

# Practical No 5

## AWS Organization

**Name:** Shivshankar Ghyar

**PRN:** 202201040031

**Batch:** CCF1

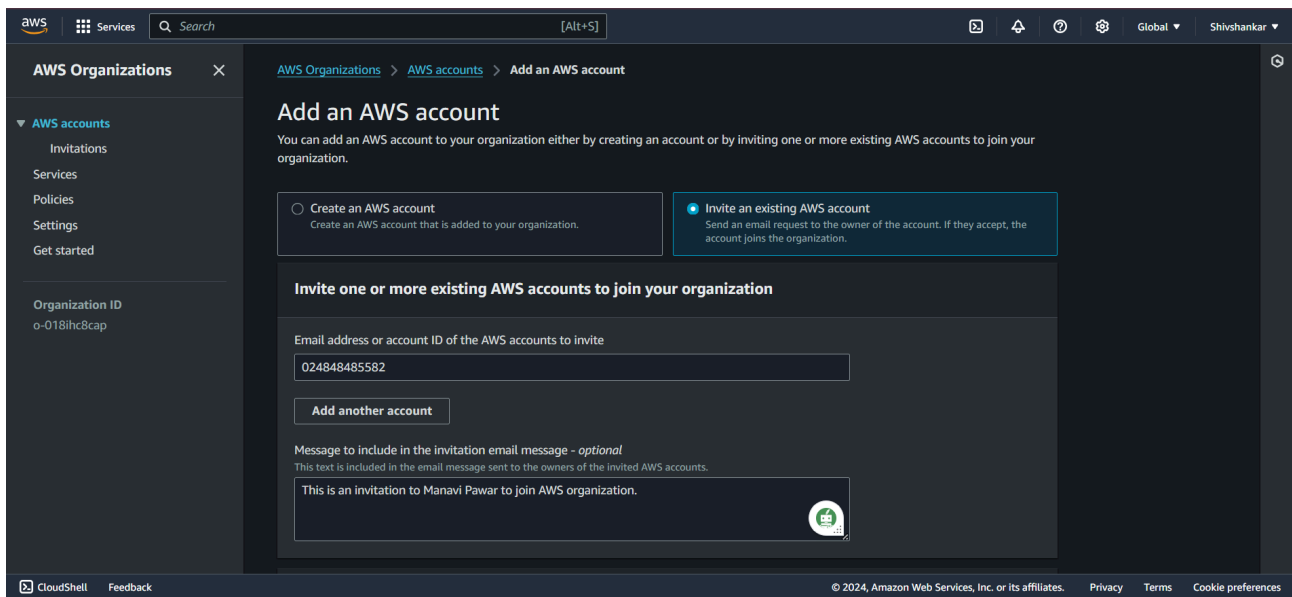
### Problem Statement

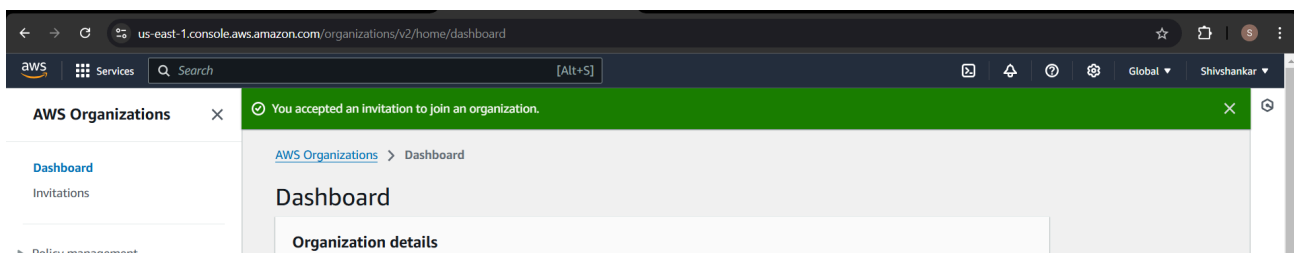
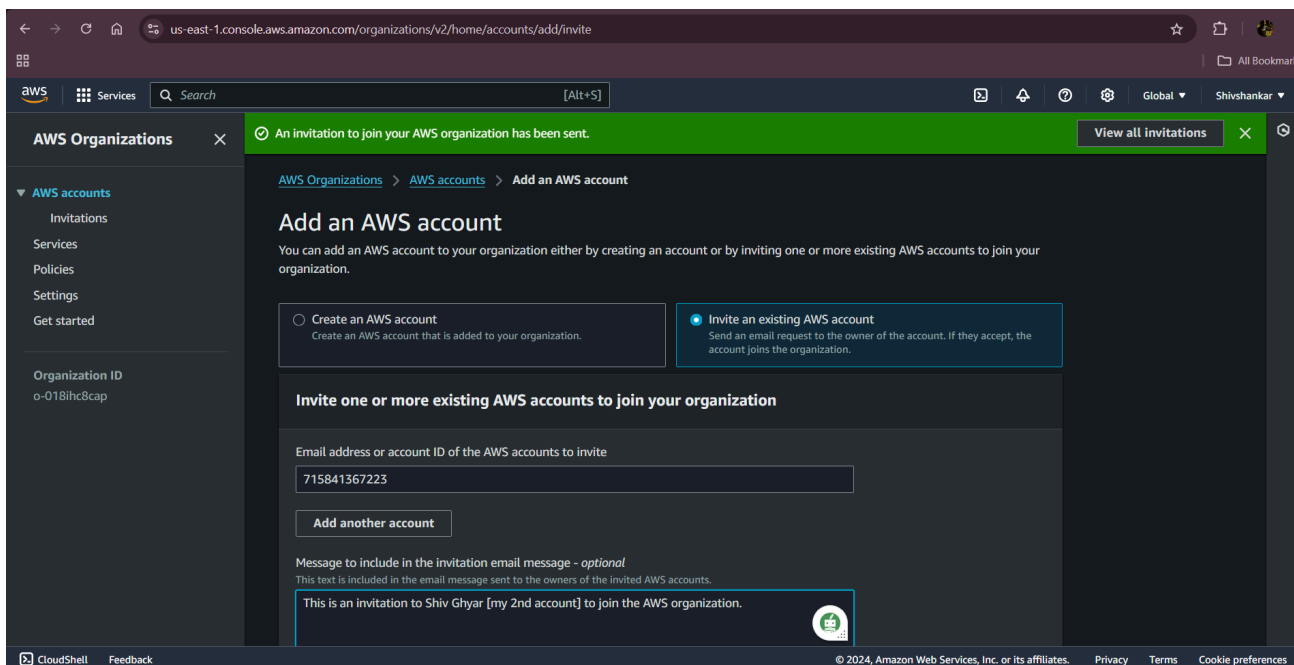
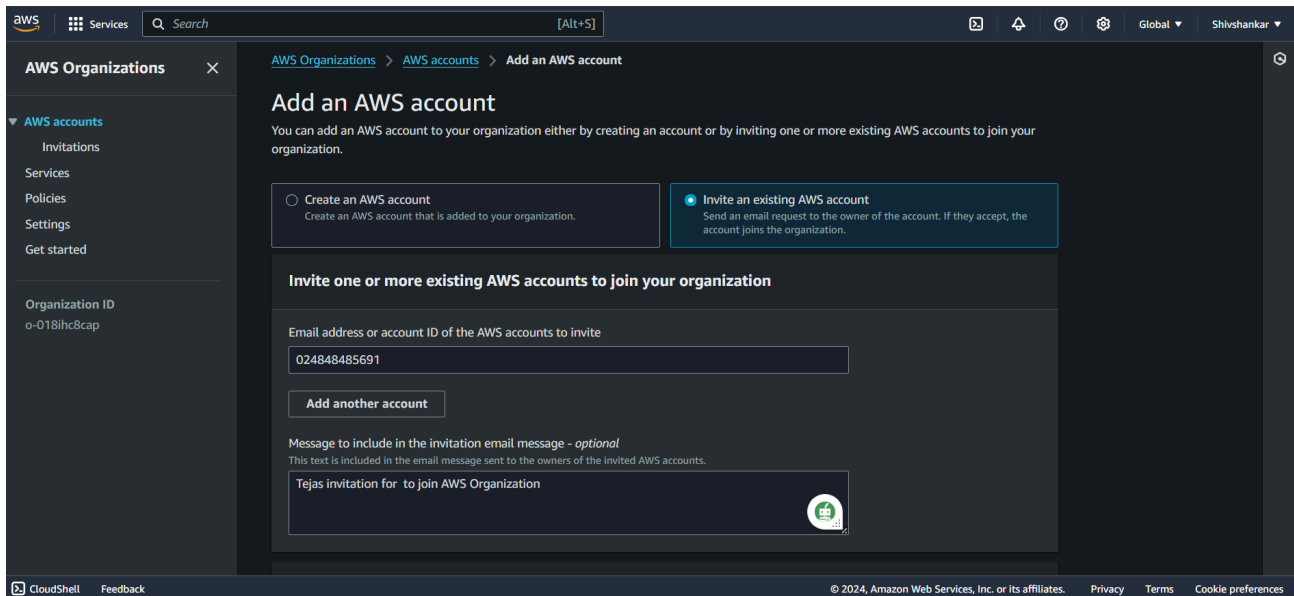
Designing a scalable and secure AWS organization that supports a multi-account structure for effective resource management and access control. The goal is to enable controlled access to AWS EC2 and S3 services across different accounts in the organization, allowing for specific user roles and permissions.

