Developing security policies for a web application on AWS infrastructure

[Activity-2]

—-----—---

Name: Shivshankar Ghyar
PRN: 202201040031
Batch: CCF1

—-- —--

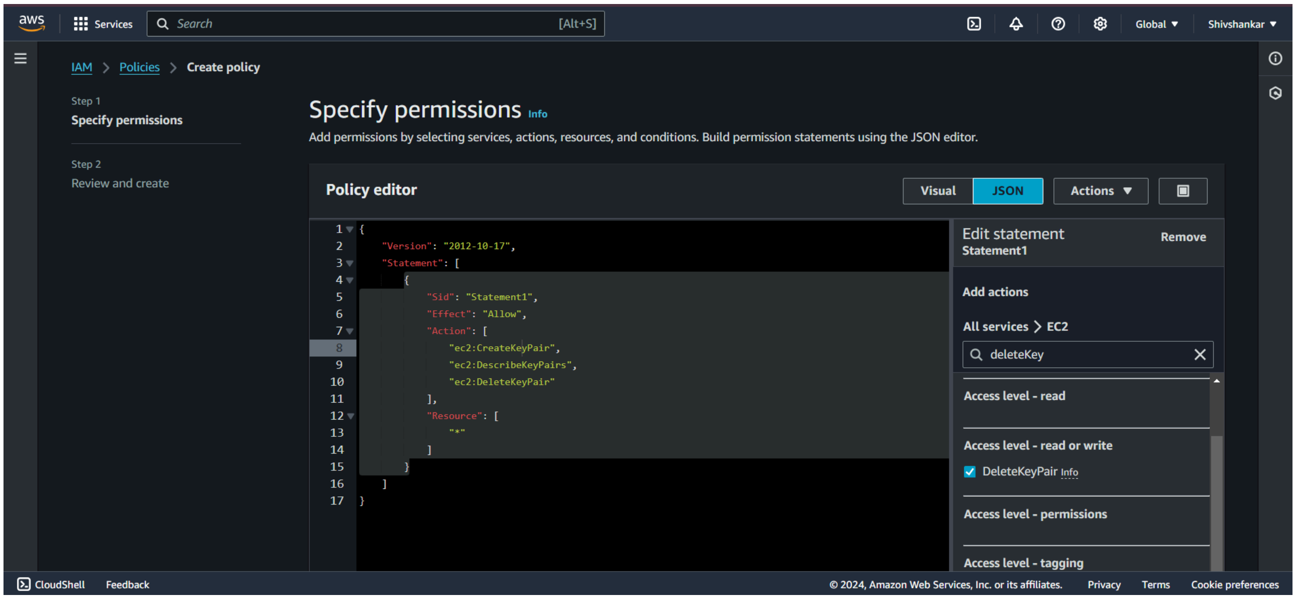
Problem Statement

Compare various types of Security Policies available on AWS for securing the application. Create all those policies using console and command line.

Case 1: Through AWS Console

Step1 :Creation of Security Policy

- ➔ Go to **IAM** > select **Policies** > click **Create policy**.
- ➔ Choose either the **Visual editor** or **JSON editor** to define the policy.
- ➔ Specify the **services**, **actions**, and **resources** that the policy will apply to.
- ➔ Add the necessary **actions**, **services**, and **resources** for your policy.

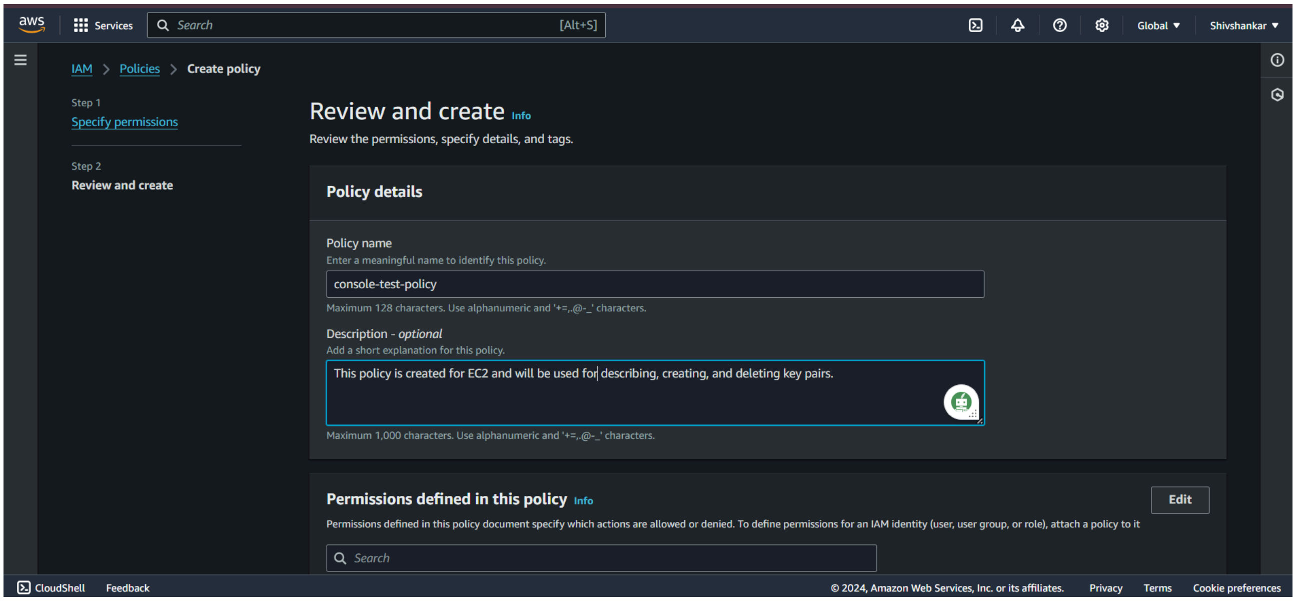


Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:DeleteKeyPair"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

deleteKey

☑ DeleteKeyPair Info



Review and create Info

Review the permissions, specify details, and tags.

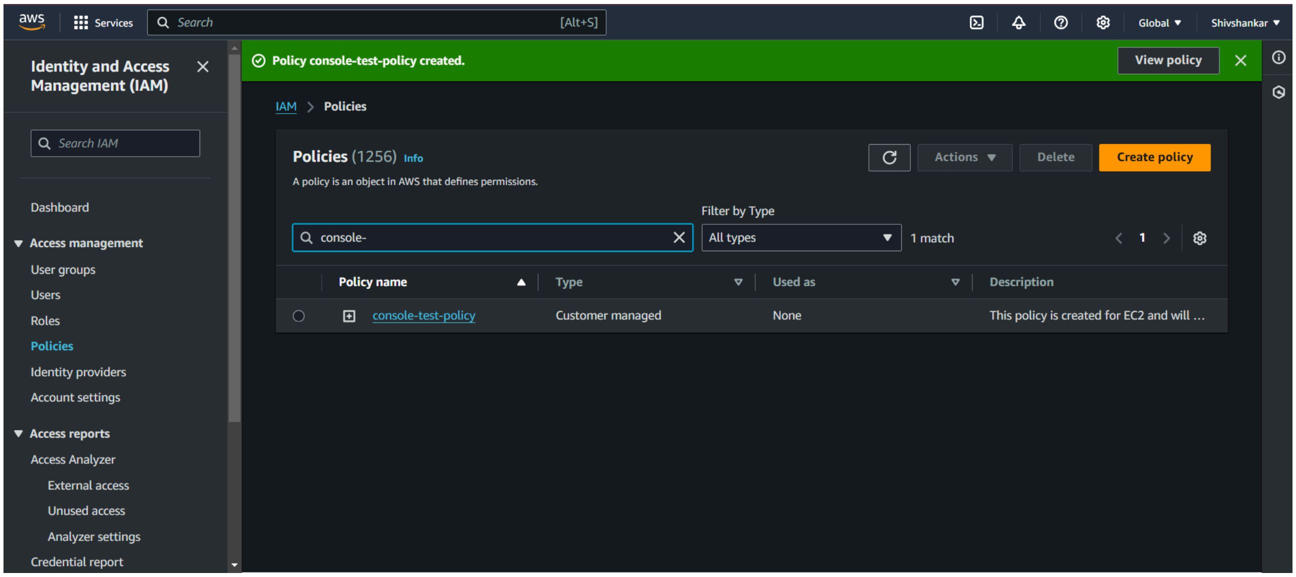
Policy details

Policy name
Enter a meaningful name to identify this policy.
console-test-policy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.
This policy is created for EC2 and will be used for describing, creating, and deleting key pairs.
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it



Policy console-test-policy created.

Policies (1256) Info

A policy is an object in AWS that defines permissions.

Filter by Type

console-   All types   1 match

	Policy name	Type	Used as	Description
○	console-test-policy	Customer managed	None	This policy is created for EC2 and will ...

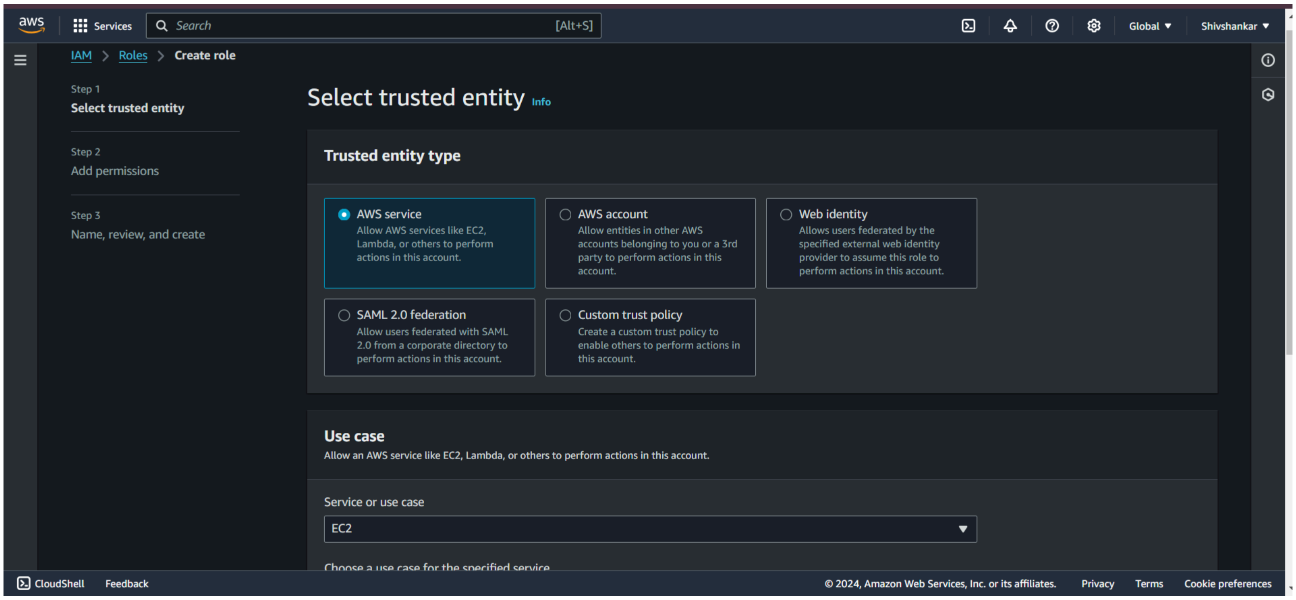
Step 2: Creating a Role

➔ Go to IAM > select Roles > click Create role.

➔ Choose the Trusted Entity Type and select the Use Case.

➔ Add permissions by attaching the previously created policy, "console-policy-test".

➔ Provide a name for the role, review the settings, and click Create role.



