Application LoadBalancer Lab

ABC corporates have decided to host their couple of websites on AWS cloud.

Their requirement is for all their public websites they wanted to have same domain name and based on uri path the required page has to be loaded.

Currently they are looking at hosing website-1 and website-2 on AWS EC2 instances. Configure application load balancer to route the request to the required website.

Step 1: Use the same VPC created in Network LoadBalancer Lab

Step 2: Launch 2 EC2 ubuntu machines

Step 3: Install Apache 2 on both the EC2 machines

Step 4: Create 2 target groups separately and add each of the VMs created

Step 5:

Step 1 : Launch EC2 instances.

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	1	Load balancers	0
Placement groups	0	Security groups	4
Snapshots	0	Volumes	0

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-0ee02acd56a52998e (64-bit x86) / ami-0e011417bd70948da (64-bit Arm)

Select

64-bit (x86)
64-bit (Arm)

Ubuntu Server 16.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

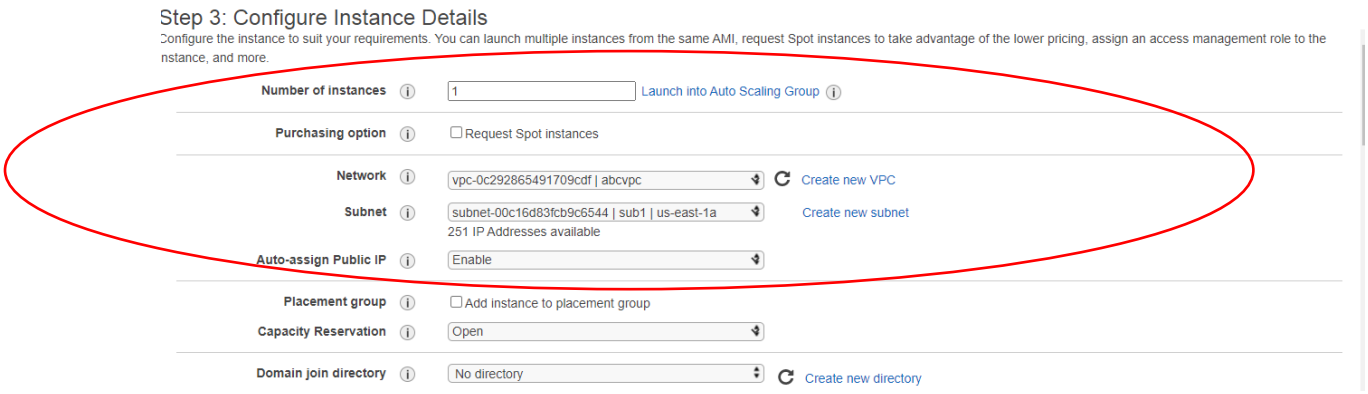
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

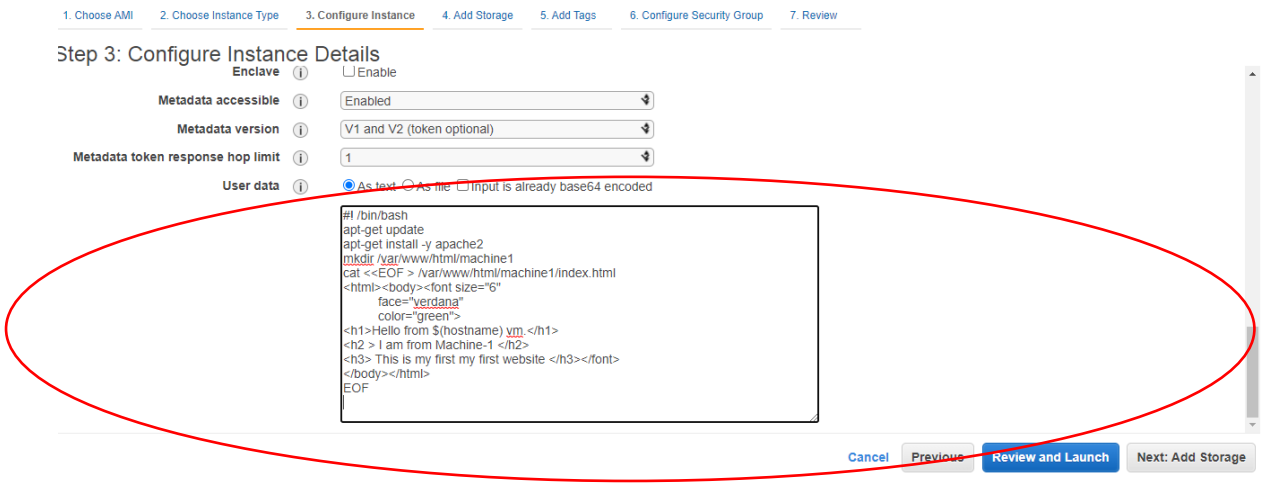


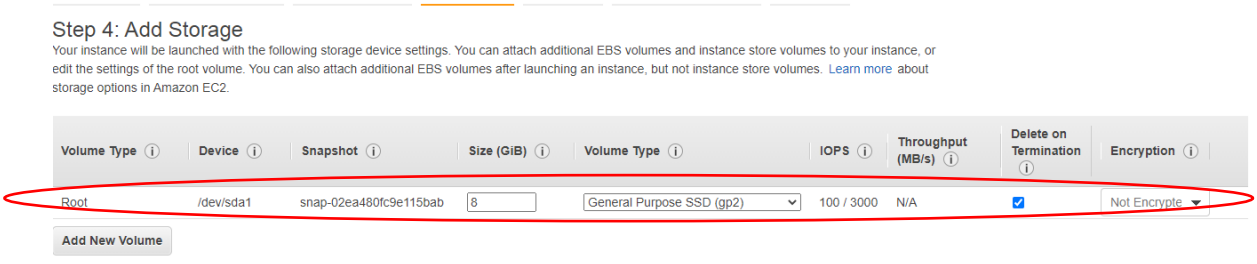

```
#! /bin/bash
apt-get update
apt-get install -y apache2
mkdir /var/www/html/machine1
cat <<EOF > /var/www/html/machine1/index.html
<html><body><font size="6"
        face="verdana"
        color="green">
<h1>Hello from $(hostname) vm.</h1>
><font size="5"
        face="verdana"
        color="blue">
<h2 > I am from Machine-1 </h2>
><font size="6"
        face="verdana"
        color="red">
```

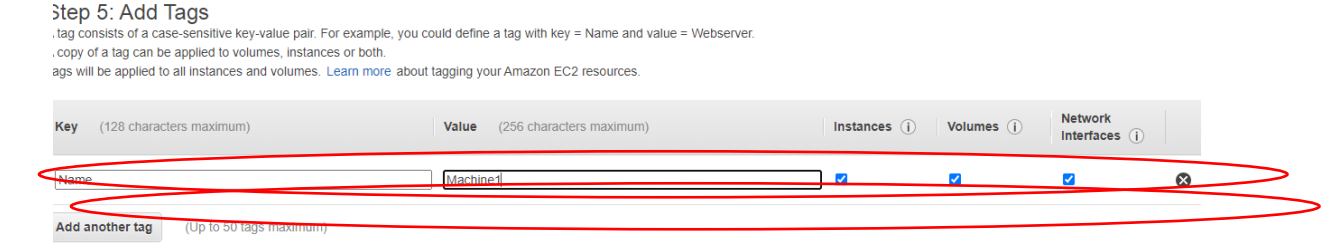
<h3> This is my first my first website </h3>

