Elastic Load Balancing

用户指南

Elastic Load Balancing: 用户指南

Table of Contents

什么是 Elastic Load Balancing？ 1
负载均衡器优势 1
Elastic Load Balancing 的功能 1
访问 Elastic Load Balancing 1
相关服务 1
定价 2
Elastic Load Balancing 的工作原理 3
可用区与负载均衡器节点 3
跨区域负载均衡 3
请求路由选择 4
路由算法 5
HTTP 连接 5
HTTP 标头 6
HTTP 标头限制 6
负载均衡器模式 6
入门 7
创建 应用程序负载均衡器 7
创建 网络负载均衡器 7
创建 传统负载均衡器 7
安全性 8
数据保护 8
静态加密 9
传输中加密 9
Identity and Access Management 9
使用 IAM 策略授予权限 9
Elastic Load Balancing 的 API 操作 10
Elastic Load Balancing 资源 10
Elastic Load Balancing 的资源级权限 12
Elastic Load Balancing 的条件密钥 13
预定义的 AWS 托管策略 15
API 权限 15
服务相关角色 17
合规性验证 18
恢复功能 18
基础设施安全 19
网络隔离 19
控制网络流量 19
接口 VPC 终端节点 20
为 Elastic Load Balancing 创建接口终端节点 20
为 Elastic Load Balancing 创建 VPC 终端节点策略 20
迁移您的 传统负载均衡器 22
步骤 1：创建新负载均衡器 22
选项 1：使用迁移向导进行迁移 22
选项 2：使用负载均衡器复制实用程序进行迁移 23
选项 3：手动迁移 23
步骤 2：逐步将流量重定向到您的新负载均衡器 23
步骤 3：更新对您的 传统负载均衡器 的引用 24
步骤 4：删除 传统负载均衡器 24

什么是 Elastic Load Balancing？

Elastic Load Balancing 跨多个可用区中的多个目标（如 Amazon EC2 实例、容器和 IP 地址）分发传入应用程序或网络流量。Elastic Load Balancing 会在应用程序的传入流量随时间的推移发生更改时扩展负载均衡器。它可以自动扩展来处理绝大部分工作负载。

负载均衡器优势

负载均衡器跨多个计算资源 (如虚拟服务器) 分布工作负载。使用负载均衡器可提高您的应用程序的可用性和容错性。

可以根据需求变化在负载均衡器中添加和删除计算资源，而不会中断应用程序的整体请求流。

您可以配置运行状况检查，这些检查监控计算资源的运行状况，以便负载均衡器只将请求发送到正常运行的目标。此外，您可以将加密和解密的工作交给负载均衡器完成，以使您的计算资源能够专注于完成主要工作。

Elastic Load Balancing 的功能

Elastic Load Balancing 支持三种类型的负载均衡器：Application Load Balancer、Network Load Balancer 和 Classic Load Balancer。可以根据应用程序需求选择负载均衡器。有关更多信息，请参阅 Elastic Load Balancing 产品比较。

有关使用每种负载均衡器的更多信息，请参阅 Application Load Balancer 用户指南、Network Load Balancer 用户指南 和 Classic Load Balancer 用户指南。

访问 Elastic Load Balancing

可以使用以下任意接口创建、访问和管理负载均衡器：

- AWS 管理控制台— 提供您可用来访问 Elastic Load Balancing 的 Web 界面。
- AWS 命令行界面 (AWS CLI) — 为众多 AWS 服务（包括 Elastic Load Balancing）提供命令。AWS CLI 在 Windows、macOS 和 Linux 上受支持。有关更多信息，请参阅 AWS Command Line Interface。
- AWS 开发工具包 — 提供了特定于语言的 API，并关注许多连接详细信息，例如计算签名、处理请求重试和错误处理。有关更多信息，请参阅 AWS 开发工具包。
- 查询 API — 提供了您使用 HTTPS 请求调用的低级别 API 操作。使用查询 API 是访问 Elastic Load Balancing 的最直接方式。但是，查询 API 需要您的应用程序处理低级别的详细信息，例如生成哈希值以签署请求以及进行错误处理。有关更多信息，请参阅下列内容：
  - Application Load Balancer 和 Network Load Balancer — API 版本 2015-12-01
  - Classic Load Balancer — API 版本 2012-06-01

相关服务

Elastic Load Balancing 可与以下服务一起使用来提高应用程序的可用性和可扩展性。

- Amazon EC2 — 在云中运行应用程序的虚拟服务器。您可以将负载均衡器配置为将流量路由到您的 EC2 实例。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例） 或 Amazon EC2 用户指南（适用于 Windows 实例）。
- Amazon EC2 Auto Scaling — 确保运行所需数量的实例（即使实例失败也是如此）。Amazon EC2 Auto Scaling 还可让您根据实例需求的变化自动增加或减少实例数。如果使用 Elastic Load Balancing 启用 Auto Scaling，则 Auto Scaling 所启动的实例会自动注册到负载均衡器。同样，Auto Scaling 所终止的实例会自动从负载均衡器取消注册。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南。
- AWS Certificate Manager — 在创建 HTTPS 侦听器时，您必须指定由 ACM 提供的证书。负载均衡器使用证书终止连接并解密来自客户端的请求。
- Amazon CloudWatch — 使您能够监控负载均衡器并执行所需操作。有关更多信息，请参阅 Amazon CloudWatch 用户指南。
- Amazon ECS — 使您能够在 EC2 实例集群上运行、停止和管理 Docker 容器。您可以将负载均衡器配置为将流量路由到您的容器。有关更多信息，请参阅 Amazon Elastic Container Service Developer Guide。
- AWS Global Accelerator — 提高应用程序的可用性和性能。使用加速器在一个或多个 AWS 区域的多个负载均衡器之间分配流量。有关更多信息，请参阅 AWS Global Accelerator 开发人员指南。
- Route 53 — 通过将域名转换为计算机相互连接所用的数字 IP 地址，以一种可靠且经济的方式将访问者路由至网站。例如，它会将 `www.example.com` 转换为数字 IP 地址 `192.0.2.1`。AWS 将向您的资源 (如负载均衡器) 分配 URL。不过，您可能希望使用方便用户记忆的 URL。例如，您可以将域名映射到负载均衡器。有关更多信息，请参阅 Amazon Route 53 开发人员指南。
- AWS WAF — 您可以结合使用 AWS WAF 和 应用程序负载均衡器 以根据 Web 访问控制列表 (Web ACL) 中的规则允许或阻止请求。有关更多信息，请参阅 AWS WAF 开发人员指南。

定价

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

Elastic Load Balancing 的工作原理

负载均衡器接受来自客户端的传入流量并将请求路由到一个或多个可用区中的已注册目标 (例如 EC2 实例)。负载均衡器还会监控已注册目标的运行状况，并确保它只将流量路由到正常运行的目标。当负载均衡器检测到不正常目标时，它会停止将流量路由到该目标。然后，当它检测到目标再次正常时，它会恢复将流量路由到该目标。

