aws

开发人员指南

AWS Global Accelerator

AWS Global Accelerator: 开发人员指南

Table of Contents

什么是 AWS Global Accelerator？

AWS Global Accelerator 是一项服务，您可以在其中创建加速器，以提高本地和 Global 用户的应用程序的性能。根据您选择的加速器的类型，您可以获得额外的好处。

- 通过使用标准加速器，您可以提高全球受众使用的 Internet 应用程序的可用性。使用标准加速器，全球加速器将 AWS 全球网络的流量引导到离客户端最近的区域中的终端节点。
- 通过使用自定义路由加速器，您可以将一个或多个用户映射到多个目标之间的特定目标。

全球加速器是一项全球服务，它支持多个 AWS 区域中的终端节点，这些终端节点在AWS Global 表。

默认情况下，全局加速器为您提供与加速器关联的两个静态 IP 地址。使用标准加速器，您可以将这些入口点配置为 IPv4 地址，而不是使用全局加速器提供的 IP 地址，而是将这些入口点配置为带入全局加速器的 IP 地址。静态 IP 地址是来自 AWS 边缘网络的任意播放的。

> **Important**
>
> 只要加速器存在，静态 IP 地址就会保持分配给您的加速器，即使您禁用了加速器并且它不再接受或路由流量也是如此。但是，当delete加速器，则会丢失分配给它的静态 IP 地址，因此无法再使用它们路由流量。您可以将 IAM 策略（如基于标签的权限）与全局加速器结合使用，以限制有权删除加速器的用户。有关更多信息，请参阅 基于标签的策略。

对于标准加速器，Global Accelerator 使用 AWS 全球网络根据您配置的运行状况、客户端位置和策略将流量路由到最佳区域终端节点，从而提高应用程序的可用性。标准加速器的终端节点可以是网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或位于一个 AWS 区域或多个区域中的弹性 IP 地址。该服务会立即响应运行状况或配置的变化，以确保来自客户端的 Internet 流量始终定向到运行状况良好的终端。

自定义路由加速器仅支持虚拟私有云 (VPC) 子网终端节点类型，并将流量路由到该子网中的私有 IP 地址。

有关当前支持和其他服务的 AWS 区域列表，请参阅AWS Global 表。

主题

- 加速器的类型
- Global Accelerator 边缘服务器的位置和 IP 地址范围
- AWS Global Accelerator 使用案例
- AWS Global Accelerator 速度比较工具
- 如何开始使用 AWS Global Accelerator
- AWS Global Accelerator 中的标签
- AWS Global Accelerator 的定价

AWS Global Accelerator 组件

AWS Global Accelerator 包括以下组件：

静态 IP 地址

全局加速器为您提供了一组两个静态 IP 地址，这些地址是来自 AWS 边缘网络的任意广播。如果您将自己的 IP 地址范围带到 AWS (BYOIP) 以用于 Global Accelerator，则可以改为从自己的池中分配 IP 地址以用于加速器。有关更多信息，请参阅 在 AWS Global Accelerator 中引入您自己的 IP 地址 (BYOIP)。

IP 地址可作为客户端的单个固定入口点。如果您已经为应用程序设置了 Elastic Load Balancing 器、Amazon EC2 实例或弹性 IP 地址资源，您可以轻松地将这些资源添加到全球加速器中的标准加速器中。这允许全局加速器使用静态 IP 地址访问资源。

只要加速器存在，静态 IP 地址就会保持分配给您的加速器，即使您禁用了加速器并且它不再接受或路由流量也是如此。但是，当delete加速器，则会丢失分配给它的静态 IP 地址，因此无法再使用它们路由流量。您可以将 IAM 策略（如基于标签的权限）与全局加速器结合使用，以限制有权删除加速器的用户。有关更多信息，请参阅 基于标签的策略。

加速器

加速器通过 AWS 全球网络将流量引导到终端节点，以提高 Internet 应用程序的性能。每个加速器都包含一个或多个侦听器。

有两种加速器：

- A标准加速器根据多个因素（包括用户的位置、终端节点的运行状况以及您配置的终端节点权重）将流量定向到最佳 AWS 终端节点。这可提高应用程序的可用性和性能。终端节点可以是网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址。

- A自定义路由加速器允许您根据某些使用案例的要求，确定地将多个用户路由到加速器后面的特定 EC2 目标。您可以通过将用户定向到加速器上的唯一 IP 地址和端口（全局加速器已映射到目标）来完成此操作。

有关更多信息，请参阅 加速器的类型。

DNS 名称

Global Accelerator 为每个加速器分配默认域名系统 (DNS) 名称，类似于`a1234567890abcdef.awsglobalaccelerator.com`，它指向全局加速器分配给您的静态 IP 地址或您从自己的 IP 地址范围中选择的静态 IP 地址。根据使用案例，您可以使用加速器的静态 IP 地址或 DNS 名称将流量路由到加速器，或者设置 DNS 记录以使用自己的自定义域名路由流量。

网络区

网络区域为来自唯一 IP 子网的加速器的静态 IP 地址提供服务。与 AWS 可用区类似，网络区域是一个具有自己一组物理基础设施的隔离单元。配置加速器时，默认情况下，全局加速器会为其分配两个 IPv4 地址。如果某个网络区域中的一个 IP 地址由于某些客户端网络的 IP 地址阻止或网络中断而变得不可用，则客户端应用程序可以重试来自另一个隔离网络区域的健康静态 IP 地址。

Listener

监听程序根据您配置的端口（或端口范围）和协议（或协议）处理从客户端到全局加速器的入站连接。可以为 TCP、UDP 或 TCP 和 UDP 协议配置侦听器。每个监听程序都有一个或多个与其关联的终端节点组，并且流量将转发到其中一个组中的终端节点。通过指定要向其分配流量的区域，可以将终端节点组与监听程序相关联。使用标准加速器，流量将分配到与监听程序关联的终端节点组中的最佳端点。

终端节点组

每个终端节点组都与特定的 AWS 区域关联。终端节点组包括区域中的一个或多个终端节点。使用标准加速器，您可以通过调整名为流量拨打拨打。流量拨号可让您轻松执行性能测试或蓝/绿部署测试，例如，针对不同 AWS 区域的新版本。

Endpoint

终端节点是全局加速器将流量定向到的资源。

标准加速器的终端节点可以是网络负载均衡器、应用程序负载均衡器、EC2 实例或弹性 IP 地址。应用程序负载均衡器终端节点可以是面向 Internet 的，也可以是内部的。标准加速器的流量将根据终端节点的运行状况以及您选择的配置选项（如端点权重）路由到端点。对于每个端点，您可以配置权重，这些权重是可用于指定路由到每个端点的流量比例的数字。例如，这对于在区域内进行性能测试非常有用。

自定义路由加速器的终端节点是具有一个或多个 Amazon EC2 实例的虚拟私有云 (VPC) 子网，这些实例是流量的目标。

AWS Global Accelerator 的工作方式

AWS Global Accelerator 提供的静态 IP 地址可作为客户端的单个固定入口点。使用全球加速器设置加速器时，将静态 IP 地址与一个或多个 AWS 区域中的区域终端节点相关联。对于标准加速器，终端节点包括网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址。对于自定义路由加速器，终端节点是具有一个或多个 EC2 实例的虚拟私有云 (VPC) 子网。静态 IP 地址接受从离用户最近的节点传入 AWS 全球网络的流量。

> **Note**
>
> 如果您将自己的 IP 地址范围带到 AWS (BYOIP) 以用于 Global Accelerator，则可以改为从自己的池中分配静态 IP 地址以用于加速器。有关更多信息，请参阅 在 AWS Global Accelerator 中引入您自己的 IP 地址 (BYOIP)。

从节点位置，根据您配置的加速器类型路由应用程序的流量。

- 对于标准加速器，流量将根据多个因素路由到最佳 AWS 终端节点，包括用户的位置、终端节点的运行状况以及您配置的终端节点权重。
- 对于自定义路由加速器，根据您提供的外部静态 IP 地址和侦听器端口，将每个客户端路由到 VPC 子网中的特定 Amazon EC2 实例和端口。

流量通过监控良好、无拥塞的冗余 AWS 全球网络传输到终端节点。通过最大限度地提高流量在 AWS 网络上的时间，全球加速器可确保流量始终通过最佳网络路径进行路由。

对于某些端点类型（在某些 AWS 区域），您可以选择保留和访问客户端 IP 地址。两种类型的终端节点可以在传入数据包中保留客户端的源 IP 地址：应用程序负载均衡器和 Amazon EC2 实例。全局加速器不支持 Network Load Balancer 器和弹性 IP 地址终端节点的客户端 IP 地址保留。自定义路由加速器上的端点始终保留客户端 IP 地址。

全局加速器会终止来自 AWS 节点位置的客户端的 TCP 连接，并且几乎同时与终端节点建立新的 TCP 连接。这使客户端能够更快地响应时间（更低的延迟）并提高吞吐量。

在标准加速器中，Global Accelerator 会持续监控所有端点的运行状况，并在确定活动端点运行状况不佳时立即开始将流量定向到另一个可用端点。这样，您就可以在 AWS 上为您的应用程序创建高可用性

架构。运行 Health 况检查不与自定义路由加速器一起使用，也不存在故障转移，因为您指定了要将流量路由到的目标。

添加加速器时，您已配置的安全组和 AWS WAF 规则将继续像添加加速器之前那样工作。

如果您希望对全局流量进行精细控制，可以在标准加速器中为终端配置权重。您还可以增加（上拨）或减少（下拨）到特定终端节点组的流量百分比，例如，用于性能测试或堆栈升级。

使用 Global Accelerator 时，请注意以下事项：

- AWS Direct Connect 不会通过公共虚拟接口宣传 AWS Global Accelerator 的 IP 地址前缀。我们建议您不要通过 AWS Direct Connect 公共虚拟接口宣传用于与全球加速器通信的 IP 地址。如果您通过 AWS Direct Connect 公共虚拟接口宣传用于与全球加速器通信的 IP 地址，则会导致流量不对称：通往全球加速器的流量通过互联网进入全球加速器，但返回来到本地的流量网络来自您的 AWS Direct Connect 公共虚拟接口。
- 全球加速器不支持将属于其他 AWS 账户的资源添加为终端节点。

主题

AWS Global Accelerator 中的空闲超时

AWS Global Accelerator 设置空闲超时期限，该期限应用于其连接。超过空闲超时期限后，如果没有发送或接收任何数据，Global Accelerator 将关闭连接。为确保连接保持活动状态，客户端或终端节点必须在空闲超时期结束之前至少发送 1 字节的数据。

网络连接的全局加速器空闲超时取决于连接类型：

- TCP 连接的超时时间为 340 秒。
- UDP 连接的超时时间为 30 秒。

全局加速器继续将流量引导到终端节点，直到达到空闲超时时间，即使终端节点被标记为运行状况不佳。如果需要，全局加速器仅在新连接启动或空闲超时后才会选择新的终端节点。

AWS Global Accelerator 中的静态 IP 地址

您可以使用 Global Accelerator 分配给您的加速器的静态 IP 地址，或者您从自己的 IP 地址池中为标准加速器指定的静态 IP 地址，将 Internet 流量路由到靠近用户所在位置的 AWS 全球网络，而无论其位置如何。对于标准加速器，您可以将地址与网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或在单个 AWS 区域或多个区域中运行的弹性 IP 地址相关联。对于自定义路由加速器，您可以将流量引导到一个或多个区域的 VPC 子网中的 EC2 目标。通过 AWS 全球网络路由流量可提高可用性和性能，因为流量不必通过公共互联网进行多个跃点。通过使用静态 IP 地址，您还可以在多个 AWS 区域的多个终端节点资源之间分配传入的应用程序流量。

此外，使用静态 IP 地址可以更轻松地将应用程序添加到更多区域或在区域之间迁移应用程序。使用固定 IP 地址意味着用户可以在进行更改时使用一致的方式连接到您的应用程序。

如果愿意，您可以将自己的自定义域名与加速器的静态 IP 地址关联起来。有关更多信息，请参阅 将自定义域流量路由到您的加速器。

全球加速器从 Amazon IP 地址池中为您提供静态 IP 地址，除非您将自己的 IP 地址范围带到 AWS，然后从该池中指定静态 IP 地址。(有关更多信息，请参阅 在 AWS Global Accelerator 中引入您自己的 IP 地址 (BYOIP)。) 要在控制台上创建加速器，第一步是通过输入加速器的名称或选择您自己的静态 IP 地址来提示 Global Accelator 预配置静态 IP 地址。要查看创建加速器的步骤，请参阅AWS Global Accelerator 入门。

只要加速器存在，静态 IP 地址就会保持分配给您的加速器，即使您禁用了加速器并且它不再接受或路由流量也是如此。但是，当delete加速器，则会丢失分配给它的静态 IP 地址，因此无法再使用它们路由流量。您可以将 IAM 策略（如基于标签的权限）与全局加速器结合使用，以限制有权删除加速器的用户。有关更多信息，请参阅 基于标签的策略。

通过流量拨号和端点权重进行流量管理

您可以通过两种方式自定义 AWS Global Accelerator 如何使用标准加速器将流量发送到终端节点：

- 更改流量拨号以限制一个或多个终端节点组的流量
- 指定权重以更改流量与组中终端节点的比例

流量拨号的工作原理

对于标准加速器中的每个终端节点组，您可以设置流量拨号来控制发送到终端节点组的通信百分比。百分比仅应用于已定向到终端节点组的流量，而不是所有监听程序流量。

流量拨号限制终端节点组接受的通信部分，表示为定向到该终端节点组的流量百分比。例如，如果您为终端节点组设置流量拨号us-east-1设置为 50（即 50%），并且加速器将 100 个用户请求定向到该终端节点组，则该组只接受 50 个请求。加速器将剩余的 50 个请求定向到其他区域中的终端节点组。

有关更多信息，请参阅 使用流量拨号调整流量。

权重的工作方式

对于标准加速器中的每个端点，您可以指定权重，这些权重是更改加速器路由到每个端点的流量比例的数字。例如，这对于在区域内进行性能测试非常有用。

权重是一个值，用于确定加速器指向终端节点的流量比例。默认情况下，端点的权重为 128，即权重 255 的最大值的一半。

加速器计算终端节点组中终端节点权重的总和，然后根据每个端点权重与总数的比率将流量定向到端点。有关权重的工作方式的示例，请参阅 终端节点权重。

流量拨号和权重影响标准加速器以不同方式服务流量的方式：

- 您可以配置流量拨号终端节点组。通过流量拨号，您可以根据其他因素（如邻近性）“拨打” 加速器已定向到该组的通信量，从而切断一定百分比的流量（或所有流量）。
- 另一方面，您可以使用权重来设置单个终端节点在终端节点组中。权重提供了一种在终端节点组内划分流量的方法。例如，您可以使用权重对区域中的特定终端进行性能测试。

> **Note**
>
> 有关通信拨打和权重如何影响故障切换的更多信息，请参阅运行状况不佳的终端的故障切换。

AWS Global Accelerator 的运行 Health 况检查

对于标准加速器，AWS Global Accelerator 会自动检查与静态 IP 地址关联的终端节点的运行状况，然后仅将用户流量定向到正常的终端节点。

全局加速器包括自动运行的默认运行状况检查，但您可以配置检查和其他选项的时间。如果您已配置自定义运行状况检查设置，则全局加速器将根据您的配置以特定方式使用这些设置。您可以在适用于 Amazon EC2 实例的全局加速器或弹性 IP 地址终端节点中配置这些设置，或者通过在 Elastic Load

Balancing 控制台上配置网络负载均衡器或应用程序负载均衡器的设置来配置这些设置。有关更多信息，请参阅 运行状况检查选项。

将终端节点添加到标准加速器时，它必须通过运行状况检查才能被视为运行状况良好，然后才能将流量定向到该加速器。如果全局加速器没有任何正常的终端节点可以将流量路由到标准加速器中，它会将请求路由到所有端点。

加速器的类型

有两种类型的加速器可用于 AWS Global Accelerator：标准加速器和自定义路由加速器。这两种类型的加速器通过 AWS 全球网络路由流量以提高性能和稳定性，但每种加速器都是针对不同的应用程序需求而设计的。

标准加速器

通过使用标准加速器，您可以提高在应用程序负载均衡器、网络负载均衡器或 Amazon EC2 实例上运行的应用程序的可用性和性能。全球加速器使用标准加速器，基于地理邻近性和终端运行状况跨区域终端节点路由客户端流量。它还允许客户根据流量拨号和终端权重等控件跨终端转移客户端流量。这适用于各种用例，包括蓝色/绿色部署、A/B 测试和多区域部署。若要查看更多用例，请参阅 AWS Global Accelerator 使用案例。

要了解更多信息，请参阅“使用 AWS Global Accelerator 中的标准加速器”。

自定义路由加速器

自定义路由加速器适用于您希望使用自定义应用程序逻辑将一个或多个用户引导到多个特定目的地和端口，同时仍能获得 Global Accelerator 的性能优势的场景。一个例子是 VoIP 应用程序，它们将多个呼叫者分配给特定媒体服务器以启动语音、视频和消息传递会话。另一个例子是在线实时游戏应用程序，您希望根据地理位置、玩家技能和游戏模式等因素将多个玩家分配给游戏服务器上的单个会话。

要了解更多信息，请参阅“在 AWS Global Accelerator 中使用自定义路由加速器”。

根据您的特定需求，您可以创建以下类型的加速器之一，以加快客户流量。

Global Accelerator 边缘服务器的位置和 IP 地址范围

有关 Global Accelerator 边缘服务器位置的列表，请参阅AWS Global Accelerator 目前在哪里部署？部分中的AWS Global Accelerator 常见问题页.

AWS 以 JSON 格式发布其当前的 IP 地址范围。要查看当前范围，请下载ip-ranges.json。有关更多信息，请参阅 。AWS 的 IP 地址范围中的Amazon Web Services 一般参考。

要查找与 AWS Global Accelerator 边缘服务器关联的 IP 地址范围，请在搜索ip-ranges.json对于以下字符串：

```
"service": "GLOBALACCELERATOR"
```

全局加速器条目包括"region": "GLOBAL"是指分配给加速器的静态 IP 地址。如果要通过加速器过滤来自某个区域的存在点 (POP) 的流量，请筛选包含特定地理区域的条目，例如us-*或者eu-*。因此，例如，如果你过滤us-*，您将只看到通过美国（美国）持久性有机污染物的流量。

AWS Global Accelerator 使用案例

使用 AWS Global Accelerator 可帮助您实现各种目标。本节列出了其中一些内容，让您了解如何使用全球加速器来满足您的需求。

扩展以提高应用程序利用率

当应用程序使用率增长时，您需要管理的 IP 地址和终端节点的数量也会增加。全球加速器使您能够向上或向下扩展网络。它允许您将区域资源（如负载均衡器和 Amazon EC2 实例）关联到两个静态 IP 地址。您只需在客户端应用程序、防火墙和 DNS 记录中将这些地址包含在允许列表中一次。借助全球加速器，您可以在 AWS 区域中添加或删除终端节点、运行蓝色/绿色部署以及执行 A/B 测试，而无需更新客户端应用程序中的 IP 地址。这对于您无法经常更新客户端应用程序的 IoT、零售、媒体、汽车和医疗保健使用案例尤其有用。

延迟敏感型应用程序的加速

许多应用程序，特别是在游戏、媒体、移动应用和财务等领域，需要非常低的延迟才能获得卓越的用户体验。为了改善用户体验，Global Accelerator 将用户流量定向到离客户端最近的应用程序端点，从而减少 Internet 延迟和抖动。全局加速器使用 Anycast 将流量路由到最近的节点位置，然后通过 AWS 全球网络将流量路由到最近的区域终端节点。全球加速器快速响应网络性能的变化，以提高用户的应用程序性能。

灾难恢复和多区域恢复

您必须能够依赖您的网络才能使用。您可能正在跨多个 AWS 区域运行应用程序，以支持灾难恢复、更高的可用性、更低的延迟或合规性。如果全球加速器检测到您的应用程序终端节点在主 AWS 区域出现故障，它会立即触发流量重新路由到下一个可用的最近 AWS 区域中的应用程序终端节点。

保护您的应用

将您的 AWS 来源（如应用程序负载均衡器或 Amazon EC2 实例）暴露于公共互联网流量之下，将创造恶意攻击的机会。全局加速器通过掩盖您的来源在两个静态入口点后面来降低攻击风险。默认情况下，这些入口点受到 AWS Shield 的分布式拒绝服务 (DDoS) 攻击的保护。全球加速器使用私有 IP 地址创建与您的 Amazon Virtual Private Cloud 的对等连接，从而将与内部应用程序负载均衡器或私有 EC2 实例的连接保持在公共互联网之外。

提高 VoIP 或在线游戏应用程序的性能

使用自定义路由加速器，您可以将全球加速器的性能优势用于 VoIP 或游戏应用程序。例如，您可以将全球加速器用于将多个玩家分配给单个游戏会话的在线游戏应用程序。对于需要自定义逻辑将用户映射到特定终端节点（如多人游戏或 VoIP 通话）的应用程序，使用全局加速器减少延迟和抖动。您可以使用单个加速器将客户端连接到在单个或多个 AWS 区域中运行的数千个 Amazon EC2 实例，同时保留对哪个客户端被定向到哪个 EC2 实例和端口的完全控制。

AWS Global Accelerator 速度比较工具

您可以使用 AWS Global Accelerator 速度比较工具查看跨 AWS 区域的全球加速器下载速度与直接互联网下载相比。使用此工具，您可以使用浏览器查看使用全局加速器传输数据时的性能差异。您可以选择要下载的文件大小，该工具通过 HTTPS/TCP 从不同区域的应用程序负载均衡器下载文件到浏览器。对于每个区域，您可以看到下载速度的直接比较。

要访问速度比较工具，请将以下 URL 复制到浏览器中：

```
https://speedtest.globalaccelerator.aws
```

Important

当您多次运行测试时，结果可能会有所不同。下载时间可能因全球加速器的外部因素而异，例如您正在使用的最后一英里网络中的连接质量、容量和距离。

如何开始使用 AWS Global Accelerator

您可以使用 API 或 AWS Global Accelerator 控制台开始设置 AWS Global Accelerator。由于全球加速器是一项全球性服务，因此它与特定 AWS 区域无关。请注意，全球加速器是支持多个 AWS 区域中的终端节点的全球服务，但您必须指定美国西部（俄勒冈）地区才能创建或更新加速器。

要开始使用全局加速器，请按照以下常规步骤操作：

1. 选择要创建的加速器的类型：标准加速器或自定义路由加速器。
2. 配置全局加速器的初始设置： 提供加速器的名称。然后，根据您指定的协议和端口（或端口范围），配置一个或多个侦听器以处理来自客户端的入站连接。
3. 为您的加速器配置区域终端节点组： 可以选择一个或多个要添加到侦听器的区域终端节点组。监听程序将请求路由到已添加到终端节点组的终端节点。

   对于标准加速器，全局加速器通过使用为每个终端节点定义的运行状况检查设置来监视组中终端节点的运行状况。对于标准加速器中的每个终端节点组，您可以配置流量拨打拨打百分比来控制终端节点组将接受的流量百分比。百分比仅应用于已定向到终端节点组的流量，而不是所有监听程序流量。默认情况下，所有区域终端节点组的流量拨号设置为 100%。

   对于自定义路由加速器，流量将根据接收流量的侦听器端口，确定性地路由到 VPC 子网中的特定目标。
4. 将终端节点添加到终端节点组： 添加的终端节点取决于加速器的类型。
   - 对于标准加速器，您可以向每个终端节点组添加一个或多个区域资源，如负载均衡器或 EC2 实例终端节点。接下来，您可以通过设置终端节点权重来决定要路由到每个终端节点的流量。
   - 对于自定义路由加速器，您可以添加一个或多个具有数千个 Amazon EC2 实例目标的虚拟私有云 (VPC) 子网。

有关如何使用 AWS Global Accelerator 控制台创建标准加速器或自定义路由加速器的详细步骤，请参阅AWS Global Accelerator 入门。要使用 API 操作，请参阅您可以与 AWS Global Accelerator 一起使用的常见操作和AWS Global Accelerator API 参考。

AWS Global Accelerator 中的标签

标签是用于标识和组织 AWS 资源的词或短语（元数据）。您可以向每个资源添加多个标签，并且每个标签都包含您定义的一个键和一个值。例如，键可能为`environment`，该值可能是`production`。您可以根据添加的标签搜索和筛选您的资源。在 AWS Global Accelerator 中，您可以标记加速器。

以下是在 Global Accelerator 中使用标签的用处的两个示例：

- 使用标签跟踪不同类别的账单信息。为此，请将标签应用于加速器或其他 AWS 资源（如网络负载均衡器、应用程序负载均衡器或 Amazon EC2 实例）并激活标签。AWS 将以逗号分隔值（CSV 文件）格式生成一份成本分配报告，其中包括按活动标签汇总的使用率和成本。您可以设置代表业务类

别 (例如成本中心、应用程序名称或所有者) 的标签，以便整理多种服务的成本。有关更多信息，请参阅 AWS 账单和成本管理用户指南中的使用成本分配标签。

- 使用标签强制实施加速器的基于标签的权限。为此，请创建用于指定标签和标签值以允许或禁止操作的 IAM 策略。有关更多信息，请参阅 基于标签的策略。

有关标记的使用约定和指向其他资源的链接，请参阅标记 AWS 资源中的AWS 一般参考。有关使用标签的提示，请参阅标记最佳实践：AWS 资源标记策略中的AWS 白皮书博客。

有关可以向 Global Accelerator 中资源添加的最大标签数，请参阅AWS Global Accelerator 的配额。

您可以使用 AWS 控制台、AWS CLI 或 Global Accelerator API 添加和更新标签。本章介绍在控制台中使用标记的步骤。有关使用 AWS CLI 和全局加速器 API 处理标签的更多信息（包括 CLI 示例），请参阅AWS Global Accelerator API 参考：

- 创建加速器
- TagResource
- UntagResource
- ListTagsForResource

全局加速器中的标记支持

AWS Global Accelerator 支持对加速器进行标记。

Global Accelerator 支持 AWS Identity Access Management (IAM) 的基于标签的访问控制功能。有关更多信息，请参阅 基于标签的策略。

在 Global Accelerator 中添加、编辑和删除标签

以下过程介绍如何在 Global Accelerator 控制台中为加速器添加、编辑和删除标签。

> **Note**
>
> 您可以使用控制台、AWS CLI 或 Global Accelerator API API 操作添加或删除标签。有关更多信息（包括 CLI 示例），请参阅TagResource中的AWS Global Accelerator API 参考。

在 Global Accelerator 中添加标签、编辑或删除标签

1. 打开全局加速器控制台https://console.aws.amazon.com/globalaccelerator/home。
2. 选择您要为其添加或更新标签的加速器。
3. 在标签部分中，可以执行以下操作：

   添加标签

   选择添加标签，然后输入标签的键和 (可选) 值。

   编辑标签

   更新键和/或值的文本。您也可以清除标签的值，但键是必需的。

   删除标签

   选择Remove值字段右侧。
4. 选择保存更改。

AWS Global Accelerator 的定价

使用 AWS Global Accelerator，您需要为账户中的加速器付费（不管状态为启用或禁用），并支付数据传输费。有关更多信息，请参阅 AWS Global Accelerator 定价。

AWS Global Accelerator 入门

这些教程提供了使用控制台开始使用 AWS Global Accelerator 的步骤。您还可以使用 AWS Global Accelerator API 操作来创建和自定义您的加速器。在本教程的每个步骤中，都有一个指向相应 API 操作的链接，用于以编程方式完成任务。设置自定义路由加速器时，必须将 API 用于某些配置步骤。 ）有关 AWS Global Accelerator API 操作的更多信息，请参阅AWS Global Accelerator API 参考。

> **Tip**
>
> 要了解如何使用全球加速器来提高 Web 应用程序的性能和可用性，请参阅以下自定进度的研讨会：AWS Global Accelerator 研讨会。

全球加速器是一项全球服务，支持多个 AWS 区域中的终端节点，这些终端节点在AWS 区域表。

本章包含两个教程：一个用于创建标准加速器，另一个用于创建自定义路由加速器。要了解有关两种类型的加速器的更多信息，请参阅使用 AWS Global Accelerator 中的标准加速器和在 AWS Global Accelerator 中使用自定义路由加速器。

