

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

Free tier eligible

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

☒ 64-bit (x86)
☐ 64-bit (Arm)

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 |
|-------------------------------------|--------|--------------------------------|-------|--------------|-----------------------|-------------------------|---------------------|--------------|
| <input type="checkbox"/> | t2 | t2.nano | 1 | 0.5 | EBS only | | Low to Moderate | Yes |
| <input checked="" type="checkbox"/> | t2 | t2.micro Free tier eligible | 1 | 1 | EBS only | - | Low to Moderate | Yes |
| <input type="checkbox"/> | t2 | t2.small | 1 | 2 | EBS only | - | Low to Moderate | Yes |
| <input type="checkbox"/> | t2 | t2.medium | 2 | 4 | EBS only | - | Low to Moderate | Yes |
| <input type="checkbox"/> | t2 | t2.large | 2 | 8 | EBS only | - | Low to Moderate | Yes |

[Cancel](#)

[Previous](#)

[Review and Launch](#)

[Next: Configure Instance Details](#)

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

| | | |
|-----------------------|--|--|
| Number of instances | 1 | Launch into Auto Scaling Group |
| Purchasing option | <input type="checkbox"/> Request Spot instances | |
| Network | vpc-0c292865491709cdf abcvpc | Create new VPC |
| Subnet | subnet-00c16d83fcb9c6544 sub1 us-east-1a 251 IP Addresses available | Create new subnet |
| Auto-assign Public IP | Enable | |
| Placement group | <input type="checkbox"/> Add instance to placement group | |
| Capacity Reservation | Open | |
| Domain join directory | No directory | Create new directory |

```
#!/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

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Enclave ☐ Enable

Metadata accessible

Metadata version

Metadata token response hop limit

User data ☒ As text ☐ As file ☐ Input is already base64 encoded

```
#!/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>
<h2> I am from Machine-1 </h2>
<h3> This is my first my first website </h3></font>
</body></html>
EOF
```

Cancel Previous **Review and Launch** Next: Add Storage

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

| Volume Type | Device | Snapshot | Size (GiB) | Volume Type | IOPS | Throughput (MB/s) | Delete on Termination | Encryption |
|-------------|-----------|------------------------|------------|---------------------------|------------|-------------------|-------------------------------------|-------------|
| Root | /dev/sda1 | snap-02ea480fc9e115bab | 8 | General Purpose SSD (gp2) | 100 / 3000 | N/A | <input checked="" type="checkbox"/> | Not Encrypt |

Add New Volume

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

| Key | Value | Instances | Volumes | Network Interfaces |
|------|-----------|-------------------------------------|-------------------------------------|-------------------------------------|
| Name | Machinell | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add another tag (Up to 50 tags maximum)

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a new security group
☒ Select an existing security group

| Security Group ID | Name | Description | Actions |
|--|---------|---|-----------------------------|
| <input type="checkbox"/> sg-0704b6be1390440c5 | default | default VPC security group | Copy to new |
| <input checked="" type="checkbox"/> sg-0b0ef6c735b48cf60 | LBsg | launch-wizard-1 created 2021-05-16T09:40:25.597+05:30 | Copy to new |

Inbound rules for sg-0b0ef6c735b48cf60 (Selected security groups: sg-0b0ef6c735b48cf60)

| Type | Protocol | Port Range | Source | Description |
|-------------|----------|------------|-----------|-------------|
| All traffic | All | All | 0.0.0.0/0 | |
| All traffic | All | All | :::0 | |

[Cancel](#) [Previous](#) [Review and Launch](#)

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more](#) about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

LBKey

☒ I acknowledge that I have access to the selected private key file (LBKey.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#)

[Launch Instances](#)

Similarly go and Launch Machine 2

```
#!/bin/bash
```

```
apt-get update
```

```
apt-get install -y apache2
```

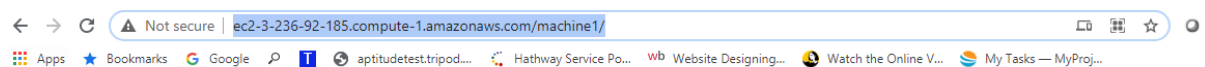
```
mkdir /var/www/html/machine2
```

```
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.

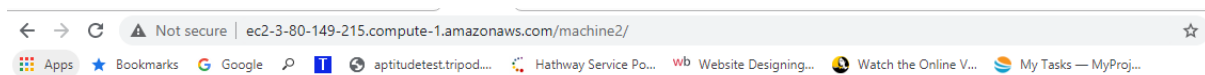
Use the public IP of both the VMs on browser to check whether apache2 was installed successfully as shown below



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

I am from Machine-1

This is my first my first website



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

I am from Machine-2

This is my second Website

Instances (2) Info

Filter instances

search: running X Clear filters

| | Name | Instance ID | Instance state | Instance type | Status check | Alarm status |
|--------------------------|-----------|---------------------|----------------|---------------|-------------------|--------------|
| <input type="checkbox"/> | Machine-2 | i-04681b0b8e0b604cb | Running | t2.micro | 2/2 checks passed | 1/1 has + |
| <input type="checkbox"/> | Machine-1 | i-0c4658458e01380d6 | Running | t2.micro | Initializing | 1/1 has + |

Create 2 targetgroup and add each VM to it.