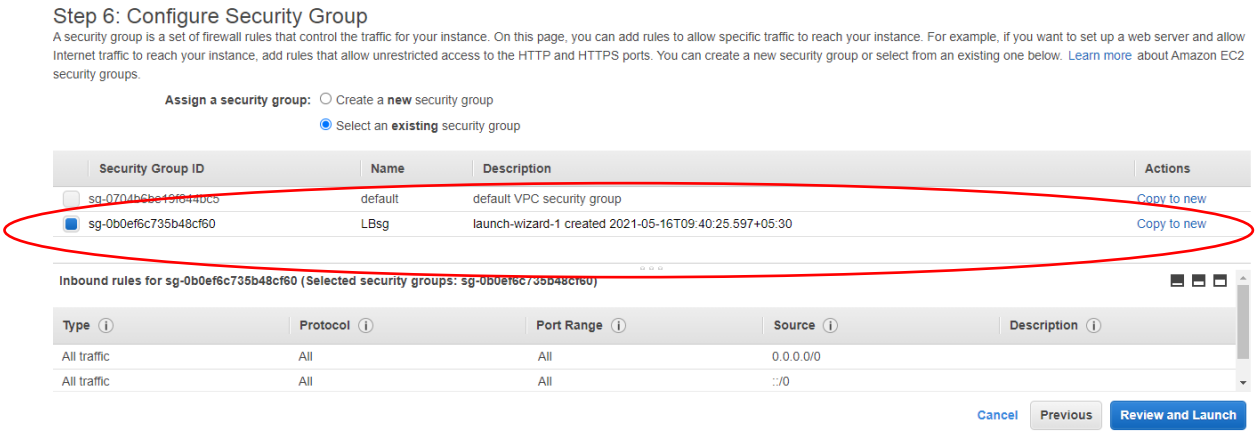
</body></html>

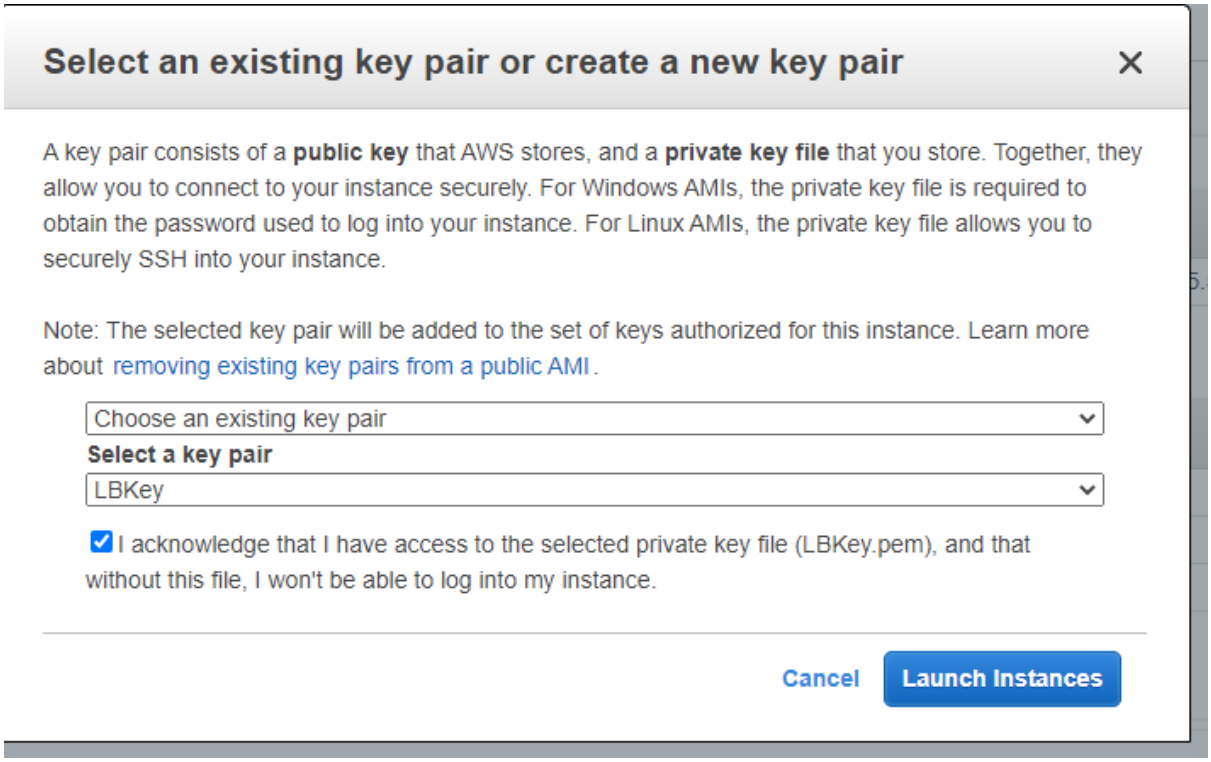
EOF











Similarly go and Launch Machine 2

#! /bin/bash

apt-get update

apt-get install -y apache2

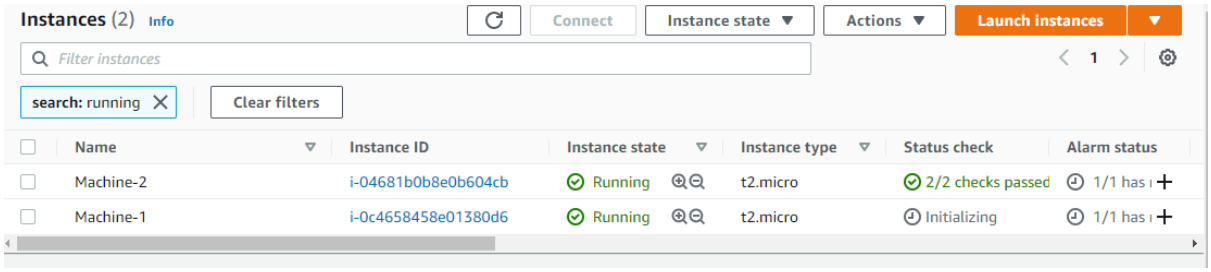
mkdir /var/www/html/machine2

cat <<EOF > /var/www/html/machine2/index.html

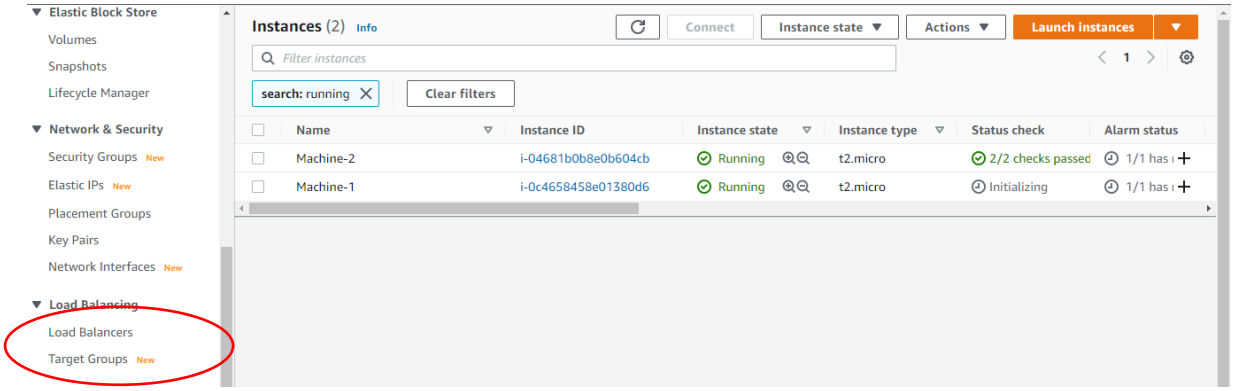
```
<html><body><font size="6"
        face="verdana"
        color="green">
<h1>Hello from $(hostname) vm.</h1>
<h2 > I am from Machine-2 </h2>
<h3> This is my second Website </h3></font>
</body></html>
EOF
```

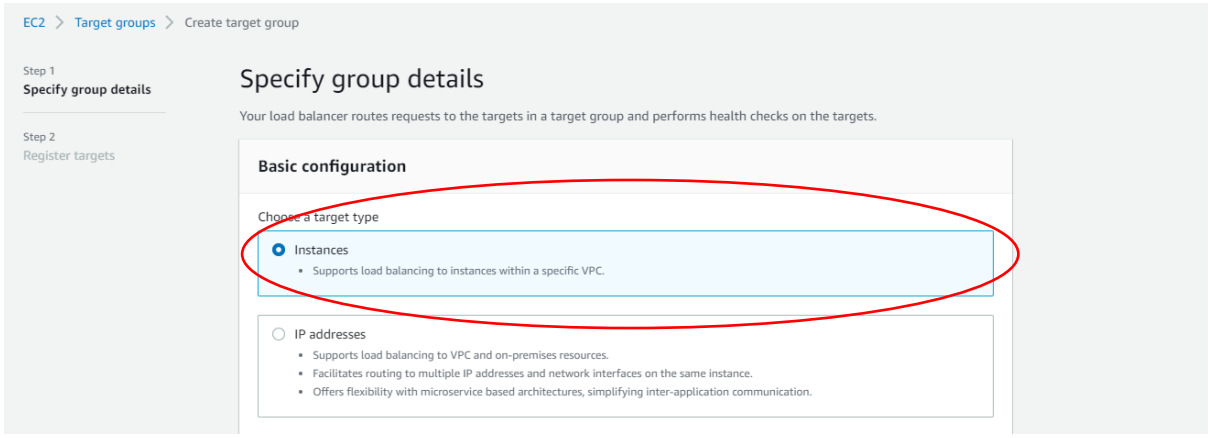
You could see both Machine 1 & Machine 2 running successfully.

