aws

用户指南

Elastic Load Balancing

Elastic Load Balancing: 用户指南

Table of Contents

什么是 Elastic Load Balancing？

Elastic Load Balancing 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。弹性负载均衡将会扩展负载均衡器容量，以响应传入流量中的变化。

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 支持以下负载均衡器：应用程序负载均衡器、Network Load Balancer、Gateway Load Balancer 和经典负载均衡器。您可以选择最适合自己需求的负载均衡器类型。有关更多信息，请参阅产品对比。

有关使用每个负载均衡器的详细信息，请参阅以下文档：

- 适用于应用程序负载均衡器的用户指南
- 适用于网络负载均衡器的用户指南
- 网关负载均衡器用户指南
- 经典负载均衡器用户指南

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 Management Console –提供可用于访问 Elastic Load Balancing 的 Web 界面。

- AWS 命令行界面 (AWS CLI) — 为包括 Elastic Load Balancing 在内的各种 AWS 服务提供命令。在 AWS CLI Windows、macOS 和 Linux 上都支持。有关更多信息，请参阅 AWS Command Line Interface。
- AWS 软件开发工具包 — 提供特定语言的 API 并处理许多连接细节，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：
  - 应用程序负载均衡器 和 Network Load Balancer — API 版本 2015-12-01
  - 经典负载均衡器— API 版本 2012-06-01

相关服务

弹性负载均衡 可与以下服务一起使用，以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。
- 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。您还可以利用 Amazon EC2 Auto Scaling 在实例需求变化时自动增加或减少实例数量。如果通过 Elastic Load Balancing 启用 Auto Scaling，则由 Auto Scaling 启动的实例将自动注册到负载均衡器。同样，由 Auto Scaling 终止的实例将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 — 使您能够监控您的负载均衡器并根据需要采取行动。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 开发人员指南。
- 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，它将`www.example.com`转换为数字 IP 地址`192.0.2.1`。 AWS 为您的资

源（例如负载均衡器）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 AWS WAF 与 Application Load Balancer 配合使用，根据网络访问控制列表 (Web ACL) 中的规则允许或阻止请求。有关更多信息，请参见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 弹性负载均衡 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 支持以下类型的负载均衡器：

- Application Load Balancer
- Network Load Balancer
- 网关负载均衡器
- 经典负载均衡器

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、Network Load Balancer 和 Gateway Load Balancer，可以在目标组中注册目标，并将流量路由到目标组。通过经典负载均衡器，可以在负载均衡器中注册实例。

可用区与负载均衡器节点

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。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。

我们建议为所有负载均衡器启用多个可用区。但对于 Application Load Balancer，要求您至少启用两个或更多可用区。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。

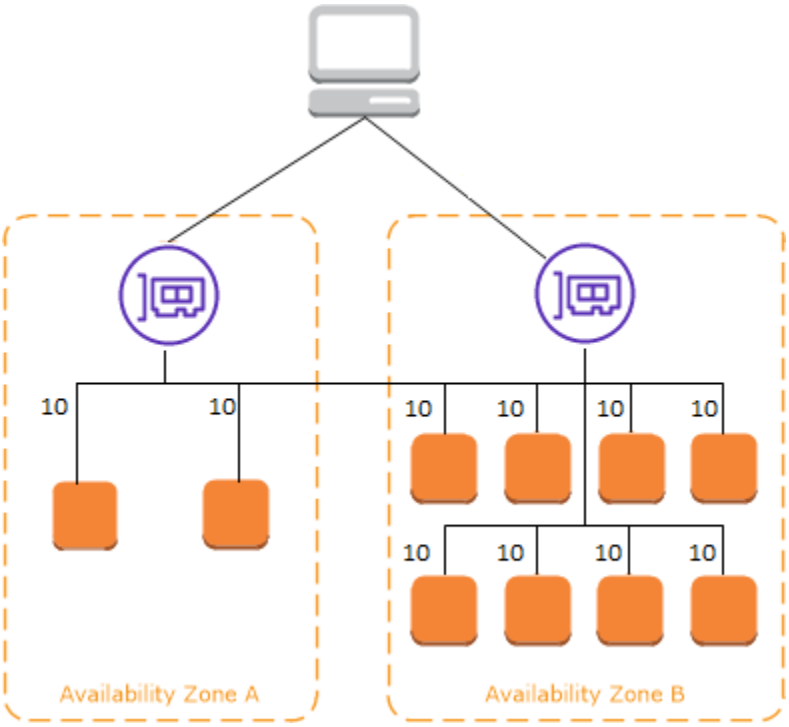
在禁用一个可用区后，该可用区中的目标将保持已注册到负载均衡器的状态。但是，即使它们保持已注册状态，负载均衡器也不会将流量路由到它们。

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。

下图演示了以轮询为默认路由算法的跨可用区负载均衡效果。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。基于轮询路由算法，系统会分配流量，以便每个负载均衡器节点接收来自客户端 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。

