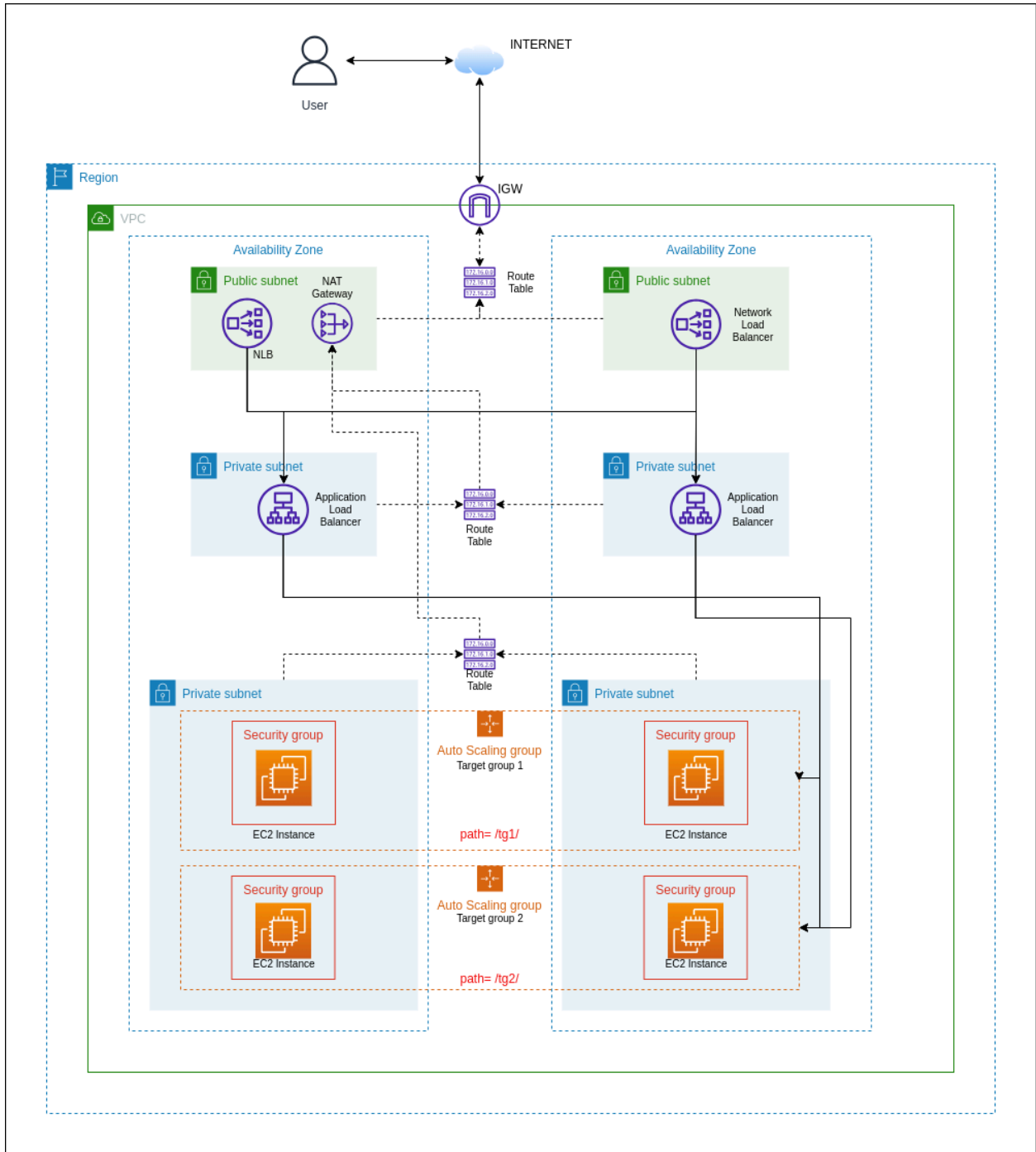


AWS Load Balancer wi



Architecture Diagram for the Solution

Step 1 - Create a VPC.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

ProjectBonus-VPC

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.20.0.0/24

IPv6 CIDR block [Info](#)

