Elastic Load Balancing

Network Load Balancer

Elastic Load Balancing: Network Load Balancer

Table of Contents

什么是网络负载均衡器？

Elastic Load Balancing 支持以下类型的负载均衡器：Application Load Balancer、Network Load Balancer 和 Classic Load Balancer。本指南讨论 Network Load Balancer。有关其他负载均衡器的更多信息，请参阅 Application Load Balancer 用户指南 和 Classic Load Balancer 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。

每个 目标组 使用您指定的 TCP 协议和端口号，再将请求路由到一个或多个注册目标，例如 EC2 实例。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，请参阅以下文档：

- 负载均衡器 (p. 9)
- 侦听器 (p. 16)
- 目标组 (p. 24)

网络负载均衡器 概述

网络负载均衡器在开放系统互连 (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已注册目标之间分配流量。有关更多信息，请参阅 可用区 (p. 10)。

如果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，那么这将提高应用程序的容错能力。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。如果一个客户端不遵守生存时间 (TTL) 而将请求发送到已从 DNS 删除的 IP 地址，则请求会失败。

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 为您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，应指定其目标类型，这决定您是否通过实例 ID 或 IP 地址注册目标。如果您使用实例 ID 注册目标，则客户端的源 IP 地址将保留并提供给您的应用程序。如果您使用 IP 地址注册目标，则源 IP 地址是负载均衡器节点的私有 IP 地址。

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。Elastic Load Balancing 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。Elastic Load Balancing 能够自动扩展以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 Elastic Load Balancing 用户指南 中的 Elastic Load Balancing 工作原理。

从 传统负载均衡器迁移的好处

使用 网络负载均衡器 而非 传统负载均衡器 有下列好处：

- 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。
- 支持单独监控每个服务的运行状况，因为运行状况检查是在目标组级别定义的，而且许多 Amazon CloudWatch 指标也是在目标组级别报告的。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。

有关每个负载均衡器类型支持的功能的更多信息，请参阅 Elastic Load Balancing 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 Balancer 入门 (p. 3)
- 教程：使用 AWS CLI 创建 网络负载均衡器 (p. 6)

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 Balancer 入门

本教程介绍通过 AWS 管理控制台（基于 Web 的界面）创建 Network Load Balancer 的实际操作。要创建第一个网络负载均衡器，请完成以下步骤。

任务

或者，要创建 应用程序负载均衡器，请参阅 Application Load Balancer 用户指南 中的 Application Load Balancer 入门。要创建 传统负载均衡器，请参阅 Classic Load Balancer 用户指南 中的创建 Classic 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 (p. 32)。

步骤 1：选择负载均衡器类型

Elastic Load Balancing 支持三种负载均衡器。在本教程中，您将创建一个网络负载均衡器。

创建集群网络负载均衡器

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航栏上，选择您的负载均衡器的区域。请确保选择用于 EC2 实例的同一区域。
3. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
4. 选择 Create Load Balancer。
5. 对于 网络负载均衡器，选择 Create (创建)。

步骤 2：配置负载均衡器和侦听器

在 Configure Load Balancer 页面上，完成以下过程。

配置负载均衡器和侦听器

1. 对于 Name，键入负载均衡器的名称。

在区域的 Application Load Balancer 和 Network Load Balancer 集内，网络负载均衡器 的名称必须唯一，最多可以有 32 个字符，只能包含字母数字字符和连字符，不能以连字符开头或结尾，并且不能以“internal-”开头。

2. 对于 Scheme，保留默认值 internet-facing。
3. 对于 Listeners，保留默认值，默认侦听器负责接收端口 80 上的 TCP 流量。
4. 对于 Availability Zones (可用区)，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，AWS 会针对其可用区从子网中为每个负载均衡器节点分配 IPv4 地址。另外，如果您创建面向 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。
5. 选择 Next: Configure Routing。

步骤 3：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。在 Configure Routing 页面上，完成以下过程。

配置目标组

1. 对于 Target group，保留默认值 New target group。
2. 对于 Name，键入新目标组的名称。
3. 将 Protocol 保留为“TCP”，Port 为“80”，Target type 为“instance”。
4. 对于 Health checks，保留默认协议。
5. 选择 Next: Register Targets。

步骤 4：向您的目标组注册目标

在 Register Targets 页面上，完成以下过程。

向目标组注册目标

1. 对于 Instances，选择一个或多个实例。
2. 保留默认端口 80，并选择 Add to registered。
3. 当您完成选择实例后，选择 Next: Review。

步骤 5：创建并测试您的负载均衡器

在创建负载均衡器之前，请检查您的设置。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。

创建并测试您的负载均衡器

1. 在 Review 页面上，选择 Create 。
2. 在您收到已成功创建负载均衡器的通知后，选择 Close。
3. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
4. 选择新创建的目标组。

5. 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。
6. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
7. 选择新创建的负载均衡器。
8. 选择 Description (描述) 并复制负载均衡器的 DNS 名称（例如，my-load-balancer-1234567890abcdef.elb.us-west-2.amazonaws.com.cn）。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 6：删除您的负载均衡器 (可选)

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。

删除您的负载均衡器

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择负载均衡器，然后选择 Actions 和 Delete。
4. 当系统提示进行确认时，选择 Yes, Delete。

教程：使用 AWS CLI 创建 网络负载均衡器

本教程介绍通过 AWS CLI 创建 Network Load Balancer 的实际操作。

开始前的准备工作

- 安装 AWS CLI，或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 命令行界面。
- 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)。
- 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 (p. 32)。

创建负载均衡器

要创建第一个负载均衡器，请完成以下步骤。

创建负载均衡器

1. 使用 create-load-balancer 命令创建负载均衡器，并为在其中启动实例的每个可用区指定公有子网。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-12345678
```

输出包含负载均衡器的 Amazon 资源名称 (ARN)，格式如下：

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

2. 使用 create-target-group 命令创建目标组，并指定用于 EC2 实例的相同 VPC：

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id
 vpc-12345678
```

输出包含目标组的 ARN，格式如下：

```
arn:aws-cn:elasticloadbalancing:us-west-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-12345678
 Id=i-23456789
```

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-cn:elasticloadbalancing:us-west-2:123456789012:listener/net/my-load-
balancer/1234567890123456/1234567890123456
```

5. (可选) 您可以使用此 describe-target-health 命令验证目标组的已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

在创建网络负载均衡器时，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-12345678,AllocationId=eipalloc-12345678
```