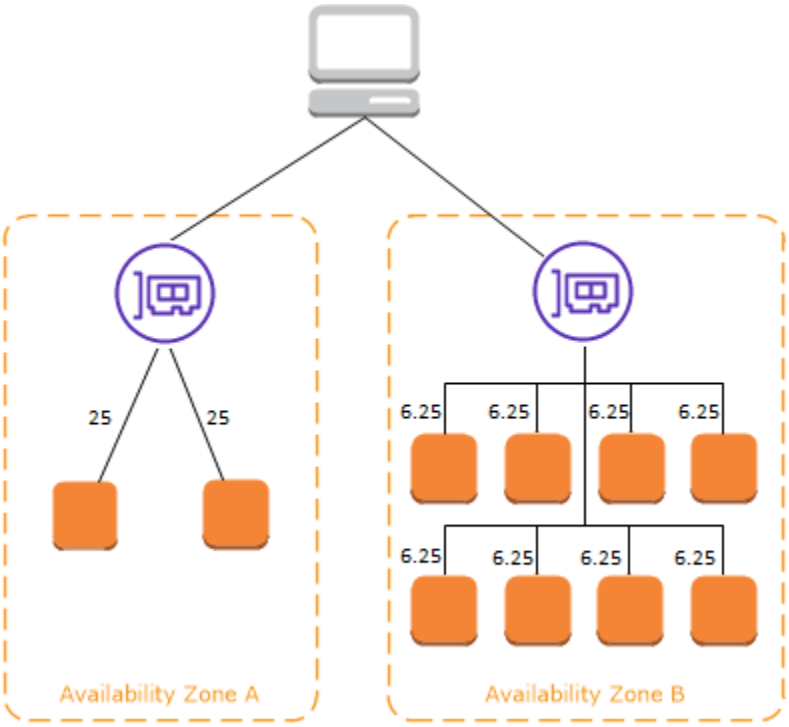
如果启用了跨区域负载均衡，则 10 个目标中的每个目标接收 10% 的流量。这是因为每个负载均衡器节点可将其 50% 的客户端流量路由到所有 10 个目标。



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。



对于应用程序负载均衡器，跨可用区负载均衡始终在负载均衡器级别启用。在目标组级别，可以禁用跨可用区负载均衡。有关更多信息，请参阅《应用程序负载均衡器用户指南》中的关闭跨可用区负载均衡。

对于 Network Load Balancer 和 Gateway Load Balancer，默认情况下会禁用跨区域负载均衡。创建负载均衡器后，您随时可以启用或禁用跨区域负载均衡。

在创建经典负载均衡器时，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。使用时 AWS Management Console，默认情况下会选择启用跨区域负载平衡的选项。创建经典负载均衡器后，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《经典负载均衡器用户指南》中的启用跨区域负载均衡。

可用区转移

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

当您启动可用区转移时，负载均衡器会停止向受影响的可用区发送这些资源的流量。Route 53 ARC 会立即创建可用区转移。但是，可能需要很短时间（通常长达几分钟）才能完成受影响可用区中正在进行的现有连接。有关更多信息，请参阅《Amazon Route 53 应用程序恢复控制器开发人员指南》中的可用区转移的工作原理：运行状况检查和区域 IP 地址。

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

在使用可用区转移之前，请查看以下内容：

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

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

请求路由

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。对于网络负载均衡器，Elastic Load Balancing 将为您启用的每个可用区创建一个网络接口，并使用该网络接口来获取静态 IP 地址。在您创建网络负载均衡器时，可以选择将一个弹性 IP 地址关联到每个网络接口。

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 条目还指定了 60 秒的 time-to-live (TTL)。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。

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。

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 经典负载均衡器，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

经典负载均衡器会使用预打开连接，但 Application Load Balancer 不会使用预打开连接。经典负载均衡器和 Application Load Balancer 均使用多路复用连接。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-alive` 标头。

对于前端连接，Application Load Balancer 和经典负载均衡器支持管道化 HTTP。对于后端连接它们均不支持管道化 HTTP。

应用程序负载均衡器支持以下 HTTP 请求方法：GET、HEAD、POST、PUT、DELETE、OPTIONS 和 PATCH。

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 连接最多可并行发送 128 个请求。应用程序负载均衡器还支持从 HTTP 升级到。 WebSockets但是，如果连接升级，Application Load Balancer 侦听器路由规则和 AWS WAF 集成将不再适用。

默认情况下，Application Load Balancer 在后端连接上使用 HTTP/1.1（负载均衡器连接到已注册的目标）。但是，您可以通过协议版本使用 HTTP/2 或 gRPC 将请求发送到目标。有关更多信息，请参阅协议版本。默认情况下，`keep-alive` 标头在后端连接上受支持。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。主机标头包含负载均衡器的 DNS 名称。

对于前端连接（客户端到负载均衡器），经典负载均衡器支持以下协议：HTTP/0.9、HTTP/1.0 和 HTTP/1.1。默认情况下，它们在后端连接（已注册目标的负载均衡器）上使用 HTTP/1.1。默认情况下，`keep-alive` 标头在后端连接上受支持。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。主机标头包含负载均衡器节点的 IP 地址。

HTTP 标头

Application Load Balancer 和经典负载均衡器会将 X-Forwarded-For、X-Forwarded-Proto 和 X-Forwarded-Port 标头自动添加到请求。

应用程序负载均衡器将 HTTP 主机标头中的主机名转换为小写，然后再将其发送到目标。

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 和经典负载均衡器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。

当使用 HTTP/1.1 的应用程序负载均衡器和经典负载均衡器收到 Expect: 100-Continue 标头时，它们会立即以 HTTP/1.1 100 Continue 响应，而不会测试内容长度标头。Expect: 100-Continue 请求标头不会转发到其目标。

使用 HTTP/2 时，应用程序负载均衡器不支持来自客户端请求的 Expect: 100-Continue 标头。应用程序负载均衡器不会以 HTTP/2 100 Continue 响应，也不会将此标头转发给其目标。

