

## IAM

What is Access Management?

Access Management: Each and every user/role will have specific rights assigned which is done by policies which are in turn given by admins

IAM is a service using which I can securely control access to AWS resources(authentication) for your users(authorization)

Components of IAM:

Users	Groups	Roles	Policies
The acc that you have created is the root acc	To group people with identical rights and access	Roles are assigned to applications, users to people	A document that explicitly lists the permissions you want to assign to a user, group, role etc
Access type is of 2 types: Programmatic access and AWS Management Console access		Defines a set of permissions for making AWS service requests	Policy is written in a json file via a code
Programmatic access- interaction with AWS APIs using different development tools, you get access keys		Roles can be assigned to any AWS service, has to be attached to a zero instance	If you add allow and deny policies both, it will prefer the one with the least number of permissions allowed
Access key ID: generated, can be viewed Secret Access Key: can only be viewed at the time of the creation of the user, so save it		Example: ec2 instance is now configured to interact with s3 in a particular acc, any application deployed in the given ec2 instance will be able to interact w S3	
Different login page for IAM users			

Created different users:

IAM > Users

Users (7) Info

Delete

Create user

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

Q Search

< 1 > ⚙

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
<a href="#">advDev</a>	/	1	✔ 13 days ago	-	✔ 13 days	June 06, 2024, 15:20 (...)
<a href="#">advika_admin</a>	/	0	✔ 5 days ago	-	✔ 13 days	June 06, 2024, 14:49 (...)
<a href="#">backdev</a>	/	0	✔ 13 days ago	-	✔ 13 days	June 06, 2024, 16:15 (...)
<a href="#">dev2</a>	/	1	✔ 13 days ago	-	✔ 13 days	June 06, 2024, 15:30 (...)
<a href="#">dev32</a>	/	2	✔ 13 days ago	-	✔ 13 days	June 06, 2024, 15:15 (...)
<a href="#">iam_dev1</a>	/	1	-	-	✔ 13 days	-
<a href="#">tf_admin</a>	/	0	✔ 5 hours ago	-	✔ 7 hours	-

For better security, it is recommended to not create access keys for users

Created 2 User Groups: groupA and groupM

IAM > User groups > groupA

groupA Info

Delete

Summary

Edit

User group name

groupA

Creation time

June 06, 2024, 15:15 (UTC+05:30)

ARN

arn:aws:iam::975050162722:group/groupA

Users (3)

Permissions

Access Advisor

Users in this group (3)

Remove

Add users

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

Q Search

< 1 > ⚙

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	<a href="#">dev2</a>	1	13 days ago	13 days ago
<input type="checkbox"/>	<a href="#">dev32</a>	2	13 days ago	13 days ago
<input type="checkbox"/>	<a href="#">iam_dev1</a>	1	None	13 days ago

Attached policies by groups, both AWS created and self-created:

groupA

Info

Delete

Summary

Edit

User group name

groupA

Creation time

June 06, 2024, 15:15 (UTC+05:30)

ARN

arn:aws:iam::975050162722:group/groupA

Users (3)

Permissions

Access Advisor

Permissions policies (4)

Info

Refresh

Simulate

Remove

Add permissions

You can attach up to 10 managed policies.





Search

Filter by Type

All types

< 1 >

Settings

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	 <a href="#">AmazonEC2FullAccess</a>	AWS managed	1
<input type="checkbox"/>	 <a href="#">AmazonS3FullAccess</a>	AWS managed	5
<input type="checkbox"/>	 <a href="#">deny_sns</a>	Customer managed	1
<input type="checkbox"/>	 <a href="#">game_allow</a>	Customer managed	1

Created IAM Roles:

IAM > Roles > ec2\_IAM\_role

ec2\_IAM\_role

Info

Delete

Allows EC2 instances to call AWS services on your behalf.

Summary

Edit

Creation date

June 06, 2024, 16:21 (UTC+05:30)

ARN

arn:aws:iam::975050162722:role/ec2\_IAM\_role

Link to switch roles in console

https://signin.aws.amazon.com/switchrole?roleName=ec2\_IAM\_role&account=975050162722

Instance profile ARN

arn:aws:iam::975050162722:instance-profile/ec2\_IAM\_role

Last activity

-

Maximum session duration

1 hour

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Permissions policies (1)

Info

Refresh

Simulate

Remove

Add permissions

You can attach up to 10 managed policies.


