Manuel du développeur

AWS Global Accelerator

AWS Global Accelerator: Manuel du développeur

Table of Contents

Qu'est-ce qu'AWS Global Accelerator

AWS Global Accelerator est un service dans lequel vous créezAccélérateurspour améliorer les performances de vos applications pour les utilisateurs locaux et mondiaux. En fonction du type d'accélérateur que vous choisissez, vous pouvez obtenir des avantages supplémentaires.

- En utilisant un accélérateur standard, vous pouvez améliorer la disponibilité de vos applications Internet qui sont utilisées par un public mondial. Avec un accélérateur standard, Global Accelerator dirige le trafic sur le réseau global AWS vers les terminaux de la région la plus proche du client.
- À l'aide d'un accélérateur de routage personnalisé, vous pouvez mapper un ou plusieurs utilisateurs à une destination spécifique parmi de nombreuses destinations.

Global Accelerator est un service global qui prend en charge les points de terminaison dans plusieurs régions AWS répertoriées dans leTable des régions AWS.

Par défaut, Global Accelerator vous fournit deux adresses IP statiques que vous associez à votre accélérateur. Avec un accélérateur standard, au lieu d'utiliser les adresses IP fournies par Global Accelerator, vous pouvez configurer ces points d'entrée pour qu'ils soient des adresses IPv4 à partir de vos propres plages d'adresses IP que vous apportez à Global Accelerator. Les adresses IP statiques sont anycast à partir du réseau périphérique AWS.

> **Important**
>
> Les adresses IP statiques restent assignées à votre accélérateur aussi longtemps qu'il existe, même si vous désactivez l'accélérateur et qu'il n'accepte plus ni achemine le trafic. Cependant, lorsque vousdeleteun accélérateur, vous perdez les adresses IP statiques qui lui sont assignées, de sorte que vous ne pouvez plus acheminer le trafic en les utilisant. Vous pouvez utiliser des stratégies IAM telles que des autorisations basées sur des balises avec Global Accelerator pour limiter les utilisateurs disposant des autorisations pour supprimer un accélérateur. Pour plus d'informations, consultez Stratégies basées sur balises.

Pour les accélérateurs standard, Global Accelerator utilise le réseau global AWS pour acheminer le trafic vers le point de terminaison régional optimal en fonction de l'intégrité, de l'emplacement du client et des stratégies que vous configurez, ce qui augmente la disponibilité de vos applications. Les points de terminaison pour les accélérateurs standard peuvent être des équilibreurs de charge réseau, des équilibreurs de charge d'application, des instances Amazon EC2 ou des adresses

IP élastiques situées dans une ou plusieurs régions AWS. Le service réagit instantanément aux changements d'intégrité ou de configuration pour s'assurer que le trafic Internet des clients est toujours dirigé vers des points de terminaison sains.

Les accélérateurs de routage personnalisés prennent en charge uniquement les types de points de terminaison de sous-réseau VPC (Virtual Private Cloud) et acheminent le trafic vers les adresses IP privées de ce sous-réseau.

Pour obtenir la liste des régions AWS où Global Accelerator et d'autres services sont actuellement pris en charge, consultezTable des régions AWS.

Rubriques

Composants AWS Global Accelerator

AWS Global Accelerator comprend les composants suivants :

Adresses IP statiques

Global Accelerator vous fournit un ensemble de deux adresses IP statiques qui sont anycast à partir du réseau périphérique AWS. Si vous apportez votre propre plage d'adresses IP à AWS (BYOIP) à utiliser avec Global Accelerator, vous pouvez attribuer les adresses IP de votre propre pool à utiliser avec votre accélérateur. Pour plus d'informations, consultez Fourniture de vos propres adresses IP (BYOIP) dans AWS Global Accelerator.

Les adresses IP servent de points d'entrée fixes uniques pour vos clients. Si vous disposez déjà d'équilibreurs de charge Elastic Load Balancing, d'instances Amazon EC2 ou de ressources

d'adresse IP Elastic configurées pour vos applications, vous pouvez facilement les ajouter à un accélérateur standard dans Global Accelerator. Cela permet à Global Accelerator d'utiliser des adresses IP statiques pour accéder aux ressources.

Les adresses IP statiques restent assignées à votre accélérateur aussi longtemps qu'il existe, même si vous désactivez l'accélérateur et qu'il n'accepte plus ni achemine le trafic. Cependant, lorsque vousdeleteun accélérateur, vous perdez les adresses IP statiques qui lui sont assignées, de sorte que vous ne pouvez plus acheminer le trafic en les utilisant. Vous pouvez utiliser des stratégies IAM telles que des autorisations basées sur des balises avec Global Accelerator pour limiter les utilisateurs disposant des autorisations pour supprimer un accélérateur. Pour plus d'informations, consultez Stratégies basées sur balises.