### Step 1: Set Up AWS Organizations

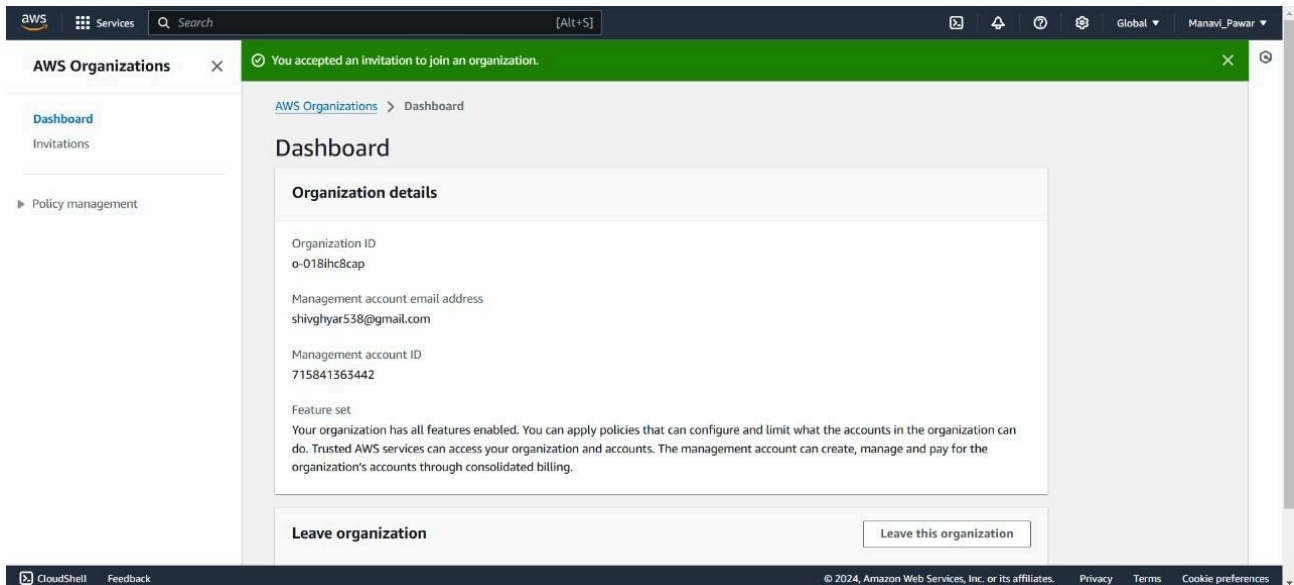
#### → Create AWS Organization

- Go to AWS organization → create organization
- Add members to the organization by sending them invitation.

