Elastic Load Balancing

网关负载均衡器

Elastic Load Balancing: 网关负载均衡器

Copyright © 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或者贬低或诋毁 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。

AWS 文档中描述的 AWS 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅中国的 AWS 服务入门。

Table of Contents

什么是网关Load Balancer?

利用网关负载均衡器，您可以部署、扩展和管理虚拟设备，例如防火墙、入侵检测和防御系统以及深层数据包检查系统。它结合了透明网络网关（即，所有流量的单个入口和退出点）并分配流量，同时根据需要扩展您的虚拟设备。

网关 Load Balancer 在开放系统互连（OSI）模型的第三个层（网络层）运行。它侦听所有端口上的所有 IP 数据包，并将流量转发到侦听器规则中指定的目标组。它使用 5-tuple对于 TCP/UDP 流）或 3 元3-tuple对于非 TCP/UDP 流）来维护流到特定目标设备的粘性。网关 Load Balancer 及其注册的虚拟设备实例在端口 6081 上使用 GENEVE 协议交换应用程序流量。它支持 8500 字节的最大传输单位（MTU）大小。

网关负载均衡器使用网关 Load Balancer 终端节点安全地跨 VPC 边界交换流量。网关 Load Balancer 终端节点是一个 VPC 终端节点，可在服务提供商 VPC 中的虚拟设备与服务使用者 VPC 中的应用程序服务器之间提供私有连接。您可以在与虚拟设备相同的 VPC 中部署网关 Load Balancer 。将虚拟设备注册到网关Load Balancer的目标组。

使用路由表配置进出网关Load Balancer终端节点的流量。流量从服务使用者 VPC 通过网关 Load Balancer 终端节点流向服务提供商 VPC 中的网关 Load Balancer 然后返回到服务使用者 VPC。您必须在不同的子网中创建网关Load Balancer终端节点和应用程序服务器。这使您能够将网关Load Balancer终端节点配置为应用程序子网的路由表中的下一跃点。

有关更多信息，请参阅《Amazon VPC 用户指南》中的网关 Load Balancer 终端节点（AWS PrivateLink

设备供应商

您负责从设备供应商处选择和限定软件。您必须信任设备软件来检查或修改来自负载均衡器的流量。作为 Elastic Load Balancing 合作伙伴列出的设备供应商已将其设备软件与 AWS 集成并取得资格。您可以对该列表中的供应商提供的设备软件给予更高的信任度。但是，AWS 不保证这些供应商的软件的安全性或可靠性。

入门

要使用 AWS 管理控制台创建网关 Load Balancer 请参阅入门 (p. 2)。要使用 AWS 命令行界面创建网关 Load Balancer 请参阅开始使用 CLI (p. 6)。

Pricing

利用负载均衡器，您可以按实际用量付费。有关更多信息，请参阅 Elastic Load Balancing 定价。

网关负载均衡器入门

利用网关负载均衡器，您可以轻松部署、扩展和管理第三方虚拟设备，如安全设备。

在本教程中，我们将使用网关Load Balancer和网关Load Balancer终端节点实施检查系统。

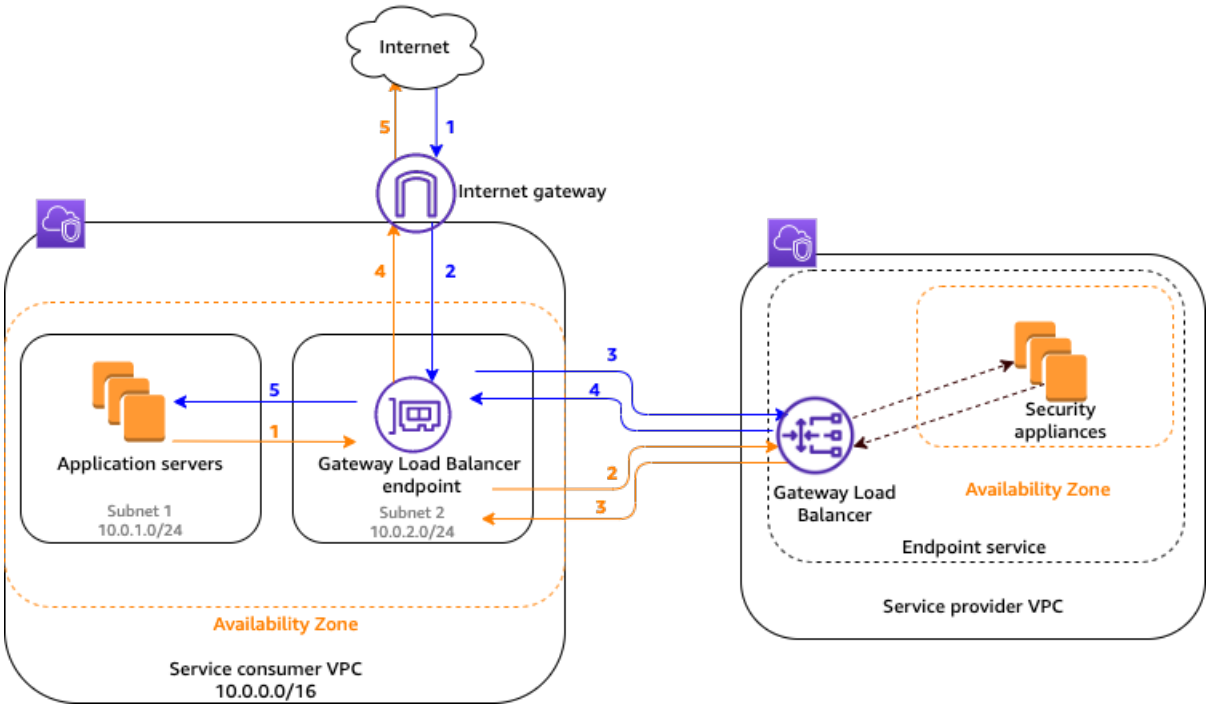
目录

Overview

网关 Load Balancer 终端节点是一个 VPC 终端节点，可在服务提供商 VPC 中的虚拟设备与服务使用者 VPC 中的应用程序服务器之间提供私有连接。网关 Load Balancer 部署在与虚拟设备负载均衡器相同的 VPC 中。这些设备注册为网关Load Balancer的目标组。

