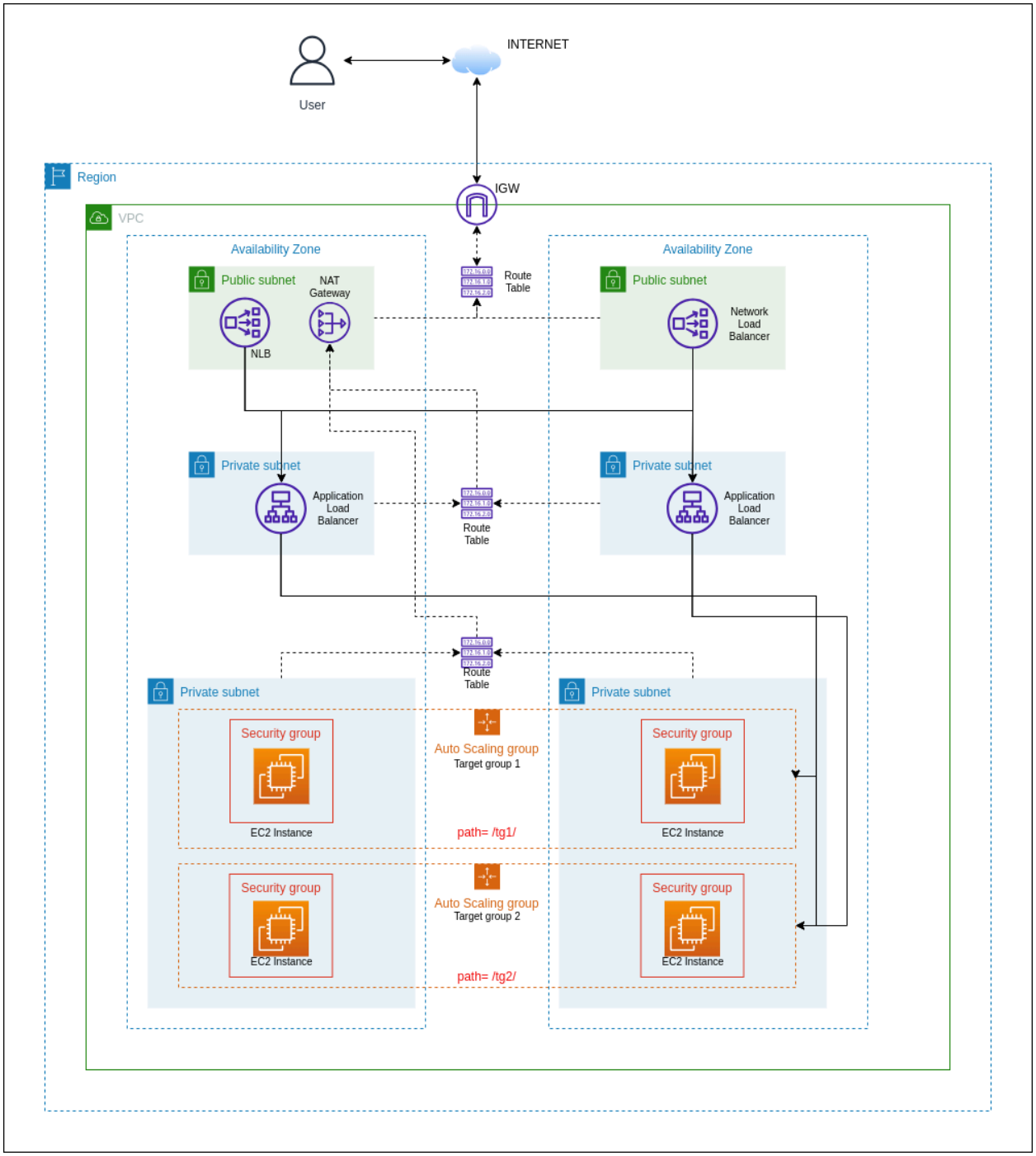
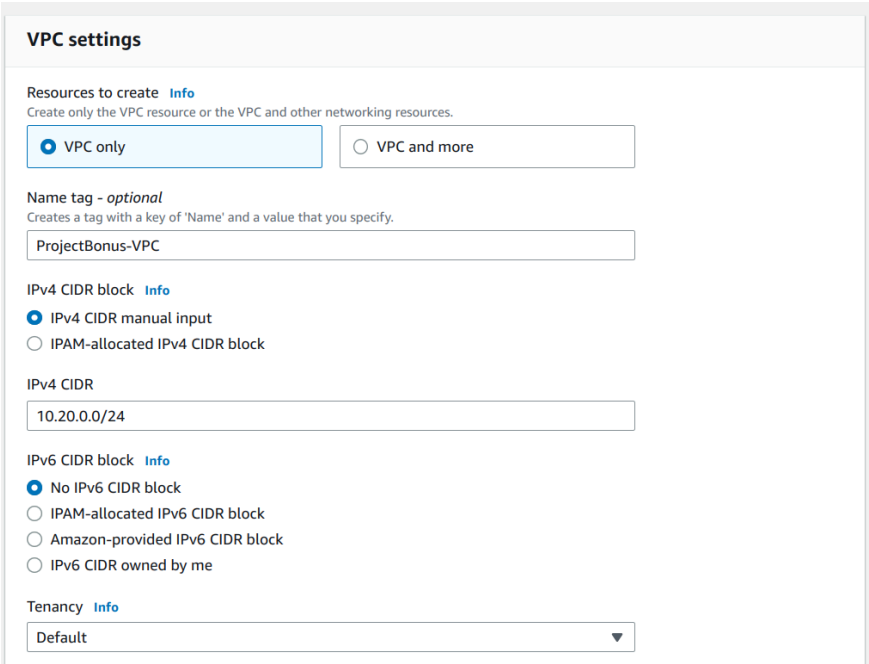
AWS Load Balancer wi



