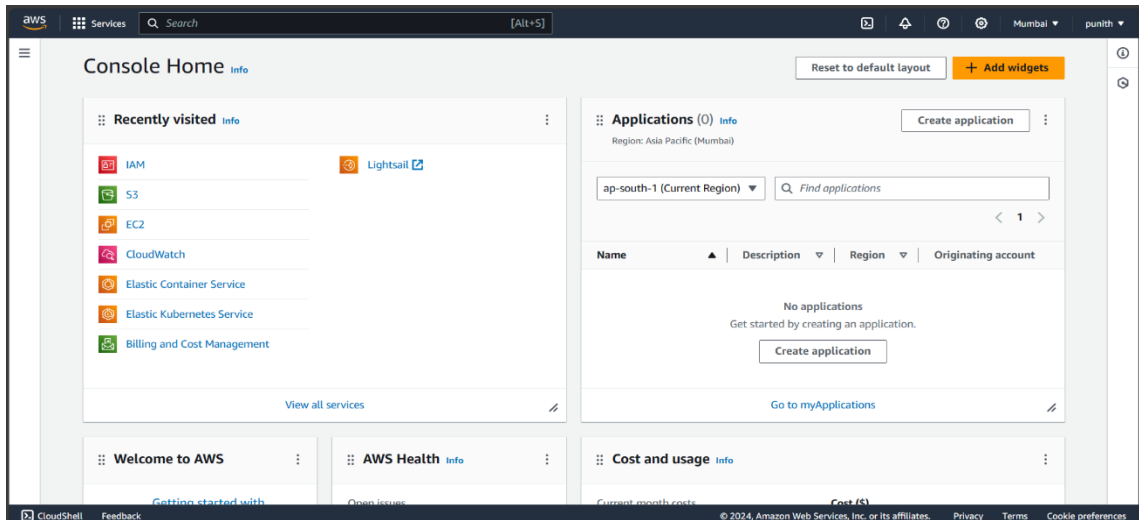


AWS IAM (Identify Access Management)

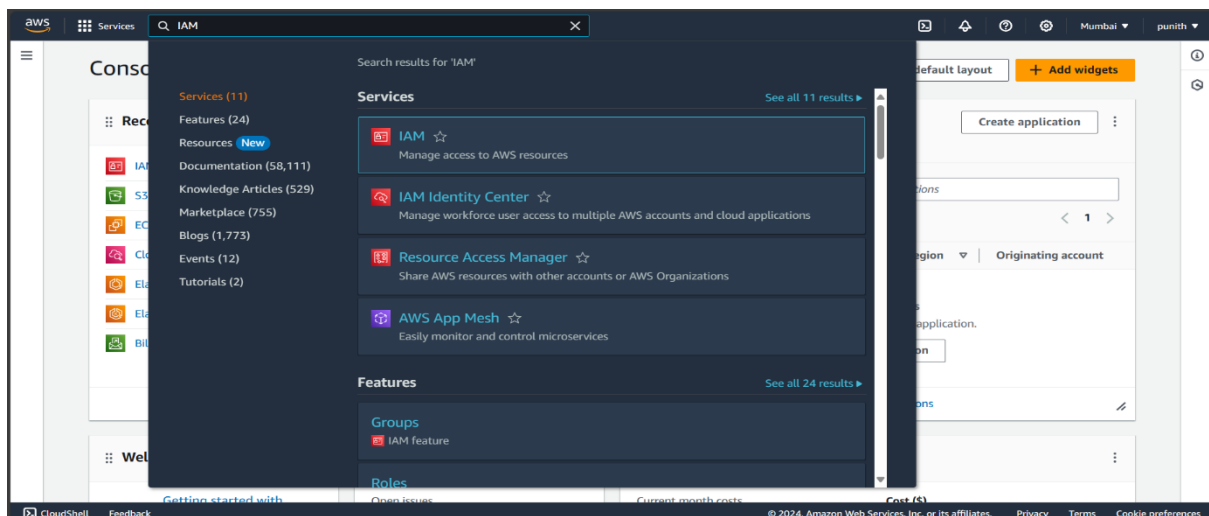
- IAM (Identify Access Management) is a service in AWS (Amazon Web Services) that provides user-level configurations for the user from root account. It is actually all about Authentication and Authorization and it also provides four set of actions to perform in the AWS cloud platform. They are:
 - 1) Users
 - 2) Policies
 - 3) Groups
 - 4) Roles
- Users: Users are those who can access the services for some extent with few set of permissions and policies that are made by admin i.e root user. For example, if a user wants to access the EC2 services, then the root user provides the permissions to access the EC2 and perform few set of actions like creating instances, launching instances.
- Policies: Policies are the set of permissions that are given to user account in IAM. They let the users to perform any action in the entire AWS account.
- Groups: In IAM, Groups are combined of multiple users that can perform the actions in AWS and the permissions are given easily to users. For example, if a organization has the three teams i.e Dev, QA, Production then we have different groups for each team and it makes easier to add users to respective groups.
- Roles: Roles are way similar to the users and it also helps to create user with specific permissions for temporary uses. It also can be created outside the AWS account and can access another AWS account i.e Cross-Account Access.

