IAM – Identity Access Management

Scenario 1: IAM users, Groups, Policy and permissions.

Need to create one UserGroup – L1 support (they should have primary support to ec2)

L1 support policy should be like allow only the below and disable everything

Can reboot instance

Can start instance

Can take snapshot

Can delete the snapshot.

Can view the ec2 instances – add ec2:DescribeInstances policy

(we shouldn't have ability to launch the instance, delete the instance,modify the instance etc etc)

Need one user account to be created with the name testuser

He should be part of L1 UserGroup.

He should be able to reboot , start the instance and take the snapshot, delete the snapshot based on the tickets/request)

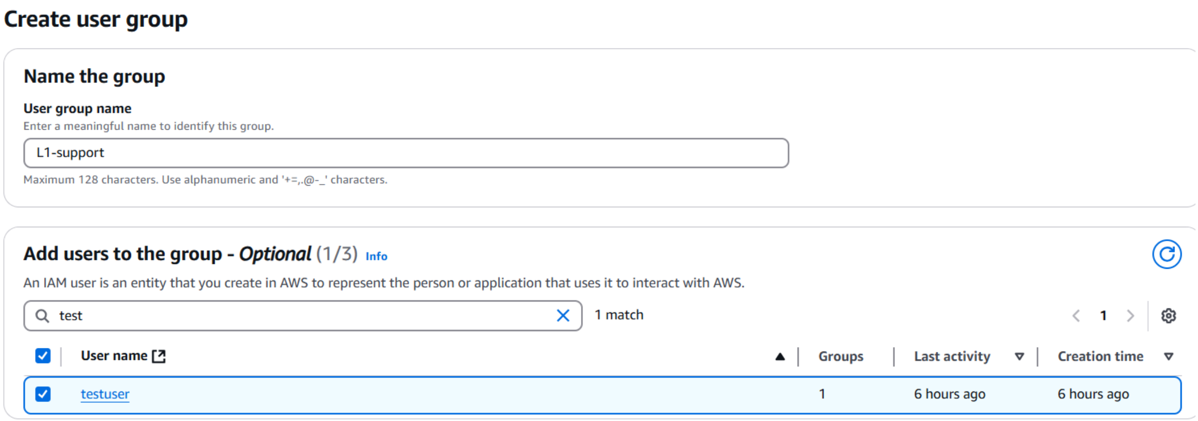
Steps

To create an group and add policy

Step 1: Go to aws console > IAM > under user group> create group

Name it – L1-support and select the user we need to.

If needed can select the policy here but to customize the policy leave it don't select anything and click on create a group.



Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

L1-support

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

Add users to the group - *Optional* (1/3) Info

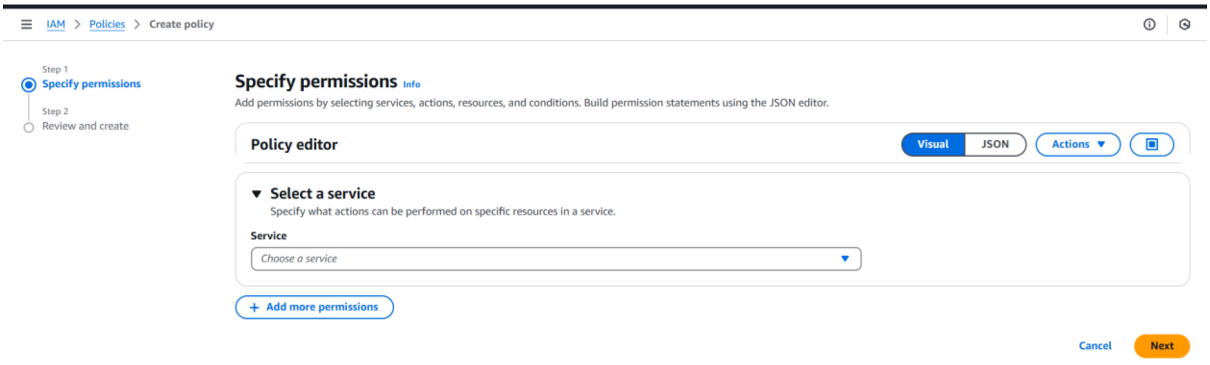
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

test

1 match

☑	User name	Groups	Last activity	Creation time
☑	testuser	1	6 hours ago	6 hours ago

