

Amazon-IAM: IAM Users Task-1

Problem Statement:

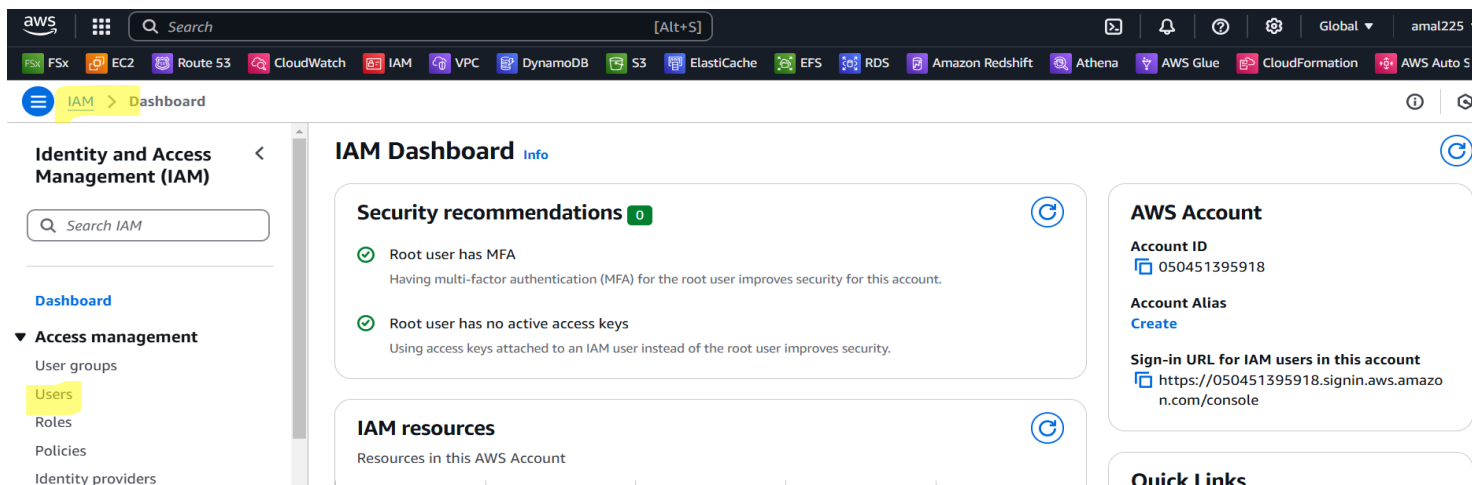
You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks To Be Performed:

1. Create 4 IAM users named “Dev1”, “Dev2”, “Test1”, and “Test2”.
2. Create 2 groups named “Dev Team” and “Ops Team”.
3. Add Dev1 and Dev2 to the Dev Team.
4. Add Dev1, Test1 and Test2 to the Ops Team.

Solution:

1. Create 4 IAM users named “Dev1”, “Dev2”, “Test1”, and “Test2”, Go to IAM Dashboard and click user and create user .



aws [Alt+S] Global amal225

FSx EC2 Route 53 CloudWatch IAM VPC DynamoDB S3 ElastiCache EFS RDS Amazon Redshift Athena AWS Glue CloudFormation AWS Auto Scaling

IAM > Users

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies

Users (1) Info

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

Search

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age	Console last
<input type="checkbox"/>	vim	/	0	-	-	-	-

IAM > Users > Create user

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Specify user details

User details

User name

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.

Info 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

aws [Alt+S] Global amal225

FSx EC2 Route 53 CloudWatch IAM VPC DynamoDB S3 ElastiCache EFS RDS Amazon Redshift Athena AWS Glue CloudFormation AWS Auto Scaling

IAM > Users > Create user

Step 4 Retrieve password

Dev1

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

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.

i 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

IAM > Users > Create user

- Step 1
- Specify user details
- Step 2
- Set permissions**
- Step 3
- Review and create
- Step 4
- Retrieve password

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.

i 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](#)

Create group

► Set permissions boundary - optional

Cancel

Previous

Next

User name
Dev1

Console password type
Custom password

Require password reset
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.

