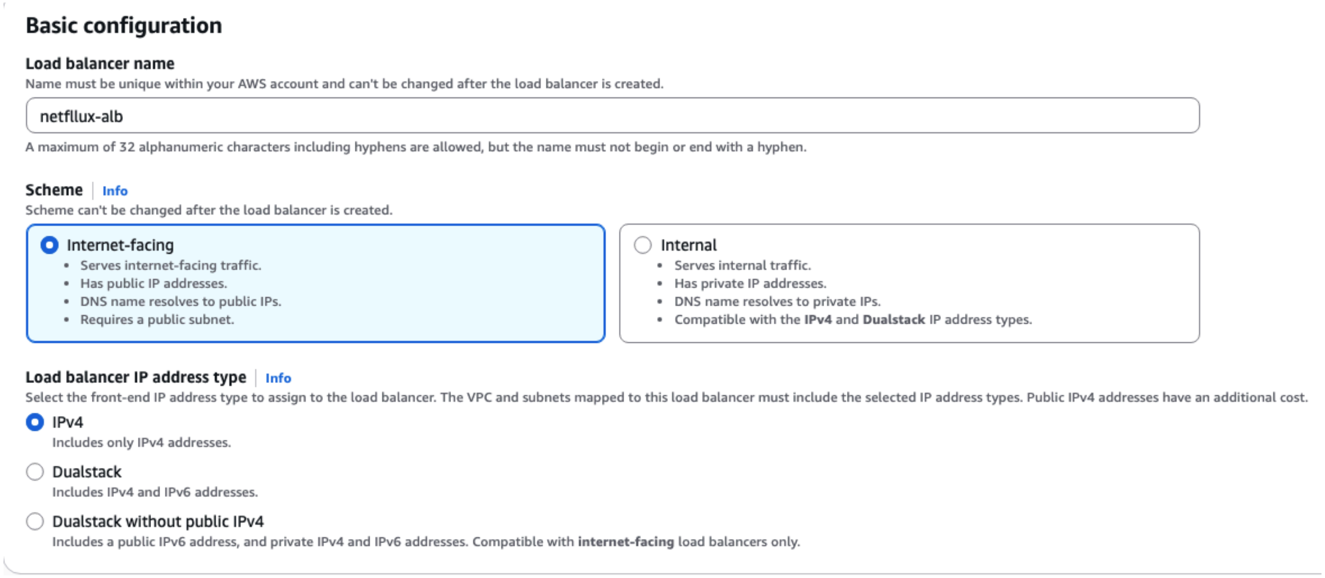
Application Load Balancer

Create ALB 1
Listener Rules 3
Verify 8

Create ALB

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



Basic configuration

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

netfllux-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
- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name resolves to public IPs.
- Requires a public subnet.

○ Internal
- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- Compatible with the **IPv4** and **Dualstack** IP address types.

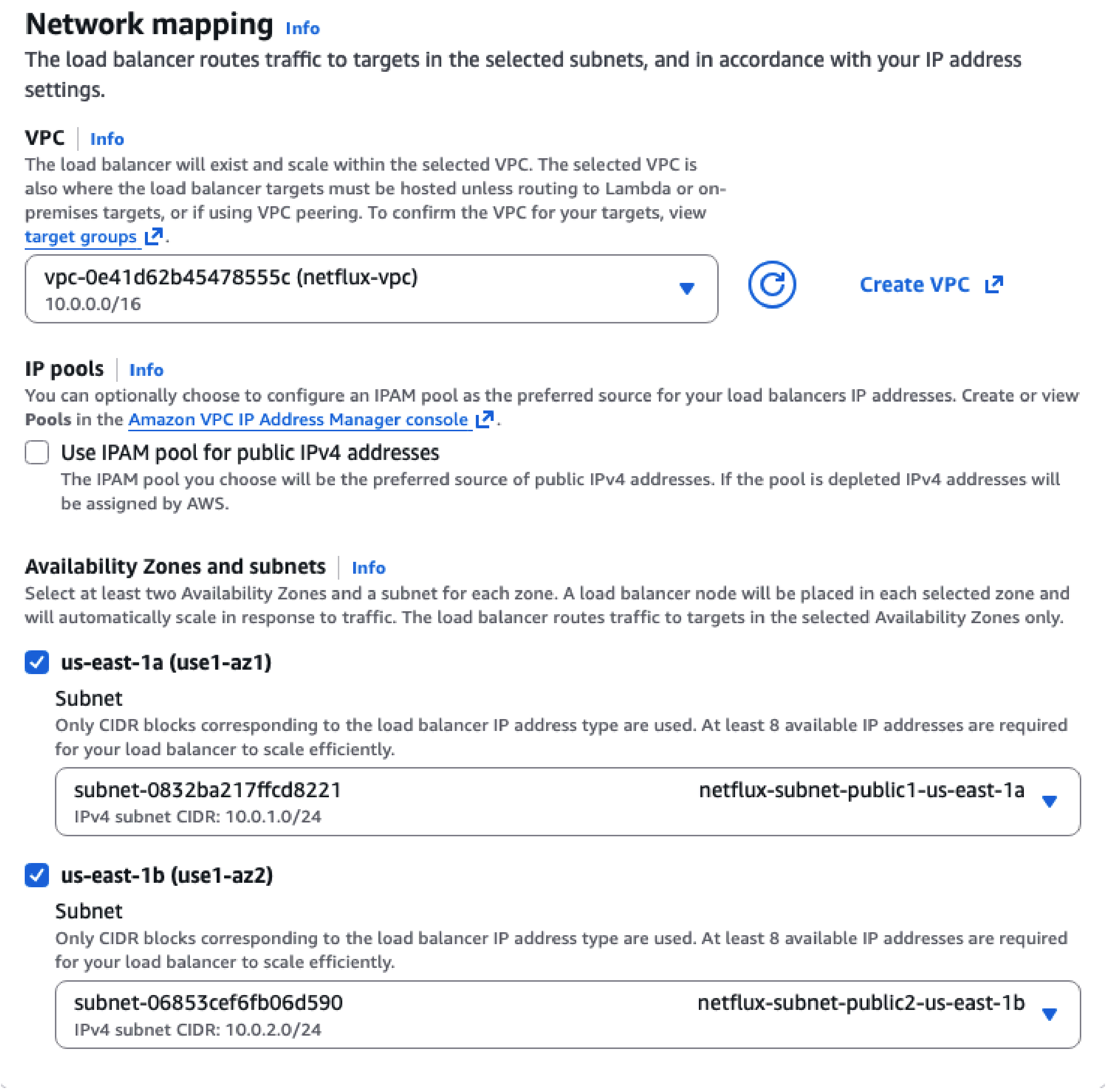
Load balancer IP address type | Info
Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