主题

标准加速器入门

本节介绍使用标准加速器创建将流量路由到最佳终端节点的步骤。

任务

开始前的准备工作

在创建加速器之前，请至少创建一个可以添加为终端节点的资源，以将流量定向到。例如，创建以下命令之一：

- 启动至少一个要添加为终端节点的 Amazon EC2 实例。有关更多信息，请参阅 。创建 EC2 资源并启动 EC2 实例中的适用于 Linux 实例的 Amazon EC2 用户指南。
- （可选）创建一个或多个包含 EC2 实例的网络负载均衡器或应用程序负载均衡器。有关更多信息，请参阅 。创建 Network Load Balancer Application Load Balancer中的适用于网络负载均衡器的用户指南。

创建要添加到 Global Accerator 的资源时，请注意以下事项：

- 当您在全球加速器中添加内部 Application Load Balancer 器或 EC2 实例终端节点时，您可以通过将互联网流量定位在私有子网中，从而使互联网流量直接流入和流出虚拟私有云 (VPC) 中的终端节点。包含负载均衡器或 EC2 实例的 VPC 必须具有互联网网关，以表示 VPC 接受互联网流量。有关更多信息，请参阅 AWS Global Accelerator 中的 VPC 连接安全。
- 全局加速器要求您的路由器和防火墙规则允许来自与 Route 53 运行状况检查程序关联的 IP 地址的入站流量完成 EC2 实例或弹性 IP 地址终端节点的运行状况检查。有关与 Amazon Route 53 运行状况检查程序关联的 IP 地址范围的信息，请参阅目标组的运行状况检查中的Amazon Route 53 开发者指南。

步骤 1: 创建速器

要创建您的加速器，请输入一个名称。

> **Note**
>
> 要使用 API 操作而不是控制台完成此任务，请参阅创建加速器中的AWS Global Accelerator API 参考。

创建速器

1. 打开全局加速器控制台https://console.aws.amazon.com/globalaccelerator/home。
2. 选择创建速器。
3. 提供加速器的名称。

4. (可选) 添加一个或多个标签来帮助您识别全局加速器资源。
5. 选择 Next。

步骤 2: 添加侦听器

创建侦听器（处理从用户到 Global Accerator 的入站连接）。

> **Note**
>
> 要使用 API 操作而不是控制台完成此任务，请参阅CreateListener中的AWS Global Accelerator API 参考。

创建侦听器

1. 在存储库的添加侦听器页面上，输入要与监听程序关联的端口或端口范围。侦听器支持 1-65535 端口。
2. 为您输入的端口选择一个或多个协议。
3. （可选）选择启用客户端关联性。监听程序的客户端关联性意味着全局加速器可确保来自特定源（客户端）IP 地址的连接始终路由到同一终结点。要启用此行为，请在下拉列表中选择源 IP。

   默认值为无，这意味着未启用客户端关联性，并且全局加速器在监听程序的终端节点组中的终端节点之间平均分配流量。

   有关更多信息，请参阅 客户端关联。
4. (可选) 选择添加侦听器添加一个额外的侦听器。
5. 添加完侦听器后，选择下一步。

步骤 3: 添加终端节点组

添加一个或多个终端节点组，每个终端节点组都与特定 AWS 区域相关联。

> **Note**
>
> 要使用 API 操作而不是控制台完成此任务，请参阅创建终端点组中的AWS Global Accelerator API 参考。

添加终端节点组

1. 在存储库的添加终端节点组页面上，在监听程序的部分中，选择区域从下拉列表中选择。
2. (可选)流量拨打中，输入 0 到 100 之间的数字以设置此终端节点组的流量百分比。百分比仅应用于已定向到此终端节点组的流量，而不是所有监听程序流量。默认情况下，终端节点组的流量拨号设置为 100（即 100%）。
3. （可选）对于自定义运行状况检查值，选择配置运行状况检查。配置运行状况检查设置时，全局加速器将使用 EC2 实例和弹性 IP 地址终端节点的运行状况检查设置。对于 Network Load Balancer 和应用程序负载平衡器终端节点，全局加速器使用您已为负载均衡器本身配置的运行状况检查设置。有关更多信息，请参阅 运行状况检查选项。
4. (可选) 选择添加终端节点组为此侦听器或其他侦听器添加其他终端节点组。
5. 选择 Next。

步骤 4: 添加终端节点

添加一个或多个与特定终端节点组关联的终端节点。此步骤不是必需的，但除非终端节点包含在终端节点组中，否则不会将流量定向到区域中的终端节点。

> **Note**
>
> 如果要以编程方式创建加速器，则可以添加终端节点作为添加终端节点组的一部分。有关更多信息，请参阅 。创建终端点组中的AWS Global Accelerator API 参考。

添加终端节点

1. 在存储库的创建终端节点页面上，在端点的部分中，选择终端节点。
2. (可选)权重中，输入一个介于 0 到 255 之间的数字，以设置将流量路由到此终端节点的权重。向终端节点添加权重时，您可以配置 Global Accelerator，以便根据您指定的比例路由流量。默认情况下，所有端点的权重都为 128。有关更多信息，请参阅 终端节点权重。
3. （可选）对于应用程序负载均衡器终端节点，在保留客户端 IP 地址中，选择保留地址。有关更多信息，请参阅 在 AWS Global Accelerator 中保留客户端 IP 地址。
4. (可选) 选择添加终端节点添加更多终端节点。
5. 选择 Next。

在您选择下一步，您将在全局加速器仪表板上看到一条消息，提示您的加速器正在进行中。该过程完成后，仪表板中的加速器状态为处于活动状态。

步骤 5: 测试加速器

采取步骤测试您的加速器，以确保流量被定向到您的终端节点。例如，运行一个 curl 命令（如下所示），替换加速器的静态 IP 地址之一，以显示处理请求的 AWS 区域。如果您为终端设置不同的权重或调整端点组上的流量拨号，这将特别有用。

运行如下所示的 curl 命令，替换加速器的静态 IP 地址之一，调用 IP 地址 100 次，然后输出处理每个请求的位置计数。

```
for ((i=0;i<100;i++)); do  curl http://198.51.100.0/ >> output.txt; done; cat
 output.txt | sort | uniq -c ; rm output.txt;
```

如果您调整了任何端点组上的流量拨号，则此命令可帮助您确认加速器是否将正确百分比的流量定向到不同的组。有关更多信息，请参阅以下博客文章中的详细示例：AWS Global Accelerator 的流量管理。

步骤 6（可选）：删除速器

如果您创建了加速器作为测试，或者您不再使用加速器，则可以将其删除。在控制台上，禁用加速器，然后您可以将其删除。您不必从加速器中删除侦听器和终端节点组。

要使用 API 操作而不是控制台删除加速器，您必须首先删除与加速器关联的所有侦听器和终端节点组，并将其禁用。有关更多信息，请参阅 。删除加速器中的操作AWS Global Accelerator API 参考。

删除终端节点或终端节点组或删除加速器时，请注意以下事项：

- 创建加速器时，全局加速器会为您提供一组两个静态 IP 地址。只要加速器存在，就会将 IP 地址分配给您的加速器，即使您禁用了加速器并且它不再接受或路由流量也是如此。但是，当delete加速器，则会丢失分配给加速器的静态 IP 地址，因此无法再使用它们路由流量。作为最佳做法，请确保您拥有权限，以避免无意中删除加速器。您可以将 IAM 策略与全局加速器（例如，基于标签的权限）结合使用，以限制有权删除加速器的用户。有关更多信息，请参阅 基于标签的策略。
- 如果您在将 EC2 实例从全球加速器的终端节点组中删除之前终止该实例，然后创建另一个具有相同私有 IP 地址的实例，并且运行状况检查通过，则全局加速器将流量路由到新终端节点。如果您不希望发生这种情况，请在终止实例之前从终端节点组中删除 EC2 实例。

删除速器

1. 打开全局加速器控制台https://console.aws.amazon.com/globalaccelerator/home。
2. 选择要删除的加速器。
3. 选择 Edit。
4. 选择禁用加速器，然后选择Save。
5. 选择要删除的加速器。
6. 选择删除速器。
7. 在确认对话框中，选择 Delete (删除)。

自定义路由加速器入门

本节介绍使用自定义路由加速器创建步骤，该加速器将流量确定性路由到 Virtual Private Cloud (VPC) 子网终端节点中的 Amazon EC2 实例目标。

任务

- 开始前的准备工作
- 步骤 1: 创建自定义路由加速器
- 步骤 2: 添加侦听器
- 步骤 3: 添加终端节点组
- 步骤 4: 添加终端节点
- 步骤 5（可选）：删除速器

开始前的准备工作

在创建自定义路由加速器之前，请创建一个资源，您可以将其添加为终端节点，以将流量定向到。自定义路由加速器终端节点必须是 Virtual Private Cloud (VPC) 子网，该子网可以包含多个 Amazon EC2 实例。有关创建资源的说明，请参阅：

- 创建 VPC 子网。有关更多信息，请参阅 。创建和配置 VPC中的AWS Directory Service 管理指南。
- （可选）在 VPC 中启动一个或多个 Amazon EC2 实例。有关更多信息，请参阅 。创建 EC2 资源并启动 EC2 实例中的适用于 Linux 实例的 Amazon EC2 用户指南。

创建要添加到 Global Accerator 的资源时，请注意以下事项：

- 当您在全球加速器中添加 EC2 实例终端节点时，您可以通过将 Internet 流量定位在私有子网中，使其能够直接流入和流出 VPC 中的终端节点。包含 EC2 实例的 VPC 必须具有互联网网关，以表示 VPC 接受互联网流量。有关更多信息，请参阅 AWS Global Accelerator 中的 VPC 连接安全。

步骤 1: 创建自定义路由加速器

> **Note**
>
> 要使用 API 操作而不是控制台完成此任务，请参阅创建自定义路程加速器中的AWS Global Accelerator API 参考。

创建速器

1. 打开全局加速器控制台https://console.aws.amazon.com/globalaccelerator/home。
2. 提供加速器的名称。
3. 适用于加速器类型中，选择自定义路由。
4. （可选）添加一个或多个标签来帮助您识别加速器资源。
5. 选择下一步添加侦听器、终端节点组和 VPC 子网终端节点。

步骤 2: 添加侦听器

创建侦听器（处理从用户到 Global Accerator 的入站连接）。

创建监听程序时指定的范围定义了可用于自定义路由加速器的监听程序端口和目标 IP 地址组合的数量。为了获得最大的灵活性，建议您指定较大的端口范围。您指定的每个侦听程序端口范围必须至少包含 16 个端口。

> **Note**
>
> 要使用 API 操作而不是控制台完成此任务，请参阅创建自定义路程监听器中的AWS Global Accelerator API 参考。

创建侦听器

1. 在存储库的添加侦听器页面上，输入要与监听程序关联的端口或端口范围。侦听器支持 1-65535 端口。
2. 为您输入的端口选择一个或多个协议。
3. (可选) 选择添加侦听器添加一个额外的侦听器。
4. 添加完侦听器后，选择下一步。

步骤 3: 添加终端节点组

添加一个或多个终端节点组，每个终端节点组都与特定 AWS 区域相关联。对于每个端点组，指定一组或多组端口范围和协议。全球加速器使用这些功能将流量引导到该地区子网中的 Amazon EC2 实例。

对于您提供的每个端口范围，您还可以指定要使用的协议：UDP、TCP 或 UDP 和 TCP 同时使用。

> **Note**
>
> 要使用 API 操作而不是控制台完成此任务，请参阅创建自定义路由点组中的AWS Global Accelerator API 参考。

添加终端节点组

1. 在存储库的添加终端节点组页面上，在监听程序的部分中，选择区域。
2. 适用于端口和协议集中，输入 Amazon EC2 实例的端口范围和协议。
   - 输入从端口和至端口指定端口范围。
   - 对于每个端口范围，指定该范围的一个或多个协议。

   端口范围不一定是监听器端口范围的子集，但监听器端口范围内必须有足够的端口总数，以支持指定的端口总数。
3. 选择保存。
4. (可选) 选择添加终端节点组为此侦听器或其他侦听器添加其他终端节点组。
5. 选择 Next。

步骤 4: 添加 VPC 子网终端节点

为此区域终端节点组添加一个或多个 Virtual Private Cloud (VPC) 子网终端节点。自定义路由加速器的终端节点定义了可通过自定义路由加速器接收流量的 VPC 子网。每个子网可以包含一个或多个 Amazon EC2 实例目标。

添加 VPC 子网终端节点时，全局加速器会生成新的端口映射，您可以使用这些映射将流量路由到子网中的目标 EC2 实例 IP 地址。然后，您可以使用全局加速器 API 获取子网所有端口映射的静态列表，并使用映射将流量确定向到特定 EC2 实例。

> **Note**
>
> 此处的步骤显示了如何在控制台中添加终端节点。如果要以编程方式创建加速器，则可以添加带有端点组的终端节点。有关更多信息，请参阅 。创建自定义路由点组中的AWS Global Accelerator API 参考。

添加终端节点

1. 在存储库的添加终端节点页面上，在要向其添加终端节点的终端节点组的部分中，选择终端节点。
2. （可选）执行以下操作之一以启用到子网中 EC2 实例目标的流量：

   - 要允许流量定向到子网上的所有 EC2 终端节点和端口，请选择允许所有流量
   - 要允许通过子网上的特定 EC2 终端节点和端口进行流量，请选择允许流量到特定目标套接字地址。然后指定要允许的 IP 地址和端口或端口范围。最后，选择允许这些目标。

   默认情况下，不允许任何流量对终端节点进行子网。如果您没有选择允许流量的选项，则会拒绝通过子网中的所有目标进行流量。

   > **Note**
   >
   > 如果要启用到子网中特定 EC2 实例和端口的流量，可以通过编程方式执行此操作。有关更多信息，请参阅 。允许自定义路线流量中的AWS Global Accelerator API 参考。

3. 选择 Next。

在您选择下一步，在全局加速器的仪表板上，您将看到一条消息，提示您的加速器正在进行中。该过程完成后，仪表板中的加速器状态为处于活动状态。

步骤 5（可选）：删除速器

如果您创建了加速器作为测试，或者您不再使用加速器，则可以将其删除。在控制台上，禁用加速器，然后您可以将其删除。您不必从加速器中删除侦听器和终端节点组。

要使用 API 操作而不是控制台删除加速器，您必须首先删除与加速器关联的所有侦听器和终端节点组，并将其禁用。有关更多信息，请参阅 。删除自定义路程加速器中的操作AWS Global Accelerator API 参考。

删除加速器时，请注意以下事项：

- 创建加速器时，全局加速器会为您提供一组两个静态 IP 地址。只要加速器存在，就会将 IP 地址分配给您的加速器，即使您禁用了加速器并且它不再接受或路由流量也是如此。但是，当delete加速器，则会丢失分配给加速器的静态 IP 地址，因此无法再使用它们路由流量。作为最佳做法，请确保您拥有权限，以避免无意中删除加速器。您可以将 IAM 策略（如基于标签的权限）与全局加速器结合使用，以限制有权删除加速器的用户。有关更多信息，请参阅 基于标签的策略。

删除速器

1. 打开全局加速器控制台https://console.aws.amazon.com/globalaccelerator/home。
2. 选择要删除的加速器。
3. 选择 Edit。
4. 选择禁用加速器，然后选择Save。
5. 选择要删除的加速器。
6. 选择删除速器。
7. 在确认对话框中，选择 Delete (删除)。

您可以与 AWS Global Accelerator 一起使用的常见操作

本节列出了您可以与全球加速器资源一起使用的常见 AWS Global Accelerator 操作，以及相关文档的链接。

用于标准资源的操作

下表列出了您可以与全局加速器标准加速器一起使用的常见全局加速器操作，以及相关文档的链接。

操作	使用全局加速器控制台	使用全局加速器 API
创建标准加速器	请参阅 标准加速器入门	请参阅 CreateAccelerator
为创建侦听器	请参阅 AWS Global Accelerator 中标准加速器的侦听器	请参阅 CreateListener
为标准加速器创建终端节点组	请参阅 AWS Global Accelerator 中标准加速器的终端节点组	请参阅 CreateEndpointGroup
更新标准加速器	请参阅 AWS Global Accelerator 中的标准加速器	请参阅 UpdateAccelerator
列出您的加速器	请参阅 查看您的加速器	请参阅 ListAccelerator
获取有关加速器的所有信息	请参阅 查看您的加速器	请参阅 DescribeAccelerator
删除加速器	请参阅 创建或更新标准加速器	请参阅 DeleteAccelerator

用于自定义路由资源的操作

下表列出了可用于自定义路由加速器的常见全局加速器操作，以及指向相关文档的链接。

操作	使用全局加速器控制台	使用全局加速器 API
创建自定义路由加速器	请参阅 自定义路由加速器入门	请参阅 CreateCustomRoutingAccelerator
为创建侦听器	请参阅 AWS Global Accelerator 中的自定义路由加速器侦听器	请参阅 CreateCustomRoutingListener
为创建终端节点组	请参阅 AWS Global Accelerator 中自定义路由加速器的终端节点组	请参阅 CreateCustomRoutingEndpointGroup
更新自定义路由加速器	请参阅 AWS Global Accelerator 中的自定义路由加速器	请参阅 UpdateCustomRoutingAccelerator
列出您的自定义路由加速器	请参阅 查看自定义路由加速器	请参阅 ListCustomRoutingAccelerator
获取有关自定义路由加速器的所有信息	请参阅 查看自定义路由加速器	请参阅 DescribeCustomRoutingAccelerator
删除自定义路由加速器	请参阅 创建或更新自定义路由加速器	请参阅 DeleteCustomRoutingAccelerator
获取自定义路由加速器的静态端口映射	不适用	请参阅 ListCustomRoutingPortMappings
允许自定义路由加速器中子网的所有目标流量	请参阅 添加、编辑或删除 VPC 子网终端节点	请参阅 AllowCustomRoutingTraffic
拒绝自定义路由加速器中子网的所有目标通信	请参阅 添加、编辑或删除 VPC 子网终端节点	请参阅 DenyCustomRoutingTraffic

操作	使用全局加速器控制台	使用全局加速器 API
允许流量到达自定义路由加速器中的特定目的地	请参阅 添加、编辑或删除 VPC 子网终端节点	请参阅 AllowCustomRoutingTraffic
拒绝自定义路由加速器中的特定目的地的流量	请参阅 添加、编辑或删除 VPC 子网终端节点	请参阅 DenyCustomRoutingTraffic

使用 AWS Global Accelerator 中的标准加速器

本章包括在 AWS Global Accelerator 中创建标准加速器的过程和建议。使用标准加速器，全球加速器可为您的流量选择最接近的运行状况良好的终端节点。

如果您希望使用自定义应用程序逻辑将一个或多个用户引导到多个端点之间的特定终端节点，请创建自定义路由加速器。有关更多信息，请参阅 在 AWS Global Accelerator 中使用自定义路由加速器。

要设置标准加速器，请执行以下操作：

1. 创建加速器，然后选择标准加速器选项。
2. 添加具有特定端口或端口范围的监听程序，然后选择要接受的协议：TCP、UDP 或两者兼有。
3. 为您拥有终端节点资源的每个 AWS 区域添加一个或多个终端节点组。
4. 向终端组中添加一个或多个终端节点。这不是必需的，但如果您没有任何终端节点，则不会路由流量。终端节点可以是网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址。

以下各节逐步介绍如何使用标准加速器、侦听器、终端节点组和终端节点。

主题

AWS Global Accelerator 中的标准加速器

A标准加速器将流量引导到 AWS Global Accelerator 通过 AWS Global Accelerator 将流量引向最佳终端节点，以提高具有全球受众的 Internet 应用程序的可用性和性能。每个加速器都包含一个或多个侦听器。监听程序根据您配置的协议（或协议）和端口（或端口范围）处理从客户端到全局加速器的入站连接。

在创建加速器时，默认情况下，全局加速器会为您提供一组两个静态 IP 地址。如果您将自己的 IP 地址范围带到 AWS (BYOIP)，则可以从自己的池中分配静态 IP 地址以配合您的加速器使用。有关更多信息，请参阅 在 AWS Global Accelerator 中引入您自己的 IP 地址 (BYOIP)。

> **Important**
>
> 只要加速器存在，就会将 IP 地址分配给您的加速器，即使您禁用了加速器并且它不再接受或路由流量也是如此。但是，当delete加速器，则会丢失分配给加速器的全局加速器静态 IP 地址，因此无法再使用它们路由流量。作为最佳做法，请确保您拥有权限，以避免无意中删除加速器。您可以将 IAM 策略与全局加速器（例如，基于标签的权限）结合使用，以限制有权删除加速器的用户。有关更多信息，请参阅 基于标签的策略。

本节介绍如何在全局加速器控制台上创建、编辑或删除标准加速器。如果要将 API 操作用于 Global Accelerator，请参阅AWS Global Accelerator API 参考。

主题

创建或更新标准加速器

本部分介绍如何在控制台上创建或更新标准加速器。若要以编程方式使用全局加速器，请参阅AWS Global Accelerator API 参考。

创建标准加速器

1. 打开全局加速器控制台https://console.aws.amazon.com/globalaccelerator/home。
2. 选择创建加速器。
3. 提供加速器的名称。
4. 适用于加速器类型中，选择标准。
5. 或者，如果您将自己的 IP 地址范围带到 AWS (BYOIP)，则可以为您的加速器指定一个静态 IP 地址，每个地址池中都有一个。为加速器的两个静态 IP 地址中的每个地址进行此选择。

    - 对于每个静态 IP 地址，选择要使用的 IP 地址池。

> **Note**
>
> 您必须为每个静态 IP 地址选择不同的 IP 地址池。此限制是因为全局加速器将每个地址范围分配给不同的网络区域，以实现高可用性。

- 如果您选择自己的 IP 地址池，请从池中选择特定的 IP 地址。如果您选择默认的 Amazon IP 地址池，则全球加速器会为您的加速器分配特定的 IP 地址。

6. （可选）添加一个或多个标签来帮助您识别加速器资源。
7. 选择下一步添加监听器、终端节点组和终端节点。

编辑标准加速器

1. 打开全局加速器控制台https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器列表中，选择一个加速器，然后选择编辑。
3. 在存储库的编辑加速器页面上，进行所需的任何更改。例如，您可以禁用加速器，以便它不再接受或路由流量，也可以删除它。或者，如果禁用了加速器，则可以启用它。
4. 选择保存更改。

删除加速器

如果您创建了加速器作为测试，或者您不再使用加速器，则可以将其删除。在控制台上，禁用加速器，然后您可以将其删除。您不必从加速器中删除侦听器和终端节点组。

要使用 API 操作而不是控制台删除加速器，您必须首先删除与该加速器关联的所有侦听器和终端节点组，然后将其禁用。有关更多信息，请参阅 。删除加速器中的操作AWS Global Accelerator API 参考。

禁用加速器

1. 打开全局加速器控制台https://console.aws.amazon.com/globalaccelerator/home。
2. 在列表中，选择要禁用的加速器。
3. 选择 Edit。
4. 选择禁用加速器，然后选择Save。

删除加速器

1. 打开全局加速器控制台https://console.aws.amazon.com/globalaccelerator/home。
2. 在列表中，选择要删除的加速器。
3. 选择 Delete。

> **Note**
>
> 如果您尚未禁用加速器，请Delete不可用。

4. 在确认对话框中，选择 Delete (删除)。

> **Important**
>
> 删除加速器时，会丢失分配给加速器的静态 IP 地址，因此无法再使用它们路由流量。

查看您的加速器

您可以在控制台上查看有关加速器的信息。要以编程方式查看加速器的说明，请参阅列表加速器和DescribeAccelerator中的AWS Global Accelerator API 参考。

查看有关您的加速器的信息

1. 打开全局加速器控制台https://console.aws.amazon.com/globalaccelerator/home。
2. 要查看有关加速器的详细信息，请在列表中选择一个加速器，然后选择查看。

在您创建负载均衡器时添加速器

当您在 AWS 管理控制台中创建 Application Load Balancer 时，您可以选择性地选择同时添加速器。Elastic Load Balancing 和全局加速器协同工作，为您透明地添加加速器。加速器在您的账户中创建，负载均衡器作为终端节点。使用加速器可提供静态 IP 地址，并提高应用程序的可用性和性能。

> **Important**
>
> 要创建加速器，您必须具有正确的权限。有关更多信息，请参阅 控制台访问、身份验证管理和访问控制所需的权限。

配置和查看您的加速器

您必须更新 DNS 配置，以将流量定向到加速器的静态 IP 地址或 DNS 名称。在配置更改完成之前，流量不会通过加速器进入负载均衡器。

通过在 Amazon EC2 控制台上选择全球加速器加载项来创建负载均衡器后，请转到集成的服务选项卡以查看加速器的静态 IP 地址和域名系统 (DNS) 名称。您可以使用此信息开始通过 AWS 全球网络将用户流量路由到负载均衡器。有关分配给您的加速器的 DNS 名称的更多信息，请参阅AWS Global Accelerator 中的 DNS 寻址和自定义域。

您可以通过导航到 Global Accelerator中的 AWS 管理控制台。例如，您可以看到与您的帐户相关联的加速器，或向您的加速器添加额外的负载均衡器。有关更多信息，请参阅 查看您的加速器 和 创建或更新标准加速器。

定价

使用 AWS Global Accelerator，您需要为账户中的加速器付费（不管状态为启用或禁用），并支付数据传输费。有关更多信息，请参阅 AWS Global Accelerator 定价。

停止使用加速器

如果要停止通过全局加速器将流量路由到负载均衡器，请执行以下操作：

1. 更新 DNS 配置以将流量直接指向负载均衡器。
2. 从加速器中删除负载均衡器。有关更多信息，请参阅 。删除终端节点在添加、编辑或删除标准端点。
3. 删除加速器。有关更多信息，请参阅 删除加速器。

使用全局静态 IP 地址而不是区域静态 IP 地址

如果您想在 AWS 资源（例如 Amazon EC2 实例）前面使用静态 IP 地址，您可以选择多种选项。例如，您可以分配一个弹性 IP 地址，该地址是一个静态 IPv4 地址，您可以与单个 AWS 区域中的 Amazon EC2 实例或网络接口相关联。

如果您有全球受众，您可以使用全球加速器创建一个加速器，以获取两个全球静态 IP 地址，这些地址是从全球 AWS 节点发布的。如果您已在一个或多个区域（包括 Amazon EC2 实例、网络负载均衡器和应用程序负载均衡器）中为您的应用程序设置了 AWS 资源，您可以轻松地将这些资源添加到全局加速器中，以便为它们提供全局静态 IP 地址。

选择使用全局加速器预配的全局静态 IP 地址还可以提高应用程序的可用性和性能。借助全球加速器，静态 IP 地址可接受从最靠近用户的节点传入 AWS 全球网络的流量。最大限度地延长流量在 AWS 网络上的时间，可以提供更快、更好的客户体验。有关更多信息，请参阅 AWS Global Accelerator 的工作方式 。

您可以从 AWS 管理控制台或通过使用 API 操作与 AWS CLI 或软件开发工具包一起添加加速器。有关更多信息，请参阅 创建或更新标准加速器。

添加速器时，请注意以下内容：

- 只要您的加速器存在，全局加速器预配的全局静态 IP 地址将一直分配给您，即使您禁用了加速器并且它不再接受或路由流量也是如此。但是，如果删除加速器，则会丢失分配给该加速器的静态 IP 地址。有关更多信息，请参阅 删除加速器。
- 使用 AWS Global Accelerator，您需要为账户中的加速器付费（不管状态为启用或禁用），并支付数据传输费。有关更多信息，请参阅 AWS Global Accelerator 定价。

AWS Global Accelerator 中标准加速器的侦听器

借助 AWS Global Accelerator，您可以添加侦听器，根据您指定的端口和协议处理来自客户端的入站连接。侦听器支持 TCP、UDP 或 TCP 和 UDP 协议。

您可在创建标准加速器时定义标准侦听器，并可随时添加侦听器。您可以将每个侦听器与一个或多个终端节点组关联，并将每个终端节点组与一个 AWS 区域相关联。

主题

- 添加、编辑或删除标准监听程序
- 客户端关联

添加、编辑或删除标准监听程序

本节介绍如何在 AWS Global Accelerator 控制台上使用侦听器。要使用 API 操作而不是控制台完成这些任务，请参阅`CreateListener`、`UpdateListener`, 和`DeleteListener`中的AWS Global Accelerator API 参考。

