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 criaAceleradoras doPara melhorar o desempenho dos seus aplicativos para usuários locais e globais. Dependendo do tipo de acelerador que você escolher, você pode obter benefícios adicionais.

- Ao usar um acelerador padrão, você pode melhorar a disponibilidade de seus aplicativos da 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.
- Usando 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 oferece suporte a endpoints em várias regiões da AWS, listadas naTabela de região da AWS.

Por padrão, o Global Accelerator fornece dois endereços IP estáticos que você associa ao acelerador. Com um acelerador padrão, em vez de usar os endereços IP fornecidos pelo Global Accelerator, você pode configurar esses pontos de entrada para endereços IPv4 de seus próprios intervalos de endereços IP que você traz para o Global Accelerator. Os endereços IP estáticos são anycast da rede de borda da AWS.

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

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 Elastic IP localizados em uma região da AWS ou em várias regiões. 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 saudáveis.

Os aceleradores de roteamento personalizados oferecem suporte apenas aos tipos de endpoint de sub-rede da nuvem privada virtual (VPC) e roteiam o tráfego de endereços IP privados nessa sub-rede.

Para obter uma lista das regiões da AWS onde o Global Accelerator e outros serviços são compatíveis com o, consulte oTabela de região da AWS.

Tópicos

Componentes do AWS Global Accelerator

O AWS Global Accelerator inclui os seguintes componentes:

Endereços IP estáticos

O Global Accelerator fornece um conjunto de dois endereços IP estáticos que são anycast da rede de borda da AWS. Se você trazer seu próprio intervalo de endereços IP para a AWS (BYOIP) para usar com o Global Accelerator, poderá atribuir endereços IP de seu próprio grupo para usar com o acelerador. Para obter mais informações, consulte Traga seus próprios endereços IP (BYOIP) no AWS Global Accelerator.

Os endereços IP servem como pontos de entrada fixos únicos para seus clientes. Se você já tiver Elastic Load Balancing load balancers, instâncias do Amazon EC2 ou recursos de endereço Elastic IP 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.

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

Acelerador

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 ouvintes.

Existem dois tipos de aceleradores:

- APadrãodireciona o tráfego para o endpoint ideal da AWS com base em vários fatores, incluindo a localização do usuário, a integridade do endpoint e os pesos de endpoint configurados. Isso aprimora a disponibilidade e o desempenho de seus aplicativos. Os endpoints podem ser Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços Elastic IP.
- ARoteamento personalizadopermite rotear deterministicamente vários usuários para um destino específico do EC2 atrás do acelerador, conforme necessário para alguns casos de uso. Você faz isso direcionando os usuários para um endereço IP exclusivo e uma porta no acelerador, que o Global Accelerator mapeou para o destino.

Para obter mais informações, consulte Tipos de aceleradores.

Nome DNS

Global Accelerator atribui a cada acelerador um nome de Domain Name System (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 de seu próprio intervalo de endereços IP. Dependendo do caso de uso, você pode usar os endereços IP estáticos do acelerador ou o nome DNS para rotear o tráfego para o acelerador ou configurar registros DNS para rotear o tráfego usando seu próprio nome de domínio personalizado.

Zona de rede

Uma zona de rede atende os endereços IP estáticos do acelerador a partir de uma sub-rede IP exclusiva. Semelhante a uma zona de disponibilidade da AWS, uma zona de rede é uma unidade

isolada com seu próprio conjunto de infraestrutura física. Quando você configura um acelerador, por padrão, o Global Accelerator aloca dois endereços IPv4 para ele. Se um endereço IP de uma zona de rede ficar indisponível devido ao bloqueio de endereços IP por determinadas redes cliente ou interrupções de rede, os aplicativos cliente poderão tentar novamente no endereço IP estático íntegro da outra zona de rede isolada.

Listener

Um ouvinte processa conexões de entrada de clientes para o Global Accelerator, com base na porta (ou intervalo de portas) e no protocolo (ou protocolos) que você configura. Um ouvinte pode ser configurado para TCP, UDP ou ambos os protocolos TCP e UDP. Cada ouvinte tem um ou mais grupos de endpoint associados a ele, e o tráfego é encaminhado para endpoints em um dos grupos. Associe grupos de pontos de extremidade a ouvintes 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 endpoint associados a um ouvinte.

Grupo de endpoints

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

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 EC2 ou endereços Elastic IP. Um endpoint do Application Load Balancer pode ser voltado para a Internet ou interno. O tráfego para aceleradores padrão é roteado para endpoints com base na integridade do endpoint juntamente com as opções de configuração escolhidas, como pesos de endpoint. Para cada ponto final, você pode configurar pesos, que são números que você pode usar para especificar a proporção de 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 de nuvem privada virtual (VPC) com uma ou várias instâncias do Amazon EC2 que são os destinos do tráfego.

Como o AWS Global Accelerator

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

> **Note**
>
> Se você trazer seu próprio intervalo de endereços IP para a AWS (BYOIP) para usar com o Global Accelerator, poderá atribuir endereços IP estáticos de seu próprio grupo para usar com o acelerador. Para obter mais informações, consulte Traga seus próprios endereços IP (BYOIP) no AWS Global Accelerator.

No ponto de presença, o tráfego do aplicativo é roteado com base no tipo de acelerador que você configura.

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

O tráfego viaja pela rede global da AWS redundante, bem monitorada, livre de congestionamento e até o endpoint. Ao maximizar o tempo em que o tráfego está na rede AWS, o Global Accelerator garante que o tráfego seja sempre roteado pelo caminho de rede ideal.

Com alguns tipos de endpoint (em algumas regiões da AWS), você tem a opção de preservar e acessar o endereço IP do cliente. Dois tipos de endpoints podem preservar o endereço IP de origem do cliente em pacotes de entrada: Application Load Balancers e instâncias do Amazon EC2. O Global Accelerator não oferece suporte à preservação de endereço IP do cliente para endpoints de

endereço IP do Network Load Balancer e Elastic IP. Os pontos de extremidade em aceleradores de roteamento personalizados sempre têm o endereço IP do cliente preservado.

O Global Accelerator encerra conexões TCP de clientes nos pontos de presença 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 taxa de transferência.

Em aceleradores padrão, o Global Accelerator monitora continuamente a integridade de todos os endpoints e começa instantaneamente a direcionar o tráfego 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 Health não são usadas com aceleradores de roteamento personalizados e não há failover, pois você especifica o destino para o qual rotear o tráfego.

Quando você adiciona um acelerador, os grupos de segurança e as regras do AWS WAF que você já configurou continuam funcionando como antes de adicionar o acelerador.

Se você quiser um controle detalhado sobre seu tráfego global, você pode configurar pesos para seus endpoints em um acelerador padrão. Também é possível aumentar (dial up) ou diminuir (dial down) o percentual de tráfego de um grupo de pontos de extremidade específico, por exemplo, para testes de desempenho ou upgrades de pilha.

Esteja ciente do seguinte ao usar o Global Accelerator:

- O AWS Direct Connect não anuncia prefixos de endereço IP para o AWS Global Accelerator em uma interface virtual pública. Recomendamos que você não anuncie endereços IP usados para se comunicar com o Global Accelerator por meio da interface virtual pública do AWS Direct Connect. Se você anunciar endereços IP que você usa para se comunicar com o Global Accelerator por meio de sua interface virtual pública do AWS Direct Connect, isso resultará em um fluxo de tráfego assimétrico: seu tráfego para o Global Accelerator vai para o Global Accelerator pela Internet, mas devolverá o tráfego no local vem através de sua interface virtual pública do AWS Direct Connect.
- O Global Accelerator não oferece suporte à adição como endpoint de um recurso que pertença a outra conta da AWS.

Tópicos

- Verificações de Health do AWS Global Accelerator

Tempo limite ocioso no AWS Global Accelerator

O AWS Global Accelerator define um período de tempo limite ocioso que se aplica às suas conexões. Se nenhum dado tiver sido enviado ou recebido até o período que o tempo limite de inatividade acabar, o Global Accelerator fechará a conexão. Para garantir que a conexão permaneça ativa, o cliente ou o endpoint deve enviar pelo menos 1 byte de dados antes que o período de tempo limite ocioso decorra.

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 a direcionar o tráfego para um endpoint até que o tempo limite ocioso seja atingido, mesmo que o endpoint esteja marcado como não íntegro. O Global Accelerator seleciona um novo endpoint, se necessário, somente quando uma nova conexão é iniciada ou após um tempo limite ocioso.

Endereços IP estáticos no AWS Global Accelerator

Você usa os endereços IP estáticos que o Global Accelerator atribui ao seu acelerador — ou que você especifica em seu próprio pool de endereços IP, para aceleradores padrão — para rotear o tráfego da Internet para a rede global da AWS perto de onde seus usuários estejam, independentemente de sua localização. Para aceleradores padrão, você associa os endereços a Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços Elastic IP executados em uma única região da AWS ou em várias regiões. Para aceleradores de roteamento personalizados, você direciona o tráfego para destinos do EC2 em sub-redes da VPC em uma ou mais regiões. O roteamento do tráfego pela rede global da AWS melhora a disponibilidade e o desempenho, pois o tráfego não precisa realizar vários saltos pela Internet pública. O uso de endereços IP estáticos também permite distribuir o tráfego de aplicativos de entrada entre 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. O uso de endereços IP fixos significa que os usuários têm uma maneira consistente de se conectar ao seu aplicativo à medida que você faz alterações.

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

O Global Accelerator fornece os endereços IP estáticos para você a partir do pool de endereços IP da Amazon, a menos que você traga seu próprio intervalo de endereços IP para a AWS e especifique os endereços IP estáticos desse pool. (Para obter mais informações, consulte Traga seus próprios endereços IP (BYOIP) no AWS Global Accelerator.) Para criar um acelerador no console, a primeira etapa é solicitar ao Global Accelerator que provisione os endereços IP estáticos inserindo um nome para o acelerador ou escolha seus próprios endereços IP estáticos. Para ver as etapas para criar um acelerador, consulteConceitos básicos do AWS Global Accelerator.

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

Gerenciamento de fluxo de tráfego com marcações de tráfego e pesos de ponto de extremidade

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

- Alterar a discagem de tráfego para limitar o tráfego de um ou mais grupos de terminais
- Especificar pesos para alterar a proporção de tráfego para os pontos finais em um grupo

Como funcionam as marcações de tráfego

Para cada grupo de pontos de extremidade em um acelerador padrão, você pode definir uma discagem de tráfego para controlar a porcentagem de tráfego que é enviado para o grupo de pontos de extremidade. A porcentagem é aplicada somente ao tráfego que já está direcionado ao grupo de pontos de extremidade, e não a todo o tráfego de ouvinte.

A discagem de tráfego limita a parte do tráfego que um grupo de terminais aceita, expressa como uma porcentagem do tráfego direcionado para esse grupo de terminais. Por exemplo, se você definir a discagem de tráfego para um grupo de pontos de extremidade nous-east-1para 50

(ou seja, 50%) e o acelerador direciona 100 solicitações de usuário para esse grupo de endpoint, somente 50 solicitações são aceitas pelo grupo. O acelerador direciona as 50 solicitações restantes para grupos de endpoint em outras regiões.

Para obter mais informações, consulte Ajustar o fluxo de tráfego com marcações de tráfego.

Como as pesas funcionam

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

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

O acelerador calcula a soma dos pesos dos pontos finais em um grupo de endpoint e, em seguida, direciona o tráfego para os pontos finais com base na proporção entre o peso de cada endpoint e o total. Para ver um exemplo de como as pesas funcionam, consulte Pesos de endpoints.

As marcações de tráfego e os pesos afetam como o acelerador padrão atende o tráfego de diferentes maneiras:

- Você configura discagens de tráfego paraGrupos de endpoints. A discagem de tráfego permite cortar uma porcentagem do tráfego — ou todo o tráfego — para o grupo, “discando” o tráfego que o acelerador já direcionou para ele com base em outros fatores, como proximidade.
- Você usa pesos, por outro lado, para definir valores paraendpoints individuaisem um grupo de endpoints. Os pesos fornecem uma maneira de dividir o tráfego dentro do grupo de endpoint. Por exemplo, você pode usar pesos para fazer testes de desempenho para endpoints específicos em uma região.

> **Note**
>
> Para obter mais informações sobre como as marcações e pesos de tráfego afetam o failover, consulteFailover para endpoints não íntegros.

Verificações de Health do AWS Global Accelerator

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 tiver configurado configurações personalizadas de verificação de integridade, o Global Accelerator usará essas configurações de maneiras específicas, dependendo de sua configuração. Você define essas configurações em endpoints de instância do Global Accelerator for Amazon EC2 ou Elastic IP ou definindo configurações no console do Elastic Load Balancing para Network Load Balancers ou Application Load Balancers. Para obter mais informações, consulte Opções de verificação de integridade.

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 ponto final íntegro para rotear o tráfego em um acelerador padrão, ele roteará solicitações para todos os endpoints.

Tipos de aceleradores

Existem dois tipos de aceleradores que você pode usar com o AWS Global Accelerator:Aceleradoras doeaceleradores de roteamento personalizados. Ambos os 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

> Usando um acelerador padrão, você pode melhorar a disponibilidade e o desempenho de seus aplicativos executados em instâncias do Application Load Balancers, Network Load Balancers ou Amazon EC2. Com um acelerador padrão, o Global Accelerator roteia o tráfego do cliente entre endpoints regionais com base na proximidade geográfica e na integridade do endpoint. Ele também permite que os clientes mudem o tráfego do cliente entre endpoints com base em controles como discagem de tráfego e pesos de endpoint. 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 Casos de uso do AWS Global Accelerator.
>
> Para saber mais, consulte Trabalhar com aceleradores padrão no AWS Global Accelerator.

Acelerador de roteamento personalizado

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

Para saber mais, consulte 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 do cliente.

Intervalos de localização e endereços IP dos pontos de presença do Global Accelerator

Para obter uma lista dos locais do servidor de borda do Global Accelerator, consulte oOnde o AWS Global Accelerator é implantado hoje?Seção doPerguntas frequentes do AWS Global Accelerator.

A AWS publica seus intervalos de endereços IP atuais no formato JSON. Para visualizar os intervalos atuais, faça o download doip-ranges.json. Para obter mais informações, consulte Intervalos de endereços IP da AWS no Amazon Web Services General Reference.

Para encontrar os intervalos de endereços IP associados aos servidores de borda do AWS Global Accelerator, pesquiseip-ranges.jsonPara a seguinte string:

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

Entradas do Global Accelerator que incluem`"region": "GLOBAL"`referem-se aos endereços IP estáticos alocados aos aceleradores. Se você deseja filtrar o tráfego através do acelerador que vem de pontos de presença (POPs) em uma área, filtre as entradas que incluem uma área geográfica específica, com`us-*`ou`eu-*`. Então, por exemplo, se você filtrar para`us-*`, você verá apenas tráfego vindo através de POPs nos Estados Unidos (EUA).

Casos de uso do AWS Global Accelerator

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

Dimensionar para maior utilização de aplicativos

Quando o uso de aplicativos aumenta, o número de endereços IP e endpoints que você precisa gerenciar também aumenta. O Global Accelerator permite que você dimensione sua rede para cima ou para baixo. Ele permite associar recursos regionais, como load balancers e instâncias do Amazon EC2, a dois endereços IP estáticos. Você inclui esses endereços em listas de permissões apenas uma vez em seus aplicativos cliente, firewalls e registros DNS. Com o Global Accelerator, você pode adicionar ou remover endpoints nas regiões da AWS, executar implantação azul/verde e fazer testes A/B sem precisar atualizar os endereços IP em seus aplicativos cliente. Isso é particularmente útil para casos de uso de IoT, varejo, mídia, automotivo e serviços de saúde nos quais você não pode atualizar facilmente aplicativos clientes com freqüência.

Aceleração para aplicativos sensíveis à latência

Muitos aplicativos, especialmente em áreas como jogos, mídia, aplicativos móveis e finanças, exigem 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 ponto de extremidade do aplicativo mais próximo do cliente, o que reduz a latência e a variação da internet. O Global Accelerator roteia o tráfego para o ponto de presença mais próximo usando o Anycast e, em seguida, o roteia para o endpoint regional mais próximo pela rede global da AWS. O Global Accelerator reage rapidamente às mudanças no desempenho da rede para melhorar o desempenho dos aplicativos dos usuários.

Recuperação de desastres e resiliência em várias regiões

Você pode confiar em sua rede para estar disponível. Você pode estar executando seu aplicativo em várias regiões da AWS para oferecer suporte à recuperação de desastres, maior disponibilidade, menor latência ou conformidade. Se o Global Accelerator detectar que seu endpoint de aplicativo está falhando na região principal da AWS, ele acionará instantaneamente o reencaminhamento de tráfego para o seu endpoint de aplicativo na próxima região da AWS disponível e mais próxima.

Proteger as suas aplicações

Expor suas origens da AWS, como Application Load Balancers ou instâncias do Amazon EC2, ao tráfego público da Internet cria uma oportunidade para ataques mal-intencionados. O Global Accelerator diminui o risco de ataque mascarando sua origem atrás de dois pontos de entrada estáticos. Esses pontos de entrada são protegidos por padrão contra ataques de negação de serviço distribuída (DDoS) com o AWS Shield. O Global Accelerator cria uma conexão de emparelhamento com o Amazon Virtual Private Cloud usando endereços IP privados, mantendo conexões com seus Application Load Balancers internos ou instâncias privadas do EC2 fora da Internet pública.

Melhore o desempenho para VoIP ou aplicações de jogos online

Usando um acelerador de roteamento personalizado, você pode aproveitar os benefícios de desempenho do Global Accelerator para seus aplicativos VoIP ou jogos. Por exemplo, você pode usar o Global Accelerator para aplicativos de jogos online que atribuem vários jogadores a uma única sessão de jogo. Use o Global Accelerator para reduzir a latência e o jitter globalmente para 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 única 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 downloads diretos da Internet, nas regiões da AWS. Essa ferramenta permite que você use seu navegador para ver a diferença de desempenho ao transferir dados usando o Global Accelerator. Escolhe um tamanho de ficheiro para transferir e a ferramenta transfere ficheiros através de HTTPS/TCP a partir do Application Load Balancers em regiões diferentes para o browser. Para cada região, você verá uma comparação direta das velocidades de download.

Para acessar a Ferramenta de Comparação de Velocidade, copie o seguinte URL em seu navegador:

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

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

Conceitos básicos do 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 específica da AWS. Observe que o Global Accelerator é um serviço global que oferece suporte a 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 deseja criar: Um acelerador padrão ou um acelerador de roteamento personalizado.
2. Configure a configuração inicial para o Global Accelerator: Forneça um nome para o acelerador. Em seguida, configure um ou mais ouvintes para processar conexões de entrada de clientes, com base no protocolo e na porta (ou intervalo de portas) que você especificar.
3. Configure grupos regionais de endpoint para o acelerador: Você pode selecionar um ou mais grupos de endpoints regionais para adicionar ao ouvinte. O ouvinte roteia solicitações para os endpoints que você adicionou a um grupo de endpoint.

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

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

4. Adicionar endpoints a grupos de endpoint: 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 endpoint. Em seguida, você pode decidir quanto tráfego deseja rotear para cada ponto final definindo pesos de ponto final.
   - Para um acelerador de roteamento personalizado, adicione uma ou mais sub-redes de nuvem privada virtual (VPC) com até milhares de destinos de instância do Amazon EC2.

Para obter etapas detalhadas sobre como criar um acelerador padrão ou um acelerador de roteamento personalizado usando o console do AWS Global Accelerator, consulteConceitos básicos do AWS Global Accelerator. Para trabalhar com as operações da API, consulteAções comuns que você pode usar com o AWS Global AcceleratorO e aReferência da API do AWS Global Accelerator.

Marcação no AWS Global Accelerator ator ator

Tags são palavras ou frases (metadados) que você usa para identificar e organizar os 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 pode ser`environmente` 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 marcar aceleradores.

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

- 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 ative as tags. Em seguida, a AWS gera um relatório de alocação de custos como um valor separado por vírgula (CSV) com seu uso e custos agregados pelas suas tags ativas. É possível aplicar tags que representem categorias de negócios (como centros de custos, nomes de aplicativos ou proprietários) para organizar seus custos de vários serviços. Para mais informações, consulte Usar tags de alocação de custos no Guia do usuário do Gerenciamento de faturamento e custos da AWS.
- Use tags para aplicar permissões baseadas em tags a aceleradoras. Para fazer isso, crie políticas do IAM que especifiquem tags e valores de tag para permitir ou não ações. Para obter mais informações, consulte Políticas baseadas em tag.

Para convenções de uso e links para outros recursos sobre marcação, consulteMarcação de recursos da AWSnoReferência geral da AWS. Para obter dicas sobre como usar tags, consultePráticas recomendadas de tags: Estratégia de marcação de recursos da AWSnoWhitepapers da AWSBlog de.

Para saber o número máximo de tags que você pode adicionar a um recurso no Global Accelerator ator, consulteCotas do AWS Global Accelerator.

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

- CreateAccelerator
- TagResource
- UntagResource
- ListTagsForResource

Suporte à marcação no Global Accelerator

O AWS Global Accelerator oferece suporte à marcação de aceleradores.

O Global Accelerator é compatível com o recurso de controle de acesso baseado em tags do AWS Identity and Access Management (IAM). Para obter mais informações, consulte Políticas baseadas em tag.

Adicionar, editar e excluir tags no Global Accelerator ator ator

O procedimento a seguir explica como adicionar, editar e excluir tags de aceleradoras no console do Global Accelerator ator.

> **Note**
>
> Você pode adicionar ou remover tags usando o console do, a CLI da AWS ou as operações da API do Global Accelerator ator. Para obter mais informações, incluindo exemplos de CLI, consulteTagResourcenoReferência da API AWS Global Accelerator ator ator.

Para adicionar, editar ou excluir tags no Global Accelerator ator ator

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Escolha o acelerador ao qual você deseja adicionar ou atualizar tags.
3. NoTagsSeção, você pode fazer o seguinte:

   Adicione um tag

   SelecioneAdicionar tag Adicionar tagEm seguida, insira uma chave e, opcionalmente, um valor para a tag.

   Editar uma tag

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

   Excluir uma tag

   SelecioneRemoverNo lado direito do campo de valor.
4. Selecione Save changes (Salvar alterações).

Definição de preço do AWS Global Accelerator

Com o AWS Global Accelerator, você paga somente por aquilo que usa. Você é cobrado por uma taxa horária e custos de transferência de dados para cada acelerador em sua conta. Para obter mais informações, consulteConceitos do AWS Global Accelerator.

Conceitos básicos do AWS Global Accelerator

Esses tutoriais fornecem as etapas para começar a usar o AWS Global Accelerator usando o console. Você também pode usar as operações da API do AWS Global Accelerator para criar e personalizar seus aceleradores. Em cada etapa deste tutorial, há um link para a operação de API correspondente para concluir a tarefa de forma programática. (Ao configurar um acelerador de roteamento personalizado, você deve usar a API para determinadas etapas de configuração.) Para obter mais informações sobre como trabalhar com as operações de API do AWS Global Accelerator, consulte oReferência de API do AWS Global Accelerator.

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

O Global Accelerator é um serviço global que oferece suporte a endpoints em várias regiões da AWS, que estão listados naTabela de região da AWS.

Este capítulo inclui dois tutoriais: um para criar um acelerador padrão e outro para criar um acelerador de roteamento personalizado. Para saber mais sobre os dois tipos de acelerador, consulteTrabalhar com aceleradores padrão no AWS Global AcceleratoreTrabalhar com aceleradores de roteamento personalizados no AWS Global Accelerator.

Tópicos

Conceitos básicos do acelerador

Esta seção apresenta as etapas para criar um acelerador padrão que roteia o tráfego para um endpoint ideal.

Tarefas

- Etapa 1: Cria um acelerador
- Etapa 2: Adicionar ouvintes
- Etapa 3: Adicionar grupos de endpoints
- Etapa 4: Adicionar endpoints
- Etapa 5: Teste o acelerador
- Passo 6 (opcional): Exclua o acelerador

Antes de começar

Antes de criar um acelerador, crie pelo menos um recurso que você pode adicionar como um ponto de extremidade para direcionar o tráfego. Por exemplo, crie uma das seguintes ações:

- Execute pelo menos uma instância do Amazon EC2 para adicionar como um endpoint. Para obter mais informações, consulteCrie os recursos do EC2 e execute a instância do EC2noGuia do usuário do Amazon EC2 para instâncias do Linux.
- Opcionalmente, crie um ou mais Network Load Balancers ou Application Load Balancers que incluam instâncias do EC2. Para obter mais informações, consulteCriar um load balancer de aplicativo de balanceador de carga de redenoGuia do usuário para Network Load Balancers.

Ao criar um recurso para adicionar ao Global Accelerator, lembre-se do seguinte:

- Ao adicionar um Application Load Balancer interno ou um endpoint de instância do EC2 no Global Accelerator, você habilita o tráfego da Internet a fluir diretamente de e para o endpoint em nuvens privadas virtuais (VPCs) direcionando-o em uma sub-rede privada. A VPC que contém o load balancer de carga ou a instância do EC2 deve ter umgateway de Internetanexado a ele, para indicar que a VPC aceita tráfego de internet. Para obter mais informações, consulte Conexões seguras da VPC 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 Route 53 conclua verificações de integridade para endpoints de instância do EC2 ou Elastic IP. Você pode encontrar informações sobre os intervalos de endereços IP associados aos verificadores de saúde do Amazon Route 53 emVerificações de integridade para seus grupos de destinonoGuia do desenvolvedor do Amazon Route 53.

Etapa 1: Cria um acelerador

Para criar o acelerador, insira um nome.

> **Note**
>
> Para concluir esta tarefa usando uma operação de API em vez do console do, consulteCreateAcceleratornoReferência de API do AWS Global Accelerator.

Para criar um acelerador

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. SelecioneCriar acelerador.
3. Forneça um nome para o acelerador.
4. Como alternativa, adicione uma ou mais tags para ajudá-lo a identificar os recursos do Global Accelerator.
5. Escolha Next (Próximo).

Etapa 2: Adicionar ouvintes

Crie um listener para processar conexões de entrada de seus usuários para o Global Accelerator.

> **Note**
>
> Para concluir esta tarefa usando uma operação de API em vez do console do, consulteCreateListenernoReferência de API do AWS Global Accelerator.

Para criar um listener

1. NoAdicionar escuta, informe as portas ou intervalos de portas que você deseja associar ao listener. Ouvintes suportam portas 1-65535.
2. Escolha o protocolo ou protocolos para as portas que você inseriu.
3. Opcionalmente, opte por ativar a afinidade do cliente. A afinidade do cliente para um ouvinte significa que o Global Accelerator garante que as conexões de um endereço IP de origem

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

O padrão éNenhum, o que significa que a afinidade do cliente não está habilitada e o Global Accelerator distribui o tráfego igualmente entre os pontos de extremidade nos grupos de endpoint para o ouvinte.

Para obter mais informações, consulte Afinidade do cliente.

4. Opcionalmente, escolhaAdicionar escutapara adicionar um ouvinte adicional.
5. Ao terminar de adicionar listeners, selecionePróximo.

Etapa 3: Adicionar grupos de endpoints

Adicione um ou mais grupos de endpoint, cada um dos quais está associado a uma região específica da AWS.

