

Application Load Balancer & Target Groups

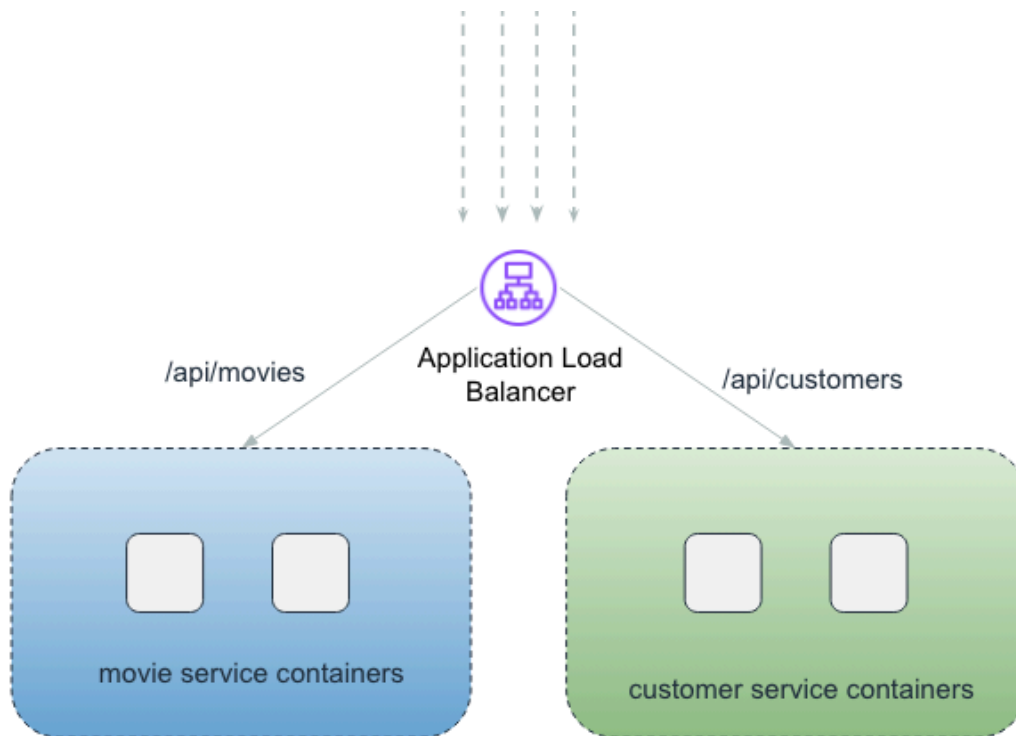
Target Groups	1
Movie Service Targets / Containers	2
Customer Service Targets / Containers	5
Application Load Balancer	7

Target Groups

We have 2 backend applications!

- customer-service
- movie-service

We will receive all the traffic via our Application Load Balancer. Based on the Path, we would route the requests to appropriate applications!



Movie Service Targets / Containers

- Select the target type as **IP addresses**

☒ 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.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

- Listening port will be 8080

Target group name

movie-service-containers

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

Protocol : Port

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

HTTP



8080

1-65535

- Select the VPC and the application protocol

VPC

Select the VPC that hosts the load balancer. Only VPCs that support the IP address type selected above are available in this list. On the **Register targets** page, you can register IP addresses from this VPC, or from private IP addresses located outside of this load balancer's VPC (such as a peered VPC, EC2-Classic, or on-premises targets that are reachable over Direct Connect or VPN).

netflux-vpc

vpc-057e4b12c96c3791e
IPv4 VPC CIDR: 10.0.0.0/16



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.

- Enter the health check details

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 perform health checks on the root, or specify a custom path if preferred.

/actuator/health

Up to 1024 characters allowed.

- advanced health check settings

Healthy Threshold

3

Unhealthy Threshold	3
Timeout	5 seconds
Interval	30 seconds
Success codes	200

▼ Advanced health check settings

Restore defaults

Health check port

The port the load balancer uses when performing health checks on targets. By default, the health check port is the same as the target group's traffic port. However, you can specify a different port as an override.

- ☒ Traffic port
- ☐ Override

Healthy threshold

The number of consecutive health checks successes required before considering an unhealthy target healthy.

3

2-10

Unhealthy threshold

The number of consecutive health check failures required before considering a target unhealthy.

3

2-10

Timeout

The amount of time, in seconds, during which no response means a failed health check.

5

seconds

2-120

Interval

The approximate amount of time between health checks of an individual target

30

seconds

5-300

Success codes

The HTTP codes to use when checking for a successful response from a target. You can specify multiple values (for example, "200,202") or a range of values (for example, "200-299").