添加侦听器

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。

2. 在存储库的加速器页面上，选择加速器。
3. 选择 Add listener (添加侦听器)。
4. 在存储库的添加侦听器页面上，输入要与监听程序关联的端口或端口范围。侦听器支持端口 1-65535。
5. 为您输入的端口选择协议。
6. （可选）选择启用客户端关联性。监听程序的客户端关联性意味着全局加速器可确保来自特定源（客户端）IP 地址的连接始终路由到同一终结点。要启用此行为，请在下拉列表中，选择源 IP。

   默认值为无，这意味着未启用客户端关联性，并且全局加速器在监听程序的终端节点组中的终端节点之间平均分配流量。

   有关更多信息，请参阅 客户端关联。
7. 选择 Add listener (添加侦听器)。

编辑标准监听程序

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择加速器。
3. 选择侦听器，然后选择编辑侦听器。
4. 在存储库的编辑侦听器页面上，更改要与监听程序关联的端口、端口范围或协议。
5. （可选）选择启用客户端关联性。监听程序的客户端关联性意味着全局加速器可确保来自特定源（客户端）IP 地址的连接始终路由到同一终结点。要启用此行为，请在下拉列表中，选择源 IP。

   默认值为无，这意味着未启用客户端关联性，并且全局加速器在监听程序的终端节点组中的终端节点之间平均分配流量。

   有关更多信息，请参阅 客户端关联。
6. 选择保存。

删除侦听器

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择加速器。
3. 选择侦听器，然后选择Remove。
4. 在确认对话框中，选择Remove。

客户端关联

如果您有与标准加速器一起使用的有状态应用程序，则可以选择让全局加速器将来自特定源（客户端）IP 地址的用户的所有请求定向到同一个终结点资源，以保持客户端关联性。

默认情况下，标准侦听器的客户端关联性设置为无和全局加速器在监听程序的终端节点组中的终端节点之间平均分配流量。

Global Accelerator 使用一致流哈希算法为用户连接选择最佳终端节点。如果将全局加速器资源的客户端关联性配置为无，则 Global Accelerator 使用 5 元组属性（源 IP、源端口、目标 IP、目标端口、目标 IP、目标端口和协议）来选择哈希值。接下来，它选择提供最佳性能的端点。如果给定客户端使用不同的端口连接到 Global Accelerator 并指定此设置，则 Global Accelerator 无法确保客户端连接总是路由到同一终端节点。

如果要在每次连接时将特定用户（由其源 IP 地址标识）路由到相同的终端节点来保持客户端关联性，请将客户端关联性设置为源 IP。当您指定此选项时，Global Accelerator 使用 2 元组属性（源 IP 和目标 IP）来选择哈希值，并在用户连接时路由用户到同一终端节点。全局加速器在您选择的终端节点组之后支持客户端关联性。

AWS Global Accelerator 中标准加速器的终端节点组

终端节点组将请求路由到 AWS Global Accelerator 中的一个或多个注册终端节点。在标准加速器中添加监听器时，您可以指定要将流量引导到的全局加速器的终端节点组。终端节点组及其中的所有终端节点必须位于一个 AWS 区域中。您可以为不同目的添加不同的终端节点组，例如，用于蓝色/绿色部署测试。

全局加速器根据客户端的位置和终端节点组的运行状况，将流量定向到标准加速器中的终端节点组。如果愿意，您还可以设置要发送到终端节点组的流量百分比。您可以使用流量拨号增加（向上拨打）或减少（下拨）到组的流量。百分比仅应用于全局加速器已经定向到终端节点组的流量，而不是所有来到监听程序的流量。

您可以为每个终端节点组定义全局加速器的运行状况检查设置。通过更新运行状况检查设置，您可以更改轮询和验证 Amazon EC2 实例和弹性 IP 地址终端节点运行状况的要求。对于 Network Load Balancer 和 Application Load Balancer 终端节点，请在 Elastic Load Balancing 控制台上配置运行状况检查设置。

全局加速器持续监视标准终端节点组中包含的所有终端的运行状况，并仅将请求路由到运行状况良好的活动终端节点。如果没有任何正常的终端节点可以将流量路由到，全局加速器会将请求路由到所有终端节点。

本节介绍如何在 AWS Global Accelerator 控制台上使用标准加速器的终端节点组。如果要将 API 操作与 AWS Global Accelerator 一起使用，请参阅AWS Global Accelerator API 参考。

主题

添加、编辑或删除标准终端节点组

您可以在 AWS Global Accelerator 控制台上或使用 API 操作使用终端节点组。您可以随时在终端节点组中添加或删除终端节点。

本节点介绍如何在 AWS Global Accelerator 控制台上使用标准终端节点组。如果要将 API 操作用于 Global Accelerator，请参阅AWS Global Accelerator API 参考。

添加标准终端节点组

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择加速器。
3. 在侦听器部分, 用于侦听器 ID中，选择要向其中添加终端节点组的侦听器的 ID。
4. 选择添加终端节点组。
5. 在监听程序的部分中，通过从下拉列表中选择一个区域来为终端节点组指定一个区域。
6. (可选)流量拨打中，输入 0 到 100 之间的数字以设置此终端节点组的流量百分比。百分比仅应用于已定向到此终端节点组的流量，而不是所有监听程序流量。默认情况下，流量拨号设置为 100。
7. （可选）要覆盖用于将流量路由到终端节点并将流量重新路由到终端上的特定端口的侦听器端口，请选择配置端口覆盖。有关更多信息，请参阅 覆盖端口。
8. （可选）要指定要应用于 EC2 实例和弹性 IP 地址终端节点的自定义运行状况检查值，请选择配置运行状况检查。有关更多信息，请参阅 运行状况检查选项。
9. (可选) 选择添加终端节点组为此侦听器或其他侦听器添加其他终端节点组。
10. 选择添加终端节点组。

编辑终端节点组

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择加速器。
3. 在侦听器部分, 用于侦听器 ID中，选择与终端节点组关联的侦听器的 ID。
4. 选择编辑终端节点组。
5. 在存储库的编辑终端节点组页面上，更改区域，调整流量拨号百分比，或选择配置运行状况检查修改运行状况检查设置。
6. 选择保存。

删除标准终端节点组

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择加速器。
3. 在侦听器部分中，选择侦听器，然后选择Remove。
4. 在终端节点组部分中，选择终端节点组，然后选择Remove。
5. 在确认对话框中，选择Remove。

使用流量拨号调整流量

对于每个标准终端节点组，您可以设置流量拨号来控制定向到该组的通信百分比。百分比仅应用于已定向到终端节点组的流量，而不是所有监听程序流量。

默认情况下，对于加速器中的所有区域终端节点组，流量拨号设置为 100（即 100%）。通过流量拨号，您可以轻松地对跨不同 AWS 区域的新版本进行性能测试或蓝/绿部署测试。

以下是几个示例，说明如何使用流量拨号将流量流更改为终端节点组。

按地区升级您的应用程序

如果要升级区域中的应用程序或进行维护，请首先将流量拨号设置为 0 以切断该区域的流量。当您完成工作并准备好将 “区域” 恢复服务时，请将流量拨号调整为 100 以备份流量。

混合两个区域之间的流量

此示例说明同时更改两个区域终端节点组的流量拨号时，流量流的工作原理。假设您的加速器有两个终端节点组-一个用于us-west-2区域和一个用于us-east-1区域 — 并且您已将每个终端节点组的流量拨号设置为 50%。

现在，假设你有 100 个请求来到你的加速器，其中 50 个来自美国东海岸，50 个来自西海岸。加速器按如下方式指导流量：

- 每个海岸上的前 25 个请求（总共 50 个请求）从其附近的终端节点组处理。也就是说，25 个请求被定向到us-west-2和 25 的终端节点组定向到us-east-1。
- 接下来的 50 个请求被定向到相对的区域。也就是说，从东海岸接下来的 25 个请求是由us-west-2，接下来的 25 个来自西海岸的请求将由us-east-1。

这种情况下的结果是两个终端节点组提供的流量相同。但是，每个区域接收来自两个区域的流量混合。

覆盖端口

默认情况下，加速器会使用您在创建监听器时指定的协议和端口范围将用户流量路由到 AWS 区域中的终端节点。例如，如果您定义了接受端口 80 和 443 上的 TCP 流量的侦听器，则加速器会将流量路由到端点上的这些端口。

但是，添加或更新终端节点组时，您可以覆盖用于将流量路由到终端节点的侦听器端口。例如，您可以创建一个端口覆盖，其侦听器在端口 80 和 443 上接收用户流量，但是您的加速器将这些流量分别路由到终端节点上的端口 1080 和 1443。

端口覆盖可帮助您避免侦听受限端口时出现问题。在终端上运行不需要超级用户（root）权限的应用程序更安全。但是，在 Linux 和其他类 Unix 系统中，您必须具有超级用户权限才能侦听受限端口（TCP 或 UDP 端口低于 1024）。通过将监听器上的受限端口映射到端点上的非受限端口，端口覆盖可以避免此问题。在全球加速器后面的终端上运行没有 root 访问权限的应用程序时，您可以接受受限端口上的流量。例如，您可以将监听程序端口 443 覆盖到端点端口 8443。

对于每个端口覆盖，您可以指定一个监听器端口，该端口接受来自用户的流量，以及全局加速器将该流量路由到的终端端口。有关更多信息，请参阅 添加、编辑或删除标准终端节点组。

创建端口覆盖时，请记住以下内容：

- 端点端口不能与监听器端口范围重叠。 在端口覆盖中指定的端点端口不能包含在您为加速器配置的任何侦听器端口范围中。例如，假设您有两个用于加速器的侦听器，并且您已将这些侦听器的端口范围分别定义为 100-199 和 200-299。创建端口覆盖时，无法定义从侦听器端口 100 到端点端口 210 之间的端口覆盖，例如，因为端点端口 (210) 包含在您定义的监听器端口范围 (200-299) 中。
- 没有重复的终端端口。 如果加速器中的一个端口覆盖指定了一个端点端口，则无法指定具有不同侦听器端口的端口覆盖的同一端点端口。例如，您不能指定从侦听器端口 80 到端点端口 90 的端口覆盖以及从监听器端口 81 到端点端口 90 的覆盖。

- 运行 Health 检查将继续使用原始端口。 如果为配置为运行状况检查端口的端口指定端口覆盖，则运行状况检查仍使用原始端口，而不是覆盖端口。例如，假设您在监听器端口 80 上指定运行状况检查，并且还指定了从侦听器端口 80 到端点端口 480 的端口覆盖。运行 Health 况检查继续使用端点端口 80。但是，通过端口 80 进入的用户流量将转到端点上的端口 480。

  此行为可维护 Network Load Balancer、Application Load Balancer、EC2 实例和弹性 IP 地址终端节点之间的一致性。由于当您在全局加速器中指定端口覆盖时，网络负载均衡器和应用程序负载均衡器不会将运行状况检查端口映射到其他终端节点端口，因此全局加速器将运行状况检查端口映射到 EC2 实例和弹性 IP 的不同终端节点端口将不一致地址端点。
- 安全组设置必须允许端口访问。 确保您的安全组允许流量到达您在端口覆盖中指定的终端节点。例如，如果您将监听器端口 443 覆盖到终端端口 1433，请确保在安全组中为该 Application Load Balancer 或 Amazon EC2 终端节点设置的任何端口限制都允许端口 1433 上的入站流量。

运行状况检查选项

AWS Global Accelerator 会定期向标准终端节点发送请求以测试其状态。这些运行状况检查会自动运行。确定每个终端的运行状况和运行状况检查时间的指南取决于终端资源的类型。

> **Important**
>
> 全局加速器要求您的路由器和防火墙规则允许来自与 Route 53 运行状况检查程序关联的 IP 地址的入站流量完成 EC2 实例或弹性 IP 地址终端节点的运行状况检查。有关与 Amazon Route 53 运行状况检查程序关联的 IP 地址范围的信息，请参阅目标组的运行状况检查中的Amazon Route 53 开发者指南。

您可以为终端节点组配置以下运行状况检查选项。如果您指定运行状况检查选项，则全局加速器将使用 EC2 实例或弹性 IP 地址运行状况检查的设置，但不适用于网络负载均衡器或应用程序负载均衡器。

- 对于 Application Load Balancer 或 Network Load Balancer 终端节点，您可以使用 Elastic Load Balancing 配置选项为资源配置运行状况检查。有关更多信息，请参阅 。目标组的运行状况检查。您在全局加速器中选择的运行 Health 检查选项不会影响已添加为终端节点的应用程序负载平衡器或网络负载均衡器。

  > **Note**
  >
  > 当您有一个包含多个目标组的 Application Load Balancer 负载均衡器或 Network Load Balancer 时，全局加速器只有在EACH目标组至少具有一个运行状况良好的目标。如果负载

均衡器的任何单个目标组只有运行状况不佳的目标，则全局加速器会将终端节点视为运行状况不佳。

- 对于添加到使用 TCP 配置的侦听器的 EC2 实例或弹性 IP 地址终端节点，您可以指定用于运行状况检查的端口。默认情况下，如果未指定运行状况检查的端口，则全局加速器将使用您为加速器指定的侦听器端口。
- 对于具有 UDP 侦听器的 EC2 实例或弹性 IP 地址终端节点，全局加速器使用侦听器端口和 TCP 协议进行运行状况检查，因此终端节点上必须有 TCP 服务器。

> **Note**
>
> 请确保检查为每个端点上的 TCP 服务器配置的端口是否与您在全局加速器中为运行状况检查指定的端口相同。如果端口号不相同，或者您尚未为终端设置 TCP 服务器，则无论端点的运行状况如何，全局加速器都会将端点标记为运行状况不佳。

运行 Health 检查端口

Global Accelerator 对属于此终端节点组的终端节点执行运行状况检查时使用的端口。

> **Note**
>
> 您无法为运行状况检查端口设置端口覆盖。

运行状况检查协议

Global Accelerator 对属于此终端节点组的终端节点执行运行状况检查时使用的协议。

运行 Health 检查间隔

终端节点的每次运行状况检查之间的间隔（以秒为单位）。

阈值计数

将不正常目标视为运行状况不正常或运行状况不正常之前所需的连续运行状况检查次数。

每个侦听器仅将请求路由到运行状况良好的终端节点。添加终端节点后，终端节点必须通过运行状况检查才会被视为正常。在完成每次运行状况检查后，侦听器将关闭为运行状况检查而建立的连接。

AWS Global Accelerator 中标准加速器的终端节点

AWS Global Accelerator 中标准加速器的终端节点可以是网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址。使用标准加速器，静态 IP 地址充当客户端的单一接触点，然后 Global Accelerator 跨正常运行的终端节点分发传入流量。全局加速器使用您为终端节点的终端节点组所属的监听程序指定的端口（或端口范围）将流量定向到端点。

每个终端节点组都可以有多个终端节点。您可以将每个终端节点添加到多个终端节点组，但终端节点组必须与不同的侦听器关联。当您将资源添加为终端节点时，资源必须是有效且活动的。

全局加速器持续监控标准终端节点组中包含的所有终端的运行状况。它仅将流量路由到运行状况良好的活动端点。如果全局加速器没有任何运行状况良好的终端节点可以将流量路由到所有端点。

对于特定类型的全局加速器标准终端节点，请注意以下事项：

负载均衡器终端节点

- Application Load Balancer 终端节点可以是面向 Internet 的，也可以是内部的。Network Load Balancer 终端节点必须面向互联网。

Amazon EC2 实例终端节点

- EC2 实例终端节点（对于标准路由加速器和自定义路由加速器）不能是以下类型之一：C1、CC1、CC1、CC1、CC2、CC2、CC2、CC2、CC2、CC1、CG1、G2、G2、HI1、HI1、HS1、M 或 T1。
- EC2 实例仅在部分 AWS 区域受支持作为终端节点受支持。有关受支持的区域的列表，请参阅支持的 AWS 区域用于客户端 IP 地址保留。
- 我们建议您在终止实例之前从全局加速器终端节点组中删除 EC2 实例。如果您在将 EC2 实例从全球加速器中的终端节点组中删除之前终止该实例，然后在同一 VPC 中创建另一个具有相同私有 IP 地址的实例，并且运行状况检查通过，则全局加速器将流量路由到新终端节点。

主题

添加、编辑或删除标准端点

您可以向终端节点组添加终端节点，以便将流量定向到您的资源。您可以编辑标准端点以更改端点的权重。或者，您可以从加速器中删除终端节点，从终端节点组中删除该终端节点。删除终端节点不会影响终端节点本身，但全局加速器不能再将流量引导到该资源。

全局加速器中的终端节点可以是网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址。您必须先创建这些资源之一，然后您可以将其添加为全局加速器中的终端节点。当您将资源添加为终端节点时，资源必须是有效且活动的。

您可以根据使用情况向终端节点组中添加或删除终端节点。例如，如果对应用程序的需求增加，您可以创建更多资源，然后向一个或多个终端节点组添加更多终端节点，以处理增加的流量。只要您添加终端节点且终端节点通过初始运行状况检查，Global Accelerator 就会开始将请求路由至终端节点。您可以通过调整终端节点上的权重来管理到端点的流量，以按比例向终端节点发送更多或更少的流量。

如果要添加具有客户端 IP 地址保留的终端节点，请首先查看支持的 AWS 区域用于客户端 IP 地址保留和在 AWS Global Accelerator 中保留客户端 IP 地址。

例如，如果您需要为终端节点提供服务，则可以从终端节点组中删除终端节点。删除终端节点将从终端节点组中移出终端节点，但不会影响终端节点。一旦从终端节点组中删除流量，全局加速器就停止将流量定向到终端节点。终端节点进入状态，等待所有当前请求完成，因此正在进行的客户端流量不会中断。当您准备好终端节点以继续接收请求时，可以将终端节点重新添加到终端节点组。

本节介绍如何使用 AWS Global Accelerator 控制台上的终端节点。如果您想要将 API 操作与 AWS Global Accelerator 结合使用，请参阅AWS Global Accelerator API 参考。

添加标准终端节点

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择加速器。
3. 在侦听器部分, 用于侦听器 ID下，选择监听程序的 ID。
4. 在终端节点组部分, 用于终端节点组 ID中，选择要向其中添加终端节点的终端节点组的 ID。
5. 在终端节点部分中，选择。添加终端节点。
6. 在存储库的添加终端节点页面上，从下拉列表中选择资源。

   如果您没有任何 AWS 资源，则列表中没有任何项目。要继续，请创建 AWS 资源，如负载均衡器、Amazon EC2 实例或弹性 IP 地址。然后回到这里的步骤，然后从列表中选择一个资源。

7. 对于是可选的权重中，输入一个介于 0 到 255 之间的数字，以设置将流量路由到此终端节点的权重。向终端节点添加权重时，您可以配置 Global Accelerator，以便根据您指定的比例路由流量。默认情况下，所有端点的权重都为 128。有关更多信息，请参阅 终端节点权重。
8. （可选）为面向 Internet 的应用程序负载均衡器终端节点启用客户端 IP 地址保留。在保留客户端 IP 地址中，选择。PRESERVE。

   始终为内部 Application Load Balancer 和 EC2 实例终端节点选择此选项，并且从未为 Network Load Balancer 和弹性 IP 地址终端节点选择此选项。有关更多信息，请参阅 在 AWS Global Accelerator 中保留客户端 IP 地址。

   > **Note**
   >
   > 在添加流量并开始将流量路由到保留客户端 IP 地址的终端之前，请确保已更新所有必需的安全配置（例如安全组），以便在允许列表中包括用户客户端 IP 地址。

9. 选择 Add endpoint (添加终端节点)。

编辑标准终端节点

您可以编辑端点配置以更改权重。有关更多信息，请参阅 终端节点权重。

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择加速器。
3. 在侦听器部分, 用于侦听器 ID下，选择监听程序的 ID。
4. 在终端节点组部分, 用于终端节点组 ID下，选择终端节点组的 ID。
5. 选择编辑终端节点。
6. 在存储库的编辑终端节点页面上，进行更新，然后选择。Save。

删除终端节点

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择加速器。
3. 在侦听器部分, 用于侦听器 ID下，选择监听程序的 ID。
4. 在终端节点组部分, 用于终端节点组 ID下，选择终端节点组的 ID。
5. 选择删除终端节点。

6. 在确认对话框中，选择。Remove。

终端节点权重

权重是一个值，用于确定全局加速器指向标准加速器中终端节点的流量比例。终端节点可以是网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址。全局加速器计算终端节点组中终端节点权重的总和，然后根据每个端点权重与总数的比率将流量定向到端点。

通过加权路由，您可以选择将多少流量路由到终端节点组中的资源。这可用于多种方式，例如负载均衡和测试新版本的应用程序等。

端点权重的工作原理

要使用权重，您可以为终端节点组中的每个终端节点分配相对权重，该权重与要发送到终端节点的流量。默认情况下，端点的权重为 128，即权重 255 的最大值的一半。Global Accelerator 将根据您分配给终端节点的权重 (占该组中所有终端节点总权重的比例) 向终端节点发送流量：

$$\frac{\text{Weight for a specified endpoint}}{\text{Sum of the weights for all endpoints}}$$

例如，如果您想要将极少的一部分流量发送到一个终端节点，并将其余流量发送到另一个终端节点，则可以指定权重 1 和 255。权重为 1 的终端节点将获得 1/256 (1/1+255) 的流量，另一个终端节点将获得 255/256 (255/1+255) 的流量。您可以通过更改权重来逐渐改变平衡。如果希望 Global Accelerator 停止向终端节点发送流量，则可以将该资源的权重更改为 0。

运行状况不佳的终端的故障切换

如果终端节点组中没有权重大于零的正常终端节点，全局加速器将尝试故障转移到另一个端点组中权重大于零的正常终端节点。对于此故障转移，全局加速器将忽略通信拨号设置。因此，例如，如果终端节点组的流量拨号设置为零，则全局加速器仍将该终端节点组包括在故障转移尝试中。

如果全球加速器在尝试三个额外终端节点组（即三个 AWS 区域）后未找到权重大于零的正常终端节点，则它会将流量路由到最接近客户端的终端节点组中的随机终端节点。也就是说，失败打开。

请注意以下几点：

- 选择进行故障转移的终端节点组可能是流量拨号设置为零的终端节点组。
- 最近的终端节点组可能不是原始终端节点组。这是因为全局加速器在选择原始终端节点组时会考虑帐户流量拨号设置。

例如，假设您的配置有两个终端节点，一个运行状况良好，一个运行状况不佳，并且您已将每个端点的权重设置为大于零。在这种情况下，全局加速器将流量路由到运行状况良好的终端节点。但是，现在假设您将唯一运行状况良好的端点的权重设置为零。然后，全局加速器会尝试三个额外的终端节点组来查找权重大于零的运行状况良好的终端节点。如果没有找到，全局加速器会将流量路由到离客户端最近的终端节点组中的随机终端节点。

使用客户端 IP 地址保留添加端点

您可以与某些端点类型（在某些区域中）一起使用的功能是客户端 IP 地址保留。使用此功能，您可以为到达终端节点的数据包保留原始客户端的源 IP 地址。您可以将此功能与应用程序负载均衡器和 Amazon EC2 实例终端节点结合使用。自定义路由加速器上的端点始终保留客户端 IP 地址。有关更多信息，请参阅 在 AWS Global Accelerator 中保留客户端 IP 地址。

如果要使用客户端 IP 地址保留功能，请在向全局加速器添加终端节点时注意以下事项：

弹性网络接口

为了支持客户端 IP 地址保留，全球加速器在您的 AWS 账户中创建弹性网络接口 — 每个存在终端节点的子网都会创建一个弹性网络接口。有关 Global Accelerator 如何使用弹性网络接口的更多信息，请参阅客户端 IP 地址保留的最佳实践。

私有子网中的终端节点

您可以使用 AWS Global Accelerator 将应用 Application Load Balancer 器或私有子网中的 EC2 实例定位为目标，但您必须具有互联网网关连接到包含终端节点的 VPC。有关更多信息，请参阅 AWS Global Accelerator 中的 VPC 连接安全。

将客户端 IP 地址添加到允许列表中

在添加流量并开始将流量路由到保留客户端 IP 地址的终端之前，请确保已更新所有必需的安全配置（例如安全组），以便在允许列表中包括用户客户端 IP 地址。网络访问控制列表 (ACL) 仅适用于出站 (出站) 流量。如果您需要筛选入站（入站）流量，则必须使用安全组。

配置网络访问控制列表 (ACL)

当您的加速器启用客户端 IP 地址保留时，与 VPC 子网关联的网络 ACL 将应用于出站（出站）流量。但是，要允许流量通过全局加速器退出，必须将 ACL 配置为入站和出站规则。

例如，要允许使用临时源端口的 TCP 和 UDP 客户端通过全局加速器连接到终端节点，请将终端节点的子网与允许发往临时 TCP 或 UDP 端口的出站流量（端口范围为 1024-65535，目标 0.0.0.0/0）的网络 ACL 相关联。此外，还可以创建匹配的入站规则（端口范围 1024-65535、源 0.0.0.0/0）。

> **Note**
>
> 安全组和 AWS WAF 规则是一组额外的功能，您可以应用它们来保护您的资源。例如，与 Amazon EC2 实例和应用程序负载均衡器关联的入站安全组规则允许您控制客户端可通过全局加速器连接到的目标端口，例如 HTTP 端口 80 或 HTTPS 端口 443。请注意，Amazon EC2 实例安全组应用于到达您实例的任何流量，包括来自全局加速器的流量以及分配给您的实例的任何公有或弹性 IP 地址。作为最佳做法，如果您希望确保流量仅由全局加速器传送，请使用私有子网。此外，请确保入站安全组规则已适当配置，以正确地允许或拒绝应用程序的流量。

转换端点以使用客户端 IP 地址保留

按照本节中的指导将加速器中的一个或多个终端转换为保留用户客户端 IP 地址的终端节点。您可以选择将应 Application Load Balancer 终端节点或弹性 IP 地址终端节点转换为具有客户端 IP 地址保留的相应终端节点（应用程序负载均衡器或 EC2 实例）。有关更多信息，请参阅 在 AWS Global Accelerator 中保留客户端 IP 地址。

我们建议您慢慢转换到使用客户端 IP 地址保留。首先，添加启用以保留客户端 IP 地址的新应用程序负载均衡器或 EC2 实例终端节点。然后，通过在终端上配置权重，慢慢地将流量从现有终端节点移动到新终端节点。

> **Important**
>
> 在开始将流量路由到保留客户端 IP 地址的终结点之前，请确保将全局加速器客户端 IP 地址包含在允许列表中的所有配置都更新为包含用户客户端 IP 地址。

客户端 IP 地址保留仅在特定的 AWS 区域提供。有关更多信息，请参阅 支持的 AWS 区域用于客户端 IP 地址保留。

本节介绍如何在 AWS Global Accelerator 控制台上使用终端节点组。如果要将 API 操作与 Global Accelerator 一起使用，请参阅AWS Global Accelerator API 参考。

将少量流量移动到具有客户端 IP 地址保留的新终端节点后，进行测试以确保您的配置正常工作。然后，通过调整相应端点上的权重，逐步增加到新端点的流量比例。

要转换到保留客户端 IP 地址的终端节点，请先按照此处的步骤添加新终端节点，对于面向 Internet 的 Application Load Balancer 终端节点，启用客户端 IP 地址保留。（始终为内部应用程序负载均衡器和 EC2 实例选择客户端 IP 地址保留选项。）

添加具有客户端 IP 地址保留的终端节点

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择加速器。
3. 在侦听器部分中，选择侦听器。
4. 在终端节点组部分中，选择终端节点组。
5. 在终端节点部分中，选择。添加终端节点。
6. 在存储库的添加终端节点页面上的终端节点下拉列表中，选择应用程序负载均衡器终端节点或 EC2 实例终端节点。
7. 在权重字段中，选择与为现有端点设置的权重相比较低的数字。例如，如果相应的应 Application Load Balancer 的权重为 255，则可以为新的应用程序负载均衡器输入权重 5，以开始。有关更多信息，请参阅 终端节点权重。
8. 对于新的面向外部的 Application Load Balancer 终端节点，请在保留客户端 IP 地址中，选择。PRESERVE。（始终为内部应用程序负载均衡器和 EC2 实例选择此选项。）
9. 选择保存更改。

接下来，按照此处的步骤编辑相应的现有终端节点（用客户端 IP 地址保留替换它们），以减少现有终端节点的权重，从而减少流向它们的流量。

减少现有终端的流量

1. 在存储库的终端节点组页面上，选择没有客户端 IP 地址保留的现有终端节点。
2. 选择 Edit。
3. 在存储库的编辑终端节点页面上的权重字段中，输入低于当前数字的数字。例如，如果现有终端节点的权重为 255，则可以为新终端节点输入权重 220（使用客户端 IP 地址保留）。
4. 选择保存更改。

