



网络负载均衡器

# Elastic Load Balancing



# Elastic Load Balancing: 网络负载均衡器

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

# Table of Contents

什么是网络负载均衡器？ .....	1
网络负载均衡器组件 .....	1
网络负载均衡器概述 .....	1
从经典负载均衡器迁移的好处 .....	2
如何开始 .....	3
定价 .....	3
开始使用 .....	4
开始前的准备工作 .....	4
步骤 1：配置目标组 .....	4
步骤 2：选择负载均衡器类型 .....	5
步骤 3：配置负载均衡器和侦听器 .....	5
步骤 4：测试负载均衡器 .....	6
步骤 5：( 可选 ) 删除您的负载均衡器 .....	7
开始使用 AWS CLI .....	8
开始前的准备工作 .....	8
创建您的 IPv4 负载均衡器 .....	8
创建您的双堆栈负载均衡器 .....	9
为负载均衡器指定弹性 IP 地址 .....	11
删除负载均衡器 .....	11
负载均衡器 .....	12
负载均衡器状态 .....	12
负载均衡器属性 .....	13
IP 地址类型 .....	14
负载均衡器资源地图 .....	15
资源地图组件 .....	15
可用区 .....	16
跨可用区负载均衡 .....	17
删除保护 .....	18
连接空闲超时 .....	18
DNS 名称 .....	19
可用区 DNS 亲和性 .....	20
监控 .....	21
开启可用区亲和性 .....	22
关闭可用区亲和性 .....	22

创建负载均衡器 .....	23
步骤 1：配置目标组 .....	23
步骤 2：注册目标 .....	24
步骤 3：配置负载均衡器和侦听器 .....	25
步骤 4：测试负载均衡器 .....	6
更新地址类型 .....	27
安全组 .....	28
注意事项 .....	29
示例：筛选客户端流量 .....	29
示例：仅接受来自负载均衡器的流量 .....	30
更新关联的安全组 .....	30
更新安全设置 .....	31
监控负载均衡器安全组 .....	31
更新标签 .....	31
删除负载均衡器 .....	32
可用区转移 .....	33
启动可用区转移 .....	34
更新可用区转移 .....	35
取消可用区转移 .....	36
侦听器 .....	37
侦听器配置 .....	37
侦听器规则 .....	38
创建侦听器 .....	38
先决条件 .....	38
添加侦听器 .....	38
配置 TLS 侦听器 .....	39
服务器证书 .....	39
安全策略 .....	42
ALPN 策略 .....	64
更新侦听器 .....	65
更新 TLS 侦听器 .....	66
替换默认证书 .....	66
将证书添加到证书列表 .....	67
从证书列表中删除证书 .....	67
更新安全策略 .....	68
更新 ALPN 策略 .....	68

删除侦听器 .....	69
目标组 .....	70
路由配置 .....	71
Target type .....	71
请求路由和 IP 地址 .....	73
将本地资源作为目标 .....	73
IP 地址类型 .....	74
已注册目标 .....	74
目标组属性 .....	75
客户端 IP 保留 .....	77
取消注册延迟 .....	79
代理协议 .....	80
运行状况检查连接 .....	80
VPC 终端节点服务 .....	81
启用代理协议 .....	81
粘性会话 .....	82
创建目标组 .....	82
配置运行状况检查 .....	84
运行状况检查设置 .....	85
目标运行状况 .....	86
运行状况检查原因代码 .....	88
检查目标的运行状况 .....	88
修改目标组的运行状况检查设置 .....	89
跨可用区负载均衡 .....	90
修改负载均衡器的跨区域负载均衡 .....	90
修改目标组的跨区域负载均衡 .....	91
目标组运行状况 .....	91
运行状况不佳状态的操作 .....	91
要求和注意事项 .....	92
示例 .....	92
修改目标组运行状况设置 .....	93
运行状况不佳的目标的连接终止 .....	94
为负载均衡器使用 Route 53 DNS 故障转移 .....	96
注册目标 .....	96
目标安全组 .....	97
网络 ACL .....	98

共享子网 .....	100
注册或取消注册目标 .....	100
作为目标的 Application Load Balancer .....	103
步骤 1：创建应用程序负载均衡器 .....	103
步骤 2：创建目标组 .....	105
步骤 3：创建 Network Load Balancer .....	106
步骤 4：( 可选 ) 启用 AWS PrivateLink .....	107
更新标签 .....	107
删除目标组 .....	108
监控负载均衡器 .....	109
CloudWatch 指标 .....	110
Network Load Balancer 指标 .....	110
网络负载均衡器的指标维度 .....	121
Network Load Balancer 指标的统计数据 .....	122
查看您的负载均衡器的 CloudWatch 指标 .....	122
访问日志 .....	124
访问日志文件 .....	125
访问日志条目 .....	126
存储桶要求 .....	128
启用访问日志记录 .....	131
禁用访问日志记录 .....	131
处理访问日志文件 .....	132
CloudTrail 日志 .....	132
在 Elastic Load Balancing CloudTrail .....	132
了解 Elastic Load Balancing 日志文件条目 .....	133
问题排查 .....	136
已注册目标未处于可用状态 .....	136
请求未路由至目标 .....	136
目标接收比预期更多的运行状况检查请求 .....	137
目标接收比预期更少的运行状况检查请求 .....	137
运行状况不佳的目标收到来自负载均衡器的请求 .....	137
由于主机标头不匹配，目标无法通过 HTTP 或 HTTPS 运行状况检查 .....	137
无法将安全组与网络负载均衡器关联 .....	137
无法删除所有安全组 .....	137
TCP_ELB_Reset_Count 指标升高 .....	138
从目标到其负载均衡器的请求连接超时 .....	138

---

当将目标移到 Network Load Balancer 时，性能会下降 .....	138
连接时出现端口分配错误 AWS PrivateLink .....	138
启用客户端 IP 保留时发生间歇性连接失败 .....	139
TCP 连接延迟 .....	139
预置负载均衡器时可能出现故障 .....	139
DNS 名称解析包含的 IP 地址少于已启用的可用区 .....	139
使用资源图对不健康的目标进行故障排除 .....	140
配额 .....	142
文档历史记录 .....	144
.....	cxlviii

# 什么是网络负载均衡器？

弹性负载均衡 在一个或多个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。它会监控已注册目标的运行状况，并仅将流量传输到运行状况良好的目标。弹性负载均衡 根据传入流量随时间的变化对负载均衡器进行扩展。它可以自动扩展来处理绝大部分工作负载。

弹性负载均衡 支持以下负载均衡器：Application Load Balancer、Network Load Balancer、Gateway Load Balancer 和经典负载均衡器。您可以选择最适合自己需求的负载均衡器类型。本指南讨论的是网络负载均衡器。有关其他负载均衡器的更多信息，请参阅 [Application Load Balancer 用户指南](#)、[Gateway Load Balancer 用户指南](#) 和 [经典负载均衡器用户指南](#)。

## 网络负载均衡器组件

负载均衡器充当客户端的单一接触点。负载均衡器在多个目标（如 Amazon EC2 实例）之间分配传入的流量。这将提高应用程序的可用性。可以向您的负载均衡器添加一个或多个侦听器。

侦听器使用您配置的协议和端口检查来自客户端的连接请求，然后将请求转发给目标组。

目标组使用指定的协议和端口号将请求路由到一个或多个已注册的目标（例如 EC2 实例）。网络负载均衡器目标组支持 TCP、UDP、TCP\_UDP 和 TLS 协议。您可以向多个目标组注册一个目标。您可以对每个目标组配置运行状况检查。在注册到目标组（它是使用负载均衡器的侦听器规则指定的）的所有目标上，执行运行状况检查。

有关更多信息，请参阅 文档：

- [负载均衡器](#)
- [侦听器](#)
- [目标组](#)

## 网络负载均衡器概述

网络负载均衡在开放系统互连 (OSI) 模型的第四层运行。它每秒可以处理数百万个请求。在负载均衡器收到连接请求后，它会从默认规则的目标组中选择一个目标。它尝试在侦听器配置中指定的端口上打开一个到该选定目标的 TCP 连接。

当您为负载均衡器启用可用区时，Elastic Load Balancing 会在该可用区中创建一个负载均衡器节点。默认情况下，每个负载均衡器节点仅在其可用区中的已注册目标之间分配流量。如果您启用了跨可用



区负载均衡，则每个负载均衡器节点会在所有启用的可用区中的已注册目标之间分配流量。有关更多信息，请参阅 [可用区](#)。

要提高应用程序的容错能力，您可以为负载均衡器启用多个可用区，并确保每个目标组在每个启用的可用区中至少有一个目标。例如，如果一个或多个目标组在可用区中没有运行状况良好的目标，我们会从 DNS 中删除相应子网的 IP 地址，但其他可用区中的负载均衡器节点仍可用于路由流量。如果客户端不遵守 time-to-live (TTL)，并在该 IP 地址从 DNS 中移除后向其发送请求，则请求将失败。

对于 TCP 流量，负载均衡器基于协议、源 IP 地址、源端口、目标 IP 地址、目标端口和 TCP 序列号，使用流哈希算法选择目标。来自客户端的 TCP 连接具有不同的源端口和序列号，可以路由到不同的目标。每个单独的 TCP 连接在连接的有效期内路由到单个目标。

对于 UDP 流量，负载均衡器基于协议、源 IP 地址、源端口、目标 IP 地址和目标端口，使用流哈希算法选择目标。UDP 流具有相同的源和目标，因此始终在其整个生命周期内路由到单个目标。不同 UDP 流具有不同的源 IP 地址和端口，因此它们可以路由到不同的目标。

Elastic Load Balancing 将为启用的每个可用区创建一个网络接口。可用区内的每个负载均衡器节点使用该网络接口来获取一个静态 IP 地址。在您创建面向 Internet 的负载均衡器时，可以选择将一个弹性 IP 地址与每个子网关联。

在创建目标组时，指定其目标类型，此类型将确定您如何注册其目标。例如，您可以注册实例 ID、IP 地址或 Application Load Balancer。目标类型还会影响是否会保留客户端 IP 地址。有关更多信息，请参阅 [the section called “客户端 IP 保留”](#)。

可以根据需求变化在负载均衡器中添加和删除目标，而不会中断应用程序的整体请求流。弹性负载均衡根据传输到应用程序的流量随时间的变化对负载均衡器进行扩展。弹性负载均衡能够自动扩展来处理绝大部分工作负载。

您可以配置运行状况检查，这些检查可用来监控注册目标的运行状况，以便负载均衡器只能将请求发送到正常运行的目标。

有关更多信息，请参阅 [弹性负载均衡 用户指南中的 Elastic Load Balancing 工作原理](#)

## 从经典负载均衡器迁移的好处

使用网络负载均衡器而不是经典负载均衡器具有以下好处：

- 可以处理急剧波动的工作负载，并可以扩展到每秒处理数百万个请求。
- 支持将静态 IP 地址用于负载均衡器。还可以针对为负载均衡器启用的每个子网分配一个弹性 IP 地址。

- 支持通过 IP 地址注册目标，包括位于负载均衡器的 VPC 之外的目标。
- 支持将请求路由到单个 EC2 实例上的多个应用程序。可以使用多个端口向同一个目标组注册每个实例或 IP 地址。
- 支持容器化的应用程序。计划任务时，Amazon Elastic Container Service (Amazon ECS) 可以选择一个未使用的端口，并可以使用此端口向目标组注册该任务。这样可以高效地使用您的群集。
- Support 支持独立监控每项服务的运行状况，因为运行状况检查是在目标群体级别定义的，而许多 Amazon CloudWatch 指标是在目标群体级别报告的。将目标组挂载到 Auto Scaling 组的功能使您能够根据需求动态扩展每个服务。

要详细了解每种负载均衡器类型支持的功能，请参阅 [弹性负载均衡 产品比较](#)。

## 如何开始

要创建网络负载均衡器，请尝试以下某个教程中介绍的方法：

- [Network Load Balancers 入门](#)
- [教程：使用 AWS CLI 创建 Network Load Balancer](#)

有关常见负载均衡器配置的演示，请参阅 [Elastic Load Balancing 演示](#)。

## 定价

有关更多信息，请参阅[网络负载均衡器定价](#)。

# Network Load Balancers 入门

本教程通过基于 Web 的界面提供了网络负载均衡器的实际操作介绍。AWS Management Console 要创建第一个 Network Load Balancer，请完成以下步骤。

## 任务

- [开始前的准备工作](#)
- [步骤 1：配置目标组](#)
- [步骤 2：选择负载均衡器类型](#)
- [步骤 3：配置负载均衡器和侦听器](#)
- [步骤 4：测试负载均衡器](#)
- [步骤 5：\(可选\) 删除您的负载均衡器](#)

有关常见负载均衡器配置的演示，请参阅 [Elastic Load Balancing 演示](#)。

## 开始前的准备工作

- 确定将用于 EC2 实例的可用区。在每个这些可用区中配置至少带有一个公有子网的 Virtual Private Cloud (VPC)。这些公有子网用于配置负载均衡器。您可以改为在这些可用区的其他子网中启动您的 EC2 实例。
- 在每个可用区中至少启动一个 EC2 实例。确保这些实例的安全组允许侦听器端口上来自客户端的 TCP 访问和来自您的 VPC 的运行状况检查请求。有关更多信息，请参阅 [目标安全组](#)。

## 步骤 1：配置目标组

创建一个要在请求路由中使用的目标组。侦听器的规则将请求路由到此目标组中的注册目标。负载均衡器使用为目标组定义的运行状况检查设置来检查此目标组中目标的运行状况。

### 使用控制台配置目标群组

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择 Create target group (创建目标组)。
4. 将目标类型保留为 instances (实例)。

5. 对于 Target group name ( 目标组名称 ) , 输入新目标组的名称。
6. 对于 Protocol ( 协议 ) , 选择 TCP , 对于 Port ( 端口 ) , 选择 80。
7. 对于 VPC , 选择包含您的实例的 VPC。
8. 对于 Health checks ( 运行状况检查 ) , 保留默认设置。
9. 选择下一步。
10. 在 Register targets ( 注册目标 ) 页面上 , 完成以下步骤。这是用于创建目标组的可选步骤。但是 , 如果要测试负载均衡器并确保负载均衡器将流量路由到目标 , 您必须注册目标。
  - a. 对于 Available instances ( 可用实例 ) , 选择一个或多个实例。
  - b. 保持默认端口 80 , 然后选择 Include as pending below ( 包括为以下待处理 ) 。
11. 选择创建目标组。

## 步骤 2 : 选择负载均衡器类型

Elastic Load Balancing 支持三类负载均衡器。在此教程中 , 您将创建一个 Network Load Balancer。

使用控制台创建 Network Load Balancer

1. 通过以下网址打开 Amazon EC2 控制台 : <https://console.aws.amazon.com/ec2/>。
2. 在导航栏上 , 选择您的负载均衡器所在的区域。请确保选择用于 EC2 实例的同一区域。
3. 在导航窗格中的负载平衡下 , 选择负载均衡器。
4. 选择创建负载均衡器。
5. 对于 Network Load Balancer , 请选择 Create ( 创建 ) 。

## 步骤 3 : 配置负载均衡器和侦听器

要创建 Network Load Balancer , 您必须首先提供负载均衡器的基本配置信息 , 例如名称、方案和 IP 地址类型。然后提供有关您的网络以及一个或多个侦听器的信息。侦听器是用于检查连接请求的进程。它配置了用于从客户端连接到负载均衡器的协议和端口。有关受支持的协议和端口的更多信息 , 请参阅[侦听器配置](#)。

配置负载均衡器和侦听器

1. 对于 Load balancer name ( 负载均衡器名称 ) , 输入负载均衡器的名称。例如 : my-nlb。
2. 对于 Scheme 和 IP address type , 请保留默认值。

- 对于 Network mapping ( 网络映射 ) ，选择用于 EC2 实例的 VPC。对于用于启动 EC2 实例的每个可用区，选择一个可用区，然后为该可用区选择公有子网。

默认情况下，为其可用区的子网中的每个负载均衡器节点 AWS 分配一个 IPv4 地址。另外，当您创建面向 Internet 的负载均衡器时，您可以为每个可用区选择弹性 IP 地址。这将为您的负载均衡器提供静态 IP 地址。

- 对于安全组，我们会为您的 VPC 预先选择默认安全组。您可以根据需要选择其他安全组。如果您没有合适的安全组，请选择创建新的安全组并创建一个满足您的安全需求的安全组。有关更多信息，请参阅《Amazon VPC 用户指南》中的[创建安全组](#)。

#### Warning

如果您现在没有将任何安全组与负载均衡器关联，则无法以后再将其关联。

- 对于侦听器 and 路由，请保留默认协议和端口，然后从列表中选择目标组。默认情况下，这将配置用于接收端口 80 上的 TCP 流量并将流量转发到所选目标组的侦听器。
- ( 可选 ) 添加标签以对负载均衡器进行分类。每个负载均衡器的标签键必须唯一。允许的字符包括字母、空格、数字 ( UTF-8 格式 ) 和以下特殊字符 : + - = . \_ : / @ 。请不要使用前导空格或尾随空格。标签值区分大小写。
- 查看配置，然后选择 Create load balancer ( 创建负载均衡器 ) 。在创建过程中，一些默认属性会应用于负载均衡器。创建负载均衡器后，您可以查看和编辑它们。有关更多信息，请参阅[负载均衡器属性](#)。

## 步骤 4：测试负载均衡器

在创建负载均衡器之后，可以验证其是否将流量发送到您的 EC2 实例。

### 测试负载均衡器

- 在您收到已成功创建负载均衡器的通知后，选择 Close。
- 在导航窗格中的 Load Balancing ( 负载均衡 ) 下，选择 Target Groups ( 目标组 ) 。
- 选择新创建的目标组。
- 选择 Targets 并验证您的实例是否已就绪。如果实例状态是 initial，很可能是因为，实例仍在注册过程中，或者未通过视为正常运行所需的运行状况检查最小数量。在您的至少一个实例的状态为 healthy 后，便可测试负载均衡器。
- 在导航窗格中的 Load Balancing ( 负载均衡 ) 下，选择 Load Balancers ( 负载均衡器 ) 。

6. 选择新创建的负载均衡器的名称以打开其详细信息页面。
7. 复制负载均衡器的 DNS 名称（例如，my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com）。将该 DNS 名称粘贴到已连接 Internet 的 Web 浏览器的地址栏中。如果一切正常，浏览器会显示您服务器的默认页面。

## 步骤 5：（可选）删除您的负载均衡器

在您的负载均衡器可用之后，您需要为保持其运行的每小时或部分小时支付费用。当您不再需要负载均衡器时，可将其删除。当负载均衡器被删除之后，您便不再需要支付负载均衡器费用。请注意，删除负载均衡器不会影响在负载均衡器中注册的目标。例如，您的 EC2 实例会继续运行。

### 使用控制台删除您的负载均衡器

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的负载平衡下，选择负载均衡器。
3. 选中负载均衡器的复选框，然后依次选择 Actions（操作）、Delete（删除）。
4. 如果提示进行确认，输入 **confirm**，并选择 Delete（删除）。

# 教程：使用 AWS CLI 创建 Network Load Balancer

本教程介绍通过 AWS CLI 使用 Network Load Balancer 的实践操作。

## 开始前的准备工作

- 安装，AWS CLI 或者如果您使用的是不支持 Network Load Balancer 的版本，则更新到最新版本的。AWS CLI 有关更多信息，请参阅 AWS Command Line Interface 用户指南中的[安装 AWS Command Line Interface](#)。
- 确定将用于 EC2 实例的可用区。在每个这些可用区中配置至少带有一个公有子网的 Virtual Private Cloud (VPC)。
- 决定是要创建 IPv4 还是双堆栈负载均衡器。如果您想要客户端仅使用 IPv4 地址与负载均衡器通信，则使用 IPv4。如果您想要客户端使用 IPv4 和 IPv6 地址与负载均衡器通信，则使用双堆栈。此外，您还可以使用双堆栈通过 IPv6 与后端目标（例如 IPv6 应用程序或双堆栈子网）进行通信。
- 在每个可用区中至少启动一个 EC2 实例。确保这些实例的安全组允许侦听器端口上来自客户端的 TCP 访问和来自您的 VPC 的运行状况检查请求。有关更多信息，请参阅[目标安全组](#)。

## 创建您的 IPv4 负载均衡器

要创建第一个负载均衡器，请完成以下步骤。

### 创建 IPv4 负载均衡器

1. 使用 `create-load-balancer` 命令创建 IPv4 负载均衡器，为启动实例的每个可用区指定一个公有子网。每个可用区您只能指定一个子网。

默认情况下，当使用 AWS CLI 创建网络负载均衡器时，这些均衡器不会自动使用 VPC 的默认安全组。如果在创建时没有将任何安全组与负载均衡器关联，则无法以后再将其关联。我们建议您在创建时使用 `--security-groups` 选项为负载均衡器指定安全组。

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
subnet-0e3f5cac72EXAMPLE --security-groups sg-0123456789EXAMPLE
```

输出包含负载均衡器的 Amazon Resource Name (ARN)，格式如下：

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:loadbalancer/net/my-load-balancer/1234567890123456
```

2. 使用 [create-target-group](#) 命令创建 IPv4 目标组，指定您用于 EC2 实例的 VPC。IPv4 目标组支持 IP 和实例类型目标。

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id vpc-0598c7d356EXAMPLE
```

输出包含目标组的 ARN，格式如下：

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/1234567890123456
```

3. 使用 [register-targets](#) 命令将您的实例注册到目标组：

```
aws elbv2 register-targets --target-group-arn targetgroup-arn --targets Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

4. 使用 [create-listener](#) 命令为您的负载均衡器创建侦听器，该侦听器带有将请求转发到目标组的默认规则：

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --protocol TCP --port 80 \ --default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

输出包含侦听器的 ARN，格式如下：

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/net/my-load-balancer/1234567890123456/1234567890123456
```

5. ( 可选 ) 您可以使用以下 [describe-target-health](#) 命令验证目标组的注册目标的运行状况：

```
aws elbv2 describe-target-health --target-group-arn targetgroup-arn
```

## 创建您的双堆栈负载均衡器

要创建第一个负载均衡器，请完成以下步骤。



## 创建双堆栈负载均衡器

1. 使用 [create-load-balancer](#) 命令创建双栈负载均衡器，为启动实例的每个可用区指定一个公有子网。每个可用区您只能指定一个子网。

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets subnet-0e3f5cac72EXAMPLE --ip-address-type dualstack
```

输出包含负载均衡器的 Amazon Resource Name (ARN)，格式如下：

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:loadbalancer/net/my-load-balancer/1234567890123456
```

2. 使用 [create-target-group](#) 命令创建目标组，指定您用于 EC2 实例的 VPC。

您的双堆栈负载均衡器必须与一个 TCP 或 TLS 目标组结合使用。

您可以创建 IPv4 和 IPv6 目标组，以便关联双堆栈负载均衡器。目标组的 IP 地址类型决定了负载均衡器用于与后端目标进行通信以及检查后端目标运行状况的 IP 版本。

IPv4 目标组支持 IP 和实例类型目标。IPv6 目标组仅支持 IP 目标。

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id vpc-0598c7d356EXAMPLE --ip-address-type [ipv4 or ipv6]
```

输出包含目标组的 ARN，格式如下：

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/1234567890123456
```

3. 使用 [register-targets](#) 命令将您的实例注册到目标组：

```
aws elbv2 register-targets --target-group-arn targetgroup-arn --targets Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

4. 使用 [create-listener](#) 命令为您的负载均衡器创建一个侦听器，该侦听器带有将请求转发到目标组的默认规则。双堆栈负载均衡器必须具有 TCP 或 TLS 侦听器。

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --protocol TCP --port 80 \
```

```
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

输出包含侦听器的 ARN，格式如下：

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/net/my-load-balancer/1234567890123456/1234567890123456
```

5. (可选) 您可以使用以下[describe-target-health](#)命令验证目标组的注册目标的运行状况：

```
aws elbv2 describe-target-health --target-group-arn targetgroup-arn
```

## 为负载均衡器指定弹性 IP 地址

在创建 Network Load Balancer 时，可以使用子网映射为每个子网指定一个弹性 IP 地址。

```
aws elbv2 create-load-balancer --name my-load-balancer --type network \  
--subnet-mappings SubnetId=subnet-0e3f5cac72EXAMPLE,AllocationId=eipalloc-12345678
```

## 删除负载均衡器

当您不再需要负载均衡器和目标组时，可以将其删除，如下所示：

```
aws elbv2 delete-load-balancer --load-balancer-arn loadbalancer-arn  
aws elbv2 delete-target-group --target-group-arn targetgroup-arn
```

# Network Load Balancer

负载均衡器充当客户端的单一接触点。客户端将请求发送到负载均衡器，然后负载均衡器将请求发送到一个或多个可用区中的目标 (例如 EC2 实例)。

要配置您的负载均衡器，可以创建[目标组](#)，然后将目标注册到目标组。如果您确保每个启用的可用区均具有至少一个注册目标，则负载均衡器将具有最高效率。您还可以创建[侦听器](#)来检查来自客户端的连接请求，并将来自客户端的请求路由到目标组中的目标。

网络负载均衡器支持客户端通过 VPC 对等互连、AWS 托管 VPN 和第三方 VPN 解决方案进行连接。  
AWS Direct Connect

## 内容

- [负载均衡器状态](#)
- [负载均衡器属性](#)
- [IP 地址类型](#)
- [Network Load Balancer 资源地图](#)
- [可用区](#)
- [跨可用区负载均衡](#)
- [删除保护](#)
- [连接空闲超时](#)
- [DNS 名称](#)
- [可用区 DNS 亲和性](#)
- [创建 Network Load Balancer](#)
- [Network Load Balancer 的 IP 地址类型](#)
- [网络负载均衡器的安全组](#)
- [您的 Network Load Balancer 的标签](#)
- [删除 Network Load Balancer](#)
- [可用区转移](#)

## 负载均衡器状态

负载均衡器具有下列状态之一：

## provisioning

正在设置负载均衡器。

## active

负载均衡器已完全设置并准备好路由流量。

## failed

无法设置负载均衡器。

## 负载均衡器属性

负载均衡器具有以下属性：

### access\_logs.s3.enabled

指示是否启用存储在 Amazon S3 中的访问日志。默认为 `false`。

### access\_logs.s3.bucket

访问日志所用的 Amazon S3 存储桶的名称。如果启用访问日志，则此属性是必需的。有关更多信息，请参阅 [存储桶要求](#)。

### access\_logs.s3.prefix

Amazon S3 存储桶中位置的前缀。

### deletion\_protection.enabled

指示是否启用[删除保护](#)。默认为 `false`。

### ipv6.deny\_all\_igw\_traffic

阻止互联网网关 (IGW) 访问负载均衡器，以防通过互联网网关意外访问内部负载均衡器。对于面向互联网的负载均衡器，它设置为 `false`；对于内部负载均衡器，它设置为 `true`。此属性不会阻止非 IGW 互联网访问（例如，通过对等互连、Transit Gateway 或 AWS Direct Connect）。AWS VPN

### load\_balancing.cross\_zone.enabled

指示是否启用了[跨可用区负载均衡](#)。默认为 `false`。

## dns\_record.client\_routing\_policy

指示将如何在负载均衡器可用区之间进行分配流量。可能的值为 `availability_zone_affinity` ( 100% 可用区亲和性 )、`partial_availability_zone_affinity` ( 85% 可用区亲和性 ) 和 `any_availability_zone` ( 0% 可用区亲和性 )。

## IP 地址类型

您可以设置客户端可与您的负载均衡器结合使用的 IP 地址类型。

网络负载均衡器支持以下 IP 地址类型：

### ipv4

客户端必须使用 IPv4 地址连接到负载均衡器 ( 例如 192.0.2.1 )。启用 IPv4 的负载均衡器 ( 面向互联网和内部 ) 支持 TCP、UDP、TCP\_UDP 和 TLS 侦听器。

