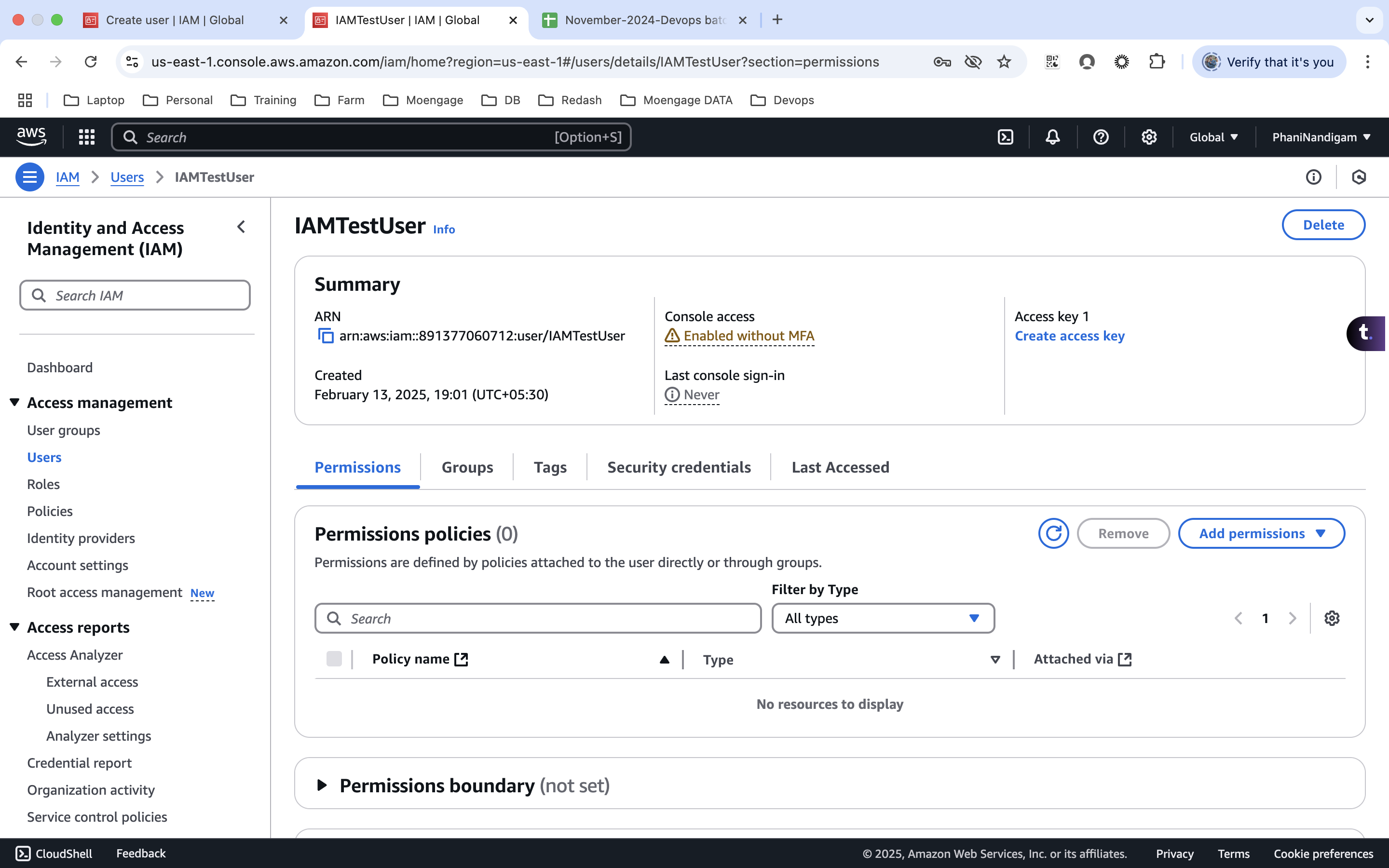