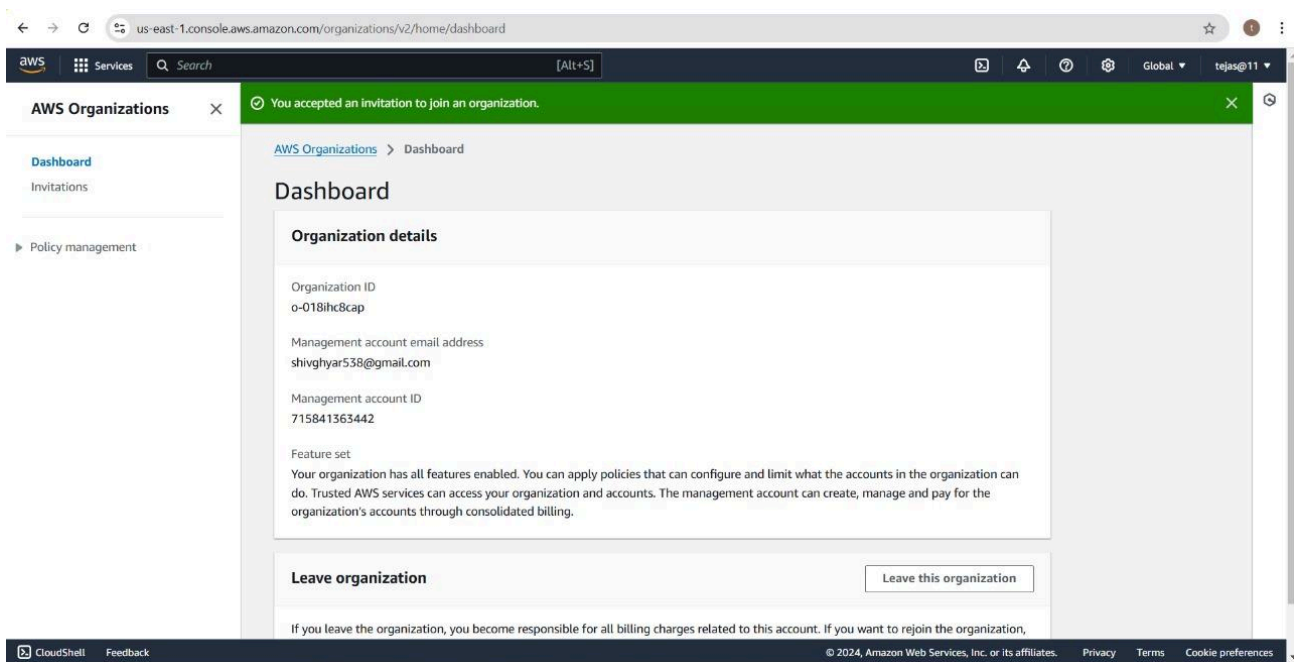




**This is my 2nd acct**



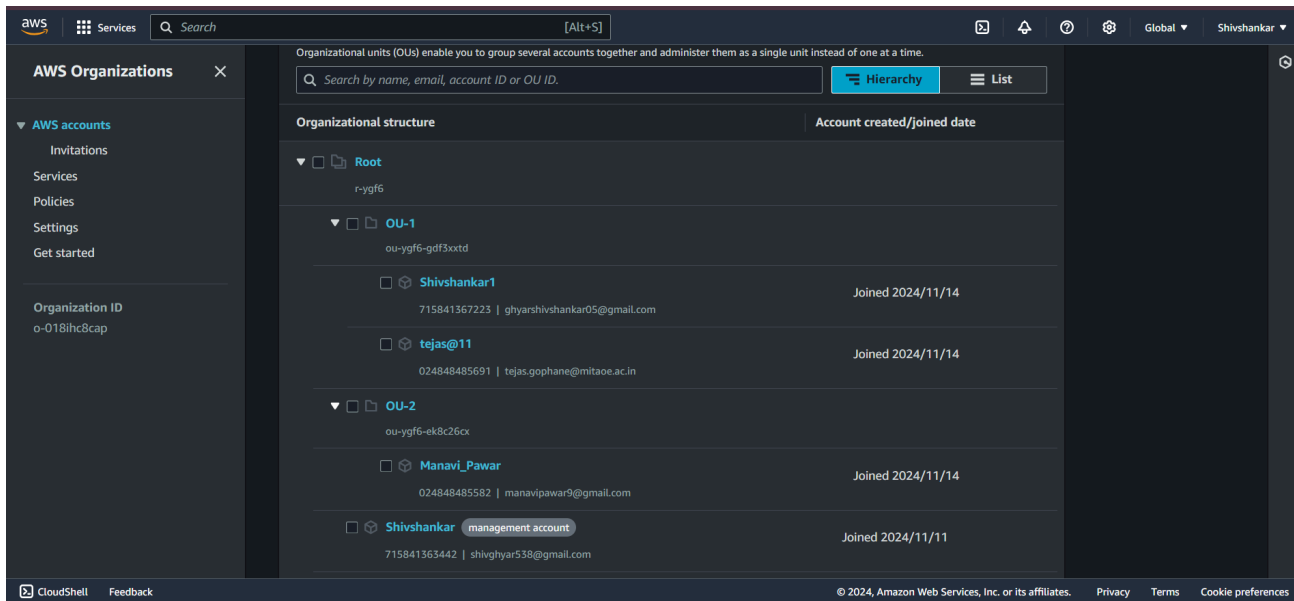
## This is Manavi Pawar's Account



## This is Tejas Account

→ Create OUs and move members to them

## ★ Final setup of AWS organization



## Step 2: Create Policies for Different OU

### OU-2 => EC2 Key pair [Explicit Deny]

1. Describe key pair
2. Create key pair
3. Delete key pair

**Users:** Manavi\_Pawar

### OU-1 => S3 Bucket [Explicit Deny]

**Users:** 1. tejas@11  
2. Shivshankar1

→ Go to AWS organization → policy → enable Service Control Policy → Create policy

## ★ OU-Policy-1

Service control policies have been enabled.

[AWS Organizations](#) > [Policies](#) > [Service control policies](#) > Create new service control policy

### Create new service control policy

A service control policy (SCP) specifies the maximum permissions that can be used by users and roles in your organization's accounts. An SCP doesn't grant permissions. You must still use IAM permission policies or resource policies to grant permissions. [Learn more](#)

**Details**

Policy name

ou-policy-1

A policy name can be up to 128 characters and can include the following characters: a-z, A-Z, 0-9, and .,\*,@,\_,-

Policy description - optional

e.g Sandbox

A description can have up to 512 characters and can include the following characters: a-z, A-Z, 0-9, and .,\*,@,\_,-

**Tags**

Tags are key-value pairs that you can add to AWS resources to help identify, organize, and secure your AWS resources.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

You can add 50 more tags.

