Practical No 5
AWS Organization

Name: Shivshankar Ghyar
PRN: 202201040031
Batch: CCF1

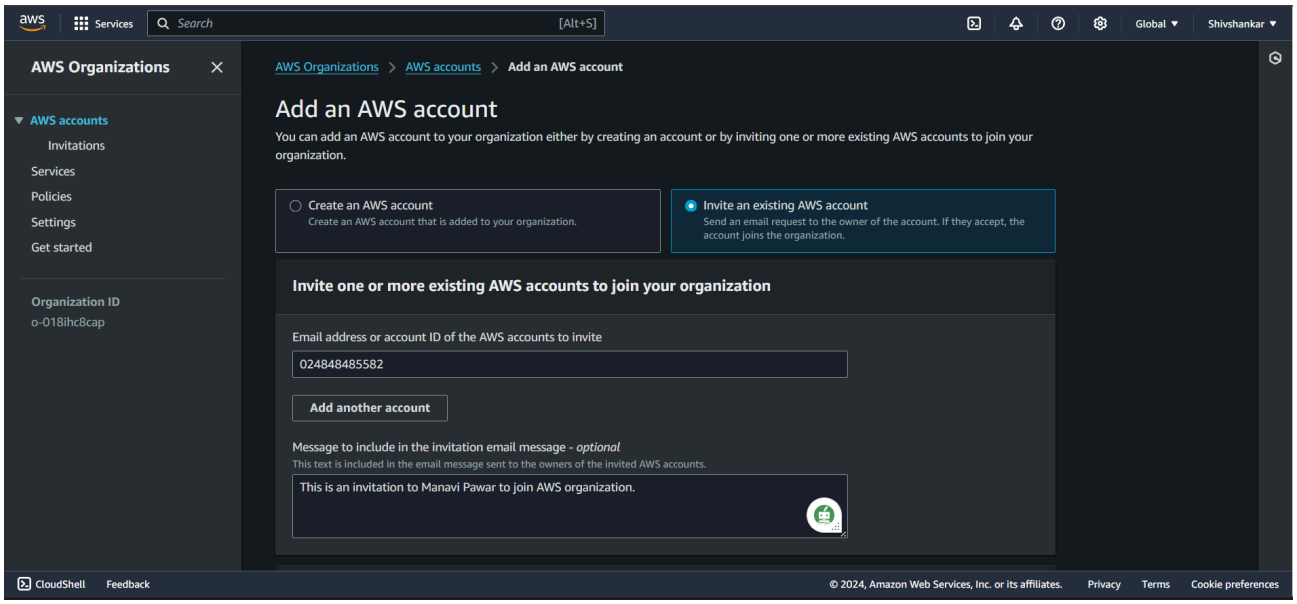
Problem Statement

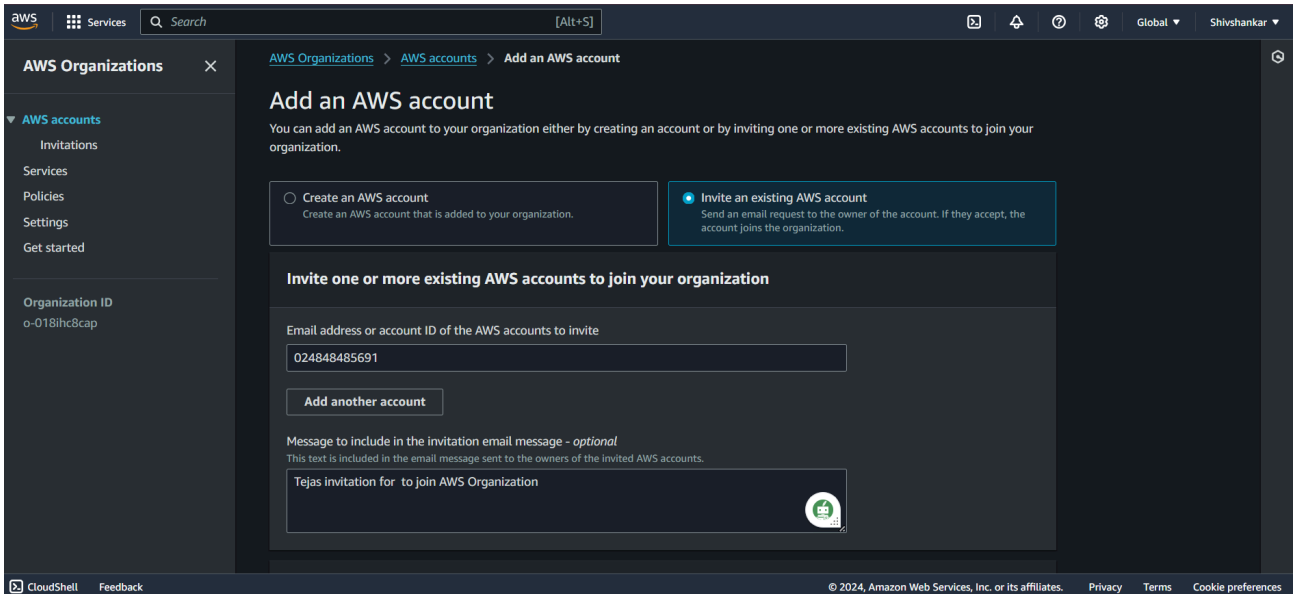
Designing a scalable and secure AWS organization that supports a multi-account structure for effective resource management and access control. The goal is to enable controlled access to AWS EC2 and S3 services across different accounts in the organization, allowing for specific user roles and permissions.

