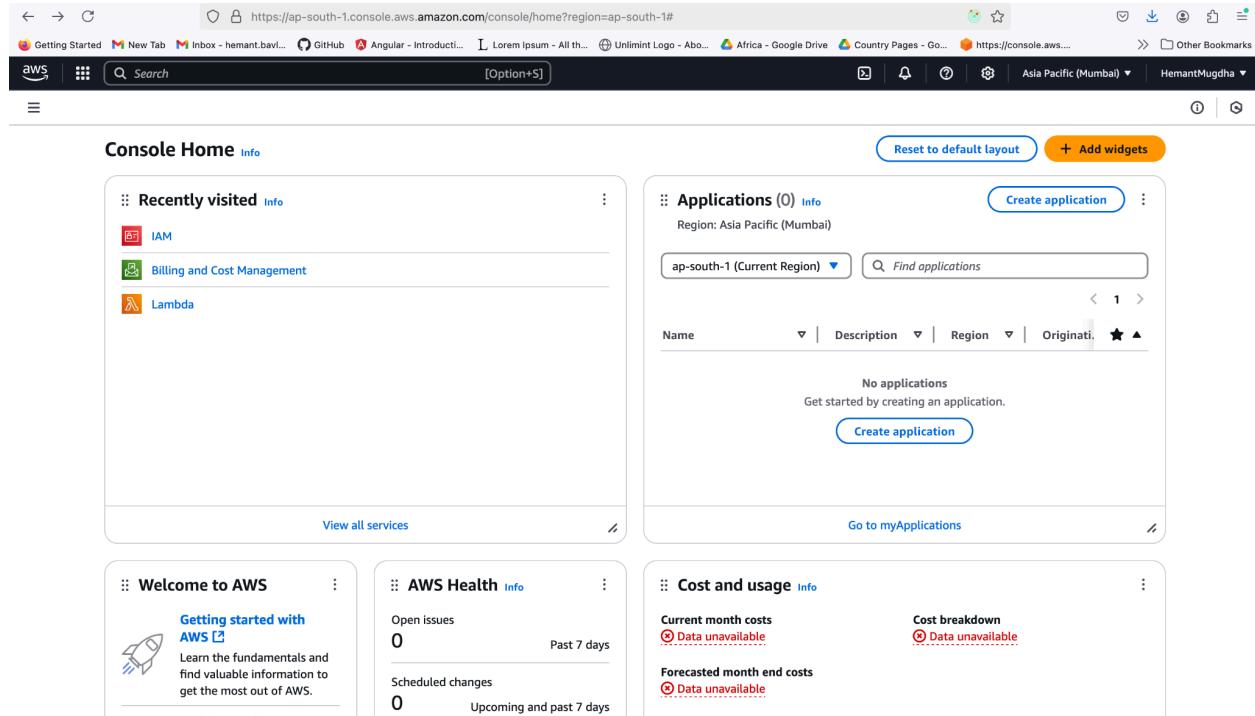
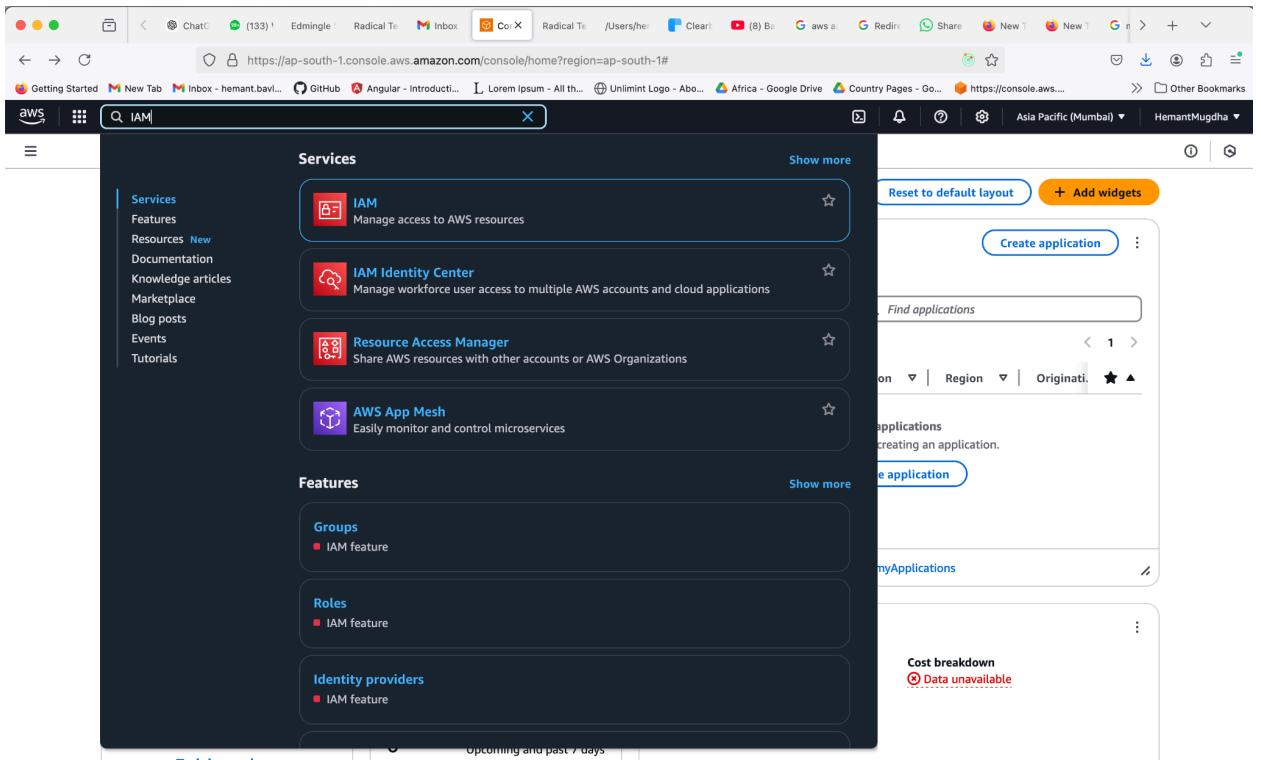


1. HOW TO CREATE AN IAM USER

1. For creating an IAM user, login with the root account and you shall screen similar to the following

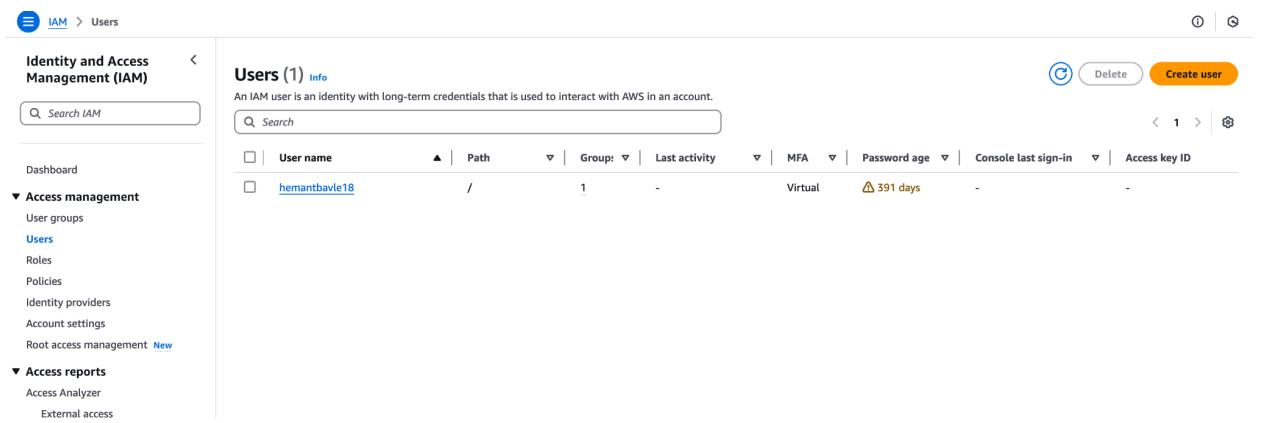


2. Type IAM in search bar or click on IAM from recently visited item list



The screenshot shows the AWS IAM dashboard. In the top navigation bar, there is a search bar with the text "IAM". Below the search bar, the "Services" section is expanded, showing the "IAM" service highlighted with a blue border. Other services listed include IAM Identity Center, Resource Access Manager, and AWS App Mesh. To the right of the services, there is a sidebar with sections for "Features" (Groups, Roles, Identity providers) and "Tutorials". On the far right, there is a "Create application" button and a "Cost breakdown" section indicating "Data unavailable".