- Now , we see the hands-on with IAM and the photos has been attached below:

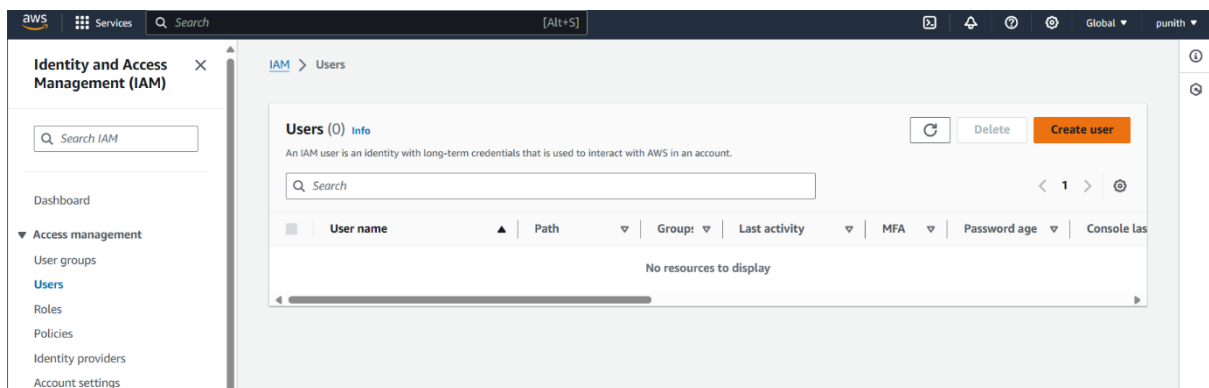
Login to AWS console.



Search for IAM service.



This is IAM interface and Now click on Create User to create a user .



Name the User and Check the box to create a IAM user.

The screenshot shows the 'Specify user details' step in the AWS IAM console. The left sidebar lists the steps: Step 1: Specify user details (active), Step 2: Set permissions, Step 3: Review and create, and Step 4: Retrieve password. The main content area is titled 'Specify user details' and contains a 'User details' section. In the 'User name' field, 'Dev' is entered. Below it, a note states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , @ _ - (hyphen)'. A checkbox labeled 'Provide user access to the AWS Management Console - optional' is checked, with a note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' Below this is a blue information box titled 'Are you providing console access to a person?' with two options: 'Specify a user in Identity Center - Recommended' (unselected) and 'I want to create an IAM user' (selected). The 'Console password' section at the bottom has two options: 'Autogenerated password' (selected) and 'Custom password' (unselected). At the bottom right, there are 'Cancel' and 'Next' buttons.

Make it autogenerated password for the first time and click on Next.

This screenshot shows the 'Console password' section of the AWS IAM console. It features two radio buttons: 'Autogenerated password' (selected) and 'Custom password' (unselected). Below the 'Custom password' option is a text input field and a list of requirements: 'Must be at least 8 characters long' and '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) = [] { } | ' '. There is also a 'Show password' checkbox. A checked checkbox states 'Users must create a new password at next sign-in - Recommended', with a note: 'Users automatically get the IAMUserChangePassword policy to allow them to change their own password.' A blue information box at the bottom explains that if creating programmatic access, credentials can be generated after the user is created, with a 'Learn more' link. At the bottom right, there are 'Cancel' and 'Next' buttons.

Set permission and select the policies that are to be given to user.