您可通过指定一个或多个侦听器 将您的负载均衡器配置为接受传入流量。侦听器是用于检查连接请求的进程。它配置了用于从客户端连接到负载均衡器的协议和端口号。同样，它配置了用于从负载均衡器连接到目标的协议和端口号。

Elastic Load Balancing 支持三种类型的负载均衡器：

- Application Load Balancer
- Network Load Balancer
- Classic Load Balancer

负载均衡器类型的配置方式具有一个关键区别。对于 Application Load Balancer 和 Network Load Balancer，可以在目标组中注册目标，并将流量路由到目标组。对于 Classic Load Balancer，可以向负载均衡器注册实例。

可用区与负载均衡器节点

如果为负载均衡器启用可用区，Elastic Load Balancing 会在该可用区中创建一个负载均衡器节点。如果您在可用区中注册目标但不启用可用区，这些已注册目标将无法接收流量。当您确保每个启用的可用区均具有至少一个已注册目标时，负载均衡器将具有最高效率。

我们建议您启用多个可用区。（对于 应用程序负载均衡器，我们要求您启用多个可用区。）此配置有助于确保负载均衡器可以继续路由流量。如果一个可用区变得不可用或没有正常目标，则负载均衡器会将流量路由到其他可用区中的正常目标。

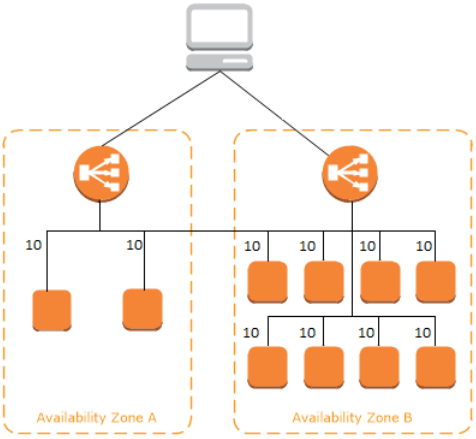
在禁用一个可用区后，该可用区中的目标将保持已注册到负载均衡器的状态。但是，即使它们保持已注册状态，负载均衡器也不会将流量路由到它们。

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。启用了跨区域负载均衡后，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。禁用了跨区域负载均衡后，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。

下图演示了跨区域负载均衡的效果。有 2 个已启用的可用区，其中可用区 A 中有 2 个目标，可用区 B 中有 8 个目标。客户端发送请求，Amazon Route 53 使用负载均衡器节点之一的 IP 地址响应每个请求。这会分配流量，以便每个负载均衡器节点接收来自客户端的 50% 的流量。每个负载均衡器节点会在其范围中的已注册目标之间分配其流量份额。

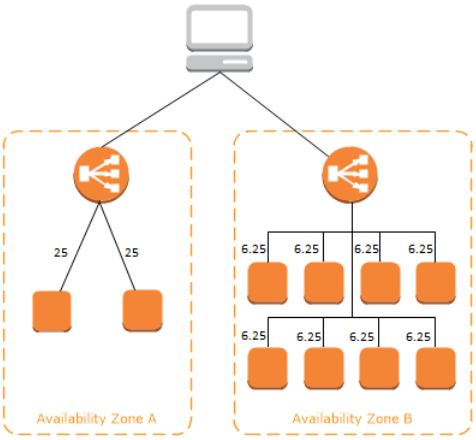
如果启用了跨区域负载均衡，则 10 个目标中的每个目标接收 10% 的流量。这是因为每个负载均衡器节点可将其 50% 的客户端流量路由到所有 10 个目标。



如果禁用了跨区域负载均衡：

- 可用区 A 中的两个目标中的每个目标接收 25% 的流量。
- 可用区 B 中的八个目标中的每个目标接收 6.25% 的流量。

这是因为每个负载均衡器节点只能将其 50% 的客户端流量路由到其可用区中的目标。



对于 Application Load Balancer，始终启用跨区域负载均衡。

对于 Network Load Balancer，默认情况下禁用跨区域负载均衡。创建 网络负载均衡器 后，您随时可以启用或禁用跨区域负载均衡。有关更多信息，请参阅 Network Load Balancer 用户指南 中的跨区域负载均衡。

在创建 传统负载均衡器 时，跨区域负载均衡的默认值取决于创建负载均衡器的方式。默认情况下，使用 API 或 CLI 时将禁用跨区域负载均衡。默认情况下，使用 AWS 管理控制台时启用跨区域负载均衡的选项处于选中状态。创建 传统负载均衡器 后，您随时可以启用或禁用跨区域负载均衡。有关更多信息，请参阅 Classic Load Balancer 用户指南 中的启用跨区域负载均衡。

请求路由选择

在客户端将请求发送到负载均衡器之前，它会利用域名系统 (DNS) 服务器解析负载均衡器的域名。DNS 条目由 Amazon 控制，因为您的负载均衡器位于 `amazonaws.com` 域中。Amazon DNS 服务器会将一个或多个 IP 地址返回到客户端。这些是您的负载均衡器的负载均衡器节点的 IP 地址。对于 Network Load Balancer，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。在您创建负载均衡器时，可以选择将一个弹性 IP 地址与每个网络接口关联。

当流向应用程序的流量随时间变化时，Elastic Load Balancing 会扩展负载均衡器并更新 DNS 条目。DNS 条目还指定生存时间 (TTL) 为 60 秒。这有助于确保可以快速重新映射 IP 地址以响应不断变化的流量。

客户端可以确定使用哪个 IP 地址将请求发送到负载均衡器。用于接收请求的负载均衡器节点会选择一个正常运行的已注册目标，并使用其私有 IP 地址将请求发送到该目标。

路由算法

借助 Application Load Balancer，接收请求的负载均衡器节点使用以下过程：

1. 按优先级顺序评估侦听器规则以确定要应用的规则。
2. 使用为目标组配置的路由算法，从目标组中为规则操作选择目标。默认路由算法是轮询。每个目标组的路由都是单独进行的，即使某个目标已在多个目标组中注册。

借助 Network Load Balancer，接收连接的负载均衡器节点使用以下过程：

1. 使用流哈希算法从目标组中为默认规则选择目标。它使算法基于：
   - 协议
   - 源 IP 地址和源端口
   - 目标 IP 地址和目标端口
   - TCP 序列号
2. 将每个单独的 TCP 连接在连接的有效期内路由到单个目标。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。

借助 Classic Load Balancer，接收请求的负载均衡器节点按照以下方式选择注册实例：

- 使用适用于 TCP 侦听器的轮询路由算法
- 使用适用于 HTTP 和 HTTPS 侦听器的最少未完成请求路由算法

HTTP 连接

Classic Load Balancer 使用提前打开的连接，但 Application Load Balancer 不使用。Classic Load Balancer 和 Application Load Balancer 都使用多路复用连接。也就是说，来自多个前端连接上的多个客户端的请求可通过单一的后端连接路由到指定目标。多路复用连接可缩短延迟并减少您的应用程序上的负载。要禁止多路复用连接，请在您的 HTTP 响应中设置 `Connection: close` 标头来禁用 HTTP `keep-alives`。

