Task of IAM- Identification for management

1) Create one IAM user and assign ec2,s3 full access role.

**Steps via AWS Console:**

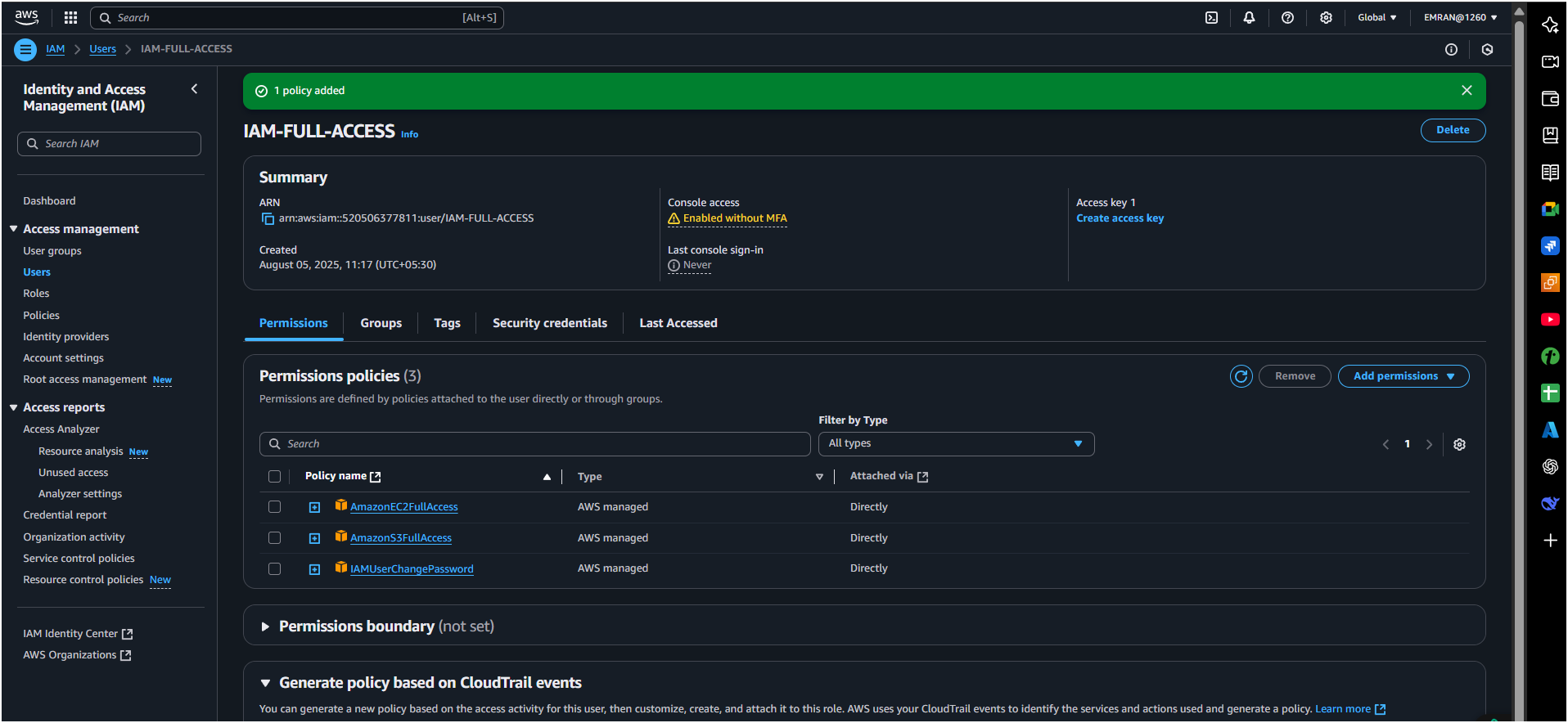
1. Go to **IAM → Users → Create user**.
   * User name: user1.
   * Enable **Programmatic access** and/or **AWS Management Console access**.
2. Attach **Policies**:
   * AmazonEC2FullAccess
   * AmazonS3FullAccess.
3. Complete user creation and download credentials.

**AWS CLI:**

aws iam create-user --user-name user1

aws iam attach-user-policy --user-name user1 --policy-arn arn:aws:iam::aws:policy/AmazonEC2FullAccess

aws iam attach-user-policy --user-name user1 --policy-arn arn:aws:iam::aws:policy/AmazonS3FullAccess



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

**Console Steps:**

1. Go to **IAM → Groups → Create group**:
   * Name: EC2ReadOnlyGroup.
2. Attach **AmazonEC2ReadOnlyAccess** policy.
3. Save.

**AWS CLI:**

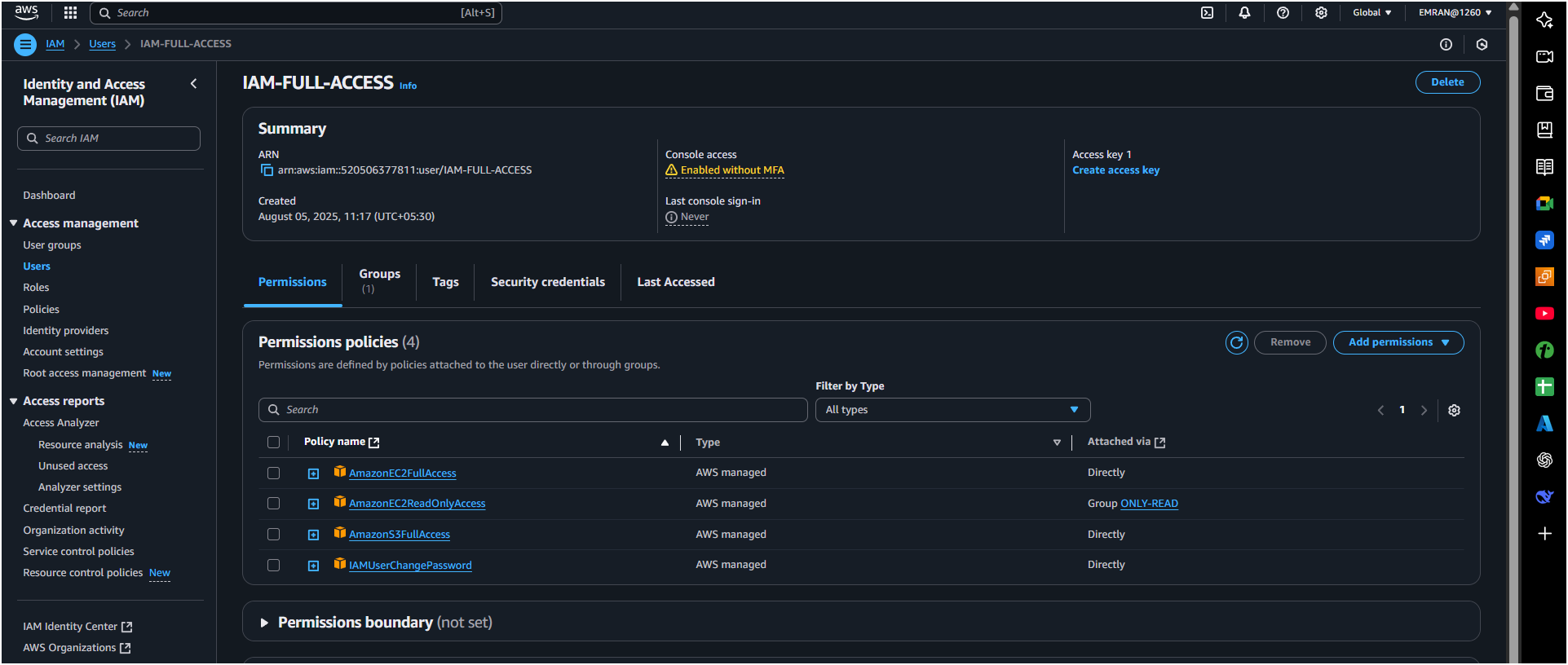
**Console Steps:**

1. Go to **IAM → Groups → Create group**:
   * Name: EC2ReadOnlyGroup.
2. Attach **AmazonEC2ReadOnlyAccess** policy.
3. Save.

