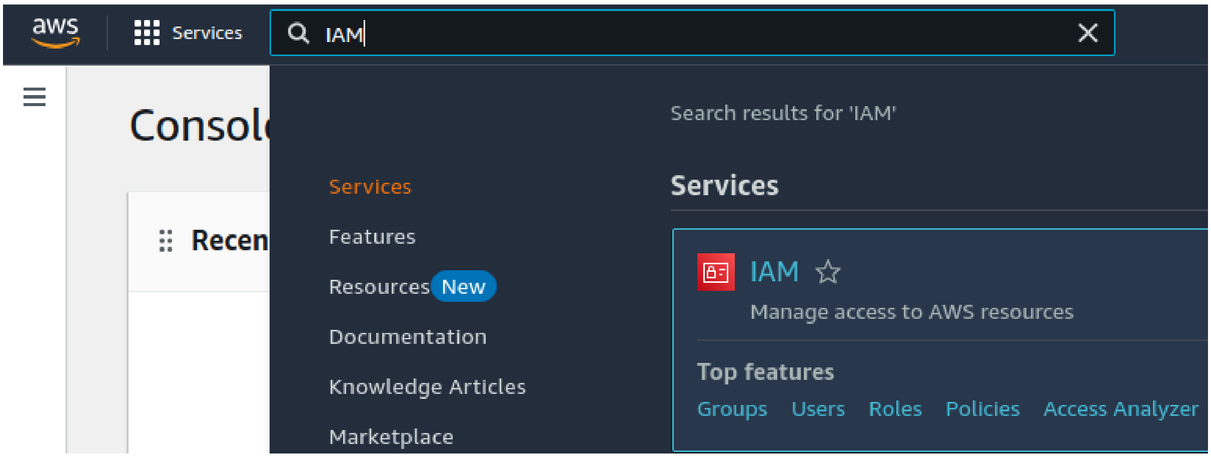
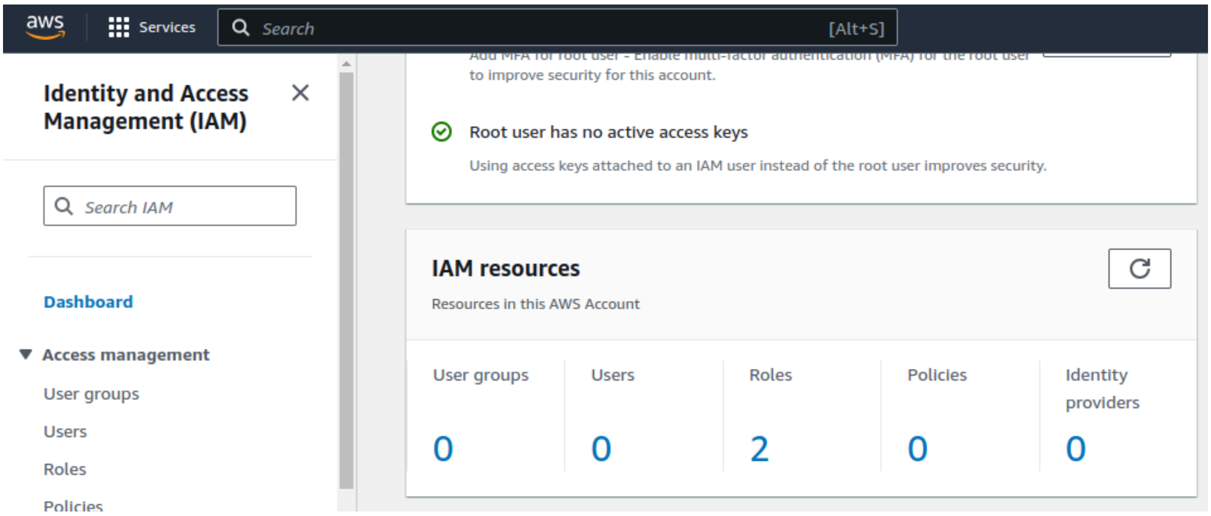
IAM Tasks

Create User and give permissions



Go to the IAM Dashboard in the AWS Management Console



Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys

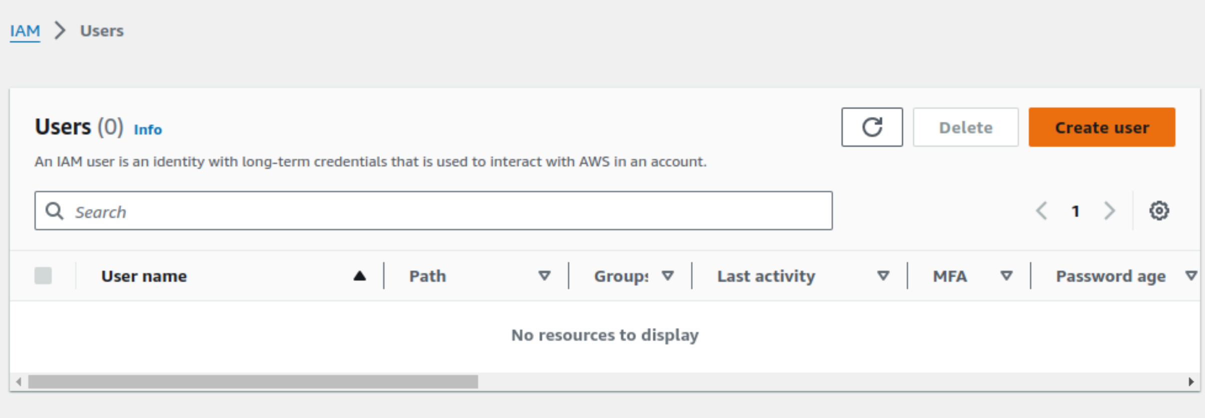
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0

Click the Add user button

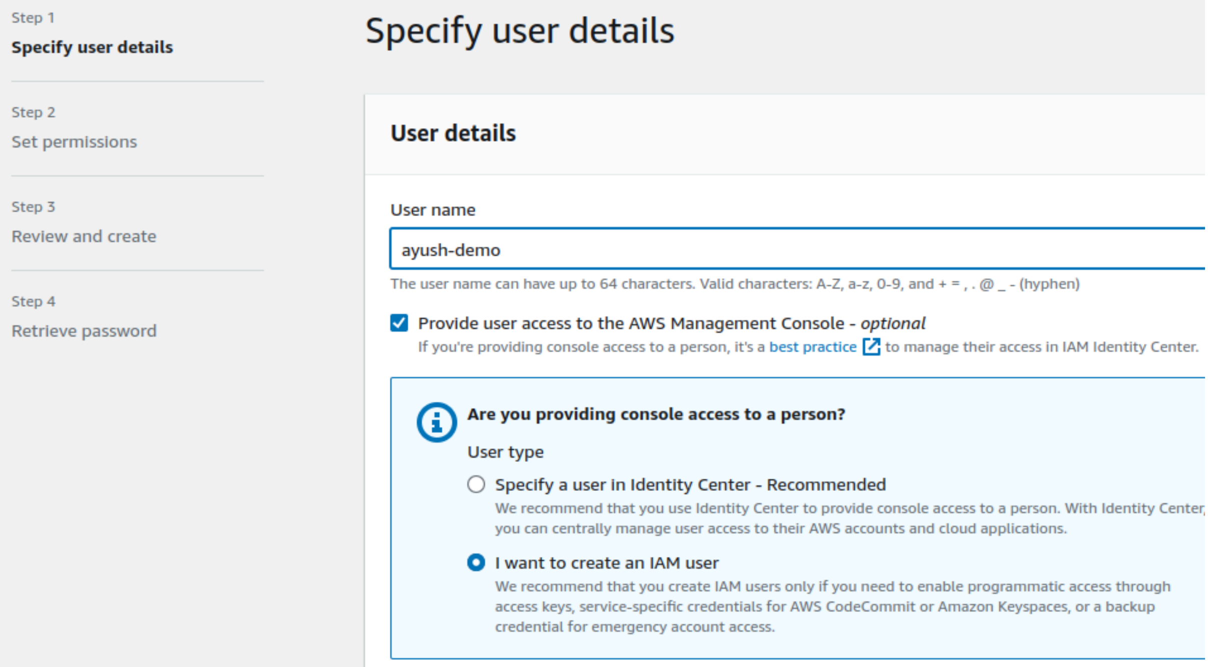


Users (0) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name ▲	Path ▽	Group: ▽	Last activity ▽	MFA ▽	Password age ▽
			No resources to display			

Provide a username for the new user



Specify user details

User details

User name: ayush-demo

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

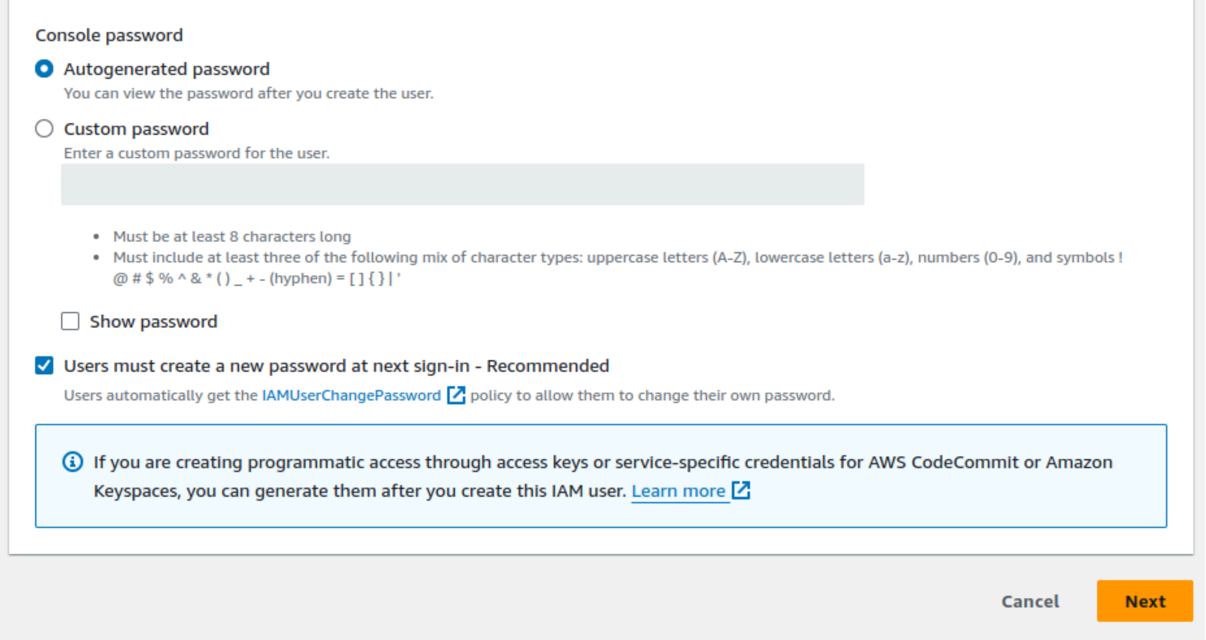
○ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Configure other details



Console password

● Autogenerated password
You can view the password after you create the user.

○ Custom password
Enter a custom password for the user.

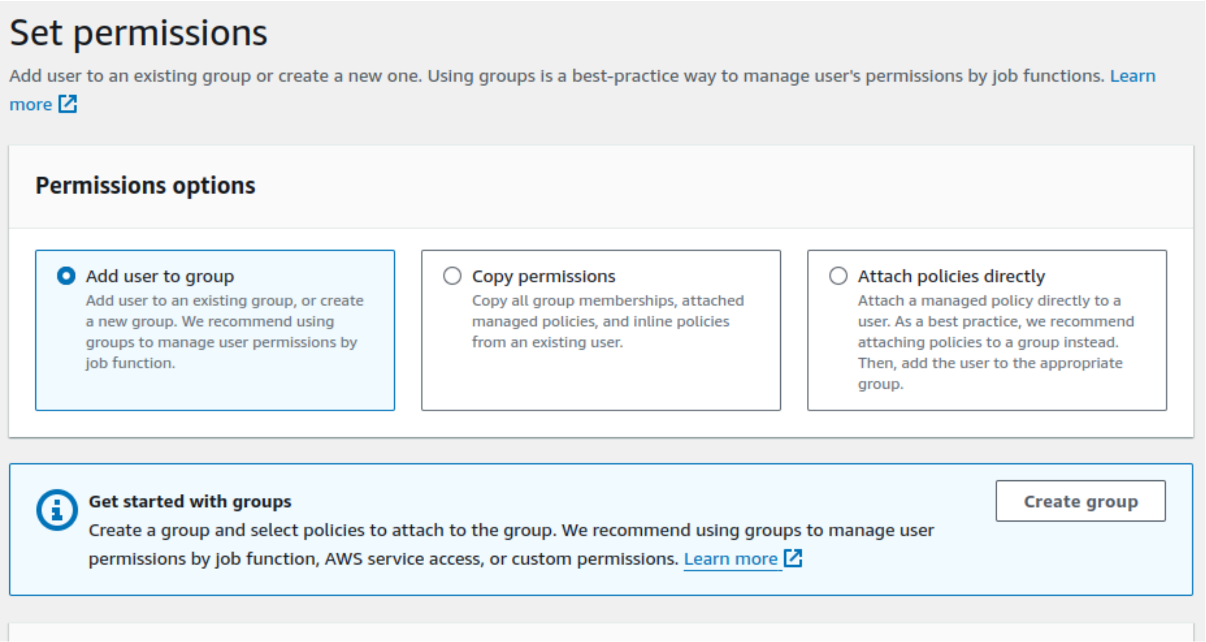
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password

