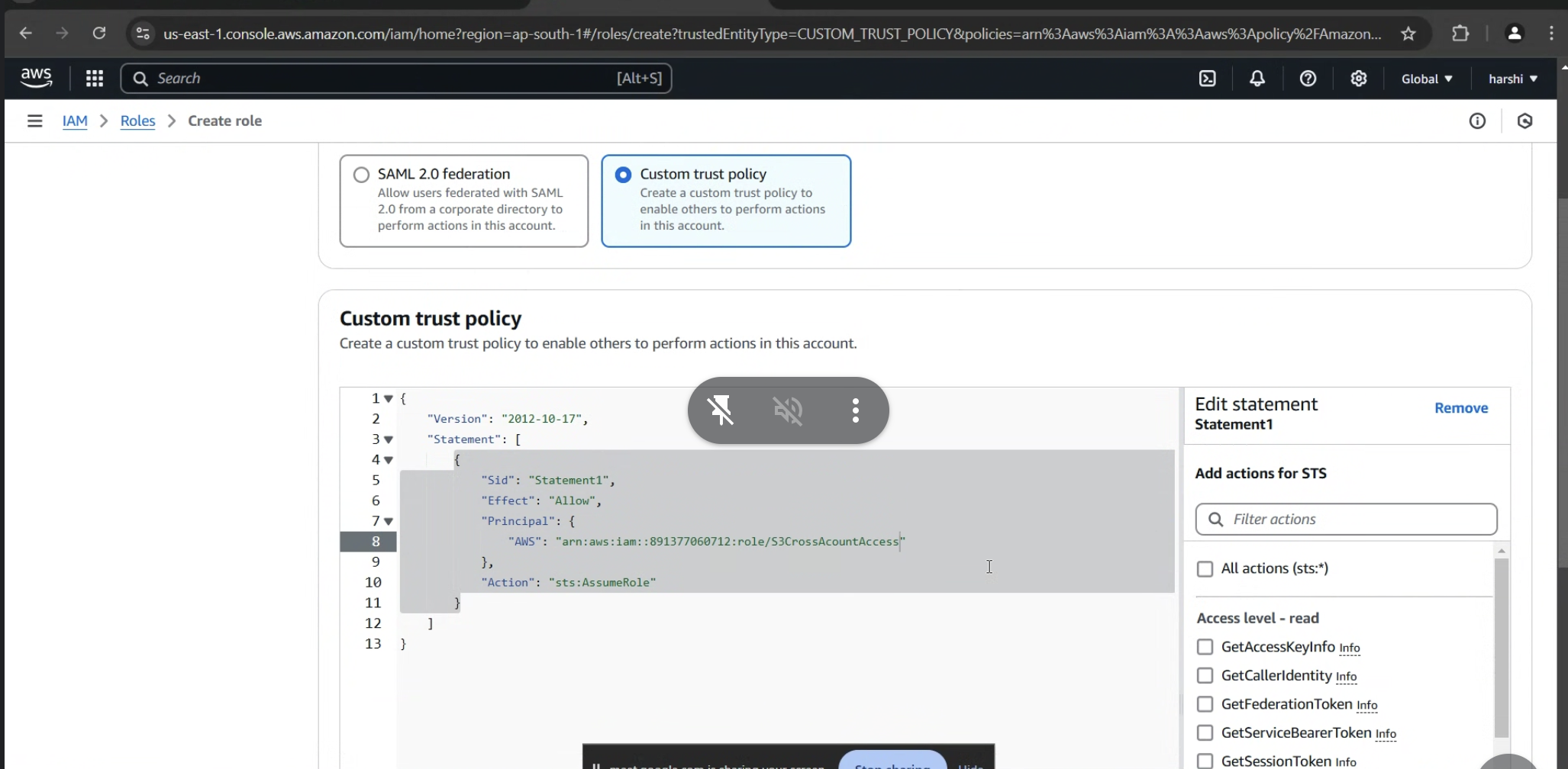