使用端口覆盖添加目标

如果您有一个微服务架构，它在单个实例上有多个服务，则每个服务在不同的端口上接受连接。您可以将实例注册到目标组多次，每次使用不同的端口进行注册。

使用端口覆盖添加目标

1. 使用 create-target-group 命令创建目标组：

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 \
--vpc-id vpc-12345678
```

2. 使用 register-targets 命令将您的实例注册到目标组。请注意，每个容器的实例 ID 相同，但端口不同。

```
aws elbv2 register-targets --target-group-arn targetgroup-arn  \
--targets Id=i-12345678,Port=80 Id=i-12345678,Port=766
```

3. 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
```

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 (p. 24)，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 (p. 16)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。

Network Load Balancer 通过 VPC 对等连接、AWS 托管 VPN 和第三方 VPN 解决方案支持来自客户端的连接。

内容

负载均衡器状态

负载均衡器可能处于下列状态之一：

`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`

负载均衡器无法设置。

负载均衡器属性

以下是负载均衡器属性：

`deletion_protection.enabled`

指示是否启用删除保护 (p. 10)。默认为 `false`。

`load_balancing.cross_zone.enabled`

指示是否启用了跨区域负载均衡 (p. 10)。默认为 `false`。

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。在创建网络负载均衡器之后，将无法为其启用或禁用可用区。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。

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。这将为您的负载均衡器提供静态 IP 地址。在创建负载均衡器之后，将无法为子网添加或更改弹性 IP 地址。

要求

- 您指定的子网必须具有至少 8 个可用 IP 地址。
- 无法指定由另一个 AWS 账户与您共享的子网。
- 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，并使用跨区域负载均衡将流量分发至受约束d 可用区中的目标。

跨区域负载均衡

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。如果您启用了跨区域负载均衡，则每个负载均衡器节点会在所有启用的可用区中的已注册目标之间分配流量。有关更多信息，请参阅 Elastic Load Balancing 用户指南 中的跨区域负载均衡。

使用控制台启用跨区域负载均衡

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择负载均衡器。
4. 选择 Description、Edit attributes。
5. 在编辑负载均衡器属性页面上，为跨区域负载均衡选择启用，然后选择保存。

使用 AWS CLI 启用跨区域负载均衡

使用带 `load_balancing.cross_zone.enabled` 属性的 modify-load-balancer-attributes 命令。

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. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择负载均衡器。
4. 选择 Description、Edit attributes。

5. 在编辑负载均衡器属性页面上，为删除保护选择启用，然后选择保存。

使用控制台禁用删除保护

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择负载均衡器。
4. 选择 Description、Edit attributes。
5. 在 Edit load balancer attributes 页面上，清除 Enable delete protection 并选择 Save。

使用 AWS CLI 启用或禁用删除保护

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 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。

对于 TCP 流，Elastic Load Balancing 将空闲超时值设为 350 秒。您不能修改此值。对于 TCP 侦听器，客户端或目标可以使用 TCP keepalive 数据包重置空闲超时。TCP keepalive 数据包不支持 TLS 侦听器。

虽然 UDP 无连接，但是负载均衡器将基于源和目标 IP 地址和端口保持 UDP 流状态，从而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。对于 UDP 流，Elastic Load Balancing 将空闲超时值设为 120 秒。

DNS 名称

每个网络负载均衡器都使用以下语法接收默认域名系统 (DNS) 名称：*name*-*id*.elb.*region*.amazonaws.com.cn。例如，my-load-balancer-1234567890abcdef.elb.us-west-2.amazonaws.com.cn。

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）创建一条别名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，您可以使用 Amazon Route 53 作为 DNS 服务。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.cn。

Linux 或 Mac

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

Windows

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

创建 网络负载均衡器

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。

要使用 AWS CLI 创建负载均衡器，请参阅教程：使用 AWS CLI 创建 网络负载均衡器 (p. 6)。

要使用 AWS 管理控制台创建负载均衡器，请完成以下任务。

任务

步骤 1：配置负载均衡器和侦听器

首先，为负载均衡器提供一些基本配置信息，如名称、网络及一个或多个侦听器。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 (p. 16)。

配置负载均衡器和侦听器

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择 Create Load Balancer。
4. 对于 网络负载均衡器，选择 Create (创建)。
5. 对于 Name，键入负载均衡器的名称。例如：**my-nlb**。
6. 对于 Scheme，面向 Internet 的负载均衡器将来自客户端的请求通过 Internet 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。
7. 对于 Listeners，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，修改协议或修改端口。选择 Add 添加另一个侦听器。
8. 对于 Availability Zones (可用区)，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。要将弹性 IP 地址与子网关联，请从 Elastic IP 选择一个地址。
9. 选择 Next: Configure Routing。

步骤 2：配置目标组

将目标 (例如 EC2 实例) 注册到目标组。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，侦听器规则负责将请求转发到目标组。有关更多信息，请参阅Network Load Balancer 的目标组 (p. 24)。

配置目标组

1. 对于 Target group，保留默认值 New target group。
2. 对于 Name，键入目标组的名称。
3. 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。
4. （可选）设置 Port (端口)。
5. 对于 Target type，选择 `instance` 通过实例 ID 指定目标，或选择 `ip` 通过 IP 地址指定目标。如果目标组协议是 UDP 或 TCP_UDP，您必须选择 `instance`。
6. 对于 Health checks，保留默认运行状况检查设置。
7. 选择 Next: Register Targets。

步骤 3：向目标组注册目标

可将 EC2 实例注册为目标组中的目标。

通过实例 ID 注册目标

1. 对于 Instances，选择一个或多个实例。
2. 保留默认实例侦听器端口，或键入一个新端口并选择 Add to registered。
3. 当您注册完实例后，选择 Next: Review。

通过 IP 地址注册目标

1. 对于每个要注册的 IP 地址，请执行以下操作：
   a. 对于 Network，如果 IP 地址来自目标组 VPC 的子网，则选择该 VPC。否则，请选择 Other private IP address。
   b. 对于 Availability Zone，选择一个可用区或选择 all。这将决定目标是只从指定可用区的负载均衡器节点接收流量，还是从所有启用的可用区接收流量。如果您要注册来自 VPC 的 IP 地址，则不会显示此字段。在这种情况下，会自动检测可用区。
   c. 对于 IP，键入地址。
   d. 对于 Port，键入端口。
   e. 选择 Add to list。
2. 在将 IP 地址添加到列表中后，选择 Next: Review。