> **Note**
>
> Para concluir esta tarefa usando uma operação de API em vez do console do, consulteCreateEndPointGroupnoReferência de API do AWS Global Accelerator.

Para adicionar um grupo de endpoints.

1. NoAdicionar grupos de endpoints, na seção de um ouvinte, escolha umaRegiãoNa lista suspensa.
2. Opcionalmente, paraDiscador de tráfego, insira um número de 0 a 100 para definir uma porcentagem de tráfego para este grupo de terminais. A porcentagem é aplicada somente ao tráfego já direcionado a esse grupo de pontos de extremidade, e não a todo o tráfego de ouvinte. Por padrão, a discagem de tráfego para um grupo de pontos de extremidade é definida como 100 (ou seja, 100%).
3. Opcionalmente, para valores de verificação de saúde personalizados, escolhaConfigurar 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 Elastic IP. Para pontos de extremidade do Network Load Balancer e do Application Load Balancer, o Global Accelerator usa as configurações de

verificação de integridade que você já configurou para os próprios load balancers. Para obter mais informações, consulte Opções de verificação de integridade.

4. Opcionalmente, escolhaAdicionar grupo de endpointsPara adicionar grupos de endpoint adicionais para este listener ou outros listeners.
5. Escolha Next (Próximo).

Etapa 4: Adicionar endpoints

Adicione um ou mais endpoints associados a grupos de endpoint específicos. Essa etapa não é necessária, mas nenhum tráfego é direcionado para endpoints em uma região, a menos que os endpoints sejam incluídos em um grupo de endpoint.

> **Note**
>
> Se você estiver criando seu acelerador de forma programática, adicione endpoints como parte da adição de grupos de endpoint. Para obter mais informações, consulteCreateEndPointGroupnoReferência de API do AWS Global Accelerator.

Para adicionar endpoints

1. NoCriar endpoints, na seção de um endpoint, escolha umEndpoint.
2. Opcionalmente, paraPeso, insira um número de 0 a 255 para definir um peso para rotear o tráfego para esse ponto de extremidade. Ao adicionar pesos a endpoints, você configura o Global Accelerator para rotear o tráfego com base nas proporções especificadas. Por padrão, todos os endpoints têm um peso de 128. Para obter mais informações, consulte Pesos de endpoints.
3. Como alternativa, para um endpoint do Application Load Balancer, emPreserve IP do cliente, selecionePreserve Address. Para obter mais informações, consulte Preservar endereços IP do cliente no AWS Global Accelerator.
4. Opcionalmente, escolhaAdicionar endpointpara adicionar mais endpoints.
5. Escolha Next (Próximo).

Depois de escolherPróximo, no painel do Global Accelerator, você verá uma mensagem informando que seu acelerador está em andamento. Quando o processo for finalizado, o status do acelerador no painel seráAtivo.

Etapa 5: Teste o acelerador

Tome medidas para testar o acelerador para se certificar de que o tráfego está sendo direcionado para seus endpoints. Por exemplo, execute um comando curl, como o seguinte, substituindo um dos endereços IP estáticos do acelerador, para mostrar as regiões da AWS onde as solicitações são processadas. Isso é especialmente útil se você definir pesos diferentes para endpoints ou ajustar a discagem de tráfego em grupos de endpoint.

Execute um comando curl como o seguinte, substituindo um dos endereços IP estáticos do 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 a discagem de tráfego em qualquer grupo de endpoint, esse comando pode ajudá-lo a confirmar que o acelerador está direcionando as porcentagens corretas de tráfego para diferentes grupos. Para obter mais informações, consulte os exemplos detalhados no seguinte post de blog,Gerenciamento de tráfego com AWS Global Accelerator.

Passo 6 (opcional): Exclua o acelerador

Se você criou um acelerador como um teste ou se não estiver mais usando um acelerador, poderá excluí-lo. No console, desative o acelerador e, em seguida, você pode excluí-lo. Não é necessário remover ouvintes e grupos de endpoint do acelerador.

Para excluir um acelerador usando uma operação de API em vez do console, primeiro você deve remover todos os ouvintes e grupos de endpoint associados ao acelerador, bem como desativá-lo. Para obter mais informações, consulte o .DeleteAcceleratoroperação emReferência de API do AWS Global Accelerator.

Tenha em atenção o seguinte quando remover pontos de extremidade ou grupos de pontos de extremidade ou eliminar um acelerador:

- Quando você cria um acelerador, o Global Accelerator fornece um conjunto de dois endereços IP estáticos. Os endereços IP são atribuídos ao acelerador enquanto ele existir, mesmo se você desativar o acelerador e ele não aceitar ou rotear o tráfego. No entanto, quando vocêdeleteum acelerador, você perde os endereços IP estáticos atribuídos ao acelerador, para que você não possa mais rotear o tráfego usando-os. Como prática recomendada, certifique-se de que você

tenha permissões em vigor para evitar excluir aceleradores inadvertidamente. Você pode usar políticas do IAM com o Global Accelerator, por exemplo, permissões baseadas em tags, para limitar os usuários que têm permissões para excluir um acelerador. Para obter mais informações, consulte Políticas baseadas em tag.

- Se você encerrar uma instância do EC2 antes de removê-la de um grupo de endpoint no Global Accelerator e, em seguida, criar outra instância com o mesmo endereço IP privado e as verificações de saúde 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 endpoint antes de encerrar a instância.

Para excluir um acelerador

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Escolha o acelerador que você deseja excluir.
3. Selecione Edit.
4. SelecioneDesabilitar aceleradore, depois, escolhaSave (Salvar).
5. Escolha o acelerador que você deseja excluir.
6. SelecioneExcluir acelerador.
7. Na caixa de diálogo de confirmação, escolha Delete.

Conceitos básicos do 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 Virtual Private Cloud (VPC).

Tarefas

- Antes de começar
- Etapa 1: Criar um acelerador de roteamento personalizado
- Etapa 2: Adicionar ouvintes
- Etapa 3: Adicionar grupos de endpoints
- Etapa 4: Adicionar endpoints

- Passo 5 (opcional): Exclua o acelerador

Antes de começar

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

- Cria uma sub-rede VPC. Para obter mais informações, consulteCriar e configurar sua VPCnoAWS Directory Service Administrator.
- Como alternativa, execute uma ou mais instâncias do Amazon EC2 em sua VPC. Para obter mais informações, consulteCrie os recursos do EC2 e execute a instância do EC2noGuia do usuário do Amazon EC2 para instâncias do Linux.

Ao criar um recurso para adicionar ao Global Accelerator, lembre-se do seguinte:

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

Etapa 1: Criar um acelerador de roteamento personalizado

> **Note**
>
> Para concluir esta tarefa usando uma operação de API em vez do console do, consulteCreateCustomRoutingAcceleratornoReferência de API do AWS Global Accelerator.

Para criar um acelerador

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Forneça um nome para o acelerador.

3. para oTipo de acelerador, selecioneRoteamento personalizado.
4. Como alternativa, adicione uma ou mais tags para ajudá-lo a identificar os recursos do acelerador.
5. SelecionePróximopara adicionar ouvintes, grupos de endpoint e endpoints de sub-rede da VPC.

Etapa 2: Adicionar ouvintes

Crie um listener para processar conexões de entrada de seus usuários para o Global Accelerator.

O intervalo que você especifica ao criar um listener define quantas combinações de portas de ouvinte e endereços IP de destino podem ser usadas com o acelerador de roteamento personalizado. Para obter flexibilidade máxima, recomendamos que você especifique um grande intervalo de portas. Cada intervalo de portas do listener especificado deve incluir um mínimo de 16 portas.

> **Note**
>
> Para concluir esta tarefa usando uma operação de API em vez do console do, consulteCreateCustomRoutingListenernoReferência de API do AWS Global Accelerator.

Para criar um listener

1. NoAdicionar escuta, informe as portas ou intervalos de portas que você deseja associar ao listener. Listeners suportam portas 1-65535.
2. Escolha o protocolo ou protocolos para as portas que você inseriu.
3. Opcionalmente, escolhaAdicionar escutapara adicionar um ouvinte adicional.
4. Ao terminar de adicionar listeners, selecionePróximo.

Etapa 3: Adicionar grupos de endpoints

Adicione um ou mais grupos de endpoint, cada um dos quais está associado a uma região específica da AWS. Para cada grupo de endpoint, 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.

> **Note**
>
> Para concluir esta tarefa usando uma operação de API em vez do console do, consulteCreateCustomRoutingEndPointGroupnoReferência de API do AWS Global Accelerator.

Para adicionar um grupo de endpoints.

1. NoAdicionar grupos de endpoints, na seção de um ouvinte, escolha umaRegião.
2. para oPortas e conjuntos de protocolos, insira intervalos de portas e protocolos para suas instâncias do Amazon EC2.

   - Insira umDa portae umPara a portabilidadePara especificar um intervalo de portas.
   - Para cada intervalo de portas, especifique o protocolo ou protocolos para esse intervalo.

   O intervalo de portas não precisa ser um subconjunto do intervalo de portas do ouvinte, mas deve haver portas totais suficientes no intervalo de portas do listener para suportar o número total de portas que você especificar.
3. Escolha Save (Salvar).
4. Opcionalmente, escolhaAdicionar grupo de endpointsPara adicionar grupos de endpoint adicionais para este listener ou outros listeners.
5. Escolha Next (Próximo).

Etapa 4: Adicionar endpoints de sub-rede da VPC

Adicione um ou mais endpoints de sub-rede de Virtual Private Cloud Cloud Cloud Cloud Cloud (VPC) para este grupo de endpoint regional. Os pontos de extremidade para aceleradores de roteamento personalizados definem as sub-redes da 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 da VPC, o Global Accelerator gera novos mapeamentos de porta 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.

> **Note**
>
> As etapas aqui mostram como adicionar pontos de extremidade no console. Se você estiver criando seu acelerador de forma programática, adicione endpoints com grupos de endpoint. Para obter mais informações, consulteCreateCustomRoutingEndPointGroupnoReferência de API do AWS Global Accelerator.

Para adicionar endpoints

1. NoAdicionar endpoints, na seção do grupo de endpoint ao qual você deseja adicionar o endpoint, escolha um ID de sub-rede paraEndpoint.
2. Opcionalmente, siga um destes procedimentos para habilitar o tráfego para destinos de instância do EC2 na sub-rede:

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

   Por padrão, nenhum tráfego é permitido para endpoints de sub-rede. Se você não selecionar uma opção para permitir tráfego, o tráfego será negado a 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 de forma programática. Para obter mais informações, consulteallowCustomRoutingTrafnoReferência de API do AWS Global Accelerator.

3. Escolha Next (Próximo).

Depois de escolherPróximo, no painel do Global Accelerator, você verá uma mensagem informando que seu acelerador está em andamento. Quando o processo for finalizado, o status do acelerador no painel seráAtivo.

Passo 5 (opcional): Exclua o acelerador

Se você criou um acelerador como um teste ou se não estiver mais usando um acelerador, poderá excluí-lo. No console, desative o acelerador e, em seguida, você pode excluí-lo. Não é necessário remover ouvintes e grupos de endpoint do acelerador.

Para excluir um acelerador usando uma operação de API em vez do console, primeiro você deve remover todos os ouvintes e grupos de endpoint associados ao acelerador, bem como desativá-lo. Para obter mais informações, consulte o .DeleteCustomRoutingAcceleratoroperação emReferência de 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 acelerador enquanto ele existir, mesmo se você desativar o acelerador e ele não aceitar ou rotear o tráfego. No entanto, quando vocêdeleteum acelerador, você perde os endereços IP estáticos atribuídos ao acelerador, para que você não possa mais rotear o tráfego usando-os. Como prática recomendada, certifique-se de que você tenha permissões em vigor para evitar excluir aceleradores inadvertidamente. Você pode usar políticas do IAM como permissões baseadas em tags com o Global Accelerator para limitar os usuários que têm permissões para excluir um acelerador. Para obter mais informações, consulte Políticas baseadas em tag.

Para excluir um acelerador

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Escolha o acelerador que você deseja excluir.
3. Selecione Edit.
4. SelecioneDesabilitar aceleradore, depois, escolhaSave (Salvar).
5. Escolha o acelerador que você deseja excluir.
6. SelecioneExcluir acelerador.
7. Na caixa de diálogo de confirmação, escolha Delete.

Ações comuns que você pode usar com o AWS Global Accelerator

Esta seção lista ações comuns do AWS Global Accelerator que você pode usar com recursos do Global Accelerator, com links para documentação relevante.

Ações a serem usadas com recursos padrão

A tabela a seguir lista ações comuns do Global Accelerator que você pode usar com aceleradores padrão do Global Accelerator, com links para documentação relevante.

Ação	Usando o Console do Global Accelerator	Usando a API do acelerador global da
Criar um acelerador padrão	Consulte Conceitos básicos do acelerador	Consulte CreateAccelerator
Criar um listener para um acelerador padrão	Consulte Ouvintes para aceleradores padrão no AWS Global Accelerator	Consulte CreateListener
Criar um grupo de terminais para um acelerador padrão	Consulte Grupos de endpoint para aceleradores padrão no AWS Global Accelerator	Consulte CreateEndpointGroup
Atualizar um acelerador padrão	Consulte Aceleradoras padrão no AWS Global Accelerator	Consulte UpdateAccelerator
Liste seus aceleradores	Consulte Visualizando seus aceleradores	Consulte ListAccelerator
Obter todas as informações sobre um acelerador	Consulte Visualizando seus aceleradores	Consulte DescribeAccelerator
Excluir um acelerador	Consulte Criando ou atualizando um acelerador padrão	Consulte DeleteAccelerator

Ações a serem usadas com recursos de roteamento personalizados

A tabela a seguir lista ações comuns do Global Accelerator que você pode usar com aceleradores de roteamento personalizados, com links para documentação relevante.

Ação	Usando o Console do Global Accelerator	Usando a API do acelerador global da
Criar um acelerador de roteamento personalizado	Consulte Conceitos básicos do acelerador de roteamento personalizado	Consulte CreateCustomRoutingAccelerator
Criar um listener para um acelerador de roteamento personalizado	Consulte Ouvintes para aceleradores de roteamento personalizados no AWS Global Accelerator	Consulte CreateCustomRoutingListener
Criar um grupo de endpoint para um acelerador de roteamento personalizado	Consulte Grupos de endpoints para aceleradores de roteamento personalizados no AWS Global Accelerator	Consulte CreateCustomRoutingEndpointGroup
Atualizar um acelerador de roteamento personalizado	Consulte Aceleradores de roteamento personalizados no AWS Global Accelerator	Consulte UpdateCustomRoutingAccelerator
Liste seus aceleradores de roteamento personalizados	Consulte Visualizando seus aceleradores de roteamento personalizados	Consulte ListCustomRoutingAccelerator
Obter todas as informações sobre um acelerador de roteamento personalizado	Consulte Visualizando seus aceleradores de roteamento personalizados	Consulte DescribeCustomRoutingAccelerator
Excluir um acelerador de roteamento personalizado	Consulte Criando ou atualizando um acelerador de roteamento personalizado	Consulte DeleteCustomRoutingAccelerator

Ação	Usando o Console do Global Accelerator	Usando a API do acelerador global da
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 Adicionando, editando ou removendo um endpoint de sub-rede da VPC	Consulte AllowCustomRoutingTraffic
Negar todo o tráfego de destino de uma sub-rede em um acelerador de roteamento personalizado	Consulte Adicionando, editando ou removendo um endpoint de sub-rede da VPC	Consulte DenyCustomRoutingTraffic
Permitir tráfego para destinos específicos em um acelerador de roteamento personalizado	Consulte Adicionando, editando ou removendo um endpoint de sub-rede da VPC	Consulte AllowCustomRoutingTraffic
Negar tráfego para destinos específicos em um acelerador de roteamento personalizado	Consulte Adicionando, editando ou removendo um endpoint de sub-rede da VPC	Consulte DenyCustomRoutingTraffic

Trabalhar com aceleradores padrão no AWS Global Accelerator

Este capítulo inclui procedimentos e recomendações para a criação de aceleradores padrão no AWS Global Accelerator. Com um acelerador padrão, o Global Accelerator escolhe o ponto de extremidade íntegro mais próximo para o seu tráfego.

Se, em vez disso, você quiser usar a lógica de aplicativo personalizada para direcionar um ou mais usuários para um ponto de extremidade específico entre muitos pontos de extremidade, crie um acelerador de roteamento personalizado. Para obter mais informações, consulte 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. Adicione um listener com um conjunto específico de portas ou intervalo de portas e escolha o protocolo a ser aceito: TCP, UDP ou ambos.
3. Adicione um ou mais grupos de endpoint, um para cada região da AWS na qual você tem recursos de endpoint.
4. Adicione um ou mais pontos de extremidade a grupos de pontos de extremidade. Isso não é necessário, mas o tráfego não será roteado se você não tiver nenhum ponto final. Os endpoints podem ser Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços Elastic IP.

As seções a seguir passam pelo trabalho com aceleradores padrão, ouvintes, grupos de endpoint e endpoints.

Tópicos

Aceleradoras padrão no AWS Global Accelerator

AAcelerador padrãoNo AWS Global Accelerator direciona o tráfego para endpoints ideais na rede global da AWS para melhorar a disponibilidade e o desempenho de seus aplicativos da Internet que têm um público global. Cada acelerador inclui um ou mais ouvintes. Um ouvinte processa conexões de entrada de clientes para o Global Accelerator, com base no protocolo (ou protocolos) e na porta (ou intervalo de portas) que você configura.

Quando você cria um acelerador, por padrão, o Global Accelerator fornece um conjunto de dois endereços IP estáticos. Se você trouxer seu próprio intervalo de endereços IP para a AWS (BYOIP), poderá atribuir endereços IP estáticos de seu próprio grupo para usar com seu acelerador. Para obter mais informações, consulte Traga seus próprios endereços IP (BYOIP) no AWS Global Accelerator.

> **Important**
>
> Os endereços IP são atribuídos ao acelerador enquanto ele existir, mesmo se você desativar o acelerador e ele não aceitar ou rotear o tráfego. No entanto, quandodeleteum acelerador, você perde os endereços IP estáticos do Global Accelerator atribuídos ao acelerador, para que você não possa mais rotear o tráfego usando-os. Como prática recomendada, certifique-se de que você tenha permissões em vigor para evitar excluir aceleradores inadvertidamente. Você pode usar políticas do IAM com o Global Accelerator, por exemplo, permissões baseadas em tags, para limitar os usuários que têm permissões para excluir um acelerador. Para obter mais informações, consulte Políticas baseadas em tag.

Esta seção explica como criar, editar ou excluir um acelerador padrão no console do Global Accelerator. Se quiser usar operações de API com o Global Accelerator, consulte oReferência da API do AWS Global Accelerator.

Tópicos

- Criando ou atualizando um acelerador padrão
- Exclui um acelerador
- Visualizando seus aceleradores
- Adicionar um acelerador ao criar um load balancer
- Usando endereços IP estáticos globais em vez de endereços IP estáticos regionais

Criando ou atualizando um acelerador padrão

Esta seção explica como criar ou atualizar aceleradoras padrão no console do. Para trabalhar com o Global Accelerator programaticamente, consulte oReferência da API do AWS Global Accelerator.

Como criar um acelerador padrão

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. SelecioneCria acelerador.
3. Forneça um nome para o acelerador.
4. para oTipo de acelerador, selecioneStandard (Padrão).
5. Opcionalmente, se você trouxe seus próprios intervalos de endereços IP para a AWS (BYOIP), poderá especificar um endereço IP estático para o acelerador, um de cada pool de endereços. Faça essa escolha para cada um dos dois endereços IP estáticos do seu acelerador.
   - Para cada endereço IP estático, escolha o pool de endereços IP a ser usado.

     > **Note**
     >
     > Você deve escolher um pool de endereços IP diferente para cada endereço IP estático. Essa restrição ocorre porque o Global Accelerator atribui cada intervalo de endereços a uma zona de 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 pool de endereços IP padrão da Amazon, o Global Accelerator atribuirá um endereço IP específico ao acelerador.
6. Como alternativa, adicione uma ou mais tags para ajudá-lo a identificar seus recursos do acelerador.
7. SelecionePróximopara adicionar ouvintes, grupos de endpoint e endpoints.

Para editar um acelerador padrão

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Na lista de aceleradoras, escolha um e, em seguida, escolhaEdite.

3. NoEditar aceleradorFaça as alterações desejadas. Por exemplo, você pode desativar o acelerador para que ele não aceite mais ou encaminhe o tráfego, ou para que você possa excluí-lo. Ou, se o acelerador estiver desativado, você poderá ativá-lo.
4. Selecione Save changes (Salvar alterações).

Exclui um acelerador

Se você criou um acelerador como um teste ou se não estiver mais usando um acelerador, poderá excluí-lo. No console, desative o acelerador e, em seguida, você pode excluí-lo. Não é necessário remover ouvintes e grupos de endpoint do acelerador.

Para excluir um acelerador usando uma operação de API em vez do console, primeiro você deve remover todos os listeners e grupos de endpoint associados ao acelerador e, em seguida, desativá-lo. Para obter mais informações, consulte o .DeleteAcceleratoroperação emReferência da API do AWS Global Accelerator.

Como desativar um acelerador

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Na lista, escolha um acelerador que você deseja desativar.
3. Selecione Edit.
4. SelecioneDesativar o aceleradore, em seguida, escolhaSave (Salvar).

Como excluir um acelerador

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Na lista, escolha um acelerador que você deseja excluir.
3. Escolha Delete (Excluir).

> **Note**
>
> Se você não tiver desativado o acelerador,Excluirestá indisponível.

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

> **Important**
>
> Quando você exclui um acelerador, você perde os endereços IP estáticos atribuídos ao acelerador, para que você não possa mais rotear o tráfego usando-os.

Visualizando seus aceleradores

É possível visualizar informações sobre seus aceleradores no console do. Para ver descrições de seus aceleradores programaticamente, consulteListAcceleratorseDescribeAcceleratornoReferência da API do AWS Global Accelerator.

Para visualizar informações sobre o acelerador

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Para ver detalhes sobre um acelerador, na lista, escolha um acelerador e escolhaExibir.

Adicionar um acelerador ao criar um load balancer

Ao criar um Application Load Balancer no Console de Gerenciamento da AWS, você pode, opcionalmente,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.

> **Important**
>
> Para criar um acelerador, você deve ter as permissões corretas no lugar. Para obter mais informações, consulte Permissões necessárias para acesso ao console, gerenciamento de autenticação e controle de acesso.

Configure e visualize o seu acelerador

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

Depois de criar seu load balancer escolhendo o complemento Global Accelerator no console do Amazon EC2, vá para aServiços integradosPara visualizar os endereços IP estáticos e o nome DNS (Domain Name System, Sistema de nomes de domínio) do acelerador. Você usa essas informações para iniciar o roteamento do tráfego do usuário para o load balancer pela rede global da AWS. Para obter mais informações sobre o nome DNS atribuído ao acelerador, consulteEndereçamento DNS e domínios personalizados no AWS Global Accelerator.

Você pode visualizar e configurar seu aceleradorComo navegar para Global AcceleratorNo Console de Gerenciamento da AWS. Por exemplo, você pode ver os aceleradores associados à sua conta ou adicionar balanceadores de carga adicionais ao acelerador. Para obter mais informações, consulte Visualizando seus aceleradores e Criando ou atualizando um acelerador padrão.

Definição de preços

Com o AWS Global Accelerator, você paga somente por aquilo que usa. Você é cobrado por uma taxa horária e custos de transferência de dados para cada acelerador da sua conta. Para obter mais informações, consultePreço do AWS Global Accelerator.

Parar de usar o acelerador

Se você quiser interromper o roteamento do tráfego através do Global Accelerator para o load balancer, faça o seguinte:

1. Atualize sua configuração de DNS para apontar seu tráfego diretamente para o balanceador de carga.
2. Exclua o balanceador de carga do acelerador. Para obter mais informações, consultePara remover um endpointemAdicionando, editando ou removendo um endpoint padrão.
3. Exclui o acelerador. Para obter mais informações, consulte Exclui um acelerador.

Usando endereços IP estáticos globais em vez de 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 Elastic IP, que é um endereço IPv4 estático que você pode associar a uma instância do Amazon EC2 ou interface de rede em uma única região da AWS.

Se você tiver um público global, poderá criar um acelerador com o Global Accelerator para obter dois endereços IP estáticos globais anunciados nos pontos de presença da AWS em todo o mundo. Se você já tiver 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 enviá-los com endereços IP estáticos globais.

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 ponto de presença mais próximo de seus usuários. Maximizar o tempo em que o tráfego está na rede da AWS pode proporcionar uma experiência mais rápida e melhor ao cliente. Para obter mais informações, consulte Como o AWS Global Accelerator .

Você pode adicionar um acelerador a partir do AWS Management Console ou usando operações de API com o AWS CLI ou SDKs. Para obter mais informações, consulte Criando ou atualizando um acelerador padrão.

Observe o seguinte ao adicionar um acelerador:

- Os endereços IP estáticos globais provisionados pelo Global Accelerator permanecem atribuídos a você enquanto o acelerador existir, mesmo se você desativar o acelerador e ele não aceitar ou rotear mais o tráfego. No entanto, se você excluir um acelerador, você perde os endereços IP estáticos atribuídos a ele. Para obter mais informações, consulte Exclui um acelerador.
- Com o Global Accelerator, você paga somente por aquilo que usa. Você é cobrado por uma taxa horária e custos de transferência de dados para cada acelerador da sua conta. Para obter mais informações, consultePreço do AWS Global Accelerator.

Ouvintes para aceleradores padrão no AWS Global Accelerator

Com o AWS Global Accelerator, você adiciona ouvintes que processam conexões de entrada de clientes com base nas portas e protocolos especificados. Os ouvintes suportam TCP, UDP ou ambos os protocolos TCP e UDP.

Você define um listener padrão ao criar seu acelerador padrão e pode adicionar mais listeners a qualquer momento. Você associa cada ouvinte a um ou mais grupos de endpoint e associa cada grupo de endpoint a uma região da AWS.

Tópicos

Adicionando, editando ou removendo um listener padrão

Esta seção explica como trabalhar com listeners no console do AWS Global Accelerator.
Para concluir essas tarefas usando uma operação de API em vez do console do, consulte`CreateListener`,`UpdateListener`, e`DeleteListener`noReferência da API do AWS Global Accelerator.

Para adicionar um listener

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradoras doEscolha um acelerador.
3. Escolha Add listener.
4. NoAdicionar listener, informe as portas ou intervalos de portas que você deseja associar ao listener. Listeners suportam portas 1-65535.
5. Escolha o protocolo para as portas que você inseriu.
6. Opcionalmente, opte por ativar a afinidade do cliente. A afinidade do cliente para um ouvinte significa que o Global Accelerator garante que as conexões de um endereço IP de origem (cliente) específico sejam sempre roteadas para o mesmo endpoint. Para ativar esse comportamento, na lista suspensa, escolhaIP de origem.

O padrão éNenhum, o que significa que a afinidade do cliente não está habilitada e o Global Accelerator distribui o tráfego igualmente entre os pontos de extremidade nos grupos de endpoint para o ouvinte.

Para obter mais informações, consulte Afinidade do cliente.