200

- Click "Next"

- We can remove the IP addresses as we do not know them. When the app starts, they will register themselves!

Step 1: Choose a network

You can add IP addresses from the VPC selected for your target group or from outside the VPC. Note that you can assemble a mix of targets from multiple network sources by returning to this step and choosing another network.

Network

netflux-vpc
vpc-057e4b12c96c3791e
IPv4 VPC CIDR: 10.0.0.0/16

Step 2: Specify IPs and define ports

You can manually enter IP addresses from the selected network.

Enter an IPv4 address from a VPC subnet.

10.0.0.

Remove

Add IPv4 address

You can add up to 4 more IP addresses.

Remove IP address 10.0.0. on row 1

- Click on “Create Target Group”.
- Once created, Go to “Attributes” and “Edit”

Targets | Monitoring | Health checks | **Attributes** | Tags

Attributes

Edit

Target deregistration management

Deregistration delay (draining interval)

300 seconds

- **Reduce the time to 30 seconds** as 5 mins would be too much!

Deregistration delay (draining interval)

The time to wait for in-flight requests to complete while deregistering a target. During this time, the state of the target is draining.

30

seconds

0-3600 seconds

Customer Service Targets / Containers

- Repeat the above steps for “customer-service-containers”

Target group name

customer-service-containers

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

Protocol : Port

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

HTTP



8080

1-65535

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 perform health checks on the root, or specify a custom path if preferred.

/actuator/health

Up to 1024 characters allowed.

Healthy Threshold	3
Unhealthy Threshold	3
Timeout	5 seconds
Interval	30 seconds
Success codes	200

Targets

Monitoring

Health checks

Attributes

Tags

Attributes

Edit

Target deregistration management

Deregistration delay (draining interval)
30 seconds

Application Load Balancer

- Let's create an application load balancer. It is **internet facing**!

Load balancer name

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

netflux-alb

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

Scheme [Info](#)

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. Compatible with the **IPv4** and **Dualstack** IP address types.

- Select VPC and Subnets. Our ALB will be placed under the public subnets!

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC [Info](#)

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](#).

netflux-vpc

vpc-057e4b12c96c3791e
IPv4 VPC CIDR: 10.0.0.0/16



Mappings [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

☒ us-east-1a (use1-az1)

Subnet

subnet-05b695fccfbce21ee

netflux-subnet-public1-us-east-1a

IPv4 address

Assigned by AWS

☒ us-east-1b (use1-az2)

Subnet

subnet-07253a8d320578845

netflux-subnet-public2-us-east-1b

IPv4 address

Assigned by AWS

- Attach the “**netflux-alb-sg**”

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

Security groups

Select up to 5 security groups ▼ ↻

netflux-alb-sg

sg-0a799e4078dcfad76 VPC: vpc-057e4b12c96c3791e

×

- Our ALB will listen on port 80. We need to provide the default target group. select “movie-service-containers”. We can update the rules later.

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 HTTP:80 Remove

Protocol

HTTP ▼

:

Port

80

1-65535

Default action [Info](#)

Forward to

movie-service-containers

Target type: IP, IPv4

HTTP ▼

↻

[Create target group](#)

- Click on “Create Load Balancer”

Listener Rules

- Once ALB is created, go to “Listeners and rules”

< **Listeners and rules** | Network mapping | Resource map - new | Security | Monitoring | Integrations >

Listeners and rules (1) [Info](#)

↻

Manage rules ▼

Manage listener ▼

Add listener

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

< 1 > ⚙

<input type="checkbox"/>	Protocol:Port ▼	Default action ▼	Rules ▼	ARN ▼	Security
<input type="checkbox"/>	HTTP:80	Forward to target group <ul style="list-style-type: none">movie-service-containers ↗: 1 (100%)Target group stickiness: Off	1 rule	📄 ARN	Not ap

- Click on “1 rule” to update the rules for this listener.
- Click on “Add rule”. Let’s add 2 rules based on the Path.

Rules
Tags

Listener rules (1) [Info](#)
[Rule limits](#)
↺
Actions ▼
Add rule

Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.

⚙️

<input type="checkbox"/>	Name tag	Priority ▲	Conditions (If)	Actions (Then)
<input type="checkbox"/>	Default	Last (default)	If no other rule applies	Forward to target group <ul style="list-style-type: none"> movie-service-containers Target group stickiness: Off

Add rule [Info](#)

Define the rule and then review it in the context of the other rules on this listener.

▶ **Listener details:** HTTP:80

Name and tags [Info](#)

Tags can help you manage, identify, organize, search for and filter resources.

Name
[Add additional tags](#)

Cancel
Next

- Add condition

Conditions (0)
[Rule limits](#)

No conditions

No conditions to display.