3. Click on IAM > Users, You will land on the following screen. Click on Create user button on the right



The screenshot shows the "Users" page under the IAM service. The left sidebar has a "Users" link under the "Access management" section. The main table displays one user entry:

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID
hemantbavle18	/	1	-	Virtual	391 days	-	-

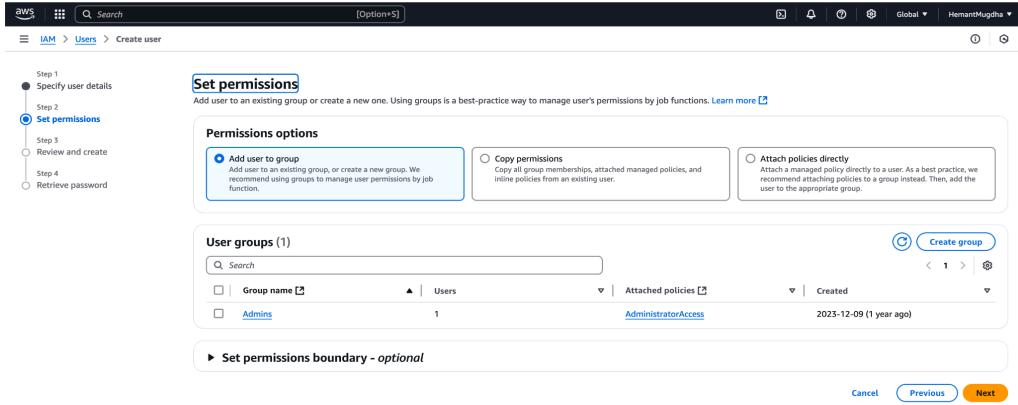
On the far right of the table, there is a "Create user" button.

4. Add details for the user and click next

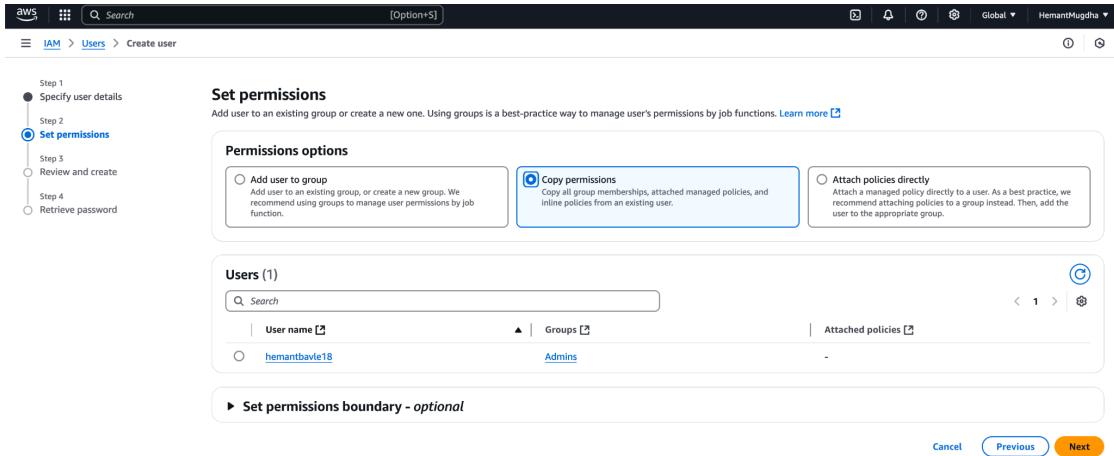
The screenshot shows the 'Specify user details' step in the AWS IAM 'Create user' wizard. The left sidebar shows steps 1 through 4: Step 1 (Specify user details, selected), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main area is titled 'Specify user details' and contains the 'User details' section. Under 'User name', 'testhemant1' is entered. A note states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)'. A checked checkbox says: 'Provide user access to the AWS Management Console - optional'. Below it, a note says: 'If you're providing console access to a person, it's a best practice [link] to manage their access in IAM Identity Center.' The 'User type' section has two options: 'Specify a user in Identity Center - Recommended' (unchecked) and 'I want to create an IAM user' (checked). A note for the second option says: '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.' The 'Console password' section has two options: 'Autogenerated password' (unchecked) and 'Custom password' (checked). A note for the second option says: 'Enter a custom password for the user.' Below is a password input field with '*****' and a 'Show password' link. A checked checkbox says: 'Users must create a new password at next sign-in - Recommended'. A note says: 'Users automatically get the IAMUserChangePassword [link] policy to allow them to change their own password.' At the bottom, a note says: '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.' A 'Learn more [link]' button is also present.

5. You can assign permission in 3 ways to the user:

- Using a user group as shown in the screenshot below



b. By copying permission from other users



C

c. By Attaching default policy directly to the user

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.

Permissions policies (1317)

Choose one or more policies to attach to your new user.

Policy name	Type	Attached entities
AccessAnalyzerServiceRolePolicy	AWS managed	0
AdministratorAccess	AWS managed - job function	2
AdministratorAccess-Amplify	AWS managed	0
AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
AIOpsAssistantPolicy	AWS managed	0
AIOpsConsoleAdminPolicy	AWS managed	0
AIOpsOperatorAccess	AWS managed	0
AIOpsReadOnlyAccess	AWS managed	0
AmazonCloudWatchLogsFullAccess	AWS managed	0

Click Next after you have used the appropriate option.

6. I created a new group with EC2 full access policy

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: testIamUser1

Console password type: Custom password

Require password reset: Yes

Permissions summary

Name	Type	Used as
EC2FullAccessGroup	Group	Permissions group
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](#)

7. On clicking Create user button, a loader will show up and then a screen like below should show up.

Screenshot of the AWS IAM 'Create user' success page.

User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

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.