Instances (2) Info

Filter instances

search: running X Clear filters

| | Name | Instance ID | Instance state | Instance type | Status check | Alarm status |
|--------------------------|-----------|---------------------|----------------|---------------|-------------------|--------------|
| <input type="checkbox"/> | Machine-2 | i-04681b0b8e0b604cb | Running | t2.micro | 2/2 checks passed | 1/1 has + |
| <input type="checkbox"/> | Machine-1 | i-0c4658458e01380d6 | Running | t2.micro | Initializing | 1/1 has + |

Load Balancing

Load Balancers

Target Groups New

EC2 > Target groups > Create target group

Step 1
Specify group details

Step 2
Register targets

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Choose a target type

☒ Instances

- Supports load balancing to instances within a specific VPC.

☐ 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.

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

Register targets

Available instances (1/2)

Filter resources by property or value

| | Instance ID | Name | State | Security groups | Zone | Subnet ID |
|-------------------------------------|---------------------|-----------|---------|-----------------|------------|--------------------------|
| <input type="checkbox"/> | i-04681b0b8e0b604cb | Machine-2 | running | LBsg | us-east-1b | subnet-0b242feccaa84dc62 |
| <input checked="" type="checkbox"/> | i-0c4658458e01380d6 | Machine-1 | running | LBsg | us-east-1b | subnet-0b242feccaa84dc62 |

1 selected

Ports for the selected instances
Ports for routing traffic to the selected instances (separate multiple ports with commas):

80

Targets (1)

Remove all pending

All Filter resources by property or value

| Remove | Status | Instance ID | Name | Port | State | Security groups | Zone | Subnet ID |
|-------------------------------------|---------|---------------------|-----------|------|---------|-----------------|------------|--------------------------|
| <input checked="" type="checkbox"/> | Pending | i-0c4658458e01380d6 | Machine-1 | 80 | running | LBsg | us-east-1b | subnet-0b242feccaa84dc62 |

1 pending

Cancel Previous **Create target group**

Similarly create Machine-2 target group.

EC2 > Target groups

Target groups (2) info

Search or filter target groups

| | Name | ARN | Port | Protocol | Target type |
|--------------------------|------------|--------------------------------|------|----------|-------------|
| <input type="checkbox"/> | Machine1TG | arn:aws:elasticloadbalancin... | 80 | HTTP | Instance |
| <input type="checkbox"/> | Machine2TG | arn:aws:elasticloadbalancin... | 80 | HTTP | Instance |

Select a target group above.

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 type that meets your needs.

[Learn more about which load balancer is right for you](#)

Application Load Balancer

HTTP
HTTPS

Create

Choose an Application Load Balancer when you need a flexible feature set for your web 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.

Network Load Balancer

TCP
TLS
UDP

Create

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 application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Gateway Load Balancer

IP

Create

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.

[Learn more >](#)

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.

Name

alb

Scheme

internet-facing

internal

IP address type

ipv4

Listeners

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

| Load Balancer Protocol | Load Balancer Port |
|------------------------|--------------------|
| HTTP | 80 |

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.

VPC

vpc-0c292865491709cdf (10.50.0.0/16) | abcvpc

Availability Zones

☒ us-east-1a

subnet-00c16d83fcb9c6544 (sub1)

IPv4 address

Assigned by AWS

☒ us-east-1b

subnet-0b242feccaa84dc62 (sub2)

IPv4 address

Assigned by AWS


☒ us-east-1c

subnet-0e542593e7f8bc157 (sub3)

IPv4 address

Assigned by AWS

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

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 |
|--|---------|---|-----------------------------|
| <input type="checkbox"/> sg-0704b6be19f644bc5 | default | default VPC security group | Copy to new |
| <input checked="" type="checkbox"/> sg-0b0ef6c735b48cf60 | LBsg | launch-wizard-1 created 2021-05-16T09:40:25.597+05:30 | Copy to new |

Cancel Previous Next: Configure Routing

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 i Existing target group

Name i Machine1TG

Target type ☒ Instance ☐ IP ☐ Lambda function

Protocol i HTTP

Port i 80

Protocol version i ☒ 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

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.amazonaws.com | 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/50ccda77a5b71ec2 |
| 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 <i>This rule cannot be moved or deleted</i> | 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.