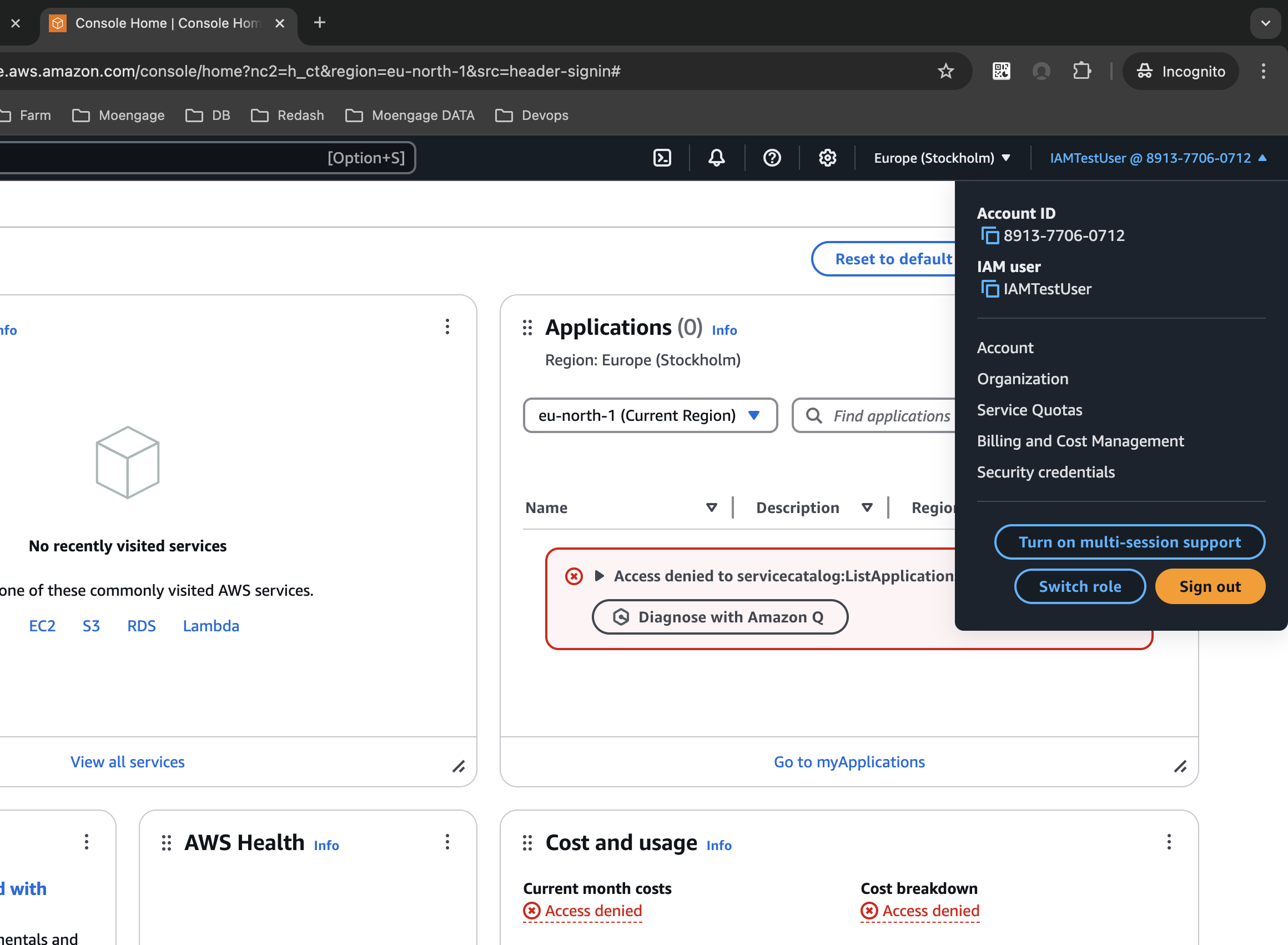