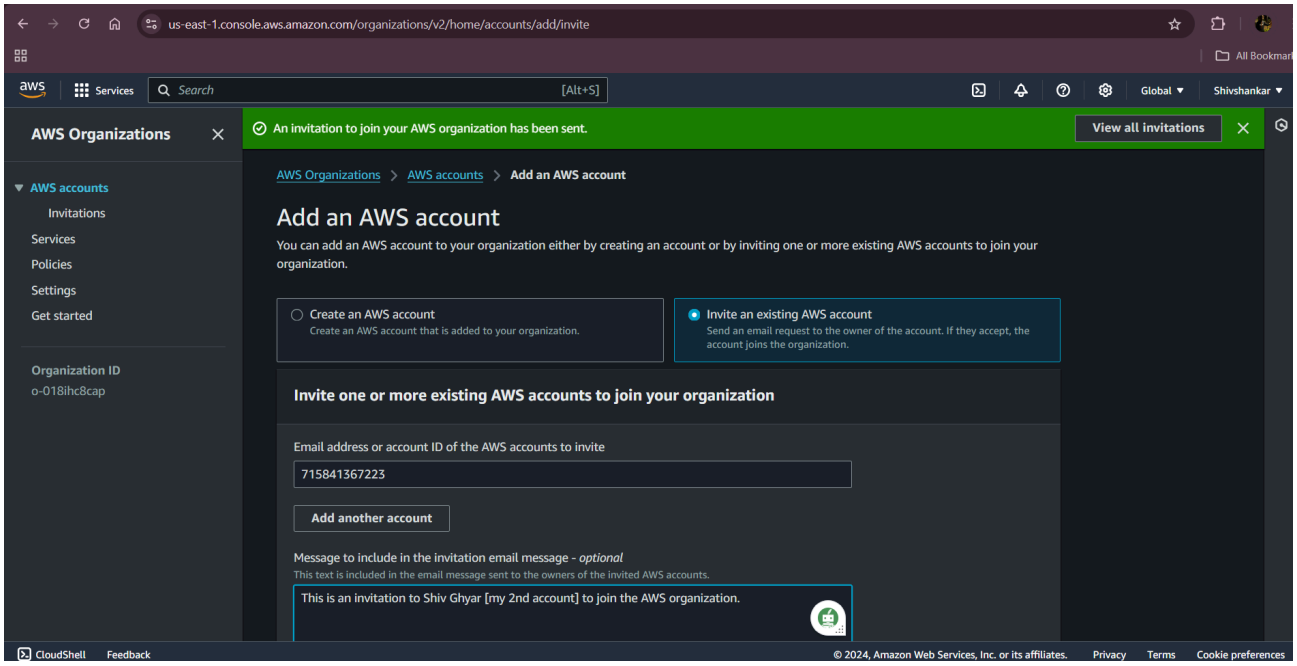
Step 1: Set Up AWS Organizations

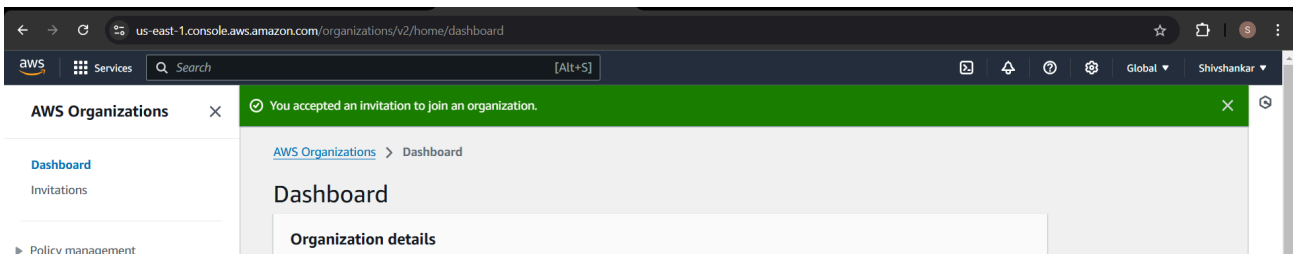
➔ **Create AWS Organization**

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

