

IAM Tasks-01

- **Objective:** To implement and manage AWS IAM users, groups, and policies by applying least-privilege access, automating user creation, restricting permissions by region, and enabling secure cross-account S3 access between AWS accounts.
- **Create one IAM user and assign EC2 and S3 full access roles.**

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
Tester

Console password type
Custom password

Require password reset
No

Permissions summary

< 1 >

| Name ↗ | Type ▲ | Used as ▼ |
|-------------------------------------|------------------------|---------------------------|
| AmazonEC2FullAccess | AWS managed | Permissions policy |
| AmazonS3FullAccess | 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.

The user “Tester” has been created with both permissions.

Tester [Info](#)

[Delete](#)

Summary

ARN
[arn:aws:iam::526018540742:user/Tester](#)

Created
January 09, 2026, 14:54 (UTC+05:30)

Console access
[Enabled without MFA](#)

Last console sign-in
[Never](#)

Access key 1
[Create access key](#)

[Permissions](#) [Groups](#) [Tags](#) [Security credentials](#) [Last Accessed](#)

Permissions policies (2)



[Remove](#)

[Add permissions](#) [▼](#)

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

| Search | | Filter by Type | |
|--|--|--------------------------------|-------------------------|
| <input type="text"/> | | All types ▼ | < 1 > ⚙ |
| <input type="checkbox"/> Policy name ↗ | ▲ Type ▼ | Attached via ↗ | |
| <input type="checkbox"/> AmazonEC2FullAccess | AWS managed | Directly | |
| <input type="checkbox"/> AmazonS3FullAccess | AWS managed | Directly | |

► [Permissions boundary](#) (not set)

IAM Tasks-01

- Create one group in IAM and assign read access for EC2.

The screenshot shows the AWS IAM console for a group named 'Testing'. The 'Permissions' tab is selected, displaying 'Permissions policies (1)'. A table lists the attached policies:

| Policy name | Type | Attached entities |
|-------------------------|-------------|-------------------|
| AmazonEC2ReadOnlyAccess | AWS managed | 1 |

A group named “Testing” has been created with the given permissions.

- Create a new user named "DevOps" and add to the group created in task 2.

The screenshot shows the AWS IAM console for the 'Testing' group, with the 'Users (1)' tab selected. It displays 'Users in this group (1)'. A table lists the users:

| User name | Groups | Last activity | Creation time |
|-----------|--------|---------------|---------------|
| DevOps | | None | Now |

A user named “DevOps” was created and added to the group “Testing”.

IAM Tasks-01

- Write a bash script to create an IAM user with VPC full access.

```
$ cat IAM.bash
#!/bin/bash

# Exit immediately if any command fails
set -e

# Prompt for IAM username
read -p "Enter IAM username: " user

# Validate input
if [ -z "$user" ]; then
    echo "Error: Username cannot be empty"
    exit 1
fi

policy="arn:aws:iam::aws:policy/AmazonVPCFullAccess"

# Create IAM user
echo "Creating IAM user: $user"
aws iam create-user --user-name "$user"

# Attach VPC Full Access policy
echo "Attaching VPC Full Access policy"
aws iam attach-user-policy \
    --user-name "$user" \
    --policy-arn "$policy"

echo "User '$user' created with VPC Full Access"
```

The script was written so that the user can input any username and create a user with VPC full access. The arn of the existing VPC full access was used in the policy variable.

```
Viqaas@LAPTOP-VG025G9U MINGW64 /d/DevOps/Me/DevOps-Learning/Scripts (main)
$ bash IAM.bash
Enter IAM username: Script
Creating IAM user: Script
{
  "User": {
    "Path": "/",
    "UserName": "Script",
    "UserId": "AIDAXU6JF6TDDXVQVMQD6",
    "Arn": "arn:aws:iam::526018540742:user/Script",
    "CreateDate": "2026-01-09T09:48:22+00:00"
  }
}
Attaching VPC Full Access policy
User 'Script' created with VPC Full Access
```

The user was successfully created.

IAM Tasks-01

The user will have to configure AWS CLI with root permissions first before executing the above script.

Script Info

Summary

ARN
[arn:aws:iam::526018540742:user/Script](#)

Created
January 09, 2026, 15:18 (UTC+05:30)

Console access
Disabled

Last console sign-in
-

Access key 1
[Create access key](#)

Permissions

Groups

Tags

Security credentials

Last Accessed

Permissions policies (1) Info

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

Filter by Type
All types

☐

Policy name [↗](#)

▲

Type

▼

Attached via [↗](#)

☐

[AmazonVPCFullAccess](#)

AWS managed

Directly

- **Create an IAM policy to allow EC2 access for a specific user in specific regions only.**

EC2AccessSpecificRegions Info Edit Delete

Allows EC2 actions only when the request is made in us-east-1 or us-west-2.