步骤 4：创建负载均衡器

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。使用完负载均衡器之后，您可将其删除。有关更多信息，请参阅 删除 网络负载均衡器 (p. 14)。

创建负载均衡器

1. 在 Review 页面上，选择 Create 。
2. 创建负载均衡器之后，选择 Close。
3. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
4. 选择新创建的目标组。
5. 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。在至少一个实例的状态为正常后，便可测试负载均衡器。

网络负载均衡器的标签

使用标签可帮助您按各种标准对负载均衡器进行分类，例如按用途、所有者或环境。

您最多可以为每个负载均衡器添加多个标签。每个负载均衡器的标签键必须唯一。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

- 每个资源的最大标签数 — 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，因为它专为 AWS 使用预留。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. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择负载均衡器。
4. 选择 Tags、Add/Edit Tags，然后执行下列一个或多个操作：
   a. 要更新标签，请编辑 Key 和 Value 的值。
   b. 要添加新标签，请选择 Create Tag。对于 Key 和 Value，键入值。
   c. 要删除标签，请选择标签旁边的删除图标 (X)。
5. 完成更新标签后，选择 Save。

使用 AWS CLI 更新负载均衡器的标签

使用 add-tags 和 remove-tags 命令。

删除 网络负载均衡器

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 (p. 10)。

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 (p. 35)。

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别名记录，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。
2. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
3. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
4. 选择负载均衡器。
5. 依次选择 Actions 和 Delete。
6. 当系统提示进行确认时，选择 Yes, Delete。

使用 AWS CLI 删除负载均衡器

使用 delete-load-balancer 命令。

Network Load Balancer 的侦听器

在开始使用 网络负载均衡器 之前，您必须添加一个或多个侦听器。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。为侦听器定义的规则可以确定负载均衡器将请求路由到一个或多个目标组中的目标的方式。

有关更多信息，请参阅 Elastic Load Balancing 用户指南 中的请求路由。

内容

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 (p. 17)。

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。

可以将 WebSockets 与您的侦听器结合使用。

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。类型 3 之外的 ICMP 请求也被视为非预期流量。Network Load Balancer会删除非预期流量而不将其转发给任何目标。作为非预期流量的一部分的 TCP 数据包因 TCP 重置 (RST) 而被拒绝。

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 (p. 20)。

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，请参阅为网络负载均衡器创建目标组 (p. 28)。
- 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 (p. 18)。

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 (p. 16)。

使用控制台添加侦听器

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择负载均衡器，然后选择 Listeners。
4. 选择 Add listener (添加侦听器)。
5. 对于 Protocol : port (协议: 端口)，选择 TCP、UDP、TCP_UDP 或 TLS。保留默认端口或键入其他端口。
6. 对于 Default actions (默认操作)，选择 Add action (添加操作)、Forward to (转发至)，然后选择可用目标组。
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：
   - 如果使用 AWS Certificate Manager 创建或导入了证书，请选择 From ACM (来自 ACM) 并选择证书。
   - 如果使用 IAM 上传了证书，则选择 From IAM (来自 IAM) 并选择证书。
9. 选择 Save。
10. [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 (p. 21)。

使用 AWS CLI 添加侦听器

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。

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第一个密码。

Network Load Balancer 不支持 TLS 重新协商。

要创建 TLS 侦听器，请参阅添加侦听器 (p. 17)。要查看相关演示，请参阅 网络负载均衡器 上的 TLS 支持以及 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。

我们建议您使用 AWS Certificate Manager (ACM) 为负载均衡器创建证书。ACM 已与 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。

此外，还可以使用 TLS 工具创建证书签名请求 (CSR)，然后获取由 CA 签署的 CSR 以生成证书，并将证书导入 ACM，或将证书上传至 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。

> Important
>
> 您无法在网络负载均衡器上安装具有大于 2048 位的 RSA 密钥或 EC 密钥的证书。

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 (p. 21)。

如果在证书列表 (p. 18)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平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 (p. 21)。

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：

- 公有密钥算法 (ECDSA 优先于 RSA)
- 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 (p. 42)。

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 AWS Certificate Manager 提供、部署在负载均衡器上的证书可以自动续订。ACM 将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 (p. 22)。

您可以选择用于前端连接的安全策略。`ELBSecurityPolicy-2016-08` 安全策略始终用于后端连接。Network Load Balancer不支持自定义安全策略。

Elastic Load Balancing 为Network Load Balancer提供以下安全策略：

- `ELBSecurityPolicy-2016-08`
- `ELBSecurityPolicy-FS-2018-06`
- `ELBSecurityPolicy-TLS-1-2-2017-01`
- `ELBSecurityPolicy-TLS-1-2-Ext-2018-06`
- `ELBSecurityPolicy-TLS-1-1-2017-01`
- `ELBSecurityPolicy-2015-05`
- `ELBSecurityPolicy-TLS-1-0-2015-04`

建议将 `ELBSecurityPolicy-2016-08` 策略用于一般用途。如果需要向前保密 (FS)，可使用 `ELBSecurityPolicy-FS-2018-06` 策略。您可以使用 `ELBSecurityPolicy-TLS` 策略之一，以满足需要禁用特定 TLS 协议版本的合规性和安全标准，或者支持需要已弃用密码的旧客户端。只有一小部分 Internet 客户端需要 TLS 版本 1.0。要查看针对负载均衡器的请求的 TLS 协议版本，请为负载均衡器启用访问日志记录并查看访问日志。有关更多信息，请参阅访问日志 (p. 41)。

下表描述了为Network Load Balancer定义的安全策略。

安全策略	2016-08 *	FS-2018-0	TLS-1-2	TLS-1-2-Ext	TLS-1-1	TLS-1-0 †
TLS 协议						
Protocol-TLSv1	♦	♦				♦
Protocol-TLSv1.1	♦	♦			♦	♦
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	2016-08 *	FS-2018-0	TLS-1-2	TLS-1-2-Ext	TLS-1-1	TLS-1-0 †
ECDHE-ECDSA-AES128-SHA	♦	♦		♦	♦	♦
ECDHE-RSA-AES128-SHA	♦	♦		♦	♦	♦
ECDHE-ECDSA-AES256- GCM-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES256- GCM-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES256-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA	♦	♦		♦	♦	♦
ECDHE-ECDSA-AES256-SHA	♦	♦		♦	♦	♦
AES128-GCM-SHA256	♦		♦	♦	♦	♦
AES128-SHA256	♦		♦	♦	♦	♦
AES128-SHA	♦			♦	♦	♦
AES256-GCM-SHA384	♦		♦	♦	♦	♦
AES256-SHA256	♦		♦	♦	♦	♦
AES256-SHA	♦			♦	♦	♦
DES-CBC3-SHA						♦