Accélérateur

Un accélérateur dirige le trafic vers les terminaux via le réseau mondial AWS afin d'améliorer les performances de vos applications Internet. Chaque accélérateur comprend un ou plusieurs auditeurs.

Il existe deux types d'accélérateurs :

- AStandarddirige le trafic vers le point de terminaison AWS optimal en fonction de plusieurs facteurs, notamment l'emplacement de l'utilisateur, l'intégrité du point de terminaison et les pondérations du point de terminaison que vous configurez. Cela permet d'améliorer la disponibilité et les performances de vos applications. Les points de terminaison peuvent être des équilibreurs de charge réseau, des équilibreurs de charge d'application, des instances Amazon EC2 ou des adresses IP élastiques.
- ARoutes personnaliséesvous permet d'acheminer de manière déterministe plusieurs utilisateurs vers une destination EC2 spécifique derrière votre accélérateur, comme cela est nécessaire pour certains cas d'utilisation. Pour ce faire, dirigez les utilisateurs vers une adresse IP et un port uniques de votre accélérateur, que Global Accelerator a mappé à la destination.

Pour plus d'informations, consultez Types d'accélérateurs.

Nom du DNS

Global Accelerator attribue à chaque accélérateur un nom DNS (Domain Name System, système de noms de domaine) par défaut, semblable à`a1234567890abcdef.awsglobalaccelerator.com`, qui pointe vers les adresses IP statiques que Global Accelerator vous attribue ou que vous choisissez dans votre propre plage d'adresses IP. Selon le cas d'utilisation, vous pouvez utiliser les adresses IP statiques ou le

nom DNS de votre accélérateur pour acheminer le trafic vers votre accélérateur, ou configurer des enregistrements DNS pour acheminer le trafic à l'aide de votre propre nom de domaine personnalisé.

Zone réseau

Une zone réseau dessert les adresses IP statiques de votre accélérateur à partir d'un sous-réseau IP unique. À l'instar d'une zone de disponibilité AWS, une zone réseau est une unité isolée dotée de son propre ensemble d'infrastructure physique. Lorsque vous configurez un accélérateur, Global Accelerator lui alloue par défaut deux adresses IPv4. Si une adresse IP d'une zone réseau devient indisponible en raison d'un blocage d'adresse IP par certains réseaux clients ou d'une interruption du réseau, les applications clientes peuvent réessayer sur l'adresse IP statique saine de l'autre zone réseau isolée.

Listener

Un écouteur traite les connexions entrantes des clients vers Global Accelerator, en fonction du port (ou de la plage de ports) et du protocole (ou des protocoles) que vous configurez. Un écouteur peut être configuré pour les protocoles TCP, UDP ou TCP et UDP. Chaque écouteur a un ou plusieurs groupes de points de terminaison qui lui sont associés, et le trafic est transféré vers les points de terminaison de l'un des groupes. Vous associez des groupes de points de terminaison à des écouteurs en spécifiant les régions vers lesquelles vous souhaitez distribuer le trafic. Avec un accélérateur standard, le trafic est distribué vers des points de terminaison optimaux au sein des groupes de points de terminaison associés à un écouteur.

Groupe de points de terminaison

Chaque groupe de points de terminaison est associé à une région AWS spécifique. Les groupes de points de terminaison incluent un ou plusieurs points de terminaison dans la région. Avec un accélérateur standard, vous pouvez augmenter ou réduire le pourcentage de trafic qui serait autrement dirigé vers un groupe de points de terminaison en ajustant un paramètre appeléNuméro de trafic. La molette de trafic vous permet d'effectuer facilement des tests de performances ou des tests de déploiement bleu/vert, par exemple, pour les nouvelles versions dans différentes régions AWS.

Point de terminaison

Un point de terminaison est la ressource vers laquelle Global Accelerator dirige le trafic.

Les points de terminaison pour les accélérateurs standard peuvent être des équilibreurs de charge réseau, des équilibreurs de charge d'application, des instances EC2 ou des adresses IP élastiques. Un point de terminaison d'équilibreur de charge d'application peut être connecté

à Internet ou interne. Le trafic des accélérateurs standard est acheminé vers des points de terminaison en fonction de l'intégrité du point de terminaison ainsi que des options de configuration que vous choisissez, telles que les pondérations des points de terminaison. Pour chaque point de terminaison, vous pouvez configurer des pondérations, qui sont des nombres que vous pouvez utiliser pour spécifier la proportion de trafic à acheminer vers chacun d'eux. Cela peut être utile, par exemple, pour effectuer des tests de performance dans une région.

Les points de terminaison des accélérateurs de routage personnalisés sont des sous-réseaux VPC (Virtual Private Cloud) avec une ou plusieurs instances Amazon EC2 qui sont les destinations du trafic.