**Statement**

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Deny",
7       "Action": [
8         "s3:*"
9       ],
10      "Resource": [
11        "*"
12      ]
13    }
14  ]
15 }
```

**Edit statement** Remove

**Add actions**

All services > S3

Q c

☒ All actions (s3:\*)

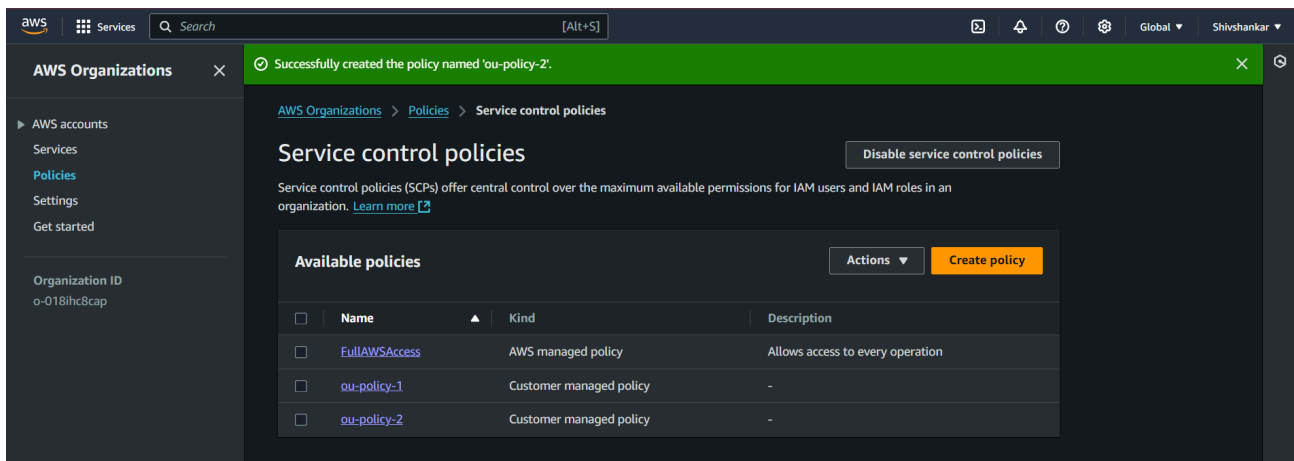
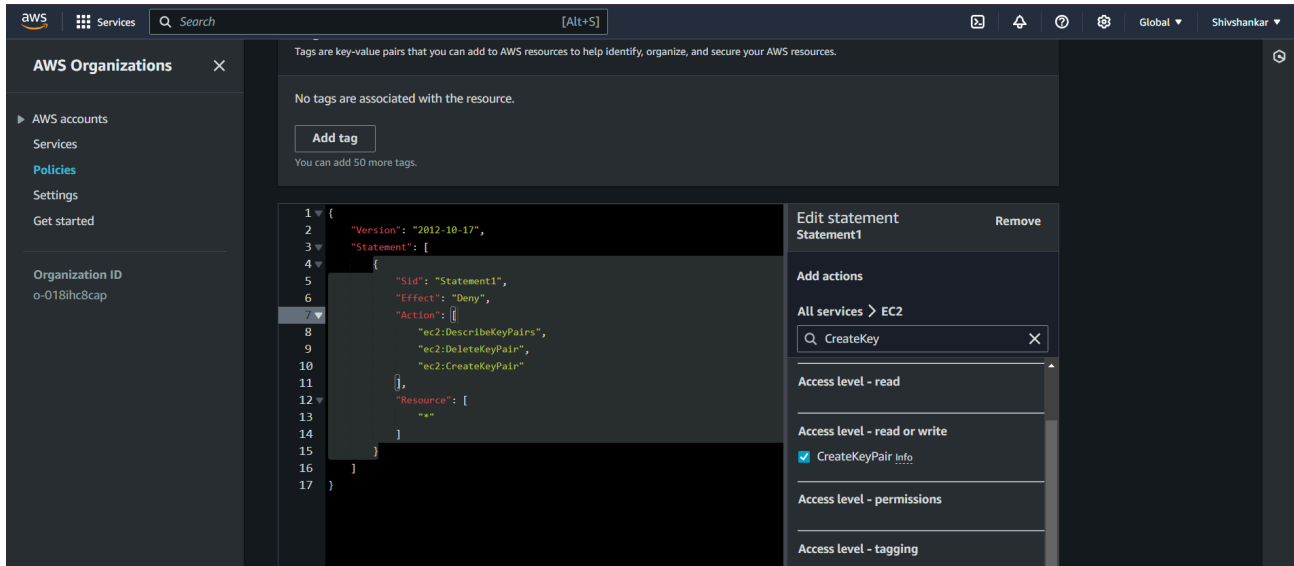
**Access level - list**

- ☒ ListAccessGrants [Info](#)
- ☒ ListAccessGrantsInstances [Info](#)