**AWS CLI:**

aws iam create-group --group-name EC2ReadOnlyGroup

aws iam attach-group-policy --group-name EC2ReadOnlyGroup --policy-arn arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess



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

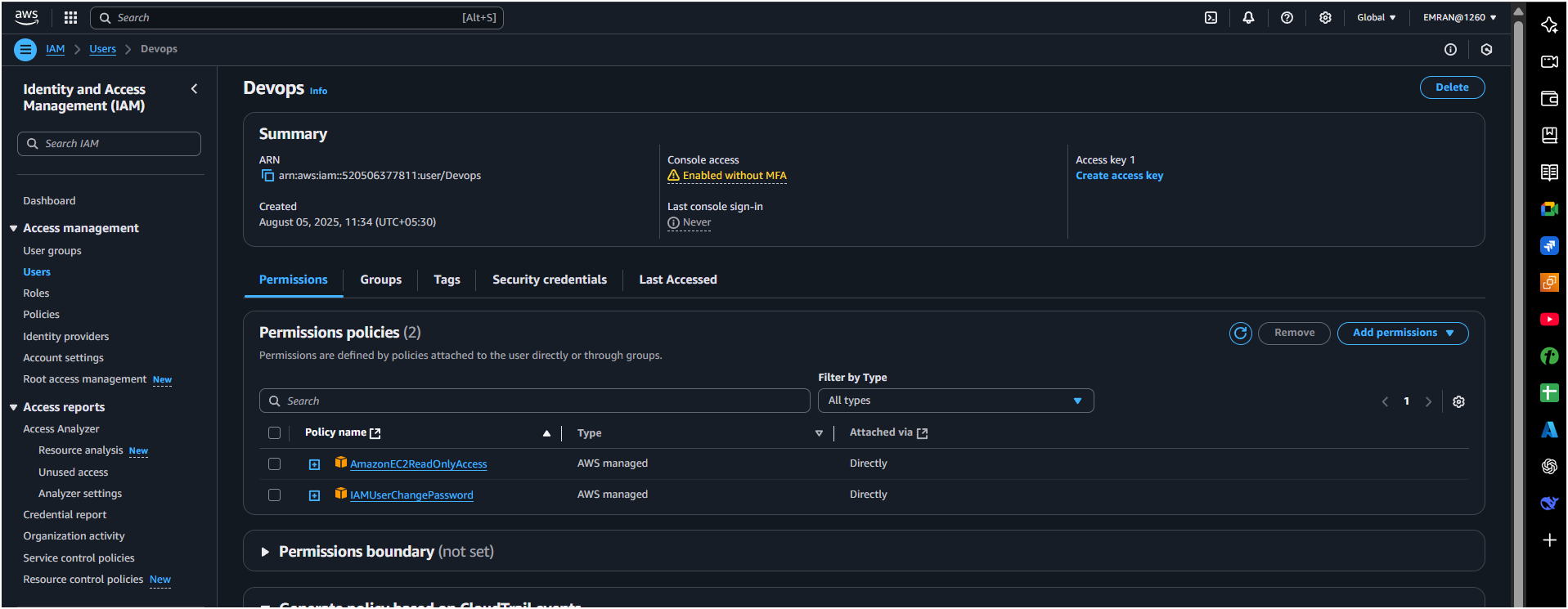
**Console Steps:**

1. Create user Devops in IAM.
2. Add to group EC2ReadOnlyGroup.

**AWS CLI:**

aws iam create-user --user-name Devops

aws iam add-user-to-group --user-name Devops --group-name EC2ReadOnlyGroup



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

#!/bin/bash

read -p "Enter IAM username: " username

# Create user

aws iam create-user --user-name $username

# Attach VPC Full Access Policy

aws iam attach-user-policy --user-name $username --policy-arn arn:aws:iam::aws:policy/AmazonVPCFullAccess

# Create login credentials (optional)

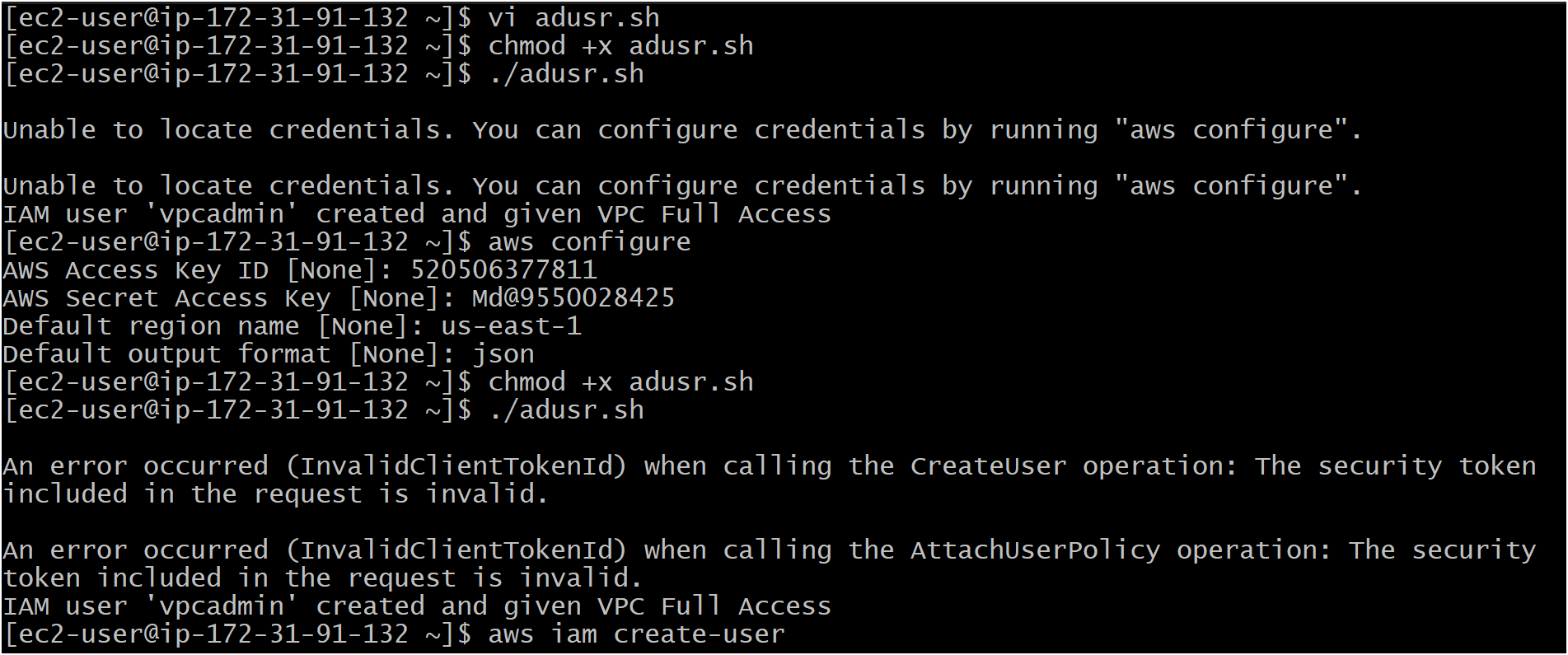
aws iam create-login-profile --user-name $username --password 'Password123!' --password-reset-required