Step 2: Go to aws console > IAM > under polices> create policy



IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

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

Policy editor

Visual | JSON | Actions ▼

▼ Select a service

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

Service: Choose a service ▼

+ Add more permissions

Cancel | Next

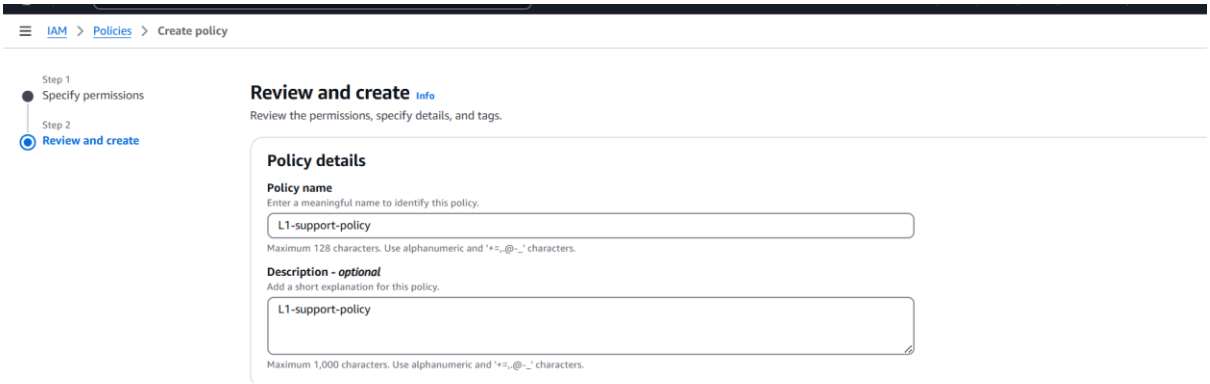
Select visual , **select a service** as – ec2

Select the action needed

And click next .

Step 3: Review and create.

Provide the name of the policy. – L1-supportpolicy



IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Review and create Info

Review the permissions, specify details, and tags.

Policy details

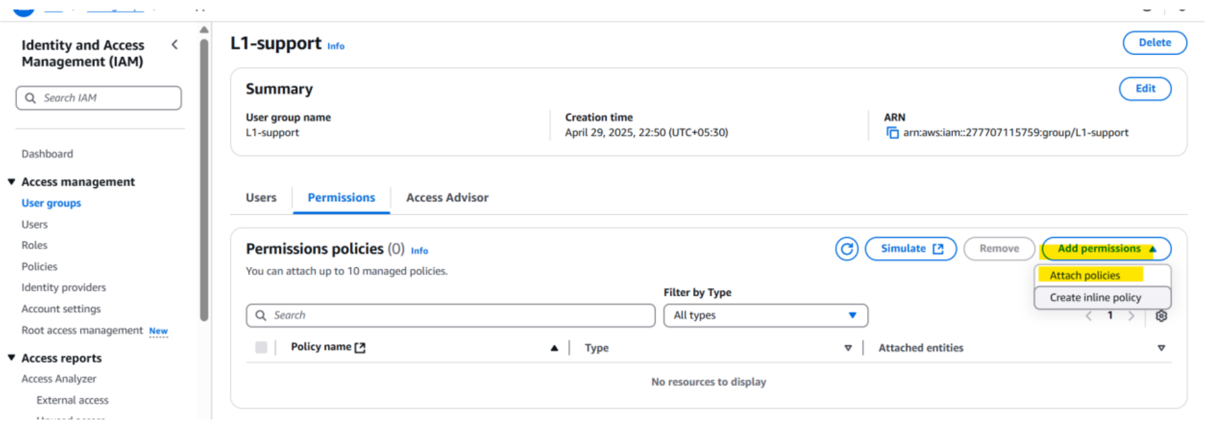
Policy name
Enter a meaningful name to identify this policy.
L1-support-policy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.
L1-support-policy
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Create a policy.

Step 4: attach the policy to L1-support group

Go to groups > select l1-support group, under Add permissions > attach policies



Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New

▼ Access reports
Access Analyzer
External access

L1-support Info | Delete

Summary | Edit

User group name	Creation time	ARN
L1-support	April 29, 2025, 22:50 (UTC+05:30)	arn:aws:iam::277707115759:group/L1-support

Users | Permissions | Access Advisor

Permissions policies (0) Info

You can attach up to 10 managed policies.

Simulate | Remove | Add permissions ▲

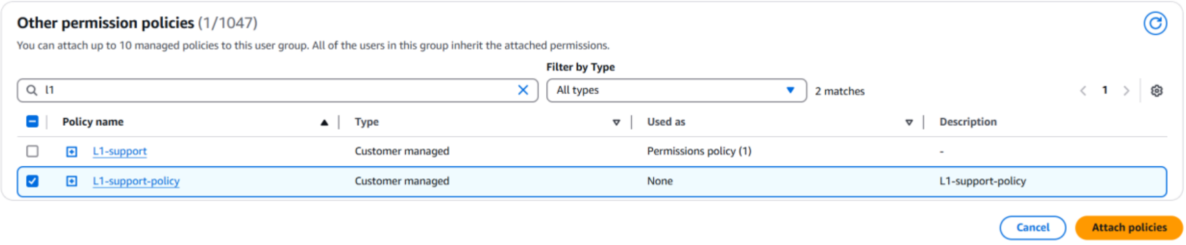
Attach policies
Create inline policy

Search | Filter by Type: All types ▼

Policy name	Type	Attached entities

No resources to display

Select the policy which we created and select **attach policies.**



Other permission policies (1/1047)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Filter by Type: All types — 2 matches

