Amazon-IAM: IAM Users Task-1

Problem Statement:

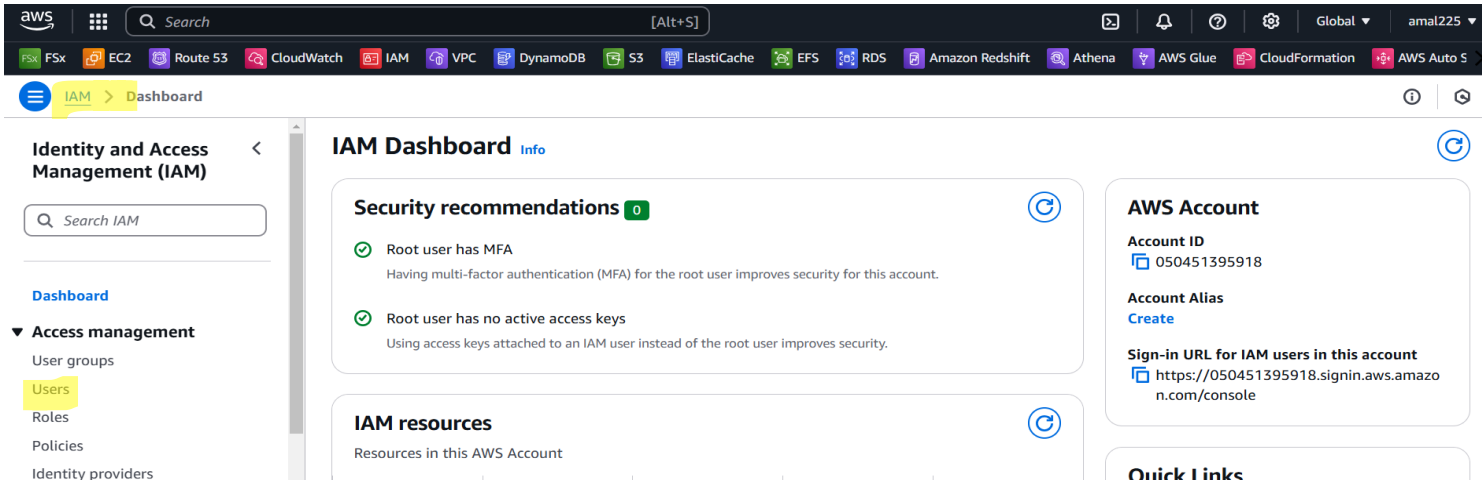
You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

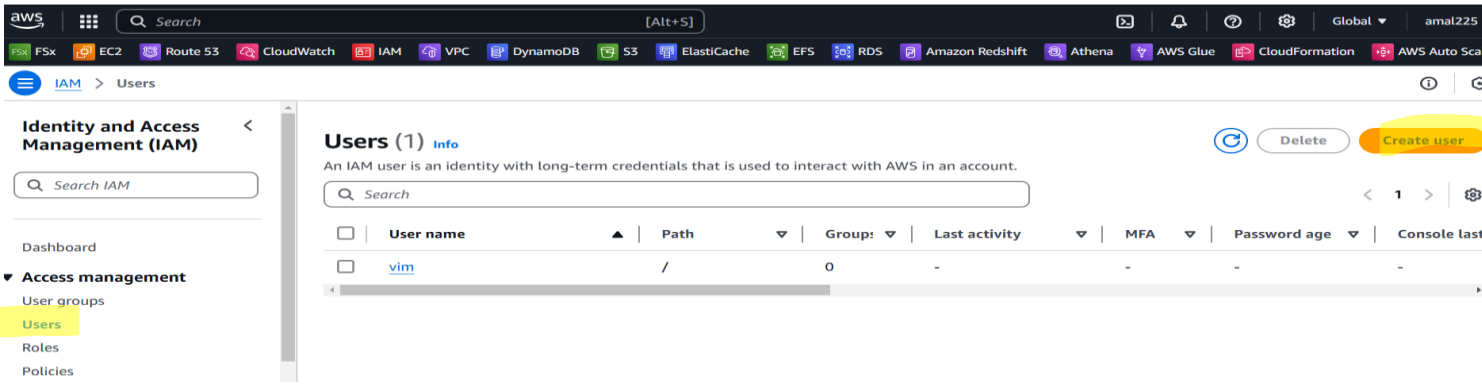
Tasks To Be Performed:

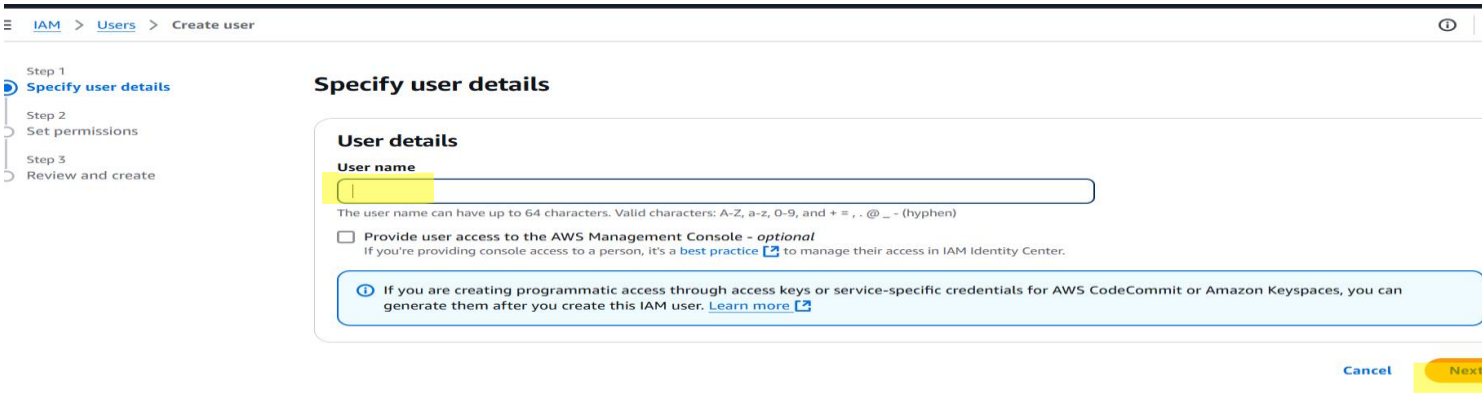
1. Create 4 IAM users named “Dev1”, “Dev2”, “Test1”, and “Test2”.
2. Create 2 groups named “Dev Team” and “Ops Team”.
3. Add Dev1 and Dev2 to the Dev Team.
4. Add Dev1, Test1 and Test2 to the Ops Team.

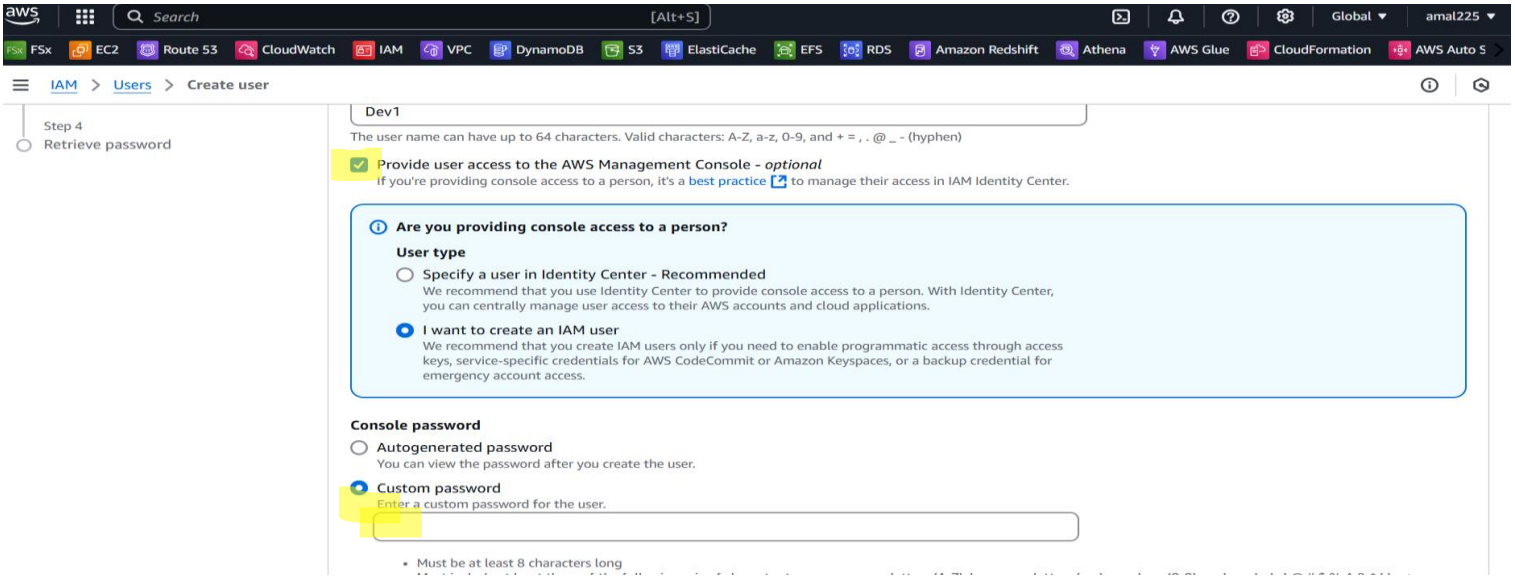
Solution:

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




Search
[Alt+S]
Global
amal225
FSx
EC2
Route 53
CloudWatch
IAM
VPC
DynamoDB
S3
ElastiCache
EFS
RDS
Amazon Redshift
Athena
AWS Glue
CloudFormation
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.
Delete
Create user
Search
User name
Path
Group:
Last activity
MFA
Password age
Console last
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.
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


Search
[Alt+S]
Global
amal225
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.