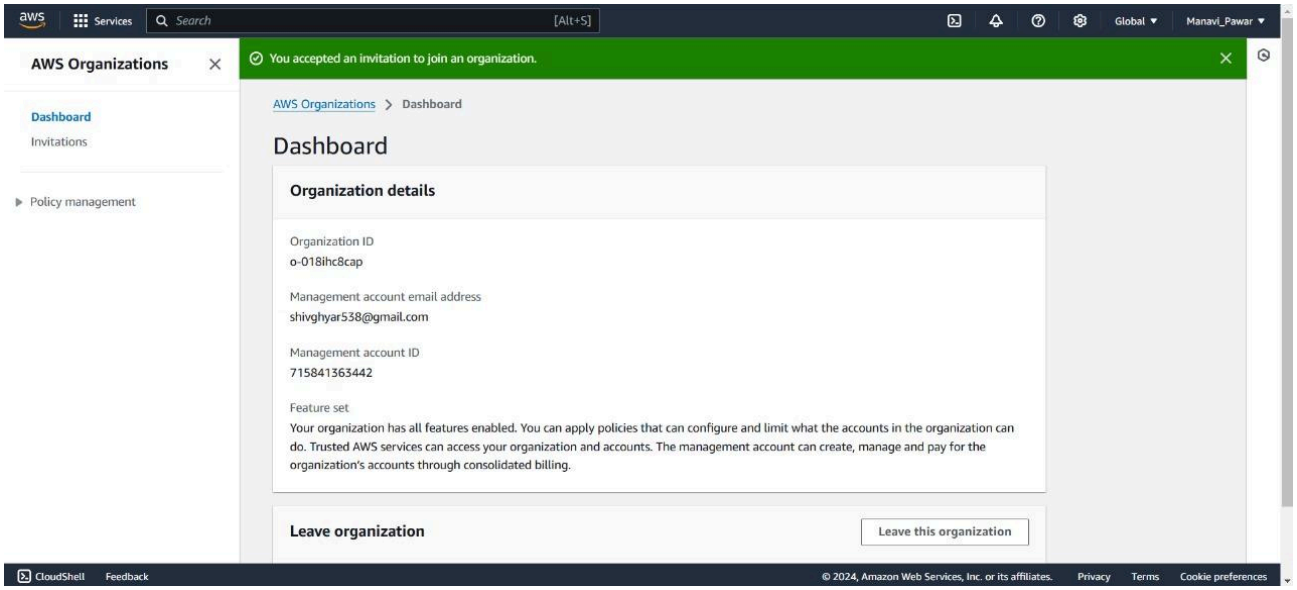




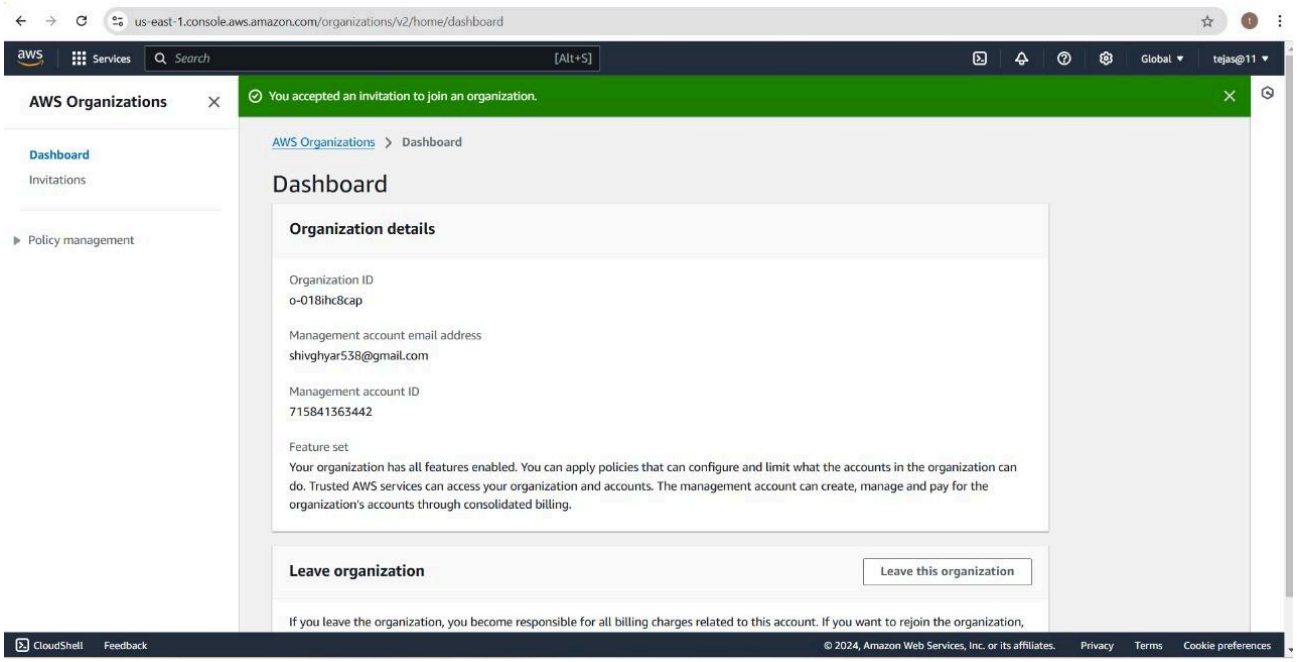




[This is my 2nd acct]



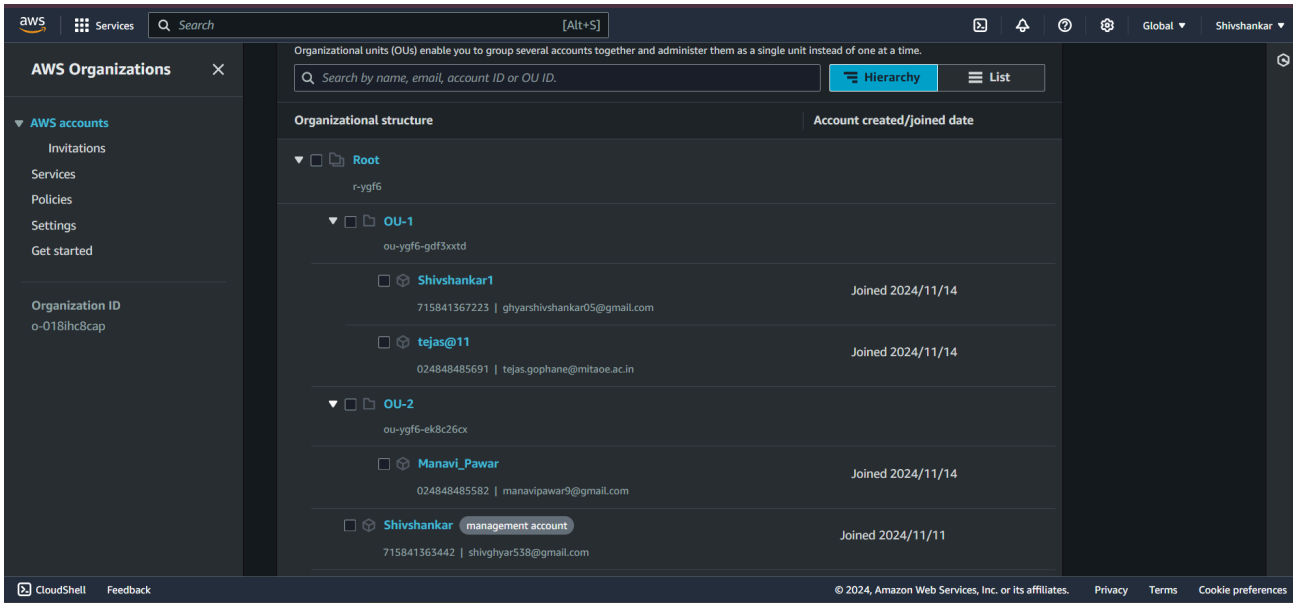
This is Manavi Pawar's Account



This is Tejas Account

➔ Create OUs and move members to them

★ **Final setup of AWS orgnization**



Step 2:Create Policies for Differnent OU

OU-2=> EC2 Key pair [Explict Deny]

