Amazon IAM: IAM Policies-Task 2

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks To Be Performed:

1. Create policy number 1 which lets the users to:
    a. Access S3 completely
    b. Only create EC2 instances
    c. Full access to RDS

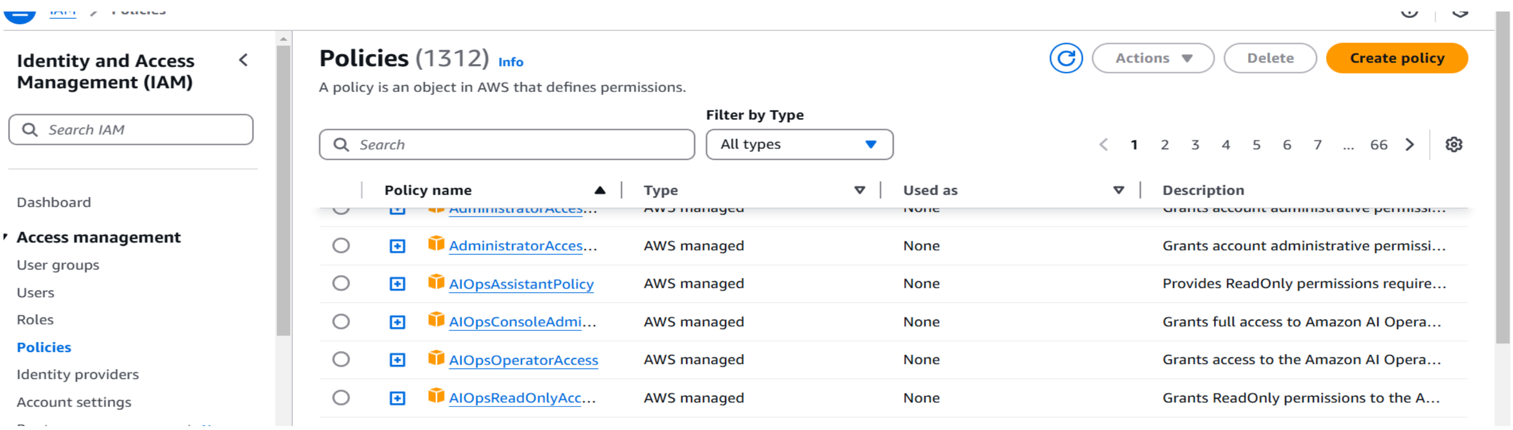
2. Create a policy number 2 which allows the users to:
    a. Access CloudWatch and billing completely
    b. Can only list EC2 and S3 resources

3. Attach policy number 1 to the Dev Team from task 1
4. Attach policy number 2 to Ops Team from task 1

Solution:

1. Create policy number 1 which lets the users to:
    a. Access S3 completely
    b. Only create EC2 instances
    c. Full access to RDS

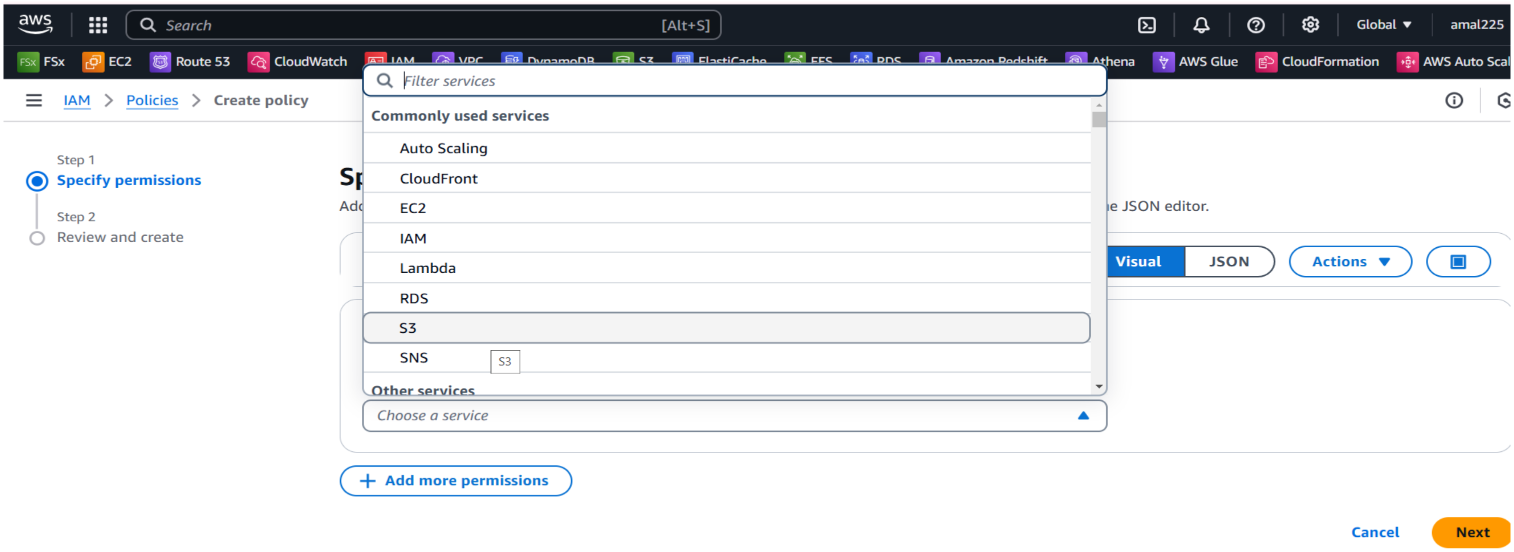
- Go to polices and click create policy and select the service click next select which you give permission and create policy
- . First create policy number 1

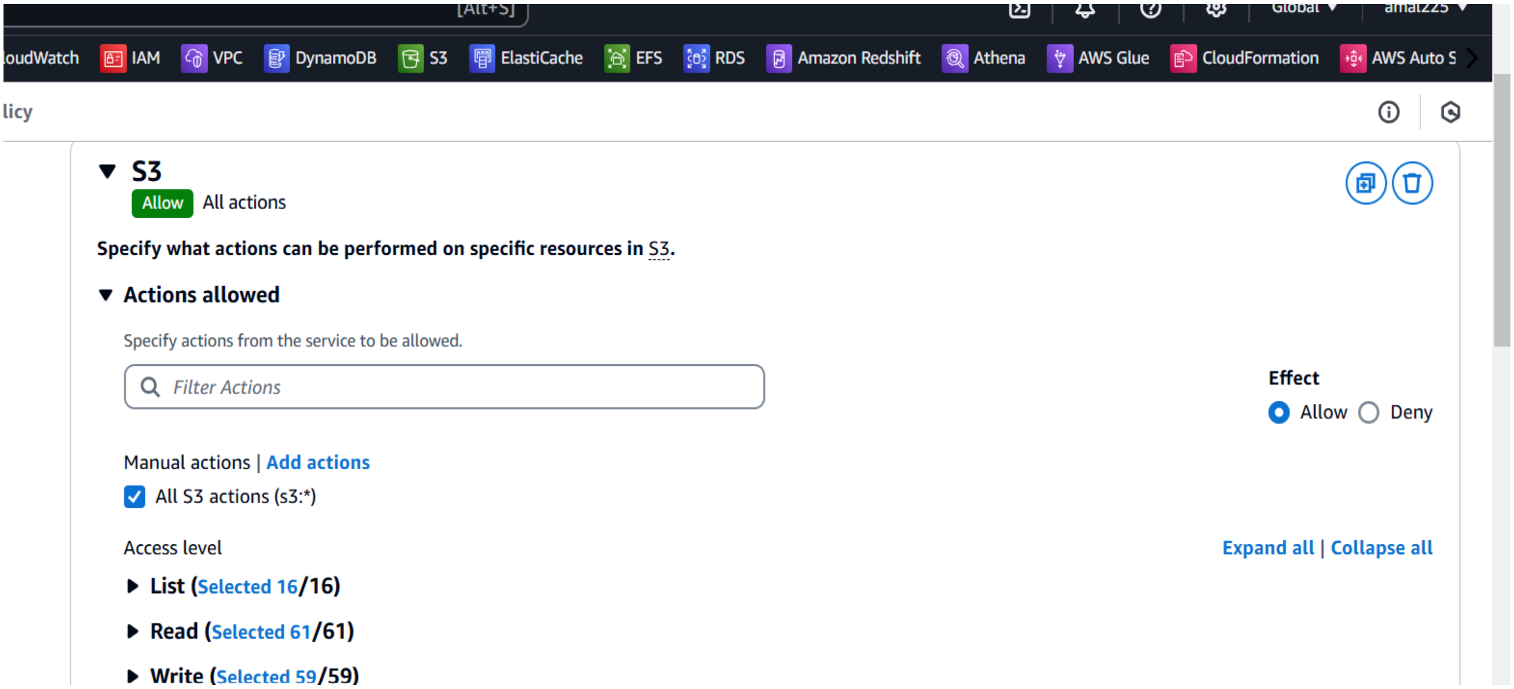


Policies (1312) Info

A policy is an object in AWS that defines permissions.

