

Application Load Balancer →

Create a 2 or 3 EC2 Instance and installed httpd (apache2) server on it

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](#)

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.

Recents: [Quick Start](#)

Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, Debian

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

Summary

Number of instances: [Info](#)

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-0f605997b4d0ff7aac

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)

[Cancel](#) [Launch instance](#) [Preview code](#)

Network settings [Info](#) [Edit](#)

Network: [Info](#)
vpc-074321e9b52b24a31

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-1' with the following rules:

☒ Allow SSH traffic from [Info](#)

☐ 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.

Summary

Number of instances: [Info](#)

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-0f605997b4d0ff7aac

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)

[Cancel](#) [Launch instance](#) [Preview code](#)

Here I have written the bash script to launch apache2 server

User data - optional [Info](#)

Upload a file with your user data or enter it in the field.

[Choose file](#)

```
#!/bin/bash
sudo -i
yum install httpd -y
systemctl start httpd
systemctl enable httpd
cd /var/www/html/
echo "this is $(hostname)" >> index.html
```

☐ User data has already been base64 encoded

Summary

Number of instances: [Info](#)

When launching more than 1 instance, consider EC2 Auto Scaling

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-0f605997b4d0ff7aac

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

[Cancel](#) [Launch instance](#) [Preview code](#)

The screenshot shows the AWS Management Console for the 'Asia Pacific (Mumbai)' region. The left sidebar contains navigation links for Dashboard, EC2 Global View, Events, and various EC2 services. The main content area displays the 'Instances (1/3)' page. A table lists three instances, all of which are 'Running'. Below the table, the details for instance 'i-01b881d344ae670c6 (server1)' are shown, including tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. The 'Instance summary' section is visible, showing the instance ID and public IPv4 address.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public
server1	i-01b881d344ae670c6	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-3-109-123-194.ap-...	3.109.
server2	i-031cd148cc7376f76	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-13-127-243-127.ap-...	13.12.
server3	i-003c38a7ae5e56a48	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-3-110-135-139.ap-...	3.110.

Check that httpd server is running on each instance

The screenshot shows a web browser window with the address bar displaying 'ec2-3-109-123-194.ap-south-1.compute.amazonaws.com'. The browser's tabs and bookmarks are visible at the top. The page content is not visible, only the browser interface.

this is ip-172-31-13-209.ap-south-1.compute.internal

Create load balancer

aws

Search

[Alt+S]

IAM

EC2

Asia Pacific (Mumbai) Rohan Borate

EC2

Load balancers

Create Application Load Balancer

Create Application Load Balancer

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

How Application Load Balancers work

Basic configuration

Load balancer name

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

lb

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

Scheme

Info

Scheme can't be changed after the load balancer is created.

☒ Internet-facing

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name is publicly resolvable.
- Requires a public subnet.

☐ Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name is publicly resolvable.
- Compatible with the IPv4 and Dualstack IP address types.

Load balancer IP address type

Info

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

☒ IPv4

- Includes only IPv4 addresses.

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

aws

Search

[Alt+S]

IAM

EC2

Asia Pacific (Mumbai) Rohan Borate

EC2

Load balancers

Create Application Load Balancer

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.

Availability Zones

☒ ap-south-1a (aps1-az1)

Subnet

subnet-0a3a36e89d871c759

IPv4 subnet CIDR: 172.31.32.0/20

IPv4 address

Assigned by AWS

☒ ap-south-1b (aps1-az3)

Subnet

subnet-020b1cc024c04ec04

IPv4 subnet CIDR: 172.31.0.0/20

IPv4 address

Assigned by AWS

☒ ap-south-1c (aps1-az2)

Subnet

subnet-063968e541fe68df9

IPv4 subnet CIDR: 172.31.16.0/20

IPv4 address

Assigned by AWS

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

aws

Search

[Alt+S]

IAM

EC2

Asia Pacific (Mumbai) Rohan Borate

EC2

Load balancers

Create Application Load Balancer

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-1

sg-0a7511efcd0b6b74c VPC: vpc-074321e9b52b24a31

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

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

Now we also need to create the target group

The image consists of three screenshots of the AWS Management Console, showing the process of creating a target group. The screenshots are arranged vertically, showing the progression from the initial configuration to the final health check settings.

Screenshot 1: Specify group details

Step 1: Specify group details (selected)
Step 2: Register targets

Specify group details
Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

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.
- ☐ **IP addresses**
 - Supports load balancing to VPC and on-premises resources.
 - Facilitates routing to multiple IP addresses and network interfaces on the same instance.
 - Offers flexibility with microservice based architectures, simplifying inter-application communication.
 - Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
- ☐ **Lambda function**
 - Facilitates routing to a single Lambda function.
 - Accessible to Application Load Balancers only.

Screenshot 2: Target group name, Protocol, and IP address type

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.

Protocol : Port
Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation.

HTTP 80
1-65535

IP address type
Only targets with the indicated IP address type can be registered to this target group.

- ☒ **IPv4**
Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.
- ☐ **IPv6**
Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

VPC
Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

vpc-074321e9b52b24a31
IPv4 VPC CIDR: 172.31.0.0/16

Protocol version
☒ HTTP1

Screenshot 3: Health checks and Attributes

Health checks
The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol
HTTP

Health check path
Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.
/
Up to 1024 characters allowed.

Advanced health check settings

Attributes
Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

Tags - optional
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Cancel](#) [Next](#)

Then select all the instance in target group

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Step 2: Register targets

Available instances (3/3)

Filter instances

<input checked="" type="checkbox"/>	Instance ID	Name	State	Security groups	Zone	Private IPv
<input checked="" type="checkbox"/>	i-01b881d344ae670c6	server1	Running	launch-wizard-1	ap-south-1b	172.31.13...
<input checked="" type="checkbox"/>	i-031cd148cc7376f76	server2	Running	launch-wizard-1	ap-south-1b	172.31.15...
<input checked="" type="checkbox"/>	i-003c38a7ae5e56a48	server3	Running	launch-wizard-1	ap-south-1b	172.31.3.1...

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](#)

We have successfully created the target group

Target groups (1)

Filter target groups

<input type="checkbox"/>	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
<input type="checkbox"/>	TG	arn:aws:elasticloadbalancin...	80	HTTP	Instance	None associated	vpc-074321e9b52b24a31

0 target groups selected

Select a target group above.

Now go back to the load balance creation , select the created target group

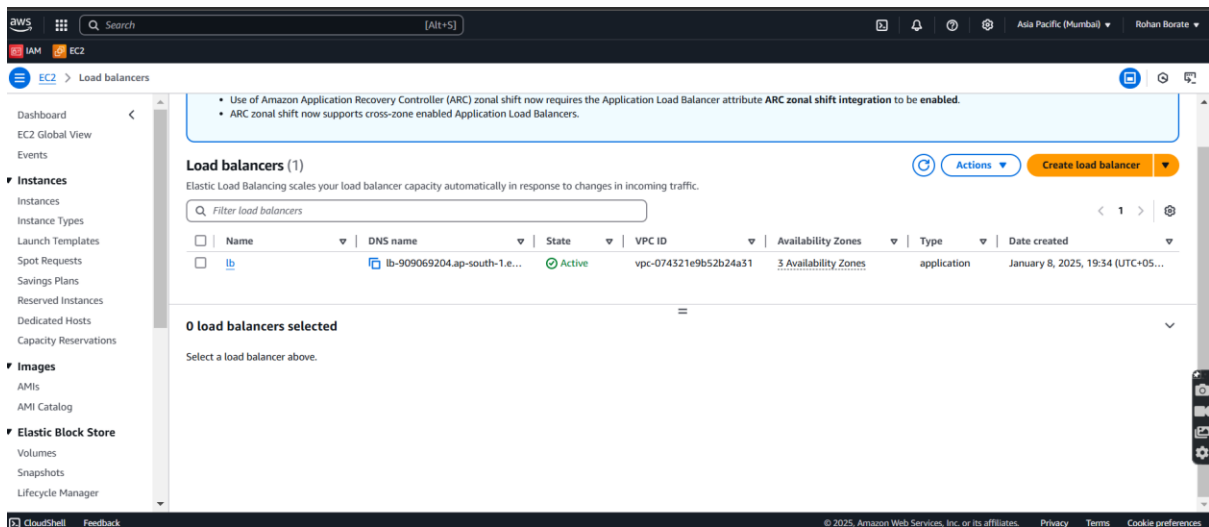
The screenshot shows the 'Listeners and routing' configuration page in the AWS Management Console. The page title is 'Create Application Load Balancer'. The main section is 'Listeners and routing', which includes a list of listeners. A single listener is configured with the following details:

- Listener HTTP-80**: Includes a 'Remove' button.
- Protocol**: HTTP
- Port**: 80
- Default action**: Forward to TG (Target type: Instance, IPv4). Includes a 'Create target group' link.
- Listener tags - optional**: A section with an 'Add listener tag' button and a note: 'You can add up to 50 more tags.'
- Add listener**: A button at the bottom of the listener configuration.

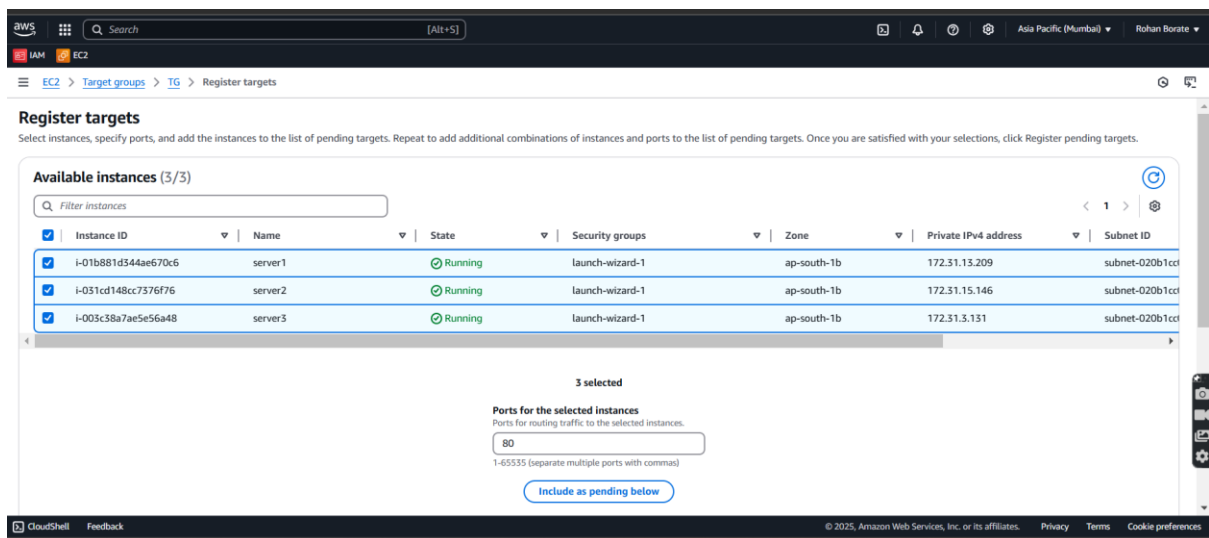
Below the listener configuration, there is a section for 'Load balancer tags - optional' with a note: 'Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.'

The bottom of the screenshot shows the 'Summary' page, which provides a review of the configurations:

- Basic configuration**: lb, Internet-facing, IPv4.
- Security groups**: launch-wizard-1, sg-0cf51fe06fb74c.
- Network mapping**: VPC vpc-074321e9b52b24a51, subnets: ap-south-1a, ap-south-1b, ap-south-1c.
- Listeners and routing**: HTTP-80 defaults to TG.
- Service integrations**: Amazon CloudFront + AWS Web Application Firewall (WAF): None, AWS WAF: None, AWS Global Accelerator: None.
- Tags**: None.
- Attributes**: A note stating 'Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.'



You have to register all instance in the target group (note – if we don't register we get error 503 as server not available)



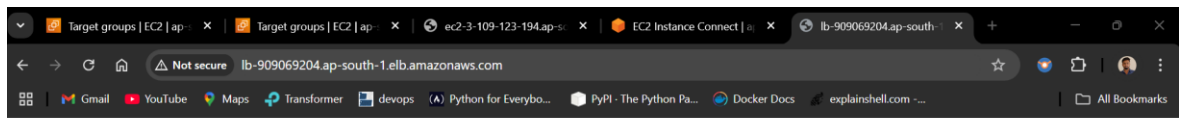
Now copy the DNS name of the load balancer, and paste to browser

Check it is accessible

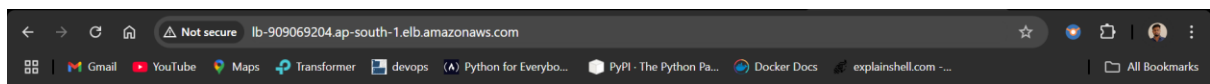
Refresh the page and check IP of the server is changing as we have created load balancing

With 3 instances so we are getting this instances IP's

In this way traffic is diverted to all instances , according to the load balancer technique

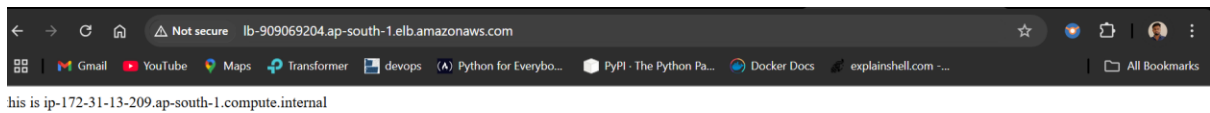


this is ip-172-31-15-146.ap-south-1.compute.internal



this is ip-172-31-3-131.ap-south-1.compute.internal





Clean up process --

Delete load balancer

De-register the instance in Target group

Delete target group

Delete instances