aws

Guía para desarrolladores

AWS Global Accelerator

AWS Global Accelerator: Guía para desarrolladores

Table of Contents

¿Qué es AWS Global Accelerator?

AWS Global Accelerator es un servicio en el que se creaAceleradores dePara mejorar el rendimiento de sus aplicaciones para usuarios locales y globales. Dependiendo del tipo de acelerador que elija, puede obtener beneficios adicionales.

- Mediante el uso de un acelerador estándar, puede mejorar la disponibilidad de las aplicaciones de Internet destinadas al público general. Con un acelerador estándar, Global Accelerator dirige el tráfico a través de la red global de AWS a los puntos finales de la región más cercana al cliente.
- Mediante un acelerador de enrutamiento personalizado, puede asignar uno o más usuarios a un destino específico entre muchos destinos.

Global Accelerator es un servicio global que admite puntos finales en varias regiones de AWS, que se enumeran en laTabla Región de AWS Region.

De forma predeterminada, Global Accelerator proporciona dos direcciones IP estáticas que se asocian con el acelerador. Con un acelerador estándar, en lugar de utilizar las direcciones IP que proporciona Global Accelerator, puede configurar estos puntos de entrada para que sean direcciones IPv4 de sus propios rangos de direcciones IP que lleve a Global Accelerator. Las direcciones IP estáticas se transmiten desde la red perimetral de AWS.

> **Important**
>
> Las direcciones IP estáticas permanecen asignadas al acelerador durante el tiempo que exista, incluso si deshabilita el acelerador y ya no acepta ni enruta el tráfico. Sin embargo, cuandodeleteun acelerador, pierde las direcciones IP estáticas que se le asignan, por lo que ya no puede enrutar el tráfico usándolas. Puede utilizar directivas de IAM como permisos basados en etiquetas con Global Accelerator para limitar los usuarios que tienen permisos para eliminar un acelerador. Para obtener más información, consulte Políticas basadas en etiquetas.

Para los aceleradores estándar, Global Accelerator utiliza la red global de AWS para enrutar el tráfico hacia el punto final regional óptimo en función del estado, la ubicación del cliente y las políticas que configure, lo que aumenta la disponibilidad de las aplicaciones. Los extremos de los aceleradores estándar pueden ser equilibradores de carga de red, equilibradores de carga de aplicaciones, instancias de Amazon EC2 o direcciones IP elásticas que se encuentran en una región de AWS o en

varias regiones. El servicio reacciona instantáneamente a los cambios en el estado o la configuración para garantizar que el tráfico de Internet de los clientes siempre se dirige a los puntos finales en buen estado.

Los aceleradores de enrutamiento personalizados solo admiten tipos de endpoints de subred de nube privada virtual (VPC) y enrutan el tráfico a direcciones IP privadas de esa subred.

Para obtener una lista de las regiones de AWS donde se admiten actualmente el acelerador global y otros servicios, consulte laTabla Región de AWS Region.

Temas

Componentes de AWS Global Accelerator

AWS Global Accelerator incluye los componentes siguientes:

Direcciones IP estáticas

Global Accelerator le proporciona un conjunto de dos direcciones IP estáticas que se transmiten desde la red perimetral de AWS. Si lleva su propio rango de direcciones IP a AWS (BYOIP) para usarlas en Global Accelerator, puede asignar direcciones IP de su propio grupo para usarlas en el acelerador. Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en el AWS Global Accelerator.

Las direcciones IP sirven como puntos de entrada fijos únicos para sus clientes. Si ya tiene configurados los equilibradores de carga de Elastic Load Balancing, las instancias de Amazon EC2 o los recursos de dirección IP Elastic para sus aplicaciones, puede agregarlos fácilmente

a un acelerador estándar en Global Accelerator. Esto permite a Global Accelerator utilizar direcciones IP estáticas para acceder a los recursos.

Las direcciones IP estáticas permanecen asignadas al acelerador durante el tiempo que exista, incluso si deshabilita el acelerador y ya no acepta ni enruta el tráfico. Sin embargo, cuandodeleteun acelerador, pierde las direcciones IP estáticas que se le asignan, por lo que ya no puede enrutar el tráfico usándolas. Puede utilizar directivas de IAM como permisos basados en etiquetas con Global Accelerator para limitar los usuarios que tienen permisos para eliminar un acelerador. Para obtener más información, consulte Políticas basadas en etiquetas.

Acelerador de

Un acelerador dirige el tráfico a los endpoints a través de la red global de AWS para mejorar el rendimiento de sus aplicaciones de Internet. Cada acelerador incluye uno o más oyentes.

Existen dos tipos de aceleradores de:

- Aestándardirige el tráfico al extremo óptimo de AWS en función de varios factores, como la ubicación del usuario, el estado del endpoint y los pesos de los endpoints que configure. De este modo, se mejora la disponibilidad y el rendimiento de las aplicaciones. Los extremos pueden ser equilibradores de carga de red, equilibradores de carga de aplicaciones, instancias de Amazon EC2 o direcciones IP elásticas.
- ARuteo personalizadole permite enrutar de forma determinística varios usuarios a un destino EC2 específico detrás del acelerador, como se requiere en algunos casos de uso. Para ello, dirija a los usuarios a una dirección IP y un puerto únicos en el acelerador, que Global Accelerator ha asignado al destino.

Para obtener más información, consulte Tipos de aceleradores de.

Nombre de DNS

Global Accelerator asigna a cada acelerator un nombre predeterminado del sistema de nombres de dominio (DNS), similar a`a1234567890abcdef.awsglobalaccelerator.com`, que apunta a las direcciones IP estáticas que Global Accelerator le asigna o que usted elija de su propio rango de direcciones IP. Dependiendo del caso de uso, puede usar las direcciones IP estáticas del acelerador o el nombre DNS para enrutar el tráfico al acelerador, o configurar registros DNS para enrutar el tráfico utilizando su propio nombre de dominio personalizado.

Zona de red

Una zona de red proporciona servicios a las direcciones IP estáticas del acelerador desde una subred IP única. Al igual que una zona de disponibilidad de AWS, una zona de red es una unidad

aislada con su propio conjunto de infraestructura física. Al configurar un acelerador, de forma predeterminada, Global Accelerator asigna dos direcciones IPv4 para él. Si una dirección IP de una zona de red deja de estar disponible debido al bloqueo de direcciones IP por determinadas redes cliente o a interrupciones de la red, las aplicaciones cliente pueden volver a intentar la dirección IP estática en buen estado desde la otra zona de red aislada.

Listener

Un listener procesa las conexiones entrantes de los clientes a Global Accelerator, según el puerto (o rango de puertos) y el protocolo (o protocolos) que configure. Se puede configurar un listener para TCP, UDP o ambos protocolos TCP y UDP. Cada listener tiene uno o más grupos de endpoints asociados y el tráfico se reenvía a los endpoints de uno de los grupos. Los grupos de endpoints se asocian a oyentes especificando las regiones a las que desea distribuir el tráfico. Con un acelerador estándar, el tráfico se distribuye a los extremos óptimos dentro de los grupos de endpoints asociados con un listener.

Grupo de puntos de enlace

Cada grupo de puntos de enlace está asociado a una región de AWS específica. Los grupos de endpoints incluyen uno o más extremos en la región. Con un acelerador estándar, puede aumentar o reducir el porcentaje de tráfico que de otro modo se dirigiría a un grupo de endpoints ajustando una configuración denominadamarcado de tráfico. El dial de tráfico le permite realizar fácilmente pruebas de rendimiento o pruebas de implementación azul/verde, por ejemplo, para nuevas versiones en diferentes regiones de AWS.

punto de enlace

Un endpoint es el recurso al que Global Accelerator dirige el tráfico.

Los extremos de los aceleradores estándar pueden ser equilibradores de carga de red, equilibradores de carga de aplicaciones, instancias EC2 o direcciones IP elásticas. Un punto de enlace del balanceador de carga de aplicaciones puede ser interno o orientado a Internet. El tráfico de los aceleradores estándar se enruta a los endpoints en función del estado del endpoint junto con las opciones de configuración que elija, como los pesos de los endpoints. Para cada extremo, puede configurar pesos, que son números que puede usar para especificar la proporción de tráfico que se va a enrutar a cada uno. Esto puede ser útil, por ejemplo, para realizar pruebas de rendimiento dentro de una región.

Los puntos finales para los aceleradores de enrutamiento personalizados son subredes de nube privada virtual (VPC) con una o varias instancias de Amazon EC2 que son los destinos del tráfico.

Cómo funciona AWS Global Accelerator

Las direcciones IP estáticas proporcionadas por el AWS Global Accelerator sirven como puntos de entrada fijos únicos para sus clientes. Cuando configura el acelerador con Global Accelerator, asocia las direcciones IP estáticas a puntos finales regionales en una o más regiones de AWS. Para los aceleradores estándar, los extremos son equilibradores de carga de red, equilibradores de carga de aplicaciones, instancias de Amazon EC2 o direcciones IP elásticas. Para los aceleradores de enrutamiento personalizados, los endpoints son subredes de nube privada virtual (VPC) con una o más instancias EC2. Las direcciones IP estáticas aceptan el tráfico entrante en la red global de AWS desde la ubicación perimetral más cercana a sus usuarios.

> **Note**
>
> Si lleva su propio rango de direcciones IP a AWS (BYOIP) para usarlas en Global Accelerator, puede asignar direcciones IP estáticas de su propio grupo para usarlas en el acelerador. Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en el AWS Global Accelerator.

Desde la ubicación de borde, el tráfico de la aplicación se enruta en función del tipo de acelerador que configure.

- En el caso de los aceleradores estándar, el tráfico se dirige al extremo óptimo de AWS en función de varios factores, como la ubicación del usuario, el estado del endpoint y los pesos de los endpoints que configure.
- En el caso de los aceleradores de enrutamiento personalizados, cada cliente se enruta a una instancia y puerto específicos de Amazon EC2 en una subred de VPC, según la dirección IP estática externa y el puerto de escucha que proporcione.

El tráfico viaja a través de la red global de AWS redundante, bien supervisada y sin congestiones hasta el punto final. Al maximizar el tiempo de tráfico en la red de AWS, Global Accelerator garantiza que el tráfico siempre se enrute a través de la ruta de red óptima.

Con algunos tipos de endpoints (en algunas regiones de AWS), tiene la opción de conservar y acceder a la dirección IP del cliente. Dos tipos de endpoints pueden conservar la dirección IP de origen del cliente en los paquetes entrantes: Equilibradores de carga de aplicaciones e instancias de Amazon EC2. Global Accelerator no admite la preservación de la dirección IP del cliente para los

extremos de Network Load Balancer y direcciones IP elásticas. Los extremos de los aceleradores de enrutamiento personalizados siempre conservan la dirección IP del cliente.

Global Accelerator finaliza las conexiones TCP de clientes en ubicaciones perimetrales de AWS y, casi simultáneamente, establece una nueva conexión TCP con sus endpoints. Esto proporciona a los clientes tiempos de respuesta más rápidos (menor latencia) y mayor rendimiento.

En los aceleradores estándar, Global Accelerator supervisa continuamente el estado de todos los endpoints y comienza instantáneamente a dirigir el tráfico a otro endpoint disponible cuando determina que un endpoint activo no está en buen estado. Esto le permite crear una arquitectura de alta disponibilidad para sus aplicaciones en AWS. Las comprobaciones de Health no se utilizan con aceleradores de enrutamiento personalizados y no hay conmutación por error, porque se especifica el destino al que se va a enrutar el tráfico.

Al agregar un acelerador, los grupos de seguridad y las reglas de AWS WAF que ya ha configurado continúan funcionando como lo hacían antes de agregar el acelerador.

Si desea un control detallado sobre el tráfico global, puede configurar los pesos para sus endpoints en un acelerador estándar. También puede aumentar (marcación hacia arriba) o disminuir (marcación hacia abajo) el porcentaje de tráfico a un grupo de endpoints determinado, por ejemplo, para pruebas de rendimiento o actualizaciones de pila.

Tenga en cuenta lo siguiente cuando utilice Global Accelerator:

- AWS Direct Connect no anuncia prefijos de dirección IP para AWS Global Accelerator a través de una interfaz virtual pública. Le recomendamos que no anuncie las direcciones IP que utilice para comunicarse con el acelerador global a través de su interfaz virtual pública de AWS Direct Connect. Si anuncia direcciones IP que utiliza para comunicarse con Global Accelerator a través de su interfaz virtual pública de AWS Direct Connect, se producirá un flujo de tráfico asimétrico: el tráfico hacia Global Accelerator se dirige a Global Accelerator a través de Internet, pero devuelve el tráfico que llega a su local llega a través de su interfaz virtual pública de AWS Direct Connect.
- Global Accelerator no admite agregar como punto final un recurso que pertenezca a otra cuenta de AWS.

Temas

- Comprobaciones de Health de AWS Global Accelerator

Tiempo de inactividad en AWS Global Accelerator

AWS Global Accelerator establece un periodo de tiempo de espera de inactividad que se aplica a sus conexiones. Si no se han enviado ni recibido datos antes de que haya transcurrido el tiempo de inactividad, Global Accelerator cerrará la conexión. Para garantizar que la conexión permanece activa, el cliente o el endpoint deben enviar al menos 1 byte de datos antes de que transcurra el período de tiempo de espera inactivo.

El tiempo de espera de inactividad del acelerador global para una conexión de red depende del tipo de conexión:

- El tiempo de espera es de 340 segundos para las conexiones TCP.
- El tiempo de espera es de 30 segundos para las conexiones UDP.

Global Accelerator continúa dirigiendo el tráfico a un endpoint hasta que se cumpla el tiempo de espera de inactividad, incluso si el endpoint está marcado como no saludable. Global Accelerator selecciona un nuevo endpoint, si es necesario, sólo cuando se inicia una nueva conexión o después de un tiempo de espera inactivo.

Direcciones IP estáticas en AWS Global Accelerator

Utilice las direcciones IP estáticas que Global Accelerator asigna a su acelerador (o que especifique desde su propio grupo de direcciones IP, para los aceleradores estándar) para enrutar el tráfico de Internet a la red global de AWS cercana a donde se encuentren sus usuarios, independientemente de su ubicación. En el caso de los aceleradores estándar, debe asociar las direcciones con equilibradores de carga de red, equilibradores de carga de aplicaciones, instancias de Amazon EC2 o direcciones IP elásticas que se ejecutan en una sola región de AWS o varias regiones. Para los aceleradores de enrutamiento personalizados, se dirige el tráfico a destinos EC2 en subredes VPC en una o más regiones. El enrutamiento del tráfico a través de la red global de AWS mejora la disponibilidad y el rendimiento, ya que el tráfico no tiene que tomar varios saltos a través de Internet público. El uso de direcciones IP estáticas también le permite distribuir el tráfico entrante de aplicaciones entre varios recursos de endpoints en varias regiones de AWS.

Además, el uso de direcciones IP estáticas facilita la adición de la aplicación a más regiones o la migración de aplicaciones entre regiones. El uso de direcciones IP fijas significa que los usuarios tienen una forma coherente de conectarse a la aplicación a medida que realiza cambios.

Si lo desea, puede asociar su propio nombre de dominio personalizado con las direcciones IP estáticas de su acelerador. Para obtener más información, consulte Enrutar el tráfico de dominio personalizado al acelerador.

Global Accelerator le proporciona las direcciones IP estáticas del grupo de direcciones IP de Amazon, a menos que lleve su propio rango de direcciones IP a AWS y, a continuación, especifique las direcciones IP estáticas de ese grupo. (Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en el AWS Global Accelerator.) Para crear un acelerador en la consola, el primer paso es solicitar a Global Accelerator que aprovisione las direcciones IP estáticas introduciendo un nombre para el acelerador o eligiendo sus propias direcciones IP estáticas. Para ver los pasos para crear un acelerador, consulteIntroducción a AWS Global Accelerator.

Las direcciones IP estáticas permanecen asignadas al acelerador durante el tiempo que exista, incluso si deshabilita el acelerador y ya no acepta ni enruta el tráfico. Sin embargo, cuandodeleteun acelerador, pierde las direcciones IP estáticas que se le asignan, por lo que ya no puede enrutar el tráfico usándolas. Puede utilizar directivas de IAM como permisos basados en etiquetas con Global Accelerator para limitar los usuarios que tienen permisos para eliminar un acelerador. Para obtener más información, consulte Políticas basadas en etiquetas.

Gestión del flujo de tráfico con diales de tráfico y pesos de punto final

Hay dos formas de personalizar la forma en que AWS Global Accelerator envía tráfico a sus terminales con un acelerador estándar:

- Cambiar el marcado de tráfico para limitar el tráfico de uno o más grupos de endpoints
- Especificar pesos para cambiar la proporción de tráfico a los extremos de un grupo

Cómo funcionan las marcas de tráfico

Para cada grupo de endpoints en un acelerador estándar, puede establecer un marcado de tráfico para controlar el porcentaje de tráfico que se envía al grupo de endpoints. El porcentaje se aplica sólo al tráfico que ya está dirigido al grupo de endpoints, no a todo el tráfico de listener.

El marcado de tráfico limita la parte del tráfico que acepta un grupo de endpoints, expresada como un porcentaje del tráfico dirigido a ese grupo de endpoints. Por ejemplo, si establece el marcado de tráfico para un grupo de extremos en`us-east-1`a 50 (es decir, 50%) y el acelerador dirige 100 solicitudes de usuario a ese grupo de puntos finales, solo 50 solicitudes son aceptadas por el grupo. El acelerador dirige las 50 solicitudes restantes a grupos de puntos finales en otras regiones.

Para obtener más información, consulte Ajuste del flujo de tráfico con diales de tráfico.

Cómo funcionan los pesos de

Para cada extremo de un acelerador estándar, puede especificar pesos, que son números que cambian la proporción de tráfico que el acelerador enruta a cada extremo. Esto puede ser útil, por ejemplo, para realizar pruebas de rendimiento dentro de una región.

Un peso es un valor que determina la proporción de tráfico que el acelerador dirige a un extremo. De forma predeterminada, el peso de un extremo es 128, es decir, la mitad del valor máximo de un peso, 255.

El acelerador calcula la suma de los pesos de los endpoints en un grupo de endpoints y, a continuación, dirige el tráfico a los endpoints en función de la relación entre el peso de cada endpoint y el total. Para ver un ejemplo de cómo funcionan los pesos, consulte Ponderaciones de punto de enlace.

Los diales y pesos de tráfico afectan a la forma en que el acelerador estándar sirve al tráfico de diferentes maneras:

- Configurar marcaciones de tráfico paraGrupos de puntos de enlace. El dial de tráfico le permite cortar un porcentaje del tráfico, o todo el tráfico, al «marcar» el tráfico que el acelerador ya le ha dirigido en función de otros factores, como la proximidad.
- Por otro lado, utiliza pesos para establecer valores dePuntos de enlace individualesdentro de un grupo de puntos de enlace. Los pesos proporcionan una forma de dividir el tráfico dentro del grupo de terminales. Por ejemplo, puede usar pesos para realizar pruebas de rendimiento para puntos finales específicos de una región.

> **Note**
>
> Para obtener más información acerca de cómo afectan las marcas y los pesos de tráfico a la conmutación por error, consulteFailover para endpoints en mal estado.

Comprobaciones de Health de AWS Global Accelerator

En el caso de los aceleradores estándar, AWS Global Accelerator comprueba automáticamente el estado de los endpoints asociados con las direcciones IP estáticas y, a continuación, dirige el tráfico del usuario únicamente a los puntos finales en buen estado.

Global Accelerator incluye comprobaciones de estado predeterminadas que se ejecutan automáticamente, pero puede configurar el tiempo para las comprobaciones y otras opciones. Si ha configurado parámetros de comprobación de estado personalizados, Global Accelerator los utiliza de formas específicas, dependiendo de la configuración. Puede configurar esos valores en los extremos de instancia de Acelerador global para Amazon EC2 o direcciones IP elásticas o configurando parámetros en la consola de Elastic Load Balancing para Equilibristas de carga de red o Equilibrios de carga de aplicaciones. Para obtener más información, consulte Opciones de comprobación de estado.

Cuando agrega un extremo a un acelerador estándar, debe pasar una comprobación de estado para que se considere saludable antes de que el tráfico se dirija a él. Si Global Accelerator no tiene endpoints en buen estado para enrutar el tráfico en un acelerador estándar, enruta las solicitudes a todos los endpoints.

Tipos de aceleradores de

Hay dos tipos de aceleradores que puede utilizar con AWS Global Accelerator:Aceleradores estándar deyaceleradores de enrutamiento personalizados. Ambos tipos de aceleradores enrutan el tráfico a través de la red global de AWS para mejorar el rendimiento y la estabilidad, pero cada uno está diseñado para las diferentes necesidades de las aplicaciones.

Acelerador estándar

> Mediante el uso de un acelerador estándar, puede mejorar la disponibilidad y el rendimiento de las aplicaciones que se ejecutan en equilibradores de carga de aplicaciones, equilibradores de carga de red o instancias de Amazon EC2. Con un acelerador estándar, Global Accelerator enruta el tráfico de los clientes a través de los endpoints regionales en función de la geo-proximidad y el estado de los endpoints. También permite a los clientes desplazar el tráfico de los clientes entre los endpoints en función de controles como las marcaciones de tráfico y los pesos de los endpoints. Esto funciona para una amplia variedad de casos de uso, incluyendo implementación azul/verde, pruebas A/B e implementación multi-región. Para ver más casos de uso, consulte Casos de uso de AWS Global Accelerator.

Para obtener más información, consulte Trabajar con aceleradores estándar en el AWS Global Accelerator.

Acelerador de direccionamiento personalizado

Los aceleradores de enrutamiento personalizados funcionan bien para escenarios en los que desea utilizar la lógica de aplicación personalizada para dirigir a uno o más usuarios a un destino y puerto específicos entre muchos, sin dejar de obtener los beneficios de rendimiento de Global Accelerator. Un ejemplo son las aplicaciones VoIP que asignan varias personas que llaman a un servidor multimedia específico para iniciar sesiones de voz, vídeo y mensajería. Otro ejemplo son las aplicaciones de juegos en tiempo real en línea en las que desea asignar varios jugadores a una sola sesión en un servidor de juegos en función de factores como la ubicación geográfica, la habilidad del jugador y el modo de juego.

Para obtener más información, consulte Trabajar con aceleradores de enrutamiento personalizados en AWS Global Accelerator.

En función de sus necesidades específicas, usted crea uno de estos tipos de aceleradores para acelerar el tráfico de sus clientes.

Rangos de ubicación y direcciones IP de servidores de borde de Global Accelerator

Para obtener una lista de ubicaciones de servidores de borde de Global Accelerator, consulte la¿Dónde se implementa AWS Global Accelerator hoy?en la sección Preguntas frecuentes sobre AWS Global Accelerator(Se ha creado el certificado).

AWS publica sus rangos de direcciones IP actuales en formato JSON. Para ver los rangos actuales, descargueip-ranges.json. Para obtener más información, consulte Rangos de direcciones IP de AWS en la Amazon Web Services General Reference.

Para dar con los rangos de direcciones IP asociadas a servidores de borde de AWS Global Accelerator, busque`ip-ranges.json`para la siguiente cadena:

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

Entradas de Global Accelerator que incluyen`"region": "GLOBAL"`se refieren a las direcciones IP estáticas que se asignan a los aceleradores. Si desea filtrar el tráfico a través del acelerador

que proviene de puntos de presencia (POP) en un área, filtre las entradas que incluyan un área geográfica específica, como `us-*` o `eu-*`. Entonces, por ejemplo, si filtra por `us-*`, solo verá el tráfico que llega a través de POP en los Estados Unidos (EE. UU.).

Casos de uso de AWS Global Accelerator

El uso de AWS Global Accelerator puede ayudarle a lograr diferentes objetivos. En esta sección se enumeran algunos de ellos, para darle una idea de cómo puede usar Global Accelerator para satisfacer sus necesidades.

Escale para aumentar la utilización de aplicaciones

Cuando aumenta el uso de aplicaciones, también aumenta el número de direcciones IP y endpoints que necesita administrar. Global Accelerator le permite escalar su red hacia arriba o hacia abajo. Permite asociar recursos regionales, como equilibradores de carga e instancias de Amazon EC2, a dos direcciones IP estáticas. Estas direcciones se incluyen en listas de permisos sólo una vez en las aplicaciones cliente, los firewalls y los registros DNS. Con Global Accelerator, puede agregar o eliminar puntos finales en las regiones de AWS, ejecutar una implementación azul/verde y realizar pruebas A/B sin tener que actualizar las direcciones IP de sus aplicaciones cliente. Esto es especialmente útil para casos de uso de IoT, minoristas, medios de comunicación, automoción y atención médica en los que no puede actualizar fácilmente las aplicaciones cliente con frecuencia.

Aceleración para aplicaciones sensibles a la latencia

Muchas aplicaciones, especialmente en áreas como juegos, medios, aplicaciones móviles y finanzas, requieren una latencia muy baja para una gran experiencia de usuario. Para mejorar la experiencia del usuario, Global Accelerator dirige el tráfico del usuario al extremo de la aplicación más cercano al cliente, lo que reduce la latencia y la fluctuación de Internet. Global Accelerator enruta el tráfico a la ubicación de borde más cercana mediante Anycast y, a continuación, lo dirige al extremo regional más cercano a través de la red global de AWS. Global Accelerator reacciona rápidamente a los cambios en el rendimiento de la red para mejorar el rendimiento de las aplicaciones de los usuarios.

Recuperación ante desastres y resiliencia multiregional

Para poder confiar en su red, debe estar disponible. Es posible que esté ejecutando su aplicación en varias regiones de AWS para respaldar la recuperación ante desastres, mayor disponibilidad, menor latencia o cumplimiento normativo. Si Global Accelerator detecta que el punto final de su aplicación está fallando en la región principal de AWS, desencadena al instante el reenrutamiento

del tráfico hacia el punto final de la aplicación en la siguiente región de AWS disponible y más cercana.

Proteja sus aplicaciones

Exponer sus orígenes de AWS, como los equilibradores de carga de aplicaciones o las instancias de Amazon EC2, al tráfico público de Internet crea una oportunidad para ataques maliciosos. Global Accelerator reduce el riesgo de ataque al enmascarar su origen detrás de dos puntos de entrada estáticos. Estos puntos de entrada están protegidos de forma predeterminada contra ataques de denegación distribuida del servicio (DDoS) con AWS Shield. Global Accelerator crea una conexión de emparejamiento con su Amazon Virtual Private Cloud mediante direcciones IP privadas, manteniendo las conexiones a sus equilibradores de carga de aplicaciones internos o instancias privadas de EC2 fuera de Internet pública.

Mejorar el rendimiento para aplicaciones de VoIP o juegos en línea

Con un acelerador de enrutamiento personalizado, puede aprovechar las ventajas de rendimiento de Global Accelerator para sus aplicaciones de VoIP o de juegos. Por ejemplo, puede usar Global Accelerator para aplicaciones de juegos en línea que asignen varios jugadores a una sola sesión de juego. Utilice Global Accelerator para reducir la latencia y la fluctuación globalmente en aplicaciones que requieren lógica personalizada para asignar usuarios a puntos finales específicos, como juegos multijugador o llamadas VoIP. Puede utilizar un solo acelerador para conectar clientes a miles de instancias de Amazon EC2 que se ejecutan en una o varias regiones de AWS, al tiempo que mantiene el control total sobre qué cliente se dirige a qué instancia y puerto de EC2.

Herramienta de comparación de velocidad de AWS Global Accelerator

Puede utilizar la herramienta de comparación de velocidad del AWS Global Accelerator para ver las velocidades de descarga del acelerador global en comparación con las descargas directas de Internet en todas las regiones de AWS. Esta herramienta le permite utilizar su navegador para ver la diferencia de rendimiento al transferir datos mediante Global Accelerator. Usted elige un tamaño de archivo para descargar y la herramienta descarga archivos a través de HTTPS/TCP desde Equilibradores de carga de aplicaciones en diferentes regiones a su navegador. Para cada región, verá una comparación directa de las velocidades de descarga.

Para acceder a la herramienta de comparación de velocidad, copie la siguiente URL en su navegador:

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

> **Important**
>
> Los resultados pueden diferir cuando se ejecuta la prueba varias veces. Los tiempos de descarga pueden variar en función de factores externos a Global Accelerator, como la calidad, la capacidad y la distancia de la conexión en la red de última milla que esté utilizando.

Primeros pasos con AWS Global Accelerator

Puede comenzar a configurar AWS Global Accelerator utilizando la API o la consola de AWS Global Accelerator. Dado que el acelerador global es un servicio global, no está vinculado a una región específica de AWS. Tenga en cuenta que Global Accelerator es un servicio global que admite puntos finales en varias regiones de AWS, pero debe especificar la región EE.UU. Oeste (Oregón) para crear o actualizar aceleradores.

Para empezar a utilizar Global Accelerator, siga estos pasos generales:

1. Elija el tipo de acelerador que desea crear: Un acelerador de direccionamiento estándar o un acelerador de direccionamiento personalizado.
2. Configure la configuración inicial de Global Accelerator: Proporcione un nombre para el acelerador de. A continuación, configure uno o más oyentes para procesar las conexiones entrantes de los clientes, según el protocolo y el puerto (o rango de puertos) que especifique.
3. Configure grupos de endpoints regionales para su acelerador: Puede seleccionar uno o varios grupos de puntos de enlace regionales para añadirlos al agente de escucha. El listener enruta las solicitudes a los endpoints que ha agregado a un grupo de endpoints.

   Para un acelerador estándar, Global Accelerator supervisa el estado de los endpoints dentro del grupo mediante la configuración de comprobación de estado definida para cada uno de los endpoints. Para cada grupo de endpoints en un acelerador estándar, puede configurar unmarcado de tráficopara controlar el porcentaje de tráfico que un grupo de terminales aceptará. El porcentaje se aplica sólo al tráfico que ya está dirigido al grupo de endpoints, no a todo el tráfico de listener. De forma predeterminada, el marcado de tráfico se establece en 100% para todos los grupos de extremos regionales.

Para los aceleradores de enrutamiento personalizados, el tráfico se enruta determinísticamente a un destino específico en una subred VPC, en función del puerto de escucha en el que se recibe el tráfico.

4. Agregar puntos finales a grupos de extremos: Los puntos de enlace que agregue dependen del tipo de acelerador de.
   - Para un acelerador estándar, puede agregar uno o más recursos regionales, como equilibradores de carga o extremos de instancias EC2, a cada grupo de extremos. A continuación, puede decidir cuánto tráfico desea enrutar a cada extremo estableciendo los pesos de los endpoints.
   - Para un acelerador de enrutamiento personalizado, puede agregar una o más subredes de nube privada virtual (VPC) con hasta miles de destinos de instancias de Amazon EC2.

Para obtener pasos detallados sobre cómo crear un acelerador estándar o un acelerador de enrutamiento personalizado mediante la consola de AWS Global Accelerator, consulteIntroducción a AWS Global Accelerator. Para trabajar con operaciones de API, consulteAcciones comunes que puede utilizar con AWS Global Acceleratory laReferencia de la API Global Accelerator.

Etiquetado en AWS Global Accelerator

Las etiquetas son palabras o frases (metadatos) que se utilizan para identificar y organizar sus recursos de AWS. Puede añadir varias etiquetas a cada recurso, y cada etiqueta incluye una clave y un valor que usted define. Por ejemplo, la clave puede ser`environmenty` el valor podría ser`production`. Puede buscar y filtrar sus recursos en función de las etiquetas que añada. En AWS Global Accelerator, puede etiquetar aceleradores.

A continuación se muestran dos ejemplos de cómo puede resultar útil trabajar con etiquetas en Global Accelerator:

- Utilizar etiquetas para realizar un seguimiento de la información de facturación en diferentes categorías. Para ello, aplique etiquetas a aceleradores u otros recursos de AWS (como Equilibradores de carga de red, Equilibradores de carga de aplicaciones o instancias de Amazon EC2) y active las etiquetas. A continuación, AWS genera un informe de asignación de costos como un valor separado por comas (archivo CSV) con el total del uso y los costos por etiqueta activa. Puede aplicar etiquetas que representen categorías de negocio (por ejemplo, centros de costos, nombres de aplicación o propietarios) para estructurar los costos entre diferentes servicios.

Para obtener más información, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de administración de costos y facturación de AWS.

- Utilizar etiquetas para aplicar permisos basados en etiquetas a los aceleradores. Para ello, cree directivas de IAM que especifiquen etiquetas y valores de etiqueta para permitir o rechazar acciones. Para obtener más información, consulte Políticas basadas en etiquetas.

Para conocer las convenciones de uso y los vínculos a otros recursos sobre el etiquetado, consulteEtiquetado de recursos de AWSen laReferencia general de AWS. Para obtener sugerencias sobre el uso de etiquetas, consultePrácticas recomendadas de etiquetado: Estrategia de etiquetado de recursos de AWSen laDocumentos técnicos de AWSBlog.

Para obtener el máximo de la cantidad de etiquetas que puede agregar a un recurso en Global Accelerator, consulteCuotas para AWS Global Accelerator.

Puede añadir y actualizar etiquetas utilizando la consola de AWS, la CLI de AWS o la API de Global Accelerator. Este capítulo incluye pasos para trabajar con el etiquetado en la consola. Para obtener más información sobre cómo trabajar con etiquetas mediante la CLI de AWS y la API de acelerador global, incluidos ejemplos de CLI, consulte las siguientes operaciones en la secciónReferencia de la API de AWS Global Accelerator:

- CreateAccelerator
- TagResource
- UntagResource
- ListTagsForResource

Compatibilidad con etiquetado en Global Accelerator

AWS Global Accelerator admite el etiquetado de aceleradores.

Global Accelerator (IAM) es compatible con la función de control de acceso basado en etiquetas de AWS Identity and Access Management). Para obtener más información, consulte Políticas basadas en etiquetas.

Agregar, editar y eliminar etiquetas en Global Accelerator

En el siguiente procedimiento se explica cómo añadir, editar y eliminar etiquetas para aceleradores en la consola de Global Accelerator.

> **Note**
>
> Puede añadir o eliminar etiquetas con la consola, la CLI de AWS o las operaciones de la API de Global Accelerator. Para obtener más información, incluidos ejemplos de CLI, consulteTagResourceen laReferencia de la API de AWS Global Accelerator.

Para añadir, editar o eliminar etiquetas en Global Accelerator

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. Elija el acelerador para el que desea añadir o actualizar etiquetas.
3. En el navegadorTags (Etiquetas):Puede hacer lo siguiente:

   Añada una etiqueta

   SeleccionarAgregue etiquetaEscriba una clave y, opcionalmente, un valor para la etiqueta.