		Policy name	Type	Used as	Description
○	⊞	AdministratorAcces...	AWS managed	None	Grants account administrative permissi...
○	⊞	AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions require...
○	⊞	AIOpsConsoleAdmi...	AWS managed	None	Grants full access to Amazon AI Opera...
○	⊞	AIOpsOperatorAccess	AWS managed	None	Grants access to the Amazon AI Opera...
○	⊞	AIOpsReadOnlyAcc...	AWS managed	None	Grants ReadOnly permissions to the A...





udWatch IAM VPC DynamoDB S3 ElastiCache EFS RDS Amazon Redshift Athena AWS Glue CloudFormation AWS Auto S
licy

S3

Allow All actions

Specify what actions can be performed on specific resources in S3.

Actions allowed

Specify actions from the service to be allowed.

Effect

● Allow ○ Deny

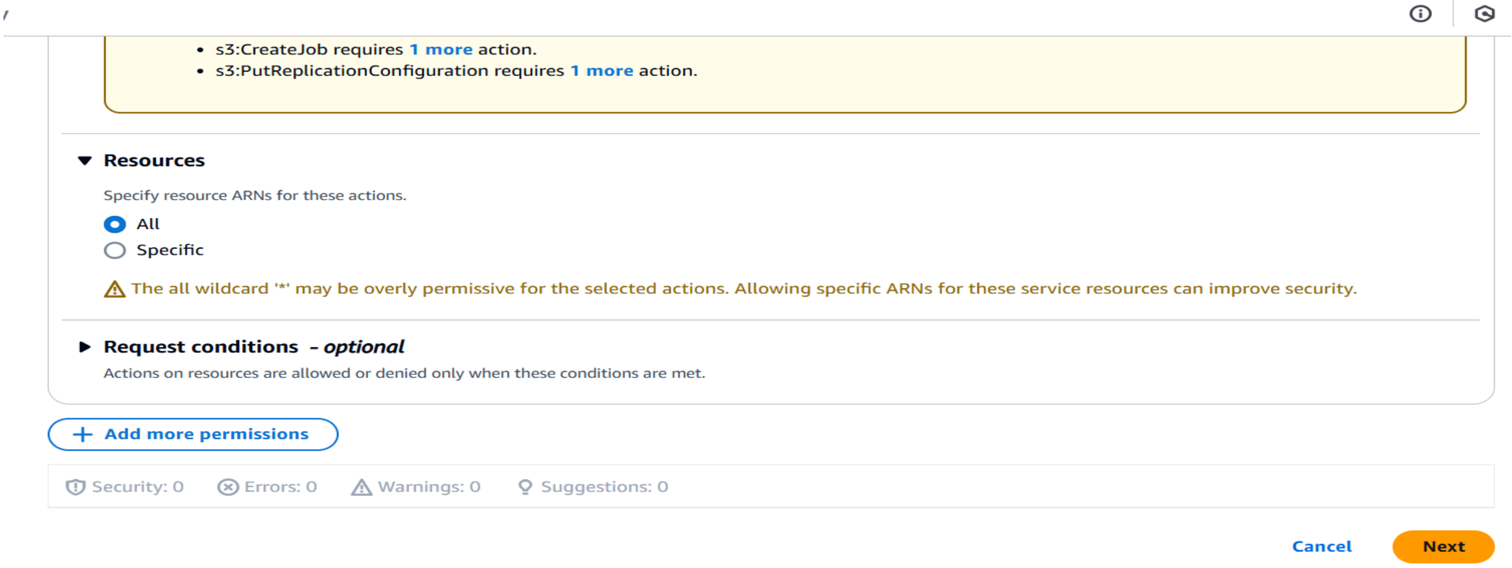
Manual actions | Add actions

☑ All S3 actions (s3:*)

Access level

Expand all | Collapse all

- List (Selected 16/16)
- Read (Selected 61/61)
- Write (Selected 59/59)



- s3:CreateJob requires **1 more** action.
- s3:PutReplicationConfiguration requires **1 more** action.

Resources

Specify resource ARNs for these actions.

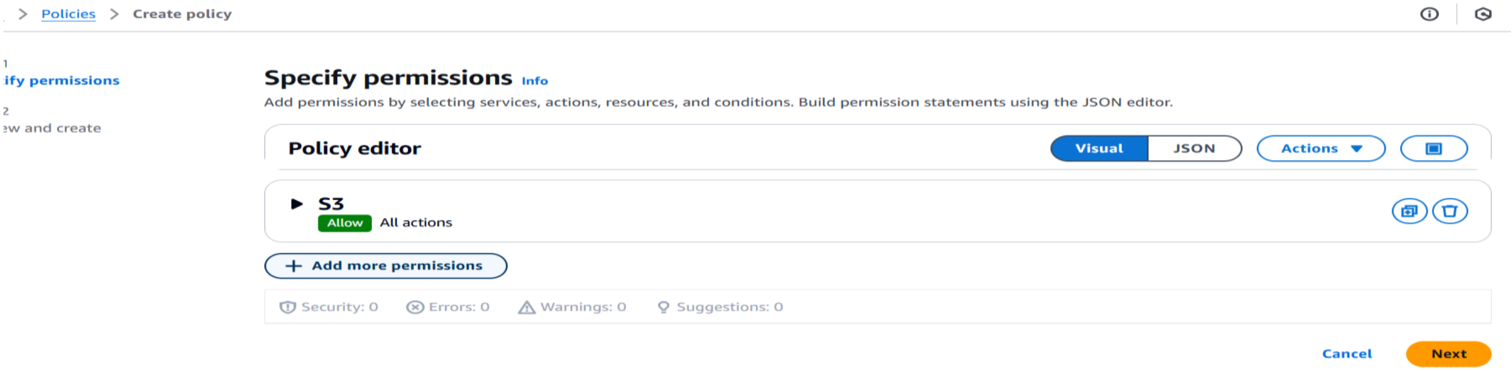
● All

○ Specific

⚠ The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

Request conditions *- optional*

Actions on resources are allowed or denied only when these conditions are met.