● IPv4
Includes only IPv4 addresses.

○ Dualstack
Includes IPv4 and IPv6 addresses.

○ Dualstack without public IPv4
Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

- Select VPC and Subnets. Our ALB will be placed under the public subnets! So ensure that you have selected **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

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view target groups.

vpc-0e41d62b45478555c (netflux-vpc)
10.0.0.0/16

IP pools | Info

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view **Pools** in the Amazon VPC IP Address Manager console.

□ Use IPAM pool for public IPv4 addresses

The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

Availability Zones and subnets | Info

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

☑ us-east-1a (use1-az1)

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-0832ba217ffcd8221 netflux-subnet-public1-us-east-1a
IPv4 subnet CIDR: 10.0.1.0/24

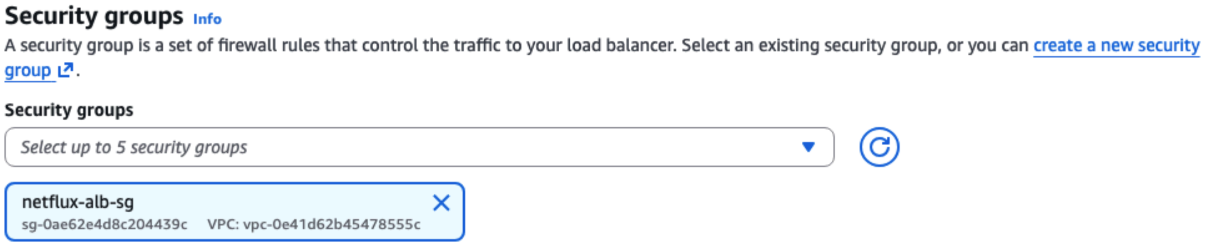
☑ us-east-1b (use1-az2)

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-06853cef6fb06d590 netflux-subnet-public2-us-east-1b
IPv4 subnet CIDR: 10.0.2.0/24

- Under Security Groups Configuration, Attach the “**netflux-alb-sg**”



Security groups Info

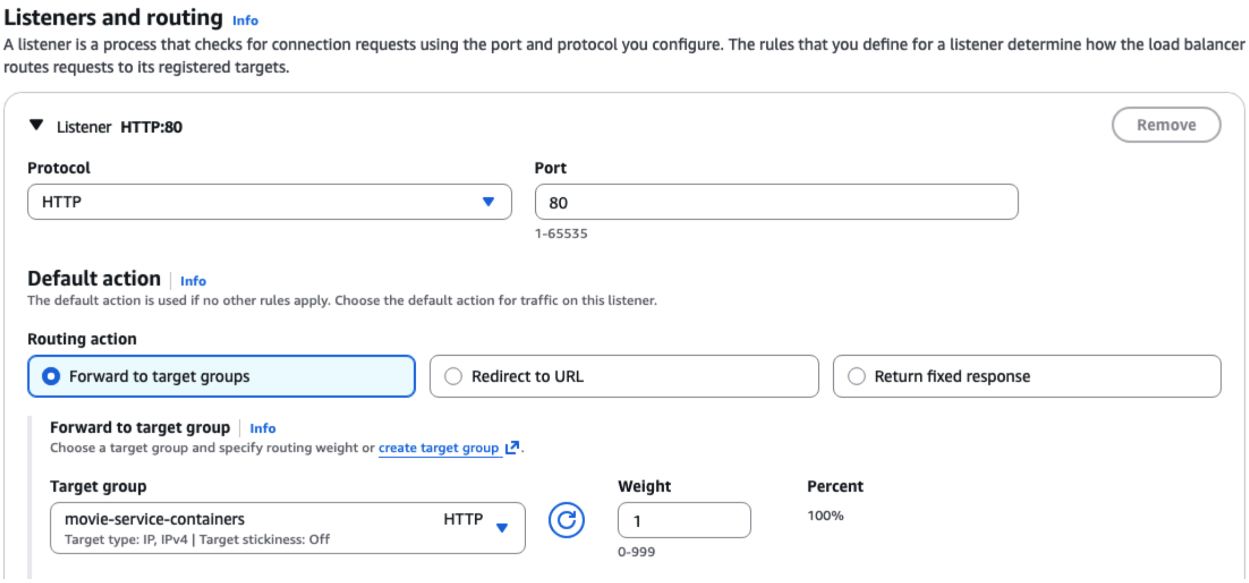
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

Select up to 5 security groups

netflux-alb-sg
sg-0ae62e4d8c204439c VPC: vpc-0e41d62b45478555c

- Under “**Listeners and routing**” configuration, 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

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**

Protocol: HTTP

Port: 80 (1-65535)