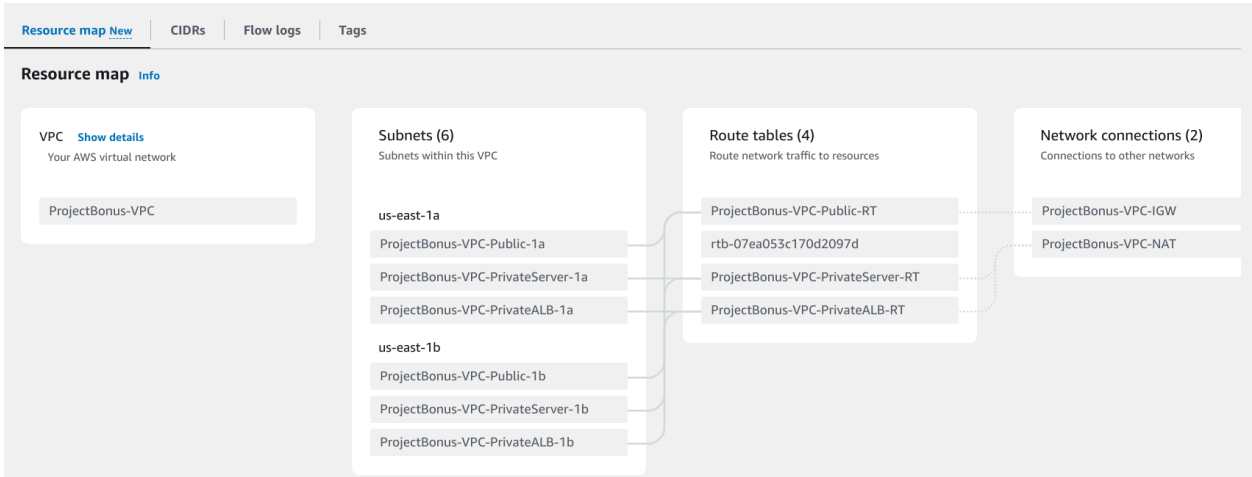
Architecture Diagram for the Solution

Step 1 - Create a VPC.



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

Filter security group rules

Security group rule...	IP version	Type	Protocol	Port range	Source	Description
sgr-0a2c255aead49f5e5	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

