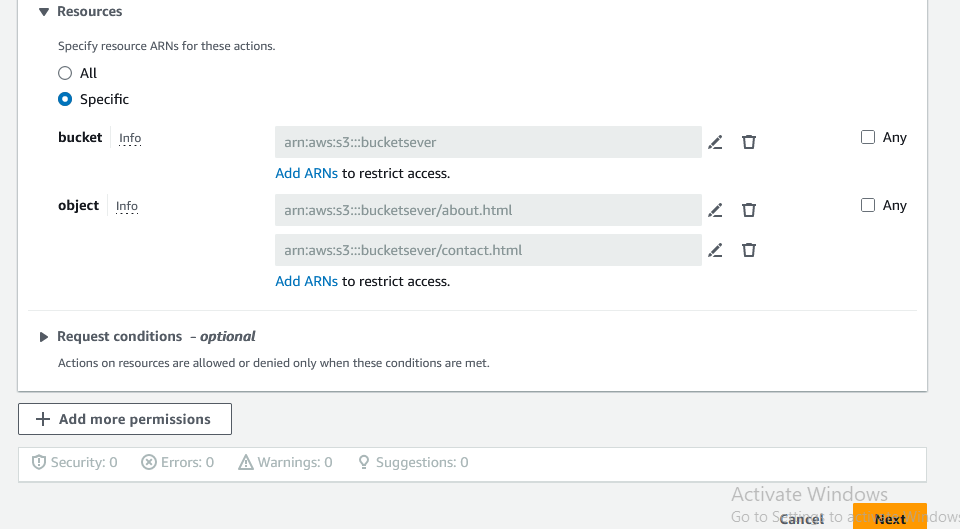
Step 2 : Choose a particular one user then click Add Permission

Step 3 : choose Create inline policy.

Step 4 : Select the service name >>> S3

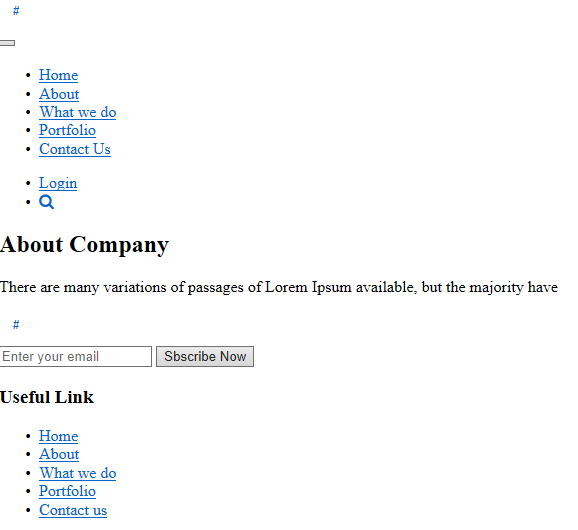
Step 5 : In Action allow choose option list bucket, list all bucket, get bucket , get object, location, put object, put bucket.

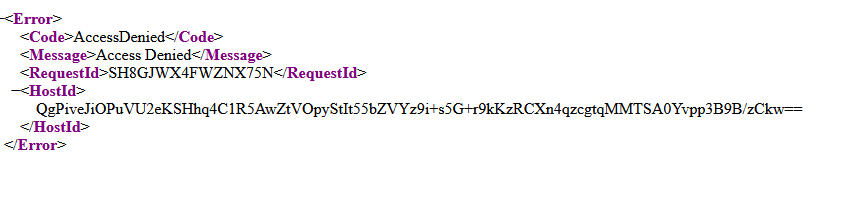
Step 6 : In Resources add Bucket ARN & Object ARN



Step 7 : Give Policy Name & choose Create policy option.