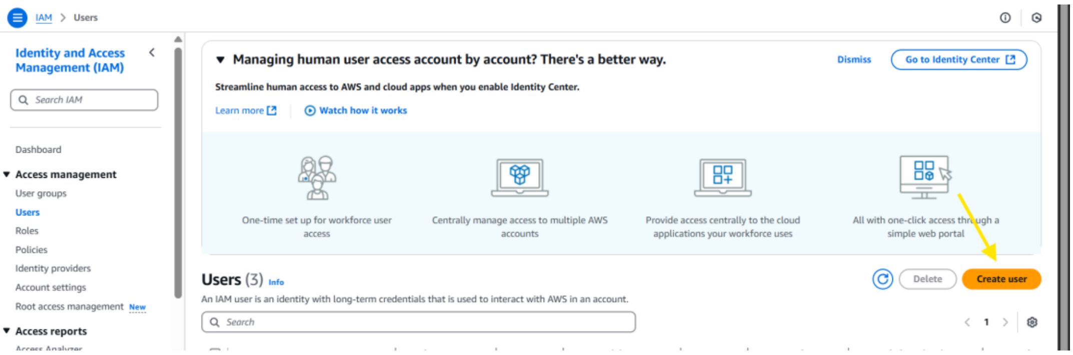
Search: l1

	Policy name	Type	Used as	Description
□	L1-support	Customer managed	Permissions policy (1)	-
☑	L1-support-policy	Customer managed	None	L1-support-policy

And also add **ec2readonlyaccess** permissions policy to the L1-support group

To Create a user account and add that user to user groups.

Step 1.Go to aws console > IAM > under user group> create user



Managing human user access account by account? There's a better way.

Streamline human access to AWS and cloud apps when you enable Identity Center.

One-time set up for workforce user access

Centrally manage access to multiple AWS accounts

Provide access centrally to the cloud applications your workforce uses

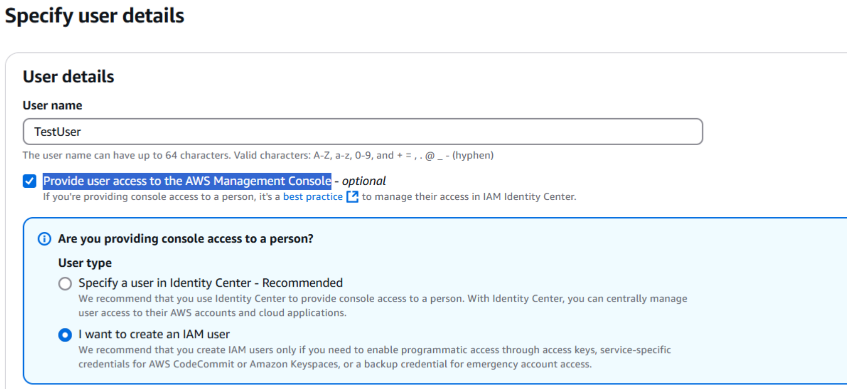
All with one-click access through a simple web portal

Users (3) Info

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

Step 2: Provide the username, select **Provide user access to the AWS Management Console**

Note: make sure it should be an unique name.



Specify user details

User details

User name

TestUser

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.

Step 3: auto generate or custom password your wish.

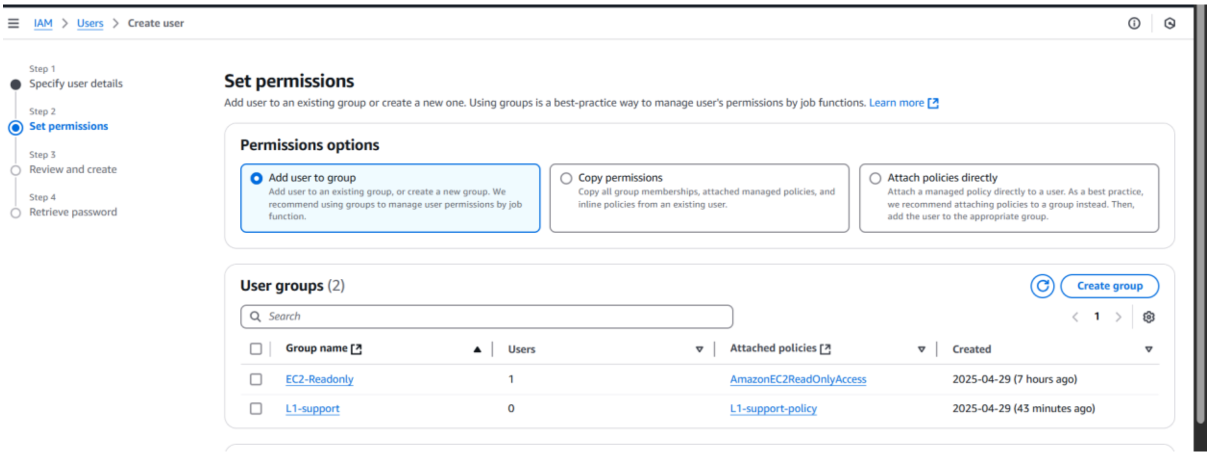
Better you select auto generate, the aws will create password for you then you can share those passwords to user.