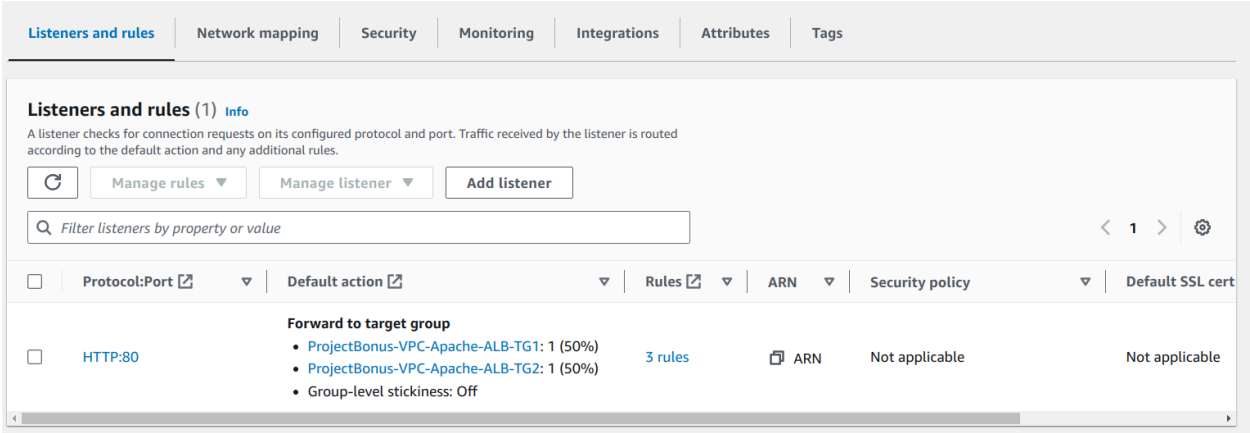
Details

Load balancer type	Status	VPC	IP address type
Application	Active	vpc-0528aa9fcf8c5078e	IPv4
Scheme	**Hosted zone**	**Availability Zones**	**Date created**
Internal	Z35SXDOTRQ7X7K	subnet-0a2d13aab2207fb4e us-east-1a (use1-az1) subnet-00938cda0976e0c44 us-east-1b (use1-az2)	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

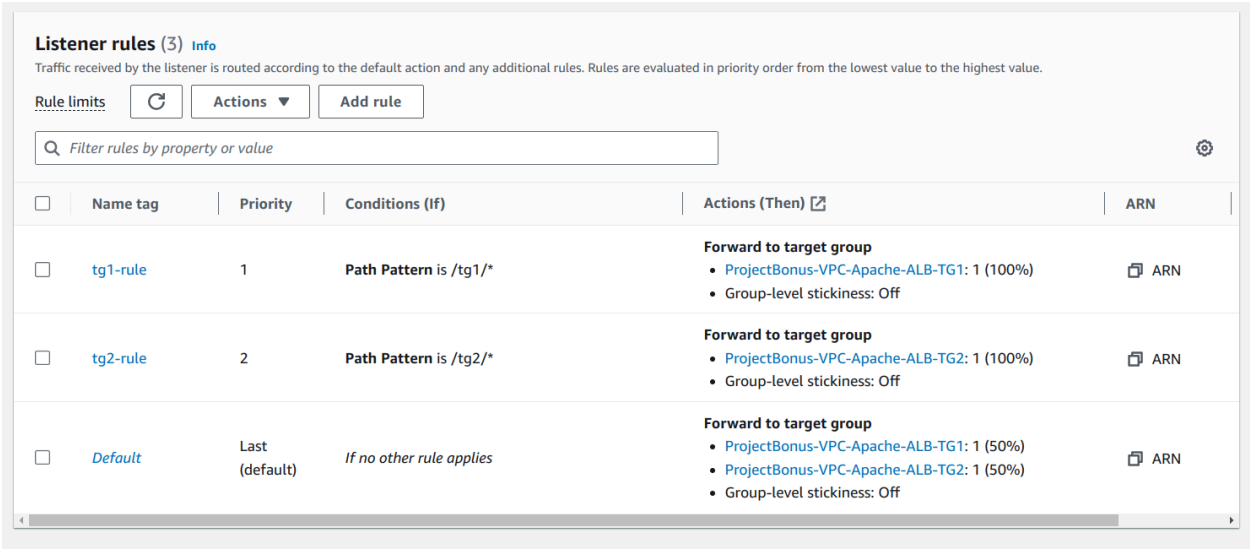
DNS name Info
internal-ProjectBonus-VPC-Apache-ALB-2131340340.us-east-1.elb.amazonaws.com (A Record)

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.



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 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.

Edit IP address type | Edit subnets

VPC
vpc-0528aa9fcf8c5078e
IPv4: 10.20.0.0/24
IPv6 : -

IP address type
IPv4

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	Security group ID	Description	VPC ID
ProjectBonus-VPC-ALB-SG	sg-029ba74e1ba445d4d	Allows traffic from NLB	vpc-0528aa9fcf8c5078e

Owner	Inbound rules count	Outbound rules count
237042273450	1 Permission entry	1 Permission entry

Inbound rules | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer — Run Reachability Analyzer

Inbound rules (1/1)

