

NAME:VADITHE USHA BAI

TASK:Cloud Security – IAM Policies, Secure Storage, and Data Encryption

Platform used:Amazon Web Services (AWS)

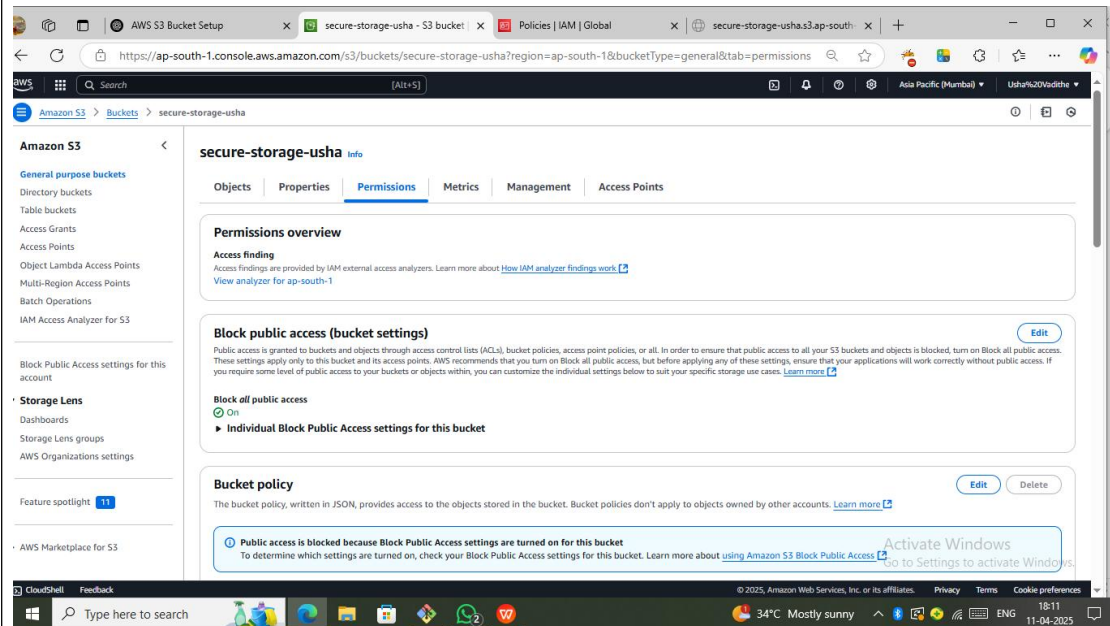
STEPS PERFORMED:

1. Created a Secure S3 Bucket

Bucket name: secure-storage-usha

Region: Asia Pacific (Mumbai)

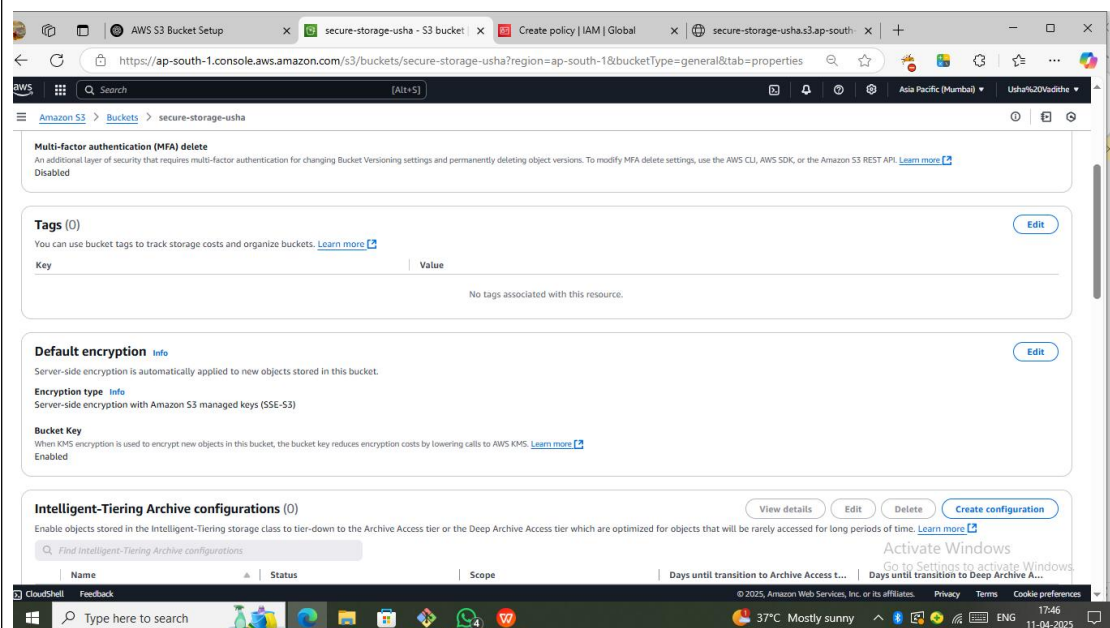
Blocked all public access to ensure data was private by default



2. Enabled Encryption

Enabled **Default Encryption** using SSE-S3 (Amazon S3-managed keys)