   Editar una etiqueta

   Actualizar el texto de una clave, un valor o ambos. También puede borrar el valor de una etiqueta, pero la clave es necesaria.

   Eliminar una etiqueta

   SeleccionarRemoveEn la parte derecha del campo de valor.
4. Elija Save changes.

Precios para AWS Global Accelerator

Con AWS Global Accelerator, paga únicamente por lo que utiliza. Se le cobrará una tarifa por hora y los costos de transferencia de datos por cada acelerador de su cuenta. Para obtener más información, consultePrecios de AWS Global Accelerator.

Introducción a AWS Global Accelerator

Estos tutoriales proporcionan los pasos necesarios para comenzar a utilizar AWS Global Accelerator mediante la consola. También puede utilizar las operaciones de la API de AWS Global Accelerator para crear y personalizar sus aceleradores. En cada paso de este tutorial, hay un enlace a la operación API correspondiente para completar la tarea mediante programación. (Cuando configure un acelerador de enrutamiento personalizado, debe usar la API para ciertos pasos de configuración.) Para obtener más información sobre las operaciones de AWS Global AcceleratorReferencia de AWS Global Accelerator.

> **Tip**
>
> Para explorar cómo puede usar Global Accelerator para mejorar el rendimiento y la disponibilidad de las aplicaciones web, consulte el siguiente taller autoguiado: Taller de AWS Global Accelerator.

Global Accelerator es un servicio global que admite puntos finales en varias regiones de AWS, que se enumeran en elTabla de regiones de AWS.

Este capítulo incluye dos tutoriales: uno para crear un acelerador estándar y otro para crear un acelerador de enrutamiento personalizado. Para obtener más información sobre los dos tipos de aceleradores de, consulteTrabajar con aceleradores estándar en el AWS Global AcceleratoryTrabajar con aceleradores de enrutamiento personalizados en AWS Global Accelerator.

Temas

- Introducción a un acelerador de
- Introducción a un acelerador de direccionamiento personalizado

Introducción a un acelerador de

En esta sección, se proporcionan los pasos para crear un acelerador de direccionamiento del tráfico a un punto de enlace óptimo.

Tareas

- Antes de empezar

- Paso 1: Crear un acelerador
- Paso 2: Añadir agentes de escucha
- Paso 3: Añadir grupos de puntos de enlace
- Paso 4: Agregar puntos finales
- Paso 5: Pruebe su acelerador
- Paso 6 (opcional): Eliminar el acelerador

Antes de empezar

Antes de crear un acelerador, cree al menos un recurso al que puede agregar como punto final para dirigir el tráfico. Por ejemplo, cree una de las opciones siguientes:

- Inicie al menos una instancia de Amazon EC2 para añadirla como punto final. Para obtener más información, consulteCree sus recursos EC2 e inicie su instancia EC2en laGuía del usuario de Amazon EC2 para instancias de Linux.
- Opcionalmente, cree uno o más equilibradores de carga de red o equilibradores de carga de aplicaciones que incluyan instancias de EC2. Para obtener más información, consulteCreación de un Network Load Balancer de Application Load Balanceren laGuía del usuario para Network Load Balancers.

Cuando cree un recurso para agregar al Global Accelerator (Global Accelerator), tenga en cuenta lo siguiente:

- Cuando se agrega un Application Load Balancer interno o un extremo de instancia EC2 en Global Accelerator, se habilita el tráfico de Internet para que fluya directamente hacia y desde el extremo en las nubes privadas virtuales (VPC) segmentándolo en una subred privada. La VPC que contiene el balanceador de carga o la instancia EC2 debe tener ungateway de Internetadjunta a él, para indicar que la VPC acepta tráfico de Internet. Para obtener más información, consulte Conexiones VPC seguras en AWS Global Accelerator.
- Global Accelerator requiere que las reglas de enrutador y firewall permitan el tráfico entrante de las direcciones IP asociadas con los comprobadores de estado de Route 53 para completar las comprobaciones de estado de los endpoints de instancias EC2 o direcciones IP elásticas. Puede encontrar información sobre los rangos de direcciones IP asociados a los comprobadores de estado de Amazon Route 53 enComprobaciones de estado de los grupos de destinoen laAmazon Route 53 Developer.

Paso 1: Crear un acelerador

Para crear el acelerador, introduzca un nombre.

> **Note**
>
> Para completar esta tarea mediante una operación de API en lugar de la consola de, consulteCreateAcceleratoren laReferencia de AWS Global Accelerator.

Para crear un acelerador

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. SeleccionarCrear un acelerador.
3. Proporcione un nombre para el acelerador de.
4. Si lo desea, añada una o varias etiquetas para ayudarle a identificar los recursos de Global Accelerator.
5. Seleccione Siguiente.

Paso 2: Añadir agentes de escucha

Cree un agente de escucha para procesar conexiones entrantes de los usuarios a Global Accelerator

> **Note**
>
> Para completar esta tarea mediante una operación de API en lugar de la consola de, consulteCreateListeneren laReferencia de AWS Global Accelerator.

Para crear un agente de escucha

1. En la páginaAñadir agente de escucha, introduzca los puertos o rangos de puertos que desea asociar al agente de escucha. Los oyentes admiten puertos 1-65535.
2. Elija el protocolo o protocolos para los puertos que ha introducido.
3. Opcionalmente, elija habilitar la afinidad del cliente. La afinidad del cliente por un agente de escucha significa que Global Accelerator garantiza que las conexiones de una dirección IP

de origen (cliente) específica se enrutan siempre al mismo punto final. Para habilitar este comportamiento, en la lista desplegable, seleccioneIP de origen.

El valor predeterminado esNone (Ninguno), lo que significa que la afinidad del cliente no está habilitada y Global Accelerator distribuye el tráfico equitativamente entre los endpoints de los grupos de endpoints para el listener.

Para obtener más información, consulte Afinidad del cliente.

4. También puede seleccionarAñadir agente de escuchapara agregar un agente de escucha adicional.
5. Cuando haya acabado de añadir agentes de escucha, seleccioneSiguiente.

Paso 3: Añadir grupos de puntos de enlace

Agregue uno o más grupos de endpoints, cada uno de los cuales está asociado a una región específica de AWS.

> **Note**
>
> Para completar esta tarea mediante una operación de API en lugar de la consola de, consulteCreateEndPointGroupen laReferencia de AWS Global Accelerator.

Para añadir un punto de enlace

1. En la páginaAñadir grupos de puntos de enlace, en la sección correspondiente a un oyente, elija unaRegiónEn la lista desplegable.
2. También puede seleccionarDial de tráfico, escriba un número de 0 a 100 para establecer un porcentaje de tráfico para este grupo de endpoints. El porcentaje se aplica sólo al tráfico ya dirigido a este grupo de puntos finales, no a todo el tráfico de listener. De forma predeterminada, el marcado de tráfico para un grupo de extremos se establece en 100 (es decir, 100%).
3. Si lo desea, para valores de comprobación de estado personalizados, elijaConfigurar comprobaciones de estado. Cuando se configuran las opciones de comprobación de estado, Global Accelerator utiliza las opciones para las comprobaciones de estado de los endpoints de direcciones IP elásticas y de instancia de EC2. Para los extremos del equilibrador de carga de red y del equilibrador de carga de aplicaciones, Global Accelerator utiliza la configuración de

comprobación de estado que ya ha configurado para los propios equilibradores de carga. Para obtener más información, consulte Opciones de comprobación de estado.

4. También puede seleccionarAñadir un punto de enlacePara agregar grupos de puntos de enlace adicionales para este agente de escucha u otros agentes de escucha.
5. Seleccione Siguiente.

Paso 4: Agregar puntos finales

Agregue uno o más extremos asociados a grupos de extremos específicos. Este paso no es necesario, pero no se dirige tráfico a los endpoints de una región a menos que los endpoints se incluyan en un grupo de endpoints.

> **Note**
>
> Si va a crear el acelerador mediante programación, puede agregar puntos finales como parte de la adición de grupos de extremos. Para obtener más información, consulteCreateEndPointGroupen laReferencia de AWS Global Accelerator.

Para añadir puntos de enlace

1. En la páginaCreación de puntos de enlace, en la sección de un endpoint, elija unaPunto de enlace.
2. También puede seleccionarPeso, introduzca un número de 0 a 255 para establecer un peso para enrutar el tráfico a este extremo. Cuando agrega ponderaciones a los puntos de enlace, configura Global Accelerator para que enrute el tráfico en función de las proporciones que especifique. De forma predeterminada, todos los puntos finales tienen un peso de 128. Para obtener más información, consulte Ponderaciones de punto de enlace.
3. Si lo desea, para un punto de enlace del Application Load Balancer, enPreserve la dirección IP de clienteEn, seleccionePreserve la dirección. Para obtener más información, consulte Conservar las direcciones IP del cliente en el AWS Global Accelerator.
4. También puede seleccionarAñadir punto de enlacepara agregar más puntos finales.
5. Seleccione Siguiente.

Después de elegirSiguiente, en el panel de control del acelerador global verás un mensaje que indica que el acelerador está en curso. Una vez terminado el proceso, el estado del acelerador en el tablero de mandos esActiva.

Paso 5: Pruebe su acelerador

Siga los pasos necesarios para probar el acelerador y asegurarse de que el tráfico se dirige a sus endpoints. Por ejemplo, ejecute un comando curl como el siguiente, sustituyendo una de las direcciones IP estáticas del acelerador, para mostrar las regiones de AWS donde se procesan las solicitudes. Esto resulta especialmente útil si establece diferentes pesos para los puntos finales o ajusta el marcado de tráfico en los grupos de extremos.

Ejecute un comando curl como el siguiente, sustituyendo una de las direcciones IP estáticas del acelerador, para llamar a la dirección IP 100 veces y luego generar un recuento de donde se procesó cada solicitud.

```
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;
```

Si ha ajustado el marcado de tráfico en cualquier grupo de endpoints, este comando puede ayudarle a confirmar que el acelerador está dirigiendo los porcentajes correctos de tráfico a diferentes grupos. Para obtener más información, consulte los ejemplos detallados en la siguiente entrada de blog,Administración del tráfico con AWS Global Accelerator.

Paso 6 (opcional): Eliminar el acelerador

Si ha creado un acelerador como prueba o si ya no utiliza un acelerador, puede eliminarlo. En la consola, deshabilite el acelerador y luego puede eliminarlo. No es necesario eliminar los oyentes y los grupos de puntos finales del acelerador.

Para eliminar un acelerador mediante una operación de API en lugar de la consola, primero debe eliminar todos los listeners y grupos de endpoints asociados al acelerador, así como deshabilitarlo. Para obtener más información, consulte laDeleteAccelerator operation in the Referencia de AWS Global Accelerator.

Tenga en cuenta lo siguiente al quitar puntos finales o grupos de extremos, o al eliminar un acelerador:

- Al crear un acelerador, Global Accelerator le proporciona un conjunto de dos direcciones IP estáticas. Las direcciones IP se asignan al acelerador durante el tiempo que exista, incluso

si deshabilita el acelerador y ya no acepta ni enruta el tráfico. Sin embargo, cuandodeleteun acelerador, pierde las direcciones IP estáticas asignadas al acelerador, por lo que ya no puede enrutar el tráfico usándolas. Como práctica recomendada, asegúrese de que dispone de permisos para evitar eliminar aceleradores inadvertidamente. Puede utilizar directivas de IAM con Global Accelerator, por ejemplo, permisos basados en etiquetas, para limitar los usuarios que tienen permisos para eliminar un acelerador. Para obtener más información, consulte Políticas basadas en etiquetas.

- Si finaliza una instancia de EC2 antes de quitarla de un grupo de endpoints en Global Accelerator y, a continuación, crea otra instancia con la misma dirección IP privada y pasan las comprobaciones de estado, Global Accelerator enrutará el tráfico al nuevo endpoint. Si no desea que esto suceda, elimine la instancia de EC2 del grupo de extremos antes de finalizar la instancia.

Para suprimir un acelerador

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. Elija el acelerador que desea eliminar.
3. Elija Edit (Editar).
4. SeleccionarDesactivar el aceleradorHaga clic en y luego enSave (Guardar).
5. Elija el acelerador que desea eliminar.
6. SeleccionarEliminar acelerador.
7. En el cuadro de diálogo de confirmación, elija Delete (Eliminar).

Introducción a un acelerador de direccionamiento personalizado

En esta sección se proporcionan los pasos para crear un acelerador de direccionamiento personalizado que enrute el tráfico de manera determinante a los destinos de instancia de Amazon EC2 en los puntos de enlace de subred de nube virtual privada (VPC).

Tareas

- Antes de empezar
- Paso 1: Creación de un acelerador de direccionamiento personalizado
- Paso 2: Añadir agentes de escucha
- Paso 3: Añadir grupos de puntos de enlace
- Paso 4: Agregar puntos finales

- Paso 5 (opcional): Eliminar el acelerador

Antes de empezar

Antes de crear un acelerador de enrutamiento personalizado, cree un recurso que puede agregar como punto final al que dirigir el tráfico. Un punto de enlace del acelerador de direccionamiento personalizado debe ser una subred de nube virtual privada (VPC), que puede incluir varias instancias de Amazon EC2. Para obtener instrucciones sobre la creación de los recursos, consulte lo siguiente:

- Crear una subred VPC. Para obtener más información, consulteCreación y configuración de la VPCen laGuía de administración de AWS Directory Service.
- Si lo desea, inicie una o varias instancias Amazon EC2 en su VPC. Para obtener más información, consulteCree sus recursos EC2 e inicie su instancia EC2en laGuía del usuario de Amazon EC2 para instancias de Linux.

Cuando cree un recurso para agregar al Global Accelerator (Global Accelerator), tenga en cuenta lo siguiente:

- Cuando agrega un extremo de instancia EC2 en Global Accelerator, habilita el tráfico de Internet para que fluya directamente hacia y desde el extremo de las VPC segmentándolo en una subred privada. La VPC que contiene la instancia EC2 debe tener ungateway de Internetadjunta a él, para indicar que la VPC acepta tráfico de Internet. Para obtener más información, consulte Conexiones VPC seguras en AWS Global Accelerator.

Paso 1: Creación de un acelerador de direccionamiento personalizado

> **Note**
>
> Para completar esta tarea mediante una operación de API en lugar de la consola de, consulteCreateCustomRoutingAcceleratoren laReferencia de AWS Global Accelerator.

Para crear un acelerador

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. Proporcione un nombre para el acelerador de.

3. ParaTipo de aceleradorEn, seleccioneEnrutamiento personalizado.
4. Si lo desea, añada una o varias etiquetas para ayudarle a identificar los recursos del acelerador.
5. SeleccionarSiguientepara agregar listeners, grupos de endpoints y endpoints de subred VPC.

Paso 2: Añadir agentes de escucha

Cree un agente de escucha para procesar conexiones entrantes de los usuarios a Global Accelerator

El rango que especifica al crear un listener define cuántas combinaciones de puertos de escucha y direcciones IP de destino se pueden utilizar con el acelerador de enrutamiento personalizado. Para obtener una flexibilidad máxima, le recomendamos que especifique un rango de puertos grande. Cada rango de puertos de escucha que especifique debe incluir un mínimo de 16 puertos.

> **Note**
>
> Para completar esta tarea mediante una operación de API en lugar de la consola de, consulteCreateCustomRoutingListeneren laReferencia de AWS Global Accelerator.

Para crear un agente de escucha

1. En la páginaAñadir agente de escucha, introduzca los puertos o rangos de puertos que desea asociar al agente de escucha. Los oyentes admiten los puertos 1-65535.
2. Elija el protocolo o protocolos para los puertos que ha introducido.
3. También puede seleccionarAñadir agente de escuchapara agregar un agente de escucha adicional.
4. Cuando haya acabado de añadir agentes de escucha, seleccioneSiguiente.

Paso 3: Añadir grupos de puntos de enlace

Agregue uno o más grupos de endpoints, cada uno de los cuales está asociado a una región específica de AWS. Para cada grupo de extremos, especifique uno o más conjuntos de rangos de puertos y protocolos. Global Accelerator las utiliza para dirigir el tráfico a instancias de Amazon EC2 en subredes de la región.

Para cada rango de puertos que proporcione, también especifique el protocolo que se va a utilizar: UDP, TCP o UDP y TCP.

> **Note**
>
> Para completar esta tarea mediante una operación de API en lugar de la consola de, consulteCreateCustomRoutingEndPointGroupen laReferencia de AWS Global Accelerator.

Para añadir un punto de enlace

1. En la páginaAñadir grupos de puntos de enlace, en la sección correspondiente a un oyente, elija unaRegión.
2. ParaConjuntos de puertos y protocolos, introduzca rangos de puertos y protocolos para sus instancias de Amazon EC2.

   - Introduzca unDesde el puertoy aAl puertoPara especificar un intervalo de puertos.
   - Para cada intervalo de puertos, especifique el protocolo o protocolos para ese rango.

   El rango de puertos no tiene que ser un subconjunto del rango de puertos de escucha, pero debe haber suficientes puertos totales en el rango de puertos del listener para admitir el número total de puertos que especifique.
3. Elija Save (Guardar).
4. También puede seleccionarAñadir un punto de enlacePara agregar grupos de puntos de enlace adicionales para este agente de escucha u otros agentes de escucha.
5. Seleccione Siguiente.

Paso 4: Agregar puntos finales de subred de VPC

Agregue uno o varios puntos de enlace de subred de nube virtual privada (VPC) para este grupo de puntos de enlace regional. Los puntos finales para aceleradores de enrutamiento personalizados definen las subredes de VPC que pueden recibir tráfico a través de un acelerador de enrutamiento personalizado. Cada subred puede contener uno o varios destinos de instancias de Amazon EC2.

Al agregar un extremo de subred de VPC, Global Accelerator genera nuevas asignaciones de puertos que puede utilizar para enrutar el tráfico a las direcciones IP de la instancia EC2 de destino en la subred. A continuación, puede utilizar la API Global Accelerator para obtener una lista estática de todas las asignaciones de puertos para la subred y utilizar la asignación para dirigir de forma determinística el tráfico a instancias EC2 específicas.

> **Note**
>
> Los pasos que se indican a continuación muestran cómo agregar puntos finales en la consola. Si está creando el acelerador mediante programación, agregará puntos finales con grupos de extremos. Para obtener más información, consulteCreateCustomRoutingEndPointGroupen laReferencia de AWS Global Accelerator.

Para añadir puntos de enlace

1. En la páginaAgregar puntos finales, en la sección del grupo de extremos al que desea agregar el extremo, elija un ID de subred paraPunto de enlace.
2. Si lo desea, realice una de las acciones siguientes para habilitar el tráfico a destinos de instancia de EC2 en la subred:

   - Para permitir que el tráfico se dirija a todos los extremos y puertos EC2 de la subred, seleccionePermitir todo el tráfico
   - Para permitir el tráfico a puntos finales y puertos específicos de EC2 en la subred, seleccionePermitir tráfico a direcciones de socket de destino específicas. A continuación, especifique las direcciones IP y los puertos o rangos de puertos que se van a permitir. Por último, seleccionePermitir estos destinos.

   De forma predeterminada, no se permite tráfico a los extremos de la subred. Si no selecciona una opción para permitir el tráfico, el tráfico se deniega a todos los destinos de la subred.

   > **Note**
   >
   > Si desea habilitar el tráfico a instancias y puertos de EC2 específicos de la subred, puede hacerlo mediante programación. Para obtener más información, consultePermitir CustomRoutingTrafficen laReferencia de AWS Global Accelerator.

3. Seleccione Siguiente.

Después de elegirSiguiente, en el panel Acelerador global, verá un mensaje en el que se indica que el acelerador está en curso. Una vez terminado el proceso, el estado del acelerador en el tablero de mandos esActiva.

Paso 5 (opcional): Eliminar el acelerador

Si ha creado un acelerador como prueba o si ya no utiliza un acelerador, puede eliminarlo. En la consola, deshabilite el acelerador y luego puede eliminarlo. No es necesario eliminar los oyentes y los grupos de puntos finales del acelerador.

Para eliminar un acelerador mediante una operación de API en lugar de la consola, primero debe eliminar todos los listeners y grupos de endpoints asociados al acelerador, así como deshabilitarlo. Para obtener más información, consulte laDeleteCustomRoutingAccelerator operation in the Referencia de AWS Global Accelerator.

Tenga en cuenta lo siguiente al eliminar un acelerador de:

- Al crear un acelerador, Global Accelerator le proporciona un conjunto de dos direcciones IP estáticas. Las direcciones IP se asignan al acelerador durante el tiempo que exista, incluso si deshabilita el acelerador y ya no acepta ni enruta el tráfico. Sin embargo, cuandodeleteun acelerador, pierde las direcciones IP estáticas asignadas al acelerador, por lo que ya no puede enrutar el tráfico usándolas. Como práctica recomendada, asegúrese de que dispone de permisos para evitar eliminar aceleradores inadvertidamente. Puede utilizar directivas de IAM como permisos basados en etiquetas con Global Accelerator para limitar los usuarios que tienen permisos para eliminar un acelerador. Para obtener más información, consulte Políticas basadas en etiquetas.

Para suprimir un acelerador

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. Elija el acelerador que desea eliminar.
3. Elija Edit (Editar).
4. SeleccionarDesactivar el aceleradorHaga clic en y luego enSave (Guardar).
5. Elija el acelerador que desea eliminar.
6. SeleccionarEliminar acelerador.
7. En el cuadro de diálogo de confirmación, elija Delete (Eliminar).

Acciones comunes que puede utilizar con AWS Global Accelerator

En esta sección se enumeran las acciones comunes del AWS Global Accelerator que puede utilizar con los recursos del Acelerador global, con vínculos a la documentación relevante.

Acciones que se deben utilizar con recursos estándar

En la siguiente tabla se enumeran las acciones comunes del Acelerador Global que se pueden utilizar con los aceleradores estándar de Global Accelerator, con vínculos a la documentación relevante.

Acción	Uso de la Consola Global Accelerator	Uso de la API de Global Accelerator
Crear un acelerador estándar	Consulte Introducción a un acelerador de	Consulte CreateAccelerator
Creación de un agente de escucha para un acelerador estándar	Consulte Listeners para aceleradores estándar en el AWS Global Accelerator	Consulte CreateListener
Crear un grupo de extremos para un acelerador estándar	Consulte Grupos de endpoints para aceleradores estándar en AWS Global Accelerator	Consulte CreateEndpointGroup
Actualizar un acelerador estándar	Consulte AWS Global Accelerator	Consulte UpdateAccelerator
Enumera tus aceleradores	Consulte Visualización de los aceleradores	Consulte ListAccelerator
Obtener toda la información de un acelerador	Consulte Visualización de los aceleradores	Consulte DescribeAccelerator
Eliminar un acelerador	Consulte Creación o actualización de un acelerador estándar	Consulte DeleteAccelerator

Acciones que se deben utilizar con recursos de enrutamiento personalizados

En la tabla siguiente se enumeran las acciones comunes del acelerador global que se pueden utilizar con aceleradores de enrutamiento personalizados, con vínculos a la documentación relevante.

Acción	Uso de la Consola Global Accelerator	Uso de la API de Global Accelerator
Creación de un acelerador de direccionamiento personalizado	Consulte Introducción a un acelerador de direccionamiento personalizado	Consulte CreateCustomRoutingAccelerator
Creación de un agente de escucha para un acelerador de direccionamiento personalizado	Consulte Listeners para aceleradores de enrutamiento personalizados en el AWS Global Accelerator	Consulte CreateCustomRoutingListener
Creación de un grupo de puntos de enlace para un acelerador de direccionamiento personalizado	Consulte Grupos de endpoints para aceleradores de enrutamiento personalizados en AWS Global Accelerator	Consulte CreateCustomRoutingEndpointGroup
Actualizar un acelerador de enrutamiento personalizado	Consulte Aceleradores de enrutamiento personalizados en el AWS Global Accelerator	Consulte UpdateCustomRoutingAccelerator
Enumere sus aceleradores de enrutamiento personalizados	Consulte Visualización de los aceleradores de enrutamiento personalizados	Consulte ListCustomRoutingAccelerator
Obtener toda la información de un acelerador de direccionamiento personalizado	Consulte Visualización de los aceleradores de enrutamiento personalizados	Consulte DescribeCustomRoutingAccelerator
Eliminar un acelerador de enrutamiento personalizado	Consulte Creación o actualización de un acelerador de direccionamiento personalizado	Consulte DeleteCustomRoutingAccelerator

Acción	Uso de la Consola Global Accelerator	Uso de la API de Global Accelerator
Obtener la asignación de puertos estáticos de un acelerador de direccion amiento personalizado	N/D	Consulte ListCustomRoutingPortMappings
Permitir todo el tráfico de destino para una subred en un acelerador de enrutamiento personalizado	Consulte Agregar, editar o quitar un extremo de subred VPC	Consulte AllowCustomRoutingTraffic
Denegar todo el tráfico de destino para una subred en un acelerador de enrutamiento personalizado	Consulte Agregar, editar o quitar un extremo de subred VPC	Consulte DenyCustomRoutingTraffic
Permitir tráfico a destinos específicos en un acelerador de enrutamiento personalizado	Consulte Agregar, editar o quitar un extremo de subred VPC	Consulte AllowCustomRoutingTraffic
Denegar tráfico a destinos específicos en un acelerador de enrutamiento personalizado	Consulte Agregar, editar o quitar un extremo de subred VPC	Consulte DenyCustomRoutingTraffic

Trabajar con aceleradores estándar en el AWS Global Accelerator

Este capítulo incluye procedimientos y recomendaciones para crear aceleradores estándar en AWS Global Accelerator. Con un acelerador estándar, Global Accelerator elige el punto final más adecuado para su tráfico.

Si, en su lugar, desea utilizar la lógica de aplicación personalizada para dirigir uno o más usuarios a un extremo específico entre muchos extremos, cree un acelerador de enrutamiento personalizado. Para obtener más información, consulte Trabajar con aceleradores de enrutamiento personalizados en AWS Global Accelerator.

Para configurar un acelerador estándar, haga lo siguiente:

1. Cree un acelerador y elija la opción de acelerador estándar.
2. Agregue un listener con un conjunto específico de puertos o rango de puertos y elija el protocolo que desea aceptar: TCP, UDP o ambos.
3. Agregue uno o más grupos de endpoints, uno para cada región de AWS en la que tenga recursos de endpoints.
4. Añada uno o más puntos finales a grupos de extremos. Esto no es necesario, pero el tráfico no se enrutará si no tienes ningún endpoints. Los extremos pueden ser equilibradores de carga de red, equilibradores de carga de aplicaciones, instancias de Amazon EC2 o direcciones IP elásticas.

En las secciones siguientes se trabaja con aceleradores estándar, oyentes, grupos de endpoints y endpoints.

Temas

AWS Global Accelerator

AEstándar AcceleradorEn AWS Global Accelerator dirige el tráfico a puntos finales óptimos a través de la red global de AWS para mejorar la disponibilidad y el rendimiento de las aplicaciones de Internet que tienen un público global. Cada acelerador incluye uno o más oyentes. Un listener procesa las conexiones entrantes de los clientes a Global Accelerator, en función del protocolo (o protocolos) y el puerto (o rango de puertos) que configure.

Al crear un acelerador, de forma predeterminada, Global Accelerator le proporciona un conjunto de dos direcciones IP estáticas. Si lleva su propio rango de direcciones IP a AWS (BYOIP), puede asignar direcciones IP estáticas de su propio grupo para usarlas con el acelerador. Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en el AWS Global Accelerator.

> **Important**
>
> Las direcciones IP se asignan al acelerador durante el tiempo que exista, incluso si deshabilita el acelerador y ya no acepta ni enruta el tráfico. Sin embargo, cuandodeleteun acelerador, pierde las direcciones IP estáticas del acelerador global que están asignadas al acelerador, por lo que ya no puede enrutar el tráfico usándolas. Como práctica recomendada, asegúrese de que dispone de permisos para evitar eliminar aceleradores inadvertidamente. Puede utilizar directivas de IAM con Global Accelerator, por ejemplo, permisos basados en etiquetas, para limitar los usuarios que tienen permisos para eliminar un acelerador. Para obtener más información, consulte Políticas basadas en etiquetas.

En esta sección se explica cómo crear, editar o eliminar un acelerador estándar en la consola de Global Accelerator. Si desea utilizar operaciones de API con Global Accelerator, consulte laReferencia de la API de AWS Global Accelerator.

Temas

Creación o actualización de un acelerador estándar

En esta sección se explica cómo crear o actualizar aceleradores estándar en la consola. Para trabajar con Global Accelerator mediante programación, consulte laReferencia de la API de AWS Global Accelerator.

Para crear un acelerador

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. SeleccionarCrear acelerador.
3. Proporcione un nombre para el acelerador.
4. ParaTipo de acelerador, seleccioneestándar.
5. Opcionalmente, si ha traído sus propios rangos de direcciones IP a AWS (BYOIP), puede especificar una dirección IP estática para el acelerador, una de cada grupo de direcciones. Haga esta elección para cada una de las dos direcciones IP estáticas de su acelerador.
   - Para cada dirección IP estática, elija el grupo de direcciones IP que desea utilizar.

     > **Note**
     >
     > Debe elegir un grupo de direcciones IP diferente para cada dirección IP estática. Esta restricción se debe a que Global Accelerator asigna cada rango de direcciones a una zona de red diferente, para una alta disponibilidad.

   - Si ha elegido su propio grupo de direcciones IP, elija también una dirección IP específica del grupo. Si elige el grupo de direcciones IP predeterminado de Amazon, Global Accelerator asigna una dirección IP específica a su acelerador.
6. Si lo desea, añada una o varias etiquetas para ayudarle a identificar los recursos del acelerador.
7. SeleccionarSiguientepara agregar oyentes, grupos de endpoints y endpoints.

Para editar un acelerador estándar

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la lista de aceleradores, elija uno y, a continuación,Editar.

3. En la páginaEdición del aceleradorHaga los cambios que desee. Por ejemplo, puede deshabilitar el acelerador para que ya no acepte o enrute el tráfico, o para que pueda eliminarlo. O bien, si el acelerador está desactivado, puede habilitarlo.
4. Elija Save changes.

Eliminación de un acelerador

Si ha creado un acelerador como prueba o si ya no utiliza un acelerador, puede eliminarlo. En la consola, deshabilite el acelerador y luego puede eliminarlo. No es necesario eliminar los oyentes y los grupos de puntos finales del acelerador.

Para eliminar un acelerador mediante una operación de API en lugar de la consola, primero debe quitar todos los listeners y grupos de extremos asociados al acelerador y, a continuación, deshabilitarlo. Para obtener más información, consulte laDeleteAcceleratorEn laReferencia de la API de AWS Global Accelerator.

Para deshabilitar un acelerador

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la lista, elija un acelerador que desee deshabilitar.
3. Elija Edit (Editar).
4. SeleccionarDeshabilitar aceleradorY, a continuación, elijaSave (Guardar).

Para eliminar un acelerador

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la lista, elija un acelerador que desee eliminar.
3. Elija Eliminar.

> **Note**
>
> Si aún no ha desactivado el aceleradorEliminarNo está disponible.

4. En el cuadro de diálogo de confirmación, elija Delete (Eliminar).

> **Important**
>
> Cuando elimina un acelerador, pierde las direcciones IP estáticas asignadas al acelerador, por lo que ya no puede enrutar el tráfico usándolas.

Visualización de los aceleradores

Puede ver información acerca de los aceleradores en la consola. Para ver las descripciones de los aceleradores mediante programación, consulteListAcceleratorsyDescribeAcceleratoren laReferencia de la API de AWS Global Accelerator.

Para ver la información del acelerador

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. Para ver detalles acerca de un acelerador, en la lista, elija un acelerador y, a continuación, elijaVista.

Añadir un acelerador cuando se crea un balanceador de carga

Si crea un Application Load Balancer en la consola de administración de AWS, puedeAñadir un acelerador. Elastic Load Balancing y Global Accelerator trabajan juntos para añadir el acelerador de forma transparente. El acelerador se crea en su cuenta, con el equilibrador de carga como punto final. Con un acelerador, se proporcionan direcciones IP estáticas y se mejora la disponibilidad y el rendimiento de las aplicaciones.

> **Important**
>
> Para crear un acelerador, debe contar con los permisos correctos. Para obtener más información, consulte Permisos necesarios para el acceso a la consola, la administración de autenticación y el control de acceso.

Configurar y ver el acelerador

Debe actualizar la configuración DNS para dirigir el tráfico a las direcciones IP estáticas o el nombre DNS del acelerador. El tráfico no pasará por el acelerador hasta el equilibrador de carga hasta que se completen los cambios de configuración.

Después de crear el equilibrador de carga mediante la selección del complemento Acelerador global en la consola de Amazon EC2, vaya a laServicios integradosPara ver las direcciones IP estáticas y el nombre del sistema de nombres de dominio (DNS) del acelerador. Utilice esta información para comenzar a enrutar el tráfico de usuario al equilibrador de carga a través de la red global de AWS. Para obtener más información acerca del nombre de DNS asignado al acelerador, consulteDireccionamiento DNS y dominios personalizados en AWS Global Accelerator.

Puede ver y configurar su aceleradorNavegación a Global AcceleratorEn la Consola de administración de AWS. Por ejemplo, puede ver los aceleradores asociados a su cuenta o agregar equilibradores de carga adicionales al acelerador. Para obtener más información, consulte Visualización de los aceleradores y Creación o actualización de un acelerador estándar.

Precios

Con AWS Global Accelerator, paga únicamente por lo que utiliza. Se le cobrará una tarifa por hora y los costos de transferencia de datos por cada acelerador de su cuenta. Para obtener más información, consultePrecios de AWS Global Accelerator.

Deje de utilizar el acelerador

Si desea detener el enrutamiento del tráfico a través de Global Accelerator hacia su equilibrador de carga, haga lo siguiente:

1. Actualice la configuración de DNS para dirigir el tráfico directamente al equilibrador de carga.
2. Elimine el equilibrador de carga del acelerador. Para obtener más información, consultePara eliminar un punto de enlaceinAgregar, editar o eliminar un extremo estándar.
3. Eliminar el acelerador. Para obtener más información, consulte Eliminación de un acelerador.

Usar direcciones IP estáticas globales en lugar de direcciones IP estáticas regionales

Si desea utilizar una dirección IP estática frente a un recurso de AWS, como una instancia de Amazon EC2, tiene varias opciones. Por ejemplo, puede asignar una dirección IP elástica, que es

una dirección IPv4 estática que puede asociar a una instancia de Amazon EC2 o interfaz de red en una sola región de AWS.

