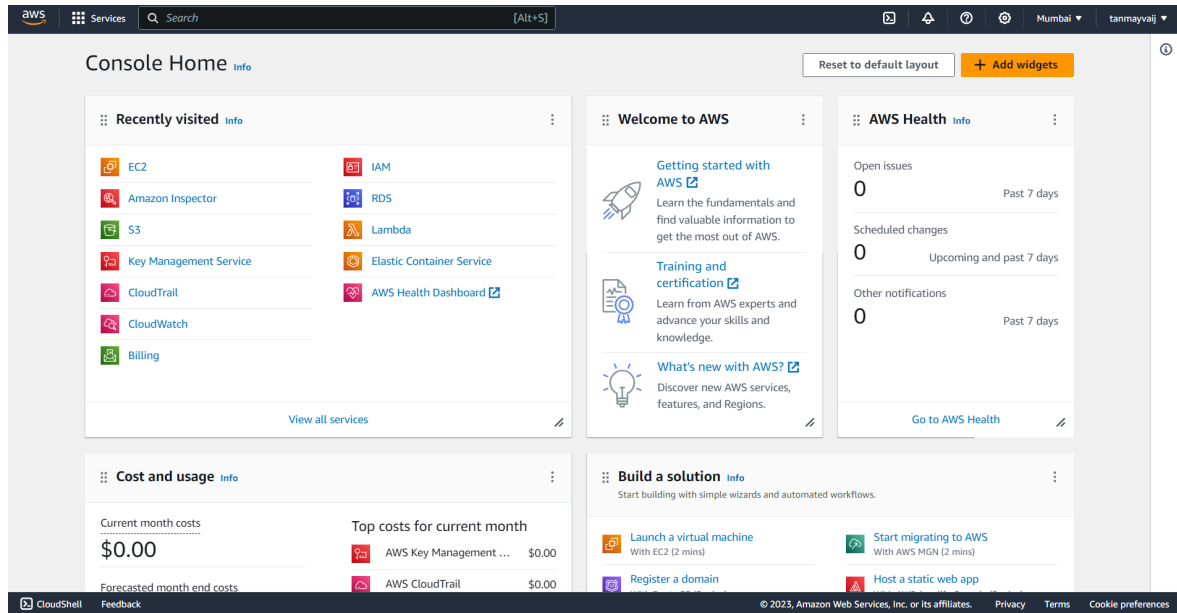
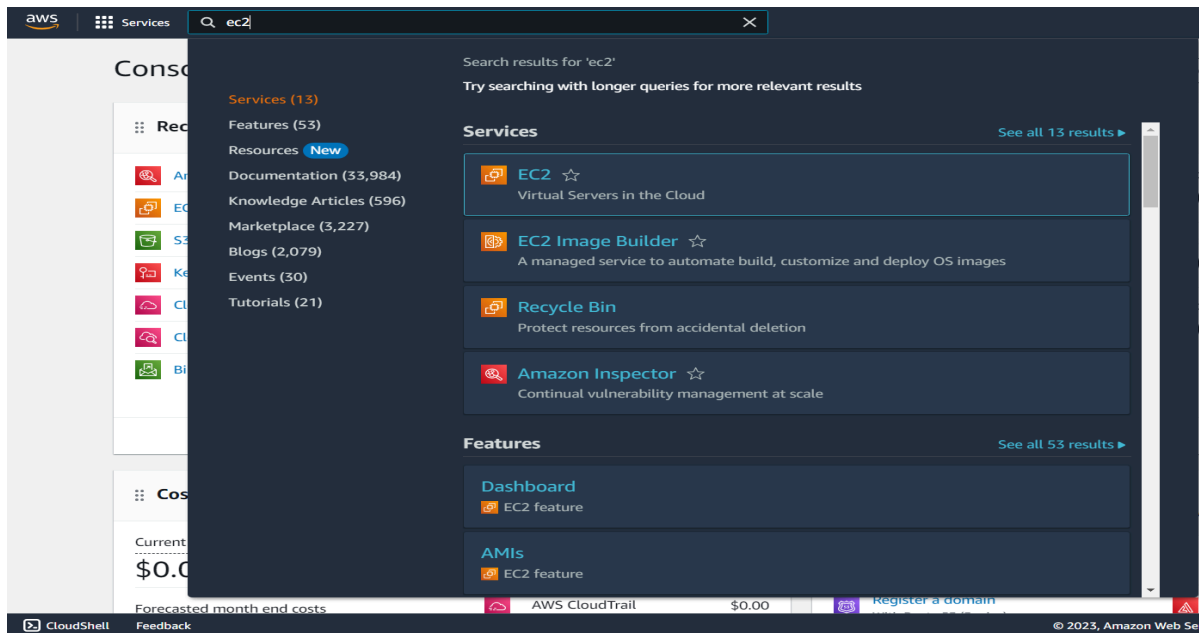


