Q.1) Create custom policy for delete bucket(before create objects by root) ?

Ans:== Create a policy to allow getting and deleting a bucket, but since my bucket already contains objects, I also want to create a policy to delete the objects inside the bucket
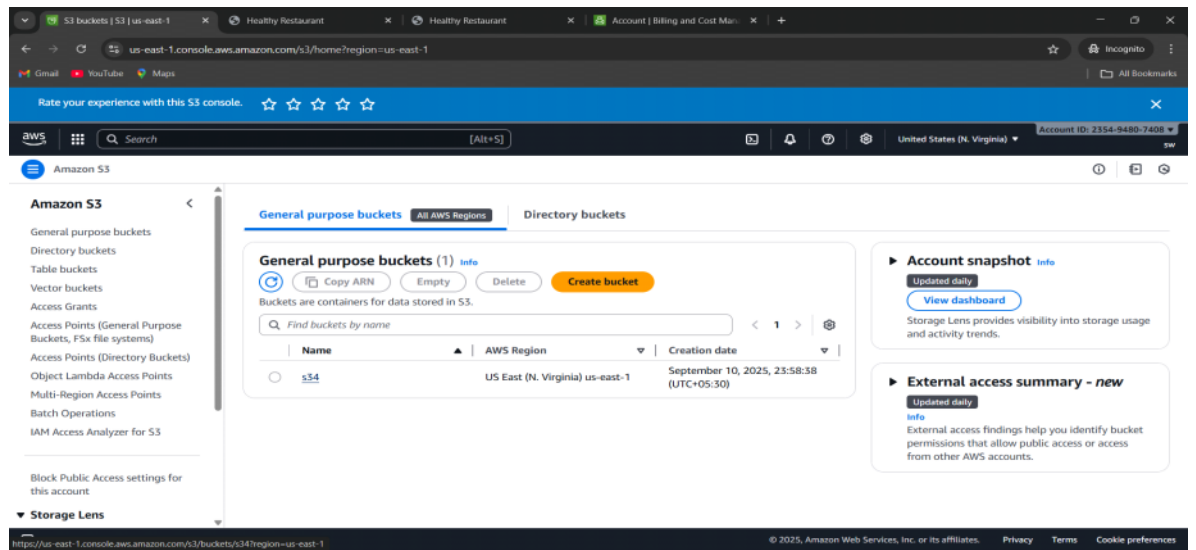===
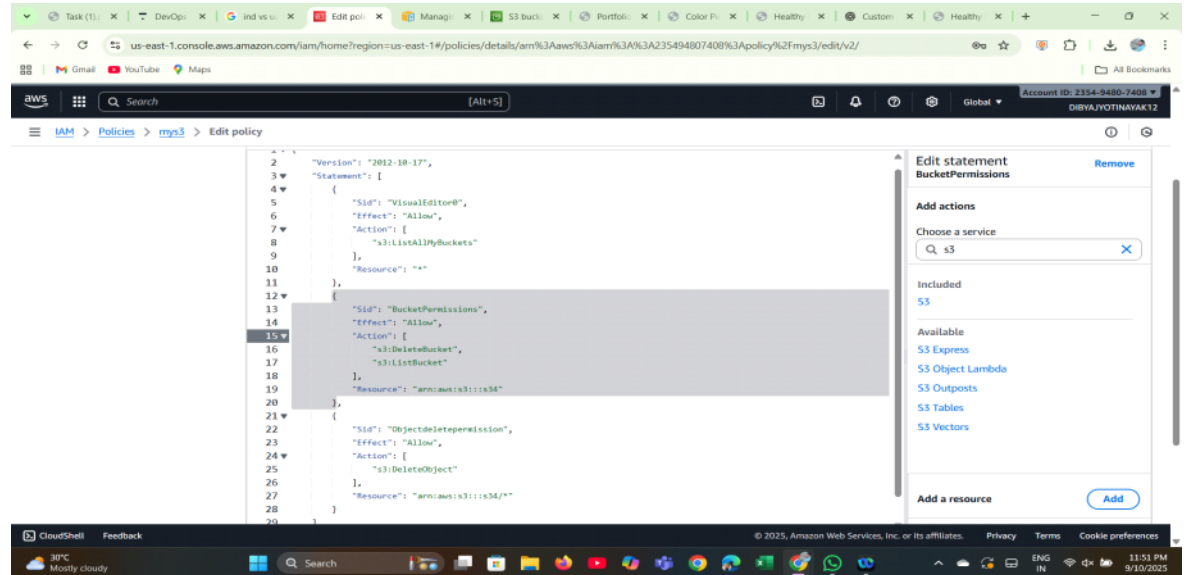
Json format policy:====

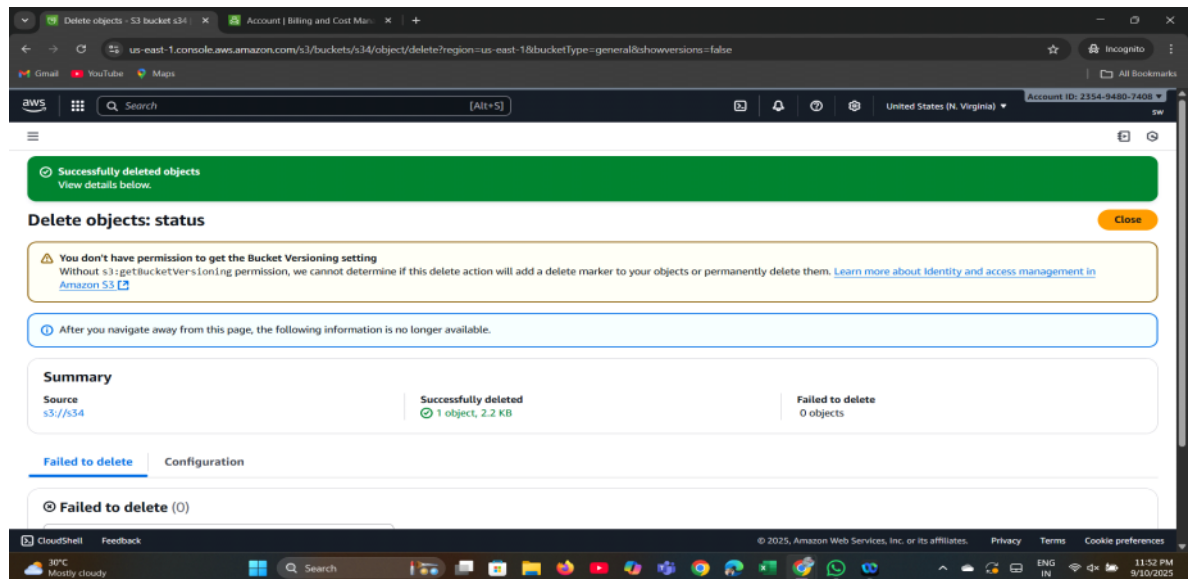```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadObjects",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::s34/*"
        },
        {
            "Sid": "DeleteObjects",
            "Effect": "Allow",
            "Action": "s3:DeleteObject",
            "Resource": "arn:aws:s3:::s34/*"
        },
        {