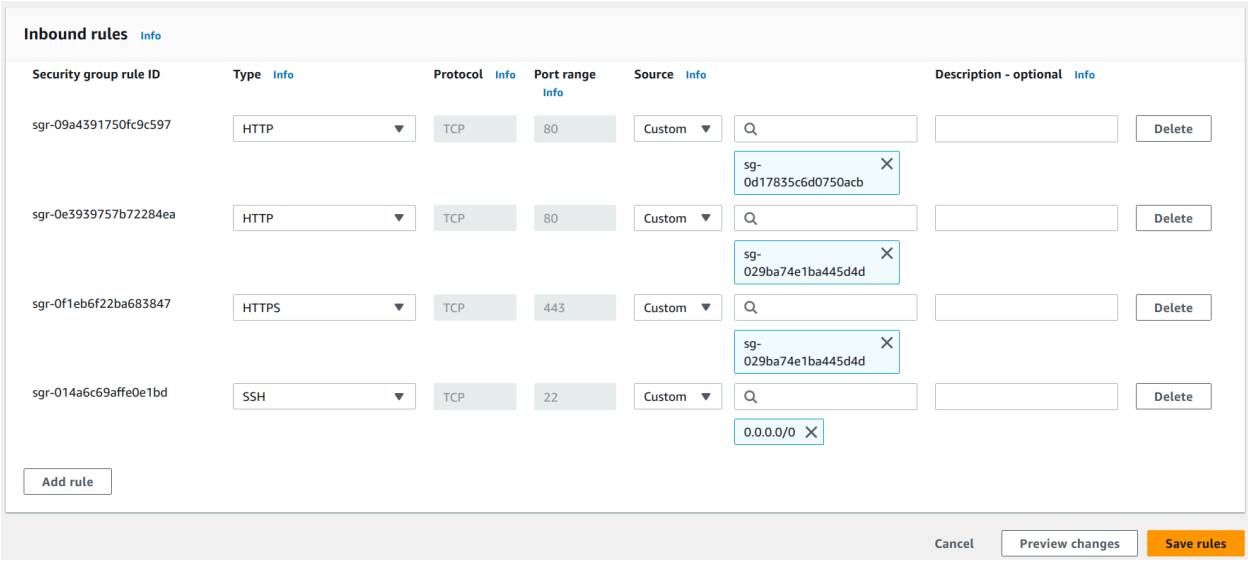
Manage tags | Edit inbound rules

Filter security group rules

1

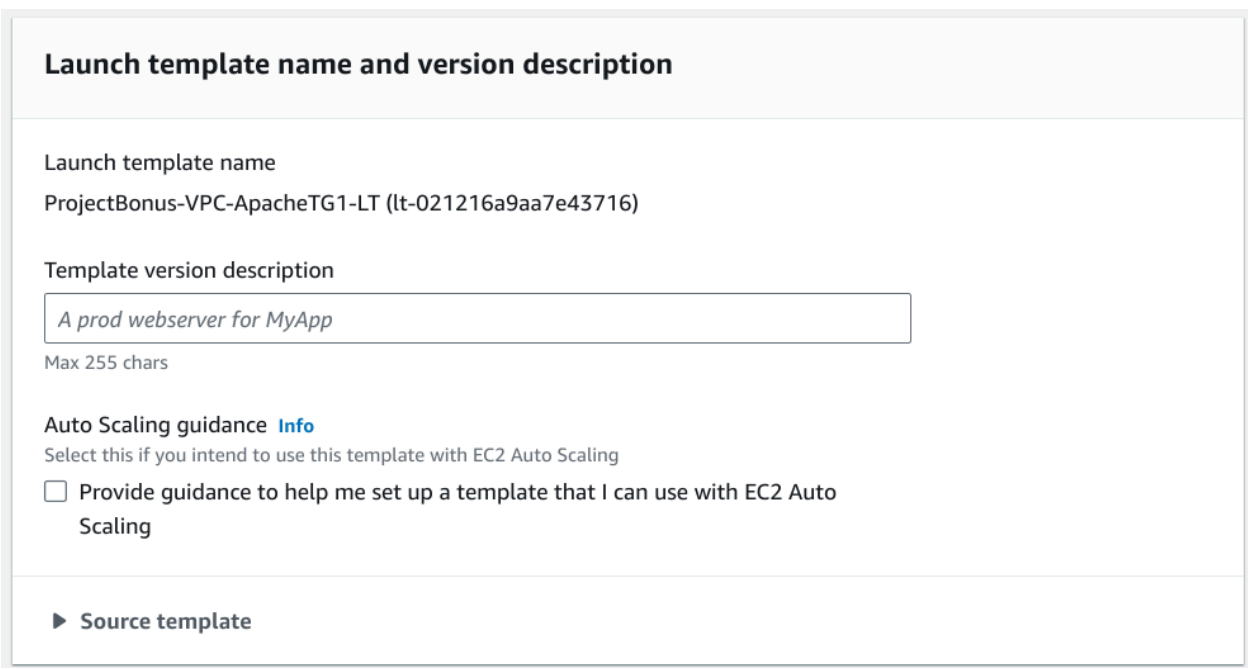
IP version	Type	Protocol	Port range	Source	Description
IPv4	HTTP	TCP	80	10.20.0.0/24	–

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



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.



