

In this guide, I documented about **IAM Users Assignment**, **IAM Policy Assignment**, and **IAM Roles**, including creation, configuration, and best-practice usage.

✓ 1. Create IAM Users

Create the following users in the IAM dashboard:

- **Dev1**
- **Dev2**
- **Test1**
- **Test2**

Steps:

1. Go to **IAM Console** → **Users** → **Create User**
2. Enter the username
3. Choose **Programmatic access** or **Console access** as needed
4. Complete the creation process
5. Repeat for all four users

The screenshot shows the AWS IAM console interface. The left sidebar has 'Identity and Access Management (IAM)' selected under 'Access management'. The main area is titled 'Users (4) Info' with a note: 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' A green banner at the top right says 'OpsTeam user group created.' Below is a table with the following data:

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access
Dev1	/	0	-	-	4 minutes	-	-
Dev2	/	0	-	-	3 minutes	-	-
Test1	/	0	-	-	-	-	-
Test2	/	0	-	-	2 minutes	-	-

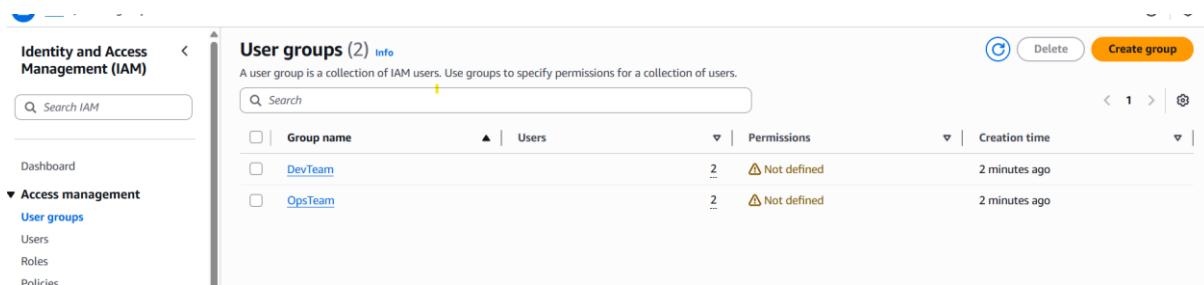
2. Create IAM Groups

Create two IAM groups:

- **Dev Team**
- **Ops Team**

Steps:

1. Go to **IAM Console** → **User Groups** → **Create Group**
2. Enter the group name
3. (Optional) Attach policies
4. Create the group
5. Repeat for both groups



The screenshot shows the AWS IAM User Groups page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. The main area has a title 'User groups (2) Info' and a subtitle 'A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.' Below this is a search bar and a table with two rows.

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	DevTeam	2	⚠ Not defined	2 minutes ago
<input type="checkbox"/>	OpsTeam	2	⚠ Not defined	2 minutes ago

IAM POLICY

Create policy number 1 which lets the users to:

- Access S3 completely
- Only create EC2 instances
- Full access to RDS

Policy details

Type Customer managed	Creation time November 15, 2025, 11:49 (UTC+05:30)	Edited time November 15, 2025, 11:49 (UTC+05:30)	ARN arn:aws:iam::395069634226:policy/PolicyNumber1
--------------------------	---	---	---

Permissions defined in this policy Info

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.

Allow (3 of 452 services)

Service	Access level	Resource	Request condition
EC2	Limited: Write	All resources	None
RDS	Full access	All resources	None
S3	Full access	All resources	None

Show remaining 449 services

2. Create a policy number 2 which allows the users to:

- Access CloudWatch and billing completely
- Can only list EC2 and S3 resources

Entity and Access Management (IAM)

Policy details

Type Customer managed	Creation time November 15, 2025, 12:10 (UTC+05:30)	Edited time November 15, 2025, 12:10 (UTC+05:30)	ARN arn:aws:iam::395069634226:policy/PolicyNumber2
--------------------------	---	---	---

Permissions defined in this policy Info

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.

Allow (4 of 452 services)

Service	Access level	Resource	Request condition
Billing	Full access	All resources	None
CloudWatch	Full access	All resources	None
EC2	Limited: List	All resources	None
S3	Limited: List	All resources	None

Show remaining 448 services

3. Attach policy number 1 to the Dev Team from task 1

The screenshot shows the AWS IAM User Groups page for the user group 'DevTeam'. The 'Permissions' tab is selected. A green banner at the top states 'Policies attached to this user group.' Below it, the 'Permissions policies' section shows one policy named 'PolicyNumber1' attached. The policy is listed with the following details:

Policy name	Type	Attached entities
PolicyNumber1	Customer managed	1

The ARN of the policy is listed as `arn:aws:iam::395069634226:group/DevTeam`.

