开发人员指南

AWS Global Accelerator

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Global Accelerator: 开发人员指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 AWS Global Accelerator？ 1
组件 2
AWS 区域 4
工作方式 6
工作原理概述 7
加速器的类型 8
空闲超时 9
全局静态 IP 地址 9
运行状况检查 10
流量拨号和端点权重 10
ICMP 响应消息 11
IP 地址范围 12
使用案例 13
速度比较工具 14
如何开始 14
标记 15
Global Accelerator 中的标记支持 16
在 Global Accelerator 中添加、编辑和删除标签 16
定价 17
入门 18
创建标准加速器 18
开始前的准备工作 19
第 1 步：创建标准加速器 19
第 2 步：添加侦听器 20
第 3 步：添加端点组 20
第 4 步：添加端点 21
第 5 步：测试加速器 21
第 6 步（可选）：删除加速器 22
创建自定义路由加速器 23
开始前的准备工作 23
第 1 步：创建自定义路由加速器 24
第 2 步：添加侦听器 24
第 3 步：添加端点组 24
第 4 步：添加 VPC 子网端点 25

第 5 步（可选）：删除加速器 26
API 操作 28
使用标准加速器 31
标准加速器 31
创建加速器 32
更新加速器 33
删除加速器 34
查看加速器 35
将 Global Accelerator 与负载均衡器创建过程相集成 36
比较全局地址和区域地址 37
标准加速器的侦听器 37
添加侦听器 38
编辑侦听器 38
移除侦听器 39
客户端亲和性的工作原理 39
标准加速器的端点组 40
添加端点组 41
编辑端点组 42
移除端点组 42
通过流量拨号调整流量流 42
覆盖侦听器端口 43
确保运行状况检查访问权限 45
标准加速器的端点 47
端点要求 48
添加端点 49
编辑端点 51
移除端点 51
端点权重的工作原理 52
运行状况不佳的端点的失效转移 52
避免 TCP 连接时间延迟 53
使用自定义路由加速器 56
自定义路由加速器的工作原理 57
自定义路由示例 58
自定义路由准则 61
自定义路由加速器 63
创建自定义路由加速器 64

编辑自定义路由加速器 64
查看自定义路由加速器 65
删除自定义路由加速器 65
自定义路由加速器的侦听器 66
添加侦听器 66
编辑侦听器 67
移除侦听器 68
自定义路由加速器的端点组 68
添加端点组 69
编辑端点组 69
移除端点组 70
VPC 子网端点 70
添加 Amazon VPC 子网端点 71
编辑 Amazon VPC 子网端点 72
移除 Amazon VPC 子网端点 73
配置跨账户访问 75
跨账户机制的工作原理 75
使用跨账户附件 76
创建跨账户附件 76
编辑跨账户附件 77
删除跨账户附件 78
使用跨账户资源 78
添加跨账户 BYOIP 地址 79
添加跨账户端点 80
移除跨账户端点 80
识别跨账户资源 81
所有者：识别跨账户资源 81
主体：识别跨账户资源 81
责任和权限 83
资源所有者的权限 83
主体的权限 83
成本计费 83
配额 84
DNS 寻址和自定义域 85
支持 DNS 寻址 85
将自定义域流量路由到您的加速器 86

自带 IP 地址 86
要求 87
IP 地址范围授权 88
预置地址范围 91
宣布地址范围 92
取消预配置地址范围 93
将 BYOIP 地址与加速器配合使用 94
更新 IP 地址 94
保留客户端 IP 地址 97
准则和限制 97
客户端 IP 地址保留的要求 99
如何保留客户端 IP 地址 100
客户端 IP 地址保留的优势 101
ENI 和安全的最佳实操 102
转换端点 104
转换端点 104
日志记录和监控 107
CloudWatch 监控 107
Global Accelerator 指标 108
加速器的指标维度 116
解决 Global Accelerator TCP 重置问题 118
Global Accelerator 指标的统计数据 119
查看适用于您的加速器的 CloudWatch 指标 119
流日志 121
启用流日志 122
处理流日志记录 123
发布到 Amazon S3 123
日志文件时间 127
流日志记录语法 128
CloudTrail 日志 130
CloudTrail 中的 Global Accelerator 信息 130
在事件历史记录中查看 Global Accelerator 事件 131
了解 Global Accelerator 日志文件条目 131
安全性 140
Identity and Access Management 140
受众 141

使用身份进行身份验证 141
使用策略管理访问 144
Global Accelerator 如何与 IAM 配合使用 146
基于身份的策略示例 151
服务相关角色 156
AWS 托管式策略 158
基于标签的策略 161
故障排除 162
安全 VPC 连接 163
日记账记录和监控 164
合规性验证 165
弹性 166
基础设施安全性 167
配额 168
常规配额 168
每个端点组的端点配额 169
相关限额 170
相关信息 171
AWS Global Accelerator 的 API 参考和产品信息 171
获取支持 171
来自 AWS 博客网站的提示 172
文档历史记录 173

什么是 AWS Global Accelerator？

AWS Global Accelerator 是一项服务，您可以在该服务中创建加速器，以提高本地用户和全球用户的应用程序性能。根据您选择的加速器类型，您可以获得额外好处：

- 借助标准加速器，您可以提高全球受众使用的互联网应用程序的可用性。借助标准加速器，Global Accelerator 可通过 AWS 全球网络将流量引导至离客户端最近的区域中的端点。
- 借助自定义路由加速器，您可以将一个或多个用户映射到多个目标中的特定目标。

Global Accelerator 是一项全球服务，可支持多个 AWS 区域中的端点。要确定特定 AWS 区域当前是否支持 Global Accelerator 或其它服务，请参阅 AWS 区域服务列表。

默认情况下，Global Accelerator 为您提供与加速器关联的静态 IP 地址。静态 IP 地址是 AWS 边缘网络中的任播。对于 IPv4，Global Accelerator 提供两个静态 IPv4 地址。对于双堆栈，Global Accelerator 提供总计四个地址：两个静态 IPv4 地址和两个静态 IPv6 地址。对于 IPv4，您可以将这些入口点配置为您带到 Global Accelerator（BYOIP）的自有 IP 地址范围中的 IPv4 地址，而不必使用 Global Accelerator 提供的地址。

> **Important**
>
> 即使您禁用加速器且加速器不再接受或路由流量，只要加速器存在，静态 IP 地址仍会分配给该加速器。但是，如果您删除加速器，您将丢失分配给该加速器的静态 IP 地址，因此您无法再使用这些地址路由流量。您可以将 IAM 策略（如基于标签的权限）与 Global Accelerator 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 ABAC 与 Global Accelerator。

对于标准加速器，根据运行状况、客户端位置和您配置的策略，Global Accelerator 使用 AWS 全球网络将流量路由到最佳的区域端点，从而提高应用程序的可用性。标准加速器的端点可以是位于一个 AWS 区域或多个区域的网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址。

该服务会立即对运行状况或配置的变化做出反应，以确保来自客户端的互联网流量始终引导至运行状况良好的端点。Global Accelerator 还遵守受支持端点的 ARC 流量重定向，以通过可用区转移或可用区自动转移重新路由来自可能受损的可用区的流量。有关更多信息，请参阅 Amazon 应用程序恢复控制器（ARC）中的多可用区恢复。

自定义路由加速器仅支持 Amazon VPC（VPC）子网端点类型，并将流量路由到该子网中的私有 IP 地址。

内容

- AWS Global Accelerator 组件
- AWS Global Accelerator 支持的 AWS 区域
- AWS Global Accelerator 的工作原理
- Global Accelerator 边缘服务器的位置和 IP 地址范围
- 了解 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
- 在 AWS Global Accelerator 中添加标签
- AWS Global Accelerator 定价

AWS Global Accelerator 组件

AWS Global Accelerator 包括以下组件：

静态 IP 地址

默认情况下，Global Accelerator 为您提供与加速器关联的静态 IP 地址。静态 IP 地址是 AWS 边缘网络中的任播。对于 IPv4，Global Accelerator 提供两个静态 IPv4 地址。对于双堆栈，Global Accelerator 提供总计四个地址：两个静态 IPv4 地址和两个静态 IPv6 地址。如果您自带 IP 地址范围到 AWS（BYOIP）以用于 Global Accelerator（仅限 IPv4），则可以改为从自己的池中分配 IPv4 地址以用于加速器。有关更多信息，请参阅 在 Global Accelerator 中自带 IP 地址（BYOIP）。

IP 地址充当客户端的单一固定入口点。如果您已为应用程序设置弹性负载均衡负载均衡器、Amazon EC2 实例或弹性 IP 地址资源，则可以轻松地将其添加到 Global Accelerator 中的标准加速器中。这让 Global Accelerator 能够使用静态 IP 地址访问资源。如果您想使用 Global Accelerator 静态 IP 地址访问 API Gateway，请参阅以下博客文章了解更多信息：Accessing an Amazon API Gateway via static IP addresses provided by AWS Global Accelerator。

即使您禁用加速器且加速器不再接受或路由流量，只要加速器存在，静态 IP 地址仍会分配给该加速器。但是，如果您删除加速器，您将丢失分配给该加速器的静态 IP 地址，因此您无法再使用这些地址路由流量。您可以将 IAM 策略（如基于标签的权限）与 Global Accelerator 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 ABAC 与 Global Accelerator。

Accelerator

加速器通过 AWS 全球网络将流量引导至端点，以提高互联网应用程序的性能。每个加速器包含一个或多个侦听器。

加速器有两种类型：

- 根据多种因素（包括用户的位置、端点的运行状况以及您配置的端点权重），标准加速器会将流量引导至最佳 AWS 端点。这会提高应用程序的可用性和性能。端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。
- 借助自定义路由加速器，您可以确定性地将多个用户路由到加速器后端的特定 EC2 目标，这是某些使用案例所必需的。为此，您可以将用户引导至到加速器上的唯一 IP 地址和端口，Global Accelerator 已将该加速器映射到目标。请注意，自定义路由加速器不支持 IP 地址的双堆栈配置。

有关更多信息，请参阅 加速器的类型。

DNS 名称

Global Accelerator 会为每个加速器分配一个默认的域名系统（DNS）名称，该名称类似于 `a1234567890abcdef.awsglobalaccelerator.com`，用于指向 Global Accelerator 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。如果您有双堆栈加速器，Global Accelerator 还会为您分配一个双堆栈 DNS 名称，类似于 `a1234567890abcdef.dualstack.awsglobalaccelerator.com`，用于指向双堆栈加速器的四个静态 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。有关更多信息，请参阅 AWS Global Accelerator 中支持 DNS 寻址。

网络区域

与 AWS 可用区类似，网络区域是一个具有自己的物理基础设施集的隔离单元。创建加速器时，Global Accelerator 会为您提供一组静态 IP 地址：两个静态 IPv4 地址用于 IP 地址类型为 IPv4 的加速器，或者四个静态 IP 地址用于双堆栈加速器（两个 IPv4 地址和两个 IPv6 地址）。Global Accelerator 从每个 IP 地址系列的唯一 IP 子网中为每个网络区域提供一个静态 IP 地址。如果由于某些客户端网络阻止 IP 地址或网络中断而导致网络区域中的一个地址不可用，则客户端应用程序可以重试来自其它隔离网络区域的正常静态 IP 地址。

Listener

根据您配置的端口（或端口范围）和协议（或多个协议），侦听器可处理从客户端到 Global Accelerator 的入站连接。可以为 TCP、UDP 或 TCP 和 UDP 协议配置侦听器。每个侦听器都有

一个或多个与其关联的端点组，流量会转发到其中一个组中的端点。通过指定要向其分配流量的区域，您可以将端点组与侦听器相关联。借助标准加速器，流量将分配到与侦听器关联的端点组中的最佳端点。

端点组

每个端点组都与一个特定的 AWS 区域相关联。端点组包括该区域中的一个或多个端点。借助标准加速器，您可以通过调整名为流量拨号的设置来增加或减少原本会引导至端点组的流量百分比。例如，流量拨号使您可以轻松地进行性能测试或蓝/绿部署测试，例如跨不同 AWS 区域测试新版本。

终端节点

端点是 Global Accelerator 将流量引导至的资源。

标准加速器的端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端点可以是面向互联网的端点，也可以是内部的端点。标准加速器的流量将根据端点的运行状况以及您选择的配置选项（例如端点权重）路由到端点。您可以为每个端点配置权重，权重是数字，可用于指定要路由到每个端点的流量比例。例如，这对于在区域内进行性能测试很有用。

自定义路由加速器的端点是带有一个或多个 Amazon EC2 实例（这些实例是流量的目标）的 Amazon VPC（VPC）子网。

AWS Global Accelerator 支持的 AWS 区域

有关 AWS Global Accelerator 的区域支持和服务端点的详细信息，请参阅《Amazon Web Services 一般参考》中的 AWS Global Accelerator 端点和配额。

> **Note**
>
> AWS Global Accelerator 是一项全球性服务。但是，您必须在区域 Global Accelerator AWS CLI 命令中指定美国西部（俄勒冈州）区域（即指定参数 `--region us-west-2`）。也就是说，当您创建资源（例如加速器）时，需要进行指定。

Global Accelerator 目前在以下 AWS 区域中可用。可用区（AZ）例外情况已注明。

区域名称	区域
美国东部（俄亥俄）	`us-east-2`

区域名称	区域
美国东部（弗吉尼亚州北部）	us-east-1
美国西部（加利福尼亚北部）	us-west-1 (except AZ usw1-az2)
美国西部（俄勒冈州）	us-west-2
非洲（开普敦）	af-south-1
亚太地区（香港）	ap-east-1
亚太地区（孟买）	ap-south-1
亚太地区（海得拉巴）	ap-south-2
亚太地区（雅加达）	ap-southeast-3
亚太地区（墨尔本）	ap-southeast-4
亚太地区（大阪）	ap-northeast-3
亚太地区（新加坡）	ap-southeast-1
亚太地区（悉尼）	ap-southeast-2
亚太地区（东京）	ap-northeast-1 (except AZ apne1-az3)
亚太地区 (首尔)	ap-northeast-2
加拿大（中部）	ca-central-1 (except AZ cac1-az3)
加拿大西部（卡尔加里）	ca-west-1
欧洲地区（法兰克福）	eu-central-1
欧洲地区（爱尔兰）	eu-west-1
欧洲地区（伦敦）	eu-west-2
欧洲地区（米兰）	eu-south-1

区域名称	区域
欧洲地区（巴黎）	eu-west-3
欧洲（西班牙）	eu-south-2
欧洲地区（斯德哥尔摩）	eu-north-1
欧洲（苏黎世）	eu-central-2
以色列（特拉维夫）	il-central-1
中东（巴林）	me-south-1
中东（阿联酋）	me-central-1
南美洲（圣保罗）	sa-east-1

AWS Global Accelerator 的工作原理

AWS Global Accelerator 提供的静态 IP 地址可充当客户端的单一固定入口点。使用 Global Accelerator 设置加速器时，可以将静态 IP 地址关联到一个或多个 AWS 区域中的区域端点。对于标准加速器，端点是网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址。对于自定义路由加速器，端点是带有一个或多个 EC2 实例的 Amazon VPC（VPC）子网。静态 IP 地址可以接受从离用户最近的边缘站点进入 AWS 全球网络的传入流量。

> **Note**
>
> 如果您自带 IP 地址范围到 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 Global Accelerator 中自带 IP 地址（BYOIP）。

从边缘站点开始，应用程序的流量将根据您配置的加速器类型进行路由。

- 对于标准加速器，流量会根据多种因素（包括用户的位置、端点的运行状况以及您配置的端点权重）路由到最佳 AWS 端点。
- 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，每个客户端会路由到 VPC 子网中的特定 Amazon EC2 实例和端口。

在使用 Global Accelerator 时，请注意以下事项：

- 覆盖端点权重：在特定的有限场景中，Global Accelerator 会覆盖您设置的端点权重，以帮助确保可用性。当 Global Accelerator 在端点组中的端点之间对流量进行负载均衡时，在某些情况下，必须在保持客户端流量的可用性和遵守端点权重之间做出选择。例如，对于保留客户端 IP 地址的加速器，Global Accelerator 可能需要覆盖端点权重设置以帮助避免连接冲突。
- 安全组和规则：添加加速器时，您已经配置的安全组和 AWS WAF 规则会像添加加速器之前一样继续工作。
- IP 分段：通过互联网或其它大型网络传输时，如果 IP 数据包过大而无法容纳标准以太网帧（1500 字节以上），则由中间路由器分段并单独发送。TCP 协议不需要 IP 分段，因为客户端和端点会自动协商较小的最大分段大小（MSS）。但是，UDP 协议需要 IP 分段。当数据包被分段时，Global Accelerator 会将 UDP 分段转发到配置的端点，该端点会重新组装原始 IP 数据包。Global Accelerator 会丢弃边缘的 TCP 分段，因为 AWS 网络不支持这些分段。

主题

- AWS Global Accelerator 的工作原理概述
- 加速器的类型
- 了解 AWS Global Accelerator 中的空闲超时
- 使用 AWS Global Accelerator 中的静态 IP 地址
- Global Accelerator 如何使用运行状况检查
- 如何使用流量拨号和端点权重管理流量流向
- ICMP 响应消息和 AWS Global Accelerator

AWS Global Accelerator 的工作原理概述

流量通过监控良好、无拥塞、冗余的 AWS 全球网络传送到端点。通过最大限度地延长流量在 AWS 网络上的时间，Global Accelerator 可确保流量始终通过最佳网络路径进行路由。Global Accelerator 会终止来自 AWS 边缘站点客户端的 TCP 连接，并几乎同时与您的端点建立新的 TCP 连接。这为客户端提供了更快的响应时间（更低的延迟）和更高的吞吐量。

Global Accelerator 始终为自定义路由加速器上的端点保留客户端 IP 地址。借助标准加速器，您可以选择保留和访问某些端点类型的客户端 IP 地址。有关 Global Accelerator 支持的端点类型和配置（包括客户端 IP 地址保留支持）的详细信息，请参阅对可添加为加速器端点的资源的要求。

借助标准加速器，Global Accelerator 可以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，立即开始将所有新连接的流量引导至另一个可用端点。这使您可以为 AWS 上的应用程序创建高可用性架构。运行状况检查不用于自定义路由加速器，也没有失效转移，因为您可以指定要将流量路由到的目标。

如果您想对全局流量进行精细控制，可以在标准加速器中为端点配置权重。此外，您还可以使用 Global Accelerator 中的流量拨号来增加（调高）或减少（调低）特定端点组的流量百分比，例如用于性能测试或堆栈升级。

加速器的类型

您可以在 AWS Global Accelerator 中使用两种类型的加速器：标准加速器和自定义路由加速器。这两种类型的加速器都通过 AWS 全球网络路由流量，以提高性能和稳定性，但它们各自针对不同的应用程序需求进行设计。

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。借助标准加速器，Global Accelerator 可根据地理邻近性和端点运行状况，将客户端流量路由到各个区域端点。此外，它还允许客户根据流量拨号和端点权重等控制在端点之间转移客户端流量。这适用于各种使用案例，包括蓝/绿部署、A/B 测试和多区域部署。要查看更多使用案例，请参阅 了解 AWS Global Accelerator 使用案例。

要了解更多信息，请参阅 在 AWS Global Accelerator 中使用标准加速器。

自定义路由加速器

自定义路由加速器非常适合您希望使用自定义应用程序逻辑将一个或多个用户引导至到特定目的地和多个端口之一，同时仍能获享 Global Accelerator 的性能优势的场景。其中一个示例是 VoIP 应用程序，它将多个呼叫方分配到特定的媒体服务器以启动语音、视频和消息会话。另一个示例是在线实时游戏应用程序，在该应用程序中您希望根据地理位置、玩家技能和游戏模式等因素将多名玩家分配给游戏服务器上的单个会话。

> **Note**
>
> 自定义路由加速器仅支持 IPv4 IP 地址类型。

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，您可以创建其中一种类型的加速器来加速客户流量。

了解 AWS Global Accelerator 中的空闲超时

AWS Global Accelerator 可设置应用于其连接的空闲超时期限。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。空闲超时期限不可自定义。

为防止连接超时，Global Accelerator 要求您在 TCP 连接超时窗口内，在入口或出口方向发送至少包含一字节数据的数据包。您不能使用 TCP 保活数据包来保持打开的连接。

网络连接的 Global Accelerator 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。

即使端点被标记为运行状况不佳或已从加速器中移除，Global Accelerator 仍会继续将已建立连接的流量引导至该端点，直到达到空闲超时为止。如果需要，Global Accelerator 仅在新连接启动时或在空闲超时后才会选择新的端点。

使用 AWS Global Accelerator 中的静态 IP 地址

默认情况下，Global Accelerator 为您提供与加速器相关联的静态 IP 地址。您可以使用 Global Accelerator 分配给加速器的静态 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）将互联网流量路由到靠近用户所在位置的 AWS 全球网络，无论用户身在何处都不受影响。对于标准加速器，您可以将地址与在单个 AWS 区域或多个区域中运行的网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址相关联。对于自定义路由加速器，您可以将流量引导至一个或多个区域的 VPC 子网中的 EC2 目标。通过 AWS 全球网络路由流量可以提高可用性和性能，因为流量不必在公共互联网上进行多重跳转。通过使用静态 IP 地址，您还可以在多个 AWS 区域中的多个端点资源中分发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您进行更改时以一致的方式连接到应用程序。

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

静态 IP 地址是 AWS 边缘网络中的任播。

对于 IPv4，Global Accelerator 提供两个静态 IPv4 地址。对于双堆栈，Global Accelerator 提供总计四个地址：两个静态 IPv4 地址和两个静态 IPv6 地址。如果您自带 IP 地址范围到 AWS（BYOIP）以用

于 Global Accelerator（仅限 IPv4），则可以改为从自己的池中分配 IPv4 地址以用于加速器。有关更多信息，请参阅 在 Global Accelerator 中自带 IP 地址（BYOIP）。

对于使用双堆栈的加速器，Global Accelerator 会从相同的两个 /64 CIDR 前缀中分配 IPv6 地址。这有助于简化设置允许列表和 ACL 控制的步骤。

您可以将仅限 IPv4 的端点添加到为 IPv4 IP 地址类型配置的标准加速器中，但是配置为双堆栈的加速器需要您仅添加同样支持双堆栈的端点。有关双堆栈加速器支持的端点的信息，请参阅对可添加为加速器端点的资源的要求。

Global Accelerator 从 Amazon 的 IP 地址池中为您提供静态 IP 地址（除非自带 IP 地址范围到 AWS），然后从该池中指定静态 IP 地址。（有关更多信息，请参阅 在 Global Accelerator 中自带 IP 地址（BYOIP）。）要在控制台上创建加速器，第一步是提示 Global Accelerator 通过输入加速器名称或选择自己的静态 IP 地址来预置静态 IP 地址。要查看加速器创建步骤，请参阅开始使用 AWS Global Accelerator。

即使您禁用加速器且加速器不再接受或路由流量，只要加速器存在，静态 IP 地址仍会分配给该加速器。但是，如果您删除加速器，您将丢失分配给该加速器的静态 IP 地址，因此您无法再使用这些地址路由流量。您可以将 IAM 策略（如基于标签的权限）与 Global Accelerator 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 ABAC 与 Global Accelerator。

Global Accelerator 如何使用运行状况检查

对于标准加速器，AWS Global Accelerator 会自动检查与您的静态 IP 地址关联的端点的运行状况，然后仅将用户流量引导至运行状况良好的端点。

Global Accelerator 包括自动运行的默认运行状况检查，但您可以配置检查的时间设置和其它选项。如果您配置了自定义运行状况检查设置，Global Accelerator 将以特定方式使用这些设置，具体取决于您的配置。您可以在 Global Accelerator 中为 Amazon EC2 实例或弹性 IP 地址端点配置这些设置，也可以在弹性负载均衡控制台上为网络负载均衡器或应用程序负载均衡器配置设置。有关更多信息，请参阅确保加速器的运行状况检查访问权限。

如果您将某个端点添加到标准加速器，该端点必须通过运行状况检查才能被视为运行状况良好，然后流量才会引导至该端点。如果 Global Accelerator 在标准加速器中没有可将流量路由到其中的运行状况良好的端点，则会将请求路由到所有端点。

如何使用流量拨号和端点权重管理流量流向

您可以通过两种方式自定义 AWS Global Accelerator 如何使用标准加速器向端点发送流量：

- 更改流量拨号以限制一个或多个端点组的流量
- 指定权重以更改流向组中端点的流量比例

流量拨号的工作原理

对于标准加速器中的每个端点组，您可以设置流量拨号以控制发送到端点组的流量百分比。该百分比仅适用于已引导至端点组的流量，而不适用于所有侦听器流量。

流量拨号可限制端点组接受的流量部分，表示为引导至该端点组的流量的百分比。例如，如果您将 `us-east-1` 中端点组的流量拨号设置为 50（即 50%），而加速器将 100 个用户请求引导至该端点组，则该组只接受 50 个请求。加速器会将剩余的 50 个请求引导至其它区域的端点组。

有关更多信息，请参阅 使用流量拨号调整流向区域的流量。

权重的工作原理

您可以为标准加速器中的每个端点指定权重，权重是数字，可用于更改加速器路由到每个端点的流量比例。例如，这对于在区域内进行性能测试很有用。

权重是一个值，用于确定加速器引导至端点的流量比例。默认情况下，端点的权重为 128，即权重最大值 255 的一半。

加速器会计算端点组中端点的权重总和，然后根据每个端点的权重与总权重的比率将流量引导至端点。有关权重工作原理的示例，请参阅 如何通过端点权重管理流量。

流量拨号和权重会以不同的方式影响标准加速器对流量的处理方式：

- 您可以为端点组配置流量拨号。通过流量拨号，您可以根据其它因素（例如邻近性）“调低”加速器已经引导至该组的流量，从而降低发送到该组的流量百分比，甚至全部切断流量。
- 另一方面，您可以使用权重为端点组中的各个端点设置值。权重提供了一种在端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端点进行性能测试。

有关流量拨号和权重如何影响失效转移的更多信息，请参阅运行状况不佳的端点的失效转移的工作原理。

ICMP 响应消息和 AWS Global Accelerator

ICMP 响应消息（例如 `ICMP Packet Too Big` 或 `Fragmentation Needed`）有助于确保在互联网上的可用性。AWS Global Accelerator 会在边缘对所有全局 IP 地址的 ICMP 回显消息（ping）做出

响应。这些 ping 不会转发到客户的端点。要借助 Global Accelerator 准确测试性能，请使用更深入的协议进行测试。

以下是 ICMP 如何帮助确保互联网可用性的简短摘要。网络连接的最大传输单位 (MTU) 是能够通过该连接传递的最大可允许数据包的大小（以字节为单位）。连接的 MTU 越大，可在单个数据包中传递的数据越多。路径 MTU 发现（PMTUD）用于确定两台设备之间的路径 MTU。路径 MTU 是原始主机和接收主机之间的路径所支持的最大数据包大小。当两个主机在网络中的 MTU 大小存在差异时，大于 MTU 的数据包将被丢弃，而丢弃了该数据包的接收主机将使用 ICMP 消息通知发送方。有关更多信息，请参阅路径 MTU 发现。

您不能在 Global Accelerator 中阻止加速器上的 ICMP 流量。阻止所有 ICMP 流量也会丢弃 ICMP 消息，例如 `ICMPv6 Packet Too Big (PTB)`（类型 2）和 `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set`（类型 3，代码 4）。这些消息是流量成功返回原始主机所必需的。反过来，这些丢弃的消息会导致 TCP 和基于 Global Accelerator 构建的协议丢弃来自网络上的 MTU 小于典型值的客户端的流量，从而阻止 PMTUD。

请注意，要让 PMTUD 正常工作，端点的安全组还必须允许 ICMP 流量。如果您遇到特定于某些最终用户网络的可用性问题，请确认端点安全组允许 ICMP 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 功能页面上的全球边缘网络。

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《Amazon Web Services 一般参考》中的 AWS IP 地址范围。

在使用 `ip-ranges.json` 文件之前，先查看以下信息：

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

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

- 包含 `"region": "GLOBAL"` 的 Global Accelerator 条目是指分配给加速器的静态 IP 地址。如果您想筛选通过加速器的来自某个区域中的入网点（PoP）的流量，请筛选包含特定地理区域的条目，例如 `us-*` 或 `eu-*`。因此，例如，如果筛选 `us-*`，则只能看到通过美国的 POP 传入的流量。
- Global Accelerator 支持两种路由流量的方式：使用客户端 IP 地址保留或使用网络地址转换（NAT）。流量的路由方式决定了 AWS WAF 可以将规则应用到的客户端 IP 地址。当您使用客户端

IP 地址保留时，AWS WAF 规则以客户端 IP 地址（即访问您的服务的客户端 IP 地址）为目标。使用 NAT 时，AWS WAF 规则将应用于 Global Accelerator 用于路由流量的全局 IP 地址。

了解 AWS Global Accelerator 使用案例

通过使用 AWS Global Accelerator，可帮助您实现各种目标。本节列出了一些使用案例，让您了解如何使用 Global Accelerator 满足您的需求。

扩展以提高应用程序利用率

随着应用程序使用量的增长，您需要管理的 IP 地址和端点数量也会增加。Global Accelerator 使您可以扩展或缩减网络。借助 Global Accelerator，您可以将区域资源（例如负载均衡器和 Amazon EC2 实例）关联到两个静态 IPv4 地址，或者对于双堆栈，则关联到两个静态 IPv4 地址和两个 IPv6 地址。您只需在客户端应用程序、防火墙和 DNS 记录中将这些地址列入允许列表一次。借助 Global Accelerator，您无需更新客户端应用程序中的 IP 地址，即可在 AWS 区域中添加或移除端点、运行蓝/绿部署以及进行 A/B 测试。这对于物联网、零售、媒体、汽车和医疗保健使用案例特别有用，在这些使用案例中，您无法轻松地频繁更新客户端应用程序。

延迟敏感型应用程序的加速

许多应用程序，尤其是在游戏、媒体、移动应用程序、广告技术和金融等领域，需要非常低的延迟才能实现出色的用户体验。为了改善用户体验，Global Accelerator 会将用户流量引导至离客户端最近的应用程序端点，从而减少互联网延迟和抖动。Global Accelerator 使用任播将流量路由到最近的边缘站点，然后通过 AWS 全球网络将其路由到最近的区域端点。Global Accelerator 可以对网络性能的变化做出快速反应，从而提高用户的应用程序性能。

