aws

Guia do Desenvolvedor

AWS Global Accelerator

AWS Global Accelerator: Guia do Desenvolvedor

Table of Contents

O que é o AWS Global Accelerator?

O AWS Global Accelerator é um serviço no qual você cria aceleradores para aprimorar o desempenho de seus aplicativos para usuários locais e globais. Dependendo do tipo de acelerador que você escolher, poderá obter benefícios adicionais:

- Com um acelerador padrão, você pode melhorar a disponibilidade de seus aplicativos de Internet que são usados por um público global. Com um acelerador padrão, o Global Accelerator direciona o tráfego pela rede global da AWS para endpoints na região mais próxima do cliente.
- Com um acelerador de roteamento personalizado, você pode mapear um ou mais usuários para um destino específico entre muitos destinos.

O Global Accelerator é um serviço global que é compatível com endpoints em várias Regiões da AWS. Para determinar se o Global Accelerator ou outros serviços são atualmente compatíveis com uma Região da AWS específica, consulte a Lista de serviços regionais da AWS.

Por padrão, o Global Accelerator fornece endereços IP estáticos que você associa ao seu acelerador. Os endereços IP estáticos são anycast da rede de borda da AWS. Para IPv4, o Global Accelerator fornece dois endereços IPv4 estáticos. Para pilha dupla, o Global Accelerator fornece um total de quatro endereços: dois endereços IPv4 estáticos e dois endereços IPv6 estáticos. Para IPv4, em vez de usar os endereços fornecidos pelo Global Accelerator, você pode configurar esses pontos de entrada para serem endereços IPv4 de seus próprios intervalos de endereços IP que você traz para o Global Accelerator (BYOIP).

> **Important**
>
> Os endereços IP estáticos permanecem atribuídos ao seu acelerador enquanto ele existir, mesmo se você desabilitar o acelerador e ele não aceitar ou rotear mais o tráfego. No entanto, ao excluir um acelerador, você perde os endereços IP estáticos atribuídos a ele e, portanto, não pode mais rotear o tráfego usando-os. Você pode usar políticas do IAM, como permissões baseadas em tags com o Global Accelerator, para limitar os usuários que têm permissão para excluir um acelerador. Para ter mais informações, consulte ABAC com Global Accelerator.

Para aceleradores padrão, o Global Accelerator usa a rede global da AWS para rotear o tráfego para o endpoint regional ideal com base na integridade, na localização do cliente e nas políticas que você

configura, o que aumenta a disponibilidade de seus aplicativos. Os endpoints para aceleradores padrão podem ser Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços IP elásticos localizados em uma Região da AWS ou em várias.

O serviço reage instantaneamente às mudanças na integridade ou na configuração para garantir que o tráfego da Internet dos clientes seja sempre direcionado para endpoints íntegros. O Global Accelerator também respeita o redirecionamento de tráfego ARC para endpoints compatíveis, para voltar a rotear o tráfego de uma zona de disponibilidade potencialmente prejudicada com uma mudança de zona ou mudança de zona automática. Para obter mais informações, consulte Recuperação Multi-AZ no Amazon Application Recovery Controller (ARC).

Os aceleradores de roteamento personalizados são compatíveis apenas com os tipos de endpoint de sub-redes da Amazon VPC (VPC) e roteiam o tráfego para endereços IP privados nessa sub-rede.

Conteúdo

Componentes do AWS Global Accelerator

O AWS Global Accelerator inclui os seguintes componentes:

Endereços IP estáticos

Por padrão, o Global Accelerator fornece endereços IP estáticos que você associa ao seu acelerador. Os endereços IP estáticos são anycast da rede de borda da AWS. Para IPv4, o Global Accelerator fornece dois endereços IPv4 estáticos. Para pilha dupla, o Global Accelerator fornece um total de quatro endereços: dois endereços IPv4 estáticos e dois endereços IPv6 estáticos. Se você trouxer seu próprio intervalo de endereços IP para a AWS (BYOIP) para usá-

lo com o Global Accelerator (somente IPv4), poderá atribuir endereços IPv4 de seu próprio grupo para usar com o acelerador. Para ter mais informações, consulte Trazer seus próprios endereços IP (BYOIP) no Global Accelerator.

Os endereços IP servem como pontos de entrada fixos únicos para seus clientes. Se você já tem balanceadores de carga do Elastic Load Balancing, instâncias do Amazon EC2 ou recursos de endereço IP elástico configurados para seus aplicativos, você pode adicioná-los facilmente a um acelerador padrão no Global Accelerator. Isso permite que o Global Accelerator use endereços IP estáticos para acessar os recursos. Se você quiser acessar um API Gateway usando endereços IP estáticos do Global Accelerator, consulte a seguinte postagem no blog para obter mais informações: Como acessar um Amazon API Gateway por meio de endereços IP estáticos fornecidos pelo AWS Global Accelerator.

Os endereços IP estáticos permanecem atribuídos ao seu acelerador enquanto ele existir, mesmo se você desabilitar o acelerador e ele não aceitar ou rotear mais o tráfego. No entanto, ao excluir um acelerador, você perde os endereços IP estáticos atribuídos a ele e, portanto, não pode mais rotear o tráfego usando-os. Você pode usar políticas do IAM, como permissões baseadas em tags, com o Global Accelerator para limitar os usuários que têm permissão para excluir um acelerador. Para ter mais informações, consulte ABAC com Global Accelerator.

Accelerator

Um acelerador direciona o tráfego para endpoints na rede global da AWS para melhorar o desempenho de seus aplicativos de internet. Cada acelerador inclui um ou mais receptores.

Há dois tipos de aceleradores:

- Um acelerador padrão direciona o tráfego para o endpoint da AWS ideal com base em vários fatores, incluindo a localização do usuário, a integridade do endpoint e os pesos do endpoint que você configura. Isso melhora a disponibilidade e o desempenho dos seus aplicativos. Os endpoints podem ser Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços IP elásticos.
- Um acelerador de roteamento personalizado permite rotear deterministicamente vários usuários para um destino específico do EC2 por trás do acelerador, conforme necessário para alguns casos de uso. Você faz isso direcionando os usuários para um endereço IP e uma porta exclusivos em seu acelerador, que o Global Accelerator mapeou para o destino. Observe que os aceleradores de roteamento personalizados não são compatíveis com pilhas duplas para endereços IP.

Para ter mais informações, consulte Tipos de aceleradores.

Nome DNS

O Global Accelerator atribui a cada acelerador um nome de Sistema de Nomes de Domínio (DNS) padrão, semelhante a `a1234567890abcdef.awsglobalaccelerator.com`, que aponta para os endereços IP estáticos que o Global Accelerator atribui a você ou que você escolhe no seu próprio intervalo de endereços IP. Se você tiver um acelerador de pilha dupla, o Global Accelerator também atribuirá um nome DNS de pilha dupla, semelhante ao `a1234567890abcdef.dualstack.awsglobalaccelerator.com`, que aponta para os quatro endereços IP estáticos do seu acelerador de pilha dupla.

Dependendo do caso de uso, você pode usar os endereços IP estáticos ou o nome de DNS do acelerador para rotear o tráfego para o acelerador ou configurar registros de DNS para rotear o tráfego usando seu próprio nome de domínio personalizado. Para ter mais informações, consulte Compatibilidade com endereçamento de DNS no AWS Global Accelerator.

Zona da rede

Semelhante a uma zona de disponibilidade da AWS, uma zona da rede é uma unidade isolada com seu próprio conjunto de infraestrutura física. Quando você cria um acelerador, o Global Accelerator fornece um conjunto de endereços IP estáticos: dois endereços IPv4 estáticos para um acelerador com um tipo de endereço IP IPv4 ou quatro endereços IP estáticos para um acelerador de pilha dupla (dois endereços IPv4 e dois endereços IPv6). O Global Accelerator fornece um endereço IP estático por zona da rede a partir de uma sub-rede IP exclusiva para cada família de endereços IP. Se um endereço de uma zona da rede ficar indisponível devido ao bloqueio de endereços IP por determinadas redes de clientes ou interrupções na rede, os aplicativos dos clientes poderão tentar novamente o endereço IP estático íntegro da outra zona da rede isolada.

Receptor

Um receptor processa conexões de entrada de clientes com o Global Accelerator, com base na porta (ou intervalo de portas) e no protocolo (ou protocolos) que você configura. Um receptor pode ser configurado para os protocolos TCP, UDP ou TCP e UDP. Cada receptor tem um ou mais grupos de endpoints associados a ele, e o tráfego é encaminhado para endpoints em um dos grupos. Você associa grupos de endpoints a receptores especificando as regiões para as quais deseja distribuir o tráfego. Com um acelerador padrão, o tráfego é distribuído para endpoints ideais dentro dos grupos de endpoints associados a um receptor.

Grupo de endpoints

Cada grupo de endpoint é associado a uma Região da AWS específica. Os grupos de endpoints incluem um ou mais endpoints na região. Com um acelerador padrão, você pode aumentar ou reduzir a porcentagem de tráfego que, de outra forma, seria direcionado para um grupo de endpoints ajustando uma configuração chamada indicador de tráfego. O indicador de tráfego permite que você faça facilmente testes de desempenho ou testes de implantação azul/verde, por exemplo, para novas versões em Regiões da AWS diferentes.

Endpoint

Um endpoint é o recurso para o qual o Global Accelerator direciona o tráfego.

Os endpoints para aceleradores padrão podem ser Network Load Balancers, Application Load Balancers, instâncias do EC2 ou endereços IP elásticos. Um endpoint do Application Load Balancer pode ser voltado para a internet ou interno. O tráfego dos aceleradores padrão é roteado para os endpoints com base na integridade do endpoint junto com as opções de configuração que você escolher, como pesos dos endpoints. Para cada endpoint, você pode configurar pesos, que são números que você pode usar para especificar a proporção do tráfego a ser roteado para cada um. Isso pode ser útil, por exemplo, para fazer testes de desempenho em uma região.

Os endpoints para aceleradores de roteamento personalizados são sub-redes da Amazon VPC (VPC) com uma ou várias instâncias do Amazon EC2 que são os destinos do tráfego.

Disponibilidade da Região da AWS para o AWS Global Accelerator

Para obter informações detalhadas sobre o suporte regional e os endpoints de serviço para o AWS Global Accelerator, consulte Endpoints e cotas do AWS Global Accelerator na Referência geral do Amazon Web Services.

> **Note**
>
> O AWS Global Accelerator é um serviço global. No entanto, você deve especificar a região Oeste dos EUA (Oregon) (ou seja, especificar o parâmetro `--region us-west-2`) nos comandos da AWS CLI do Global Accelerator Regional. Ou seja, quando você cria recursos, como aceleradores.

No momento, o Global Accelerator está disponível nas seguintes regiões da AWS. Exceções da Zona de Disponibilidade (AZ) são anotadas.

Nome da região	Região
Leste dos EUA (Ohio)	`us-east-2`
Leste dos EUA (N. da Virgínia)	`us-east-1`
Oeste dos EUA (N. da Califórnia)	`us-west-1 (except AZ usw1-az2)`
Oeste dos EUA (Oregon)	`us-west-2`
África (Cidade do Cabo)	`af-south-1`
Ásia-Pacífico (Hong Kong)	`ap-east-1`
Asia Pacific (Mumbai)	`ap-south-1`
Ásia-Pacífico (Hyderabad)	`ap-south-2`
Ásia-Pacífico (Jacarta)	`ap-southeast-3`
Ásia-Pacífico (Melbourne)	`ap-southeast-4`
Ásia-Pacífico (Osaka)	`ap-northeast-3`
Ásia-Pacífico (Singapura)	`ap-southeast-1`
Ásia-Pacífico (Sydney)	`ap-southeast-2`
Ásia-Pacífico (Tóquio)	`ap-northeast-1 (except AZ apne1-az3)`
Ásia-Pacífico (Seul)	`ap-northeast-2`
Canadá (Central)	`ca-central-1 (except AZ cac1-az3)`
Oeste do Canadá (Calgary)	`ca-west-1`
Europa (Frankfurt)	`eu-central-1`

Nome da região	Região
Europa (Irlanda)	`eu-west-1`
Europa (Londres)	`eu-west-2`
Europa (Milão)	`eu-south-1`
Europe (Paris)	`eu-west-3`
Europa (Espanha)	`eu-south-2`
Europa (Estocolmo)	`eu-north-1`
Europa (Zurique)	`eu-central-2`
Israel (Tel Aviv)	`il-central-1`
Oriente Médio (Barém)	`me-south-1`
Oriente Médio (Emirados Árabes Unidos)	`me-central-1`
América do Sul (São Paulo)	`sa-east-1`

Como o AWS Global Accelerator funciona

Os endereços IP estáticos fornecidos pelo AWS Global Accelerator servem como pontos de entrada fixos únicos para seus clientes. Ao configurar seu acelerador com o Global Accelerator, você associa os endereços IP estáticos aos endpoints regionais em um ou mais Regiões da AWS. Para aceleradores padrão, os endpoints são Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços IP elásticos. Para aceleradores de roteamento personalizados, os endpoints são sub-redes da Amazon VPC (VPC) com uma ou mais instâncias do EC2. Os endereços IP estáticos aceitam tráfego de entrada na rede global da AWS a partir do local da borda mais próximo de seus usuários.

> **Note**
>
> Se você trouxer seu próprio intervalo de endereços IP para a AWS (BYOIP) para usá-lo com o Global Accelerator, poderá atribuir endereços IP estáticos de seu próprio grupo para usar

com o acelerador. Para ter mais informações, consulte Trazer seus próprios endereços IP (BYOIP) no Global Accelerator.

Do local da borda, o tráfego do seu aplicativo é roteado com base no tipo de acelerador que você configura.

- Para aceleradores padrão, o tráfego é roteado para o endpoint da AWS ideal com base em vários fatores, incluindo a localização do usuário, a integridade do endpoint e os pesos do endpoint que você configura.
- Para aceleradores de roteamento personalizados, cada cliente é roteado para uma instância e porta específicas do Amazon EC2 em uma sub-rede VPC, com base no endereço IP estático externo e na porta do receptor que você fornece.

Esteja ciente do seguinte ao usar o Global Accelerator:

- Substituição dos pesos dos endpoints: em cenários específicos e limitados, o Global Accelerator substitui os pesos dos endpoints que você define para ajudar a garantir a disponibilidade. Quando o Global Accelerator está balanceando a carga do tráfego entre endpoints em um grupo de endpoints, ele deve, em determinadas circunstâncias, escolher entre preservar a disponibilidade do tráfego do cliente e respeitar os pesos dos endpoints. Por exemplo, com aceleradores em que o endereço IP do cliente é preservado, o Global Accelerator pode precisar substituir uma configuração de peso do endpoint para ajudar a evitar colisões de conexão.
- Grupos e regras de segurança: quando você adiciona um acelerador, os grupos de segurança e as regras do AWS WAF que você já configurou continuam funcionando da mesma forma que funcionavam antes de você adicionar o acelerador.
- Fragmentação de IP: pacotes IP grandes demais para caber em um quadro Ethernet padrão (mais de 1500 bytes) quando transmitidos pela Internet ou por outras redes grandes são fragmentados por roteadores intermediários e enviados individualmente. O protocolo TCP não exige fragmentação de IP porque clientes e endpoints negociam automaticamente um tamanho máximo de segmento (MSS) menor. No entanto, o protocolo UDP requer fragmentação de IP. Quando os pacotes são fragmentados, o Global Accelerator encaminha fragmentos do UDP para o endpoint configurado, que remonta o pacote IP original. O Global Accelerator descarta fragmentos de TCP na borda, porque eles não são compatíveis com a rede da AWS.

Tópicos

Visão geral de como o AWS Global Accelerator funciona

O tráfego viaja pela rede global da AWS redundante, bem monitorada e livre de congestionamentos até o endpoint. Ao maximizar o tempo em que o tráfego permanece na rede da AWS, o Global Accelerator garante que o tráfego seja sempre roteado pelo caminho de rede ideal. O Global Accelerator encerra conexões TCP de clientes em locais da borda da AWS e, quase simultaneamente, estabelece uma nova conexão TCP com seus endpoints. Isso proporciona aos clientes tempos de resposta mais rápidos (menor latência) e maior throughput.

O Global Accelerator sempre preserva os endereços IP do cliente para endpoints em aceleradores de roteamento personalizados. Com aceleradores padrão, você tem a opção de preservar e acessar o endereço IP do cliente para alguns tipos de endpoint. Para obter informações detalhadas sobre os tipos e configurações de endpoints com os que o Global Accelerator é compatível, incluindo compatibilidade com a preservação do endereço IP do cliente, consulte Requisitos para recursos que você adiciona como endpoints do acelerador.

Com aceleradores padrão, o Global Accelerator monitora continuamente a integridade de todos os endpoints e começa instantaneamente a direcionar o tráfego de todas as novas conexões para outro endpoint disponível quando determina que um endpoint ativo não está íntegro. Isso permite que você crie uma arquitetura de alta disponibilidade para seus aplicativos na AWS. As verificações de integridade não são usadas com aceleradores de roteamento personalizados e não há failover, porque você especifica o destino para o qual rotear o tráfego.

Se você quiser um controle refinado sobre seu tráfego global, você pode configurar pesos para seus endpoints em um acelerador padrão. Além disso, você pode usar o indicador de tráfego no Global Accelerator para aumentar ou diminuir a porcentagem de tráfego para um grupo específico de endpoints, por exemplo, para testes de desempenho ou atualizações de pilha.

Tipos de aceleradores

Há dois tipos de aceleradores que você pode usar com o AWS Global Accelerator: aceleradores padrão e aceleradores de roteamento personalizados. Os dois tipos de aceleradores roteiam o tráfego pela rede global da AWS para melhorar o desempenho e a estabilidade, mas cada um deles foi projetado para diferentes necessidades de aplicativos.

Acelerador padrão

Ao usar um acelerador padrão, você pode melhorar a disponibilidade e o desempenho de seus aplicativos executados em Application Load Balancers, Network Load Balancers ou instâncias do Amazon EC2. Com um acelerador padrão, o Global Accelerator roteia o tráfego de clientes entre endpoints regionais com base na proximidade geográfica e na integridade do endpoint. Ele também permite que os clientes transfiram o tráfego de clientes entre os endpoints com base em controles como indicadores de tráfego e pesos dos endpoints. Isso funciona para uma ampla variedade de casos de uso, incluindo implantação azul/verde, testes A/B e implantação em várias regiões. Para ver mais casos de uso, consulte Noções básicas dos casos de uso do AWS Global Accelerator.

Para saber mais, consulte Como trabalhar com aceleradores padrão no AWS Global Accelerator.

Acelerador de roteamento personalizado

Os aceleradores de roteamento personalizados funcionam bem em cenários em que você deseja usar a lógica de aplicativo personalizada para direcionar um ou mais usuários para um destino e porta específicos entre muitos, sem deixar de obter os benefícios de desempenho do Global Accelerator. Um exemplo são os aplicativos de VoIP que atribuem vários chamadores a um servidor de mídia específico para iniciar sessões de voz, vídeo e mensagens. Outro exemplo são os aplicativos de jogos on-line em tempo real, nos quais você deseja atribuir vários jogadores a uma única sessão em um servidor de jogos com base em fatores como localização geográfica, habilidade do jogador e modo de jogo.

> **Note**
>
> Os aceleradores de roteamento personalizados são compatíveis apenas com o tipo de endereço IP IPv4.

Para saber mais, consulte Como trabalhar com aceleradores de roteamento personalizados no AWS Global Accelerator.

Com base em suas necessidades específicas, você cria um desses tipos de aceleradores para acelerar o tráfego de seus clientes.

Noções básicas sobre o tempo limite de inatividade no AWS Global Accelerator

O AWS Global Accelerator define um período de tempo limite de inatividade que se aplica às suas conexões. Se nenhum dado tiver sido enviado ou recebido até o período que o tempo limite de inatividade terminar, o Global Accelerator encerrará a conexão. Os períodos de tempo limite de inatividade não são personalizáveis.

Para evitar o tempo limite da conexão, o Global Accelerator exige que você envie um pacote com no mínimo um byte de dados, na direção de entrada ou saída, dentro da janela de tempo limite da conexão TCP. Você não pode usar pacotes TCP keep-alive para manter uma conexão aberta.

O tempo limite de inatividade do Global Accelerator para uma conexão de rede depende do tipo de conexão:

- O tempo limite é de 340 segundos para conexões TCP.
- O tempo limite é de 30 segundos para conexões UDP.

O Global Accelerator continua direcionando o tráfego das conexões estabelecidas para um endpoint até que o tempo limite de inatividade seja atingido, mesmo que o endpoint esteja marcado como não íntegro ou que tenha sido removido do acelerador. O Global Accelerator seleciona um novo endpoint, se necessário, somente quando uma nova conexão é iniciada ou após um tempo limite de inatividade.

Como usar endereços IP estáticos no AWS Global Accelerator

Por padrão, o Global Accelerator fornece endereços IP estáticos que são associados ao seu acelerador. Você usa os endereços IP estáticos que o Global Accelerator atribui ao seu acelerador, ou que você especifica do seu próprio grupo de endereços IP, para aceleradores padrão, para rotear o tráfego da Internet para a rede global da AWS perto de onde seus usuários estão, independentemente de sua localização. Para aceleradores padrão, você associa os endereços a Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços IP elásticos que são executados em uma Região da AWS ou várias. Para aceleradores de roteamento personalizados, você direciona o tráfego para destinos do EC2 em sub-redes de VPC em uma

ou mais regiões. O roteamento do tráfego pela rede global da AWS melhora a disponibilidade e o desempenho porque o tráfego não precisa passar por vários saltos pela Internet pública. O uso de endereços IP estáticos também permite distribuir o tráfego de entrada do aplicativo em vários recursos de endpoint em várias Regiões da AWS.

Além disso, o uso de endereços IP estáticos facilita a adição do aplicativo a mais regiões ou a migração de aplicativos entre regiões. Usar endereços IP fixos significa que os usuários têm uma maneira consistente de se conectar ao seu aplicativo à medida que você faz alterações.

Se quiser, você pode associar seu próprio nome de domínio personalizado aos endereços IP estáticos do seu acelerador. Para ter mais informações, consulte Rotear o tráfego de domínio personalizado para o seu acelerador.

Os endereços IP estáticos são anycast da rede de borda da AWS.

Para IPv4, o Global Accelerator fornece dois endereços IPv4 estáticos. Para pilha dupla, o Global Accelerator fornece um total de quatro endereços: dois endereços IPv4 estáticos e dois endereços IPv6 estáticos. Se você trouxer seu próprio intervalo de endereços IP para a AWS (BYOIP) para usá-lo com o Global Accelerator (somente IPv4), poderá atribuir endereços IPv4 de seu próprio grupo para usar com o acelerador. Para ter mais informações, consulte Trazer seus próprios endereços IP (BYOIP) no Global Accelerator.

Para aceleradores com pilha dupla, o Global Accelerator aloca os endereços IPv6 dos mesmos dois prefixos CIDR /64. Isso pode ajudar a simplificar as etapas de listagem de permissões e configuração de controles de ACL.

Você pode adicionar apenas endpoints IPv4 aos aceleradores padrão configurados para tipos de endereço IP IPv4, mas os aceleradores que você configura como pilha dupla exigem que você adicione somente endpoints que também sejam compatíveis com pilhas duplas. Para obter informações sobre endpoints compatíveis com aceleradores de pilha dupla, consulte Requisitos para recursos que você adiciona como endpoints do acelerador.

O Global Accelerator fornece os endereços IP estáticos para você do grupo de endereços IP da Amazon, a menos que você traga seu próprio intervalo de endereços IP para a AWS e, em seguida, especifique os endereços IP estáticos desse grupo. (Para ter mais informações, consulte Trazer seus próprios endereços IP (BYOIP) no Global Accelerator.) Para criar um acelerador no console, a primeira etapa é solicitar que o Global Accelerator provisione os endereços IP estáticos inserindo um nome para seu acelerador ou escolhendo seus próprios endereços IP estáticos. Para ver as etapas para criar um acelerador, consulte Conceitos básicos do AWS Global Accelerator.

Os endereços IP estáticos permanecem atribuídos ao seu acelerador enquanto ele existir, mesmo se você desabilitar o acelerador e ele não aceitar ou rotear mais o tráfego. No entanto, ao excluir um acelerador, você perde os endereços IP estáticos atribuídos a ele e, portanto, não pode mais rotear o tráfego usando-os. Você pode usar políticas do IAM, como permissões baseadas em tags, com o Global Accelerator para limitar os usuários que têm permissão para excluir um acelerador. Para ter mais informações, consulte ABAC com Global Accelerator.

Como o Global Accelerator usa verificações de integridade

Para aceleradores padrão, o AWS Global Accelerator verifica automaticamente a integridade dos endpoints associados aos seus endereços IP estáticos e, em seguida, direciona o tráfego do usuário somente para endpoints íntegros.

O Global Accelerator inclui verificações de integridade padrão que são executadas automaticamente, mas você pode configurar o tempo para as verificações e outras opções. Se você definiu configurações personalizadas de verificação de integridade, o Global Accelerator usa essas configurações de maneiras específicas, dependendo da sua configuração. Você define essas configurações no Global Accelerator para a instância do Amazon EC2 ou endpoints de endereço IP elástico ou definindo as configurações no console do Elastic Load Balancing para Network Load Balancers ou Application Load Balancers. Para ter mais informações, consulte Garantir acesso à verificação de integridade do seu acelerador.

Quando você adiciona um endpoint a um acelerador padrão, ele deve passar por uma verificação de integridade para ser considerado íntegro antes que o tráfego seja direcionado para ele. Se o Global Accelerator não tiver nenhum endpoint íntegro para rotear o tráfego em um acelerador padrão, ele roteia as solicitações para todos os endpoints.

Como você pode gerenciar o fluxo de tráfego com indicadores de tráfego e pesos de endpoint

Há duas maneiras de personalizar a forma como o AWS Global Accelerator envia tráfego para seus endpoints com um acelerador padrão:

- Altere o indicador de tráfego para limitar o tráfego para um ou mais grupos de endpoints
- Especifique os pesos para alterar a proporção do tráfego para os endpoints em um grupo

Como funcionam os indicadores de tráfego

Para cada grupo de endpoints em um acelerador padrão, você pode definir um indicador de tráfego para controlar a porcentagem do tráfego que é enviado para o grupo de endpoints. A porcentagem é aplicada somente ao tráfego que já está direcionado ao grupo de endpoints, não a todo o tráfego de receptores.

O indicador de tráfego limita a parte do tráfego que um grupo de endpoints aceita, expressa como uma porcentagem do tráfego direcionado a esse grupo de endpoints. Por exemplo, se você definir o indicador de tráfego de um grupo de endpoints em `us-east-1` como 50 (ou seja, 50%) e o acelerador direcionar 100 solicitações de usuários para esse grupo de endpoints, somente 50 solicitações serão aceitas pelo grupo. O acelerador direciona as 50 solicitações restantes para grupos de endpoints em outras regiões.

Para ter mais informações, consulte Usar indicadores de tráfego para ajustar o fluxo de tráfego para regiões.

Como funcionam os pesos

Para cada endpoint em um acelerador padrão, você pode especificar pesos, que são números que alteram a proporção do tráfego que o acelerador roteia para cada endpoint. Isso pode ser útil, por exemplo, para fazer testes de desempenho em uma região.

Um peso é um valor que determina a proporção do tráfego que o acelerador direciona para um endpoint. Por padrão, o peso de um endpoint é 128, ou seja, metade do valor máximo de um peso, 255.

O acelerador calcula a soma dos pesos dos endpoints em um grupo de endpoints e, em seguida, direciona o tráfego para os endpoints com base na proporção do peso de cada endpoint em relação ao total. Para obter um exemplo de como os pesos funcionam, consulte Como os pesos dos endpoints funcionam para gerenciar o volume de tráfego.

Os indicadores e pesos de tráfego afetam a forma como o acelerador padrão distribui o tráfego de diferentes maneiras:

- Você configura indicadores de tráfego para grupos de endpoints. O indicador de tráfego permite que você corte uma porcentagem do tráfego (ou todo o tráfego) do grupo, “diminuindo” o tráfego que o acelerador já direcionou para ele com base em outros fatores, como a proximidade.
- Você usa pesos, por outro lado, para definir valores para endpoints individuais dentro de um grupo de endpoints. Os pesos fornecem uma forma de dividir o tráfego dentro do grupo de endpoints. Por

exemplo, você pode usar pesos para fazer testes de desempenho para endpoints específicos em uma região.

Para obter mais informações sobre como os indicadores e pesos do tráfego afetam o failover, consulte Como o failover funciona para endpoints não íntegros.

Mensagens de resposta do ICMP e AWS Global Accelerator

Mensagens de resposta do ICMP, como `ICMP Packet Too Big` ou `Fragmentation Needed`, ajudam a garantir a disponibilidade na Internet. O AWS Global Accelerator responde às mensagens de eco do ICMP (pings) na borda para todos os endereços IP globais. Esses pings não são encaminhados para os endpoints dos clientes. Para testar com precisão o desempenho com o Global Accelerator, use um protocolo mais profundo para seus testes.

A seguir, um breve resumo de como o ICMP ajuda a garantir a disponibilidade da Internet. A unidade de transmissão máxima (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser passado pela conexão. Quanto maior a MTU de uma conexão, mais dados podem ser passados em um único pacote. A descoberta de caminho MTU (PMTUD) é usada para determinar a MTU do caminho entre dois dispositivos. A MTU do caminho é o tamanho de pacote máximo com suporte no caminho entre o host de origem e o host de recepção. Quando há alguma diferença no tamanho da MTU da rede entre dois hosts, pacotes maiores do que a MTU são descartados, e o host de recepção que descartou o pacote notifica o remetente com uma mensagem do ICMP. Para obter mais informações, consulte descoberta de caminho MTU.

Você não pode bloquear o tráfego do ICMP em seu acelerador no Global Accelerator. O bloqueio de todo o tráfego do ICMP também eliminaria mensagens do ICMP, como `ICMPv6 Packet Too Big (PTB)` (Tipo 2) e `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipo 3, Código 4). Essas mensagens são necessárias para que o tráfego retorne com sucesso ao host de origem. Por sua vez, essas mensagens descartadas fariam com que o TCP e os protocolos criados com base no Global Accelerator eliminassem o tráfego de clientes que estão em redes com MTUs menores do que o normal, evitando a PMTUD.

Observe que, para que a PMTUD funcione, os grupos de segurança dos seus endpoints também devem permitir o tráfego do ICMP. Se você tiver problemas de disponibilidade específicos de determinadas redes de usuários finais, confirme se seus grupos de segurança de endpoint permitem tráfego do ICMP.

Localização e intervalos de endereços IP dos servidores de borda do Global Accelerator

Para obter uma lista das localizações dos servidores de borda do Global Accelerator, consulte Rede de borda global na página de Atributos do AWS Global Accelerator.

A AWS publica seus intervalos de endereços IP atuais em formato JSON. Para visualizar os intervalos atuais, faça download do arquivo ip-ranges.json. Para obter mais informações, consulte Intervalos de endereços IP da AWS no Referência geral da Amazon Web Services.

Antes de trabalhar com o arquivo `ip-ranges.json`, analise primeiro as seguintes informações:

- Para encontrar os intervalos de endereços IP associados aos servidores de borda do AWS Global Accelerator, pesquise por `ip-ranges.json` na seguinte string:

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

- As entradas do Global Accelerator que incluem `"region": "GLOBAL"` referem-se aos endereços IP estáticos que são alocados aos aceleradores. Se você quiser filtrar o tráfego por meio de seu acelerador proveniente de pontos de presença (POPs) em uma área, filtre as entradas que incluam uma área geográfica específica, como `us-*` ou `eu-*`. Então, por exemplo, se você filtrar por `us-*`, verá apenas o tráfego vindo por POPs nos Estados Unidos (EUA).
- O Global Accelerator é compatível com duas formas de rotear o tráfego: usando a preservação do endereço IP do cliente ou usando a conversão de endereços de rede (NAT). A forma como o tráfego é roteado determina o endereço IP do cliente ao qual as regras do AWS WAF podem ser aplicadas. Quando você usa a preservação do endereço IP do cliente, as regras do AWS WAF têm como alvo o endereço IP do cliente, ou seja, o endereço IP dos clientes que acessam seu serviço. Quando você usa o NAT, as regras do AWS WAF são aplicadas aos endereços IP globais que o Global Accelerator usa para rotear o tráfego.

Noções básicas dos casos de uso do AWS Global Accelerator

Usar o AWS Global Accelerator pode ajudar você a realizar vários objetivos. Esta seção lista alguns deles, para dar uma ideia de como você pode usar o Global Accelerator para atender às suas necessidades.

Escale para maior utilização do aplicativo

Quando o uso do aplicativo aumenta, o número de endereços IP e endpoints que você precisa gerenciar também aumenta. O Global Accelerator permite que você aumente ou diminua sua rede. Ele permite associar recursos regionais, como balanceadores de carga e instâncias do Amazon EC2, a dois endereços IPv4 estáticos ou, para pilha dupla, a dois endereços IPv4 estáticos e dois endereços IPv6. Você inclui esses endereços nas listas de permissões apenas uma vez nos aplicativos, firewalls e registros DNS do seus clientes. Com o Global Accelerator, você pode adicionar ou remover endpoints em Regiões da AWS, executar a implantação azul/verde e fazer testes A/B sem precisar atualizar os endereços IP nos aplicativos dos seus clientes. Isso é especialmente útil para casos de uso de IoT, varejo, mídia, indústria automotiva e assistência médica em que você não pode atualizar facilmente os aplicativos dos seus clientes com frequência.

Aceleração para aplicativos sensíveis à latência

Muitos aplicativos, especialmente em áreas como jogos, mídia, aplicativos móveis, tecnologia de anúncios e finanças, exigem uma latência muito baixa para uma ótima experiência do usuário. Para melhorar a experiência do usuário, o Global Accelerator direciona o tráfego do usuário para o endpoint do aplicativo mais próximo do cliente, o que reduz a latência e a instabilidade da Internet. O Global Accelerator roteia o tráfego para o local da borda mais próximo usando o Anycast e, em seguida, o roteia para o endpoint regional mais próximo na rede global da AWS. O Global Accelerator reage rapidamente às mudanças no desempenho da rede para melhorar o desempenho dos aplicativos de seus usuários.

Recuperação de desastres e resiliência em várias regiões

É preciso poder confiar na rede para estar disponível. Você pode estar executando seu aplicativo em várias Regiões da AWS para ter compatibilidade com recuperação de desastres, maior disponibilidade, menor latência ou conformidade. Se o Global Accelerator detectar que o endpoint do seu aplicativo está falhando na Região da AWS primária, ele aciona instantaneamente o redirecionamento do tráfego para o endpoint do aplicativo no próximo ponto da Região da AWS disponível e mais próximo.

Para obter mais informações sobre como o Global Accelerator possui uma compatibilidade inerente à resiliência e com os aplicativos que usam o serviço, leia a seguinte postagem no blog: Como maximizar a resiliência do aplicativo com o AWS Global Accelerator.

Proteja seus aplicativos

Como expor suas origens da AWS, como Application Load Balancers ou instâncias do Amazon EC2, ao tráfego público da Internet cria uma oportunidade para ataques maliciosos. O Global Accelerator diminui o risco de ataque ao mascarar sua origem por trás de dois pontos de entrada estáticos. Esses pontos de entrada são protegidos por padrão contra ataques distribuídos de negação de serviço (Distributed Denial of Service, DDoS) com o AWS Shield. O Global Accelerator cria uma conexão de emparelhamento com sua nuvem privada virtual da Amazon usando endereços IP privados, mantendo as conexões com seus Application Load Balancers internos ou instâncias do EC2 privadas fora da Internet pública.

Melhore o desempenho de aplicativos de VoIP ou jogos on-line

Com um acelerador de roteamento personalizado, você pode aproveitar os benefícios de desempenho do Global Accelerator para seus aplicativos de VoIP ou jogos. Por exemplo, você pode usar o Global Accelerator para aplicativos de jogos on-line que atribuem vários jogadores a uma única sessão de jogo. Use o Global Accelerator para reduzir a latência e a instabilidade globalmente em aplicativos que exigem lógica personalizada para mapear usuários para endpoints específicos, como jogos multijogador ou chamadas VoIP. Você pode usar um único acelerador para conectar clientes a milhares de instâncias do Amazon EC2 em execução em uma ou várias Regiões da AWS, mantendo o controle total sobre qual cliente é direcionado para qual instância e porta do EC2.

Ferramenta de comparação de velocidade do AWS Global Accelerator

Você pode usar a ferramenta de comparação de velocidade do AWS Global Accelerator para ver as velocidades de download do Global Accelerator em comparação com os downloads diretos da Internet, em todas as Regiões da AWS. Essa ferramenta permite que você use seu navegador para ver a diferença de desempenho ao transferir dados usando o Global Accelerator. Você escolhe um tamanho de arquivo para fazer download, e a ferramenta faz download de arquivos via HTTPS/TCP dos Application Load Balancers em diferentes regiões para o seu navegador. Para cada região, você vê uma comparação direta das velocidades de download.

Para acessar a ferramenta de comparação de velocidade, copie o URL a seguir em seu navegador:

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

> **Important**
>
> Os resultados podem ser diferentes quando você executa o teste várias vezes. Os tempos de download podem variar com base em fatores externos ao Global Accelerator, como a qualidade, a capacidade e a distância da conexão na rede de última milha que você está usando.

Como começar a usar o AWS Global Accelerator

Você pode começar a configurar o AWS Global Accelerator usando a API ou usando o console do AWS Global Accelerator. Como o Global Accelerator é um serviço global, ele não está vinculado a uma Região da AWS específica. Observe que o Global Accelerator é um serviço global que oferece compatibilidade com endpoints em várias Regiões da AWS, mas você deve especificar a região Oeste dos EUA (Oregon) para criar ou atualizar aceleradores.

Para começar a usar o Global Accelerator, siga estas etapas gerais:

1. Escolha o tipo de acelerador que você deseja criar: um acelerador padrão ou um acelerador de roteamento personalizado.
2. Faça a configuração inicial do Global Accelerator: forneça um nome para seu acelerador e escolha o tipo de acelerador e o tipo de endereço.
3. Configure um ou mais receptores para seu acelerador: os receptores processam conexões de entrada de clientes, com base no protocolo e na porta (ou intervalo de portas) que você especificar.
4. Configure grupos de endpoints regionais para seu acelerador: você pode selecionar um ou mais grupos de endpoints regionais para adicionar ao seu receptor. O receptor roteia as solicitações para os endpoints que você adicionou a um grupo de endpoints.

   Para um acelerador padrão, o Global Accelerator monitora a integridade dos endpoints dentro do grupo usando as configurações de verificação de integridade definidas para cada um dos seus endpoints. Para cada grupo de endpoints em um acelerador padrão, você pode configurar uma porcentagem de indicador de tráfego para controlar a porcentagem de tráfego que um grupo de endpoints aceitará. A porcentagem é aplicada somente ao tráfego que já está direcionado ao grupo de endpoints, não a todo tráfego de receptores. Por padrão, o indicador de tráfego é definido como 100% para todos os grupos de endpoints regionais.

Para aceleradores de roteamento personalizados, o tráfego é roteado deterministicamente para um destino específico em uma sub-rede VPC, com base na porta do receptor na qual o tráfego é recebido.

5. Adicione endpoints a grupos de endpoints: os endpoints que você adiciona dependem do tipo de acelerador.
   - Para um acelerador padrão, você pode adicionar um ou mais recursos regionais, como balanceadores de carga ou endpoints de instâncias do EC2, a cada grupo de endpoints. Em seguida, você pode decidir quanto tráfego deseja rotear para cada endpoint definindo os pesos dos endpoints.
   - Para um acelerador de roteamento personalizado, você adiciona uma ou mais sub-redes da Amazon VPC (VPC) com até milhares de destinos de instância do Amazon EC2.