Also select the box **"Users must create a new password at next sign-in – Recommended" – so that user can change is password once he logins.**

If you prefer that user shouldn’t change the password which you gave and he should you the same password, then **uncheck the box**

Step 4: set permissions

Select **“add user to group”** and select the **L1-support group.**



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.

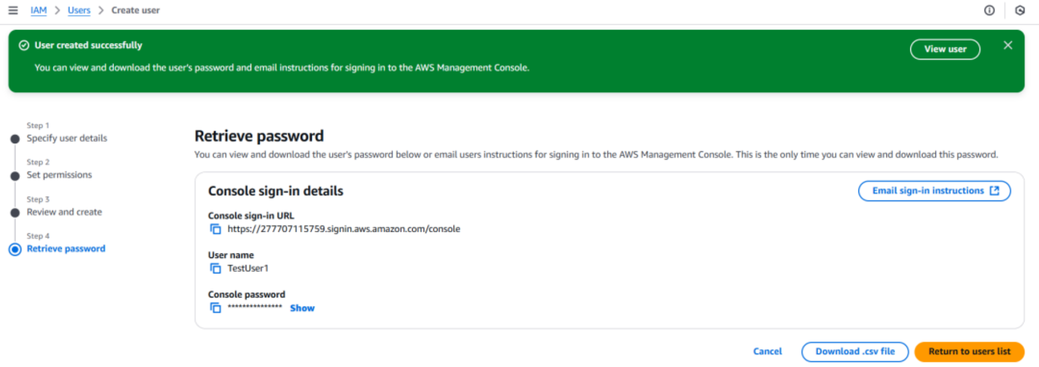
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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.

User groups (2)

□	Group name	Users	Attached policies	Created
□	EC2-Readonly	1	AmazonEC2ReadOnlyAccess	2025-04-29 (7 hours ago)
□	L1-support	0	L1-support-policy	2025-04-29 (43 minutes ago)

Step 5: next and create



IAM > Users > 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.

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve 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://277707115759.signin.aws.amazon.com/console

User name
TestUser1

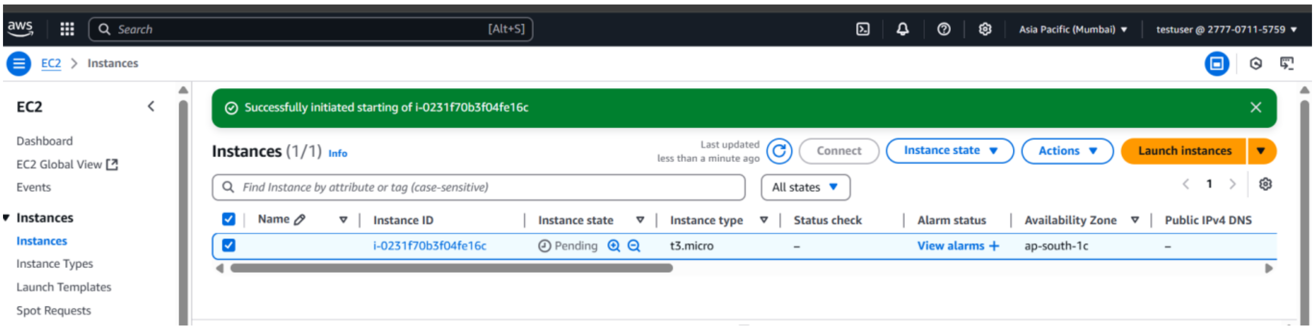
Console password
*************** Show

Note: gather than giving user an account id, username and password.

Provide him with the console sign-in URL (alias)

So that user needs not to enter account id manually he can just enter username and password.

Validation; user can start the stopped instance



Asia Pacific (Mumbai) ▾ testuser @ 2777-0711-5759 ▾

EC2 > Instances

Successfully initiated starting of i-0231f70b3f04fe16c

Instances (1/1) Info

Last updated less than a minute ago

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☑		i-0231f70b3f04fe16c	Pending	t3.micro	–	View alarms +	ap-south-1c	–