HTTP 标头限制

应用程序负载均衡器的以下大小限制是无法更改的硬限制：

- 请求行：16K
- 单个标头：16K
- 整个响应标头：32 K
- 整个请求标头：64 K

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。

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。

您的负载均衡器的网络 MTU

最大传输单位（MTU）决定了可以通过网络发送的最大数据包大小（以字节为单位）。连接的 MTU 越大，可在单个数据包中传递的数据越多。以太网帧由数据包（即您发送的实际数据）以及相关网络开销信息组成。通过互联网网关发送的流量具有 1500 的 MTU。这意味着，如果数据包超过 1500 字节，则将其分段以使用多个帧发送，或者如果在 IP 标头中设置 `Don't Fragment`，则将其丢弃。

负载均衡器节点上的 MTU 大小不可配置。Jumbo 帧 (9001 MTU) 在应用程序负载均衡器、网络负载均衡器和经典负载均衡器的负载均衡器节点中是标准的。网关负载均衡器支持 8500 MTU。有关更多信息，请参阅网关负载均衡器用户指南中的最大传输单位 (MTU)。

路径 MTU 是原始主机和接收主机之间的路径所支持的最大数据包大小。路径 MTU 发现 (PMTUD) 用于确定两台设备之间的路径 MTU。如果客户端或目标不支持巨型帧，路径 MTU 发现特别重要。

如果主机发送一个大于接收主机的 MTU 或大于路径上某台设备的 MTU 的数据包，则接收主机或设备将丢弃此数据包，然后返回以下 ICMP 消息：`Destination Unreachable: Fragmentation Needed and Don't Fragment was Set (Type 3, Code 4)`。这将指示传输主机将有效负载拆分为多个较小的数据包，并重新传输。

如果继续丢弃大于客户端或目标接口 MTU 大小的数据包，则可能是路径 MTU 发现 (PMTUD) 不起作用。为了避免这种情况，请确保路径 MTU 发现端到端工作，并且您已在客户端和目标上启用了巨型帧。有关路径 MTU 发现和启用巨型帧的详细信息，请参阅 Amazon EC2 用户指南中的路径 MTU 发现。

Elastic Load Balancing 入门

Elastic Load Balancing 支持以下负载均衡器：Application Load Balancer、Network Load Balancer、Gateway Load Balancer 和经典负载均衡器。您可以选择最适合自己需求的负载均衡器类型。有关更多信息，请参阅产品对比。

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

如果您有现有的经典负载均衡器，则可以迁移到 Application Load Balancer 或 Network Load Balancer。有关更多信息，请参阅 迁移您的经典负载均衡器。

目录

创建 Application Load Balancer

要使用 AWS Management Console 创建 Application Load Balancer，请参阅 Application Load Balancers 用户指南中的 Application Load Balancer 入门。

要使用 AWS CLI 创建 Application Load Balancer，请参阅 Application Load Balancers 用户指南中的使用 AWS CLI 创建 Application Load Balancer。

创建网络负载均衡器

要使用 AWS Management Console 创建 Network Load Balancer，请参阅 Network Load Balancers 用户指南中的Network Load Balancers 入门。

要使用 AWS CLI 创建 Network Load Balancer，请参阅 Network Load Balancers 用户指南中的使用 AWS CLI 创建 Network Load Balancer。

创建网关负载均衡器

要使用 AWS Management Console 创建网关负载均衡器，请参阅网关负载均衡器用户指南中的网关负载均衡器入门。

要使用 AWS CLI 创建网关负载均衡器，请参阅网关负载均衡器用户指南中的使用 AWS CLI 网关负载均衡器入门。

创建经典负载均衡器

要使用 AWS Management Console 创建经典负载均衡器，请参阅 Classic Load Balancers 用户指南中的创建经典负载均衡器。

Elastic Load Balancing 中的安全性

AWS 的云安全性具有优先级最高。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。责任共担模式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措施的有效性。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。您还需要对其它因素负责，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 时应用责任共担模式。其中说明了如何配置 Elastic Load Balancing 以实现您的安全性和合规性目标。您还会了解如何使用其他 AWS 服务以帮助您监控和保护 Elastic Load Balancing 资源。

对于网关负载均衡器，您要负责从设备供应商那里选择和鉴定软件。您必须信任设备软件才能检查或修改来自负载均衡器的流量，负载均衡器在开放系统互连 (OSI) 模型的第 3 层（网络层）运行。列为 Elastic Load Balancing 合作伙伴的设备供应商已与 AWS 集成并已鉴定其提供的设备软件。您可以对该列表中的供应商提供的设备软件给予更高的信任度。但是，AWS 不能保证这些供应商提供的软件的安全性或可靠性。

目录

Elastic Load Balancing 中的数据保护

分担责任模型 AWS 分担责任模型适用于 Elastic Load Balancing 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内

容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得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数据：

- 对每个账户使用 multi-factor authentication（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 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 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API 或软件开发工具包 AWS 服务 使用 Elastic Load Balancin AWS CLI g 或其他 AWS 软件开发工具包的情况。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

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 还会在您对访问日志文件进行访问时对其进行解密。每个日志文件都使用唯一的密钥进行加密，该密钥本身使用定期轮换的 KMS 密钥进行加密。

传输中加密

Elastic Load Balancing 通过在负载均衡器上终止来自客户端的 HTTPS 和 TLS 流量，从而简化了构建安全 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。您可以使用 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。经典负载均衡器同时支持 HTTPS 和 TLS 侦听器。