Search

Filter by Type

All types

< 1 >

Settings

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	 <a href="#">AmazonS3FullAccess</a>	AWS managed	5

[IAM](#) > [Roles](#) > ECR\_calls\_ECS\_try

# ECR\_calls\_ECS\_try

Info

Delete

Allows ECS tasks to call AWS services on your behalf.

Summary

Edit

Creation date

June 14, 2024, 15:10 (UTC+05:30)

ARN

arn:aws:iam::975050162722:role/ECR\_calls\_ECS\_try

Last activity

5 days ago

Maximum session duration

1 hour

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Permissions policies (2)

Info

Refresh

Simulate

Remove

Add permissions



You can attach up to 10 managed policies.

Search

Filter by Type

All types

< 1 > Settings

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	 <a href="#">AmazonECS_FullAccess</a>	AWS managed	1
<input type="checkbox"/>	 <a href="#">AmazonECSTaskExecutionRolePolicy</a>	AWS managed	1

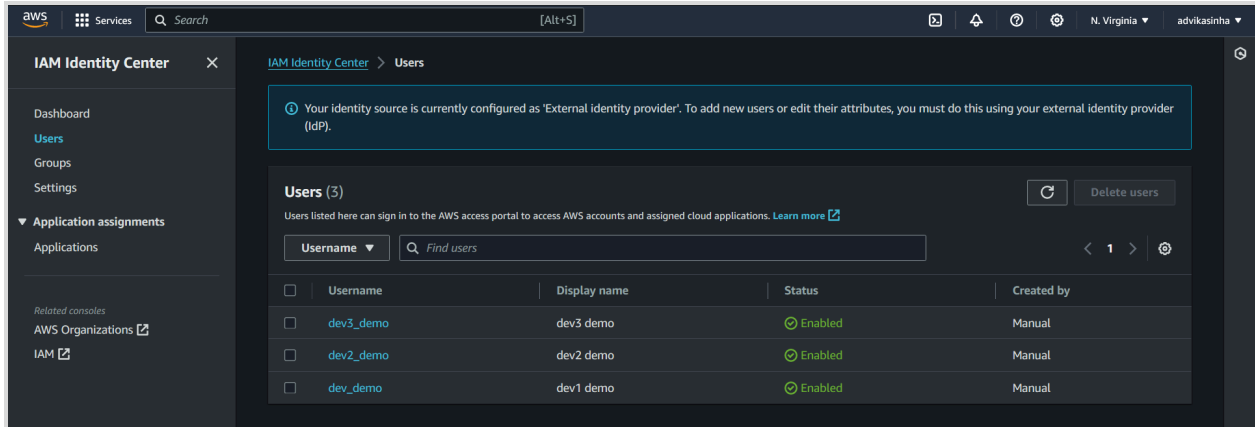
Encountered an API error in EC2 resources since I granted it permissions for S3:  
You are not authorized to perform this operation. not authorized to perform because no identity-based policy allows the ec2:DescribeAddresses action

## IAM IDENTITY CENTER USER:

Not tied to a single AWS account and they gain access to AWS accounts by assuming an IAM role in the chosen AWS account