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.

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	Console password type	Require password reset
Dev1	Custom password	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.

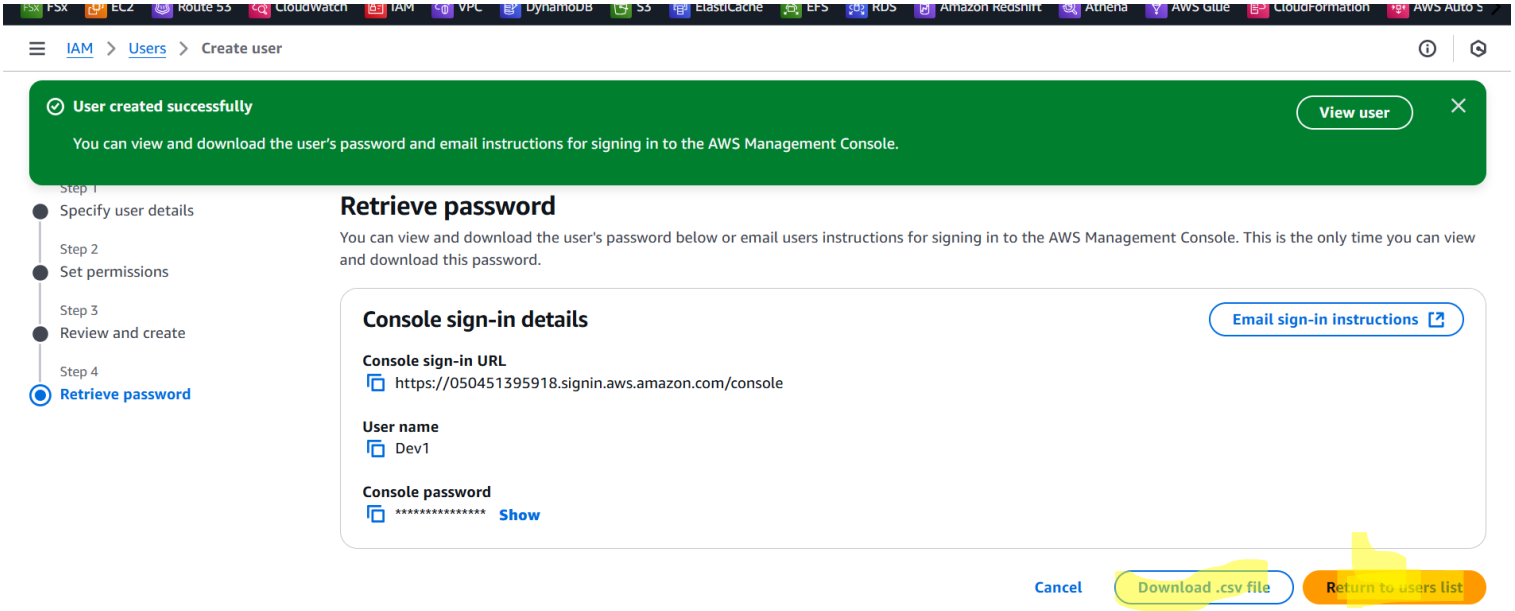
No tags associated with the resource.