Fonctionnement AWS Global Accelerator

Les adresses IP statiques fournies par AWS Global Accelerator servent de points d'entrée fixes uniques pour vos clients. Lorsque vous configurez votre accélérateur avec Global Accelerator, vous associez les adresses IP statiques à des points de terminaison régionaux dans une ou plusieurs régions AWS. Pour les accélérateurs standard, les points de terminaison sont les équilibreurs de charge réseau, les équilibreurs de charge d'application, les instances Amazon EC2 ou les adresses IP Elastic. Pour les accélérateurs de routage personnalisés, les points de terminaison sont des sous-réseaux de cloud privé virtuel (VPC) avec une ou plusieurs instances EC2. Les adresses IP statiques acceptent le trafic entrant sur le réseau global AWS à partir de l'emplacement périphérique le plus proche de vos utilisateurs.

> **Note**
>
> Si vous apportez votre propre plage d'adresses IP à AWS (BYOIP) à utiliser avec Global Accelerator, vous pouvez à la place attribuer les adresses IP statiques de votre propre pool à utiliser avec votre accélérateur. Pour plus d'informations, consultez Fourniture de vos propres adresses IP (BYOIP) dans AWS Global Accelerator.

À partir de l'emplacement périphérique, le trafic de votre application est acheminé en fonction du type d'accélérateur que vous configurez.

- Pour les accélérateurs standard, le trafic est acheminé vers le point de terminaison AWS optimal en fonction de plusieurs facteurs, notamment l'emplacement de l'utilisateur, l'intégrité du point de terminaison et les pondérations de point de terminaison que vous configurez.

- Pour les accélérateurs de routage personnalisés, chaque client est routé vers une instance et un port Amazon EC2 spécifiques dans un sous-réseau VPC, en fonction de l'adresse IP statique externe et du port d'écoute que vous fournissez.

Le trafic circule sur le réseau global AWS redondant et sans congestionnance jusqu'au point de terminaison. En maximisant la durée du trafic sur le réseau AWS, Global Accelerator garantit que le trafic est toujours acheminé sur le chemin réseau optimal.

Avec certains types de point de terminaison (dans certaines régions AWS), vous avez la possibilité de conserver et d'accéder à l'adresse IP du client. Deux types de points de terminaison peuvent conserver l'adresse IP source du client dans les paquets entrants : Équilibreurs de charge des applications et instances Amazon EC2. Global Accelerator ne prend pas en charge la préservation des adresses IP des clients pour les points de terminaison de l'Network Load Balancer et des adresses IP Elastic Les points de terminaison des accélérateurs de routage personnalisés ont toujours l'adresse IP du client conservée.

Global Accelerator met fin aux connexions TCP à partir de clients sur les emplacements périphériques AWS et établit, presque simultanément, une nouvelle connexion TCP avec vos terminaux. Cela donne aux clients des temps de réponse plus rapides (latence réduite) et un débit accru.

Dans les accélérateurs standard, Global Accelerator surveille en permanence l'état de tous les points de terminaison et commence instantanément à diriger le trafic vers un autre point de terminaison disponible lorsqu'il détermine qu'un point de terminaison actif est défectueux. Cela vous permet de créer une architecture haute disponibilité pour vos applications sur AWS. Les contrôles d'Health ne sont pas utilisés avec les accélérateurs de routage personnalisés et il n'y a pas de basculement, car vous spécifiez la destination vers laquelle acheminer le trafic.

Lorsque vous ajoutez un accélérateur, les groupes de sécurité et les règles AWS WAF que vous avez déjà configurés continuent de fonctionner comme avant l'ajout de l'accélérateur.

Si vous souhaitez un contrôle précis de votre trafic global, vous pouvez configurer des pondérations pour vos terminaux dans un accélérateur standard. Vous pouvez également augmenter ou réduire le pourcentage de trafic vers un groupe de points de terminaison particulier, par exemple, pour les tests de performances ou les mises à niveau de pile.

Soyez conscient des points suivants lorsque vous utilisez Global Accelator

- AWS Direct Connect ne publie pas de préfixes d'adresse IP pour AWS Global Accelerator sur une interface virtuelle publique. Nous vous recommandons de ne pas annoncer les adresses IP que vous utilisez pour communiquer avec Global Accelerator via votre interface virtuelle publique AWS Direct Connect. Si vous annoncez des adresses IP que vous utilisez pour communiquer avec Global Accelerator via votre interface virtuelle publique AWS Direct Connect, cela entraînera un flux de trafic asymétrique : votre trafic vers Global Accelerator passe à Global Accelerator via Internet, mais renvoie le trafic vers votre site vient via votre interface virtuelle publique AWS Direct Connect.
- Global Accelerator ne prend pas en charge l'ajout en tant que point de terminaison d'une ressource appartenant à un autre compte AWS.

