# AWS Global Accelerator

## Guía para desarrolladores

# AWS Global Accelerator: Guía para desarrolladores

# Table of Contents

# ¿Qué es AWS Global Accelerator?

AWS Global Accelerator es un servicio en el que usted crea aceleradores para mejorar la disponibilidad y el rendimiento de sus aplicaciones para usuarios locales y globales. Global Accelerator dirige el tráfico a puntos de enlace óptimos a través de AWS de red global. Esto mejora la disponibilidad y el rendimiento de las aplicaciones de Internet que utiliza un público global. Global Accelerator es un servicio global que admite puntos de enlace en varios AWS Regiones, que se enumeran en la AWS Tabla de regiones.

Por defecto, Global Accelerator le proporciona dos direcciones IP estáticas que asocia a su acelerador. (O, en lugar de utilizar las direcciones IP que Global Accelerator proporciona, puede configurar estos puntos de entrada para que sean direcciones IPv4 de sus propios rangos de direcciones IP que traiga a Global Accelerator.) Las direcciones IP estáticas son Anycast de la AWS de red perimetral y distribuir el tráfico entrante de las aplicaciones a través de múltiples recursos de endpoint en múltiples AWS Regiones, lo que aumenta la disponibilidad de las aplicaciones. Los puntos de enlace pueden ser Network Load Balancersde Application Load Balancersde Amazon EC2 o direcciones IP elásticas que se encuentran en un AWS Región o varias regiones.

> **Important**
>
> Las direcciones IP estáticas permanecen asignadas a su acelerador durante tanto tiempo como exista, incluso si deshabilitas la acelerador y ya no acepta ni dirige el tráfico. Sin embargo, cuando eliminar un acelerador, pierde las direcciones IP estáticas que se le asignan, por lo que ya no puede dirigir el tráfico con ellas. Puede utilizar políticas 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 (p. 72).

Global Accelerator utiliza AWS de red global para dirigir el tráfico al punto de enlace regional óptimo en función del estado, la ubicación del cliente y las políticas que configure. 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 dirija a los puntos de enlace en buen estado.

Para obtener una lista de las AWS Regiones en las que Global Accelerator y otros servicios son compatibles actualmente, consulte la sección AWS Tabla de regiones.

Temas



# Componentes de AWS Global Accelerator

AWS Global Accelerator incluye los siguientes componentes que funcionan juntos para ayudarle a mejorar la disponibilidad y el rendimiento de sus aplicaciones:

Direcciones IP estáticas

Global Accelerator proporciona un conjunto de dos direcciones IP estáticas que son Anycast desde el AWS de red de borde de. Si trae su propio rango de direcciones IP a AWS (BYOIP), puede asignar direcciones IP de su propio grupo para utilizarlas con su acelerador. Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en AWS Global Accelerator (p. 20).

Las direcciones IP sirven como puntos de entrada fijos únicos para sus clientes. Si ya tiene Elastic Load Balancing de balanceadores de carga de , instancias EC2 o recursos de direcciones IP elásticas configurados para sus aplicaciones, puede añadirlos fácilmente a Global Accelerator. Esto permite Global Accelerator para utilizar direcciones IP estáticas para obtener acceso a los recursos de.

Las direcciones IP estáticas permanecen asignadas a su acelerador durante tanto tiempo como exista, incluso si deshabilitas la acelerador y ya no acepta ni dirige el tráfico. Sin embargo, cuando eliminar un acelerador, pierde las direcciones IP estáticas que se le asignan, por lo que ya no puede dirigir el tráfico con ellas. Puede utilizar políticas 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 (p. 72).

Acelerador

Un acelerador dirige el tráfico a puntos de enlace óptimos a través de AWS de red global para mejorar la disponibilidad y el rendimiento de sus aplicaciones de Internet. Cada acelerador incluye uno o varios agentes de escucha.

Nombre de DNS

Global Accelerator asigna cada uno acelerador un nombre de sistema de nombres de dominio (DNS) predeterminado, similar a `a1234567890abcdef.awsglobalaccelerator.com`, que apunta a las direcciones IP estáticas que Global Accelerator le asigna a usted o lo que elija de su propio rango de direcciones IP. En función del caso de uso, puede utilizar las direcciones IP estáticas o el nombre de DNS del acelerador para dirigir el tráfico a su aceleradoro configure registros de DNS para dirigir el tráfico utilizando su propio nombre de dominio personalizado.

Zona de red

La zona de red los servicios de las direcciones IP estáticas de su acelerador desde una subred IP única. Similar a un AWS de disponibilidad, una zona de red es una unidad aislada con su propio conjunto de infraestructura física. Cuando configura un acelerador, de forma predeterminada, Global Accelerator asigna dos direcciones IPv4 para ella. Si una dirección IP de una zona de red deja de estar disponible debido al bloqueo de direcciones IP por parte de determinadas redes cliente o interrupciones de red, las aplicaciones cliente pueden reintentar en la dirección IP estática en buen estado de la otra dirección aislada zona de red.

Listener

Un agente de escucha procesa las conexiones entrantes de los clientes a Global Accelerator, en función del puerto (o rango de puertos) y el protocolo que configure. Global Accelerator admite protocolos TCP y UDP. Cada agente de escucha tiene uno o varios grupos de puntos de enlace asociados y el tráfico se reenvía a los puntos de enlace de uno de los grupos de. Puede asociar grupos de puntos de enlace con agentes de escucha especificando las regiones de a las que desea distribuir el tráfico. El tráfico se distribuye a puntos de enlace óptimos dentro de los grupos de puntos de enlace asociados a un agente de escucha.

Grupo de punto de enlace

Cada grupo de puntos de enlace está asociado a un determinado AWS Región. Los grupos de puntos de enlace incluyen uno o varios puntos de enlace en la región. Puede aumentar o reducir el porcentaje de tráfico que, de lo contrario, se dirigiría a un grupo de puntos de enlace ajustando una configuración denominada marcación de tráfico. La marcación de tráfico le permite realizar fácilmente pruebas de rendimiento o pruebas de implementación blue/green, por ejemplo, para nuevas versiones en diferentes AWS Regiones.

Punto de enlace

Los puntos de enlace pueden ser Network Load Balancersde Application Load Balancers, instancias EC2 o direcciones IP elásticas. Un Balanceador de carga de aplicaciones El punto de enlace de puede ser un expuesto a Internet o interno. El tráfico se direcciona a los puntos de enlace en función de las opciones de configuración que elija, como las ponderaciones de los puntos de enlace. Para cada punto de enlace, puede configurar ponderaciones, que son números que puede utilizar para especificar la proporción de tráfico que se dirigirá a cada uno de ellos. Esto puede ser útil, por ejemplo, para realizar pruebas de rendimiento dentro de una región.

# Funcionamiento de AWS Global Accelerator

AWS Global Accelerator proporciona un conjunto de direcciones IP estáticas que son Anycast desde el AWS de red de borde de. Si usted Traiga su propio rango de direcciones IP (p. 20) de AWS (BYOIP), puede asignar direcciones IP estáticas de su propio grupo para utilizarlas con su acelerador.

Las direcciones IP estáticas sirven como puntos de entrada fijos únicos para sus clientes. Cuando configuras tu acelerador con Global Accelerator, asocia las direcciones IP estáticas a los puntos de enlace regionales—Network Load Balancersde Application Load Balancersde Amazon EC2 o direcciones IP elásticas—en uno o más AWS Regiones. Las direcciones IP estáticas aceptan el tráfico entrante en el AWS La red global de desde la ubicación de borde de que está más cerca de los usuarios de.

Desde la ubicación de borde de , el tráfico de su aplicación se enruta al óptimo AWS punto de enlace basado en varios factores, incluida la ubicación del usuario, el estado del punto de enlace y las ponderaciones del punto de enlace que configure. El tráfico se desplaza por encima de la red redundante, bien monitorizada y sin congestión AWS de red global al punto de enlace. Al maximizar el tiempo que el tráfico está en el AWS de red, Global Accelerator garantiza que el tráfico siempre se dirija a través de la ruta de red óptima.

Con algunos tipos de puntos de enlace (en algunos AWS Regiones), tienes la opción de conservar y acceder a la dirección IP del cliente (p. 41). Dos tipos de puntos de enlace pueden conservar la dirección IP de origen del cliente en paquetes entrantes: Application Load Balancers y Amazon EC2 Instancias de. Global Accelerator no admite la conservación de la dirección IP del cliente para Balanceador de carga de red y puntos de enlace de dirección IP elástica.

Para puntos de enlace que tienen habilitada la conservación de direcciones IP de cliente, Global Accelerator termina las conexiones TCP de los clientes en AWS ubicaciones de borde de. Casi al mismo tiempo, Global Accelerator establece una nueva conexión TCP con los puntos de enlace que tienen habilitada la conservación de direcciones IP de cliente, en compatible AWS Regiones. Esto proporciona a los clientes tiempos de respuesta más rápidos (menor latencia) y un mayor rendimiento.

Global Accelerator monitoriza continuamente el estado de todos los puntos de enlace y comienza a dirigir el tráfico a otro punto de enlace disponible al instante cuando determina que un punto de enlace activo no está en buen estado. Esto le permite crear una arquitectura de alta disponibilidad para sus aplicaciones en AWS.

Cuando añades un acelerador, grupos de seguridad y AWS WAF las reglas que ya ha configurado siguen funcionando como lo hacían antes de agregar el acelerador.

Si desea un control preciso sobre el tráfico global, puede configurar pesos (p. 36) para sus puntos de enlace. También puede aumentar (marcar arriba) o disminuir (marcar abajo) (p. 31) el porcentaje de tráfico a un grupo de puntos de enlace determinado, por ejemplo, para pruebas de rendimiento o actualizaciones de pilas.

Global Accelerator admite protocolos TCP y UDP.

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 Global Accelerator sobre su AWS Direct Connect La interfaz virtual pública de. Si anuncia direcciones IP que utiliza para comunicarse con Global Accelerator sobre su AWS Direct Connect la interfaz virtual pública, dará como resultado un flujo de tráfico asimétrico: su tráfico hacia Global Accelerator va a Global Accelerator a través de Internet, pero el tráfico de retorno que llega a su red on-premise llega a su AWS Direct Connect La interfaz virtual pública de.
- Global Accelerator no admite el procesamiento de fragmentos de paquetes IP ni el reensamblaje. Un enrutador o puerta de enlace intermedio que funcione en la capa 3 podría fragmentar un paquete en varios paquetes más pequeños entre el cliente y el Global Accelerator Punto de enlace de. Si esto sucede, los fragmentos no se procesan ni se vuelven a ensamblar por Global Accelerator y no se entregan al punto de enlace.

Temas



# Tiempo de espera de inactividad en AWS Global Accelerator

El tiempo de espera de inactividad en AWS Global Accelerator afecta al tiempo que las conexiones se mantienen en una tabla de flujo y se marcan como activas en las ubicaciones de borde de. En cada ubicación de borde, para cada nueva conexión de red, Global Accelerator mantiene un registro de la conexión en la tabla de flujo siempre que los paquetes sigan pasando por. Si hay un periodo de tiempo en el que Global Accelerator no detecta nuevos paquetes para una conexión—es decir, el periodo de tiempo de inactividad que se ha establecido para cada tipo de conexión—Global Accelerator elimina la entrada de conexión de la tabla de flujo. Si llegan paquetes adicionales después de que se supera el tiempo de espera para un flujo específico, Global Accelerator vuelve a seleccionar un destino de punto de enlace en función del estado, la ubicación del cliente y las políticas que configure.

El tiempo de espera de inactividad para la conexión de red depende del tipo de conexión:

- El tiempo de espera es de 350 segundos para conexiones TCP a puntos de enlace de con La conservación de la dirección IP del cliente de está habilitada (Application Load Balancers y instancias EC2).
- El tiempo de espera es de 90 segundos para conexiones TCP a puntos de enlace de sin la conservación de la dirección IP del cliente (Network Load Balancers y direcciones IP elásticas).
- El tiempo de espera para las conexiones UDP es de 30 segundos.

Global Accelerator continúa dirigiendo el tráfico a un punto de enlace hasta que se alcanza el tiempo de espera de inactividad, incluso si el punto de enlace está marcado como en mal estado. Global Accelerator selecciona un nuevo punto de enlace, si es necesario, solo cuando se inicia una nueva conexión o después de un tiempo de inactividad.

# Direcciones IP estáticas en AWS Global Accelerator

Utilice las direcciones IP estáticas que Global Accelerator que asigna a su acelerador—o que especifique desde su propio grupo de direcciones IP—para dirigir el tráfico de Internet al AWS de red global cercana al lugar donde se encuentran los usuarios, independientemente de su ubicación. Se asocian las direcciones

con Network Load Balancersde Application Load Balancers, instancias EC2 o direcciones IP elásticas que se ejecutan en un único AWS Región o varias regiones. Direccionamiento del tráfico a través de AWS La red global de mejora la disponibilidad y el rendimiento porque el tráfico no tiene que realizar varios saltos a través de la Internet pública. El uso de direcciones IP estáticas también le permite distribuir el tráfico entrante de la aplicación entre varios recursos de punto de enlace en varios AWS Regiones.

Además, el uso de direcciones IP estáticas facilita la adición de la aplicación a más regiones de o la migración de aplicaciones entre regiones de. 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 Direccionamiento del tráfico de dominio personalizado a su acelerador de (p. 27).

Global Accelerator proporciona las direcciones IP estáticas automáticamente desde el grupo de direcciones IP de Amazon, a menos que traiga su propio rango de direcciones IP a AWS y especifique las direcciones IP estáticas de ese grupo. Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en AWS Global Accelerator (p. 20). Para crear un acelerador en la consola, el primer paso es solicitar Global Accelerator para aprovisionar las direcciones IP estáticas introduciendo un nombre para su acelerador o elija sus propias direcciones IP estáticas. Para ver los pasos para crear un acelerador, consulte Creación o actualización de un acelerador de (p. 17).

Las direcciones IP estáticas permanecen asignadas a su acelerador durante tanto tiempo como exista, incluso si deshabilitas la acelerador y ya no acepta ni dirige el tráfico. Sin embargo, cuando eliminar un acelerador, pierde las direcciones IP estáticas que se le asignan, por lo que ya no puede dirigir el tráfico con ellas. Puede utilizar políticas 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 (p. 72).

# Administración del flujo de tráfico con marcaciones de tráfico y pesos de terminales

Hay dos formas de personalizar cómo AWS Global Accelerator envía tráfico a los puntos de enlace de :

- Cambiar la marcación de tráfico para limitar el tráfico de uno o varios grupos de puntos de enlace
- Especificar ponderaciones para cambiar la proporción de tráfico a los puntos de enlace de un grupo

Cómo funcionan las secciones de tráfico

Para cada grupo de puntos de enlace en un acelerador, puede establecer una marcación de tráfico para controlar el porcentaje de tráfico que se envía al grupo de puntos de enlace. El porcentaje se aplica solo al tráfico que ya está dirigido al grupo de puntos de enlace, no a todo el tráfico del agente de escucha.

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

Para obtener más información, consulte Ajustar el flujo de tráfico con marcaciones de tráfico (p. 31).

Cómo funcionan los pesos

Para cada punto de enlace, puede especificar ponderaciones, que son números que cambian la proporción de tráfico que el acelerador se dirige a cada punto de enlace. 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 punto de enlace. De forma predeterminada, la ponderación de un punto de enlace es 128, es decir, la mitad del valor máximo de una ponderación, 255.

El acelerador calcula la suma de las ponderaciones de los puntos de enlace de un grupo de puntos de enlace y, a continuación, dirige el tráfico a los puntos de enlace en función de la relación entre la ponderación de cada punto de enlace y el total de. Para ver un ejemplo de cómo funcionan los pesos, consulte Ponderaciones de punto final (p. 36).

Las marcas de tráfico y los pesos afectan a la forma en que el acelerador distribuye el tráfico de diferentes maneras:

- Puede configurar las secciones de tráfico para grupos de puntos de enlace. La marcación de tráfico le permite reducir un porcentaje de tráfico—o todo el tráfico—al grupo, "marcando hacia abajo" el tráfico que acelerador ya se ha dirigido a él basándose en otros factores, como la proximidad.
- Por otro lado, se utilizan pesos para establecer valores para criterios de valoración individuales dentro de un grupo de puntos de enlace. Las ponderaciones proporcionan una forma de dividir el tráfico dentro del grupo de puntos de enlace. Por ejemplo, puede utilizar ponderaciones para realizar pruebas de rendimiento para puntos de enlace específicos en una región.

Note

Para obtener más información acerca de cómo afectan las llamadas de tráfico y las ponderaciones a la conmutación por error, consulte Conmutación por error para puntos de enlace en mal estado (p. 37).

## Comprobaciones de estado para AWS Global Accelerator

AWS Global Accelerator comprueba automáticamente el estado de los puntos de enlace que están asociados a las direcciones IP estáticas y, a continuación, dirige el tráfico de usuarios solo a los puntos de enlace en buen estado.

Global Accelerator incluye comprobaciones de estado predeterminadas que se ejecutan automáticamente, pero puede configurar el tiempo de las comprobaciones y otras opciones. Si ha configurado los ajustes de comprobación de estado personalizados, Global Accelerator utiliza estos ajustes de formas específicas, en función de la configuración. Puede configurar estos ajustes en Global Accelerator para los puntos de enlace de la instancia EC2 o la dirección IP elástica o configurando los ajustes en la Elastic Load Balancing consola de para Network Load Balancers o bien Application Load Balancers. Para obtener más información, consulte Opciones de comprobación de estado (p. 32).

Al añadir un punto de enlace, debe pasar una comprobación de estado para que se considere que está en buen estado antes de que el tráfico se dirija a él. Si Global Accelerator no tiene ningún punto de enlace en buen estado al que dirigir el tráfico, dirige las solicitudes a todos los puntos de enlace.

# Los rangos de ubicación y dirección IP de Global Accelerator servidores perimetrales

Para obtener una lista de Global Accelerator de servidores perimetrales, consulte la ¿Dónde se implementa AWS Global Accelerator hoy? en la sección AWS Global Accelerator Preguntas frecuentes página.

AWS publica sus rangos de direcciones IP actuales en formato JSON. Para ver los rangos actuales, descargue rangos-ip.json. Para obtener más información, consulte Rangos de direcciones IP de AWS en la Referencia general de Amazon Web Services.

Para buscar los rangos de direcciones IP asociados a AWS Global Accelerator servidores perimetrales, buscar `ip-ranges.json` para la siguiente cadena:

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

Global Accelerator entradas que incluyen `"region": "GLOBAL"` consulte las direcciones IP estáticas que se asignan a los aceleradores del cliente. 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 bien `eu-*`. 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. Esta sección enumera algunos de ellos para darle una idea de cómo puede utilizar Global Accelerator para satisfacer sus necesidades.

Aumente la escala para una mayor utilización de la aplicación

Cuando el uso de la aplicación aumenta, el número de direcciones IP y puntos de enlace que debe administrar también aumenta. Global Accelerator le permite escalar su red hacia arriba o hacia abajo. Le permite asociar recursos regionales, como balanceadores de carga e instancias EC2, a dos direcciones IP estáticas. Puede incluir estas direcciones en las listas de permitidos solo una vez en sus aplicaciones cliente, firewalls y registros DNS. Con Global Accelerator, puede añadir o eliminar puntos de enlace en AWS las regiones, ejecute la implementación blue/green y realice pruebas A/B sin tener que actualizar las direcciones IP en las aplicaciones cliente. Esto es especialmente útil para casos de uso de IoT, comercio minorista, medios, automoción y atención sanitaria en los que no se pueden actualizar fácilmente las aplicaciones cliente con frecuencia.

Aceleración para aplicaciones sensibles a la latencia

Muchas aplicaciones, especialmente en áreas como juegos, multimedia, aplicaciones móviles y financieras, 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 punto de enlace de la aplicación más cercano al cliente, lo que reduce la latencia de Internet y la fluctuación. Global Accelerator dirige el tráfico a la ubicación de borde más cercana mediante Anycast y, a continuación, lo dirige al punto de enlace regional más cercano a través de AWS de red global. 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 en varias regiones

Debe poder confiar en su red para estar disponible. Es posible que esté ejecutando su aplicación en varios AWS Regiones para admitir la recuperación de desastres, mayor disponibilidad, menor latencia o conformidad. Si Global Accelerator detecta que el punto de enlace de la aplicación está fallando en el principal AWS región, activa instantáneamente el redireccionamiento del tráfico al punto de enlace de la aplicación en el siguiente punto de enlace de la aplicación disponible, el más cercano AWS Región.