对于前端连接（客户端到负载均衡器），Classic Load Balancer 支持以下协议：HTTP/0.9、HTTP/1.0 和 HTTP/1.1。

对于前端连接，Application Load Balancer 支持以下协议：HTTP/0.9、HTTP/1.0、HTTP/1.1 和 HTTP/2。HTTP/2 仅适用于 HTTPS 侦听器，使用一个 HTTP/2 连接可并行发送多达 128 个请求。Application Load Balancer 还支持将连接从 HTTP 升级到 WebSockets。

Application Load Balancer 和 Classic Load Balancer 都在后端连接（负载均衡器到已注册目标）上使用 HTTP/1.1。默认情况下，后端连接支持 `Keep-alive`。如果 HTTP/1.0 请求来自没有主机标头的客户端，负载均衡器会对后端连接发送的 HTTP/1.1 请求生成一个主机标头。对于应用程序负载均衡器，主机标头包含负载均衡器的 DNS 名称。对于传统负载均衡器，主机标头包含负载均衡器节点的 IP 地址。

对于前端连接，Application Load Balancer 和 Classic Load Balancer 均支持管道化 HTTP。对于后端连接它们均不支持管道化 HTTP。

HTTP 标头

Application Load Balancer 和 Classic Load Balancer 会将 X-Forwarded-For、X-Forwarded-Proto 和 X-Forwarded-Port 标头添加到请求。

对于使用 HTTP/2 的前端连接，标头名称是小写的。使用 HTTP/1.1 将请求发送到目标之前，以下标头名称将转换为混合大小写：X-Forwarded-For、X-Forwarded-Proto、X-Forwarded-Port、Host、X-Amzn-Trace-Id、Upgrade 和 Connection。所有其他标头名称是小写的。

Application Load Balancer 和 Classic Load Balancer 将响应代理返回客户端后，遵守来自传入客户端请求的连接标头。

当 Application Load Balancer 和 Classic Load Balancer 收到 Expect 标头时，它们会立即使用 HTTP 100 Continue 响应客户端而不测试内容长度标头，然后会删除 Expect 标头，再路由请求。

HTTP 标头限制

Application Load Balancer 的以下大小限制是无法更改的硬限制。

HTTP/1.x 标头

- 请求行：16K
- 单个标头：16K
- 整个标头：64K

HTTP/2 标头

- 请求行：8K
- 单个标头：8K
- 整个标头：64K

负载均衡器模式

在创建负载均衡器时，您必须选择使其成为内部负载均衡器还是面向 Internet 的负载均衡器。请注意，当您在 EC2-Classic 中创建 传统负载均衡器 时，它必须是面向 Internet 的负载均衡器。

面向 Internet 的负载均衡器的节点具有公共 IP 地址。面向 Internet 的负载均衡器的 DNS 名称可公开解析为节点的公共 IP 地址。因此，面向 Internet 的负载均衡器可以通过 Internet 路由来自客户端的请求。

内部负载均衡器的节点只有私有 IP 地址。内部负载均衡器的 DNS 名称可公开解析为节点的私有 IP 地址。因此，内部负载均衡器可路由的请求只能来自对负载均衡器的 VPC 具有访问权限的客户端。

面向 Internet 的负载均衡器和内部负载均衡器均使用私有 IP 地址将请求路由到您的目标。因此，您的目标无需使用公有 IP 地址从内部负载均衡器或面向 Internet 的负载均衡器接收请求。

如果您的应用程序具有多个层，则可以设计一个同时使用内部负载均衡器和面向 Internet 的负载均衡器的架构。例如，如果您的应用程序使用必须连接到 Internet 的 Web 服务器，以及仅连接到 Web 服务器的应用程序服务器，则可以如此。创建一个面向 Internet 的负载均衡器并向其注册 Web 服务器。创建一个内部负载均衡器并向它注册应用程序服务器。Web 服务器从面向 Internet 的负载均衡器接收请求，并将对应用程序服务器的请求发送到内部负载均衡器。应用程序服务器从内部负载均衡器接收请求。

Elastic Load Balancing 入门

有三种类型的负载均衡器：Application Load Balancer、Network Load Balancer 和 Classic Load Balancer。可以根据应用程序需求选择负载均衡器。有关更多信息，请参阅 Elastic Load Balancing 产品比较。

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

如果您现在有 传统负载均衡器，则可以迁移到 应用程序负载均衡器 或 网络负载均衡器。有关更多信息，请参阅迁移您的 传统负载均衡器 (p. 22)。

创建 应用程序负载均衡器

要使用 AWS 管理控制台 创建 应用程序负载均衡器，请使用 Application Load Balancer 用户指南 中的 Application Load Balancer 入门。

要使用 AWS CLI 创建 应用程序负载均衡器，请参阅 Application Load Balancer 用户指南 中的使用 AWS CLI 创建 应用程序负载均衡器

创建 网络负载均衡器

要使用 AWS 管理控制台 创建 网络负载均衡器，请参阅 Network Load Balancer 用户指南 中的 Network Load Balancer 入门。

要使用 AWS CLI 创建 网络负载均衡器，请参阅 Network Load Balancer 用户指南 中的使用 AWS CLI 创建 网络负载均衡器

创建 传统负载均衡器

要使用 AWS 管理控制台 创建 传统负载均衡器，请参阅 Classic Load Balancer 用户指南 中的创建 传统负载均衡器。

Elastic Load Balancing 中的安全性

AWS 的云安全性的优先级最高。作为 AWS 客户，您将从专为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益。

安全性是 AWS 和您的共同责任。责任共担模型将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。作为 AWS 合规性计划的一部分，第三方审计人员将定期测试和验证安全性的有效性。要了解适用于 Elastic Load Balancing 的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云中的安全性 – 您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Elastic Load Balancing 时应用责任共担模型。其中说明如何配置 Elastic Load Balancing 以实现您的安全性和合规性目标。您还将了解如何使用其他 AWS 服务来帮助您监控和保护 Elastic Load Balancing 资源。

内容

- Elastic Load Balancing 中的数据保护 (p. 8)
- 适用于 Elastic Load Balancing 的 Identity and Access Management (p. 9)
- Elastic Load Balancing 的合规性验证 (p. 18)
- Elastic Load Balancing 中的弹性 (p. 18)
- Elastic Load Balancing 中的基础设施安全性 (p. 19)
- Elastic Load Balancing 和接口 VPC 终端节点 (p. 20)

Elastic Load Balancing 中的数据保护

Elastic Load Balancing 符合 AWS责任共担模型，此模型包含适用于数据保护的法规和准则。AWS 负责保护运行所有 AWS 服务的全球基础设施。AWS 保持对此基础设施上托管的数据的控制，包括用于处理客户内容和个人数据的安全配置控制。充当数据控制者或数据处理者的 AWS 客户和 APN 合作伙伴对他们在 AWS 云中放置的任何个人数据承担责任。