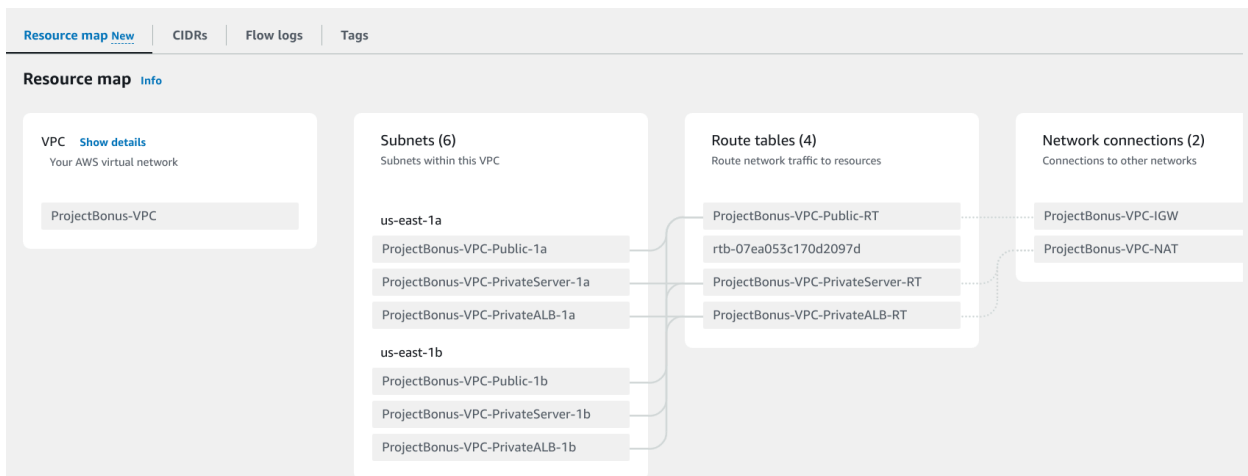
☒ No IPv6 CIDR block ☐ IPAM-allocated IPv6 CIDR block ☐ Amazon-provided IPv6 CIDR block ☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default

Create one public subnet and two private subnets across two availability zones. Create the route tables for each layer of subnets and edit the route for each.

- Public-1a and Public-1b - Route the internet facing traffic to the internet gateway.
- PrivateALB-1a and PrivateALB-1b - Route the internet facing traffic to the NAT gateway deployed in the public subnet.
- PrivateServer-1a and PrivateServer-1b - Route the internet facing traffic to the NAT gateway deployed in the public subnet.



Step 2 - Create a security group for the ALB to allow incoming TCP traffic from the VPC CIDR block. It will allow traffic only from the resources inside the VPC.

EC2 > Security Groups > sg-029ba74e1ba445d4d - ProjectBonus-VPC-ALB-SG

sg-029ba74e1ba445d4d - ProjectBonus-VPC-ALB-SG Actions

Details

Security group name ProjectBonus-VPC-ALB-SG	Security group ID sg-029ba74e1ba445d4d	Description Allows traffic from NLB	VPC ID vpc-0528aa9fcf8c5078e
Owner 237042273450	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

? You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer ×

Inbound rules (2) Manage tags Edit inbound rules

Security group rule...	IP version	Type	Protocol	Port range	Source	Description
sgr-0a2c255ae49f5e5	IPv4	HTTP	TCP	80	0.0.0.0/0	-
sgr-0c4d073e7743140...	IPv4	All TCP	TCP	0 - 65535	10.20.0.0/24	-

Step 3 - Create ALB in the level 2 private subnets across two AZs.

