APPLICATION LOAD BALANCER

STEPS	
1	CREATE TARGET GROUP
2	CREATE LOAD BALANCER
3	CREATE & LAUNCH EC2 AMAZON LINUX
4	ADD NEW LISTENER RULE IN LOAD BALANCER-PATH BASED ROUTING
5	EDIT SECURITY GROUP-INBOUND RULES
6	COPY THE DNS AND CHECK IN THE BROWSER

Step 1 create a target group

Target group name

appl-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.

defaultvpc
vpc-07f48dec5a3f9030a
IPv4 VPC CIDR: 172.31.0.0/16 ▼

Protocol version

● HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or

---

0 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

Review targets

Targets (0)

Remove all pending

🔍 Filter targets

⬤ Show only pending

< 1 > ⚙

Instance ID ▽	Name ▽	Port ▽	State ▽	Security groups ▽	Zone ▽	Private IPv4 address	Subnet ID ▽	Launch t

No instances added yet
Specify instances above, or leave the group empty if you prefer to add targets later.

0 pending

Cancel | Previous | **Create target group**

Step 2

EC2 > Load balancers

Load balancers

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

↻ | Actions ▼ | **Create load balancer** | ▼

🔍 Filter load balancers

< 1 > ⚙

☐	Name ▽	DNS name ▽	State ▽	VPC ID ▽	Availability Zones ▽	Type ▽

No load balancers
You don't have any load balancers in ap-south-1

Target groups (1/1) Info

[Actions ▲] [Create target group]

Delete
Register targets
Edit health check settings
Edit target group attributes
Manage tags
Associate with a new load balancer
Associate with an existing load balancer

Filter target groups

☑	Name	▽	ARN	▽	Port	▽	Protocol	▽	Target
☑	appl-tg		arn:aws:elasticloadbalanci…		80		HTTP		Instanc

Basic configuration

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

demo-alb

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**
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more. ☑

○ **Internal**
An internal load balancer routes requests from clients to targets using private IP addresses. Compatible with the **IPv4** and **Dualstack** IP address types.

IP address type | Info
Select the type of IP addresses that your subnets use. Public IPv4 addresses have an additional cost.

● **IPv4**
Includes only IPv4 addresses.

○ **Dualstack**
Includes IPv4 and IPv6 addresses.

○ **Dualstack without public IPv4**
Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

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

Shell   Feedback   © 2

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 ☑.

defaultvpc
vpc-07f48dec5a3f9030a
IPv4 VPC CIDR: 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)**
Subnet

subnet-059fa228354025dfa   default1 ▼

Step 3 create a EC2

Network settings Info

VPC - required Info

vpc-07f48dec5a3f9030a (defaultvpc) (default)
172.31.0.0/16

Subnet Info

subnet-059fa228354025dfa default1
VPC: vpc-07f48dec5a3f9030a Owner: 637423530978
Availability Zone: ap-south-1a IP addresses available: 4090 CIDR: 172.31.0.0/20)

Create new subnet

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

Common security groups Info

Select security groups

default sg-0b8f682f438e5936b ✕
VPC: vpc-07f48dec5a3f9030a

Compare security group rules

Security groups that you add or remove here will be added or removed from all your network interfaces.

▼ Summary

Number of instances Info

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-04f8d7ed2f1a54b14

Virtual server type (instance type)
t2.micro

Firewall (security group)
default

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 ✕

Cancel   **Launch instance**

Review commands

Shell   Feedback   © 2024, Amazon Web Services, Inc. or its affiliates.

Services   Q Search [Alt+S]

Allow tags in metadata Info

Select

User data - optional Info
Upload a file with your user data or enter it in the field.

Choose file

```
#bin/bash
yum install httpd -y
service httpd start
mkdir /var/www/html/dem
echo '<h1>***PRIYANKA***<h1/> '> /var/www/html/dem/index.html
```

☐ User data has already been base64 encoded

▼ Summary

Number of instances Info

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-04f8d7ed2f1a54b14

Virtual server type (instance type)
t2.micro

Firewall (security group)
default

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 ✕

Cancel   **Launch instance**

Review commands

CloudShell   Feedback   © 2024, Amazon Web Services, Inc. or its affiliates.

[Alt+S]   Mumbai ▾ priyu ▾

Instances (1/1) Info   ↻ Connect Instance state ▾ Actions ▾ **Launch instances** ▾

Q Find Instance by attribute or tag (case-sensitive)   All states ▾   < 1 >

	Name ✎	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
☑	alb-ec2	i-09d0fc7237744f824	⊘ Running ⊕ ⊖	t2.micro	⊘ 2/2 checks passed	View alarms +	ap-south-1a	–

http://52.66.203.61/

⬅ ➡ ↻ ⚠ Not secure 52.66.203.61

PRIYANKA

Step 4 Edit the default rule

	Scheme	Hosted zone	Availability Zones	Date created
	Internet-facing	ZP97RAFLXTNZK	subnet-059fa228354025dfa ⬈ ap-south-1a (aps1-az1)	June 25, 2024, 12:27 (UTC+05:30)
			subnet-0b506d5402b693a4d ⬈ ap-south-1b (aps1-az3)	

Load balancer ARN
⬚ arn:aws:elasticloadbalancing:ap-south-1:637423530978:loadbalancer/app/demo-alb/73b71bc 079789e24

DNS name Info
⬚ demo-alb-1823611245.ap-south-1.elb.amazonaws.com (A Record)

Listeners and rules | Network mapping | Resource map - new | Security | Monitoring | Integrations | Attributes | Tags

Listeners and rules (1/1) Info

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

[Manage rules ▾] [Manage listener ▾] [Add listener]

🔍 Filter listeners   < 1 > ⚙

☑	Protocol:Port ▾	Default action ▾	Rules ▾	ARN ▾	Security policy ▾	Default SSL/TLS certificate ▾
☑	HTTP:80	**Forward to target group** • appl-tg ⬈: 1 (100%) • Target group stickiness: Off	1 rule	⬚ ARN	Not applicable	Not applicable

https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ELBListenerV2:listenerArn=arn:aws:elasticloadbalancing:ap-south-1:637423530978:listener/app/demo-alb/73b71bc079789e24/f12c12af5ba4dbc7   Terms   Cook

▼ **Details**

A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how the Application Load Balancer routes requests to its registered targets.

Protocol:Port	Load balancer	Default actions
HTTP:80	demo-alb	**Forward to target group** • appl-tg ⬈: 1 (100%) • Target group stickiness: Off

Listener ARN
⬚ arn:aws:elasticloadbalancing:ap-south-1:637423530978:listener/app/demo-alb/73b71bc079789e24/f12c12af5ba4dbc7

Rules | Tags

Listener rules (1/1) Info

Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.

Rule limits ↻ [Actions ▲] [Add rule]

🔍 Filter rules

		View rule	⚙
		Edit rule	
		Delete rule	
		Reprioritize rules	

☑	Name tag	Priority ▲	Conditions (If)	Actions (Then)	ARN
☑	Default	Last (default)	If no other rule applies	**Forward to target group** • appl-tg ⬈: 1 (100%) • Target group stickiness: Off	⬚ ARN 0 tags

---

Listener configuration

The listener will be identified by the protocol and port.

Protocol
Used for connections from clients to the load balancer.

[HTTP ▾]

Port
The port on which the load balancer is listening for connections.

[81]
1–65535

Default actions | Info

The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Routing actions

○ Forward to target groups   ○ Redirect to URL   ● Return fixed response

Return fixed response | Info

Use fixed-response actions to drop client requests and return a custom HTTP response. When a fixed-response action is taken, the action and the URL of the redirect target are recorded in the access logs.

Response code
The type of message you want to send.

[503]
2xx, 4xx, 5xx

Content type - optional
The format of your message.
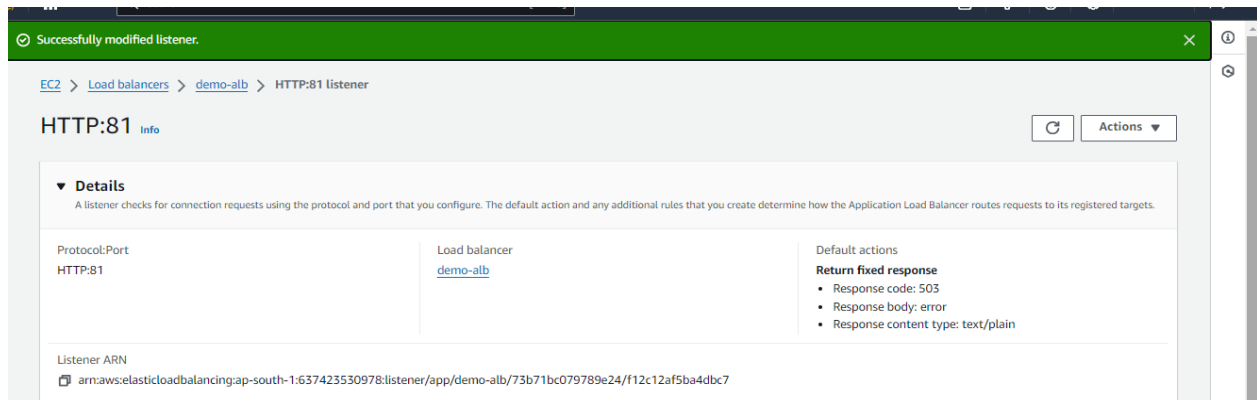
[text/plain ▾]

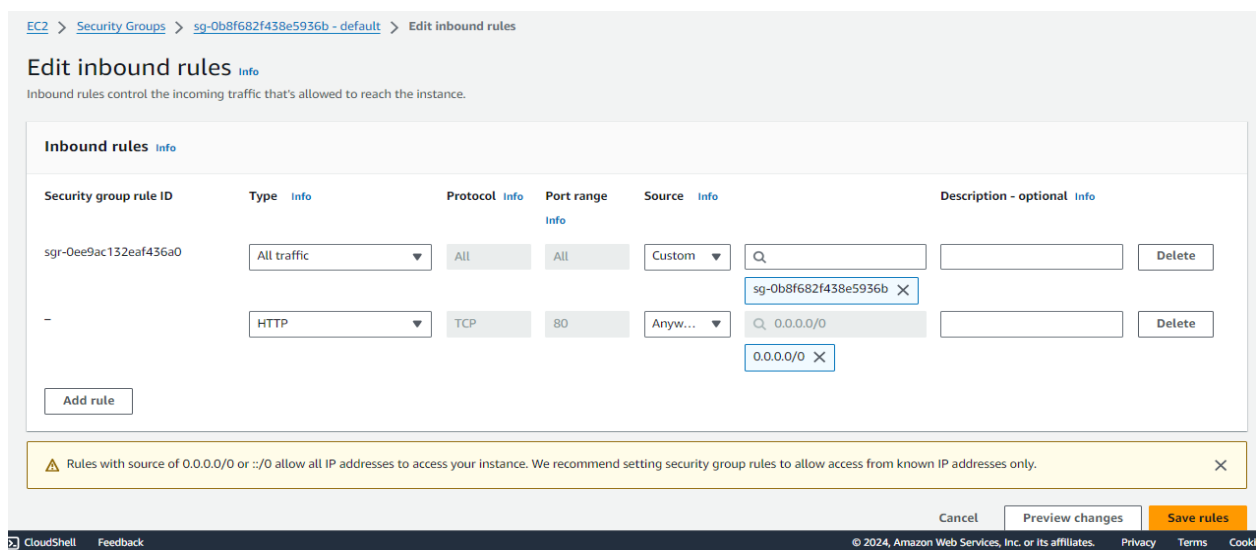**Response body - optional**
Enter your response message.

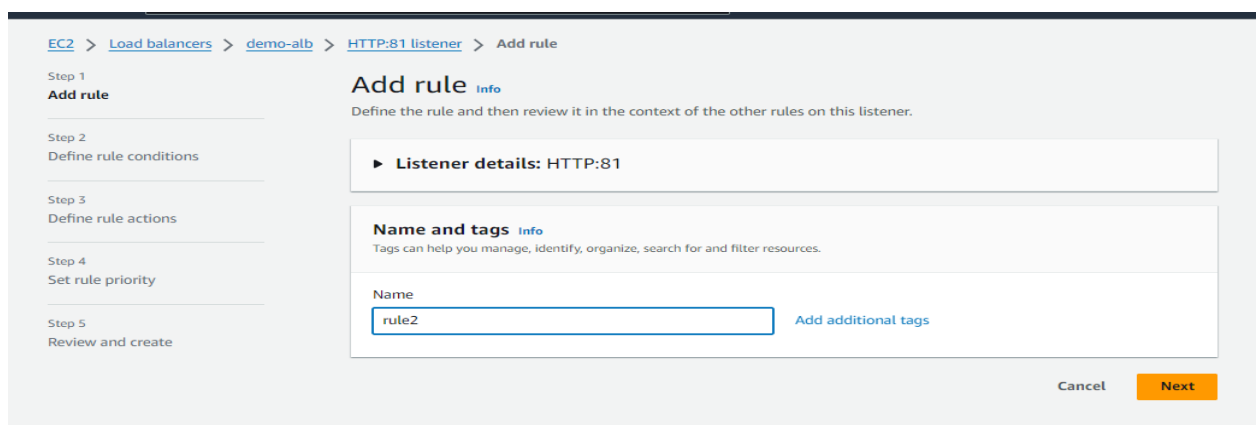[error]

1024 character maximum

Step 5 Edit security group

Step 6 Add new listener rules in the created load balancer

Add condition Rule limits

×

Rule condition types

Route traffic based on the condition type of each request. Each rule can include one of each of the following conditions: host-header, path, http-request-method and source-ip. Each rule can include one or more of each of the following conditions: http-header and query-string.

Path ▼

Path
Define the path. For example: /item/*. Case sensitive.

is /demo* 🗑

Maximum 128 characters. Allowed characters are `a-z`, `A-Z`, `0-9`; the following special characters: `_ - . $ / ~ " ' @ : +`; `&` (using `&`); and wildcards (`*` and `?`).

Add new value

You can add up to 4 more condition values for this rule.

Cancel   **Confirm**

Step 1
Add rule

Step 2
Define rule conditions

Step 3
Define rule actions

Step 4
Set rule priority

Step 5
Review and create

Define rule conditions Info

Requests reaching this rule must match all specified conditions for the rule to apply. At least 1 condition is required.

▶ **Listener details:** HTTP:81

Conditions (1)   Rule limits   Edit   Delete   **Add condition**

Path (1) Info   ☐
If
Path

is
/demo*

AND

Cancel   Previous   **Next**

CloudShell   Feedback   © 2024, Amazon Web Services, Inc. or its affiliates.

Step 1
Add rule

Step 2
Define rule conditions

Step 3
Define rule actions

Step 4
Set rule priority

Step 5
Review and create

Define rule actions Info

These actions will be applied to requests matching the rule conditions.

▶ **Listener details:** HTTP:81

Actions

Action types
Routing actions

◉ Forward to target groups   ○ Redirect to URL   ○ Return fixed response

Forward to target group | Info
Choose a target group and specify routing weight or Create target group ↗

Target group		Weight	Percent
appl-tg HTTP ▼	⟳	1	100%
Target type: Instance, IPv4		0-999	

Add target group

You can add up to 4 more target groups.

CloudShell   Feedback   © 2024, Amazon Web Services, Inc. or it

Step 3
Define rule actions

Step 4
Set rule priority

Step 5
Review and create

▶ **Listener details: HTTP:81**

Rule: rule2

Priority
Rule priority controls the evaluation order of a rule within the listener's set of rules. You can leave gaps in priority numbers.

| 1 | ⇕ |

1 - 50000

Listener rules (2) Info

Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.

🔍 Filter rules

Name tag	Priority ▲	Conditions (If)	Actions (Then)	ARN
rule2	1	**Path Pattern** is /demo*	**Forward to target group** • appl-tg ↗: 1 (100%) • Target group stickiness: Off	Pending
			Forward to target group	

CloudShell   Feedback   © 2024, Amazon Web Services, Inc. or it

---

**Rules**   **Tags**

Listener rules (2) Info

Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.

🔍 Filter rules   Rule limits | Actions ▼ | Add rule

	Name tag	Priority ▲	Conditions (If)	Actions (Then)	ARN
☐	rule2	1	**Path Pattern** is /dem*	**Forward to target group** • appl-tg ↗: 1 (100%) • Target group stickiness: Off	ARN
☐	*Default*	Last (default)	*If no other rule applies*	**Return fixed response** • Response code: 503 • Response body: error • Response content type: text/plain	ARN

© 2024, Amazon Web Services, Inc. or its affiliates.   Privacy   Terms   Cookie

---

http://demo-alb-1823611245.ap-south-1.elb.amazonaws.com/dem/

← → C   ⚠ Not secure   demo-alb-1823611245.ap-south-1.elb.amazonaws.com/dem/

✳✳✳PRIYANKA✳✳✳
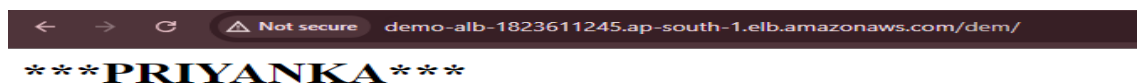
Step 6 terminate everything

Instances (1/1) Info   Connect | Instance state ▼ | Actions ▼ | **Launch instances** ▼

🔍 Find Instance by attribute or tag (case-sensitive)   All states ▼

	Name ✎	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	Availability Zone ▼	Public
☑	alb-ec2	i-09d0fc7237744f824	⊖ Terminated ⊕ ⊖	t2.micro	⊘ 2/2 checks passec	View alarms ＋	ap-south-1a	–

Load balancers (1/1)

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

Actions ▲ | Create load balancer ▼

Q Filter load balancers

1 > ⚙

	Name	▽	DNS name	▽	State	▽	VPC ID	Type	▽
☑	demo-alb		🗇 demo-alb-1823611245.ap...		⊘ Active		vpc-07f48dec5a3f9030a	application	

Actions menu:
- Edit IP address type
- Edit subnets
- Manage instances
- Edit health check settings
- Manage listeners
- Edit security groups
- Edit load balancer attributes
- Manage tags
- **Delete load balancer**

Load balancer: ✕

Delete load balancer ✕

Delete load balancer **demo-alb** permanently? This action can't be undone.

⚠ Proceeding with this action deletes the load balancer and its listeners. Target groups associated to this load balancer will become available for association to another load balancer and their registered targets remain unaffected.

To avoid accidental deletion we ask you to provide additional written consent.

Type **confirm** to agree.

confirm

Cancel | **Delete**

Target groups (1/1) Info

Actions ▲ | Create target group

Q Filter target groups

	Name	▽	ARN	▽	Port	▽	Protocol	▽	Target
☑	appl-tg		🗇 arn:aws:elasticloadbalanci...		80		HTTP		Instanc

Actions menu:
- **Delete**
- Register targets
- Edit health check settings
- Edit target group attributes
- Manage tags
- Associate with a new load balancer
- Associate with an existing load balancer

Delete target group? ✕

You can't undo this action.

Deleting a target group deletes the group; the individual resources registered to the target group don't get deleted as a result of this action.

Are you sure you want to delete this target group?

- appl-tg

Cancel | **Yes, delete**

Network Load Balancer

STEPS	
1	CREATE & LAUNCH EC2 AMAZON LINUX
2	CREATE TARGET GROUP
3	CREATE LOAD BALANCER
4	ADD NEW LISTENER RULE IN LOAD BALANCER
5	EDIT SECURITY GROUP-INBOUND RULES
6	COPY THE DNS AND CHECK IN THE BROWSER

Step 1 create a target group

You can add IP addresses from the VPC selected for your target group or from outside the VPC. Note that you can assemble a mix of targets from multiple network sources by returning to this step and choosing another network.

Network

defaultvpc
vpc-07f48dec5a3f9030a
IPv4 VPC CIDR: 172.31.0.0/16

Step 2: Specify IPs and define ports
You can manually enter IP addresses from the selected network.

Enter an IPv4 address from a VPC subnet.

172.31.0.   [Remove]

[Add IPv4 address]
You can add up to 4 more IP addresses.

Ports
Ports for routing to this target.
80
1-65535 (separate multiple ports with commas)

[Include as pending below]

1 selection is now pending below. Include more or register targets when ready.

⊘ Successfully created the target group: **nlb**.   ✕

EC2 > Target groups > nlb

nlb   [Actions ▼]

Details
arn:aws:elasticloadbalancing:ap-south-1:637423530978:targetgroup/nlb/71429792d402d6b7

Target type	Protocol : Port	VPC	IP address type
IP	TCP: 80	vpc-07f48dec5a3f9030a ☑	IPv4

Load balancer
ⓘ None associated

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
0	⊘ 0	⊗ 0	⊖ 0	⊕ 0	⊖ 0

Step 2 create a network load balancer

> Load balancers

Load balancers   [⟳]   [Actions ▼]   [**Create load balancer**] [▲]
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.
                                                                     Compare load balancer types
🔍 Filter load balancers   Create Application Load Balancer
                                                                     Create Network Load Balancer
☐ | Name ▽ | DNS name ▽ | State ▽ | VPC ID ▽ | Availa Create Gateway Load Balancer
                                                                     Create Classic Load Balancer
                                    No load balancers
                        You don't have any load balancers in ap-south-1

EC2 > Load balancers > Create Network Load Balancer

Create Network Load Balancer Info
The Network Load Balancer distributes incoming TCP and UDP traffic across multiple targets such as Amazon EC2 instances, microservices, and containers. When the load balancer receives a connection request, it selects a target based on the protocol and port that are specified in the listener configuration, and the routing rule specified as the default action.

▶ **How Network 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.

nlb-sp

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

Scheme
Scheme can't be changed after the load balancer is created.
⦿ Internet-facing
    An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more. ☑
◯ Internal
    An internal load balancer routes requests from clients to targets using private IP addresses.

Network mapping Info

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

VPC

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 🗗.

```
defaultvpc
vpc-07f48dec5a3f9030a
IPv4 VPC CIDR: 172.31.0.0/16                                              ▼      ⟳
```

Mappings

Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the selected Availability Zones. Zones that are not supported by the load balancer or VPC can't be selected. Subnets can be added, but not removed, once a load balancer is created.

☑ **ap-south-1a (aps1-az1)**

Subnet

```
subnet-059fa228354025dfa                                      default1   ▼
```

IPv4 address

● Assigned by AWS	○ Use an Elastic IP address

☐ **ap-south-1b (aps1-az3)**

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 - *recommended*

Security groups support on Network Load Balancers can only be enabled at creation by including at least one security group. You can change security groups after creation. The security groups for your load balancer must allow it to communicate with registered targets on both the listener port and the health check port. For PrivateLink Network Load Balancers, security group rules are enforced on PrivateLink traffic; however, you can turn off inbound rule evaluation after creation within the load balancer's Security tab or using the API.

```
Select up to 5 security groups                                          ▼      ⟳
```

```
default                                                    ✕
sg-0b8f682f438e5936b    VPC: vpc-07f48dec5a3f9030a
```

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 **TCP:80**   [Remove]

Protocol		Port		Default action Info

```
TCP    ▼    :    80                Forward to    nlb                              TCP  ▼    ⟳
                 1-65535                          Target type: Instance, IPv4
```

Create target group 🗗

Listener tags - *optional*

---

dShell   Feedback   © 2024, Amazon Web Services, Inc. or

✓ Successfully created load balancer   ✕

EC2 > Load balancers > nlb-sp

nlb-sp   ⟳   [Actions ▼]

▼ **Details**

Load balancer type	Status	VPC	IP address type
Network	⊙ Provisioning	vpc-07f48dec5a3f9030a 🗗	IPv4
Scheme	**Hosted zone**	**Availability Zones**	**Date created**
Internet-facing	ZVDDRBQ08TROA	subnet-059fa228354025dfa 🗗 ap-south-1a (aps1-az1)	June 29, 2024, 19:43 (UTC+05:30)

Load balancer ARN		DNS name Info
⧉ arn:aws:elasticloadbalancing:ap-south-1:637423530978:loadbalancer/net/nlb-sp/0c82138f4244e6e9		⧉ nlb-sp-0c82138f4244e6e9.elb.ap-south-1.amazonaws.com (A Record)

Step 3 create an EC2 instance

Name and tags Info

Name

nlb-ec2   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

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

Recents   **Quick Start**

Amazon Linux	macOS	Ubuntu	Windows	Red Hat	SUSE L
aws	Mac	ubuntu®	■ Microsoft	Red Hat	SUS

🔍 Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

▼ Summary

Number of instances Info

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-04f8d7ed2f1a54b14

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

Cancel   **Launch instance**

Review commands

▼ Network settings Info

VPC - *required* Info

vpc-07f48dec5a3f9030a (defaultvpc)   (default) ⌄
172.31.0.0/16   ↻

Subnet Info

subnet-059fa228354025dfa   default1
VPC: vpc-07f48dec5a3f9030a   Owner: 637423530978   ⌄   ↻ Create new subnet ⧉
Availability Zone: ap-south-1a   IP addresses available: 4090   CIDR: 172.31.0.0/20)

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

Common security groups Info

Select security groups   ⌄   ↻ Compare security
                                                               group rules
default sg-0b8f682f438e5936b ✕
VPC: vpc-07f48dec5a3f9030a

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▸ Advanced network configuration

▼ Summary

Number of instances Info

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...read more
ami-04f8d7ed2f1a54b14

Virtual server type (instance type)
t2.micro

Firewall (security group)
default

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

Cancel   **Launch instance**

Review commands

User data - *optional* | Info
Upload a file with your user data or enter it in the field.

⊞ **Choose file**

```
#!/bin/bash
yum install httpd -y
service httpd start
```

Instances (1/1) Info

	Name	Instance ID	Instance state		Instance type	Status check	Alarm status	Ava
☑	nlb-ec2	i-0b758e4858eb92e5a	⊘ Running	⊕ ⊖	t2.micro	⏱ Initializing	View alarms +	ap-

i-0b758e4858eb92e5a (nlb-ec2)

Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags

▼ Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0b758e4858eb92e5a (nlb-ec2)	13.233.216.66 | open address	172.31.15.83
IPv6 address	Instance state	Public IPv4 DNS
–	⊘ Running	ec2-13-233-216-66.ap-south-1.compute.amazonaws.com | open address
Hostname type	Private IP DNS name (IPv4 only)	
IP name: ip-172-31-15-83.ap-south-1.compute.internal	ip-172-31-15-83.ap-south-1.compute.internal	

← → C ⚠ Not secure 13.233.216.66

It works!

http://nlb-c5c436a631230b65.elb.ap-south-1.amazonaws.com/

← → C ⚠ Not secure nlb-c5c436a631230b65.elb.ap-south-1.amazonaws.com

It works!

After completing the task delete the used services