4. Attach policy number 2 to the Ops Team from task 1

The screenshot shows the AWS IAM User Groups page for the user group 'OpsTeam'. The 'Permissions' tab is selected. A green banner at the top states 'Policies attached to this user group.' Below it, the 'Permissions policies' section shows one policy named 'PolicyNumber2' attached. The policy is listed with the following details:

Policy name	Type	Attached entities
PolicyNumber2	Customer managed	1

The ARN of the policy is listed as `arn:aws:iam::395069634226:group/OpsTeam`.

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar lists 'Identity and Access Management (IAM)' sections: Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management), Access reports (Access Analyzer, Resource analysis, Unused access, Analyzer settings, Credential report), and Tools (CloudShell, Feedback). A status bar at the bottom indicates 'Rainy days ahead'.

IAM resources section: A red box highlights an 'Access denied to iam:GetAccountSummary' error. It states: 'You don't have permission to `iam:GetAccountSummary`. To request access, copy the following text and send it to your AWS administrator.' Below this is a snippet of JSON policy code.

AWS Account section: Two errors are listed under 'Access denied to iam:ListAccountAliases'. Both mention the user lacks permission to perform the action on the specified resource.

What's new: Updates for features in IAM include Amazon Bedrock API keys, AWS Service Reference annotations, and RCP support for two additional services.

IAM Roles

Create a role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB.

The screenshot shows the 'Role1' details page. The sidebar is identical to the previous dashboard. The main content includes:

- Summary** section: Creation date (November 15, 2025, 13:12 UTC+05:30), Last activity (none), ARN (arn:aws:iam::395069634226:role/Role1), Maximum session duration (1 hour), and a 'Link to switch roles in console' button.
- Permissions** tab: Shows two attached policies: 'AmazonDynamoDBFullAccess' and 'AmazonVPCFullAccess', both listed as 'AWS managed'.

Update, Set Trust Policy to allow Dev 1 and Dev 2

Identity and Access Management (IAM)

Creation date: November 15, 2025, 13:12 (UTC+05:30)

ARN: arn:aws:iam::395069634226:role/Role1

Last activity: -

Maximum session duration: 1 hour

Link to switch roles in console: <https://signin.aws.amazon.com/switchrole?roleName=Role1&account=395069634226>

Permissions | **Trust relationships** | Tags | Last Accessed | Revoke sessions

Trusted entities

```

1 = [
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": [
8           "arn:aws:iam::395069634226:user/Dev1",
9           "arn:aws:iam::395069634226:user/Dev2"
10      ]
11    },
12    "Action": "sts:AssumeRole"
13  }
14 ]
15 ]

```

Edit trust policy

Logged in as Dev1, able to switch the role “role1” to access “VPC and Dynamo DB”

VPC dashboard

Create VPC | **Launch EC2 Instances**

Resources by Region

You are using the following Amazon VPC resources:

VPCs	Stockholm 1	NAT Gateways	Stockholm 0
Subnets	Stockholm 3	VPC Peering Connections	Stockholm 0
Route Tables	Stockholm 1	Network ACLs	Stockholm 1
Internet Gateways	Stockholm 1	Security Groups	Stockholm 5
Egress-only Internet Gateways	Stockholm 0	Customer Gateways	Stockholm 0

Service Health

Settings

Additional Information

AWS Network Manager

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Dashboard | Amazon DynamoDB

https://eu-north-1.console.aws.amazon.com/dynamodbv2/home?region=eu-north-1#dashboard

AWS Search [Alt+S] Europe (Stockholm) Account ID: 3950-6963-4226 Role1 @ 395069634226

DynamoDB > Dashboard

Dashboard

Favorite tables

Find favorite tables

Table name Status Created at (UTC)

No favorite tables

To get started, click the star icon on the tables page or table details page to favorite a table.

Alarms (0) Info

Find alarms

Alarm name Status

No custom alarms

DAX clusters (0) Info

Find clusters

Create resources

Create an Amazon DynamoDB table for fast and predictable database performance at any scale. [Learn more](#)

Create table

Amazon DynamoDB Accelerator (DAX) is a fully-managed, highly-available, in-memory caching service for DynamoDB. [Learn more](#)

Create DAX cluster

What's new

NOV 6 Amazon DynamoDB Streams expands AWS PrivateLink support to FIPS endpoints

OCT 31 Amazon DynamoDB Accelerator now supports AWS PrivateLink

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

This screenshot shows the Amazon DynamoDB Dashboard. The left sidebar includes links for Dashboard, Tables, Explore items, PartiQL editor, Backups, Exports to S3, Imports from S3, Integrations, Reserved capacity, Settings, Clusters, Subnet groups, Parameter groups, and Events. The main content area has three main sections: 'Favorite tables' (empty), 'Alarms (0)', and 'DAX clusters (0)'. A 'Create resources' sidebar offers options to 'Create table' or 'Create DAX cluster'. A 'What's new' sidebar lists recent changes, such as the expansion of AWS PrivateLink support for Amazon DynamoDB Streams and the support for AWS PrivateLink for Amazon DynamoDB Accelerator. The bottom of the page includes links for CloudShell, Feedback, and copyright information.