Rubriques

Délai d'inactivité dans AWS Global Accelerator

AWS Global Accelerator définit un délai d'inactivité qui s'applique à ses connexions. Si aucune donnée n'a été envoyée ou reçue avant que la période d'inactivité soit écoulée, Global Accelerator ferme la connexion. Pour garantir que la connexion reste active, le client ou le point de terminaison doit envoyer au moins 1 octet de données avant l'expiration du délai d'inactivité.

Le délai d'inactivité Global Accelerator pour une connexion réseau dépend du type de connexion :

- Le délai d'expiration est de 340 secondes pour les connexions TCP.
- Le délai d'attente est de 30 secondes pour les connexions UDP.

Global Accelerator continue à diriger le trafic vers un point de terminaison jusqu'à ce que le délai d'inactivité soit atteint, même si le point de terminaison est marqué comme défectueux. Global Accelerator sélectionne un nouveau point de terminaison, si nécessaire, uniquement lorsqu'une nouvelle connexion démarre ou après un délai d'inactivité.

Adresses IP statiques dans AWS Global Accelerator

Vous utilisez les adresses IP statiques que Global Accelerator attribue à votre accélérateur (ou que vous spécifiez à partir de votre propre pool d'adresses IP, pour les accélérateurs standard) pour acheminer le trafic Internet vers le réseau global AWS près de l'endroit où se trouvent vos utilisateurs, quel que soit leur emplacement. Pour les accélérateurs standard, vous associez les adresses à des équilibreurs de charge réseau, des équilibreurs de charge d'application, des instances Amazon EC2 ou des adresses IP élastiques qui s'exécutent dans une seule région AWS ou plusieurs régions. Pour les accélérateurs de routage personnalisés, vous dirigez le trafic vers des destinations EC2 dans les sous-réseaux VPC d'une ou plusieurs régions. Le routage du trafic via le réseau mondial AWS améliore la disponibilité et les performances, car le trafic n'a pas à prendre plusieurs sauts sur Internet public. L'utilisation d'adresses IP statiques vous permet également de distribuer le trafic d'applications entrant sur plusieurs ressources de point de terminaison dans plusieurs régions AWS.

En outre, l'utilisation d'adresses IP statiques facilite l'ajout de votre application à d'autres régions ou la migration d'applications entre régions. L'utilisation d'adresses IP fixes signifie que les utilisateurs disposent d'un moyen cohérent de se connecter à votre application lorsque vous apportez des modifications.

Si vous le souhaitez, vous pouvez associer votre propre nom de domaine personnalisé aux adresses IP statiques de votre accélérateur. Pour plus d'informations, consultez Router le trafic de domaine personnalisé vers votre accélérateur.

Global Accelerator fournit les adresses IP statiques à partir du pool d'adresses IP Amazon, sauf si vous apportez votre propre plage d'adresses IP à AWS, puis spécifiez les adresses IP statiques de ce pool. (Pour plus d'informations, consultez Fourniture de vos propres adresses IP (BYOIP) dans AWS Global Accelerator.) Pour créer un accélérateur sur la console, la première étape consiste à demander à Global Accelerator de provisionner les adresses IP statiques en saisissant un nom pour votre accélérateur ou en choisissant vos propres adresses IP statiques. Pour voir les étapes de création d'un accélérateur, voirMise en route d'AWS Global Accelerator.

Les adresses IP statiques restent assignées à votre accélérateur aussi longtemps qu'il existe, même si vous désactivez l'accélérateur et qu'il n'accepte plus ni achemine le trafic. Cependant, lorsque vousdeleteun accélérateur, vous perdez les adresses IP statiques qui lui sont assignées, de sorte que vous ne pouvez plus acheminer le trafic en les utilisant. Vous pouvez utiliser des stratégies IAM telles que des autorisations basées sur des balises avec Global Accelerator pour limiter les

utilisateurs disposant des autorisations pour supprimer un accélérateur. Pour plus d'informations, consultez Stratégies basées sur balises.

Gestion du flux de trafic avec cadrans de trafic et poids des points d'extrémité

Vous pouvez personnaliser la façon dont AWS Global Accelerator envoie le trafic vers vos terminaux avec un accélérateur standard de deux façons :

- Modifier la numérotation du trafic pour limiter le trafic pour un ou plusieurs groupes de points de terminaison
- Spécifiez des pondérations pour modifier la proportion du trafic par rapport aux points de terminaison d'un groupe

Fonctionnement des cadrans de trafic

Pour chaque groupe de points de terminaison d'un accélérateur standard, vous pouvez définir une numérotation de trafic pour contrôler le pourcentage de trafic envoyé au groupe de points de terminaison. Le pourcentage est appliqué uniquement au trafic déjà dirigé vers le groupe de points de terminaison, et non à tout le trafic d'écoute.