Si tiene una audiencia global, puede crear un acelerador con Global Accelerator para obtener dos direcciones IP estáticas globales que se anuncian desde ubicaciones de borde de AWS de todo el mundo. Si ya tiene los recursos de AWS configurados para sus aplicaciones, en una o varias regiones, incluidas las instancias de Amazon EC2, los equilibradores de carga de red y los equilibradores de carga de aplicaciones, puede agregarlos fácilmente a Global Accelerator para enfrentarlos con direcciones IP estáticas globales.

La opción de utilizar direcciones IP estáticas globales aprovisionadas por Global Accelerator también puede mejorar la disponibilidad y el rendimiento de sus aplicaciones. Con Global Accelerator, las direcciones IP estáticas aceptan el tráfico entrante en la red global de AWS desde la ubicación perimetral más cercana a sus usuarios. Maximizar el tiempo de tráfico en la red de AWS puede proporcionar una experiencia de cliente más rápida y mejor. Para obtener más información, consulte Cómo funciona AWS Global Accelerator .

Puede agregar un acelerador desde AWS Management Console o mediante operaciones de API con la CLI o SDK de AWS. Para obtener más información, consulte Creación o actualización de un acelerador estándar.

Tenga en cuenta lo siguiente cuando añada un acelerador:

- Las direcciones IP estáticas globales aprovisionadas por Global Accelerator permanecen asignadas a usted durante el tiempo que el acelerador exista, incluso si deshabilita el acelerador y ya no acepta ni enruta el tráfico. Sin embargo, si elimina un acelerador, pierde las direcciones IP estáticas que se le asignan. Para obtener más información, consulte Eliminación de un acelerador.
- Con Global Accelerator, paga únicamente por lo que utiliza. Se le cobrará una tarifa por hora y los costos de transferencia de datos por cada acelerador de su cuenta. Para obtener más información, consultePrecios de AWS Global Accelerator.

Listeners para aceleradores estándar en el AWS Global Accelerator

Con AWS Global Accelerator, puede agregar oyentes que procesan las conexiones entrantes de los clientes en función de los puertos y protocolos que especifique. Los oyentes admiten TCP, UDP o ambos protocolos TCP y UDP.

Siempre que se crea el acelerador estándar, se crea un agente de escucha estándar, se crea un agente de escucha estándar y se crea más agentes de escucha en cualquier momento. Asocia cada oyente a uno o más grupos de endpoints y asocia cada grupo de endpoints a una región de AWS.

Temas

Agregar, editar o quitar un listener estándar

En esta sección se explica cómo trabajar con agentes de escucha en la consola de AWS Global Accelerator. Para completar estas tareas mediante una operación API en lugar de la consola, consulte`CreateListener`,`UpdateListener`, y`DeleteListener`en laReferencia de AWS Global Accelerator API.

Para agregar un agente de escucha

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores deElija un acelerador.
3. Elija Add listener (Añadir agente de escucha).
4. En la páginaAgregar un agente de escucha, introduzca los puertos o rangos de puertos que desea asociar al agente de escucha. Los agentes de escucha admiten puertos 1-65535.
5. Elija el protocolo para los puertos que ha introducido.
6. Opcionalmente, elija habilitar la afinidad del cliente. La afinidad del cliente por un agente de escucha significa que Global Accelerator garantiza que las conexiones de una dirección IP de origen (cliente) específica se enrutan siempre al mismo punto final. Para habilitar este comportamiento, en la lista desplegable, elijaIP de origen.

   El valor predeterminado esNone (Ninguno), lo que significa que la afinidad del cliente no está habilitada y Global Accelerator distribuye el tráfico equitativamente entre los extremos de los grupos de endpoints para el listener.

   Para obtener más información, consulte Afinidad del cliente.
7. Elija Add listener (Añadir agente de escucha).

Para editar un listener estándar

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores deElija un acelerador.
3. Elija un oyente y, a continuación, elijaEditar agente de escucha.
4. En la páginaEditar agente de escucha, cambie los puertos, rangos de puertos o protocolos que desee asociar al agente de escucha.
5. Opcionalmente, elija habilitar la afinidad del cliente. La afinidad del cliente por un agente de escucha significa que Global Accelerator garantiza que las conexiones de una dirección IP de origen (cliente) específica se enrutan siempre al mismo punto final. Para habilitar este comportamiento, en la lista desplegable, elijaIP de origen.

   El valor predeterminado esNone (Ninguno), lo que significa que la afinidad del cliente no está habilitada y Global Accelerator distribuye el tráfico equitativamente entre los extremos de los grupos de endpoints para el listener.

   Para obtener más información, consulte Afinidad del cliente.
6. Elija Save (Guardar).

Para quitar un agente de escucha

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores deElija un acelerador.
3. Elija un oyente y, a continuación, elijaRemove.
4. En el cuadro de diálogo de confirmación, elijaRemove.

Afinidad del cliente

Si tiene aplicaciones con estado que utiliza con un acelerador estándar, puede elegir que Global Accelerator dirija todas las solicitudes de un usuario en una dirección IP de origen (cliente) específica al mismo recurso de endpoint, para mantener la afinidad del cliente.

De forma predeterminada, la afinidad del cliente para un listener estándar se establece enNone (Ninguno)y Global Accelerator distribuye el tráfico de manera equitativa entre los endpoints de los grupos de endpoints para el listener.

Global Accelerator utiliza un algoritmo hash de flujo coherente para elegir el punto de enlace óptimo para la conexión de un usuario. Si configura la afinidad del cliente para que el recurso de Global Accelerator seaNone (Ninguno)Para seleccionar el valor hash, Global Accelerator utiliza las propiedades de 5 tuplas (IP de origen, puerto de origen, IP de destino y protocolo). A continuación, elige el endpoint que proporciona el mejor rendimiento. Si un cliente determinado utiliza puertos diferentes para conectarse a Global Accelerator y ha especificado esta configuración, Global Accelerator no puede garantizar que las conexiones del cliente siempre se enruten al mismo punto de enlace.

Si desea mantener la afinidad del cliente mediante el enrutamiento de un usuario específico (identificado por su dirección IP de origen) al mismo extremo cada vez que se conecte, establezca la afinidad del cliente enIP de origen. Cuando se especifica esta opción, Global Accelerator utiliza las propiedades de dos tuplas (IP de origen e IP de destino) para seleccionar el valor hash y enrutar al usuario al mismo punto de enlace cada vez que se conecta. Global Accelerator respeta la afinidad del cliente después del grupo de endpoints que seleccione.

Grupos de endpoints para aceleradores estándar en AWS Global Accelerator

Un grupo de puntos de enlace enruta las solicitudes a uno o más puntos de enlace registrados en AWS Global Accelerator. Cuando se agrega un listener en un acelerador estándar, se especifican los grupos de extremos a los que Global Accelerator dirigirá el tráfico. Un grupo de endpoints, y todos los endpoints que contiene, deben estar en una región de AWS. Puede agregar diferentes grupos de endpoints para diferentes propósitos, por ejemplo, para pruebas de implementación azul/verde.

Global Accelerator dirige el tráfico a grupos de endpoints en aceleradores estándar según la ubicación del cliente y el estado del grupo de endpoints. Si lo desea, también puede establecer el porcentaje de tráfico que se va a enviar a un grupo de puntos de enlace. Para ello, utilice el marcado de tráfico para aumentar (marcación hacia arriba) o disminuir (marcación hacia abajo) el tráfico al grupo. El porcentaje se aplica sólo al tráfico que Global Accelerator ya está dirigiendo al grupo de puntos finales, no a todo el tráfico que llega a un agente de escucha.

Puede definir la configuración de comprobación de estado de Global Accelerator para cada grupo de endpoints. Al actualizar la configuración de comprobación de estado, puede cambiar los requisitos para sondeo y verificar el estado de los extremos de direcciones IP elásticas y de instancias de Amazon EC2. Para los extremos de Network Load Balancer y Application Load Balancer, configure los parámetros de comprobación de estado en la consola de Elastic Load Balancing.

Global Accelerator supervisa continuamente el estado de todos los endpoints incluidos en un grupo de endpoints estándar y envía solicitudes sólo a los endpoints activos que están en buen estado. Si no hay endpoints en buen estado para enrutar el tráfico, Global Accelerator enruta las solicitudes a todos los endpoints.

En esta sección se explica cómo trabajar con grupos de terminales para aceleradores estándar en la consola de AWS Global Accelerator. Si desea utilizar operaciones de API con AWS Global Accelerator, consulte laReferencia de la API de AWS Global Accelerator.

Temas

- Agregar, editar o eliminar un grupo de extremos estándar
- Ajuste del flujo de tráfico con diales de tráfico
- Sobrescritura de puerto
- Opciones de comprobación de estado

Agregar, editar o eliminar un grupo de extremos estándar

Trabaja con grupos de puntos de enlace en la consola de AWS Global Accelerator o mediante una operación de API. Puede agregar o quitar puntos de enlace de un grupo de puntos de enlace en cualquier momento.

En esta sección se explica cómo trabajar con grupos de puntos de enlace estándar en la consola de AWS Global Accelerator. Si desea utilizar operaciones de API con Global Accelerator, consulte laReferencia de la API de AWS Global Accelerator.

Para añadir un grupo de puntos de enlace estándar

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores deElija un acelerador.
3. En el navegadorAgentes de escuchasección, paraID del agente de escuchaElija el ID del agente de escucha al que desea agregar un grupo de puntos de enlace.
4. SeleccionarAñadir un grupo de puntos de enlace.
5. En la sección de un listener, especifique una región para el grupo de extremos eligiendo una de la lista desplegable.
6. Opcionalmente, paraMarcado de tráfico, escriba un número de 0 a 100 para establecer un porcentaje de tráfico para este grupo de endpoints. El porcentaje se aplica sólo al tráfico

que ya está dirigido a este grupo de endpoints, no a todo el tráfico de listener. De forma predeterminada, el marcado de tráfico está establecido en 100.

7. Si lo desea, para anular el puerto de escucha utilizado para enrutar el tráfico a los endpoints y redirigir el tráfico a puertos específicos de los endpoints, elijaConfigurar anulaciones de puertos. Para obtener más información, consulte Sobrescritura de puerto.
8. Opcionalmente, para especificar valores de comprobación de estado personalizados que se aplicarán a los extremos de la instancia de EC2 y la dirección IP elástica, elijaConfigurar comprobaciones de estado. Para obtener más información, consulte Opciones de comprobación de estado.
9. También puede seleccionarAñadir un grupo de puntos de enlacePara agregar grupos de puntos de enlace adicionales para este agente de escucha u otros agentes de escucha.
10. SeleccionarAñadir un grupo de puntos de enlace.

Para editar un grupo de puntos de enlace

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores deElija un acelerador.
3. En el navegadorAgentes de escuchasección, paraID del agente de escuchaElija el ID del agente de escucha al que está asociado el grupo de puntos de enlace.
4. SeleccionarEditar el grupo de puntos de enlace.
5. En la páginaEditar el grupo de puntos de enlace, cambie la región, ajuste el porcentaje de marcado de tráfico o elijaConfigurar comprobaciones de estadoPara modificar la configuración de comprobación de estado.
6. Elija Save (Guardar).

Para eliminar un grupo de puntos de enlace normalizados

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores deElija un acelerador.
3. En el navegadorAgentes de escuchaElija un agente de escucha y luego elijaRemove.
4. En el navegadorGrupos de puntos de enlaceElija un grupo de puntos de enlace y luego elijaRemove.
5. En el cuadro de diálogo de confirmación, elijaRemove.

Ajuste del flujo de tráfico con diales de tráfico

Para cada grupo de endpoints estándar, puede establecer un marcado de tráfico para controlar el porcentaje de tráfico que se dirige al grupo. El porcentaje se aplica sólo al tráfico que ya está dirigido al grupo de endpoints, no a todo el tráfico de listener.

De forma predeterminada, el marcado de tráfico se establece en 100 (es decir, 100%) para todos los grupos de extremos regionales de un acelerador. El dial de tráfico le permite realizar fácilmente pruebas de rendimiento o pruebas de implementación azul/verde para nuevas versiones en diferentes regiones de AWS, por ejemplo.

A continuación se presentan algunos ejemplos para ilustrar cómo puede utilizar las marcaciones de tráfico para cambiar el flujo de tráfico a grupos de puntos finales.

Actualice su aplicación por región

Si desea actualizar una aplicación en una región o realizar tareas de mantenimiento, establezca primero el marcado de tráfico en 0 para cortar el tráfico de la región. Cuando finalice el trabajo y esté listo para volver a poner en servicio la Región, ajuste el dial de tráfico a 100 para marcar el tráfico de nuevo.

Mezclar el tráfico entre dos regiones

En este ejemplo se muestra cómo funciona el flujo de tráfico al cambiar las marcaciones de tráfico de dos grupos de extremos regionales al mismo tiempo. Supongamos que tiene dos grupos de endpoints para el acelerador, uno para el`us-west-2`Región y una para el`us-east-1`Región y ha establecido las marcaciones de tráfico en 50% para cada grupo de puntos finales.

Ahora, digamos que tiene 100 solicitudes llegando a su acelerador, con 50 de la costa este de los Estados Unidos y 50 de la costa oeste. El acelerador dirige el tráfico de la siguiente manera:

- Las primeras 25 solicitudes en cada costa (50 solicitudes en total) se atienden desde su grupo de terminales cercano. Es decir, 25 solicitudes se dirigen al grupo de endpoints en`us-west-2`y 25 se dirigen al grupo de puntos finales en`us-east-1`.
- Las siguientes 50 solicitudes se dirigen a las regiones opuestas. Es decir, las próximas 25 solicitudes de la Costa Este son atendidas por`us-west-2`, y las siguientes 25 solicitudes de la Costa Oeste son atendidas por`us-east-1`.

El resultado en este escenario es que ambos grupos de endpoints sirven la misma cantidad de tráfico. Sin embargo, cada una recibe una mezcla de tráfico de ambas regiones.

Sobrescritura de puerto

De forma predeterminada, un acelerador enruta el tráfico de usuario a los extremos de las regiones de AWS mediante el protocolo y los rangos de puertos especificados al crear un listener. Por ejemplo, si define un agente de escucha que acepta tráfico TCP en los puertos 80 y 443, el acelerador enruta el tráfico a esos puertos en un extremo.

Sin embargo, cuando agrega o actualiza un grupo de puntos de enlace, puede anular el puerto del agente de escucha utilizado para direccionar el tráfico a puntos de enlace. Por ejemplo, puede crear una sobrescritura de puerto en la que el agente de escucha reciba tráfico del usuario en los puertos 80 y 443, pero el acelerador enrutará dicho tráfico hacia los puertos 1080 y 1443, respectivamente, en los puntos de enlace.

Las anulaciones de puertos pueden ayudarle a evitar problemas de escucha en puertos restringidos. Es más seguro ejecutar aplicaciones que no requieren privilegios de superusuario (root) en sus endpoints. Sin embargo, en Linux y otros sistemas similares a UNIX, debe tener privilegios de superusuario para escuchar en puertos restringidos (puertos TCP o UDP inferiores a 1024). Al asignar un puerto restringido de un agente de escucha a un puerto no restringido de un extremo, las anulaciones de puerto le permiten evitar este problema. Puede aceptar tráfico en puertos restringidos mientras ejecuta aplicaciones sin acceso root en sus endpoints detrás de Global Accelerator. Por ejemplo, puede anular un puerto de escucha 443 a un puerto de extremo 8443.

Para cada modificación de puerto, especifique un puerto de escucha que acepte el tráfico de los usuarios y el puerto de extremo al que Global Accelerator enrutará ese tráfico. Para obtener más información, consulte Agregar, editar o eliminar un grupo de extremos estándar.

Cuando cree una modificación de puerto, tenga en cuenta lo siguiente:

- Los puertos de extremo no pueden superponerse a rangos de puertos de escucha. Los puertos de punto final que especifique en una modificación de puerto no se pueden incluir en ninguno de los rangos de puertos de escucha que haya configurado para el acelerador. Por ejemplo, supongamos que tiene dos oyentes para un acelerador y que ha definido los rangos de puertos para esos oyentes como 100-199 y 200-299, respectivamente. Al crear modificaciones de puerto, no se puede definir una desde el puerto 100 del listener al puerto de extremo 210, por ejemplo, porque el puerto de extremo (210) se incluye en un rango de puertos de escucha definido (200-299).
- No hay puertos de extremo duplicados. Si una anulación de puerto en un acelerador especifica un puerto de punto final, no puede especificar el mismo puerto de punto final con anulación de puerto desde otro puerto de escucha. Por ejemplo, no se puede especificar una modificación de puerto

desde el puerto de escucha 80 al puerto de extremo 90 junto con una modificación del puerto de escucha 81 al puerto de extremo 90.

- La Health de estado continúa utilizando el puerto original. Si especifica una modificación de puerto para un puerto que está configurado como puerto de comprobación de estado, la comprobación de estado seguirá utilizando el puerto original, no el puerto de sustitución. Por ejemplo, supongamos que especifica comprobaciones de estado en el puerto 80 del listener y que también especifica una modificación de puerto desde el puerto de escucha 80 al puerto de extremo 480. Las Health aciones de estado siguen utilizando el puerto de extremo 80. Sin embargo, el tráfico de usuario que entra a través del puerto 80 va al puerto 480 del endpoint.

  Este comportamiento mantiene la coherencia entre el Network Load Balancer, el Application Load Balancer, la instancia de EC2 y los extremos de direcciones IP elásticas. Dado que los equilibradores de carga de red y los equilibradores de carga de aplicaciones no asignan puertos de comprobación de estado a otros puertos de punto final cuando se especifica una anulación de puerto en Global Accelerator, sería incoherente que Global Accelerator asignara puertos de comprobación de estado a diferentes puertos de extremo para la instancia de EC2 y Elastic IP puntos finales de dirección.
- La configuración del grupo de seguridad debe permitir el acceso al puerto. Asegúrese de que los grupos de seguridad permiten el tráfico a los puertos de punto de enlace que ha designado en las modificaciones de puerto. Por ejemplo, si anula el puerto 443 del listener al puerto de endpoint 1433, asegúrese de que las restricciones de puerto establecidas en el grupo de seguridad para ese Application Load Balancer o el endpoint de Amazon EC2 permiten el tráfico entrante en el puerto 1433.

Opciones de comprobación de estado

AWS Global Accelerator envía periódicamente solicitudes a puntos de enlace estándar para comprobar su estado. Estas comprobaciones de estado se ejecutan automáticamente. La guía para determinar el estado de cada endpoint y el tiempo para las comprobaciones de estado dependen del tipo de recurso de endpoint.

> **Important**
>
> Global Accelerator requiere que las reglas de enrutador y firewall permitan el tráfico entrante de las direcciones IP asociadas con los comprobadores de estado de Route 53 para completar las comprobaciones de estado de los endpoints de instancias EC2 o direcciones IP elásticas. Puede encontrar información sobre los rangos de direcciones IP asociados a los

comprobadores de estado de Amazon Route 53 enComprobaciones de estado de los grupos de destinoen laAmazon Route 53 Guía del desarrollador.

Puede configurar las siguientes opciones de comprobación de estado para un grupo de endpoints. Si especifica opciones de comprobación de estado, Global Accelerator utiliza la configuración de las comprobaciones de estado de la instancia de EC2 o de la dirección IP elástica, pero no para los Equilibradores de carga de red o los Equilibradores de carga de aplicaciones.

- Para los extremos de Equilibrio de carga de aplicaciones o Equilibrio de carga de red, puede configurar las comprobaciones de estado de los recursos mediante las opciones de configuración de Elastic Load Balancing. Para obtener más información, consulteComprobaciones de estado de los grupos de destino. Las opciones de Health de estado que elija en el acelerador global no afectan a los equilibradores de carga de aplicaciones ni a los equilibradores de carga de red que haya agregado como endpoints.

  > **Note**
  >
  > Cuando tiene un equilibrador de carga de aplicaciones o un equilibrNetwork Load Balancer que incluye varios grupos de destino, Global Accelerator considera que el extremo del equilibrador de carga es correcto sólo siEACHdetrás del equilibrador de carga tiene al menos un objetivo en buen estado. Si un solo grupo de destino para el equilibrador de carga solo tiene destinos en mal estado, Global Accelerator considera que el punto final no es correcto.

- Para los extremos de dirección IP elástica o de instancia de EC2 que se agregan a un listener configurado con TCP, puede especificar el puerto que se utilizará para las comprobaciones de estado. De forma predeterminada, si no especifica un puerto para las comprobaciones de estado, Global Accelerator utiliza el puerto de escucha que especificó para el acelerador.
- Para los extremos de direcciones IP elásticas o instancias de EC2 con oyentes UDP, Global Accelerator utiliza el puerto de escucha y el protocolo TCP para las comprobaciones de estado, por lo que debe tener un servidor TCP en el endpoint.

  > **Note**
  >
  > Asegúrese de comprobar que el puerto que ha configurado para el servidor TCP en cada extremo es el mismo que el puerto especificado para la comprobación de estado en Global Accelerator. Si los números de puerto no son los mismos, o si no ha configurado

un servidor TCP para el endpoint, Global Accelerator marca el endpoint como incorrecto, independientemente del estado del endpoint.

Puerto Health comprobación de estado

El puerto que se va a utilizar cuando Global Accelerator realiza comprobaciones de estado de los puntos de enlace que forman parte de este grupo de puntos de enlace.

> **Note**
>
> No se puede establecer una anulación de puerto para los puertos de comprobación de estado.

Protocolo de comprobación de estado

Protocolo que se utiliza cuando Global Accelerator realiza comprobaciones de estado de los puntos de enlace que forman parte de este grupo de puntos de enlace.

Intervalo de Health de

Intervalo, en segundos, entre cada comprobación de estado de un punto de enlace.

Número de umbrales

Número de comprobaciones de estado consecutivas que deben superarse para considerar que un destino que no está en buen estado está en buen estado o que un destino que no

Cada listener enruta las solicitudes sólo a puntos finales en buen estado. Después de agregar un punto de enlace, debe superar una comprobación de estado para que se considere que se encuentra en buen estado. Después de completar cada comprobación de estado, el agente de escucha cierra la conexión que se estableció para la comprobación de estado.

Puntos finales para aceleradores estándar en el AWS Global Accelerator

Los puntos finales para los aceleradores estándar del AWS Global Accelerator pueden ser equilibradores de carga de red, equilibradores de carga de aplicaciones, instancias de Amazon

EC2 o direcciones IP elásticas. Con los aceleradores estándar, una dirección IP estática sirve como un único punto de contacto para los clientes, y Global Accelerator, a continuación, distribuye el tráfico entrante entre los puntos de enlace en buen estado. Global Accelerator dirige el tráfico a los endpoints mediante el puerto (o rango de puertos) que especifique para el listener al que pertenece el grupo de endpoints del endpoint.

Cada grupo de puntos de enlace puede tener varios puntos de enlace. Puede agregar cada extremo a varios grupos de endpoints, pero los grupos de endpoints deben estar asociados a distintos oyentes. Un recurso debe ser válido y activo cuando se agrega como punto de enlace.

Global Accelerator supervisa continuamente el estado de todos los endpoints incluidos en un grupo de endpoints estándar. Envía el tráfico sólo a los endpoints activos que están en buen estado. Si Global Accelerator no tiene endpoints en buen estado para enrutar el tráfico, enruta el tráfico a todos los endpoints.

Tenga en cuenta lo siguiente para tipos específicos de endpoints estándar de Global Accelerator:

Puntos de enlace del equilibrador de carga

- Un punto de enlace del Application Load Balancer puede estar expuesto a internet o interno. Un extremo del Network Load Balancer debe estar orientado a Internet.

Puntos de enlace de instancias de Amazon EC2

- Un extremo de instancia EC2 (para aceleradores de enrutamiento estándar y personalizado) no puede ser uno de los siguientes tipos: C1, CC1, CC2, CG1, CG2, CR1, G2, HI1, HS1, HS1, M2, M2, M3 o T1.
- Las instancias EC2 solo se admiten como puntos de enlace en algunas regiones de AWS. Para obtener una lista de las regiones admitidas, consulte Regiones de AWS admitidas para la preservación de direcciones IP.
- Se recomienda quitar una instancia de EC2 de los grupos de extremos de Global Accelerator antes de finalizar la instancia. Si finaliza una instancia de EC2 antes de quitarla de un grupo de endpoints en Global Accelerator y, a continuación, crea otra instancia en la misma VPC con la misma dirección IP privada y pasan las comprobaciones de estado, Global Accelerator enrutará el tráfico al nuevo endpoint.

Temas

- Agregar puntos finales con preservación de direcciones IP del cliente
- Transición de endpoints para utilizar la preservación de direcciones IP del cliente

Agregar, editar o eliminar un extremo estándar

Agregue endpoints a grupos de endpoints para que el tráfico pueda dirigirse a sus recursos. Puede editar un extremo estándar para cambiar el peso del extremo. O puede eliminar un extremo del acelerador quitándolo de un grupo de extremos. La eliminación de un endpoint no afecta al endpoint en sí, pero Global Accelerator ya no puede dirigir el tráfico a ese recurso.

Los extremos de Global Accelerator pueden ser equilibradores de carga de red, equilibradores de carga de aplicaciones, instancias de Amazon EC2 o direcciones IP elásticas. Primero debe crear uno de esos recursos y, a continuación, puede agregarlo como un extremo en Global Accelerator. Un recurso debe ser válido y activo cuando se agrega como punto de enlace.

Puede añadir o quitar puntos de enlace de grupos de punto de enlace en función del uso. Por ejemplo, si aumenta la demanda de la aplicación, puede crear más recursos y, a continuación, agregar más puntos finales a uno o más grupos de endpoints para controlar el aumento del tráfico. Global Accelerator comienza a direccionar las solicitudes a un punto de enlace tan pronto como se agrega y el punto de enlace supera las comprobaciones de estado iniciales. Puede administrar el tráfico a los endpoints ajustando los pesos de un endpoint para enviar proporcionalmente más o menos tráfico al endpoint.

Si va a agregar un extremo con la preservación de la dirección IP del cliente, primero revise la información enRegiones de AWS admitidas para la preservación de direcciones IPyConservar las direcciones IP del cliente en el AWS Global Accelerator.

Puede eliminar endpoints de sus grupos de endpoints, por ejemplo, si necesita dar servicio a los endpoints. Al quitar un punto de enlace, este se lleva del grupo de puntos de enlace, pero no se ve afectado de ningún otro modo. Global Accelerator deja de dirigir el tráfico a un endpoint tan pronto como lo elimina de un grupo de endpoints. El endpoint entra en un estado en el que espera a que se completen todas las solicitudes actuales, de modo que no se interrumpa el tráfico del cliente que está en curso. Puede volver a añadir el punto de enlace al grupo de puntos de enlace cuando esté preparado para reanudar la recepción de solicitudes.

En esta sección se explica cómo trabajar con puntos de enlace en la consola de AWS Global Accelerator. Si desea utilizar las operaciones de API con AWS Global Accelerator, consulte laReferencia de la API de AWS Global Accelerator.

Para añadir un punto de enlace estándar

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores deElija un acelerador.
3. En el navegadorAgentes de escuchasección, paraID del agente de escucha, elija el ID de un oyente.
4. En el navegadorGrupos de punto de enlacesección, paraID de grupo de punto de enlace, elija el ID del grupo de puntos de enlace al que desea añadir un punto de enlace.
5. En el navegadorPuntos de enlace deElija en la secciónAñadir punto de enlace.
6. En la páginaAgregar puntos finalesElija un recurso de la lista desplegable.

   Si no tiene recursos de AWS, no hay elementos en la lista. Para continuar, cree recursos de AWS como equilibradores de carga, instancias de Amazon EC2 o direcciones IP elásticas. A continuación, vuelva a los pasos aquí y elija un recurso de la lista.
7. Opcionalmente, paraPeso, introduzca un número de 0 a 255 para establecer un peso para enrutar el tráfico a este extremo. Cuando agrega ponderaciones a los puntos de enlace, configura Global Accelerator para que enrute el tráfico en función de las proporciones que especifique. De forma predeterminada, todos los puntos finales tienen un peso de 128. Para obtener más información, consulte Ponderaciones de punto de enlace.
8. Opcionalmente, habilite la preservación de la dirección IP del cliente para un punto de enlace del Application Load Balancer orientado a internet. BajoPreserve la dirección IP de cliente, seleccionePreserve la dirección.

   Esta opción siempre se selecciona para los extremos internos del Application Load Balancer y de instancias EC2, y nunca se selecciona para los extremos de direcciones IP elásticas y Network Load Balancer. Para obtener más información, consulte Conservar las direcciones IP del cliente en el AWS Global Accelerator.

   > **Note**
   >
   > Antes de agregar y comenzar a enrutar el tráfico a los extremos que conservan la dirección IP del cliente, asegúrese de que todas las configuraciones de seguridad necesarias, por ejemplo, grupos de seguridad, se actualizan para incluir la dirección IP del cliente de usuario en las listas de permisos.
9. Seleccione Add endpoint (Añadir punto de enlace).

Para editar un extremo estándar

Puede editar una configuración de endpoint para cambiar el peso. Para obtener más información, consulte Ponderaciones de punto de enlace.

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores deElija un acelerador.
3. En el navegadorAgentes de escuchasección, paraID del agente de escucha, elija el ID de un oyente.
4. En el navegadorGrupos de punto de enlacesección, paraID de grupo de punto de enlace, elija el ID del grupo de puntos de enlace.
5. SeleccionarEditar punto de enlace.
6. En la páginaEditar punto de enlace, realice actualizaciones y, a continuación, elijaSave (Guardar).

Para eliminar un punto de enlace

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores deElija un acelerador.
3. En el navegadorAgentes de escuchasección, paraID del agente de escucha, elija el ID de un oyente.
4. En el navegadorGrupos de punto de enlacesección, paraID de grupo de punto de enlace, elija el ID del grupo de puntos de enlace.
5. SeleccionarEliminar punto final.
6. En el cuadro de diálogo de confirmación, elijaRemove.

Ponderaciones de punto de enlace

Un peso es un valor que determina la proporción de tráfico que Global Accelerator dirige a un punto final en un acelerador estándar. Los extremos pueden ser equilibradores de carga de red, equilibradores de carga de aplicaciones, instancias de Amazon EC2 o direcciones IP elásticas. Global Accelerator calcula la suma de los pesos de los endpoints en un grupo de endpoints y, a continuación, dirige el tráfico a los endpoints en función de la relación entre el peso de cada endpoint y el total.

El enrutamiento ponderado le permite elegir cuánto tráfico se enruta a un recurso en un grupo de endpoints. Esto puede resultar útil de varias maneras, entre otras, equilibrar la carga y probar nuevas versiones de una aplicación.

Cómo funcionan los pesos de punto final

Para utilizar ponderaciones, debe asignar a cada punto de enlace de un grupo de puntos de enlace un peso relativo que se corresponda con la cantidad de tráfico que desea enviar. De forma predeterminada, el peso de un extremo es 128, es decir, la mitad del valor máximo de un peso, 255. Global Accelerator envía el tráfico a un punto de enlace en función del peso que se asigna, como una proporción del peso total de todos los puntos de enlace del grupo:

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

Por ejemplo, si desea enviar una pequeña parte del tráfico a un punto de enlace y el resto a otro punto de enlace, puede especificar pesos de 1 y 255. El punto de enlace con un peso de 1 se lleva una fracción de 1/256 del tráfico (1/1+255), y el otro punto de enlace, 255/256 (255/1+255). Para modificar gradualmente el equilibrio puede cambiar los pesos. Si desea que Global Accelerator deje de enviar tráfico a un punto de enlace, puede cambiar el peso de ese recurso a 0.

Failover para endpoints en mal estado

Si no hay endpoints en buen estado en un grupo de endpoints que tengan un peso mayor que cero, Global Accelerator intenta realizar una conmutación por error a un endpoint en buen estado con un peso mayor que cero en otro grupo de endpoints. Para esta conmutación por error, Global Accelerator ignora la configuración de marcado de tráfico. Por lo tanto, si, por ejemplo, un grupo de endpoints tiene un marcado de tráfico establecido en cero, Global Accelerator seguirá incluyendo ese grupo de endpoints en el intento de conmutación por error.

Si Global Accelerator no encuentra un endpoint en buen estado con un peso superior a cero después de probar tres grupos de endpoints adicionales (es decir, tres regiones de AWS), enruta el tráfico a un extremo aleatorio del grupo de endpoints más cercano al cliente. Es decir, esfalla en la apertura.

Tenga en cuenta lo siguiente:

- El grupo de endpoints elegido para la conmutación por error puede ser uno que tenga un marcado de tráfico establecido en cero.

- Es posible que el grupo de extremos más cercano no sea el grupo de extremos original. Esto se debe a que Global Accelerator considera la configuración de marcado de tráfico de cuenta cuando elige el grupo de endpoints original.

Por ejemplo, supongamos que su configuración tiene dos puntos finales, uno sano y otro no saludable, y que ha establecido que el peso para cada uno de ellos sea mayor que cero. En este caso, Global Accelerator enruta el tráfico al endpoint en buen estado. Sin embargo, ahora digamos que establece el peso del único extremo saludable en cero. A continuación, Global Accelerator intenta tres grupos de puntos finales adicionales para encontrar un punto final saludable con un peso mayor que cero. Si no encuentra uno, Global Accelerator enruta el tráfico a un extremo aleatorio del grupo de endpoints más cercano al cliente.

Agregar puntos finales con preservación de direcciones IP del cliente

Una característica que puede usar con algunos tipos de punto final (en algunas regiones) esPreserve la dirección IP de cliente. Con esta característica, conserva la dirección IP de origen del cliente original para los paquetes que llegan al extremo. Puede utilizar esta función con Application Load Balancer y los extremos de instancia de Amazon EC2. Los extremos de los aceleradores de enrutamiento personalizados siempre conservan la dirección IP del cliente. Para obtener más información, consulte Conservar las direcciones IP del cliente en el AWS Global Accelerator.

Si tiene intención de utilizar la característica de preservación de direcciones IP del cliente, tenga en cuenta lo siguiente al agregar endpoints a Global Accelerator:

Interfaces de red elásticas

Para admitir la preservación de direcciones IP del cliente, Global Accelerator crea interfaces de red elásticas en su cuenta de AWS, una para cada subred en la que esté presente un endpoint. Para obtener más información acerca del funcionamiento de Global Accelerator con interfaces de red elásticas, consultePrácticas recomendadas para la conservación de direcciones IP del cliente.

Puntos de enlace en subredes privadas

Puede dirigirse a un Application Load Balancer o a una instancia EC2 en una subred privada mediante el AWS Global Accelerator, pero debe tener ungateway de Internetconectado a la VPC que contiene los extremos. Para obtener más información, consulte Conexiones VPC seguras en AWS Global Accelerator.

