

SVKM'S NMIM'S Nilkamal School of Mathematics, Applied Statistics & Analytics

Master of Science (Data Science)

Practical-5 Identity Access Management.

Anthea_Gamjya_A022

Date:-11/03/2024

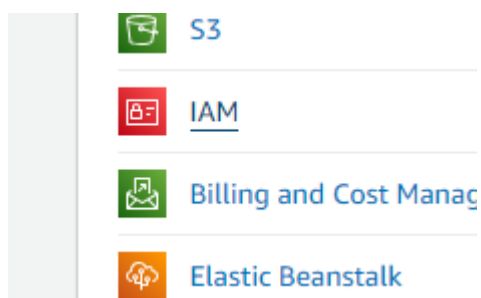
Submission Date:- 18/03/2024

Writeup:-

- Users and groups
- IAM
- Role of IAM

Create and Implement policies IAM user for accessing any 4 services from the aws user and group.

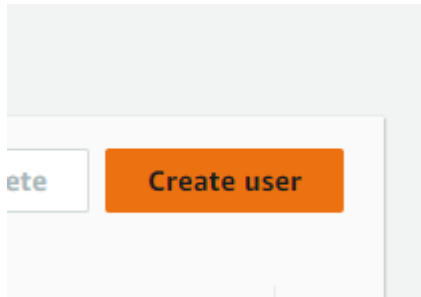
- 1) Select location as Mumbai
- 2) select IAM



User groups

Users

Roles



User name

awsuser

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](#).

☒

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](#)

Cancel

Next

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.

Permissions policies (1/1179)

ec2

×

Filter by Type

All types

40 matches

< 1 2 > ⚙

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonEC2ContainerRegistryFullAccess	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerRegistryPowerUser	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerRegistryReadOnly	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerServiceAutoscaleRole	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerServiceEventsRole	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerServiceforEC2Role	AWS managed	0
<input type="checkbox"/>	AmazonEC2ContainerServiceRole	AWS managed	0
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	AWS managed	2
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS managed	0

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
awsuser

Console password type
None

Require password reset
No

Permissions summary

< 1 >

Name

▲ Type ▼

Used as ▼

No resources

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.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create user

✔ User created successfully

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

View user

IAM > Users

Users (1) Info

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

Refresh

Delete

Create user

Search

< 1 > ⚙

☐

User name

▲

Path

▼

Group:

▼

Last activity

▼

MFA

▼

Password age

▼

Console last sign-in

▼

Access key ID

▼

Active key age

☐

awsuser

/

0

-

-

-

-

-

IAM > Users > awsuser

awsuser Info

Delete

Summary

ARN
 am:aws:iam::339712887637:user/awsuser

Console access
Disabled

Access key 1
[Create access key](#)

Created
March 12, 2024, 07:59 (UTC+05:30)

Last console sign-in
-

Permissions

Groups

Tags

Security credentials

Access Advisor

Permissions policies (0)

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

Refresh

Remove

Add permissions ▼

Search

Filter by Type
All types ▼

< 1 > ⚙

☐

Policy name

▲

Type

▼

Attached via

No resources to display

► Permissions boundary (not set)

▼ Generate policy based on CloudTrail events

PermissionsGroupsTagsSecurity credentialsAccess Advisor

Console sign-in

Enable console access

Console sign-in link

https://339712887637.signin.aws.amazon.com/console

Console password

Not enabled

Multi-factor authentication (MFA) (0)