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 — Free tier eligible
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

All generations

Compare instance types

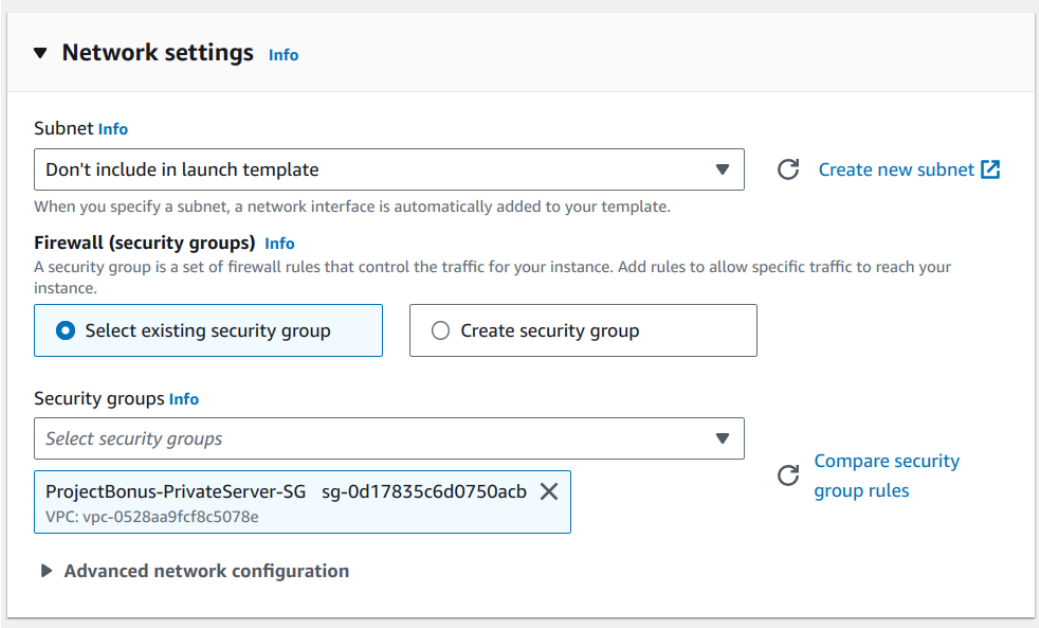
Key pair (login) Info

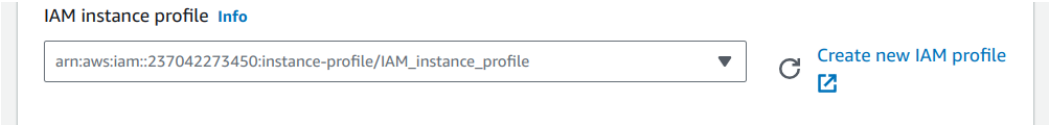
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name