ProjectBonus-VPC-Apache-ALB Actions

Details

Load balancer type Application	Status Active	VPC vpc-0528aa9fcf8c5078e	IP address type IPv4
Scheme Internal	Hosted zone Z35SXDOTRQ7X7K	Availability Zones subnet-0a2d13aab2207fb4e us-east-1a (use1-az1) subnet-00938cda0976e0c44 us-east-1b (use1-az2)	Date created August 9, 2023, 10:39 (UTC+05:30)
Load balancer ARN arn:aws:elasticloadbalancing:us-east-1:237042273450:loadbalancer/app/ProjectBonus-VPC-Apache-ALB/7f046325a51b181c	DNS name Info internal-ProjectBonus-VPC-Apache-ALB-2131340340.us-east-1.elb.amazonaws.com (A Record)		

The ALB has one listener on port 80 with two target groups of instances running two different applications. The instances are not yet added to the target group as they will be automatically added by the Auto Scaling Group.

The screenshot shows the 'Listeners and rules' page for an ALB. The 'Listeners and rules (1)' section is active. It displays a single listener with the following details:

Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL cert
HTTP:80	Forward to target group <ul style="list-style-type: none">ProjectBonus-VPC-Apache-ALB-TG1: 1 (50%)ProjectBonus-VPC-Apache-ALB-TG2: 1 (50%)Group-level stickiness: Off	3 rules	ARN	Not applicable	Not applicable

Edit rules on the listener to forward the traffic to different target groups based on the url path.

Here, requests which match the path pattern “/tg1/*” will be forwarded to target group 1. And requests which match the path pattern “/tg2/*” will be forwarded to target group 2.

The screenshot shows the 'Listener rules (3)' page for the same ALB. It displays three rules configured for path-based forwarding:

Name tag	Priority	Conditions (If)	Actions (Then)	ARN
tg1-rule	1	Path Pattern is /tg1/*	Forward to target group <ul style="list-style-type: none">ProjectBonus-VPC-Apache-ALB-TG1: 1 (100%)Group-level stickiness: Off	ARN
tg2-rule	2	Path Pattern is /tg2/*	Forward to target group <ul style="list-style-type: none">ProjectBonus-VPC-Apache-ALB-TG2: 1 (100%)Group-level stickiness: Off	ARN
Default	Last (default)	If no other rule applies	Forward to target group <ul style="list-style-type: none">ProjectBonus-VPC-Apache-ALB-TG1: 1 (50%)ProjectBonus-VPC-Apache-ALB-TG2: 1 (50%)Group-level stickiness: Off	ARN

The ALB is deployed across two AZs in private subnets.

Network mapping [Info](#)

Targets in the listed zones and subnets are available for traffic from the load balancer using the IP addresses shown.

VPC

vpc-0528aa9fcf8c5078e [↗](#)

IPv4: 10.20.0.0/24

IPv6 : -

IP address type

IPv4

Edit IP address type

Edit subnets

Mappings

Including two or more Availability Zones, and corresponding subnets, increases the fault tolerance of your applications.

Zone	Subnet	IPv4 address	Private IPv4 address	IPv6 address
us-east-1a (use1-az1)	subnet-0a2d13aab2207fb4e ↗	Not applicable	Assigned from CIDR 10.20.0.32/27	Not applicab
us-east-1b (use1-az2)	subnet-00938cda0976e0c44 ↗	Not applicable	Assigned from CIDR 10.20.0.128/27	Not applicab

Attach the previously created security group.

sg-029ba74e1ba445d4d - ProjectBonus-VPC-ALB-SG

Actions

Details

Security group name

ProjectBonus-VPC-ALB-SG

Security group ID

sg-029ba74e1ba445d4d

Description

Allows traffic from NLB

VPC ID

vpc-0528aa9fcf8c5078e

Owner

237042273450

Inbound rules count

1 Permission entry

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Inbound rules (1/1)

Filter security group rules

1

IP version	Type	Protocol	Port range	Source	Description
IPv4	HTTP	TCP	80	10.20.0.0/24	–

Step 4 - Create a security group for the private instances. It allows HTTP and HTTPS traffic from the ALBs security group.

Inbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info		
sgr-09a4391750fc9c597	HTTP ▼	TCP	80	Custom ▼	<input type="text" value="Q"/>	<input type="text" value=""/> <div>sg-0d17835c6d0750acb ✕</div>	<input type="button" value="Delete"/>
sgr-0e3939757b72284ea	HTTP ▼	TCP	80	Custom ▼	<input type="text" value="Q"/>	<input type="text" value=""/> <div>sg-029ba74e1ba445d4d ✕</div>	<input type="button" value="Delete"/>
sgr-0f1eb6f22ba683847	HTTPS ▼	TCP	443	Custom ▼	<input type="text" value="Q"/>	<input type="text" value=""/> <div>sg-029ba74e1ba445d4d ✕</div>	<input type="button" value="Delete"/>
sgr-014a6c69affe0e1bd	SSH ▼	TCP	22	Custom ▼	<input type="text" value="Q"/> <div>0.0.0.0/0 ✕</div>	<input type="text" value=""/>	<input type="button" value="Delete"/>

Step 5 - Create two launch templates for both the applications.

Basic configurations will be the same for both the templates but the user data will be different as instances in different ASGs will host different applications which will be defined in the user data.

Launch template name and version description

Launch template name

ProjectBonus-VPC-ApacheTG1-LT (lt-021216a9aa7e43716)

Template version description

Max 255 chars

Auto Scaling guidance [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

☐ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

► Source template

▼ 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

AMI from catalog

Recents

My AMIs

Quick Start

Amazon Machine Image (AMI)

amzn2-ami-kernel-5.10-hvm-2.0.20230727.0-
x86_64-gp2
ami-09538990a0c4fe9be

Verified provider

Free tier eligible



[Browse more AMIs](#)

Including AMIs from
AWS, Marketplace and
the Community

Published	Architecture	Virtualization	Root device type	ENA Enabled
2023-07-27T02:57:10.000Z	x86_64	hvm	ebs	Yes

▼ Instance type [Info](#)

[Simple](#)

☒ Manually select instance type

Select an instance type that meets your computing, memory, networking, or storage needs

☐ Specify instance type attributes

Specify instance attributes that match your compute requirements

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour

Free tier eligible

☒ All generations

[Compare instance types](#)

▼ 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

ProjectBonus-PrivateKey

Template value ▼

 [Create new key pair](#)

▼

Network settings

Info

Subnet

Info

Don't include in launch template

▼

↻

Create new subnet

🔗

When you specify a subnet, a network interface is automatically added to your template.

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.

☒

Select existing security group

☐

Create security group

Security groups

Info

Select security groups

▼

↻

Compare security group rules

🔗

ProjectBonus-PrivateServer-SG

sg-0d17835c6d0750acb

✕

VPC: vpc-0528aa9fcf8c5078e

▶

Advanced network configuration

IAM instance profile

Info

arn:aws:iam::237042273450:instance-profile/IAM_instance_profile

▼

↻

Create new IAM profile

🔗

User data for application in target group 1

User data - optional

Info

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

📎

Choose file

```
#!/bin/bash


sudo yum update -y
sudo yum install httpd -y
sudo systemctl start httpd.service
systemctl enable httpd.service

sudo mkdir /var/www/html/tg1
sudo echo "Target group 1 Default Home Page $(hostname -f)" >
/var/www/html/index.html
sudo echo "Target group 1 $(hostname -f)" > /var/www/html/tg1/index.html
```


User data for application in target group 2

User data - optional [Info](#)

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

 Choose file

```
#!/bin/bash

sudo yum update -y
sudo yum install httpd -y
sudo systemctl start httpd.service
systemctl enable httpd.service

sudo mkdir /var/www/html/tg2
sudo echo "Target group 2 Default Home Page $(hostname -f)" >
/var/www/html/index.html
sudo echo "Target group 2 $(hostname -f)" > /var/www/html/tg2/index.html
```

Step 6 - Create two auto scaling groups for both the applications.