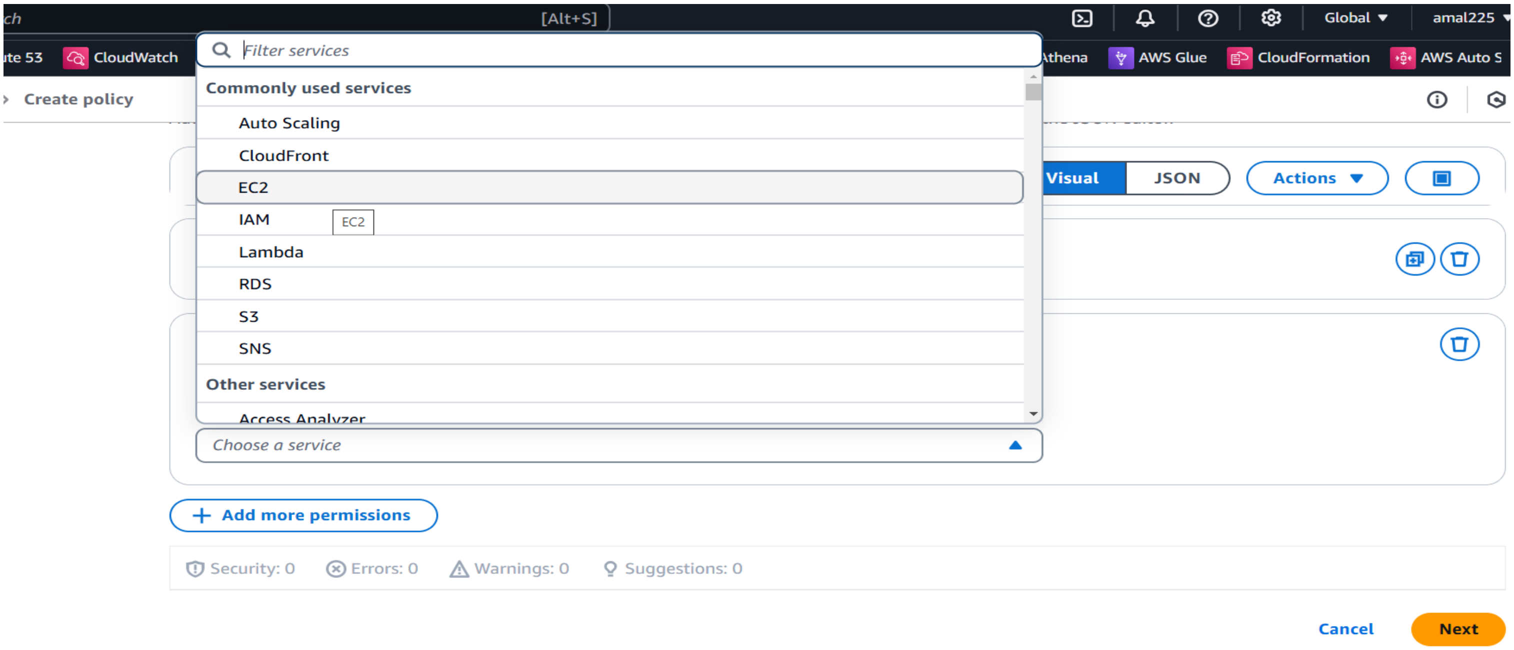
Specify permissions Info

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

Policy editor

S3

Allow All actions

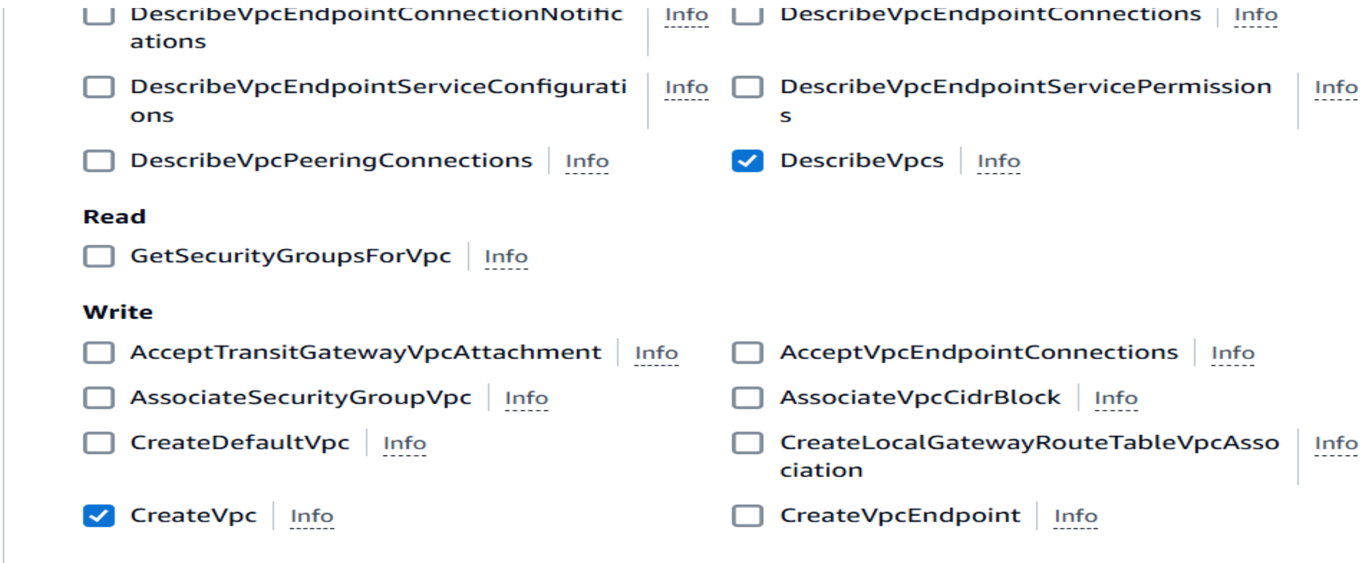


Commonly used services

- Auto Scaling
- CloudFront
- EC2
- IAM
- Lambda
- RDS
- S3
- SNS

Other services

- Access Analyzer



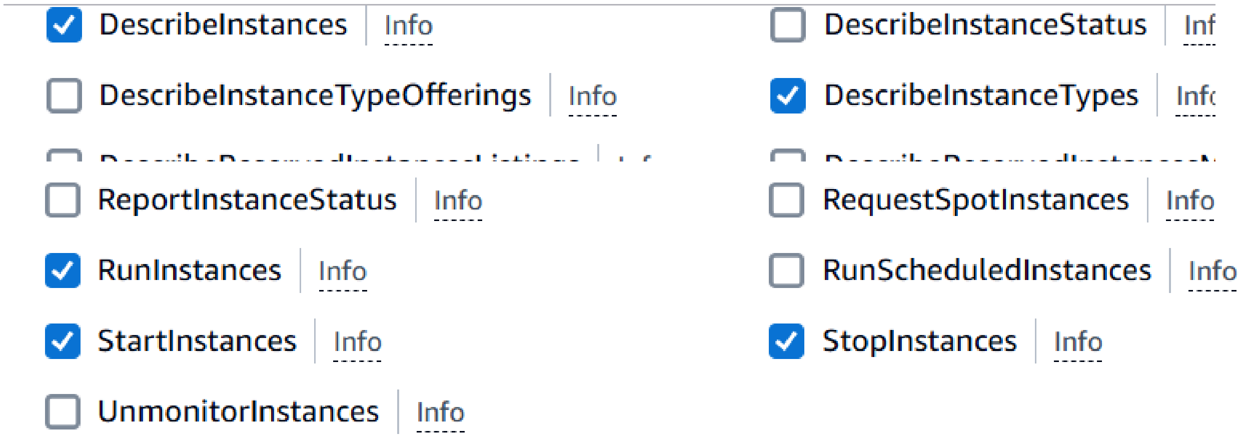
□ DescribeVpcEndpointConnectionNotifications | Info
□ DescribeVpcEndpointConnections | Info
□ DescribeVpcEndpointServiceConfigurations | Info
□ DescribeVpcEndpointServicePermissions | Info
□ DescribeVpcPeeringConnections | Info
☑ DescribeVpcs | Info