出于数据保护的目的，我们建议您保护 AWS 账户凭证并使用 AWS Identity and Access Management (IAM) 设置单个用户账户，以便仅向每个用户提供履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 TLS 与 AWS 资源进行通信。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的个人数据。

我们强烈建议您切勿将敏感的可识别信息（例如您客户的账号）放入自由格式字段或元数据（例如函数名称和标签）。您输入到元数据的任何数据都可能被选取以包含在诊断日志中。当您向外部服务器提供 URL 时，请勿在 URL 中包含凭证信息来验证您对该服务器的请求。

有关数据保护的更多信息，请参阅 AWS 安全性博客上的 AWS 责任共担模型和 GDPR 博客文章。

静态加密

如果您为用于 Elastic Load Balancing 访问日志的 S3 存储桶启用了使用 Amazon S3 托管加密密钥 (SSE-S3) 的服务器端加密，则 Elastic Load Balancing 会先自动加密每个访问日志文件，然后再存储到 S3 存储桶中。Elastic Load Balancing 还会在您访问日志文件时自动解密文件。每个日志文件都使用一个唯一密钥进行加密，此密钥本身将使用定期轮换的主密钥进行加密。

传输中加密

通过在负载均衡器上终止来自客户端的 HTTPS 和 TLS 流量，Elastic Load Balancing 简化了构建安全 Web 应用程序的过程。负载均衡器会执行加密和解密流量的工作，而不要求每个 EC2 实例来处理 TLS 终止工作。在配置安全侦听器时，您可以指定应用程序支持的密码套件和协议版本，以及要在您的负载均衡器上安装的服务器证书。可以使用 AWS Certificate Manager (ACM) 或 AWS Identity and Access Management (IAM) 来管理您的服务器证书。Application Load Balancer 支持 HTTPS 侦听器。Network Load Balancer 支持 TLS 侦听器。Classic Load Balancer 同时支持 HTTPS 和 TLS 侦听器。

适用于 Elastic Load Balancing 的 Identity and Access Management

AWS 使用安全凭证来识别您的身份并向您授予对 AWS 资源的访问权。利用 AWS Identity and Access Management (IAM) 的功能，可允许其他用户、服务和应用程序完全使用或受限使用您的 AWS 资源。您可以在不共享安全凭证的情况下执行此操作。

默认情况下，IAM 用户没有创建、查看或修改 AWS 资源的权限。要允许 IAM 用户访问资源（如负载均衡器）并执行任务，您可以：

1. 创建授予 IAM 用户使用所需特定资源和 API 操作的权限的 IAM 策略。
2. 将该策略附加到 IAM 用户或 IAM 用户所属的组。

在将策略附加到一个用户或一组用户时，它会授权或拒绝用户使用指定资源执行指定任务。

例如，您可以使用 IAM 在您的 AWS 账户下创建用户和组。IAM 用户可以是人员、系统或应用程序。然后，使用 IAM 策略向用户和组授予对指定资源执行特定操作的权限。

使用 IAM 策略授予权限

在将策略附加到一个用户或一组用户时，它会授权或拒绝用户使用指定资源执行指定任务。

IAM 策略是包含一个或多个语句的 JSON 文档。每个语句的结构如下例所示。

```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect": "effect",
    "Action": "action",
    "Resource": "resource-arn",
    "Condition": {
      "condition": {
        "key":"value"
      }
    }
```

```
  }]
}
```

- Effect — effect 可以为 `Allow` 或 `Deny`。默认情况下 IAM 用户没有使用资源和 API 操作的权限，因此，所有请求均会被拒绝。显式允许将覆盖默认规则。显式拒绝将覆盖任何允许。
- Action — action 是对其授予或拒绝权限的特定 API 操作。有关指定 action 的更多信息，请参阅 Elastic Load Balancing 的 API 操作 (p. 10)。
- Resource — 受操作影响的资源。利用许多 Elastic Load Balancing API 操作，您可以限制对特定负载均衡器授予或拒绝的权限。为此，请在此语句中指定其 Amazon 资源名称 (ARN)。否则，您可以使用 * 通配符指定所有负载均衡器。有关更多信息，请参阅Elastic Load Balancing 资源 (p. 10)。
- Condition — 您可以选择性地使用条件来控制策略的生效时间。有关更多信息，请参阅Elastic Load Balancing 的条件密钥 (p. 13)。

有关更多信息，请参见 IAM 用户指南。

Elastic Load Balancing 的 API 操作

在 IAM 策略语句的 Action 元素中，您可以指定 Elastic Load Balancing 所提供的任意 API 操作。如以下示例所示，您必须使用小写形式的字符串 `elasticloadbalancing:` 作为操作名称的前缀。

```
"Action": "elasticloadbalancing:DescribeLoadBalancers"
```

要在单个语句中指定多项操作，请使用方括号将操作括起来并以逗号分隔，如以下示例所示。

```
"Action": [
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DeleteLoadBalancer"
]
```

您也可以使用 * 通配符指定多项操作。以下示例指定 Elastic Load Balancing 的以 `Describe` 开头的所有 API 操作名称。

```
"Action": "elasticloadbalancing:Describe*"
```

要指定 Elastic Load Balancing 的所有 API 操作，请按下例所示使用通配符 *。

```
"Action": "elasticloadbalancing:*"
```

有关 Elastic Load Balancing API 操作的完整列表，请参阅以下文档：

- Application Load Balancer 和 Network Load Balancer — API 参考版本 2015-12-01
- Classic Load Balancer — API 参考版本 2012-06-01

Elastic Load Balancing 资源

资源级权限 是指指定允许用户对哪些资源执行操作的能力。Elastic Load Balancing 对资源级权限提供部分支持。对于支持资源级权限的 API 操作，您可以控制用户可与操作结合使用的资源。要在策略中指定资源，您必须使用其 Amazon 资源名称 (ARN)。指定 ARN 时，您可以在路径中使用 * 通配符。例如，当您不想指定确切的负载均衡器名称时，可以使用 * 通配符。

应用程序负载均衡器 的 ARN 具有以下示例中显示的格式。

```
arn:aws:elasticloadbalancing:region-code:account-id:loadbalancer/app/load-balancer-name/load-balancer-id
```

网络负载均衡器 的 ARN 具有以下示例中显示的格式。

```
arn:aws:elasticloadbalancing:region-code:account-id:loadbalancer/net/load-balancer-name/load-balancer-id
```

传统负载均衡器 的 ARN 具有以下示例中显示的格式。

```
arn:aws:elasticloadbalancing:region-code:account-id:loadbalancer/load-balancer-name
```