灾难恢复和多区域弹性

必须能够依靠网络才可用。为了支持灾难恢复、更高的可用性、更低的延迟或合规性，您可能会在多个 AWS 区域运行应用程序。如果 Global Accelerator 检测到应用程序端点在主 AWS 区域出现故障，则会立即触发流量重新路由到下一个可用的、最近的 AWS 区域中的应用程序端点。

要详细了解 Global Accelerator 如何从本质上以及使用该服务的应用程序中支持弹性，请阅读以下博客文章：Maximising application resiliency with AWS Global Accelerator。

保护应用程序

将 AWS 源（例如应用程序负载均衡器或 Amazon EC2 实例）向公共互联网流量公开，将会为恶意攻击创造机会。Global Accelerator 将源隐藏在两个静态入口点后面，从而降低攻击风险。默认情况下，使用 AWS Shield 保护这些入口点免受分布式拒绝服务（DDoS）攻击。Global Accelerator 使

用私有 IP 地址与 Amazon Virtual Private Cloud 创建对等连接，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 Global Accelerator 的性能优势用于 VoIP 或游戏应用程序。例如，您可以将 Global Accelerator 用于为单个游戏会话分配多个玩家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端点的应用程序（例如多人游戏或 VoIP 通话），可使用 Global Accelerator 在全球范围内减少延迟和抖动。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，同时保留对将哪个客户端引导至哪个 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 速度比较工具来查看 AWS 区域中 Global Accelerator 的下载速度与互联网直接下载速度的对比。使用此工具，您可以使用浏览器查看通过 Global Accelerator 传输数据时的性能差异。您可以选择要下载的文件大小，然后该工具通过 HTTPS/TCP 将文件从不同区域的应用程序负载均衡器下载到浏览器。对于每个区域，您会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**
>
> 多次运行测试时，结果可能会有所不同。下载时间可能会因 Global Accelerator 之外的因素而异，例如您正在使用的最后一英里网络中的连接的质量、容量和距离。

如何开始使用 AWS Global Accelerator

您可以使用 API 或 AWS Global Accelerator 控制台来开始设置 AWS Global Accelerator。由于 Global Accelerator 是一项全球服务，因此它与特定 AWS 区域无关。请注意，Global Accelerator 是一项全球服务，支持多个 AWS 区域中的端点，但您必须指定美国西部（俄勒冈州）区域才能创建或更新加速器。

要开始使用 Global Accelerator，请按照以下一般步骤操作：

1. 选择要创建的加速器类型：标准加速器或自定义路由加速器。

2. 配置 Global Accelerator 的初始设置：提供加速器的名称，然后选择加速器的类型和地址类型。
3. 为加速器配置一个或多个侦听器：侦听器根据您指定的协议和端口（或端口范围）处理来自客户端的入站连接。
4. 为加速器配置区域端点组：您可以选择一个或多个区域端点组，以添加到侦听器中。侦听器会将请求路由到已添加到端点组的端点。

   对于标准加速器，Global Accelerator 使用为每个端点定义的运行状况检查设置来监控组内端点的运行状况。对于标准加速器中的每个端点组，您可以配置一个流量拨号百分比来控制端点组将接受的流量百分比。该百分比仅适用于已引导至端点组的流量，而不适用于所有侦听器流量。默认情况下，所有区域端点组的流量拨号设置为 100%。

   对于自定义路由加速器，根据接收流量的侦听器端口，将流量确定性地路由到 VPC 子网中的特定目标。
5. 向端点组添加端点：您添加的端点取决于加速器的类型。
   - 对于标准加速器，您可以向每个端点组添加一个或多个区域资源，例如负载均衡器或 EC2 实例端点。接下来，您可以通过设置端点权重来决定要将多少流量路由到每个端点。
   - 对于自定义路由加速器，您可以添加一个或多个 Amazon VPC（VPC）子网，其中包含多达数千个 Amazon EC2 实例目标。

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，请参阅开始使用 AWS Global Accelerator。要使用 API 操作，请参阅 AWS Global Accelerator 的常见 API 操作和 AWS Global Accelerator API 参考。

在 AWS Global Accelerator 中添加标签

标签是用于标识和组织 AWS 资源的词语或短语（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，键可能是 `environment`，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，您可以为加速器添加标签。

以下是两个示例，说明在 Global Accelerator 中使用标签的用途：

- 使用标签跟踪不同类别的账单信息。要执行此操作，请将标签应用于加速器或其它 AWS 资源（例如网络负载均衡器、应用程序负载均衡器或 Amazon EC2 实例）并激活标签。然后，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量和成本。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 Billing 用户指南》中的使用成本分配标签。

- 使用标签为加速器执行基于标签的权限。要执行此操作，请创建指定标签和标签值的 IAM 策略，以允许或禁止操作。有关更多信息，请参阅 ABAC 与 Global Accelerator。

有关标记的使用惯例和指向其它资源的链接，请参阅《AWS 一般参考》中的为 AWS 资源添加标签。有关使用标签的提示，请参阅 AWS 白皮书博客中的标记最佳实践：AWS 资源标记策略。

有关可为 Global Accelerator 中的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。本章包括在控制台中使用标记的步骤。有关通过 AWS CLI 和 Global Accelerator API 使用标签的更多信息（包括 CLI 示例），请参阅 AWS Global Accelerator API 参考中的以下操作：

- CreateAccelerator
- CreateCrossAccountAttachment
- TagResource
- UntagResource
- ListTagsForResource

Global Accelerator 中的标记支持

AWS Global Accelerator 支持为加速器和跨账户附件添加标签。

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

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。

您可以通过 AWS 控制台、CLI 或 Global Accelerator API 操作添加或移除标签。有关更多信息（包括 CLI 示例），请参阅 AWS Global Accelerator API 参考中的 TagResource。

在 Global Accelerator 中添加、编辑或删除标签的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 选择要为其添加或更新标签的加速器。
3. 在标签部分中，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、值或两者的文本。您也可以清除标签的值，但键是必需的。

删除标签

选择值字段右侧的移除。

4. 选择 Save changes（保存更改）。

AWS Global Accelerator 定价

借助 AWS Global Accelerator，您需要为账户中配置的每个加速器（无论是启用还是禁用）收取固定的小时费用，除了标准数据传输费率外，还需要为流经加速器的主要方向的每小时流量收取增量费用。增量速率取决于负责处理请求的 AWS 区域（源）和响应被引导至的 AWS 边缘站点（目标）。客户通常会为每个应用程序创建一个加速器，但是拥有复杂应用程序的客户可能需要更多的加速器。

有关定价的详细信息、按来源和目标区域定价的信息以及定价示例，请参阅 AWS Global Accelerator 定价。

开始使用 AWS Global Accelerator

为了帮助您开始使用 AWS Global Accelerator，本章提供了关于设置标准加速器和自定义路由加速器的教程。

要详细了解可以在 Global Accelerator 中创建的两种类型的加速器，请参阅在 AWS Global Accelerator 中使用标准加速器和在 AWS Global Accelerator 中使用自定义路由加速器。

教程中提供了使用 AWS Management Console 的主要步骤。请注意，在设置自定义路由加速器时，某些配置步骤必须使用 API。

> **Tip**
>
> 如果想要了解如何使用 Global Accelerator 来提高 Web 应用程序的性能和可用性，请查看以下自定进度的讲习会：AWS Global Accelerator 讲习会。

此外，您还可以将 Global Accelerator API 操作与 AWS Command Line Interface（AWS CLI）或 AWS SDK 结合使用，来创建和自定义您的加速器。以下是使用 Global Accelerator API 的资源。

- 有关 API 操作的列表，请参阅AWS Global Accelerator 的常见 API 操作。
- 有关使用 AWS Global Accelerator API 操作的详细信息，请参阅《AWS Global Accelerator API 参考》https://docs.aws.amazon.com/global-accelerator/latest/api/Welcome.html。

Global Accelerator 是一项全球服务，支持多个 AWS 区域的端点。支持的区域已在 AWS 区域表中列出。

内容

- 开始使用标准加速器
- 开始使用自定义路由加速器

开始使用标准加速器

本节将介绍创建标准加速器的步骤，该加速器可将流量路由至最佳端点。

任务

- 开始前的准备工作
- 第 1 步：创建标准加速器
- 第 2 步：添加侦听器
- 第 3 步：添加端点组
- 第 4 步：添加端点
- 第 5 步：测试加速器
- 第 6 步（可选）：删除加速器

开始前的准备工作

在创建加速器之前，请至少创建一个资源，您可以将其添加为端点来引导流量。例如，创建以下资源之一：

- 至少启动一个 Amazon EC2 实例，以将其添加为端点。有关更多信息，请参阅《Amazon EC2 用户指南》中的创建您的 EC2 资源并启动您的 EC2 实例。
- 或者，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《网络负载均衡器用户指南》中的创建网络负载均衡器。

创建资源以添加到 Global Accelerator 时，请注意以下事项：

- 在 Global Accelerator 中添加内部应用程序负载均衡器或 EC2 实例端点时，您可以通过将互联网流量定位到私有子网中，让互联网流量直接流入虚拟私有云（VPC）中的端点或从这些端点中流出。包含负载均衡器或 EC2 实例的 VPC 必须附带互联网网关，以表示 VPC 接受互联网流量。有关更多信息，请参阅 AWS Global Accelerator 中的安全 VPC 连接。
- Global Accelerator 要求路由器和防火墙规则允许来自与 Amazon 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 地址端点的运行状况检查。要查看与 Route 53 运行状况检查程序关联的 IP 地址范围的信息，请参阅《Amazon Route 53 开发者指南》中的 Amazon Route 53 服务器的 IP 地址范围。

第 1 步：创建标准加速器

创建标准加速器时，可以选择 IPv4 或双堆栈作为 Global Accelerator 分配给加速器的静态 IP 地址。双堆栈同时支持 IPv4 和 IPv6 IP 地址。

要创建加速器，请执行以下操作

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 选择创建加速器。
3. 提供加速器的名称。
4. 对于加速器类型，选择标准。
5. 对于 IP 地址类型，选择 IPv4 或双堆栈。
6. 或者，添加一个或多个标签来帮助您识别 Global Accelerator 资源。
7. 选择下一步。

第 2 步：添加侦听器

创建一个侦听器，处理从用户到加速器的入站连接。

要创建侦听器，请执行以下操作

1. 在添加侦听器页面上，输入要与侦听器关联的端口或端口范围。侦听器支持端口 1-65535。
2. 为您输入的端口选择一个或多个协议。
3. 或者，选择以启用客户端亲和性。侦听器的客户端亲和性是指 Global Accelerator 可确保来自特定来源（客户端）IP 地址的连接始终路由到同一端点。要启用此行为，请在下拉列表中选择源 IP。

   默认值为无，这表示未启用客户端亲和性，Global Accelerator 会在侦听器端点组中的端点之间平均分配流量。

   有关更多信息，请参阅 Global Accelerator 中客户端亲和性的工作原理。
4. 或者，选择添加侦听器，以添加其它侦听器。
5. 添加完标签后，选择下一步。

第 3 步：添加端点组

添加一个或多个端点组，每个端点组都与特定 AWS 区域相关联。

要添加端点组，请执行以下操作

1. 在添加端点组页面的侦听器部分，从下拉列表中选择一个区域。

2. 或者，在流量拨号中，输入 0 到 100 之间的数字，以设置此端点组的流量百分比。该百分比仅适用于已引导到此端点组的流量，而不适用于所有侦听器流量。默认情况下，端点组的流量拨盘设置为 100（即 100%）。
3. 或者，在自定义运行状况检查值中，选择配置运行状况检查。配置运行状况检查设置时，Global Accelerator 会使用这些设置对 EC2 实例和弹性 IP 地址端点进行运行状况检查。对于网络负载均衡器和应用程序负载均衡器端点，Global Accelerator 会使用您已经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 确保加速器的运行状况检查访问权限。
4. 或者，选择添加端点组，为此侦听器或其它侦听器添加更多端点组。
5. 选择下一步。

第 4 步：添加端点

添加一个或多个与特定端点组关联的端点。此步骤并非必需步骤，但除非端点包含在某个端点组中，否则不会将流量引导到区域中的端点。

要添加端点，请执行以下操作

1. 在创建端点页面的端点部分中，选择一个端点。
2. 或者，在权重中，输入 0 到 255 之间的数字，以设置将流量路由到此端点的权重。向端点添加权重时，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，所有端点的权重均为 128。有关更多信息，请参阅 如何通过端点权重管理流量。
3. 或者，在保留客户端 IP 地址下，选择保留地址。（对于某些端点类型，已选中此选项且无法清除。）有关更多信息，请参阅 在 AWS Global Accelerator 中保留客户端 IP 地址。
4. 或者，选择添加端点，以添加更多端点。
5. 选择下一步。

选择下一步后，Global Accelerator 控制面板上会显示一条消息，提示您的加速器正在进行中。该过程完成后，控制面板中的加速器状态会显示为活动。

第 5 步：测试加速器

按步骤测试您的加速器，以确保将流量引导到您的端点。例如，运行如下所示的 curl 命令，替换您加速器的一个静态 IP 地址，即可显示处理请求的 AWS 区域。这对于为端点设置不同的权重或调整端点组的流量拨盘非常有用。