☑ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

Add permissions if necessary



Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

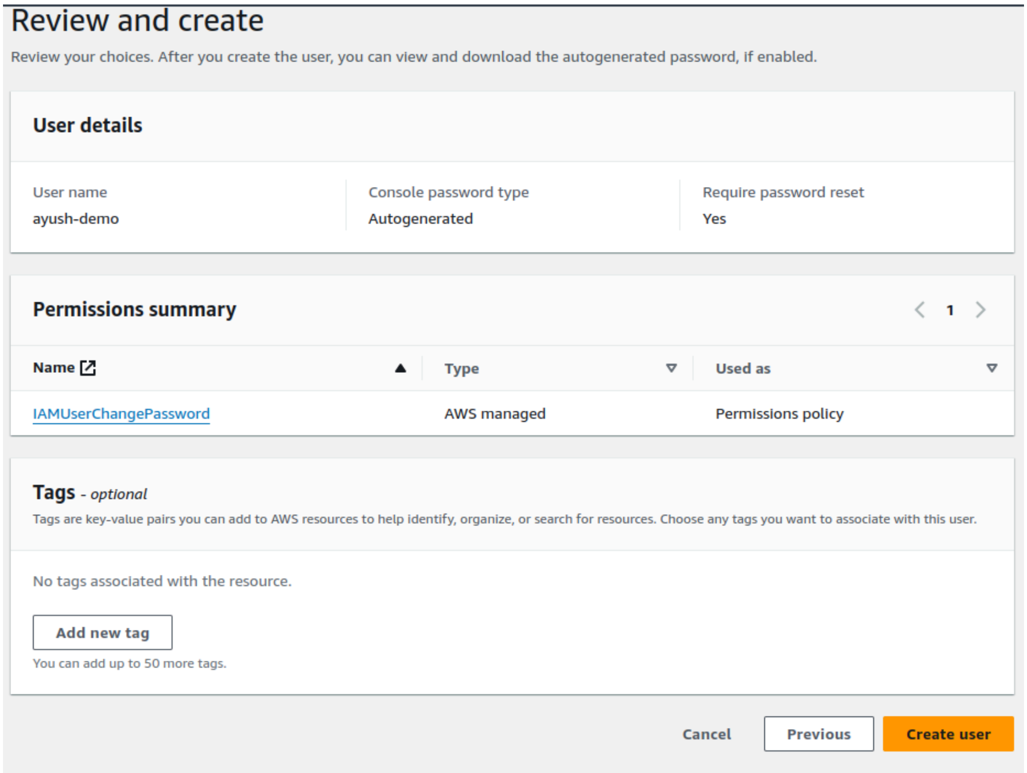
● Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more

Click on Create



Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
ayush-demo	Autogenerated	Yes

Permissions summary < 1 >

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

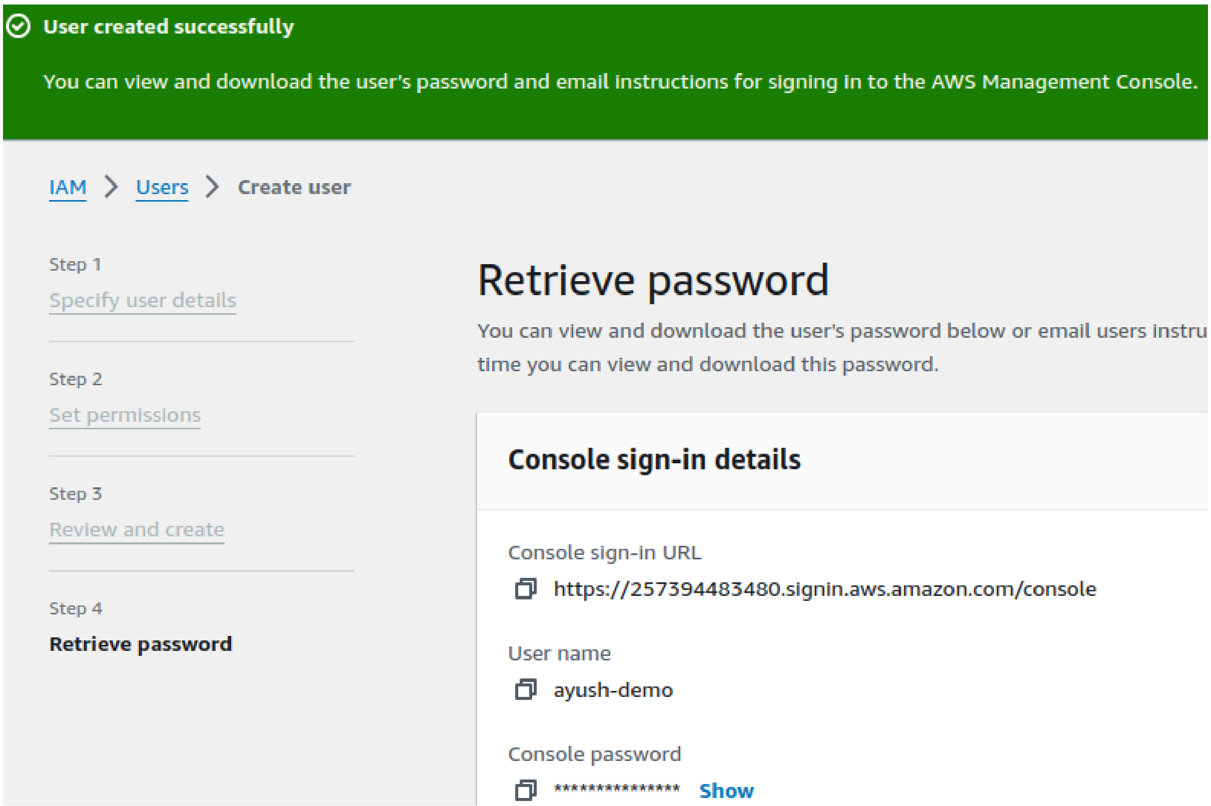
Tags - *optional*

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

You can add up to 50 more tags.

User Created Successfully



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Retrieve password

You can view and download the user's password below or email users instru
time you can view and download this password.

Console sign-in details

Console sign-in URL

https://257394483480.signin.aws.amazon.com/console

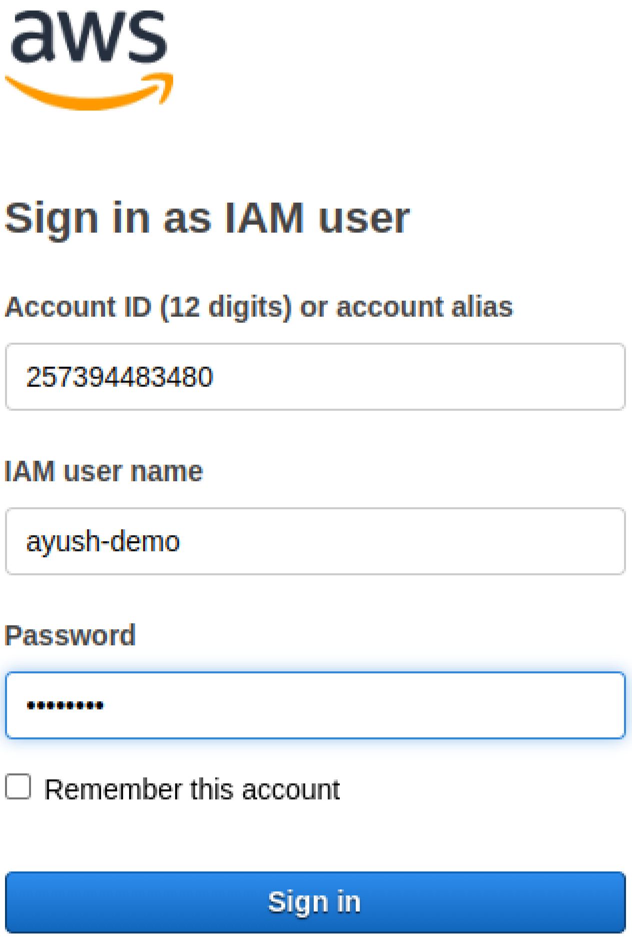
User name

ayush-demo

Console password

*************** Show

Sign in as IAM User



Sign in as IAM user

Account ID (12 digits) or account alias

257394483480

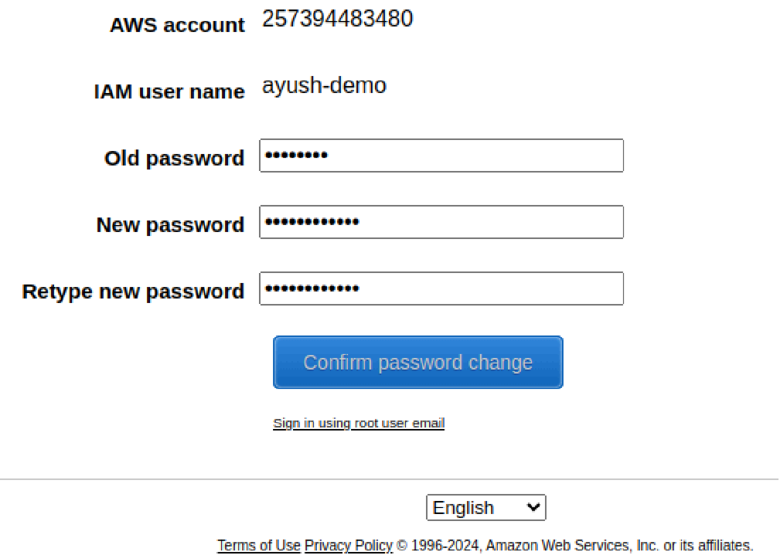
IAM user name

ayush-demo

Password

••••••••

□ Remember this account



AWS account 257394483480

IAM user name ayush-demo

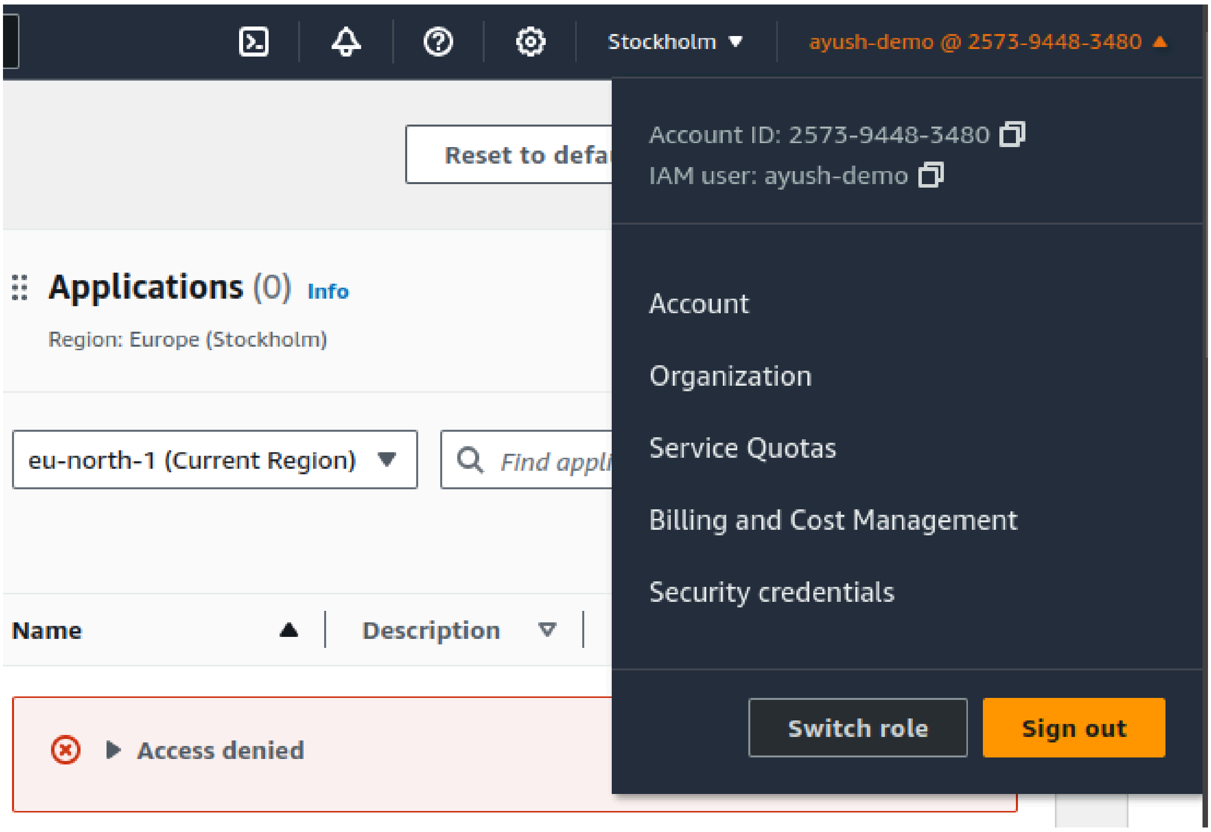
Old password ••••••••

New password ••••••••••••

Retype new password ••••••••••••

Terms of Use Privacy Policy © 1996-2024, Amazon Web Services, Inc. or its affiliates.

Sign in Successful



Account ID: 2573-9448-3480

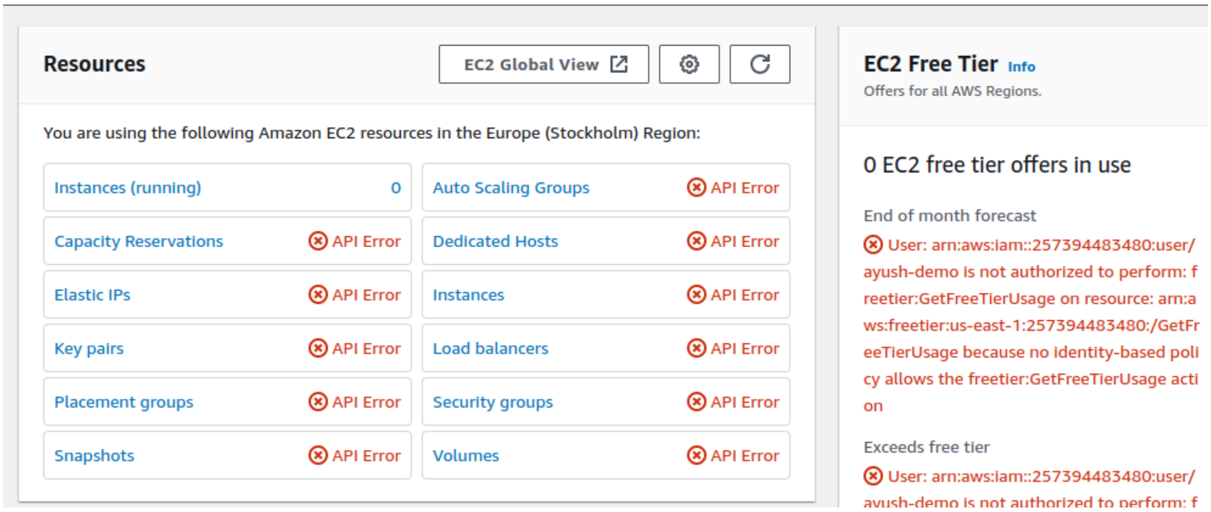
IAM user: ayush-demo

Applications (0)

Region: Europe (Stockholm)

eu-north-1 (Current Region)

Access denied



You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

Instances (running)	0	Auto Scaling Groups	⊗ API Error
Capacity Reservations	⊗ API Error	Dedicated Hosts	⊗ API Error
Elastic IPs	⊗ API Error	Instances	⊗ API Error
Key pairs	⊗ API Error	Load balancers	⊗ API Error
Placement groups	⊗ API Error	Security groups	⊗ API Error
Snapshots	⊗ API Error	Volumes	⊗ API Error

Offers for all AWS Regions.