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

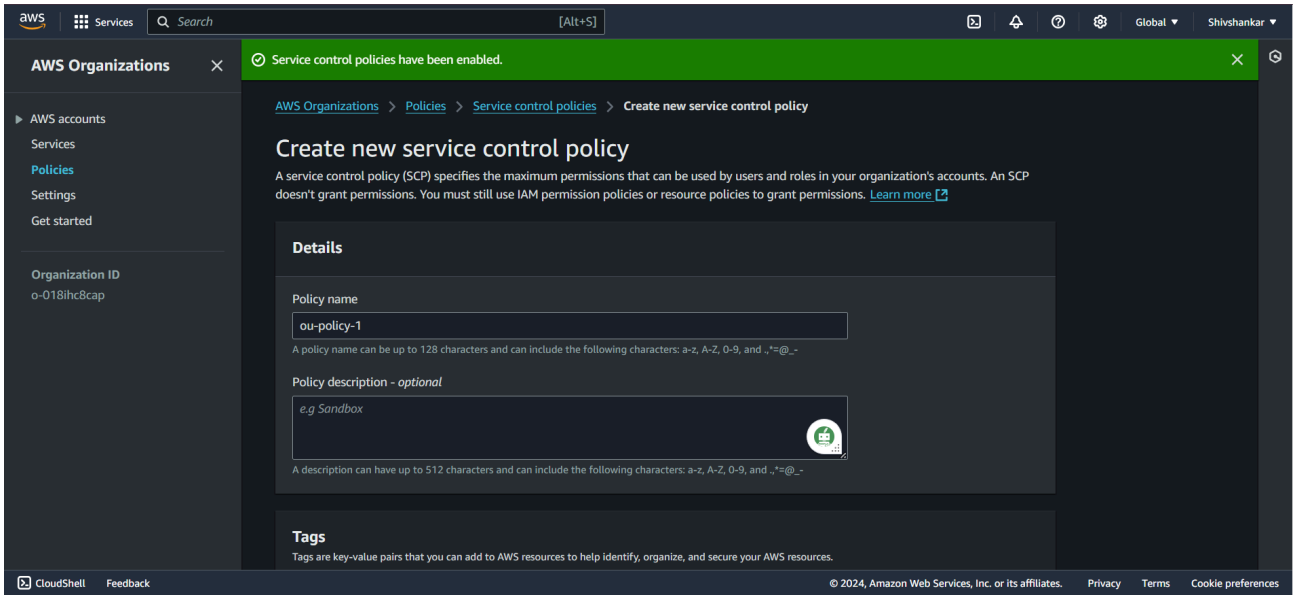
Users: Manavi_Pawar

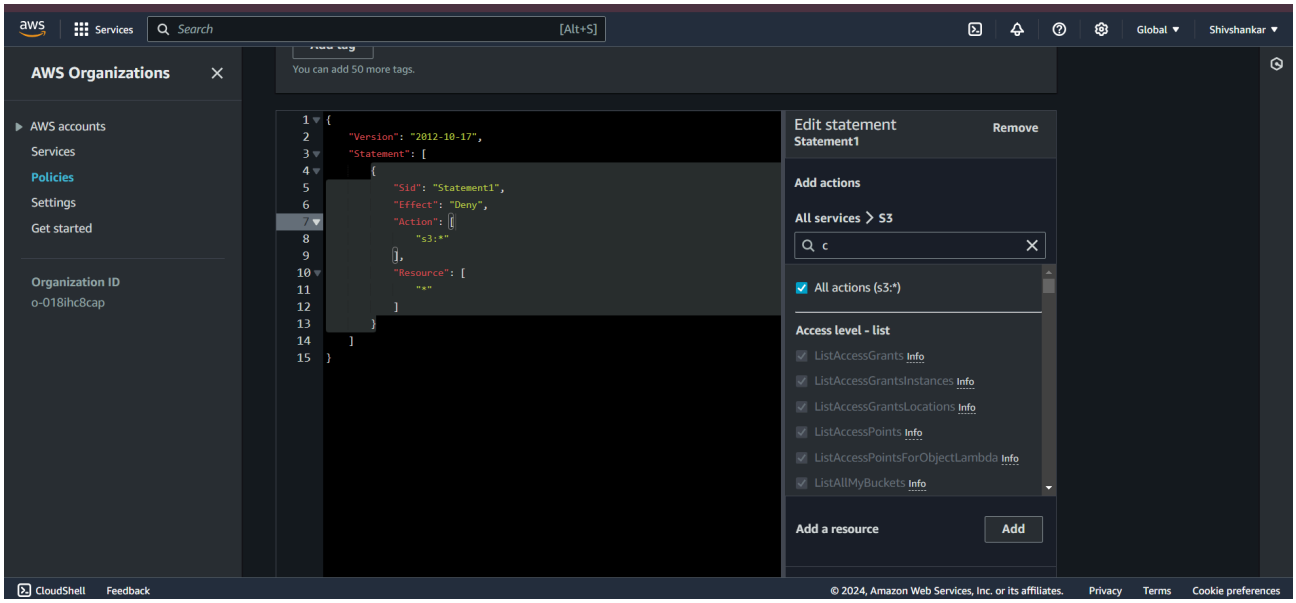
OU-1 => S3 Bucket [Explict Deny]