运行如下所示的 curl 命令，替换您加速器的一个静态 IP 地址，即可调用 IP 地址 100 次，然后输出处理每个请求的位置的计数。

```
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的流量拨盘，则此命令可以帮助您确认您的加速器是否将正确百分比的流量引导到不同的组。有关更多信息，请参阅博客文章 Traffic management with AWS Global Accelerator 中的详细示例。

第 6 步（可选）：删除加速器

如果您创建加速器是为了进行测试，或者不再需要使用某个加速器，则可以将其删除。在控制台上，禁用该加速器，然后即可将其删除。您不必从该加速器中移除侦听器和端点组。

要使用 API 操作（而不是控制台）删除加速器，必须先移除与加速器关联的所有侦听器和端点组，并将其禁用。有关更多信息，请参阅《AWS Global Accelerator API 参考》中的删除加速器操作。

移除端点或端点组或删除加速器时，请注意以下事项：

- 创建加速器时，Global Accelerator 会为您提供一组两个静态 IP 地址。即使禁用加速器且加速器不再接受或路由流量，只要加速器存在，IP 地址就会分配给该加速器。但是，当您删除加速器时，您将丢失分配给该加速器的静态 IP 地址，因此您无法再使用这些地址路由流量。最佳实践是，确保您拥有适当的权限，以免无意中删除加速器。您可以将 IAM 策略（例如基于标签的权限）与 Global Accelerator 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 ABAC 与 Global Accelerator。
- 如果您在将 EC2 实例从 Global Accelerator 的端点组中移除之前将其终止，然后创建了使用同一 IP 地址的另一个实例，并且通过了运行状况检查，则 Global Accelerator 会将流量路由至新的端点。如果您不希望发生这种情况，请先从端点组中移除该 EC2 实例，然后再将其终止。

要删除加速器，请执行以下操作

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 选择要删除的加速器。
3. 选择编辑。
4. 选择禁用加速器，然后选择保存。

5. 选择要删除的加速器。
6. 选择删除加速器。
7. 在确认对话框中，选择删除。

开始使用自定义路由加速器

本节介绍了创建自定义路由加速器的步骤，该加速器将流量确定性地路由至虚拟私有云（VPC）子网端点中的 Amazon EC2 实例目标。

任务

- 开始前的准备工作
- 第 1 步：创建自定义路由加速器
- 第 2 步：添加侦听器
- 第 3 步：添加端点组
- 第 4 步：添加端点
- 第 5 步（可选）：删除加速器

开始前的准备工作

在创建自定义路由加速器之前，先创建一个资源，您可以将其添加为端点以将流量引导到该端点。自定义路由加速器端点必须是虚拟私有云（VPC）子网，其中可以包含多个 Amazon EC2 实例。有关创建这些资源的说明，请参阅以下内容：

- 创建一个 VPC 子网。有关更多信息，请参阅《AWS Directory Service 管理指南》中的创建和配置您的 VPC。
- 或者，在您的 VPC 中启动一个或多个 Amazon EC2 实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的创建您的 EC2 资源并启动您的 EC2 实例。

创建资源以添加到 Global Accelerator 时，请注意以下事项：

- 您在 Global Accelerator 中添加 EC2 实例端点时，可以通过将互联网流量定位到私有子网中，让互联网流量直接流入 VPC 中的端点和从 VPC 中的端点流出。包含 EC2 实例的 VPC 必须连接互联网网关，以表示 VPC 接收互联网流量。有关更多信息，请参阅 AWS Global Accelerator 中的安全 VPC 连接。

在创建自定义路由加速器之前，请确保查看自定义路由加速器的准则和限制中描述的最佳实践。

第 1 步：创建自定义路由加速器

要创建加速器，请执行以下操作

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 提供加速器的名称。
3. 对于加速器类型，请选择自定义路由。
4. 或者，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、端点组和 VPC 子网端点。

第 2 步：添加侦听器

创建一个侦听器，处理从用户到加速器的入站连接。

您在创建侦听器时指定的范围定义了您可以在自定义路由加速器中使用的侦听器端口和目标 IP 地址组合的数量。为了最大限度地提高灵活性，建议您指定较大的端口范围。您指定的每个侦听器端口范围必须包含至少 16 个端口。

要创建侦听器，请执行以下操作

1. 在添加侦听器页面上，输入要与侦听器关联的端口或端口范围。侦听器支持端口 1-65535。
2. 为您输入的端口选择一个或多个协议。
3. 或者，选择添加侦听器，以添加其它侦听器。
4. 添加完标签后，选择下一步。

第 3 步：添加端点组

添加一个或多个端点组，每个端点组都与特定 AWS 区域相关联。为每个端点组指定一组或多组端口范围和协议。Global Accelerator 使用这些端口将流量引导到区域子网中的 Amazon EC2 实例。

对于您提供的每个端口范围，您还要指定要使用的协议：UDP、TCP 或同时指定 UDP 和 TCP。

要添加端点组，请执行以下操作

1. 在添加端点组页面的侦听器部分，选择一个区域。

2. 对于端口和协议集，输入 Amazon EC2 实例的端口范围和协议。

   - 输入起始端口和目标端口，以指定端口范围。
   - 对于每个端口范围，为该范围指定一个或多个协议。

   端口范围不必是侦听器端口范围的子集，但侦听器端口范围中的端口总数必须足以支持您指定的端口总数。

3. 选择保存。
4. 或者，选择添加端点组，为此侦听器或其它侦听器添加更多端点组。
5. 选择下一步。

第 4 步：添加 VPC 子网端点

为该区域端点组添加一个或多个虚拟私有云（VPC）子网端点。自定义路由加速器的端点定义了可以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 子网端点时，Global Accelerator 会生成新的端口映射，您可以使用这些映射将流量路由至子网中的目标 EC2 实例 IP 地址。然后，您可以使用 Global Accelerator API 获取子网所有端口映射的静态列表，并使用该映射确定性地将流量引导到特定 EC2 实例。

要添加端点，请执行以下操作

1. 在添加端点页面上，在要向其添加端点的端点组部分，为端点选择子网 ID。
2. 或者，执行以下操作之一以启用流向子网中 EC2 实例目标的流量：

   - 要允许将流量引导到子网上的所有 EC2 端点和端口，请选择允许所有流量。
   - 要允许流量流向子网上的特定 EC2 端点和端口，请选择允许流量流向特定的目标套接字地址。然后指定允许的 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，不允许流量流向子网端点。如果您不选择允许流量的选项，则流向子网中所有目标的流量都将被拒绝。

> **Note**
>
> 如果您想允许流量流向子网中的特定 EC2 实例和端口，可以通过编程方式实现。有关更多信息，请参阅《AWS Global Accelerator API 参考》中的AllowCustomRoutingTraffic

3. 选择下一步。

选择下一步后，Global Accelerator 控制面板上会显示一条消息，提示您的加速器正在进行中。该过程完成后，控制面板中的加速器状态会显示为活动。

第 5 步（可选）：删除加速器

如果您创建加速器是为了进行测试，或者不再需要使用某个加速器，则可以将其删除。在控制台上，禁用该加速器，然后即可将其删除。您不必从该加速器中移除侦听器和端点组。

要使用 API 操作（而不是控制台）删除加速器，必须先移除与加速器关联的所有侦听器和端点组，并将其禁用。有关更多信息，请参阅《AWS Global Accelerator API 参考》中的 DeleteCustomRoutingAccelerator 操作。

删除加速器时，请注意以下事项：

- 创建加速器时，Global Accelerator 会为您提供一组两个静态 IP 地址。即使禁用加速器且加速器不再接受或路由流量，只要加速器存在，IP 地址就会分配给该加速器。但是，当您删除加速器时，您将丢失分配给该加速器的静态 IP 地址，因此您无法再使用这些地址路由流量。最佳实践是，确保您拥有适当的权限，以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 Global Accelerator 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 ABAC 与 Global Accelerator。

要删除加速器，请执行以下操作

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 选择要删除的加速器。
3. 选择编辑。
4. 选择禁用加速器，然后选择保存。
5. 选择要删除的加速器。

6. 选择删除加速器。
7. 在确认对话框中，选择删除。

AWS Global Accelerator 的常见 API 操作

本节列出了可用于 Global Accelerator 资源的常见 AWS Global Accelerator 操作，以及相关文档的链接。

用于标准加速器的操作

下表列出了可用于标准加速器的常见 Global Accelerator 操作以及相关文档的链接。

操作	使用 Global Accelerator 控制台	使用 Global Accelerator API
创建标准加速器	请参阅 开始使用标准加速器。	请参阅 CreateAccelerator
为标准加速器创建侦听器	请参阅 AWS Global Accelerator 中的标准加速器的侦听器。	请参阅 CreateListener
为标准加速器创建端点组	请参阅 AWS Global Accelerator 中的标准加速器的端点组。	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
更新端点组	请参阅 添加标准端点组。	请参阅 UpdateEndpointGroup
添加端点	请参阅 添加标准端点。	请参阅 AddEndpoints
移除端点	请参阅 添加标准端点。	请参阅 RemoveEndpoints
列出标准加速器	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 创建加速器。	请参阅 DeleteAccelerator

用于自定义路由加速器的操作

下表列出了用于自定义路由加速器的常见 Global Accelerator 操作以及相关文档的链接。

操作	使用 Global Accelerator 控制台	使用 Global Accelerator API
创建自定义路由加速器	请参阅 开始使用自定义路由加速器。	请参阅 CreateCustomRoutingAccelerator
为自定义路由加速器创建侦听器	请参阅 Global Accelerator 中自定义路由加速器的侦听器。	请参阅 CreateCustomRoutingListener
为自定义路由加速器创建端点组	请参阅 Global Accelerator 中的自定义路由加速器端点组。	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 在 Global Celerator 中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 在 Global Celerator 中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 在 Global Celerator 中创建自定义路由加速器。	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 。
在自定义路由加速器中允许子网的所有目标流量	请参阅 添加自定义路由加速器的 VPC 子网端点。	请参阅 AllowCustomRoutingTraffic

操作	使用 Global Accelerator 控制台	使用 Global Accelerator API
在自定义路由加速器中拒绝子网的所有目标流量	请参阅 添加自定义路由加速器的 VPC 子网端点。	请参阅 DenyCustomRoutingTraffic
在自定义路由加速器中允许流向特定目标的流量	请参阅 添加自定义路由加速器的 VPC 子网端点。	请参阅 AllowCustomRoutingTraffic
在自定义路由加速器中拒绝流向特定目标的流量	请参阅 添加自定义路由加速器的 VPC 子网端点。	请参阅 DenyCustomRoutingTraffic

在 Global Accelerator 中用于跨账户支持的操作

下表列出了在 Global Accelerator 中可用于跨账户支持的常见 Global Accelerator 操作以及相关文档的链接。

操作	使用 Global Accelerator 控制台	使用 Global Accelerator API
创建跨账户附件	请参阅 在 AWS Global Accelerator 中创建跨账户附件。	请参阅 CreateCrossAccountAttachment
删除跨账户附件	请参阅 在 AWS Global Accelerator 中创建跨账户附件。	请参阅 DeleteCrossAccountAttachment
描述跨账户附件中的信息	请参阅 在 Global Accelerator 中识别跨账户资源。	请参阅 DescribeCrossAccountAttachment
列出账户的跨账户附件	请参阅 在 Global Accelerator 中识别跨账户资源。	请参阅 ListCrossAccountAttachments
更新跨账户附件	请参阅 在 AWS Global Accelerator 中创建跨账户附件。	请参阅 UpdateCrossAccountAttachment

在 AWS Global Accelerator 中使用标准加速器

本章包含在 AWS Global Accelerator 中创建标准加速器的步骤和建议，包括配置加速器、侦听器、端点组和端点。借助标准加速器，Global Accelerator 会为流量选择最近的运行状况良好的端点。

如果您想改用自定义应用程序逻辑将一个或多个用户引导至多个端点中的特定端点，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. 创建一个加速器，然后选择标准加速器选项。
2. 对于地址类型，选择 IPv4 或双堆栈。
3. 或者，使用自带 IP 地址来配置静态 IP 地址。
4. 添加具有一组特定端口或端口范围的侦听器，然后选择要接受的协议：TCP 或 UDP。
5. 添加一个或多个端点组，每个具有端点资源的 AWS 区域对应一个端点组。
6. 向端点组中添加一个或多个端点。这不是必需的，但是如果您没有任何端点，则流量不会进行路由。要了解端点的类型和要求，请参阅???。

以下各节提供了添加、删除和配置标准加速器及其组件（包括侦听器、端点组和端点）的步骤。

主题

- AWS Global Accelerator 中的标准加速器
- AWS Global Accelerator 中的标准加速器的侦听器
- AWS Global Accelerator 中的标准加速器的端点组
- AWS Global Accelerator 中的标准加速器的端点

AWS Global Accelerator 中的标准加速器

AWS Global Accelerator 中的标准加速器通过 AWS 全球网络将流量引导至指定的 AWS 区域中包含的端点。每个加速器包含一个或多个侦听器。根据您配置的协议和端口（或端口范围），侦听器可处理从客户端到 Global Accelerator 的入站连接。

对于标准加速器，Global Accelerator 会根据运行状况、客户端位置和您配置的策略将流量引导至最佳的区域端点，从而提高应用程序的可用性。标准加速器的端点可以是位于一个 AWS 区域或多个区域的网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址。

> **Important**
>
> 默认情况下，Global Accelerator 为您提供与加速器关联的静态 IP 地址。这些 IP 地址会在加速器存在期间持续分配给您，即使您将加速器禁用并且它不再接受或路由流量也是如此。但是，如果您删除某个加速器，您将丢失分配给该加速器的 Global Accelerator 静态 IP 地址，因此您无法再使用这些地址路由流量。最佳实践是，确保您拥有适当的权限，以免无意中删除加速器。您可以将 IAM 策略（例如基于标签的权限）与 Global Accelerator 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 ABAC 与 Global Accelerator。

本节包括在 Global Accelerator 控制台上使用标准加速器的操作步骤。要将 API 操作与 Global Accelerator 结合使用，请参阅 AWS Global Accelerator API 参考。

内容

- 创建加速器
- 更新加速器
- 删除加速器
- 查看您的加速器
- 创建负载均衡器时添加加速器
- 对使用全局静态 IP 地址与区域静态 IP 地址进行比较

创建加速器

本节介绍如何在控制台上创建标准加速器。要以编程方式使用 Global Accelerator，请参阅 AWS Global Accelerator API 参考。

创建标准加速器的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 选择创建加速器。
3. 提供加速器的名称。
4. 对于加速器类型，选择标准。
5. 对于 IP 地址类型，选择 IPv4 或双堆栈。

6. 或者，如果您将自己的 IP 地址范围引入到 AWS（BYOIP），则可以为加速器指定静态 IP 地址：从每个地址池中指定一个。针对加速器的两个静态 IP 地址中的每一个做出此选择。

   - 对于每个静态 IP 地址，选择要使用的 IP 地址池。

     > **Note**
     >
     > 必须为每个静态 IP 地址选择一个独立的 IP 地址池。之所以存在这种限制，是因为为了实现高可用性，Global Accelerator 会将每个地址范围分配给不同的网络区域。

   - 如果您选择自己的 IP 地址池，则还要从池中选择特定的 IP 地址。如果您选择默认 Amazon IP 地址池，则 Global Accelerator 会为您的加速器分配特定的 IP 地址。

   有关使用 BYOIP 指定或更新静态 IP 地址的要求的更多信息，请参阅更新加速器以更改 IP 地址时的要求。

7. 或者，添加一个或多个标签来帮助您识别加速器资源。
8. 选择下一步添加侦听器、端点组和端点。

更新加速器

本节介绍如何在控制台中更新标准加速器。要以编程方式使用 Global Accelerator，请参阅 AWS Global Accelerator API 参考。

更新标准加速器的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器列表中，选择一个加速器，然后选择编辑。
3. 在编辑加速器页面上，进行如下更改：

   - 更改加速器的名称。
   - 禁用加速器，使其不再接受或路由流量，或者您可以将其删除。
   - 启用加速器（如果已禁用）。
   - 更新 IP 地址类型。如果已设置为 IPv4，请将其更改为双堆栈。或者，如果是双堆栈，请将其更改为 IPv4。
   - 更新标签。

4. 选择 Save changes（保存更改）。

如果您禁用加速器，请注意以下几点：

- 即使您禁用加速器且加速器不再接受或路由流量，Global Accelerator 静态 IP 地址仍会分配给该加速器。只要加速器存在，加速器就会保留相同的静态 IP 地址。
- 但是，如果您删除加速器，则会丢失分配给该加速器的 Global Accelerator 静态 IP 地址。届时，您无法再使用这些地址来路由流量。

如果您更改 IP 地址类型，请注意以下几点：

- 只能将具有双堆栈端点的加速器更改为双堆栈类型的 IP 地址。
- 如果将加速器的 IP 地址类型从双堆栈更改为 IPv4，则 Global Accelerator 会保存分配给加速器的 IPv6 IP 地址。这意味着，如果将加速器的 IP 地址类型重新改为双堆栈，则会恢复加速器的原始 IPv6 静态 IP 地址。

如果您想更改加速器的其它功能，例如添加或移除端点、更新流量拨号或调整端点权重，请参阅涵盖这些主题的特定部分，如下所示：

- 添加标准侦听器
- 添加标准端点组
- 添加标准端点

删除加速器

如果您创建加速器是为了进行测试，或者不再需要使用某个加速器，则可以将其删除。在控制台上，禁用该加速器，然后即可将其删除。您不必从该加速器中移除侦听器和端点组。

要使用 API 操作（而不是控制台）删除某个加速器，必须先移除与该加速器关联的所有侦听器和端点组，然后将其禁用。有关更多信息，请参阅《AWS Global Accelerator API 参考》中的 DeleteAccelerator 操作。

禁用加速器的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。

2. 在列表中，选择要禁用的加速器。
3. 选择编辑。
4. 选择禁用加速器，然后选择保存。

要删除加速器，请执行以下操作

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在列表中，选择要删除的加速器。
3. 选择删除。

> **Note**
> 如果尚未禁用加速器，则无法删除。

4. 在确认对话框中，选择删除。

> **Important**
> 如果您删除某个加速器，您将丢失分配给该加速器的静态 IP 地址，因此您无法再使用这些地址路由流量。

查看您的加速器

您可以在控制台上查看加速器相关信息。要以编程方式查看加速器描述，请参阅 AWS Global Accelerator API 参考中的 ListAccelerators 和 DescribeAccelerator。

查看加速器相关信息的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
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。

创建负载均衡器时添加加速器

在 AWS Management Console中创建应用程序负载均衡器或网络负载均衡器时，可以选择同时添加加速器。Elastic Load Balancing 和 Global Accelerator 协同工作，透明地为您添加加速器。加速器是在您的账户中创建的，负载均衡器作为端点。使用加速器可提供静态 IP 地址，并可提高应用程序的可用性和性能。（要了解有关加速器的更多信息，请参阅什么是 AWS Global Accelerator？。）

> **Important**
>
> 您必须拥有适当的权限，才能创建加速器。有关更多信息，请参阅 AWS Global Accelerator 的基于身份的策略示例。

配置和查看加速器

您必须更新 DNS 配置，才能将流量定向至加速器的静态 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到达负载均衡器。

通过在 Amazon EC2 控制台上选择 Global Accelerator 插件创建负载均衡器后，转到集成服务选项卡，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，通过 AWS 全球网络开始将用户流量路由到负载均衡器。有关为加速器分配的 DNS 名称的更多信息，请参阅 AWS Global Accelerator 中的 DNS 寻址和自定义域。

在 AWS Management Console中，您可以通过导航至 Global Accelerator 来查看和配置加速器。例如，您可以查看与账户关联的加速器，也可以向加速器中添加其它负载均衡器。有关更多信息，请参阅查看您的加速器 和 创建加速器。

定价

使用 AWS Global Accelerator，您可以按实际用量付费。您需要按小时为账户中的每个加速器付费，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

如果不想继续通过 Global Accelerator 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 添加标准端点中的移除端点。

3. 删除加速器。有关更多信息，请参阅 删除加速器。

对使用全局静态 IP 地址与区域静态 IP 地址进行比较

如果您想在 AWS 资源（例如 Amazon EC2 实例）前使用静态 IP 地址，则有多种选择。例如，您可以分配弹性 IP 地址，这是静态 IPv4 或 IPv6 地址，您可以将其与单个 AWS 区域中的 Amazon EC2 实例或网络接口相关联。

如果您的受众遍布全球，则可以使用 Global Accelerator 创建加速器，以获取从世界各地的 AWS 边缘站点公布的全局静态地址。对于 IPv4，Global Accelerator 提供两个全局静态 IPv4 地址。对于双堆栈，Global Accelerator 提供总计四个全局静态 IP 地址：两个 IPv4 地址和两个 IPv6 地址。如果您已经在一个或多个区域为应用程序设置了 AWS 资源，包括 Amazon EC2 实例、网络负载均衡器和应用程序负载均衡器，则可以轻松地将这些资源添加到 Global Accelerator，以便使用全局静态 IP 地址作为这些资源的前端入口。有关更多信息，请参阅 对可添加为加速器端点的资源的要求。

选择使用由 Global Accelerator 预置的全局静态 IP 地址还可以提高应用程序的可用性和性能。借助 Global Accelerator，静态 IP 地址可以接受从离用户最近的边缘站点进入 AWS 全球网络的传入流量。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 的工作原理 。

您可以通过 AWS Management Console添加加速器，也可以使用 API 操作及 AWS CLI 或 SDK 添加加速器。有关更多信息，请参阅 创建加速器。

添加加速器时应注意以下几点：

- 即使禁用加速器且加速器不再接受或路由流量，只要加速器存在，由 Global Accelerator 预置的全局静态 IP 地址就会一直分配给您。但是，如果您删除加速器，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 Global Accelerator，您只需按实际用量付费。您需要按小时为账户中的每个加速器付费，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 中的标准加速器的侦听器

使用 AWS Global Accelerator，您可以添加侦听器，这些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 和 UDP 协议。

您可在创建标准加速器时定义标准侦听器，并可随时添加更多侦听器。您可将每个侦听器与一个或多个端点组相关联，并将每个端点组与一个 AWS 区域相关联。

或者，您可以为侦听器配置客户端亲和性。借助客户端亲和性，Global Accelerator 将来自特定来源（客户端）IP 地址的用户的所有请求引导至相同的端点资源。选择此选项可保持用户的客户端亲和性。

内容

- 添加标准侦听器
- 编辑标准侦听器
- 移除标准侦听器
- Global Accelerator 中客户端亲和性的工作原理

添加标准侦听器

本节可提供在 AWS Global Accelerator 控制台上创建标准侦听器的步骤。要使用 API 操作（而不是控制台）来完成此任务，请参阅 AWS Global Accelerator API 参考中的 `CreateListener`。

添加侦听器

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个加速器。
3. 选择添加侦听器。
4. 在添加侦听器页面上，输入要与侦听器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. 或者，选择以启用客户端亲和性。侦听器的客户端亲和性是指 Global Accelerator 可确保来自特定来源（客户端）IP 地址的连接始终路由到同一端点。要启用此行为，请在下拉列表中选择源 IP。

   默认值为无，这表示未启用客户端亲和性，Global Accelerator 会在侦听器的端点组中的端点之间平均分配流量。

   有关更多信息，请参阅 Global Accelerator 中客户端亲和性的工作原理。
7. 选择添加侦听器。

编辑标准侦听器

本节提供在 AWS Global Accelerator 控制台上编辑标准侦听器的步骤。要使用 API 操作（而不是控制台）来完成此任务，请参阅 AWS Global Accelerator API 参考中的 `UpdateListener`。

编辑标准侦听器的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个加速器。
3. 选择一个侦听器，然后选择编辑侦听器。
4. 在编辑侦听器页面上，更改要与侦听器关联的端口、端口范围或协议。
5. 或者，选择以启用客户端亲和性。侦听器的客户端亲和性是指 Global Accelerator 可确保来自特定来源（客户端）IP 地址的连接始终路由到同一端点。要启用此行为，请在下拉列表中选择源 IP。

   默认值为无，这表示未启用客户端亲和性，Global Accelerator 会在侦听器的端点组中的端点之间平均分配流量。

   有关更多信息，请参阅 Global Accelerator 中客户端亲和性的工作原理。
6. 选择保存。

移除标准侦听器

本节提供在 AWS Global Accelerator 控制台上移除标准侦听器的步骤。要使用 API 操作（而不是控制台）来完成此任务，请参阅 AWS Global Accelerator API 参考中的 `DeleteListener`。

移除侦听器的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个加速器。
3. 选择一个侦听器，然后选择移除。
4. 在确认对话框中，选择移除。

Global Accelerator 中客户端亲和性的工作原理

如有与标准加速器配合使用的有状态应用程序，则可以将客户端亲和性配置为让 Global Accelerator 将来自特定来源（客户端）IP 地址的用户的所有请求引导至同一端点资源。选择此选项可保持用户的客户端亲和性。

默认情况下，标准侦听器的客户端亲和性设置为无，Global Accelerator 在侦听器的端点组中的端点之间平均分配流量。

Global Accelerator 使用一致流哈希算法为用户的连接选择最佳端点。如果将 Global Accelerator 资源的客户端亲和性配置为无，则 Global Acelerator 使用五元组属性（源 IP、源端口、目标 IP、目标端口和协议）来选择哈希值。接下来，它选择可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 Acelerator，并且您指定了此设置，则 Global Acelerator 无法确保来自客户端的连接始终路由到同一端点。

如果您想通过在每次连接时将特定用户（由其源 IP 地址标识）路由到同一端点来保持客户端亲和性，请将客户端亲和性设置为源 IP。指定此选项后，Global Acelerator 会使用二元组属性（源 IP 和目标 IP）来选择哈希值，并在用户连接时将用户路由到同一端点。此外，Global Accelerator 还通过将具有同一源 IP 地址的所有连接路由到同一端点组来遵循客户端亲和性。

有时，由互联网流量路由的变化造成的网络维护或中断可能会导致客户端流量转移到不同的 Global Accelerator 边缘站点。发生这种情况时，如果现在为客户端流量提供服务的边缘站点首选其它 AWS 区域，则无法保证保持客户端亲和性。

此外，请注意，如果您在加速器中设置了端点权重，在特定的有限场景中，Global Accelerator 会覆盖这些权重，以帮助确保可用性。当 Global Accelerator 在端点组中的端点之间对流量进行负载均衡时，在某些情况下，必须在保持客户端流量的可用性和遵守端点权重之间做出选择。例如，对于保留客户端 IP 地址的加速器，Global Accelerator 可能需要覆盖端点权重设置以帮助避免连接冲突。

AWS Global Accelerator 中的标准加速器的端点组