### dualstack

客户端可以同时使用 IPv4 地址 ( 例如 192.0.2.1 ) 和 IPv6 地址 ( 例如, 2001:0db8:85a3:0:0:8a2e:0370:7334 ) 连接到负载均衡器。启用双堆栈的负载均衡器 ( 面向互联网和内部 ) 支持 TCP 和 TLS 侦听器。

### 注意事项

- 负载均衡器根据目标组的 IP 地址类型与目标进行通信。
- 当您为负载均衡器启用双堆栈模式时，Elastic Load Balancing 为负载均衡器提供 AAAA DNS 记录。使用 IPv4 地址与负载均衡器通信的客户端解析 A DNS 记录。使用 IPv6 地址与负载均衡器通信的客户端解析 AAAA DNS 记录。
- 阻止通过互联网网关对内部双堆栈负载均衡器的访问，以防意外访问互联网。但是，这并不能阻止其他互联网访问 ( 例如，通过对等互连、Transit Gateway 或 AWS VPN )。AWS Direct Connect

有关 IP 地址类型的更多信息，请参阅[Network Load Balancer 的 IP 地址类型](#)。

## Network Load Balancer 资源地图

Network Load Balancer 资源地图以交互方式显示您的负载均衡器的架构，包括其关联的侦听器、目标组和目标。资源图还突出显示了所有资源之间的关系和路由路径，从而直观地呈现了您的负载均衡器的配置。

使用控制台查看网络负载均衡器的资源地图

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器。
4. 选择资源映射选项卡以显示负载均衡器的资源映射。

### 资源地图组件

#### 地图视图

Network Load Balancer 资源图中有两个视图可用：概述和不健康目标地图。默认情况下，“概述”处于选中状态，并显示您的负载均衡器的所有资源。选择“不健康的目标地图”视图将仅显示不健康的目标以及与之相关的资源。

不健康的目标地图视图可用于对运行状况检查失败的目标进行故障排除。有关更多信息，请参阅 [使用资源图对不健康的目标进行故障排除](#)。

#### 资源列

Network Load Balancer 资源图包含三个资源列，每种资源类型各占一列。资源组包括侦听器、目标组和目标。

#### 资源方块

列中的每个资源都有自己的图块，显示有关该特定资源的详细信息。

- 将鼠标悬停在资源图块上会突出显示该资源与其他资源之间的关系。
- 选择资源图块会突出显示该资源与其他资源之间的关系，并显示有关该资源的其他详细信息。
  - 目标组健康状况摘要：每种健康状态的注册目标数量。
  - 目标生命值：目标的当前生命状态和描述。

**Note**

您可以关闭显示资源详细信息以隐藏资源图中的其他详细信息。

- 每个资源图块都包含一个链接，选择该链接后，该链接将导航到该资源的详细信息页面。
- 监听器-选择监听器协议:端口。例如，TCP:80
- 目标群体-选择目标群体名称。例如，my-target-group
- 目标-选择目标 ID。例如，i-1234567890abcdef0

## 导出资源地图

选择“导出”后，您可以选择将网络负载均衡器资源地图的当前视图导出为 PDF。

## 可用区

在创建负载均衡器时，可为其启用一个或多个可用区。如果为负载均衡器启用多个可用区，则可以提高应用程序的容错能力。您无法在创建可用区后对网络负载均衡器禁用这些可用区，但可以启用其他可用区。

当启用某个可用区时，应指定该可用区中的一个子网。Elastic Load Balancing 会在该可用区中创建一个负载均衡器节点，并为子网创建一个网络接口（描述以“ELB net”开头并包括负载均衡器的名称）。可用区内的每个负载均衡器节点使用该网络接口来获取一个 IPv4 地址。请注意，您可以查看此网络接口，但是不能修改它。

在您创建面向 Internet 的负载均衡器时，可以选择为每个子网指定一个弹性 IP 地址。如果您不选择自己的弹性 IP 地址之一，Elastic Load Balancing 将为每个子网提供一个弹性 IP 地址。这些弹性 IP 地址为您的负载均衡器提供静态 IP 地址，这些地址在负载均衡器的生命周期内不会更改。创建负载均衡器后，您无法更改这些弹性 IP 地址。

在您创建内部负载均衡器时，可以选择为每个子网指定一个私有 IP 地址。如果您没有从子网指定 IP 地址，Elastic Load Balancing 将为您选择一个 IP 地址。这些私有 IP 地址为您的负载均衡器提供静态 IP 地址，这些地址在负载均衡器的生命周期内不会更改。创建负载均衡器后，您无法更改这些私有 IP 地址。

## 注意事项

- 对于面向 Internet 的负载均衡器，您指定的子网必须至少具有 8 个可用 IP 地址。对于内部负载均衡器，只有在允许从子网 AWS 中选择私有 IPv4 地址时，才需要这样做。

- 无法指定受约束可用区中的子网。错误消息为“Load balancers with type 'network' are not supported in az\_name (az\_name 中不支持“网络”类型的负载均衡器)”。您可以在不受约束的其他可用区中指定子网，并使用跨可用区负载均衡将流量分发至受约束可用区中的目标。
- 您可以指定已经与您共享的子网。
- 您无法在本地区域中指定子网。

在启用一个可用区后，负载均衡器会开始将请求路由到该可用区中的已注册目标。如果您确保每个启用的可用区均具有至少一个注册目标，则负载均衡器将具有最高效率。

### 使用控制台添加可用区

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在 Network mapping (网络映射) 选项卡上，选择 Edit subnets (编辑子网)。
5. 要启用一个可用区，请选中该可用区的复选框。如果该可用区有一个子网，则将选择此子网。如果该可用区有多个子网，请选择其中一个子网。请注意，您只能为每个可用区选择一个子网。

对于面向 Internet 的负载均衡器，您可以为每个可用区选择弹性 IP 地址。对于内部负载均衡器，您可以从每个子网的 IPv4 范围分配私有 IP 地址，而不是让 Elastic Load Balancing 分配一个 IP 地址。

6. 选择保存更改。

要添加可用区，请使用 AWS CLI

使用 [set-subnets](#) 命令。

## 跨可用区负载均衡

默认情况下，每个负载均衡器节点仅在其可用区中的已注册目标之间分配流量。如果您开启了跨区域负载均衡，则每个负载均衡器节点会在所有启用的可用区中的注册目标之间分配流量。您也可以开启目标组级别的跨区域负载均衡。有关更多信息，请参阅 Elastic Load Balancing 用户指南中的 [the section called “跨可用区负载均衡”](#) 和 [跨区域负载均衡](#)。



## 删除保护

为了防止您的负载均衡器被意外删除，您可以启用删除保护。默认情况下，已为负载均衡器禁用删除保护。

如果您为负载均衡器启用删除保护，则必须先禁用删除保护，然后才能删除负载均衡器。

### 使用控制台启用删除保护

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在配置下，打开删除保护。
6. 选择保存更改。

### 使用控制台禁用删除保护

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在配置下，打开删除保护。
6. 选择保存更改。

要启用或禁用删除保护，请使用 AWS CLI

使用带 `deletion_protection.enabled` 属性的 [modify-load-balancer-attributes](#) 命令。

## 连接空闲超时

对于客户端通过 Network Load Balancer 发出的每个 TCP 请求，都将跟踪该连接的状态。如果客户端或目标通过连接发送数据的间隔超过空闲超时期限，则连接将关闭。如果客户端或目标在空闲超时期限后发送数据，则会收到一个 TCP RST 数据包，以指示连接不再有效。

我们将 TCP 流的空闲超时值设置为 350 秒。您无法修改此值。客户端或目标可以使用 TCP keepalive 数据包重置空闲超时值。为维护 TLS 连接而发送的 Keepalive 数据包不能包含数据或负载。

当 TLS 侦听器收到来自客户端或目标的 TCP keepalive 数据包时，负载均衡器会生成 TCP keepalive 数据包，并每 20 秒将它们发送到前端和后端连接。您不能修改此行为。

虽然 UDP 无连接，但是负载均衡器将根据源和目标 IP 地址和端口保持 UDP 流状态。这可确保属于同一个流中的数据包始终发送到相同的目标。空闲超时期限后，负载均衡器会考虑将传入的 UDP 数据包作为新流，并路由到新的目标。Elastic Load Balancing 将 UDP 流的空闲超时值设置为 120 秒。

EC2 实例必须在 30 秒内响应新请求，才能建立退回路径。

## DNS 名称

每个 Network Load Balancer 都会收到具有以下语法的默认域名系统 (DNS) 名称：*name-id.elb.region.amazonaws.com*。例如，*my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com*。

如果您更喜欢使用更容易记住的 DNS 名称，则可以创建自定义域名并将其与负载均衡器的 DNS 名称相关联。在客户端使用此自定义域名进行请求时，DNS 服务器将它解析为负载均衡器的 DNS 名称。

首先，向经认可的域名注册商注册域名。下一步，通过您的 DNS 服务（如您的域注册商）创建一条 DNS 记录将请求路由到您的负载均衡器。有关更多信息，请参阅您的 DNS 服务的文档。例如，如果您将 Amazon Route 53 用作 DNS 服务，请创建一条指向负载均衡器的别名记录。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的[将流量路由到 ELB 负载均衡器](#)。

负载均衡器针对每个启用的可用区都有一个 IP 地址。这些是负载均衡器节点的 IP 地址。负载均衡器的 DNS 名称解析为这些地址。例如，假设您的负载均衡器的自定义域名是 *example.networkloadbalancer.com*。使用以下 `dig` 或 `nslookup` 命令确定负载均衡器节点的 IP 地址。

Linux 或 Mac

```
$ dig +short example.networkloadbalancer.com
```

Windows

```
C:\> nslookup example.networkloadbalancer.com
```

负载均衡器具有其负载均衡器节点的 DNS 记录。您可以使用具有以下语法的 DNS 名称来确定负载均衡器节点的 IP 地址：*az.name-id.elb.region.amazonaws.com*。

Linux 或 Mac

```
$ dig +short us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Windows

```
C:\> nslookup us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

## 可用区 DNS 亲和性

使用默认客户端路由策略时，发送到网络负载均衡器 DNS 名称的请求将收到任何运行正常的负载均衡器 IP 地址。这会导致跨负载均衡器可用区分配客户端连接。使用可用区亲和性路由策略时，客户端 DNS 查询会优先考虑自身可用区中的负载均衡器 IP 地址。这有助于降低延迟和提高弹性，因为客户端在连接到目标时无需跨越可用区边界。

使用 Amazon Route 53 Resolver 的网络负载均衡器的可用客户端路由策略：

- 可用区亲和性 – 100% 可用区亲和性

客户端 DNS 查询将优先使用自身可用区中的负载均衡器 IP 地址。如果自身可用区中没有运行正常的负载均衡器 IP 地址，则查询可能会解析到其他可用区。

- 部分可用区亲和性 – 85% 可用区亲和性

85% 的客户端 DNS 查询会优先选择自身可用区中的负载均衡器 IP 地址，剩余的查询会解析到任何运行正常的可用区。如果自身可用区中没有运行正常的 IP 地址，则查询可能会解析到其他运行正常的可用区。如果所有可用区中都没有运行正常的 IP 地址，则查询会解析到任何可用区。

- 任意可用区 (默认值) – 0% 可用区亲和性

客户端 DNS 查询将在所有负载均衡器可用区中运行正常的负载均衡器 IP 地址中进行解析。

### Note

可用区亲和性路由策略仅适用于使用 Route 53 Resolver 解析网络负载均衡器 DNS 名称的客户端。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的 [什么是 Amazon Route 53 Resolver ?](#)。

可用区亲和性有助于将请求从客户端路由到负载均衡器，而跨可用区负载平衡有助于将请求从负载均衡器路由到目标。使用可用区关联性时，应关闭跨区域负载平衡，这样可以确保从客户端到目标的负载均衡器流量保持在同一个可用区内。使用此配置，客户端流量将发送到同一个网络负载均衡器可用区，因此建议将您的应用程序配置为在每个可用区中独立扩展。当每个可用区域的客户端数量或每个可用区的流量不相同，这是一个重要的考虑因素。有关更多信息，请参阅 [目标组的跨区域负载均衡](#)。

当可用区被认为运行不正常或开始可用区转移时，除非故障打开生效，否则该可用区 IP 地址将被视为运行不正常，并且不会返回至客户端。当 DNS 记录处于故障打开状态时，可用区亲和性将保持不变。这有助于保持可用区的独立性，并防止潜在的跨可用区故障。

使用可用区亲和性时，预计可用区之间有时会出现不平衡的情况。建议确保目标在可用区级别进行扩展，以支持每个可用区工作负载。如果不平衡情况十分严重，则建议关闭可用区亲和性。这样将可以在 60 秒内在所有负载均衡器可用区之间均匀分配客户端连接，或者在 DNS TTL 之间均匀分配。

在使用可用区亲和性之前，应注意以下几点：

- 可用区亲和性会导致使用 Route 53 Resolver 的所有网络负载均衡器客户端发生变化。
  - 客户端无法决定是要使用本可用区 DNS 解析，还是多可用区解析，相关决定由可用区亲和性代为作出。
  - 客户端并没有可靠的方法来确定其何时受到可用区亲和性的影响，也没有可靠的方法来确定 IP 地址所位于的具体可用区。
- 在 DNS 运行状况检查认为其可用区本地 IP 地址完全不正常并将其从 DNS 中移除前，客户端将继续分配该本地地址。
- 如果在开启跨区域负载平衡的情况下使用可用区亲和性，则可能会导致可用区之间的客户端连接分配失衡。建议将应用程序堆栈配置为在每个可用区中独立扩展，从而确保其可以支持相应的可用区客户端流量。
- 如果开启了跨可用区负载平衡，网络负载均衡器将受到跨可用区影响。
- 每个网络负载均衡器可用区的负载将与客户端请求的可用区位置成正比。如果您未配置在特定可用区中运行的客户端数量，则必须以被动方式独立扩展每个可用区。

## 监控

建议使用可用区负载均衡器指标来跟踪可用区之间的连接分配情况。您可以使用指标来查看每个可用区的新连接数和活跃连接数。

我们建议跟踪以下指标：

- **ActiveFlowCount** – 从客户端发往目标的并发流（或连接）总数。
- **NewFlowCount** – 指定时间段内建立的从客户端到目标的新流（或连接）总数。
- **HealthyHostCount** – 被视为运行正常的目标数量。
- **UnHealthyHostCount** – 被视为运行不正常的目标数量。

有关更多信息，请参阅[CloudWatch 您的 Network Load Balancer 的指标](#)

## 开启可用区亲和性

本过程中的步骤说明了如何使用 Amazon EC2 控制台开启可用区亲和性。

使用控制台开启可用区亲和性

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在可用区路由配置、客户端路由策略（DNS 记录）下，选择可用区亲和性或部分可用区亲和性。
6. 选择保存更改。

要开启可用区关联性，请使用 AWS CLI

使用带 `dns_record.client_routing_policy` 属性的 [modify-load-balancer-attributes](#) 命令。

## 关闭可用区亲和性

本过程中的步骤说明了如何使用 Amazon EC2 控制台关闭可用区亲和性。

使用控制台关闭可用区亲和性

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在可用区路由配置、客户端路由策略（DNS 记录）下，选择任何可用区亲和性。

## 6. 选择保存更改。

要关闭可用区关联性，请使用 AWS CLI

使用带 `dns_record.client_routing_policy` 属性的 [modify-load-balancer-attributes](#) 命令。

## 创建 Network Load Balancer

负载均衡器接收来自客户端的请求，并将请求分发给目标组中的目标 (如 EC2 实例)。

在开始之前，请确保您的负载均衡器的 Virtual Private Cloud (VPC) 在目标使用的每个可用区中至少有一个公有子网。您还必须配置目标组并注册至少一个目标以设置为默认值，才能将流量路由到目标组。

要使用创建负载均衡器 AWS CLI，请参阅[教程：使用 AWS CLI 创建 Network Load Balancer](#)。

要使用创建负载均衡器 AWS Management Console，请完成以下任务。

### 任务

- [步骤 1：配置目标组](#)
- [步骤 2：注册目标](#)
- [步骤 3：配置负载均衡器和侦听器](#)
- [步骤 4：测试负载均衡器](#)

## 步骤 1：配置目标组

配置目标组可使您注册 EC2 实例之类的目标。当您配置负载均衡器时，您在此步骤中配置的目标组将用作侦听器规则中的目标组。有关更多信息，请参阅[Network Load Balancer 的目标组](#)。

使用控制台配置目标群组

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择目标组。
3. 选择创建目标组。
4. 在基本配置窗格中执行以下操作：
  - a. 对于 Choose a target type (选择目标类型)，选择 Instance (实例) 以按实例 ID 注册目标，选择 IP addresses (IP 地址) 以按 IP 地址注册目标，或者选择 Application Load Balancer (应用程序负载均衡器) 以将某个应用程序负载均衡器注册为目标。

- b. 对于目标组名称，输入目标组的名称。
  - c. 对于 Protocol (协议)，选择协议，如下所示：
    - 如果侦听器协议为 TCP，选择 TCP 或 TCP\_UDP。
    - 如果侦听器协议为 TLS，选择 TCP 或 TLS。
    - 如果侦听器协议为 UDP，选择 UDP 或 TCP\_UDP。
    - 如果侦听器协议为 TCP\_UDP，选择 TCP\_UDP。
  - d. ( 可选 ) 对于端口，请根据需要修改默认值。
  - e. 对于 IP 地址类型，选择 IPv4 或 IPv6。此选项仅在目标类型为实例或 IP 地址且协议是 TCP 或 TLS 时可用。

您必须将一个 IPv6 目标组关联到一个双堆栈负载均衡器。目标组中的所有目标必须具有相同的 IP 地址类型。在创建目标组后，您将无法更改 IP 地址类型。
  - f. 对于 VPC，选择具有要注册的目标的虚拟私有云 ( VPC )。
5. 对于运行状况检查窗格，根据需要修改默认设置。对于高级运行状况检查，选择运行状况检查端口、计数、超时、间隔以及成功代码。如果运行状况检查连续超过不正常运行阈值计数，负载均衡器将使目标停止服务。如果运行状况检查连续超过运行状况正常阈值计数，负载均衡器将使目标恢复使用。有关更多信息，请参阅 [目标组的运行状况检查](#)。
  6. ( 可选 ) 要添加标签，请展开标签，选择添加标签，然后输入标签键和标签值。
  7. 选择 Next (下一步)。

## 步骤 2：注册目标

您可以向目标组注册 EC2 实例、IP 地址或 Application Load Balancer。这是创建负载均衡器的可选步骤。但是，您必须注册目标，以确保负载均衡器将流量路由到目标。

1. 在注册目标页面中，按如下方式添加一个或多个目标：
  - 如果目标类型为实例，请选择实例，输入端口，然后选择在下面以待注册的形式添加。
  - 如果目标类型为 IP 地址，请选择网络，输入 IP 地址和端口，然后选择在下面以待注册的形式添加。
  - 如果目标类型为 Application Load Balancer，选择一个 Application Load Balancer。
2. 选择 Create target group (创建目标组)。

## 步骤 3：配置负载均衡器和侦听器

要创建 Network Load Balancer，您必须首先提供负载均衡器的基本配置信息，例如名称、方案和 IP 地址类型。然后提供有关您的网络以及一个或多个侦听器的信息。侦听器是用于检查连接请求的进程。它配置了用于从客户端连接到负载均衡器的协议和端口。有关受支持的协议和端口的更多信息，请参阅[侦听器配置](#)。

使用控制台配置您的负载均衡器和侦听器

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择创建负载均衡器。
4. 在网络负载均衡器下，选择创建。
5. 基本配置
  - a. 对于 Load balancer name（负载均衡器名称），输入负载均衡器的名称。例如：**my-nlb**。您的 Network Load Balancer 的名称在该区域的 Application Load Balancer 和 Network Load Balancer 集中必须唯一。它最多可包含 32 个字符，并且只包含字母数字字符和连字符。它不能以连字符或 `internal-` 开头或结尾。
  - b. 对于 Scheme（方案），选择 Internet-facing（面向 Internet）或 Internal（内部）。面向互联网的负载均衡器将来自客户端的请求通过互联网路由到目标。内部负载均衡器使用私有 IP 地址将请求路由到目标。
  - c. 对于 IP 地址类型，如果您的客户端使用 IPv4 地址与负载均衡器通信，请选择 IPv4；如果客户端同时使用 IPv4 和 IPv6 地址与负载均衡器通信，则选择双堆栈。
6. 网络映射
  - a. 对于 VPC，选择您用于 EC2 实例的 VPC。

如果您为方案选择了 Internet-facing（面向 Internet），只有带有互联网网关的 VPC 可供选择。
  - b. 对于 Mappings（映射），选择一个或多个可用区和相应的子网。启用多个可用区可提高应用程序的容错能力。您可以指定已经与您共享的子网。

对于面向 Internet 的负载均衡器，您可以为每个可用区选择弹性 IP 地址。这将为您的负载均衡器提供静态 IP 地址。或者，对于内部负载均衡器，您可以从每个子网的 IPv4 范围内分配一个私有 IP 地址，而不必让您 AWS 分配一个。



7. 对于安全组，我们会为您的 VPC 预先选择默认安全组。您可以根据需要选择其他安全组。如果您没有合适的安全组，请选择创建新的安全组并创建一个满足您的安全需求的安全组。有关更多信息，请参阅《Amazon VPC 用户指南》中的[创建安全组](#)。

#### Warning

如果您现在没有将任何安全组与负载均衡器关联，则无法以后再将其关联。

### 8. 侦听器 and 路由

- a. 默认值是负责接收端口 80 上的 TCP 流量的侦听器。您可保留默认侦听器设置，或者根据需要修改协议和端口。
  - b. 对于默认操作，选择目标组以转发流量。如果以前没有创建任何目标组，则必须立即创建一个目标组。您还可以选择添加侦听器以添加其他侦听器（例如，TLS 侦听器）。
  - c. （可选）添加标签以对侦听器进行分类。
  - d. 对于安全侦听器设置（仅适用于 TLS 侦听器），请执行以下操作：
    - i. 对于安全策略，请选择符合您要求的安全策略。
    - ii. 对于 ALPN 策略，请选择一个策略以启用 ALPN，或选择无以禁用 ALPN。
    - iii. 对于默认 SSL 证书，选择来自 ACM（推荐）并选择证书。如果您没有可用证书，则可以将证书导入 ACM，或使用 ACM 为您预调配证书。有关更多信息，请参阅《AWS Certificate Manager 用户指南》中的[发布和管理证书](#)。
9. （可选）您可以将加载项服务与负载均衡器配合使用。例如，您可以选择为您 AWS Global Accelerator 创建加速器，并将您的负载均衡器与加速器关联。加速器名称可以包含以下字符（最多 64 个字符）：a-z、A-Z、0-9、。（句点）和-（连字符）。创建加速器后，进入 AWS Global Accelerator 控制台完成配置。有关更多信息，请参阅在[创建负载均衡器时添加加速器](#)

### 10. 标签

（可选）添加标签以对负载均衡器进行分类。有关更多信息，请参阅[标签](#)。

### 11. 摘要

查看配置，然后选择创建负载均衡器。在创建过程中，一些默认属性会应用于负载均衡器。创建负载均衡器后，您可以查看和编辑它们。有关更多信息，请参阅[负载均衡器属性](#)。

## 步骤 4：测试负载均衡器

在创建负载均衡器之后，您可验证您的 EC2 实例是否通过了初始运行状况检查，然后测试负载均衡器是否会将流量发送至您的 EC2 实例。要删除负载均衡器，请参阅 [删除 Network Load Balancer](#)。

### 要测试负载均衡器

1. 创建负载均衡器之后，选择关闭。
2. 在左侧导航窗格中，选择目标组。
3. 选择新目标组。
4. 选择 Targets (目标) 并验证您的实例是否已就绪。如果实例状态是 `initial`，很可能是因为，实例仍在注册过程中，或者未通过视为正常运行所需的运行状况检查最小数量。在至少一个实例的状态为正常后，便可测试负载均衡器。有关更多信息，请参阅 [目标运行状况](#)。
5. 在导航窗格中，选择负载均衡器。
6. 选择新的负载均衡器。
7. 复制负载均衡器的 DNS 名称（例如，`my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com`）。将该 DNS 名称粘贴到已连接 Internet 的 Web 浏览器的地址栏中。如果一切正常，浏览器会显示您服务器的默认页面。

## Network Load Balancer 的 IP 地址类型

您可以配置您的 Network Load Balancer，以便客户端可以仅使用 IPv4 地址或同时使用 IPv4 和 IPv6 地址（双堆栈）与负载均衡器进行通信。负载均衡器根据目标组的 IP 地址类型与目标进行通信。有关更多信息，请参阅 [IP 地址类型](#)。

### dualstack 要求

- 您可以在创建负载均衡器时设置 IP 地址类型并随时更新它。
- 您为负载均衡器指定的 Virtual Private Cloud (VPC) 和子网必须具有关联的 IPv6 CIDR 块。有关更多信息，请参阅 Amazon EC2 用户指南中的 [IPv6 地址](#)。
- 负载均衡器必须有 TCP 或 TLS 侦听器。
- 负载均衡器子网的路由表必须路由 IPv6 流量。
- 负载均衡器子网的网络 ACL 必须允许 IPv6 流量。

### 在创建时设置 IP 地址类型

如 [创建负载均衡器](#) 中所述配置设置。

使用控制台更新 IP 地址类型

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选中负载均衡器对应的复选框。
4. 选择操作和编辑 IP 地址类型。
5. 对于 IP 地址类型，选择 ipv4 可仅支持 IPv4 地址，选择 dualstack 可同时支持 IPv4 和 IPv6 地址。
6. 选择保存更改。

要更新 IP 地址，请使用 AWS CLI

使用 [set-ip-address-type](#) 命令。

## 网络负载均衡器的安全组

您可以将安全组与网络负载均衡器关联，以控制允许到达和离开负载均衡器的流量。您可以指定允许入站流量的端口、协议和来源，以及允许出站流量的端口、协议和目的地。如果您没有为负载均衡器分配安全组，则所有客户端流量都可以到达负载均衡器侦听器，并且所有流量都可以离开负载均衡器。

您可以向与目标关联的安全组添加规则，该规则引用与网络负载均衡器关联的安全组。这允许客户端通过负载均衡器向目标发送流量，但不会将流量直接发送到您的目标。在与目标关联的安全组中引用与网络负载均衡器关联的安全组，可确保即使对负载均衡器启用了[客户端 IP 保留](#)，目标也能接受来自负载均衡器的流量。

您无需为入站安全组规则阻止的流量付费。

内容

- [注意事项](#)
- [示例：筛选客户端流量](#)
- [示例：仅接受来自负载均衡器的流量](#)
- [更新关联的安全组](#)
- [更新安全设置](#)

- [监控负载均衡器安全组](#)

## 注意事项

- 在创建网络负载均衡器时，您可以将安全组与网络负载均衡器相关联。如果您在创建网络负载均衡器时未关联任何安全组，则以后也无法将其与负载均衡器关联。我们建议您在创建负载均衡器时，将安全组与负载均衡器相关联。
- 创建网络负载均衡器并关联安全组后，您可以随时更改与负载均衡器关联的安全组。
- 运行状况检查受出站规则的约束，但不受入站规则的约束。您必须确保出站规则不会阻止运行状况检查流量。否则，负载均衡器会认为目标运行状况不佳。
- 您可以控制 PrivateLink 流量是否受入站规则的约束。如果您对 PrivateLink 流量启用入站规则，则流量来源是客户端的私有 IP 地址，而不是端点接口。

## 示例：筛选客户端流量

与网络负载均衡器关联的安全组中的以下入站规则仅允许来自指定地址范围的流量。如果这是内部负载均衡器，则可以指定 VPC CIDR 范围作为来源，以仅允许来自特定 VPC 的流量。如果这是面向互联网的负载均衡器，其必须接受来自互联网任何位置的流量，则可以指定 0.0.0.0/0 作为来源。