Select trusted entity

Trusted entity type

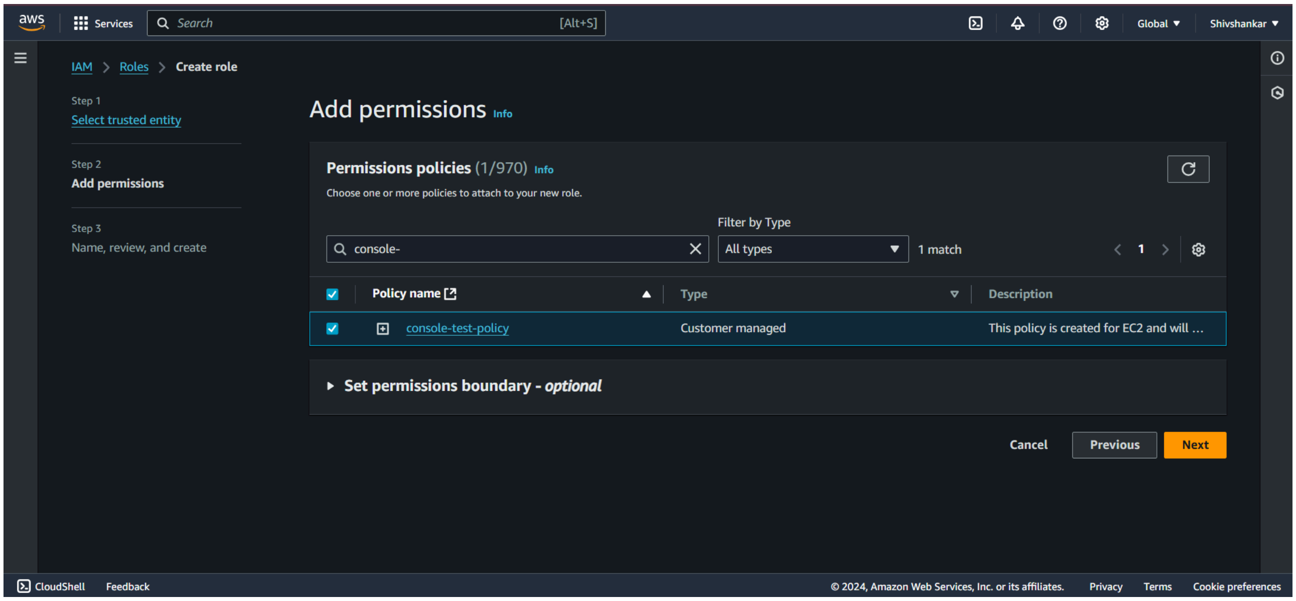
- ● AWS service — Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ○ AWS account — Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ○ Web identity — Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ○ SAML 2.0 federation — Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ○ Custom trust policy — Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case: EC2

Choose a use case for the specified service



Add permissions

Permissions policies (1/970)

Choose one or more policies to attach to your new role.

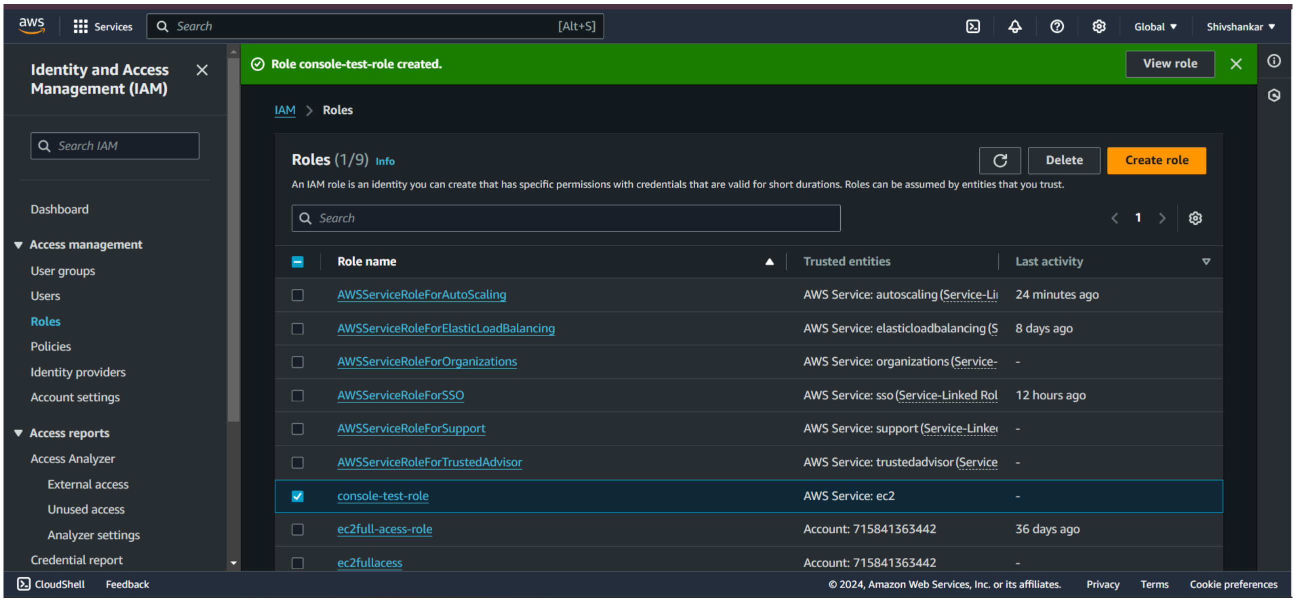
Search: console-

Filter by Type: All types

1 match

☑	Policy name	Type	Description
☑	console-test-policy	Customer managed	This policy is created for EC2 and will …

▸ Set permissions boundary - *optional*



Role console-test-role created.

IAM > Roles

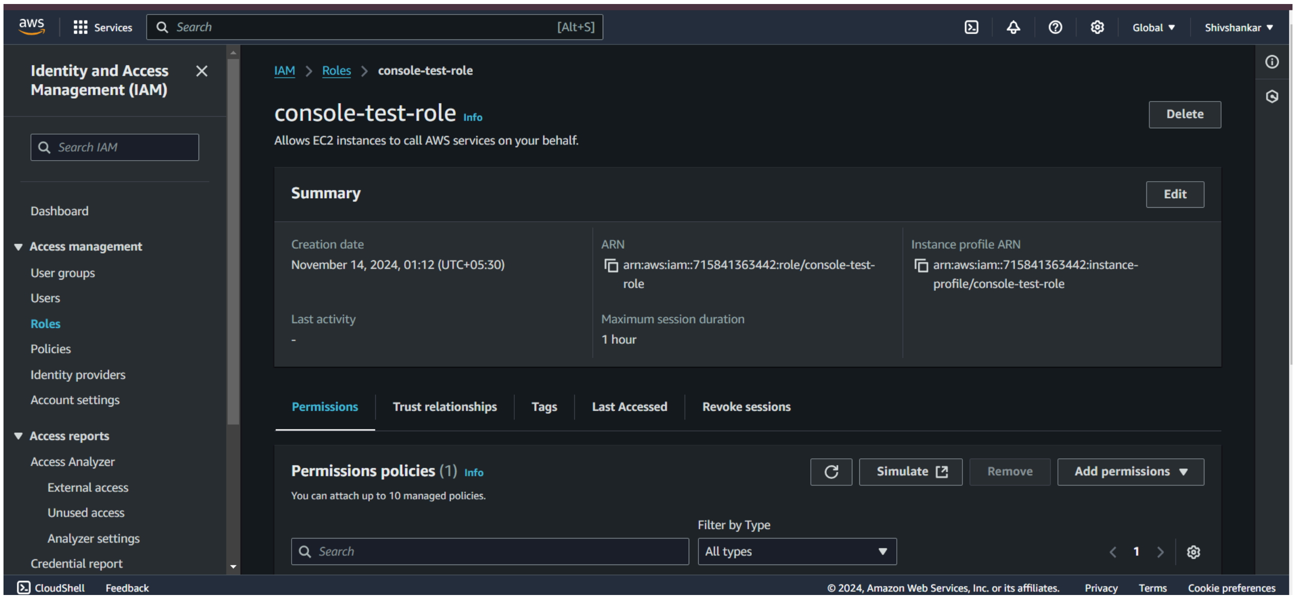
Roles (1/9) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

	Role name	Trusted entities	Last activity
□	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Li	24 minutes ago
□	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (S	8 days ago
□	AWSServiceRoleForOrganizations	AWS Service: organizations (Service-	-
□	AWSServiceRoleForSSO	AWS Service: sso (Service-Linked Rol	12 hours ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
☑	console-test-role	AWS Service: ec2	-
□	ec2full-acess-role	Account: 715841363442	36 days ago
□	ec2fullaccess	Account: 715841363442	-

Step 3: Creation of Permission Boundary

- ➔ Go to IAM > select Roles > choose the created role, "console-test-role".
- ➔ Navigate to Permission boundary and set the permission boundary.
- ➔ Add permissions by attaching the previously created policy, "console-test-policy".



IAM > Roles > console-test-role

console-test-role Info

Allows EC2 instances to call AWS services on your behalf.

Summary

Creation date: November 14, 2024, 01:12 (UTC+05:30)

ARN: arn:aws:iam::715841363442:role/console-test-role

Instance profile ARN: arn:aws:iam::715841363442:instance-profile/console-test-role