Default action

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

Routing action

● Forward to target groups ○ Redirect to URL ○ Return fixed response

Forward to target group

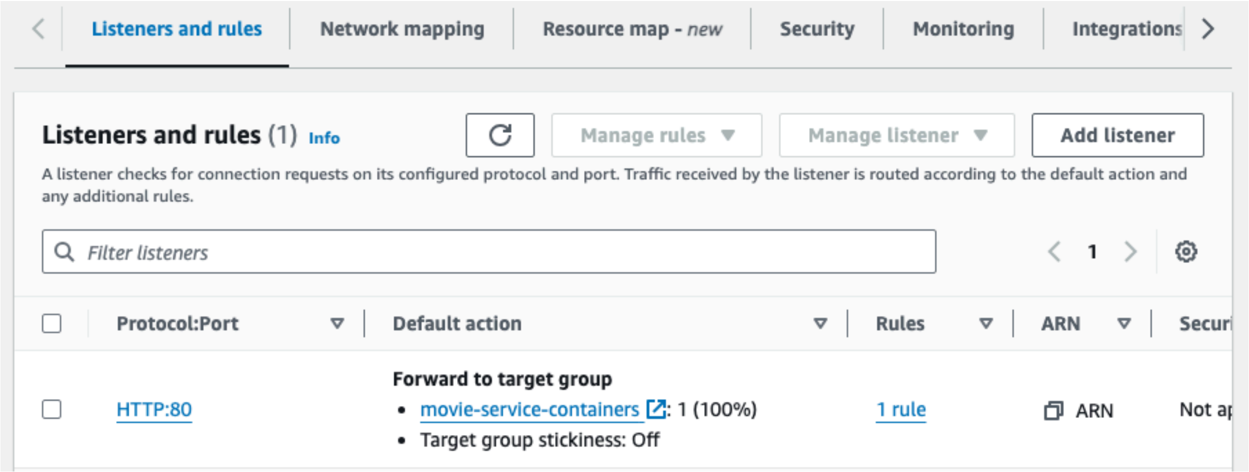
Choose a target group and specify routing weight or create target group.

Target group	Weight	Percent
movie-service-containers HTTP Target type: IP, IPv4 | Target stickiness: Off	1 0-999	100%

- Click on “Create Load Balancer”

Listener Rules

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

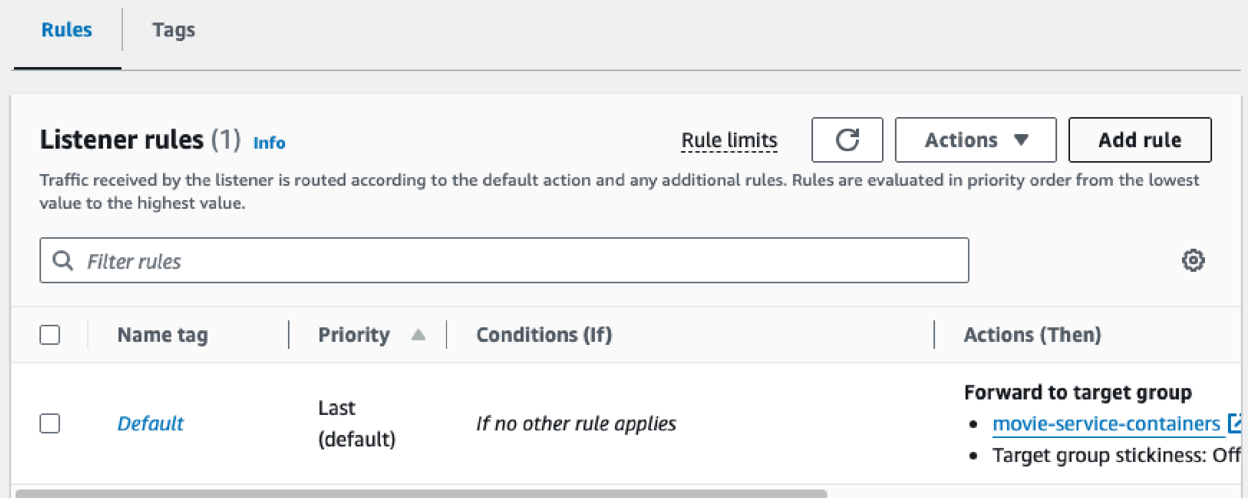


Listeners and rules (1)

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.

□	Protocol:Port	Default action	Rules	ARN	Securi
□	HTTP:80	Forward to target group • movie-service-containers: 1 (100%) • Target group stickiness: Off	1 rule	ARN	Not ap

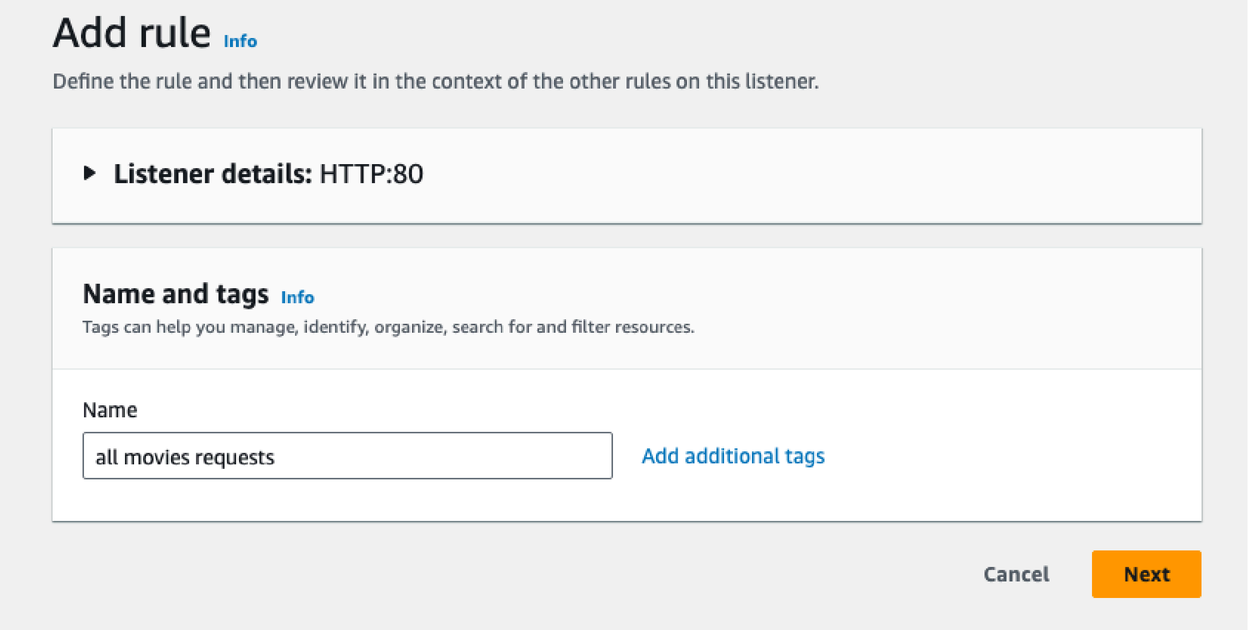
- Click on “**1 rule**” to update the rules for this listener.
- Click on “**Add rule**”. Let’s add 2 rules based on the Path.