Añadir la dirección IP de cliente a la lista de permisos

Antes de agregar y comenzar a enrutar el tráfico a los extremos que conservan la dirección IP del cliente, asegúrese de que todas las configuraciones de seguridad necesarias, por ejemplo, grupos de seguridad, se actualizan para incluir la dirección IP del cliente del usuario en la lista de permisos. Listas de control de acceso (ACL) de red solo se aplican al tráfico de salida (saliente). Si necesita filtrar el tráfico de entrada (entrante), debe usar grupos de seguridad.

Configurar listas de control de acceso a la red (ACL)

Las ACL de red asociadas a las subredes de VPC se aplican al tráfico de salida (saliente) cuando la preservación de la dirección IP del cliente está habilitada en el acelerador. Sin embargo, para que el tráfico pueda salir a través del acelerador global, debe configurar la ACL como regla de entrada y salida.

Por ejemplo, para permitir que los clientes TCP y UDP que utilicen un puerto de origen efímero se conecten al endpoint mediante Global Accelerator, asocie la subred del endpoint con una ACL de red que permita el tráfico saliente destinado a un puerto TCP o UDP efímero (rango de puertos 1024-65535, destino 0.0.0.0/0). Además, cree una regla de entrada coincidente (rango de puertos 1024-65535, origen 0.0.0.0/0).

> **Note**
>
> El grupo de seguridad y las reglas de AWS WAF son un conjunto adicional de capacidades que puede aplicar para proteger sus recursos. Por ejemplo, las reglas del grupo de seguridad entrante asociadas a las instancias de Amazon EC2 y los equilibradores de carga de aplicaciones le permiten controlar los puertos de destino a los que pueden conectarse los clientes a través del acelerador global, como el puerto 80 para HTTP o el puerto 443 para HTTPS. Tenga en cuenta que los grupos de seguridad de instancias de Amazon EC2 se aplican a cualquier tráfico que llegue a sus instancias, incluido el tráfico de Global Accelerator y cualquier dirección IP pública o elástica asignada a su instancia. Como práctica recomendada, utilice subredes privadas si desea asegurarse de que el tráfico sólo lo entregue Global Accelerator. Asegúrese también de que las reglas del grupo de seguridad entrante están configuradas adecuadamente para permitir o denegar correctamente el tráfico para las aplicaciones.

Transición de endpoints para utilizar la preservación de direcciones IP del cliente

Siga las instrucciones de esta sección para realizar la transición de uno o más puntos finales del acelerador a puntos finales que conserven la dirección IP del cliente del usuario. Opcionalmente, puede optar por pasar un extremo del Application Load Balancer o un extremo de dirección IP elástica a un punto final correspondiente (un equilibrador de carga de aplicaciones o una instancia EC2) que tenga preservación de la dirección IP del cliente. Para obtener más información, consulte Conservar las direcciones IP del cliente en el AWS Global Accelerator.

Recomendamos que realice una transición a utilizar la preservación de la dirección IP del cliente lentamente. Primero, agregue nuevos endpoints de instancia de EC2 o Application Load Balancer que habilite para conservar la dirección IP del cliente. A continuación, mueva lentamente el tráfico de los endpoints existentes a los nuevos endpoints configurando los pesos en los endpoints.

> **Important**
>
> Antes de comenzar a enrutar el tráfico a los endpoints que conservan la dirección IP del cliente, asegúrese de que todas las configuraciones en las que ha incluido direcciones IP de cliente de Global Accelerator en listas de permisos se actualizan para incluir la dirección IP del cliente del usuario en su lugar.

La preservación de la dirección IP del cliente solo está disponible en regiones de AWS específicas. Para obtener más información, consulte Regiones de AWS admitidas para la preservación de direcciones IP.

En esta sección se explica cómo trabajar con grupos de puntos de enlace en la consola de AWS Global Accelerator. Si desea utilizar operaciones de API con Global Accelerator, consulte laReferencia de la API de AWS Global Accelerator.

Después de mover una pequeña cantidad de tráfico al nuevo endpoint con la preservación de la dirección IP del cliente, pruebe para asegurarse de que la configuración funciona de la forma esperada. A continuación, aumente gradualmente la proporción de tráfico al nuevo endpoint ajustando los pesos en los extremos correspondientes.

Para realizar la transición a endpoints que preserven las direcciones IP del cliente, comience siguiendo los pasos que se indican a continuación para agregar un nuevo endpoint y, en el caso de los endpoints de Application Load Balancer con conexión a Internet, habilite la preservación de

la dirección IP del cliente. (La opción de preservación de la dirección IP del cliente siempre está seleccionada para los equilibradores de carga de aplicaciones internos y las instancias de EC2.)

Para agregar un extremo con la preservación de la dirección IP del cliente

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores deElija un acelerador.
3. En el navegadorAgentes de escuchaElija un agente de escucha.
4. En el navegadorGrupo de punto de enlaceElija un punto de enlace.
5. En el navegadorPuntos de enlace deElija en la secciónAñadir punto de enlace.
6. En la páginaAgregar puntos finales, en laPuntos de enlace de, elija un extremo del Application Load Balancer o un extremo de instancia EC2.
7. En el navegadorPeso, elija un número bajo en comparación con los pesos establecidos para los puntos finales existentes. Por ejemplo, si el peso de un Application Load Balancer correspondiente es 255, puede introducir un peso de 5 para el nuevo equilibrador de carga de aplicaciones, para empezar. Para obtener más información, consulte Ponderaciones de punto de enlace.
8. Para un nuevo extremo de Application Load Balancer externo, enPreserve la dirección IP de cliente, seleccionePreserve la dirección. (Esta opción siempre está seleccionada para equilibradores de carga de aplicaciones internos e instancias EC2.)
9. Elija Save changes.

A continuación, siga los pasos que se indican aquí para editar los endpoints existentes correspondientes (que va a reemplazar por los nuevos endpoints con la preservación de la dirección IP del cliente) para reducir los pesos de los endpoints existentes, de modo que se destinen menos tráfico a ellos.

Para reducir el tráfico de los endpoints existentes

1. En la páginaGrupo de punto de enlace, elija un endpoint existente que no tenga preservación de la dirección IP del cliente.
2. Elija Edit (Editar).
3. En la páginaEditar punto de enlace, en laPeso, introduzca un número inferior al número actual. Por ejemplo, si el peso de un extremo existente es 255, podría introducir un peso de 220 para el nuevo extremo (con la preservación de la dirección IP del cliente).

4. Elija Save changes.

Después de probar con una pequeña parte del tráfico original estableciendo el peso del nuevo endpoint en un número bajo, puede transitar lentamente todo el tráfico si continúa ajustando los pesos de los endpoints originales y nuevos.

Por ejemplo, supongamos que comienza con un Application Load Balancer existente con un peso establecido en 200 y agrega un nuevo extremo del equilibrador de carga de aplicaciones con la preservación de la dirección IP del cliente habilitada con un peso establecido en 5. Cambie gradualmente el tráfico del Application Load Balancer original al nuevo equilibrador de carga de aplicaciones aumentando el peso del nuevo equilibrador de carga de aplicaciones y disminuyendo el peso del equilibrador de carga de aplicaciones original. Por ejemplo:

- Peso original 190/nuevo peso 10
- Peso original 180/nuevo peso 20
- Peso original 170/nuevo peso 30, y así sucesivamente.

Cuando se ha reducido el peso a 0 para el extremo original, todo el tráfico (en este escenario de ejemplo) va al nuevo extremo del Application Load Balancer, que incluye la preservación de la dirección IP del cliente.

Si tiene endpoints adicionales (Equilibradores de carga de aplicaciones o instancias EC2) que desea realizar la transición para utilizar la preservación de direcciones IP del cliente, repita los pasos de esta sección para realizar la transición.

Si necesita revertir la configuración de un endpoint para que el tráfico al endpoint no conserve la dirección IP del cliente, puede hacerlo en cualquier momento: aumente el peso del endpoint quenotener la preservación de la dirección IP del cliente al valor original y disminuir el peso del endpointporpreservación de la dirección IP del cliente a 0.

Trabajar con aceleradores de enrutamiento personalizados en AWS Global Accelerator

Este capítulo incluye procedimientos y recomendaciones para crear aceleradores de enrutamiento personalizados en AWS Global Accelerator. Un acelerador de enrutamiento personalizado le permite utilizar la lógica de aplicaciones para asignar directamente a uno o más usuarios a una instancia específica de Amazon EC2 entre muchos destinos, a la vez que obtiene las mejoras de rendimiento de enrutar el tráfico a través del acelerador global. Esto resulta útil cuando se tiene una aplicación que requiere que un grupo de usuarios interactúe entre sí en la misma sesión que se ejecuta en una instancia y puerto EC2 específicos, como aplicaciones de juegos o sesiones de Voz sobre IP (VoIP).

Los extremos de los aceleradores de enrutamiento personalizados deben ser subredes de nube privada virtual (VPC), y un acelerador de enrutamiento personalizado solo puede enrutar el tráfico a instancias de Amazon EC2 en esas subredes. Al crear un acelerador de enrutamiento personalizado, puede incluir miles de instancias de Amazon EC2 que se ejecutan en una o varias subredes de VPC. Para obtener más información, consulte Cómo funcionan los aceleradores de enrutamiento personalizados en AWS Global Accelerator.

Si en su lugar desea que Global Accelerator elija automáticamente el punto final correcto más cercano a sus clientes, cree un acelerador estándar. Para obtener más información, consulte Trabajar con aceleradores estándar en el AWS Global Accelerator.

Haga lo siguiente para configurar un acelerador de direccionamiento personalizado:

1. Revise las directrices y los requisitos para crear un acelerador de direccionamiento personalizado. Consulte Directrices y restricciones para aceleradores de enrutamiento personalizados.
2. Cree una subred de VPC. Puede agregar instancias EC2 a la subred en cualquier momento después de agregar la subred a Global Accelerator.
3. Cree un acelerador y seleccione la opción de un acelerador de direccionamiento personalizado.
4. Agregue un listener y especifique un rango de puertos para que Global Accelerator pueda escuchar. Asegúrese de incluir un amplio rango con suficientes puertos para que Global Accelerator se asigne a todos los destinos que espera tener. Estos puertos son distintos de los puertos de destino, que especificará en el siguiente paso. Para obtener más información sobre los requisitos de puertos de escucha, consulteDirectrices y restricciones para aceleradores de enrutamiento personalizados.

5. Agregue uno o varios grupos de endpoints para las regiones de AWS en las que tenga subredes de VPC. Para cada grupo de puntos de enlace, especifique lo siguiente:
   - Intervalo de puertos de extremo, que representa los puertos de las instancias de EC2 de destino que podrán recibir tráfico.
   - El protocolo para cada rango de puertos de destino: UDP, TCP o UDP y TCP.
6. Para la subred de punto final, seleccione un ID de subred. Puede agregar varias subredes en cada grupo de extremos y las subredes pueden tener diferentes tamaños (hasta /17).

En las secciones siguientes se trabaja con aceleradores de enrutamiento personalizados, oyentes, grupos de endpoints y endpoints.

Temas

Cómo funcionan los aceleradores de enrutamiento personalizados en AWS Global Accelerator

Mediante el uso de un acelerador de enrutamiento personalizado en el AWS Global Accelerator, puede utilizar la lógica de aplicaciones para asignar directamente a uno o más usuarios a un destino específico entre muchos destinos, sin dejar de obtener las ventajas de rendimiento de Global Accelerator. Un acelerador de enrutamiento personalizado asigna rangos de puertos de escucha a destinos de instancia EC2 en subredes de nube privada virtual (VPC). Esto permite a Global Accelerator enrutar de forma determinística el tráfico a una dirección IP privada de Amazon EC2 y a un destino de puerto en su subred.

Por ejemplo, puede utilizar un acelerador de enrutamiento personalizado con una aplicación de juegos en tiempo real en la que asigne varios jugadores a una sola sesión en un servidor de juegos

de Amazon EC2 en función de los factores que elija, como la ubicación geográfica, la habilidad del jugador y el modo de juego. O puede que tenga una aplicación de VoIP o redes sociales que asigne varios usuarios a un servidor multimedia específico para sesiones de voz, vídeo y mensajería.

Su aplicación puede llamar a una API Global Accelerator y recibir una asignación estática completa de los puertos de Global Accelerator y sus direcciones IP de destino y puertos asociados. Puede guardar esa asignación estática y, a continuación, el servicio de emparejamiento la utilice para enrutar usuarios a instancias de EC2 de destino específicas. No es necesario hacer ninguna modificación en el software del cliente para empezar a utilizar Global Accelerator con la aplicación.

Para configurar un acelerador de enrutamiento personalizado, seleccione un extremo de subred VPC. A continuación, defina un rango de puertos de destino al que se asignarán las conexiones entrantes, de modo que el software pueda escuchar en el mismo conjunto de puertos en todas las instancias. Global Accelerator crea una asignación estática que permite que el servicio de emparejamiento traduzca una dirección IP de destino y un número de puerto para una sesión a una dirección IP externa y un puerto que usted proporciona a los usuarios.

La pila de red de su aplicación puede funcionar a través de un único protocolo de transporte, o puede usar UDP para una entrega rápida y TCP para una entrega confiable. Puede establecer UDP, TCP o ambos UDP y TCP para cada rango de puertos de destino, para brindarle la máxima flexibilidad sin tener que duplicar la configuración para cada protocolo.

> **Note**
>
> De forma predeterminada, todos los destinos de subred de VPC en un acelerador de enrutamiento personalizado no pueden recibir tráfico. Esto debe ser seguro de forma predeterminada y también para proporcionarle un control granular sobre qué destinos de instancia privada de EC2 de su subred pueden recibir tráfico. Puede permitir o denegar el tráfico a la subred, o a combinaciones específicas de direcciones IP y puertos (sockets de destino). Para obtener más información, consulte Agregar, editar o quitar un extremo de subred VPC. También puede especificar destinos mediante la API Global Accelerator. Para obtener más información, consultePermitir CustomRoutingTrafficyDenyCustomRoutingTraffic.

Ejemplo de cómo funciona el enrutamiento personalizado en Global Accelerator

Por ejemplo, supongamos que desea admitir 10.000 sesiones en las que interactúen grupos de usuarios, como sesiones de juegos o sesiones de llamadas VoIP, en 1.000 instancias de Amazon EC2 detrás de Global Accelerator. En este ejemplo, especificaremos un rango de puertos de escucha de 10001—20040 y un rango de puertos de destino de 81—90. Diremos que tenemos las cuatro subredes VPC en us-east-1: subnet-1, subnet-2, subnet-3 y subnet-4.

En nuestra configuración de ejemplo, cada subred de VPC tiene un tamaño de bloque de /24, por lo que puede admitir 251 instancias de Amazon EC2. (Cinco direcciones están reservadas y no están disponibles en cada subred, y estas direcciones no están asignadas). Cada servidor que se ejecuta en cada instancia de EC2 sirve a los siguientes 10 puertos, que especificamos para los puertos de destino en nuestro grupo de endpoints: 81 a 90. Esto significa que tenemos 2510 puertos (10 x 251) asociados a cada subred. Cada puerto se puede asociar a una sesión.

Debido a que hemos especificado 10 puertos de destino en cada instancia de EC2 de nuestra subred, Global Accelerator los asocia internamente con 10 puertos de escucha que puede utilizar para acceder a instancias de EC2. Para ilustrar esto simplemente, diremos que hay un bloque de puertos de escucha que comienza con la primera dirección IP de la subred del extremo para el primer conjunto de 10 y, a continuación, se mueve a la siguiente dirección IP para el siguiente conjunto de 10 puertos de escucha.

> **Note**
>
> En realidad, el mapeo no es predecible como este, pero estamos usando un mapeo secuencial aquí para ayudar a mostrar cómo funciona el mapeo de puertos. Para determinar la asignación real para los rangos de puertos de escucha, utilice las siguientes operaciones de API: ListCustomRoutingPortMappingsyListCustomRoutingPortMappingsByDestination.

En nuestro ejemplo, el primer puerto de escucha es 10001. Ese puerto está asociado con la primera dirección IP de subred, 192.0.2.4, y el primer puerto EC2, 81. El siguiente puerto de escucha, 10002, está asociado con la primera dirección IP de subred, 192.0.2.4, y el segundo puerto EC2, 82. En la tabla siguiente se muestra cómo continúa esta asignación de ejemplo a través de la última dirección IP de la primera subred VPC y, a continuación, a la primera dirección IP de la segunda subred VPC.

Global Accelerator	Subredes de la VPC	Puerto de instancia 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

Global Accelerator	Subredes de la VPC	Puerto de instancia 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

Global Accelerator	Subredes de la VPC	Puerto de instancia EC2
12519	192.0.3.4	89
12520	192.0.3.4	90

Directrices y restricciones para aceleradores de enrutamiento personalizados

Cuando cree aceleradores de enrutamiento personalizados y trabaje con ellos en el AWS Global Accelerator, tenga en cuenta las siguientes directrices y restricciones.

Destinos de la instancia de Amazon EC2

- Los puntos de enlace de subred de nube virtual pública (VPC) de un acelerador de direccionamiento personalizado solo pueden incluir instancias EC2. No se admiten otros recursos, como equilibradores de carga, para el acelerador de enrutamiento personalizado.
- Los tipos de instancias EC2 compatibles con Global Accelerator se enumeran enPuntos finales para aceleradores estándar en el AWS Global Accelerator.

Asignaciones de puertos

- Al agregar una subred VPC, Global Accelerator crea una asignación de puertos estáticos de rangos de puertos de escucha a los rangos de puertos admitidos por la subred. La asignación de puertos para una subred específica nunca cambia.
- Puede ver la lista de mapeos de puertos de un acelerador de direccionamiento personalizado mediante programación. Para obtener más información, consulte `ListCustomRoutingPortMappings`.

Tamaño de subred de VPC

- Las subredes VPC que agregue a un acelerador de enrutamiento personalizado deben tener un mínimo de /28 y un máximo de /17.

Rangos de puertos de escucha

- Debe especificar suficientes puertos de listener, especificando rangos de puertos de listener, para acomodar el número de destinos incluidos en las subredes que planea agregar al acelerador

de enrutamiento personalizado. El rango que especifique al crear un listener determina cuántas combinaciones de puertos de escucha y direcciones IP de destino se pueden utilizar con el acelerador de enrutamiento personalizado. Para obtener la máxima flexibilidad y reducir la posibilidad de que se produzca un error que no tenga suficientes puertos de escucha disponibles, le recomendamos que especifique un rango de puertos grande.

Global Accelerator asigna rangos de puertos en bloques cuando se agrega una subred a un acelerador de enrutamiento personalizado. Se recomienda asignar rangos de puertos de escucha linealmente y hacer que los rangos sean lo suficientemente grandes como para admitir el número de puertos de destino que desea tener. Es decir, el número de puertos que debe asignar debe ser al menos el tamaño de subred por el número de puertos y protocolos de destino (configuraciones de destino) que tendrá en la subred.

> **Note**
>
> El algoritmo que Global Accelerator utiliza para asignar asignaciones de puertos puede requerir que agregue más puertos de escucha, más allá de este total.

Después de crear un listener, puede editarlo para agregar rangos de puertos adicionales y protocolos asociados, pero no puede disminuir los rangos de puertos existentes. Por ejemplo, si tiene un rango de puertos de escucha de 5.000 a 10.000, no puede cambiar el rango de puertos a 5900 a 10.000 y no puede cambiar el rango de puertos a 5.000 a 9.900.

Cada intervalo de puertos de escucha debe incluir un mínimo de 16 puertos. Los agentes de escucha admiten los puertos 1-65535.

Rangos de los puertos

Hay dos lugares en los que se especifican rangos de puertos para un acelerador de enrutamiento personalizado: los rangos de puertos que se especifican al agregar un listener y los rangos de puertos de destino y protocolos que se especifican para un grupo de extremos.

- Rangos de los puertos de escucha: Los puertos de escucha en las direcciones IP estáticas del Acelerador global a las que se conectan sus clientes. Global Accelerator asigna cada puerto a una dirección IP de destino única y un puerto en una subred VPC detrás del acelerador.
- Rangos de puertos de destino Los conjuntos de rangos de puertos de destino que especifique para un grupo de extremos (también denominados configuraciones de destino) son los puertos de instancia de EC2 que reciben tráfico. Para recibir tráfico en los puertos de destino, los grupos de seguridad asociados con las instancias de EC2 deben permitir el tráfico en ellos.

Comprobaciones de Health y conmutación por error

Global Accelerator no realiza comprobaciones de estado para aceleradores de enrutamiento personalizados y no realiza failover a endpoints en buen estado. El tráfico de los aceleradores de enrutamiento personalizados se enruta determinísticamente, independientemente del estado de un recurso de destino.

Todo el tráfico se deniega de forma predeterminada

De forma predeterminada, el tráfico dirigido a través de un acelerador de enrutamiento personalizado se deniega a todos los destinos de la subred. Para permitir que las instancias de destino reciban tráfico, debe permitir específicamente todo el tráfico a la subred o, alternativamente, permitir el tráfico a direcciones IP de instancia específicas y puertos de la subred.

Actualizar una subred o un destino específico para permitir o denegar el tráfico lleva tiempo propagarse a través de Internet. Para determinar si un cambio se ha propagado, puede llamar al método`DescribeCustomRoutingAccelerator`Acción de API para comprobar el estado del acelerador. Para obtener más información, consulteDescribeCustomRoutingAccelerator.

AWS CloudFormation no es compatible

AWS CloudFormation no es compatible con los aceleradores de enrutamiento personalizados.

Aceleradores de enrutamiento personalizados en el AWS Global Accelerator

APersonalizado del acelerador deen AWS Global Accelerator le permite utilizar la lógica de aplicación personalizada para dirigir a uno o más usuarios a un destino específico entre muchos destinos, mientras utiliza la red global de AWS para mejorar la disponibilidad y el rendimiento de la aplicación.

Un acelerador de enrutamiento personalizado enruta el tráfico sólo a puertos de instancias de Amazon EC2 que se ejecutan en subredes de nube privada virtual (VPC). Con un acelerador de enrutamiento personalizado, Global Accelerator no enruta el tráfico según la geoproximidad o el estado del endpoint. Para obtener más información, consulte Cómo funcionan los aceleradores de enrutamiento personalizados en AWS Global Accelerator.

Al crear un acelerador, de forma predeterminada, Global Accelerator le proporciona un conjunto de dos direcciones IP estáticas. Si transporta su propio rango de direcciones IP a AWS (BYOIP), en

su lugar puede asignar direcciones IP estáticas de su propio grupo para usarlas con su acelerador. Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en el AWS Global Accelerator.

> **Important**
>
> Las direcciones IP se asignan al acelerador durante el tiempo que exista, incluso si deshabilita el acelerador y ya no acepta ni enruta el tráfico. Sin embargo, cuandodeleteun acelerador, pierde las direcciones IP estáticas del acelerador global que están asignadas al acelerador, por lo que ya no puede enrutar el tráfico usándolas. Como práctica recomendada, asegúrese de que dispone de permisos para evitar eliminar aceleradores inadvertidamente. Puede utilizar directivas de IAM como permisos basados en etiquetas con Global Accelerator para limitar los usuarios que tienen permisos para eliminar un acelerador. Para obtener más información, consulte Políticas basadas en etiquetas.

En esta sección se explica cómo crear, editar o eliminar un acelerador de enrutamiento personalizado en la consola de Global Accelerator. Para obtener más información sobre el uso de operaciones de API con Global Accelerator, consulte laReferencia de la API de AWS Global Accelerator.

Temas

- Creación o actualización de un acelerador de direccionamiento personalizado
- Visualización de los aceleradores de enrutamiento personalizados
- Eliminación de un acelerador de enrutamiento personalizado

Creación o actualización de un acelerador de direccionamiento personalizado

Para crear un acelerador de direccionamiento personalizado

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. SeleccionarCrear acelerador.
3. Proporcione un nombre para su acelerador.
4. ParaTipo de aceleradorEn, seleccioneEnvío personalizado.

5. Opcionalmente, si ha traído su propio rango de direcciones IP a AWS (BYOIP), puede especificar direcciones IP estáticas para el acelerador desde ese grupo de direcciones. Haga esta elección para cada una de las dos direcciones IP estáticas de su acelerador.

   - Para cada dirección IP estática, elija el grupo de direcciones IP que desea utilizar.
   - Si ha elegido su propio grupo de direcciones IP, elija también una dirección IP específica del grupo. Si elige el grupo de direcciones IP predeterminado de Amazon, Global Accelerator asigna una dirección IP específica a su acelerador.

6. Si lo desea, añada una o varias etiquetas para ayudarle a identificar los recursos del acelerador.
7. SeleccionarSiguientepara ir a las siguientes páginas del asistente para agregar listeners, grupos de endpoints y endpoints de subred VPC.

Para editar un acelerador de direccionamiento personalizado

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la lista de aceleradores de enrutamiento personalizados, elija uno y, a continuación, elijaEditar.
3. En la páginaEdición del acelerador deHaga los cambios que desee. Por ejemplo, puede desactivar el acelerador para poder eliminarlo.
4. Elija Save (Guardar).

Visualización de los aceleradores de enrutamiento personalizados

Puede ver información acerca de sus aceleradores de direccionamiento personalizados en la consola. Para ver las descripciones de los aceleradores de enrutamiento personalizados mediante programación, consulteListCustomRoutingAcceleratoryDescribeCustomRoutingAcceleratorEn la Referencia de la API de AWS Global Accelerator.

Para ver la información de los aceleradores de enrutamiento personalizados

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. Para ver detalles acerca de un acelerador, elija un acelerador y luego elijaVista.

Eliminación de un acelerador de enrutamiento personalizado

Si ha creado un acelerador de enrutamiento personalizado como prueba, o si ya no utiliza un acelerador, puede eliminarlo. En la consola, deshabilite el acelerador y luego puede eliminarlo. No es necesario eliminar los oyentes y los grupos de puntos finales del acelerador.

Para eliminar un acelerador de enrutamiento personalizado mediante una operación de API en lugar de la consola, primero debe quitar todos los listeners y grupos de extremos asociados al acelerador y, a continuación, deshabilitarlo. Para obtener más información, consulte laDeleteAcceleratorEn laReferencia de la API de AWS Global Accelerator.

Para deshabilitar un acelerador de direccionamiento personalizado

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la lista, elija un acelerador que desee deshabilitar.
3. Elija Edit (Editar).
4. SeleccionarDeshabilitar aceleradorHaga clic en y luego enSave (Guardar).

Para eliminar un acelerador de direccionamiento personalizado

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la lista, elija un acelerador que desee eliminar.
3. Elija Eliminar.

> **Note**
>
> Si aún no ha desactivado el acelerador,EliminarNo está disponible. Para deshabilitar el acelerador, consulte el procedimiento anterior.

4. En el cuadro de diálogo de confirmación, elija Delete (Eliminar).

> **Important**
>
> Cuando elimina un acelerador, pierde las direcciones IP estáticas asignadas al acelerador, por lo que ya no puede enrutar el tráfico usándolas.

Listeners para aceleradores de enrutamiento personalizados en el AWS Global Accelerator

Para un acelerador de enrutamiento personalizado en el AWS Global Accelerator, debe configurar un listener que especifique un rango de puertos de escucha con protocolos asociados que Global Accelerator asigna a instancias específicas de Amazon EC2 de destino en los extremos de subred de VPC. Al agregar un extremo de subred de VPC, Global Accelerator crea una asignación de puertos estáticos entre los rangos de puertos que se definen para el listener y las direcciones IP de destino y los puertos de la subred. A continuación, puede utilizar la asignación de puertos para especificar las direcciones IP estáticas del acelerador junto con un puerto y un protocolo de escucha para dirigir el tráfico del usuario a direcciones IP de instancia de Amazon EC2 de destino específico y puertos de la subred de la VPC.

Los agentes de escucha se definen cuando se crea el acelerador de direccionamiento personalizado, pero se pueden agregar otros agentes de escucha en cualquier momento. Cada oyente puede tener uno o más grupos de endpoints, uno para cada región de AWS en la que tenga endpoints de subred de VPC. Un agente de escucha en un acelerador de enrutamiento personalizado admite protocolos TCP y UDP. Especifique el protocolo o protocolos para cada rango de puertos de destino que defina: UDP, TCP o UDP y TCP.

Para obtener más información, consulte Cómo funcionan los aceleradores de enrutamiento personalizados en AWS Global Accelerator.

Agregar, editar o quitar un agente de escucha de enrutamiento personalizado

En esta sección se explica cómo trabajar con agentes de escucha de direccionamiento personalizados en la consola de AWS Global Accelerator. Para obtener más información sobre el uso de las operaciones de API con AWS Global Accelerator, consulte laReferencia de la API de AWS Global Accelerator.

Para agregar un agente de escucha de un acelerador de direccionamiento personalizado

El rango que especifica al crear un listener define cuántas combinaciones de puertos de escucha y direcciones IP de destino se pueden utilizar con el acelerador de enrutamiento personalizado. Para obtener la máxima flexibilidad, le recomendamos que especifique un rango de puertos de gran tamaño. Cada rango de puertos de escucha que especifique debe incluir un mínimo de 16 puertos.

> **Note**
>
> Después de crear un listener, puede editarlo para agregar rangos de puertos adicionales y protocolos asociados, pero no puede disminuir los rangos de puertos existentes.

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradoresElija un acelerador de direccionamiento personalizado.
3. Elija Add listener (Añadir agente de escucha).
4. En la páginaAgregar agente de escuchaIntroduzca el rango de puertos de agente de escucha que desee asociar con el acelerador.

   Los agentes de escucha admiten los puertos 1-65535. Para obtener la máxima flexibilidad con un acelerador de enrutamiento personalizado, se recomienda especificar un rango de puertos grande.
5. Elija Add listener (Añadir agente de escucha).

Para editar un agente de escucha de un acelerador de direccionamiento personalizado

Cuando edite un listener para un acelerador de enrutamiento personalizado, tenga en cuenta que puede agregar rangos de puertos adicionales y protocolos asociados, aumentar rangos de puertos existentes o cambiar protocolos, pero no puede disminuir los rangos de puertos existentes.

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradoresElija un acelerador.
3. Elija un oyente y, a continuación, elijaEditar agente de escucha.
4. En la páginaEditar agente de escucha, realice los cambios que desee en los rangos de puertos o protocolos existentes o agregue nuevos rangos de puertos.

   Tenga en cuenta que no puede disminuir el rango de un rango de puertos existente.
5. Elija Save (Guardar).

Para quitar un agente de escucha

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradoresElija un acelerador.

3. Elija un oyente y, a continuación, elijaRemove.
4. En el cuadro de diálogo de confirmación, elijaRemove.

Grupos de endpoints para aceleradores de enrutamiento personalizados en AWS Global Accelerator

Con un acelerador de enrutamiento personalizado en el AWS Global Accelerator, un grupo de puntos finales define los puertos y protocolos a los que se destinan las instancias de Amazon EC2 en las subredes de nube privada virtual (VPC) que aceptan tráfico en.

Cree un grupo de endpoints para el acelerador de enrutamiento personalizado para cada región de AWS en la que se encuentran las subredes de VPC y las instancias de EC2. Cada grupo de endpoints de un acelerador de enrutamiento personalizado puede tener varios extremos de subred VPC. Del mismo modo, puede agregar cada VPC a varios grupos de endpoints, pero los grupos de endpoints deben estar asociados a distintos oyentes.

Para cada grupo de endpoints, especifique un conjunto de uno o más rangos de puertos que incluyen los puertos a los que desea dirigir el tráfico en las instancias de EC2 de la Región. Para cada rango de puertos de grupo de extremos, especifique el protocolo que se va a utilizar: UDP, TCP o UDP y TCP. Esto le proporciona la máxima flexibilidad, sin tener que duplicar conjuntos de rangos de puertos para cada protocolo. Por ejemplo, puede tener un servidor de juegos con tráfico de juegos corriendo a través de UDP en los puertos 8080-8090, mientras que también tiene un servidor que escucha mensajes de chat a través de TCP en el puerto 80.

Para obtener más información, consulte Cómo funcionan los aceleradores de enrutamiento personalizados en AWS Global Accelerator.

Añadir, editar o quitar un grupo de puntos de enlace de un acelerador de direccionamiento personalizado

Trabaja con un grupo de endpoints para su acelerador de enrutamiento personalizado en la consola de AWS Global Accelerator o mediante una operación de API. Puede agregar o quitar puntos de enlace de subred de VPC de un grupo de puntos de enlace en cualquier momento.

En esta sección se explica cómo trabajar con grupos de endpoints para el acelerador de enrutamiento personalizado en la consola de AWS Global Accelerator. Para obtener más información sobre el uso de operaciones de API con Global Accelerator, consulte laReferencia de AWS Global Accelerator.

Para agregar un grupo de puntos de enlace de un acelerador de direccionamiento personalizado

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradoresElija un acelerador de direccionamiento personalizado.
3. En el navegadorAgentes de escuchasección, paraID del agente de escuchaElija el ID del agente de escucha al que desee agregar un grupo de puntos de enlace.
4. SeleccionarAñadir grupo de puntos de enlace.
5. En la sección de un listener, especifique una región para el grupo de extremos.
6. ParaConjuntos de puertos y protocolos, introduzca rangos de puertos y protocolos para sus instancias de Amazon EC2.

   - Introduzca unDesde el puertoy aAl puertoPara especificar un intervalo de puertos.
   - Para cada intervalo de puertos, especifique el protocolo o protocolos para ese rango.

   El rango de puertos no tiene que ser un subconjunto del rango de puertos de escucha, pero debe haber suficientes puertos totales en el rango de puertos del listener para admitir el número total de puertos que especifique para los grupos de extremos en el acelerador de enrutamiento personalizado.
7. Elija Save (Guardar).
8. También puede seleccionarAñadir grupo de puntos de enlaceAñadir grupos de puntos de enlace adicionales para este agente de escucha. También puede elegir otro oyente y agregar grupos de extremos.
9. SeleccionarAñadir grupo de puntos de enlace.

Para editar un grupo de puntos de enlace de un acelerador de direccionamiento personalizado

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradoresElija un acelerador de direccionamiento personalizado.
3. En el navegadorAgentes de escuchasección, paraID del agente de escuchaElija el ID del agente de escucha al que está asociado el grupo de puntos de enlace.
4. SeleccionarEditar grupo de puntos de enlace.
5. En la páginaEditar grupo de puntos de enlace, cambie la región, el rango de puertos o el protocolo de un rango de puertos.
6. Elija Save (Guardar).