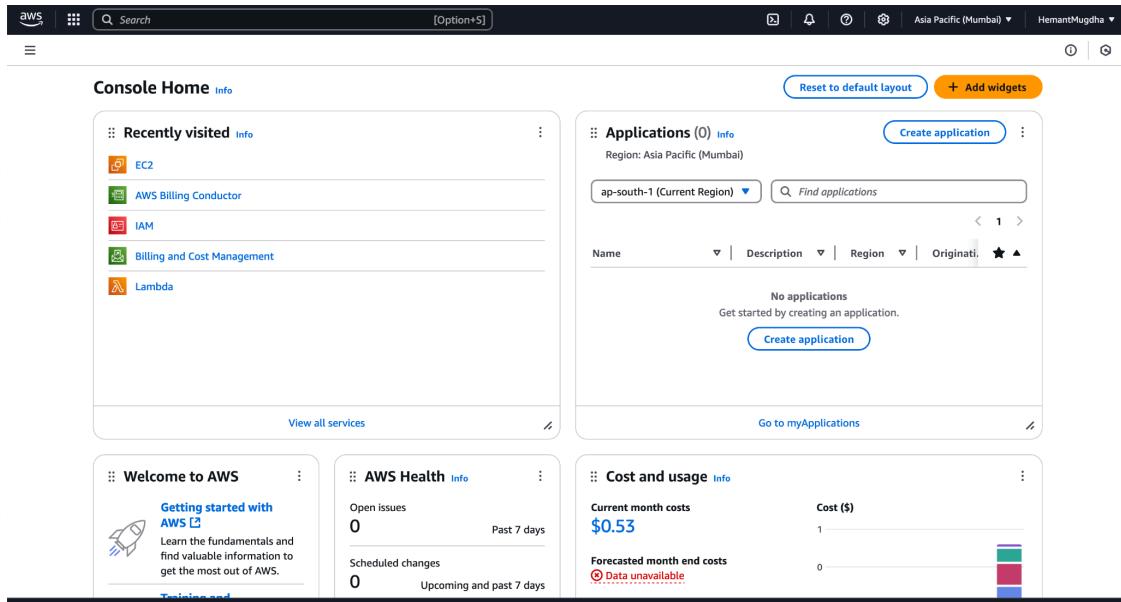
Console sign-in details

- Console sign-in URL:** <https://999331376056.signin.aws.amazon.com/console>
- User name:** testHemant1
- Console password:** [*****](#) [Show](#)

Actions: [View user](#) [Email sign-in instructions](#) [Cancel](#) [Download .csv file](#) [Return to users list](#)

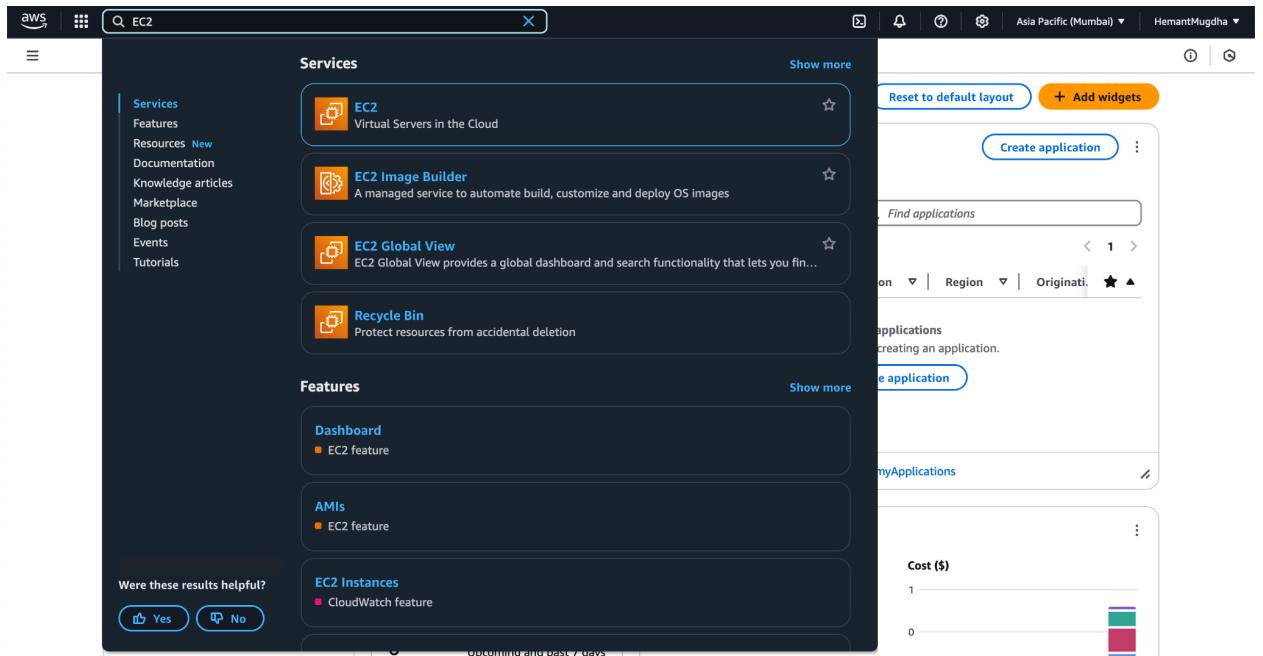
2. Creating an EC2 Instance

- Login to your aws account



The screenshot shows the AWS Console Home page. At the top, there is a search bar with the placeholder "Search" and a note "[Option+S]". The top right corner displays the region "Asia Pacific (Mumbai)" and the user "HemantMugdha". Below the header, there are several sections: "Recently visited" (EC2, AWS Billing Conductor, IAM, Billing and Cost Management, Lambda), "Applications (0)" (Create application), "Welcome to AWS" (Getting started with AWS), "AWS Health" (Info: Open issues 0, Past 7 days; Scheduled changes 0, Upcoming and past 7 days), and "Cost and usage" (Info: Current month costs \$0.53, Forecasted month end costs Data unavailable). A "View all services" link is located at the bottom of the recently visited section.

- In the search bar type, EC2



The screenshot shows the search results for "EC2" in the AWS search bar. On the left, a sidebar lists "Services" (Features, Resources, Documentation, Knowledge articles, Marketplace, Blog posts, Events, Tutorials) and a feedback section ("Were these results helpful? Yes No"). The main content area displays four cards: "EC2" (Virtual Servers in the Cloud), "EC2 Image Builder" (A managed service to automate build, customize and deploy OS images), "EC2 Global View" (EC2 Global View provides a global dashboard and search functionality that lets you fin...), and "Recycle Bin" (Protect resources from accidental deletion). To the right of the search results, the same "Cost and usage" dashboard from the previous screenshot is visible.

c. Click to EC2 to open EC2 Home page as shown below

The screenshot shows the AWS EC2 Home page. On the left, a sidebar menu includes: Dashboard, Instances (selected), Images, Elastic Block Store, Network & Security. The main content area displays:

- Resources:** A summary of Amazon EC2 resources in the Asia Pacific (Mumbai) Region. It shows 0 Instances (running), 0 Auto Scaling Groups, 0 Capacity Reservations, 0 Dedicated Hosts, 0 Elastic IPs, 0 Instances, 1 Key pairs, 0 Load balancers, 0 Placement groups, 2 Security groups, 0 Snapshots, 0 Volumes.
- Launch instance:** Options to launch an instance or migrate a server. Note: Your instances will launch in the Asia Pacific (Mumbai) Region.
- Service health:** Shows the status of the AWS Health Dashboard. Status: This service is operating normally.
- Zones:** A table mapping Zone names to Zone IDs:

Zone name	Zone ID
ap-south-1a	aps1-az1
ap-south-1b	aps1-az3
ap-south-1c	aps1-az2
- Account attributes:** Details about the Default VPC (vpc-0a0874a2e48ae681).
- Explore AWS:** Promotional links for GuardDuty Malware Protection, Better Price Performance (T4g instances), and 10 Things You Can Do Today to Reduce AWS Costs.

d. From the left hand menu, click on Instances, it will open a list of instances(show instances if they do exist else an empty list like below is shown)

The screenshot shows the AWS EC2 Instances page. The left sidebar menu is identical to the previous screenshot. The main content area displays:

- Instances Info:** A search bar and filters for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4.
- A message: "No instances" and "You do not have any instances in this region".
- A "Launch instances" button.
- A "Select an instance" section.