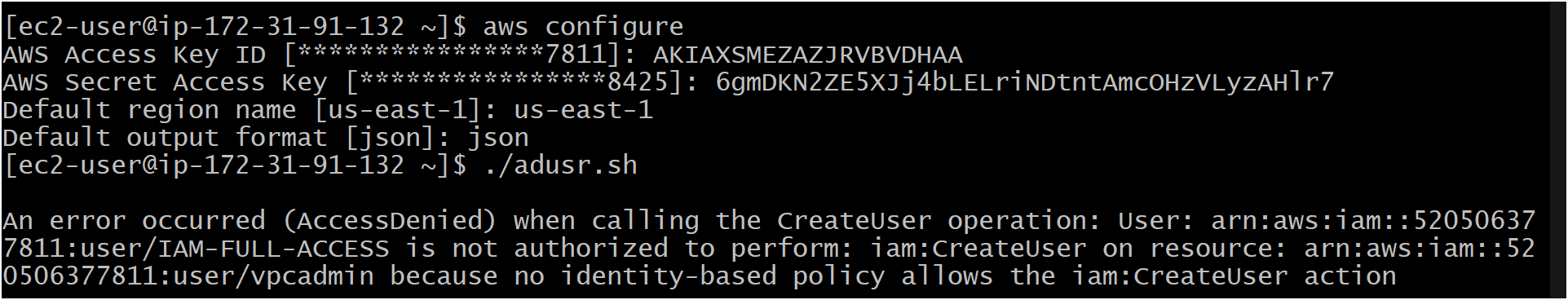
echo "User $username created with VPC Full Access."