# Demonstration of AWS Load Balancer

1. Sign in to the AWS console.



2. Search for EC2 and click on the EC2 tab.



3. Click and open the instance dashboard by clicking on “Instances” in the “Resources” card.

**EC2 Dashboard** ×

EC2 Global View  
Events

▼ **Instances**

- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity Reservations
- New

▼ **Images**

- AMIs
- AMI Catalog

▼ **Elastic Block Store**

- Volumes
- Snapshots
- Lifecycle Manager

▼ **Network & Security**

- Security Groups

**Resources** EC2 Global view ⚙️ 🔄

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0	Key pairs	1
Load balancers	0	Placement groups	0	Security groups	2
Snapshots	0	Volumes	0		

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) ▼

[Migrate a server](#) 🔗

Note: Your instances will launch in the Asia Pacific (Mumbai) Region

**Scheduled events** 🔄

**Service health**

[AWS Health Dashboard](#) 🔗 🔄

Region  
Asia Pacific (Mumbai)

**Zones**

Zone name	Zone ID
ap-south-1a	aps1-az1
ap-south-1b	aps1-az3
ap-south-1c	aps1-az2

CloudShell Feedback © 2023, Amazon

4. Click on “Launch instances”.

**Instances** Info 🔄 Connect Instance state ▼ Actions ▼ Launch instances ▼

1 ⚙️

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
No instances							
You do not have any instances in this region							

[Launch instances](#)

5. Give a name to the instance

**Name and tags** Info

Name

[Add additional tags](#)

## 6. Select the OS Image

▼ **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

Q Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Li

SUSE

Q

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

Free tier eligible ▼

ami-0287a05f0ef0e9d9a (64-bit (x86)) / ami-0b6581fde9e6e7779 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-09-19

Architecture

AMI ID

64-bit (x86) ▼

ami-0287a05f0ef0e9d9a

Verified provider

## 7. Create a key pair or select one if it is already created.

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

root ▼

↻ Create new key pair

8. Create a security group or select an existing one. ( https, http, ssh should be given anywhere access ).

▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-0dbe7bc3f6036f9b4

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

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

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

×

9. Enter the number of instances to create.

▼ Summary

Number of instances [Info](#)

When launching more than 1 instance, [consider EC2 Auto Scaling](#)

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...[read more](#)  
ami-0287a05f0ef0e9d9a

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

❏ Free tier: 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

×

Cancel

Launch instance

[Review commands](#)

10. Rename these instances to identify them uniquely and wait till each instance passes the status check. Then select one instance and click connect.