Select the appropriate launch template created for the applications and deploy the ASG in the 3rd level private subnets. The instances in the ASGs will be able to connect to the internet using NAT gateway deployed in the public subnet and will be accessible to end users using the NLB's DNS name.


ASG for target group 1 (Sample application 1)

[EC2](#) > [Auto Scaling groups](#) > ProjectBonus-VPC-ApacheTG1-ASG

ProjectBonus-VPC-ApacheTG1-ASG




[Details](#) | [Activity](#) | [Automatic scaling](#) | [Instance management](#) | [Monitoring](#) | [Instance refresh](#)

Group details [Edit](#)

Auto Scaling group name ProjectBonus-VPC-ApacheTG1-ASG	Desired capacity 1	Status -	Amazon Resource Name (ARN)  arn:aws:autoscaling:us-east-1:237042273450:autoScalingGroup:ba614c88-d8a2-48cf-81f3-e46570992fc2:autoScalingGroup/ProjectBonus-VPC-ApacheTG1-ASG
Date created Tue Aug 08 2023 17:09:25 GMT+0530 (India Standard Time)	Minimum capacity 1		
	Maximum capacity 1		

Launch template

Edit

Launch template  lt-021216a9aa7e43716 ProjectBonus-VPC-ApacheTG1-LT	AMI ID  ami-09538990a0c4fe9be	Instance type t2.micro	Owner arn:aws:iam::237042273450:user/IAM_user-ShreyasK
Version Default	Security groups -	Security group IDs  sg-0d17835c6d0750acb	Create time Wed Aug 09 2023 11:39:47 GMT+0530 (India Standard Time)
Description -	Storage (volumes) -	Key pair name ProjectBonus-PrivateKey	Request Spot Instances No

[View details in the launch template console](#)

Attach the load balancer’s target group 1 to the ASG.

Load balancing


Edit

Load balancer target groups ProjectBonus-VPC-Apache-ALB-TG1	Classic Load Balancers -
--	-----------------------------

ASG for target group 2 (Sample application 2)




Group details

Edit

Auto Scaling group name ProjectBonus-VPC-ApacheTG2-ASG	Desired capacity 1	Status -	Amazon Resource Name (ARN)  arn:aws:autoscaling:us-east-1:237042273450:autoScalingGroup:d8488c3c-e9a1-46bd-afbe-cc2e690cfbb4:autoScalingGroupName/ProjectBonus-VPC-ApacheTG2-ASG
Date created Tue Aug 08 2023 17:11:27 GMT+0530 (India Standard Time)	Minimum capacity 1		
	Maximum capacity 1		

Launch template

Edit

Launch template  lt-09d0b1f7cea59b1f2 ProjectBonus-VPC-ApacheTG2-LT	AMI ID  ami-09538990a0c4fe9be	Instance type t2.micro	Owner arn:aws:iam::237042273450:user/IAM_user-ShreyasK
Version Default	Security groups -	Security group IDs  sg-0d17835c6d0750acb	Create time Wed Aug 09 2023 11:38:03 GMT+0530 (India Standard Time)
Description -	Storage (volumes) -	Key pair name ProjectBonus-PrivateKey	Request Spot Instances No

[View details in the launch template console](#)

Attach the load balancer’s target group 2 to the ASG.