通过将新终端节点的权重设置为较低数量，对原始流量的一小部分进行测试后，您可以通过继续调整原始终端和新终端节点的权重来缓慢转换所有流量。

例如，假设您从权重设置为 200 的现有 Application Load Balancer 开始，然后添加一个启用客户端 IP 地址保留且权重设置为 5 的新应用程序负载均衡器终端节点。通过增加新 Application Load Balancer 的权重并减少原始 Application Load Balancer 的权重，逐步将流量从原始应用程序负载均衡器转移到新的应用程序负载均衡器。例如：

- 原始重量190/新重量 10
- 原始重量180/新重量 20
- 原始重量 170/新重量30，依此类推。

当您将原始终端节点的权重减小到 0 时，所有流量（在本示例情况下）都将转到新的 Application Load Balancer 终结点，其中包括客户端 IP 地址保留。

如果您有其他终端节点（应用程序负载均衡器或 EC2 实例）要转换为使用客户端 IP 地址保留，请重复本节中的步骤以转换它们。

如果您需要恢复终端节点的配置，以便到达终端的流量不会保留客户端 IP 地址，则可以随时执行此操作：增加不将客户端 IP 地址保留为原始值，并减少端点的权重替换为客户端 IP 地址保留为 0。

在 AWS Global Accelerator 中使用自定义路由加速器

本章包括在 AWS Global Accelerator 中创建自定义路由加速器的过程和建议。通过自定义路由加速器，您可以使用应用程序逻辑将一个或多个用户直接映射到多个目标之间的特定 Amazon EC2 实例，同时通过全球加速器路由流量获得性能改进。当您的应用程序需要一组用户在特定 EC2 实例和端口上运行的同一会话（如游戏应用程序或 IP 语音 (VoIP) 会话）上相互交互时，此操作非常有用。

自定义路由加速器的终端节点必须是虚拟私有云 (VPC) 子网，自定义路由加速器只能将流量路由到这些子网中的 Amazon EC2 实例。创建自定义路由加速器时，您可以包含在单个或多个 VPC 子网中运行的数千个 Amazon EC2 实例。要了解更多信息，请参阅“自定义路由加速器在 AWS Global Accelerator 中的工作原理”。

如果您希望 Global Accelerator 自动选择最接近客户端运行状况的终端节点，请创建标准加速器。有关更多信息，请参阅 使用 AWS Global Accelerator 中的标准加速器。

要设置自定义路由加速器，请执行以下操作：

1. 查看创建自定义路由加速器的指导原则和要求。请参阅 自定义路由加速器的指南和限制。
2. 创建 VPC 子网。将子网添加到全局加速器后，您可以随时将 EC2 实例添加到子网。
3. 创建加速器，然后选择自定义路由加速器的选项。
4. 添加监听程序并指定要监听的全局加速器的端口范围。请确保您包含一个大范围的端口，以便全局加速器映射到您预期拥有的所有目的地。这些端口与您在下一步中指定的目标端口不同。有关侦听器端口要求的更多信息，请参阅自定义路由加速器的指南和限制。
5. 为您拥有 VPC 子网的 AWS 区域添加一个或多个终端节点组。请为每个终端节点组指定以下内容：
   - 终端节点端口范围，表示目标 EC2 实例上能够接收流量的端口。
   - 每个目标端口范围的协议：UDP、TCP 或 UDP 和 TCP 同时使用。
6. 对于终端子网，请选择一个子网 ID。您可以在每个端点组中添加多个子网，子网可以是不同的大小（最多 /17）。

以下各节逐步介绍如何使用自定义路由加速器、侦听器、终端节点组和终端节点。

主题

- AWS Global Accelerator 中的自定义路由加速器侦听器
- AWS Global Accelerator 中自定义路由加速器的终端节点组
- AWS Global Accelerator 中的自定义路由加速器的 VPC 子网终端节点

自定义路由加速器在 AWS Global Accelerator 中的工作原理

通过在 AWS Global Accelerator 中使用自定义路由加速器，您可以使用应用程序逻辑将一个或多个用户直接映射到多个目的地之间的特定目标，同时仍能获得全球加速器的性能优势。自定义路由加速器将侦听器端口范围映射到虚拟私有云 (VPC) 子网中的 EC2 实例目标。这使得全球加速器能够确定性地将流量路由到您子网中的特定 Amazon EC2 私有 IP 地址和端口目标。

例如，您可以将自定义路由加速器与在线实时游戏应用程序一起使用，在该应用程序中，您可以根据您选择的因素（如地理位置、玩家技能和游戏模式）将多个玩家分配给 Amazon EC2 游戏服务器上的单个会话。或者，您可能有一个 VoIP 或社交媒体应用程序，该应用程序将多个用户分配给特定媒体服务器，以进行语音、视频和消息传递会话。

您的应用程序可以调用全局加速器 API 并接收全局加速器端口及其关联的目标 IP 地址和端口的完整静态映射。您可以保存该静态映射，然后您的匹配服务使用它将用户路由到特定的目标 EC2 实例。您不必对客户端软件进行任何修改即可将 Global Accelerator 与应用程序一起使用。

要配置自定义路由加速器，请选择 VPC 子网终端节点。然后，您可以定义传入连接将映射到的目标端口范围，这样您的软件就可以在所有实例中侦听同一组端口。全局加速器创建一个静态映射，允许匹配服务将会话的目标 IP 地址和端口号转换为您提供给用户的外部 IP 地址和端口。

您的应用程序的网络堆栈可能通过单个传输协议运行，或者您可以使用 UDP 进行快速交付，并使用 TCP 实现可靠的传输。您可以为每个目标端口范围设置 UDP、TCP 或 UDP 和 TCP，以便为您提供最大的灵活性，而无需为每个协议复制配置。

> **Note**
>
> 默认情况下，自定义路由加速器中的所有 VPC 子网目标都不允许接收流量。这在默认情况下是安全的，并且还可以让您精细控制子网中允许哪些私有 EC2 实例目标接收流量。您可以允许或拒绝向子网或特定 IP 地址和端口组合（目标套接字）的流量。有关更多信息，请参阅 添加、编辑或删除 VPC 子网终端节点。您还可以使用全局加速器 API 指定目标。有关更多信息，请参阅 。允许自定义路线流量和拒绝自定义路线流量。

全局加速器中自定义路由如何工作的示例

例如，假设您希望支持 10,000 个会话，其中用户组在全球加速器后面的 1,000 个 Amazon EC2 实例之间进行交互，例如游戏会话或 VoIP 通话会话。在此示例中，我们将指定监听程序端口范围 10001-20040，目标端口范围为 81-90。我们将说，我们在 us-east-1 中有四个 VPC 子网：子网-1、子网-2、子网-3 和子网 4。

在我们的示例配置中，每个 VPC 子网的块大小为 /24，因此它可以支持 251 个 Amazon EC2 实例。（每个子网中有五个地址保留且不可用，而且这些地址不会映射。）每个 EC2 实例上运行的每个服务器都提供以下 10 个端口，这些端口是我们为终端节点组中的目标端口指定的：81-90 这意味着我们有 2510 个端口（10 x 251）与每个子网相关联。每个端口都可以与一个会话相关联。

由于我们已在子网中的每个 EC2 实例上指定了 10 个目标端口，因此全球加速器在内部将它们与 10 个侦听器端口相关联，您可以使用这些端口访问 EC2 实例。为了简单地说明这一点，我们将说有一个侦听器端口块，它们以第一组 10 的终端子网的第一个 IP 地址开始，然后移动到下一组 10 个侦听器端口的下一个 IP 地址。

> **Note**
>
> 映射实际上是不可预测的，但我们在这里使用顺序映射来帮助显示端口映射的工作原理。要确定侦听器端口范围的实际映射，请使用以下 API 操作：列表自定义路程端口映射和列出自定义路程端口映射按目标。

在我们的示例中，第一个侦听器端口是 10001。该端口与第一个子网 IP 地址 192.0.2.4 和第一个 EC2 端口 81 相关联。下一个侦听器端口 10002 与第一个子网 IP 地址 192.0.2.4 和第二个 EC2 端口 82 相关联。下表说明了此示例映射如何继续通过第一个 VPC 子网的最后一个 IP 地址，然后继续到第二个 VPC 子网的第一个 IP 地址。

Global Accelerator 侦听器端口	VPC 子网	EC2 实例端口
10001	192.0.2.4	81
10002	192.0.2.4	82
10003	192.0.2.4	83
10004	192.0.2.4	84

Global Accelerator 侦听器端口	VPC 子网	EC2 实例端口
10005	192.0.2.4	85
10006	192.0.2.4	86
10007	192.0.2.4	87
10008	192.0.2.4	88
10009	192.0.2.4	89
10010	192.0.2.4	90
10011	192.0.2.5	81
10012	192.0.2.5	82
10013	192.0.2.5	83
10014	192.0.2.5	84
10015	192.0.2.5	85
10016	192.0.2.5	86
10017	192.0.2.5	87
10018	192.0.2.5	88
10019	192.0.2.5	89
10020	192.0.2.5	90
...	...	...
12501	192.0.2.244	81
12502	192.0.2.244	82
12503	192.0.2.244	83

Global Accelerator 侦听器端口	VPC 子网	EC2 实例端口
12504	192.0.2.244	84
12505	192.0.2.244	85
12506	192.0.2.244	86
12507	192.0.2.244	87
12508	192.0.2.244	88
12509	192.0.2.244	89
12510	192.0.2.244	90
12511	192.0.3.4	81
12512	192.0.3.4	82
12513	192.0.3.4	83
12514	192.0.3.4	84
12515	192.0.3.4	85
12516	192.0.3.4	86
12517	192.0.3.4	87
12518	192.0.3.4	88
12519	192.0.3.4	89
12520	192.0.3.4	90

自定义路由加速器的指南和限制

在 AWS Global Accelerator 中创建和使用自定义路由加速器时，请牢记以下准则和限制。

Amazon EC2 实例目的地

自定义路由加速器中的 Virtual Cloud (VPC) 子网终端节点只能包含 EC2 实例。自定义路由加速器不支持任何其他资源（如负载平衡器）。

全局加速器支持的 EC2 实例类型列于AWS Global Accelerator 中标准加速器的终端节点。

端口映射

添加 VPC 子网时，全局加速器会创建监听器端口范围与子网支持的端口范围的静态端口映射。特定子网的端口映射永远不会改变。

您可以以编程方式查看自定义路由加速器的端口映射列表。有关更多信息，请参阅 `ListCustomRoutingPortMappings`。

VPC 子网大小

添加到自定义路由加速器的 VPC 子网必须至少为 /28，最大值为 /17。

侦听器端口范围

必须通过指定监听程序端口范围来指定足够的侦听程序端口，以适应计划添加到自定义路由加速器的子网中的目标数。创建监听程序时指定的范围决定了您可以与自定义路由加速器一起使用的监听程序端口和目标 IP 地址组合的数量。为了获得最大的灵活性，并且为了减少出现没有足够可用侦听器端口的错误的可能性，我们建议您指定一个较大的端口范围。

当您向自定义路由加速器添加子网时，全局加速器会以块分配端口范围。我们建议您以线性方式分配监听程序端口范围，并使范围足够大，以支持您希望拥有的目标端口数。也就是说，应分配的端口数应至少为子网中的目标端口和协议（目标配置）数量的子网大小乘以。

> **Note**
>
> 全局加速器用于分配端口映射的算法可能要求您添加更多的侦听器端口（超出此总数）。

创建监听程序后，您可以对其进行编辑以添加其他端口范围和相关协议，但不能减少现有端口范围。例如，如果您的监听程序端口范围为 5,000—10,000，则无法将端口范围更改为 5900—10,000，并且不能将端口范围更改为 5,000—9,900。

每个侦听器端口范围必须至少包含 16 个端口。侦听器支持端口 1-65535。

目的地端口范围

有两个位置可以为自定义路由加速器指定端口范围：添加监听程序时指定的端口范围以及为终端节点组指定的目标端口范围和协议。

- 侦听器端口范围：客户端连接到的全局加速器静态 IP 地址上的监听程序端口。全局加速器将每个端口映射到加速器后面 VPC 子网上的唯一目标 IP 地址和端口。
- 目的地端口范围：您为终端节点组指定的目标端口范围集（也称为目标配置）是接收流量的 EC2 实例端口。要在目标端口上接收流量，与 EC2 实例关联的安全组必须允许其上的流量。

运行 Health 况检查和故障转

全局加速器不对自定义路由加速器执行运行状况检查，也不会故障切换到运行状况良好的终端节点。无论目标资源的运行状况如何，自定义路由加速器的流量都会以确定方式路由。

默认情况下，所有流量都被拒绝

默认情况下，通过自定义路由加速器定向到您子网中的所有目标的流量将被拒绝。要使目标实例能够接收流量，您必须明确允许进入子网的所有流量，或者允许通过子网中的特定实例 IP 地址和端口进行流量。

更新子网或特定目标以允许或拒绝流量需要一段时间才能在互联网上传播。要确定更改是否已传播，可以调用`DescribeCustomRoutingAcceleratorAPI` 操作来检查加速器状态。有关更多信息，请参阅 。描述路程加速器。

不支持 AWS CloudFormation

自定义路由加速器不支持 AWS CloudFormation。

AWS Global Accelerator 中的自定义路由加速器

A自定义路由加速器允许您使用自定义应用程序逻辑将一个或多个用户引导到多个目标之间的特定目标，同时使用 AWS 全球网络提高应用程序的可用性和性能。

自定义路由加速器仅将流量路由到在虚拟私有云 (VPC) 子网中运行的 Amazon EC2 实例上的端口。使用自定义路由加速器，全局加速器不会根据终端节点的地理邻近程度或运行状况路由流量。要了解更多信息，请参阅“自定义路由加速器在 AWS Global Accelerator 中的工作原理”。

在创建加速器时，默认情况下，全局加速器会为您提供一组两个静态 IP 地址。如果您将自己的 IP 地址范围添加到 AWS (BYOIP)，则可以从自己的池中分配静态 IP 地址以用于加速器。有关更多信息，请参阅 在 AWS Global Accelerator 中引入您自己的 IP 地址 (BYOIP)。

> **Important**
>
> 只要加速器存在，就会将 IP 地址分配给您的加速器，即使您禁用了加速器并且它不再接受或路由流量也是如此。但是，当您delete加速器，则会丢失分配给加速器的全局加速器静态 IP 地址，因此无法再使用它们路由流量。作为最佳做法，请确保您拥有权限，以避免无意中删除加速器。您可以使用 IAM 策略（如基于标签的权限）来限制有权删除加速器的用户。有关更多信息，请参阅 基于标签的策略。

本节介绍如何在全局加速器控制台上创建、编辑或删除自定义路由加速器。要了解有关将 API 操作与全局加速器结合使用的信息，请参阅AWS Global Accelerator API 参考。

主题

创建或更新自定义路由加速器

创建自定义路由加速器

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 选择创建加速器。
3. 提供加速器的名称。
4. 适用于加速器类型中，选择自定义路由。
5. 或者，如果您已将自己的 IP 地址范围引入 AWS (BYOIP)，则可以从该地址池中为您的加速器指定静态 IP 地址。为加速器的两个静态 IP 地址中的每个地址进行此选择。
   - 对于每个静态 IP 地址，选择要使用的 IP 地址池。
   - 如果您选择自己的 IP 地址池，请从池中选择特定的 IP 地址。如果您选择了默认的 Amazon IP 地址池，则全球加速器会为您的加速器分配特定的 IP 地址。
6. （可选）添加一个或多个标签以帮助您识别加速器资源。
7. 选择下一步转到向导中的下一页以添加监听程序、终端节点组和 VPC 子网终端节点。

编辑自定义路由加速器

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在自定义路由加速器列表中，选择一个，然后选择编辑。
3. 在存储库的编辑加速器页面上，进行所需的任何更改。例如，您可以禁用加速器，以便将其删除。
4. 选择保存。

查看自定义路由加速器

您可以在控制台上查看有关自定义路由加速器的信息。要以编程方式查看自定义路由加速器的说明，请参阅列出自定义路程加速器和描述路程加速器AWS Global Accelerator API 参考。

查看自定义路由加速器的信息

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 要查看加速器的详细信息，请选择加速器，然后选择查看。

删除自定义路由加速器

如果您创建了自定义路由加速器作为测试，或者您不再使用加速器，则可以将其删除。在控制台上，禁用加速器，然后您可以将其删除。您不必从加速器中删除侦听器和终端节点组。

要使用 API 操作而不是控制台删除自定义路由加速器，必须首先删除与该加速器关联的所有侦听器和终端节点组，然后将其禁用。有关更多信息，请参阅 。删除加速器中的AWS Global Accelerator API 参考。

禁用自定义路由加速器

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在列表中，选择要禁用的加速器。
3. 选择 Edit。
4. 选择禁用加速器，然后选择Save。

删除自定义路由加速器

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。

2. 在列表中，选择要删除的加速器。
3. 选择 Delete。

> **Note**
>
> 如果您尚未禁用加速器，请Delete不可用。要禁用加速器，请参阅前一过程。

4. 在确认对话框中，选择 Delete (删除)。

> **Important**
>
> 删除加速器时，会丢失分配给加速器的静态 IP 地址，因此无法再使用它们路由流量。

AWS Global Accelerator 中的自定义路由加速器侦听器

对于 AWS Global Accelerator 中的自定义路由加速器，您可以配置一个侦听器，该监听器使用关联的协议来指定一系列监听器端口，全球加速器将这些协议映射到 VPC 子网终端节点中的特定目标 Amazon EC2 实例。添加 VPC 子网终端节点时，全局加速器会在您为监听程序定义的端口范围与子网中的目标 IP 地址和端口之间创建静态端口映射。然后，您可以使用端口映射指定加速器静态 IP 地址以及监听器端口和协议，将用户流量引导到 VPC 子网中的特定目标 Amazon EC2 实例 IP 地址和端口。

您可在创建自定义路由加速器时定义侦听器，并可随时添加更多侦听器。每个侦听器可以有一个或多个终端节点组，每个 AWS 区域都有一个 VPC 端节点组。自定义路由加速器中的侦听器同时支持 TCP 和 UDP 协议。您可以为定义的每个目标端口范围指定一个或多个协议：UDP、TCP 或 UDP 和 TCP。

有关更多信息，请参阅 自定义路由加速器在 AWS Global Accelerator 中的工作原理。

添加、编辑或删除自定义路由监听器

本节介绍如何使用 AWS Global Accelerator 控制台上的自定义路由侦听器。要了解有关将 API 操作与 AWS Global Accelerator 结合使用的信息，请参阅AWS Global Accelerator API 参考。

添加自定义路由加速器侦听器

创建监听程序时指定的范围定义了可用于自定义路由加速器的监听程序端口和目标 IP 地址组合的数量。为获得最大的灵活性，建议您指定较大的端口范围。您指定的每个侦听程序端口范围必须至少包含 16 个端口。

> **Note**
>
> 创建监听程序后，您可以对其进行编辑以添加其他端口范围和相关协议，但不能减少现有端口范围。

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页上，选择自定义路由加速器。
3. 选择 Add listener (添加侦听器)。
4. 在存储库的添加侦听器页上，输入要与加速器关联的侦听器端口范围。

   侦听器支持 1-65535 端口。为了使用自定义路由加速器获得最大的灵活性，我们建议您指定较大的端口范围。
5. 选择 Add listener (添加侦听器)。

编辑自定义路由加速器的侦听器

编辑自定义路由加速器的侦听程序时，请注意，您可以添加其他端口范围和相关协议、增加现有端口范围或更改协议，但不能减少现有端口范围。

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页上，选择加速器。
3. 选择侦听器，然后选择编辑侦听器。
4. 在存储库的编辑侦听器页面上，对现有端口范围或协议进行更改，或添加新端口范围。

   请注意，您不能减小现有端口范围的范围。
5. 选择保存。

删除侦听器

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页上，选择加速器。
3. 选择侦听器，然后选择Remove。
4. 在确认对话框中，选择Remove。

AWS Global Accelerator 中自定义路由加速器的终端节点组

使用 AWS Global Accelerator 中的自定义路由加速器，终端节点组定义虚拟私有云 (VPC) 子网中目标 Amazon EC2 实例接受流量的端口和协议。

您可以为 VPC 子网和 EC2 实例所在的每个 AWS 区域创建自定义路由加速器的终端节点组。自定义路由加速器中的每个终端节点组可以具有多个 VPC 子网终端节点。同样，您可以将每个 VPC 添加到多个终端节点组，但终端节点组必须与不同的侦听器关联。

对于每个终端节点组，您可以指定一组或多个端口范围，其中包括要将流量引导到该区域中 EC2 实例上的端口。对于每个端点组端口范围，您可以指定要使用的协议：UDP、TCP 或 UDP 和 TCP。这为您提供了最大的灵活性，而无需为每个协议复制端口范围集。例如，您可能有一个游戏服务器，其游戏流量通过端口 8080-8090 上的 UDP 运行，而您还有一台服务器通过端口 80 上的 TCP 侦听聊天消息。

要了解更多信息，请参阅“自定义路由加速器在 AWS Global Accelerator 中的工作原理”。

添加、编辑或删除自定义路由加速器的终端节点组

您可以在 AWS Global Accelerator 控制台上或使用 API 操作来处理自定义路由加速器的终端节点组。您可以随时在终端节点组中添加或删除 VPC 子网终端节点。

本节介绍如何在 AWS Global Accelerator 控制台上使用自定义路由加速器的终端节点组。要了解有关将 API 操作与全局加速器结合使用的信息，请参阅AWS Global Accelerator API。

为自定义路由加速器添加终端节点组

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择自定义路由加速器。
3. 在侦听器部分,侦听器 ID下，选择要向其中添加终端节点组的侦听器的 ID。
4. 选择添加终端节点组。
5. 在监听程序的部分中，为终端节点组指定一个区域。
6. 适用于端口和协议集中，输入 Amazon EC2 实例的端口范围和协议。
   - 输入从端口和移植指定端口范围。
   - 对于每个端口范围，指定该范围的一个或多个协议。

端口范围不一定是监听器端口范围的子集，但监听器端口范围中必须有足够的端口总数，以支持您为自定义路由加速器中的终端节点组指定的端口总数。

7. 选择保存。
8. (可选) 选择添加终端节点组为此侦听器添加其他终端节点组。您还可以选择其他侦听器并添加终端节点组。
9. 选择添加终端节点组。

编辑自定义路由加速器的终端节点组

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择自定义路由加速器。
3. 在侦听器部分,侦听器 ID中，选择与终端节点组关联的侦听器的 ID。
4. 选择编辑终端节点组。
5. 在存储库的编辑终端节点组页面上，更改区域、端口范围或端口范围的协议。
6. 选择保存。

删除自定义路由加速器

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择加速器。
3. 在侦听器部分中，选择侦听器，然后选择Remove。
4. 在终端节点组部分中，选择终端节点组，然后选择Remove。
5. 在确认对话框中，选择Remove。

AWS Global Accelerator 中的自定义路由加速器的 VPC 子网终端节点

自定义路由加速器的终端节点是虚拟私有云 (VPC) 子网，可通过加速器接收流量。每个子网可以包含一个或多个 Amazon EC2 实例目标。添加子网终端节点时，全局加速器会生成新的端口映射。然后，您可以使用全局加速器 API 获取子网所有端口映射的静态列表，您可以使用该列表将流量路由到子网中的目标 EC2 实例 IP 地址。有关更多信息，请参阅 。列表自定义路程端口映射。

您只能将流量引导到子网中的 EC2 实例，而不能将其他资源（如负载均衡器）（与标准加速器相比）。支持的 EC2 实例类型列于AWS Global Accelerator 中标准加速器的终端节点。

要了解更多信息，请参阅“自定义路由加速器在 AWS Global Accelerator 中的工作原理”。

当您为自定义路由加速器添加 VPC 子网时，请注意以下事项：

- 默认情况下，通过自定义路由加速器定向的流量无法到达子网中的任何目的地。要使目标实例能够接收流量，您必须选择允许进入子网的所有流量，或者启用到子网中特定实例 IP 地址和端口（目标套接字）的流量。

  > **Important**
  >
  > 更新子网或特定目标以允许或拒绝流量需要一段时间才能在互联网上传播。要确定更改是否已传播，可以调用`DescribeCustomRoutingAccelerator`API 操作来检查加速器状态。有关更多信息，请参阅 。描述路程加速器。

- 由于 VPC 子网保留客户端 IP 地址，因此您应在将子网添加为自定义路由加速器的终端节点时查看相关的安全性和配置信息。有关更多信息，请参阅 使用客户端 IP 地址保留添加端点。

添加、编辑或删除 VPC 子网终端节点

您可以将虚拟私有云 (VPC) 子网终端节点添加到自定义路由加速器中的终端节点组，以便将用户流量定向到子网中的目标 Amazon EC2 实例。

当您从子网中添加和删除 EC2 实例，或者启用或禁用到 EC2 目标的流量时，您可以更改这些目标是否可以接收流量。但是，全局加速器端口映射不会更改。

要允许流量流向子网中的某些目标（但不是所有目标），请输入要允许的每个 EC2 实例的 IP 地址，以及要接收流量的实例上的端口。您指定的 IP 地址必须是子网中 EC2 实例的 IP 地址。您可以从为子网映射的端口指定端口或端口范围。

您可以从加速器中删除 VPC 子网，从终端节点组中删除该 VPC 子网。删除子网不会影响子网本身，但全局加速器不能再将流量引导到子网或子网中的 Amazon EC2 实例。此外，全局加速器将回收 VPC 子网的端口映射，以便可能将它们用于您添加的新子网。

本节中的步骤介绍如何在 AWS Global Accelerator 控制台上添加、编辑或删除 VPC 子网终端节点。要了解有关将 API 操作与 AWS Global Accelerator 结合使用的信息，请参阅AWS Global Accelerator API 参考。

添加 VPC 子网终端节点

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择自定义路由加速器。
3. 在侦听器部分, 用于侦听器 ID下，选择监听程序的 ID。
4. 在终端节点组部分, 用于终端节点组 ID中，选择要向其添加 VPC 子网终端节点的终端节点组（AWS 区域）的 ID。
5. 在终端节点部分，选择添加终端节点。
6. 在存储库的添加终端节点页面, 用于终端节点中，选择 VPC 子网。

   如果您没有任何 VPC，列表中没有任何项目。要继续，请至少添加一个 VPC，然后返回此处的步骤，然后从列表中选择一个 VPC。
7. 对于您添加的 VPC 子网终端节点，您可以选择允许或拒绝向子网中所有目标的流量，也可以仅允许流向特定 EC2 实例和端口。默认设置为拒绝向子网中所有目标的流量。
8. 选择 Add endpoint (添加终端节点)。

允许或拒绝流向特定目标的流量

您可以编辑终端节点的 VPC 子网端口映射，以允许或拒绝流向子网中的特定 EC2 实例和端口（目标套接字）的流量。

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择自定义路由加速器。
3. 在侦听器部分, 用于侦听器 ID下，选择监听程序的 ID。
4. 在终端节点组部分, 用于终端节点组 ID中，选择要编辑的 VPC 子网终端节点的终端节点组（AWS 区域）的 ID。
5. 选择终端节点子网，然后选择查看详细信息。
6. 在存储库的终端节点页面，在端口映射，选择 IP 地址，然后选择编辑。
7. 输入要为其启用流量的端口，然后选择允许这些目标。

允许或拒绝子网的所有流量

您可以更新终端节点以允许或拒绝流向 VPC 子网中所有目标的流量。

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。

2. 在存储库的加速器页面上，选择自定义路由加速器。
3. 在侦听器部分, 用于侦听器 ID下，选择监听程序的 ID。
4. 在终端节点组部分, 用于终端节点组 ID中，选择要更新的 VPC 子网终端节点的终端节点组（AWS 区域）的 ID。
5. 选择允许/拒绝所有流量。
6. 选择一个选项，允许所有流量或拒绝所有流量，然后选择Save。

删除终端节点

1. 打开全局加速器控制台，网址为https://console.aws.amazon.com/globalaccelerator/home。
2. 在存储库的加速器页面上，选择自定义路由加速器。
3. 在侦听器部分, 用于侦听器 ID下，选择监听程序的 ID。
4. 在终端节点组部分, 用于终端节点组 ID中，选择要删除的 VPC 子网终端节点的终端节点组（AWS 区域）的 ID。
5. 选择删除终端节点。
6. 在确认对话框中，选择Remove。

AWS Global Accelerator 中的 DNS 寻址和自定义域

本章介绍 AWS Global Accelerator 如何进行 DNS 路由，并包括有关将自定义域与全球加速器结合使用的信息。

主题

Support 全局加速器中的 DNS 寻址

创建自定义路由或标准加速器时，全局加速器会为您预配两个静态 IP 地址。它还将为加速器分配默认域名系统 (DNS) 名称，与`a1234567890abcdef.awsglobalaccelerator.com`，它指向静态 IP 地址。静态 IP 地址通过从 AWS 边缘网络到终端节点的任意广播进行全球通告。您可以使用加速器的静态 IP 地址或 DNS 名称将流量路由到加速器。DNS 服务器和 DNS 解析器使用循环来解析加速器的 DNS 名称，因此该名称将解析为加速器的静态 IP 地址，由 Amazon Route 53 按随机顺序返回。客户端通常使用返回的第一个 IP 地址。

> **Note**
>
> 全局加速器创建两个指针 (PTR) 记录，将加速器的静态 IP 地址映射到由全局加速器生成的相应 DNS 名称，以支持反向 DNS 查找。该区域也称作反向托管区域。请注意，全局加速器为您生成的 DNS 名称不可配置，并且您无法创建指向您的自定义域名的 PTR 记录。全球加速器也不会为您带到 AWS (BYOIP) 的 IP 地址范围内的静态 IP 地址创建 PTR 记录。

将自定义域流量路由到您的加速器

在大多数情况下，您可以将 DNS 配置为使用自定义域名（例如`www.example.com`），而不是使用分配的静态 IP 地址或默认 DNS 名称。首先，使用 Amazon Route 53 或其他 DNS 提供商创建域名，然后使用您的全球加速器 IP 地址添加或更新 DNS 记录。您也可以将自定义域名与加速器的 DNS 名称相关联。完成 DNS 配置并等待更改在互联网上传播。现在，在客户端使用自定义域名进行请求时，DNS 服务器将它解析为 IP 地址 (随机顺序) 或加速器的 DNS 名称。

若要在使用 Route 53 作为 DNS 服务时将自定义域名与全局加速器一起使用，请创建一个别名记录，将您的自定义域名指向分配给加速器的 DNS 名称。别名记录是 DNS 的 Route 53 扩展。别名记录与 CNAME 记录相似，但您既可以为根域 (如`example.com`，以及子域，例如`www.example.com`。有关更多信息，请参阅 。在别名和非别名记录之间做出选择Amazon Route 53 开发人员指南中的 Create。

要使用加速器的别名记录设置 Route 53，请遵循以下主题中包含的指导：别名目标Amazon Route 53 开发人员指南中的 Create。要查看全局加速器的信息，请向下滚动别名目标页.