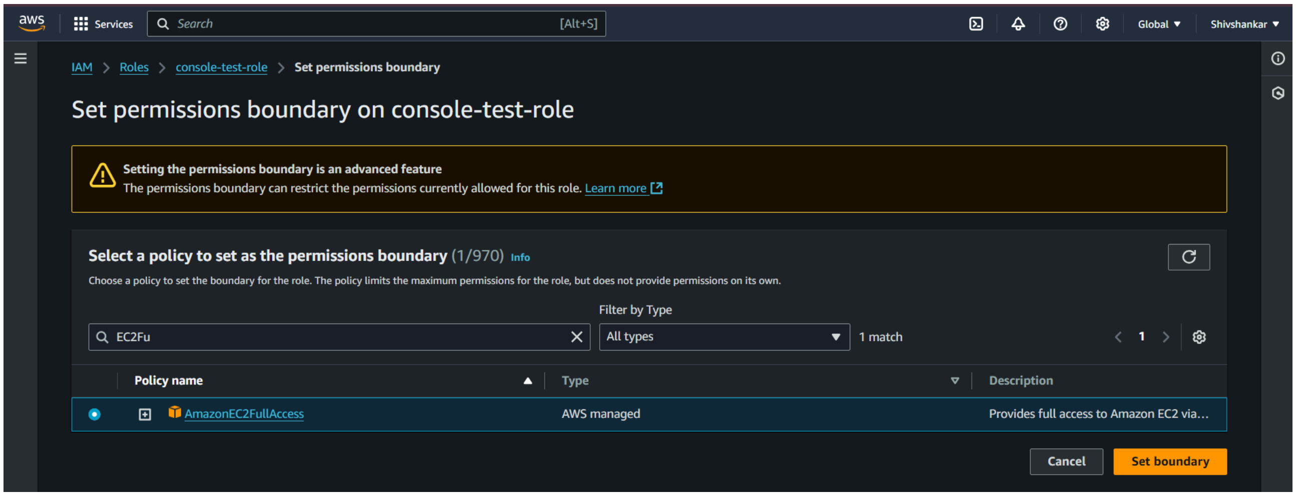
Last activity: -

Maximum session duration: 1 hour

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type: All types



IAM > Roles > console-test-role > Set permissions boundary

Set permissions boundary on console-test-role

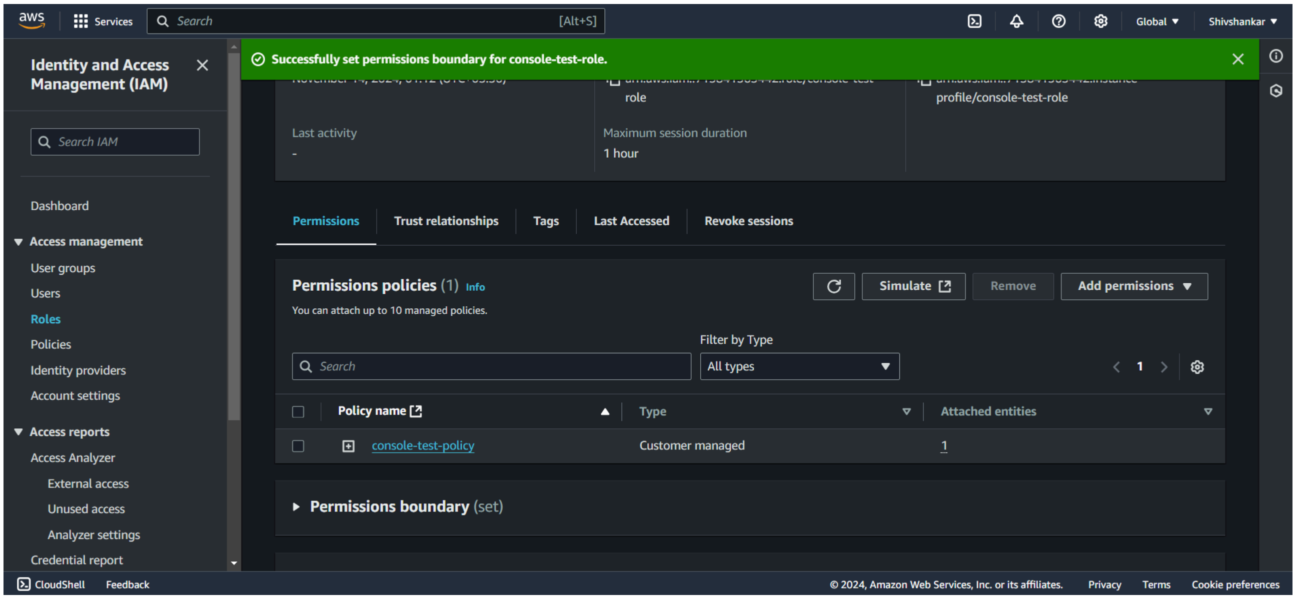
Setting the permissions boundary is an advanced feature
The permissions boundary can restrict the permissions currently allowed for this role. Learn more

Select a policy to set as the permissions boundary (1/970) Info

Choose a policy to set the boundary for the role. The policy limits the maximum permissions for the role, but does not provide permissions on its own.

Search: EC2Fu
Filter by Type: All types
1 match

	Policy name	Type	Description
●	AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via…



Successfully set permissions boundary for console-test-role.

role
profile/console-test-role

Last activity: -
Maximum session duration: 1 hour

Permissions policies (1) Info

You can attach up to 10 managed policies.

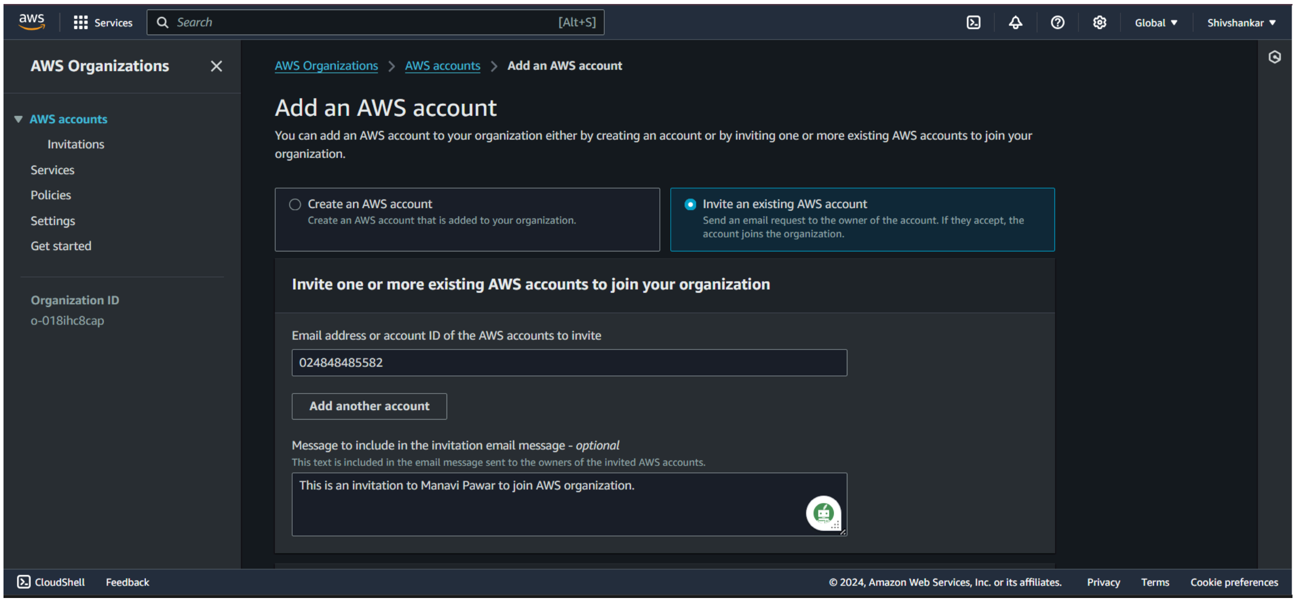
Filter by Type: All types

	Policy name	Type	Attached entities
□	console-test-policy	Customer managed	1

Permissions boundary (set)

Step 4: Creation of Service Control Policy (SCP)

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



Organization ID
o-018ihc8cap

AWS Organizations > AWS accounts > **Add an AWS account**

Add an AWS account

You can add an AWS account to your organization either by creating an account or by inviting one or more existing AWS accounts to join your organization.

○ Create an AWS account
Create an AWS account that is added to your organization.

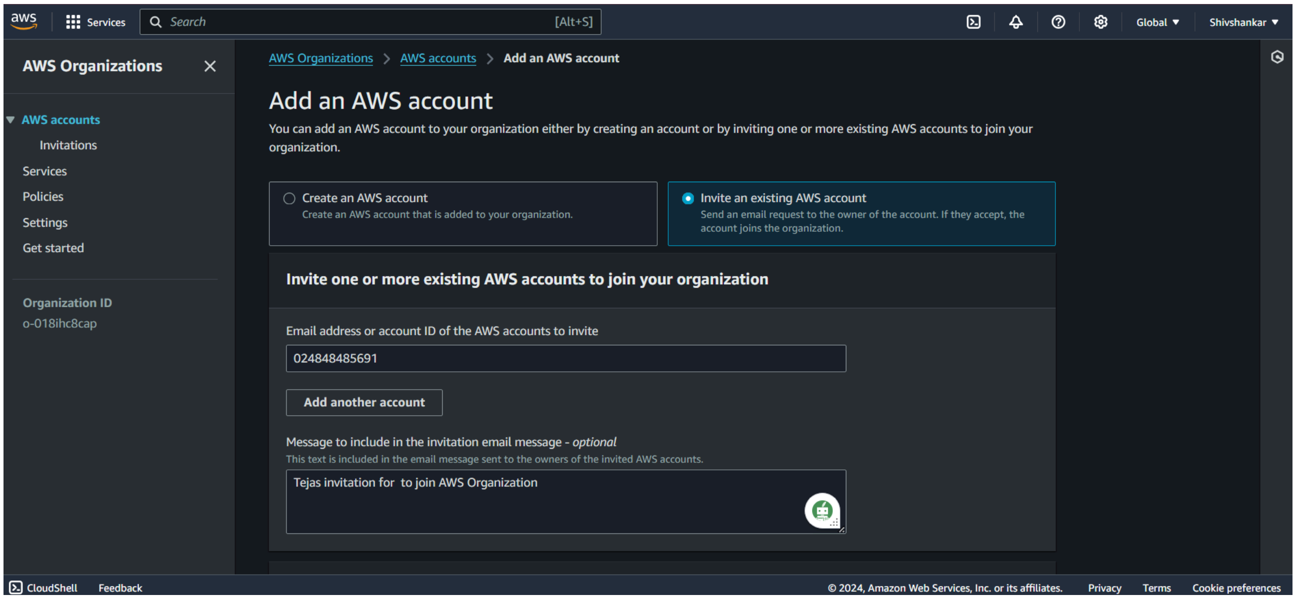
● Invite an existing AWS account
Send an email request to the owner of the account. If they accept, the account joins the organization.

Invite one or more existing AWS accounts to join your organization

Email address or account ID of the AWS accounts to invite
024848485582

Add another account

Message to include in the invitation email message - *optional*
This text is included in the email message sent to the owners of the invited AWS accounts.
This is an invitation to Manavi Pawar to join AWS organization.



Organization ID
o-018ihc8cap

AWS Organizations > AWS accounts > **Add an AWS account**

Add an AWS account

You can add an AWS account to your organization either by creating an account or by inviting one or more existing AWS accounts to join your organization.

○ Create an AWS account
Create an AWS account that is added to your organization.

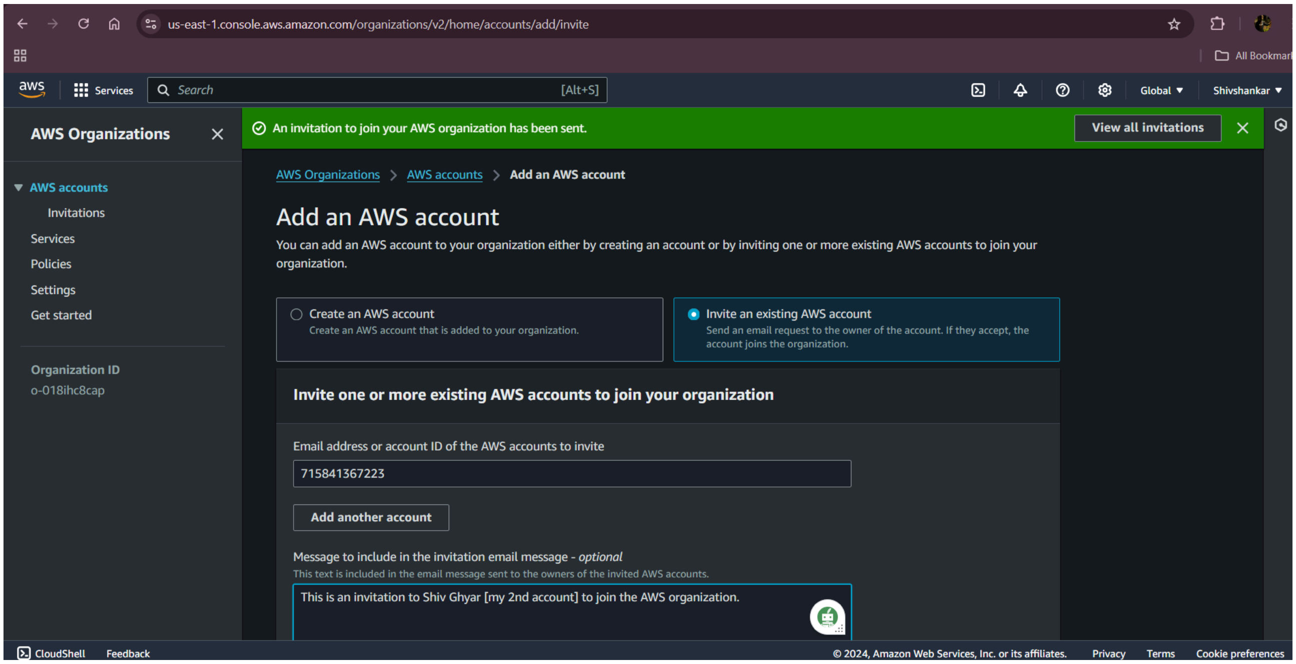
● Invite an existing AWS account
Send an email request to the owner of the account. If they accept, the account joins the organization.

Invite one or more existing AWS accounts to join your organization

Email address or account ID of the AWS accounts to invite
024848485691

Add another account

Message to include in the invitation email message - *optional*
This text is included in the email message sent to the owners of the invited AWS accounts.
Tejas invitation for to join AWS Organization



An invitation to join your AWS organization has been sent.

Organization ID
o-018ihc8cap

AWS Organizations > AWS accounts > Add an AWS account

Add an AWS account

You can add an AWS account to your organization either by creating an account or by inviting one or more existing AWS accounts to join your organization.

