网络负载均衡器

Elastic Load Balancing

Elastic Load Balancing: 网络负载均衡器

Table of Contents

什么是网络负载均衡器？

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

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

网络负载均衡器组件

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

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

目标组使用指定的协议和端口号将请求路由到一个或多个已注册的目标（例如 EC2 实例）。网络负载均衡器目标组支持 TCP、UDP、TCP_UDP、TLS、QUIC 和 TCP_QUIC 协议。您可以向多个目标组注册一个目标。您可以对每个目标组配置运行状况检查。对负载均衡器的默认操作中指定的目标组所注册的所有目标执行运行状况检查。

有关更多信息，请参阅以下文档：

- 负载均衡器
- 侦听器
- 目标组

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。负载均衡器从客户端接收请求后，会从默认操作中的目标组中选择目标。将尝试使用您指定的协议和端口将请求发送至所选目标。

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

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

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

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

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

对于 QUIC 流量，负载均衡器将根据 Connection ID (CID) 中指定的 Server ID 来选择目标。对于初始连接尝试中缺少 Server ID 的情况，将采用基于协议、源 IP 地址、源端口、目标 IP 地址和目标端口的流哈希算法进行选择。一旦建立 Connection ID，该 CID 的流量将在该 CID 的生命周期内始终路由至同一目标。

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

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

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

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

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

从经典负载均衡器迁移的好处

使用网络负载均衡器而不是经典负载均衡器具有以下好处：

- 可以处理急剧波动的工作负载，并可以扩展到每秒处理数百万个请求。
- 支持将静态 IP 地址用于负载均衡器。还可以针对为负载均衡器启用的每个子网分配一个弹性 IP 地址。
- 支持通过 IP 地址注册目标，包括位于负载均衡器的 VPC 之外的目标。
- 支持将请求路由到单个 EC2 实例上的多个应用程序。可以使用多个端口向同一个目标组注册每个实例或 IP 地址。
- 支持容器化的应用程序。计划任务时，Amazon Elastic Container Service (Amazon ECS) 可以选择一个未使用的端口，并可以使用此端口向目标组注册该任务。这样可以高效地使用您的群集。
- Support 支持独立监控每项服务的运行状况，因为运行状况检查是在目标群体级别定义的，而许多 Amazon CloudWatch 指标是在目标群体级别报告的。将目标组挂载到 Auto Scaling 组的功能使您能够根据需求动态扩展每个服务。
- 支持 QUIC 和 TCP_QUIC 协议，具备高级拥塞控制、更少的往返连接建立次数、内置 TLS 以及跨网络连接迁移功能。

要详细了解每种负载均衡器类型支持的功能，请参阅 弹性负载均衡 产品比较。

开始使用

要使用 AWS 管理控制台、 AWS CLI或创建 Network Load Balancer AWS CloudFormation，请参阅创建网络负载均衡器。

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

定价

有关更多信息，请参阅 弹性负载均衡 定价。

网络负载均衡器

网络负载均衡器充当客户端的单一接触点。客户端向网络负载均衡器发送请求，网络负载均衡器将请求发送到一个或多个可用区域中的目标，例如 EC2 实例。

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

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

内容

负载均衡器状态

网络负载均衡器可能处于下列状态之一：

`provisioning`

正在设置网络负载均衡器。

`active`

网络负载均衡器已完全设置并准备好路由流量。

`failed`

无法设置网络负载均衡器。

IP 地址类型

您可以设置客户端可与您的网络负载均衡器结合使用的 IP 地址类型。

网络负载均衡器支持以下 IP 地址类型：

`ipv4`

客户端必须使用 IPv4 地址（例如 192.0.2.1）进行连接。

`dualstack`

客户端可以使用地址（例如 192.0.2.1）和 IPv4 IPv6 地址（例如，2001:0 db 8:85 a 3:0:0:8 a2e：0370:7334）连接到 Network Load Balancer。

注意事项

- 网络负载均衡器根据目标组的 IP 地址类型与目标进行通信。
- 要支持 UDP IPv6 侦听器的源 IP 保留，请确保已启用 “为 IPv6 源 NAT 启用前缀”。
- 当您为网络负载均衡器启用双堆栈模式时，弹性负载均衡为网络负载均衡器提供 AAAA DNS 记录。使用 IPv4 地址与 Network Load Balancer 通信的客户端解析 A DNS 记录。使用 IPv6 地址与 Network Load Balancer 通信的客户端会解析 AAAA DNS 记录。
- 阻止通过互联网网关对内部双堆栈网络负载均衡器的访问，以防意外访问互联网。但是，这并不能阻止其他互联网访问（例如，通过对等互连、Transit Gateway 或 Site-to-Site VPN）。 AWS Direct Connect

有关更多信息，请参阅 更新网络负载均衡器的 IP 地址类型。

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。如果客户端或目标在空闲超时期限内没有通过连接发送任何数据，则不再跟踪该连接。如果客户端或目标在空闲超时期限后发送数据，则客户端会收到一个 TCP RST 数据包，以指示连接不再有效。

TCP 流的默认空闲超时值为 350 秒，但可以更新为 60-6000 秒之间的任何值。客户端或目标可以使用 TCP keepalive 数据包重启空闲超时。为维护 TLS 连接而发送的 Keepalive 数据包不能包含数据或负载。

TLS 侦听器的连接空闲超时为 350 秒，且无法修改。当 TLS 侦听器收到来自客户端或目标的 TCP keepalive 数据包时，负载均衡器会生成 TCP keepalive 数据包，并每 20 秒将它们发送到前端和后端连接。您不能修改此行为。

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

EC2 实例必须在 30 秒内响应新请求才能建立返回路径。

有关更多信息，请参阅 更新空闲超时。

负载均衡器属性

您可以通过编辑网络负载均衡器的属性来对其进行配置。有关更多信息，请参阅 编辑负载均衡器属性。

网络负载均衡器的负载均衡器属性如下：

`access_logs.s3.enabled`

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

`access_logs.s3.bucket`

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

`access_logs.s3.prefix`

Amazon S3 存储桶中位置的前缀。

`deletion_protection.enabled`

指示是否启用删除保护。默认为 `false`。

`ipv6.deny_all_igw_traffic`

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

`load_balancing.cross_zone.enabled`

指示是否启用了跨可用区负载均衡。默认值为 `false`。

`dns_record.client_routing_policy`

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

`secondary_ips.auto_assigned.per_subnet`

需要配置的辅助 IP 地址数量。当无法添加目标时，可用于解决端口分配错误。有效范围为 0 到 7。默认值是 0。此值设定后无法降低。

`zonal_shift.config.enabled`

指示是否已启用可用区转移。默认值为 `false`。

跨可用区负载均衡

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

DNS 名称

每个 Network Load Balancer 都会收到一个默认的域名系统 (DNS) 名称，其语法如下：*name-id* .elb。 *region*.amazonaws.com。例如， my-load-balancer-1234567890abcdef。elb.us-east-2.amazonaws.com。

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

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

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

Linux 或 Mac

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

Windows

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

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

Linux 或 Mac

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

Windows

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

负载均衡器可用区运行状况

对于每个已启用的可用区，网络负载均衡器在 Route 53 中都具有可用区 DNS 记录和 IP 地址。当网络负载均衡器未能通过特定可用区的可用区运行状况检查时，将从 Route 53 中移除其 DNS 记录。负载均衡器区域运行状况使用 Amazon CloudWatch 指标进行监控`ZonalHealthStatus`，让您可以更深入地了解导致故障转移的事件，从而实施预防措施来确保最佳的应用程序可用性。有关更多信息，请参阅网络负载均衡器指标。

网络负载均衡器可能由于多种原因无法通过可用区运行状况检查，从而导致其变得运行状况不佳。请参阅下文，了解未通过可用区运行状况检查导致网络负载均衡器运行状况不佳的常见原因。

请检查以下可能原因：

- 负载均衡器没有运行状况正常目标
- 运行状况正常目标数量少于配置的最小值
- 正在进行可用区转移或可用区自动移位
- 由于检测到问题，流量正在自动转移到运行状况良好区域

创建网络负载均衡器

Network Load Balancer 接受来自客户端的请求，并将其分配到目标组中的目标（例如 EC2 实例）。有关更多信息，请参阅the section called “网络负载均衡器概述”。

任务

- 先决条件
- 创建负载均衡器
- 测试负载均衡器
- 后续步骤

先决条件

- 确定您的应用程序将支持哪些可用区和 IP 地址类型。在每个可用区中配置包含子网的负载均衡器 VPC。如果应用程序同时支持 IPv4 和 IPv6 流量，请确保子网同时支持 IPv4 和。 IPv6 CIDRs在每个可用区中至少部署一个目标。

- 确保目标实例的安全组允许侦听器端口上来自客户端 IP 地址 (如果目标通过实例 ID 指定) 或负载均衡器节点 (如果目标通过 IP 地址指定) 的流量。有关更多信息，请参阅 the section called “目标安全组”。
- 确保目标实例的安全组允许来自负载均衡器的流量使用运行状况检查协议通过运行状况检查端口。
- 如果您计划为负载均衡器提供静态 IP 地址，请确保每个弹性 IP IPv4 地址都来自亚马逊的地址池，并且其网络边界组与负载均衡器相同。
- 如果您计划使用 QUIC 或 TCP_QUIC 侦听器，请确保网络负载均衡器使用 `ipv4` 地址类型并且没有与之关联的安全组。

创建负载均衡器

在创建网络负载均衡器的过程中，您将创建负载均衡器、至少一个侦听器和至少一个目标组。当负载均衡器在每个已启用的可用区中至少有一个正常运行的注册目标时，它即可处理客户端请求。

Console

要创建网络负载均衡器

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择负载均衡器。
3. 选择创建负载均衡器。
4. 在网络负载均衡器下，选择创建。
5. 基本配置
   a. 对于负载均衡器名称，输入网络负载均衡器的名称。名称必须在区域的负载均衡器组中是唯一的。它最多可包含 32 个字符，并且只包含字母数字字字符和连字符。它不能以连字符或 `internal-` 开头或结尾。
   b. 对于 Scheme (方案)，选择 Internet-facing (面向 Internet) 或 Internal (内部)。面向互联网的网络负载均衡器将来自客户端的请求通过互联网路由到目标。内部网络负载均衡器使用私有 IP 地址将请求路由到目标。
   c. 对于负载均衡器 IP 地址类型，请选择IPv4您的客户端是使用 IPv4 地址与网络负载均衡器通信，如果您的客户端同时使用 IPv4 和 IPv6 地址与网络负载均衡器通信，则选择双栈通信。
6. 网络映射

a. 对于 VPC，请选择您为负载均衡器准备的 VPC。对于面向互联网的负载均衡器，只能选择 VPCs 带有互联网网关的负载均衡器。

b. 使用双栈负载均衡器，除非源 NAT 的启用前缀为 On（每个子网的 IPv6 源 NAT 前缀），否则无法添加 UDP 侦听器。

c. 对于可用区和子网，请至少选择一个可用区，然后为每个区域选择一个子网。请注意，共享给您的子网可供选择。

   如果您选择多个可用区，并确保在每个选定区域中都注册了目标，那么这将提高您应用程序的容错能力。

d. 借助面向互联网的负载均衡器，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。

   使用内部负载均衡器，您可以从每个子网 IPv4 的地址范围内输入私有地址，也可以让您 AWS 选择一个私有地址。

   使用双栈负载均衡器，您可以从每个子网的地址范围内输入一个 IPv6 地址，也可以让您 AWS 选择一个地址。

   对于启用了源 NAT 的负载均衡器，您可以输入自定义 IPv6 前缀或让我们为您 AWS 选择一个前缀。

7. 安全组

我们会为负载均衡器 VPC 预选默认安全组。您可以根据需要选择其他安全组。如果您没有可满足您需求的安全组，请选择创建新的安全组，以立即创建一个。有关更多信息，请参阅《Amazon VPC 用户指南》中的创建安全组。

> **Warning**
>
> 如果您现在没有将任何安全组与网络负载均衡器关联，则无法以后再将其关联。

> **Warning**
>
> 要使用 QUIC 或 TCP_QUIC 侦听器，您的网络负载均衡器必须没有安全组。

8. 侦听器和路由

a. 默认值是负责接收端口 80 上的 TCP 流量的侦听器。您可保留默认侦听器设置，或者根据需要修改协议和端口。

b. 对于默认操作，选择一个要将流量转发到的目标组。

要添加其他目标组，请选择添加目标组，并根据需要更新权重。

如果您还没有能满足您需求的目标组，请选择创建目标组，以立即创建一个目标组。有关更多信息，请参阅 创建目标组。

c. （可选）选择添加侦听器标签，然后输入标签键和标签值。

d. （可选）选择添加侦听器，以添加其他侦听器（例如，TLS 侦听器）。

9. 安全侦听器设置

仅当您添加 TLS 侦听器时，才会显示此部分。

a. 对于安全策略，请选择符合您要求的安全策略。有关更多信息，请参阅 安全策略。

b. 对于默认 SSL/TLS 服务器证书，请选择来自 ACM 作为证书来源。选择您使用 AWS Certificate Manager预置或导入的证书。如果您在 ACM 中没有可用的证书，但有可用于负载均衡器的证书，请选择导入证书，并提供所需的信息。否则，请选择请求新的 ACM 证书。有关更多信息，请参阅《AWS Certificate Manager 用户指南》中的 AWS Certificate Manager 证书。

c. （可选）对于 ALPN 策略，请选择一个策略以启用 ALPN。有关更多信息，请参阅 the section called “ALPN 策略”。

10. 负载均衡器标签

（可选）展开负载均衡器标签。（可选）选择添加新的标签，然后输入标签键和标签值。有关更多信息，请参阅标签。

11. 摘要

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

AWS CLI

要创建网络负载均衡器

使用 create-load-balancer 命令。

以下示例创建了一个面向互联网的负载均衡器，包括两个已启用的可用区和一个安全组。

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

要创建内部负载均衡器

包含如下示例所示的 `--scheme` 选项。

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --scheme internal \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

要创建双堆栈网络负载均衡器

包含如下示例所示的 `--ip-address-type` 选项。

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --ip-address-type dualstack \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

添加侦听器

使用 create-listener 命令。有关示例，请参阅 创建侦听器。

CloudFormation

要创建网络负载均衡器

定义类型为的资源AWS::ElasticLoadBalancingV2::LoadBalancer。

```
Resources:
```

```
myLoadBalancer:
  Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
  Properties:
    Name: my-nlb
    Type: network
    Scheme: internal
    IpAddressType: dualstack
    Subnets:
      - !Ref subnet-AZ1
      - !Ref subnet-AZ2
    SecurityGroups:
      - !Ref mySecurityGroup
    Tags:
      - Key: 'department'
        Value: '123'
```

添加侦听器

定义类型为的资源AWS::ElasticLoadBalancingV2::Listener。有关示例，请参阅 创建侦听器。

测试负载均衡器

创建网络负载均衡器后，您可以验证您的 EC2 实例是否已通过初始运行状况检查，然后测试网络负载均衡器是否正在向您的 EC2 实例发送流量。要删除网络负载均衡器，请参阅删除网络负载均衡器。

测试网络负载均衡器

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

后续步骤

创建负载均衡器后，您可能需要执行以下操作：

- 配置负载均衡器属性。
- 配置目标组属性。
- [TLS 侦听器] 将证书添加到可选证书列表。
- 配置监控功能。

更新网络负载均衡器的可用区

您可随时启用或禁用网络负载均衡器的可用区。当启用某个可用区时，您必须指定该可用区中的一个子网。在启用一个可用区后，负载均衡器会开始将请求路由到该可用区中的已注册目标。如果您确保每个启用的可用区均具有至少一个注册目标，则负载均衡器将具有最高效率。启用多个可用区有助于提高应用程序的容错能力。

Elastic Load Balancing 会在您选择的可用区中创建一个网络负载均衡器节点，并在该可用区中为选定子网创建一个网络接口。可用区中的每个 Network Load Balancer 节点都使用网络接口获取 IPv4 地址。您可以查看这些网络接口，但无法对其进行修改。

注意事项

- 对于面向互联网的网络负载均衡器，您指定的子网必须至少具有 8 个可用 IP 地址。对于内部网络负载均衡器，只有当您允许从子网 AWS 中选择私有 IPv4 地址时，才需要这样做。
- 无法指定受约束可用区中的子网。但是，您可以在不受约束的其他可用区中指定子网，并使用跨可用区负载均衡将流量分发至受约束可用区中的目标。
- 您无法在本地区域中指定子网。
- 如果网络负载均衡器具有活跃的 Amazon VPC 端点关联，则无法删除子网。
- 在添加回之前删除的子网时，将创建一个具有不同 ID 的新网络接口。
- 同一可用区内的子网变更必须作为独立操作执行。您需先完成现有子网的删除，随后方可添加新的子网。
- 删除子网可能最多需要 3 分钟。

创建面向互联网的网络负载均衡器时，您可以选择为每个可用区指定弹性 IP 地址。弹性 IP 地址将为您的网络负载均衡器提供静态 IP 地址。如果您选择不指定弹性 IP 地址，则 AWS 将为每个可用区分配一个弹性 IP 地址。

创建内部网络负载均衡器时，您可以选择从每个子网指定一个私有 IP 地址。私有 IP 地址将为您的网络负载均衡器提供静态 IP 地址。如果您选择不指定私有 IP 地址，则会为您 AWS 分配一个。

在更新网络负载均衡器的可用区域之前，我们建议您评估对现有连接、流量或生产工作负载的任何潜在影响。

⚠ 更新可用区可能会造成中断

- 删除子网后，其关联的弹性网络接口（ENI）也会被删除。这会导致可用区中的所有活跃连接终止。
- 删除子网后，与其关联的可用区内的所有目标都将被标记为 unused。这会导致这些目标从可用目标池中删除，并且与这些目标的所有连接都将终止。这包括在使用跨可用区负载均衡时，源自其他可用区的任何连接。
- 网络负载均衡器的完全限定域名（FQDN）有 60 秒的生存时间（TTL）。删除包含活跃目标的可用区后，任何现有的客户端连接都可能出现超时，直到 DNS 再次解析，并且流量会转移到任何剩余的可用区中。

Console

要修改可用区

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器。
4. 在网络映射选项卡上，选择编辑子网。
5. 要启用可用区，请选中其复选框并选择一个子网。如果只有一个可用区，则会选择此子网。
6. 要更改已启用的可用区的子网，请从列表中选择其他子网之一。
7. 要禁用可用区，请清除其复选框。
8. 选择保存更改。

AWS CLI

要修改可用区

使用 set-subnets 命令。

```
aws elbv2 set-subnets \
    --load-balancer-arn load-balancer-arn \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890
```

CloudFormation

要修改可用区

更新AWS::ElasticLoadBalancingV2::LoadBalancer资源。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref new-subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

更新网络负载均衡器的 IP 地址类型

您可以配置您的网络负载均衡器，以便客户端可以仅使用地址或同时使用 IPv4 IPv6 地址 IPv4 和地址（双堆栈）与网络负载均衡器通信。网络负载均衡器根据目标组的 IP 地址类型与目标进行通信。有关更多信息，请参阅 IP 地址类型。

dualstack 要求

- 您可以在创建网络负载均衡器时设置 IP 地址类型并随时更新它。
- 您为 Network Load Balancer 指定的虚拟私有云 (VPC) 和子网必须具有关联的 IPv6 CIDR 块。有关更多信息，请参阅 Amazon EC2 用户指南中的IPv6地址。
- Network Load Balancer 子网的路由表必须路由 IPv6 流量。
- Network L ACLs oad Balancer 子网的网络必须允许 IPv6 流量。
- 网络负载均衡器上未连接任何 QUIC 或 TCP_QUIC 侦听器。

Console

要更新 IP 地址类型

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择负载均衡器。
3. 选中网络负载均衡器对应的复选框。
4. 选择操作和编辑 IP 地址类型。
5. 对于 IP 地址类型，请选择IPv4仅支持 IPv4 地址，或者选择 Dualstack 以同时支持 IPv4 和 IPv6 地址。
6. 选择保存更改。

AWS CLI

要更新 IP 地址类型

使用 set-ip-address-type 命令。

```
aws elbv2 set-ip-address-type \
    --load-balancer-arn load-balancer-arn \
    --ip-address-type dualstack
```

CloudFormation

要更新 IP 地址类型

更新AWS::ElasticLoadBalancingV2::LoadBalancer资源。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      IpAddressType: dualstack
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
```

```
        - !Ref mySecurityGroup
```

编辑网络负载均衡器的属性

创建网络负载均衡器之后，您可以编辑其属性。

负载均衡器属性

- 删除保护
- 跨可用区负载均衡
- 可用区 DNS 亲和性
- 辅助 IP 地址

删除保护

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

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

Console

要启用或禁用删除保护

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择负载均衡器。
3. 选择网络负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 在保护部分，启用或禁用删除保护。
6. 选择保存更改。

AWS CLI

要启用或禁用删除保护

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

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=deletion_protection.enabled,Value=true"
```

CloudFormation

要启用或禁用删除保护

更新AWS::ElasticLoadBalancingV2::LoadBalancer资源以包含该deletion_protection.enabled属性。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "deletion_protection.enabled"
          Value: "true"
```

跨可用区负载均衡

对于网络负载均衡器，负载均衡器级别的跨区域负载均衡默认为关闭，但您可以随时启动它。对于目标组，默认设置是使用负载均衡器设置，但您可以通过在目标组级别明确启动或关闭跨区域负载均衡来覆盖默认设置。有关更多信息，请参阅 the section called “跨可用区负载均衡”。

Console

要启用或禁用负载均衡器的跨区域负载均衡

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中的 Load Balancing (负载平衡) 下，选择 Load Balancers (负载均衡器)。
3. 选择负载均衡器的名称以打开其详细信息页面。

4. 在属性选项卡上，选择编辑。
5. 在 Edit load balancer attributes（编辑负载均衡器属性）页面上，开启或关闭 Cross-zone load balancing（跨区域负载均衡）。
6. 选择保存更改。

AWS CLI

要启用或禁用负载均衡器的跨区域负载均衡

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

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

要启用或禁用负载均衡器的跨区域负载均衡

更新AWS::ElasticLoadBalancingV2::LoadBalancer 资源以包含该`load_balancing.cross_zone.enabled`属性。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "load_balancing.cross_zone.enabled"
          Value: "true"
```