### 入站

协议	来源	端口范围	注释
<i>protocol</i>	<i>### IP ###</i>	<i>#####</i>	在侦听器端口上允许来自源 CIDR 的入站流量
ICMP	0.0.0.0/0	全部	允许入站 ICMP 流量，以支持 MTU 或路径 MTU 发现 †

† 有关更多信息，请参阅 Amazon EC2 用户指南中的 [MTU 发现路径](#)。

### 出站

协议	目标位置	端口范围	注释
全部	Anywhere	全部	允许所有出站流量

## 示例：仅接受来自负载均衡器的流量

假设您的网络负载均衡器有安全组 sg-111112222233333。在与目标实例关联的安全组中使用以下规则，确保它们仅接受来自网络负载均衡器的流量。您必须确保目标在目标端口和运行状况检查端口上都接受来自负载均衡器的流量。有关更多信息，请参阅 [the section called “目标安全组”](#)。

### 入站

协议	来源	端口范围	注释
<i>protocol</i>	sg-111112 222233333	####	在目标端口上允许来自负载均衡器的入站流量
<i>protocol</i>	sg-111112 222233333	#####	在运行状况检查端口上允许来自负载均衡器的入站流量

### 出站

协议	目标位置	端口范围	注释
全部	Anywhere	任何	允许所有出站流量

## 更新关联的安全组

如果您在创建负载均衡器时，将至少一个安全组与该负载均衡器关联，则可以随时更新该负载均衡器的安全组。

### 使用控制台更新安全组

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的 Load Balancing ( 负载均衡 ) 下，选择 Load Balancers ( 负载均衡器 ) 。
3. 选择负载均衡器。
4. 在安全性选项卡上，选择编辑。
5. 要将一个安全组与负载均衡器关联，请选择此安全组。要从负载均衡器中删除一个安全组，请清除该安全组。
6. 选择保存更改。

要更新安全组，请使用 AWS CLI

使用 [set-security-groups](#) 命令。

## 更新安全设置

默认情况下，我们将入站安全组规则应用于发送到负载均衡器的所有流量。但是，您可能不想将这些规则应用于通过负载均衡器发送的流量 AWS PrivateLink，这些流量可能来自重叠的 IP 地址。在这种情况下，您可以配置负载均衡器，这样我们就不会对通过发送到负载均衡器的流量应用入站规则 AWS PrivateLink。

使用控制台更新安全设置

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的 Load Balancing（负载均衡）下，选择 Load Balancers（负载均衡器）。
3. 选择负载均衡器。
4. 在安全性选项卡上，选择编辑。
5. 在“安全”设置下，清除“对 PrivateLink 流量强制执行入站规则”。
6. 选择保存更改。

要更新安全设置，请使用 AWS CLI

使用 [set-security-groups](#) 命令。

## 监控负载均衡器安全组

使

用 SecurityGroupBlockedFlowCount\_Inbound 和 SecurityGroupBlockedFlowCount\_Outbound CloudWatch 指标来监控被负载均衡器安全组阻止的流量数量。被阻止的流量未反映在其他指标中。有关更多信息，请参阅 [the section called “CloudWatch 指标”](#)。

使用 VPC 流日志来监控负载均衡器安全组接受或拒绝的流量。有关更多信息，请参阅 Amazon VPC 用户指南中的 [VPC 流日志](#)。

## 您的 Network Load Balancer 的标签

借助标签，您可以按不同的方式对负载均衡器进行分类。例如，您可以按用途、所有者或环境为资源添加标签。

您最多可以为每个负载均衡器添加多个标签。如果您添加的标签中的键已经与负载均衡器关联，它将更新该标签的值。

当您用完标签时，可以从负载均衡器中将其删除。

### 限制

- 每个资源的标签数上限 - 50
- 最大密钥长度 - 127 个 Unicode 字符
- 最大值长度 - 255 个 Unicode 字符
- 标签键和值区分大小写。允许使用的字符包括可用 UTF-8 格式表示的字母、空格和数字，以及以下特殊字符：+ - = 。 \_ : / @。请不要使用前导空格或尾随空格。
- 请勿在标签名称或值中使用aws:前缀，因为它已保留供 AWS 使用。您无法编辑或删除带此前缀的标签名称或值。具有此前缀的标签不计入每个资源的标签数限制。

### 使用控制台更新负载均衡器的标签

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在标签选项卡上，选择管理标签。
5. 要添加标签，请选择添加标签，然后输入标签键和值。允许的字符包括字母、空格、数字（UTF-8 格式）和以下特殊字符：+ - = 。 \_ : / @。请不要使用前导空格或尾随空格。标签值区分大小写。
6. 要更新标签，请在键和值中输入新值。
7. 要删除标签，请选择标签旁边的删除按钮。
8. 完成后，请选择保存更改。

要更新负载均衡器的标签，请使用 AWS CLI

使用 [add-tags](#) 和 [remove-tags](#) 命令。

## 删除 Network Load Balancer

在您的负载均衡器可用之后，您需要为保持其运行的每小时或部分小时支付费用。当您不再需要该负载均衡器时，可将其删除。当负载均衡器被删除之后，您便不再需要支付负载均衡器费用。

如果已启用删除保护，则无法删除负载均衡器。有关更多信息，请参阅 [删除保护](#)。

如果其他服务正在使用负载均衡器，则无法删除该负载均衡器。例如，如果负载均衡器与 VPC 终端节点服务关联，则必须先删除终端节点服务配置，然后才能删除关联的负载均衡器。

删除负载均衡器也将删除其侦听器。删除负载均衡器不会影响其注册目标。例如，您的 EC2 实例将继续运行并仍注册到其目标组。要删除目标组，请参阅 [删除目标组](#)。

### 使用控制台删除负载均衡器

1. 如果您有一个指向负载均衡器的域的一个 DNS 记录，请将它指向新的位置并等待 DNS 更改生效，然后再删除您的负载均衡器。

例如：

- 如果此记录是存活时间 (TTL) 为 300 秒的 CNAME 记录，请至少等待 300 秒，然后再继续执行下一步。
- 如果此记录是 Route 53 别名 (A) 记录，请至少等待 60 秒。
- 如果使用 Route 53，则记录更改需要 60 秒才能传播到所有全局 Route 53 名称服务器。将此时间添加到正在更新的记录的 TTL 值。

2. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
3. 在导航窗格中，选择负载均衡器。
4. 选中负载均衡器对应的复选框。
5. 依次选择操作、删除负载均衡器。
6. 如果提示进行确认，输入 **confirm**，并选择删除。

要删除负载均衡器，请使用 AWS CLI

使用 [delete-load-balancer](#) 命令。

## 可用区转移

可用区转移是 Amazon Route 53 应用程序恢复控制器 (Route 53 ARC) 中的一项功能。通过可用区转移，只需执行一次操作即可将负载均衡器资源从受损的可用区转移出去。这样，您就可以继续从 AWS 区域中的其他运行状况良好的可用区运行。

当您启动可用区转移时，负载均衡器会停止向受影响的可用区发送这些资源的流量。Route 53 ARC 会立即创建可用区转移。但是，可能需要很短时间 (通常长达几分钟) 才能完成受影响可用区中正在进行



的现有连接。有关更多信息，请参阅《Amazon Route 53 应用程序恢复控制器开发人员指南》中的[可用区转移的工作原理：运行状况检查和区域 IP 地址](#)。

只有关闭了跨可用区负载均衡的应用程序负载均衡器和网络负载均衡器才支持可用区转移。如果您开启了跨可用区负载均衡，则无法启动可用区转移。有关更多信息，请参阅《Amazon Route 53 应用程序恢复控制器开发人员指南》中的[可用区转移支持的资源](#)。

在使用可用区转移之前，请查看以下内容：

- 可用区转移不支持跨区域负载均衡。要使用此功能，必须关闭跨可用区负载均衡。
- 在 AWS Global Accelerator 中将应用程序负载均衡器用作加速器端点时，不支持可用区转移。
- 只能为单个可用区中的特定负载均衡器启动可用区转移。无法为多个可用区启动可用区转移。
- AWS 当多个基础设施问题影响服务时，主动从 DNS 中删除区域负载均衡器 IP 地址。在开始可用区转移之前，请务必检查当前的可用区容量。如果您的负载均衡器已关闭跨可用区负载均衡，而您使用可用区转移来删除可用区负载均衡器 IP 地址，则受可用区转移影响的可用区也会失去目标容量。
- 当应用程序负载均衡器是网络负载均衡器的目标时，请始终从网络负载均衡器启动可用区转移。如果从应用程序负载均衡器启动可用区转移，则网络负载均衡器将不会识别转移，并继续向应用程序负载均衡器发送流量。

有关更多指南和信息，请参阅《Amazon Route 53 应用程序恢复控制器开发人员指南》中的[Route 53 ARC 可用区转移最佳实践](#)。

## 启动可用区转移

本程序中的步骤介绍如何使用 Amazon EC2 控制台启动可用区转移。有关使用 Route 53 ARC 控制台启动可用区转移的步骤，请参阅《Amazon Route 53 应用程序恢复控制器开发人员指南》中的[启动可用区转移](#)。

使用控制台启动可用区转移

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择负载均衡器名称。
4. 在 Integrations (集成) 选项卡上的 Route 53 Application Recovery Controller (Route 53 应用程序恢复控制器) 下，选择 Start zonal shift (启动可用区转移)。
5. 选择要将流量移离的可用区。

6. 选择或输入可用区转移的到期时间。可用区转移最初可以从 1 分钟设置为三天 ( 72 小时 ) 。

所有可用区转移都是暂时的。您必须设置过期时间，但可以稍后更新活跃转移以设置新的过期时间。

7. 输入注释。如果您愿意，可以稍后更新可用区转移以编辑注释。
8. 选中该复选框以确认启动可用区转移，这会将流量移离该可用区，从而减少应用程序的容量。
9. 选择启动。

要开始区域移动，请使用 AWS CLI

要以编程方式使用可用区转移，请参阅《[可用区转移 API 参考指南](#)》。

## 更新可用区转移

本程序中的步骤介绍如何使用 Amazon EC2 控制台更新可用区转移。有关使用 Amazon Route 53 应用程序恢复控制器控制台更新可用区转移的步骤，请参阅《Amazon Route 53 应用程序恢复控制器开发人员指南》中的[更新可用区转移](#)。

使用控制台更新可用区转移

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择具有活跃可用区转移的负载均衡器名称。
4. 在集成选项卡的 Route 53 应用程序恢复控制器下，选择更新可用区转移。

此时将打开 Route 53 ARC 控制台以继续更新。

5. 对于设置可用区转移到期时间，可以选择或输入到期时间。
6. 对于 Comment ( 注释 )，可以选择编辑现有注释或输入新注释。
7. 选择更新。

要更新区域偏移，请使用 AWS CLI

要以编程方式使用可用区转移，请参阅《[可用区转移 API 参考指南](#)》。

## 取消可用区转移

本程序中的步骤介绍如何使用 Amazon EC2 控制台取消可用区转移。有关使用 Amazon Route 53 应用程序恢复控制器控制台取消可用区转移的步骤，请参阅《Amazon Route 53 应用程序恢复控制器开发人员指南》中的[取消可用区转移](#)。

### 使用控制台取消可用区转移

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择具有活跃可用区转移的负载均衡器名称。
4. 在集成选项卡上的 Route 53 应用程序恢复控制器下，选择取消可用区转移。

此时将打开 Route 53 ARC 控制台以继续取消。

5. 选择 Cancel zonal shift (取消可用区转移)。
6. 在确认对话框中，选择 Confirm (确认)。

要取消区域偏移，请使用 AWS CLI

要以编程方式使用可用区转移，请参阅《[可用区转移 API 参考指南](#)》。

# 网络负载均衡器的侦听器

侦听器是一个使用您配置的协议和端口检查连接请求的进程。您必须至少添加一个侦听器，然后才能开始使用网络负载均衡器。如果您的负载均衡器没有侦听器，则无法接收来自客户端的流量。您为侦听器定义的规则决定了负载均衡器会如何将请求路由到您注册的目标（例如 EC2 实例）。

内容

- [侦听器配置](#)
- [侦听器规则](#)
- [为网络负载均衡器创建侦听器](#)
- [网络负载均衡器的 TLS 侦听器](#)
- [更新网络负载均衡器的侦听器](#)
- [更新网络负载均衡器的 TLS 侦听器](#)
- [删除网络负载均衡器的侦听器](#)

## 侦听器配置

侦听器支持以下协议和端口：

- 协议：TCP、TLS、UDP TCP\_UDP
- 端口：1-65535

可以使用 TLS 侦听器将加密和解密的工作交给负载均衡器完成，以便应用程序可以专注于其业务逻辑。如果侦听器协议为 TLS，您必须在侦听器上确切地部署一个 SSL 服务器证书。有关更多信息，请参阅 [网络负载均衡器的 TLS 侦听器](#)。

如果必须确保目标解密 TLS 流量而不是负载均衡器，则可以在端口 443 上创建 TCP 侦听器，而不是创建 TLS 侦听器。通过 TCP 侦听器，负载均衡器将加密流量传递到目标，而不会对其进行解密。

要在同一端口上同时支持 TCP 和 UDP，请创建一个 TCP\_UDP 侦听器。TCP\_UDP 侦听器的目标组必须使用 TCP\_UDP 协议。

对于 dualstack Network Load Balancer，仅支持 TCP 和 TLS 协议。

您可以与听众 WebSockets 一起使用。

发送到已配置侦听器的所有网络流量都归类为预期流量。与配置的侦听器不匹配的网络流量被归类为非预期流量。除类型 3 以外的 ICMP 请求也被视为意外流量。网络负载均衡器会丢弃意外流量，而不会将其转发到任何目标。如果发送到已配置侦听器的侦听器端口的 TCP 数据包不是新的连接，或者不是有效 TCP 连接的一部分，则将通过 TCP 重置 (RST) 拒绝。

有关更多信息，请参阅 Elastic Load Balancing 用户指南中的[请求路由](#)。

## 侦听器规则

在创建侦听器时，将会指定用于路由请求的规则。该规则将请求转发到指定的目标组。要更新此规则，请参阅[更新网络负载均衡器的侦听器](#)。

## 为网络负载均衡器创建侦听器

侦听器是用于检查连接请求的进程。您可在创建负载均衡器时定义侦听器，并可随时向负载均衡器添加侦听器。

### 先决条件

- 必须为侦听器规则指定目标组。有关更多信息，请参阅[为 Network Load Balancer 创建目标组](#)。
- 您必须指定 TLS 监听器的 SSL 证书。负载均衡器先使用证书终止连接，然后解密来自客户端的请求，最后再将请求路由到目标。有关更多信息，请参阅[服务器证书](#)。

## 添加侦听器

您为侦听器配置用于从客户端连接到负载均衡器的协议和端口，并为默认侦听器规则配置目标组。有关更多信息，请参阅[侦听器配置](#)。

### 使用控制台添加侦听器

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在 Listeners ( 侦听器 ) 选项卡上，选择 Add listener ( 添加侦听器 ) 。
5. 对于 Protocol ( 协议 ) ，选择 TCP、UDP、TCP\_UDP 或 TLS。保留默认端口或键入其他端口。  
对于双堆栈网络负载均衡器，仅支持 TCP 和 TLS 协议。
6. 对于 Default action ( 默认操作 ) ，选择可用目标组。

7. [TLS 侦听器] 对于 Security policy (安全策略), 建议您保留默认安全策略。
8. [TLS 侦听器] 对于 Default SSL certificate (默认 SSL 证书), 请执行下列操作之一：
  - 如果您使用创建或导入了证书 AWS Certificate Manager, 请选择 From ACM 并选择证书。
  - 如果使用 IAM 上传了证书, 则选择从 IAM 并选择证书。
9. [TLS 侦听器] 对于 ALPN policy (ALPN 策略), 请选择一个策略以启用 ALPN, 或选择 None (无) 以禁用 ALPN。有关更多信息, 请参阅 [ALPN 策略](#)。
10. 选择 添加。
11. [TLS 侦听器] 要添加用于 SNI 协议的可选证书列表, 请参阅[将证书添加到证书列表](#)。

要添加侦听器, 请使用 AWS CLI

使用 [create-listener](#) 命令来创建侦听器。

## 网络负载均衡器的 TLS 侦听器

要使用 TLS 侦听器, 您必须在负载均衡器上部署至少一个服务器证书。负载均衡器先使用此服务器证书终止前端连接, 再解密来自客户端的请求, 然后将请求发送到目标。注意, 如果您需要将加密流量传输至目标且负载均衡器不对其进行解密, 则可以在端口 443 上创建 TCP 侦听器, 而不是创建 TLS 侦听器。负载均衡器将按原样将请求传输至目标, 而不解密请求。

Elastic Load Balancing 使用 TLS 协商配置 (称为安全策略) 在客户端与负载均衡器之间协商 TLS 连接。安全策略是协议和密码的组合。协议在客户端与服务器之间建立安全连接, 确保在客户端与负载均衡器之间传递的所有数据都是私密数据。密码是使用加密密钥创建编码消息的加密算法。协议使用多种密码对 Internet 上的数据进行加密。在连接协商过程中, 客户端和负载均衡器会按首选项顺序提供各自支持的密码和协议的列表。为安全连接选择服务器列表中与任一客户端的密码匹配的密码。

网络负载均衡器不支持 TLS 重新协商或双向 TLS 身份验证 (mTLS)。要获得 mTLS 支持, 请创建 TCP 侦听器, 而不是 TLS 侦听器。负载均衡器按原样传输请求, 因此您可以在目标上实施 mTLS。

要创建 TLS 侦听器, 请参阅[添加侦听器](#)。有关相关演示, 请参阅[网络负载均衡器上的 TLS 支持](#)和[网络负载均衡器上的 SNI 支持](#)。

## 服务器证书

负载均衡器需要 X.509 证书 (服务器证书)。证书是由证书颁发机构 (CA) 颁发的数字化身份。证书包含标识信息、有效期限、公有密钥、序列号以及发布者的数字签名。

在创建用于负载均衡器的证书时，您必须指定域名。证书上的域名必须与自定义域名记录匹配，以确保我们能够验证 TLS 连接。如果不匹配，则流量不会加密。

必须为证书指定完全限定域名 (FQDN) (例如 `www.example.com`) 或顶点域名 (例如 `example.com`)。您还可以使用星号 (\*) 作为通配符来保护同一域中的多个站点名称。请求通配符证书时，星号 (\*) 必须位于域名的最左侧位置，而且只能保护一个子域级别。例如，`*.example.com` 保护 `corp.example.com` 和 `images.example.com`，但无法保护 `test.login.example.com`。另请注意，`*.example.com` 仅保护 `example.com` 的子域，而不保护裸域或顶点域 (`example.com`)。通配符名称显示在证书的 Subject (主题) 字段和 Subject Alternative Name (主题替代名称) 扩展中。有关公有证书的更多信息，请参阅《AWS Certificate Manager 用户指南》中的 [请求公有证书](#)。

我们建议您使用 [AWS Certificate Manager \(ACM\)](#) 为您的负载均衡器创建证书。ACM 与 Elastic Load Balancing 集成，以便您可以在负载均衡器上部署证书。有关更多信息，请参阅 [AWS Certificate Manager 用户指南](#)。

或者，您可以使用 TLS 工具创建证书签名请求 (CSR)，然后获取 CA 签署的 CSR 以生成证书，然后将证书导入 ACM 或将证书上传到 AWS Identity and Access Management (IAM)。有关更多信息，请参阅 AWS Certificate Manager 用户指南中的 [导入证书](#) 或 IAM 用户指南中的 [使用服务器证书](#)。

## 内容

- [支持的密钥算法](#)
- [默认证书](#)
- [证书列表](#)
- [证书续订](#)

## 支持的密钥算法

- RSA 1024 位
- RSA 2048 位
- RSA 3072 位
- ECDSA 256 位
- ECDSA 384 位
- ECDSA 521 位

## 默认证书

创建 TLS 侦听器时，必须仅指定一个证书。此证书称为默认证书。创建 TLS 侦听器后，您可以替换默认证书。有关更多信息，请参阅 [替换默认证书](#)。

如果在[证书列表](#)中指定其他证书，则仅当客户端在不使用服务器名称指示 (SNI) 协议的情况下连接以指定主机名或证书列表中没有匹配的证书时，才使用默认证书。

如果您未指定其他证书但需要通过单一负载均衡器托管多个安全应用程序，则可以使用通配符证书或为证书的每个其他域添加使用者备用名称 (SAN)。

## 证书列表

创建 TLS 侦听器后，它具有默认证书和空证书列表。您可以选择将证书添加到侦听器的证书列表中。使用证书列表可使负载均衡器在同一端口上支持多个域，并为每个域提供不同的证书。有关更多信息，请参阅 [将证书添加到证书列表](#)。

负载均衡器使用支持 SNI 的智能证书选择算法。如果客户端提供的主机名与证书列表中的一个证书匹配，则负载均衡器将选择此证书。如果客户端提供的主机名与证书列表中的多个证书匹配，则负载均衡器将选择客户端可支持的最佳证书。根据以下标准，按下面的顺序选择证书：

- 哈希算法 (SHA 优先于 MD5)
- 密钥长度 (首选最大值)
- 有效期

负载均衡器访问日志条目指示客户端指定的主机名和向客户端提供的证书。有关更多信息，请参阅 [访问日志条目](#)。

## 证书续订

每个证书都有有效期限。您必须确保在有效期结束之前续订或替换负载均衡器的每个证书。这包括默认证书和证书列表中的证书。续订或替换证书不影响负载均衡器节点已收到的进行中的请求，并暂停指向正常运行的目标的路由。续订证书之后，新的请求将使用续订后的证书。更换证书之后，新的请求将使用新证书。

您可以按如下方式管理证书续订和替换：

- 由您的负载均衡器提供 AWS Certificate Manager 并部署在您的负载均衡器上的证书可以自动续订。ACM 会尝试在到期之前续订证书。有关更多信息，请参阅 AWS Certificate Manager 用户指南中的[托管续订](#)。



- 如果您将证书导入 ACM，则必须监视证书的到期日期并在到期前续订。有关更多信息，请参阅 [AWS Certificate Manager 用户指南中的导入证书](#)。
- 如果您已将证书导入 IAM 中，则必须创建一个新证书，将该新证书导入 ACM 或 IAM 中，将该新证书添加到负载均衡器，并从负载均衡器删除过期的证书。

## 安全策略

创建 TLS 侦听器时，您必须选择一个安全策略。可以根据需要更新安全策略。有关更多信息，请参阅 [更新安全策略](#)。

注意事项：

- 该 `ELBSecurityPolicy-TLS13-1-2-2021-06` 策略是使用创建的 TLS 侦听器的默认安全策略。AWS Management Console
  - 我们推荐使用 `ELBSecurityPolicy-TLS13-1-2-2021-06` 安全策略，该策略包括 TLS 1.3，并且向后兼容 TLS 1.2。
- 该 `ELBSecurityPolicy-2016-08` 策略是使用创建的 TLS 侦听器的默认安全策略。AWS CLI
- 您可以选择用于前端连接的安全策略，但不能选择用于后端连接的安全策略。
  - 对于后端连接，如果您的 TLS 侦听器使用的是 TLS 1.3 安全策略，则使用 `ELBSecurityPolicy-TLS13-1-0-2021-06` 安全策略。否则，`ELBSecurityPolicy-2016-08` 安全策略用于后端连接。
- 为了满足要求禁用某些 TLS 协议版本的合规性和安全标准，或者为了支持需要已弃用密码的旧客户端，您可以使用其中一个安全策略。ELBSecurityPolicy-TLS-您可以启用访问日志，以获取有关发送到您的 Network Load Balancer 的 TLS 请求的信息，分析 TLS 流量模式，管理安全策略升级，并对问题进行故障排除。为您的负载均衡器启用访问日志记录并检查相应的访问日志条目。有关更多信息，请参阅 [访问日志](#) 和 [Network Load Balancer 示例查询](#)。
- 您可以分别使用您 AWS 账户的 IAM 中的 [Elastic Load Balancing 条件密钥](#) 和服务控制策略 (SCP) 来限制用户可以使用哪些安全策略。AWS Organizations 有关更多信息，请参阅《AWS Organizations 用户指南》中的 [服务控制策略 \(SCP\)](#)

## TLS 1.3 安全策略

Elastic Load Balancing 为网络负载均衡器提供以下 TLS 1.3 安全策略：

- `ELBSecurityPolicy-TLS13-1-2-2021-06` (推荐)
- `ELBSecurityPolicy-TLS13-1-2-Res-2021-06`

- ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06
- ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06
- ELBSecurityPolicy-TLS13-1-1-2021-06
- ELBSecurityPolicy-TLS13-1-0-2021-06
- ELBSecurityPolicy-TLS13-1-3-2021-06

## FIPS 安全政策

联邦信息处理标准 (FIPS) 是美国和加拿大政府的一项标准，它规定了保护敏感信息的加密模块的安全要求。要了解更多信息，请参阅AWS 云安全合规性页面上的[联邦信息处理标准 \(FIPS\) 140](#)。

所有 FIPS 策略都使用 AWS-LC FIPS 验证的加密模块。要了解更多信息，请参阅 NIST 加密模块验证计划网站上的 AWS-LC 加密[模块](#)页面。

Elastic Load Balancing 为网络负载均衡器提供以下 FIPS 安全策略：

- ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 ( 推荐 )
- ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04

## FS 支持的策略

Elastic Load Balancing 为网络负载均衡器提供了以下 FS ( 向前保密 ) 支持的安全策略：

- ELBSecurityPolicy-FS-1-2-Res-2020-10
- ELBSecurityPolicy-FS-1-2-Res-2019-08
- ELBSecurityPolicy-FS-1-2-2019-08
- ELBSecurityPolicy-FS-1-1-2019-08
- ELBSecurityPolicy-FS-2018-06

## TLS 1.0-1.2 安全策略

Elastic Load Balancing 为网络负载均衡器提供以下 TLS 1.0-1.2 安全策略：

- ELBSecurityPolicy-TLS-1-2-Ext-2018-06
- ELBSecurityPolicy-TLS-1-2-2017-01
- ELBSecurityPolicy-TLS-1-1-2017-01
- ELBSecurityPolicy-2016-08
- ELBSecurityPolicy-TLS-1-0-2015-04
- ELBSecurityPolicy-2015-05 ( 等同于 **ELBSecurityPolicy-2016-08** )

## TLS 协议和密码

### TLS 1.3

下表描述了可用的 TLS 1.3 安全策略支持的 TLS 协议和密码。

注意：该ELBSecurityPolicy-前缀已从安全策略行的策略名称中删除。

示例：安全策略显示ELBSecurityPolicy-TLS13-1-2-2021-06为TLS13-1-2-2021-06。

安全策略	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
TLS 协议							
Protocol-TLSv1							✓
Protocol-TLSv1.1						✓	✓
Protocol-TLSv1.2	✓		✓	✓	✓	✓	✓

## 安全策略

	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-1-2021-06	TLS13-1-0-2021-06
协议- tlsv1.3	✓	✓	✓	✓	✓	✓	✓
TLS 密码							
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓
TLS_CHACHA20_POLY1305_SHA256	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓

## 安全策略

	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
ECDHE- ECDSA- AES128- SHA256	✓			✓	✓	✓	✓
ECDHE- RSA- AES128- SHA256	✓			✓	✓	✓	✓
ECDHE- ECDSA- AES128- SHA				✓		✓	✓
ECDHE- RSA- AES128- SHA				✓		✓	✓
ECDHE- ECDSA- AES256 - GCM- SHA384	✓		✓	✓	✓	✓	✓
ECDHE- RSA- AES256- GCM- SHA384	✓		✓	✓	✓	✓	✓