Instances (3) <a href="#">Info</a>									
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>									
<div><div>Refresh</div><div>Connect</div><div>Instance state ▼</div><div>Actions ▼</div><div>Launch instances ▼</div></div>									
<div>&lt; 1 &gt; ⚙</div>									
<input type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	
<input type="checkbox"/>	VM-1	i-00a180ce361e36ea0	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	ec2-15-207-106-	
<input type="checkbox"/>	VM-2	i-0e3c070e37c16eef6	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	ec2-43-205-231-	
<input type="checkbox"/>	VM-3	i-0871f2de8eb75403d	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	ec2-3-110-62-33	

11. Simply click “Connect” and a terminal will open.

[EC2](#) > [Instances](#) > [i-00a180ce361e36ea0](#) > Connect to instance

## Connect to instance [Info](#)

Connect to your instance i-00a180ce361e36ea0 (VM-1) using any of these options


EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID


 i-00a180ce361e36ea0 (VM-1)

Connection Type

☒ **Connect using EC2 Instance Connect**  
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.


☐ **Connect using EC2 Instance Connect Endpoint**  
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address

 15.207.106.97

User name

Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ubuntu.

 **Note:** In most cases, the default user name, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel

Connect

12. Enter the command “`sudo apt update -y && sudo apt install apache2 -y && sudo echo '<h1>Instance VM-1</h1>' | sudo tee /var/www/html/index.html`”. Repeat the same steps with the other two instances.

```
System information as of Wed Nov 22 14:33:40 UTC 2023

System load:  0.01904296875   Processes:      101
Usage of /:   20.5% of 7.57GB   Users logged in: 0
Memory usage: 21%             IPv4 address for eth0: 172.31.33.108
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

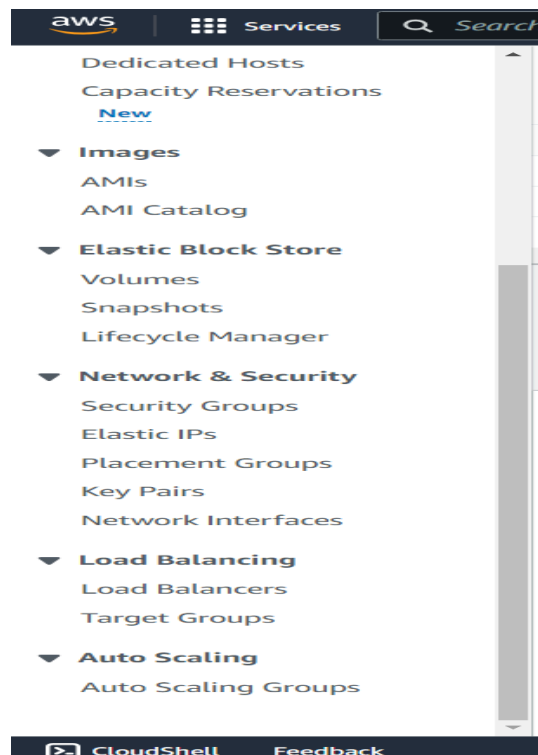
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-33-108:~$ sudo apt update -y && sudo apt install apache2 -y && sudo echo "<h1>Instance VM-1</h1>" | sudo tee /var/www/html/index.html
```

i-00a180ce361e36ea0 (VM-1)

PublicIPs: 15.207.106.97 PrivateIPs: 172.31.33.108

13. Now select ‘Load Balancers’ from the side menu.



14. Click on “Create load balancer”.

### Load balancers

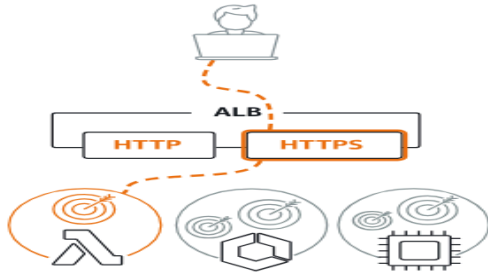
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

< 1 > ⚙

	Name	DNS name	State	VPC ID	Availability Zones	Type	Data
No load balancers							
You don't have any load balancers in ap-south-1							
<button>Create load balancer</button>							

15. Select the “Application Load Balancer”.

### Application Load Balancer [Info](#)



Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Create

16. Enter a name for load balancer.

### Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.