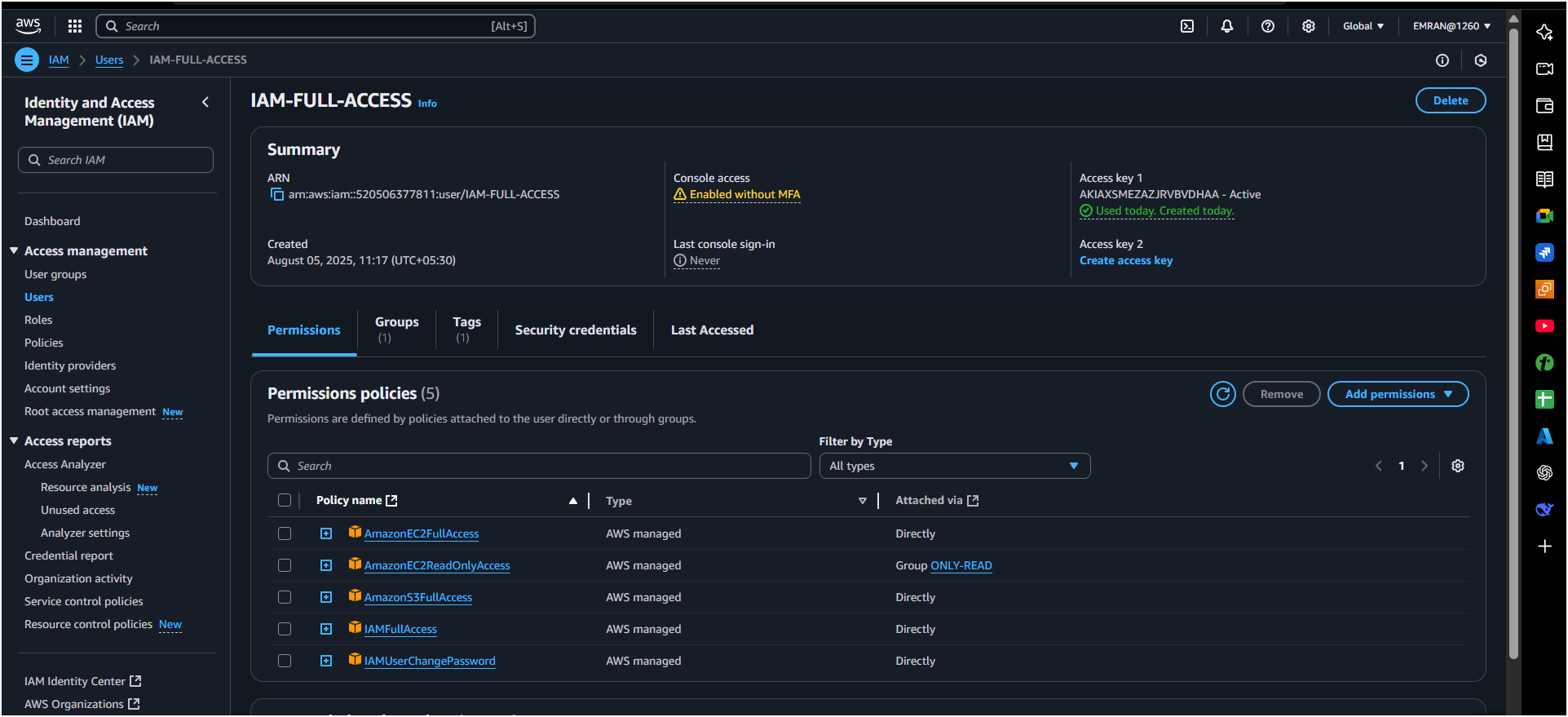
**Make executable:**

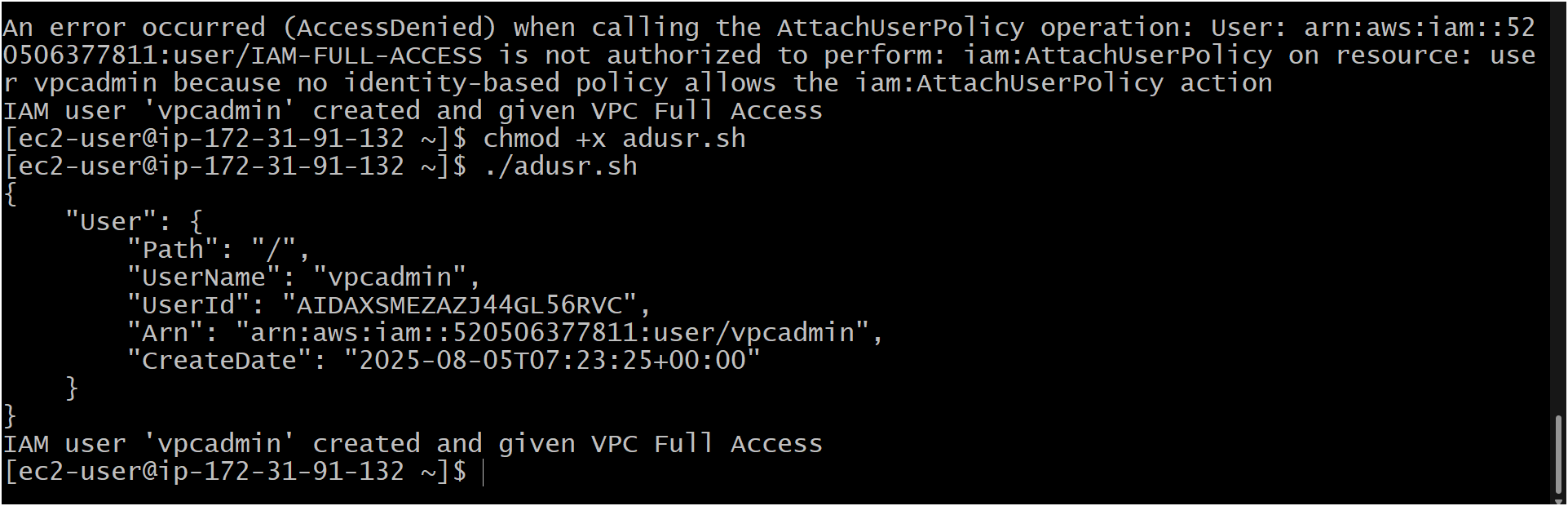
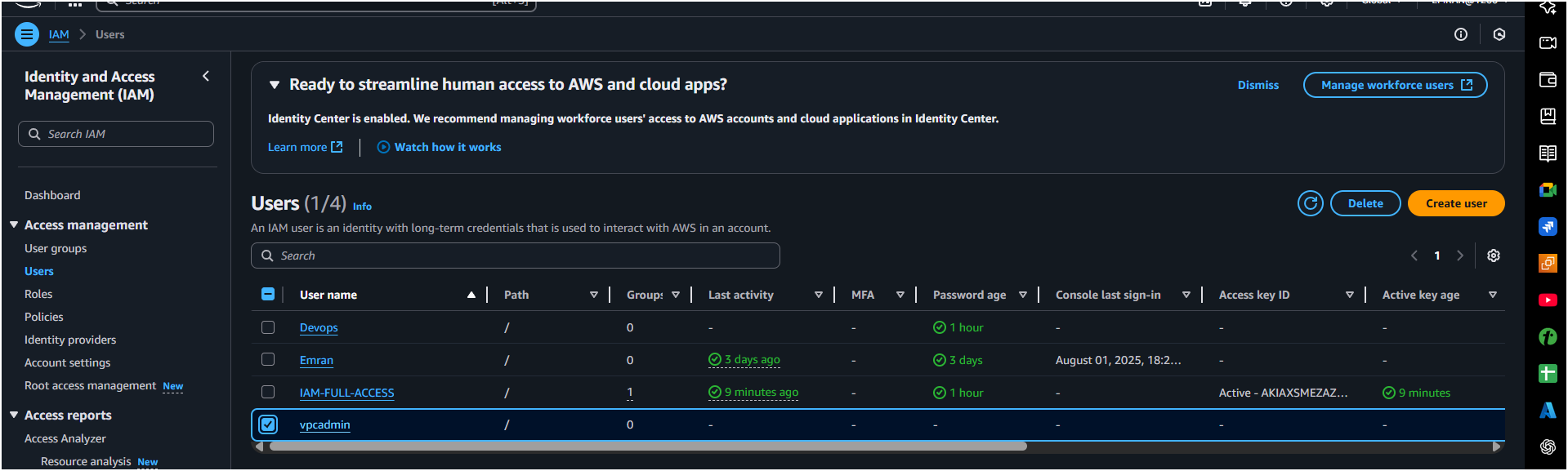
chmod +x create\_iam\_user.sh

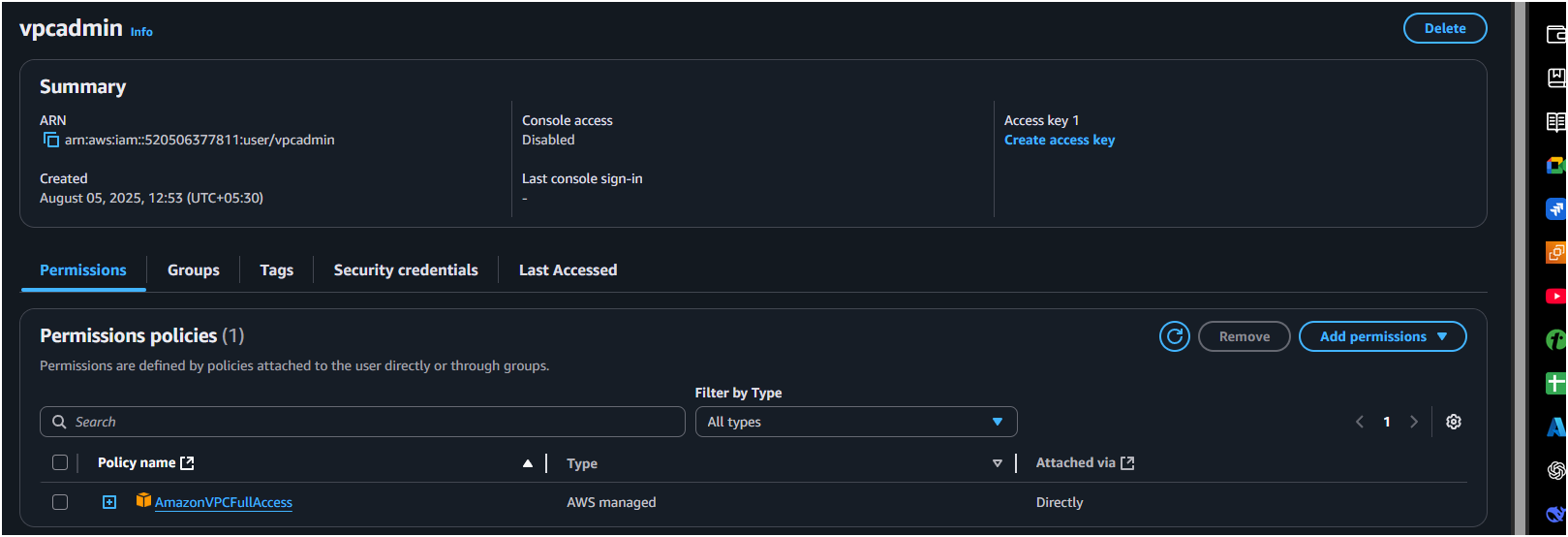
./create\_iam\_user.sh









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

**Policy JSON Example (Allow EC2 only in us-east-1 and us-west-2):**

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": "ec2:\*",

"Resource": "\*",

"Condition": {

"StringEquals": {

"aws:RequestedRegion": [

"us-east-1",

"us-west-2"

]