Para quitar un acelerador de direccionamiento personalizado

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradoresElija un acelerador.
3. En el navegadorAgentes de escuchaElija un agente de escucha y, a continuación, elijaRemove.
4. En el navegadorGrupos de puntos de enlaceElija un grupo de puntos de enlace y, a continuación, elijaRemove.
5. En el cuadro de diálogo de confirmación, elijaRemove.

Extremos de subred VPC para aceleradores de enrutamiento personalizados en AWS Global Accelerator

Los puntos finales para los aceleradores de enrutamiento personalizados son subredes de nube privada virtual (VPC) que pueden recibir tráfico a través de un acelerador. Cada subred puede contener uno o varios destinos de instancias de Amazon EC2. Al agregar un extremo de subred, Global Accelerator genera una nueva asignación de puertos. A continuación, puede utilizar la API Global Accelerator para obtener una lista estática de todas las asignaciones de puertos para la subred, que puede utilizar para enrutar el tráfico a las direcciones IP de la instancia EC2 de destino en la subred. Para obtener más información, consulteListCustomRoutingPortMappings.

Sólo puede dirigir el tráfico a instancias de EC2 en las subredes, no a otros recursos como equilibradores de carga (a diferencia de los aceleradores estándar). Los tipos de instancia de EC2 admitidos se enumeran enPuntos finales para aceleradores estándar en el AWS Global Accelerator.

Para obtener más información, consulte Cómo funcionan los aceleradores de enrutamiento personalizados en AWS Global Accelerator.

Tenga en cuenta lo siguiente al agregar subredes VPC para el acelerador de enrutamiento personalizado:

- De forma predeterminada, el tráfico dirigido a través de un acelerador de enrutamiento personalizado no puede llegar a ningún destino de la subred. Para permitir que las instancias de destino reciban tráfico, debe optar por permitir todo el tráfico a la subred o, alternativamente, habilitar el tráfico a direcciones IP de instancia específicas y puertos (sockets de destino) en la subred.

> **Important**
>
> Actualizar una subred o un destino específico para permitir o denegar el tráfico lleva tiempo propagarse a través de Internet. Para determinar si un cambio se ha propagado, puede llamar al método`DescribeCustomRoutingAccelerator`Acción de API para comprobar el estado del acelerador. Para obtener más información, consulte[DescribeCustomRoutingAccelerator](#).

- Dado que las subredes de VPC conservan la dirección IP del cliente, debe revisar la información de configuración y seguridad relevante al agregar subredes como puntos finales para aceleradores de enrutamiento personalizados. Para obtener más información, consulte [Agregar puntos finales con preservación de direcciones IP del cliente](#).

Agregar, editar o quitar un extremo de subred VPC

Agregue extremos de subred de nube privada virtual (VPC) a grupos de endpoints en sus aceleradores de enrutamiento personalizados para que pueda dirigir el tráfico del usuario a las instancias de Amazon EC2 de destino en la subred.

Cuando agrega y quita instancias EC2 de la subred, o habilita o deshabilita el tráfico a destinos EC2, cambia si esos destinos pueden recibir tráfico. Sin embargo, la asignación de puertos del Acelerador Global no cambia.

Para permitir el tráfico a algunos destinos de la subred, pero no a todos, introduzca direcciones IP para cada instancia de EC2 que desee permitir, junto con los puertos de la instancia que desea recibir tráfico. Las direcciones IP que especifique deben ser para instancias EC2 en la subred. Puede especificar un puerto o intervalo de puertos, desde los puertos asignados para la subred.

Puede quitar la subred VPC del acelerador quitándola de un grupo de extremos. La eliminación de una subred no afecta a la propia subred, pero Global Accelerator ya no puede dirigir el tráfico a la subred o a las instancias de Amazon EC2 que contiene. Además, Global Accelerator recuperará la asignación de puertos para la subred VPC para utilizarlos potencialmente para las nuevas subredes que agregue.

En los pasos de esta sección se explica cómo agregar, editar o eliminar puntos de enlace de subred de VPC en la consola de AWS Global Accelerator. Para obtener más información sobre el uso de las operaciones de API con AWS Global Accelerator, consulte la[Referencia de API AWS Global Accelerator](#).

Para agregar un extremo de subred de VPC

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores, elija un acelerador de direccionamiento personalizado.
3. En el navegadorAgentes de escuchasección, paraID del agente de escucha, elija el ID de un oyente.
4. En el navegadorGrupos de punto de enlacesección, paraID del grupo de puntos de enlace, elija el ID del grupo de endpoints (región de AWS) al que desea agregar el extremo de subred de VPC.
5. En el navegadorPuntos de enlace de, elijaAgregar punto de enlace.
6. En la páginaAgregar puntos finalespágina, paraPunto de enlace, elija una subred VPC.

   Si no dispone de ninguna VPC, no hay elementos en la lista. Para continuar, agregue al menos una VPC, vuelva a los pasos aquí indicados y elija una VPC de la lista.
7. Para el extremo de subred VPC que agregue, puede optar por permitir o denegar el tráfico a todos los destinos de la subred, o bien permitir el tráfico sólo a instancias y puertos de EC2 específicos. El valor predeterminado es denegar el tráfico a todos los destinos de la subred.
8. Seleccione Add endpoint (Añadir punto de enlace).

Para permitir o denegar el tráfico a destinos específicos

Puede editar la asignación de puertos de subred de VPC para un extremo para permitir o denegar el tráfico a instancias y puertos EC2 específicos (sockets de destino) de una subred.

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores, elija un acelerador de direccionamiento personalizado.
3. En el navegadorAgentes de escuchasección, paraID del agente de escucha, elija el ID de un oyente.
4. En el navegadorGrupos de punto de enlacesección, paraID del grupo de puntos de enlace, elija el ID del grupo de endpoints (región de AWS) del extremo de subred de VPC que desea editar.
5. Seleccione una subred de punto de enlace y, a continuación, elijaView details (Ver detalles)..
6. En la páginaPunto de enlacepágina, enAsignaciones de puertos, elija una dirección IP y, a continuación, elijaEditar.
7. Introduzca los puertos para los que desea habilitar el tráfico y, a continuación, elijaPermitir estos destinos.

Para permitir o denegar TODO el tráfico a una subred

Puede actualizar un endpoint para permitir o denegar el tráfico a todos los destinos de la subred VPC.

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores, elija un acelerador de direccionamiento personalizado.
3. En el navegadorAgentes de escuchasección, paraID del agente de escucha, elija el ID de un oyente.
4. En el navegadorGrupos de punto de enlacesección, paraID del grupo de puntos de enlace, elija el ID del grupo de endpoints (región de AWS) del extremo de subred de VPC que desea actualizar.
5. SeleccionarPermitir/Denegar todo el tráfico.
6. Elija una opción para permitir todo el tráfico o denegar todo el tráfico y, a continuación, elijaSave (Guardar).

Para eliminar un punto de enlace

1. Abra la consola Global Accelerator enhttps://console.aws.amazon.com/globalaccelerator/home.
2. En la páginaAceleradores, elija un acelerador de direccionamiento personalizado.
3. En el navegadorAgentes de escuchasección, paraID del agente de escucha, elija el ID de un oyente.
4. En el navegadorGrupos de punto de enlacesección, paraID del grupo de puntos de enlace, elija el ID del grupo de endpoints (región de AWS) del extremo de subred de VPC que desea eliminar.
5. SeleccionarEliminar punto final.
6. En el cuadro de diálogo de confirmación, elijaRemove.

Direccionamiento DNS y dominios personalizados en AWS Global Accelerator

En este capítulo se explica cómo AWS Global Accelerator realiza el enrutamiento DNS e incluye información sobre el uso de un dominio personalizado con Global Accelerator.

Temas

Support con el direccionamiento DNS en Global Accelerator

Al crear un enrutamiento personalizado o un acelerador estándar, Global Accelerator aprovisiona dos direcciones IP estáticas. También asigna un nombre predeterminado del sistema de nombres de dominio (DNS), similar `aa1234567890abcdef.awsglobalaccelerator.com`, que apunta a las direcciones IP estáticas. Las direcciones IP estáticas se anuncian globalmente utilizando anycast desde la red perimetral de AWS hasta sus endpoints. Puede usar las direcciones IP estáticas del acelerador o el nombre DNS para enrutar el tráfico hacia el acelerador. Los servidores DNS y los solucionadores DNS utilizan un round robin para resolver el nombre DNS de un acelerador, de modo que el nombre se resuelve en las direcciones IP estáticas del acelerador, devueltas por Amazon Route 53 en orden aleatorio. Los clientes suelen usar la primera dirección IP que se devuelve.

> **Note**
>
> Global Accelerator crea dos registros de puntero (PTR) que asignan las direcciones IP estáticas de un acelerador al nombre DNS correspondiente generado por Global Accelerator, para admitir búsquedas DNS inversas. Esto es lo que también se conoce como zona alojada inversa. Tenga en cuenta que el nombre DNS que Global Accelerator genera para usted no es configurable y no puede crear registros PTR que apunten a su nombre de dominio personalizado. Global Accelerator tampoco crea registros PTR para direcciones IP estáticas desde un rango de direcciones IP que lleva a AWS (BYOIP).

Enrutar el tráfico de dominio personalizado al acelerador

En la mayoría de los escenarios, puede configurar DNS para que use su nombre de dominio personalizado (como`www.example.com`) con el acelerador, en lugar de usar las direcciones IP estáticas asignadas o el nombre DNS predeterminado. En primer lugar, con Amazon Route 53 u otro proveedor DNS, cree un nombre de dominio y, a continuación, agregue o actualice registros DNS con sus direcciones IP del acelerador global. O puede asociar su nombre de dominio personalizado con el nombre DNS del acelerador. Complete la configuración DNS y espere a que los cambios se propaguen a través de Internet. Ahora cuando un cliente realiza una solicitud utilizando su nombre de dominio personalizado, el servidor DNS lo resuelve para hallar las direcciones IP, en orden aleatorio, o para hallar el nombre de DNS del acelerador.

Para utilizar el nombre de dominio personalizado con Global Accelerator cuando utilice Route 53 como servicio DNS, cree un registro de alias que señale el nombre de dominio personalizado al nombre DNS asignado al acelerador. Un registro de alias es una extensión de Route 53 para DNS. Es similar a un registro CNAME, pero puede crear un registro de alias tanto para el dominio raíz, por ejemplo, por ejemplo,`example.com`, y para subdominios, como`www.example.com`. Para obtener más información, consulteElección entre registros de alias y sin aliasEn la Guía para desarrolladores de Amazon Route 53.

Para configurar Route 53 con un registro de alias para un acelerador, siga las instrucciones incluidas en el tema siguiente: Alias TargetEn la Guía para desarrolladores de Amazon Route 53. Para ver la información de Global Accelerator, desplácese hacia abajo en elAlias Target(Se ha creado el certificado).

Traiga sus propias direcciones IP (BYOIP) en el AWS Global Accelerator

AWS Global Accelerator utiliza direcciones IP estáticas como puntos de entrada para sus aceleradores. Estas direcciones IP se distribuyen desde ubicaciones de borde de AWS. De forma predeterminada, Global Accelerator proporciona direcciones IP estáticas desde elGrupo de direcciones IP de Amazon. En lugar de utilizar las direcciones IP que proporciona Global Accelerator, puede configurar estos puntos de entrada para que sean direcciones IPv4 de sus propios rangos de direcciones. En este tema se explica cómo utilizar sus propios intervalos de direcciones IP con el Acelerador Global.

Puede traer parte o todo su intervalo de direcciones IPv4 públicas de su red local a su cuenta de AWS para utilizarlo con el acelerador global. Sigue siendo el propietario de los rangos de direcciones pero AWS los anuncia en Internet.

No puede utilizar las direcciones IP que trae a AWS para un servicio AWS con otro servicio. En los pasos de este capítulo se describe cómo traer su propio intervalo de direcciones IP para su uso solo en el AWS Global Accelerator. Para obtener información sobre los pasos necesarios para traer su propio intervalo de direcciones IP para su uso en Amazon EC2, consulteTraiga sus propias direcciones IP (del inglés BYOIP)En la Guía del usuario de Amazon EC2.

> **Important**
>
> Debe dejar de anunciar su intervalo de direcciones IP desde otras ubicaciones antes de anunciarlo a través de AWS. Si un intervalo de direcciones IP es multihomed (es decir, el rango es anunciado por varios proveedores de servicios al mismo tiempo), no podemos garantizar que el tráfico al rango de direcciones ingrese a nuestra red o que su flujo de trabajo publicitario BYOIP se complete correctamente.

Una vez que traiga su gama de direcciones a AWS, aparecerá en su cuenta como un grupo de direcciones. Cuando crea un acelerador, puede asignarle una dirección IP de su rango. Global Accelerator le asigna una segunda dirección IP estática desde un rango de direcciones IP de Amazon. Si trae dos rangos de direcciones IP a AWS, puede asignar una dirección IP de cada rango al acelerador. Esta restricción se debe a que Global Accelerator asigna cada rango de direcciones a una zona de red diferente, para una alta disponibilidad.

Para utilizar su propio intervalo de direcciones IP con Global Accelerator, revise los requisitos y, a continuación, siga los pasos que se indican en este tema.

Temas

Requirements

Puede incluir hasta dos rangos de direcciones IP aptos para el AWS Global Accelerator por cuenta de AWS.

Para obtener información sobre el valor de, su intervalo de direcciones IP debe cumplir los siguientes requisitos:

- El rango de direcciones IP debe estar registrado con uno de los siguientes registros regionales de Internet (RIR, por sus siglas en inglés): el Registro Americano de Números de Internet (ARIN, por sus siglas en inglés), el Centro de Coordinación de Redes IP Europeas (RIPE, por sus siglas en francés) o el Centro de Información de Red de Asia y el Pacífico (APNIC, por sus siglas en inglés). El rango de direcciones debe estar registrado en una empresa o entidad institucional. No se puede registrar a nombre de un individuo.
- El rango de direcciones más específico que puede traer es /24. Los primeros 24 bits de la dirección IP especifican el número de red. Por ejemplo, 198.51.100 es el número de red para la dirección IP 198.51.100.0.
- Las direcciones IP del rango de direcciones deben tener un historial limpio. Es decir, no pueden tener una mala reputación o estar asociados con un comportamiento malicioso. Nos reservamos el derecho de rechazar el intervalo de direcciones IP si investigamos la reputación del intervalo de direcciones IP y descubrimos que contiene una dirección IP que no tiene un historial limpio.

Además, requerimos los siguientes tipos o estados de red de asignación y asignación, dependiendo del lugar en el que registró su intervalo de direcciones IP:

- ARIN:`Direct Allocation`y`Direct Assignment`Tipos de red
- MADURO:`ALLOCATED PA`,`LEGACY`, y`ASSIGNED PI`Estados de asignación
- APNIC:`ALLOCATED PORTABLE`y`ASSIGNED PORTABLE`Estados de asignación

Prepárese para traer su rango de direcciones IP a su cuenta de AWS: Autorización

Para asegurarnos de que solo tú puedes llevar tu espacio de direcciones IP a Amazon, necesitamos dos autorizaciones:

- Debes autorizar a Amazon a anunciar el intervalo de direcciones IP.

- Debe proporcionar pruebas de que es propietario del intervalo de direcciones IP y, por tanto, tener la autoridad para llevarlo a AWS.

> **Note**
>
> Cuando utiliza BYOIP para llevar un rango de direcciones IP a AWS, no puede transferir la propiedad de ese rango de direcciones a otra cuenta o empresa mientras lo anunciamos. Tampoco puede transferir directamente un rango de direcciones IP de una cuenta de AWS a otra cuenta. Para transferir la propiedad o transferir entre cuentas de AWS, debe desaprovisionar el intervalo de direcciones y, a continuación, el nuevo propietario debe seguir los pasos para agregar el intervalo de direcciones a su cuenta de AWS.

Para autorizar a Amazon a anunciar el intervalo de direcciones IP, proporciona a Amazon un mensaje de autorización firmado. Utilice una autorización de origen de ruta (ROA) para proporcionar esta autorización. Un ROA es una declaración criptográfica sobre los anuncios de ruta que crea a través de su Registro Regional de Internet (RIR, por sus siglas en inglés). Un ROA contiene el intervalo de direcciones IP, los Números de Sistema Autónomo (ASN, por sus siglas en inglés) que pueden anunciar el rango de direcciones IP y una fecha de vencimiento. Un ROA da permiso a Amazon para anunciar un rango de direcciones IP de un Sistema Autónomo (AS, por sus siglas en inglés) específico.

Una ROA no permite que su cuenta de AWS traiga el rango de direcciones IP a AWS. Para proporcionar esta autorización, debe anunciar un certificado X.509 autofirmado en los comentarios del Protocolo de Acceso a Datos de Registro (RDAP, por sus siglas en inglés) para el rango de direcciones IP. El certificado contiene una clave pública que AWS utiliza para verificar la firma del contexto de autorización que proporcionó. Conserve su clave privada en un lugar seguro y utilícela para firmar el mensaje del contexto de autorización.

En las secciones siguientes se proporcionan pasos detallados para completar estas tareas de autorización. Los comandos de estos pasos son compatibles con Linux. Si usa Windows, puede acceder a laWindows Subsystem for Linuxpara ejecutar comandos de Linux.

Pasos para proporcionar autorización

- Paso 1: Cree un objeto ROA
- Paso 2: Cree un certificado autofirmado X.509
- Paso 3: Cree un mensaje de autorización firmada

Paso 1: Cree un objeto ROA

Cree un objeto ROA para permitir que Amazon ASN 16509 anuncie su intervalo de direcciones IP, así como los ASN que cuentan actualmente con autorización para anunciar el rango de direcciones IP. El ROA debe contener la dirección IP /24 que quiera traer a AWS y debe fijar la longitud máxima en /24.

Para obtener más información acerca de la creación de una solicitud de ROA, consulte las secciones siguientes, dependiendo de dónde haya registrado el intervalo de direcciones IP:

- ARIN: ROA Requests
- MADURO: Administración del ROAS
- APNIC: Administración de rutas

Paso 2: Cree un certificado autofirmado X.509

Cree un key pair y un certificado X.509 autofirmado y, a continuación, agregue el certificado al registro de RDAP para su RIR. En los siguientes pasos se describe cómo realizar estas tareas.

> **Note**
>
> Laopensslos comandos de estos pasos requieren la versión 1.0.2 o posterior de OpenSSL.

Para crear y agregar un certificado X.509

1. Genere un key pair RSA de 2048 bits utilizando el siguiente comando.

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

2. Cree un certificado X.509 público a partir del key pair con el siguiente comando.

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

   En este ejemplo, el certificado vence en 365 días, tiempo transcurrido el cual no se puede confiar. Cuando ejecute el comando, asegúrese de establecer la-daysal valor deseado para la caducidad correcta. Cuando se pida otra información, puede aceptar los valores predeterminados.

3. Actualice el registro RDAP para su RIR con el certificado X.509 siguiendo los siguientes pasos, dependiendo de su RIR.

   1. Para ver el certificado, use el siguiente comando.

      ```
      cat publickey.cer
      ```

   2. Agregue el certificado haciendo lo siguiente:

      > **Important**
      >
      > Asegúrese de incluir el`-----BEGIN CERTIFICATE-----`y`-----END CERTIFICATE-----`del certificado.

      - Para ARIN, añada el certificado en la`Public Comments`Para obtener información sobre el rango de direcciones IP.
      - Para RIPE, añada el certificado como un`descr`Para su rango de direcciones IP.
      - Para APNIC, envíe la clave pública por correo electrónico a`helpdesk@apnic.net`Para solicitar que lo añada manualmente al contacto autorizado de APNIC para las direcciones IP,`remarks`El campo de.

Paso 3: Cree un mensaje de autorización firmada

Crea el mensaje de autorización firmado para permitir a Amazon anunciar tu intervalo de direcciones IP.

El formato del mensaje es el siguiente, donde el`YYYYMMDD`fecha es la fecha de caducidad del mensaje.

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

Para crear el mensaje de autorización firmada

1. Cree un mensaje de autorización de texto sin formato y guárdelo en una variable denominada`text_message`, como se muestra en el siguiente ejemplo. Reemplace el número de cuenta de ejemplo, el intervalo de direcciones IP y la fecha de vencimiento por sus propios valores.

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

2. Firma el mensaje de autorización en`text_message`Con el key pair que creó en la sección anterior.
3. Almacene el mensaje en una variable denominada`signed_message`, como se muestra en el siguiente ejemplo.

```
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")
```

Aprovisionar el rango de direcciones para utilizarlo con el AWS Global Accelerator

Al aprovisionar un rango de direcciones para utilizarlo con AWS, está confirmando que es propietario de dicho rango de direcciones y que autoriza que Amazon lo anuncie. Verificaremos que tiene el rango de direcciones.

Debe aprovisionar su rango de direcciones mediante las operaciones de CLI o API de Global Accelerator. Esta funcionalidad no está disponible en la consola de AWS.

Para aprovisionar el rango de direcciones, use la siguienteProvisionByoipCidrEl comando de. La`--cidr-authorization-context`El parámetro utiliza las variables que ha creado en la sección anterior, no el mensaje ROA.

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

A continuación se muestra un ejemplo de aprovisionamiento de un intervalo de direcciones.

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

Aprovisionar un rango de direcciones es una operación asincrónica, por lo que la llamada se devuelve de forma inmediata. Sin embargo, el rango de direcciones no está listo para usar hasta que

su estado cambie de`PENDING_PROVISIONING`De a`READY`. El proceso de aprovisionamiento puede tardar hasta 3 semanas en completarse. Para monitorizar el estado de los intervalos de direcciones aprovisionados, utilice los siguientesListByoipcidrsComando de la :

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

Para ver una lista de los estados de un intervalo de direcciones IP, consulteBIOIPCIDR.

Cuando se aprovisiona el intervalo de direcciones IP, el`State`Devuelta por`list-byoip-cidrs`es`READY`. Por ejemplo:

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

Anunciar el rango de direcciones mediante AWS

Una vez aprovisionado el rango de direcciones, ya se puede anunciar. Debe anunciar el rango de direcciones exacto que ha aprovisionado. No puede anunciar solo una parte del rango de direcciones aprovisionado. Además, debe dejar de anunciar su intervalo de direcciones IP desde otras ubicaciones antes de anunciarlo a través de AWS.

Debe anunciar (o dejar de anunciar) su rango de direcciones mediante las operaciones de CLI o API de Global Accelerator. Esta funcionalidad no está disponible en la consola de AWS.

> **Important**
>
> Asegúrese de que AWS anuncia su rango de direcciones IP antes de utilizar una dirección IP de su grupo con Global Accelerator.

Para anunciar el rango de direcciones, use la siguienteAdvertiseByoIPCIDREl comando de.

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

A continuación se muestra un ejemplo de solicitud de Global Accelerator para anunciar un intervalo de direcciones.

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

Para monitorizar el estado de los intervalos de direcciones anunciados, utilice los siguientesListByoipcidrsEl comando de.

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

Cuando se anuncia el intervalo de direcciones IP, el`State`Devuelta por`list-byoip-cidrs`es`ADVERTISING`. Por ejemplo:

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

Para dejar de anunciar el rango de direcciones, use la siguiente`withdraw-byoip-cidr`El comando de.

> **Important**
>
> Para dejar de anunciar el intervalo de direcciones, primero debe eliminar cualquier acelerador que tenga direcciones IP estáticas asignadas desde el grupo de direcciones. Para eliminar un acelerador mediante la consola o mediante operaciones de API, consulte Eliminación de un acelerador.

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

A continuación se muestra un ejemplo de solicitud de Global Accelerator para retirar un intervalo de direcciones.

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

Desaprovisionar el rango de direcciones

Para dejar de usar su rango de direcciones con AWS, primero debe eliminar los aceleradores que tengan una dirección IP estática asignada del grupo de direcciones y dejar de anunciar su rango de direcciones. Después de completar estos pasos, puede desaprovisionar el intervalo de direcciones.

Debe detener la publicidad y desaprovisionar su rango de direcciones mediante las operaciones de CLI o API de Global Accelerator. Esta funcionalidad no está disponible en la consola de AWS.

Paso 1: Elimine los aceleradores asociados.Para eliminar un acelerador mediante la consola o mediante operaciones de API, consulte Eliminación de un acelerador.

Paso 2. Deje de anunciar el rango de direcciones. Para dejar de anunciar el rango, use el siguiente procedimiento:RetiradoIPCIDREl comando de.

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

Paso 3. Desaprovisionar el rango de direcciones. Para desaprovisionar el rango, utilice la siguienteDesaprovisionamientoIPCIDREl comando de.

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

Cree un acelerador con sus direcciones IP

Ahora puede crear un acelerador con sus direcciones IP. Si ha traído un rango de direcciones a AWS, puede asignar una dirección IP a su acelerador. Si ha traído dos rangos de direcciones, puede asignar una dirección IP de cada rango de direcciones a su acelerador.

Tiene varias opciones para crear un acelerador utilizando sus propias direcciones IP para las direcciones IP estáticas:

- Utilice la consola Global Accelerator para crear un acelerador. Para obtener más información, consulte Creación o actualización de un acelerador estándar y Creación o actualización de un acelerador de direccionamiento personalizado.

- Utilice la API Global Accelerator para crear un acelerador. Para obtener más información, incluidos ejemplos del uso de la CLI, consulteCreateAcceleratoryCreateCustomRoutingAcceleratorEn la Referencia de la API de AWS Global Accelerator.

Conservar las direcciones IP del cliente en el AWS Global Accelerator

Las opciones para conservar y acceder a la dirección IP del cliente para el AWS Global Accelerator dependen de los puntos finales que haya configurado con el acelerador. Existen dos tipos de endpoints que pueden conservar la dirección IP de origen del cliente en los paquetes entrantes: Equilibradores de carga de aplicaciones e instancias de Amazon EC2.

- Cuando se utiliza un Application Load Balancer orientado a Internet como punto final con Global Accelerator, la preservación de la dirección IP del cliente está habilitada de forma predeterminada para los nuevos aceleradores. Esto significa que la dirección IP de origen del cliente original se conserva para los paquetes que llegan al equilibrador de carga. Puede optar por desactivar la opción cuando cree el acelerador o editando el acelerador más tarde.
- Cuando se utiliza un Application Load Balancer interno o una instancia de EC2 con Global Accelerator, el extremo siempre tiene habilitada la preservación de la dirección IP del cliente.

> **Note**
>
> Global Accelerator no admite la preservación de la dirección IP del cliente para los extremos de Network Load Balancer y direcciones IP elásticas.

Al agregar la preservación de direcciones IP de cliente, tenga en cuenta lo siguiente:

- Antes de agregar y comenzar a enrutar el tráfico a los extremos que conservan la dirección IP del cliente, asegúrese de que todas las configuraciones de seguridad necesarias, por ejemplo, grupos de seguridad, se actualizan para incluir la dirección IP del cliente de usuario en las listas de permisos.
- La preservación de la dirección IP del cliente solo se admite en regiones específicas de AWS. Para obtener más información, consulte Regiones de AWS admitidas para la preservación de direcciones IP.

Temas

- Beneficios de la preservación de direcciones IP
- Cómo se conserva la dirección IP del cliente en el AWS Global Accelerator
- Prácticas recomendadas para la conservación de direcciones IP del cliente
- Regiones de AWS admitidas para la preservación de direcciones IP

Cómo habilitar la preservación de la dirección IP del cliente

Al crear un nuevo acelerador, la preservación de la dirección IP del cliente está habilitada, de forma predeterminada, para los extremos admitidos.

Tenga en cuenta lo siguiente:

- Los equilibradores de carga de aplicaciones internos y las instancias EC2 siempre tienen habilitada la preservación de la dirección IP del cliente. No puede deshabilitar la opción para estos puntos de enlace.
- Cuando utiliza la consola de AWS para crear un nuevo acelerador, la opción de conservación de la dirección IP del cliente está habilitada de forma predeterminada para los extremos de Application Load Balancer. Puede deshabilitar la opción en cualquier momento si no desea conservar la dirección IP del cliente para un extremo del Application Load Balancer orientado a Internet.
- Cuando utiliza la CLI de AWS o una acción de API para crear un nuevo acelerador y no especifica la opción para la preservación de direcciones IP del cliente, los extremos de Application Load Balancer con conexión a Internet tienen habilitada la preservación de direcciones IP del cliente de forma predeterminada.
- Global Accelerator no admite la preservación de la dirección IP del cliente para los extremos de Network Load Balancer y direcciones IP elásticas.

En el caso de los aceleradores existentes, puede realizar la transición de los endpoints sin la preservación de la dirección IP del cliente a los endpoints que sí conserven la dirección IP del cliente. Los endpoints existentes de Application Load Balancer se pueden cambiar a nuevos endpoints de Application Load Balancer, y los endpoints de direcciones IP elásticas existentes se pueden cambiar a endpoints de instancia EC2. (Los extremos del Network Load Balancer no admiten la preservación de la dirección IP del cliente.) Para realizar la transición a los nuevos endpoints, le recomendamos que mueva lentamente el tráfico de un endpoint existente a un nuevo endpoint que tenga preservación de la dirección IP del cliente haciendo lo siguiente:

- Para los extremos existentes de Application Load Balancer, agregue primero a Global Accelerator un extremo duplicado de Application Load Balancer que esté dirigido a los mismos backends y, si se trata de un Application Load Balancer con conexión a Internet, habilite la preservación de la dirección IP del cliente para él. A continuación, ajuste los pesos en los puntos finales para mover lentamente el tráfico desde el equilibrador de carga quenotener habilitada la preservación de la dirección IP del cliente para el equilibrador de cargaporPreservación de direcciones IP de cliente.
- Para un extremo de dirección IP elástica existente, puede mover el tráfico a un extremo de instancia EC2 con la preservación de la dirección IP del cliente. En primer lugar, agregue un extremo de instancia EC2 a Global Accelerator y, a continuación, ajuste los pesos de los endpoints para mover lentamente el tráfico desde el extremo de dirección IP elástica al extremo de la instancia EC2.

Para obtener instrucciones paso a paso sobre la transición, consulte Transición de endpoints para utilizar la preservación de direcciones IP del cliente.

Beneficios de la preservación de direcciones IP

Para los endpoints que no tienen habilitada la preservación de direcciones IP del cliente, las direcciones IP utilizadas por el servicio Global Accelerator en la red perimetral reemplazan la dirección IP del usuario solicitante como dirección de origen en los paquetes que llegan. La información de conexión del cliente original, como la dirección IP del cliente y el puerto del cliente, no se conserva a medida que el tráfico viaja a los sistemas detrás de un acelerador. Esto funciona bien para muchas aplicaciones, especialmente aquellas que están disponibles para todos los usuarios, como sitios web públicos.

Sin embargo, para otras aplicaciones es posible que desee acceder a la dirección IP del cliente original mediante el uso de endpoints con la preservación de la dirección IP del cliente. Por ejemplo, cuando tiene la dirección IP del cliente, puede recopilar estadísticas basadas en las direcciones IP del cliente. También puede usar filtros basados en direcciones IP comoGrupos de seguridad en Application Load Balancerspara filtrar el tráfico. Puede aplicar una lógica específica de la dirección IP de un usuario en las aplicaciones que se ejecutan en los servidores de nivel web detrás de ese extremo de Application Load Balancer mediante el`X-Forwarded-For`, que contiene la información original de la dirección IP del cliente. También puede utilizar la preservación de direcciones IP del cliente en las reglas de grupo de seguridad de los grupos de seguridad asociados con el Application Load Balancer. Para obtener más información, consulte Cómo se conserva la dirección IP del cliente en el AWS Global Accelerator. Para los extremos de instancia EC2, se conserva la dirección IP del cliente original.

Para los endpoints que no tienen preservación de la dirección IP del cliente, puede filtrar la dirección IP de origen que utiliza Global Accelerator cuando reenvía tráfico desde el perímetro. Puede ver información acerca de las direcciones IP de origen (que también son direcciones IP de cliente, cuando la preservación de direcciones IP del cliente está habilitada) de los paquetes entrantes revisando los registros de flujo de Global Accelerator. Para obtener más información, consulte Rangos de ubicación y direcciones IP de servidores de borde de Global Accelerator y Registros de flujo en AWS Global Accelerator.

Cómo se conserva la dirección IP del cliente en el AWS Global Accelerator

AWS Global Accelerator conserva la dirección IP de origen del cliente de forma diferente para las instancias de Amazon EC2 y los equilibradores de carga de aplicaciones:

- Para un extremo de instancia EC2, la dirección IP del cliente se conserva para todo el tráfico.
- Para un extremo del Application Load Balancer con preservación de la dirección IP del cliente, Global Accelerator trabaja junto con el Application Load Balancer para proporcionar un`X-Forwarded`Encabezado,`X-Forwarded-For`, que incluye la dirección IP del cliente original para que su nivel web pueda acceder a él.

Las solicitudes y respuestas HTTP utilizan campos de encabezado para enviar información sobre los mensajes HTTP. Los campos de encabezado son pares nombre-valor separados por signos de dos puntos, separados a su vez por un retorno de carro (CR) y un salto de línea (LF). Un conjunto estándar de campos de encabezado HTTP se define en RFC 2616,Encabezados de mensajes. También hay encabezados HTTP no estándar disponibles que se utilizan habitualmente en las aplicaciones. Algunos de los encabezados HTTP no estándar tienen el valor`X-Forwarded`prefijo.

Dado que un Application Load Balancer finaliza las conexiones TCP entrantes y crea nuevas conexiones a los destinos de back-end, no conserva las direcciones IP del cliente hasta el código de destino (como instancias, contenedores o código Lambda). La dirección IP de origen que los destinos ven en el paquete TCP es la dirección IP del Application Load Balancer. Sin embargo, un Application Load Balancer conserva la dirección IP del cliente original eliminándola de la dirección de respuesta del paquete original e insertándola en un encabezado HTTP antes de enviar la solicitud al backend a través de una nueva conexión TCP.

La`X-Forwarded-For`el encabezado de solicitud tiene el siguiente formato:

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

En el siguiente ejemplo se muestra un`X-Forwarded-For`Para un cliente con una dirección IP de 203.0.113.7.

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

Prácticas recomendadas para la conservación de direcciones IP del cliente

Cuando utilice la preservación de direcciones IP del cliente en el AWS Global Accelerator, tenga en cuenta la información y las prácticas recomendadas de esta sección para las interfaces de red elásticas y los grupos de seguridad.

Para admitir la preservación de direcciones IP del cliente, Global Accelerator crea interfaces de red elásticas en su cuenta de AWS, una para cada subred en la que esté presente un endpoint. Una interfaz de red elástica es un componente de red lógico en una VPC que representa una tarjeta de red virtual. Global Accelerator utiliza estas interfaces de red elásticas para enrutar el tráfico a los endpoints configurados detrás de un acelerador. Los extremos admitidos para enrutar el tráfico de esta manera son los equilibradores de carga de aplicaciones (internos y orientados a Internet) y las instancias de Amazon EC2.