## 安全策略

	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
ECDHE- ECDSA- AES256- SHA384	✓			✓	✓	✓	✓
ECDHE- RSA- AES256- SHA384	✓			✓	✓	✓	✓
ECDHE- RSA- AES256- SHA				✓		✓	✓
ECDHE- ECDSA- AES256- SHA				✓		✓	✓
AES128- GCM- SHA256				✓	✓	✓	✓
AES128- SHA256				✓	✓	✓	✓
AES128- SHA				✓		✓	✓

安全策略	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
AES256-GCM-SHA384				✓	✓	✓	✓
AES256-SHA256				✓	✓	✓	✓
AES256-SHA				✓		✓	✓

使用 CLI 创建使用 TLS 1.3 策略的 TLS 侦听器

在任何 [TLS 1.3 安全策略](#) 中使用 [create-listener](#) 命令。

该示例使用 ELBSecurityPolicy-TLS13-1-2-2021-06 安全策略。

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

使用 CLI 修改 TLS 侦听器以使用 TLS 1.3 策略

在任何 [TLS 1.3 安全策略](#) 中使用 [modify-listener](#) 命令。

该示例使用 ELBSecurityPolicy-TLS13-1-2-2021-06 安全策略。

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

使用 CLI 查看侦听器使用的安全策略

将 desc [ribe-listener](#) 命令与你的[监听器](#)配合使用arn。

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

使用 CLI 查看 TLS 1.3 安全策略的配置

将该[describe-ssl-policies](#)命令与任何 [TLS 1.3 安全策略](#)一起使用。

该示例使用ELBSecurityPolicy-TLS13-1-2-2021-06安全策略。

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-2021-06
```

## FIPS

### Important

提供策略ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04和仅ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04是为了兼容旧版。虽然他们使用FIPS140 模块使用 FIPS 加密，但它们可能不符合 NIST 最新的 TLS 配置指南。

下表描述了可用的 FIPS 安全策略支持的 TLS 协议和密码。

注意：该ELBSecurityPolicy-前缀已从安全策略行的策略名称中删除。

示例：安全策略显示ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04为TLS13-1-2-FIPS-2023-04。

安全策略	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
TLS 协议								



## 安全策略

	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
Protocol-TLSv1								✓
Protocol-TLSv1.1							✓	✓
Protocol-TLSv1.2		✓	✓	✓	✓	✓	✓	✓
协议-tlsv1.3	✓	✓	✓	✓	✓	✓	✓	✓
TLS 密码								
TLS_AES_128_GCM_SHA256		✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-SHA256		✓	✓	✓	✓	✓	✓	✓

## 安全策略

安全策略	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES128-GCM-SHA256		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECD-SA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-ECD-SA-AES128-SHA				✓		✓	✓	✓

## 安全策略

	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES128-SHA				✓		✓	✓	✓
ECDHE-ECD SA-AES256 - GCM- SHA384	✓	✓	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECD SA-AES256 - SHA384			✓	✓	✓	✓	✓	✓

## 安全策略

	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES256-SHA384			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA				✓		✓	✓	✓
ECDHE-ECDHE-SHA-AES256-SHA				✓		✓	✓	✓
AES128-GCM-SHA256					✓	✓	✓	✓
AES128-SHA256					✓	✓	✓	✓
AES128-SHA						✓	✓	✓

安全策略	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
AES256-GCM-SHA384					✓	✓	✓	✓
AES256-SHA A256					✓	✓	✓	✓
AES256-SHA						✓	✓	✓

使用 CLI 创建使用 FIPS 策略的 TLS 侦听器

将 [create-listener](#) 命令与任何 [FIPS](#) 安全策略一起使用。

该示例使用 `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` 安全策略。

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

使用 CLI 修改 TLS 侦听器以使用 FIPS 策略

在任何 [FIPS](#) 安全策略中使用 [modify-listener](#) 命令。

该示例使用 `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` 安全策略。

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

使用 CLI 查看监听器使用的安全策略

将 desc [ribe-listener](#) 命令与你的[监听器](#)配合使用arn。

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

使用 CLI 查看 FIPS 安全策略的配置

将该[describe-ssl-policies](#)命令与任何 [FIPS 安全策略](#)一起使用。

该示例使用ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04安全策略。

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

## FS

下表描述了支持的 TLS 协议和可用的 FS 支持的安全策略的密码。

注意：该ELBSecurityPolicy-前缀已从安全策略行的策略名称中删除。

示例：安全策略显示ELBSecurityPolicy-FS-2018-06为FS-2018-06。

安全策略	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
TLS 协议						
Protocol-TLSv1	✓					✓
Protocol-TLSv1.1	✓				✓	✓

## 安全策略

	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
Protocol-TLSv1.2	✓	✓	✓	✓	✓	✓
TLS 密码						
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓		✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓		✓	✓	✓	✓

安全策略	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE- ECDSA- AES128- SHA	✓			✓	✓	✓
ECDHE- RSA- AES128-S HA	✓			✓	✓	✓
ECDHE- ECDSA- AES256 - GCM- SHA384	✓	✓	✓	✓	✓	✓
ECDHE- RSA- AES256- GCM- SHA384	✓	✓	✓	✓	✓	✓
ECDHE- ECDSA- AES256- SHA384	✓		✓	✓	✓	✓



安全策略	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-RSA-AES256-SHA384	✓		✓	✓	✓	✓
ECDHE-RSA-AES256-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-SHA	✓			✓	✓	✓
AES128-GCM-SHA256	✓					
AES128-SHA256	✓					
AES128-SHA	✓					
AES256-GCM-SHA384	✓					

安全策略	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
AES256-SHA256	✓					
AES256-SHA	✓					

使用 CLI 创建使用 FS 支持策略的 TLS 侦听器

将 [create-listener](#) 命令与任何 [FS 支持的安全策略](#) 一起使用。

该示例使用ELBSecurityPolicy-FS-2018-06安全策略。

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

使用 CLI 修改 TLS 侦听器以使用 FS 支持的策略

将 [modify-listener](#) 命令与任何 [FS 支持的安全策略](#) 一起使用。

该示例使用ELBSecurityPolicy-FS-2018-06安全策略。

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

使用 CLI 查看侦听器使用的安全策略

将 [describe-listener](#) 命令与你的 [侦听器](#) 配合使用arn。

```
aws elbv2 describe-listener \
```

```
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

使用 CLI 查看 FS 支持的安全策略的配置

将该[describe-ssl-policies](#)命令与任何 [FS 支持的安全策略](#) 一起使用。

该示例使用ELBSecurityPolicy-FS-2018-06安全策略。

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-FS-2018-06
```

## TLS 1.0 - 1.2

下表描述了可用的 TLS 1.0-1.2 安全策略支持的 TLS 协议和密码。

注意：该ELBSecurityPolicy-前缀已从安全策略行的策略名称中删除。

示例：安全策略显示ELBSecurityPolicy-TLS-1-2-Ext-2018-06为TLS-1-2-Ext-2018-06。

安全策略	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
TLS 协议					
Protocol-TLSv1	✓				✓
Protocol-TLSv1.1	✓			✓	✓
Protocol-TLSv1.2	✓	✓	✓	✓	✓

安全策略	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
TLS 密码					
ECDHE-ECD SA-AES128- GCM-SHA256	✓	✓	✓	✓	✓
ECDHE-RSA -AES128- GCM-SHA256	✓	✓	✓	✓	✓
ECDHE-ECD SA-AES128- SHA256	✓	✓	✓	✓	✓
ECDHE-RSA -AES128-S HA256	✓	✓	✓	✓	✓
ECDHE-ECD SA-AES128- SHA	✓	✓		✓	✓
ECDHE-RSA -AES128-S HA	✓	✓		✓	✓

安全策略	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
ECDHE-ECD SA-AES256- GCM-SHA384	✓	✓	✓	✓	✓
ECDHE-RSA -AES256- GCM-SHA384	✓	✓	✓	✓	✓
ECDHE-ECD SA-AES256- SHA384	✓	✓	✓	✓	✓
ECDHE-RSA -AES256-S HA384	✓	✓	✓	✓	✓
ECDHE-RSA -AES256-S HA	✓	✓		✓	✓
ECDHE-ECD SA-AES256- SHA	✓	✓		✓	✓
AES128-GC M-SHA256	✓	✓	✓	✓	✓

安全策略	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
AES128-SH A256	✓	✓	✓	✓	✓
AES128-SH A	✓	✓		✓	✓
AES256-GC M-SHA384	✓	✓	✓	✓	✓
AES256-SH A256	✓	✓	✓	✓	✓
AES256-SH A	✓	✓		✓	✓
DES-CBC3- SHA					✓

\* 除非您必须支持需要 DES-CBC3-SHA 密码（这是一种弱密码）的旧客户端，否则请勿使用此策略。

使用 CLI 创建使用 TLS 1.0-1.2 策略的 TLS 侦听器

将 [create-listener](#) 命令与任何 [TLS 1.0-1.2](#) 支持的安全策略一起使用。

该示例使用 ELBSecurityPolicy-2016-08 安全策略。

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-2016-08
```

使用 CLI 修改 TLS 侦听器以使用 TLS 1.0-1.2 策略

将 `modify-listener` 命令与任何 [TLS 1.0-1.2 支持的安全策略](#) 一起使用。

该示例使用 `ELBSecurityPolicy-2016-08` 安全策略。

```
aws elbv2 modify-listener \  
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \  
--ssl-policy ELBSecurityPolicy-2016-08
```

使用 CLI 查看侦听器使用的安全策略

将 `describe-listener` 命令与你的侦听器配合使用 `arn`。

```
aws elbv2 describe-listener \  
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

使用 CLI 查看 TLS 1.0-1.2 安全策略的配置

将该 `describe-ssl-policies` 命令与任何 [TLS 1.0-1.2 支持的安全策略](#) 一起使用。

该示例使用 `ELBSecurityPolicy-2016-08` 安全策略。

```
aws elbv2 describe-ssl-policies \  
--names ELBSecurityPolicy-2016-08
```

## ALPN 策略

应用层协议协商 (ALPN) 是在最初的 TLS 握手 hello 消息上发送的 TLS 扩展。通过 ALPN，应用层能够协商应在安全连接（例如 HTTP/1 和 HTTP/2）上使用什么协议。

当客户端启动 ALPN 连接时，负载均衡器将客户端 ALPN 首选项列表与其 ALPN 策略进行比较。如果客户端支持来自 ALPN 策略的协议，则负载均衡器会根据 ALPN 策略的首选项列表建立连接。否则，负载均衡器不使用 ALPN。

支持的 ALPN 策略

以下是支持的 ALPN 策略：

## HTTP10nly

仅协商 HTTP/1.\*。ALPN 首选项列表为 http/1.1、http/1.0。

## HTTP20nly

仅协商 HTTP/2。ALPN 首选项列表为 h2。

## HTTP20ptional

首选 HTTP/1.\* 而不是 HTTP/2 ( 这对 HTTP/2 测试非常有用 )。ALPN 首选项列表为 http/1.1、http/1.0、h2。

## HTTP2Preferred

首选 HTTP/2 而不是 HTTP/1.\*。ALPN 首选项列表为 h2、http/1.1、http/1.0。

## None

不协商 PN。这是默认模式。

## 启用 ALPN 连接

您可以在创建或修改 TLS 侦听器时启用 ALPN 连接。有关更多信息，请参阅 [添加侦听器](#) 和 [更新 ALPN 策略](#)。

## 更新网络负载均衡器的侦听器

您可以更新侦听器协议、侦听器端口或从转发操作接收流量的目标组。默认操作 ( 也称为默认规则 ) 会将请求转发到选定的目标组。

如果您将协议从 TCP 更改为 UDP 或 TLS，则必须指定安全策略和服务器证书。如果您将协议从 TLS 更改为 TCP 或 UDP，则将删除安全策略和服务器证书。

当侦听器默认操作的目标组更新时，新连接将路由到新配置的目标组。但是，这不影响在此更改之前创建的任何活动连接。如果正在发送流量，则这些活动连接会与原始目标组中的目标保持关联长达一个小时；如果未发送流量，则保持关联的最长时间为空闲超时期，以先发生者为准。更新侦听器时未应用参数 `Connection termination on deregistration`，因为在取消注册目标时应用此参数。

## 使用控制台更新侦听器

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。



3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在侦听器选项卡上，选择协议:端口列中的文本以打开侦听器的详细信息页面。
5. 选择编辑。
6. (可选) 根据需要更改协议和端口的特定值。
7. (可选) 为默认操作选择不同的目标组。
8. (可选) 根据需要添加、更新或删除标签。
9. 选择保存更改。

要更新您的听众，请使用 AWS CLI

使用 [modify-listener](#) 命令。

## 更新网络负载均衡器的 TLS 侦听器

创建 TLS 侦听器后，您可以替换默认证书、在证书列表中添加或删除证书、更新安全策略或更新 ALPN 策略。

### 任务

- [替换默认证书](#)
- [将证书添加到证书列表](#)
- [从证书列表中删除证书](#)
- [更新安全策略](#)
- [更新 ALPN 策略](#)

## 替换默认证书

您可以使用以下过程替换 TLS 侦听器的默认证书。有关更多信息，请参阅 [默认证书](#)。

### 使用控制台替换默认证书

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在侦听器选项卡上，选择协议:端口列中的文本以打开侦听器的详细信息页面。

- 对于默认 SSL 证书，请执行下列操作之一：
  - 如果您使用创建或导入了证书 AWS Certificate Manager，请选择 From ACM 并选择证书。
  - 如果使用 IAM 上传了证书，则选择从 IAM 并选择证书。
- 选择保存更改。

要使用替换默认证书 AWS CLI

将 [modify-listener](#) 命令与 --certificates 选项一起使用。

## 将证书添加到证书列表

您可使用以下过程将证书添加到侦听器的证书列表。首次创建 TLS 侦听器时，证书列表为空。可以添加一个或多个证书。您可以选择添加默认证书，以确保此证书与 SNI 协议一起使用，即使它被替换为默认证书也是如此。有关更多信息，请参阅 [证书列表](#)。

使用控制台将证书添加到证书列表

- 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
- 在导航窗格中，选择负载均衡器。
- 选择负载均衡器的名称以打开其详细信息页面。
- 在侦听器选项卡上，选择协议:端口列中的文本以打开侦听器的详细信息页面。
- 选中侦听器对应的复选框，然后选择操作、添加 SNI 的 SSL 证书。
- 要添加已由 ACM 或 IAM 管理的证书，请选中证书对应的复选框并选择在下面以待注册的形式添加。
- 如果您有一个未由 ACM 或 IAM 管理的证书，则选择导入证书，完成表格，然后选择导入。
- 选择添加待处理证书。

要将证书添加到证书列表中，请使用 AWS CLI

使用 [add-listener-certificates](#) 命令。

## 从证书列表中删除证书

您可以使用以下过程从 TLS 侦听器的证书列表中删除证书。要删除 TLS 侦听器的默认证书，请参阅 [替换默认证书](#)。

## 使用控制台从证书列表中删除证书

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在侦听器选项卡上，选择协议:端口列中的文本以打开侦听器的详细信息页面。
5. 选中侦听器对应的复选框，然后选择操作、添加 SNI 的 SSL 证书。
6. 选中证书对应的复选框，然后选择删除。
7. 提示进行确认时，输入 **confirm**，然后选择移除。

要从证书列表中删除证书，请使用 AWS CLI

使用 [remove-listener-certificates](#) 命令。

## 更新安全策略

在创建 TLS 侦听器时，您可以选择满足您的需求的安全策略。添加新的安全策略后，您可以将 TLS 侦听器更新为使用此新安全策略。网络负载均衡器不支持自定义安全策略。有关更多信息，请参阅 [安全策略](#)。

使用控制台更新安全策略

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在侦听器选项卡上，选择协议:端口列中的文本以打开侦听器的详细信息页面。
5. 选择编辑。
6. 对于安全策略，选择安全策略。
7. 选择保存更改。

要更新安全策略，请使用 AWS CLI

将 [modify-listener](#) 命令与 `--ssl-policy` 选项一起使用。

## 更新 ALPN 策略

您可以使用以下过程更新 TLS 侦听器的 ALPN 策略。有关更多信息，请参阅 [ALPN 策略](#)。

## 使用控制台更新 ALPN 策略

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在侦听器选项卡上，选择协议:端口列中的文本以打开侦听器的详细信息页面。
5. 选择编辑。
6. 对于 ALPN 策略，请选择一个策略以启用 ALPN，或选择无以禁用 ALPN。
7. 选择保存更改。

要更新 ALPN 政策，请使用 AWS CLI

将 [modify-listener](#) 命令与 `--alpn-policy` 选项一起使用。

## 删除网络负载均衡器的侦听器

可以随时删除侦听器。

使用控制台删除侦听器

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选中负载均衡器对应的复选框。
4. 在侦听器选项卡上，选中侦听器对应的复选框，然后依次选择操作、删除侦听器。
5. 如果提示进行确认，输入 **confirm**，并选择删除。

要删除监听器，请使用 AWS CLI

使用 [delete-listener](#) 命令。

# Network Load Balancer 的目标组

每个目标组均用于将请求路由到一个或多个已注册的目标。创建侦听器时，您为其默认操作指定目标组。流量将转发到在侦听器规则中指定的目标组。您可以为不同类型的请求创建不同的目标组。例如，为一般请求创建一个目标组，为应用程序的微服务请求创建其他目标组。有关更多信息，请参阅 [网络负载均衡器组件](#)。

您基于每个目标组定义负载均衡器的运行状况检查设置。每个目标组均使用默认运行状况检查设置，除非您在创建目标组时将其覆盖或稍后对其进行修改。在侦听器规则中指定一个目标组后，负载均衡器将持续监控已注册到该目标组的所有目标（这些目标位于已为负载均衡器启用的可用区中）的运行状况。负载均衡器将请求路由到正常运行的已注册目标。有关更多信息，请参阅 [目标组的运行状况检查](#)。

## 目录

- [路由配置](#)
- [Target type](#)
- [IP 地址类型](#)
- [已注册目标](#)
- [目标组属性](#)
- [客户端 IP 保留](#)
- [取消注册延迟](#)
- [代理协议](#)
- [粘性会话](#)
- [为 Network Load Balancer 创建目标组](#)
- [目标组的运行状况检查](#)
- [目标组的跨区域负载均衡](#)
- [目标组运行状况](#)
- [向您的目标组注册目标](#)
- [作为目标的 Application Load Balancer](#)
- [适用于目标组的标签](#)
- [删除目标组](#)

## 路由配置

默认情况下，负载均衡器会使用您在创建目标组时指定的协议和端口号将请求路由到其目标。此外，您可以覆盖在将目标注册到目标组时用于将流量路由到目标的端口。

Network Load Balancer 的目标组支持以下协议和端口：

- 协议：TCP、TLS、UDP TCP\_UDP
- 端口：1-65535

如果目标组使用 TLS 协议配置，则负载均衡器将使用您在目标上安装的证书与目标建立 TLS 连接。负载均衡器不验证这些证书。因此，您可以使用自签名证书或已过期的证书。由于负载均衡器位于虚拟私有云 (VPC) 中，因此负载均衡器与目标之间的流量将在数据包级别进行身份验证，因此即使目标上的证书无效，也不会面临 man-in-the-middle 攻击或欺骗的风险。

下表总结了侦听器协议和目标组设置的组合。

侦听器协议	目标组协议	目标组类型	运行状况检查协议
TCP	TCP   TCP_UDP	实例   ip	HTTP   HTTPS   TCP
TCP	TCP	alb	HTTP   HTTPS
TLS	TCP   TLS	实例   ip	HTTP   HTTPS   TCP
UDP	UDP   TCP_UDP	实例   ip	HTTP   HTTPS   TCP
TCP_UDP	TCP_UDP	实例   ip	HTTP   HTTPS   TCP

## Target type

在创建目标组时，应指定其目标类型，这决定您如何指定其目标。创建目标组后，您无法更改其目标类型。

以下是可能的目标类型：

`instance`

这些目标通过实例 ID 指定。

## ip

这些目标通过 IP 地址指定。

## alb

目标是 Application Load Balancer。

当目标类型为 ip 时，您可以指定来自以下 CIDR 块之一的 IP 地址：

- 目标组的 VPC 的子网
- 10.0.0.0/8 ([RFC 1918](#))
- 100.64.0.0/10 ([RFC 6598](#))
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

### Important

不能指定可公开路由的 IP 地址。

您可以使用所有支持的 CIDR 块，向目标组注册以下目标：

- AWS 可通过 IP 地址和端口寻址的资源（例如数据库）。
- AWS 通过 AWS Direct Connect 或点对点 VPN 连接链接的本地资源。

为您的目标组禁用客户端 IP 保留后，针对网络负载均衡器 IP 地址和唯一目标（IP 地址和端口）的组合，负载均衡器可支持每分钟约 5.5 万个连接。如果连接数超过该值，则会增大出现端口分配错误的几率。如果您收到端口分配错误，请将多个目标添加到目标组。

在共享 Amazon VPC 中启动 Network Load Balancer 时（作为参与者），您只能在已共享的子网中注册目标。

当目标类型为 alb 时，您可以将单个 Application Load Balancer 注册为目标。有关更多信息，请参阅 [作为目标的 Application Load Balancer](#)。

Network Load Balancer 不支持 lambda 目标类型。Application Load Balancer 是支持 lambda 目标类型的唯一负载均衡器。有关更多信息，请参阅应用程序负载均衡器用户指南中的 [Lambda 函数作为目标](#)。

如果在向网络负载均衡器注册的实例中存在微服务，则不能使用负载均衡器在这些服务之间提供通信，除非该负载均衡器是面向互联网的，或者实例是通过 IP 地址注册的。有关更多信息，请参阅 [从目标到其负载均衡器的请求连接超时](#)。

## 请求路由和 IP 地址

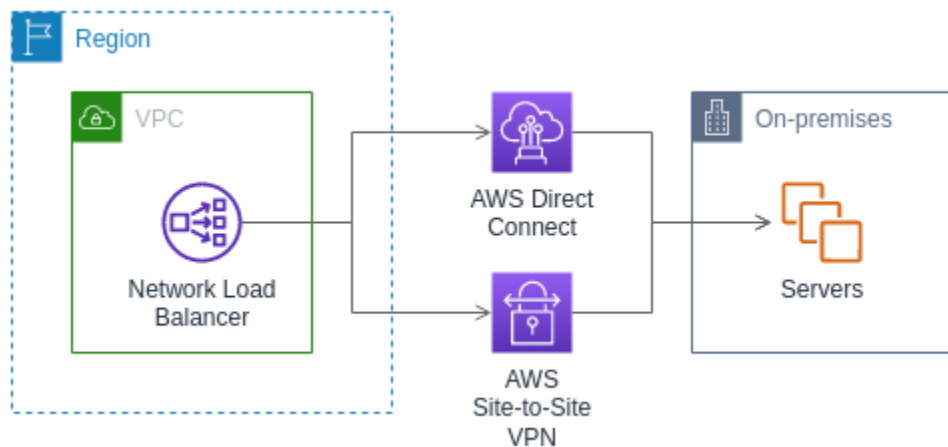
如果使用实例 ID 指定目标，则使用实例的主网络接口中指定的主私有 IP 地址将流量路由到实例。负载均衡器在将数据包转发到目标实例之前重写目的地 IP 地址。

如果使用 IP 地址指定目标，则可以使用来自一个或多个网络接口的任何私有 IP 地址将流量路由到实例。这使一个实例上的多个应用程序可以使用同一端口。请注意，每个网络接口都可以有自己的安全组。负载均衡器在将数据包转发到目标之前重写目的地 IP 地址。

有关允许实例的流量的更多信息，请参阅 [目标安全组](#)。

## 将本地资源作为目标

当目标类型为 `ip` 时，通过链接的本地资源 AWS Direct Connect 或站点到站点 VPN 连接可以作为目标。



使用本地资源时，这些目标的 IP 地址必须仍来自下列 CIDR 块之一：

- 10.0.0.0/8 ([RFC 1918](#))
- 100.64.0.0/10 ([RFC 6598](#))
- 172.16.0.0/12 ([RFC 1918](#))



- 192.168.0.0/16 (RFC 1918)

有关的更多信息 AWS Direct Connect，请参阅[什么是 AWS Direct Connect？](#)

有关的更多信息 AWS Site-to-Site VPN，请参阅[什么是 AWS Site-to-Site VPN？](#)

## IP 地址类型

创建新目标组时，可以选择目标组的 IP 地址类型。此 IP 地址控制用于与目标进行通信并检查其运行状况的 IP 版本。

Network Load Balancer 支持 IPv4 和 IPv6 目标组。默认选择为 IPv4。IPv6 目标组只能与双堆栈网络负载均衡器关联。

### 注意事项

- 目标组中的所有 IP 地址均必须具有相同的 IP 地址类型。例如，您无法向 IPv6 目标组注册 IPv4 目标。
- IPv6 目标组只能用于具有 TCP 或 TLS 侦听器的 dualstack 负载均衡器。
- IPv6 目标组支持 IP 和实例类型目标。

## 已注册目标

您的负载均衡器充当客户端的单一接触点，并跨其正常运行的已注册目标分发传入流量。每个目标组在为负载均衡器启用的每个可用区中必须至少有一个已注册目标。您可以将每个目标注册到一个或多个目标组中。

如果应用程序需求增加，您可以向一个或多个目标组注册其他目标以便满足该需求。无论配置的阈值如何，只要注册过程完成并且目标通过了第一次初始运行状况检查，负载均衡器就会开始将流量路由到新注册的目标。

如果应用程序需求减少或者您需要为目标提供服务，您可以从目标组取消注册目标。取消注册目标将从目标组中删除目标，但不会影响目标。一旦取消注册，负载均衡器就会停止将流量路由到目标。目标将进入 draining 状态，直至进行中请求完成。当您准备好恢复接收流量时，可以再次向目标组注册目标。

如果要通过实例 ID 来注册目标，则可以将负载均衡器与 Auto Scaling 组一同使用。将一个目标组挂接到 Auto Scaling 组后，Auto Scaling 在启动目标时会为您向该目标组注册目标。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的[将负载均衡器挂接到 Auto Scaling 组](#)。

## 要求和注意事项

- 如果实例采用以下实例类型，则不能利用实例 ID 注册实例：  
C1、CC1、CC2、CG1、CG2、CR1、G1、G2、H11、HS1、M1、M2、M3 或 T1。
- 当按实例 ID 为 IPv6 目标组注册目标时，必须为目标分配主 IPv6 地址。要了解更多信息，请参阅 Amazon EC2 用户指南中的 [IPv6 地址](#)
- 按实例 ID 注册目标时，实例必须与网络负载均衡器位于同一个 Amazon VPC 中。如果实例所在的 VPC 与负载均衡器 VPC 是对等的（位于同一区域或不同区域），则不能按实例 ID 注册实例。可以用 IP 地址注册这些实例。
- 如果您按 IP 地址注册目标，并且该 IP 地址与负载均衡器位于同一 VPC 中，则负载均衡器会验证其是否来自可以访问的子网。
- 负载均衡器仅将流量路由到已启用的可用区中的目标。未启用的区域中的目标未使用。
- 对于 UDP 和 TCP\_UDP 目标组，如果实例位于负载均衡器 VPC 之外，或者采用以下实例类型之一，则不要用 IP 地址注册实例：  
C1、CC1、CC2、CG1、CG2、CR1、G1、G2、H11、HS1、M1、M2、M3 或 T1。如果目标驻留在负载均衡器 VPC 之外或者采用不受支持的实例类型，则目标可能能够接收来自负载均衡器的流量，但随后无法响应。

## 目标组属性

支持以下目标组属性。只有当目标组类型为 `instance` 或 `ip` 时，才能修改这些属性。如果目标组类型为 `alb`，则这些属性将始终使用其默认值。

### `deregistration_delay.timeout_seconds`

Elastic Load Balancing 在将取消注册目标的状态从 `draining` 更改为 `unused` 之前需等待的时间。范围为 0-3600 秒。默认值为 300 秒。

### `deregistration_delay.connection_termination.enabled`

指示负载均衡器是否在取消注册超时结束时终止连接。该值为 `true` 或 `false`。对于新的 UDP/TCP\_UDP 目标组，默认值为 `true`。否则，默认值为 `false`。

### `load_balancing.cross_zone.enabled`

指示是否启用了跨区域负载均衡。该值为 `true`、`false` 或 `use_load_balancer_configuration`。默认为 `use_load_balancer_configuration`。

## `preserve_client_ip.enabled`

指示是否启用客户端 IP 保留。该值为 `true` 或 `false`。如果目标组类型为 IP 地址且目标组协议是 TCP 或 TLS，则默认处于禁用状态。否则，默认处于启用状态。无法为 UDP 和 TCP\_UDP 目标组禁用客户端 IP 保留。

## `proxy_protocol_v2.enabled`

指示是否已启用代理协议版本 2。默认情况下，禁用代理协议。

## `stickiness.enabled`

指示是否启用粘性会话。

## `stickiness.type`

粘性的类型。可能的值为 `source_ip`。

## `target_group_health.dns_failover.minimum_healthy_targets.count`

必须运行状况良好的目标数量下限。如果运行状况良好的目标数量低于此值，请在 DNS 中将该区域标记为运行状况不佳，以便流量仅路由到运行状况良好的区域。可能的值是 `off` 或 1 到目标数量上限之间的整数。当 `off` 时，DNS 故障转移被禁用，这意味着每个目标组都独立地为 DNS 故障转移做出贡献。默认为 1。

## `target_group_health.dns_failover.minimum_healthy_targets.percentage`

必须运行状况良好的目标最低百分比。如果运行状况良好的目标百分比低于此值，请在 DNS 中将该区域标记为运行状况不佳，以便流量仅路由到运行状况良好的区域。可能的值为 `off` 或者 1 到 100 之间的整数。当 `off` 时，DNS 故障转移被禁用，这意味着每个目标组都独立地为 DNS 故障转移做出贡献。默认为 1。

## `target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

必须运行状况良好的目标数量下限。如果运行状况良好的目标数量低于此值，则将流量发送到所有目标（包括运行状况不佳的目标）。范围为 1 到目标数量上限。默认为 1。

## `target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

必须运行状况良好的目标最低百分比。如果运行状况良好的目标百分比低于此值，则将流量发送到所有目标（包括运行状况不佳的目标）。可能的值为 `off` 或者 1 到 100 之间的整数。默认值为 `off`。

## `target_health_state.unhealthy.connection_termination.enabled`

指示负载均衡器是否终止与运行状况不佳的目标的连接。该值为 `true` 或 `false`。默认为 `true`。

## target\_health\_state.unhealthy.draining\_interval\_seconds

Elastic Load Balancing 在将运行状况不佳的目标的状态从unhealthy.draining更改为之前等待的时间。unhealthy范围为 0-36000 秒。默认值为 0 秒。

注意：只有在为  
时target\_health\_state.unhealthy.connection\_termination.enabled才能配置此属性false。

## 客户端 IP 保留

在将请求路由到后端目标时，Network Load Balancer 可以保留客户端的源 IP 地址。禁用客户端 IP 保留时，网络负载均衡器的私有 IP 地址将成为所有传入流量的客户端 IP 地址。

默认情况下，对于使用 UDP 和 TCP\_UDP 协议的实例和 IP 类型目标组，客户端 IP 保留处于启用状态（且不能禁用）。但您可以使用 preserve\_client\_ip.enabled 目标组属性为 TCP 和 TLS 目标组启用或禁用客户端 IP 保留。

### 默认设置

- 实例类型目标组：已启用
- IP 类型目标组（UDP、TCP\_UDP）：已启用
- IP 类型目标组（TCP、TLS）：已禁用

### 要求和注意事项

- 启用客户端 IP 保留后，目标必须与网络负载均衡器位于同一 VPC 中，并且流量必须直接从网络负载均衡器流向目标。
- 使用网关负载均衡器端点检查网络负载均衡器和目标（实例或 IP）之间的流量时，即使目标与网络负载均衡器位于同一个 Amazon VPC 中，也不支持客户端 IP 保留。
- 以下实例类型不支持客户端 IP 保留：  
C1、CC1、CC2、CG1、CG2、CR1、G1、G2、H1、HS1、M1、M2、M3 和 T1。我们建议您在禁用客户端 IP 保留的情况下将这些实例类型注册为 IP 地址。
- 客户端 IP 保留对来自的入站流量没有影响 AWS PrivateLink。AWS PrivateLink 流量的源 IP 始终是 Network Load Balancer 的私有 IP 地址。
- 当目标组包含 AWS PrivateLink ENI 或其他网络负载均衡器的 ENI 时，不支持保留客户端 IP。这将导致与那些目标的通信中断。

- 客户端 IP 保留对于从 IPv6 转换为 IPv4 的流量没有影响。此类型流量的源 IP 始终是 Network Load Balancer 的私有 IP 地址。
- 当您按 Application Load Balancer 类型指定目标时，Network Load Balancer 将保留所有传入流量的客户端 IP 并发送到 Application Load Balancer。然后，Application Load Balancer 会将客户端 IP 附加到 X-Forwarded-For 请求标头，之后才发送此请求标头。
- 客户端 IP 保留更改仅对新的 TCP 连接生效。
- 启用客户端 IP 保留后，不支持 NAT 环回（也称为发夹转换）。启用后，您可能会遇到与目标上观察到的套接字重用相关的 TCP/IP 连接限制。如果客户端或客户端前面的 NAT 设备在同时连接到多个负载均衡器节点时使用相同的源 IP 地址和源端口，则可能会出现这些连接限制。如果负载均衡器将这些连接路由到同一个目标，则这些连接对目标来说似乎是来自同一源套接字，从而导致连接错误。当发生这种情况时，客户端可能会重试（如果连接失败）或重新连接（如果连接中断）。您可以通过增加源临时端口的数量或增加负载均衡器的目标数来减少此类连接错误。您可以通过禁用客户端 IP 保留或禁用跨区域负载均衡来防止此类连接错误。
- 当禁用客户端 IP 保留时，网络负载均衡器支持到每个唯一目标（IP 地址和端口）的 5.5 万个并发连接或每分钟大约 5.5 万个连接。如果连接数超过该值，则会增大出现端口分配错误的几率，进而导致无法建立新连接。可以使用 PortAllocationErrorCount 指标跟踪端口分配错误。要修复端口分配错误，请将更多目标添加到目标组。有关更多信息，请参阅 [CloudWatch 您的 Network Load Balancer 的指标](#)。

### 使用控制台配置客户端 IP 保留

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Attributes（属性）选项卡上，选择 Edit（编辑）。
5. 要启用客户端 IP 保留，请开启 Preserve client IP addresses（保留客户端 IP 地址）。要禁用客户端 IP 保留，请关闭 Preserve client IP addresses（保留客户端 IP 地址）。
6. 选择保存更改。

要启用或禁用客户端 IP 保留，请使用 AWS CLI

使用带 `preserve_client_ip.enabled` 属性的 [modify-target-group-attributes](#) 命令。

例如，使用以下命令禁用客户端 IP 保留。