*`ELBSecurityPolicy-2016-08` 和 `ELBSecurityPolicy-2015-05` 安全策略是相同的。

† 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，否则请勿使用此安全策略。

要使用 AWS CLI 查看负载均衡器的安全策略的配置，请使用 describe-ssl-policies 命令。

更新网络负载均衡器的侦听器

您可以更新侦听器端口、侦听器协议或默认侦听器规则。

默认侦听器规则将请求转发到指定的目标组。

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。

使用控制台更新侦听器

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择负载均衡器，然后选择 Listeners。
4. 选中该侦听器的复选框，然后选择 Edit (编辑)。
5. （可选）更改 Protocol: port (协议: 端口) 的指定值。

6. （可选）单击铅笔图标来为 Default action (默认操作) 选择不同的目标组。
7. 选择 Update。

使用 AWS CLI 更新侦听器

使用 modify-listener 命令。

更新您的 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、更新证书列表或替换安全策略。

限制

您无法在网络负载均衡器上安装具有大于 2048 位的 RSA 密钥或 EC 密钥的证书。

任务

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 (p. 18)。

使用控制台更改默认证书

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择负载均衡器，然后选择 Listeners。
4. 选中侦听器对应的复选框，然后选择 Edit (编辑)。
5. 对于 Default SSL certificate (默认 SSL 证书)，请执行下列操作之一：
   - 如果使用 AWS Certificate Manager 创建或导入了证书，请选择 From ACM (来自 ACM) 并选择证书。
   - 如果使用 IAM 上传了证书，则选择 From IAM (来自 IAM) 并选择证书。
6. 选择 Update。

使用 AWS CLI 更改默认证书

使用 modify-listener 命令。

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 (p. 18)。

使用控制台将证书添加到证书列表

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。

2. 在导航窗格上的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择负载均衡器，然后选择 Listeners。
4. 对于要更新的 HTTPS 侦听器，请选择 View/edit certificates (查看/编辑证书)，这将显示默认证书，后跟已添加到侦听器的任何其他证书。
5. 选择菜单栏中的 Add certificates (添加证书) 图标（加号），这将显示默认证书，后跟由 ACM 和 IAM 管理的任何其他证书。如果已将证书添加到侦听器，则其复选框处于选中和禁用状态。
6. 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 Add (添加)。
7. 如果您有一个未由 ACM 或 IAM 管理的证书，则按如下方式将其导入 ACM 中，并将其添加到侦听器：
   a. 选择 Import certificate。
   b. 对于 Certificate private key，粘贴证书的 PEM 编码的未加密私有密钥。
   c. 对于 Certificate body，粘贴 PEM 编码的证书。
   d. (可选) 对于 Certificate chain，粘贴 PEM 编码的证书链。
   e. 选择 Import。新导入的证书将显示在可用证书列表中并处于选中状态。
   f. 选择 Add。
8. 要离开此屏幕，请选择菜单栏中的 Back to the load balancer (返回到负载均衡器) 图标（后退按钮）。

使用 AWS CLI 将证书添加到证书列表

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 (p. 21)。

使用控制台从证书列表中删除证书

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择负载均衡器，然后选择 Listeners。
4. 对于要更新的侦听器，请选择 View/edit certificates (查看/编辑证书)，这将显示默认证书，后跟已添加到侦听器的任何其他证书。
5. 在菜单栏中选择 Remove certificates 图标 (减号)。
6. 选中证书对应的复选框，然后选择 Remove (删除)。
7. 要离开此屏幕，请选择菜单栏中的 Back to the load balancer (返回到负载均衡器) 图标（后退按钮）。

使用 AWS CLI 从证书列表中删除证书

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。Network Load Balancer不支持自定义安全策略。有关更多信息，请参阅安全策略 (p. 19)。

使用控制台更新安全策略

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Load Balancers。

3. 选择负载均衡器，然后选择 Listeners。
4. 选中 TLS 侦听器对应的复选框，然后选择 Edit (编辑)。
5. 对于 Security policy (安全策略)，选择安全策略。
6. 选择 Update。

使用 AWS CLI 更新安全策略

使用 modify-listener 命令。

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. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择负载均衡器，然后选择 Listeners。选中侦听器对应的复选框，然后选择 Delete (删除)。
4. 当系统提示进行确认时，选择 Yes, Delete。

使用 AWS CLI 删除侦听器

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。在创建每个侦听器规则时，可以指定目标组和条件。满足规则条件时，流量会转发到相应的目标组。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 (p. 1)。

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。

内容

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

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
TLS	TCP | TLS	实例 | ip	HTTP | HTTPS | TCP
UDP	UDP | TCP_UDP	实例	HTTP | HTTPS | TCP
TCP_UDP	TCP_UDP	实例	HTTP | HTTPS | TCP

目标类型

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，将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。

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。

通过这些支持的 CIDR 块，您可以将以下内容注册到目标组：ClassicLink 实例、可通过 IP 地址和端口寻址的 AWS 资源 (例如数据库)，以及通过 AWS Direct Connect 或软件 VPN 连接链接到 AWS 的本地资源。

当目标类型为 `ip` 时，负载均衡器可支持针对每个唯一目标（IP 地址和端口）的 55000 个并发连接或每分钟约 55000 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。

如果目标组协议是 UDP 或 TCP_UDP，目标类型必须为 `instance`。

Network Load Balancer不支持 `lambda` 目标类型，仅 Application Load Balancer 支持 `lambda` 目标类型。有关更多信息，请参阅 Application Load Balancer 用户指南 中的作为目标的 Lambda 函数。

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。

源 IP 保留

如果您使用实例 ID 指定目标，则客户端的源 IP 地址将保留并提供给您的应用程序。

如果您用 IP 地址指定目标，则源 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。

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 (p. 49)。

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。您可以使用不同的端口多次向同一目标组注册每个 EC2 实例或 IP 地址，从而使负载均衡器能够将请求路由到微服务。