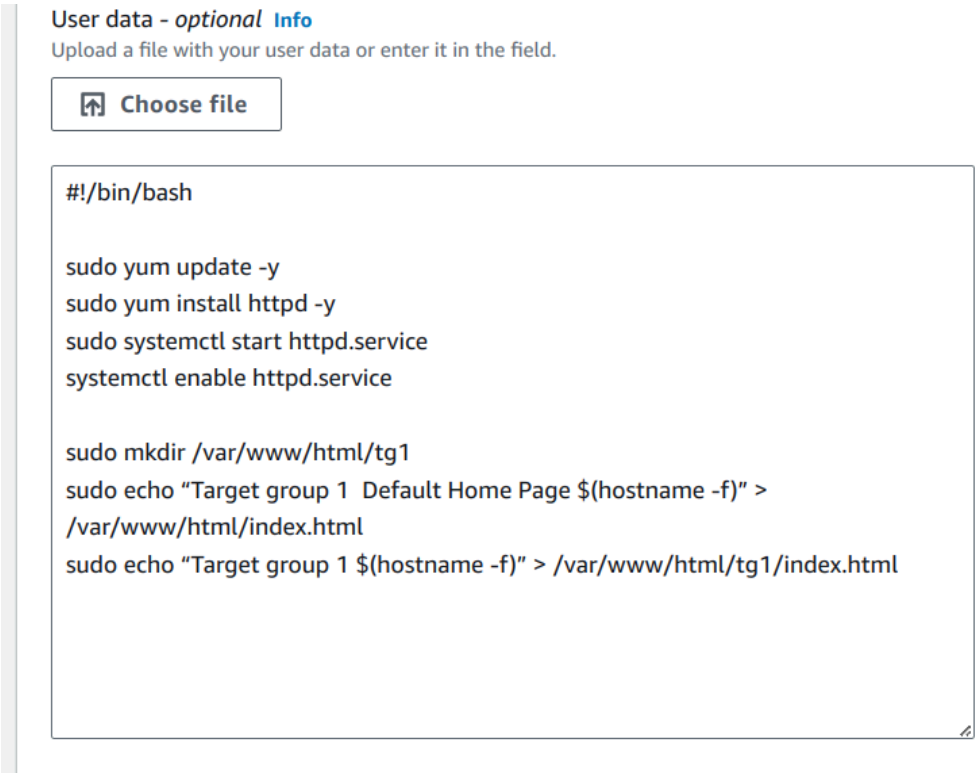
ProjectBonus-PrivateKey — Template value

Create new key pair





User data for application in target group 1



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	**Desired** capacity	Status	Amazon Resource Name (ARN)
ProjectBonus-VPC-ApacheTG1-ASG	1	-	arn:aws:autoscaling:us-east-1:237042273450:autoScalingGroup:ba614c88-d8a2-48cf-81f3-e46570992fc2:autoScalingGroupName/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.