            "Sid": "ListBucket",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::s34"
        },
        {
            "Sid": "DeleteBucket",
            "Effect": "Allow",
            "Action": "s3:DeleteBucket",
            "Resource": "arn:aws:s3:::s34"
        }
```
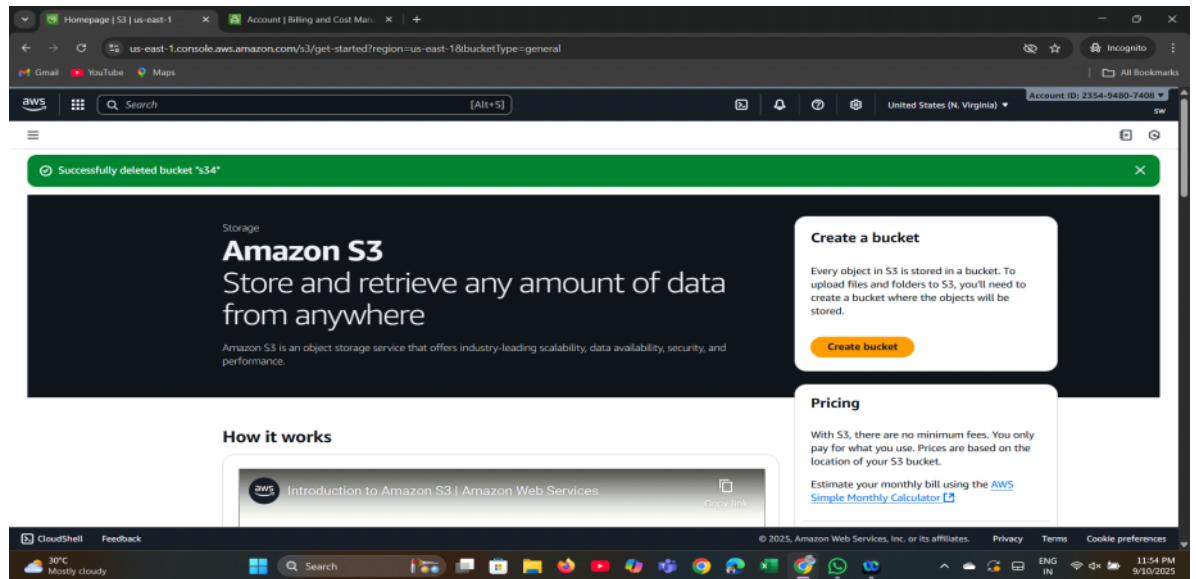
```
      ]
}
```
================================================================================

I was able to successfully see the bucket and object as a user

-----------------------------------------------------------------------



--------------------------------------------------------------------------------------------------------------------------------------

I successfully deleted the bucket and object as a user.