侦听器的 ARN 和 应用程序负载均衡器 的侦听器规则具有以下示例中显示的格式。

```
arn:aws:elasticloadbalancing:region-code:account-id:listener/app/load-balancer-name/load-balancer-id/listener-id
arn:aws:elasticloadbalancing:region-code:account-id:listener-rule/app/load-balancer-name/load-balancer-id/listener-id/rule-id
```

网络负载均衡器 的侦听器的 ARN 具有以下示例中显示的格式。

```
arn:aws:elasticloadbalancing:region-code:account-id:listener/net/load-balancer-name/load-balancer-id/listener-id
```

目标组的 ARN 具有以下示例中显示的格式。

```
arn:aws:elasticloadbalancing:region-code:account-id:targetgroup/target-group-name/target-group-id
```

不支持资源级权限的 API 操作

以下 Elastic Load Balancing 操作不支持资源级权限：

- API 版本 2015-12-01：
  - `DescribeAccountLimits`
  - `DescribeListenerCertificates`
  - `DescribeListeners`
  - `DescribeLoadBalancerAttributes`
  - `DescribeLoadBalancers`
  - `DescribeRules`
  - `DescribeSSLPolicies`
  - `DescribeTags`
  - `DescribeTargetGroupAttributes`
  - `DescribeTargetGroups`
  - `DescribeTargetHealth`
- API 版本 2012-06-01：
  - `DescribeInstanceHealth`
  - `DescribeLoadBalancerAttributes`
  - `DescribeLoadBalancerPolicyTypes`
  - `DescribeLoadBalancers`

- DescribeLoadBalancerPolicies
- DescribeTags

对于不支持资源级权限的 API 操作，必须指定以下示例中显示的资源语句。

```
"Resource": "*"
```

Elastic Load Balancing 的资源级权限

下面的各表介绍支持资源级权限的 Elastic Load Balancing 操作，以及每个操作支持的资源。

API 版本 2015-12-01

API 操作	资源 ARN
AddListenerCertificates	侦听器
AddTags	负载均衡器，目标组
CreateListener	负载均衡器
CreateLoadBalancer	负载均衡器
CreateRule	侦听器
CreateTargetGroup	目标组
DeleteListener	侦听器
DeleteLoadBalancer	负载均衡器
DeleteRule	侦听器规则
DeleteTargetGroup	目标组
DeregisterTargets	目标组
ModifyListener	侦听器
ModifyLoadBalancerAttributes	负载均衡器
ModifyRule	侦听器规则
ModifyTargetGroup	目标组
ModifyTargetGroupAttributes	目标组
RegisterTargets	目标组
RemoveListenerCertificates	侦听器
RemoveTags	负载均衡器，目标组
SetIpAddressType	负载均衡器
SetRulePriorities	侦听器规则
SetSecurityGroups	负载均衡器
SetSubnets	负载均衡器

API 版本 2012-06-01

API 操作	资源 ARN
AddTags	负载均衡器
ApplySecurityGroupsToLoadBalancer	负载均衡器
AttachLoadBalancerToSubnets	负载均衡器
ConfigureHealthCheck	负载均衡器
CreateAppCookieStickinessPolicy	负载均衡器
CreateLBCookieStickinessPolicy	负载均衡器
CreateLoadBalancer	负载均衡器
CreateLoadBalancerListeners	负载均衡器
CreateLoadBalancerPolicy	负载均衡器
DeleteLoadBalancer	负载均衡器
DeleteLoadBalancerListeners	负载均衡器
DeleteLoadBalancerPolicy	负载均衡器
DeregisterInstancesFromLoadBalancer	负载均衡器
DetachLoadBalancerFromSubnets	负载均衡器
DisableAvailabilityZonesForLoadBalancer	负载均衡器
EnableAvailabilityZonesForLoadBalancer	负载均衡器
ModifyLoadBalancerAttributes	负载均衡器
RegisterInstancesWithLoadBalancer	负载均衡器
RemoveTags	负载均衡器
SetLoadBalancerListenerSSLCertificate	负载均衡器
SetLoadBalancerPoliciesForBackendServer	负载均衡器
SetLoadBalancerPoliciesOfListener	负载均衡器

Elastic Load Balancing 的条件密钥

在创建策略时，您可指定控制策略生效时间的条件。每个条件都包含一个或多个键值对。有全局条件键和特定于服务的条件键。

不能将 `aws:SourceIp` 条件键与 Elastic Load Balancing 一起使用。

`elasticloadbalancing:ResourceTag/`*`key`* 条件键特定于 Elastic Load Balancing。以下操作支持此条件键：

API 版本 2015-12-01

- AddTags

- CreateListener
- CreateLoadBalancer
- DeleteLoadBalancer
- DeleteTargetGroup
- DeregisterTargets
- ModifyLoadBalancerAttributes
- ModifyTargetGroup
- ModifyTargetGroupAttributes
- RegisterTargets
- RemoveTags
- SetIpAddressType
- SetSecurityGroups
- SetSubnets

API 版本 2012-06-01

- AddTags
- ApplySecurityGroupsToLoadBalancer
- AttachLoadBalancersToSubnets
- ConfigureHealthCheck
- CreateAppCookieStickinessPolicy
- CreateLBCookieStickinessPolicy
- CreateLoadBalancer
- CreateLoadBalancerListeners
- CreateLoadBalancerPolicy
- DeleteLoadBalancer
- DeleteLoadBalancerListeners
- DeleteLoadBalancerPolicy
- DeregisterInstancesFromLoadBalancer
- DetachLoadBalancersFromSubnets
- DisableAvailabilityZonesForLoadBalancer
- EnableAvailabilityZonesForLoadBalancer
- ModifyLoadBalancerAttributes
- RegisterInstancesWithLoadBalancer
- RemoveTags
- SetLoadBalancerListenerSSLCertificate
- SetLoadBalancerPoliciesForBackendServer
- SetLoadBalancerPoliciesOfListener

有关全局条件键的更多信息，请参阅 IAM 用户指南 中的 AWS 全局条件上下文键。

以下操作支持 `aws:RequestTag/key` 和 `aws:TagKeys` 条件键：

- AddTags
- CreateLoadBalancer

- RemoveTags

预定义的 AWS 托管策略

AWS 创建的托管策略将授予针对常用案例的必要权限。您可以根据您的 IAM 用户对 Elastic Load Balancing 所需的访问权限将这些策略附加到这些用户：

- ElasticLoadBalancingFullAccess — 授予使用 Elastic Load Balancing 功能所需的完整访问权限。
- ElasticLoadBalancingReadOnly — 授予对 Elastic Load Balancing 功能的只读访问权限。

有关每个 Elastic Load Balancing 操作所需的权限的更多信息，请参阅Elastic Load Balancing API 权限 (p. 15)。

Elastic Load Balancing API 权限

您必须为 IAM 用户授予调用所需 Elastic Load Balancing API 操作的权限，如Elastic Load Balancing 的 API 操作 (p. 10)中所述。此外，对于某些 Elastic Load Balancing 操作，您必须授予 IAM 用户从 Amazon EC2 API 调用特定操作的权限。