在 AWS Global Accelerator 中引入您自己的 IP 地址 (BYOIP)

AWS Global Accelerator 使用静态 IP 地址作为加速器的入口点。这些 IP 地址是来自 AWS 节点位置的任意播放的。默认情况下，全局加速器从Amazon IP 地址池。您可以将这些入口点配置为来自您自己的地址范围的 IPv4 地址，而不是使用全局加速器提供的 IP 地址。本主题介绍了如何将您自己的 IP 地址范围用于全局加速器。

您可将自己的部分或全部公有 IPv4 地址从本地网络引入到 AWS 账户中以用于全球加速器。您将继续拥有地址范围，但 AWS 会将其公布在 Internet 上。

您不能将您带到 AWS 的 IP 地址用于一个 AWS 服务与另一个服务一起使用。本章中的步骤介绍了如何将您自己的 IP 地址范围仅用于 AWS Global Accelerator。有关在 Amazon EC2 中使用自己的 IP 地址范围的步骤，请参阅自带 IP 地址 (BYOIP)Amazon EC2 用户指南中。

> **Important**
>
> 在通过 AWS 对 IP 地址范围进行发布之前，您必须停止从其他位置公布它。如果 IP 地址范围是多宿主（即，该范围由多个服务提供商同时通告），我们无法保证到达地址范围的流量将进入我们的网络或您的 BYOIP 广告工作流程会成功完成。

在将地址范围引入 AWS 中之后，它会在您的账户中显示为地址池。创建加速器时，您可以将范围内的一个 IP 地址分配给该加速器。全局加速器会从 Amazon IP 地址范围为您分配第二个静态 IP 地址。如果您将两个 IP 地址范围带到 AWS，则可以将每个范围中的一个 IP 地址分配给您的加速器。此限制是因为全局加速器将每个地址范围分配给不同的网络区域，以实现高可用性。

要将您自己的 IP 地址范围与全局加速器结合使用，请查看要求，然后按照本主题中提供的步骤操作。

主题

Requirements

每个 AWS 账户最多可将两个合格 IP 地址范围调至 AWS Global Accelerator。

要符合条件，您的 IP 地址范围必须满足以下要求：

- IP 地址范围必须在以下区域 Internet 注册表 (RIR) 中注册 IP 地址范围：American Registry Registry (ARIN)、Réseaux IP Européens Network Centre (RIPE) 或 Aserican Network Network Instry Instry Centre (APNIC)。地址范围必须由企业或机构实体注册。它不能由个人注册。
- 您可以引入的最具体地址范围是 /24。IP 地址的前 24 位指定网络号。例如，198.51.100 是 IP 地址 198.51.100.0 的网络号。
- 地址范围中的 IP 地址必须具有干净的历史记录。也就是说，他们不能拥有不良的声誉或与恶意行为相关联。如果我们调查 IP 地址范围的声誉，并发现其中包含的 IP 地址没有干净的历史记录，我们保留拒绝此 IP 地址范围的权利。

此外，我们还需要以下分配和分配网络类型或状态，具体取决于您注册 IP 地址范围的位置：

- 阿林：`Direct Allocation`和`Direct Assignment`网络类型
- 成熟:`ALLOCATED PA`、`LEGACY`, 和`ASSIGNED PI`分配状态
- APNIC：`ALLOCATED PORTABLE`和`ASSIGNED PORTABLE`分配状态

准备将您的 IP 地址范围引入您的 AWS 账户：授权

为确保只有您可以将您的 IP 地址空间带到亚马逊，我们需要两项授权：

- 您必须授权亚马逊公布 IP 地址范围。
- 您必须提供证据证明您拥有 IP 地址范围，因此有权将其带到 AWS。

> **Note**
>
> 当您使用 BYOIP 将 IP 地址范围带入 AWS 时，您无法在我们进行广告时将该地址范围的所有权转让给其他账户或公司。您也不能将 IP 地址范围从一个 AWS 账户直接转移到另一个账户。要转让所有权或在 AWS 账户之间进行转移，您必须取消配置地址范围，然后新所有者必须按照步骤将地址范围添加到其 AWS 账户。

要授权亚马逊宣传 IP 地址范围，您需要向亚马逊提供签名的授权消息。使用路由起点授权 (ROA) 提供此授权。ROA 是您通过区域 Internet 注册表 (RIR) 创建的路由通告的加密声明。ROA 包含 IP 地址范围、允许发布 IP 地址范围的自治系统编号 (ASN) 以及失效日期。ROA 授权 Amazon 在特定自治系统 (AS) 下公布 IP 地址范围。

ROA 不会授权您的 AWS 账户将 IP 地址范围引入 AWS。要提供此授权，您必须在 IP 地址范围的注册数据访问协议 (RDAP) 备注中发布自签名 X.509 证书。该证书包含一个公有密钥，AWS 使用该密钥验证您所提供的授权上下文签名。请确保您的私有密钥的安全，并使用该密钥对授权上下文消息进行签名。

下面几节提供了完成这些授权任务的详细步骤。这些步骤中的命令在 Linux 上受支持。如果您使用 Windows，则可以访问适用于 Linux 的 Windows 子系统来运行 Linux 命令。

提供授权的步骤

- 步骤 1: 创建一个 ROA 对象
- 步骤 2: 创建自签名 X.509 证书
- 步骤 3: 创建签名授权消息

步骤 1: 创建一个 ROA 对象

创建 ROA 对象以授权 Amazon ASN 16509 来公布您的 IP 地址范围以及当前授权的 ASN 来公布该 IP 地址范围。ROA 必须包含您要引入 AWS 的 /24 IP 地址，并且您必须将最大长度设置为 /24。

有关创建 ROA 请求的详细信息，请参阅以下部分，具体取决于您注册 IP 地址范围的位置：

- 阿林：ROA 请求
- 成熟: 管理 ROA
- APNIC：路由管理

步骤 2: 创建自签名 X.509 证书

创建 key pair 和自签名 X.509 证书，然后将该证书添加到您的 RIR 的 RDAP 记录。以下步骤介绍了如何执行这些任务。

> **Note**
>
> 这些区域有：`openssl`命令需要 OpenSSL 版本 1.0.2 或更高版本。

创建和添加 X.509 证书

1. 使用以下命令生成 RSA 2048 位 key pair。

   ```
   openssl genrsa -out private.key 2048
   ```

2. 使用以下命令从该 key pair 创建一个公有 X.509 证书。

   ```
   openssl req -new -x509 -key private.key -days 365 | tr -d "\n" > publickey.cer
   ```

   在此示例中，该证书在 365 天后过期，在此日期后它将不能是受信任的。在运行命令时，请确保将`-days`选项设置为所需的值，以获得正确的过期。当系统提示您提供其他信息时，您可以接受默认值。

3. 使用 X.509 证书更新 RIR 的 RDAP 记录，具体取决于您的 RIR。

   1. 使用以下命令查看您的证书。

      ```
      cat publickey.cer
      ```

   2. 通过执行以下操作添加证书：

      > **Important**
      >
      > 请务必包含`-----BEGIN CERTIFICATE-----`和`-----END CERTIFICATE-----`从证书。

      - 对于 ARN，将证书添加到`Public Comments`部分，了解您的 IP 地址范围。
      - 对于 RIPE，将证书添加为新`descr`字段中的 IP 地址范围。

- 对于 APNIC，请将公钥以电子邮件形式发送至helpdesk@apnic.net，APNIC 授权的 IP 地址联系人，请求他们将其手动添加到remarks字段。

步骤 3: 创建签名授权消息

创建签名的授权消息，以允许亚马逊公布您的 IP 地址范围。

消息的格式如下所示，其中YYYYMMDD日期是消息的到期日期。

```
1|aws|aws-account|address-range|YYYYMMDD|SHA256|RSAPSS
```

创建签名授权消息

1. 创建一个明文授权消息，并将其存储在名为的text_message，如以下示例所示。将示例账号、IP 地址范围和失效日期替换为您自己的值。

   ```
   text_message="1|aws|123456789012|203.0.113.0/24|20191201|SHA256|RSAPSS"
   ```

2. 签署授权消息text_message使用在上一部分中创建的 key pair。
3. 将消息存储在名为的变量中signed_message，如以下示例所示。

   ```
   signed_message=$(echo $text_message | tr -d "\n" | openssl dgst -sha256 -sigopt
         rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private.key -keyform
    PEM | openssl base64 |
         tr -- '+=/' '-_~' | tr -d "\n")
   ```

预配置地址范围以用于 AWS Global Accelerator

在预置一个地址范围以用于 AWS 时，您需要确认您拥有该地址范围，并授权 Amazon 公布该地址范围。我们将验证您拥有该地址范围。

您必须使用 CLI 或全局加速器 API 操作预配置地址范围。此功能不适用于 AWS 控制台。

要预配置地址范围，请使用以下ProvisionByoipCidr命令。这些区域有：--cidr-authorization-context参数使用您在上一节中创建的变量，而不是 ROA 消息。

```
aws globalaccelerator provision-byoip-cidr --cidr address-range --cidr-authorization-
context Message="$text_message",Signature="$signed_message"
```

以下是预配地址范围的示例。

```
aws globalaccelerator provision-byoip-cidr
    --cidr 203.0.113.25/24
    --cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

预置地址范围是一项异步操作，因此该调用会立即返回。但是，地址范围尚未准备好使用，直到其状态从PENDING_PROVISIONING到READY。完成预置过程最多可能需要 3 周时间。要监控您预置的地址范围的状态，请使用以下列表命令：

```
aws globalaccelerator list-byoip-cidrs
```

要查看 IP 地址范围的状态列表，请参阅比奥普契医生。

配置 IP 地址范围后，State返回方list-byoip-cidrs是READY。例如：

```
{
    "ByoipCidrs": [
        {
            "Cidr": "203.0.113.0/24",
            "State": "READY"
        }
    ]
}
```

通过 AWS 发布地址范围

预配置地址范围后，即可对其进行公布。您必须发布预配置的确切地址范围。您不能只发布预配置的地址范围的一部分。此外，您必须停止从其他位置公布您的 IP 地址范围，然后才能通过 AWS 公布它。

您必须使用 CLI 或全球加速器 API 操作来宣传（或停止广告）您的地址范围。此功能不适用于 AWS 控制台。

> **Important**
>
> 在您使用全球加速器池中的 IP 地址之前，请确保您的 IP 地址范围已由 AWS 公布。

要发布地址范围，请使用以下广告命令。

```
aws globalaccelerator advertise-byoip-cidr --cidr address-range
```

以下是请求全局加速器通告地址范围的示例。

```
aws globalaccelerator advertise-byoip-cidr --cidr 203.0.113.0/24
```

要监控您公布的地址范围的状态，请使用以下列表命令。

```
aws globalaccelerator list-byoip-cidrs
```

当您的 IP 地址范围被通告时，State返回方list-byoip-cidrs是ADVERTISING。例如：

```
{
    "ByoipCidrs": [
        {
            "Cidr": "203.0.113.0/24",
            "State": "ADVERTISING"
        }
    ]
}
```

要停止公布地址范围，请使用以下withdraw-byoip-cidr命令。

> **Important**
>
> 要停止广告您的地址范围，首先必须删除具有从地址池中分配的静态 IP 地址的所有加速器。要使用控制台或使用 API 操作删除加速器，请参阅 删除加速器。

```
aws globalaccelerator withdraw-byoip-cidr --cidr address-range
```

以下是请求全局加速器撤回地址范围的示例。

```
aws globalaccelerator withdraw-byoip-cidr
    --cidr 203.0.113.25/24
```

取消预配置地址范围

要停止在 AWS 上使用您的地址范围，您必须先删除具有从地址池中分配的静态 IP 地址的任何加速器，并停止公布您的地址范围。完成这些步骤后，您可以取消配置地址范围。

您必须使用 CLI 或全球加速器 API 操作停止广告并取消配置您的地址范围。此功能不适用于 AWS 控制台。

步骤 1: 删除所有关联的加速器。要使用控制台或使用 API 操作删除加速器，请参阅 删除加速器。

步骤 2. 停止公布地址范围。要停止公布范围，请使用以下提款命令。

```
aws globalaccelerator withdraw-byoip-cidr --cidr address-range
```

步骤 3. 取消预配置地址范围。要取消预配置范围，请使用以下取消预配置命令。

```
aws globalaccelerator deprovision-byoip-cidr --cidr address-range
```

使用您的 IP 地址创建加速器

现在，您可以使用您的 IP 地址创建加速器。如果您将一个地址范围带到 AWS，则可以为您的加速器分配一个 IP 地址。如果您带来了两个地址范围，则可以将每个地址范围中的一个 IP 地址分配给加速器。

可以使用您自己的 IP 地址创建静态 IP 地址的加速器：

- 使用全局加速器控制台创建加速器。 有关更多信息，请参阅 创建或更新标准加速器 和 创建或更新自定义路由加速器。
- 使用全局加速器 API 创建加速器。 有关更多信息，包括使用 CLI 示例，请参阅创建加速器和创建自定义路程加速器AWS Global Accelerator API 参考中。

在 AWS Global Accelerator 中保留客户端 IP 地址

保留和访问 AWS Global Accelerator 客户端 IP 地址的选项取决于您使用加速器设置的终端节点。有两种类型的终端节点可以在传入数据包中保留客户端的源 IP 地址：应用程序负载均衡器和 Amazon EC2 实例。

- 使用面向 Internet 的应用 Application Load Balancer 器作为带有全局加速器的终端节点时，默认情况下为新加速器启用客户端 IP 地址保留。这意味着对于到达负载均衡器的数据包，原始客户端的源 IP 地址将保留。您可以选择在创建加速器时禁用此选项，也可以在稍后编辑加速器。
- 当您将内部应用程序负载均衡器或 EC2 实例与全局加速器结合使用时，终端节点始终启用客户端 IP 地址保留。

> **Note**
>
> 全局加速器不支持 Network Load Balancer 器和弹性 IP 地址终端节点的客户端 IP 地址保留。

当您计划添加客户端 IP 地址保留时，需要注意以下事项：

- 在添加流量并开始将流量路由到保留客户端 IP 地址的终端之前，请确保已更新所有必需的安全配置（例如安全组），以便在允许列表中包括用户客户端 IP 地址。
- 仅在特定 AWS 区域支持客户端 IP 地址保留。有关更多信息，请参阅 支持的 AWS 区域用于客户端 IP 地址保留。

主题

如何启用客户端 IP 地址保留

创建新的加速器时，默认情况下会为受支持的终端启用客户端 IP 地址保留。

请注意以下事项：

- 内部应用程序负载均衡器和 EC2 实例始终启用客户端 IP 地址保留。您不能禁用这些终端节点的选项。
- 当您使用 AWS 控制台创建新的加速器时，默认情况下为应用 Application Load Balancer 器终端节点启用客户端 IP 地址保留选项。如果您不希望为面向 Internet 的应用 Application Load Balancer 终端节点保留客户端 IP 地址，则可以随时禁用此选项。
- 当您使用 AWS CLI 或 API 操作创建新的加速器并且未指定客户端 IP 地址保留选项时，面向 Internet 的应用 Application Load Balancer 器终端节点默认启用客户端 IP 地址保留。
- 全局加速器不支持 Network Load Balancer 器和弹性 IP 地址终端节点的客户端 IP 地址保留。

对于现有加速器，您可以将不保留客户端 IP 地址的终端转换为保留客户端 IP 地址的终端节点。现有 Application Load Balancer 终端节点可转换为新的 Application Load Balancer 终端节点，并且可以将现有弹性 IP 地址终端节点转换为 EC2 实例终端节点。（Network Load Balancer 终端节点不支持客户端 IP 地址保留。）要转换到新终端节点，我们建议您通过执行以下操作将流量从现有终端节点缓慢移动到具有客户端 IP 地址保留的新终端节点：

- 对于现有 Application Load Balancer 器终端节点，首先向 Global 加速器添加一个重复的 Application Load Balancer 器终结点，该终结点针对相同的后端，如果它是面向 Internet 的应用程序负载均衡器，则为其启用客户端 IP 地址保留。然后调整终端上的权重，以便从负载均衡器中慢慢移动流量不是启用负载均衡器的客户端 IP 地址保留替换为客户端 IP 地址保留。
- 对于现有弹性 IP 地址终端节点，您可以将流量移动到具有客户端 IP 地址保留的 EC2 实例终端节点。首先将 EC2 实例终端节点添加到全局加速器，然后调整终端节点上的权重，以便将流量从弹性 IP 地址终端节点缓慢移动到 EC2 实例终端节点。

如需分步过渡指导，请参阅 转换端点以使用客户端 IP 地址保留。

客户端 IP 地址保留的好处

对于未启用客户端 IP 地址保留的端点，全局加速器服务在边缘网络中使用的 IP 地址将替换请求用户的 IP 地址作为到达数据包中的源地址。当流量传输到加速器后面的系统时，原始客户端的连接信息（例如客户端的 IP 地址和客户端端口）不会保留。这适用于许多应用程序，尤其是那些可供所有用户（如公共网站）使用的应用程序。

但是，对于其他应用程序，您可能希望通过使用带客户端 IP 地址保留的终端来访问原始客户端 IP 地址。例如，当您拥有客户端 IP 地址时，您可以根据客户端 IP 地址收集统计信息。您还可以使用基于

IP 地址的过滤器，例如Application Load Balancers 上的安全组来过滤流量。您可以在应用程序中应用特定于用户 IP 地址的逻辑，这些应用程序在该应用 Application Load Balancer 器终结点后面的 Web 层服务器上运行，方法是使用负载均衡器的X-Forwarded-For标头，其中包含原始客户端 IP 地址信息。您还可以在与应用 Application Load Balancer 关联的安全组规则中使用客户端 IP 地址保留。有关更多信息，请参阅 如何在 AWS Global Accelerator 中保留客户端 IP 地址。对于 EC2 实例终端节点，将保留原始客户端 IP 地址。

对于没有客户端 IP 地址保留的终端，您可以筛选全局加速器从边缘转发流量时使用的源 IP 地址。通过查看全局加速器流日志，您可以查看有关传入数据包的源 IP 地址（也是客户端 IP 地址，当启用客户端 IP 地址保留时）的信息。有关更多信息，请参阅 Global Accelerator 边缘服务器的位置和 IP 地址范围和 AWS Global Accelerator 中的流日志。

如何在 AWS Global Accelerator 中保留客户端 IP 地址

AWS Global Accelerator 为 Amazon EC2 实例和应用程序负载均衡器以不同方式保留客户端的源 IP 地址：

- 对于 EC2 实例终端节点，将为所有流量保留客户端的 IP 地址。
- 对于具有客户端 IP 地址保留的 Application Load Balancer 器终端节点，全局加速器与 Application Load Balancer 器一起工作，以提供X-Forwarded标头，X-Forwarded-For，其中包括原始客户端的 IP 地址，以便您的 Web 层可以访问它。

HTTP 请求和 HTTP 响应使用标头字段发送有关 HTTP 消息的信息。标头字段为冒号分隔的名称值对，各个值对之间由回车符 (CR) 和换行符 (LF) 进行分隔。RFC 2616 中定义了标准 HTTP 标头字段集，消息头。此外还有应用程序广泛使用的非标准 HTTP 标头。某些非标准 HTTP 标头具有X-Forwardedprefix.

由于 Application Load Balancer 终止传入的 TCP 连接并创建到您的后端目标的新连接，因此它不会将客户端 IP 地址一直保留到您的目标代码（例如实例、容器或 Lambda 代码）。您的目标在 TCP 数据包中看到的源 IP 地址是 Application Load Balancer 的 IP 地址。但是，Application Load Balancer 通过将原始客户端 IP 地址从原始数据包的回复地址中删除并将其插入 HTTP 标头，然后再通过新的 TCP 连接将请求发送到您的后端，从而保留原始客户端 IP 地址。

这些区域有：X-Forwarded-For请求标头的格式如下所示：

```
X-Forwarded-For: client-ip-address
```

以下示例显示了X-Forwarded-ForIP 地址为 203.0.113.7 的客户端的请求标头。

```
X-Forwarded-For: 203.0.113.7
```

客户端 IP 地址保留的最佳实践

在 AWS Global Accelerator 中使用客户端 IP 地址保留时，请记住本节中有关弹性网络接口和安全组的信息和最佳实践。

为支持客户端 IP 地址保留，全球加速器在您的 AWS 账户中创建弹性网络接口 — 每个存在终端节点的子网一个。弹性网络接口 是 VPC 中表示虚拟网卡的逻辑网络组件。全局加速器使用这些弹性网络接口将流量路由到加速器后面配置的端点。支持以这种方式路由流量的终端节点是应用程序负载均衡器（内部和面向互联网的）和 Amazon EC2 实例。

> **Note**
>
> 在全球加速器中添加内部 Application Load Balancer 器或 EC2 实例终端节点时，您可以通过将互联网流量定位在私有子网中，从而使互联网流量直接流入和流出虚拟私有云 (VPC) 中的终端节点。有关更多信息，请参阅 AWS Global Accelerator 中的 VPC 连接安全。

全局加速器如何使用弹性网络接口

如果启用了客户端 IP 地址保留的应用 Application Load Balancer 器，则负载均衡器所在的子网数量决定了全局加速器在您的帐户中创建的弹性网络接口的数量。全局加速器为每个子网创建一个 elastic network interface，该子网中至少有一个 Application Load Balancer 器的 elastic network interface，该接口由您账户中的加速器前面。

以下示例说明了它的工作原理：

- 示例 1：如果应用程序负载均衡器在子网 A 和子网 B 中具有弹性网络接口，然后将负载均衡器添加为加速器终端节点，则全局加速器会创建两个弹性网络接口，每个子网中一个。
- 示例 2：例如，如果将子网 A 和子网 B 中具有弹性网络接口的 ALB1 添加到加速器 1，然后在子网 A 和子网 B 中添加具有弹性网络接口的 ALB2 到加速器 2，则全局加速器只创建两个弹性网络接口：一个在子网 A 中，一个在子网 B 中。
- 示例 3：如果将子网 A 和子网 B 中具有弹性网络接口的 ALB1 添加到加速器 1，然后将具有子网 A 和子网 C 中弹性网络接口的 ALB2 添加到加速器 2，全局加速器将创建三个弹性网络接口：一个在子网 A，一个在子网 B 中，一个，一个在子网络接口，一个在子网络。子 NetA 中的 elastic network interface 为加速器 1 和加速器 2 提供通信。

如示例 3 所示，如果同一子网中的端点位于多个加速器后面，则弹性网络接口将在加速器之间重复使用。

全局加速器创建的逻辑弹性网络接口不代表单个主机、吞吐量瓶颈或单点故障。与在可用区或子网中显示为单个 elastic network interface 的其他 AWS 服务（如网络地址转换 (NAT) 网关或网络负载均衡器）一样，全球加速器是作为水平扩展、高可用性的服务实现的。

评估加速器中端点使用的子网数量，以确定全局加速器将创建的弹性网络接口的数量。在创建加速器之前，请确保您有足够的 IP 地址空间容量用于所需的弹性网络接口，每个相关子网至少有一个可用 IP 地址。如果没有足够的可用 IP 地址空间，则必须创建或使用具有足够可用 IP 地址空间的子网，用于应用 Application Load Balancer 器和关联的全局加速器弹性网络接口。

当全局加速器确定您帐户中加速器中的任何终端节点未使用 elastic network interface 时，全局加速器将删除该接口。

由全局加速器创建的安全组

使用全局加速器和安全组时，请查看以下信息和最佳做法。

- 全局加速器创建与其弹性网络接口关联的安全组。尽管系统不会阻止您执行此操作，但您不应编辑这些组的任何安全组设置。
- 全局加速器不会删除它创建的安全组。但是，如果您帐户中的加速器中的任何终端节点没有使用 elastic network interface，则全局加速器会删除该接口。
- 您可以将全局加速器创建的安全组用作您维护的其他安全组中的源组，但全局加速器仅将流量转发到您在 VPC 中指定的目标。
- 如果修改全局加速器创建的安全组规则，则终端节点可能会变得不正常。如果发生这种情况，请联系AWS Support以获取帮助。
- 全局加速器为每个 VPC 创建一个特定的安全组。无论 elastic network interface 与哪个子网关联，为特定 VPC 中的终端节点创建的弹性网络接口都使用相同的安全组。

支持的 AWS 区域用于客户端 IP 地址保留

您可以在以下 AWS 区域为 AWS Global Accelerator 启用客户端 IP 地址保留。

区域名称	区域
US East (Ohio)	`us-east-2`
US East (N. Virginia)	`us-east-1`

区域名称	区域
US West (N. California)	us-west-1 (except AZ usw1-az2)
US West (Oregon)	us-west-2
Africa (Cape Town)	af-south-1
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Osaka)	ap-northeast-3
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1 (except AZ apne1-az3)
Asia Pacific (Seoul)	ap-northeast-2
Canada (Central)	ca-central-1 (except AZ cac1-az3)
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europe (Milan)	eu-south-1
Europe (Paris)	eu-west-3
Europe (Stockholm)	eu-north-1
Middle East (Bahrain)	me-south-1
South America (São Paulo)	sa-east-1

中的日志记录和监控

您可以使用流日志记录和 AWS CloudTrail 监控您的 AWS Global Accelerator 中的加速器，分析流量模式，以及解决与您的监控器和终端节点相关的问题。

主题

AWS Global Accelerator 中的流日志

流日志允许您在 AWS Global Accelerator 中捕获有关传入和传出 AWS Global Accelerator 的加速器中进出网络接口的 IP 地址流量的信息。流日志数据将发布到 Amazon S3，您可以在创建流日志后检索和查看您的数据。

流日志可以帮助您完成大量任务。例如，您可以排查流量未到达终端节点的原因，这反过来又可帮助您诊断限制过于严格的安全组规则。您还可以使用流日志作为安全工具来监视到达终端节点的流量。

流日志记录代表您的流日志中的网络流。每个记录捕获特定捕获窗口中的特定 5 元组的网络流。5 元组是一组 5 个不同的值，指定 IP 流的源、目标和协议。捕获窗口是一段持续时间，在这段时间内流日志服务会聚合数据，然后再发布流日志记录。捕获窗口大约为 10 秒钟，但最长可以为 1 分钟。

使用流日志时会收取 CloudWatch 日志费用，即使日志直接发布到 Amazon S3。有关更多信息，请参阅 。将日志传送到 S3atAmazon CloudWatch 定价。

主题

将流日志发布到 Amazon S3

AWS Global Accelerator 的流日志将发布到 Amazon S3，发布到您指定的现有 S3 存储桶。流日志记录将发布到存储桶中存储的一系列日志文件对象。

要创建与流日志配合使用的 Amazon S3 存储桶，请参阅创建存储桶中的Amazon Simple Storage Service 入门指南。

流日志文件

流日志收集流日志记录，将它们合并到日志文件，然后每隔 5 分钟将日志文件发布到 Amazon S3 存储桶。每个日志文件包含在上一个 5 分钟内记录的 IP 地址流量的流日志记录。

日志文件的最大文件大小为 75 MB。如果日志文件在 5 分钟期间内达到文件大小限制，流日志会停止向它添加流日志记录，将它发布到 Amazon S3 存储桶，然后创建一个新的日志文件。

日志文件将保存到指定的 Amazon S3 存储桶，并使用由流日志的 ID、区域及其创建日期决定的文件夹结构。存储桶文件夹结构使用以下格式：