Para ver etapas detalhadas sobre como criar um acelerador padrão ou um acelerador de roteamento personalizado usando o console do AWS Global Accelerator, consulte Conceitos básicos do AWS Global Accelerator. Para trabalhar com operações de API, consulte Ações comuns de API para o AWS Global Accelerator e a Referência da API do AWS Global Accelerator.

Marcar no AWS Global Accelerator

As tags são palavras ou frases (metadados) que podem ser usadas para identificar e organizar seus recursos da AWS. É possível adicionar várias tags a cada recurso, e cada tag inclui uma chave e um valor definidos por você. Por exemplo, a chave de tag pode ser `environment` e o valor pode ser `production`. Você pode pesquisar e filtrar seus recursos de acordo com as tags que adicionar. No AWS Global Accelerator, você pode aplicar tags a aceleradores.

Veja a seguir dois exemplos de como pode ser útil trabalhar com tags no Global Accelerator:

- Use as tags para rastrear informações de faturamento em categorias diferentes. Para fazer isso, aplique tags a aceleradores ou outros recursos da AWS (como Network Load Balancers, Application Load Balancers ou instâncias do Amazon EC2) e habilite as tags. Em seguida, a AWS gera um relatório de alocação de custos como um arquivo de valores separados por vírgulas (CSV) com uso e custos agregados pelas tags ativas. É possível aplicar tags que representem categorias de negócios (como centros de custos, nomes da aplicações ou proprietários) para organizar seus custos de vários serviços. Para obter mais informações, consulte Usar tags de alocação de custos no Guia do usuário do AWS Billing.

- Use tags para aplicar permissões baseadas em tags para aceleradores. Para fazer isso, crie políticas do IAM que especificam tags e valores de tags para permitir ou proibir ações. Para ter mais informações, consulte ABAC com Global Accelerator.

Para convenções de uso e links para outros recursos sobre marcação, consulte Como aplicar tags a seus recursos da AWS em Referência geral da AWS. Para obter dicas sobre o uso de tags, consulte Práticas recomendadas de marcação: estratégia de marcação recursos da AWS no blog Whitepapers da AWS.

Para saber o número máximo de tags que podem ser adicionadas a um recurso no Global Accelerator, consulte Cotas para o AWS Global Accelerator.

Você pode adicionar e atualizar tags usando o console da AWS, a AWS CLI ou a API do Global Accelerator. Este capítulo inclui etapas para trabalhar com a marcação no console. Para obter mais informações sobre como trabalhar com tags usando a AWS CLI e a API do Global Accelerator, incluindo exemplos de CLI, consulte as seguintes operações na Referência da API do AWS Global Accelerator:

- CreateAccelerator
- CreateCrossAccountAttachment
- TagResource
- UntagResource
- ListTagsForResource

Compatibilidade de marcação no Global Accelerator

O AWS Global Accelerator é compatível com a marcação para aceleradores e anexos entre contas.

O Global Accelerator é compatível com o atributo de controle de acesso baseado em tags do AWS Identity and Access Management (IAM). Para ter mais informações, consulte ABAC com Global Accelerator.

Como adicionar, editar e excluir tags no Global Accelerator

O procedimento a seguir explica como adicionar, editar e excluir tags dos aceleradores no console do Global Accelerator.

Você pode adicionar ou remover tags usando o console, a AWS CLI ou as operações da API do Global Accelerator. Para obter mais informações, incluindo exemplos de CLI, consulte TagResource na Referência da API do AWS Global Accelerator.

Para adicionar, editar ou excluir tags no Global Accelerator

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Selecione o acelerador para o qual você deseja adicionar ou atualizar tags.
3. Na seção Tags, você pode fazer o seguinte:

   Adicione um tag

   Escolha Adicionar tag, insira uma chave e, opcionalmente, um valor para a tag.

   Editar uma tag

   Atualize o texto para uma chave, um valor ou ambos. Você também pode limpar o valor de uma tag, mas a chave é obrigatória.

   Excluir uma tag

   Escolha Remover à direita do campo de valor.
4. Escolha Salvar alterações.

Precificação para AWS Global Accelerator

Com o AWS Global Accelerator, é cobrada uma taxa horária fixa para cada acelerador provisionado em sua conta (esteja ele habilitado ou desabilitado) e uma taxa incremental, além das taxas de transferência de dados padrão, para cada hora de tráfego na direção dominante que flui pelo acelerador. A taxa incremental depende da Região da AWS que atende à solicitação (a origem) e do local da borda da AWS para a qual as respostas são direcionadas (o destino). Normalmente, os clientes criam um acelerador para cada aplicativo, mas clientes com aplicativos complexos podem precisar de mais aceleradores.

Para obter detalhes sobre preços, informações sobre preços por regiões de origem e destino e um exemplo de preços, consulte Preços do AWS Global Accelerator.

Conceitos básicos do AWS Global Accelerator

Para ajudar você a começar a usar o AWS Global Accelerator, este capítulo fornece tutoriais para configurar um acelerador padrão e um acelerador de roteamento personalizado.

Para saber mais sobre os dois tipos de aceleradores que você pode criar no Global Accelerator, consulte Como trabalhar com aceleradores padrão no AWS Global Accelerator e Como trabalhar com aceleradores de roteamento personalizados no AWS Global Accelerator.

Os tutoriais fornecem etapas que usam primariamente o AWS Management Console. Observe que, ao configurar um acelerador de roteamento personalizado, você deve usar a API para determinadas etapas de configuração.

> **Tip**
>
> Para explorar como você pode usar o Global Accelerator para melhorar o desempenho e a disponibilidade de aplicativos web, confira o seguinte workshop individualizado: Workshop do AWS Global Accelerator.

Você também pode usar as operações da API do Global Accelerator com a AWS Command Line Interface (AWS CLI) ou SDKs da AWS para criar e personalizar seus aceleradores. Veja a seguir os recursos para trabalhar com as APIs do Global Accelerator.

- Para obter uma lista das operações de API, consulte Ações comuns de API para o AWS Global Accelerator.
- Para obter informações detalhadas sobre como trabalhar com operações de API do AWS Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

O Global Accelerator é um serviço global que é compatível com endpoints em várias regiões da AWS. As regiões compatíveis estão listadas na tabela de regiões da AWS.

Conteúdo

Introdução ao acelerador padrão

Esta seção fornece etapas para criar um acelerador padrão, que roteia o tráfego para um endpoint ideal.

Tarefas

- Antes de começar
- Etapa 1: criar um acelerador padrão
- Etapa 2: adicionar receptores
- Etapa 3: adicionar grupos de endpoints
- Etapa 4: adicionar endpoints
- Etapa 5: testar seu acelerador
- Etapa 6 (opcional): excluir seu acelerador

Antes de começar

Antes de criar um acelerador, crie pelo menos um recurso que você possa adicionar como um endpoint para o qual direcionar o tráfego. Por exemplo, crie um dos seguintes:

- Inicie pelo menos uma instância do Amazon EC2 para adicionar como endpoint. Para obter mais informações, consulte Criar seus recursos do EC2 e iniciar sua instância do EC2 no Guia do usuário do Amazon EC2.
- Opcionalmente, crie um ou mais Network Load Balancers ou Application Load Balancers que incluam instâncias do EC2. Para obter mais informações, consulte Criar um Network Load Balancer no Guia do usuário para Network Load Balancers.

Ao criar um recurso para adicionar ao Global Accelerator, esteja ciente do seguinte:

- Ao adicionar um Application Load Balancer interno ou um endpoint de instância do EC2 no Global Accelerator, você permite que o tráfego da Internet flua diretamente de e para o endpoint em nuvens privadas virtuais (VPCs), direcionando-o para uma sub-rede privada. A VPC que contém o balanceador de carga ou a instância do EC2 deve ter um gateway da internet vinculado a ela, para indicar que a VPC aceita o tráfego da Internet. Para ter mais informações, consulte Conexões de VPC seguras no AWS Global Accelerator.

- O Global Accelerator exige que suas regras de roteador e firewall permitam que o tráfego de entrada dos endereços IP associados aos verificadores de integridade do Amazon Route 53 conclua verificações de integridade para endpoints de endereço IP Elastic ou de instâncias do EC2. Você pode encontrar informações sobre os intervalos de endereços IP associados aos verificadores de integridade do Route 53 em Intervalos de endereços IP dos servidores do Amazon Route 53 no Guia do desenvolvedor do Amazon Route 53.

Etapa 1: criar um acelerador padrão

Ao criar um acelerador padrão, você pode escolher IPv4 ou pilha dupla para os endereços IP estáticos que o Global Accelerator atribui ao seu acelerador. A pilha dupla é compatível com endereços IP IPv4 e IPv6.

Para criar um acelerador

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Escolha Criar acelerador.
3. Forneça um nome para o acelerador.
4. Em Tipo de acelerador, selecione Padrão.
5. Em Tipo de endereço IP, selecione IPv4 ou Pilha dupla.
6. Opcionalmente, adicione uma ou mais tags para ajudar você a identificar seus recursos do Global Accelerator.
7. Escolha Próximo.

Etapa 2: adicionar receptores

Criar um receptor para processar conexões de entrada de seus usuários para o Global Accelerator.

Para criar um receptor

1. Na página Adicionar receptor, insira as portas ou os intervalos de portas que você deseja associar ao receptor. Os receptores são compatíveis com as portas 1 a 65535.
2. Escolha o protocolo ou protocolos para as portas que você inseriu.
3. Opcionalmente, escolha habilitar a afinidade com o cliente. A afinidade com o cliente para um receptor significa que o Global Accelerator garante que as conexões de um endereço IP de

origem específico (cliente) sejam sempre roteadas para o mesmo endpoint. Para habilitar esse comportamento, na lista suspensa, escolha IP de origem.

O padrão é Nenhum, o que significa que a afinidade com o cliente não está habilitada e o Global Accelerator distribui o tráfego igualmente entre os endpoints nos grupos de endpoints do receptor.

Para ter mais informações, consulte Como funciona a afinidade com o cliente no Global Accelerator.

4. Opcionalmente, escolha Adicionar receptor para adicionar um receptor adicional.
5. Quando terminar de adicionar receptores, escolha Avançar.

Etapa 3: adicionar grupos de endpoints

Adicione um ou mais grupos de endpoints, cada um associado a uma região da AWS específica.

Para adicionar um grupo de endpoints

1. Na página Adicionar grupos de endpoints, na seção para um receptor, escolha uma Região na lista suspensa.
2. Opcionalmente, em Indicador de tráfego, insira um número de 0 a 100 para definir uma porcentagem de tráfego para esse grupo de endpoints. A porcentagem é aplicada somente ao tráfego já direcionado a esse grupo de endpoints, não a todo tráfego de receptores. Por padrão, o indicador de tráfego para um grupo de endpoints é definido como 100 (ou seja, 100%).
3. Opcionalmente, para valores de verificação de integridade personalizados, escolha Configurar verificações de integridade. Quando você define as configurações de verificação de integridade, o Global Accelerator usa as configurações para verificações de integridade para endpoints de instância do EC2 e endereço IP elástico. Para endpoints do Network Load Balancer e do Application Load Balancer, o Global Accelerator usa as configurações de verificação de integridade que você já definiu para os próprios balanceadores de carga. Para ter mais informações, consulte Garantir acesso à verificação de integridade do seu acelerador.
4. Opcionalmente, escolha Adicionar grupo de endpoints para adicionar outros grupos de endpoints para esse ou outros receptores.
5. Escolha Próximo.

Etapa 4: adicionar endpoints

Adicionar um ou mais endpoints que estejam associados a grupos de endpoints específicos. Essa etapa não é obrigatória, mas nenhum tráfego é direcionado aos endpoints em uma região, a menos que os endpoints estejam incluídos em um grupo de endpoints.

Para adicionar endpoints

1. Na página Criar endpoints, na seção de um endpoint, escolha um Endpoint.
2. Opcionalmente, em Peso, insira um número de 0 a 255 para definir um peso para rotear o tráfego para esse endpoint. Ao adicionar pesos a endpoints, você configura o Global Accelerator para encaminhar o tráfego com base nas proporções especificadas. Por padrão, todos os endpoints têm peso de 128. Para ter mais informações, consulte Como os pesos dos endpoints funcionam para gerenciar o volume de tráfego.
3. Opcionalmente, em Preservar endereço IP do cliente, selecione Preservar endereço. (Para alguns tipos de endpoint, essa opção está selecionada e não pode ser desmarcada). Para ter mais informações, consulte Preservar os endereços IP do cliente no AWS Global Accelerator.
4. Opcionalmente, escolha Adicionar endpoint para adicionar mais endpoints.
5. Escolha Próximo.

Depois de escolher Avançar, no painel do Global Accelerator, você verá uma mensagem informando que seu acelerador está em andamento. Quando o processo estiver concluído, o status do acelerador no painel será Ativo.

Etapa 5: testar seu acelerador

Siga os passos para testar seu acelerador e garantir que o tráfego esteja sendo direcionado para seus endpoints. Por exemplo, execute um comando curl como o seguinte, substituindo um dos endereços IP estáticos do seu acelerador para mostrar as regiões da AWS em que as solicitações são processadas. Isso é especialmente útil se você definir pesos diferentes para endpoints ou ajustar o indicador de tráfego em grupos de endpoints.

Execute um comando curl como o seguinte, substituindo um dos endereços IP estáticos do seu acelerador, para chamar o endereço IP 100 vezes e, em seguida, gerar uma contagem de onde cada solicitação foi processada.

```
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;
```

Se você ajustou o indicador de tráfego em qualquer grupo de endpoints, esse comando pode ajudar você a confirmar se o acelerador está direcionando as porcentagens corretas de tráfego para grupos diferentes. Para obter mais informações, consulte os exemplos detalhados na seguinte postagem no blog, Gerenciamento de tráfego com o AWS Global Accelerator.

Etapa 6 (opcional): excluir seu acelerador

Se você criou um acelerador como teste ou se não estiver mais usando um acelerador, poderá excluí-lo. No console, desabilite o acelerador e, em seguida, você poderá excluí-lo. Você não precisa remover receptores e grupos de endpoints do acelerador.

Para excluir um acelerador usando uma operação de API em vez do console, você deve primeiro remover todos os receptores e grupos de endpoints associados ao acelerador e desabilitá-lo. Para obter mais informações, consulte a operação DeleteAccelerator na Referência da API do AWS Global Accelerator.

Lembre-se do seguinte ao remover endpoints ou grupos de endpoints ou excluir um acelerador:

- Quando você cria um acelerador, o Global Accelerator fornece um conjunto de dois endereços IP estáticos. Os endereços IP são atribuídos ao seu acelerador enquanto ele existir, mesmo se você desabilitar o acelerador e ele não aceitar ou rotear mais o tráfego. No entanto, ao excluir um acelerador, você perde os endereços IP estáticos atribuídos ao acelerador e, portanto, não pode mais rotear o tráfego usando-os. Como prática recomendada, verifique se você tem permissões para evitar excluir os aceleradores acidentalmente. Você pode usar políticas do IAM com o Global Accelerator, por exemplo, permissões baseadas em tags, para limitar os usuários que têm permissão para excluir um acelerador. Para ter mais informações, consulte ABAC com Global Accelerator.
- Se você encerrar uma instância do EC2 antes de removê-la de um grupo de endpoints no Global Accelerator e depois criar outra instância com o mesmo endereço IP privado e as verificações de integridade passarem, o Global Accelerator roteará o tráfego para o novo endpoint. Se você não quiser que isso aconteça, remova a instância do EC2 do grupo de endpoints antes de encerrar a instância.

Para excluir um acelerador

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Escolha o acelerador que você deseja excluir.
3. Selecione a opção Editar.
4. Selecione Desabilitar acelerador e depois Salvar.
5. Escolha o acelerador que você deseja excluir.
6. Escolha Excluir acelerador.
7. Na caixa de diálogo de confirmação, escolha Excluir.

Introdução ao acelerador de roteamento personalizado

Esta seção fornece etapas para criar um acelerador de roteamento personalizado, que roteia o tráfego de forma determinística para destinos de instância do Amazon EC2 em endpoints de sub-rede de nuvem privada virtual (VPC).

Tarefas

- Antes de começar
- Etapa 1: criar um acelerador de roteamento personalizado
- Etapa 2: adicionar receptores
- Etapa 3: adicionar grupos de endpoints
- Etapa 4: adicionar endpoints
- Etapa 5 (opcional): excluir seu acelerador

Antes de começar

Antes de criar um acelerador de roteamento personalizado, crie um recurso que você possa adicionar como um endpoint para o qual direcionar o tráfego. Um endpoint de acelerador de roteamento personalizado deve ser uma sub-rede de nuvem privada virtual (VPC), que pode incluir várias instâncias do Amazon EC2. Para obter instruções sobre como criar os recursos, consulte o seguinte:

- Crie uma sub-rede VPC. Para obter mais informações, consulte Criar e configurar sua VPC no Guia de administração do AWS Directory Service.
- Opcionalmente, inicie uma ou mais instâncias do Amazon EC2 em sua VPC. Para obter mais informações, consulte Criar seus recursos do EC2 e iniciar sua instância do EC2 no Guia do usuário do Amazon EC2.

Ao criar um recurso para adicionar ao Global Accelerator, esteja ciente do seguinte:

- Ao adicionar um endpoint de instância do EC2 no Global Accelerator, você permite que o tráfego da Internet flua diretamente de e para o endpoint em uma VPC, direcionando-o para uma sub-rede privada. A VPC que contém a instância do EC2 deve ter um gateway da internet anexado a ela, para indicar que a VPC aceita o tráfego da Internet. Para ter mais informações, consulte Conexões de VPC seguras no AWS Global Accelerator.

Antes de criar um acelerador de roteamento personalizado, verifique as práticas recomendadas descritas em Diretrizes e restrições para aceleradores de roteamento personalizados.

Etapa 1: criar um acelerador de roteamento personalizado

Para criar um acelerador

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Forneça um nome para o acelerador.
3. Em Tipo de acelerador, selecione Roteamento personalizado.
4. Opcionalmente, adicione uma ou mais tags para ajudá-lo a identificar seus recursos do acelerador.
5. Escolha Avançar para adicionar receptores, grupos de endpoints e endpoints de sub-rede VPC.

Etapa 2: adicionar receptores

Criar um receptor para processar conexões de entrada de seus usuários para o Global Accelerator.

O intervalo que você especifica ao criar um receptor define quantas combinações de portas de receptor e endereços IP de destino você pode usar com seu acelerador de roteamento personalizado. Para obter o máximo de flexibilidade, recomendamos que você especifique um

grande intervalo de portas. Cada intervalo de portas do receptor que você especificar deve incluir no mínimo 16 portas.

Para criar um receptor

1. Na página Adicionar receptor, insira as portas ou os intervalos de portas que você deseja associar ao receptor. Os receptores são compatíveis com as portas 1 a 65535.
2. Escolha o protocolo ou protocolos para as portas que você inseriu.
3. Opcionalmente, escolha Adicionar receptor para adicionar um receptor adicional.
4. Quando terminar de adicionar receptores, escolha Avançar.

Etapa 3: adicionar grupos de endpoints

Adicione um ou mais grupos de endpoints, cada um associado a uma região da AWS específica. Para cada grupo de endpoints, especifique um ou mais conjuntos de intervalos de portas e protocolos. O Global Accelerator os usa para direcionar o tráfego para instâncias do Amazon EC2 em sub-redes na região.

Para cada intervalo de portas fornecido, você também especifica o protocolo a ser usado: UDP, TCP ou UDP e TCP.

Para adicionar um grupo de endpoints

1. Na página Adicionar grupos de endpoints, na seção para um receptor, escolha uma Região.
2. Em Conjuntos de portas e protocolos, insira intervalos de portas e protocolos para suas instâncias do Amazon EC2.

   - Insira Da porta e Até a porta para especificar um intervalo de portas.
   - Para cada intervalo de portas, especifique o protocolo ou protocolos desse intervalo.

   O intervalo de portas não precisa ser um subconjunto do intervalo de portas do receptor, mas deve haver um total de portas suficiente no intervalo de portas do receptor para ser compatível com o número total de portas que você especificar.
3. Escolha Salvar.
4. Opcionalmente, escolha Adicionar grupo de endpoints para adicionar outros grupos de endpoints para esse ou outros receptores.

5. Escolha Próximo.

Etapa 4: adicionar endpoints de sub-rede VPC

Adicionar um ou mais endpoints de sub-rede de nuvem privada virtual (VPC) para esse grupo de endpoint regional. Os endpoints para aceleradores de roteamento personalizados definem as sub-redes VPC que podem receber tráfego por meio de um acelerador de roteamento personalizado. Cada sub-rede pode conter um ou vários destinos de instância do Amazon EC2.

Quando você adiciona um endpoint de sub-rede VPC, o Global Accelerator gera novos mapeamentos de portas que você pode usar para rotear o tráfego para os endereços IP da instância do EC2 de destino na sub-rede. Em seguida, você pode usar a API do Global Accelerator para obter uma lista estática de todos os mapeamentos de portas para a sub-rede e usar o mapeamento para direcionar deterministicamente o tráfego para instâncias específicas do EC2.

Para adicionar endpoints

1. Na página Adicionar endpoints, na seção do grupo de endpoints ao qual você deseja adicionar o endpoint, escolha uma ID de sub-rede para o Endpoint.
2. Opcionalmente, siga um dos procedimentos a seguir para habilitar o tráfego para destinos de instâncias do EC2 na sub-rede:

   - Para permitir que o tráfego seja direcionado para todos os endpoints e portas do EC2 na sub-rede, selecione Permitir todo o tráfego
   - Para permitir tráfego para endpoints e portas do EC2 específicos na sub-rede, selecione Permitir tráfego para endereços de socket de destino específicos. Em seguida, especifique os endereços IP e as portas ou os intervalos de portas a serem permitidos. Por fim, escolha Permitir esses destinos.

   Por padrão, nenhum tráfego é permitido nos endpoints da sub-rede. Se você não selecionar uma opção para permitir o tráfego, o tráfego será negado para todos os destinos na sub-rede.

   > **Note**
   >
   > Se você quiser habilitar o tráfego para instâncias e portas específicas do EC2 na sub-rede, você pode fazer isso programaticamente. Para obter mais informações, consulte AllowCustomRoutingTraffic na Referência da API do AWS Global Accelerator.

3. Escolha Próximo.

Depois de escolher Avançar, no painel do Global Accelerator, você verá uma mensagem informando que seu acelerador está em andamento. Quando o processo estiver concluído, o status do acelerador no painel será Ativo.

Etapa 5 (opcional): excluir seu acelerador

Se você criou um acelerador como teste ou se não estiver mais usando um acelerador, poderá excluí-lo. No console, desabilite o acelerador e, em seguida, você poderá excluí-lo. Você não precisa remover receptores e grupos de endpoints do acelerador.

Para excluir um acelerador usando uma operação de API em vez do console, você deve primeiro remover todos os receptores e grupos de endpoints associados ao acelerador e desabilitá-lo. Para obter mais informações sobre essa operação, consulte DeleteCustomRoutingAccelerator na Referência da API do AWS Global Accelerator.

Esteja ciente do seguinte ao excluir um acelerador:

- Quando você cria um acelerador, o Global Accelerator fornece um conjunto de dois endereços IP estáticos. Os endereços IP são atribuídos ao seu acelerador enquanto ele existir, mesmo se você desabilitar o acelerador e ele não aceitar ou rotear mais o tráfego. No entanto, ao excluir um acelerador, você perde os endereços IP estáticos atribuídos ao acelerador e, portanto, não pode mais rotear o tráfego usando-os. Como prática recomendada, verifique se você tem permissões para evitar excluir os aceleradores acidentalmente. Você pode usar políticas do IAM, como permissões baseadas em tags, com o Global Accelerator para limitar os usuários que têm permissão para excluir um acelerador. Para ter mais informações, consulte ABAC com Global Accelerator.

Para excluir um acelerador

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Escolha o acelerador que você deseja excluir.
3. Selecione a opção Editar.
4. Selecione Desabilitar acelerador e depois Salvar.
5. Escolha o acelerador que você deseja excluir.

6. Escolha Excluir acelerador.
7. Na caixa de diálogo de confirmação, escolha Excluir.

Ações comuns de API para o AWS Global Accelerator

Esta seção lista as ações comuns para o AWS Global Accelerator usadas com os recursos do Global Accelerator, com links para a documentação relevante.

Ações a serem usadas com aceleradores padrão

A tabela a seguir lista as ações comuns do Global Accelerator usadas com aceleradores padrão, com links para a documentação relevante.

Ação	Como usar o console do Global Accelerator	Como usar a API do Global Accelerator
Criar um acelerador padrão	Consulte Introdução ao acelerador padrão	Consulte `CreateAccelerator`
Criar um receptor para um acelerador padrão	Consulte Receptores de aceleradores padrão no AWS Global Accelerator	Consulte `CreateListener`
Criar um grupo de endpoints para um acelerador padrão	Consulte Grupos de endpoints para aceleradores padrão no AWS Global Accelerator	Consulte `CreateEndpointGroup`
Atualizar um acelerador padrão	Consulte Aceleradores padrão no AWS Global Accelerator	Consulte `UpdateAccelerator`
Atualizar um grupo de endpoints	Consulte Adicionar um grupo de endpoints padrão	Consulte `UpdateEndpointGroup`
Adicionar um endpoint	Consulte Adicionar um endpoint padrão	Consulte `AddEndpoints`
Remover um endpoint	Consulte Adicionar um endpoint padrão	Consulte `RemoveEndpoints`
Listar aceleradores padrão	Consulte Visualizar seus aceleradores	Consulte `ListAccelerator`

Ação	Como usar o console do Global Accelerator	Como usar a API do Global Accelerator
Obter todas as informações sobre um acelerador	Consulte Visualizar seus aceleradores	Consulte DescribeAccelerator
Excluir um acelerador	Consulte Criar acelerador	Consulte DeleteAccelerator

Ações a serem usadas com aceleradores de roteamento personalizados

A tabela a seguir lista as ações comuns do Global Accelerator usadas com aceleradores de roteamento personalizados, com links para a documentação relevante.

Ação	Como usar o console do Global Accelerator	Como usar a API do Global Accelerator
Criar um acelerador de roteamento personalizado	Consulte Introdução ao acelerador de roteamento personalizado	Consulte CreateCustomRoutingAccelerator
Criar um receptor para um acelerador de roteamento personalizado	Consulte Receptores de aceleradores de roteamento personalizados no Global Accelerator	Consulte CreateCustomRoutingListener
Criar um grupo de endpoints para um acelerador de roteamento personalizado	Consulte Grupos de endpoints para aceleradores de roteamento personalizados no Global Accelerator	Consulte CreateCustomRoutingEndpointGroup
Atualizar um acelerador de roteamento personalizado	Consulte Aceleradores de roteamento personalizados no AWS Global Accelerator	Consulte UpdateCustomRoutingAccelerator

Ação	Como usar o console do Global Accelerator	Como usar a API do Global Accelerator
Listar seus aceleradores de roteamento personalizados	Consulte Visualizar aceleradores de roteamento personalizados no Global Accelerator	Consulte ListCustomRoutingAccelerator
Obter todas as informações sobre um acelerador de roteamento personalizado	Consulte Visualizar aceleradores de roteamento personalizados no Global Accelerator	Consulte DescribeCustomRoutingAccelerator
Excluir um acelerador de roteamento personalizado	Consulte Criar um acelerador de roteamento personalizado no Global Accelerator	Consulte DeleteCustomRoutingAccelerator
Obter o mapeamento de portas estáticas para um acelerador de roteamento personalizado	N/D	Consulte ListCustomRoutingPortMappings
Permitir todo o tráfego de destino para uma sub-rede em um acelerador de roteamento personalizado	Consulte Adicionar um endpoint de sub-rede da VPC a um acelerador de roteamento personalizado	Consulte AllowCustomRoutingTraffic
Negar todo o tráfego de destino de uma sub-rede em um acelerador de roteamento personalizado	Consulte Adicionar um endpoint de sub-rede da VPC a um acelerador de roteamento personalizado	Consulte DenyCustomRoutingTraffic
Permitir o tráfego para destinos específicos em um acelerador de roteamento personalizado	Consulte Adicionar um endpoint de sub-rede da VPC a um acelerador de roteamento personalizado	Consulte AllowCustomRoutingTraffic

Ação	Como usar o console do Global Accelerator	Como usar a API do Global Accelerator
Negar o tráfego para destinos específicos em um acelerador de roteamento personalizado	Consulte Adicionar um endpoint de sub-rede da VPC a um acelerador de roteamento personalizado	Consulte DenyCustomRoutingTraffic

Ações a serem usadas com a compatibilidade entre contas no Global Accelerator

A tabela a seguir lista as ações comuns do Global Accelerator usadas com a compatibilidade entre contas no Global Accelerator, com links para a documentação relevante.

Ação	Como usar o console do Global Accelerator	Como usar a API do Global Accelerator
Criar um anexo entre contas	Consulte Criar um anexo entre contas no AWS Global Accelerator	Consulte CreateCrossAccountAttachment
Excluir um anexo entre contas	Consulte Criar um anexo entre contas no AWS Global Accelerator	Consulte DeleteCrossAccountAttachment
Descrever as informações incluídas em um anexo entre contas	Consulte Identificar recursos entre contas no Global Accelerator	Consulte DescribeCrossAccountAttachment
Listar anexos entre contas em uma conta	Consulte Identificar recursos entre contas no Global Accelerator	Consulte ListCrossAccountAttachments
Atualizar um anexo entre contas	Consulte Criar um anexo entre contas no AWS Global Accelerator	Consulte UpdateCrossAccountAttachment

Como trabalhar com aceleradores padrão no AWS Global Accelerator

Este capítulo inclui procedimentos e recomendações para criar aceleradores padrão no AWS Global Accelerator, incluindo a configuração de aceleradores, receptores, grupos de endpoints e endpoints. Com um acelerador padrão, o Global Accelerator escolhe o endpoint íntegro mais próximo para seu tráfego.

Se, em vez disso, você quiser usar a lógica de aplicativo personalizada para direcionar um ou mais usuários para um endpoint específico entre muitos endpoints, crie um acelerador de roteamento personalizado. Para ter mais informações, consulte Como trabalhar com aceleradores de roteamento personalizados no AWS Global Accelerator.

Para configurar um acelerador padrão, faça o seguinte:

1. Crie um acelerador e escolha a opção de acelerador padrão.
2. Em Tipo de endereço, selecione IPv4 ou Pilha dupla.
3. Opcionalmente, configure os endereços IP estáticos trazendo seu próprio endereço IP.
4. Adicione um receptor com um conjunto específico de portas ou intervalo de portas e escolha o protocolo a ser aceito: TCP ou UDP.
5. Adicione um ou mais grupos de endpoints, um para cada Região da AWS em que você tenha recursos de endpoint.
6. Adicione um ou mais endpoints aos grupos de endpoints. Isso não é necessário, mas o tráfego não será roteado se você não tiver nenhum endpoint. Para saber mais sobre os tipos de endpoints e requisitos, consulte ???.

As seções a seguir fornecem etapas para adicionar, excluir e configurar aceleradores padrão e seus componentes, incluindo receptores, grupos de endpoints e endpoints.

Tópicos

Aceleradores padrão no AWS Global Accelerator

Um acelerador padrão no AWS Global Accelerator direciona o tráfego pela rede global da AWS para os endpoints que você inclui nas Regiões da AWS especificadas. Cada acelerador inclui um ou mais receptores. Um receptor processa conexões de entrada de clientes com o Global Accelerator, com base no protocolo (ou protocolos) e na porta (ou intervalo de portas) que você configura.

Para aceleradores padrão, o Global Accelerator direciona o tráfego para o endpoint regional ideal com base na integridade, na localização do cliente e nas políticas que você configura, o que aumenta a disponibilidade de seus aplicativos. Os endpoints para aceleradores padrão podem ser Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços IP elásticos localizados em uma Região da AWS ou em várias.

> **Important**
>
> Por padrão, o Global Accelerator fornece endereços IP estáticos associados ao seu acelerador. Os endereços IP são atribuídos ao seu acelerador enquanto ele existir, mesmo se você desabilitar o acelerador e ele não aceitar ou rotear mais o tráfego. No entanto, ao excluir um acelerador, você perde os endereços IP estáticos do Global Accelerator que estão atribuídos ao acelerador, de modo que você não pode mais rotear o tráfego usando-os. Como prática recomendada, verifique se você tem permissões para evitar excluir os aceleradores acidentalmente. Você pode usar políticas do IAM com o Global Accelerator, por exemplo, permissões baseadas em tags, para limitar os usuários que têm permissão para excluir um acelerador. Para ter mais informações, consulte ABAC com Global Accelerator.

Esta seção inclui procedimentos para trabalhar com um acelerador padrão no console do Global Accelerator. Se você quiser usar operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Conteúdo

- Comparar o uso de endereços IP estáticos globais com endereços IP estáticos regionais

Criar acelerador

Esta seção explica como criar um acelerador padrão no console. Para trabalhar com o Global Accelerator de forma programática, consulte a Referência da API do AWS Global Accelerator.

Para criar um acelerador padrão

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Escolha Criar acelerador.
3. Forneça um nome para o acelerador.
4. Em Tipo de acelerador, selecione Padrão.
5. Em Tipo de endereço IP, selecione IPv4 ou Pilha dupla.
6. Opcionalmente, se você trouxe seus próprios intervalos de endereços IP para a AWS (BYOIP), você pode especificar um endereço IP estático para seu acelerador, um de cada grupo de endereços. Faça essa escolha para cada um dos dois endereços IP estáticos do seu acelerador.

   - Para cada endereço IP estático, escolha o grupo de endereços IP a ser usado.

     > **Note**
     >
     > Você deve escolher um grupo de endereços IP diferente para cada endereço IP estático. Essa restrição ocorre porque o Global Accelerator atribui cada intervalo de endereços a uma zona da rede diferente, para alta disponibilidade.

   - Se você escolheu seu próprio grupo de endereços IP, escolha também um endereço IP específico do grupo. Se você escolher o grupo de endereços IP padrão da Amazon, o Global Accelerator atribuirá um endereço IP específico ao seu acelerador.

   Para obter mais informações sobre os requisitos para especificar ou atualizar endereços IP estáticos com BYOIP, consulte Requisitos ao atualizar um acelerador para alterar o endereço IP.
7. Opcionalmente, adicione uma ou mais tags para ajudá-lo a identificar seus recursos do acelerador.
8. Escolha Avançar para adicionar receptores, grupos de endpoints e endpoints.

Atualizar acelerador

Esta seção explica como atualizar um acelerador padrão no console. Para trabalhar com o Global Accelerator de forma programática, consulte a Referência da API do AWS Global Accelerator.

Para atualizar um acelerador padrão

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na lista de aceleradores, escolha um e, em seguida, escolha Editar.
3. Na página Editar acelerador, faça alterações, como as seguintes:
   - Altere o nome do acelerador.
   - Desabilite o acelerador para que ele não aceite ou roteie mais o tráfego, ou para que você possa excluí-lo.
   - Habilite o acelerador, se ele estiver desabilitado.
   - Atualize o tipo de endereço IP. Se estiver definido como IPv4, altere-o para pilha dupla. Ou, se for de pilha dupla, altere-o para IPv4.
   - Atualize as tags.
4. Escolha Salvar alterações.

Se você desabilitar um acelerador, lembre-se de que:

- Os endereços IP estáticos do Global Accelerator permanecem atribuídos ao seu acelerador, mesmo se você desabilitar o acelerador e ele não aceitar ou rotear mais o tráfego. Seu acelerador retém os mesmos endereços IP estáticos enquanto o acelerador existir.
- No entanto, se você excluir o acelerador, perderá os endereços IP estáticos do Global Accelerator que estão atribuídos a ele. Nesse momento, você não pode mais rotear o tráfego usando os endereços.

Se fizer alterações no tipo de endereço IP, lembre-se de que:

- Somente um acelerador com endpoints de pilha dupla pode ser alterado para um tipo de endereço IP de pilha dupla.
- Se você alterar o tipo de endereço IP de um acelerador de pilha dupla para IPv4, o Global Accelerator salvará os endereços IP IPv6 atribuídos ao acelerador. Isso significa que, se você

alterar o tipo de endereço IP do acelerador de volta para pilha dupla, os endereços IP estáticos IPv6 originais serão restaurados para o acelerador.

Se você quiser alterar outras funcionalidades do seu acelerador, como adicionar ou remover endpoints, atualizar indicadores de tráfego ou ajustar os pesos dos endpoints, consulte as seções específicas que abordam esses tópicos, como as seguintes:

- Adicionar um receptor padrão
- Adicionar um grupo de endpoints padrão
- Adicionar um endpoint padrão

Excluir acelerador

Se você criou um acelerador como teste ou se não estiver mais usando um acelerador, poderá excluí-lo. No console, desabilite o acelerador e, em seguida, você poderá excluí-lo. Você não precisa remover receptores e grupos de endpoints do acelerador.

Para excluir um acelerador usando uma operação de API em vez do console, você deve primeiro remover todos os receptores e grupos de endpoints associados ao acelerador e depois desabilitá-lo. Para obter mais informações, consulte a operação DeleteAccelerator na referência da API do AWS Global Accelerator.

Para desabilitar um acelerador

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na lista, escolha um acelerador que você deseja desabilitar.
3. Selecione a opção Editar.
4. Selecione Desabilitar acelerador e depois Salvar.

Para excluir um acelerador

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na lista, escolha um acelerador que você deseja excluir.
3. Escolha Excluir.

> **Note**
>
> Se você não tiver desabilitado o acelerador, a opção Excluir não estará disponível.

4. Na caixa de diálogo de confirmação, escolha Excluir.

> **Important**
>
> Ao excluir um acelerador, você perde os endereços IP estáticos atribuídos ao acelerador e, portanto, não pode mais rotear o tráfego usando-os.

Visualizar seus aceleradores

Você pode visualizar informações sobre os aceleradores no console. Para ver as descrições de seus aceleradores programaticamente, consulte ListAccelerators e DescribeAccelerator na Referência da API do AWS Global Accelerator.

Para visualizar informações sobre seu acelerador

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Para ver detalhes sobre um acelerador, na lista, escolha um acelerador e, em seguida, escolha Visualizar.

Adicionar um acelerador ao criar um balanceador de carga

Ao criar um Application Load Balancer ou Network Load Balancer no AWS Management Console, você tem a opção de adicionar um acelerador ao mesmo tempo. O Elastic Load Balancing e o Global Accelerator trabalham juntos para adicionar o acelerador de forma transparente para você. O acelerador é criado em sua conta, com o balanceador de carga como um endpoint. O uso de um acelerador fornece endereços IP estáticos e melhora a disponibilidade e o desempenho de seus aplicativos. (Saiba mais sobre aceleradores lendo O que é o AWS Global Accelerator?).

> **Important**
>
> Para criar um acelerador, é necessário que as permissões corretas estejam em vigor. Para ter mais informações, consulte Exemplos de políticas baseadas em identidade para o AWS Global Accelerator.

Configurar e visualizar seu acelerador

Você deve atualizar sua configuração de DNS para direcionar o tráfego para os endereços IP estáticos ou o nome de DNS do acelerador. O tráfego não passará do acelerador ao seu balanceador de carga até que suas alterações de configuração sejam concluídas.

Depois de criar seu balanceador de carga escolhendo o complemento do Global Accelerator no console do Amazon EC2, acesse a guia Serviços integrados para ver os endereços IP estáticos e o nome do Sistema de Nomes de Domínio (DNS) do seu acelerador. Você usa essas informações para começar a rotear o tráfego do usuário para o balanceador de carga pela rede global da AWS. Para obter mais informações sobre o nome do DNS atribuído ao acelerador, consulte Endereçamento de DNS e domínios personalizados no AWS Global Accelerator.

Você pode visualizar e configurar seu acelerador navegando até o Global Accelerator no AWS Management Console. Por exemplo, você pode ver os aceleradores associados à sua conta ou adicionar outros balanceadores de carga ao seu acelerador. Para ter mais informações, consulte Visualizar seus aceleradores e Criar acelerador.