7. Escolha Add listener.

Para editar um listener padrão

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradoras doEscolha um acelerador.
3. Escolha um listener e, em seguida, escolhaEditar listener.
4. NoEditar listener, altere as portas, intervalos de portas ou protocolos que você deseja associar ao listener.
5. Opcionalmente, opte por ativar a afinidade do cliente. A afinidade do cliente para um ouvinte significa que o Global Accelerator garante que as conexões de um endereço IP de origem (cliente) específico sejam sempre roteadas para o mesmo endpoint. Para ativar esse comportamento, na lista suspensa, escolhaIP de origem.

   O padrão éNenhum, o que significa que a afinidade do cliente não está habilitada e o Global Accelerator distribui o tráfego igualmente entre os pontos de extremidade nos grupos de endpoint para o ouvinte.

   Para obter mais informações, consulte Afinidade do cliente.
6. Escolha Save (Salvar).

Para remover um listener

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradoras doEscolha um acelerador.
3. Escolha um listener e, em seguida, escolhaRemover.
4. Na caixa de diálogo de confirmação, escolhaRemover.

Afinidade do cliente

Se você tiver aplicativos com monitoração de estado usados com um acelerador padrão, poderá optar por fazer com que o Global Accelerator direcione todas as solicitações de um usuário em um endereço IP de origem (cliente) específico para o mesmo recurso de ponto final, para manter a afinidade do cliente.

Por padrão, a afinidade do cliente para um listener padrão é definida comoNenhume o Global Accelerator distribui o tráfego igualmente entre os endpoints nos grupos de endpoint para o ouvinte.

O Global Accelerator usa um algoritmo de hash de fluxo consistente para escolher o endpoint ideal para a conexão de um usuário. Se você configurar a afinidade do cliente para o recurso do Global Accelerator para serNenhumO Global Accelerator usa as propriedades 5 tuplas (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 oferece o melhor desempenho. Se um determinado cliente usar portas diferentes para se conectar ao Global Accelerator e você especificar essa configuração, o Global Accelerator não pode garantir que as conexões do cliente sejam sempre roteadas para o mesmo endpoint.

Se você quiser manter a afinidade do cliente roteando um usuário específico — identificado pelo endereço IP de origem — para o mesmo ponto final sempre que se conectar, defina a afinidade do cliente comoIP de origem. Quando você especifica essa opção, o Global Accelerator usa as propriedades 2 tuplas (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. O Global Accelerator honra a afinidade do cliente após o grupo de pontos de extremidade selecionado.

Grupos de endpoint 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 ouvinte em um acelerador padrão, você especifica os grupos de endpoint para os quais o Global Accelerator direcionará o tráfego. Um grupo de endpoint e todos os endpoints nele devem estar em uma região da AWS. Você pode adicionar diferentes grupos de endpoint para diferentes fins, por exemplo, para testes de implantação azul/verde.

O Global Accelerator direciona o tráfego para grupos de pontos de extremidade em aceleradores padrão com base na localização do cliente e na integridade do grupo de terminais. Se quiser,

também é possível definir a porcentagem de tráfego a ser enviado para um grupo de endpoints. Você pode fazer isso usando a discagem 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 endpoint, nem todo o tráfego que chega a um ouvinte.

Você pode definir as configurações de verificação de integridade do Global Accelerator para cada grupo de endpoint. Ao atualizar as configurações de verificação de saúde, você pode alterar seus requisitos de pesquisa e verificação da integridade da instância do Amazon EC2 e dos endpoints de endereço Elastic IP. Para endpoints de Network Load Balancer e Application Load Balancer, configure 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 endpoint padrão e encaminha solicitações somente para os endpoints ativos que estão íntegros. Se não houver nenhum ponto final íntegro para o qual rotear o tráfego, o Global Accelerator encaminhará as solicitações para todos os endpoints.

Esta seção explica como trabalhar com grupos de endpoint para aceleradores padrão no console do AWS Global Accelerator. Se quiser usar as operações de API com o AWS Global Accelerator, consulte oReferência da API do AWS Global Accelerator.

Tópicos

Adicionando, editando ou removendo um grupo de pontos de extremidade 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 trabalhar com grupos de endpoints padrão no console do AWS Global Accelerator. Se quiser usar as operações da API com o Global Accelerator, consulte oReferência da API do AWS Global Accelerator.

Para adicionar um grupo de endpoints padrão

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradoras do, escolha um acelerador.
3. NoListenersseção, paraID do listener, escolha o ID do listener ao qual você deseja adicionar um grupo de endpoints.
4. SelecioneAdicionar grupo de endpoints.
5. Na seção de um ouvinte, especifique uma Região para o grupo de endpoint escolhendo uma na lista suspensa.
6. Opcionalmente,Disco de tráfego, insira um número de 0 a 100 para definir uma porcentagem de tráfego para este grupo de terminais. A porcentagem é aplicada somente ao tráfego que já está direcionado a esse grupo de pontos de extremidade, e não a todo o tráfego de ouvinte. Por padrão, a discagem de tráfego é definida como 100.
7. Opcionalmente, para substituir a porta do listener usada para rotear o tráfego para endpoints e redirecionar o tráfego para portas específicas em seus endpoints, escolhaConfigurar substituições de porta. Para obter mais informações, consulte Substituições.
8. Opcionalmente, para especificar valores de verificação de integridade personalizados a serem aplicados a endpoints de instância do EC2 e endereço Elastic IP, escolhaConfigurar verificações de integridade. Para obter mais informações, consulte Opções de verificação de integridade.
9. Opcionalmente, escolhaAdicionar grupo de endpointsPara adicionar grupos de endpoints adicionais para este listener ou outros listeners.
10. SelecioneAdicionar grupo de endpoints.

Para editar um grupo de endpoints.

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradoras do, escolha um acelerador.
3. NoListenersseção, paraID do listener, escolha o ID do listener ao qual o grupo de endpoints está associado.
4. SelecioneEditar grupo de endpoints.

5. NoEditar grupo de endpoints, altere a Região, ajuste a porcentagem de discagem de tráfego ou escolhaConfigurar verificações de integridadePara modificar as configurações de verificação de integridade.
6. Escolha Save (Salvar).

Como remover um grupo de endpoints padrão

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradoras do, escolha um acelerador.
3. NoListenersSeção, escolha um listener e,Remover.
4. NoGrupos de endpointsSeção, escolha um grupo de endpoints eRemover.
5. Na caixa de diálogo de confirmação, escolhaRemover.

Ajustar o fluxo de tráfego com marcações de tráfego

Para cada grupo de pontos de extremidade padrão, você pode definir uma discagem de tráfego para controlar a porcentagem de tráfego direcionada ao grupo. A porcentagem é aplicada somente ao tráfego que já está direcionado ao grupo de pontos de extremidade, e não a todo o tráfego de ouvinte.

Por padrão, a discagem de tráfego é definida como 100 (ou seja, 100%) para todos os grupos de endpoint regionais em um acelerador. A discagem 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.

Aqui estão alguns exemplos para ilustrar como você pode usar discagens de tráfego para alterar o fluxo de tráfego para grupos de terminais.

Atualize seu aplicativo por região

> Se você quiser atualizar um aplicativo em uma região ou fazer manutenção, primeiro defina a discagem 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 em serviço, ajuste a discagem de tráfego para 100 para discar o tráfego de volta.

Misturar tráfego entre duas regiões

Este exemplo mostra como o fluxo de tráfego funciona quando você altera as marcações de tráfego para dois grupos de endpoint regionais ao mesmo tempo. Digamos que você tenha dois grupos de endpoint para seu acelerador — um para o`us-west-2`Região e um para o`us-east-1`região — e você definiu as marcações de tráfego para 50% para cada grupo de endpoint.

Agora, digamos que você tem 100 pedidos chegando ao seu acelerador, com 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 de seu grupo de endpoint próximo. Ou seja, 25 solicitações são direcionadas para o grupo de endpoint no`us-west-2`e 25 são direcionados para o grupo de endpoint em`us-east-1`.
- Os próximos 50 pedidos são direcionados para as regiões opostas. Ou seja, os próximos 25 pedidos da Costa Leste são atendidos por`us-west-2`, e os próximos 25 pedidos da Costa Oeste são atendidos por`us-east-1`.

O resultado nesse cenário é que ambos os grupos de endpoint atendem a mesma quantidade de tráfego. No entanto, cada um recebe uma combinação de tráfego de ambas as regiões.

Substituições

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

No entanto, ao adicionar ou atualizar um grupo de endpoints, você pode substituir a porta do listener 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.

As substituições de porta podem ajudá-lo a evitar problemas de escuta em portas restritas. É mais seguro executar aplicativos que não exigem privilégios de superusuário (root) em seus endpoints. No entanto, no Linux e em outros sistemas semelhantes ao Unix, você deve ter privilégios de superusuário para escutar em portas restritas (portas TCP ou UDP abaixo de 1024). Mapeando uma porta restrita em um ouvinte para uma porta não restrita em um endpoint, as substituições de porta permitem evitar esse problema. Você pode aceitar tráfego em portas restritas enquanto executa

aplicativos sem acesso root em seus endpoints atrás do Global Accelerator. Por exemplo, você pode substituir uma porta de ouvinte 443 para uma porta de ponto de extremidade 8443.

Para cada substituição de porta, você especifica uma porta de ouvinte que aceita tráfego de usuários e a porta de endpoint para a qual o Global Accelerator roteará esse tráfego. Para obter mais informações, consulte Adicionando, editando ou removendo um grupo de pontos de extremidade padrão.

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

- As portas de ponto final não podem sobrepor intervalos de portas de ouvinte. As portas de ponto final especificadas em uma substituição de porta não podem ser incluídas em nenhum dos intervalos de portas do listener que você configurou para o acelerador. Por exemplo, digamos que você tenha dois ouvintes para um acelerador e definiu os intervalos de portas para esses ouvintes como 100-199 e 200-299, respectivamente. Ao criar substituições de porta, não é possível definir uma da porta de ouvinte 100 para a porta de ponto de extremidade 210, por exemplo, porque a porta de ponto final (210) está incluída em um intervalo de portas de ouvinte que você definiu (200-299).
- Nenhuma porta de ponto final duplicada. Se uma substituição de porta em um acelerador especificar uma porta de ponto de extremidade, você não poderá especificar a mesma porta de ponto de extremidade com substituição de porta de ouvinte diferente. Por exemplo, você não pode especificar uma substituição de porta da porta do listener 80 para a porta do endpoint 90 juntamente com uma substituição da porta do listener 81 para a porta do endpoint 90.
- A verificação de Health continua a usar a porta original. Se você especificar uma substituição de porta para uma porta configurada como uma 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 saúde na porta 80 do listener e também especifique uma substituição de porta da porta do listener 80 para a porta do endpoint 480. As verificações de Health continuam a usar a porta 80 do endpoint. No entanto, o tráfego de usuário que entra 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 Elastic IP. Como os Network Load Balancers e 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 para o Global Accelerator mapear portas de verificação de integridade para diferentes portas de endpoint para instâncias do EC2 e Elastic IP endpoints de endereço.

- As configurações do grupo de segurança devem permitir o acesso à porta. Certifique-se de que os grupos de segurança permitam o tráfego chegar às portas de endpoints que você designou em substituições de porta. Por exemplo, se você substituir a porta de ouvinte 443 para a porta de ponto final 1433, certifique-se de que quaisquer restrições de porta definidas em seu security group para esse Application Load Balancer ou endpoint do Amazon EC2 permitam tráfego de entrada na porta 1433.

Opções de verificação de integridade

O AWS Global Accelerator enviará regularmente solicitações para endpoints padrão para testar o status deles. Essas verificações de saúde são executadas automaticamente. As orientações para determinar a integridade de cada ponto final e o tempo para as verificações de integridade dependem do tipo de recurso de ponto final.

> **Important**
>
> 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 Route 53 conclua verificações de integridade para endpoints de instância do EC2 ou Elastic IP. Você pode encontrar informações sobre os intervalos de endereços IP associados aos verificadores de saúde do Amazon Route 53 emVerificações de integridade para seus grupos de destinonoGuia do desenvolvedor do Amazon Route 53.

Você pode configurar as seguintes opções de verificação de integridade para um grupo de endpoint. Se você especificar opções de verificação de integridade, o Global Accelerator usará as configurações para verificações de integridade de instância do EC2 ou de endereço Elastic IP, mas não para Network Load Balancers ou Application Load Balancers.

- Para endpoints do Application Load Balancer ou do Network Load Balancer, configure verificações de integridade para os recursos usando as opções de configuração do Elastic Load Balancing cer. Para obter mais informações, consulteVerificações de integridade para seus grupos de destino. As opções de verificação de Health escolhidas no Global Accelerator não afetam os Application Load Balancers ou Network Load Balancers que você adicionou como endpoints.

> **Note**
>
> Quando você tem um Application Load Balancer ou Network Load Balancer que inclui vários grupos de destino, o Global Accelerator considera o ponto de extremidade do load balancer como íntegro somente seCadaatrás do load balancer tem pelo menos um destino íntegro. Se qualquer grupo de destino único para o balanceador de carga tiver apenas destinos não íntegros, o Global Accelerator considerará o ponto final como não íntegro.

- Para endpoints de instância do EC2 ou endereço Elastic IP que são adicionados a um ouvinte configurado com TCP, você pode especificar a porta a ser usada para verificações de saúde. Por padrão, se você não especificar uma porta para verificações de integridade, o Global Accelerator usará a porta do listener especificada para o acelerador.
- Para endpoints de instância do EC2 ou endereço Elastic IP com ouvintes UDP, o Global Accelerator usa a porta do ouvinte e o protocolo TCP para verificações de integridade, portanto, você deve ter um servidor TCP em seu endpoint.

> **Note**
>
> Certifique-se de verificar se a porta configurada para o servidor TCP em cada ponto final é a mesma que a porta especificada para a verificação de integridade no Global Accelerator. Se os números de porta 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.

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.

> **Note**
>
> Não é possível 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.

InterHealth o de verificação

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

Contagem de limites

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

Cada ouvinte roteia solicitações somente para endpoints íntegros. Depois de adicionar um endpoint, ele deve passar por uma verificação de integridade para ser considerado íntegro. Após cada verificação de integridade ser concluída, o listener fechará a conexão estabelecida para a verificação de integridade.

Endpoints para aceleradores padrão no AWS Global Accelerator

Os endpoints para aceleradores padrão no AWS Global Accelerator podem ser Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços Elastic IP. Com aceleradores padrão, um endereço IP estático serve como um ponto único de contato para clientes e o Global Accelerator distribui o tráfego de entrada por endpoints íntegros. O Global Accelerator direciona o tráfego para endpoints usando a porta (ou intervalo de portas) especificada para o ouvinte ao qual pertence o grupo de pontos de extremidade do ponto de extremidade.

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

O Global Accelerator monitora continuamente a integridade de todos os endpoints incluídos em um grupo de terminais padrão. Ele roteia o tráfego somente para os endpoints ativos que estão íntegros. Se o Global Accelerator não tiver nenhum ponto de extremidade íntegro para o qual rotear o tráfego, ele encaminhará o tráfego para todos os endpoints.

Tenha em atenção o seguinte para tipos específicos de endpoints padrão do Global Accelerator:

Pontos finais do Load balancer

- Um endpoint do Application Load Balancer pode ser voltado para a Internet ou interno. Um ponto final do Network Load Balancer de Carga de Rede deve estar voltado para a Internet.

endpoints das instâncias do Amazon EC2

- Um endpoint de instância do EC2 (para aceleradores de roteamento padrão e personalizado) não pode ser um dos seguintes tipos: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, CG1, CG1, CG2, CG1, CG2, G1, G2, HI1, HS1, G1
- As instâncias do EC2 são compatíveis com endpoints em apenas algumas regiões da AWS. Para obter uma lista de regiões compatíveis, consulte Regiões da AWS compatíveis para preservação de endereço IP do cliente.
- Recomendamos que você remova uma instância do EC2 dos grupos de endpoint do Global Accelerator antes de encerrar a instância. Se você encerrar uma instância do EC2 antes de removê-la de um grupo de endpoint no Global Accelerator e, em seguida, criar outra instância na mesma VPC com o mesmo endereço IP privado e as verificações de saúde passarem, o Global Accelerator roteará o tráfego para o novo endpoint.

Tópicos

Adicionando, editando ou removendo um endpoint padrão

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

Os endpoints no Global Accelerator podem ser Network Load Balancers, Application Load Balancers, instâncias do Amazon EC2 ou endereços Elastic IP. Você deve criar um desses recursos primeiro e, em seguida, você pode adicioná-lo como um endpoint no Global Accelerator. Um recurso deve ser válido e estar ativo quando adicionado como um endpoint.

Você pode adicionar ou remover endpoints de grupos de endpoints com base no uso. Por exemplo, se a demanda em seu aplicativo aumentar, você pode criar mais recursos e, em seguida, adicionar mais endpoints a um ou mais grupos de endpoint para lidar com o aumento do tráfego. O Global Accelerator inicia as solicitações de roteamento para um endpoint assim que você o adiciona e o endpoint passa pelas 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.

Se você estiver adicionando um endpoint com preservação de endereço IP do cliente, primeiro revise as informações emRegiões da AWS compatíveis para preservação de endereço IP do clienteePreservar endereços IP do cliente no AWS Global Accelerator.

Você pode remover endpoints de seus grupos de endpoint, por exemplo, se precisar atender seus endpoints. Remover um endpoint o tira do grupo de endpoint, mas não afeta o endpoint de outra forma. O Global Accelerator pára de direcionar o tráfego para um ponto de extremidade assim que você o remove de um grupo de terminais. O ponto de extremidade entra em um estado em que aguarda que todas as solicitações atuais sejam concluídas para que não haja interrupção para o tráfego do cliente em andamento. Você pode adicionar o endpoint de volta ao grupo de endpoint quando estiver pronto para retomar o recebimento de solicitações.

Esta seção explica como trabalhar com endpoints no console do AWS Global Accelerator. Se você deseja usar operações de API com o AWS Global Accelerator, consulte oReferência da API do AWS Global Accelerator.

Para adicionar um endpoint padrão

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradoras do, escolha um acelerador.
3. NoListenersseção, paraID do listener, escolha o ID de um ouvinte.
4. NoGrupos de endpointsseção, paraID do grupo do endpoint, selecione o ID do grupo de endpoint ao qual você deseja adicionar um endpoint.
5. NoEndpoints doseção, escolhaAdicionar endpoint.
6. NoAdicionar endpoints, escolha um recurso na lista suspensa.

   Se você não tiver nenhum recurso da AWS do, não há nenhum item na lista. Para continuar, crie recursos da AWS, como balanceadores de carga, instâncias do Amazon EC2 ou endereços Elastic IP. Em seguida, volte para as etapas aqui e escolha um recurso na lista.

7. Opcionalmente, paraPeso, insira um número de 0 a 255 para definir um peso para rotear o tráfego para esse ponto de extremidade. Ao adicionar pesos a endpoints, você configura o Global Accelerator para rotear o tráfego com base nas proporções especificadas. Por padrão, todos os endpoints têm um peso de 128. Para obter mais informações, consulte Pesos de endpoints.
8. Opcionalmente, habilite a preservação do endereço IP do cliente para um endpoint do Application Load Balancer voltado para a Internet. SobPreserve o endereço IP do cliente, selecionePRESERVE endereço.

   Essa opção é sempre selecionada para endpoints internos de instância do Application Load Balancer e do EC2 e nunca selecionada para endpoints de endereço IP Elastic Load Balancer e Network Load Balancer. Para obter mais informações, consulte Preservar 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, são atualizadas para incluir o endereço IP do cliente do usuário nas listas de permissões.

9. Escolha Add endpoint.

Para editar um ponto de extremidade padrão

Você pode editar uma configuração de endpoint para alterar o peso. Para obter mais informações, consulte Pesos de endpoints.

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradoras do, escolha um acelerador.
3. NoListenersseção, paraID do listener, escolha o ID de um ouvinte.
4. NoGrupos de endpointsseção, paraID do grupo do endpoint, escolha o ID do grupo de endpoints.
5. SelecioneEdite endpoint.
6. NoEdite endpointpágina, faça atualizações e escolhaSave (Salvar).

Para remover um endpoint

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradoras do, escolha um acelerador.
3. NoListenersseção, paraID do listener, escolha o ID de um ouvinte.
4. NoGrupos de endpointsseção, paraID do grupo do endpoint, escolha o ID do grupo de endpoints.
5. SelecioneRemover ponto final.
6. Na caixa de diálogo de confirmação, escolhaRemover.

Pesos de endpoints

Um peso é um valor que determina a proporção de 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 Elastic IP. O Global Accelerator calcula a soma dos pesos dos pontos finais em um grupo de terminais e, em seguida, direciona o tráfego para os pontos finais com base na proporção entre o peso de cada endpoint e o total.

O roteamento ponderado permite que você escolha quanto tráfego é roteado para um recurso em um grupo de endpoint. Isso pode ser útil de várias maneiras, incluindo balanceamento de carga e teste de novas versões de um aplicativo.

Como funcionam os pesos de endpoint

Para usar pesos, você atribui a cada endpoint de um grupo de endpoint 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 para um peso, 255. O Global Accelerator envia o tráfego para um endpoint com base no peso que você atribui a ele como uma proporção do peso total para todos os endpoints no 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. 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 alterando os pesos. Se quiser que o Global Accelerator pare de enviar o tráfego para um endpoint, você pode alterar o peso desse recurso para 0.

Failover para endpoints não íntegros

Se não houver pontos finais íntegros em um grupo de endpoint com um peso maior que zero, o Global Accelerator tentará fazer failover para um endpoint íntegro com um peso maior do que zero em outro grupo de endpoint. Para esse failover, o Global Accelerator ignora a configuração de discagem de tráfego. Portanto, se, por exemplo, um grupo de terminais tiver uma discagem de tráfego definida como zero, o Global Accelerator ainda incluirá esse grupo de pontos de extremidade na tentativa de failover.

Se o Global Accelerator não encontrar um endpoint íntegro com um peso maior que zero depois de tentar três grupos de endpoint adicionais (ou seja, três regiões da AWS), ele roteará o tráfego para um endpoint aleatório no grupo de endpoint mais próximo do cliente. Isto é, éfalha ao abrir.

Observe o seguinte:

- O grupo de pontos de extremidade escolhido para failover pode ser aquele que tem uma discagem de tráfego definida como zero.
- O grupo de pontos finais mais próximo pode não ser o grupo de pontos finais original. Isso ocorre porque o Global Accelerator considera as configurações de discagem de tráfego de conta quando escolhe o grupo de endpoint original.

Por exemplo, digamos que sua configuração tenha dois endpoints, um íntegro e um iníntegro, e você definiu o peso para cada um deles para ser maior que zero. Nesse caso, o Global Accelerator roteia o tráfego para o endpoint íntegro. No entanto, agora digamos que você definiu o peso do único endpoint saudável como zero. Em seguida, o Global Accelerator tenta três grupos de terminais adicionais para encontrar um endpoint íntegro com um peso maior que zero. Se não encontrar um, o Global Accelerator encaminhará o tráfego para um ponto final aleatório no grupo de pontos de extremidade mais próximo do cliente.

Adicionando endpoints com preservação de endereço IP do cliente

Um recurso que você pode usar com alguns tipos de endpoint — em algumas Regiões— éPreservar endereço IP do cliente. Com esse recurso, você preserva o endereço IP de origem do cliente original para pacotes que chegam ao ponto de extremidade. Você pode usar esse recurso com endpoints de instância do Application Load Balancer e do Amazon EC2. Os pontos de extremidade em

aceleradores de roteamento personalizados sempre têm o endereço IP do cliente preservado. Para obter mais informações, consulte Preservar endereços IP do cliente no AWS Global Accelerator.

Se você pretende usar o recurso de preservação de endereço IP do cliente, esteja ciente do seguinte ao adicionar endpoints ao Global Accelerator:

Interfaces de rede elástica

Para oferecer suporte à 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 trabalha com interfaces de rede elástica, consultePráticas recomendadas para preservação do endereço IP do cliente.

Pontos de endpoints em sub-redes privadas

Você pode direcionar um Application Load Balancer ou uma instância do EC2 em uma sub-rede privada usando o AWS Global Accelerator, mas você deve ter umgateway de Internetanexado à VPC que contém os endpoints. Para obter mais informações, consulte Conexões seguras da VPC no AWS Global Accelerator.

Adiciona o endereço IP do cliente à lista de permissões

Antes de adicionar e começar a encaminhar o tráfego para pontos de extremidade que preservam o endereço IP do cliente, certifique-se de que todas as configurações de segurança necessárias, por exemplo, grupos de segurança, são atualizadas para incluir o endereço IP do cliente do usuário na lista de permissões. Lista de controle de acesso (ACLs) de rede se aplicam somente ao tráfego de saída (saída). Se você precisar filtrar o tráfego de entrada (entrada), você deve usar grupos de segurança.

Configurar listas de controle de acesso (ACLs)

As ACLs de rede associadas às sub-redes da VPC se aplicam ao tráfego de saída (saída) quando a preservação do endereço IP do cliente estiver habilitada no acelerador. No entanto, para que o tráfego possa sair por meio do 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 endpoint por meio do Global Accelerator, associe a sub-rede do endpoint a uma ACL de rede que permite o tráfego de saída destinado a uma porta TCP ou UDP efêmera (intervalo de portas 1024-65535, destino 0.0.0/0). Além disso, crie uma regra de entrada correspondente (intervalo de portas 1024-65535, origem 0.0.0.0/0).

> **Note**
>
> As regras do grupo de segurança e do AWS WAF são um conjunto adicional de recursos que você pode aplicar para proteger seus recursos. Por exemplo, as regras de grupo de segurança de entrada associadas às instâncias do Amazon EC2 e Application Load Balancers permitem controlar 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. Observe que os security groups de instâncias do Amazon EC2 se aplicam a qualquer tráfego que chegue às suas instâncias, incluindo tráfego do Global Accelerator e qualquer endereço público ou Elastic IP atribuído à sua instância. Como prática recomendada, use sub-redes privadas se quiser garantir que o tráfego seja entregue somente pelo Global Accelerator. Certifique-se também de que as regras de grupo de segurança de entrada estão configuradas apropriadamente para permitir ou negar tráfego corretamente para seus aplicativos.

Transição de pontos de extremidade para usar a preservação do endereço IP do cliente

Siga as orientações nesta seção para fazer a transição de um ou mais endpoints no acelerador para endpoints que preservam o endereço IP do cliente do usuário. Opcionalmente, você pode optar por fazer a transição de um endpoint do Application Load Balancer ou de um endpoint do endereço Elastic IP para um ponto final correspondente — um Application Load Balancer ou uma instância do EC2 — que tenha preservação do endereço IP do cliente. Para obter mais informações, consulte Preservar endereços IP do cliente no AWS Global Accelerator.

Recomendamos que você mude para usar a preservação do endereço IP do cliente lentamente. Primeiro, adicione novos endpoints de instância do Application Load Balancer ou EC2 que você habilita para preservar o endereço IP do cliente. Em seguida, mova lentamente o tráfego de endpoints existentes para os novos endpoints configurando pesos nos endpoints.

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

A preservação do endereço IP do cliente está disponível apenas em regiões específicas da AWS. Para obter mais informações, consulte Regiões da AWS compatíveis para preservação de endereço IP do cliente.