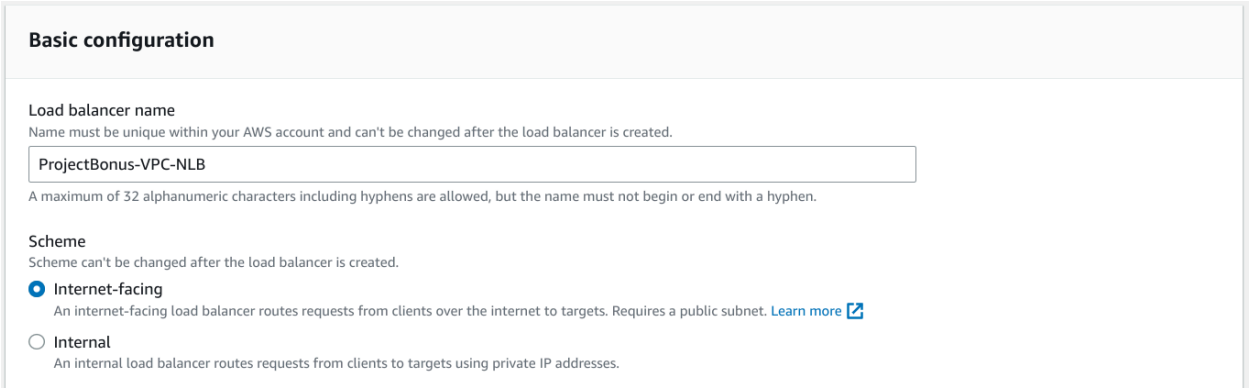
Load balancing Edit

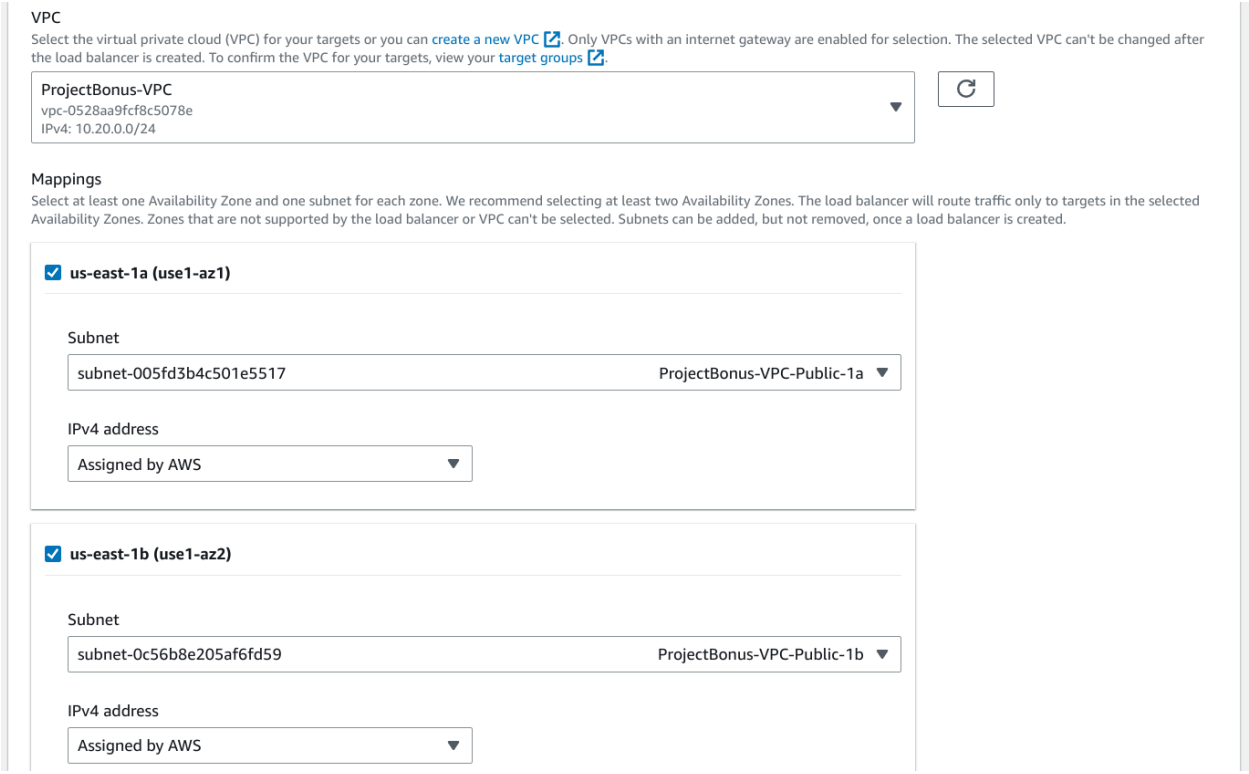
Load balancer target groups ProjectBonus-VPC-Apache-ALB-TG2	Classic Load Balancers -

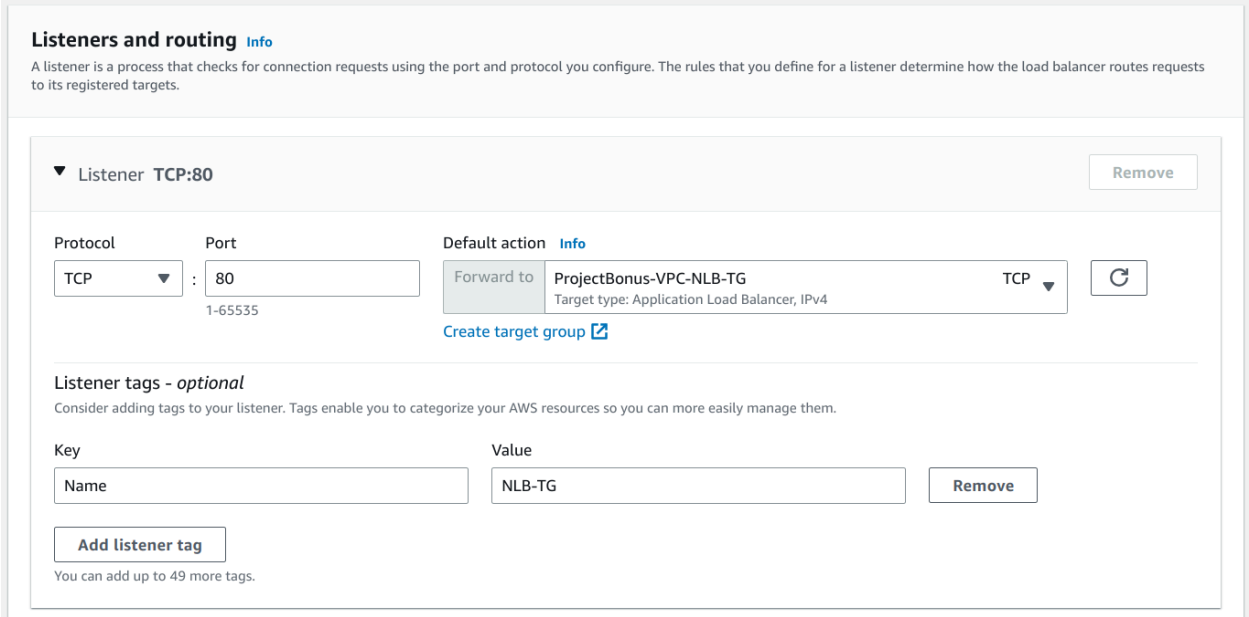
Step 7 - Connect to one of the instances from the ASG and check if the ALB's DNS redirects to the applications hosted in the private instances.

```
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"
```