0 EC2 free tier offers in use

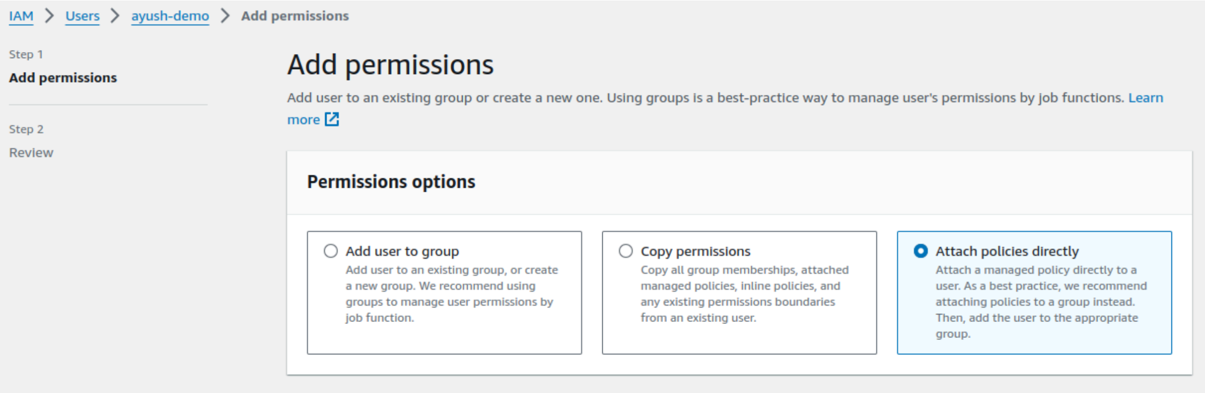
End of month forecast

⊗ User: arn:aws:iam::257394483480:user/ayush-demo is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:257394483480:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action

Exceeds free tier

⊗ User: arn:aws:iam::257394483480:user/ayush-demo is not authorized to perform: f

Adding Admin Permissions



IAM > Users > ayush-demo > Add permissions

Step 1
Add permissions

Step 2
Review

Add permissions

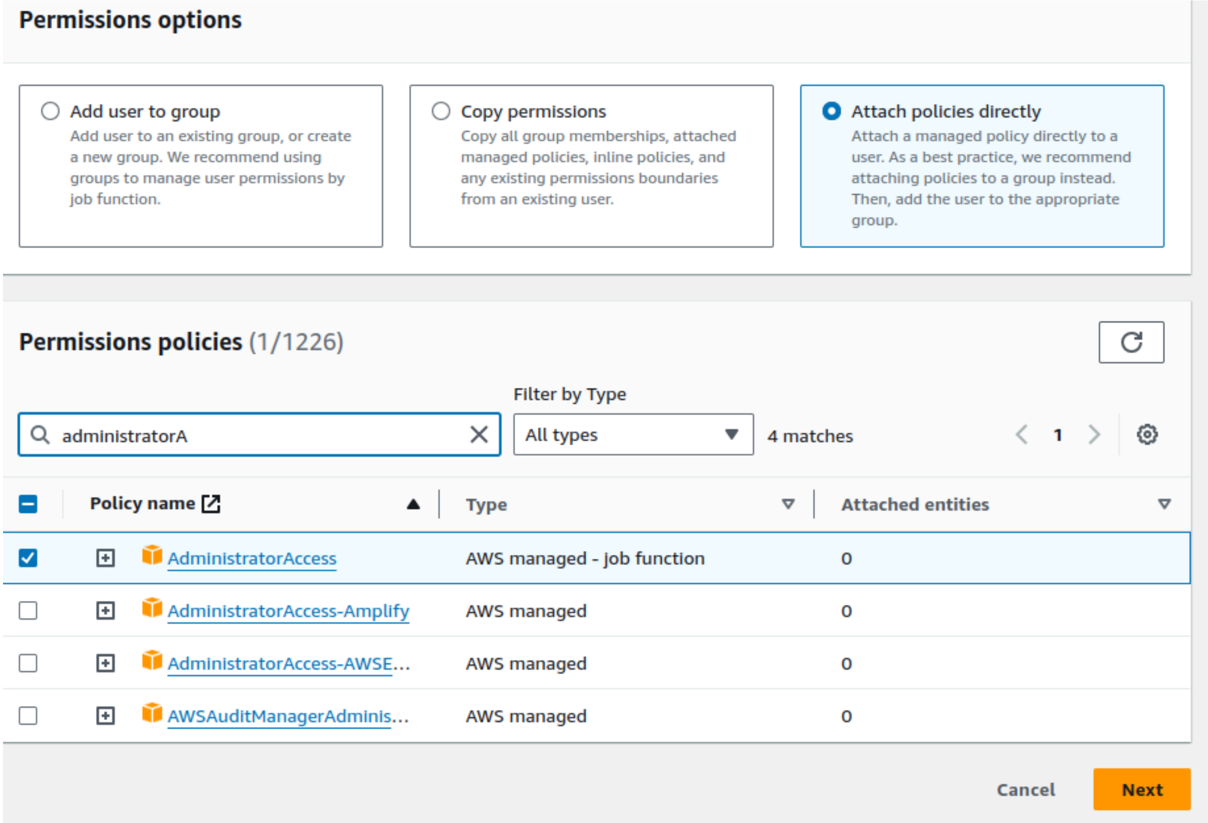
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.

● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.



Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.

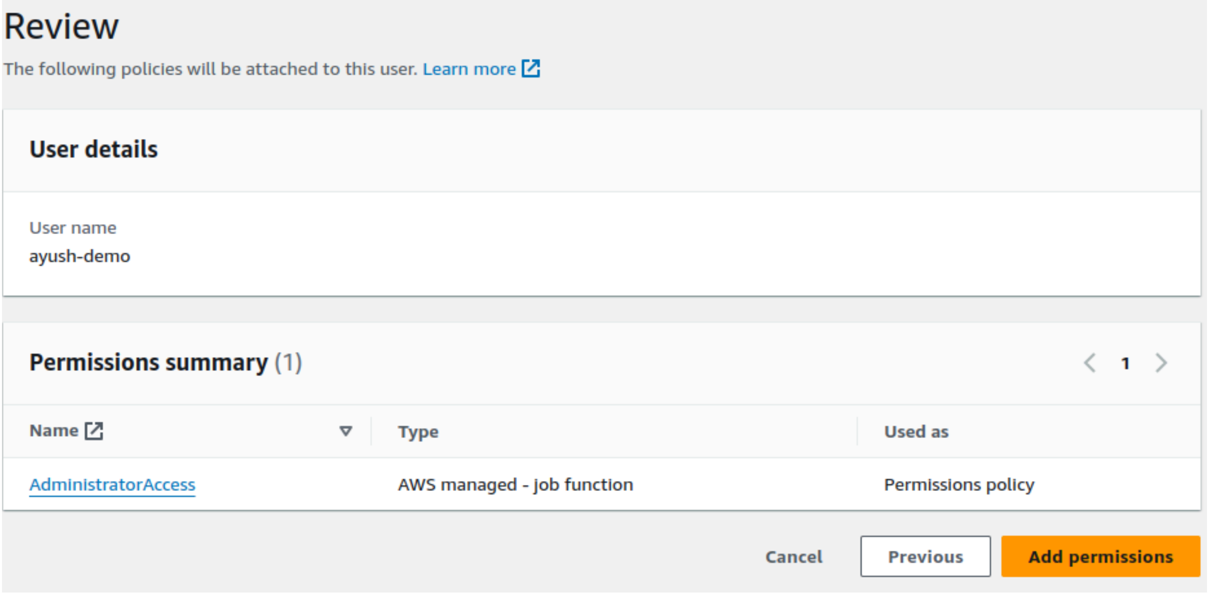
● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1226)

Filter by Type

administratorA | All types | 4 matches | < 1 >

☐	Policy name	Type	Attached entities
☑	AdministratorAccess	AWS managed - job function	0
☐	AdministratorAccess-Amplify	AWS managed	0
☐	AdministratorAccess-AWSE...	AWS managed	0
☐	AWSAuditManagerAdminis...	AWS managed	0



Review

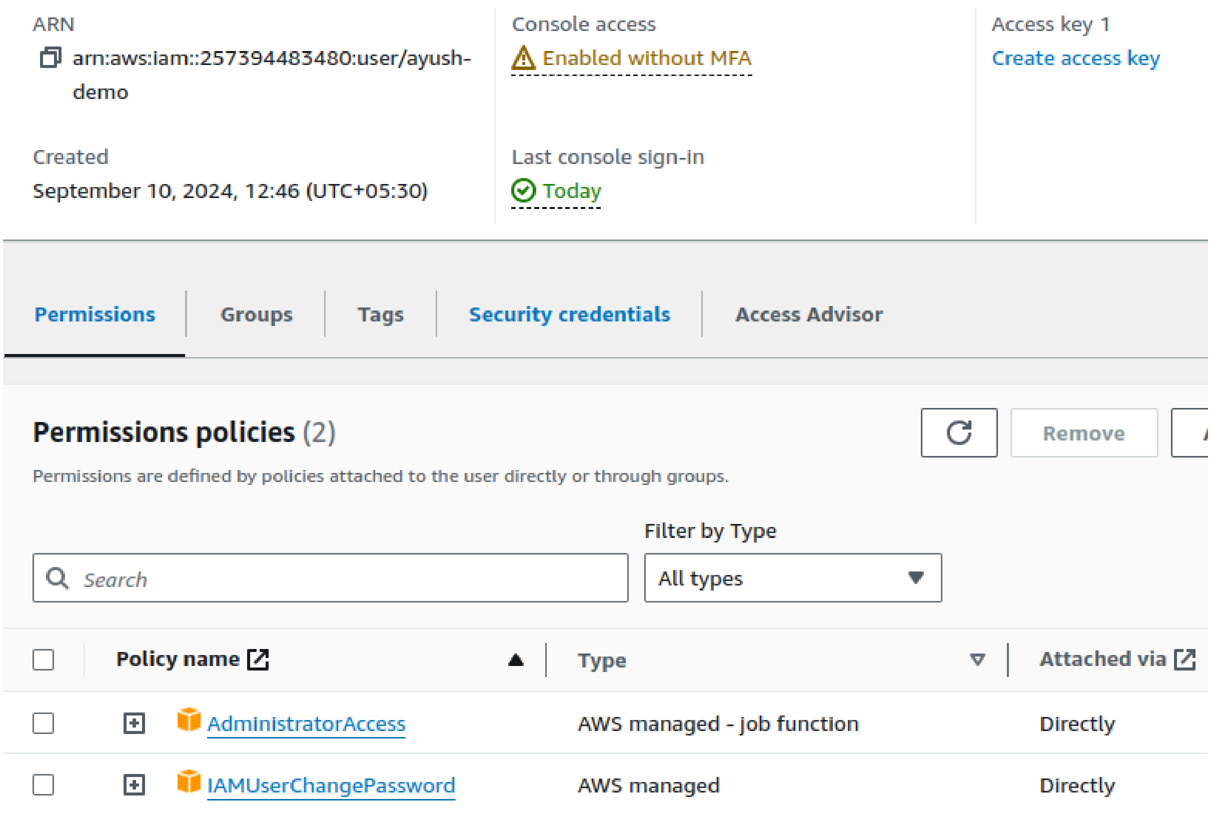
The following policies will be attached to this user. Learn more

User details

User name
ayush-demo

Permissions summary (1)

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy



ARN
arn:aws:iam::257394483480:user/ayush-demo

Console access
Enabled without MFA

Access key 1
Create access key

Created
September 10, 2024, 12:46 (UTC+05:30)

Last console sign-in
Today

Permissions policies (2)

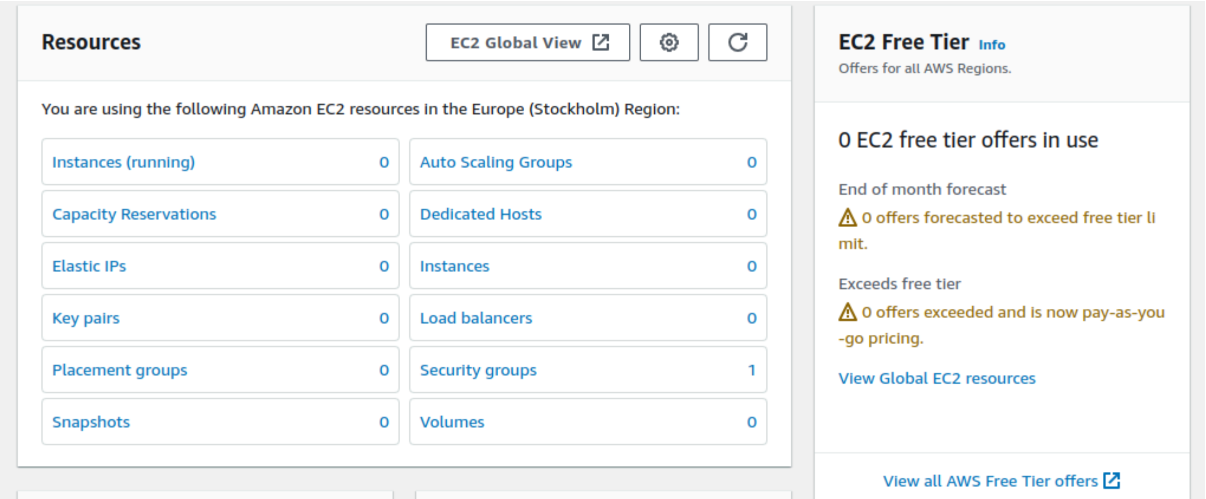
Permissions are defined by policies attached to the user directly or through groups.