La numérotation de trafic limite la partie du trafic qu'un groupe de points de terminaison accepte, exprimée en pourcentage du trafic dirigé vers ce groupe de points de terminaison. Par exemple, si vous définissez la numérotation de trafic pour un groupe de points de terminaison dans`us-east-1`à 50 (c'est-à-dire 50 %) et que l'accélérateur dirige 100 demandes d'utilisateurs vers ce groupe de points de terminaison, seules 50 demandes sont acceptées par le groupe. L'accélérateur dirige les 50 demandes restantes vers des groupes de points de terminaison dans d'autres régions.

Pour plus d'informations, consultez Réglage du flux de trafic avec les cadrans de trafic.

Fonctionnement des poids

Pour chaque point de terminaison d'un accélérateur standard, vous pouvez spécifier des pondérations, qui sont des nombres qui modifient la proportion de trafic que l'accélérateur achemine vers chaque point de terminaison. Cela peut être utile, par exemple, pour effectuer des tests de performance dans une région.

Un poids est une valeur qui détermine la proportion de trafic que l'accélérateur dirige vers un terminal. Par défaut, le poids d'un point de terminaison est 128, c'est-à-dire la moitié de la valeur maximale d'un poids, 255.

L'accélérateur calcule la somme des pondérations des points de terminaison d'un groupe de points de terminaison, puis dirige le trafic vers les points de terminaison en fonction du rapport entre le poids de chaque point de terminaison et le total. Pour obtenir un exemple de fonctionnement des poids, consultezPondérations des points de.

Les cadrans et les poids influent sur la façon dont l'accélérateur standard sert le trafic de différentes manières :

- Vous configurez les cadrans de trafic pourGroupes de points de terminaison. La molette de trafic vous permet de couper un pourcentage du trafic (ou l'ensemble du trafic) vers le groupe, en « numérotant » le trafic que l'accélérateur lui a déjà dirigé en fonction d'autres facteurs, tels que la proximité.
- Vous utilisez des poids, d'autre part, pour définir des valeurs pourPoints de terminaison individuelsdans un groupe de points de terminaison. Les pondérations permettent de diviser le trafic au sein du groupe de points de terminaison. Par exemple, vous pouvez utiliser des pondérations pour effectuer des tests de performances pour des points de terminaison spécifiques dans une région.

> **Note**
>
> Pour plus d'informations sur l'incidence des cadrans et poids de trafic sur le basculement, consultezBasculement sur incident pour les terminaux non sains.

Contrôles de l'état d'AWS Global Accelerator

Pour les accélérateurs standard, AWS Global Accelerator vérifie automatiquement l'intégrité des points de terminaison associés à vos adresses IP statiques, puis dirige le trafic utilisateur uniquement vers des points de terminaison sains.

Global Accelerator inclut des contrôles d'intégrité par défaut qui sont exécutés automatiquement, mais vous pouvez configurer la synchronisation des vérifications et d'autres options. Si vous avez configuré des paramètres de vérification de l'intégrité personnalisés, Global Accelerator utilise

ces paramètres de manière spécifique, en fonction de votre configuration. Vous configurez ces paramètres dans l'instance Global Accelerator pour Amazon EC2 ou les points de terminaison d'adresse IP Elastic ou en configurant les paramètres sur la console Elastic Load Balancing pour les équilibreurs de charge réseau ou les équilibreurs de charge d'application. Pour plus d'informations, consultez Health check options (Options de vérification de l'état).

Lorsque vous ajoutez un point de terminaison à un accélérateur standard, il doit passer un contrôle d'intégrité pour être considéré comme sain avant que le trafic ne soit dirigé vers lui. Si Global Accelerator ne dispose pas de points de terminaison sains vers lesquels acheminer le trafic dans un accélérateur standard, il achemine les demandes vers tous les points de terminaison.

Types d'accélérateurs

Il existe deux types d'accélérateurs que vous pouvez utiliser avec AWS Global Accelerator :Accélérateurs standardandaccélérateurs de routage personnalisés. Les deux types d'accélérateurs acheminent le trafic sur le réseau mondial AWS pour améliorer les performances et la stabilité, mais ils sont tous conçus pour répondre à différents besoins des applications.

Accélérateur standard

> En utilisant un accélérateur standard, vous pouvez améliorer la disponibilité et les performances de vos applications exécutées sur des équilibreurs de charge d'application, des équilibreurs de charge réseau ou des instances Amazon EC2. Avec un accélérateur standard, Global Accelerator achemine le trafic client entre les points de terminaison régionaux en fonction de la géo-proximité et de l'intégrité des points de terminaison. Il permet également aux clients de transférer le trafic client entre les points de terminaison en fonction de contrôles tels que les cadrans de trafic et les poids des points de terminaison. Cela fonctionne pour une grande variété de cas d'utilisation, y compris le déploiement bleu/vert, les tests A/B et le déploiement multi-régions. Pour voir plus de cas d'utilisation, voirCas d'utilisation AWS Global Accelerator.
>
> Pour en savoir plus, consultez la section Travailler avec des accélérateurs standard dans AWS Global Accelerator.