Add new tag

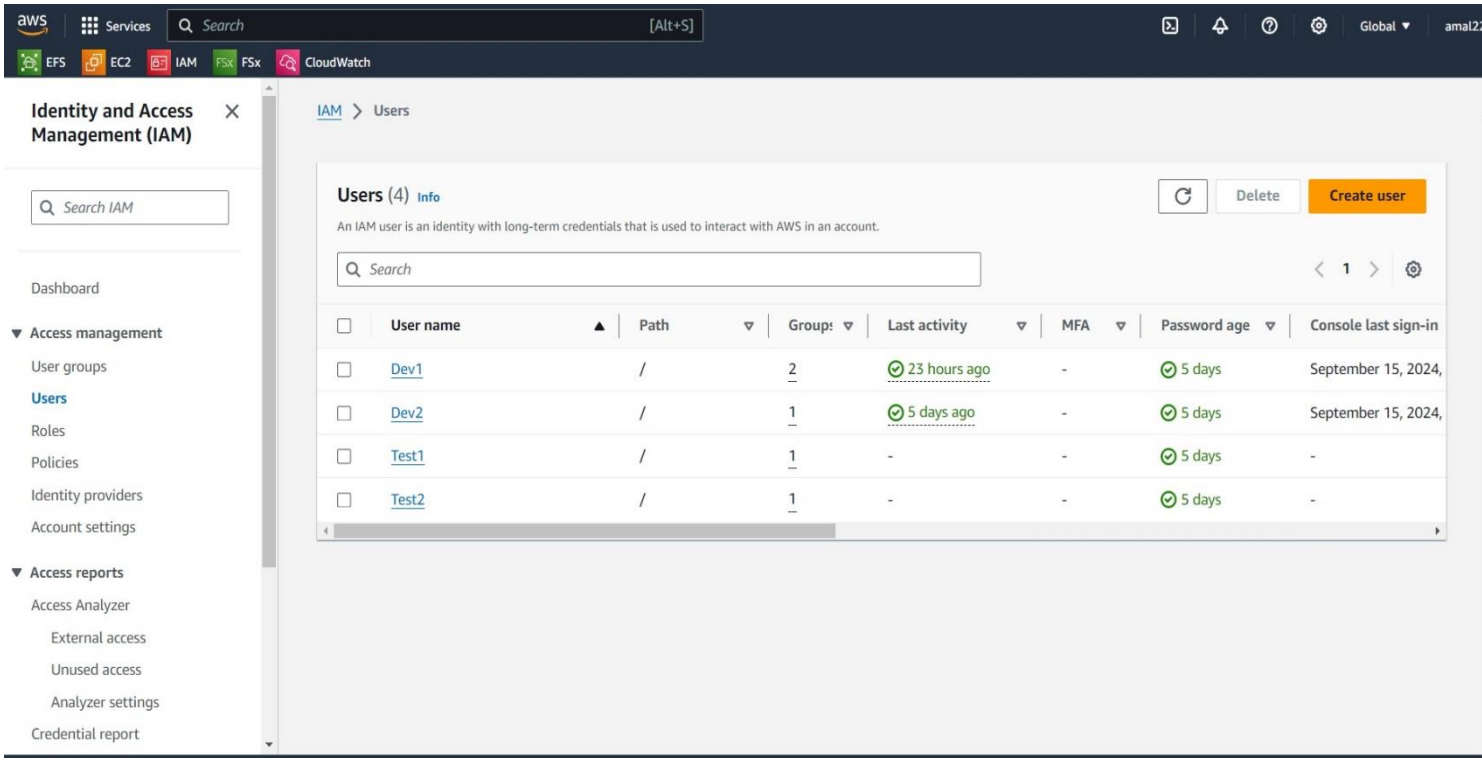
You can add up to 50 more tags.