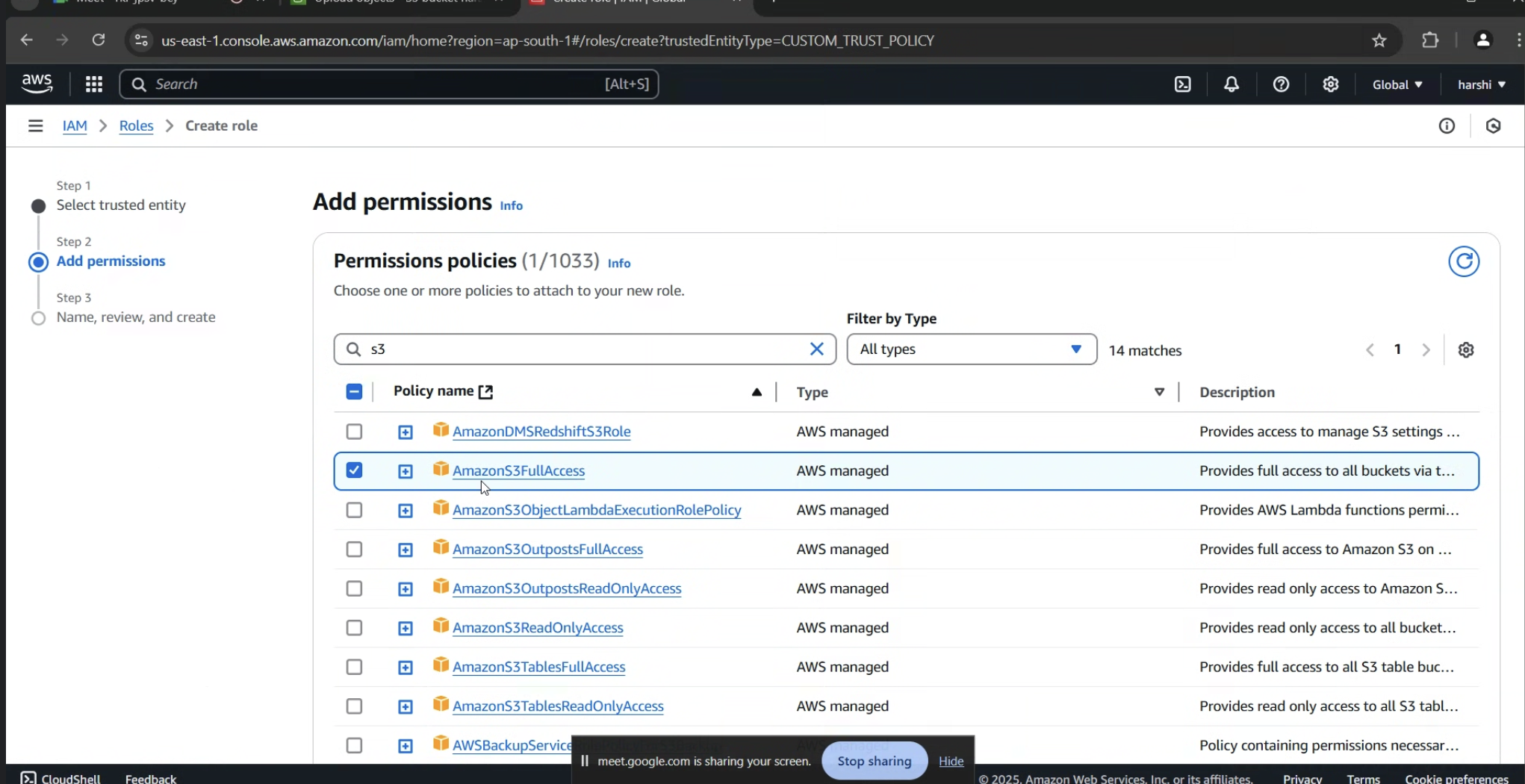
S3