Accélateur de routage personnalisé

> Les accélérateurs de routage personnalisés fonctionnent bien pour les scénarios dans lesquels vous souhaitez utiliser une logique d'application personnalisée pour diriger un ou plusieurs utilisateurs vers une destination et un port spécifiques parmi d'autres, tout en profitant des avantages de performances de Global Accelerator. Par exemple, les applications VoIP attribuent

plusieurs appelants à un serveur multimédia spécifique pour démarrer des sessions vocales, vidéo et messagerie. Un autre exemple est les applications de jeu en ligne en temps réel où vous souhaitez assigner plusieurs joueurs à une seule session sur un serveur de jeu en fonction de facteurs tels que l'emplacement géographique, la compétence du joueur et le mode de jeu.

Pour en savoir plus, consultez la section Travailler avec des accélérateurs de routage personnalisés dans AWS Global Accelerator.

En fonction de vos besoins spécifiques, vous créez l'un de ces types d'accélérateurs pour accélérer le trafic client.

Plages d'adresses IP et d'emplacements des serveurs périphériques Global Accelator

Pour obtenir la liste des emplacements de serveurs périphériques Global AccelatorOù AWS Global Accelerator est-il déployé aujourd'hui ?dans la sectionFAQ AWS Global Accelerator.

AWS publie ses plages d'adresses IP actuelles au format JSON. Pour afficher les plages actuelles, téléchargezip-ranges.json. Pour plus d'informations, consultez AWS IP Address Ranges dans le manuel Amazon Web Services General Reference.

Pour trouver les plages d'adresses IP associées aux serveurs périphériques AWS Global Accelerator, effectuez une rechercheip-ranges.jsonpour la chaîne suivante :

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

Entrées Global Accelerator qui incluent`"region": "GLOBAL"`font référence aux adresses IP statiques qui sont allouées aux accélérateurs. Si vous souhaitez filtrer le trafic via votre accélérateur provenant de points de présence (POP) d'une zone, filtrez les entrées qui incluent une zone géographique spécifique, commeus-*oueu-*. Ainsi, par exemple, si vous filtrez pourus-*, vous ne verrez que le trafic transitant par les POP aux États-Unis (États-Unis).

Cas d'utilisation AWS Global Accelerator

L'utilisation d'AWS Global Accelerator peut vous permettre d'atteindre différents objectifs. Cette section répertorie certains d'entre eux, pour vous donner une idée de la façon dont vous pouvez utiliser Global Accelerator pour répondre à vos besoins.

Échelle pour une utilisation accrue des applications

Lorsque l'utilisation des applications augmente, le nombre d'adresses IP et de points de terminaison que vous devez gérer augmente également. Global Accelerator vous permet de faire évoluer votre réseau vers le haut ou vers le bas. Il vous permet d'associer des ressources régionales, telles que des équilibreurs de charge et des instances Amazon EC2, à deux adresses IP statiques. Vous incluez ces adresses dans les listes autorisées une seule fois dans vos applications clientes, pare-feu et enregistrements DNS. Avec Global Accelerator, vous pouvez ajouter ou supprimer des points de terminaison dans les régions AWS, exécuter un déploiement bleu/vert et effectuer des tests A/B sans avoir à mettre à jour les adresses IP de vos applications clientes. Ceci est particulièrement utile pour les cas d'utilisation de l'IoT, de la vente au détail, des médias, de l'automobile et de la santé dans lesquels vous ne pouvez pas facilement mettre à jour les applications clientes fréquemment.

Accélération pour les applications sensibles à la latence

De nombreuses applications, en particulier dans des domaines tels que les jeux, les médias, les applications mobiles et les finances, nécessitent une latence très faible pour une expérience utilisateur optimale. Pour améliorer l'expérience utilisateur, Global Accelerator dirige le trafic utilisateur vers le point de terminaison de l'application le plus proche du client, ce qui réduit la latence et la gigue d'Internet. Global Accelerator achemine le trafic vers l'emplacement périphérique le plus proche à l'aide d'Anycast, puis le achemine vers le point de terminaison régional le plus proche via le réseau global AWS. Global Accelerator réagit rapidement aux changements dans les performances du réseau pour améliorer les performances des applications de vos utilisateurs.

Reprise après sinistre et résilience multi-régions

Vous devez être en mesure de vous fier à votre réseau pour être disponible. Vous pouvez exécuter votre application dans plusieurs régions AWS pour prendre en charge la reprise après sinistre, une disponibilité accrue, une latence réduite ou la conformité. Si Global Accelerator détecte que votre point de terminaison d'application tombe en panne dans la région AWS principale, il déclenche instantanément le réacheminement du trafic vers votre point de terminaison d'application dans la région AWS la plus proche disponible.