```
s3-bucket_name/s3-bucket-prefix/AWSLogs/aws_account_id/globalaccelerator/region/yyyy/mm/dd/
```

同样，流日志的 ID、区域及其创建日期和时间决定。文件名使用以下格式：

```
aws_account_id_globalaccelerator_accelerator_id_flow_log_id_timestamp_hash.log.gz
```

请注意以下有关日志文件的文件夹和文件名结构的内容：

- 时间戳使用 YYYYMMDDTHHmmZ 格式。
- 如果您为 S3 存储桶前缀指定斜杠 (/)，则日志文件存储桶文件夹结构将包含双斜杠 (//)，如下所示：

  ```
  s3-bucket_name//AWSLogs/aws_account_id
  ```

以下示例显示了 AWS 账户创建的流日志日志的文件夹结构和文件名123456789012的加速器，ID 为1234abcd-abcd-1234-abcd-1234abcdefgh，于 2018 年 11 月 23 日上午 0 时 05 分举行：

```
my-s3-bucket/prefix1/AWSLogs/123456789012/globalaccelerator/us-west-2/2018/11/23/123456789012_globalaccelerator_1234abcd-abcd-1234-abcd-1234abcdefgh_20181123T0005Z_1fb1234.log.gz
```

单个流日志文件包含具有多个 5 元组记录的交错条目；即client_ip、client_port、accelerator_ip、accelerator_port、protocol。要查看加速器的所有流日志文件，请查找accelerator_id和您的account_id。

用于将流日志发布到 Amazon S3 的 IAM 角色

IAM 委托人（例如，IAM 用户）必须具有足够的权限才能将流日志发布到 Amazon S3 存储桶。IAM 策略必须包含以下权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeliverLogs",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowGlobalAcceleratorService",
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "s3Perms",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

针对流日志的 Amazon S3 存储桶权限

默认情况下，Amazon S3 存储桶及其中包含的对象是私有的。只有存储桶拥有者才能访问存储桶和其中存储的对象。不过，存储桶拥有者可以通过编写访问策略来向其他资源和用户授予访问权限。

如果创建流日志的用户拥有存储桶，服务会自动将以下策略附加到存储桶，以授予流日志将日志发布到存储桶的权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/
*",
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-
control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name"
        }
    ]
}
```

如果创建流日志的用户不拥有存储桶，也没有存储桶的 GetBucketPolicy 和 PutBucketPolicy 权限，流日志创建操作会失败。在这种情况下，存储桶拥有者必须手动将上述策略添加到存储桶，并指定流日志创建者的 AWS 账户 ID。有关更多信息，请参阅 。如何添加 S3 存储桶策略？中的Amazon Simple Storage Service 入门指南。如果存储桶从多个账户接收流日志，则将 Resource 元素条目添加到每个账户的 AWSLogDeliveryWrite 策略声明。

例如，以下存储桶策略允许 AWS 账户 123123123123123 和 456456 将流日志发布到名为flow-logs名为的存储桶中log-bucket：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
```

```
            "Action": "s3:PutObject",
            "Resource": [
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/123123123123/*",
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/456456456456/*"
             ],
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-
control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::log-bucket"
        }
    ]
}
```

> **Note**
>
> 我们建议您授予AWSLogDeliveryAclCheck和AWSLogDeliveryWrite权限添加到日志传输服务委托人（而不是单个 AWS 账户 ARN）。

与 SSE-KMS 存储桶结合使用时必需的 CMK 密钥策略

如果使用具有客户托管的客户主密钥 (CMK) 的 AWS KMS 托管密钥 (SSE-KMS) 为 Amazon S3 存储桶启用了服务器端加密，则必须将以下内容添加到 CMK 的密钥策略中，以便流日志可以将日志文件写入存储桶：

```
{
    "Sid": "Allow AWS Global Accelerator Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Amazon S3 日志文件权限

除了必需的存储桶策略之外，Amazon S3 使用访问控制列表 (ACL) 管理对流日志创建的日志文件的访问。默认情况下，存储桶拥有者对每个日志文件具有 FULL_CONTROL 权限。如果日志传输拥有者与存储桶拥有者不同，则没有权限。日志传输账户具有 READ 和 WRITE 权限。有关更多信息，请参阅 。访问控制列表 (ACL) 概述中的Amazon Simple Storage Service 入门指南。

允许将流日志发布到 Amazon S3

要在 AWS Global Accelerator 中启用流日志，请按照此过程中的步骤操作。

在 AWS Global Accelerator 中启用流日志

1. 为 AWS 账户中的流日志创建 Amazon S3 存储桶。
2. 为启用流日志的 AWS 用户添加所需的 IAM 策略。有关更多信息，请参阅 用于将流日志发布到 Amazon S3 的 IAM 角色。
3. 使用要用于日志文件的 Amazon S3 存储桶名称和前缀运行以下 AWS CLI 命令：

```
aws globalaccelerator update-accelerator-attributes
       --accelerator-arn
 arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh
       --region us-west-2
       --flow-logs-enabled
       --flow-logs-s3-bucket s3-bucket-name
       --flow-logs-s3-prefix s3-bucket-prefix
```

处理 Amazon S3 中的流日志记录

日志文件是压缩文件。如果您使用 Amazon S3 控制台打开这些日志文件，则将对其进行解压缩，并且将显示流日志记录。如果您下载这些文件，则必须对其进行解压才能查看流日志记录。

日志文件传输计时

AWS Global Accelerator 一个小时内会为您配置的加速器提交若干次日志文件。一般而言，日志文件包含有关加速器在给定时间段内收到的请求的信息。Global Accelerator 通常会在日志中所显示事件发生后的一个小时内将该时间段内的日志文件传输至 Amazon S3 存储桶。某个时间段内的某些或所有日志文件条目有时可延迟长达 24 小时。当日志条目延迟后，Global Accelerator 会将它们保存在其文件名称包括发生请求的时间段的日期和时间（而不是文件传输的日期和时间）的日志文件中。

创建日志文件时，Global Accelerator 将在日志文件涵盖的时间段内从收到请求的所有边缘站点整合加速器的信息。

Global Accelerator 在您启用日志记录后大约四个小时开始可靠地传输日志文件。您可能会获得一些在此时间之前的日志文件。

> **Note**
>
> 如果在此期间没有用户连接到您的加速器，您将不会收到该期间的任何日志文件。

流日志记录语法

流日志记录是以空格分隔的字符串，采用以下格式：

```
<version> <aws_account_id> <accelerator_id> <client_ip>
<client_port> <accelerator_ip> <accelerator_port> <endpoint_ip>
<endpoint_port> <protocol> <ip_address_type> <packets>
<bytes> <start_time> <end_time> <action> <log-status>
<globalaccelerator_source_ip> <globalaccelerator_source_port>
<endpoint_region> <globalaccelerator_region> <direction> <vpc_id>
```

1.0 版格式不包括 VPC 标识符vpc_id。版本 2.0 版格式，其中包含vpc_id，是在全局加速器将流量发送到具有客户端 IP 地址保留的终端节点时生成的。

下表描述了流日志记录的各个字段。

字段	描述
version	流日志版本。
aws_account_id	流日志的 AWS 账户 ID。
accelerator_id	为其记录流量的加速器的 ID。
client_ip	源 IPv4 地址。
client_port	源端口。

字段	描述
accelerator_ip	加速器的 IP 地址。
accelerator_port	加速器的端口。
endpoint_ip	流量的目标 IP 地址。
endpoint_port	流量的目标端口。
protocol	流量的 IANA 协议编号。有关更多信息，请参阅分配的 Internet 协议编号。
ip_address_type	IPv4.
packets	捕获窗口中传输的数据包的数量。
bytes	捕获窗口中传输的字节数。
start_time	捕获窗口启动的时间，采用 Unix 秒的格式。
end_time	捕获窗口结束的时间，采用 Unix 秒的格式。
action	与流量关联的操作： • ACCEPT：安全组或网络 ACL 允许记录的流量。该值当前始终为 “接受”。
log-status	流日志的日志记录状态： • OK：数据正常记录到选定目标。 • NODATA：捕获窗口中没有传入或传出网络接口的网络流量。 • SKIPDATA：捕获窗口中跳过了一些流日志记录。这可能是由于内部容量限制或内部错误。

字段	描述
globalaccelerator_source_ip	全局加速器网络接口使用的 IP 地址。
globalaccelerator_source_port	全局加速器网络接口使用的端口。
endpoint_region	终端节点所在的 AWS 区域。
globalaccelerator_region	服务请求的边缘站点（存在点）。每个边缘站点具有三个字母的代码和任意分配的数字，例如，DFW3。三个字母代码通常对应邻近边缘站点的机场的国际航空协会机场代码。(这些缩写将来可能会更改。)
direction	流量的方向。表示进入全局加速器网络 (INGRESS）或返回到客户端 (EGRESS)。
vpc_id	VPC 标识符。当全局加速器将流量发送到具有客户端 IP 地址保留的终端节点时，包含在 2.0 版流日志中。

如果某个字段不适用于特定记录，则记录会显示该条目的 “-” 符号。

Amazon CloudWatch 与 AWS Global Accelerator 结合使用

AWS Global Accelerator 向 Amazon CloudWatch 发布用于加速器的数据点。利用 CloudWatch，您可以按一组有序的时间序列数据（称为指标。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通过加速器的流量。每个数据点都有相关联的时间戳和可选测量单位。

您可使用指标来验证系统是否正常运行。例如，您可以创建 CloudWatch 警报来监控指定的指标，并在指标超出您的可接受范围时启动某个操作 (如向电子邮件地址发送通知)。

只有当请求流经加速器时，Global Accelerator 才会向 CloudWatch 报告指标。如果请求流经加速器，则 Global Accelerator 会以 60 秒的间隔测量并发送其指标。如果没有请求流经加速器或指标无数据，则不报告指标。

有关更多信息，请参阅 Amazon CloudWatch 用户指南。

目录

Global Accelerator 指标

AWS/GlobalAccelerator 命名空间包括以下指标。

指标	描述
NewFlowCount	时段内建立的客户端至终端的新 TCP 和 UDP 流（或连接）的总数。 报告标准：有非零值。 统计数据：唯一有用的统计数据是Sum。 Dimensions • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress
ProcessedBytesIn	加速器处理的传入字节总数，包括 TCP/IP 标头。此计数包括到端点的所有流量。 报告标准：有非零值。 统计数据：唯一有用的统计数据是Sum。

指标	描述
	Dimensions • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress
ProcessedBytesOut	加速器处理的传出字节总数，包括 TCP/IP 标头。此计数包括来自终端的流量，减去运行状况检查流量。 报告标准：有非零值。 统计数据：唯一有用的统计数据是Sum。 Dimensions • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress

加速器的指标维度

要筛选您的加速器的指标，请使用以下维度。

维度	描述
Accelerator	按加速器筛选指标数据。通过加速器 ID（加速器 ARN 的最后部分）指定加速器。例如，如果 ARN 为arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh ，则可以指定以下内容：**1234abcd-abcd-1234-abcd-1234abcdefgh** 。
Listener	按监听程序筛选指标数据。通过监听程序 ID（监听程序 ARN 的最后一部分）指定监听程序。例如，如果 ARN 为arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123wxyz ，则可以指定以下内容：**0123wxyz**。
EndpointGroup	按终端组筛选指标数据。按 AWS 区域指定终端节点组，例如**us-east-1**（全部为小写）。
SourceRegion	按源区域筛选指标数据，该区域是运行应用程序终端节点的 AWS 区域的地理区域。源区域为以下区域之一： • 北美 — 美国和加拿大 • EU — 欧洲 • 美联社 — 亚太 * • KR — 韩国 • IN — 印度 • AU — 澳大利亚 • ME — 中东 • SA — 南美洲 * 不包括韩国和印度
DestinationEdge	按目标边缘（即为客户端流量提供服务的 AWS 节点位置的地理区域）筛选指标数据。目标边为下列选项之一： • 北美 — 美国和加拿大 • EU — 欧洲

维度	描述
	• 美联社 — 亚太 * • KR — 韩国 • IN — 印度 • AU — 澳大利亚 • ME — 中东 • SA — 南美洲 • ZA — 南非 * 不包括韩国和印度
`TransportProtocol`	按传输协议筛选指标数据：联合发展方案或技术合作方案。
`AcceleratorIPAddress`	按加速器的 IP 地址筛选指标数据：即分配给加速器的静态 IP 地址之一。

Global Accelerator 指标统计数据

CloudWatch 提供基于 Global Accelerator 发布的指标数据点的统计数据。统计数据是指定时间段内的指标数据的聚合。当请求统计数据时，返回的数据流按指标名称和维度进行识别。维度是用于唯一标识指标的名称/值对。例如，您可以请求从欧洲的 AWS 节点位置（目标边缘为 “EU”）提供字节的加速器的处理字节。

以下是您可能会发现有用的度量/维度组合示例：

- 查看两个加速器 IP 地址中每个地址提供的流量（例如处理 BytesOout），以验证您的 DNS 配置是否正确。
- 查看用户流量的地理分布，并监控其中有多少是本地流量（例如，北美到北美）或全球流量（例如，澳大利亚或印度到北美）。要确定这一点，请查看已处理的度量字节在维 “目标边缘” 和 “SourceRegion” 设置为特定值的情况下或已处理的字节。

查看您的加速器的 CloudWatch 指标

您可以使用 CloudWatch 控制台或 AWS CLI 查看您的加速器的 CloudWatch 指标。在控制台中，指标显示为监控图表。只有当加速器处于活动状态并且正在接收请求时，监控图表才会显示数据点。

您必须在控制台或使用 AWS CLI 时查看美国西部（俄勒冈）区域的 CloudWatch 指标。使用 AWS CLI 时，请通过包含以下参数为您的命令指定美国西部（俄勒冈）区域：`--region us-west-2`。

使用 CloudWatch 控制台查看指标

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

使用 AWS CLI 查看指标

使用以下 list-metrics 命令列出可用指标：

```
aws cloudwatch list-metrics --namespace AWS/GlobalAccelerator --region us-west-2
```

使用 AWS CLI 获取指标的统计数据

请使用以下内容get 指标统计数据命令获取指定指标和维度的统计数据。请注意 CloudWatch 将不同维度的每种唯一组合视为一个单独的指标。您无法使用未专门发布的维度组合检索统计数据。您必须指定创建指标时使用的同一维度。

以下示例列出了从北美 (NA) 目标边缘提供服务的加速器的处理字节总数，以每分钟为单位。

```
aws cloudwatch get-metric-statistics --namespace AWS/GlobalAccelerator \
--metric-name ProcessedBytesIn \
--region us-west-2 \
--statistics Sum --period 60 \
--dimensions Name=Accelerator,Value=1234abcd-abcd-1234-abcd-1234abcdefgh
 Name=DestinationEdge,Value=NA \
--start-time 2019-12-18T20:00:00Z --end-time 2019-12-18T21:00:00Z
```

下面是此命令中的示例输出：

```
{
    "Label": "ProcessedBytesIn",
    "Datapoints": [
        {
            "Timestamp": "2019-12-18T20:45:00Z",
            "Sum": 2410870.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:47:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:46:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:42:00Z",
            "Sum": 1560.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:48:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:43:00Z",
            "Sum": 1343.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:49:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:44:00Z",
            "Sum": 35791560.0,
            "Unit": "Bytes"
        }
```

```
    ]
}
```

使用 AWS CloudTrail 记录 AWS Global Accelerator API 调用

AWS Global Accelerator 与 AWS CloudTrail 集成，后者是一项提供用户、角色或 AWS 服务在 Global Accelerator 中所采取操作的记录的服务。CloudTrail 将对 Global Accelerator 的所有 API 调用作为事件捕获，包括来自 Global Accelerator 控制台的调用和对 Global Accelerator API 的代码调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 Global Accelerator 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台的 Event history (事件历史记录) 中查看最新事件。

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

CloudTrail 中的 Global Accelerator 信息

在您创建 CloudTrail 账户时，即针对该账户启用了 AWS。当 Global Accelerator 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一起保存在事件历史记录。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

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

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 接收多个区域中的 CloudTrail 日志文件和从多个账户中接收 CloudTrail 日志文件

所有 Global Accelerator 操作都由 CloudTrail 记录，并记录在AWS Global Accelerator API 参考。例如，对`CreateAccelerator`、`ListAccelerators`和`UpdateAccelerator`操作将在 CloudTrail 日志文件中生成条目。

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

- 请求是使用根用户凭证还是 IAM 用户凭证发出的

- 请求是使用角色还是联合身份用户的临时安全凭证发出的
- 请求是否由其他 AWS 服务发出

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解全局加速器日志文件条目条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。每个 JSON 格式的 CloudTrail 日志文件可以包含一个或多个日志条目。一个日志条目表示来自任何源的一个请求，并包括有关所请求的操作的信息，如任何参数以及操作的日期和时间等。不能保证日志条目具有任何特定顺序，它们不是 API 调用的有序堆栈跟踪。

下面的示例显示了一个 CloudTrail 日志条目，该条目包括这些 Global Accelerator 操作：

- 列出账户的加速器：eventName是ListAccelerators。
- 创建侦听器：eventName是CreateListener。
- 更新侦听器：eventName是UpdateListener。
- 描述侦听器：eventName是DescribeListener。
- 列出帐户的侦听器：eventName是ListListeners。
- 删除侦听器：eventName是DeleteListener。

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
```

```
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:03:14Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "ListAccelerators",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "083cae81-28ab-4a66-862f-096e1example",
      "eventID": "fe8b1c13-8757-4c73-b842-fe2a3example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:04:49Z",
      "eventSource": "globalaccelerator.amazonaws.com",
```

```
      "eventName": "CreateListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample",
        "portRanges": [
          {
            "fromPort": 80,
            "toPort": 80
          }
        ],
        "protocol": "TCP"
      },
      "responseElements": {
        "listener": {
          "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
          "portRanges": [
            {
              "fromPort": 80,
              "toPort": 80
            }
          ],
          "protocol": "TCP",
          "clientAffinity": "NONE"
        }
      },
      "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
      "eventID": "9cab44ef-0777-41e6-838f-f249example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:03:52Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "CreateAccelerator",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "name": "cloudTrailTest"
      },
      "responseElements": {
        "accelerator": {
          "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample",
          "name": "cloudTrailTest",
          "ipAddressType": "IPV4",
          "enabled": true,
          "ipSets": [
            {
              "ipFamily": "IPv4",
              "ipAddresses": [
                "192.0.2.213",
                "192.0.2.200"
              ]
            }
          ],
          "status": "IN_PROGRESS",
          "createdTime": "Nov 17, 2018 9:03:52 PM",
          "lastModifiedTime": "Nov 17, 2018 9:03:52 PM"
        }
```

```
      },
      "requestID": "d2d7f300-2f0b-4bda-aa2d-e67d6e4example",
      "eventID": "11f9a762-8c00-4fcc-80f9-848a29example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:05:27Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "UpdateListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
        "portRanges": [
          {
            "fromPort": 80,
            "toPort": 80
          },
          {
```

```
            "fromPort": 81,
            "toPort": 81
          }
        ]
      },
      "responseElements": {
        "listener": {
          "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
          "portRanges": [
            {
              "fromPort": 80,
              "toPort": 80
            },
            {
              "fromPort": 81,
              "toPort": 81
            }
          ],
          "protocol": "TCP",
          "clientAffinity": "NONE"
        }
      },
      "requestID": "008ef93c-b3a3-44b4-afb3-768example",
      "eventID": "85958f0d-63ff-4a2c-99e3-6ffbexample",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
```

```
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:06:05Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "DescribeListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234"
      },
      "responseElements": null,
      "requestID": "9980e368-82fa-40da-95a3-4b0example",
      "eventID": "885a02e9-2a60-4626-b1ba-57285example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
```

```
        }
      },
      "eventTime": "2018-11-17T21:05:47Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "ListListeners",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample"
      },
      "responseElements": null,
      "requestID": "08e4b0f7-689b-4c84-af2d-47619example",
      "eventID": "f4fb8e41-ed21-404d-af9d-037c4example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:06:24Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "DeleteListener",
```

```
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234"
      },
      "responseElements": null,
      "requestID": "04d37bf9-3e50-41d9-9932-6112example",
      "eventID": "afedb874-2e21-4ada-b1b0-2ddb2example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

AWS Global Accelerator 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，第三方审计师会定期测试和验证安全的有效性。要了解适用于全局加速器的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云中的安全性 – 您的责任是由使用的 AWS 服务决定的。您还需要对其他因素负责，包括您的数据的敏感性、您组织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全球加速器时应用责任共担模型。以下主题说明如何配置全局加速服务以实现您的安全目标。

主题

AWS Global Accelerator 的身份和访问管理

AWS Identity and Access Management (IAM) 是一个 AWS 服务，可以帮助管理员安全地控制对 AWS 资源（包括 AWS Global Accelerator 资源）的访问。管理员使用 IAM 控制谁身份验证(已登录)和AUTH（具有权限）来使用全局加速器资源。IAM 是您的 AWS 账户中包含的一项功能，不会另外收费。

> **Important**
>
> 如果您不熟悉 IAM，请查看此页面上的介绍性信息，然后参阅入门。（可选）您可以选择查看有关身份验证和访问控制的更多信息。什么是身份验证？、什么是访问控制？, 和什么是策略？。

主题

概念和术语

身份验证— 要登录 AWS，您必须使用下列选项之一：根用户凭证（不推荐）、IAM 用户凭证或采用 IAM 角色的临时凭证。要了解有关这些实体的更多信息，请参阅什么是身份验证？。

访问控制— AWS 管理员使用策略来控制对 AWS 资源（例如全球加速器中的加速器）的访问。要了解更多信息，请参阅什么是访问控制？和什么是策略？。

> **Important**
>
> 无论谁创建了某个账户中的资源，所有这些资源都归该账户所有。您必须被授予创建资源的访问权限。但是，仅仅创建资源并不意味着您自动获得对该资源的完全访问权限。管理员必须为您要执行的每个操作明确授予权限。该管理员也可以随时撤销您的权限。

为帮助您了解 IAM 的基础知识，请查看以下术语：

资源

AWS 服务（如全局加速器和 IAM）通常包括称为资源的对象。在大多数情况下，您可以从该服务创建、管理和删除这些资源。IAM 资源包括用户、组、角色和策略：

用户

IAM 用户表示使用其凭证与 AWS 交互的人员或应用程序。用户由用于登录 AWS 管理控制台的名称和密码组成，最多可包含用于 AWS CLI 或 AWS API 的两个访问密钥。

组

IAM 组是 IAM 用户的集合。管理员可以使用组来为成员用户指定权限。这使管理员可以更轻松地管理多个用户的权限。

角色

IAM 角色没有关联的任何长期凭证（密码或访问密钥）。任何需要角色并具有权限的人都可以代入角色。IAM 用户可担任角色来暂时获得针对特定任务的不同权限。联合身份用户可以通过使用映射到该角色的外部身份提供商来代入角色。某些 AWS 服务可以假设服务角色代您访问 AWS 资源。

策略

策略是 JSON 文档，定义所附加到的对象的权限。AWS Support基于身份的策略您将其附加到身份（用户、组或角色）。某些 AWS 服务允许您将基于资源的策略来控制委托人（人员或应用程序）可以对该资源执行的操作。Global Accelerator 不支持基于资源的策略。

身份

身份是您可以为其定义权限的 IAM 资源。其中包括用户、组和角色。

实体

实体是您用于进行身份验证的 IAM 资源。其中包括用户和角色。

委托人

在 AWS 中，委托人是使用实体登录并向 AWS 发出请求的人或应用程序。作为委托人，您可以使用 AWS 管理控制台、AWS CLI 或 AWS API 来执行操作（如删除加速器）。这将为该操作创建一个请求。您的请求指定操作、资源、委托人、委托人账户以及有关您的请求的任何其他信息。所有这些信息为 AWS 提供了context以获取您的请求。AWS 检查应用于请求上下文的所有策略。只有在策略允许请求的每个部分时，AWS 才会授权该请求。

要查看身份验证和访问控制过程的图表，请参阅了解 IAM 的工作方式中的IAM 用户指南。有关 AWS 如何确定是否允许请求的详细信息，请参阅。策略评估逻辑中的IAM 用户指南。

控制台访问、身份验证管理和访问控制所需的权限

要使用全局加速器或者管理自己或他人的授权和访问控制，您必须具有正确的权限。

创建全局加速器加速器所需的权限

要创建 AWS Global Accelerator 加速器，用户必须具有创建与全球加速器关联的服务链接角色的权限。

要确保用户具有在全局加速器中创建加速器的正确权限，请将策略附加到用户，如下所示。

> **Note**
>
> 如果创建更为严格的基于身份的权限策略，具有该策略的用户将无法创建加速器。

```
{
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "globalaccelerator.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*"
    }
```

使用全局加速器控制台所需的权限

要访问 AWS Global Accelerator 控制台，您必须具有一组最小权限，以允许您列出和查看有关 AWS 账户中全球加速器资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的权限策略，对于附加了该策略的实体，控制台将无法按预期正常运行。

要确保这些实体仍可使用全球加速器控制台或 API 操作，也可向用户附加下列 AWS 托管策略之一，如[在“JSON”选项卡上创建策略](#)：

```
        GlobalAcceleratorReadOnlyAccess
        GlobalAcceleratorFullAccess
```

附加第一个策略GlobalAcceleratorReadOnlyAccess，如果用户只需在控制台中查看信息或调用 AWS CLI 或使用List*或者Describe*操作。

附上第二个策略GlobalAcceleratorFullAccess提供给需要创建加速器或更新加速器的用户。完全访问策略包括FULL全局加速器的权限以及描述权限 Amazon EC2 性负载均衡。

> **Note**
>
> 如果您创建的基于身份的权限策略不包括 Amazon EC2 和 Elastic Load Balancing 所需的权限，则具有该策略的用户将无法向加速器添加 Amazon EC2 和 Elastic Load Balancing 资源。