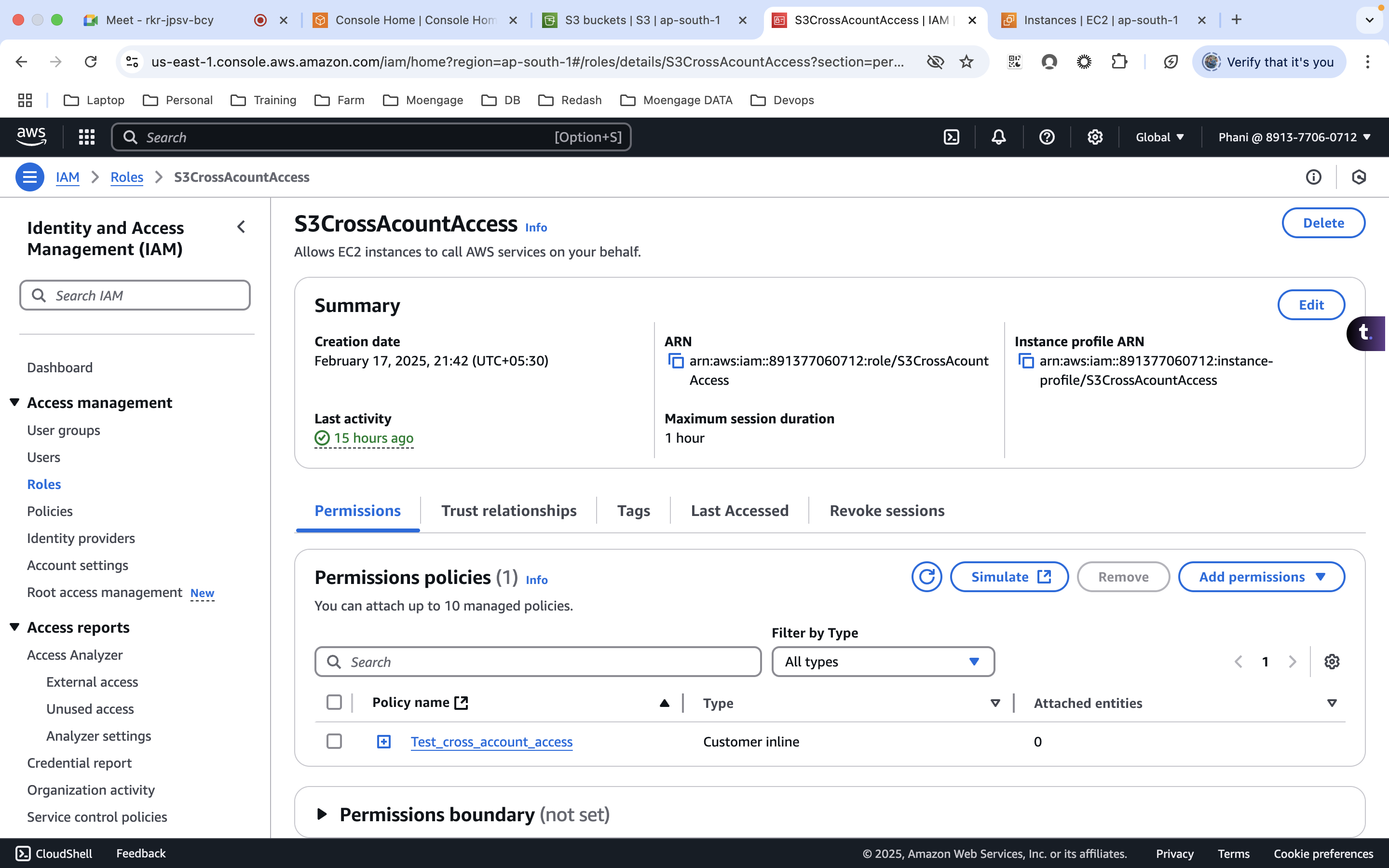
Account A – Phani

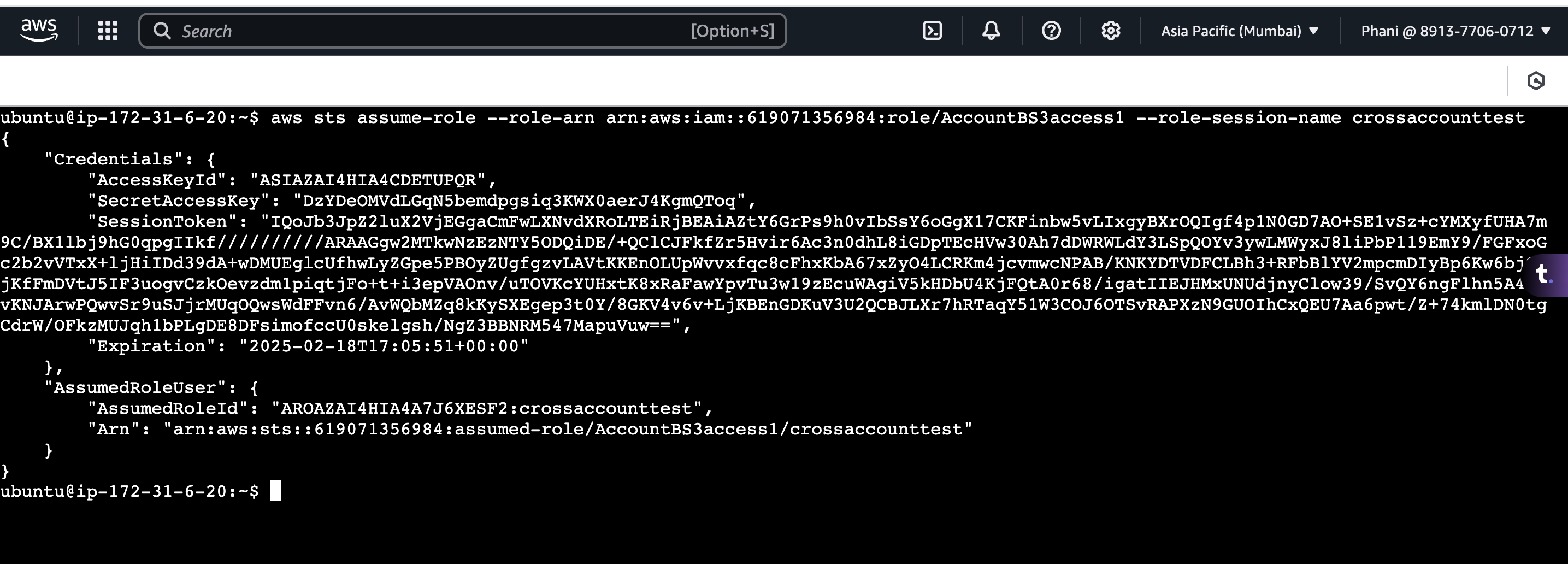
Account B – Harshit K G

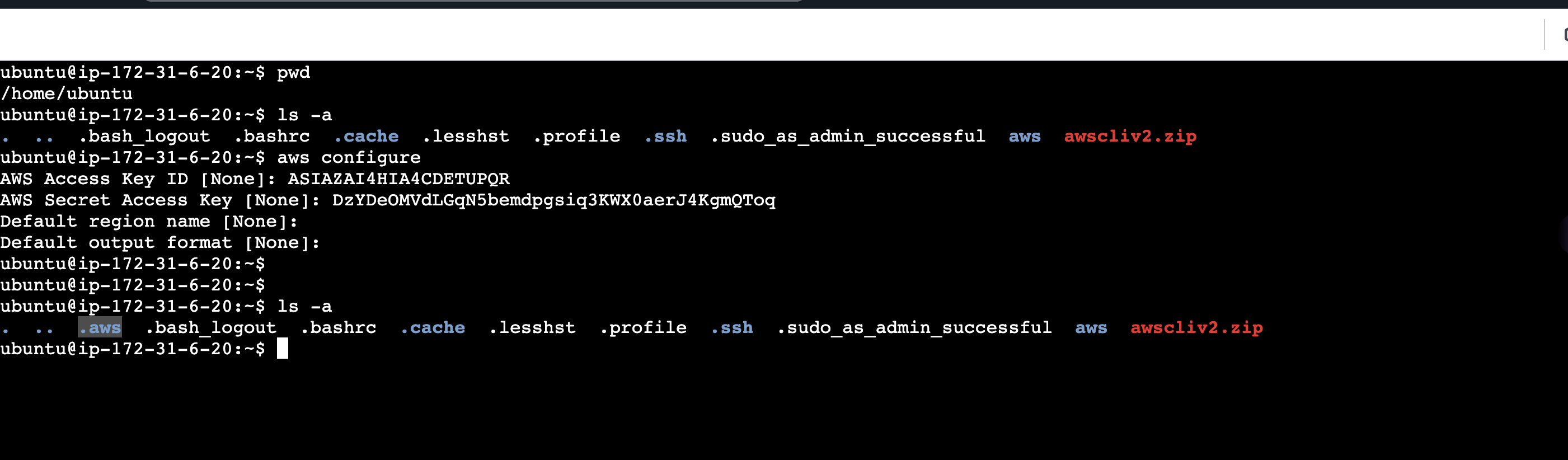
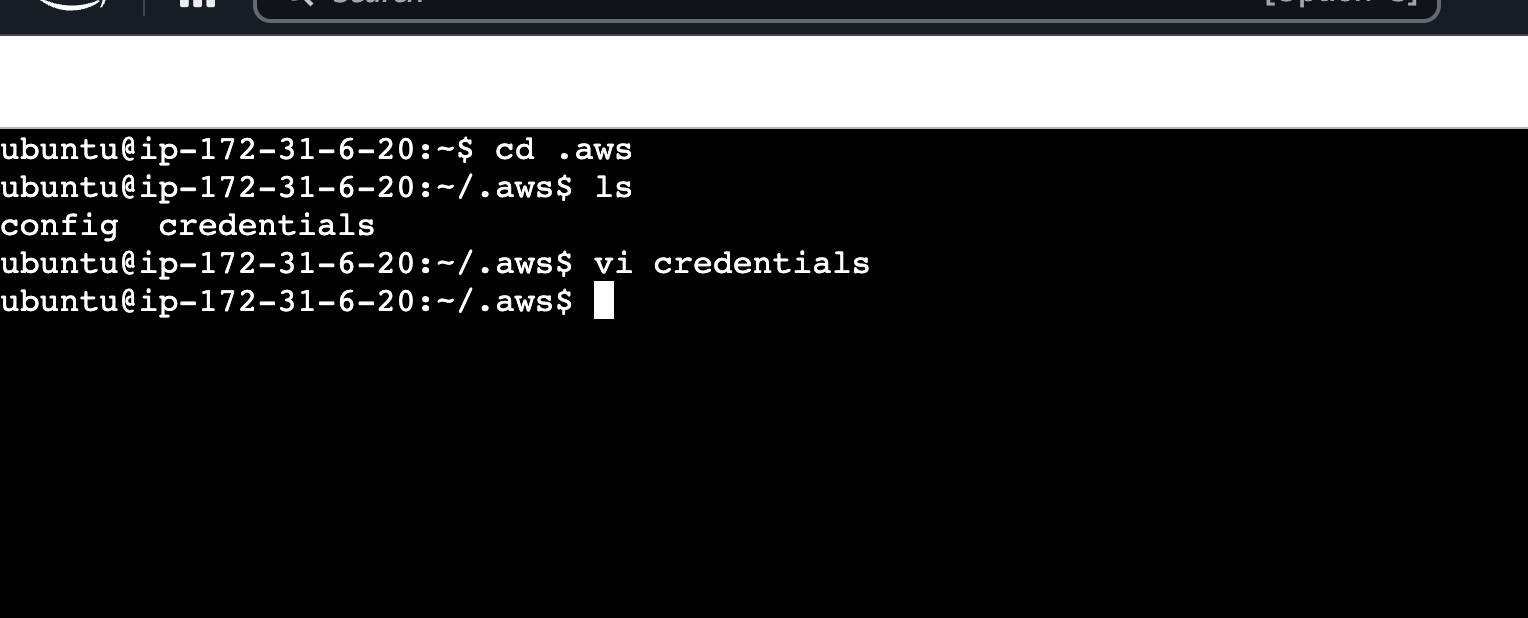
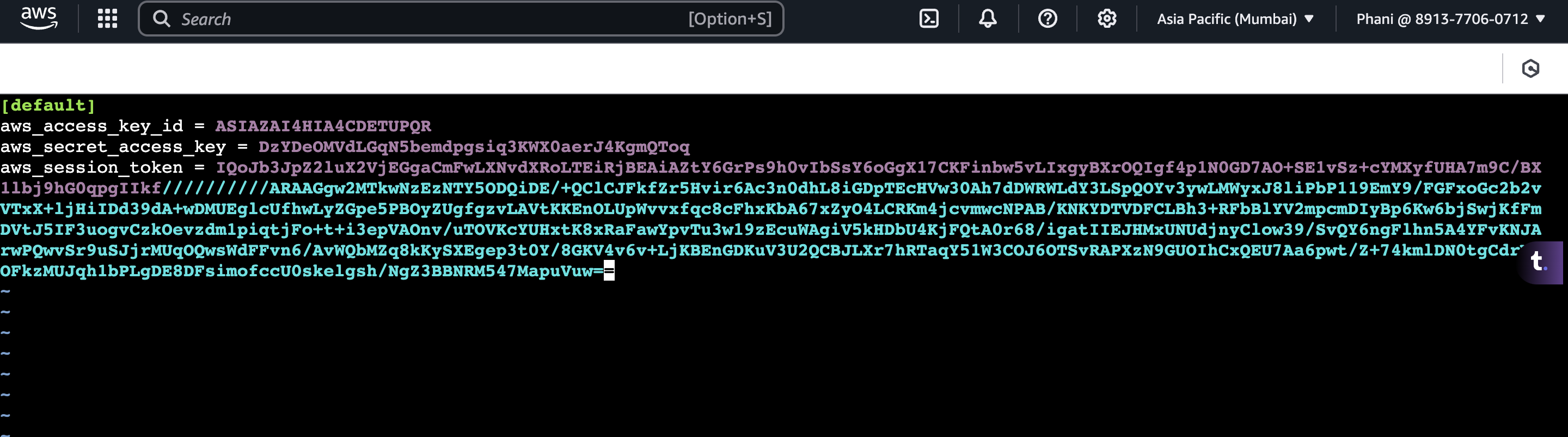
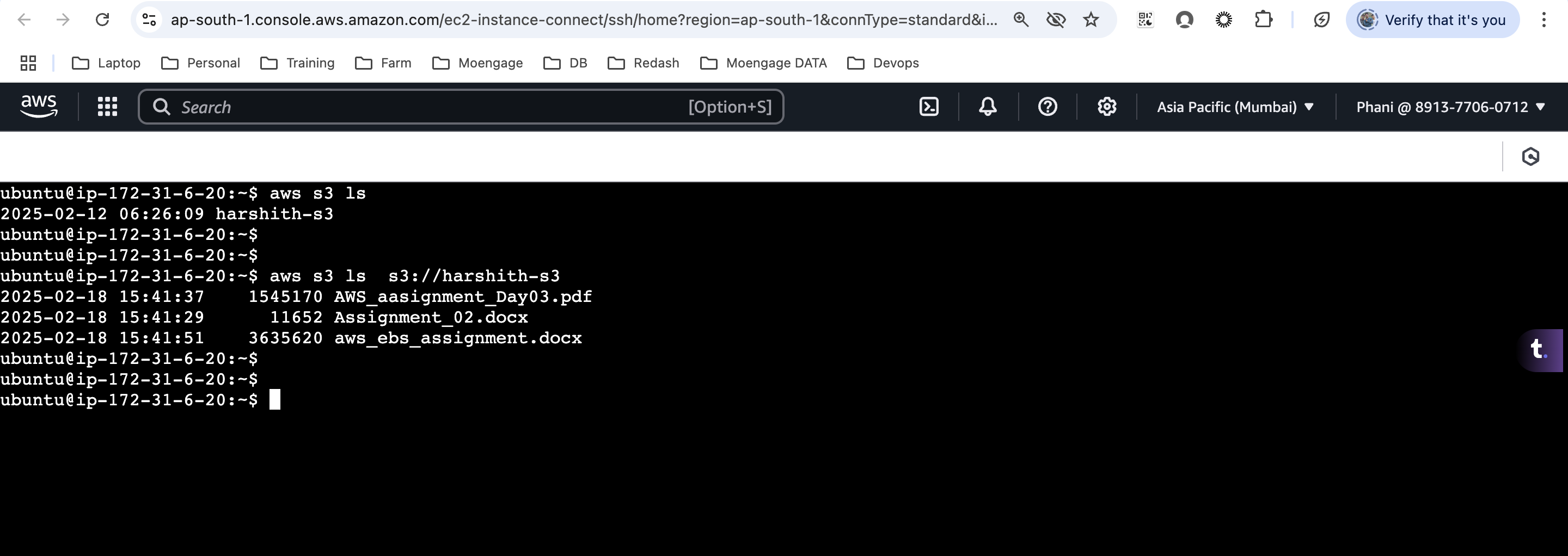
In this case, I will be trying to access the Harshit’s s3 bucket from my ec2 instance.

1. Create a Role in my account.
2. Create an EC2 instance and add the above role to the instance
3. Create a custom policy in the account B and add the ARN details of my role which we have created in step 1 to this role. Provide the s3 full access on the 2nd step.  
     
   
4. Edit the role which we have created in step 1, create inline policy, add STS  
   A screenshot of a computer

   AI-generated content may be incorrect.  
   A screenshot of a computer

   AI-generated content may be incorrect.
5. Once we select the STS and write permission, click on Add ARNs and provide the Account B details(Account ID and ARN of the role)  
     
   
6. Run the below commands to install aws CLI  
   $ curl "<https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip>" -o "awscliv2.zip"  
   unzip awscliv2.zip  
   sudo ./aws/install
7. Run the below command on account A to get the session token, which will be valid for 1 hour.  
   **aws sts assume-role --role-arn arn:aws:iam::619071356984:role/AccountBS3access1 --role-session-name crossaccounttest**



1. Run the aws configure command, which will create a .aws folder  
     
   
2. Add the session token to the credentials file  
     
   
3. Now I can access the s3 bucket  
   
4. Able to upload and download the files to the bucket  
   