RemoveResyncAssign MFA device

Device typeIdentifierCertificationsCreated on

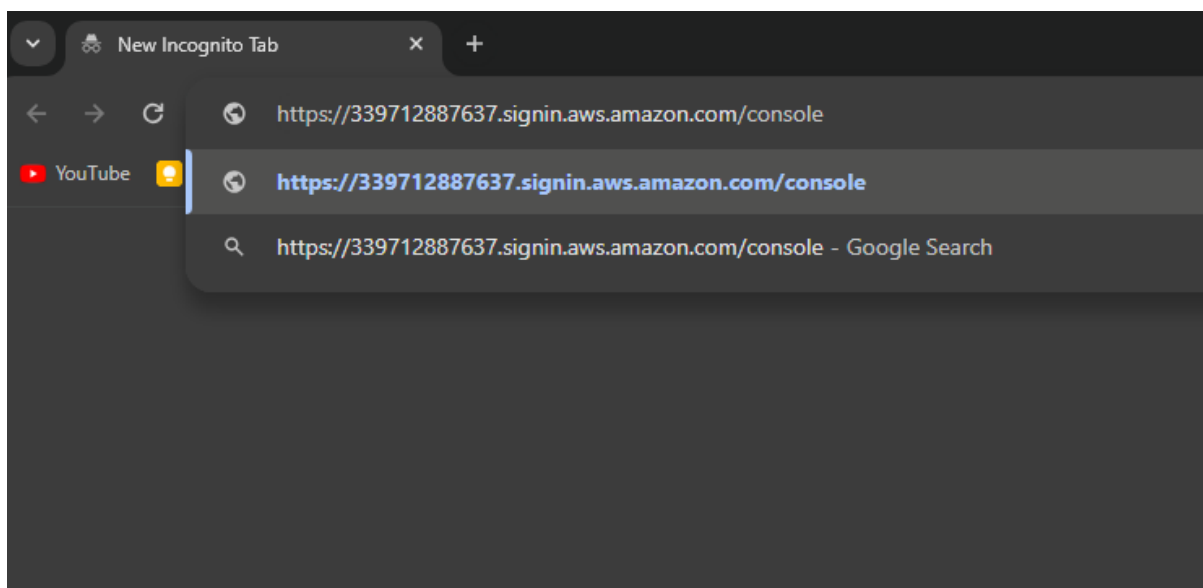
No MFA devices. Assign an MFA device to improve the security of your AWS environment

Assign MFA device

Access keys (0)

Create access key

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)



Previous

Manage console access



Manage awsuser's AWS console access and password.

Console access

- ☒ Enable
- ☐ Disable
Disabling removes the pre-existing password.

Set password

- ☐ Keep existing password
- ☒ Autogenerated password
- ☐ Custom password
- ☒ User must create new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Cancel

Apply

user

Enabled without MFA

Last console sign-in

Secure

amazon.com

(A) (0)

Environment

Identifier


Certifications

08:

MF

Console password


✕




You have successfully enabled the user's new password.

This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.


Console sign-in URL

 <https://339712887637.signin.aws.amazon.com/console>

User name

 awsuser

Console password

 ***** [Show](#)

Download .csv file

Close



Sign in as IAM user

Account ID (12 digits) or account alias

IAM user name

Password

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

A

Lig
to



E

© 2023 Amazon Web Services, Inc. All rights reserved.

AWS account 339712887637

IAM user name awsuser

Old password

New password

Retype new password

Confirm password change

[Sign in using root user email](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2024, Amazon Web Services, Inc. or its affiliates.

anthea@15

Service menu
You can access all AWS services here. There are sections for recently visited and you can save your favorite services too.

Next

Recently visited

No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 RDS Lambda

View all services

Applications (0)

Region: Europe (Stockholm)

eu-north-1 (Current Region)

Find applications

< 1 >

Name	Description	Region	Originating account
Access denied			

Go to myApplications

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

IAM > Policies

Policies (1/1176)

A policy is an object in AWS that defines permissions.

ec2

Filter by Type

All types

40 matches

< 1 2 >

Policy name	Type	Used as	Description
AmazonEC2ContainerRegistryFullAccess	AWS managed	None	Provides administrative access to Ama...
AmazonEC2ContainerRegistryPowerUser	AWS managed	None	Provides full access to Amazon EC2 Co...
AmazonEC2ContainerRegistryReadOnly	AWS managed	None	Provides read-only access to Amazon E...
AmazonEC2ContainerServiceAutoscaleRole	AWS managed	None	Policy to enable Task Autoscaling for A...
AmazonEC2ContainerServiceEventsRole	AWS managed	None	Policy to enable CloudWatch Events fo...

us-east-1console.aws.amazon.com/iam/home?region=ap-south-1#/policies/create

ServicesSearch[Alt+S]

GlobalAnthea

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions

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

Policy editor

VisualJSONActions

▼ EC2

AllowAll actions

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

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Manual actions | Add actions

☒ All EC2 actions (ec2:*)

Access level

► List (Selected 172/172)

► Read (Selected 35/35)

► Write (Selected 417/417)

► Permissions management (Selected 5/5)

Effect

☒ Allow ☐ Deny

Expand all | Collapse all

ec2:DescribeLaunchTemplateVersions 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.