Read

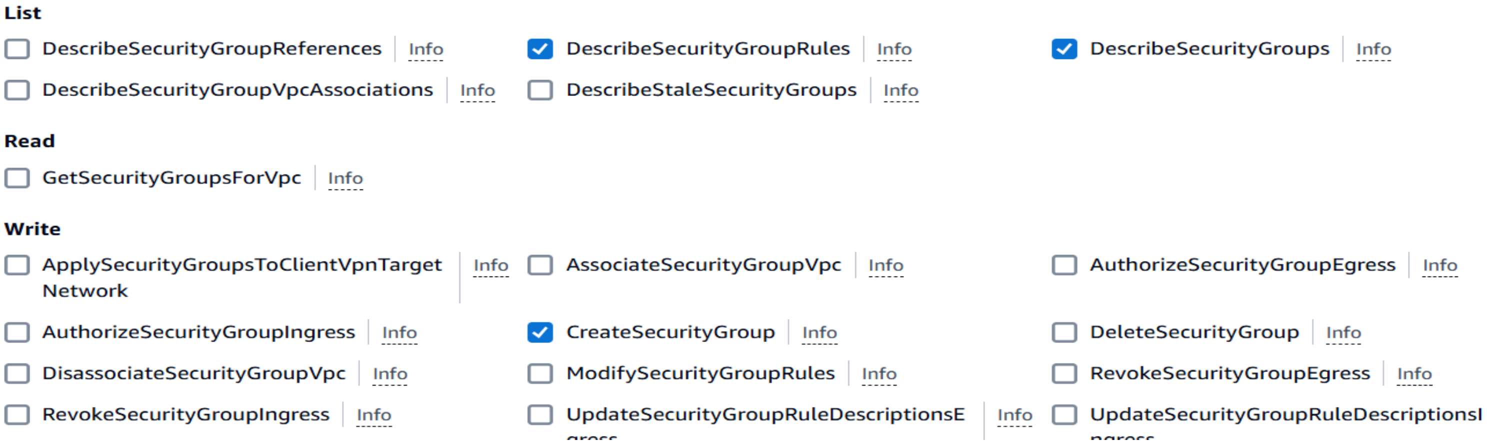
□ GetSecurityGroupsForVpc | Info

Write

□ AcceptTransitGatewayVpcAttachment | Info
□ AcceptVpcEndpointConnections | Info
□ AssociateSecurityGroupVpc | Info
□ AssociateVpcCidrBlock | Info
□ CreateDefaultVpc | Info
□ CreateLocalGatewayRouteTableVpcAssociation | Info
☑ CreateVpc | Info
□ CreateVpcEndpoint | Info



☑ DescribeInstances | Info
□ DescribeInstanceStatus | Inf
□ DescribeInstanceTypeOfferings | Info
☑ DescribeInstanceTypes | Inf
□ ReportInstanceStatus | Info
□ RequestSpotInstances | Info
☑ RunInstances | Info
□ RunScheduledInstances | Info
☑ StartInstances | Info
☑ StopInstances | Info
□ UnmonitorInstances | Info



List

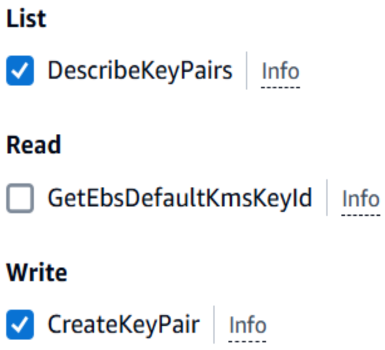
□ DescribeSecurityGroupReferences | Info
☑ DescribeSecurityGroupRules | Info
☑ DescribeSecurityGroups | Info
□ DescribeSecurityGroupVpcAssociations | Info
□ DescribeStaleSecurityGroups | Info

Read

□ GetSecurityGroupsForVpc | Info

Write

□ ApplySecurityGroupsToClientVpnTargetNetwork | Info
□ AssociateSecurityGroupVpc | Info
□ AuthorizeSecurityGroupEgress | Info
□ AuthorizeSecurityGroupIngress | Info
☑ CreateSecurityGroup | Info
□ DeleteSecurityGroup | Info
□ DisassociateSecurityGroupVpc | Info
□ ModifySecurityGroupRules | Info
□ RevokeSecurityGroupEgress | Info
□ RevokeSecurityGroupIngress | Info
□ UpdateSecurityGroupRuleDescriptionsEgress | Info
□ UpdateSecurityGroupRuleDescriptionsIngress



List

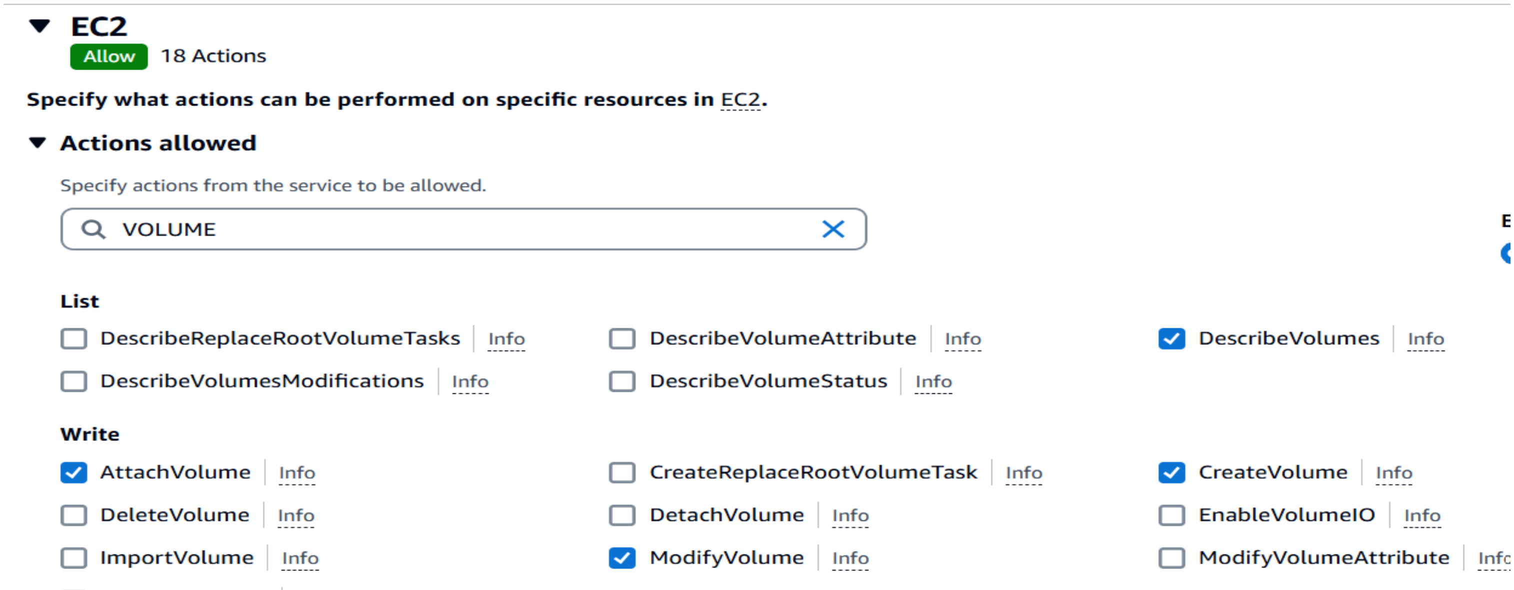
☑ DescribeKeyPairs | Info

Read

□ GetEbsDefaultKmsKeyId | Info

Write

☑ CreateKeyPair | Info



▼ **EC2**

Allow 18 Actions

Specify what actions can be performed on specific resources in EC2.

▼ **Actions allowed**

Specify actions from the service to be allowed.

VOLUME

List

□ DescribeReplaceRootVolumeTasks | Info □ DescribeVolumeAttribute | Info ☑ DescribeVolumes | Info