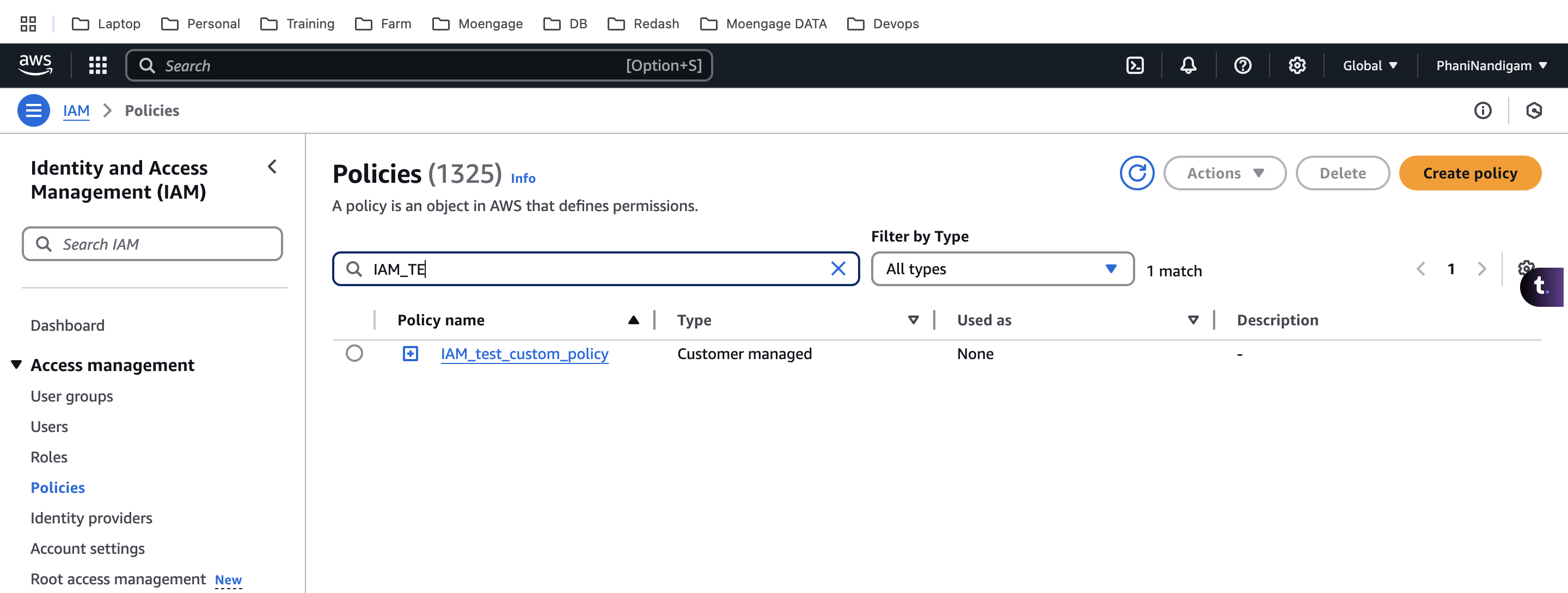
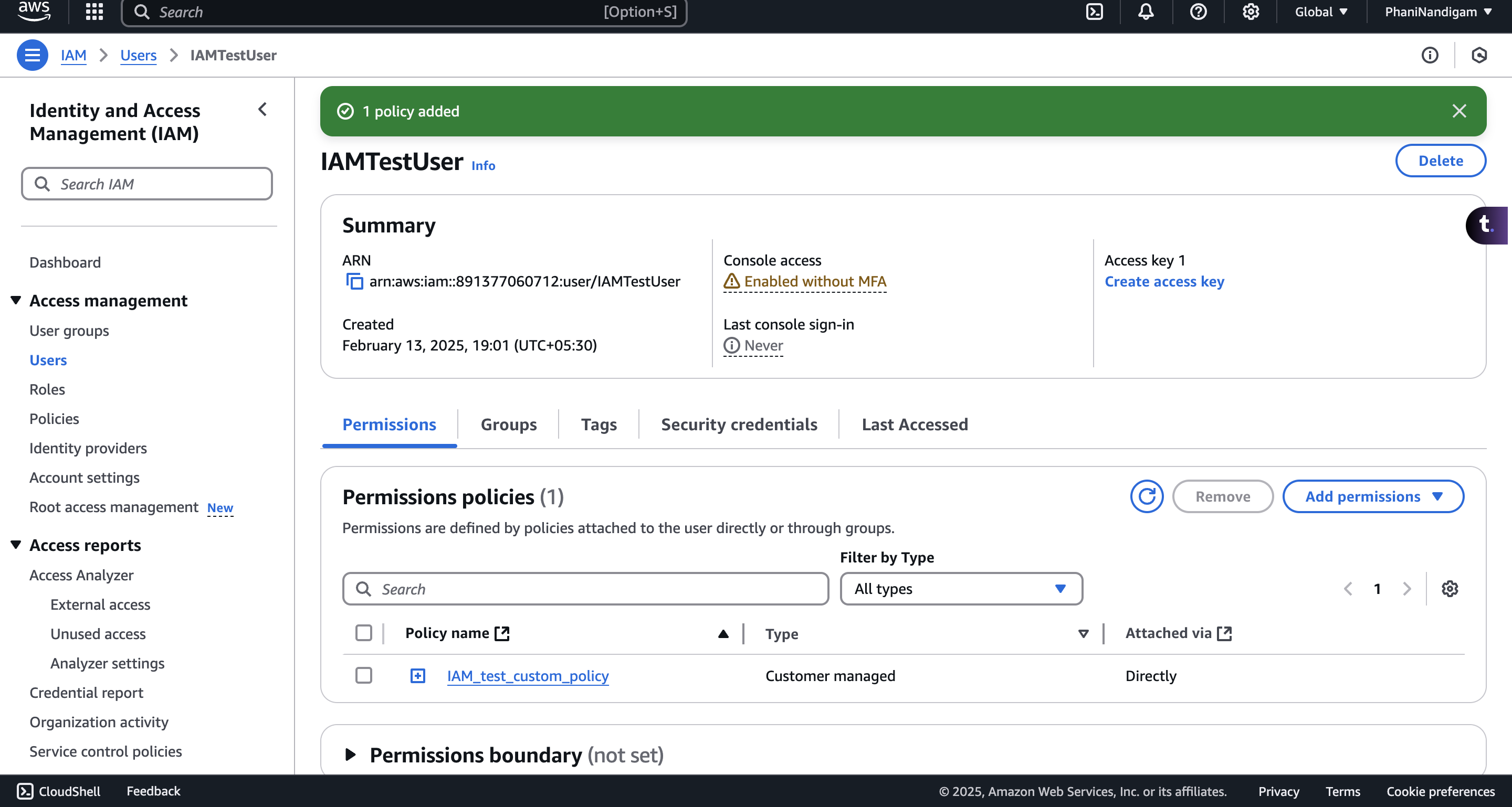