可用区 DNS 亲和性

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

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

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

- 可用区亲和性 – 100% 可用区亲和性

  客户端 DNS 查询将优先使用自身可用区中的网络负载均衡器 IP 地址。如果自身可用区中没有运行状况良好的网络负载均衡器 IP 地址，则查询可能会解析到其他可用区。
- 部分可用区亲和性 – 85% 可用区亲和性

  85% 的客户端 DNS 查询会优先选择自身可用区中的网络负载均衡器 IP 地址，剩余的查询会解析到任何运行状况良好的可用区。如果自身可用区中没有运行正常的 IP 地址，则查询可能会解析到其他运行正常的可用区。如果所有可用区中都没有运行正常的 IP 地址，则查询会解析到任何可用区。
- 任意可用区（默认值）– 0% 可用区亲和性

  客户端 DNS 查询将在所有网络负载均衡器可用区中运行状况良好的网络负载均衡器 IP 地址中进行解析。

可用区亲和性有助于将请求从客户端路由到网络负载均衡器，而跨可用区负载均衡有助于将请求从网络负载均衡器路由到目标。使用可用区亲和性时，应关闭跨可用区负载均衡，这可确保从客户端到目标的网络负载均衡器流量保持在同一可用区内。使用此配置，客户端流量将发送到网络负载均衡器可用区，因此建议将您的应用程序配置为在每个可用区中独立扩展。当每个可用区的客户端数量或每个可用区的流量不同时，这是一个重要的考虑因素。有关更多信息，请参阅 目标组的跨区域负载均衡。

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

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

在使用可用区亲和性之前，应注意以下几点：

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

监控

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

我们建议跟踪以下指标：

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

有关更多信息，请参阅 CloudWatch 您的 Network Load Balancer 的指标。

启用可用区亲和性

Console

要启用可用区亲和性

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

AWS CLI

要启用可用区亲和性

使用带 `dns_record.client_routing_policy` 属性的 modify-load-balancer-attributes 命令。

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes
 "Key=dns_record.client_routing_policy,Value=partial_availability_zone_affinity"
```

CloudFormation

要启用可用区亲和性

更新AWS::ElasticLoadBalancingV2::LoadBalancer资源以包含该`dns_record.client_routing_policy`属性。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
```

```
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "dns_record.client_routing_policy"
          Value: "partial_availability_zone_affinity"
```

辅助 IP 地址

如果您遇到端口分配错误，并且无法向目标组添加目标来解决这些错误，则可以向负载平衡器网络接口添加辅助 IP 地址。对于启用了负载均衡器的每个区域，我们从负载均衡器子网中选择 IPv4地址并将其分配给相应的网络接口。这些辅助 IP 地址用于与目标建立连接。它们还用于运行状况检查流量。我们建议您先添加一个辅助 IP 地址，监控 `PortAllocationErrors` 指标，并仅在端口分配错误未解决时再添加另一个辅助 IP 地址。

> **Warning**
>
> 添加辅助 IP 地址后，您无法将其删除。释放辅助 IP 地址的唯一方法是删除负载均衡器。在添加辅助 IP 地址之前，请验证负载均衡器子网中是否有足够的可用 IPv4地址。

Console

要添加辅助 IP 地址

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择负载均衡器。
3. 选择网络负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 展开特殊情况属性，解锁按子网自动分配辅助 IP 地址属性，并选择辅助 IP 地址的数量。
6. 选择保存更改。

AWS CLI

要添加辅助 IP 地址

使用带 secondary_ips.auto_assigned.per_subnet 属性的 modify-load-balancer-attributes 命令。

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=secondary_ips.auto_assigned.per_subnet,Value=1"
```

您可以使用describe-network-interfaces命令获取负载均衡器网络接口 IPv4的地址。--filters 参数将结果范围限定为网络负载均衡器的网络接口，而 --query 参数进一步将结果范围限定为指定名称的负载均衡器，并仅显示指定字段。您可以包括所需的其他字段。

```
aws elbv2 describe-network-interfaces \
    --filters "Name=interface-type,Values=network_load_balancer" \
    --query "NetworkInterfaces[?contains(Description,'my-nlb')].
{ID:NetworkInterfaceId,AZ:AvailabilityZone,Addresses:PrivateIpAddresses[*]}"
```

CloudFormation

要添加辅助 IP 地址

更新AWS::ElasticLoadBalancingV2::LoadBalancer资源以包含该secondary_ips.auto_assigned.per_subnet属性。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "secondary_ips.auto_assigned.per_subnet"
          Value: "1"
```

更新网络负载均衡器的安全组

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

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

您无需为入站安全组规则阻止的流量付费。

内容

注意事项

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

示例：筛选客户端流量

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

入站

协议	来源	端口范围	Comment
protocol	*client IP address range*	*listener port*	在侦听器端口上允许来自源 CIDR 的入站流量
ICMP	0.0.0.0/0	全部	允许入站 ICMP 流量，以支持 MTU 或路径 MTU 发现 †

† 有关更多信息，请参阅《亚马逊 EC2 用户指南》中的 Path MTU 发现。

出站

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

示例：仅接受来自网络负载均衡器的流量

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

入站

协议	来源	端口范围	Comment
protocol	sg-111112222233333	*target port*	在目标端口上允许来自网络负载均衡器的入站流量

协议	来源	端口范围	Comment
protocol	sg-111112 222233333	*health check*	在运行状况检查端口上允许来自网络负载均衡器的入站流量

出站

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

更新关联的安全组

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

Console

要更新安全组

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的 Load Balancing（负载均衡）下，选择 Load Balancers（负载均衡器）。
3. 选择网络负载均衡器。
4. 在安全性选项卡上，选择编辑。
5. 要将一个安全组与网络负载均衡器关联，请选择此安全组。要从网络负载均衡器中移除一个安全组，请清除该安全组。
6. 选择保存更改。

AWS CLI

要更新安全组

使用 set-security-groups 命令。

```
aws elbv2 set-security-groups \
    --load-balancer-arn load-balancer-arn \
```

```
    --security-groups sg-1234567890abcdef0 sg-0abcdef0123456789
```

CloudFormation

要更新安全组

更新AWS::ElasticLoadBalancingV2::LoadBalancer资源。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
        - !Ref myNewSecurityGroup
```

更新安全设置

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

Console

要更新安全设置

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

AWS CLI

要更新安全设置

使用 set-security-groups 命令。

```
aws elbv2 set-security-groups \
    --load-balancer-arn load-balancer-arn \
    --enforce-security-group-inbound-rules-on-private-link-traffic off
```

CloudFormation

要更新安全设置

更新AWS::ElasticLoadBalancingV2::LoadBalancer资源。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      EnforceSecurityGroupInboundRulesOnPrivateLinkTraffic: off
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

监控网络负载均衡器安全组

使用`SecurityGroupBlockedFlowCount_Inbound`和`SecurityGroupBlockedFlowCount_Outbound` CloudWatch 指标来监控 Network Load Balancer 安全组阻止的流量数量。被阻止的流量未反映在其他指标中。有关更多信息，请参阅 the section called “CloudWatch 指标”。

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

标记网络负载均衡器

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

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

当您用完标签时，可以从网络负载均衡器中将其移除。

限制

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

Console

要更新负载均衡器的标签

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择负载均衡器。
3. 选中网络负载均衡器对应的复选框。
4. 在标签选项卡上，选择管理标签。
5. 要添加标签，请选择添加标签，然后输入标签键和值。允许的字符包括字母、空格、数字（UTF-8 格式）和以下特殊字符：+ - = 。_ : / @。请不要使用前导空格或尾随空格。标签值区分大小写。
6. 要更新标签，请在键或值中输入新值。
7. 要删除标签，请选择标签旁边的删除。
8. 选择保存更改。

AWS CLI

添加 标签

使用 add-tags 命令。以下示例将添加两个标签。

```
aws elbv2 add-tags \
    --resource-arns load-balancer-arn \
    --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

删除标签

使用 remove-tags 命令。以下示例将移除具有指定键的标签。

```
aws elbv2 remove-tags \
    --resource-arns load-balancer-arn \
    --tag-keys project department
```

CloudFormation

添加 标签

定义 resource 类型的AWS::ElasticLoadBalancingV2::LoadBalancer资源以包含该Tags属性。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

删除网络负载均衡器

在您的网络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。当您不再需要该网络负载均衡器时，可将其删除。当网络负载均衡器被删除之后，您便不再需要支付网络负载均衡器费用。

如果已启用删除保护，则无法删除网络负载均衡器。有关更多信息，请参阅 删除保护。

如果其他服务正在使用网络负载均衡器，则无法删除该网络负载均衡器。例如，如果网络负载均衡器与 VPC 端点服务关联，则必须先删除端点服务配置，然后才能删除关联的网络负载均衡器。

删除网络负载均衡器也将删除其侦听器。删除网络负载均衡器不会影响其注册目标。例如，您的 EC2 实例会继续运行，并且仍会注册到其目标组。要删除目标组，请参阅删除网络负载均衡器的目标组。

Console

要删除网络负载均衡器

1. 如果您有一个指向网络负载均衡器的域的一个 DNS 记录，请将它指向新的位置并等待 DNS 更改生效，然后再删除您的网络负载均衡器。例如：
   - 如果此记录是存活时间（TTL）为 300 秒的 CNAME 记录，请至少等待 300 秒，然后再继续执行下一步。
   - 如果此记录是 Route 53 别名（A）记录，请至少等待 60 秒。
   - 如果使用 Route 53，则记录更改需要 60 秒才能传播到所有全局 Route 53 名称服务器。将此时间添加到正在更新的记录的 TTL 值。
2. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
3. 在导航窗格中，选择负载均衡器。
4. 选中网络负载均衡器对应的复选框。
5. 依次选择操作、删除负载均衡器。
6. 如果提示进行确认，输入 **`confirm`**，并选择删除。

AWS CLI

要删除网络负载均衡器

使用 delete-load-balancer 命令。

```
aws elbv2 delete-load-balancer \
    --load-balancer-arn load-balancer-arn
```

查看网络负载均衡器资源地图

网络负载均衡器资源地图以交互式显示您的网络负载均衡器架构，包括关联的侦听器、目标组和目标。资源地图还突出显示了所有资源之间的关系和路由路径，从而直观地呈现了您的网络负载均衡器配置。

要查看负载均衡器的资源地图

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择负载均衡器。
3. 选择网络负载均衡器。
4. 选择资源地图选项卡。

资源地图组件

地图视图

网络负载均衡器资源地图中有两个可用视图：概览和运行状况不佳的目标地图。默认情况下，概览处于选中状态，并显示您的网络负载均衡器的所有资源。选择运行状况不佳的目标地图视图将仅显示运行状况不佳的目标以及与之关联的资源。

不正常目标地图视图可用于对未通过运行状况检查的目标进行故障排除。有关更多信息，请参阅 使用资源地图对运行状况不佳的目标进行故障排除。

资源列

网络负载均衡器资源地图包含三个资源列，每种资源类型各一列。资源组包括侦听器、目标组和目标。

资源图块

列内的每个资源都有自己的图块，显示有关该特定资源的详细信息。

- 将鼠标悬停在资源图块上，以突出显示该资源与其他资源之间的关系。
- 选择资源图块，以突出显示该资源与其他资源之间的关系，并显示有关该资源的其他详细信息。
  - 目标组运行状况摘要：每种运行状况的注册目标数量。

- 目标运行状况：目标的当前运行状况和描述。

> **Note**
>
> 您可以关闭显示资源详细信息，以隐藏资源地图内的其他详细信息。

- 每个资源磁贴都包含一个链接，选中后，该链接将导航到该资源的详细信息页面。
  - 侦听器 - 选择侦听器 protocol:port。例如，`TCP:80`
  - 目标组 - 选择目标组名称。例如，`my-target-group`
  - 目标 - 选择目标 ID。例如，`i-1234567890abcdef0`

导出资源地图

选择导出后，您可以选择将网络负载均衡器资源地图的当前视图导出为 PDF。

CloudWatch 你的 Network Load Balancer 的日志

Amazon CloudWatch Logs 支持 Network Load Balancer 访问日志作为销售日志，从而提高了可观察性并简化了网络流量模式的调试。您可以直接分析 Network Load Balancer 访问日志，深入了解客户端连接、流量分布和连接状态，从而帮助您更快地识别和解决网络问题。 CloudWatch

您可以配置向支持 Apache Parquet 格式的亚马逊 CloudWatch 日志、亚马逊数据 Firehose 和亚马逊简单存储服务 (Amazon S3) 的传输网络负载均衡器访问日志。

> **Important**
>
> 仅当负载均衡器具有 TLS 侦听器且日志仅包含有关 TLS 请求的信息时，才创建访问日志。访问日志将尽力记录请求。我们建议您使用访问日志来了解请求性质，而不是作为所有请求的完整描述。

> **Important**
>
> 网络负载均衡器仍可使用传统的“旧式”访问日志。要管理“旧式”访问日志的配置，请访问您负载均衡器的属性选项卡。有关“旧式”访问日志的更多信息，请参阅 您的网络负载均衡器的访问日志。

通过此 CloudWatch 日志集成，您可以使用 CloudWatch Logs Insights 查询跟踪详细的访问模式，创建用于监控的指标筛选器，并使用 Live Tail 实时查看流量模式。

您可以从控制台中负载均衡器的 “集成” 选项卡中启用 CloudWatch Network Load Balancer 访问日志的日志。要启用日志记录，您必须以具有特定权限的用户身份登录。此外，您必须 AWS 向授予权限才能发送日志。

有关每个日志记录目标所需的权限，请参阅启用来自 AWS 服务的日志记录。

有关更多信息，请参阅什么是 Amazon CloudWatch 日志？ 。

有关定价信息，请参阅 Amazon CloudWatch 定价。

您的网络负载均衡器的可用区转移

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

当您启动可用区转移时，您的网络负载均衡器将停止将流量路由到受影响可用区中的目标。与受影响可用区中目标的现有连接不会因可用区转移而终止。这些连接可能需要数分钟才能正常完成。

内容

在开始可用区转移之前

- 默认情况下，可用区转移处于禁用状态，并且必须在每个网络负载均衡器上启用。有关更多信息，请参阅 为网络负载均衡器启用可用区转移。
- 只能为单个可用区中的特定网络负载均衡器启动可用区转移。无法为多个可用区启动可用区转移。

- AWS 当多个基础架构问题影响服务时，会主动从 DNS 中删除区域 Network Load Balancer IP 地址。在开始可用区转移之前，请务必检查当前的可用区容量。如果您在网络负载均衡器上使用可用区转移，则受可用区转移影响的可用区也会失去目标容量。
- 在启用跨区域负载均衡的网络负载均衡器上进行可用区转移期间，将从 DNS 中移除可用区负载均衡器 IP 地址。与受损可用区中目标的现有连接会一直持续，直到它们自然关闭，而新的连接将不再路由到受损可用区中的目标。

有关更多信息，请参阅《Amazon Application Recovery Controller（ARC）开发人员指南》中的 ARC 的可用区转移最佳实践。

可用区转移管理覆盖

属于网络负载均衡器的目标将包括一个独立于 `TargetHealth` 状态的新状态 `AdministrativeOverride`。

当网络负载均衡器启动可用区转移时，被转移区域内的所有目标都将视为被管理覆盖。网络负载均衡器将停止向被管理覆盖的目标路由新流量。现有连接将保持不变，直至其自然终止。

可能的 `AdministrativeOverride` 状态包括：

unknown

由于内部错误，无法传播状态

no_override

目标上当前没有活动的覆盖

zonal_shift_active

可用区转移在目标可用区处于活动状态

zonal_shift_delegated_to_dns

此目标的区域偏移状态不可通过获得，`DescribeTargetHealth`但可以直接通过 AWS ARC - Zonal Shift API 或控制台查看。

为网络负载均衡器启用可用区转移

默认情况下，可用区转移处于禁用状态，并且必须在每个网络负载均衡器上启用。这确保了您仅能使用所需的特定网络负载均衡器来启动可用区转移。有关更多信息，请参阅 the section called “可用区转移”。

先决条件

如果您为负载均衡器启用了跨区域负载均衡，则连接到该负载均衡器的每个目标组都必须满足以下要求。

- 目标组协议必须为 TCP 或 TLS。
- 目标组类型不能为 alb。
- 必须禁用对运行状况不佳的目标终止连接功能。
- load_balancing.cross_zone.enabled 目标组属性必须为 true 或 use_load_balancer_configuration（默认）。

Console

要启用可用区转移

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的 Load Balancing（负载均衡）下，选择 Load Balancers（负载均衡器）。
3. 选择网络负载均衡器。
4. 在属性选项卡上，选择编辑。
5. 在可用区路由配置部分，对于 ARC 可用区转移集成，请选择 启用。
6. 选择保存更改。

AWS CLI

要启用可用区转移

使用带 zonal_shift.config.enabled 属性的 modify-load-balancer-attributes 命令。

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=zonal_shift.config.enabled,Value=true"
```

CloudFormation

要启用可用区转移

更新AWS::ElasticLoadBalancingV2::LoadBalancer资源以包含该zonal_shift.config.enabled属性。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        -Key: "zonal_shift.config.enabled"
         Value: "true"
```

为网络负载均衡器启动可用区转移

ARC 中的区域切换允许您暂时将受支持资源的流量从可用区移开，这样您的应用程序就可以继续在某个 AWS 区域中的其他可用区正常运行。

先决条件

在开始之前，请确认您已为负载均衡器负载均衡器启用可用区转移。

Console

此过程说明了如何使用 Amazon EC2 控制台开始区域移动。有关使用 ARC 控制台启动可用区转移的步骤，请参阅《Amazon 应用程序恢复控制器（ARC）开发人员指南》中的 Starting a zonal shift。

启动可用区转移

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的 Load Balancing（负载均衡）下，选择 Load Balancers（负载均衡器）。
3. 选择网络负载均衡器。
4. 在集成选项卡中，展开 Amazon Application Recovery Controller（ARC），然后选择启动可用区转移。
5. 选择要将流量移离的可用区。

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

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

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

AWS CLI

启动可用区转移

使用 Amazon 应用程序恢复控制器 (ARC) start-zonal-shift命令。

```
aws arc-zonal-shift start-zonal-shift \
    --resource-identifier load-balancer-arn \
    --away-from use2-az2 \
    --expires-in 2h \
    --comment "zonal shift due to scheduled maintenance"
```

更新网络负载均衡器的可用区转移

您可以更新可用区转移，以设置新的到期时间，也可以编辑或替换可用区转移的注释。

Console

此过程说明如何使用 Amazon EC2 控制台更新区域偏移。有关使用 Amazon 应用程序恢复控制器（ARC）控制台更新可用区转移的步骤，请参阅《Amazon 应用程序恢复控制器（ARC）开发人员指南》中的 Updating a zonal shift。

更新可用区转移

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的 Load Balancing（负载均衡）下，选择 Load Balancers（负载均衡器）。
3. 选择具有活跃可用区转移的应用程序负载均衡器。
4. 在集成选项卡中，展开 Amazon Application Recovery Controller（ARC），然后选择更新可用区转移。

此操作将打开 ARC 控制台以继续更新流程。

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

AWS CLI

更新可用区转移

使用 Amazon 应用程序恢复控制器 (ARC) update-zonal-shift命令。

```
aws arc-zonal-shift update-zonal-shift \
    --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE \
    --expires-in 1h \
    --comment "extending zonal shift for scheduled maintenance"
```

取消网络负载均衡器的可用区转移

在可用区转移到期之前，您可以随时取消它。你可以取消你启动的区域移动，也可以取消为区域自动移位练习跑而 AWS 开始的区域移动。

Console

此过程说明了如何使用 Amazon EC2 控制台取消区域偏移。有关使用 Amazon 应用程序恢复控制器（ARC）控制台取消可用区转移的步骤，请参阅《Amazon 应用程序恢复控制器（ARC）开发人员指南》中的 Canceling a zonal shift。

取消可用区转移

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的 Load Balancing（负载均衡）下，选择 Load Balancers（负载均衡器）。
3. 选择具有活跃可用区转移的网络负载均衡器。
4. 在集成选项卡中的 Amazon Application Recovery Controller（ARC） 部分，选择取消可用区转移。

   此操作将打开 ARC 控制台以继续取消流程。
5. 选择 Cancel zonal shift（取消可用区转移）。

6. 当系统提示进行确认时，选择 Confirm。

AWS CLI

取消可用区转移

使用 Amazon 应用程序恢复控制器 (ARC) cancel-zonal-shift命令。

```
aws arc-zonal-shift cancel-zonal-shift \
    --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE
```

您网络负载均衡器的容量预留

负载均衡器容量单位 (LCU) 预留让您可以为负载均衡器预留静态最小容量。网络负载均衡器会自动扩展，以支持检测到的工作负载并满足容量需求。配置最小容量后，您的负载均衡器会根据接收到的流量继续纵向或横向扩展，但也可以防止容量低于配置的最小容量。

在以下情况下，可以考虑使用 LCU 预留：

- 您即将举办的活动将出现突发性异常高流量，需要确您的保负载均衡器能够在活动期间支撑突发的流量峰值。
- 您的工作负载特性导致短期内存在不可预测的流量峰值。
- 您正在配置负载均衡器，以便在特定启动时间接入或迁移服务，且需要从高容量开始运行，而非等待自动扩缩生效。
- 您正在负载均衡器之间迁移工作负载，并希望将目标配置调整为与源负载均衡器的规模相匹配。

估算您需要的容量

在确定为负载均衡器预留的容量时，我们建议您进行负载测试或分析代表预期未来流量的历史工作负载数据。使用弹性负载均衡控制台，您可以根据审核的流量估算需要预留的容量大小票。

或者，您可以参考 CloudWatch 指标ProcessedBytes来确定正确的容量级别。您的负载均衡器的容量已预留在中 LCUs，每个 LCU 等于 2.2Mbps。您可以使用 Max (ProcessedBytes) 指标来查看负载均衡器上每分钟的最大吞吐量流量，然后将该吞吐量转换为 LCUs 使用 2.2Mbps 等于 1 LCU 的转换率。