Esta seção explica como trabalhar com grupos de endpoint no console do AWS Global Accelerator. Se quiser usar as operações da API do Global Accelerator, consulte oReferência da API do AWS Global Accelerator.

Depois de mover uma pequena quantidade de tráfego para o novo ponto de extremidade com preservação de endereço IP do cliente, teste para se certificar de que a configuração está funcionando como esperado. Em seguida, aumente gradualmente a proporção de tráfego para o novo endpoint ajustando os pesos nos pontos finais correspondentes.

Para fazer a transição para endpoints que preservam endereços IP do cliente, comece seguindo as etapas aqui para adicionar um novo endpoint e, para os pontos de extremidade do Application Load Balancer voltados para a Internet, habilite a preservação do endereço IP do cliente. (A opção de preservação do endereço IP do cliente é sempre selecionada para instâncias internas do Application Load Balancers e EC2.)

Para adicionar um endpoint com preservação de endereço IP do cliente

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradoras do, escolha um acelerador.
3. NoListenersseção, escolha um listener.
4. NoGrupo de endpointsseção, escolha um grupo de endpoints.
5. NoEndpoints doseção, escolhaAdicionar endpoint.
6. NoAdicionar endpointspágina, noEndpoints do, escolha um endpoint do Application Load Balancer ou um endpoint da instância do EC2.
7. NoPeso, escolha um número baixo em comparação com os pesos definidos para os 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 obter mais informações, consulte Pesos de endpoints.
8. Para um novo endpoint do Application Load Balancer voltado para o exterior, emPreserve o endereço IP do cliente, selecionePRESERVE endereço. (Essa opção é sempre selecionada para instâncias internas do Application Load Balancers e EC2.)
9. Selecione Save changes (Salvar alterações).

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

Para reduzir o tráfego para os endpoints existentes

1. NoGrupo de endpoints, escolha um endpoint existente que não tenha preservação de endereço IP do cliente.
2. Selecione Edit.
3. NoEdite endpointpágina, noPeso, insira um número menor 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. Selecione Save changes (Salvar alterações).

Depois de testar com uma pequena parte do tráfego original definindo o peso do novo ponto de extremidade para um número baixo, você pode fazer a transição lenta de todo o tráfego continuando a ajustar os pesos dos pontos finais originais e novos.

Por exemplo, digamos que você comece com um Application Load Balancer existente com um peso definido como 200 e adicione um novo ponto de extremidade do Application Load Balancer com a preservação do endereço IP do cliente ativada 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/novo peso 10
- Peso original 180/novo peso 20
- Peso original 170/novo peso 30, e assim por diante.

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

Se você tiver pontos de extremidade adicionais — Application Load Balancers ou instâncias do EC2 — que deseja fazer a transição para usar a preservação do endereço IP do cliente, repita as etapas nesta seção para fazer a transição deles.

Se você 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 quenãotêm a preservação do endereço IP do cliente para o valor original e diminuir o peso do ponto de extremidadeporpreservação do endereço IP do cliente para 0.

Trabalhar com aceleradores de roteamento personalizados no AWS Global Accelerator

Este capítulo inclui procedimentos e recomendações para a criação de aceleradores de roteamento personalizados no AWS Global Accelerator. 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 muitos destinos, ao mesmo tempo em que obtém melhorias de desempenho ao rotear seu tráfego através do Global Accelerator. Isso é útil quando você tem um aplicativo que exige que um grupo de usuários interaja uns com os outros na mesma sessão em execução em uma instância e porta específicas do EC2, como aplicativos de jogos ou sessões VoIP (VoIP).

Os endpoints para aceleradores de roteamento personalizados devem ser sub-redes de nuvem privada virtual (VPC), e um acelerador de roteamento personalizado só pode rotear o 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 única ou várias sub-redes da VPC. Para saber mais, consulte Como os aceleradores de roteamento personalizados funcionam no AWS Global Accelerator.

Se você quiser que o Global Accelerator escolha automaticamente o endpoint íntegro mais próximo de seus clientes, crie um acelerador padrão. Para obter mais informações, consulte Trabalhar com aceleradores padrão no AWS Global Accelerator.

Para configurar o acelerador de roteamento personalizado, faça o seguinte:

1. Revise as diretrizes e requisitos para criar um acelerador de roteamento personalizado. Consulte Diretrizes e restrições para aceleradores de roteamento personalizados.
2. Crie uma sub-rede da 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 e selecione a opção de um acelerador de roteamento personalizado.
4. Adicione um ouvinte e especifique um intervalo de portas para que o Global Accelerator ouça. Certifique-se de incluir um grande alcance 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 listener, consulteDiretrizes e restrições para aceleradores de roteamento personalizados.

5. Adicione um ou mais grupos de endpoint para regiões da AWS nas quais você tem sub-redes da VPC. Para cada grupo de endpoints, especifique o seguinte:
   - 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 de ponto final, selecione um ID de sub-rede. Você pode adicionar várias sub-redes em cada grupo de endpoint e as sub-redes podem ter tamanhos diferentes (até /17).

As seções a seguir passam pelo trabalho com aceleradores de roteamento, ouvintes, grupos de endpoint e endpoints personalizados.

Tópicos

Como os aceleradores de roteamento personalizados funcionam no AWS 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 intervalos de portas de ouvinte para destinos de instância do EC2 em sub-redes de nuvem privada virtual (VPC). Isso permite que o Global Accelerator encaminhe deterministicamente o tráfego para um endereço IP privado específico do Amazon EC2 e um destino de porta 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 escolhidos, como localização geográfica,

habilidade do jogador e modo de jogo. Ou você pode ter um aplicativo VoIP ou de mídia social que atribui 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 seus endereços IP e portas de destino associados. Você pode salvar esse mapeamento estático e, em seguida, seu serviço de matchmaking usá-lo para rotear usuários para instâncias específicas do EC2 de destino. Você não precisa fazer modificações para seu software cliente para começar a usar Global Accelerator com seu aplicativo.

Para configurar um acelerador de roteamento personalizado, selecione um endpoint de sub-rede da 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 um número de porta de uma sessão para um endereço IP externo e uma porta que você fornece aos usuários.

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

> **Note**
>
> Por padrão, todos os destinos de sub-rede da VPC em um acelerador de roteamento personalizado não têm permissão para receber tráfego. Isso deve ser seguro por padrão e também para fornecer controle granular sobre quais destinos de instância privada do EC2 em sua sub-rede têm permissão para receber tráfego. Você pode permitir ou negar tráfego para a sub-rede ou para combinações específicas de endereços IP e portas (soquetes de destino). Para obter mais informações, consulte Adicionando, editando ou removendo um endpoint de sub-rede da VPC. Você também pode especificar destinos usando a API do Global Accelerator. Para obter mais informações, consulteallowCustomRoutingTrafeDenyCustomRoutingTraffic.

Exemplo de como o roteamento personalizado funciona no Global Accelerator

Por exemplo, digamos que você queira oferecer suporte a 10.000 sessões em que grupos de usuários interagem, como sessões de jogos ou sessões de chamada VoIP, em 1.000 instâncias do Amazon EC2 atrás do Global Accelerator. Neste exemplo, especificaremos um intervalo de portas de ouvinte de 10001—20040 e um intervalo de portas de destino de 81—90. Vamos dizer que temos as quatro sub-redes VPC em us-east-1: sub-net-1, sub-net-2, sub-net-3 e sub-net-4.

Em nossa configuração de exemplo, cada sub-rede da VPC tem um tamanho de bloco de /24 para que possa suportar 251 instâncias do Amazon EC2. (Cinco endereços são reservados e indisponíveis de cada sub-rede, e esses endereços não são mapeados.) Cada servidor em execução em cada instância do EC2 atende às 10 portas a seguir especificadas para as portas de destino em nosso grupo de endpoint: 81-90. 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 associa-as internamente a 10 portas de ouvinte que você pode usar para acessar instâncias do EC2. Para ilustrar isso simplesmente, diremos que há um bloco de portas de ouvinte que começa com o primeiro endereço IP da sub-rede de ponto final para o primeiro conjunto de 10 e, em seguida, passa para o próximo endereço IP para o próximo conjunto de 10 portas de ouvinte.

> **Note**
>
> O mapeamento não é previsível assim, mas estamos usando um mapeamento sequencial aqui para ajudar a mostrar como funciona o mapeamento de portas. Para determinar o mapeamento real para os intervalos de portas do ouvinte, use as seguintes operações de API: ListCustomRoutingPortMappingseListCustomRoutingPortMappingsByDestination.

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

Porta do ouvinte Global Accelerator	Sub-rede VPC	Porta da 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
10017	192.0.2.5	87
10018	192.0.2.5	88
10019	192.0.2.5	89

Porta do ouvinte Global Accelerator	Sub-rede VPC	Porta da instância do EC2
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
12516	192.0.3.4	86
12517	192.0.3.4	87
12518	192.0.3.4	88

Porta do ouvinte Global Accelerator	Sub-rede VPC	Porta da instância do EC2
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, tenha em mente as seguintes diretrizes e restrições.

Destinos da instância do Amazon EC2

Os endpoints de sub-rede de Virtual Public Cloud (VPC) em um acelerador de roteamento personalizado podem incluir somente instâncias do EC2. Nenhum outro recurso, como balanceadores de carga, é suportado para o acelerador de roteamento personalizado.

Os tipos de instâncias do EC2 compatíveis com o Global Accelerator estão listados emEndpoints para aceleradores padrão no AWS Global Accelerator.

Mapeamentos de porta

Quando você adiciona uma sub-rede da VPC, o Global Accelerator cria um mapeamento de portas estáticas de intervalos de portas do ouvinte para os intervalos de portas suportados pela sub-rede. O mapeamento de porta para uma sub-rede específica nunca muda.

Você pode exibir programaticamente a lista de mapeamento de porta para um acelerador de roteamento personalizado. Para obter mais informações, consulte `ListCustomRoutingPortMappings`.

Tamanho da sub-rede da VPC

As sub-redes da VPC adicionadas a um acelerador de roteamento personalizado devem ter um mínimo de /28 e um máximo de /17.

Faixas de porta do ou

Você deve especificar portas de ouvinte suficientes, especificando intervalos de portas de ouvinte, para acomodar o número de destinos incluídos nas sub-redes que você planeja adicionar

ao acelerador de roteamento personalizado. O intervalo que você especifica ao criar um ouvinte determina quantas combinações de portas de ouvinte e endereços IP de destino podem ser usadas com o acelerador de roteamento personalizado. Para obter flexibilidade máxima e reduzir a possibilidade de obter um erro de que você não tem portas de ouvinte 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 intervalos de portas de ouvinte linearmente e torne os intervalos grandes o suficiente para suportar 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 vezes o 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 porta pode exigir que você adicione mais portas de ouvinte, além desse total.

Depois de criar um ouvinte, você pode editá-lo para adicionar intervalos de portas adicionais e protocolos associados, mas não pode diminuir intervalos de portas existentes. Por exemplo, se você tiver um intervalo de portas de ouvinte de 5.000 a 10.000, não poderá alterar o intervalo de portas para 5900—10.000 e não poderá alterar o intervalo de portas para 5.000—9.900.

Cada intervalo de portas de ouvinte deve incluir um mínimo de 16 portas. Os listeners suportam portas 1-65535.

Intervalos de porta

Há dois locais que você especifica intervalos de portas para um acelerador de roteamento personalizado: os intervalos de portas que você especifica quando adiciona um listener e os intervalos de portas de destino e protocolos especificados para um grupo de pontos finais.

- Faixas de porta do ouvinte As portas do listener 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 exclusivo e uma porta em uma sub-rede VPC atrás do acelerador.
- Os intervalos de portas de destino: Os conjuntos de intervalos de portas de destino especificados para um grupo de endpoint (também chamados de configurações de destino) são as portas de instância do EC2 que recebem tráfego. Para receber tráfego nas portas de

destino, os grupos de segurança associados às instâncias do EC2 devem permitir o tráfego nelas.

Verificações de Health e failover

O Global Accelerator não executa verificações de integridade para aceleradores de roteamento personalizados e não faz failover para endpoints íntegros. O tráfego para aceleradores de roteamento personalizados é roteado deterministicamente, 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, alternativamente, permitir o tráfego para endereços IP de instância específicos e portas 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 o método`DescribeCustomRoutingAccelerator`Ação da API 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

Aacelerador de roteamento personalizadono 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 sendo executadas 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 AWS Global Accelerator](#).

Quando você cria um acelerador, por padrão, o Global Accelerator fornece um conjunto de dois endereços IP estáticos. Se você trazer seu próprio intervalo de endereços IP para a AWS (BYOIP), poderá atribuir endereços IP estáticos de seu próprio grupo para usar com o acelerador. Para obter mais informações, consulte Traga seus próprios endereços IP (BYOIP) no AWS Global Accelerator.

> **Important**
>
> Os endereços IP são atribuídos ao acelerador enquanto ele existir, mesmo se você desativar o acelerador e ele não aceitar ou rotear o tráfego. No entanto, quando vocêdeleteum acelerador, você perde os endereços IP estáticos do Global Accelerator atribuídos ao acelerador, para que você não possa mais rotear o tráfego usando-os. Como prática recomendada, certifique-se de que você tenha permissões em vigor para evitar excluir aceleradores inadvertidamente. Você pode usar políticas do IAM, como permissões baseadas em tags com o Global Accelerator, para limitar os usuários que têm permissões para excluir um acelerador. Para obter mais informações, consulte Políticas baseadas em tag.

Esta seção explica como criar, editar ou excluir 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 oReferência da API do AWS Global Accelerator.

Tópicos

- Criando ou atualizando um acelerador de roteamento personalizado
- Visualizando seus aceleradores de roteamento personalizados
- Excluindo um acelerador de roteamento personalizado

Criando ou atualizando um acelerador de roteamento personalizado

Para criar um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. SelecioneCriar acelerador.
3. Forneça um nome para o acelerador.
4. para oTipo de acelerador ador, selecioneRotear rotas personalizadas.

5. Opcionalmente, se você trouxe seu próprio intervalo de endereços IP para a AWS (BYOIP), poderá especificar endereços IP estáticos para o acelerador a partir desse pool de endereços. Faça essa escolha para cada um dos dois endereços IP estáticos do seu acelerador.

   - Para cada endereço IP estático, escolha o pool 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 escolher o pool de endereços IP padrão da Amazon, o Global Accelerator atribuirá um endereço IP específico ao acelerador.

6. Como alternativa, adicione uma ou mais tags para ajudá-lo a identificar seus recursos acelerador.
7. SelecionePróximopara ir para as próximas páginas do assistente para adicionar ouvintes, grupos de endpoint e pontos de extremidade de sub-rede da VPC.

Para editar um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Na lista de aceleradores de roteamento personalizados, escolha um e escolhaEdite.
3. NoEditar acelerador deFaça as alterações desejadas. Por exemplo, você pode desativar o acelerador para que você possa excluí-lo.
4. Escolha Save (Salvar).

Visualizando seus aceleradores de roteamento personalizados

Você pode criar um acelerador de roteamento personalizado no console da. Para ver descrições de seus aceleradores de roteamento personalizados programaticamente, consulteListCustomRoutingAcceleratoreDescribeCustomRoutingAcceleratorNa Referência da API do AWS Global Accelerator.

Para exibir informações sobre seus aceleradores de roteamento personalizados

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Para ver detalhes sobre um acelerador, escolha um acelerador e, em seguida, escolha um acelerador.Exibir.

Excluindo um acelerador de roteamento personalizado

Se você criou um acelerador de roteamento personalizado como um teste ou se não estiver mais usando um acelerador, poderá excluí-lo. No console, desative o acelerador e, em seguida, você pode excluí-lo. Não é necessário remover ouvintes e grupos de endpoint do acelerador.

Para excluir um acelerador de roteamento personalizado usando uma operação de API em vez do console, primeiro você deve remover todos os listeners e grupos de endpoint associados ao acelerador e, em seguida, desativá-lo. Para obter mais informações, consulte o .DeleteAcceleratoroperação emReferência da API do AWS Global Accelerator.

Para desativar um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Na lista, escolha um acelerador que você deseja desativar.
3. Selecione Edit.
4. SelecioneDesabilitar aceleradore, em seguida, escolhaSave (Salvar).

Para excluir um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. Na lista, escolha um acelerador que você deseja excluir.
3. Escolha Delete (Excluir).

> **Note**
>
> Se você não tiver desativado o acelerador,ExcluirEstá indisponível. Para desativar o acelerador, consulte o procedimento anterior.

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

> **Important**
>
> Quando você exclui um acelerador, você perde os endereços IP estáticos atribuídos ao acelerador, para que você não possa mais rotear o tráfego usando-os.

Ouvintes para aceleradores de roteamento personalizados no AWS Global Accelerator

Para um acelerador de roteamento personalizado no AWS Global Accelerator, você configura um listener que especifica um intervalo de portas de ouvinte 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 de portas estáticas entre os intervalos de portas que você define para o ouvinte e os endereços IP de destino e as portas na sub-rede. Em seguida, você pode usar o mapeamento de portas para especificar seus endereços IP estáticos do acelerador juntamente com uma porta de ouvinte e um protocolo para direcionar o tráfego do usuário para endereços IP e portas de instância do Amazon EC2 de destino específico em sua sub-rede da VPC.

Você define um listener ao criar seu acelerador de roteamento personalizado e você pode adicionar mais listeners a qualquer momento. Cada ouvinte pode ter um ou mais grupos de endpoint, um para cada região da AWS na qual você tem endpoints de sub-rede da VPC. Um ouvinte em um acelerador de roteamento personalizado suporta 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 obter mais informações, consulte Como os aceleradores de roteamento personalizados funcionam no AWS Global Accelerator.

Adicionando, editando ou removendo um listener de roteamento personalizado

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

Para adicionar um listener para um acelerador de roteamento personalizado

O intervalo que você especifica ao criar um listener define quantas combinações de portas de ouvinte e endereços IP de destino podem ser usadas com o acelerador de roteamento personalizado. Para flexibilidade máxima, recomendamos que você especifique um grande intervalo de portas. Cada intervalo de portas do listener especificado deve incluir um mínimo de 16 portas.

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

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradores, escolha um acelerador de roteamento personalizado.
3. Escolha Add listener.
4. NoAdicionar listener, informe o intervalo de portas do listener que você deseja associar ao acelerador.

   Listeners suportam portas 1-65535. Para obter máxima flexibilidade com um acelerador de roteamento personalizado, recomendamos que você especifique um grande intervalo de portas.
5. Escolha Add listener.

Para editar um listener para um acelerador de roteamento personalizado

Ao editar um ouvinte para um acelerador de roteamento personalizado, esteja ciente de que você pode adicionar intervalos de portas adicionais e protocolos associados, aumentar intervalos de portas existentes ou alterar protocolos, mas não pode diminuir intervalos de portas existentes.

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradores, escolha um acelerador.
3. Escolha um listener e, em seguida, escolhaEditar listener.
4. NoEditar listener, faça as alterações desejadas nos intervalos de portas ou protocolos existentes ou adicione novos intervalos de portas.

   Lembre-se de que não é possível diminuir o intervalo de um intervalo de portas existente.
5. Escolha Save (Salvar).

Para remover um listener

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradores, escolha um acelerador.
3. Escolha um listener e, em seguida, escolhaRemover.
4. Na caixa de diálogo de confirmação, escolhaRemover.

Grupos de endpoints para aceleradores de roteamento personalizados no AWS Global Accelerator

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

Você cria um grupo de endpoint para o 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 endpoint 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 endpoint, mas os grupos de endpoint devem estar associados a ouvintes diferentes.

Para cada grupo de endpoint, você especifica um conjunto de um ou mais intervalos de portas que incluem as portas para as quais deseja direcionar o tráfego nas instâncias do EC2 na região. Para cada intervalo de portas do grupo de ponto final, você especifica o protocolo a ser usado: UDP, TCP ou UDP e TCP. Isso fornece 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 executando sobre UDP nas portas 8080-8090, enquanto você também tem um servidor escutando mensagens de bate-papo por TCP na porta 80.

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

Adicionar, editar ou remover um grupo de endpoints para um acelerador de roteamento personalizado

Você trabalha com um grupo de endpoint 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 trabalhar com grupos de endpoint 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 oReferência da API do AWS Global Accelerator.

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

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradores, escolha um acelerador de roteamento personalizado.
3. NoListenersseção, paraID do listener, escolha o ID do listener ao qual você deseja adicionar um grupo de endpoints.
4. SelecioneAdicionar grupo de endpoints.
5. Na seção de um listener, especifique uma Região para o grupo de endpoint.
6. para oConjuntos de portas e protocolos, insira intervalos de portas e protocolos para suas instâncias do Amazon EC2.

   - Digite umA partir da portae umPara a portabilidadePara especificar um intervalo de portas.
   - Para cada intervalo de portas, especifique o protocolo ou protocolos para esse intervalo.

   O intervalo de portas não precisa ser um subconjunto do intervalo de portas do ouvinte, mas deve haver portas totais suficientes no intervalo de portas do listener para suportar o número total de portas que você especifica para os grupos de endpoint no acelerador de roteamento personalizado.
7. Escolha Save (Salvar).
8. Opcionalmente, escolhaAdicionar grupo de endpointsPara adicionar grupos de endpoints adicionais para este listener. Você também pode escolher outro ouvinte e adicionar grupos de endpoint.
9. SelecioneAdicionar grupo de endpoints.

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

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradores, escolha um acelerador de roteamento personalizado.
3. NoListenersseção, paraID do listener, escolha o ID do listener ao qual o grupo de endpoints está associado.
4. SelecioneEditar grupo de endpoints.
5. NoEditar grupo de endpoints, altere a Região, o intervalo de portas ou o protocolo para um intervalo de portas.
6. Escolha Save (Salvar).

Para remover um acelerador de roteamento personalizado

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradores, escolha um acelerador.
3. NoListeners, escolha um listener e, depois,Remover.
4. NoGrupos de endpoints, escolha um grupo de endpoints e, depois,Remover.
5. Na caixa de diálogo de confirmação, escolhaRemover.

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

Os pontos de extremidade para aceleradores de roteamento personalizados são sub-redes de nuvem privada virtual (VPC) 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 ponto de extremidade de sub-rede, o Global Accelerator gera um novo mapeamento de porta. Em seguida, você pode usar a API do Global Accelerator para obter uma lista estática de todos os mapeamentos de porta para a sub-rede, que você pode usar para rotear o tráfego para endereços IP de instância do EC2 de destino na sub-rede. Para obter mais informações, consulteListCustomRoutingPortMappings.

Você só pode direcionar o tráfego para instâncias do EC2 nas sub-redes, não para outros recursos, como balanceadores de carga (em contraste com aceleradores padrão). Os tipos de instância do EC2 suportados estão listados emEndpoints para aceleradores padrão no AWS Global Accelerator.

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

Esteja ciente do seguinte ao adicionar sub-redes da VPC para o acelerador de roteamento personalizado:

- Por padrão, o tráfego direcionado por meio de um acelerador de roteamento personalizado não pode chegar a nenhum destino em 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, alternativamente, habilitar o tráfego para endereços IP de instância específicos e portas (soquetes 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 chamar o método`DescribeCustomRoutingAccelerator`Ação da API para verificar o status do acelerador. Para obter mais informações, consulteDescribeCustomRoutingAccelerator.

- Como as sub-redes da VPC preservam o endereço IP do cliente, você deve revisar as informações relevantes de segurança e configuração ao adicionar sub-redes como pontos de extremidade para aceleradores de roteamento personalizados. Para obter mais informações, consulte Adicionando endpoints com preservação de endereço IP do cliente.

Adicionando, editando ou removendo um endpoint de sub-rede da VPC

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

Quando você adiciona e remove instâncias do EC2 da sub-rede, ou habilita ou desabilita o tráfego para destinos do EC2, você altera se esses destinos podem receber tráfego. No entanto, o mapeamento de porta do Global Accelerator não é alterado.

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

Você pode remover a sub-rede da VPC do acelerador removendo-a de um grupo de endpoint. A remoção de uma sub-rede não afeta a própria sub-rede, 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 porta para a sub-rede da VPC para potencialmente usá-los para novas sub-redes adicionadas.

As etapas desta seção explicam como adicionar, editar ou remover endpoints de sub-rede da VPC no console do AWS Global Accelerator. Para saber mais sobre o uso de operações de API com o AWS Global Accelerator, consulte oReferência da API do AWS Global Accelerator.

Para adicionar um ponto de extremidade de sub-rede da VPC

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradores, escolha um acelerador de roteamento personalizado.
3. NoListenersseção, paraID do listener, escolha o ID de um ouvinte.
4. NoGrupos de endpointsseção, paraID do grupo de endpoint, escolha o ID do grupo de endpoint (região da AWS) ao qual você deseja adicionar o endpoint de sub-rede da VPC.
5. NoEndpoints doseção, selecioneAdicionar endpoint.
6. NoAdicionar endpoints, paraEndpoint, escolha uma sub-rede da VPC.

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

Para permitir ou negar tráfego para destinos específicos

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

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradores, escolha um acelerador de roteamento personalizado.
3. NoListenersseção, paraID do listener, escolha o ID de um ouvinte.
4. NoGrupos de endpointsseção, paraID do grupo de endpoint, escolha o ID do grupo de endpoint (região da AWS) do endpoint de sub-rede da VPC que você deseja editar.
5. Selecione uma sub-rede de terminal e escolhaView details (Visualizar os detalhes).
6. NoEndpointpágina, emMapeamentos de porta, escolha um endereço IP e depois selecioneEdite.
7. Insira as portas para as quais deseja habilitar o tráfego e selecionePermitir estes 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 emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradores, escolha um acelerador de roteamento personalizado.
3. NoListenersseção, paraID do listener, escolha o ID de um ouvinte.
4. NoGrupos de endpointsseção, paraID do grupo de endpoint, escolha o ID do grupo de endpoint (região da AWS) do endpoint de sub-rede da VPC que você deseja atualizar.
5. SelecionePermissão/Negação de todo tráfego.
6. Escolha uma opção, para permitir todo o tráfego ou negar todo o tráfego e, em seguida, escolhaSave (Salvar).

Para remover um endpoint

1. Abra o console do Global Accelerator emhttps://console.aws.amazon.com/globalaccelerator/home.
2. NoAceleradores, escolha um acelerador de roteamento personalizado.

3. NoListenersseção, paraID do listener, escolha o ID de um ouvinte.
4. NoGrupos de endpointsseção, paraID do grupo de endpoint, escolha o ID do grupo de endpoint (região da AWS) do endpoint de sub-rede da VPC que você deseja remover.
5. SelecioneRemover ponto final.
6. Na caixa de diálogo de confirmação, escolhaRemover.

Endereçamento DNS e domínios personalizados no AWS Global Accelerator

Este capítulo explica como o AWS Global Accelerator faz roteamento de DNS e inclui informações sobre o uso de um domínio personalizado com o Global Accelerator.