The screenshot shows the 'Set permissions' step in the AWS IAM console. The left sidebar lists the steps: Step 1: Specify user details, Step 2: Set permissions (active), Step 3: Review and create, and Step 4: Retrieve password. The main content area is titled 'Set permissions' and includes a sub-header 'Permissions options'. There are three radio buttons: 'Add user to group' (unselected), 'Copy permissions' (unselected), and 'Attach policies directly' (selected). Below these is a section titled 'Permissions policies (1187)' with a search bar and a 'Filter by Type' dropdown set to 'All types'. A table lists available policies, with 'AccessAnalyzerServiceRolePolicy' and 'AdministratorAccess' visible. At the bottom right, there are 'Cancel' and 'Next' buttons.

Search for EC2 and Check on to the policy and click on Next.

Permissions policies (1/1187) Refresh Create policy

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

Filter by Type

Search: ec2full × All types 1 match

| <input checked="" type="checkbox"/> | Policy name | Type | Attached entities |
|-------------------------------------|---------------------|-------------|-------------------|
| <input checked="" type="checkbox"/> | AmazonEC2FullAccess | AWS managed | 0 |

► Set permissions boundary - optional

Cancel Previous Next

Review the details and click on Create User.

User details

| | | |
|------------------|--|-------------------------------|
| User name Dev | Console password type Autogenerated | Require password reset Yes |
|------------------|--|-------------------------------|

Permissions summary < 1 >

| Name | Type | Used as |
|-----------------------|-------------|--------------------|
| AmazonEC2FullAccess | AWS managed | Permissions policy |
| 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

After creating user, you receive the password and account ID of the user.

[IAM](#) > [Users](#) > Create user

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 Email sign-in instructions

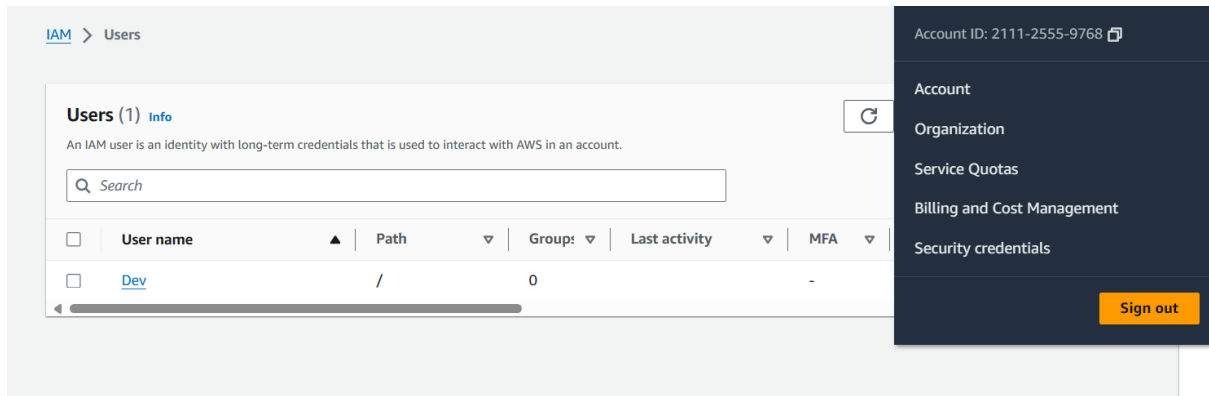
Console sign-in URL
 <https://21112559768.signin.aws.amazon.com/console>

User name
 Dev

Console password
 ***** [Show](#)

Cancel Download .csv file Return to users list

Sign out from the Root account and try logging with the user created now from IAM console.



Enter the details and sign in into IAM console.



Sign in as IAM user

Account ID (12 digits) or account alias

211125559768

IAM user name

Dev

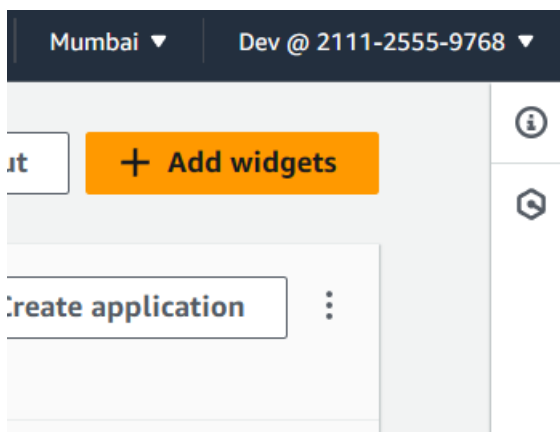
Password

.....

☐ Remember this account

Sign in

You can see , The user Dev is successfully logged into the IAM console.



Go to EC2 and Launch an instance. Name the instance.