如果您没有历史工作负载数据可供参考，也无法执行负载测试，则可以使用 LCU 预留计算器来估算所需容量。LCU 预留计算器使用基于 AWS 观察到的历史工作负载的数据，可能无法代表您的特定工作负载。有关更多信息，请参阅负载均衡器容量单位预留计算器。

支持的区域：

此功能仅在以下区域可用：

- 美国东部（弗吉尼亚州北部）
- 美国东部（俄亥俄州）
- 美国西部（俄勒冈州）
- 亚太地区（香港）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太地区（东京）
- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）
- 欧洲地区（斯德哥尔摩）

LCU 预留的最小值和最大值

每个可用区的总预留请求必须至少为 2,750 LCU。最大值由您账户的配额决定。有关更多信息，请参阅 the section called “负载均衡器容量单位”。

为您的网络负载均衡器请求负载均衡器容量单位预留

在使用 LCU 预留之前，请先查看以下信息：

- 使用 TLS 侦听器的网络负载均衡器不支持 LCU 预留。
- LCU 预留仅支持为网络负载均衡器预留吞吐能力。申请 LCU 预留时，请将您的容量需求从 Mbps 转换为 LCUs 使用 1 LCU 到 2.2 Mbps 的转换速率。
- 容量是在区域层面预留的，并将在可用区之间平均分配。在启用 LCU 预留之前，请确认每个可用区中都有足够的均匀分布目标。
- LCU 预留请求遵循“先到先得”原则，具体取决于该可用区当时的可用容量。多数请求通常在一小时内完成，但也有可能需要数小时。
- 更新现有预留时，需待先前的请求完成配置或失败。您可以按需多次增加预留容量，但每日仅限两次“减少”操作。
- 所有预留或已配置容量在终止或取消前将持续计费。

Console

要请求 LCU 预留

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器名称。
4. 在容量选项卡中，选择编辑 LCU 预留。
5. 选择基于历史参考的估算。
6. 选择参考时段，以查看推荐的预留 LCU 级别。
7. 如果您没有历史参考工作量，则可以选择手动估算并输入 LCUs 要保留的数量。
8. 选择保存。

AWS CLI

要请求 LCU 预留

使用 modify-capacity-reservation 命令。

```
aws elbv2 modify-capacity-reservation \
    --load-balancer-arn load-balancer-arn \
    --minimum-load-balancer-capacity CapacityUnits=3000
```

CloudFormation

要请求 LCU 预留

更新AWS::ElasticLoadBalancingV2::LoadBalancer资源。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-alb
      Type: application
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
```

```
      SecurityGroups:
        - !Ref mySecurityGroup
      MinimumLoadBalancerCapacity:
        CapacityUnits: 3000
```

更新或取消您网络负载均衡器的负载均衡器容量单位预留

如果您负载均衡器的流量模式发生变化，您可以更新或取消您负载均衡器的 LCU 预留。

Console

要更新或取消 LCU 预留

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器名称。
4. 在容量选项卡中，执行以下操作之一：
   a. 要更新 LCU 预留，请选择编辑 LCU 预留。
   b. 要取消 LCU 预留，请选择取消容量。

AWS CLI

要取消 LCU 预订

使用 modify-capacity-reservation 命令。

```
aws elbv2 modify-capacity-reservation \
    --load-balancer-arn load-balancer-arn \
    --reset-capacity-reservation
```

监控您网络负载均衡器的负载均衡器容量单位预留

预留状态

以下是 LCU 预留的可能状态值：

- pending - 表示该预留正在配置中。

- `provisioned` - 表示预留容量已准备就绪，可供使用。
- `failed` - 表示当前无法完成请求。
- `rebalancing` - 表示可用区已添加或删除，负载均衡器正在重新分配容量。

LCU 使用率

要确定预留 LCU 的使用率，您可以将每分钟的 `ProcessedBytes` 指标与每小时的 `Sum(ReservedLCUs)` 进行比较。要将每分钟字节数转换为每小时 LCU，请使用公式：（字节/分钟）*8/60/ (10^6)/2.2。

Console

要查看 LCU 预留的状态

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器名称。
4. 在容量选项卡中，您可以查看预留状态和预留 LCU 值。

AWS CLI

要监控 LCU 预留的状态

使用 describe-capacity-reservation 命令。

```
aws elbv2 describe-capacity-reservation \
    --load-balancer-arn load-balancer-arn
```

网络负载均衡器的侦听器

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

内容

侦听器配置

侦听器支持以下协议和端口：

- 协议：TCP、TLS、UDP、TCP_UDP、QUIC、TCP_QUIC
- 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，您必须在侦听器上部署至少一个 SSL 服务器证书。有关更多信息，请参阅 服务器证书。

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

您可以使用 QUIC 侦听器来接受 QUIC 流量。网络负载均衡器作为符合 RFC9000 标准的直通式负载均衡器运行。利用 QUIC 侦听器和支持 QUIC 的后端，为移动设备实现无缝连接迁移。

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。

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

双栈负载均衡器的 UDP 侦听器需要有 IPv6 目标组。

WebSockets 只有 TCP、TLS、TCP_UDP 和 TCP_QUIC 侦听器支持。

QUIC 流量不支持版本协商。QUIC v1 是唯一受支持的 QUIC 版本。

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

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

默认操作

创建侦听器时，您需要指定路由请求的默认操作。默认操作将请求转发到您指定的目标组。

向多个目标组分配流量

如果您为默认操作指定多个目标组，那么请求将根据这些目标组的相对权重进行分配。您必须为每个目标组指定 0 至 999 之间的权重值。权重为 0 的目标组不会收到任何流量。在您添加目标组或更新目标组权重后，新连接将根据新的目标组权重进行路由。现有连接不受影响，将继续按常规方式运行直至关闭。

例如，如果指定两个目标组，每个目标组的权重为 10，则每个目标组将接收一半的请求。如果指定两个目标组，一个权重为 10，另一个权重为 20，则权重为 20 的目标组接收的请求数量是权重为 10 的目标组的两倍。

常见用例是从一个目标组向另一个目标组迁移流量。这意味着您需逐步增加新目标组的权重，同时降低原始目标组的权重，直至其变为 0。如果您将目标组的权重更新为 0，经过短暂时间后，该组将不再接收新的连接，且现有连接也将关闭。

粘性会话和加权目标组

在监听器上执行的转发操作可指定是否启用目标组粘性。启用后，目标组粘性会使来自相同源 IP 地址的后续连接优先选择先前选定的目标组。

注意事项

- 对于 TLS 侦听器，您无法将 TCP 目标组和 TLS 目标组同时添加到侦听器规则中。所有目标组必须使用相同的协议。
- 对于 TLS 侦听器，不支持目标组粘性。
- 对于双栈负载均衡器，您无法将 IPv4 目标组和 IPv6 目标组同时添加到同一个默认操作中。默认操作中的所有目标组必须使用相同的 IP 地址类型。
- 对于侦听器，如果转发操作包含多个目标组且其中任何一个启用了粘性策略，则该转发操作也必须启用目标组粘性策略。

侦听器属性

网络负载均衡器的侦听器属性如下：

`tcp.idle_timeout.seconds`

tcp 空闲超时值（以秒为单位）。有效范围为 60-6000 秒。默认值为 350 秒。

有关更多信息，请参阅 更新空闲超时。

安全侦听器

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

Elastic Load Balancing 使用 TLS 协商配置（称为安全策略）在客户端与负载均衡器之间协商 TLS 连接。安全策略是协议和密码的组合。协议在客户端与服务器之间建立安全连接，确保在客户端与负载均衡器之间传递的所有数据都是私密数据。密码是使用加密密钥创建编码消息的加密算法。协议使用多种密码对 Internet 上的数据进行加密。在 连接协商过程中，客户端和负载均衡器会按首选项顺序提供各自支持的密码和协议的列表。为安全连接选择服务器列表中与任一客户端的密码匹配的第一个密码。

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

网络负载均衡器支持使用 PSK 进行 TLS 1.3 的 TLS 恢复，以及使用会话票证进行 TLS 1.2 及更早版本的 TLS 恢复。不支持基于会话 ID 的恢复，也不支持在侦听器中配置多个证书并使用 SNI 时的恢复。未实现 0-RTT 数据功能和 early_data 扩展。

有关相关演示，请参阅网络负载均衡器上的 TLS 支持和网络负载均衡器上的 SNI 支持。

ALPN 策略

Application-Layer 协议协商 (ALPN) 是一种 TLS 扩展，在最初的 TLS 握手问候消息上发送。ALPN 使应用层能够通过安全连接（例如 HTTP/1和 HTTP/2）协商应使用哪些协议。

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

支持的 ALPN 策略

以下是支持的 ALPN 策略：

`HTTP1Only`

仅限谈判 HTTP/1。*. ALPN 首选项列表为 http/1 .1、 http/1 .0。

`HTTP2Only`

仅限谈判 HTTP/2。ALPN 首选项列表为 h2。

`HTTP2Optional`

优先使用 HTTP/1 .* HTTP/2 （这可能对 HTTP/2 测试很有用）。ALPN 首选项列表为 http/1 .1、http/1 .0、h2。

`HTTP2Preferred`

HTTP/2 优先于 HTTP/1 .*. ALPN 首选项列表为 h2、 http/1 .1、 http/1 .0。

`None`

不协商 PN。这是默认模式。

启用 ALPN 连接

您可以在创建或修改 TLS 侦听器时启用 ALPN 连接。有关更多信息，请参阅添加侦听器和更新 ALPN 策略。

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

- 您必须为默认操作指定目标组。有关更多信息，请参阅 为网络负载均衡器创建目标组。
- 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 网络负载均衡器的服务器证书。
- 您无法在 dualstack 负载均衡器上将 IPv4 目标组与 UDP 侦听器结合使用。
- QUIC 和 TCP_QUIC 侦听器不支持在 dualstack 负载均衡器或关联安全组的负载均衡器上使用。
- QUIC 和 TCP_QUIC 侦听器不支持在关联安全组的负载均衡器上使用。
- 在任何给定时间，网络负载均衡器上仅允许存在一个 QUIC 或 TCP_QUIC 侦听器。
- 在具有 UDP 或 TCP_UDP 侦听器的网络负载均衡器上，不允许配置 QUIC 和 TCP_QUIC 侦听器。

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。

Console

添加侦听器

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在 Listeners（侦听器）选项卡上，选择 Add listener（添加侦听器）。
5. 对于协议，请选择 TCP、UDP、TCP_UDP、TLS、QUIC 或 TCP_QUIC。保留默认端口或键入其他端口。
6. 对于默认操作，选择一个要将流量转发到的目标组。

要添加其他目标组，请选择添加目标组，并根据需要更新权重。

如果您还没有能满足您需求的目标组，请选择创建目标组，以立即创建一个目标组。有关更多信息，请参阅 创建目标组。

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] 对于默认 SSL/TLS 服务器证书，请选择默认证书。您可从以下任一来源选择证书：

   - 如果您使用创建或导入了证书 AWS Certificate Manager，请选择从 ACM，然后从证书（来自 ACM）中选择证书。
   - 如果您使用 IAM 导入了证书，请选择来自 ACM，然后从证书（来自 ACM）中选择该证书。
   - 如果您有证书，请选择导入证书。选择导入到 ACM 或者导入到 IAM。对于证书私钥，请复制并粘贴私钥文件 (PEM-encoded) 的内容。对于证书正文，复制并粘贴公钥证书文件的内容 (PEM-encoded)。对于证书链，请复制并粘贴证书链文件 (PEM-encoded) 的内容，除非您使用的是自签名证书，并且浏览器是否隐式接受该证书并不重要。
9. [TLS 侦听器] 对于 ALPN policy (ALPN 策略)，请选择一个策略以启用 ALPN，或选择 None (无) 以禁用 ALPN。有关更多信息，请参阅 ALPN 策略。
10. （可选）要添加标签，请展开侦听器标签。选择添加新标签，然后输入标签键和标签值。
11. 选择添加。
12. [TLS 侦听器] 要向可选证书列表添加证书，请参阅将证书添加到证书列表。

AWS CLI

创建目标组

如果您没有可以用于默认操作的目标组，请立即使用 create-target-group 命令来创建一个目标组。有关示例，请参阅 创建目标组。

添加 TCP 侦听器

使用 create-listener 命令，指定 TCP 协议。

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

要添加具有多个目标组的 TCP 侦听器

使用 create-listener 命令，指定 TCP 协议、目标组和权重。

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TCP \
    --port 80 \
    --default-actions '[{
        "Type":"forward",
        "ForwardConfig":{
            "TargetGroups":[
                {"TargetGroupArn":"target-group-1-arn","Weight":10},
                {"TargetGroupArn":"target-group-2-arn","Weight":30}
            ]
        }
    }]'
```

要添加 TLS 侦听器

使用 create-listener 命令，指定 TLS 协议。

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TLS \
    --port 443 \
    --certificates CertificateArn=certificate-arn \
    --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

要添加 UDP 侦听器

使用 create-listener 命令，指定 UDP 协议。

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol UDP \
    --port 53 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

要添加 QUIC 侦听器

使用 create-listener 命令，指定 QUIC 协议。

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol QUIC \
    --port 443 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

CloudFormation

要添加 TCP 侦听器

使用 TCP 协议定义 AWS::ElasticLoadBalancingV2:: Listener 类型的资源。

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

要添加具有多个目标组的 TCP 侦听器

使用 TCP 协议定义 AWS::ElasticLoadBalancingV2:: Listener 类型的资源。

```
Resources:
    myTCPListener:
        Type: 'AWS::ElasticLoadBalancingV2::Listener'
        Properties:
        LoadBalancerArn: !Ref myLoadBalancer
        Protocol: TCP
        Port: 80
        DefaultActions:
            - Type: forward
            ForwardConfig:
                TargetGroups:
                - TargetGroupArn: !Ref myTargetGroup1,
                    Weight: 10
                - TargetGroupArn: !Ref myTargetGroup2,
                    Weight: 30
            TargetGroupStickinessConfig:
```

```
                Enabled: true
```

要添加 TLS 侦听器

使用 TLS 协议定义 AWS::ElasticLoadBalancingV2:: Listener 类型的资源。

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"
      Certificates:
        - CertificateArn: "certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

要添加 UDP 侦听器

使用 UDP 协议定义 AWS::ElasticLoadBalancingV2:: Listener 类型的资源。

```
Resources:
  myUDPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: UDP
      Port: 53
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

要添加 QUIC 侦听器

使用 QUIC 协议定义 AWS::ElasticLoadBalancingV2:: Listener 类型的资源。

```
Resources:
  myQUICListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
```

```
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: QUIC
      Port: 443
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

网络负载均衡器的服务器证书

在为网络负载均衡器创建安全侦听器时，您必须在负载均衡器上部署至少一个证书。负载均衡器需要 X.509 证书（服务器证书）。证书是由证书颁发机构 (CA) 颁发的数字化身份。证书包含标识信息、有效期限、公有密钥、序列号以及发布者的数字签名。

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

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

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

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

支持的密钥算法

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

- ECDSA 384 位
- ECDSA 521 位

重要-使用 IAM-imported 证书时的行为

如果您将证书导入 AWS 身份与访问管理 (IAM) 和 Access Management 并将其附加到 NLB TLS 侦听器，则在附加时不会验证证书密钥大小和算法。证书与侦听器关联后，将异步进行验证。如果证书使用不支持的密钥大小（例如 RSA 4096 位），则侦听器将进入非功能状态，您将通过 Person AWS al Health Dashboard (PHD) 收到通知。

请注意，如果您的监听器配置了以前有效的证书，则在不支持的证书被拒绝时，该证书可能会继续为流量提供服务。PHD 通知将表明监听器配置了不支持的证书，但不会确认流量是否仍由以前的证书提供服务。

为避免这种情况，请在将证书导入 IAM 之前验证其密钥大小。对于 RSA 证书，NLB TLS 侦听器支持的最大密钥大小为 3072 位。

如果您使用 AWS Certifice Manager (ACM) 来配置或导入证书，则在附加时会拒绝不支持的密钥大小，从而立即提供反馈。

默认证书

创建 TLS 监听器时，您必须至少指定一个证书。此证书称为默认证书。创建 TLS 侦听器后，您可以替换默认证书。有关更多信息，请参阅 替换默认证书。

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

如果您未指定其他证书但需要通过单一负载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。

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。

证书续订

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

您可以按如下方式管理证书续订和替换：

- 由您的负载均衡器提供 AWS Certificate Manager 并部署在您的负载均衡器上的证书可以自动续订。ACM 会尝试在到期之前续订证书。有关更多信息，请参阅 AWS Certificate Manager 用户指南中的托管续订。
- 如果您将证书导入 ACM，则必须监视证书的到期日期并在到期前续订。有关更多信息，请参阅 AWS Certificate Manager 用户指南中的导入证书。
- 如果您已将证书导入 IAM 中，则必须创建一个新证书，将该新证书导入 ACM 或 IAM 中，将该新证书添加到负载均衡器，并从负载均衡器删除过期的证书。

网络负载均衡器的安全策略

创建 TLS 侦听器时，您必须选择一个安全策略。安全策略确定了在负载均衡器与客户端之间进行 SSL 协商期间支持的密码和协议。如果您的要求更改或者当我们发布新的安全策略时，您可以更新负载均衡器的安全策略。有关更多信息，请参阅 更新安全策略。

注意事项

- TLS 侦听器需要有安全策略。如果您在创建侦听器时未指定安全策略，我们将使用默认安全策略。默认安全策略取决于您创建 TLS 侦听器的方式：
  - 控制台 – 默认安全策略为 `ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09`。

  - 其他方法（例如 AWS CLI AWS CloudFormation、和 AWS CDK）-默认安全策略是ELBSecurityPolicy-2016-08。
- 以 PQ 命名的安全策略提供混合后量子密钥交换。出于兼容性考虑，它们支持经典和后量子 ML-KEM 密钥交换算法。客户端必须支持 ML-KEM 密钥交换，才能使用混合后量子 TLS 进行密钥交换。混合后量子策略支持 secp256r1mlkem768、secp384r1mlkem1024 和 X25519MLKEM768 算法。有关更多信息，请参阅Post-quantum 密码学。
- AWS 建议实施新的基于后量子 TLS (PQ-TLS) 的安全策略ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09或ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09。该策略通过支持能够协商混合 PQ-TLS、仅限 TLS 1.3 或仅限 TLS 1.2 的客户端，从而最大限度地减少向后量子加密过渡期间的服务中断，从而最大限度地减少向后量子密码学过渡期间的服务中断。随着您的客户端应用程序开发出协商 PQ-TLS 密钥交换操作的能力，您可以逐步迁移到更严格的安全策略。
- 您可以启用访问日志以了解有关发送到网络负载均衡器的 TLS 请求的信息、分析 TLS 流量模式、管理安全策略升级以及排查问题。为负载均衡器启用访问日志记录，然后检查相应的访问日志条目。有关更多信息，请参阅访问日志和网络负载均衡器示例查询。
- 要查看负载均衡器访问请求的 TLS 协议版本（日志字段位置 5）和密钥交换（日志字段位置 13），请启用访问日志并检查相应的日志条目。有关更多信息，请参阅访问日志。
- 您可以分别使用您 AWS 账户 的 IAM 中的 Elastic Load Balancing 条件密钥和服务控制策略 (SCP) 来限制用户可以使用哪些安全策略。 AWS Organizations 有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略（SCP）。
- 仅支持 TLS 1.3 的策略支持向前保密（FS）。支持 TLS 1.3 和 TLS 1.2 且仅包含 TLS_* 和 ECDHE_* 格式密码的策略也提供 FS。
- 网络负载均衡器支持 TLS 1.2 的 Extended Master Secret（EMS）扩展。

后端连接

您可以选择用于前端连接但不能选择用于后端连接的安全策略。后端连接的安全策略取决于侦听器的安全策略。如果你的听众中有人在使用：

- FIPS 后量子 TLS 策略-后端连接使用 ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09
- FIPS 策略-后端连接使用 ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04
- Post-quantum TLS 策略-后端连接使用 ELBSecurityPolicy-TLS13-1-0-PQ-2025-09
- TLS 1.3 政策-后端连接使用 ELBSecurityPolicy-TLS13-1-0-2021-06
- 后端连接使用的所有其他 TLS 策略 ELBSecurityPolicy-2016-08

您可以使用 describe-ssl-policies AWS CLI 命令描述协议和密码，也可以参考下表。

安全策略

TLS 安全策略

您可以使用 TLS 安全策略来满足需要禁用某些 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。

仅支持 TLS 1.3 的策略支持向前保密 (FS)。支持 TLS 1.3 和 TLS 1.2 且仅包含 TLS_* 和 ECDHE_* 格式密码的策略也提供 FS。

内容

按策略划分的协议

下表描述了每个 TLS 安全策略支持的协议。

安全策略	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS13-1-3-2021-06	是	没有	没有	没有
ELBSecurityPolicy-TLS13-1-3-PQ-2025-09	是	没有	没有	没有
ELBSecurityPolicy-TLS13-1-2-2021-06	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-PQ-2025-09	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Res-2021-06	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-1-2021-06	是	是	是	没有
ELBSecurityPolicy-TLS13-1-0-2021-06	是	是	是	是
ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	是	是	是	是
ELBSecurityPolicy-TLS-1-2-Ext-2018-06	没有	是	没有	没有
ELBSecurityPolicy-TLS-1-2-2017-01	没有	是	没有	没有
ELBSecurityPolicy-TLS-1-1-2017-01	没有	是	是	没有
ELBSecurityPolicy-2016-08	没有	是	是	是
ELBSecurityPolicy-2015-05	没有	是	是	是

按策略划分的密码

下表描述了每个 TLS 安全策略支持的密码。

安全策略	密码
ELBSecurityPolicy-TLS13-1-3-2021-06 ELBSecurityPolicy-TLS13-1-3-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256
ELBSecurityPolicy-TLS13-1-2-2021-06 ELBSecurityPolicy-TLS13-1-2-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-TLS13-1-2-Res-2021-06 ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384
ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256

安全策略	密码
	• ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

安全策略	密码
ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256

安全策略	密码
ELBSecurityPolicy-TLS13-1-1-2021-06	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

安全策略	密码
ELBSecurityPolicy-TLS13-1-0-2021-06 ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