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

+ 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

alb | HTTP:80 (2 rules)

▶ Rule limits for condition values, wildcards, and total rules.

↑

Insert Rule

↓

| RULE ID | IF (all match) | THEN |
|---------|---|---|
| 1 | <div><div><div><div><div><div>+</div>Add condition</div><div>Host header...</div><div>Path...</div><div>Http header...</div><div>Http request method...</div><div>Query string...</div><div>Source IP...</div></div></div><div></div></div></div> | <div><div><div><div><div>+</div>Add action</div></div></div></div> |
| last | HTTP 80: default action <i>This rule cannot be moved or deleted</i> | 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.

CancelSave

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. | <div>Path... is <input type="text" value="Value"/></div> <div>+ Add condition</div> | <div>+ Add action</div> <div>Forward to...</div> <div>Redirect to...</div> <div>Return fixed response...</div> <div>Note: Additional actions are available for HTTPS listeners.</div> |

Rules

alb | HTTP:80

Click a location for your new rule. Each rule must include one action of type forward, redirect, fixed response.

CancelSave

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. | <div>Path... <input type="text" value="/machine1/"/></div> <div>or <input type="text" value="Value"/></div> <div>+ Add condition</div> | <div>1. Forward to...</div> <div>Target group - Weight (0-999)</div> <div><input type="text" value="Machine1TG"/> 1</div> <div>Traffic distribution 100%</div> <div>Select a target group 0</div> <div>Group-level stickiness</div> |

Rules

alb | HTTP:80

New rule was created successfully.

Rule limits for condition values, wildcards, and total rules.

Insert Rule

| | | |
|---|--|--|
| 1 arn...09d73 | <div>IF</div> <div>✓ Path is /machine1/</div> | <div>THEN</div> <div>Forward to</div> <div>Machine1TG: 1 (100%)</div> <div>Group-level stickiness: Off</div> |
| last HTTP 80: default action This rule cannot be moved or deleted | <div>IF</div> <div>✓ Requests otherwise not routed</div> | <div>THEN</div> <div>Forward to</div> <div>Machine1TG: 1 (100%)</div> <div>Group-level stickiness: Off</div> |

< 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. | <div>+ Add condition</div> <div>Host header... Path... Http header... Http request method... Query string... Source IP...</div> | <div>+ Add action</div> <div>THEN Forward to Machine1TG: 1 (100%) Group-level stickiness: Off</div> |
| 2 arn...09d73 | | |

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. | <div>Path...</div> <div>is Value</div> <div>+ Add condition</div> | <div>+ Add action</div> <div>Forward to... Redirect to... Return fixed response... Note: Additional actions are available for HTTPS listeners.</div> |

< 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. | <div>Path...</div> <div>is /machine2/</div> <div>or Value</div> <div>+ Add condition</div> | <div>1. Forward to...</div> <div>Target group - Weight (0-999)</div> <div>Machine2TG 1</div> <div>Traffic distribution 100%</div> <div>Select a target group 0</div> <div>▶ Group-level stickiness</div> |

Rules

Click a location for your new rule. Each rule must include one action of type forward, redirect, fixed response.

New rule was created successfully.

1 **arn...5ef6b** IF ✓ Path is /machine2/ THEN Forward to Machine2TG: 1 (100%)
Group-level stickiness: Off

2 **arn...09d73** IF ✓ Path is /machine1/ THEN Forward to Machine1TG: 1 (100%)
Group-level stickiness: Off

last **HTTP 80: default action** IF ✓ Requests otherwise not routed THEN Forward to Machine1TG: 1 (100%)
This rule cannot be moved or Group-level stickiness: Off

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... | active | vpc-0c292865491709cdf | us-east-1a, us-east-1b,... | application |

Description Listeners Monitoring Integrated services Tags

Basic Configuration

Name alb

ARN [arn:aws:elasticloadbalancing:us-east-1:639078425870:loadbalancer/app/alb/50ccda7a5b71ec2](#)

DNS name [alb-683892853.us-east-1.elb.amazonaws.com](#) (A Record)

State active

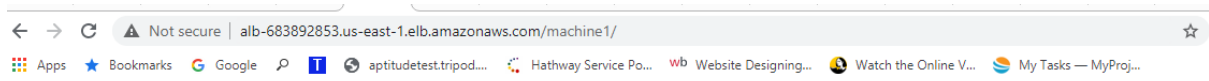
Type application

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.

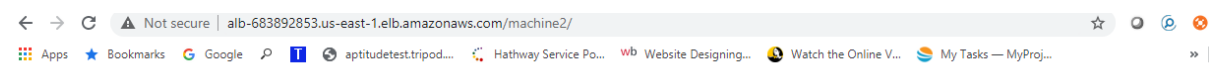
I am from Machine-1

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!!!!