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。一旦注册过程完成，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。将一个目标组附加到 Auto Scaling 组后，Auto Scaling 将在启动目标时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 中的将负载均衡器附加到 Auto Scaling 组。

限制

- 如果实例为以下类型，则不能用实例 ID 注册实例：C1、CC1、CC2、CG1、CG2、CR1、G1、G2、HI1、HS1、M1、M2、M3 和 T1。可以用 IP 地址注册这些类型的实例。
- 如果实例位于与负载均衡器 VPC 对等的 VPC 中，则不能用实例 ID 注册这些实例。可以用 IP 地址注册这些实例。

目标组属性

以下是目标组属性：

`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。

`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。

取消注册延迟

取消注册实例时，负载均衡器将停止创建与实例的新连接。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实例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实例。为保证现有连接关闭，您可以在取消注册实例之前确保该实例运行状况不佳，或者您可以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。

使用控制台更新取消注册延迟值

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。

3. 选择目标组。
4. 选择 Description、Edit attributes。
5. 根据需要更改 Deregistration delay 的值，然后选择 Save。

使用 AWS CLI 更新取消注册延迟值

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，如源和目的地。代理协议版本 2 提供代理协议标头的二进制编码。负载均衡器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，包括客户端或任何其他代理、负载均衡器或网络路径中的服务器所发送的任何代理协议标头。因此，可以接收多个代理协议标头。此外，如果您的网络负载均衡器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网络负载均衡器中的标题。

如果您通过 IP 地址指定目标，则提供给应用程序的源 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。

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。

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

对于来自服务使用器并通过 VPC 端点服务的流量，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)	说明
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

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
3. 选择目标组。
4. 选择 Description、Edit attributes。
5. 选择 Enable proxy protocol v2，然后选择 Save。

使用 AWS CLI 启用代理协议

使用 modify-target-group-attributes 命令。

为网络负载均衡器创建目标组

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 (p. 16)。

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 (p. 32)。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 (p. 31)。

使用控制台创建目标组

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
3. 选择 Create target group。
4. 对于 Target group name，键入目标组的名称。
5. 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。
6. (可选) 对于 Port，请根据需要修改默认值。
7. 对于 Target type，选择 `instance` 通过实例 ID 指定目标，或选择 `ip` 通过 IP 地址指定目标。如果目标组协议是 UDP 或 TCP_UDP，您必须选择 `instance`。
8. 对于 VPC，选择 Virtual Private Cloud (VPC)。
9. (可选) 对于 Health check settings 和 Advanced health check settings，根据需要修改默认设置。选择 Create。
10. (可选) 添加一个或多个标签，如下所示：
    a. 选择新创建的目标组。
    b. 选择 Tags、Add/Edit Tags。
    c. 在 Add/Edit Tags 页面上，对于添加的每个标签，选择 Create Tag，然后指定标签键和标签值。添加完标签后，选择 Save。

11. (可选) 要向目标组添加目标，请参阅向您的目标组注册目标 (p. 32)。

使用 AWS CLI 创建目标组

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

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 跨区域负载均衡 (p. 10)。

借助主动的运行状况检查，负载均衡器会定期向每个已注册的目标发送请求以检查其状态。每个负载均衡器节点均使用每个目标注册到的目标组的运行状况检查设置来检查该目标的运行状况。在完成每次运行状况检查后，负载均衡器节点将关闭为运行状况检查而建立的连接。

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。

如果一个或多个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。如果每个目标组中不存在具有运行状况良好的目标的已启用可用区，则请求将被路由到所有已启用可用区中的目标。

如果您将 TLS 侦听器添加到网络负载均衡器，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 ping 从负载均衡器发送到向 TLS 侦听器注册的目标。您可以识别这些 TCP ping，因为它们具有网络负载均衡器的源 IP 地址，并且连接不包含数据包。

对于 UDP 服务，使用针对目标的 TCP 端口的 TCP 活动运行状况检查来测试可用性。您可以使用目标的任何 TCP 端口来验证 UDP 服务的可用性。如果侦听运行状况检查端口的服务失败，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，并关闭运行状况检查端口。

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出了 UnhealthyThresholdCount 连续失败次数，则负载均衡器将使目标停止服务。如果运行状况检查超出了 HealthyThresholdCount 连续成功次数，则负载均衡器将使目标恢复服务。

设置	说明
HealthCheckProtocol	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。
HealthCheckPort	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。
HealthCheckPath	[HTTP/HTTPS 运行状况检查] 进行运行状况检查的目标上的目的地的 ping 路径。默认值为 /。

设置	说明
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。对于 HTTP 运行状况检查，该值必须为 6 秒；对于 TCP 和 HTTPS 运行状况检查，该值必须为 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)。该值可以是 10 或 30 秒。默认值为 30 秒。 Important 网络负载均衡器 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。
HealthyThresholdCount	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 至 10。默认值为 3。
UnhealthyThresholdCount	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。该值必须与正常阈值计数相同。
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。此值必须介于 200 到 399 之间。

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`	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。
`healthy`	目标正常。
`unhealthy`	目标未响应运行状况检查或未通过运行状况检查。
`unused`	目标未注册到目标组，负载均衡器的侦听器规则中未使用目标组，或者目标在没有为负载均衡器启用的可用区中。
`draining`	目标正在取消注册，连接即将耗尽。

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.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
`Target.ResponseCodeMismatch`	运行状况检查失败，显示以下代码：[code]
`Target.Timeout`	请求超时

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. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
3. 选择目标组。
4. 选择 Targets，并查看 Status 列中的每个目标的状态。如果状态是 `Healthy` 以外的任何值，请查看工具提示以了解更多信息。

使用 AWS CLI 检查目标的运行状况

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。

修改目标组的运行状况检查设置

您可以修改目标组的部分运行状况检查设置。如果目标组的协议是 TCP、TLS、UDP 或 TCP_UDP，则无法修改运行状况检查协议、间隔、超时或成功代码。

使用控制台修改目标组的运行状况检查设置

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。

3. 选择目标组。
4. 选择 Health checks、Edit。
5. 在 Edit target group 页面上，根据需要修改设置，然后选择 Save。

使用 AWS CLI 修改目标组的运行状况检查设置

使用 modify-target-group 命令。

向您的目标组注册目标

您可以将目标注册到一个或多个目标组中。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。您可以通过实例 ID 或 IP 地址注册目标。有关更多信息，请参阅 Network Load Balancer 的目标组 (p. 24)。