}

}

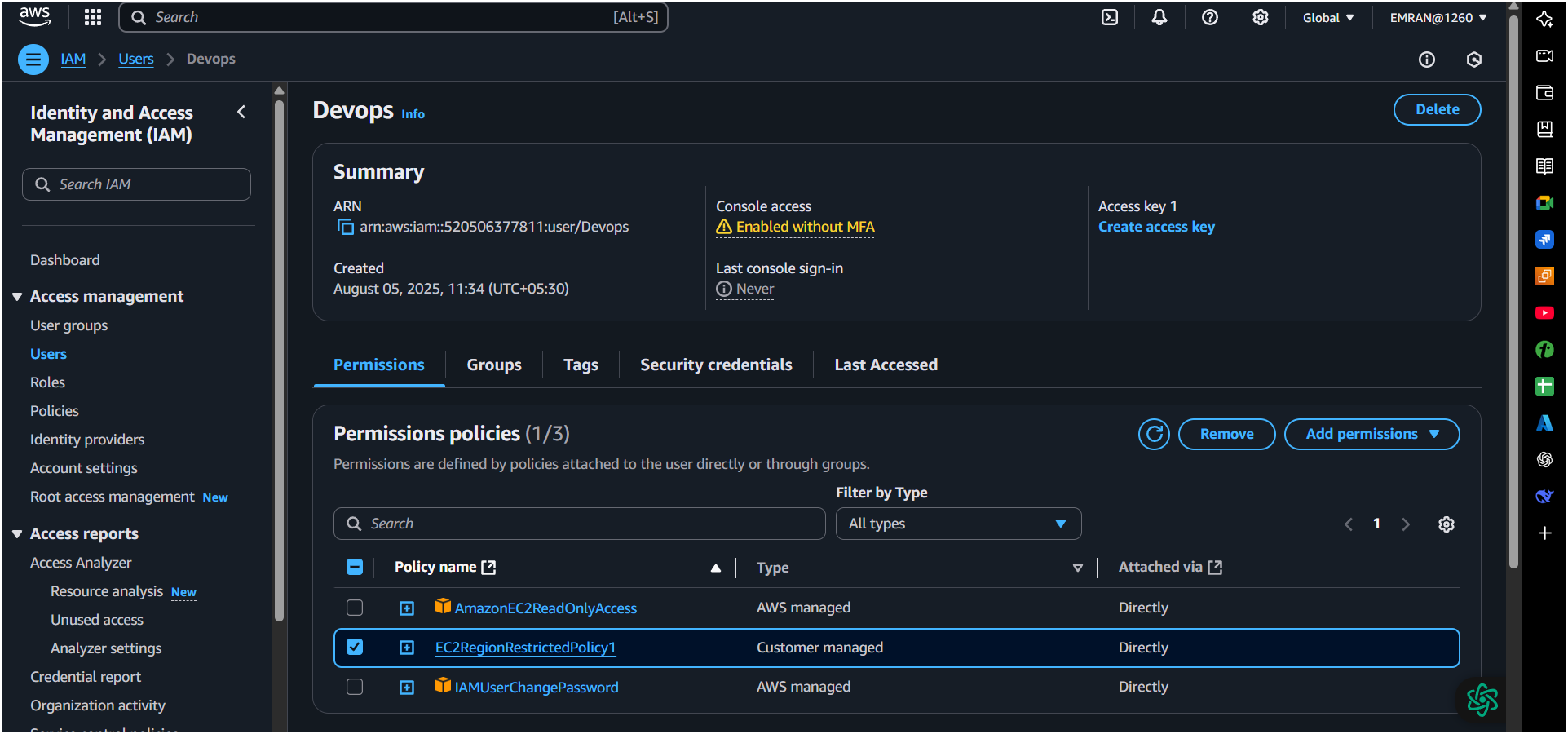
}

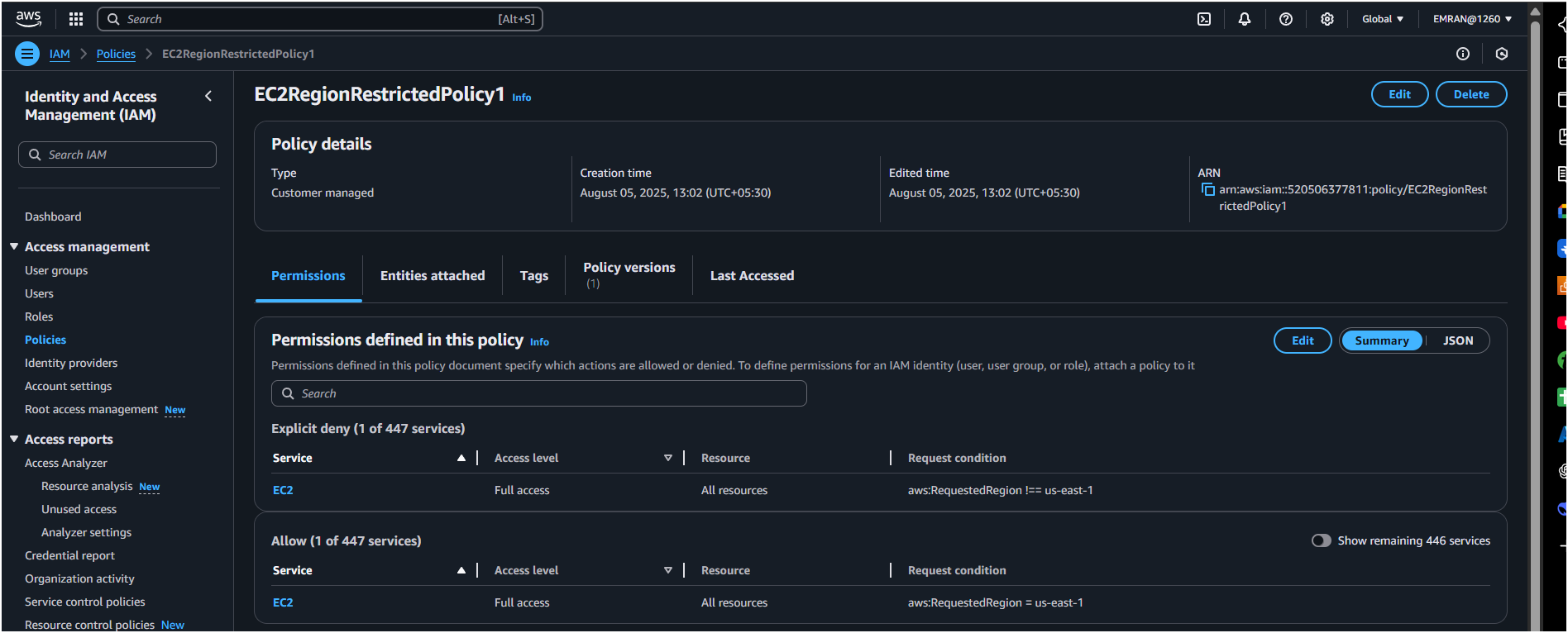
]