安全策略	密码
ELBSecurityPolicy-TLS-1-2-Ext-2018-06	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

安全策略	密码
ELBSecurityPolicy-TLS-1-2-2017-01	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256

安全策略	密码
ELBSecurityPolicy-TLS-1-1-2017-01	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

安全策略	密码
ELBSecurityPolicy-2016-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

安全策略	密码
ELBSecurityPolicy-2015-05	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

按密码划分的策略

下表描述了支持每个密码的 TLS 安全策略。

密码名称	安全策略	密码套件
OpenSSL – TLS_AES_128_GCM_SHA256 IANA – TLS_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-3-2021-06 • ELBSecurityPolicy-TLS13-1-3-PQ-2025-09	1301

密码名称	安全策略	密码套件
	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	

密码名称	安全策略	密码套件
OpenSSL – TLS_AES_256_GCM_SHA384 IANA – TLS_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-3-2021-06 • ELBSecurityPolicy-TLS13-1-3-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	1302

密码名称	安全策略	密码套件
OpenSSL – TLS_CHACHA20_POLY1305_SHA256 IANA – TLS_CHACHA20_POLY1305_SHA256	• ELBSecurityPolicy-TLS13-1-3-2021-06 • ELBSecurityPolicy-TLS13-1-3-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	1303

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES128-GCM-SHA256 IANA：TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c02b

密码名称	安全策略	密码套件
OpenSSL — ECDHE-RSA-AES128-GCM-SHA256 IANA：TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c02f

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES128-SHA256 IANA：TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c023

密码名称	安全策略	密码套件
OpenSSL — ECDHE-RSA-AES128-SHA256 IANA：TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c027

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES128-SHA IANA：TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c009
OpenSSL — ECDHE-RSA-AES128-SHA IANA：TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c013

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES256-GCM-SHA384 IANA：TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c02c

密码名称	安全策略	密码套件
OpenSSL — ECDHE-RSA-AES256-GCM-SHA384 IANA：TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c030

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES256-SHA384 IANA：TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c024

密码名称	安全策略	密码套件
OpenSSL — ECDHE-RSA-AES256-SHA384 IANA：TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c028

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES256-SHA IANA：TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c00a
OpenSSL — ECDHE-RSA-AES256-SHA IANA：TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c014

密码名称	安全策略	密码套件
OpenSSL — AES128-GCM-SHA256 IANA：TLS_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	9c

密码名称	安全策略	密码套件
OpenSSL — AES128-SHA256 IANA：TLS_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	3c

密码名称	安全策略	密码套件
OpenSSL — AES128-SHA IANA：TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	2f

密码名称	安全策略	密码套件
OpenSSL — AES256-GCM-SHA384 IANA：TLS_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	9d

密码名称	安全策略	密码套件
OpenSSL — AES256-SHA256 IANA：TLS_RSA_WITH_AES_256_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	3d

密码名称	安全策略	密码套件
OpenSSL — AES256-SHA IANA：TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	35

FIPS 安全策略

联邦信息处理标准（FIPS）是美国和加拿大政府标准，其中规定了对保护敏感信息的加密模块的安全要求。要了解更多信息，请参阅 AWS Cloud 安全性合规性页面上的美国联邦信息处理标准（FIPS）140。

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

> **Important**
>
> 策略 `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04` 和 `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` 只是为了与旧版兼容而提供。虽然它们利用使用 FIPS140 模块的 FIPS 加密，但它们可能不符合最新的 NIST TLS 配置指导。

内容

- 按策略划分的密码
- 按密码划分的策略

按策略划分的协议

下表描述了每个 FIPS 安全策略支持的协议。

安全策略	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04	是	没有	没有	没有
ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09	是	没有	没有	没有
ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09	是	是	没有	没有
ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04	是	是	是	没有
ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	是	是	是	是
ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	是	是	是	是

按策略划分的密码

下表描述了每个 FIPS 安全策略支持的密码。

安全策略	密码
ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384
ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384
ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256

安全策略	密码
	• ECDHE-RSA-AES128-SHA256 • 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

安全策略	密码
ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256
ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA

安全策略	密码
ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • 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

安全策略	密码
ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • 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

按密码划分的策略

下表描述了支持每个密码的 FIPS 安全策略。

密码名称	安全策略	密码套件
OpenSSL – TLS_AES_128_GCM_SHA256 IANA – TLS_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04	1301

密码名称	安全策略	密码套件
	• ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	

密码名称	安全策略	密码套件
OpenSSL – TLS_AES_256_GCM_SHA384 IANA – TLS_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	1302

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES128-GCM-SHA256 IANA：TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c02b

密码名称	安全策略	密码套件
OpenSSL — ECDHE-RSA-AES128-GCM-SHA256 IANA：TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c02f

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES128-SHA256 IANA：TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c023

密码名称	安全策略	密码套件
OpenSSL — ECDHE-RSA-AES128-SHA256 IANA：TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c027

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES128-SHA IANA：TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c009
OpenSSL — ECDHE-RSA-AES128-SHA IANA：TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c013

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES256-GCM-SHA384 IANA：TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c02c

密码名称	安全策略	密码套件
OpenSSL — ECDHE-RSA-AES256-GCM-SHA384 IANA：TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c030

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES256-SHA384 IANA：TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c024

密码名称	安全策略	密码套件
OpenSSL — ECDHE-RSA-AES256-SHA384 IANA：TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c028

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES256-SHA IANA：TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c00a
OpenSSL — ECDHE-RSA-AES256-SHA IANA：TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c014

密码名称	安全策略	密码套件
OpenSSL — AES128-GCM-SHA256 IANA：TLS_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	9c
OpenSSL — AES128-SHA256 IANA：TLS_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	3c

密码名称	安全策略	密码套件
OpenSSL — AES128-SHA IANA：TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	2f
OpenSSL — AES256-GCM-SHA384 IANA：TLS_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	9d

密码名称	安全策略	密码套件
OpenSSL — AES256-SHA256 IANA：TLS_RSA_WITH_AES_256_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	3d
OpenSSL — AES256-SHA IANA：TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	35

FIPS 支持的安全策略

FS（前向保密）支持的安全策略通过使用唯一的随机会话密钥提供了额外的保护措施，防止加密数据侦听。即使秘密的长期密钥被泄露，这也可以防止对捕获的数据进行解码。

本节中的策略支持 FS，且其名称中包含“FS”字样。但是，这些并不是唯一支持 FS 的策略。仅支持 TLS 1.3 的策略支持向前保密 (FS)。支持 TLS 1.3 和 TLS 1.2 且仅包含 TLS_* 和 ECDHE_* 格式密码的策略也提供 FS。

内容

按策略划分的协议

下表描述了每个 FS 支持的安全策略支持的协议。

安全策略	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-FS-1-2-Res-2020-10	没有	是	没有	没有
ELBSecurityPolicy-FS-1-2-Res-2019-08	没有	是	没有	没有
ELBSecurityPolicy-FS-1-2-2019-08	没有	是	没有	没有
ELBSecurityPolicy-FS-1-1-2019-08	没有	是	是	没有
ELBSecurityPolicy-FS-2018-06	没有	是	是	是

按策略划分的密码

下表描述了每个 FS 支持的安全策略支持的密码。

安全策略	密码
ELBSecurityPolicy-FS-1-2-Res-2020-10	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384

安全策略	密码
ELBSecurityPolicy-FS-1-2-Res-2019-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-FS-1-2-2019-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA

安全策略	密码
ELBSecurityPolicy-FS-1-1-2019-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA
ELBSecurityPolicy-FS-2018-06	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA

按密码划分的策略

下表描述了支持每个密码的 FS 支持的安全策略。

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES128-GCM-SHA256 IANA：TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c02b
OpenSSL — ECDHE-RSA-AES128-GCM-SHA256 IANA：TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c02f
OpenSSL — ECDHE-ECDSA-AES128-SHA256 IANA：TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c023
OpenSSL — ECDHE-RSA-AES128-SHA256 IANA：TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c027
OpenSSL — ECDHE-ECDSA-AES128-SHA IANA：TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c009

密码名称	安全策略	密码套件
OpenSSL — ECDHE-RSA-AES128-SHA IANA：TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c013
OpenSSL — ECDHE-ECDSA-AES256-GCM-SHA384 IANA：TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c02c
OpenSSL — ECDHE-RSA-AES256-GCM-SHA384 IANA：TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c030
OpenSSL — ECDHE-ECDSA-AES256-SHA384 IANA：TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c024
OpenSSL — ECDHE-RSA-AES256-SHA384 IANA：TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c028

密码名称	安全策略	密码套件
OpenSSL — ECDHE-ECDSA-AES256-SHA IANA：TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c00a
OpenSSL — ECDHE-RSA-AES256-SHA IANA：TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c014

更新网络负载均衡器的侦听器

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

如果您将协议从 TCP、UDP 或 QUIC 更改为 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、UDP 或 QUIC，则将删除安全策略和服务器证书。

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

不允许对 QUIC 或 TCP_QUIC 侦听器的端口进行更新。要更新处理 QUIC 流量的侦听器端口，必须先删除该侦听器，再通过新端口重新创建。

Console

更新侦听器

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。

4. 在 Li steners 选项卡上，选择Protocol:Port列中的文本以打开监听器的详细信息页面。
5. 选择操作，然后选择编辑侦听器。
6. 根据需要更新值。
   - （可选）更改协议。
   - （可选）更改端口。
   - （可选）为默认操作选择不同的目标组。
   - （可选）要添加其他目标组，请选择添加目标组，并根据需要更新权重。
   - （可选）要移除目标组，请选择移除。
7. （可选）根据需要添加、更新或移除标签。
8. 选择保存更改。

AWS CLI

要更新默认操作

使用以下 modify-listener 命令来更改目标组。

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --default-actions Type=forward,TargetGroupArn=new-target-group-arn
```

以下示例将更新具有多个目标组的侦听器。

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --default-actions '[{
        "Type":"forward",
        "ForwardConfig":{
            "TargetGroups":[
                {"TargetGroupArn":"target-group-1-arn","Weight":10},
                {"TargetGroupArn":"target-group-2-arn","Weight":30}
            ]
        }
    }]'
```

添加 标签

使用 add-tags 命令。以下示例将添加两个标签。

```
aws elbv2 add-tags \
    --resource-arns listener-arn \
    --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

删除标签

使用 remove-tags 命令。以下示例将移除具有指定键的标签。

```
aws elbv2 remove-tags \
    --resource-arns listener-arn \
    --tag-keys project department
```

CloudFormation

要更新默认操作

更新 AWS::ElasticLoadBalancingV2:: Listener 资源以包含新的目标组。

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref newTargetGroup
```

或者，要在多个目标组之间分配流量，请按以下方式定义 DefaultActions。

```
DefaultActions:
    - Type: forward
    ForwardConfig:
        TargetGroups:
        - TargetGroupArn: !Ref TargetGroup1
            Weight: 10
        - TargetGroupArn: !Ref TargetGroup2
            Weight: 30
```

添加 标签

更新 AWS::ElasticLoadBalancingV2:: Listener 资源以包含 Tags 属性。

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

更新网络负载均衡器侦听器的 TCP 空闲超时

对于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。

注意事项

- TCP 流量的默认空闲超时值为 350 秒。
- TLS 侦听器的连接空闲超时为 350 秒，且无法修改。

Console

要更新 TCP 空闲超时

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中的 Load Balancing (负载平衡) 下，选择 Load Balancers (负载均衡器)。
3. 选中网络负载均衡器对应的复选框。
4. 在侦听器选项卡上，选中 TCP 侦听器的复选框，然后依次选择操作、查看侦听器详细信息。
5. 在侦听器详细信息页面的属性选项卡中，选择编辑。如果监听器使用 TCP 以外的协议，则此选项卡将不可用。

6. 输入 TCP 空闲超时值，范围为 60 至 6000 秒。
7. 选择保存更改。

AWS CLI

要更新 TCP 空闲超时

使用带 `tcp.idle_timeout.seconds` 属性的 modify-listener-attributes 命令。

```
aws elbv2 modify-listener-attributes \
    --listener-arn listener-arn \
    --attributes Key=tcp.idle_timeout.seconds,Value=500
```

下面是示例输出。

```
{
    "Attributes": [
        {
            "Key": "tcp.idle_timeout.seconds",
            "Value": "500"
        }
    ]
}
```

CloudFormation

要更新 TCP 空闲超时

更新 AWS::ElasticLoadBalancingV2:: Listener 资源以包含监`tcp.idle_timeout.seconds`听器属性。

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
```

```
          TargetGroupArn: !Ref myTargetGroup
      ListenerAttributes:
        - Key: "tcp.idle_timeout.seconds"
          Value: "500"
```

更新网络负载均衡器的 TLS 侦听器

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

任务

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

替换默认证书

您可以根据需要替换 TLS 侦听器的默认证书。有关更多信息，请参阅 默认证书。

Console

要替换默认证书

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器。
4. 在 Li steners 选项卡上，选择Protocol:Port列中的文本以打开监听器的详细信息页面。
5. 在证书选项卡上，选择更改默认值。
6. 在 ACM 和 IAM 证书表中，选择新的默认证书。
7. （可选）默认情况下，我们选择将之前的默认证书添加到侦听器证书列表中。我们建议您保持此选项的选中状态，除非您当前没有用于 SNI 的侦听器证书且依赖于 TLS 会话恢复功能。
8. 选择另存为默认值。

AWS CLI

要替换默认证书

使用 modify-listener 命令。

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --certificates CertificateArn=new-default-certificate-arn
```

CloudFormation

替换默认证书

使用新的默认证书更新 AWS::ElasticLoadBalancingV2:: Listener 资源。

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "new-default-certificate-arn"
```

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。您可以将默认证书添加到证书列表，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。

Console

要将证书添加到证书列表

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

2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在 Li steners 选项卡上，选择Protocol:Port列中的文本以打开监听器的详细信息页面。
5. 选择 Certificates (证书) 选项卡。
6. 要将默认证书添加到列表，请选择将默认证书添加到列表。
7. 要将非默认证书添加大列表，请执行以下操作：

   a. 选择添加证书。
   b. 要添加已由 ACM 或 IAM 管理的证书，请选中证书对应的复选框并选择在下面以待注册的形式添加。
   c. 要添加未由 ACM 或 IAM 管理的证书，请选择导入证书，完成表格，然后选择导入。
   d. 选择添加待处理证书。

AWS CLI

要将证书添加到证书列表

使用 add-listener-certificates 命令。

```
aws elbv2 add-listener-certificates \
    --listener-arn listener-arn \
    --certificates \
        CertificateArn=certificate-arn-1 \
        CertificateArn=certificate-arn-2 \
        CertificateArn=certificate-arn-3
```

CloudFormation

要将证书添加到证书列表

定义类型为 AWS::ElasticLoadBalancingV2:: ListenerCertificate 的资源。

```
Resources:
  myCertificateList:
    Type: 'AWS::ElasticLoadBalancingV2::ListenerCertificate'
    Properties:
      ListenerArn: !Ref myTLSListener
      Certificates:
```

```
        - CertificateArn: "certificate-arn-1"
        - CertificateArn: "certificate-arn-2"
        - CertificateArn: "certificate-arn-3"

  myTLSListener:
    Type: AWS::ElasticLoadBalancingV2::Listener
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLSS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "certificate-arn-1"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

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。删除证书后，侦听器将无法再使用该证书建立连接。为确保客户端不受影响，在从列表中删除证书之前，请先将新的证书添加至列表并确认连接功能正常。

要删除 TLS 侦听器的默认证书，请参阅替换默认证书。

Console

要从证书列表中删除证书

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在 Li steners 选项卡上，选择Protocol:Port列中的文本以打开监听器的详细信息页面。
5. 在证书选项卡上，选中证书对应的复选框，然后选择删除。
6. 提示进行确认时，输入 **confirm**，然后选择删除。

AWS CLI

要从证书列表中删除证书

使用 remove-listener-certificates 命令。

```
aws elbv2 remove-listener-certificates \
    --listener-arn listener-arn \
    --certificates CertificateArn=certificate-arn
```

更新安全策略

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

如果负载均衡器处理大量流量，则更新安全策略可能会导致中断。为降低负载均衡器高负载状态下的中断风险，请创建额外的负载均衡器来分担流量，或请求 LCU 预留。

Console

要更新安全策略

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在 Li steners 选项卡上，选择Protocol:Port列中的文本以打开监听器的详细信息页面。
5. 选择操作，然后选择编辑侦听器。
6. 在安全侦听器设置部分的安全策略下，选择新的安全策略。
7. 选择保存更改。

AWS CLI

要更新安全策略

使用 modify-listener 命令。

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06
```

CloudFormation

要更新安全策略

使用新的安全策略更新 AWS::ElasticLoadBalancingV2:: Listener 资源。

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "default-certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

更新 ALPN 策略

您可以根据需要更新 TLS 侦听器的 ALPN 策略。有关更多信息，请参阅 ALPN 策略。

Console

要更新 ALPN 策略

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择负载均衡器。
3. 选择负载均衡器的名称以打开其详细信息页面。
4. 在 Li steners 选项卡上，选择Protocol:Port列中的文本以打开监听器的详细信息页面。
5. 选择操作，然后选择编辑侦听器。
6. 在安全侦听器设置部分，针对 ALPN 策略，选择一项策略以启用 LPN，或选择无以禁用 ALPN。
7. 选择保存更改。

AWS CLI

要更新 ALPN 策略

使用 modify-listener 命令。

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --alpn-policy HTTP2Preferred
```

CloudFormation

要更新 ALPN 策略

更新 AWS::ElasticLoadBalancingV2:: Listener 资源以包含 ALPN 政策。

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"
      AlpnPolicy:
        - HTTP2Preferred
      Certificates:
        - CertificateArn: "certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

删除网络负载均衡器的侦听器

在删除侦听器之前，请考虑其对应用程序的影响：

- [TCP 和 TLS 侦听器] 负载均衡器会立即停止在监听器上接收新的连接请求。任何正在进行的 TLS 握手都可能会失败。现有连接将保持打开状态，直到它们自然关闭或超时。 In-flight对现有连接的请求成功完成。
- [UDP 和 QUIC 侦听器] 任何传输中的数据包都可能无法到目标位置。

Console

删除侦听器

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

AWS CLI

删除侦听器

使用 delete-listener 命令。

```
aws elbv2 delete-listener \
    --listener-arn listener-arn
```

网络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。流量将转发到在侦听器规则中指定的目标组。您可以为不同类型的请求创建不同的目标组。例如，为一般请求创建一个目标组，为应用程序的微服务请求创建其他目标组。有关更多信息，请参阅 网络负载均衡器组件。

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

目录

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。

网络负载均衡器的目标组支持以下协议和端口：

- 协议：TCP、TLS、UDP TCP_UDP、QUIC、TCP_QUIC
- 端口：1-65535

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

下表总结了侦听器协议和目标组设置的组合。

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

Target type

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

以下是可能的目标类型：

`instance`

这些目标通过实例 ID 指定。

`ip`

这些目标通过 IP 地址指定。

`alb`

目标是应用程序负载均衡器。

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

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

> **Important**
>
> 不能指定可公开路由的 IP 地址。

您可以使用所有支持的 CIDR 块，向目标组注册以下目标：

- AWS 可通过 IP 地址和端口寻址的资源（例如数据库）。
- AWS 通过 Direct Connect 或 Site-to-Site VPN 连接链接到的本地资源。

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

在共享 VPC 中启动网络负载均衡器时（作为参与者），您只能在已共享的子网中注册目标。

当目标类型为 `alb` 时，您可以将单个应用程序负载均衡器注册为目标。有关更多信息，请参阅 将应用程序负载均衡器作为网络负载均衡器的目标。

网络负载均衡器不支持 `lambda` 目标类型。应用程序负载均衡器是支持 `lambda` 目标类型的唯一负载均衡器。有关更多信息，请参阅应用程序负载均衡器用户指南中的 Lambda 函数作为目标。

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

请求路由和 IP 地址

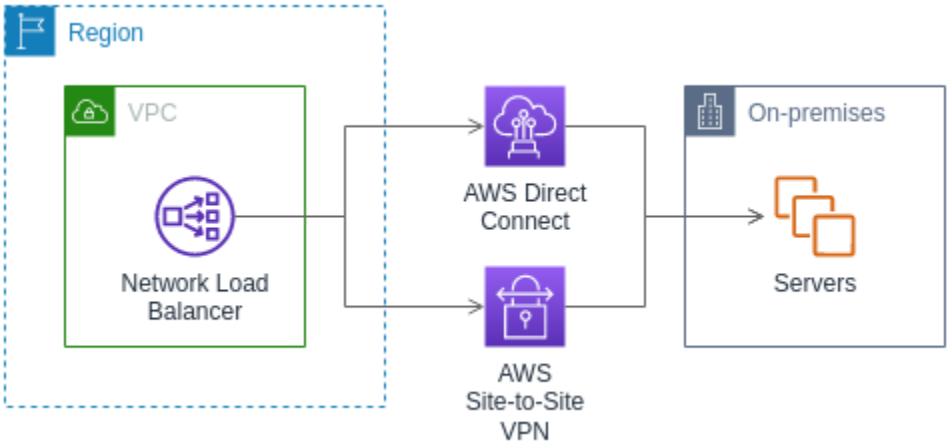
如果使用实例 ID 指定目标，则使用实例的主网络接口中指定的主私有 IP 地址将流量路由到实例。负载均衡器在将数据包转发到目标实例之前重写目的地 IP 地址。

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

有关允许实例的流量的更多信息，请参阅目标安全组。

将本地资源作为目标

当目标类型为时，通过 Direct Connect 或 Site-to-Site VPN 连接链接的本地资源可以用作目标`ip`。



使用本地资源时，这些目标的 IP 地址必须仍来自下列 CIDR 块之一：

- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

有关的更多信息 Direct Connect，请参阅什么是 Direct Connect？

有关的更多信息 AWS Site-to-Site VPN，请参阅什么是 AWS Site-to-Site VPN？

IP 地址类型

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

您网络负载均衡器的目标组支持以下 IP 地址类型：

ipv4

负载均衡器使用 IPv4与目标通信。

ipv6

负载均衡器使用 IPv6与目标通信。

注意事项

- 负载均衡器根据目标组的 IP 地址类型与目标进行通信。 IPv4 目标组的目标必须接受来自负载均衡器的 IPv4流量， IPv6 目标组的目标必须接受来自负载均衡器的 IPv6 流量。
- 您不能将 IPv6 目标组与`ipv4`负载均衡器一起使用。
- 您不能将 IPv4 目标组与`dualstack`负载均衡器的 UDP 侦听器配合使用。
- 您无法向 IPv6 目标组注册 Application Load Balancer。
- 您不能将 IPv6 目标群体与 QUIC 或 TCP_QUIC 协议一起使用。