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。在目标准备好处理请求后，将目标注册到您的目标组。只要注册过程完成且目标通过初始运行状况检查，负载均衡器就会开始将请求路由至目标。

如果已注册目标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。取消注册某个目标后，负载均衡器立即停止将请求路由到该目标。在目标准备好接收请求时，您可以再次将目标注册到目标组。

在取消注册目标时，Elastic Load Balancing 会等待，直到进行中请求完成。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 (p. 26)。

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 中的将负载均衡器附加到 Auto Scaling 组。

目标安全组

在将 EC2 实例注册为目标时，必须确保这些实例的安全组允许侦听器端口和运行状况检查端口上的流量。

限制

- Network Load Balancer 没有关联的安全组。因此，您的目标的安全组必须使用 IP 地址以允许来自负载均衡器的流量。
- 您不能在目标的安全组中允许来自客户端的流量通过使用客户端的安全组的负载均衡器传递到目标。请改为使用目标安全组中的客户端 CIDR 块。

推荐的规则

Inbound		
Source	Port Range	Comment
### IP ##	*#####*	在实例侦听器端口上允许来自客户端的流量
VPC CIDR	*######*	在运行状况检查端口上允许来自负载均衡器的流量

如果您不想授予对整个 VPC CIDR 的访问权限，则可以授予对负载均衡器节点所使用的私有 IP 地址的访问权限。每个负载均衡器的子网有一个 IP 地址。要查找这些地址，请按照下列过程操作。

查找要列入白名单的私有 IP 地址

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格中，选择 Network Interfaces。
3. 在搜索字段中，键入您的网络负载均衡器的名称。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 Details (详细信息) 选项卡上，从 Primary private IPv4 IP (主要私有 IPv4 IP) 复制地址。

网络 ACL

VPC 的默认网络访问控制列表 (ACL) 允许所有入站和出站流量。如果您创建自定义网络 ACL，它们必须允许负载均衡器和实例在侦听器端口、运行状况检查端口和临时端口 (1024-65535) 上进行双向通信。

注册或取消注册目标

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，请参阅目标类型 (p. 25)。

限制

- 如果实例为以下类型，则不能用实例 ID 注册实例：C1、CC1、CC2、CG1、CG2、CR1、G1、G2、HI1、HS1、M1、M2、M3 和 T1。可以用 IP 地址注册这些类型的实例。
- 如果实例位于与负载均衡器 VPC 对等的 VPC 中，则不能用实例 ID 注册这些实例。可以用 IP 地址注册这些实例。

目录

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。

通过实例 ID 注册或取消注册目标

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
3. 选择目标组。
4. 选择 Targets、Edit。
5. (可选) 对于 Registered instances，选择要取消注册的任何实例，然后选择 Remove。
6. (可选) 对于 Instances，选择要注册的任何正在运行的实例，根据需要修改默认实例端口，然后选择 Add to registered。
7. 选择 Save。

通过 IP 地址注册或取消注册目标

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)

通过 IP 地址注册或取消注册目标

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
3. 选择目标组，然后依次选择 Targets、Edit。
4. 要注册 IP 地址，请在菜单栏中选择 Register targets 图标 (加号)。对于每个 IP 地址，请指定网络、可用区、IP 地址和端口，然后选择 Add to list。指定完地址后，选择 Register。
5. 要取消注册 IP 地址，请在菜单栏中选择 Deregister targets 图标 (减号)。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。选择 IP 地址并选择 Deregister。
6. 要离开此屏幕，请选择菜单栏中的 Back to target group 图标 (后退按钮)。

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。

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

- 每个资源的最大标签数 — 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，因为它专为 AWS 使用预留。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组的标签

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
3. 选择目标组。
4. 在 Tags 选项卡上，选择 Add/Edit Tags，然后执行以下一项或多项操作：
   a. 要更新标签，请编辑 Key 和 Value 的值。
   b. 要添加新标签，请选择 Create Tag，然后为 Key 和 Value 键入值。
   c. 要删除标签，请选择标签旁边的删除图标 (X)。

5. 完成更新标签后，选择 Save。

使用 AWS CLI 更新目标组的标签

使用 add-tags 和 remove-tags 命令。

删除目标组

如果目标组未由任何操作引用，则删除目标组。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 EC2 实例，则可停止或终止该实例。

使用控制台删除目标组

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
3. 选择目标组，然后依次选择 Actions、Delete。
4. 当系统提示您确认时，选择 Yes。

使用 AWS CLI 删除目标组

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

可以使用 Amazon CloudWatch 将有关负载均衡器和目标的数据点的统计数据作为一组有序时间序列数据（称作指标）进行检索。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，请参阅网络负载均衡器 的 CloudWatch 指标 (p. 36)。

VPC 流日志

您可以使用 VPC 流日志来捕获有关往来于您的网络负载均衡器的流量的详细信息。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 网络负载均衡器 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。

通过您的网络负载均衡器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。如果目标由实例 ID 注册，连接将作为来自客户端的实例向实例显示。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“ACCEPT OK (接受 OK)”，同时实例的网络接口的日志将对连接显示“REJECT OK (拒绝 OK)”。

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，请参阅网络负载均衡器的访问日志 (p. 41)。

CloudTrail 日志

您可以使用 AWS CloudTrail 捕获有关向 Elastic Load Balancing API 发出的调用的详细信息，并将这些详细信息作为日志文件存储在 Amazon S3 中。可以使用这些 CloudTrail 日志确定已发出的调用、从中发出调用的源 IP 地址、调用的发出方、调用的发出时间等。有关更多信息，请参阅使用 AWS CloudTrail 记录 网络负载均衡器 的 API 调用 (p. 45)。

网络负载均衡器 的 CloudWatch 指标

Elastic Load Balancing 将数据点发布到您的负载均衡器和目标的 Amazon CloudWatch。利用 CloudWatch，您可以按一组有序的时间序列数据（称为指标）来检索有关这些数据点的统计数据。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，并在指标超出您的可接受范围时启动某个操作 (如向电子邮件地址发送通知)。

只有当请求流经负载均衡器时，Elastic Load Balancing 才会向 CloudWatch 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。

