

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports


- Access analyzer
 - Archive rules
 - Analyzers
 - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)


[IAM](#) > [User groups](#) > [Ops-Team](#) > Add permissions

Attach permission policies to Ops-Team


▶ Current permissions policies (0)













Other permission policies (Selected 1/825)
You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.



Create policy 

Filter policies by property or policy name and press enter.

< 1 2 3 4 5 6 7 ... 42 > 

	Policy name 	Type	Description
<input type="checkbox"/>	 AWSCodePipelineServiceRole-ca-central-1-pipeline	Customer managed	Policy used in trust relationship with CodePipeline
<input type="checkbox"/>	 CodeBuildBasePolicy-codebuild_CodeDeployWebsite-ca-central-1	Customer managed	Policy used in trust relationship with CodeBuild
<input type="checkbox"/>	 CustomS3IAMPolicy	Customer managed	read access to first bucket full access to second bucket
<input checked="" type="checkbox"/>	 ploicynumber2	Customer managed	ploicynumber2
<input type="checkbox"/>	 policynumber1	Customer managed	
<input type="checkbox"/>	  AWSDirectConnectReadOnlyAccess	AWS managed	Provides read only access to AWS Direct Connect via the AWS Management Console.
<input type="checkbox"/>	  AmazonGlacierReadOnlyAccess	AWS managed	Provides read only access to Amazon Glacier via the AWS Management Console.
<input type="checkbox"/>	  AWSMarketplaceFullAccess	AWS managed	Provides the ability to subscribe and unsubscribe to AWS Marketplace software, allows us...

Create policy

1

2

3

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

Import managed policy

[Expand all](#) | [Collapse all](#)

▼ S3 (All actions)

Clone | Remove

▶ Service

S3

▶ Actions

Manual actions

*

▶ Resources

All resources

▶ Request conditions

[Specify request conditions \(optional\)](#)

[+ Add additional permissions](#)

Create policy

1

2

3

Review policy

Name*

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

Description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (3 of 369 services) Show remaining 366			
EC2	Limited: Write	All resources	None
RDS	Full access	All resources	None
S3	Full access	All resources	None

Tags

Key	Value
-----	-------

No tags associated with the resource.

* Required

Cancel

Previous

Create policy

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users
 - Roles
- Policies
- Identity providers
- Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
 - Credential report
 - Organization activity
 - Service control policies (SCPs)

Policies > ploicynumber2

Summary

Delete policy

Policy ARN arn:aws:iam::278048362884:policy/ploicynumber2

Description ploicynumber2

- Permissions
- Policy usage
- Tags
- Policy versions
- Access Advisor

- Policy summary
- { } JSON
- Edit policy

Filter

Service	Access level	Resource	Request condition
Allow (2 of 369 services) Show remaining 367			
Billing	Full access	All resources	None
CloudWatch	Full access	All resources	None

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > User groups > Dev-Team > Add permissions

Attach permission policies to Dev-Team

Current permissions policies (0)

Other permission policies (Selected 1/825)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Filter policies by property or policy name and press enter.

1 2 3 4 5 6 7 ... 42

Create policy

	Policy name	Type	Description
<input type="checkbox"/>	AWSCodePipelineServiceRole-ca-central-1-pipeline	Customer managed	Policy used in trust relation
<input type="checkbox"/>	CodeBuildBasePolicy-codebuild_CodeDeployWebsite-ca-central-1	Customer managed	Policy used in trust relation
<input type="checkbox"/>	CustomS3IAMPolicy	Customer managed	read access to first bucket
<input type="checkbox"/>	ploicynumber2	Customer managed	ploicynumber2
<input checked="" type="checkbox"/>	policynumber1	Customer managed	
<input type="checkbox"/>	AWSDirectConnectReadOnlyAccess	AWS managed	Provides read only access
<input type="checkbox"/>	AmazonGlacierReadOnlyAccess	AWS managed	Provides read only access