Cancel Previous Create user

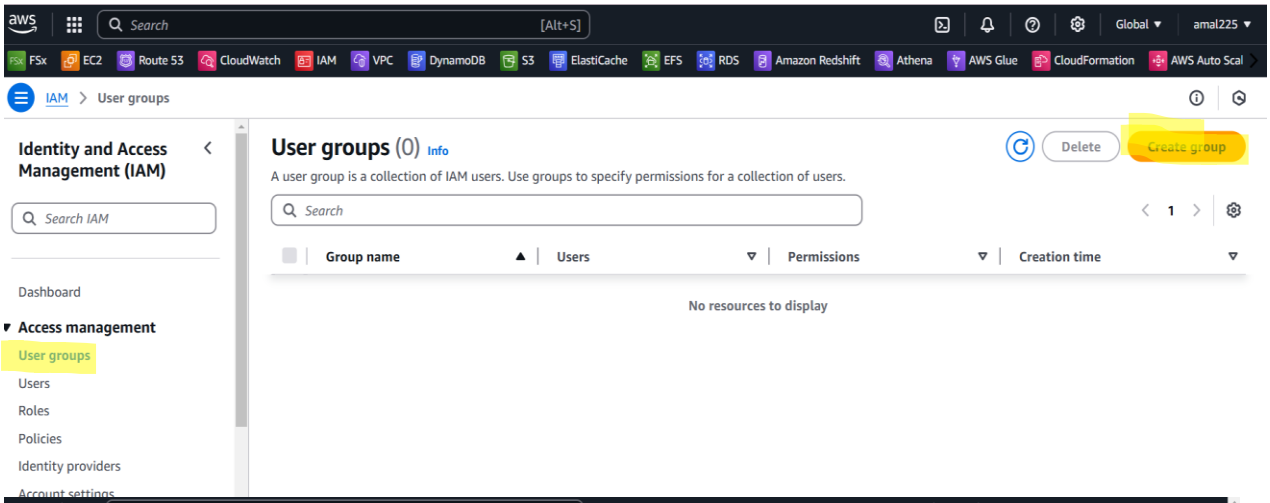
-

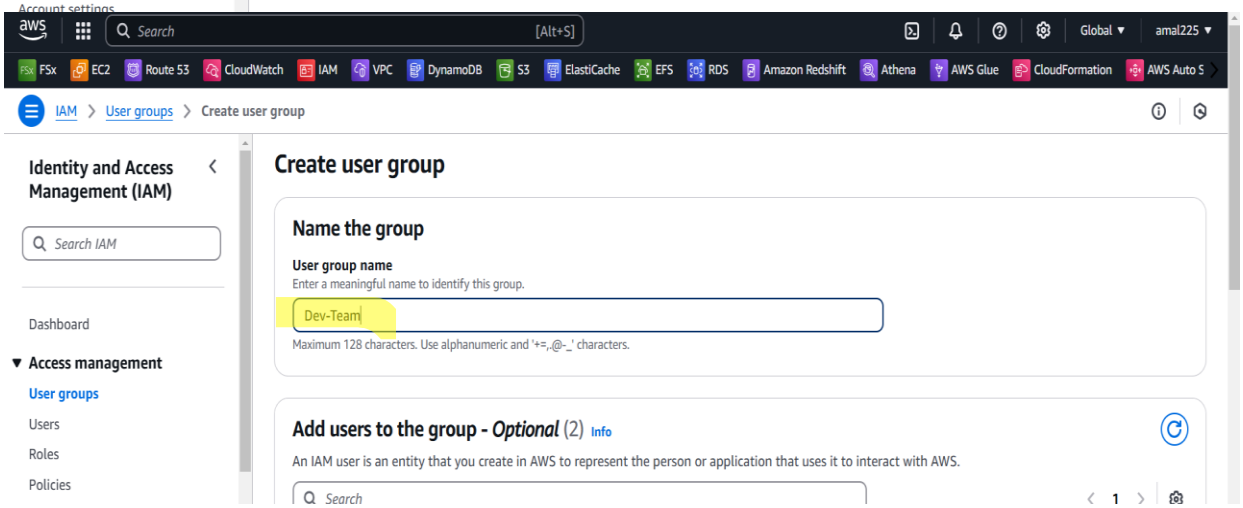


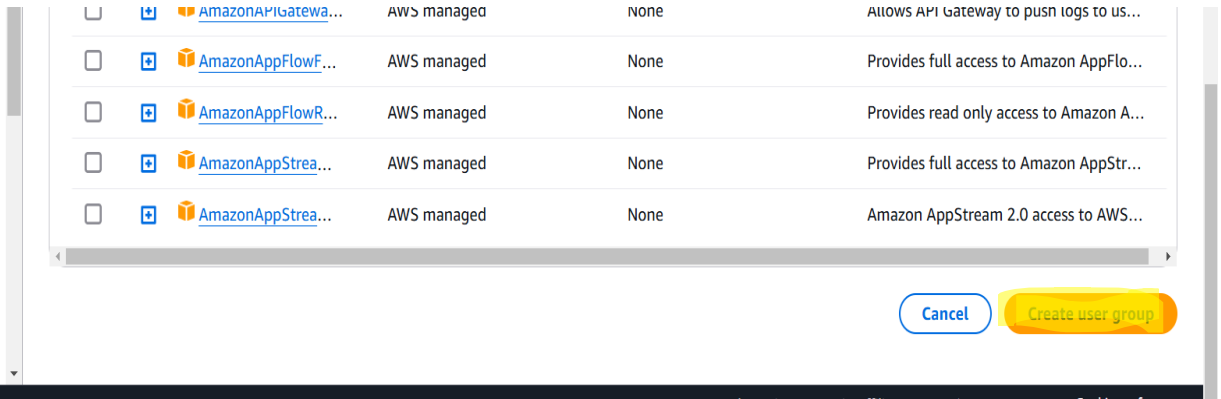
- Download the password and all user Dve2, Test1,Test2 create as it is , download the password for login . look at given below I have created all user same as it .

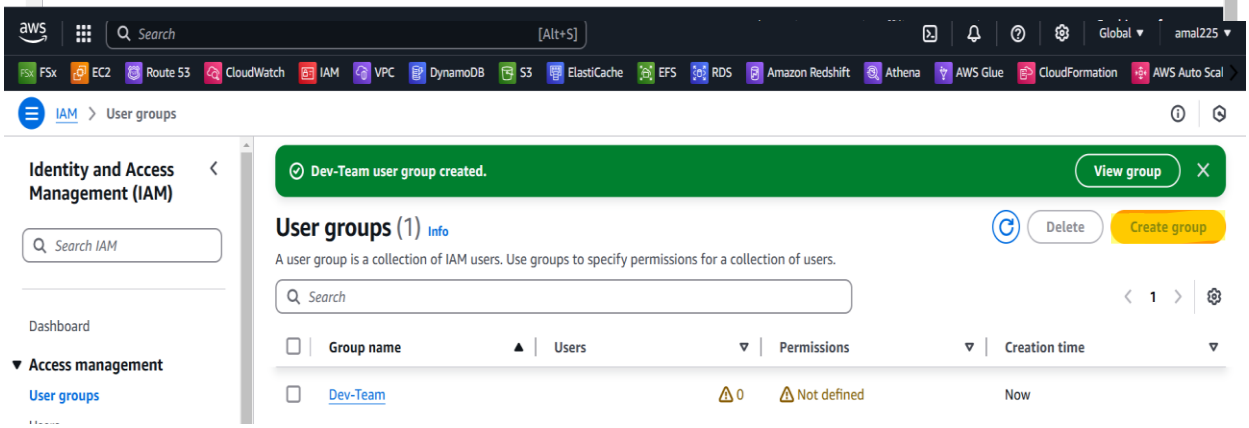


2. Create 2 groups named “Dev Team” and “Ops Team”
    - In IAM dashboard ,go to Group and click create group, and provide group name and , create user group.