Proteja sus aplicaciones

Puede configurar Application Load Balancers para estar expuesto a Internet o instancias de Amazon EC2 para ser públicas y servir a los usuarios. Sin embargo, el acceso desde Internet también aumenta su exposición a ataques maliciosos. Puede ayudar a mitigar este riesgo utilizando AWS Global

Accelerator. Primero, añada un Balanceador de carga de aplicaciones o una instancia EC2 privada como punto de enlace en Global Accelerator. Entonces puedes usar Global Accelerator como el único punto de acceso expuesto a Internet para el punto de enlace de. Esto reduce el riesgo de ataques de denegación de servicio distribuidos (DDoS) y controla cómo los usuarios llegan a sus aplicaciones. Global Accelerator crea una interconexión entre su acelerador de Virtual Private Cloud (VPC) y su Amazon VPC. El tráfico entre las dos VPC utiliza direcciones IP privadas.

# AWS Global Accelerator Herramienta de comparación de velocidad

Puedes utilizar la función AWS Global Accelerator Herramienta de comparación de velocidad para ver Global Accelerator en comparación con las descargas directas por Internet, en AWS Regiones. Esta herramienta le permite utilizar su navegador para ver la diferencia de rendimiento al transferir datos mediante Global Accelerator. Puede elegir el tamaño de archivo que desea descargar y la herramienta descarga archivos a través de HTTPS/TCP desde Application Load Balancers en diferentes regiones de su navegador. Para cada región, verá una comparación directa de las velocidades de descarga.

To access the Speed Comparison Tool, copy the following URL into your browser:

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

Important

Results may differ when you run the test multiple times. Los tiempos de descarga pueden variar en función de factores externos a Global Accelerator, such as the quality, capacity, and distance of the connection in the last-mile network that you're using.

# Primeros pasos con AWS Global Accelerator

Puede comenzar a configurar AWS Global Accelerator con la API de o con la AWS Global Accelerator consola de. Porque Global Accelerator es un servicio global, no vinculado a un servicio AWS Región.

Para comenzar a utilizar Global Accelerator, sigue estos pasos generales:

1. Configurar la configuración inicial para Global Accelerator: Proporcione un nombre para su acelerador. A continuación, configure uno o varios agentes de escucha para procesar las conexiones entrantes de los clientes, en función del protocolo y el puerto (o el rango de puertos) que especifique.
2. Configuración de grupos de puntos de enlace regionales para su acelerador: Puede seleccionar uno o varios grupos de puntos de enlace regionales para añadirlos al agente de escucha especificando las regiones de a las que desea distribuir el tráfico. El agente de escucha direcciona las solicitudes a los puntos de enlace que ha añadido a un grupo de puntos de enlace. Global Accelerator monitoriza el estado de los puntos de enlace dentro del grupo de mediante la configuración de comprobación de estado definida para cada uno de los puntos de enlace de. Para cada grupo de puntos de enlace, puede configurar un marcación de tráfico porcentaje para controlar el porcentaje de tráfico que un grupo de puntos de enlace aceptará. El porcentaje se aplica solo al tráfico que ya se ha dirigido al grupo de puntos de enlace, no a todo el tráfico del agente de escucha. De forma predeterminada, la marcación de tráfico se establece en 100 % para todos los grupos de puntos de enlace regionales.
3. Añada puntos de enlace a grupos de puntos de enlace: Puede añadir uno o varios recursos regionales, como balanceadores de carga o puntos de enlace de instancias EC2, a cada grupo de puntos de enlace. A continuación, puede decidir cuánto tráfico desea dirigir a cada punto de enlace estableciendo las ponderaciones de punto de enlace.

Para conocer los pasos detallados sobre cómo crear un acelerador con AWS Global Accelerator consola, consulte Introducción a AWS Global Accelerator (p. 11). Para trabajar con operaciones de API de , consulte Acciones comunes que puede utilizar con AWS Global Accelerator (p. 16) y Referencia de la API de AWS Global Accelerator.

# Etiquetado en AWS Global Accelerator

Las etiquetas son palabras o frases que utilizas para identificar y organizar tu AWS Los recursos de. Puede añadir varias etiquetas a cada recurso, y cada etiqueta incluye una clave y un valor que usted define. Por ejemplo, la clave podría ser `environment` y el valor podría ser `production`. Puede buscar y filtrar sus recursos en función de las etiquetas que añada. En AWS Global Accelerator, puedes 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 otro AWS recursos (como Network Load Balancersde Application Load Balancerso instancias de Amazon EC2) y active las etiquetas. Luego AWS genera un informe de asignación de costos como un valor separado por comas (archivo CSV) con el uso y los costos agregados por las etiquetas activas. 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 AWS Billing and Cost Management.
- Uso de etiquetas para aplicar permisos basados en etiquetas para aceleradores. Para ello, cree políticas de IAM que especifiquen etiquetas y valores de etiqueta para permitir o no permitir acciones de. Para obtener más información, consulte Políticas basadas en etiquetas (p. 72).

Para conocer las convenciones de uso y los enlaces a otros recursos sobre el etiquetado, consulte Etiquetado de recursos de AWS en el AWS General Reference. Para obtener consejos sobre el uso de etiquetas, consulte Prácticas recomendadas de etiquetado: Estrategia de etiquetado de recursos de AWS en el Documentos técnicos de AWS del blog de.

Para el número máximo de etiquetas que puede añadir a un recurso en Global Accelerator, consulte Cuotas para AWS Global Accelerator (p. 95).

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

- [EMPTY]
- TagResource ()
- UntagResource
- ListTagsForResource

## Compatibilidad de etiquetado en Global Accelerator

AWS Global Accelerator admite el etiquetado para aceleradores.

Global Accelerator admite la característica de control de acceso basado en etiquetas de AWS Identity and Access Management (IAM). Para obtener más información, consulte Políticas basadas en etiquetas (p. 72).

# Adición, edición y eliminación de etiquetas en Global Accelerator

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

> Note
>
> Puede añadir o eliminar etiquetas mediante la consola de , la AWS la CLI, o Global Accelerator Operaciones de la API de. Para obtener más información, incluidos ejemplos de CLI, consulte Recurso de etiqueta en el Referencia de la API de AWS Global Accelerator.

Para añadir, editar o eliminar etiquetas en Global Accelerator

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. Elija la opción acelerador que desea añadir o actualizar etiquetas para.
3. En la pestaña Etiquetas , puede hacer lo siguiente:

   Añada una etiqueta.

   Elegir Añadir etiqueta, a continuación, escriba una clave y, opcionalmente, un valor para la etiqueta.

   Editar una etiqueta

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

   Eliminar una etiqueta

   Elegir Eliminar en el lado derecho del campo de valor.
4. Elija Save changes.

# Precios de AWS Global Accelerator

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

# Introducción a AWS Global Accelerator

Este tutorial proporciona los pasos para comenzar a utilizar AWS Global Accelerator con la consola de. También puede utilizar AWS Global Accelerator Operaciones de la API de para crear y personalizar su acelerador. En cada paso de este tutorial, hay un enlace a la operación de la API correspondiente para completar la tarea mediante programación. Para obtener más información sobre cómo trabajar con AWS Global Accelerator Operaciones de la API de , consulte la Referencia de la API de AWS Global Accelerator.

> Tip
>
> Para explorar cómo puede utilizar Global Accelerator para mejorar el rendimiento y la disponibilidad de las aplicaciones web, consulte el siguiente taller a su propio ritmo: AWS Global Accelerator Seminario.

Global Accelerator es un servicio global que admite puntos de enlace en varios AWS Regiones, que se enumeran en la AWS Tabla de regiones.

Tareas



# Antes de empezar

Antes de crear un acelerador, cree al menos un recurso que pueda añadir como punto de enlace para dirigir el tráfico a. Por ejemplo, cree una de las siguientes opciones:

- Lanzar al menos un Amazon EC2 instancia que se va a añadir como punto de enlace. Para obtener más información, consulte Creación de los recursos de EC2 y lanzamiento de la instancia EC2 en el Guía del usuario de Amazon EC2 para instancias de Linux.
- Opcionalmente, cree uno o más Network Load Balancers o bien Application Load Balancers que incluye instancias EC2. Para obtener más información, consulte Crear un Balanceador de carga de red Balanceador de carga de aplicaciones en el Guía del usuario de Network Load Balancers.

  > Tip
  >
  > Puedes añadir un acelerador al mismo tiempo que creas un Balanceador de carga de aplicaciones, seleccionando la opción en la pestaña Amazon EC2 al crear el balanceador de carga. Para obtener más información, consulte Creación de un Balanceador de carga de aplicaciones.

Cuando crea un recurso para añadirlo a Global Accelerator, tenga en cuenta lo siguiente:

- Cuando se añade un Balanceador de carga de aplicaciones o un punto de enlace de instancia EC2 en Global Accelerator, habilita el tráfico de Internet para que fluya directamente hacia y desde el punto de enlace en las nubes virtuales privadas (VPC) dirigiéndolo a una subred privada. La VPC que contiene el balanceador de carga o la instancia EC2 debe tener una puerta de enlace de Internet asociado a ella, para indicar que la VPC acepta tráfico de Internet. Para obtener más información, consulte Proteger las conexiones de VPC en AWS Global Accelerator (p. 91).
- Global Accelerator requiere las reglas de router y firewall para permitir el tráfico entrante desde las direcciones IP asociadas a Route 53 Los comprobadores de estado de para completar las comprobaciones de estado de los puntos de enlace de instancia EC2 o dirección IP elástica. Puede encontrar información sobre los rangos de direcciones IP asociados a Amazon Route 53 Comprobadores de estado de en Comprobaciones de estado de los grupos de destino en el Guía para desarrolladores de Amazon Route 53.

  Important

  Global Accelerator es un servicio global que puede dirigir puntos de enlace de aplicaciones en múltiples AWS pero debes estar en el campo EE.UU. Oeste (Oregón) Región para crear o actualizar aceleradores utilizando la función Consola de administración de AWS o bien AWS CLI.

# Paso 1. Crear un acelerador.

Para empezar a crear su acelerador, introduzca un nombre para él.

Note

Para completar esta tarea mediante una operación de la API en lugar de la consola de , consulte [EMPTY] en el Referencia de la API de AWS Global Accelerator.

### Para crear un acelerador

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. Seleccione Create (Crear)acelerador.
3. Proporcione un nombre para su acelerador.
4. Opcionalmente, añada una o varias etiquetas para ayudarle a identificar su Global Accelerator Los recursos de.
5. Seleccione Next (Siguiente).

# Paso 2. Añadir agentes de escucha

Crear un agente de escucha para procesar las conexiones entrantes de los usuarios a Global Accelerator.

Note

Para completar esta tarea mediante una operación de la API en lugar de la consola de , consulte Contendor de creación en el Referencia de la API de AWS Global Accelerator.

### Para crear un agente de escucha

1. En la Añadir agente de escucha , escriba los puertos o rangos de puertos que desea asociar al agente de escucha. Los agentes de escucha admiten puertos 1-65535.
2. Elija el protocolo para los puertos que ha introducido.

3. De forma opcional, elija para habilitar la afinidad del cliente. La afinidad del cliente por un oyente significa que Global Accelerator garantiza que las conexiones desde una dirección IP de origen (cliente) específica siempre se direccionen al mismo punto de enlace. Para habilitar este comportamiento, en la lista desplegable, elija IP de origen.

   El valor predeterminado es Ninguno, lo que significa que la afinidad del cliente no está habilitada y Global Accelerator distribuye el tráfico de forma equitativa entre los puntos de enlace de los grupos de puntos de enlace para el agente de escucha.

   Para obtener más información, consulte Afinidad del cliente (p. 29).
4. Opcionalmente, elija Añadir agente de escucha para añadir un agente de escucha adicional.
5. Cuando haya terminado de añadir agentes de escucha, elija Siguiente.

# Paso 3. Añadir grupos de puntos de enlace

Añadir uno o varios grupos de puntos de enlace, cada uno de los cuales está asociado a un determinado AWS Región.

Note

Para completar esta tarea mediante una operación de la API en lugar de la consola de , consulte Crear grupo de criterios de valoración en el Referencia de la API de AWS Global Accelerator.

Para añadir un grupo de puntos de enlace

1. En la Añadir grupos de puntos de enlace , en la sección de un agente de escucha, elija un Región de la lista desplegable.
2. Opcionalmente, para Marcación de tráfico, introduzca un número de 0 a 100 para establecer un porcentaje de tráfico para este grupo de puntos de enlace. El porcentaje se aplica solo al tráfico ya dirigido a este grupo de puntos de enlace, no a todo el tráfico del agente de escucha. De forma predeterminada, la marcación de tráfico para un grupo de puntos de enlace se establece en 100 (es decir, 100%).
3. De forma opcional, para los valores de comprobación de estado personalizados, elija Configurar comprobaciones de estado. Cuando configura los ajustes de comprobación de estado, Global Accelerator utiliza la configuración de las comprobaciones de estado de la instancia EC2 y los puntos de enlace de direcciones IP elásticas. Para Balanceador de carga de red y Balanceador de carga de aplicaciones puntos de enlace, Global Accelerator utiliza la configuración de comprobación de estado que ya ha configurado para los propios balanceadores de carga. Para obtener más información, consulte Opciones de comprobación de estado (p. 32).
4. Opcionalmente, elija Añadir grupo de puntos de enlace para añadir grupos de puntos de enlace adicionales para este agente de escucha u otros agentes de escucha.
5. Seleccione Next (Siguiente).

# Paso 4. Añadir puntos de enlace

Añada uno o varios puntos de enlace que estén asociados a grupos de puntos de enlace específicos. Este paso no es necesario, pero no se dirige tráfico a los puntos de enlace de una región a menos que los puntos de enlace se incluyan en un grupo de puntos de enlace.

Note

Si estás creando tu acelerador mediante programación, se añaden puntos de enlace como parte de la adición de grupos de puntos de enlace. Para obtener más información, consulte Crear grupo de criterios de valoración en el Referencia de la API de AWS Global Accelerator.

Para añadir puntos de enlace

1. En la Creación de puntos de enlace , en la sección de un punto de enlace, elija un punto de enlace en la lista desplegable.
2. Opcionalmente, para Peso, introduzca un número de 0 a 255 para establecer una ponderación para el tráfico de enrutamiento a este punto de enlace. Cuando se añaden ponderaciones a los puntos de enlace, se configura Global Accelerator para dirigir el tráfico en función de las proporciones que especifique. De forma predeterminada, todos los puntos de enlace tienen una ponderación de 128. Para obtener más información, consulte Ponderaciones de punto final (p. 36).
3. Opcionalmente, para un Balanceador de carga de aplicaciones punto de enlace, en Conservar dirección IP del cliente, selecciona Conservar dirección. Para obtener más información, consulte Conservar direcciones IP de cliente en AWS Global Accelerator (p. 41).
4. Opcionalmente, elija Añadir punto de enlace para añadir más puntos de enlace.
5. Seleccione Next (Siguiente).

Después de elegir Siguiente, en la Global Accelerator verás un mensaje de que tu acelerador está en curso. Cuando el proceso haya terminado, el botón acelerador del panel de control es Activo.

# Paso 5. Probar el acelerador

Toma medidas para probar tu acelerador para asegurarse de que el tráfico se dirige a los puntos de enlace de. Por ejemplo, ejecute un comando curl como el siguiente, sustituyendo una de las direcciones IP estáticas de su acelerador, para mostrar la AWS Regiones donde se procesan las solicitudes. Esto resulta especialmente útil si establece diferentes ponderaciones para los puntos de enlace o ajusta la marcación de tráfico en los grupos de puntos de enlace.

Ejecute un comando curl como el siguiente, sustituyendo una de las direcciones IP estáticas de su acelerador, para llamar a la dirección IP 100 veces y, a continuación, genere 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 la marcación de tráfico en cualquier grupo de puntos de enlace, este comando puede ayudarle a confirmar que su acelerador está dirigiendo los porcentajes correctos de tráfico a diferentes grupos de. Para obtener más información, consulte los ejemplos detallados en la siguiente entrada de blog, Administración del tráfico con AWS Global Accelerator.

# Paso 6. Eliminación del acelerador de

Si has creado una acelerador como una prueba o si ya no estás usando un acelerador, puede eliminarlo. En la consola de , deshabilite la aceleradory, a continuación, puede eliminarlo. No es necesario eliminar los agentes de escucha y grupos de puntos de enlace de la acelerador.

Para eliminar un acelerador utilizando una operación de API en lugar de la consola de , primero debe eliminar todos los agentes de escucha y grupos de puntos de enlace asociados a la acelerador así como deshabilitarlo. Para obtener más información, consulte la EliminarAcelerador en la operación Referencia de la API de AWS Global Accelerator.

Tenga en cuenta lo siguiente al eliminar puntos de enlace o grupos de puntos de enlace, o al eliminar un acelerador:

- Cuando creas un aceleradorde Global Accelerator le proporciona un conjunto de dos direcciones IP estáticas. Las direcciones IP se asignan a su acelerador durante tanto tiempo como exista, incluso si deshabilitas la acelerador y ya no acepta ni dirige el tráfico. Sin embargo, cuando eliminar un acelerador, perderás las direcciones IP estáticas que están asignadas a la acelerador, por lo que ya no puede dirigir el tráfico con. Como práctica recomendada, asegúrese de tener permisos para evitar la eliminación accidental aceleradores. Puede utilizar políticas 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 (p. 72).
- Si termina una instancia EC2 antes de eliminarla de un grupo de puntos de enlace en Global Acceleratory, a continuación, cree otra instancia con la misma dirección IP privada y supere las comprobaciones de estado, Global Accelerator dirigirá el tráfico al nuevo punto de enlace. Si no desea que esto suceda, elimine la instancia EC2 del grupo de puntos de enlace antes de terminar la instancia.

### Para eliminar un acelerador

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. Elija la opción acelerador que desea eliminar.
3. Elija Edit.
4. Elija Deshabilitaracelerador y, a continuación, Guardar.
5. Elija la opción acelerador que desea eliminar.
6. Elija Eliminaracelerador.
7. En el cuadro de diálogo de confirmación, elija Delete (Eliminar).

# Acciones comunes que puede utilizar con AWS Global Accelerator

La siguiente tabla muestra las comunes AWS Global Accelerator de acciones que puede utilizar con Global Accelerator Los recursos de. La tabla también proporciona enlaces a la documentación relevante.

| Acción: | Mediante la consola de Global Accelerator. | Uso de la API Global Accelerator |
|---|---|---|
| Creación de un acelerador | Consulte Introducción a AWS Global Accelerator (p. 11) | Consulte `CreateAccelerator` |
| Crear un agente de escucha | Consulte Adición, edición o eliminación de un agente de escucha (p. 28) | Consulte `CreateListener` |
| Creación de un grupo de puntos de enlace | Consulte Adición, edición o eliminación de un grupo de puntos de enlace (p. 30) | Consulte `CreateEndpointGroup` |
| Enumere su aceleradores | Consulte Visualización de los aceleradores de (p. 19) | Consulte `ListAccelerator` |
| Obtener toda la información sobre un acelerador | Consulte Visualización de los aceleradores de (p. 19) | Consulte `DescribeAccelerator` |
| Actualizar un acelerador | Consulte Creación o actualización de un acelerador de (p. 17) | Consulte `UpdateAccelerator` |
| Para eliminar un acelerador | Consulte Creación o actualización de un acelerador de (p. 17) | Consulte `DeleteAccelerator` |

# Aceleradores en AWS Global Accelerator

Un acelerador en AWS Global Accelerator dirige el tráfico a puntos de enlace óptimos a través de AWS de red global para mejorar la disponibilidad y el rendimiento de sus aplicaciones de Internet que tienen un público global. Cada acelerador incluye uno o varios agentes de escucha. Un agente de escucha procesa las conexiones entrantes de los clientes a Global Accelerator, en función del protocolo y el puerto (o el rango de puertos) que configure.

Cuando creas un acelerador, de forma predeterminada, Global Accelerator le proporciona un conjunto de dos direcciones IP estáticas. Si trae su propio rango de direcciones IP a AWS (BYOIP), puede asignar direcciones IP estáticas de su propio grupo para utilizarlas con su acelerador. Para obtener más información, consulte Traiga sus propias direcciones IP (BYOIP) en AWS Global Accelerator (p. 20).