2015-12-01 API 所需的权限

从 2015-12-01 API 调用以下操作时，您必须授予 IAM 用户调用指定操作的权限。

CreateLoadBalancer
- elasticloadbalancing:CreateLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeAddresses
- ec2:DescribeInternetGateways
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- iam:CreateServiceLinkedRole

CreateTargetGroup
- elasticloadbalancing:CreateTargetGroup
- ec2:DescribeInternetGateways
- ec2:DescribeVpcs

RegisterTargets
- elasticloadbalancing:RegisterTargets
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeSubnets
- ec2:DescribeVpcs

SetIpAddressType
- elasticloadbalancing:SetIpAddressType
- ec2:DescribeSubnets

SetSubnets
- elasticloadbalancing:SetSubnets
- ec2:DescribeSubnets

2012-06-01 API 所需的权限

从 2012-06-01 API 调用以下操作时，您必须授予 IAM 用户调用指定操作的权限。

ApplySecurityGroupsToLoadBalancer
- elasticloadbalancing:ApplySecurityGroupsToLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeSecurityGroups

AttachLoadBalancerToSubnets
- elasticloadbalancing:AttachLoadBalancerToSubnets
- ec2:DescribeSubnets

CreateLoadBalancer
- elasticloadbalancing:CreateLoadBalancer
- ec2:CreateSecurityGroup
- ec2:DescribeAccountAttributes
- ec2:DescribeInternetGateways
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- iam:CreateServiceLinkedRole

DeregisterInstancesFromLoadBalancer
- elasticloadbalancing:DeregisterInstancesFromLoadBalancer
- ec2:DescribeClassicLinkInstances
- ec2:DescribeInstances

DescribeInstanceHealth
- elasticloadbalancing:DescribeInstanceHealth
- ec2:DescribeClassicLinkInstances
- ec2:DescribeInstances

DescribeLoadBalancers
- elasticloadbalancing:DescribeLoadBalancers
- ec2:DescribeSecurityGroups

DisableAvailabilityZonesForLoadBalancer
- elasticloadbalancing:DisableAvailabilityZonesForLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeInternetGateways
- ec2:DescribeVpcs

EnableAvailabilityZonesForLoadBalancer
- elasticloadbalancing:EnableAvailabilityZonesForLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeInternetGateways
- ec2:DescribeSubnets
- ec2:DescribeVpcs

RegisterInstancesWithLoadBalancer
- elasticloadbalancing:RegisterInstancesWithLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeClassicLinkInstances

- ec2:DescribeInstances
- ec2:DescribeVpcClassicLink

Elastic Load Balancing 服务相关角色

Elastic Load Balancing 使用服务相关角色来获取它代表您调用其他 AWS 服务所需的权限。有关更多信息，请参阅 IAM 用户指南 中的使用服务相关角色。

服务相关角色授予的权限

Elastic Load Balancing 使用名为 AWSServiceRoleForElasticLoadBalancing 的服务相关角色代表您调用以下操作：

- ec2:DescribeAddresses
- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcs
- ec2:DescribeInternetGateways
- ec2:DescribeAccountAttributes
- ec2:DescribeClassicLinkInstances
- ec2:DescribeVpcClassicLink
- ec2:CreateSecurityGroup
- ec2:CreateNetworkInterface
- ec2:DeleteNetworkInterface
- ec2:ModifyNetworkInterfaceAttribute
- ec2:AuthorizeSecurityGroupIngress
- ec2:AssociateAddress
- ec2:DisassociateAddress
- ec2:AttachNetworkInterface
- ec2:DetachNetworkInterface
- ec2:AssignPrivateIpAddresses
- ec2:AssignIpv6Addresses
- ec2:UnassignIpv6Addresses
- logs:CreateLogDelivery
- logs:GetLogDelivery
- logs:UpdateLogDelivery
- logs:DeleteLogDelivery
- logs:ListLogDeliveries

AWSServiceRoleForElasticLoadBalancing 信任 elasticloadbalancing.amazonaws.com 服务来代入该角色。

创建服务相关角色

您无需手动创建 AWSServiceRoleForElasticLoadBalancing 角色。Elastic Load Balancing 将在您创建负载均衡器时为您创建此角色。

要让 Elastic Load Balancing 代表您创建服务相关角色，您必须具有所需权限。有关更多信息，请参阅 IAM 用户指南 中的服务相关角色权限。

如果您在 2018 年 1 月 11 日之前创建了负载均衡器，则 Elastic Load Balancing 已在您的 AWS 账户中创建了 AWSServiceRoleForElasticLoadBalancing。有关更多信息，请参阅 IAM 用户指南 中的我的 AWS 账户中出现新角色。

编辑服务相关角色

您可以使用 IAM 编辑 AWSServiceRoleForElasticLoadBalancing 的描述。有关更多信息，请参阅 IAM 用户指南 中的编辑服务相关角色。

删除服务相关角色

如果您不再需要使用 Elastic Load Balancing，我们建议您删除 AWSServiceRoleForElasticLoadBalancing。

只有在删除 AWS 账户中的所有负载均衡器后，才能删除此服务相关角色。这可确保您不会无意中删除访问您的负载均衡器的权限。有关更多信息，请参阅删除 应用程序负载均衡器、删除网络负载均衡器 和删除 传统负载均衡器。

您可以使用 IAM 控制台、IAM CLI 或 IAM API 删除服务相关角色。有关更多信息，请参阅 IAM 用户指南 中的删除服务相关角色。

在您删除 AWSServiceRoleForElasticLoadBalancing 之后，Elastic Load Balancing 将在您创建负载均衡器时再次为您创建该角色。

Elastic Load Balancing 的合规性验证

作为多个 AWS 合规性计划的一部分，第三方审计员将评估 Elastic Load Balancing 的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规性计划范围内的 AWS 服务列表，请参阅合规性计划范围内的 AWS 服务。有关常规信息，请参阅 AWS 合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅在 AWS Artifact 中下载报告。

您在使用 Elastic Load Balancing 时的合规性责任由您数据的敏感性、您公司的合规性目标以及适用的法律法规决定。AWS 提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南 – 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署基于安全性和合规性的基准环境的步骤。
- 《设计符合 HIPAA 安全性和合规性要求的架构》白皮书 – 此白皮书介绍公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。
- AWS 合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- AWS Config Developer Guide 中的使用规则评估资源 – AWS Config；评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub – 此 AWS 服务提供了 AWS 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。

Elastic Load Balancing 中的弹性

AWS 全球基础设施围绕 AWS 区域和可用区构建。区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断

地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅 AWS 全球基础设施。

除了 AWS 全球基础设施以外，Elastic Load Balancing 还提供以下功能以支持数据弹性：

- 在一个或多个可用区中的多个实例之间分配传入流量。
- 您可以将 AWS Global Accelerator 与 Application Load Balancer 一起使用，在一个或多个 AWS 区域中的多个负载均衡器之间分配传入流量。有关更多信息，请参阅 AWS Global Accelerator 开发人员指南。
- Amazon ECS 使您能够在 EC2 实例集群上运行、停止和管理 Docker 容器。您可以将 Amazon ECS 服务配置为使用负载均衡器在群集中的服务之间分配传入流量。有关更多信息，请参阅 Amazon Elastic Container Service Developer Guide。