> **Note**
>
> Cuando se agrega un Application Load Balancer interno o un extremo de instancia EC2 en Global Accelerator, se habilita el tráfico de Internet para que fluya directamente hacia y desde el extremo en las nubes privadas virtuales (VPC) dirigiéndolo a una subred privada. Para obtener más información, consulte Conexiones VPC seguras en AWS Global Accelerator.

Cómo utiliza Global Accelerator las interfaces de red elásticas

Cuando tiene un Application Load Balancer con la preservación de direcciones IP del cliente habilitada, el número de subredes en las que se encuentra el equilibrador de carga determina el número de interfaces de red elásticas que Global Accelerator crea en su cuenta. Global Accelerator crea una elastic network interface para cada subred que tiene al menos una elastic network interface del Application Load Balancer que está enfrente de un acelerador en su cuenta.

Los siguientes ejemplos ilustran cómo funciona:

- Ejemplo 1: Si un Application Load Balancer tiene interfaces de red elásticas en la subred A y la subred B y, a continuación, agrega el equilibrador de carga como punto final del acelerador, Global Accelerator crea dos interfaces de red elásticas, una en cada subred.
- Ejemplo 2: Si agrega, por ejemplo, un ALB1 que tiene interfaces de red elásticas en SubNetA y SubnetB a Accelerator1 y, a continuación, agrega un ALB2 con interfaces de red elásticas en la subred A y la subred B a Accelerator2, Global Accelerator crea sólo dos interfaces de red elásticas: una en SubNetA y otra en la subnetB.
- Ejemplo 3: Si agrega un ALB1 que tiene interfaces de red elásticas en SubNetA y SubnetB a Accelerator1 y, a continuación, agrega un ALB2 con interfaces de red elásticas en SubNetA y SubNetC a Accelerator2, Global Accelerator crea tres interfaces de red elásticas: una en SubNetA, una en SubnetB y otra en SubNetC. La elastic network interface de SubNetA ofrece tráfico activado para Accelerator1 y Accelerator2.

Como se muestra en el ejemplo 3, las interfaces de red elásticas se reutilizan en los aceleradores si los extremos de la misma subred se colocan detrás de varios aceleradores.

Las interfaces de red elásticas lógicas que crea Global Accelerator no representan un solo host, un cuello de botella de rendimiento o un único punto de falla. Al igual que otros servicios de AWS que aparecen como una única elastic network interface en una zona de disponibilidad o subred (servicios como una puerta de enlace de traducción de direcciones de red (NAT) o un equilibrador de carga de red), el acelerador global se implementa como un servicio de alta disponibilidad y escalado horizontalmente.

Evalúe el número de subredes que utilizan los extremos de los aceleradores para determinar el número de interfaces de red elásticas que creará Global Accelerator. Antes de crear un acelerador, asegúrese de que tiene suficiente capacidad de espacio de direcciones IP para las interfaces de red elásticas necesarias, al menos una dirección IP libre por subred relevante. Si no dispone de suficiente espacio libre de direcciones IP, debe crear o utilizar una subred que tenga espacio de direcciones IP libre adecuado para el Application Load Balancer y las interfaces de red elásticas asociadas a Global Accelerator.

Cuando Global Accelerator determina que ninguno de los extremos de los aceleradores de su cuenta utiliza una elastic network interface, Global Accelerator elimina la interfaz.

Grupos de seguridad creados por Global Accelerator

Revise la siguiente información y las prácticas recomendadas cuando trabaje con Global Accelerator y grupos de seguridad.

- Global Accelerator crea grupos de seguridad asociados a sus interfaces de red elásticas. Aunque el sistema no le impide hacerlo, no debe editar ninguna de las configuraciones del grupo de seguridad para estos grupos.
- Global Accelerator no elimina los grupos de seguridad que crea. Sin embargo, Global Accelerator elimina una elastic network interface si no está siendo utilizada por ninguno de los puntos finales de los aceleradores de su cuenta.
- Puede utilizar los grupos de seguridad creados por Global Accelerator como grupo de origen en otros grupos de seguridad que mantenga, pero Global Accelerator sólo reenvía tráfico a los destinos que especifique en la VPC.
- Si modifica las reglas de grupo de seguridad creadas por Global Accelerator, es posible que el extremo no funcione correctamente. En ese caso, póngase en contacto con elAWS SupportPara obtener ayuda.
- Global Accelerator crea un grupo de seguridad específico para cada VPC. Las interfaces de red elásticas que se crean para los extremos dentro de una VPC específica utilizan el mismo grupo de seguridad, independientemente de la subred a la que esté asociada una elastic network interface.

Regiones de AWS admitidas para la preservación de direcciones IP

Puede habilitar la preservación de direcciones IP del cliente para el AWS Global Accelerator en las siguientes regiones de AWS.

Nombre de la región	Región
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`
Asia Pacific (Mumbai)	`ap-south-1`

Nombre de la región	Región
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 y monitoreo en el AWS Global Accelerator

Puede utilizar los registros de flujo y AWS CloudTrail para monitorizar el acelerador en el AWS Global Accelerator, analizar los patrones de tráfico y solucionar los problemas de los puntos de enlace de.

Temas

Registros de flujo en AWS Global Accelerator

Los logs de flujo le permiten capturar información acerca del tráfico IP entrante y saliente de las interfaces de red en el acelerador de AWS Global Accelerator. Los datos del log de flujo se publican en Amazon S3, donde puede recuperarlos y ver los datos después de crear un log de flujo.

Los logs de flujo pueden ayudarle en una serie de tareas. Por ejemplo, puede solucionar problemas de por qué un tráfico específico no llega a un punto de enlace, lo cual a su vez le ayuda a diagnosticar reglas de grupo de seguridad excesivamente restrictivas. También puede utilizar logs de flujo como herramienta de seguridad para controlar el tráfico que llega a sus puntos de enlace.

Un registro de log de flujo representa un flujo de red en su log de flujo. Cada registro captura el flujo de red para una ventana específica de captura de 5 tuplas. Una tupla de 5 es un conjunto de cinco valores distintos que especifican el origen, el destino y el protocolo para un flujo IP. La ventana de captura es la duración del tiempo durante el cual el servicio de logs de flujo agrega datos antes de publicar registros de logs de flujo. La ventana de captura es de aproximadamente 10 segundos, pero puede ser de hasta 1 minuto.

Se aplican cargos de CloudWatch Logs cuando se usan registros de flujo, incluso cuando se publican registros directamente en Amazon S3. Para obtener más información, consulteEntregar registros a S3a lasPrecios de Amazon CloudWatch.

Temas

- Sintaxis de registros de log de flujo

Publicación de registros de flujo en Amazon S3

Los logs de flujo de AWS Global Accelerator se publican en Amazon S3 en un bucket de S3 existente que especifique. Los registros de log de flujo se publican en una serie de objetos de archivos de registro que se almacenan en el bucket.

Para crear un bucket de Amazon S3 para utilizar con registros de flujo, consulte Crear un bucket en la Guía de introducción de Amazon Simple Storage Service.

Archivos de logs de flujo

Los registros de flujo recopilan entradas de registros de flujo, las consolidan en archivos de registro y, a continuación, publican los archivos de registro en el bucket de Amazon S3 en intervalos de cinco minutos. Cada archivo log contiene registros de logs de flujo del tráfico IP registrado en los cinco minutos anteriores.

El tamaño de archivo máximo de un archivo log es de 75 MB. Si el archivo log alcanza el límite de tamaño de archivo en el periodo de cinco minutos, el log de flujo deja de añadir registros de logs de flujo a este archivo, publica el archivo en el bucket de Amazon S3 y después crea un nuevo archivo log.

Los archivos de registro se guardan en el bucket de Amazon S3 especificado con una estructura de carpetas que viene determinada por el ID de registro de flujo, la región y la fecha en que se crearon. La estructura de carpetas del bucket usa el siguiente formato:

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

Del mismo modo, el nombre del archivo log viene determinado por el ID del log de flujo, la región y la fecha y hora en que se creó. Los nombres de archivo utilizan el formato siguiente:

```
aws_account_id_globalaccelerator_accelerator_id_flow_log_id_timestamp_hash.log.gz
```

Tenga en cuenta lo siguiente acerca de la estructura de nombres de carpetas y archivos para archivos de registro:

- La marca de tiempo utiliza el formato `YYYYMMDDTHHmmZ`.

- Si especifica barra diagonal (/) para el prefijo de depósito de S3, la estructura de la carpeta del depósito del archivo de registro incluirá una barra diagonal doble (//), como la siguiente:

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

El ejemplo siguiente muestra una estructura de carpetas y el nombre de archivo de un archivo log para un log de flujo creado por la cuenta de AWS123456789012para un acelerador con un ID de1234abcd-abcd-1234-abcd-1234abcdefgh, el 23 de noviembre de 2018 a las 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
```

Un único archivo de registro de flujo contiene entradas entrelazadas con múltiples registros de 5 tupla; es decir,`client_ip`,`client_port`,`accelerator_ip`,`accelerator_port`,`protocol`. Para ver todos los archivos de registro de flujo del acelerador, busque las entradas agregadas por la`accelerator_id`y su`account_id`.

Roles de IAM para publicar registros de flujo en Amazon S3

Una entidad principal de IAM, como un usuario de IAM, debe tener permisos suficientes para publicar registros de flujo en el bucket de Amazon S3. La política de IAM debe incluir los permisos siguientes:

```
{
    "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": "*"
        }
    ]
}
```

Permisos del bucket de Amazon S3 para registros de flujo

De forma predeterminada, los buckets de Amazon S3 y los objetos que contienen son privados. Solo el propietario del bucket puede tener acceso al bucket y a los objetos almacenados en él. Sin embargo, el propietario del bucket puede conceder acceso a otros recursos y usuarios escribiendo una política de acceso.

Si el usuario que crea el log de flujo es el propietario del bucket, el servicio asocia automáticamente la siguiente política al bucket para conceder al log de flujo permiso para publicar registros en él:

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

Si el usuario que va a crear el log de flujo no es el propietario del bucket o no tiene los permisos `GetBucketPolicy` y `PutBucketPolicy` para el bucket, se produce un error al crear el log de flujo. En este caso, el propietario del bucket debe agregar manualmente la política anterior al bucket y especificar el ID de cuenta de AWS del creador del log de flujo. Para obtener más información, consulte¿Cómo agrego una política de bucket en S3?en laAmazon Simple Storage Service Getting Started Guide. Si el bucket recibe logs de flujo de varias cuentas, añada un entrada del elemento `Resource` a la instrucción `AWSLogDeliveryWrite` de la política para cada cuenta.

Por ejemplo, la siguiente política de bucket permite a las cuentas de AWS 123123123 y 456456456456 publicar registros de flujo en una carpeta denominada`flow-logs`en un depósito llamado`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**
>
> Le recomendamos que conceda el`AWSLogDeliveryAclCheck`y`AWSLogDeliveryWrite`Los permisos para el principal del servicio de entrega de logs en lugar de los distintos ARN de la cuenta de AWS.

Política de claves CMK necesarias para usar con buckets de SSE-KMS

Si habilitó el cifrado en el servidor para su bucket de Amazon S3 utilizando claves administradas por AWS KMS (SSE-KMS) con una clave maestra de cliente (CMK) administrada por el cliente, debe agregar lo siguiente a la política de claves de la CMK de modo que los registros de flujo puedan escribir archivos de registro en el bucket:

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

Permisos de archivos de registro de Amazon S3

Además de las políticas de bucket necesarias, Amazon S3 utiliza listas de control de acceso (ACL) para administrar el acceso a los archivos de registro creados por un registro de flujo. De forma predeterminada, el propietario del bucket tiene los permisos `FULL_CONTROL` en cada archivo log. El propietario de la entrega de logs, si es diferente del propietario del bucket, no tiene permisos. La cuenta de entrega de logs tiene los permisos `READ` y `WRITE`. Para obtener más información, consulte Información general de las Access Control Lists (ACL, Listas de control de acceso) en la Amazon Simple Storage Service Getting Started Guide.

Habilitar registros de flujo de publicación en Amazon S3

Para habilitar los registros de flujo en AWS Global Accelerator, siga los pasos de este procedimiento.

Para habilitar los registros de flujo en AWS Global Accelerator

1. Cree un bucket de Amazon S3 para sus registros de flujo en su cuenta de AWS.
2. Agregue la política de IAM necesaria para el usuario de AWS que habilita los registros de flujo. Para obtener más información, consulte Roles de IAM para publicar registros de flujo en Amazon S3.
3. Ejecute el siguiente comando de la CLI de AWS, con el nombre y el prefijo del bucket de Amazon S3 que desea utilizar para los archivos de registro:

```
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
```

Procesamiento de entradas de registro de flujo en Amazon S3

Los archivos log están comprimidos. Si abre los archivos de registro con la consola de Amazon S3, se descomprimen y se muestran las entradas de registro de flujo. Si descarga los archivos, debe descomprimirlos para ver los registros de logs de flujo.

Tiempo de entrega de archivos de registro

AWS Global Accelerator proporciona archivos de registro para el acelerador configurado hasta varias veces cada hora. En general, un archivo de registro contiene información acerca de las solicitudes que ha recibido el acelerador durante un periodo determinado. Normalmente, Global Accelerator entrega el archivo de registro de ese periodo en el bucket de Amazon S3 en el plazo máximo de una hora después de que se produzcan los eventos reflejados en el registro. Algunas o todas las entradas de archivos de registro de un periodo a veces pueden retrasarse hasta 24 horas. Cuando se retrasan entradas de registro, Global Accelerator las guarda en un archivo de registro cuyo nombre incluye la fecha y la hora del periodo en el que se realizaron las solicitudes en lugar de incluir la fecha y la hora de entrega del archivo.

Al crear un archivo de registro, Global Accelerator consolida información para el acelerador desde todas las ubicaciones de borde que recibieron solicitudes durante el periodo que abarca dicho archivo de registro.

Global Accelerator comienza a enviar de forma fiable los archivos de registro sobre cuatro horas después de activar los registros. Es posible obtener algunos archivos de registro antes del momento de envío.

> **Note**
>
> Si ningún usuario conecta con el acelerador durante ese periodo, no recibirá archivos de registro para ese periodo.

Sintaxis de registros de log de flujo

Un registro de log de flujo es una cadena separada por espacios con el siguiente 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>
```

El formato de la versión 1.0 no incluye el identificador de VPC,`vpc_id`. El formato de la versión 2.0, que incluye`vpc_id`, se genera cuando Global Accelerator envía tráfico a un endpoint con la preservación de la dirección IP del cliente.

En la siguiente tabla se describen los campos de un registro de logs de flujo.

Campo	Descripción
`version`	La versión de los registros de flujo.
`aws_account_id`	El ID de cuenta de AWS el log de flujo.

Campo	Descripción
`accelerator_id`	El ID del acelerador para el que se registra el tráfico.
`client_ip`	La dirección IPv4 de origen.
`client_port`	El puerto de origen.
`accelerator_ip`	La dirección IP del acelerador
`accelerator_port`	El puerto del acelerador.
`endpoint_ip`	La dirección IP de destino del tráfico.
`endpoint_port`	El puerto de destino del tráfico.
`protocol`	El número de protocolo IANA del tráfico. Para obtener más información, consulte Assigned Internet Protocol Numbers.
`ip_address_type`	IPv4.
`packets`	El número de paquetes transferidos durante la ventana de captura.
`bytes`	El número de bytes transferidos durante la ventana de captura.
`start_time`	La hora, en segundos Unix, de inicio de la ventana de captura.
`end_time`	La hora, en segundos Unix, de finalización de la ventana de captura.
`action`	La acción asociada al tráfico: • `ACCEPT`: los grupos de seguridad o las ACL de red han permitido el tráfico registrado. El valor es actualmente siempre ACEPTAR.

Campo	Descripción
log-status	El estado de registro del log de flujo: • OK: los datos se registran normalmente en los destinos elegidos. • NODATA: no ha habido tráfico de red entrante ni saliente de la interfaz de red durante la ventana de captura. • SKIPDATA: algunos registros de logs de flujo se han omitido durante la ventana de captura. Esto puede deberse a una restricción de capacidad interna, o a un error interno.
globalaccelerator_source_ip	La dirección IP utilizada por la interfaz de red del acelerador global.
globalaccelerator_source_port	El puerto utilizado por la interfaz de red del acelerador global.
endpoint_region	La región de AWS en la que se encuentra el punto de enlace.
globalaccelerator_region	La ubicación de borde (punto de presencia) que atendió la solicitud. Cada ubicación de borde tiene un código de tres letras y un número asignado arbitrariamente, por ejemplo, DFW3. El código de tres letras normalmente se corresponde con el código de aeropuerto (según la Asociación de Transporte Aéreo Internacional) más cercano a la ubicación de borde. Estas abreviaturas pueden cambiar en el futuro.
direction	La dirección del tráfico. Indica el tráfico que entra en la red Global Accelerator (INGRESS) o volviendo al cliente (EGRESS).
vpc_id	El identificador de VPC. Se incluye con los registros de flujo de la versión 2.0 cuando Global Accelerator envía tráfico a un endpoint con la preservación de la dirección IP del cliente.

Si un campo no aplica para un registro específico, el registro mostrará un símbolo '-' para esa entrada.

Uso de Amazon CloudWatch con el AWS Global Accelerator

AWS Global Accelerator publica puntos de datos en Amazon CloudWatch para sus aceleradores. CloudWatch permite recuperar estadísticas sobre estos puntos de datos en conjuntos ordenados de datos de serie temporal denominadosMétricas de. Una métrica es una variable que hay que monitorizar y los puntos de datos son los valores de esa variable a lo largo del tiempo. Por ejemplo, puede monitorear el tráfico a través de un acelerador durante un periodo de tiempo especificado. Cada punto de datos tiene una marca temporal asociada y una unidad de medida opcional.

Puede utilizar estas métricas para comprobar si el sistema funciona de acuerdo con lo esperado. Por ejemplo, puede crear una alarma de CloudWatch para monitorizar una métrica determinada e iniciar una acción (por ejemplo, enviar una notificación a una dirección de correo electrónico) si la métrica no está comprendida dentro del intervalo que considera aceptable.

Global Accelerator notifica las métricas a CloudWatch únicamente cuando las solicitudes están fluyendo a través del acelerador. Si las solicitudes están fluyendo a través del acelerador, Global Accelerator mide y envía las métricas a intervalos de 60 segundos. Si no fluye ninguna solicitud a través del acelerador o no hay datos para una métrica, no se notifica la métrica.

Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

Contenido

Métricas de Global Accelerator

El espacio de nombres de `AWS/GlobalAccelerator` incluye las siguientes métricas.

Métrica	Descripción
`NewFlowCount`	Número total de flujos (o conexiones) TCP nuevos establecidos desde los clientes a los endpoints en el periodo indicado.

Métrica	Descripción
	criterios de notificación: Hay un valor distinto de cero. Estadísticas: La única estadística útil es`Sum`. Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`
`ProcessedBytesIn`	Número total de bytes entrantes procesados por el acelerador, incluidos los encabezados TCP/IP. Este recuento incluye todo el tráfico a los endpoints. criterios de notificación: Hay un valor distinto de cero. Estadísticas: La única estadística útil es`Sum`. Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`

Métrica	Descripción
`ProcessedBytesOut`	Número total de bytes salientes procesados por el acelerador, incluidos los encabezados TCP/IP. Este recuento incluye el tráfico desde los puntos finales, menos el tráfico de comprobación del estado. criterios de notificación: Hay un valor distinto de cero. Estadísticas: La única estadística útil es`Sum`. Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`

Dimensiones de métricas para los aceleradores

Para filtrar las métricas del acelerador, utilice las siguientes dimensiones.

Dimensión	Descripción
`Accelerator`	Filtra los datos de métricas por acelerador. Especifique el acelerador por el id del acelerador (la parte final del ARN del acelerador). Por ejemplo, si el ARN es`arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh` , especifique lo siguiente:**`1234abcd-abcd-1234-abcd-1234abcdefgh`** .
`Listener`	Filtra los datos de métricas por listener. Especifique el listener por el id del listener (la parte final del ARN del listener). Por ejemplo, si el ARN

Dimensión	Descripción
	`esarn:aws:globalaccelerator::012345678901:accel erator/1234abcd-abcd-1234-abcd-1234abcdefgh/l istener/0123wxyz` , especifique lo siguiente:**`0123wxyz`**.
`EndpointGroup`	Filtra los datos de métricas por grupo de puntos finales. Especifique el grupo de puntos finales por la región de AWS, por ejemplo,**`us-east-1`** (todas minúsculas).
`SourceRegion`	Filtra los datos de métrica por región de origen, que es el área geográfic a de las regiones de AWS donde se ejecutan los extremos de la aplicación. La región de origen es una de las siguientes opciones: • NA — Estados Unidos y Canadá • EU — Europa • AP — Asia Pacífico* • KR — Corea del Sur • IN — India • AU — Australia • ME — Oriente Medio • SA — América del Sur *Excluyendo Corea del Sur y la India

Dimensión	Descripción
`DestinationEdge`	Filtra los datos de métrica por borde de destino, que es el área geográfica de las ubicaciones de borde de AWS que sirven al tráfico de su cliente. El borde de destino es uno de los siguientes: • NA — Estados Unidos y Canadá • EU — Europa • AP — Asia Pacífico* • KR — Corea del Sur • IN — India • AU — Australia • ME — Oriente Medio • SA — América del Sur • ZA — Sudáfrica *Excluyendo Corea del Sur y la India
`TransportProtocol`	Filtra los datos de métricas por protocolo de transporte: UDP o TCP.
`AcceleratorIPAddress`	Filtra los datos de métricas por la dirección IP del acelerador: es decir, una de las direcciones IP estáticas asignadas a un acelerador.

Estadísticas de métricas de Global Accelerator

CloudWatch proporciona estadísticas en función de los puntos de datos de las métricas publicadas por Global Accelerator. Las estadísticas son agregaciones de los datos de las métricas a lo largo de un periodo de tiempo especificado. Cuando se solicitan estadísticas, el flujo de datos devuelto se identifica mediante el nombre de la métrica y su dimensión. Una dimensión es un par de nombre/valor que identifica una métrica de forma inequívoca. Por ejemplo, puede solicitar la salida de bytes procesados para un acelerador en el que los bytes se sirven desde ubicaciones de borde de AWS en Europa (el borde de destino es «UE»).

Los siguientes son ejemplos de combinaciones métricas/dimensiones que pueden resultar útiles:

- Vea la cantidad de tráfico servido (como ProcessedBytesOut) por cada una de las dos direcciones IP del acelerador para validar que la configuración DNS es correcta.
- Vea la distribución geográfica del tráfico de usuario y supervise cuánto es local (por ejemplo, Norteamérica a Norteamérica) o global (por ejemplo, Australia o India a Norteamérica). Para determinar esto, vea las métricas ProcessedByteSin o ProcessedBytesOut con las dimensiones DestinationEdge y SourceRegion establecidas en valores específicos.

Consulte métricas de CloudWatch para sus aceleradores

Puede ver las métricas de CloudWatch para sus aceleradores desde la consola de CloudWatch o la CLI de AWS. En la consola, las métricas se muestran en gráficos de monitorización. Los gráficos de monitorización muestran puntos de datos únicamente si el acelerador se encuentra activo y recibiendo solicitudes.

Debe consultar las métricas de CloudWatch para Global Accelerator en la región EE.UU. Oeste (Oregón), tanto en la consola como al utilizar la CLI de AWS. Cuando utilice la CLI de AWS, especifique la región EE.UU. Oeste (Oregón) para su comando incluyendo el siguiente parámetro:`--region us-west-2`.

Para consultar métricas mediante la consola de CloudWatch

1. Abra la consola de CloudWatch enhttps://us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2.
2. En el panel de navegación, seleccione Metrics.
3. Seleccione laGlobalAcceleratorEspacio de nombres.
4. (Opcional) Para ver una métrica en todas las dimensiones, escriba su nombre en el campo de búsqueda.

Para ver métricas mediante la CLI de AWS

Utilice el siguiente comando list-metrics para obtener una lista de las métricas disponibles:

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

Para obtener las estadísticas de una métrica desde la CLI de AWS

Utilice el siguienteget-metric-statisticsPara obtener estadísticas de una métrica y dimensión especificada. Tenga en cuenta que CloudWatch trata cada combinación exclusiva de dimensiones como una métrica independiente. No se pueden recuperar estadísticas utilizando combinaciones de dimensiones que no se han publicado específicamente. Debe especificar las mismas dimensiones que se utilizaron al crear las métricas.

En el ejemplo siguiente se muestra el total de bytes procesados en, por minuto, para el acelerador que sirve desde el borde de destino de Norteamérica (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 continuación se muestra un ejemplo de salida del 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"
        }
    ]
}
```

Uso de AWS CloudTrail para registrar las llamadas a la API de AWS Global Accelerator

AWS Global Accelerator está integrado con AWS CloudTrail, un servicio que registra las acciones de usuarios, roles o servicios de AWS en Global Accelerator. CloudTrail captura todas las llamadas a la API de Global Accelerator como eventos, incluidas las llamadas procedentes de la consola de Global Accelerator y las llamadas de código a la API de Global Accelerator. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Global Accelerator. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Event history (Historial de eventos).

Para obtener más información sobre CloudTrail, consulte la AWS CloudTrail User Guide.

Información de CloudTrail

CloudTrail se habilita en una cuenta de AWS al crearla. Cuando se produce una actividad en Global Accelerator, dicha actividad se registra en un evento de CloudTrail junto con los demás eventos de

servicios de AWS enHistorial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos de la cuenta de AWS, incluidos los eventos de Global Accelerator, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También puede configurar otros servicios de AWS para analizar y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las acciones de Global Accelerator y se documentan enReferencia de AWS Global Accelerator. Por ejemplo, las llamadas a`CreateAccelerator`,`ListAccelerators`y`UpdateAccelerator`generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información acerca de quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado
- Si la solicitud la realizó otro servicio de AWS

Para obtener más información, consulte el elemento userIdentity de CloudTrail.

Descripción de las entradas de archivos de registro de Global Acceler

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registro en un bucket de Amazon S3 que especifique. Cada archivo de registro con formato JSON de CloudTrail puede contener una o más entradas de registro. Una entrada de registro representa una única solicitud de cualquier origen e incluye información acerca de la acción solicitada, incluidos todos los parámetros, la fecha y la hora de la acción, etcétera. No se garantiza que las entradas de registro sigan un orden específico; es decir, no son un rastro del stack ordenado de llamadas a la API.

En el ejemplo siguiente, se muestra una entrada de registro de CloudTrail que incluye estas acciones de Global Accelerator:

- Listado de los aceleradores de una cuenta:`eventNameesListAccelerators`.
- Crear un agente de escucha:`eventNameesCreateListener`.
- Actualizar un agente de escucha:`eventNameesUpdateListener`.
- Describiendo un agente de escucha:`eventNameesDescribeListener`.
- Enumerar los oyentes de una cuenta:`eventNameesListListeners`.
- Eliminar un agente de escucha:`eventNameesDeleteListener`.

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

Seguridad de AWS Global Accelerator

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información acerca de los programas de conformidad que se aplican a Global Accelerator, consulteServicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad dependerá del servicio de AWS que utilice. Usted también es responsable de otros factores incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación lo ayudará a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Global Accelerator. En los siguientes temas, se le mostrará cómo configurar el acelerador global para satisfacer sus objetivos de seguridad.

Temas

Administración de identidades y accesos para AWS Global Accelerator

AWS Identity and Access Management (IAM) es un servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos de AWS, incluidos los recursos de AWS Global Accelerator. Los administradores usan IAM para controlar quién esautenticado(iniciado sesión) yAutorizado(tiene permisos) para utilizar recursos de Global Accelerator. La IAM es una característica incluida en la cuenta de AWS sin cargo adicional.

> **Important**
>
> Si no está familiarizado con IAM, revise la información introductoria de esta página y, a continuación, consulteIntroducción a IAM. Si lo desea, puede obtener más información sobre la autenticación y el control de acceso en¿Qué es la autenticación?,¿Qué es el control de acceso?, y¿Qué son las políticas?.

Temas

Conceptos y términos

AutenticaciónPara iniciar sesión en AWS, debe utilizar una de las siguientes opciones: credenciales de usuario raíz (no se recomienda), credenciales de usuario de IAM o credenciales temporales mediante roles de IAM. Para obtener más información acerca de estas entidades, consulte ¿Qué es la autenticación?.

Control de acceso: los administradores de AWS utilizan políticas para controlar el acceso a los recursos de AWS, tales como aceleradores de Acelerador global. Para obtener más información, consulte ¿Qué es el control de acceso? y ¿Qué son las políticas?.

> **Important**
>
> Todos los recursos de una cuenta son propiedad de esta última, independientemente de quién los haya creado. Debe tener acceso para crear un recurso. Sin embargo, el mero hecho de haber creado un recurso no significa que automáticamente vaya a tener acceso completo a dicho recurso. Un administrador debe conceder permisos de forma explícita para cada acción que se desee realizar. Ese administrador también puede revocar los permisos en cualquier momento.

Para ayudarle a comprender los conceptos básicos del funcionamiento de IAM, revise los siguientes términos:

Recursos

Los servicios de AWS, como el acelerador global e IAM, suelen incluir objetos denominados recursos. En la mayoría de los casos, puede crear, administrar y eliminar estos recursos del servicio. Los recursos de IAM incluyen usuarios, grupos, roles y políticas:

Usuarios

Un usuario de IAM representa a la persona o aplicación que utiliza sus credenciales para interactuar con AWS. Un usuario consta de un nombre, una contraseña para iniciar sesión en la consola de administración de AWS y un máximo de dos claves de acceso que se pueden utilizar con la CLI o la API de AWS.

Grupos

Un grupo de IAM es un conjunto de usuarios de IAM. Los administradores pueden usar los grupos para especificar permisos para los usuarios que lo componen. Esto facilita el proceso de administrar los permisos de varios usuarios.

Roles

Un rol de IAM no tiene asociadas unas credenciales a largo plazo (contraseña o claves de acceso). Cualquier persona que la necesite y tenga permiso para ello puede asumir un rol. Un usuario de IAM puede asumir una función para disponer temporalmente de diferentes permisos para una tarea específica. Los usuarios federados puede asumir un rol mediante un proveedor de identidad externo mapeado a ese rol. Algunos servicios de AWS pueden asumir unRol de servicio dePara obtener acceso a los recursos de AWS en su nombre.

Políticas

Las políticas son documentos JSON que definen los permisos para el objeto al que están asociadas. AWS admitePolíticas de basadas en identidadesque asocie a identidades (usuarios, grupos o roles). Algunos servicios de AWS le permiten adjuntarPolíticas de basadas en recursosPara controlar lo que una entidad principal (persona o aplicación) puede hacer con ese recurso. Global Accelerator no admite políticas basadas en recursos de.

Identidades

Las identidades son recursos de IAM para los cuales se pueden definir permisos. Estos incluyen usuarios, grupos y roles.

Entidades

Las entidades son recursos de IAM que se utilizan para la autenticación. Estos incluyen usuarios y roles.

Entidades principales

En AWS, una entidad principal es una persona o aplicación que utiliza una entidad para iniciar sesión en y realizar solicitudes a AWS. Como entidad principal, puede utilizar la consola de administración de AWS o la CLI o la API de AWS para llevar a cabo una operación (por ejemplo, eliminar un acelerador). Esto crea una solicitud para esa operación. La solicitud especifica la acción, el recurso, la entidad principal, la cuenta de la entidad principal y la información adicional deseada sobre la solicitud. Toda esta información proporciona a AWS concontextPara su solicitud. AWS comprueba todas las políticas que se aplican al contexto de una solicitud. AWS autoriza la solicitud únicamente si cada parte de la solicitud está permitida por las políticas.

Para ver un diagrama del proceso de autenticación y control de acceso, consulteEntender cómo funciona IAMen laGuía del usuario de IAM. Para obtener información detallada acerca de cómo AWS determina si una solicitud está permitida, consulteLógica de evaluación de políticasen laGuía del usuario de IAM.

Permisos necesarios para el acceso a la consola, la administración de autenticación y el control de acceso

Para utilizar Global Accelerator o para administrar la autorización y el control de acceso para sí mismo o para otros, debe contar con los permisos adecuados.

Permisos necesarios para crear un acelerador Global Accelerator

Para crear un AWS Global Accelerator, los usuarios deben tener permiso para crear roles vinculados a servicios asociados a Global Accelerator.

Para asegurarse de que los usuarios tienen los permisos correctos para crear aceleradores en Global Accelerator, adjunte una directiva al usuario como la siguiente.

> **Note**
>
> Si crea una política de permisos basados en identidad que sea más restrictiva, los usuarios con dicha política no podrán crear un 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*"
    }
```

Permisos necesarios para usar la consola Global Accelerator

Para obtener acceso a la consola de AWS Global Accelerator, debe tener un conjunto mínimo de permisos que le permita mostrar y ver detalles sobre los recursos de Global Accelerator de su cuenta de AWS. Si crea una política de permisos basados en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades que tengan esa política.

Para asegurarse de que esas entidades puedan seguir usando la consola de Global Accelerator o las acciones de la API, asocie también una de las políticas administradas de AWS siguientes al usuario, tal y como se describe enCreación de políticas en la pestaña JSON:

```
        GlobalAcceleratorReadOnlyAccess
        GlobalAcceleratorFullAccess
```

Adjuntar la primera política,`GlobalAcceleratorReadOnlyAccess`, si los usuarios solo necesitan ver información en la consola o realizar llamadas a la CLI de AWS o a la API que utilizan`List*`or`Describe*`Operaciones.

Adjuntar la segunda política,`GlobalAcceleratorFullAccess`, a los usuarios que necesitan crear o actualizar los aceleradores. La política de acceso completa incluyeFULLpermisos para Global Accelerator, así comodescribepermisos para Amazon EC2 y Elastic Load Balancing.

> **Note**
>
> Si crea una política de permisos basada en identidades que no incluya los permisos necesarios para Amazon EC2 y Elastic Load Balancing, los usuarios con esa política no podrán agregar recursos de Amazon EC2 y Elastic Load Balancing a los aceleradores.