Tópicos

Support para endereçamento DNS no Global Accelerator

Quando você cria um roteamento personalizado ou acelerador padrão, o Global Accelerator provisiona dois endereços IP estáticos para você. Ele também atribui um nome de Domain Name System (DNS, sistema de nome de domínios) padrão ao seu acelerador, semelhante `aa1234567890abcdef.awsglobalaccelerator.com`, que aponta para os endereços IP estáticos. Os endereços IP estáticos são anunciados globalmente usando anycast da rede de borda da AWS para seus endpoints. Você pode usar os endereços IP estáticos do acelerador ou o nome DNS para rotear o tráfego para o acelerador. Os servidores DNS e os resolvedores DNS usam um round robin para resolver o nome DNS de um acelerador, de modo que o nome seja resolvido para os endereços IP estáticos do acelerador, retornados pelo Amazon Route 53 em ordem aleatória. Os clientes normalmente usam o primeiro endereço IP que é retornado.

> **Note**
>
> O Global Accelerator cria dois registros de Pointer (PTR) que mapeiam os endereços IP estáticos de um acelerador para o nome DNS correspondente gerado pelo Global Accelerator, para suportar a pesquisa inversa de DNS. Isso também é conhecido como uma zona hospedada reversa. Lembre-se de que o nome DNS que o Global Accelerator gera para você não é configurável e não é possível criar registros PTR que apontam 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).

Encaminhe 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 o acelerador, em vez de usar os endereços IP estáticos atribuídos ou o nome DNS padrão. Primeiro, usando o Amazon Route 53 ou outro provedor DNS, crie um nome de domínio e, em seguida, adicione ou atualize registros DNS com seus endereços IP do Global Accelerator. Ou você pode associar seu nome de domínio personalizado ao nome DNS do acelerador. Conclua a configuração do DNS e aguarde até que as alterações se propaguem pela Internet. Agora, quando um cliente faz uma solicitação usando seu nome de domínio personalizado, o servidor DNS o resolverá para os endereços IP, em ordem aleatória, ou para o nome DNS para seu acelerador.

Para usar seu nome de domínio personalizado com o Global Accelerator ao usar o Route 53 como seu serviço DNS, crie um registro de alias que aponte seu nome de domínio personalizado para o nome 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`e para subdomínios, como`www.example.com`. Para obter mais informações, consulteEscolher entre registros de alias e não aliasNo 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 tópico a seguir: Alvo do aliasNo Guia do desenvolvedor do Amazon Route 53. Para ver as informações sobre o Global Accelerator, role para baixo na guiaAlvo do alias.

Traga seus próprios endereços IP (BYOIP) no AWS Global Accelerator

O AWS Global Accelerator usa endereços IP estáticos como pontos de entrada para seus aceleradores. Esses endereços IP são anycast de pontos de presença da AWS. Por padrão, o Global Accelerator fornece endereços IP estáticos doGrupo 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.

É possível trazer parte ou todo o intervalo de endereços IPv4 públicos da rede local para sua conta da AWS para uso com o Global Accelerator. Você continua a ter os intervalos de endereços, mas a AWS os anuncia na Internet.

Você não pode usar os endereços IP que você traz para a AWS para um serviço da AWS com outro serviço. As etapas neste capítulo descrevem como trazer seu próprio intervalo de endereços IP para uso somente no AWS Global Accelerator. Para obter as etapas para trazer seu próprio intervalo de endereços IP para uso no Amazon EC2, consulteTraga 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 for multihomed (ou seja, o intervalo é anunciado por vários provedores de serviços ao mesmo tempo), não podemos garantir que o tráfego para o intervalo de endereços entre em nossa rede ou que seu fluxo de trabalho de publicidade BYOIP será concluído com êxito.

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

Tópicos

Requirements

Você pode trazer 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 em um dos seguintes registros de Internet regionais (RIRs): o American Registry for Internet Numbers (ARIN) ou o Réseaux IP Européens Network Coordination Centre (RIPE) ou o Asia-Pacific Network Information Centre (APNIC). O intervalo de endereços deve ser registrado como uma entidade empresarial ou institucional. Ele não pode ser registrado como um indivíduo.
- O intervalo de endereços mais específico que pode ser trazido é /24. Os primeiros 24 bits do endereço IP especificam o número da rede. Por exemplo, 198.51.100 é o número de 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 má reputação 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 tenha 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:`Direct Allocation`e`Direct Assignment`Tipos de rede
- MADURA:`ALLOCATED PA`,`LEGACY`, e`ASSIGNED PI`Status de alocação
- APNIC:`ALLOCATED PORTABLE`e`ASSIGNED PORTABLE`Status de alocação

Preparar-se para levar seu intervalo de endereços IP para sua conta da AWS: Autorização

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

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

> **Note**
>
> Quando você usa o BYOIP para trazer um intervalo de endereços IP para a AWS, não é possível transferir a propriedade desse intervalo de endereços para uma conta ou empresa diferente enquanto o publicamos. Você também não pode transferir diretamente um intervalo de endereços IP de uma conta da AWS para outra conta. Para transferir a propriedade ou para 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 sua conta da AWS.

Para autorizar a Amazon a anunciar o intervalo de endereços IP, forneça à Amazon uma mensagem de autorização assinada. Use uma Autorização de Origem de Rota (ROA) para fornecer essa autorização. Um ROA é uma declaração de criptografia sobre os anúncios de sua rota que você cria por meio de seu Regional Internet Registry (RIR). Um ROA contém o intervalo de endereços IP, os números de sistema autônomo (ASNs) com permissão para anunciar o intervalo de endereços IP e uma data de expiração. O ROA autoriza a Amazon a anunciar um intervalo de endereços IP em um sistema autônomo (AS) específico.

Um 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 apresentam etapas detalhadas para concluir essas tarefas de autorização. Os comandos nestas etapas são aceitos no Linux. Se você usa o Windows, você pode acessar o Subssistema Windows para Linux para executar comandos do Linux.

Etapas para fornecer autorização

- Etapa 1: Criar um objeto ROA
- Etapa 2: Criar um certificado autoassinado X.509
- 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 seu intervalo de endereços IP, bem como os ASNs atualmente autorizados a anunciar o intervalo de endereços IP. O ROA deve conter o endereço IP /24 que você deseja levar para a AWS e você 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
- MADURA: Gerenciamento de ROAs
- APNIC: Gerenciamento de rotas

Etapa 2: Criar um certificado autoassinado X.509

Crie um key pair e um certificado X.509 autoassinado e adicione o certificado ao registro RDAP para seu RIR. As etapas a seguir descrevem como executar essas tarefas.

> **Note**
>
> Oopenssl Esses passos requerem o OpenSSL versão 1.0.2 ou posterior.

Para criar e adicionar um certificado X.509

1. Gere um key pair RSA de 2048 bits usando o seguinte comando.

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

2. Crie um certificado X.509 público a partir do key pair 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, defina o `-days` para o valor desejado para a expiração correta. Quando forem solicitadas outras informações, aceite 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. Exibir seu certificado usando o comando a seguir.

      ```
      cat publickey.cer
      ```

   2. Adicione o certificado fazendo o seguinte:

      > **Important**
      >
      > Certifique-se de incluir o`-----BEGIN CERTIFICATE-----`e`-----END CERTIFICATE-----`Do certificado.

      - No ARIN, inclua o certificado no`Public Comments`Para obter o intervalo de endereços IP.
      - No RIPE, inclua o certificado como um novo`descr`Para o intervalo de endereços IP.
      - Para APNIC, envie a chave pública por e-mail para`helpdesk@apnic.net`O contato autorizado da APNIC para os endereços IP, para solicitar que eles o adicionem manualmente ao`remarks`field.

Etapa 3: Criar uma mensagem de autorização assinada

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

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

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

Para criar a mensagem de autorização assinada

1. Crie uma mensagem de autorização de texto não criptografado e armazene-a em uma variável chamada`text_message`, como mostra o 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 key pair que você criou na seção anterior.
3. Armazena a mensagem em uma variável chamada`signed_message`, como mostra o 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 AWS 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 autoriza a a Amazon a anunciá-lo. Vamos verificar 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 seguinteProvisionByoipCIDRComando da. O`--cidr-authorization-context`O parâmetro usa as variáveis criadas na seção anterior, não a mensagem ROA.

```
aws globalaccelerator 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 provision-byoip-cidr
    --cidr 203.0.113.25/24
    --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 usar até que seu estado seja alterado 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 seguinteListbyoipcidrsComando da :

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

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

Quando o 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 interromper a publicidade) seu intervalo de endereços usando as operações da CLI ou da API do 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 pool com o Global Accelerator.

Para anunciar o intervalo de endereços, use o seguintePublicidade ByoipcidrComando da.

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

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

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

Para monitorar o estado dos intervalos de endereços anunciados por você, use o seguinteListbyoipcidrsComando da.

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

Quando o 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`withdraw-byoip-cidr`Comando da.

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

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

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

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

Desprovisionar o intervalo de endereços

Para parar de usar seu intervalo de endereços com a AWS, primeiro você deve remover todos os aceleradores com endereços IP estáticos alocados do grupo de endereços e parar de anunciar seu intervalo de endereços. Depois de concluir essas etapas, você pode desprovisionar o intervalo de endereços.

Você deve interromper a publicidade 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: Exclua todos os aceleradores associados.Para excluir um acelerador usando o console ou usando operações de API, consulte Exclui um acelerador.

Etapa 2. Pare de anunciar o intervalo de endereços. Para interromper o anúncio do intervalo, use o seguinteLevantamentooIPCIDRComando da.

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

Etapa 3. Desprovisionar o intervalo de endereços. Para desprovisionar o intervalo, use o seguinteDeprovisionbyoipCIDRComando da.

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

Crie um acelerador com seus endereços IP

Agora você pode criar um acelerador com seus endereços IP. Se você trouxe um intervalo de endereços para a AWS, poderá atribuir um endereço IP ao acelerador. Se você trouxe dois intervalos de endereços, poderá atribuir um endereço IP de cada intervalo de endereços ao acelerador.

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 Criando ou atualizando um acelerador padrão e Criando ou atualizando um acelerador de roteamento personalizado.

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

Preservar 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. Existem dois tipos de pontos de extremidade que podem preservar o endereço IP de origem do cliente em pacotes de entrada: Application Load Balancers e instâncias do Amazon EC2.

- 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. Isso significa que o endereço IP de origem do cliente original é preservado para pacotes que chegam ao balanceador de carga. Você pode optar por desativar a opção ao criar o acelerador ou editando o acelerador 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 ativada.

> **Note**
>
> O Global Accelerator não oferece suporte à preservação de endereço IP do cliente para endpoints de endereço IP do Network Load Balancer e Elastic IP.

Ao planejar adicionar a preservação do endereço 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, são atualizadas para incluir o endereço IP do cliente do usuário nas listas de permissões.
- A preservação do endereço IP do cliente é suportada apenas em regiões específicas da AWS. Para obter mais informações, consulte Regiões da AWS compatíveis para preservação de endereço IP do cliente.

Tópicos

Como habilitar a preservação do endereço IP do cliente

Quando você cria um novo acelerador, a preservação do endereço IP do cliente é habilitada, por padrão, para endpoints com suporte.

Esteja ciente do seguinte:

- Os Application Load Balancers internos e as instâncias do EC2 sempre têm a preservação do endereço IP do cliente ativada. Não é possível desabilitar a opção desses endpoints.
- Quando você usa o console da AWS para criar um novo acelerador, a opção de preservação de endereço IP do cliente é habilitada por padrão para endpoints do Application Load Balancer. Você pode desativar a opção a qualquer momento se não quiser a preservação do endereço IP do cliente para um ponto de extremidade do Application Load Balancer voltado para a Internet.
- Quando você usa a ILC da AWS ou uma ação de API para criar um novo acelerador e não especifica a opção para preservação de endereço IP do cliente, os endpoints do Application Load Balancer voltados para a Internet têm a preservação de endereço IP do cliente ativada por padrão.
- O Global Accelerator não oferece suporte à preservação de endereço IP do cliente para endpoints de endereço IP do Network Load Balancer e Elastic IP.

Para aceleradores existentes, você pode fazer a transição de endpoints sem a preservação do endereço IP do cliente para endpoints que preservam o endereço IP do cliente. Os endpoints existentes do Application Load Balancer podem ser transferidos para novos endpoints do Application Load Balancer, e os endpoints de endereço Elastic IP existentes podem ser transferidos para endpoints de instância do EC2. (Os pontos finais do Network Load Balancer não suportam a preservação do endereço IP do cliente. Para fazer a transição para os novos pontos de extremidade, recomendamos que você mova lentamente o tráfego de um ponto de extremidade existente para um novo ponto de extremidade que tenha preservação de endereço IP do cliente fazendo o seguinte:

- Para endpoints existentes do Application Load Balancer, primeiro adicione ao Global Accelerator um endpoint duplicado do Application Load Balancer que tenha como alvo os mesmos back-ends e, se for um Application Load Balancer voltado para a Internet, habilite a preservação do endereço

IP do cliente para ele. Em seguida, ajuste os pesos nos pontos finais para mover lentamente o tráfego do balanceador de carga quenãotêm a preservação do endereço IP do cliente habilitada para o balanceador de cargaporPreservação do endereço IP do cliente

- Para um endpoint de endereço Elastic IP existente, você pode mover o tráfego para um endpoint de instância do EC2 com preservação de 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 do endereço IP Elastic para o endpoint da instância do EC2.

Para obter orientação passo a passo de transição, consulte Transição de pontos de extremidade para usar a preservação do endereço IP do cliente.

Benefícios da preservação do endereço IP do cliente

Para endpoints que não têm a preservação do endereço IP do cliente ativada, os endereços IP usados pelo serviço Global Accelerator na rede de borda substituem o endereço IP do usuário solicitante como o 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 sistemas atrás de um acelerador. Isso funciona bem para muitas aplicações, especialmente aquelas que estão disponíveis para todos os usuários, como sites públicos.

No entanto, para outros aplicativos, você pode querer acessar o endereço IP do cliente original usando pontos de extremidade com preservação de endereço IP do cliente. Por exemplo, quando você tem o endereço IP do cliente, você pode coletar estatísticas com base em endereços IP do cliente. Você também pode usar filtros baseados em endereço IP, comoGrupos de segurança nos Application Load Balancerspara filtrar o tráfego. Você pode aplicar uma lógica específica ao endereço IP de um usuário em seus aplicativos que são executados nos servidores da camada da Web atrás desse endpoint do Application Load Balancer usando o`X-Forwarded-For`, que contém as informações de endereço IP do cliente original. Você também pode usar a preservação do endereço IP do cliente em regras de grupo de segurança nos grupos de segurança associados ao Application Load Balancer. Para obter mais informações, consulte Como o endereço IP do cliente é preservado no AWS Global Accelerator. Para endpoints de instância do EC2, o endereço IP do cliente original é preservado.

Para endpoints que não têm preservação de endereço IP do cliente, você pode filtrar o endereço IP de origem que o Global Accelerator usa quando encaminha 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 de entrada revisando seus

logs de fluxo do Global Accelerator. Para obter mais informações, consulte Intervalos de localização e endereços IP dos pontos de presença do Global Accelerator e Logs de fluxo no AWS Global Accelerator.

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 e Application Load Balancers:

- Para um endpoint de instância do EC2, o endereço IP do cliente é preservado para todo o tráfego.
- Para um ponto de extremidade do Application Load Balancer com preservação de endereço IP do cliente, o Global Accelerator trabalha em conjunto com o Application Load Balancer para fornecer umX-ForwardedCabeçalhoX-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 2616Cabeçalhos de. Há também cabeçalhos HTTP não padrão que são amplamente usados pelos aplicativos. Alguns dos cabeçalhos HTTP não padrão possuem umX-Forwardedprefixo.

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

OX-Forwarded-Forcabeçalho de solicitação é formatado assim:

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

O exemplo a seguir mostra umX-Forwarded-ForCabeçalho de solicitação para um cliente com o endereço IP 203.0.113.7.

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

Práticas recomendadas para preservação do endereço IP do cliente

Ao usar a preservação do endereço IP do cliente no AWS Global Accelerator, tenha em mente as informações e as práticas recomendadas nesta seção para interfaces de rede elásticas e grupos de segurança.

Para oferecer suporte à 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 elásticas de rede para rotear o tráfego para os endpoints configurados atrás de um acelerador. Os endpoints compatíveis para rotear tráfego dessa maneira são Application Load Balancers (internos e voltados para a Internet) e instâncias do Amazon EC2.

> **Note**
>
> Ao adicionar um Application Load Balancer interno ou um endpoint de instância do EC2 no Global Accelerator, você habilita o tráfego da Internet a fluir diretamente de e para o endpoint em VPCs (Virtual Private Clouds) direcionando-o em uma sub-rede privada. Para obter mais informações, consulte Conexões seguras da VPC no AWS Global Accelerator.

Como o Global Accelerator usa interfaces de rede elásticas

Quando você tem um Application Load Balancer com a preservação do endereço IP do cliente habilitada, o número de sub-redes em que o load balancer está determina o número de interfaces de rede elásticas que o Global Accelerator cria em sua conta. O Global Accelerator cria uma elastic network interface para cada sub-rede que tenha pelo menos uma elastic network interface do Application Load Balancer que é apresentada por um acelerador em sua conta.

Os exemplos a seguir ilustram 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, em seguida, você adicionar o load balancer como um endpoint acelerador, o Global Accelerator criará duas interfaces de rede elástica, uma em cada sub-rede.

- Exemplo 2: Se você adicionar, por exemplo, um ALB1 que tenha interfaces de rede elásticas em SubNetA e SubNetB ao Accelerator1 e, em seguida, adicionar um ALB2 com interfaces de rede elásticas na sub-rede A e sub-rede B ao Accelerator2, o Global Accelerator criará apenas duas interfaces de rede elásticas: uma em SubNetA e outra em SubnetB.
- Exemplo 3: Se você adicionar um ALB1 que tenha interfaces de rede elásticas em SubNetA e SubNetB ao Accelerator1 e, em seguida, adicionar um ALB2 com interfaces de rede elásticas em SubNetA e SubNetC ao Accelerator2, o Global Accelerator criará três interfaces de rede elásticas: uma em SubNetA, uma em SubnetB e outra em SubnetC. A elastic network interface no SubNetA fornece tráfego ligado tanto para o Accelerator1 como para o Accelerator2.

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

As interfaces de rede elásticas lógicas criadas pelo Global Accelerator 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 elastic network interface 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 dimensionado horizontalmente.

Avalie o número de sub-redes que são usadas por endpoints em seus aceleradores para determinar o número de interfaces de rede elásticas que o Global Accelerator criará. Antes de criar um acelerador, certifique-se de que tem capacidade de espaço de endereço IP suficiente para as interfaces de rede elástica necessárias, pelo menos um endereço IP gratuito 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 o Application Load Balancer e as interfaces de rede elástica associadas do Global Accelerator.

Quando o Global Accelerator determina que uma elastic network interface não está sendo usada por nenhum dos pontos finais em aceleradores em sua conta, o Global Accelerator exclui a interface.

Grupos de segurança criados pelo Global Accelerator

Reveja as seguintes informações e práticas recomendadas ao trabalhar com o Global Accelerator e grupos de segurança.

- O Global Accelerator cria security groups associados a qualquer interface de rede elástica. Embora o sistema não o impeça de o fazer, não deve editar nenhuma das definições de grupo de segurança para estes grupos.
- O Global Accelerator não exclui grupos de segurança criados por ele. No entanto, o Global Accelerator exclui uma elastic network interface se ela não estiver sendo usada por nenhum dos pontos finais em aceleradores em sua conta.
- Você pode usar os security groups criados pelo Global Accelerator como um grupo de origem em outros security groups mantidos, mas o Global Accelerator encaminha apenas o tráfego para os destinos especificados na VPC.
- Se você modificar as regras de grupo de segurança criadas pelo Global Accelerator, o ponto de extremidade pode ficar inintegro. Se isso acontecer, entre em contato comAWS SupportPara obter ajuda.
- O Global Accelerator cria um security group específico para cada VPC. As interfaces de rede elásticas criadas para os endpoints em uma VPC específica usam o mesmo security group, independentemente da sub-rede que uma elastic network interface esteja associada.

Regiões da AWS compatíveis para preservação de endereço IP do cliente

Você pode ativar a preservação do endereço IP do cliente para o AWS Global Accelerator nas seguintes regiões da AWS.

Nome da região	Região
US East (Ohio)	`us-east-2`
US East (N. Virginia)	`us-east-1`
US West (N. California)	`us-west-1 (except AZ usw1-az2)`
US West (Oregon)	`us-west-2`
Africa (Cape Town)	`af-south-1`
Asia Pacific (Hong Kong)	`ap-east-1`

Nome da região	Região
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Osaka)	ap-northeast-3
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1 (except AZ apne1-az3)
Asia Pacific (Seoul)	ap-northeast-2
Canada (Central)	ca-central-1 (except AZ cac1-az3)
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europe (Milan)	eu-south-1
Europe (Paris)	eu-west-3
Europe (Stockholm)	eu-north-1
Middle East (Bahrain)	me-south-1
South America (São Paulo)	sa-east-1

Registro em log e monitoramento no AWS Global Accelerator

Você pode usar logs de fluxo e o AWS CloudTrail para monitorar seu acelerador no AWS Global Accelerator, analisar padrões de tráfego e solucionar problemas com seus ouvintes e endpoints do.

Tópicos

Logs de fluxo no AWS Global Accelerator

Os logs de fluxo permitem que você capture informações sobre o tráfego de endereços IP para e proveniente de interfaces de rede no acelerador no AWS Global Accelerator. Os dados do log de fluxo são publicados no Amazon S3, onde é possível recuperar e visualizar seus dados depois de criar um log de fluxo.

Os logs de fluxo podem ajudar em diversas tarefas. Por exemplo, você pode solucionar problemas de por que um tráfego específico não está chegando a um endpoint, o que, por sua vez, ajuda a diagnosticar regras de security group excessivamente restritivas. Também é possível usar os logs de fluxo como ferramenta de segurança para monitorar o tráfego que está chegando aos 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. Uma tupla de 5 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 aproximadamente 10 segundos, mas pode demorar até 1 minuto.

As cobranças do CloudWatch Logs são aplicáveis ao usar logs de fluxo, mesmo quando os logs são publicados diretamente no Amazon S3. Para obter mais informações, consulteEntregar logs para o S3àsPreço do Amazon CloudWatch.

Tópicos

- Tempo de entrega do arquivo de log
- Sintaxe 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 existente do S3 especificado por você. Os registros de log de fluxo são publicados em uma série de objetos de arquivo de log armazenados no bucket.

Para criar um bucket do Amazon S3 para uso com logs de fluxo, consulte Criar um bucket no Guia de conceitos básicos do Amazon Simple Storage Service.

Arquivos de logs 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. Cada arquivo de log contém registros de log de fluxo para o tráfego de endereços 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 deixará 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, pela região e pela data e a hora em que foi criada. 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 nome de pasta e arquivo 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 o seguinte:

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

O exemplo a seguir mostra a estrutura de pasta e o nome de um arquivo de log para um fluxo de log criado por uma conta da AWS123456789012para um acelerador com um ID de1234abcd-abcd-1234-abcd-1234abcdefgh, em 23 de novembro de 2018 às 00:05 UTC:

```
my-s3-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 de 5 tuplas; isto é,`client_ip`,`client_port`,`accelerator_ip`,`accelerator_port`,`protocol`. Para ver todos os arquivos de log de fluxo para o acelerador, procure entradas agregadas pelo`accelerator_id`e suas receitas`account_id`.