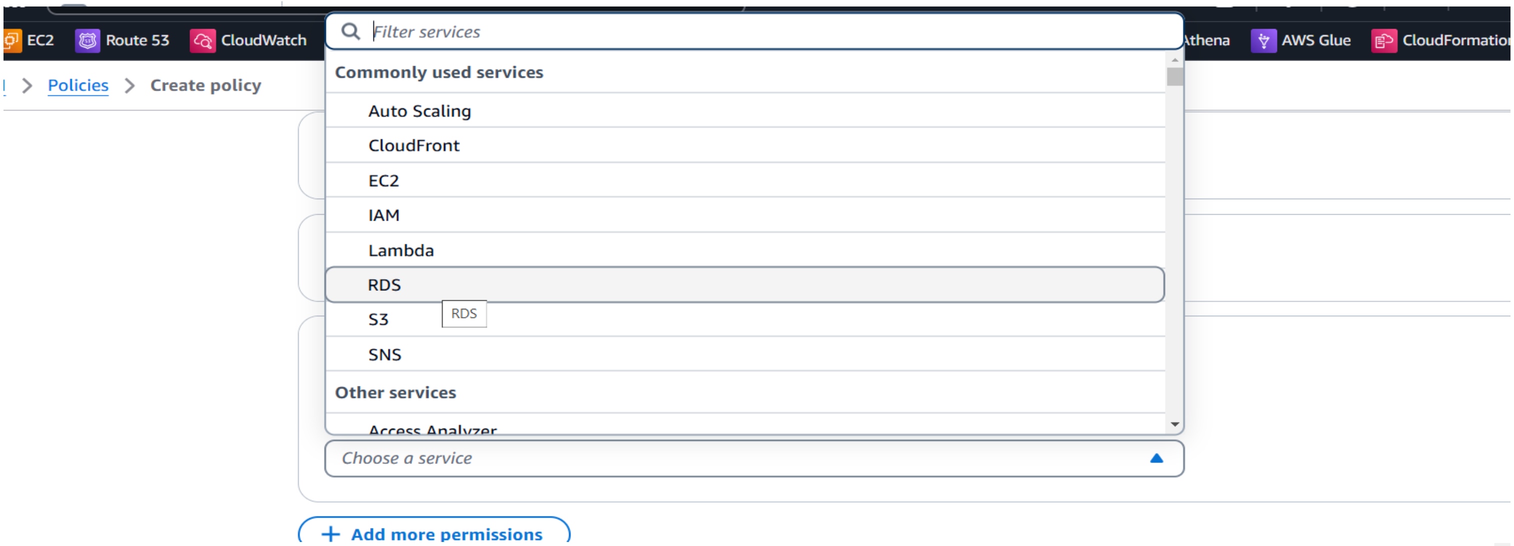
□ DescribeVolumesModifications | Info □ DescribeVolumeStatus | Info