应用程序服务器在服务使用者 VPC 中的一个子网（目标子网）中运行，而网关 Load Balancer 终端节点位于同一 VPC 的另一个子网中。通过互联网网关进入服务使用者 VPC 的所有流量首先路由到网关 Load Balancer 终端节点进行检查，然后路由到目标子网。

同样，离开应用程序服务器（目标子网）的所有流量都会路由到网关 Load Balancer 终端节点进行检查，然后再路由回 Internet。以下网络图是网关Load Balancer终端节点如何用于访问终端节点服务的可视化表示。



后面的编号项目，突出显示并说明上图中显示的元素。

从 Internet 到应用程序的流量（蓝色箭头）：

1. 流量通过 Internet 网关进入服务使用者 VPC。
2. 由于入口路由，流量将发送到网关Load Balancer终端节点。
3. 流量将通过安全设备发送到网关Load Balancer以进行检查。
4. 检查后，流量将发送回网关Load Balancer终端节点。
5. 流量将发送到应用程序服务器（目标子网）。

从应用程序到 Internet 的流量（橙色箭头）：

1. 由于在应用程序服务器子网上配置的默认路由，流量将发送到网关Load Balancer终端节点。
2. 流量将通过安全设备发送到网关Load Balancer以进行检查。
3. 检查后，流量将发送回网关Load Balancer终端节点。
4. 流量将根据路由表配置发送到 Internet 网关。
5. 流量将路由回 Internet。

Routing

Internet 网关的路由表必须有一个条目，以将目标为应用程序服务器的流量路由到网关 Load Balancer 终端节点。要指定网关 Load Balancer 终端节点，请使用 VPC 终端节点的 ID。

目的地	目标
10.0.0.0/16	本地
10.0.1.0/24	*vpc-endpoint-id*

具有应用程序服务器的子网的路由表必须具有一个条目，该条目将所有流量从应用程序服务器路由到网关 Load Balancer 终端节点（0.0.0.0/0）。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	*vpc-endpoint-id*

具有网关 Load Balancer 终端节点的子网的路由表必须将 从检查返回的流量路由到其最终目的地。对于源自 Internet 的流量，本地路由可确保它到达应用程序服务器。对于源自应用程序服务器的流量，请添加一个将所有流量路由到 Internet 网关的条目（0.0.0.0/0）。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	*internet-gateway-id*

Prerequisites

- 确保服务使用者 VPC 对于每个包含应用程序服务器的可用区至少具有两个子网。一个子网用于网关Load Balancer终端节点，另一个子网用于应用程序服务器。
- 网关Load Balancer和目标可以位于同一子网中。
- 在服务提供商 VPC 中的每个安全设备子网中至少启动一个安全设备实例。这些实例的安全组必须允许端口 6081 上的 UDP 流量。

步骤 1：创建网关 Load Balancer 并注册目标

使用以下过程创建负载均衡器、侦听器和目标组，并将安全设备实例注册为目标。

创建网关Load Balancer并注册目标

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择 Create Load Balancer。
4. 对于 Gateway Load Balancer（网关负载均衡器），选择 Create（创建）。
5. 对于名称，输入负载均衡器的名称。例如，**`my-load-balancer`**。
6. 对于 Availability Zones（可用区），选择服务提供商 VPC。对于您在其中启动安全设备实例的每个可用区，请选择该可用区，然后选择一个公有子网。
7. （可选）展开 Tags（标签）并添加标签。
8. 选择 Next: Configure Routing。
9. 对于 Name（名称），输入目标组的名称。例如，**`my-targets`**。
10. 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。
11. 协议必须为 `GENEVE`，端口必须为 `6081`。
12. （可选）对于 Health checks（运行状况检查），根据需要修改运行状况检查设置。
13. 选择 Next: Register Targets。
14. 将您的实例或 IP 地址添加到列表中，然后选择 Next： Review（下一步： 审核）。
15. 选择创建。

步骤 2：创建网关 Load Balancer 终端节点

要创建网关Load Balancer终端节点，请按照以下过程操作。Gateway Load Balancer 终端节点为可用区。我们建议您为每个区域创建一个网关Load Balancer终端节点。有关更多信息，请参阅网关 Load Balancer 终端节点（AWS PrivateLink

要创建网关负载均衡器终端节点

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择终端节点服务。
3. 选择 Create Endpoint Service（创建终端节点服务），然后执行以下操作：

   a. 对于 Associate Load Balancer（关联负载均衡器），选择您的网关 Load Balancer 。
   b. 对于 Require acceptance for endpoint（需要接受终端节点），选择 Acceptance required to accepting connection requests to your service manually（需要接受以手动接受您的服务的连接请求）。否则，将自动接受终端节点连接。
   c. （可选）要添加标签，请选择 Add tag（添加标签），然后指定标签的键和值。

d. 选择 Create service。选择服务 ID。从 Details （详细信息）选项卡中保存服务名称；您在创建终端节点时需要使用该名称。
e. 选择 Actions、Add principals to whitelist。输入允许为您的服务创建终端节点的服务使用者的 ARNs。服务使用者可以是 IAM 用户、IAM 角色或 AWS 账户。

4. 在导航窗格中，选择终端节点。
5. 选择 Create Endpoint （创建终端节点），然后执行以下操作：

a. 对于 Service category，选择 Find service by name。
b. 对于 Service name （服务名称），输入您之前保存的服务名称，然后选择 Verify （验证）。如果找到该名称，请继续下一步。否则，请确保您使用了正确的服务名称。
c. 对于 VPC，选择服务使用者 VPC。
d. 对于 Subnets （子网），选择网关 Load Balancer 终端节点的子网。
e. （可选）要添加标签，请选择 Add tag（添加标签），然后为标签指定键和值。
f. 选择Create endpoint。初始状态为 `pending acceptance`。