Funções do IAM para publicar logs de fluxo no Amazon S3

Um principal do IAM, como um usuário do IAM, deve ter permissões suficientes para publicar logs de fluxo no bucket do Amazon S3. A política do IAM deve incluir as seguintes permissões:

```
{
    "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 possui o bucket, o serviço anexará 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 anteriores ao bucket e especificar o ID de conta da AWS do criador do log de fluxo. Para obter mais informações, consulteComo eu faço para adicionar uma política de bucket do S3?noGuia de conceitos básicos 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 123123123 e 456456456456 publiquem logs de fluxo em uma pasta chamada de`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 que você conceda oAWSLogDeliveryAclCheckeAWSLogDeliveryWritePermissões do principal serviço de entrega de logs em vez dos ARNs de contas da AWS individuais.

Política de chaves de CMK obrigatórias para uso com buckets de SSE-KMS

Se você habilitar a criptografia no lado do servidor para o bucket do Amazon S3 usando chaves gerenciadas pelo AWS KMS (SSE-KMS) com uma chave mestra de cliente gerenciada pelo cliente (CMK), você deve adicionar o seguinte à política de chaves para seu CMK de modo que os logs de fluxos possam ser gravados 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, consulteVisão geral da Lista de controle de acesso (ACL)noGuia de conceitos básicos do Amazon Simple Storage Service.

Habilitar publicar logs de fluxo no Amazon S3

Para ativar logs de fluxo no AWS Global Accelerator, siga as etapas deste procedimento.

Para ativar logs de fluxo no AWS Global Accelerator

1. Crie um bucket do Amazon S3 para seus logs de fluxo na sua conta da AWS.
2. Adicione a política do IAM necessária para o usuário da AWS que está habilitando os logs de fluxo. Para obter mais informações, consulte Funções do IAM para publicar logs de fluxo no Amazon S3.
3. Execute o seguinte comando da ILC da AWS, com o nome do bucket do Amazon S3 e o prefixo 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.

Tempo de entrega do arquivo de log

O AWS Global Accelerator oferece arquivos de log para o acelerador configurado até várias vezes por hora. Em geral, um arquivo de log contém informações sobre as solicitações recebidas pelo 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 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 acelerador de todos os pontos de presença que receberam solicitações durante o período de cobertura do arquivo de log.

O Global Accelerator começa a entregar os arquivos de log cerca de quatro horas depois de você habilitar o registro. É possível que você receba alguns arquivos de log antes disso.

> **Note**
>
> Se nenhum usuário se conectar ao acelerador durante o período, você não receberá arquivos de log referentes a esse período.

Sintaxe 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 da VPC,`vpc_id`. O formato versão 2.0, incluindo`vpc_id`, é gerado quando o Global Accelerator envia tráfego para um endpoint com preservação de 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`	ID da conta da AWS para o log de fluxo.
`accelerator_id`	O ID do acelerador para o qual o tráfego é registrado.
`client_ip`	O endereço IPv4 de origem.
`client_port`	A porta de origem.

Campo	Descrição
`accelerator_ip`	O endereço IP do acelerador.
`accelerator_port`	A bombordo 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.
`packets`	O número de pacotes transferidos durante a 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.
`action`	A ação associada como tráfego: • `ACCEPT`: O tráfego registrado foi permitido por grupos de segurança ou Network ACLs. No momento, o valor é sempre ACCEPT.

Campo	Descrição
`log-status`	O status de registro do log de fluxo: • `OK`: os dados são registrados em log normalmente nos destinos selecionados. • `NODATA`: Não havia nenhum tráfego de rede para ou proveniente da interface de rede durante a janela de captura. • `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.
`globalaccelerator_source_ip`	O endereço IP usado pela interface de rede do Global Accelerator.
`globalaccelerator_source_port`	A porta usada pela interface de rede do Global Accelerator.
`endpoint_region`	A região da AWS onde o endpoint está localizado.
`globalaccelerator_region`	O ponto de presença (ponto de presença) que atendeu à solicitação. Cada ponto de presença possui 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.)
`direction`	A direção do tráfego. Denota tráfego que entra na rede Global Accelerator (`INGRESS`) ou retornar ao cliente (`EGRESS`).
`vpc_id`	O identificador da VPC. Incluído nos logs de fluxo da versão 2.0 quando o Global Accelerator envia tráfego para um ponto de extremidade com preservação de endereço IP do cliente.

Se um campo não for aplicável a um registro específico, o registro exibirá o símbolo '-' para essa entrada.

Usando o Amazon CloudWatch com o AWS Global Accelerator

O AWS Global Accelerator publica pontos de dados no Amazon CloudWatch para seus aceleradores. O CloudWatch permite que você recupere estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecidos comoMétricas do. 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, é possível monitorar o tráfego por meio de um acelerador ao longo de um período especificado. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

Você 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 iniciar 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 ao CloudWatch somente quando as solicitações são enviadas pelo acelerator. Se as solicitações são enviadas pelo acelerator, 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 reportada.

Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch.

Tópicos

- Métricas do Global Accelerator
- Dimensões da métrica dos aceleradores
- Estatísticas de métricas do Global Accelerator
- Veja as métricas do CloudWatch para seus aceleradores

Métricas do Global Accelerator

O namespace `AWS/GlobalAccelerator` inclui as métricas a seguir.

Métrica	Descrição
`NewFlowCount`	O número total de novos fluxos (ou conexões) TCP estabelecidos dos clientes para os pontos finais no período. Critérios: Há um valor diferente de zero. Estatísticas: A única estatística útil é `Sum`. Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`
`ProcessedBytesIn`	O número total de bytes de entrada processados pelo acelerator, incluindo cabeçalhos TCP/IP. Essa contagem inclui todo o tráfego para endpoints. Critérios: Há um valor diferente de zero. Estatísticas: A única estatística útil é `Sum`. Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`

Métrica	Descrição
`ProcessedBytesOut`	O número total de bytes de saída processados pelo acelerator, incluindo cabeçalhos TCP/IP. Essa contagem inclui o tráfego dos pontos finais, menos o tráfego da verificação de integridade. Critérios: Há um valor diferente de zero. Estatísticas: A única estatística útil é`Sum`. Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`

Dimensões da métrica dos aceleradores

Para filtrar as métricas do acelerator, use as dimensões a seguir.

Dimensão	Descrição
`Accelerator`	Filtra os dados da métrica por acelerator. 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-1234abcdefgh` Você deve especificar o seguinte:**`1234abcd-abcd-1234-abcd-1234abcdefgh`** .
`Listener`	Filtra os dados da métrica por listener. Especifique o listener pelo id do listener (a parte final do ARN do listener). Por exemplo, se o ARN for`arn:aws:globalaccelerator::012345678901:accel`

Dimensão	Descrição
	`erator/1234abcd-abcd-1234-abcd-1234abcdefgh/l istener/0123wxyz` Você deve especificar o seguinte:**`0123wxyz`**.
`EndpointGroup`	Filtra os dados da métrica por grupo de ponto final. Especifique o grupo de endpoint pela Região da AWS, por exemplo,**`us-east-1`** (todas em minúsculas).
`SourceRegion`	Filtra os dados de métrica por região de origem, que é a área geográfica das regiões da AWS onde seus endpoints de aplicativo estão sendo executados. A região de origem é uma das seguintes opções: • NA — Estados Unidos e Canadá • EU — Europa Oriental • AP — Ásia* • KR — Coreia do Sul • IN — Índia • AU — Austrália • ME — Oriente Médio • SA — América do Sul *Excluindo Coréia do Sul e Índia

Dimensão	Descrição
`DestinationEdge`	Filtra os dados métricos por borda de destino, que é a área geográfica dos pontos de presença da AWS que atendem ao tráfego do cliente. A borda de destino é uma das seguintes opções: • NA — Estados Unidos e Canadá • EU — Europa Oriental • AP — Ásia* • KR — Coreia do Sul • IN — Índia • AU — Austrália • ME — Oriente Médio • SA — América do Sul • ZA — África do Sul *Excluindo Coréia do Sul e Índia
`TransportProtocol`	Filtra os dados da métrica por protocolo de transporte: UDP ou TCP.
`AcceleratorIPAddress`	Filtra os dados da métrica pelo endereço IP do acelerator: ou seja, um dos endereços IP estáticos atribuídos a um acelerator.

Estatísticas de 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 espaço de tempo específico. 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 onde os bytes são atendidos a partir de pontos de presença da AWS na Europa (a borda de destino é “UE”).

Veja a seguir exemplos de combinações métrica/dimensão que você pode achar úteis:

- Exiba a quantidade de tráfego servido (como processedBytesOut) por cada um dos seus dois endereços IP do acelerador para validar se a configuração do DNS está correta.
- Visualize a distribuição geográfica do seu tráfego de usuário e monitore o quanto dele é local (por exemplo, América do Norte para América do Norte) ou global (por exemplo, Austrália ou Índia para América do Norte). Para determinar isso, exiba as métricas processedBytesIn ou processedBytesOut com as dimensões destinationEdge e SourceRegion definidas como valores específicos.

Veja as métricas do CloudWatch para seus aceleradores

Você pode visualizar as métricas do CloudWatch para seus aceleradores usando o console do CloudWatch ou a CLI da AWS. No console, as métricas são exibidas como gráficos de monitoramento. Os gráficos de monitoramento mostrarão pontos de dados somente 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), no console ou ao usar a CLI da AWS. Ao usar a ILC da AWS, especifique a região Oeste dos EUA (Oregon) para seu comando, incluindo o seguinte parâmetro:`--region us-west-2`.

Como exibir métricas usando o console do CloudWatch

1. Abra o console do CloudWatch emhttps://us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2.
2. No painel de navegação, selecione Métricas.
3. Selecione oGlobalAcceleratorNamespace.
4. (Opcional) Para visualizar uma métrica em todas as dimensões, digite o nome no campo de pesquisa.

Para visualizar métricas usando o AWS CLI

Use o comando list-metrics para listar as métricas disponíveis:

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

Para obter as estatísticas de uma métrica usando a CLI da AWS

Use o seguinteget-metric-statisticsPara obter estatísticas de uma métrica e dimensão especificada. Observe que o CloudWatch trata cada combinação única de dimensões como uma métrica distinta. Você não pode 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 em, por minuto, para seu acelerador servindo 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"
        }
    ]
}
```

Usando 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 realizadas por um usuário, uma função ou um serviço da AWS no Global Accelerator. O CloudTrail captura todas as chamadas de API do 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 não configurar uma trilha, você ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history.

Para saber mais sobre CloudTrail, consulte o AWS CloudTrail User Guide.

Informações do Global Accelerator no CloudTrail

O CloudTrail está habilitado na sua conta da AWS ao criá-la. Quando ocorre atividade no Global Accelerator, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS emHistórico do evento. Você pode visualizar, pesquisar e fazer download de eventos recentes em sua conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro de eventos em andamento na sua conta da AWS, incluindo eventos do Global Accelerator, crie uma trilha. Uma trilha permite CloudTrail para fornecer arquivos de log a um bucket do 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 serviços da AWS para analisar mais profundamente e agir sobre os dados de evento coletados nos logs do CloudTrail. Para obter mais informações, consulte os tópicos a seguir:

- Visão geral da criação de uma trilha
- CloudTrail Serviços compatíveis e integrações do
- Configuração de notificações do Amazon SNS para o 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 documentadas noReferência da API do AWS Global Accelerator. Por exemplo, as chamadas para as operações`CreateAccelerator`,`ListAccelerators`e`UpdateAccelerator`As operações 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 IAM
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado
- Se a solicitação foi feita por outro serviço da AWS

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre as entradas dos arquivos de log do

Uma trilha é uma configuração que permite a entrega de eventos como registros de log a um bucket do Amazon S3 especificado. Cada arquivo de log do CloudTrail no formato JSON pode conter 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. Não há garantia de que as entradas de log estarão em uma ordem específica. Elas não são um rastreamento de pilha ordenado das chamadas de API.

O exemplo a seguir mostra uma entrada de log do CloudTrail que inclui essas ações do Global Accelerator:

- Listando os aceleradores de uma conta:`eventName`é`ListAccelerators`.
- Criando um listener:`eventName`é`CreateListener`.
- Atualizar um listener:`eventName`é`UpdateListener`.
- Descrevendo um listener:`eventName`é`DescribeListener`.
- Listeners para uma conta:`eventName`é`ListListeners`.
- Excluir um listener:`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": [
            {
              "ipFamily": "IPv4",
              "ipAddresses": [
                "192.0.2.213",
                "192.0.2.200"
              ]
            }
          ],
          "status": "IN_PROGRESS",
          "createdTime": "Nov 17, 2018 9:03:52 PM",
          "lastModifiedTime": "Nov 17, 2018 9:03:52 PM"
        }
      },
      "requestID": "d2d7f300-2f0b-4bda-aa2d-e67d6e4example",
      "eventID": "11f9a762-8c00-4fcc-80f9-848a29example",
```

```
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:05:27Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "UpdateListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
        "portRanges": [
          {
            "fromPort": 80,
            "toPort": 80
          },
          {
            "fromPort": 81,
            "toPort": 81
          }
```

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

```
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:06:05Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "DescribeListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234"
      },
      "responseElements": null,
      "requestID": "9980e368-82fa-40da-95a3-4b0example",
      "eventID": "885a02e9-2a60-4626-b1ba-57285example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:05:47Z",
```

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

```
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234"
      },
      "responseElements": null,
      "requestID": "04d37bf9-3e50-41d9-9932-6112example",
      "eventID": "afedb874-2e21-4ada-b1b0-2ddb2example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Segurança do AWS Global Accelerator

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você aproveita um datacenter e uma arquitetura 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 a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem: a AWS é responsável por proteger a infraestrutura que executa serviços da AWS na Nuvem AWS. A AWS também fornece serviços que você pode usar com segurança. A eficácia de nossa segurança é regularmente testada e verificada por auditores de terceiros como parte dos programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Global Accelerator, consulteServiços da AWS no escopo pelo programa de conformidade.
- Segurança na nuvem: a responsabilidade é determinada pelo serviço da AWS usado. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua organização e as leis e regulamentos aplicáveis.

Esta documentação ajudará você 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.

Tópicos

Identity and Access Management para o AWS Global Accelerator

O AWS Identity and Access Management (IAM) é um serviço da AWS que ajuda um administrador a controlar com segurança o acesso aos recursos da AWS, incluindo os recursos do AWS Global

Accelerator. Os administradores usam o IAM para controlar quem éAutenticado(conectado) eautorizado(tem permissões) para usar recursos do Global Accelerator. O IAM é um recurso incluído na conta da AWS gratuitamente.

> **Important**
>
> Se não estiver familiarizado com o IAM, reveja as informações introdutórias nesta página e consulteConceitos básicos do IAM. Opcionalmente, você pode saber mais sobre autenticação e controle de acesso consultandoO que é autenticação?,O que é controle de acesso?, eO que são políticas?.

Tópicos

Conceitos e termos

Autenticação— para fazer login na AWS, você deve usar um dos seguintes: credenciais de usuário raiz (não recomendadas), credenciais de usuário do IAM ou credenciais temporárias usando funções do IAM. Para saber mais sobre essas entidades, consulte O que é autenticação?.

Controle de acesso— os administradores da AWS usam políticas para controlar o acesso aos recursos da AWS, como os aceleradores do Global Accelerator. Para saber mais, consulte O que é controle de acesso? e O que são políticas?.

> **Important**
>
> Todos os recursos de uma conta são de propriedade da conta, independentemente de quem os criou. Você deve receber acesso para criar um recurso. No entanto, você não tem acesso completo a um recurso automaticamente só porque o criou. Um administrador deve conceder permissões explicitamente para cada ação que você deseja executar. Esse administrador também pode revogar suas permissões a qualquer momento.

Para ajudar a compreender os conceitos básicos de como o IAM funciona, reveja os termos a seguir:

Recursos

Os serviços da AWS, como o Global Accelerator e o IAM, geralmente incluem objetos chamados objetos. Na maioria dos casos, você pode criar, gerenciar e excluir esses recursos do serviço. Os recursos do IAM incluem usuários, grupos, funções e políticas:

Usuários

Um usuário do IAM representa a pessoa ou o aplicativo que usa suas credenciais para interagir com a AWS. Um usuário consiste em um nome, uma senha para fazer login no Console de Gerenciamento da AWS e até duas chaves de acesso que podem ser usadas com a CLI da AWS ou a API da AWS.

Grupos

Um grupo do IAM é um conjunto de usuários do IAM. Os administradores podem usar grupos para especificar permissões para usuários membros. Isso facilita o gerenciamento de permissões de vários usuários.

Funções

Uma função do IAM não tem nenhuma credencial de longo prazo (senha ou chaves de acesso) associada a ela. Uma função pode ser assumida por qualquer pessoa que precise dela e tenha permissões. Um usuário do IAM pode assumir uma função para conseguir temporariamente permissões diferentes para uma tarefa específica. Os usuários federados podem assumir uma função usando um provedor de identidade externo que esteja mapeado para a função. Alguns serviços da AWS podem assumir umaFunção de serviço doPara acessar os recursos da AWS em seu nome.

Políticas

Políticas são documentos JSON que definem as permissões do objeto ao qual são anexadas. A AWS oferece suportePolíticas baseadas em identidade doque você anexa a identidades (usuários, grupos ou funções do). Alguns serviços da AWS permitem que você anexePolíticas baseadas em recursos doPara recursos a fim de controlar o que um principal (pessoa ou aplicativo) pode fazer com esse recurso. O Global Accelerator não oferece suporte a políticas baseadas em recurso.

Identidades

Identidades são os recursos do IAM para os quais você pode definir permissões. Entre eles estão usuários, grupos e funções.

Entidades

Entidades são os recursos do IAM do que você usa para autenticação. Entre eles estão usuários e funções.

Principais

Na AWS, um principal é uma pessoa ou um aplicativo que usa uma entidade para fazer login e solicitações à AWS. Como um principal, você pode usar o Console de Gerenciamento da AWS, a CLI da AWS ou a API da AWS para executar uma operação (como excluir um acelerador). Isso cria uma solicitação para essa operação. Sua solicitação especifica a ação, o recurso, o principal, a conta do principal e qualquer informação adicional sobre a solicitação. Todas essas informações fornecem à AWS ocontextpara o seu pedido. A AWS verifica todas as políticas aplicáveis ao contexto da sua solicitação. A AWS autorizará a solicitação somente se cada parte de sua solicitação tiver permissão concedida pelas políticas.

Para visualizar um diagrama do processo de autenticação e de controle de acesso, consulteNoções básicas sobre o funcionamento donoGuia do usuário do IAM. Para obter detalhes sobre como a AWS determina se uma solicitação deve obter permissão, consulteLógica da avaliação de políticasnoGuia do usuário do IAM.

Permissões necessárias para acesso ao console, gerenciamento de autenticação e controle de acesso

Para usar o Global Accelerator ou gerenciar sua própria autorização e controle de acesso ou de outros usuários, você deve ter as permissões corretas.

Permissões necessárias para criar um acelerador Global Accelerator

Para criar um acelerador do AWS Global Accelerator, os usuários devem ter permissão para criar funções vinculadas ao serviço associadas 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 que seja mais restritiva, os usuários com essa política 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*"
    }
```

Permissões necessárias para usar o console do Global Accelerator

Para acessar o console do AWS Global Accelerator, é necessário ter um conjunto mínimo de permissões que permitam listar e visualizar detalhes sobre os recursos do Global Accelerator na conta da AWS. Se você criar uma política de permissões baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades com essa política.

Para garantir que essas entidades ainda consigam usar o console do Global Accelerator ou as ações da API, anexe também ao usuário uma das seguintes políticas gerenciadas pela AWS, conforme descrito emCriar políticas na guia JSON:

```
        GlobalAcceleratorReadOnlyAccess
        GlobalAcceleratorFullAccess
```

Anexar a primeira política,`GlobalAcceleratorReadOnlyAccess`, se os usuários só precisarem visualizar informações no console ou fazer chamadas para a CLI da AWS ou a API que usam`List*`ou`Describe*`operações.

Anexar a segunda política,`GlobalAcceleratorFullAccess`, para usuários que precisam criar ou fazer atualizações em aceleradores. A política de acesso total inclui oCompletopermissões para o Global Accelerator, bem comodescribepermissões para o Amazon EC2 e 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.

Segue-se a política de acesso completo:

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

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

Permissões necessárias para o gerenciamento de autenticação

Para gerenciar suas próprias credenciais, como senha, chaves de acesso e dispositivos de autenticação multifator (MFA - Multi-factor Authentication), o administrador deve conceder a você as permissões necessárias. Para visualizar a política que inclui essas permissões, consulte Permitir que usuários do gerenciem automaticamente suas credenciais.

Como administrador da AWS, você precisa de acesso completo ao IAM para que possa criar e gerenciar usuários, grupos, funções e políticas no IAM. Você deve usar oAdministratorAccessPolítica gerenciada pela AWS que inclui acesso completo a toda a AWS. Esta política não fornece acesso ao console de Billing and Cost Management da AWS nem permite tarefas que exigem credenciais de usuário raiz da conta da AWS. Para obter mais informações, consulteTarefas da AWS que exigem credenciais do usuário raiz da conta da AWSnoReferência geral da AWS.

> **Warning**
>
> Somente um usuário administrador deve ter acesso completo à AWS. Quem tem essa política tem permissão para gerenciar completamente a autenticação e o controle de acesso, além de modificar todos os recursos da AWS. Para saber como criar esse usuário, consulte Crie seu usuário administrador do IAM.

Permissões necessárias para o controle de acesso

Se o administrador tiver lhe fornecido credenciais de usuário do IAM, ele terá anexado políticas a seu usuário do IAM para controlar os recursos que você acessa. Para visualizar as políticas anexadas a sua identidade de usuário no Console de Gerenciamento da AWS, você deve ter as seguintes permissões:

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

```
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Se precisar de permissões adicionais, peça ao administrador para atualizar suas políticas para permitir acesso às ações de que você precisa.

Entendendo como o Global Accelerator funciona com o IAM

Os serviços podem funcionar com o IAM de várias maneiras:

Ações

O Global Accelerator oferece suporte ao uso de ações em uma política. Isso permite que um administrador controle se uma entidade pode concluir uma operação no Global Accelerator. Por exemplo, para permitir que uma entidade chame o método`GetPolicy`Para visualizar uma política da AWS, um administrador deve anexar uma política que permita o`iam:GetPolicy`Ação .

O exemplo a seguir permite que um usuário execute o`CreateAccelerator`para criar programaticamente um acelerador para sua conta da AWS:

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

Permissões em nível de recurso

O Global Accelerator oferece suporte a permissões no nível do recurso. As permissões em nível de recurso permitem usar ARNs para especificar recursos individuais na política.

Políticas baseadas em recursos

O Global Accelerator não oferece suporte a políticas baseadas em recurso. Com políticas baseadas em recurso, você pode anexar uma política a um recurso do serviço. As políticas baseadas em recursos incluem um`Principal`Para especificar quais identidades do IAM podem acessar esse recurso.

Autorização baseada em tags

O Global Accelerator oferece suporte a tags baseadas em autorização. Esse recurso permite que você use tags de recursos na condição de uma política.

Credenciais temporárias

Global Accelerator oferece suporte a credenciais temporárias. Com credenciais temporárias, você pode fazer login com federação, assumir uma função do IAM ou assumir uma função entre contas. As credenciais de segurança temporárias são obtidas chamando operações da API do AWS STS, como o`AssumeRole`ou`GetFederationToken`.

Funções vinculadas ao serviço

O Global Accelerator oferece suporte a funções vinculadas ao serviço. Esse recurso permite que um serviço assuma uma função vinculada ao serviço em seu nome. A função permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

Funções de serviço

O Global Accelerator não oferece suporte a funções de serviço. Esse recurso permite que um serviço assuma uma função de serviço em seu nome. A função permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. As funções de serviço aparecem em sua conta do IAM e são de propriedade da conta. Isso significa que um administrador do IAM pode alterar as permissões para essa função. Porém, isso pode alterar a funcionalidade do serviço.

Solucionando problemas de autenticação e controle

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o IAM.

Tópicos

Não tenho autorização para executar uma ação no Global Accelerator

Se o Console de Gerenciamento da AWS informar que você não está autorizado a executar uma ação, entre em contato com o administrador que forneceu o nome de usuário e a senha para você.

O exemplo a seguir ocorre quando um usuário do IAM chamado`my-user-name`O tenta usar o console do para executar o`globalaccelerator:CreateAccelerator`ação, mas não tem permissões:

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

Neste caso, peça ao administrador para atualizar suas políticas a fim de permitir acesso aos`my-example-accelerator`Usando o`aws-globalaccelerator:CreateAccelerator`Ação .

Sou administrador e desejo permitir que outros usuários tenham acesso ao Global Accelerator

Para permitir que outros usuários acessem o Global Accelerator, é necessário criar uma entidade do IAM (usuário ou função) para a pessoa ou a aplicação que precisa do acesso. Eles usarão as credenciais dessa entidade para acessar a AWS. Você deve anexar uma política à entidade que concede a eles as permissões corretas no Global Accelerator.

Para começar a usar rapidamente, consulte Conceitos básicos do IAM.

Desejo saber do IAM sem me tornar um especialista

Para saber mais sobre os termos, conceitos e procedimentos do IAM, consulte os tópicos a seguir:

- O que é autenticação?
- O que é controle de acesso?
- O que são políticas?

Políticas baseadas em tag

Ao criar políticas do IAM, você pode definir permissões granulares concedendo acesso a recursos específicos. À medida que o número de recursos que você gerencia cresce, essa tarefa se torna mais difícil. Marcar aceleradores e usar tags em condições de declaração de política pode facilitar essa tarefa. Você concede acesso em massa a qualquer acelerador com uma determinada tag. Depois, você aplica essa tag repetidamente a aceleradores relevantes, quando você criar o acelerador ou atualizando o acelerador posteriormente.

> **Note**
>
> O uso de tags em condições é uma forma de controlar o acesso a recursos e solicitações. Para obter informações sobre marcação no Global Accelerator, consulteMarcação no AWS Global Accelerator ator ator.

As tags podem ser anexadas a um recurso ou passadas na solicitação para serviços que ofereçam suporte a tags. No Global Accelerator, apenas aceleradores podem incluir tags. Quando você criar uma política do IAM, 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.

Para obter a sintaxe a semântica completas das chaves de condição de tag, consulteControle o acesso usando tags do IAMnoGuia do usuário do IAM.

Por exemplo, o Global Accelerator`GlobalAcceleratorFullAccess`A política gerenciada do 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 qualquerProduçãoAceleradores. 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"
            }
         }
      }
   ]
}
```

Função vinculada ao serviço para o Global Accelerator

O AWS Global Accelerator usa um AWS Identity and Access Management (IAM)Função vinculada ao serviço do. Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a um serviço. As funções vinculadas a serviços são predefinidas pelo serviço e incluem todas as permissões de que ele precisa para chamar outros serviços da AWS; em seu nome.

O Global Accelerator usa a seguinte função vinculada ao serviço do IAM:

- AWSServiceRoleForGlobalAccelerator—O Global Accelerator usa essa função para permitir que o Global Accelerator crie e gerencie os recursos necessários para a preservação do endereço IP do cliente.

O Global Accelerator cria automaticamente uma função chamada AWSServiceRoleForGlobalAccelerator quando a função é necessária pela primeira

vez para dar suporte a uma operação de API do Global Accelerator. A função AWSServiceRoleForGlobalAccelerator permite que o Global Accelerator crie e gerencie os recursos necessários para a preservação do endereço IP do cliente. Essa função é necessária para usar aceleradores no Global Accelerator. O ARN para a função AWSServiceRoleForGlobalAccelerator é semelhante a:

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

Uma função vinculada ao serviço facilita a configuração e o uso do Global Accelerator, pois você não precisa adicionar as permissões necessárias manualmente. O Global Accelerator define as permissões da função vinculada ao serviço e apenas o Global Accelerator pode assumir as funções do. As permissões definidas incluem a política de confiança e a política de permissões. A política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você deve remover quaisquer recursos do Global Accelerator associados para poder excluir a função vinculada ao serviço. Isso ajuda a proteger seus recursos do Global Accelerator, certificando-se de não remover uma função vinculada ao serviço que ainda seja necessária para acessar os recursos ativos.

Para obter informações sobre outros serviços que oferecem suporte às funções vinculadas a serviço, consulte Serviços da AWS compatíveis que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Função vinculada ao serviço.

Permissões de função vinculada ao serviço para o Global Accelerator

O Global Accelerator usa uma função vinculada ao serviço chamadaAWSServiceRoleForGlobalAccelerator. As seções a seguir descrevem as permissões para a função.

Permissões de função vinculada ao serviço

Essa função vinculada a serviços permite que o Global Accelerator gerencie interfaces de rede elástica do EC2 e ajude a diagnosticar erros.

A função vinculada ao serviço AWSServiceRoleForGlobalAccelerator confia no seguinte serviço para assumir a função:

- `globalaccelerator.amazonaws.com`

A política de permissões da função permite que o Global Accelerator conclua as seguintes ações nos recursos especificados, conforme mostrado na política:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSecurityGroup",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSServiceName": "GlobalAccelerator"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
    ]
}
```

Você deve configurar permissões para que uma entidade do IAM (como um usuário, grupo ou função) exclua a a função vinculada ao serviço do Global Accelerator. Para obter mais informações, consulte Permissões de função vinculada ao serviço no Guia do usuário do IAM.

Criar uma função vinculada ao serviço para o Global Accelerator

Você não precisa criar manualmente a função vinculada ao serviço para o Global Accelerator. O serviço cria a função para você automaticamente na primeira vez que você cria um acelerador. Se você remover seus recursos do Global Accelerator e excluir a função vinculada ao serviço, o serviço criará a função novamente automaticamente quando você criar um novo acelerador.

Editar a função vinculada ao serviço Global Accelerator

O Global Accelerator não permite editar a função vinculada 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.

Excluir a função vinculada ao serviço do Global Accelerator

Se você não precisa mais usar um grupo do Global Accelerator, recomendamos que exclua a função vinculada ao serviço. Dessa forma, você não tem entidades não utilizadas que não sejam monitoradas ou mantidas ativamente. No entanto, você deve limpar os recursos da Global Accelerator em sua conta antes de poder excluir manualmente as funções.

Depois de desabilitar e excluir os aceleradores do, você pode excluir a função vinculada ao serviço. Para obter mais informações sobre como excluir aceleradores, consulte Criando ou atualizando um acelerador padrão.

> **Note**
>
> Se você tiver desativado e excluído seus aceleradores, mas o Global Accelerator não tiver concluído a atualização, a exclusão da função vinculada ao serviço poderá falhar. Se isso acontecer, espere alguns minutos e tente as etapas de exclusão de funções vinculadas ao serviço novamente.

Para excluir manualmente a função vinculada ao serviço AWSServiceRoleForGlobalAccelerator

1. Faça login no Console de Gerenciamento da AWS 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 um serviço da AWS pela última vez. Isso ajuda você a confirmar se a função está ativo no momento. Se você deseja continuar, escolha Sim, excluir para enviar a função vinculada ao serviço para exclusão.
5. Observe as notificações do console do IAM para monitorar o 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 para a função vinculada ao serviço do Global Accelerator (uma política gerenciada pela AWS)

Exiba detalhes sobre atualizações da função vinculada ao serviço desde que este serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações nesta página, assine o feed RSS no AWS Global AcceleratorHistórico do documento.