EC2 > Instances > Launch an instance

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

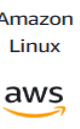
 [Add additional tags](#)


Select the OS images and version of the OS.


▼ Application and OS Images (Amazon Machine Image) [Info](#)


An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below


Quick Start
















[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
ami-007020fd9c84e18c7 (64-bit (x86)) / ami-09c443d9277298026 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

Create a key-pair for the instance. We will discuss deeply about OS instance type and key-pairs in the session of EC2.

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

ec2-instance-keypair

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Cancel

Create key pair

Create a security group and allow all protocols.

▼ Network settings Info

Edit

Network Info

vpc-0a86523624e51656e

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

We'll create a new security group called 'launch-wizard-2' with the following rules:

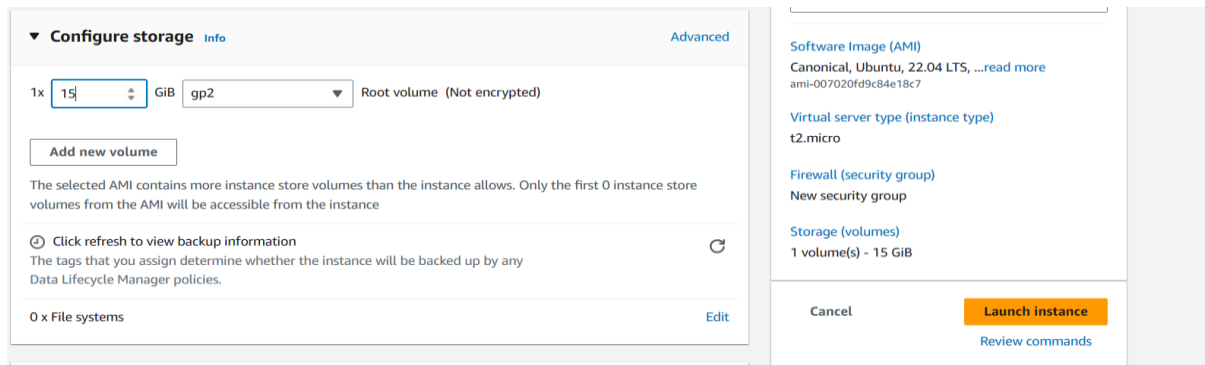
☒ Allow SSH traffic from
Helps you connect to your instance

Anywhere
0.0.0.0/0

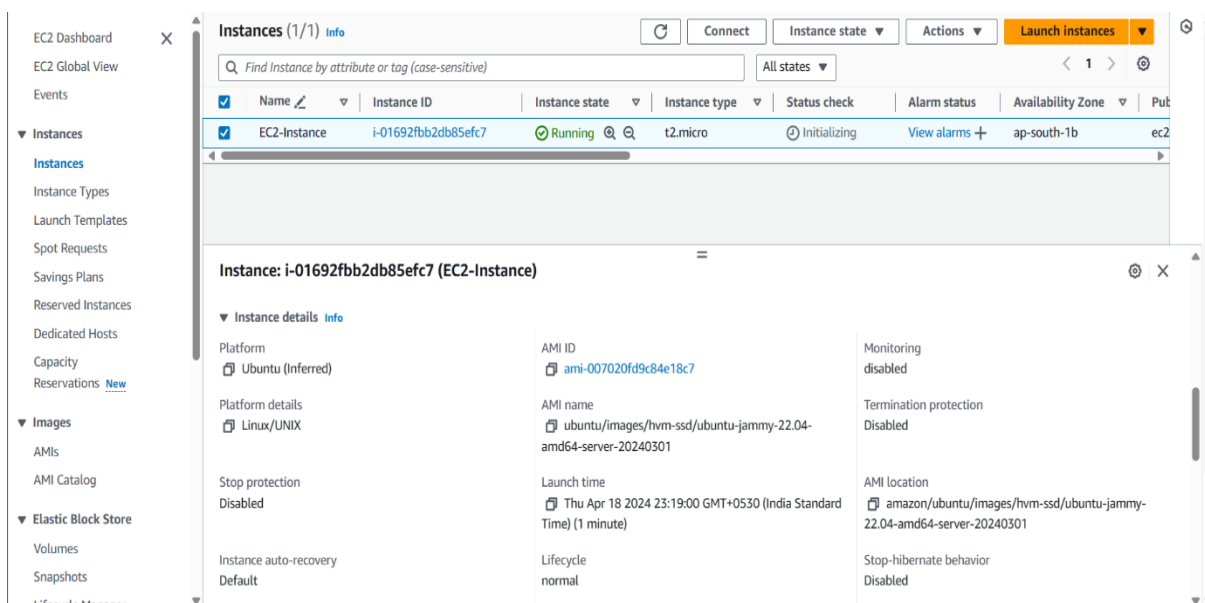
☒ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