Listener rules (1) 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 value.

□	Name tag	Priority ▲	Conditions (If)	Actions (Then)
□	*Default*	Last (default)	*If no other rule applies*	**Forward to target group** • 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.

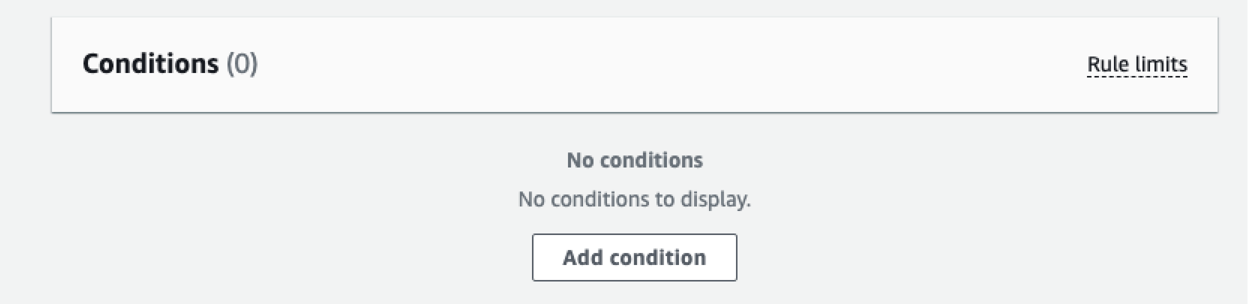
▸ **Listener details:** HTTP:80

Name and tags Info

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

Name: all movies requests

- Add condition

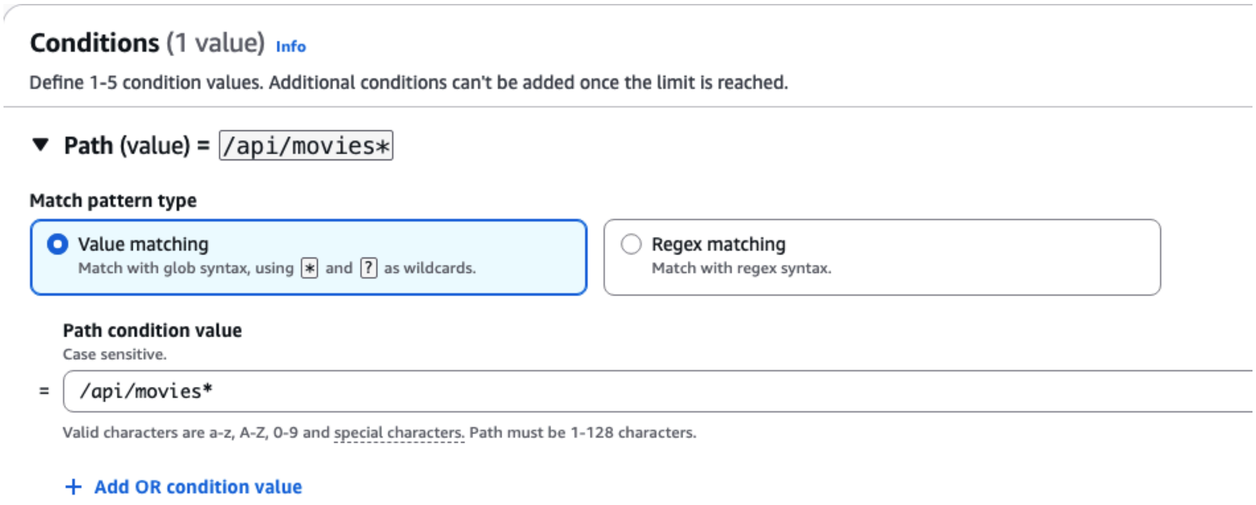


Conditions (0)

No conditions

No conditions to display.

- Under “Conditions”, we need the “Path” based routing.
  - Any request with the path /api/movies should go to movie-service.
    - path condition value: “**/api/movies***”
    - Forward to **movie-service-containers**



Conditions (1 value) Info

Define 1-5 condition values. Additional conditions can't be added once the limit is reached.

▼ **Path (value) =** `/api/movies*`

Match pattern type

● Value matching
Match with glob syntax, using `*` and `?` as wildcards.