适用于 Elastic Load Balancing 的 Identity and Access Management

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制可以通过身份验证（登录）和授权（具有权限）使用 Elastic Load Balancing 资源的人员。您可以使用 IAM AWS 服务 ，无需支付额外费用。

内容

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Elastic Load Balancing 中所做的工作。

服务用户 - 如果您使用 Elastic Load Balancing 服务来完成工作，您的管理员会为您提供所需的凭证和权限。当您使用更多 Elastic Load Balancing 功能来完成工作时，您可能需要其他权限。了解如何管理访问权限有助于您向管理员请求适合的权限。

服务管理员 – 如果您在公司负责管理 Elastic Load Balancing 资源，您可能具有 Elastic Load Balancing 的完全访问权限。您有责任确定您的服务用户应访问哪些 Elastic Load Balancing 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。

IAM 管理员 – 如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 Elastic Load Balancing 的访问权限的详细信息。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建帐户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和

应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM 策略。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表（ACL）概览。

其它策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 - 权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界

的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。

- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 AWS Organizations 用户指南中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

Elastic Load Balancing 如何与 IAM 一起工作

在使用 IAM 管理对 Elastic Load Balancing 的访问权限之前，您应该了解哪些 IAM 功能可与 Elastic Load Balancing 配合使用。

可与 Elastic Load Balancing 配合使用的 IAM 功能

IAM 功能	Elastic Load Balancing 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACL	否
ABAC（策略中的标签）	是
临时凭证	是

IAM 功能	Elastic Load Balancing 支持
主体权限	是
服务角色	否
服务相关角色	是

Elastic Load Balancing 基于身份的策略

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM 策略。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Elastic Load Balancing 内基于资源的策略

支持基于资源的策略	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

Elastic Load Balancing 的策略操作

支持策略操作	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Elastic Load Balancing 操作的列表，请参阅《服务授权参考》中的 Elastic Load Balancing 定义的操作。

Elastic Load Balancing 中的策略操作在操作前使用以下前缀：

```
elasticloadbalancing
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
    "elasticloadbalancing:action1",
    "elasticloadbalancing:action2"
]
```

您也可以使用通配符（*）指定多个操作。例如，要指定以单词 `Describe` 开头的所有操作，包括以下操作：

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

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

- 应用程序负载均衡器、网络负载均衡器和网关负载平衡器 — API 参考版本 2015-12-01
- 经典负载均衡器— API 参考版本 2012-06-01

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。

Elastic Load Balancing 的策略资源

支持策略资源	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

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

某些 Elastic Load Balancing API 操作支持多个资源。要在单个语句中指定多个资源，请使用逗号分隔 ARN。

```
"Resource": [
    "resource1",
    "resource2"
]
```

要查看 Elastic Load Balancing 的资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 Elastic Load Balancing 定义的资源。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 Elastic Load Balancing 定义的操作。

Elastic Load Balancing 的策略条件键

支持特定于服务的策略条件键	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅 IAM 用户指南中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Elastic Load Balancing 条件键的列表，请参阅《服务授权参考》中的 Elastic Load Balancing 的条件键。要了解您可以对哪些操作和资源使用条件键，请参阅 Elastic Load Balancing 定义的操作。

elasticloadbalancing:ResourceTag 条件键

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

elasticloadbalancing:ListenerProtocol 条件键

elasticloadbalancing:ListenerProtocol条件键可用于定义可以创建和使用的侦听器类型的条件。以下操作支持此条件键：

API 版本 2015-12-01

- `CreateListener`
- `ModifyListener`

API 版本 2012-06-01

- `CreateLoadBalancer`
- `CreateLoadBalancerListeners`

该策略适用于应用程序负载均衡器、网络负载均衡器和传统负载均衡器。以下是一个策略示例，该策略仅允许用户为其监听器选择一个指定的协议。

支持的协议：

- HTTPS
- HTTP
- TCP
- SSL
- TLS
- UDP
- TCP_UDP

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateListener",
            "elasticloadbalancing:ModifyListener"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals":{
                    "elasticloadbalancing:ListenerProtocol": [
                    "HTTPS",
                    "TLS"
                    ]
            },
```

```
        }
```

elasticloadbalancing:SecurityPolicy 条件键

elasticloadbalancing:SecurityPolicy条件密钥可用于在负载均衡器上定义和强制执行特定安全策略的条件。以下操作支持此条件键：

API 版本 2015-12-01

- CreateListener
- ModifyListener

API 版本 2012-06-01

- CreateLoadBalancerPolicy
- SetLoadBalancerPoliciesOfListener

该策略适用于应用程序负载均衡器、网络负载均衡器和传统负载均衡器。以下是一个策略示例，该策略仅允许用户为其负载均衡器选择一个指定的安全策略。

```
"Resource": [
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateListener",
            "elasticloadbalancing:ModifyListener"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals":{
                "elasticloadbalancing:SecurityPolicy": [
                    "ELBSecurityPolicy-TLS13-1-2-2021-06",
                    "ELBSecurityPolicy-TLS13-1-2-Res-2021-06",
                    "ELBSEcurityPolicy-TLS13-1-1-2021-06"
                ]
            },
        }
]
```

`elasticloadbalancing:Scheme` 条件键

`elasticloadbalancing:Scheme`条件键可用于定义在创建负载均衡器期间可以选择哪个方案的条件。以下操作支持此条件键：

API 版本 2015-12-01

- `CreateLoadBalancer`

API 版本 2012-06-01

- `CreateLoadBalancer`

该策略适用于应用程序负载均衡器、网络负载均衡器和传统负载均衡器。以下是一个策略示例，该策略仅允许用户为其负载均衡器选择一个指定的方案。

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action":"elasticloadbalancing:CreateLoadBalancer",
        "Resource": "*",
        "Condition": {
            "StringEquals":{
                "elasticloadbalancing:Scheme": "internal"
            },
        }
```