以下是完全访问策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSubnets",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": "ec2:DeleteSecurityGroup",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSServiceName": "GlobalAccelerator"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
    ]
}
```

身份验证管理所需的权限

要管理自己的凭证（例如密码、访问密钥和多重验证 (MFA) 设备），管理员必须授予您所需的权限。要查看包含这些权限的策略，请参阅允许用户自行管理其凭据。

作为 AWS 管理员，您需要的完全访问 IAM，以便您可以在 IAM 中创建和管理用户、组、角色和策略。您应使用AdministratorAccessAWS 托管策略，其中包含所有 AWS 的完全访问权限。此策略不提供对 AWS Billing and Cost Management 控制台的访问权限，也不允许需要 AWS 账户根用户凭证的任务。有关更多信息，请参阅 。需要 AWS 账户根用户凭证的 AWS 任务中的AWS 一般参考。

> **Warning**
>
> 只有管理员用户才应具有 AWS 的完全访问权限。除了修改 AWS 中的每个资源之外，拥有此策略的任何人都有权完全管理身份验证和访问控制。要了解如何创建此用户，请参阅创建您的 IAM 管理员用户。

访问控制所需的权限

如果管理员为您提供了 IAM 用户凭证，则他们会将策略附加到您的 IAM 用户，以控制您可以访问的资源。要在 AWS 管理控制台中查看附加到您的用户身份的策略，您必须具有以下权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": [
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
            "Sid": "ListUsersViewGroupsAndPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

如果您需要其他权限，请要求管理员更新策略以允许您访问所需的操作。

了解全球加速器如何与 IAM 配合使用

服务可以用几种方式与 IAM 协同工作：

操作

Global Accelerator 支持在策略中使用操作。这允许管理员控制实体是否可以在全局加速器中完成操作。例如，要允许实体调用`GetPolicy`AWS API 操作来查看策略，管理员必须附加一个允许`iam:GetPolicy`action.

以下示例策略允许用户执行`CreateAccelerator`操作以编程方式为您的 AWS 账户创建加速器：

```
{
   "Version": "2018-08-08",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "globalaccelerator:CreateAccelerator"
         ],
         "Resource":"*"
      }
   ]
}
```

资源级权限

Global Accelerator 支持资源级权限。资源级权限允许您使用 ARN 在策略中指定各个资源。

基于资源的策略

Global Accelerator 不支持基于资源的策略。使用基于资源的策略，您可以将策略附加到该服务中的资源。基于资源的策略包括`Principal`元素来指定哪些 IAM 身份可以访问此资源。

根据标签进行授权

全局加速器支持基于授权的标签。此功能允许您在策略条件中使用资源标签。

临时凭证

全局加速器支持临时凭证。借助，可以使用联合身份登录、代入 IAM 角色或代入跨账户角色。您可以通过调用 AWS STS API 操作（如AssumeRole或者GetFederationToken。

服务相关角色

Global Accelerator 支持服务相关角色。此功能允许服务代表您代入服务相关角色。此角色允许服务访问其他服务中的资源以代表您完成操作。服务相关角色显示在您的 IAM 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

服务角色

全局加速器不支持服务角色。此功能允许服务代表您代入服务角色。此角色允许服务访问其他服务中的资源以代表您完成操作。服务角色显示在您的 IAM 账户中，并归该账户所有。这意味着，IAM 管理员可以更改该角色的权限。但是，这可能会中断服务的功能。

身份验证和访问控制的故障

使用以下信息可帮助您诊断和修复在使用 IAM 时可能遇到的常见问题。

主题

- 我无权在 Global Accelerator 中执行操作
- 我是管理员并希望允许其他人访问全局加速器
- 我想了解 IAM 而不想成为专家

我无权在 Global Accelerator 中执行操作

如果 AWS 管理控制台指示您无权执行操作，则必须与向您提供了用户名和密码的管理员联系。

以下示例出现在名为my-user-name尝试使用控制台执行globalaccelerator:CreateAccelerator操作，但没有权限：

```
User: arn:aws:iam::123456789012:user/my-user-name is not authorized to perform: aws-globalaccelerator:CreateAccelerator on resource: my-example-accelerator
```

在此情况下，请要求您的管理员更新您的策略以允许您访问my-example-accelerator资源使用aws-globalaccelerator:CreateAcceleratoraction.

我是管理员并希望允许其他人访问全局加速器

要允许其他人访问全球加速器，您必须为需要访问权限的人员或应用程序创建一个 IAM 实体（用户或角色）。他们将使用该实体的凭证访问 AWS。然后，您必须将策略附加到实体，以便在全局加速器中为他们（它们）授予正确的权限。

要立即开始，请参阅入门。

我想了解 IAM 而不想成为专家

要了解有关 IAM 术语、概念和过程的更多信息，请参阅以下主题：

- 什么是身份验证？
- 什么是访问控制？
- 什么是策略？

基于标签的策略

在设计 IAM 策略时，您可以通过授予对特定资源的访问权限来设置精细权限。但随着您管理的资源数量的增加，此任务会变得日益复杂。标记加速器并在策略声明条件中使用标签可以简化这一任务。您可以向具有特定标签的任何加速器批量授予访问权限。然后，在创建加速器时或稍后更新加速器时，您可以将此标签反复应用到相关加速器。

> **Note**
>
> 使用条件中的标签是控制对资源和请求的访问的一种方法。有关在全局加速器中进行标记的信息，请参阅。AWS Global Accelerator 中的标签。

标签可以附加到资源，也可以从请求传入支持标签的服务。在全局加速器中，只有加速器可以包含标签。在创建 IAM 策略时，您可以使用标签条件键来控制：

- 哪些用户可以基于加速器已有的标签对加速器执行操作。
- 哪些标签可以在操作的请求中传递。
- 是否特定标签键可在请求中使用。

有关标签条件键的完整语法和语义，请参阅。使用 IAM 标签控制访问中的IAM 用户指南。

例如，全局加速器GlobalAcceleratorFullAccess托管用户策略为用户提供对任意资源执行任意全局加速器操作的不受限权限。以下策略限制此权力并拒绝未经授权的用户具有对任何生产加速器。除托管用户策略外，客户的管理员还必须将此 IAM 策略附加到未经授权的 IAM 用户。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Deny",
         "Action":"*",
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:RequestTag/stage":"prod"
            }
         }
      },
      {
         "Effect":"Deny",
         "Action":"*",
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:ResourceTag/stage":"prod"
            }
         }
      }
   ]
}
```

Global Accelerator 的服务相关角色

AWS Global Accelerator 使用 AWS Identity and Access Management (IAM)服务相关角色。服务相关角色是一种与服务直接关联的独特类型的 IAM 角色。服务相关角色由服务预定义，具有服务代表您调用其他 AWS 服务所需的所有权限。

全局加速器使用以下 IAM 服务相关角色：

- 用于全球加速器的 AWS 服务-全局加速器使用此角色允许全局加速器创建和管理客户端 IP 地址保留所需的资源。

当首次需要该角色来支持全局加速器 API 操作时，全局加速器会自动创建名为 AWSServicerolee 的角色。全球加速器的 AWS 服务器角色允许全局加速器创建和管理客户端 IP 地址保留所需的资源。在全局加速器中使用加速器时需要此角色。AWSServiceRoleFor全球加速器角色的 ARN 如下所示：

```
arn:aws:iam::123456789012:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator
```

通过使用服务相关角色，您可以更轻松地设置和使用全局加速器，因为您不必手动添加所需的权限。全局加速器定义其服务相关角色的权限，并且仅全局加速器可以担任这些角色。定义的权限包括信任策略和权限策略。不能将该权限策略附加到任何其他 IAM 实体。

必须先删除任何关联的全局加速器资源，然后才能删除服务相关角色。这确保您不会删除在访问活动资源时仍需要的服务相关角色，从而有助于保护您的全局加速器资源。

有关支持服务相关角色的其他服务的信息，请参阅。使用 IAM 的 AWS 服务并寻找具有是中的服务相关角色column.

Global Accelerator 的服务相关角色权限

Global Accelerator 使用名为的服务相关角色。用于全球加速器的 AWS 服务。以下部分介绍角色的权限。

服务相关角色权限

此服务链接角色允许全球加速器管理 EC2 弹性网络接口和安全组，并帮助诊断错误。

AWSServiceRoleForGlobal 加速器服务相关角色信任以下服务代入该角色：

- `globalaccelerator.amazonaws.com`

角色权限策略策略允许 Global Access 对指定资源完成以下操作，如策略中所示：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSecurityGroup",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSServiceName": "GlobalAccelerator"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
    ]
}
```

您必须配置权限以允许 IAM 实体（例如，用户、组或角色）删除全局加速器服务相关角色。有关更多信息，请参阅 。服务相关角色权限中的IAM 用户指南。

为 Global Accelerator 创建服务相关角色

您不需要为全局加速器手动创建服务相关角色。当您首次创建加速器时，该服务自动为您创建角色。如果您删除全局加速器资源并删除服务相关角色，则在您创建新加速器时，服务将再次自动创建该角色。

编辑全局加速器服务相关角色

全局加速器不允许您编辑 AWSServiceRoleForGlobal 加速器服务相关角色。在该服务创建服务相关角色后，您无法更改该角色的名称，因为不同的实体可能会引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅 。编辑服务相关角色中的IAM 用户指南。

删除全局加速器服务相关角色

如果您不再需要使用全局加速器，我们建议您删除服务相关角色。这样，就不会主动监控或维护您的未使用实体。但是，您必须先清除您账户中的全局加速器资源，然后才能手动删除角色。

在禁用并删除加速器后，您可以删除服务相关角色。有关删除加速器的更多信息，请参阅。 创建或更新标准加速器。

> **Note**
>
> 如果您已经禁用和删除了加速器，但全局加速器未完成更新，删除服务相关角色可能会失败。如果发生这种情况，请等待几分钟，然后重试服务相关角色删除步骤。

手动删除全球加速器服务相关角色

1. 登录 AWS 管理控制台，并通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在 IAM 控制台的导航窗格中，选择角色。然后，选中要删除的角色名称旁边的复选框，而不是名称或行本身。
3. 对于页面顶部的角色操作，请选择删除角色。
4. 在确认对话框中，查看上次访问服务数据，该数据显示每个选定角色上次访问 AWS 服务的时间。这样可帮助您确认角色当前是否处于活动状态。如果要继续，请选择 Yes, Delete 以提交服务相关角色进行删除。
5. 监视 IAM 控制台通知，以监控服务相关角色的删除进度。由于 IAM 服务相关角色删除是异步的，因此，在您提交角色进行删除后，删除任务可能成功，也可能失败。有关更多信息，请参阅 。删除服务相关角色中的IAM 用户指南。

全球加速器服务关联角色的更新（AWS 托管策略）

查看有关自此服务开始跟踪这些更改以来对的服务链接角色的更新的详细信息。有关此页面更改的自动警报，请订阅 AWS Global Accelerator 上的 RSS 源文档历史记录页.

变更	描述	日期
用于全球加速器的 AWS 服务— 更新的策略	全局加速器添加了一个新的权限，以帮助全局加速器诊断错误。 Global Accelerator 使用`ec2:DescribeRegions` 来确定客户所在的 AWS 区域，这有助于全球加速器排除错误。	2021 年 5 月 18 日
全球加速器开始跟踪更改	全球加速器开始跟踪其 AWS 托管策略的更改。	2021 年 5 月 18 日

Global Accelerator 服务相关角色支持的区域

全球加速服务支持在支持全球加速服务的 AWS 区域中使用服务相关角色。

有关当前支持全球加速服务和其他服务的 AWS 区域列表，请参阅AWS 区域表。

访问和身份验证概述

如果您是首次接触 IAM，请阅读以下主题了解 AWS 中的授权和访问。

主题

- 什么是身份验证？
- 什么是访问控制？
- 什么是策略？
- 入门

什么是身份验证？

身份验证是指如何使用您的凭证登录到 AWS。

> **Note**
>
> 要快速开始，您可以忽略此部分。首先，审核有关的介绍性信息AWS Global Accelerator 的身份和访问管理，然后参阅入门。

作为委托人，您必须身份验证（登录到 AWS）使用实体（根用户、IAM 用户或 IAM 角色）向 AWS 发送请求。IAM 用户可能具有长期凭证，例如用户名和密码或一组访问密钥。当您代入 IAM 角色时，您将收到临时安全凭证。

要作为用户从 AWS 管理控制台中获得身份验证，您必须使用用户名和密码登录。要从 AWS CLI 或 AWS API 中获取身份验证，您必须提供访问密钥和私有密钥或临时凭证。AWS 提供了开发工具包和 CLI 工具，以使用您的凭证对您的请求进行加密签名。如果您不使用 AWS 工具，则必须自行对请求进行签名。无论使用何种身份验证方法，您可能还需要提供其他安全信息。例如，AWS 建议您使用多重验证 (MFA) 以提高您的账户的安全性。

作为委托人，您可以使用以下实体（用户或角色）登录 AWS：

AWS 账户根用户

在首次创建 AWS 账户时，您最初使用一个具有账户中的所有 AWS 服务和资源的完全访问权限的单点登录身份。此身份称为 AWS 账户根用户，可以通过使用您用于创建账户的电子邮件地址和密码进行登录来访问该身份。强烈建议您不使用根用户执行日常任务，即使是管理任务。相反，请遵循仅使用根用户创建您的第一个 IAM 用户的最佳实践。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。

IAM 用户

一个IAM 用户是您的 AWS 账户中具有特定权限的实体。Global Accelerator 支持签名版本 4，这是用于对入站 API 请求进行身份验证的协议。有关验证请求的更多信息，请参阅。签名版本 4 签名过程中的AWS 一般参考。

IAM 角色

一个IAM 角色是您可以在账户中创建的一种具有特定权限的 IAM 身份。IAM 角色类似于 IAM 用户，因为它是一个 AWS 身份，具有确定其在 AWS 中可执行和不可执行的操作的权限策略。但是，角色旨在让需要它的任何人代入，而不是唯一地与某个人员关联。此外，角色没有关联的标

准长期凭证（如密码或访问密钥）。相反，当您代入角色时，它会为您提供角色会话的临时安全凭证。具有临时凭证的 IAM 角色在以下情况下很有用：

联合身份用户访问

您可以使用来自 AWS Directory Service、您的企业用户目录或 Web 身份提供商的现有身份，而不创建 IAM 用户。他们被称为联合身份用户。在通过身份提供商请求访问权限时，AWS 将为联合身份用户分配角色。有关联合身份用户的详细信息，请参阅联合身份用户和角色中的IAM 用户指南。

临时用户权限

IAM 用户可暂时担任角色来获得针对特定任务的不同权限。

跨账户访问

您可以使用 IAM 角色允许不同账户中的可信任委托人访问您账户中的资源。角色是授予跨账户访问权限的主要方式。不过，对于某些 AWS 服务，您可以将策略直接附加到资源（而不是将角色作为代理）。全局加速器不支持这些基于资源的策略。有关选择是使用角色还是基于资源的策略以允许跨账户访问的更多信息，请参阅控制对不同账户中的委托人的访问。

AWS 服务访问

服务角色是IAM 角色服务为了代表您执行操作而担任的。服务角色只在您的账户内提供访问权限，不能用于为访问其他账户中的服务授权。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 。创建向 AWS 服务委托权限的角色中的IAM 用户指南。

在 Amazon 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凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个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 。使用 IAM 角色向在 Amazon EC2 实例上运行的应用程序授予权限中的IAM 用户指南。

什么是访问控制？

在您登录（经过身份验证）AWS 后，您对 AWS 资源和操作的访问由策略控制。访问控制也称为授权。

> **Note**
>
> 要快速开始，您可以忽略此页面。首先，审核有关的介绍性信息AWS Global Accelerator 的身份和访问管理，然后参阅入门。

在授权期间，AWS 使用请求上下文来检查应用的策略。然后，它使用策略来确定是允许还是拒绝请求。大多数策略作为 JSON 文档存储在 AWS 中，并指定为委托人允许或拒绝的权限。有关 JSON 策略文档的结构和内容的更多信息，请参阅什么是策略？。

通过使用策略，管理员可以指定哪些用户有权访问 AWS 资源，以及他们可以对这些资源执行哪些操作。每个 IAM 实体（用户或角色）最初没有任何权限。换而言之，在默认状态下，用户什么都不能做，甚至不能查看自己的访问密钥。要为用户授予执行某些操作的权限，管理员必须将权限策略附加到用户。或者，管理员可以将用户添加到具有所需权限的组中。之后当管理员授予某个组访问权限时，该组内的全部用户都会获得这些访问权限。

您可能使用有效的凭证来对自己的请求进行身份验证，但管理员还必须向您授予权限，您才能创建或访问 AWS Global Accelerator ess 资源。例如，您必须明确拥有权限才能创建 AWS Global Accelerator。

作为管理员，您可以编写策略来控制对以下各项的访问：

- 委托人— 控制发出请求的人员或应用程序（委托人）被允许这样做。
- IAM 身份— 控制可访问哪些 IAM 身份（组、用户和角色）以及如何进行访问。
- IAM 策略— 控制哪些用户可以创建、编辑和删除客户托管策略，以及哪些用户可以附加和分离所有托管策略。
- AWS 资源— 使用基于身份的策略或基于资源的策略控制哪些用户有权访问资源。
- AWS 账户— 控制是否仅允许特定账户的成员发出请求。

控制 委托人进行的访问

权限策略控制您作为委托人可以执行的操作。管理员必须将基于身份的权限策略附加到提供权限的身份（用户、组或角色）。权限策略允许或拒绝访问 AWS。管理员还可以设置 IAM 实体（用户或角色）的权限边界以定义该实体可以具有的最大权限。权限边界是一项高级 IAM 功能。有关权限边界的更多信息，请参阅。IAM 身份的权限边界中的IAM 用户指南。

有关如何控制委托人的 AWS 访问的更多信息和示例，请参阅控制委托人的访问中的IAM 用户指南。

控制对身份的访问

管理员通过创建限制可以对身份执行的操作或谁可以访问身份的策略，来控制您对 IAM 身份（用户、组或角色）可以执行的操作。然后，他们将该策略附加到提供您的权限的身份。

例如，管理员可能允许您重置三个特定用户的密码。为此，他们将一个策略附加到您的 IAM 用户，以允许您仅为自己和具有三个指定用户的 ARN 的用户重置密码。这使您可以重置团队成员的密码，但不能重置其他 IAM 用户的密码。

有关使用策略控制 AWS 对身份的访问的更多信息和示例，请参阅控制对身份的访问中的IAM 用户指南。

控制对策略的访问

管理员可以控制哪些用户可以创建、编辑和删除客户托管策略，以及哪些用户可以附加和分离所有托管策略。当您查看一个策略时，您可以查看策略摘要，其中包括该策略中每个服务的访问权限级别的摘要。AWS 将每个服务操作分为四个操作之一访问级别基于每个操作的功能：`List`、`Read`、`Write`，或者`Permissions management`。您可以使用这些访问权限级别确定将哪些操作包含在您的策略中。有关更多信息，请参阅 。了解策略摘要中的访问级别摘要中的IAM 用户指南。

> **Warning**
>
> 您应限制`Permissions Management`访问级别权限。否则，您的账户成员为自己创建的策略所拥有的权限可能比他们应有的权限更多。或者，他们可以创建具有 AWS 完全访问权限的单独用户。

有关如何控制 AWS 访问策略的更多信息和示例，请参阅控制对策略的访问中的IAM 用户指南。

控制对 资源的访问

管理员可以使用基于身份的策略或基于资源的策略控制对资源的访问。在基于身份的策略中，您将策略附加到一个身份并指定该身份可以访问哪些资源。在基于资源的策略中，您将策略附加到要控制的资源。在该策略中，您指定哪些委托人可以访问该资源。

有关更多信息，请参阅 。控制对资源的访问中的IAM 用户指南。

资源创建者不会自动拥有权限

无论谁创建了某个账户中的资源，所有这些资源都归该账户所有。AWS 账户根用户是账户所有者，因此具有对账户中的任意资源执行任意操作的权限。

> **Important**
>
> 强烈建议您不使用根用户执行日常任务，即使是管理任务。而是应按照仅使用根用户创建您的第一个 IAM 用户的最佳实践。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。要查看需要您以根用户身份登录的任务，请参阅需要根用户的 AWS 任务。

必须授予 AWS 账户中的实体（用户或角色）创建资源的访问权限。但是，仅仅因为这些实体创建了资源，并不意味着他们自动拥有对该资源的完全访问权限。管理员必须为每个操作明确授予权限。此外，只要管理员有权管理用户和角色权限，就可以随时撤销这些权限。

控制对不同账户中的委托人的访问

管理员可以使用基于 AWS 资源的策略、IAM 跨账户角色或 AWS Organizations 服务，以允许其他账户中的委托人访问您账户中的资源。

对于一些 AWS 服务，管理员可授予对资源的跨账户访问权限。为此，管理员将策略直接附加到要共享的资源，而不是将角色用作代理。如果服务支持此策略类型，则管理员共享的资源还必须支持基于资源的策略。与基于用户的策略不同，基于资源的策略指定哪些人（以 AWS 账户 ID 号列表的形式）可以访问该资源。Global Accelerator 不支持基于资源的策略。

与角色相比，使用基于资源的策略进行跨账户访问具有一些优势。利用通过基于资源的策略访问的资源，委托人（人员或应用程序）仍在可信账户中工作，并且无需放弃用于代替角色权限的用户权限。换句话说，委托人可以同时访问可信账户和 信任账户中的资源。这对于从一个账户向另一个账户中复制信息之类的任务非常有用。有关使用跨账户角色的更多信息，请参阅。在您拥有的另一个 AWS 账户中向 IAM 用户提供访问权限中的IAM 用户指南。

AWS Organizations 可以针对您拥有的多个 AWS 账户实现基于策略的管理。借助，可以创建账户 Organizations、自动创建账户以及应用和管理这些组的策略。Organizations 支持您针对多个账户集中管理策略，无需使用自定义脚本和手动操作流程。使用 AWS Organizations，您可以创建服务控制策略 (SCP)，从而集中控制 AWS 账户对 AWS 服务的使用。有关更多信息，请参阅 。什么是 AWS Organizations？中的AWS Organizations 用户指南。

什么是策略？

您可以创建策略并将其附加到 IAM 身份或 AWS 资源，以便控制 AWS 中的访问。

> **Note**
>
> 要快速开始，您可以忽略此页面。首先，审核有关的介绍性信息AWS Global Accelerator 的身份和访问管理，然后参阅入门。

策略是 AWS 中的一个对象；在与实体或资源相关联时，策略定义了它们的权限。在委托人（如用户）发出请求时，AWS 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 AWS 中存储为 JSON 文档。

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，如果策略允许GetUser操作，则具有该策略的用户可以从 AWS 管理控制台、AWS CLI 或 AWS API 中获取用户信息。在创建 IAM 用户时，您可以设置用户以允许控制台或编程访问。IAM 用户可以使用用户名和密码登录到控制台。或者，他们也可以使用访问密钥来使用 CLI 或 API。

按频率顺序列出的以下策略类型可能会影响请求是否已获得授权。有关更多详细信息，请参阅策略类型中的IAM 用户指南。

基于身份的策略

您可以将托管策略和内联策略挂载到 IAM 身份（用户、用户所属组和角色）。

基于资源的策略

您可以将内联策略附加到一些 AWS 服务中的资源。基于资源的策略的最常见示例是 Amazon S3 存储桶策略和 IAM 角色信任策略。Global Accelerator 不支持基于资源的策略。

SCP Organizations

您可以使用 AWS Organizations 服务控制策略 (SCP) 将权限边界应用于 AWS Organizations 组织或组织单元 (OU)。这些权限会应用到成员账户中的所有实体。

访问控制列表 (ACL)

您可以使用 ACL 来控制哪些委托人可以访问资源。ACL 类似于基于资源的策略，但它们是唯一不使用 JSON 策略文档结构的策略类型。全局加速器支持 OR 不支持 ACL。

这些策略类型可分类为权限策略 或权限边界。

权限策略

您可以将权限策略挂载到 AWS 中的资源，以定义该对象的权限。在单个账户中，AWS 一起评估所有权限策略。权限策略是最常用的策略。您可以使用以下策略类型作为权限策略：

基于身份的策略

当您将托管策略或内联策略附加到 IAM 用户、组或角色时，策略定义该实体的权限。

基于资源的策略

将 JSON 策略文档附加到资源时，定义该资源的权限。服务必须支持基于资源的策略。

访问控制列表 (ACL)

将 ACL 附加到资源时，定义具有访问该资源的权限的委托人的列表。资源必须支持 ACL。

权限边界

您可以使用策略来定义实体（用户或角色）的权限边界。权限边界控制实体可以具有的最大权限。权限边界是一项高级 AWS 功能。当多个权限边界应用于请求时，AWS 会单独评估每个权限边界。您可以在以下情况下应用权限边界：

组织

您可以使用 AWS Organizations 服务控制策略 (SCP) 将权限边界应用于 AWS Organizations 组织或组织单元 (OU)。

IAM 用户或角色

您可以对用户或角色的权限边界使用托管策略。有关更多信息，请参阅 。IAM 实体的权限边界中的IAM 用户指南。

主题

基于身份的策略

您可以向 IAM 身份附加策略。例如，您可以执行以下操作：

将权限策略附加到账户中的用户或组

要向用户授予创建 AWS Global Accelerator ess 资源（例如加速器）的权限，您可以将权限策略附加到用户或用户所属的组。

将权限策略附加到角色（授予跨账户权限）

您可以将基于身份的权限策略挂载到 IAM 角色，以授予跨账户的权限。例如，账户 A 中的管理员可以创建一个角色，以向其他 AWS 账户（如账户 B）或某项 AWS 服务授予跨账户权限，如下所述：

1. 账户 A 管理员可以创建一个 IAM 角色，然后向该角色附加授予其访问账户 A 中资源的权限的权限策略。
2. 账户 A 管理员可以向角色挂载信任策略，将账户 B 标识为能够担任该角色的委托人。
3. 之后，账户 B 管理员可以委派权限，指派账户 B 中的任何用户担任该角色。这样，账户 B 中的用户就可以创建或访问账户 A 中的资源了。如果您需要授予 AWS 服务权限来担任该角色，则信任策略中的委托人也可以是 AWS 服务委托人。

有关使用 IAM 委派权限的更多信息，请参阅访问控制中的IAM 用户指南。

有关用户、组、角色和权限的更多信息，请参阅《IAM 用户指南》 中的身份 (用户、组和角色)。

以下是您可以与全球加速器一起使用的两个策略示例第一个示例策略授予用户对 AWS 账户中加速器的所有 “列表” 和 “描述” 操作的编程访问权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:List*",
                "globalaccelerator:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

以下示例授予对ListAccelerators操作:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:ListAccelerators",
            ],
            "Resource": "*"
        }
    ]
}
```

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。这些策略允许您指定，指定的委托人可在何种条件下对该资源执行哪些操作。最常见的基于资源的策略是面向 Amazon S3 存储桶的。基于资源的策略是仅存在于资源上的内联策略。没有基于托管资源的策略。

使用基于资源的策略向其他 AWS 账户的成员授予权限比 IAM 角色具有一些优势。有关更多信息，请参阅 。IAM 角色与基于资源的策略有何不同中的IAM 用户指南。

策略访问级别分类

在 IAM 控制台中，使用以下访问级别分类对操作进行分组：

List

提供权限列出服务内的资源以确定某个对象是否存在。此访问权限级别的操作可以列出对象，但是看不到资源的内容。具有 List (列表) 访问级别的大多数操作都无法在特定资源上执行。使用这些操作创建策略语句时，必须指定 All resources (所有资源) ("*")。

Read

提供权限读取服务中资源的内容和属性但不对其进行编辑。例如，Amazon S3 操作`GetObject`和`GetBucketLocation`具有Read访问级别。

写入

提供在服务中创建、删除或修改资源的权限。例如，Amazon S3 操作`CreateBucket`、`DeleteBucket`, 和`PutObject`具有写入访问级别。

权限管理

提供权限在服务中授予或修改资源权限。例如，大多数 IAM 和 AWS Organizations 策略操作具有权限管理访问级别。

> **Tip**
>
> 要提高您的 AWS 账户的安全性，请限制或定期监控包括权限管理访问级别分类。

标记

提供权限创建、删除或修改附加到服务中的资源的标签。例如，Amazon EC2`CreateTags`和`DeleteTags`操作具有标记访问级别。

入门

AWS Identity and Access Management (IAM) 是一项 AWS 服务，可让您安全地管理对服务和资源的访问。IAM 是为您的 AWS 账户提供的一项功能，不会另外收费。

> **Note**
>
> 在开始使用 IAM 之前，请阅读有关AWS Global Accelerator 的身份和访问管理。

在首次创建 AWS 账户时，您最初使用一个具有账户中的所有 AWS 服务和资源的完全访问权限的单点登录身份。此身份称为 AWS 账户根用户，可以通过使用您用于创建账户的电子邮件地址和密码进行登录来访问该身份。强烈建议您不使用根用户执行日常任务，即使是管理任务。相反，请遵循仅使用根用户创建您的第一个 IAM 用户的最佳实践。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。