> **Important**
>
> Las direcciones IP se asignan a su acelerador durante tanto tiempo como exista, incluso si deshabilitas la acelerador y ya no acepta ni dirige el tráfico. Sin embargo, cuando eliminar un acelerador, pierdes el Global Accelerator direcciones IP estáticas asignadas a la acelerador, por lo que ya no puede dirigir el tráfico con. Como práctica recomendada, asegúrese de tener permisos para evitar la eliminación accidental aceleradores. Puede utilizar políticas 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 (p. 72).

Esta sección incluye los pasos para crear, editar o eliminar un acelerador en Global Accelerator consola de. Si desea utilizar operaciones de API de con Global Accelerator, consulta la sección Referencia de la API de AWS Global Accelerator.

Temas



# Creación o actualización de un acelerador de

Esta sección explica cómo crear o actualizar con aceleradores en la consola de. Para trabajar con Global Accelerator mediante programación, consulte la Referencia de la API de AWS Global Accelerator.

> **Important**
>
> Global Accelerator es un servicio global que puede dirigir puntos de enlace de aplicaciones en múltiples AWS pero debes estar en el campo EE.UU. Oeste (Oregón) Región para crear o actualizar aceleradores utilizando la función Consola de administración de AWS o bien AWS CLI.

### Para crear un acelerador

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. Seleccione Create (Crear)acelerador.
3. Proporcione un nombre para su acelerador.
4. Opcionalmente, si ha traído su propio rango de direcciones IP a AWS (BYOIP), puedes especificar direcciones IP estáticas para tu acelerador de ese grupo de direcciones. Elija esta opción 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 eligió su propio grupo de direcciones IP, elija también una dirección IP específica del grupo. Si eligió el grupo de direcciones IP de Amazon predeterminado, Global Accelerator asigna una dirección IP específica a su acelerador.
5. Opcionalmente, añada una o varias etiquetas para ayudarle a identificar su acelerador Los recursos de.
6. Elegir Siguiente para añadir agentes de escucha, grupos de puntos de enlace y puntos de enlace.

### Para editar una acelerador

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la lista de aceleradores, elija uno y, a continuación, elija [EMPTY].
3. En la [EMPTY] acelerador , haz los cambios que te gusten. Por ejemplo, puede deshabilitar la función acelerador para que ya no acepte o dirija el tráfico, o para que pueda eliminarlo. O, si la opción acelerador está deshabilitado, puede habilitarlo.
4. Elija Save changes.

# Eliminación de un acelerador de

Si has creado una acelerador como una prueba o si ya no estás usando un acelerador, puede eliminarlo. En la consola de , deshabilite la aceleradory, a continuación, puede eliminarlo. No es necesario eliminar los agentes de escucha y grupos de puntos de enlace de la acelerador.

> **Important**
>
> Global Accelerator es un servicio global que puede dirigir puntos de enlace de aplicaciones en múltiples AWS pero debes estar en el campo EE.UU. Oeste (Oregón) Región para eliminar aceleradores utilizando la función Consola de administración de AWS o bien AWS CLI.

Para eliminar un acelerador utilizando una operación de API en lugar de la consola de , primero debe eliminar todos los agentes de escucha y grupos de puntos de enlace asociados a la aceleradory, a continuación, desactívelo. Para obtener más información, consulte la EliminarAcelerador en la operación Referencia de la API de AWS Global Accelerator.

### Para deshabilitar un acelerador

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la lista , elige una opción acelerador que desea deshabilitar.
3. Elija Edit.
4. Elija Deshabilitaracelerador y, a continuación, Guardar.

Para eliminar un acelerador

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la lista , elige una opción acelerador que desea eliminar.
3. Elija Eliminar.

   Note

   Si no has deshabilitado la función aceleradorde Eliminar no está disponible.
4. En el cuadro de diálogo de confirmación, elija Delete (Eliminar).

   Important

   Cuando eliminas un acelerador, perderás las direcciones IP estáticas que están asignadas a la acelerador, por lo que ya no puede dirigir el tráfico con.

# Visualización de los aceleradores de

Puedes ver información sobre tu aceleradores en la consola de. Para ver las descripciones de su aceleradores mediante programación, consulte Aceleradores de lista y Acelerador de descripción en el Referencia de la API de AWS Global Accelerator.

Para ver información sobre su acelerador

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. Para ver detalles sobre un acelerador, en la lista, elige un aceleradory, a continuación, selecciona [EMPTY].

# Añadir un acelerador al crear un balanceador de carga

Cuando creas un Balanceador de carga de aplicaciones en el Consola de administración de AWS, puede elegir añadir un acelerador al mismo tiempo. Elastic Load Balancing y Global Accelerator trabajar juntos para añadir de forma transparente el acelerador para ti. El acelerador se crea en su cuenta de , con el balanceador de carga como punto de enlace. Uso de un acelerador proporciona direcciones IP estáticas y mejora la disponibilidad y el rendimiento de las aplicaciones.

Important

Para crear un acelerador, debe tener los permisos correctos en su lugar. Para obtener más información, consulte Permisos necesarios para el acceso a la consola, la administración de la autenticación y el control de acceso (p. 67).

## Configure y vea su acelerador

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

Después de crear el balanceador de carga eligiendo la opción Global Accelerator del complemento en el Amazon EC2 , vaya a la Servicios integrados para ver las direcciones IP estáticas y el nombre del

sistema de nombres de dominio (DNS) de su acelerador. Puede utilizar esta información para comenzar a dirigir el tráfico de usuarios al balanceador de carga a través de la AWS de red global. Para obtener más información sobre el nombre de DNS asignado a su acelerador, consulte Compatibilidad con el direccionamiento de DNS en Global Accelerator (p. 26).

Puede ver y configurar su acelerador por navegando hasta Global Accelerator en el Consola de administración de AWS. Por ejemplo, puede ver el cuadro de diálogo aceleradores que están asociados a su cuenta o añadir balanceadores de carga adicionales a su acelerador. Para obtener más información, consulte Visualización de los aceleradores de (p. 19) y Creación o actualización de un acelerador de (p. 17).

## Precios

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

## Deja de utilizar la función acelerador

Si desea detener el enrutamiento del tráfico a través de Global Accelerator en el balanceador de carga, haga lo siguiente:

1. Actualice la configuración de DNS para dirigir el tráfico directamente al balanceador de carga.
2. Eliminar el balanceador de carga de la acelerador. Para obtener más información, consulte Para eliminar un punto de enlace de en Adición, edición o eliminación de un punto de enlace (p. 34).
3. Elimine la acelerador. Para obtener más información, consulte Eliminación de un acelerador de (p. 18).

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

AWS Global Accelerator utiliza direcciones IP estáticas como puntos de entrada para su aceleradores. Estas direcciones IP son Anycast de AWS ubicaciones de borde de. Por defecto, Global Accelerator proporciona direcciones IP estáticas desde la Grupo de direcciones IP de Amazon. en lugar de utilizar las direcciones IP que Global Accelerator proporciona , 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 rangos de direcciones IP con Global Accelerator.

Puede traer parte o todos los rangos de direcciones IPv4 públicas de su red local a su cuenta de AWS para utilizar con Global Accelerator. Usted continúa siendo el propietario de los rangos de direcciones, pero AWS los anuncia en Internet.

No puede utilizar las direcciones IP que traiga a AWS para uno AWS con otro servicio. Los pasos de este capítulo describen cómo utilizar su propio rango de direcciones IP para su uso en AWS Global Accelerator solo. Para conocer los pasos para traer su propio rango de direcciones IP para su uso en Amazon EC2, consulte Traiga sus propias direcciones IP (BYOIP) en el Amazon EC2 Guía del usuario.

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

Después de llevar un rango de direcciones a AWS, aparece en su cuenta como un grupo de direcciones. Cuando creas un acelerador, puede asignarle una o dos de las direcciones IP de su rango. Le recomendamos que traiga dos rangos de direcciones IP para que pueda elegir una dirección IP de diferentes rangos para cada dirección IP estática. Si decide asignar solo una dirección IP de su rango de direcciones IP a un aceleradorde Global Accelerator asigna una segunda dirección IP estática para el acelerador desde el paso AWS Grupo de direcciones IP.

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

Temas



# Requirements

Puede llevar hasta dos rangos de direcciones IP que cumplan los requisitos a AWS Global Accelerator por AWS cuenta.

Para cumplir los requisitos, su rango de direcciones IP debe cumplir los siguientes requisitos:

- El rango de direcciones IP debe estar registrado en uno de los siguientes registros regionales de Internet (RIR): el Registro Americano de Números de Internet (ARIN), el Centro de Coordinación de Redes de Réseaux IP Européens (RIPE) o el Centro de Información de Redes de Asia-Pacífico (APNIC). El rango de direcciones debe estar registrado en una empresa o entidad institucional. No se puede registrar en 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 a un comportamiento malicioso. Nos reservamos el derecho a rechazar el rango de direcciones IP si investigamos la reputación del rango de direcciones IP y descubrimos que contiene una dirección IP que no tiene un historial limpio.

Además, necesitamos los siguientes tipos o estados de red de asignación y asignación, dependiendo de dónde haya registrado su rango de direcciones IP:

- [EMPTY] `Direct Allocation` y `Direct Assignment` tipos de red
- [EMPTY] `ALLOCATED PA`de `LEGACY`, y `ASSIGNED PI` estados de asignación
- Centro de formación de aneurismas avanzados (AP `ALLOCATED PORTABLE` y `ASSIGNED PORTABLE` estados de asignación

# Prepárate para llevar tu rango de direcciones IP a tu AWS cuenta: Autorización, *

Para garantizar que solo usted pueda llevar su espacio de direcciones IP a Amazon, necesitamos dos autorizaciones:

- Debe autorizar a Amazon a anunciar el rango de direcciones IP.
- Debe proporcionar pruebas de que es propietario del rango de direcciones IP y, por tanto, tener la autoridad para llevarlo a AWS.

  Note

  Cuando se utiliza BYOIP para llevar un rango de direcciones IP a AWS, no puedes transferir la propiedad de ese rango de direcciones a una cuenta o empresa diferente mientras la anunciamos. Tampoco puede transferir directamente un rango de direcciones IP de un AWS cuenta a otra cuenta. Para transferir la propiedad o transferir entre AWS , debes desaprovisionar el rango de direcciones y, a continuación, el nuevo propietario debe seguir los pasos para añadir el rango de direcciones a su AWS cuenta.

Para autorizar a Amazon a anunciar el rango de direcciones IP, debe proporcionar a Amazon un mensaje de autorización firmado. Utilice una autorización de origen de ruta (ROA) para proporcionar esta autorización. Una ROA es una instrucción criptográfica sobre los anuncios de ruta que crea a través de su Registro regional de Internet (RIR). Un ROA contiene el rango de direcciones IP, los números de sistema autónomo (ASN) que pueden anunciar el rango de direcciones IP y una fecha de vencimiento. El ROA autoriza a Amazon a anunciar un rango de direcciones IP bajo un sistema autónomo (AS) específico.

Un ROA no autoriza su AWS cuenta para llevar el rango de direcciones IP a AWS. Para proporcionar esta autorización, debe publicar un certificado X.509 autofirmado en los comentarios del protocolo de acceso a datos del registro (RDAP) para el rango de direcciones IP. El certificado contiene una clave pública que AWS utiliza para verificar la firma del contexto de autorización que ha proporcionado. Conserve su clave privada en un lugar seguro y utilícela para firmar el mensaje del contexto de autorización.

En las siguientes secciones se proporcionan pasos detallados para completar estas tareas de autorización. Los comandos de estos pasos se admiten en Linux. Si utiliza Windows, puede obtener acceso a la Subsistema de Windows para Linux para ejecutar comandos de Linux.

## Pasos para proporcionar autorización



## Paso 1. Cree un objeto ROA

Cree un objeto ROA para autorizar a Amazon ASN 16509 a anunciar su rango de direcciones IP, así como los ASN que actualmente están autorizados para anunciar el rango de direcciones IP. El ROA debe contener la dirección IP /24 que desea traer a AWS y debe establecer la longitud máxima en /24.

Para obtener más información acerca de cómo crear una solicitud de ROA, consulte las siguientes secciones, en función de dónde haya registrado su rango de direcciones IP:

- [EMPTY] Solicitudes de ROA
- [EMPTY]  Gestión de ROA
- Centro de formación de aneurismas avanzados (AP  Administración de rutas

## Paso 2. Crear un certificado X.509 autofirmado

Cree un par de claves y un certificado X.509 autofirmado y, a continuación, añada el certificado al registro RDAP para su RIR. Los siguientes pasos describen cómo realizar estas tareas.

Note

El `openssl` Los comandos de la de estos pasos requieren OpenSSL versión 1.0.2 o posterior.

Para crear y añadir un certificado X.509

1. Genere un par de claves RSA de 2048 bits con el siguiente comando.

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

2. Cree un certificado X.509 público a partir del par de claves utilizando el siguiente comando.

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

   En este ejemplo, el certificado caduca en 365 días, después de los cuales no se puede confiar en él. Cuando ejecute el comando , asegúrese de que establece la `-days` al valor deseado para la caducidad correcta. Cuando se le solicite otra información, puede aceptar los valores predeterminados.
3. Actualice el registro RDAP de su RIR con el certificado X.509 siguiendo los pasos que se indican a continuación, en función de su RIR.

   1. Vea el certificado con el siguiente comando de la.

```
cat publickey.cer
```

   2. Añada el certificado haciendo lo siguiente:

      Important

      Asegúrese de incluir la `-----BEGIN CERTIFICATE-----` y `-----END CERTIFICATE-----` del certificado.

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

## Paso 3. Cree un mensaje de autorización firmada

Cree el mensaje de autorización firmado para permitir que Amazon anuncie su rango de direcciones IP.