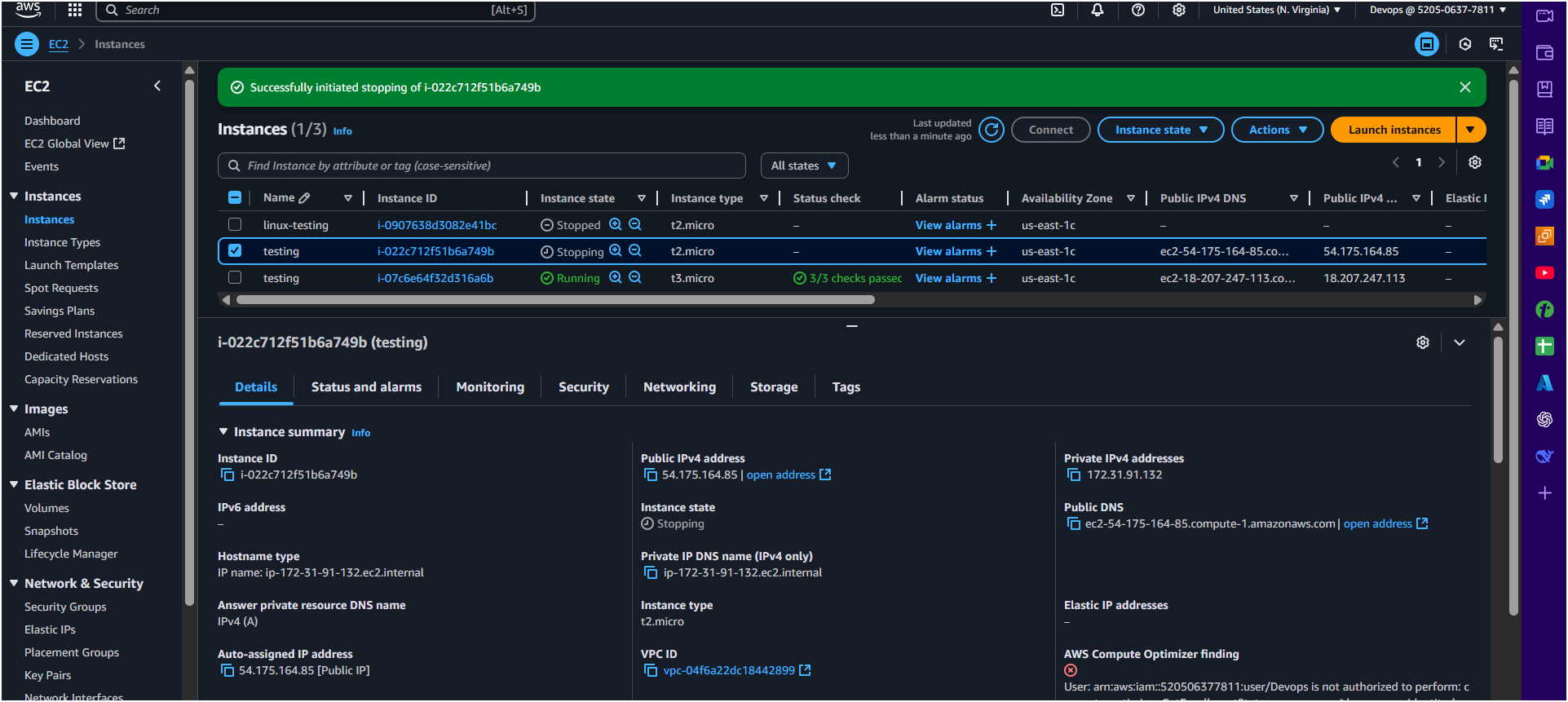
}

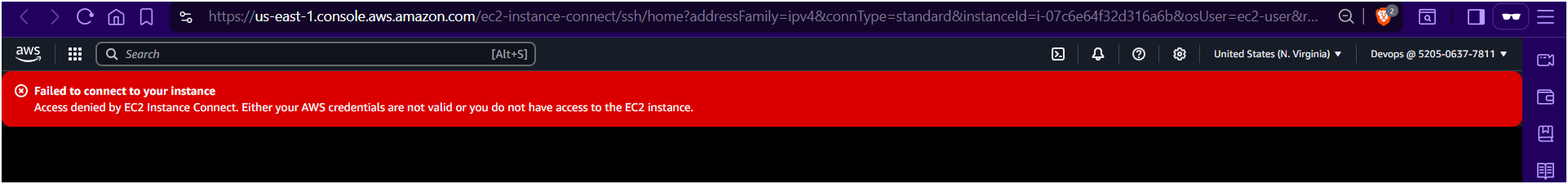
**Steps:**

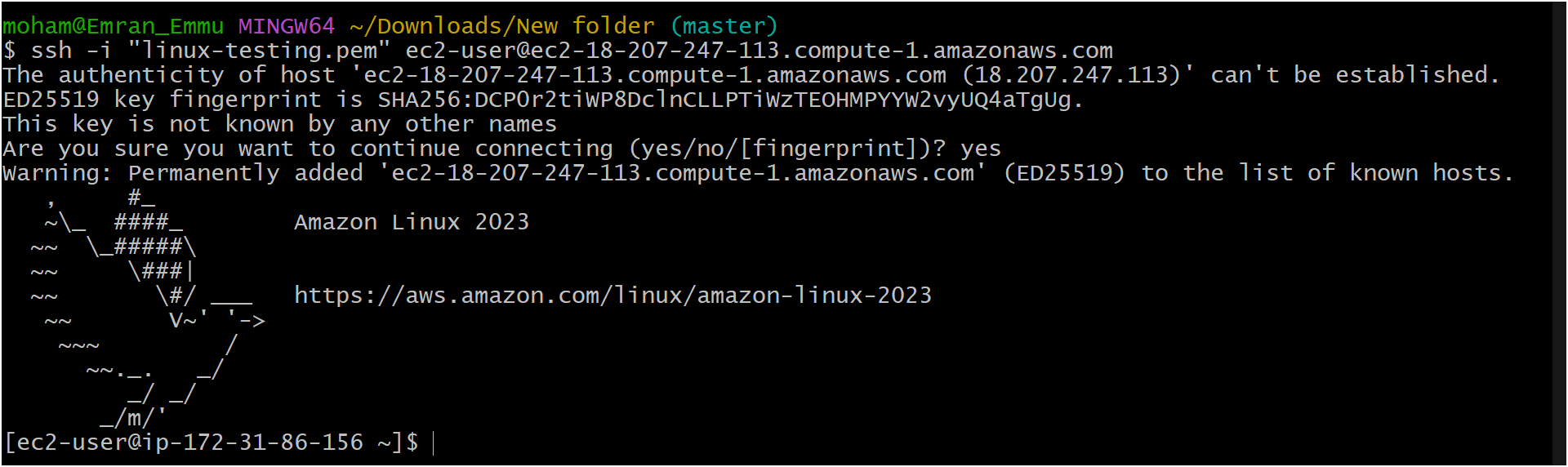
1. Go to **IAM → Policies → Create policy**.
2. Switch to **JSON**, paste the above.
3. Save as EC2SpecificRegionPolicy.
4. Attach this policy to the specific user.











6) We have two accounts Account A and Account B,

**Steps:**

1. Go to **IAM → Policies → Create policy**.
2. Switch to **JSON**, paste the above.
3. Save as EC2SpecificRegionPolicy.
4. Attach this policy to the specific user.