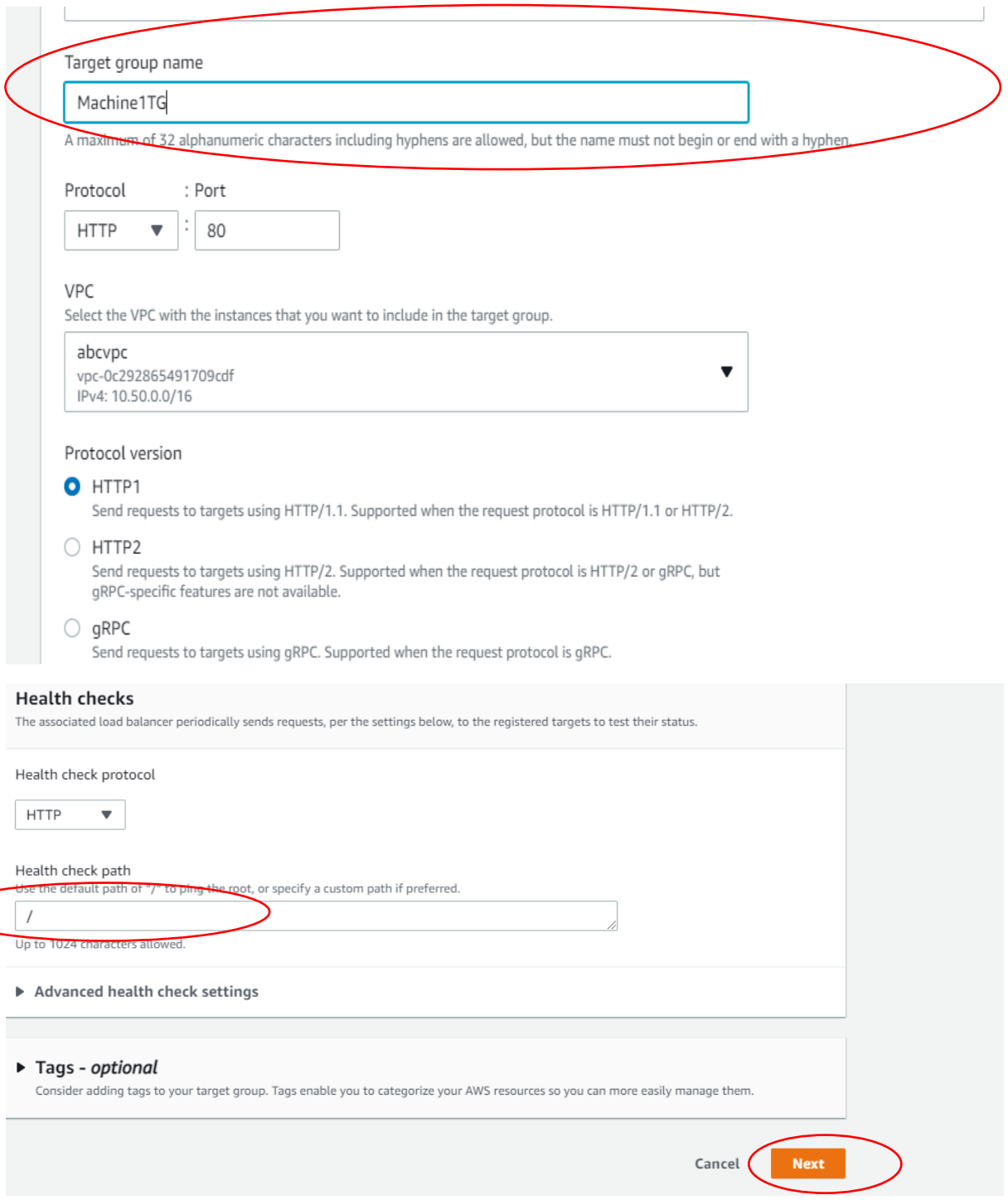
Use the public IP of both the VMs on browser to check whether apache2 was installed successfully as shown below

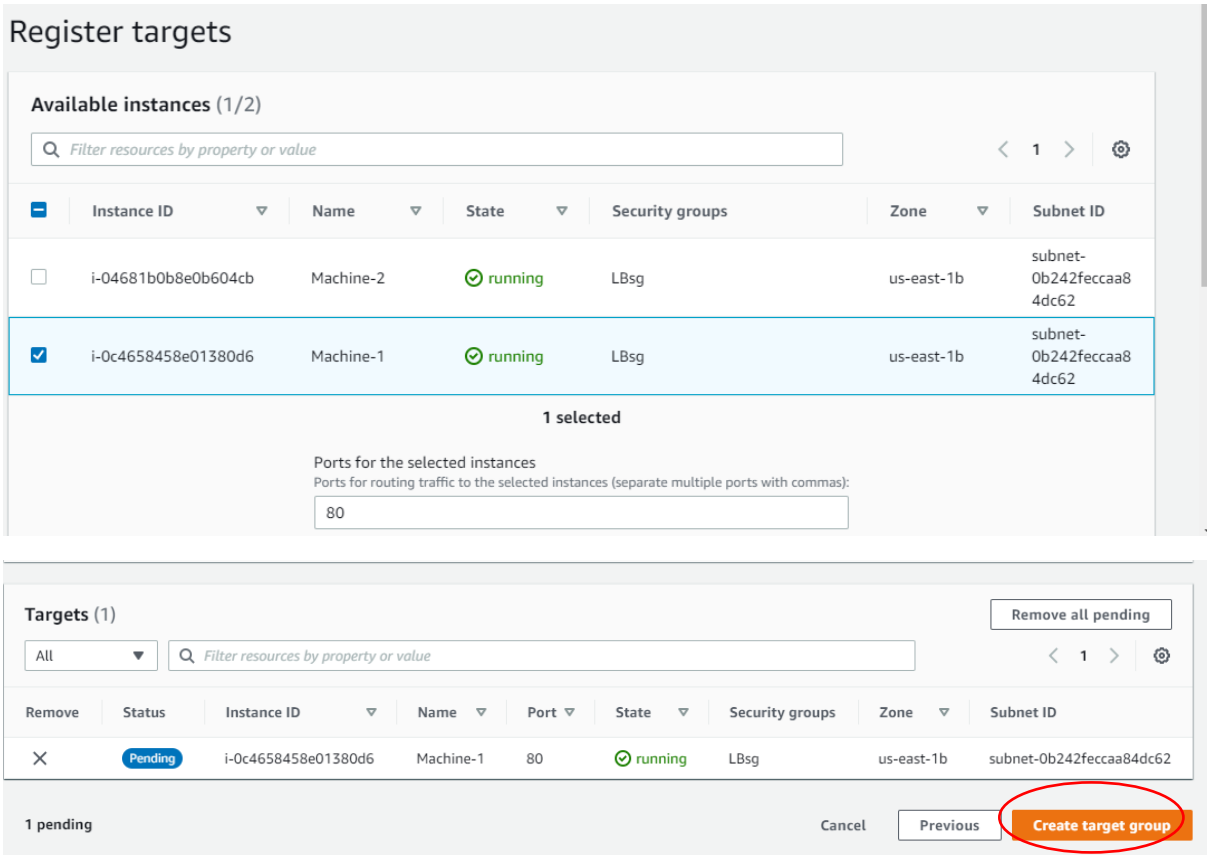


Create 2 targetgroup and add each VM to it.

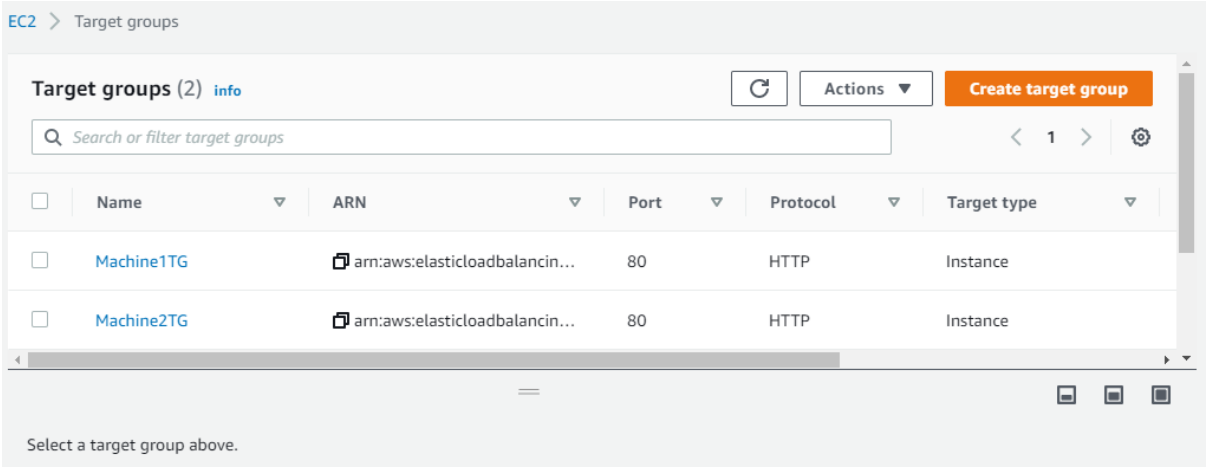





Target group name
Machine1TG
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.
Protocol
: Port
HTTP
80
VPC
Select the VPC with the instances that you want to include in the target group.
abcvpc
vpc-0c292865491709cdf
IPv4: 10.50.0.0/16
Protocol version
HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
HTTP2
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
gRPC
Send requests to targets using gRPC. Supported when the request protocol is gRPC.
Health checks
The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.
Health check protocol
HTTP
Health check path
Use the default path of "/" to ping the root, or specify a custom path if preferred.
/
Up to 1024 characters allowed.
Advanced health check settings
Tags - optional
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.
Cancel
Next



Similarly create Machine-2 target group.