步骤 3：配置路由

按如下所示为服务使用者 VPC 配置路由表。这允许安全设备对发往应用程序服务器的入站流量执行安全检查。

配置路由

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Route Tables。
3. 选择 Internet 网关的路由表，然后执行以下操作：

a. 依次选择 Actions (操作)、Edit routes (编辑路由)。
b. 选择 Add route (添加路由)。对于 Destination （目标），输入应用程序服务器子网的 CIDR 块（例如 10.0.1.0/24）。对于 Target （目标），选择 VPC 终端节点。
c. 选择 Save routes (保存路由)。

4. 选择具有应用程序服务器的子网的路由表，然后执行以下操作：

a. 依次选择 Actions (操作)、Edit routes (编辑路由)。
b. 选择 Add route (添加路由)。对于 Destination，输入 **`0.0.0.0/0`**。对于 Target （目标），选择 VPC 终端节点。
c. 选择 Save routes (保存路由)。

5. 选择具有网关Load Balancer终端节点的子网的路由表，然后执行以下操作：

a. 依次选择 Actions (操作)、Edit routes (编辑路由)。
b. 选择 Add route (添加路由)。对于 Destination，输入 **`0.0.0.0/0`**。对于 Target （目标），选择 Internet 网关。
c. 选择 Save routes (保存路由)。

通过 AWS CLI 开始使用网关负载均衡器

利用网关负载均衡器，您可以轻松部署、扩展和管理第三方虚拟设备，如安全设备。

在本教程中，我们将使用网关Load Balancer和网关Load Balancer终端节点实施检查系统。

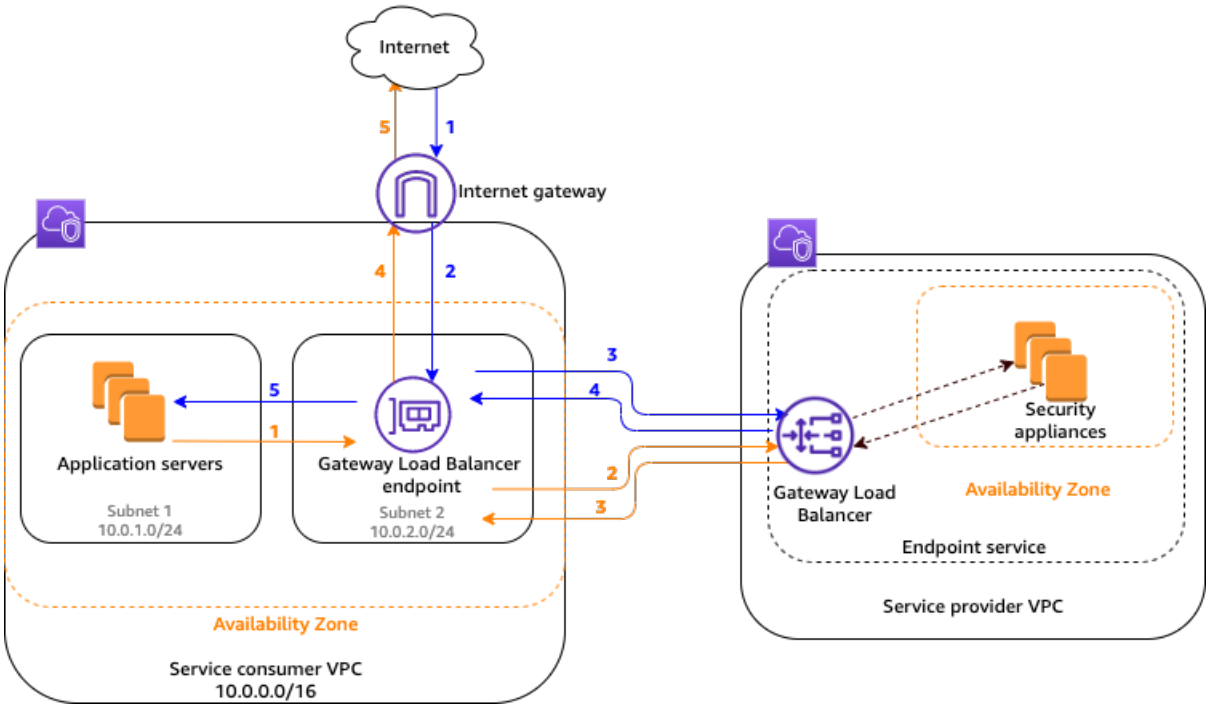
目录

Overview

网关 Load Balancer 终端节点是一个 VPC 终端节点，可在服务提供商 VPC 中的虚拟设备与服务使用者 VPC 中的应用程序服务器之间提供私有连接。网关 Load Balancer 部署在与虚拟设备的负载均衡器相同的 VPC 中。这些设备注册为网关Load Balancer的目标组。

应用程序服务器在服务使用者 VPC 中的一个子网（目标子网）中运行，而网关 Load Balancer 终端节点位于同一 VPC 的另一个子网中。通过互联网网关进入服务使用者 VPC 的所有流量首先路由到网关 Load Balancer 终端节点进行检查，然后路由到目标子网。

同样，离开应用程序服务器（目标子网）的所有流量都会路由到网关 Load Balancer 终端节点进行检查，然后再路由回 Internet。以下网络图是网关Load Balancer终端节点如何用于访问终端节点服务的可视化表示。



后面的编号项目，突出显示并说明上图中显示的元素。

从 Internet 到应用程序的流量（蓝色箭头）：

1. 流量通过 Internet 网关进入服务使用者 VPC。
2. 由于入口路由，流量将发送到网关Load Balancer终端节点。
3. 流量将通过安全设备发送到网关Load Balancer以进行检查。
4. 检查后，流量将发送回网关Load Balancer终端节点。
5. 流量将发送到应用程序服务器（目标子网）。