* Account A user should access s3 bucket in
* Account B. (Collaborate with team member and execute this.Mostly asked in every interview)  
    
  Accounts-A (mine)
* 1ST create a iam user open you user and u will get an option permission policies there you’ll get add permission click on it then you get an option create inline policy
* add this permission/policy in json and save

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "Example",

"Effect": "Allow",

"Action": [

"s3:ListBucket"

],

"Resource": [

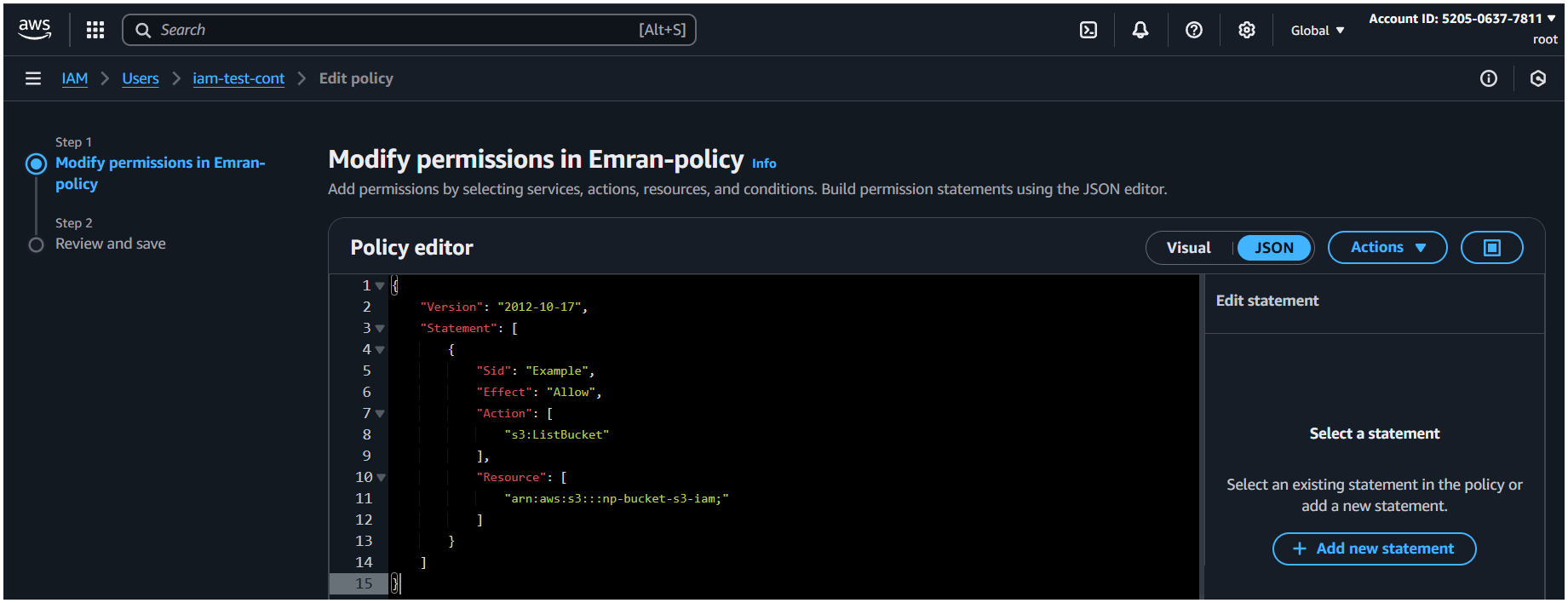
"arn:aws:s3:::np-bucket-s3-iam;"

]

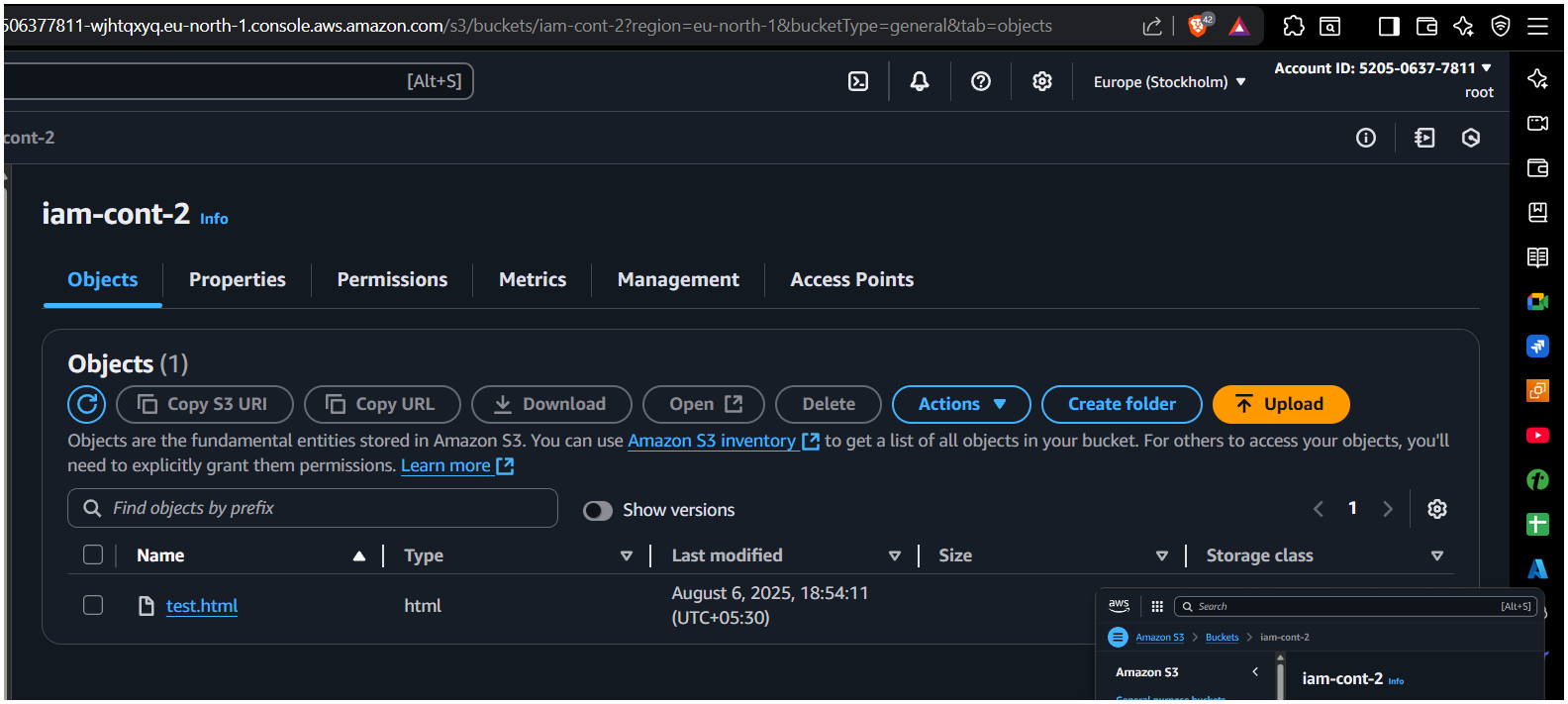
}

]

}



* 2nd create a bucket and in permission add script with ur Aws id and bucket name of your frd

  
Add this Script/permission/policy

* Add your Frd Aws id and then add your bucket name here in your s3 bucket.