已注册目标

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

如果应用程序需求增加，您可以向一个或多个目标组注册其他目标以便满足该需求。一旦注册过程完成，并且目标通过了第一项初始运行状况检查，负载均衡器就会开始将流量路由到新注册的目标，而不管配置的阈值如何。

如果应用程序需求减少或者您需要为目标提供服务，您可以从目标组取消注册目标。取消注册目标将从目标组中删除目标，但不会影响目标。一旦取消注册，负载均衡器就会停止将流量路由到目标。目标将

进入 `draining` 状态，直至进行中请求完成。当您准备好恢复接收流量时，可以再次向目标组注册目标。

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

要求和注意事项

- 如果实例使用以下实例类型之一，则无法按实例 ID 注册实例：C1、、、、、 CC1 CC2、G1 CG1 CG2、G2 CR1、、、、M1 HI1、M2 HS1、M3 或 T1。
- 按实例 ID 为 IPv6 目标组注册目标时，必须为目标分配主 IPv6 地址。要了解更多信息，请参阅 Amazon EC2 用户指南中的 IPv6 地址
- 按实例 ID 注册目标时，实例必须与网络负载均衡器位于同一个 VPC 中。如果实例所在的 VPC 与负载均衡器 VPC 是对等的（位于同一区域或不同区域），则不能按实例 ID 注册实例。可以用 IP 地址注册这些实例。
- 如果您按 IP 地址注册目标，并且该 IP 地址与负载均衡器位于同一 VPC 中，则负载均衡器会验证其是否来自可以访问的子网。
- 负载均衡器仅将流量路由到已启用的可用区中的目标。未启用的区域中的目标未使用。
- 对于 UDP、TCP_UDP、QUIC 和 TCP_QUIC 目标组，如果实例位于负载均衡器 VPC 之外或使用以下实例类型之一：C1、、、、、、G1、G2、、、、、、M1、M2 CC1 CC2 CG1 CG2 CR1、M3 或 T1，则不要按 IP 地址注册实例。 HI1 HS1如果目标驻留在负载均衡器 VPC 之外或者采用不受支持的实例类型，则目标可能能够接收来自负载均衡器的流量，但随后无法响应。

目标组属性

您可以通过编辑目标组的属性来配置它。有关更多信息，请参阅 编辑目标组属性。

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

`deregistration_delay.timeout_seconds`

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

deregistration_delay.connection_termination.enabled

指示负载均衡器是否在取消注册超时结束时终止连接。该值为 true 或 false。对于新的 UDP/TCP_UDP 目标组，默认值为 true。否则，默认值为 false。此属性不适用于 QUIC 流量。

load_balancing.cross_zone.enabled

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

preserve_client_ip.enabled

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

proxy_protocol_v2.enabled

指示是否已启用代理协议版本 2。默认情况下，禁用代理协议。

stickiness.enabled

指示是否启用粘性会话。该值为 true 或 false。默认为 false。此属性不适用于 QUIC 流量。

stickiness.type

粘性的类型。可能的值为 source_ip。

target_group_health.dns_failover.minimum_healthy_targets.count

必须运行状况良好的目标数量下限。如果运行状况良好的目标数量低于此值，请在 DNS 中将该区域标记为运行状况不佳，以便流量仅路由到运行状况良好的区域。可能的值是 off 或者 1 到目标数量上限之间的整数。当 off 时，DNS 故障转移被禁用，这意味着即使目标组中的所有目标都运行状况不佳，也不会从 DNS 中移除该区域。默认 为 1。

target_group_health.dns_failover.minimum_healthy_targets.percentage

必须运行状况良好的目标最低百分比。如果运行状况良好的目标百分比低于此值，请在 DNS 中将该区域标记为运行状况不佳，以便流量仅路由到运行状况良好的区域。可能的值为 off 或者 1 到 100 之间的整数。当 off 时，DNS 故障转移被禁用，这意味着即使目标组中的所有目标都运行状况不佳，也不会从 DNS 中移除该区域。默认值为 off。

target_group_health.unhealthy_state_routing.minimum_healthy_targets.count

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

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

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

`target_health_state.unhealthy.connection_termination.enabled`

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

`target_health_state.unhealthy.draining_interval_seconds`

弹性负载均衡在将运行状况不佳目标的状态从 `unhealthy.draining` 更改为 `unhealthy` 之前需等待的时间。范围为 0-360000 秒。默认值为 0 秒。

注意：只有在 `target_health_state.unhealthy.connection_termination.enabled` 为 `false` 时才能配置此属性。

目标组运行状况

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

内容

运行状况不佳状态的操作

您可以为以下操作配置运行状况良好阈值：

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

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

要求和注意事项

- 如果为某项操作指定了两种类型的阈值（计数和百分比），则负载均衡器会在违反任一阈值时执行该操作。
- 如果为这两项操作都指定了阈值，则 DNS 故障转移的阈值必须大于或等于路由故障转移的阈值，以便 DNS 故障转移会在路由故障转移时或之前发生。
- 如果您将阈值指定为百分比，我们将根据在目标组中注册的目标总数动态计算该值。
- 目标总数取决于关闭还是打开跨区域负载均衡。如果跨区域负载均衡处于关闭状态，则每个节点仅向自己区域中的目标发送流量，这意味着阈值将分别应用于每个已启用区域中的目标数量。如果跨区域负载均衡处于打开状态，则每个节点将流量发送到所有已启用区域中的所有目标，这意味着指定的阈值将应用于所有已启用区域中的目标总数。有关更多信息，请参阅 跨可用区负载均衡。
- 当发生 DNS 故障转移时，会影响与负载均衡器关联的所有目标组。请确保剩余区域中有足够的容量来处理这些额外流量，尤其是在跨区域负载均衡关闭的情况下。
- 通过 DNS 故障转移，我们会从负载均衡器的 DNS 主机名中删除运行状况不佳区域的 IP 地址。但是，在 DNS 记录中的 time-to-live (TTL) 到期（60 秒）之前，本地客户端 DNS 缓存可能包含这些 IP 地址。
- 使用 DNS 故障转移时，如果有多个目标组连接到网络负载均衡器，并且一个目标组在某个区域中运行状况不佳，则会发生 DNS 故障转移，即使该区域中的另一个目标组运行状况良好。
- 使用 DNS 故障转移时，如果所有负载均衡器区域都被视为运行状况不佳，则负载均衡器会将流量发送到所有区域（包括运行状况不佳的区域）。
- 除了是否有足够运行状况良好的目标可能会导致 DNS 故障转移之外，还有其他因素，例如区域的运行状况。

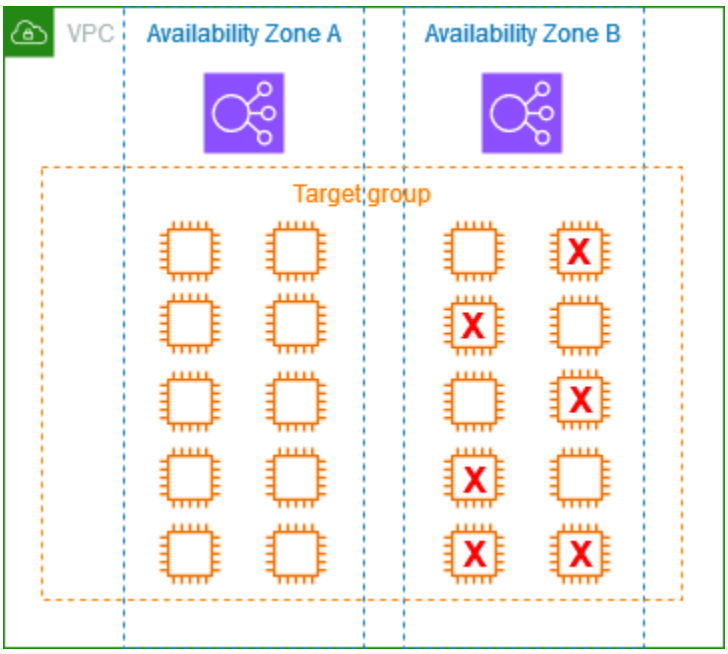
示例

以下示例演示了如何应用目标组运行状况设置。

场景

- 支持 A 和 B 两个可用区的负载均衡器
- 每个可用区中包含 10 个注册目标

- 目标组具有以下目标组运行状况设置：
  - DNS 故障转移 - 50%
  - 路由故障转移 - 50%
- 可用区 B 中有六个目标失败



如果跨区域负载均衡关闭

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

如果跨区域负载均衡打开

- 每个负载均衡器节点可以向两个可用区中的所有 20 个注册目标发送流量。

- 可用区 A 中有 10 个运行状况良好的目标，可用区 B 中有 4 个运行状况良好的目标，总共有 14 个运行状况良好的目标。这是两个可用区中负载均衡器节点目标的 70%，符合所需的运行状况良好的目标百分比。
- 负载均衡器将在两个可用区内 14 个运行状况良好的目标之间分配流量。

为负载均衡器使用 Route 53 DNS 故障转移

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

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

如何评估目标的运行状况

- 如果网络负载均衡器别名记录上的“评估目标运行状况”设置为 `Yes`，则 Route 53 将评估 `alias target` 值指定的资源的运行状况。Route 53 使用目标组运行状况检查。
- 如果连接到网络负载均衡器的所有目标组均运行正常，则 Route 53 会将别名记录标记为“运行正常”。如果您为目标组配置了阈值且该目标组满足其阈值要求，则视为“通过运行状况检查”。否则，只要目标组包含至少一个运行正常的目标，即视为“通过运行状况检查”。如果“通过运行状况检查”，则 Route 53 会根据您的路由策略返回记录。如果使用失效转移路由策略，则 Route 53 会返回主记录。
- 如果连接到网络负载均衡器的所有目标组运行状况不佳，则别名记录无法通过 Route 53 运行状况检查（失效时开放）。如果使用“评估目标的运行状况”，这将导致失效转移路由策略将流量重定向至辅助资源。
- 如果网络负载均衡器中的所有目标组均为空（无目标），则 Route 53 会认为此记录运行状况不佳（失效时开放）。如果使用“评估目标的运行状况”，这将导致失效转移路由策略将流量重定向至辅助资源。

有关更多信息，请参阅 AWS 博客中的使用负载均衡器目标组运行状况阈值来提高可用性和 Amazon Route 53 开发人员指南中的配置 DNS 故障转移。

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。

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 默认操作。您可以在多个侦听器中指定同一个目标组，但这些侦听器必须属于同一个网络负载均衡器。要将目标组与负载均衡器结合使用，您必须确认目标组没有被任何其他负载均衡器的侦听器使用。

您可以随时在目标组中添加或删除目标。有关更多信息，请参阅 为网络负载均衡器注册目标。您也可以修改目标组的运行状况检查设置。有关更多信息，请参阅 更新网络负载均衡器目标组的运行状况检查设置。

要求

- 创建目标组后，您将无法更改其目标类型或其 IP 地址类型。
- 目标组中的所有目标必须与目标组具有相同的 IP 地址类型： IPv4 或 IPv6。
- 您必须使用带有双栈负载均衡器的 IPv6 目标组。
- 您不能将 IPv4 目标组与`dualstack`负载均衡器的 UDP 侦听器配合使用。
- 您不能将 IPv6 目标群体与 QUIC 或 TCP_QUIC 协议一起使用。

Console

创建目标组

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择目标组。
3. 选择创建目标组。
4. 在基本配置窗格中执行以下操作：
   a. 对于 Choose a target type（选择目标类型），选择 Instance（实例）以按实例 ID 注册目标，选择 IP addresses（IP 地址）以按 IP 地址注册目标，或者选择 Application Load Balancer（应用程序负载均衡器）以将某个应用程序负载均衡器注册为目标。
   b. 对于目标组名称，输入目标组的名称。此名称在每个区域的每个账户中必须唯一，最多可以有 32 个字符，只能包含字母数字字符或连字符，不得以连字符开头或结尾。

c. 对于 Protocol (协议)，选择协议，如下所示：

- 如果侦听器协议为 TCP，选择 TCP 或 TCP_UDP。
- 如果侦听器协议为 TLS，选择 TCP 或 TLS。
- 如果侦听器协议为 UDP，选择 UDP 或 TCP_UDP。
- 如果侦听器协议为 TCP_UDP，选择 TCP_UDP。
- 如果侦听器协议为 QUIC，则选择 QUIC。
- 如果侦听器协议为 TCP_QUIC，则选择 TCP_QUIC。
- 如果目标类型为应用程序负载均衡器，则协议必须是 TCP。

d. 对于端口，请根据需要修改默认值。

如果目标类型为应用程序负载均衡器，则端口必须与应用程序负载均衡器的侦听器端口匹配。

e. 对于 IP 地址类型，请选择IPv4或IPv6。仅当目标类型为实例或 IP 地址时，此选项才可用。

f. 对于 VPC，选择具有要注册的目标的虚拟私有云（VPC）。

5. 对于运行状况检查窗格，根据需要修改默认设置。对于高级运行状况检查，选择运行状况检查端口、计数、超时、间隔并指定成功代码。如果运行状况检查连续超过不正常运行阈值计数，负载均衡器将使目标停止服务。如果运行状况检查连续超过运行状况正常阈值计数，负载均衡器将使目标恢复使用。有关更多信息，请参阅 ???。
6. （可选）要添加标签，请展开标签，选择添加标签，然后输入标签键和标签值。
7. 选择下一步。
8. （可选）注册目标。目标组的目标类型决定了您需要提供的信息。如果您现在还没有准备好注册目标，则可以稍后进行注册。
   - 实例 - 选择 EC2 实例，输入端口，然后选择在下面以待注册的形式添加。
   - IP 地址 - 选择包含 IP 地址或其他私有 IP 地址的 VPC，输入 IP 地址和端口，然后选择在下面以待注册的形式添加。
   - 应用程序负载均衡器 - 选择应用程序负载均衡器。有关更多信息，请参阅 使用应用程序负载均衡器作为目标。
9. 选择创建目标组。

AWS CLI

创建目标组

使用 create-target-group 命令。以下示例通过 TCP 协议、按 IP 地址注册的目标、一个标签和默认运行状况检查设置来创建目标组。

```
aws elbv2 create-target-group \
    --name my-target-group \
    --protocol TCP \
    --port 80 \
    --target-type ip \
    --vpc-id vpc-1234567890abcdef0 \
    --tags Key=department,Value=123
```

要注册目标

使用 register-targets 命令将目标注册到目标组。有关示例，请参阅 the section called “注册目标”。

CloudFormation

创建目标组

定义类型为的资源AWS::ElasticLoadBalancingV2::TargetGroup。以下示例通过 TCP 协议、按 IP 地址注册的目标、一个标签、默认运行状况检查设置和两个已注册目标来创建目标组。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      Tags:
        - Key: 'department'
          Value: '123'
      Targets:
        - Id: 10.0.50.10
          Port: 80
        - Id: 10.0.50.20
          Port: 80
```

更新网络负载均衡器的目标组运行状况设置

默认情况下，网络负载均衡器将监控目标的运行状况，并将请求路由到运行状况良好的目标。然而，如果负载均衡器没有足够的运行状况良好的目标，它会自动将流量发送到所有已注册的目标（失效时开放）。您可以修改目标组的运行状况设置，为 DNS 故障转移和路由故障转移定义阈值。有关更多信息，请参阅 the section called “目标组运行状况”。

Console

要更新目标组的运行状况设置

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Attributes（属性）选项卡上，选择 Edit（编辑）。
5. 展开 Target group health requirements（目标组运行状况要求）。
6. 对于 Configuration type（配置类型），我们建议您选择 Unified configuration（统一配置），它会为 DNS 故障转移和路由故障转移设置相同的阈值。
7. 对于 Healthy state requirements（运行状况良好状态要求），请执行以下操作之一：
   - 选择 Minimum healthy target count（运行状况良好的目标最低计数），然后输入介于 1 到目标组的最大目标数之间的数字。
   - 选择 Minimum healthy target percentage（运行状况良好的目标最低百分比），然后输入 1 到 100 之间的数字。
8. 信息文本会显示目标组是否启用了跨区域负载均衡。如果跨区域负载均衡处于禁用状态，您可以启用该功能以确保拥有足够的容量。在目标选择配置部分，更新跨区域负载均衡。

   以下文本表明跨区域负载均衡处于禁用状态：

   ```
   Healthy state requirements apply to each zone independently.
   ```

   以下文本表明跨区域负载均衡处于启用状态：

   ```
   Healthy state requirements apply to the total targets across all applicable
    zones.
   ```

9. 选择保存更改。

AWS CLI

要更新目标组的运行状况设置

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

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes \

 "Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50"
 \

 "Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=5
```

CloudFormation

要修改目标组的运行状况设置

更新AWS::ElasticLoadBalancingV2::TargetGroup资源。以下示例将两个运行状况不佳状态操作的运行状况良好阈值设置为 50%。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_group_health.dns_failover.minimum_healthy_targets.percentage"
          Value: "50"
        - Key:
 "target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage"
          Value: "50"
```

网络负载均衡器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。只要注册过程完成且新注册的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此目标。完成注册过程和开始运行状况检查可能需要几分钟时间。

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

借助被动的运行状况检查，负载均衡器观察目标如何响应连接。借助被动的运行状况检查，负载均衡器能够在主动的运行状况检查报告目标运行状况不佳之前，检测出此运行状况不佳的目标。您无法禁用、配置或监视被动运行状况检查。UDP 流量和已开启粘性的目标组不支持被动运行状况检查。有关更多信息，请参阅粘性会话。

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

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

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

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

如果您将 TLS 侦听器添加到网络负载均衡器，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 连接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 连接，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 和 QUIC 服务，可以对目标组执行非 UDP 运行状况检查来测试目标可用性。您可以通过任何可用的运行状况检查（TCP、HTTP 或 HTTPS）和目标上的任何端口来验证您服务的可用性。如果接收运行状况检查的服务失败，则目标会视为不可用。要提高针对您的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 或 QUIC 服务的状态，并停止运行状况检查。

有关更多信息，请参阅 the section called “目标组运行状况”。

内容

运行状况检查设置

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

设置	说明	默认
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。如果目标类型为 `alb`，支持的运行状况检查协议为 HTTP 和 HTTPS。	TCP
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。	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运行状况检查路径。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 2–120 秒。HTTP 运行状况检查时间的默认值为 6 秒，TCP 和 HTTPS 运行状况检查时间的默认值为 10 秒。	HTTP 运行状况检查需要 6 秒，TCP 和 HTTPS 运行状况检查需要 10 秒。

设置	说明	默认
HealthCheckIntervalSeconds	各个目标的运行状况检查之间的大约时间量 (以秒为单位)。范围为 5–300 秒。默认值为 30 秒。 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。	30 秒
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 2–10。默认值为 5。	5
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 2–10。默认值为 2。	2
Matcher	[HTTP/HTTPS 运行状况检查] 检查来自目标的成功响应时使用的 HTTP 代码。范围为 200 至 599。默认值为 200-399。	200-399

目标运行状况

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

下表描述已注册目标的正常状态的可能值。

值	说明
`initial`	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。

值	说明
	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，未通过运行状况检查，或目标处于停止状态。 相关原因代码：Target.FailedHealthChecks
draining	目标正在取消注册，连接即将耗尽。 相关原因代码：Target.DeregistrationInProgress
unhealthy.draining	目标未响应运行状况检查或未通过运行状况检查并进入宽限期。目标支持现有连接，且在此宽限期内不接受任何新连接。 相关原因代码：Target.FailedHealthChecks
unavailable	目标运行状况不可用。 相关原因代码：Elb.InternalError
unused	目标未注册到目标组，侦听器规则中未使用目标组，或者目标在未启用的可用区中。 相关原因代码：Target.NotRegistered |Target.NotInUse |Target.InvalidState |Target.IpUnusable

运行状况检查原因代码

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

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

检查网络负载均衡器目标的运行状况

您可以检查已注册到目标组的目标的运行状况。有关运行状况检查失败问题的帮助，请参阅问题排查：已注册目标未处于可用状态。

Console

要检查目标的运行状况

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

接收有关运行状况不佳的目标的电子邮件通知

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

AWS CLI

要检查目标的运行状况

使用 describe-target-health 命令。此示例对输出进行筛选，以仅包括运行状况不良的目标。对于运行状况不良的目标，输出将包含原因代码。

```
aws elbv2 describe-target-health \
    --target-group-arn target-group-arn \
    --query "TargetHealthDescriptions[?TargetHealth.State!='healthy'].
[Target.Id,TargetHealth.State,TargetHealth.Reason]" \
    --output table
```

下面是示例输出。

```
-------------------------------------------------
|            DescribeTargetHealth              |
+--------------+---------+--------------------+
|  172.31.0.57 |  unused |  Target.NotInUse   |
|  172.31.0.50 |  unused |  Target.NotInUse   |
+--------------+---------+--------------------+
```

目标状态和原因代码

下表列出了每种目标状态的可能原因代码。

目标状态为 healthy

未提供原因代码。

目标状态为 initial

- `Elb.RegistrationInProgress` - 目标正处于与负载均衡器的注册流程中。
- `Elb.InitialHealthChecking` - 负载均衡器仍在向目标发送最低数量的运行状况检查，以确定其运行状况。

目标状态为 unhealthy

- `Target.FailedHealthChecks` - 负载均衡器在建立与目标的连接时收到错误，或目标响应格式错误。

目标状态为 unused

- `Target.NotRegistered` - 目标未注册到目标组
- `Target.NotInUse` - 该目标组未被任何负载均衡器使用，或目标所在的可用区未启用其负载均衡器。
- `Target.InvalidState` - 目标处于停止或终止状态。
- `Target.IpUnusable` - 目标 IP 地址已保留，供负载均衡器使用。

目标状态为 draining

- `Target.DeregistrationInProgress` - 目标正处于注销过程中，且注销延迟期尚未到期。

目标状态为 unavailable

- `Elb.InternalError` - 由于内部错误，目标的运行状况无法获取。

更新网络负载均衡器目标组的运行状况检查设置

您可以随时更新目标组的运行状况检查设置。有关运行状况检查设置的列表，请参阅 the section called “运行状况检查设置”。

Console

要更新运行状况检查设置

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

2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Health checks 选项卡上，选择 Edit。
5. 在编辑运行状况检查设置页面上，根据需要修改设置。
6. 选择保存更改。

AWS CLI

要更新运行状况检查设置

使用 modify-target-group 命令。以下示例更新了HealthyThresholdCount和HealthCheckTimeoutSeconds设置。