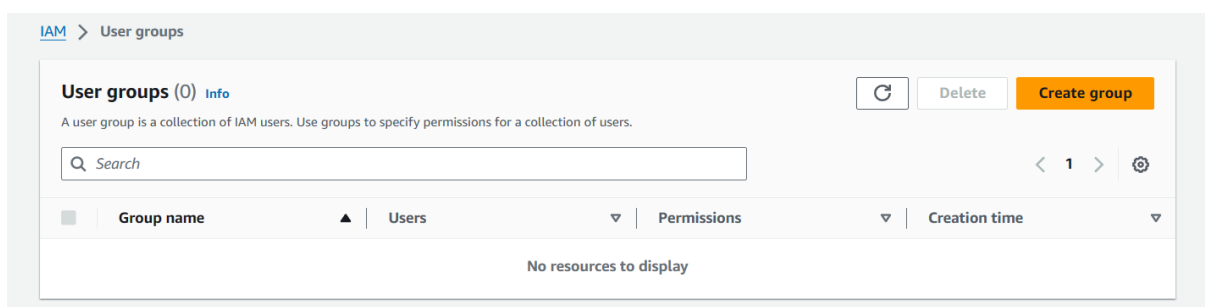
Select the size of the volume and Click on launch instance.



You can see, We have launched an instance but few permissions are disabled for the user Dev.



Now , sign out from user Dev and comeback to Root account and Open IAM to create Groups for Users.



Name the Group and select the users that you want to add in the group. Here, I have created two users and added them to Developer Group.

IAM > User groups > Create user group

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

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

Add users to the group - Optional (2/2) [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.

| <input checked="" type="checkbox"/> | User name ? | Groups | Last activity | Creation time |
|-------------------------------------|-----------------------------|--------|----------------|----------------|
| <input checked="" type="checkbox"/> | Dev | 0 | 16 minutes ago | 20 minutes ago |
| <input checked="" type="checkbox"/> | Dev2 | 0 | None | Now |

Attach the policy permissions to the group like EKS , EC2 permissions.
Click on Create Group.

Attach permissions policies - Optional (2/919) [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type 8 matches

| <input type="checkbox"/> | Policy name | Type | Used as | Description |
|-------------------------------------|-----------------------|-------------|---------|--|
| <input type="checkbox"/> | AmazonEKS_CNI_P... | AWS managed | None | This policy provides the Amazon VPC ... |
| <input type="checkbox"/> | AmazonEKSCluster... | AWS managed | None | This policy provides Kubernetes the pe... |
| <input type="checkbox"/> | AmazonEKSFargate... | AWS managed | None | Provides access to other AWS service r... |
| <input type="checkbox"/> | AmazonEKSLocalQ... | AWS managed | None | This policy provides permissions to EK... |
| <input checked="" type="checkbox"/> | AmazonEKSService... | AWS managed | None | This policy allows Amazon Elastic Cont... |
| <input type="checkbox"/> | AmazonEKSVPCRes... | AWS managed | None | Policy used by VPC Resource Controlle... |
| <input type="checkbox"/> | AmazonEKSWorker... | AWS managed | None | This policy allows Amazon EKS worker ... |
| <input type="checkbox"/> | AWSFaultInjectionS... | AWS managed | None | This policy grants the Fault Injection Si... |

After creating, You can view the group and the Users, Permissions in the group

Developer [Info](#)

Summary

| | | |
|------------------------------|--|--|
| User group name Developer | Creation time April 18, 2024, 23:31 (UTC+05:30) | ARN arn:aws:iam::211125559768:group/Developer |
|------------------------------|--|--|

[Users \(2\)](#) | [Permissions](#) | [Access Advisor](#)

Users in this group (2)

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

| <input type="checkbox"/> | User name ? | Groups | Last activity | Creation time |
|--------------------------|-----------------------------|--------|----------------|----------------|
| <input type="checkbox"/> | Dev | 1 | 18 minutes ago | 22 minutes ago |
| <input type="checkbox"/> | Dev2 | 1 | None | 1 minute ago |