Definição de preço

Com o AWS Global Accelerator, você paga somente por aquilo que usa. Uma taxa por hora e custos de transferência de dados são cobrados para cada acelerador em sua conta. Para obter mais informações, consulte Preços do AWS Global Accelerator.

Interromper o uso do acelerador

Se quiser deixar de rotear o tráfego pelo Global Accelerator para o balanceador de carga, faça o seguinte:

1. Atualize sua configuração do DNS para apontar seu tráfego diretamente para o balanceador de carga.
2. Exclua o balanceador de carga do acelerador. Para obter mais informações, consulte Para remover um endpoint em Adicionar um endpoint padrão.

3. Exclui o acelerador. Para ter mais informações, consulte Excluir acelerador.

Comparar o uso de endereços IP estáticos globais com endereços IP estáticos regionais

Se você quiser usar um endereço IP estático na frente de um recurso da AWS, como uma instância do Amazon EC2, você tem várias opções. Por exemplo, você pode alocar um endereço IP elástico, que é um endereço IPv4 ou IPv6 estático que você pode associar a uma instância ou interface de rede do Amazon EC2 em uma única região da AWS.

Se você tem um público global, pode criar um acelerador com o Global Accelerator para obter endereços estáticos globais que são anunciados a partir de locais da borda da AWS em todo o mundo. Para IPv4, o Global Accelerator fornece dois endereços IPv4 estáticos globais. Para pilha dupla, o Global Accelerator fornece um total de quatro endereços IP estáticos globais: dois endereços IPv4 e dois endereços IPv6. Se você já tem recursos da AWS configurados para seus aplicativos, em uma ou várias regiões, incluindo instâncias do Amazon EC2, Network Load Balancers e Application Load Balancers, você pode adicioná-los facilmente ao Global Accelerator para fornecê-los com endereços IP estáticos globais. Para ter mais informações, consulte Requisitos para recursos que você adiciona como endpoints do acelerador.

Optar por usar endereços IP estáticos globais provisionados pelo Global Accelerator também pode melhorar a disponibilidade e o desempenho de seus aplicativos. Com o Global Accelerator, os endereços IP estáticos aceitam tráfego de entrada na rede global da AWS a partir do local da borda mais próximo de seus usuários. Maximizar o tempo de permanência do tráfego na rede da AWS pode proporcionar uma experiência melhor e mais rápida ao cliente. Para ter mais informações, consulte Como o AWS Global Accelerator funciona .

Você pode adicionar um acelerador a partir do AWS Management Console ou usando operações de API com a CLI ou os SDKs da AWS. Para ter mais informações, consulte Criar acelerador.

Observe o seguinte ao adicionar um acelerador:

- Os endereços IP estáticos globais provisionados pelo Global Accelerator permanecem atribuídos a você enquanto seu acelerador existir, mesmo se você desabilitar o acelerador e ele não aceitar ou não rotear mais o tráfego. No entanto, se excluir um acelerador, você perderá todos os endereços IP estáticos que estão atribuídos a ele. Para ter mais informações, consulte Excluir acelerador.

- No caso do Global Accelerator, você paga somente por aquilo que usa. Uma taxa por hora e custos de transferência de dados são cobrados para cada acelerador em sua conta. Para obter mais informações, consulte Preços do AWS Global Accelerator.

Receptores de aceleradores padrão no AWS Global Accelerator

Com o AWS Global Accelerator, você adiciona receptores que processam conexões de entrada de clientes com base nas portas e protocolos que você especifica. Os receptores são compatíveis com os protocolos TCP e UDP.

Você define um receptor padrão ao criar seu acelerador padrão e pode adicionar mais receptores a qualquer momento. Você associa cada receptor a um ou mais grupos de endpoints e associa cada grupo de endpoints a uma região da AWS.

Opcionalmente, você pode configurar a afinidade com o cliente para um receptor. Com a afinidade com o cliente, o Global Accelerator direciona todas as solicitações de um usuário em um endereço IP de origem específico (cliente) para o mesmo recurso de endpoint. A escolha dessa opção mantém a afinidade com o cliente para seus usuários.

Conteúdo

Adicionar um receptor padrão

Esta seção fornece as etapas para criar um receptor padrão no console do AWS Global Accelerator. Para concluir essa tarefa usando uma operação de API em vez do console, consulte `CreateListener` na Referência de API do AWS Global Accelerator.

Para adicionar um listener

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na página Aceleradores, escolha um acelerador.

3. Escolha Add listener.
4. Na página Adicionar receptor, insira as portas ou os intervalos de portas que você deseja associar ao receptor. Os receptores são compatíveis com as portas 1 a 65535.
5. Escolha o protocolo para as portas que você inseriu.
6. Opcionalmente, escolha habilitar a afinidade com o cliente. A afinidade com o cliente para um receptor significa que o Global Accelerator garante que as conexões de um endereço IP de origem específico (cliente) sejam sempre roteadas para o mesmo endpoint. Para habilitar esse comportamento, na lista suspensa, escolha IP de origem.

   O padrão é Nenhum, o que significa que a afinidade com o cliente não está habilitada e o Global Accelerator distribui o tráfego igualmente entre os endpoints nos grupos de endpoints do receptor.

   Para ter mais informações, consulte Como funciona a afinidade com o cliente no Global Accelerator.
7. Escolha Add listener.

Editar um receptor padrão

Esta seção fornece as etapas para editar um receptor padrão no console do AWS Global Accelerator. Para concluir essa tarefa usando uma operação de API em vez do console, consulte `UpdateListener` na Referência de API do AWS Global Accelerator.

Para editar um receptor padrão

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na página Aceleradores, escolha um acelerador.
3. Escolha um receptor e, em seguida, escolha Editar receptor.
4. Na página Editar receptor, altere as portas, os intervalos de portas ou os protocolos que você deseja associar ao receptor.
5. Opcionalmente, escolha habilitar a afinidade com o cliente. A afinidade com o cliente para um receptor significa que o Global Accelerator garante que as conexões de um endereço IP de origem específico (cliente) sejam sempre roteadas para o mesmo endpoint. Para habilitar esse comportamento, na lista suspensa, escolha IP de origem.

O padrão é Nenhum, o que significa que a afinidade com o cliente não está habilitada e o Global Accelerator distribui o tráfego igualmente entre os endpoints nos grupos de endpoints do receptor.

Para ter mais informações, consulte Como funciona a afinidade com o cliente no Global Accelerator.

6. Escolha Salvar.

Remover um receptor padrão

Esta seção fornece as etapas para remover um receptor padrão no console do AWS Global Accelerator. Para concluir essa tarefa usando uma operação de API em vez do console, consulte `DeleteListener` na Referência de API do AWS Global Accelerator.

Para remover um receptor

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na página Aceleradores, escolha um acelerador.
3. Escolha um receptor e, em seguida, escolha Remover.
4. Na caixa de diálogo de confirmação, escolha Remover.

Como funciona a afinidade com o cliente no Global Accelerator

Se você usa aplicativos com estado com um acelerador padrão, pode configurar a afinidade com o cliente para que o Global Accelerator direcione todas as solicitações de um usuário em um endereço IP de origem (cliente) específico para o mesmo recurso de endpoint. A escolha dessa opção mantém a afinidade com o cliente para seus usuários.

Por padrão, a afinidade com o cliente para um receptor padrão é definida como Nenhuma e o Global Accelerator distribui o tráfego igualmente entre os endpoints nos grupos de endpoints do receptor.

O Global Accelerator usa um algoritmo de hash de fluxo consistente para escolher o endpoint ideal para uma conexão do usuário. Se você configurar a afinidade com o cliente para seu recurso do Global Accelerator como Nenhuma, o Global Accelerator usará propriedades do conjunto de valores 5-tuple (IP de origem, porta de origem, IP de destino, porta de destino e protocolo) para selecionar o valor de hash. Em seguida, ele escolhe o endpoint que fornece o melhor desempenho. Se um

determinado cliente usar portas diferentes para se conectar ao Global Accelerator e você tiver especificado essa configuração, o Global Accelerator não poderá garantir que as conexões do cliente sejam sempre roteadas para o mesmo endpoint.

Se você quiser manter a afinidade com o cliente roteando um usuário específico, identificado pelo endereço IP de origem, para o mesmo endpoint sempre que ele se conectar, defina a afinidade com o cliente como IP de origem. Quando você especifica essa opção, o Global Accelerator usa as propriedades do conjunto de valores 2-tuple (IP de origem e IP de destino) para selecionar o valor de hash e rotear o usuário para o mesmo endpoint sempre que ele se conectar. Além disso, o Global Accelerator respeita a afinidade com o cliente ao rotear todas as conexões com o mesmo endereço IP de origem para o mesmo grupo de endpoints.

Às vezes, a manutenção da rede ou as interrupções criadas por variações no roteamento do tráfego da internet podem fazer com que o tráfego do cliente mude para diferentes locais da borda do Global Accelerator. Quando isso acontece, se o local da borda que agora atende ao tráfego do cliente preferir uma região da AWS diferente, não é garantido que a afinidade com o cliente seja mantida.

Além disso, lembre-se de que, quando você define pesos de endpoints em seu acelerador, em cenários específicos e limitados, o Global Accelerator substitui esses pesos para ajudar a garantir a disponibilidade. Quando o Global Accelerator está balanceando a carga do tráfego entre endpoints em um grupo de endpoints, ele deve, em determinadas circunstâncias, escolher entre preservar a disponibilidade do tráfego do cliente e respeitar os pesos dos endpoints. Por exemplo, com aceleradores em que o endereço IP do cliente é preservado, o Global Accelerator pode precisar substituir uma configuração de peso do endpoint para ajudar a evitar colisões de conexão.

Grupos de endpoints para aceleradores padrão no AWS Global Accelerator

Um grupo de endpoints roteia as solicitações para um ou mais endpoints registrados no AWS Global Accelerator. Ao adicionar um receptor em um acelerador padrão, você especifica os grupos de endpoints para os quais o Global Accelerator direcionará o tráfego. Um grupo de endpoints e todos os endpoints nele contidos devem estar em uma região da AWS. Você pode adicionar grupos de endpoints diferentes para finalidades diferentes, por exemplo, para testes de implantação azul/verde.

O Global Accelerator direciona o tráfego para grupos de endpoints em aceleradores padrão com base na localização do cliente e na integridade do grupo de endpoints. Se quiser, você também pode definir o percentual de tráfego a ser enviado para um grupo de endpoints. Você faz isso usando o indicador de tráfego para aumentar (dial up) ou diminuir (dial down) o tráfego do grupo. A

porcentagem é aplicada somente ao tráfego que o Global Accelerator já está direcionando para o grupo de endpoints, não a todo tráfego que chega a um receptor.

Você pode definir as configurações de verificação de integridade do Global Accelerator para cada grupo de endpoints. Ao atualizar as configurações de verificação de integridade, você pode alterar seus requisitos de pesquisa e verificação da integridade da instância do Amazon EC2 e dos endpoints de endereço IP elástico. Para endpoints do Network Load Balancer e do Application Load Balancer, defina as configurações de verificação de integridade no console do Elastic Load Balancing.

O Global Accelerator monitora continuamente a integridade de todos os endpoints incluídos em um grupo de endpoints padrão e roteia as solicitações somente para os endpoints ativos que estão íntegros. Para obter mais informações, consulte Garantir acesso à verificação de integridade do seu acelerador. Se não houver nenhum endpoint íntegro para o qual rotear o tráfego, o Global Accelerator roteia as solicitações para todos os endpoints.

Esta seção explica como trabalhar com grupos de endpoints para aceleradores padrão no console do AWS Global Accelerator. Se você quiser usar operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Conteúdo

Adicionar um grupo de endpoints padrão

Você trabalha com grupos de endpoints no console do AWS Global Accelerator ou usando uma operação de API. Você pode adicionar ou remover endpoints de um grupo de endpoints a qualquer momento.

Esta seção explica como adicionar grupos de endpoints padrão no console do AWS Global Accelerator. Se você quiser usar operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para adicionar um grupo de endpoints padrão

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na página Aceleradores, escolha um acelerador.
3. Na seção Receptores, em ID do receptor, escolha o ID do receptor ao qual você deseja adicionar um grupo de endpoints.
4. Escolha Adicionar grupo de endpoints.
5. Na seção do receptor, especifique uma região para o grupo de endpoints escolhendo uma na lista suspensa.
6. Opcionalmente, em Indicador de tráfego, insira um número de 0 a 100 para definir uma porcentagem de tráfego para esse grupo de endpoints. A porcentagem é aplicada somente ao tráfego que já está direcionado a esse grupo de endpoints, não a todo tráfego de receptores. Por padrão, o indicador de tráfego está definido como 100.
7. Como opção, para substituir a porta do receptor usada para rotear o tráfego para endpoints e rotear o tráfego para portas específicas nos endpoints, escolha Configurar substituições de portas. Para ter mais informações, consulte Substituir portas do receptor para portas restritas ou colisões de conexão.
8. Opcionalmente, para especificar valores personalizados de verificação de integridade a serem aplicados à instância do EC2 e aos endpoints de endereço IP elástico, escolha Configurar verificações de integridade. Para ter mais informações, consulte Garantir acesso à verificação de integridade do seu acelerador.
9. Opcionalmente, escolha Adicionar grupo de endpoints para adicionar outros grupos de endpoints para esse ou outros receptores.
10. Escolha Adicionar grupo de endpoints.

Editar um grupo de endpoints padrão

Esta seção explica como editar grupos de endpoints padrão no console do AWS Global Accelerator. Se você quiser usar operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para editar um grupo de endpoints

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na página Aceleradores, escolha um acelerador.
3. Na seção Receptores, em ID do receptor, escolha o ID do receptor ao qual o grupo de endpoints está associado.
4. Escolha Editar grupo de endpoints.
5. Na página Editar grupo de endpoints, altere a região, ajuste a porcentagem do indicador de tráfego ou escolha Configurar verificações de integridade para modificar as configurações da verificação de integridade.
6. Escolha Salvar.

Remover um grupo de endpoints padrão

Esta seção explica como remover grupos de endpoints padrão no console do AWS Global Accelerator. Se você quiser usar operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para remover um grupo de endpoints padrão

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na página Aceleradores, escolha um acelerador.
3. Na seção Receptores, escolha um receptor.
4. Na seção Grupos de endpoints, escolha um grupo de endpoints e, em seguida, escolha Remover.
5. Na caixa de diálogo de confirmação, escolha Remover.

Usar indicadores de tráfego para ajustar o fluxo de tráfego para regiões

Para cada grupo de endpoints padrão, você pode definir um indicador de tráfego para controlar a porcentagem de tráfego direcionado ao grupo de endpoints (Região da AWS). A porcentagem é aplicada somente ao tráfego que já está direcionado ao grupo de endpoints, não a todo o tráfego de receptores.

Observe que, quando você altera um indicador de tráfego, a configuração atualizada se aplica somente às novas conexões. As conexões existentes não são encerradas para ajustar o fluxo de tráfego atual.

Por padrão, o indicador de tráfego é definido como 100 (ou seja, 100%) para todos os grupos de endpoints regionais em um acelerador. O indicador de tráfego permite que você faça facilmente testes de desempenho ou testes de implantação azul/verde para novas versões em diferentes regiões da AWS, por exemplo.

A seguir, alguns exemplos para ilustrar como você pode usar indicadores de tráfego para alterar o fluxo de tráfego para grupos de endpoints.

Atualizar seu aplicativo por região

Se você quiser atualizar um aplicativo em uma região ou fazer manutenção, primeiro defina o indicador de tráfego como 0 para cortar o tráfego para a região. Quando você concluir o trabalho e estiver pronto para colocar a região de volta ao serviço, ajuste o indicador de tráfego em 100 para aumentar o tráfego.

Combinar tráfego entre duas regiões

Este exemplo mostra como o fluxo de tráfego funciona quando você altera os indicadores de tráfego de dois grupos de endpoints regionais ao mesmo tempo. Digamos que você tenha dois grupos de endpoints para seu acelerador, um para a região `us-west-2` e outro para a região `us-east-1`, e tenha definido os indicadores de tráfego em 50% para cada grupo de endpoints.

Agora, digamos que você tenha 100 solicitações chegando ao seu acelerador, sendo 50 da Costa Leste dos Estados Unidos e 50 da Costa Oeste. O acelerador direciona o tráfego da seguinte forma:

- As primeiras 25 solicitações em cada costa (50 solicitações no total) são atendidas por seu grupo de endpoints mais próximo. Ou seja, 25 solicitações são direcionadas para o grupo de endpoints em `us-west-2` e 25 são direcionadas para o grupo de endpoints em `us-east-1`.
- As próximas 50 solicitações são direcionadas para as regiões opostas. Ou seja, as próximas 25 solicitações da Costa Leste são atendidas por `us-west-2`, e as próximas 25 solicitações da Costa Oeste são atendidas por `us-east-1`.

O resultado nesse cenário é que os dois grupos de endpoints atendem à mesma quantidade de tráfego. No entanto, cada um recebe uma combinação de tráfego das duas regiões.

Arquiteturas de compartilhamento de carga de várias regiões

Você também pode configurar o indicador de tráfego e os pesos do endpoint para implementar cenários complexos e configurar o compartilhamento de carga entre os endpoints do aplicativo. Com esses atributos do Global Accelerator, você pode implantar e executar aplicativos em arquiteturas multirregionais, incluindo configurações ativa-ativa e ativas em espera. Para obter mais informações e exemplos detalhados, consulte a seguinte postagem no blog: Implantação de aplicativos multirregionais na AWS usando o AWS Global Accelerator

Substituir portas do receptor para portas restritas ou colisões de conexão

Por padrão, um acelerador roteia o tráfego de usuários para endpoints em regiões da AWS usando os intervalos de protocolo e portas que você especifica ao criar um receptor. Por exemplo, se você definir um receptor que aceita tráfego TCP nas portas 80 e 443, o acelerador roteia o tráfego para essas portas em um endpoint.

No entanto, ao adicionar ou atualizar um grupo de endpoints, você pode substituir a porta do receptor usada para rotear o tráfego para endpoints. Por exemplo, você pode criar uma substituição de porta na qual o listener recebe tráfego de usuário nas portas 80 e 443, mas seu acelerador roteia esse tráfego para as portas 1080 e 1443, respectivamente, nos endpoints.

Um benefício de usar substituições de porta pode ser ajudar a evitar colisões de conexão, que podem causar problemas intermitentes de conectividade no Global Accelerator, resultando em atrasos no tempo de conexão TCP, em determinados cenários. Essas colisões podem ocorrer quando usuários (com o mesmo IP de origem e porta de origem) acessam recursos no Global Accelerator. Você pode evitar as colisões e, assim, evitar os atrasos, configurando as substituições de portas em seus aceleradores. Para ter mais informações, consulte Como evitar colisões de conexão que resultam em atrasos no tempo de conexão TCP.

A substituição de uma porta também pode ajudar a evitar problemas de recepção em portas restritas. É mais seguro executar aplicativos que não exijam privilégios de superusuário (raiz) em seus endpoints. No entanto, no Linux e em outros sistemas semelhantes ao UNIX, você deve ter privilégios de superusuário para receber em portas restritas (portas TCP ou UDP abaixo de 1024). Ao mapear uma porta restrita em um receptor para uma porta não restrita em um endpoint, você evita esse problema. Você pode aceitar tráfego em portas restritas enquanto executa aplicativos sem acesso raiz em seus endpoints por trás do Global Accelerator. Por exemplo, você pode substituir a porta 443 de um receptor por uma porta 8443 de um endpoint.

Para cada substituição de porta, você especifica uma porta de receptor que aceita tráfego de usuários e a porta de endpoint para a qual o Global Accelerator roteará esse tráfego. Para ter mais informações, consulte Adicionar um grupo de endpoints padrão.

Ao criar uma substituição de porta, lembre-se do seguinte:

- As portas do endpoint não podem se sobrepor aos intervalos de portas do receptor. As portas de endpoint que você especifica em uma substituição de porta não podem ser incluídas em nenhum dos intervalos de portas do receptor que você configurou para o acelerador. Por exemplo, digamos que você tenha dois receptores para um acelerador e tenha definido os intervalos de portas para esses receptores como 100 a 199 e 200 a 299, respectivamente. Ao criar uma substituição de porta, você não pode definir uma da porta 100 do receptor até a porta 210 do endpoint, por exemplo, porque a porta do endpoint (210) está incluída em um intervalo de portas do receptor que você definiu (200 a 299).
- Sem portas de endpoint duplicadas. Se uma substituição de porta em um acelerador especificar uma porta de endpoint, você não poderá especificar a mesma porta de endpoint com a substituição de porta de uma porta de receptor diferente. Por exemplo, você não pode especificar uma substituição de porta da porta 80 do receptor para a porta 90 do endpoint junto com uma substituição da porta 81 do receptor para a porta 90 do endpoint.
- A verificação de integridade continua usando a porta original. Se você especificar uma substituição de porta para uma porta configurada como porta de verificação de integridade, a verificação de integridade ainda usará a porta original, não a porta de substituição. Por exemplo, digamos que você especifique verificações de integridade na porta 80 do receptor e também especifique uma substituição de porta da porta 80 do receptor para a porta 480 do endpoint. As verificações de integridade continuam usando a porta 80 do endpoint. No entanto, o tráfego do usuário que chega pela porta 80 vai para a porta 480 no endpoint.

  Esse comportamento mantém a consistência entre o Network Load Balancer, o Application Load Balancer, a instância do EC2 e os endpoints de endereço IP elástico. Como os Network Load Balancers e os Application Load Balancers não mapeiam portas de verificação de integridade para portas de endpoint diferentes quando você especifica uma substituição de porta no Global Accelerator, seria inconsistente que o Global Accelerator mapeasse portas de verificação de integridade para portas de endpoint diferentes para endpoints de instância do EC2 e de endereço IP elástico.
- As configurações do grupo de segurança devem permitir o acesso à porta. Verifique se seus grupos de segurança permitem que o tráfego chegue às portas de endpoint que você designou nas substituições de portas. Por exemplo, se você substituir a porta 443 do receptor pela porta

1433 do endpoint, verifique que todas as restrições de porta definidas no seu grupo de segurança para esse endpoint do Application Load Balancer ou do Amazon EC2 permitem tráfego de entrada na porta 1433.

Garantir acesso à verificação de integridade do seu acelerador

Cada receptor de um acelerador padrão roteia solicitações somente para endpoints ativos e íntegros. Quando você adiciona um endpoint, ele deverá ser aprovado por uma verificação de integridade para ser considerado íntegro. O AWS Global Accelerator também envia regularmente solicitações de verificação de integridade para todos os endpoints em aceleradores padrão, para testar seu status. O Global Accelerator executa automaticamente essas verificações de integridade regulares. Após a conclusão de cada verificação de integridade, o receptor fechará a conexão que foi estabelecida para a verificação de integridade.

Observe que, se não houver nenhum endpoint íntegro para o qual rotear o tráfego, o Global Accelerator roteia as solicitações de entrada do cliente para todos os endpoints no grupo de endpoints. Para ter mais informações, consulte Como o failover funciona para endpoints não íntegros.

Os detalhes sobre como as verificações de integridade funcionam e as orientações sobre o uso das verificações de integridade dependem do tipo de recurso do endpoint. Este tópico fornece informações sobre como trabalhar com verificações de integridade para diferentes tipos de endpoints, incluindo etapas para atualizar as opções de verificação de integridade no Global Accelerator (aplica-se a endpoints de instância do EC2 ou endereço IP elástico).

Garantir acesso às verificações de integridade do seu acelerador

Para garantir que o acesso às verificações de integridade seja concluído com êxito para endpoints de instância do EC2 ou endereço IP elástico, verifique se suas regras de roteador e firewall permitem tráfego de entrada dos endereços IP associados aos verificadores de integridade do Amazon Route 53. Para ver a lista de intervalos de endereços IP associados aos verificadores de integridade do Route 53, consulte Intervalos de endereços IP dos servidores do Route 53 no Guia do desenvolvedor do Amazon Route 53.

As verificações de integridade do Global Accelerator funcionam recebendo tráfego para as verificações de integridade do Route 53, que é encaminhado para a porta de verificação de integridade configurada para o grupo de endpoints. Normalmente, as portas configuradas para verificações de integridade correspondem à configuração do receptor. Se, em vez disso, você

configurar uma porta diferente para verificações de integridade, revise a configuração do grupo de segurança para garantir que você não permita tráfego público na porta.

Por exemplo, se seu receptor estiver configurado na porta 80, sua porta de verificação de integridade também será 80. Se você optar por configurar portas de integridade em outra porta, por exemplo, a porta 83, configure seus grupos de segurança para permitir tráfego na porta 83 somente de endereços IP que estejam no intervalo de endereços IP para verificações de integridade do Route 53.

Orientação de verificação de integridade para diferentes tipos de endpoints

Analise as informações nesta seção para obter orientações sobre as verificações de integridade que você especifica para cada tipo de endpoint do seu acelerador.

Além disso, certifique-se de que as verificações de integridade escolhidas para endpoints com workloads HTTP representem a integridade geral do seu aplicativo e siga as orientações para garantir o acesso às verificações de integridade descritas na seção anterior, Garantir a segurança e o acesso às verificações de integridade.

As orientações a seguir se aplicam a cada tipo de endpoint especificado:

- Para endpoints do Network Load Balancer ou do Application Load Balancer, esteja ciente do seguinte:
  - As opções de verificação de integridade escolhidas no Global Accelerator não afetam os Network Load Balancers ou os Application Load Balancers que você adicionou como endpoints. Ou seja, as opções de verificação de integridade que você especifica no Global Accelerator são usadas para verificações de integridade de endereços IP elásticos e Amazon EC2, mas não para verificações de integridade em endpoints de balanceadores de carga.

    Para endpoints do balanceador de carga, configure as verificações de integridade usando as opções de configuração do Elastic Load Balancing. Para obter mais informações, consulte Verificações de integridade para seus grupos de destino.
  - O Global Accelerator considera um Network Load Balancer ou um Application Load Balancer íntegro se houver pelo menos uma zona de disponibilidade íntegra. Uma zona de disponibilidade está íntegra se todos os grupos-alvo do balanceador de carga nessa zona de disponibilidade estiverem íntegros. Para obter mais informações, consulte Verificações de integridade para seus grupos de destino.
- Para endpoints de instância do EC2 ou endereço IP elástico, esteja ciente do seguinte:

- Ao adicionar endpoints de instância do EC2 ou endereço IP elástico a um receptor configurado com TCP, você pode especificar a porta a ser usada para verificações de integridade. Por padrão, se você não especificar uma porta para verificações de integridade, o Global Accelerator usa a porta de receptor que você especificou para seu acelerador.
- Quando você adiciona esses tipos de endpoint com um receptor UDP, o Global Accelerator usa a porta do receptor e o protocolo TCP para verificações de integridade, portanto, você deve ter um servidor TCP em seu endpoint.

  Verifique se a porta que você configurou para o servidor TCP em cada endpoint é a mesma que você especificou para a verificação de integridade no Global Accelerator. Se os números das portas não forem os mesmos ou se você não tiver configurado um servidor TCP para o endpoint, o Global Accelerator marcará o endpoint como não íntegro, independentemente da integridade do endpoint.
- Siga as orientações de segurança e acesso ao configurar portas para verificações de integridade para sua instância do EC2 ou endpoints de endereço IP elástico.

Definir opções de verificação de integridade

Para definir as opções de verificação de integridade do seu acelerador, especifique uma ou mais das opções a seguir ao criar um acelerador ou ao editar um grupo de endpoints.

Você pode adicionar as seguintes opções de verificação de integridade para um grupo de endpoints.

Porta de verificação de integridade

A porta a ser usada quando o Global Accelerator executa verificações de integridade em endpoints que fazem parte desse grupo de endpoints.

Observe que você não pode definir uma substituição de porta para portas de verificação de integridade.

Health check protocol (Protocolo da verificação de integridade)

O protocolo a ser usado quando o Global Accelerator executa verificações de integridade em endpoints que fazem parte desse grupo de endpoints.

Intervalo de verificação de integridade

O intervalo, em segundos, entre cada verificação de integridade de um endpoint.

Contagem de limites

O número de verificações de integridade consecutivas necessárias antes de considerar um destino não íntegro como íntegro, ou um íntegro como não íntegro.

Endpoints para aceleradores padrão no AWS Global Accelerator

Endpoints para aceleradores padrão do AWS Global Accelerator podem ser Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços IP elásticos. No AWS Global Accelerator, endereços IP estáticos servem como um ponto único de contato para clientes e, com um acelerador padrão, o Global Accelerator distribui o tráfego de entrada nos endpoints íntegros. O Global Accelerator direciona o tráfego para os endpoints usando a porta (ou intervalo de portas) que você especifica para o receptor ao qual o grupo de endpoints do endpoint pertence.

Cada grupo de endpoints pode ter vários endpoints. Você pode adicionar cada endpoint a vários grupos de endpoints, mas os grupos de endpoints devem estar associados a diferentes receptores. Um recurso deve ser válido e estar ativo quando adicionado como um endpoint.

> **Important**
>
> Os aceleradores que você configura como pilha dupla (ou seja, aceleradores aos quais você deseja oferecer compatibilidade com IPv4 e IPv6) exigem que você adicione somente endpoints que também sejam compatíveis com pilhas duplas. Network Load Balancers, Application Load Balancers e instâncias do Amazon EC2 podem ser adicionados como endpoints de pilha dupla.

O Global Accelerator monitora continuamente a integridade de todos os endpoints incluídos em um grupo de endpoints padrão. Ele roteia o tráfego somente para os endpoints ativos que estão íntegros. Se o Global Accelerator não tiver nenhum endpoint íntegro para rotear o tráfego, ele roteará o tráfego para todos os endpoints na Região da AWS.

Conteúdo

- Remover um endpoint padrão
- Como os pesos dos endpoints funcionam para gerenciar o volume de tráfego
- Como o failover funciona para endpoints não íntegros
- Como evitar colisões de conexão que resultam em atrasos no tempo de conexão TCP

Requisitos para recursos que você adiciona como endpoints do acelerador

Esteja ciente dos seguintes requisitos e limitações para diferentes tipos de recursos que você pode adicionar como endpoints para aceleradores padrão no AWS Global Accelerator.

Se você planeja habilitar a preservação do endereço IP do cliente para endpoints, há requisitos adicionais a serem considerados. Para ter mais informações, consulte Endpoints de transição com preservação do endereço IP do cliente.

Observação: antes de encerrar ou excluir um recurso que você adicionou como um endpoint por trás de um acelerador, recomendamos que você remova o endpoint dos grupos de endpoints do Global Accelerator.

Endpoints do Application Load Balancer

- Um endpoint do Application Load Balancer pode ser voltado para a internet ou interno.
- Os Application Load Balancers de pilha dupla podem ser adicionados como endpoints.
- O Global Accelerator só é compatível com Application Load Balancers executados dentro de uma Região da AWS. O Global Accelerator não é compatível com um Application Load Balancer executado como um endpoint em uma zona local.

Endpoints do Network Load Balancer

- Um endpoint do Network Load Balancer pode ser voltado para a internet ou interno.
- Os Network Load Balancers de pilha dupla podem ser adicionados como endpoints, mas há algumas restrições:
  - Para aceleradores de pilha dupla, quando você adiciona um Network Load Balancer de pilha dupla, o Network Load Balancer não pode ter um grupo-alvo com um tipo de destino de `ip` ou um tipo de destino de `instance` e um tipo de endereço IP de `ipv6`.
  - Para aceleradores IPv4, ao adicionar um Network Load Balancer de pilha dupla, você não pode habilitar a preservação do endereço IP do cliente para o endpoint no Global Accelerator.

- O Global Accelerator só é compatível com Network Load Balancers executados dentro de uma Região da AWS. O Global Accelerator não é compatível com um Network Load Balancer executado como um endpoint em uma zona local.
- Para endpoints do Network Load Balancer, recomendamos que você desabilite o tráfego entre zonas para os balanceadores de carga para evitar colisões de conexão, o que pode resultar em maior tempo de conexão TCP. Para ter mais informações, consulte Como evitar colisões de conexão que resultam em atrasos no tempo de conexão TCP.

Endpoints de instância do Amazon EC2

- Um endpoint de instância do EC2 não pode ser um dos seguintes tipos: C1, CC1, CC2, CG1, CG2, CR1, CS1, G1, G2, HI1, HS1, M1, M2, M3 ou T1.
- As instâncias do EC2 são compatíveis como endpoints em Regiões da AWS específicas. Para ter mais informações, consulte Disponibilidade da Região da AWS para o AWS Global Accelerator.

  O Global Accelerator só é compatível com instâncias do EC2 dentro de uma Região da AWS. O Global Accelerator não é compatível com o roteamento para um endereço IP elástico como um endpoint em uma zona local.
- Recomendamos que você remova uma instância do EC2 dos grupos de endpoints do Global Accelerator antes de encerrar a instância. Se você encerrar uma instância do EC2 antes de removê-la de um grupo de endpoints no Global Accelerator e depois criar outra instância na mesma VPC com o mesmo endereço IP privado e as verificações de integridade passarem, o Global Accelerator roteará o tráfego para o novo endpoint.
- Instâncias do EC2 de pilha dupla podem ser adicionadas como endpoints. No entanto, as instâncias devem ter uma interface de rede elástica (ENI) IPv6 primária anexada a elas. Para obter mais informações, consulte Trabalhar com interfaces de rede no Guia do usuário do Amazon Elastic Compute Cloud.

Endereços IP elásticos

- Endereços IP elásticos de pilha dupla não podem ser adicionados como endpoints.

Para todos os endpoints, ao configurar recursos como endpoints por trás do Global Accelerator, recomendamos que você também não envie tráfego diretamente para os mesmos endpoints pela internet. O envio de tráfego direto pode causar problemas de colisão na conexão.

Além disso, esteja ciente de que os recursos que você adiciona como endpoints para um acelerador e para o próprio acelerador devem pertencer à mesma conta, a menos que você configure a

compatibilidade entre contas. No entanto, as instâncias de destino por trás de um endpoint do balanceador de carga podem pertencer a contas diferentes. Nesse cenário, as contas que possuem as instâncias de destino devem ter permissão para acessar uma sub-rede de propriedade da conta que possui o balanceador de carga e o acelerador. Para ter mais informações, consulte Configurar o acesso entre contas no Global Accelerator.

Adicionar um endpoint padrão

Você adiciona endpoints aos grupos de endpoints para que o tráfego possa ser direcionado para seus recursos. Você pode editar um endpoint padrão para alterar o peso do endpoint. Você também pode remover um endpoint do seu acelerador removendo-o de um grupo de endpoints. A remoção de um endpoint não afeta o endpoint em si, mas o Global Accelerator não pode mais direcionar o tráfego para esse recurso.

Primeiro, você deve criar um recurso e depois adicioná-lo como um endpoint no Global Accelerator. Um recurso deve ser válido e estar ativo quando adicionado como um endpoint. Para obter informações detalhadas sobre os tipos e configurações de endpoints com os que o Global Accelerator é compatível, consulte Requisitos para recursos que você adiciona como endpoints do acelerador.

Um dos motivos pelos quais você pode adicionar ou remover endpoints de grupos de endpoints é o uso. Por exemplo, se a demanda de seu aplicativo aumentar, você poderá criar mais recursos. Em seguida, você pode adicionar mais endpoints a um ou mais grupos de endpoints para lidar com o aumento do tráfego. O Global Accelerator inicia as solicitações de roteamento a um endpoint assim que você o adiciona e o endpoint passa nas verificações de integridade iniciais.

Você pode gerenciar o tráfego para endpoints ajustando os pesos em um endpoint para enviar proporcionalmente mais ou menos tráfego para o endpoint. Para ter mais informações, consulte Como os pesos dos endpoints funcionam para gerenciar o volume de tráfego.

Observação: se você estiver pensando em adicionar um endpoint com preservação do endereço IP do cliente, primeiro revise as informações em Preservar os endereços IP do cliente no AWS Global Accelerator.

Esta seção explica como adicionar endpoints no console do AWS Global Accelerator. Se você quiser usar operações de API com o AWS Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para adicionar um endpoint padrão

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na página Aceleradores, escolha um acelerador.
3. Na seção Receptores, em ID do receptor, escolha o ID de um receptor.
4. Na seção Grupos de endpoints, em ID do grupo de endpoints, escolha o ID do grupo de endpoints ao qual você deseja adicionar o endpoint.
5. Selecione a opção Editar.
6. Na seção Endpoints, escolha Adicionar endpoint.
7. Na página Adicionar endpoints, escolha um recurso na lista suspensa.

   Se você não tiver recursos da AWS, não haverá itens na lista. Para continuar, crie recursos da AWS como balanceadores de carga, instâncias do Amazon EC2 ou endereços IP elásticos. Em seguida, volte às etapas aqui e escolha um recurso da lista.

   > **Note**
   >
   > Se você tiver um acelerador de pilha dupla, deverá adicionar um endpoint de pilha dupla. Network Load Balancers, Application Load Balancers e instâncias do Amazon EC2 podem ser adicionados como endpoints de pilha dupla.

8. Opcionalmente, em Peso, insira um número de 0 a 255 para definir um peso para rotear o tráfego para esse endpoint. Ao adicionar pesos a endpoints, você configura o Global Accelerator para encaminhar o tráfego com base nas proporções especificadas. Por padrão, todos os endpoints têm peso de 128. Para ter mais informações, consulte Como os pesos dos endpoints funcionam para gerenciar o volume de tráfego.
9. Opcionalmente, habilite a preservação do endereço IP do cliente para o endpoint. Em Preservar endereço IP do cliente, selecione Preservar endereço. Para ter mais informações, consulte Preservar os endereços IP do cliente no AWS Global Accelerator.

   > **Note**
   >
   > Antes de adicionar e começar a rotear o tráfego para endpoints que preservam o endereço IP do cliente, certifique-se de que todas as configurações de segurança

necessárias, por exemplo, grupos de segurança, estejam atualizadas para incluir o endereço IP do cliente do usuário nas listas de permissões.

10. Escolha Add endpoint.

Editar um endpoint padrão

Esta seção explica como editar um endpoint no console do AWS Global Accelerator. Se você quiser usar operações de API com o AWS Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para editar um endpoint padrão

Você pode editar uma configuração de endpoint para alterar o peso. Para ter mais informações, consulte Como os pesos dos endpoints funcionam para gerenciar o volume de tráfego.

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na página Aceleradores, escolha um acelerador.
3. Na seção Receptores, em ID do receptor, escolha o ID de um receptor.
4. Na seção Grupos de endpoints, em ID do grupo de endpoints, escolha o ID do grupo de endpoints.
5. Escolha Editar endpoint.
6. Na página Editar endpoint, faça atualizações e escolha Salvar.

Remover um endpoint padrão

Esta seção explica como remover um endpoint no console do AWS Global Accelerator. Se você quiser usar operações de API com o AWS Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Você pode remover endpoints de seus grupos de endpoints, por exemplo, se precisar fazer a manutenção de seus endpoints. A remoção de um endpoint o retira do grupo de endpoints, mas não afeta o endpoint de outra forma. O Global Accelerator para de direcionar o tráfego para um endpoint assim que você o remove de um grupo de endpoints. O endpoint entra em um estado em que espera que todas as solicitações atuais sejam concluídas para que não haja interrupção no tráfego do

cliente que está em andamento. Você pode adicionar o endpoint novamente ao grupo de endpoints quando estiver pronto para que ele continue recebendo solicitações.

Observação: antes de encerrar ou excluir um recurso que você adicionou como um endpoint por trás de um acelerador, recomendamos que você remova o endpoint dos grupos de endpoints do Global Accelerator.

Para remover um endpoint

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na página Aceleradores, escolha um acelerador.
3. Na seção Receptores, em ID do receptor, escolha o ID de um receptor.
4. Na seção Grupos de endpoints, em ID do grupo de endpoints, escolha o ID do grupo de endpoints.
5. Escolha Remover endpoint.
6. Na caixa de diálogo de confirmação, escolha Remover.

Como os pesos dos endpoints funcionam para gerenciar o volume de tráfego

O roteamento ponderado permite que você escolha quanto tráfego é roteado para um recurso específico (endpoint) em um grupo de endpoints. Isso pode ser útil de várias maneiras, inclusive para balanceamento de carga e para testar novas versões do seu aplicativo.