从应用程序到 Internet 的流量（橙色箭头）：

1. 由于在应用程序服务器子网上配置的默认路由，流量将发送到网关Load Balancer终端节点。
2. 流量将通过安全设备发送到网关Load Balancer以进行检查。
3. 检查后，流量将发送回网关Load Balancer终端节点。
4. 流量将根据路由表配置发送到 Internet 网关。
5. 流量将路由回 Internet。

Routing

Internet 网关的路由表必须有一个条目，以将目标为应用程序服务器的流量路由到网关 Load Balancer 终端节点。要指定网关 Load Balancer 终端节点，请使用 VPC 终端节点的 ID。

目的地	目标
10.0.0.0/16	本地
10.0.1.0/24	*vpc-endpoint-id*

具有应用程序服务器的子网的路由表必须具有一个条目，该条目将所有流量从应用程序服务器路由到网关 Load Balancer 终端节点（0.0.0.0/0）。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	*vpc-endpoint-id*

具有网关 Load Balancer 终端节点的子网的路由表必须将 从检查返回的流量路由到其最终目的地。对于源自 Internet 的流量，本地路由可确保它到达应用程序服务器。对于源自应用程序服务器的流量，请添加一个将所有流量路由到 Internet 网关的条目（0.0.0.0/0）。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	*internet-gateway-id*

Prerequisites

- 如果您使用的版本不支持网关负载均衡器，请安装 AWS CLI 或更新到 AWS CLI 的当前版本。有关更多信息，请参阅《AWS 命令行界面用户指南》中的“安装 AWS 命令行界面”。
- 确保服务使用者 VPC 对于每个包含应用程序服务器的可用区至少具有两个子网。一个子网用于网关Load Balancer终端节点，另一个子网用于应用程序服务器。
- 确保服务提供商 VPC 对于每个包含安全设备实例的可用区至少拥有两个子网。一个子网用于网关Load Balancer，另一个子网用于实例。
- 在服务提供商 VPC 中的每个安全设备子网中至少启动一个安全设备实例。这些实例的安全组必须允许端口 6081 上的 UDP 流量。

步骤 1：创建网关 Load Balancer 并注册目标

使用以下过程创建负载均衡器、侦听器和目标组，并将安全设备实例注册为目标。

创建网关Load Balancer并注册目标

1. 使用 create-load-balancer 命令创建 类型的负载均衡器gateway。您可以为在其中启动安全设备实例的每个可用区指定一个子网。

```
aws elbv2 create-load-balancer --name my-load-balancer --type gateway --
subnets provider-subnet-id
```

输出包含负载均衡器的 Amazon 资源名称（ARN），格式如以下示例所示。

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

2. 使用 create-target-group 命令创建目标组，并指定在其中启动实例的服务提供商 VPC。

```
aws elbv2 create-target-group --name my-targets --protocol GENEVE --port 6081 --vpc-
id provider-vpc-id
```

输出包含目标组的 ARN，格式如下。

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/0123456789012345
```

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，该侦听器具有将请求转发到目标组的默认规则。

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --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/gwy/my-load-
balancer/1234567890123456/abc1234567890123
```

5. （可选）您可以使用以下 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
```

步骤 2：创建网关 Load Balancer 终端节点

要创建网关Load Balancer终端节点，请按照以下过程操作。Gateway Load Balancer 终端节点为可用区。我们建议您为每个区域创建一个网关Load Balancer终端节点。有关更多信息，请参阅网关 Load Balancer 终端节点（AWS PrivateLink

要创建网关负载均衡器终端节点

1. 使用 create-vpc-endpoint-service-configuration 命令，通过网关 Load Balancer 创建终端节点服务配置。

```
aws ec2 create-vpc-endpoint-service-configuration --gateway-load-balancer-
arns loadbalancer-arn --no-acceptance-required
```

输出包含服务 ID（例如vpce-svc-12345678901234567和服务名称（例如us-east-2.vpce-svc-12345678901234567

2. 使用 modify-vpc-endpoint-service-permissions 命令可允许服务使用者创建与您的服务连接的终端节点。服务使用者可以是 IAM 用户、IAM 角色或 AWS 账户。以下示例为指定的 AWS 账户添加权限。

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-12345678901234567
 --add-allowed-principals arn:aws:iam::123456789012:root
```

3. 使用 create-vpc-endpoint 命令为您的服务创建网关 Load Balancer 终端节点。

```
aws ec2 create-vpc-endpoint --vpc-endpoint-type GatewayLoadBalancer --service-
name com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567 --vpc-id consumer-vpc-id
 --subnet-ids consumer-subnet-id
```

输出包含网关 Load Balancer 终端节点的 ID（例如vpce-01234567890abcdef

步骤 3：配置路由

按如下所示为服务使用者 VPC 配置路由表。这允许安全设备对发往应用程序服务器的入站流量执行安全检查。

配置路由

1. 使用 create-route 命令向 Internet 网关的路由表添加一个条目，以将发往应用程序服务器的流量路由到网关 Load Balancer 终端节点。

```
aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block 10.0.1.0/24
 --vpc-endpoint-id vpce-01234567890abcdef
```

2. 使用 create-route 命令向应用程序服务器的子网的路由表添加一个条目，以将来自应用程序服务器的所有流量路由到网关 Load Balancer 终端节点。

```
aws ec2 create-route --route-table-id application-rtb --destination-cidr-block
 0.0.0.0/0 --vpc-endpoint-id vpce-01234567890abcdef
```

3. 使用 create-route 命令向具有网关 Load Balancer 终端节点的子网的路由表中添加条目，该终端节点将来自应用程序服务器的所有流量路由到 Internet 网关。

```
aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block 0.0.0.0/0
 --gateway-id igw-01234567890abcdef
```

4. 对每个区域中的每个应用程序子网路由表重复此操作。

网关负载均衡器

使用网关 Load Balancer 部署和管理支持 GENEVE 协议的虚拟设备队列。

网关 Load Balancer 在开放系统互连（OSI）模型的第三个层运行。它侦听所有端口上的所有 IP 数据包，并使用端口 6081 上的 GENEVE 协议将流量转发到侦听器规则中指定的目标组。