一个端点组将请求路由到 AWS Global Accelerator 中已注册的一个或多个端点。在标准加速器中添加侦听器时，可以指定 Global Accelerator 要将流量引导到的端点组。端点组以及其中的所有端点必须位于一个 AWS 区域中。您可以出于不同的目的（例如，为了蓝/绿部署测试）添加不同的端点组。

Global Accelerator 会根据客户端的位置和端点组的运行状况将流量引导至标准加速器中的端点组。如果需要，您还可以设置要发送到端点组的流量百分比。您可以通过使用流量拨号增加（调高）或减少（调低）发送到端点组的流量来实现此操作。该百分比仅适用于 Global Accelerator 已引导至端点组的流量，而不适用于所有流向侦听器的流量。

您可以为每个端点组定义 Global Accelerator 的运行状况检查设置。通过更新运行状况检查设置，您可以更改轮询与验证 Amazon EC2 实例和弹性 IP 地址端点运行状况的要求。对于网络负载均衡器和应用程序负载均衡器端点，请在弹性负载均衡控制台上配置运行状况检查设置。

Global Accelerator 会持续监控标准端点组中包含的所有端点的运行状况，并且仅将请求路由到运行状况良好的活动端点。有关更多信息，请参阅确保加速器的运行状况检查访问权限。如果没有可将流量路由到其中的运行状况良好的端点，Global Accelerator 会将请求路由到所有端点。

本节介绍如何在 AWS Global Accelerator 控制台上使用标准加速器的端点组。要将 API 操作与 Global Accelerator 结合使用，请参阅 AWS Global Accelerator API 参考。

内容

- 添加标准端点组
- 编辑标准端点组
- 移除标准端点组
- 使用流量拨号调整流向区域的流量
- 为受限端口或连接冲突覆盖侦听器端口
- 确保加速器的运行状况检查访问权限

添加标准端点组

您可以在 AWS Global Accelerator 控制台上或通过 API 操作来使用端点组。您可以随时从端点组中添加或移除端点。

本节介绍如何在 AWS Global Accelerator 控制台上添加标准端点组。要将 API 操作与 Global Accelerator 结合使用，请参阅 AWS Global Accelerator API 参考。

添加标准端点组的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个加速器。
3. 在侦听器部分的侦听器 ID 中，选择要向其添加端点组的侦听器的 ID。
4. 选择添加端点组。
5. 在侦听器部分中，通过从下拉列表中选择一个区域来为端点组指定区域。
6. 或者，在流量拨号中，输入 0 到 100 之间的数字，以设置此端点组的流量百分比。该百分比仅适用于已引导至此端点组的流量，而不适用于所有侦听器流量。默认情况下，流量拨号设置为 100。
7. 或者，要覆盖用于将流量路由到端点的侦听器端口，并将流量重新路由到端点上的特定端口，请选择配置端口覆盖。有关更多信息，请参阅 为受限端口或连接冲突覆盖侦听器端口。
8. 或者，要指定要应用于 EC2 实例和弹性 IP 地址端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 确保加速器的运行状况检查访问权限。
9. 或者，选择添加端点组，为此侦听器或其它侦听器添加更多端点组。
10. 选择添加端点组。

编辑标准端点组

本节介绍如何在 AWS Global Accelerator 控制台上编辑标准端点组。要将 API 操作与 Global Accelerator 结合使用，请参阅 AWS Global Accelerator API 参考。

编辑端点组的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个加速器。
3. 在侦听器部分的侦听器 ID 中，选择与端点组关联的侦听器的 ID。
4. 选择编辑端点组。
5. 在编辑端点组页面上，更改相应区域，调整流量拨号百分比，或选择配置运行状况检查以修改运行状况检查设置。
6. 选择保存。

移除标准端点组

本节介绍如何在 AWS Global Accelerator 控制台上移除标准端点组。要将 API 操作与 Global Accelerator 结合使用，请参阅 AWS Global Accelerator API 参考。

移除标准端点组的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个加速器。
3. 在侦听器部分中，选择一个侦听器。
4. 在端点组部分中，选择一个端点组，然后选择移除。
5. 在确认对话框中，选择移除。

使用流量拨号调整流向区域的流量

对于每个标准端点组，您可以设置流量拨号以控制引导至端点组的流量百分比（AWS 区域）。该百分比仅适用于已引导至端点组的流量，而不适用于所有侦听器流量。

请注意，如果您更改流量拨号，更新后的设置将仅适用于新连接。不会为了调整当前流量流而终止现有连接。

默认情况下，加速器中所有区域端点组的流量拨号设置为 100（即 100%）。例如，流量拨号使您可以轻松地对不同 AWS 区域的新版本进行性能测试或蓝/绿部署测试。

以下这些示例会说明如何使用流量拨号更改流向端点组的流量。

按区域升级应用程序

如果要升级某个区域中的应用程序或进行维护，请先将流量拨号设置为 0，以切断该区域的流量。当完成工作并准备好让该区域恢复服务时，将流量拨号调整为 100 以恢复流量。

在两个区域之间混合流量

此示例显示了同时更改两个区域端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端点组（一个用于 `us-west-2` 区域，一个用于 `us-east-1` 区域），并且您已将每个端点组的流量拨号设置为 50%。

现在，假设有 100 个请求传入加速器，其中 50 个来自美国东海岸，50 个来自西海岸。加速器会按如下方式引导流量：

- 每个海岸的前 25 个请求（总共 50 个请求）由其附近的端点组处理。也就是说，将 25 个请求引导至 `us-west-2` 中的端点组，将 25 个请求引导至 `us-east-1` 中的端点组。
- 将后续的 50 个请求引导至相反的区域。也就是说，后续的 25 个来自东海岸的请求由 `us-west-2` 处理，而后续的 25 个来自西海岸的请求由 `us-east-1` 处理。

在这种情况下，结果是两个端点组处理相同数量的流量。但是，每个端点组都会接收来自两个区域的混合流量。

负载共享多区域架构

您还可以配置流量拨号和端点权重以实现复杂场景，从而配置应用程序端点之间的负载共享。借助这些 Global Accelerator 功能，您可以在多区域架构中部署和运行应用程序，包括主动-主动和主动-备用设置。有关更多信息和详细示例，请参阅以下博客文章：Deploying multi-Region applications in AWS using AWS Global Accelerator

为受限端口或连接冲突覆盖侦听器端口

默认情况下，加速器使用您在创建侦听器时指定的协议和端口范围将用户流量路由到 AWS 区域中的端点。例如，如果您定义了一个接收端口 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，在添加或更新端点组时，您可以覆盖用于将流量路由到端点的侦听器端口。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端点上的端口 1080 和 1443。

使用端口覆盖的一个好处是可以帮助避免连接冲突，在某些情况下，连接冲突可能会导致 Global Accelerator 出现间歇性连接问题，从而导致 TCP 连接时间延迟。当用户（具有相同的源 IP 和源端口）访问 Global Accelerator 中的资源时，可能会发生这些冲突。您可以通过在加速器中配置端口覆盖来防止冲突，从而避免延迟。有关更多信息，请参阅 如何避免导致 TCP 连接时间延迟的连接冲突。

覆盖端口还可以帮助您避免在受限端口上侦听时出现问题。在端点上运行不需要超级用户（root）权限的应用程序会更安全。但是，在 Linux 和其它类似 Unix 的系统中，您必须具有超级用户权限才能在受限端口（1024 以下的 TCP 或 UDP 端口）上进行侦听。通过将侦听器上的受限端口映射到端点上的非受限端口，可以避免此问题。在 Global Accelerator 后面的端点上运行没有 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，您可以将侦听器端口 443 覆盖为端点端口 8443。

对于每个端口覆盖，您可以指定用于接受来自用户的流量的侦听器端口，以及 Global Accelerator 将该流量路由到的端点端口。有关更多信息，请参阅 添加标准端点组。

在创建端口覆盖时，请记住以下几点：

- 端点端口不能与侦听器端口范围重叠。您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。例如，在创建端口覆盖时，您无法定义从侦听器端口 100 到端点端口 210 的端口覆盖，因为端点端口（210）包含在您定义的侦听器端口范围（200-299）中。
- 端点端口不得重复。如果加速器中的一个端口覆盖指定了一个端点端口，则您不能使用来自其它侦听器端口的端口覆盖来指定相同的端点端口。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，以及从侦听器端口 81 到端点端口 90 的覆盖。
- 运行状况检查继续使用原始端口。如果您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，假设您在侦听器端口 80 上指定了运行状况检查，并且还指定了从侦听器端口 80 到端点端口 480 的覆盖端口。运行状况检查会继续使用端点端口 80。但是，通过端口 80 传入的用户流量会流向端点上的端口 480。

  此行为可保持网络负载均衡器、应用程序负载均衡器、EC2 实例和弹性 IP 地址端点之间的一致性。由于您在 Global Accelerator 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不同的端点端口，因此若 Global Accelerator 将运行状况检查端口映射到 EC2 实例和弹性 IP 地址端点的不同端点端口，则会导致不一致的行为。

- 安全组设置必须允许端口访问。确保安全组允许流量到达您在端口覆盖中指定的端点端口。例如，如果您将侦听器端口 443 覆盖为端点端口 1433，请确保安全组中为该应用程序负载均衡器或 Amazon EC2 端点设置的任何端口限制都允许端口 1433 上的入站流量。

确保加速器的运行状况检查访问权限

标准加速器的每个侦听器仅将请求路由到运行状况良好、处于活动状态的端点。在您添加端点时，端点必须通过运行状况检查才会被视为运行状况良好。AWS Global Accelerator 还会定期向标准加速器上的所有端点发送运行状况检查请求，以测试其状态。Global Accelerator 会自动运行这些常规运行状况检查。每次运行状况检查完成后，侦听器将关闭为运行状况检查建立的连接。

请注意，如果没有可将流量路由到其中的运行状况良好的端点，Global Accelerator 会将传入的客户端请求路由到端点组中的所有端点。有关更多信息，请参阅 运行状况不佳的端点的失效转移的工作原理。

有关运行状况检查工作原理的详细信息以及有关使用运行状况检查的指导，取决于端点资源的类型。本主题提供有关如何使用不同端点类型的运行状况检查的信息，包括更新 Global Accelerator 中运行状况检查选项的步骤（适用于 EC2 实例或弹性 IP 地址端点）。

确保加速器运行状况检查的访问权限

为确保运行状况检查能成功完成对 EC2 实例或弹性 IP 地址端点的访问，请确保路由器和防火墙规则允许来自与 Amazon Route 53 运行状况检查程序关联的 IP 地址的入站流量。要查看与 Route 53 运行状况检查程序关联的 IP 地址范围列表，请参阅《Amazon Route 53 开发人员指南》中的 Route 53 服务器的 IP 地址范围。

Global Accelerator 运行状况检查的工作原理是接收 Route 53 运行状况检查的流量，这些流量会转发到为端点组配置的运行状况检查端口。通常，为运行状况检查配置的端口会与侦听器配置相匹配。如果改为配置其它端口进行运行状况检查，请检查安全组配置，以确保该端口上不允许公共流量。

例如，如果侦听器配置在端口 80，则运行状况检查端口也是 80。如果选择在其它端口（例如端口 83）上配置运行状况端口，请确保将安全组配置为仅允许端口 83 上的流量来自处于 Route 53 运行状况检查的 IP 地址范围内的 IP 地址。

适用于不同端点类型的运行状况检查指导

请查看本节中的信息，了解有关为加速器的每种端点类型指定的运行状况检查的准则。

此外，请确保为包含 HTTP 工作负载的端点选择的运行状况检查能够代表应用程序的整体运行状况，并确保遵循上一节，即确保运行状况检查的安全和访问权限中描述的有关确保访问运行状况检查的指导。

以下准则适用于每种指定的端点类型：

- 对于网络负载均衡器或应用程序负载均衡器端点，请注意以下几点：
  - 在 Global Accelerator 中选择的运行状况检查选项不会影响您添加为端点的网络负载均衡器或应用程序负载均衡器。也就是说，您在 Global Accelerator 中指定的运行状况检查选项可用于 Amazon EC2 和弹性 IP 地址运行状况检查，但不用于负载均衡器端点上的运行状况检查。

    对于负载均衡器端点，请使用弹性负载均衡配置选项配置运行状况检查。有关更多信息，请参阅目标组的运行状况检查。
  - 如果至少有一个运行状况良好的可用区，Global Accelerator 就会认为网络负载均衡器或应用程序负载均衡器运行状况良好。如果可用区内的所有负载均衡器目标组都运行状况良好，则表明该可用区运行状况良好。有关更多信息，请参阅目标组的运行状况检查。
- 对于 EC2 实例或弹性 IP 地址端点，请注意以下几点：
  - 在为配置了 TCP 的侦听器添加 EC2 实例或弹性 IP 地址端点时，您可以指定用于运行状况检查的端口。默认情况下，如果您不指定用于运行状况检查的端口，Global Accelerator 将使用您为加速器指定的侦听器端口。
  - 当您使用 UDP 侦听器添加这些端点类型时，Global Accelerator 会使用侦听器端口和 TCP 协议进行运行状况检查，因此您在端点上必须有 TCP 服务器。

    请务必检查您在每个端点上为 TCP 服务器配置的端口是否与在 Global Accelerator 中为运行状况检查指定的端口相同。如果端口号不相同，或者您尚未为端点设置 TCP 服务器，则无论端点的运行状况如何，Global Accelerator 都会将该端点标记为运行状况不佳。
  - 在为 EC2 实例或弹性 IP 地址端点配置用于运行状况检查的端口时，请务必遵循安全和访问指导。

设置运行状况检查选项

要为加速器设置运行状况检查选项，请在创建加速器或编辑端点组时指定以下一个或多个选项。

您可以为端点组添加以下运行状况检查选项。

运行状况检查端口

Global Accelerator 对属于此端点组的端点执行运行状况检查时要使用的端口。

请注意，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 对属于此端点组的端点执行运行状况检查时要使用的协议。

运行状况检查间隔

端点的每次运行状况检查之间的间隔（以秒为单位）。

阈值计数

将运行状况不佳的目标视为运行状况良好，或将运行状况良好的目标视为运行状况不佳之前，所需的连续运行状况检查次数。

AWS Global Accelerator 中的标准加速器的端点

AWS Global Accelerator 中的标准加速器的端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。在 AWS Global Accelerator 中，静态 IP 地址充当客户端的单一接触点，并且 Global Accelerator 会通过标准加速器，将传入流量分配到各个运行状况良好的端点。Global Accelerator 通过您为侦听器指定的端口（或端口范围），将流量引导至端点所属的端点组中的端点。

每个端点组可以有多个端点。您可以将每个端点添加到多个端点组，但这些端点组必须与不同的侦听器相关联。当您将资源添加为端点时，资源必须是有效且活动的。

> **Important**
>
> 您配置为双堆栈的加速器（即要支持 IPv4 和 IPv6 的加速器）要求仅添加同样支持双堆栈的端点。网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例可添加为双堆栈端点。

Global Accelerator 会持续监控标准端点组中包含的所有端点的运行状况。它仅将流量路由到运行状况良好的活动端点。如果 Global Accelerator 没有可将流量路由到其中的运行状况良好的端点，则会将流量路由到 AWS 区域 中的所有端点。

内容

- 对可添加为加速器端点的资源的要求
- 添加标准端点
- 编辑标准端点

- 移除标准端点
- 如何通过端点权重管理流量
- 运行状况不佳的端点的失效转移的工作原理
- 如何避免导致 TCP 连接时间延迟的连接冲突

对可添加为加速器端点的资源的要求

对于可以添加为 AWS Global Accelerator 中标准加速器的端点的不同类型的资源，请注意以下要求和限制。

如果您计划为端点启用客户端 IP 地址保留，则还需要记住其它要求。有关更多信息，请参阅 具有客户端 IP 地址保留功能的转换端点。

注意：在终止或删除已添加为加速器后端端点的资源之前，建议您将该端点从 Global Accelerator 端点组中移除。

应用程序负载均衡器端点

- 应用程序负载均衡器端点可以是面向互联网的端点，也可以是内部的端点。
- 可以将双堆栈应用程序负载均衡器添加为端点。
- Global Accelerator 仅支持在 AWS 区域 内运行的应用程序负载均衡器。Global Accelerator 不支持在本地区域中作为端点运行的应用程序负载均衡器。

网络负载均衡器端点

- 网络负载均衡器端点可以是面向互联网的端点，也可以是内部的端点。
- 可以将双堆栈网络负载均衡器添加为端点，但需遵循一些限制：
  - 对于双堆栈加速器，当您添加双堆栈网络负载均衡器时，网络负载均衡器不能有目标类型为 `ip` 的目标组，也不能有目标类型为 `instance` 和 IP 地址类型为 `ipv6` 的目标组。
  - 对于 IPv4 加速器，当您添加双堆栈网络负载均衡器时，您无法在 Global Accelerator 中为端点启用客户端 IP 地址保留。
- Global Accelerator 仅支持在 AWS 区域 内运行的网络负载均衡器。Global Accelerator 不支持在本地区域中作为端点运行的网络负载均衡器。
- 对于网络负载均衡器端点，建议禁用负载均衡器的跨区域流量，以避免连接冲突，这可能会导致 TCP 连接时间延长。有关更多信息，请参阅 如何避免导致 TCP 连接时间延迟的连接冲突。

Amazon EC2 实例端点

- EC2 实例端点不能是以下类型之一：
  C1、CC1、CC2、CG1、CG2、CR1、CS1、G1、G2、HI1、HS1、M1、M2、M3 或 T1。

- 支持 EC2 实例作为特定 AWS 区域中的端点。有关更多信息，请参阅 AWS Global Accelerator 支持的 AWS 区域。

  Global Accelerator 仅支持 AWS 区域内的 EC2 实例。Global Accelerator 不支持路由到作为本地区域中端点的弹性 IP 地址。
- 建议您在终止某个 EC2 实例之前，先将其从 Global Accelerator 端点组中移除。如果您在将某个 EC2 实例从 Global Accelerator 的端点组中移除之前将其终止，然后在同一 VPC 中使用相同的私有 IP 地址创建另一实例，并且运行状况检查通过，则 Global Accelerator 会将流量路由到该新端点。
- 可以将双堆栈 EC2 实例添加为端点。但是，这些实例必须附带主 IPv6 弹性网络接口（ENI）。有关更多信息，请参阅《Amazon Elastic Compute Cloud 用户指南》中的使用网络接口。

弹性 IP 地址

- 不能将双堆栈弹性 IP 地址添加为端点。

对于所有端点，如果您将资源配置为 Global Accelerator 后端端点，建议您不要通过互联网将流量直接发送到相同的端点。发送直接流量可能会导致连接冲突问题。

此外，请注意，除非配置跨账户支持，否则您添加为加速器的端点的资源以及加速器本身必须归同一个账户所有。但是，负载均衡器端点后端的目标实例可归不同的账户所有。在这种情况下，必须向拥有目标实例的账户授予权限，以便其访问拥有负载均衡器和加速器的账户所拥有的子网。有关更多信息，请参阅 在 Global Accelerator 中配置跨账户访问。

添加标准端点

您可以向端点组添加端点，以便将流量引导至您的资源。您可以编辑标准端点以更改端点的权重。您也可以将某个端点从端点组中移除，以将其从加速器中移除。移除端点不会影响端点本身，但 Global Accelerator 无法再将流量引导至该资源。

您必须先创建资源，然后才能将其添加为 Global Accelerator 中的端点。当您将资源添加为端点时，资源必须是有效且活动的。有关 Global Accelerator 支持的端点类型和配置的详细信息，请参阅对可添加为加速器端点的资源的要求。

根据使用情况，您可能会在端点组中添加或移除端点。例如，如果对应用程序的需求增加，则可以创建更多资源。然后，您可以向一个或多个端点组添加更多端点来处理增加的流量。在您添加端点，并且端点通过初始运行状况检查后，Global Accelerator 就会开始将请求路由到端点。

您可以通过调整端点的权重来管理流向端点的流量，从而按比例向端点发送更多或更少的流量。有关更多信息，请参阅 如何通过端点权重管理流量。

注意：如果您正在考虑添加具有客户端 IP 地址保留功能的端点，请先查看在 AWS Global Accelerator 中保留客户端 IP 地址中的信息。

本节介绍如何在 AWS Global Accelerator 控制台上添加端点。要将 API 操作与 AWS Global Accelerator 结合使用，请参阅 AWS Global Accelerator API 参考。

添加标准端点的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个加速器。
3. 在侦听器部分的侦听器 ID 中，选择一个侦听器的 ID。
4. 在端点组部分的端点组 ID 中，选择您要向其添加端点的端点组的 ID。
5. 选择编辑。
6. 在端点部分中，选择添加端点。
7. 在添加端点页面上，从下拉列表中选择资源。

   如果您没有任何 AWS 资源，则该列表中将没有任何项。要继续操作，请创建诸如负载均衡器、Amazon EC2 实例或弹性 IP 地址之类的 AWS 资源。然后返回此处的步骤，并从列表中选择一种资源。

   > **Note**
   > 如果您有双堆栈加速器，则必须添加双堆栈端点。网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例可添加为双堆栈端点。

8. 或者，在权重中，输入 0 到 255 之间的数字，以设置将流量路由到此端点的权重。向端点添加权重时，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，所有端点的权重均为 128。有关更多信息，请参阅 如何通过端点权重管理流量。
9. 或者，为端点启用客户端 IP 地址保留。在保留客户端 IP 地址下，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。

   > **Note**
   > 在您添加流量并开始将流量路由到保留客户端 IP 地址的端点之前，请确保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含用户客户端 IP 地址。

10. 选择 Add endpoint (添加终端节点)。

编辑标准端点

本节介绍如何在 AWS Global Accelerator 控制台上编辑端点。要将 API 操作与 AWS Global Accelerator 结合使用，请参阅 AWS Global Accelerator API 参考。

编辑标准端点的步骤

您可以编辑端点配置以更改权重。有关更多信息，请参阅 如何通过端点权重管理流量。

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个加速器。
3. 在侦听器部分的侦听器 ID 中，选择一个侦听器的 ID。
4. 在端点组部分的端点组 ID 中，选择端点组的 ID。
5. 选择编辑终端节点。
6. 在编辑端点页面上，进行更新，然后选择保存。

移除标准端点

本节介绍如何在 AWS Global Accelerator 控制台上移除端点。要将 API 操作与 AWS Global Accelerator 结合使用，请参阅 AWS Global Accelerator API 参考。

例如，如果您需要为端点提供服务，可以从端点组中移除端点。移除端点会将端点从端点组中移除，但不会对端点产生其它影响。从端点组中移除某个端点后，Global Accelerator 会立即停止将流量引导至该端点。该端点会进入一种等待所有当前请求完成的状态，这样正在进行的客户端流量就不会中断。当您准备好让该端点恢复接收请求时，可以将该端点重新添加到端点组。

注意：在终止或删除已添加为加速器后端端点的资源之前，建议您将该端点从 Global Accelerator 端点组中移除。

删除终端节点

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个加速器。

3. 在侦听器部分的侦听器 ID 中，选择一个侦听器的 ID。
4. 在端点组部分的端点组 ID 中，选择端点组的 ID。
5. 选择移除端点。
6. 在确认对话框中，选择移除。

如何通过端点权重管理流量

通过加权路由，您可以选择将多少流量路由到端点组中的特定资源（端点）。这可以通过多种方式发挥作用，包括用于负载均衡和测试应用程序的新版本。

权重是可以设置的值，用于确定 Global Accelerator 向标准加速器中的端点引导的流量比例。端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。Global Accelerator 会计算端点组中端点的权重总和，然后根据每个端点的权重与总权重的比率将流量引导至这些端点。默认情况下，端点的权重设置为 128，即最大值 255 的一半。

端点权重的工作原理

要使用权重，您可以为端点组中的每个端点分配相对权重，该权重与您希望向端点发送的流量数量相对应。默认情况下，端点的权重为 128，即权重最大值 255 的一半。Global Accelerator 将根据您分配给端点的权重（占该组中所有端点总权重的比例）向端点发送流量：

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

例如，如果您想要将极少的一部分流量发送到一个端点，并将其余流量发送到另一个端点，则可以分别指定权重为 1 和 255。权重为 1 的端点将获得 1/256（1/1+255）的流量，另一个端点将获得 255/256（255/1+255）的流量。通过更改权重，可以逐渐更改每个端点的流量平衡。如果您希望 Global Accelerator 停止向某个端点发送流量，可以将该资源的权重更改为 0。

请注意，即使在加速器中设置了端点权重，在特定的有限场景中，Global Accelerator 也会覆盖这些权重，以帮助确保可用性。也就是说，当 Global Accelerator 对端点组中的端点之间的流量进行负载均衡时，在某些情况下，必须在保持客户端流量的可用性和遵守端点权重之间做出选择。例如，对于保留客户端 IP 地址的加速器，Global Accelerator 可能需要覆盖端点权重设置以帮助避免连接冲突。

运行状况不佳的端点的失效转移的工作原理

如果一个端点组中没有权重大于零的运行状况良好的端点，Global Accelerator 会尝试失效转移到另一个端点组中权重大于零的运行状况良好的端点。请注意，对于此失效转移，Global Accelerator 会忽略

流量拨号设置。因此，例如，如果某个端点组的流量拨号设置为零，则 Global Accelerator 仍将该端点组包含在失效转移尝试中。

如果 Global Accelerator 在尝试了三个最近的端点组（即 AWS 区域）后未找到权重大于零的运行状况良好的端点，则会将流量路由到离客户端最近的端点组中的随机端点。也就是说，它处于故障打开状态。

请注意以下几点：

- 为失效转移选择的端点组可能是流量拨号设置为零的端点组。
- 最近的端点组可能不是原始端点组。这是因为 Global Accelerator 在选择原始端点组时会考虑账户流量拨号设置。

例如，假设您的配置有两个端点，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，Global Accelerator 会将流量路由到运行状况良好的端点。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，Global Accelerator 会尝试另外三个端点组来查找权重大于零的运行状况良好的端点。如果找不到，Global Accelerator 会将流量路由到离客户端最近的端点组中的随机端点。

当恢复发生（即区域恢复正常运行）时，Global Accelerator 会恢复到正常的路由行为。这意味着通常情况下，路由将在约 30 秒左右后开始返回到运行状况良好的端点，前提是相应端点的流量拨号未设置为零。但请注意，已建立的活动连接不会移动。这些活动连接会继续路由到零权重区域，直到客户端或服务器重置连接，或者直到客户端建立新的连接。

如何避免导致 TCP 连接时间延迟的连接冲突

间歇性连接问题可能是由 AWS Global Accelerator 中的连接冲突引起。当用户在特定场景下通过相同的源 IP 和源端口访问 Global Accelerator 中的资源时，可能会发生这些情况。冲突可能导致通过加速器的流量出现 TCP 连接时间延迟。

您可以通过为加速器配置端口覆盖来避免这些延迟，端口覆盖是 Global Accelerator 中的一项功能，使您可以将传入流量路由到加速器端点上的其它目标端口。按照本节中的指导，了解如何使用端口覆盖来防止连接冲突并避免潜在的 TCP 连接时间延迟。

可能导致连接冲突的情况

Global Accelerator 中有三种情况可能导致连接冲突，从而导致 TCP 连接时间延迟：

- 您将相同的资源配置为具有多个加速器的端点。

- 您将资源配置为 Global Accelerator 后端端点，还直接通过互联网将流量从最终用户发送到相同的资源。
- 您为跨区域流量配置网络负载均衡器端点。

对于网络负载均衡器端点，建议禁用负载均衡器的跨区域流量，以避免连接冲突。有关更多信息，请参阅《网络负载均衡器用户指南》中的 TCP 连接延迟。

对于其它情况，建议在端点组中使用端口覆盖功能以防止冲突。通过使用端口覆盖，您可以将 Global Accelerator 侦听器端口映射到端点资源上的不同目标端口号。默认情况下，侦听器端口使用端点资源上的相同端口号。通过使用端口覆盖，加速器可以将来自相同用户（具有源 IP 和源端口）的流量路由到相同的端点，但使用不同的目标端口号，从而避免冲突。

下一节将为每种情况提供具体示例，说明如何配置端口覆盖以避免连接冲突。有关配置端口覆盖的更多信息，请参阅为受限端口或连接冲突覆盖侦听器端口。

如何通过使用端口覆盖来防止连接冲突

默认情况下，加速器使用在创建侦听器时指定的相同协议和相同目标端口范围将用户流量路由到 AWS 区域中的端点。但是，您可以选择覆盖侦听器端口的端口号映射。也就是说，您可以映射侦听器端口号，以将流量路由到端点上的其它目标端口号。

例如，如果您定义了一个接受端口 80 和 443 上的 TCP 流量的侦听器，默认情况下，加速器会将流量路由到端点上的相同端口 80 和 443。但是，通过使用端口覆盖功能，加速器可以将这些端口上传入的流量路由到端点上的不同端口，例如 8080 和 8443。

通过为两个（或更多）加速器中的侦听器创建不同的端口映射，并在其后配置相同的资源，可以为每个加速器使用不同的目标端口号，从而避免冲突。

例如，假设有加速器 A 和加速器 B，并且每个加速器都有一个为 TCP 和端口 443 配置的侦听器。您可以为加速器 A 的侦听器设置端口覆盖，将端口 443 映射到 8443，并为加速器 B 的侦听器设置端口覆盖，将端口 443 映射到 9443。现在，将应用程序负载均衡器端点（例如 ALB-1234）配置为同时侦听端口 8443 和 9443。然后，从同一个用户 IP 地址进入端口 443（两个加速器的侦听器）的流量将到达 ALB-1234，而不会出现连接冲突或 TCP 连接时间延迟。

您可以看到此示例的流量路径，如下所示：