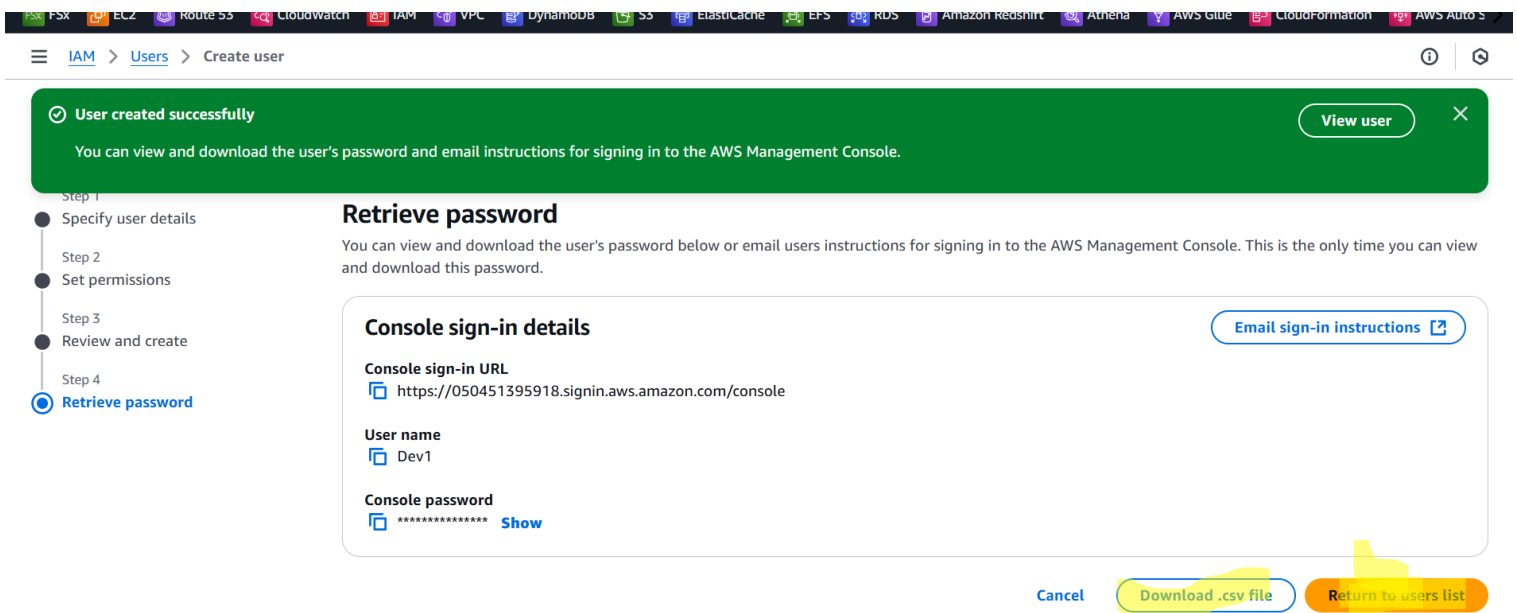
Add new tag

You can add up to 50 more tags.

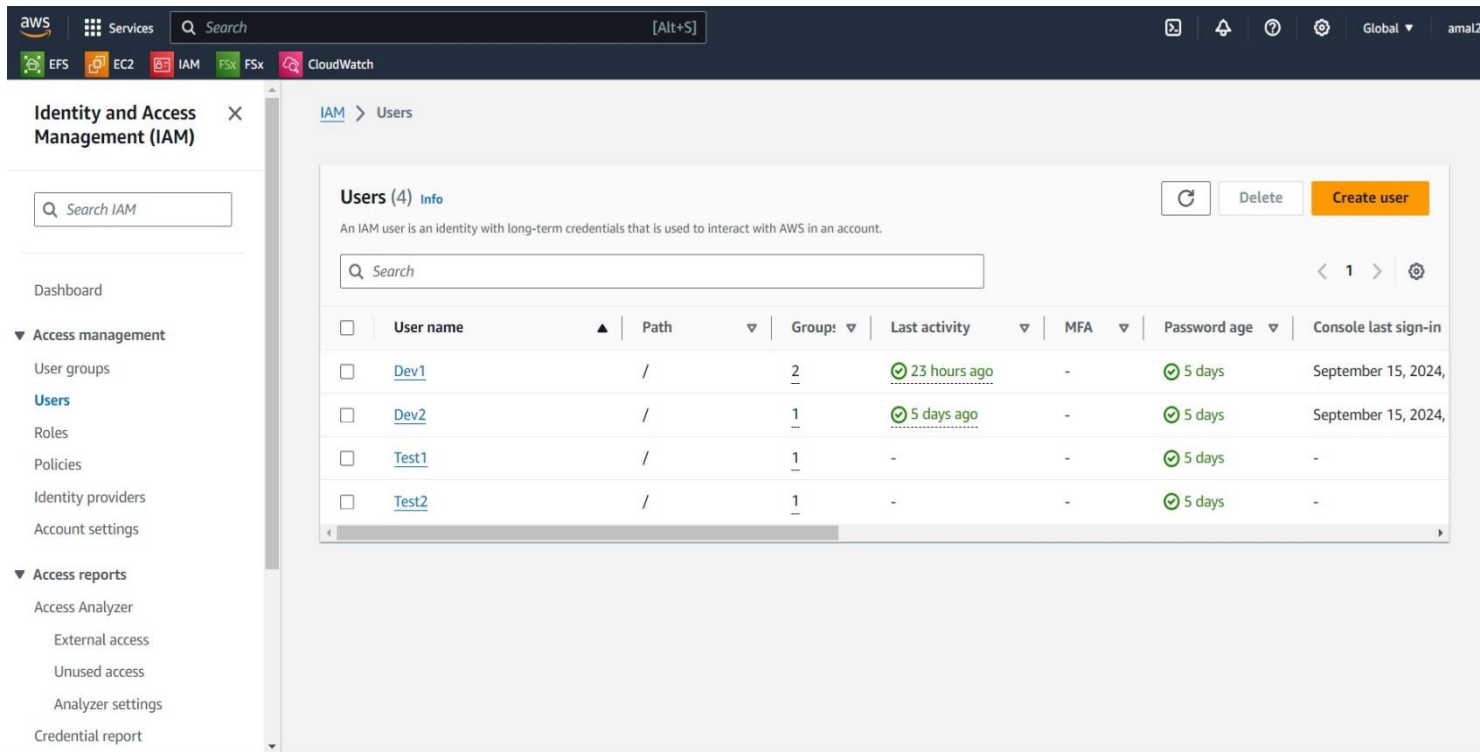
Cancel

Previous

Create user



- Download the password and all user Dve2, Test1,Test2 create as it is , download the password for login . look at given below I have created all user same as it .