```
aws elbv2 modify-target-group \
    --target-group-arn target-group-arn \
    --healthy-threshold-count 3 \
    --health-check-timeout-seconds 20
```

CloudFormation

要更新运行状况检查设置

更新AWS::ElasticLoadBalancingV2::TargetGroup资源以包含更新的运行状况检查设置。以下示例更新了HealthyThresholdCount和HealthCheckTimeoutSeconds设置。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      HealthyThresholdCount: 3
      HealthCheckTimeoutSeconds: 20
```

编辑网络负载均衡器的目标组属性

创建网络负载均衡器的目标组之后，您可以编辑其目标组属性。

目标组属性

- 客户端 IP 保留
- 取消注册延迟
- 代理协议
- 粘性会话
- 目标组的跨区域负载均衡
- 运行状况不佳的目标的连接终止
- 运行状况不佳的耗尽间隔

客户端 IP 保留

在将请求路由到后端目标时，网络负载均衡器可以保留客户端的源 IP 地址。禁用客户端 IP 保留时，源 IP 地址为网络负载均衡器的私有 IP 地址。

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

默认设置

- 实例类型目标组：已启用
- IP 类型目标组（UDP、TCP_UDP、QUIC、TCP_QUIC）：已启用
- IP 类型目标组（TCP、TLS）：已禁用

当启用客户端 IP 保留时

下表说明了启用客户端 IP 保留时目标接收的 IP 地址。

Targets	IPv4 客户请求	IPv6 客户请求
实例类型 (IPv4)	客户 IPv4 地址	负载均衡器 IPv4 地址

Targets	IPv4 客户请求	IPv6 客户请求
IP 类型 (IPv4)	客户 IPv4 地址	负载均衡器 IPv4 地址
IP 类型 (IPv6)	负载均衡器 IPv6 地址	客户 IPv6 地址

当禁用客户端 IP 保留时

下表说明了禁用客户端 IP 保留时目标接收的 IP 地址。

Targets	IPv4 客户请求	IPv6 客户请求
实例类型 (IPv4)	负载均衡器 IPv4 地址	负载均衡器 IPv4 地址
IP 类型 (IPv4)	负载均衡器 IPv4 地址	负载均衡器 IPv4 地址
IP 类型 (IPv6)	负载均衡器 IPv6 地址	负载均衡器 IPv6 地址

要求和注意事项

- 客户端 IP 保留更改仅对新的 TCP 连接生效。
- 启用客户端 IP 保留后，流量必须直接从网络负载均衡器流向目标。目标必须与负载均衡器位于同一 VPC 中，或位于同一区域的对等 VPC 中。
- 当目标通过中转网关访问时，不支持客户端 IP 保留。
- 使用网关负载均衡器端点检查网络负载均衡器和目标（实例或 IP 地址）之间的流量时，即使目标与网络负载平衡器位于同一个 VPC 中，也不支持客户端 IP 保留。
- 以下实例类型不支持保留客户端 IP：C1、、、、、 CC1、 CC2、G1 CG1 CG2 CR1、G2、、、、M1 HI1、M2 HS1、M3 和 T1。我们建议您在禁用客户端 IP 保留的情况下将这些实例类型注册为 IP 地址。
- 客户端 IP 保留对于 AWS PrivateLink入站流量没有影响。 AWS PrivateLink 流量的源 IP 地址始终是 Network Load Balancer 的私有 IP 地址。
- 当目标组包含 AWS PrivateLink 网络接口或其他网络负载均衡器的网络接口时，不支持客户端 IP 保留。这将导致与这些目标的通信中断。
- 客户端 IP 保留对从 IPv6 到的流量没有影响 IPv4。此类型流量的源 IP 地址始终是网络负载均衡器的私有 IP 地址。

- 当您按应用程序负载均衡器类型指定目标时，网络负载均衡器将保留所有传入流量的客户端 IP 并发送到应用程序负载均衡器。然后，应用程序负载均衡器会将客户端 IP 附加到 `X-Forwarded-For` 请求标头，之后才发送此请求标头。
- 启用客户端 IP 保留后，不支持 NAT 环回（也称为发夹转换）。当使用内部网络负载均衡器时，会发生这种情况，而在网络负载均衡器后面注册的目标会创建与同一个网络负载均衡器的连接。该连接可能会被路由到正在尝试创建连接的目标，从而导致连接错误。我们建议您避免从同一网络负载均衡器后面的目标连接至网络负载均衡器，您也可以通过禁用客户端 IP 保留来防止此类连接错误。如果您需要客户端 IP 地址，则可以使用代理协议 v2 进行检索。有关更多信息，请参阅 代理协议。
- 当禁用客户端 IP 保留时，网络负载均衡器支持到每个唯一目标（IP 地址和端口）的 5.5 万个并发连接或每分钟大约 5.5 万个连接。如果连接数超过该值，则会增大出现端口分配错误的几率，进而导致无法建立新连接。有关更多信息，请参阅 后端流端口分配错误。

Console

要修改客户端 IP 保留

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在属性选项卡中，选择编辑，然后找到流量配置窗格。
5. 要启用客户端 IP 保留，请开启 Preserve client IP addresses（保留客户端 IP 地址）。要禁用客户端 IP 保留，请关闭 Preserve client IP addresses（保留客户端 IP 地址）。
6. 选择保存更改。

AWS CLI

要启用客户端 IP 保留

使用带 `preserve_client_ip.enabled` 属性的 modify-target-group-attributes 命令。

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=preserve_client_ip.enabled,Value=true"
```

CloudFormation

要启用客户端 IP 保留

更新AWS::ElasticLoadBalancingV2::TargetGroup 资源以包含该preserve_client_ip.enabled属性。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "preserve_client_ip.enabled"
          Value: "true"
```

取消注册延迟

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

取消注册的目标的初始状态为 `draining`，在此期间，该目标将停止接收新连接。但是，由于配置传播延迟，目标可能仍然会收到连接。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。对于 QUIC 流量，该值始终为 300 秒，且无法调整。

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

Console

要修改取消注册延迟属性

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

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

AWS CLI

要修改取消注册延迟属性

使用带有deregistration_delay.timeout_seconds和deregistration_delay.connection_termin性的modify-target-group-attributes命令。

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes \
      "Key=deregistration_delay.timeout_seconds,Value=60" \
      "Key=deregistration_delay.connection_termination.enabled,Value=true"
```

CloudFormation

要修改取消注册延迟属性

更新AWS::ElasticLoadBalancingV2::TargetGroup资源以包含deregistration_delay.timeout_seconds和deregistration_delay.connection_termin性。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "deregistration_delay.timeout_seconds"
          Value: "60"
        - Key: "deregistration_delay.connection_termination.enabled"
          Value: "true"
```

代理协议

网络负载均衡器使用代理协议版本 2 来发送其他连接信息，如源和目标。代理协议版本 2 提供代理协议标头的二进制编码。

对于 TCP 侦听器，负载均衡器会将代理协议标头预添加到 TCP 数据中。它不会丢弃或覆盖任何现有数据，包括客户端或网络路径中的任何其他代理、负载均衡器或服务器发送的任何传入代理协议标头。因此，可以接收多个代理协议标头。此外，如果您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负载均衡器中的标头。

TLS 侦听器不支持带有客户端或任何其他代理发送的代理协议标头的传入连接。

QUIC 流量不支持代理协议版本 2。

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

- TCP 和 TLS：默认情况下，已禁用客户端 IP 保留，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。要保留客户端的 IP 地址，请确保目标位于同一 VPC 或对等 VPC 内，并启用客户端 IP 保留。如果您需要客户端的 IP 地址并且不满足这些条件，请启用代理协议并从代理协议标头获取客户端 IP 地址。
- UDP 和 TCP_UDP：源 IP 地址是客户端的 IP 地址，因为默认情况下，将为这些协议启用客户端 IP 保留，且无法禁用。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。

如果目标无法解析代理协议标头，则可能无法通过运行状况检查。例如，它们可能会返回以下错误：HTTP 400：错误请求。

VPC 端点服务

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

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

字段	长度 (8 位字节)	描述
Type	1	PP2_TYPE_AWS (0xEA)
Length	2	值的长度
值	1	PP2_SUBTYPE AWS_VPCE_ID _ (0x01)
	可变 (值长度减 1)	终端节点的 ID

有关解析 TLV 类型 0xEA 的示例，请参见/。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。

Console

要启用代理协议版本 2

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

AWS CLI

要启用代理协议版本 2

使用带 `proxy_protocol_v2.enabled` 属性的 modify-target-group-attributes 命令。

```
aws elbv2 modify-target-group-attributes \
```

```
    --target-group-arn target-group-arn \
    --attributes "Key=proxy_protocol_v2.enabled,Value=true"
```

CloudFormation

要启用代理协议版本 2

更新AWS::ElasticLoadBalancingV2::TargetGroup 资源以包含该proxy_protocol_v2.enabled属性。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "proxy_protocol_v2.enabled"
          Value: "true"
```

粘性会话

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

注意事项

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

Console

要启用粘性会话

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

AWS CLI

要启用粘性会话

使用带 `stickiness.enabled` 属性的 modify-target-group-attributes 命令。

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=stickiness.enabled,Value=true"
```

CloudFormation

要启用粘性会话

更新AWS::ElasticLoadBalancingV2::TargetGroup 资源以包含该`stickiness.enabled`属性。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "stickiness.enabled"
          Value: "true"
```

目标组的跨区域负载均衡

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

对于网络负载均衡器，跨区域负载均衡在负载均衡器层级默认处于禁用状态，但您可随时启用它。对于目标组，默认使用负载均衡器设置，但您可以通过在目标组级别上明确启用或禁用跨区域负载均衡来覆盖默认设置。

注意事项

- 为网络负载均衡器启用跨区域负载均衡后，将收取 EC2 数据传输费用。有关更多信息，请参阅《AWS 数据导出用户指南》中的了解数据传输费用
- 目标组设置将决定目标组的负载均衡行为。例如，假设启用了负载均衡器级别的跨区域负载均衡，并禁用了目标组级别的跨区域负载均衡，则发送到目标组的流量不会进行跨区域路由。
- 禁用跨区域负载平衡时，请确保每个负载均衡器的区域中都有足够的目标容量，以便每个区域都能够为其关联的工作负载提供服务。
- 禁用跨区域负载平衡时，请确保所有目标组均参与到相同的可用区中。空的可用区被视为运行状况不佳。
- 如果目标组类型为 `instance` 或 `ip`，您可以启用或禁用目标组级别的跨区域负载均衡。如果目标组类型为 `alb`，则目标组始终从负载均衡器继承跨区域负载均衡设置。

有关在负载均衡器级别上启用跨区域负载均衡的更多信息，请参阅 the section called “跨可用区负载均衡”。

Console

要启用目标组的跨区域负载均衡

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

6. 选择保存更改。

AWS CLI

要启用目标组的跨区域负载均衡

使用带 `load_balancing.cross_zone.enabled` 属性的 modify-target-group-attributes 命令。

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

要启用目标组的跨区域负载均衡

更新AWS::ElasticLoadBalancingV2::TargetGroup 资源以包含该`load_balancing.cross_zone.enabled`属性。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "load_balancing.cross_zone.enabled"
          Value: "true"
```

运行状况不佳的目标的连接终止

默认情况下启用连接终止。当网络负载均衡器的目标未通过配置的运行状况检查并且被认为运行状况不佳时，负载均衡器会终止已建立的连接，并停止将新连接路由到目标。在禁用连接终止的情况下，目标仍被视为运行状况不佳且不接受新连接，但已建立的连接保持活动状态，允许它们正常关闭。

针对运行状况不佳的目标的连接终止，在目标组级别上进行配置。

Console

要修改连接终止属性

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Attributes（属性）选项卡上，选择 Edit（编辑）。
5. 在目标运行状况不佳状态管理下，选择当目标变得运行状况不佳时终止连接已启用还是已禁用。
6. 选择保存更改。

AWS CLI

要禁用连接终止属性

使用带 `target_health_state.unhealthy.connection_termination.enabled` 属性的 modify-target-group-attributes 命令。

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes
 "Key=target_health_state.unhealthy.connection_termination.enabled,Value=false"
```

CloudFormation

要禁用连接终止属性

更新AWS::ElasticLoadBalancingV2::TargetGroup 资源以包含该`target_health_state.unhealthy.connection_termination.enabled`属性。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
```

```
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_health_state.unhealthy.connection_termination.enabled"
          Value: "false"
```

运行状况不佳的耗尽间隔

将处于 unhealthy.draining 状态的目标视为运行状况不佳，不会接收新连接，但在配置的间隔内保留已建立的连接。运行状况不佳的连接间隔确定了目标在状态变为 unhealthy 之前保持 unhealthy.draining 状态的时间。如果目标在运行状况不佳的连接间隔期间通过运行状况检查，则其状态将再次变为 healthy。如果触发取消注册，则目标状态变为 draining，且取消注册延迟超时开始。

要求

在启用运行状况不佳的耗尽间隔之前，必须先禁用连接终止。

Console

要修改运行状况不佳的耗尽间隔

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在 Attributes（属性）选项卡上，选择 Edit（编辑）。
5. 在目标运行状况不佳状态管理下，确保已关闭当目标变得运行状况不佳时终止连接。
6. 为运行状况不佳的耗尽间隔输入一个值。
7. 选择保存更改。

AWS CLI

要修改运行状况不佳的耗尽间隔

使用带 target_health_state.unhealthy.draining_interval_seconds 属性的 modify-target-group-attributes 命令。

```
aws elbv2 modify-target-group-attributes \
```

```
    --target-group-arn target-group-arn \
    --attributes
 "Key=target_health_state.unhealthy.draining_interval_seconds,Value=60"
```

CloudFormation

要修改运行状况不佳的耗尽间隔

更新AWS::ElasticLoadBalancingV2::TargetGroup 资源以包含该target_health_state.unhealthy.draining_interval_seconds属性。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_health_state.unhealthy.draining_interval_seconds"
          Value: "60"
```

为网络负载均衡器注册目标

当您的目标准备好处理请求时，您将其注册到一个或多个目标组。目标组的目标类型将确定如何注册目标。例如，您可以注册实例 IDs、IP 地址或 Application Load Balancer。只要注册过程完成且目标通过初始运行状况检查，网络负载均衡器就会开始将请求路由至目标。完成注册过程和开始运行状况检查可能需要几分钟时间。有关更多信息，请参阅 网络负载均衡器目标组的运行状况检查。

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

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

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

内容

目标安全组

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

对目标安全组的建议（如果负载均衡器有与之关联的安全组）

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

对目标安全组的建议（如果负载均衡器没有与安全组关联）

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

客户端 IP 保留的工作原理

除非将 `preserve_client_ip.enabled` 属性设置为 `true`，否则网络负载均衡器不会保留客户端 IP 地址。此外，使用双栈网络负载均衡器，在将地址转换为地址或 IPv6 转换为地址时 IPv6，客户端 IP IPv4 地址保留不起作用。 IPv4 只有当客户端 IP 地址和目标 IP 地址同时存在 IPv4 或两者兼而有时，客户端 IP 地址保留才有效 IPv6。

使用控制台查找负载均衡器私有 IP 地址

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择 Network Interfaces。
3. 在搜索字段中，输入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. 在每个网络接口的详细信息选项卡上，从私有地址复制 IPv4 地址。

有关更多信息，请参阅 更新网络负载均衡器的安全组。

网络 ACLs

将 EC2 实例注册为目标时，必须确保您的实例子网的网络 ACLs允许侦听器端口和运行状况检查端口上的流量。VPC 的默认网络访问控制列表 (ACL) 允许所有入站和出站流量。如果您创建自定义网络 ACLs，请确认它们允许适当的流量。

与您的实例子网 ACLs 关联的网络必须允许面向 Internet 的负载均衡器的以下流量。

实例子网的推荐规则

Inbound

源	协议	端口范围	评论
Client IP addresses	*listener*	*target port*	允许客户端流量（IP 保留：ON）
VPC CIDR	*listener*	*target port*	允许客户端流量（IP 保留：OFF）
VPC CIDR	*health check*	*health check*	允许运行状况检查流量

Outbound

目标位置	协议	端口范围	评论

Client IP addresses	*listener*	1024-65535	允许向客户端返回流量（IP 保留:0N）
VPC CIDR	*listener*	1024-65535	允许向客户端返回流量（IP 保留:0FF）
VPC CIDR	*health check*	1024-65535	允许运行状况检查流量

与您的负载均衡器子网 ACLs 关联的网络必须允许面向 Internet 的负载均衡器传输以下流量。

负载均衡器子网的推荐规则

Inbound

源	协议	端口范围	评论
Client IP addresses	*listener*	*listener*	允许客户端流量
VPC CIDR	*listener*	1024-65535	允许来自目标的响应
VPC CIDR	*health check*	1024-65535	允许运行状况检查流量

Outbound

目标位置	协议	端口范围	评论
Client IP addresses	*listener*	1024-65535	允许回复客户端
VPC CIDR	*listener*	*target port*	允许向目标发出请求
VPC CIDR	*health check*	*health check*	允许对目标进行运行状况检查

对于内部负载均衡器，您的实例和负载均衡器节点的子网网络 ACLs 必须允许通过侦听器端口和临时端口进出VPC CIDR的入站和出站流量。

共享子网

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

所有 AWS 区域都支持网络负载均衡器的共享子网，但不包括：

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

注册目标

每个目标组在为负载均衡器启用的每个可用区中必须至少有一个已注册目标。

目标组的目标类型决定了您可以注册的目标类型。有关更多信息，请参阅 Target type。使用以下信息将目标注册到类型为 instance 或 ip 的目标组中。如果目标类型为 alb，请参阅 使用应用程序负载均衡器作为目标。

要求和注意事项

- 当您注册实例时，实例必须处于 running 状态。
- 如果实例使用以下实例类型之一，则无法按实例 ID 注册实例：C1、、、、、 CC1 CC2、G1 CG1 CG2、G2 CR1、、、、M1 HI1、M2 HS1、M3 或 T1。
- 按实例 ID 注册目标时，实例必须与网络负载均衡器位于同一个 VPC 中。如果实例所在的 VPC 与负载均衡器 VPC 是对等的（位于同一区域或不同区域），则不能按实例 ID 注册实例。可以用 IP 地址注册这些实例。
- 按实例 ID 为 IPv6 目标组注册目标时，必须为目标分配主 IPv6 地址。要了解更多信息，请参阅 Amazon EC2 用户指南中的 IPv6 地址
- 按 IP 地址为 IPv4 目标组注册目标时，您注册的 IP 地址必须来自以下 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)

- 按照 IP 地址为 IPv6 目标组注册目标时，您注册的 IP 地址必须位于 VPC IPv6 CIDR 块内或对等 VPC 的 IPv6 CIDR 块内。
- 如果您按 IP 地址注册目标，并且该 IP 地址与负载均衡器位于同一 VPC 中，则负载均衡器会验证其是否来自可以访问的子网。
- 对于 UDP、TCP_UDP、QUIC 和 TCP_QUIC 目标组，如果实例位于负载均衡器 VPC 之外或使用以下实例类型之一：C1、、、、、、G1、G2、、、、、、M1、M2 CC1 CC2 CG1 CG2 CR1、M3 或 T1，则不要按 IP 地址注册实例。 HI1 HS1如果目标驻留在负载均衡器 VPC 之外或者采用不受支持的实例类型，则目标可能能够接收来自负载均衡器的流量，但随后无法响应。

QUIC 特定要求和注意事项

- 注册到 QUIC 或 TCP_QUIC 目标组的所有目标都必须指定服务器 ID。
- 对于存在于 Network Load Balancer 侦听器中的所有目标，服务器 IDs 必须是唯一的。
- QUIC 服务器始终 IDs 为 8 个字节。在注册目标时，服务器 ID 必须采用 `0x` 后接 16 位十六进制字符的格式。
- 使用服务器 ID 注册目标后，该 ID 将不可更改。要更改目标的服务器 ID，必须先将其取消注册，然后再使用新的服务器 ID 进行注册。
- 目标标识符和端口组合必须具有一个服务器 ID。在同一 VPC 内，不支持为相同的 IP 或实例 ID 与端口组合使用不同的服务器 ID。
- 避免在 6 小时内为不同的目标重复使用相同的服务器 ID。

Console

要注册目标

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 选择目标选项卡。
5. 选择注册目标。
6. 如果目标组的目标类型是 `instance`，则选择可用的实例，根据需要覆盖默认端口，然后选择在下面以待注册的形式添加。
7. 若目标组的目标类型为 `ip`，则需为每个 IP 地址选择网络，输入 IP 地址及端口，并选择在下面以待注册的形式添加。

8. 如果目标组的目标类型为 alb，则根据需要覆盖默认端口，然后选择应用程序负载均衡器。有关更多信息，请参阅 使用应用程序负载均衡器作为目标。
9. 如果目标组的协议为 QUIC 或 TCP_QUIC，请确保服务器 ID 已指定。
10. 选择注册待处理目标。

AWS CLI

要注册目标

使用 register-targets 命令。以下示例通过实例 ID 注册目标。由于未指定端口，负载均衡器将使用目标组端口。

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

以下示例通过 IP 地址注册目标。由于未指定端口，负载均衡器将使用目标组端口。

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=10.0.50.10 Id=10.0.50.20
```

以下示例将应用程序负载均衡器注册为目标。

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=application-load-balancer-arn
```

以下示例将目标注册到 QUIC 或 TCP_QUIC 目标组中。

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=10.0.50.10,QuicServerId=0xa1b2c3d4e5f65890
 Id=10.0.50.20,QuicServerId=0xa1b2c3d4e5f65999
```