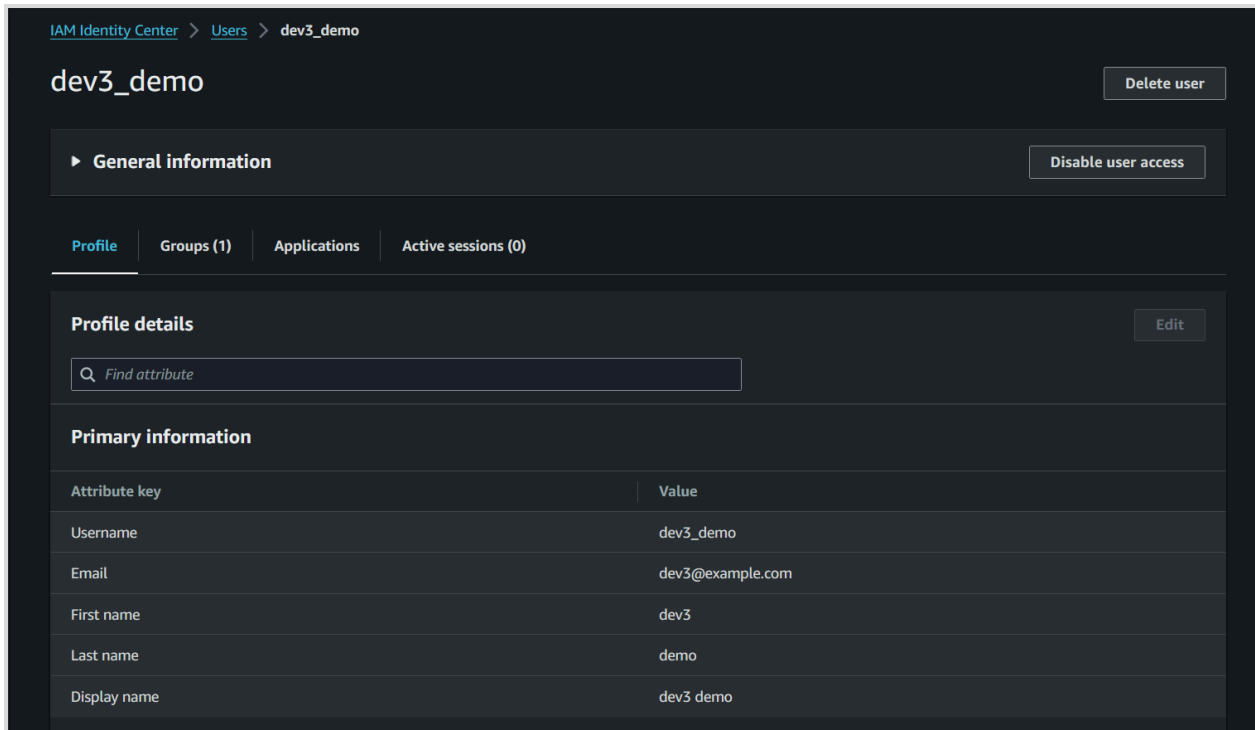
Identity center defined for IAM to specify user details

### Manually created IAM Users and Groups using the IAM Identity Center



The screenshot shows the AWS IAM Identity Center console. The left sidebar contains navigation links: Dashboard, Users, Groups, Settings, Application assignments, and Applications. The main content area is titled 'IAM Identity Center > Users'. A blue notification box states: 'Your identity source is currently configured as "External identity provider". To add new users or edit their attributes, you must do this using your external identity provider (IdP)'. Below this, a section titled 'Users (3)' shows a list of users. A search bar with the placeholder 'Find users' is present. The user list has columns for Username, Display name, Status, and Created by. The users listed are dev3\_demo, dev2\_demo, and dev1\_demo, all with a status of 'Enabled' and created manually.

Username	Display name	Status	Created by
dev3_demo	dev3 demo	Enabled	Manual
dev2_demo	dev2 demo	Enabled	Manual
dev1_demo	dev1 demo	Enabled	Manual




The screenshot shows the details page for a user named 'dev3\_demo' in the AWS IAM Identity Center console. The breadcrumb trail is 'IAM Identity Center > Users > dev3\_demo'. The page title is 'dev3\_demo'. There are buttons for 'Delete user' and 'Disable user access'. The 'General information' section is expanded. Below it, there are tabs for 'Profile', 'Groups (1)', 'Applications', and 'Active sessions (0)'. The 'Profile details' section is active, showing a search bar for attributes. The 'Primary information' section displays a table of user attributes.

Attribute key	Value
Username	dev3_demo
Email	dev3@example.com
First name	dev3
Last name	demo
Display name	dev3 demo

# Making Groups of Users

[IAM Identity Center](#) > [Groups](#) > [dev\\_demo\\_group](#)



Did you know?

You can assign permissions to a group through either the [AWS accounts](#) link or the [Applications](#) link in the navigation pane. [Learn more](#)

dev\_demo\_group

Delete group

▶ General Information

UsersApplications

Users in this group (3)

Remove users from group

Workforce users in this group inherit permissions to the AWS accounts and Identity Center enabled applications that are assigned to this group.

Find users by username or display name

Q Search for users in this group

< 1 > ⚙

<input type="checkbox"/>	Username ▲	Display name ▼	Status ▼	Email ▼
<input type="checkbox"/>	dev_demo	dev1 demo	✔ Enabled	dev@example.com
<input type="checkbox"/>	dev2_demo	dev2 demo	✔ Enabled	dev2@example.com
<input type="checkbox"/>	dev3_demo	dev3 demo	✔ Enabled	dev3@example.com