Step 8: Login with 2nd user & select object you applied permission on & download it & check status. Two object access permission remaining object denied permission





**3. Create a policy to deny the access of Specific bucket.**

**Ans :** Step 1: First to create user

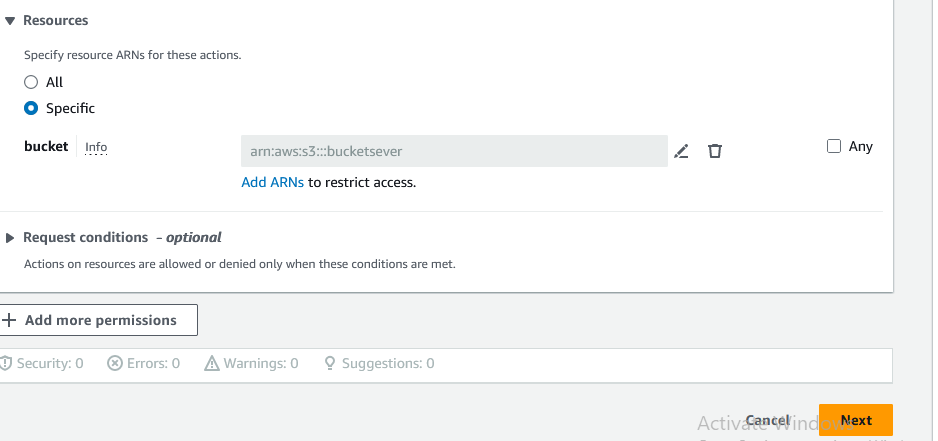
Step 2 : Choose a particular one user then click Add Permission

Step 3 : choose Create inline policy.

Step 4 : Select the service name >>> S3

Step 5 : In Action allow choose option list bucket, get bucketpolicy, put bucketpolicy, Location.

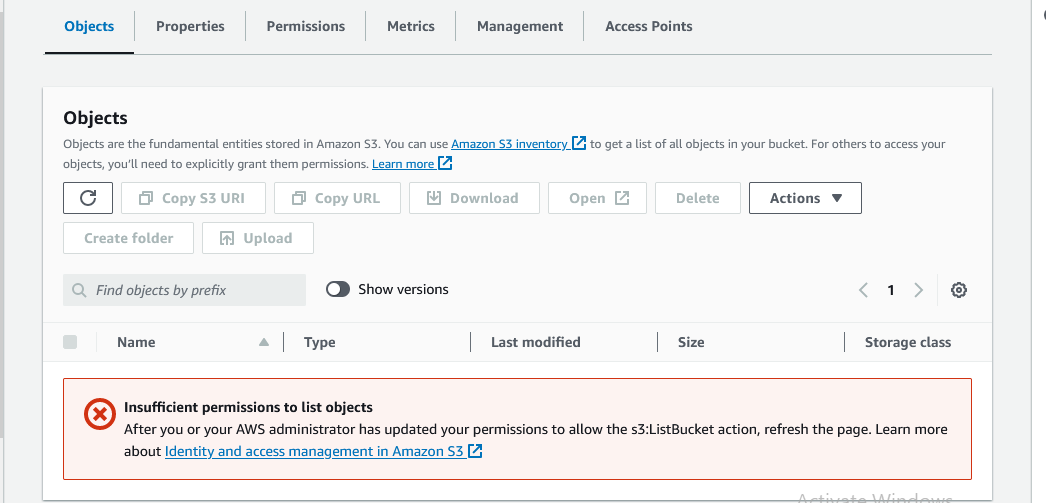
Step 6: In Resources add Bucket.ARN



Step 7 : Give Policy Name & choose Create policy option.

Step 8 : Login with 2nd user & select object you applied permission on & download it & check status. Two object access permission remaining object denied permission.