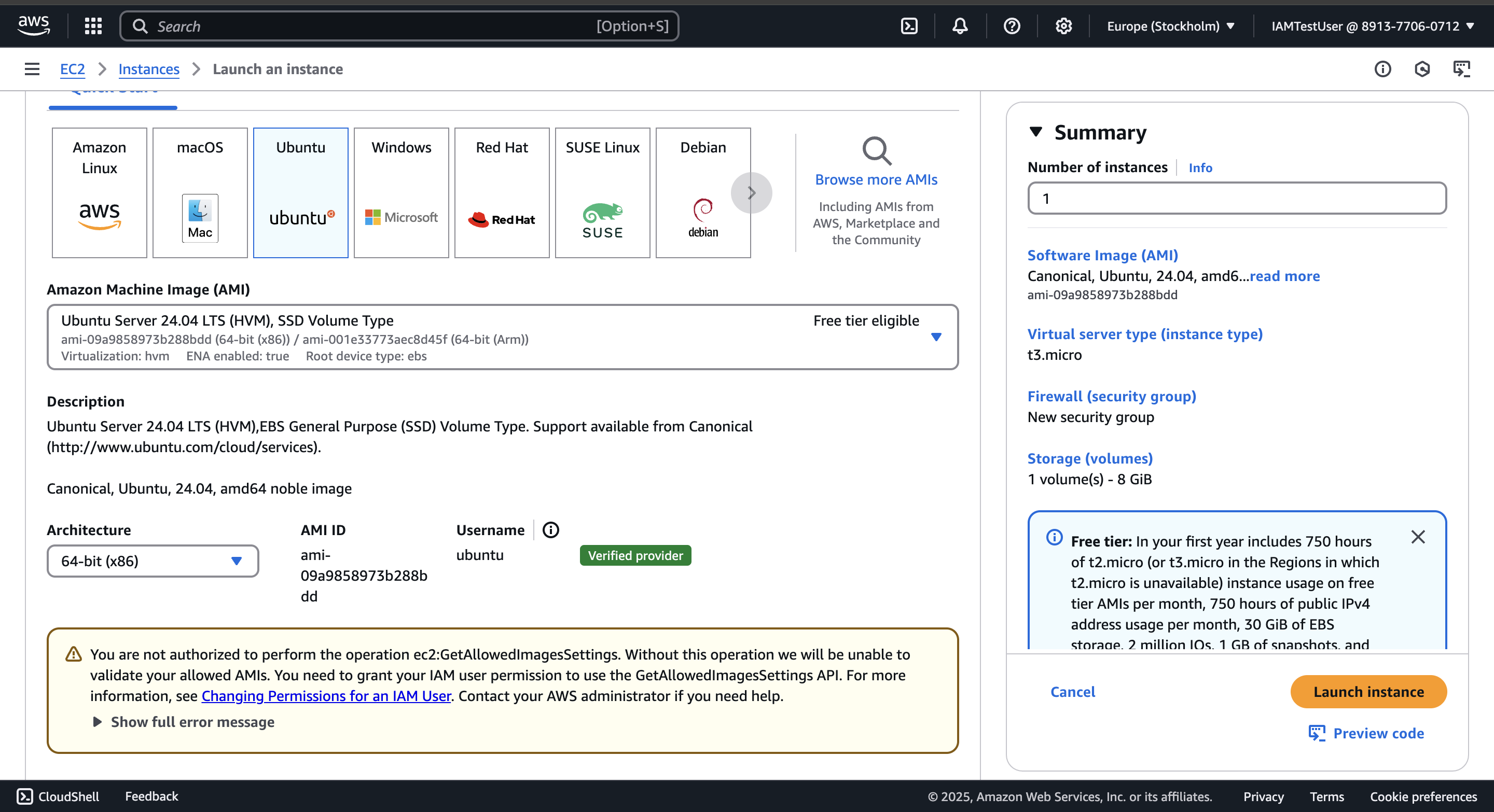