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

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

Para crear el mensaje de autorización firmado

1. Crear un mensaje de autorización de texto sin formato y almacenarlo en una variable denominada `text_message`, como en el siguiente ejemplo se muestra. Reemplace el número de cuenta de ejemplo, el rango 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. Firme el mensaje de autorización en `text_message` con el par de claves que creó en la sección anterior.
3. Almacena el mensaje en una variable denominada `signed_message`, como en el siguiente ejemplo se muestra.

```
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 su uso con AWS Global Accelerator

Cuando aprovisiona un rango de direcciones para su uso con AWS, confirma que es propietario del rango de direcciones y autoriza a Amazon a anunciarlo. Verificaremos que eres el propietario del rango de direcciones.

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

Para aprovisionar el rango de direcciones, utilice lo siguiente Elemento de aprovisionamientoByoipCidr del comando. El `--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 rango de direcciones de.

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

El aprovisionamiento de un rango de direcciones de es una operación asíncrona, por lo que la llamada devuelve inmediatamente. However, the address range is not ready to use until its state changes from `PENDING_PROVISIONING` de `READY`. El proceso de aprovisionamiento puede tardar hasta 3 semanas en completarse. Para monitorizar el estado de los rangos de direcciones que ha aprovisionado, utilice lo siguiente EnumerarCidrsByoip comando:

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

Para ver una lista de los estados de un rango de direcciones IP, consulte ElementoCidr de Byoip.

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

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

# Anunciar el rango de direcciones a través de AWS

Una vez aprovisionado el rango de direcciones, está listo para ser anunciado. 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 rango de direcciones IP desde otras ubicaciones antes de publicitarlo a través de AWS.

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

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

Para anunciar el rango de direcciones, utilice lo siguiente [EMPTY] del comando.

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

El siguiente es un ejemplo de solicitud de Global Accelerator para anunciar un rango de direcciones.

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

Para monitorizar el estado de los rangos de direcciones que ha anunciado, utilice lo siguiente EnumerarCidrsByoip del comando.

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

Cuando se anuncia su rango de direcciones IP, el campo `State` devuelto 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, utilice lo siguiente `withdraw-byoip-cidr` del comando.

> **Important**
>
> Para dejar de anunciar tu rango de direcciones, primero debes eliminar cualquier aceleradores que tienen direcciones IP estáticas asignadas desde el grupo de direcciones. Para eliminar un acelerador con la consola de o mediante operaciones de la API, consulte Eliminación de un acelerador de (p. 18).

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

El siguiente es un ejemplo de solicitud de Global Accelerator para retirar un rango de direcciones.

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

## Desaprovisionar el rango de direcciones

Para dejar de utilizar el rango de direcciones con AWS, primero debes eliminar cualquier aceleradores que tienen direcciones IP estáticas asignadas desde el grupo de direcciones y dejan de anunciar su rango de direcciones. Después de completar estos pasos, puede desaprovisionar el rango de direcciones.

Debe dejar de anunciar y desaprovisionar su rango de direcciones utilizando la CLI o Global Accelerator Operaciones de la API de. Esta funcionalidad no está disponible en el AWS consola de.

Paso 1. Eliminar cualquier asociado aceleradores. Para eliminar un acelerador con la consola de o mediante operaciones de la API, consulte Eliminación de un acelerador de (p. 18).

Paso 2. Deje de anunciar el rango de direcciones. Para dejar de anunciar la gama, utilice lo siguiente [EMPTY] del comando.

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

Paso 3 Quite el aprovisionamiento del rango de direcciones. Para desaprovisionar el rango, utilice lo siguiente [EMPTY] del comando.

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

## Creación de un acelerador de con sus direcciones IP

Tienes varias opciones para crear una acelerador con sus propias direcciones IP para las direcciones IP estáticas:

- Uso Global Accelerator para crear una acelerador. Para obtener más información, consulte Creación o actualización de un acelerador de (p. 17).
- Utiliza el botón Global Accelerator La API para crear un acelerador de. Para obtener más información, incluido un ejemplo de uso de la CLI, consulte [EMPTY] en el Referencia de la API de AWS Global Accelerator.

# Compatibilidad con el direccionamiento de DNS en Global Accelerator

Cuando creas un aceleradorde Global Accelerator aprovisiona dos direcciones IP estáticas para usted. También asigna un nombre de sistema de nombres de dominio (DNS) predeterminado a su acelerador, similar a `a1234567890abcdef.awsglobalaccelerator.com`, que apunta a las direcciones IP estáticas. Las direcciones IP estáticas se anuncian globalmente utilizando anycast desde el AWS de borde a sus puntos de enlace, como Network Load Balancersde Application Load Balancers, instancias EC2 o direcciones IP elásticas. Puede utilizar las direcciones IP estáticas o el nombre de DNS del acelerador para dirigir el tráfico a su acelerador. Los servidores DNS y los solucionadores de DNS utilizan un turno rotativo para resolver el nombre DNS de un acelerador, por lo que el nombre se resuelve en las direcciones IP estáticas del acelerador, devuelto por Amazon Route 53 en orden aleatorio. Los clientes suelen utilizar la primera dirección IP que se devuelve.

> Note
>
> Global Accelerator crea dos registros de puntero (PTR) que asignan direcciones IP estáticas de acelerador al nombre de DNS correspondiente generado por Global Accelerator, para admitir

la búsqueda de DNS inversa. Esto también se conoce como zona hospedada inversa. Tenga en cuenta que el nombre de DNS que Global Accelerator genera por usted no es configurable y no puede crear registros PTR que apunten a su nombre de dominio personalizado. Global Accelerator también no crea registros PTR para direcciones IP estáticas de un rango de direcciones IP que se trae a AWS (BYOIP).

# Direccionamiento del tráfico de dominio personalizado a su acelerador de

En la mayoría de las situaciones, puede configurar DNS para utilizar su nombre de dominio personalizado (como `www.example.com`) con tu acelerador, en lugar de utilizar las direcciones IP estáticas asignadas o el nombre de DNS predeterminado. Primero, usando Amazon Route 53 u otro proveedor de DNS, cree un nombre de dominio y, a continuación, añada o actualice registros de DNS con su Global Accelerator Direcciones IP. O bien, puede asociar su nombre de dominio personalizado con el nombre de DNS de su acelerador. Complete la configuración de DNS y espere a que los cambios se propaguen a través de Internet. Ahora, cuando un cliente realiza una solicitud con su nombre de dominio personalizado, el servidor DNS la resuelve en las direcciones IP, en orden aleatorio, o en el nombre DNS de su acelerador.

Para utilizar su nombre de dominio personalizado con Global Accelerator cuando usas Route 53 como servicio DNS, debe crear un registro de alias que apunte su nombre de dominio personalizado al nombre de DNS asignado a su 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 para el dominio raíz, como `example.com`, y para subdominios, como `www.example.com`. Para obtener más información, consulte Elección entre registros de alias y no alias en el 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 siguiente tema: Destino de alias en el Guía para desarrolladores de Amazon Route 53. Desplácese hacia abajo para ver la información de Global Accelerator.

# Agentes de escucha en AWS Global Accelerator

Con AWS Global Accelerator, añade agentes de escucha que procesan las conexiones entrantes de los clientes en función de los puertos y protocolos que especifique. Global Accelerator admite protocolos TCP y UDP.

Puede definir un agente de escucha al crear su aceleradory puede añadir más agentes de escucha en cualquier momento. Debe asociar cada agente de escucha a uno o varios grupos de puntos de enlace y asociar cada grupo de puntos de enlace a uno AWS Región.

Temas



## Adición, edición o eliminación de un agente de escucha

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

### Para agregar un agente de escucha

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la aceleradores , selecciona un acelerador.
3. Elija Add listener (Añadir agente de escucha).
4. En la Añadir agente de escucha , escriba 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. De forma opcional, elija para habilitar la afinidad del cliente. La afinidad del cliente por un oyente significa que Global Accelerator garantiza que las conexiones desde una dirección IP de origen (cliente) específica siempre se direccionen al mismo punto de enlace. Para habilitar este comportamiento, en la lista desplegable, elija IP de origen.

   El valor predeterminado es Ninguno, lo que significa que la afinidad del cliente no está habilitada y Global Accelerator distribuye el tráfico de forma equitativa entre los puntos de enlace de los grupos de puntos de enlace para el agente de escucha.

   Para obtener más información, consulte Afinidad del cliente (p. 29).
7. Elija Add listener (Añadir agente de escucha).

### Para editar un agente de escucha

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.

2. En la aceleradores , selecciona un acelerador.
3. Elija un agente de escucha y, a continuación, elija Editar agente de escucha.
4. En la Editar agente de escucha , cambie los puertos, rangos de puertos o protocolos que desea asociar al agente de escucha.
5. De forma opcional, elija para habilitar la afinidad del cliente. La afinidad del cliente por un oyente significa que Global Accelerator garantiza que las conexiones desde una dirección IP de origen (cliente) específica siempre se direccionen al mismo punto de enlace. Para habilitar este comportamiento, en la lista desplegable, elija IP de origen.

   El valor predeterminado es Ninguno, lo que significa que la afinidad del cliente no está habilitada y Global Accelerator distribuye el tráfico de forma equitativa entre los puntos de enlace de los grupos de puntos de enlace para el agente de escucha.

   Para obtener más información, consulte Afinidad del cliente (p. 29).
6. Seleccione Save.

Para eliminar un agente de escucha

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la aceleradores , selecciona un acelerador.
3. Elija un agente de escucha y, a continuación, elija Eliminar.
4. En el cuadro de diálogo de confirmación, elija Eliminar.

# Afinidad del cliente

Si tiene aplicaciones con estado, puede elegir que Global Accelerator dirigir todas las solicitudes de un usuario a una dirección IP de origen (cliente) específica al mismo recurso de punto de enlace para mantener la afinidad del cliente.

De forma predeterminada, la afinidad del cliente para un agente de escucha está establecida en Ninguno y Global Accelerator distribuye el tráfico de forma equitativa entre los puntos de enlace de los grupos de puntos de enlace para el agente de escucha.

Global Accelerator utiliza un algoritmo de hash de flujo consistente para elegir el punto de enlace óptimo para la conexión de un usuario. Si configura la afinidad de cliente para su Global Accelerator recurso a ser Ningunode Global Accelerator utiliza las propiedades de 5 tuplas—la IP de origen, el puerto de origen, la IP de destino, el puerto de destino y el protocolo—para seleccionar el valor hash. A continuación, elige el punto de enlace que proporciona el mejor desempeño. 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 direccionen al mismo punto de enlace.

Si desea mantener la afinidad del cliente enrutando a un usuario específico—identificado por su dirección IP de origen—al mismo punto de enlace cada vez que se conecten, establezca la afinidad del cliente en IP de origen. Cuando especifique esta opción, Global Accelerator utiliza las propiedades de 2 tuplas—IP de origen e IP de destino—para seleccionar el valor hash y dirigir al usuario al mismo punto de enlace cada vez que se conecte a. Global Accelerator respeta la afinidad del cliente después del grupo de puntos de enlace que ha seleccionado.

# Grupos de puntos de enlace en AWS Global Accelerator

Un grupo de puntos de enlace direcciona las solicitudes a uno o varios puntos de enlace registrados en AWS Global Accelerator. Cuando se añade un agente de escucha, se especifican los grupos de puntos de enlace para Global Accelerator para dirigir el tráfico a. Un grupo de puntos de enlace y todos los puntos de enlace que contiene deben estar en uno AWS Región. Puede añadir diferentes grupos de puntos de enlace para diferentes fines, por ejemplo, para pruebas de implementación blue/green (azul/verde).

Global Accelerator dirige el tráfico a los grupos de puntos de enlace en función de la ubicación del cliente y el estado del grupo de puntos de enlace. Si lo desea, también puede establecer el porcentaje de tráfico que se enviará a un grupo de puntos de enlace. Para ello, utilice la marcación de tráfico para aumentar (marcación ascendente) o disminuir (marcación descendente) el tráfico al grupo. El porcentaje se aplica únicamente al tráfico que Global Accelerator ya está dirigiendo al grupo de puntos de enlace, no todo el tráfico que llega a un agente de escucha.

Puede definir la configuración de comprobación de estado para Global Accelerator para cada grupo de puntos de enlace. Al actualizar la configuración de comprobación de estado, puede cambiar sus requisitos para sondear y verificar el estado de la instancia EC2 y los puntos de enlace de direcciones IP elásticas. Para Balanceador de carga de red y Balanceador de carga de aplicaciones puntos de enlace, configurar los ajustes de comprobación de estado en la Elastic Load Balancing consola de.

Global Accelerator monitoriza continuamente el estado de todos los puntos de enlace que se incluyen en un grupo de puntos de enlace y dirige las solicitudes únicamente a los puntos de enlace activos que están en buen estado. Si no hay ningún punto de enlace en buen estado al que dirigir el tráfico, Global Accelerator dirige las solicitudes a todos los puntos de enlace de.

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

Temas



## Adición, edición o eliminación de un grupo de puntos de enlace

Se trabaja con grupos de puntos de enlace en la AWS Global Accelerator o mediante una operación de API de. Puede añadir o eliminar puntos de enlace de un grupo de puntos de enlace en cualquier momento. Un recurso debe ser válido y estar activo cuando lo añada como punto de enlace.

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

### Para añadir un grupo de puntos de enlace

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la aceleradores , selecciona un acelerador.
3. En la pestaña Agentes de escucha sección, para ID de agente de escucha, elija el ID del agente de escucha al que desea añadir un grupo de puntos de enlace.
4. Elegir Añadir grupo de puntos de enlace.
5. En la sección de un agente de escucha, especifique una región para el grupo de puntos de enlace eligiendo una de la lista desplegable.
6. Opcionalmente, para Marcación de tráfico, introduzca un número de 0 a 100 para establecer un porcentaje de tráfico para este grupo de puntos de enlace. El porcentaje se aplica solo al tráfico que ya se ha dirigido a este grupo de puntos de enlace, no a todo el tráfico del agente de escucha. De forma predeterminada, la marcación de tráfico se establece en 100.
7. De forma opcional, para especificar los valores de comprobación de estado personalizados que se aplicarán a la instancia EC2 y a los puntos de enlace de dirección IP elástica, elija Configurar comprobaciones de estado. Para obtener más información, consulte Opciones de comprobación de estado (p. 32).
8. Opcionalmente, elija Añadir grupo de puntos de enlace para añadir grupos de puntos de enlace adicionales para este agente de escucha u otros agentes de escucha.
9. Elegir Añadir grupo de puntos de enlace.

### Para editar un grupo de puntos de enlace

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la aceleradores , selecciona un acelerador.
3. En la pestaña Agentes de escucha sección, para ID de agente de escucha, elija el ID del agente de escucha al que está asociado el grupo de puntos de enlace.
4. Elegir Editar grupo de puntos de enlace.
5. En la Editar grupo de puntos de enlace , cambia la región, ajusta el porcentaje de marcación de tráfico o selecciona Configurar comprobaciones de estado para modificar la configuración de la comprobación de estado.
6. Seleccione Save.

### Para eliminar un grupo de puntos de enlace

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la aceleradores , selecciona un acelerador.
3. En la pestaña Agentes de escucha , elija un agente de escucha y, a continuación, elija Eliminar.
4. En la pestaña Grupos de punto de enlace , elija un grupo de puntos de enlace y, a continuación, elija Eliminar.
5. En el cuadro de diálogo de confirmación, elija Eliminar.

# Ajustar el flujo de tráfico con marcaciones de tráfico

Para cada grupo de puntos de enlace, puede establecer una marcación de tráfico para controlar el porcentaje de tráfico que se dirige al grupo de. El porcentaje se aplica solo al tráfico que ya está dirigido al grupo de puntos de enlace, no a todo el tráfico del agente de escucha.

De forma predeterminada, la marcación de tráfico se establece en 100 (es decir, 100 %) para todos los grupos de puntos de enlace regionales en un acelerador. La marcación de tráfico le permite realizar fácilmente pruebas de rendimiento o pruebas de implementación blue/green para nuevas versiones en diferentes AWS Regiones, por ejemplo.

A continuación se muestran algunos ejemplos para ilustrar cómo puede utilizar las llamadas de tráfico para cambiar el flujo de tráfico a grupos de punto de enlace.

Actualice su aplicación por región

Si desea actualizar una aplicación en una región o realizar el mantenimiento, establezca primero la marcación de tráfico en 0 para cortar el tráfico de la región. Cuando haya completado el trabajo y esté listo, vuelva a poner la región en servicio, ajuste la marcación del tráfico a 100 para marcar la copia de seguridad del tráfico.

Mezclar el tráfico entre dos regiones

Este ejemplo muestra cómo funciona el flujo de tráfico al cambiar las secciones de tráfico para dos grupos de puntos de enlace regionales al mismo tiempo. Supongamos que tiene dos grupos de puntos de enlace para su acelerador—uno para `us-west-2` y una para la región `us-east-1` Región—y ha establecido las marcas de tráfico en el 50 % para cada grupo de puntos de enlace.

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

- Las primeras 25 solicitudes en cada costa (50 solicitudes en total) se sirven desde su grupo de puntos de enlace cercano. Es decir, 25 solicitudes se dirigen al grupo de puntos de enlace en `us-west-2` y 25 se dirigen al grupo de punto final en `us-east-1`.
- Las siguientes 50 solicitudes se dirigen a las regiones opuestas. Es decir, las siguientes 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 de este escenario es que ambos grupos de puntos de enlace sirven la misma cantidad de tráfico. Sin embargo, cada una de ellas recibe una combinación de tráfico de ambas regiones.

# Opciones de comprobación de estado

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

Important

Global Accelerator requiere las reglas de router y firewall para permitir el tráfico entrante desde las direcciones IP asociadas a Route 53 Los comprobadores de estado de para completar las comprobaciones de estado de los puntos de enlace de instancia EC2 o dirección IP elástica. Puede encontrar información sobre los rangos de direcciones IP asociados a Amazon Route 53 Comprobadores de estado de en Comprobaciones de estado de los grupos de destino en el Guía para desarrolladores de Amazon Route 53.

Puede configurar las siguientes opciones de comprobación de estado para un grupo de puntos de enlace. Si especifica opciones de comprobación de estado, Global Accelerator utiliza la configuración de para las comprobaciones de estado de la instancia EC2 o la dirección IP elástica, pero no para Network Load Balancers o bien Application Load Balancers.

- Para Balanceador de carga de aplicaciones o bien Balanceador de carga de red puntos de enlace, configure las comprobaciones de estado de los recursos mediante Elastic Load Balancing opciones de

configuración. Para obtener más información, consulte Comprobaciones de estado de los grupos de destino. Opciones de comprobación de estado que elija en Global Accelerator no afectan Application Load Balancers o bien Network Load Balancers que ha añadido como puntos de enlace.

- Para los puntos de enlace de la instancia EC2 o la dirección IP elástica que se añaden a un agente de escucha 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 agente de escucha que especificó para su acelerador.
- Para puntos de enlace de instancia EC2 o dirección IP elástica con agentes de escucha UDP, Global Accelerator utiliza el puerto del agente de escucha y el protocolo TCP para las comprobaciones de estado, por lo que debe tener un servidor TCP en el punto de enlace.

  Note

  Asegúrese de comprobar que el puerto que ha configurado para el servidor TCP en cada punto de enlace es el mismo que el puerto que especifica 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 punto de enlace, Global Accelerator marca el punto de enlace como en mal estado, independientemente del estado del punto de enlace.

Puerto de comprobación de estado

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

Protocolo de comprobación de estado

El protocolo que utilizar cuando Global Accelerator realiza comprobaciones de estado en los puntos de enlace que forman parte de este grupo de puntos de enlace.

Intervalo de comprobación de estado

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

Recuento de umbrales

El número de comprobaciones de estado consecutivas necesarias antes de considerar un destino en mal estado o un destino en mal estado.

Cada agente de escucha dirige las solicitudes únicamente a los puntos de enlace en buen estado. Después de añadir un punto de enlace, debe pasar una comprobación de estado para que se considere que está en buen estado. Una vez completada cada comprobación de estado, el agente de escucha cierra la conexión establecida para la comprobación de estado.

# Puntos de enlace en AWS Global Accelerator

Puntos de enlace en AWS Global Accelerator puede ser Network Load Balancersde Application Load Balancers, instancias de Amazon EC2 o direcciones IP elásticas. 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 puntos de enlace mediante el puerto (o el rango de puertos) que especifique para el agente de escucha al que pertenece el grupo de puntos de enlace del punto de enlace.

Cada grupo de puntos de enlace puede tener varios puntos de enlace. Puede añadir cada punto de enlace a varios grupos de puntos de enlace, pero los grupos de puntos de enlace deben estar asociados a diferentes agentes de escucha. Un recurso debe ser válido y estar activo cuando lo añada como punto de enlace.

Global Accelerator monitoriza continuamente el estado de todos los puntos de enlace que se incluyen en un grupo de puntos de enlace. Dirige el tráfico solo a los puntos de enlace activos que están en buen estado. Si Global Accelerator no tiene ningún punto de enlace en buen estado al que dirigir el tráfico, dirige el tráfico a todos los puntos de enlace.

Tenga en cuenta lo siguiente para tipos específicos de Global Accelerator Puntos de enlace de :

Puntos de enlace del balanceador de carga

- Un Balanceador de carga de aplicaciones El punto de enlace de puede estar expuesto a Internet o interno. La Balanceador de carga de red El punto de enlace de debe estar expuesto a Internet.

Amazon EC2 Puntos de enlace de instancia de

- Un punto de enlace de instancia EC2 no puede ser uno de los siguientes tipos: C1, CC1, CC2, CG1, CG2, CR1, CS1, G1, G2, HI1, HS1, M1, M3, M3 o T1.
- Las instancias EC2 se admiten como puntos de enlace solo en algunas AWS Regiones. Para obtener una lista de las regiones admitidas, consulte Compatible AWS Regiones para la conservación de direcciones IP de cliente (p. 45).
- Le recomendamos que elimine una instancia EC2 de Global Accelerator grupos de puntos de enlace de antes de terminar la instancia. Si termina una instancia EC2 antes de eliminarla de un grupo de puntos de enlace en Global Acceleratory, a continuación, cree otra instancia en la misma VPC con la misma dirección IP privada y supere las comprobaciones de estado, Global Accelerator dirigirá el tráfico al nuevo punto de enlace.

Temas



## Adición, edición o eliminación de un punto de enlace

Puede añadir puntos de enlace a grupos de puntos de enlace para que el tráfico se pueda dirigir a sus recursos de. Puede editar un punto de enlace para cambiar la ponderación del punto de enlace. O

puede eliminar un punto de enlace de su acelerador eliminándolo de un grupo de puntos de enlace. La eliminación de un punto de enlace no afecta al propio punto de enlace, pero Global Accelerator ya no puede dirigir el tráfico a ese recurso.

Puede añadir o eliminar puntos de enlace de grupos de puntos de enlace en función del uso de. Por ejemplo, si aumenta la demanda de la aplicación, puede añadir más puntos de enlace a uno o varios grupos de puntos de enlace para gestionar el aumento del tráfico. Global Accelerator comienza a direccionar las solicitudes a un punto de enlace tan pronto como lo añade y el punto de enlace supera las comprobaciones de estado iniciales. Puede administrar el tráfico a los puntos de enlace ajustando las ponderaciones de un punto de enlace para enviar proporcionalmente más o menos tráfico al punto de enlace.

Si va a añadir un punto de enlace con conservación de la dirección IP del cliente, revise primero la información en Compatible AWS Regiones para la conservación de direcciones IP de cliente (p. 45) y Conservar direcciones IP de cliente en AWS Global Accelerator (p. 41).

Puede eliminar los puntos de enlace de los grupos de puntos de enlace, por ejemplo, si necesita prestar servicio a los puntos de enlace de. La eliminación de un punto de enlace lo saca del grupo de puntos de enlace, pero no afecta al punto de enlace de otro modo. Global Accelerator deja de dirigir el tráfico a un punto de enlace en cuanto lo elimina de un grupo de puntos de enlace. El punto de enlace pasa a un estado en el que espera a que se completen todas las solicitudes actuales para que no haya ninguna interrupción del tráfico del cliente que esté en curso. Puede volver a añadir el punto de enlace al grupo de puntos de enlace cuando esté listo para reanudar la recepción de solicitudes.

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

### Para añadir un punto de enlace

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la aceleradores , selecciona un acelerador.
3. En la pestaña Agentes de escucha sección, para ID de agente de escucha, elija el ID de un agente de escucha.
4. En la pestaña Grupos de punto de enlace sección, para ID de grupo de punto de enlace, elija el ID del grupo de puntos de enlace que desea añadir a un punto de enlace.
5. En la pestaña Puntos de enlace selecciona Añadir punto de enlace.
6. En la Añadir puntos de enlace , elija un punto de enlace en la lista desplegable.
7. Opcionalmente, para Peso, introduzca un número de 0 a 255 para establecer una ponderación para el tráfico de enrutamiento a este punto de enlace. Cuando se añaden ponderaciones a los puntos de enlace, se configura Global Accelerator para dirigir el tráfico en función de las proporciones que especifique. De forma predeterminada, todos los puntos de enlace tienen una ponderación de 128. Para obtener más información, consulte Ponderaciones de punto final (p. 36).
8. Opcionalmente, habilite la conservación de la dirección IP del cliente para una Balanceador de carga de aplicaciones Punto de enlace de. Por debajo de Conservar dirección IP del cliente, selecciona Conservar dirección.

   Esta opción siempre está seleccionada para el uso interno Balanceador de carga de aplicaciones y puntos de enlace de instancia EC2 y nunca seleccionados para Balanceador de carga de red y puntos de enlace de dirección IP elástica. Para obtener más información, consulte Conservar direcciones IP de cliente en AWS Global Accelerator (p. 41).

   > **Note**
   >
   > Antes de añadir y comenzar a dirigir el tráfico a los puntos de enlace que conservan la dirección IP del cliente, asegúrese de que todas las configuraciones de seguridad necesarias,

por ejemplo, los grupos de seguridad, se actualizan para incluir la dirección IP del cliente de usuario en las listas de permitidos.

9. Seleccione Add endpoint (Añadir punto de enlace).

### Para editar un punto de enlace

Puede editar una configuración de punto de enlace para cambiar el peso. Para obtener más información, consulte Ponderaciones de punto final (p. 36).

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la aceleradores , selecciona un acelerador.
3. En la pestaña Agentes de escucha sección, para ID de agente de escucha, elija el ID de un agente de escucha.
4. En la pestaña Grupos de punto de enlace sección, para ID de grupo de punto de enlace, elija el ID del grupo de puntos de enlace.
5. Elegir Editar punto de enlace.
6. En la Editar punto de enlace , haz actualizaciones y, a continuación, elige [EMPTY].

### Para eliminar un punto de enlace

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la aceleradores , selecciona un acelerador.
3. En la pestaña Agentes de escucha sección, para ID de agente de escucha, elija el ID de un agente de escucha.
4. En la pestaña Grupos de punto de enlace sección, para ID de grupo de punto de enlace, elija el ID del grupo de puntos de enlace.
5. Elegir Eliminar punto de enlace.
6. En el cuadro de diálogo de confirmación, elija Eliminar.

# Ponderaciones de punto final

Un peso es un valor que determina la proporción de tráfico que Global Accelerator dirige a un punto de enlace. Global Accelerator calcula la suma de las ponderaciones de los puntos de enlace de un grupo de puntos de enlace y, a continuación, dirige el tráfico a los puntos de enlace en función de la relación entre la ponderación de cada punto de enlace y el total de.

El direccionamiento ponderado le permite elegir cuánto tráfico se direcciona a un recurso en un grupo de puntos de enlace. Esto puede ser útil de varias maneras, incluido el balanceo de carga y la prueba de nuevas versiones de una aplicación.