+ Add more permissions

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

CancelNext

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

aws

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

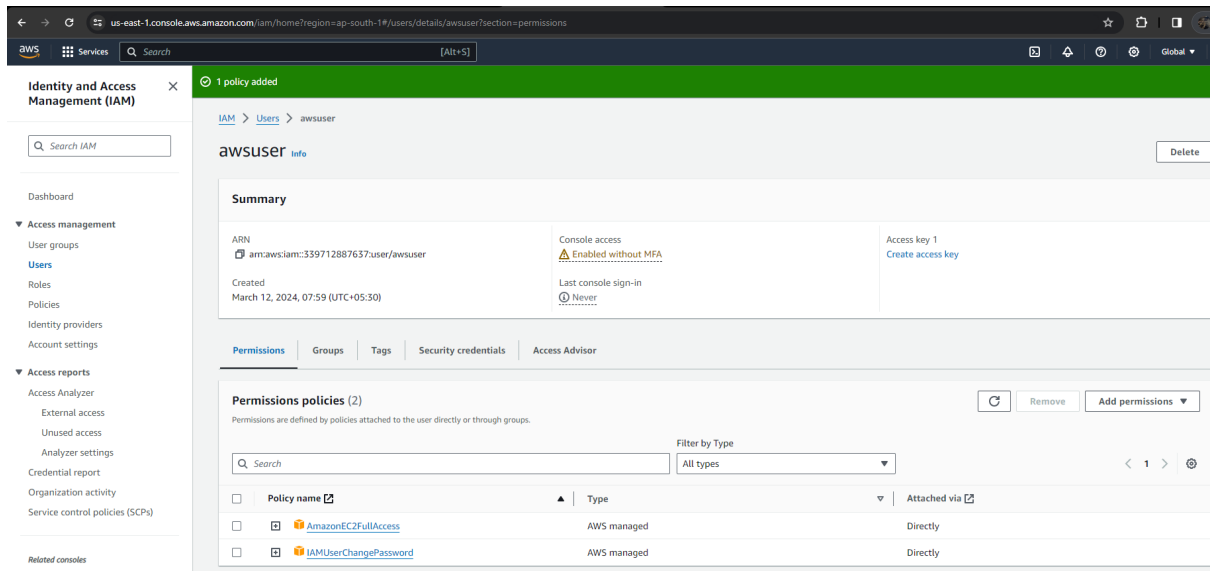
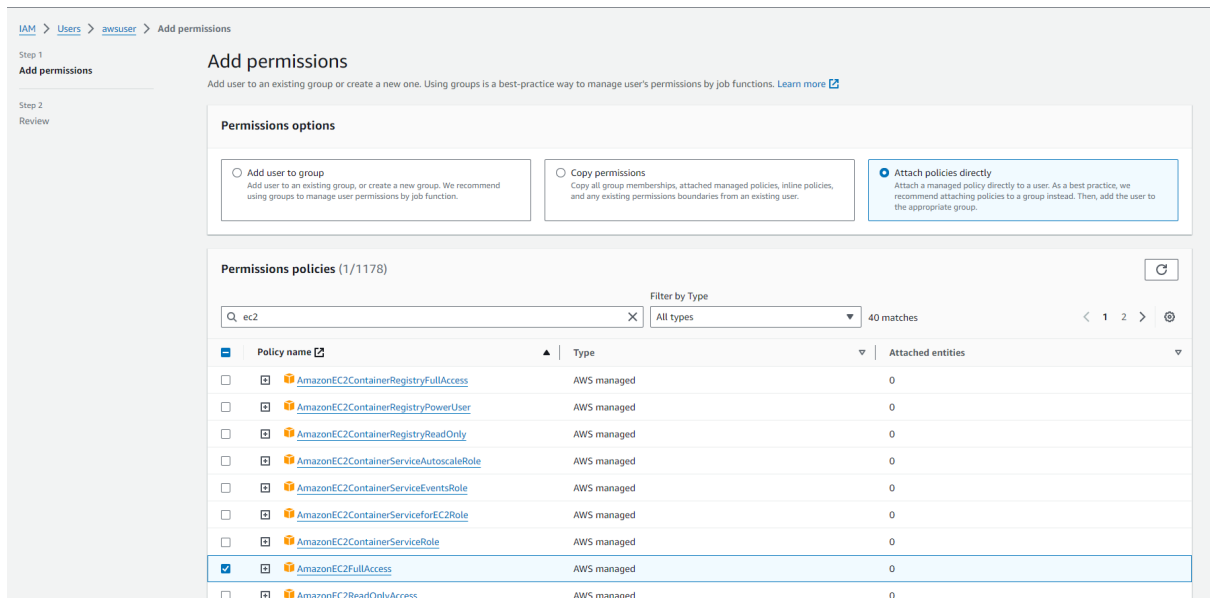
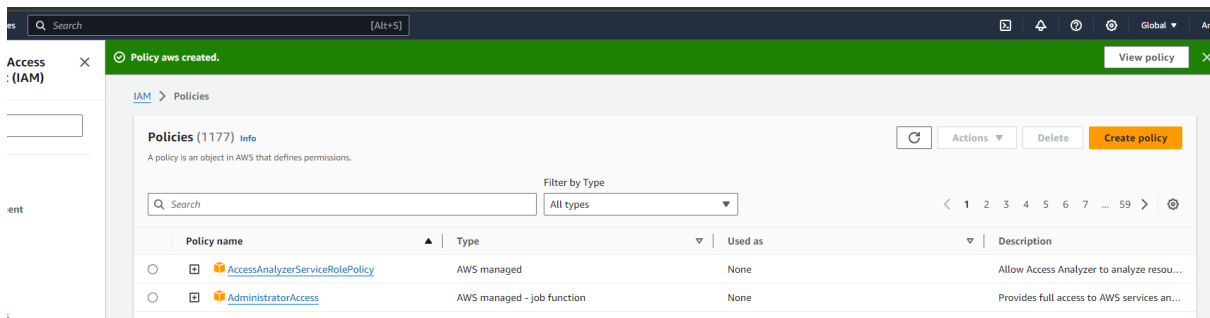
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