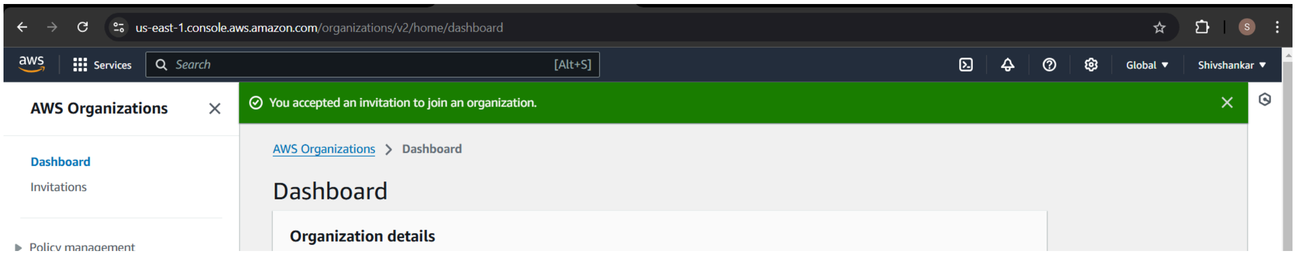
○ Create an AWS account
Create an AWS account that is added to your organization.

● Invite an existing AWS account
Send an email request to the owner of the account. If they accept, the account joins the organization.

Invite one or more existing AWS accounts to join your organization

Email address or account ID of the AWS accounts to invite
715841367223

Message to include in the invitation email message - *optional*
This text is included in the email message sent to the owners of the invited AWS accounts.
This is an invitation to Shiv Ghyar [my 2nd account] to join the AWS organization.



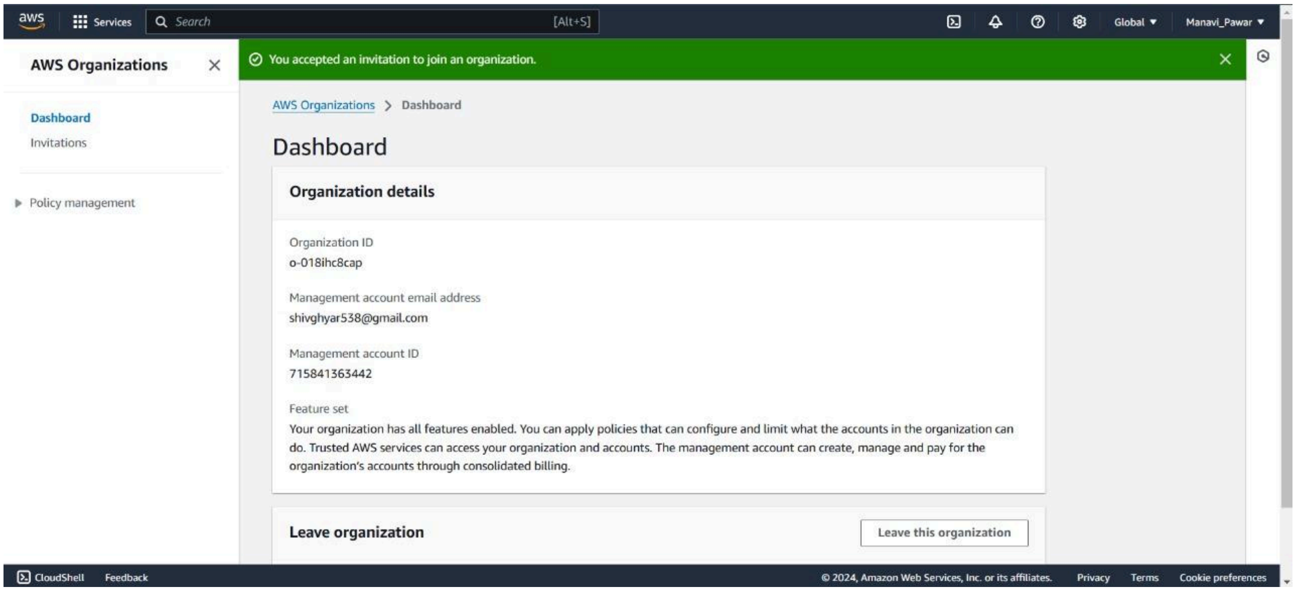
You accepted an invitation to join an organization.

AWS Organizations > Dashboard

Dashboard

Organization details

This is my 2nd acct



You accepted an invitation to join an organization.

AWS Organizations > Dashboard

Dashboard

Organization details

Organization ID
o-018ihc8cap

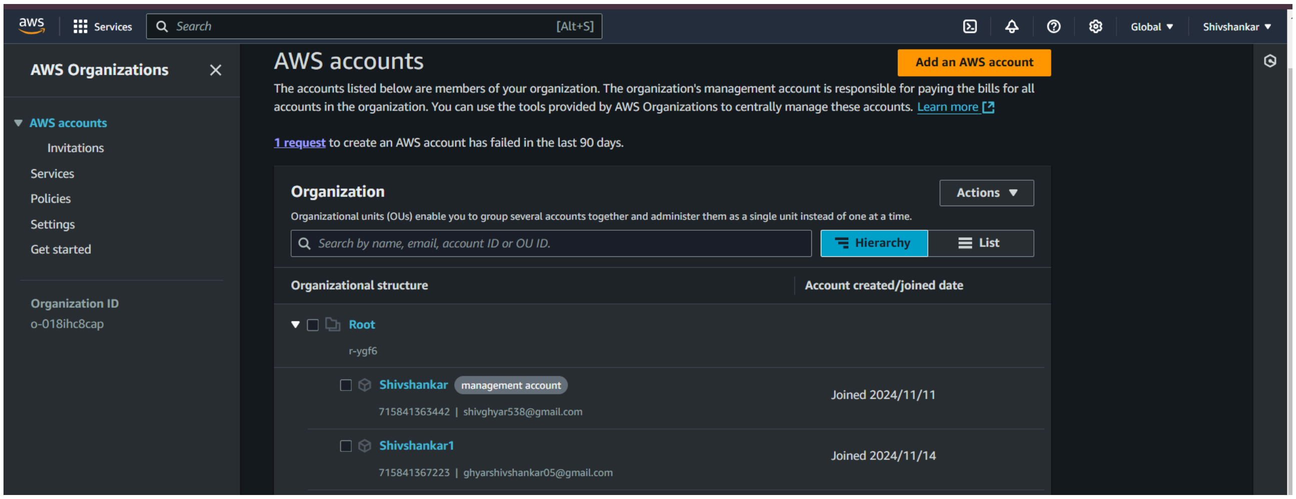
Management account email address
shivghyar538@gmail.com

Management account ID
715841363442

Feature set
Your organization has all features enabled. You can apply policies that can configure and limit what the accounts in the organization can do. Trusted AWS services can access your organization and accounts. The management account can create, manage and pay for the organization's accounts through consolidated billing.

Leave organization

This is Manavi Pawar’s Account



Organization ID
o-018ihc8cap

AWS accounts

The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more

1 request to create an AWS account has failed in the last 90 days.

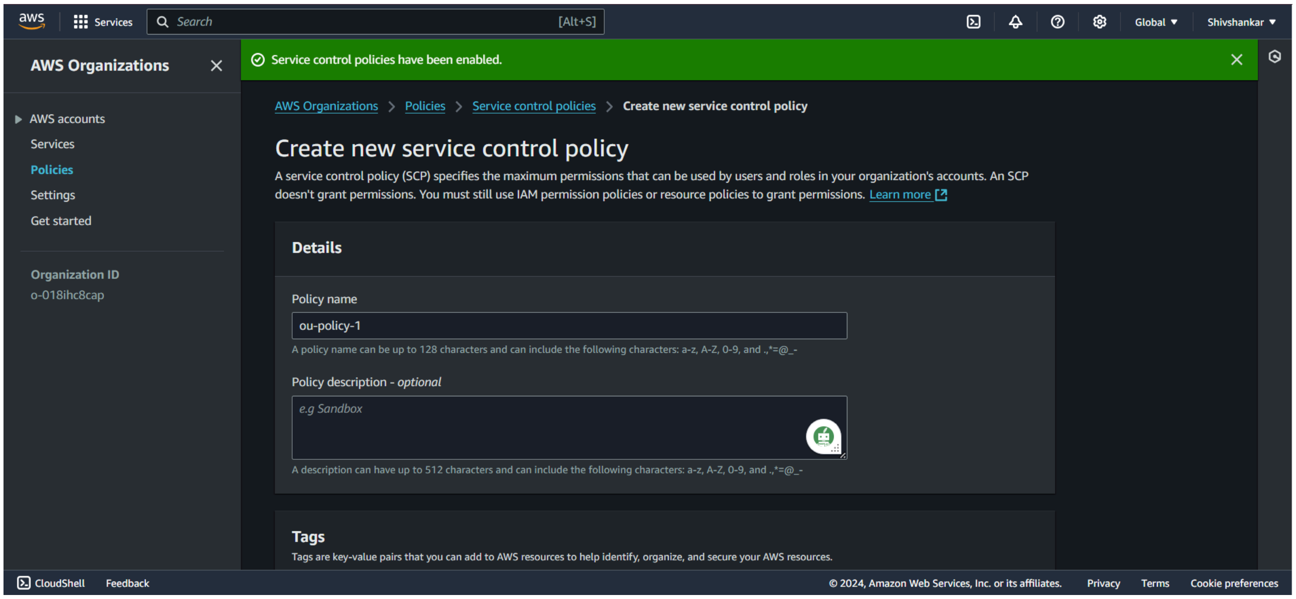
Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Search by name, email, account ID or OU ID.

Organizational structure	Account created/joined date
▾ □ Root r-ygf6	
□ Shivshankar management account 715841363442 | shivghyar538@gmail.com	Joined 2024/11/11
□ Shivshankar1 715841367223 | ghyarshivshankar05@gmail.com	Joined 2024/11/14

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



Service control policies have been enabled.

Organization ID
o-018ihc8cap

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*

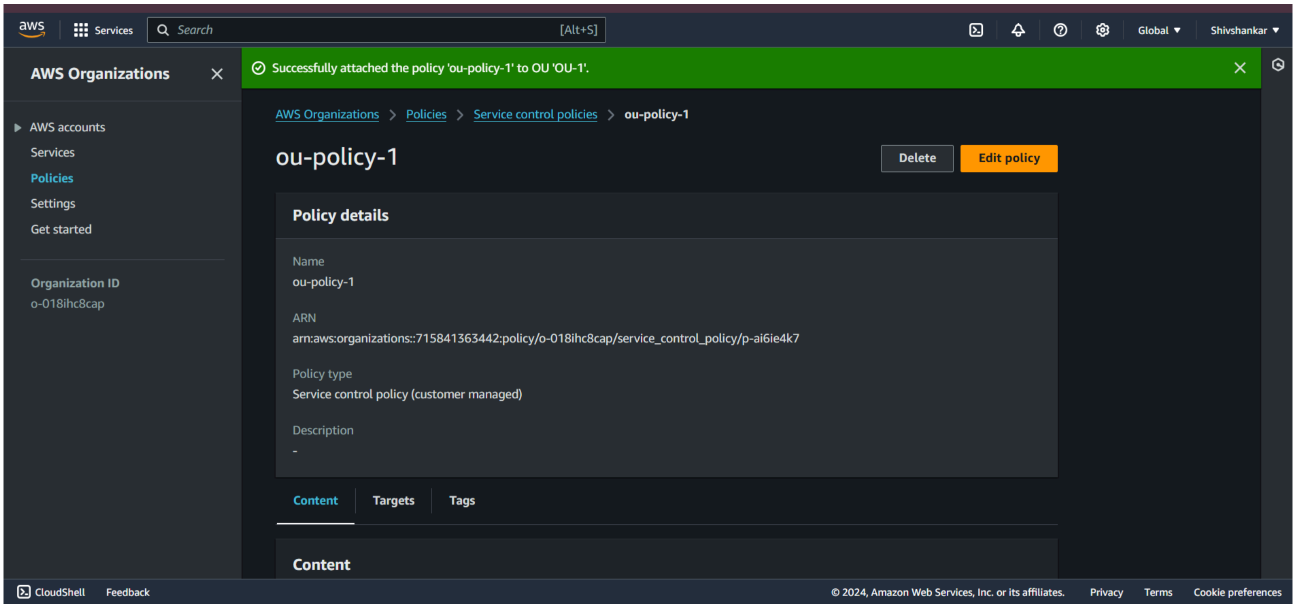
e.g Sandbox

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.