Alteração	Descrição	Data
AWSServiceRoleForGlobalAccelerator— Atualizado	O Global Accelerator adicionou uma nova	18 de maio de 2021

Alteração	Descrição	Data
	permissão para ajudar o Global Accelerator a diagnosticar erros. Global Accelerator usa `ec2:DescribeRegions` para determinar a região da AWS em que um cliente está, o que pode ajudar o Global Accelerator a solucionar erros.	
O Global Accelerator começou a acompanhar as alterações	O Global Accelerator começou a rastrear alterações em suas políticas gerenciadas pela AWS.	18 de maio de 2021

Regiões compatíveis com funções vinculadas ao serviço do Global Accelerator

O Global Accelerator oferece suporte a funções vinculadas a serviços nas regiões da AWS em que o Global Accelerator é compatível com o.

Para obter uma lista das regiões da AWS em que o Global Accelerator e outros serviços são compatíveis com o, consulte aTabela da região da AWS.

Visão geral do acesso e autenticação

Se você for novo no IAM, leia os seguintes tópicos para começar a usar autorização e acesso na AWS.

Tópicos

- O que é autenticação?
- O que é controle de acesso?
- O que são políticas?
- Conceitos básicos do IAM

O que é autenticação?

A autenticação é a forma como você faz login na AWS usando suas credenciais.

> **Note**
>
> Para começar a usar rapidamente, ignore esta seção. Primeiro, reveja as informações introdutórias emIdentity and Access Management para o AWS Global Acceleratore depois consulteConceitos básicos do IAM.

Como um diretor, você deve serAutenticado(conectado à AWS) usando uma entidade (usuário raiz, usuário do IAM ou função do IAM) para enviar uma solicitação à AWS. Um usuário do IAM pode ter credenciais de longo prazo, como um nome de usuário e uma senha ou um conjunto de chaves de acesso. Ao assumir uma função do IAM, você recebe credenciais de segurança temporárias.

Para autenticar-se no AWS Management Console como um usuário, você deve fazer login com seu nome de usuário e senha. Para obter a autenticação na CLI da AWS ou na API da AWS, você deve fornecer sua chave de acesso e chave secreta ou credenciais temporárias. A AWS fornece ferramentas de SDK e CLI para assinar de forma criptográfica sua solicitação usando suas credenciais. Se você não utilizar ferramentas da AWS, assine a solicitação você mesmo. Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, a AWS recomenda o uso de autenticação multifator (MFA) para aumentar a segurança de conta.

Como principal, você pode fazer login na AWS usando as seguintes entidades (usuários ou funções):

Usuário raiz da conta da AWS

Ao criar uma conta do AWS pela primeira vez, você começa com uma única identidade de login que tem acesso completo a todos os serviços e recursos da AWS na conta. Essa identidade é denominada usuário raiz da conta da AWS e é acessada pelo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável que você não use o usuário raiz nas tarefas diárias, nem mesmo nas administrativas. Em vez disso, siga as práticas recomendadas para o uso do usuário raiz somente a fim de criar seu primeiro usuário do IAM. Depois, armazene as credenciais do usuário raiz com segurança e use-as para executar somente algumas tarefas de gerenciamento de contas e de serviços.

Usuário do IAM

UmaUsuário do IAMO é uma entidade dentro de sua conta da AWS que tem permissões específicas. O Global AcceleratorSignature versão 4, um protocolo para autenticar solicitações de API de entrada. Para obter mais informações sobre solicitações de autenticação, consulte Processo de assinatura do Signature versão 4 na Referência geral da AWS.

IAM role (Função do IAM)

UmaIAM role (Função do IAM)O é uma identidade do IAM que você pode criar em sua conta que tem permissões específicas. Uma função do IAM é semelhante a um usuário do IAM, pois é uma identidade da AWS com políticas de permissão que determinam o que a identidade pode e não pode fazer na AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, uma função destina-se a ser assumida por qualquer pessoa que precisar dela. Além disso, uma função não tem credenciais de longo prazo padrão, como uma senha ou chaves de acesso, associadas a ela. Em vez disso, quando você assumir uma função, ela fornecerá credenciais de segurança temporárias para sua sessão de função. As funções do IAM com credenciais temporárias são úteis nas seguintes situações:

Acesso de usuário federado

Em vez de criar um usuário do IAM, é possível usar identidades existentes do AWS Directory Service, o diretório de usuários da sua empresa ou um provedor de identidades da web. Estes são conhecidos como usuários federados. A AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de um provedor de identidades. Para obter mais informações sobre usuários federados, consulte Usuários e funções federados no Guia do usuário do IAM.

Permissões temporárias de

Um usuário do IAM pode assumir temporariamente uma função para adquirir permissões diferentes para uma tarefa específica.

Acesso entre contas

Você pode usar uma função do IAM para permitir que um principal confiável em outra conta acesse recursos em sua conta. As funções são a principal forma de conceder acesso entre contas. No entanto, com alguns serviços da AWS, é possível anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). O Global Accelerator não oferece suporte a essas políticas baseadas em recurso. Para obter mais informações sobre como escolher usar uma política baseada em função ou uma política baseada em recurso para

permitir acesso entre contas, consulte Controlar o acesso a entidades principais em outra conta.

Acesso ao serviço da AWS

Uma função de serviço é umIAM role (Função do IAM)que um serviço assume para realizar ações em seu nome. As funções de serviço fornecem acesso apenas dentro de sua conta e não podem ser usadas para conceder acesso a serviços em outras contas. Um administrador do IAM pode criar, modificar e excluir uma função de serviço do IAM. Para obter mais informações, consulte Criar uma função para delegar permissões a um serviço da AWS no Guia do usuário do IAM.

Aplicativos em execução no Amazon EC2

Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos em execução em uma instância do EC2 que fazem solicitações AWS API ou da CLI da AWS. É preferível fazer isso do que armazenar chaves de acesso na instância do EC2. Para atribuir uma função da AWS a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, crie um perfil de instância para ser anexado à instância. Um perfil de instância contém a função e permite que programas que estão em execução na instância do EC2 obtenham credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

O que é controle de acesso?

Depois de fazer login (ser autenticado) na AWS, o acesso aos recursos e operações da AWS é regido por políticas. O controle de acesso também é conhecido como autorização.

> **Note**
>
> Para começar a usar rapidamente, ignore esta página. Primeiro, reveja as informações introdutórias emIdentity and Access Management para o AWS Global Acceleratore depois consulteConceitos básicos do IAM.

Durante a autorização, a AWS usa valores doContexto da solicitaçãoPara verificar as políticas aplicáveis. Em seguida, ela usa as políticas para determinar se deve permitir ou negar uma solicitação. A maioria das políticas são armazenadas na AWS como documentos JSON e

especificam as permissões que são permitidas ou negadas aos principais. Para obter mais informações sobre a estrutura e o conteúdo de documentos JSON de políticas, consulte O que são políticas?.

As políticas permitem que um administrador especifique quem tem acesso aos recursos da AWS e quais ações essas pessoas podem realizar neles. Cada entidade do IAM (usuário ou função) começa sem permissões. Em outras palavras, por padrão, os usuários não podem fazer nada, nem mesmo visualizar suas próprias chaves de acesso. Para dar permissão a um usuário para fazer algo, um administrador deve anexar uma política de permissões ao usuário. Ou pode adicionar o usuário a um grupo que tenha as permissões pretendidas. Quando um administrador concede permissões a um grupo, todos os usuários desse grupo obtêm essas permissões.

Você pode ter credenciais válidas para autenticar solicitações, mas, a menos que um administrador conceda permissões a você, você não pode criar nem acessar os recursos do AWS Global Accelerator. Por exemplo, é necessário ter permissões explícitas para criar um acelerador do AWS Global Accelerator.

Como administrador, você pode escrever uma política para controlar o acesso ao seguinte:

- Principais— Controle o que a pessoa ou o aplicativo que está fazendo a solicitação (aprincipal) tem permissão para fazer.
- Identidades do IAM— Controle quais identidades do IAM (grupos, usuários e funções) podem ser acessadas e como.
- Políticas do IAM— Controle quem pode criar, editar e excluir políticas gerenciadas pelo cliente, e quem pode anexar e desanexar todas as políticas gerenciadas.
- Recursos da AWS— controle quem tem acesso aos recursos usando uma política baseada em identidade ou em recurso.
- Contas da AWS— Controle se uma solicitação é permitida somente para membros de uma conta específica.

Controlar o acesso de principais do

As políticas de permissão controlam o que você, como um principal, tem permissão para fazer. Um administrador deve anexar uma política de permissões baseada em identidade à identidade (usuário, grupo ou função) que fornece suas permissões. As políticas de permissões permitem ou negam acesso à AWS. Os administradores também podem definir um limite de permissões para uma entidade do IAM (usuário ou função) para definir o número máximo de permissões que a entidade

pode ter. Os limites de permissões são um recurso avançado do IAM. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

Para obter mais informações e um exemplo de como controlar o acesso à AWS para principais, consulteControlar o acesso de principaisnoGuia do usuário do IAM.

Controlar o acesso às identidades

Os administradores controlam o que você pode fazer para uma identidade do IAM (usuário, grupo ou função) criando uma política que limite o que pode ser feito para uma identidade ou quem pode acessá-la. Em seguida, eles anexam essa política à identidade que fornece suas permissões.

Por exemplo, um administrador pode permitir que você redefina a senha para três usuários específicos. Para fazer isso, eles anexam uma política ao usuário do IAM que permite que você redefina a senha para você mesmo e para os usuários com o ARN dos três usuários especificados. Isso permite que você redefina a senha dos membros de sua equipe, mas não de outros usuários do IAM.

Para obter mais informações e um exemplo de como usar uma política para controlar o acesso à AWS a identidades, consulteControlar o acesso às identidadesnoGuia do usuário do IAM.

Controlar o acesso às políticas

Os administradores podem controlar quem pode criar, editar e excluir políticas gerenciadas pelo cliente, e quem pode anexar e desanexar todas as políticas gerenciadas. Ao revisar uma política, você pode visualizar o resumo de política que inclui um resumo do nível de acesso para cada serviço dentro da política. A AWS categoriza cada ação de serviço em uma das quatroNíveis de acessocom base no que cada ação faz:`List`,`Read`,`Write`, ou`Permissions management`. Você pode usar esses níveis de acesso para determinar quais ações incluir em suas políticas. Para obter mais informações, consulteNoções básicas sobre resumos em nível de acesso em resumos denoGuia do usuário do IAM.

> **Warning**
>
> Você deve limitar`Permissions Management`Permissões de nível de acesso em sua conta. Caso contrário, os membros de sua conta poderão criar políticas para si mesmos com mais permissões do que as que devem ter. Ou podem criar usuários separados com acesso completo à AWS.

Para obter mais informações e um exemplo de como controlar o acesso à AWS a políticas, consulteControlar o acesso às políticasnoGuia do usuário do IAM.

Controlar o acesso aos recursos do

Os administradores podem controlar o acesso aos recursos usando uma política baseada em identidade ou em recurso. Em uma política baseada em identidade, você anexa a política a uma identidade e especifica que recursos essa identidade pode acessar. Em uma política baseada em recursos, você anexa uma política ao recurso que deseja controlar. Na política, você especifica quais entidades principais podem acessar esse recurso.

Para obter mais informações, consulteControle de acesso aos recursosnoGuia do usuário do IAM.

Os criadores de recursos não têm permissões automaticamente

Todos os recursos de uma conta são de propriedade da conta, independentemente de quem os criou. O usuário raiz da conta da AWS é o proprietário da conta e, portanto,A tem permissão para executar qualquer ação em qualquer recurso da conta.

> **Important**
>
> É altamente recomendável que você não use o usuário raiz nas tarefas diárias, nem mesmo nas administrativas. Em vez disso, siga aPrática recomendada de usar o usuário raiz somente para criar seu primeiro usuário do IAM. Depois, armazene as credenciais do usuário raiz com segurança e use-as para executar somente algumas tarefas de gerenciamento de contas e de serviços. Para visualizar as tarefas que exigem que você faça login como usuário raiz, consulteTarefas da AWS que exigem usuário root.

As entidades (usuários ou funções) na conta da AWS devem receber acesso para criar um recurso. No entanto, eles não têm acesso completo a um recurso automaticamente só porque o criaram. Os administradores devem conceder essas permissões explicitamente para cada ação. Além disso, os administradores podem revogar essas permissões a qualquer momento, desde tenham acesso para gerenciar permissões de usuários e funções.

Controlar o acesso a entidades principais em outra conta

Os administradores podem usar políticas baseadas em recurso da AWS, funções entre contas do IAM ou o serviço de AWS Organizations para permitir que os principais de outra conta acessem recursos da conta.

Para alguns serviços da AWS, os administradores podem conceder acesso entre contas para os seus recursos. Para fazer isso, um administrador anexa uma política diretamente ao recurso que deseja compartilhar em vez de usar uma função como um proxy. Se o serviço oferecer suporte a esse tipo de política, o recurso que o administrador compartilha também deve oferecer suporte a políticas baseadas em recurso. Ao contrário de uma política baseada em usuários, uma política baseada em recursos especifica quem (na forma de uma lista de números de ID de contas da AWS) pode acessar aquele recurso. O Global Accelerator não oferece suporte a políticas baseadas em recurso.

O acesso entre contas com uma política baseada em recurso tem algumas vantagens sobre uma função. Com um recurso acessado por meio de uma política baseada em recurso, o principal (pessoa ou aplicativo) ainda trabalha na conta confiável e não precisa abrir mão de suas permissões de usuário no lugar das permissões de função. Em outras palavras, o principal tem acesso aos recursos na conta confiável e, ao mesmo tempo, na conta de confiança. Isso é útil para tarefas como cópia de informações de uma conta para outra. Para obter mais informações sobre o uso de funções entre contas, consulteComo fornecer acesso a um usuário do IAM em outra conta da AWS que você possuinoGuia do usuário do IAM.

As AWS Organizations oferecem gerenciamento baseado em políticas para várias contas da AWS de sua propriedade. Com as Organizations, você pode criar grupos de contas, automatizar a criação de contas e aplicar e gerenciar políticas para esses grupos. As Organizations permitem gerenciar políticas centralmente entre várias contas, sem necessidade de scripts personalizados e processos manuais. Usando as AWS Organizations, você pode criar Service Control Policies (SCPs) que controlam de maneira central o uso de serviços da AWS entre contas da AWS. Para obter mais informações, consulteO que são AWS Organizations?noGuia do usuário das AWS Organizations.

O que são políticas?

Você controla o acesso na AWS criando políticas e anexando-as às identidades do IAM ou aos recursos da AWS.

> **Note**
>
> Para começar a usar rapidamente, ignore esta página. Primeiro, reveja as informações introdutórias emIdentity and Access Management para o AWS Global Acceleratore depois consulteConceitos básicos do IAM.

Uma política é um objeto na AWS que, quando associado a uma entidade ou a um recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade principal, como um usuário, faz uma solicitação. As permissões nas políticas determinam se a solicitação é consentida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, se uma política permitir que oGetUserUm usuário com essa política pode obter informações do usuário no Console de Gerenciamento da AWS, na CLI da AWS ou na API da AWS. Ao criar um usuário do IAM, você pode configurar o usuário para permitir acesso ao console ou programático. O usuário do IAM pode fazer login no console usando um nome de usuário e uma senha. Ou pode usar chaves de acesso para trabalhar com a CLI ou a API.

Os seguintes tipos de política, listados em ordem de frequência, podem afetar se uma solicitação é autorizada. Para obter mais detalhes, consulte .Tipos de políticasnoGuia do usuário do IAM.

Políticas baseadas em identidade

Você pode associar políticas gerenciadas e em linha a identidades do IAM (usuários, grupos aos quais os usuários pertencem e funções).

Políticas baseadas em recursos

Você pode anexar políticas em linha a recursos em alguns serviços da AWS. Os exemplos de políticas baseadas em recurso mais comuns são as políticas de bucket do Amazon S3 e as políticas de confiança de funções do IAM. O Global Accelerator não oferece suporte a políticas baseadas em recurso.

Organizations SCPs

Você pode usar uma política de controle de serviço (SCP) do para aplicar um limite de permissões a uma organização do ou a uma unidade organizacional (UO). Essas permissões são aplicadas a todas as entidades dentro das contas-membro.

Listas de controle de acesso (ACLs)

Você pode usar ACLs para controlar quais entidades principais podem acessar um recurso. As ACLs são semelhantes às políticas baseadas em recurso, embora sejam o único tipo de política que não usa a estrutura de documento de política JSON. O Global Accelerator oferece suporte a OU não oferece suporte a ACLs.

Esses tipos de políticas podem ser categorizados como políticas de permissões ou como limites de permissões.

Políticas de permissões

Você pode associar políticas de permissões a um recurso na AWS para definir as permissões desse objeto. Em uma única conta, a AWS avalia todas as políticas de permissões em conjunto. As políticas de permissões são as políticas mais comuns. Você pode usar os seguintes tipos de políticas como políticas de permissões:

Políticas baseadas em identidade

Quando você anexa uma política gerenciada ou em linha a um usuário, grupo ou função do IAM, a política define as permissões para essa entidade.

Políticas baseadas em recursos

Ao anexar um documento de política JSON a um recurso, você define as permissões desse recurso. O serviço deve ser compatível com políticas baseadas em recurso.

Listas de controle de acesso (ACLs)

Ao anexar uma ACL a um recurso, você define uma lista de entidades principais com permissão para acessar esse recurso. O recurso deve ser compatível com ACLs.

Limites de permissões

Você pode usar políticas para definir o limite de permissões para uma entidade (usuário ou função). Um limite de permissões controla o número máximo de permissões que uma entidade pode ter. Os limites de permissões são um recurso avançado da AWS. Quando mais de um limite de permissões se aplica a uma solicitação, a AWS avalia cada limite de permissões separadamente. Você pode aplicar um limite de permissões nas seguintes situações:

Organizações

Você pode usar uma política de controle de serviço (SCP) do para aplicar um limite de permissões a uma organização do ou a uma unidade organizacional (UO).

Usuários ou funções do IAM

Você pode usar uma política gerenciada para um usuário ou para um limite de permissões da função. Para obter mais informações, consulteLimites de permissões para entidades IAMnoGuia do usuário do IAM.

Tópicos

- Políticas baseadas em identidade

- Políticas baseadas em recursos
- Classificações de nível de acesso à política

Políticas baseadas em identidade

Você pode anexar as políticas a identidades do IAM. Por exemplo, você pode fazer o seguinte:

Anexar uma política de permissões a um usuário ou grupo na sua conta

Para conceder a um usuário permissões para criar um recurso do AWS Global Accelerator, como um acelerador, você pode anexar uma política de permissões a um usuário ou a um grupo ao qual o usuário pertence.

Anexar uma política de permissões a uma função (conceder permissões entre contas)

Você pode associar uma política de permissões baseada em identidade a uma função do IAM para conceder permissões entre contas. Por exemplo, o administrador na conta A pode criar uma função para conceder permissões entre contas a outra conta da AWS (por exemplo, conta B) ou um serviço da AWS da seguinte forma:

1. Um administrador da Conta A cria uma função do IAM e anexa uma política de permissões à função que concede permissões a recursos da conta A.
2. Um administrador da conta A anexa uma política de confiança à função identificando a conta B como a principal, que pode assumir a função.
3. O administrador da conta B pode acabar delegando permissões para assumir a função para todos os usuários na conta B. Isso permite que os usuários na conta B criem ou acessem recursos na conta A. O principal na política de confiança também poderá ser um serviço da AWS principal se você quiser conceder a um serviço da AWS permissões para assumir a função.

Para obter mais informações sobre como usar o IAM para delegar permissões, consulteGerenciamento de acessonoGuia do usuário do IAM.

Para obter mais informações sobre usuários, grupos, funções e permissões, consulte Identidades (usuários, grupos e funções) no Guia do usuário do IAM.

Veja a seguir dois exemplos de políticas que você pode usar com o Global Accelerator O primeiro exemplo de política concede a um usuário acesso programático a todas as ações Lista e Descreva para aceleradores em sua conta da AWS:

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

O exemplo a seguir concede acesso programático à`ListAccelerators`operação:

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

Políticas baseadas em recursos

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. Essas políticas permitem especificar quais ações uma entidade principal especificada pode executar nesse recurso e em quais condições. A política baseada em recurso mais comum é para um bucket do Amazon S3. As políticas baseadas em recurso são políticas em linha que existem apenas no recurso. Não há políticas baseadas em recurso gerenciadas.

A concessão de permissões a membros de outras contas da AWS usando uma política baseada em recurso tem algumas vantagens sobre uma função do IAM. Para mais informações, consulte Como as funções do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Classificações de nível de acesso à política

No console do IAM, as ações são agrupadas usando as seguintes classificações de nível de acesso:

Lista

Fornece permissão para listar recursos dentro do serviço a fim de determinar se um objeto existe. Ações com esse nível de acesso podem listar objetos, mas não podem ver os conteúdos de um recurso. A maioria das ações com o nível de acesso List (Lista) não podem ser executadas em um recurso específico. Ao criar uma declaração de política com essas ações, você deve especificar All resources (Todos os recursos) (`"*"`).

Leia

Oferece permissão para ler, mas não para editar o conteúdo e os atributos de recursos no serviço. Por exemplo, as operações do Amazon S3`GetObject`e`GetBucketLocation`Tenha oLeiaNível de acesso.

Gravação

Oferece permissão para criar, excluir ou modificar recursos no serviço. Por exemplo, as operações do Amazon S3`CreateBucket`,`DeleteBucket`, e`PutObject`Tenha oGravaçãoNível de acesso.

Gerenciamento de permissões

Fornece permissão para conceder ou modificar permissões de recursos no serviço. Por exemplo, a maioria das ações de políticas do IAM e das AWS Organizations têm oGerenciamento de permissõesNível de acesso.

> **Tip**
>
> Para melhorar a segurança da sua conta da AWS, restrinja ou monitore regularmente políticas que incluam aGerenciamento de permissõesclassificação de nível de acesso.

Atribuição de tags (tagging)

Fornece permissão para criar, excluir ou modificar tags que são anexadas a um recurso no serviço. Por exemplo, o Amazon EC2`CreateTags`e`DeleteTags`as operações têm oAtribuição de tags (tagging)Nível de acesso.

Conceitos básicos do IAM

O AWS Identity and Access Management (IAM) é um serviço da AWS que permite gerenciar o acesso aos serviços e aos recursos da com segurança. O IAM é um recurso da conta da AWS oferecido gratuitamente.

> **Note**
>
> Antes de começar a usar o IAM, revise as informações introdutórias emIdentity and Access Management para o AWS Global Accelerator.

Ao criar uma conta do AWS pela primeira vez, você começa com uma única identidade de login que tem acesso completo a todos os serviços e recursos da AWS na conta. Essa identidade é denominada usuário raiz da conta da AWS e é acessada pelo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável que você não use o usuário raiz nas tarefas diárias, nem mesmo nas administrativas. Em vez disso, siga as práticas recomendadas para o uso do usuário raiz somente a fim de criar seu primeiro usuário do IAM. Depois, armazene as credenciais do usuário raiz com segurança e use-as para executar somente algumas tarefas de gerenciamento de contas e de serviços.

Crie seu usuário administrador do IAM

Para criar um usuário administrador para você mesmo e adicionar o usuário a um grupo de administradores (console)

1. Faça login no console do IAM como o proprietário da conta escolhendo Root user (Usuário raiz) e inserindo seu endereço de e-mail da conta da AWS. Na próxima página, insira sua senha.

   > **Note**
   >
   > Recomendamos seguir as melhores práticas para utilizar o**`Administrator`**Usuário do IAM que segue e armazene as credenciais do usuário raiz com segurança. Cadastre-se como o usuário raiz apenas para executar algumas tarefas de gerenciamento de serviços e contas.

2. No painel de navegação, escolha Usuários e depois Adicionar usuário.
3. Em User name (Nome do usuário), digite **`Administrator`**.

4. Marque a caixa de seleção ao lado de AWS Management Console access (Acesso ao Console de Gerenciamento da AWS). Então, selecione Custom password (Senha personalizada), e insira sua nova senha na caixa de texto.
5. (Opcional) Por padrão, a AWS exige que o novo usuário crie uma senha ao fazer login pela primeira vez. Você pode desmarcar a caixa de seleção próxima de User must create a new password at next sign-in (O usuário deve criar uma senha no próximo login) para permitir que o novo usuário redefina a senha depois de fazer login.
6. SelecionePróximo: Permissões
7. Em Set permissions (Conceder permissões), escolha Add user to group (Adicionar usuário ao grupo).
8. Escolha Create group (Criar grupo).
9. Na caixa de diálogo Create group (Criar grupo), em Group name (Nome do grupo), digite **`Administrators`**.
10. SelecionePolíticas de filtroe depois selecioneAWS gerenciado — função de trabalhopara filtrar o conteúdo da tabela.
11. Na lista de políticas, marque a caixa de seleção AdministratorAccess. A seguir escolha Criar grupo.

    > **Note**
    >
    > Ative acesso do usuário e da função do IAM ao Faturamento para poder usar as permissões de `AdministratorAccess` para acessar o console de Gerenciamento de custos e faturamento da AWS. Para fazer isso, siga as instruções na etapa 1 do tutorial sobre como delegar acesso ao console de faturamento.

12. Suporte a lista de grupos, selecione a caixa de seleção para seu novo grupo. Escolha Refresh (Atualizar) caso necessário, para ver o grupo na lista.
13. SelecionePróximo: Tags.
14. (Opcional) Adicione metadados ao usuário anexando tags como pares de chave-valor. Para obter mais informações sobre como usar tags no IAM, consulte Marcar entidades do IAM no Guia do usuário do IAM.
15. SelecionePróximo: Review (Revisar)Para ver a lista de associações a grupos a serem adicionadas ao novo usuário. Quando você estiver pronto para continuar, selecione Criar usuário.

É possível usar esse mesmo processo para criar mais grupos e usuários e conceder aos usuários acesso aos recursos da conta da AWS. Para saber como usar políticas para restringir as permissões de usuário a recursos específicos da AWS, consulte Gerenciamento de acesso e Políticas de exemplo.

Criar usuários delegados para o Global Accelerator

Para oferecer suporte a vários usuários na conta da AWS, você deve delegar permissão para permitir que outras pessoas executem apenas as ações que deseja permitir. Para fazer isso, crie um grupo do IAM com as permissões de que essas pessoas precisam e adicione usuários do IAM aos grupos necessários ao criá-los. Você pode usar esse processo para configurar os grupos, os usuários e as permissões para toda a conta da AWS. Essa solução é mais bem usada por organizações pequenas e médias em que um administrador da AWS pode gerenciar manualmente os usuários e os grupos. Para grandes organizações, você pode usarFunções personalizadas do IAM,federação, ouLogon único do.

No procedimento a seguir, você cria três usuários chamados**`arnav`**,**`carlos`**, e**`martha`**e anexe uma política que concede permissão para criar um acelerador chamado**`my-example-accelerator`**, mas apenas nos próximos 30 dias. Você pode usar as etapas fornecidas aqui para adicionar usuários com diferentes permissões.