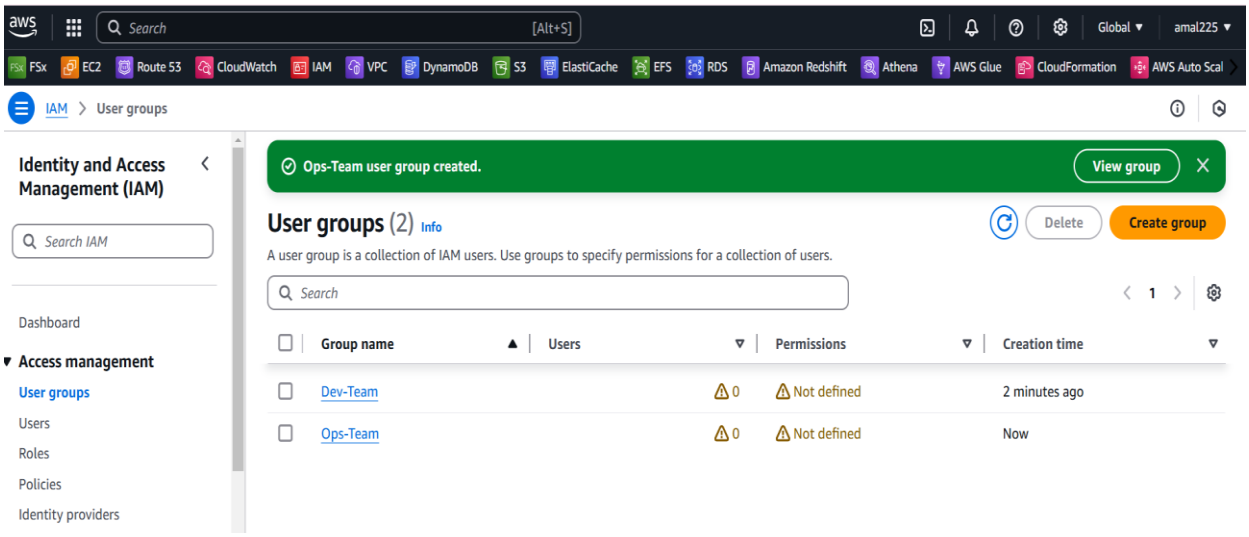




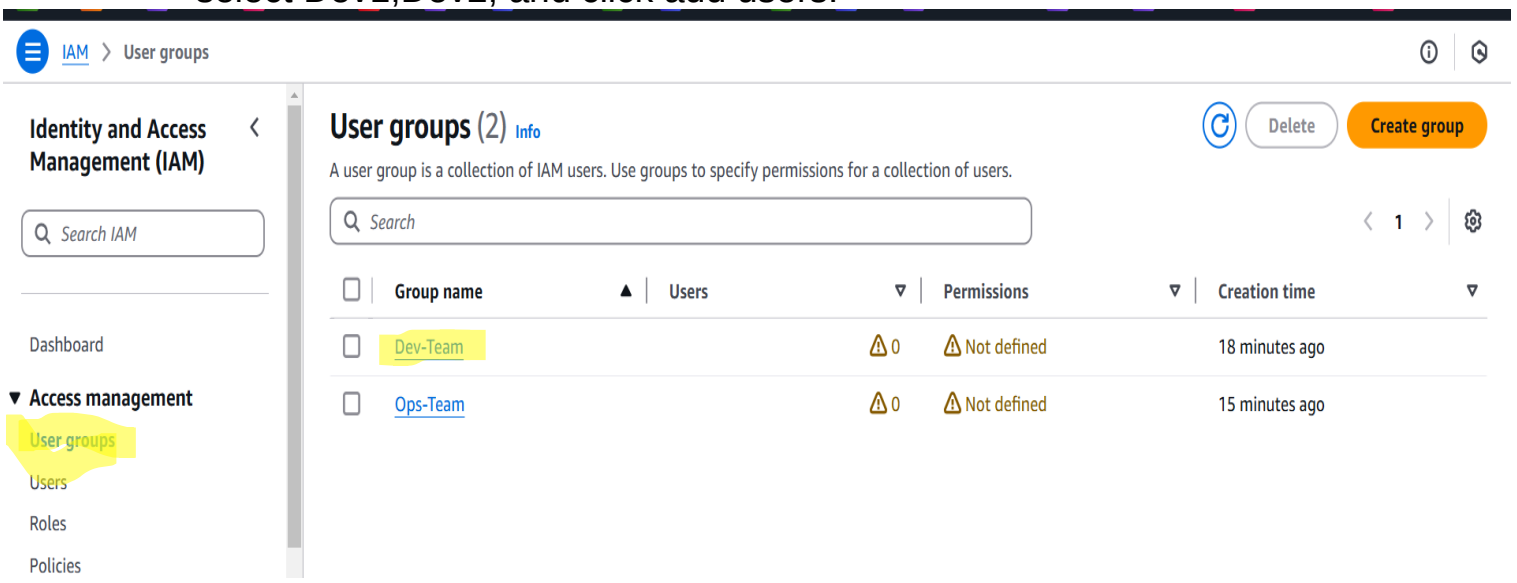


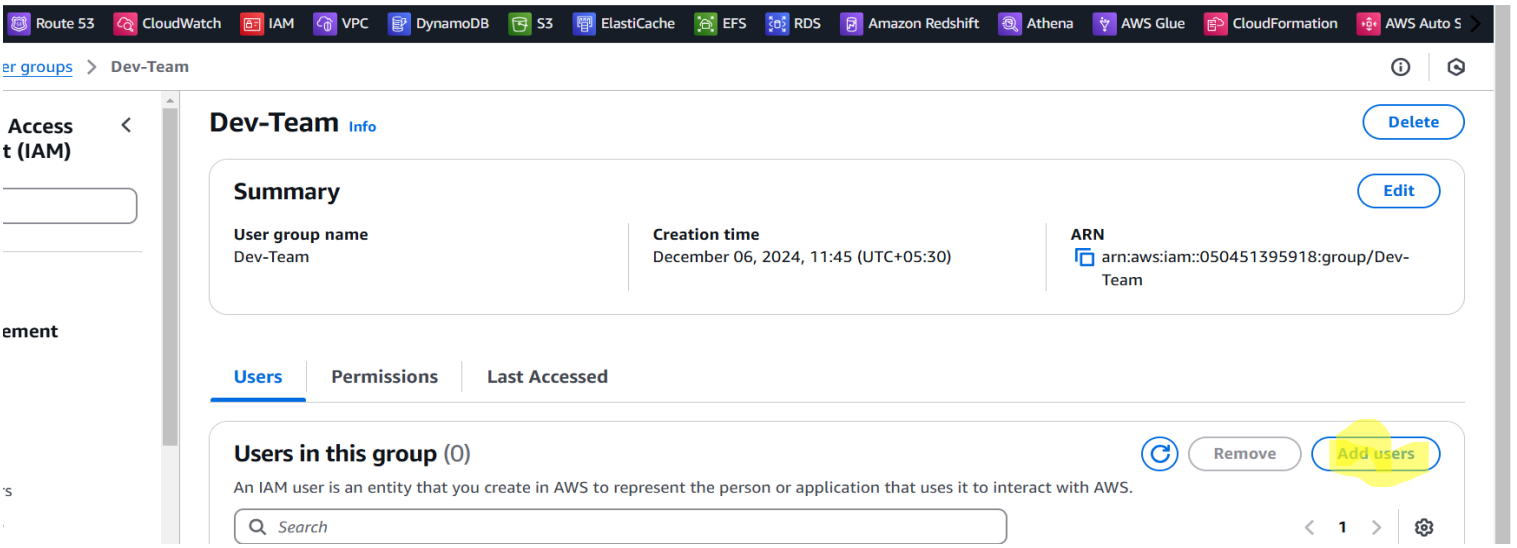


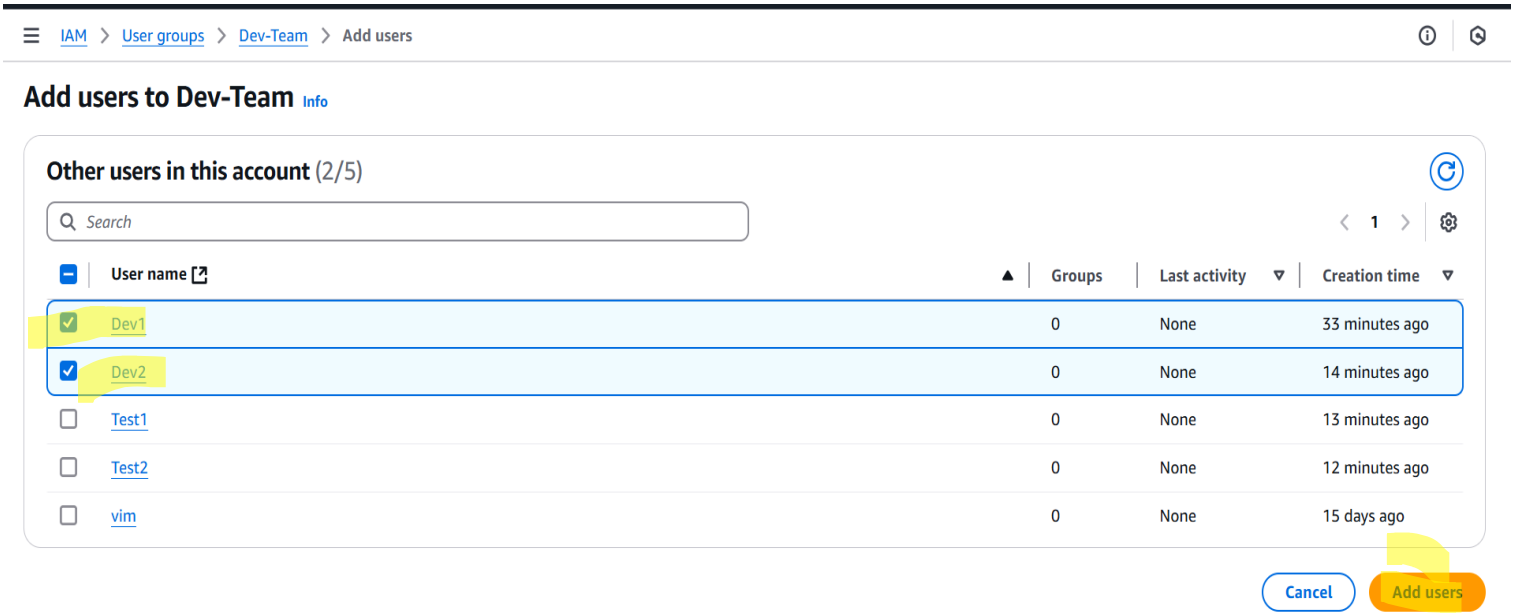