```
aws elbv2 modify-target-group-attributes --attributes
Key=preserve_client_ip.enabled,Value=false --target-group-arn ARN
```

您的输出应类似于以下示例。

```
{
  "Attributes": [
    {
      "Key": "proxy_protocol_v2.enabled",
      "Value": "false"
    },
    {
      "Key": "preserve_client_ip.enabled",
      "Value": "false"
    },
    {
      "Key": "deregistration_delay.timeout_seconds",
      "Value": "300"
    }
  ]
}
```

## 取消注册延迟

取消注册目标时，负载均衡器将停止创建与目标的新连接。负载均衡器会使用连接耗尽来确保进行中的流量在现有连接上完成。如果已经取消注册的目标运行状况良好并且现有连接未处于空闲状态，负载均衡器可以继续将流量发送到该目标。要确保现有连接关闭，您可以执行以下任一操作：为连接终止启用目标组属性、确保在取消注册之前实例运行状况不佳或者定期关闭客户端连接。

取消注册的目标的初始状态为 `draining`。默认情况下，负载均衡器会在 300 秒后将取消注册的目标的状态更改为 `unused`。如需更改负载均衡器在将取消注册的目标的状态更改为 `unused` 之前等待的时长，请更新取消注册延迟值。我们建议您指定至少 120 秒的值以确保完成请求。

如果为连接终止启用目标组属性，则对取消注册目标的连接将在取消注册超时结束后不久关闭。

使用控制台更新取消注册属性

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。

4. 在 Attributes ( 属性 ) 选项卡上, 选择 Edit ( 编辑 )。
5. 要更改取消注册超时, 请在 Deregistration delay 中输入新值。要确保在取消注册目标后现有连接关闭, 请选择 Terminate connections on deregistration ( 取消注册时终止连接 )。
6. 选择保存更改。

要更新取消注册属性, 请使用 AWS CLI

使用 [modify-target-group-attributes](#) 命令。

## 代理协议

Network Load Balancer 使用代理协议版本 2 来发送其他连接信息, 如源和目标。代理协议版本 2 提供代理协议标头的二进制编码。对于 TCP 侦听器, 负载均衡器会将代理协议标头预添加到 TCP 数据中。它不会丢弃或覆盖任何现有数据, 包括客户端或网络路径中的任何其他代理、负载均衡器或服务器发送的任何传入代理协议标头。因此, 可以接收多个代理协议标头。此外, 如果您的 Network Load Balancer 之外的目标还有另一个网络路径, 则第一个代理协议标头可能不是您的 Network Load Balancer 中的标头。

如果您使用 IP 地址指定目标, 则向您的应用程序提供的源 IP 地址取决于目标组的协议, 如下所示:

- TCP 和 TLS: 源 IP 地址是负载均衡器节点的私有 IP 地址。如果您需要客户端的 IP 地址, 请启用代理协议并从代理协议标头获取客户端 IP 地址。
- UDP 和 TCP\_UDP: 源 IP 地址是客户端的 IP 地址。

如果您通过实例 ID 指定目标, 则提供给应用程序的源 IP 地址将是客户端 IP 地址。但是, 如果您愿意, 可以启用代理协议并从代理协议标头中获取客户端 IP 地址。

### Note

TLS 侦听器不支持带有客户端或任何其他代理发送的代理协议标头的传入连接。

## 运行状况检查连接

启用代理协议后, 代理协议标头也会包含在来自负载均衡器的运行状况检查连接中。但是, 使用运行状况检查连接, 客户端连接信息不会在代理协议标头中发送。

## VPC 终端节点服务

对于来自服务使用者并通过 [VPC 终端节点服务](#) 的流量，提供给您的应用程序的源 IP 地址是负载均衡器节点的私有 IP 地址。如果您的应用程序需要服务使用器的 IP 地址，请启用代理协议并从代理协议标头获取这些 IP 地址。

代理协议标头还包括终端节点的 ID。此信息使用自定义类型-长度-值 (TLV) 向量进行编码，如下所示。

字段	长度 (8 位字节)	描述
Type	1	PP2_TYPE_AWS (0xEA)
Length	2	值的长度
值	1	PP2_SUBTYPE_AWS_VPCE_ID (0x01)
	可变 (值长度减 1)	终端节点的 ID

有关解析 TLV 类型 0xEA 的示例，请参阅 <https://github.com/aws/elastic-load-balancing-tools/tree/master/proprot>。

## 启用代理协议

在目标组上启用代理协议之前，请确保您的应用程序预料到并且可以解析代理协议版本 2 标头，否则它们可能会失败。有关更多信息，请参阅[代理协议版本 1 和 2](#)。

使用控制台启用代理协议版本 2

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Attributes (属性) 选项卡上，选择 Edit (编辑)。
5. 在编辑属性页面上，选择代理协议 v2。
6. 选择保存更改。

要启用代理协议 v2，请使用 AWS CLI

使用 [modify-target-group-attributes](#) 命令。



## 粘性会话

粘性会话是用于将客户端流量传输到目标组中的同一目标的机制。对于维护状态信息以便向客户端提供持续体验的服务器来说，这很有用。

### 注意事项

- 使用粘性会话可能会导致连接和流分布不均，这可能会影响目标的可用性。例如，相同 NAT 设备背后的所有客户端都具有相同的源 IP 地址。这会使系统将来自这些客户端的所有流量传输到同一目标。
- 如果目标组中的任何目标的运行状况发生变化，或者您向目标组注册或取消注册了目标，则负载均衡器可能会重置该目标组的粘性会话。
- 当为目标群组开启粘性属性时，不支持被动健康检查。有关更多信息，请参阅[目标群体的健康检查](#)。
- TLS 侦听器不支持粘滞会话。

### 使用控制台启用粘性会话

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Attributes ( 属性 ) 选项卡上，选择 Edit ( 编辑 ) 。
5. 在 Target selection configuration ( 目标选择配置 ) 下，开启 Stickiness ( 粘性 ) 。
6. 选择保存更改。

要启用粘性会话，请使用 AWS CLI

使用带 `stickiness.enabled` 属性的 [modify-target-group-attributes](#) 命令。

## 为 Network Load Balancer 创建目标组

为网络负载均衡器向目标组注册目标。默认情况下，负载均衡器使用您为目标组指定的端口和协议将请求发送到已注册目标。在将每个目标注册到目标组时，可以覆盖此端口。

在创建目标组后，您可以添加标签。

要将流量路由到目标组中的目标，请创建侦听器，并在侦听器的默认操作中指定目标组。有关更多信息，请参阅[侦听器规则](#)。您可以在多个侦听器中指定同一个目标组，但这些侦听器必须属于同一个

Network Load Balancer。要将目标组与负载均衡器结合使用，您必须确认目标组没有被任何其他负载均衡器的侦听器使用。

您可以随时在目标组中添加或删除目标。有关更多信息，请参阅 [向您的目标组注册目标](#)。您也可以修改目标组的运行状况检查设置。有关更多信息，请参阅 [修改目标组的运行状况检查设置](#)。

### 使用控制台创建目标组

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择目标组。
3. 选择创建目标组。
4. 在基本配置窗格中执行以下操作：
  - a. 对于 Choose a target type (选择目标类型)，选择 Instance (实例) 以按实例 ID 注册目标，选择 IP addresses (IP 地址) 以按 IP 地址注册目标，或者选择 Application Load Balancer (应用程序负载均衡器) 以将某个应用程序负载均衡器注册为目标。
  - b. 对于目标组名称，输入目标组的名称。此名称在每个区域的每个账户中必须唯一，最多可以有 32 个字符，只能包含字母数字字符或连字符，不得以连字符开头或结尾。
  - c. 对于 Protocol (协议)，选择协议，如下所示：
    - 如果侦听器协议为 TCP，选择 TCP 或 TCP\_UDP。
    - 如果侦听器协议为 TLS，选择 TCP 或 TLS。
    - 如果侦听器协议为 UDP，选择 UDP 或 TCP\_UDP。
    - 如果侦听器协议为 TCP\_UDP，选择 TCP\_UDP。
  - d. (可选) 对于端口，请根据需要修改默认值。
  - e. 对于 IP 地址类型，选择 IPv4 或 IPv6。此选项仅在目标类型为实例或 IP 地址且协议是 TCP 或 TLS 时可用。

您必须将一个 IPv6 目标组关联到一个双堆栈负载均衡器。目标组中的所有目标必须具有相同的 IP 地址类型。在创建目标组后，您将无法更改 IP 地址类型。
  - f. 对于 VPC，选择具有要注册的目标的虚拟私有云 (VPC)。
5. 对于运行状况检查窗格，根据需要修改默认设置。对于高级运行状况检查，选择运行状况检查端口、计数、超时、间隔并指定成功代码。如果运行状况检查连续超过不正常运行阈值计数，负载均衡器将使目标停止服务。如果运行状况检查连续超过运行状况正常阈值计数，负载均衡器将使目标恢复使用。有关更多信息，请参阅 [目标组的运行状况检查](#)。
6. (可选) 要添加标签，请展开标签，选择添加标签，然后输入标签键和标签值。

7. 选择下一步。
8. 在注册目标页面中，按如下方式添加一个或多个目标：
  - 如果目标类型为实例，请选择实例，输入端口，然后选择在下面以待注册的形式添加。  
  
注意：实例必须具有分配的主 IPv6 地址，才能向 IPv6 目标组注册。
  - 如果目标类型为 IP 地址，请选择网络，输入 IP 地址和端口，然后选择在下面以待注册的形式添加。
9. 选择创建目标组。

要创建目标群组，请使用 AWS CLI

使用 [create-target-group](#) 命令创建目标组，使用 [add-tags](#) 命令标记目标组，使用 [register-targets](#) 命令添加目标。

## 目标组的运行状况检查

您可以将目标注册到一个或多个目标组中。一旦注册过程完成，负载均衡器就会开始将请求路由到新注册的目标。完成注册过程和开始运行状况检查可能需要几分钟时间。

Network Load Balancer 使用主动和被动的运行状况检查，以确定目标是否可用于处理请求。默认情况下，每个负载均衡器节点仅将请求路由到其可用区中运行状况良好的目标。如果您启用跨区域负载均衡，则每个负载均衡器节点都会将请求路由到所有已启用的可用区中运行状况良好的目标。有关更多信息，请参阅 [跨可用区负载均衡](#)。

借助被动的运行状况检查，负载均衡器观察目标如何响应连接。借助被动的运行状况检查，负载均衡器能够在主动的运行状况检查报告目标运行状况不佳之前，检测出此运行状况不佳的目标。您无法禁用、配置或监视被动运行状况检查。UDP 流量不支持被动运行状况检查，且开启了粘性目标群体。有关更多信息，请参阅[粘性会话](#)。

如果目标运行不正常，除非运行不正常的目标触发了负载均衡器故障断开，否则负载均衡器会为关联到目标的客户端连接上收到的数据包发送 TCP RST。

如果目标组在已启用的可用区中没有运行状况良好的目标，我们会从 DNS 中删除相应子网的 IP 地址，以便请求无法路由到该可用区中的目标。如果在所有已启用的可用区中，所有目标同时未通过运行状况检查，则负载均衡器将在失败时开放。当目标组为空时，网络负载均衡器也将无法打开。失败时开放的效果是允许传输到所有已启用的可用区中的所有目标的流量，而不考虑这些目标的运行状况。

如果目标组配置了 HTTPS 运行状况检查，则如果其注册目标仅支持 TLS 1.3，则无法通过运行状况检查。这些目标必须支持 TLS 的早期版本，例如 TLS 1.2。

对于 HTTP 或 HTTPS 运行状况检查请求，主机标头包含负载均衡器节点和侦听器端口的 IP 地址，但不包含目标和运行状况检查端口的 IP 地址。

如果您将 TLS 侦听器添加到 Network Load Balancer，我们将执行侦听器连接性测试。由于 TLS 终止也会终止 TCP 连接，因此在负载均衡器和目标之间建立新的 TCP 连接。因此，您可能会看到此测试的 TCP 连接从您的负载均衡器发送到在 TLS 侦听器中注册的目标。您可以识别这些 TCP 连接，因为它们具有您的 Network Load Balancer 的源 IP 地址，并且这些连接不包含数据包。

对于 UDP 服务，可以对目标组执行非 UDP 运行状况检查来测试目标可用性。您可以通过任何可用的运行状况检查 (TCP、HTTP 或 HTTPS) 和目标上的任何端口来验证 UDP 服务的可用性。如果接收运行状况检查的服务失败，则目标会视为不可用。要提高针对 UDP 服务进行运行状况检查的准确性，如果服务不可用，请配置侦听运行状况检查端口的服务，以跟踪您的 UDP 服务的状态，并停止运行状况检查。

## 运行状况检查设置

可以使用以下设置为目标组中的目标配置主动的运行状况检查。如果运行状况检查超过 `C UnhealthyThresholdout` 连续失败次数，则负载均衡器会使目标停止服务。当运行状况检查超过 `C HealthyThresholdout` 连续成功次数时，负载均衡器会将目标重新投入使用。

设置	描述	默认
HealthCheck协议	对目标执行运行状况检查时负载均衡器使用的协议。可能的协议有 HTTP、HTTPS 和 TCP。默认值为 TCP 协议。如果目标类型为 alb，支持的运行状况检查协议为 HTTP 和 HTTPS。	TCP
HealthCheck端口	对目标执行运行状况检查时负载均衡器使用的端口。默认设置是使用每个目标用来从负载均衡器接收流量的端口。	每个目标用来从负载均衡器接收流量的端口。
HealthCheck路径	[HTTP/HTTPS 运行状况检查] 运行状况检查路径，它是运行状况检查目标上的目的地。默认值为 /。	/
HealthCheckTimeoutSeconds	以秒为单位的时间长度，在此期间内，没有来自目标的响应意味着无法通过运行状况检查。范围为 2–120 秒。HTTP 运行状况检查时间的	HTTP 运行状况检查需要 6

设置	描述	默认
	默认值为 6 秒，TCP 和 HTTPS 运行状况检查时间的默认值为 10 秒。	秒，TCP 和 HTTPS 运行状况检查需要 10 秒。
HealthCheckIntervalSeconds	各个目标的运行状况检查之间的大约时间量 (以秒为单位)。范围为 5–300 秒。默认值为 30 秒。	30 秒
	<div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; background-color: #fff9f9;"> <p><b>⚠ Important</b></p> <p>Network Load Balancer 的运行状况检查是分布式的，使用共识机制来确定目标运行状况。因此，目标可以接收超过所配置数量的运行状况检查。要在使用 HTTP 运行状况检查时减少对目标的影响，请在目标上使用更简单的目标（例如，静态 HTML 文件）或切换到 TCP 运行状况检查。</p> </div>	
HealthyThreshold计数	将不正常目标视为正常运行之前所需的连续运行状况检查成功次数。范围为 2–10。默认值为 5。	5
UnhealthyThreshold计数	将目标视为不正常之前所需的连续运行状况检查失败次数。范围为 2–10。默认值为 2。	2
Matcher	[HTTP/HTTPS 运行状况检查] 检查来自目标的成功响应时使用的 HTTP 代码。范围为 200 至 599。默认值为 200-399。	200-399

## 目标运行状况

在负载均衡器向目标发送运行状况检查请求之前，您必须将目标注册到目标组，在侦听器规则中指定其目标组，并确保已为负载均衡器启用目标的可用区。

下表描述已注册目标的正常状态的可能值。

值	说明
initial	<p>负载均衡器正处于注册目标或对目标执行初始运行状况检查的过程中。</p> <p>相关原因代码：Elb.RegistrationInProgress   Elb.InitialHealthChecking</p>
healthy	<p>目标正常。</p> <p>相关原因代码：无</p>
unhealthy	<p>目标未响应运行状况检查、运行状况检查失败或目标处于停止状态。</p> <p>相关原因代码：Target.FailedHealthChecks</p>
draining	<p>目标正在取消注册，连接即将耗尽。</p> <p>相关原因代码：Target.DeregistrationInProgress</p>
unhealthy.draining	<p>目标未对运行状况检查做出响应或未通过运行状况检查并进入宽限期。目标支持现有连接，并且在此宽限期内不接受任何新连接。</p> <p>相关原因代码：Target.FailedHealthChecks</p>
unavailable	<p>目标运行状况不可用。</p> <p>相关原因代码：Elb.InternalError</p>
unused	<p>目标未在目标组中注册，目标组未在监听器规则中使用，或者目标位于未启用的可用区中。</p> <p>相关原因代码：Target.NotRegistered   Target.NotInUse   Target.InvalidState   Target.IpUnusable</p>

## 运行状况检查原因代码

如果目标的状态是 Healthy 以外的任何值，API 将返回问题的原因代码和描述，并且控制台将在工具提示中显示相同的描述。请注意，以 Elb 开头的原因代码源自负载均衡器端，以 Target 开头的原因代码源自目标端。

原因代码	说明
Elb.InitialHealthChecking	正在进行初始运行状况检查
Elb.InternalError	由于内部错误，运行状况检查失败
Elb.RegistrationInProgress	目标注册正在进行中
Target.DeregistrationInProgress	目标取消注册正在进行中
Target.FailedHealthChecks	运行状况检查失败
Target.InvalidState	目标处于停止状态 目标处于终止状态 目标处于终止或停止状态 目标处于无效状态
Target.IpUnusable	该 IP 地址正被负载均衡器使用，因此无法用作目标
Target.NotInUse	目标组没有被配置为接收来自负载均衡器的流量 目标处于没有为负载均衡器启用的可用区
Target.NotRegistered	目标未注册到目标组

## 检查目标的运行状况

您可以检查已注册到目标组的目标的运行状况。

## 使用控制台检查目标的运行状况

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. Details ( 详细信息 ) 窗格显示目标总数，以及每种运行状况的目标数。
5. 在 Targets ( 目标 ) 选项卡上，Health status ( 运行状况 ) 列指示每个目标的状态。
6. 如果目标状态是 Healthy 以外的任何值，则 Health status ( 运行状况 ) 列中将包含更多信息。

要检查目标的生命值，请使用 AWS CLI

使用 [describe-target-health](#) 命令。此命令的输出包含目标运行状况。如果状态是 Healthy 以外的任何值，则它包括原因代码。

接收有关运行状况不佳的目标的电子邮件通知

使用 CloudWatch 警报触发 Lambda 函数以发送有关不健康目标的详细信息。有关 step-by-step 说明，请参阅以下博客文章：[识别负载均衡器的运行状况不佳的目标](#)。

## 修改目标组的运行状况检查设置

您可以随时修改目标组的运行状况检查设置。

使用控制台修改目标组的运行状况检查设置

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Health checks 选项卡上，选择 Edit。
5. 在 Edit health check settings (编辑运行状况检查设置) 页面上，根据需要修改设置，然后选择 Save changes (保存更改)。

要修改目标群体的健康检查设置，请使用 AWS CLI

使用 [modify-target-group](#) 命令。



## 目标组的跨区域负载均衡

负载均衡器的节点将来自客户端的请求分配给已注册目标。启用跨区域负载均衡后，每个负载均衡器节点会在所有已注册可用区中的已注册目标之间分配流量。禁用跨区域负载均衡后，每个负载均衡器节点会仅在其可用区中的已注册目标之间分配流量。如果区域故障域优先于区域性故障域，这可以用于确保运行状况良好区域不受运行状况不佳区域的影响，或者改善整体延迟。

对于网络负载均衡器，负载均衡器级别的跨区域负载均衡默认为关闭，但您可以随时启动它。对于目标组，默认设置是使用负载均衡器设置，但您可以通过在目标组级别明确启动或关闭跨区域负载均衡来覆盖默认设置。

### 注意事项

- 为 Network Load Balancer 启用跨区域负载平衡时，将收取 EC2 数据传输费用。有关更多信息，请参阅 [《数据导出用户指南》中的了解AWS 数据传输费用](#)
- 目标组设置将决定目标组的负载均衡行为。例如，假设启用了负载均衡器级别的跨区域负载均衡，并禁用了目标组级别的跨区域负载均衡，则发送到目标组的流量不会进行跨区域路由。
- 关闭跨区域负载平衡时，请确保每个负载均衡器的区域中都有足够的目标容量，以便每个区域都能够为其关联的工作负载提供服务。
- 关闭跨区域负载平衡时，请确保所有目标组均参与到相同的可用区中。空的可用区被视为运行状况不佳。

## 修改负载均衡器的跨区域负载均衡

您可以随时开启或关闭负载均衡器级别的跨区域负载均衡。

### 使用控制台修改负载均衡器的跨区域负载均衡

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中的负载平衡下，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在 Edit load balancer attributes ( 编辑负载均衡器属性 ) 页面上，开启或关闭 Cross-zone load balancing ( 跨区域负载均衡 )。
6. 选择保存更改。

要修改负载均衡器的跨区域负载均衡，请使用 AWS CLI

使用带 `load_balancing.cross_zone.enabled` 属性的 [modify-load-balancer-attributes](#) 命令。

## 修改目标组的跨区域负载均衡

目标组级别的跨区域负载均衡设置会覆盖负载均衡器级别的设置。

如果目标组类型为 `instance` 或 `ip`，您可以开启或关闭目标组级别的跨区域负载均衡。如果目标组类型为 `alb`，则目标组始终从负载均衡器继承跨区域负载均衡设置。

使用控制台修改目标组的跨区域负载均衡

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的 Load Balancing ( 负载均衡 ) 下，选择 Target Groups ( 目标组 )。
3. 选择目标组的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在 Edit target group attributes ( 编辑目标组属性 ) 页面上，为 Cross-zone load balancing ( 跨区域负载均衡 ) 选择 On ( 开 )。
6. 选择保存更改。

要修改目标组的跨区域负载均衡，请使用 AWS CLI

使用带 `load_balancing.cross_zone.enabled` 属性的 [modify-target-group-attributes](#) 命令。

## 目标组运行状况

默认情况下，只要目标组至少有一个运行状况良好的目标，就会被视为运行状况良好。如果您的实例集很大，则仅有一个运行状况良好的目标为流量提供服务是不够的。相反，您可以指定必须运行状况良好的目标数量下限或最低百分比，以及当运行状况良好的目标低于指定阈值时负载均衡器将采取哪些操作。这样可以提高可用性。

## 运行状况不佳状态的操作

您可以为以下操作配置运行状况良好阈值：

- **DNS 故障转移** — 当某区域中运行状况良好的目标低于阈值时，我们会在 DNS 中将该区域的负载均衡器节点的 IP 地址标记为运行状况不佳。因此，当客户端解析负载均衡器 DNS 名称时，流量将会仅路由到运行状况良好的区域。

- 路由故障转移 - 当某区域中运行状况良好的目标低于阈值时，负载均衡器会将流量发送到负载均衡器节点可用的所有目标（包括运行状况不佳的目标）。这增加了客户端连接成功的机会，尤其是在目标暂时未能通过运行状况检查时，并降低了运行状况良好的目标过载的风险。

## 要求和注意事项

- 如果为某项操作指定了两种类型的阈值（计数和百分比），则负载均衡器会在违反任一阈值时执行该操作。
- 如果为这两项操作都指定了阈值，则 DNS 故障转移的阈值必须大于或等于路由故障转移的阈值，以便 DNS 故障转移会在路由故障转移时或之前发生。
- 如果您将阈值指定为百分比，我们将根据在目标组中注册的目标总数动态计算该值。
- 目标总数取决于关闭还是打开跨区域负载均衡。如果跨区域负载均衡处于关闭状态，则每个节点仅向自己区域中的目标发送流量，这意味着阈值将分别应用于每个已启用区域中的目标数量。如果跨区域负载均衡处于打开状态，则每个节点将流量发送到所有已启用区域中的所有目标，这意味着指定的阈值将应用于所有已启用区域中的目标总数。有关更多信息，请参阅 [跨可用区负载均衡](#)。
- 通过 DNS 故障转移，我们会从负载均衡器的 DNS 主机名中删除运行状况不佳区域的 IP 地址。但是，在 DNS 记录中的 time-to-live (TTL) 到期（60 秒）之前，本地客户端 DNS 缓存可能包含这些 IP 地址。
- 当发生 DNS 故障转移时，这会影响与负载均衡器关联的所有目标组。请确保剩余区域中有足够的容量来处理这些额外流量，尤其是在跨区域负载均衡关闭的情况下。
- 使用 DNS 故障转移时，如果所有负载均衡器区域都被视为运行状况不佳，则负载均衡器会将流量发送到所有区域（包括运行状况不佳的区域）。
- 除了是否有足够运行状况良好的目标可能会导致 DNS 故障转移之外，还有其他因素，例如区域的运行状况。

## 示例

以下示例演示了如何应用目标组运行状况设置。

### 场景

- 支持 A 和 B 两个可用区的负载均衡器
- 每个可用区中包含 10 个注册目标
- 目标组具有以下目标组运行状况设置：

- DNS 故障转移 - 50%
- 路由故障转移 - 50%
- 可用区 B 中有六个目标失败

#### 如果跨区域负载均衡关闭

- 每个可用区中的负载均衡器节点只能将流量发送到其可用区内的 10 个目标。
- 可用区 A 中有 10 个运行状况良好的目标，符合所需的运行状况良好的目标百分比。负载均衡器继续在 10 个运行状况良好的目标之间分配流量。
- 可用区 B 中只有 4 个运行状况良好的目标，占可用区 B 中负载均衡器节点目标的 40%。由于这低于所需的运行状况良好的目标百分比，负载均衡器会执行以下操作：
  - DNS 故障转移 - 可用区 B 在 DNS 中被标记为运行状况不佳。由于客户端无法将负载均衡器名称解析为可用区 B 中的负载均衡器节点，并且可用区 A 运行状况良好，因此客户端会向可用区 A 发送新连接。
  - 路由故障转移 - 当新连接明确发送到可用区 B 时，负载均衡器会将流量分配到可用区 B 中的所有目标（包括运行状况不佳的目标）。这样可以防止剩余运行状况良好的目标发生中断。

#### 如果跨区域负载均衡打开

- 每个负载均衡器节点可以向两个可用区中的所有 20 个注册目标发送流量。
- 可用区 A 中有 10 个运行状况良好的目标，可用区 B 中有 4 个运行状况良好的目标，总共有 14 个运行状况良好的目标。这是两个可用区中负载均衡器节点目标的 70%，符合所需的运行状况良好的目标百分比。
- 负载均衡器将在两个可用区内 14 个运行状况良好的目标之间分配流量。

## 修改目标组运行状况设置

您可以按如下方式修改目标组的目标组运行状况设置。

#### 使用控制台修改目标组运行状况设置

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Attributes（属性）选项卡上，选择 Edit（编辑）。

5. 检查是开启还是关闭了跨区域负载均衡。根据需要更新此设置，以确保在区域出现故障时您有足够的容量来处理额外流量。
6. 展开 Target group health requirements ( 目标组运行状况要求 )。
7. 对于 Configuration type ( 配置类型 )，我们建议您选择 Unified configuration ( 统一配置 )，它会为两个操作设置相同的阈值。
8. 对于 Healthy state requirements ( 运行状况良好状态要求 )，请执行以下操作之一：
  - 选择 Minimum healthy target count ( 运行状况良好的目标最低计数 )，然后输入介于 1 到目标组的最大目标数之间的数字。
  - 选择 Minimum healthy target percentage ( 运行状况良好的目标最低百分比 )，然后输入 1 到 100 之间的数字。
9. 选择保存更改。

要修改目标群体的健康设置，请使用 AWS CLI

使用 [modify-target-group-attributes](#) 命令。以下示例将两个运行状况不佳状态操作的运行状况良好阈值设置为 50%。