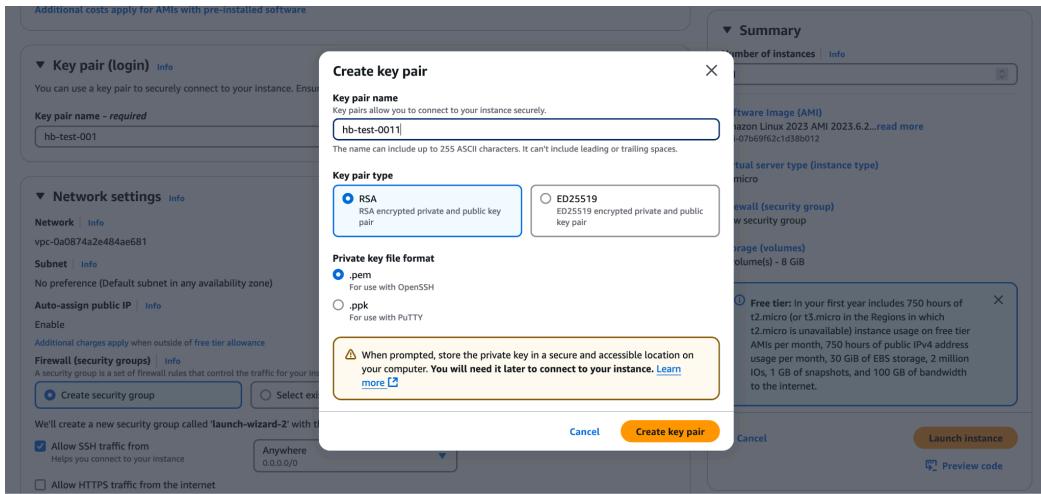
- e. Click on Launch Instances and Add name > Select OS Image from Amazon Machine Image section

The screenshot shows the 'Launch an instance' wizard. In the 'Name and tags' section, the name 'hb-test-001' is entered. In the 'Application and OS Images (Amazon Machine Image)' section, the 'Amazon Linux 2023 AMI' is selected. On the right, a summary panel shows the configuration: 1 instance, Software Image (AMI) set to 'Amazon Linux 2023 AMI 2023.6.2...', Virtual server type set to 't2.micro', and Storage (volumes) set to 1 volume(s) - 8 GiB. A callout box highlights the 'Free tier' information: 'In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.'

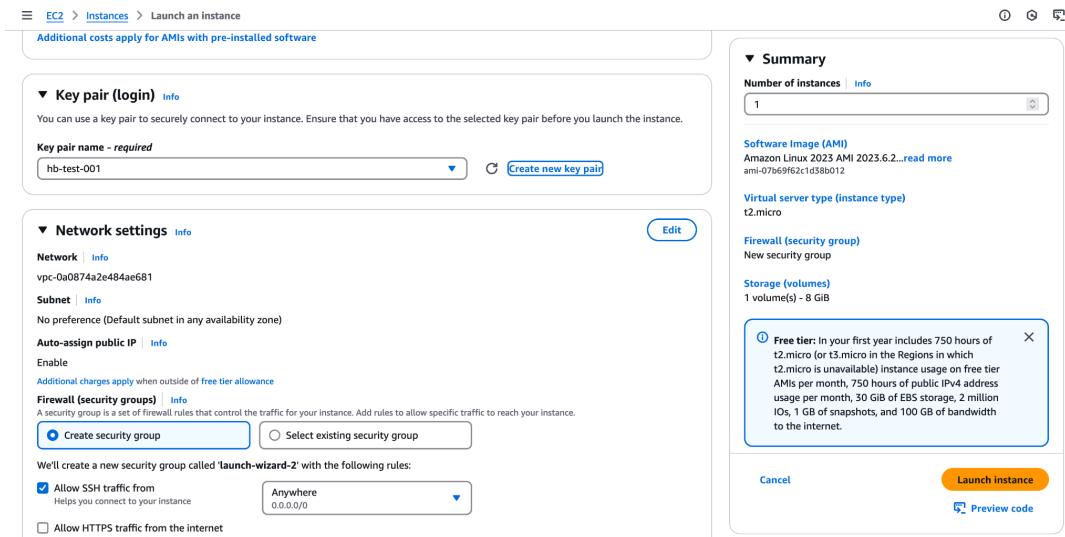
- f. Scroll down > In Key pair section > Click Create new key pair > Add details in modal >

click add key

The screenshot shows the 'Launch an instance' wizard. In the 'Key pair (login)' section, a new key pair 'hb-test-001' is being created. In the 'Network settings' section, a new security group 'launch-wizard-2' is being created with rules for SSH and HTTPS traffic. On the right, a summary panel shows the configuration: 1 instance, Software Image (AMI) set to 'Amazon Linux 2023 AMI 2023.6.2...', Virtual server type set to 't2.micro', and Storage (volumes) set to 1 volume(s) - 8 GiB. A callout box highlights the 'Free tier' information: 'In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.'



- g. After creating the key pair, **download it and save it in a folder.**
- h. After creating the key pair, click on launch instance as shown below



- i. After clicking launch instance you can see the following screen. This means the instance has been created.

The screenshot shows the AWS EC2 Instances Launch log page. At the top, there's a green success message: "Successfully initiated launch of instance (i-089f0bb0152cabe9e)". Below this, there's a "Next Steps" section with several options:

- Create billing and free tier usage alerts**: To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds. Includes a "Create billing alerts" button.
- Connect to your instance**: Once your instance is running, log into it from your local computer. Includes a "Connect to instance" button and a "Learn more" link.
- Connect an RDS database**: Configure the connection between an EC2 instance and a database to allow traffic flow between them. Includes a "Connect an RDS database" button and a "Create a new RDS database" link.
- Create EBS snapshot policy**: Create a policy that automates the creation, retention, and deletion of EBS snapshots. Includes a "Create EBS snapshot policy" button.
- Manage detailed monitoring**: Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period. Includes a "Create Load Balancer" button.
- Create Load Balancer**: Create a application, network gateway or classic Elastic Load Balancer. Includes a "Create Load Balancer" button.
- Create AWS budget**: AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location. Includes a "Create AWS budget" button.
- Manage CloudWatch alarms**: Create or update Amazon CloudWatch alarms for the instance. Includes a "Manage CloudWatch alarms" button.

- j. The screen below shows the created instance.

The screenshot shows the AWS EC2 Instances page. The left sidebar includes navigation links for Dashboard, EC2 Global View, Events, Instances (selected), Images, Elastic Block Store, Network & Security, and Volumes. The main content area displays the "Instances (1) Info" table with one row:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv-
hb-test-001	i-089f0bb0152cabe9e	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-3-110

Below the table, there's a "Select an instance" dropdown menu.

3. Connect to EC2 using Command line and Create user and group

1. Go to EC2 Home Page after logging into AWS
2. Click on the EC2 instance you want to use to connect via command line as shown below

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like Dashboard, EC2 Global View, Events, Instances (selected), Images, Elastic Block Store, Network & Security, and KMS. The main area displays a table titled 'Instances (1/1) info'. A single instance, 'hb-test-001', is listed with the following details:

- Instance ID: i-089f0bb0152cabe9e
- Instance state: Running
- Instance type: t2.micro
- Status check: 2/2 checks passed
- Alarm status: View alarms
- Availability Zone: ap-south-1b
- Public IP: ec2-3-110

Below the table, a specific instance ('i-089f0bb0152cabe9e (hb-test-001)') is selected. The 'Details' tab is active, showing:

- Instance ID: i-089f0bb0152cabe9e
- Public IPv4 address: 3.110.92.252 | open address
- Private IPv4 addresses: 172.31.9.29
- IPv6 address: -
- Instance state: Running
- Private IP DNS name (IPv4 only): ec2-3-110-92-252.ap-south-1.compute.amazonaws.com | open address
- Hostname type: Private IP DNS name (IPv4 only)