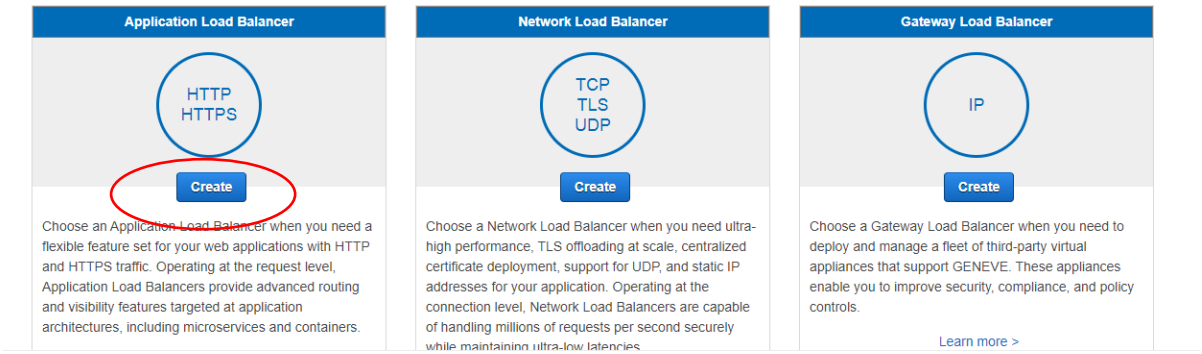


Click on LoadBalancers→Create Load Balancer

Select load balancer type

Elastic Load Balancing supports four types of load balancers: Application Load Balancers, Network Load Balancers, Gateway Load Balancers, and Classic Load Balancers. Choose the load balancer typ
your needs.

Learn more about which load balancer is right for you

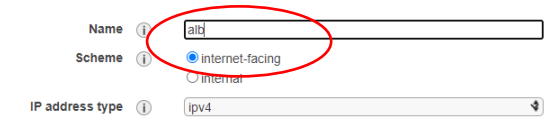


1. Configure Load Balancer | 2. Configure Security Settings | 3. Configure Security Groups | 4. Configure Routing | 5. Register Targets | 6. Review

Step 1: Configure Load Balancer

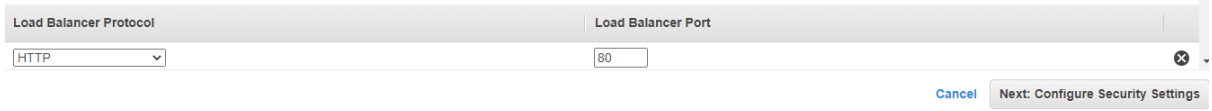
Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.



Listeners

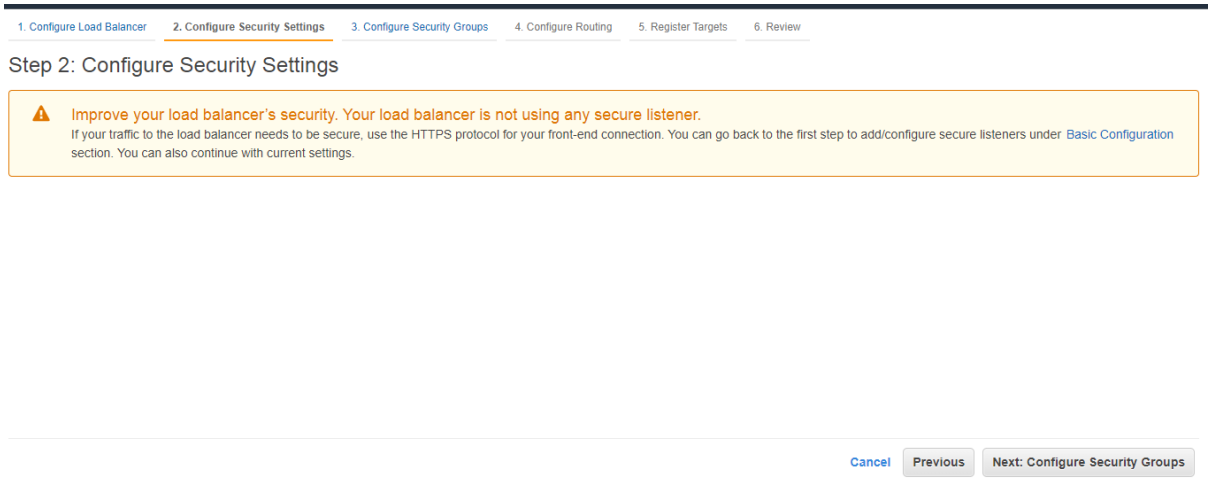
A listener is a process that checks for connection requests, using the protocol and port that you configured.

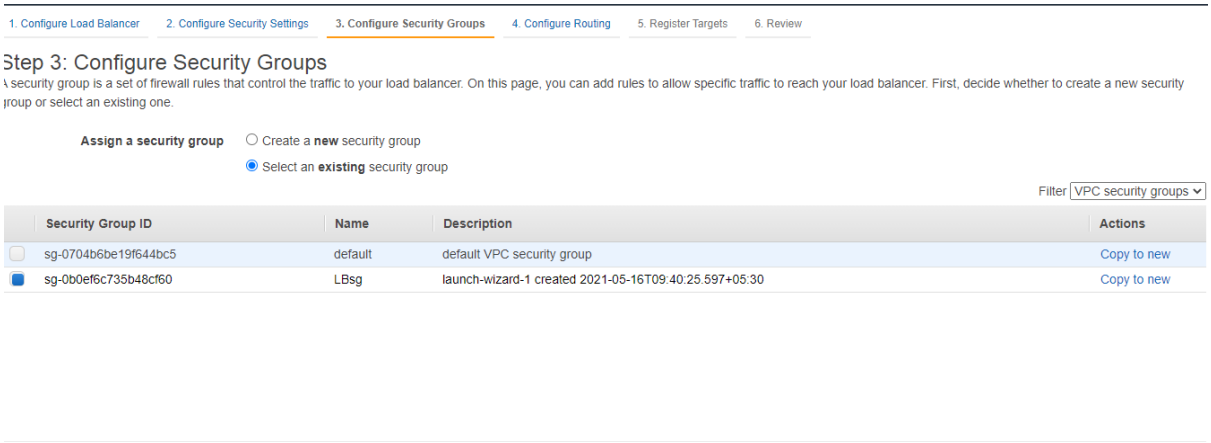


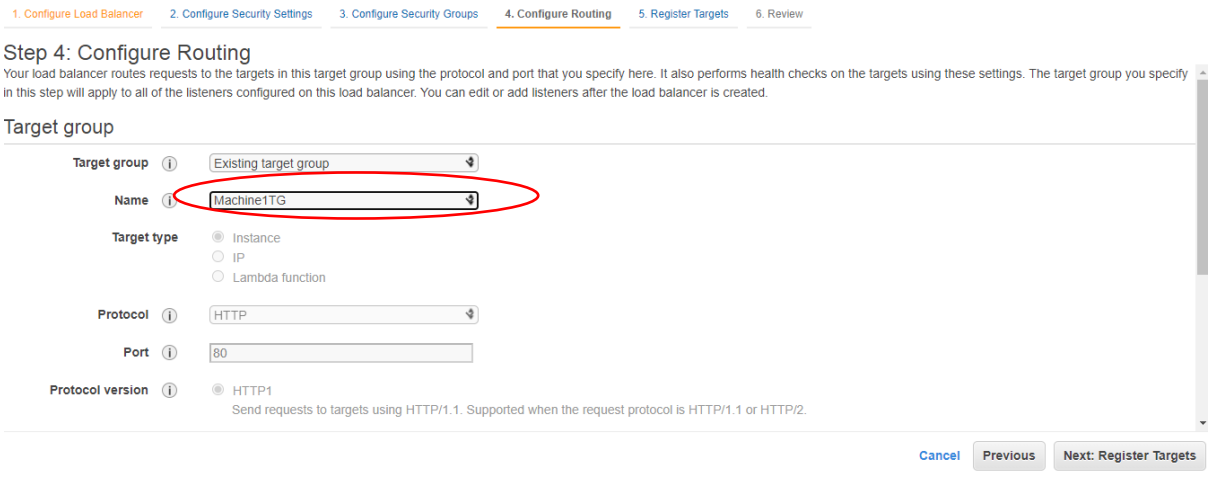
Cancel | Next: Configure Security Settings