`elasticloadbalancing:Subnet` 条件键

> **Important**
>
> Elastic Load Balancing 接受子网 ID 的所有大写形式。但是，请务必使用适当的不区分大小写的条件运算符。`StringEqualsIgnoreCase`

`elasticloadbalancing:Subnet`条件密钥可用于定义可以创建哪些子网并将其连接到负载均衡器的条件。以下操作支持此条件键：

API 版本 2015-12-01

- `CreateLoadBalancer`

- SetSubnets

API 版本 2012-06-01

- CreateLoadBalancer
- AttachLoadBalancerToSubnets

该策略适用于应用程序负载均衡器、网络负载均衡器、网关负载均衡器和传统负载均衡器。以下是一个策略示例，该策略仅允许用户为其负载均衡器选择一个指定的子网。

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateLoadBalancer",
            "elasticloadbalancing:SetSubnets"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEqualsIgnoreCase":{
                "elasticloadbalancing:Subnet": [
                    "subnet-01234567890abcdef",
                    "subnet-01234567890abcdeg "
                ]
            },
        }
```

elasticloadbalancing:SecurityGroup 条件键

> **Important**
>
> Elastic Load Balancing 接受 ID 的所有大写形式 SecurityGroup 。但是，请务必使用适当的不区分大小写的条件运算符。StringEqualsIgnoreCase

elasticloadbalancing:SecurityGroup条件密钥可用于定义哪些安全组可以应用于负载均衡器的条件。以下操作支持此条件键：

API 版本 2015-12-01

- CreateLoadBalancer

- SetSecurityGroups

API 版本 2012-06-01

- CreateLoadBalancer
- ApplySecurityGroupsToLoadBalancer

该策略适用于应用程序负载均衡器、网络负载均衡器和传统负载均衡器。以下是一个策略示例，该策略仅允许用户为其负载均衡器选择一个指定的安全组。

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateLoadBalancer",
            "elasticloadbalancing:SetSecurityGroup"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEqualsIgnoreCase":{
                "elasticloadbalancing:SecurityGroup": [
                    "sg-51530134",
                    "sg-51530144",
                    "sg-51530139"
                ]
            },
        }
```

Elastic Load Balancing 中的 ACL

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

具有 Elastic Load Balancing 的 ABAC

支持 ABAC（策略中的标签）	是

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为 Yes（是）。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为 Partial（部分）。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时凭证与 Elastic Load Balancing 配合使用

支持临时凭证	是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Elastic Load Balancing 的跨服务主体权限

支持转发访问会话 (FAS)	是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下

游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Elastic Load Balancing 的服务角色

支持服务角色	否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

Elastic Load Balancing 的服务相关角色

支持服务相关角色	是

服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 Elastic Load Balancing 服务相关角色的详细信息，请参阅 Elastic Load Balancing 服务相关角色。

Elastic Load Balancing API 权限

您必须向用户授予调用所需 Elastic Load Balancing API 操作的权限。此外，对于某些 Elastic Load Balancing 操作，您必须授予用户从 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

在创建过程中为资源添加标签的 Elastic Load Balancing API 权限

为使用户在创建过程中为资源添加标签，他们必须具有使用创建该资源的操作（如 elasticloadbalancing:CreateLoadBalancer 或 elasticloadbalancing:CreateTargetGroup）的权限。如果在资源创建操作中指定标签，则需要在 elasticloadbalancing:AddTags 操作上执行额外的授权，以验证用户是否具备为所创建资源应用标签的权限。因此，用户还必须具有使用 elasticloadbalancing:AddTags 操作的显式权限。

在 elasticloadbalancing:AddTags 操作的 IAM policy 定义中，可使用带有 Condition 条件键的 elasticloadbalancing:CreateAction 元素，为创建资源的操作授予添加标签的权限。

如下的示例演示了一个策略，其允许用户创建目标组并在创建过程中向其应用任何标签。用户无权标记任何现有资源 (他们无法直接调用 elasticloadbalancing:AddTags 操作)。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "elasticloadbalancing:AddTags"
```

```
      ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
             "elasticloadbalancing:CreateAction" : "CreateTargetGroup"
          }
       }
    }
  ]
}
```

同样，下面的策略允许用户创建负载均衡器并在创建过程中应用标签。用户无权标记任何现有资源 (他们无法直接调用 elasticloadbalancing:AddTags 操作)。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "elasticloadbalancing:AddTags"
      ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
             "elasticloadbalancing:CreateAction" : "CreateLoadBalancer"
          }
       }
    }
  ]
}
```

仅当用户在资源创建操作中应用了标签时，系统才会评估 elasticloadbalancing:AddTags 操作。因此，如果未在此请求中指定任何标签，则拥有创建资源权限 (假定没有标记条件) 的用户

无需具备使用 elasticloadbalancing:AddTags 操作的权限。但是，如果用户不具备使用 elasticloadbalancing:AddTags 操作的权限而又试图创建带标签的资源，则请求将失败。

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AWSServiceRoleForElasticLoadBalancing为的服务相关角色代表您调用以下操作：