Protection de vos applications

L'exposition de vos origines AWS, telles que les équilibreurs de charge d'application ou les instances Amazon EC2, au trafic Internet public crée une opportunité pour des attaques malveillantes. Global Accelerator réduit le risque d'attaque en masquant votre origine derrière deux points d'entrée statiques. Ces points d'entrée sont protégés par défaut contre les attaques

par déni de service distribué (DDoS) avec AWS Shield. Global Accelerator crée une connexion d'appairage avec votre Amazon Virtual Private Cloud à l'aide d'adresses IP privées, ce qui permet de conserver les connexions à vos équilibreurs de charge d'application internes ou aux instances EC2 privées hors de l'Internet public.

Améliorer les performances pour les applications VoIP ou de jeux en ligne

Grâce à un accélérateur de routage personnalisé, vous pouvez tirer parti des avantages de performances de Global Accelerator pour vos applications VoIP ou de jeu. Par exemple, vous pouvez utiliser Global Accelerator pour les applications de jeu en ligne qui attribuent plusieurs joueurs à une seule session de jeu. Utilisez Global Accelerator pour réduire la latence et la gigue globalement pour les applications qui nécessitent une logique personnalisée pour mapper les utilisateurs à des points de terminaison spécifiques, tels que les jeux multijoueurs ou les appels VoIP. Vous pouvez utiliser un accélérateur unique pour connecter des clients à des milliers d'instances Amazon EC2 s'exécutant dans une ou plusieurs régions AWS, tout en conservant le contrôle total du client dirigé vers quelle instance EC2 et quel port.

Outil de comparaison de vitesse AWS Global Accelerator

Vous pouvez utiliser l'outil AWS Global Accelerator Speed Comparaison Tool pour voir les vitesses de téléchargement de Global Accelerator comparées aux téléchargements directs sur Internet, dans les régions AWS. Cet outil vous permet d'utiliser votre navigateur pour voir la différence de performances lorsque vous transférez des données à l'aide de Global Accelerator. Vous choisissez une taille de fichier à télécharger, et l'outil télécharge les fichiers via HTTP/TCP à partir des équilibreurs de charge d'application dans différentes régions vers votre navigateur. Pour chaque région, vous voyez une comparaison directe des vitesses de téléchargement.

Pour accéder à l'outil de comparaison de vitesse, copiez l'URL suivante dans votre navigateur :

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

Important

Les résultats peuvent différer lorsque vous exécutez le test plusieurs fois. Les temps de téléchargement peuvent varier en fonction de facteurs externes à Global Accelerator, tels que la qualité, la capacité et la distance de la connexion dans le réseau de dernier kilomètre que vous utilisez.

Procédure de démarrage d'AWS Global Accelerator

Vous pouvez commencer à configurer AWS Global Accelerator à l'aide de l'API ou de la console AWS Global Accelerator. Étant donné que Global Accelerator est un service global, il n'est pas lié à une région AWS spécifique. Notez que Global Accelerator est un service global qui prend en charge les points de terminaison dans plusieurs régions AWS, mais vous devez spécifier la région USA West (Oregon) pour créer ou mettre à jour des accélérateurs.

Pour commencer à utiliser Global Accelerator, procédez comme suit :

1. Choisissez le type d'accélérateur que vous voulez créer : Un accélérateur standard ou accélérateur de routage personnalisé
2. Configurez la configuration initiale pour Global Accelerator : Fournissez un nom pour votre accélérateur Configurez ensuite un ou plusieurs écouteurs pour traiter les connexions entrantes à partir de clients, en fonction du protocole et du port (ou plage de ports) que vous spécifiez.
3. Configurez des groupes de points de terminaison régionaux pour votre accélérateur : Vous pouvez sélectionner un ou plusieurs groupes de points de terminaison régionaux à ajouter à votre processus d'écoute. Le processus d'écoute achemine les demandes vers les points de terminaison que vous avez ajoutés à un groupe de points de terminaison.

   Pour un accélérateur standard, Global Accelerator surveille l'état des points de terminaison au sein du groupe à l'aide des paramètres de vérification de l'état définis pour chacun de vos points de terminaison. Pour chaque groupe de points de terminaison dans un accélérateur standard, vous pouvez configurer unNuméro de traficpour contrôler le pourcentage de trafic qu'un groupe de points de terminaison acceptera. Le pourcentage est appliqué uniquement au trafic qui est déjà dirigé vers le groupe de points de terminaison, et non à l'ensemble du trafic d'écoute. Par défaut, la numérotation de trafic est définie sur 100 % pour tous les groupes de points de terminaison régionaux.