2. Create 2 groups named “Dev Team” and “Ops Team”

- In IAM dashboard ,go to Group and click create group, and provide group name and , create user group.

The first screenshot shows the 'User groups (0)' page in the AWS IAM console. The left sidebar contains the 'Identity and Access Management (IAM)' menu with 'User groups' highlighted. The main content area shows a table with columns: Group name, Users, Permissions, and Creation time. The table is empty, displaying 'No resources to display'. Buttons for 'Delete' and 'Create group' are visible in the top right.

The second screenshot shows the 'Create user group' page. The 'Name the group' section has a text input field containing 'Dev-Team'. Below it, the 'Add users to the group - Optional (2)' section is visible, showing a search bar and a list of AWS managed policies.

The third screenshot shows the list of AWS managed policies available for selection. The policies listed are:

Policy Name	Managed By	Permissions	Description
AmazonAPIGatewayFullAccess	AWS managed	None	Allows API Gateway to push logs to us...
AmazonAppFlowFullAccess	AWS managed	None	Provides full access to Amazon AppFlo...
AmazonAppFlowReadOnlyAccess	AWS managed	None	Provides read only access to Amazon A...
AmazonAppStreamFullAccess	AWS managed	None	Provides full access to Amazon AppStr...
AmazonAppStreamReadOnlyAccess	AWS managed	None	Amazon AppStream 2.0 access to AWS...

Buttons for 'Cancel' and 'Create user group' are at the bottom right.

The fourth screenshot shows the 'User groups (1)' page after the 'Dev-Team' group has been created. A green notification banner at the top says 'Dev-Team user group created.' with a 'View group' button. The table now contains one entry:

Group name	Users	Permissions	Creation time
Dev-Team	0	Not defined	Now

- Ops-Team create same as it ,same process we can follow it.

aws [Search] [Alt+S] Global amal225

FSx EC2 Route 53 CloudWatch IAM VPC DynamoDB S3 ElastiCache EFS RDS Amazon Redshift Athena AWS Glue CloudFormation AWS Auto Scal

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Ops-Team user group created. View group

User groups (2) Info

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

Search

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	Dev-Team	0	Not defined	2 minutes ago
<input type="checkbox"/>	Ops-Team	0	Not defined	Now

3. Add Dev1 and Dev2 to the Dev Team.

- Go to User Group and click Dev-Team, into Dev-Team ,click add user and select Dev1,Dev2, and click add users.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

User groups (2) Info

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

Search

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	Dev-Team	0	Not defined	18 minutes ago
<input type="checkbox"/>	Ops-Team	0	Not defined	15 minutes ago

Route 53 CloudWatch IAM VPC DynamoDB S3 ElastiCache EFS RDS Amazon Redshift Athena AWS Glue CloudFormation AWS Auto S

er groups > Dev-Team

Dev-Team Info

Summary

User group name: Dev-Team

Creation time: December 06, 2024, 11:45 (UTC+05:30)

ARN: arn:aws:iam::050451395918:group/Dev-Team

Users Permissions Last Accessed

Users in this group (0)

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

Add users

Add users to Dev-Team [Info](#)

Other users in this account (2/5)

< 1 >

⚙️

<input type="checkbox"/>	User name 🔗	▲	Groups	Last activity ▼	Creation time ▼
<input checked="" type="checkbox"/>	Dev1		0	None	33 minutes ago
<input checked="" type="checkbox"/>	Dev2		0	None	14 minutes ago
<input type="checkbox"/>	Test1		0	None	13 minutes ago
<input type="checkbox"/>	Test2		0	None	12 minutes ago
<input type="checkbox"/>	vim		0	None	15 days ago

[Cancel](#) [Add users](#)

and Access
ent (IAM)

IAM

agement

iders

ngs

management [New](#)

orts

zer

ress

Summary

[Edit](#)**User group name**
Dev-Team**Creation time**
December 06, 2024, 11:45 (UTC+05:30)**ARN**
[arn:aws:iam::050451395918:group/Dev-Team](#)Users
(2)

Permissions

Last Accessed

Users in this group (2)

[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.

< 1 >

⚙️

1. Add Dev1, Test1 and Test2 to the Ops Team.

Same as it add user in Ops-Team .follow same process.

 3 users added to this group. [✕](#)Users
(3)

Permissions

Last Accessed

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.

< 1 >

⚙️

[New](#)[View](#)