Step 8 : Choose Bucket which you are given permission



**4. Create policy to create the user only and can attach policy to them.**

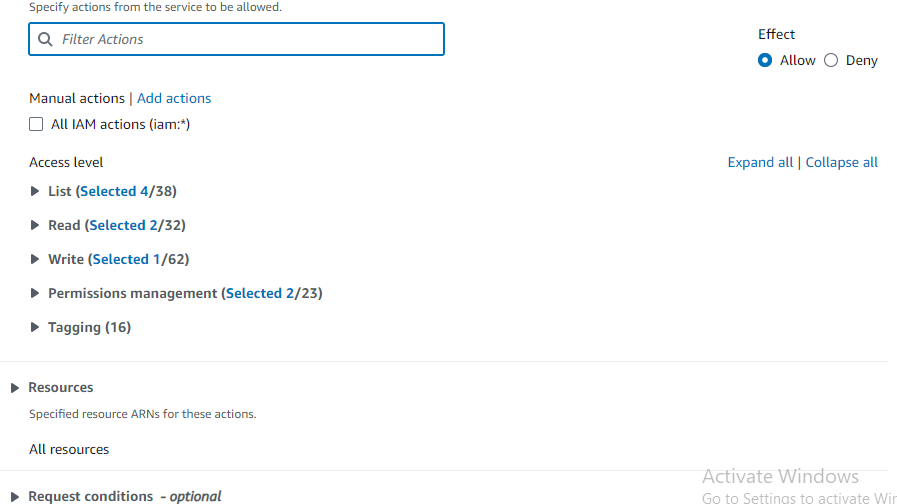
**Ans:** Step 1: First to create user

Step 2 : Choose a particular one user then click Add Permission

Step 3 : choose Create inline policy.

Step 4 : Select the service name >>> IAM

Step 5 : In Action allow choose option List user, Get user, Create user, Attached user policy, Get Account Password policy, List Policies.



Step 5 : Give Policy Name & choose Create policy option.

**5. Create a policy to place the user in a group only.**

**Ans :**

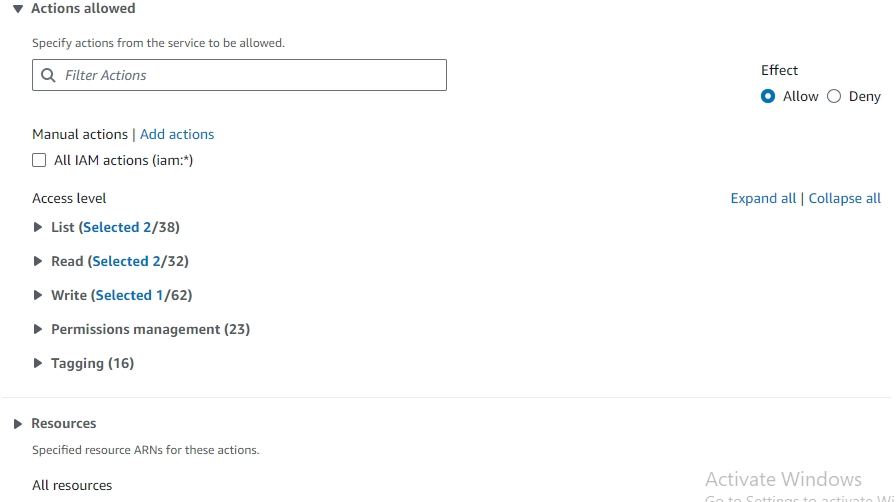
Step 1: First to create user

Step 2 : Choose a particular one user then click Add Permission

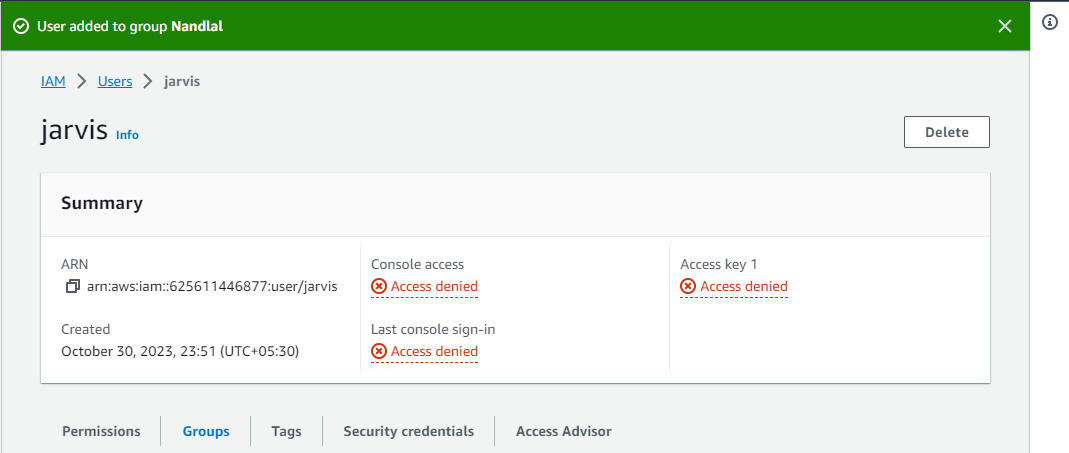
Step 3 : choose Create inline policy.