## Cómo funcionan las ponderaciones de punto de enlace

Para utilizar las ponderaciones, asigne a cada punto de enlace de un grupo de puntos de enlace una ponderación relativa que se corresponda con la cantidad de tráfico que desea que le envíe. De forma predeterminada, la ponderación de un punto de enlace es 128—es decir, la mitad del valor máximo para un peso, 255. Global Accelerator envía tráfico a un punto de enlace en función de la ponderación que le asigne como proporción de la ponderación 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 de su tráfico a un punto de enlace y el resto a otro punto de enlace, puede especificar ponderaciones de 1 y 255. El punto de enlace con una ponderación de 1 obtiene 1/256 del tráfico (1/1+255) y el otro punto de enlace obtiene 255/256 (255/1+255). Para modificar gradualmente el equilibrio puede cambiar los pesos. Si desea Global Accelerator para dejar de enviar tráfico a un punto de enlace, puede cambiar la ponderación de ese recurso a 0.

## Conmutación por error para puntos de enlace en mal estado

Si no hay puntos de enlace en buen estado en un grupo de puntos de enlace que tengan una ponderación mayor que cero, Global Accelerator intenta realizar una conmutación por error a un punto de enlace en buen estado con una ponderación mayor que cero en otro grupo de puntos de enlace. Para esta conmutación por error, Global Accelerator pasa por alto el ajuste de marcación de tráfico. Por ejemplo, si un grupo de puntos de enlace tiene una marcación de tráfico establecida en cero, Global Accelerator aún incluye ese grupo de puntos de enlace en el intento de conmutación por error.

Si Global Accelerator no encuentra un punto de enlace en buen estado con una ponderación mayor que cero después de probar tres grupos de puntos de enlace adicionales (es decir, tres AWS Regiones), dirige el tráfico a un punto de enlace aleatorio en el grupo de puntos de enlace más cercano al cliente. Es decir, falla al abrirse.

Tenga en cuenta lo siguiente:

- El grupo de puntos de enlace elegido para la conmutación por error podría ser uno que tenga una marcación de tráfico establecida en cero.
- El grupo de puntos de enlace más cercano podría no ser el grupo de puntos de enlace original. Esto se debe a que Global Accelerator tiene en cuenta la configuración de marcación del tráfico de la cuenta cuando elige el grupo de puntos de enlace original.

Por ejemplo, supongamos que su configuración tiene dos puntos de enlace, uno en buen estado y otro en mal estado, y que ha establecido el peso de cada uno de ellos para que sea mayor que cero. En este caso, Global Accelerator dirige el tráfico al punto de enlace en buen estado. Sin embargo, ahora digamos que establece el peso del único punto de enlace en buen estado en cero. Global Accelerator A continuación, intenta tres grupos de puntos de enlace adicionales para encontrar un punto de enlace en buen estado con una ponderación mayor que cero. Si no encuentra uno, Global Accelerator dirige el tráfico a un punto de enlace aleatorio del grupo de puntos de enlace que está más cerca del cliente.

# Adición de puntos de enlace con conservación de direcciones IP de cliente

Una característica que puede utilizar con algunos tipos de puntos de enlace—en algunas regiones— es conservación de dirección IP de cliente. Con esta característica, se conserva la dirección IP de origen del cliente original para los paquetes que llegan al punto de enlace. Puede utilizar esta característica con Balanceador de carga de aplicaciones y puntos de enlace de instancia EC2. Para obtener más información, consulte Conservar direcciones IP de cliente en AWS Global Accelerator (p. 41).

Si tiene previsto utilizar la característica de conservación de direcciones IP de cliente, tenga en cuenta lo siguiente cuando añada puntos de enlace a Global Accelerator:

Interfaces de red elásticas

Para admitir la conservación de direcciones IP de cliente, Global Accelerator crea interfaces de red elásticas en su AWS cuenta—uno para cada subred en la que haya un punto de enlace. Para obtener más información sobre cómo Global Accelerator funciona con interfaces de red elásticas, consulte Prácticas recomendadas para la conservación de direcciones IP de clientes (p. 44).

Puntos de enlace en subredes privadas

Puedes dirigirte a un Balanceador de carga de aplicaciones o una instancia EC2 en una subred privada con AWS Global Accelerator pero debe tener un puerta de enlace de Internet asociada a la VPC que contiene los puntos de enlace. Para obtener más información, consulte Proteger las conexiones de VPC en AWS Global Accelerator (p. 91).

Añadir la dirección IP del cliente a la lista de permitidos

Antes de añadir y comenzar a dirigir el tráfico a puntos de enlace que conservan la dirección IP del cliente, asegúrese de que todas las configuraciones de seguridad necesarias, por ejemplo, los grupos de seguridad, se actualizan para incluir la dirección IP del cliente de usuario en la lista de permitidos. Las listas de control de acceso (ACL) de red solo se aplican al tráfico de salida (salida). Si necesita filtrar el tráfico de entrada (de entrada), debe utilizar grupos de seguridad.

Configurar listas de control de acceso (ACL) de red

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

Por ejemplo, para permitir que los clientes TCP y UDP utilicen un puerto de origen efímero para conectarse a su punto de enlace a través de Global Accelerator, asocie la subred de su punto de enlace 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 entrante coincidente (rango de puertos 1024-65535, origen 0.0.0.0/0).

Note

El grupo de seguridad y AWS WAF Las reglas de son un conjunto adicional de capacidades que puede aplicar para proteger sus recursos de. Por ejemplo, las reglas de grupo de seguridad entrante asociadas a su Amazon EC2 de instancias de y Application Load Balancers permite controlar los puertos de destino a los que los clientes pueden conectarse a través de Global Accelerator, como el puerto 80 para HTTP o el puerto 443 para HTTPS. Observe que Amazon EC2 Los grupos de seguridad de instancias se aplican a cualquier tráfico que llegue a las instancias, incluido el tráfico de Global Accelerator y cualquier dirección IP pública o elástica que se asigne a su instancia. Como práctica recomendada, utilice subredes privadas si desea asegurarse de que el tráfico se entregue únicamente por Global Accelerator. Asegúrese también de que las reglas del grupo de seguridad de entrada estén configuradas correctamente para permitir o denegar correctamente el tráfico para sus aplicaciones.

# Transición de puntos de enlace para utilizar la conservación de direcciones IP de cliente

Siga las instrucciones de esta sección para realizar la transición de uno o varios puntos de enlace en su acelerador to endpoints that preserve the user client IP address. Si lo desea, puede optar por realizar la transición de un Balanceador de carga de aplicaciones o un punto de enlace de dirección IP elástica a un punto de enlace correspondiente—un Balanceador de carga de aplicaciones o una instancia EC2—que

tiene la conservación de la dirección IP del cliente. Para obtener más información, consulte Conservar direcciones IP de cliente en AWS Global Accelerator (p. 41).

Recomendamos que pase lentamente a utilizar la conservación de direcciones IP de cliente. Primero, añadir nuevo Balanceador de carga de aplicaciones o puntos de enlace de instancia EC2 que habilita para conservar la dirección IP del cliente. A continuación, mueva lentamente el tráfico de los puntos de enlace existentes a los nuevos puntos de enlace configurando las ponderaciones en los puntos de enlace.

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

La conservación de la dirección IP del cliente solo está disponible en determinados AWS Regiones. Para obtener más información, consulte Compatible AWS Regiones para la conservación de direcciones IP de cliente (p. 45).

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

Después de mover una pequeña cantidad de tráfico al nuevo punto de enlace con la conservación de la dirección IP del cliente, pruebe para asegurarse de que la configuración funciona como espera. A continuación, aumente gradualmente la proporción de tráfico al nuevo punto de enlace ajustando las ponderaciones en los puntos de enlace correspondientes.

Para realizar la transición a puntos de enlace que conservan las direcciones IP de cliente, comience por seguir los pasos que se indican aquí para añadir un nuevo punto de enlace y, para estar orientado a Internet Balanceador de carga de aplicaciones , habilite la conservación de direcciones IP de cliente. (La opción de preservación de la dirección IP del cliente siempre está seleccionada para la Application Load Balancers y instancias EC2).

### Para añadir un punto de enlace con conservación de direcciones IP de cliente

1. Abra el cuadro de diálogo Global Accelerator consola de en https://us-west-2.consola.aws.amazon.com/ec2/v2/home?región=us-west-2#Global Accelerator:.
2. En la aceleradores , selecciona un acelerador.
3. En la pestaña Agentes de escucha , elija un agente de escucha.
4. En la pestaña Grupo de punto de enlace , elija un grupo de puntos de enlace.
5. En la pestaña Puntos de enlace selecciona Añadir punto de enlace.
6. En la Añadir puntos de enlace , en la página Puntos de enlace , selecciona un Balanceador de carga de aplicaciones o un punto de enlace de instancia EC2.
7. En la pestaña Peso , elija un número bajo comparado con las ponderaciones que se establecen para los puntos de enlace existentes. Por ejemplo, si el peso de un Balanceador de carga de aplicaciones es 255, podría introducir un peso de 5 para el nuevo Balanceador de carga de aplicaciones, para comenzar con. Para obtener más información, consulte Ponderaciones de punto final (p. 36).
8. Para una nueva Balanceador de carga de aplicaciones punto de enlace, en Conservar dirección IP del cliente, selecciona Conservar dirección. (Esta opción siempre está seleccionada para la Application Load Balancers y instancias EC2).
9. Elija Save changes.

A continuación, siga los pasos que se indican aquí para editar los puntos de enlace existentes correspondientes (que va a sustituir por los nuevos puntos de enlace con la conservación de direcciones

IP de cliente) para reducir las ponderaciones de los puntos de enlace existentes de forma que se les envíe menos tráfico.

### Para reducir el tráfico de los puntos de enlace existentes

1. En la Grupo de punto de enlace , elija un punto de enlace existente que no tenga la conservación de la dirección IP del cliente.
2. Elija Edit.
3. En la Editar punto de enlace , en la página Peso , introduzca un número inferior al número actual. Por ejemplo, si la ponderación de un punto de enlace existente es 255, podría introducir una ponderación de 220 para el nuevo punto de enlace (con conservación de la dirección IP del cliente).
4. Elija Save changes.

Después de probar con una pequeña parte del tráfico original estableciendo la ponderación del nuevo punto de enlace en un número bajo, puede pasar lentamente todo el tráfico ajustando las ponderaciones de los puntos de enlace originales y nuevos.

Por ejemplo, supongamos que comienza con un Balanceador de carga de aplicaciones con un peso establecido en 200, y se añade un nuevo Balanceador de carga de aplicaciones Punto de enlace de con la conservación de la dirección IP del cliente habilitada con una ponderación establecida en 5. Desviar gradualmente el tráfico desde el original Balanceador de carga de aplicaciones a la nueva Balanceador de carga de aplicaciones aumentando el peso de la nueva Balanceador de carga de aplicaciones y reducir el peso del original Balanceador de carga de aplicaciones. Por ejemplo:

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

Cuando ha reducido la ponderación a 0 para el punto de enlace original, todo el tráfico (en este ejemplo) va al nuevo Balanceador de carga de aplicaciones punto de enlace de , que incluye la conservación de la dirección IP del cliente.

Si tiene puntos de enlace adicionales—Application Load Balancers o instancias EC2—que desea realizar la transición para utilizar la conservación de direcciones IP de cliente, repita los pasos de esta sección para realizar la transición.

Si necesita revertir la configuración de un punto de enlace para que el tráfico al punto de enlace no conserve la dirección IP del cliente, puede hacerlo en cualquier momento: aumente la ponderación del punto de enlace que sí lo hace no tiene la conservación de la dirección IP del cliente con el valor original y reduce el peso del punto de enlace con de la dirección IP del cliente a 0.

# Conservar direcciones IP de cliente en AWS Global Accelerator

Sus opciones para conservar y acceder a la dirección IP del cliente para AWS Global Accelerator dependen de los puntos de enlace que ha configurado con su acelerador de. Hay dos tipos de puntos de enlace que pueden conservar la dirección IP de origen del cliente en los paquetes entrantes: Application Load Balancers y Amazon EC2 Instancias de.

- Cuando se utiliza una interfaz Balanceador de carga de aplicaciones como punto de enlace con Global Accelerator, la conservación 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 balanceador de carga. Puede elegir deshabilitar la opción al crear el acelerador o editando el botón acelerador más tarde.
- Cuando se utiliza un sistema interno Balanceador de carga de aplicaciones o una instancia EC2 con Global Accelerator, el punto de enlace siempre tiene habilitada la conservación de la dirección IP del cliente.

> Note
>
> Global Accelerator no admite la conservación de la dirección IP del cliente para Balanceador de carga de red y puntos de enlace de dirección IP elástica.

Cuando planifique añadir la conservación de la dirección IP del cliente, tenga en cuenta lo siguiente:

- Antes de añadir y comenzar a dirigir el tráfico a los puntos de enlace que conservan la dirección IP del cliente, asegúrese de que todas las configuraciones de seguridad necesarias, por ejemplo, los grupos de seguridad, se actualizan para incluir la dirección IP del cliente de usuario en las listas de permitidos.
- La conservación de la dirección IP del cliente solo se admite en determinados AWS Regiones. Para obtener más información, consulte Compatible AWS Regiones para la conservación de direcciones IP de cliente (p. 45).

Temas



## Cómo habilitar la conservación de direcciones IP de clientes

Cuando creas un nuevo acelerador, la conservación de la dirección IP del cliente está habilitada, de forma predeterminada, para los puntos de enlace admitidos.

Tenga en cuenta lo siguiente:

- Interno Application Load Balancers Las instancias EC2 y siempre tienen habilitada la conservación de direcciones IP de cliente. No puede deshabilitar la opción para estos puntos de enlace.
- Cuando utilizas la opción AWS para crear una nueva acelerador, la opción para la conservación de la dirección IP del cliente está habilitada de forma predeterminada para Balanceador de carga de aplicaciones Puntos de enlace de. Puede deshabilitar la opción en cualquier momento si no desea la conservación de la dirección IP del cliente para una Balanceador de carga de aplicaciones Punto de enlace de.
- Cuando utilizas la opción AWS La CLI de o una acción de la API para crear una nueva acelerador y no especifica la opción para la conservación de la dirección IP del cliente, orientada a Internet Balanceador de carga de aplicaciones Los puntos de enlace de tienen la conservación de direcciones IP de cliente habilitada de forma predeterminada.
- Global Accelerator no admite la conservación de la dirección IP del cliente para Balanceador de carga de red y puntos de enlace de dirección IP elástica.

Para los aceleradores, puede realizar la transición de puntos de enlace sin que se conserve la dirección IP del cliente a puntos de enlace que conserven la dirección IP del cliente. Existente Balanceador de carga de aplicaciones Los puntos de enlace de se pueden pasar a nuevos Balanceador de carga de aplicaciones Los puntos de enlace de y los puntos de enlace de direcciones IP elásticas existentes se pueden pasar a puntos de enlace de instancia EC2. (Balanceador de carga de red Los puntos de enlace de no admiten la conservación de direcciones IP de cliente). Para realizar la transición a los nuevos puntos de enlace, le recomendamos que mueva el tráfico lentamente desde un punto de enlace existente a un nuevo punto de enlace que tenga la conservación de la dirección IP del cliente haciendo lo siguiente:

- Para los Balanceador de carga de aplicaciones puntos de enlace, añadir primero a Global Accelerator un duplicado Balanceador de carga de aplicaciones punto de enlace que tiene como destino los mismos backends y, si es un Balanceador de carga de aplicaciones, habilite la conservación de la dirección IP del cliente para él. A continuación, ajuste las ponderaciones en los puntos de enlace para mover lentamente el tráfico desde el balanceador de carga que no tener habilitada la conservación de direcciones IP de cliente en el balanceador de carga con la conservación de la dirección IP del cliente.
- Para un punto de enlace de dirección IP elástica existente, puede mover el tráfico a un punto de enlace de instancia EC2 con la conservación de la dirección IP del cliente. Añada primero un punto de enlace de instancia EC2 a Global Acceleratory, a continuación, ajuste las ponderaciones en los puntos de enlace para mover lentamente el tráfico desde el punto de enlace de la dirección IP elástica al punto de enlace de la instancia EC2.

Para obtener orientación sobre la transición paso a paso, consulte Transición de puntos de enlace para utilizar la conservación de direcciones IP de cliente (p. 38).

# Ventajas de la conservación de la dirección IP del cliente

Para los puntos de enlace que no tienen habilitada la conservación de direcciones IP de cliente, las direcciones IP utilizadas por el Global Accelerator El servicio de en la red de borde de sustituye la dirección IP del usuario solicitante como dirección de origen en los paquetes entrantes. La información de conexión del cliente original—como la dirección IP del cliente y el puerto del cliente—no se conserva ya que el tráfico viaja a 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 obtener acceso a la dirección IP del cliente original mediante puntos de enlace con la conservación de direcciones IP del cliente. Por ejemplo, cuando

tiene la dirección IP del cliente, puede recopilar estadísticas basadas en las direcciones IP del cliente. También puede utilizar filtros basados en direcciones IP, como grupos de seguridad en balanceadores de carga de aplicaciones para filtrar el tráfico. Puede aplicar una lógica específica a la dirección IP de un usuario en las aplicaciones que se ejecutan en los servidores de capa web detrás de esa Balanceador de carga de aplicaciones punto de enlace mediante el uso del punto de enlace del balanceador de carga `X-Forwarded-For` , que contiene la información de la dirección IP del cliente original. También puede utilizar la conservación de direcciones IP de cliente en reglas de grupos de seguridad en los grupos de seguridad asociados a su Balanceador de carga de aplicaciones. Para obtener más información, consulte Cómo se conserva la dirección IP del cliente en AWS Global Accelerator (p. 43). Para los puntos de enlace de instancia EC2, la dirección IP del cliente original se conserva.

Para los puntos de enlace que no tienen conservación de la dirección IP del cliente, puede filtrar por la dirección IP de origen que Global Accelerator utiliza cuando reenvía el tráfico desde el borde. Puede ver información sobre las direcciones IP de origen (que también son direcciones IP de cliente, cuando la conservación de direcciones IP de cliente está habilitada) de los paquetes entrantes revisando su Global Accelerator Los registros de flujo de. Para obtener más información, consulte Los rangos de ubicación y dirección IP de Global Accelerator servidores perimetrales (p. 6) y Registros de flujo en AWS Global Accelerator (p. 47).

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

AWS Global Accelerator conserva la dirección IP de origen del cliente de forma diferente para Amazon EC2 de instancias de y Application Load Balancers:

- Para un punto de enlace de instancia EC2, la dirección IP del cliente se conserva para todo el tráfico.
- Para un Balanceador de carga de aplicaciones punto de enlace con conservación de la dirección IP del cliente, Global Accelerator funciona junto con el Balanceador de carga de aplicaciones para proporcionar un `X-Forwarded` encabezado, `X-Forwarded-For`, que incluye la dirección IP del cliente original para que la capa web pueda obtener acceso a ella.

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 mensaje. También hay encabezados HTTP no estándar disponibles que se utilizan habitualmente en las aplicaciones. Algunos de los encabezados HTTP no estándar tienen un `X-Forwarded` prefijo.

Porque un Balanceador de carga de aplicaciones termina las conexiones TCP entrantes y crea nuevas conexiones a los destinos del backend; 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 Balanceador de carga de aplicaciones. Sin embargo, un Balanceador de carga de aplicaciones 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.

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

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

El siguiente ejemplo 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 de clientes

Cuando se utiliza la conservación de direcciones IP de cliente en 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 conservación de direcciones IP de cliente, Global Accelerator crea interfaces de red elásticas en su AWS cuenta—uno para cada subred en la que haya un punto de enlace. 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 dirigir el tráfico a los puntos de enlace configurados detrás de un acelerador de. Los puntos de enlace admitidos para enrutar el tráfico de esta forma son Application Load Balancers (internos y orientados a Internet) y Amazon EC2 Instancias de.

> Note
>
> Cuando se añade un Balanceador de carga de aplicaciones o un punto de enlace de instancia EC2 en Global Accelerator, habilita el tráfico de Internet para que fluya directamente hacia y desde el punto de enlace en las nubes virtuales privadas (VPC) dirigiéndolo a una subred privada. Para obtener más información, consulte Proteger las conexiones de VPC en AWS Global Accelerator (p. 91).

Cómo Global Accelerator utiliza interfaces de red elásticas

Cuando tienes un Balanceador de carga de aplicaciones con la preservación de la dirección IP del cliente habilitada, el número de subredes en las que se encuentra el balanceador de carga determina el número de interfaces de red elásticas que Global Accelerator crea en su cuenta. Global Accelerator crea una interfaz de red elástica para cada subred que tiene al menos una interfaz de red elástica de la Balanceador de carga de aplicaciones que está enfrentada por un acelerador en su cuenta.

Los siguientes ejemplos ilustran cómo funciona:

- Ejemplo: = 1. Si un Balanceador de carga de aplicaciones tiene interfaces de red elásticas en subnetA y subnetB y, a continuación, añade el balanceador de carga como un acelerador punto de enlace, Global Accelerator crea dos interfaces de red elásticas, una en cada subred.
- Ejemplo: = 2. Si añade, por ejemplo, un ALB1 que tiene interfaces de red elásticas en subnetA y subnetB a Accelerator1 y, a continuación, añade un ALB2 con interfaces de red elásticas en subnetA y subnetB a Accelerator2, Global Accelerator crea solo dos interfaces de red elásticas: una en la subred A y otra en la subred B.
- Ejemplo 3 Si añade un ALB1 que tiene interfaces de red elásticas en subredA y subredB a Accelerator1 y, a continuación, añade un ALB2 con adaptadores de red elásticos en subredA y subredC a Accelerator2, Global Accelerator crea tres interfaces de red elásticas: una en la subred A, otra en la subred B y otra en la subred C. La interfaz de red elástica de la subredA entrega tráfico en para Accelerator1 y Accelerator2.

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

Las interfaces de red elástica lógicas que Global Accelerator Las crea no representan un único host, un cuello de botella de rendimiento ni un único punto de error. Como otros AWS Servicios de que aparecen como una única interfaz de red elástica en una zona de disponibilidad o subred—servicios como una gateway de traducción de direcciones de red (NAT) o un balanceador de carga de red—Global Accelerator se implementa como un servicio de escalado horizontal de alta disponibilidad.

Evaluar el número de subredes que utilizan los puntos de enlace de los aceleradores de para determinar el número de interfaces de red elásticas que Global Accelerator creará. Antes de crear un acelerador, asegúrese de que dispone de suficiente espacio de dirección IP para las interfaces de

red elásticas necesarias, al menos una dirección IP libre por subred relevante. Si no tiene suficiente espacio de direcciones IP libres, debe crear o utilizar una subred que tenga suficiente espacio de direcciones IP libres para su Balanceador de carga de aplicaciones y asociados Global Accelerator de redes elásticas.

¿Cuándo? Global Accelerator determina que una interfaz de red elástica no se está utilizando en ninguno de los puntos de enlace en aceleradores en tu cuenta, Global Accelerator elimina la interfaz.

Grupos de seguridad creados por Global Accelerator

Revise la siguiente información y 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 de grupo de seguridad para estos grupos.
- Global Accelerator no elimina los grupos de seguridad que crea. Sin embargo, Global Accelerator elimina una interfaz de red elástica si no la utiliza ninguno de los puntos de enlace de aceleradores en su cuenta.
- Puede utilizar los grupos de seguridad creados por Global Accelerator como un grupo de origen en otros grupos de seguridad que mantenga, pero Global Accelerator solo reenvía el tráfico a los destinos que especifique en la VPC.
- Si modifica las reglas del grupo de seguridad creadas por Global Accelerator, el punto de enlace podría volverse en mal estado. Si esto sucede, póngase en contacto con AWS Asistencia para obtener ayuda.
- Global Accelerator crea un grupo de seguridad específico para cada VPC. Las interfaces de red elásticas que se crean para los puntos de enlace de dentro de una VPC específica utilizan el mismo grupo de seguridad, independientemente de la subred con la que esté asociada una interfaz de red elástica.

# Compatible AWS Regiones para la conservación de direcciones IP de cliente

Puede habilitar la conservación de direcciones IP de cliente para AWS Global Accelerator en los siguientes AWS Regiones.

| Nombre de la región | Región |
|---|---|
| US East (N. Virginia) | `us-east-1` |
| EE.UU. Este (Ohio) | `us-east-2` |
| EE.UU. Oeste (Norte de California) | `us-west-1` |
| EE.UU. Oeste (Oregón) | `us-west-2` |
| África (Ciudad del Cabo) | `af-south-1` |
| Asia Pacífico (Hong Kong) | `ap-east-1` |
| Asia Pacífico (Mumbai) | `ap-south-1` |
| Asia Pacífico (Singapur) | `ap-southeast-1` |
| Asia Pacífico (Sídney) | `ap-southeast-2` |

| Nombre de la región | Región |
|---|---|
| Asia Pacífico (Tokio) | `ap-northeast-1` |
| Asia Pacífico (Seúl) | `ap-northeast-2` |
| Canadá (Central) | `ca-central-1` |
| Europa (Fráncfort) | `eu-central-1` |
| Europa (Irlanda) | `eu-west-1` |
| Europa (Londres) | `eu-west-2` |
| Europa (Milán) | `eu-south-1` |
| Europa (París) | `eu-west-3` |
| Europa (Estocolmo) | `eu-north-1` |
| Medio Oriente (Baréin) | `me-south-1` |
| América del Sur (São Paulo) | `sa-east-1` |

# Registro y monitoreo en AWS Global Accelerator

Puede utilizar registros de flujo de y AWS CloudTrail para controlar su acelerador en AWS Global Accelerator, analizar patrones de tráfico y solucionar problemas con los agentes de escucha y puntos de enlace.

Temas



## Registros de flujo en AWS Global Accelerator

Los logs de flujo le permiten capturar información sobre el tráfico de dirección IP que entra y sale de las interfaces de red de su acelerador en AWS Global Accelerator. Los datos de registro de flujo se publican en Amazon S3, donde puede recuperar y ver los datos después de haber creado un registro de flujo.

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

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 5 tuplas es un conjunto de cinco valores diferentes que especifican el origen, el destino y el protocolo de un flujo de 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 tardar hasta 1 minuto.

CloudWatch Logs Los cargos de se aplican cuando se utilizan registros de flujo de , incluso cuando los registros se publican directamente en Amazon S3. Para obtener más información, consulte Entregar registros a S3 en Amazon CloudWatch Precios.

Temas



### Publicar logs de flujo en Amazon S3

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

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

## Archivos de registros de flujo

Los logs de flujo recopilan registros de logs de flujo, los consolidan en archivos log y, a continuación, se publican los archivos de log en el bucket de Amazon S3 a intervalos de cinco minutos. Cada archivo de registro contiene registros de registro de flujo para el tráfico de dirección 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 log se guardan en el bucket de Amazon S3 especificado con una estructura de carpetas que viene determinada por el ID del log 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 de registro 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 carpetas y nombres de archivos para los archivos de registro:

- La marca de tiempo utiliza el formato `YYYYMMDDTHHmmZ`.
- Si especifica la barra inclinada (/) para el prefijo del bucket de S3, la estructura de carpetas del bucket de archivos de registro incluirá una barra inclinada doble (//), como la siguiente:

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

El siguiente ejemplo muestra la estructura de carpetas y el nombre de archivo de un archivo de registro para un registro de flujo creado por AWS cuenta `123456789012` para una acelerador con un ID de `1234abcd-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 intercaladas con varios registros de 5 tuplas; es decir, `client_ip`de `client_port`de `accelerator_ip`de `accelerator_port`de `protocol`. Para ver todos los archivos de log de flujo de su acelerador, busque las entradas agregadas por el `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 logs de flujo

Por defecto, Amazon S3 Los buckets de 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 permisos de acceso a otros recursos y usuarios escribiendo una política de acceso.

Si el usuario que crea el registro de flujo es el propietario del bucket, el servicio asocia automáticamente la siguiente política al bucket para conceder al registro 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 añadir manualmente la política anterior al bucket y especificar el creador del log de flujo AWS del ID de cuenta de. Para obtener más información, consulte ¿Cómo agrego una política de bucket en S3? en la Guía de introducción a Amazon Simple Storage Service. 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 AWS cuentas 123123123123 y 456456456456 para publicar registros de flujo en una carpeta denominada `flow-logs` en un bucket denominado `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

Te recomendamos que concedas la `AWSLogDeliveryAclCheck` y `AWSLogDeliveryWrite` Los permisos a la entidad principal del servicio de entrega de registros en lugar de a los permisos AWS del ARN de la cuenta de.

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

Si ha habilitado el cifrado del lado del servidor para su Amazon S3 bucket de con AWS Claves administradas por KMS (SSE-KMS) con una clave maestra del cliente (CMK) administrada por el cliente: debe añadir lo siguiente a la política de claves de su CMK para que los registros de flujo puedan escribir archivos de registro en el bucket de :