Users: 1.tejas@11
2.Shivshankar1

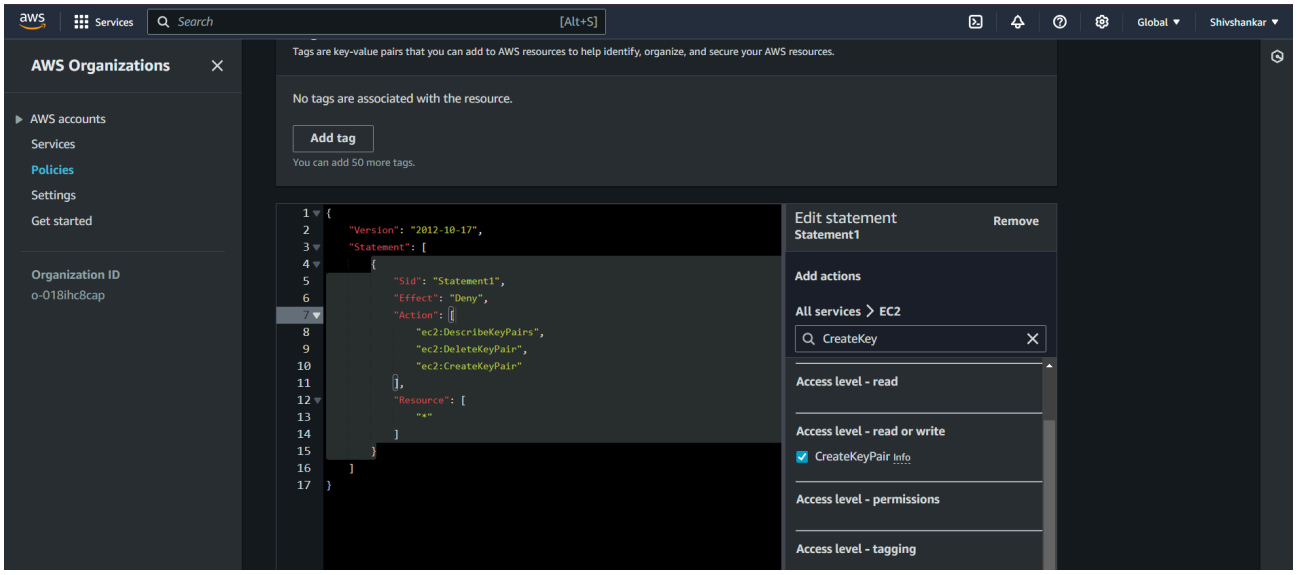
➔ Go to AWS organization → policy → enable Service Control Policy → Create policy