创建您的 IAM 管理员用户

自行创建管理员用户并将该用户添加到管理员组（控制台）

1. 登录到IAM 控制台作为帐户所有者，方法是选择根用户并输入您的 AWS 账户电子邮件地址。在下一页上，输入您的密码。

   > **Note**
   >
   > 强烈建议您遵守使用**`Administrator`**跟随并安全地锁定根用户凭证的 IAM 用户。只在执行少数账户和服务管理任务时才作为根用户登录。

2. 在导航窗格中，选择用户，然后选择添加用户。

3. 对于 User name (用户名)，输入 **Administrator**。
4. 选中 AWS Management Console access (AWS 管理控制台访问) 旁边的复选框。然后选择自定义密码，并在文本框中输入新密码。
5. （可选）默认情况下，AWS 要求新用户在首次登录时创建新密码。您可以清除 User must create a new password at next sign-in (用户必须在下次登录时创建新密码) 旁边的复选框以允许新用户在登录后重置其密码。
6. 选择后续：权限。
7. 在设置权限下，选择将用户添加到组。
8. 选择创建组。
9. 在 Create group (创建组) 对话框中，对于 Group name (组名称)，输入 **Administrators**。
10. 选择筛选策略，然后选择AWS 托管-工作职能来过滤表格内容。
11. 在策略列表中，选中 AdministratorAccess 的复选框。然后选择 Create group (创建组)。

> **Note**
>
> 您必须先激活 IAM 用户和角色对账单的访问权限，然后才能使用 AdministratorAccess 权限访问 AWS 账单和成本管理控制台。为此，请按照“向账单控制台委派访问权限”教程第 1 步中的说明进行操作。

12. 返回到组列表中，选中您的新组所对应的复选框。如有必要，选择 Refresh 以在列表中查看该组。
13. 选择后续：标签。
14. （可选）通过以键值对的形式附加标签来向用户添加元数据。有关在 IAM 中使用标签的更多信息，请参阅。标记 IAM 实体中的IAM 用户指南。
15. 选择后续：审核查看要添加到新用户的组成员资格的列表。如果您已准备好继续，请选择 Create user。

您可使用此相同的流程创建更多的组和用户，并允许您的用户访问 AWS 账户资源。要了解有关使用策略限制用户对特定 AWS 资源的权限的信息，请参阅访问管理和示例策略。

为 Global Accelerator 创建委托用户

要支持 AWS 账户中的多个用户，您必须委派权限以允许其他人仅执行您要允许的操作。为此，请创建一个 IAM 组（其中具有这些用户所需的权限），然后在创建 IAM 用户时将其添加到必要的组。您可以

使用此过程为您的整个 AWS 账户设置组、用户和权限。此解决方案最适合中小型组织，其中 AWS 管理员可以手动管理用户和组。对于大型组织，您可以使用自定义 IAM 角色、联合身份验证，或者单点登录。

在以下过程中，您将创建名为**arnav**、**carlos**, 和**martha**并附加一个策略，该策略授予创建名为**my-example-accelerator**，但只能在接下来的 30 天内。您可以使用此处提供的步骤添加具有不同权限的用户。

为其他人创建委托用户（控制台）

1. 登录 AWS 管理控制台，并通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Users，然后选择 Add user。
3. 对于 User name (用户名)，输入 **arnav**。
4. 选择 Add another user (添加其他用户) 并输入 **carlos** 作为第二个用户。然后选择 Add another user (添加其他用户) 并输入 **martha** 作为第三个用户。
5. 选中 旁边的复选框AWS 管理控制台访问，然后选择自动生成的密码。
6. 清除 User must create a new password at next sign-in (用户必须在下次登录时创建新密码) 旁边的复选框以允许新用户在登录后重置其密码。
7. 选择后续：权限。
8. 选择直接附加现有策略。您将为用户创建新的托管策略。
9. 选择创建策略。

   将在新的选项卡或浏览器窗口中打开 Create policy (创建策略) 向导。
10. 在可视化编辑器选项卡上，选择选择服务。然后选择 Global Accelerator。您可以使用顶部的搜索框限制服务列表中的结果。

    这些区域有：服务部分关闭，操作部分会自动打开。
11. 选择要允许的全局加速器操作。例如，要授予创建加速器的权限，请在**globalaccelerator:CreateAccelerator**中的筛选操作文本框。当筛选全局加速器操作列表时，选中**globalaccelerator:CreateAccelerator**。

    全局加速器操作按访问级别分类进行分组，以便您轻松快速确定每个操作提供的访问级别。有关更多信息，请参阅 策略访问级别分类。
12. 如果在前面的步骤中选择的操作不支持选择特定的资源，则会所有资源为您选择。在这种情况下，您无法编辑该部分。

如果您选择了一个或多个支持资源级权限的操作，则可视化编辑器会在 Resources (资源) 部分中列出这些资源类型。选择您选择了需要加速器资源类型选择是否要为策略输入特定的加速器。

13. 如果您想要允许针对所有资源执行 `globalaccelerator:CreateAccelerator` 操作，请选择 All resources (所有资源)。

    如果您要指定一个资源，请选择 Add ARN (添加 ARN)。指定区域和账户 ID（或账户 ID）（或者选择任何)，然后输入**`my-example-accelerator`**对于资源。然后，选择添加。

14. 选择 Specify request conditions (optional) (指定请求条件 (可选))。
15. 选择添加条件授予创建加速器的权限接下来的 7 天内。假定当天日期为 2019 年 1 月 1 日。
16. 对于 Condition Key (条件键)，选择 aws: CurrentTime。此条件键检查用户发出请求的日期和时间。它返回 true，因此仅当日期和时间在指定范围内时才允许 **`globalaccelerator:CreateAccelerator`** 操作。
17. 适用于限定词，请保留默认值。
18. 要指定允许的日期和时间范围的开始日期，对于 Operator (运算符)，请选择 DateGreaterThan。然后，对于 Value (值)，输入 **`2019-01-01T00:00:00Z`**。
19. 选择 Add (添加) 以保存您的条件。
20. 选择 Add another condition (添加另一个条件) 以指定结束日期。
21. 按照类似步骤指定允许的日期和时间范围的结束日期。对于 Condition Key (条件键)，选择 aws: CurrentTime。对于 Operator (运算符)，请选择 DateLessThan。对于 Value (值)，请输入 **`2019-01-06T23:59:59Z`**，值为第一个日期之后的第 7 天。然后，选择 Add (添加) 以保存您的条件。
22. （可选）要查看您正在创建的策略的 JSON 策略文档，请选择JSON选项卡。您可以随时在可视化编辑器和 JSON 选项卡之间切换。但是，如果您进行更改或选择查看策略中的可视化编辑器选项卡上，IAM 可能会调整您的策略结构以针对可视化编辑器进行优化。有关更多信息，请参阅 。调整策略结构中的IAM 用户指南。
23. 完成后，选择查看策略。
24. 在存储库的查看策略页面, 用于名称输入，输入**`globalaccelerator:CreateAcceleratorPolicy`**。对于描述，输入 **`Policy to grants permission to create an accelerator`**。查看策略摘要以确保您授予了所需的权限，然后选择创建策略以保存新策略。
25. 返回到原始选项卡或窗口，然后刷新您的策略列表。
26. 在搜索框中，输入 **`globalaccelerator:CreateAcceleratorPolicy`**。选中新策略旁边的复选框。然后选择 Next Step。

27. 选择后续：审核以预览您的新用户。如果您准备好继续，请选择 Create users (创建用户)。
28. 下载或复制新用户的密码并安全地将其提供给用户。另外，为用户提供链接到您的 IAM 用户控制台页面和刚刚创建的用户名。

允许用户自行管理其凭据

您必须拥有对将托管用户的虚拟 MFA 设备的硬件的物理访问权限以便配置 MFA。例如，您可能为使用在智能手机上运行的虚拟 MFA 设备的用户配置 MFA。在这种情况下，您必须具有智能手机才能完成该向导。因此，您可能想让用户配置和管理他们自己的虚拟 MFA 设备。在此情况下，您必须授予用户执行必要的 IAM 操作所需的权限。

创建允许凭证自我管理的策略（控制台）

1. 登录 AWS 管理控制台，并通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择策略，然后选择创建策略。
3. 选择 JSON 选项卡，然后复制以下 JSON 策略文档中的文本。将该文本粘贴到 JSON 文本框中。

> **Important**
>
> 本示例策略不允许用户在登录时重置密码。新用户和密码过期的用户可以执行此操作。您可以通过向语句 `BlockMostAccessUnlessSignedInWithMFA` 中添加 `iam:ChangePassword` 和 `iam:CreateLoginProfile` 来允许此操作。但是，IAM 不建议这样做。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllUsersToListAccounts",
            "Effect": "Allow",
            "Action": [
                "iam:ListAccountAliases",
                "iam:ListUsers",
                "iam:ListVirtualMFADevices",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid":
"AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation",
            "Effect": "Allow",
            "Action": [
                "iam:ChangePassword",
                "iam:CreateAccessKey",
                "iam:CreateLoginProfile",
                "iam:DeleteAccessKey",
                "iam:DeleteLoginProfile",
                "iam:GetLoginProfile",
                "iam:ListAccessKeys",
                "iam:UpdateAccessKey",
                "iam:UpdateLoginProfile",
                "iam:ListSigningCertificates",
                "iam:DeleteSigningCertificate",
                "iam:UpdateSigningCertificate",
                "iam:UploadSigningCertificate",
                "iam:ListSSHPublicKeys",
                "iam:GetSSHPublicKey",
                "iam:DeleteSSHPublicKey",
                "iam:UpdateSSHPublicKey",
                "iam:UploadSSHPublicKey"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowIndividualUserToViewAndManageTheirOwnMFA",
            "Effect": "Allow",
            "Action": [
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice",
                "iam:EnableMFADevice",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:mfa/${aws:username}",
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
```

```
            "Sid":
 "AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA",
            "Effect": "Allow",
            "Action": [
                "iam:DeactivateMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:mfa/${aws:username}",
                "arn:aws:iam::*:user/${aws:username}"
            ],
            "Condition": {
                "Bool": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        },
        {
            "Sid": "BlockMostAccessUnlessSignedInWithMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice",
                "iam:ListVirtualMFADevices",
                "iam:EnableMFADevice",
                "iam:ResyncMFADevice",
                "iam:ListAccountAliases",
                "iam:ListUsers",
                "iam:ListSSHPublicKeys",
                "iam:ListAccessKeys",
                "iam:ListServiceSpecificCredentials",
                "iam:ListMFADevices",
                "iam:GetAccountSummary",
                "sts:GetSessionToken"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

此策略有何作用？

- 这些区域有：AllowAllUsersToListAccounts语句让用户可以在 IAM 控制台中查看账户及其用户的基本信息。这些权限必须位于自己的语句中，因为它们不支持或不需要指定特定的资源 ARN，而需要指定 "Resource" : "*"。
- 这些区域有：AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation语句让用户可以在 IAM 控制台中管理自己的用户、密码、访问密钥、签名证书、SSH 公有密钥和 MFA 信息。它还允许用户首次登录（尽管管理员要求他们设置首次密码）。资源 ARN 仅限在用户自己的 IAM 用户实体中使用这些权限。
- AllowIndividualUserToViewAndManageTheirOwnMFA 语句让用户可以查看或管理其 MFA 设备。请注意，此语句中的资源 ARN 仅允许访问 MFA 设备，或者与当前登录用户完全同名的用户。用户不能创建或更改除自己设备外的任何 MFA 设备。
- AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA 语句让用户可以仅停用自己的 MFA 设备（仅在用户使用 MFA 登录时）。这可防止仅具有访问密钥（但没有 MFA 设备）的其他用户停用 MFA 设备和访问账户。
- 这些区域有：BlockMostAccessUnlessSignedInWithMFA语句使用"Deny"和"NotAction"拒绝访问 IAM 和其他 AWS 服务中除少数操作外的所有操作if用户未登录 MFA。有关此语句的逻辑的更多信息，请参阅。NotAction 与 Deny中的IAM 用户指南。如果用户使用 MFA 登录，则 "Condition" 测试失败，最后一个 "deny" 语句失效，而用户的其他策略或语句确定用户的权限。此语句可确保，当用户未使用 MFA 登录时，他们只能执行所列出的操作，并且仅当另一个语句或策略允许访问这些操作时方可执行。

  ...IfExists 运算符的 Bool 版本可确保：如果 aws:MultiFactorAuthPresent 键缺失，条件将返回 true。这意味着使用长期凭证（例如访问密钥）访问 API 的用户被拒绝访问非 IAM API 操作。

4. 完成后，选择查看策略。
5. 在 Review (查看) 页面上，输入 **Force_MFA** 作为策略名称。对于策略描述，输入**This policy allows users to manage their own passwords and MFA devices but nothing else unless they authenticate with MFA.**查看策略摘要以查看策略授予的权限，然后选择创建策略以保存您的工作。

   将在托管策略列表中显示新策略，并已准备好附加该策略。

将策略附加到用户（控制台）

1. 在导航窗格中，选择 Users。
2. 选择要编辑的用户的名称（不是复选框）。
3. 在权限选项卡中，请选择添加权限。
4. 选择直接附加现有策略。
5. 在搜索框中输入 **`Force`**，然后选中列表中 Force_MFA 旁的复选框。接下来，选择 Next (下一步)：审核。
6. 检查更改，然后选择 Add permissions (添加权限)。

为 IAM 用户启用 MFA

为增强安全性，我们建议所有 IAM 用户配置多重验证 (MFA) 以帮助保护您的全球加速器资源。MFA 增强了安全性，因为它要求用户除了其常规登录凭证之外，还要提供来自 AWS 支持的 MFA 设备的唯一身份验证。最安全的 AWS MFA 设备是 U2F 安全密钥。如果您的公司已经有 U2F 设备，我们建议您为 AWS 启用这些设备。否则，您必须为每个用户购买设备并等待硬件到达。有关更多信息，请参阅 。启用 U2F 安全密钥中的IAM 用户指南。

如果您还没有 U2F 设备，则可以通过启用虚拟 MFA 设备快速、低成本地开始使用。这要求您在现有手机或其他移动设备上安装软件应用程序。该设备将基于进行了时间同步的一次性密码算法生成一个六位数字代码。当用户登录 AWS 时，系统会提示从设备输入代码。分配给用户的每个虚拟 MFA 设备必须是唯一的。用户无法从另一个用户的虚拟 MFA 设备代码输入代码来进行身份验证。有关可用作虚拟 MFA 设备的一些受支持应用程序的列表，请参阅 Multi-Factor Authentication。

> **Note**
>
> 您必须拥有对将托管用户的虚拟 MFA 设备的移动设备的物理访问权限以便为 IAM 用户配置 MFA。

为 IAM 用户启用虚拟 MFA 设备（控制台）

1. 登录 AWS 管理控制台，并通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Users。
3. 在 User Name 列表中，选择目标 MFA 用户的名称。

4. 选择 Security Credentials 选项卡。在 Assigned MFA device (已分配 MFA 设备) 旁边，选择 Manage (管理)。
5. 在 Manage MFA Device (管理 MFA 设备) 向导中，选择 Virtual MFA device (虚拟 MFA 设备)，然后选择 Continue (继续)。

   IAM 将生成并显示虚拟 MFA 设备的配置信息，包括 QR 代码图形。此图形是秘密配置密钥的表示形式，适用于不支持 QR 代码的设备上的手动输入。
6. 打开您的虚拟 MFA 应用程序。

   有关可用于托管虚拟 MFA 设备的应用程序的列表，请参阅 Multi-Factor Authentication。如果虚拟 MFA 应用程序支持多个账户 (多个虚拟 MFA 设备)，请选择相应的选项以创建新账户 (新的虚拟 MFA 设备)。
7. 确定 MFA 应用程序是否支持 QR 代码，然后执行以下操作之一：

   - 在向导中，选择 Show QR 代码 (显示 QR 代码)，然后使用该应用程序扫描 QR 代码。例如，您可选择摄像头图标或选择类似于 Scan code 的选项，然后使用设备的摄像头扫描此代码。
   - 在 Manage MFA Device (管理 MFA 设备) 向导中，选择 Show secret key (显示私有密钥)，然后在您的 MFA 应用程序中输入私有密钥。

   完成操作后，虚拟 MFA 设备会开始生成一次性密码。
8. 在 Manage MFA Device (管理 MFA 设备) 向导的 MFA code 1 (MFA 代码 1) 框中，输入虚拟 MFA 设备上当前显示的一次性密码。请等候 30 秒，以便设备生成新的一次性密码。然后在 MFA code 2 (MFA 代码 2) 框中输入第二个一次性密码。选择 Assign MFA (分配 MFA)。

   > **Important**
   >
   > 生成代码之后立即提交您的请求。如果生成代码后等待很长时间才提交请求，MFA 设备会成功与用户关联，但 MFA 设备无法同步。这是因为基于时间的一次性密码 (TOTP) 很快会过期。这种情况下，您可以重新同步设备。有关更多信息，请参阅 。重新同步虚拟和硬件 MFA 设备中的IAM 用户指南。

   虚拟 MFA 设备现在已准备好与 AWS 一起使用了。

AWS Global Accelerator 中的 VPC 连接安全

当您在 AWS Global Accelerator 中添加内部 Application Load Balancer 器或 Amazon EC2 实例终端节点时，您可以通过将互联网流量定位在私有子网中，从而使互联网流量直接流入和流出虚拟私有云 (VPC) 中的终端节点。包含负载均衡器或 EC2 实例的 VPC 必须具有互联网网关，以表示 VPC 接受互联网流量。但是，您不需要负载均衡器或 EC2 实例上的公有 IP 地址。您也不需要子网相关联的 Internet 网关路由。

这不同于典型的互联网网关使用情形，即互联网流量流向 VPC 中的实例或负载均衡器需要公有 IP 地址和互联网网关路由。即使目标的弹性网络接口存在于公有子网（即具有 Internet 网关路由的子网）中，当您使用全局加速器进行 Internet 流量时，全局加速器会覆盖典型的 Internet 路由和所有通过全局到达的逻辑连接加速器还通过全球加速器返回，而不是通过互联网网关返回。

> **Note**
>
> 对您的 Amazon EC2 实例使用公有 IP 地址和使用公有子网并不常见，尽管您可以使用它们设置配置。安全组应用于到达实例的任何流量，包括来自全局加速器的流量以及分配给您的实例 ENI 的任何公有或弹性 IP 地址。使用私有子网确保流量仅由全局加速器传输。

在考虑网络外围问题和配置与 Internet 访问管理相关的 IAM 权限时，请牢记这些信息。有关控制对 VPC 的互联网访问的更多信息，请参阅此服务控制策略示例。

AWS Global Accelerator 中的日志记录和监控

监控是保持全球加速器和 AWS 解决方案的可用性和性能的重要环节。您应从 AWS 解决方案的所有部分收集监控数据，以便更轻松地调试出现的多点故障。AWS 提供了多种工具来监控全球加速器资源和活动并对潜在的事件做出响应：

AWS Global Accelerator 流日志

服务器流日志提供有关通过加速器流向端点的流量的详细记录。服务器流日志对于许多应用程序很有用。例如，流日志信息可能在安全和访问权限审核方面很有用。有关更多信息，请参阅 AWS Global Accelerator 中的流日志。

Amazon CloudWatch 指标和警报

使用 CloudWatch，您可以实时监控您的 AWS 资源以及在 AWS 上运行的应用程序。CloudWatch 会收集和跟踪指标，这些指标是您在一段时间内测量的变量。您可以创建警报，这些警报监视特

定指标，然后在指标超出特定阈值时，发送通知或者对您所监控的资源自动进行更改。有关更多信息，请参阅 Amazon CloudWatch 与 AWS Global Accelerator 结合使用。

AWS CloudTrail 日志

CloudTrail 提供了用户、角色或 AWS 服务在全球加速服务中所执行操作的记录。CloudTrail 将对全局加速器的所有 API 调用均作为事件捕获，包括来自全局加速器控制台的调用和对全局加速器 API 的代码调用。有关更多信息，请参阅 使用 AWS CloudTrail 记录 AWS Global Accelerator API 调用。

AWS Global Accelerator 的合规性验证

作为多项 AWS 合规性计划的一部分，第三方审计员将评估 AWS Global Accelerator 的安全性和合规性。其中包括 SOC、PCI、HIPAA、GDPR、ISO 和 ENS 高。

有关特定合规性计划范围内的 AWS 服务的列表，包括全球加速器，请参阅按合规性计划提供范围内 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 Accelerator 中下载报告。

您在使用 Global Access 时的合规性责任由您的数据的敏感性、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实现合规性：

- 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。
- 使用规则评估资源中的AWS Config 开发人员指南— AWS Config 服务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。

AWS Global Accelerator 中的弹性

AWS 全球基础设施围绕 AWS 区域和可用区构建。AWS 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。

除了支持 AWS 全球基础设施外，全球加速器还提供以下功能，以帮助支持数据恢复：

- 网络区域为来自唯一 IP 子网的加速器的静态 IP 地址提供服务。与 AWS 可用区类似，网络区域是一个具有自己一组物理基础设施的隔离单元。配置加速器时，全局加速器会为其分配两个 IPv4 地址。如果某个网络区域中的一个 IP 地址由于某些客户端网络的 IP 地址阻止或由于网络中断而变得不可用，则客户端应用程序可以重试来自另一个隔离网络区域的健康静态 IP 地址。
- 全球加速器持续监控所有终端的运行状况。当它确定活动终端节点运行状况不佳时，全局加速器会立即开始将流量定向到另一个可用终端节点。这样，您就可以在 AWS 上为您的应用程序创建高可用性架构。

AWS Global Accelerator 中的基础设施安全性

作为一项托管服务，AWS Global Accelerator 由 AWS 全球网络安全程序（Amazon Web Services：安全过程概述白皮书。

您可以使用 AWS 发布的 API 调用通过网络访问全球加速器。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。

AWS Global Accelerator 的配额

您的 AWS 账户具有与 AWS Global Accelerator 相关的特定配额（也称为限制）。

“Service Quotas” 控制台提供有关 Global Accelerator 配额的信息 除了查看默认配额外，还可以使用 “Service Quotas” 控制台请求配额增加以获取可调配额。请注意，当您请求增加全球加速器的配额时，您必须位于美国东部（弗吉尼亚北部）。

主题

常规配额

以下是全局加速器的总体配额。

实体	配额
每个 AWS 账户的加速器	20 您可以请求提高配额。
每个加速器的侦听器	10 您可以请求提高配额。
每个侦听器的端口范围	10
每个端点组的端口覆盖	10 您可以请求提高配额。

每个端点组的终端节点配额

以下是适用于终端节点组中终端节点数量的全局加速器配额。

实体	描述	配额
具有多个终端节点类型的终端节点组	包含多个终端节点类型的终端节点组中的终端节点数。	10
仅使用应用程序负载均衡器的终端节点组	仅包含应用程序负载均衡器终端节点的终端节点组中的应用程序负载均衡器数。	10
仅使用网络负载均衡器的端点组	仅包含网络负载平衡器终端节点的终端节点组中的 Network Load Balancer 数量。	10
仅具有 Amazon EC2 实例的终端节点组	仅包含 EC2 实例终端节点的终端节点组中 EC2 实例的数量。	10 您可以请求提高配额。
仅具有弹性 IP 地址的终端节点组	仅包含弹性 IP 地址终端节点的终端节点组中的弹性 IP 地址数。	10 您可以请求提高配额。
仅具有 Amazon Virtual Private Cloud 子网的终端节点组	终端节点组中仅包含子网终端节点的 Amazon VPC 子网数量。	10 您可以请求提高配额。

相关配额

除了 Global Accelerator 中的配额外，还存在适用于用作加速器终端节点的资源的配额。有关更多信息，请参阅下列内容：

- 弹性 IP 地址配额中的Amazon EC2 用户指南。
- Amazon EC2 服务配额中的Amazon EC2 用户指南。
- 网络负载均衡器的配额中的适用于网络负载均衡器的用户指南。
- 您的应用程序负载均衡器的配额中的适用于应用程序负载均衡器的用户指南。
- Amazon VPC 配额中的Amazon VPC 用户指南。

AWS Global Accelerator 相关信息

此处列出的信息和资源可以帮助您了解有关 Global Accelerator 的更多信息。

主题

其他 AWS Global Accelerator 文档

下列相关资源在您使用此服务的过程中会有所帮助。

- AWS Global Accelerator API 参考— 提供 API 操作、参数和数据类型的完整说明，以及该服务返回的错误的列表。
- AWS Global Accelerator 产品信息— 提供 Global Accelerator 相关信息的主要网页，包括各种功能和定价信息。
- 使用条款— 有关我们的版权和商标、您的账户、许可、网站访问和其他主题的详细信息。

获取支持

对全局加速器的 Support 有多种形式。

- 开发论坛— 基于社区的论坛，供开发人员讨论与 Global Accelerator 有关的技术问题。
- AWS Support 中心 – 此站点汇集了有关您近期的支持案例的信息，以及来自 AWS Trusted Advisor 和运行状况检查的结果，并提供了指向开发论坛、技术常见问题解答、服务运行状况控制面板以及有关 AWS 支持计划的信息的链接。
- AWS Premium Support 信息 – 提供有关 AWS Premium Support 信息的主要网页，AWS Premium Support 是一种一对一的快速响应支持渠道，可帮助您在 AWS 基础设施服务上构建和运行应用程序。
- 联系我们 – 用于咨询有关您的账单或账户的问题的链接。如有技术问题，请使用上述开发论坛或支持连接。

来自 Amazon Web Services 博客的提示

AWS 博客包含很多文章，可帮助您使用 AWS 服务。例如，可参阅以下博客文章以了解 Global Accelerator：

- AWS 全球可用性和性能加速服务
- AWS Global Accelerator 的流量管理
- 使用亚马逊雅典娜和亚马 Amazon QuickSight 分析和可视化 AWS Global Accelerator 流日志

有关 AWS Global Accelerator 博客的完整列表，请参阅AWS Global Accelerator在 AWS 博客文章的“网络和内容交付” 类别中。

文档历史记录

以下条目介绍了 AWS Global Accelerator 文档的一些重要更改。

- API 版本：最新
- 最近文档更新时间：2020 年 12 月 9 日

变更	描述	日期
更新到全球加速器现有与服务相关的角色	全局加速器添加了一个新权限`ec2:DescribeRegions` ，以允许全球加速器获取 AWS 区域信息以帮助诊断错误。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/security-iam-awsmanpol-updates.html。	2021 年 5 月 7 日
添加了自定义路由加速器	全球加速器推出了一种新型的加速器自定义路由加速器。自定义路由加速器适用于您希望使用自定义应用程序逻辑将一个或多个用户引导到多个特定目的地和端口，同时仍能获得全球加速器的性能优势的场景。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/work-with-custom-routing-accelerators.html。	2020 年 12 月 9 日
添加端口覆盖支持	全局加速器现在支持覆盖用于将流量路由到终端节点的侦听器端口，以便您可以将流量重新路由到终端上的特定	2020 年 10 月 21 日

变更	描述	日期
	端口。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-port-override.html。	
增加了两个新区域	Global Accelerator 现在支持非洲（开普敦）和欧洲（米兰）。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/preserve-client-ip-address.regions.html。	2020 年 5 月 20 日
标记和 BYOIP	此版本增加了对向加速器添加标签以及将您自己的 IP 地址引入 AWS Global Accelerator (BYOIP) 的支持。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/tagging-in-global-accelerator.html 和 https://docs.aws.amazon.com/global-accelerator/latest/dg/using-byoip.html。	2020 年 2 月 27 日
更新了安全性章节	增加了法规遵从性、恢复性和基础架构安全性的内容。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/security.html。	2019 年 12 月 20 日

变更	描述	日期
Support EC2 实例和默认 DNS 名称	AWS Global Accelerator 现在支持在受支持的 AWS 区域中添加 EC2 实例。此外，全局加速器会创建一个默认 DNS 名称，该名称映射到加速器的静态 IP 地址。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html 和 https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.html#about-accelerators.dns-addressing。	2019 年 10 月 29 日
应用程序负载平衡器的客户端 IP 地址保留	现在，您可以选择让 AWS Global Accelerator 在受支持的 AWS 区域中保留应用程序负载均衡器的客户端 IP 地址。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html。	2019 年 8 月 28 日
AWS Global Accelerator 服务的发布	《AWS Global Accelerator 开发人员指南》提供了有关设置和使用加速器（网络层流量管理器）的信息，这些加速器可提高具有全球受众群体的互联网应用程序的可用性和性能。	2018 年 11 月 26 日

AWS 词汇表

For the latest AWS terminology, see the AWS glossary in the AWS General Reference.

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。