
Assignment:9 Load_Configure Network Load Balancer

Create Network Load Balancer and configure the DNS in your web server

1. Navigate to EC2 Load Balancer and click on Create Load Balancer
2. In the Load Balancer type choose Network Load Balancer and click on Create option
3. Provide the load balancer name, select Internal-facing, and IPv4 address type
4. In the network mapping select your VPC
5. In the subnet mapping select the availability zones and select the private subnets where you run the two mattermost instance

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](#).

my-vpc-01
vpc-0e190ca43b317839f
IPv4: 10.0.0.0/16

↺

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

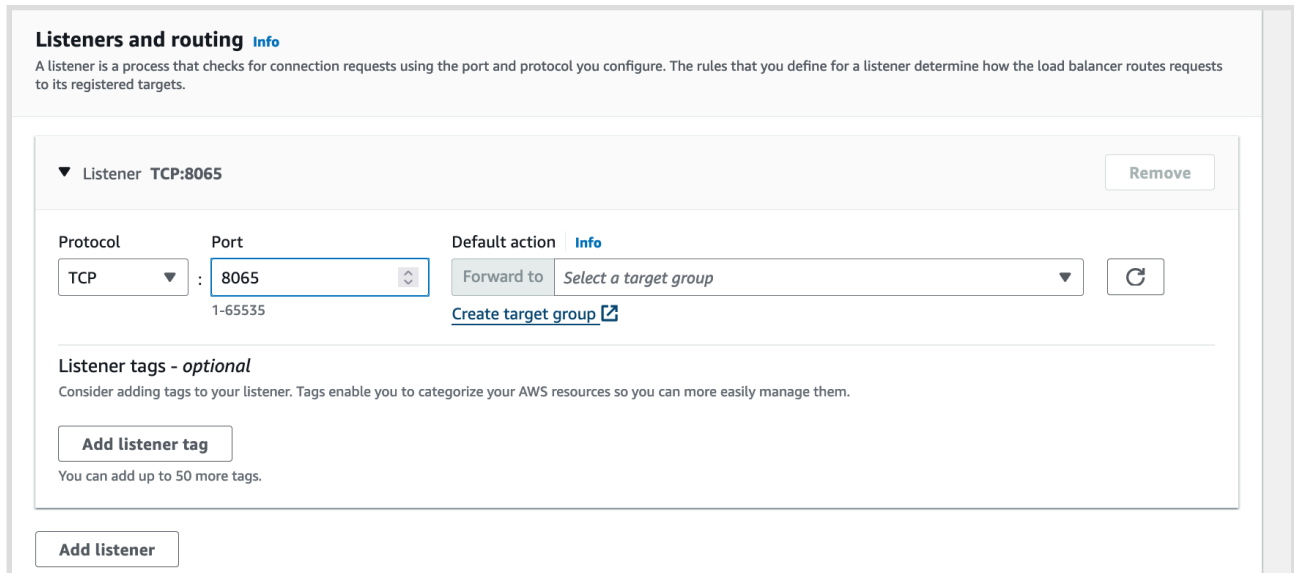
subnet-0691fa12817842c2dprivate_01 ▼

⚠

The selected subnet does not have a route to an internet gateway. This means that your load balancer will not receive internet traffic.
You can proceed with this selection; however, for internet traffic to reach your load balancer, you must update the subnet's route table in the [VPC console](#).

IPv4 address
Assigned by AWS ▼

6. In the Listeners and Routing provide the TCP port 8065 , click on Create target group and select your VPC from the list, provide the target group name other options can be default.