Load balancing

Edit

Load balancer target groups ProjectBonus-VPC-Apache-ALB-TG2	Classic Load Balancers -
--	-----------------------------

Step 7 - Connect to one of the instances from the ASG and check if the ALB's DNS redirects to the applications hosted in the private instances.

```
sh-4.2$ curl internal-ProjectBonus-VPC-Apache-ALB-2131340340.us-east-1.elb.amazonaws.com/tg1/
"Target group 1 ip-10-20-0-87.ec2.internal"
sh-4.2$ curl internal-ProjectBonus-VPC-Apache-ALB-2131340340.us-east-1.elb.amazonaws.com/tg2/
"Target group 2 ip-10-20-0-80.ec2.internal"
sh-4.2$ curl internal-ProjectBonus-VPC-Apache-ALB-2131340340.us-east-1.elb.amazonaws.com/
"Target group 1 Default Home Page ip-10-20-0-87.ec2.internal"
```

Step 8 - Create NLB in the public subnets.

Basic configuration

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

ProjectBonus-VPC-NLB

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.

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](#).

ProjectBonus-VPC
vpc-0528aa9fcf8c5078e
IPv4: 10.20.0.0/24

↻

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.

☒ **us-east-1a (use1-az1)**

Subnet
subnet-005fd3b4c501e5517 ProjectBonus-VPC-Public-1a ▼

IPv4 address
Assigned by AWS ▼

☒ **us-east-1b (use1-az2)**

Subnet
subnet-0c56b8e205af6fd59 ProjectBonus-VPC-Public-1b ▼

IPv4 address
Assigned by AWS ▼

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 1-65535	Forward to	ProjectBonus-VPC-NLB-TG Target type: Application Load Balancer, IPv4 Create target group
			TCP ▼ ↺

Listener tags - *optional*

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

Key	Value	
Name	NLB-TG	Remove

[Add listener tag](#)

You can add up to 49 more tags.

Target group for the NLB will include the ALB of a private subnet as the target. Traffic coming to the NLB will be redirected to the ALB and further to the private instances based on the url path.

ProjectBonus-VPC-NLB-TG

[Actions ▼](#)

Details

`arn:aws:elasticloadbalancing:us-east-1:237042273450:targetgroup/ProjectBonus-VPC-NLB-TG/3cda1b399a4ebe69`

Target type Application Load Balancer	Protocol : Port TCP: 80	VPC vpc-0528aa9fcf8c5078e	IP address type IPv4
Load balancer ProjectBonus-VPC-NLB			

ProjectBonus-VPC-NLB is routing traffic to this Application Load Balancer target group. You can now use static IP addresses, enable AWS PrivateLink, and route multi-protocol connections. [Learn more](#) [×](#)

[Targets](#) | [Health checks](#) | [Attributes](#) | [Tags](#)

Registered target

Application Load Balancer target groups are limited to a single Application Load Balancer target. The load balancer starts routing requests to a newly registered target as soon as the registration process is completed and the target passes initial health checks.

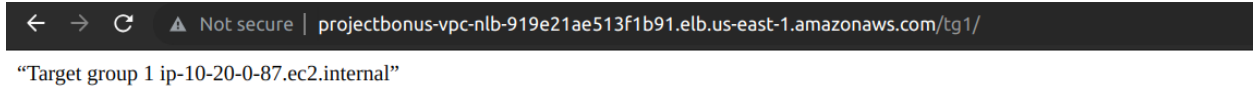
[Deregister](#)

Application Load Balancer ProjectBonus-VPC-Apache-ALB	Health status healthy
ARN <code>arn:aws:elasticloadbalancing:us-east-1:237042273450:loadbalancer/app/ProjectBonus-VPC-Ap...</code>	Health status details

Step 9 - Enter the NLB's DNS name in the browser to see if the applications are accessible.

- URL path for target group 1 -

“<http://projectbonus-vpc-nlb-919e21ae513f1b91.elb.us-east-1.amazonaws.com/tg1/>”



- URL path for target group 2 -

“<http://projectbonus-vpc-nlb-919e21ae513f1b91.elb.us-east-1.amazonaws.com/tg2/>”