```
Accelerator-A [listener: tcp,443] # Endpoint-Group [port-override:
443#8443] # ALB-1234 (listener: HTTPS,8443)
```

```
Accelerator-B [listener: tcp,443] # Endpoint-Group [port-override:
443#9443] # ALB-1234 (listener: HTTPS,9443)
```

您可以通过类似的方式使用端口覆盖，通过覆盖加速器的侦听器端口号的默认映射，防止资源在被直接用户访问和通过加速器访问时产生连接冲突。在这种情况下，要防止发生冲突，请执行以下操作：

1. 确定希望资源侦听直接流量的端口。
2. 为加速器配置侦听器以覆盖默认端口，并将资源上的侦听器配置为在该端口上侦听加速器流量。

例如，您可以为加速器的侦听器设置端口覆盖，以将端口 443 映射到端口 8443。例如，现在可以配置一个应用程序负载均衡器端点，以侦听端口 8443 上的加速器流量和端口 443 上的直接流量。使用此配置，可以避免来自同一用户 IP 地址的流量在应用程序负载均衡器上发生连接冲突。

在 AWS Global Accelerator 中使用自定义路由加速器

本章包括有关自定义路由加速器如何在 AWS Global Accelerator 中工作，以及如何为自定义路由加速器配置加速器、侦听器、端点组和 VPC 子网端点的信息。

借助自定义路由加速器，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中的特定 Amazon EC2 实例，同时提高通过 Global Accelerator 路由流量的性能。当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中相互交互（例如游戏应用程序或基于 IP 的语音传输（VoIP）会话）时，这一功能非常有用。

自定义路由加速器的端点必须是 Amazon VPC（VPC）子网，并且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 Global Accelerator 中的工作原理。

> **Note**
>
> 如果您希望 Global Accelerator 自动选择离客户端最近的运行状况良好的端点，请创建一个标准加速器。有关更多信息，请参阅 在 AWS Global Accelerator 中使用标准加速器。

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准则和要求。请参阅 自定义路由加速器的准则和限制。
2. 创建一个 VPC 子网。在将该子网添加到 Global Accelerator 后，您可以随时向子网添加 EC2 实例。
3. 在 Global Accelerator 中创建加速器。选择自定义路由加速器的选项。
4. 添加一个侦听器，在其中指定 Global Accelerator 要侦听的端口范围。确保您包括一个端口数量充足的大范围，以便 Global Accelerator 能够映射到您期望拥有的所有目标。这些端口不同于目标端口，目标端口将在下一步中指定。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准则和限制。
5. 为您拥有 VPC 子网的 AWS 区域添加一个或多个端点组。您可以为每个端点组指定以下内容：
   - 端点端口范围，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，或者同时指定 UDP 和 TCP。
6. 对于端点子网，选择一个子网 ID。您可以在每个端点组中添加多个子网，并且子网的大小可以不同（最大 /17）。

以下各节说明了自定义路由加速器的工作原理，并提供了创建和使用自定义路由加速器及其组件（包括侦听器、端点组和 VPC 子网端点）的步骤。

主题

- 自定义路由加速器在 Global Accelerator 中的工作原理
- Global Accelerator 中自定义路由的工作原理示例
- 自定义路由加速器的准则和限制
- AWS Global Accelerator 中的自定义路由加速器
- Global Accelerator 中自定义路由加速器的侦听器
- Global Accelerator 中的自定义路由加速器端点组
- Global Accelerator 中的自定义路由加速器的 Amazon VPC 子网端点

自定义路由加速器在 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标中的特定目标，同时仍可获得 Global Accelerator 的性能优势。自定义路由加速器将侦听器端口范围映射到 Amazon VPC（VPC）子网中的 EC2 实例目标。这样，Global Accelerator 就可以确定性地将流量路由到子网中的特定 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配合使用，在该应用程序中，您可以根据自己选择的因素（例如地理位置、玩家技能和游戏模式）将多名玩家分配给 Amazon EC2 游戏服务器上的单个会话。或者，您可能有 VoIP 或社交媒体应用程序，它可以将多个用户分配到特定媒体服务器以进行语音、视频和消息会话。

您的应用程序可以调用 Global Accelerator API 并接收 Global Accelerator 端口及其关联目标 IP 地址和端口的完整静态映射。您可以保存该静态映射，然后您的配对服务会使用该静态映射将用户路由到特定的目标 EC2 实例。您无需对客户端软件进行任何修改，即可开始在应用程序中使用 Global Accelerator。

要配置自定义路由加速器，请选择一个 VPC 子网端点。然后，您可以定义传入连接将映射到的目标端口范围，以便您的软件在所有实例中侦听同一组端口。Global Accelerator 会创建一个静态映射，通过该静态映射，您的配对服务可将会话的目标 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。

应用程序的网络堆栈可能通过单一传输协议运行，或者您可以改用 UDP 进行快速传输，使用 TCP 进行可靠传输。您可以为每个目标端口范围设置 UDP、TCP，或者同时设置 UDP 和 TCP，从而获得最大的灵活性，而不必为每个协议重复配置。

> **Note**
>
> 默认情况下，自定义路由加速器中的所有 VPC 子网目标都不能接收流量。此举是为了确保默认情况下的安全性，也是为了让您可以精细地控制子网中哪些私有 EC2 实例目标可以接收流量。您可以允许或拒绝流向子网或特定 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 添加自定义路由加速器的 VPC 子网端点。您也可以使用 Global Accelerator API 指定目标。有关更多信息，请参阅 AllowCustomRoutingTraffic 和 DenyCustomRoutingTraffic。

Global Accelerator 中自定义路由的工作原理示例

举个例子，假设您想在 Global Accelerator 后端的 1,000 个 Amazon EC2 实例中支持 10,000 个用户组交互的会话，例如游戏会话或 VoIP 通话会话。在此示例中，我们将侦听器端口范围指定为 10001—20040，将目标端口范围指定为 81—90。假设我们在 us-east-1 中有四个 VPC 子网：subnet-1、subnet-2、subnet-3 和 subnet-4。

在示例配置中，每个 VPC 子网的数据块大小为 /24，因此可以支持 251 个 Amazon EC2 实例。（每个子网中保留五个不可用的地址，而且这些地址未进行映射。）每个 EC2 实例上运行的每个服务器都提供以下 10 个端口，这些端口是我们在端点组中为目标端口指定的：81-90。这表示我们有与每个子网关联的 2510 个端口（10 x 251）。每个端口都可以与会话关联。

由于在子网中的每个 EC2 实例上指定了 10 个目标端口，因此 Global Accelerator 在内部将这些目标端口与可用于访问 EC2 实例的 10 个侦听器端口相关联。为了简单地说明这一点，我们假设有一个侦听器端口块，从第一组 10 个端点子网的第一个 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**
>
> 实际上映射并不具备这样的可预测性，但是我们在这里使用顺序映射来帮助展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：ListCustomRoutingPortMappings 和 ListCustomRoutingPortMappingsByDestination。

在示例中，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 关联。下表说明了此示例映射如何延续到第一个 VPC 子网的最后一个 IP 地址，然后延续到第二个 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
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

Global Accelerator 侦听器端口	VPC 子网	EC2 实例端口
...	...	...
12501	192.0.2.244	81
12502	192.0.2.244	82
12503	192.0.2.244	83
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

Global Accelerator 侦听器端口	VPC 子网	EC2 实例端口
12520	192.0.3.4	90

自定义路由加速器的准则和限制

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。

支持的端点目标

自定义路由加速器中的虚拟公有云（VPC）子网端点只能包含 EC2 实例。自定义路由加速器不支持其它资源（例如负载均衡器）。AWS Global Accelerator 中的标准加速器的端点中列出了 Global Accelerator 支持的 EC2 实例类型。

使用自定义路由加速器，Global Accelerator 只能将流量路由到 VPC 子网中 Amazon EC2 实例上的私有 IP 端点。但是，想要使用自定义路由的游戏客户可能需要连接到有状态会话。为此，客户在 Amazon Elastic Kubernetes Service（EKS）上运行游戏服务器，将会话托管在 Kubernetes 容器组（pod）内运行的特定容器上。

要在此场景中使用自定义路由，您可以配置 VPC-CNI 插件，以通过弹性网络接口（ENI）将流量发送到 Kubernetes 容器组（pod），该弹性网络接口（ENI）是 Global Accelerator 为每个存在端点的子网创建的。这是一种在 EKS 中使用自定义路由加速器的方法。同样的配置也适用于在 Amazon Elastic Container Service（ECS）中使用自定义路由加速器。要了解更多信息，请参阅以下博客文章中提供的详细步骤：AWS Global Accelerator Custom Routing with Amazon Elastic Kubernetes Service。

端口映射

添加 VPC 子网时，Global Accelerator 会创建静态端口映射，将侦听器端口范围映射到子网支持的端口范围。特定子网的端口映射永远不会改变。

您可以通过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

您添加到自定义路由加速器的 VPC 子网必须最小为 /28，最大为 /17。

IP 地址类型

自定义路由加速器仅支持 IPv4 IP 地址类型。

侦听器端口范围

您必须通过指定侦听器端口范围来指定足够的侦听器端口，以容纳您计划添加到自定义路由加速器的子网中包含的目标数量。您在创建侦听器时指定的范围决定了您可以在自定义路由加速器中使用的侦听器端口和目标 IP 地址组合的数量。为了最大限度地提高灵活性并降低因侦听器端口不足而出现错误的可能性，建议您指定较大的端口范围。

当您向自定义路由加速器添加子网时，Global Accelerator 会按区块分配端口范围。建议您线性分配侦听器端口范围，并将范围设置得足够大，以支持您打算拥有的目标端口数量。也就是说，您应分配的端口数量，应至少等于子网大小乘以您将在子网中拥有的目标端口和协议（目标配置）的数量。

> **Note**
>
> Global Accelerator 用于分配端口映射的算法可能需要您添加更多的侦听器端口，超出此总数。

创建侦听器后，您可以对其进行编辑以添加更多端口范围和相关协议，但不能减少现有端口范围。例如，如果侦听器端口范围为 5,000-10,000，则无法将端口范围更改为 5900-10,000，也无法将端口范围更改为 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。

目标端口范围

您可以从两个位置为自定义路由加速器指定端口范围：添加侦听器时指定的端口范围，以及为端点组指定的目标端口范围和协议。

- 侦听器端口范围：您的客户端连接到的 Global Accelerator 静态 IP 地址上的侦听器端口。Global Accelerator 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。
- 目标端口范围：您为端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在这些端口上接收流量。

运行状况检查和失效转移

Global Accelerator 不会对自定义路由加速器执行运行状况检查，也不会失效转移到运行状况良好的端点。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将以确定性方式进行路由。

默认情况下，所有流量均被拒绝

默认情况下，通过自定义路由加速器引导的流量无法发送到子网中的所有目标。要使目标实例能够接收流量，必须特别允许所有流量流向子网，或者允许流量流向子网中的特定实例 IP 地址和端口。

更新子网或特定目标以允许或拒绝流量这一操作需要一定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 DescribeCustomRoutingAccelerator。

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

通过 AWS Global Accelerator 中的自定义路由加速器，您可以使用自定义应用程序逻辑将一个或多个用户定向到多个目标中的特定目标，同时使用 AWS 全球网络来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虚拟私有云（VPC）子网中运行的 Amazon EC2 实例的端口。使用自定义路由加速器，Global Accelerator 不会根据端点的地理位置或运行状况来路由流量。要了解更多信息，请参阅 自定义路由加速器在 Global Accelerator 中的工作原理。

创建加速器时，默认情况下，Global Accelerator 会为您提供一组（两个）静态 IPv4 地址。自定义路由加速器仅支持 IPv4 IP 地址类型。如果您将自己的 IP 地址范围引入到 AWS（BYOIP），则可以从自己的池中分配静态 IPv4 地址，以用于加速器。有关更多信息，请参阅 在 Global Accelerator 中自带 IP 地址（BYOIP）。

> **Important**
>
> 即使禁用加速器且加速器不再接受或路由流量，只要加速器存在，IP 地址就会分配给该加速器。但是，如果您删除某个加速器，您将丢失分配给该加速器的 Global Accelerator 静态 IP 地址，因此您无法再使用这些地址路由流量。最佳实践是，确保您拥有适当的权限，以免无意中删除加速器。您可以将 IAM 策略（例如基于标签的权限）与 Global Accelerator 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 ABAC 与 Global Accelerator。

本节介绍如何在 Global Accelerator 控制台上使用自定义路由加速器。要了解如何将 API 操作与 Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

内容

- 在 Global Celerator 中创建自定义路由加速器
- 在 Global Celerator 中编辑自定义路由加速器
- 在 Global Celerator 中查看自定义路由加速器

- 在 Global Celerator 中删除自定义路由加速器

在 Global Celerator 中创建自定义路由加速器

本节提供有关如何在控制台上创建自定义加速器的步骤。要以编程方式使用 Global Accelerator，请参阅 AWS Global Accelerator API 参考。

创建自定义路由加速器的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 选择创建加速器。
3. 提供加速器的名称。
4. 对于加速器类型，请选择自定义路由。
5. 或者，如果您已将自己的 IP 地址范围引入到 AWS（BYOIP），则可以从该地址池中为加速器指定静态 IP 地址。针对加速器的两个静态 IP 地址中的每一个做出此选择。
   - 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，则还要从池中选择特定的 IP 地址。如果您选择默认 Amazon IP 地址池，则 Global Accelerator 会为您的加速器分配特定的 IP 地址。
6. 或者，添加一个或多个标签来帮助您识别加速器资源。
7. 选择下一步转到向导中的下一页，以添加侦听器、端点组和 VPC 子网端点。

在 Global Celerator 中编辑自定义路由加速器

本节提供有关如何在控制台上更新自定义加速器的步骤。要以编程方式使用 Global Accelerator，请参阅 AWS Global Accelerator API 参考。

编辑自定义路由加速器的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在自定义路由加速器列表中，选择一个加速器，然后选择编辑。
3. 在编辑加速器页面上，根据需要进行更改。例如，您可以禁用该加速器，以便将其删除。
4. 选择保存。

在 Global Celerator 中查看自定义路由加速器

本节提供在控制台上查看自定义路由加速器相关信息的步骤。要以编程方式查看自定义路由加速器的描述，请参阅 AWS Global Accelerator API 参考中的 ListCustomRoutingAccelerator 和 DescribeCustomRoutingAccelerator。

查看自定义路由加速器相关信息的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 要查看有关加速器的详细信息，请选择加速器，然后选择查看。

在 Global Celerator 中删除自定义路由加速器

如果您创建自定义路由加速器是为了进行测试，或者不再需要使用某个加速器，则可以将其删除。在控制台上，禁用该加速器，然后即可将其删除。您不必从该加速器中移除侦听器和端点组。

要使用 API 操作（而不是控制台）删除某个自定义路由加速器，必须先移除与该加速器关联的所有侦听器和端点组，然后将其禁用。有关更多信息，请参阅《AWS Global Accelerator API 参考》中的 DeleteAccelerator 操作。

禁用自定义路由加速器的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在列表中，选择要禁用的加速器。
3. 选择编辑。
4. 选择禁用加速器，然后选择保存。

删除自定义路由加速器的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在列表中，选择要删除的加速器。
3. 选择删除。

> **Note**
> 如果尚未禁用加速器，则无法删除。要禁用加速器，请参阅前面的步骤。

4. 在确认对话框中，选择删除。

> **Important**
> 如果您删除某个加速器，您将丢失分配给该加速器的静态 IP 地址，因此您无法再使用这些地址路由流量。

Global Accelerator 中自定义路由加速器的侦听器

对于 AWS Global Accelerator 中的自定义路由加速器，您可以配置侦听器，指定一系列侦听器端口及相关协议，Global Accelerator 会将这些端口和相关协议映射到 VPC 子网端点中的特定目标 Amazon EC2 实例。添加 VPC 子网端点时，Global Accelerator 会在您为侦听器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来指定加速器静态 IP 地址以及侦听器端口和协议，以便将用户流量引导至特定目标 Amazon EC2 实例 IP 地址和 VPC 子网中的端口。

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端点组，每个端点组对应您拥有 VPC 子网端点的每个 AWS 区域。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，或者同时指定 UDP 和 TCP。

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

内容

- 在 Global Accelerator 中为自定义路由加速器添加侦听器
- 在 Global Accelerator 中为自定义路由加速器编辑侦听器
- 在 Global Accelerator 中移除自定义路由加速器的侦听器

在 Global Accelerator 中为自定义路由加速器添加侦听器

本节介绍如何在 AWS Global Accelerator 控制台上为自定义路由加速器添加侦听器。要了解如何将 API 操作与 AWS Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

为自定义路由加速器添加侦听器的步骤

您在创建侦听器时指定的范围定义了您可以在自定义路由加速器中使用的侦听器端口和目标 IP 地址组合的数量。为了最大限度地提高灵活性，建议您指定较大的端口范围。您指定的每个侦听器端口范围必须包含至少 16 个端口。

> **Note**
>
> 创建侦听器后，您可以对其进行编辑以添加更多端口范围和相关协议，但不能减少现有端口范围。

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器页面上，选择一个自定义路由加速器。
3. 选择添加侦听器。
4. 在添加侦听器页面上，输入要与加速器关联的侦听器端口范围。

   侦听器支持端口 1-65535。为了最大限度地提高自定义路由加速器的灵活性，建议您指定较大的端口范围。
5. 选择添加侦听器。

在 Global Accelerator 中为自定义路由加速器编辑侦听器

本节介绍如何在 AWS Global Accelerator 控制台上为自定义路由加速器编辑侦听器。要了解如何将 API 操作与 AWS Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

为自定义路由加速器编辑侦听器的步骤

为自定义路由加速器编辑侦听器时，请注意，您可以添加更多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. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器页面上，选择一个加速器。
3. 选择一个侦听器，然后选择编辑侦听器。

4. 在编辑侦听器页面上，根据需要对现有端口范围或协议进行更改，或者添加新的端口范围。

   请注意，您不能缩小现有端口范围的范围。

5. 选择保存。

在 Global Accelerator 中移除自定义路由加速器的侦听器

本节介绍如何在 AWS Global Accelerator 控制台上移除自定义路由加速器的侦听器。要了解如何将 API 操作与 AWS Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

移除侦听器的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器页面上，选择一个加速器。
3. 选择一个侦听器，然后选择移除。
4. 在确认对话框中，选择移除。

Global Accelerator 中的自定义路由加速器端点组

通过 AWS Global Accelerator 中的自定义路由加速器，端点组可定义虚拟私有云（VPC）子网中的目标 Amazon EC2 实例用于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端点组。自定义路由加速器中的每个端点组可以有多个 VPC 子网端点。同样，您可以将每个 VPC 添加到多个端点组，但这些端点组必须与不同的侦听器相关联。

对于每个端点组，可以指定一组（一个或多个）端口范围，其中包括要在该区域的 EC2 实例上将流量引导到的端口。对于每个端点组的端口范围，可以指定要使用的协议：UDP、TCP 或同时使用 UDP 和 TCP。这可为您提供最大限度的灵活性，而不必为每种协议重复设置端口范围集。例如，您可能有一台游戏服务器，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 Global Accelerator 中的工作原理。

内容

- 在 Global Accelerator 中为自定义路由加速器添加端点组

- 在 Global Accelerator 中为自定义路由加速器编辑端点组
- 在 Global Accelerator 中移除自定义路由加速器的端点组

在 Global Accelerator 中为自定义路由加速器添加端点组

您可以在 AWS Global Accelerator 控制台上或通过 API 操作使用自定义路由加速器的端点组。您可以随时从端点组中添加或移除 VPC 子网端点。

本节介绍如何在 AWS Global Accelerator 控制台上创建自定义路由加速器的端点组。要了解如何将 API 操作与 Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

为自定义路由加速器添加端点组的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个自定义路由加速器。
3. 在侦听器部分的侦听器 ID 中，选择要向其添加端点组的侦听器的 ID。
4. 选择添加端点组。
5. 在侦听器部分中，为端点组指定区域。
6. 对于端口和协议集，输入 Amazon EC2 实例的端口范围和协议。
   - 输入起始端口和目标端口，以指定端口范围。
   - 对于每个端口范围，为该范围指定一个或多个协议。

   端口范围不必是侦听器端口范围的子集，但侦听器端口范围中的端口总数必须足以支持在自定义路由加速器中为端点组指定的端口总数。
7. 选择保存。
8. 或者，选择添加端点组，为此侦听器添加其它端点组。也可以选择其它侦听器并添加端点组。
9. 选择添加端点组。

在 Global Accelerator 中为自定义路由加速器编辑端点组

您可以在 AWS Global Accelerator 控制台上或通过 API 操作使用自定义路由加速器的端点组。您可以随时从端点组中添加或移除 VPC 子网端点。

本节介绍如何在 AWS Global Accelerator 控制台上编辑自定义路由加速器的端点组。要了解如何将 API 操作与 Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

编辑自定义路由加速器的端点组的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个自定义路由加速器。
3. 在侦听器部分的侦听器 ID 中，选择与端点组关联的侦听器的 ID。
4. 选择编辑端点组。
5. 在编辑端点组页面上，更改区域、端口范围或端口范围的协议。
6. 选择保存。

在 Global Accelerator 中移除自定义路由加速器的端点组

您可以在 AWS Global Accelerator 控制台上或通过 API 操作使用自定义路由加速器的端点组。

本节介绍如何在 AWS Global Accelerator 控制台上移除自定义路由加速器的端点组。要了解如何将 API 操作与 Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

移除自定义路由加速器的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:。
2. 在加速器页面上，选择一个加速器。
3. 在侦听器部分中，选择一个侦听器，然后选择移除。
4. 在端点组部分中，选择一个端点组，然后选择移除。
5. 在确认对话框中，选择移除。

Global Accelerator 中的自定义路由加速器的 Amazon VPC 子网端点

自定义路由加速器的端点是可通过加速器接收流量的 Amazon Virtual Private Cloud（VPC）子网。每个子网可以包含一个或多个 Amazon EC2 实例目标。添加子网端点时，Global Accelerator

会生成新的端口映射。然后，您可以使用 Global Accelerator 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 ListCustomRoutingPortMappings。

在为自定义路由加速器添加 VPC 子网和目标时，请注意以下几点：

- 您只能将流量引导到子网中的 EC2 实例，而不能将流量引导到其它资源，例如负载均衡器（与标准加速器不同）。
- 子网端点中的 EC2 实例目标不能是以下类型之一：C1、CC1、CC2、CG1、CG2、CR1、CS1、G1、G2、HI1、HS1、M1、M2、M3 或 T1。
- 默认情况下，通过自定义路由加速器引导的流量无法到达子网中的任何目标。要使目标实例能够接收流量，必须选择允许所有流量流向子网，或者选择允许流量流向子网中的特定实例 IP 地址和端口（目标套接字）。

> **Important**
>
> 更新子网或特定目标以允许或拒绝流量这一操作需要一定时间才能在互联网上传播。要确定更改是否已传播，可以使用 `DescribeCustomRoutingAccelerator` API 操作来检查加速器状态。有关更多信息，请参阅 DescribeCustomRoutingAccelerator。

- 由于 VPC 子网保留客户端 IP 地址，因此在添加子网作为自定义路由加速器的端点时，应查看相关的安全和配置信息。有关更多信息，请参阅 对保留客户端 IP 地址的端点的要求。
- 当您将资源配置为 Global Accelerator 后面的端点时，建议您不要通过互联网将流量直接发送到相同的端点。发送直接流量可能会导致连接冲突问题。

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

内容

- 添加自定义路由加速器的 VPC 子网端点
- 编辑自定义路由加速器的 VPC 子网端点
- 移除自定义路由加速器的 VPC 子网端点

添加自定义路由加速器的 VPC 子网端点

您可以将 Amazon Virtual Private Cloud（VPC）子网端点添加到自定义路由加速器中的端点组，以便将用户流量引导到子网中的目标 Amazon EC2 实例。

如果在子网中添加和移除 EC2 实例，或者允许或禁止流量流向 EC2 目标，会更改这些目标是否可以接收流量。但是，Global Accelerator 端口映射不会更改。

要允许流量流向子网中的某些目标（但不是全部），请输入您要允许的每个 EC2 实例的 IP 地址，以及您要接收流量的实例上的端口。您指定的 IP 地址必须是子网中的 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。

将 VPC 子网从端点组中移除，即可将其从加速器中移除。移除某个子网不会影响其本身，但是 Global Accelerator 无法再将流量引导至该子网或该子网中的 Amazon EC2 实例。此外，Global Accelerator 将回收 VPC 子网的端口映射，以便有可能将其用于您添加的新子网。

本节中的步骤说明如何在 AWS Global Accelerator 控制台上添加 VPC 子网端点。要了解如何将 API 操作与 AWS Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

添加 VPC 子网端点的步骤

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器页面上，选择一个自定义路由加速器。
3. 在侦听器部分的侦听器 ID 中，选择一个侦听器的 ID。
4. 在端点组部分的端点组 ID 中，选择要向其添加 VPC 子网端点的端点组（AWS 区域）的 ID。
5. 在端点部分中，选择添加端点。
6. 在添加端点页面上的端点中，选择一个 VPC 子网。

   如果您没有 VPC，则该列表中将没有任何项。要继续操作，请至少添加一个 VPC，然后返回此处的步骤，并从列表中选择一个 VPC。
7. 对于您添加的 VPC 子网端点，您可以选择允许或拒绝流量流向子网中的所有目标，也可以仅允许流量流向特定 EC2 实例和端口。默认设置是拒绝流量流向子网中的所有目标。
8. 选择 Add endpoint (添加终端节点)。

编辑自定义路由加速器的 VPC 子网端点

您可以编辑自定义路由加速器的 Amazon Virtual Private Cloud（VPC）子网端点，以便您可以更改将用户流量引导至目标 Amazon EC2 实例的位置，也可以允许或拒绝流量流向子网中的所有目标。

如果在子网中添加和移除 EC2 实例，或者允许或禁止流量流向 EC2 目标，会更改这些目标是否可以接收流量。但是，Global Accelerator 端口映射不会更改。

本节中的步骤说明如何在 AWS Global Accelerator 控制台上编辑 VPC 子网端点。要了解如何将 API 操作与 AWS Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

允许或拒绝流量流向特定目标的步骤

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

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器页面上，选择一个自定义路由加速器。
3. 在侦听器部分的侦听器 ID 中，选择一个侦听器的 ID。
4. 在端点组部分的端点组 ID 中，选择要编辑的 VPC 子网端点的端点组（AWS 区域）的 ID。
5. 选择一个端点子网，然后选择查看详细信息。
6. 在端点页面上的端口映射下，选择一个 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。

允许或拒绝所有流量流向子网的步骤

您可以更新端点，以允许或拒绝流量流向 VPC 子网中的所有目标。

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器页面上，选择一个自定义路由加速器。
3. 在侦听器部分的侦听器 ID 中，选择一个侦听器的 ID。
4. 在端点组部分的端点组 ID 中，选择要更新的 VPC 子网端点的端点组（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，然后选择保存。

移除自定义路由加速器的 VPC 子网端点

您可以从自定义路由加速器中移除 Amazon Virtual Private Cloud（VPC）子网端点，以便用户流量不再转到子网中的目标 Amazon EC2 实例。

本节中的步骤说明如何在 AWS Global Accelerator 控制台上移除 VPC 子网端点。要了解如何将 API 操作与 AWS Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

删除终端节点

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器页面上，选择一个自定义路由加速器。
3. 在侦听器部分的侦听器 ID 中，选择一个侦听器的 ID。
4. 在端点组部分的端点组 ID 中，选择要移除的 VPC 子网端点的端点组（AWS 区域）的 ID。
5. 选择移除端点。
6. 在确认对话框中，选择移除。

在 Global Accelerator 中配置跨账户访问

利用跨账户支持，您可以将 AWS Global Accelerator 用作访问多个账户中资源的应用程序的固定入口点，或从共享 CIDR 块中为加速器选择 IP 地址。AWS 最佳做法是使用跨账户权限来允许访问不同账户中的资源。通过针对自带 IP（BYOIP）地址 CIDR 块的跨账户支持，您可以将相同的地址池用于组织中不同账户的加速器。您还可以将 AWS 资源整理到一个账户下，通过该账户来控制应用程序的互联网访问权限，从而简化监控和安全保障，并提供入站连接的可见性。

Global Accelerator 中的跨账户支持让您可以执行以下操作：

- 将其他账户的端点（例如网络负载均衡器）添加到加速器。
- 为 IP 地址选择一个 BYOIP 地址池，然后从池中为不同账户下的加速器选择 IP 地址。通过共享 BYOIP 地址池，您可以使用来自同一 CIDR 块的更多地址，从而减少所需 CIDR 块数量。

您可以 Global Accelerator 控制台中使用跨账户附件和资源，也可以通过 AWS Command Line Interface（AWS CLI）或 AWS SDK 使用 Global Accelerator API 操作。例如，作为主体，您可以使用 UpdateEndpoints 操作将跨账户资源添加为加速器的端点。使用 API 操作时，您需要指定跨账户附件 ARN 和端点 ID。有关更多信息，请参阅《AWS Global Accelerator API 参考指南》。

内容

- Global Accelerator 中跨账户机制的工作原理
- 在 Global Accelerator 中使用跨账户附件
- 在 Global Accelerator 中使用跨账户资源
- 在 Global Accelerator 中识别跨账户资源
- Global Accelerator 中跨账户资源的责任和权限
- Global Accelerator 中跨账户资源的账单费用
- Global Accelerator 中跨账户资源的配额

Global Accelerator 中跨账户机制的工作原理

通过 Global Accelerator 中的跨账户支持，资源所有者可以控制自己的资源是否与其他账户拥有的加速器共享。要为您的资源启用资源共享，您以资源所有者的身份创建 Global Accelerator 跨账户附件，以授权其他账户将您账户中的资源添加到加速器。

您可以在 Global Accelerator 中创建跨账户附件。附件列出了您要共享的资源，以及经授权可以使用这些资源的主体（其他账户或特定的加速器 ARN）。资源可以是您作为端点添加到加速器端点组的 AWS 资源，例如网络负载均衡器，也可以是您通过自带 IP 地址（BYOIP）流程引入 Global Accelerator 的 IP 地址范围。

> **Important**
>
> 在向跨账户附件中添加 BYOIP IP 地址范围以与主体共享之前，必须完成预配和公告该地址范围的过程。有关更多信息，请参阅 在 Global Accelerator 中自带 IP 地址（BYOIP）。

在您以资源所有者身份创建附件后，附件中列出的主体可以使用附件中列出的资源。也就是说，他们可以将列出的 AWS 资源添加为端点，或者从列出的 CIDR 前缀中选择一个 BYOIP 地址作为静态 IP 地址。在主体想为加速器添加跨账户资源时，他们必须指定跨账户附件，以授权他们作为有权使用该资源的主体。

在 Global Accelerator 中使用跨账户附件

要允许某人将来自其他账户的资源添加为加速器的端点或 BYOIP 地址，该资源的所有者必须在 Global Accelerator 中创建跨账户附件。在附件中，资源所有者指定一个或多个允许添加资源的加速器或账户（主体），以及此类主体可向加速器添加的特定资源。

请注意，作为资源所有者，要在跨账户附件中指定资源，您必须拥有 AWS 账户中的资源。也就是说，资源必须在您的账户中分配或预配；您不能指定他人与您共享的资源，例如共享子网。

内容

- 在 AWS Global Accelerator 中创建跨账户附件
- 在 AWS Global Accelerator 中编辑跨账户附件
- 在 Global Accelerator 中删除跨账户附件

在 AWS Global Accelerator 中创建跨账户附件

请按照本节中的步骤操作，以使用 AWS Global Accelerator 控制台创建跨账户附件。

本部分介绍如何使用 AWS Global Accelerator 控制台创建跨账户附件。要了解如何将 API 操作与 Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

创建跨账户附件的方法

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 选择创建跨账户附件。
3. 在创建跨账户附件页面上，输入附件名称。
4. 为加速器添加要允许添加资源的 AWS 账户和/或 ARN。
5. 选择您希望允许使用的资源。例如，要添加可作为端点添加的资源，请为每个资源选择一个 AWS 区域。然后从下拉菜单中选择要添加的端点类型（资源类型）和端点（资源）。
6. 选择 Create attachment (创建挂载)。

注意：要在附件列表中查看新的跨账户附件，请刷新跨账户附件页面。

在 AWS Global Accelerator 中编辑跨账户附件

请按照本节中的步骤操作，以使用 AWS Global Accelerator 控制台编辑跨账户附件。

本部分介绍如何使用 AWS Global Accelerator 控制台编辑跨账户附件。要了解如何将 API 操作与 Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

您可以编辑跨账户附件，以添加或移除主体或资源、重命名附件或删除附件。

移除主体或资源或删除附件时，请注意以下事项：

- 要从附件中移除主体或 CIDR，主体必须首先从所有使用共享 IP 地址的加速器中移除这些地址。随后您就可以从附件中移除主体（即 CIDR）。
- 只有在没有任何加速器正在使用共享 CIDR 的共享 IP 地址时，才能移除共享 IP 地址或取消主体从附件访问共享 CIDR 的授权。
- 如果您从允许主体添加一个或多个共享端点的跨账户附件中移除主体，Global Accelerator 将从任何针对附件中所列跨账户资源使用该权限的加速器中移除这些跨账户端点。
- 如果您从跨账户附件中移除端点资源，Global Accelerator 会根据附件中的权限，将跨账户端点从任何将其作为端点添加的加速器中移除。
- 如果您删除了跨账户附件，Global Accelerator 会根据附件中的权限，将附件中所列的跨账户端点从任何将相应资源作为端点添加的加速器中移除。
- 如果有多个包含主体或包含资源的跨账户附件，Global Accelerator 将继续允许任何现有附件提供的访问权限。因此，举例来说，如果您从一个附件中移除了主体，但该主体仍然有权访问由第二个附件授予的资源，Global Accelerator 将继续允许主体访问跨账户资源。

编辑跨账户附件的方法

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 选择跨账户附件。
3. 选择需要更新的跨账户附件，然后选择编辑。
4. 修改附件以执行所需更改。例如，您可以添加或移除主体、重命名附件，还可以添加或移除资源。
5. 选择 Save changes（保存更改）。

在 Global Accelerator 中删除跨账户附件

请按照本节中的步骤操作，以使用 AWS Global Accelerator 控制台删除跨账户附件。

本部分介绍如何使用 AWS Global Accelerator 控制台删除跨账户附件。要了解如何将 API 操作与 Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

删除跨账户附件的方法

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 选择跨账户附件。
3. 选择跨账户附件，然后选择删除。
4. 在对话框内的文本框中键入 delete 以确认删除跨账户附件。
5. 选择删除。

在 Global Accelerator 中使用跨账户资源

如果您的账户或您有权访问的加速器在 AWS Global Accelerator 中的跨账户附件中被指定为主体，则您可以使用其他账户与您共享的资源。

例如，您可在创建加速器时选择自带 IP（BYOIP）地址作为静态 IP 地址，也可将端点添加到加速器的加速器端点组中。您还必须在附件中指定可添加的资源。

以下各节包括在 Global Accelerator 中添加或移除跨账户附件的步骤。

内容

- 在 Global Accelerator 中添加跨账户 BYOIP 地址
- 在 AWS Global Accelerator 中添加跨账户端点
- 在 Global Accelerator 中移除跨账户端点

在 Global Accelerator 中添加跨账户 BYOIP 地址

按照本节中的步骤，使用 Global Accelerator 控制台配置跨账户自带 IP（BYOIP）IP 地址。

本节介绍如何使用 AWS Global Accelerator 控制台使用 BYOIP 地址。要了解如何将 API 操作与 Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

您可以更改用于加速器的 BYOIP 地址，但存在一些限制。有关更多信息，请参阅 如何更新加速器以更改 IP 地址。

使用跨账户 BYOIP IP 地址

1. 通过以下网址打开 Global Accelerator 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. 选择加速器类型。
5. 为 IP 地址类型选择 IPv4。
6. 选中使用跨账户授权的 CIDR 中的静态 IP 地址复选框。
7. 针对将您指定为主体，包括已与您共享的 BYOIP 地址块的跨账户附件，为该跨账户附件所有者选择账户 ID。

   请注意，由于必须选择一个账户以从中选择地址，因此如果您在创建加速器时选择了两个 BYOIP IP 地址，则这些 IP 地址必须具有相同的所有者，并且必须在同一个跨账户附件中获得授权。
8. 为加速器指定一个或两个静态 IP 地址。

   - 对于每个静态 IP 地址，选择要使用的 IP 地址池。

   > **Note**
   >
   > 必须为每个静态 IP 地址选择一个独立的 IP 地址池。之所以存在这种限制，是因为为了实现高可用性，Global Accelerator 会将每个地址范围分配给不同的网络区域。

- 如果您选择自己的 IP 地址池，则还要从池中选择特定的 IP 地址。如果您选择默认 Amazon IP 地址池，则 Global Accelerator 会为您的加速器分配特定的 IP 地址。

9. 或者，添加一个或多个标签来帮助您识别加速器资源。
10. 选择下一步添加侦听器、端点组和端点。

在 AWS Global Accelerator 中添加跨账户端点

请按照本节中的步骤操作，使用 Global Accelerator 控制台添加跨账户端点。

本节介绍如何使用 AWS Global Accelerator 控制台添加跨账户端点。要了解如何将 API 操作与 Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

添加跨账户端点

1. 创建或更新加速器时，在端点部分中选择添加端点。
2. 在添加端点页面上，选择添加跨账户附件中指定的资源。
3. 在下拉菜单中选择已创建跨账户附件（包括您或加速器作为主体）的 AWS 账户。
4. 为端点类型选择要添加的资源类型。

   请注意，只有跨账户附件中包含的资源类型才会出现在下拉菜单中。
5. 为端点选择要添加的资源。

   请注意，只有跨账户附件中包含的资源才会出现在下拉菜单中。要查看未通过跨账户附件启用的资源，请清除添加跨账户附件中指定的资源复选框。

在 Global Accelerator 中移除跨账户端点

请按照本节中的步骤操作，使用 Global Accelerator 控制台移除跨账户端点。

本节介绍如何使用 AWS Global Accelerator 控制台移除跨账户端点。要了解如何将 API 操作与 Global Accelerator 配合使用，请参阅 AWS Global Accelerator API 参考。

移除跨账户端点

1. 创建或更新加速器时，在端点组详细信息页面上，选择要移除的端点。
2. 选择移除。

在 Global Accelerator 中识别跨账户资源

资源所有者和主体可使用 AWS Global Accelerator 控制台或使用 AWS CLI 及 Global Accelerator 操作来识别共享资源。例如，您可以执行以下操作：

- 作为所有者，您可以查看跨账户附件的列表，并查看每个附件中的主体和资源。
- 作为主体，您可以查看列出您的全部跨账户附件，也可以列出可添加为加速器、特定附件的端点或 IP 地址范围的资源。

有关使用 API 操作查看跨账户附件和共享资源的更多信息，请参阅 AWS Global Accelerator API 参考指南。

使用所有者身份：在 Global Accelerator 中识别跨账户资源

作为所有者，您可以在 AWS Management Console 中查看跨账户附件，或者使用 AWS Command Line Interface 与 Global Accelerator API 操作查看跨账户附件。

查看跨账户附件

- 在 Global Accelerator 控制台中，选择跨账户附件。

查看跨账户附件中包含的信息的方法

1. 在 Global Accelerator 控制台的跨账户附件页面上，选择一个附件，然后选择查看详细信息。

   -或-

2. 例如，通过使用 AWS Command Line Interface 来使用 API 操作 ListCrossAccountResources。此操作会返回账户中每个附件、每项资源的唯一附件资源对列表。

   例如，假设您有两个跨账户附件，第一个包含两个端点和一个 CIDR 块，而第二个包含三个端点，则 `ListCrossAccountResources` 会返回六个附件资源对：attachment1-endpoint1、attachment1-endpoint2、attachment1-CIDR、attachment2-endpoint3、attachment2-endpoint4 和 attachment2-endpoint5。

作为主体：在 Global Accelerator 中识别跨账户资源

作为主体，在获得跨账户附件授权以将资源作为端点添加到加速器后，无需执行任何其他操作即可将资源添加为端点。

您可以看到，AWS 账户 已创建跨账户附件，您在其中被列为主体。您还可以看到，每个账户创建的附件中指定的资源，您可以将这些资源添加为加速器的端点或 IP 地址范围。

查看已创建跨账户附件且您在其中被列为主体的账户的方法

1. 在 Global Accelerator 控制台中，在加速器的端点详细信息页面上选择添加端点。
2. 在添加端点页面上，选择添加跨账户附件中指定的资源。
3. 在为跨账户附件所有者选择账户 ID 下拉菜单中，查看允许您在跨账户附件中向加速器添加资源的一个或多个账户。

查看每个账户创建的附件中指定端点资源的方法

1. 在 Global Accelerator 控制台中，在加速器的端点详细信息页面上选择添加端点。
2. 在添加端点页面上，选择添加跨账户附件中指定的资源。
3. 在下拉菜单中，选择一个允许您在跨账户附件中向加速器添加资源的账户。
4. 为端点类型选择一种资源类型。

   请注意，只有跨账户附件中包含的资源类型才会出现在下拉菜单中。
5. 端点下拉菜单中包含一个资源列表。这些资源是由创建跨账户附件的账户授权添加的，用于特定资源类型的端点。
6. 要查看您可以添加的、由其他账户创建的跨账户附件中指定的资源，请执行以下操作：在为跨账户附件所有者选择账户 ID 下拉菜单中，选择不同的 AWS 账户。

查看账户创建的附件中指定 IP 地址资源的方法

1. 在 Global Accelerator 控制台中，选择创建加速器。
2. 在输入名称页面上，为 IP 地址类型选择 IPv4。
3. 在 IP 地址池选择下，选择使用跨账户附件中指定的共享 IP 地址池。
4. 选择一个允许您在跨账户附件中从共享 IP 地址池选择 IP 地址的账户。
5. 对于 IP 地址池，您可在下拉列表中查看共享 IP 地址池。

   请注意，只有包含在跨账户附件中且允许您使用的共享 IP 地址池才会出现在下拉菜单中。

Global Accelerator 中跨账户资源的责任和权限

以下几节列出了您作为资源所有者或主体在 AWS Global Accelerator 中拥有的跨账户访问权限。

资源所有者的权限

作为资源所有者，当您授权主体人将您的 AWS 账户 资源添加到其加速器或特定加速器时，主体可添加您在跨账户附件中列出的任何资源。

作为资源所有者，您负责创建、管理和删除您的资源。除非您的角色已获授权，否则您无法在加速器中添加或移除资源。

如果您拥有加速器并且需要添加跨账户资源，主体可在 IAM 中设置一个拥有资源访问权限的角色，并将您的账户添加到该角色。

您可以在跨账户附件中添加或移除主体或资源，以管理您拥有的资源是用作加速器的端点还是共享 IP 地址池。

主体的权限

通常而言，主体可向附件提供权限的加速器添加跨账户附件中列出的资源。对于其有权访问的跨账户资源，他们只能查看、添加或移除端点，或者从 BYOIP 地址池中选择共享 IP 地址。

以下内容适用于主体：

- 主体只能在跨账户附件中查看、添加或移除作为加速器端点或共享 IP 地址池的资源。
- 主体只能修改自己拥有的资源，例如负载均衡器。他们不能修改跨账户附件中指定的资源，因为这些资源属于资源所有者。

尽管主体无法修改实际的跨账户资源，但基于跨账户附件，资源所有者可创建一个 IAM 角色以提供资源访问权限。然后，所有者可授予主体承担该角色的权限，这样主体即可按照所有者通过角色权限指定的方式访问资源。

Global Accelerator 中跨账户资源的账单费用

AWS Global Accelerator 中的加速器所有者需要支付与该加速器相关的费用。对于加速器所有者或资源所有者而言，将跨账户资源添加为端点或作为加速器自带 IP 地址（BYOIP）池无需支付额外的费用。

有关定价的更多信息，请参阅AWS Global Accelerator 定价。

Global Accelerator 中跨账户资源的配额

您在 AWS Global Accelerator 中使用跨账户附件和跨账户资源时，以下内容适用：

- 添加为加速器端点的所有跨账户资源和其他资源（包括所有拥有跨账户权限的主体添加的资源）都会计入对该加速器生效的配额。
- 系统会对主体强制执行加速器配额。
- Global Accelerator 中的跨账户附件配额会对资源所有者强制执行。

有关限额的更多信息，请参阅AWS Global Accelerator 的配额。

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，还包括有关在 Global Accelerator 中使用自定义域的信息。它还包括配置自带 IP（BYOIP）地址以与 Global Accelerator 中的加速器配合使用的步骤。

- DNS 寻址：创建加速器时，Global Accelerator 会为您的加速器分配一个默认的域名系统（DNS）名称。
- 自定义域：您可以将 DNS 配置为在加速器中使用您的自定义域（例如 `www.example.com`），而非所分配的静态 IP 地址或默认 DNS 名称。
- BYOIP IP 地址：您可以将自己的 IP 地址添加到 AWS，以添加到加速器中，而不使用或同时使用 Global Accelerator 分配给您的静态 IP 地址。

内容

- AWS Global Accelerator 中支持 DNS 寻址
- 将自定义域流量路由到您的加速器
- 在 Global Accelerator 中自带 IP 地址（BYOIP）

AWS Global Accelerator 中支持 DNS 寻址

在创建 IP 地址类型为 IPv4 的加速器时，Global Accelerator 会为您预配两个静态 IPv4 地址。它还会为加速器分配默认域名系统（DNS）名称，类似于指向静态 IP 地址的 `a1234567890abcdef.awsglobalaccelerator.com`。

对于使用双堆栈 IP 地址类型的加速器，Global Accelerator 总共提供四个地址：两个静态 IPv4 地址和两个静态 IPv6 地址。Global Accelerator 会创建一个新的 DNS 名称，该名称同时指向 A 记录以及指向全部四个 IP 地址的 AAAA 记录。新的 DNS 记录使 Global Accelerator 能够将加速器升级到双协议栈，而不会影响当前引用非双协议栈原始 DNS 记录的客户端。使用双协议栈 IP 地址的加速器的 DNS 名称示例如下：`a1234567890abcdef.dualstack.awsglobalaccelerator.com`

静态地址使用从 AWS 边缘网络到您的端点的任播在全球范围内进行通告。您可以使用加速器静态地址或 DNS 名称将流量路由到加速器。DNS 服务器和 DNS 解析器使用轮询 DNS 过程来解析加速器 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。客户端通常使用所返回的第一个 IP 地址。

> **Note**
>
> 对于与您的加速器关联的每个 IPv4 和 IPv6 地址，Global Accelerator 都会创建一个指针（PTR）记录，该记录将加速器的静态 IP 地址映射到 Global Accelerator 生成的相应 DNS 名称，以支持反向 DNS 查询。这也称为反向托管区。请注意，Global Accelerator 为您生成的 DNS 名称不可配置，您也不能创建指向您的自定义域的 PTR 记录。Global Accelerator 也不会为您引入 AWS 的自带 IP 地址范围（BYOIP）中的静态 IP 地址创建 PTR 记录。

将自定义域流量路由到您的加速器

在大多数情景中，您都可以将 DNS 配置为在加速器中使用您的自定义域（例如 `www.example.com`），而非所分配的静态 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 Global Accelerator 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，并等待更改通过互联网传播。现在，在客户端使用您的自定义域名发出请求时，DNS 服务器会按照随机顺序将它解析为 IP 地址或加速器的 DNS 名称。

在将 Route 53 用作 DNS 服务时，要将自定义域名与 Global Acelerator 一起使用，请创建一条别名记录，将您的自定义域名指向分配给您的加速器的 DNS 名称。别名记录是 DNS 的 Route 53 扩展。这与 CNAME 记录相似，但您既可以为根域（如 `example.com`）又可以为子域（如 `www.example.com`）创建别名记录。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的在别名与非别名记录之间进行选择。

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南：《Amazon Route 53 开发人员指南》中的别名目标。要查看 Global Accelerator 的信息，请向下滚动到别名目标页面。

在 Global Accelerator 中自带 IP 地址（BYOIP）

您可将自己的部分或全部公有 IPv4 地址范围从本地网络带到 AWS 账户，以便与 AWS Global Accelerator 配合使用。您仍然拥有这些地址范围，但 AWS 会在互联网上发布这些地址范围。目前不支持 IPv6 的 BYOIP 功能。

Global Accelerator 使用静态 IP 地址作为加速器的入口点。这些 IP 地址是 AWS 边缘站点中的任播。默认情况下，Global Accelerator 会提供来自 Amazon IP 地址池的静态 IP 地址。您可以将这些入口点配置为自己地址范围中的 IPv4 地址，而不必使用 Global Accelerator 提供的 IP 地址。本主题介绍如何在 Global Accelerator 中使用您自己的 IP 地址范围。

您不能将针对一项 AWS 服务带到 AWS 的 IP 地址用于另一项服务。本章中的步骤描述了如何仅在 AWS Global Accelerator 中使用自带 IP 地址范围。有关在 Amazon EC2 中使用自带 IP 地址范围的步骤，请参阅《Amazon EC2 用户指南》中的自带 IP 地址（BYOIP）。

> **Important**
>
> 在通过 AWS 宣布地址范围之前，您必须停止从其它站点宣布 IP 地址范围。如果某个 IP 地址范围是多宿主（也就是说，该范围由多个服务提供商同时宣布），我们无法保证流向该地址范围的流量会进入我们的网络，也无法保证您的 BYOIP 宣布工作流程会成功完成。

在将地址范围带到 AWS 之后，它会在您的账户中显示为地址池。创建加速器时，您可以从该地址范围中为加速器分配一个 IP 地址。Global Accelerator 为您分配来自 Amazon IP 地址范围的第二个静态 IP 地址。如果将两个 IP 地址范围带到 AWS，则可以将每个范围中的一个 IP 地址分配给加速器。之所以存在这种限制，是因为为了实现高可用性，Global Accelerator 会将每个地址范围分配给不同的网络区域。

要在 Global Accelerator 中使用自己的 IP 地址范围，请查看相关要求，然后按照本主题中提供的步骤进行操作。

内容

- 要求
- 准备将您的 IP 地址范围带到 AWS 账户：授权
- 预置 Global Accelerator 中使用的地址范围
- 通过 AWS 公告地址范围
- 取消预配置地址范围
- 在 Global Accelerator 中将 BYOIP 地址与加速器配合使用
- 更新加速器以更改 IP 地址

要求

对于每个 AWS 账户，最多可以将两个符合条件的 IP 地址范围带到 AWS Global Accelerator。

要符合条件，IP 地址范围必须满足以下要求：

- 必须在以下某个区域互联网注册机构（RIR）注册 IP 地址范围：美洲互联网号码注册管理机构（ARIN）、欧洲 IP 网络资源协调中心（RIPE）或亚太互联网络信息中心（APNIC）。地址范围必须注册在企业或机构实体名下。地址范围不能注册到个人名下。
- 您可以自带的唯一地址范围是 /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 地址必须具有良好的历史记录。也就是说，这些地址不能声誉不佳或与恶意行为有关。如果我们在调查 IP 地址范围的声誉时发现发现该范围内有 IP 地址存在不良历史记录，那么我们保留拒绝该 IP 地址范围的权利。

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

- ARIN：`Direct Allocation` 和 `Direct Assignment` 网络类型
- RIPE：`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 地址范围带到 AWS 账户：授权

要确保只有您可以将 IP 地址空间带到 Amazon，我们需要两项授权：

- 您必须授权 Amazon 宣布 IP 地址范围。
- 您必须提供证据，证明您拥有该 IP 地址范围，因此有权将其带到 AWS。

> **Note**
>
> 如果您使用 BYOIP 将 IP 地址范围带到 AWS，则不能在我们宣布该地址范围时将该地址范围的所有权转让给其他账户或公司。您也不能直接将 IP 地址范围从一个 AWS 账户转移到另一个账户。要转让所有权或在不同 AWS 账户之间转移，您必须取消预置该地址范围，然后新的所有者必须按照步骤将该地址范围添加到自己的 AWS 账户。

要授权 Amazon 宣布 IP 地址范围，您需要向 Amazon 提供签名授权消息。使用路由来源授权（ROA）来提供此授权。ROA 是有关通过区域互联网注册机构（RIR）创建的路由公告的加密声明。ROA 包含 IP 地址范围、允许宣布 IP 地址范围的自治系统编号（ASN）以及到期日期。ROA 授权 Amazon 在特定自治系统（AS）下宣布 IP 地址范围。

ROA 不会授权您的 AWS 账户将 IP 地址范围带到 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。

以下几节提供完成这些授权任务的详细步骤。Linux 支持这些步骤中的命令。如果您使用的是 Windows，则可以访问适用于 Linux 的 Windows 子系统以运行 Linux 命令。

提供授权的步骤

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

第 1 步：创建 ROA 对象

创建 ROA 对象以授权 Amazon ASN 16509 宣布您的 IP 地址范围，以及当前已获授权的 ASN 宣布 IP 地址范围。ROA 必须包含要带到 AWS 的 /24 IP 地址，并且必须将最大长度设置为 /24。

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

- ARIN：ROA 请求
- RIPE：管理 ROA
- APNIC：路由管理

第 2 步：创建自签名 X.509 证书

创建密钥对和自签名 X.509 证书，然后将该证书添加到 RIR 的 RDAP 记录。以下步骤介绍如何执行这些任务。

> **Note**
>
> 在这些步骤中，`openssl` 命令需要 OpenSSL 版本 1.0.2 或更高版本。

创建和添加 X.509 证书的步骤

1. 使用以下命令生成一个 RSA 2048 位密钥对。

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

2. 使用以下命令从该密钥对创建一个公有 X.509 证书。

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

在此示例中，该证书将在 365 天后过期，在此日期后该证书将不可信。运行该命令时，请确保将 `-days` 选项设置为所需的值以获得适当的到期时间。当系统提示您提供其它信息时，您可以接受默认值。

3. 根据您的 RIR，按照以下步骤使用 X.509 证书更新 RIR 的 RDAP 记录。

   1. 使用以下命令查看证书。

   ```
   cat publickey.cer
   ```

   2. 将之前创建的证书添加到 RIR 的 RDAP 记录。请务必在编码部分前后包含 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 字符串。所有这些内容必须都在单个长线上。更新 RDAP 的过程取决于您的 RIR：

      - 对于 ARIN，使用客户经理门户，在代表您地址范围的“网络信息”对象的“公共注释”部分中添加证书。请勿将其添加到您组织的注释部分。
      - 对于 RIPE，将证书作为新的“descr”字段添加到代表您地址范围的“inetnum”或“inet6num”对象中。通常可在 RIPE 数据库门户的“我的资源”部分中了解到相关信息。请勿将其添加到您所在组织的注释部分或上述对象的“备注”字段中。
      - 对于 APNIC，通过电子邮件将证书发送到 helpdesk@apnic.net，以手动将其添加到您的地址范围的“remarks”（备注）字段中。请以 IP 地址的 APNIC 授权联系人身份发送电子邮件。

      完成下方预调配阶段后，可从 RIR 的记录中删除证书。

第 3 步：创建签名授权消息

创建签名授权消息，以允许 Amazon 宣布 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
```