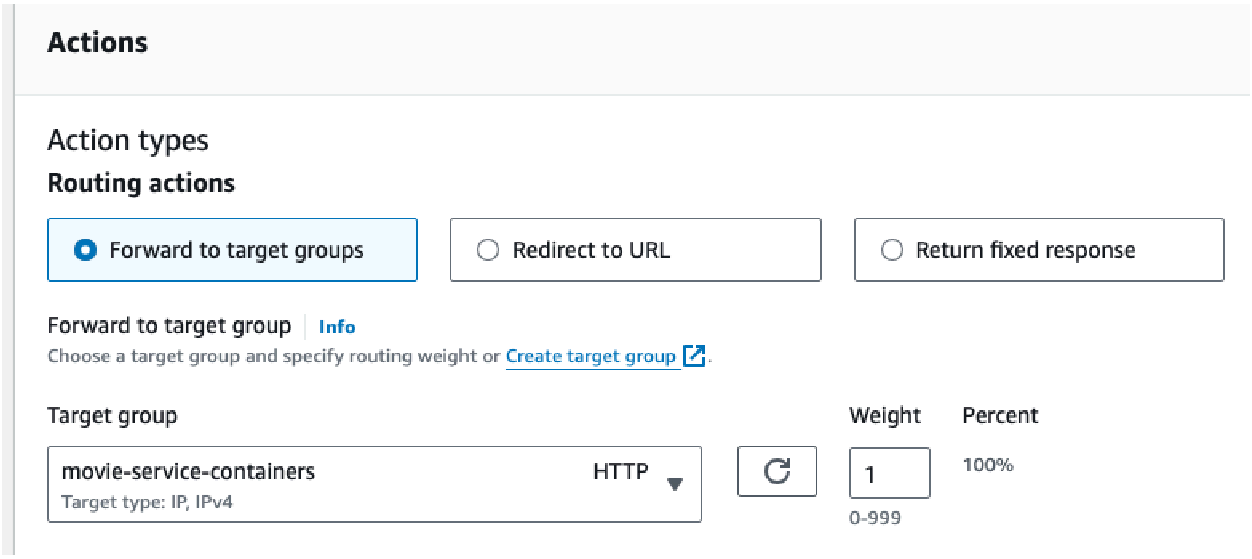
○ Regex matching
Match with regex syntax.

Path condition value
Case sensitive.

= `/api/movies*`

Valid characters are a-z, A-Z, 0-9 and special characters. Path must be 1-128 characters.

- Then go to “Actions”. Select the appropriate target. In this case, it is as shown below.



Actions

Action types

Routing actions

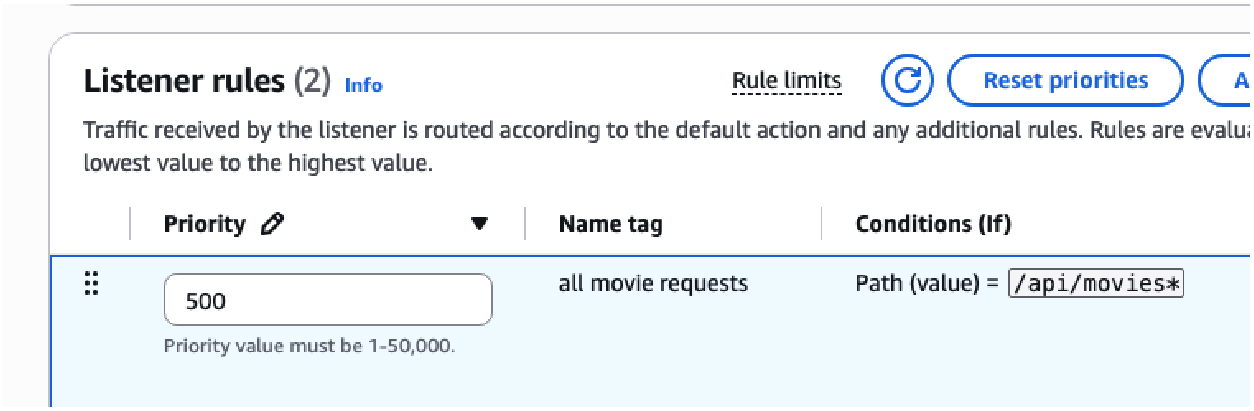
● Forward to target groups ○ Redirect to URL ○ Return fixed response

Forward to target group | Info

Choose a target group and specify routing weight or Create target group.

Target group	Weight	Percent
movie-service-containers HTTP Target type: IP, IPv4	1 0-999	100%

- Click Next to set the **priority**. I give ***500***.