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



Organization ID
o-018ihc8cap

Successfully attached the policy 'ou-policy-1' to OU 'OU-1'.

AWS Organizations > Policies > Service control policies > ou-policy-1

ou-policy-1

Policy details

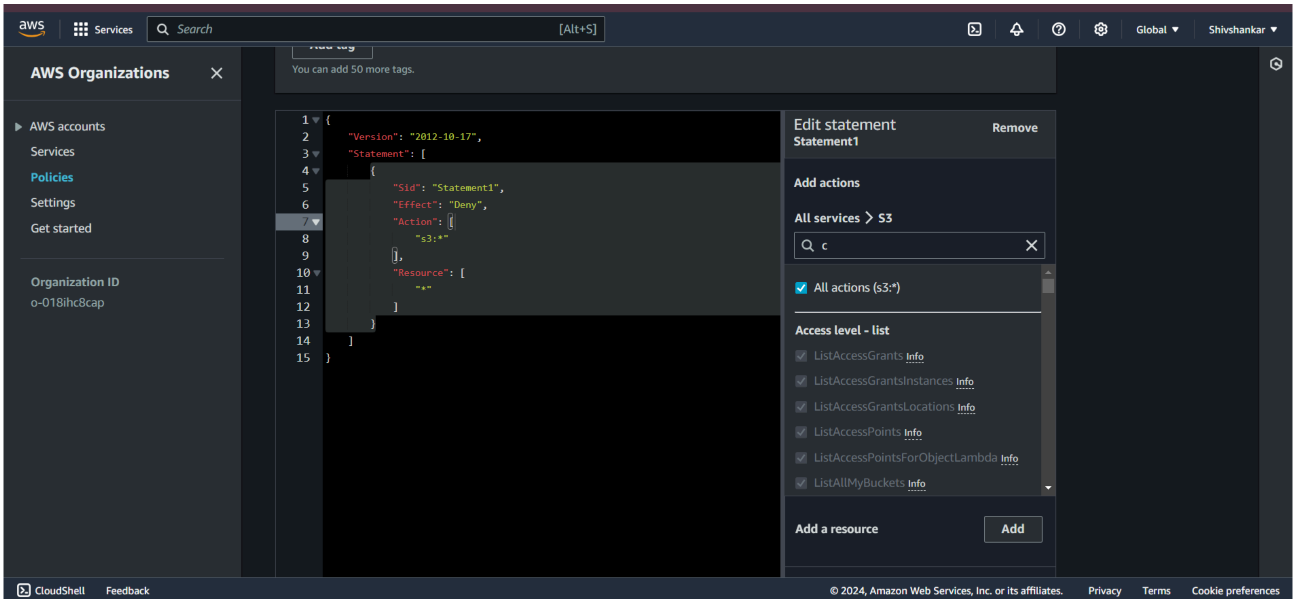
Name
ou-policy-1

ARN
arn:aws:organizations::715841363442:policy/o-018ihc8cap/service_control_policy/p-ai6ie4k7

Policy type
Service control policy (customer managed)

Description
-

Content



Organization ID
o-018ihc8cap

You can add 50 more tags.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Edit statement
Statement1

Add actions

All services > S3

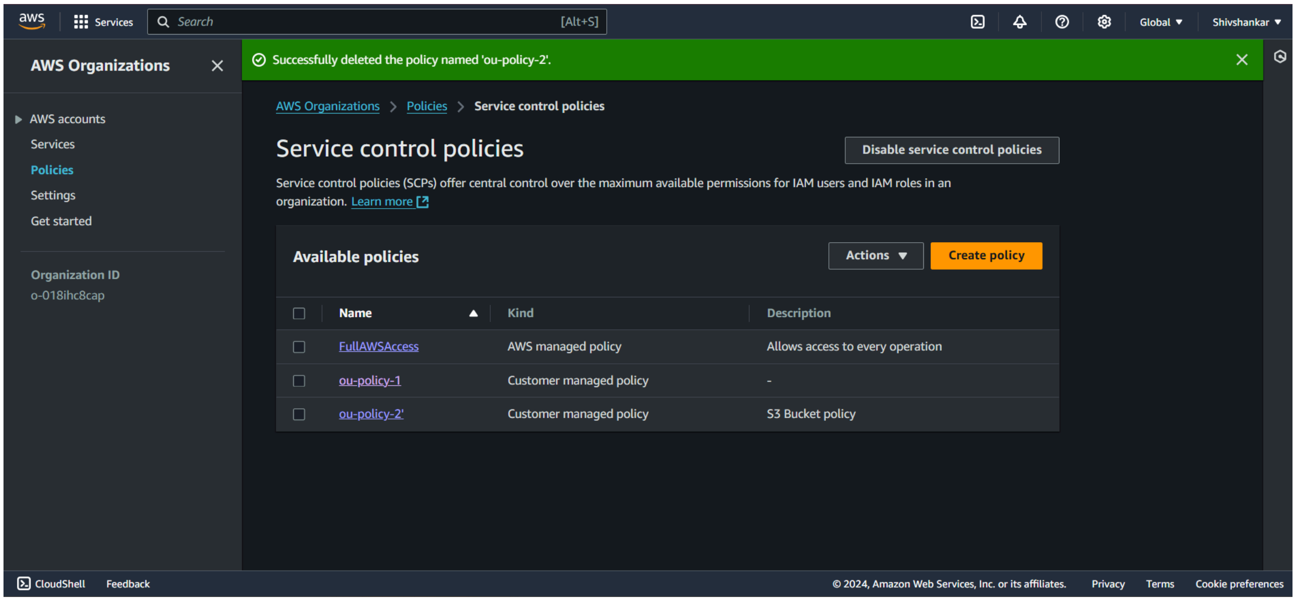
c

☑ All actions (s3:*)

Access level - list

☑ ListAccessGrants Info
☑ ListAccessGrantsInstances Info
☑ ListAccessGrantsLocations Info
☑ ListAccessPoints Info
☑ ListAccessPointsForObjectLambda Info
☑ ListAllMyBuckets Info

Add a resource



Successfully deleted the policy named 'ou-policy-2'.

AWS Organizations > Policies > Service control policies

Service control policies

Disable service control policies

Service control policies (SCPs) offer central control over the maximum available permissions for IAM users and IAM roles in an organization. Learn more

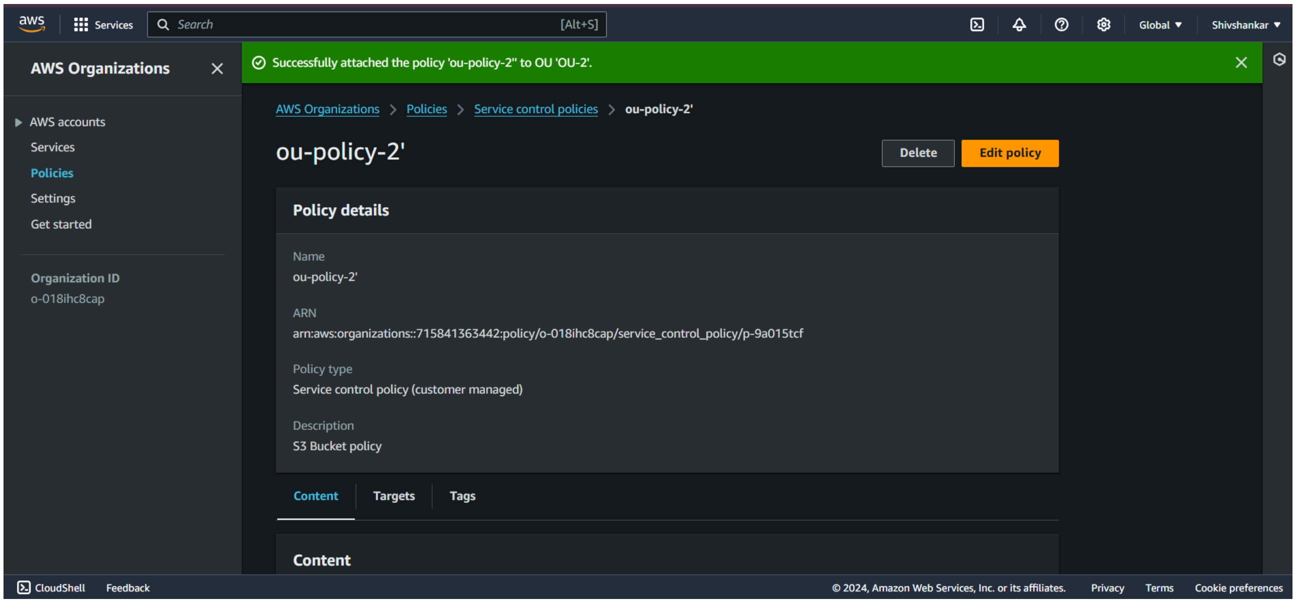
Organization ID
o-018ihc8cap

Available policies

Actions ▼ | Create policy

□	Name ▲	Kind	Description
□	FullAWSAccess	AWS managed policy	Allows access to every operation
□	ou-policy-1	Customer managed policy	-
□	ou-policy-2'	Customer managed policy	S3 Bucket policy

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



Successfully attached the policy 'ou-policy-2'' to OU 'OU-2'.

AWS Organizations > Policies > Service control policies > ou-policy-2'

ou-policy-2'

Delete | Edit policy

Organization ID
o-018ihc8cap

Policy details

Name
ou-policy-2'

ARN
arn:aws:organizations::715841363442:policy/o-018ihc8cap/service_control_policy/p-9a015tcf

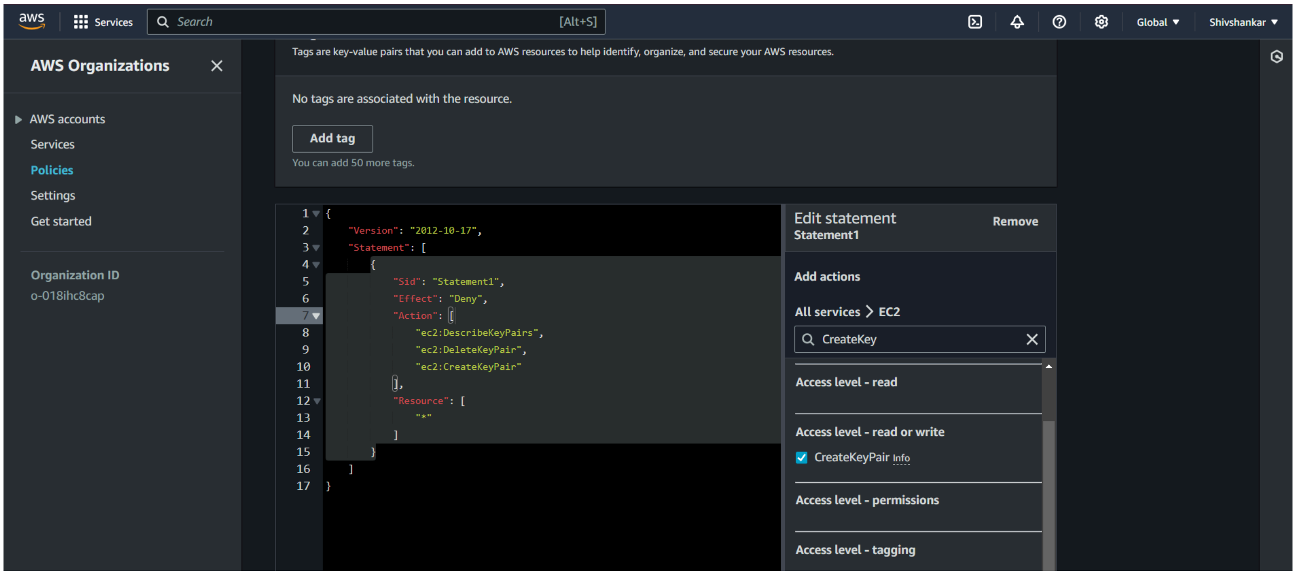
Policy type
Service control policy (customer managed)

Description
S3 Bucket policy

Content

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

Verification of attached SCP



Organization ID
o-018ihc8cap

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

No tags are associated with the resource.