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:8065** [Remove](#)

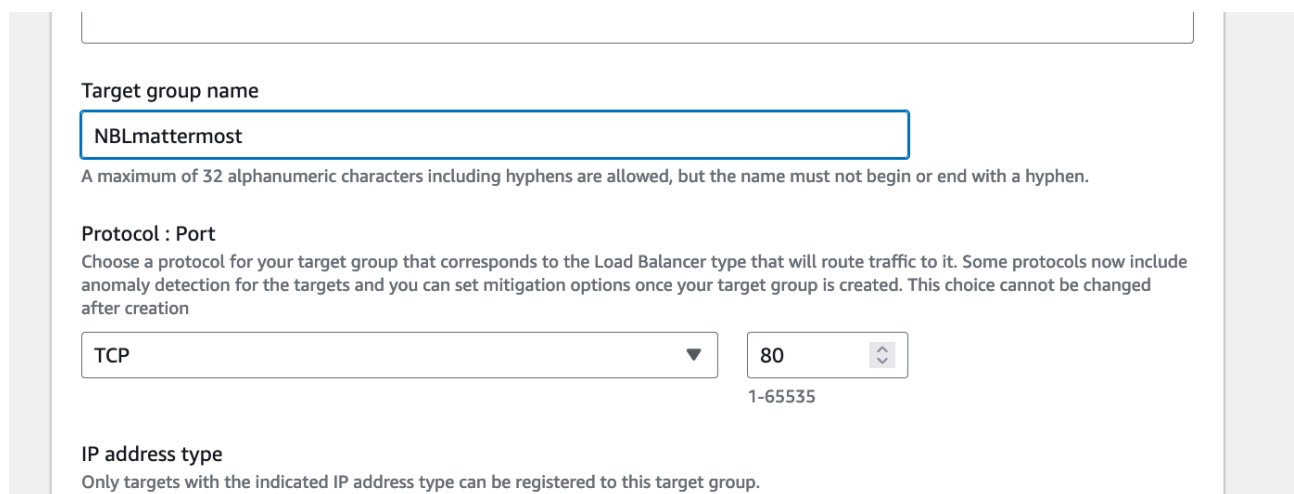
Protocol: TCP Port: 8065 (1-65535) Default action: [Info](#)

Forward to: [Select a target group](#) [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](#)



Target group name: NBLmattermost

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

Protocol : Port: TCP : 80 (1-65535)

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

IP address type: IPv4

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

7. In the Advanced health check settings you can give your custom values in the traffic port. (you can leave as default if you don't wish to change it)

8. Click on 'Next' option and in the List of Registered Instances select your private instances where you are running the mattermost

Available instances (2/5)				
<input type="text" value="Filter instances"/>				
<input type="checkbox"/>	Instance ID	Name	State	Security g
<input type="checkbox"/>	i-05a4e1f88e7ed4668	public-insta(nginx)-2	Running	launch-wiz
<input checked="" type="checkbox"/>	i-0afa5896198d39468	private-insta(appserver)-2	Running	launch-wiz
<input type="checkbox"/>	Instance private-insta(appserver)-2	public-insta(nginx)-1	Running	launch-wiz
<input checked="" type="checkbox"/>	i-0e7568659b5b24589	private-insta(appserver)-1	Running	launch-wiz
<input type="checkbox"/>	i-0a6d610ce310ab3bf	private-insta(dbserver)	Running	launch-wiz

9. Change the port number to 8065 and 'click include as pending below' and then create the target group.

public-insta(nginx)-1	Running	launch-wizard-29	ap-south-1
private-insta(appserver)-1	Running	launch-wizard-31	ap-south-1
private-insta(dbserver)	Running	launch-wizard-30	ap-south-1

2 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

1-65535 (separate multiple ports with commas)

Include as pending below

10. Map the Target group in the Load balancer configuration

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:8065

Remove

Protocol

Port

Default action [Info](#)

TCP ▼

:

8065

1-65535

Forward to

NBLmattermost

TCP ▼

Target type: Instance, IPv4

↻

[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.