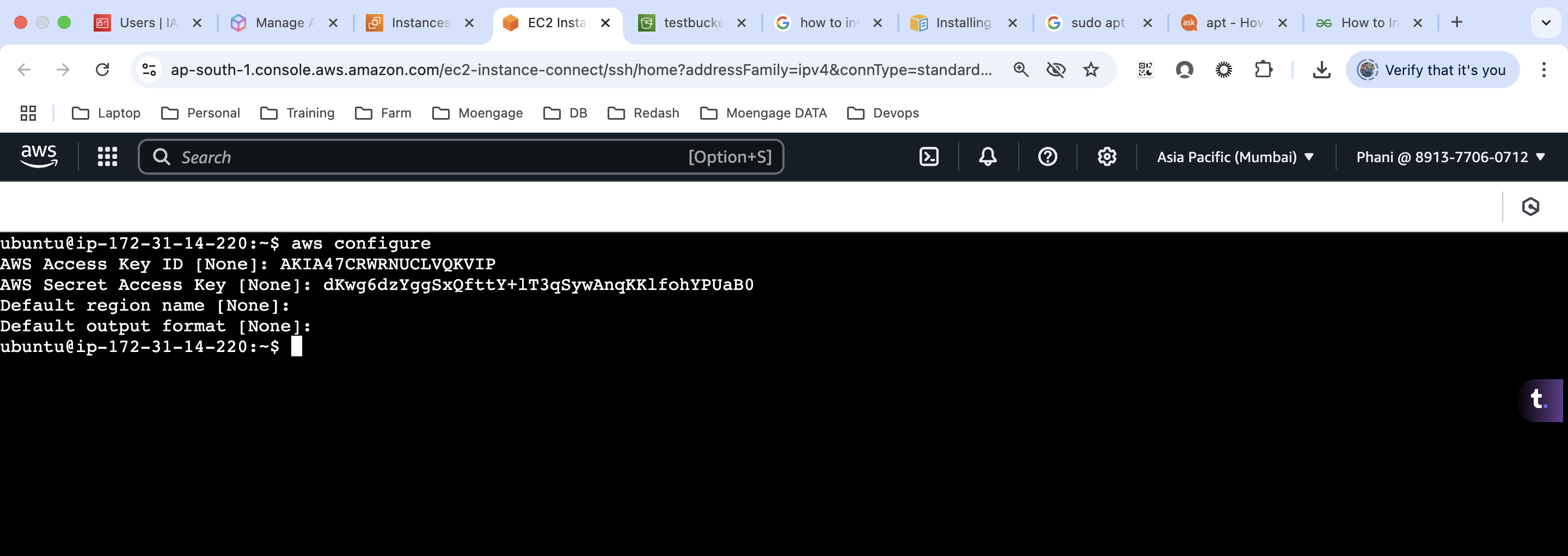
IAM