创建签名授权消息的步骤

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

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

2. 使用您在上一节中创建的密钥对，在 `text_message` 中对授权消息进行签名。
3. 将消息存储在名为 `signed_message` 的变量中，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")
```

预置 Global Accelerator 中使用的地址范围

预置在 AWS 中使用的地址范围，即表示您确认您拥有该地址范围，并授权 Amazon 宣布该地址范围。我们将验证您是否拥有该地址范围。

您必须使用 CLI 或 Global Accelerator API 操作预置地址范围。此功能在 AWS 控制台中不可用。

要预置地址范围，请使用以下 ProvisionByoipCidr 命令。`--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 --region us-west-2 provision-byoip-cidr --cidr address-range --
cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

以下是预置地址范围的示例。

```
aws globalaccelerator --region us-west-2 provision-byoip-cidr
    --cidr 203.0.113.0/24
    --cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

预置地址范围是一项异步操作，因此相应调用会立即返回。但是，地址范围只有在其状态从 `PENDING_PROVISIONING` 更改为 `READY` 后才可供使用。完成预置过程最多可能需要三周时间。要监控您已预置的地址范围的状态，请使用以下 ListByoipCidrs 命令：

```
aws globalaccelerator --region us-west-2 list-byoip-cidrs
```

要查看 IP 地址范围的状态列表，请参阅 ByoipCidr。

预置 IP 地址范围后，由 `list-byoip-cidrs` 返回的 `State` 为 `READY`。例如：

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

通过 AWS 公告地址范围

预置地址范围后，即可对其进行宣布。您必须公告预配置的确切地址范围。您不能只公告预配置的地址范围的一部分。此外，在通过 AWS 宣布地址范围之前，您必须停止从其它站点宣布 IP 地址范围。

您必须使用 CLI 或 Global Accelerator API 操作宣布（或停止宣布）地址范围。此功能在 AWS 控制台中不可用。

> **Important**
>
> 在 Global Accelerator 中使用池中的 IP 地址之前，请确保 AWS 已宣布您的 IP 地址范围。

要宣布地址范围，请使用以下 AdvertiseByoipCidr 命令。

```
aws globalaccelerator --region us-west-2 advertise-byoip-cidr --cidr address-range
```

以下是请求 Global Accelerator 宣布地址范围的示例。

```
aws globalaccelerator --region us-west-2 advertise-byoip-cidr --cidr 203.0.113.0/24
```

要监控您已宣布的地址范围的状态，请使用以下 ListByoipCidrs 命令。

```
aws globalaccelerator --region us-west-2 list-byoip-cidrs
```

宣布 IP 地址范围后，由 `list-byoip-cidrs` 返回的 `State` 为 `ADVERTISING`。例如：

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

要停止宣布地址范围，请使用以下 `withdraw-byoip-cidr` 命令。

> **Important**
>
> 要停止宣布地址范围，您必须先移除任何具有从地址池中分配的静态 IP 地址的加速器。要使用控制台或 API 操作删除加速器，请参阅 删除加速器。

```
aws globalaccelerator --region us-west-2 withdraw-byoip-cidr --cidr address-range
```

以下是请求 Global Accelerator 撤回地址范围的示例。

```
aws globalaccelerator --region us-west-2 withdraw-byoip-cidr
    --cidr 203.0.113.0/24
```

取消预配置地址范围

要停止在 AWS 上使用您的地址范围，您必须先移除任何具有从地址池中分配的静态 IP 地址的加速器，并停止宣布您的地址范围。完成这些步骤后，您可以取消预置地址范围。

您必须使用 CLI 或 Global Accelerator API 操作来停止宣传及取消预置地址范围。此功能在 AWS 控制台中不可用。

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

第 2 步。停止宣布地址范围。要停止宣布范围，请使用以下 WithdrawByoipCidr 命令。

```
aws globalaccelerator --region us-west-2 withdraw-byoip-cidr --cidr address-range
```

第 3 步。取消预置地址范围。要取消预置范围，请使用以下 DeprovisionByoipCidr 命令。

```
aws globalaccelerator --region us-west-2 deprovision-byoip-cidr --cidr address-range
```

在 Global Accelerator 中将 BYOIP 地址与加速器配合使用

完成通过 BYOIP 添加地址范围的步骤后，您可以使用 BYOIP IP 地址创建加速器，也可以将 BYOIP IP 地址与现有加速器配合使用。如果您已将一个地址范围带到 AWS，则可以为加速器分配一个 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。

您还可以更新现有加速器以使用一个或多个 BYOIP IP 地址。有关更多信息，请参阅 更新加速器以更改 IP 地址

另一种方法是使用共享 BYOIP 地址。如果另一个账户与您共享了一个或多个其他 CIDR 地址，则在选择一个或两个 BYOIP IP 地址时，您可以从共享的 BYOIP CIDR 中进行选择。请注意，如果您选择使用两个共享 BYOIP 地址，则这些地址都必须来自同一个账户拥有的 CIDR。有关更多信息，请参阅 在 Global Accelerator 中配置跨账户访问。

您可以通过多种方式使用自己的 IP 地址作为静态 IP 地址创建加速器：

- 使用 Global Accelerator 控制台创建加速器。有关更多信息，请参阅下列内容：
  - 创建加速器
  - 在 Global Celerator 中创建自定义路由加速器
  - 在 AWS Global Accelerator 中添加跨账户端点
- 使用 Global Accelerator API 创建加速器。有关更多信息（包括使用 CLI 的示例），请参阅 AWS Global Accelerator API 参考中的以下内容：
  - CreateAccelerator
  - CreateCustomRoutingAccelerator

更新加速器以更改 IP 地址

在您将 BYOIP 地址分配为 AWS Global Accelerator 中加速器的静态 IP 地址后，您可以稍后更新加速器，以使用地址范围中的不同 IP 地址。您也可以将使用您自己的 IP 地址的加速器更新为改用 AWS Global Accelerator 提供的 IP 地址。

更改 Amazon 拥有的静态 IP 地址后，您可以恢复到原来的静态 IP 地址，但您必须在更改后的 10 天内执行此操作。10 天后，原来的静态 IP 地址将返回到 Amazon IP 地址池并重复使用。之后，如果您更新加速器以将 BYOIP 地址更改为 Global Accelerator 分配的 IP 地址，则会从 Amazon IP 地址池中为您分配一个新的 IP 地址。要了解有关恢复 IP 地址的更多信息，请参阅恢复静态 IP 地址更改。

以下部分提供了有关在 Global Accelerator 中使用自带 IP 地址（BYOIP）时如何更改 IP 地址的信息，并列出了更改静态 IP 地址时的要求和注意事项。

如何更新加速器以更改 IP 地址

要更改加速器的 IP 地址，请编辑加速器，然后在 IP 地址下选择一个新的 IP 地址。您是否可以从您自己的 BYOIP 地址池或 Amazon IP 地址池中选择地址，取决于加速器已为静态 IP 地址进行的设置，以及其它因素。

在开始之前，请务必查看更改加速器静态 IP 地址的要求和注意事项。

以下主题提供更新加速器的过程。

- 使用 Global Accelerator 控制台更新加速器。有关更多信息，请参阅下列内容：
  - 更新加速器
  - 在 Global Celerator 中编辑自定义路由加速器
- 使用 Global Accelerator API 更新加速器。有关更多信息（包括使用 CLI 的示例），请参阅 AWS Global Accelerator API 参考中的以下内容：
  - UpdateAccelerator
  - UpdateCustomRoutingAccelerator

更新加速器以更改 IP 地址时的要求

更新加速器以更改一个或两个静态 IP 地址时，请牢记以下几点：

- 您可以更改标准加速器和自定义路由加速器的 BYOIP 地址。在您创建一个具有一个或两个 BYOIP 地址的加速器后，该加速器必须始终至少具有一个 BYOIP 地址。但是，您可以更新该加速器，将一个或两个静态 IP 地址更改为使用 BYOIP 地址，或者更改 BYOIP 地址
- 如果您的加速器有两个 BYOIP 静态 IP 地址，则只能将其中一个地址更改为使用 Global Accelerator 分配的静态 IP 地址。请注意以下有关将加速器的 BYOIP 静态 IP 地址更改为 Global Accelerator 分配的静态 IP 地址的信息：
  - 如果您在将地址更改为 BYOIP 地址后的 10 天内进行此更改，则只能将地址更改回原来的 Global Accelerator 静态 IP 地址之一。10 天后，原来的静态 IP 地址将返回到 Global Accelerator IP 地址

池并重复使用。之后，如果您更新加速器以将 BYOIP 地址更改为 Global Accelerator 分配的 IP 地址，则系统会从 Global Accelerator IP 地址池中为您分配一个新的 IP 地址。

- 您不能将两个 BYOIP 静态 IP 地址更改为改用 Global Accelerator 静态 IP 地址。要将 Global Accelerator 分配的两个静态 IP 地址与加速器配合使用，请创建一个新的加速器。

- 如果您的加速器使用两个 BYOIP 地址，则可以将其中一个地址更改为不同的 BYOIP 地址。但是，当您添加 BYOIP 地址时，适用的限制与创建加速器时相同。例如，如果您更新加速器以使用两个不同的 BYOIP 地址，则这些地址必须来自您已添加到 Global Accelerator 的不同 BYOIP 地址范围。
- 如果您配置了跨账户 BYOIP 地址，则在更新加速器的静态 IP 地址时，可以使用跨账户地址。
- 在一种特定情况下，当您更新 BYOIP 地址时，Global Accelerator 可能需要更改 Amazon 静态 IP 地址，这样才能成功完成更新。只有在以下情况下，Amazon 静态 IP 地址才会受到影响：1) 您更新加速器的 BYOIP 静态 IPv4 地址以使用其他账户中的 BYOIP 地址（即跨账户 BYOIP 地址）；2) 加速器上的第二个静态 IP 地址来自 Amazon 池。

  如果您不想更改 Amazon 静态 IP 地址，则可以恢复到之前的 Amazon IP 地址，但前提是自更新后不超过 10 天。如果您恢复更改，会针对加速器恢复原来的 Amazon IP 地址。但是，在 10 天之后，Amazon IP 地址会被释放回可用的 IP 地址池，并且无法恢复。

恢复静态 IP 地址更改

要恢复到加速器原来的 Amazon IP 地址，请执行以下操作：

- 将加速器更新为原来的 BYOIP 静态 IP 地址（您已将其更改为新地址）。

当您进行此更新时，Global Accelerator 也将恢复原来的 Amazon 静态 IP 地址。

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 地址的选项取决于加速器设置的端点。启用客户端 IP 地址保留后，到达负载均衡器的数据包将保留原始客户端的源 IP 地址。

自定义路由加速器上的端点始终保留客户端 IP 地址。标准加速器有三种类型的端点可以在传入的数据包中保留客户端的源 IP 地址：应用程序负载均衡器、Amazon EC2 实例和带有安全组的网络负载均衡器。对于添加为端点并启用客户端 IP 地址保留的特定资源具有一些要求和限制。有关更多信息，请参阅 具有客户端 IP 地址保留功能的转换端点。

请注意，对于以下端点类型，Global Accelerator 不支持保留客户端 IP 地址：

- 不带安全组的网络负载均衡器
- 弹性 IP 地址

有关端点要求的详细信息，请参阅对可添加为加速器端点的资源的要求。

内容

- Global Accelerator 中保留客户端 IP 地址的准则和限制
- 对保留客户端 IP 地址的端点的要求
- 如何在 AWS Global Accelerator 中保留客户端 IP 地址
- 客户端 IP 地址保留的优势
- 具有客户端 IP 地址保留功能的 ENI 和安全组的最佳实践
- 具有客户端 IP 地址保留功能的转换端点

Global Accelerator 中保留客户端 IP 地址的准则和限制

在 AWS Global Accelerator 中准备和使用客户端 IP 地址保留功能时，请注意以下准则和限制。

计划添加客户端 IP 地址保留功能时，请注意以下事项：

- 在您添加流量并开始将流量路由到保留客户端 IP 地址的端点之前，请确保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含用户客户端 IP 地址。
- 您可能会在 AWS WAF 中看到客户端 IP 地址，而看不到 Global Accelerator IP 地址。将 Global Accelerator 配置为保留客户端 IP 地址并启用 AWS WAF 阻止来自应用程序负载均衡器的连接时(这些连接并非来自 Global Accelerator），客户端 IP 地址会显示在 AWS WAF 中。

- 支持 Global Accelerator 的所有 AWS 区域 都支持客户端 IP 地址保留功能。有关受支持的 区域的列表，请参阅AWS Global Accelerator 支持的 AWS 区域。

创建新加速器时，默认情况下会为支持的端点启用客户端 IP 地址保留。是否默认启用客户端 IP 地址保留取决于端点类型：

- 在 Global Accelerator 中使用面向互联网的应用程序负载均衡器作为端点时，新加速器会默认启用客户端 IP 地址保留。在创建加速器时您可以选择禁用该选项，也可以在稍后编辑加速器。
- 在 Global Accelerator 中使用内部应用程序负载均衡器或 EC2 实例时，端点始终启用客户端 IP 地址保留。
- 在 Global Accelerator 中添加带有安全组的网络负载均衡器作为端点时，默认不启用客户端 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。对于这些端点，您无法禁用该选项。
- 使用 AWS 控制台创建新加速器时，对于应用程序负载均衡器端点，“客户端 IP 地址保留”选项默认处于启用状态。对于带有安全组的网络负载均衡器端点，该选项默认处于不启用状态。添加端点后，您可以随时更新这些端点的“客户端 IP 地址保留”选项。
- 使用 AWS CLI 或 API 操作创建新加速器且未指定“客户端 IP 地址保留”选项时，以下是客户端 IP 地址保留的默认设置：
  - 面向互联网的应用程序负载均衡器端点默认启用客户端 IP 地址保留。
  - 带有安全组的网络负载均衡器端点默认不启用客户端 IP 地址保留。

对于现有的加速器，您可以将不具有客户端 IP 地址保留功能的端点转换到保留客户端 IP 地址的端点。例如，现有的应用程序负载均衡器端点可以转换到新的应用程序负载均衡器端点。要转换到新端点，我们建议您执行以下操作，将流量从现有端点逐步转移到保留客户端 IP 地址的新端点：

- 对于带有安全组的现有应用程序负载均衡器或网络负载均衡器端点，请先向 Global Accelerator 添加一个针对相同后端的重复的负载均衡器端点，并确保已启用客户端 IP 地址保留。然后调整端点的权重，将流量从不具有客户端 IP 地址保留功能的负载均衡器逐步转移到具有客户端 IP 地址保留功能的负载均衡器。

- 对于现有的弹性 IP 地址端点，您可以将流量转移到具有客户端 IP 地址保留功能的 EC2 实例端点。首先向 Global Accelerator 添加 EC2 实例端点，然后调整端点的权重，将流量从弹性 IP 地址端点逐步转移到 EC2 实例端点。

有关分步转换指导，请参阅 转换端点以使用客户端 IP 地址保留功能。

对保留客户端 IP 地址的端点的要求

使用客户端 IP 地址保留功能对端点类型有一些特定的要求。> 您可以将此功能用于应用程序负载均衡器、带有安全组的网络负载均衡器和 Amazon EC2 实例类型端点，但须遵守本节中描述的其它要求。自定义路由加速器上的端点始终保留客户端 IP 地址。

本节介绍了与要添加的具有客户端 IP 地址保留功能的端点相关的特定信息。有关端点总体要求的信息，请参阅对可添加为加速器端点的资源的要求。

此外，有关客户端 IP 地址保留的最佳实践的更多信息，请参阅具有客户端 IP 地址保留功能的 ENI 和安全组的最佳实践。

如果您打算使用客户端 IP 地址保留功能，除了对 Global Accelerator 中端点的总体要求外，在向 Global Accelerator 添加端点时还需注意以下事项。

弹性 IP 地址

Global Accelerator 中的弹性 IP 地址端点不支持客户端 IP 地址保留。

网络负载均衡器端点

如果您想在 Global Accelerator 中添加网络负载均衡器资源作为端点时启用客户端 IP 地址保留，请注意以下情况不支持客户端 IP 地址保留功能：

- 不带安全组的网络负载均衡器
- 带有安全组且安全组连接了 TLS 侦听器的网络负载均衡器
- 带有安全组且安全组对其 EC2 目标执行 IPv4 到 IPv6 的 NAT 转换的网络负载均衡器

此外，对于网络负载均衡器，仅当目标与网络负载均衡器位于同一 VPC 中时，才支持客户端 IP 地址保留功能。流量必须直接从网络负载均衡器流向目标。

弹性网络接口

为了支持客户端 IP 地址保留功能，Global Accelerator 会在您的 AWS 账户中创建弹性网络接口，每个存在端点的子网都有一个弹性网络接口。有关 Global Acccelerator 如何使用弹性网络接口的更多信息，请参阅具有客户端 IP 地址保留功能的 ENI 和安全组的最佳实践。

私有子网中的端点

您可以使用 Global Accelerator 将应用程序负载均衡器、网络负载均衡器或私有子网中的 EC2 实例作为目标，但必须将互联网网关连接到包含端点的 VPC。有关更多信息，请参阅 AWS Global Accelerator 中的安全 VPC 连接。

最为最佳实践，如果要确保流量仅由 Global Accelerator 传送，请使用私有子网。此外，请确保恰当配置入站安全组规则，以正确允许或拒绝应用程序的流量。

将客户端 IP 地址添加到允许列表

在您添加流量并开始将流量路由到保留客户端 IP 地址的端点之前，请确保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含用户客户端 IP 地址。网络访问控制列表（ACL）仅适用于出口（出站）流量。如果您需要筛选入口（入站）流量，则必须使用安全组。

配置网络访问控制列表（ACL）

在加速器上启用客户端 IP 地址保留时，与您的 VPC 子网关联的网络 ACL 将适用于出口（出站）流量。但是，要允许流量通过 Global Accelerator 流出，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 Global Accelerator 连接到端点，请将端点的子网与允许发往临时 TCP 或 UDP 端口（端口范围 1024-65535，目标 0.0.0.0/0）的出站流量的网络 ACL 相关联。此外，创建匹配的入站规则（端口范围 1024-65535，源 0.0.0.0/0）。

对于安全组和 WAF 请注意以下事项：

- 安全组和 AWS WAF 规则是用来保护资源的一组附加功能。例如，与您的 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以通过 Global Accelerator 连接的目标端口，例如 HTTP 的端口 80 或 HTTPS 的 443 端口。
- Amazon EC2 实例安全组适用于到达实例的任何流量，包括来自 Global Accelerator 的流量以及分配给实例的任何公有或弹性 IP 地址。

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

对于 Amazon EC2 实例、网络负载均衡器和应用程序负载均衡器，AWS Global Accelerator 以不同的方式保留客户端的源 IP 地址：

- 对于 EC2 实例端点，会为所有流量保留客户端的 IP 地址。
- 对于具有客户端 IP 地址保留功能的网络负载均衡器端点，Global Accelerator 与网络负载均衡器协作，在数据包的 IP 标头中包含原始客户端的 IP 地址，以便您的应用程序可以访问它。

- 对于具有客户端 IP 地址保留功能的应用程序负载均衡器端点，Global Accelerator 与应用程序负载均衡器协作，提供 X-Forwarded 标头 X-Forwarded-For（其中包含原始客户端的 IP 地址），以便您的网络层可以访问它。

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 信息标头中定义了标准 HTTP 标头字段集。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-Forwarded 前缀。

由于应用程序负载均衡器会终止传入的 TCP 连接并创建后端目标的新连接，因此它不会将客户端 IP 地址一直保留到目标代码（例如实例、容器或 Lambda 代码）中。您的目标在 TCP 数据包中看到的源 IP 地址是应用程序负载均衡器的 IP 地址。但是，应用程序负载均衡器确实保留了原始客户端 IP 地址，方法是先将其从原始数据包的回复地址中删除，再将其插入到 HTTP 标头中，然后通过新的 TCP 连接将请求发送到您的后端。

X-Forwarded-For 请求标头的格式如下所示：

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

下面是 IP 地址为 203.0.113.7 的客户端的 X-Forwarded-For 请求标头的示例。

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

下面是 IPv6 地址为 2001:DB8::21f:5bff:febf:ce22:8a2e 的客户端的 X-Forwarded-For 请求标头的示例。

```
X-Forwarded-For: 2001:DB8::21f:5bff:febf:ce22:8a2e
```

客户端 IP 地址保留的优势

您可以在 Global Accelerator 中为特定端点配置客户端 IP 地址保留。对于使用 AWS Global Accelerator 配置的一些应用程序，您可能需要使用具有客户端 IP 地址保留功能的端点来访问原始客户端 IP 地址。

例如，如果您拥有客户端 IP 地址，则可以根据客户端 IP 地址收集统计信息。您还可以使用基于 IP 地址的筛选条件（例如应用程序负载均衡器上的安全组）来筛选流量。您可以使用负载均衡器的 X-Forwarded-For 标头（其中包含原始客户端 IP 地址信息）在运行于应用程序负载均衡器端点后的

Web 层服务器之上的应用程序中应用特定于用户 IP 地址的逻辑。您还可以在与应用程序负载均衡器或网络负载均衡器关联的安全组的安全组规则中使用客户端 IP 地址保留功能。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 实例端点，会保留原始客户端 IP 地址。

对于未启用客户端 IP 地址保留的端点，边缘网络上的 Global Accelerator 服务使用的 IP 地址会将请求用户的 IP 地址替换为到达数据包中的源地址。流量流向加速器后面的系统时，将不会保留原始客户端的连接信息（例如客户端的 IP 地址和客户端的端口）。这适用于许多应用程序，尤其是那些可供所有用户使用的应用程序，例如公共网站。

对于不具有客户端 IP 地址保留功能的端点，您可以筛选 Global Accelerator 从边缘转发流量时使用的源 IP 地址。通过查看 Global Accelerator 流日志，您可以看到有关传入数据包的源 IP 地址（启用客户端 IP 地址保留时，这些地址也是客户端 IP 地址）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 和在 AWS Global Accelerator 中配置和使用流日志。

具有客户端 IP 地址保留功能的 ENI 和安全组的最佳实践

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

为了支持客户端 IP 地址保留功能，Global Accelerator 会在您的 AWS 账户中创建弹性网络接口，每个存在端点的子网都有一个弹性网络接口。弹性网络接口 是 VPC 中表示虚拟网卡的逻辑网络组件。Global Accelerator 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端点包括应用程序负载均衡器（内部和面向互联网）、带有安全组的网络负载均衡器以及 Amazon EC2 实例。

> **Note**
>
> 在 Global Accelerator 中添加内部应用程序负载均衡器或 EC2 实例端点时，您可以通过将互联网流量定位到私有子网中，让互联网流量直接流入虚拟私有云（VPC）中的端点或从这些端点中流出。有关更多信息，请参阅 AWS Global Accelerator 中的安全 VPC 连接。

Global Accelerator 如何使用弹性网络接口

您具有启用了客户端 IP 地址保留的应用程序负载均衡器或网络负载均衡器端点时，负载均衡器所在的子网数量将决定 Global Accelerator 在您的账户中创建的弹性网络接口的数量。Global Accelerator 会为每个子网创建一个弹性网络接口，这些子网中至少有一个应用程序负载均衡器或网络负载均衡器的弹性网络接口，作为您账户中加速器的前端。

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，然后您将该负载均衡器添加为加速器端点，则 Global Accelerator 会创建两个弹性网络接口，每个子网中一个。
- 示例 2：如果将在子网 A 和子网 B 中具有弹性网络接口的 ALB1 添加到 Accelerator1，然后将在子网 A 和子网 B 中具有弹性网络接口的 ALB2 添加到 Accelerator2，则 Global Accelerator 仅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：如果将在子网 A 和子网 B 中具有弹性网络接口的 ALB1 添加到 Accelerator1，然后将在子网 A 和子网 C 中具有弹性网络接口的 ALB2 添加到 Accelerator2，则 Global Accelerator 会创建三个弹性网络接口：一个在子网 A 中，一个在子网 B 中，一个在子网 C 中。子网 A 中的弹性网络接口为 Accelerator1 和 Accelerator2 提供流量。

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

Global Accelerator 创建的逻辑弹性网络接口并不呈现单台主机、吞吐量瓶颈或单点故障。与其它在可用区或子网中显示为单个弹性网络接口的 AWS 服务（例如网络地址转换（NATI）网关或网络负载均衡器等 服务）一样，Global Accelerator 是作为水平扩缩的高可用性服务实施的。

估算加速器中端点使用的子网数量，以确定 Global Accelerator 将创建的弹性网络接口的数量。在创建加速器之前，请确保有足够的 IP 地址空间容量来容纳所需的弹性网络接口：即每个相关子网至少有一个空闲的 IP 地址。如果您没有足够的空闲 IP 地址空间，则必须为应用程序负载均衡器或网络负载均衡器以及相关的 Global Accelerator 弹性网络接口创建或使用一个有足够空闲 IP 地址空间的子网。

当 Global Accelerator 确定账户中存在并未被加速器中的任何端点使用的弹性网络接口时，Global Accelerator 会删除该接口。

Global Acccelerator 创建的安全组

在使用 Global Accelerator 和安全组时，请查看以下信息和最佳实践。

- 您可以将 Global Accelerator 创建的安全组用作您维护的其他安全组中的源组，但是 Global Accelerator 只能将流量转发到您在 VPC 中指定的目标。
- 如果您修改 Global Accelerator 创建的安全组规则，则端点的运行状况可能会变得不佳。如果发生这种情况，请联系AWS Support 寻求帮助。
- Global Accelerator 会为每个 VPC 创建一个特定的安全组。无论弹性网络接口与哪个子网关联，为特定 VPC 内的端点创建的弹性网络接口均使用同一个安全组。

> **Important**
>
> Global Accelerator 会创建与其弹性网络接口关联的安全组。尽管系统不会阻止，但您不应对这些组的任何安全组设置进行编辑。

具有客户端 IP 地址保留功能的转换端点

如果您尚未为加速器中的端点配置客户端 IP 地址保留，请按照本节中的指南进行操作，添加一个或多个端点，并将其转换到保留用户客户端 IP 地址的端点。您可以选择将应用程序负载均衡器、带有安全组的网络负载均衡器或弹性 IP 地址端节转换到具有客户端 IP 地址保留功能的相应端点（相应的负载均衡器端点或 EC2 实例端点）。

本节介绍了如何使用 AWS Global Accelerator 控制台添加和转换端点。要将 API 操作与 Global Accelerator 结合使用，请参阅 AWS Global Accelerator API 参考。

转换端点以使用客户端 IP 地址保留功能

我们建议您逐步将端点转换到使用客户端 IP 地址保留功能的端点。

- 添加新端点：首先，向 Global Accelerator 中添加将新的负载均衡器或 EC2 实例端点，以便您可以保留客户端 IP 地址。
- 逐步增加流量：然后通过在端点上配置权重，将流量从现有端点逐步转移到新端点。
- 随用随测：将少量流量转移到具有客户端 IP 地址保留功能的新端点后，进行测试以确保您的配置按预期运行。然后，通过调整相应端点的权重，逐渐增加流向新端点的流量比例。

按照以下各节中的步骤转换端点。

支持 Global Accelerator 的所有 AWS 区域 都支持客户端 IP 地址保留功能。有关受支持的 区域的列表，请参阅AWS Global Accelerator 支持的 AWS 区域。

> **Important**
>
> 在开始将流量路由到保留客户端 IP 地址的端点之前，请确保已将允许列表中包含 Global Accelerator 客户端 IP 地址的所有配置都更新为包含用户客户端 IP 地址。

添加具有客户端 IP 地址保留功能的端点

1. 通过以下网址打开 Global Accelerator 控制台：https://console.aws.amazon.com/globalaccelerator/home。
2. 在“加速器”页面上，选择一个加速器。
3. 在侦听器部分中，选择一个侦听器。
4. 在端点组部分中，选择一个端点组。
5. 在端点部分中，选择添加端点。
6. 在添加端点页面找到端点下拉菜单，从中选择支持客户端 IP 地址保留的端点。
7. 在权重字段中，与为现有端点设置的权重相比，选择一个较低的数字。例如，如果相应的应用程序负载均衡器的权重为 255，则可以先为新的应用程序负载均衡器输入权重 5。有关更多信息，请参阅 如何通过端点权重管理流量。
8. 如果需要，在保留客户端 IP 地址下，选择保留地址。
9. 选择 Save changes（保存更改）。