Um peso é um valor que você pode definir para determinar a proporção do tráfego que o Global Accelerator direciona para um endpoint em um acelerador padrão. Os endpoints podem ser Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços IP elásticos. O Global Accelerator calcula a soma dos pesos dos endpoints em um grupo de endpoints e, em seguida, direciona o tráfego para os endpoints com base na proporção do peso de cada endpoint em relação ao total. Por padrão, o peso de um endpoint é definido como 128, que é metade do valor máximo de 255.

Como funcionam os pesos dos endpoints

Para usar pesos, você atribui a cada endpoint em um grupo de endpoints um peso relativo que corresponde à quantidade de tráfego que deseja enviar a ele. Por padrão, o peso de um endpoint é

128, ou seja, metade do valor máximo de um peso, 255. O Global Accelerator envia o tráfego a um endpoint com base no peso que você atribui a ele como uma proporção do peso total de todos os endpoints do grupo:

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

Por exemplo, se você deseja enviar uma pequena parte do seu tráfego para um endpoint e o restante para outro endpoint, pode especificar pesos 1 e 255 respectivamente. O endpoint com peso 1 recebe 1/256 do tráfego (1/1+255) e o outro endpoint recebe 255/256 (255/1+255). Você pode alterar gradualmente o equilíbrio do volume de tráfego para cada endpoint alterando os pesos. Se você deseja que o Global Accelerator interrompa o envio de tráfego para um endpoint, pode alterar o peso desse recurso para 0.

Esteja ciente de que, mesmo quando você define pesos de endpoints em seu acelerador, em cenários específicos e limitados, o Global Accelerator substitui esses pesos para ajudar a garantir a disponibilidade. Ou seja, quando o Global Accelerator está balanceando a carga do tráfego entre endpoints em um grupo de endpoints, ele deve, em determinadas circunstâncias, escolher entre preservar a disponibilidade do tráfego do cliente e respeitar os pesos dos endpoints. Por exemplo, com aceleradores em que o endereço IP do cliente é preservado, o Global Accelerator pode precisar substituir uma configuração de peso do endpoint para ajudar a evitar colisões de conexão.

Como o failover funciona para endpoints não íntegros

Se não houver endpoints íntegros em um grupo de endpoints com peso maior que zero, o Global Accelerator tentará passar para um endpoint íntegro com peso maior que zero em outro grupo de endpoints. Observe que, para esse failover, o Global Accelerator ignora a configuração de indicador de tráfego. Portanto, se, por exemplo, um grupo de endpoints tiver um indicador de tráfego definido como zero, o Global Accelerator ainda incluirá esse grupo de endpoints na tentativa de failover.

Se o Global Accelerator não encontrar um endpoint íntegro com peso maior que zero depois de testar os três grupos de endpoints mais próximos (ou seja, Regiões da AWS), ele roteará o tráfego para um endpoint aleatório no grupo de endpoints mais próximo do cliente. Ou seja, ele apresenta falha na abertura.

Observe o seguinte:

- O grupo de endpoints escolhido para failover pode ser aquele que tenha um indicador de tráfego definido como zero.

- O grupo de endpoints mais próximo pode não ser o grupo de endpoints original. Isso ocorre porque o Global Accelerator considera as configurações do indicador de tráfego da conta ao escolher o grupo de endpoints original.

Por exemplo, digamos que sua configuração tenha dois endpoints, um íntegro e outro não íntegro, e você tenha definido o peso de cada um deles como maior que zero. Nesse caso, o Global Accelerator roteia o tráfego para o endpoint íntegro. Agora digamos que você define o peso do único endpoint íntegro como zero. Em seguida, o Global Accelerator experimenta três grupos adicionais de endpoints para encontrar um endpoint íntegro com peso maior que zero. Se não encontrar um, o Global Accelerator roteia o tráfego a um endpoint aleatório no grupo de endpoints mais próximo do cliente.

Quando ocorre a recuperação, ou seja, as regiões estão íntegras novamente, o Global Accelerator retorna ao comportamento normal de roteamento. Isso significa que, normalmente, o roteamento retornará a endpoints íntegros com indicadores de tráfego que não são definidos como zero em cerca de 30 segundos. No entanto, observe que as conexões ativas estabelecidas não são movidas. Elas continuam roteando para a região de peso zero até que a conexão seja redefinida pelo cliente ou pelo servidor, ou até que o cliente faça uma nova conexão.

Como evitar colisões de conexão que resultam em atrasos no tempo de conexão TCP

Problemas intermitentes de conectividade podem ser causados por colisões de conexão no AWS Global Accelerator. Isso pode ocorrer quando usuários (com o mesmo IP de origem e porta de origem) acessam recursos no Global Accelerator em determinados cenários. As colisões podem resultar em atrasos no tempo de conexão TCP para o tráfego que passa por seus aceleradores.

Você pode evitar esses atrasos configurando seus aceleradores com substituições de portas, um atributo do Global Accelerator que permite rotear o tráfego de entrada para portas de destino diferentes nos endpoints do acelerador. Siga as orientações nesta seção para saber como usar substituições de porta para evitar colisões de conexão e evitar possíveis atrasos no tempo de conexão TCP.

Cenários que podem causar colisões de conexão

Há três cenários no Global Accelerator que podem levar a colisões de conexão e, portanto, a atrasos no tempo de conexão TCP:

- Você configura o mesmo recurso como um endpoint com vários aceleradores.
- Você configura recursos como endpoints por trás do Global Accelerator e também envia tráfego diretamente pela internet de seus usuários finais para os mesmos recursos.
- Você configura os endpoints do Network Load Balancer para tráfego entre zonas.

Para endpoints do Network Load Balancer, recomendamos que você desabilite o tráfego entre zonas para os balanceadores de carga para evitar colisões de conexão. Para obter mais informações, consulte Atrasos de conexão TCP no Guia do usuário para Network Load Balancers.

Para os outros cenários, recomendamos que você use o atributo de substituição de porta com o grupo de endpoints para evitar colisões. Ao usar substituições de porta, você pode mapear portas de receptor do Global Accelerator para números de porta de destino diferentes em um recurso de endpoint. As portas do receptor usam como padrão os mesmos números de porta nos recursos do endpoint. Ao usar substituições de porta, os aceleradores podem rotear o tráfego dos mesmos usuários (com o IP de origem e a porta de origem) para o mesmo endpoint, mas usar números de porta de destino diferentes, o que evita colisões.

A próxima seção fornece exemplos específicos para cada um dos cenários de como você pode configurar substituições de portas para evitar colisões de conexão. Para obter mais informações sobre como configurar substituições de portas, consulte Substituir portas do receptor para portas restritas ou colisões de conexão.

Como evitar colisões de conexão usando substituições de portas

Por padrão, um acelerador roteia o tráfego do usuário para os endpoints em Regiões da AWS usando o mesmo protocolo e os mesmos intervalos de portas de destino que você especifica ao criar um receptor. No entanto, você pode optar por substituir o mapeamento do número da porta para a porta do receptor. Ou seja, você pode mapear um número de porta do receptor para rotear o tráfego para um número de porta de destino diferente em um endpoint.

Por exemplo, se você definir um receptor que aceite tráfego TCP nas portas 80 e 443, por padrão, o acelerador roteará o tráfego para essas mesmas portas, 80 e 443, nos endpoints. No entanto, se você usar o atributo de substituição de portas, o acelerador pode rotear o tráfego que entra nessas portas para portas diferentes em endpoints, como 8080 e 8443.

Ao criar mapeamentos de portas diferentes para receptores em dois (ou mais) aceleradores que têm os mesmos recursos configurados por trás deles, você pode usar números de porta de destino separados para cada acelerador e evitar colisões.

Por exemplo, digamos que você tenha o Acelerador-A e o Acelerador-B, e cada um tem um receptor configurado para TCP e a porta 443. Você pode configurar uma substituição de porta para que o receptor do Acelerador-A mapeie a porta 443 para 8443, e o receptor do Acelerador-B mapeie a porta 443 para 9443. Agora você configura um endpoint do Application Load Balancer, o ALB-1234, por exemplo, para receber nas portas 8443 e 9443. Então, o tráfego que entra na porta 443 (para os receptores dos dois aceleradores) do mesmo endereço IP do usuário chegará ao ALB-1234, sem colisões de conexão ou atrasos no tempo de conexão TCP.

Você pode ver os caminhos de tráfego desse exemplo ilustrados a seguir:

```
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)
```

Você pode usar uma substituição de porta de forma semelhante para evitar colisões de conexão para recursos que são acessados pelo tráfego direto do usuário e por meio de um acelerador, substituindo o mapeamento padrão para o número da porta do receptor do acelerador. Para evitar colisões nesse cenário, faça o seguinte:

1. Determine a porta na qual você deseja que o recurso receba seu tráfego direto.
2. Configure o receptor do seu acelerador para substituir a porta padrão e configure o receptor do seu recurso para receber o tráfego do acelerador nessa porta.

Por exemplo, você pode configurar uma substituição de porta para o receptor do seu acelerador mapear a porta 443 para a porta 8443. Agora, você pode configurar um endpoint do Application Load Balancer, por exemplo, para receber o tráfego do acelerador na porta 8443 e o tráfego direto na porta 443. Com essa configuração, você evita colisões de conexão no Application Load Balancer para o tráfego proveniente do mesmo endereço IP do usuário.

Como trabalhar com aceleradores de roteamento personalizados no AWS Global Accelerator

Este capítulo inclui informações sobre como um acelerador de roteamento personalizado no AWS Global Accelerator funciona e como configurar aceleradores, receptores, grupos de endpoints e endpoints de sub-rede VPC para um acelerador de roteamento personalizado.

Um acelerador de roteamento personalizado permite que você use a lógica do aplicativo para mapear diretamente um ou mais usuários para uma instância específica do Amazon EC2 entre vários destinos, ao mesmo tempo em que obtém as melhorias de desempenho ao rotear seu tráfego por meio do Global Accelerator. Isso é útil quando você tem um aplicativo que exige que um grupo de usuários interaja entre si na mesma sessão em execução em uma instância e porta do EC2 específicas, como aplicativos de jogos ou sessões de voz sobre IP (VoIP).

Os endpoints para aceleradores de roteamento personalizados devem ser sub-redes da Amazon VPC (VPC), e um acelerador de roteamento personalizado só pode rotear tráfego para instâncias do Amazon EC2 nessas sub-redes. Ao criar um acelerador de roteamento personalizado, você pode incluir milhares de instâncias do Amazon EC2 em execução em uma ou várias sub-redes VPC. Para saber mais, consulte Como os aceleradores de roteamento personalizados funcionam no Global Accelerator.

> **Note**
>
> Se você quiser que o Global Accelerator escolha automaticamente o endpoint íntegro mais próximo de seus clientes, crie um acelerador padrão. Para ter mais informações, consulte Como trabalhar com aceleradores padrão no AWS Global Accelerator.

Para configurar o acelerador de roteamento personalizado, você deve fazer o seguinte:

1. Revise as diretrizes e os requisitos para criar um acelerador de roteamento personalizado. Consulte Diretrizes e restrições para aceleradores de roteamento personalizados.
2. Crie uma sub-rede VPC. Você pode adicionar instâncias do EC2 à sub-rede a qualquer momento depois de adicionar a sub-rede ao Global Accelerator.
3. Crie um acelerador no Global Accelerator. Selecione a opção de um acelerador de roteamento personalizado.

4. Adicione um receptor no qual você especifica um intervalo de portas para o Global Accelerator receber. Certifique-se de incluir uma grande variedade com portas suficientes para que o Global Accelerator mapeie todos os destinos que você espera ter. Essas portas são distintas das portas de destino, que você especifica na próxima etapa. Para obter mais informações sobre os requisitos de porta de receptor, consulte Diretrizes e restrições para aceleradores de roteamento personalizados.
5. Adicione um ou mais grupos de endpoints para regiões da AWS nas quais você tem sub-redes VPC. Você especifica o seguinte para cada grupo de endpoints:
   - Um intervalo de portas de endpoint, que representa as portas em suas instâncias do EC2 de destino que poderão receber tráfego.
   - O protocolo para cada intervalo de portas de destino: UDP, TCP ou UDP e TCP.
6. Para a sub-rede do endpoint, selecione um ID de sub-rede. Você pode adicionar várias sub-redes em cada grupo de endpoints e as sub-redes podem ter tamanhos diferentes (até /17).

As seções a seguir explicam como os aceleradores de roteamento personalizados funcionam e fornecem etapas para criar e trabalhar com aceleradores de roteamento personalizados e seus componentes, incluindo receptores, grupos de endpoints e endpoints de sub-rede VPC.

Tópicos

Como os aceleradores de roteamento personalizados funcionam no Global Accelerator

Ao usar um acelerador de roteamento personalizado no AWS Global Accelerator, você pode usar a lógica do aplicativo para mapear diretamente um ou mais usuários para um destino específico entre

muitos destinos e, ao mesmo tempo, obter os benefícios de desempenho do Global Accelerator. Um acelerador de roteamento personalizado mapeia os intervalos de portas do receptor para destinos de instância do EC2 nas sub-redes da Amazon VPC (VPC). Isso permite que o Global Accelerator roteie deterministicamente o tráfego para um endereço IP privado e destino de porta específicos do Amazon EC2 em sua sub-rede.

Por exemplo, você pode usar um acelerador de roteamento personalizado com um aplicativo de jogos on-line em tempo real no qual você atribui vários jogadores a uma única sessão em um servidor de jogos do Amazon EC2 com base em fatores que você escolhe, como localização geográfica, habilidade do jogador e modo de jogo. Ou você pode ter um aplicativo de VoIP ou de mídia social que atribua vários usuários a um servidor de mídia específico para sessões de voz, vídeo e mensagens.

Seu aplicativo pode chamar uma API do Global Accelerator e receber um mapeamento estático completo das portas do Global Accelerator e dos endereços IP e portas de destino associados. Você pode salvar esse mapeamento estático e, em seguida, seu serviço de matchmaking o usa para rotear os usuários para instâncias do EC2 de destino específicas. Você não precisa fazer nenhuma modificação no software-cliente para começar a usar o Global Accelerator com seu aplicativo.

Para configurar um acelerador de roteamento personalizado, você seleciona um endpoint de sub-rede VPC. Em seguida, você define um intervalo de portas de destino para o qual as conexões de entrada serão mapeadas, para que seu software possa escutar no mesmo conjunto de portas em todas as instâncias. O Global Accelerator cria um mapeamento estático que permite que seu serviço de matchmaking traduza um endereço IP de destino e número de porta de uma sessão em um endereço IP externo e porta que você fornece aos usuários.

A pilha de rede do seu aplicativo pode operar em um único protocolo de transporte ou, em vez disso, você usa o UDP para entrega rápida e o TCP para entrega confiável. Você pode definir UDP, TCP ou UDP e TCP para cada intervalo de portas de destino, para oferecer o máximo de flexibilidade sem precisar duplicar sua configuração para cada protocolo.

> **Note**
>
> Por padrão, todos os destinos de sub-rede VPC em um acelerador de roteamento personalizado não têm permissão para receber tráfego. Isso deve ser seguro por padrão e também fornecer controle granular sobre quais destinos de instâncias do EC2 privadas em sua sub-rede podem receber tráfego. Você pode permitir ou negar tráfego para a sub-rede ou para combinações específicas de endereços IP e portas (sockets de destino). Para ter mais informações, consulte Adicionar um endpoint de sub-rede da VPC a um acelerador

de roteamento personalizado. Você também pode especificar destinos usando a API do Global Accelerator. Para obter mais informações, consulte AllowCustomRoutingTraffic e DenyCustomRoutingTraffic.

Exemplo de como o roteamento personalizado funciona no Global Accelerator

Como exemplo, digamos que você queira oferecer compatibilidade com 10 000 sessões em que grupos de usuários interajam, como sessões de jogos ou sessões de chamadas VoIP, em 1000 instâncias do Amazon EC2 por trás do Global Accelerator. Neste exemplo, especificaremos um intervalo de portas de receptor de 10001 a 20040 e um intervalo de portas de destino de 81 a 90. Digamos que temos as quatro sub-redes VPC em us-east-1: subnet-1, subnet-2, subnet-3 e subnet-4.

Em nosso exemplo de configuração, cada sub-rede VPC tem um tamanho de bloco de /24 para que possa ser compatível com 251 instâncias do Amazon EC2. (Cinco endereços estão reservados e não estão disponíveis em cada sub-rede, e esses endereços não estão mapeados). Cada servidor executado em cada instância do EC2 atende às 10 portas a seguir, que especificamos para as portas de destino em nosso grupo de endpoints: 81 a 90. Isso significa que temos 2510 portas (10 x 251) associadas a cada sub-rede. Cada porta pode ser associada a uma sessão.

Como especificamos 10 portas de destino em cada instância do EC2 em nossa sub-rede, o Global Accelerator as associa internamente a 10 portas de receptor que você pode usar para acessar instâncias do EC2. Para ilustrar isso de forma simples, diremos que há um bloco de portas de receptor que começa com o primeiro endereço IP da sub-rede do endpoint para o primeiro conjunto de 10 e, em seguida, passa para o próximo endereço IP do próximo conjunto de 10 portas de receptor.

> **Note**
>
> Na verdade, o mapeamento não é previsível dessa forma, mas estamos usando um mapeamento sequencial aqui para ajudar a mostrar como o mapeamento de portas funciona. Para determinar o mapeamento real dos intervalos de portas do receptor, use as seguintes operações de API: ListCustomRoutingPortMappings e ListCustomRoutingPortMappingsByDestination.

Em nosso exemplo, a primeira porta do receptor é 10001. Essa porta está associada ao primeiro endereço IP da sub-rede, 192.0.2.4, e à primeira porta EC2, 81. A próxima porta do receptor, 10002, está associada ao primeiro endereço IP da sub-rede, 192.0.2.4, e à segunda porta EC2, 82. A tabela a seguir ilustra como esse exemplo de mapeamento continua até o último endereço IP da primeira sub-rede VPC e, em seguida, até o primeiro endereço IP da segunda sub-rede VPC.

Porta de receptor do Global Accelerator	sub-rede VPC	Porta de instância do EC2
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

Porta de receptor do Global Accelerator	sub-rede VPC	Porta de instância do EC2
10017	192.0.2.5	87
10018	192.0.2.5	88
10019	192.0.2.5	89
10020	192.0.2.5	90
...	...	...
12501	192.0.2.244	81
12502	192.0.2.244	82
12503	192.0.2.244	83
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

Porta de receptor do Global Accelerator	sub-rede VPC	Porta de instância do EC2
12516	192.0.3.4	86
12517	192.0.3.4	87
12518	192.0.3.4	88
12519	192.0.3.4	89
12520	192.0.3.4	90

Diretrizes e restrições para aceleradores de roteamento personalizados

Ao criar e trabalhar com aceleradores de roteamento personalizados no AWS Global Accelerator, lembre-se das diretrizes e restrições a seguir.

Destinos de endpoints compatíveis

Os endpoints de sub-rede de sub-rede da nuvem pública virtual (VPC) em um acelerador de roteamento personalizado só podem incluir instâncias do EC2. Nenhum outro recurso, como balanceadores de carga, é compatível com aceleradores de roteamento personalizados. Os tipos de instâncias do EC2 compatíveis com o Global Accelerator estão listados em Endpoints para aceleradores padrão no AWS Global Accelerator.

Com aceleradores de roteamento personalizados, o Global Accelerator só pode rotear tráfego para endpoints de IP privadas em instâncias do Amazon EC2 em sub-redes da VPC. No entanto, os clientes de jogos que desejam usar o roteamento personalizado podem precisar se conectar a sessões com estado. Para fazer isso, os clientes executam seus servidores de jogos no Amazon Elastic Kubernetes Service (EKS), com sessões hospedadas em um contêiner específico executado dentro de um pod do Kubernetes.

Para usar o roteamento personalizado nesse cenário, você pode configurar um plug-in VPC-CNI para enviar tráfego para os pods do Kubernetes por meio de uma interface de rede elástica (ENI) que o Global Accelerator cria para cada sub-rede em que um endpoint está presente. Essa é uma forma de usar um acelerador de roteamento personalizado com o EKS. A mesma

configuração funciona para usar um acelerador de roteamento personalizado com o Amazon Elastic Container Service (ECS). Para saber mais, consulte as etapas detalhadas fornecidas na seguinte postagem do blog: Roteamento personalizado do AWS Global Accelerator com o Amazon Elastic Kubernetes Service.

Mapeamentos de porta

Quando você adiciona uma sub-rede da VPC, o Global Accelerator cria um mapeamento de portas estáticas dos intervalos de portas do receptor para os intervalos de portas compatíveis com a sub-rede. O mapeamento de portas para uma sub-rede específica nunca muda.

Você pode visualizar a lista de mapeamento de portas para um acelerador de roteamento personalizado de forma programática. Para ter mais informações, consulte `ListCustomRoutingPortMappings`.

Tamanho das sub-redes da VPC

As sub-redes da VPC que você adiciona a um acelerador de roteamento personalizado devem ter no mínimo /28 e no máximo /17.

Tipo de endereço IP

Os aceleradores de roteamento personalizados são compatíveis apenas com o tipo de endereço IP IPv4.

Intervalos de portas do receptor

Você deve especificar portas do receptor suficientes, especificando intervalos de portas do receptor, para acomodar o número de destinos incluídos nas sub-redes que você planeja adicionar ao seu acelerador de roteamento personalizado. O intervalo que você especifica ao criar um receptor determina quantas combinações de portas de receptores e endereços IP de destino você pode usar com seu acelerador de roteamento personalizado. Para obter o máximo de flexibilidade e reduzir a possibilidade de receber um erro que diz que você não tem portas de receptor suficientes disponíveis, recomendamos que você especifique um grande intervalo de portas.

O Global Accelerator aloca intervalos de portas em blocos quando você adiciona uma sub-rede a um acelerador de roteamento personalizado. Recomendamos que você aloque os intervalos de portas do receptor linearmente e torne os intervalos grandes o suficiente para serem compatíveis com o número de portas de destino que você pretende ter. Ou seja, o número de portas que você deve alocar deve ser pelo menos o tamanho da sub-rede multiplicado pelo número de portas e protocolos de destino (configurações de destino) que você terá na sub-rede.

> **Note**
>
> O algoritmo que o Global Accelerator usa para alocar mapeamentos de portas pode exigir que você adicione mais portas de receptor, além desse total.

Depois de criar um receptor, você pode editá-lo para adicionar mais intervalos de portas e protocolos associados, mas não pode diminuir os intervalos de portas existentes. Por exemplo, se você tiver um intervalo de portas do receptor de 5000 a 10 000, não poderá alterar o intervalo de portas para 5900 a 10 000 e não poderá alterar o intervalo de portas para 5000 a 9900.

Cada intervalo de portas do receptor deve incluir no mínimo 16 portas. Os receptores são compatíveis com as portas 1 a 65535.

Intervalos de portas de destino

Há dois lugares onde você especifica intervalos de portas para um acelerador de roteamento personalizado: os intervalos de portas que você especifica ao adicionar um receptor e os intervalos e protocolos de portas de destino que você especifica para um grupo de endpoints.

- Intervalos de portas do receptor: as portas do receptor nos endereços IP estáticos do Global Accelerator aos quais seus clientes se conectam. O Global Accelerator mapeia cada porta para um endereço IP de destino e porta exclusivos em uma sub-rede da VPC atrás do acelerador.
- Intervalos de portas de destino: os conjuntos de intervalos de portas de destino que você especifica para um grupo de endpoints (também chamados de configurações de destino) são as portas da instância do EC2 que recebem tráfego. Para receber tráfego nas portas de destino, os grupos de segurança associados às suas instâncias do EC2 devem permitir o tráfego nelas.

Verificações de integridade e failover

O Global Accelerator não realiza verificações de integridade para aceleradores de roteamento personalizados e não realiza failover para endpoints íntegros. O tráfego para aceleradores de roteamento personalizados é roteado de forma determinística, independentemente da integridade de um recurso de destino.

Todo o tráfego é negado por padrão

Por padrão, o tráfego direcionado por meio de um acelerador de roteamento personalizado é negado a todos os destinos em sua sub-rede. Para permitir que as instâncias de destino recebam

tráfego, você deve permitir especificamente todo o tráfego para a sub-rede ou, como alternativa, permitir o tráfego para endereços IP e portas de instâncias específicas na sub-rede.

Atualizar uma sub-rede ou destino específico para permitir ou negar tráfego leva tempo para se propagar pela internet. Para determinar se uma alteração foi propagada, você pode chamar a ação da API `DescribeCustomRoutingAccelerator` para verificar o status do acelerador. Para obter mais informações, consulte DescribeCustomRoutingAccelerator.

O AWS CloudFormation não é compatível

O AWS CloudFormation não é compatível com aceleradores de roteamento personalizados.

Aceleradores de roteamento personalizados no AWS Global Accelerator

Um acelerador de roteamento personalizado no AWS Global Accelerator permite que você use a lógica de aplicativo personalizada para direcionar um ou mais usuários para um destino específico entre muitos destinos, enquanto usa a rede global da AWS para melhorar a disponibilidade e o desempenho do seu aplicativo.

Um acelerador de roteamento personalizado roteia o tráfego somente para portas em instâncias do Amazon EC2 que estão em execução em sub-redes de nuvem privada virtual (VPC). Com um acelerador de roteamento personalizado, o Global Accelerator não roteia o tráfego com base na geoproximidade ou na integridade do endpoint. Para saber mais, consulte Como os aceleradores de roteamento personalizados funcionam no Global Accelerator.

Quando você cria um acelerador, por padrão, o Global Accelerator fornece um conjunto de dois endereços IPv4 estáticos. Os aceleradores de roteamento personalizados são compatíveis apenas com o tipo de endereço IP IPv4. Se você trouxer seu próprio intervalo de endereços IP para a AWS (BYOIP), poderá atribuir endereços IPv4 estáticos de seu próprio grupo para usar com seu acelerador. Para ter mais informações, consulte Trazer seus próprios endereços IP (BYOIP) no Global Accelerator.

Important

Os endereços IP são atribuídos ao seu acelerador enquanto ele existir, mesmo se você desabilitar o acelerador e ele não aceitar ou rotear mais o tráfego. No entanto, ao excluir um acelerador, você perde os endereços IP estáticos do Global Accelerator que estão

atribuídos ao acelerador, de modo que você não pode mais rotear o tráfego usando-os. Como prática recomendada, verifique se você tem permissões para evitar excluir os aceleradores acidentalmente. Você pode usar políticas do IAM, como permissões baseadas em tags, com o Global Accelerator para limitar os usuários que têm permissão para excluir um acelerador. Para ter mais informações, consulte ABAC com Global Accelerator.

Esta seção explica como trabalhar com um acelerador de roteamento personalizado no console do Global Accelerator. Para saber mais sobre o uso de operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Conteúdo

Criar um acelerador de roteamento personalizado no Global Accelerator

Esta seção fornece etapas sobre como criar um acelerador personalizado no console. Para trabalhar com o Global Accelerator de forma programática, consulte a Referência da API do AWS Global Accelerator.

Para criar um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Escolha Criar acelerador.
3. Forneça um nome para o acelerador.
4. Em Tipo de acelerador, selecione Roteamento personalizado.
5. Opcionalmente, se você trouxe seu próprio intervalo de endereços IP para a AWS (BYOIP), você pode especificar endereços IP estáticos para seu acelerador a partir desse grupo de endereços. Faça essa escolha para cada um dos dois endereços IP estáticos do seu acelerador.
   - Para cada endereço IP estático, escolha o grupo de endereços IP a ser usado.

- Se você escolheu seu próprio grupo de endereços IP, escolha também um endereço IP específico do grupo. Se você escolheu o grupo de endereços IP padrão da Amazon, o Global Accelerator atribuirá um endereço IP específico ao seu acelerador.

6. Opcionalmente, adicione uma ou mais tags para ajudá-lo a identificar seus recursos do acelerador.
7. Escolha Avançar para ir para as próximas páginas do assistente e adicionar receptores, grupos de endpoints e endpoints de sub-rede da VPC.

Editar um acelerador de roteamento personalizado no Global Accelerator

Esta seção fornece etapas sobre como atualizar um acelerador personalizado no console. Para trabalhar com o Global Accelerator de forma programática, consulte a Referência da API do AWS Global Accelerator.

Para editar um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na lista de aceleradores de roteamento personalizados, escolha um e, em seguida, escolha Editar.
3. Na página Editar acelerador, faça as alterações que desejar. Por exemplo, é possível desabilitar o acelerador para poder excluí-lo.
4. Escolha Salvar.

Visualizar aceleradores de roteamento personalizados no Global Accelerator

Esta seção fornece etapas para visualizar informações sobre seus aceleradores de roteamento personalizados no console. Para ver as descrições de seus aceleradores de roteamento personalizados de forma programática, consulte ListCustomRoutingAccelerator e DescribeCustomRoutingAccelerator na Referência da API do AWS Global Accelerator.

Para visualizar informações sobre aceleradores de roteamento personalizados

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.

2. Para ver detalhes sobre um acelerador, escolha um acelerador e, em seguida, escolha Visualizar.

Excluir um acelerador de roteamento personalizado no Global Accelerator

Se você criou um acelerador de roteamento personalizado como teste ou se não estiver mais usando um acelerador, poderá excluí-lo. No console, desabilite o acelerador e, em seguida, você poderá excluí-lo. Você não precisa remover receptores e grupos de endpoints do acelerador.

Para excluir um acelerador de roteamento personalizado usando uma operação de API em vez do console, você deve primeiro remover todos os receptores e grupos de endpoints associados ao acelerador e depois desabilitá-lo. Para obter mais informações, consulte a operação DeleteAccelerator na referência da API do AWS Global Accelerator.

Para desabilitar um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na lista, escolha um acelerador que você deseja desabilitar.
3. Selecione a opção Editar.
4. Selecione Desabilitar acelerador e depois Salvar.

Para excluir um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na lista, escolha um acelerador que você deseja excluir.
3. Escolha Excluir.

> **Note**
>
> Se você não tiver desabilitado o acelerador, a opção Excluir não estará disponível. Para desabilitar o acelerador, consulte o procedimento anterior.

4. Na caixa de diálogo de confirmação, escolha Excluir.

> **Important**
>
> Ao excluir um acelerador, você perde os endereços IP estáticos atribuídos ao acelerador e, portanto, não pode mais rotear o tráfego usando-os.

Receptores de aceleradores de roteamento personalizados no Global Accelerator

Para um acelerador de roteamento personalizado do AWS Global Accelerator, você configura um receptor que especifica uma variedade de portas do receptor com protocolos associados que o Global Accelerator mapeia para instâncias específicas do Amazon EC2 de destino em seus endpoints de sub-rede da VPC. Quando você adiciona um endpoint de sub-rede da VPC, o Global Accelerator cria um mapeamento estático de portas entre os intervalos de portas que você define para seu receptor e os endereços IP e portas de destino na sub-rede. Em seguida, você pode usar o mapeamento de portas para especificar os endereços IP estáticos do acelerador junto com uma porta e um protocolo do receptor para direcionar o tráfego do usuário para endereços IP e portas específicas da instância Amazon EC2 de destino na sua sub-rede da VPC.

Você define um receptor ao criar seu acelerador de roteamento personalizado e pode adicionar mais receptores a qualquer momento. Cada receptor pode ter um ou mais grupos de endpoints, um para cada região da AWS na qual você tem endpoints de sub-rede da VPC. Um receptor em um acelerador de roteamento personalizado é compatível com os protocolos TCP e UDP. Você especifica o protocolo ou protocolos para cada intervalo de portas de destino definido: UDP, TCP ou UDP e TCP.

Para ter mais informações, consulte Como os aceleradores de roteamento personalizados funcionam no Global Accelerator.

Conteúdo

Adicionar um receptor para um acelerador de roteamento personalizado no Global Accelerator

Esta seção explica como adicionar um receptor para um acelerador de roteamento personalizado no console do AWS Global Accelerator. Para saber mais sobre como usar operações de API com o AWS Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para adicionar um receptor para um acelerador de roteamento personalizado

O intervalo que você especifica ao criar um receptor define quantas combinações de portas de receptor e endereços IP de destino você pode usar com seu acelerador de roteamento personalizado. Para obter o máximo de flexibilidade, recomendamos que você especifique um grande intervalo de portas. Cada intervalo de portas do receptor que você especificar deve incluir no mínimo 16 portas.

> **Note**
>
> Depois de criar um receptor, você pode editá-lo para adicionar mais intervalos de portas e protocolos associados, mas não pode diminuir os intervalos de portas existentes.

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Na página Aceleradores, escolha um acelerador de roteamento personalizado.
3. Escolha Add listener.
4. Na página Adicionar receptor, insira o intervalo de portas do receptor que você deseja associar ao acelerador.

   Os receptores são compatíveis com as portas 1 a 65535. Para máxima flexibilidade com um acelerador de roteamento personalizado, recomendamos que você especifique um grande intervalo de portas.
5. Escolha Add listener.

Editar um receptor para um acelerador de roteamento personalizado no Global Accelerator

Esta seção explica como editar um receptor para um acelerador de roteamento personalizado no console do AWS Global Accelerator. Para saber mais sobre como usar operações de API com o AWS Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para editar um receptor para um acelerador de roteamento personalizado

Ao editar um receptor para um acelerador de roteamento personalizado, lembre-se de que você pode adicionar mais intervalos de portas e protocolos associados, aumentar os intervalos de portas existentes ou alterar protocolos, mas não pode diminuir os intervalos de portas existentes.

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Na página Aceleradores, escolha um acelerador.
3. Escolha um receptor e, em seguida, escolha Editar receptor.
4. Na página Editar receptor, faça as alterações desejadas nos intervalos de portas ou protocolos existentes ou adicione novos intervalos de portas.

   Esteja ciente de que você não pode diminuir um intervalo de portas existente.
5. Escolha Salvar.

Remover um receptor para um acelerador de roteamento personalizado no Global Accelerator

Esta seção explica como remover um receptor para um acelerador de roteamento personalizado no console do AWS Global Accelerator. Para saber mais sobre como usar operações de API com o AWS Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para remover um receptor

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Na página Aceleradores, escolha um acelerador.
3. Escolha um receptor e, em seguida, escolha Remover.

4. Na caixa de diálogo de confirmação, escolha Remover.

Grupos de endpoints para aceleradores de roteamento personalizados no Global Accelerator

Com um acelerador de roteamento personalizado no AWS Global Accelerator, um grupo de endpoints define as portas e protocolos nos quais as instâncias do Amazon EC2 de destino em suas sub-redes de nuvem privada virtual (VPC) aceitam tráfego.

Você cria um grupo de endpoints para seu acelerador de roteamento personalizado para cada Região da AWS em que suas sub-redes da VPC e instâncias do EC2 estão localizadas. Cada grupo de endpoints em um acelerador de roteamento personalizado pode ter vários endpoints de sub-rede da VPC. Da mesma forma, você pode adicionar cada VPC a vários grupos de endpoints, mas os grupos de endpoints devem estar associados a diferentes receptores.

Para cada grupo de endpoints, você especifica um conjunto de um ou mais intervalos de portas que incluem as portas para as quais você deseja direcionar o tráfego nas instâncias do EC2 na região. Para cada intervalo de portas do grupo de endpoints, você especifica o protocolo a ser usado: UDP, TCP, ou UDP e TCP. Isso oferece flexibilidade máxima para você, sem precisar duplicar conjuntos de intervalos de portas para cada protocolo. Por exemplo, você pode ter um servidor de jogos com tráfego de jogos em execução por UDP nas portas 8080 a 8090, enquanto você também tem um servidor que receba mensagens de chat via TCP na porta 80.

Para saber mais, consulte Como os aceleradores de roteamento personalizados funcionam no Global Accelerator.

Conteúdo

Adicionar um grupo de endpoints para um acelerador de roteamento personalizado no Global Accelerator

Você trabalha com um grupo de endpoints para seu acelerador de roteamento personalizado no console do AWS Global Accelerator ou usando uma operação de API. Você pode adicionar ou remover endpoints de sub-rede da VPC de um grupo de endpoints a qualquer momento.

Esta seção explica como criar grupos de endpoints para seu acelerador de roteamento personalizado no console do AWS Global Accelerator. Para saber mais sobre o uso de operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para adicionar um grupo de endpoints em um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na página Aceleradores, escolha um acelerador de roteamento personalizado.
3. Na seção Receptores, em ID do receptor, escolha o ID do receptor ao qual você deseja adicionar um grupo de endpoints.
4. Escolha Adicionar grupo de endpoints.
5. Na seção de um receptor, especifique uma região para o grupo de endpoints.
6. Em Conjuntos de portas e protocolos, insira intervalos de portas e protocolos para suas instâncias do Amazon EC2.

   - Insira Da porta e Até a porta para especificar um intervalo de portas.
   - Para cada intervalo de portas, especifique o protocolo ou protocolos desse intervalo.

   O intervalo de portas não precisa ser um subconjunto do intervalo de portas do receptor, mas deve haver um total de portas suficiente no intervalo de portas do receptor para ser compatível com número total de portas que você especifica para os grupos de endpoints em seu acelerador de roteamento personalizado.
7. Escolha Salvar.
8. Opcionalmente, escolha Adicionar grupo de endpoints para adicionar outros grupos de endpoints para esse receptor. Você também pode escolher outro receptor e adicionar grupos de endpoints.
9. Escolha Adicionar grupo de endpoints.

Editar um grupo de endpoints para um acelerador de roteamento personalizado no Global Accelerator

Você trabalha com um grupo de endpoints para seu acelerador de roteamento personalizado no console do AWS Global Accelerator ou usando uma operação de API. Você pode adicionar ou remover endpoints de sub-rede da VPC de um grupo de endpoints a qualquer momento.

Esta seção explica como editar grupos de endpoints para seu acelerador de roteamento personalizado no console do AWS Global Accelerator. Para saber mais sobre o uso de operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para editar um grupo de endpoints em um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.
2. Na página Aceleradores, escolha um acelerador de roteamento personalizado.
3. Na seção Receptores, em ID do receptor, escolha o ID do receptor ao qual o grupo de endpoints está associado.
4. Escolha Editar grupo de endpoints.
5. Na página Editar grupo de endpoints, altere a região, o intervalo de portas ou o protocolo de um intervalo de portas.
6. Escolha Salvar.

Remover um grupo de endpoints para um acelerador de roteamento personalizado no Global Accelerator

Você trabalha com um grupo de endpoints para seu acelerador de roteamento personalizado no console do AWS Global Accelerator ou usando uma operação de API.

Esta seção explica como remover grupos de endpoints para seu acelerador de roteamento personalizado no console do AWS Global Accelerator. Para saber mais sobre o uso de operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para remover um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator em https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome:.

2. Na página Aceleradores, escolha um acelerador.
3. Na seção Receptores, escolha um receptor e, em seguida, escolha Remover.
4. Na seção Grupos de endpoints, escolha um grupo de endpoints e, em seguida, escolha Remover.
5. Na caixa de diálogo de confirmação, escolha Remover.

Endpoints de sub-rede da Amazon VPC para aceleradores de roteamento personalizados no Global Accelerator

Os endpoints para aceleradores de roteamento personalizados são sub-redes da nuvem privada virtual (VPC) da Amazon que podem receber tráfego por meio de um acelerador. Cada sub-rede pode conter um ou vários destinos de instância do Amazon EC2. Quando você adiciona um endpoint de sub-rede, o Global Accelerator gera um novo mapeamento de portas. Em seguida, você pode usar a API do Global Accelerator para obter uma lista estática de todos os mapeamentos de portas da sub-rede, que você pode usar para rotear o tráfego para os endereços IP da instância do EC2 de destino na sub-rede. Para obter mais informações, consulte ListCustomRoutingPortMappings.