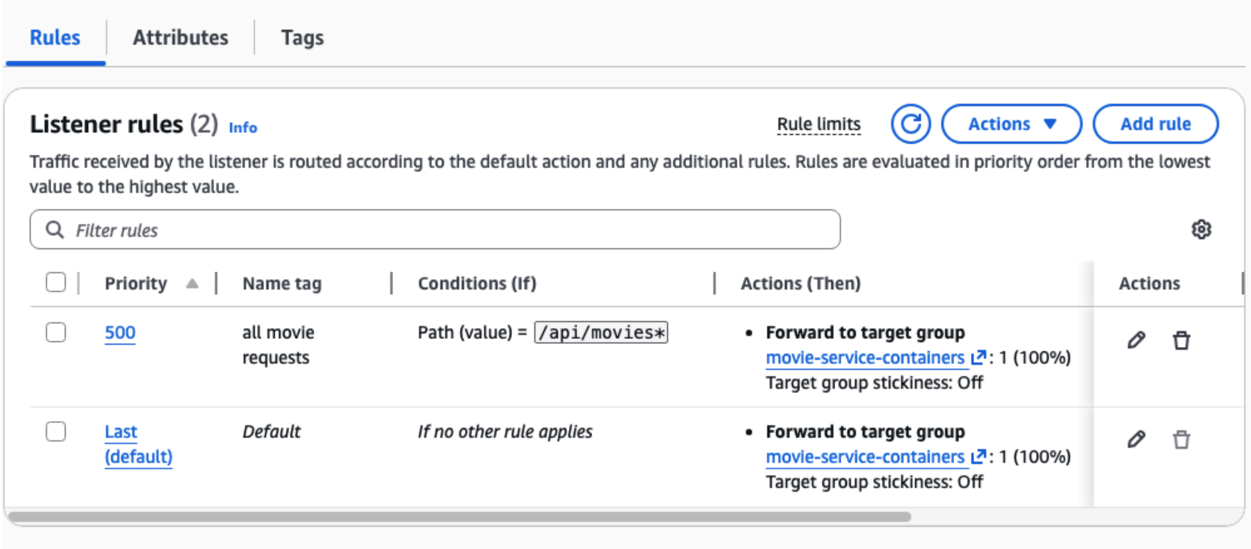


Listener rules (2) Info

Traffic received by the listener is routed according to the default action and any additional rules. Rules are evalu lowest value to the highest value.

Priority	Name tag	Conditions (If)
500 Priority value must be 1-50,000.	all movie requests	Path (value) = `/api/movies*`

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

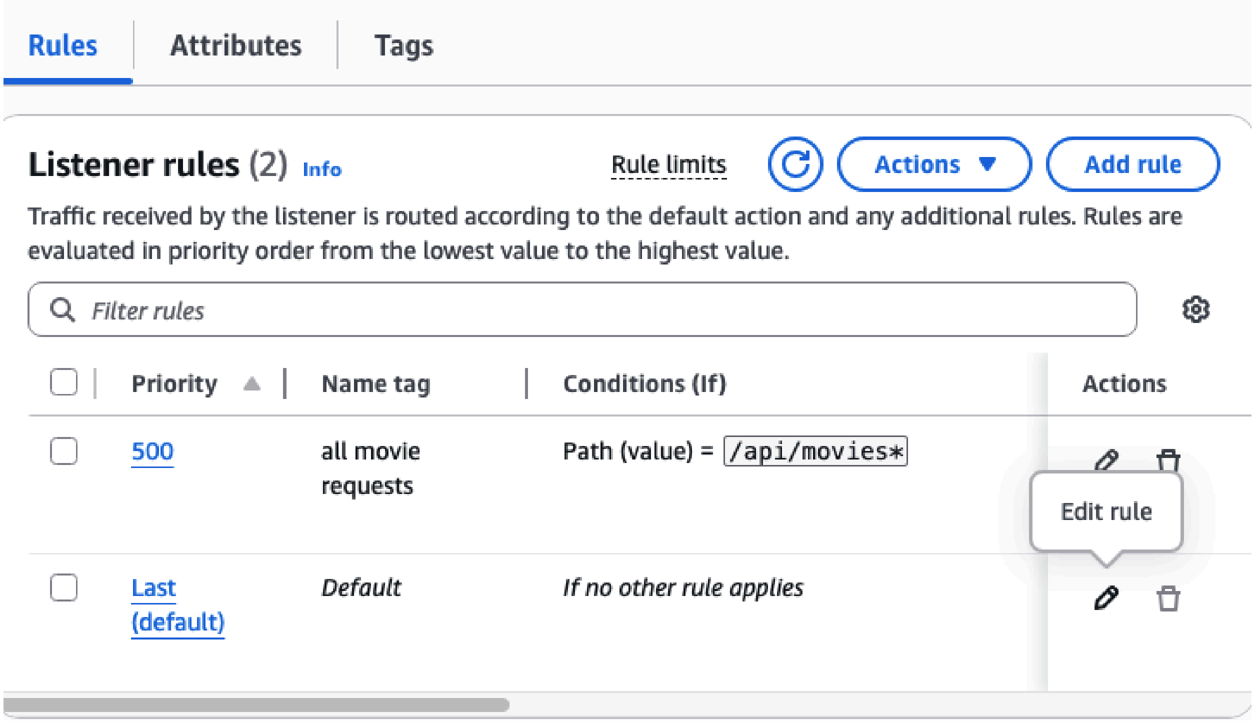


Listener rules (2) Info

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 value.

□	Priority ▲	Name tag	Conditions (If)	Actions (Then)	Actions
□	500	all movie requests	Path (value) = `/api/movies*`	• **Forward to target group** movie-service-containers: 1 (100%) Target group stickiness: Off	
□	Last (default)	*Default*	*If no other rule applies*	• **Forward to target group** movie-service-containers: 1 (100%) Target group stickiness: Off	

- We can edit the “Default” rule.