- ec2:AssignIpv6Addresses
- ec2:AssignPrivateIpAddresses
- ec2:AssociateAddress
- ec2:AttachNetworkInterface
- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateNetworkInterface
- ec2:CreateSecurityGroup
- ec2:DeleteNetworkInterface
- ec2:DescribeAccountAttributes
- ec2:DescribeAddresses
- ec2:DescribeClassicLinkInstances
- ec2:DescribeCoipPools
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcClassicLink
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DetachNetworkInterface

- ec2:DisassociateAddress
- ec2:GetCoipPoolUsage
- ec2:ModifyNetworkInterfaceAttribute
- ec2:ReleaseAddress
- ec2:UnassignIpv6Addresses
- logs:CreateLogDelivery
- logs:DeleteLogDelivery
- logs:GetLogDelivery
- logs:ListLogDeliveries
- logs:UpdateLogDelivery
- outposts:GetOutpostInstanceTypes

AWSServiceRoleForElasticLoadBalancing信任该elasticloadbalancing.amazonaws.com服务来代替该角色。

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或目标组时为您创建此角色。

要让 Elastic Load Balancing 用户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，则会在您的 AWS 账户AWSServiceRoleForElasticLoadBalancing中创建 Elastic Load Balancing。有关更多信息，请参阅 IAM 用户指南中的我的 AWS 账户中出现了一个新角色。

编辑服务相关角色

您可以编辑AWSServiceRoleForElasticLoadBalancing使用 IAM 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，我们建议您将其删除AWSServiceRoleForElasticLoadBalancing。

只有在删除账户中的所有负载均衡器后，才能删除此服务相关角色。 AWS 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 Application Load Balancer、删除 Network Load Balancer 和删除经典负载均衡器。

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。

删除后，如果您创建了负载均衡器 AWSServiceRoleForElasticLoadBalancing，Elastic Load Balancing 会再次创建该角色。

AWS Elastic Load Balancing 托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略： AWSElasticLoadBalancingClassicServiceRolePolicy

该策略包括 Elastic Load Balancing（Classic Load Balancer）代表您调用其他 AWS 服务所需的所有权限。服务相关角色已预先定义。使用预定义角色，您不必手动添加 Elastic Load Balancing 代表您完成操作所需的权限。您不能附加、分离、修改或删除此策略。

要查看此策略的权限，请参阅《AWS 托管策略参考》AWSElasticLoadBalancingClassicServiceRolePolicy中的。

AWS 托管策略： AWSElasticLoadBalancingServiceRolePolicy

此策略包含 Elastic Load Balancing 代表您调用其他 AWS 服务所需的所有权限。服务相关角色已预先定义。使用预定义角色，您不必手动添加 Elastic Load Balancing 代表您完成操作所需的权限。您不能附加、分离、修改或删除此策略。

要查看此策略的权限，请参阅《AWS 托管策略参考》AWSElasticLoadBalancingServiceRolePolicy中的。

AWS 托管策略： ElasticLoadBalancingFullAccess

该策略允许用户完全访问 Elastic Load Balancing 服务，并通过 AWS 管理控制台对其他服务的有限访问权限。

要查看此策略的权限，请参阅《AWS 托管策略参考》ElasticLoadBalancingFullAccess中的。

AWS 托管策略： ElasticLoadBalancingReadOnly

此策略提供对 Elastic Load Balancing 和相关服务的只读访问权限

要查看此策略的权限，请参阅《AWS 托管策略参考》ElasticLoadBalancingReadOnly中的。

Elastic Load Balancing 更新 AWS 了托管策略

查看自该服务开始跟踪这些更改以来，Elastic Load Balancing AWS 托管策略更新的详细信息。

更改	描述	日期
AWS 托管策略： ElasticLoadBalancingFullAccess – 对现有策略的更新	Elastic Load Balancing 添加了一个新的操作来授予使用可用区转移的权限。此操作已添加到 Elastic Load Balancing 完全访问策略中。它与 `arc-zonal-shift:*` API 操作相关联。	2022 年 11 月 28 日
AWS 托管策略： ElasticLoadBalancingReadOnly – 对现有策略的更新	Elastic Load Balancing 添加了一个新的操作来授予使用可用区转移的权限。此操作已添加到 Elastic Load Balancing 只读策略。它与 `arc-zonal-shift:GetManagedResource` 、`arc-zonal-shift:ListManagedResources` 和 `arc-zonal-shift:ListZonalShifts` 操作相关联。	2022 年 11 月 28 日
AWS 托管策略： AWSElasticLoadBalancingServiceRolePolicy – 对现有策略的更新	Elastic Load Balancing 添加了一个新的操作来授予使用对等连接的权限。此操作已添加到适用于 Elastic Load Balancing 控制面板的服务相关角色策略中。它与 `ec2:DescribeVpcPeeringConnections` API 操作关联。	2021 年 10 月 11 日

更改	描述	日期
AWS 托管策略： ElasticLoadBalancingFullAccess – 对现有策略的更新	Elastic Load Balancing 添加了一个新的操作来授予使用对等连接的权限。此操作已添加到 Elastic Load Balancing 完全访问策略中。它与 `ec2:DescribeVpcPeeringConnections` API 操作关联。	2021 年 10 月 11 日
AWS 托管策略： AWSElasticLoadBalancingClassicServiceRolePolicy – 对现有策略的更新	Elastic Load Balancing 为经典负载均衡器添加了服务相关角色策略（用于控制面板）。此更新适用于版本 2（默认模式）。	2019 年 10 月 7 日
AWS 托管策略： ElasticLoadBalancingReadOnly	提供对 Elastic Load Balancing 和相关服务的只读访问。这是版本 1（默认模式）。	2018 年 9 月 20 日
Elastic Load Balancing 开始跟踪更改	Elastic Load Balancing 开始跟踪其 AWS 托管策略的更改。	2021 年 7 月 23 日