Lembre-se do seguinte ao adicionar sub-redes e destinos da VPC ao seu acelerador de roteamento personalizado:

- Você só pode direcionar o tráfego para instâncias do EC2 nas sub-redes, não para outros recursos, como balanceadores de carga (em contraste com os aceleradores padrão).
- Um destino de instância do EC2 em um endpoint de sub-rede não pode ser um dos seguintes tipos: C1, CC1, CC2, CG1, CG2, CR1, CS1, G1, G2, HI1, HS1, M1, M2, M3 ou T1.
- Por padrão, o tráfego direcionado por meio de um acelerador de roteamento personalizado não pode chegar a nenhum destino na sua sub-rede. Para permitir que as instâncias de destino recebam tráfego, você deve optar por permitir todo o tráfego para a sub-rede ou, como alternativa, habilitar o tráfego para endereços IP e portas específicas da instância (sockets de destino) na sub-rede.

> **Important**
>
> Atualizar uma sub-rede ou destino específico para permitir ou negar tráfego leva tempo para se propagar pela internet. Para determinar se uma alteração foi propagada, você

pode usar a ação de API `DescribeCustomRoutingAccelerator` para verificar o status do acelerador. Para obter mais informações, consulte DescribeCustomRoutingAccelerator.

- Como as sub-redes de VPC preservam o endereço IP do cliente, você deve revisar as informações relevantes de segurança e configuração ao adicionar sub-redes como endpoints para aceleradores de roteamento personalizados. Para ter mais informações, consulte Requisitos para endpoints com preservação do endereço IP do cliente.
- Ao configurar recursos como endpoints por trás do Global Accelerator, recomendamos que você também não envie tráfego diretamente para os mesmos endpoints pela internet. O envio de tráfego direto pode causar problemas de colisão na conexão.

Para saber mais, consulte Como os aceleradores de roteamento personalizados funcionam no Global Accelerator.

Conteúdo

Adicionar um endpoint de sub-rede da VPC a um acelerador de roteamento personalizado

Você adiciona endpoints de sub-rede da nuvem privada virtual (VPC) da Amazon a grupos de endpoints em seus aceleradores de roteamento personalizados para que você possa direcionar o tráfego de usuários para instâncias do Amazon EC2 de destino na sub-rede.

Ao adicionar e remover instâncias do EC2 da sub-rede, ou habilitar ou desabilitar o tráfego para destinos do EC2, você decide se esses destinos podem receber tráfego. No entanto, o mapeamento de portas do Global Accelerator não muda.

Para permitir o tráfego para alguns destinos na sub-rede, mas não para todos, insira endereços IP para cada instância do EC2 que você deseja permitir, junto com as portas da instância em que você deseja receber tráfego. Os endereços IP que você especificar devem ser para instâncias do EC2 na sub-rede. Você pode especificar uma porta ou um intervalo de portas a partir das portas mapeadas para a sub-rede.

Você pode remover a sub-rede da VPC do seu acelerador removendo-a de um grupo de endpoints. A remoção de uma sub-rede não afeta a sub-rede em si, mas o Global Accelerator não pode mais direcionar o tráfego para a sub-rede ou para as instâncias do Amazon EC2 nela. Além disso, o Global Accelerator recuperará o mapeamento de portas da sub-rede da VPC para potencialmente usá-las em novas sub-redes que você adicionar.

As etapas desta seção explicam como adicionar endpoints de sub-rede da VPC no console do AWS Global Accelerator. Para saber mais sobre como usar operações de API com o AWS Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para adicionar um endpoint de sub-rede da VPC

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Na página Aceleradores, escolha um acelerador de roteamento personalizado.
3. Na seção Receptores, em ID do receptor, escolha o ID de um receptor.
4. Na seção Grupos de endpoints, em ID do grupo de endpoints, escolha o ID do grupo de endpoints (região da AWS) ao qual você deseja adicionar o endpoint de sub-rede da VPC.
5. Na seção Endpoints, escolha Adicionar endpoint.
6. Na página Adicionar endpoints, em Endpoint, escolha uma sub-rede da VPC.

   Se você não tiver VPCs, não haverá itens na lista. Para continuar, adicione pelo menos uma VPC, depois volte às etapas aqui e escolha uma VPC na lista.
7. Para o endpoint de sub-rede da VPC que você adiciona, você pode optar por permitir ou negar tráfego para todos os destinos na sub-rede, ou você pode permitir tráfego somente para instâncias e portas EC2 específicas. O padrão é negar tráfego para todos os destinos na sub-rede.
8. Escolha Add endpoint.

Editar um endpoint de sub-rede da VPC para um acelerador de roteamento personalizado

Você pode editar endpoints de sub-rede da nuvem privada virtual (VPC) da Amazon para seus aceleradores de roteamento personalizados para que você possa direcionar o tráfego de usuários para instâncias do Amazon EC2 de destino, ou permitir ou negar o tráfego a todos os destinos na sub-rede.

Ao adicionar e remover instâncias do EC2 da sub-rede, ou habilitar ou desabilitar o tráfego para destinos do EC2, você decide se esses destinos podem receber tráfego. No entanto, o mapeamento de portas do Global Accelerator não muda.

As etapas desta seção explicam como editar endpoints de sub-rede da VPC no console do AWS Global Accelerator. Para saber mais sobre como usar operações de API com o AWS Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para permitir ou negar tráfego para destinos específicos

Você pode editar o mapeamento de portas de sub-rede para um endpoint da VPC para permitir ou negar tráfego para instâncias e portas EC2 específicas (sockets de destino) em uma sub-rede.

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Na página Aceleradores, escolha um acelerador de roteamento personalizado.
3. Na seção Receptores, em ID do receptor, escolha o ID de um receptor.
4. Na seção Grupos de endpoints, em ID do grupo de endpoints, escolha o ID do grupo de endpoints (região da AWS) do endpoint de sub-rede da VPC que você deseja editar.
5. Escolha uma sub-rede de endpoint e, em seguida, escolha Visualizar detalhes.
6. Na página Endpoint, em Mapeamentos de portas, escolha um endereço IP e, em seguida, escolha Editar.
7. Insira as portas para as quais você deseja habilitar o tráfego e escolha Permitir esses destinos.

Para permitir ou negar TODO o tráfego para uma sub-rede

Você pode atualizar um endpoint para permitir ou negar tráfego para todos os destinos na sub-rede da VPC.

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Na página Aceleradores, escolha um acelerador de roteamento personalizado.
3. Na seção Receptores, em ID do receptor, escolha o ID de um receptor.
4. Na seção Grupos de endpoints, em ID do grupo de endpoints, escolha o ID do grupo de endpoints (região da AWS) do endpoint de sub-rede da VPC que você deseja atualizar.
5. Escolha Permitir/Negar todo o tráfego.

6. Escolha uma opção para permitir ou negar todo o tráfego e, em seguida, escolha Salvar.

Remover um endpoint de sub-rede da VPC para um acelerador de roteamento personalizado

Você pode remover um endpoint de sub-rede da nuvem privada virtual (VPC) da Amazon do seu acelerador de roteamento personalizado para que o tráfego do usuário não vá mais para as instâncias do Amazon EC2 de destino na sub-rede.

As etapas desta seção explicam como remover um endpoint de sub-rede da VPC no console do AWS Global Accelerator. Para saber mais sobre como usar operações de API com o AWS Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para remover um endpoint

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Na página Aceleradores, escolha um acelerador de roteamento personalizado.
3. Na seção Receptores, em ID do receptor, escolha o ID de um receptor.
4. Na seção Grupos de endpoints, em ID do grupo de endpoints, escolha o ID do grupo de endpoints (região da AWS) do endpoint de sub-rede da VPC que você deseja remover.
5. Escolha Remover endpoint.
6. Na caixa de diálogo de confirmação, escolha Remover.

Configurar o acesso entre contas no Global Accelerator

Ao usar a compatibilidade entre contas, você pode usar o AWS Global Accelerator como um ponto de entrada fixo para seu aplicativo que acessa recursos em várias contas ou escolher endereços IP para seu acelerador a partir de blocos CIDR compartilhados. Usar permissões entre contas para permitir o acesso a recursos em contas diferentes é uma prática recomendada pela AWS. Com a compatibilidade entre contas para blocos CIDR de endereços traga seu próprio IP (BYOIP), você pode usar o mesmo grupo de endereços para aceleradores em contas diferentes em sua organização. Você também pode organizar recursos da AWS em uma conta que controla o acesso à internet aos seus aplicativos, o que pode simplificar o monitoramento e a segurança, além de fornecer visibilidade às conexões de entrada.

A compatibilidade entre contas no Global Accelerator permite que você:

- Adicione endpoints, como Network Load Balancers, de outras contas a um acelerador.
- Escolha um grupo de endereços BYOIP para endereços IP e, em seguida, selecione endereços IP do grupo para aceleradores em contas diferentes. Ao compartilhar um grupo de endereços BYOIP, você pode usar mais endereços do mesmo bloco CIDR, reduzindo o número de blocos CIDR necessários.

Você pode trabalhar com anexos e recursos entre contas no console do Global Accelerator ou usando as operações da API do Global Accelerator com a AWS Command Line Interface (AWS CLI) ou um SDK da AWS. Por exemplo, como entidade principal, você pode usar a operação UpdateEndpoints para adicionar um recurso entre contas como um endpoint para um acelerador. Ao usar a operação de API, você especifica o ARN do anexo entre contas e o ID do endpoint. Para obter mais informações, consulte o Guia de referência da API do AWS Global Accelerator.

Conteúdo

Como a compatibilidade entre contas funciona no Global Accelerator

Com a compatibilidade entre contas no Global Accelerator, os proprietários de recursos controlam se seus recursos são compartilhados com aceleradores pertencentes a outras contas. Para permitir o compartilhamento de recursos para seus recursos, você, como proprietário do recurso, cria um anexo entre contas do Global Accelerator para autorizar recursos em sua conta a serem adicionados a um acelerador por outra conta.

Você cria o anexo entre contas no Global Accelerator. O anexo lista os recursos que você deseja compartilhar e as entidades principais, outras contas ou ARNs específicos do acelerador, que estão autorizadas a usar os recursos. Os recursos podem ser recursos da AWS, como Network Load Balancers, que você adiciona como endpoints aos grupos de endpoints do acelerador, ou os recursos podem ser intervalos de endereços IP que você trouxe para o Global Accelerator com o processo traga seu próprio endereço IP (BYOIP).

> **Important**
>
> Antes de adicionar um intervalo de endereços IP BYOIP a um anexo entre contas para compartilhar com as entidades principais, você deve concluir o processo para provisionar e anunciar o intervalo de endereços. Para ter mais informações, consulte Trazer seus próprios endereços IP (BYOIP) no Global Accelerator.

Depois que você, como proprietário do recurso, cria um anexo, as entidades principais listadas no anexo podem trabalhar com os recursos listados no anexo. Ou seja, eles podem adicionar como endpoints os recursos da AWS listados ou selecionar como endereço IP estático um endereço BYOIP dos prefixos CIDR listados. Quando uma entidade principal deseja adicionar um recurso entre contas para um acelerador, ela deve especificar o anexo entre contas que a autoriza a ser uma entidade principal com permissão para usar o recurso.

Trabalhar com anexos entre contas no Global Accelerator

Para permitir que alguém adicione um recurso de outra conta como um endpoint ou endereço BYOIP para um acelerador, o proprietário do recurso deve criar um anexo entre contas no Global Accelerator. No anexo, o proprietário do recurso especifica um ou mais aceleradores ou contas

(entidades principais) que podem adicionar recursos, junto com os recursos específicos que as entidades principais podem adicionar aos aceleradores.

Como proprietário de um recurso, esteja ciente de que, para especificar um recurso em um anexo entre contas, você deve possuir o recurso em sua conta da AWS. Ou seja, o recurso deve ser alocado ou provisionado em sua conta. Você não pode especificar um recurso que tenha sido compartilhado com você, como uma sub-rede compartilhada.

Conteúdo

Criar um anexo entre contas no AWS Global Accelerator

Siga as etapas desta seção para criar um anexo entre contas usando o console do AWS Global Accelerator.

Esta seção explica como criar um anexo entre contas usando o console do AWS Global Accelerator. Para saber mais sobre o uso de operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para criar um anexo entre contas

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Escolha Criar anexo entre contas.
3. Na página Criar anexo entre contas, insira um nome para o anexo.
4. Adicione as Contas da AWS ou os ARNs dos aceleradores, ou ambos, que você deseja permitir para adicionar seus recursos.
5. Escolha os recursos que você deseja permitir que sejam usados. Por exemplo, para adicionar recursos que podem ser adicionados como endpoints, para cada recurso, escolha uma Região da AWS. Em seguida, nos menus suspensos, selecione um tipo de endpoint (tipo de recurso) e o endpoint (recurso) a ser adicionado.
6. Escolha Create attachment (Criar anexo).

Observação: para ver o novo anexo entre contas na sua lista de anexos, atualize a página Anexos entre contas.

Editar um anexo entre contas no AWS Global Accelerator

Siga as etapas desta seção para editar um anexo entre contas usando o console do AWS Global Accelerator.

Esta seção explica como editar um anexo entre contas usando o console do AWS Global Accelerator. Para saber mais sobre o uso de operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Você pode editar um anexo entre contas para adicionar ou remover entidades principais ou recursos, renomear o anexo ou excluir o anexo.

Esteja ciente do seguinte ao remover entidades principais, recursos ou excluir um anexo:

- Para remover uma entidade principal ou CIDR de um anexo, a entidade principal deve primeiro remover endereços IP compartilhados de todos os aceleradores que os usam. Em seguida, você pode remover a entidade principal, ou CIDRs, do anexo.
- Antes de remover endereços IP compartilhados ou remover a autorização para que as entidades principais acessem um CIDR compartilhado a partir de um anexo, os endereços IP compartilhados do CIDR não devem ser usados atualmente por nenhum acelerador.
- Se você remover uma entidade principal de um anexo entre contas que permita que a entidade principal adicione um ou mais endpoints compartilhados, o Global Accelerator removerá esses endpoints entre contas de qualquer acelerador que use essa permissão para os recursos entre contas listados no anexo.
- Se você remover um recurso de endpoint de um anexo entre contas, o Global Accelerator removerá o endpoint de várias contas de qualquer acelerador em que ele tenha sido adicionado como um endpoint com base nas permissões do anexo.
- Se você excluir um anexo entre contas, o Global Accelerator removerá todos os endpoints entre contas listados no anexo de todos os aceleradores nos quais os recursos foram adicionados como endpoints com base nas permissões no anexo.
- Se houver vários anexos entre contas que incluem uma entidade principal ou um recurso, o Global Accelerator continuará a permitir o acesso que qualquer anexo existente fornece. Assim, por exemplo, se você remover uma entidade principal de um anexo, mas a entidade principal ainda tiver permissão para acessar um recurso concedido por um segundo anexo, o Global Accelerator continuará permitindo que a entidade principal acesse o recurso entre contas.

Para editar um anexo entre contas

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Escolha Anexos entre contas.
3. Escolha um anexo entre contas para atualizar e, em seguida, escolha Editar.
4. Modifique o anexo para fazer as alterações necessárias. Por exemplo, você pode adicionar ou remover entidades principais, renomear o anexo ou adicionar ou remover recursos.
5. Escolha Salvar alterações.

Excluir um anexo entre contas no Global Accelerator

Siga as etapas desta seção para excluir um anexo entre contas usando o console do AWS Global Accelerator.

Esta seção explica como excluir um anexo entre contas usando o console do AWS Global Accelerator. Para saber mais sobre o uso de operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para excluir um anexo entre contas

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Escolha Anexos entre contas.
3. Escolha um anexo entre contas e, em seguida, escolha Excluir.
4. Na caixa de diálogo, digite excluir na caixa de texto para confirmar que deseja excluir o anexo entre contas.
5. Escolha Excluir.

Trabalhar com recursos entre contas no Global Accelerator

Se sua conta, ou um acelerador que você tem permissão para acessar, for especificado como entidade principal em um anexo entre contas no AWS Global Accelerator, você poderá usar recursos que foram compartilhados com você de outra conta.

Por exemplo, você pode selecionar endereços traga seu próprio IP (BYOIP) como endereços IP estáticos ao criar um acelerador ou adicionar endpoints aos grupos de endpoints do acelerador para um acelerador. Os recursos que você pode adicionar também devem ser especificados no anexo.

As seções a seguir incluem as etapas para adicionar ou remover anexos entre contas no Global Accelerator.

Conteúdo

Adicionar um endereço BYOIP entre contas no Global Accelerator

Siga as etapas desta seção para configurar seus próprios endereços de ID traga seu próprio IP (BYOIP) entre contas usando o console do Global Accelerator.

Esta seção explica como usar um endereço IP BYOIP usando o console do AWS Global Accelerator. Para saber mais sobre o uso de operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Você pode alterar os endereços BYOIP que você usa para seu acelerador, mas algumas restrições se aplicam. Para ter mais informações, consulte Como atualizar um acelerador para alterar um endereço IP.

Para usar um endereço IP BYOIP entre contas

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Escolha Criar acelerador.
3. Forneça um nome para o acelerador.
4. Selecione um Tipo de acelerador.
5. Em Tipo de endereço IP, selecione IPv4.
6. Marque a caixa de seleção Usar um endereço IP estático de um CIDR autorizado entre contas.
7. Selecione o ID da conta do proprietário do anexo entre contas que especifica você como entidade principal e que inclui o bloco de endereços BYOIP que foi compartilhado com você.

Observe que, como você deve escolher uma conta para selecionar endereços, se você selecionar dois endereços IP BYOIP ao criar um acelerador, os endereços IP devem ter o mesmo proprietário e estar autorizados no mesmo anexo entre contas.

8. Especifique um ou ambos os endereços IP estáticos para seu acelerador.

   - Para cada endereço IP estático, escolha o grupo de endereços IP a ser usado.

     > **Note**
     >
     > Você deve escolher um grupo de endereços IP diferente para cada endereço IP estático. Essa restrição ocorre porque o Global Accelerator atribui cada intervalo de endereços a uma zona da rede diferente, para alta disponibilidade.

   - Se você escolheu seu próprio grupo de endereços IP, escolha também um endereço IP específico do grupo. Se você escolher o grupo de endereços IP padrão da Amazon, o Global Accelerator atribuirá um endereço IP específico ao seu acelerador.

9. Opcionalmente, adicione uma ou mais tags para ajudá-lo a identificar seus recursos do acelerador.
10. Escolha Avançar para adicionar receptores, grupos de endpoints e endpoints.

Adicionar endpoint entre contas no AWS Global Accelerator

Siga as etapas desta seção para adicionar endpoints entre contas usando o console do Global Accelerator.

Esta seção explica como adicionar endpoints entre contas usando o console do AWS Global Accelerator. Para saber mais sobre o uso de operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para adicionar um endpoint entre contas

1. Ao criar ou atualizar um acelerador, na seção Endpoints, escolha Adicionar endpoint.
2. Na página Adicionar endpoints, selecione Adicionar um recurso especificado em um anexo entre contas.
3. No menu suspenso, selecione uma Conta da AWS que tenha criado um anexo entre contas que inclua você ou o acelerador como entidade principal.

4. Em Tipo de endpoint, escolha o tipo de recurso que você deseja adicionar.

   Observe que somente os tipos de recursos incluídos no anexo entre contas aparecem no menu suspenso.

5. Em Endpoint, escolha o recurso que você deseja adicionar.

   Observe que somente os recursos incluídos no anexo entre contas aparecem no menu suspenso. Para ver os recursos que não estão habilitados por um anexo entre contas, desmarque a caixa de seleção Adicionar um recurso especificado em um anexo entre contas.

Remover um endpoint entre contas no Global Accelerator

Siga as etapas desta seção para remover endpoints entre contas usando o console do Global Accelerator.

Esta seção explica como remover endpoints entre contas usando o console do AWS Global Accelerator. Para saber mais sobre o uso de operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Para remover um endpoint entre contas

1. Ao criar ou atualizar um acelerador, na página de detalhes do Grupo de endpoints, escolha o endpoint que você deseja remover.
2. Escolha Remover.

Identificar recursos entre contas no Global Accelerator

Entidades principais e proprietários de recursos podem identificar recursos compartilhados usando o console do AWS Global Accelerator ou usando a AWS CLI com operações do Global Accelerator. Por exemplo, você pode fazer o seguinte:

- Como proprietário, você pode ver uma lista dos anexos entre contas e ver as entidades principais e os recursos em cada anexo.
- Como entidades principais, você pode visualizar todos os anexos entre contas nos quais está listado e listar os recursos que podem ser adicionados como endpoints ou intervalos de endereços IP para um acelerador, para um anexo específico.

Para obter mais informações sobre o uso de operações de API para visualizar anexos entre contas e recursos compartilhados, consulte o Guia de referência de API do AWS Global Accelerator.

Como proprietário: identifique seus recursos entre contas no Global Accelerator

Como proprietário, você pode visualizar seus anexos entre contas no AWS Management Console, ou usando a AWS Command Line Interface com operações de API do Global Accelerator.

Para visualizar anexos entre contas

- No console do Global Accelerator, escolha Anexos entre contas.

Para ver as informações incluídas em um anexo entre contas

1. No console do Global Accelerator, na página Anexos entre contas, escolha um anexo e escolha Exibir detalhes.

   —OU—

2. Use a operação de API ListCrossAccountResources, por exemplo, usando a AWS Command Line Interface. Essa operação retorna uma lista de pares exclusivos de anexo-recurso, para cada recurso, em cada anexo, na conta.

   Por exemplo, se você tiver dois anexos entre contas, e o primeiro incluir dois endpoints e um bloco CIDR, enquanto o segundo incluir três endpoints, `ListCrossAccountResources` retornará seis pares de anexo-recurso: attachment1-endpoint1, attachment1-endpoint2, attachment1-CIDR, attachment2-endpoint3, attachment2-endpoint4 e attachment2-endpoint5.

Como entidade principal: identifique seus recursos entre contas no Global Accelerator

Como entidade principal, depois de ser autorizado por um anexo entre contas a adicionar um recurso a um acelerador como um endpoint, não há nenhuma ação adicional a ser tomada antes de adicionar um recurso como endpoint.

Você pode ver as Contas da AWS que criaram um anexo entre contas no qual você está listado como entidade principal. Você também pode ver os recursos especificados no anexo que cada conta criou, que você pode adicionar como endpoints ou intervalos de endereços IP para um acelerador.

Para ver as contas que criaram um anexo entre contas nas quais você está listado como entidade principal no

1. No console do Global Accelerator, na página Detalhes do endpoint de um acelerador, escolha Adicionar endpoint.
2. Na página Adicionar endpoints, selecione Adicionar um recurso especificado em um anexo entre contas.
3. No menu suspenso em Selecionar ID da conta do proprietário do anexo entre contas, visualize a conta ou contas que lhe dão permissão em um anexo entre contas para adicionar recursos ao acelerador.

Para ver os recursos de endpoint especificados no anexo que cada conta criou

1. No console do Global Accelerator, na página Detalhes do endpoint de um acelerador, escolha Adicionar endpoint.
2. Na página Adicionar endpoints, selecione Adicionar um recurso especificado em um anexo entre contas.
3. No menu suspenso, selecione uma conta que lhe dê permissão em um anexo entre contas para adicionar recursos ao acelerador.
4. Em Tipo de endpoint, escolha um tipo de recurso.

   Observe que somente os tipos de recursos incluídos no anexo entre contas aparecem no menu suspenso.
5. No menu suspenso do Endpoint, há uma lista dos recursos. Esses são os recursos que você está autorizado pela conta que criou o anexo entre contas para adicionar como endpoints, para um tipo de recurso específico.
6. Para ver os recursos que você pode adicionar e que estão especificados no anexo entre contas criado por uma conta diferente, faça o seguinte: no menu suspenso em Selecionar ID da conta do proprietário do anexo entre contas, selecione uma Conta da AWS diferente.

Para ver os recursos de endereço IP especificados no anexo que uma conta criou

1. No console do Global Accelerator, escolha Criar acelerador.
2. Na página Inserir nome, em tipo de endereço IP, selecione IPv4.

3. Na seleção do grupo de endereços IP, selecione Usar um grupo de endereços IP compartilhado especificado em um anexo entre contas.
4. Selecione uma conta que lhe dê permissão em um anexo entre contas para escolher endereços IP de um grupo de endereços IP compartilhados.
5. Em grupo de endereços IP, na lista suspensa, você pode ver os grupos de endereços IP compartilhados.

   Observe que somente os grupos de endereços IP compartilhados incluídos em um anexo entre contas que você tem permissão para usar aparecem no menu suspenso.

Responsabilidades e permissões para recursos entre contas no Global Accelerator

As seções a seguir listam as permissões que você tem como proprietário do recurso ou como entidade principal para acesso entre contas no AWS Global Accelerator.

Permissões para proprietários de recursos

Quando você, como proprietário de um recurso, autoriza as entidades principais a adicionarem recursos de sua Conta da AWS aos seus aceleradores ou a um acelerador específico, as entidades principais podem adicionar quaisquer recursos que você tenha listado no anexo entre contas.

Como proprietário do recurso, você é responsável por criar, gerenciar e excluir seus recursos. Você não pode adicionar ou remover recursos em aceleradores, a menos que tenha um perfil com autorização para fazer isso.

Se você tem um acelerador e precisa adicionar ou remover recursos entre contas, uma entidade principal pode configurar um perfil no IAM com permissão para acessar os recursos e adicionar sua conta ao perfil.

Você pode adicionar ou remover entidades principais ou recursos de um anexo entre contas para gerenciar se os recursos que você possui são usados como endpoints ou grupos de endereços IP compartilhados para aceleradores.

Permissões para entidades principais

Em geral, as entidades principais podem adicionar recursos listados em um anexo entre contas para um acelerador para o qual o anexo fornece permissão. Eles só podem visualizar, adicionar ou

remover endpoints ou selecionar endereços IP compartilhados dos grupos de endereços BYOIP para os recursos de várias contas para os quais têm permissão.

O seguinte se aplica às entidades principais:

- As entidades principais só podem visualizar, adicionar ou remover recursos como endpoints ou grupos de endereços IP compartilhados de um acelerador para o qual tenham recebido permissão em um anexo entre contas.
- As entidades principais só podem modificar recursos, como balanceadores de carga, de sua propriedade. Eles não podem modificar os recursos especificados em um anexo entre contas, porque os recursos pertencem ao proprietário do recurso.

Embora as entidades principais não possam modificar os recursos entre contas, com base em um anexo entre contas, o proprietário do recurso pode criar um perfil do IAM que proporciona a permissão para acessar o recurso. Em seguida, o proprietário pode conceder a uma entidade principal permissões para assumir o perfil, para que a entidade principal possa acessar o recurso, embora o proprietário tenha especificado isso por meio das permissões do perfil.

Custos de cobrança de recursos entre contas no Global Accelerator

O proprietário de um acelerador no AWS Global Accelerator é cobrado pelos custos associados ao acelerador. Não há custos adicionais, para proprietários de aceleradores ou proprietários de recursos, para adicionar recursos entre contas como endpoints ou como grupos de endereços traga seu próprio endereço IP (BYOIP) para um acelerador.

Para obter mais informações sobre a definição de preços, consulte Precificação para AWS Global Accelerator.

Cotas para recursos entre contas no Global Accelerator

O seguinte se aplica quando você trabalha com anexos e recursos de várias contas no AWS Global Accelerator:

- Todos os recursos entre contas e outros recursos que são adicionados como endpoints para um acelerador, incluindo recursos adicionados por todas as entidades principais com permissão entre contas, contam para as cotas vigentes para o acelerador.

- As cotas para aceleradores são aplicadas às entidades principais.
- As cotas para anexos entre contas no Global Accelerator são aplicadas aos proprietários de recursos.

Para obter mais informações sobre cotas, consulte Cotas para o AWS Global Accelerator.

Endereçamento de DNS e domínios personalizados no AWS Global Accelerator

Este capítulo explica como o AWS Global Accelerator roteia o DNS e inclui informações sobre o uso de um domínio personalizado com o Global Accelerator. Também inclui as etapas para configurar os seus endereços traga seu próprio IP (BYOIP) para uso com aceleradores no Global Accelerator.

- Endereçamento de DNS: quando você cria um acelerador, o Global Accelerator atribui um nome de Sistema de Nomes de Domínio (DNS) padrão ao seu acelerador.
- Nome de domínio personalizado: você pode configurar o DNS para usar seu nome de domínio personalizado (como `www.example.com`) com seu acelerador, em vez de usar os endereços IP estáticos atribuídos ou o nome DNS padrão.
- Endereços IP BYOIP: você pode trazer seus próprios endereços IP para a AWS adicionar a um acelerador em vez de, ou junto com, os endereços IP estáticos que o Global Accelerator atribui a você.

Conteúdo

Compatibilidade com endereçamento de DNS no AWS Global Accelerator

Quando você cria um acelerador com um tipo de endereço IP IPv4, o Global Accelerator provisiona dois endereços IPv4 estáticos para você. Também atribui um nome do Sistema de Nomes de Domínio (DNS) padrão ao acelerador, semelhante a `a1234567890abcdef.awsglobalaccelerator.com`, que aponta para os endereços IP estáticos.

Para aceleradores com tipos de endereço IP de pilha dupla, o Global Accelerator fornece um total de quatro endereços: dois endereços IPv4 estáticos e dois endereços IPv6 estáticos. O Global Accelerator cria um novo nome de DNS que aponta tanto para o registro A quanto para o registro AAAA que aponta para todos os quatro endereços IP. O novo registro de DNS

permite que o Global Accelerator atualize um acelerador para pilha dupla sem afetar os clientes que atualmente fazem referência ao registro de DNS original que não é de pilha dupla. Um exemplo de nome de DNS para um acelerador com endereços IP de pilha dupla é o seguinte: `a1234567890abcdef.dualstack.awsglobalaccelerator.com`

Os endereços estáticos são anunciados globalmente usando o anycast da rede de borda da AWS até seus endpoints. Você pode usar os endereços estáticos ou o nome de DNS do acelerador para rotear o tráfego para o acelerador. Servidores de DNS e resolvedores de DNS usam o processo DNS round-robin para resolver o nome de DNS de um acelerador, então o nome é resolvido para os endereços IP estáticos do acelerador, retornados pelo Amazon Route 53 em ordem aleatória. Os clientes geralmente usam o primeiro endereço IP retornado.

> **Note**
>
> Para cada endereço IPv4 e IPv6 associado ao seu acelerador, o Global Accelerator cria um registro Pointer (PTR) que mapeia o endereço IP estático de um acelerador para o nome de DNS correspondente gerado pelo Global Accelerator, para oferecer compatibilidade com a pesquisa reversa de DNS. Isso também é conhecido como uma zona hospedada reversa. Lembre-se de que o nome de DNS que o Global Accelerator gera para você não é configurável e você não pode criar registros PTR que apontem para seu nome de domínio personalizado. O Global Accelerator também não cria registros PTR para endereços IP estáticos de um intervalo de endereços IP que você traz para a AWS (BYOIP).

Rotear o tráfego de domínio personalizado para o seu acelerador

Na maioria dos cenários, você pode configurar o DNS para usar seu nome de domínio personalizado (como `www.example.com`) com seu acelerador, em vez de usar os endereços IP estáticos atribuídos ou o nome de DNS padrão. Primeiro, usando o Amazon Route 53 ou outro provedor de DNS, crie um nome de domínio e, em seguida, adicione ou atualize registros de DNS com seus endereços IP do Global Accelerator. Você também pode associar seu nome de domínio personalizado ao nome de DNS do seu acelerador. Conclua a configuração do DNS e aguarde que as alterações se propaguem pela Internet. Agora, quando um cliente fizer uma solicitação usando seu nome de domínio personalizado, o servidor de DNS o resolverá para os endereços IP, em ordem aleatória, ou para o nome de DNS do acelerador.

Para usar o nome de domínio personalizado com o Global Accelerator ao usar o Route 53 como serviço de DNS, crie um registro de alias que apontará o nome de domínio personalizado para o

nome de DNS atribuído ao acelerador. Um registro de alias é uma extensão do Route 53 para DNS. Ele é semelhante a um registro CNAME, mas você pode criar um registro de alias tanto para o domínio raiz, como `example.com`, quanto para subdomínios, como `www.example.com`. Para obter mais informações, consulte Escolher entre registros de alias e não alias no Guia do desenvolvedor do Amazon Route 53.

Para configurar o Route 53 com um registro de alias para um acelerador, siga as orientações incluídas no seguinte tópico: Destino do alias no Guia do desenvolvedor do Amazon Route 53. Para ver as informações do Global Accelerator, role para baixo na página Destino do alias.

Trazer seus próprios endereços IP (BYOIP) no Global Accelerator

É possível trazer parte ou todo o seu intervalo de endereços IPv4 públicos da rede on-premises para sua conta da AWS para usar com o AWS Global Accelerator. Você continua a ter os intervalos de endereços, mas a AWS os anuncia na Internet. O BYOIP com IPv6 não é compatível no momento.

O Global Accelerator usa endereços IP estáticos como pontos de entrada para seus aceleradores. Esses endereços IP são anycast a partir de locais da borda da AWS. Por padrão, o Global Accelerator fornece endereços IP estáticos do grupo de endereços IP da Amazon. Em vez de usar os endereços IP fornecidos pelo Global Accelerator, você pode configurar esses pontos de entrada para serem endereços IPv4 de seus próprios intervalos de endereços. Este tópico explica como usar seus próprios intervalos de endereços IP com o Global Accelerator.

Você não pode usar os endereços IP que você traz para a AWS para um serviço da AWS com outro serviço. As etapas nesse capítulo descrevem como trazer seu próprio intervalo de endereços IP para uso somente no AWS Global Accelerator. Para conhecer as etapas para trazer seus próprios intervalos de endereços de IP para serem usados no Amazon EC2, consulte Traga seus próprios endereços IP (BYOIP) no Guia do usuário do Amazon EC2.

> **Important**
>
> Você deve parar de anunciar seu intervalo de endereços IP em outros locais antes de anunciá-lo por meio da AWS. Se um intervalo de endereços IP tiver hospedagem múltipla (ou seja, o intervalo for anunciado por vários provedores de serviços ao mesmo tempo), não podemos garantir que o tráfego para o intervalo de endereços entrará em nossa rede ou que seu fluxo de trabalho de anúncio do BYOIP será concluído com êxito.

Depois de levar o intervalo de endereços para a AWS, ele aparece em sua conta como um grupo de endereços. Ao criar um acelerador, você pode atribuir a ele um endereço IP do seu intervalo. O Global Accelerator atribui a você um segundo endereço IP estático de um intervalo de endereços IP da Amazon. Se você trouxer dois intervalos de endereços IP para a AWS, poderá atribuir um endereço IP de cada intervalo ao seu acelerador. Essa restrição ocorre porque o Global Accelerator atribui cada intervalo de endereços a uma zona da rede diferente, para alta disponibilidade.

Para usar seu próprio intervalo de endereços IP com o Global Accelerator, revise os requisitos e siga as etapas fornecidas neste tópico.

Conteúdo

Requisitos

Você pode aumentar até dois intervalos de endereços IP qualificados para o AWS Global Accelerator por conta da AWS.

Para se qualificar, seu intervalo de endereços IP deve atender aos seguintes requisitos:

- O intervalo de endereços IP deve ser registrado com um dos seguintes registros de Internet regional (RIRs, regional internet registries): o American Registry for Internet Numbers (ARIN), o Réseaux IP Européens Network Coordination Centre (RIPE) ou o Asia-Pacific Network Information Centre (APNIC). O intervalo de endereços deve ser registrado para uma entidade empresarial ou institucional. Ele não pode ser registrado para uma pessoa física.
- O único intervalo de endereços que é possível trazer é /24. Os primeiros 24 bits do endereço IP especificam o número da rede. Por exemplo, 198.51.100 é o número da rede para o endereço IP 198.51.100.0.
- Os endereços IP no intervalo de endereços devem ter um histórico limpo. Ou seja, eles não podem ter uma reputação ruim ou estar associados a comportamentos maliciosos. Reservamo-

nos o direito de rejeitar o intervalo de endereços IP se investigarmos a reputação do intervalo de endereços IP e descobrirmos que ele contém um endereço IP que não tem um histórico limpo.

Além disso, exigimos os seguintes tipos ou status de rede de alocação e atribuição, dependendo de onde você registrou seu intervalo de endereços IP:

- ARIN: tipos de rede `Direct Allocation` e `Direct Assignment`
- RIPE: status de alocação `ALLOCATED PA`, `LEGACY` e `ASSIGNED PI`
- APNIC: status de alocação `ALLOCATED PORTABLE` e `ASSIGNED PORTABLE`

Prepare-se para levar seu intervalo de endereços IP para sua conta da AWS: autorização

Para garantir que somente você possa levar seu espaço de endereço IP para a Amazon, exigimos duas autorizações:

- Você deve autorizar a Amazon a anunciar o intervalo de endereços IP.
- Você deve fornecer prova de que possui o intervalo de endereços IP e, portanto, tem autoridade para trazê-lo para a AWS.

> **Note**
>
> Quando você usa o BYOIP para trazer um intervalo de endereços IP para a AWS, você não pode transferir a propriedade desse intervalo de endereços para uma conta ou empresa diferente enquanto o anunciamos. Você também não pode transferir diretamente um intervalo de endereços IP de uma conta da AWS para outra. Para transferir a propriedade ou transferir entre contas da AWS, você deve desprovisionar o intervalo de endereços e, em seguida, o novo proprietário deve seguir as etapas para adicionar o intervalo de endereços à conta da AWS.

Para autorizar a Amazon a anunciar o intervalo de endereços IP, você fornece à Amazon uma mensagem de autorização assinada. Use uma Autorização de Origem de Rota (ROA) para fornecer essa autorização. Uma ROA é uma declaração de criptografia sobre anúncios de sua rota que podem ser criados por meio de seu Registro Regional de Internet (RIR). Uma ROA contém o intervalo de endereços IP, os números de sistema autônomo (ASN) com permissão para anunciar

o intervalo de endereços IP e uma data de expiração. A ROA autoriza a Amazon a anunciar um intervalo de endereços IP em um Sistema Autônomo (AS) específico.

Uma ROA não autoriza sua conta da AWS a levar o intervalo de endereços IP para a AWS. Para fornecer essa autorização, você deve publicar um certificado X.509 autoassinado nas observações do protocolo de acesso de dados de registro (RDAP) para o intervalo de endereços IP. O certificado contém uma chave pública, que a AWS usa para verificar a assinatura do contexto de autorização que você fornece. Mantenha sua chave privada segura e use-a para assinar a mensagem em contexto de autorização.

As seções a seguir fornecem etapas detalhadas para concluir essas tarefas de autorização. Os comandos nestas etapas são compatíveis com o Linux. Se você usa o Windows, é possível usar o Subsistema Windows para Linux para executar comandos do Linux.

Etapas para fornecer autorização

- Etapa 1: criar um objeto ROA
- Etapa 2: Criar um certificado X.509 autoassinado
- Etapa 3: criar uma mensagem de autorização assinada

Etapa 1: criar um objeto ROA

Crie um objeto ROA para autorizar o Amazon ASNs 16509 a anunciar o intervalo de endereços IP, bem como os ASNs atualmente autorizados a anunciar o intervalo de endereços IP. A ROA deve conter o endereço IP /24 que você deseja levar para a AWS e deve definir o tamanho máximo como /24.

Para obter mais informações sobre como criar uma solicitação de ROA, consulte as seções a seguir, dependendo de onde você registrou seu intervalo de endereços IP:

- ARIN: solicitações de ROA
- RIPE: gerenciamento de ROAs
- APNIC: gerenciamento de rota

Etapa 2: Criar um certificado X.509 autoassinado

Crie um par de chaves e um certificado X.509 autoassinado e, em seguida, adicione o certificado ao registro RDAP para seu RIR. As etapas a seguir descrevem como executar essas tarefas.

> **Note**
>
> Os comandos `openssl` nessas etapas requerem o OpenSSL versão 1.0.2 ou posterior.