接下来，按照此处的步骤编辑相应的现有端点（要用具有客户端 IP 地址保留功能的新端点替换掉的端点），来降低现有端点的权重，从而减少流向这些端点的流量。

要减少现有端点的流量

1. 在端点组页面上，选择不具有客户端 IP 地址保留功能的现有端点。
2. 选择编辑。
3. 在编辑端点页面的权重字段中，输入一个小于当前数字的数字。例如，如果现有端点的权重为 255，则可以为新端点输入 220 的权重（具有客户端 IP 地址保留功能）。
4. 选择 Save changes（保存更改）。

通过将新端点权重设置为较低的数字，对原始流量的一小部分进行测试后，您可以继续调整原始端点和新端点的权重来逐步转换所有流量。

例如，假设您从权重设置为 200 的现有应用程序负载均衡器开始，然后添加一个新的应用程序负载均衡器端点（该端点具有客户端 IP 地址保留功能），权重设置为 5。通过增加新应用程序负载均衡器的权重和减少原始应用程序负载均衡器的权重，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：

- 原始权重 190/新权重 10

- 原始权重 180/新权重 20
- 原始权重 170/新权重 30，依此类推。

将原始端点的权重降低到 0 后，所有流量（在本示例场景中）都将流向新的应用程序负载均衡器端点（具有客户端 IP 地址保留功能）。

如果您还有其它端点（负载均衡器或 EC2 实例）需要转换到使用客户端 IP 地址保留功能的端点，请重复本节中的步骤进行转移。

如果您需要恢复端点的配置，以使流向该端点的流量不保留客户端 IP 地址，则可以随时这样做：先将不具有客户端 IP 地址保留功能的端点的权重增加到原始值，然后将具有客户端 IP 地址保留功能的端点的权重降低到 0。

AWS Global Accelerator 中的日志记录和监控

您可以使用 Amazon CloudWatch、流日志和 AWS CloudTrail 在 AWS Global Accelerator 中监控加速器。例如，您可以解决与侦听器和端点相关的问题、分析流量模式，以及获取审计所需的信息。

这些日志和监控方法可能会有一些重叠。以下是每种方法的典型用途：

- CloudWatch 指标提供实时信息，无需额外设置即可帮助您解决设置问题。您还可以创建警报来提醒您，例如在出现生产问题时提醒您。
- 流日志提供有关进入加速器并返回到客户端的流量的详细信息。流日志对于解决可达性问题以及为全面审计提供信息非常有用。（请注意，流日志需要设置并使用 Amazon S3 存储。）
- CloudTrail 会自动跟踪您调用 Global Accelerator API 的操作，这对于审计等非常有用。

> **Note**
>
> 您必须在控制台中或使用 AWS CLI 查看美国西部（俄勒冈州）区域中 Global Accelerator 的 CloudWatch 指标和日志。使用 AWS CLI 时，请通过加入以下参数为您的命令指定美国西部（俄勒冈州）区域：`--region us-west-2`。

主题

- 使用 Amazon CloudWatch 与 AWS Global Accelerator
- 在 AWS Global Accelerator 中配置和使用流日志
- 使用 AWS CloudTrail 记录 AWS Global Accelerator API 调用

使用 Amazon CloudWatch 与 AWS Global Accelerator

AWS Global Accelerator 向 Amazon CloudWatch 发布关于加速器的数据点。利用 CloudWatch，您可以按一组有序的时间序列数据（称为指标）来检索关于这些数据点的统计数据。可将指标视为要监控的变量，而将数据点视为该变量随时间变化的值。例如，您可以监控在指定时间段内通过加速器的流量。每个数据点都有相关联的时间戳和可选测量单位。

> **Note**
>
> 您必须在控制台中或使用 AWS CLI 查看美国西部（俄勒冈州）区域中 Global Accelerator 的 CloudWatch 指标和日志。使用 AWS CLI 时，请通过加入以下参数为您的命令指定美国西部（俄勒冈州）区域：`--region us-west-2`。

您可以使用这些指标对初始 Global Accelerator 进行问题排查，帮助确定流量是否到达端点，并在随后返回响应。查看自动记入日志的 CloudWatch 指标，以查看流量是否传输到您的端点，例如网络负载均衡器。其中应该包括从 Global Accelerator 到端点的出站指标，然后从 Global Accelerator 返回客户端的指标，对于端点（例如负载均衡器）也应该有同样的指标。如果流量从 Global Accelerator 流入但未返回，或者未能到达负载均衡器，则可能表明您需要验证配置，确定是否允许流量流经预期端口，以及您的安全组设置是否允许访问。

您还可以使用指标来验证系统是否按照预期运行。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采取行动（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。如果有请求流经加速器，Global Accelerator 会进行测量并按 60 秒的间隔发送其指标。如果没有请求流经加速器，或者指标无数据，则不报告指标。

有关更多信息，请参阅 Amazon CloudWatch 用户指南。

内容

- Global Accelerator 指标
- 加速器的指标维度
- 解决 Global Accelerator TCP 重置问题
- Global Accelerator 指标的统计数据
- 查看适用于您的加速器的 CloudWatch 指标

Global Accelerator 指标

`AWS/GlobalAccelerator` 命名空间包括以下指标。

指标	描述
ActiveFlowCount	Global Accelerator 中某个加速器从客户端到端点的 TCP 和 UDP 并发连接总数。对于在加速器上终止的 TCP 连接，客户端与端点建立的 TCP 连接计为一个流。 您可以利用此指标来更好地了解有多少活跃用户（连接数）正在访问端点，或者确定是否需要扩展资源来处理流量。 报告标准：针对已配置和已启用的加速器进行报告。 统计数据：唯一有用的统计数据是 Sum。 尺寸 • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress
Flows_Dropped_No_Endpoint_Found	由于无 IPv6 端点可用而被丢弃的 TCP IPv6 数据包流总数。例如，如果您的加速器采用双协议栈 IP 地址类型，并且将加速器端点的 IP 地址类型更改为 IPv4，则可能会发生这种情况。 报告标准：针对具有双协议栈 IP 地址类型的加速器进行报告，这些加速器在发生以下情况之一时正在接收 IPv6 流量： • 使用 IPv6 端点传送流量的加速器报告的指标为 0 • 端点配置错误的加速器报告丢弃的流总数 统计数据：唯一有用的统计数据是 Sum。 尺寸 • Accelerator

指标	描述
	• Accelerator, Listener • Accelerator, AcceleratorIPAddress
HealthyEndpointCount	被视为正常运行的端点总数。Global Accelerator 会定期检查标准加速器上的端点状态。这些运行状况检查将自动运行。这些运行状况检查的运行方式和运行时间取决于端点类型和端点运行状况检查选项。要了解更多信息，请参阅 确保加速器的运行状况检查访问权限。 报告标准：针对已配置和已启用的加速器进行报告。 统计数据：最有用的统计工具为 Minimum 和 Maximum。 尺寸 • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup
NewFlowCount	时段内建立的客户端至端点的新 TCP 和 UDP 流（或连接）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。 尺寸 • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress • Accelerator, NetworkProtocol

指标	描述
ProcessedBytesIn	加速器处理的传入字节总数，包括 TCP/IP 标头。此计数包括所有传输到端点的流量。 报告标准：有非零值。 统计数据：唯一有用的统计数据是 Sum。 尺寸 • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress • Accelerator, NetworkProtocol

指标	描述
ProcessedBytesOut	加速器处理的传出字节总数，包括 TCP/IP 标头。此计数来自端点的流量，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。 尺寸 • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress • Accelerator, NetworkProtocol

指标	描述
PacketsProcessed	Global Accelerator 为加速器处理的数据包总数，包括进出终端节点的流量，运行状况检查流量也包括在内。您可借助该指标对特定时间段内的流量进行基准测试。 报告标准：针对已配置和已启用的加速器进行报告。 统计数据：唯一有用的统计数据是 Sum。 尺寸 • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress
UnhealthyEndpointCount	被视为运行不正常的端点总数。Global Accelerator 会定期检查标准加速器上的端点状态。这些运行状况检查将自动运行。这些运行状况检查的运行方式和运行时间取决于端点类型和端点运行状况检查选项。要了解更多信息，请参阅 确保加速器的运行状况检查访问权限。 报告标准：针对已配置和已启用的加速器进行报告。 统计数据：最有用的统计工具为 Minimum 和 Maximum。 尺寸 • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup

指标	描述
TCP_AGA_Reset_Count	AWS Global Accelerator（“AGA”）生成的重置（RST）数据包的总数。使用此指标，您可以确定 Global Accelerator 是否正在终止客户端连接，并将重置发回到客户端端点。 有关评估 Global Accelerator 生成的 TCP RST 并排查相关错误的更多信息，请参阅解决 Global Accelerator TCP 重置问题。 报告标准：在有流量且存在非零值时报告。 统计数据：唯一有用的统计数据是 Sum。 尺寸 • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, AcceleratorIPAddress

指标	描述
TCP_Client_Reset_Count	从客户端发送至端点的重置（RST）数据包的总数。利用此指标，您可以确定客户端能否保持与 Global Accelerator 之间的连接处于开放状态，或者连接是否会提前意外重置。这在一些情况下非常有用，比如最初配置 Global Accelerator 时，此外，在对创建连接重置的客户端进行更改时，也可借此保持可见性。 有关评估 Global Accelerator 生成的 TCP RST 并排查相关错误的更多信息，请参阅解决 Global Accelerator TCP 重置问题。 报告标准：在有流量且存在非零值时报告。 统计数据：唯一有用的统计数据是 Sum。 尺寸 • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, AcceleratorIPAddress

指标	描述
TCP_Endpoint_Reset_Count	从端点发送至客户端的重置（RST）数据包的总数。您可以利用此指标确定客户端端点何时过载。 有关评估 Global Accelerator 生成的 TCP RST 并排查相关错误的更多信息，请参阅解决 Global Accelerator TCP 重置问题。 报告标准：在有流量且存在非零值时报告。 统计数据：唯一有用的统计数据是 Sum。 尺寸 • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, AcceleratorIPAddress

加速器的指标维度

要筛选您的加速器的指标，可以使用以下维度。

维度	描述
Accelerator	按加速器筛选指标数据。按加速器 ID（加速器 ARN 的最后一部分）指定加速器。例如，如果 ARN 是 arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh ，则指定以下内容：**1234abcd-abcd-1234-abcd-1234abcdefgh** 。
Listener	按侦听器筛选指标数据。按侦听器 ID（侦听器 ARN 的最后一部分）指定侦听器。例如，如果 ARN 是 arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-a

维度	描述
	`bcd-1234abcdefgh/listener/0123wxyz` ，则指定以下内容：**`0123wxyz`**。
`EndpointGroup`	按端点组筛选指标数据。例如，按 AWS 区域指定端点组 **`us-east-1`** （全部为小写字母）。
`SourceRegion`	按源区域筛选指标数据，源区域是运行应用程序端点的 AWS 区域的地理区域。源区域是下列区域之一： • NA – 美国与加拿大 • EU – 欧洲 • AP – 亚太地区* • 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

维度	描述
DestinationEdge	按目标边缘筛选指标数据，目标边缘是传输您的客户端流量的 AWS 边缘站点的地理区域。目标边缘是下列区域之一： • NA – 美国与加拿大 • EU – 欧洲 • AP – 亚太地区* • 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
Transport Protocol	按传输协议筛选指标数据：UDP 或 TCP。
AcceleratorIPAddress	按加速器 IP 地址筛选指标数据：即分配至某加速器的静态 IP 地址之一。

解决 Global Accelerator TCP 重置问题

每个加速器都会报告从 Global Accelerator 生成和发送的 TCP 重置（TCP RST）的数量。以下是 Global Accelerator 发送 TCP 重置的常见原因：

- 在客户端或端点使用 FIN 握手或重置关闭连接时，Global Accelerator 将 TCP 连接标记为已关闭。如果客户端或端点通过已关闭的 TCP 连接发送数据包，则 Global Accelerator 会生成 TCP 重置，表示连接已关闭且无法接受流量。
- 如果客户端或端点在空闲超时期限后发送数据，则会收到 Global Accelerator 发来的一个 TCP 重置数据包，以指示连接不再有效。
- 在 TCP 握手期间，如果 Global Accelerator 在与客户端或端点建立连接时收到意外数据包，则 Global Accelerator 会生成 TCP 重置。

如果您看到加速器的 `AGA_Reset_Count` 指标数量稳定，原因在于客户端或端点向已关闭或过期的连接发送了发往 Global Accelerator 的数据。

如果您注意到 `AGA_Reset_Count` 指标急剧增加，并且增长与端点方面的相关指标变化一致，例如纵向扩展、缩减或端点运行状况不佳，则该端点可能已无法访问并触发了 Global Accelerator TCP 重置。如果在调查此问题时需要帮助，请联系 AWS 支持人员。

Global Accelerator 指标的统计数据

CloudWatch 提供基于 Global Accelerator 发布的指标数据点的统计数据。统计数据是在指定的时间段内汇总的指标数据。当请求统计数据时，返回的数据流按指标名称和维度进行识别。维度是用于唯一标识指标的名称/值对。例如，您可以为加速器请求输出已处理的字节，这些字节从欧洲的 AWS 边缘站点（目标边缘为“EU”）传输而来。

以下是您可能认为有用的指标/维度组合示例：

- 查看两个加速器 IP 地址中每个地址所处理的流量（例如 ProcessedBytesOut），以验证您的 DNS 配置是否正确。
- 查看用户流量的地理分布情况，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）。为确定此信息，请查看 ProcessedBytesIn 或 ProcessedBytesOut 指标，并将维度 DestinationEdge 和 SourceRegion 设置为特定值。
- 查看加速器中运行状况不佳的端点数量，并确定它们属于哪些端点组。如果您有大量端点组，这对于帮您快速找到端点出现问题的端点组特别有用。为确定此信息，请查看指标 UnhealthyEndpointCount 以及维度 Accelerator、Listener 和 EndpointGroup。

查看适用于您的加速器的 CloudWatch 指标

您可以使用 CloudWatch 控制台或 AWS CLI 查看加速器的 CloudWatch 指标。在控制台中，这些指标显示为监控图表。如果加速器处于活动状态并且正在接收请求，则监控图表会显示数据点。

您必须在控制台中或使用 AWS CLI 查看美国西部（俄勒冈州）区域中 Global Accelerator 的 CloudWatch 指标。使用 AWS CLI 时，请通过加入以下参数为您的命令指定美国西部（俄勒冈州）区域：`--region us-west-2`。

要使用 CloudWatch 控制台查看指标，请按照《Amazon CloudWatcer 用户指南》中的步骤操作，并选择 GlobalAccelerator 命名空间。如需了解详情，请参阅查看可用指标。

使用 AWS CLI 获取指标的统计数据

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

下面的示例列出了针对您的加速器，每分钟处理的从北美（NA）目的地传入的字节总数。

```
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
```

下面是该命令的示例输出：

```
{
    "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"
        }
    ]
}
```

在 AWS Global Accelerator 中配置和使用流日志

流日志允许您在 AWS Global Accelerator 中捕获有关进出加速器中的网络接口的 IP 地址流量的信息。流日志数据将发布到 Amazon S3，创建流日志后，您可以在其中检索和查看您的数据。

> **Note**
>
> 您必须在控制台中或使用 AWS CLI 查看美国西部（俄勒冈州）区域中 Global Accelerator 的 CloudWatch 指标和日志。使用 AWS CLI 时，请通过加入以下参数为您的命令指定美国西部（俄勒冈州）区域：`--region us-west-2`。

流日志可帮助您处理许多任务。例如，您可以排查特定流量未到达端点的原因，这反过来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您的端点的流量。

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，用于指定 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。捕获窗口最长为 1 分钟。也就是说，日志的发布频率可能会高于每分钟一次，但至少每分钟发布一次。

使用流日志时会收取 CloudWatch Logs 费用，即使日志直接发布到 Amazon S3。有关更多信息，请参阅 Amazon CloudWatch 定价页面上日志选项卡中的已出售日志。

> **Tip**
>
> 将 Amazon Athena 和 Amazon QuickSight 与 Global Accelerator 流日志数据配合使用，可以帮助您解决应用程序的可达性问题、识别安全漏洞，以及概要了解用户如何访问您的应用程序。要了解更多信息，请参阅以下 AWS 博客文章：Analyzing and visualizing AWS Global Accelerator flow logs using Amazon Athena and Amazon QuickSight。

内容

- 启用将流日志发布到 Amazon S3 的功能
- 处理 Amazon S3 中的流日志记录
- 将流日志发布到 Amazon S3
- 日志文件传输时间
- 流日志记录语法

启用将流日志发布到 Amazon S3 的功能

要在 AWS Global Accelerator 中启用流日志，请执行此程序中的步骤。本章的其它章节提供了配置 Amazon S3 存储桶和设置权限的步骤，以便可以发布和访问流日志。

在 AWS Global Accelerator 中启用流日志的步骤

1. 在 AWS 账户中为流日志创建 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. 使用您要在日志文件中使用的 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。

将流日志发布到 Amazon S3

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

要创建用于流日志的 Amazon S3 存储桶，请参阅《Amazon Simple Storage Service 用户指南》中的创建您的第一个 S3 存储桶。

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。也就是说，日志文件每 5 分钟写入一次，并且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，流日志会停止向其中添加流日志记录，将其发布到 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，流日志文件名由流日志的 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信息：

- 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 123456789012 于 UTC 时间 2018 年 11 月 23 日 00:05 为 ID 为 1234abcd-abcd-1234-abcd-1234abcdefgh 的加速器创建的流日志的日志文件的文件夹结构和文件名。

```
amzn-s3-demo-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条 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 汇总的条目。

用于将流日志发布到 Amazon S3 的 IAM 角色

IAM 主体（例如，IAM 角色或用户）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 存储桶以及其中包含的对象都是私有的。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，服务会自动向存储桶附加以下策略，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《Amazon Simple Storage Service 用

户指南》中的使用 Amazon S3 控制台添加存储桶策略。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 123123123123 和 456456456456 将流日志发布到 `log-bucket` 存储桶中的 `flow-logs` 文件夹中。

```
{
    "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**
>
> 我们建议您向日志传输服务主体（而不是单个 AWS 账户 ARN）授予 `AWSLogDeliveryAclCheck` 和 `AWSLogDeliveryWrite` 权限。

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 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 的密钥政策中，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《Amazon Simple Storage Service 用户指南》 中的访问控制列表（ACL）概述。

日志文件传输时间

AWS Global Accelerator 每小时最多可为配置好的加速器提交数次日志文件。一般而言，流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包括请求发生时间段的日期和时间（而不是文件传输日期和时间）的日志文件中。

创建日志文件时，Global Accelerator 会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您的加速器，您就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>
```

版本 1.0 格式不包括 VPC 标识符 `vpc_id`。版本 2.0 格式（包括 `vpc_id`）是在 Global Accelerator 向启用了客户端 IP 地址保留的端点发送流量时生成的。

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`	已记录其流量的加速器的 ID。
`client_ip`	源 IPv4 或 IPv6 地址。
`client_port`	源端口。
`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。

字段	描述
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 或 IPv6。
packets	捕获窗口中传输的数据包的数量。当数据包数量为 0（零）时，流处于活动状态，但在捕获窗口中不显示该方向上的数据包。
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 ACCEPT。
log-status	流日志的日志记录状态： • OK：数据正常记录到选定目标。 • SKIPDATA：捕获窗口中跳过了一些流日志记录。这可能是因为存在内部容量限制或内部错误。
globalaccelerator_source_ip	Global Accelerator 网络接口使用的 IP 地址。如果启用了客户端 IP 地址保留，则此值将设置为“-”（连字符）。 有关更多信息，请参阅 在 AWS Global Accelerator 中保留客户端 IP 地址。
globalaccelerator_source_port	Global Accelerator 网络接口使用的端口。如果启用了客户端 IP 地址保留，则此值设置为 0（零）。 有关更多信息，请参阅 在 AWS Global Accelerator 中保留客户端 IP 地址。
endpoint_region	端点所在的 AWS 区域。

字段	描述
globalaccelerator_region	已对请求进行处理的边缘站点（接入点）。每个边缘站点代码均由含三个字母的代码和一个任意分配的数字组成，例如 DFW3。三个字母代码通常对应邻近节点位置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	流量方向。表示进入 Global Accelerator 网络（INGRESS）或返回客户端（EGRESS）的流量。
vpc_id	VPC 标识符。当 Global Accelerator 向启用了客户端 IP 地址保留的端点发送流量时，会包含在版本 2.0 流日志中。

如果某个字段不适用于特定记录，则记录会针对该条目显示一个“-”符号。

使用 AWS CloudTrail 记录 AWS Global Accelerator API 调用

AWS Global Accelerator 与 AWS CloudTrail 集成，后者是在 Global Accelerator 中记录用户、角色或 AWS 服务所执行操作的服务。CloudTrail 将对 Global Accelerator 的所有 API 调用均作为事件捕获，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 控制台中的 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 用户指南。

CloudTrail 中的 Global Accelerator 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。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 服务事件一同保存在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

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记录时，此跟踪记录应用于所有区域。此跟踪记录在 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 Simple Storage Service (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
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

CloudTrail 记录所有 Global Accelerator 操作，AWS Global Accelerator API 参考中介绍了这些操作。例如，对 `CreateAccelerator`、`ListAccelerators` 和 `UpdateAccelerator` 操作的调用将在 CloudTrail 日志文件中生成条目。

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management (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。

在事件历史记录中查看 Global Accelerator 事件

CloudTrail 可让您在 Event history（事件历史记录）中查看最新事件。要查看 Global Accelerator API 请求事件，您必须在控制台顶部的“区域”选择器中选择美国西部（俄勒冈州）。有关更多信息，请参阅《AWS CloudTrail 用户指南》中的使用 CloudTrail 事件历史记录查看事件。

了解 Global Accelerator 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。每个 JSON 格式的 CloudTrail 日志文件均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。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

下面的示例显示了一个 CloudTrail 日志条目，其中包含以下 Global Accelerator 操作：

- 列出一个账户的加速器：`eventName` 为 `ListAccelerators`。
- 创建侦听器：`eventName` 为 `CreateListener`。
- 更新侦听器：`eventName` 为 `UpdateListener`。
- 描述侦听器：`eventName` 为 `DescribeListener`。
- 列出一个账户的侦听器：`eventName` 为 `ListListeners`。
- 删除侦听器：`eventName` 为 `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": [
            {
              "ipAddressFamily": "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 中的安全性

AWS 的云安全性的优先级最高。为了满足对安全性最敏感的组织的需求，我们打造了具有超高安全性的数据中心和网络架构。作为 AWS 的客户，您也可以从这些数据中心和网络架构受益。

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

- 云的安全性 – AWS 负责保护在 AWS Cloud 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。第三方审核员定期测试和验证我们的安全性的有效性，作为 AWS Compliance Programs 的一部分。要了解适用于 AWS Global Accelerator 的合规性计划，请参阅按合规性计划提供的范围内 AWS 服务。
- 云中的安全性：您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Global Accelerator 时应用责任共担模型。以下主题说明如何配置 Global Accelerator 以实现您的安全性和合规性目标。您还会了解如何使用其它 AWS 服务以帮助您监控和保护 Global Accelerator 资源。

内容

- AWS Global Accelerator 的 Identity and Access Management
- AWS Global Accelerator 中的安全 VPC 连接
- AWS Global Accelerator 中的日志记录和监控
- AWS Global Accelerator 的合规性验证
- AWS Global Accelerator 中的弹性
- AWS Global Accelerator 中的基础设施安全性

AWS Global Accelerator 的 Identity and Access Management

AWS Identity and Access Management（IAM）是一项 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制可以通过身份验证（登录）和授权（具有权限）使用 Global Accelerator 资源的人员。IAM 是一项无需额外费用即可使用的AWS 服务。

内容

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- AWS Global Accelerator 如何与 IAM 配合使用
- AWS Global Accelerator 的基于身份的策略示例
- AWS Global Accelerator的服务相关角色
- 适用于 AWS Global Accelerator 的 AWS 托管式策略
- 将基于标签的策略与 AWS Global Accelerator 配合使用
- 对 AWS Global Accelerator 身份和访问进行故障排除

受众

使用 AWS Identity and Access Management（IAM）的方式因您可以在 Global Accelerator 中执行的操作而异。

服务用户 – 如果使用 Global Accelerator 服务来完成任务，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Global Accelerator 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Global Accelerator 中的功能，请参阅对 AWS Global Accelerator 身份和访问进行故障排除。

服务管理员 – 如果您在公司负责管理 Global Accelerator 资源，则您可能具有 Global Accelerator 的完全访问权限。您有责任确定您的服务用户应访问哪些 Global Accelerator 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Global Accelerator 搭配使用的更多信息，请参阅AWS Global Accelerator 如何与 IAM 配合使用。

IAM 管理员 – 如果您是 IAM 管理员，您可能希望了解有关如何编写策略以管理对 Global Accelerator 的访问权限的详细信息。要查看您可在 IAM 中使用的 Global Accelerator 基于身份的策略示例，请参阅 AWS Global Accelerator 的基于身份的策略示例。

使用身份进行身份验证

身份验证是您使用身份凭证登录 AWS 的方法。您必须作为 AWS 账户根用户、IAM 用户或通过代入 IAM 角色进行身份验证（登录到 AWS）。

您可以使用通过身份源提供的凭证以联合身份登录到 AWS。AWS IAM Identity Center（IAM Identity Center）用户、您公司的单点登录身份验证以及您的 Google 或 Facebook 凭证都是联合身份的示例。

当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合身份验证访问 AWS 时，您就是在间接代入角色。

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

如果您以编程方式访问 AWS，则 AWS 将提供软件开发工具包 (SDK) 和命令行界面 (CLI)，以便使用您的凭证以加密方式签署您的请求。如果您不使用 AWS 工具，则必须自行对请求签名。有关使用建议的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的 AWS 签名版本 4。

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

AWS 账户 根用户

当您创建 AWS 账户 时，最初使用的是一个对账户中所有 AWS 服务 和资源拥有完全访问权限的登录身份。此身份称为 AWS 账户 根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 AWS 服务。

联合身份是来自企业用户目录、Web 身份提供程序、AWS Directory Service、Identity Center 目录的用户，或任何使用通过身份源提供的凭证来访问 AWS 服务 的用户。当联合身份访问 AWS 账户 时，他们代入角色，而角色提供临时凭证。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和组，也可以连接并同步到您自己的身份源中的一组用户和组以跨所有 AWS 账户 和应用程序使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？

IAM 用户和群组

IAM 用户是 AWS 账户 内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些

特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 对于需要长期凭证的使用场景定期轮换访问密钥。

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

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

IAM 角色是 AWS 账户 中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。要在 AWS Management Console 中临时代入 IAM 角色，可以从用户切换到 IAM 角色（控制台）。您可以调用 AWS CLI 或 AWS API 操作或使用自定义网址以担任角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的 权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。
- 跨服务访问：某些 AWS 服务使用其它 AWS 服务中的特征。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service (Amazon S3) 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话：当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用 AWS 服务 的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务 委派权限的角色。
- 服务相关角色 – 服务相关角色是与 AWS 服务 关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 AWS 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。

- 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实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您将创建策略并将其附加到 AWS 身份或资源，以控制 AWS 中的访问。策略是 AWS 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）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。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

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

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

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

基于身份的策略

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

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管式策略是可以附加到 AWS 账户 中的多个用户、组和角色的独立策略。托管式策略包括 AWS 托管

式策略和客户管理型策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

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

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

访问控制列表 (ACL)

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

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

其他策略类型

AWS 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCP) – SCP 是 JSON 策略，指定了组织或组织单元 (OU) 在 AWS Organizations 中的最大权限。AWS Organizations 服务可以分组和集中管理您的企业拥有的多个 AWS 账户 账户。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体（包括每个 AWS 账户根用户）的权限。有关组织和 SCP 的更多信息，请参阅《AWS Organizations User Guide》中的 Service control policies。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的

策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

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

AWS Global Accelerator 如何与 IAM 配合使用

在使用 IAM 管理对 Global Accelerator 的访问权限之前，您应该了解哪些 IAM 功能可用于 Global Accelerator。

要查看显示 AWS 服务如何与大多数 IAM 功能结合使用的类似高级视图的表格，请参阅《IAM 用户指南》中的与 IAM 结合使用的 AWS 服务。

可以与 AWS Global Accelerator 配合使用的 IAM 功能

IAM 功能	Global Accelerator 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACL	是
ABAC（策略中的标签）	部分
临时凭证	是
主体权限	是
服务角色	否

IAM 功能	Global Accelerator 支持
服务相关角色	是

Global Accelerator 的基于身份的策略

支持基于身份的策略：是

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

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

要查看 Global Accelerator 基于身份的策略的示例，请参阅 AWS Global Accelerator 的基于身份的策略示例。

Global Accelerator 内基于资源的策略

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。

Global Accelerator 的策略操作

支持策略操作：是

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

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

在策略中包含操作以授予执行关联操作的权限。

要查看 Global Accelerator 操作的列表，请参阅《服务授权参考》中的 AWS Global Accelerator 定义的操作。

Global Accelerator 中的策略操作在操作前使用以下前缀：

```
aws-globalaccelerator
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "aws-globalaccelerator:action1",
      "aws-globalaccelerator:action2"
         ]
```

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