3. Select the insurance by clicking the check box before the name
4. You shall see all the setting of that instance just below the instance list
5. From the Details tab copy the Public IPv4 address and save it somewhere
6. Now open the command line tool you use and switch to the directory where you saved the .PEM file(key pairs of EC2 downloaded in Section 2)
 - a. Use **ls -a** command to list out all the directories in the path
 - b. Use **cd** command to switch to the directory wherever you have save the PEM file(you might end up using it multiple times)
7. From the command line use the following command in the order they are mentioned and also refer to the screenshot for the usage
 - a. Connect to EC2
 - i. Format: ssh -i {{keypair_file_name}} ec2-user@public IPV4 address
 - ii. Actual Usage: ssh -i hb-test-001-ec2-pem.pem ec2-user@65.0.73.25

b. Creating User from Command Line

i. Format: aws iam create-user --user-name {{username}}

ii. Actual Usage: aws iam create-user --user-name mhbtst1

c. Creating User group from Command line

i. Format: aws iam create-group --group-name {{groupname}}

ii. Actual Usage: aws iam create-group --group-name test-group-ec2

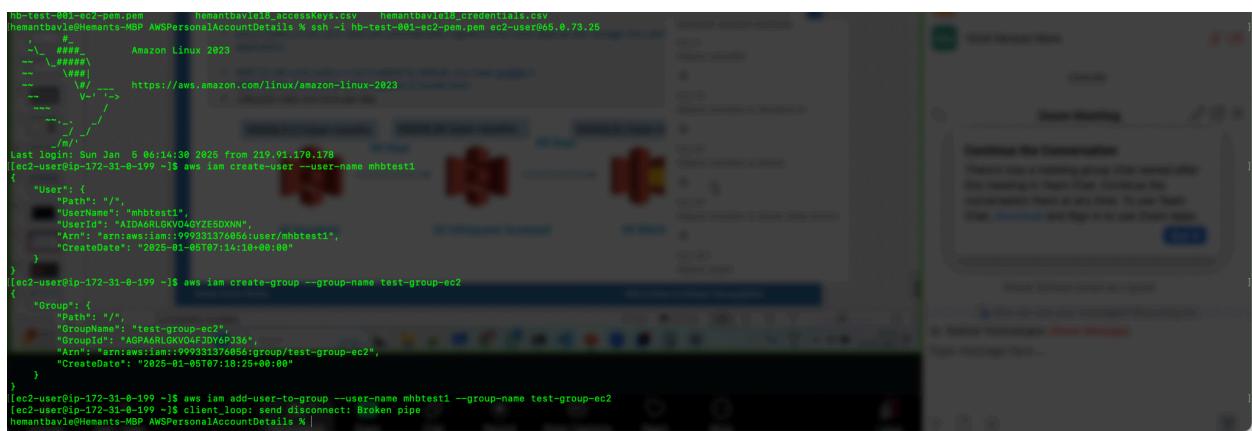
d. Adding User to the group from Command line

i. Format: aws iam add-user-to-group --username {{username}}
--group-name {{groupname}}

ii. Actual Usage: aws iam add-user-to-group --username mhbtst1
--group-name test-group-ec2

e. Screenshot of usage

i.



The screenshot shows a terminal session on an Amazon Linux 2023 system with root privileges. The user is executing AWS IAM commands to create a user, a group, and add the user to the group. The terminal output is as follows:

```
[ec2-user@ip-172-31-0-199 ~]$ aws iam create-user --user-name mhbtst1
{
    "User": {
        "Path": "/",
        "UserName": "mhbtst1",
        "UserId": "AIDAA6RLKV04GYZE6000N",
        "AccessKeyId": "V99332370854:user/mhbtst1",
        "CreateDate": "2025-01-05T07:14:18+00:00"
    }
}[ec2-user@ip-172-31-0-199 ~]$ aws iam create-group --group-name test-group-ec2
{
    "Group": {
        "Path": "/",
        "GroupName": "test-group-ec2",
        "GroupId": "AGPAGRLDKYUFLDyP236",
        "Arn": "arn:aws:iam::999331376856:group/test-group-ec2",
        "CreateDate": "2025-01-05T07:18:25+00:00"
    }
}[ec2-user@ip-172-31-0-199 ~]$ aws iam add-user-to-group --user-name mhbtst1 --group-name test-group-ec2
[ec2-user@ip-172-31-0-199 ~]$ client_loop: send disconnect: Broken pipe
hemantbavie@Hemants-MBP AWSPersonalAccountDetails % |
```

In the background, a browser window is open to the AWS IAM Groups page, showing the newly created 'test-group-ec2' group.

4. Terminating an EC2 Instance

1. Login and Open EC2 Home page as shown below

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, Placement Groups, and Key Pairs. The main content area displays 'Instances (1/1) Info'. A search bar at the top says 'Find Instance by attribute or tag (case-sensitive)'. Below it, a table lists one instance: 'hb-test-001' with Instance ID 'i-089f0bb0152cabe9e', State 'Running', Type 't2.micro', and two checks passed. Buttons for 'Connect', 'Actions', and 'Launch instances' are visible. Below the table, the instance details for 'i-089f0bb0152cabe9e (hb-test-001)' are shown, including its summary, public and private IP addresses, and DNS names.

2. Select the instance from the list > Click on instance state dropdown

This screenshot is similar to the previous one, showing the EC2 Instances page. However, the 'Actions' dropdown menu is open over the instance table, revealing options: Stop instance, Start instance, Reboot instance, Hibernate instance, and Terminate (delete) instance. The rest of the interface and instance details are identical to the first screenshot.

3. Click on Stop Instance and you will see a similar screen instance state changed to stopped for the selected instance

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like Dashboard, EC2 Global View, Events, Instances (selected), Images, Elastic Block Store, Network & Security, and more. The main content area shows a table of instances. One instance, 'hb-test-001' with ID 'i-089f0bb0152cabe9e', is highlighted. Its status is listed as 'Stopped'. Below the table, a detailed view for 'hb-test-001' is shown, including its instance ID, public and private IP addresses, and security group information.

4. Click on Instance State again like Step 2, and click on Stop Instance and you will see the screens as shown below in the screen shot.

This screenshot shows the same AWS EC2 Instances page as the previous one, but the instance 'hb-test-001' is now listed as 'Running'. The 'Actions' dropdown menu is open, and the 'Stop instance' option is highlighted. The detailed view for the instance shows its current running status along with its network and security details.

The screenshot shows the AWS EC2 Instances page. A green banner at the top indicates "Successfully initiated termination (deletion) of i-089f0bb0152cabe9e". The main table lists one instance:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
hb-test-001	i-089f0bb0152cabe9e	Shutting-down	t2.micro	2/2 checks passed	View alarms	ap-south-1b	-

The instance details page for "i-089f0bb0152cabe9e (hb-test-001)" is shown. The "Details" tab is selected. The "Instance summary" section contains the following information:

Instance ID	Public IPv4 address	Private IPv4 addresses
i-089f0bb0152cabe9e	-	172.31.9.29
IPv6 address	Instance state	Public IPv4 DNS
-	Shutting-down	-
Hostname type	Private IP DNS name (IPv4 only)	
IP name: ip-172-51-9-29.ap-south-1.compute.internal	ip-172-51-9-29.ap-south-1.compute.internal	

5. Click on search bar > Type Security Group > Delete the Security group as well that was created during instance creation else it might get reflected in your billing.

3. CREATING A CUSTOM ROLE IN IAM

A. Using AWS Service

1. Login into AWS Console. Based on your history of using the service, you can see the options to open different services. You can also use the search bar at the top to look for IAM service and then click on it to open its home page.