- ☒ ListAccessGrantsLocations [Info](#)
- ☒ ListAccessPoints [Info](#)
- ☒ ListAccessPointsForObjectLambda [Info](#)
- ☒ ListAllMyBuckets [Info](#)

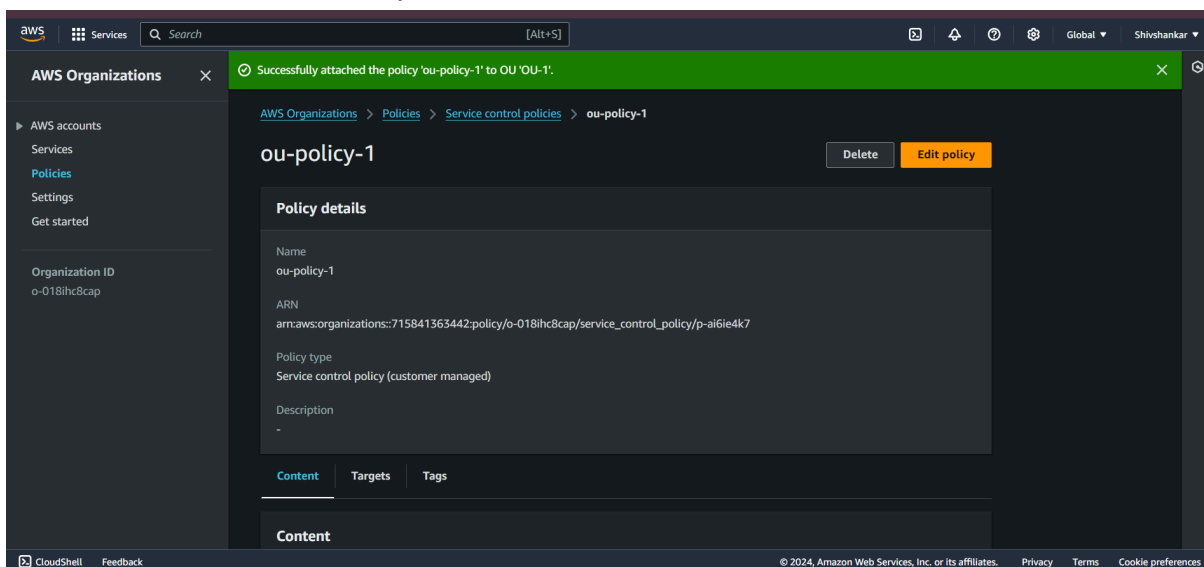
**Add a resource** Add

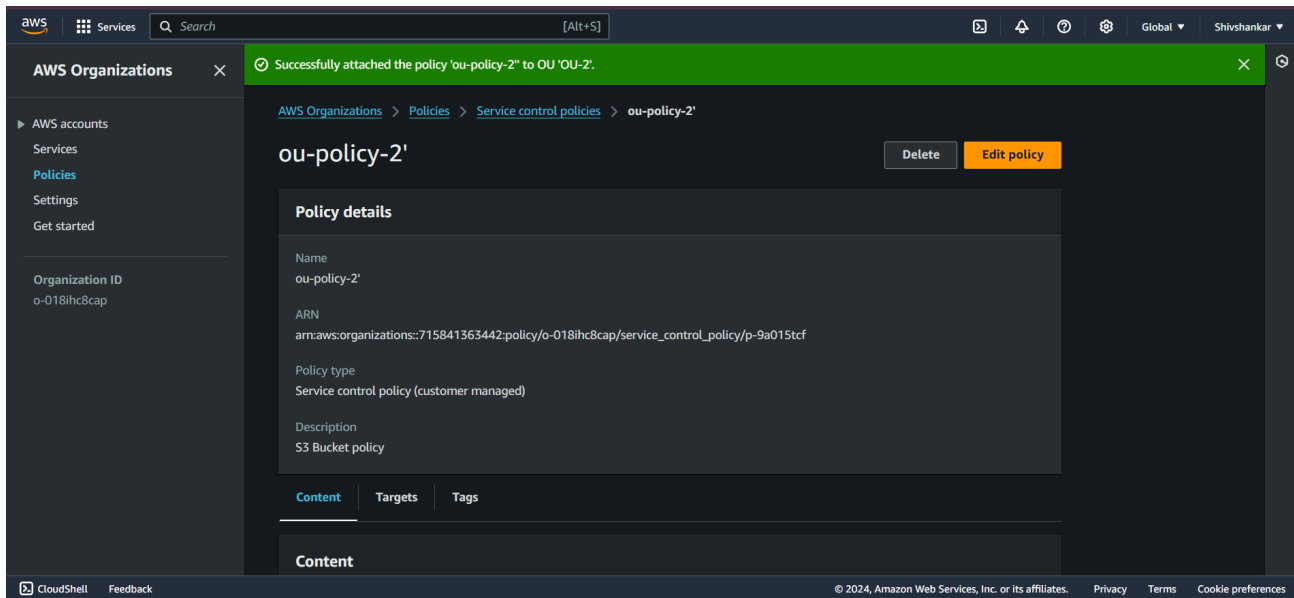
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## ★ OU-Policy -2



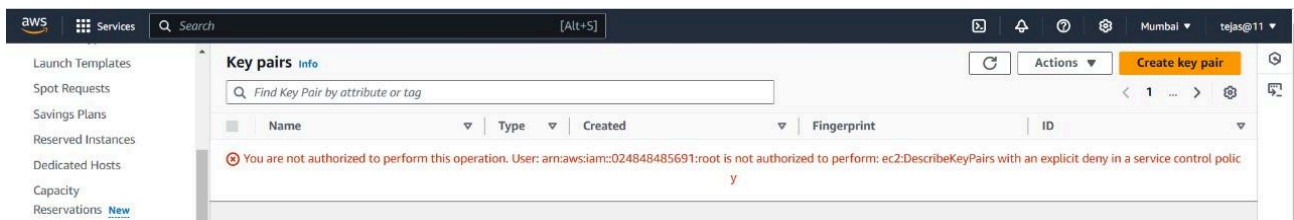
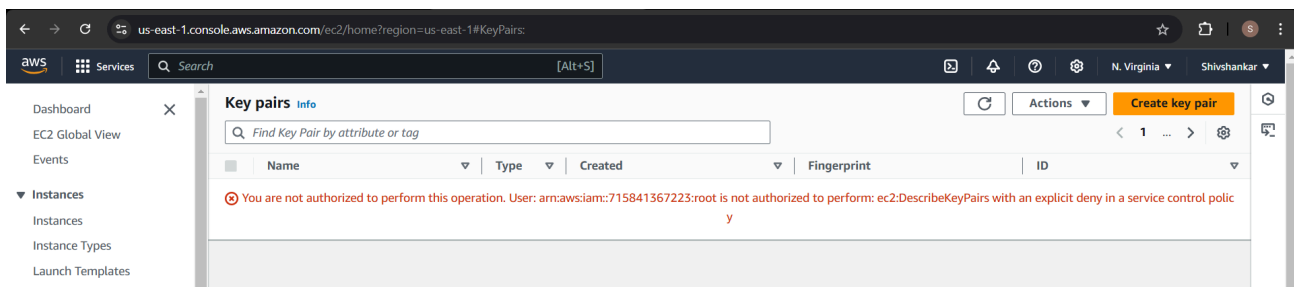
→ Attach Policies to respective OUs





## Step 3: Verify attached Policies

### ★ OU-1



### ★ OU-2

aws

Services

Search

[Alt+S]

Mumbai

Manavi\_Pawar

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable

☒ Enable

Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Failed to create bucket

To create a bucket, the `s3:CreateBucket` permission is required.

View your permissions in the [IAM console](#). [Identity and Access Management in Amazon S3](#)

API response

Cancel

Create bucket

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences