

## LAB 2: NETWORK LOAD BALANCER

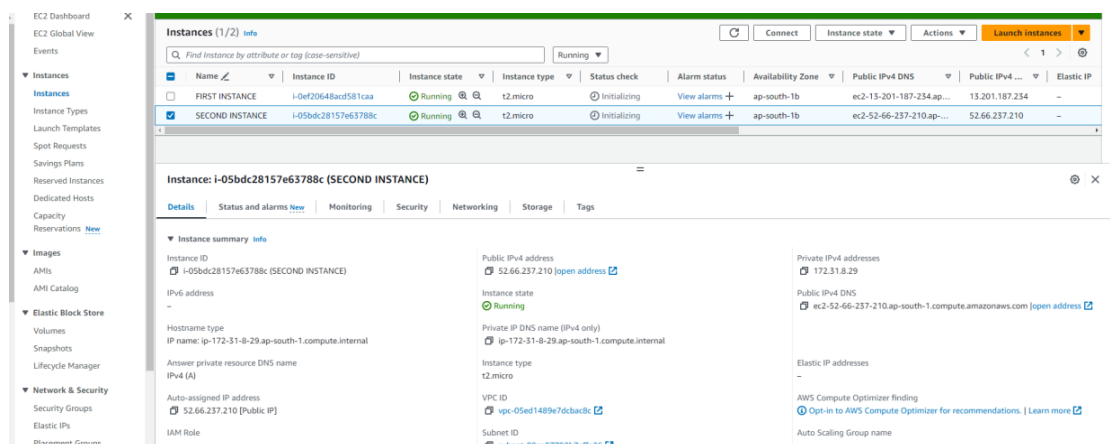
**AIM:** To launch a network load balancer.

### THEORY:

- A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model.
- It can handle millions of requests per second. After the load balancer receives a connection request, it selects a target from the target group for the default rule.
- It attempts to open a TCP connection to the selected target on the port specified in the listener configuration.
- When you enable an Availability Zone for the load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone.
- By default, each load balancer node distributes traffic across the registered targets in its Availability Zone only.
- If you enable cross-zone load balancing, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones.

### PROCEDURE:

1. Launch two instances.



## 2. Choose network load balancer.

EC2 > Load balancers > Compare and select load balancer type

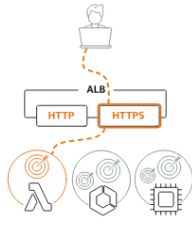
### Compare and select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

#### Load balancer types

##### Application Load Balancer

[Info](#)

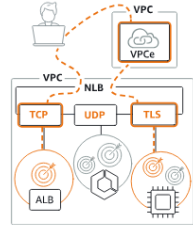


Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Create

##### Network Load Balancer

[Info](#)




Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Create

##### Gateway Load Balancer

[Info](#)



Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create

## 3. Create target groups.

Step 2  
Register 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.

☐ **Application Load Balancer**

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

demo-tg-nlb

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

TCP 80

1-65535

EC2 > Target groups > Create target group

Step 1  
[Specify group details](#)

Step 2  
**Register targets**

### Register targets

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.

**Available instances (2)**

Filter instances

<input type="checkbox"/>	Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID
<input type="checkbox"/>	i-0ef20648acd581caa	FIRST INSTANCE	Running	launch-wizard-1	ap-south-1b	172.31.12.147	subnet-08aa87792b7ef
<input type="checkbox"/>	i-05bdc28157e6378bc	SECOND INSTANCE	Running	launch-wizard-1	ap-south-1b	172.31.8.29	subnet-08aa87792b7ef

0 selected

Ports for the selected instances

Ports for routing traffic to the selected instances

80

1-40535 (separate multiple ports with comma)

Include as pending below

2 selections are now pending below. Include more or register targets when ready.

### Review targets

**Targets (2)**

Filter targets

Show only pending

Remove all pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-0ef20648acd581caa	FIRST INSTANCE	80	Running	launch-wizard-1	ap-south-1b	172.31.12.147	subnet-08aa87792b7ef	March 31, 2024, 00:52 (UTC+05:30)

## 4. Launch the load balancer.

Subnet

subnet-0b678bf93da49f82d

IPv4 address

Assigned by AWS

### Security groups

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

demo-sg-nlb  
sg-04a5023ee28daf37 VPC: vpc-05ed1489e7dcba8c

### Listeners and routing

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 TCP Port 80

Default action Forward to demo-tg-nlb Target type Instance, IPv4

1-40535

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

Successfully created load balancer

EC2 > Load balancers > demo-nlb

### demo-nlb

Details

Load balancer type Network	Status Provisioning	VPC vpc-05ed1489e7dcba8c	IP address type IPv4
Scheme Internet-facing	Hosted zone ZVDRBQ8TROA	Availability Zones subnet-0d2a8a51b672e15d9 ap-south-1a (aps1-az1) subnet-08aa87792b7effa26 ap-south-1b (aps1-az3) subnet-0b678bf93da49f82d ap-south-1c (aps1-az2)	Date created March 31, 2024, 01:20 (UTC+05:30)
Load balancer ARN arn:aws:elasticloadbalancing:ap-south-1:058264174589:loadbalancer/net/demo-nlb/f08e5b445268c288		DNS name demo-nlb-f08e5b445268c288.elb.ap-south-1.amazonaws.com (A Record)	

Listeners Network mapping Security Monitoring Integrations Attributes Tags

### Listeners (1)

A listener checks for connection requests using the protocol and port you configure. Traffic received by a Network Load Balancer listener is forwarded to the selected target group.

Filter listeners

<input type="checkbox"/>	Protocol:Port	Default action	ARN	Security policy	Default SSL/TLS certificate	ALPN policy	Tags
<input type="checkbox"/>	TCP:80	Forward to target group demo-tg-nlb	ARN	Not applicable	Not applicable	None	0 tags

5. Testing the load balancer.

**Hello World from ip-172-31-12-147.ap-south-1.compute.internal**