Verified that all uploaded objects are encrypted automatically



3. Created a Custom IAM Policy

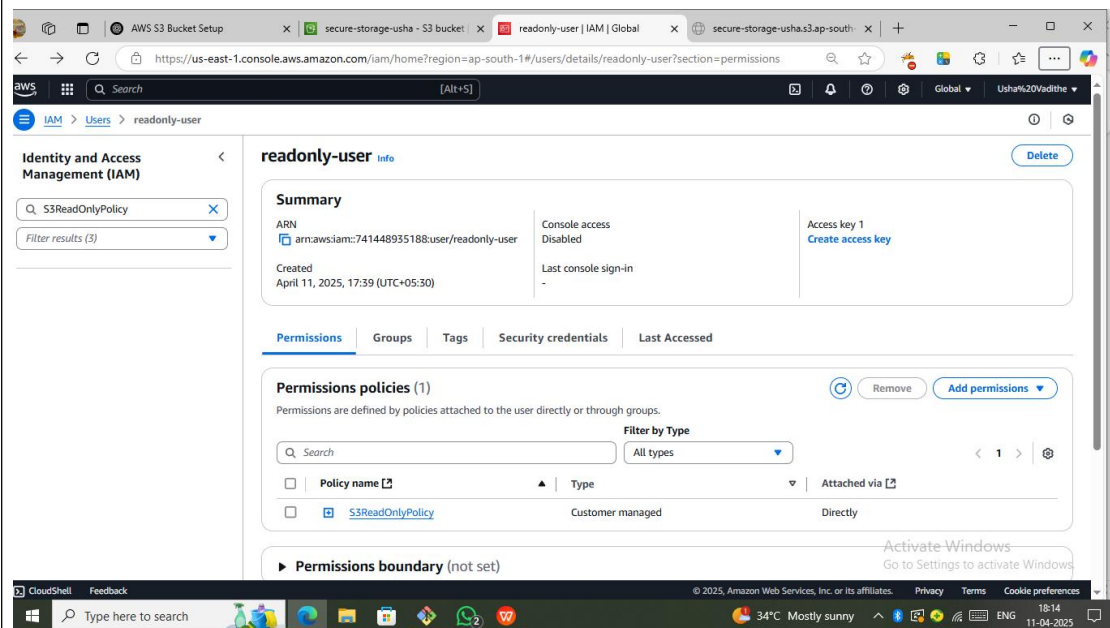
Policy name: S3ReadOnlyPolicy

Allowed the following actions:

s3:GetObject – to read/download objects

JSON Policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": "arn:aws:s3:::secure-storage-usha/*"
    },
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": "arn:aws:s3:::secure-storage-usha"
    }
  ]
}
```



4. Created a Secure IAM User

Username: readonly-user

Granted **programmatic access**

Attached S3ReadOnlyPolicy during creation

Downloaded **Access Key ID** and **Secret Access Key** for CLI testing

```
ec2-user@ip-172-31-6-230:~$ ssh -i ~/Downloads/kp1.pem ec2-user@15.207.223.7
ssh: connect to host 15.207.223.7 port 22: Connection timed out

ec2-user@ip-172-31-6-230:~$ ssh -i ~/Downloads/kp1.pem ec2-user@3.109.157.175
The authenticity of host '3.109.157.175 (3.109.157.175)' can't be established.
ED25519 key fingerprint is SHA256:N3FPubgMETPqhdjdmwFtwI2nF18m1mFfZF05XAm2NE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.109.157.175' (ED25519) to the list of known hosts.

Amazon Linux 2
AL2 End of Life is 2026-06-30.

A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028
https://aws.amazon.com/linux/amazon-linux-2023/

ec2-user@ip-172-31-6-230:~$ aws --version
aws-cli/1.18.147 Python/2.7.18 Linux/5.10.234-225.921.amzn2.x86_64 botocore/1.18.6
ec2-user@ip-172-31-6-230:~$ aws configure
AWS Access Key ID [None]: AKIA22IQM44KFS0LB3MT
AWS Secret Access Key [None]: Jw7UwLrX0vP6S2mW7eJw8hF0FHzRkaz3Reh2j
Default region name [None]: ap-south-1
Default output format [None]: json
ec2-user@ip-172-31-6-230:~$ aws s3 ls s3://secure-storage-usha
An error occurred (AccessDenied) when calling the ListObjectsV2 operation: User: arn:aws:iam::741448935188:user/readonly-user is not authorized to perform: s3:ListBucket on resource: "arn:aws:s3:::secure-storage-usha" because no identity-based policy allows the s3:ListBucket action
ec2-user@ip-172-31-6-230:~$
```

5. Tested Permissions Using AWS CLI

Configured AWS CLI using readonly-user credentials on EC2

Ran the following tests:

`aws s3 ls s3://secure-storage-usha`

`aws s3 rm s3://secure-storage-usha/yourfile.txt`

```
AWS S3 Bucket Setup | secure-storage-usha - S3 bucket | readonly-user | IAM | Global | secure-storage-usha.s3.ap-south-1 | https://secure-storage-usha.s3.ap-south-1.amazonaws.com/c.jpg

This XML file does not appear to have any style information associated with it. The document tree is shown below.
<?xml version="1.0" encoding="UTF-8" standalone="yes">
  <Error>
    <Code>AccessDenied</Code>
    <Message>Access Denied</Message>
    <RequestId>CGB3B0621D08M5ID</RequestId>
    <HostId>+n8Vkb5suRo3h3t49Zqn1J0V3FxFn6x8nqvRmn0i87g1LT1yuKldR+KP7C7yeuq21he1tKKXy8adt9QL7Qm2BfaU0SUL</HostId>
  </Error>
</xml>
```

Conclusion:

Successfully implemented secure cloud storage using IAM policies for access control
Server-side encryption (SSE-S3) Verified that access is correctly restricted to read-only for specific users