Para criar um usuário delegado para outra pessoa (console)

1. Faça login no Console de Gerenciamento da AWS e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Usuários e depois Adicionar usuário.
3. Em User name (Nome do usuário), digite **`arnav`**.
4. Escolha Add another user (Adicionar outro usuário) e digite **`carlos`** para o segundo usuário. Em seguida, escolha Add another user (Adicionar outro usuário) e digite **`martha`** para o terceiro usuário.
5. Marque a caixa de seleção ao lado deAcesso ao Console de Gerenciamento da AWSe depois selecioneAutogenerated password.
6. Desmarque a caixa de seleção próxima de User must create a new password at next sign-in (O usuário deve criar uma senha no próximo login) para permitir que o novo usuário redefina a senha depois de fazer login.
7. SelecionePróximo: Permissões

8. Selecione Attach existing policies directly. Você criará uma nova política gerenciada para os usuários.
9. Escolha Create policy (Criar política).

   A página Create policy (Criar política) é aberta em uma nova guia ou janela do navegador.
10. Na guia Editor visual, selecione Escolher um serviço. Em seguida, escolha Global Accelerator. Você pode usar a caixa de pesquisa na parte superior para limitar os resultados da lista de serviços.

    OServiçofecha e a seçãoAçõesabre automaticamente.
11. Escolha as ações do Global Accelerator que você deseja permitir. Por exemplo, para conceder permissão para criar um acelerador, insira**`globalaccelerator:CreateAccelerator`**noAções de filtro. Quando a lista de ações do Global Accelerator for filtrada, marque a caixa de seleção ao lado de**`globalaccelerator:CreateAccelerator`**.

    As ações do Global Accelerator são agrupadas por classificação de nível de acesso para facilitar a determinação rápida do nível de acesso que cada ação fornece. Para obter mais informações, consulte Classificações de nível de acesso à política.
12. Se as ações selecionadas nas etapas anteriores não oferecerem suporte à escolha de recursos específicos, então oTodos os recursosestá selecionado para você. Nesse caso, você não pode editar esta seção.

    Se você escolher uma ou mais ações que ofereçam suporte a permissões em nível de recurso, o editor visual listará esses tipos de recurso na seção Resources (Recursos). SelecioneVocê escolheu as ações que exigem oAccelerator doTipo de recurso doPara escolher se você deseja inserir um acelerador específico para a política.
13. Se você desejar permitir a ação `globalaccelerator:CreateAccelerator` para todos os recursos, escolha All resources (Todos os recursos).

    Se você desejar especificar um recurso, escolha Add ARN (Adicionar ARN). Especifique a região e o ID da conta (ou ID da conta) (ou escolhaQuaisquer) e, em seguida, digite**`my-example-accelerator`**para o recurso. Em seguida, escolha Adicionar.
14. Escolha Specify request conditions (optional) (Especificar condições de solicitação (opcional)).
15. SelecioneAdicionar condiçãoConcede permissão para criar um aceleradornos próximos 7 dias. Suponha que hoje seja 1º de janeiro de 2019.

16. Em Condition Key (Chave de condição), escolha aws:CurrentTime. Essa chave de condição verifica a data e a hora em que o usuário faz a solicitação. Ela retorna verdadeiro (e, portanto, permitirá a ação **`globalaccelerator:CreateAccelerator`** apenas se a data e a hora estiverem dentro do intervalo especificado).
17. para oQualifier, mantenha o valor padrão.
18. Para especificar o início do intervalo de data e hora permitido, em Operator (Operador), escolha DateGreaterThan. Em seguida, em Value (Valor), digite **`2019-01-01T00:00:00Z`**.
19. Escolha Add (Adicionar) para salvar a condição.
20. Escolha Add another condition (Adicionar outra condição) para especificar a data de término.
21. Siga etapas semelhantes para especificar o término do intervalo de data e hora permitido. Em Condition Key (Chave de condição), escolha aws:CurrentTime. Em Operator (Operador), escolha DateLessThan. Em Value (Valor), digite **`2019-01-06T23:59:59Z`**, sete dias depois da primeira data. Em seguida, escolha Add (Adicionar) para salvar a condição.
22. (Opcional) Para ver o documento JSON da política que você está criando, escolha a opçãoJSON. Você pode alternar entre as guias Editor visual e JSON sempre que quiser. No entanto, se você fizer alterações ou escolherRevisar políticanoEditor visual, o IAM pode reestruturar sua política a fim de otimizá-la para o editor visual. Para obter mais informações, consulteReestruturação da políticanoGuia do usuário do IAM.
23. Ao concluir, selecione Revisar política.
24. NoRevisar política, paraName (Nome), insira**`globalaccelerator:CreateAcceleratorPolicy`**. Em Descrição, insira **`Policy to grants permission to create an accelerator`**. Revise o resumo da política para assegurar-se de ter concedido as permissões que pretendia e, em seguida, escolha Criar política para salvar sua nova política.
25. Retorne para a guia ou a janela original e atualize a lista de políticas.
26. Na caixa de pesquisa, insira **`globalaccelerator:CreateAcceleratorPolicy`**. Marque a caixa de seleção ao lado da nova política. Em seguida, escolha Próxima etapa.
27. SelecionePróximo: Review (Revisar)Para visualizar os novos usuários. Quando você estiver pronto para continuar, escolha Create users (Criar usuários).
28. Faça download ou copie as senhas dos novos usuários e as envie aos usuários com segurança. Separadamente, forneça aos seus usuários umlink para a página do console do usuário do IAMe os nomes de usuário que você acabou de criar.

Permitir que usuários do gerenciem automaticamente suas credenciais

Você deve ter acesso físico ao hardware que hospedará o dispositivo MFA virtual do usuário para configurar a MFA. Por exemplo, você pode configurar a MFA para um usuário que usa um dispositivo MFA virtual executando em um smartphone. Neste caso, você precisa que o smartphone esteja disponível para concluir o assistente. Por isso, você pode optar por permitir que os usuários configurem e gerenciem seus próprios dispositivos MFA virtual. Neste caso, você deve conceder aos usuários permissões para executar as ações do IAM necessárias.

Para criar uma política para permitir autogerenciamento de credenciais (console)

1. Faça login no Console de Gerenciamento da AWS e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Políticas e, em seguida, Criar política.
3. Escolha a guia JSON e copie o texto do documento de política JSON a seguir. Cole este texto na caixa de texto do JSON.

> **Important**
>
> Esta política de exemplo não permite que os usuários redefinam sua senha ao fazer login. Novos usuários e usuários com a senha expirada podem tentar fazer isso. É possível permitir isso adicionando `iam:ChangePassword` e `iam:CreateLoginProfile` à instrução `BlockMostAccessUnlessSignedInWithMFA`. No entanto, o IAM não recomenda isso.

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

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

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

```
}
```

O que essa política faz?

- O`AllowAllUsersToListAccounts`A instrução permite que o usuário veja informações básicas sobre a conta e seus usuários no console do IAM. Essas permissões devem estar nas suas respectivas instruções, pois não oferecem suporte ou não precisam especificar o nome de recurso da Amazon (ARN) de um determinado recurso, mas especificam `"Resource" : "*"`.
- O`AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation`A instrução permite que o usuário gerencie suas próprias informações de usuário, senha, chaves de acesso, certificados de assinatura, chaves públicas SSH e MFA no console do IAM. Ela também permite que os usuários façam login pela primeira vez em um administrador e exige que definam uma senha da primeira vez. O nome de recurso da ARN do recurso limita o uso dessas permissões a apenas a entidade de usuário do IAM do próprio usuário.
- A instrução `AllowIndividualUserToViewAndManageTheirOwnMFA` permite que o usuário visualize ou gerencie seu próprio dispositivo MFA. Observe que os ARNs dos recursos dessa instrução permitem acesso somente a um dispositivo MFA ou usuário que tenha exatamente o mesmo nome do usuário conectado. Os usuários não podem criar nem alterar nenhum dispositivo MFA que não sejam os seus próprios.
- A instrução `AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA` permite que o usuário desative somente seu próprio dispositivo MFA, e somente se o usuário fez login usando a MFA. Isso evita que outras pessoas que tenham somente as chaves de acesso (e não o dispositivo MFA) desativem o dispositivo MFA e acessem a conta.
- O`BlockMostAccessUnlessSignedInWithMFA`usa uma combinação de`"Deny"`e`"NotAction"`para negar acesso a todas as ações, exceto algumas, no IAM e em outros serviços da AWSseo usuário não está conectado com a MFA. Para obter mais informações sobre a lógica dessa instrução, consulteNotAction com DenynoGuia do usuário do IAM. Se o usuário tiver feito login com a MFA, ocorrerá uma falha no teste `"Condition"`, e a instrução “negar” final não terá efeito e outras políticas ou instruções para o usuário determinarão suas permissões. Essa instrução garante que quando o usuário não tiver feito login com a MFA, ele só possa executar as ações listadas e somente se outra instrução ou política conceder acesso a essas ações.

A versão `...IfExists` do operador `Bool` garante que se a chave `aws:MultiFactorAuthPresent` estiver ausente, a condição retornará verdadeiro. Isso significa que, ao acessar uma API com credenciais de longo prazo, como uma chave de acesso, o usuário terá seu acesso negado às operações de API não relacionadas ao IAM.

4. Ao concluir, selecione Revisar política.
5. Na página Review (Revisar), digite **`Force_MFA`** para o nome da política. Para obter a descrição da política, insira**`This policy allows users to manage their own passwords and MFA devices but nothing else unless they authenticate with MFA.`**Revisar a políticaSummary (Resumo)Para ver as permissões concedidas pela política e, em seguida, escolhaCriar políticapara salvar seu trabalho.

   A nova política aparece na lista de políticas gerenciadas e está pronta para ser anexada.

Para anexar a política a um usuário (console)

1. No painel de navegação, escolha Usuários.
2. Escolha o nome (não a caixa de seleção) do usuário que você deseja editar.
3. Na guia Permissions (Permissões), escolha Add permissions (Adicionar permissões).
4. Selecione Attach existing policies directly.
5. Na caixa de pesquisa, digite **`Force`** e, em seguida, marque a caixa de seleção ao lado de Force_MFA na lista. Depois, selecione Next (Próximo): Review (Revisar).
6. Reveja as alterações e escolha Add permissions (Adicionar permissões).

Habilitar MFA para o usuário do IAM

Para obter mais segurança, recomendamos que todos os usuários do IAM configurem a autenticação multifator (MFA) para ajudar a proteger seus recursos do Global Accelerator. A MFA adiciona mais segurança porque requer que os usuários forneçam autenticação exclusiva de um dispositivo MFA com suporte da AWS, além de suas credenciais de login normais. O dispositivo MFA da AWS mais seguro é a chave de segurança U2F. Se sua empresa já tiver dispositivos U2F, recomendamos habilitar esses dispositivos para a AWS. Caso contrário, você deverá comprar um dispositivo para cada um dos usuários e esperar pela chegada do hardware. Para obter mais informações, consulteHabilitar uma chave de segurança U2FnoGuia do usuário do IAM.

Se você não tiver um dispositivo U2F, poderá começar a usar rapidamente e a um baixo custo habilitando um dispositivo MFA virtual. Isso exige que você instale um aplicativo de software em um telefone ou outro dispositivo móvel existente. O dispositivo gera um código numérico de seis dígitos com base em um algoritmo de senha única sincronizado com o tempo. Quando o usuário fizer login na AWS, ele será solicitado a inserir um código do dispositivo. Cada dispositivo MFA virtual atribuído a um usuário deve ser exclusivo. Um usuário não pode digitar um código de outro dispositivo MFA virtual para se autenticar. Para obter uma lista de alguns aplicativos compatíveis que podem ser usados como dispositivos MFA virtuais, consulte a página Autenticação multifator.

> **Note**
>
> Você deve ter acesso físico ao dispositivo móvel que hospedará o dispositivo MFA virtual do usuário para configurar a MFA para um usuário do IAM.

Para habilitar um dispositivo MFA virtual para um usuário do IAM (console)

1. Faça login no Console de Gerenciamento da AWS e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Usuários.
3. Na lista Nome do usuário, selecione o nome do usuário de MFA desejado.
4. Selecione a guia Credenciais de segurança. Ao lado de Dispositivo MFA atribuído, escolha Gerenciar.
5. No assistente Gerenciar dispositivo MFA, selecione Dispositivo MFA virtual e, em seguida, selecione Continuar.

   O IAM gera e exibe informações de configuração para o dispositivo MFA virtual, incluindo um código QR gráfico. O gráfico é uma representação da "chave de configuração secreta" que está disponível para entrada manual em dispositivos que não suportam códigos QR.
6. Abra o seu aplicativo de MFA virtual.

   Para obter uma lista de aplicativos que você pode usar para hospedar dispositivos MFA virtuais, consulte Autenticação multifator. Se o aplicativo de MFA virtual oferecer suporte a várias contas (vários dispositivos MFA virtuais), selecione a opção para criar uma nova conta (um novo dispositivo MFA virtual).
7. Determine se o aplicativo de MFA é compatível com códigos QR e, em seguida, execute uma das seguintes ações:

- No assistente, escolha Mostrar código de QR e, em seguida, use o app para digitalizar o código de QR. Por exemplo, você pode escolher o ícone de câmera ou escolher uma opção semelhante a Digitalizar código e, em seguida, usar a câmera do dispositivo para digitalizar o código.
- No assistente Manage MFA Device (Gerenciar dispositivo MFA), selecione Show secret key (Mostrar chave secreta) e, em seguida, digite a chave secreta em seu aplicativo MFA.

Quando você tiver concluído, o dispositivo MFA virtual inicia a geração de senhas de uso único.

8. No assistente Manage MFA Device (Gerenciar dispositivo MFA), na caixa MFA code 1 (Código MFA 1), digite a senha de uso único exibida no momento no dispositivo MFA virtual. Espere até 30 segundos para que o dispositivo gere uma nova senha de uso único. Em seguida, digite a segunda senha de uso único na caixa MFA code 2 (Código MFA 2). Escolha Atribuir MFA.

> **Important**
>
> Envie sua solicitação imediatamente após gerar os códigos. Se você gerar os códigos e esperar muito tempo para enviar a solicitação, o dispositivo MFA associa com êxito ao usuário, mas o dispositivo MFA está fora de sincronia. Isso ocorre porque as senhas únicas baseadas em tempo (TOTP) expiram após um curto período. Caso isso ocorra, você pode ressincronizar o dispositivo. Para obter mais informações, consulteSincronizar novamente dispositivos MFA virtuais e de hardwarenoGuia do usuário do IAM.

O dispositivo MFA virtual está pronto para uso com a AWS.

Conexões seguras da VPC no AWS Global Accelerator

Ao adicionar um Application Load Balancer interno ou um endpoint de instância do Amazon EC2 no AWS Global Accelerator, você permite que o tráfego da Internet flua diretamente de e para o endpoint em Virtual Private Clouds (VPCs) direcionando-o em uma sub-rede privada. A VPC que contém o load balancer ou a instância do EC2 deve ter umgateway de Internetanexado a ele, para indicar que a VPC aceita tráfego de 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 de Internet associada para a sub-rede.

Isso é diferente do caso de uso típico do gateway da Internet em que os endereços IP públicos e as rotas de 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 de 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 através do O Accelerator também retorna através do Global Accelerator em vez de através do gateway de Internet.

> **Note**
>
> Usar endereços IP públicos e usar uma sub-rede pública para suas instâncias do Amazon EC2 não são típicos, embora seja possível configurar sua configuração com elas. Os grupos de segurança se aplicam a qualquer tráfego que chegue às suas instâncias, incluindo tráfego do Global Accelerator e qualquer endereço público ou Elastic IP atribuído à sua instância ENI. Use sub-redes privadas para garantir que o tráfego seja entregue somente pelo Global Accelerator.

Tenha essas informações em mente ao considerar problemas de perímetro de rede e configurar privilégios do IAM relacionados ao gerenciamento de acesso à Internet. Para obter mais informações sobre como controlar o acesso à Internet à VPC, consulte esteExemplo de política de controle de serviço.

Registro em log e monitoramento no AWS Global Accelerator

O monitoramento é uma parte importante da manutenção da confiabilidade e do desempenho 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 ser mais fácil realizar a depuração de uma falha de vários pontos (caso ocorra). A AWS fornece várias ferramentas para monitorar os recursos do Global Accelerator e responder a possíveis incidentes:

Logs de fluxo do AWS Global Accelerator

Os logs de fluxo do servidor fornecem registros detalhados sobre o tráfego que flui através de um acelerador para um ponto de extremidade. Os logs de fluxo do servidor são úteis para muitos aplicativos. Por exemplo, as informações de log de fluxo podem ser úteis em auditorias de segurança e acesso. Para obter mais informações, consulte Logs de fluxo no AWS Global Accelerator.

Métricas e alarmes do Amazon CloudWatch

Com o CloudWatch, você pode monitorar, em tempo real, os recursos da AWS e os aplicativos que você executa na AWS. O CloudWatch coleta e rastreia métricas, que são variáveis que você mede ao longo do tempo. É possível criar alarmes que observem métricas específicas e enviem notificações ou façam alterações automaticamente nos recursos que você está monitorando quando a métrica excede um determinado limite por um período de tempo. Para obter mais informações, consulte Usando o Amazon CloudWatch com o AWS Global Accelerator.

Logs do AWS CloudTrail

O CloudTrail fornece um registro de ações executadas por um usuário, uma função ou um serviço da AWS no Global Accelerator. O CloudTrail captura todas as chamadas de API do Global Accelerator como eventos, incluindo chamadas do console do Global Accelerator e chamadas de código para a API do Global Accelerator. Para obter mais informações, consulte Usando o AWS CloudTrail para registrar chamadas de API do AWS Global Accelerator.

Validação de conformidade do AWS Global Accelerator

Auditores terceiros avaliam a segurança e a conformidade do AWS Global Accelerator como parte de vários programas de conformidade da AWS. Isso inclui SOC, PCI, HIPAA, GDPR, ISO e ENS High.

Para obter uma lista dos serviços da AWS, incluindo o Global Accelerator, no escopo de programas de conformidade específicos, consulteServiços da AWS no escopo por programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

É possível fazer download de relatórios de auditoria externa usando o AWS Artifact. Para obter mais informações, consulteFazer download de relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Global Accelerator é determinada pela confidencialidade dos dados, pelos objetivos de conformidade da empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- Guias Quick Start de segurança e conformidade – esses guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de linha de base focados em conformidade e segurança na AWS.
- Whitepaper Arquitetura para segurança e conformidade com HIPAA – esse whitepaper descreve como as empresas podem usar a AWS para criar aplicativos em conformidade com a HIPAA.

- Recursos de conformidade da AWS – esta coleção de manuais e guias pode ser aplicada ao seu setor e local.
- 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.
- Security Hub da AWS – esse serviço da AWS fornece uma visão abrangente do estado da segurança na AWS que ajuda você a verificar sua conformidade com padrões e melhores práticas de segurança do setor.

Resiliência no AWS Global Accelerator

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões da AWS fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, altas taxas de transferência e redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicativos 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 obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

Além do suporte da infraestrutura global da AWS, o Global Accelerator oferece os seguintes recursos que ajudam a oferecer suporte à resiliência de dados:

- Uma zona de rede atende os endereços IP estáticos do acelerador a partir de uma sub-rede IP exclusiva. Semelhante a uma zona de disponibilidade da AWS, uma zona de rede é uma unidade isolada com seu próprio conjunto de infraestrutura física. Quando você configura um acelerador, o Global Accelerator aloca dois endereços IPv4 para ele. Se um endereço IP de uma zona de rede ficar indisponível devido ao bloqueio de endereços IP por determinadas redes cliente ou devido a interrupções de rede, os aplicativos cliente podem tentar novamente no endereço IP estático íntegro da outra zona de rede isolada.
- O Global Accelerator monitora continuamente a integridade de todos os endpoints. Quando ele 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

Como serviço gerenciado, o AWS Global Accelerator é protegido pelos procedimentos de segurança da rede global da AWS descritos naAmazon Web Services: Visão geral dos processos de segurançaWhitepaper.

Use as chamadas de API publicadas da AWS para acessar o Global Accelerator por meio da rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos TLS 1.2 ou posterior. Os clientes também devem ter suporte a pacotes de criptografia com sigilo de encaminhamento perfeito (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece suporte a 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 do AWS Global Accelerator

Sua conta da AWS tem cotas específicas, também chamadas de limites, relacionadas ao AWS Global Accelerator.

O console de Service Quotas fornece informações sobre as cotas do Global Accelerator. Além de exibir as cotas padrão, você pode usar o console de Service Quotas paraaumentos de cotapara quotas ajustáveis. Observe que você deve estar no Leste dos EUA (Norte da Virgínia) ao solicitar aumentos de cota para o Global Accelerator.

Tópicos

Cotas gerais

Veja a seguir as cotas gerais para o Global Accelerator.

Entidade	Quota
Aceleradores por conta da AWS	20 Você podeSolicitar um aumento de cota.
Listeners por acelerador	10 Você podeSolicitar um aumento de cota.
Intervalos de portas por ouvinte	10
Substituições de porta por grupo de endpoint	10 Você podeSolicitar um aumento de cota.

Cotas para endpoints por grupo de endpoint

Veja a seguir as cotas do Global Accelerator que se aplicam ao número de endpoints em grupos de endpoint.

Entidade	Descrição	Quota
Grupos de endpoints com mais de um tipo de endpoint	Número de endpoints em um grupo de endpoint que contém mais de um tipo de endpoint.	10
Grupos de terminais com apenas Application Load Balancers	Número de Application Load Balancers em um grupo de endpoint contendo apenas os pontos finais do Application Load Balancer.	10
Grupos de terminais com apenas balanceadores de carga de rede	Número de balanceadores de carga de rede em um grupo de endpoint contendo apenas pontos finais do Network Load Balancer.	10
Grupos de endpoints com instâncias do Amazon EC2	Número de instâncias EC2 em um grupo de endpoints contendo apenas endpoints de instância EC2.	10 Você pode Solicitar um aumento de cota.
Grupos de endpoints com apenas endereços Elastic IP	Número de endereços Elastic IP em um grupo de endpoint contendo apenas endpoints de endereço Elastic IP.	10 Você pode Solicitar um aumento de cota.
Grupos de endpoints com sub-redes do Amazon Virtual Private Cloud	Número de sub-redes da Amazon VPC em um grupo de endpoint contendo apenas endpoints de sub-rede.	10 Você pode Solicitar um aumento de cota.

Cotas relacionadas

Além de cotas no Global Accelerator, há cotas que se aplicam aos recursos usados como endpoints para um acelerador. Para obter mais informações, consulte:

- Cotas de endereços IP elásticosnoGuia do usuário do Amazon EC2.
- Cotas de serviço do Amazon EC2noGuia do usuário do Amazon EC2.
- Cotas para os Network Load BalancersnoGuia do usuário para Network Load Balancers.
- Cotas para os Application Load BalancersnoGuia do usuário para Application Load Balancers.
- Cotas da Amazon VPCnoGuia do usuário do 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

Documentação adicional do AWS Global Accelerator

Os recursos relacionados a seguir podem ajudar você à medida que trabalha com este serviço.

- Referência da API do AWS Global Accelerator: fornece descrições completas de ações de API, parâmetros e tipos de dados, além de uma lista de erros retornados pelo serviço.
- Informações sobre o produto AWS Global Accelerator: a principal página da Web para obter informações sobre o Global Accelerator, incluindo recursos e definições de preços.
- Termos de usoInformações detalhadas sobre os nossos direitos autorais e marca registrada; a sua conta, licença e acesso ao site e outros tópicos.

Obter suporte

O Support para o Global Accelerator está disponível em várias formas.

- Fóruns de discussãoUm fórum comunitário para que os desenvolvedores discutam questões técnicas relacionadas ao Global Accelerator.
- AWS Support Center: este site reúne informações sobre seus casos de suporte e resultados do AWS Trusted Advisor recentes e de verificações de integridade, além de fornecer links para fóruns de discussão, perguntas técnicas frequentes, o painel de status dos serviços e informações sobre os planos do AWS Support.
- Informações sobre o AWS Premium Support: a principal página da Web para obter informações sobre o AWS Premium Support, um canal de suporte de resposta rápida e com atendimento individual, para ajudá-lo 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 Amazon Web Services

O Blog da AWS tem vários posts para ajudar você a usar os serviços da AWS. Por exemplo, consulte as seguintes postagens do blog sobre o Global Accelerator:

- AWS Global Accelerator para disponibilidade e desempenho
- Gerenciamento de tráfego com AWS Global Accelerator
- Analisando e visualizando logs de fluxo do AWS Global Accelerator usando o Amazon Athenae o Amazon QuickSight

Para obter uma lista completa de blogs do AWS Global Accelerator, consulteAWS Global Acceleratorna categoria Rede e entrega de conteúdo das postagens de 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 de documentação: 9 de dezembro de 2020

Alteração	Descrição	Data
Atualização para a função vinculada ao serviço existente do Global Accelerator	Global Accelerator adicionou uma nova permissão ,`ec2:DescribeRegions` , para permitir que o Global Accelerator obtenha informações sobre a região da AWS para ajudar a diagnosticar erros. Para obter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/security-iam-awsmanpol-updates.html.	7 de maio de 2021
Adicionados aceleradores de roteamento personalizados	O Global Accelerator introduziu um novo tipo de aceleradores de roteamento personalizados do acelerador. Os aceleradores de roteamento personalizados funcionam bem para cenários em que você deseja usar a lógica de aplicativo personalizada para direcionar um ou mais usuários para um destino específico e uma porta entre muitos, enquanto ainda obtém	9 de dezembro de 2020

Alteração	Descrição	Data
	os benefícios de desempenho do Global Accelerator. Para obter mais informações, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/work-with-custom-routing-accelerators.html.	
Adicionado suporte a substituições de porta	Agora, o Global Accelerator oferece suporte à substituição da porta do listener usada para rotear o tráfego para endpoints para que você possa redirecionar o tráfego para portas específicas em seus endpoints. Para obter 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	Agora o Global Accelerator oferece suporte a África (Cidade do Cabo) e Europa (Milão). Para obter 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
Marcação e BYOIP	Esta versão adiciona suporte para adicionar tags aos aceleradores e trazer seu próprio endereço IP para o AWS Global Accelerator (BYOIP). Para obter 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	Adicionado conteúdo para conformidade, resiliência e segurança de infraestrutura. Para obter mais informaçõ es, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/security.html.	20 de dezembro de 2019

Alteração	Descrição	Data
Support para instâncias do EC2 e nome DNS padrão	O AWS Global Accelerator agora oferece suporte à adição de instâncias do EC2 em regiões da AWS compatíveis. Além disso, o Global Accelerator cria um nome DNS padrão que é mapeado para os endereços IP estáticos do acelerador. Para obter 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 de endereço IP do cliente para Application Load Bal	Agora você pode optar por fazer com que o AWS Global Accelerator preserve o endereço IP do cliente para Application Load Balancers em regiões da AWS compatíveis. Para obter 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 AWS Global Accelerator	O AWS Global Accelerator Developer Guide fornece informações sobre como configurar e usar aceleradores — gerenciadores de tráfego de 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

Glossário da AWS

Para obter a terminologia mais recente da AWS, consulte o Glossário da AWS na Referência geral da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.