La siguiente es la política de acceso 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/*"
            ]
        }
    ]
}
```

Permisos necesarios para la administración de autenticación

Para administrar sus propias credenciales, tales como su contraseña, claves de acceso y dispositivos Multi-Factor Authentication (MFA), el administrador debe concederle los permisos necesarios. Para ver la política que incluye estos permisos, consulte Permitir a los usuarios de administrar ellos mismos sus credenciales.

Como administrador de AWS, necesita acceso completo a IAM para poder crear y administrar usuarios, grupos, roles y políticas de IAM. Debe utilizar la opciónAdministratorAccessPolítica Administrada por AWS que incluye acceso completo a la totalidad de AWS. Esta política no proporciona acceso a la consola de Billing and Cost Management de AWS ni permite tareas que requieren credenciales de usuario raíz de la cuenta de AWS. Para obtener más información, consulteTareas de AWS que requieren credenciales de usuario raíz de la cuenta de AWSen laReferencia general de AWS.

> **Warning**
>
> Solo un usuario administrador debe tener acceso completo a AWS. Cualquier persona que tenga esta política dispondrá de permiso para administrar totalmente la autenticación y el control de acceso, además de para modificar todos los recursos de AWS. Para obtener más información sobre cómo crear este usuario, consulte Cree su usuario administrador de IAM.

Permisos necesarios para el control de acceso

Si el administrador le ha proporcionado credenciales de usuario de IAM, habrán asociado políticas a ese usuario de IAM para controlar a qué recursos puede tener acceso. Para ver las políticas asociadas a su identidad de usuario en AWS Management Console, debe tener los permisos siguientes:

```
{
    "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": "*"
        }
    ]
}
```

Si necesita permisos adicionales, pida a su administrador que actualice las políticas de tal forma que pueda tener acceso a las acciones que necesita.

Comprender cómo funciona Global Accelerator con IAM

Los servicios pueden funcionar con IAM de varias maneras:

Actions

Global Accelerator admite el uso de acciones en una política. Esto permite que un administrador controle si una entidad puede completar una operación de Global Accelerator. Por ejemplo, para permitir que una entidad llame al método`GetPolicy`Para ver una política de la API de AWS, un administrador debe asociar una política que permita que la`iam:GetPolicy`action.

En la siguiente política de ejemplo se permite a un usuario realizar la instrucción de`CreateAccelerator`para crear mediante programación un acelerador para su cuenta de AWS:

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

Permisos de nivel de recursos

Global Accelerator admite permisos de nivel de recurso. Los permisos de nivel de recursos permiten usar ARN para especificar recursos individuales en la política.

Políticas basadas en recursos

Global Accelerator no admite políticas basadas en recursos de. Con las políticas basadas en recursos, puede asociar una política a un recurso dentro del servicio. Las políticas basadas en recursos incluyen un`Principal`Para especificar qué identidades de IAM pueden obtener acceso a dicho recurso.

Autorización basada en etiquetas

Global Accelerator admite etiquetas basadas en autorización. Esta característica le permite utilizar etiquetas de recursos en la condición de una política.

Credenciales temporales

Global Accelerator admite las credenciales temporales. Con credenciales temporales, puede iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen mediante una llamada a operaciones de la API de AWS STS como`AssumeRole`or`GetFederationToken`.

Roles vinculados a servicios

Global Accelerator admite roles vinculados a servicios. Esta característica permite que un servicio asuma un rol vinculado a un servicio en nombre de usted. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Roles de servicio

Global Accelerator no es compatible con roles de servicio. Esta característica permite que un servicio asuma un rol de servicio en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en su cuenta de IAM y son propiedad de la cuenta. Esto significa que un administrador de IAM puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

Solución de problemas de autenticación y control de acceso

Utilice la información siguiente para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con IAM.

Temas

- No tengo autorización para realizar una acción en Global Accelerator
- Soy administrador y deseo permitir que otros obtengan acceso a Global Accelerator
- Quiero entender IAM sin convertirme en un experto

No tengo autorización para realizar una acción en Global Accelerator

Si la consola de administración de AWS le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con el administrador que le haya proporcionado su nombre de usuario y contraseña.

El ejemplo siguiente se produce cuando un usuario de IAM denominado`my-user-name`intenta usar la consola de para realizar la`globalaccelerator:CreateAccelerator`pero no tiene permisos:

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

En este caso, pida al administrador que actualice sus políticas de forma que pueda obtener acceso a la`my-example-accelerator`Uso de la herramienta`aws-globalaccelerator:CreateAccelerator`action.

Soy administrador y deseo permitir que otros obtengan acceso a Global Accelerator

Para permitir que otros obtengan acceso a Global Accelerator, debe crear una entidad de IAM (usuario o rol) para la persona o aplicación que necesita acceso. Esta persona utilizará las credenciales de la entidad para obtener acceso a AWS. A continuación, debe asociar una política a la entidad que les conceda los permisos correctos en Global Accelerator.

Para comenzar trabajar enseguida, consulte Introducción a IAM.

Quiero entender IAM sin convertirme en un experto

Para obtener más información sobre los términos, conceptos y procedimientos de IAM, consulte los siguientes temas:

- ¿Qué es la autenticación?
- ¿Qué es el control de acceso?
- ¿Qué son las políticas?

Políticas basadas en etiquetas

Al diseñar políticas de IAM, es posible establecer permisos pormenorizados mediante la concesión de acceso a recursos específicos. A medida que crezca la cantidad de recursos que administra, esta tarea será más complicada. El etiquetado de aceleradores y uso de etiquetas en las condiciones de declaración de política pueden facilitar esta tarea. Puede conceder acceso de forma masiva a cualquier acelerador con una determinada etiqueta. A continuación, aplique repetidamente esta etiqueta a los aceleradores pertinentes, al crear el acelerador o al actualizar el acelerador más tarde.

> **Note**
>
> El uso de etiquetas en las condiciones es una manera de controlar el acceso a los recursos y las solicitudes. Para obtener información acerca del etiquetado en Global Accelerator, consulteEtiquetado en AWS Global Accelerator.

Las etiquetas se pueden asociar a un recurso o pasarse dentro de la solicitud a los servicios que admiten etiquetado. En Global Accelerator, sólo los aceleradores pueden incluir etiquetas. Al crear una política de IAM, puede utilizar las claves de condición de etiqueta para controlar:

- Qué usuarios pueden realizar acciones en un acelerador, basándose en las etiquetas que ya tiene.
- Las etiquetas que se pueden pasar en la solicitud de una acción.
- Si claves de etiqueta específicas se pueden utilizar en una solicitud.

Para obtener la sintaxis y semántica completas de claves de condición de etiquetas, consulteControlar el acceso mediante etiquetas de IAMen laGuía del usuario de IAM.

Por ejemplo, el Acelerador Global`GlobalAcceleratorFullAccess`La política de usuario administrada proporciona a los usuarios permisos ilimitados para realizar cualquier acción de Acelerador global en cualquier recurso. La siguiente política deniega permiso a usuarios no autorizados para realizar cualquier acción de Global Accelerator en cualquierProducciónAceleradores de El administrador de un cliente debe asociar esta política de IAM a los usuarios de IAM no autorizados, además de la política de usuario administrada.

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

Función vinculada al servicio de Global Accelerator

El AWS Global Accelerator de AWS utiliza una gestión de acceso e identidad de AWS (IAM).Rol vinculado al servicio de. Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a un servicio. Las funciones vinculadas a servicios son predefinidos por el servicio e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Global Accelerator usa la siguiente función vinculada al servicio de IAM:

- AWSServiceRoleForGlobalAccelerator: Global Accelerator utiliza esta función para permitir que Global Accelerator cree y administre los recursos necesarios para la preservación de la dirección IP del cliente.

Global Accelerator crea automáticamente un rol llamado AWSServiceRoleForGlobalAccelerator cuando el rol se requiere por primera vez para admitir una operación de la API de Global Accelerator. El rol AWSServiceRoleForGlobalAccelerator permite a Global Accelerator crear y administrar los recursos necesarios para la preservación de la dirección IP del cliente. Este rol es necesario para utilizar aceleradores en Global Accelerator. El ARN del rol AWSServiceRoleForGlobalAccelerator tiene este aspecto:

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

Los roles vinculados a servicios simplifican la configuración y el uso de Global Accelerator porque ya no tendrá que agregar manualmente los permisos necesarios. Global Accelerator define los permisos de su rol vinculado a servicio y solo Global Accelerator puede asumir estos roles. Los permisos definidos incluyen la política de confianza y la política de permisos. La política de permisos no se puede asociar a ninguna otra entidad de IAM.

Debe eliminar los recursos de Global Accelerator asociados para poder eliminar un rol vinculado a servicio. Esto ayuda a proteger sus recursos de Global Accelerator al asegurarse de que no elimina un rol vinculado a un servicio que sigue siendo necesario para obtener acceso a los recursos activos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que tienen Sí en la columna Rol vinculado a servicio.

Permisos de roles vinculados a servicios para Global Accelerator

Global Accelerator usa un rol vinculado a un servicio denominadoAWSServiceRoleForGlobalAccelerator. En las siguientes secciones se describen los permisos de la función.

Permisos de roles vinculados a servicios

Esta función vinculada a servicios permite a Global Accelerator administrar las interfaces de red elásticas EC2 y los grupos de seguridad, así como ayudar a diagnosticar errores.

El rol vinculado al servicio AWSServiceRoleForGlobalAccelerator confía en el siguiente servicio para asumir el rol:

- `globalaccelerator.amazonaws.com`

La política de permisos del rol permite que Global Accelerator realice las siguientes acciones en los recursos especificados, tal y como se muestra en la 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/*"
            ]
        }
    ]
}
```

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) eliminar el rol vinculado al servicio de Global Accelerator. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación del rol vinculado a un servicio de Global Accelerator

No es necesario crear manualmente el rol vinculado al servicio para Global Accelerator. El servicio crea automáticamente el rol automáticamente la primera vez que se crea un acelerador. Si elimina sus recursos de Global Accelerator y elimina el rol vinculado a un servicio, el servicio volverá a crear el rol automáticamente al crear un nuevo acelerador.

Edición de la función vinculada al servicio de Global Accelerator

Acelerador global no permite editar el rol vinculado al servicio AWSServiceRoleForGlobalAccelerator. Una vez que el servicio ha creado un rol vinculado a un servicio, no puede cambiarle el nombre, ya

que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción de un rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación del rol vinculado al servicio de Global Accelerator

Si ya no tiene que utilizar el acelerador global, le recomendamos que elimine el rol vinculado al servicio. De esta forma no tendrá entidades no utilizadas que no se monitoricen ni mantengan de forma activa. Sin embargo, debe limpiar los recursos de Global Accelerator de la cuenta antes de poder eliminar manualmente los roles.

Después de haber desactivado y eliminado los aceleradores de, puede eliminar el rol vinculado al servicio. Para obtener más información acerca de la eliminación de aceleradores, consulte Creación o actualización de un acelerador estándar.

> **Note**
>
> Si ha deshabilitado y eliminado sus aceleradores pero el acelerador global no ha finalizado la actualización, la eliminación del rol vinculado a servicio puede dar un error. En tal caso, espere unos minutos y realice de nuevo los pasos de eliminación de roles vinculados a servicios.

Para eliminar manualmente el rol vinculado al servicio AWSServiceRoleForGlobalAccelerator

1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, elija Roles. A continuación, seleccione la casilla junto al nombre del rol que desea eliminar, no el nombre ni la fila.
3. En Role actions (Acciones de rol) en la parte superior de la página, elija Delete role (Eliminar rol).
4. En el cuadro de diálogo de confirmación, revise los datos del último acceso al servicio, que muestra cuándo cada uno de los roles seleccionados tuvo acceso a un servicio de AWS por última vez. Esto le ayuda a confirmar si el rol está actualmente activo. Si desea continuar, seleccione Yes, Delete para enviar la solicitud de eliminación del rol vinculado al servicio.
5. Consulte las notificaciones de la consola de IAM para monitorear el progreso de la eliminación del rol vinculado al servicio. Como el proceso de eliminación del rol vinculado al servicio de

IAM es asíncrono, dicha tarea puede realizarse correctamente o fallar después de que envía la solicitud de eliminación. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Actualizaciones de la función vinculada al servicio del Acelerador global (una política administrada por AWS)

Ver detalles acerca de las actualizaciones de la función vinculada al servicio desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en AWS Global AcceleratorHistorial de revisión(Se ha creado el certificado).

Cambio	Descripción	Fecha
AWSServiceRoleForGlobalAccelerator— Actualización de la política	Global Accelerator agregó un nuevo permiso para ayudar a Global Accelerator a diagnosticar errores. Utiliza Global Acceleratorec2:DescribeRegions para determinar la región de AWS en la que se encuentra un cliente, lo que puede ayudar a Global Accelerator a solucionar errores.	18 de mayo de 2021
Global Accelerator comenzó el seguimiento de los cambios	Global Accelerator comenzó a realizar el seguimiento de los cambios en sus políticas administradas de AWS.	18 de mayo de 2021

Regiones admitidas para roles vinculados a servicios de Global Accelerator

El acelerador global admite el uso de roles vinculados a servicios en las regiones de AWS en las que se admite el acelerador global.

Para obtener una lista de las regiones de AWS en las que actualmente se admiten el acelerador global y otros servicios, consulte laTabla de regiones de AWS.

Información general del acceso y la autenticación

Si no conoce, lea los siguientes temas para comenzar a usar la autorización y el acceso a través de AWS.

Temas

- ¿Qué es la autenticación?
- ¿Qué es el control de acceso?
- ¿Qué son las políticas?
- Introducción a IAM

¿Qué es la autenticación?

La autenticación es la manera de iniciar sesión en AWS mediante credenciales.

> **Note**
>
> Para comenzar a utilizar el servicio rápidamente, puede omitir esta sección. En primer lugar, revise la información introductoria deAdministración de identidades y accesos para AWS Global Acceleratory, a continuación, consulteIntroducción a IAM.

Como principal, debe serautenticado(con la sesión iniciada en AWS) mediante una entidad (usuario raíz, usuario de IAM o rol de IAM) para enviar una solicitud a AWS. Un usuario de IAM puede tener credenciales a largo plazo, como un nombre de usuario y una contraseña o un conjunto de claves de acceso. Al asumir un rol de IAM, se le proporcionan unas credenciales de seguridad temporales.

Para autenticarse desde la AWS Management Console como usuario de, debe iniciar sesión con su nombre de usuario y contraseña. Para autenticarse desde la CLI de AWS o la API de AWS, debe proporcionar su clave de acceso y clave secreta o credenciales temporales. AWS proporciona SDK y herramientas de CLI para firmar criptográficamente su solicitud con sus credenciales. Si no utiliza las herramientas de AWS, debe firmar usted mismo la solicitud. Independientemente del método de autenticación que utilice, es posible que también deba proporcionar información de

seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta.

Como entidad principal, puede iniciar sesión en AWS utilizando las siguientes entidades (usuarios o roles):

Usuario de la cuenta raíz de AWS

Cuando crea por primera vez una cuenta de AWS, comienza únicamente por una identidad de inicio de sesión único que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la cuenta de AWS y para obtener acceso a ella se inicia sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Le recomendamos encarecidamente que no utilice el usuario raíz en sus tareas cotidianas, ni siquiera en las tareas administrativas. En lugar de ello, es mejor ceñirse a la práctica recomendada de utilizar el usuario final exclusivamente para crear al primer usuario de IAM. A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilícelas tan solo para algunas tareas de administración de cuentas y servicios.

Usuario de IAM

UnaUsuario de IAMes una entidad de su cuenta de AWS que dispone de permisos específicos. admite Global AcceleratorSignature Version 4, un protocolo para autenticar solicitudes de API de entrada. Para obtener más información sobre las solicitudes de autenticación, consulte Proceso de firma de Signature Version 4 en la Referencia general de AWS.

Rol de IAM

UnaRol de IAMLa identidad de IAM es una identidad de IAM que puede crear en la cuenta y que tiene permisos específicos. Un rol de IAM es similar a un usuario de IAM, ya que se trata de una AWS Identity con políticas de permisos que determinan lo que la identidad puede hacer y lo que no en AWS. Sin embargo, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Además, un rol no tiene asociadas credenciales a largo plazo estándar, como una contraseña o claves de acceso. En su lugar, cuando se asume un rol, este proporciona credenciales de seguridad temporales para la sesión de rol. Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

Acceso de usuarios federados

En lugar de crear un usuario de IAM, puede utilizar identidades existentes de AWS Directory Service, el directorio de usuarios de la compañía o un proveedor de identidad web. Esto se conoce como usuarios federados. AWS asigna un rol a un usuario federado cuando se solicita

acceso a través de un proveedor de identidad. Para obtener más información acerca de los usuarios federados, consulte Usuarios y roles federados en la Guía del usuario de IAM.

Permisos de usuario temporales

Un usuario de IAM puede asumir temporalmente un rol para disponer de diferentes permisos para una tarea específica.

Acceso entre cuentas

Puede utilizar un rol de IAM para permitir que una entidad principal de confianza de otra cuenta obtenga acceso a los recursos de su cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos servicios de AWS, puede asociar una política directamente a un recurso (en lugar de utilizar un rol como proxy). Global Accelerator no admite estas políticas basadas en recursos de. Para obtener más información sobre si debe elegir un rol o una política basada en recursos para permitir el acceso entre cuentas, consulte Control del acceso a entidades principales en una cuenta diferente.

Acceso a los servicios de AWS

Un rol de servicio es unRol de IAMque un servicio asume para realizar acciones en su nombre. Los roles de servicio ofrecen acceso solo dentro de su cuenta y no se pueden utilizar para otorgar acceso a servicios en otras cuentas. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un servicio de AWS en la Guía del usuario de IAM.

Aplicaciones que se ejecutan en Amazon EC2

Puede utilizar un rol de IAM para administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia EC2 y realizan solicitudes de la API y la CLI de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la misma. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

¿Qué es el control de acceso?

Después de iniciar sesión (autenticarse) en AWS, el acceso a los recursos y las operaciones de AWS se rige por políticas. El control de acceso también se denomina autorización.

> **Note**
>
> Para comenzar a utilizar el servicio rápidamente, puede omitir esta página. En primer lugar, revise la información introductoria deAdministración de identidades y accesos para AWS Global Acceleratory, a continuación, consulteIntroducción a IAM.

Durante la autorización, AWS utiliza valores de laContexto de solicitudPara comprobar las políticas de que se aplican. A continuación, utiliza las políticas para determinar si se debe permitir o denegar la solicitud. La mayoría de las políticas se almacenan en AWS como documentos JSON y especifican los permisos que se permiten o deniegan para las entidades principales. Para obtener más información acerca de la estructura y los contenidos de los documentos de política JSON, consulte ¿Qué son las políticas?.

Las políticas permiten al administrador especificar quién tiene acceso a los recursos de AWS y qué acciones se pueden realizar en dichos recursos. Cada entidad de IAM (usuario o rol) comienza sin permisos. En otras palabras, de forma predeterminada, los usuarios no pueden hacer nada, ni siquiera consultar sus propias claves de acceso. Para conceder permiso a un usuario para hacer algo, el administrador debe asociarle una política de permisos. También puede añadir el usuario a un grupo que tenga los permisos necesarios. Cuando un administrador concede permisos a un grupo, todos los usuarios de ese grupo obtienen los permisos.

Aunque disponga de credenciales válidas para autenticar solicitudes, si un administrador no le ha concedido permisos, no podrá crear recursos de AWS Global Accelerator ni obtener acceso a ellos. Por ejemplo, debe tener permisos explícitos para crear un AWS Global Accelerator.

Como administrador, puede escribir una política para controlar el acceso a lo siguiente:

- Entidades principalesControl de qué es la persona o aplicación que realiza la solicitud (laprincipal) está permitido hacer.
- Identidades de IAM: controle a qué identidades de IAM (grupos, usuarios y roles) se puede tener acceso y cómo.
- Políticas de IAMControle quién puede crear, editar y eliminar políticas administradas por el cliente y quién puede asociar y desasociar todas las políticas administradas.
- Recursos de AWS: controle quién tiene acceso a los recursos a través de una política basada en identidad o una política basada en recursos.
- Cuentas de AWS: controle si una solicitud se permite únicamente para los miembros de una cuenta determinada.

Control del acceso para entidades principales de

Las políticas de permisos controlan lo que se le permite hacer a usted, en calidad de entidad principal. Un administrador debe asociar una política de permisos basada en identidad a la identidad (usuario, grupo o rol) que le conceda permisos a usted. Las políticas de permisos permiten o deniegan el acceso a AWS. Los administradores también pueden establecer un límite de permisos para una entidad de IAM (usuario o rol), con el fin de definir los permisos máximos que esa entidad puede tener. Los límites de permisos son una característica avanzada de IAM. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

Para obtener más información y un ejemplo de cómo controlar el acceso a AWS para las entidades principales, consulteControl del acceso de entidades principales deen laGuía del usuario de IAM.

Control del acceso a las identidades

Los administradores controlan lo que se puede hacer con una identidad de IAM (usuario, grupo o rol) mediante la creación de una política que limite lo que se puede hacer con una identidad o quién puede tener acceso a ella. A continuación, se debe asociar esa política a la identidad que le concede los permisos.

Por ejemplo, un administrador podría permitirle restablecer la contraseña de tres usuarios concretos. Para ello, asociará una política a su usuario de IAM que le permite restablecer la contraseña solo de sí mismo y de los usuarios con el ARN de los tres usuarios especificados. Esto le permitirá restablecer la contraseña de los miembros de su equipo, pero no las de otros usuarios de IAM.

Para obtener más información y ver un ejemplo de cómo utilizar una política para controlar el acceso a las identidades de AWS, consulteControl del acceso a las identidadesen laGuía del usuario de IAM.

Controlar el acceso a las políticas

Los administradores pueden controlar quién está autorizado a crear, editar y eliminar políticas administradas por el cliente y/o a asociar y desasociar todas las políticas administradas. Al revisar una política, puede ver el resumen de políticas que incluye un resumen del nivel de acceso de cada servicio de dicha política. AWS clasifica cada acción de servicio en una de las cuatroNivel de accesobasado en lo que hace cada acción:`List`,`Read`,`Write`, o bien`Permissions management`. Puede utilizar estos niveles de acceso para determinar qué acciones deben incluirse en las políticas. Para obtener más información, consulteDescripción de los resúmenes de nivel de acceso en los resúmenes de políticasen laGuía del usuario de IAM.

> **Warning**
>
> Debe limitar`Permissions Management`Permisos de nivel de acceso en su cuenta. De lo contrario, los miembros de su cuenta podrán crear políticas para sí mismos con más permisos de los que deben tener. O pueden crear usuarios independientes con acceso completo a AWS.

Para obtener más información y un ejemplo de cómo controlar el acceso de AWS a las políticas, consulteControlar el acceso a las políticasen laGuía del usuario de IAM.

Control del acceso a los recursos de

Los administradores pueden controlar el acceso a los recursos a través de una política basada en identidad o una política basada en recursos. En una política basada en la identidad, la política se asocia a una identidad y se especifica a qué recursos tiene acceso dicha identidad. En una política basada en recursos, se asocia una política al recurso que desea controlar. En la política, especifica las entidades principales que pueden tener acceso a dicho recurso.

Para obtener más información, consulteControl del acceso a los recursosen laGuía del usuario de IAM.

Los creadores de recursos no tienen permisos automáticamente

Todos los recursos de una cuenta son propiedad de esta última, independientemente de quién los haya creado. El usuario raíz de la cuenta de AWS es el propietario de la cuenta y, por lo tanto,tiene permiso para realizar cualquier acción en cualquier recurso de la cuenta.

> **Important**
>
> Le recomendamos encarecidamente que no utilice el usuario raíz en sus tareas cotidianas, ni siquiera en las tareas administrativas. En su lugar, siga elLas prácticas recomendadas de utilizar el usuario raíz únicamente para crear el primer usuario de IAM. A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilícelas tan solo para algunas tareas de administración de cuentas y servicios. Para ver las tareas que exigen que inicie sesión como usuario raíz, consulteTareas de AWS que requieren usuario raíz.

Las entidades (usuarios o roles) de la cuenta de AWS deben disponer de acceso para crear un recurso. Sin embargo, el mero hecho de haber creado un recurso no significa que automáticamente

vayan a tener acceso completo a dicho recurso. Los administradores deben conceder de forma explícita los permisos para cada acción. Además, los administradores pueden revocar esos permisos en cualquier momento, siempre y cuando dispongan de acceso para administrar permisos de usuarios y roles.

Control del acceso a entidades principales en una cuenta diferente

Los administradores pueden utilizar políticas basadas en recursos de AWS, roles de IAM de entre cuentas o el servicio AWS Organizations para permitir que las entidades principales de otras cuentas obtengan acceso a los recursos de su cuenta.

Para algunos servicios de AWS, los administradores pueden conceder acceso entre cuentas a los recursos. Para ello, un administrador de asocia una política directamente al recurso que desea compartir, en lugar de usar un rol como proxy. Si el servicio admite este tipo de política, el recurso que el administrador comparte también debe ser compatible con las políticas basadas en recursos. A diferencia de una política basada en usuarios, una política basada en recursos especifica quién (en una lista de números de ID de cuenta de AWS) pueden obtener acceso a dicho recurso. Global Accelerator no admite políticas basadas en recursos de.

El acceso entre cuentas con una política basada en recursos tiene algunas ventajas sobre el uso de un rol. Con un recurso al que se obtiene acceso a través de una política basada en recursos, la entidad principal (persona o aplicación) sigue trabajando en la cuenta de confianza y no tiene que renunciar a sus permisos de usuario en favor de los permisos del rol. En otras palabras, la entidad principal tiene acceso al mismo tiempo a los recursos de la cuenta de confianza y también a los de la cuenta que confía. Esto resulta útil para tareas como copiar información de una cuenta a otra. Para obtener más información acerca del uso de roles entre cuentas, consulteProporcionar acceso a un usuario de IAM a otra cuenta de AWS de de la que es propietarioen laGuía del usuario de IAM.

AWS Organizations ofrecen administración basada en políticas para varias cuentas de AWS de de de su propiedad. Con Organizations, puede crear grupos de cuentas, automatizar la creación de cuentas y aplicar y administrar las políticas de esos grupos. Organizations le permiten administrar las políticas de forma centralizada para varias cuentas de, sin scripts personalizados ni procesos manuales. Con AWS Organizations, puede crear políticas de control de servicio (SCP) que centralizan el control del uso de los servicios de AWS en varias cuentas de AWS. Para obtener más información, consulte¿Qué son las AWS Organizations?en laGuía del usuario de AWS Organizations.

¿Qué son las políticas?

Para controlar el acceso en AWS, cree políticas y asócielas a identidades de IAM o recursos de AWS.

> **Note**
>
> Para comenzar a utilizar el servicio rápidamente, puede omitir esta página. En primer lugar, revise la información introductoria deAdministración de identidades y accesos para AWS Global Acceleratory, a continuación, consulteIntroducción a IAM.

Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal, como un usuario, realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, si una política permite que elGetUserA continuación, un usuario con dicha política puede obtener información de los usuarios desde la consola de administración de AWS o la CLI o la API de AWS. Cuando se crea un usuario de IAM, se le puede configurar para permitirle el acceso a la consola o el acceso mediante programación. Los usuarios de IAM pueden iniciar sesión en la consola con un nombre de usuario y una contraseña. O bien pueden utilizar claves de acceso para trabajar con la CLI o la API.

Los siguientes tipos de políticas, enumerados en orden de frecuencia, pueden afectar a si se autoriza o no una solicitud. Para obtener más información, consulte .Tipos de políticasen laGuía del usuario de IAM.

Políticas basadas en identidad

Puede asociar políticas administradas e insertadas a identidades de IAM (usuarios, grupos a los que pertenecen los usuarios y roles).

Políticas basadas en recursos

Puede asociar políticas insertadas a los recursos de algunos servicios de AWS. Los ejemplos más comunes de políticas basadas en recursos son las políticas de bucket de Amazon S3 y las políticas de confianza de roles de IAM. Global Accelerator no admite políticas basadas en recursos de.

Organizations SCP

Organizaciones Puede utilizar una política de control de servicios (SCP) de AWS para aplicar un límite de permisos a una organización o unidad organizativa (OU) de AWS. Estos permisos se aplican a todas las entidades que pertenecen a las cuentas miembro.

Listas de control de acceso (ACL)

Puede usar ACL para controlar qué entidades principales pueden tener acceso a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque son el único tipo de política que no utiliza la estructura de los documentos de política JSON. El Acelerador Global admite O no admite ACL.

Estos tipos de políticas se pueden clasificar como políticas de permisos o límites de permisos.

Políticas de permisos

Puede asociar políticas de permisos a un recurso de AWS para definir los permisos de ese objeto. AWS evalúa conjuntamente todas las políticas de permisos de una cuenta. Las políticas de permisos son las políticas más comunes. Puede utilizar los tipos de políticas siguientes como políticas de permisos:

Políticas basadas en identidad

Al asociar una política administrada o insertada a un usuario, grupo o rol de IAM, la política define los permisos de esa entidad.

Políticas basadas en recursos

Cuando se asocia un documento de política JSON a un recurso, se definen los permisos de dicho recurso. El servicio debe ser compatible con las políticas basadas en recursos.

Listas de control de acceso (ACL)

Cuando se asocia una ACL a un recurso, se define una lista de entidades principales con permiso para obtener acceso a dicho recurso. El recurso debe ser compatible con las ACL.

Límites de permisos

Puede usar políticas para definir el límite de permisos de una entidad (usuario o rol). Un límite de permisos controla los permisos máximos que puede tener una entidad. Los límites de permisos son una característica avanzada de AWS. Cuando se aplican varios límites de permisos a una

solicitud, AWS evalúa cada límite de permisos por separado. Puede aplicar un límite de permisos en las situaciones siguientes:

Organizaciones

Organizaciones Puede utilizar una política de control de servicios (SCP) de AWS para aplicar un límite de permisos a una organización o unidad organizativa (OU) de AWS.

Usuarios o roles de IAM

Puede utilizar una política administrada para el límite de permisos de un usuario o un rol. Para obtener más información, consulteLímites de permisos para las entidades de IAMen laGuía del usuario de IAM.

Temas

- Políticas basadas en identidad
- Políticas basadas en recursos
- Clasificaciones de nivel de acceso a directivas

Políticas basadas en identidad

Puede asociar políticas a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

Asociar una política de permisos a un usuario o grupo de su cuenta

Asociar una política de permisos a un usuario para crear un recurso de AWS Global Accelerator, como un acelerador, puede asociar una política de permisos a un usuario o a un grupo al que pertenezca el usuario.

Asociar una política de permisos a un rol (conceder permisos entre cuentas)

Puede asociar una política de permisos basada en identidad a un rol de IAM para conceder permisos entre cuentas. Por ejemplo, el administrador de la cuenta A puede crear un rol para conceder permisos entre cuentas a otra cuenta de AWS (por ejemplo, la cuenta B) o un servicio de AWS como se indica a continuación:

1. Cuenta El administrador de la Cuenta A crea un rol de IAM y asocia una política de permisos a dicho rol, que concede permisos sobre los recursos de la cuenta A.
2. El administrador de la cuenta A asocia una política de confianza al rol que identifica la cuenta B como la entidad principal que puede asumir el rol.

3. A continuación, el administrador de la cuenta B puede delegar permisos para asumir el rol a cualquier usuario de la cuenta B. De este modo, los usuarios de la cuenta B podrán crear recursos y tener acceso a ellos en la cuenta A. La entidad principal de la política de confianza también puede ser la entidad principal de un servicio de AWS si desea conceder permisos para asumir el rol a un servicio de AWS.

Para obtener más información acerca del uso de IAM para delegar permisos, consulteAdministración de accesosen laGuía del usuario de IAM.

Para obtener más información sobre usuarios, grupos, roles y permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

Los siguientes son dos ejemplos de políticas que podría utilizar con el acelerador global. El primer ejemplo de política otorga a un usuario acceso programático a todas las acciones de lista y descripción para aceleradores de su cuenta de AWS:

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

En el siguiente ejemplo se concede acceso mediante programación a la propiedad de`ListAccelerators`.

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

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

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Estas políticas le permiten especificar qué acciones puede realizar una entidad principal especificada en dicho recurso y en qué condiciones. La política basada en recursos más común es para un bucket de Amazon S3. Las políticas basadas en recursos son políticas insertadas que existen únicamente en el recurso. No existen políticas basadas en recursos que sean administradas.

Conceder permisos a los miembros de otras cuentas de AWS mediante una política basada en recursos tiene algunas ventajas respecto al uso de un rol de IAM. Para obtener más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Clasificaciones de nivel de acceso a directivas

En la consola de IAM, las acciones se agrupan utilizando las siguientes clasificaciones de nivel de acceso:

List

Proporciona permiso para enumerar los recursos dentro del servicio con el fin de determinar si existe un objeto. Las acciones con este nivel de acceso pueden enumerar objetos pero no pueden ver el contenido de un recurso. La mayoría de acciones cuyo nivel de acceso es List (Lista) no se puede llevar a cabo en un recurso específico. Al crear una declaración de política con estas acciones, debe especificar All resources (Todos los recursos) (`"*"`).

Lectura

Proporciona permiso para leer, pero no editar, el contenido y los atributos de los recursos del servicio. Por ejemplo, las operaciones de Amazon S3`GetObject`y`GetBucketLocation`Tiene elLecturaNivel de acceso.

Escritura

Proporciona permiso para crear, eliminar o modificar los recursos del servicio. Por ejemplo, las operaciones de Amazon S3`CreateBucket`,`DeleteBucket`, y`PutObject`Tiene elEscrituraNivel de acceso.

Administración de permisos

Proporciona permiso para conceder o modificar permisos en el nivel de recursos del servicio. Por ejemplo, la mayoría de las acciones de política de IAM y AWS Organizations tienen laAdministración de permisosNivel de acceso.

> **Tip**
>
> Para mejorar la seguridad de su cuenta de AWS, limite o monitorice periódicamente las políticas que incluyen elAdministración de permisosclasificación de nivel de acceso.

Etiquetado

Proporciona permiso para crear, eliminar o modificar las etiquetas que están asociadas a un recurso del servicio. Por ejemplo, Amazon EC2`CreateTagsy``DeleteTags`tienen elEtiquetadoNivel de acceso.

Introducción a IAM

AWS Identity and Access Management (IAM) es un servicio de AWS que le permite administrar de forma segura el acceso a los servicios y recursos de. La IAM es una característica de la cuenta de AWS que se ofrece sin cargo adicional.

> **Note**
>
> Antes de comenzar a usar la IAM, revise la información introductoria enAdministración de identidades y accesos para AWS Global Accelerator.

Cuando crea por primera vez una cuenta de AWS, comienza únicamente por una identidad de inicio de sesión único que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la cuenta de AWS y para obtener acceso a ella se inicia sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Le recomendamos encarecidamente que no utilice el usuario raíz en sus tareas cotidianas, ni siquiera en las tareas administrativas. En lugar de ello, es mejor ceñirse a la práctica recomendada de utilizar el usuario final exclusivamente para crear al primer usuario de IAM. A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilícelas tan solo para algunas tareas de administración de cuentas y servicios.