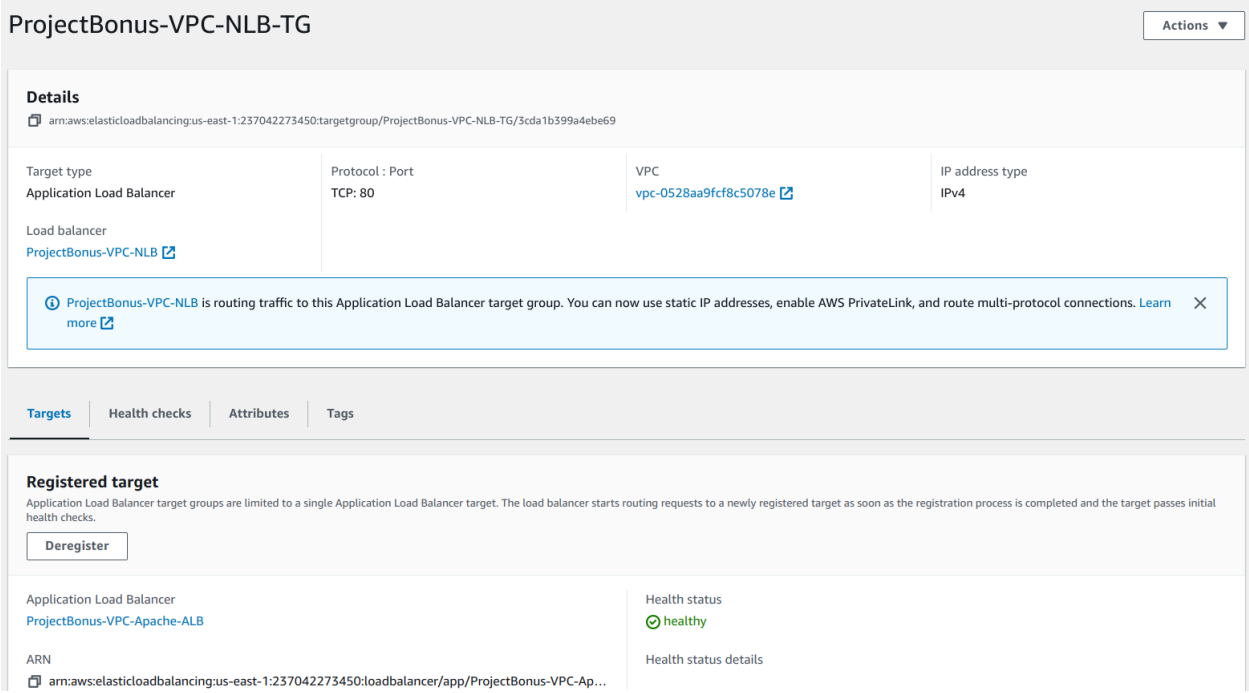
Step 8 - Create NLB in the public subnets.







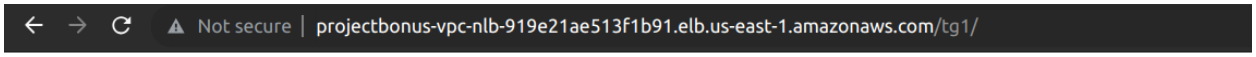
Target group for the NLB will include the ALB of a private subnet as the target. Traffic coming to the NLB will be redirected to the ALB and further to the private instances based on the url path.



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

- URL path for target group 1 -

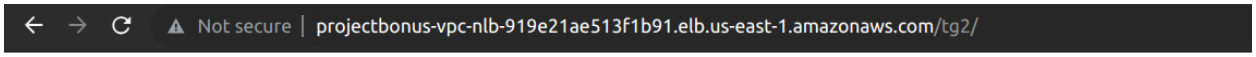
  "http://projectbonus-vpc-nlb-919e21ae513f1b91.elb.us-east-1.amazonaws.com/tg1/"



"Target group 1 ip-10-20-0-87.ec2.internal"

- URL path for target group 2 -

  "http://projectbonus-vpc-nlb-919e21ae513f1b91.elb.us-east-1.amazonaws.com/tg2/"



"Target group 2 ip-10-20-0-184.ec2.internal"