--------------------------------------------------------------------------------------------------------------------------------------



--------------------------------------------------------------------------------------------------------------------------------------

---

Q.2 Create Inline Policy to get Objcets in same User ?



```json
getobject
1 ▾ {
2       "Version": "2012-10-17",
3 ▾     "Statement": [
4 ▾         {
5               "Sid": "getobjectinlinepolicy",
6               "Effect": "Allow",
7 ▾             "Action": [
8                   "s3:GetObject"
9               ],
10              "Resource": "arn:aws:s3:::s34/*"
11          },
12 ▾         {
13              "Sid": "listbucketinlinepolicy",
14              "Effect": "Allow",
15 ▾             "Action": [
16                  "s3:ListBucket"
17              ],
18              "Resource": "arn:aws:s3:::s34"
19          },
20 ▾         {
```
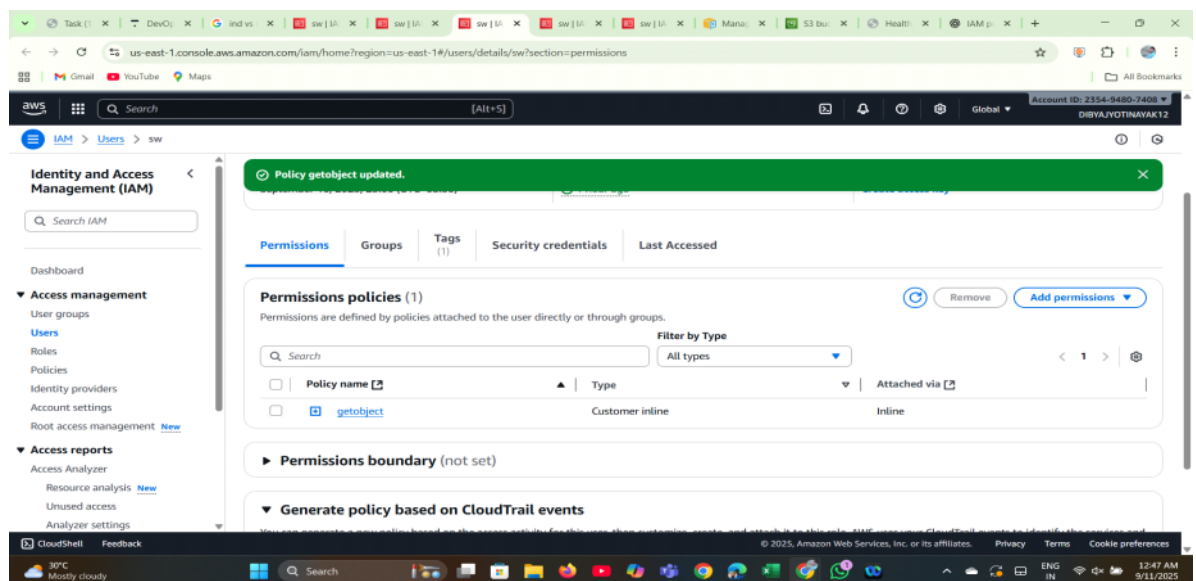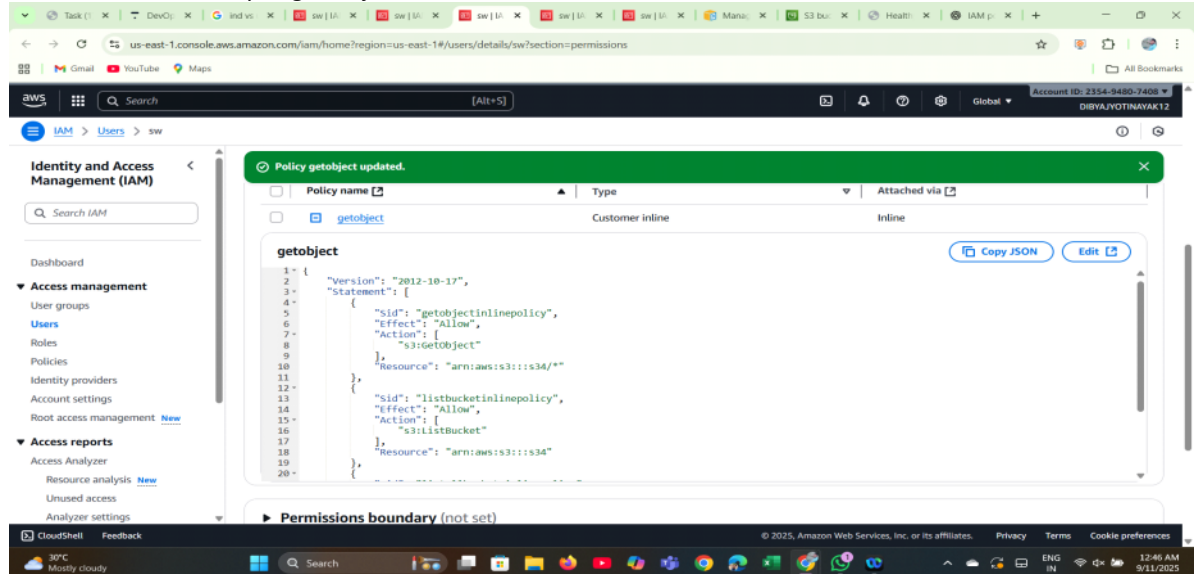
HERE IS POLICY JSON FORMAT

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "getobjectinlinepolicy",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListAllMyBuckets",
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::s34/"
        }
    ]
}
```
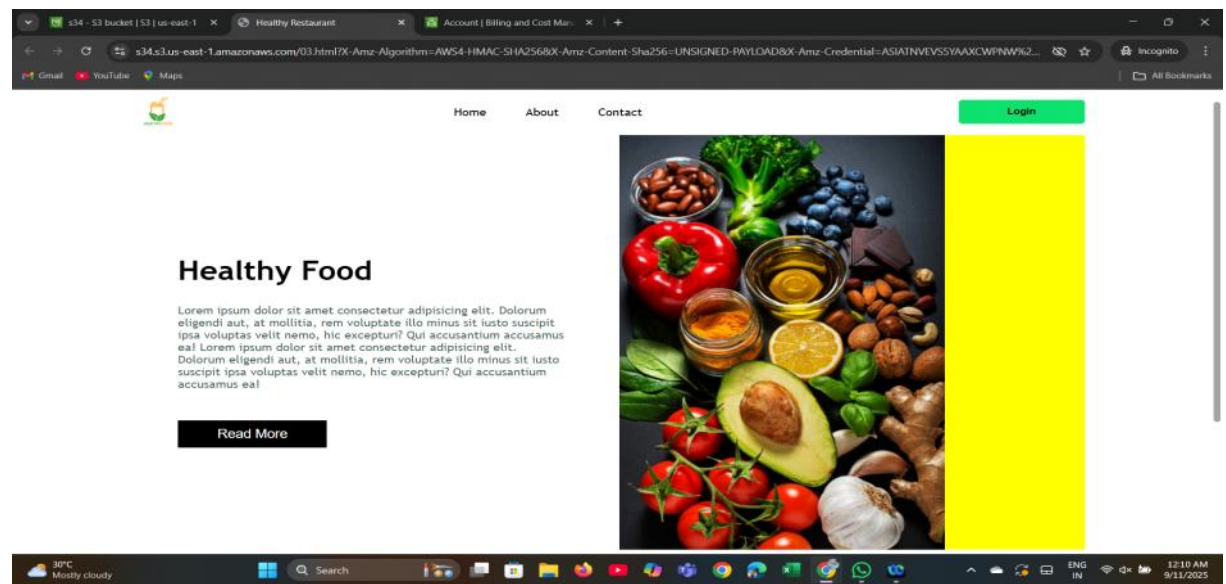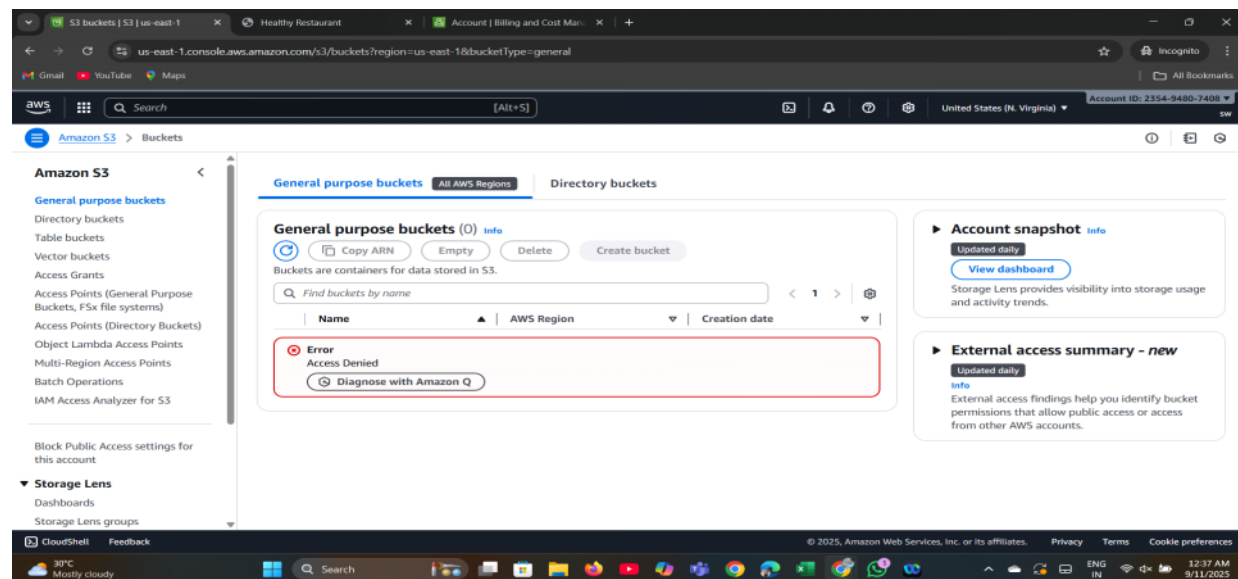

GETTING OBJECT CONTENT FROM THE USERSIDE

→When deny statement present with same policy with same permissions……

JSON FORMAT:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListBuckets",