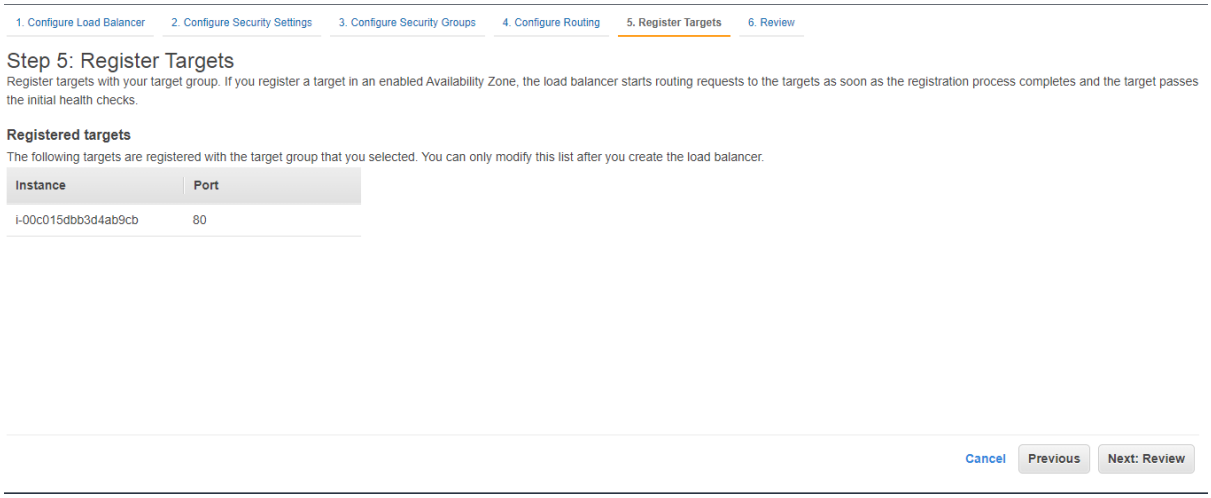
Step 1: Configure Load Balancer
Availability Zones

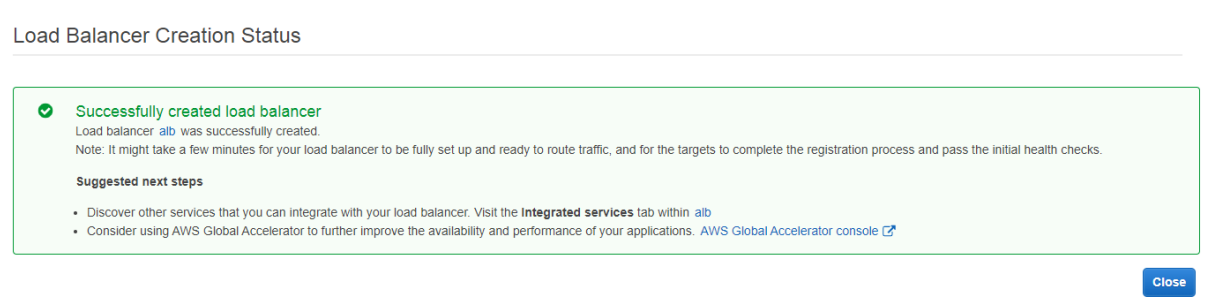
Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer.

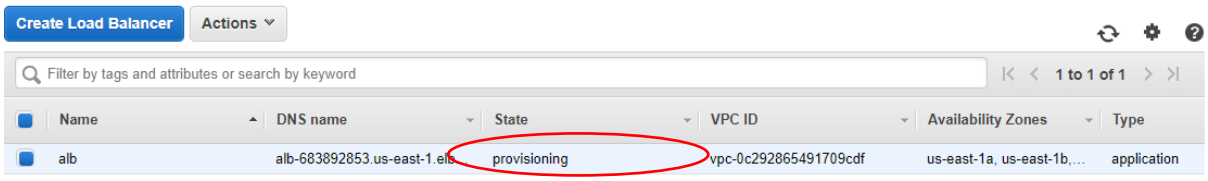

1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review
Step 2: Configure Security Settings
Improve your load balancer's security. Your load balancer is not using any secure listener.
If your traffic to the load balancer needs to be secure, use the HTTPS protocol for your front-end connection. You can go back to the first step to add/configure secure listeners under Basic Configuration section. You can also continue with current settings.
Cancel
Previous
Next: Configure Security Groups

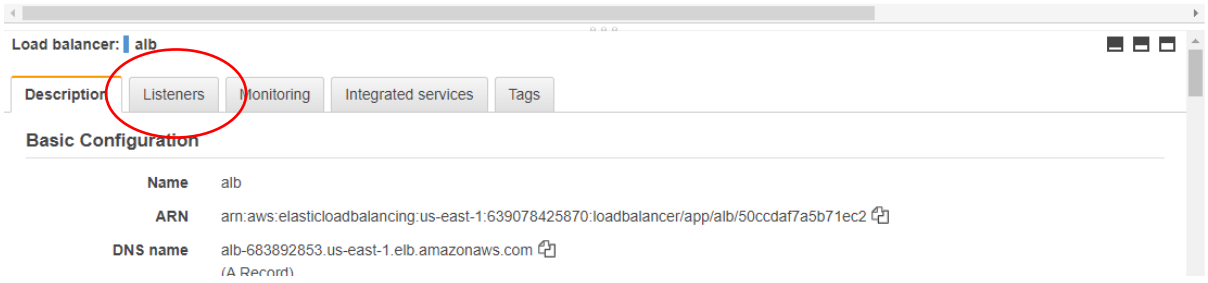

1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review
Step 3: Configure Security Groups
A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.
Assign a security group
Create a new security group
Select an existing security group
Filter VPC security groups
Security Group ID
Name
Description
Actions
sg-0704b6be19f644bc5
default
default VPC security group
Copy to new
sg-0b0ef6c735b48cf60
LBsg
launch-wizard-1 created 2021-05-16T09:40:25.597+05:30
Copy to new
Cancel
Previous
Next: Configure Routing

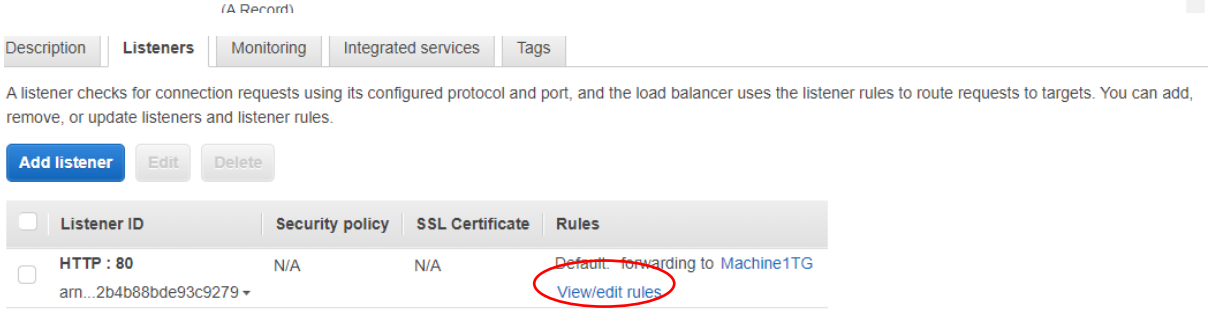

1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review
Step 4: Configure Routing
Your load balancer routes requests to the targets in this target group using the protocol and port that you specify here. It also performs health checks on the targets using these settings. The target group you specify in this step will apply to all of the listeners configured on this load balancer. You can edit or add listeners after the load balancer is created.
Target group
Target group
Existing target group
Name
Machine1TG
Target type
Instance
IP
Lambda function
Protocol
HTTP
Port
80
Protocol version
HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
Cancel
Previous
Next: Register Targets

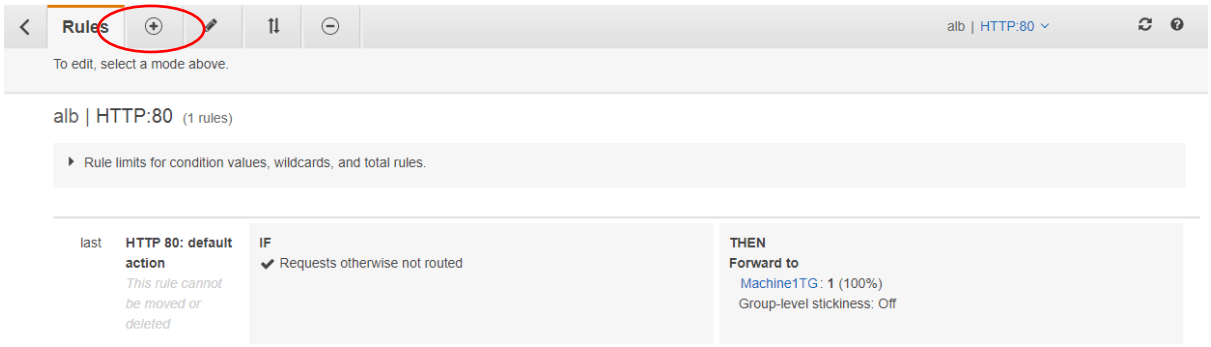

1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review
Step 5: Register Targets
Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.
Registered targets
The following targets are registered with the target group that you selected. You can only modify this list after you create the load balancer.
Instance
Port
i-00c015dbb3d4ab9cb
80
Cancel
Previous
Next: Review