Policy details

Type
Customer managed

Creation time
January 09, 2026, 15:34 (UTC+05:30)

Edited time
January 09, 2026, 15:34 (UTC+05:30)

ARN
[arn:aws:iam::526018540742:policy/EC2AccessSpecificRegions](#)

Permissions

Entities attached

Tags

Policy versions (1)

Last Accessed

Permissions defined in this policy Info Copy Edit Summary JSON

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

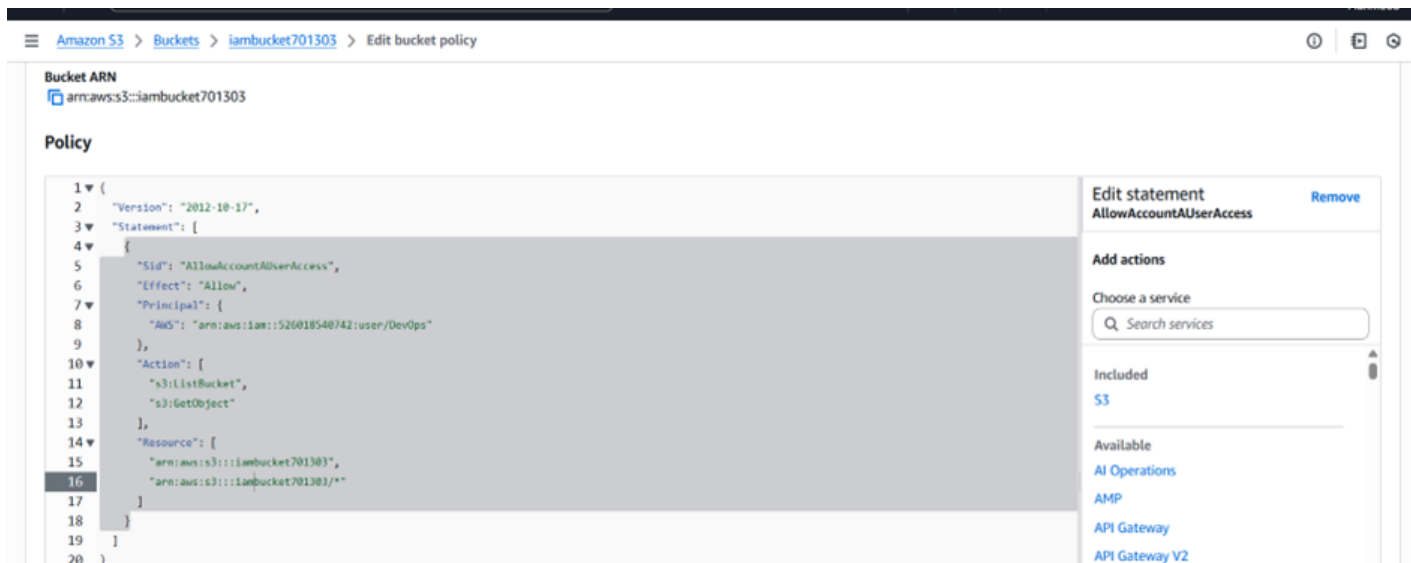
```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "AllowEC2SpecificRegions",
6       "Effect": "Allow",
7       "Action": "ec2:*",
8       "Resource": "*",
9       "Condition": {
10        "StringEquals": {
11          "aws:RequestedRegion": [
12            "us-east-1",
13            "us-west-2"
14          ]
15        }
16      }
17    ]
18  }
```

The policy above allows EC2 actions only when the request is made in “us-east-1” or “us-west-2”.

- The regions can be changed as per requirement.
- The policy was created in json format with the name “EC2AccessSpecificRegions”.
- We can attach this policy to a specific user or a group.

IAM Tasks-01

- We have two accounts: Account A and Account B. Account A user should access an S3 bucket in Account B.
- First, Account A user needs S3 full access to access the bucket in Account B.
- Then Account B needs to create a bucket policy which gives access to Account A.



- Then Account A can use AWS CLI to access the bucket.

```
Viqaas@LAPTOP-VG025G9U MINGW64 ~/Desktop
$ aws sts get-caller-identity
{
  "UserId": "AIDAXU6JF6TDPEQY2VEMM",
  "Account": "526018540742",
  "Arn": "arn:aws:iam::526018540742:user/DevOps"
}

Viqaas@LAPTOP-VG025G9U MINGW64 ~/Desktop
$ aws s3 ls s3://iambucket701303
PRE bucket folder/
```

- Successfully completed all assigned AWS IAM tasks, including user, group, policy management, automation, and secure cross-account S3 access.