```
{
    "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 log 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 log creados por un log 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 Guía de introducción a Amazon Simple Storage Service.

## Habilitar la publicación de registros de flujo 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. Creación de un Amazon S3 para los registros de flujo en su AWS cuenta.
2. Añada el campo IAM para la política de AWS El usuario de que habilita los registros de flujo de. Para obtener más información, consulte Roles de IAM para publicar registros de flujo en Amazon S3 (p. 48).
3. Ejecute lo siguiente AWS Comando de la CLI de , con la Amazon S3 El nombre y el prefijo del bucket de 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
```

## Procesar registros de logs de flujo en Amazon S3

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

# Tiempo de entrega del archivo de registro

AWS Global Accelerator envía archivos de registro para el acelerador hasta varias veces por hora. En general, un archivo de registro contiene información sobre las solicitudes que el acelerador recibido durante un periodo de tiempo determinado. Global Accelerator suele entregar el archivo de registro para ese periodo de tiempo a su Amazon S3 del bucket de en el plazo de una hora desde los eventos que aparecen en el registro. Algunas o todas las entradas del archivo de registro de un periodo de tiempo pueden a veces 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 la información para su acelerador de todas las ubicaciones de borde de que recibieron solicitudes durante el periodo de tiempo que abarca el archivo de registro.

Global Accelerator comienza a entregar archivos de registro de forma fiable unas cuatro horas después de habilitar el registro de. Es posible que obtenga algunos archivos de registro antes de esa hora.

Note

Si ningún usuario se conecta a tu acelerador durante el periodo de tiempo, no recibirá ningún archivo de registro para ese periodo.

# Sintaxis de registro de logs 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 de , que incluye `vpc_id`, se genera cuando Global Accelerator envía tráfico a un punto de enlace con la conservación 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 logs de flujo. |
| `aws_account_id` | El AWS : ID de cuenta de para el registro de flujo. |
| `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:<br>• `ACCEPT`: : los grupos de seguridad o las ACL de red han permitido el tráfico registrado. El valor es siempre ACEPTAR. |
| `log-status` | El estado de registro del log de flujo: |

| Campo | Descripción |
| --- | --- |
| | • `OK`: : los datos se registran normalmente en los destinos elegidos.<br>• `NODATA`: : no ha habido tráfico de red entrante ni saliente de la interfaz de red durante la ventana de captura.<br>• `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_address_ip` | La dirección IP utilizada por el Global Accelerator de la interfaz de red de. |
| `globalaccelerator_port_used` | El puerto utilizado por el Global Accelerator de la interfaz de red de. |
| `endpoint_region` | El AWS Región en la que se encuentra el punto de enlace. |
| `globalaccelerator_region` | La ubicación de borde (punto de presencia) que atienda 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 el Global Accelerator de red (`INGRESS`) o devolviéndole al cliente (`EGRESS`). |
| `vpc_id` | El identificador de VPC. Incluido con los registros de flujo de la versión 2.0 cuando Global Accelerator envía tráfico a un punto de enlace con la conservación de la dirección IP del cliente. |

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

# Uso de Amazon CloudWatch con AWS Global Accelerator

AWS Global Accelerator publica puntos de datos en Amazon CloudWatch sobre sus aceleradores. CloudWatch le permite recuperar estadísticas sobre esos puntos de datos en un conjunto ordenado de datos de series temporales que reciben el nombre de métricas. 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 monitorizar el tráfico a través de una 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 únicamente notifica las métricas a CloudWatch cuando las solicitudes fluyen a través de la acelerador. Si las solicitudes fluyen a través de la aceleradorde Global Accelerator mide y envía sus métricas en intervalos de 60 segundos. Si no hay solicitudes que fluyan a través del acelerador o no hay datos para una métrica, la métrica no se notifica.

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

Instancias de destino que están fuera de línea especificando un grupo de recursos de AWS como destino.Contenido

# Métricas de Global Accelerator

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

| Métrica | Descripción |
|---|---|
| `NewFlowCount` | El número total de nuevos flujos TCP y UDP (o conexiones) establecidos desde los clientes a los puntos de enlace en el periodo de tiempo.<br><br>Criterios de notificación: Hay un valor distinto de cero.<br><br>Estadísticas: La única estadística útil es `Sum`.<br><br>Dimensions<br><br>• `Accelerator`<br>• `Accelerator, Listener`<br>• `Accelerator, Listener, EndpointGroup`<br>• `Accelerator, SourceRegion`<br>• `Accelerator, DestinationEdge`<br>• `Accelerator, TransportProtocol`<br>• `Accelerator, AcceleratorIPAddress` |
| `ProcessedBytesIn` | El número total de bytes entrantes procesados por el acelerador, incluidos los encabezados TCP/IP. Este recuento incluye el tráfico a los puntos de enlace, menos el tráfico de comprobación de estado.<br><br>Criterios de notificación: Hay un valor distinto de cero.<br><br>Estadísticas: La única estadística útil es `Sum`.<br><br>Dimensions<br><br>• `Accelerator`<br>• `Accelerator, Listener`<br>• `Accelerator, Listener, EndpointGroup`<br>• `Accelerator, SourceRegion`<br>• `Accelerator, DestinationEdge`<br>• `Accelerator, TransportProtocol`<br>• `Accelerator, AcceleratorIPAddress` |
| `ProcessedBytesOut` | El número total de bytes salientes procesados por el acelerador, incluidos los encabezados TCP/IP. Este recuento incluye el tráfico de los puntos de enlace de , menos el tráfico de comprobación de estado.<br><br>Criterios de notificación: Hay un valor distinto de cero.<br><br>Estadísticas: La única estadística útil es `Sum`. |

| Métrica | Descripción |
| --- | --- |
| | Dimensions<br>• `Accelerator`<br>• `Accelerator, Listener`<br>• `Accelerator, Listener, EndpointGroup`<br>• `Accelerator, SourceRegion`<br>• `Accelerator, DestinationEdge`<br>• `Accelerator, TransportProtocol`<br>• `Accelerator, AcceleratorIPAddress` |

# Dimensiones métricas de los aceleradores

Para filtrar las métricas de su acelerador, utilice las siguientes dimensiones.

| Dimensión | Descripción |
| --- | --- |
| `Accelerator` | Filtra los datos de métricas por acelerador. Especifique la acelerador por el identificador del acelerador (la parte final del acelerador del ARN). 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 agente de escucha. Especifique el agente de escucha mediante el ID de agente de escucha (la última parte del ARN del agente de escucha). Por ejemplo, si el ARN es `arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123wxyz`, especifique lo siguiente: **`0123wxyz`**. |
| `EndpointGroup` | Filtra los datos de métricas por grupo de puntos de enlace. Especifique el grupo de puntos de enlace mediante la AWS la región, por ejemplo, **`us-east-1`** (todo en minúsculas). |
| `SourceRegion` | Filtra los datos de métricas por región de origen, que es el área geográfica del AWS Las regiones en las que los puntos de enlace de la aplicación ejecutan. La región de origen es una de las siguientes:<br>• [EMPTY] – Estados Unidos y Canadá<br>• UE – Europa<br>• [EMPTY] – Pacífico asiático*<br>• [EMPTY] – Corea del Sur<br>• [EMPTY] – La India<br>• [EMPTY] – Australia<br>• [EMPTY] – Oriente Medio<br>• [EMPTY] – América del Sur<br><br>*Excepto Corea del Sur e India |

| Dimensión | Descripción |
| --- | --- |
| `DestinationEdge` | Filtra los datos de indicador por borde de destino, que es el área geográfica del AWS Las ubicaciones de borde de que sirven al tráfico del cliente. El límite de destino es uno de los siguientes:<br>• [EMPTY] – Estados Unidos y Canadá<br>• UE – Europa<br>• [EMPTY] – Pacífico asiático*<br>• [EMPTY] – Corea del Sur<br>• [EMPTY] – La India<br>• [EMPTY] – Australia<br>• [EMPTY] – Oriente Medio<br>• [EMPTY] – América del Sur<br>• [EMPTY] – Sudáfrica<br><br>*Excepto Corea del Sur e India |
| `TransportProtocol` | Filtra los datos de métricas por protocolo de transporte: de 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 las 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 datos de métricas durante 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 los bytes procesados para una acelerador donde los bytes se distribuyen desde AWS de borde en Europa (el borde de destino es "EU").

A continuación se muestran ejemplos de combinaciones de métricas/dimensiones que podrían resultarle útiles:

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

# [EMPTY] CloudWatch Métricas de para sus aceleradores de

Puedes ver el CloudWatch Métricas de para los aceleradores de mediante la CloudWatch o la consola de AWS CLI. En la consola de , las métricas se muestran como gráficos de monitorización. Los gráficos de monitorización solo muestran puntos de datos si el acelerador está activo y recibe solicitudes.

Debe ver CloudWatch Métricas de para Global Accelerator en el EE.UU. Oeste (Oregón) Región , tanto en la consola de como al utilizar la AWS CLI. Cuando utilizas la opción AWS CLI, especifica el EE.UU.

Oeste (Oregón) Región del comando de la mediante la inclusión del siguiente parámetro: `--region us-west-2`.

### Para consultar las métricas desde la consola de CloudWatch

1. Abra la consola de CloudWatch en https://us-west-2.console.aws.amazon.com/cloudwatch/home?región=us-west-2.
2. En el panel de navegación, seleccione Metrics.
3. Seleccione la opción AceleradorGlobal espacio 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 AWS CLI

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 AWS CLI

Utilice lo siguiente obtener-estadísticas-métricas para obtener estadísticas de una métrica y dimensión especificadas. Observe que CloudWatch trata cada combinación única de dimensiones como una métrica independiente. No puede recuperar estadísticas mediante combinaciones de dimensiones que no se hayan publicado específicamente. Debe especificar las mismas dimensiones que se utilizaron al crear las métricas.

En el siguiente ejemplo 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 AWS Global Accelerator Llamadas a la API de

AWS Global Accelerator está integrado con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Global Accelerator. CloudTrail captura todas las llamadas a la API para Global Accelerator como eventos, incluidas las llamadas desde el Global Accelerator y desde las llamadas de código a la consola de Global Accelerator de la API de. 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 Global Accelerator en CloudTrail

CloudTrail se habilita en su 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 eventos de los demás servicios de AWS en el Event history (Historial 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

- CloudTrail Servicios e integraciones compatibles
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recepción de 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, que están documentadas en la Referencia de la API de AWS Global Accelerator. Por ejemplo, las llamadas a la `CreateAcceleratorde` `ListAccelerators` y `UpdateAccelerator` Las operaciones de generan entradas en el CloudTrail Archivos de registro de.

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 del nodo 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 los archivos de registro de Global Accelerator

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. Cada archivo de registro con formato JSON de CloudTrail puede contener una o varias 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.

El siguiente ejemplo muestra una CloudTrail que incluye estas Global Accelerator acciones:

- Enumeración de los aceleradores de una cuenta: `eventName` es `ListAccelerators`.
- Creación de un agente de escucha: `eventName` es `CreateListener`.
- Actualización de un agente de escucha: `eventName` es `UpdateListener`.
- Descripción de un oyente: `eventName` es `DescribeListener`.
- Enumeración de los agentes de escucha de una cuenta: `eventName` es `ListListeners`.
- Eliminación de un agente de escucha: `eventName` es `DeleteListener`.

```
v{
  "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 servicios de AWS en la nube de AWS. AWS también 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, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube – su responsabilidad viene determinada por el 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 muestra cómo configurar Global Accelerator para cumplir sus objetivos de seguridad.

Temas:



# Administración de identidades y accesos para AWS Global Accelerator

AWS Identity and Access Management (IAM) es un AWS que ayuda a un administrador a controlar de forma segura el acceso a AWS recursos, incluidos AWS Global Accelerator Los recursos de. Los administradores utilizan IAM para controlar quién es autenticado (inició sesión) y autorizado (tiene permisos) para utilizar Global Accelerator Los recursos de. IAM es una característica incluida con su AWS cuenta sin cargo adicional.