您可以根据需求变化在负载均衡器中添加或删除目标，而不会中断请求的整体流。Elastic Load Balancing 会在应用程序的流量随时间的推移发生更改时扩展负载均衡器。Elastic Load Balancing 可以自动扩展到绝大部分工作负载。

目录

负载均衡器状态

网关Load Balancer可能处于下列状态之一：

`provisioning`

正在设置网关Load Balancer。

`active`

网关Load Balancer已完全设置并准备好路由流量。

`failed`

无法设置网关Load Balancer。

负载均衡器属性

以下是网关负载均衡器的负载均衡器属性：

`deletion_protection.enabled`

指示是否启用删除保护 (p. 11)。默认值为 `false`。

`load_balancing.cross_zone.enabled`

指示是否启用了跨区域负载均衡 (p. 12)。默认值为 `false`。

删除保护

要防止网关Load Balancer被意外删除，您可以启用删除保护。默认情况下，将禁用删除保护。

如果您为网关Load Balancer启用删除保护，则必须先禁用删除保护，然后才能删除网关Load Balancer。

使用控制台启用删除保护

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择 Gateway Load Balancer（网关负载均衡器）。
4. 选择 Actions（操作）、Edit attributes（编辑属性）。
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. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择 Gateway Load Balancer（网关负载均衡器）。
4. 依次选择 Actions（操作）和 Edit attributes（编辑属性
5. 在编辑负载均衡器属性页面上，为删除保护清除启用，然后选择保存。

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。

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。如果您启用跨区域负载均衡，则每个网关Load Balancer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. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择 Gateway Load Balancer（网关负载均衡器）。
4. 依次选择 Actions（操作）和 Edit attributes（编辑属性
5. 在 Edit load balancer attributes（编辑负载均衡器属性）页面上，为 Cross-Zone Load Balancing（跨区域负载均衡）选择 Enable（启用），然后选择 Save（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。

创建网关负载均衡器

网关 Load Balancer 从客户端接收请求，并在目标组（如 EC2 实例）中的目标之间分配这些请求。

在开始之前，请确保您的网关 Load Balancer 的 Virtual Private Cloud（VPC）在您具有目标的每个可用区中至少有一个子网。

要使用 AWS CLI 创建网关 Load Balancer 请参阅开始使用 CLI (p. 6)。

要使用 AWS 管理控制台创建网关 Load Balancer 请完成以下任务。

任务

- 步骤 1：配置负载均衡器和侦听器 (p. 13)
- 步骤 4：配置目标组 (p. 13)
- 步骤 3：向目标组注册目标 (p. 13)
- 步骤 6：创建负载均衡器 (p. 12)

步骤 1：配置负载均衡器和侦听器

首先，为网关Load Balancer提供一些基本配置信息，例如名称和网络。负载均衡器的侦听器将侦听所有端口上的所有 IP 数据包。

配置负载均衡器和侦听器

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择 Create Load Balancer。
4. 对于 Gateway Load Balancer （网关负载均衡器），选择 Create （创建）。
5. 对于 Name （名称），输入网关 Load Balancer 的名称。例如，**`my-load-balancer`**。
6. 对于 Availability Zones （可用区），选择用于设备实例的 VPC。对于用于启动实例的每个可用区，选择一个可用区，然后为该可用区选择子网。
7. （可选）展开 Tags （标签） 并添加标签。
8. 选择 Next: Configure Routing。

步骤 4：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，请参阅目标组 (p. 17)。

配置目标组

1. 对于 Target group，保留默认值 New target group。
2. 对于名称，输入目标组的名称。
3. 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。
4. 协议必须为 `GENEVE`，端口必须为 `6081`。
5. （可选）对于 Health checks （运行状况检查），根据需要修改运行状况检查设置。
6. 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。目标组的目标类型确定如何向该目标组注册目标。

通过实例 ID 注册目标

1. 对于 Instances，选择一个或多个实例，然后选择 Add to registered。
2. 将实例添加到列表后，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 IP，输入地址。
   c. 选择 Add to list。
2. 在将 IP 地址添加到列表中后，选择 Next: Review。

步骤 6：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，请参阅删除负载均衡器 (p. 15)。

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. 在导航窗格的 Load Balancing (负载均衡) 下，选择 Target Groups (目标组)。
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。

网关Load Balancer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。每个网关Load Balancer的标签键必须是唯一的。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。

使用完标签后，您可以从网关Load Balancer中将其删除。

Restrictions

- 每个资源的标签数上限 – 50
- 最大键长度 – 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：+ - = . _ : / @。 请勿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。

使用控制台更新网关Load Balancer的标签

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择 Gateway Load Balancer （网关负载均衡器）。
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 （键） 和 Value （值），输入值。
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 更新网关 Load Balancer 的标签

使用 add-tags 和 remove-tags 命令。

删除网关Load Balancer

一旦您的网关Load Balancer变为可用状态，您就需要为保持其运行的每小时或部分小时付费。当您不再需要网关Load Balancer时，可以将其删除。在删除网关Load Balancer后，您便不再需要支付其费用。

如果网关Load Balancer正被其他服务使用，则无法删除该负载均衡器。例如，如果网关 Load Balancer 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网关 Load Balancer 。

删除网关Load Balancer也会删除其侦听器。删除网关Load Balancer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. 27)。

使用控制台删除 n 网关 Load Balancer

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择 Gateway Load Balancer （网关负载均衡器）。
4. 依次选择 Actions 和 Delete。
5. 当系统提示进行确认时，选择 Yes, Delete。

使用 AWS CLI 删除网关 Load Balancer

使用 delete-load-balancer 命令。

网关负载均衡器的侦听器

在创建网关Load Balancer时，您将添加一个侦听器。侦听器是用于检查连接请求的进程。

网关负载均衡器的侦听器将侦听所有端口上的所有 IP 数据包。为网关Load Balancer创建侦听器时，无法指定协议或端口。您无法删除网关Load Balancer的侦听器。