Filter by Type

All types

□	Policy name	Type	Attached via
□	AdministratorAccess	AWS managed - job function	Directly
□	IAMUserChangePassword	AWS managed	Directly

Permission successfully granted



Resources

EC2 Global View

You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

Instances (running)	0	Auto Scaling Groups	0
Capacity Reservations	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	0	Load balancers	0
Placement groups	0	Security groups	1
Snapshots	0	Volumes	0

EC2 Free Tier Info

Offers for all AWS Regions.

0 EC2 free tier offers in use

End of month forecast

⚠ 0 offers forecasted to exceed free tier limit.

Exceeds free tier

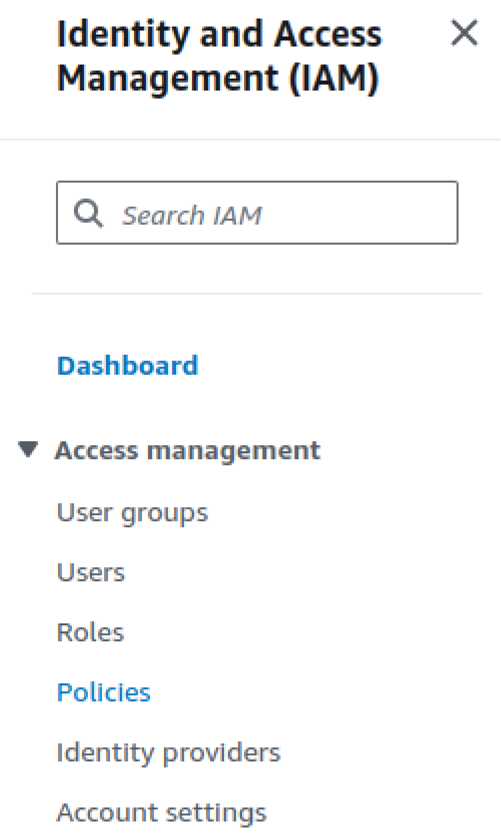
⚠ 0 offers exceeded and is now pay-as-you-go pricing.

View Global EC2 resources

View all AWS Free Tier offers

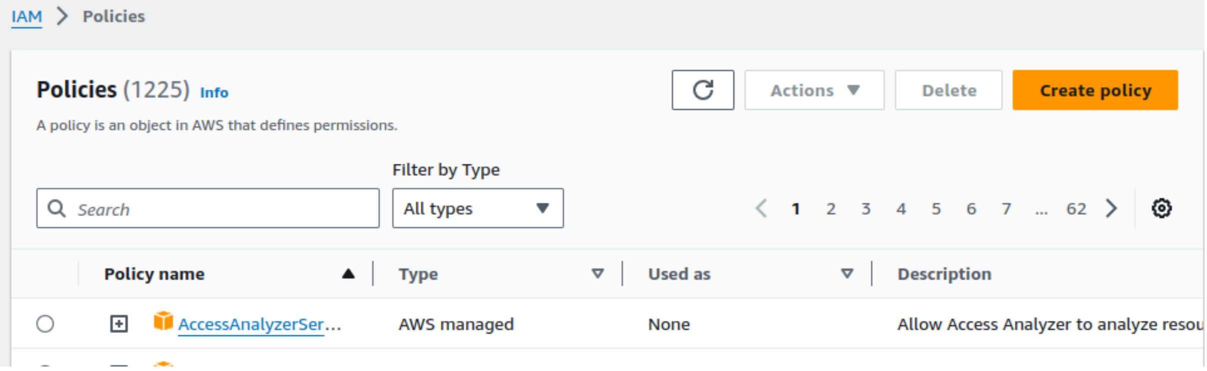
Custom Policy

Navigate to Policy in IAM Dashboard



Identity and Access Management (IAM)

Create a Policy

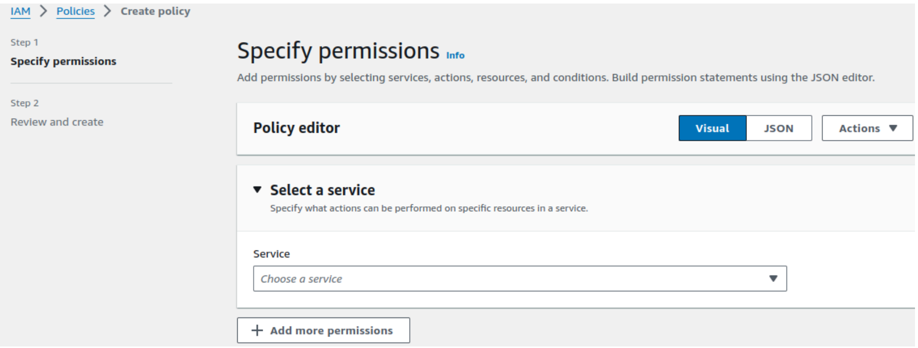


Policies (1225) Info

A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as	Description
○	AccessAnalyzerSer…	AWS managed	None	Allow Access Analyzer to analyze resou

Scroll to Specify Permissions



Specify permissions Info

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

Policy editor

▼ Select a service

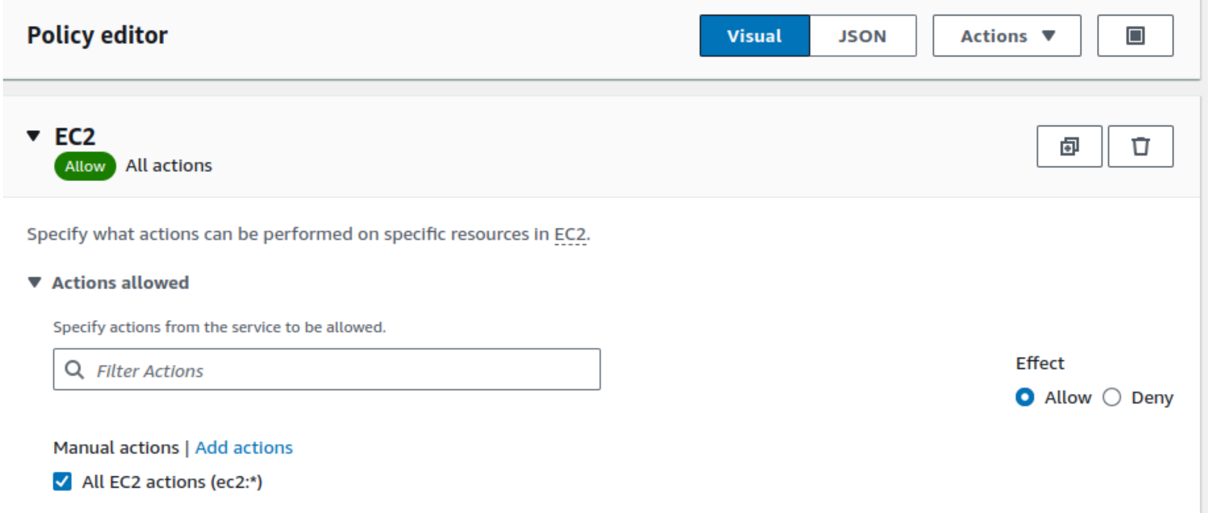
Specify what actions can be performed on specific resources in a service.

Service

Create a custom policy to get access to EC2 instances and all services in IAM.

Under the **Visual editor** tab, start defining permissions

- **Service**: Click on **Choose a service** and select **EC2**.
- **Actions**: Choose **All EC2 actions** by selecting the checkbox next to **All EC2 actions**.
- **Resources**: Keep the default selection, which is **All resources**.



▼ EC2

Allow All actions

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

▼ Actions allowed

Specify actions from the service to be allowed.

Effect

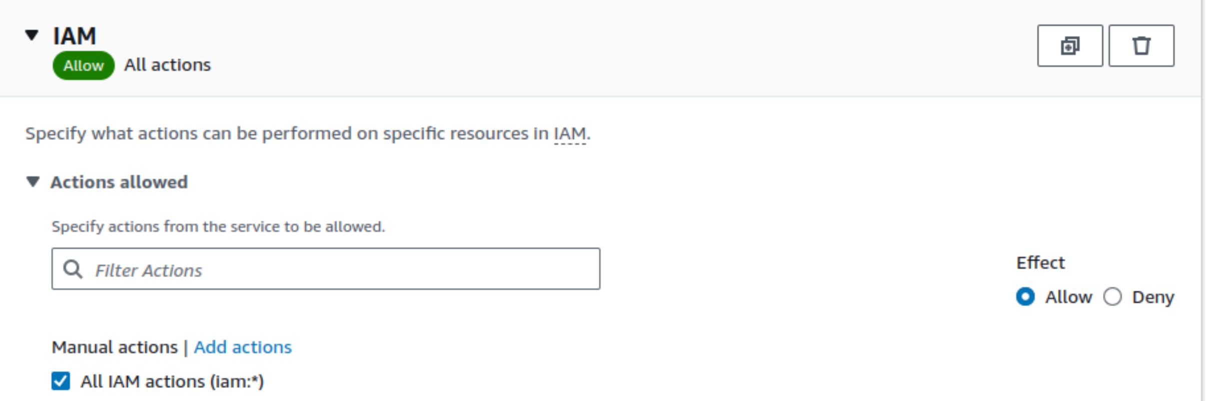
● Allow ○ Deny

Manual actions | Add actions

☑ All EC2 actions (ec2:*)

Now, add permissions for IAM services

- **Service**: Click **Add additional permissions** and select **IAM**.
- **Actions**: Select **All IAM actions** by choosing the checkbox next to **All IAM actions**.
- **Resources**: Leave it as **All resources**.



▼ IAM

Allow All actions

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

▼ Actions allowed

Specify actions from the service to be allowed.

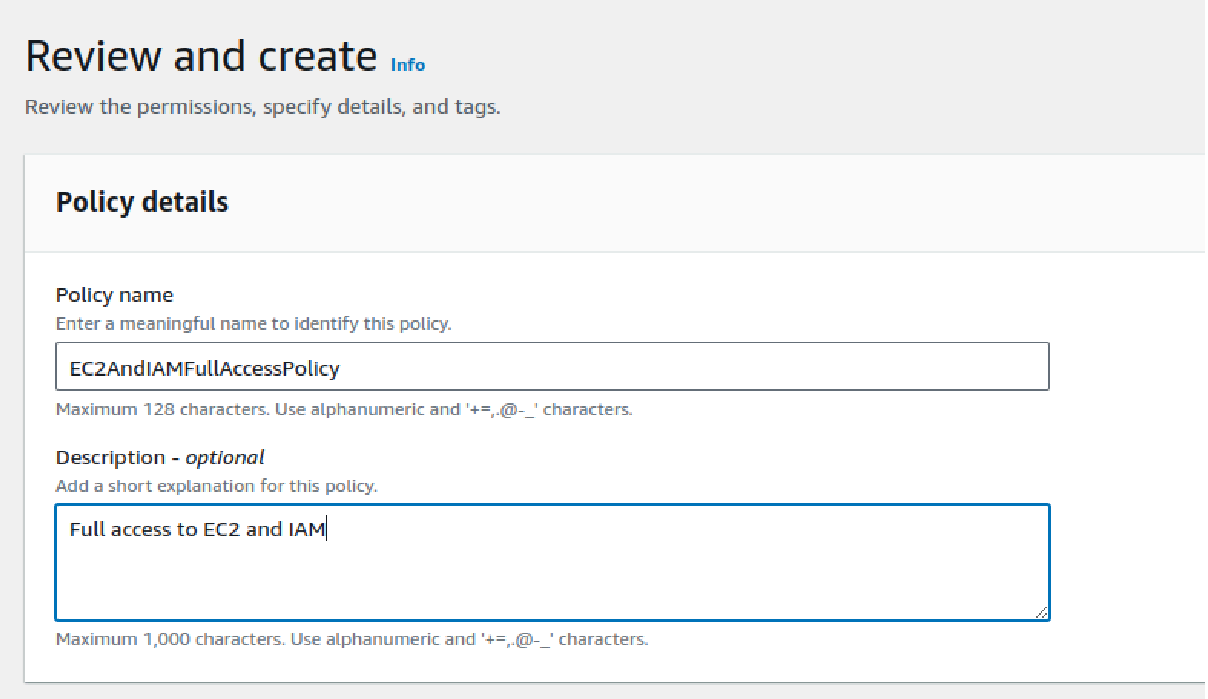
Effect

● Allow ○ Deny

Manual actions | Add actions

☑ All IAM actions (iam:*)

Provide a **Name**



Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

EC2AndIAMFullAccessPolicy

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

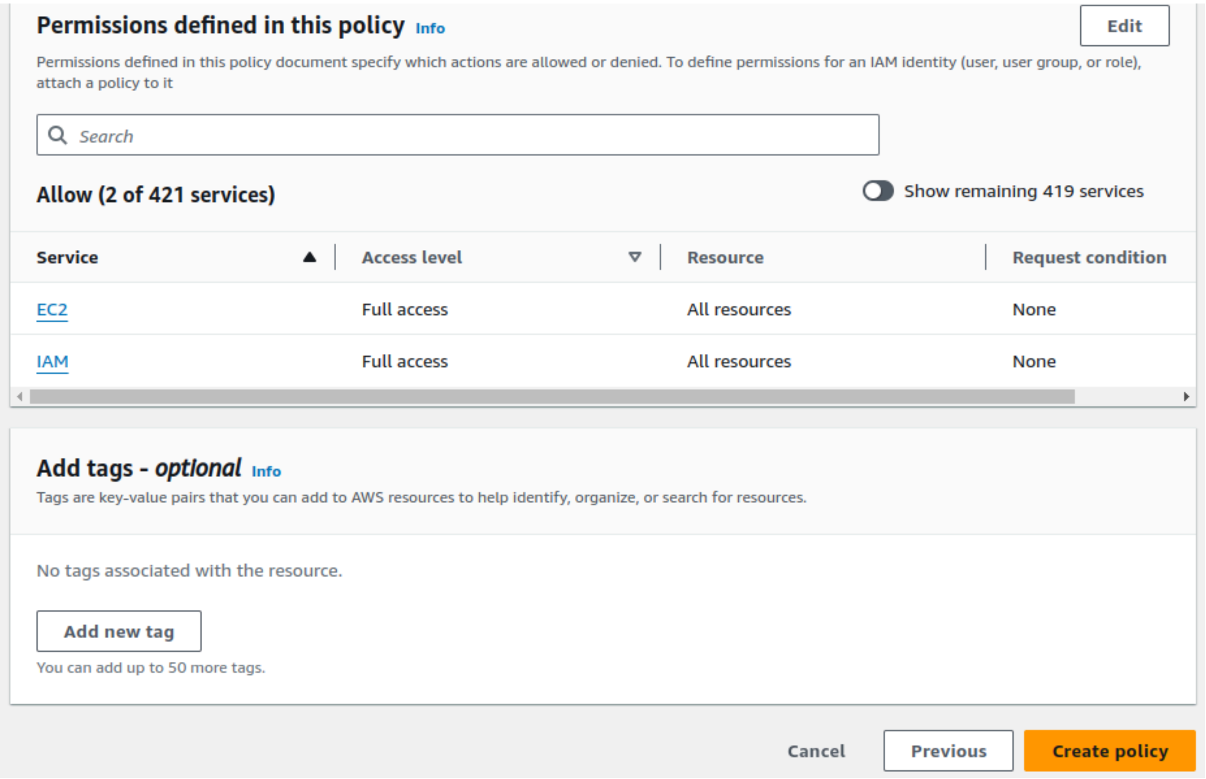
Description - *optional*

Add a short explanation for this policy.