```
"Action": "aws-globalaccelerator:Describe*"
```

要查看 Global Accelerator 基于身份的策略的示例，请参阅 AWS Global Accelerator 的基于身份的策略示例。

Global Acelerator 的策略资源

支持策略资源：是

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

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

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

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

在《服务授权参考》中，您可以看到以下与 Global Accelerator 相关的信息：

- 要查看 Global Accelerator 资源类型及其 ARN 的列表，请参阅 AWS Global Accelerator 定义的资源。
- 要了解可以使用每个资源的 ARN 指定的操作，请参阅 AWS Global Accelerator 定义的操作。

要查看 Global Accelerator 基于身份的策略的示例，请参阅 AWS Global Accelerator 的基于身份的策略示例。

Global Accelerator 的策略条件键

支持特定于服务的策略条件键：是

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

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

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

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

AWS 支持全局条件键和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅《IAM 用户指南》中的 AWS 全局条件上下文键。

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

要查看 Global Accelerator 基于身份的策略的示例，请参阅 AWS Global Accelerator 的基于身份的策略示例。

Global Acelerator 中的 ACL

支持 ACL：是

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

ABAC 与 Global Accelerator

支持 ABAC（策略中的标签）：部分支持

Global Accelerator 部分支持策略中的标签。它支持标记一种资源，即加速器。要了解有关在策略声明条件中使用标签的更多信息，以及查看基于资源上的标签来限制对该资源的访问的示例策略，请参阅将基于标签的策略与 AWS Global Accelerator 配合使用。

有关为 Global Accelerator 资源添加标签的更多信息，请参阅在 AWS Global Accelerator 中添加标签。

要了解有关在策略中使用标签的更多信息，请查看以下信息。

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

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

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

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

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

将临时凭证用于 Global Accelerator

支持临时凭证：是

某些 AWS 服务 在您使用临时凭证登录时无法正常工作。有关更多信息，包括 AWS 服务 与临时凭证配合使用，请参阅 IAM 用户指南中的使用 IAM 的 AWS 服务。

如果您不使用用户名和密码而用其它方法登录到 AWS Management Console，则使用临时凭证。例如，当您使用贵公司的单点登录（SSO）链接访问 AWS 时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 AWS CLI 或者 AWS API 创建临时凭证。之后，您可以使用这些临时凭证访问 AWS。AWS 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Global Accelerator 的跨服务主体权限

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用 AWS 服务 的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Global Acelerator 的服务角色

支持服务角色：否

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

Global Accelerator 的服务相关角色

支持服务相关角色：是

服务相关角色是一种与 AWS 服务 相关的服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 AWS 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。

要了解 Global Accelerator 的服务相关角色的更多信息，请参阅 AWS Global Accelerator的服务相关角色。

有关在 AWS 中创建或管理服务相关角色的大概详细信息，请参阅与 IAM 协同工作的 AWS 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

AWS Global Accelerator 的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Global Accelerator 资源的权限。他们也无法使用 AWS Management Console、AWS Command Line Interface（AWS CLI）或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关 Global Accelerator 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅《服务授权参考》中的 AWS Global Accelerator 的操作、资源和条件键。

主题

- 策略最佳实践
- 创建 Global Accelerator 加速器
- 使用 Global Accelerator 控制台
- 使用 Global Accelerator API 操作
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Global Accelerator 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- AWS 托管策略及转向最低权限许可入门 – 要开始向用户和工作负载授予权限，请使用 AWS 托管策略来为许多常见使用场景授予权限。您可以在 AWS 账户 中找到这些策略。我们建议通过定义特定于您的使用场景的 AWS 客户管理型策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略或工作职能的 AWS 托管策略。
- 应用最低权限 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定（AWS 服务例如 AWS CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证（MFA） – 如果您所处的场景要求您的 AWS 账户 中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

创建 Global Accelerator 加速器

要创建 AWS Global Accelerator 加速器，用户必须有权创建与 Global Accelerator 关联的服务相关角色。

为确保用户拥有在 Global Accelerator 中创建加速器的适当权限，请为用户附加如下策略。

> **Note**
>
> 如果您创建的基于身份的权限策略比以下策略更严格，则采用更严格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 Global Accelerator 控制台

要访问 AWS Global Accelerator 控制台，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您的 AWS 账户 中的 Global Accelerator 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策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于只需要调用 AWS CLI 或 AWS API 的用户，无需为其提供最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍可使用 Global Accelerator 控制台，还请将 Global Accelerator `GlobalAcceleratorReadOnlyAccess` 或 `GlobalAcceleratorFullAccess` AWS 托管策略添加到实体。

如果用户只需要在控制台中查看信息或调用 AWS Command Line Interface 或 API（使用 `List*` 或 `Describe*` 操作），则附加第一个策略 `GlobalAcceleratorReadOnlyAccess`。

请将第二个策略 `GlobalAcceleratorFullAccess` 附加到需要创建加速器或更新加速器的用户。完全访问策略包括 Global Accelerator 的完全权限以及 Amazon EC2 和 Elastic Load Balancing 的描述权限。

> **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，则拥有该策略的用户将无法为加速器添加 Amazon EC2 和 Elastic Load Balancing 资源。

有关更多信息，请参阅 Global Accelerator 的 AWS 托管策略页面或《IAM 用户指南》中的向用户添加权限。

使用 Global Accelerator API 操作

AWS Global Acelerator 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 Global Accelerator 中完成操作。

例如，以下策略允许用户执行 `CreateAccelerator` 操作以通过编程方式在 AWS 账户中创建加速器：

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

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管策略。此策略包括在控制台上完成此操作或者以编程方式使用 AWS CLI 或 AWS API 所需的权限。

```
{
    "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": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 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独特类型的 IAM 角色，它与 Global Accelerator 直接相关。服务相关角色是由 Global Accelerator 预定义的，包含该服务代表您调用其它 AWS 服务所需的所有权限。

服务相关角色可让您更轻松地设置 Global Accelerator，因为您不必手动添加必要的权限。Global Accelerator 定义其服务相关角色的权限，除非另外定义，否则只有 Global Accelerator 可以代入其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

只有在首先删除服务相关角色的相关资源后，才能删除该角色。这将保护您的 Global Accelerator 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 配合使用的 AWS 服务，并查找 Service-linked role（服务相关角色）列中显示为 Yes（是）的服务。选择是和链接，查看该服务的服务相关角色文档。

Global Accelerator 的服务相关角色权限

AWS Global Accelerator 使用名为 AWSServiceRoleForGlobalAccelerator 的服务相关角色。此角色允许 Global Accelerator 访问您账户中的资源，例如负载均衡器和其它端点，以帮助确保您只能添加配置为与 Global Accelerator 配合使用的资源。AWSServiceRoleForGlobalAccelerator 角色还允许 Global Accelerator 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 Global Accelerator API 操作时，Global Accelerator 会自动创建名为 AWSServiceRoleForGlobalAccelerator 的角色。在 Global Accelerator 中使用加速器需要此角色。AWSServiceRoleForGlobalAccelerator 角色的 ARN 与以下内容类似：

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

服务相关角色权限

Global Accelerator 使用名为 AWSServiceRoleForGlobalAccelerator 的服务相关角色来访问资源和配置以检查准备情况。此服务相关角色使用托管策略 `AWSGlobalAcceleratorSLRPolicy`。

AWSServiceRoleForGlobalAccelerator 服务相关角色信任以下服务来代入该角色：

- `globalaccelerator.amazonaws.com`

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

您必须配置权限以允许 IAM 实体（如用户、组或角色）删除 Global Accelerator 服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

创建 Global Accelerator 的服务相关角色

不要手动创建 Global Accelerator 的服务相关角色。在首次创建加速器时，该服务会自动为您创建角色。如果移除 Global Accelerator 资源并删除服务相关角色，则在创建新加速器时，该服务会自动重新创建该角色。

编辑 Global Acelerator 服务相关角色

Global Accelerator 不允许您编辑 AWSServiceRoleForGlobalAccelerator 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 IAM 用户指南 中的编辑服务相关角色。

删除 Global Acelerator 服务相关角色

如果不再需要使用 Global Accelerator，建议删除服务相关角色。这样，就不会主动监控或维护您的未使用实体。但是，您必须先清除账户中的 Global Accelerator 资源，然后才能手动删除角色。

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 创建加速器。

> **Note**
>
> 如果您已禁用并删除加速器，但 Global Accelerator 尚未完成更新，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。

要手动删除 AWSServiceRoleForGlobalAccelerator 服务相关角色，请执行以下操作

1. 登录 AWS Management Console，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《IAM 用户指南》中的删除服务相关角色。

Global Accelerator 服务相关角色的策略更新

有关 `AWSGlobalAcceleratorSLRPolicy`（即 Global Accelerator 服务相关角色的 AWS 托管策略）的更新，请参阅 AWS 托管策略更新表。您也可以在 AWS Global Accelerator 文档历史记录页面上订阅自动 RSS 提醒。

适用于 AWS Global Accelerator 的 AWS 托管式策略

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

请记住，AWS 托管式策略可能不会为您的特定使用场景授予最低权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户托管式策略来进一步减少权限。

您无法更改 AWS 托管式策略中定义的权限。如果 AWS 更新在 AWS 托管式策略中定义的权限，则更新会影响该策略所附加到的所有主体身份（用户、组和角色）。当新的 AWS 服务 启动或新的 API 操作可用于现有服务时，AWS 最有可能更新 AWS 托管式策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略：AWSServiceRoleForGlobalAccelerator

您不能将 `AWSServiceRoleForGlobalAccelerator` 附加到自己的 IAM 实体。此策略将附加到某个允许 AWS Global Accelerator 访问由 Global Accelerator 使用或管理的 AWS 服务和资源的服务相关角色。有关更多信息，请参阅 AWS Global Accelerator的服务相关角色。

AWS 托管策略：GlobalAcceleratorReadOnlyAccess

您可以将 `GlobalAcceleratorReadOnlyAccess` 附加到 IAM 实体。此策略授予对 Global Accelerator 中使用加速器的操作的只读访问权限。如果用户只需要在控制台中查看信息或调用 AWS Command Line Interface 或 API（使用 `List*` 或 `Describe*` 操作），这很有用。

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

AWS 托管策略：GlobalAcceleratorFullAccess

您可以将 `GlobalAcceleratorFullAccess` 附加到 IAM 实体。此策略授予对 Global Accelerator 中使用加速器的操作的完全访问权限。将此策略附加到需要对 Global Accelerator 的完全访问权限的 IAM 用户和其它主体。

> **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，则拥有该策略的用户将无法为加速器添加 Amazon EC2 和 Elastic Load Balancing 资源。

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

AWS 托管策略的 Global Accelerator 更新

查看有关 Global Accelerator 的 AWS 托管策略更新的详细信息（从该服务开始跟踪这些更改开始）。有关此页面更改的自动提示，请订阅 Global Accelerator 文档历史记录页面上的 RSS 源。

更改	描述	日期
AWSGlobalAcceleratorSLRPolicy – 更新的策略	Global Accelerator 添加了新的权限来描述负载均衡器上的目标组。 Global Accelerator 使用 `elasticloadbalancing:DescribeTargetGroups` 识别目标类型为 `ip` 的负载均衡器，该目标类型是 Global Accelerator 中双堆栈负载均衡器端点不支持的目标类型。	2023 年 10 月 20 日
AWSGlobalAcceleratorSLRPolicy – 更新的策略	Global Accelerator 添加了新权限来描述负载均衡器上的侦听器以及 EC2 实例上的地址。	2023 年 5 月 23 日

更改	描述	日期
	Global Accelerator 使用 `elasticloadbalancing:DescribeListeners` 支持根据侦听器配置为负载均衡器制定侦听器管理决策。 Global Accelerator 使用 `ec2:DescribeAddresses` 向加速器添加弹性 IP 地址端点。	
AWSGlobalAcceleratorSLRPolicy – 更新的策略	Global Acelerator 添加了新权限以支持 IPv6 地址。 Global Accelerator 使用 `ec2:AssignIpv6Addresses` 将客户子网上的 Global Accelerator ENI 更新为用于发送和接收 IPv6 流量的 IPv6 地址，并在不再需要 IPv6 地址时使用 `UnassignIpv6Addresses` 将其移除。	2021 年 11 月 15 日
AWSGlobalAcceleratorSLRPolicy – 更新的策略	Global Accelerator 添加了新权限，以帮助 Global Accelerator 诊断错误。 Global Accelerator 使用 `ec2:DescribeRegions` 确定客户所在的 AWS 区域，这可以帮助 Global Accelerator 对错误进行故障排除。	2021 年 5 月 18 日
Global Accelerator 开始跟踪更改	Global Accelerator 开始跟踪其 AWS 托管策略的更改。	2021 年 5 月 18 日

将基于标签的策略与 AWS Global Accelerator 配合使用

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。为资源添加标签后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资源批量授予访问权限。在创建资源时，或在以后更新资源时，您可以将此标签反复应用于相关资源。

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。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 Global Accelerator 中，只有加速器可以包含标签。有关在 Global Accelerator 中添加标签的更多信息，请参阅在 AWS Global Accelerator 中添加标签。

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。

例如，AWS `GlobalAcceleratorFullAccess` 托管用户策略为用户提供对任意资源执行任意 Global Accelerator 操作的无限权限。以下策略限制此权力并拒绝未经授权的用户对生产加速器执行任意 Global Accelerator 操作的权限。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"
            }
         }
      }
   ]
}
```

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

对 AWS Global Accelerator 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 Global Accelerator 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Global Accelerator 中执行操作
- 我无权执行 iam:PassRole
- 我想要允许我的 AWS 账户 之外的用户访问我的 Global Accelerator 资源

我无权在 Global Accelerator 中执行操作

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `aws-globalaccelerator:`*`GetWidget`* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: aws-
globalaccelerator:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 `mateojackson` 用户的策略，以允许使用 `aws-globalaccelerator:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

如果您需要帮助，请联系 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam:PassRole

如果收到错误，则表明您无权执行 `iam:PassRole` 操作，必须更新策略以允许您将角色传递给 Global Accelerator。

有些 AWS 服务 允许将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Global Accelerator 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系 AWS 管理员。您的管理员是提供登录凭证的人。

我想要允许我的 AWS 账户 之外的用户访问我的 Global Accelerator 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Global Accelerator 是否支持这些功能，请参阅 AWS Global Accelerator 如何与 IAM 配合使用。
- 要了解如何为您拥有的 AWS 账户中的资源提供访问权限，请参阅《IAM 用户指南》中的为您拥有的另一个 AWS 账户中的 IAM 用户提供访问权限。
- 要了解如何为第三方 AWS 账户 提供您的资源的访问权限，请参阅 IAM 用户指南中的为第三方拥有的 AWS 账户 提供访问权限。
- 要了解如何通过联合身份验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

AWS Global Accelerator 中的安全 VPC 连接

在 AWS Global Accelerator 中添加网络负载均衡器、内部应用程序负载均衡器或 Amazon EC2 实例端点时，通过将互联网流量定向到私有子网，使互联网流量能够直接流入和流出虚拟私有云（VPC）中

的端点。包含负载均衡器或 EC2 实例的 VPC 必须附带互联网网关，以表示 VPC 接受互联网流量。但是，在负载均衡器或 EC2 实例上，不需要公有 IP 地址。您也不需要子网的相关互联网网关路由。

这与典型的互联网网关用例不同，在典型的互联网网关用例中，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（即带有互联网网关路由的子网）中，当使用 Global Accelerator 处理互联网流量时，Global Accelerator 也会覆盖典型的互联网路由，并且通过 Global Accelerator 到达的所有逻辑连接也将通过 Global Accelerator（而不是通过互联网网关）返回。

> **Note**
>
> 为 Amazon EC2 实例使用公有 IP 地址和公有子网并不典型，但可以通过它们设置配置。安全组适用于到达实例的任何流量，包括来自 Global Accelerator 的流量以及分配给实例 ENI 的任何公有或弹性 IP 地址。使用私有子网确保流量只能由 Global Accelerator 传送。
> 要了解有关使用 ENI、安全组和 Global Accelerator 的更多信息，请参阅 对保留客户端 IP 地址的端点的要求。

在考虑网络边界问题和配置与互联网访问管理相关的 IAM 权限时，请记住这些信息。有关控制对 VPC 的互联网访问权限的更多信息，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 Global Accelerator 和 AWS 解决方案的可用性和性能的重要环节。您应该从 AWS 解决方案的所有部分收集监控数据，以便您可以更轻松地调试多点故障（如果发生）。AWS 提供了多种工具来监控您的 Global Accelerator 资源和活动并对潜在事件做出响应：

Global Accelerator 可提供以下三种主要的日志记录和跟踪途径：

Amazon CloudWatch 指标和警报

使用 CloudWatch 可以实时监控您的 AWS 资源以及在 AWS 上运行的应用程序。部署加速器后，CloudWatch 就会开始收集和跟踪 Global Accelerator 的指标。指标是您可以查看的变量，以确认流量是否流动，或者您可以随时间推移进行衡量。

例如，您可以使用指标来验证流量是否通过 Global Accelerator 流向您的端点，然后流回客户端，并帮助解决问题。您还可以创建监视特定指标的警报，当指标在一段时间内超出阈值时，它们会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 使用 Amazon CloudWatch 与 AWS Global Accelerator。

Global Accelerator 流日志

服务器流日志是您在 Global Accelerator 中设置的日志，用于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，用于安全和访问审计的应用程序。有关更多信息，请参阅 在 AWS Global Accelerator 中配置和使用流日志。

AWS CloudTrail 日志

CloudTrail 提供了用户、角色或 AWS 服务在 Global Accelerator 中所执行操作的记录。CloudTrail 将对 Global Accelerator 的所有 API 调用均作为事件捕获，包括来自 Global Accelerator 控制台的调用和对 Global Accelerator API 的代码调用。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

要了解某个 AWS 服务是否在特定合规性计划范围内，请参阅 合规性计划范围内的 AWS 服务，然后选择您感兴趣的合规性计划。有关常规信息，请参阅 AWS 合规性计划 。

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

您使用 AWS 服务 的合规性责任取决于您数据的敏感度、贵公司的合规性目标以及适用的法律法规。AWS 提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南 – 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署以安全性和合规性为重点的基准环境的步骤。
- 亚马逊云科技上的 HIPAA 安全性和合规性架构设计– 该白皮书介绍了公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。

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

- AWS 合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- AWS 客户合规指南：从合规角度了解责任共担模式。这些指南总结了保护 AWS 服务 的最佳实践，并将指南映射到跨多个框架的安全控制，包括美国国家标准与技术研究院（NIST）、支付卡行业安全标准委员会（PCI）和国际标准化组织（ISO）。

- AWS Config 开发人员指南中的使用规则评估资源 - 此 AWS Config 服务评测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 向您提供 AWS 中安全状态的全面视图。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty – 该 AWS 服务 通过监控您的环境中是否存在可疑和恶意活动，来检测您的 AWS 账户、工作负载、容器和数据面临的潜在威胁。GuardDuty 可以通过满足某些合规性框架规定的入侵检测要求，来协助您满足各种合规性要求，如 PCI DSS。
- AWS Audit Manager——此 AWS 服务 可帮助您持续审计您的 AWS 使用情况，以简化管理风险以及与相关法规和行业标准的合规性的方式。

AWS Global Accelerator 中的弹性

AWS全球基础架构围绕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架构相比，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 全球基础架构。

除了支持 AWS 全球基础设施之外，Global Accelerator 还提供了以下功能，以帮助支持数据弹性：

- 与 AWS 中的可用区类似，网络区域是一个具有自己的物理基础设施集的隔离单元。创建加速器时，Global Accelerator 会为您提供一组静态 IP 地址：两个静态 IPv4 地址用于 IP 地址类型为 IPv4 的加速器，或者四个静态 IP 地址用于双堆栈加速器（两个 IPv4 地址和两个 IPv6 地址）。Global Accelerator 从每个 IP 地址系列的唯一 IP 子网中为每个网络区域提供一个静态 IP 地址。如果由于某些客户端网络阻止 IP 地址或网络中断而导致网络区域中的一个地址不可用，则客户端应用程序可以重试来自其它隔离网络区域的正常静态 IP 地址。
- Global Accelerator 持续监控所有端点的运行状况。当 Global Accelerator 确定活动端点运行状况不佳时，会立即开始将流量定向到另一个可用端点。这使您可以为 AWS 上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

作为一项托管式服务，AWS Global Accelerator 受 AWS 全球网络安全保护。有关 AWS 安全服务以及 AWS 如何保护基础设施的信息，请参阅 AWS 云安全。要按照基础架构安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的 基础架构保护。

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

- 传输层安全性协议 (TLS) 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

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

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）。

服务配额控制台提供有关 Global Accelerator 配额的信息。除了查看默认配额外，还可以使用服务配额控制台为可调整的配额请求提高配额。

您必须位于美国东部（弗吉尼亚州北部）（us-east-1）区域，才能在服务配额控制台中管理服务限制并请求增加 Global Accelerator 的配额。Global Accelerator 服务配额在美国东部（弗吉尼亚州北部）区域中管理，因为 AWS 全球服务配额是在此区域定义的。在其它任何 AWS 区域，您都不会看到 Global Accelerator 配额，也无法更改配额。但是请注意，所有 Global Accelerator API 操作都必须在美国西部（俄勒冈州）（us-west-2）区域中运行。

主题

- 常规配额
- 每个端点组的端点配额
- 相关限额

常规配额

以下是 Global Accelerator 的总配额。

实体	限额
每个 AWS 账户的标准加速器	20 您可以请求提高配额。
每个 AWS 账户的自定义路由加速器	10 您可以请求提高配额。
每个加速器的侦听器数	10 您可以请求提高配额。
所有侦听器中每个加速器的端点组数	42

实体	限额
Global Accelerator 可指向的 AWS 区域，涵盖所有侦听器和端点组	42 如果您的加速器有一个侦听器，则可以使用加速器的端点组配置指向 Global Accelerator 支持的所有区域。 请注意，随着侦听器数量的增加，您可以使用端点组在加速器中引用的最大区域数量会按比例减少。您的（侦听器总数）x（端点组数量）不得超过 42。
每个侦听器的端口范围数	10
每个终端节点组的端口覆盖数	10 您可以请求提高配额。
每个跨账户附件的主体	10 您可以请求提高配额。
每个跨账户附件的资源	500

每个端点组的端点配额

以下是适用于端点组中端点数量的 Global Accelerator 配额。

实体	描述	限额
具有多个端点类型的端点组	包含多个端点类型的端点组中的端点数量。	10
仅含应用程序负载均衡器的端点组	仅包含应用程序负载均衡器端点的端点组中的应用程序负载均衡器数量。	10
仅含网络负载均衡器的端点组	仅包含网络负载均衡器端点的端点组中的网络负载均衡器数量。	10 您可以请求提高配额。

实体	描述	限额
仅含 Amazon EC2 实例的端点组	仅包含 E2 实例端点的端点组中的 EC2 实例数量。	10 您可以请求提高配额。
仅含弹性 IP 地址的端点组	仅包含弹性 IP 地址端点的端点组中的弹性 IP 地址数量。	10 您可以请求提高配额。
仅含 Amazon Virtual Private Cloud 子网的端点组	仅包含子网端点的端点组中的 Amazon VPC 子网数量。	10 您可以请求提高配额。

相关限额

除 Global Accelerator 中的配额外，还有一些配额适用于您用作加速器端点的资源。有关更多信息，请参阅下列内容：

- 《Amazon EC2 用户指南》中的弹性 IP 地址配额。
- 《Amazon EC2 用户指南》中的 Amazon EC2 服务配额。
- 《网络负载均衡器用户指南》中的网络负载均衡器的配额。
- 《应用程序负载均衡器用户指南》中的应用程序负载均衡器的配额。
- 《Amazon VPC 用户指南》中的 Amazon VPC 配额。

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

- AWS Global Accelerator 的 API 参考和产品信息
- 获取支持
- 来自 AWS 博客网站的提示

AWS Global Accelerator 的 API 参考和产品信息

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 – 完整说明了 API 操作、参数和数据类型，以及该服务返回的错误列表。
- Global Accelerator 新增功能 – 发布了新的 Global Accelerator 功能并新增了边缘站点。
- AWS Global Accelerator 产品信息 – 提供 Global Accelerator 相关信息的主要网页，包括功能和定价信息。
- 使用条款 – 有关我们的版权和商标以及您的账户、许可、网站访问和其他主题的详细信息。

获取支持

我们通过多种形式支持 Global Accelerator。

- 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。
- 支持 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，该服务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 AWS 博客网站的提示

AWS 博客网站上有许多文章可帮助您使用 AWS 服务，包括以下关于 Global Accelerator 的博客文章：

- Use AWS Global Accelerator to improve application performance
- Best practices for deployment with AWS Global Accelerator
- Announcing cross-account support for AWS Global Accelerator
- Accessing an Amazon API Gateway via static IP addresses provided by AWS Global Accelerator
- AWS Global Accelerator Custom Routing with Amazon Elastic Kubernetes Service
- Deploying multi-Region applications in AWS using AWS Global Accelerator
- Maximising application resiliency with AWS Global Accelerator
- Starting Small with AWS Global Accelerator
- Traffic management with AWS Global Accelerator
- Analyzing and visualizing AWS Global Accelerator flow logs using Amazon Athena and Amazon QuickSight

有关 AWS Global Accelerator 博客的完整列表，请参阅 AWS 博客文章的“联网和内容分发”类别中的 AWS Global Accelerator。

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
- 文档最新更新时间：2024 年 3 月 27 日

更改	描述	日期
添加了对 BYOIP 的跨账户支持	Global Accelerator 现在支持另外五个 CloudWatch 指标，您可以使用这些指标更轻松地检测加速器端点的问题。有关更多信息，请参阅使用 Amazon CloudWatch 与 AWS Global Accelerator。	2024 年 3 月 27 日
添加了对 BYOIP 的跨账户支持	Global Accelerator 现在支持跨 AWS 账户使用自带 IP（BYOIP）地址。有关更多信息，请参阅在 AWS Global Accelerator 中使用跨账户附件和资源。	2024 年 3 月 25 日
为网络负载均衡器添加了双协议栈支持	Global Accelerator 现支持为标准加速器添加双协议栈网络负载均衡器。有关更多信息，请参阅 AWS Global Accelerator 中的加速器端点要求。	2023 年 11 月 2 日
添加了对跨账户资源的支持	Global Accelerator 现支持向加速器添加跨账户资源。要为跨账户资源添加权限，您要在 Global Accelerator 中创建跨账户附件。有关更多信息，请参	2023 年 11 月 1 日

更改	描述	日期
	阅在 AWS Global Accelerator 中使用跨账户附件和端点。	
新增对四个 AWS 区域 的支持	为 Global Accelerator 添加了对以下 AWS 区域的支持：亚太地区（墨尔本）、欧洲（苏黎世）和以色列（特拉维夫）。有关更多信息，请参阅 AWS Global Accelerator 的 AWS 区域可用性。	2023 年 9 月 26 日
更新了服务相关角色	向服务添加了新的 `elasticloadbalancing:DescribeTargetGroups` 权限 Global Accelerator 使用该权限来识别目标类型为 `ip` 的负载均衡器，该目标类型是 Global Accelerator 中双协议栈负载均衡器端点不支持的目标类型。有关更多信息，请参阅 AWS Global Accelerator 的服务相关角色。	2023 年 9 月 12 日
为网络负载均衡器添加了对保留客户端 IP 地址的支持	Global Accelerator 现支持为带有安全组的网络负载均衡器启用客户端 IP 地址保留。有关更多信息，请参阅添加或更新具有保留客户端 IP 地址的端点。	2023 年 8 月 22 日

更改	描述	日期
为 EC2 实例添加了 IPv6 支持	Global Accelerator 现支持将 Amazon EC2 实例添加到双协议栈加速器，以启用发送到 EC2 端点的 IPv4 和 IPv6 流量。有关支持的端点类型的完整列表和更多信息，请参阅 AWS Global Accelerator 中的标准加速器端点。	2023 年 8 月 8 日
添加了新区域	Global Accelerator 现已支持亚太地区（雅加达）。有关受支持区域的完整列表，请参阅 AWS Global Accelerator 的 AWS 区域可用性。	2023 年 6 月 15 日
添加了两个新区域	Global Accelerator 现已支持亚太地区（海得拉巴）和中东（阿联酋）。有关受支持区域的完整列表，请参阅 AWS Global Accelerator 的 AWS 区域可用性。	2023 年 5 月 23 日
更新了服务相关角色	在 Global Accelerator 的服务关联角色中添加了新的 `elasticloadbalancing:DescribeListeners` 和 `ec2:DescribeAddresses` 权限，以支持根据侦听器配置为负载均衡器做出侦听器管理决策，并向加速器添加弹性 IP 地址端点。有关更多信息，请参阅 AWS Global Accelerator 的服务相关角色。	2023 年 5 月 23 日

更改	描述	日期
添加自定义路由加速器配额	添加自定义路由加速器配额。Global Accelerator 也有标准加速器的配额。有关更多信息，请参阅 AWS Global Accelerator 配额。	2023 年 2 月 13 日
更新了指南中的 IAM 指南	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践。	2023 年 2 月 10 日
更新了 `AddEndpoints` 和 `RemoveEndpoints`	Global Accelerator 现支持使用新的 `AddEndpoints` 和 `RemoveEndpoints` API 操作，从而利用 `UpdateEndpointGroup` API 操作来分别添加和移除端点。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/global-accelerator-actions.html。	2022 年 10 月 20 日
针对双协议栈加速器的更新	Global Accelerator 现支持双协议栈加速器。对于 IPv4，Global Accelerator 提供两个静态 IPv4 地址。对于双堆栈，Global Accelerator 提供总计四个地址：两个静态 IPv4 地址和两个静态 IPv6 地址。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html。	2022 年 7 月 27 日

更改	描述	日期
Global Accelerator 现有服务相关角色的更新	Global Acelerator 添加了新的 `ec2:AssignIpv6Addresses` 和 `ec2:UnassignIpv6Addresses` 权限以支持 IPv6 地址。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 11 月 2 日
添加了新的 CloudWatch 指标	Global Accelerator 添加了两个新的 CloudWatch 指标。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/cloudwatch-monitoring.html。	2021 年 10 月 28 日
更新流日志捕获时间窗口	Global Accelerator 已将流日志捕获时间窗口从 10 秒延长到 60 秒。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/monitoring-global-accelerator.flow-logs.html。	2021 年 7 月 30 日
Global Accelerator 现有服务相关角色的更新	Global Accelerator 添加了一项新的 `ec2:DescribeRegions` 权限，允许 Global Accelerator 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

更改	描述	日期
添加了自定义路由加速器	Global Accelerator 推出了一种新型加速器自定义路由加速器。自定义路由加速器非常适合您希望使用自定义应用程序逻辑将一个或多个用户引导至到特定目的地和多个端口之一，同时仍能获享 Global Accelerator 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
添加了端口覆盖支持	Global Accelerator 现已支持覆盖用于将流量路由到端点的侦听器端口。有关更多信息，请参阅 https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-port-override.html。	2020 年 10 月 21 日
添加了两个新区域	Global Accelerator 现已支持非洲（开普敦）和欧洲地区（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

更改	描述	日期
标签添加和 BYOIP	此版本新增为加速器添加标签以及将您自己的 IP 地址添加到 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	添加了有关合规性、弹性和基础设施安全性的内容。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
支持 EC2 实例和默认 DNS 名称	AWS Global Accelerator 现支持在受支持的 AWS 区域中添加 EC2 实例。此外，Global Accelerator 还会创建默认 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

更改	描述	日期
为应用程序负载均衡器保留客户端 IP 地址	现在，您可以选择让 AWS Global Accelerator 为受支持 AWS 区域中的应用程序负载均衡器保留客户端 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，这些加速器可为拥有全球受众的互联网应用程序提高可用性和性能。	2018 年 11 月 26 日