Para criar e adicionar um certificado X.509

1. Gere um par de chaves RSA de 2048 bits usando o comando a seguir.

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

2. Crie um certificado X.509 público a partir do par de chaves usando o seguinte comando.

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

   Neste exemplo, o certificado expira em 365 dias, após o qual ele não é mais confiável. Ao executar o comando, certifique-se de definir a opção `–days` com o valor desejado para a expiração correta. Quando forem solicitadas outras informações, você pode aceitar os valores padrão.

3. Atualize o registro RDAP para seu RIR com o certificado X.509 usando as etapas a seguir, dependendo do seu RIR.

   1. Visualize seu certificado executando o seguinte comando.

      ```
      cat publickey.cer
      ```

   2. Adicione o certificado criado anteriormente ao registro RDAP do RIR. Certifique-se de incluir as strings `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` antes e depois da parte codificada. Todo esse conteúdo deve estar em uma única e longa linha. O procedimento para atualizar o RDAP depende do RIR:

      - Para o ARIN, use o portal do Account Manager para adicionar o certificado na seção “Comentários públicos” para o objeto “Informações de rede” que representa seu intervalo de endereços. Não o adicione à seção de comentários da sua organização.
      - Para o RIPE, adicione o certificado como um novo campo “descr” ao objeto “inetnum” ou “inet6num” que representa seu intervalo de endereços. Geralmente, eles podem ser encontrados na seção “Meus recursos” do portal do banco de dados RIPE. Não o adicione à seção de comentários da sua organização ou ao campo “comentários” dos objetos acima.

- Para o APNIC, envie o certificado por e-mail para helpdesk@apnic.net para adicioná-lo manualmente ao campo “remarks” (observações) do intervalo de endereços. Envie o e-mail usando o contato autorizado do APNIC para os endereços IP.

É possível remover o certificado do seu registro do RIR após a conclusão da etapa de provisionamento abaixo.

Etapa 3: criar uma mensagem de autorização assinada

Crie uma mensagem de autorização assinada para permitir que a Amazon anuncie seu intervalo de endereços IP.

O formato da mensagem é o seguinte, em que a data YYYYMMDD é a data de expiração da mensagem.

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

Para criar uma mensagem de autorização assinada

1. Crie uma mensagem de autorização de texto não criptografado e armazene-a em uma variável chamada `text_message`, conforme mostrado no exemplo a seguir. Substitua o número de conta, o intervalo de endereços IP e a data de expiração de exemplo por seus próprios valores.

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

2. Assine a mensagem de autorização em `text_message` usando o par de chaves criado na seção anterior.
3. Armazene a mensagem em uma variável chamada `signed_message`, conforme mostrado no exemplo a seguir.

   ```
   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")
   ```

Provisionar o intervalo de endereços para uso com o Global Accelerator

Ao provisionar um intervalo de endereços para uso com a AWS, você está confirmando que é o proprietário do intervalo de endereços e autorizando a Amazon a anunciá-lo. Verificaremos se você possui o intervalo de endereços.

Você deve provisionar seu intervalo de endereços usando as operações da CLI ou da API do Global Accelerator. Essa funcionalidade não está disponível no console da AWS.

Para provisionar o intervalo de endereços, use o seguinte comando ProvisionByoipCidr. O parâmetro `--cidr-authorization-context` usa as variáveis que você criou na seção anterior, não a mensagem de ROA.

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

Veja a seguir um exemplo de provisionamento de um intervalo de endereços.

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

O provisionamento de um intervalo de endereços é uma operação assíncrona, de modo que a chamada retorna imediatamente. No entanto, o intervalo de endereços não está pronto para uso até que seu estado mude de `PENDING_PROVISIONING` para `READY`. Pode levar até 3 semanas para concluir o processo de provisionamento. Para monitorar o estado dos intervalos de endereços provisionados por você, use o seguinte comando ListByoipCidrs:

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

Para ver uma lista dos estados de um intervalo de endereços IP, consulte ByoipCidr.

Quando seu intervalo de endereços IP é provisionado, o `State` retornado por `list-byoip-cidrs` é `READY`. Por exemplo:

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

```
        }
    ]
}
```

Anunciar o intervalo de endereços por meio da AWS

Após ser provisionado, o intervalo de endereços estará pronto para ser anunciado. É necessário anunciar o intervalo de endereço exato que você provisionou. Não é possível anunciar apenas uma parte do intervalo de endereço provisionado. Além disso, você deve parar de anunciar seu intervalo de endereços IP em outros locais antes de anunciá-lo por meio da AWS.

Você deve anunciar (ou parar de anunciar) seu intervalo de endereços usando as operações da CLI ou da API Global Accelerator. Essa funcionalidade não está disponível no console da AWS.

> **Important**
>
> Certifique-se de que seu intervalo de endereços IP seja anunciado pela AWS antes de usar um endereço IP do seu grupo com o Global Accelerator.

Para anunciar o intervalo de endereços, use o seguinte comando AdvertiseByoipCidr.

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

Veja a seguir um exemplo de solicitação ao Global Accelerator para anunciar um intervalo de endereços.

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

Para monitorar o estado dos intervalos de endereços anunciados por você, use o seguinte comando ListByoipCidrs.

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

Quando seu intervalo de endereços IP é anunciado, o `State` retornado por `list-byoip-cidrs` é `ADVERTISING`. Por exemplo:

```
{
```

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

Para interromper o anúncio do intervalo de endereços, use o seguinte comando `withdraw-byoip-cidr`.

> **Important**
>
> Para parar de anunciar seu intervalo de endereços, primeiro você deve remover todos os aceleradores que tenham endereços IP estáticos alocados do grupo de endereços. Para excluir um acelerador usando o console ou usando operações de API, consulte Excluir acelerador.

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

Veja a seguir um exemplo de solicitação ao Global Accelerator para retirar um intervalo de endereços.

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

Desprovisionar o intervalo de endereços

Para interromper o uso do intervalo de endereços com a AWS, primeiro remova todos os aceleradores que tenham endereços IP estáticos alocados do grupo de endereços e interrompa o anúncio do intervalo de endereços. Depois de concluir essas etapas, você pode desprovisionar o intervalo de endereços.

Você deve parar de anunciar e desprovisionar seu intervalo de endereços usando as operações da CLI ou da API do Global Accelerator. Essa funcionalidade não está disponível no console da AWS.

Etapa 1: excluir todos os aceleradores associados.Para excluir um acelerador usando o console ou usando operações de API, consulte Excluir acelerador.

Etapa 2. Pare de anunciar o intervalo de endereços. Para interromper o anúncio do intervalo, use o seguinte comando WithdrawByoipCidr.

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

Etapa 3. Desprovisionar o intervalo de endereços. Para desprovisionar o intervalo, use o seguinte comando DeprovisionByoipCidr.

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

Use seu endereço BYOIP com um acelerador no Global Accelerator

Depois de concluir as etapas para adicionar um intervalo de endereços com BYOIP, você pode criar um acelerador com seus endereços IP BYOIP ou usar seus endereços IP BYOIP com um acelerador existente. Se você trouxe um intervalo de endereços para a AWS, você pode atribuir um endereço IP ao seu acelerador. Se você trouxe dois intervalos de endereços, você pode atribuir um endereço IP de cada intervalo de endereços ao seu acelerador.

Você também pode atualizar um acelerador existente para usar um ou mais dos seus endereços IP BYOIP. Para ter mais informações, consulte Atualize um acelerador para alterar seus endereços IP.

Outra opção é usar um endereço BYOIP compartilhado. Se um ou mais endereços CIDR adicionais tiverem sido compartilhados com você de outra conta, você poderá escolher entre um CIDR BYOIP compartilhado ao selecionar um ou ambos os endereços IP BYOIP. Observe que, se você optar por usar dois endereços BYOIP compartilhados, ambos devem vir de CIDRs pertencentes à mesma conta. Para ter mais informações, consulte Configurar o acesso entre contas no Global Accelerator.

Você tem várias opções para criar um acelerador usando seus próprios endereços IP para os endereços IP estáticos:

- Use o console do Global Accelerator para criar um acelerador. Para obter mais informações, consulte as informações a seguir.
  - Criar acelerador
  - Criar um acelerador de roteamento personalizado no Global Accelerator
  - Adicionar endpoint entre contas no AWS Global Accelerator

- Use a API do Global Accelerator para criar um acelerador. Para obter mais informações, incluindo exemplos de uso da CLI, consulte Referência da API do AWS Global Accelerator:
  - CreateAccelerator
  - CreateCustomRoutingAccelerator

Atualize um acelerador para alterar seus endereços IP

Depois de atribuir endereços BYOIP como endereços IP estáticos para um acelerador no AWS Global Accelerator, você pode atualizar o acelerador posteriormente para usar endereços IP diferentes dos seus intervalos de endereços. Você também pode atualizar um acelerador que usa seus próprios endereços IP para, em vez disso, usar os endereços IP fornecidos pelo AWS Global Accelerator.

Depois que um endereço IP estático de propriedade da Amazon for alterado, você poderá reverter para o endereço IP estático original, mas deverá fazer isso dentro de 10 dias após a alteração. Após 10 dias, o endereço IP estático original é retornado ao grupo de endereços IP da Amazon e reutilizado. Depois disso, se você atualizar seu acelerador para alterar um endereço BYOIP para um endereço IP atribuído pelo Global Accelerator, você receberá um novo endereço IP do grupo de endereços IP da Amazon. Para saber mais sobre como reverter seu endereço IP, consulte Reverter uma alteração de endereço IP estático.

As seções a seguir fornecem informações sobre como alterar endereços IP ao usar traga seu próprio endereço IP (BYOIP) com o Global Accelerator e listam os requisitos e o que você deve saber ao alterar endereços IP estáticos.

Como atualizar um acelerador para alterar um endereço IP

Para alterar um endereço IP para um acelerador, edite o acelerador e, em Endereços IP, selecione um novo endereço IP. As opções para selecionar um endereço do seu próprio grupo de endereços BYOIP ou do grupo de endereços IP da Amazon dependem do que seu acelerador já tem para endereços IP estáticos e de outros fatores.

Certifique-se de revisar os requisitos e os itens que você deve conhecer para alterar os endereços IP estáticos do acelerador antes de começar.

Os tópicos a seguir fornecem procedimentos para atualizar aceleradores.

- Use o console do Global Accelerator para atualizar um acelerador. Para obter mais informações, consulte as informações a seguir.

  - Atualizar acelerador
  - Editar um acelerador de roteamento personalizado no Global Accelerator
- Use a API do Global Accelerator para atualizar um acelerador. Para obter mais informações, incluindo exemplos de uso da CLI, consulte Referência da API do AWS Global Accelerator:
  - UpdateAccelerator
  - UpdateCustomRoutingAccelerator

Requisitos ao atualizar um acelerador para alterar endereços IP

Ao atualizar um acelerador para alterar um ou ambos os endereços IP estáticos, lembre-se do seguinte:

- Você pode alterar o endereço BYOIP para aceleradores padrão e aceleradores de roteamento personalizados. Depois de criar um acelerador com um ou dois endereços BYOIP, esse acelerador deve sempre ter pelo menos um endereço BYOIP. No entanto, você pode atualizar o acelerador para alterar um ou ambos os endereços IP estáticos, usar endereços BYOIP ou alterar o endereço BYOIP.
- Se você tiver um acelerador com dois endereços IP estáticos BYOIP, poderá alterar somente um deles para usar um endereço IP estático atribuído pelo Global Accelerator. Observe o seguinte sobre a alteração de um endereço IP estático BYOIP de um acelerador para um endereço IP estático atribuído pelo Global Accelerator:
  - Você só pode alterar o endereço de volta para um dos endereços IP estáticos originais do Global Accelerator se fizer a alteração dentro de 10 dias após a alteração para um endereço BYOIP. Após 10 dias, o endereço IP estático original é retornado ao grupo de endereços IP do Global Accelerator e reutilizado. Depois disso, se você atualizar seu acelerador para alterar um endereço BYOIP para um endereço IP atribuído pelo Global Accelerator, você receberá um novo endereço IP do grupo de endereços IP do Global Accelerator.
  - Você não pode alterar os dois endereços IP estáticos do BYOIP para usar os endereços IP estáticos do Global Accelerator. Para usar dois endereços IP estáticos atribuídos pelo Global Accelerator com um acelerador, crie um novo acelerador.
- Se você tiver um acelerador usando dois endereços BYOIP, poderá alterar qualquer um deles para um endereço BYOIP diferente. No entanto, as mesmas restrições se aplicam quando você adiciona endereços BYOIP ao criar um acelerador. Por exemplo, se você atualizar um acelerador para usar dois endereços BYOIP diferentes, os endereços devem ser de intervalos de endereços BYOIP diferentes que você adicionou ao Global Accelerator.

- Se você configurou endereços BYOIP entre contas, ao atualizar os endereços IP estáticos para um acelerador, você pode usar um endereço entre contas.
- Em um cenário específico, quando você atualiza um endereço BYOIP, o Global Accelerator pode precisar alterar seu endereço IP estático da Amazon para que possa concluir a atualização com sucesso. O endereço IP estático da Amazon só pode ser afetado quando 1) você atualiza um endereço IPv4 estático BYOIP para que seu acelerador use um endereço BYOIP de outra conta (ou seja, um endereço BYOIP entre contas) e 2) seu segundo endereço IP estático no acelerador é do grupo da Amazon.

  Se você não quiser que o endereço IP estático da Amazon mude, você pode reverter para o endereço IP anterior da Amazon, mas somente se não tiverem passado mais de 10 dias desde que você fez a atualização. Quando você reverte a alteração, o endereço IP original da Amazon é restaurado para o seu acelerador. No entanto, após 10 dias, o endereço IP da Amazon é liberado de volta para o grupo de endereços IP disponíveis e não pode ser restaurado.

Reverter uma alteração de endereço IP estático

Para reverter para o endereço IP original da Amazon para seu acelerador, faça o seguinte:

- Atualize o acelerador com o endereço IP estático BYOIP original que você alterou para um novo endereço.

Quando você fizer essa atualização, o Global Accelerator também restaurará o endereço IP estático original da Amazon.

Preservar os endereços IP do cliente no AWS Global Accelerator

Suas opções para preservar e acessar o endereço IP do cliente para o AWS Global Accelerator dependem dos endpoints que você configurou com seu acelerador. Quando a preservação do endereço IP do cliente está habilitada, o endereço IP de origem do cliente original é preservado para os pacotes que chegam ao balanceador de carga.

Os endpoints em aceleradores de roteamento personalizados sempre têm o endereço IP do cliente preservado. Há três tipos de endpoints para aceleradores padrão que podem preservar o endereço IP de origem do cliente nos pacotes recebidos: Application Load Balancers, instâncias do Amazon EC2 e Network Load Balancers com grupos de segurança. Há requisitos e limitações para recursos específicos que você adiciona como endpoint com preservação do endereço IP do cliente. Para ter mais informações, consulte Endpoints de transição com preservação do endereço IP do cliente.

Observe que o Global Accelerator não é compatível com a preservação do endereço IP do cliente para os seguintes tipos de endpoint:

- Network Load Balancer sem grupos de segurança
- Endereços IP elásticos

Para obter detalhes sobre os requisitos de endpoint, consulte Requisitos para recursos que você adiciona como endpoints do acelerador.

Conteúdo

Orientações e restrições para preservação do endereço IP do cliente no Global Accelerator

Ao se preparar e usar a preservação do endereço IP do cliente no AWS Global Accelerator, esteja ciente das orientações e restrições a seguir.

Ao planejar adicionar a preservação de endereços IP do cliente, esteja ciente do seguinte:

- Antes de adicionar e começar a rotear o tráfego para endpoints que preservam o endereço IP do cliente, certifique-se de que todas as configurações de segurança necessárias, por exemplo, grupos de segurança, estejam atualizadas para incluir o endereço IP do cliente do usuário nas listas de permissões.
- Você pode ver os endereços IP do cliente no AWS WAF, em vez dos endereços IP do Global Accelerator. Os endereços IP do cliente aparecem no AWS WAF quando você configura o Global Accelerator para preservação do endereço IP do cliente e você permite ao AWS WAF bloquear conexões dos seus Application Load Balancers que não vêm do Global Accelerator.
- A preservação do endereço IP do cliente é compatível em todas as Regiões da AWS onde o Global Accelerator é compatível. Para obter uma lista de regiões compatíveis, consulte Disponibilidade da Região da AWS para o AWS Global Accelerator.

Quando você cria um novo acelerador, a preservação do endereço IP do cliente é habilitada, por padrão, para endpoints compatíveis. O padrão para preservação do endereço IP do cliente depende do tipo de endpoint:

- Quando você usa um Application Load Balancer voltado para a Internet como um endpoint com o Global Accelerator, a preservação do endereço IP do cliente é habilitada por padrão para novos aceleradores. Você pode optar por desabilitar a opção ao criar o acelerador ou editá-lo posteriormente.
- Quando você usa um Application Load Balancer interno ou uma instância do EC2 com o Global Accelerator, o endpoint sempre tem a preservação do endereço IP do cliente habilitada.
- Quando você adiciona um Network Load Balancer com grupos de segurança como um endpoint no Global Accelerator, a preservação do endereço IP do cliente não é habilitada por padrão.

Esteja ciente do seguinte:

- Os Application Load Balancers internos e as instâncias do EC2 sempre têm a preservação do endereço IP do cliente habilitada. Você não pode desabilitar a opção para esses endpoints.
- Quando você usa o console da AWS para criar um novo acelerador, a opção de preservação do endereço IP do cliente é habilitada por padrão para endpoints do Application Load Balancer. A opção não está habilitada por padrão para o Network Load Balancer com endpoints de grupos de segurança. Você pode atualizar a opção de preservação do endereço IP do cliente para esses endpoints a qualquer momento depois de adicioná-la.
- Quando você usa a AWS CLI ou uma ação de API para criar um novo acelerador e não especifica a opção de preservação do endereço IP do cliente, a seguinte é a configuração padrão para preservação do endereço IP do cliente:
  - Os endpoints do Application Load Balancer voltados para a Internet têm a preservação do endereço IP do cliente habilitada por padrão.
  - O Network Load Balancer com endpoints de grupo de segurança não tem a preservação do endereço IP do cliente habilitada por padrão.

Para aceleradores existentes, você pode fazer a transição de endpoints sem preservação do endereço IP do cliente para endpoints que preservam o endereço IP do cliente. Por exemplo, os endpoints existentes do Application Load Balancer podem ser transferidos para novos endpoints do Application Load Balancer. Para fazer a transição para os novos endpoints, recomendamos que você mova o tráfego lentamente de um endpoint existente para um novo endpoint que tenha preservação do endereço IP do cliente, fazendo o seguinte:

- Para os endpoints existentes do Application Load Balancer ou do Network Load Balancer com grupos de segurança, primeiro adicione ao Global Accelerator um endpoint duplicado do balanceador de carga que tenha como alvo os mesmos backends e certifique-se de que a preservação do endereço IP do cliente esteja habilitada para ele. Em seguida, ajuste os pesos nos endpoints para mover lentamente o tráfego do balanceador de carga que não tem a preservação do endereço IP do cliente habilitada para o balanceador de carga com preservação do endereço IP do cliente.
- Para um endpoint de endereço IP elástico existente, você pode mover o tráfego para um endpoint de instância do EC2 com preservação do endereço IP do cliente. Primeiro, adicione um endpoint de instância do EC2 ao Global Accelerator e, em seguida, ajuste os pesos nos endpoints para mover lentamente o tráfego do endpoint de endereço IP elástico para o endpoint da instância do EC2.

Para obter orientação passo a passo sobre a transição, consulte Como fazer a transição de endpoints para usar a preservação do endereço IP do cliente.

Requisitos para endpoints com preservação do endereço IP do cliente

Há requisitos específicos para tipos de endpoints que você pode usar com a preservação do endereço IP do cliente. >Você pode usar esse atributo com endpoints que são Application Load Balancers, Network Load Balancers com grupos de segurança e instâncias do Amazon EC2, sujeito aos requisitos adicionais descritos nesta seção. Os endpoints em aceleradores de roteamento personalizados sempre têm o endereço IP do cliente preservado.

Esta seção fornece informações específicas aos endpoints que você deseja adicionar com a preservação do endereço IP do cliente habilitada. Para obter mais informações sobre os requisitos gerais para endpoints, consulte Requisitos para recursos que você adiciona como endpoints do acelerador.

Além disso, para obter mais informações sobre as práticas recomendadas de preservação do endereço IP do cliente, consulte Práticas recomendadas para ENIs e grupos de segurança com preservação do endereço IP do cliente.

Se você pretende usar o atributo de preservação do endereço IP do cliente, esteja ciente do seguinte ao adicionar endpoints ao Global Accelerator, além dos requisitos gerais para endpoints no Global Accelerator.

Endereços IP elásticos

A preservação do endereço IP do cliente não é compatível com endpoints de endereço IP elástico no Global Accelerator.

Endpoints do Network Load Balancer

Se você quiser habilitar a preservação do endereço IP do cliente ao adicionar recursos do Network Load Balancer como endpoints ao Global Accelerator, saiba que a preservação do endereço IP do cliente não é compatível com o seguinte:

- Network Load Balancer sem grupos de segurança
- Network Load Balancers com grupos de segurança que têm receptores TLS conectados
- Network Load Balancers com grupos de segurança que realizam tradução NAT de IPv4 para IPv6 para seus destinos de EC2

Além disso, para Network Load Balancer, a preservação de endereços IP do cliente é compatível somente quando os destinos estão na mesma VPC que o Network Load Balancer. O tráfego deve fluir diretamente do Network Load Balancer para o destino.

Interfaces de rede elástica

Para oferecer compatibilidade com a preservação do endereço IP do cliente, o Global Accelerator cria interfaces de rede elásticas em sua conta da AWS, uma para cada sub-rede em que um endpoint está presente. Para obter mais informações sobre como o Global Accelerator funciona com interfaces de rede elásticas, consulte Práticas recomendadas para ENIs e grupos de segurança com preservação do endereço IP do cliente.

Endpoints em sub-redes privadas

Você pode direcionar um Application Load Balancer, Network Load Balancer ou uma instância do EC2 em uma sub-rede privada usando o Global Accelerator, mas precisa ter um gateway da internet anexado à VPC que contenha os endpoints. Para ter mais informações, consulte Conexões de VPC seguras no AWS Global Accelerator.

Como prática recomendada, use sub-redes privadas se quiser garantir que o tráfego seja entregue somente pelo Global Accelerator. Além disso, certifique-se de que as regras do grupo de segurança de entrada estejam configuradas adequadamente para permitir ou negar tráfego corretamente para seus aplicativos.

Adicionar o endereço IP do cliente à lista de permissões

Antes de adicionar e começar a rotear o tráfego para endpoints que preservam o endereço IP do cliente, certifique-se de que todas as configurações de segurança necessárias, por exemplo, grupos de segurança, estejam atualizadas para incluir o endereço IP do cliente do usuário na lista de permissões. As listas de controle de acesso (ACLs) de rede só se aplicam ao tráfego de saída. Se você precisar filtrar o tráfego de entrada, deverá usar grupos de segurança.

Configurar listas de controle de acesso (ACLs) de rede

As ACLs de rede associadas às suas sub-redes VPC se aplicam ao tráfego de saída quando a preservação do endereço IP do cliente está habilitada em seu acelerador. No entanto, para que o tráfego possa sair pelo Global Accelerator, você deve configurar a ACL como uma regra de entrada e saída.

Por exemplo, para permitir que clientes TCP e UDP que usam uma porta de origem efêmera se conectem ao seu endpoint por meio do Global Accelerator, associe a sub-rede do seu endpoint

a uma Network ACL que permita tráfego de saída destinado a uma porta TCP ou UDP efêmera (intervalo de portas 1024 a 65535, destino 0.0.0.0/0). Além disso, crie uma regra de entrada correspondente (intervalo de portas 1024 a 65535, fonte 0.0.0.0/0).

Esteja ciente do seguinte para grupos de segurança e WAF:

- O grupo de segurança e as regras do AWS WAF são um conjunto adicional de recursos que você pode aplicar para proteger seus recursos. Por exemplo, as regras do grupo de segurança de entrada associadas às suas instâncias do Amazon EC2 e aos Application Load Balancers permitem que você controle as portas de destino às quais os clientes podem se conectar por meio do Global Accelerator, como a porta 80 para HTTP ou a porta 443 para HTTPS.
- Os grupos de segurança de instâncias do Amazon EC2 se aplicam a qualquer tráfego que chega às suas instâncias, incluindo tráfego do Global Accelerator e qualquer endereço IP público ou elástico atribuído à sua instância.

Como o endereço IP do cliente é preservado no AWS Global Accelerator

O AWS Global Accelerator preserva o endereço IP de origem do cliente de forma diferente para instâncias do Amazon EC2, Network Load Balancers e Application Load Balancers:

- Para um endpoint de instância do EC2, o endereço IP do cliente é preservado para todo o tráfego.
- Para um endpoint do Network Load Balancer com preservação do endereço IP do cliente, o Global Accelerator trabalha em conjunto com o Network Load Balancer para incluir o endereço IP do cliente original no cabeçalho IP do pacote para que seu aplicativo possa acessá-lo.
- Para um endpoint do Application Load Balancer com preservação do endereço IP do cliente, o Global Accelerator trabalha em conjunto com o Application Load Balancer para fornecer um cabeçalho `X-Forwarded`, `X-Forwarded-For`, que inclui o endereço IP do cliente original para que sua camada da Web possa acessá-lo.

As solicitações HTTP e as respostas HTTP usam campos de cabeçalho para enviar informações sobre as mensagens HTTP. Os campos de cabeçalho são pares de nome-valor separados por dois pontos e separados por um retorno de carro (CR) e um avanço de linha (LF). Um conjunto padrão de campos de cabeçalho HTTP está definido na RFC 2616, Cabeçalhos de mensagem. Há também cabeçalhos HTTP não padrão que são amplamente usados pelos aplicativos. Alguns dos cabeçalhos HTTP não padrão possuem um prefixo `X-Forwarded`.

Como um Application Load Balancer encerra as conexões TCP de entrada e cria novas conexões com seus destinos de backend, ele não preserva os endereços IP do cliente até o código de destino (como instâncias, contêineres ou código Lambda). O endereço IP de origem que seus destinos veem no pacote TCP é o endereço IP do Application Load Balancer. No entanto, um Application Load Balancer preserva o endereço IP original do cliente removendo-o do endereço de resposta do pacote original e inserindo-o em um cabeçalho HTTP antes de enviar a solicitação ao seu backend por meio de uma nova conexão TCP.

O cabeçalho da solicitação `X-Forwarded-For` é formatado da seguinte maneira:

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

O exemplo a seguir mostra um cabeçalho de solicitação `X-Forwarded-For` para um cliente com o endereço IP 203.0.113.7.

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

O exemplo a seguir mostra um cabeçalho de solicitação `X-Forwarded-For` para um cliente com um endereço IPv6 de 2001:DB8::21f:5bff:febf:ce22:8a2e.

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

Benefícios da preservação de endereços IP do cliente

Você pode configurar a preservação do endereço IP do cliente para endpoints específicos no Global Accelerator. Para alguns aplicativos com os quais você configura o AWS Global Accelerator, talvez você queira acessar o endereço IP original do cliente usando endpoints com preservação do endereço IP do cliente.

Por exemplo, quando você tem o endereço IP do cliente, pode coletar estatísticas com base nos endereços IP do cliente. Você também pode usar filtros baseados em endereço IP, como grupos de segurança em Application Load Balancers, para filtrar o tráfego. Você pode aplicar uma lógica específica ao endereço IP de um usuário em seus aplicativos que são executados nos servidores de camada da Web por trás desse endpoint do Application Load Balancer usando o cabeçalho `X-Forwarded-For` do balanceador de carga, que contém as informações originais do endereço IP do cliente. Você também pode usar a preservação de endereços IP do cliente nas regras de grupos

de segurança nos grupos de segurança associados ao Application Load Balancer ou ao Network Load Balancer. Para ter mais informações, consulte Como o endereço IP do cliente é preservado no AWS Global Accelerator. Para endpoints de instâncias do EC2, o endereço IP original do cliente é preservado.

Para endpoints que não têm a preservação do endereço IP do cliente habilitada, os endereços IP usados pelo serviço Global Accelerator na rede de borda substituem o endereço IP do usuário solicitante como endereço de origem nos pacotes que chegam. As informações de conexão do cliente original, como o endereço IP do cliente e a porta do cliente, não são preservadas à medida que o tráfego viaja para os sistemas atrás de um acelerador. Isso funciona bem para muitos aplicativos, especialmente aqueles que estão disponíveis para todos os usuários, como sites públicos.

Para endpoints que não têm preservação do endereço IP do cliente, você pode filtrar o endereço IP de origem que o Global Accelerator usa ao encaminhar o tráfego da borda. Você pode ver informações sobre os endereços IP de origem (que também são endereços IP do cliente, quando a preservação do endereço IP do cliente está habilitada) dos pacotes recebidos revisando seus logs de fluxo do Global Accelerator. Para ter mais informações, consulte Localização e intervalos de endereços IP dos servidores de borda do Global Accelerator e Como configurar e usar logs de fluxo no AWS Global Accelerator.

Práticas recomendadas para ENIs e grupos de segurança com preservação do endereço IP do cliente

Ao usar a preservação do endereço IP do cliente no AWS Global Accelerator, lembre-se das informações e das práticas recomendadas nesta seção para interfaces de rede elásticas (ENIs) e grupos de segurança.

Para oferecer compatibilidade com a preservação do endereço IP do cliente, o Global Accelerator cria interfaces de rede elásticas em sua conta da AWS, uma para cada sub-rede em que um endpoint está presente. Uma interface de rede elástica é um componente lógico de redes em uma VPC que representa uma cartão de rede virtual. O Global Accelerator usa essas interfaces de rede elásticas para rotear o tráfego para os endpoints configurados por trás de um acelerador. Os endpoints compatíveis para rotear o tráfego dessa forma são Application Load Balancers (internos e voltados para a Internet), Network Load Balancers com grupos de segurança e instâncias do Amazon EC2.

> **Note**
>
> Ao adicionar um Application Load Balancer interno ou um endpoint de instância do EC2 no Global Accelerator, você permite que o tráfego da Internet flua diretamente de e para o endpoint em nuvens privadas virtuais (VPCs), direcionando-o para uma sub-rede privada. Para ter mais informações, consulte Conexões de VPC seguras no AWS Global Accelerator.

Como o Global Accelerator usa interfaces de rede elásticas

Quando você tem um endpoint do Application Load Balancer ou do Network Load Balancer com a preservação do endereço IP do cliente habilitada, o número de sub-redes em que o balanceador de carga está determina o número de interfaces de rede elásticas que o Global Accelerator cria em sua conta. O Global Accelerator cria uma interface de rede elástica para cada sub-rede que tem pelo menos uma interface de rede elástica do Application Load Balancer ou do Network Load Balancer, liderada por um acelerador em sua conta.

Os seguintes exemplos mostram como isso funciona:

- Exemplo 1: se um Application Load Balancer tiver interfaces de rede elásticas na sub-rede A e na sub-rede B e você adicionar o balanceador de carga como um endpoint do acelerador, o Global Accelerator cria duas interfaces de rede elásticas, uma em cada sub-rede.
- Exemplo 2: se você adicionar, por exemplo, um ALB1 que tenha interfaces de rede elásticas na sub-rede A e sub-rede B ao Acelerador1 e, em seguida, adicionar um ALB2 com interfaces de rede elásticas na sub-rede A e a sub-rede B ao Acelerador2, o Global Accelerator cria somente duas interfaces de rede elásticas: uma na sub-rede A e outra na sub-rede B.
- Exemplo 3: se você adicionar um ALB1 que tenha interfaces de rede elásticas na sub-rede A e sub-rede B ao Acelerador1 e, em seguida, adicionar um ALB2 com interfaces de rede elásticas na sub-rede A e sub-rede C ao Acelerador2, o Global Accelerator cria três interfaces de rede elásticas: uma na sub-rede A, uma na sub-rede B e uma na sub-rede C. A interface de rede elástica na sub-rede A fornece tráfego para o Acelerador1 e o Acelerador2.

Conforme mostrado no Exemplo 3, as interfaces de rede elásticas são reutilizadas nos aceleradores se os endpoints na mesma sub-rede forem colocados atrás de vários aceleradores.

As interfaces de rede elásticas lógicas que o Global Accelerator cria não representam um único host, um gargalo de throughput ou um único ponto de falha. Como outros serviços da AWS que aparecem como uma única interface de rede elástica em uma zona de disponibilidade ou sub-

rede (serviços como um gateway de conversão de endereços de rede (NAT) ou um Network Load Balancer) o Global Accelerator é implementado como um serviço altamente disponível e escalado horizontalmente.

Avalie o número de sub-redes usadas pelos endpoints em seus aceleradores para determinar o número de interfaces de rede elásticas que o Global Accelerator criará. Antes de criar um acelerador, verifique se você tem capacidade de espaço de endereço IP suficiente para as interfaces de rede elásticas necessárias, ou seja, pelo menos um endereço IP livre por sub-rede relevante. Se você não tiver espaço de endereço IP livre suficiente, deverá criar ou usar uma sub-rede que tenha espaço de endereço IP livre adequado para seu Application Load Balancer ou Network Load Balancer e as interfaces de rede elásticas associadas do Global Accelerator.

Quando o Global Accelerator determina que uma interface de rede elástica não está sendo usada por nenhum dos endpoints nos aceleradores da sua conta, o Global Accelerator exclui a interface.

Grupos de segurança criados pelo Global Accelerator

Analise as informações e as práticas recomendadas a seguir ao trabalhar com o Global Accelerator e grupos de segurança.

- Você pode usar os grupos de segurança criados pelo Global Accelerator como um grupo de origem em outros grupos de segurança que você mantém, mas o Global Accelerator só encaminha o tráfego para os destinos que você especifica em sua VPC.
- Se você modificar as regras do grupo de segurança criadas pelo Global Accelerator, o endpoint poderá ficar não íntegro. Se isso acontecer, entre em contato com o Suporte da AWS para obter ajuda.
- O Global Accelerator cria um grupo de segurança específico para cada VPC. Todas as interfaces de rede elásticas criadas para os endpoints em uma VPC específica usam o mesmo grupo de segurança, independentemente da sub-rede à qual uma interface de rede elástica esteja associada.

> **Important**
>
> O Global Accelerator cria grupos de segurança associados a interfaces de rede elásticas. Embora o sistema não impeça você de fazer isso, você não deve editar nenhuma das configurações do grupo de segurança desses grupos.

Endpoints de transição com preservação do endereço IP do cliente

Se você ainda não configurou a preservação do endereço IP do cliente para os endpoints em seu acelerador, siga as orientações nesta seção para adicionar e fazer a transição de um ou mais endpoints para endpoints que preservam o endereço IP do cliente do usuário. Você pode optar por fazer a transição de um Application Load Balancer, um Network Load Balancer com grupos de segurança ou um endpoint de endereço IP elástico para um endpoint correspondente (um endpoint de balanceador de carga correspondente ou um endpoint de instância do EC2) que tenha preservação do endereço IP do cliente.

Esta seção explica como adicionar e fazer a transição de endpoints usando o console do AWS Global Accelerator. Se você quiser usar operações de API com o Global Accelerator, consulte a Referência da API do AWS Global Accelerator.

Como fazer a transição de endpoints para usar a preservação do endereço IP do cliente

Recomendamos que você faça a transição dos endpoints para usar lentamente a preservação do endereço IP do cliente.

- Adicione o novo endpoint: primeiro, adicione ao Global Accelerator o novo balanceador de carga ou endpoints da instância do EC2 que você habilita para preservar o endereço IP do cliente.
- Aumente lentamente o tráfego: em seguida, mova lentamente o tráfego dos endpoints existentes para os novos endpoints configurando pesos nos endpoints.
- Teste conforme avança: depois de mover uma pequena quantidade de tráfego para o novo endpoint com a preservação do endereço IP do cliente, teste para garantir que sua configuração esteja funcionando conforme o esperado. Em seguida, aumente gradualmente a proporção de tráfego para o novo endpoint ajustando os pesos nos endpoints correspondentes.

Siga as etapas nas seguintes seções para fazer a transição de endpoints.

A preservação do endereço IP do cliente é compatível em todas as Regiões da AWS onde o Global Accelerator é compatível. Para obter uma lista de regiões compatíveis, consulte Disponibilidade da Região da AWS para o AWS Global Accelerator.

> **Important**
>
> Antes de começar a rotear o tráfego para endpoints que preservam o endereço IP do cliente, certifique-se de que todas as configurações nas quais você incluiu os endereços IP do cliente do Global Accelerator nas listas de permissões sejam atualizadas para incluir o endereço IP do cliente do usuário.

Para adicionar um endpoint com preservação do endereço IP do cliente

1. Abra o console do Global Accelerator em https://console.aws.amazon.com/globalaccelerator/home.
2. Na página Aceleradores, escolha um acelerador.
3. Na seção Receptores, escolha um receptor.
4. Na seção Grupo de endpoints, escolha um grupo de endpoints.
5. Na seção Endpoints, escolha Adicionar endpoint.
6. Na página Adicionar endpoints, no menu suspenso Endpoints, escolha um endpoint que seja compatível com a preservação do endereço IP do cliente.
7. No campo Peso, escolha um número baixo em comparação com os pesos definidos para seus endpoints existentes. Por exemplo, se o peso de um Application Load Balancer correspondente for 255, você poderá inserir um peso de 5 para o novo Application Load Balancer, para começar. Para ter mais informações, consulte Como os pesos dos endpoints funcionam para gerenciar o volume de tráfego.
8. Se necessário, em Preservar endereço IP do cliente, selecione Preservar endereço.
9. Escolha Salvar alterações.

Em seguida, siga as etapas incluídas aqui para editar os endpoints existentes correspondentes (que você está substituindo pelos novos endpoints com preservação do endereço IP do cliente) para reduzir os pesos dos endpoints existentes para que menos tráfego vá para eles.

Para reduzir o tráfego para os endpoints existentes

1. Na página do Grupo de endpoints, escolha um endpoint existente que não tenha preservação do endereço IP do cliente.
2. Selecione a opção Editar.

3. Na página Editar endpoint, no campo Peso, insira um número menor do que o número atual. Por exemplo, se o peso de um endpoint existente for 255, você poderá inserir um peso de 220 para o novo endpoint (com preservação do endereço IP do cliente).
4. Escolha Salvar alterações.

Depois de testar com uma pequena parte do tráfego original, definindo o peso do novo endpoint para um número baixo, você pode fazer lentamente a transição de todo o tráfego continuando a ajustar os pesos do endpoint original e do novo.

Por exemplo, digamos que você comece com um Application Load Balancer existente com um peso definido como 200 e adicione um novo endpoint do Application Load Balancer com a preservação do endereço IP do cliente habilitada com um peso definido como 5. Mude gradualmente o tráfego do Application Load Balancer original para o novo Application Load Balancer aumentando o peso do novo Application Load Balancer e diminuindo o peso do Application Load Balancer original. Por exemplo:

- Peso original 190/peso novo 10
- Peso original 180/peso novo 20
- Peso original 170/peso novo 30 e assim por diante.

Quando você diminui o peso do endpoint original para 0, todo o tráfego (neste exemplo) vai para o novo endpoint do Application Load Balancer, que inclui a preservação do endereço IP do cliente.

Se você tiver endpoints adicionais (balanceadores de carga ou instâncias do EC2) que deseja transicionar para usar a preservação do endereço IP do cliente, repita as etapas desta seção para fazer a transição.

Se precisar reverter a configuração de um endpoint para que o tráfego para o endpoint não preserve o endereço IP do cliente, você pode fazer isso a qualquer momento: aumente o peso do endpoint que não tem preservação do endereço IP do cliente para o valor original e diminua o peso do endpoint com a preservação do endereço IP do cliente para 0.

Registrar em log e monitorar no AWS Global Accelerator

Você pode usar o Amazon CloudWatch, os logs de fluxo e o AWS CloudTrail para monitorar seu acelerador no AWS Global Accelerator. Por exemplo, você pode solucionar problemas com seus receptores e endpoints, analisar padrões de tráfego e obter as informações necessárias para auditorias.