CloudFormation

要注册目标

更新AWS::ElasticLoadBalancingV2::TargetGroup资源以包含新目标。以下示例通过实例 ID 注册两个目标。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: HTTP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      Targets:
        - Id: !GetAtt Instance1.InstanceId
          Port: 80
        - Id: !GetAtt Instance2.InstanceId
          Port: 80
```

以下示例通过实例 ID 将两个目标注册到 QUIC 或 TCP_QUIC 协议目标组中。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: HTTP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      Targets:
        - Id: !GetAtt Instance1.InstanceId
          Port: 80
          QuicServerId: 0xa1b2c3d4e5f65999
        - Id: !GetAtt Instance2.InstanceId
          Port: 80
          QuicServerId: 0xa1b2c3d4e5f65000
```

取消注册目标

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。

Console

要取消注册目标

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组的名称以打开其详细信息页面。
4. 在目标选项卡中，选择要删除的目标。
5. 选择注销。

AWS CLI

要取消注册目标

使用 deregister-targets 命令。以下示例取消注册两个通过实例 ID 注册的目标。

```
aws elbv2 deregister-targets \
    --target-group-arn target-group-arn \
    --targets Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

将应用程序负载均衡器作为网络负载均衡器的目标

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

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

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

注意事项

- 每个目标组只能注册一个应用程序负载均衡器。
- 要将应用程序负载均衡器关联为网络负载均衡器的目标，这些负载均衡器必须位于同一账户内的同一 VPC 中。
- 您可以将应用程序负载均衡器关联为最多两个网络负载均衡器的目标。为此，使用单独的目标组为每个网络负载均衡器注册应用程序负载均衡器。
- 您使用网络负载均衡器注册的每个应用程序负载均衡器会将每个网络负载均衡器在每个可用区的最大目标数减少 50 个。您可以在这两个负载均衡器中禁用跨区域负载均衡，以尽量减少延迟并避免区域数据传输费用。有关更多信息，请参阅 网络负载均衡器的配额。
- 当目标组类型为 `alb` 时，您无法修改目标组属性。这些属性始终使用其默认值。
- 注册应用程序负载均衡器作为目标，只有从所有目标组中取消注册此应用程序负载均衡器才能将其删除。
- Network Load Balancer 和 Application Load Balancer 之间的通信始终使用 IPv4。

任务

- 先决条件
- 步骤 1：创建 alb 类型的目标组
- 步骤 2：创建网络负载均衡器并配置路由
- 步骤 3：（可选）创建 VPC 终端节点服务

先决条件

如果您还没有可用作目标的应用程序负载均衡器，请创建负载均衡器、其侦听器以及其目标组。有关更多信息，请参阅《应用程序负载均衡器用户指南》中的创建应用程序负载均衡器。

步骤 1：创建 alb 类型的目标组

创建 `alb` 类型的目标组。您可以在创建目标组时或创建之后，将您的应用程序负载均衡器注册为目标。

Console

要为作为目标的应用程序负载均衡器创建目标组

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格上的 Load Balancing (负载均衡) 下，选择 Target Groups (目标组)。
3. 选择 Create target group (创建目标组)。
4. 在基本配置窗格中，对于选择目标类型，请选择应用程序负载均衡器。
5. 对于目标组名称，输入目标组的名称。
6. 对于 Protocol (协议)，只允许 TCP。为您的目标组选择 Port (端口)。此目标组的端口必须与应用程序负载均衡器的侦听器端口匹配。如果您为该目标组选择了其他端口，则可以更新应用程序负载均衡器上的侦听器端口，以使其匹配。
7. 对于 VPC，请为目标组选择虚拟私有云（VPC）。这必须与应用程序负载均衡器所使用的 VPC 相同。
8. 对于运行状况检查，选择 HTTP 或 HTTPS 作为运行状况检查协议。运行状况检查将发送到应用程序负载均衡器并使用指定的端口、协议和 ping 路径转发到其目标。确保应用程序负载均衡器可以通过侦听器来接收这些运行状况检查结果，该侦听器的端口和协议与运行状况检查端口和协议匹配。
9. （可选）展开标签。对于每个标签，请选择添加新标签，然后输入标签键和标签值。
10. 选择下一步。
11. 如果您已经准备号注册应用程序负载均衡器，请选择立即注册，根据需要覆盖默认端口，然后选择应用程序负载均衡器。应用程序负载均衡器必须在与目标组相同的端口上配置侦听器。您可以在此负载均衡器上添加或编辑侦听器以匹配目标组的端口，或返回上一步并更改目标组的端口。

    如果您尚未准备好将应用程序负载均衡器注册为目标，请选择稍后注册，以便稍后再进行目标注册。有关更多信息，请参阅 the section called “注册目标”。
12. 选择创建目标组。

AWS CLI

创建 alb 类型的目标组

使用 create-target-group 命令。协议必须为 TCP，并且端口必须与应用程序负载均衡器的侦听器端口匹配。

```
aws elbv2 create-target-group \
    --name my-target-group \
    --protocol TCP \
    --port 80 \
    --target-type alb \
    --vpc-id vpc-1234567890abcdef0 \
    --tags Key=department,Value=123
```

CloudFormation

要创建 alb 类型的目标组

定义类型为的资源AWS::ElasticLoadBalancingV2::TargetGroup。协议必须为 TCP，并且端口必须与应用程序负载均衡器的侦听器端口匹配。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: alb
      VpcId: !Ref myVPC
      Tags:
        - Key: 'department'
          Value: '123'
      Targets:
        - Id: !Ref myApplicationLoadBalancer
          Port: 80
```

步骤 2：创建网络负载均衡器并配置路由

创建网络负载均衡器时，您可以将默认操作配置为将流量转发到应用程序负载均衡器。

Console

要创建网络负载均衡器

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格上的 Load Balancing（负载均衡）下，选择 Load Balancers（负载均衡器）。

3. 选择创建负载均衡器。
4. 在网络负载均衡器下，选择创建。
5. 基本配置

   a. 对于负载均衡器名称，输入网络负载均衡器的名称。

   b. 对于 Scheme (方案)，选择互联网-facing (面向互联网) 或 Internal (内部)。面向互联网的网络负载均衡器将来自客户端的请求通过互联网路由到目标。内部网络负载均衡器使用私有 IP 地址将请求路由到目标。

   c. 对于负载均衡器 IP 地址类型，请选择IPv4您的客户端是使用 IPv4 地址与网络负载均衡器通信，如果您的客户端同时使用 IPv4 和 IPv6 地址与网络负载均衡器通信，则选择双栈通信。
6. 网络映射

   a. 对于 VPC，请选择您用于应用程序负载均衡器的相同 VPC。对于面向互联网的负载均衡器，只能选择 VPCs 带有互联网网关的负载均衡器。

   b. 对于可用区和子网，请至少选择一个可用区，然后为每个区域选择一个子网。我们建议您选择与应用程序负载均衡器所启用的可用区相同的可用区。这有助于优化可用性、扩展性和性能。

      （可选）要使用静态 IP 地址，请在每个可用区的IPv4设置中选择使用弹性 IP 地址。使用静态 IP 地址，您可以将某些 IP 地址添加到防火墙允许列表中，也可以对客户端进行 IP 地址硬编码。
7. 安全组

   我们会为负载均衡器 VPC 预选默认安全组。您可以根据需要选择其他安全组。如果您没有可满足您需求的安全组，请选择创建新的安全组，以立即创建一个。有关更多信息，请参阅《Amazon VPC 用户指南》中的创建安全组。

   > **Warning**
   >
   > 如果您现在没有将任何安全组与网络负载均衡器关联，则无法以后再将其关联。

   > **Warning**
   >
   > 要使用 QUIC 或 TCP_QUIC 侦听器，您的网络负载均衡器必须没有安全组。

8. 侦听器和路由

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

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

   b. 对于默认操作，请选择您在之前步骤中创建的目标组。

   c. （可选）选择添加侦听器标签，然后输入标签键和标签值。

9. 负载均衡器标签

   （可选）展开负载均衡器标签。（可选）选择添加新的标签，然后输入标签键和标签值。有关更多信息，请参阅标签。

10. 摘要

    查看您的配置，然后选择创建负载均衡器。

AWS CLI

要创建网络负载均衡器

使用 create-load-balancer 命令。我们建议您使用与应用程序负载均衡器所启用的可用区相同的可用区。

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --scheme internal \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

要添加 TCP 侦听器

使用 create-listener 命令来添加 TCP 侦听器。只有 TCP 侦听器才能将流量转发到应用程序负载均衡器。对于默认操作，请使用您在之前步骤中创建的目标组。

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

```
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

CloudFormation

要创建网络负载均衡器

定义类型为的资源AWS::ElasticLoadBalancingV2::LoadBalancer和类型的资源AWS::ElasticLoadBalancingV2::Listener。只有 TCP 侦听器才能将流量转发到应用程序负载均衡器。对于默认操作，请使用您在之前步骤中创建的目标组。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-load-balancer
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup

  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

步骤 3：（可选）创建 VPC 终端节点服务

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

要使用您的网络负载均衡器创建 VPC 端点服务

1. 在导航窗格中，选择负载均衡器。

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

为网络负载均衡器标记目标组

标签有助于按各种标准 (例如，用途、所有者或环境) 对目标组进行分类。

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

用完标签后可以将其删除。

限制

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

Console

要管理目标组的标签

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

5. 选择保存更改。

AWS CLI

添加 标签

使用 add-tags 命令。以下示例将添加两个标签。

```
aws elbv2 add-tags \
    --resource-arns target-group-arn \
    --tags "Key=project,value=lima" "Key=department,Value=digital-media"
```

删除标签

使用 remove-tags 命令。以下示例将移除具有指定键的标签。

```
aws elbv2 remove-tags \
    --resource-arns target-group-arn \
    --tag-keys project department
```

CloudFormation

添加 标签

更新AWS::ElasticLoadBalancingV2::TargetGroup资源以包含该Tags属性。

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

删除网络负载均衡器的目标组

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。

Console

删除目标组

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格上的负载均衡下，选择目标组。
3. 选择目标组，然后依次选择操作、删除。
4. 选择删除。

AWS CLI

删除目标组

使用 delete-target-group 命令。

```
aws elbv2 delete-target-group \
    --target-group-arn target-group-arn
```

监控 Network Load Balancer

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

CloudWatch 指标

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

VPC 流日志

您可以使用 VPC 流日志来捕获有关往来于您的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。如果目标组的客户端 IP 保留属性已启用，连接将作为来自客户端的连接向实例显示。否则，连接的源 IP 是负载均衡器的私有 IP 地址。如果实例的安全组不允许来自客户端的连接，但负载均衡器子网的网络 ACLs 允许这些连接，则负载均衡器的网络接口日志将显示前端和后端连接的 “接受确定”，而实例网络接口的日志显示该连接的 “拒绝确定”。

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

Amazon CloudWatch 互联网监视器

您可以使用 Internet Monitor 来了解互联网问题如何影响托管在上的应用程序与最终用户之间的性能 AWS 和可用性。您还可以近乎实时地探索如何通过切换到使用其他服务或通过其他服务将流量重新路由到您的工作负载，来改善应用程序的预计延迟。 AWS 区域有关更多信息，请参阅使用 Amazon CloudWatch 互联网监视器。

访问日志

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

CloudTrail 日志

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

CloudWatch 您的 Network Load Balancer 的指标

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

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

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

有关更多信息，请参阅 Amazon CloudWatch 用户指南。

内容

网络负载均衡器指标

AWS/NetworkELB 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。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：始终报告。 统计数据：最有用的统计工具是 Average、Maximum 和 Minimum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer • TargetGroup
ActiveFlowCount_TCP	客户端至目标的并发 TCP 流（或连接）的总数。此指标包含处于 SYN_SENT 和 ESTABLISHED 状态的连接。TCP 连接未在负载均衡器上终止，因此，一个开放与目标的 TCP 连接的客户端将计为一个流。 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。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer • TargetGroup
ActiveFlowCount_TLS	客户端至目标的并发 TLS 流（或连接）的总数。此指标包含处于 SYN_SENT 和 ESTABLISHED 状态的连接。 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。

指标	描述
	Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer • TargetGroup
ActiveFlowCount_UDP	客户端至目标的并发 UDP 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 Average、Maximum 和 Minimum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer • TargetGroup
ActiveZonalShiftHostCount	当前积极参与可用区转移的目标数量。 报告标准：当负载均衡器选择加入可用区转移时报告。 统计数据：最有用的统计数据为 Maximum 和 Minimum。 Dimensions • LoadBalancer ，TargetGroup • AvailabilityZone ，LoadBalancer ，TargetGroup
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。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer

指标	描述
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 LCUs 的使用量付费。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
ConsumedLCUs_TCP	负载均衡器为 TCP 使用的负载均衡器容量单位 (LCU) 数量。您需要为每小时 LCUs 的使用量付费。有关更多信息，请参阅 Elastic Load Balancing 定价。 报告标准：有非零值。 统计数据：全部 Dimensions • LoadBalancer
ConsumedLCUs_TLS	负载均衡器为 TLS 使用的负载均衡器容量单位 (LCU) 数量。您需要为每小时 LCUs 的使用量付费。有关更多信息，请参阅 Elastic Load Balancing 定价。 报告标准：有非零值。 统计数据：全部 Dimensions • LoadBalancer

指标	描述
ConsumedLCUs_UDP	负载均衡器为 UDP 使用的负载均衡器容量单位 (LCU) 数量。您需要为每小时 LCUs 的使用量付费。有关更多信息，请参阅 Elastic Load Balancing 定价。 报告标准：有非零值。 统计数据：全部 Dimensions • LoadBalancer
HealthyHostCount	被视为正常运行的目标数量。此指标不包括注册为目标的任何应用程序负载均衡器。 报告标准：在有注册目标时报告。 统计数据：最有用的统计工具为 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：始终报告。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer • TargetGroup

指标	描述
NewFlowCount_TCP	时段内建立的客户端至目标的新 TCP 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 • TargetGroup
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。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer • TargetGroup
NewFlowCount_UDP	时段内建立的客户端至目标的新 UDP 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 • TargetGroup

指标	描述
NewFlowCount_QUIC	该时间段内需要做出路由决策的 UDP 数据报总数。 报告标准：有非零值。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
PeakBytesPerSecond	每秒处理字节数的最高平均值，在采样窗口内每 10 秒计算一次。此指标不包含运行状况检查流量。 报告标准：始终报告 Statistics：最有用的统计工具是 Maximum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
PeakPacketsPerSecond	最高平均数据包速率（每秒处理的数据包数），在采样窗口期间每 10 秒计算一次。此指标包含运行状况检查流量。 报告标准：始终报告。 Statistics：最有用的统计工具是 Maximum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer

指标	描述
PortAllocationErrorCount	客户端 IP 转换操作期间临时端口分配错误的总数。非零值表示断开的客户端连接。 注意：当执行客户端地址转换时，网络负载均衡器支持与每个唯一目标（IP 地址和端口）的 55,000 个并发连接或每分钟约 55,000 个连接。要修复端口分配错误，请将更多目标添加到目标组。 报告标准：始终报告。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
ProcessedBytes	负载均衡器处理的总字节数，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：始终报告。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
ProcessedBytes_TCP	TCP 侦听器处理的字节的总数。 报告标准：有非零值。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer

指标	描述
ProcessedBytes_TLS	TLS 侦听器处理的字节的总数。 报告标准：有非零值。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
ProcessedBytes_UDP	UDP 侦听器处理的字节的总数。 报告标准：有非零值 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
ProcessedBytes_QUIC	QUIC 侦听器处理的字节的总数。 报告标准：有非零值 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer

指标	描述
ProcessedPackets	负载均衡器处理的总数据包数。此计数包含往返目标的流量，以及运行状况检查流量。 报告标准：始终报告。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
RejectedFlowCount	遭负载均衡器拒绝的流量（或连接）的总数。 报告标准：始终报告。 统计数据：最有用的统计工具是 Average、Maximum 和 Minimum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
RejectedFlowCount_TCP	遭负载均衡器拒绝的 TCP 流量（或连接）的数量。 报告标准：有非零值。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer

指标	描述
ReservedLCUs	使用 LCU 预留为您的负载均衡器预留的负载均衡器容量单位数 (LCUs)。 报告标准：有非零值 统计数据：全部 Dimensions • LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_ICMP	被负载均衡器安全组的入站规则拒绝的新 ICMP 消息的数量。 报告标准：有非零值。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_TCP	被负载均衡器安全组的入站规则拒绝的新 TCP 流的数量。 报告标准：有非零值。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer

指标	描述
SecurityGroupBlockedFlowCount_Inbound_UDP	被负载均衡器安全组的入站规则拒绝的新 UDP 流的数量。 报告标准：有非零值。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_ICMP	被负载均衡器安全组的出站规则拒绝的新 ICMP 消息的数量。 报告标准：有非零值。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_TCP	被负载均衡器安全组的出站规则拒绝的新 TCP 流的数量。 报告标准：有非零值。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer

指标	描述
SecurityGroupBlockedFlowCount_Outbound_UDP	被负载均衡器安全组的出站规则拒绝的新 UDP 流的数量。 报告标准：有非零值。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
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。 Statistics：最有用的统计工具是 Sum。 Dimensions • 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：始终报告。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer

指标	描述
TCP_ELB_Reset_Count	负载均衡器生成的重置 (RST) 数据包的总数。有关更多信息，请参阅故障排除。 报告标准：始终报告。 Statistics：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：始终报告。 Statistics：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。此指标不包括注册为目标的任何应用程序负载均衡器。 报告标准：在有注册目标时报告。 统计数据：最有用的统计工具为 Maximum 和 Minimum。 Dimensions • LoadBalancer ，TargetGroup • AvailabilityZone ，LoadBalancer ，TargetGroup

指标	描述
UnhealthyRoutingFlowCount	使用路由失效转移操作（失败时开放）路由的流（或连接）数量。TLS 侦听器不支持此指标。 报告标准：有非零值。 Statistics：最有用的统计工具是 Sum。
ZonalHealthStatus	负载均衡器认为运行状况良好的可用区的数量。负载均衡器为每个运行状况良好的可用区发出“1”，为每个运行状况不良的可用区发出“0”。 报告标准：在启用了运行状况检查时报告。 统计数据：最有用的统计工具为 Maximum 和 Minimum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer
QUIC_Unknown_Server_ID_Packet_Drop_Count	丢弃的 UDP 数据报的数量，其中包含与网络负载均衡器中的目标无关的服务器 ID。 报告标准：仅针对 QUIC 侦听器进行报告。 Statistics：最有用的统计工具是 Sum。 Dimensions • LoadBalancer • AvailabilityZone ，LoadBalancer

网络负载均衡器的指标维度

要筛选负载均衡器的指标，请使用以下维度。

维度	描述
AvailabilityZone	按可用区筛选指标数据。
LoadBalancer	按负载均衡器筛选指标数据。按如下方式指定负载均衡器：net load-balancer-name/1234567890123456（负载均衡器 ARN 的最后一部分）。
TargetGroup	按目标组筛选指标数据。按如下方式指定目标组：targetgroup target-group-name/1234567890123456（目标组 ARN 的最后一部分）。

网络负载均衡器指标的统计数据

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

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

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

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

查看您的负载均衡器的 CloudWatch 指标

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

或者，您可以使用 CloudWatch 控制台查看负载均衡器的指标。

使用控制台查看指标

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

使用 CloudWatch 控制台查看指标

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

要查看指标，请使用 AWS CLI

使用以下 list-metrics 命令列出可用指标：

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

要获取指标的统计数据，请使用 AWS CLI

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