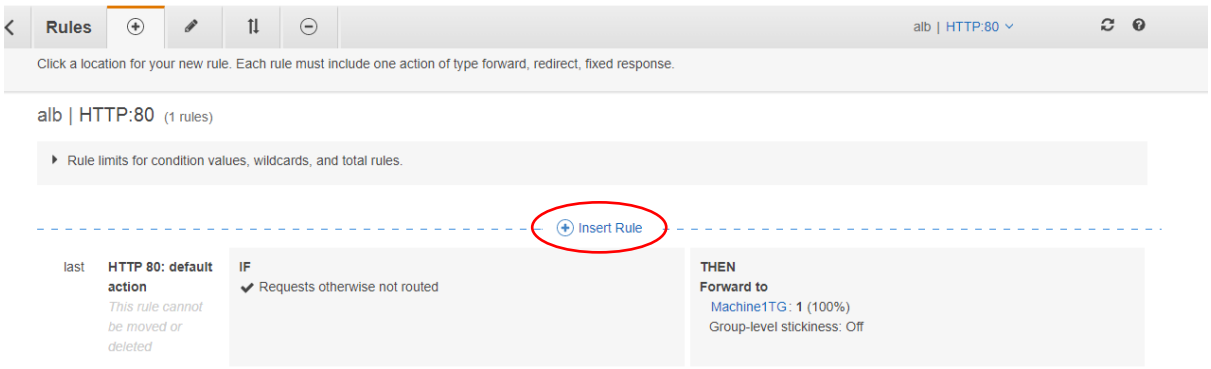

Load Balancer Creation Status
Successfully created load balancer
Load balancer alb was successfully created.
Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks.
Suggested next steps
Discover other services that you can integrate with your load balancer. Visit the Integrated services tab within alb
Consider using AWS Global Accelerator to further improve the availability and performance of your applications. AWS Global Accelerator console
Close

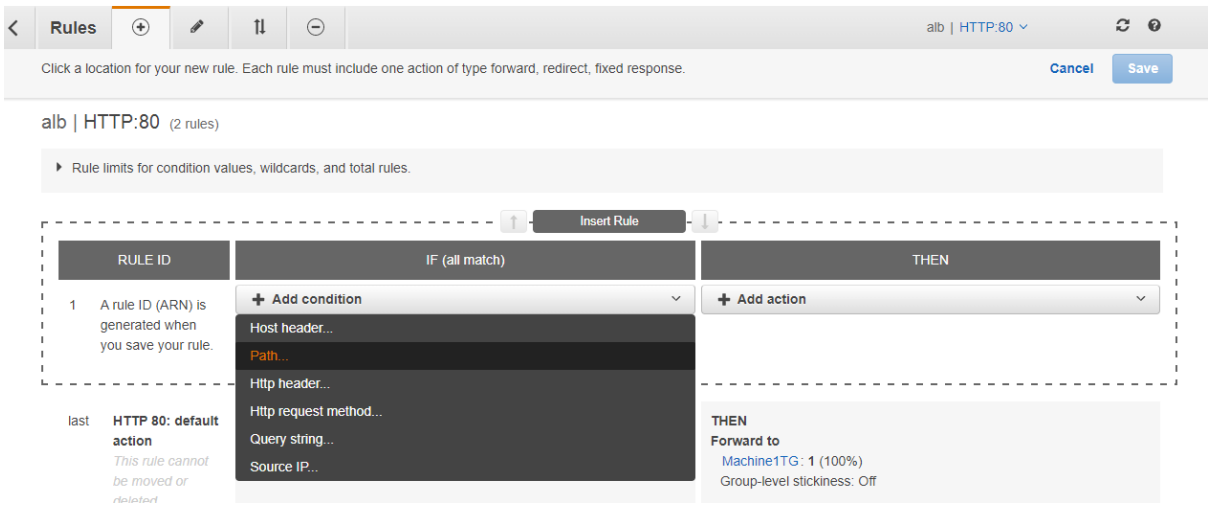

Create Load Balancer
Actions
Filter by tags and attributes or search by keyword
1 to 1 of 1
Name
DNS name
State
VPC ID
Availability Zones
Type
alb
alb-683892853.us-east-1.elb
provisioning
vpc-0c292865491709cdf
us-east-1a, us-east-1b,...
application

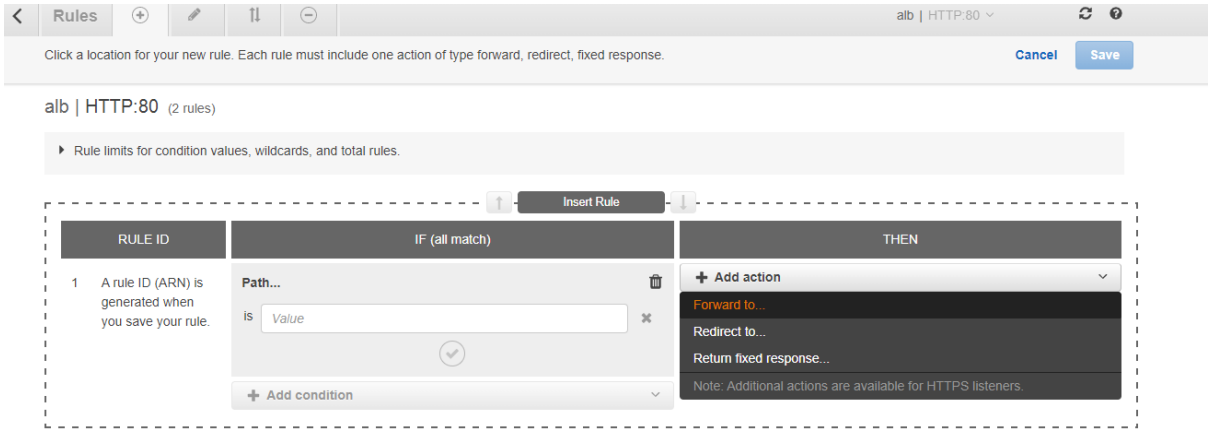

Load balancer: alb
Description
Listeners
Monitoring
Integrated services
Tags
Basic Configuration
Name
alb
ARN
arn:aws:elasticloadbalancing:us-east-1:639078425870:loadbalancer/app/alb/50ccdaf7a5b71ec2
DNS name
alb-683892853.us-east-1.elb.amazonaws.com
(A Record)

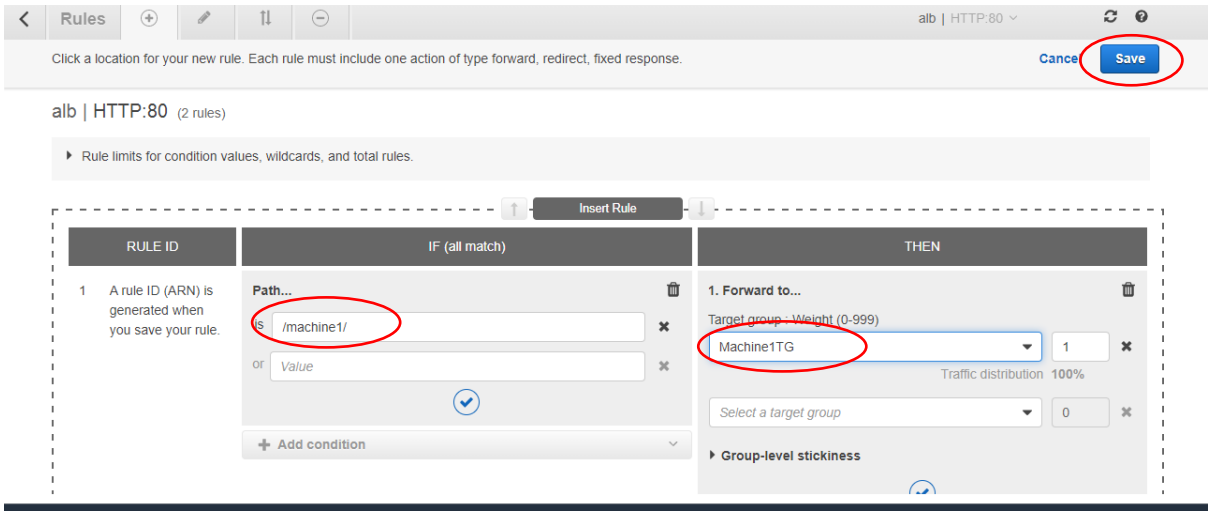

Description
Listeners
Monitoring
Integrated services
Tags
A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.
Add listener
Edit
Delete
Listener ID
Security policy
SSL Certificate
Rules
HTTP : 80
arn...2b4b88bde93c9279
N/A
N/A
Default: forwarding to Machine1TG
View/edit rules