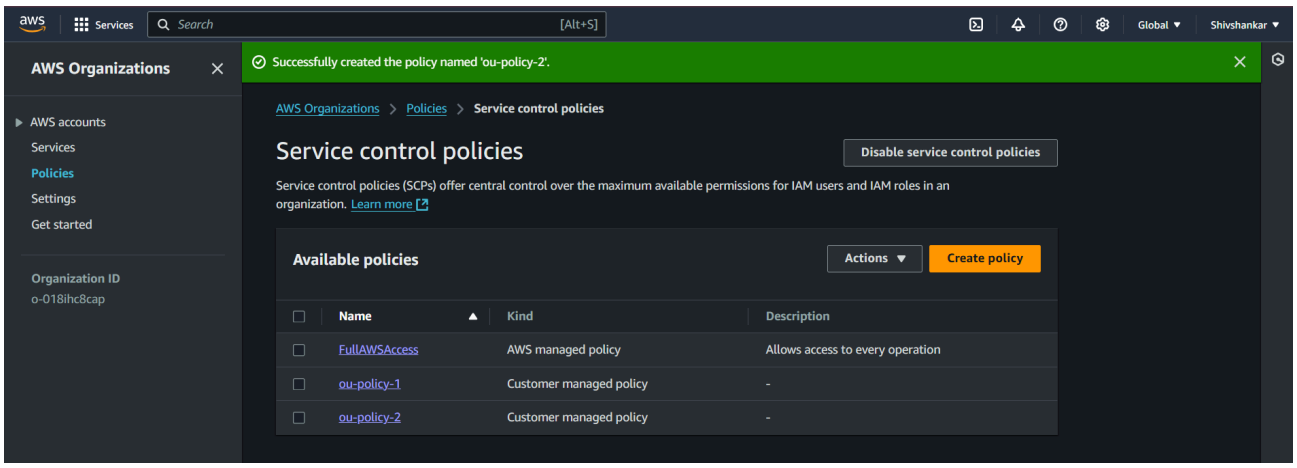
★ **OU-Policy-1**



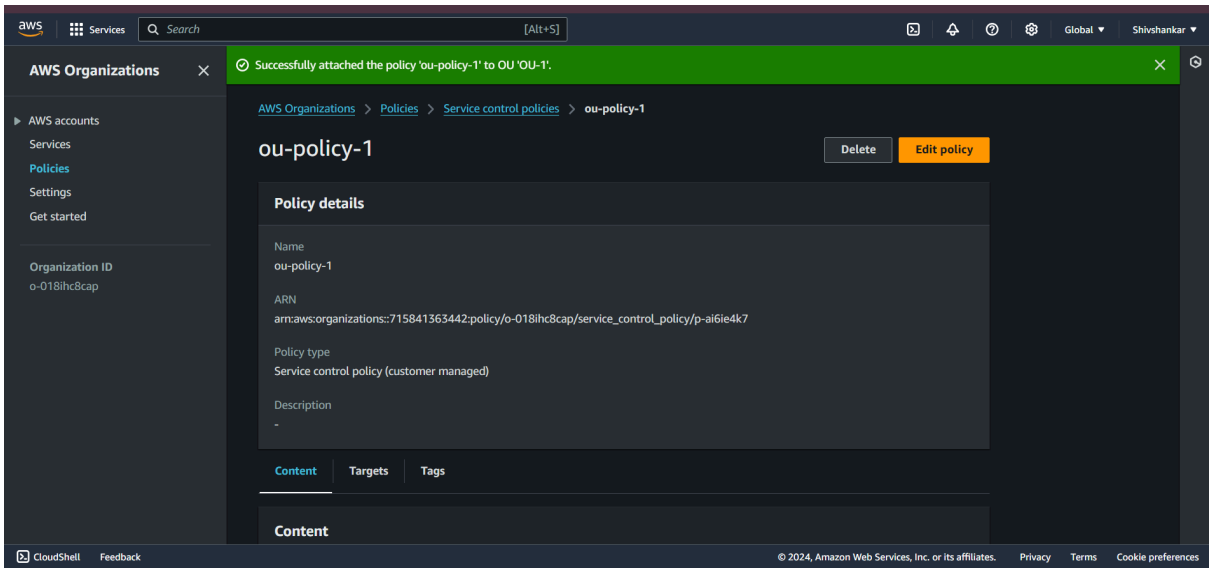


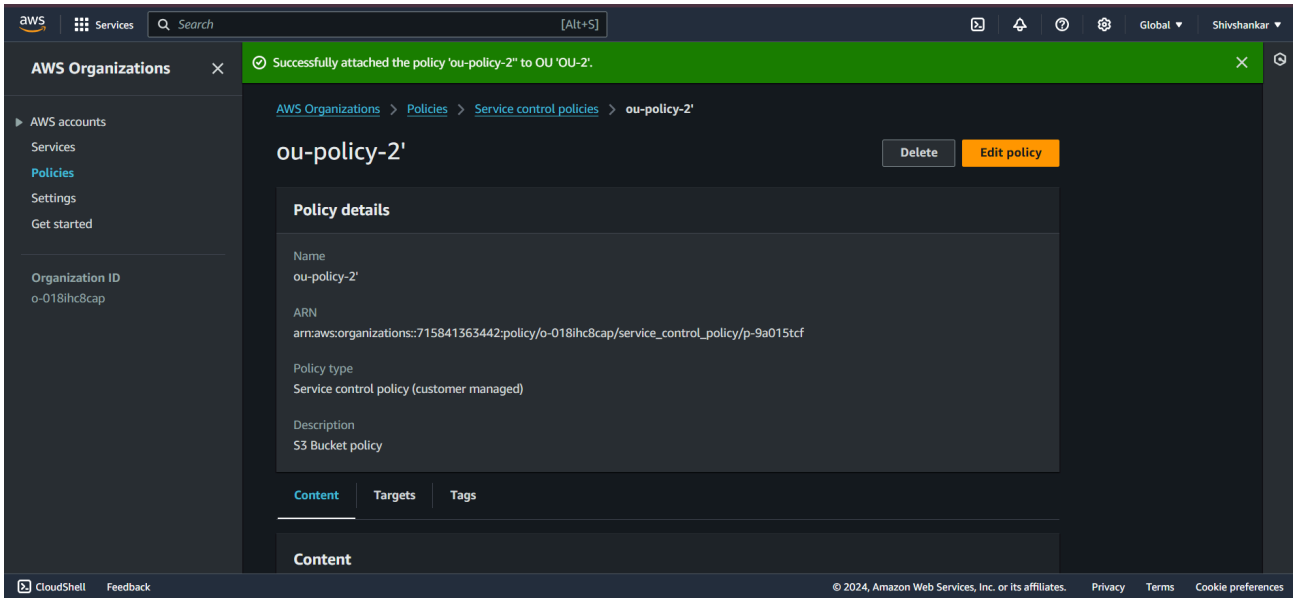
★ **OU-Policy -2**





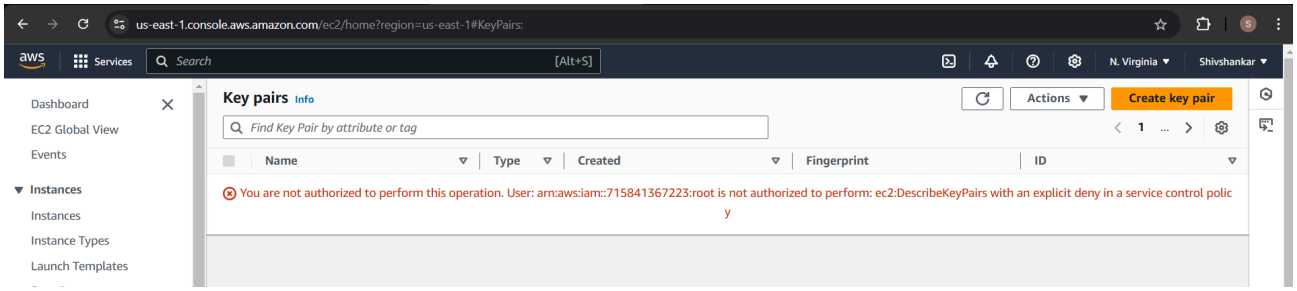