Full access to EC2 and IAM

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Click **Create policy**



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 (2 of 421 services)

Show remaining 419 services

Service	Access level	Resource	Request condition
EC2	Full access	All resources	None
IAM	Full access	All resources	None

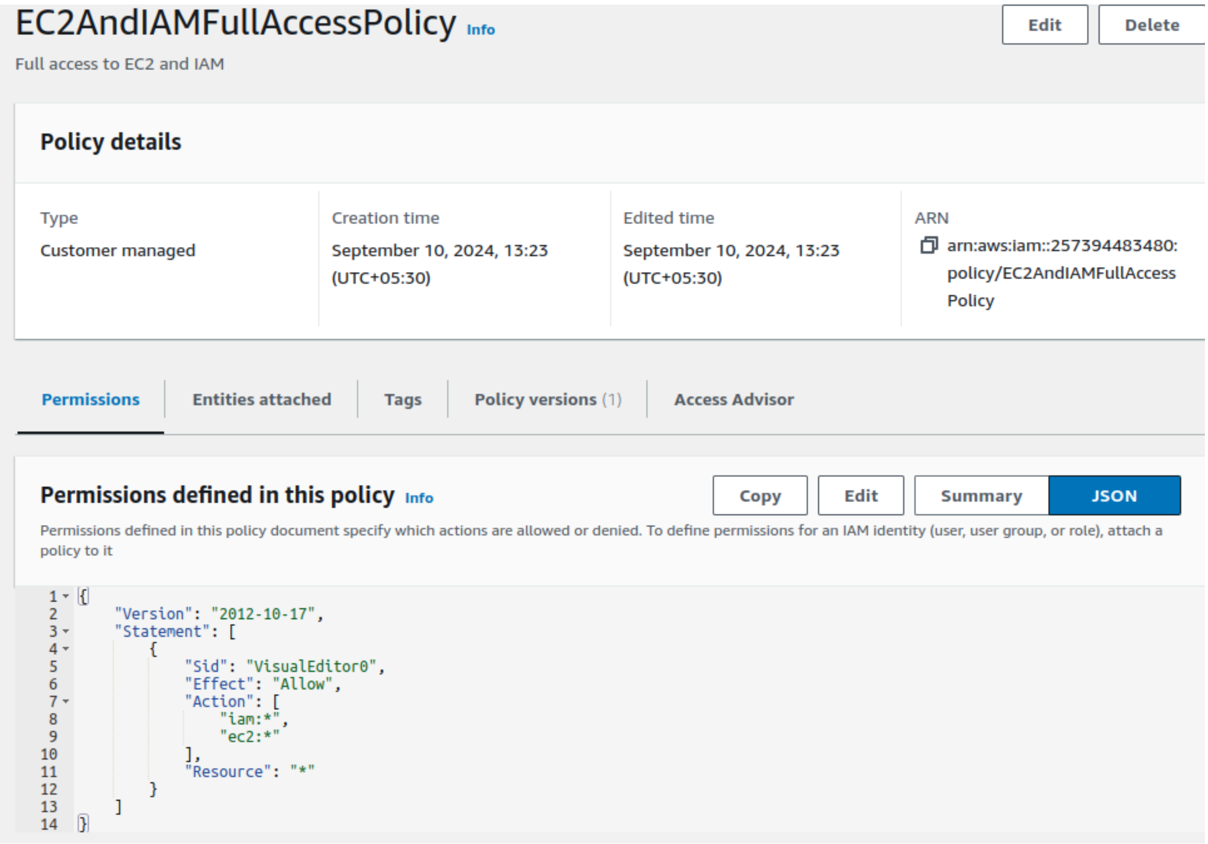
Add tags - *optional*

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 Successfully Created



Full access to EC2 and IAM

Policy details

Type	Creation time	Edited time	ARN
Customer managed	September 10, 2024, 13:23 (UTC+05:30)	September 10, 2024, 13:23 (UTC+05:30)	arn:aws:iam::257394483480:policy/EC2AndIAMFullAccessPolicy