Elastic Load Balancing 的合规性验证

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全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，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

Elastic Load Balancing 中的故障恢复能力

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恢复：

- 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 结合使用，以在一个或多个 AWS 区域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集群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 开发人员指南。

Elastic Load Balancing 中的基础设施安全性

作为一项托管式服务，弹性负载均衡受 AWS 全球网络安全保护。有关 AWS 安全服务以及 AWS 如何保护基础设施的信息，请参阅 AWS 云安全。要按照基础设施安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的基础设施保护。

您可以使用 AWS 发布的 API 调用，以通过网络访问 Elastic Load Balancing。客户端必须支持以下内容：

- 传输层安全性协议（TLS） 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。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 主体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。

要使用私有 IP 地址从 VPC 调用 Elastic Load Balancing API，请使用 AWS PrivateLink。有关更多信息，请参见 使用接口端点访问 Elastic Load Balancing（AWS PrivateLink）。

控制网络流量

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：

- 使用安全侦听器支持客户端和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。经典负载均衡器同时支持 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) 或者 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。
- 配置 Application Load Balancer 和经典负载均衡器的安全组，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 Application Load Balancer，以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 Application Load Balancer 对用户进行身份验证。
- 将 AWS WAF 与 Application Load Balancer 结合使用，根据 Web 访问控制列表 (Web ACL) 中的规则允许或阻止请求。

使用接口端点访问 Elastic Load Balancing（AWS PrivateLink）

您可以通过创建接口 VPC 终端节点在 Virtual Private Cloud (VPC) 与 Elastic Load Balancing API 之间建立私有连接。您可以使用此连接从 VPC 调用 Elastic Load Balancing API，而无需将互联网网关、NAT 实例或 VPN 连接附加到您的 VPC。终端节点提供了与用于创建和管理负载均衡器的 2015-12-01 版和 2012-06-01 版 Elastic Load Balancing API 的可靠、可扩展连接。

接口 VPC 端点由 AWS PrivateLink 提供支持，此功能使用私有 IP 地址在应用程序与 AWS 服务 之间进行通信。有关更多信息，请参阅AWS PrivateLink。

限制

AWS PrivateLink 不支持包含超过 50 个侦听器的 Network Load Balancer。

为 Elastic Load Balancing 创建接口终端节点

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

```
com.amazonaws.region.elasticloadbalancing
```

有关更多信息，请参阅 AWS PrivateLink 指南中的创建接口端点。

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，以控制对 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 AWS PrivateLink 指南中的使用端点策略控制对服务的访问权限。

迁移您的经典负载均衡器

Elastic Load Balancing 支持以下类型的负载均衡器：应用程序负载均衡器、网络负载均衡器、网关负载均衡器和经典负载均衡器。有关每种负载均衡器类型的不同功能的信息，请参阅 Elastic Load Balancing 产品对比。

您也可以选择将 VPC 中的现有 Classic 负载均衡器迁移到应用程序负载均衡器或网络负载均衡器。

从经典负载均衡器迁移的好处

每种类型的负载均衡器都有自己独特的特性、功能和配置。查看每种负载均衡器的优点，以帮助确定哪一种最适合您。

Application Load Balancer

使用应用程序负载均衡器代替 Classic 负载均衡器具有以下好处：

Support for：

- 路径条件、主机条件和 HTTP 标头条件。
- 将请求从一个 URL 重定向到另一个 URL，并将请求路由到单个 EC2 实例上的多个应用程序。
- 返回自定义 HTTP 响应。
- 通过 IP 地址注册目标，并将 Lambda 函数注册为目标。包括负载均衡器的 VPC 之外的目标。
- 通过企业或社交身份对用户进行身份验证。
- 亚马逊弹性容器服务 (Amazon ECS) Service 容器化应用程序。
- 独立监控每项服务的运行状况。

访问日志包含其他信息，并以压缩格式存储。

提高了负载均衡器的整体性能。

Network Load Balancer

使用网络负载均衡器代替 Classic 负载均衡器具有以下好处：

Support for：

- 静态 IP 地址，允许为负载均衡器启用的每个子网分配一个弹性 IP 地址。

- 按 IP 地址注册目标，包括负载均衡器的 VPC 之外的目标。
- 将请求路由到单个 EC2 实例上的多个应用程序。
- 亚马逊弹性容器服务 (Amazon ECS) Service 容器化应用程序。
- 独立监控每项服务的运行状况。

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。

使用迁移向导进行迁移

迁移向导使用 Classic Load Balancer 的配置来创建等效的应用程序负载均衡器或网络负载均衡器。与其他方法相比，它减少了迁移 Classic Load Balancer 所需的时间和精力。

> **Note**
>
> 向导将创建一个新的负载均衡器。该向导不会将现有的 Classic Load Balancer 转换为应用程序负载均衡器或网络负载均衡器。您必须手动将流量重定向到新创建的负载均衡器。

限制

- 新负载均衡器的名称不能与同一区域中相同类型的现有负载均衡器的名称相同。
- 如果 Classic Load Balancer 有任何标签的密钥中包含`aws:`前缀，则不会迁移这些标签。