Elastic Load Balancing 中的基础设施安全性

作为一项托管服务，Elastic Load Balancing 由 Amazon Web Services：安全流程概述白皮书中所述的 AWS 全球网络安全程序提供保护。

您可以使用 AWS 发布的 API 调用通过网络访问 Elastic Load Balancing。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service (AWS STS) 生成临时安全凭证来对请求进行签名。

网络隔离

Virtual Private Cloud (VPC) 是 AWS 云内您自己的逻辑隔离区域中的虚拟网络。子网是 VPC 中的 IP 地址范围。当您创建负载均衡器时，可以为负载均衡器节点指定一个或多个子网。您可以在您的 VPC 的子网中部署 EC2 实例，并将这些实例注册到您的负载均衡器。有关 VPC 和子网的更多信息，请参阅Amazon VPC 用户指南。

当您在 VPC 中创建负载均衡器时，它可以面向 Internet，也可以面向内部。内部负载均衡器可路由的请求只能来自对负载均衡器的 VPC 具有访问权限的客户端。

您的负载均衡器会使用私有 IP 地址向已注册目标发送请求。因此，您的目标无需使用公有 IP 地址，即可接收来自负载均衡器的请求。

要从 VPC 调用 Elastic Load Balancing API，而不通过公共 Internet 发送流量，请使用 AWS PrivateLink。有关更多信息，请参阅Elastic Load Balancing 和接口 VPC 终端节点 (p. 20)。

控制网络流量

Elastic Load Balancing 支持三种类型的负载均衡器：Application Load Balancer、Network Load Balancer 和 Classic Load Balancer。Application Load Balancer 在开放系统互连 (OSI) 模型的请求级别（第 7 层）操作。Network Load Balancer 在 OSI 模型的连接级别（第 4 层）操作。Classic Load Balancer 则同时在请求级别和连接级别操作。

当您使用负载均衡器时，请考虑使用以下选项来保护网络流量：

- 使用安全侦听器来支持客户端与您的负载均衡器之间的加密通信。Application Load Balancer 支持 HTTPS 侦听器。Network Load Balancer 支持 TLS 侦听器。Classic Load Balancer 则同时支持 HTTPS 和 TLS 侦听器。您可以从您的负载均衡器的预定义安全策略中选择，指定您的应用程序支持的密码套件和协议版

本。可以使用 AWS Certificate Manager (ACM) 或 AWS Identity and Access Management (IAM) 管理安装在您的负载均衡器上的服务器证书。您可以利用服务器名称指示 (SNI) 协议，使用单个安全侦听器为多个安全网站提供服务。当您将多个服务器证书与安全侦听器关联时，会自动为您的负载均衡器启用 SNI。

- 为您的 Application Load Balancer 和 Classic Load Balancer 配置安全组，以便以仅接受来自特定客户端的流量。这些安全组必须在侦听器端口上允许来自客户端的入站流量以及流向客户端的出站流量。
- 为您的 Amazon EC2 实例配置安全组，以仅接受来自负载均衡器的流量。这些安全组必须在侦听器端口和运行状况检查端口上允许来自负载均衡器的入站流量。
- 配置您的 应用程序负载均衡器，以便通过身份提供商或使用公司身份安全地对用户进行身份验证。有关更多信息，请参阅使用 应用程序负载均衡器 对用户进行身份验证。
- 您可以将 AWS WAF 与您的 Application Load Balancer 结合使用，以根据 Web 访问控制列表 (Web ACL) 中的规则允许或阻止请求。

Elastic Load Balancing 和接口 VPC 终端节点

您可以通过创建接口 VPC 终端节点来在 Virtual Private Cloud (VPC) 与 Elastic Load Balancing API 之间建立专用连接。您可以使用此连接从 VPC 调用 Elastic Load Balancing API，而无需通过 Internet 发送流量。终端节点提供了与 2015-12-01 版和 2012-06-01 版 Elastic Load Balancing API 的可靠、可扩展的连接。它无需 Internet 网关、NAT 实例或 VPN 连接即可完成此操作。

接口 VPC 终端节点由 AWS PrivateLink 提供支持，此功能使用私有 IP 地址在 AWS 服务之间实现私有通信。有关更多信息，请参阅AWS PrivateLink。

限制

AWS PrivateLink 不支持具有超过 50 个侦听器的 网络负载均衡器。

为 Elastic Load Balancing 创建接口终端节点

使用以下服务名称之一为 Elastic Load Balancing 创建终端节点：

- com.amazonaws.*region*.elasticloadbalancing — 为 Elastic Load Balancing API 操作创建终端节点。
- com.amazonaws.*region*.elasticloadbalancing-fips — 为 Elastic Load Balancing API 创建符合美国政府标准联邦信息处理标准 (FIPS) 140-2 的终端节点。

有关更多信息，请参阅 Amazon VPC 用户指南 中的创建接口终端节点。

为 Elastic Load Balancing 创建 VPC 终端节点策略

您可以向 VPC 终端节点附加策略来控制对 Elastic Load Balancing API 的访问。该策略指定：

- 可执行操作的委托人。
- 可执行的操作。
- 可对其执行操作的资源。

以下示例显示了一个 VPC 终端节点策略，该策略拒绝所有人通过终端节点创建负载均衡器的权限。示例策略还授予所有人执行所有其他操作的权限。

```
{
   "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
```

```
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "elasticloadbalancing:CreateLoadBalancer",
            "Effect": "Deny",
            "Resource": "*",
            "Principal": "*"
        }
    ]
}
```

有关更多信息，请参阅 Amazon VPC 用户指南 中的使用 VPC 终端节点策略。

迁移您的 传统负载均衡器

如果您在 VPC 中已经有 传统负载均衡器，并且确信 应用程序负载均衡器 或 网络负载均衡器 满足您的需求，那么您就可以迁移 传统负载均衡器。在迁移过程完成后，您就可以利用新负载均衡器的功能了。有关更多信息，请参阅 Elastic Load Balancing 产品比较。

迁移过程

- 步骤 1：创建新负载均衡器 (p. 22)
- 步骤 2：逐步将流量重定向到您的新负载均衡器 (p. 23)
- 步骤 3：更新对您的 传统负载均衡器 的引用 (p. 24)
- 步骤 4：删除 传统负载均衡器 (p. 24)

步骤 1：创建新负载均衡器

创建配置等同于您的 传统负载均衡器 的 应用程序负载均衡器 或 网络负载均衡器。

您可以使用以下方法之一来创建负载均衡器和目标组：

- 控制台中的迁移向导 (p. 22)
- 负载均衡器复制实用工具 (p. 23)
- 手动方式 (p. 23)