➔ Attach Policies to respective OUs

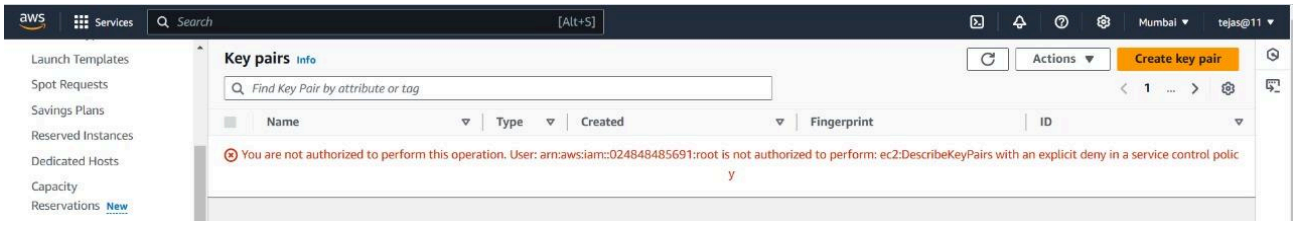




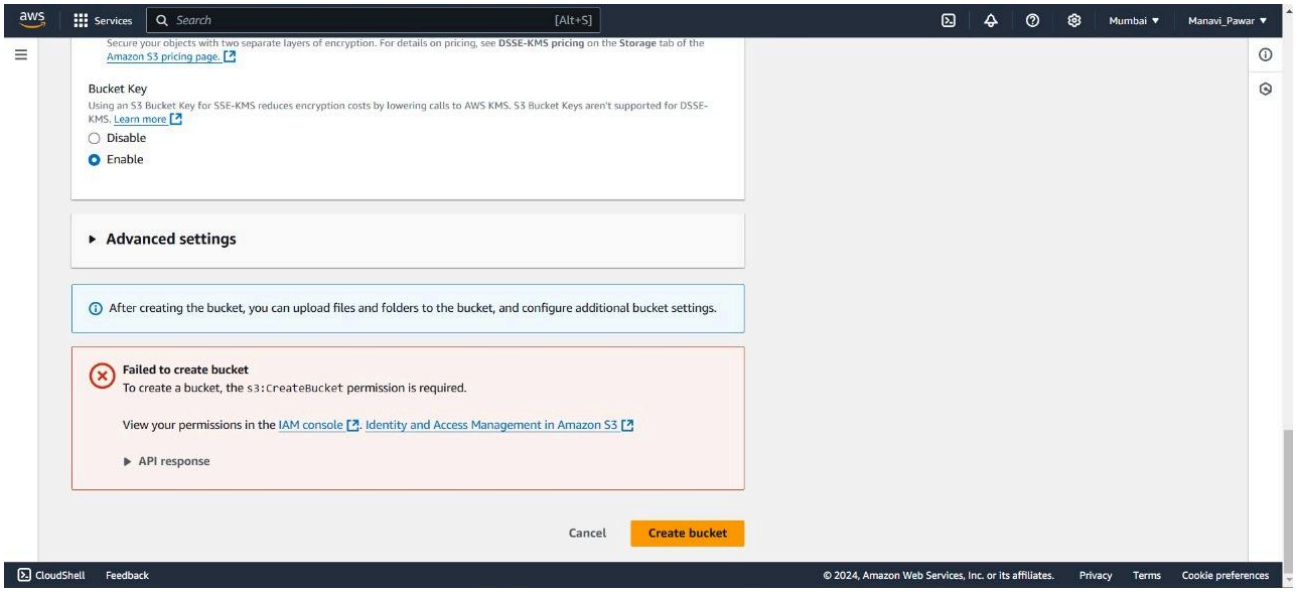
Step 3: Verify attached Policies

★ **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