Esses métodos de registro de logs e monitoramento podem ter alguma sobreposição. A seguir estão os usos típicos de cada método:

- As métricas do CloudWatch fornecem informações em tempo real, sem configuração adicional, que podem ajudar você a solucionar problemas de configuração. Você também pode criar alarmes para alertar, por exemplo, quando houver problemas de produção.
- Os logs de fluxo fornecem informações detalhadas sobre o tráfego que entra em um acelerador e retorna aos clientes. Os logs de fluxo são úteis para solucionar problemas de acessibilidade e fornecer informações para auditorias abrangentes. (Observe que os logs de fluxo exigem configuração e uso do armazenamento do Amazon S3).
- O CloudTrail rastreia automaticamente as ações que você realiza, chamadas de APIs do Global Accelerator, que podem ser úteis para auditorias, por exemplo.

> **Note**
>
> Você deve visualizar as métricas e os registros do CloudWatch para o Global Accelerator na região Oeste dos EUA (Oregon), tanto no console quanto ao usar a AWS CLI. Ao usar a AWS CLI, especifique a região Oeste dos EUA (Oregon) para seu comando incluindo o seguinte parâmetro: `--region us-west-2`.

Tópicos

Como usar Amazon CloudWatch com o AWS Global Accelerator

O AWS Global Accelerator publica pontos de dados no Amazon CloudWatch para seus aceleradores. O CloudWatch permite recuperar estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecidos como métricas. Considere uma métrica como uma variável a ser monitorada, e os pontos de dados como os valores dessa variável ao longo do tempo. Por exemplo, você pode monitorar o tráfego em um acelerador durante um período especificado. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

> **Note**
>
> Você deve visualizar as métricas e os registros do CloudWatch para o Global Accelerator na região Oeste dos EUA (Oregon), tanto no console quanto ao usar a AWS CLI. Ao usar a AWS CLI, especifique a região Oeste dos EUA (Oregon) para seu comando incluindo o seguinte parâmetro: `--region us-west-2`.

Você pode usar métricas para solucionar problemas de uma configuração inicial do Global Accelerator, para ajudar a determinar se o tráfego está chegando a um endpoint e, em seguida, as respostas estão retornando. Veja as métricas do CloudWatch, que são registradas automaticamente, para ver se o tráfego está chegando aos seus endpoints, como um Network Load Balancer. Deve haver métricas para saída do Global Accelerator para os endpoints e, em seguida, do Global Accelerator para o cliente, e o mesmo para um endpoint, como um balanceador de carga. O tráfego que entra do Global Accelerator, mas não retorna ou não atinge o balanceador de carga, pode indicar que você precisa verificar se sua configuração permite que o tráfego flua pelas portas esperadas e se as configurações do grupo de segurança permitem acesso.

Você também pode usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um alarme do CloudWatch para monitorar uma métrica específica e depois realizar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica sair do que você considera um intervalo aceitável.

O Global Accelerator relata métricas para o CloudWatch somente quando as solicitações fluem pelo acelerador. Se as solicitações estão passando pelo acelerador, o Global Accelerator mede e envia suas métricas em intervalos de 60 segundos. Se não há solicitações passando pelo acelerador ou não há dados para uma métrica, a métrica não é relatada.

Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch.

Conteúdo

Métricas do Global Accelerator

O namespace `AWS/GlobalAccelerator` inclui as métricas a seguir.

Métrica	Descrição
`ActiveFlowCount`	O número total de conexões TCP e UDP simultâneas de clientes a endpoints para um acelerador no Global Accelerator. Para conexões TCP que são encerradas no acelerador, um cliente que abre uma conexão TCP com um endpoint conta como um único fluxo. Você pode usar essa métrica para entender melhor quantos usuários ativos (contagem de conexões) estão acessando um endpoint ou para determinar se seus recursos precisam ser escalados para lidar com o tráfego. Critérios de relatório: relatados para aceleradores configurados e habilitados. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge`

Métrica	Descrição
	• `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`
`Flows_Dropped_No_Endpoint_Found`	O número total de fluxos de pacotes TCP IPv6 que foram descartados porque nenhum endpoint IPv6 estava disponível. Isso poderia acontecer, por exemplo, se você tivesse um acelerador com um tipo de endereço IP de pilha dupla e alterasse o tipo de endereço IP para IPv4 para um endpoint do acelerador. Critérios de relatório: relatados para aceleradores com tipos de endereço IP de pilha dupla que estão recebendo tráfego IPv6 quando ocorre uma das seguintes situações: • Um acelerador com endpoints IPv6 servindo relatórios de tráfego com uma métrica 0 • Um acelerador com endpoints mal configurados relata o número total de fluxos descartados Estatísticas: a estatística mais útil é `Sum`. Dimensões • `Accelerator` • `Accelerator, Listener` • `Accelerator, AcceleratorIPAddress`

Métrica	Descrição
`HealthyEndpointCount`	O número total de endpoints considerados íntegros. O Global Accelerator verifica regularmente o status dos endpoints nos aceleradores padrão. Essas verificações de integridade são executadas automaticamente. Como e quando essas verificações de integridade são executadas depende do tipo de endpoint e das opções de verificação de integridade do endpoint. Para saber mais, consulte Garantir acesso à verificação de integridade do seu acelerador. Critérios de relatório: relatados para aceleradores configurados e habilitados. Estatísticas: as estatísticas mais úteis são `Minimum` e `Maximum`. Dimensões • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup`

Métrica	Descrição
NewFlowCount	O número total de novos fluxos (ou conexões) TCP e UDP estabelecidos dos clientes para os endpoints no período. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress • Accelerator, NetworkProtocol

Métrica	Descrição
`ProcessedBytesIn`	O número total de bytes de entrada processados pelo acelerador, incluindo cabeçalhos TCP/IP. Essa contagem inclui todo o tráfego para endpoints. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress` • `Accelerator, NetworkProtocol`

Métrica	Descrição
`ProcessedBytesOut`	O número total de bytes de saída processados pelo acelerador, incluindo cabeçalhos TCP/IP. Essa contagem inclui o tráfego de endpoints, menos o tráfego de verificação de integridade. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress` • `Accelerator, NetworkProtocol`

Métrica	Descrição
PacketsProcessed	O número total de pacotes processados pelo Global Accelerator para um acelerador, incluindo tráfego de e para endpoints, incluindo tráfego de verificação de integridade. Essa métrica pode ajudar você a comparar os volumes de tráfego em um período específico. Critérios de relatório: relatados para aceleradores configurados e habilitados. Estatísticas: a estatística mais útil é Sum. Dimensões • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress

Métrica	Descrição
`UnhealthyEndpointCount`	O número total de endpoints considerados sem integridade. O Global Accelerator verifica regularmente o status dos endpoints nos aceleradores padrão. Essas verificações de integridade são executadas automaticamente. Como e quando essas verificações de integridade são executadas depende do tipo de endpoint e das opções de verificação de integridade do endpoint. Para saber mais, consulte Garantir acesso à verificação de integridade do seu acelerador. Critérios de relatório: relatados para aceleradores configurados e habilitados. Estatísticas: as estatísticas mais úteis são `Minimum` e `Maximum`. Dimensões • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup`

Métrica	Descrição
`TCP_AGA_Reset_Count`	O número total de pacotes de redefinição (RST) gerados pelo AWS Global Accelerator (“AGA”). Usando essa métrica, você pode determinar se o Global Accelerator está encerrando as conexões do cliente e enviando redefinições de volta ao endpoint do cliente. Para obter mais informações sobre como avaliar e solucionar problemas de TCP RST gerado pelo Global Accelerator, consulte Solução de problemas de redefinição TCP do Global Accelerator. Critérios de relatório: relatados quando há tráfego e há um valor diferente de zero. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, AcceleratorIPAddress`

Métrica	Descrição
`TCP_Client_Reset_Count`	O número total de pacotes de redefinição (RST) enviados de um cliente para um endpoint. Ao usar essa métrica, você pode determinar se um cliente pode manter uma conexão aberta com o Global Accelerator ou se a conexão é redefinida inesperadamente cedo. Isso é útil, por exemplo, quando você configura o Global Accelerator inicialmente e para visibilidade quando você faz uma alteração nos clientes que criam redefinições de conexão. Para obter mais informações sobre como avaliar e solucionar problemas de TCP RST gerado pelo Global Accelerator, consulte Solução de problemas de redefinição TCP do Global Accelerator. Critérios de relatório: relatados quando há tráfego e há um valor diferente de zero. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, AcceleratorIPAddress`

Métrica	Descrição
`TCP_Endpoint_Reset_Count`	O número total de pacotes de redefinição (RST) enviados de um endpoint para um cliente. O uso dessa métrica pode ajudar você a determinar quando os endpoints do seu cliente estão sobrecarregados. Para obter mais informações sobre como avaliar e solucionar problemas de TCP RST gerado pelo Global Accelerator, consulte Solução de problemas de redefinição TCP do Global Accelerator. Critérios de relatório: relatados quando há tráfego e há um valor diferente de zero. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, AcceleratorIPAddress`

Dimensões de métricas para aceleradores

Para filtrar as métricas do acelerador, use as dimensões a seguir.

Dimensão	Descrição
`Accelerator`	Filtra os dados de métrica por acelerador. Especifique o acelerador pelo ID do acelerador (a parte final do ARN do acelerador). Por exemplo, se o ARN for `arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234a`

Dimensão	Descrição
	`bcdefgh` , você especifica o seguinte: **`1234abcd-abcd-1234-abcd-1234abcdefgh`** .
`Listener`	Filtra os dados de métrica por receptor. Especifique o receptor pelo ID do receptor (a parte final do ARN do receptor). Por exemplo, se o ARN for `arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123wxyz` , você especifica o seguinte: **`0123wxyz`**.
`EndpointGroup`	Filtra os dados de métrica por grupo de endpoints. Especifique o grupo de endpoints por região da AWS, por exemplo, **`us-east-1`** (tudo em minúsculas).
`SourceRegion`	Filtra os dados de métrica por região de origem, que é a área geográfica das regiões da AWS em que os endpoints do seu aplicativo estão sendo executados. A região de origem é uma das seguintes: • NA: Estados Unidos e Canadá • EU: Europa • AP: Ásia-Pacífico* • KR: Coreia do Sul • IN: Índia • AU: Austrália • OM: Oriente Médio • SA: América do Sul • ZA: África do Sul *Exceto Coreia do Sul e Índia

Dimensão	Descrição
`DestinationEdge`	Filtra os dados de métrica por borda de destino, que é a área geográfica dos locais de borda da AWS que atendem ao tráfego de seus clientes. A borda de destino é uma das seguintes: • NA: Estados Unidos e Canadá • EU: Europa • AP: Ásia-Pacífico* • KR: Coreia do Sul • IN: Índia • AU: Austrália • OM: Oriente Médio • SA: América do Sul • ZA: África do Sul *Exceto Coreia do Sul e Índia
`TransportProtocol`	Filtra os dados de métrica por protocolo de transporte: UDP ou TCP.
`AcceleratorIPAddress`	Filtra os dados de métrica por endereço IP do acelerador: ou seja, um dos endereços IP estáticos atribuídos a um acelerador.

Solução de problemas de redefinição TCP do Global Accelerator

Cada acelerador relata o número de redefinições TCP (TCP RSTs) que foram geradas e enviadas do Global Accelerator. Os motivos comuns pelos quais o Global Accelerator envia uma redefinição TCP são os seguintes:

- O Global Accelerator marca uma conexão TCP como fechada quando o cliente ou o endpoint fecha a conexão, usando o handshake FIN ou a redefinição. Se o cliente ou o endpoint enviar pacotes de dados em uma conexão TCP fechada, o Global Accelerator gerará uma redefinição TCP para indicar que a conexão está fechada e não pode aceitar tráfego.

- Se um cliente ou endpoint envia dados depois do tempo limite de inatividade, ele recebe um pacote de redefinição TCP do Global Accelerator para indicar que a conexão não é mais válida.
- Se o Global Accelerator receber um pacote inesperado ao criar a conexão com o cliente ou o endpoint durante o handshake TCP, o Global Accelerator gerará uma redefinição TCP.

Se você vê um número estável de métricas `AGA_Reset_Count` para um acelerador, isso ocorre porque o cliente ou o endpoint enviou dados para o Global Accelerator a uma conexão fechada ou expirada.

Se você notar um aumento acentuado nas métricas `AGA_Reset_Count` e o aumento estiver alinhado às mudanças de métricas relacionadas no lado do endpoint, como aumentar ou reduzir a escala verticalmente, ou um endpoint com problemas de integridade, o endpoint pode ter ficado inacessível e acionado a redefinição TCP do Global Accelerator. Para obter ajuda na investigação desse problema, entre em contato com o suporte da AWS.

Estatísticas das métricas do Global Accelerator

O CloudWatch fornece estatísticas com base nos pontos de dados da métrica publicados pelo Global Accelerator. As estatísticas são agregações de dados de métrica ao longo de um período especificado. Quando você solicita estatísticas, o fluxo de dados apresentado é identificado pelo nome da métrica e pela dimensão. Dimensão é um par de nome/valor que identifica exclusivamente uma métrica. Por exemplo, você pode solicitar os bytes processados para um acelerador em que os bytes são servidos a partir de locais da borda da AWS na Europa (a borda de destino é “EU”).

Veja a seguir exemplos de combinações de métrica/dimensão que podem ser úteis:

- Visualize a quantidade de tráfego veiculada (como ProcesssedBytesOut) por cada um dos dois endereços IP do acelerador para validar se a configuração de DNS está correta.
- Visualize a distribuição geográfica do seu tráfego de usuários e monitore quanto dele é local (por exemplo, da América do Norte para a América do Norte) ou global (por exemplo, da Austrália ou da Índia para a América do Norte). Para determinar isso, visualize as métricas ProcessedBytesIn ou ProcessedBytesOut com as dimensões DestinationEdge e SourceRegion definidas com valores específicos.
- Visualize o número de endpoints não íntegros em seu acelerador e determine a quais grupos de endpoints eles pertencem. Se você tiver um grande número de grupos de endpoints, isso é especialmente útil para ajudá-lo a encontrar rapidamente grupos de endpoints com endpoints que

estão enfrentando problemas. Para determinar isso, visualize a métrica UnhealthyEndpointCount com as dimensões Accelerator, Listener e EndpointGroup.

Visualizar métricas do CloudWatch para seus aceleradores

Você pode visualizar as métricas do CloudWatch para seus aceleradores usando o console do CloudWatch ou a AWS CLI. No console, essas métricas são exibidas como gráficos de monitoramento. Os gráficos de monitoramento mostram pontos de dados apenas se o acelerador estiver ativo e recebendo solicitações.

Você deve visualizar as métricas do CloudWatch para o Global Accelerator na região Oeste dos EUA (Oregon), tanto no console quanto ao usar a AWS CLI. Ao usar a AWS CLI, especifique a região Oeste dos EUA (Oregon) para seu comando incluindo o seguinte parâmetro: `--region us-west-2`.

Para visualizar métricas usando o console do CloudWatch, siga as etapas no Guia do usuário do Amazon CloudWatch e selecione o namespace do GlobalAccelerator. Para saber mais, consulte Visualizar métricas disponíveis.

Para obter as estatísticas de uma métrica usando a AWS CLI

Use o comando get-metric-statistics para obter estatísticas para a métrica e a dimensão especificadas. Observe que o CloudWatch trata cada combinação única de dimensões como uma métrica distinta. Não é possível recuperar estatísticas usando combinações de dimensões que não tenham sido especificamente publicadas. Você deve especificar as mesmas dimensões usadas ao criar as métricas.

O exemplo a seguir lista o total de bytes processados, por minuto, para o acelerador que opera a partir da borda de destino da América do Norte (NA).

```
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
```

A seguir está um exemplo de saída do comando:

```
{
    "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"
        }
```

```
    ]
}
```

Como configurar e usar logs de fluxo no AWS Global Accelerator

Os logs de fluxo permitem que você capture informações sobre o tráfego do endereço IP que percorre as interfaces de rede em seu acelerador no AWS Global Accelerator. Os dados do log de fluxo são publicados no Amazon S3, de onde é possível recuperá-los e visualizá-los depois de criar um log de fluxo.

> **Note**
>
> Você deve visualizar as métricas e os registros do CloudWatch para o Global Accelerator na região Oeste dos EUA (Oregon), tanto no console quanto ao usar a AWS CLI. Ao usar a AWS CLI, especifique a região Oeste dos EUA (Oregon) para seu comando incluindo o seguinte parâmetro: `--region us-west-2`.

Os logs de fluxo podem ajudar em diversas tarefas. Por exemplo, você pode solucionar o motivo pelo qual um tráfego específico não está chegando a um endpoint, o que, por sua vez, ajuda a diagnosticar regras de grupos de segurança extremamente restritivas. Além disso, você pode usar os logs de fluxo como ferramenta de segurança para monitorar o tráfego que está chegando aos seus endpoints.

Um registro de log de fluxo representa um fluxo de rede em seu log de fluxo. Todo registro captura o fluxo de rede para um 5-tuple específico e uma janela de captura específica. Um 5-tuple é um conjunto de cinco valores diferentes que especificam a origem, o destino e o protocolo para um fluxo de IP. A janela de captura é um espaço de tempo durante o qual o serviço de logs de fluxo agrega dados, antes de publicar os registros de log de fluxo. A janela de captura é de até 1 minuto. Ou seja, os logs podem ser publicados com mais frequência do que a cada minuto, mas serão publicados pelo menos a cada minuto.

As cobranças do CloudWatch Logs se aplicam ao usar logs de fluxo, mesmo quando os logs são publicados diretamente no Amazon S3. Para obter mais informações, consulte Logs fornecidos na guia Logs em Preços do Amazon CloudWatch.

> **Tip**
>
> Usar o Amazon Athena e o Amazon QuickSight com seus dados de log de fluxo do Global Accelerator pode ajudar você a solucionar problemas de acessibilidade do seu aplicativo, identificar vulnerabilidades de segurança e obter uma visão geral de como os usuários acessam seu aplicativo. Para saber mais, consulte a seguinte postagem no blog da AWS: Análise e visualização de logs de fluxo do AWS Global Accelerator usando o Amazon Athena e o Amazon QuickSight.

Conteúdo

Habilitar a publicação de logs de fluxo no Amazon S3

Para habilitar os logs de fluxo no AWS Global Accelerator, siga as etapas deste procedimento. Seções adicionais neste capítulo fornecem as etapas para configurar seu bucket do Amazon S3 e definir permissões, para que os logs de fluxo possam ser publicados e acessados.

Para habilitar os logs de fluxo no AWS Global Accelerator

1. Crie um bucket do Amazon S3 para seus logs de fluxo em sua conta da AWS.
2. Adicione a política do IAM necessária para o usuário da AWS que está habilitando os logs de fluxo. Para ter mais informações, consulte Perfis do IAM para publicar logs de fluxo no Amazon S3.
3. Execute o seguinte comando da AWS CLI, com o nome e o prefixo do bucket do Amazon S3 que você deseja usar para seus arquivos de log:

```
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
```

Processar registros de log de fluxo no Amazon S3

Os arquivos de log são compactados. Se você abrir os arquivos de log usando o console do Amazon S3, eles serão descompactados, e os registros de log de fluxo serão exibidos. Se você baixar os arquivos, será necessário descompactá-los para visualizar os registros de log de fluxo.

Publicar logs de fluxo no Amazon S3

Os logs de fluxo do AWS Global Accelerator são publicados no Amazon S3 em um bucket do S3 existente especificado por você. Os registros de log de fluxo são publicados em uma série de objetos de arquivos de log armazenados no bucket.

Para criar um bucket do Amazon S3 para uso com logs de fluxo, consulte Criar seu primeiro bucket do S3 no Guia do usuário do Amazon Simple Storage Service.

Arquivos de log de fluxo

Os logs de fluxo coletam registros de log de fluxo, os consolidam em arquivos de log e publicam os arquivos de log no bucket do Amazon S3; em intervalos de 5 minutos. Ou seja, os arquivos de log são gravados a cada cinco minutos e cada arquivo de log contém os registros de log de fluxo para o tráfego de endereço IP registrado nos últimos cinco minutos.

O tamanho máximo de um arquivo de log é de 75 MB. Se o arquivo de log atingir o limite de tamanho no período de 5 minutos, o log de fluxo para de adicionar registros de log de fluxo, publica o arquivo no bucket do Amazon S3 e cria um novo arquivo de log.

Os arquivos de log são salvos no bucket do Amazon S3 especificado por meio de uma estrutura de pastas determinada pelo ID do log de fluxo, pela região e pela data em que são criados. A estrutura de pasta do bucket usa o seguinte formato:

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

Da mesma maneira, o nome do arquivo de log é determinado pelo ID do log de fluxo, região, e data e hora em que foi criado. Os nomes de arquivo usam o seguinte formato:

```
aws_account_id_globalaccelerator_accelerator_id_flow_log_id_timestamp_hash.log.gz
```

Observe o seguinte sobre a estrutura de pastas e nomes de arquivos para arquivos de log:

- O time stamp usa o formato YYYYMMDDTHHmmZ.
- Se você especificar barra (/) para o prefixo do bucket do S3, a estrutura da pasta do bucket do arquivo de log incluirá uma barra dupla (//), como a seguir:

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

O exemplo a seguir mostra a estrutura de pasta e o nome de arquivo de um arquivo de log para um log de fluxo criado pela conta da AWS 123456789012 de um acelerador com um ID de 1234abcd-abcd-1234-abcd-1234abcdefgh, em 23 de novembro de 2018 às 00:05 UTC:

```
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
```

Um único arquivo de log de fluxo contém entradas intercaladas com vários registros 5-tuple, ou seja, client_ip, client_port, accelerator_ip, accelerator_port, protocol. Para ver todos os arquivos de log de fluxo de seu acelerador, procure entradas agregadas pelo accelerator_id e seu account_id.

Perfis do IAM para publicar logs de fluxo no Amazon S3

Uma entidade principal do IAM na sua conta, como um perfil do IAM ou usuário do IAM, deve ter permissões suficientes para publicar logs de fluxo no bucket do Amazon S3. A política do IAM deve incluir as permissões a seguir:

```
{
    "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": "*"
        }
    ]
}
```

Permissões do bucket do Amazon S3 para logs de fluxo

Por padrão, os buckets do Amazon S3 e os objetos que eles contêm são privados. Somente o proprietário do bucket pode acessá-los. No entanto, o proprietário do bucket pode conceder acesso a outros recursos e usuários por meio da criação de uma política de acesso.

Se o usuário que cria um log de fluxo é proprietário do bucket, o serviço anexa automaticamente as políticas de bucket a seguir para conceder permissão ao log de fluxo para publicar logs nele:

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

Se o usuário que cria um evento de fluxo não possui o bucket nem tem as permissões `GetBucketPolicy` e `PutBucketPolicy` para o bucket, ocorre uma falha na criação do log de fluxo. Nesse caso, o proprietário do bucket deve adicionar manualmente as políticas acima ao bucket e especificar o ID da conta da AWS do criador do log de fluxo. Para obter mais informações, consulte Como adicionar uma política de bucket usando o console do Amazon S3 no Guia do usuário do Amazon Simple Storage Service. Se o bucket recebe logs de fluxo de várias contas, adicione uma entrada de elemento `Resource` à declaração de política `AWSLogDeliveryWrite` para cada conta.

Por exemplo, a política de bucket a seguir permite que as Contas da AWS 123123123123 e 456456456456 publiquem logs de fluxo na pasta chamada `flow-logs` em um bucket chamado `log-bucket`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": [
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/123123123123/*",
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/456456456456/*"
             ],
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-
control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
```

```
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::log-bucket"
        }
    ]
}
```

> **Note**
>
> Recomendamos conceder as permissões `AWSLogDeliveryAclCheck` e `AWSLogDeliveryWrite` para a entidade principal do serviço de entrega de log em vez de ARNs individuais da conta da AWS.

Política de chaves de CMK obrigatórias para uso com buckets de SSE-KMS

Se você habilitou a criptografia no lado do servidor para o bucket do Amazon S3 usando chaves gerenciadas pelo AWS KMS (SSE-KMS) com uma CMK gerenciado pelo cliente, deverá adicionar o seguinte à política de chaves para sua CMK de modo que os logs de fluxos possam escrever logs de arquivos no bucket:

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

Permissões de arquivo de log do Amazon S3

Além das políticas de bucket necessárias, o Amazon S3 usa listas de controle de acesso (ACLs) para gerenciar o acesso aos arquivos de log criados por um log de fluxo. Por padrão, o proprietário do bucket tem permissões `FULL_CONTROL` em cada arquivo de log. O proprietário da entrega de logs, se é diferente do proprietário do bucket, não tem nenhuma permissão. A conta de entrega de logs tem permissões `READ` e `WRITE`. Para obter mais informações, consulte Visão geral da lista de controle de acesso (ACL) no Guia do usuário do Amazon Simple Storage Service.

Prazos de entrega dos arquivos de log

O AWS Global Accelerator oferece arquivos de log para seu acelerador configurado até várias vezes por hora. Em geral, um arquivo de log contém informações sobre as solicitações recebidas pelo seu acelerador durante um período específico. O Global Accelerator geralmente entrega o arquivo de log desse período no seu bucket do Amazon S3 em até uma hora após os eventos serem exibidos no log. Algumas ou todas as entradas do arquivo de log referentes a um período podem demorar até 24 horas. Quando entradas de log atrasam, o Global Accelerator as salva em um arquivo de log no qual o nome do arquivo inclui a data e a hora do período de ocorrência das solicitações, não de entrega do arquivo.

Ao criar um arquivo de log, o Global Accelerator consolida as informações do seu acelerador de todos os locais da borda que receberam solicitações durante o período de cobertura do arquivo de log.

O Global Accelerator começa a entregar os arquivos de logs cerca de quatro horas depois de você habilitar o registro de logs. É possível que você receba alguns arquivos de logs antes disso.

> **Note**
>
> Se nenhum usuário se conectar ao seu acelerador nesse período, você não receberá arquivos de log referentes a ele.

Sintaxe de registros de log de fluxo

Um registro de log de fluxo é uma string separada por espaço com o seguinte formato:

```
<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>
```

O formato da versão 1.0 não inclui o identificador de VPC, `vpc_id`. O formato da versão 2.0, que inclui `vpc_id`, é gerado quando o Global Accelerator envia tráfego para um endpoint com preservação do endereço IP do cliente.

A tabela a seguir descreve os campos de um registro de log de fluxo.

Campo	Descrição
`version`	A versão dos logs de fluxo.
`aws_account_id`	O ID da Conta da AWS do log de fluxo.
`accelerator_id`	O ID do acelerador para o qual o tráfego é registrado.
`client_ip`	O endereço IPv4 ou IPv6 de origem.
`client_port`	A porta de origem.
`accelerator_ip`	O endereço IP do acelerador.
`accelerator_port`	A porta do acelerador.
`endpoint_ip`	O endereço IP de destino do tráfego.
`endpoint_port`	A porta de destino do tráfego.
`protocol`	O número do protocolo IANA do tráfego. Para obter mais informações, consulte Assigned Internet Protocol Numbers.
`ip_address_type`	IPv4 ou IPv6.
`packets`	O número de pacotes transferidos durante a janela de captura. Quando o número de pacotes é 0 (zero), o fluxo está ativo, mas nenhum pacote foi visto nessa direção durante uma janela de captura.
`bytes`	O número de bytes transferidos durante a janela de captura.
`start_time`	O tempo, em segundos Unix, do início da janela de captura.
`end_time`	O tempo, em segundos Unix, do fim da janela de captura.

Campo	Descrição
`action`	A ação associada como tráfego: • `ACCEPT`: O tráfego registrado foi permitido por grupos de segurança ou Network ACLs. Atualmente, o valor é sempre ACCEPT.
`log-status`	O status de registro do log de fluxo: • `OK`: os dados são registrados em log normalmente nos destinos seleciona dos. • `SKIPDATA`: Alguns registros de log de fluxo foram ignorados durante a janela de captura. Isso pode ocorrer em virtude de uma restrição de capacidade interna ou de um erro interno.
`globalacc elerator_ source_ip`	O endereço IP usado pela interface de rede do Global Accelerator. Se a preservação do endereço IP do cliente estiver habilitada, esse valor será definido como - (hífen). Para ter mais informações, consulte Preservar os endereços IP do cliente no AWS Global Accelerator.
`globalacc elerator_ source_port`	A porta usada pela interface de rede do Global Accelerator. Se a preservação de endereço IP do cliente estiver habilitada, esse valor será definido como 0 (zero). Para ter mais informações, consulte Preservar os endereços IP do cliente no AWS Global Accelerator.
`endpoint_ region`	A Região da AWS onde o endpoint está localizado.
`globalacc elerator_ region`	O local da borda (ponto de presença) que atendeu à solicitação. Cada local da borda tem um código de três letras e um número atribuído arbitrariamente, por exemplo, DFW3. O código de três letras normalmente corresponde ao código da Associação Internacional de Transportes Aéreos de um aeroporto perto do ponto de presença. (Essas abreviações podem mudar no futuro.)

Campo	Descrição
`direction`	A direção do tráfego. Indica o tráfego que entra na rede do Global Accelerator (`INGRESS`) ou retorna ao cliente (`EGRESS`).
`vpc_id`	O identificador do VPC. Incluído nos logs de fluxo da versão 2.0 quando o Global Accelerator envia tráfego para um endpoint com preservação do endereço IP do cliente.

Se um campo não for aplicável a um registro específico, o registro exibirá o símbolo '-' para essa entrada.

Como usar o AWS CloudTrail para registrar chamadas de API do AWS Global Accelerator

O AWS Global Accelerator é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações desempenhadas por um usuário, um perfil ou um serviço da AWS no Global Accelerator. O CloudTrail captura todas as chamadas de API para o Global Accelerator, como eventos, incluindo as chamadas do console do Global Accelerator e de chamadas de código para a API do Global Accelerator. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Global Accelerator. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos).

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações sobre o Global Accelerator no CloudTrail

O CloudTrail é habilitado em sua AWS conta ao criá-la. Quando a atividade ocorre no Global Accelerator, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS no Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos em sua conta da AWS, incluindo eventos do Global Accelerator, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas

as regiões. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros AWS serviços para melhor analisar e agir de acordo com dados coletados do evento nos logs CloudTrail. Para obter mais informações, consulte os tópicos a seguir.

- Visão geral da criação de uma trilha
- Serviços e Integrações Compatíveis com CloudTrail
- Configurando Notificações Amazon SNS para CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e receber arquivos de log do CloudTrail de várias contas

Todas as ações do Global Accelerator são registradas pelo CloudTrail e são documentadas na Referência de API do AWS Global Accelerator. Por exemplo, as chamadas para as operações `CreateAccelerator`, `ListAccelerators` e `UpdateAccelerator` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM)
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado
- Se a solicitação foi feita por outro serviço da AWS

Para obter mais informações, consulte o Elemento userIdentity do CloudTrail.

Como visualizar eventos do Global Accelerator no histórico de eventos

O CloudTrail permite visualizar eventos recentes no Event history (Histórico de eventos). Para visualizar os eventos de solicitações da API do Global Accelerator, você deve escolher Oeste dos EUA (Oregon) no seletor de região na parte superior do console. Para obter mais informações, consulte o tópico sobre como Visualizar eventos com o histórico de eventos do CloudTrail, no Guia do usuário do AWS CloudTrail.

Noções básicas sobre entradas de arquivos de log do Global Accelerator

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Cada arquivo de log do CloudTrail no formato JSON contém uma ou mais entradas de log. Uma entrada de log representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, incluindo quaisquer parâmetros, a data e hora da ação, e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que inclui as seguintes ações do Global Accelerator:

- Como listar os aceleradores de uma conta: `eventName` é `ListAccelerators`.
- Como criar um receptor: `eventName` é `CreateListener`.
- Como atualizar um receptor: `eventName` é `UpdateListener`.
- Como descrever um receptor: `eventName` é `DescribeListener`.
- Como listar os receptores de uma conta: `eventName` é `ListListeners`.
- Como excluir um receptor: `eventName` é `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"
    }
  ]
}
```

Segurança no AWS Global Accelerator

A segurança na nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de data centers e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: AWS é responsável pela proteção da infraestrutura que executaAWS produtos da Nuvem AWS na AWS. A também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao AWS Global Accelerator, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem –- Sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Global Accelerator. Os tópicos a seguir mostram como configurar o Global Accelerator para atender aos seus objetivos de segurança e conformidade. Saiba também como usar outros produtos da AWS que ajudam a monitorar e proteger os recursos do Global Accelerator.

Conteúdo

Gerenciamento de identidade e acesso para o AWS Global Accelerator

AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda o administrador no controle de segurança de acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar recursos do Global Accelerator. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Conteúdo

Público

O uso do AWS Identity and Access Management (IAM) varia dependendo do trabalho realizado no Global Accelerator.

Usuário do serviço: se você usa o serviço Global Accelerator para fazer o trabalho, o administrador fornece as credenciais e as permissões necessárias. À medida que usar mais recursos do Global Accelerator para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no Global Accelerator, consulte Solução de problemas de identidade e acesso do AWS Global Accelerator.

Administrador do serviço: se você for o responsável pelos recursos do Global Accelerator na empresa, provavelmente terá acesso total ao Global Accelerator. Cabe a você determinar quais

atributos e recursos do Global Accelerator os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Global Accelerator, consulte Como o AWS Global Accelerator funciona com o IAM.

Administrador do IAM: se você é um administrador do IAM, talvez queira saber detalhes sobre como pode escrever políticas para gerenciar o acesso ao Global Accelerator. Para visualizar exemplos de políticas baseadas em identidade do Global Accelerator que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o AWS Global Accelerator.

Autenticando com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como Usuário raiz da conta da AWS, como usuário do IAM, ou assumindo um perfil do IAM.

Você pode fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS IAM Identity Center Os usuários (IAM Identity Center), a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

A depender do tipo de usuário, você pode fazer login no AWS Management Console ou no portal de acesso AWS. Para obter mais informações sobre como fazer login na AWS, consulte Como fazer login na contaConta da AWS no Início de Sessão da AWS Guia do usuário .

Se você acessar a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar as ferramentas AWS, deverá designar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar as solicitações por conta própria, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Multi-factor

authentication no Guia do usuário do AWS IAM Identity Center e Código da autenticação multifator no IAM da AWS no Guia do usuário do IAM.

Usuário raiz Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login com acesso completo a todos os Serviços da AWS e recursos na conta. Essa identidade, chamada usuário raiz da Conta da AWS, é acessada por login com o endereço de e-mail e a senha usada para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários, inclusive os que precisam de acesso de administrador, usem a federação com um provedor de identidades para acessar os Serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da web, o AWS Directory Service, o diretório do Identity Center, ou qualquer usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou conectar-se e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicações. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Manual do Usuário doAWS IAM Identity Center.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente um perfil do IAM no AWS Management Console, você pode alternar de um usuário para um perfil do IAM (console). É possível presumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center.
- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar um perfil como proxy). Para saber a

diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

- Acesso entre serviços: alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Perfil vinculado a serviço: um perfil vinculado a serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir a função de executar uma ação em seu nome. Funções vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.
- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou atributos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário raiz ou sessão de perfil) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a o quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfis do AWS Management Console, da AWS CLI ou da API da AWS.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Defina permissões personalizadas do IAM com políticas gerenciadas pelo cliente no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em atributos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços que oferecem compatibilidade com ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS oferece compatibilidade com tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.

- Políticas de controle de serviço (SCPs) –- SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço que agrupa e gerencia centralmente várias Contas da AWS pertencentes a sua empresa. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas membro, o que inclui cada Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizations e SCPs, consulte Service control policies no Guia do usuário do AWS Organizations.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do Usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina permitir ou não uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliação de políticas no Guia do Usuário do IAM.

Como o AWS Global Accelerator funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Global Accelerator, saiba quais atributos do IAM estão disponíveis para uso com o Global Accelerator.

Para ver tabelas que mostrem uma visão similar de alto nível sobre como os serviços da AWS funcionam com a maioria dos recursos do IAM, consulte Serviços da AWS compatíveis com o IAM no Guia do usuário do IAM.

atributos do IAM que você pode usar com o AWS Global Accelerator

Atributo do IAM	Compatibilidade do Global Accelerator
Políticas baseadas em identidade	Sim

Atributo do IAM	Compatibilidade do Global Accelerator
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Sim
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Políticas baseadas em identidade para o Global Accelerator

Compatível com políticas baseadas em identidade: Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões do IAM personalizadas com políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Para visualizar exemplos de políticas baseadas em identidade do Global Accelerator, consulte Exemplos de políticas baseadas em identidade para o AWS Global Accelerator.

Políticas baseadas em recursos no Global Accelerator

Suporte a políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico.

Ações de políticas para o Global Accelerator

Compatível com ações de políticas: Sim

Os administradores podem usar AWS as políticas JSON para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de políticas geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações do Global Accelerator, consulte Ações definidas pelo AWS Global Accelerator na Referência de autorização do serviço.

As ações de políticas no Global Accelerator usam o seguinte prefixo antes da ação:

```
aws-globalaccelerator
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

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

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

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

Para visualizar exemplos de políticas baseadas em identidade do Global Accelerator, consulte Exemplos de políticas baseadas em identidade para o AWS Global Accelerator.

Recursos de políticas para o Global Accelerator

Compatível com recursos de políticas: Sim

Os administradores podem usar AWS as políticas JSON para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Na Referência de autorização de serviço, é possível ver as informações a seguir relacionadas ao Global Accelerator:

- Para ver uma lista de tipos de recursos do Global Accelerator e seus ARNs, consulte Recursos definidos pelo AWS Global Accelerator.
- Para saber quais ações é possível especificar com o ARN de cada recurso, consulte Ações definidas pelo AWS Global Accelerator.

Para visualizar exemplos de políticas baseadas em identidade do Global Accelerator, consulte Exemplos de políticas baseadas em identidade para o AWS Global Accelerator.

Chaves de condição de políticas para o Global Accelerator

Compatível com chaves de condição de política específicas de serviço: Sim

Os administradores podem usar AWS as políticas JSON para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece compatibilidade com chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte Chaves de Contexto de Condição Globais da AWS no Guia do Usuário do IAM.

Para ver uma lista das chaves de condição do Global Accelerator, consulte Chaves de condição do AWS Global Accelerator na Referência de autorização do serviço. Para saber com quais ações e recursos é possível usar uma chave de condição, consulte Ações definidas pelo AWS Global Accelerator.

Para visualizar exemplos de políticas baseadas em identidade do Global Accelerator, consulte Exemplos de políticas baseadas em identidade para o AWS Global Accelerator.

ACLs no Global Accelerator

Compatível com ACLs: sim

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com Global Accelerator

Compatível com ABAC (tags em políticas): Parcial

O Global Accelerator é compatível parcialmente com tags nas políticas. Ele é compatível com a aplicação de tags a um recurso, os aceleradores. Para obter mais informações sobre o uso de tags nas condições da declaração de políticas e para visualizar um exemplo de política para limitar o acesso a um recurso com base nas tags do recurso, consulte Como usar políticas baseadas em tags com o AWS Global Accelerator.

Para obter mais informações sobre recursos de aplicação de tags do Global Accelerator, consulte Marcar no AWS Global Accelerator.

Para saber mais sobre o uso de tags em políticas, consulte as informações a seguir.

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos recursos da AWS. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre ABAC, consulte Definir permissões com autorização ABAC no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Utilizar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Como usar credenciais temporárias com o Global Accelerator

Compatível com credenciais temporárias: Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, como quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS que funcionem com o IAM no Guia do Usuário do IAM.

Você está usando credenciais temporárias se fizer login no AWS Management Console por qualquer método, exceto nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria credenciais temporárias automaticamente. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar de um usuário para um perfil do IAM (console) no Guia do Usuário do IAM.

Você pode criar credenciais temporárias manualmente usando a API AWS CLI ou AWS. Em seguida, você pode usar essas credenciais temporárias para acessar aAWS .AWS A recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões de entidade principal entre serviços para o Global Accelerator

Suporte ao recurso de encaminhamento de sessões de acesso (FAS): sim

Quando você usa um usuário ou um perfil do IAM para executar ações na AWS, você é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Perfis de serviço do Global Accelerator

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais

informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

Perfil vinculado ao serviço do Global Accelerator

Suporte a perfis vinculados a serviços: sim

Um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir a função de executar uma ação em seu nome. Funções vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter mais informações sobre o perfil vinculado ao serviço para o Global Accelerator, consulte Função vinculada ao serviço para AWS Global Accelerator.

Para obter detalhes sobre a criação ou o gerenciamento de funções vinculadas a serviços em geral na AWS, consulte Serviços da AWS compatíveis com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para o AWS Global Accelerator

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Global Accelerator. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a API AWS. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

Para saber como criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Global Accelerator, incluindo o formato dos ARNs para cada tipo de recurso, consulte Ações, recursos e chaves de condição para o AWS Global Accelerator na Referência de autorização de serviço.

Tópicos

- Melhores práticas de política

- Como criar um acelerador do Global Accelerator
- Como usar o console do Global Accelerator
- Como usar uma ação de API do Global Accelerator
- Permitir que usuários visualizem suas próprias permissões

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Global Accelerator em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo –- para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS, que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis em seus Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente AWS específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do Usuário do IAM.
- Aplique permissões de privilégio mínimo –- ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do Usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso –- você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: Condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais –- o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a

criar políticas seguras e funcionais. Para obter mais informações, consulte Validar políticas com o IAM Access Analyzer no Guia do usuário do IAM.

- Exigir autenticação multifator (MFA) –- se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Acesso seguro à API com MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas Recomendadas de Segurança no IAM no Guia do Usuário do IAM.

Como criar um acelerador do Global Accelerator

Para criar um acelerador do AWS Global Accelerator, os usuários devem ter permissão para criar perfis vinculados a serviços associados ao Global Accelerator.

Para garantir que os usuários tenham as permissões corretas para criar aceleradores no Global Accelerator, anexe uma política ao usuário como a seguinte.

> **Note**
>
> Se você criar uma política de permissões baseada em identidade mais restritiva do que a política a seguir, os usuários com a política mais restritiva não poderão criar um acelerador.