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。您可以更新侦听器规则以将请求转发到不同的目标组。

使用控制台更新侦听器

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
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 Edit listener （编辑侦听器）。
5. 对于 Forwarding to target group （转发到目标组），选择一个目标组。
6. 选择 Save。

使用 AWS CLI 更新侦听器

使用 modify-listener 命令。

网关负载均衡器的目标组

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。

您可以为每个目标组定义网关Load Balancer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。在侦听器的规则中指定目标组后，网关Load Balancer会持续监控已注册到目标组（位于为网关Load Balancer启用的可用区中）的所有目标的运行状况。网关Load Balancer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 (p. 20)。

目录

路由配置

网关负载均衡器的目标组支持以下协议和端口：

- 协议：GENEVE
- 端口：6081

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，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。

已注册目标

您的网关Load Balancer充当客户端的单一接触点，并在其正常运行的已注册目标之间分配传入流量。每个目标组必须在为网关Load Balancer启用的每个可用区中至少有一个注册目标。您可以将每个目标注册到一个或多个目标组中。

如果需求增加，您可以向一个或多个目标组注册其他目标，以满足需求。一旦注册过程完成，网关Load Balancer就会开始将流量路由到新注册的目标。

如果需求减少，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。一旦取消注册网关Load Balancer，它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。

目标组属性

以下是目标组属性：

`deregistration_delay.timeout_seconds`

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

取消注册延迟

当您取消注册实例时，网关Load Balancer会停止创建与实例的新连接。网关Load Balancer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，则网关Load Balancer可以继续向该实例发送流量。要确保关闭现有连接，您可以在取消注册实例之前验证实例是否运行状况不佳，也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，网关 Load Balancer 会在 300 秒`unused`后将取消注册的目标的状态更改为 。要更改网关 Load Balancer 在将取消注册的目标的状态更改为 之前等待的时间`unused`，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。

New console

使用新控制台更新注销延迟值

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格的 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. 在组详细信息页面的属性部分中，选择编辑。

5. 在编辑属性页面上，根据需要更改注销延迟的值。
6. 选择保存更改。

Old console

使用旧控制台更新注销延迟值

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格的 Load Balancing (负载均衡) 下，选择 Target Groups (目标组)。
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。

为网关Load Balancer创建目标组

您可以使用目标组为网关Load Balancer注册目标。

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 (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，请参阅注册目标 (p. 23)。您也可以修改目标组的运行状况检查设置。有关更多信息，请参阅修改运行状况检查设置 (p. 23)。

New console

使用新控制台创建目标组

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
3. 选择 Create target group。
4. 对于选择目标类型，选择实例以使用实例 ID 注册目标，或者选择 IP 地址以通过 IP 地址注册目标。
5. 对于 Target group name （目标组名称），输入目标组的名称。此名称在每个 账户的每个区域必须唯一，最多可以有 32 个字符，只能包含字母数字字符或连字符，并且不能以连字符开头或结尾。
6. 对于 Protocol （协议），请使用 GENEVE。使用 GENEVE 协议时，Port （端口） 必须为 6081。
7. 对于 VPC，选择 Virtual Private Cloud (VPC)。
8. （可选）在运行状况检查部分中，根据需要修改默认设置。
9. （可选）展开 Tags （标签） 部分并添加一个或多个标签。要添加标签，请选择 Add tag （添加标签），然后输入标签键和标签值。
10. 选择 Next。
11. （可选）添加一个或多个目标，如下所示：
    - 如果目标类型为实例，请选择一个或多个实例，输入一个或多个端口，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。
12. 选择 Create target group。

Old console

使用旧控制台创建目标组

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
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（目标组名称），输入目标组的名称。此名称在每个 账户的每个区域必须唯一，最多可以有 32 个字符，只能包含字母数字字符或连字符，并且不能以连字符开头或结尾。
5. 对于 Protocol（协议），请使用 GENEVE。对于 GENENVE 协议，Port 必须为 6081。
6. 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。
7. 对于 VPC，选择 Virtual Private Cloud (VPC)。
8. (可选) 对于 Health check settings 和 Advanced health check settings，根据需要修改默认设置。选择创建。
9. (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。
10. (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. 23)。

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

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，网关Load Balancer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。

网关Load Balancer会定期向每个已注册目标发送请求以检查其状态。每个节点都使用目标注册到的目标组的运行状况检查设置来检查每个目标的运行状况。完成每个运行状况检查后，节点将关闭为运行状况检查而建立的连接。

运行状况检查设置

您可以使用以下设置为目标组中的目标配置主动运行状况检查。如果运行状况检查超出了指定的 UnhealthyThresholdCount 连续失败次数，则网关 Load Balancer 将禁用目标。当运行状况检查超过指定的 HealthyThresholdCount 连续成功次数时，网关 Load Balancer 会将目标恢复运行。

设置	描述
HealthCheckProtocol	负载均衡器在对目标执行运行状况检查时使用的协议。可能的协议有 HTTP、HTTPS 和 TCP。默认值为 TCP。
HealthCheckPort	Gateway Load Balancer 在对目标执行运行状况检查时使用的端口。范围为 1 至 65535。默认值为 80。

设置	描述
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 /。
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 至 120。默认值为 5。
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 至 300。默认值为 10 秒。此值必须大于或等于 HealthCheckTimeoutSeconds。 Important 分配网关负载均衡器的运行状况检查，并使用共识机制来确定目标运行状况。因此，您应该期望目标设备在配置的时间间隔内接收多个运行状况检查。
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。范围为 2 至 10。默认值为 3。
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。该值必须为 200-399。

目标运行状况

在网关Load Balancer将运行状况检查请求发送到目标之前，您必须将其注册到目标组，在侦听器规则中指定其目标组，并确保为网关Load Balancer启用了目标的可用区。