Write

☑ AttachVolume | Info □ CreateReplaceRootVolumeTask | Info ☑ CreateVolume | Info

□ DeleteVolume | Info □ DetachVolume | Info □ EnableVolumeIO | Info

□ ImportVolume | Info ☑ ModifyVolume | Info □ ModifyVolumeAttribute | Info



Filter services

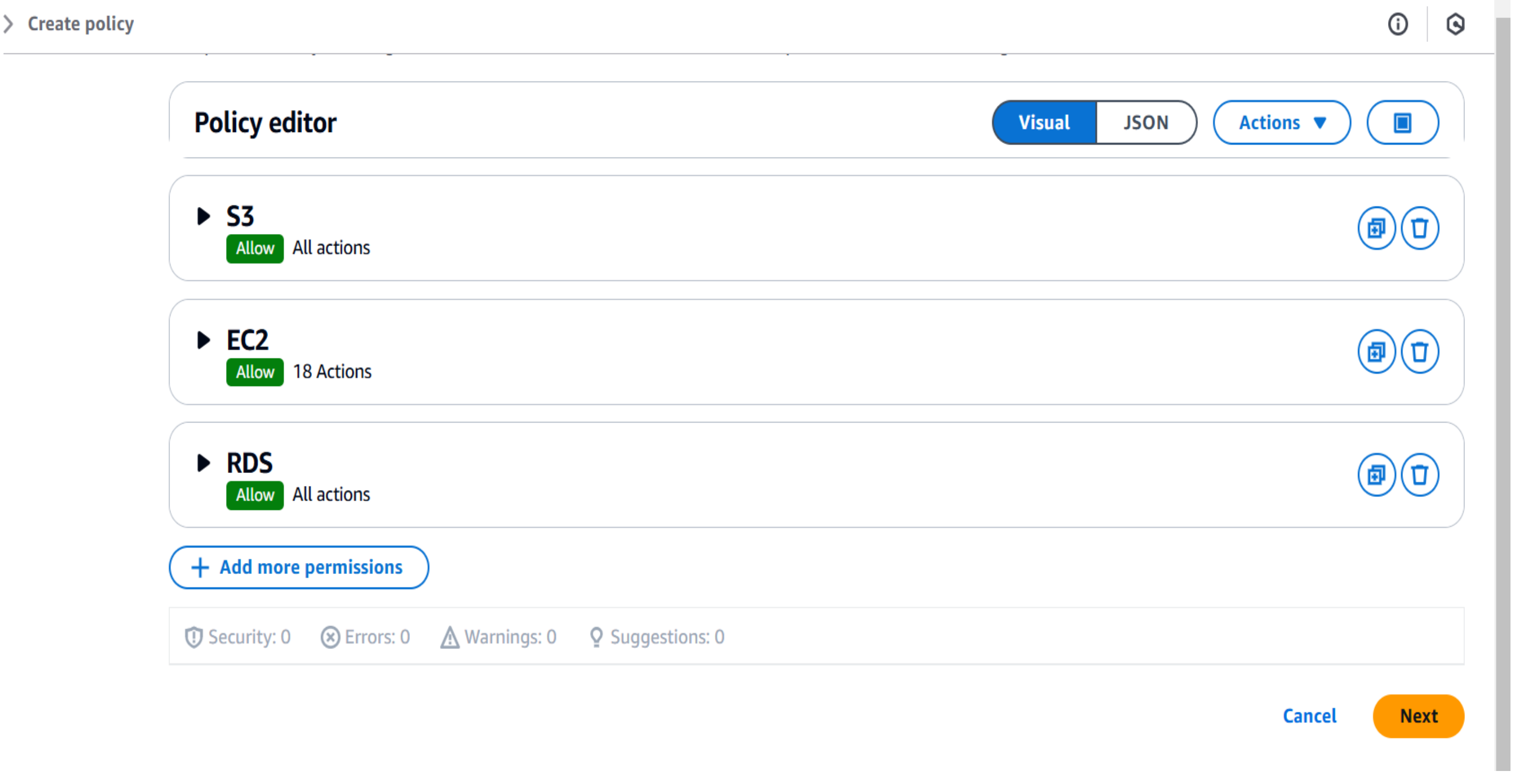
Commonly used services

- Auto Scaling
- CloudFront
- EC2
- IAM
- Lambda
- RDS
- S3
- SNS

Other services

- Access Analyzer

Choose a service



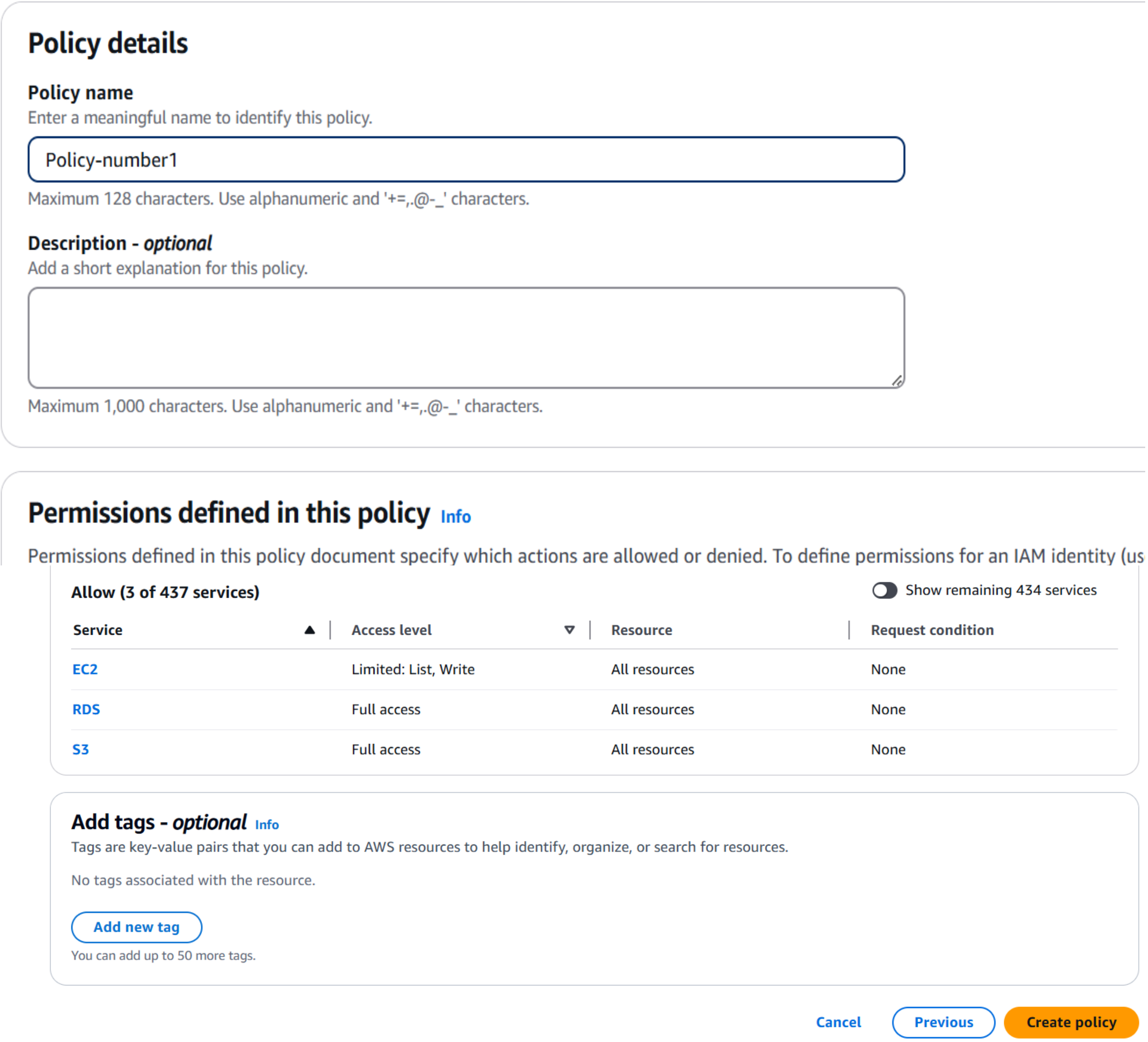
Policy editor

▶ **S3**
Allow All actions

▶ **EC2**
Allow 18 Actions

▶ **RDS**
Allow All actions

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0



Policy details

Policy name

Enter a meaningful name to identify this policy.

Policy-number1

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*

Add a short explanation for this policy.

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 (us

Allow (3 of 437 services)

Show remaining 434 services

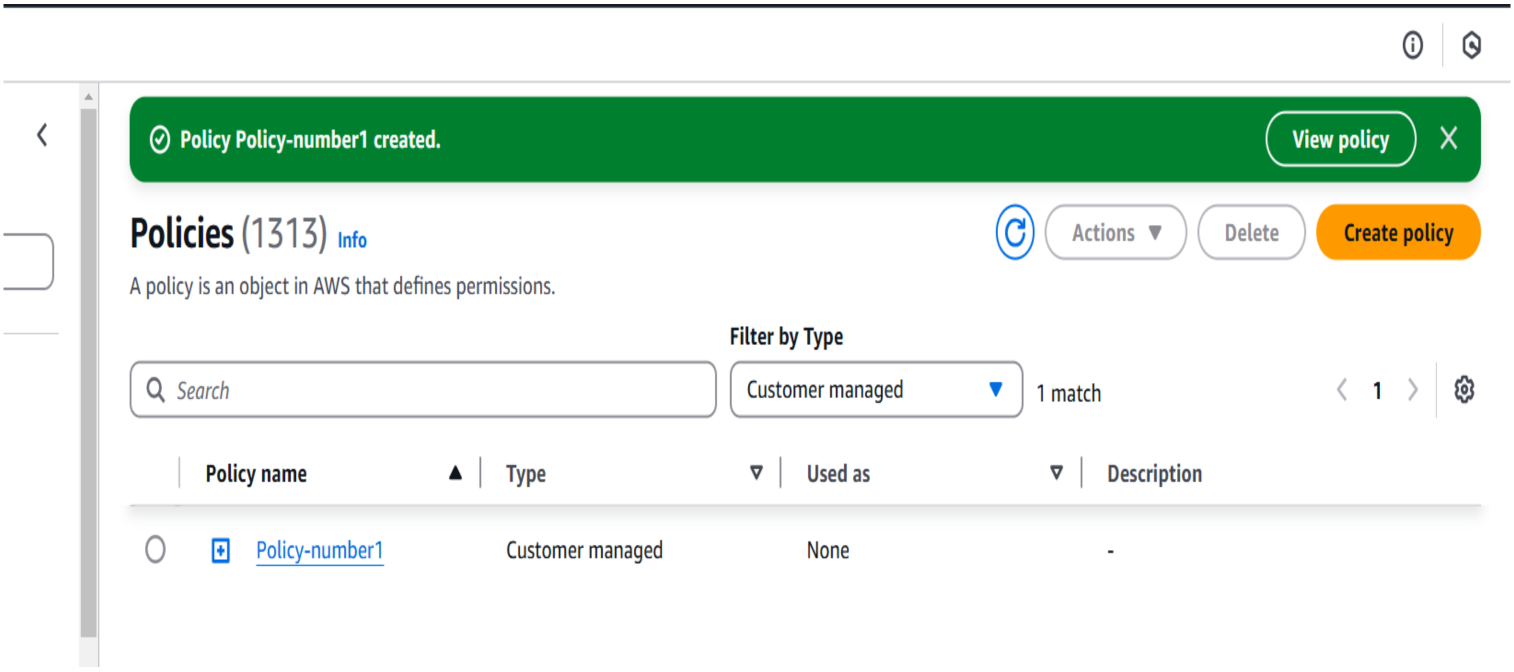
Service	Access level	Resource	Request condition
EC2	Limited: List, Write	All resources	None
RDS	Full access	All resources	None
S3	Full access	All resources	None

Add tags - *optional* Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.



Policy Policy-number1 created.

Policies (1313) Info

A policy is an object in AWS that defines permissions.

Filter by Type: Customer managed

Search

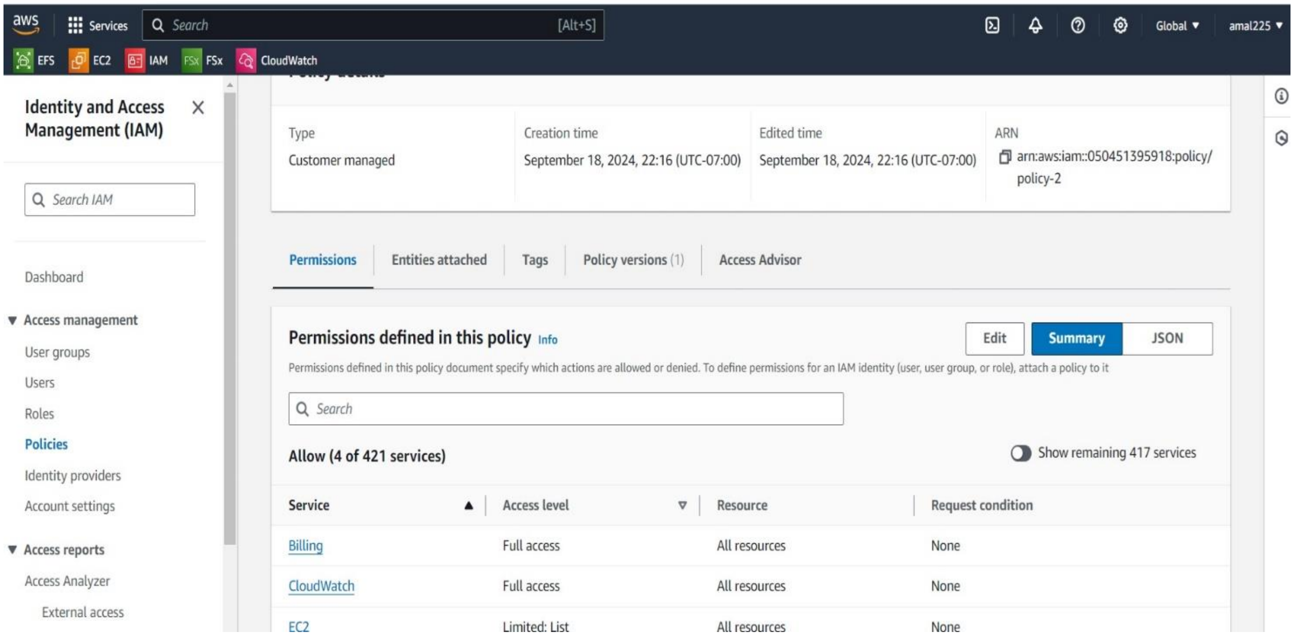
1 match

Policy name	Type	Used as	Description
○ Policy-number1	Customer managed	None	-

2 Create a policy number 2 which allows the users to:

a. Access CloudWatch and billing completely

b. Can only list EC2 and S3 resources

- Create same as it is, follow same process above policy-number1 .here I am created policy-number2
- .
- 