11. Click on Create Load Balancer and it should now be created successfully

12. Navigate to target group and you can see the details of the targets

[EC2](#) > [Load balancers](#) > NLBsecuritygroup

NLBsecuritygroup

↻ Actions ▼

▼ Details

Load balancer type
Network

Status
Active

VPC
[vpc-0e190ca43b317839f](#)

IP address type
IPv4

Scheme
Internet-facing

Hosted zone
ZVDDRQBQ8TROA

Availability Zones
[subnet-0691fa12817842c2d](#) ap-south-1a (aps1-az1)
[subnet-01e1b5812ebeece9](#) ap-south-1b (aps1-az3)

Date created
December 1, 2023, 20:11 (UTC+05:30)

Load balancer ARN
[arn:aws:elasticloadbalancing:ap-south-1:405819896469:loadbalancer/net/NLBsecuritygroup/f7d74fe03439000c](#)

DNS name [Info](#)
[NLBsecuritygroup-f7d74fe03439000c.elb.ap-south-1.amazonaws.com](#) (A Record)

Listeners

Network mapping

Security

Monitoring

Integrations

Attributes

Tags

Listeners (1)

↻ Actions ▼ Add listener

Filter listeners

< 1 > ⚙

<input type="checkbox"/>	Protocol:Port ▼	Default action ▼	ARN ▼	Security policy ▼	Default SSL/TLS certificate ▼	ALPN policy ▼	Tags ▼
<input type="checkbox"/>	TCP:8065	Forward to target group • NLBtargetgroup	ARN	Not applicable	Not applicable	None	0 tags

Introducing Automatic Target Weights (ATW) to increase application availability
 Automatic Target Weights is achieved by turning on anomaly mitigation, which provides responsive, dynamic distribution of traffic to targets based on anomaly detection results. All HTTP/HTTPS target groups now include anomaly detection by default. [Learn more](#)

NLBtargetgroup

Actions

Details

arn:aws:elasticloadbalancing:ap-south-1:405819896469:targetgroup/NLBtargetgroup/3ba7d3cd236cbd00

Target type

Instance

Protocol : Port

TCP: 80

VPC

[vpc-0e190ca43b317839f](#)

IP address type

IPv4

Load balancer

[NLBsecuritygroup](#)

Total targets

2

Healthy

2

Unhealthy

0

Unused

0

Initial

0

Draining

0

► Distribution of targets by Availability Zone (AZ)

Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets

Monitoring

Health checks

Attributes

Tags

Registered targets (2)

Filter targets

1

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details	Launch time
<input type="checkbox"/>	i-Oe7568659b5b24589	private-insta(appserve...	8065	ap-south-1a	Healthy		December 1, 2023, ...
<input type="checkbox"/>	i-Oafa5896198d39468	private-insta(appserve...	8065	ap-south-1b	Healthy		December 1, 2023, ...

13. Open your web server Instance , navigate to `/etc/nginx/conf.d/mattermost`.
 Provide the DNS of your Network Load Balancer
 For both machine I have done

NIGNX-1

NIGNX-2

+

```

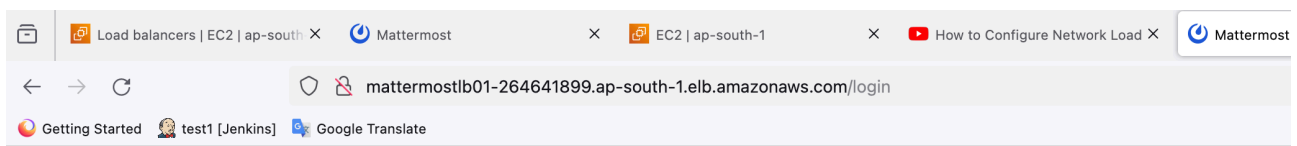
upstream backend {
    server NLBsecuritygroup-f7d74fe03439000c.elb.ap-south-1.amazonaws.com:8065;
    keepalive 32;
}

proxy_cache_path /var/cache/nginx levels=1:2 keys_zone=mattermost_cache:10m max_size=3g inactive=1

server {
    listen 80;
    server_name 10.0.1.178;
  
```

14. Now try to access your mattermost using the DNS of Application Load balancer

15. Now check the load balancing works by stopping the service / instance and also make a check on the Target health



After launching DNS

Mattermost

All team communication in one place,
searchable and accessible anywhere

Sign in

[I forgot my password.](#)