You can add 50 more tags.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "ec2:DescribeKeyPairs",
                "ec2:DeleteKeyPair",
                "ec2:CreateKeyPair"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Statement1

Add actions

All services > EC2

CreateKey

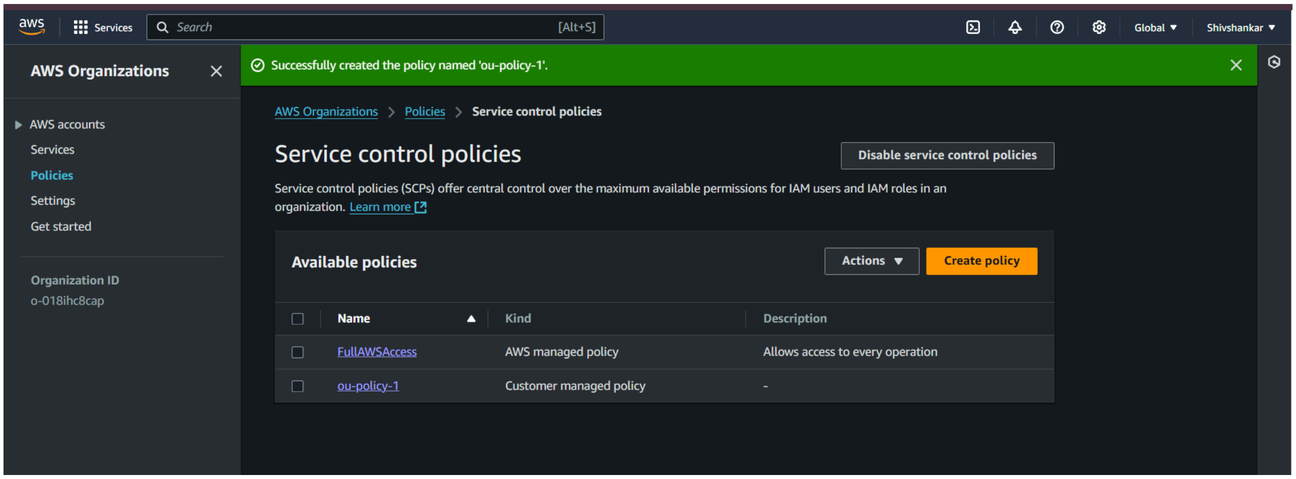
Access level - read

Access level - read or write

☑ CreateKeyPair Info

Access level - permissions

Access level - tagging



Organization ID
o-018ihc8cap

Successfully created the policy named 'ou-policy-1'.

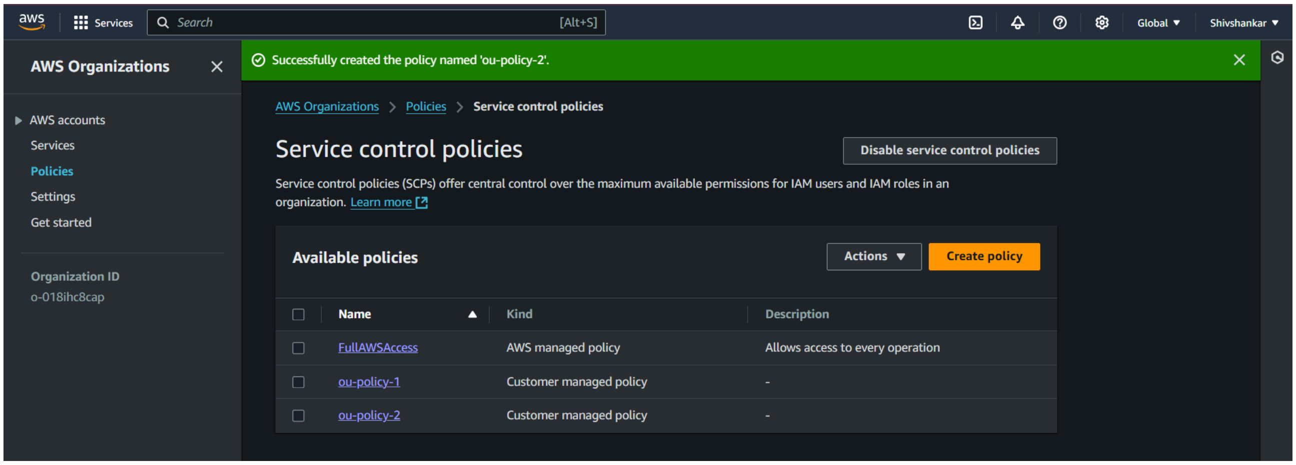
AWS Organizations > Policies > Service control policies

Service control policies

Service control policies (SCPs) offer central control over the maximum available permissions for IAM users and IAM roles in an organization. Learn more

Available policies

□	Name ▲	Kind	Description
□	FullAWSAccess	AWS managed policy	Allows access to every operation
□	ou-policy-1	Customer managed policy	-



Organization ID
o-018ihc8cap

Successfully created the policy named 'ou-policy-2'.

AWS Organizations > Policies > Service control policies

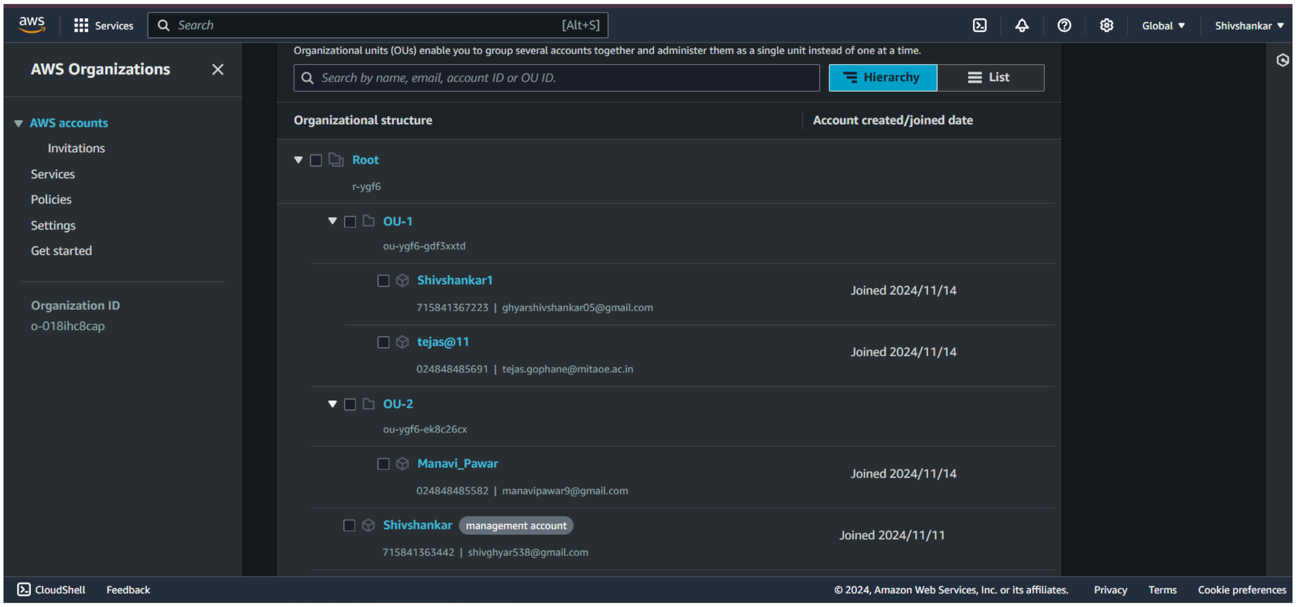
Service control policies

Service control policies (SCPs) offer central control over the maximum available permissions for IAM users and IAM roles in an organization. Learn more

Available policies

□	Name ▲	Kind	Description
□	FullAWSAccess	AWS managed policy	Allows access to every operation
□	ou-policy-1	Customer managed policy	-
□	ou-policy-2	Customer managed policy	-

➔ Create OUs and move members to them



Organization ID
o-018ihc8cap

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

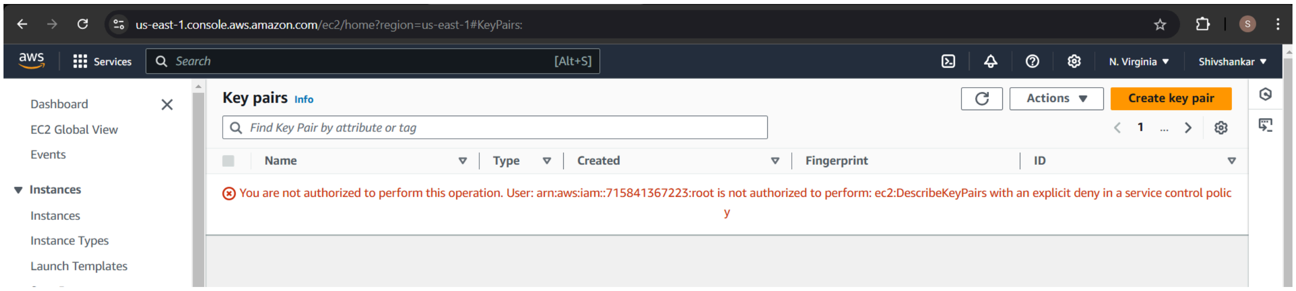
Search by name, email, account ID or OU ID.

Organizational structure	Account created/joined date
▼ □ Root r-ygf6	
▼ □ OU-1 ou-ygf6-gdf3xxtd	
□ Shivshankar1 715841367223 | ghyarshivshankar05@gmail.com	Joined 2024/11/14
□ tejas@11 024848485691 | tejas.gophane@mitaoe.ac.in	Joined 2024/11/14
▼ □ OU-2 ou-ygf6-ek8c26cx	
□ Manavi_Pawar 024848485582 | manavipawar9@gmail.com	Joined 2024/11/14
□ Shivshankar management account 715841363442 | shivghyar538@gmail.com	Joined 2024/11/11

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

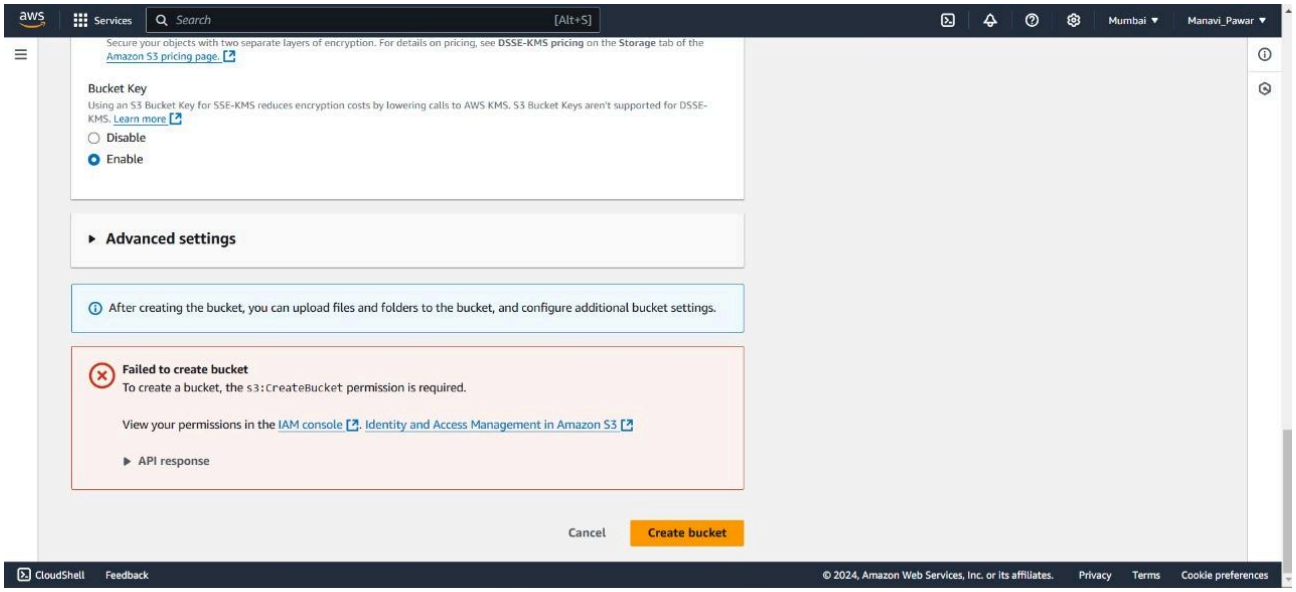
Verification of attached SCP

My 2nd Acct



You are not authorized to perform this operation. User: arn:aws:iam::715841367223:root is not authorized to perform: ec2:DescribeKeyPairs with an explicit deny in a service control polic
y