Step 4 : Select the service name >>>> IAM

Step 5 : In Action allow choose option List User,List Groups, Add User To Group,Get User, Get Group.



Step 6 : Give Policy Name & choose Create policy option. As well as login by user & check in that user create another one user and attach a policy with them.



**6. Policy to get "read" access of all users, groups but not policy.**

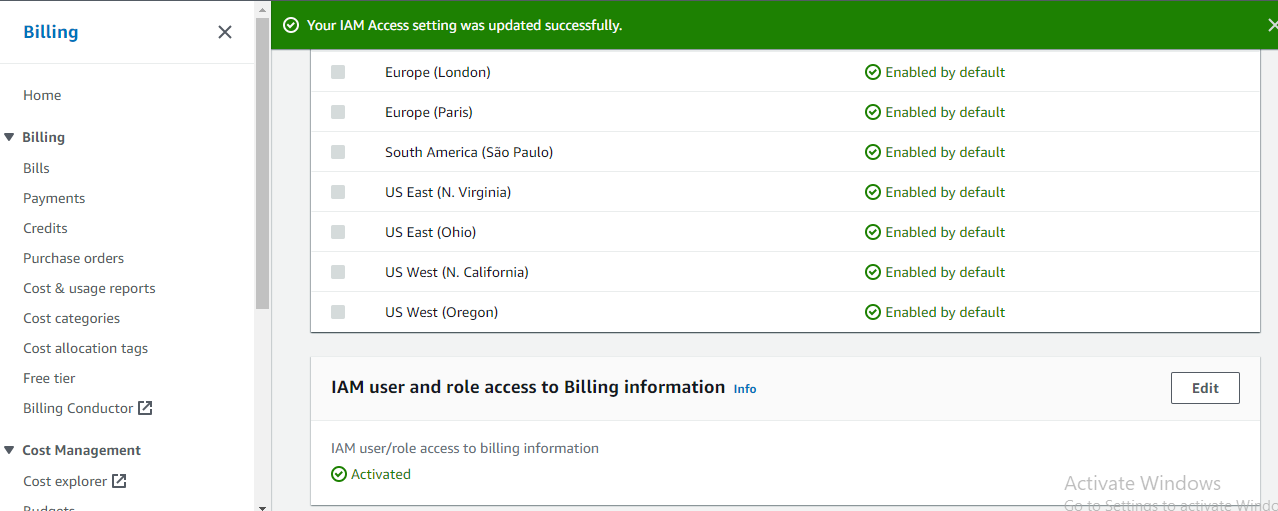
**Ans :**

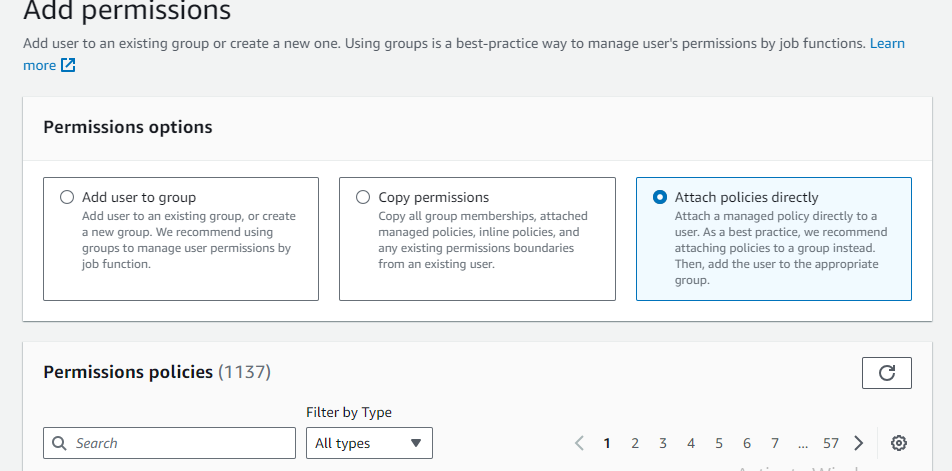
**7.Policy to get access to billing, ec2 and cloudwatch.**

**Ans :**

Step 1: We need to first login with admin account

Step 2 : Click on profile a Go to Account then click on IAM user and role access billing information section & edit then enable access to billing info.

****



**8. How to give access only to northern virginia.**

**Ans :**