```
{
      "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*"
    }
```

Como usar o console do Global Accelerator

Para acessar o console do AWS Global Accelerator, você deve ter um conjunto mínimo de permissões. Essas permissões dão autorização para que você liste e visualize detalhes sobre os recursos do Global Accelerator na sua conta da Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Não é necessário conceder permissões mínimas do console para usuários fazendo chamadas somente para AWS CLI ou para a API do AWS. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e perfis ainda possam usar o console do Global Accelerator, anexe também a política gerenciada da AWS `GlobalAcceleratorReadOnlyAccess` ou `GlobalAcceleratorFullAccess` às entidades.

Anexe a primeira política, `GlobalAcceleratorReadOnlyAccess`, se os usuários precisarem apenas visualizar as informações no console ou fazer chamadas para a AWS Command Line Interface ou para a API que usa as operações `List*` ou `Describe*`.

Anexe a segunda política, `GlobalAcceleratorFullAccess`, aos usuários que precisam criar ou fazer atualizações nos aceleradores. A política de acesso total inclui permissões full para o Global Accelerator, bem como permissões describe para o Amazon EC2 e o Elastic Load Balancing.

> **Note**
>
> Se você criar uma política de permissões baseada em identidade que não inclua as permissões necessárias para o Amazon EC2 e o Elastic Load Balancing, os usuários com essa política não poderão adicionar recursos do Amazon EC2 e do Elastic Load Balancing aos aceleradores.

Para obter mais informações, consulte a Página de políticas gerenciadas pela AWS do Global Accelerator ou Adicionar permissões a um usuário no Guia do usuário do IAM.

Como usar uma ação de API do Global Accelerator

O AWS Global Accelerator é compatível com o uso de ações em uma política. Isso permite que um administrador controle se uma entidade pode concluir uma operação no Global Accelerator.

Por exemplo, a política a seguir permite que um usuário execute a operação `CreateAccelerator` para criar, de modo programático, um acelerador em uma conta da AWS:

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

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a AWS API.

```
{
    "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": "*"
        }
    ]
}
```

Função vinculada ao serviço para AWS Global Accelerator

O AWS Global Accelerator usa um perfil vinculado ao serviço do AWS Identity and Access Management (IAM). O perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao Global Accelerator. O perfil vinculado ao serviço é predefinido pelo Global Accelerator e inclui todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Um perfil vinculado ao serviço facilita a configuração do Global Accelerator porque não é preciso adicionar as permissões necessárias manualmente. O Global Accelerator define as permissões do perfil vinculado ao serviço e, exceto se definido de outra forma, somente o Global Accelerator pode assumir seu perfil. As permissões definidas incluem as políticas de confiança e de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você só pode excluir um perfil vinculado a serviço depois de excluir os recursos relacionados. Isso protege seus recursos do Global Accelerator, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas aos serviços, consulte Serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Funções vinculadas aos serviços. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de perfil vinculado ao serviço para o Global Accelerator

O AWS Global Accelerator usa um perfil vinculado ao serviço chamado AWSServiceRoleForGlobalAccelerator. Esse perfil permite que o Global Accelerator acesse recursos em sua conta, como balanceadores de carga e outros endpoints, para ajudar a garantir, por exemplo, que você possa adicionar somente recursos configurados para funcionar com o Global Accelerator. O perfil AWSServiceRoleForGlobalAccelerator também permite que o Global Accelerator crie e gerencie os recursos necessários para a preservação do endereço IP do cliente.

O Global Accelerator cria automaticamente um perfil chamado AWSServiceRoleForGlobalAccelerator quando o perfil é exigido pela primeira vez para oferecer compatibilidade com uma operação de API do Global Accelerator. Esse perfil é necessário para usar aceleradores no Global Accelerator. O ARN para o perfil AWSServiceRoleForGlobalAccelerator é semelhante a:

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

Permissões de perfil vinculado ao serviço

O Global Accelerator usa o perfil vinculado ao serviço chamado AWSServiceRoleForGlobalAccelerator para acessar recursos e configurações para verificar a prontidão. Esse perfil vinculado ao serviço usa a política gerenciada `AWSGlobalAcceleratorSLRPolicy`.

O perfil vinculado ao serviço AWSServiceRoleForGlobalAccelerator confia no serviço a seguir para assumir o perfil:

- `globalaccelerator.amazonaws.com`

Para visualizar as permissões para esta política, consulte AWSGlobalAcceleratorSLRPolicy na Referência de políticas gerenciadas pela AWS.

Você deve configurar permissões para permitir que uma entidade do IAM (como um usuário, grupo ou perfil) exclua um perfil vinculado ao serviço do Global Accelerator. Para mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Como criar um perfil vinculado ao serviço do Global Accelerator

Você não precisa criar manualmente um perfil vinculado ao serviço para o Global Accelerator. O serviço cria o perfil para você automaticamente quando você cria um acelerador pela primeira vez.

Se você remover seus recursos do Global Accelerator e excluir o perfil vinculado ao serviço, o serviço criará o perfil outra vez automaticamente quando você criar um novo acelerador.

Como editar o perfil vinculado ao serviço do Global Accelerator

O Global Accelerator não permite editar o perfil vinculado ao serviço AWSServiceRoleForGlobalAccelerator. Depois que o serviço criar uma função vinculada a serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, você poderá editar a descrição de uma função usando o IAM. Para obter mais informações, consulte Editar uma função vinculada ao serviço no Guia do usuário do IAM.

Como excluir o perfil vinculado ao serviço do Global Accelerator

Se você não precisa mais usar o Global Accelerator, recomendamos que exclua o perfil vinculado ao serviço. Dessa forma, você não tem entidades não utilizadas que não sejam monitoradas ou mantidas ativamente. No entanto, você deve limpar os recursos do Global Accelerator em sua conta antes de poder excluir manualmente os perfis.

Depois de desabilitar e excluir seus aceleradores, você poderá excluir o perfil vinculado ao serviço. Para obter mais informações sobre a exclusão de aceleradores, consulte Criar acelerador.

> **Note**
>
> Se você desabilitou e excluiu seus aceleradores, mas a atualização do Global Accelerator não foi concluída, a exclusão do perfil vinculado ao serviço poderá falhar. Se isso acontecer, espere alguns minutos e tente as etapas de exclusão do perfil vinculado ao serviço novamente.

Para excluir o perfil vinculado ao serviço AWSServiceRoleForGlobalAccelerator manualmente

1. Faça login em AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, escolha Roles. Selecione a caixa de marcação ao lado do nome da função que você deseja excluir, não o nome ou a linha em si.
3. Em ações de Role (Função) na parte superior da página, escolha a função Delete (Excluir).
4. Na caixa de diálogo de confirmação, revise os dados do último acesso ao serviço que mostram quando cada uma das funções selecionadas acessou pela última vez um produto da AWS. Isso

ajuda você a confirmar se a função está ativo no momento. Se quiser prosseguir, escolha Sim, Excluir para enviar a função vinculada ao serviço para exclusão.

5. Monitore as notificações do console do IAM para progresso da exclusão da função vinculada ao serviço. Como a exclusão da função vinculada ao serviço do IAM é assíncrona, depois de enviar a função para exclusão, a tarefa de exclusão pode ou não ser bem-sucedida. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Atualizações na política do perfil vinculado ao serviço do Global Accelerator

Para conferir as atualizações de `AWSGlobalAcceleratorSLRPolicy`, a política gerenciada pela AWS para perfis vinculados ao serviço do Global Accelerator, consulte a Tabela de atualizações das políticas gerenciadas pela AWS. Você também pode assinar alertas automáticos de RSS na página do AWS Global Accelerator Histórico do documento.

Políticas gerenciadas pela AWS para o AWS Global Accelerator

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para seus casos de uso específicos, por estarem disponíveis para uso por todos os clientes da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas AWS. Se AWS atualiza as permissões definidas em um política gerenciada por AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política estiver vinculada. É provável que AWS atualize uma política gerenciada por AWS quando um novo AWS service (Serviço da AWS) for lançado, ou novas operações de API forem disponibilizadas para os serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Política gerenciada pela AWS: AWSServiceRoleForGlobalAccelerator

Não é possível anexar `AWSServiceRoleForGlobalAccelerator` às entidades do IAM. Esta política é anexada a um perfil vinculado ao serviço que permite que o AWS Global Accelerator acesse os serviços e recursos da AWS que são usados ou gerenciados pelo Global Accelerator. Para ter mais informações, consulte Função vinculada ao serviço para AWS Global Accelerator.

Política gerenciada pela AWS: GlobalAcceleratorReadOnlyAccess

Você pode anexar `GlobalAcceleratorReadOnlyAccess` às entidades do IAM. Esta política concede acesso de somente leitura a ações para trabalhar com aceleradores no Global Accelerator. É útil para usuários que só precisam visualizar informações no console ou fazer chamadas para a AWS Command Line Interface ou para a API que usa as operações `List*` ou `Describe*`.

Para visualizar as permissões para esta política, consulte GlobalAcceleratorReadOnlyAccess na Referência de políticas gerenciadas pela AWS.

Política gerenciada pela AWS: GlobalAcceleratorFullAccess

Você pode anexar `GlobalAcceleratorFullAccess` às entidades do IAM. Esta política concede acesso total a ações para trabalhar com aceleradores no Global Accelerator. Anexe-a aos usuários do IAM e a outras entidades principais que precisam de acesso completo a ações do Global Accelerator.

> **Note**
>
> Se você criar uma política de permissões baseada em identidade que não inclua as permissões necessárias para o Amazon EC2 e o Elastic Load Balancing, os usuários com essa política não poderão adicionar recursos do Amazon EC2 e do Elastic Load Balancing aos aceleradores.

Para visualizar as permissões para esta política, consulte GlobalAcceleratorFullAccess na Referência de políticas gerenciadas pela AWS.

Atualizações do Global Accelerator para políticas gerenciadas pela AWS

Visualize detalhes sobre atualizações em políticas gerenciadas pela AWS para o Global Accelerator desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações realizadas nesta página, assine o feed RSS na página de histórico do documento do Global Accelerator.

Alteração	Descrição	Data
AWSGlobalAcceleratorSLRPolicy: política atualizada	O Global Accelerator adicionou uma nova permissão para descrever	20 de outubro de 2023

Alteração	Descrição	Data
	grupos destino em balanceadores de carga. O Global Accelerator usa `elasticloadbalancing:DescribeTargetGroups` para identificar balanceadores de carga com o tipo de destino `ip`, que não é um tipo de destino compatível com endpoints de balanceador de carga de pilha dupla no Global Accelerator.	
AWSGlobalAcceleratorSLRPolicy: política atualizada	O Global Accelerator adicionou novas permissões para descrever receptores em balanceadores de carga e descrever endereços em instâncias do EC2. O Global Accelerator usa `elasticloadbalancing:DescribeListeners` para oferecer compatibilidade com a tomada de decisões de gerenciamento de receptores para balanceadores de carga, com base nas configurações do receptor. O Global Accelerator usa `ec2:DescribeAddresses` para adicionar endpoints de endereço IP elástico aos aceleradores.	23 de maio de 2023

Alteração	Descrição	Data
AWSGlobalAccelerat orSLRPolicy: política atualizad a	O Global Accelerator adicionou novas permissões para oferecer compatibilidade com endereços IPv6. O Global Accelerator usa `ec2:AssignIpv6Addr esses` para atualizar a ENI do Global Accelerator em uma sub-rede do cliente com um endereço IPv6 para enviar e receber tráfego IPv6 e usa `UnassignI pv6Addresses` para remover o endereço IPv6 quando ele não é mais necessário.	15 de novembro de 2021
AWSGlobalAccelerat orSLRPolicy: política atualizad a	O Global Accelerator adicionou uma nova permissão para ajudar o Global Accelerator a diagnosti car erros. O Global Accelerator usa `ec2:DescribeRegions` para determinar a região da AWS em que o cliente está, o que pode ajudar o Global Accelerator a solucionar erros.	18 de maio de 2021
O Global Accelerator começou a rastrear alterações	O Global Accelerator começou a rastrear alterações de suas políticas gerenciadas pela AWS.	18 de maio de 2021

Como usar políticas baseadas em tags com o AWS Global Accelerator

Ao criar políticas do IAM, você pode definir permissões granulares concedendo acesso a recursos específicos. No entanto, à medida que o número de recursos que você gerencia aumenta, essa tarefa se torna mais difícil. Aplicar tags a recursos e depois usá-las em condições de declaração de política pode facilitar essa tarefa. Você pode conceder acesso em massa a qualquer recurso que tenha determinada tag. Você pode aplicar essa tag repetidamente a recursos relevantes ao criar o recurso ou ao atualizá-lo posteriormente.

O uso de tags em condições é uma forma de controlar o acesso a recursos e solicitações. As tags podem ser anexadas a um recurso ou passadas na solicitação para serviços compatíveis com tags. No Global Accelerator, somente aceleradores podem incluir tags. Para obter mais informações sobre a aplicação de tags no Global Accelerator, consulte Marcar no AWS Global Accelerator.

Ao criar uma política do IAM, você poderá usar chaves de condição de tag para controlar:

- Quais usuários podem executar ações em um acelerador, com base nas tags que ele já tem.
- Quais tags podem ser transmitidas na solicitação de uma ação.
- Se chaves de tags específicas podem ser usadas em uma solicitação.

Por exemplo, a política de usuário gerenciada pela AWS `GlobalAcceleratorFullAccess` oferece aos usuários permissão ilimitada para executar qualquer ação do Global Accelerator em qualquer recurso. A seguinte política limita esse poder e nega a usuários não autorizados permissão para realizar qualquer ação do Global Accelerator em qualquer acelerador de produção. O administrador de um cliente deve anexar essa política do IAM a usuários não autorizados do IAM, além da política de usuário gerenciada.

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

Para obter a sintaxe e a semântica completas das chaves de condição de tag, consulte Controlar o acesso usando tags do IAM no Guia do usuário do IAM.

Solução de problemas de identidade e acesso do AWS Global Accelerator

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Global Accelerator e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Global Accelerator
- Não estou autorizado a executar iam:PassRole
- Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do Global Accelerator

Não tenho autorização para executar uma ação no Global Accelerator

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `aws-globalaccelerator:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: aws-
globalaccelerator:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `aws-globalaccelerator:`*`GetWidget`*.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a executar iam:PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as políticas deverão ser atualizadas para permitir que você exerça um perfil no Global Accelerator.

Alguns Serviços da AWS permitem que você passe um perfil existente para o serviço, em vez de criar um novo perfil de serviço ou perfil vinculado ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para executar uma ação no Global Accelerator. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do Global Accelerator

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Global Accelerator é compatível com esses atributos, consulte Como o AWS Global Accelerator funciona com o IAM.
- Para saber como conceder acesso a seus recursos em todas as Contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para terceiros Contas da AWS, consulte Fornecimento de acesso a Contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Conexões de VPC seguras no AWS Global Accelerator

Quando você adiciona um Network Load Balancer, um Application Load Balancer interno ou um endpoint de instância do Amazon EC2 ao AWS Global Accelerator, você permite que o tráfego da Internet flua diretamente de e para o endpoint em nuvens privadas virtuais (VPCs) direcionando-o para uma sub-rede privada. A VPC que contém o balanceador de carga ou a instância do EC2 deve ter um gateway da internet vinculado a ela, para indicar que a VPC aceita o tráfego da Internet. No entanto, você não precisa de endereços IP públicos no balanceador de carga ou na instância do EC2. Você também não precisa de uma rota de gateway da internet associada para a sub-rede.

É diferente do caso de uso típico do gateway da internet, no qual tanto os endereços IP públicos quanto as rotas do gateway da internet são necessários para que o tráfego da internet flua para instâncias ou balanceadores de carga em uma VPC. Mesmo que as interfaces de rede elásticas de seus destinos estejam presentes em uma sub-rede pública (ou seja, uma sub-rede com uma rota de gateway da internet), quando você usa o Global Accelerator para tráfego de internet, o Global Accelerator substitui a rota típica da internet e todas as conexões lógicas que chegam pelo Global Accelerator também retornam pelo Global Accelerator em vez de pelo gateway da internet.

> **Note**
>
> Usar endereços IP públicos e uma sub-rede pública para suas instâncias do Amazon EC2 não é comum, embora seja possível definir sua configuração com eles. Os grupos de

segurança se aplicam a qualquer tráfego que chega às suas instâncias, incluindo tráfego do Global Accelerator e qualquer endereço IP público ou elástico atribuído à ENI da sua instância. Use sub-redes privadas para garantir que o tráfego seja entregue somente pelo Global Accelerator.
Para saber mais sobre como trabalhar com ENIs, grupos de segurança e o Global Accelerator, consulte Requisitos para endpoints com preservação do endereço IP do cliente.

Lembre-se dessas informações ao considerar problemas de perímetro de rede e configurar os privilégios do IAM relacionados ao gerenciamento de acesso à internet. Para obter mais informações sobre como controlar o acesso à internet à sua VPC, consulte este exemplo de política de controle de serviços.

Como registrar logs e monitorar no AWS Global Accelerator

O monitoramento é uma parte importante para manter a disponibilidade e a performance do Global Accelerator e das suas soluções da AWS. Você deve coletar dados de monitoramento de todas as partes de sua solução da AWS para depurar uma falha de vários pontos com facilidade, caso ocorra. A AWS fornece várias ferramentas para monitorar seus recursos e suas atividades no Global Accelerator e responder a incidentes em potencial:

O Global Accelerator fornece as seguintes três vias principais para registrar logs e rastrear:

Métricas e alarmes do Amazon CloudWatch

Ao usar o CloudWatch, você monitora os recursos da AWS e as aplicações que você executa na AWS em tempo real. Assim que seu acelerador é implantado, o CloudWatch começa a coletar e rastrear métricas para o Global Accelerator. As métricas são variáveis que você pode visualizar para confirmar que o tráfego está fluindo ou que você pode medir ao longo do tempo.

Você pode usar métricas, por exemplo, para verificar se o tráfego está fluindo pelo Global Accelerator para seus endpoints e de volta para os clientes, além de ajudar a solucionar problemas. Você também pode criar alarmes que monitoram métricas específicas e, em seguida, enviar notificações ou fazer alterações automaticamente nos recursos que você está monitorando quando a métrica exceder um determinado limite por um período.

Para ter mais informações, consulte Como usar Amazon CloudWatch com o AWS Global Accelerator.

Logs de fluxo do Global Accelerator

Os logs de fluxo do servidor são logs que você configura no Global Accelerator que fornecem registros detalhados sobre o tráfego que flui de um acelerador até um endpoint. Os logs de fluxo do servidor são úteis para muitos aplicativos, por exemplo, para auditorias de segurança e acesso. Para ter mais informações, consulte Como configurar e usar logs de fluxo no AWS Global Accelerator.

Logs do AWS CloudTrail

O CloudTrail fornece um registro de ações executadas por um usuário, um perfil ou um serviço da AWS no Global Accelerator. O CloudTrail captura todas as chamadas de API para o Global Accelerator, como eventos, incluindo as chamadas do console do Global Accelerator e de chamadas de código para a API do Global Accelerator. Para ter mais informações, consulte Como usar o AWS CloudTrail para registrar chamadas de API do AWS Global Accelerator.

Validação de conformidade do AWS Global Accelerator

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade e selecione o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de Conformidade da AWS.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Baixar relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- Guias de início rápido de segurança e conformidade: estes guias de implantação discutem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services: esse whitepaper descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

> **Note**
>
> Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- Recursos de Conformidade da AWS: essa coleção de manuais e guias pode ser aplicada ao seu setor e local.
- Guias de conformidade do cliente da AWS: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliar recursos com regras no Guia do desenvolvedor do AWS Config: o serviço AWS Config avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty: este AWS service (Serviço da AWS) detecta possíveis ameaças às suas Contas da AWS, workloads, contêineres e dados ao monitorar o ambiente em busca de atividades suspeitas e maliciosas. O GuardDuty pode ajudar você a atender a diversos requisitos de conformidade, como o PCI DSS, com o cumprimento dos requisitos de detecção de intrusões requeridos por determinadas estruturas de conformidade.
- AWS Audit Manager: esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Resiliência no AWS Global Accelerator

A infraestrutura global da AWS é criada com base em regiões da AWS e zonas de disponibilidade. As regiões da AWS As regiões fornecem várias zonas de disponibilidade separadas e isoladas

fisicamente, as quais são conectadas com baixa latência, alto throughput e redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para mais informações sobre regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

Além de ser compatível com a infraestrutura global da AWS, o Global Accelerator oferece os seguintes recursos que ajudam a oferecer compatibilidade com a resiliência de dados:

- Semelhante a uma zona de disponibilidade na AWS, uma zona da rede é uma unidade isolada com seu próprio conjunto de infraestrutura física. Quando você cria um acelerador, o Global Accelerator fornece um conjunto de endereços IP estáticos: dois endereços IPv4 estáticos para um acelerador com um tipo de endereço IP IPv4 ou quatro endereços IP estáticos para um acelerador de pilha dupla (dois endereços IPv4 e dois endereços IPv6). O Global Accelerator fornece um endereço IP estático por zona da rede a partir de uma sub-rede IP exclusiva para cada família de endereços IP. Se um endereço de uma zona da rede ficar indisponível devido ao bloqueio de endereços IP por determinadas redes de clientes ou interrupções na rede, os aplicativos dos clientes poderão tentar novamente o endereço IP estático íntegro da outra zona da rede isolada.
- O Global Accelerator monitora continuamente a integridade de todos os endpoints. Quando determina que um endpoint ativo não está íntegro, o Global Accelerator começa instantaneamente a direcionar o tráfego para outro endpoint disponível. Isso permite que você crie uma arquitetura de alta disponibilidade para seus aplicativos na AWS.

Segurança da infraestrutura no AWS Global Accelerator

Por ser um serviço gerenciado, o AWS Global Accelerator é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança da infraestrutura, consulte Proteção de Infraestrutura em Pilar de Segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar o Global Accelerator por meio da rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.

- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Cotas para o AWS Global Accelerator

Sua conta da AWS tem cotas específicas, também conhecidas como limites, relacionadas ao AWS Global Accelerator.

O console de Service Quotas fornece informações sobre as cotas do Global Accelerator. Além de visualizar as cotas padrão, você pode usar o console de Service Quotas para solicitar aumentos de cota para aquelas que podem ser ajustadas.

Você deve estar na região Leste dos EUA (Norte da Virgínia) (us-east-1) para gerenciar limites de serviço e solicitar aumentos de cotas para o Global Accelerator no console de Service Quotas. As cotas de serviço do Global Accelerator são gerenciadas na região Leste dos EUA (Norte da Virgínia) porque é onde as cotas de serviço globais da AWS são definidas. Em qualquer outra Região da AWS, você não verá as cotas do Global Accelerator e não poderá alterá-las. No entanto, observe que todas as operações da API do Global Accelerator devem ser executadas na região Oeste dos EUA (Oregon) (us-west-2).

Tópicos

Cotas gerais

As cotas gerais do Global Accelerator são as seguintes.

Entidade	Quota
Aceleradores padrão por conta da AWS	20 É possível solicitar um aumento da cota.
Aceleradores de roteamento personalizados por conta da AWS	10 É possível solicitar um aumento da cota.
Receptores por acelerador	10

Entidade	Quota
	É possível solicitar um aumento da cota.
Grupos de endpoints por acelerador, em todos os receptores	42
Regiões da AWS para as quais o Global Accelerator pode apontar, em todos os receptores e grupos de endpoints	42 Se o seu acelerador tiver um receptor, você poderá apontar para todas as regiões compatíveis com o Global Accelerator com a configuração do grupo de endpoints do seu acelerador. Observe que o número máximo de regiões que você pode referenciar em um acelerador usando grupos de endpoints diminui proporcionalmente à medida que você aumenta o número de receptores. Seu (número total de receptores) x (número de grupos de endpoints) não deve exceder 42.
Intervalos de portas por receptor	10
Substituições de portas por grupo de endpoints	10 É possível solicitar um aumento da cota.
Princípios por anexo entre contas	10 É possível solicitar um aumento da cota.
Recursos por anexo entre contas	500

Cotas para endpoints por grupo de endpoints

A seguir estão as cotas do Global Accelerator que se aplicam ao número de endpoints em grupos de endpoints.

Entidade	Descrição	Quota
Grupos de endpoints com mais de um tipo de endpoint	Número de endpoints em um grupo de endpoints contendo mais de um tipo de endpoint.	10
Grupos de endpoints com apenas Application Load Balancers	O número de Application Load Balancers em um grupo de endpoints contendo somente endpoints de Application Load Balancers.	10
Grupos de endpoints com apenas Network Load Balancers	Número de Network Load Balancers em um grupo de endpoints contendo somente endpoints de Network Load Balancers.	10 É possível solicitar um aumento da cota.
Grupos de endpoints com apenas instâncias do Amazon EC2	Número de instâncias do EC2 em um grupo de endpoints contendo somente endpoints de instâncias do EC2.	10 É possível solicitar um aumento da cota.
Grupos de endpoints com apenas endereços IP elásticos	Número de endereços IP elásticos em um grupo de endpoints contendo somente endpoints de endereços IP elásticos.	10 É possível solicitar um aumento da cota.
Grupos de endpoints com sub-redes da nuvem privada virtual da Amazon	Número de sub-redes VPC da Amazon em um grupo de endpoints contendo somente endpoints de sub-rede.	10 É possível solicitar um aumento da cota.

Cotas relacionadas

Além das cotas no Global Accelerator, há cotas que se aplicam aos recursos que você usa como endpoints para um acelerador. Para obter mais informações, consulte as informações a seguir.

- Cotas de endereço IP elástico no Guia do usuário do Amazon EC2.
- Cotas de serviço do Amazon EC2 no Guia do usuário do Amazon EC2.

- Cotas para seus Network Load Balancers no Guia do usuário para Network Load Balancers.
- Cotas para seus Application Load Balancers no Guia do usuário para Application Load Balancers.
- Cotas da Amazon VPC no Manual do usuário da Amazon VPC.

Informações relacionadas ao AWS Global Accelerator

As informações e os recursos listados aqui podem ajudar você a saber mais sobre o Global Accelerator.

Tópicos

Referência da API e informações do produto para o AWS Global Accelerator

Os recursos relacionados a seguir podem ajudar você à medida que trabalha com este serviço.

- Referência da API AWS Global Accelerator: fornece descrições completas das ações, parâmetros e tipos de dados da API, e uma lista de erros retornados pelo serviço.
- Novidades do Global Accelerator: anúncios de novos atributos do Global Accelerator e locais da borda adicionados recentemente.
- Informações sobre o produto do AWS Global Accelerator: a principal página da web para obter informações sobre o Global Accelerator, incluindo recursos e definição de preço.
- Termos de uso: informações detalhadas sobre nossos direitos autorais e marca registrada, sua conta, licença e acesso ao site, entre outros tópicos.

Obter suporte

O suporte para o Global Accelerator está disponível de várias formas.

- Fóruns de discussão: um fórum comunitário para desenvolvedores discutirem questões técnicas relacionadas ao Global Accelerator.
- Atendimento ao cliente do Support: este site reúne informações sobre casos de compatibilidade e resultados recentes do AWS Trusted Advisor e de verificações de integridade, além de links para fóruns de discussão, perguntas técnicas frequentes, o painel de integridade do serviço e informações sobre os planos do AWS Support.

- Informações do Premium Support da AWS: a principal página da Web para obter informações sobre o Premium Support da AWS, um canal de compatibilidade de resposta rápida e com atendimento individual para ajudar você a criar e executar aplicações nos serviços de infraestrutura da AWS.
- Entre em contato conosco: links para consultas sobre sua conta ou faturamento. Para dúvidas técnicas, use os fóruns de discussão ou links de suporte acima.

Dicas do blog da AWS

O blog da AWS tem vários posts para ajudar você a usar os serviços da AWS, incluindo os seguintes posts sobre o Global Accelerator:

- Usar o AWS Global Accelerator para melhorar o desempenho do aplicativo
- Práticas recomendadas para implantação com o AWS Global Accelerator
- Anúncio da compatibilidade entre contas para o AWS Global Accelerator
- Como acessar um Amazon API Gateway por meio de endereços IP estáticos fornecidos pelo AWS Global Accelerator
- Roteamento personalizado do AWS Global Accelerator com o Amazon Elastic Kubernetes Service
- Como implantar aplicativos multirregionais na AWS usando o AWS Global Accelerator
- Como maximizar a resiliência do aplicativo com o AWS Global Accelerator
- Como começar aos poucos com o AWS Global Accelerator
- Gerenciamento de tráfego com o AWS Global Accelerator
- Como analisar e visualizar logs de fluxo do AWS Global Accelerator usando o Amazon Athena e o Amazon QuickSight

Para obter uma lista completa dos blogs do AWS Global Accelerator, consulte AWS Global Accelerator na categoria Rede e entrega de conteúdo dos posts do blog da AWS.

Histórico do documento

As entradas a seguir descrevem alterações importantes feitas na documentação do AWS Global Accelerator.

- Versão da API: mais recente
- Última atualização da documentação: 27 de março de 2024

Alteração	Descrição	Data
Adiciona compatibilidade entre contas para BYOIP	O Global Accelerator agora é compatível com cinco métricas adicionais do CloudWatch que você pode usar para detectar problemas com mais facilidad e nos endpoints do acelerado r. Para obter mais informaçõ es, consulte Como usar o Amazon CloudWatch com o AWS Global Accelerator.	27 de março de 2024
Adiciona compatibilidade entre contas para BYOIP	O Global Accelerator agora é compatível com o uso de endereços traga seu próprio IP (BYOIP) em todas as contas da AWS. Para obter mais informações, consulte Trabalhar com anexos e recursos entre contas no AWS Global Accelerator.	25 de março de 2024
Adiciona compatibilidade com pilhas duplas para Network Load Balancers	O Global Accelerator agora é compatível com a adição de Network Load Balancers de pilha dupla aos acelerado res padrão. Para obter	2 de novembro de 2023

Alteração	Descrição	Data
	mais informações, consulte Requisitos de endpoint para aceleradores no AWS Global Accelerator.	
Adiciona compatibilidade com recursos entre contas	O Global Accelerator agora é compatível com a adição de recursos entre contas aos aceleradores. Para adicionar permissões para um recurso de várias contas, você cria um anexo entre contas no Global Accelerator. Para obter mais informações, consulte Como trabalhar com anexos e endpoints entre contas no AWS Global Accelerator.	1.º de novembro de 2023
Compatibilidade com quatro Regiões da AWS adicionada	Foi adicionado a compatibilidade com as seguintes Regiões da AWS para o Global Accelerator: Ásia-Pacífico (Melbourne), Europa (Espanha) e Europa (Zurique) e Israel (Tel Aviv). Para obter mais informações, consulte Disponibilidade da Região da AWS para o AWS Global Accelerator.	26 de setembro de 2023

Alteração	Descrição	Data
Atualiza o perfil vinculado ao serviço	Adiciona uma nova permissão , `elasticloadbalancing:DescribeTargetGroups` , ao serviço. O Global Accelerator usa a permissão para identificar balanceadores de carga com tipo de destino `ip`, que não é um tipo de destino compatível com endpoints de balanceador de carga de pilha dupla no Global Accelerator. Para obter mais informações, consulte Perfis vinculados ao serviço para o AWS Global Accelerator.	12 de setembro de 2023
Adiciona compatibilidade com a preservação do endereço IP do cliente para Network Load Balancers	O Global Accelerator agora é compatível com a preservação do endereço IP do cliente para Network Load Balancers com grupos de segurança. Para obter mais informações, consulte Adicionar ou atualizar endpoints com preservação do endereço IP do cliente.	22 de agosto de 2023

Alteração	Descrição	Data
Adiciona compatibilidade com IPv6 para instâncias do EC2	O Global Accelerator agora é compatível com a adição de instâncias do Amazon EC2 a aceleradores de pilha dupla, para permitir tráfego IPv4 e IPv6 para endpoints do EC2. Para obter uma lista completa dos tipos de endpoints compatíveis e obter mais informações, consulte Endpoints para aceleradores padrão no AWS Global Accelerator.	8 de agosto de 2023
Nova região adicionada	O Global Accelerator agora é compatível com Ásia-Pacífico (Jacarta). Para obter uma lista completa das regiões compatíveis, consulte Disponibilidade da Região da AWS para o AWS Global Accelerator.	15 de junho de 2023
Duas novas regiões adicionadas	O Global Accelerator agora é compatível com Ásia-Pacífico (Hyderabad) e Oriente Médio (Emirados Árabes Unidos). Para obter uma lista completa das regiões compatíveis, consulte Disponibilidade da Região da AWS para o AWS Global Accelerator.	23 de maio de 2023

Alteração	Descrição	Data
Atualiza o perfil vinculado ao serviço	Adiciona novas permissões, `elasticloadbalancing:DescribeListeners` e `ec2:DescribeAddresses`, ao perfil vinculado ao serviço do Global Accelerator, para oferecer compatibilidade com a tomada de decisões de gerenciamento de receptores para balanceadores de carga, com base nas configurações do receptor, e adiciona endpoints de endereço IP elástico aos aceleradores. Para obter mais informações, consulte Perfis vinculados ao serviço para o AWS Global Accelerator.	23 de maio de 2023
Adiciona cotas do acelerador de roteamento personalizado	Adiciona cotas do acelerador de roteamento personalizado. O Global Accelerator também tem cotas para aceleradores padrão. Para mais informações, consulte Cotas para o AWS Global Accelerator.	13 de fevereiro de 2023
Atualiza a orientação do IAM no guia	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	10 de fevereiro de 2023

Alteração	Descrição	Data
Atualizações para `AddEndpoints` e `RemoveEndpoints`	O Global Accelerator agora é compatível com a adição e remoção de endpoints separadamente do uso da operação de API `UpdateEndpointGroup`, usando as operações novas de API `AddEndpoints` e `RemoveEndpoints`. Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/global-accelerator-actions.html.	20 de outubro de 2022
Atualizações para aceleradores de pilha dupla	O Global Accelerator agora é compatível com aceleradores de pilha dupla. Para IPv4, o Global Accelerator fornece dois endereços IPv4 estáticos. Para pilha dupla, o Global Accelerator fornece um total de quatro endereços: dois endereços IPv4 estáticos e dois endereços IPv6 estáticos. Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html.	27 de julho de 2022

Alteração	Descrição	Data
Atualização no perfil vinculado ao serviço do Global Accelerator	O Global Accelerator adicionou novas permissões, `ec2:AssignIpv6Addresses` e `ec2:UnassignIpv6Addresses`, para oferecer compatibilidade com endereços IPv6. Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/security-iam-awsmanpol-updates.html.	2 de novembro de 2021
Novas métricas do CloudWatch adicionadas	O Global Accelerator adicionou duas novas métricas do CloudWatch. Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/cloudwatch-monitoring.html.	28 de outubro de 2021
Atualização na janela de captura de logs de fluxo	O Global Accelerator expandiu a janela de captura do logs de fluxo de 10 segundos para 60 segundos. Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/monitoring-global-accelerator.flow-logs.html.	30 de julho de 2021

Alteração	Descrição	Data
Atualização no perfil vinculado ao serviço do Global Accelerator	O Global Accelerator adicionou uma nova permissão, `ec2:DescribeRegions`, para permitir que o Global Accelerator obtenha informações da região da AWS para ajudar a diagnosticar erros. Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/security-iam-awsmanpol-updates.html.	7 de maio de 2021
Aceleradores de roteamento personalizados adicionados	O Global Accelerator introduziu um novo tipo de acelerador: aceleradores de roteamento personalizados. Os aceleradores de roteamento personalizados funcionam bem em cenários em que você deseja usar a lógica de aplicativo personalizada para direcionar um ou mais usuários para um destino e porta específicos entre muitos, sem deixar de obter os benefícios de desempenho do Global Accelerator. Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/work-with-custom-routing-accelerators.html.	9 de dezembro de 2020

Alteração	Descrição	Data
Compatibilidade com substituições de portas adicionada	O Global Accelerator agora é compatível com a substituição da porta do receptor usada para rotear o tráfego para endpoints para que você possa voltar a rotear o tráfego para portas específicas em seus endpoints. Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-port-override.html.	21 de outubro de 2020
Duas novas regiões adicionadas	O Global Accelerator agora é compatível com África (Cidade do Cabo) e Europa (Milão). Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/preserve-client-ip-address.regions.html.	20 de maio de 2020

Alteração	Descrição	Data
Aplicação de tags e BYOIP	Esta versão adiciona compatibilidade com a adição de tags aos aceleradores e trazer seu próprio endereço IP para o AWS Global Accelerator (BYOIP). Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/tagging-in-global-accelerator.html e https://docs.aws.amazon.com/global-accelerator/latest/dg/using-byoip.html.	27 de fevereiro de 2020
Capítulo Segurança atualizado	Conteúdo para conformidade, resiliência e segurança da infraestrutura adicionado. Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/security.html.	20 de dezembro de 2019

Alteração	Descrição	Data
Compatibilidade com instâncias do EC2 e nome de DNS padrão	O AWS Global Accelerator agora é compatível com a adição de instâncias do EC2 em regiões da AWS compatíveis. Além disso, o Global Accelerator cria um nome de DNS padrão que é mapeado para os endereços IP estáticos do seu acelerador. Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html e https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.html#about-accelerators.dns-addressing.	29 de outubro de 2019
Preservação do endereço IP do cliente para Application Load Balancers	Agora você pode optar por deixar que o AWS Global Accelerator preserve o endereço IP do cliente para Application Load Balancers nas regiões da AWS compatíveis. Para ter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html.	28 de agosto de 2019

Alteração	Descrição	Data
Lançamento do serviço do AWS Global Accelerator	O Guia do desenvolvedor do AWS Global Accelerator fornece informações sobre como configurar e usar aceleradores (gerenciadores de tráfego da camada de rede) que melhoram a disponibilidade e o desempenho de seus aplicativos de internet que têm um público global.	26 de novembro de 2018