"Version": "2012-10-17",

"Statement": [

{

"Sid": "Example permissions",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::216612007883:root"

},

"Action": [

"s3:GetLifecycleConfiguration",

"s3:ListBucket"

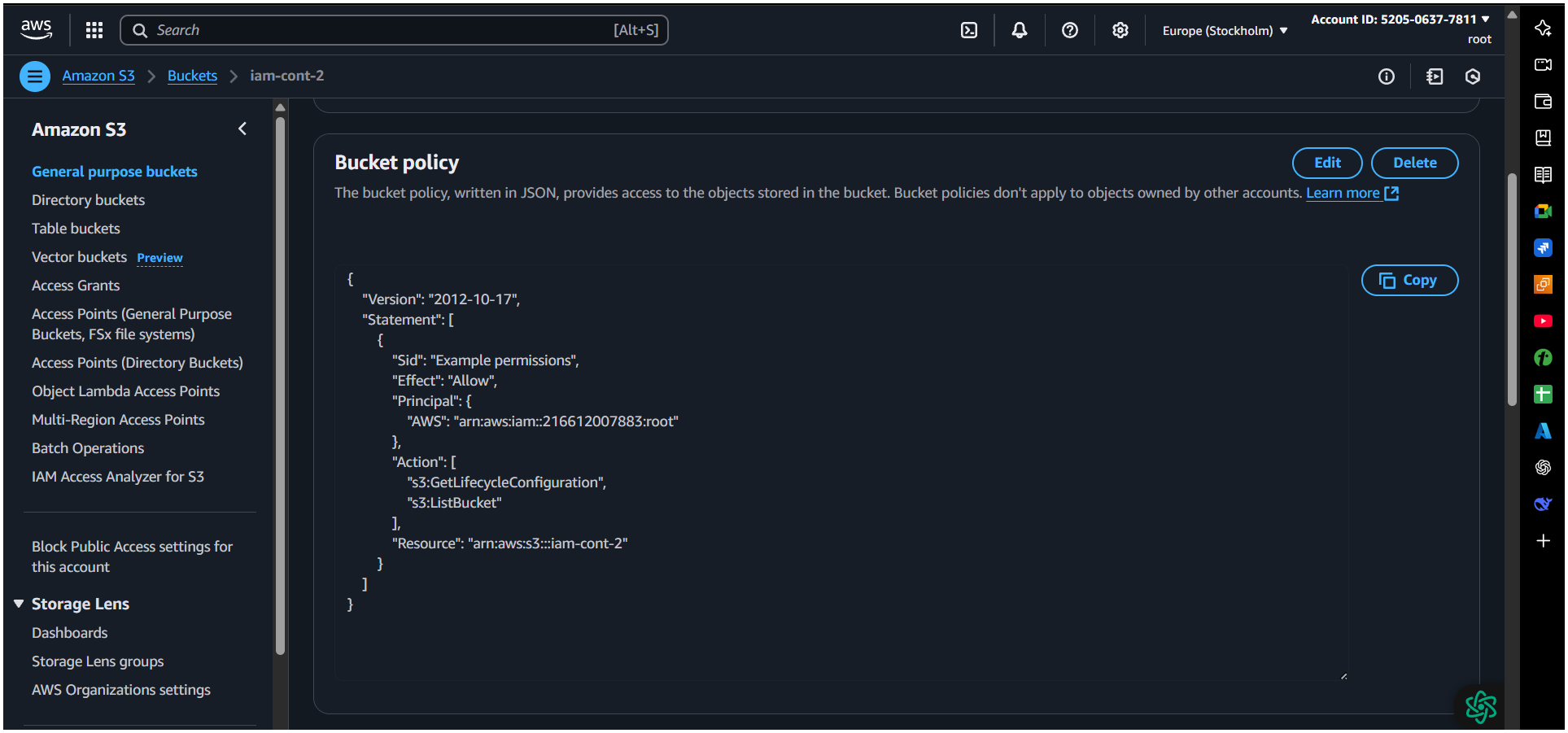
],

"Resource": "arn:aws:s3:::iam-cont-2"

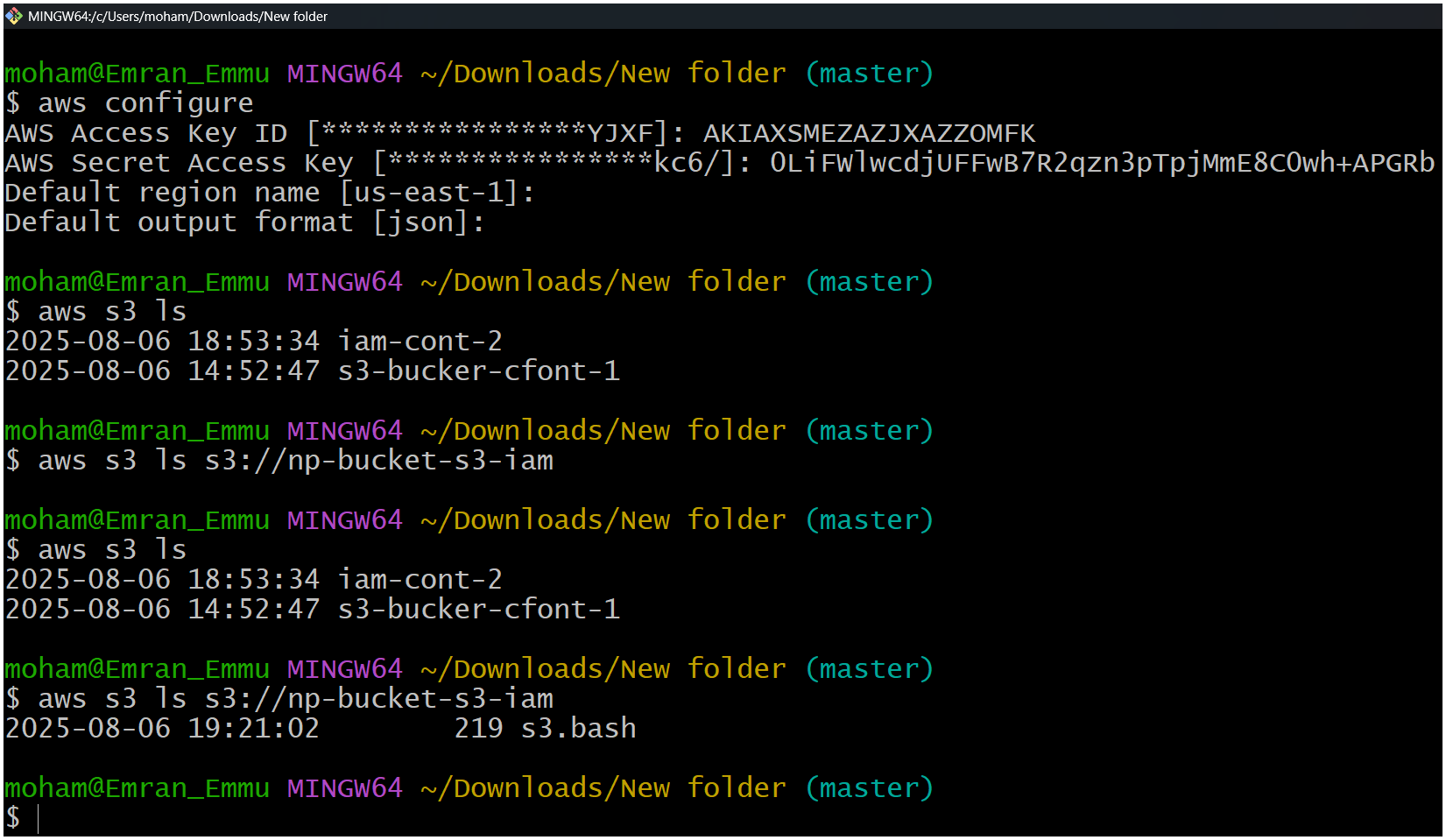
}

]

}



* Open your bash and Type this command and follow the step below
* Aws configure > your access id and password > region (us-east-1) > json >
* Aws s3 ls :- To Check your s3 bucket
* Aws s3 ls s3:// < here your frd s3 bucket name >



Account -B ( your frd side)