```
aws cloudwatch get-metric-statistics --namespace AWS/NetworkELB \
```

```
--metric-name UnHealthyHostCount --statistics Average  --period 3600 \
--dimensions Name=LoadBalancer,Value=net/my-load-balancer/50dc6c495c0c9188 \
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \
--start-time 2017-04-18T00:00:00Z --end-time 2017-04-21T00:00:00Z
```

下面是示例输出：

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

您的网络负载均衡器的访问日志

弹性负载均衡提供了访问日志，该访问日志可捕获有关使用网络负载均衡器建立的 TLS 连接的详细信息。您可以使用这些访问日志分析流量模式并解决问题。

> **Important**
>
> 虽然传统的“传统”访问日志（如本节所述）仍然可用，但 Network Load Balancer 现在通过 CloudWatch 日志提供了增强的日志记录选项。 CloudWatch 日志提供了更灵活的传输选项，包括发送到亚马逊 CloudWatch 日志、亚马逊数据 Firehose 和亚马逊简单存储服务。要配置这些改进的日志记录选项，请访问负载均衡器的集成选项卡。有关 CloudWatch 日志的更多信息，请参阅CloudWatch 你的 Network Load Balancer 的日志。

> **Important**
>
> 仅当负载均衡器具有 TLS 侦听器且日志仅包含有关 TLS 请求的信息时，才创建访问日志。访问日志将尽力记录请求。我们建议您使用访问日志来了解请求性质，而不是作为所有请求的完整描述。

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

您可以使用 Amazon S3 托管加密密钥（SSE-S3）启用服务器端加密，也可使用 Key Management Service 与 S3 存储桶的客户管理的密钥（SSE-KMS CMK）来启用服务器端加密。每个访问日志文件在存储到 S3 存储桶中之前将自动加密，并在您访问它时进行解密。您不需要执行任何操作，因为这与您访问加密的日志文件或未加密的日志文件的方式基本相同。每个日志文件都使用一个唯一密钥进行加密，此密钥本身将使用定期轮换的 KMS 密钥进行加密。有关更多信息，请参阅 Amazon S3 用户指南中的指定 Amazon S3 加密 (SSE-S3) 和使用 AWS KMS (SSE-KMS) 指定服务器端加密。

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

目录

访问日志文件

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

访问日志的文件名采用以下格式：

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

bucket

S3 存储桶的名称。

prefix

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

aws-account-id

所有者的 AWS 账户 身份证。

region

负载均衡器和 S3 存储桶所在的区域。

yyyy/mm/dd

传输日志的日期。

load-balancer-id

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

end-time

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

random-string

系统生成的随机字符串。

以下是示例日志文件名：

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

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

访问日志条目

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

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

字段	描述
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、tlsv12 和 tlsv13。如果 TLS 协商未完成，则此值设置为 -。
tls_keyex	TLS 或 PQ-TLS 握手期间使用的密钥交换。如果 TLS 或 PQ-TLS 协商未完成，则此值将设置为。-
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 -。
alpn_fe_protocol	与客户端协商的应用程序协议，采用字符串格式。可能的值为 h2、http/1.1和http/1.0。如果 TLS 侦听器中未配置 ALPN 策略、找不到匹配协议或者没有发送有效的协议列表，则此值设置为 -。
alpn_be_protocol	与目标协商的应用程序协议，采用字符串格式。可能的值为h2、http/1.1和http/1.0。如果 TLS 侦听器中未配置 ALPN 策略、找不到匹配协议或者没有发送有效的协议列表，则此值设置为 -。
alpn_client_preference_list	客户端 hello 消息中 application_layer_protocol_negotiation 扩展的值。此值是 URL 编码的。每个协议都用双引号括起来，协议用逗号分隔。如果在 TLS 侦听器中未配置 ALPN 策略、未发送有效的客户端 hello 消息或扩展名不存在，则此值设置为 -。字符串长度在超过 256 个字节时将会截断。
tls_connection_creation_time	在 TLS 连接开始时记录的时间（采用 ISO 8601 格式）。

示例日志条目

以下是示例日志条目。请注意，文本以多行形式显示只是为了更方便阅读。

以下是没有 ALPN 策略的 TLS 侦听器的示例。

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

以下是具有 ALPN 策略的 TLS 侦听器的示例。

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

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)。您可能无法使用处理来 line-by-line处理如此大量的数据。因此，您可能必须使用提供并行处理解决方案的分析工具。例如，您可以使用以下分析工具分析和处理访问日志：

- Amazon Athena 是一种交互式查询服务，让您能够轻松使用标准 SQL 分析 Amazon S3 中的数据。有关更多信息，请参阅《Amazon Athena 用户指南》中的查询网络负载均衡器日志。
- Loggly
- Splunk
- Sumo Logic

为网络负载均衡器启用访问日志

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。存储桶必须具有为 Elastic Load Balancing 授予写入存储桶的权限的存储桶策略。

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

存储桶要求

您可以使用现有存储桶，也可以创建专门用于访问日志的存储桶。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。该存储桶和负载均衡器可由不同的账户拥有。
- 您指定的前缀不得包含 AWSLogs。我们会在您指定的存储桶名称和前缀后添加以 AWSLogs 开头的文件名部分。
- 存储桶必须具有授予将访问日志写入存储桶的权限的存储桶策略。存储桶策略是 JSON 语句的集合，这些语句以访问策略语言编写，用于为存储桶定义访问权限。

存储桶策略的示例

以下是示例策略。对于Resource元素，请*amzn-s3-demo-destination-bucket*替换为访问日志的 S3 存储桶的名称。*Prefix/*如果您未使用存储桶前缀，请务必省略。对于aws:SourceAccount，请指定负载均衡器 AWS 账户的 ID。对于aws:SourceArn，将*region*和*012345678912*，分别替换为负载均衡器的区域和账户 ID。

JSON

```
{
    "Version":"2012-10-17",
    "Id": "AWSLogDeliveryWrite",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceAccount": [
                        "012345678912"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:012345678912:*"
                    ]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-
bucket/Prefix/AWSLogs/account-ID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": [
                        "012345678912"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:012345678912:*"
                    ]
                }
            }
        }
    ]
}
```

加密

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

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

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

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

密钥策略必须允许服务对日志进行加密和解密。以下是示例策略。

JSON

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

配置访问日志

使用以下过程配置访问日志，以捕获请求信息并将日志文件传输到 S3 存储桶。

Console

启用访问日志

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择负载均衡器。
3. 选择您的负载均衡器的名称以打开其详细信息页面。
4. 在属性选项卡上，选择编辑。
5. 对于监控，打开访问日志。
6. 对于 S3 URI，输入日志文件的 S3 URI。您指定的 URI 取决于您是否使用前缀。
   - 带有前缀的 URI: s3://*amzn-s3-demo-logging-bucket*/*logging-prefix*
   - 不带前缀的 URI: s3://*amzn-s3-demo-logging-bucket*
7. 选择保存更改。

AWS CLI

启用访问日志

使用带有相关属性的modify-load-balancer-attributes命令。

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes \
        Key=access_logs.s3.enabled,Value=true \
        Key=access_logs.s3.bucket,Value=amzn-s3-demo-logging-bucket \
        Key=access_logs.s3.prefix,Value=logging-prefix
```

CloudFormation

启用访问日志

更新AWS::ElasticLoadBalancingV2::LoadBalancer资源以包含相关属性。

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
```

```
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "access_logs.s3.enabled"
          Value: "true"
        - Key: "access_logs.s3.bucket"
          Value: "amzn-s3-demo-logging-bucket"
        - Key: "access_logs.s3.prefix"
          Value: "logging-prefix"
```

禁用网络负载均衡器的访问日志

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 S3 用户指南》中的创建、配置和使用 S3 存储桶。

Console

要禁用访问日志

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

AWS CLI

要禁用访问日志

使用 modify-load-balancer-attributes 命令。

```
aws elbv2 modify-load-balancer-attributes \
```

```
    --load-balancer-arn load-balancer-arn \
    --attributes Key=access_logs.s3.enabled,Value=false
```

排查您的网络负载均衡器问题

以下信息可帮助您排查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 网络负载均衡器目标组的运行状况检查。

验证您的实例是否通过运行状况检查，然后检查以下各项：

安全组不允许流量

与实例关联的安全组必须允许来自负载均衡器的使用运行状况检查端口和运行状况检查协议的流量。有关更多信息，请参阅 目标安全组。负载均衡器的安全组也必须允许流入实例的流量。有关更多信息，请参阅 更新网络负载均衡器的安全组。

网络访问控制列表 (ACL) 不允许流量

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

请求未路由至目标

检查以下各项：

安全组不允许流量

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

网络访问控制列表 (ACL) 不允许流量

与您的 VPC 子网 ACLs 关联的网络必须允许负载均衡器和目标在侦听器端口上进行双向通信。有关更多信息，请参阅 网络 ACLs。

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。

配置的服务器 ID 与目标上配置的 ID 不匹配

如果您使用的是 QUIC 侦听器，请确保在目标上配置的 ID 与在网络负载均衡器目标组中配置的 ID 相匹配。

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

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

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

由于主机标头不匹配，目标无法通过 HTTP 或 HTTPS 运行状况检查

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

无法将安全组与网络负载均衡器关联

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

无法删除所有安全组

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

TCP_ELB_Reset_Count 指标升高

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

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

从目标到其负载均衡器的请求连接超时

检查目标组是否启用了客户端 IP 保留。启用客户端 IP 保留后，不支持 NAT 环回（也称为发夹转换）。

如果实例是它注册到的负载均衡器的客户端，且它启用了客户端 IP 保留，则连接仅在请求路由到不同的实例时才会成功。如果请求路由到发送请求的同一个实例，连接会超时，因为源地址和目的地 IP 地址相同。请注意，这适用于在同一 EC2 Worker 节点实例中运行的 Amazon EKS 容器组（pod），即使它们的 IP 地址不同。

如果实例必须将请求发送到它注册到的负载均衡器，请执行下列操作之一：

- 禁用客户端 IP 保留。建议改用代理协议 v2 来获取客户端 IP 地址。
- 确保必须相互通信的容器位于不同的容器实例上。

当将目标移到网络负载均衡器时，性能会下降

经典负载均衡器和应用程序负载均衡器都使用多路复用连接，但网络负载均衡器不使用。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。

后端流端口分配错误

在 PrivateLink 流量或禁用客户端 IP 保留时，Network Load Balancer 支持与每个唯一目标（IP 地址和端口）的 55,000 个同步连接或每分钟大约 55,000 个连接。如果超过这些限制，则会增大出现端口分配错误的几率。您可以使用 `PortAllocationErrorCount` 指标来跟踪端口分配错误。您可以使用 `ActiveFlowCount` 指标来跟踪活跃的连接。有关更多信息，请参阅 CloudWatch 您的 Network Load Balancer 的指标。

要修复端口分配错误，我们建议您请将目标添加到目标组。

或者，如果您无法向目标组添加目标，则可以向负载平衡器网络接口最多添加 7 个辅助 IP 地址。辅助 IP 地址是从相应子网的 IPv4 CIDR 块中自动分配的。每个辅助 IP 地址消耗 6 个网络寻址单元。请注意，添加辅助 IP 地址后，您无法将其删除。释放辅助 IP 地址的唯一方法是删除负载均衡器。

TCP 连接建立间歇性失败或 TCP 连接建立延迟

启用“客户端 IP 地址保留”后，客户端可以使用相同的源临时端口连接到不同的目标 IP 地址。这些目标IP地址可以来自同一负载均衡器（位于不同可用区），前提是启用了跨区域负载均衡；或者来自不同的网络负载均衡器，但这些均衡器必须使用相同的注册目标 IP 地址和端口。在此情况下，如果这些连接被路由至相同的目标 IP 地址和端口，则目标将检测到重复连接，因为它们均来自相同的客户端 IP 地址和端口。在建立其中一个连接时，会导致连接错误和延迟。如果客户端前面有 NAT 设备，并且在同时连接到多个网络负载均衡器 IP 地址时分配相同的源 IP 地址和源端口，则经常发生这种情况。

您可以通过增加客户端或 NAT 设备分配的源临时端口的数量或增加负载均衡器的目标数来减少此类连接错误。我们建议客户端在连接失败后，进行重新连接时更改所使用的源端口。为了防止此类连接错误，如果您使用的是单个网络负载均衡器，则可以考虑禁用跨区域负载均衡，或者如果您使用的是多个网络负载均衡器，则可以考虑避免使用在多个目标组中注册的相同目标 IP 地址和端口。或者，您可以考虑禁用客户端 IP 保留。如果您需要客户端 IP，则可以使用代理协议 v2 进行检索。要了解有关代理协议 v2 的更多信息，请参阅 代理协议。

预置负载均衡器时可能出现故障

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

目标之间的流量分布不均匀

TCP 和 TLS 监听器负责路由 TCP 连接，而 UDP 侦听器则负责路由 UDP 流。负载均衡器使用流哈希算法来选择目标。来自客户端的单个连接本质上是粘性的。

如果您发现某些目标接收的流量似乎比其他目标要多，我们建议您查看 VPC 流日志。比较每个目标 IP 地址的唯一连接数。尽可能缩小时间窗口，因为目标注册、目标取消注册和运行状况不佳的目标会影响这些连接数。

以下是可能导致连接分配不均的情况：

- 若初始目标数量较少，后续又注册了更多目标，则原始目标仍会保留与客户端的连接。对于 HTTP 工作负载，keepalive 可确保客户端重复使用连接。如果您降低 Web 应用程序的最大 keepalives 数，则客户端将更频繁地建立新连接。
- 当启用“目标组粘性”时，若存在少量客户端且这些客户端通过具有单一源 IP 地址的 NAT 设备通信，则来自这些客户端的连接将被路由至同一目标。
- 如果“跨区域负载均衡”处于禁用状态，且客户端优先选择来自某个负载均衡器区域的 IP 地址，则连接将在负载均衡器区域之间分配不均。

DNS 名称解析包含的 IP 地址少于已启用的可用区

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

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

- 如果可用区 A 中的已注册目标实例运行状况不佳，则系统将从 DNS 中删除网络负载均衡器的可用区 A 的相应 IP 地址。
- 如果任意两个已启用的可用区没有运行正常的已注册目标实例，则系统将从 DNS 中删除网络负载均衡器的相应两个 IP 地址。

- 如果在所有已启用的可用区中都没有运行良好的注册目标实例，则会启用失效开放模式，DNS 将提供结果 AZs 中启用的三个 IP 地址中的所有 IP 地址。

IP 分段数据包不会路由到目标

网络负载均衡器不支持非 UDP 流量的 IP 分段数据包。

使用资源地图对运行状况不佳的目标进行故障排除

如果您的网络负载均衡器目标未通过运行状况检查，则可以使用资源地图查找运行状况不佳的目标并根据失败原因代码采取措施。有关更多信息，请参阅 查看网络负载均衡器资源地图。

资源地图提供了两个视图：概述和不正常目标地图。默认情况下，概览处于选中状态，并显示您的负载均衡器的所有资源。选择运行状况不佳的目标地图视图将仅显示与网络负载均衡器关联的每个目标组中运行状况不佳的目标。

> **Note**
>
> 必须启用显示资源详细信息才能查看资源地图内所有适用资源的运行状况检查摘要和错误消息。如果未启用，您必须选择每个资源才能查看其详细信息。

目标组列显示每个目标组的正常目标和不正常目标的摘要。这样可以帮助确定是所有目标都未通过运行状况检查，还是只有特定目标失败。如果目标组中的所有目标都未通过运行状况检查，则请检查目标组的运行状况检查设置。选择目标组的名称，以在新选项卡中打开详细信息页面。

目标列显示每个目标的 TargetID 和当前运行状况检查状态。当目标运行状况不佳时，将显示运行状况检查失败的原因代码。当单个目标未通过运行状况检查时，请验证该目标是否有足够的资源。选择目标的 ID，以在新选项卡中打开详细信息页面。

选择导出后，您可以选择将网络负载均衡器资源地图的当前视图导出为 PDF。

验证您的实例是否未通过运行状况检查，然后根据失败原因代码检查以下问题：

- 运行状况不佳：请求超时
  - 验证与您的目标和网络负载均衡器关联的安全组和网络访问控制列表（ACL）没有阻止连接。
  - 验证目标具有足够的可用容量来接受来自网络负载均衡器的连接。

- 在每个目标的应用程序日志中，可以查看网络负载均衡器的运行状况检查响应。有关更多信息，请参阅运行状况检查原因代码。

- 不健康： FailedHealthChecks
  - 验证目标正在侦听运行状况检查端口上的流量。

    使用 TLS 侦听器时

    您选择用于前端连接的安全策略。用于后端连接的安全策略是根据正在使用的前端安全策略自动选择的。如果你的听众有：

    - FIPS 后量子 TLS 策略-后端连接使用 ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09
    - FIPS 策略-后端连接使用 ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04
    - 后量子 TLS 策略-后端连接使用 ELBSecurityPolicy-TLS13-1-0-PQ-2025-09
    - TLS 1.3 政策-后端连接使用 ELBSecurityPolicy-TLS13-1-0-2021-06
    - 后端连接使用的所有其他 TLS 策略 ELBSecurityPolicy-2016-08

    有关更多信息，请参阅安全策略。

  - 验证目标是否以安全策略指定的正确格式提供了服务器证书和密钥。
  - 验证目标是否支持一个或多个匹配的密码，以及网络负载均衡器提供的用于建立 TLS 握手的协议。

网络负载均衡器的配额

您的每项 AWS 服务 AWS 账户 都有默认配额，以前称为限制。除非另有说明，否则，每个限额是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。

要查看网络负载均衡器的配额，请打开服务配额控制台。在导航窗格中，选择 AWS 服务，然后选择 Elastic Load Balancing（弹性负载均衡）。您也可以使用 describe-account-limits(AWS CLI) 命令进行 Elastic Load Balancing。

要请求提高配额，请参阅《服务配额用户指南》中的请求提高配额。如果配额在“服务配额”中尚不可用，请提交服务配额增加请求。

配额

- 负载均衡器
- 目标组
- 负载均衡器容量单位

负载均衡器

您 AWS 账户 有以下与网络负载均衡器相关的配额。

Name	默认值	可调整
每个网络负载均衡器的证书数	25	是
每个网络负载均衡器的侦听器数	50	不可以
ENIs 每个 VPC 的网络负载均衡器	1,200 [1]	是
每个区域的网络负载均衡器数	50	是
每个网络负载均衡器每个可用区的目标数	500 [2, 3]	是
每个网络负载均衡器的目标数	3,000 [3]	是

[1] 每个网络负载均衡器在每个区域使用一个网络接口。配额在 VPC 级别设置。共享子网或时 VPCs，使用量是按所有租户计算的。

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

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

目标组

以下配额适用于目标组。

Name	默认值	可调整
每个区域的目标组数	3,000 [1]	是
每个区域每个目标组的目标数（实例或 IP 地址）	1000	是
每个区域每个目标组的目标数（应用程序负载均衡器）	1	否

[1] 此配额由应用程序负载均衡器和网络负载均衡器共享。

负载均衡器容量单位

以下配额适用于 Load Balancer 容量单位 (LCUs)。

Name	默认值	可调整
每个可用区每个网络负载均衡器的预留网络负载均衡器容量单位 (LCUs)	45000	是
每个区域的预留网络负载均衡器容量单位 (LCU)	0	是

网络负载均衡器的文档历史记录

下表介绍了网络负载均衡器的版本。

变更	说明	日期
加权目标组	此版本增加了对带有加权目标组的默认操作的支持。	2025 年 11 月 19 日
QUIC 和 TCP_QUIC 协议支持	此版本增加了对 QUIC 和 TCP_QUIC 协议的支持。	2025 年 11 月 13 日
辅助 IPv4 地址	此版本增加了对向负载平衡器网络接口添加辅助 IPv4 地址的支持。	2025 年 7 月 29 日
禁用可用区	此版本增加了对禁用现有负载均衡器的可用区的支持。	2025 年 2 月 13 日
容量单位预留	此版本增加了对为负载均衡器设置最小容量的支持。	2024 年 11 月 20 日
双栈负载均衡器 IPv6 的 UDP 支持已结束	此版本允许客户端使用访问基于 UDP 的应用程序。 IPv6	2024 年 10 月 31 日
RSA 3072 位和 ECDSA 256/384/521 位证书	此版本增加了对 RSA 3072 位证书以及通过 (ACM) 进行的 Elliptic Curve 数字签名算法 (ECDSA) 256、384 和 521 位证书的支持。 AWS Certificate Manager	2024 年 1 月 19 日
FIPS 140-3 TLS 终止	此版本添加了在终止 TLS 连接时使用 FIPS 140-3 加密模块的安全策略。	2023 年 11 月 20 日
可用区 DNS 亲和性	此版本增加了相关支持，客户端可解析负载均衡器 DNS，以	2023 年 10 月 12 日

	接收其所在的同一可用区（AZ）中的 IP 地址。	
禁用运行状况不佳的目标连接终止	此版本增加了相关支持，可以保持与未通过运行状况检查的目标的活动连接。	2023 年 10 月 12 日
默认 UDP 连接终止	此版本增加了默认在取消注册超时结束时终止 UDP 连接的支持。	2023 年 10 月 12 日
使用注册目标 IPv6	此版本增加了对通过解决实例时将实例注册为目标的支持 IPv6。	2023 年 10 月 2 日
网络负载均衡器的安全组	此版本增加了支持功能，可在创建时将安全组与网络负载均衡器关联。	2023 年 8 月 10 日
目标组运行状况	此版本增加了对配置必须运行状况良好的目标数量下限或最低百分比以及在未达到阈值时负载均衡器采取哪些操作的支持。	2022 年 11 月 17 日
运行状况检查配置	此版本提供了对运行状况检查配置的改进。	2022 年 11 月 17 日
跨可用区负载均衡	此版本增加了对在目标组级别配置跨区域负载均衡的支持。	2022 年 11 月 17 日
IPv6 目标群体	此版本增加了对网络负载均衡器配置 IPv6 目标组的支持。	2021 年 11 月 23 日
IPv6 内部负载均衡器	此版本增加了对网络负载均衡器配置 IPv6 目标组的支持。	2021 年 11 月 23 日
TLS 1.3	此版本增加了支持 TLS 1.3 版的安全策略。	2021 年 10 月 14 日

作为目标的应用程序负载均衡器	此版本增加了对将应用程序负载均衡器配置为网络负载均衡器目标的支持。	2021 年 9 月 27 日
客户端 IP 保留	此版本增加了对配置客户端 IP 保留的支持。	2021 年 2 月 4 日
支持 TLS 1.2 版的 FS 安全策略	此版本增加了支持 TLS 1.2 版的向前保密 (FS) 安全策略。	2020 年 11 月 24 日
双堆栈模式	此版本增加了对双栈模式的支持，使客户端能够同时使用 IPv4 地址和 IPv6地址连接到负载均衡器。	2020 年 11 月 13 日
取消注册时连接终止	此版本增加了对取消注册超时结束后关闭取消注销目标连接的支持。	2020 年 11 月 13 日
ALPN 策略	此版本增加了对应用层协议协商 (ALPN) 首选项列表的支持。	2020 年 5 月 27 日
粘性会话	此版本根据源 IP 地址和协议增加了对粘性会话的支持。	2020 年 2 月 28 日
共享子网	此版本增加了对指定子网的支持，此类子网是由其他 AWS 账户与您所共享。	2019 年 11 月 26 日
私有 IP 地址	此版本允许您在为内部负载均衡器启用可用区时指定的子网 IPv4 地址范围提供私有 IP 地址。	2019 年 11 月 25 日
添加子网	此版本增加了在创建负载均衡器后启用其他可用区的支持。	2019 年 11 月 25 日

适用于 FS 的安全策略	此版本增加了对三个额外预定义向前保密安全策略的支持。	2019 年 10 月 8 日
SNI 支持	此版本增加了对服务器名称指示 (SNI) 的支持。	2019 年 9 月 12 日
UDP 协议	此版本增加了对 UDP 协议的支持。	2019 年 6 月 24 日
在新区域中可用	此版本增加了对亚太地区（大阪）区域中的网络负载均衡器的支持。	2019 年 6 月 12 日
TLS 协议	此版本增加了对 TLS 协议的支持。	2019 年 1 月 24 日
跨可用区负载均衡	此版本增加了对启用跨区域负载均衡的支持。	2018 年 2 月 22 日
代理协议	此版本增加了对启用代理协议的支持。	2017 年 11 月 17 日
IP 地址即目标	此版本增加了将 IP 地址注册为目标的支持。	2017 年 9 月 21 日
新负载均衡器类型	此版本的 Elastic Load Balancing 引入了网络负载均衡器。	2017 年 9 月 7 日

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