下表描述已注册目标的正常状态的可能值。

值	描述
`initial`	网关Load Balancer正在注册目标或在目标上执行初始运行状况检查。 相关原因代码：`Elb.RegistrationInProgress` | `Elb.InitialHealthChecking`
`healthy`	目标正常。 相关原因代码：无
`unhealthy`	目标未响应运行状况检查或未通过运行状况检查。 相关原因代码：`Target.FailedHealthChecks`
`unused`	目标未注册到目标组，侦听器规则中未使用目标组，或者目标在没有启用的可用区中，或者目标处于停止或终止状态。 相关原因代码： `Target.NotRegistered` | `Target.NotInUse` | `Target.InvalidState` | `Target.IpUnusable`

值	描述
`draining`	目标正在取消注册，连接即将耗尽。 相关原因代码：`Target.DeregistrationInProgress`
`unavailable`	目标运行状况不可用。 相关原因代码：`Elb.InternalError`

运行状况检查原因代码

如果目标的状态是 以外的任何值`Healthy`，则 API 将返回问题的原因代码和描述，并且控制台将显示相同的描述。以 开头的原因代码`Elb`源自网关 Load Balancer 端，以 开头的原因代码`Target`源自目标端。

原因代码	描述
`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`	目标组未配置为从网关Load Balancer接收流量 目标位于未为网关Load Balancer启用的可用区中
`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。

New console

使用新控制台检查目标的运行状况

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Targets 选项卡上，Status 列指示每个目标的状态。
5. 如果目标状态是 `Healthy` 以外的任何值，则状态详细信息列将包含更多信息。

Old console

使用旧控制台检查目标的运行状况

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
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 以外的任何值`Healthy`，则控制台将显示更多信息。

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。

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 函数以发送有关运行状况不佳的目标的详细信息。有关分步说明，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。

New console

使用新控制台修改目标组的运行状况检查设置

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
3. 选择目标组的名称以打开其详细信息页面。
4. 在组详细信息选项卡的运行状况检查设置部分中，选择编辑。
5. 在编辑运行状况检查设置页面上，根据需要修改设置，然后选择保存更改。

Old console

使用旧控制台修改目标组的运行状况检查设置

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
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

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。您可以通过实例 ID 或 IP 地址注册目标。一旦注册过程完成且目标通过初始运行状况检查，网关Load Balancer就会开始将请求路由到目标。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 (p. 20)。

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网关Load Balancer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。

取消注册目标时 Elastic Load Balancing 会等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 (p. 18)。

目标安全组

将 EC2 实例注册为目标时，必须确保这些实例的安全组允许端口 6081 上的流量。

网关负载均衡器没有关联的安全组。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。

网络 ACL

将 EC2 实例注册为目标时，必须确保实例子网的网络访问控制列表（ACL）允许端口 6081 上的流量。VPC 的默认网络 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。

注册或取消注册目标

每个目标组必须在为网关Load Balancer启用的每个可用区中至少有一个注册目标。

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 (p. 17)。

Requirements

- 如果实例位于与负载均衡器 VPC 对等的 VPC（相同区域或不同区域）中，则不能用实例 ID 注册实例。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。

New console

使用新控制台按实例 ID 注册或取消注册目标

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格的 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. 选择 Targets 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，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。

6. 要取消注册实例，请选择实例，然后选择取消注册。

Old console

使用旧控制台按实例 ID 注册或取消注册目标

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
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（实例），选择要注册的任何正在运行的实例，然后选择 Add to registered（添加到已注册实例）。
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)

New console

使用新控制台按 IP 地址注册或取消注册目标

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格的 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. 选择 Targets 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 地址和端口，然后选择在下面以待注册的形式添加。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，然后选择注销。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。

Old console

使用旧控制台按 IP 地址注册或取消注册目标

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
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。

Restrictions

- 每个资源的标签数上限 – 50
- 最大键长度 – 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：+ - = . _ : / @。 请勿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。

New console

使用新控制台更新目标组的标签

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格的 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。

Old console

使用旧控制台更新目标组的标签

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
2. 在导航窗格的 Load Balancing (负载均衡) 下，选择 Target Groups (目标组)。
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，请选择创建标签，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。

New console

使用新控制台删除目标组

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
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. 当系统提示进行确认时，选择是，删除。

Old console

使用旧控制台删除目标组

1. 通过 https://console.aws.amazon.com/ec2/ 打开 Amazon EC2 控制台。
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。

监控网关负载均衡器

您可以使用以下功能来监控网关负载均衡器以分析流量模式并解决问题。但是，网关 Load Balancer 不会生成访问日志，因为它是不会终止流的透明第 3 层负载均衡器。要接收访问日志，您必须在网关 Load Balancer 目标设备（如防火墙、IDS/IPS 和安全设备）上启用访问日志记录。此外，您还可以选择在网关负载均衡器上启用 VPC 流日志。

CloudWatch 指标

您可以使用 Amazon CloudWatch 检索有关网关负载均衡器和目标的数据点的统计数据，作为一组有序的时间序列数据（称为指标）。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，请参阅网关 Load Balancer 的 CloudWatch 指标 (p. 28)。

VPC 流日志

您可以使用 VPC 流日志来捕获有关传入和传出网关 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。

为网关Load Balancer的每个网络接口创建流日志。每个子网有一个网络接口。要标识网关Load Balancer的网络接口，请在网络接口的描述字段中查找网关Load Balancer的名称。

每个通过网关Load Balancer的连接有两个条目，一个用于客户端和网关Load Balancer之间的前端连接，另一个用于网关Load Balancer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，但子网的网络 ACLs 允许连接，则网关 Load Balancer 的网络接口的日志将显示前端和后端连接的“ACCEPT OK”，而实例的网络接口的日志显示“REJECT OK”。

CloudTrail 日志

您可以使用 AWS CloudTrail 捕获有关对 Elastic Load Balancing API 进行的调用的详细信息，并将其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 记录网关 Load Balancer 的 API 调用 (p. 31)。