迁移到 Application Load Balancer 时

- 如果 Classic Load Balancer 只有一个子网，则必须指定第二个子网。
- 如果 Classic Load Balancer 有使用 TCP 运行状况检查的 HTTP/HTTPS 侦听器，则运行状况检查协议将更新为 HTTP，路径设置为 “/”。
- 如果 Classic Load Balancer 的 HTTPS 侦听器使用自定义或不支持的安全策略，则迁移向导将使用新的负载均衡器类型的默认安全策略。

迁移到 Network Load Balancer 时

- 以下实例类型不会在新目标组中注册：
  C1、CC1、CC2、CG1、CG2、CR1、CS1、G1、G2、HI1、HS1、M1、M2、M3、T1、M2、M3、T1

- Classic Load Balancer 中的某些运行状况检查设置可能无法转移到新的目标组。这些案例将在迁移向导的摘要部分中显示为更改。
- 如果 Classic Load Balancer 有 SSL 侦听器，则迁移向导会使用 SSL 侦听器中的证书和安全策略创建 TLS 侦听器。

迁移向导进程

使用迁移向导迁移 Classic Load Balancer

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格上的负载均衡下，选择负载均衡器。
3. 选择要迁移的 Classic Load Balancer。
4. 在负载均衡器详细信息部分，选择启动迁移向导。
5. 选择 “迁移到 Application Load Balancer” 或 “迁移到 Network Load Balancer”，打开迁移向导。
6. 在名称新负载均衡器下，在负载均衡器名称中输入您的新负载均衡器的名称。
7. 在 “命名新目标组并查看目标” 下，在目标组名称中输入新目标组的名称。
8. （可选）在 “目标” 下，您可以查看将在新目标组中注册的目标实例。
9. （可选）在 Review 标签下，您可以查看将应用于新负载均衡器的标签
10. 在 App lication Load Balancer 的摘要或 Network Load Balancer 的摘要下，查看并验证迁移向导分配的配置选项。
11. 对配置摘要感到满意后，选择创建应用程序负载均衡器或创建网络负载均衡器以开始迁移。

使用负载平衡器复制实用程序进行迁移

该 AWS GitHub 页面上的 Elastic Load Balancing Tools 存储库中提供了负载均衡器复制工具。

资源

- Elastic 负载平衡工具
- Classic Load Balancer to Application 负载平衡器复制实用程序
- Classic Load Balancer to Network 负载平衡器复制实用程序

手动迁移您的负载均衡器

以下信息提供了基于 VPC 中的现有经典负载均衡器手动创建新的 Application Load Balancer 或 Network Load Balancer 的常规说明。您可以使用 AWS Management Console AWS CLI、或 AWS SDK 进行迁移。有关更多信息，请参阅 Elastic Load Balancing 入门。

在迁移过程完成后，您就可以利用新负载均衡器的功能了。

手动迁移流程

步骤 1：创建新负载均衡器

创建配置等效于经典负载均衡器的负载均衡器以进行迁移。

1. 创建具有与经典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。
2. 使用与经典负载均衡器相同的运行状况检查设置为负载均衡器创建一个目标组。
3. 请执行下列操作之一：
   - 如果您的经典负载均衡器已附加到 Auto Scaling 组，请将目标组附加到 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。
4. 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，则可指定您为经典负载均衡器所指定的同一证书。建议您使用默认安全策略。
5. 如果您的经典负载均衡器具有标签，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

在向新负载均衡器注册您的实例后，您可以开始将流量从旧负载均衡器重定向到新负载均衡器的过程。这使您能够测试新的负载均衡器，同时将应用程序可用性风险降至最低。

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，浏览器会显示您应用程序的默认页面。
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；对于您的旧负载均衡器的现有 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% 的流量定向到旧负载均衡器。
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 time-to-live (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 秒内将流量路由到旧负载均衡器。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，您可以删除旧负载均衡器的 DNS 记录。

步骤 3：更新策略、脚本和代码

如果要将经典负载均衡器迁移到 Application Load Balancer 或 Network Load Balancer，请务必执行以下操作：

- 将使用 API 版本 2012-06-01 的 IAM 策略更新为使用版本 2015-12-01。
- 更新使用`AWS/ELB`命名空间中 CloudWatch 指标的进程，以使用`AWS/ApplicationELB`或`AWS/NetworkELB`命名空间中的指标。
- 更新使用命令来使用aws elb AWS CLI 命令的脚本。aws elbv2 AWS CLI
- 更新使用`AWS::ElasticLoadBalancing::LoadBalancer`资源来使用`AWS::ElasticLoadBalancingV2`资源的 AWS CloudFormation 模板。
- 将使用 Elastic Load Balancing API 版本 2012-06-01 的代码更新为使用版本 2015-12-01。

资源

- AWS CLI 命令参考中的 elbv2
- Elastic Load Balancing API 参考（2015 年 12 月 1 日版）
- 适用于 Elastic Load Balancing 的 Identity and Access Management
- Application Load Balancer 用户指南中的 Application Load Balancer 指标
- Network Load Balancer 用户指南中的 Network Load Balancer 指标
- 《AWS CloudFormation 用户指南》中的 AWS::ElasticLoadBalancingV2::LoadBalancer

步骤 4：删除旧负载均衡器

您可以在完成以下步骤后删除旧经典负载均衡器：

- 您已将旧负载均衡器的所有流量重定向到新负载均衡器。
- 已完成路由到旧负载均衡器的所有现有请求。

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。