The screenshot shows the AWS Console Home page. At the top left, there's a search bar with the placeholder "Search" and a "Reset to default layout" button. The top right includes account information ("Asia Pacific (Mumbai) HemantMugdha") and navigation icons. The main area has several sections:

- Recently visited:** IAM, Billing and Cost Management, EC2, AWS Billing Conductor, Lambda.
- Applications:** (0) Info. Region: Asia Pacific (Mumbai). A "Create application" button is available. Below it, a message says "No applications. Get started by creating an application." with a "Create application" link.
- Welcome to AWS:** Getting started with AWS. It features a "Getting started with AWS" icon and a brief description: "Learn the fundamentals and find valuable information to get the most out of AWS." Below this are links for "Tutorials and..." and "Feedback".
- AWS Health:** Info. Shows "Open issues: 0" and "Past 7 days" status. Also shows "Scheduled changes: 0" and "Upcoming and past 7 days" status.
- Cost and usage:** Info. Shows "Current month costs: \$0.55" and "Forecasted month end costs: Data unavailable".

At the bottom, there are links for "CloudShell", "Feedback", and copyright information: "© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

The screenshot shows the AWS IAM service page. At the top left, there's a search bar with the placeholder "Search" and a "Reset to default layout" button. The top right includes account information ("Asia Pacific (Mumbai) HemantMugdha") and navigation icons. The main area has two main sections:

- Services:** A list of services including IAM (selected), IAM Identity Center, Resource Access Manager, and AWS App Mesh. Each service item has a "Show more" link.
- Features:** A list of features including Groups (IAM feature), Roles (IAM feature), and Identity providers (IAM feature).

At the bottom, there's a question "Were these results helpful?" with "Yes" and "No" buttons. On the right side, there's a sidebar with a "Find applications" search bar, a "Create application" button, and a "Cost (\$)" chart.

2. Click On IAM. You will land on the screen similar to below

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with navigation links like 'Identity and Access Management (IAM)', 'Dashboard', 'Access management', 'Access reports', and 'AWS Organizations'. The main area displays the following information:

- Security recommendations:**
 - Root user has MFA (Having multi-factor authentication (MFA) for the root user improves security for this account.)
 - Root user has no active access keys (Using access keys attached to an IAM user instead of the root user improves security.)
- IAM resources:** Shows 4 User groups, 3 Users, 4 Roles, 0 Policies, and 0 Identity providers.
- What's new:** Lists recent changes:
 - Introducing resource control policies (RCPs) to centrally restrict access to AWS resources. 2 months ago
 - AWS IAM now supports PrivateLink in the AWS GovCloud (US) Regions. 2 months ago
 - Streamline automation of policy management workflows with service reference information. 3 months ago
 - Amazon S3 Access Grants introduce the ListCallerAccessGrants API. 5 months ago
- AWS Account:** Displays Account ID (999331376056), Account Alias (Create), and Sign-in URL for IAM users in this account (<https://999331376056.signin.aws.amazon.com/> console).
- Quick Links:** My security credentials (Manage your access keys, multi-factor authentication (MFA) and other credentials).
- Tools:** Policy simulator (The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify).
- Additional information:** Security best practices in IAM (IAM documentation).

3. Click on the **Roles** menu as highlighted in blue on the left

This screenshot is identical to the one above, showing the AWS IAM Dashboard. The difference is that the 'Roles' link under the 'Access management' section in the sidebar is highlighted in blue, indicating it has been selected.

4. If you have some roles already created, then the landing page will look like below.

The screenshot shows the AWS IAM Roles page. The left sidebar includes sections for Identity and Access Management (IAM), Access management, Access reports, and IAM Identity Center/AWS Organizations. The main content area displays a table of roles with columns for Role name, Trusted entities, and Last activity. There are four entries:

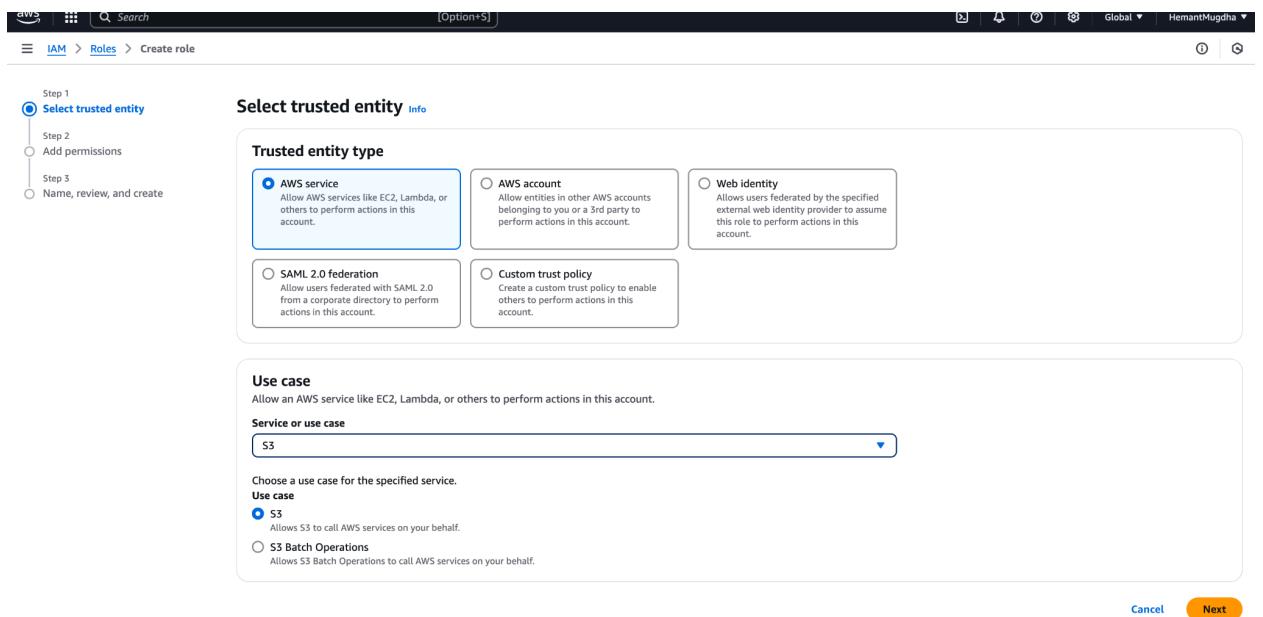
Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	407 days ago
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
cli-test-role	AWS Service: ec2	13 days ago
code-build-main	AWS Service: codebuild	-

Below the table, there are two sections: "Access AWS from your non AWS workloads" and "X.509 Standard". A "Temporary credentials" section is also present.

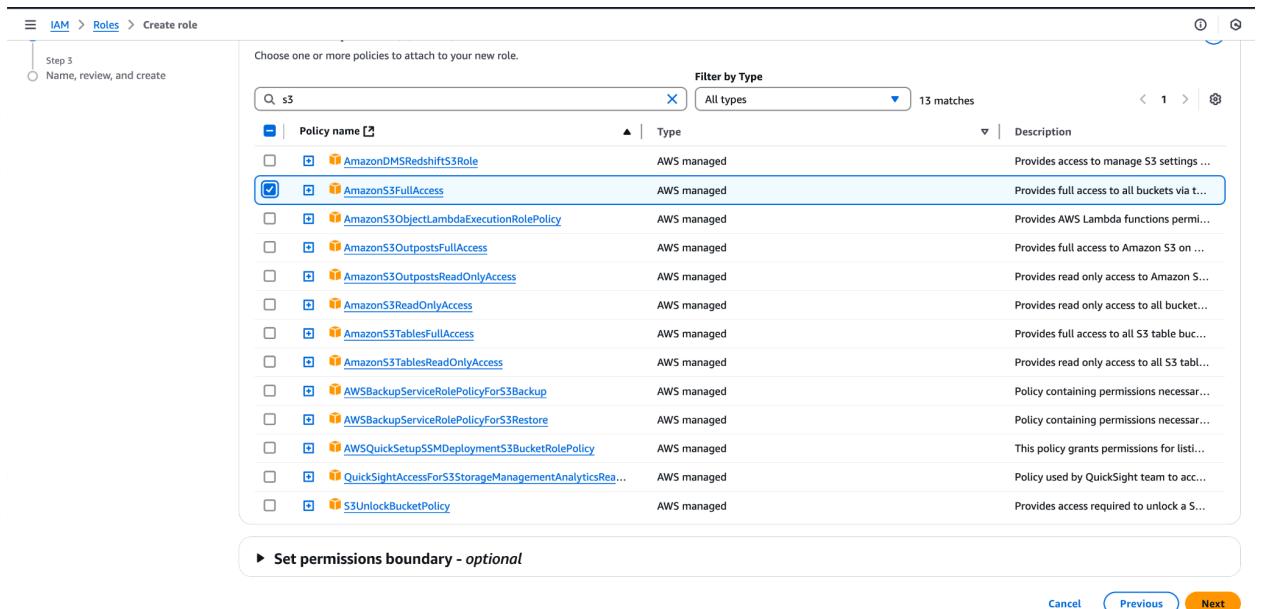
5. To create a new role, click on Create Role button.