> **Important**
>
> Si no está familiarizado con IAM, revise la información introductoria de esta página y, a continuación, consulte Introducción a IAM (p. 83). Opcionalmente, puede obtener más información sobre la autenticación y el control de acceso viendo ¿Qué es la autenticación? (p. 76)de ¿Qué es el control de acceso? (p. 77), y ¿Qué son las políticas? (p. 80).

Temas:

# Conceptos y términos

Autenticación – Para iniciar sesión en AWS, debe utilizar una de las siguientes opciones: usuario raíz credenciales (no se recomienda), IAM las credenciales de usuario de o las credenciales temporales mediante IAM Roles de. Para obtener más información acerca de estas entidades, consulte ¿Qué es la autenticación? (p. 76).

Control de acceso – AWS Los administradores de utilizan políticas de para controlar el acceso a AWS recursos, como aceleradores en Global Accelerator. Para obtener más información, consulte ¿Qué es el control de acceso? (p. 77) y ¿Qué son las políticas? (p. 80).

> 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, solo porque haya creado un recurso no significa que tenga acceso completo automáticamente a ese 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:

AWS servicios, como Global Accelerator y IAM, normalmente incluyen objetos denominados recursos. En la mayoría de los casos, puede crear, administrar y eliminar estos recursos del servicio. IAM Los recursos de incluyen usuarios, grupos, roles y políticas:

Usuarios

Un IAM El usuario de 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 AWS CLI o con la API de AWS.

Grupos

Un IAM grupo es una colección de IAM usuarios de. Los administradores pueden utilizar grupos de para especificar permisos para los usuarios miembros. Esto facilita a un administrador la administración de permisos para varios usuarios.

Roles:

Un IAM El rol de no tiene ninguna credencial a largo plazo (contraseña o claves de acceso) asociada. Cualquier persona que la necesite y tenga permiso para ello puede asumir un rol. Un usuario de IAM puede asumir un rol 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 puede asumir un rol de servicio para obtener acceso a los recursos de AWS en nombre de usted.

Políticas:

Las políticas son documentos JSON que definen los permisos para el objeto al que se asocian. AWS es compatible Políticas basadas en identidad de que asocia a identidades de (usuarios,

grupos o roles). Algunos servicios de AWS permiten asociar políticas basadas en recursos a los recursos para controlar lo que una entidad principal (persona o aplicación) puede hacer con ese recurso. Global Accelerator es compatible con (no admite) las políticas basadas en recursos.

Identidades

Las identidades son IAM Los recursos de para los que puede definir permisos. Estos incluyen usuarios, grupos y roles.

Entidades

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

Entidades principales

En AWS, una entidad principal es una persona o aplicación que utiliza una entidad para iniciar sesión y realizar solicitudes a AWS. Como entidad principal, puede utilizar la función Consola de administración de AWS, el AWS CLI, o el AWS La API para realizar una operación (como eliminar una 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 un contexto para la 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, consulte Entender cómo funciona IAM en la Guía del usuario de IAM. Para obtener más información acerca de cómo AWS determina si una solicitud está permitida, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

# Permisos necesarios para el acceso a la consola, la administración de la 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 Global Accelerator acelerador

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

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

Note

Si crea una política de permisos basada en identidad que es más restrictiva, los usuarios con esa política no podrán crear un acelerador de.

```
{
      "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 de 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 pueden seguir utilizando el Global Accelerator de la consola de o de la API, asocie también una de las siguientes AWS Las políticas administradas por al usuario de , tal y como se describe en Creación de políticas en la pestaña JSON:

```
        GlobalAcceleratorReadOnlyAccess
        GlobalAcceleratorFullAccess
```

Adjunte la primera política, `GlobalAcceleratorReadOnlyAccess`, si los usuarios solo necesitan ver información en la consola de o realizar llamadas al AWS CLI o la API que utiliza `List*` o bien `Describe*` de las operaciones de.

Adjunte la segunda política, `GlobalAcceleratorFullAccess`, a los usuarios que necesitan crear o realizar actualizaciones en aceleradores de. La política de acceso completo incluye lleno permisos para Global Accelerator así como también describir permisos para Amazon EC2 y Elastic Load Balancing.

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

A continuación se muestra 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 la 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 autoadministrar sus credenciales (p. 87).

Como administrador de AWS, necesita acceso completo a IAM, con el fin de poder crear y administrar los usuarios, los grupos, los roles y las políticas de IAM. Debe usar la política AdministratorAccess administrada por AWS, que incluye acceso completo a la totalidad de AWS. Esta política no proporciona acceso a la AWS Billing and Cost Management o permitir tareas que requieren Usuario de la cuenta raíz de AWS las credenciales. Para obtener más información, consulte Tareas de AWS que requieren credenciales de Usuario raíz de la cuenta de AWS en la AWS General Reference.

> 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 IAM usuario administrador (p. 84).

## Permisos necesarios para el control de acceso

Si el administrador le ha proporcionado credenciales de usuario de IAM, estas habrán asociado políticas a ese usuario de IAM para controlar a qué recursos puede tener acceso. Para ver las políticas de que están

asociadas a su identidad de usuario en la Consola de administración de AWS, debe tener los siguientes permisos:

```
{
    "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.

# Cómo entender cómo Global Accelerator funciona con IAM

Los servicios pueden funcionar con IAM de varias maneras:

Acciones

Global Accelerator admite el uso de acciones de 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 a la `GetPolicy` AWS La operación de la API para ver una política, un administrador debe asociar una política que permita el `iam:GetPolicy` acción.

El siguiente ejemplo de política permite a un usuario realizar el `CreateAccelerator` operación para crear mediante programación un acelerador para su AWS cuenta:

```
{
   "Version": "2018-08-08",
   "Statement": [
      {
```

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

Permisos de nivel de recursos

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

Políticas basadas en recursos

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

Autorización basada en etiquetas

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

Credenciales temporales

Global Accelerator admite las credenciales temporales. Con las credenciales temporales, puede iniciar sesión con federación, asumir un IAM rol de o asumir un rol de entre cuentas. Puede obtener credenciales de seguridad temporales llamando a AWS STS Operaciones de API como, por ejemplo, `AssumeRole` o bien `GetFederationToken`.

Roles vinculados a servicios

Global Accelerator admite Roles vinculados a servicios de. 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 admite roles de servicio de. Esta característica permite que un servicio asuma un rol de 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 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 roles de IAM.

Temas

## No tengo autorización para realizar una acción en Global Accelerator

Si el Consola de administración de AWS indica que no está autorizado para realizar una acción, debe ponerse en contacto con el administrador que le proporcionó su nombre de usuario y contraseña.

El siguiente ejemplo se produce cuando un IAM nombre de usuario `my-user-name` intenta utilizar 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 a su administrador que actualice sus políticas para permitirle acceder a la `my-example-accelerator` del recurso con la `aws-globalaccelerator:CreateAccelerator` acción.

## 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 le conceda los permisos correctos en Global Accelerator.

Para comenzar trabajar enseguida, consulte Introducción a IAM (p. 83).

## Deseo entender IAM sin convertirme en un experto

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

- ¿Qué es la autenticación? (p. 76)
- ¿Qué es el control de acceso? (p. 77)
- ¿Qué son las políticas? (p. 80)

# Políticas basadas en etiquetas

Al diseñar políticas de IAM, es posible establecer permisos detallados mediante la concesión de acceso a recursos específicos. A medida que crezca la cantidad de recursos que administra, esta tarea será más complicada. Etiquetado aceleradores y el uso de etiquetas en las condiciones de declaración de política pueden facilitar esta tarea. Usted concede acceso en bloque a cualquier acelerador con una determinada etiqueta. Luego aplica repetidamente esta etiqueta a los aceleradores, cuando crees el acelerador o actualizando 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 más información acerca del etiquetado en Global Accelerator, consulte Etiquetado en AWS Global Accelerator (p. 9).

Las etiquetas se pueden asociar a un recurso o transferirse en la solicitud a servicios que admiten el etiquetado de. En Global Accelerator, solo aceleradores puede 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, en función de 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 las claves de condición de etiqueta, consulte Control del acceso mediante etiquetas de IAM en el Guía del usuario de IAM.

Por ejemplo, la política de usuario administrada `GlobalAcceleratorFullAccess` de Global Accelerator proporciona a los usuarios permisos ilimitados para realizar cualquier acción de Global Accelerator en cualquier recurso. La siguiente política limita esta capacidad y deniega a los usuarios no autorizados el permiso para realizar cualquier Global Accelerator acción en cualquier producción aceleradores. El administrador de un cliente debe asociar esta política de IAM a 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"
            }
         }
      }
   ]
}
```

# Rol vinculado al servicio de Global Accelerator

AWS Global Accelerator usa un rol vinculado a un servicio de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a un servicio. Los roles vinculados a servicios están 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 utiliza lo siguiente IAM Rol vinculado a servicio:

- AWSServiceRoleForGlobalAccelerator–Global Accelerator utiliza este rol para permitir Global Accelerator para crear y administrar los recursos necesarios para la conservación de direcciones IP de clientes.

Cuando crea un acelerador por primera vez en Global Accelerator y añadir un grupo de puntos de enlace, un rol denominado AWSServiceRoleForGlobalAccelerator se crea automáticamente para permitir Global Accelerator cree y administre los recursos necesarios para la conservación de direcciones IP de 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
```

Un rol vinculado a un servicio hace que la configuración y el uso de Global Accelerator más fácil, ya que no tiene que añadir manualmente los permisos necesarios. Global Accelerator define los permisos de su rol vinculado al servicio y solo Global Accelerator puede asumir los roles de. 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 cualquier Global Accelerator para poder eliminar un rol vinculado a un servicio. Esto ayuda a proteger su Global Accelerator Los recursos de asegurándose 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 de Global Accelerator

Global Accelerator utiliza un rol vinculado a un servicio denominado AWSServiceRoleForGlobalAccelerator. En las siguientes secciones se describen los permisos para el rol.

## Permisos de roles vinculados a servicios

This service-linked role allows Global Accelerator to manage EC2 Elastic Network Interfaces and security groups.

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

- `globalaccelerator.amazonaws.com`

La política de permisos de rol permite que Global Accelerator realice las siguientes acciones en los recursos especificados:

- Acción: `ec2:CreateNetworkInterface` en `arn:aws:lambda:*:*:function:*`
- Acción: `ec2:DescribeNetworkInterfaces` en `arn:aws:lambda:*:*:function:*`
- Acción: `ec2:ModifyNetworkInterfaceAttribute` en `arn:aws:lambda:*:*:function:*`
- Acción: `ec2:DeleteNetworkInterface` en `arn:aws:lambda:*:*:function:*`
- Acción: `ec2:DeleteSecurityGroup` en `arn:aws:lambda:*:*:function:*` cuando `ec2:ResourceTag/AWSServiceName` es `GlobalAccelerator`
- Acción: `ec2:CreateSecurityGroup` en `arn:aws:lambda:*:*:function:*`
- Acción: `ec2:DescribeSecurityGroups` en `arn:aws:lambda:*:*:function:*`
- Acción: `elasticloadbalancing:DescribeLoadBalancers` en `arn:aws:lambda:*:*:function:*`
- Acción: `ec2:CreateTags` en `arn:aws:ec2:*:*:security-group/*`
- Acción: `ec2:CreateTags` en `arn:aws:ec2:*:*:network-interface/*`

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

# Creación del rol vinculado al servicio para Global Accelerator

No crea manualmente el rol vinculado al servicio para Global Accelerator. El servicio crea el rol automáticamente la primera vez que crea un acelerador de. Si eliminas tu Global Accelerator y elimine el rol vinculado al servicio, el servicio volverá a crear el rol automáticamente cuando cree un nuevo acelerador de.

## Edición de la Global Accelerator rol vinculado a servicio

Global Accelerator no le permite editar el rol vinculado a 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 Edición de un rol vinculado a un servicio en la Guía del usuario de IAM.

## Eliminación de la Global Accelerator rol vinculado a servicio

Si ya no necesita utilizar Global Accelerator, 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 el Global Accelerator de su cuenta de antes de poder eliminar manualmente los roles de.

Después de deshabilitar y eliminar los aceleradores, puede eliminar el rol vinculado al servicio. Para obtener más información acerca de cómo eliminar aceleradores, consulte Creación o actualización de un acelerador de (p. 17).

> **Note**
>
> Si ha deshabilitado y eliminado sus aceleradores pero Global Accelerator no ha terminado de actualizarse, la eliminación de roles vinculados a servicios podría producir un error. Si esto sucede, espere unos minutos y, a continuación, pruebe de nuevo los pasos de eliminación de roles vinculados al servicio.

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 (Funciones). A continuación, seleccione la casilla junto al nombre del rol que desea eliminar, no el nombre ni la fila.
3. Para Role actions en la parte superior de la página, elija Delete role.
4. En el cuadro de diálogo de confirmación, revise los datos del último acceso al servicio, que muestra cuándo cada una de las funciones seleccionadas 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 monitorizar el progreso de la eliminación de la función vinculada al servicio. Como el proceso de eliminación del rol vinculado a un servicio de IAM es asíncrono, dicha tarea puede realizarse correctamente o fallar después de enviar la solicitud de eliminación. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

## Regiones admitidas en los roles vinculados a un servicio de Global Accelerator

Global Accelerator admite el uso de roles vinculados a servicios en AWS Regiones en las que Global Accelerator es compatible con.

Para obtener una lista de las AWS Regiones en las que Global Accelerator y otros servicios son compatibles actualmente, consulte la sección AWS Tabla de regiones.

# Descripción general del acceso y la autenticación

Si es la primera vez que IAM, lea los siguientes temas para comenzar a utilizar la autorización y el acceso en AWS.

Temas



# ¿Qué es la autenticación?

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

> Note
>
> Para comenzar rápidamente, puede ignorar esta sección. En primer lugar, revise la información de introducción a Administración de identidades y accesos para AWS Global Accelerator (p. 65) y, a continuación, consulte Introducción a IAM (p. 83).

Como entidad principal, debe estar autenticado (haber iniciado sesión 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 Consola de administración de AWS como usuario, debe iniciar sesión con su nombre de usuario y contraseña. Para autenticarse desde la AWS CLI o bien AWS La API de , debe proporcionar su clave de acceso y clave secreta o credenciales temporales. AWS proporciona herramientas de SDK y CLI para firmar criptográficamente su solicitud con sus credenciales de. 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 mediante las siguientes entidades (usuarios o roles):

Usuario de la cuenta raíz de AWS

Cuando se crea por primera vez una cuenta de AWS, se comienza con una única identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de AWS de la cuenta de usuario raíz y se obtiene acceso a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Le recomendamos que no utilice 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 exclusivamente usuario raíz para crear el primer usuario de IAM. A continuación, guarde las credenciales de usuario raíz en un lugar seguro y utilícelas únicamente para algunas tareas de administración de cuentas y servicios.

IAM usuario

Un IAM usuario es una entidad dentro de su AWS cuenta de que tiene permisos específicos. Global Accelerator admite Versión de la firma 4, un protocolo para autenticar solicitudes de API entrantes. Para obtener más información acerca de la autenticación de solicitudes, consulte Proceso de firma Signature Version 4 en la AWS General Reference.

IAM rol

Un rol de IAM es una identidad de IAM con permisos específicos que puede crear en su cuenta. Un rol de IAM es similar a un usuario de IAM, ya que se trata de una identidad de AWS con políticas de permisos que determinan lo que la identidad puede hacer o 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. IAM Los roles de 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, del directorio de usuarios de la empresa o de un proveedor de identidades web. A estas identidades se les llama usuarios federados. AWS asigna una función 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 federados y roles en la Guía del usuario de IAM.

Permisos de usuario temporales

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

Acceso entre cuentas.

Puedes utilizar un IAM para permitir que una entidad principal de confianza de una cuenta diferente obtenga acceso a los recursos de su cuenta de. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos servicios de AWS, se puede asociar una política directamente a un recurso (en lugar de utilizar un rol como proxy). Global Accelerator es compatible con (no admite) las políticas basadas en recursos. 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 pPrincipals en una cuenta diferente (p. 79).

AWS acceso al servicio

Un rol de servicio es un rol de IAM que adopta un servicio 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 AWS CLI o la API 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 (están autenticados) en AWS, tu acceso a AWS Los recursos de y las operaciones de se rigen por las políticas de. 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 de introducción a Administración de identidades y accesos para AWS Global Accelerator (p. 65) y, a continuación, consulte Introducción a IAM (p. 83).

Durante la autorización, AWS utiliza valores de la contexto de la solicitud para comprobar las políticas que se aplican a. 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? (p. 80).

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 entonces permisos a un grupo, todos los usuarios de ese grupo obtienen esos permisos.

Aunque disponga de credenciales válidas para autenticar sus 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 acelerador de AWS Global Accelerator.

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

- Entidades principales (p. 78) – Controlar lo que la persona o aplicación que realiza la solicitud (el principal) puede hacer.
- IAM identidades (p. 78) – ¿Qué control IAM Se puede obtener acceso a las identidades de (grupos, usuarios y roles) y cómo.
- IAM políticas (p. 79) – Controle quién puede crear, editar y eliminar políticas administradas por el cliente y quién puede asociar y desasociar todas las políticas administradas por.
- AWS recursos (p. 79) – Controle quién tiene acceso a los recursos de mediante una política basada en identidad o una política basada en recursos.
- AWS cuentas (p. 79) – Controle si una solicitud está permitida solo para miembros de una cuenta específica.

## Control del acceso para entidades principales

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 esta entidad puede tener. Los límites de permisos son una característica avanzada de IAM. Para obtener más información acerca de los límites de permisos, consulte Límites de permisos para IAM identidades en el Guía del usuario de IAM.

Para obtener más información y un ejemplo de cómo controlar AWS para los principales, consulte Control del acceso para entidades principales en el Guía del usuario de IAM.

## Control del acceso a las identidades de

Los administradores controlan lo que puede hacer en un IAM (usuario, grupo o rol) mediante la creación de una política que limita lo que se puede hacer con una identidad o quién puede obtener acceso a ella. A continuación, asocian esa política a la identidad que proporciona 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 permita restablecer la contraseña únicamente de sí mismo y de los usuarios cuyos ARN coincidan con los 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 un ejemplo de uso de una política para controlar AWS acceso a identidades, consulte Control del acceso a las identidades de en el Guía del usuario de IAM.

## Control del acceso a las políticas de

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 política que incluye un resumen del nivel de acceso de cada servicio dentro de esa política. AWS clasifica cada acción de servicio en una de cuatro niveles de acceso en función de lo que hace cada acción: `List`de `Read`de `Write`, o bien `Permissions management`. Puede utilizar estos niveles de acceso para determinar qué acciones incluir en sus políticas de. Para obtener más información, consulte Comprensión de los resúmenes de nivel de acceso dentro de los resúmenes de políticas en el Guía del usuario de IAM.

> Warning
>
> Debe limitar los permisos de nivel de acceso de `Permissions Management` de 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 los usuarios independientes con acceso completo a AWS.

Para obtener más información y un ejemplo sobre cómo controlar AWS acceso a las políticas, consulte Control del acceso a las políticas de en el Guía 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, consulte Control del acceso a los recursos en la Guía 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 de la cuenta raíz 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 que no utilice el usuario raíz en sus tareas cotidianas, ni siquiera en las tareas administrativas. En su lugar, sigue las instrucciones de la mejor práctica de uso de la usuario raíz solo para crear su primera IAM usuario. A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilícelas únicamente para algunas tareas de administración de cuentas y servicios. Para ver las tareas que requieren que inicie sesión como usuario usuario raíz, consulte Tareas de AWS que requieren Usuario raíz de la cuenta de AWS.

Entidades (usuarios o roles) en la AWS La cuenta de debe tener acceso para crear un recurso. Pero solo porque creen un recurso no significa que tengan acceso completo automáticamente a ese recurso. Los administradores deben conceder permisos explícitamente para cada acción. Además, los administradores pueden revocar esos permisos en cualquier momento, siempre que tengan acceso para administrar los permisos de usuario y rol.

## Control del acceso a pPrincipals en una cuenta diferente

Los administradores pueden utilizar las políticas basadas en recursos de AWS, roles de IAM 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 AWS Los administradores de pueden conceder acceso entre cuentas a los recursos de. Para ello, un administrador asocia una política directamente al recurso que desea compartir, en lugar de utilizar un rol como proxy. Si el servicio admite este tipo de política, el recurso que el administrador comparte

también debe admitir 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 es compatible con (no admite) las políticas basadas en recursos.