有关更多信息，请参阅 Amazon CloudWatch 用户指南。

内容

网络负载均衡器指标

AWS/NetworkELB 命名空间包括以下指标。

指标	说明
ActiveFlowCount	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。 报告标准：有非零值 统计数据：最有用的统计工具是 Average、Maximum 和 Minimum。 维度 • LoadBalancer • AvailabilityZone、LoadBalancer
ActiveFlowCount_TLS	客户端至目标的并发 TLS 流 (或连接) 的总数。此指标仅包含处于 ESTABLISHED 状态的连接。 报告标准：有非零值 统计数据：最有用的统计工具是 Average、Maximum 和 Minimum。 维度 • LoadBalancer • AvailabilityZone、LoadBalancer
ClientTLSNegotiationErrorCount	在客户端和 TLS 侦听器之间协商期间失败的 TLS 握手的总数。 报告标准：有非零值 统计数据：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone、LoadBalancer
ConsumedLCUs	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 Elastic Load Balancing 定价。 报告标准：始终报告 统计数据：全部 维度 • LoadBalancer
HealthyHostCount	被视为正常运行的目标数量。 报告标准：在启用了运行状况检查时报告 统计数据：最有用的统计工具是 Maximum 和 Minimum。

指标	说明
	维度 • LoadBalancer、TargetGroup • AvailabilityZone，LoadBalancer，TargetGroup
NewFlowCount	时段内建立的客户端至目标的新流（或连接）的总数。 报告标准：有非零值 统计数据：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone、LoadBalancer
NewFlowCount_TLS	时段内建立的客户端至目标的新 TLS 流 (或连接) 的总数。 报告标准：有非零值 统计数据：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone、LoadBalancer
ProcessedBytes	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。 报告标准：有非零值 统计数据：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone、LoadBalancer
ProcessedBytes_TLS	TLS 侦听器处理的字节的总数。 报告标准：有非零值 统计数据：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone、LoadBalancer

指标	说明
TargetTLSNegotiationErrorCount	在 TLS 侦听器和目标之间协商期间失败的 TLS 握手的总数。 报告标准：有非零值 统计数据：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone、LoadBalancer
TCP_Client_Reset_Count	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。 报告标准：有非零值 统计数据：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone、LoadBalancer
TCP_ELB_Reset_Count	负载均衡器生成的重置 (RST) 数据包的总数。 报告标准：有非零值 统计数据：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone、LoadBalancer
TCP_Target_Reset_Count	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。 报告标准：有非零值 统计数据：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone、LoadBalancer
UnHealthyHostCount	被视为未正常运行的目标数量。 报告标准：在启用了运行状况检查时报告 统计数据：最有用的统计工具是 Maximum 和 Minimum。 维度 • LoadBalancer、TargetGroup • AvailabilityZone，LoadBalancer，TargetGroup

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	说明
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）。

网络负载均衡器 指标的统计数据

CloudWatch 提供基于 Elastic Load Balancing 发布的指标数据点的统计数据。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。因此，我们建议您使用HealthyHostCount 的最大值或 UnHealthyHostCount 的最小值监控您的 网络负载均衡器。

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。

查看负载均衡器的 CloudWatch 指标

您可以使用 Amazon EC2 控制台查看负载均衡器的 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 Amazon EC2 控制台查看指标

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/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. 通过以下网址打开 CloudWatch 控制台：https://console.amazonaws.cn/cloudwatch/。
2. 在导航窗格中，选择 Metrics。
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。

使用 AWS CLI 查看指标

使用以下 list-metrics 命令列出可用指标：

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

使用 AWS CLI 获取指标的统计数据

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 将不同维度的每种唯一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"
}
```

网络负载均衡器的访问日志

Elastic Load Balancing 提供了访问日志，该访问日志可捕获有关发送到网络负载均衡器的 TLS 请求的详细信息。您可以使用这些访问日志分析流量模式并解决问题。

> **Important**
>
> 仅当负载均衡器具有 TLS 侦听器且它们仅包含有关 TLS 请求的信息时，才创建访问日志。

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 以压缩文件形式捕获日志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。

如果为 S3 存储桶启用了使用 Amazon S3 托管加密密钥 (SSE-S3) 的服务器端加密，则每个访问日志文件在存储到 S3 存储桶之前会自动加密，并在您访问它时自动解密。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一个唯一密钥进行加密，此密钥本身将使用定期轮换的主密钥进行加密。有关更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的使用具有 Amazon S3托管加密密钥的服务器端加密 (SSE-S3) 保护数据。

使用访问日志无需额外付费。您将需要支付 Amazon S3 的存储费用，但无需为 Elastic Load Balancing 用来将日志文件发送到 Amazon S3 的带宽付费。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_load-balancer-id_end-time_random-string.log.gz
```

存储桶

S3 存储桶的名称。

前缀

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

拥有者的 AWS 账户 ID。

区域

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。

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 Simple Storage Service 开发人员指南 中的对象生命周期管理。

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	说明
type	侦听器的类型。支持的值为 `tls`。

字段	说明
version	日志条目的版本。支持的版本为 1.0。
timestamp	在 TLS 连接结束时记录的时间戳（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。
listener:port	侦听器的 IP 地址和端口。
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 connection_time 字段中。
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 tlsv10、tlsv11 和 tlsv12。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 server_name 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 - 。

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。

```
tls 1.0 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-cn:acm:us-west-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-west-2.amazonaws.com
```