## 17. In the network mapping card select at least two zones.

**Network mapping** [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

**VPC** [Info](#)

Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

-  
vpc-0dbe7bc3f6036f9b4  
IPv4: 172.31.0.0/16

↻

**Mappings** [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

☐ ap-south-1a (aps1-az1)

☐ ap-south-1b (aps1-az3)

☐ ap-south-1c (aps1-az2)

## 18. Select the security group used for instances.

**Security groups** [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

**Security groups**

Select up to 5 security groups

↻

↺

launch-wizard-2  
sg-0cadeaeef47c246a2 VPC: vpc-0dbe7bc3f6036f9b4

×

default  
sg-0b3233960a24871c0 VPC: vpc-0dbe7bc3f6036f9b4

×

## 19. Now create a target group by clicking on “Create target group”.

**Listeners and routing** [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Remove

Protocol

Port

Default action

[Info](#)

HTTP

:

80

Forward to

Select a target group

↻

1-65535

[Create target group](#)

**Listener tags - optional**

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add listener tag

You can add up to 50 more tags.

Add listener

20. Select “Instances” as the target type.

### Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

☒ Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

21. Give a name to the target group.

Target group name

TG

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

22. Select all the instances and click on “Include as pending below” and click on create target group.

Available instances (3/3)

Filter instances

<input checked="" type="checkbox"/>	Instance ID	Name	State	Security groups	Zone
<input checked="" type="checkbox"/>	i-00a180ce361e36ea0	VM-1	Running	launch-wizard-2	ap-sou
<input checked="" type="checkbox"/>	i-0e3c070e37c16eef6	VM-2	Running	launch-wizard-2	ap-sou
<input checked="" type="checkbox"/>	i-0871f2de8eb75403d	VM-3	Running	launch-wizard-2	ap-sou

3 selected

Ports for the selected instances  
Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

Include as pending below

23. Now select the target group in load balancer creation and click on create load balancer

Default action | [Info](#)

Forward to

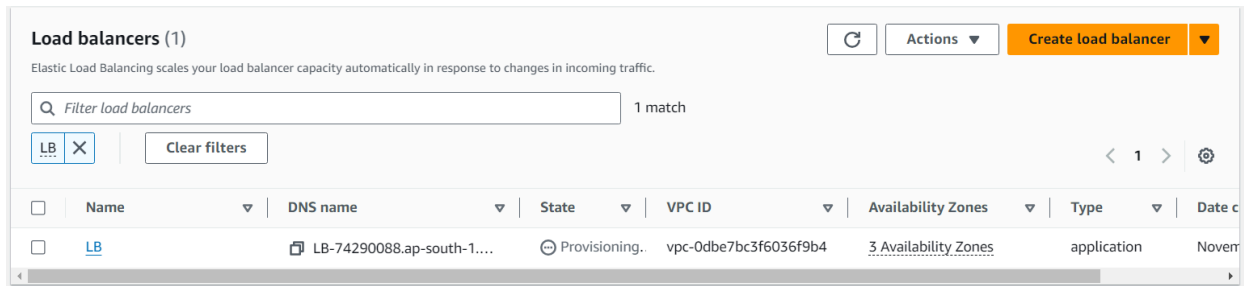
TG  
Target type: Instance, IPv4

HTTP ▼

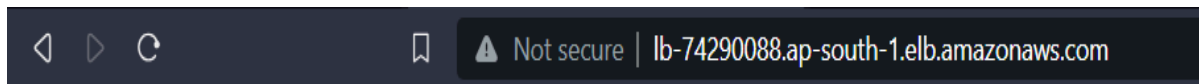
↻

[Create target group](#)

24. Now wait till the “State” becomes “Active”.



25. Now copy paste the dns name, and keep reloading the page, it should keep changing the page.



## Instance VM-3

26. Now if one instance is stopped or terminated the load balancer will not be able to send traffic to that instance. The traffic will be diverted to other instances