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:*",
                "ec2:*"
            ],
            "Resource": "*"
        }
    ]
}
```

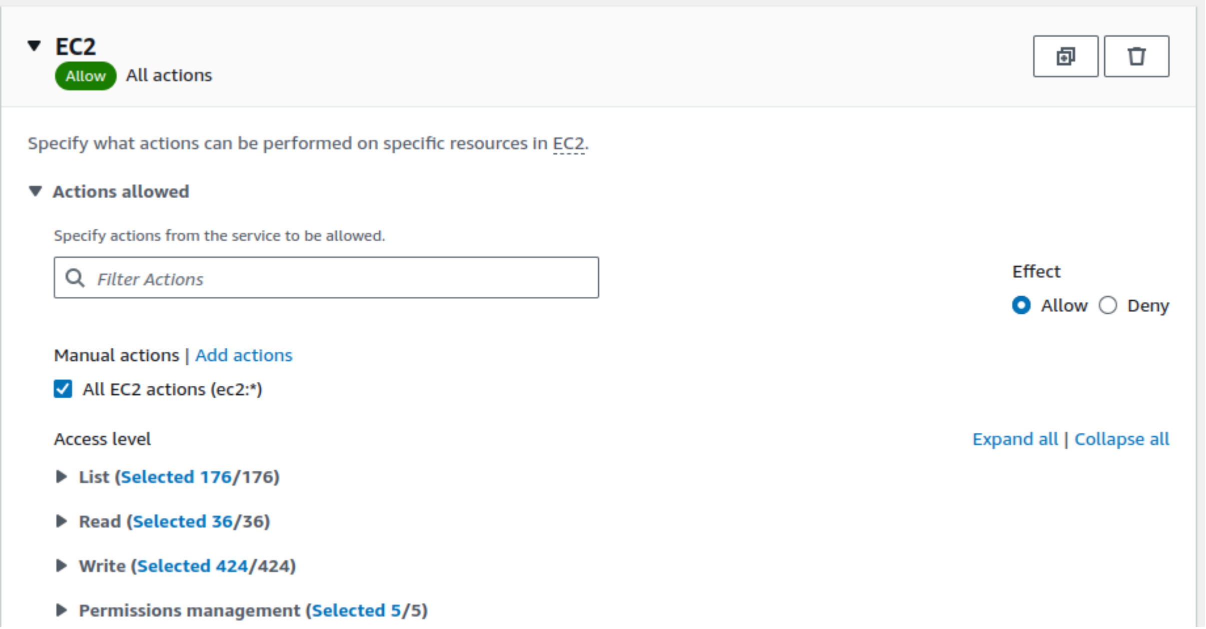
JSON code

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:*",
                "ec2:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Create custom policy to get access to all EC2 services and get IAM users

Under the **Visual editor** tab, start defining permissions

- **Service**: Select **EC2**.
- **Actions**: Choose **All EC2 actions** by selecting **All EC2 actions**.
- **Resources**: Keep the default option of **All resources**.



▼ EC2

Allow All actions

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

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect

● Allow ○ Deny

Manual actions | Add actions

☑ All EC2 actions (ec2:*)

Access level

▶ List (Selected 176/176)

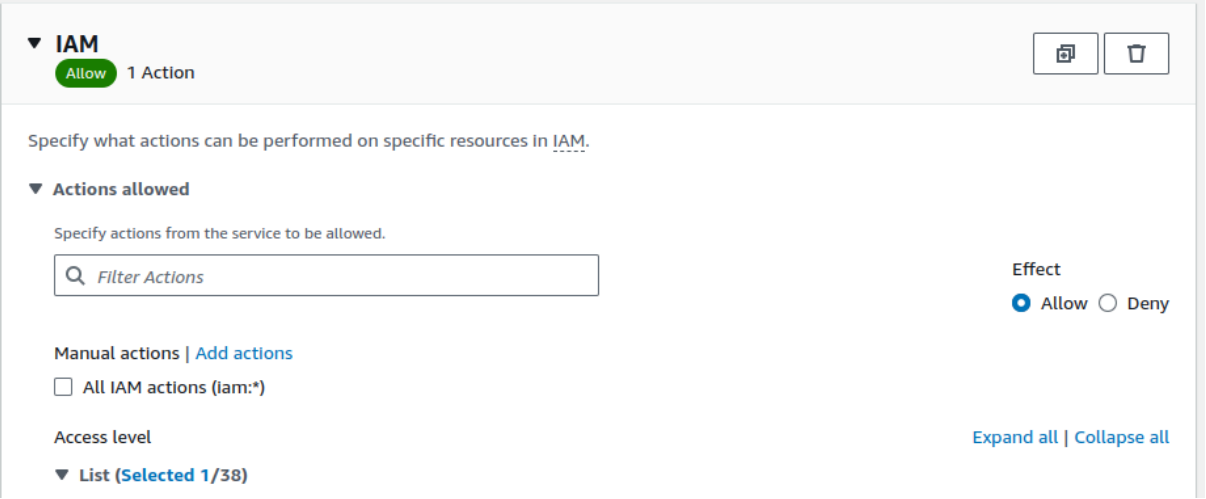
▶ Read (Selected 36/36)

▶ Write (Selected 424/424)

▶ Permissions management (Selected 5/5)

Add permissions for IAM services

- **Service**: Click **Add additional permissions** and select **IAM**.
- **Actions**: In the search bar, type `GetUser` and select **GetUser**. Similarly, type `ListUsers` and select **ListUsers**.
- **Resources**: Leave it as **All resources**.



▼ IAM

Allow 1 Action

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

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect

● Allow ○ Deny

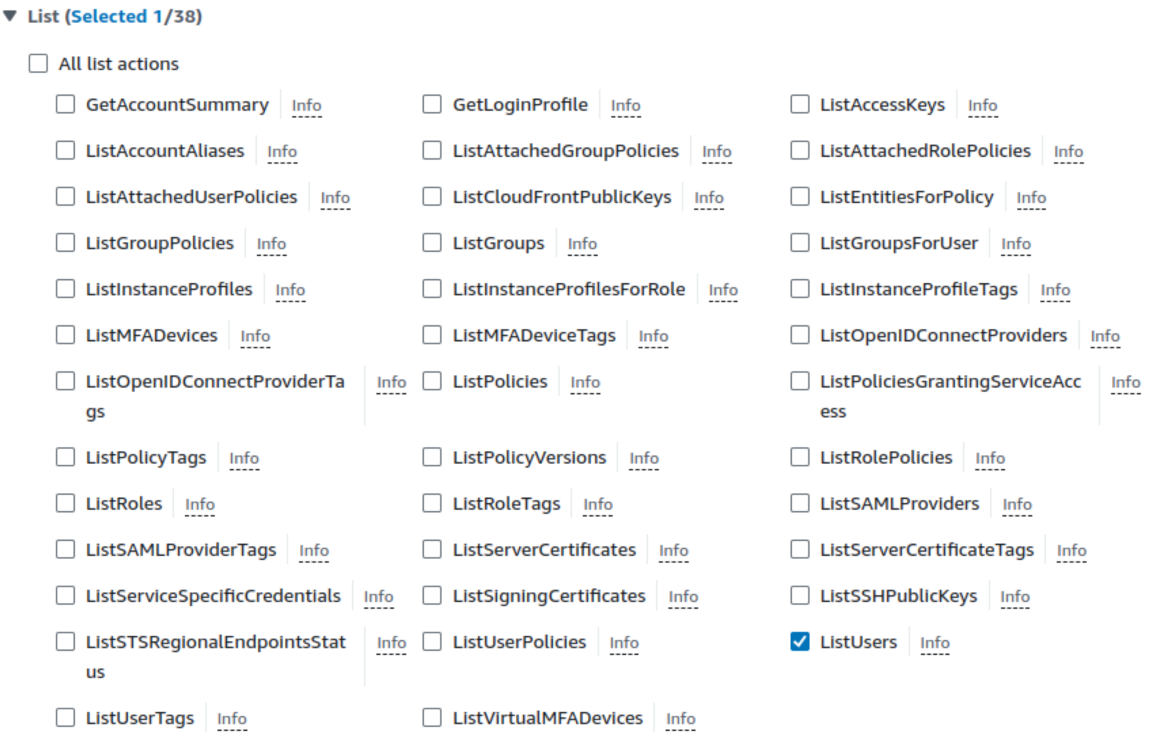
Manual actions | Add actions

☐ All IAM actions (iam:*)

Access level

Expand all | Collapse all

▼ List (Selected 1/38)

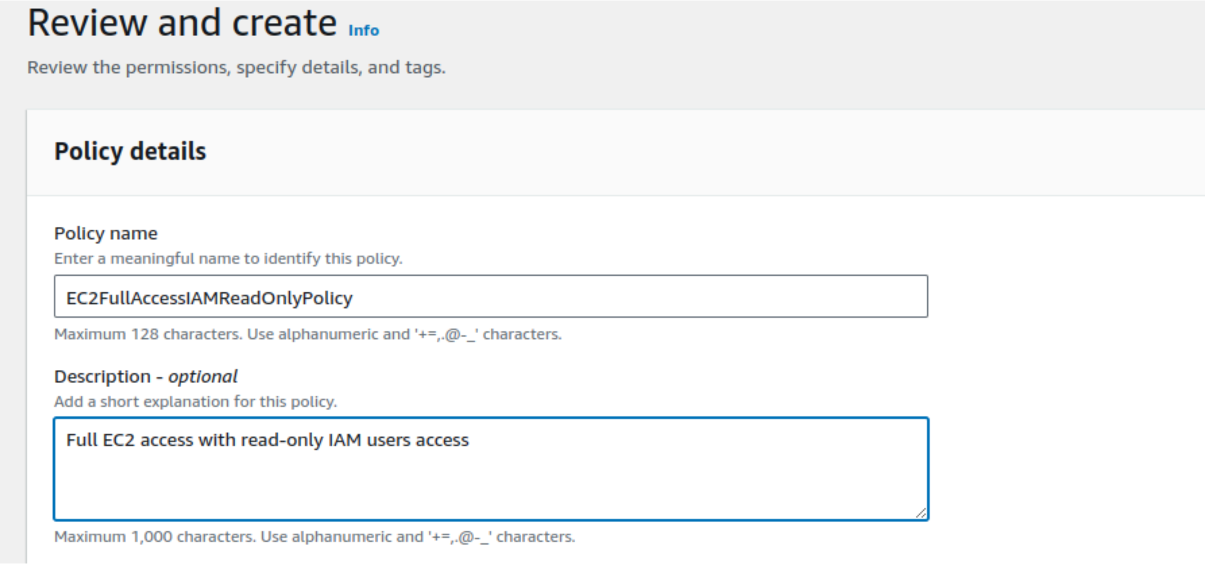


▼ List (Selected 1/38)

☐ All list actions

- ☐ GetAccountSummary Info
- ☐ GetLoginProfile Info
- ☐ ListAccessKeys Info
- ☐ ListAccountAliases Info
- ☐ ListAttachedGroupPolicies Info
- ☐ ListAttachedRolePolicies Info
- ☐ ListAttachedUserPolicies Info
- ☐ ListCloudFrontPublicKeys Info
- ☐ ListEntitiesForPolicy Info
- ☐ ListGroupPolicies Info
- ☐ ListGroups Info
- ☐ ListGroupsForUser Info
- ☐ ListInstanceProfiles Info
- ☐ ListInstanceProfilesForRole Info
- ☐ ListInstanceProfileTags Info
- ☐ ListMFADevices Info
- ☐ ListMFADeviceTags Info
- ☐ ListOpenIDConnectProviders Info
- ☐ ListOpenIDConnectProviderTags Info
- ☐ ListPolicies Info
- ☐ ListPoliciesGrantingServiceAccess Info
- ☐ ListPolicyTags Info
- ☐ ListPolicyVersions Info
- ☐ ListRolePolicies Info
- ☐ ListRoles Info
- ☐ ListRoleTags Info
- ☐ ListSAMLProviders Info
- ☐ ListSAMLProviderTags Info
- ☐ ListServerCertificates Info
- ☐ ListServerCertificateTags Info
- ☐ ListServiceSpecificCredentials Info
- ☐ ListSigningCertificates Info
- ☐ ListSSHPublicKeys Info