Cree su usuario administrador de IAM

Para crearse usted mismo un usuario administrador y agregarlo a un grupo de administradores (consola)

1. Inicie sesión en la consola de IAM como propietario de la cuenta seleccionando Root user (Usuario raíz) y escribiendo la dirección de correo electrónico de su cuenta de AWS. En la siguiente página, escriba su contraseña.

   > **Note**
   >
   > Le recomendamos que siga la práctica recomendada de utilizar la**`Administrator`**Usuario de IAM que sigue y bloquea de forma segura las credenciales de usuario raíz. Inicie sesión como usuario raíz únicamente para realizar algunas tareas de administración de servicios y de cuentas.

2. En el panel de navegación, elija Users (Usuarios) y, a continuación, elija Add user (Añadir usuario).
3. En User name (Nombre de usuario), escriba **`Administrator`**.
4. Active la casilla de verificación situada junto al AWS Management Console access (Acceso a la consola de administración de AWS). A continuación, seleccione Custom password (Contraseña personalizada) y luego escriba la nueva contraseña en el cuadro de texto.
5. (Opcional) De forma predeterminada, AWS requiere que el nuevo usuario cree una nueva contraseña la primera vez que inicia sesión. Puede quitar la marca de selección de la casilla de verificación situada junto a User must create a new password at next sign-in (El usuario debe crear una nueva contraseña en el siguiente inicio de sesión) para permitir al nuevo usuario restablecer su contraseña después de iniciar sesión.
6. SeleccionarSiguiente: Permisos.
7. En Set permissions (Establecer persmisos), elija Add user to group (Añadir usuario a grupo).
8. Elija Create group (Crear grupo).
9. En el cuadro de diálogo Create group (Crear grupo), en Group name (Nombre del grupo) escriba **`Administrators`**.
10. SeleccionarPolíticas de filtroy, a continuación, seleccioneAWS administrado - función de trabajopara filtrar el contenido de la tabla.
11. En la lista de políticas, active la casilla de verificación AdministratorAccess. A continuación, elija Create group (Crear grupo).

> **Note**
>
> Debe activar el acceso de usuario y rol de IAM a Facturación antes de poder utilizar los permisos `AdministratorAccess` para acceder a la consola de AWS Billing and Cost Management. Para ello, siga las instrucciones que se indican en el paso 1 del tutorial sobre cómo delegar el acceso a la consola de facturación.

12. Retroceda a la lista de grupos y active la casilla de verificación del nuevo grupo. Elija Refresh si es necesario para ver el grupo en la lista.
13. SeleccionarSiguiente: Tags (Etiquetas):.
14. (Opcional) Añadir metadatos al rol asociando las etiquetas como pares de clave-valor. Para obtener más información sobre el uso de etiquetas en IAM, consulte Etiquetado de entidades de IAM en la guía del usuario de IAM.
15. SeleccionarSiguiente: Review (Revisar)Para ver la lista de suscripciones a grupos que se agregarán al nuevo usuario. Cuando esté listo para continuar, elija Create user (Crear usuario).

Puede usar este mismo proceso para crear más grupos y usuarios, y para conceder a los usuarios acceso los recursos de su cuenta de AWS. Para obtener información sobre cómo usar las políticas que restringen los permisos de los usuarios a recursos de AWS específicos, consulte Administración de acceso y Políticas de ejemplo.

Crear usuarios delegados para Global Accelerator

Para admitir varios usuarios en su cuenta de AWS, debe delegar el permiso para permitir que otras personas realicen solo las acciones que desea permitir. Para ello, cree un grupo de IAM con los permisos que esas personas necesitan y, a continuación, añada usuarios de IAM a los grupos necesarios al crearlos. Puede utilizar este proceso para configurar los grupos, usuarios y permisos de toda su cuenta de AWS. Esta solución es la mejor opción utilizada por pequeñas y medianas organizaciones donde un administrador de AWS puede administrar manualmente usuarios y grupos. Para organizaciones grandes, puede usarRoles de IAM personalizados,federación, o bienInicio de sesión único de.

En el siguiente procedimiento, creará tres usuarios denominados**`arnav`**,**`carlos`**, y**`martha`**y adjuntar una directiva que concede permiso para crear un acelerador llamado**`my-example-accelerator`**, pero sólo dentro de los próximos 30 días. Puede utilizar los pasos indicados aquí para añadir usuarios con diferentes permisos.

Para crear un usuario delegado para otra persona (consola)

1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, elija Users y luego elija la opción Add user.
3. En User name (Nombre de usuario), escriba **arnav**.
4. Seleccione Add another user (Añadir otro usuario) y escriba **carlos** para el segundo usuario. A continuación, seleccione Add another user (Añadir otro usuario) y escriba **martha** para el tercer usuario.
5. Marque la casilla situada junto aAWS Management Console accessy, a continuación, seleccionecontraseña generada automáticamente.
6. Quite la marca de selección de la casilla de verificación situada junto a User must create a new password at next sign-in (El usuario debe crear una nueva contraseña en el siguiente inicio de sesión) para permitir al nuevo usuario restablecer su contraseña después de iniciar sesión.
7. SeleccionarSiguiente: Permisos.
8. Elija Attach existing policies directly. Creará una política administrada para los usuarios.
9. Elija Create Policy.

   Se abre el asistente Create policy (Crear política) en una nueva pestaña o ventana del navegador.
10. En la pestaña Visual editor (Editor visual), seleccione Choose a service (Elegir un servicio). A continuación, elija Global Accelerator. Puede utilizar el cuadro de búsqueda en la parte superior para limitar los resultados en la lista de servicios.

    LaService (Servicio)se cierra, y la secciónActionsse abre automáticamente.
11. Elija las acciones del Acelerador Global que desea permitir. Por ejemplo, para conceder permiso para crear un acelerador, escriba**globalaccelerator:CreateAccelerator**en laAcciones de filtro(Cuadro de texto). Cuando la lista de acciones del acelerador global se haya filtrado, active la casilla de verificación situada junto a**globalaccelerator:CreateAccelerator**.

    Las acciones del Acelerador global se agrupan según su clasificación de nivel de acceso para que le resulte más fácil determinar rápidamente el nivel de acceso que cada acción proporciona. Para obtener más información, consulte Clasificaciones de nivel de acceso a directivas.
12. Si las acciones que ha seleccionado en los pasos anteriores no admiten la elección de recursos específicos,Todos los recursosestá seleccionado para usted. En ese caso, no puede editar esta sección.

Si eligió una o más acciones que admiten permisos en el nivel de recursos, el editor visual enumera dichos tipos de recursos en la sección Resources (Recursos). SeleccionarHa elegido acciones que requierenAcelerador deTipo de recurso dePara elegir si desea introducir un acelerador específico para la política.

13. Si desea permitir la acción `globalaccelerator:CreateAccelerator` para todos los recursos, elija All resources (Todos los recursos).

    Si desea especificar un recurso, elija Add ARN (Añadir ARN). Especifique la región y el ID de cuenta (o ID de cuenta) (o elijaCualquiera) y, a continuación, escriba**`my-example-accelerator`**para el recurso. A continuación, elija Add (Añadir).
14. Elija Specify request conditions (optional) (Especificar condiciones de solicitud (opcional)).
15. SeleccionarAñadir condiciónOtorga permiso para crear un aceleradoren los próximos siete días. Supongamos que la fecha de hoy es el 1 de enero de 2019.
16. En Condition Key (Clave de condición), elija aws:CurrentTime. Esta clave de condición comprueba la fecha y la hora en que el usuario realiza la solicitud. Devuelve true (y, por lo tanto, permite la acción **`globalaccelerator:CreateAccelerator`**) solo si la fecha y la hora están comprendidas en el intervalo especificado.
17. ParaQualifier, mantenga el valor predeterminado.
18. Para especificar el inicio del intervalo de fecha y hora permitido, en Operator (Operador), elija DateGreaterThan. A continuación, en Value (Valor) escriba **`2019-01-01T00:00:00Z`**.
19. Elija Add (Añadir) para guardar la condición.
20. Elija Add another condition (Añadir otra condición) para especificar la fecha de finalización.
21. Realice un procedimiento similar para especificar el final del intervalo de fecha y hora permitido. En Condition Key (Clave de condición), elija aws:CurrentTime. En Operator (Operador), elija DateLessThan. En Value (Valor), escriba **`2019-01-06T23:59:59Z`**, siete días después de la primera fecha. A continuación, elija Add (Añadir) para guardar la condición.
22. (Opcional) Para ver el documento de política JSON de la política que está creando, elija laJSON. Puede alternar entre las pestañas Visual editor (Editor visual) y JSON en cualquier momento. Sin embargo, si realiza cambios o eligePolítica de revisiónen laVisual editor (Editor visual), IAM podría reestructurar la política para optimizarla para el editor visual. Para obtener más información, consulteReestructuración de políticasen laGuía del usuario de IAM.
23. Cuando haya terminado, seleccione Review policy.
24. En la páginaPolítica de revisiónPágina, paraNombre, introduzca**`globalaccelerator:CreateAcceleratorPolicy`**. En Descripción, escriba

`Policy to grants permission to create an accelerator`. Revise el resumen de política para asegurarse de que ha concedido los permisos deseados y, a continuación, elija Create policy (Crear política) para guardar su nueva política.

25. Vuelva a la pestaña o ventana original y actualice la lista de políticas.
26. En el cuadro de búsqueda, escriba **`globalaccelerator:CreateAcceleratorPolicy`**. Seleccione la casilla de verificación situada junto a la nueva política. A continuación, elija Next Step.
27. SeleccionarSiguiente: Review (Revisar)Para obtener una vista previa de sus nuevos usuarios. Cuando esté listo para continuar, elija Create users (Crear usuarios).
28. Descargue o copie las contraseñas de nuevos usuarios y entréguelas a los usuarios de forma segura. Por separado, proporcione a sus usuarios unenlace a la página de la consola de usuario de IAMy los nombres de usuario de que acaba de crear.

Permitir a los usuarios de administrar ellos mismos sus credenciales

Debe tener acceso físico al hardware que alojará el dispositivo MFA virtual del usuario para poder configurar la MFA. Por ejemplo, puede configurar MFA para un usuario que use un dispositivo MFA virtual que se ejecute en un smartphone. En ese caso, debe tener el smartphone disponible para completar el asistente. Por este motivo, puede interesarle que los usuarios puedan configurar y administrar sus propios dispositivos MFA virtuales. En ese caso, debe conceder a los usuarios los permisos necesarios para realizar las acciones de IAM necesarias.

Para crear una política que permita a los usuarios administrar sus propias credenciales (consola)

1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Policies (Políticas) y, a continuación, seleccione Create policy (Crear política).
3. Seleccione la pestaña JSON y copie el texto del siguiente documento de política JSON. Pegue el texto en el cuadro de texto JSON.

> **Important**
>
> Este ejemplo de política no permite a los usuarios restablecer sus contraseñas al iniciar sesión. Los nuevos usuarios y los usuarios que tengan una contraseña caducada podrían intentar hacerlo. Puede permitir esto añadiendo

`iam:ChangePassword` y `iam:CreateLoginProfile` a la instrucción `BlockMostAccessUnlessSignedInWithMFA`. Sin embargo, IAM no recomienda esto.

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

¿Qué hace esta política?

- LaAllowAllUsersToListAccountspermite al usuario ver información básica sobre la cuenta y sus usuarios en la consola de IAM. Estos permisos deben estar en su propia instrucción, ya que no admiten o no es necesario que especifique un ARN de recurso específico y, en su lugar, se especifica `"Resource" : "*"`.
- LaAllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformationLa instrucción permite al usuario administrar sus propias claves de acceso, contraseña, usuario, certificados de inicio de sesión, las claves públicas SSH e información de MFA en la consola de IAM. También permite a los usuarios iniciar sesión por primera vez si un administrador exige que establezcan una contraseña de primera vez. El recurso ARN limita el uso de estos permisos únicamente a la propia entidad de usuario de IAM del usuario.
- La instrucción `AllowIndividualUserToViewAndManageTheirOwnMFA` permite al usuario ver o administrar su propio dispositivo MFA. Tenga en cuenta que los ARN de recurso de esta instrucción permiten el acceso únicamente a un dispositivo MFA o a un usuario que tenga el mismo nombre que el usuario que ha iniciado sesión en ese momento. Los usuarios no pueden crear ni modificar un dispositivo MFA que no sea el suyo.
- La instrucción `AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA` permite al usuario desactivar solo su propio dispositivo MFA y solo si el usuario ha iniciado sesión

utilizando MFA. Esto impide que otras personas con solo las claves de acceso (y no el dispositivo MFA) desactiven el dispositivo MFA y accedan a la cuenta.

- `LaBlockMostAccessUnlessSignedInWithMFA`utiliza una combinación de`"Deny"y"NotAction"`para denegar el acceso a todas las acciones excepto algunas en IAM y otros servicios de AWSifel usuario no ha iniciado sesión con MFA. Para obtener más información acerca de la lógica de esta instrucción, consulteNotAction con Denyen laGuía del usuario de IAM. Si el usuario inicia sesión con MFA, se producirá un error en la prueba `"Condition"`, la instrucción final "deny" no tendrá ningún efecto y otras políticas o instrucciones para el usuario determinan los permisos del usuario. Esta instrucción garantiza que cuando el usuario no ha iniciado sesión con MFA pueda realizar solo las acciones indicadas y solo si otra instrucción o política permite el acceso a estas acciones.

  La versión `...IfExists` del operador `Bool` garantiza que si falta la clave `aws:MultiFactorAuthPresent`, la condición devuelve el valor verdadero. Esto significa que a un usuario que accede a una API con credenciales a largo plazo, como una clave de acceso, se le deniega el acceso a las operaciones de la API que no son de IAM.

4. Cuando haya terminado, seleccione Review policy.
5. En la página Review (Revisar), escriba **`Force_MFA`** como nombre de la política. En la descripción de la política, escriba**`This policy allows users to manage their own passwords and MFA devices but nothing else unless they authenticate with MFA.`**Consulte la políticaResumenPara ver los permisos concedidos por la política y, a continuación, elijaCrear políticapara guardar su trabajo.

   La nueva política aparece en la lista de las políticas administradas y está lista para asociar.

Para asociar la política a un usuario (consola)

1. En el panel de navegación, seleccione Users.
2. Elija el nombre (no la casilla) del usuario que desee editar.
3. En la pestaña Permissions (Permisos), seleccione Add permissions (Añadir permisos).
4. Elija Attach existing policies directly.
5. En el cuadro de búsqueda, escriba **`Force`** y, a continuación, seleccione la casilla de verificación junto a Force_MFA en la lista. A continuación, elija Next (Siguiente): Review (Revisar).
6. Revise los cambios y seleccione Add permissions (Añadir permisos).

Habilitar la MFA para su usuario de IAM

Para más seguridad, le recomendamos que todos los usuarios de IAM configuren la autenticación multifactor (MFA) para ayudar a proteger sus recursos de Global Accelerator. MFA aporta seguridad adicional, ya que exige a los usuarios que proporcionen una autenticación exclusiva obtenida de un dispositivo de MFA admitido por AWS, además de sus credenciales de inicio de sesión habituales. El dispositivo AWS MFA más seguro para es la clave de seguridad U2F. Si su empresa ya utiliza dispositivos U2F, le recomendamos que habilite esos dispositivos para AWS. De lo contrario, debe adquirir un dispositivo para cada uno de sus usuarios y esperar a recibir el hardware. Para obtener más información, consulteHabilitación de una llave de seguridad U2Fen laGuía del usuario de IAM.

Si aún no tiene un dispositivo U2F, puede comenzar a trabajar de manera rápida y a un costo bajo habilitando un dispositivo MFA virtual. Para ello, debe instalar una aplicación de software en un teléfono u otro dispositivo móvil que ya tenga. El dispositivo genera un código de seis dígitos basándose en un algoritmo de contraseña de uso único y sincronización de tiempo. Cuando el usuario inicia sesión en AWS, se le solicita que introduzca un código en el dispositivo. Cada dispositivo MFA virtual asignado a un usuario debe ser único. Un usuario no puede escribir un código desde el dispositivo MFA virtual de otro usuario para autenticarse. Para ver una lista de algunas aplicaciones compatibles que puede utilizar como dispositivo MFA virtual, consulte Autenticación multifactor.

> **Note**
>
> Debe tener acceso físico al dispositivo móvil que alojará el dispositivo de MFA virtual del usuario para poder configurar la MFA para un usuario de IAM.

Para habilitar un dispositivo de MFA virtual para un usuario de IAM (consola)

1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Users.
3. En la lista User Name (Nombre de usuario), elija el nombre del usuario de MFA previsto.
4. Seleccione la pestaña de credenciales de seguridad. Al lado de Assigned MFA device (Dispositivo MFA asignado), seleccione Manage (Administrar).
5. En el asistente Manage MFA Device (Administrar dispositivo MFA), elija Virtual MFA device (Dispositivo MFA virtual) y, a continuación, elija Continue (Continuar).

IAM generará y mostrará la información de configuración del dispositivo de MFA virtual, incluido un gráfico de código QR. El gráfico es una representación de la "clave de configuración secreta" que se puede introducir manualmente en dispositivos que no admiten códigos QR.

6. Abra su aplicación de MFA virtual.

   Para ver una lista de las aplicaciones que puede utilizar para alojar dispositivos MFA virtuales, consulte Multi-Factor Authentication. Si la aplicación de MFA virtual admite varias cuentas (varios dispositivos de MFA virtuales), elija la opción para crear una nueva cuenta (un nuevo dispositivo MFA virtual).

7. Determine si la aplicación MFA admite códigos QR y, a continuación, lleve a cabo alguna de las siguientes operaciones:

   - Desde el asistente, elija Show QR code (Mostrar código QR) y, a continuación, utilice la aplicación para escanear el código QR. Por ejemplo, puede elegir el icono de la cámara o una opción similar a Scan code (Escanear código) y, a continuación, utilizar la cámara del dispositivo para escanear el código.
   - En el asistente Manage MFA Device (Administrar dispositivo MFA), elija Show secret key (Mostrar clave secreta) y, a continuación, escriba la clave secreta en su aplicación de MFA.

   Cuando haya terminado, el dispositivo MFA virtual comenzará a generar contraseñas de uso único.

8. En el asistente Manage MFA Device (Administrar dispositivo MFA), en el cuadro MFA code 1 (Código MFA 1) escriba la contraseña de uso único que aparece actualmente en el dispositivo MFA virtual. Espere hasta 30 segundos a que el dispositivo genere una nueva contraseña de uso único. A continuación, escriba la otra contraseña de uso único en el cuadro MFA code 2 (Código MFA 2). Elija Assign MFA (Asignar MFA).

   > **Important**
   >
   > Envíe su solicitud inmediatamente después de generar los códigos. Si genera los códigos y después espera demasiado tiempo a enviar la solicitud, el dispositivo MFA se asociará correctamente al usuario, pero no estará sincronizado. Esto ocurre porque las contraseñas de un solo uso basadas en el tiempo (TOTP) caducan tras un corto periodo de tiempo. Si esto ocurre, puede volver a sincronizar el dispositivo. Para obtener más

información, consulteResincronización de dispositivos MFA físicos y virtualesen laGuía del usuario de IAM.

Ahora el dispositivo MFA virtual ya está listo para usarlo con AWS.

Conexiones VPC seguras en AWS Global Accelerator

Cuando agrega un Application Load Balancer interno o un extremo de instancia de Amazon EC2 en AWS Global Accelerator, habilita el tráfico de Internet para que fluya directamente hacia y desde el extremo en las nubes privadas virtuales (VPC) segmentándolo en una subred privada. La VPC que contiene el balanceador de carga o la instancia EC2 debe tener ungateway de Internetadjunta a él, para indicar que la VPC acepta tráfico de Internet. Sin embargo, no necesita direcciones IP públicas en el equilibrador de carga o en la instancia EC2. Tampoco necesita una ruta de puerta de enlace de Internet asociada para la subred.

Esto es diferente del caso de uso típico de la puerta de enlace de Internet en el que se requieren tanto direcciones IP públicas como rutas de puerta de enlace de Internet para que el tráfico de Internet fluya a instancias o equilibradores de carga en una VPC. Incluso si las interfaces de red elásticas de sus destinos están presentes en una subred pública (es decir, una subred con una ruta de puerta de enlace de Internet), cuando utiliza Global Accelerator para el tráfico de Internet, Global Accelerator anula la ruta típica de Internet y todas las conexiones lógicas que llegan a través de la El acelerador también regresa a través del acelerador global en lugar de a través de la puerta de enlace de Internet

> **Note**
>
> El uso de direcciones IP públicas y el uso de una subred pública para sus instancias de Amazon EC2 no son típicos, aunque es posible configurar su configuración con ellas. Los grupos de seguridad se aplican a cualquier tráfico que llegue a sus instancias, incluido el tráfico de Global Accelerator y cualquier dirección IP pública o elástica asignada a su instancia ENI. Utilice subredes privadas para asegurarse de que el tráfico sólo lo entregue Global Accelerator.

Tenga en cuenta esta información cuando considere problemas de perímetro de la red y configure los privilegios de IAM relacionados con la administración del acceso a Internet. Para obtener más

información sobre el control de acceso a Internet a la VPC, consulte estaEjemplo de política de control de servicios.

Registro y monitorización en AWS Global Accelerator

La monitorización es una parte importante del mantenimiento de la disponibilidad y el rendimiento de Global Accelerator y sus soluciones de AWS. Debe recopilar datos de monitorización de todas las partes de su solución de AWS para que le resulte más sencillo depurar un error que se produce en distintas partes del código, en caso de que ocurra. AWS proporciona varias herramientas para monitorear sus recursos de Global Accelerator y responder a posibles incidentes.

Registros de flujo de AWS Global Accelerator

Los registros de flujo de servidor proporcionan registros detallados sobre el tráfico que fluye a través de un acelerador hasta un punto final. Los registros de flujo de servidor son útiles para muchas aplicaciones. Por ejemplo, la información del registro de flujo puede ser útil en auditorías de acceso y seguridad. Para obtener más información, consulte Registros de flujo en AWS Global Accelerator.

Métricas y alarmas de Amazon CloudWatch

Con CloudWatch, puede supervisar, en tiempo real, los recursos y las aplicaciones de AWS que se ejecutan en AWS. CloudWatch recopila y realiza un seguimiento de las métricas, que son variables que se miden a lo largo del tiempo. Puede crear alarmas que vigilen métricas específicas y enviar notificaciones o realizar cambios automáticamente en los recursos que está monitoreando cuando la métrica excede un determinado umbral durante un período de tiempo. Para obtener más información, consulte Uso de Amazon CloudWatch con el AWS Global Accelerator.

Logs de AWS CloudTrail

CloudTrail proporciona un registro de las medidas adoptadas por un usuario, un rol o un servicio de AWS en el Acelerador global. CloudTrail captura todas las llamadas a la API de Global Accelerator como eventos, incluidas las llamadas procedentes de la consola de Global Accelerator y las llamadas de código a la API de Global Accelerator. Para obtener más información, consulte Uso de AWS CloudTrail para registrar las llamadas a la API de AWS Global Accelerator.

Validación de conformidad en AWS Global Accelerator

Auditores externos evalúan la seguridad y la conformidad del AWS Global Accelerator en distintos programas de conformidad de AWS. Esto incluye SOC, PCI, HIPAA, GDPR, ISO y ENS High.

Para obtener una lista de los servicios de AWS, incluido el acelerador global, en el ámbito de programas de conformidad específicos, consultePrograma de conformidad de servicios de AWS en el ámbito del programa. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulteDescarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar Global Accelerator se determina en función de la confidencialidad de los datos, los objetivos de conformidad de su empresa, así como de la legislación y los reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad– estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Documento técnico sobre arquitectura para seguridad y conformidad de HIPAA– este documento técnico describe cómo las empresas pueden utilizar AWS para crear aplicaciones conformes con HIPAA.
- Recursos de conformidad de AWS– este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio de AWS Config evalúa en que medida las configuraciones de recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- Centro de seguridad de AWS– este servicio de AWS ofrece una vista integral de su estado de seguridad en AWS que le ayuda a comprobar la conformidad con las normas del sector de seguridad y las prácticas recomendadas.

Resiliencia en AWS Global Accelerator

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. Las regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes

y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre zonas de disponibilidad y las regiones de AWS, consulte Infraestructura global de AWS.

Además de la compatibilidad con la infraestructura global de AWS, el acelerador global ofrece las siguientes características que le ayudan con la resiliencia de los datos:

- Una zona de red proporciona servicios a las direcciones IP estáticas del acelerador desde una subred IP única. Al igual que una zona de disponibilidad de AWS, una zona de red es una unidad aislada con su propio conjunto de infraestructura física. Cuando configura un acelerador, Global Accelerator asigna dos direcciones IPv4 para él. Si una dirección IP de una zona de red deja de estar disponible debido al bloqueo de direcciones IP por determinadas redes cliente, o debido a interrupciones en la red, las aplicaciones cliente pueden volver a intentar la dirección IP estática en buen estado desde la otra zona de red aislada.
- Global Accelerator monitoriza continuamente el estado de todos los puntos finales. Cuando determina que un endpoint activo no está en buen estado, Global Accelerator comienza instantáneamente a dirigir el tráfico a otro endpoint disponible. Esto le permite crear una arquitectura de alta disponibilidad para sus aplicaciones en AWS.

Seguridad de la infraestructura en AWS Global Accelerator

Al tratarse de un servicio administrado, el AWS Global Accelerator está protegido por los procedimientos de seguridad de red globales de AWS, que se describen en laAmazon Web Services: Información general de los procesos de seguridadDocumento técnico.

Puede utilizar llamadas a la API publicadas de AWS para obtener acceso a Global Accelerator a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.0 o una versión posterior. Le recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos. Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta

que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Cuotas para AWS Global Accelerator

Su cuenta de AWS tiene cuotas específicas, también conocidas como límites, relacionadas con AWS Global Accelerator.

La consola Service Quotas proporciona información sobre las cuotas de Global Accelerator. Además de ver las cuotas predeterminadas, puede utilizar la consola Service Quotas paraaumento de la cuota de solicitudpara las cuotas ajustables. Tenga en cuenta que debe estar en EE.UU. Este (Norte de Virginia) cuando solicite aumentos de cuota para Global Accelerator.

Temas

Cuotas generales

Las siguientes son las cuotas generales para Global Accelerator.

Entidad	Cuota
Acceleradores por cuenta de AWS	20 Puede hacer lo siguientePara solicitar un aumento de cuota.
Listeners por acelerador	10 Puede hacer lo siguientePara solicitar un aumento de cuota.
Rangos de puertos por oyente	10
Sobrescritura de puerto por grupo de endpoints	10 Puede hacer lo siguientePara solicitar un aumento de cuota.

Cuotas para endpoints por grupo de endpoints

A continuación se indican las cuotas de Global Accelerator que se aplican al número de endpoints en grupos de endpoints.

Entidad	Descripción	Cuota
Grupos de puntos de enlace con más de un tipo de punto de enlace	Número de extremos en un grupo de extremos que contiene más de un tipo de extremo.	10
Grupos de endpoints con equilibradores de carga de aplicaciones	Número de equilibradores de carga de aplicaciones en un grupo de extremos que contiene sólo los extremos del Application Load Balancer.	10
Grupos de endpoints con equilibradores de carga de red	Número de equilibradores de carga de red en un grupo de extremos que contiene sólo los extremos del Network Load Balancer.	10
Grupos de puntos de enlace con instancias Amazon EC2	Número de instancias EC2 en un grupo de puntos de enlace que contiene sólo los puntos de enlace de instancia EC2.	10 Puede hacer lo siguiente Para solicitar un aumento de cuota.
Grupos de endpoints con solo direcciones IP elásticas	Número de direcciones IP elásticas en un grupo de extremos que contiene sólo los extremos de direcciones IP elásticas .	10 Puede hacer lo siguiente Para solicitar un aumento de cuota.
Grupos de puntos de enlace con las subredes de Amazon Virtual Private Cloud	Número de subredes de Amazon VPC en un grupo de extremos que contiene únicamente puntos finales de subred.	10 Puede hacer lo siguiente Para solicitar un aumento de cuota.

Cuotas afines

Además de las cuotas en Global Accelerator, existen cuotas que se aplican a los recursos que utiliza como puntos de enlace para un acelerador. Para obtener más información, consulte los siguientes temas:

- Cuotas de direcciones IP elásticasen laGuía del usuario de Amazon EC2.
- Cuotas de servicio Amazon EC2en laGuía del usuario de Amazon EC2.
- Cuotas para los balanceadores de carga de reden laGuía del usuario para Network Load Balancers.
- Cuotas de los balanceadores de carga de aplicacionesen laGuía del usuario para Application Load Balancers.
- Cuotas de Amazon VPCen laGuía del usuario de Amazon VPC.

Información relacionada con AWS Global Accelerator

La información y los recursos que se enumeran aquí pueden ayudarle a obtener más información acerca de Global Accelerator.

Temas

- Documentación adicional de AWS Global Accelerator
- Cómo obtener soporte
- Consejos del blog de Amazon Web Services

Documentación adicional de AWS Global Accelerator

Los recursos relacionados siguientes pueden serle de ayuda cuando trabaje con este servicio.

- Referencia de la API de AWS Global Accelerator: ofrece descripciones completas de las acciones, parámetros y tipos de datos de la API, así como una lista de errores que el servicio devuelve.
- Información del producto AWS Global Accelerator: la página web principal para obtener información acerca de Global Accelerator incluidas características e información sobre precios.
- Términos de usoInformación detallada sobre nuestros derechos de autor y marca comercial, su cuenta, licencia y acceso al sitio, entre otros temas.

Cómo obtener soporte

El Support para Global Accelerator está disponible en varias formas.

- foros de debateForo de la comunidad para desarrolladores donde se tratan aspectos técnicos relacionados con Global Accelerator.
- Centro de soporte de AWS: este sitio aúna información acerca de casos de soporte recientes y resultados de AWS Trusted Advisor y comprobaciones de estado. Además, proporciona enlaces a foros de debate, preguntas técnicas más frecuentes, panel de estado del servicio e información acerca de los planes de soporte de AWS.
- información acerca de AWS Premium Support: página web principal con información acerca de AWS Premium Support, un canal de soporte individualizado y de respuesta rápida que le ayudará a crear y ejecutar aplicaciones en AWS Infrastructure Services.

- Contacte con nosotros: enlaces para hacernos llegar sus preguntas sobre facturación o su cuenta. Para preguntas técnicas, utilice los foros de debate o los enlaces de soporte previamente proporcionados.

Consejos del blog de Amazon Web Services

En el blog de AWS encontrará diversas publicaciones que le ayudarán a utilizar los servicios de AWS. Por ejemplo, consulte las siguientes entradas de blog acerca de Global Accelerator:

- AWS Global Accelerator para disponibilidad y rendimiento
- AWS Global Accelerator
- Análisis y visualización de registros de flujo de AWS Global Accelerator mediante Amazon Athena y Amazon QuickSight

Para obtener una lista completa de los blogs de AWS Global Accelerator, consulteAWS Global Acceleratoren la categoría Entrega de contenido y redes de contenido de las publicaciones de blog de AWS.

Historial de revisión

Las siguientes entradas describen cambios importantes realizados en la documentación de AWS Global Accelerator.

- Versión de la API: la más reciente
- Última actualización de la documentación: 9 de diciembre de 2020

Cambio	Descripción	Fecha
Actualizar a la función vinculada al servicio existente del Acelerador Global	Global Accelerator agregó un nuevo permiso,`ec2:DescribeRegions` , para permitir que Global Accelerator obtenga información sobre la región de AWS para ayudar a diagnosticar errores. Para obtener más información, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/security-iam-awsmanpol-updates.html.	7 de mayo de 2021
Aceleradores de enrutamiento personalizados agregados	Global Accelerator introdujo un nuevo tipo de aceleradores de enrutamiento personalizados de aceleradores. Los aceleradores de enrutamiento personalizados funcionan bien en escenarios en los que desea utilizar la lógica de aplicación personalizada para dirigir a uno o más usuarios a un destino y puerto específicos entre muchos, sin dejar de obtener los beneficios	9 de diciembre de 2020

Cambio	Descripción	Fecha
	de rendimiento de Global Accelerator. Para obtener más información, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/work-with-custom-routing-accelerators.html.	
Agregado soporte para anulaciones de puerto	Global Accelerator ahora admite la anulación del puerto de escucha utilizado para enrutar el tráfico a los endpoints, de modo que pueda redirigir el tráfico a puertos específicos de los endpoints. Para obtener más información, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-port-override.html.	21 de octubre de 2020
Se han añadido dos nuevas regiones	Global Accelerator ahora admite África (Ciudad del Cabo) y Europa (Milán). Para obtener más información, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/preserve-client-ip-address.regions.html.	20 de mayo de 2020

Cambio	Descripción	Fecha
Etiquetado y BYOIP	Esta versión añade compatibilidad con la adición de etiquetas a los aceleradores y la incorporación de su propia dirección IP a AWS Global Accelerator (BYOIP). Para obtener más información, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/tagging-in-global-accelerator.html y https://docs.aws.amazon.com/global-accelerator/latest/dg/using-byoip.html.	27 de febrero de 2020
Capítulo Seguridad actualizada	Contenido añadido para el cumplimiento de normas, la resiliencia y la seguridad de la infraestructura. Para obtener más información, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/security.html.	20 de diciembre de 2019

Cambio	Descripción	Fecha
Support con instancias EC2 y nombre DNS predeterminado	El AWS Global Accelerator ahora admite la adición de instancias EC2 en las regiones de AWS admitidas. Además, Global Accelerator crea un nombre DNS predeterminado que se asigna a las direcciones IP estáticas del acelerador. Para obtener más información, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html y https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.html#about-accelerators.dns-addressing.	29 de octubre de 2019
Conservación de la dirección IP del cliente para equilibradores de carga de aplicaciones	Ahora puede elegir que AWS Global Accelerator preserve la dirección IP del cliente para los equilibradores de carga de aplicaciones en las regiones de AWS admitidas. Para obtener más información, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html.	28 de agosto de 2019

Cambio	Descripción	Fecha
Lanzamiento de AWS Global Accelerator	La Guía para desarrolladores de AWS Global Accelerator proporciona información sobre la configuración y el uso de aceleradores (administradores de tráfico de capa de red) que mejoran la disponibilidad y el rendimiento de las aplicacio nes de Internet que tienen una audiencia global.	26 de noviembre de 2018

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el glosario de AWS en la referencia general de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.