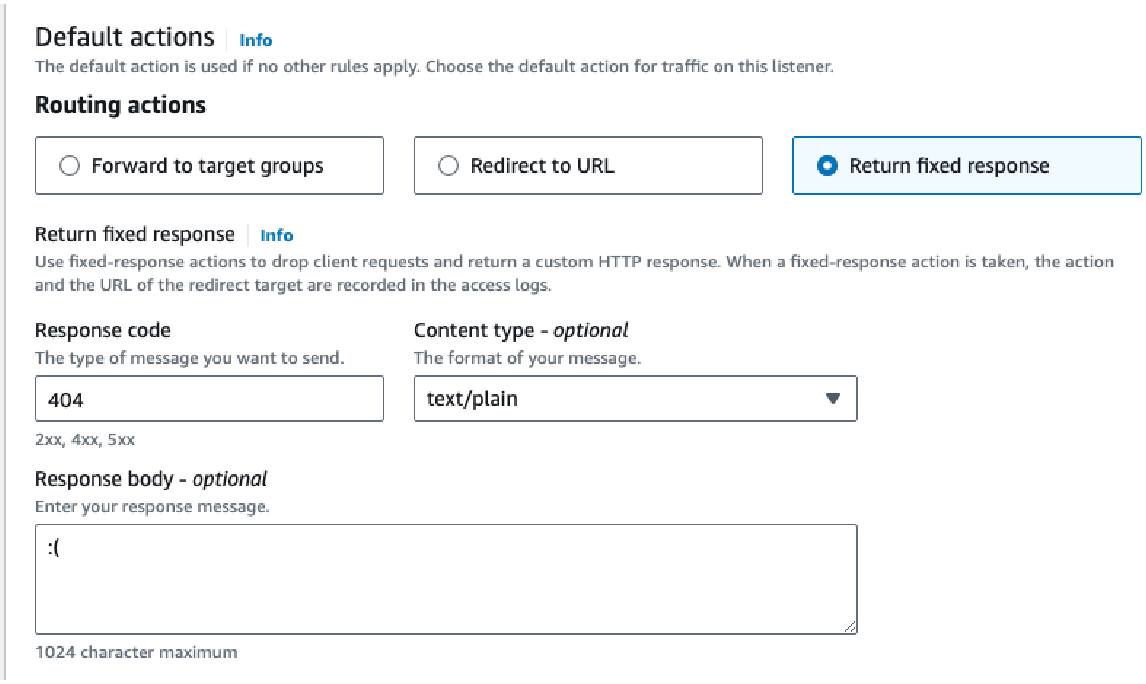


Listener rules (2) Info

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 value.

□	Priority ▲	Name tag	Conditions (If)	Actions
□	500	all movie requests	Path (value) = `/api/movies*`	
□	Last (default)	*Default*	*If no other rule applies*	

- 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

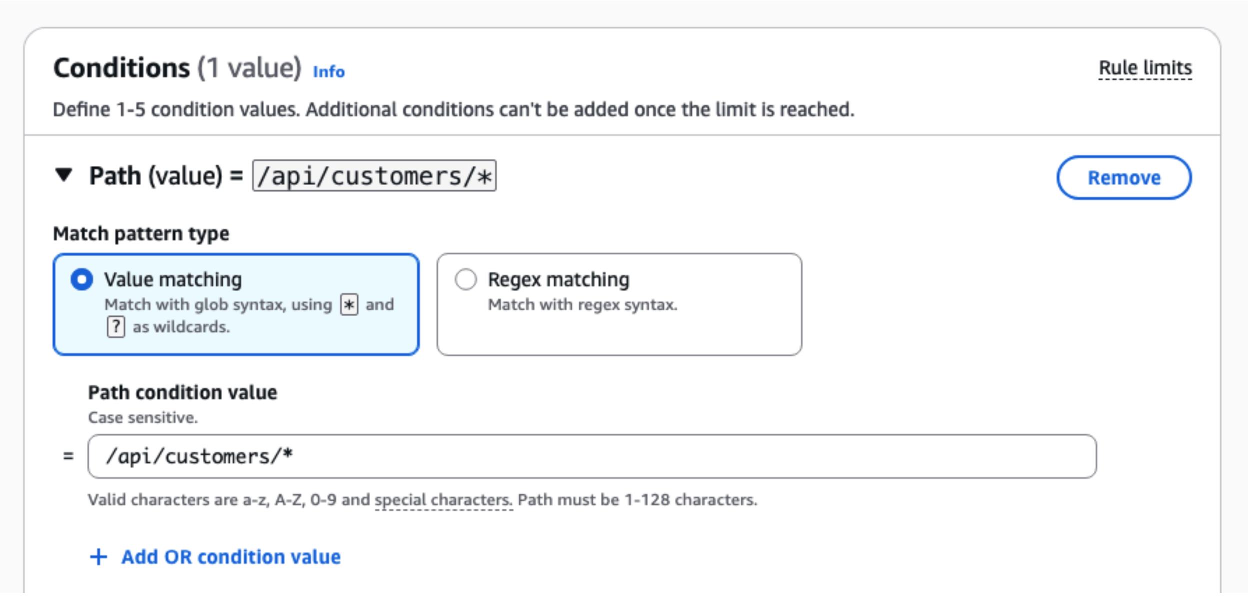
Use fixed-response actions to drop client requests and return a custom HTTP response. When a fixed-response action is taken, the action and the URL of the redirect target are recorded in the access logs.

Response code
The type of message you want to send.
404
2xx, 4xx, 5xx

Content type - *optional*
The format of your message.
text/plain ▼

Response body - *optional*
Enter your response message.
:(
1024 character maximum

- Repeat the same for customer-service requests. Ensure that condition is selected as shown below.



Conditions (1 value) Info Rule limits

Define 1-5 condition values. Additional conditions can't be added once the limit is reached.

▼ **Path** (value) = `/api/customers/*` Remove

Match pattern type

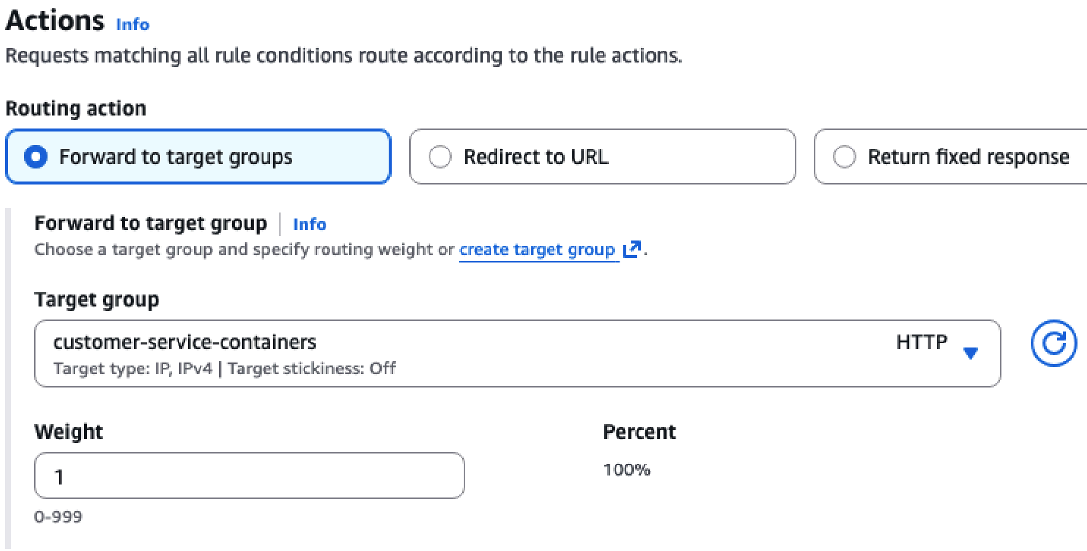
● Value matching
Match with glob syntax, using * and ? as wildcards.