Add condition

- We need the “Path” based routing.
 - Any “**/api/movies***” should go to **movie-service-containers**

Add condition Rule limits



Rule condition types

Route traffic based on the condition type of each request. Each rule can include one of each of the following conditions: host-header, path, http-request-method and source-ip. Each rule can include one or more of each of the following conditions: http-header and query-string.

Path ▼

Path

Define the path. For example: /item/*. Case sensitive.

is



Maximum 128 characters. Allowed characters are `a-z`, `A-Z`, `0-9`; the following special characters: `_.$/~"!@:+`; `&` (using `&`); and wildcards (`*` and `?`).

Add new value

You can add up to 4 more condition values for this rule.

Cancel

Confirm

Conditions (1)

Rule limits

Edit

Delete

Add condition

Path (1) [Info](#)



If

Path

is

/api/movies*

AND

- Click on “Next”
- Select the appropriate target. In this case, It is as shown below.

Actions

Action types

Routing actions

☒ Forward to target groups

☐ Redirect to URL

☐ Return fixed response

Forward to target group [Info](#)

Choose a target group and specify routing weight or [Create target group](#).

Target group

movie-service-containers

Target type: IP, IPv4

HTTP ▼



Weight

1

0-999

Percent

100%

- We have to set the priority. I give **500**.

Rule: all movies requests

Priority

Rule priority controls the evaluation order of a rule within the listener's set of rules. You can leave gaps in priority numbers.

500

1 - 50000

- Create the rule. We should see 2 rules as shown below.

[Rules](#) | [Tags](#)

Listener rules (2) [Info](#) [Rule limits](#) [Refresh](#) [Actions ▼](#) [Add rule](#)

Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.

<input type="checkbox"/>	Name tag	Priority ▲	Conditions (If)	Actions (Then)	ARN
<input type="checkbox"/>	all movies requests	500	Path Pattern is /api/movies*	Forward to target group <ul style="list-style-type: none">movie-service-containers: 1 (100%)Target group stickiness: Off	ARN
<input type="checkbox"/>	Default	Last (default)	If no other rule applies	Forward to target group <ul style="list-style-type: none">movie-service-containers: 1 (100%)Target group stickiness: Off	ARN

- We can edit the “Default” rule.

Rules | Tags

Listener rules (1/2) [Info](#)

Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest.

[Rule limits](#) [Refresh](#) [Actions](#) [Add rule](#)

[View rule](#)
[Edit rule](#)
[Delete rule](#)
[Reprioritize rules](#)

<input type="checkbox"/>	Name tag	Priority	Conditions (If)	Actions (Then)
<input type="checkbox"/>	all movies requests	500	Path Pattern is /api/movies*	Forward to target group <ul style="list-style-type: none"> movie-service-containers: 1 (100%) Target group stickiness: Off
<input checked="" type="checkbox"/>	Default	Last (default)	If no other rule applies	Forward to target group <ul style="list-style-type: none"> movie-service-containers: 1 (100%) Target group stickiness: Off

- We can change the default response as shown below or anything you prefer!

Default actions | [Info](#)

The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Routing actions

☐ Forward to target groups
 ☐ Redirect to URL
 ☒ Return fixed response

Return fixed response | [Info](#)

Use fixed-response actions to drop client requests and return a custom HTTP response. When a fixed-response action is taken, the action and the URL of the redirect target are recorded in the access logs.

Response code
 The type of message you want to send.

2xx, 4xx, 5xx

Content type - optional
 The format of your message.

Response body - optional
 Enter your response message.

1024 character maximum

- Repeat the same for customer-service requests. Finally we should have 3 rules as shown below.

RulesTags					
<div><div>Listener rules (3)<div>Info</div></div><div>Rule limits</div><div>Actions</div><div>Add rule</div></div> <div>Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.</div> <div><div>Filter rules</div><div></div></div>					
<input type="checkbox"/>	Name tag	Priority ▲	Conditions (If)	Actions (Then)	ARN
<input type="checkbox"/>	all movies requests	500	Path Pattern is /api/movies*	<div>Forward to target group</div> <ul style="list-style-type: none">movie-service-containers ↗: 1 (100%)Target group stickiness: Off	<div>ARN</div>
<input type="checkbox"/>	all customer requests	1000	Path Pattern is /api/customers/*	<div>Forward to target group</div> <ul style="list-style-type: none">customer-service-containers ↗: 1 (100%)Target group stickiness: Off	<div>ARN</div>
<input type="checkbox"/>	Default	Last (default)	If no other rule applies	<div>Return fixed response</div> <ul style="list-style-type: none">Response code: 404Response body: {Response content type: text/plain	<div>ARN</div>