选项 1：使用迁移向导进行迁移

迁移向导根据 传统负载均衡器 的配置创建 应用程序负载均衡器 或 网络负载均衡器。所创建负载均衡器的类型取决于 传统负载均衡器 的配置。

迁移向导发行说明

- 传统负载均衡器必须位于 VPC 中。
- 如果 传统负载均衡器 具有 HTTP 或 HTTPS 侦听器，则该向导可以创建 应用程序负载均衡器。如果 传统负载均衡器 具有 TCP 侦听器，则该向导可以创建 网络负载均衡器。
- 如果 传统负载均衡器 的名称与现有 应用程序负载均衡器 或 网络负载均衡器 的名称匹配，则该向导将要求您在迁移过程中指定不同的名称。
- 如果 传统负载均衡器 具有一个子网，则该向导将要求您在创建 应用程序负载均衡器 时指定另一个子网。
- 如果传统负载均衡器已在 EC2-Classic 中注册实例，这些实例不会注册到新负载均衡器的目标组。
- 如果 传统负载均衡器 具有以下类型的已注册实例，不会向 网络负载均衡器 的目标组注册它们：C1、CC1、CC2、CG1、CG2、CR1、CS1、G1、G2、HI1、HS1、M1、M2、M3 和 T1。
- 如果 传统负载均衡器 具有 HTTP/HTTPS 侦听器，但使用 TCP 运行状况检查，则向导将更改为 HTTP 运行状况检查。然后在创建 应用程序负载均衡器 时，默认情况下，它将路径设置为“/”。
- 如果将 传统负载均衡器 迁移到 网络负载均衡器，则将更改运行状况检查设置以满足 Network Load Balancer 的要求。
- 如果传统负载均衡器有多个 HTTPS 侦听器，则向导将选择一个侦听器并使用其证书和策略。如果端口 443 上有一个 HTTPS 侦听器，向导将选择此侦听器。如果所选侦听器使用自定义策略或 Application Load Balancer 不支持的策略，则向导将更改为默认安全策略。

- 如果 传统负载均衡器 具有安全的 TCP 侦听器，则 网络负载均衡器 使用 TCP 侦听器。但它不使用证书或安全策略。
- 如果传统负载均衡器有多个侦听器，该向导将使用端口值最低的侦听器端口作为目标组端口。注册到这些侦听器的每个实例都会在所有侦听器的侦听器端口上注册到目标组。
- 如果 传统负载均衡器 的一些标签在标签名称中具有 `aws` 前缀，则这些标签不会添加到新的负载均衡器。

使用迁移向导迁移传统负载均衡器

1. 打开 Amazon EC2 控制台 https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的 LOAD BALANCING 下，选择 Load Balancers。
3. 选择您的传统负载均衡器。
4. 在 Migration 选项卡上，选择 Launch ALB Migration Wizard 或 Launch NLB Migration Wizard。显示的按钮取决于在检查 传统负载均衡器 后由向导选择的负载均衡器类型。
5. 在 Review 页面上，验证向导选择的配置选项。要更改某个选项，请选择 Edit。
6. 当您完成配置新的负载均衡器时，选择 Create。

选项 2：使用负载均衡器复制实用程序进行迁移

此实用程序在 GitHub 上提供。有关更多信息，请参阅负载均衡器复制实用程序。

选项 3：手动迁移

以下信息提供了基于 传统负载均衡器 手动创建新负载均衡器的一般说明。您可以使用 AWS 管理控制台、AWS CLI 或 AWS 软件开发工具包进行迁移。有关更多信息，请参阅Elastic Load Balancing 入门 (p. 7)。

- 创建具有与 传统负载均衡器 相同的模式（面向 Internet 或内部）、子网和安全组的新负载均衡器。
- 使用传统负载均衡器的运行状况检查设置为负载均衡器创建一个目标组。
- 执行以下任一操作：
  - 如果您的 传统负载均衡器 附加到 Auto Scaling 组，请将您的目标组附加到 Auto Scaling 组。这样还可以向目标组注册 Auto Scaling 实例。
  - 向目标组注册您的 EC2 实例。
- 创建一个或多个侦听器，每个都具有将请求转发到目标组的默认规则。如果创建 HTTPS 侦听器，则可指定您为 传统负载均衡器 所指定的同一证书。建议您使用默认安全策略。
- 如果您的 传统负载均衡器 有标签，请进行检查并将相关标签添加到新负载均衡器。

步骤 2：逐步将流量重定向到您的新负载均衡器

在您的实例注册到新负载均衡器后，您可以开始将流量重定向到它的过程。这允许您测试新负载均衡器。

逐步将流量重定向到您的新负载均衡器

1. 将新负载均衡器的 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。
2. 创建一个用于将域名与您的新负载均衡器关联的新 DNS 记录。如果您的 DNS 服务支持权重，则在新 DNS 记录中指定权重为 1；对于您传统负载均衡器的现有 DNS 记录，指定权重为 9。这样可以将 10% 的流量定向到新负载均衡器，而将 90% 的流量定向到 传统负载均衡器。
3. 监控您的新负载均衡器，验证它能否接收流量并将请求路由到您的实例。

Important

DNS 记录中的生存时间 (TTL) 为 60 秒。这意味着，解析域名的任何 DNS 服务器在其缓存中保留记录信息的时间为 60 秒，同时更改会传播。因此，在您完成上一步后，这些 DNS 服务器仍然可以在 60 秒内将流量路由到 传统负载均衡器。在传输过程中，流量可以定向到任一负载均衡器。

4. 继续更新您的 DNS 记录的权重，直到所有流量都定向到您的新负载均衡器。完成后，您可以删除传统负载均衡器的 DNS 记录。

步骤 3：更新对您的 传统负载均衡器 的引用

现在您已迁移到 传统负载均衡器，请务必更新对它的任何引用，如下所示：

- 使用 AWS CLI aws elb 命令（而不是 aws elbv2 命令）的脚本
- 使用 Elastic Load Balancing 版本 2012-06-01 (而不是 API 版本 2015-12-01) 的代码
- 使用 API 版本 2012-06-01 (而不是 2015-12-01 版本) 的 IAM 策略
- 使用 CloudWatch 指标的过程
- AWS CloudFormation 模板

资源

- AWS CLI Command Reference 中的 elbv2
- Elastic Load Balancing API 参考第 2015-12-01 版
- 适用于 Elastic Load Balancing 的 Identity and Access Management (p. 9)
- Application Load Balancer 用户指南 中的应用程序负载均衡器 指标
- Network Load Balancer 用户指南 中的网络负载均衡器 指标
- AWS CloudFormation 用户指南 中的 AWS::ElasticLoadBalancingV2::LoadBalancer

步骤 4：删除 传统负载均衡器

在满足以下条件后，您可以删除 传统负载均衡器：

- 您已将所有流量都重定向到新负载均衡器。
- 路由到 传统负载均衡器 的所有现有请求都已完成。