○ Regex matching
Match with regex syntax.

Path condition value
Case sensitive.
= /api/customers/*
Valid characters are a-z, A-Z, 0-9 and special characters. Path must be 1-128 characters.

+ Add OR condition value

- Select **Actions** as shown below.



Actions Info

Requests matching all rule conditions route according to the rule actions.

Routing action

● 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

customer-service-containers HTTP

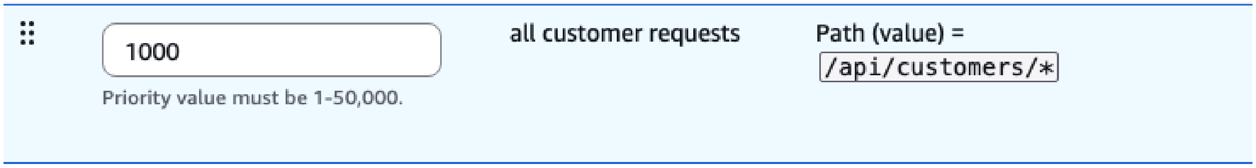
Target type: IP, IPv4 | Target stickiness: Off

Weight: 1

0-999

Percent: 100%

- I set the priority as 1000



1000

Priority value must be 1-50,000.

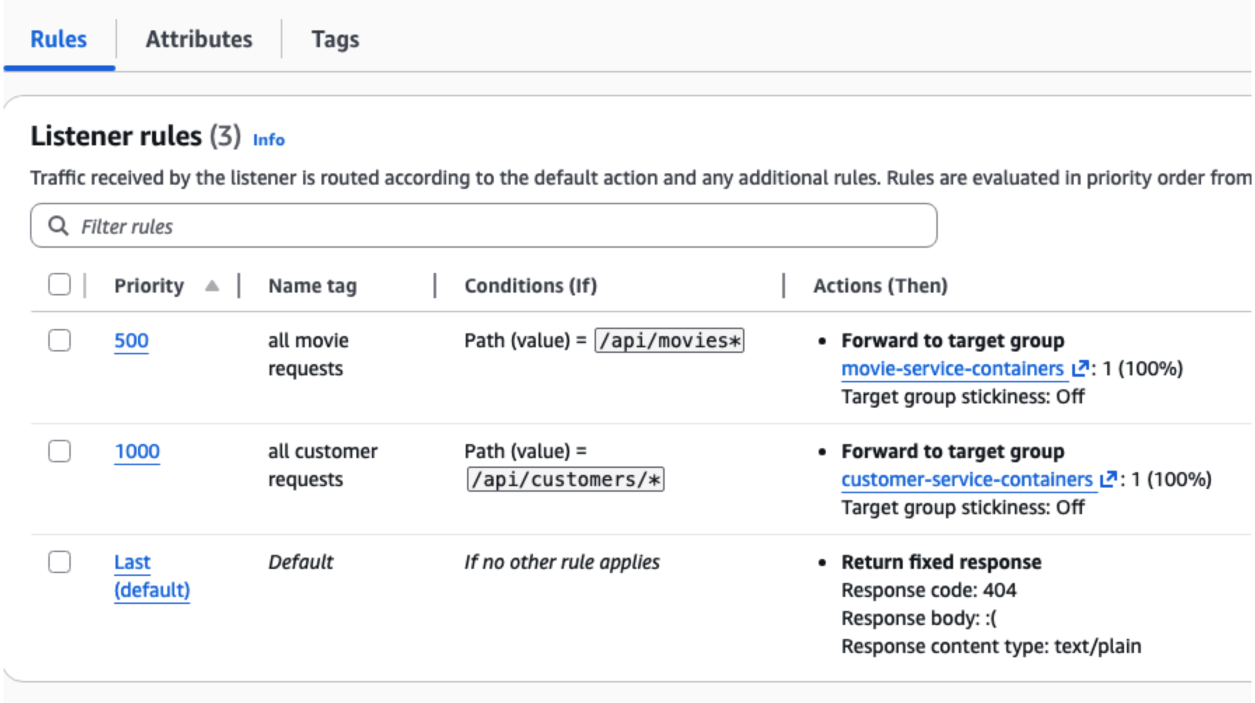
all customer requests

Path (value) = `/api/customers/*`

- Add the rule.

Verify

- Finally we should have 3 rules as shown below.



Listener rules (3) Info

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

Filter rules

□	Priority ▲	Name tag	Conditions (If)	Actions (Then)
□	500	all movie requests	Path (value) = `/api/movies*`	• **Forward to target group** movie-service-containers : 1 (100%) Target group stickiness: Off
□	1000	all customer requests	Path (value) = `/api/customers/*`	• **Forward to target group** customer-service-containers : 1 (100%) Target group stickiness: Off
□	Last (default)	*Default*	*If no other rule applies*	• **Return fixed response** Response code: 404 Response body: :(Response content type: text/plain