- Ops-Team create same as it ,same process we can follow it.

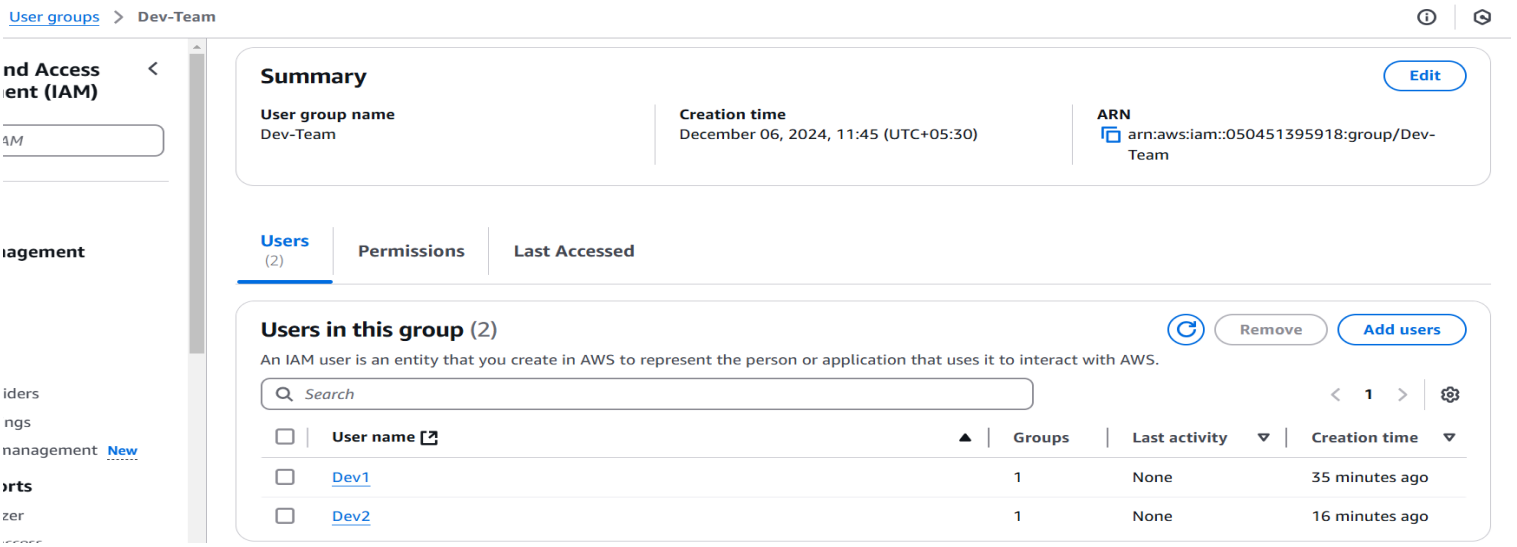


3. Add Dev1 and Dev2 to the Dev Team.
    - Go to User Group and click Dev-Team, into Dev-Team ,click add user and select Dev1,Dev2, and click add users.









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

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