This screenshot is identical to the one above, showing the AWS IAM Roles page with four existing roles. The "Create role" button at the top right of the main content area is highlighted in orange, indicating it is the next step to take.

6. On clicking the Create Role button, you shall see the following screen. We will work on creating a role, which can be used by an AWS's service itself.



7. On clicking next button in Step 6 above, you can see the following window. Select a policy > Click next



8. On clicking next in the previous step you can see the following screen with JSON of the policy and fields to provide Role name and description. Scroll down and click on **Create Role** button

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
s3-test-role

Maximum 64 characters. Use alphanumeric and `_, ., @, -` characters.

Description
Add a short explanation for this role.
Allows S3 to call AWS services on your behalf.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: `_, ., @, /[\{\}]\\$\%^\`~`

Step 1: Select trusted entities

Trust policy

```

1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Principal": {
7-         "Service": "s3.amazonaws.com"
8-       },
9-       "Action": "sts:AssumeRole"
10-    }
11-  ]
12- }

```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

Step 3: Add tags

Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

Key **Value - optional**

Add new tag

You can add up to 49 more tags.

Cancel **Previous** **Create role**

9. Once a role is successfully created, there will be a green colored notification at the top will show up as shown below:

The screenshot shows the AWS IAM Roles page. At the top, a green notification bar displays the message "Role s3-test-role created." Below this, the "Roles (5) Info" section is visible, stating that an IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust. The main table lists five roles:

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	407 days ago
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
cli-test-role	AWS Service: ec2	13 days ago
code-build-main	AWS Service: codebuild	-
s3-test-role	AWS Service: s3	-

Below the table, there are three sections: "Roles Anywhere" (Info), "Access AWS from your non AWS workloads" (X.509 Standard), and "Temporary credentials". The "Temporary credentials" section includes a note about using AWS Certificate Manager Private Certificate Authority to authenticate identities.

10. You can select a role and click on it to open the role details as shown in screenshots below

The screenshot shows the AWS IAM Roles page. On the left, there's a navigation sidebar with options like Dashboard, Access management (selected), Roles (selected), Policies, Identity providers, Account settings, Root access management, Access reports, and more. The main content area displays a table of roles:

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	407 days ago
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
cli-test-role	AWS Service: ec2	13 days ago
code-build-main	AWS Service: codebuild	-
s3-test-role	AWS Service: s3	-

Below the table, there are sections for "Roles Anywhere" and "Access AWS from your non AWS workloads".

This screenshot shows the detailed view for the "s3-test-role". The left sidebar is identical to the previous one. The main content area includes:

- Summary** section with Creation date (January 20, 2025, 01:01 (UTC+05:30)), Last activity (-), ARN (arn:aws:iam::399331376056:role/s3-test-role), and Maximum session duration (1 hour).
- Permissions** tab selected, showing one policy attached: "AmazonS3FullAccess" (AWS managed).
- Permissions policies (1)** section with a table for filtering by type.
- Permissions boundary (not set)** section.
- Generate policy based on CloudTrail events** section.

B. USING AWS ACCOUNT

1. Login into AWS Console. Based on your history of using the service, you can see the options to open different services. You can also use the search bar at the top to look for IAM service and then click on it to open its home page.

aws | Search [Option+S] | Asia Pacific (Mumbai) | HemantMugdha | ⓘ | ⓘ

Console Home Info

Recently visited Info

- IAM
- Billing and Cost Management
- EC2
- AWS Billing Conductor
- Lambda

[View all services](#)

Applications (0) Info

Region: Asia Pacific (Mumbai)

ap-south-1 (Current Region) ▼

Name	Description	Region	Originati.
No applications Get started by creating an application.			

[Create application](#)

[Go to myApplications](#)

Welcome to AWS

Getting started with AWS Info

Learn the fundamentals and find valuable information to get the most out of AWS.

[Tutorials and](#)

AWS Health Info

Open issues 0 Past 7 days

Scheduled changes 0 Upcoming and past 7 days

Cost and usage Info

Current month costs \$0.55

Forecasted month end costs Data unavailable

Cost (\$) 1 0

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

CloudShell Feedback

aws | IAM | Search X | Asia Pacific (Mumbai) | HemantMugdha | ⓘ | ⓘ

IAM

Services

- IAM Manage access to AWS resources
- IAM Identity Center Manage workforce user access to multiple AWS accounts and cloud applications
- Resource Access Manager Share AWS resources with other accounts or AWS Organizations
- AWS App Mesh Easily monitor and control microservices

Features

- Groups IAM feature
- Roles IAM feature
- Identity providers IAM feature

Were these results helpful?

Applications (0) Info

Region: Asia Pacific (Mumbai)

ap-south-1 (Current Region) ▼

Name	Description	Region	Originati.
No applications Get started by creating an application.			

[Create application](#)

[Go to myApplications](#)

Cost and usage Info

Current month costs \$0.55

Forecasted month end costs Data unavailable

Cost (\$) 1 0

2. Click On IAM. You will land on the screen similar to below

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with navigation links like 'Identity and Access Management (IAM)', 'Dashboard', 'Access management', 'Access reports', and 'AWS Organizations'. The main area displays the following information:

- Security recommendations:**
 - Root user has MFA (Having multi-factor authentication (MFA) for the root user improves security for this account.)
 - Root user has no active access keys (Using access keys attached to an IAM user instead of the root user improves security.)
- IAM resources:** Shows 4 User groups, 3 Users, 4 Roles, 0 Policies, and 0 Identity providers.
- What's new:** Lists recent changes:
 - Introducing resource control policies (RCPs) to centrally restrict access to AWS resources. 2 months ago
 - AWS IAM now supports PrivateLink in the AWS GovCloud (US) Regions. 2 months ago
 - Streamline automation of policy management workflows with service reference information. 3 months ago
 - Amazon S3 Access Grants introduce the ListCallerAccessGrants API. 5 months ago
- AWS Account:** Displays Account ID (999331376056), Account Alias (Create), and Sign-in URL for IAM users in this account (<https://999331376056.signin.aws.amazon.com/> console).
- Quick Links:** My security credentials (Manage your access keys, multi-factor authentication (MFA) and other credentials).
- Tools:** Policy simulator (The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify).
- Additional information:** Security best practices in IAM (IAM documentation).

3. Click on the **Roles** menu as highlighted in blue on the left

This screenshot is identical to the one above, showing the AWS IAM Dashboard. The difference is that the 'Roles' link under the 'Access management' section in the sidebar is highlighted in blue, indicating it has been selected.