- ☐ ListSTSRegionalEndpointsStatus Info
- ☐ ListUserPolicies Info
- ☑ ListUsers Info
- ☐ ListUserTags Info
- ☐ ListVirtualMFADevices Info

Provide a **Name and Description**



Review and create

Info

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

EC2FullAccessIAMReadOnlyPolicy

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

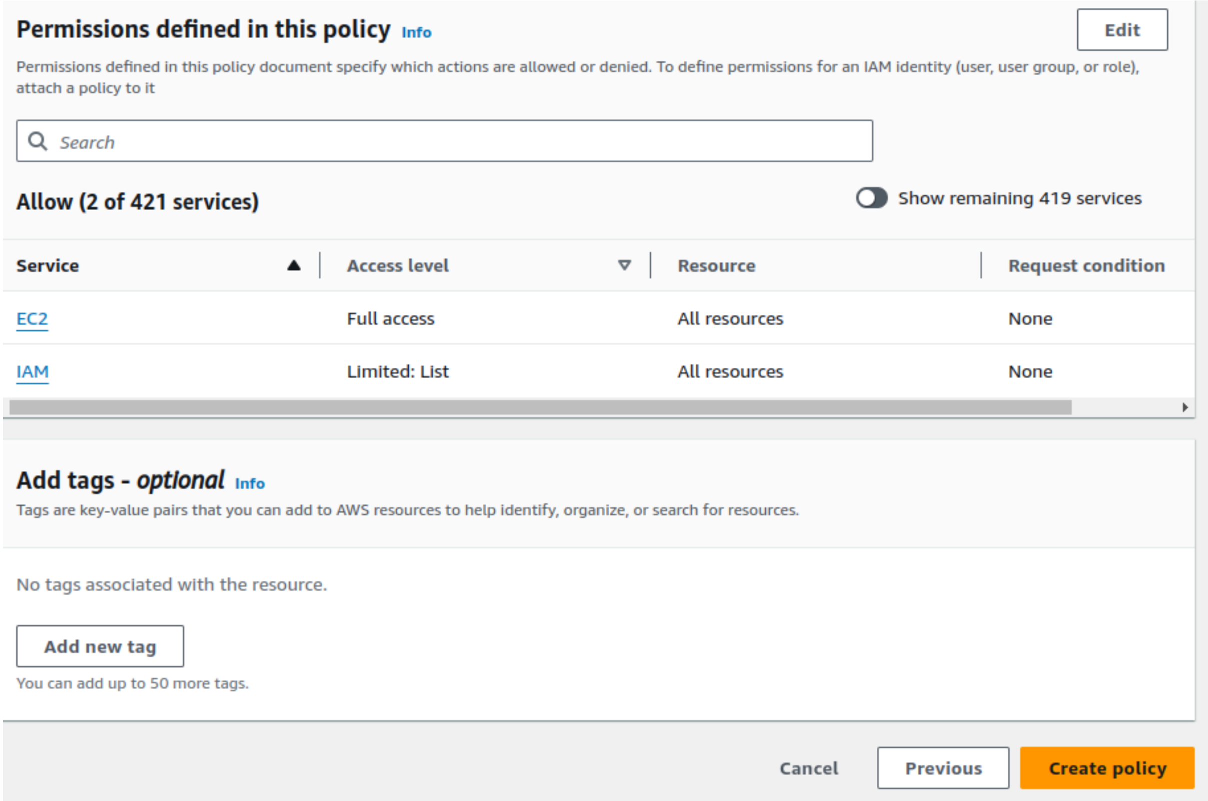
Description - *optional*

Add a short explanation for this policy.

Full EC2 access with read-only IAM users access

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Click **Create policy**



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 (2 of 421 services)

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

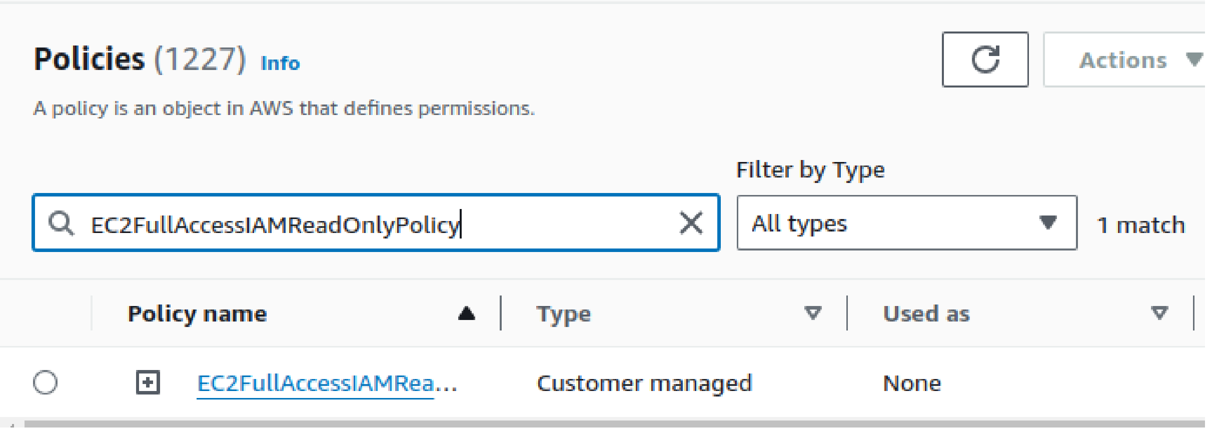
Add tags - *optional*

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 Successfully Created



Policies (1227) Info

A policy is an object in AWS that defines permissions.

Filter by Type

EC2FullAccessIAMReadOnlyPolicy

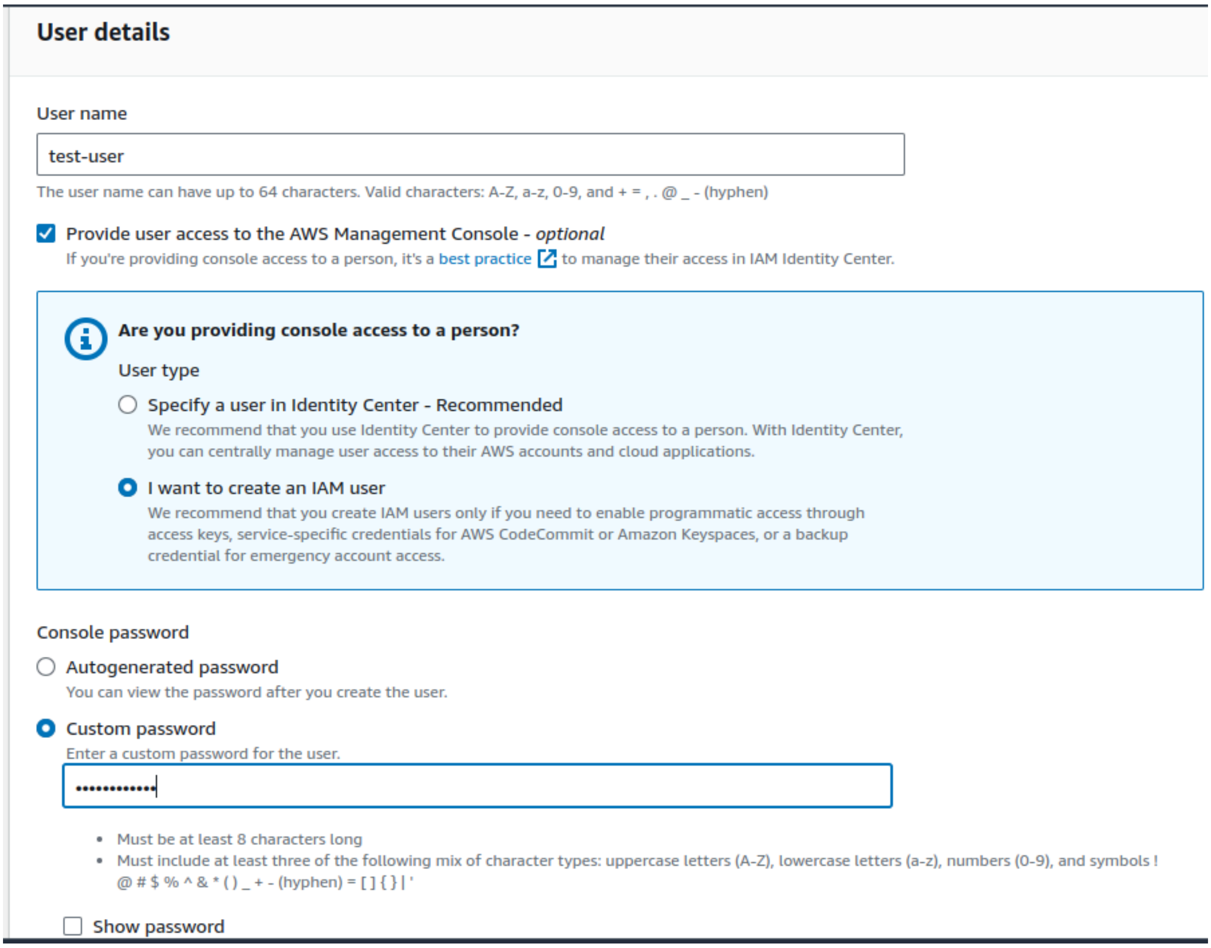
All types ▼

1 match

	Policy name ▲	Type	Used as
○	⊞ EC2FullAccessIAMRea...	Customer managed	None

Create a new User

Following all the steps as mentioned above to create a user



User details

User name

test-user

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

○ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

○ Autogenerated password

You can view the password after you create the user.

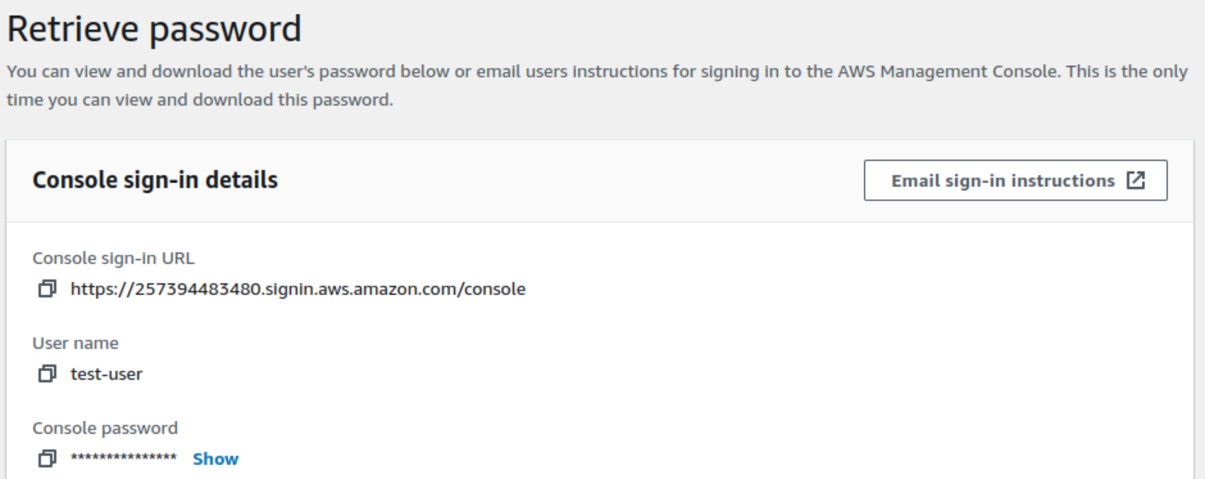
● Custom password

Enter a custom password for the user.

••••••••••••

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password



Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

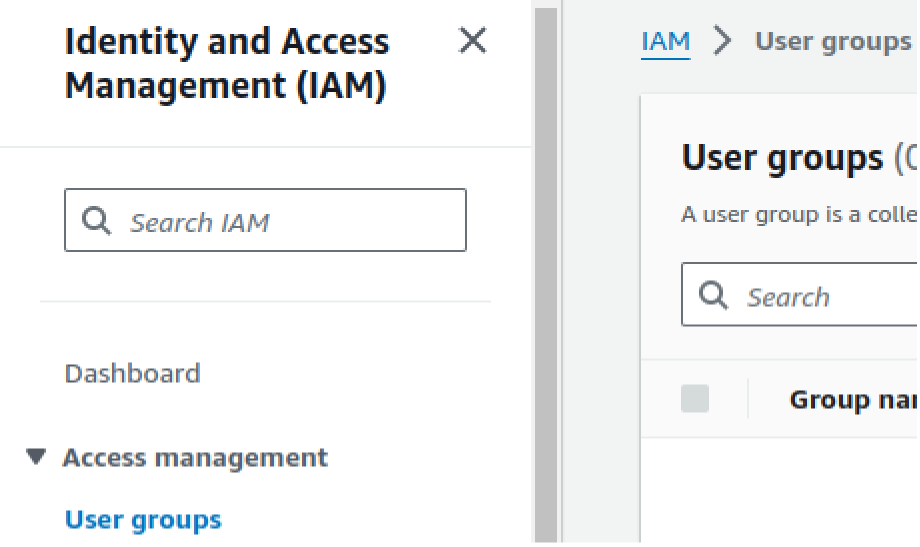
Console sign-in URL
https://257394483480.signin.aws.amazon.com/console

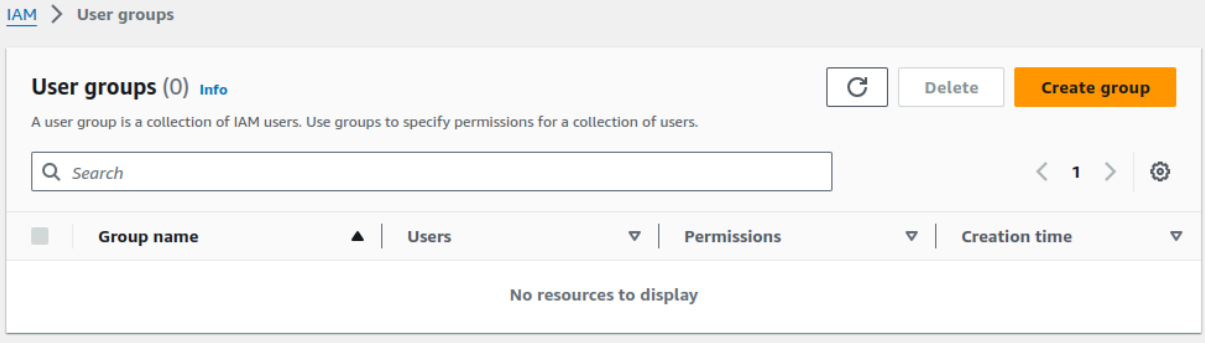
User name
test-user

Console password
****

Create User Group

In the IAM Dashboard, go to User groups and click Create group.





IAM > User groups

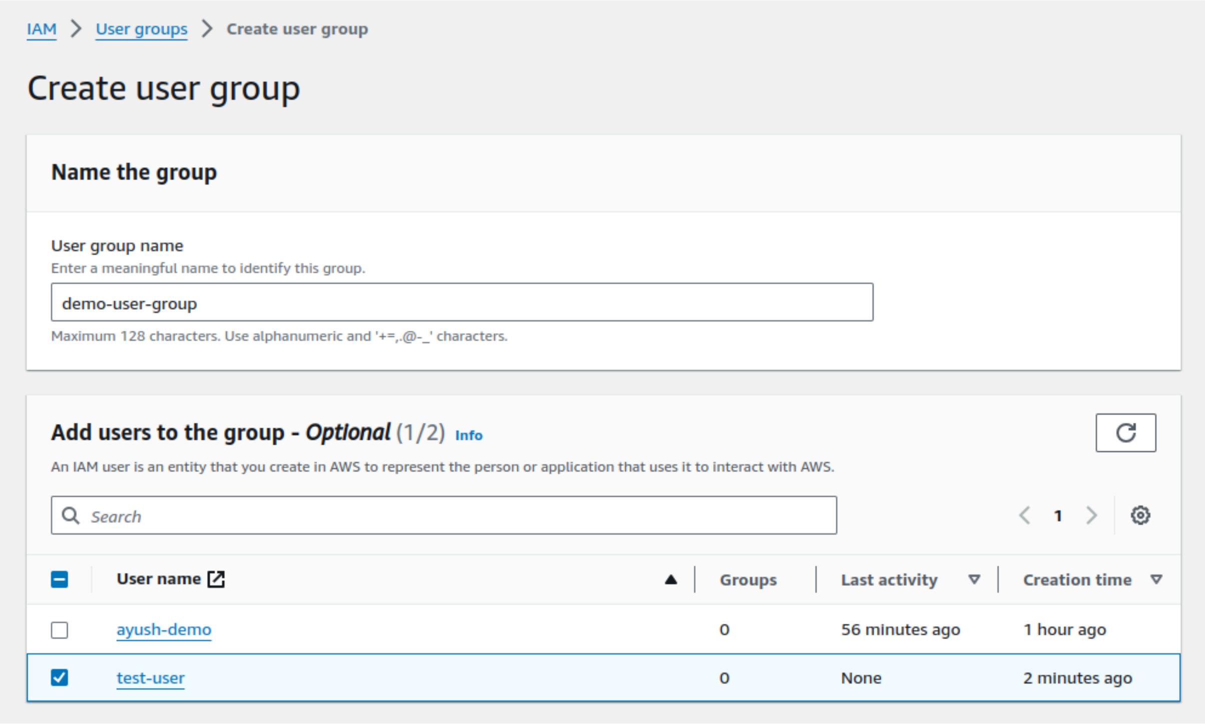
User groups (0)

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

No resources to display

Add user to the user group



IAM > User groups > Create user group

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

demo-user-group

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

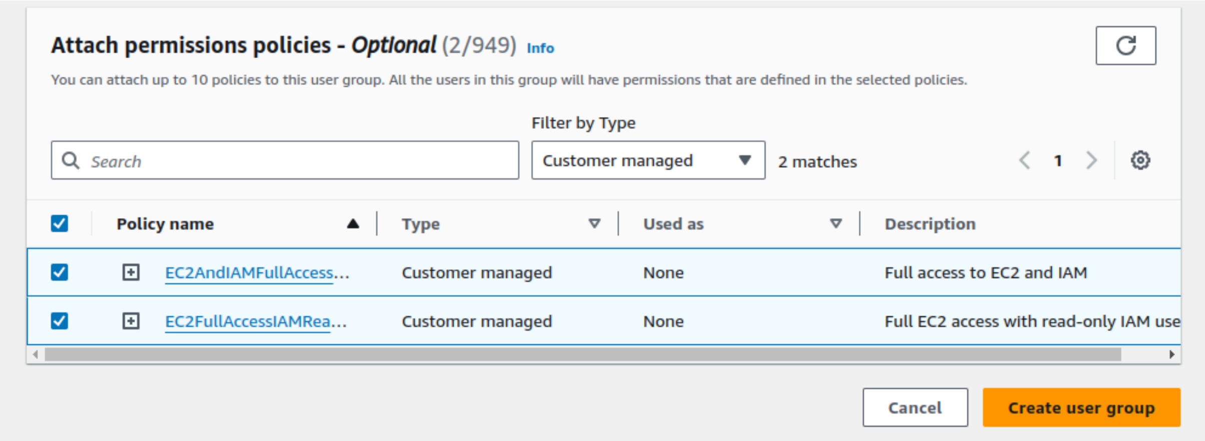
Add users to the group - *Optional* (1/2) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

▣	User name ▲	Groups	Last activity ▽	Creation time ▽
□	ayush-demo	0	56 minutes ago	1 hour ago
☑	test-user	0	None	2 minutes ago

Attach permissions policies page



Attach permissions policies - *Optional* (2/949) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