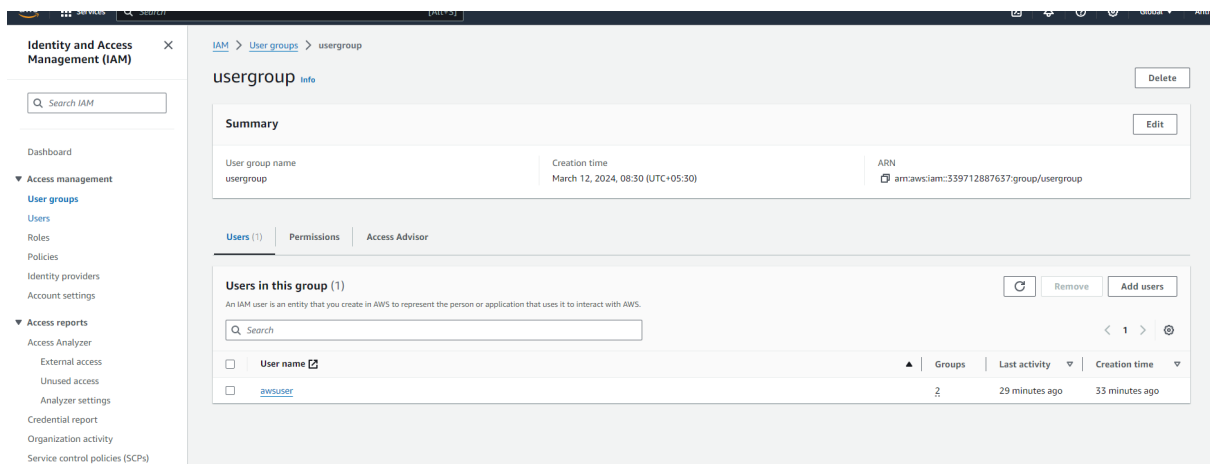
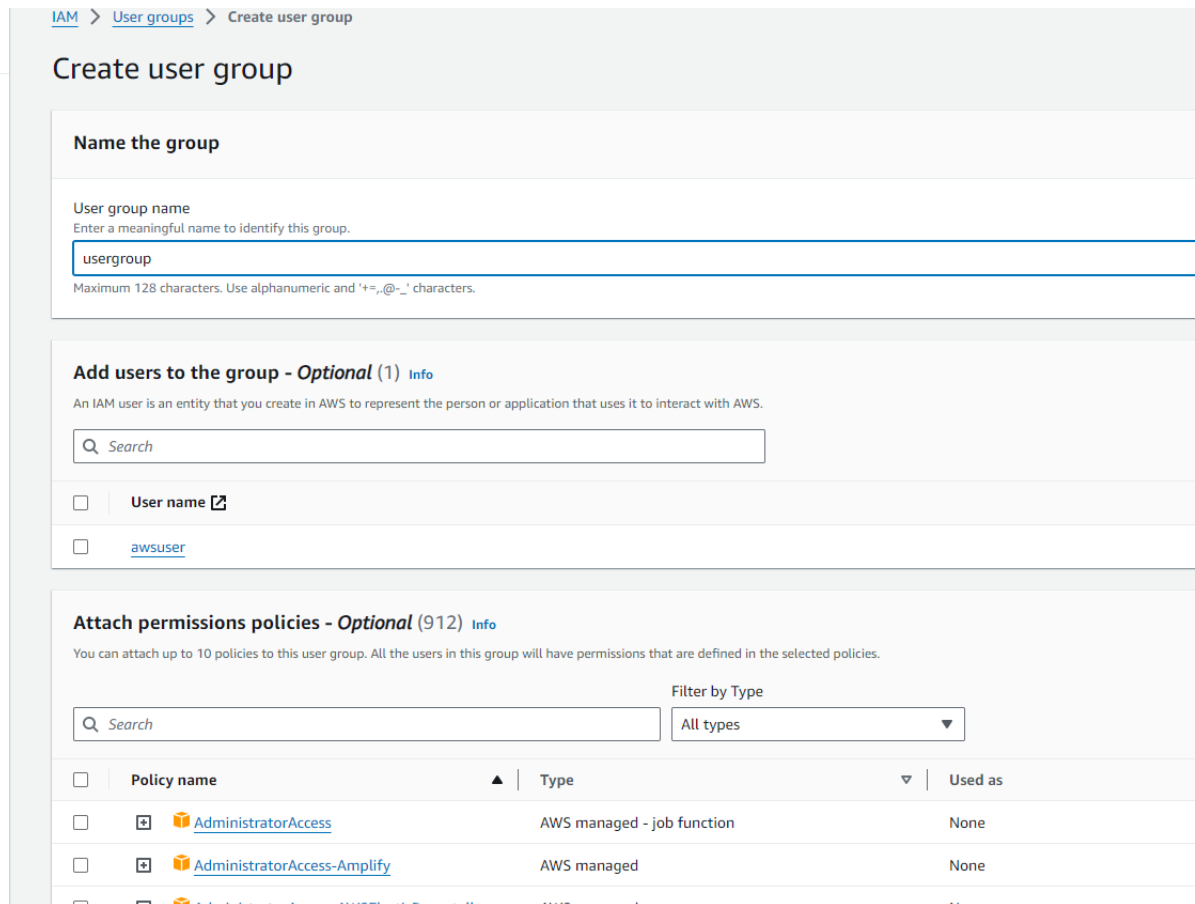
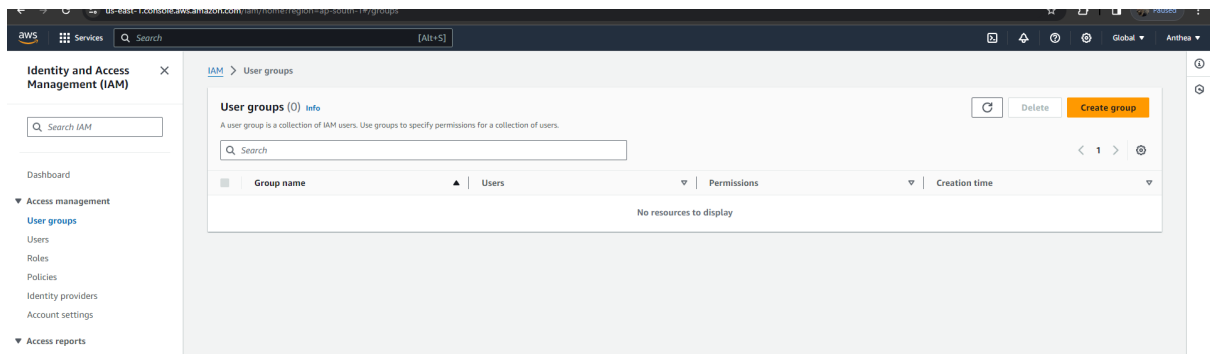
Allow (1 of 404 services)

Show remaining

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














Creating groups



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

All

<input type="checkbox"/>	<input type="checkbox"/>	Policy name	Type
<input type="checkbox"/>	<input type="checkbox"/>	 AmazonEC2ContainerRegistryFullAccess	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	 AmazonEC2ContainerRegistryPowerUser	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	 AmazonEC2ContainerRegistryReadOnly	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	 AmazonEC2ContainerServiceAutoscaleRole	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	 AmazonEC2ContainerServiceEventsRole	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	 AmazonEC2ContainerServiceforEC2Role	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	 AmazonEC2ContainerServiceRole	AWS managed
<input checked="" type="checkbox"/>	<input type="checkbox"/>	 AmazonEC2FullAccess	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	 AmazonEC2ReadOnlyAccess	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	 AmazonEC2RoleforAWSCodeDeploy	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	 AmazonEC2RoleforAWSCodeDeployLimited	AWS managed