```
aws elbv2 modify-target-group-attributes \  
--target-group-arn arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-  
targets/73e2d6bc24d8a067 \  
--attributes  
Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50 \  
  
Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=50
```

## 运行状况不佳的目标的连接终止

默认情况下，连接终止处于启用状态。当 Network Load Balancer 的目标未通过配置的运行状况检查并被视为不健康时，负载均衡器会终止已建立的连接并停止将新连接路由到目标。禁用连接终止后，目标仍被视为运行状况不佳，不会接收新连接，但已建立的连接会保持活动状态，从而使它们能够优雅地关闭。

可以为每个目标组单独设置运行状况不佳的目标的连接终止。

使用控制台修改连接终止设置

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。

2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Attributes ( 属性 ) 选项卡上，选择 Edit ( 编辑 )。
5. 在目标运行状况不佳状态管理下，选择当目标变得运行状况不佳时终止连接已启用还是已禁用。
6. 选择保存更改。

要修改连接终止设置，请使用 AWS CLI

使用带 `target_health_state.unhealthy.connection_termination.enabled` 属性的 [modify-target-group-attributes](#) 命令。

## 排水间隔不正常

### Important

在启用不健康的耗尽间隔之前，必须先禁用连接终止。

处于该 `unhealthy.draining` 状态的目标被视为运行状况不佳，不会接收新连接，但在配置的时间间隔内保留已建立的连接。不健康的连接间隔决定了目标在状态变 `unhealthy` 为之前保持 `unhealthy.draining` 状态的时间长度。如果目标在不健康的连接间隔内通过了运行状况检查，则其状态将 `healthy` 再次变为。如果触发了取消注册，则目标状态变为 `draining` 并且取消注册延迟超时开始。

可以为每个目标组单独设置不健康的排水间隔。

使用控制台修改不健康的排水间隔

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Attributes ( 属性 ) 选项卡上，选择 Edit ( 编辑 )。
5. 在 Target 不健康状态管理下，确保关闭了当目标变得不健康时终止连接。
6. 为不健康的排水间隔输入一个值。
7. 选择保存更改。

要修改不健康的排水间隔，请使用 AWS CLI

使用带 `target_health_state.unhealthy.draining_interval_seconds` 属性的 [modify-target-group-attributes](#) 命令。

## 为负载均衡器使用 Route 53 DNS 故障转移

如果使用 Route 53 将 DNS 查询路由到您的负载均衡器，您也可以使用 Route 53 为您的负载均衡器配置 DNS 故障转移。在失效转移配置中，Route 53 将检查负载均衡器的目标组目标的运行状况以确定目标是否可用。如果没有已注册到负载均衡器的运行状况正常的目标，或如果负载均衡器本身运行状况不佳，则 Route 53 会将流量路由到其他可用资源，例如 Amazon S3 中运行状况正常的负载均衡器或静态网站。

例如，假设您有一个用于 `www.example.com` 的 Web 应用程序，并且您希望使用在不同区域内的两个负载均衡器之后运行的冗余实例。您希望流量主要路由到一个区域中的负载均衡器，并且您希望在发生故障期间将另一个区域中的负载均衡器用作备份。如果配置 DNS 故障转移，则可以指定您的主和辅助（备份）负载均衡器。如果主负载均衡器可用，则 Route 53 会将流量定向到主负载均衡器，否则会将流量定向到辅助负载均衡器。

### 使用评估目标运行状况功能

- 当网络负载均衡器别名记录上的“评估目标运行状况”设置为 Yes 时，Route 53 将评估 `alias target` 值指定的资源的运行状况。对于网络负载均衡器，Route 53 使用与负载均衡器关联的目标组运行状况检查。
- 当网络负载均衡器中的所有目标组均运行正常时，Route 53 会将别名记录标记为运行正常。如果目标组至少包含一个运行正常的目标，目标组将通过运行状况检查。然后，Route 53 会根据您的路由策略返回记录。如果使用失效转移路由策略，则 Route 53 返回主记录。
- 如果网络负载均衡器中的任何目标组运行状况不佳，则别名记录无法通过 Route 53 运行状况检查（失效时开放）。如果使用评估目标运行状况功能，则失效转移路由策略会失败。
- 如果网络负载均衡器中的所有目标组均为空（无目标），则 Route 53 会认为此记录运行状况不佳（失效时开放）。如果使用评估目标运行状况功能，则失效转移路由策略会失败。

有关更多信息，请参阅 Amazon Route 53 开发人员指南中的[配置 DNS 故障转移](#)。

## 向您的目标组注册目标

当您的目标准备好处理请求时，您将其注册到一个或多个目标组。目标组的目标类型将确定如何注册目标。例如，您可以注册实例 ID、IP 地址或 Application Load Balancer。只要注册过程完成且目标通过

初始运行状况检查，Network Load Balancer 就会开始将请求路由至目标。完成注册过程和开始运行状况检查可能需要几分钟时间。有关更多信息，请参阅 [目标组的运行状况检查](#)。

如果当前已注册目标的需求增加，您可以注册其他目标以便满足该需求。如果对已注册目标的需求减少，您可以从目标组中取消注册目标。完成取消注册过程和负载均衡器停止将请求路由到目标可能需要几分钟时间。如果需求随后增加，您可以再次向目标组注册已取消注册的目标。如果您需要为目标提供服务，您可以取消注册，然后在服务完成后重新注册。

在取消注册目标时，Elastic Load Balancing 会一直等待，直到进行中的请求完成。这称作连接耗尽。在连接耗尽期间，目标的状态为 `draining`。在取消注册完成后，目标的状态将更改为 `unused`。有关更多信息，请参阅 [取消注册延迟](#)。

如果要通过实例 ID 来注册目标，则可以将负载均衡器与 Auto Scaling 组一同使用。将目标组挂接到 Auto Scaling 组并且该组扩展后，由 Auto Scaling 组启动的实例将自动在目标组中注册。如果您将负载均衡器与 Auto Scaling 组分离，则实例会自动从目标组中取消注册。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的 [将负载均衡器挂接到 Auto Scaling 组](#)。

## 目标安全组

在将目标添加到目标组之前，请将与目标关联的安全组配置为接受来自网络负载均衡器的流量。

对目标安全组的建议（如果负载均衡器有与之关联的安全组）

- 允许客户端流量：添加规则，其引用与负载均衡器关联的安全组
- 允许 PrivateLink 流量：如果您将负载均衡器配置为评估通过流量的入站规则 AWS PrivateLink，请添加一条规则，在流量端口上接受来自负载均衡器安全组的流量。否则，添加规则，其在流量端口上接受来自负载均衡器私有 IP 地址的流量。
- 接受负载均衡器运行状况检查：添加规则，其在运行状况检查端口上接受来自负载均衡器安全组的运行状况检查流量。

对目标安全组的建议（如果负载均衡器没有与安全组关联）

- 允许客户端流量：如果负载均衡器保留客户端 IP 地址，则添加规则，其在流量端口上接受来自自己批准客户端 IP 地址的流量。否则，添加规则，其在流量端口上接受来自负载均衡器私有 IP 地址的流量。
- 允许 PrivateLink 流量：添加一条规则，在流量端口上接受来自负载均衡器私有 IP 地址的流量。
- 接受负载均衡器运行状况检查：添加规则，其在运行状况检查端口上接受来自负载均衡器私有 IP 地址的运行状况检查流量。



## 客户端 IP 保留的工作原理

除非将 `preserve_client_ip.enabled` 属性设置为 `true`，否则网络负载均衡器不会保留客户端 IP 地址。此外，使用双栈网络负载均衡器，我们在将 IPv4 地址转换为 IPv6 时保留客户端 IP 地址。但是，在将 IPv6 地址转换为 IPv4 时，源 IP 始终是 Network Load Balancer 的私有 IP 地址。

### 使用控制台查找负载均衡器的私有 IP 地址

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择 Network Interfaces。
3. 在搜索字段中，输入 Network Load Balancer 的名称。每个负载均衡器的子网有一个网络接口。
4. 在每个网络接口的详细信息选项卡上，从私有 IPv4 地址中复制地址。

有关更多信息，请参阅 [网络负载均衡器的安全组](#)。

## 网络 ACL

在将 EC2 实例注册为目标时，必须确保实例子网的网络 ACL 允许侦听器端口和运行状况检查端口上的流量。VPC 的默认网络访问控制列表 (ACL) 允许所有入站和出站流量。如果要创建自定义网络 ACL，请确保它们允许相应的流量。

与实例子网关联的网络 ACL 必须允许面向 Internet 的负载均衡器的以下流量。

### 实例子网的推荐规则

#### Inbound

源	协议	端口范围	评论
<i>### IP ##</i>	<i>###</i>	<i>###</i>	允许客户端流量 ( instance 目标类型 )
<i>VPC CIDR</i>	<i>###</i>	<i>###</i>	允许客户端流量 ( ip 目标类型 )
<i>VPC CIDR</i>	<i>#####</i>	<i>#####</i>	允许来自负载均衡器的运行状况检查流量

#### Outbound

目标位置	协议	端口范围	评论
### IP ##	###	###	允许响应客户端 ( instance 目标类型 )
VPC CIDR	###	###	允许响应客户端 ( ip 目标类型 )
VPC CIDR	#####	1024-65535	允许运行状况检查流量

与负载均衡器子网关联的网络 ACL 必须允许面向 Internet 的负载均衡器的以下流量。

#### 负载均衡器子网的推荐规则

##### Inbound

源	协议	端口范围	评论
### IP ##	###	###	允许客户端流量 ( instance 目标类型 )
VPC CIDR	###	###	允许客户端流量 ( ip 目标类型 )
VPC CIDR	#####	1024-65535	允许运行状况检查流量

##### Outbound

目标位置	协议	端口范围	评论
### IP ##	###	###	允许响应客户端 ( instance 目标类型 )
VPC CIDR	###	###	允许响应客户端 ( ip 目标类型 )

<i>VPC CIDR</i>	<i>#####</i>	<i>#####</i>	允许运行状况检查流量
<i>VPC CIDR</i>	<i>#####</i>	1024-65535	允许运行状况检查流量

对于内部负载均衡器，您的实例和负载均衡器节点的子网的网络 ACL 必须在侦听器端口和临时端口上允许进出 VPC CIDR 的入站流量和出站流量。

## 共享子网

参与者可以在共享 VPC 中创建网络负载均衡器。参与者无法注册在未与其共享的子网中运行的目标。

所有 AWS 区域都支持网络负载均衡器的共享子网，但不包括：

- 亚太地区 ( 大阪 ) ap-northeast-3
- 亚太地区 ( 香港 ) ap-east-1
- 中东 ( 巴林 ) me-south-1
- AWS 中国 ( 北京 ) cn-north-1
- AWS 中国 ( 宁夏 ) cn-northwest-1

## 注册或取消注册目标

每个目标组在为负载均衡器启用的每个可用区中必须至少有一个已注册目标。

您的目标组的目标类型将确定如何向该目标组注册目标。有关更多信息，请参阅 [Target type](#)。

### 要求和注意事项

- 如果实例采用以下实例类型，则不能利用实例 ID 注册实例：  
C1、CC1、CC2、CG1、CG2、CR1、G1、G2、H11、HS1、M1、M2、M3 或 T1。
- 当按实例 ID 为 IPv6 目标组注册目标时，必须为目标分配主 IPv6 地址。要了解更多信息，请参阅 Amazon EC2 用户指南中的 [IPv6 地址](#)
- 按实例 ID 注册目标时，实例必须与网络负载均衡器位于同一个 Amazon VPC 中。如果实例所在的 VPC 与负载均衡器 VPC 是对等的（位于同一区域或不同区域），则不能按实例 ID 注册实例。可以用 IP 地址注册这些实例。

- 如果您按 IP 地址注册目标，并且该 IP 地址与负载均衡器位于同一 VPC 中，则负载均衡器会验证其是否来自可以访问的子网。
- 对于 UDP 和 TCP\_UDP 目标组，如果实例位于负载均衡器 VPC 之外，或者采用以下实例类型之一，则不要用 IP 地址注册实例：C1、CC1、CC2、CG1、CG2、CR1、G1、G2、H11、HS1、M1、M2、M3 或 T1。如果目标驻留在负载均衡器 VPC 之外或者采用不受支持的实例类型，则目标可能能够接收来自负载均衡器的流量，但随后无法响应。

## 目录

- [通过实例 ID 注册或取消注册目标](#)
- [通过 IP 地址注册或取消注册目标](#)
- [使用 AWS CLI 注册或取消注册目标](#)

## 通过实例 ID 注册或取消注册目标

当您注册实例时，实例必须处于 running 状态。

使用控制台按实例 ID 注册或取消注册目标

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 选择目标选项卡。
5. 要注册实例，请选择注册目标。选择一个或多个实例，根据需要输入默认实例端口，然后选择在下面以待注册的形式添加。添加完实例后，选择注册待注册目标。

注意：

- 实例必须具有分配的主 IPv6 地址，才能向 IPv6 目标组注册。
  - AWS GovCloud (US) Region 不支持使用控制台分配主 IPv6 地址。您必须使用 API 在 AWS GovCloud (US) Region s 中分配主 IPv6 地址。
6. 要取消注册实例，请选择实例，然后选择取消注册。

## 通过 IP 地址注册或取消注册目标

### IPv4 目标

您注册的 IP 地址必须来自下列 CIDR 块之一：

- 目标组的 VPC 的子网
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

创建目标组后，无法更改 IP 地址类型。

以参与者身份在共享 Amazon VPC 中启动网络负载均衡器时，您只能在已共享的子网中注册目标。

### IPv6 目标

- 您注册的 IP 地址必须位于 VPC CIDR 块内或在对等 VPC CIDR 块内。
- 创建目标组后，无法更改 IP 地址类型。
- 您只能将 IPv6 目标组与具有 TCP 或 TLS 侦听器的双堆栈负载均衡器关联。

### 使用控制台按 IP 地址注册或取消注册目标

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 选择 Targets (目标) 选项卡。
5. 要注册 IP 地址，请选择注册目标。对于每个 IP 地址，选择网络、可用区、IP 地址 (IPv4 或 IPv6) 和端口，然后选择 Include as pending below (在下面添加为待处理)。指定完地址后，选择注册待注册目标。
6. 要注销 IP 地址，请选择 IP 地址，然后选择取消注册。如果您有多个注册的 IP 地址，则可能会发现添加筛选器或更改排序顺序很有帮助。

## 使用 AWS CLI 注册或取消注册目标

使用 [register-targets](#) 命令添加目标，并使用 [deregister-targets](#) 命令删除目标。

## 作为目标的 Application Load Balancer

您可以使用单个 Application Load Balancer 作为目标来创建目标组，然后配置 Network Load Balancer 以将流量转发到目标组。在这种情况下，Application Load Balancer 将在流量到达后立即接管负载均衡决策。此配置结合了两种负载均衡器的功能，并具有以下优点：

- 您可以将应用程序负载均衡器基于第 7 层请求的路由功能与网络负载均衡器支持的功能结合使用，例如端点服务 (AWS PrivateLink) 和静态 IP 地址。
- 您可以将此配置用于对于多个协议需要单个端点的应用程序，例如使用 HTTP 进行信号发送的媒体服务和用于流式传输内容的 RTP。

您可以将此功能与内部或面向 Internet 的应用程序负载均衡器搭配使用，作为内部或面向 Internet 的网络负载均衡器的目标。

### 注意事项

- 要将应用程序负载均衡器关联为网络负载均衡器的目标，它们必须位于同一账户中的同一 Amazon VPC 中。
- 您可以将应用程序负载均衡器作为多个网络负载均衡器的目标。为此，使用单独的目标组为每个网络负载均衡器注册应用程序负载均衡器。
- 您使用网络负载均衡器注册的每个应用程序负载均衡器会将每个网络负载均衡器在每个可用区的最大目标数减少 50 个（如果禁用跨区域负载均衡）或 100 个（如果启用跨区域负载均衡）。您可以在这两个负载均衡器中禁用跨区域负载均衡，以尽量减少延迟并避免区域数据传输费用。有关更多信息，请参阅 [Network Load Balancer 的配额](#)。
- 当目标组类型为 alb 时，您无法修改目标组属性。这些属性始终使用其默认值。
- 注册应用程序负载均衡器作为目标，只有从所有目标组中取消注册此应用程序负载均衡器才能将其删除。

## 步骤 1：创建应用程序负载均衡器

在开始之前，请配置此应用程序负载均衡器将使用的目标组。确保您有一个虚拟私有云 (VPC)，其中包含您将在目标组中注册的目标。此 VPC 必须在目标使用的每个可用区中至少有一个公有子网。

## 使用控制台创建 Application Load Balancer

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的 Load Balancing (负载均衡) 下，选择 Load Balancers (负载均衡器)。
3. 选择创建负载均衡器。
4. 在应用程序负载均衡器下，选择创建。
5. 在 Create Application Load Balancer (创建应用程序负载均衡器) 页面上的 Basic configuration (基本配置) 下，指定 Load balancer name (负载均衡器名称)、Scheme (方案) 和 IP address type (IP 地址类型)。
6. 对于侦听器，您可以在任何端口上创建 HTTP 或 HTTPS 侦听器。但是，您必须确保此侦听器的端口号与 Application Load Balancer 将驻留的目标组的端口匹配。
7. 在 Availability Zones (可用区) 下，请执行以下操作：
  - a. 对于 VPC，选择一个虚拟私有云 (VPC)，其中包含您作为 Application Load Balancer 的目标包含的实例或 IP 地址。您必须使用与用于 [步骤 3：创建 Network Load Balancer，并将 Application Load Balancer 配置为其目标](#) 中的 Network Load Balancer 相同的 VPC。
  - b. 选择两个或多个 Availability Zones (可用区) 和相应的子网。确保这些可用区与为 Network Load Balancer 启用的可用区匹配，以优化可用性、扩展性和性能。
8. 您可以通过创建新安全组或选择现有安全组，以 Assign a security group (分配安全组) 给您的负载均衡器。

您选择的新安全组应包含一条规则，该规则允许将流量传送到此负载均衡器的侦听器端口。使用客户端计算机的 CIDR 块 (IP 地址范围) 作为安全组入站规则中的流量源。这可让客户端通过此 Application Load Balancer 传送流量。有关将应用程序负载均衡器的安全组配置为网络负载均衡器的目标的更多信息，请参阅《应用程序负载均衡器用户指南》中的 [应用程序负载均衡器的安全组](#)。

9. 对于 Configure Routing (配置路由)，选择您为此 Application Load Balancer 配置的目标组。如果没有可用的目标组，并且想要配置新的目标组，请参阅适用于 Application Load Balancer 的用户指南中的 [创建目标组](#)。
10. 查看配置，然后选择 Create load balancer (创建负载均衡器)。

## 使用 Application Load Balancer AWS CLI

使用 [create-load-balancer](#) 命令。

## 步骤 2：以 Application Load Balancer 作为目标创建目标组

创建目标组可让您将新的或现有的 Application Load Balancer 注册为目标。每个目标组只能添加一个 Application Load Balancer。同一个 Application Load Balancer 也可以在单独的目标组中使用，作为最多两个 Network Load Balancer 的目标。

使用控制台创建目标组并将 Application Load Balancer 注册为目标

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择 Create target group (创建目标组)。
4. 在 Specify group details (指定组详细信息)页面的 Basic configuration (基本配置)下，选择 Application Load Balancer。
5. 对于 Target group name (目标组名称)，输入 Application Load Balancer 目标组的名称。
6. 对于 Protocol (协议)，只允许 TCP。为您的目标组选择 Port (端口)。此目标组端口必须与 Application Load Balancer 的侦听器端口匹配。或者，您可以在应用程序负载均衡器上添加或编辑侦听器端口以匹配此端口。
7. 对于 VPC，选择一个带有应用程序负载均衡器的虚拟私有云 (VPC)，以便向目标组注册。
8. 对于运行状况检查，选择 HTTP 或 HTTPS 作为运行状况检查协议。运行状况检查将发送到 Application Load Balancer 并使用指定的端口、协议和 ping 路径转发到其目标。确保应用程序负载均衡器可以通过侦听器来接收这些运行状况检查结果，该侦听器的端口和协议与运行状况检查端口和协议匹配。
9. (可选) 根据需要添加一个或多个标签。
10. 选择下一步。
11. 在 Register targets (注册目标) 页面中，选择要注册为目标的 Application Load Balancer。从列表中选择的应用程序负载均衡器必须具有与所创建目标组位于同一端口上的侦听器。您可以在该负载均衡器上添加或编辑侦听器以匹配目标组的端口，或返回上一步并更改为目标组指定的端口。如果您不确定要添加哪个 Application Load Balancer 作为目标，或者此时不想添加它，则可以选择稍后添加 Application Load Balancer。
12. 选择 Create target group (创建目标组)。

若要使用 AWS CLI 创建目标组并将应用程序负载均衡器注册为目标

使用 [create-target-group](#) 和 [register-targets](#) 命令。



## 步骤 3：创建 Network Load Balancer，并将 Application Load Balancer 配置为其目标

使用以下步骤创建 Network Load Balancer，然后使用控制台将 Application Load Balancer 配置为其目标。

使用控制台创建 Network Load Balancer 和侦听器

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的 Load Balancing (负载均衡) 下，选择 Load Balancers (负载均衡器)。
3. 选择创建负载均衡器。
4. 在网络负载均衡器下，选择创建。
5. 基本配置

在基本配置窗格中，配置负载均衡器名称、方案和 IP 地址类型。

6. 网络映射
  - a. 对于 VPC，选择用于应用程序负载均衡器目标的相同 VPC。如果您为 Scheme (方案) 选择了 Internet-facing (面向 Internet)，只有带有互联网网关的 VPC 可供选择。
  - b. 对于 Mappings (映射)，选择一个或多个可用区和相应的子网。我们建议您选择与 Application Load Balancer 目标相同的可用区，以优化可用性、扩展性和性能。

(可选) 要使用静态 IP 地址，请针对每个可用区选择 IPv4 设置中的使用弹性 IP 地址。使用静态 IP 地址，您可以将某些 IP 地址添加到防火墙允许列表中，也可以对客户端进行 IP 地址硬编码。

7. 侦听器 and 路由
  - a. 默认值是负责接收端口 80 上的 TCP 流量的侦听器。只有 TCP 侦听器才能将流量转发到应用程序负载均衡器目标组。您必须将协议保留为 TCP，但可以根据需要修改端口。

通过此配置，您可以在应用程序负载均衡器上使用 HTTPS 侦听器终止 TLS 流量。

- b. 对于默认操作，选择向其转发流量的应用程序负载均衡器目标组。如果在列表中没有看到此目标组，或者无法选择目标组（因为它已被另一个网络负载均衡器使用），则可以创建一个应用程序负载均衡器目标组，如 [步骤 2：以 Application Load Balancer 作为目标创建目标组](#) 中所示。

8. 标签

( 可选 ) 添加标签以对负载均衡器进行分类。有关更多信息，请参阅[标签](#)。

## 9. 摘要

查看配置，然后选择创建负载均衡器。

使用创建 Network Load Balancer AWS CLI

使用 [create-load-balancer](#) 命令。

## 步骤 4：( 可选 ) 创建 VPC 端点服务

要使用您在上一步中设置的网络负载均衡器作为私有连接的端点，您可以启用 AWS PrivateLink。这将建立与负载均衡器作为终端节点服务的私有连接。

要使用您的网络负载均衡器创建 VPC 端点服务

1. 在导航窗格中，选择负载均衡器。
2. 选择网络负载均衡器的名称以打开其详细信息页面。
3. 在集成选项卡上，展开 VPC 端点服务 ( AWS PrivateLink )。
4. 选择创建端点服务以打开端点服务页面。有关其余步骤，请参阅《AWS PrivateLink 指南》中的[创建端点服务](#)。

## 适用于目标组的标签

标签有助于按各种标准 (例如用途、所有者或环境) 对目标组进行分类。

您可以为每个目标组添加多个标签。每个目标组的标签键必须是唯一的。如果您添加的标签中的键已经与目标组关联，它将更新该标签的值。

用完标签后可以将其删除。

### 限制

- 每个资源的标签数上限 - 50
- 最大密钥长度 - 127 个 Unicode 字符
- 最大值长度 - 255 个 Unicode 字符

- 标签键和值区分大小写。允许使用的字符包括可用 UTF-8 格式表示的字母、空格和数字，以及以下特殊字符：+ - = 。 \_ : / @。请不要使用前导空格或尾随空格。
- 请勿在标签名称或值中使用aws:前缀，因为它已保留供 AWS 使用。您无法编辑或删除带此前缀的标签名称或值。具有此前缀的标签不计入每个资源的标签数限制。

### 使用控制台更新目标群组的标签

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在标签选项卡上，选择管理标签，然后执行以下一项或多项操作：
  - a. 要更新标签，请为键和值输入新值。
  - b. 要添加标签，请选择添加标签，然后为键和值输入值。
  - c. 要删除标签，请选择标签旁边的删除。
5. 更新完标签后，选择保存更改。

要更新目标群组的标签，请使用 AWS CLI

使用 [add-tags](#) 和 [remove-tags](#) 命令。

## 删除目标组

如果目标组未由任何侦听器规则的转发操作引用，则可以删除该目标组。删除目标组不会影响已注册到目标组的目标。如果您不再需要已注册的 EC2 实例，则可以停止或终止该实例。

### 使用控制台删除目标组

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组，然后依次选择操作、删除。
4. 当系统提示进行确认时，选择是，删除。

要使用删除目标组 AWS CLI

使用 [delete-target-group](#) 命令。

# 监控 Network Load Balancer

您可使用以下功能监控负载均衡器，分析流量模式及解决与负载均衡器和目标相关的问题。

## CloudWatch 指标

您可以使用 Amazon CloudWatch 以一组有序的时间序列数据（称为指标）的形式检索有关负载均衡器和目标的数据点的统计数据。您可使用这些指标来验证您的系统是否按预期运行。有关更多信息，请参阅 [CloudWatch 您的 Network Load Balancer 的指标](#)。

## VPC 流日志

您可以使用 VPC 流日志来捕获有关往来于您的 Network Load Balancer 的流量的详细信息。有关更多信息，请参阅 Amazon VPC 用户指南中的 [VPC 流日志](#)。

为负载均衡器的每个网络接口创建流日志。每个负载均衡器的子网有一个网络接口。要确定 Network Load Balancer 的网络接口，请在网络接口的描述字段中查找负载均衡器的名称。

通过您的 Network Load Balancer 的每个连接有两个条目，一个用于客户端和负载均衡器之间的前端连接，另一个用于负载均衡器和目标之间的后端连接。如果目标组的客户端 IP 保留属性已启用，连接将作为来自客户端的连接向实例显示。否则，连接的源 IP 是负载均衡器的私有 IP 地址。如果实例的安全组不允许来自客户端的连接，但负载均衡器子网的网络 ACL 允许这些连接，负载均衡器的网络接口的日志将对前端和后端连接显示“接受 OK”，同时实例的网络接口的日志将对连接显示“拒绝 OK”。

如果网络负载均衡器关联了安全组，则流日志将包含安全组允许或拒绝的流量条目。对于带有 TLS 侦听器的网络负载均衡器，流日志条目将仅反映被拒绝的条目。

## 访问日志

您可以使用访问日志捕获有关向负载均衡器发出的 TLS 请求的详细信息。日志文件存储在 Amazon S3 中。您可以使用这些访问日志分析流量模式并解决与目标相关的问题。有关更多信息，请参阅 [您的 Network Load Balancer 的访问日志](#)。

## CloudTrail 日志

您可以使用 AWS CloudTrail 捕获有关对 Elastic Load Balancing API 的调用的详细信息，并将其作为日志文件存储在 Amazon S3 中。您可以使用这些 CloudTrail 日志来确定拨打了哪些呼叫、呼叫来自哪个源 IP 地址、谁拨打了电话、何时拨打了呼叫等。有关更多信息，请参阅 [使用 AWS CloudTrail 记录 Network Load Balancer 的 API 调用](#)。

## CloudWatch 您的 Network Load Balancer 的指标

Elastic Load Balancing 将您的 CloudWatch 负载均衡器和目标的数据点发布到亚马逊。CloudWatch 允许您以一组有序的时间序列数据（称为指标）的形式检索有关这些数据点的统计信息。可将指标视为要监控的变量，而将数据点视为该变量随时间变化的值。例如，您可以在指定时间段内监控负载均衡器的正常目标的总数。每个数据点都有相关联的时间戳和可选测量单位。

您可使用指标来验证系统是否正常运行。例如，您可以创建 CloudWatch 警报来监控指定的指标，并在该指标超出您认为可接受的范围时启动操作（例如向电子邮件地址发送通知）。

CloudWatch 仅当请求流经负载均衡器时，Elastic Load Balancing 才会向其报告指标。如果有请求流经负载均衡器，则 Elastic Load Balancing 进行测量并以 60 秒的间隔发送其指标。如果没有请求流经负载均衡器或指标无数据，则不报告指标。对于带有安全组的网络负载均衡器，CloudWatch 指标中不会捕获安全组拒绝的流量。

有关更多信息，请参阅 [Amazon CloudWatch 用户指南](#)。

### 内容

- [Network Load Balancer 指标](#)
- [网络负载均衡器的指标维度](#)
- [Network Load Balancer 指标的统计数据](#)
- [查看您的负载均衡器的 CloudWatch 指标](#)

## Network Load Balancer 指标

AWS/NetworkELB 命名空间包括以下指标。

指标	描述
ActiveFlowCount	<p>客户端至目标的并发流（或连接）的总数。此指标包含处于 SYN_SENT 和 ESTABLISHED 状态的连接。TCP 连接未在负载均衡器上终止，因此，一个开放与目标的 TCP 连接的客户端将计为一个流。</p> <p>报告标准：始终报告。</p> <p>统计数据：最有用的统计工具是 Average、Maximum 和 Minimum。</p>

指标	描述
	<p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> <li>• AvailabilityZone , LoadBalancer</li> </ul>
ActiveFlowCount_TCP	<p>客户端至目标的并发 TCP 流 ( 或连接 ) 的总数。此指标包含处于 SYN_SENT 和 ESTABLISHED 状态的连接。TCP 连接未在负载均衡器上终止, 因此, 一个开放与目标的 TCP 连接的客户端将计为一个流。</p> <p>报告标准: 有非零值</p> <p>统计数据: 最有用的统计工具是 Average、Maximum 和 Minimum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> <li>• AvailabilityZone , LoadBalancer</li> </ul>
ActiveFlowCount_TLS	<p>客户端至目标的并发 TLS 流 ( 或连接 ) 的总数。此指标包含处于 SYN_SENT 和 ESTABLISHED 状态的连接。</p> <p>报告标准: 有非零值。</p> <p>统计数据: 最有用的统计工具是 Average、Maximum 和 Minimum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> <li>• AvailabilityZone , LoadBalancer</li> </ul>

指标	描述
ActiveFlowCount_UDP	<p>客户端至目标的并发 UDP 流（或连接）的总数。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Average、Maximum 和 Minimum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> <li>• AvailabilityZone , LoadBalancer</li> </ul>
ClientTLSNegotiationErrorCount	<p>在客户端和 TLS 侦听器之间协商期间失败的 TLS 握手的总数。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> </ul>
ConsumedLCUs	<p>负载均衡器使用的负载均衡器容量单位 (LCU) 数量。您需要为每小时使用的 LCU 数量付费。有关更多信息，请参阅 <a href="#">Elastic Load Balancing 定价</a>。</p> <p>报告标准：始终报告。</p> <p>统计数据：全部</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> </ul>

指标	描述
ConsumedLCUs_TCP	<p>负载均衡器为 TCP 使用的负载均衡器容量单位 (LCU) 数量。您需要为每小时使用的 LCU 数量付费。有关更多信息，请参阅 <a href="#">Elastic Load Balancing 定价</a>。</p> <p>报告标准：有非零值。</p> <p>统计数据：全部</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li></ul>
ConsumedLCUs_TLS	<p>负载均衡器为 TLS 使用的负载均衡器容量单位 (LCU) 数量。您需要为每小时使用的 LCU 数量付费。有关更多信息，请参阅 <a href="#">Elastic Load Balancing 定价</a>。</p> <p>报告标准：有非零值。</p> <p>统计数据：全部</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li></ul>
ConsumedLCUs_UDP	<p>负载均衡器为 UDP 使用的负载均衡器容量单位 (LCU) 数量。您需要为每小时使用的 LCU 数量付费。有关更多信息，请参阅 <a href="#">Elastic Load Balancing 定价</a>。</p> <p>报告标准：有非零值。</p> <p>统计数据：全部</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li></ul>



指标	描述
HealthyHostCount	<p>被视为正常运行的目标数量。此指标不包括注册为目标的任何 Application Load Balancer。</p> <p>报告标准：在启用了运行状况检查时报告。</p> <p>统计数据：最有用的统计工具为 Maximum 和 Minimum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer , TargetGroup</li> <li>• AvailabilityZone , LoadBalancer , TargetGroup</li> </ul>
NewFlowCount	<p>时段内建立的客户端至目标的新流 ( 或连接 ) 的总数。</p> <p>报告标准：始终报告。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> <li>• AvailabilityZone , LoadBalancer</li> </ul>
NewFlowCount_TCP	<p>时段内建立的客户端至目标的新 TCP 流 ( 或连接 ) 的总数。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> <li>• AvailabilityZone , LoadBalancer</li> </ul>

指标	描述
NewFlowCount_TLS	<p>时段内建立的客户端至目标的新 TLS 流 (或连接) 的总数。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>
NewFlowCount_UDP	<p>时段内建立的客户端至目标的新 UDP 流 (或连接) 的总数。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>
PeakPacketsPerSecond	<p>最高平均数据包速率 (每秒处理的数据包数)，在采样窗口期间每 10 秒计算一次。此指标包含运行状况检查流量。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Maximum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>

指标	描述
PortAllocationErrorCount	<p>客户端 IP 转换操作期间临时端口分配错误的总数。非零值表示断开的客户端连接。</p> <p>注意：当执行客户端地址转换时，Network Load Balancer 支持与每个唯一目标（IP 地址和端口）的 55,000 个并发连接或每分钟约 55,000 个连接。要修复端口分配错误，请将更多目标添加到目标组。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> <li>• AvailabilityZone , LoadBalancer</li> </ul>
ProcessedBytes	<p>负载均衡器处理的字节总数，包括 TCP/IP 标头。此计数包括往返目标的流量，减去运行状况检查流量。</p> <p>报告标准：始终报告。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> <li>• AvailabilityZone , LoadBalancer</li> </ul>
ProcessedBytes_TCP	<p>TCP 侦听器处理的字节的总数。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> <li>• AvailabilityZone , LoadBalancer</li> </ul>

指标	描述
ProcessedBytes_TLS	<p>TLS 侦听器处理的字节的总数。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>
ProcessedBytes_UDP	<p>UDP 侦听器处理的字节的总数。</p> <p>报告标准：有非零值</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>
ProcessedPackets	<p>负载均衡器处理的总数据包数。此计数包含往返目标的流量，以及运行状况检查流量。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>

指标	描述
SecurityGroupBlockedFlowCount_Inbound_ICMP	<p>被负载均衡器安全组的入站规则拒绝的新 ICMP 消息的数量。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>
SecurityGroupBlockedFlowCount_Inbound_TCP	<p>被负载均衡器安全组的入站规则拒绝的新 TCP 流的数量。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>
SecurityGroupBlockedFlowCount_Inbound_UDP	<p>被负载均衡器安全组的入站规则拒绝的新 UDP 流的数量。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>

指标	描述
SecurityGroupBlockedFlowCount_Outbound_ICMP	<p>被负载均衡器安全组的出站规则拒绝的新 ICMP 消息的数量。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>
SecurityGroupBlockedFlowCount_Outbound_TCP	<p>被负载均衡器安全组的出站规则拒绝的新 TCP 流的数量。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>
SecurityGroupBlockedFlowCount_Outbound_UDP	<p>被负载均衡器安全组的出站规则拒绝的新 UDP 流的数量。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>

指标	描述
TargetTLSNegotiationErrorCount	<p>在 TLS 侦听器和目标之间协商期间失败的 TLS 握手的总数。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li></ul>
TCP_Client_Reset_Count	<p>从客户端发送至目标的重置 (RST) 数据包的总数。这些重置由客户端生成，然后由负载均衡器转发。</p> <p>报告标准：始终报告。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>
TCP_ELB_Reset_Count	<p>负载均衡器生成的重置 (RST) 数据包的总数。有关更多信息，请参阅<a href="#">故障排除</a>。</p> <p>报告标准：始终报告。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"><li>• LoadBalancer</li><li>• AvailabilityZone , LoadBalancer</li></ul>

指标	描述
TCP_Target_Reset_Count	<p>从目标发送至客户端的重置 (RST) 数据包的总数。这些重置由目标生成，然后由负载均衡器转发。</p> <p>报告标准：始终报告。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> <li>• AvailabilityZone , LoadBalancer</li> </ul>
UnHealthyHostCount	<p>被视为未正常运行的目标数量。此指标不包括注册为目标任何 Application Load Balancer。</p> <p>报告标准：在启用了运行状况检查时报告。</p> <p>统计数据：最有用的统计工具为 Maximum 和 Minimum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer , TargetGroup</li> <li>• AvailabilityZone , LoadBalancer , TargetGroup</li> </ul>
UnhealthyRoutingFlowCount	<p>使用路由失效转移操作 (失败时开放) 路由的流 (或连接) 数量。</p> <p>报告标准：有非零值。</p> <p>统计数据：最有用的统计工具是 Sum。</p> <p>尺寸</p> <ul style="list-style-type: none"> <li>• LoadBalancer</li> <li>• AvailabilityZone , LoadBalancer</li> </ul>

## 网络负载均衡器的指标维度

要筛选负载均衡器的指标，请使用以下维度。



维度	描述
AvailabilityZone	按可用区筛选指标数据。
LoadBalancer	按负载均衡器筛选指标数据。按以下方式指定负载均衡器：net/load-balancer-name/1234567890123456 (负载均衡器 ARN 的结尾部分)。
TargetGroup	按目标组筛选指标数据。按以下方式指定目标组：targetgroup/target-group-name/1234567890123456 (目标组 ARN 的结尾部分)。

## Network Load Balancer 指标的统计数据

CloudWatch 根据 Elastic Load Balancing 发布的指标数据点提供统计数据。统计数据是在指定的时间段内汇总的指标数据。当请求统计数据时，返回的数据流按指标名称和维度进行识别。维度是用于唯一标识指标的名称/值对。例如，您可以请求在特定可用区内启动的负载均衡器背后所有正常状态 EC2 实例的统计数据。

Minimum 和 Maximum 统计数据反映每个采样窗口中各个负载均衡器节点报告的数据点的最小值和最大值。HealthyHostCount 最大值的增加与 UnHealthyHostCount 最小值的减少相对应。建议监控最大值 HealthyHostCount，在最大值 HealthyHostCount 低于所需的最小值或为 0 时调用警报。这有助于确定目标运行状况何时变得不佳。还建议监控最小值 UnHealthyHostCount，当最小值 UnHealthyHostCount 超过 0 时调用警报。这使您能够在不再有注册目标时意识到此情况。

Sum 统计数据是所有负载均衡器节点的汇总值。由于这些指标在每个周期均包含多个报告，因此 Sum 仅适用于对所有负载均衡器节点进行汇总的指标。

SampleCount 统计数据是测量的样本数。由于这些指标是基于采样间隔和事件进行收集的，因此此统计信息一般没有用。例如，对于 HealthyHostCount，SampleCount 基于每个负载均衡器节点报告的样本数，而不是运行状况正常的主机数。

## 查看您的负载均衡器的 CloudWatch 指标

您可以使用 Amazon EC2 控制台查看您的负载均衡器的 CloudWatch 指标。这些指标显示为监控图表。如果负载均衡器处于活动状态并且正在接收请求，则监控图表会显示数据点。

或者，您可以使用 CloudWatch 控制台查看负载均衡器的指标。

## 使用控制台查看指标

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 要查看按目标组筛选的指标，请执行以下操作：
  - a. 在导航窗格中，选择 Target Groups。
  - b. 选择目标组并选择 Monitoring。
  - c. (可选) 要按时间筛选结果，请从 Showing data for 中选择时间范围。
  - d. 要获得单个指标的一个较大视图，请选择其图形。
3. 要查看按负载均衡器筛选的指标，请执行以下操作：
  - a. 在导航窗格中，选择 Load Balancers。
  - b. 选择负载均衡器并选择 Monitoring。
  - c. (可选) 要按时间筛选结果，请从 Showing data for 中选择时间范围。
  - d. 要获得单个指标的一个较大视图，请选择其图形。

## 使用 CloudWatch 控制台查看指标

1. 打开 CloudWatch 控制台，[网址为 https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/)。
2. 在导航窗格中，选择指标。
3. 选择 NetworkELB 命名空间。
4. (可选) 要跨所有维度查看某个指标，请在搜索字段中键入其名称。

要查看指标，请使用 AWS CLI

使用以下 [list-metrics](#) 命令列出可用指标：