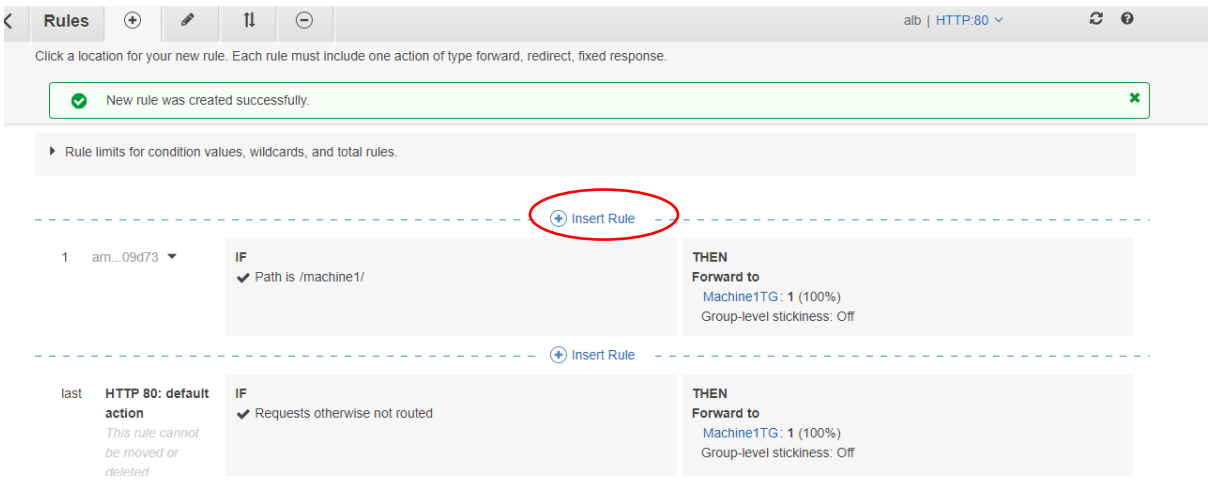

Rules
alb | HTTP:80
To edit, select a mode above.
alb | HTTP:80 (1 rules)
Rule limits for condition values, wildcards, and total rules.
last
HTTP 80: default action
This rule cannot be moved or deleted
IF
Requests otherwise not routed
THEN
Forward to
Machine1TG: 1 (100%)
Group-level stickiness: Off

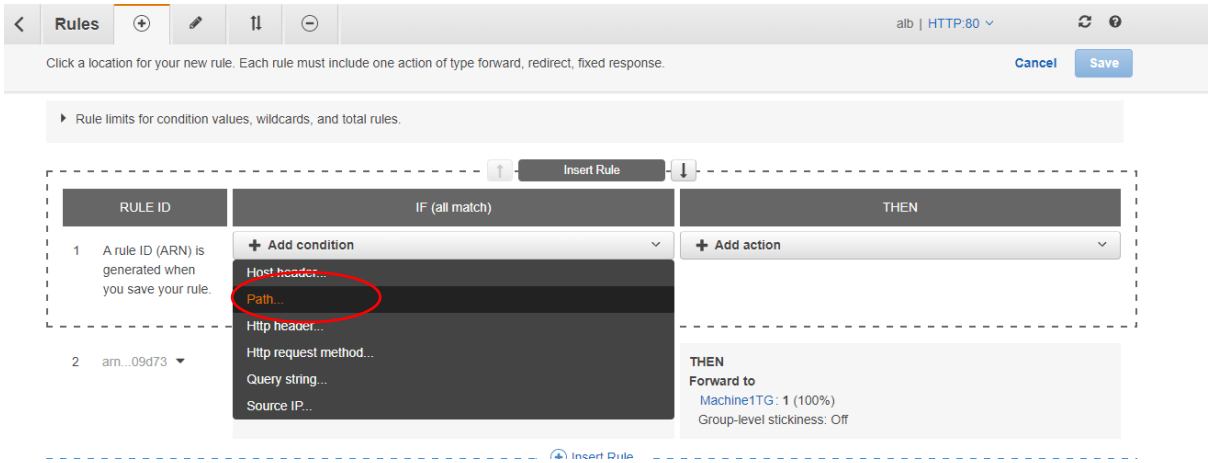

Rules
alb | HTTP:80
Click a location for your new rule. Each rule must include one action of type forward, redirect, fixed response.
alb | HTTP:80 (1 rules)
Rule limits for condition values, wildcards, and total rules.
Insert Rule
last
HTTP 80: default action
This rule cannot be moved or deleted
IF
Requests otherwise not routed
THEN
Forward to
Machine1TG: 1 (100%)
Group-level stickiness: Off

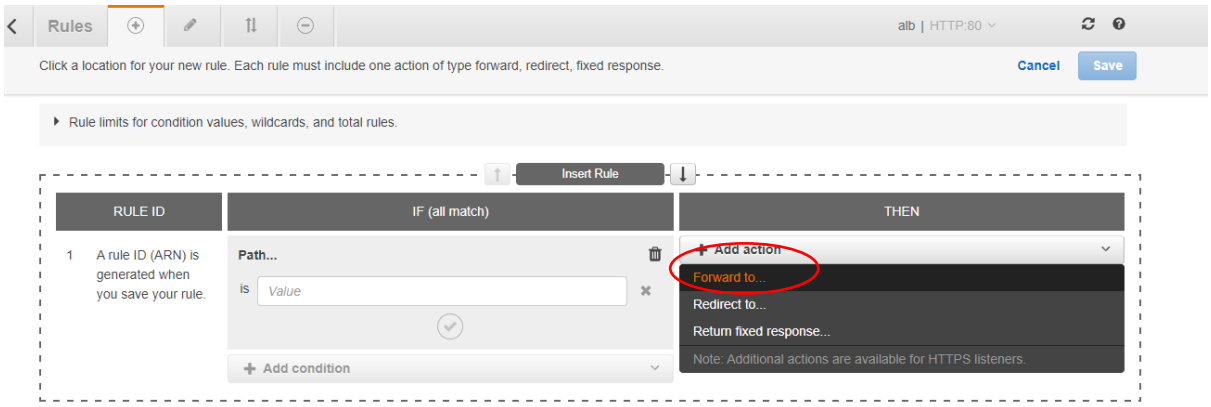

Rules
alb | HTTP:80
Click a location for your new rule. Each rule must include one action of type forward, redirect, fixed response.
Cancel
Save
alb | HTTP:80 (2 rules)
Rule limits for condition values, wildcards, and total rules.
Insert Rule
RULE ID
IF (all match)
THEN
1
A rule ID (ARN) is generated when you save your rule.
Add condition
Add action
Host header...
Path...
Http header...
Http request method...
Query string...
Source IP...
last
HTTP 80: default action
This rule cannot be moved or deleted
THEN
Forward to
Machine1TG: 1 (100%)
Group-level stickiness: Off

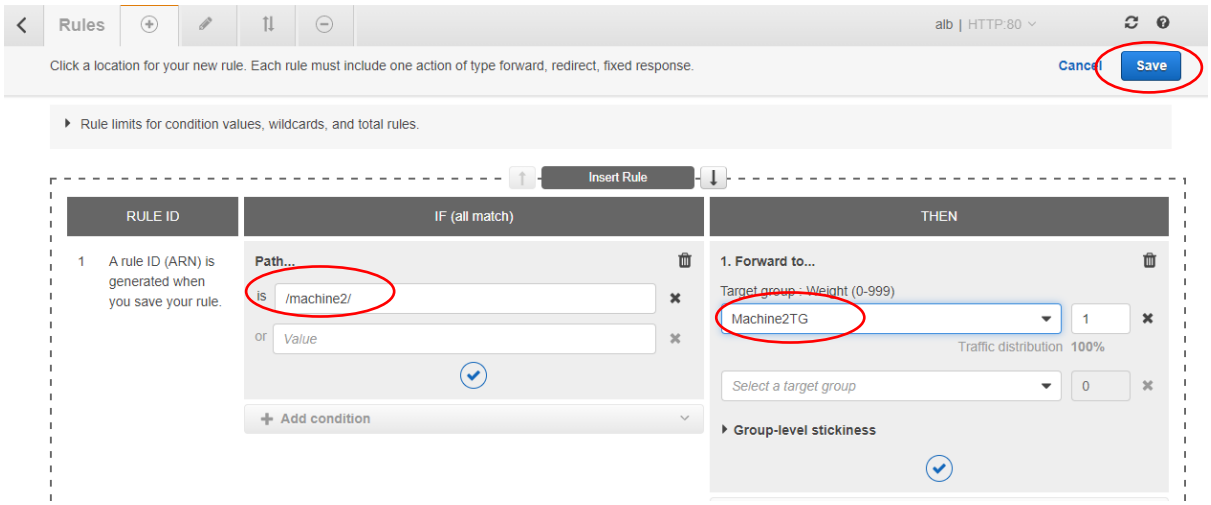

Rules
alb | HTTP:80
Click a location for your new rule. Each rule must include one action of type forward, redirect, fixed response.
Cancel
Save
alb | HTTP:80 (2 rules)
Rule limits for condition values, wildcards, and total rules.
Insert Rule
RULE ID
IF (all match)
THEN
1
A rule ID (ARN) is generated when you save your rule.
Path...
is
Value
Add condition
Add action
Forward to...
Redirect to...
Return fixed response...
Note: Additional actions are available for HTTPS listeners.