Manavi Pawar’s acct



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

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

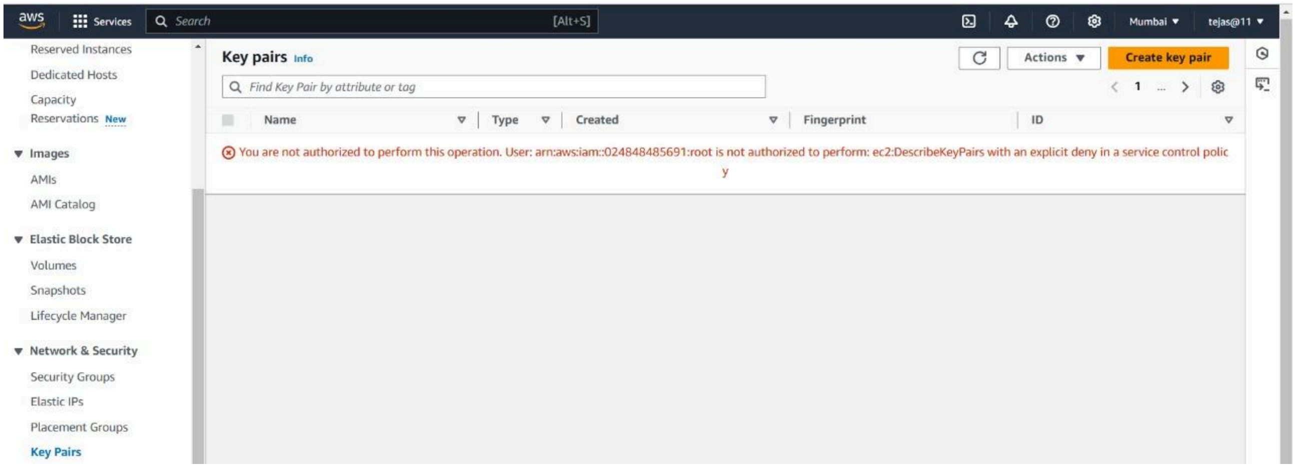
Failed to create bucket

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

Tejas acct

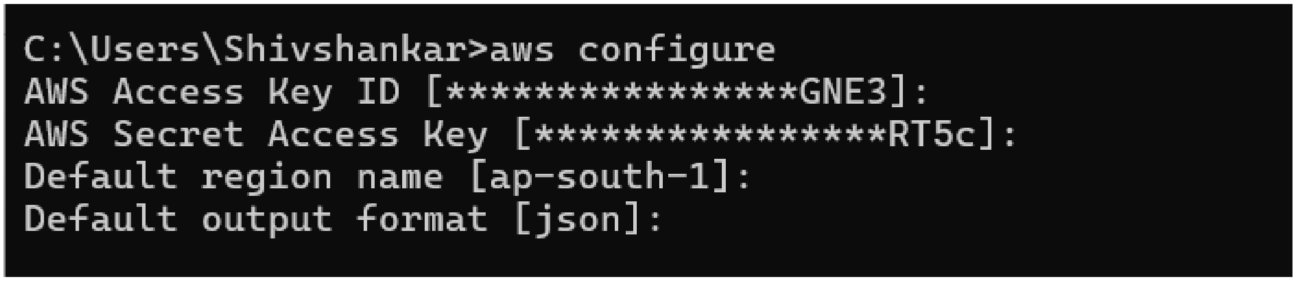


You are not authorized to perform this operation. User: arn:aws:iam::024848485691:root is not authorized to perform: ec2:DescribeKeyPairs with an explicit deny in a service control polic
y

Case 2: Using AWS CLI

Step 1: Configure AWS CLI

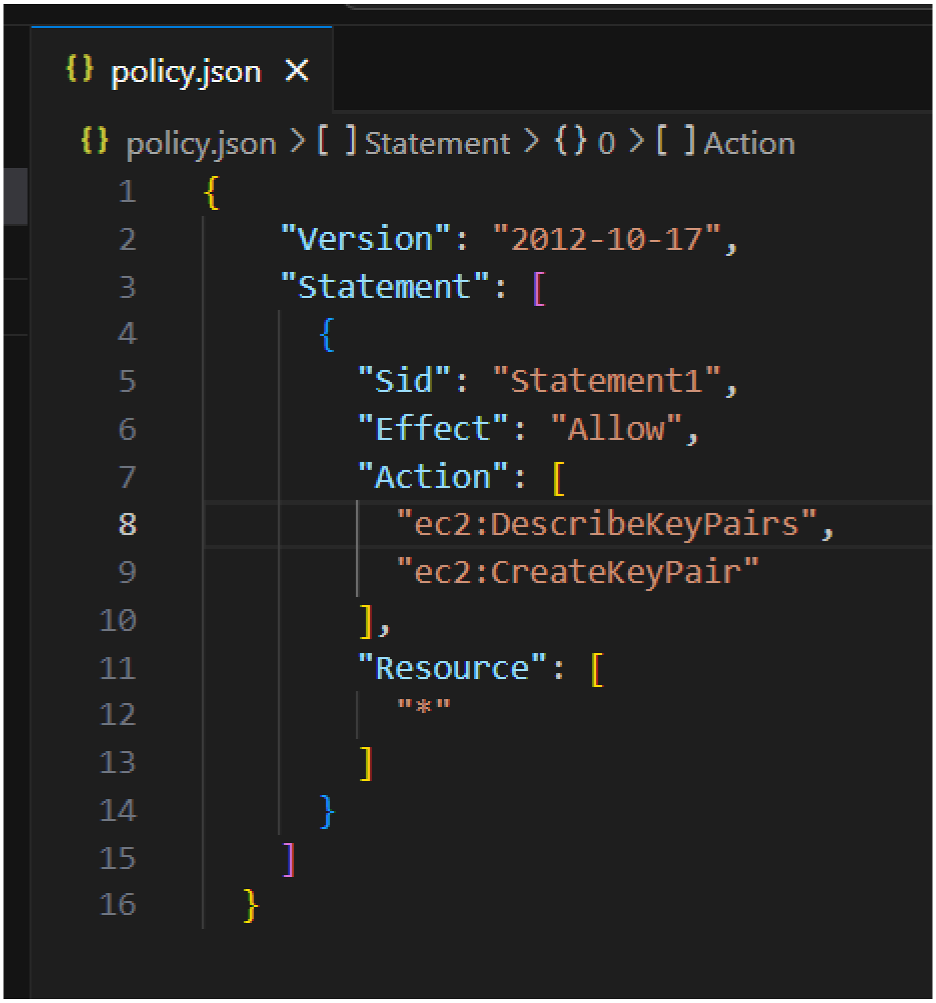
Command: aws configure



```
C:\Users\Shivshankar>aws configure
AWS Access Key ID [****************GNE3]:
AWS Secret Access Key [****************RT5c]:
Default region name [ap-south-1]:
Default output format [json]:
```

Step 2: Creation of Security Policy

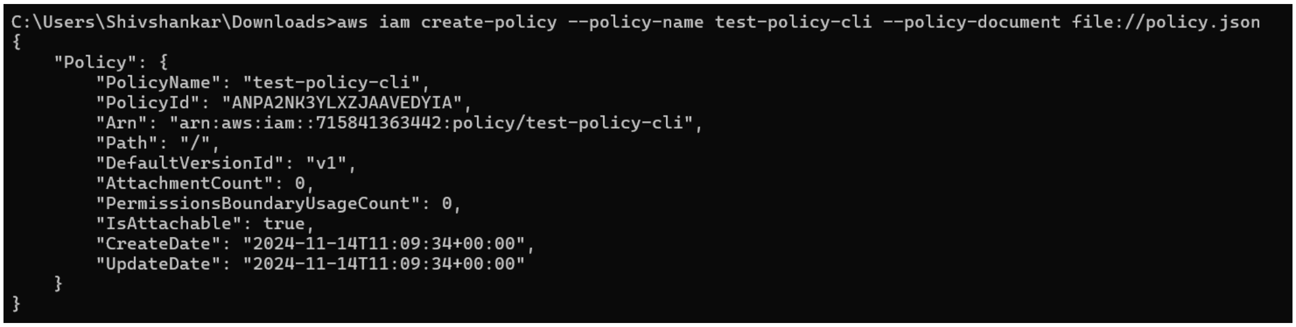
Create Policy JSON File



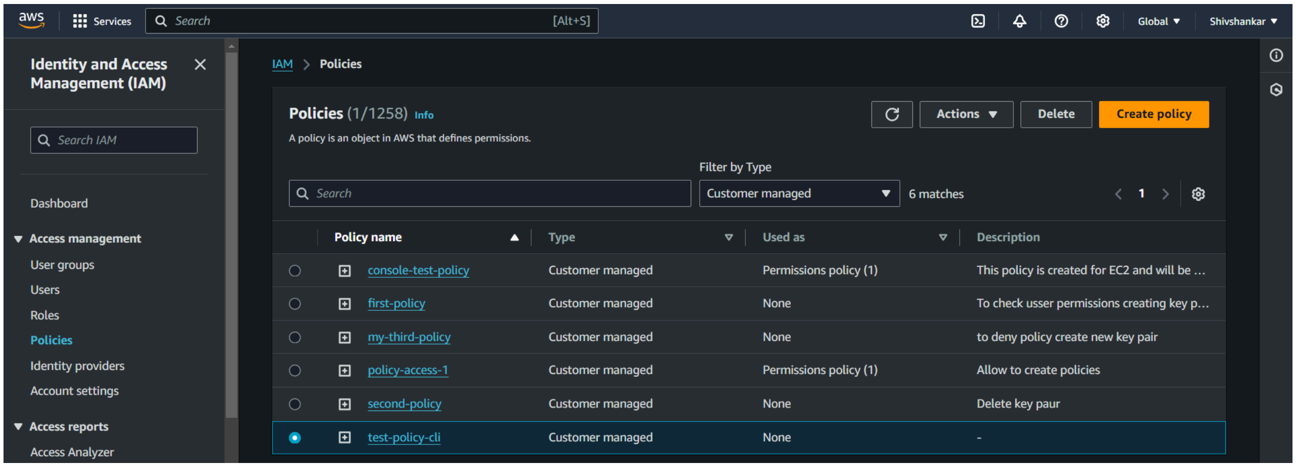
```json
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "Statement1",
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeKeyPairs",
          "ec2:CreateKeyPair"
        ],
        "Resource": [
          "*"
        ]
      }
    ]
  }
```