```
aws cloudwatch list-metrics --namespace AWS/NetworkELB
```

要获取指标的统计数据，请使用 AWS CLI

使用以下 [get-metric-statistics](#) 命令获取指定指标和维度的统计数据。请注意，CloudWatch 将每个唯一的维度组合视为一个单独的指标。您无法使用未专门发布的维度组合检索统计数据。您必须指定创建指标时使用的同一维度。

```
aws cloudwatch get-metric-statistics --namespace AWS/NetworkELB \  
--metric-name UnHealthyHostCount --statistics Average --period 3600 \  

```

```
--dimensions Name=LoadBalancer,Value=net/my-load-balancer/50dc6c495c0c9188 \  
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \  
--start-time 2017-04-18T00:00:00Z --end-time 2017-04-21T00:00:00Z
```

下面是示例输出：

```
{  
  "Datapoints": [  
    {  
      "Timestamp": "2017-04-18T22:00:00Z",  
      "Average": 0.0,  
      "Unit": "Count"  
    },  
    {  
      "Timestamp": "2017-04-18T04:00:00Z",  
      "Average": 0.0,  
      "Unit": "Count"  
    },  
    ...  
  ],  
  "Label": "UnHealthyHostCount"  
}
```

## 您的 Network Load Balancer 的访问日志

Elastic Load Balancing 提供的访问日志可捕获与您的网络负载均衡器建立的 TLS 连接的详细信息。您可以使用这些访问日志分析流量模式并解决问题。

### Important

只有在 Network Load Balancer 具有 TLS 侦听器并且仅包含有关 TLS 连接的信息时，才会创建访问日志。

访问日志记录是 Elastic Load Balancing 的一项可选功能，默认情况下已禁用此功能。为负载均衡器启用访问日志记录之后，Elastic Load Balancing 将日志捕获为压缩文件并将其存储在您指定的 Amazon S3 存储桶中。您可以随时禁用访问日志记录。

您可以使用 Amazon S3 托管加密密钥 (SSE-S3) 启用服务器端加密，也可使用 Key Management Service 与 S3 存储桶的客户管理的密钥 (SSE-KMS CMK) 来启用服务器端加密。每个访问日志文件在存储到 S3 存储桶之前将自动加密，并在您访问它时进行解密。您不需要执行任何操作，因为这与

您访问加密的日志文件或未加密的日志文件的方式基本相同。每个日志文件都使用唯一的密钥加密，该密钥本身使用定期轮换的 KMS 密钥进行加密。有关更多信息，请参阅 [Amazon S3 用户指南中的指定 Amazon S3 加密 \(SSE-S3\) 和使用 AWS KMS \(SSE-KMS\) 指定服务器端加密](#)。

使用访问日志无需额外付费。您需要支付 Amazon S3 的存储费用，但无需支付 Elastic Load Balancing 用以将日志文件发送到 Amazon S3 的带宽费用。有关存储成本的更多信息，请参阅 [Amazon S3 定价](#)。

## 访问日志文件

Elastic Load Balancing 每 5 分钟为每个负载均衡器节点发布一次日志文件。日志传输最终是一致的。负载均衡器可以传输相同时间段的多个日志。通常，如果站点具有高流量，会出现此情况。

访问日志的文件名采用以下格式：

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_net.load-balancer-id_end-time_random-string.log.gz
```

### bucket

S3 存储桶的名称。

### prefix

存储桶中的前缀 (逻辑层级结构)。如果您不指定前缀，则会将日志置于存储桶的根级。

### aws-account-id

所有者的 AWS 账户 身份证。

### region

负载均衡器和 S3 存储桶所在的区域。

### yyyy/mm/dd

传输日志的日期。

### load-balancer-id

负载均衡器的资源 ID。如果资源 ID 包含任何正斜杠 (/)，这些正斜杠将替换为句点 (.)。

### end-time

日志记录间隔结束的日期和时间。例如，结束时间 20181220T2340Z 包含在 23:35 和 23:40 之间发出的请求的条目。

## random-string

系统生成的随机字符串。

以下是示例日志文件名：

```
s3://my-bucket/prefix/AWSLogs/123456789012/elasticloadbalancing/us-east-2/2020/05/01/123456789012_elasticloadbalancing_us-east-2_net.my-loadbalancer.1234567890abcdef_20200501T0000Z_20sg8hgm.log.gz
```

日志文件可以在存储桶中存储任意长时间，不过您也可以定义 Amazon S3 生命周期规则以自动存档或删除日志文件。有关更多信息，请参阅《Amazon S3 用户指南》中的[管理存储生命周期](#)。

## 访问日志条目

下表按顺序描述了访问日志条目的字段。使用空格分隔所有字段。在引入新的字段时，会将这些字段添加到日志条目的末尾。在处理日志文件时，您应忽略日志条目结尾的任何不需要的字段。

字段	描述
类型	侦听器的类型。支持的值为 <code>tls</code> 。
版本	日志条目的版本。当前版本为 2.0。
time	在 TLS 连接结束时记录的时间（采用 ISO 8601 格式）。
elb	负载均衡器的资源 ID。
侦听器	连接的 TLS 侦听器的资源 ID。
client:port	客户端的 IP 地址和端口。
目的地：端口	目的地 IP 地址和端口。如果客户端直接连接到负载均衡器，则目的地是侦听器。如果客户端使用 VPC 终端节点服务进行连接，则目的地是 VPC 终端节点。
connection_time	连接完成（从开始到结束）的总时间（以毫秒为单位）。
tls_handshake_time	建立 TCP 连接后完成 TLS 握手的总时间，包括客户端延迟（以毫秒为单位）。此时间包括在 <code>connection_time</code> 字段中。

字段	描述
received_bytes	解密后，负载均衡器从客户端处收到的字节数。
sent_bytes	在加密之前，负载均衡器发送到客户端的字节数。
incoming_tls_alert	负载均衡器从客户端处收到的 TLS 提醒的整数值（如果存在）。否则，该值将设置为 -。
chosen_cert_arn	提供给客户端的证书的 ARN。如果未发送有效的客户端 hello 消息，则此值设置为 -。
chosen_cert_serial	留待将来使用。此值始终设置为 -。
tls_cipher	与客户端协商的密码套件（采用 OpenSSL 格式）。如果 TLS 协商未完成，则此值设置为 -。
tls_protocol_version	与客户端协商的 TLS 协议（采用字符串格式）。可能的值为 <code>tlsv10</code> 、 <code>tlsv11</code> 、 <code>tlsv12</code> 和 <code>tlsv13</code> 。如果 TLS 协商未完成，则此值设置为 -。
tls_named_group	留待将来使用。此值始终设置为 -。
domain_name	客户端 hello 消息中的 <code>server_name</code> 扩展名的值。此值是 URL 编码的。如果未发送有效的客户端 hello 消息或扩展名不存在，则此值设置为 -。
alpn_fe_protocol	与客户端协商的应用程序协议，采用字符串格式。可能的值为 <code>h2</code> 、 <code>http/1.1</code> 和 <code>http/1.0</code> 。如果 TLS 侦听器中未配置 ALPN 策略、找不到匹配协议或者没有发送有效的协议列表，则此值设置为 -。
alpn_be_protocol	与目标协商的应用程序协议，采用字符串格式。可能的值为 <code>h2</code> 、 <code>http/1.1</code> 和 <code>http/1.0</code> 。如果 TLS 侦听器中未配置 ALPN 策略、找不到匹配协议或者没有发送有效的协议列表，则此值设置为 -。
alpn_client_preference_list	客户端 hello 消息中 <code>application_layer_protocol_negotiation</code> 扩展的值。此值是 URL 编码的。每个协议都用双引号括起来，协议用逗号分隔。如果在 TLS 侦听器中未配置 ALPN 策略、未发送有效的客户端 hello 消息或扩展名不存在，则此值设置为 -。字符串长度在超过 256 个字节时将会截断。

字段	描述
tls_connection_creation_time	在 TLS 连接开始时记录的时间（采用 ISO 8601 格式）。

## 示例日志条目

以下是示例日志条目。请注意，文本以多行形式显示只是为了更方便阅读。

以下是没有 ALPN 策略的 TLS 侦听器的示例。

```
tls 2.0 2018-12-20T02:59:40 net/my-network-loadbalancer/c6e77e28c25b2234
g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
- - - 2018-12-20T02:59:30
```