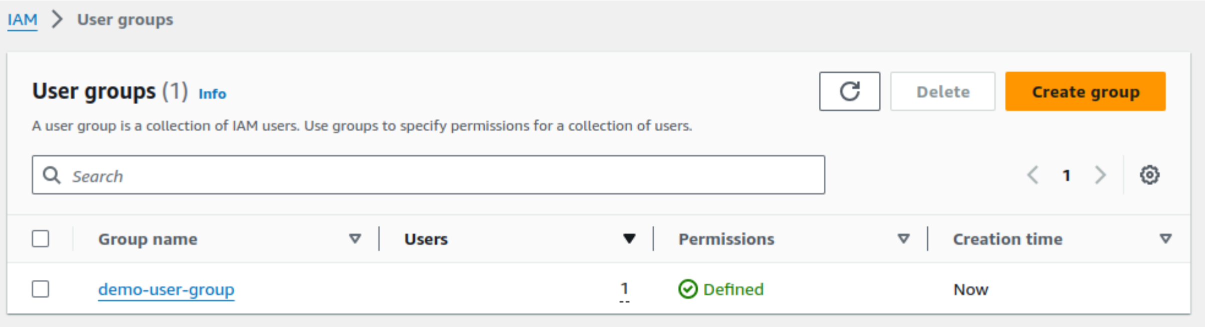
Filter by Type: Customer managed

Search

2 matches

☑	Policy name ▲	Type ▽	Used as ▽	Description
☑	⊞ EC2AndIAMFullAccess...	Customer managed	None	Full access to EC2 and IAM
☑	⊞ EC2FullAccessIAMRea...	Customer managed	None	Full EC2 access with read-only IAM use

User group Created



IAM > User groups

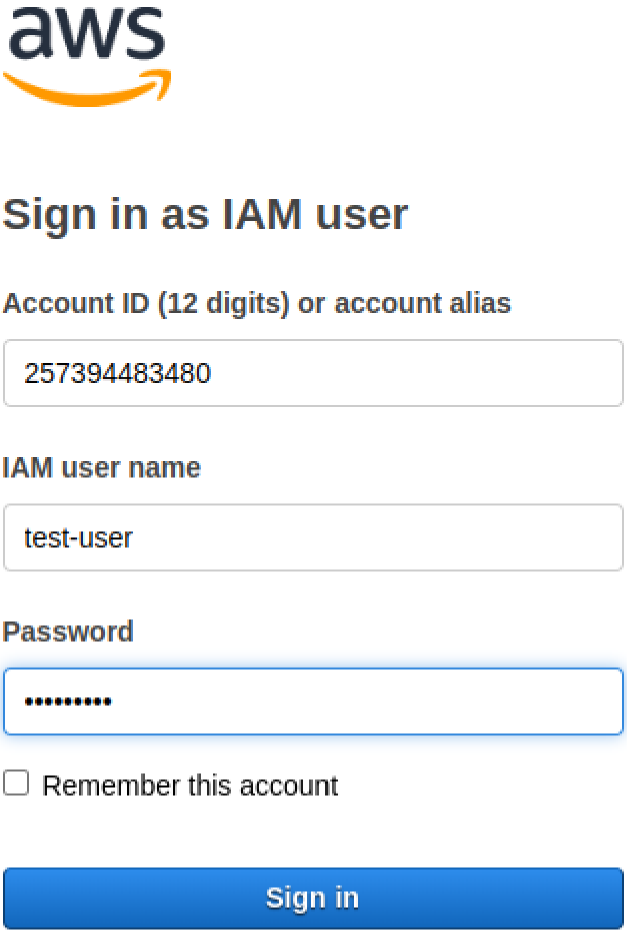
User groups (1) Info

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
□	demo-user-group	1	✓ Defined	Now

Sign in Using New User

Enter Credentials



Sign in as IAM user

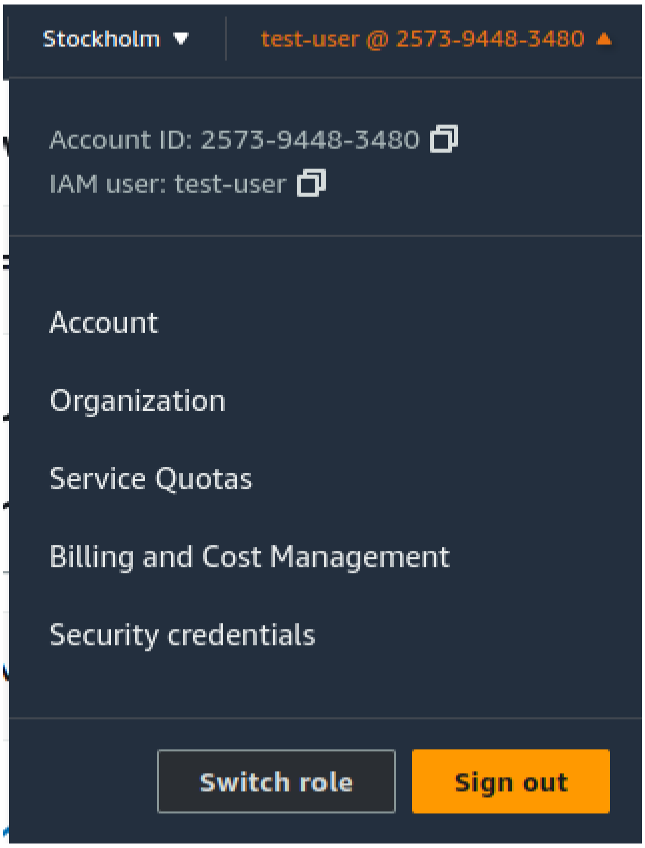
Account ID (12 digits) or account alias: 257394483480

IAM user name: test-user

Password: ••••••••••

□ Remember this account

Sign In Successful

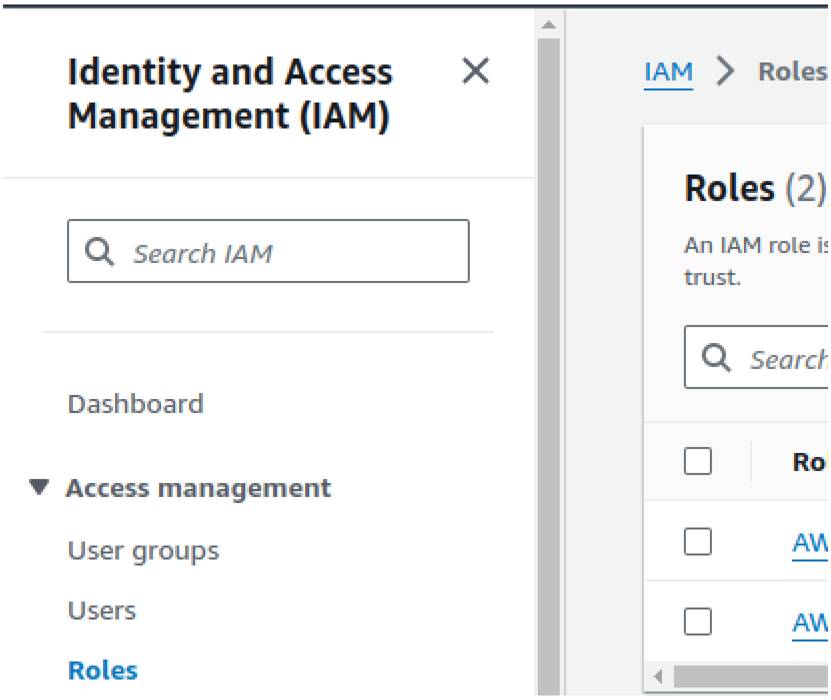


Account ID: 2573-9448-3480

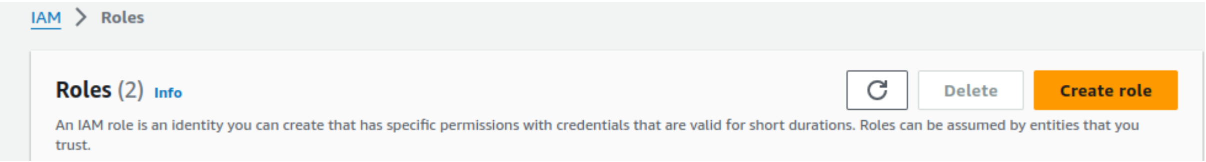
IAM user: test-user

Create Roles

Navigate to Roles in IAM Dashboard

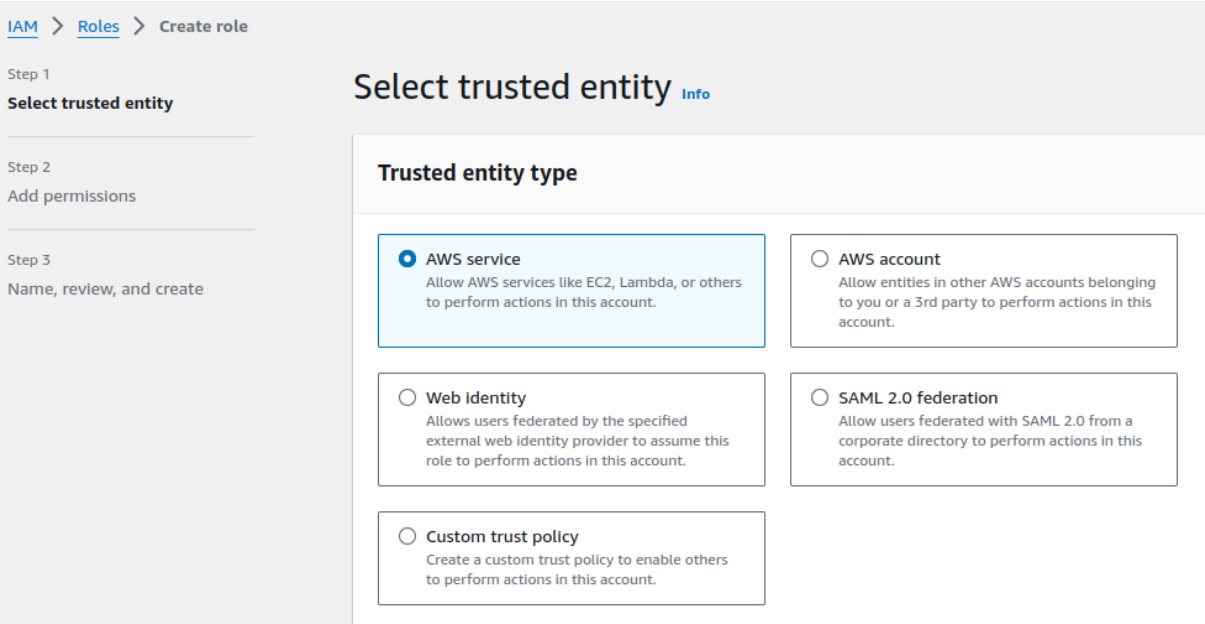


Click on Create Role



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.

Select trusted entity



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

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

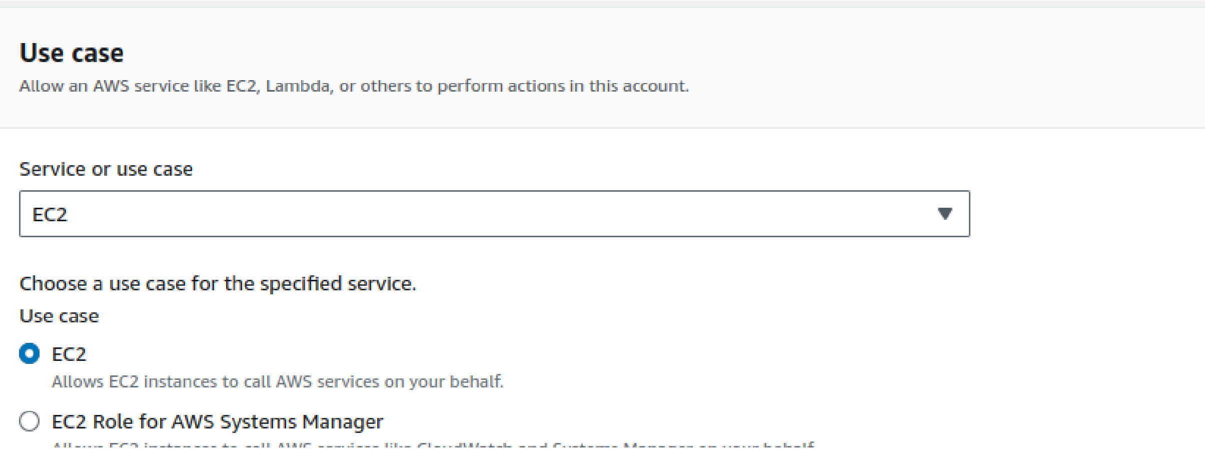
○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ 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.

Enter Service Name



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

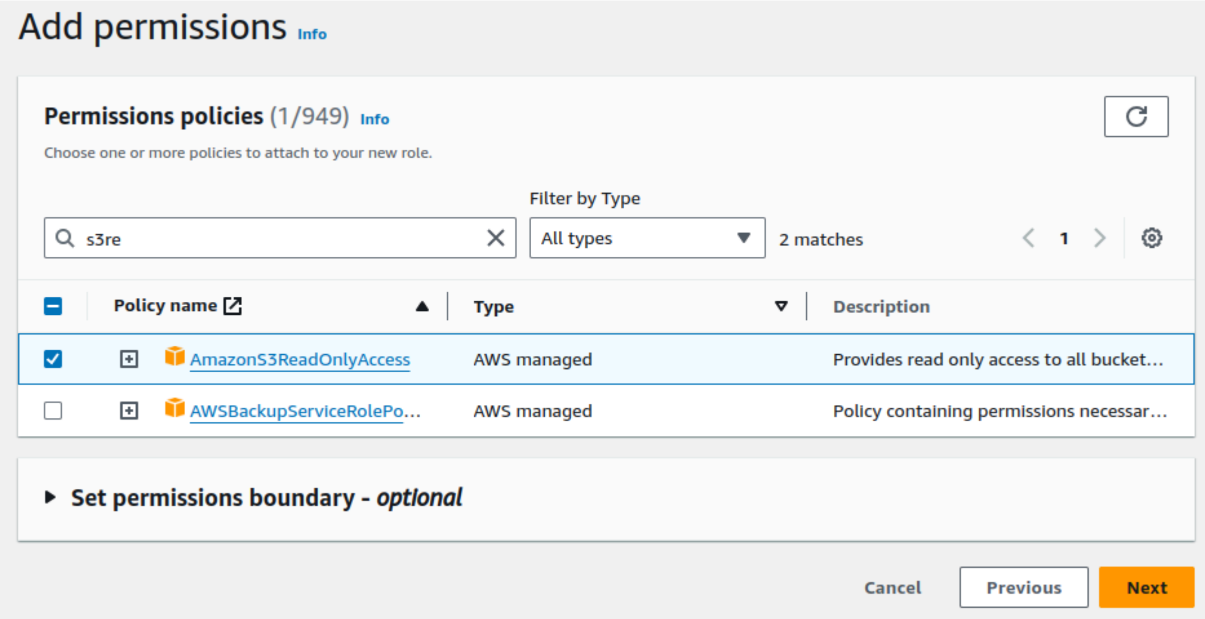
Service or use case
EC2 ▼

Choose a use case for the specified service.
Use case

● EC2
Allows EC2 instances to call AWS services on your behalf.

○ EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

Add Permissions to the role



Add permissions Info

Permissions policies (1/949) Info

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

Filter by Type

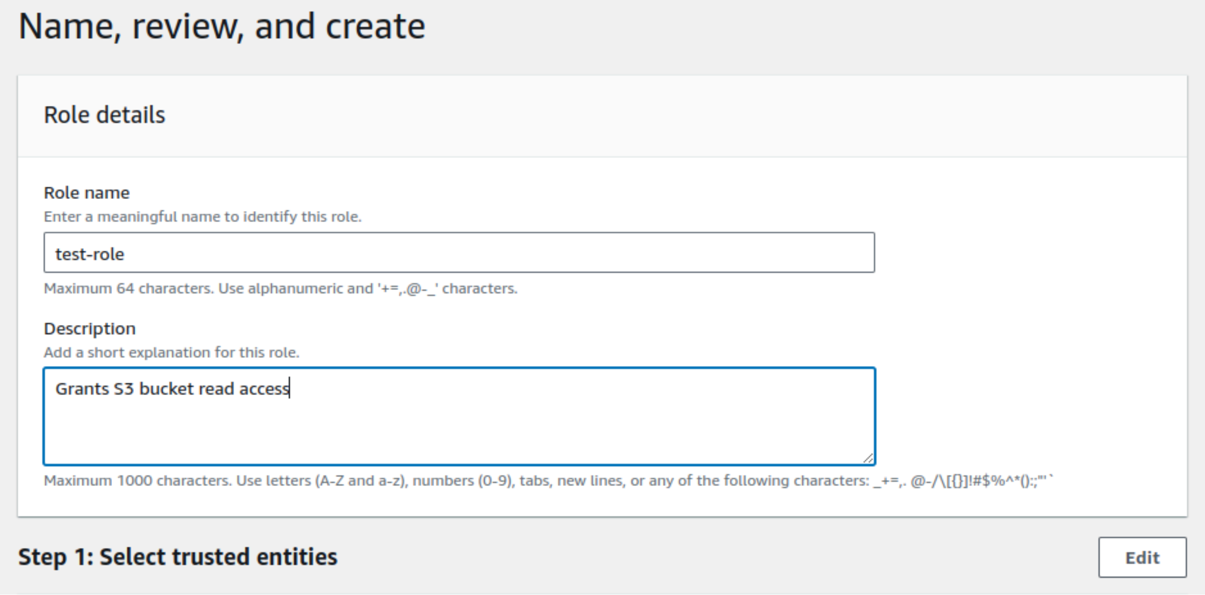
s3re | All types | 2 matches

	Policy name	Type	Description
☑	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all bucket…
□	AWSBackupServiceRolePo…	AWS managed	Policy containing permissions necessar…

▸ **Set permissions boundary - *optional***

Review and Create

Enter name and description



Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

test-role

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description

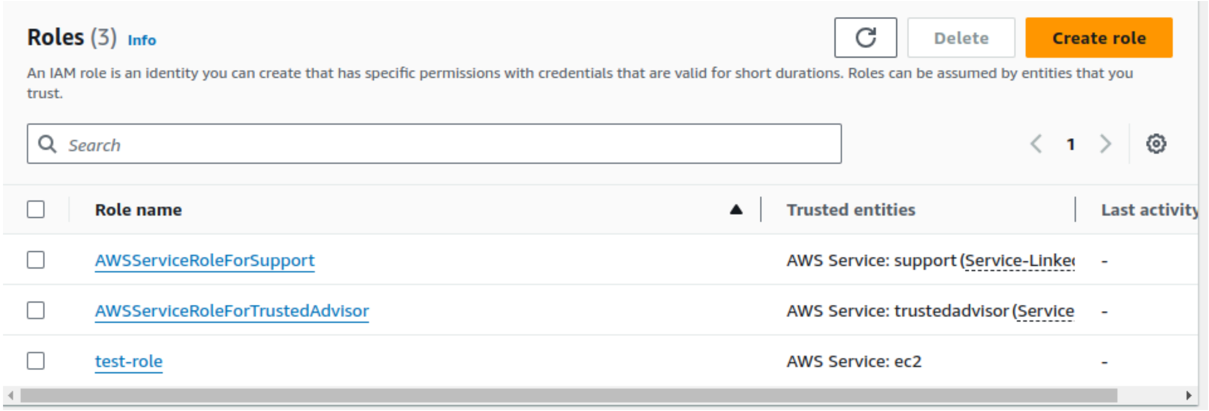
Add a short explanation for this role.

Grants S3 bucket read access

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*():;"'`

Step 1: Select trusted entities

Role Created Successfully



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
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
□	test-role	AWS Service: ec2	-