Command to Create Security Policy

aws iam create-policy--policy-name test-policy-cli--policy-document file://policy.json



```
C:\Users\Shivshankar\Downloads>aws iam create-policy --policy-name test-policy-cli --policy-document file://policy.json
{
    "Policy": {
        "PolicyName": "test-policy-cli",
        "PolicyId": "ANPA2NK3YLXZJAAVEDYIA",
        "Arn": "arn:aws:iam::715841363442:policy/test-policy-cli",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "2024-11-14T11:09:34+00:00",
        "UpdateDate": "2024-11-14T11:09:34+00:00"
    }
}
```



Policies (1/1258)

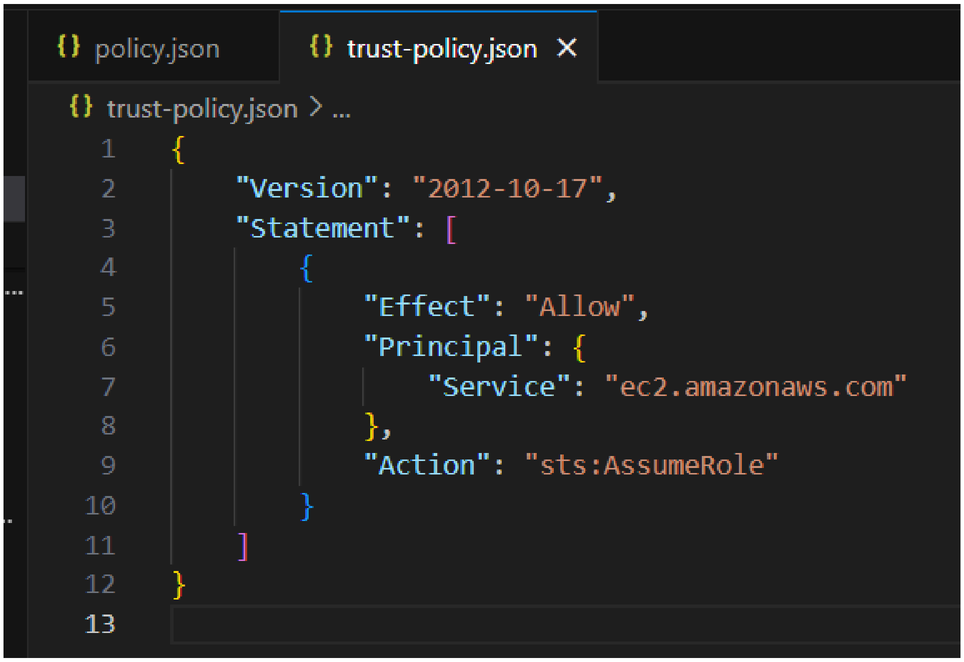
A policy is an object in AWS that defines permissions.

Filter by Type: Customer managed — 6 matches

Policy name	Type	Used as	Description
○ console-test-policy	Customer managed	Permissions policy (1)	This policy is created for EC2 and will be ...
○ first-policy	Customer managed	None	To check usser permissions creating key p...
○ my-third-policy	Customer managed	None	to deny policy create new key pair
○ policy-access-1	Customer managed	Permissions policy (1)	Allow to create policies
○ second-policy	Customer managed	None	Delete key paur
● test-policy-cli	Customer managed	None	-

Step 3: Creation of Role

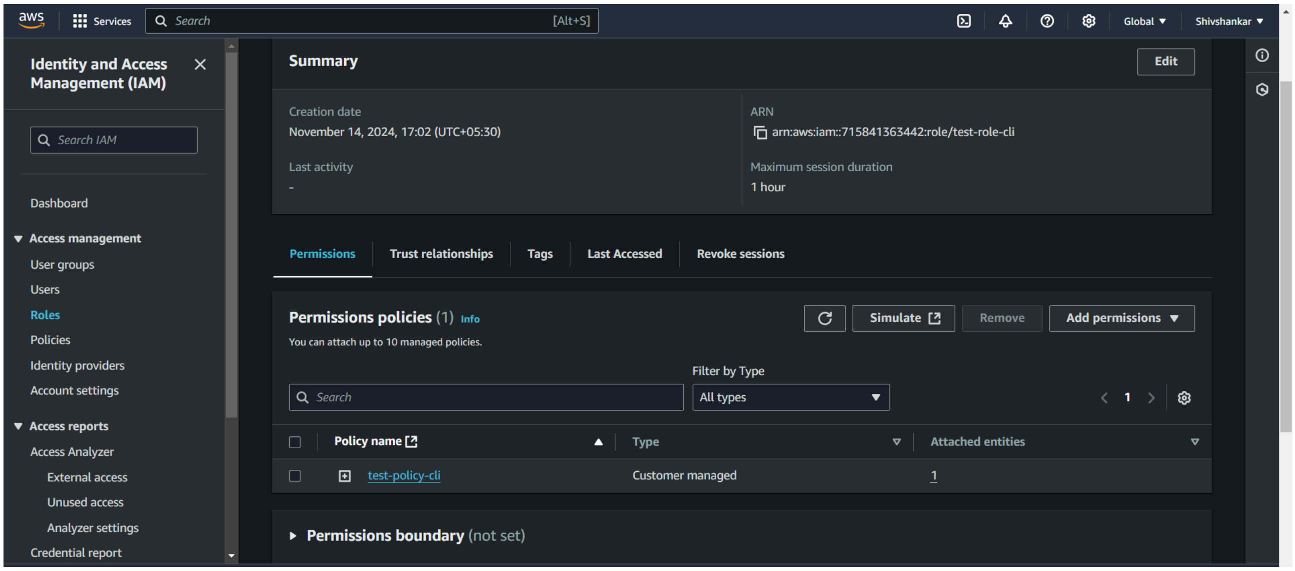
- Create Trust Policy JSON File



```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Command to Create Role :

```
aws iam create-role--role-name test-role-cli--assume-role-policy-document file://trust-policy.json
```



Summary

Creation date
November 14, 2024, 17:02 (UTC+05:30)

Last activity
-

ARN
arn:aws:iam::715841363442:role/test-role-cli

Maximum session duration
1 hour

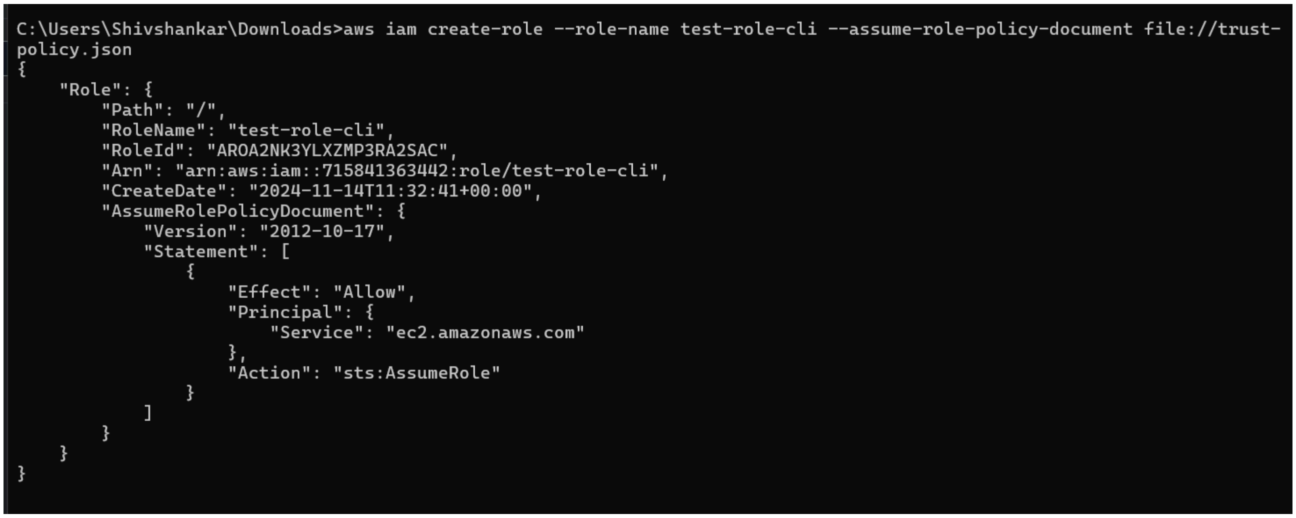
Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type: All types

□	Policy name	Type	Attached entities
□	test-policy-cli	Customer managed	1

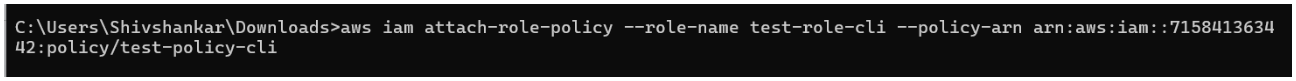
▸ **Permissions boundary** (not set)



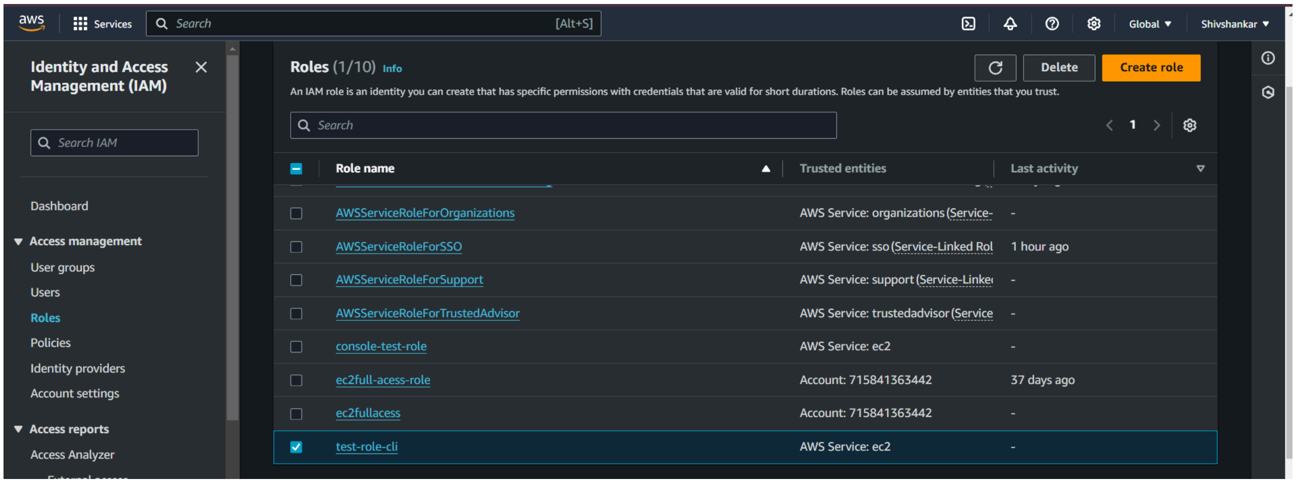
```
C:\Users\Shivshankar\Downloads>aws iam create-role --role-name test-role-cli --assume-role-policy-document file://trust-
policy.json
{
    "Role": {
        "Path": "/",
        "RoleName": "test-role-cli",
        "RoleId": "AROA2NK3YLXZMP3RA2SAC",
        "Arn": "arn:aws:iam::715841363442:role/test-role-cli",
        "CreateDate": "2024-11-14T11:32:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ec2.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Step 4: Attach policy to Role

Command: aws iam attach-role-policy --role-name test-role-cli --policy-arn arn:aws:iam::715841363442:policy/test-policy-cli



```
C:\Users\Shivshankar\Downloads>aws iam attach-role-policy --role-name test-role-cli --policy-arn arn:aws:iam::7158413634
42:policy/test-policy-cli
```



Roles (1/10) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

	Role name	Trusted entities	Last activity
□	AWSServiceRoleForOrganizations	AWS Service: organizations (Service-	-
□	AWSServiceRoleForSSO	AWS Service: sso (Service-Linked Rol	1 hour ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
□	console-test-role	AWS Service: ec2	-
□	ec2full-acess-role	Account: 715841363442	37 days ago
□	ec2fullacess	Account: 715841363442	-
☑	test-role-cli	AWS Service: ec2	-