Create a new custom policy and attach it to user/group having permission of readonly and list for AWS EC2.

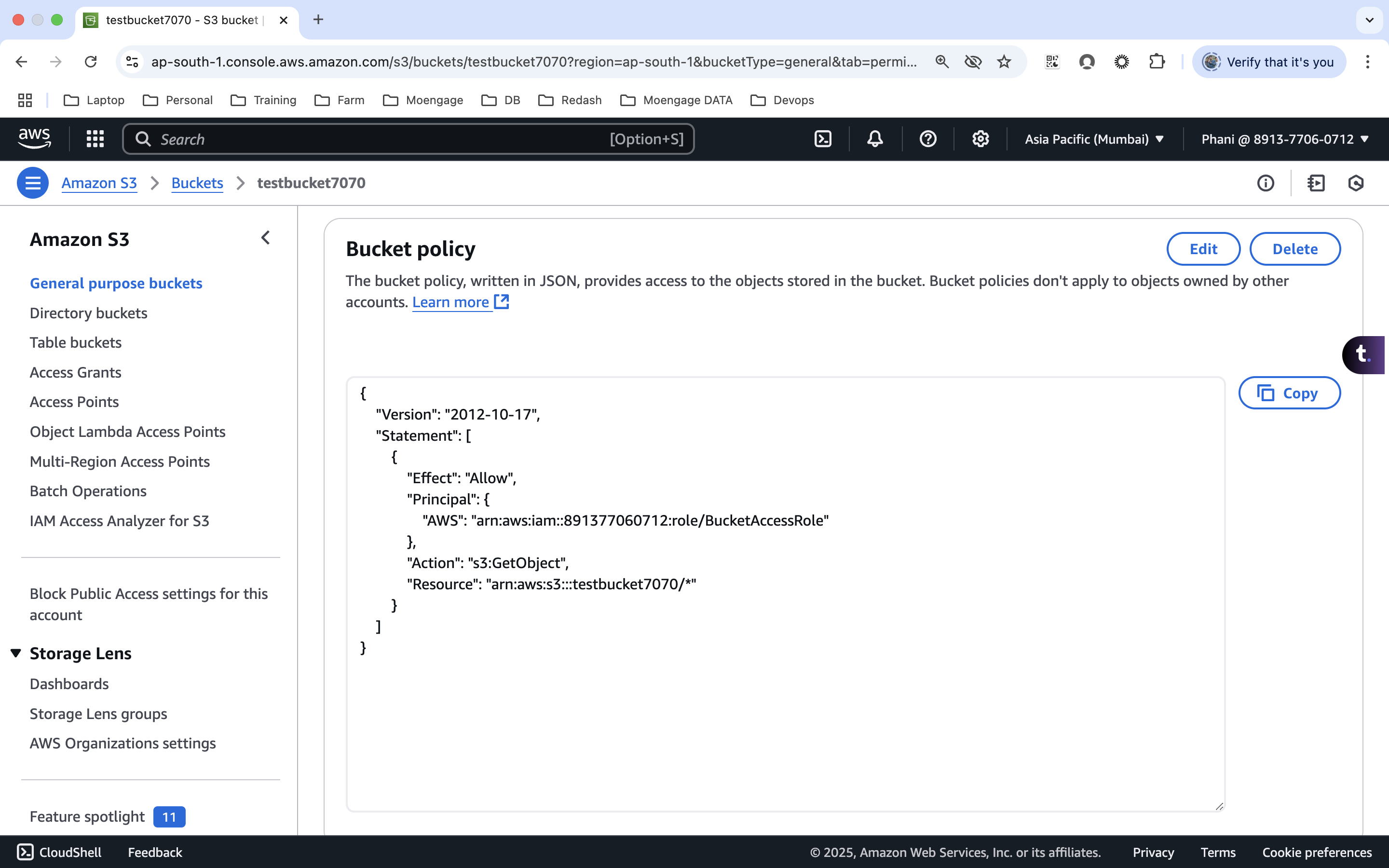
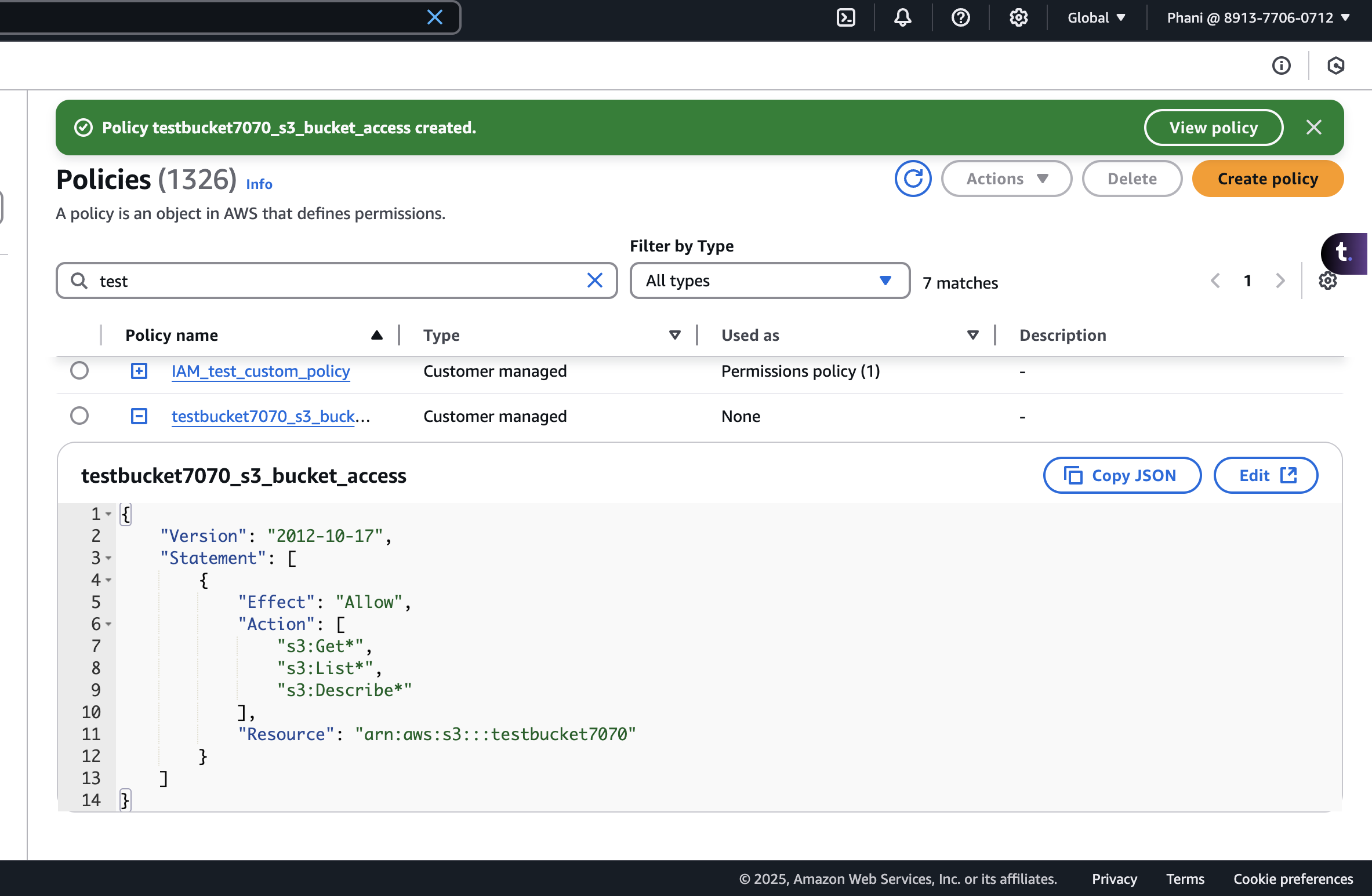
* Created a new IAM user  
  
* Able to login as an IAM User  
  
* Now we need to provide the respective permissions by creating the policy.  
    
    
  A screenshot of a computer

  AI-generated content may be incorrect.
* Attach it to the user  
  
* Not able to create the EC2 due to the policy restrictions  
  

Create a role with S3 readonly access and use that role to access from a ec2 instance. You should use AWS cli to list the objects of the bucket

* install aws cli and connect to the instance  
  

|  |
| --- |
| $ curl "<https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip>" -o "awscliv2.zip" unzip awscliv2.zip sudo ./aws/install |

* Create s3 buckets with the below permissions
  + 
  + Create a policy  
    
  + Create the role and select the policy  
    A screenshot of a computer

    AI-generated content may be incorrect.
  + Now apply this role to the ec2  
    A screenshot of a computer

    AI-generated content may be incorrect.
* Now from the aws CLI, we can access the s3 buckets  
  