以下是具有 ALPN 策略的 TLS 侦听器的示例。

```
tls 2.0 2020-04-01T08:51:42 net/my-network-loadbalancer/c6e77e28c25b2234
g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
h2 h2 "h2", "http/1.1" 2020-04-01T08:51:20
```

## 存储桶要求

在启用访问日志记录时，您必须为访问日志指定 S3 存储桶。该存储桶可由与拥有负载均衡器的账户不同的账户拥有。存储桶必须满足以下要求。

### 要求

- 存储桶必须位于与负载均衡器相同的区域中。
- 您指定的前缀不得包含 AWSLogs。我们会在您指定的存储桶名称和前缀后添加以 AWSLogs 开头的文件名部分。

- 存储桶必须具有授予将访问日志写入存储桶的权限的存储桶策略。存储桶策略是 JSON 语句的集合，这些语句以访问策略语言编写，用于为存储桶定义访问权限。以下是示例策略。

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryWrite",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::my-bucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": ["012345678912"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:us-east-1:012345678912:*"]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-bucket/AWSLogs/account-ID/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["012345678912"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:us-east-1:012345678912:*"]
        }
      }
    }
  ]
}
```



```
}
```

在之前的策略中，对于 `aws:SourceAccount`，请指定将日志传送到此存储桶的账号列表。对于 `aws:SourceArn`，请按 `arn:aws:logs:source-region:source-account-id:*` 格式指定生成日志的资源 ARN 列表。

## 加密

您可以使用下列任何一种方式为 Amazon S3 访问日志存储桶启用服务器端加密：

- Amazon S3 托管式密钥 (SSE-S3)
- AWS KMS 存储在 AWS Key Management Service (SSE-KMS) 中的密钥†

† 对于 Network Load Balancer 访问日志，您无法使用 AWS 托管密钥，必须使用客户托管密钥。

有关更多信息，请参阅 [Amazon S3 用户指南中的指定 Amazon S3 加密 \(SSE-S3\) 和使用 AWS KMS \(SSE-KMS\) 指定服务器端加密](#)。

密钥策略必须允许服务对日志进行加密和解密。以下是示例策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
  ]
}
```

## 启用访问日志记录

在为负载均衡器启用访问日志记录时，您必须指定负载均衡器将在其中存储日志的 S3 桶。请确保您拥有此桶，且配置了此桶的必要桶策略。有关更多信息，请参阅 [存储桶要求](#)。

### 使用控制台启用访问日志记录

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择您的负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在编辑负载均衡器属性页面上，执行以下操作：
  - a. 对于监控，打开访问日志。
  - b. 选择浏览 S3 并选中要使用的桶。或者，输入 S3 桶的位置，包括任何前缀。
  - c. 选择保存更改。

要启用访问日志记录，请使用 AWS CLI

使用 [modify-load-balancer-attributes](#) 命令。

## 禁用访问日志记录

您随时可为您的负载均衡器禁用访问日志记录。在禁用访问日志记录后，您的访问日志将在 S3 存储桶中保留，直至您将其删除。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的 [使用存储桶](#)。

### 使用控制台禁用访问日志记录

1. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择负载均衡器。
3. 选择您的负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 对于监控，关闭访问日志。
6. 选择保存更改。

要禁用访问日志记录，请使用 AWS CLI

使用 [modify-load-balancer-attributes](#) 命令。

## 处理访问日志文件

访问日志文件是压缩文件。如果您使用 Amazon S3 控制台打开这些文件，则将其进行解压缩，并将显示信息。如果您下载这些文件，则必须对其进行解压才能查看信息。

如果您的网站上有大量需求，则负载均衡器可以生成包含大量数据的日志文件 (以 GB 为单位)。您可能无法使用处理来 line-by-line 处理如此大量的数据。因此，您可能必须使用提供并行处理解决方案的分析工具。例如，您可以使用以下分析工具分析和处理访问日志：

- Amazon Athena 是一种交互式查询服务，让您能够轻松使用标准 SQL 分析 Amazon S3 中的数据。有关更多信息，请参阅《Amazon Athena 用户指南》中的[查询 Network Load Balancer 日志](#)。
- [Loggly](#)
- [Splunk](#)
- [Sumo Logic](#)

## 使用 AWS CloudTrail记录 Network Load Balancer 的 API 调用

Elastic Load Balancing 与 AWS CloudTrail 集成，该服务提供用户、角色或 Elastic Load Balancing 中执行的操作的记录。CloudTrail 将 Elastic Load Balancing 的所有 API 调用捕获为事件。捕获的调用包括来自的调用 AWS Management Console 以及对 Elastic Load Balancing API 操作的代码调用。如果您创建跟踪，则可以将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Elastic Load Balancing 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的“事件历史记录”中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 Elastic Load Balancing 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅[AWS CloudTrail 用户指南](#)。

## 在 Elastic Load Balancing CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。在 Elastic Load Balancing 中发生活动时，该活动会与其他 CloudTrail AWS 服务 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅[使用事件历史查看 CloudTrail 事件](#)。

要持续记录您的事件 AWS 账户，包括 Elastic Load Balancing 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪

将应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送到您指定的 Simple Storage Service ( Amazon S3 ) 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅以下内容：

- [创建跟踪记录概述](#)
- [CloudTrail 支持的服务和集成](#)
- [配置 Amazon SNS 通知 CloudTrail](#)
- [接收来自多个区域的 CloudTrail 日志文件](#)和[接收来自多个账户的 CloudTrail 日志文件](#)

网络负载均衡器的所有弹性负载平衡操作均由 [Elastic Load Balancing API 参考版本 2015-12-01](#) 记录 CloudTrail 并记录在案。例如，调用 `CreateLoadBalancer` 和 `DeleteLoadBalancer` 操作会在 CloudTrail 日志文件中生成条目。

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根凭证还是用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅[CloudTrail 用户身份元素](#)。

## 了解 Elastic Load Balancing 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序出现。

日志文件包括您的 AWS 账户所有 AWS API 调用的事件，而不仅仅是 Elastic Load Balancing API 调用。您可通过检查是否有包含值 `elasticloadbalancing.amazonaws.com` 的 `eventSource` 元素来查找对 Elastic Load Balancing API 的调用。要查看特定操作（如 `CreateLoadBalancer`）的记录，请检查是否有具有操作名称的 `eventName` 元素。

以下是 Elastic Load Balancing 的示例 CloudTrail 日志记录，该用户创建了网络负载均衡器，然后使用 `awscli` 将其删除。您可以使用 `userAgent` 元素标识 CLI。可使用 `eventName` 元素标识请求的 API 调用。有关用户 (Alice) 的信息可在 `userIdentity` 元素中找到。

## Example 示例 : CreateLoadBalancer

```
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2016-04-01T15:31:48Z",
  "eventSource": "elasticloadbalancing.amazonaws.com",
  "eventName": "CreateLoadBalancer",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "198.51.100.1",
  "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
  "requestParameters": {
    "subnets": ["subnet-8360a9e7","subnet-b7d581c0"],
    "securityGroups": ["sg-5943793c"],
    "name": "my-load-balancer",
    "scheme": "internet-facing",
    "type": "network"
  },
  "responseElements": {
    "loadBalancers": [{
      "type": "network",
      "ipAddressType": "ipv4",
      "loadBalancerName": "my-load-balancer",
      "vpcId": "vpc-3ac0fb5f",
      "securityGroups": ["sg-5943793c"],
      "state": {"code": "provisioning"},
      "availabilityZones": [
        {"subnetId": "subnet-8360a9e7", "zoneName": "us-west-2a"},
        {"subnetId": "subnet-b7d581c0", "zoneName": "us-west-2b"}
      ],
      "dnsName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
      "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
      "createdTime": "Apr 11, 2016 5:23:50 PM",
      "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0",
      "scheme": "internet-facing"
    }]
  }
}
```

```

},
"requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
"eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
"eventType": "AwsApiCall",
"apiVersion": "2015-12-01",
"recipientAccountId": "123456789012"
}

```

### Example 示例 : DeleteLoadBalancer

```

{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2016-04-01T15:31:48Z",
  "eventSource": "elasticloadbalancing.amazonaws.com",
  "eventName": "DeleteLoadBalancer",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "198.51.100.1",
  "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 boto3/1.4.1",
  "requestParameters": {
    "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0"
  },
  "responseElements": null,
  "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
  "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
  "eventType": "AwsApiCall",
  "apiVersion": "2015-12-01",
  "recipientAccountId": "123456789012"
}

```

# 排查您的 Network Load Balancer 问题

以下信息可帮助您排查与 Network Load Balancer 相关的问题。

## 已注册目标未处于可用状态

如果目标进入 InService 状态所花费的时间超过预期，则该目标可能无法通过运行状况检查。您的目标未处于可用状态，除非通过一次运行状况检查。有关更多信息，请参阅 [目标组的运行状况检查](#)。

验证您的实例是否通过运行状况检查，然后检查以下各项：

### 安全组不允许流量

与实例关联的安全组必须允许来自负载均衡器的使用运行状况检查端口和运行状况检查协议的流量。有关更多信息，请参阅 [目标安全组](#)。

### 网络访问控制列表 (ACL) 不允许流量

与实例子网以及负载均衡器子网关联的网络 ACL 必须允许来自负载均衡器的流量和运行状况检查。有关更多信息，请参阅 [网络 ACL](#)。

## 请求未路由至目标

检查以下各项：

### 安全组不允许流量

与实例相关联的安全组必须允许侦听器端口上来自客户端 IP 地址 (如果目标通过实例 ID 指定) 或负载均衡器节点 (如果目标通过 IP 地址指定) 的流量。有关更多信息，请参阅 [目标安全组](#)。

### 网络访问控制列表 (ACL) 不允许流量

与 VPC 的子网关联的网络 ACL 必须允许负载均衡器和目标在侦听器端口上双向通信。有关更多信息，请参阅 [网络 ACL](#)。

### 目标处于未启用的可用区中

如果您在可用区中注册目标但未启用该可用区，这些已注册目标将无法从负载均衡器接收流量。

### 实例位于对等的 VPC 中

如果您在与负载均衡器 VPC 对等的 VPC 中拥有实例，则必须通过 IP 地址而不是实例 ID 将这些实例注册到负载均衡器。

## 目标接收比预期更多的运行状况检查请求

Network Load Balancer 的运行状况检查是分布式的，使用共识机制来确定目标运行状况。因此，目标可以接收的运行状况检查数量可以超过通过 `HealthCheckIntervalSeconds` 设置配置的数量。

## 目标接收比预期更少的运行状况检查请求

检查是否启用了 `net.ipv4.tcp_tw_recycle`。已知此设置会导致负载均衡器出现问题。`net.ipv4.tcp_tw_reuse` 设置被认为是更安全的替代设置。

## 运行状况不佳的目标收到来自负载均衡器的请求

当所有注册的目标皆运行状况不佳时，就会发生这种情况。如果至少有一个运行正常的已注册目标，则网络负载均衡器仅将请求路由到运行正常的已注册目标。

如果只有运行状况不佳的已注册目标，则网络负载均衡器会将请求路由到所有已注册目标（即失效时开放模式）。当所有目标都运行状况不佳且相应的可用区没有运行正常的目标可供发送请求时，网络负载均衡器会执行此操作，而不是从 DNS 中删除所有 IP 地址。

## 由于主机标头不匹配，目标无法通过 HTTP 或 HTTPS 运行状况检查

运行状况检查请求中的 HTTP 主机标头包含负载均衡器节点和侦听器端口的 IP 地址，但不包含目标和运行状况检查端口的 IP 地址。如果要通过主机标头映射传入请求，则必须确保运行状况检查与任何 HTTP 主机标头匹配。另一种选择是在其他端口上添加单独的 HTTP 服务，并配置目标组，改为使用该端口进行运行状况检查。或者，可以考虑使用 TCP 运行状况检查。

## 无法将安全组与网络负载均衡器关联

如果创建网络负载均衡器时没有关联安全组，则在创建后将无法关联安全组。您只能在创建时将安全组与负载均衡器相关联，或将安全组与最初使用安全组创建的现有负载均衡器相关联。

## 无法删除所有安全组

如果创建网络负载均衡器时关联了安全组，则必须始终至少有一个与之关联的安全组。您不能从负载均衡器中同时删除所有安全组。



## TCP\_ELB\_Reset\_Count 指标升高

对于客户端通过网络负载均衡器发出的每个 TCP 请求，都将跟踪该连接的状态。如果客户端或目标通过连接发送数据的间隔超过空闲超时期限，则连接将关闭。如果客户端或目标在空闲超时期限后发送数据，则会收到一个 TCP RST 数据包，以指示连接不再有效。此外，如果目标运行不正常，除非运行不正常的目标触发了负载均衡器故障断开，否则负载均衡器会为关联到目标的客户端连接上收到的数据包发送 TCP RST。

如果您在 UnhealthyHostCount 指标升高之前或之时看到 TCP\_ELB\_Reset\_Count 指标出现峰值，则可能是发送了 TCP RST 数据包，因为目标开始失败但尚未被标记为运行不良。如果您在 TCP\_ELB\_Reset\_Count 中看到持续升高且目标未被标记为运行不良，则可以查看 VPC 流日志，以便客户端发送与过期流相关的数据。

## 从目标到其负载均衡器的请求连接超时

检查目标组是否启用了客户端 IP 保留。启用客户端 IP 保留后，不支持 NAT 环回（也称为发夹转换）。如果实例是它注册到的负载均衡器的客户端，且它启用了客户端 IP 保留，则连接仅在请求路由到不同的实例时才会成功。如果请求路由到发送请求的同一个实例，连接会超时，因为源地址和目的地 IP 地址相同。

如果实例必须将请求发送到它注册到的负载均衡器，请执行下列操作之一：

- 禁用客户端 IP 保留。
- 确保必须相互通信的容器位于不同的容器实例上。

## 当将目标移到 Network Load Balancer 时，性能会下降

Classic Load Balancer 和 Application Load Balancer 都使用多路复用连接，但 Network Load Balancer 不使用。因此，您的目标可能会在 Network Load Balancer 后面收到更多的 TCP 连接。请确保您的目标准备好处理它们可能会收到的连接请求量。

## 连接时出现端口分配错误 AWS PrivateLink

如果您的 Network Load Balancer 与 VPC 终端节点服务关联，则它可以支持到每个唯一目标（IP 地址和端口）的 55,000 个并发连接或每分钟大约 55,000 个连接。如果连接数超过该值，则会增大出现端口分配错误的几率。可以使用 PortAllocationErrorCount 指标跟踪端口分配错误。要修复端

口分配错误，请将更多目标添加到目标组。有关更多信息，请参阅 [CloudWatch 您的 Network Load Balancer 的指标](#)。

## 启用客户端 IP 保留时发生间歇性连接失败

如果启用客户端 IP 保留，则可能会遇到与目标上观察到的套接字重用相关的 TCP/IP 连接限制。如果客户端或客户端前面的 NAT 设备在同时连接到多个负载均衡器节点时使用相同的源 IP 地址和源端口，则可能会出现这些连接限制。如果负载均衡器将这些连接路由到同一个目标，则这些连接对目标来说似乎是来自同一源套接字，从而导致连接错误。当发生这种情况时，客户端可能会重试（如果连接失败）或重新连接（如果连接中断）。您可以通过增加源临时端口的数量或增加负载均衡器的目标数来减少此类连接错误。您可以通过禁用客户端 IP 保留或禁用跨区域负载均衡来防止此类连接错误。

此外，启用客户端 IP 保留后，如果连接到 Network Load Balancer 的客户端也连接到负载均衡器后面的目标，则连接可能会失败。要解决此问题，您可以在受影响的目标组上禁用客户端 IP 保留。或者，让您的客户端仅连接到 Network Load Balancer，或者仅连接到目标，但不能同时连接到此两者。

## TCP 连接延迟

启用跨区负载均衡和客户端 IP 保留时，连接到同一负载均衡器上不同 IP 的客户端可能会路由到同一个目标。如果客户端对这两个连接使用相同的源端口，则目标将收到看似重复的连接，这可能导致连接错误和因建立新连接而导致 TCP 延迟。您可以通过禁用跨区负载均衡来防止此类连接错误。有关更多信息，请参阅 [跨可用区负载均衡](#)。

## 预置负载均衡器时可能出现故障

Network Load Balancer 在预置时可能失败的原因之一是您使用已在其他地方指定或分配的 IP 地址（例如，为 EC2 实例分配的辅助 IP 地址）。此 IP 地址阻止设置负载均衡器，其状态为 failed。您可以通过取消分配关联的 IP 地址并重试创建过程来解决此问题。

## DNS 名称解析包含的 IP 地址少于已启用的可用区

理想情况下，可用区中至少有一台运行正常的主机时，网络负载均衡器会为每个已启用的可用区提供一个 IP 地址。特定可用区中没有运行正常的主机并且禁用了跨区域负载均衡时，系统将从 DNS 中删除此可用区的相应网络负载均衡器的 IP 地址。

例如，假设您的网络负载均衡器启用了三个可用区，则所有可用区都至少有一个运行正常的已注册目标实例。

- 如果可用区 A 中的已注册目标实例运行状况不佳，则系统将从 DNS 中删除网络负载均衡器的可用区 A 的相应 IP 地址。
- 如果任意两个已启用的可用区没有运行正常的已注册目标实例，则系统将从 DNS 中删除网络负载均衡器的相应两个 IP 地址。
- 如果在所有已启用的可用区中没有运行正常的已注册目标实例，则系统会启用失效时开放模式，并且 DNS 将在结果中提供来自三个已启用可用区的所有 IP 地址。

## 使用资源图对不健康的目标进行故障排除

如果您的 Network Load Balancer 目标未通过运行状况检查，则可以使用资源图查找不健康的目标并根据失败原因代码采取措施。有关更多信息，请参阅 [Network Load Balancer 资源地图](#)。

资源地图提供两个视图：概述和不健康的目标地图。默认情况下，“概述”处于选中状态，并显示您的负载均衡器的所有资源。选择“不健康的目标地图”视图将仅显示与 Network Load Balancer 关联的每个目标组中的不健康目标。

### Note

必须启用“显示资源详细信息”，才能查看资源图中所有适用资源的运行状况检查摘要和错误消息。如果未启用，则必须选择每个资源才能查看其详细信息。

目标组列显示每个目标组的健康和不健康目标的摘要。这可以帮助确定是所有目标都未通过运行状况检查，还是只有特定目标失败。如果目标组中的所有目标都未通过运行状况检查，请检查目标组的运行状况检查设置。选择目标群组的名称，在新选项卡中打开其详情页面。

“目标”列显示每个目标的 targetID 和当前运行状况检查状态。当目标运行状况不佳时，将显示运行状况检查失败原因代码。当单个目标未通过运行状况检查时，请验证该目标是否有足够的资源。选择目标的 ID，在新选项卡中打开其详情页面。

选择“导出”后，您可以选择将网络负载均衡器资源地图的当前视图导出为 PDF。

验证您的实例是否未通过运行状况检查，然后根据失败原因代码检查以下问题：

- 不正常：请求超时
  - 验证与您的目标关联的安全组和网络访问控制列表 (ACL) 以及 Network Load Balancer 是否阻塞连接。
  - 验证目标是否有足够的可用容量来接受来自网络负载均衡器的连接。

- 可以在每个目标的应用程序日志中查看网络负载均衡器的运行状况检查响应。有关更多信息，请参阅 [Health check 原因代码](#)。
- 不健康：FailedHealthChecks
- 验证目标是否在监听运行状况检查端口上的流量。

#### 使用 TLS 侦听器时

您可以选择使用哪种安全策略进行前端连接。用于后端连接的安全策略是根据使用的前端安全策略自动选择的。

- 如果您的 TLS 侦听器对前端连接使用 TLS 1.3 安全策略，则该ELBSecurityPolicy-TLS13-1-0-2021-06安全策略将用于后端连接。
  - 如果您的 TLS 侦听器未对前端连接使用 TLS 1.3 安全策略，则该ELBSecurityPolicy-2016-08安全策略将用于后端连接。
- 有关更多信息，请参阅[安全策略](#)。

- 验证目标是否按照安全策略指定的正确格式提供了服务器证书和密钥。
- 验证目标是否支持一个或多个匹配的密码，以及 Network Load Balancer 提供的用于建立 TLS 握手的协议。

## Network Load Balancer 的配额

对于每项 AWS 服务，您的 AWS 账户都具有默认配额（以前称为限制）。除非另有说明，否则，每个配额是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。

要查看 Network Load Balancer 的配额，请打开 [Service Quotas 控制台](#)。在导航窗格中，选择 AWS 服务，然后选择 Elastic Load Balancing（弹性负载均衡）。您也可以对 Elastic Load Balancing 使用 [describe-account-limits](#) (AWS CLI) 命令。

要请求提高配额，请参阅 Service Quotas 用户指南中的 [请求增加配额](#)。如果 Service Quotas 中尚未提供配额，请使用 [Elastic Load Balancing 限制增加表单](#)。

### 负载均衡器

您的 AWS 账户 具有以下与网络负载均衡器相关的配额。

名称	默认值	可调整
每个 Network Load Balancer 的证书数	25	<a href="#">是</a>
每个 Network Load Balancer 的侦听器数	50	否
每个 VPC 的 Network Load Balancer ENI 数	1,200 <sup>1</sup>	<a href="#">是</a>
每个区域的 Network Load Balancer 数	50	<a href="#">是</a>
每个 Network Load Balancer 每个操作的目标组数	1	否
每个 Network Load Balancer 每个可用区的目标数	500 <sup>2, 3</sup>	<a href="#">是</a>
每个 Network Load Balancer 的目标数	3,000 <sup>3</sup>	<a href="#">是</a>

<sup>1</sup> 每个 Network Load Balancer 在每个区域使用一个网络接口。配额在 VPC 级别设置。共享子网或 VPC 时，所有租户的使用量都会计算在内。

<sup>2</sup> 如果一个目标注册了 N 个目标组，则它会针对此限制计为 N 个目标。如果禁用跨区域负载平衡，则作为网络负载均衡器目标的每个应用程序负载均衡器都计为 50 个目标；如果启用跨区域负载平衡，则计为 100 个目标。

<sup>3</sup> 如果启用了跨可用区负载均衡，则每个负载均衡器的最大目标数为 500，不受可用区数量的影响。

## 目标组

以下配额适用于目标组。

名称	默认值	可调整
每个区域的目标组数	3,000 <sup>1</sup>	<a href="#">是</a>
每个区域每个目标组的目标数 (实例或 IP 地址)	1000	<a href="#">是</a>
每个区域每个目标组的目标数 (Application Load Balancer)	1	否

<sup>1</sup> 此配额由 Application Load Balancer 和 Network Load Balancer 共享。

# Network Load Balancer 的文档历史记录

下表介绍了网络负载均衡器的版本。

变更	说明	日期
<a href="#">RSA 3072 位和 ECDSA 256/384/521 位证书</a>	此版本增加了对 RSA 3072 位证书以及通过 (ACM) 进行的 Elliptic Curve 数字签名算法 (ECDSA) 256、384 和 521 位证书的支持。AWS Certificate Manager	2024 年 1 月 19 日
<a href="#">FIPS 140-3 TLS 终止</a>	此版本添加了在终止 TLS 连接时使用 FIPS 140-3 加密模块的安全策略。	2023 年 11 月 20 日
<a href="#">区域 DNS 亲和力</a>	此版本增加了对客户端解析负载均衡器 DNS 以接收与其所在可用区 (AZ) 相同的 IP 地址的支持。	2023 年 10 月 12 日
<a href="#">禁用不健康的目标连接终止功能</a>	此版本增加了对与未通过运行状况检查的目标保持活动连接的支持。	2023 年 10 月 12 日
<a href="#">默认 UDP 连接终止</a>	此版本增加了默认情况下在取消注册超时结束时终止 UDP 连接的支持。	2023 年 10 月 12 日
<a href="#">使用 IPv6 注册目标</a>	此版本增加了在通过 IPv6 寻址时将实例注册为目标的支持。	2023 年 10 月 2 日
<a href="#">网络负载均衡器的安全组</a>	此版本增加了支持功能，可在创建时将安全组与网络负载均衡器关联。	2023 年 8 月 10 日

<a href="#">目标组运行状况</a>	此版本增加了对配置必须运行状况良好的目标数量下限或最低百分比以及在未达到阈值时负载均衡器采取哪些操作的支持。	2022 年 11 月 17 日
<a href="#">运行状况检查配置</a>	此版本提供了对运行状况检查配置的改进。	2022 年 11 月 17 日
<a href="#">跨可用区负载均衡</a>	此版本增加了对在目标组级别配置跨区域负载平衡的支持。	2022 年 11 月 17 日
<a href="#">IPv6 目标组</a>	此版本增加了对为网络负载均衡器配置 IPv6 目标组的支持。	2021 年 11 月 23 日
<a href="#">IPv6 内部负载均衡器</a>	此版本增加了对为网络负载均衡器配置 IPv6 目标组的支持。	2021 年 11 月 23 日
<a href="#">TLS 1.3</a>	此版本增加了支持 TLS 1.3 版的安全策略。	2021 年 10 月 14 日
<a href="#">作为目标的 Application Load Balancer</a>	此版本增加了对将 Application Load Balancer 配置为 Network Load Balancer 目标的支持。	2021 年 9 月 27 日
<a href="#">客户端 IP 保留</a>	此版本增加了对配置客户端 IP 保留的支持。	2021 年 2 月 4 日
<a href="#">支持 TLS 1.2 版的 FS 安全策略</a>	此版本增加了支持 TLS 1.2 版的向前保密 (FS) 安全策略。	2020 年 11 月 24 日
<a href="#">双堆栈模式</a>	此版本增加了对双堆栈模式的支持，允许客户端使用 IPv4 地址和 IPv6 地址连接到负载均衡器。	2020 年 11 月 13 日
<a href="#">取消注册时连接终止</a>	此版本增加了对取消注册超时结束后关闭取消注册目标连接的支持。	2020 年 11 月 13 日



<a href="#">ALPN 策略</a>	此版本增加了对应用层协议协商 (ALPN) 首选项列表的支持。	2020 年 5 月 27 日
<a href="#">粘性会话</a>	此版本根据源 IP 地址和协议增加了对粘性会话的支持。	2020 年 2 月 28 日
<a href="#">共享子网</a>	此版本增加了对指定子网的支持，此类子网是由其他 AWS 账户与您所共享。	2019 年 11 月 26 日
<a href="#">私有 IP 地址</a>	通过此版本，您可以在为内部负载均衡器启用可用区时，从您指定的子网的 IPv4 地址范围中提供私有 IP 地址。	2019 年 11 月 25 日
<a href="#">添加子网</a>	此版本增加了在创建负载均衡器后启用其他可用区的支持。	2019 年 11 月 25 日
<a href="#">FS 的安全策略</a>	此版本增加了对另外三个预定义的前向保密安全策略的支持。	2019 年 10 月 8 日
<a href="#">SNI 支持</a>	此版本增加了对服务器名称指示 (SNI) 的支持。	2019 年 9 月 12 日
<a href="#">UDP 协议</a>	此版本增加了对 UDP 协议的支持。	2019 年 6 月 24 日
<a href="#">在新地区可用</a>	此版本增加了对亚太地区 ( 大阪 ) 区域的网络负载均衡器的支持。	2019 年 6 月 12 日
<a href="#">TLS 协议</a>	此版本增加了对 TLS 协议的支持。	2019 年 1 月 24 日
<a href="#">跨可用区负载均衡</a>	此版本增加了对启用跨区域负载均衡的支持。	2018 年 2 月 22 日

[代理协议](#)

此版本增加了对启用代理协议的支持。

2017 年 11 月 17 日

[IP 地址即目标](#)

此版本增加了将 IP 地址注册为目标的支持。

2017 年 9 月 21 日

[新负载均衡器类型](#)

此版本的 Elastic Load Balancing 引入了网络负载均衡器。

2017 年 9 月 7 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。