网关 Load Balancer 的 CloudWatch 指标

Elastic Load Balancing 将网关负载均衡器和目标的数据点发布到 Amazon CloudWatch 。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网关Load Balancer的正常运行的目标总数。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）。

Elastic Load Balancing 仅在请求流经网关 Load Balancer 时才向 CloudWatch 报告指标。如果存在请求流 Elastic Load Balancing 会每隔 60-second测量并发送其指标。如果没有请求流式处理或指标没有数据，则不会报告指标。

有关更多信息，请参阅 Amazon CloudWatch 用户指南。

目录

- 查看网关 Load Balancer 的 CloudWatch 指标 (p. 30)

网关Load Balancer指标

AWS/GatewayELB 命名空间包括以下指标。

指标	描述
ActiveFlowCount	客户端至目标的并发流（或连接）的总数。 报告标准：有非零值 Statistics：最有用的统计工具是 Average、Maximum 和 Minimum。 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 Dimensions • 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。 Dimensions • 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 Statistics：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。此计数包括进出目标的流量，但不包括运行状况检查流量。 报告标准：有非零值 Statistics：最有用的统计工具是 Sum。

指标	描述
	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。 Dimensions • LoadBalancer, TargetGroup • AvailabilityZone, LoadBalancer, TargetGroup

网关负载均衡器的指标维度

要筛选网关Load Balancer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	按网关Load Balancer筛选指标数据。按如下所示指定网关 Load Balancer 网关/负载均衡器名称/1234567890123456 的最后部分）。
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）。

查看网关 Load Balancer 的 CloudWatch 指标

您可以使用 Amazon EC2 控制台查看网关负载均衡器的 CloudWatch 指标。这些指标显示为监控图表。如果网关Load Balancer处于活动状态并收到请求，监控图表会显示数据点。

或者，您可以使用 CloudWatch 控制台查看网关 Load Balancer 的指标。

使用 Amazon EC2 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. 要查看按网关Load Balancer筛选的指标，请执行以下操作：
   a. 在导航窗格中，选择 Load Balancers。
   b. 选择网关Load Balancer，然后选择监控。
   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.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择 Metrics。
3. 选择 GatewayELB 命名空间。
4. （可选）要跨所有维度查看某个指标，请在搜索字段中输入其名称。

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/GatewayELB
```

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/GatewayELB \
--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": "2020-12-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2020-12-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

使用 AWS CloudTrail 记录网关 Load Balancer 的 API 调用

Elastic Load Balancing 与 AWS CloudTrail 集成，后者是一项在 Elastic Load Balancing 中提供用户、角色或 AWS 服务所采取操作的记录的服务。CloudTrail 将 Elastic Load Balancing 的所有 API 调用作为事件捕获。捕获的调用包括来自 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 控制台中的 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 CloudTrail 的更多信息，请参阅 AWS CloudTrail 用户指南。

CloudTrail 中的 Elastic Load Balancing 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 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https://docs.amazonaws.cn/awscloudtrail/latest/userguide/view-cloudtrail-events.html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 trail (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。此跟踪记录来自 AWS 分区中的所有区域的事件，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操作。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
- 从多个区域接收 CloudTrail 日志文件和从多个账户https://docs.amazonaws.cn/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.html中接收 CloudTrail 日志文件

网关负载均衡器的所有 Elastic Load Balancing 操作均由 CloudTrail 记录，并记录在 Elastic Load Balancing API 参考版本 2015-12-01 中。例如，对 `CreateLoadBalancer` 和 `DeleteLoadBalancer` 操作的调用将在 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：

- 发出请求使用的是根凭证还是 AWS Identity and Access Management (IAM) 用户凭证。
- 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。
- 是否由其他 AWS 服务发出请求。

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，因此它们不会按任何特定顺序显示。

日志文件包含您的 AWS 账户的所有 AWS API 调用（而不只是 Elastic Load Balancing API 调用）的事件。您可以通过检查是否有值为 的`eventSource`元素来查找对 Elastic Load Balancing API 的调用`elasticloadbalancing.amazonaws.com`。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。

以下是为使用 AWS CLI 创建并删除网关 Load Balancer 的用户创建 Elastic Load Balancing 的示例 CloudTrail 日志记录。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": "2020-12-11T15:31:48Z",
    "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"],
        "name": "my-load-balancer",
        "type": "gateway"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "gateway",
            "loadBalancerName": "my-load-balancer",
            "vpcId": "vpc-3ac0fb5f",
            "state": {"code":"provisioning"},
            "availabilityZones": [
               {"subnetId":"subnet-8360a9e7","zoneName":"us-west-2a"},
               {"subnetId":"subnet-b7d581c0","zoneName":"us-west-2b"}
            ],
            "createdTime": "Dec 11, 2020 5:23:50 PM",
            "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/gateway/my-load-balancer/ffcddace1759e1d0",
        }]
    },
    "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": "2020-12-12T15:31:48Z",
    "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/gateway/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"
}
```

网关负载均衡器的配额

您的 AWS 账户对于每个 AWS 服务都具有默认配额（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。

要查看网关负载均衡器的配额，请打开 Service Quotas 控制台。在导航窗格中，选择 AWS services (AWS 服务)，然后选择 Elastic Load Balancing。

要请求增加配额，请参阅 Service Quotas 用户指南中的请求增加配额。如果配额在 Service Quotas 中尚不可用，请使用 限制提高表单。

您的 AWS 账户具有以下与网关负载均衡器相关的配额。

负载均衡器

- 每个区域的网关负载均衡器数：20
- 每个 VPC 的网关负载均衡器数：10

目标组

- 使用 GENEVE 协议的目标组数：100
- 使用 GENEVE 协议的每个目标组的每个可用区的目标数：300

网关负载均衡器的文档历史记录

下表介绍了网关负载均衡器的版本。

update-history-change	update-history-description	update-history-date
首次发布 (p. 36)	此版本的 Elastic Load Balancing 引入了网关负载均衡器。	2020 年 11 月 10 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。