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::s34"
        },
        {
            "Sid": "ListObjectsInBucket",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::s34"
        },
        {
            "Sid": "GetObjects",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::s34/*"
        },
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::s34"
        },
        {
            "Sid": "Statement2",
            "Effect": "Deny",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::s34"
        },
        {
            "Sid": "Statement3",
            "Effect": "Deny",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::s34/*"
        }
    ]
}
```

Q.4)Creation policy for specific ec2 but not full access ?

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowEC2InstanceLaunch",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:DescribeImages",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeInstances",
                "ec2:CreateTags"
            ],
```
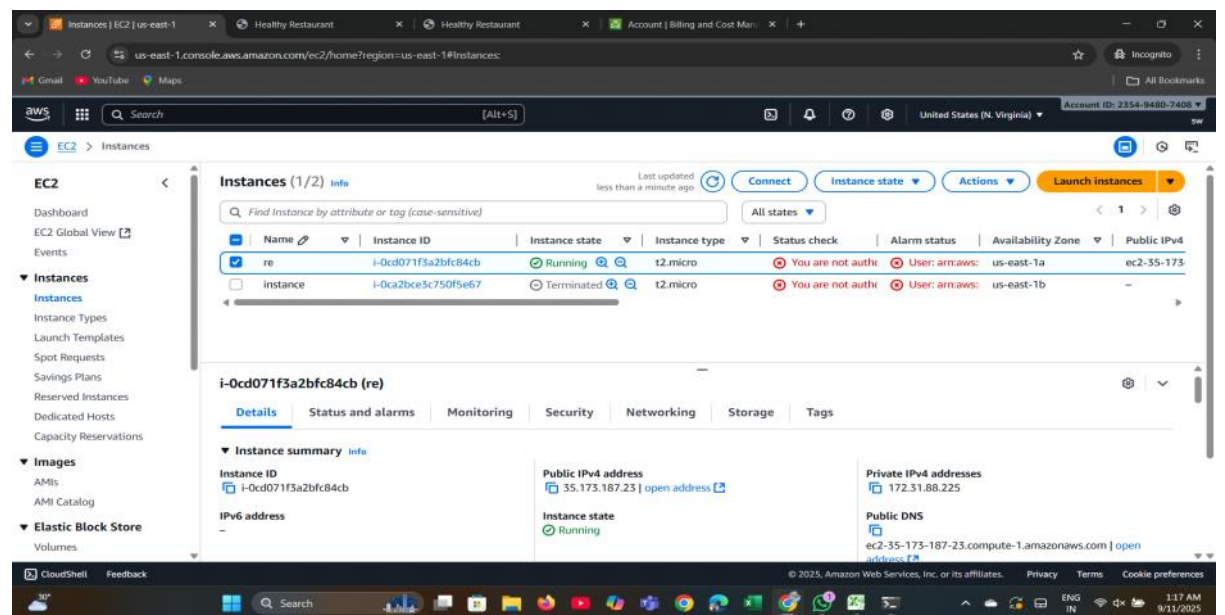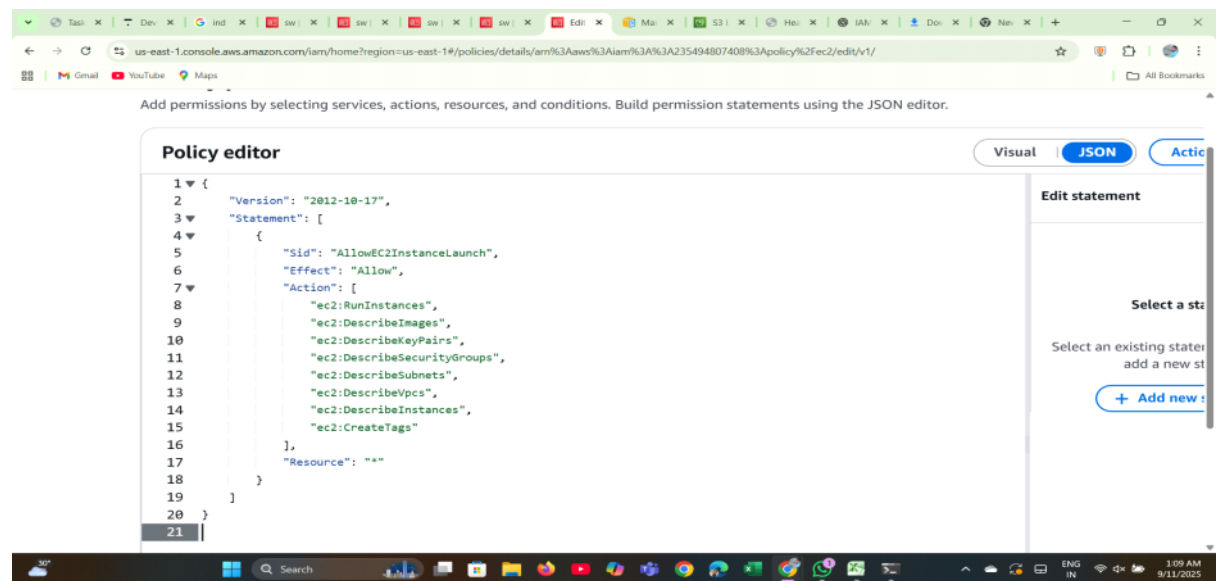
```
        "Resource": "*"
    }
  ]
}
```

CHECK S3 BUCKET LIST AND OTHER INFORMATION USING THE CLI BY LOGGING IN AS AN IAM USER.

```
Microsoft Windows [Version 10.0.26100.5074]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dibya>aws configure
AWS Access Key ID [****************3HWE]: AKIATNVEVS5YPCJOPKBW
AWS Secret Access Key [****************y3Il]: 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
Default region name [us-east-1]: us-east-1
Default output format [json]: json

C:\Users\dibya>aws s3 ls
2025-09-10 23:58:38 s34

C:\Users\dibya>aws configure --profile sw
AWS Access Key ID [None]: AKIATNVEVS5YPCJOPKBW
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json

C:\Users\dibya>aws s3 ls
2025-09-10 23:58:38 s34

C:\Users\dibya>aws s3 ls --profile sw
2025-09-10 23:58:38 s34

C:\Users\dibya>aws s3 ls s3://s34/ --profile sw
2025-09-10 23:59:23       5435 03.html

C:\Users\dibya>aws s3 cp s3://s34/ C:\Users\dibya\Downloads\s34\ --recursive --profile sw
download: s3://s34/03.html to Downloads\s34\03.html

C:\Users\dibya>aws s3 cp s3://s34/ C:\Users\dibya\Downloads\s34\ --recursive --profile sw
download: s3://s34/03.html to Downloads\s34\03.html

C:\Users\dibya>
```