Type: Customer managed

Creation time: September 18, 2024, 22:16 (UTC-07:00)

Edited time: September 18, 2024, 22:16 (UTC-07:00)

ARN: arn:aws:iam::050451395918:policy/policy-2

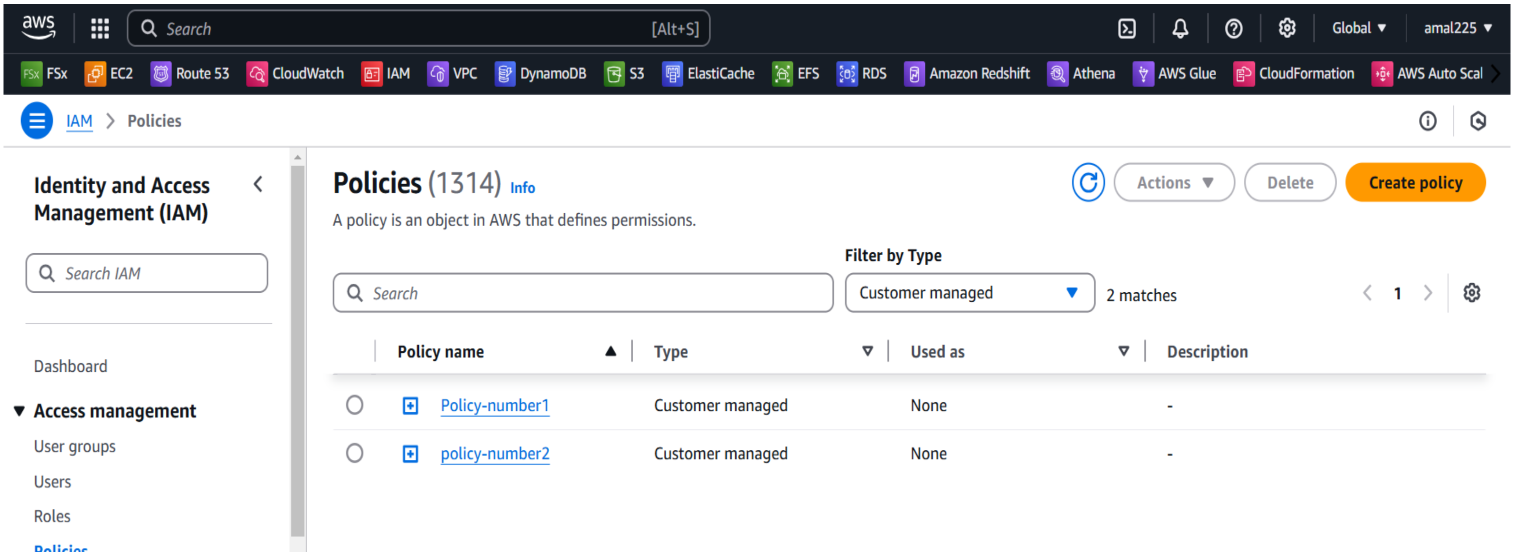
Permissions defined in this policy

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

Allow (4 of 421 services)

Show remaining 417 services

Service	Access level	Resource	Request condition
Billing	Full access	All resources	None
CloudWatch	Full access	All resources	None
EC2	Limited: List	All resources	None



Policies (1314)

A policy is an object in AWS that defines permissions.

Filter by Type: Customer managed

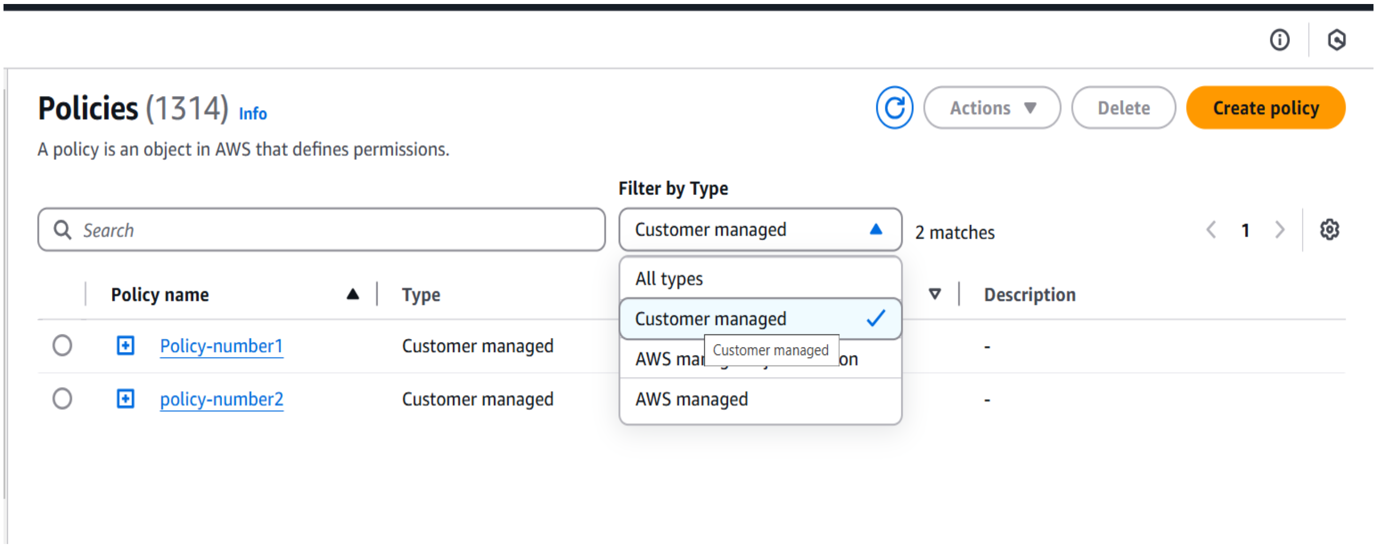
2 matches

	Policy name	Type	Used as	Description
○	Policy-number1	Customer managed	None	-
○	policy-number2	Customer managed	None	-

1. Attach policy number 1 to the Dev Team from task1

- In policy , go to custom policy select your policy and click action , click attach, select group name, Dev-Team and attach policy.