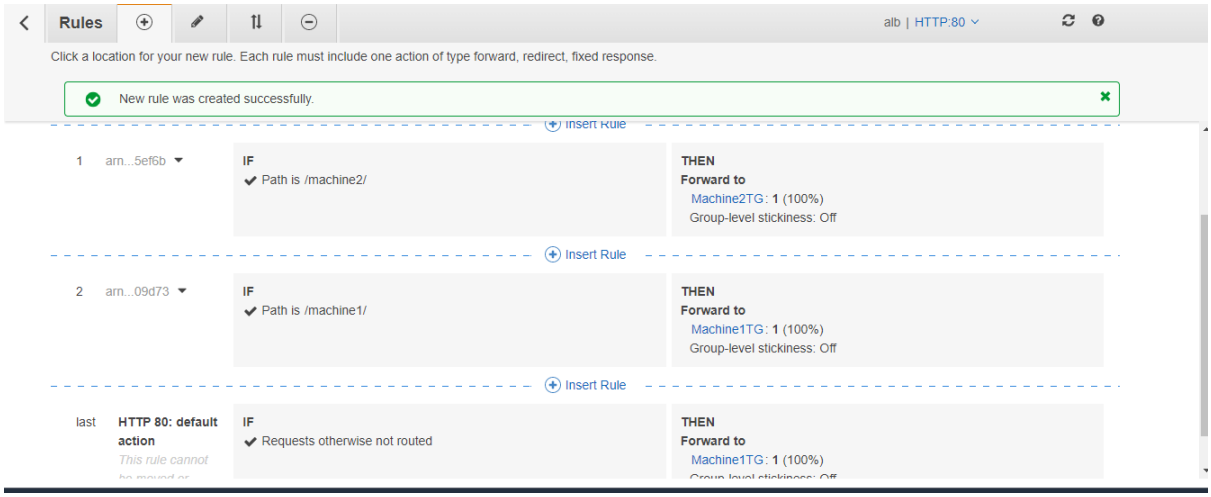

Rules
alb | HTTP:80
Click a location for your new rule. Each rule must include one action of type forward, redirect, fixed response.
Cancel
Save
alb | HTTP:80 (2 rules)
Rule limits for condition values, wildcards, and total rules.
Insert Rule
RULE ID
IF (all match)
THEN
1
A rule ID (ARN) is generated when you save your rule.
Path...
is
/machine1/
or
Value
Add condition
1. Forward to...
Target group : Weight (0-999)
Machine1TG
1
Traffic distribution 100%
Select a target group
0
Group-level stickiness

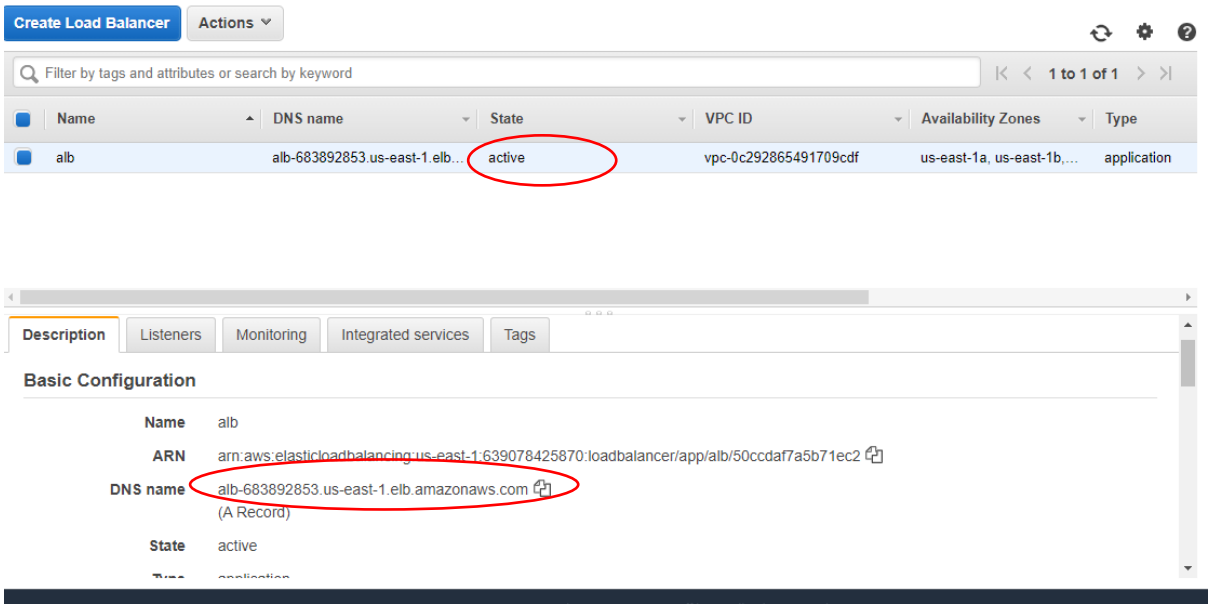

Rules
alb | HTTP:80
Click a location for your new rule. Each rule must include one action of type forward, redirect, fixed response.
New rule was created successfully.
Rule limits for condition values, wildcards, and total rules.
Insert Rule
1
arn...09d73
IF
Path is /machine1/
THEN
Forward to
Machine1TG: 1 (100%)
Group-level stickiness: Off
Insert Rule
last
HTTP 80: default action
This rule cannot be moved or deleted
IF
Requests otherwise not routed
THEN
Forward to
Machine1TG: 1 (100%)
Group-level stickiness: Off


Rules
alb | HTTP:80
Click a location for your new rule. Each rule must include one action of type forward, redirect, fixed response.
Cancel
Save
Rule limits for condition values, wildcards, and total rules.
Insert Rule
RULE ID
IF (all match)
THEN
1
A rule ID (ARN) is generated when you save your rule.
Add condition
Add action
Host header...
Path...
Http header...
Http request method...
Query string...
Source IP...
2
arn...09d73
THEN
Forward to
Machine1TG: 1 (100%)
Group-level stickiness: Off
Insert Rule


Rules
alb | HTTP:80
Click a location for your new rule. Each rule must include one action of type forward, redirect, fixed response.
Cancel
Save
Rule limits for condition values, wildcards, and total rules.
Insert Rule
RULE ID
IF (all match)
THEN
1
A rule ID (ARN) is generated when you save your rule.
Path...
is
Value
Add condition
Add action
Forward to...
Redirect to...
Return fixed response...
Note: Additional actions are available for HTTPS listeners.


Rules
alb | HTTP:80
Click a location for your new rule. Each rule must include one action of type forward, redirect, fixed response.
Cancel
Save
Rule limits for condition values, wildcards, and total rules.
Insert Rule
RULE ID
IF (all match)
THEN
1
A rule ID (ARN) is generated when you save your rule.
Path...
is
/machine2/
or
Value
Add condition
1. Forward to...
Target group : Weight (0-999)
Machine2TG
1
Traffic distribution 100%
Select a target group
0
Group-level stickiness



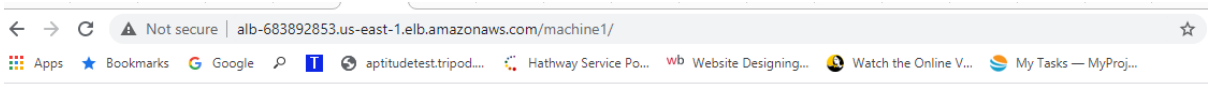


Copy the DNS name in Browser window

<DNS NAME>/machine1

alb-683892853.us-east-1.elb.amazonaws.com/machine1

you will see the output as below



Hello from ip-10-50-1-190 vm.

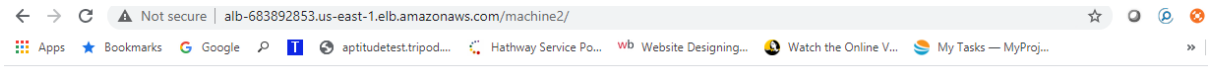
I am from Machine-1

This is my first my first website

Now route path machine2 keep the DNS Name same.

alb-683892853.us-east-1.elb.amazonaws.com/machine2/

You will see control routed to machine 2



Hello from ip-10-50-2-120 vm.

I am from Machine-2

This is my second Website

This completes the application load balancer.

Happy Learning!!!!!