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。

- 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",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws-cn:s3:::bucket_name/prefix/AWSLogs/123456789012/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws-cn:s3:::bucket_name"
    }
  ]
}
```

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 存储桶的名称。有关更多信息，请参阅 存储桶要求 (p. 43)。

使用控制台启用访问日志记录

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格中，选择 Load Balancers。
3. 选择您的负载均衡器。
4. 在 Description 选项卡上，选择 Edit attributes。
5. 在 Edit load balancer attributes 页面上，执行以下操作：
   a. 对于 Access logs (访问日志)，选择 Enable (启用)。
   b. 对于 S3 location，键入 S3 存储桶的名称，包括任何前缀 (例如，`my-loadbalancer-logs/my-app`)。您可以指定现有存储桶的名称或新存储桶名称。如果您指定现有存储桶，请确保您拥有此存储桶，且配置了必要的存储桶策略。
   c. (可选) 如果存储桶不存在，请选择 Create this location for me。您必须指定在 Amazon S3 中的所有现有存储桶名称中唯一的名称，并遵循 DNS 命名约定。有关更多信息，请参阅 Amazon Simple Storage Service 开发人员指南中的存储桶命名规则。
   d. 选择 Save。

使用 AWS CLI 启用访问日志记录

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 控制台用户指南 中的使用存储桶。

使用控制台禁用访问日志记录

1. 打开 Amazon EC2 控制台 https://console.amazonaws.cn/ec2/。
2. 在导航窗格中，选择 Load Balancers。
3. 选择您的负载均衡器。
4. 在 Description 选项卡上，选择 Edit attributes。
5. 对于 Access logs (访问日志)，清除 Enable (启用)。
6. 选择 Save。

使用 AWS CLI 禁用访问日志记录

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，则将对其进行解压缩，并且将显示信息。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)。您可能无法通过逐行处理来处理数量如此庞大的数据。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，让您能够使用标准 SQL 在 Amazon S3 中轻松分析数据。有关更多信息，请参阅 Amazon Athena 用户指南 中的查询网络负载均衡器日志。
- Loggly
- Splunk
- Sumo Logic

使用 AWS CloudTrail 记录 网络负载均衡器 的 API 调用

Elastic Load Balancing 与 AWS CloudTrail 集成，后者是一项服务，该服务提供了由用户、角色或 Elastic Load Balancing 中的 AWS 服务执行的操作的记录。CloudTrail 将 Elastic Load Balancing 的所有 API 调用作为事件捕获。捕获的调用包含来自 AWS 管理控制台的调用和对 Elastic Load Balancing API 操作的代码调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 Elastic Load Balancing 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台的 Event history (事件历史记录) 中查看最新事件。通过使用 CloudTrail 收集的信息，您可以确定向 Elastic Load Balancing 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅 AWS CloudTrail User Guide。

CloudTrail 中的 Elastic Load Balancing 信息

在您创建 CloudTrail 账户时，即针对该账户启用了 AWS。Elastic Load Balancing 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在 Event history (事件历史记录) 中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 AWS 账户中的事件（包括 Elastic Load Balancing 的事件），请创建跟踪。通过跟踪，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 接收来自多个区域的 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

Network Load Balancer 的所有 Elastic Load Balancing 操作均由 CloudTrail 记录下来并记载到 Elastic Load Balancing API 参考第 2015-12-01 版 中。例如，对 `CreateLoadBalancer` 和 `DeleteLoadBalancer` 操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员的信息。身份信息帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management (IAM) 用户凭证发出的。
- 请求是使用角色还是联合身份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 userIdentity 元素。

了解 Elastic Load Balancing 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 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 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会以任何特定顺序显示。

这些日志文件包含 AWS 账户的所有 AWS API 调用（而不只是 Elastic Load Balancing API 调用）的相关事件。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。

以下是一位用户的 Elastic Load Balancing 的示例 CloudTrail 日志记录，该用户使用 AWS CLI 创建了一个网络负载均衡器，然后又删除了它。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 botocore/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"
}
```

网络负载均衡器故障排除

以下信息可帮助您解决与 网络负载均衡器 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 (p. 29)。

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。

网络访问控制列表 (ACL) 不允许流量

与实例的子网关联的网络 ACL 必须允许运行状况检查端口上的入站流量，以及临时端口 (1024-65535) 上的出站流量。与您负载均衡器节点的子网关联的网络 ACL 必须允许临时端口上的入站流量，以及运行状况检查端口和临时端口上的出站流量。

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。

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。

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

网络负载均衡器 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

如果您的负载均衡器至少有一个运行正常的已注册目标，则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，则负载均衡器将请求路由到所有已注册目标。

从目标到其负载均衡器的请求连接超时

检查您是否有一个内部负载均衡器的目标是通过实例 ID 注册的。内部负载均衡器不支持“发夹”(hairpin) 转换或回环。通过实例 ID 注册目标时，客户端的源 IP 地址会保留。如果实例是它通过实例 ID 注册到的内部负载均衡器的客户端，则连接仅在请求路由到不同的实例时才会成功。否则，源地址和目的地 IP 地址相同，连接会超时。

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：

- 通过 IP 地址 (而不是实例 ID) 注册实例。当使用 Amazon Elastic Container Service 时，请为您的任务使用 `awsvpc` 网络模式，以确保目标组要求通过 IP 地址注册。
- 确保必须相互通信的容器位于不同的容器实例上。
- 使用面向 Internet 的负载均衡器。

当将目标移到 网络负载均衡器 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 网络负载均衡器 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。

通过 AWS PrivateLink 连接时发生端口分配错误

如果您的 网络负载均衡器 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。要修复端口分配错误，请将更多目标添加到目标组。

Network Load Balancer 的限制

要查看 Network Load Balancer 的当前限制，请使用 Amazon EC2 控制台的 Limits (限制) 页面，或者使用 describe-account-limits (AWS CLI) 命令。要请求提高限制，请使用Elastic Load Balancing限制表单。

您的 AWS 账户存在以下与 Network Load Balancer 相关的限制。

区域限制

- 每个区域的 Network Load Balancer 数量：20
- 每个区域的目标组：3000 *

负载均衡器限制 †

- 每个负载均衡器的侦听器数：50
- 每个负载均衡器每个可用区的子网数：1
- [禁用了跨区域负载均衡] 每个负载均衡器的每个可用区的目标数：500
- [启用了跨区域负载均衡] 每个负载均衡器的目标数：500
- 每个目标组的负载均衡器数：1

* Application Load Balancer 和 Network Load Balancer 的目标组共享此限制。

† 这些限制是不能增加的。

Network Load Balancer 文件历史记录

下表介绍了 Network Load Balancer 的版本。

update-history-change	update-history-description	update-history-date
SNI 支持	此版本增加了对服务器名称指示 (SNI) 的支持。	September 12, 2019
UDP 协议 (p. 51)	此版本增加了对 UDP 协议的支持。	June 24, 2019
TLS 协议	此版本增加了对 TLS 协议的支持。	January 24, 2019
跨区域负载均衡 (p. 51)	此版本增加了对启用跨区域负载均衡的支持。	February 22, 2018
代理协议	此版本增加了对启用代理协议的支持。	November 17, 2017
IP 地址即目标	此版本增加了将 IP 地址注册为目标的支持。	September 21, 2017
新负载均衡器类型 (p. 51)	Elastic Load Balancing 的此发行版本引入了 Network Load Balancer。	September 7, 2017