-

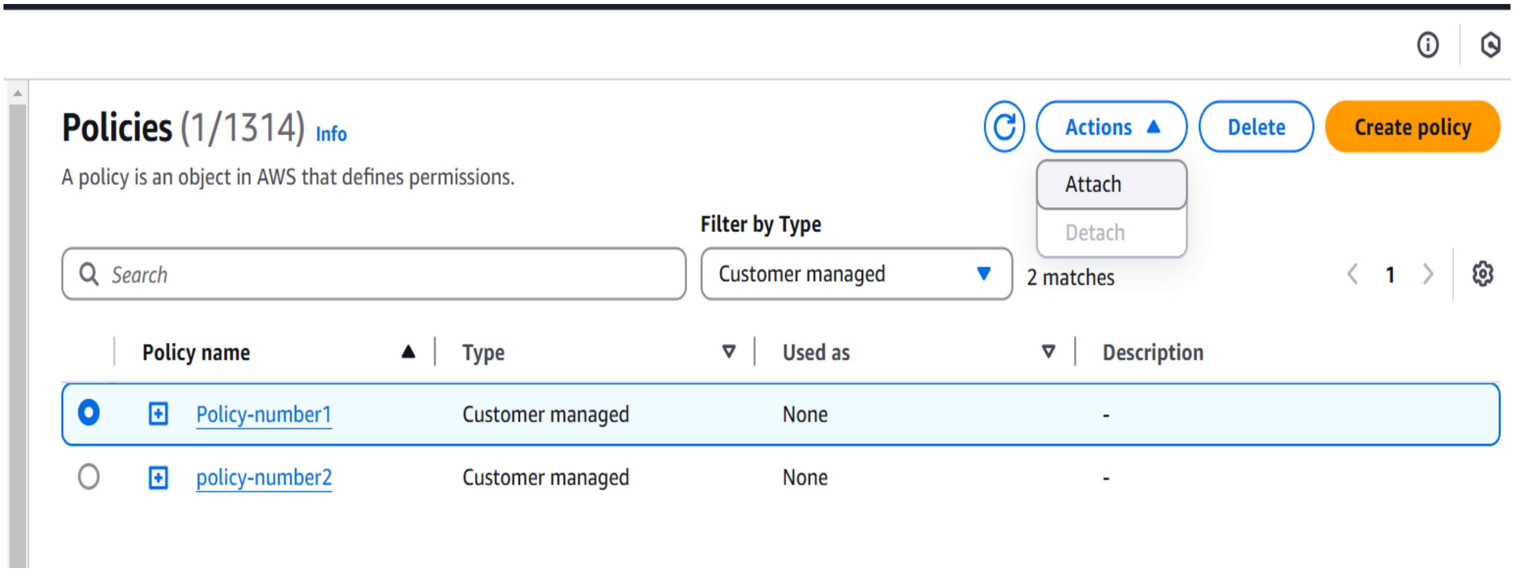


Policies (1314) Info

A policy is an object in AWS that defines permissions.

Filter by Type: Customer managed ▲ — 2 matches

	Policy name ▲	Type	Description
○	Policy-number1	Customer managed	-
○	policy-number2	Customer managed	-

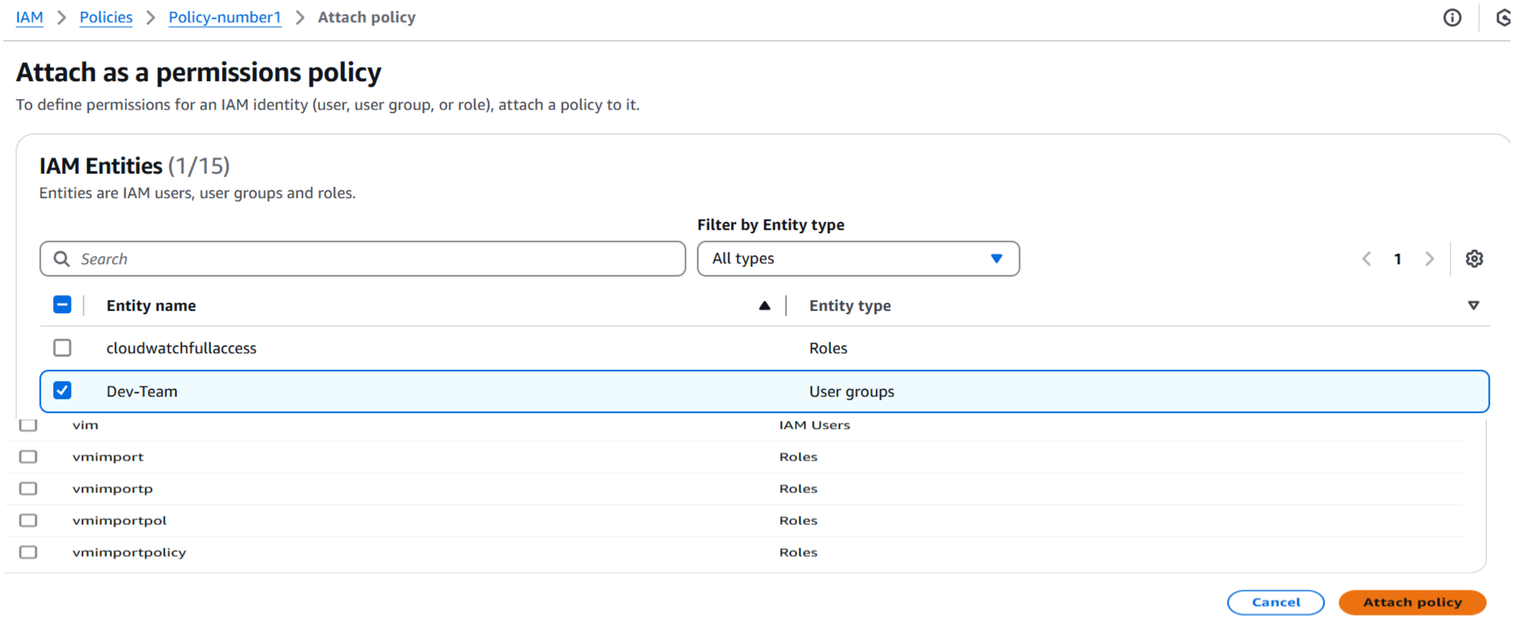


Policies (1/1314) Info

A policy is an object in AWS that defines permissions.

Filter by Type: Customer managed ▼ — 2 matches

	Policy name ▲	Type	Used as	Description
●	Policy-number1	Customer managed	None	-
○	policy-number2	Customer managed	None	-



Attach as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

IAM Entities (1/15)

Entities are IAM users, user groups and roles.

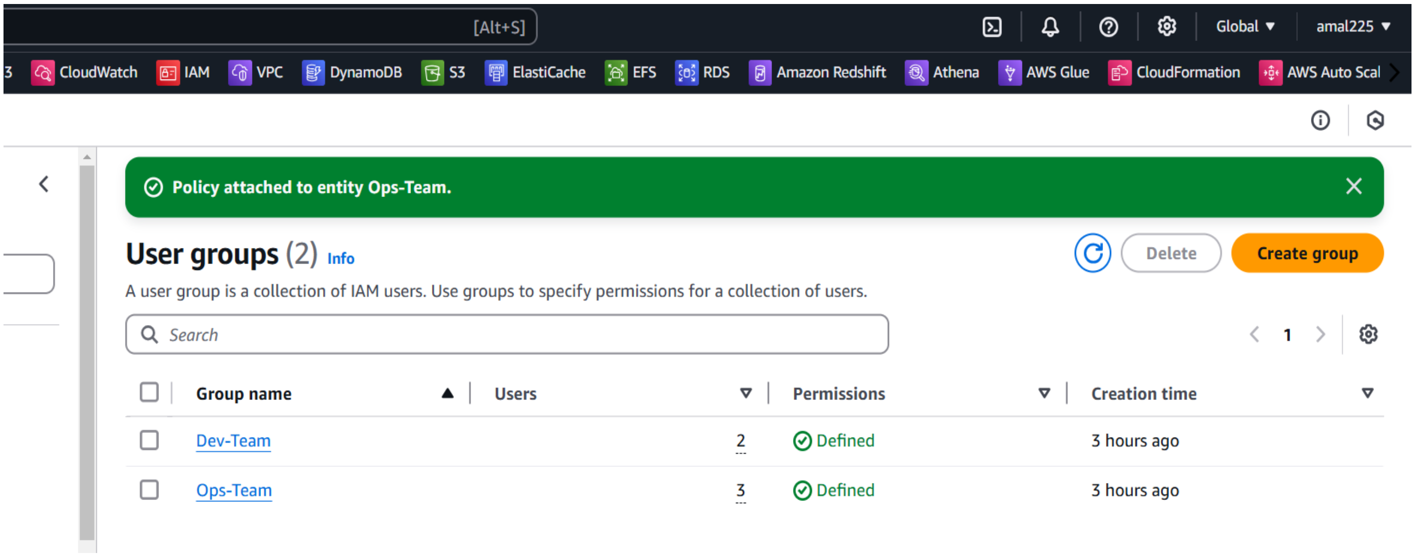
Filter by Entity type: All types ▼

☐	Entity name ▲	Entity type
☐	cloudwatchfullaccess	Roles
☑	Dev-Team	User groups
☐	vim	IAM Users
☐	vmimport	Roles
☐	vmimportp	Roles
☐	vmimportpol	Roles
☐	vmimportpolicy	Roles

- Attach policy number 2 to Ops Team from task 1

-

- Attach policy number 2 to ops-Team same at it follow above process.



Policy attached to entity Ops-Team.

User groups (2) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time
Dev-Team	2	Defined	3 hours ago
Ops-Team	3	Defined	3 hours ago