4. If you have some roles already created, then the landing page will look like below.

The screenshot shows the AWS IAM Roles page. The left sidebar includes sections for Identity and Access Management (IAM), Access management, Access reports, and IAM Identity Center/AWS Organizations. The main content area displays a table of roles with columns for Role name, Trusted entities, and Last activity. There are four entries:

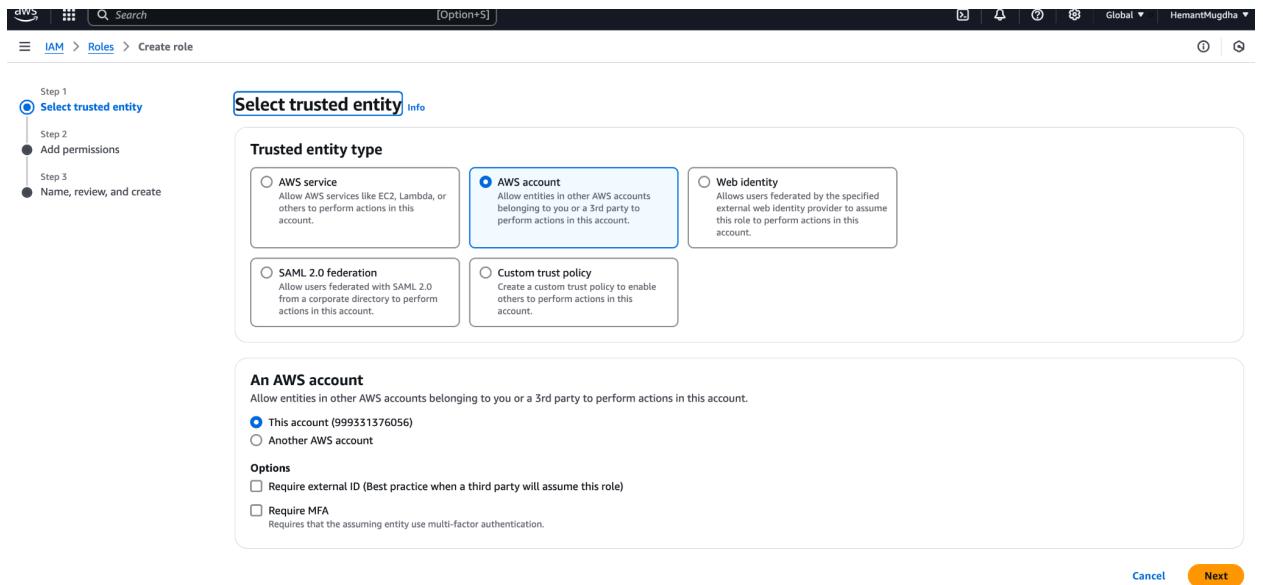
Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	407 days ago
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
cli-test-role	AWS Service: ec2	13 days ago
code-build-main	AWS Service: codebuild	-

Below the table, there are two sections: "Access AWS from your non AWS workloads" and "X.509 Standard". A "Temporary credentials" section is also present.

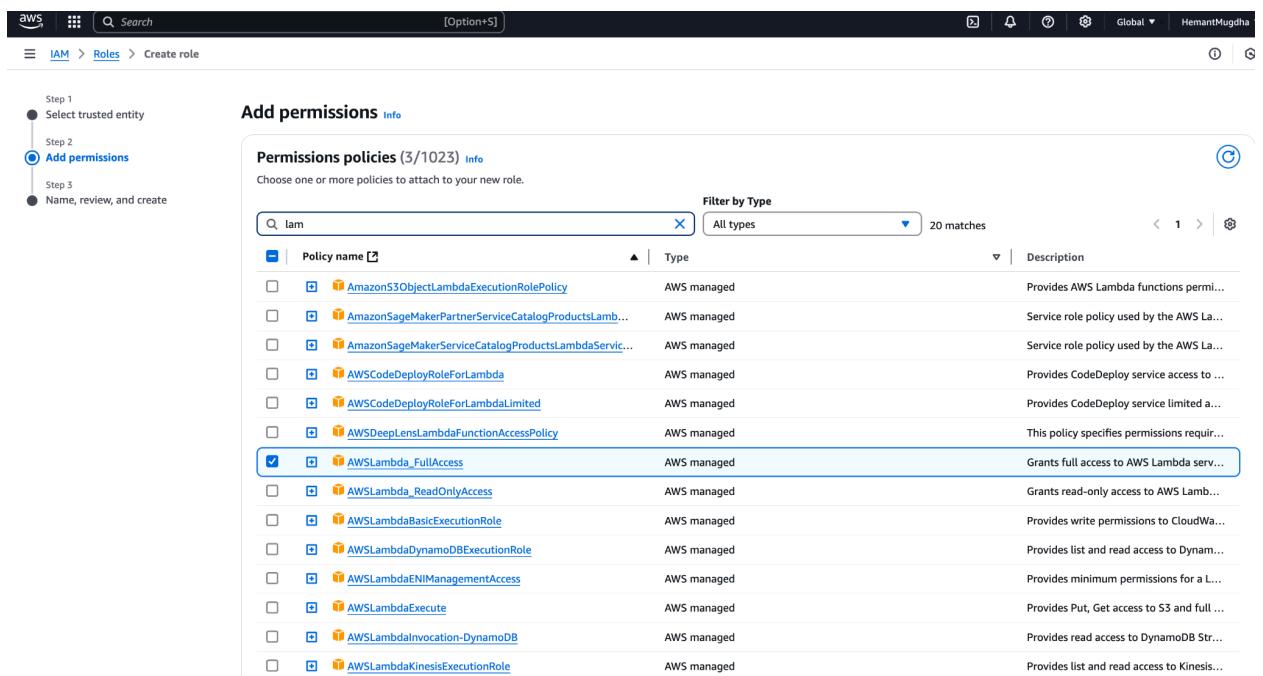
5. To create a new role, click on Create Role button.

This screenshot is identical to the one above, showing the AWS IAM Roles page with four existing roles. The "Create role" button at the top right of the main content area is highlighted in orange, indicating it is the target for the next step.

6. On clicking Create Role, screen shown as below shows up, choose AWS Account option and select this Account in “An AWS account” section.



7. To add permission to the role, click next in Step 6 and below screen shows up. Choose the set of permission you want to allow for the role. Click Next after choosing the required permissions.



8. Provide details like role name, tags etc as shown in the screen below and click “Create Role”

Step 1: Name, review, and create

Role details

Role name: test-role-power

Description: (empty)

Step 2: Select trusted entities

Trust policy:

```

1 ~ {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Principal": {
8         "AWS": "999331376056"
9       },
10      "Condition": {}
11    }
12  ]
13 }

```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonEC2FullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy
AWSLambda_FullAccess	AWS managed	Permissions policy

Step 3: Add tags

Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create role](#)

9. The confirmation screen of successful role creation is shown below

The screenshot shows the AWS Identity and Access Management (IAM) service. On the left, there's a navigation sidebar with options like Dashboard, Access management, Access reports, and IAM Identity Center. The main area is titled 'Roles (6)' and shows a list of six roles: AWSServiceRoleForSupport, AWSServiceRoleForTrustedAdvisor, cli-test-role, code-build-main, s3-test-role, and test-role-power. A green banner at the top says 'Role test-role-power created.' Below the table, there are sections for 'Roles Anywhere' (with a note about X.509 Standard), 'Access AWS from your non AWS workloads' (with a note about using X.509 certificates), and 'Temporary credentials' (with a note about using temporary credentials for enhanced security).

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	410 days ago
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
cli-test-role	AWS Service: ec2	16 days ago
code-build-main	AWS Service: codebuild	-
s3-test-role	AWS Service: s3	-
test-role-power	Account: 999331376056	-