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, consulte Proporcionar acceso a un usuario de IAM a otra cuenta de AWS de la que es propietario en la Guía del usuario de IAM.

AWS Organizations le ofrece administración basada en políticas para varias cuentas de AWS de su propiedad. Con Organizaciones, puede crear grupos de cuentas, automatizar la creación de cuentas y aplicar y administrar las políticas de esos grupos. Organizaciones permite administrar las políticas de forma centralizada para varias cuentas, 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 es AWS Organizations? en la Guía del usuario de AWS Organizations.

## ¿Qué son las políticas?

Para controlar el acceso en AWS, se crean políticas y se asocian 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 de introducción a Administración de identidades y accesos para AWS Global Accelerator (p. 65) y, a continuación, consulte Introducción a IAM (p. 83).

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. Las 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 la acción GetUser, un usuario con dicha política puede obtener información de los usuarios desde la Consola de administración de AWS, la AWS 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 políticas en la Guía del usuario de IAM.

Políticas basadas en identidad

Puede asociar políticas administradas y en línea a IAM Las identidades de (usuarios, grupos a los que pertenecen los usuarios y roles de ).

Políticas basadas en recursos

Puede asociar políticas insertadas a los recursos de algunos AWS servicios de. 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 es compatible con (no admite) las políticas basadas en recursos.

SCP de organizaciones

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

Listas de control de acceso (ACL)

Puede utilizar las ACL para controlar qué entidades principales pueden obtener 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 documentos de política JSON. Global Accelerator admite o no admite Las 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 en AWS para definir los permisos para 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

Cuando asocia una política administrada o insertada a un IAM user, group, or role, the policy defines the permissions for that entity.

Políticas basadas en recursos

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

Listas de control de acceso (ACL)

Cuando asocia una ACL a un recurso, 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 utilizar políticas de para definir el límite de permisos de una entidad de (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

Puedes utilizar un AWS Organizations La política de control de servicios de (SCP) para aplicar un límite de permisos a un AWS Organizations de organización o unidad organizativa (OU).

IAM usuarios o funciones

Puede utilizar una política administrada para el límite de permisos de un usuario o rol. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

Temas



## 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?

Para conceder a un usuario permisos para crear un AWS Global Accelerator del recurso, como, por ejemplo, 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, a la cuenta B) o a un servicio de AWS, tal y como se indica a continuación:

1. 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 obtener 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, consulte Administración de accesos en la Guía del usuario de IAM.

Para obtener más información acerca de los usuarios, grupos, funciones y permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

A continuación se muestran dos ejemplos de políticas de que podría utilizar con Global Accelerator La primera política de ejemplo concede a un usuario acceso mediante programación a todas las acciones List y Describe para aceleradores de en su cuenta de AWS:

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

El siguiente ejemplo concede acceso mediante programación a la `ListAccelerators` operación:

```
{
    "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 Amazon S3 del bucket de. 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 de política

En la consola de IAM, las acciones se agrupan utilizando las siguientes clasificaciones de nivel de acceso:

List

Proporciona permiso para enumerar recursos dentro del servicio de para 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 para editar, el contenido y los atributos de los recursos del servicio. Por ejemplo, el campo Amazon S3 operaciones `GetObject` y `GetBucketLocation` tienen el [EMPTY] del nivel de acceso.

Escritura

Proporciona permiso para crear, eliminar o modificar recursos en el servicio. Por ejemplo, el campo Amazon S3 operaciones `CreateBucket`de `DeleteBucket`, y `PutObject` tienen el Escribir del nivel de acceso.

Administración de permisos

Concede permiso para conceder o modificar permisos de recursos en el servicio. Por ejemplo, la mayoría de las acciones de las políticas de IAM y AWS Organizations tienen el nivel de acceso Permissions management (Administración de permisos).

> **Tip**
>
> Para mejorar la seguridad de su cuenta de AWS, limite o monitorice periódicamente las políticas que incluyen la clasificación de nivel de acceso Permissions management (Administración de permisos).

Etiquetado

Proporciona permiso para crear, eliminar o modificar etiquetas que se asocian a un recurso en el servicio. Por ejemplo, el campo Amazon EC2 `CreateTags` y `DeleteTags` las operaciones tienen el Etiquetado del nivel de acceso.

## Introducción a IAM

AWS Identity and Access Management (IAM) es un servicio de AWS que permite administrar el acceso a los servicios y recursos de forma segura. IAM es una característica de la cuenta de AWS que se ofrece sin cargo adicional.

Note

Antes de comenzar a usar IAM, revise la información introductoria de Administración de identidades y accesos para AWS Global Accelerator (p. 65).

Cuando se crea por primera vez una cuenta de AWS, se comienza con una única identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de AWS de la cuenta de usuario raíz y se obtiene acceso a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Le recomendamos que no utilice 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 exclusivamente usuario raíz para crear el primer usuario de IAM. A continuación, guarde las credenciales de usuario raíz en un lugar seguro y utilícelas únicamente para algunas tareas de administración de cuentas y servicios.

## Cree su IAM usuario administrador

Para crearse usted mismo un usuario administrador y agregarlo a un grupo de administradores (consola)

1. Inicie sesión en la consola de IAM como el propietario de la cuenta; para ello, elija usuario raíz y escriba su dirección de correo electrónico de la cuenta de AWS. En la siguiente página, escriba su contraseña.

   Note

   Recomendamos que siga la práctica recomendada de utilizar el usuario de IAM de **`Administrator`** como se indica a continuación, y guardar de forma segura las credenciales del 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. Marque la casilla situada junto a Consola de administración de AWS 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 al nuevo usuario que 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. Elija Next: Permissions.
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. Elija Filter policies (Filtrar políticas) y, a continuación, seleccione AWS managed - job function (Función de trabajo administrada por AWS) para 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 usuarios y roles de IAM a Facturación para poder utilizar la los permisos `AdministratorAccess` para el acceso 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. Elija Next: Tags (Siguiente: 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. Elija Next: Review para ver la lista de suscripciones a grupos que se van a añadir 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 a los recursos de la 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 AWS , debe delegar el permiso para permitir que otras personas realicen únicamente las acciones que desea permitir. Para ello, cree un grupo de IAMcon los permisos que esas personas necesitan y, a continuación, añada usuarios de IAM a los grupos necesarios al crearlos. Puede usar 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 de gran tamaño, puede utilizar roles de IAM personalizados, federación o inicio de sesión único.

En el siguiente procedimiento, creará tres usuarios denominados **`arnav`**de **`carlos`**, y **`martha`** y asociar una política que concede permiso para crear un acelerador denominado **`my-example-accelerator`**, pero solo en 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. Seleccione la casilla de verificación junto a Consola de administración de AWS accesoy, a continuación, selecciona Contraseña 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. Seleccione Next (Siguiente). Permissions (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.

    Se cerrará la sección Service (Servicio) y se abrirá automáticamente la sección Actions (Acciones).

11. Elija las acciones de Global Accelerator que desea permitir. Por ejemplo, para concede permiso para crear un acelerador, introduzca **`globalaccelerator:CreateAccelerator`** en el Acciones de filtro del cuadro de texto. Cuando la lista de Global Accelerator se filtran, seleccione la casilla de verificación junto a **`globalaccelerator:CreateAccelerator`**.

    Las acciones de Global Accelerator 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 de política (p. 83).

12. Si las acciones que ha seleccionado en los pasos anteriores no admiten la elección de recursos específicos, Todos los recursos está 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). Elegir Ha elegido acciones que requieren el acelerador tipo de recurso para elegir si desea introducir un valor acelerador para su 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 el región e ID de cuenta (o ID de cuenta) (o elija Any (Cualquiera)) y, a continuación, introduzca **`my-example-accelerator`** para el recurso. A continuación, elija Add (Añadir).

14. Elija Specify request conditions (optional) (Especificar condiciones de solicitud (opcional)).
15. Elegir Añadir condición de concede permiso para crear un acelerador en los próximos 7 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. Para Calificador, 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 la opción Código JSON. Puede alternar entre las pestañas Visual editor (Editor visual) y JSON en cualquier momento. Sin embargo, si realiza cambios o elige Review policy (Revisar política) en la pestaña Visual editor (Editor visual), IAM podría reestructurar la política para optimizarla para el editor visual. Para obtener más información, consulte Reestructuración de políticas en la Guía del usuario de IAM.
23. Cuando haya terminado, seleccione Review policy.
24. En la Revisar política página, para Nombre, introduzca **`globalaccelerator:CreateAcceleratorPolicy`**. Para Descripción, introduzca **`Policy to concede permiso para crear un acelerador`**. Revise el resumen de política para asegurarse de que ha concedido los permisos previstos y, a continuación, elija 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, introduzca **`globalaccelerator:CreateAcceleratorPolicy`**. Seleccione la casilla de verificación situada junto a la nueva política. A continuación, elija Next Step.

27. Seleccione Next (Siguiente). Revisión para obtener una vista previa de los 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 un enlace a su IAM página de la consola del usuario de y los nombres de usuario que acaba de crear.

## Permitir a los usuarios autoadministrar 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 declaración `BlockMostAccessUnlessSignedInWithMFA`. Sin embargo, IAM no recomienda este.

```
{
    "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?

- La instrucción `AllowAllUsersToListAccounts` permite 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" : "*"`.
- La instrucción `AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation` 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.
- La instrucción `BlockMostAccessUnlessSignedInWithMFA` utiliza una combinación de `"Deny"` y `"NotAction"` para denegar el acceso a todas excepto algunas acciones en IAM y otros servicios de AWS si el usuario no ha iniciado sesión con MFA. Para obtener más información acerca de la lógica de esta instrucción, consulte NotAction con Deny en la Guía 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. Para 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.`** Revisar la política [EMPTY] para ver los permisos concedidos por su política y, a continuación, elija Crear política para 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 (Usuarios).
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 IAM usuario

Para más seguridad, le recomendamos que se configure la Multi-Factor Authentication (MFA) de todos los usuarios de IAM, con el fin de 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 MFA admitido por AWS, además de sus credenciales de inicio de sesión habituales. El dispositivo MFA más seguro para AWS 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, consulte Habilitación de una llave de seguridad U2F en la Guía 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 en el que se alojará el dispositivo MFA virtual del usuario con el fin de poder configurar la MFA para un usuario de IAM.

### Para habilitar un dispositivo 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 (Usuarios).
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 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, consulte Resincronización de dispositivos MFA físicos y virtuales en la Guía del usuario de IAM.

Ahora el dispositivo MFA virtual ya está listo para usarlo con AWS.

# Proteger las conexiones de VPC en AWS Global Accelerator

Cuando se añade un Balanceador de carga de aplicaciones o un Amazon EC2 Punto de enlace de instancia de en AWS Global Accelerator, habilita el tráfico de Internet para que fluya directamente hacia y desde el punto de enlace en las nubes virtuales privadas (VPC) dirigiéndolo a una subred privada. La VPC que contiene el balanceador de carga o la instancia EC2 debe tener una puerta de enlace de Internet asociado a ella, para indicar que la VPC acepta tráfico de Internet. Sin embargo, no necesita direcciones IP públicas en el balanceador de carga ni en la instancia EC2. Tampoco necesita una ruta de gateway de Internet asociada para la subred.

Esto es diferente del caso de uso típico de la gateway de Internet en el que se requieren tanto direcciones IP públicas como rutas de gateway de Internet para que el tráfico de Internet fluya a instancias o balanceadores de carga en una VPC. Aunque las interfaces de red elásticas de sus destinos estén presentes en una subred pública (es decir, una subred con una ruta de gateway de Internet), cuando utilice Global Accelerator para el tráfico de Internet, Global Accelerator anula la ruta de Internet típica y todas las conexiones lógicas que llegan a través del Global Accelerator también vuelven a través de Global Accelerator en lugar de a través de la gateway de Internet.

Note

Uso de direcciones IP públicas y uso de una subred pública para su Amazon EC2 Las instancias de no son típicas, aunque es posible establecer la configuración con ellas. Los grupos de seguridad se aplican a cualquier tráfico que llegue a las instancias, incluido el tráfico de Global Accelerator y cualquier dirección IP pública o elástica que se asigne a la ENI de la instancia. Utilizar subredes privadas para garantizar que el tráfico se entregue solo por Global Accelerator.

Tenga en cuenta esta informaciÃ3n al considerar problemas de perímetro de red y configurar IAM privilegios relacionados con la administración de acceso a Internet. Para obtener más información acerca del control del acceso a Internet a su VPC, consulte este ejemplo de política de control de servicios.

# Registro y monitoreo 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 pueda más fácilmente depurar un error multipunto si se produce. AWS proporciona varias herramientas para monitorizar sus recursos de Global Accelerator y responder a posibles incidentes:

Registros de flujo de AWS Global Accelerator

Los registros de flujo del servidor proporcionan registros detallados sobre el tráfico que fluye a través de un acelerador a un punto de enlace. Los registros de flujo del servidor son útiles para muchas aplicaciones. Por ejemplo, la información del log de flujo puede ser útil en las auditorías de seguridad y acceso. Para obtener más información, consulte Registros de flujo en AWS Global Accelerator (p. 47).

Métricas y alarmas de Amazon CloudWatch

Uso de CloudWatchpuedes supervisar, en tiempo real, tu AWS y las aplicaciones que ejecuta en AWS. CloudWatch recopila y realiza un seguimiento de las métricas de , que son variables que se miden a lo largo del tiempo. Puede crear alarmas de que vigilen métricas específicas y, a continuación, enviar notificaciones o realizar cambios automáticamente en los recursos que monitorice cuando la métrica supere un determinado umbral durante un periodo de tiempo. Para obtener más información, consulte Uso de Amazon CloudWatch con AWS Global Accelerator (p. 53).

Registros de AWS CloudTrail

CloudTrail proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Global Accelerator. CloudTrail captura todas las llamadas a la API para Global Accelerator como eventos, incluidas las llamadas desde el Global Accelerator y desde las llamadas de código a la consola de Global Accelerator de la API de. Para obtener más información, consulte Uso de AWS CloudTrail para registrar AWS Global Accelerator Llamadas a la API de (p. 58).

# Validación de conformidad para AWS Global Accelerator

Hay auditores externos que evalúan la seguridad y la conformidad de AWS Global Accelerator en distintos programas de conformidad de AWS. Estos incluyen SOC, PCI, HIPAA, GDPR, ISO y ENS High.

Para obtener una lista de AWS servicios, incluidos Global Accelerator, dentro del alcance de programas de cumplimiento específicos, consulte Servicios de AWS en el ámbito del programa de conformidad. 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, consulte Descarga de informes en AWS Artifact.

Su responsabilidad en el ámbito de la conformidad al usar Global Accelerator viene determinada por la confidencialidad de los datos, los objetivos de conformidad de su empresa y las leyes y regulaciones aplicables. AWS proporciona los siguientes recursos para ayudarlo con los requisitos de 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: en este documento técnico, se 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 AWS Config evalúa en qué medida las configuraciones de los 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

El AWS la infraestructura global se basa en AWS Regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad separadas físicamente y aisladas, que están conectadas con redes de baja latencia, alto rendimiento y altamente redundantes. 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 del apoyo de AWS la infraestructura global, Global Accelerator ofrece las siguientes características que ayudan a respaldar la resiliencia de los datos:

- La zona de red los servicios de las direcciones IP estáticas de su acelerador desde una subred IP única. Similar a un AWS de disponibilidad, una zona de red es una unidad aislada con su propio conjunto de infraestructura física. Cuando configura un aceleradorde Global Accelerator asigna dos direcciones IPv4 para ella. Si una dirección IP de una zona de red deja de estar disponible debido al bloqueo de direcciones IP por parte de determinadas redes cliente, o debido a interrupciones de red, las aplicaciones cliente pueden reintentar en la dirección IP estática en buen estado de la otra dirección aislada zona de red.
- Global Accelerator monitoriza continuamente el estado de todos los puntos de enlace. Cuando determina que un punto de enlace activo está en mal estado, Global Accelerator comienza a dirigir el tráfico al instante a otro punto de enlace disponible. Esto le permite crear una arquitectura de alta disponibilidad para sus aplicaciones en AWS.

# Seguridad de la infraestructura en AWS Global Accelerator

Como servicio administrado, AWS Global Accelerator está protegido por el AWS los procedimientos de seguridad de red global que se describen en el Amazon Web Services: : Información general acerca de los procesos de seguridad (documento técnico)

Puede utilizar llamadas a la API publicadas en AWS para tener 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), 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 AWS cuenta tiene las siguientes cuotas, también conocidas como límites, relacionadas con AWS Global Accelerator.

AWS Global Accelerator Cuotas

- Número de aceleradores para cada AWS cuenta – 20 años
- Número de oyentes para cada uno acelerador – 10 años
- Número de rangos de puertos para cada agente de escucha – 10 años
- Número de puntos de enlace para cada grupo de puntos de enlace – 10 años
- Número de etiquetas para cada acelerador – [EMPTY]

Además, hay cuotas para Network Load Balancersde Application Load Balancersde Amazon EC2 o direcciones IP elásticas que se utilizan como puntos de enlace para un acelerador. Para obtener más información, consulte lo siguiente: .

- Cuota de dirección IP elástica en el Amazon EC2 Guía del usuario.
- Cuotas de servicio de Amazon EC2 en el Amazon EC2 Guía del usuario.
- Cuotas para tu Network Load Balancers en el Guía del usuario de Network Load Balancers.
- Cuotas para tu Application Load Balancers en el Guía del usuario de Application Load Balancers.

# AWS Global Accelerator Información relacionada

La información y los recursos que se enumeran aquí pueden ayudarle a obtener más información acerca de Global Accelerator.

Temas



## Adicional AWS Global Accelerator documentación

Los recursos relacionados siguientes pueden serle de ayuda cuando trabaje con este servicio.

- Referencia de la API de AWS Global Accelerator – contiene 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 – página web principal para obtener información acerca de Global Accelerator, incluidos precios, características, etc.
- Términos de uso: información detallada sobre nuestros derechos de autor y marca comercial, y su cuenta, licencia y acceso al sitio, entre otros temas.

## Cómo obtener soporte

Compatibilidad con Global Accelerator está disponible en varios formatos.

- Foros de debate – un foro de la comunidad en el que los desarrolladores pueden debatir 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.

## Sugerencias adicionales del blog de Amazon Web Services

El blog de AWS tiene varias publicaciones para ayudarle a utilizar AWS servicios de. Por ejemplo, consulte las siguientes entradas de blog sobre Global Accelerator:

- AWS Global Accelerator para disponibilidad y rendimiento
- Administración del tráfico con AWS Global Accelerator
- Análisis y visualización de registros de flujo de AWS Global Accelerator con Amazon Athena y Amazon QuickSight

# 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: 20 de mayo de 2020

| Cambiar | Descripción | Date |
| --- | --- | --- |
| Se han añadido dos nuevas regiones | Global Accelerator ahora es compatible con 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 |
| Etiquetado y BYOIP | Esta versión añade compatibilidad para añadir etiquetas a aceleradores de y traer 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 |
| Se ha actualizado el capítulo Seguridad | Se ha añadido contenido para conformidad, resiliencia y seguridad de infraestructura. Para obtener más información, consulte https://docs.aws.amazon.com/global-accelerator/latest/dg/security.html. | 20 de diciembre de 2019 |
| Compatibilidad con instancias EC2 y nombre de DNS predeterminado | AWS Global Accelerator ahora admite la adición de instancias EC2 en compatibles AWS Regiones. Además, Global Accelerator crea un nombre de DNS predeterminado que se asigna a las direcciones IP estáticas de su acelerador. Para obtener más información, consulte https://docs.aws.amazon.com/global- | 29 de octubre de 2019 |

| Cambiar | Descripción | Date |
| --- | --- | --- |
| | 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. | |
| Conservación de la dirección IP del cliente para Application Load Balancers | Ahora puede elegir tener AWS Global Accelerator conservar la dirección IP del cliente para Application Load Balancers en compatible AWS Regiones. 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 |
| Liberación de AWS Global Accelerator servicio | El Guía para desarrolladores de AWS Global Accelerator proporciona información sobre la configuración y el uso de aceleradores de—administradores de trÃ¡fico de capa de red—que mejoran la disponibilidad y el rendimiento de sus aplicaciones de Internet con un público global. | 26 de noviembre de 2018 |

# AWS glossary

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

Si proporcionásemos una traducción de la versión en inglés de la guía, prevalecerá la versión en inglés de la guía si hubiese algún conflicto. La traducción se proporciona mediante traducción automática.