   Pour un accélérateur de routage personnalisé, le trafic est routé de manière déterministe vers une destination spécifique dans un sous-réseau VPC, en fonction du port d'écoute sur lequel le trafic est reçu.
4. Ajouter des points de terminaison aux groupes de points de terminaison : Les points de terminaison que vous ajoutez dépendent du type d'accélérateur.
   - Pour un accélérateur standard, vous pouvez ajouter une ou plusieurs ressources régionales, telles que des équilibreurs de charge ou des points de terminaison d'instances EC2, à chaque groupe de points de terminaison. Ensuite, vous pouvez décider de la quantité de trafic que vous

souhaitez acheminer vers chaque point de terminaison en définissant des pondérations de point de terminaison.

- Pour un accélérateur de routage personnalisé, vous ajoutez un ou plusieurs sous-réseaux de cloud privé virtuel (VPC) avec jusqu'à des milliers de destinations d'instance Amazon EC2.

Pour obtenir des étapes détaillées sur la création d'un accélérateur standard ou d'un accélérateur de routage personnalisé à l'aide de la console AWS Global Accelerator, consultezMise en route d'AWS Global Accelerator. Pour utiliser les opérations d'API, consultezActions courantes que vous pouvez utiliser avec AWS Global Acceleratoret l'Référence de l'API AWS Global Accelerator.

Balisage dans AWS Global Accelerator

Les balises sont des mots ou des expressions (métadonnées) que vous utilisez pour identifier et organiser vos ressources AWS. Vous pouvez ajouter plusieurs balises à une ressource, chacune de ces balises étant composée d'une clé et d'une valeur que vous définissez. Par exemple, la clé peut être`environment`et la valeur peut être`production`. Vous pouvez rechercher et filtrer vos ressources en fonction des balises que vous ajoutez. Dans AWS Global Accelerator, vous pouvez marquer les accélérateurs.

Voici deux exemples montrant l'utilité de l'utilisation des balises dans Global Accelerator :

- Utilisez des balises pour suivre les informations de facturation dans différentes catégories. Pour ce faire, appliquez des balises aux accélérateurs ou à d'autres ressources AWS (telles que les équilibreurs de charge réseau, les équilibreurs de charge d'application ou les instances Amazon EC2) et activez les balises. AWS génère ensuite un rapport de répartition des coûts sous forme de valeurs séparées par des virgules (fichier CSV), détaillant l'utilisation et les coûts pour vos balises actives. Vous pouvez appliquer des balises associées à des catégories métier (telles que les centres de coûts, les noms d'applications ou les propriétaires) pour organiser les coûts relatifs à divers services. Pour de plus amples informations, veuillez consulter Utilisation des balises de répartition des coûts dans le Guide de l'utilisateur pour la gestion des coûts et de la facturation AWS.
- Utilisez des balises pour appliquer des autorisations basées sur des balises pour les accélérateurs. Pour ce faire, créez des stratégies IAM qui spécifient des balises et des valeurs de balise pour autoriser ou interdire les actions. Pour plus d'informations, consultez Stratégies basées sur balises.

Pour connaître les conventions d'utilisation et les liens vers d'autres ressources sur le balisage, voirBalisage des ressources AWSdans leRéférences générales AWS. Pour obtenir des conseils sur l'utilisation des balises, consultezBalisage des meilleures pratiques : Stratégie de balisage des ressources AWSdans leLivres blancs AWSBlog.

Pour connaître le nombre maximal de balises que vous pouvez ajouter à une ressource dans Global Accelerator, consultez la pageQuotas pour AWS Global Accelerator.

Vous pouvez ajouter et mettre à jour des balises à l'aide de la console AWS, de l'interface de ligne de commande AWS ou de l'API Global Accelerator. Ce chapitre comprend les étapes à suivre pour utiliser le balisage dans la console. Pour plus d'informations sur l'utilisation des balises à l'aide de l'interface de ligne de commande AWS et de l'API Global Accelerator, y compris des exemples d'interface de ligne de commande, consultez les opérations suivantes dans laRéférence de l'API AWS Global Accelerator :

- CreateAccelerator
- TagResource
- UntagResource
- ListTagsForResource

Prise en charge du balisage dans Global Accelerator

AWS Global Accelerator prend en charge le balisage des accélérateurs.

Global Accelerator prend en charge la fonction de contrôle d'accès basée sur des balises d'AWS Identity and Access Management (IAM). Pour plus d'informations, consultez Stratégies basées sur balises.

Ajout, modification et suppression de balises dans Global Accelerator

La procédure suivante explique comment ajouter, modifier et supprimer des balises pour les accélérateurs dans la console Global Accelerator.

> **Note**
>
> Vous pouvez ajouter ou supprimer des balises à l'aide des opérations de la console, de l'interface de ligne de commande AWS ou des API Global Accelerator. Pour

plus d'informations, y compris des exemples de ligne de commande, consultez la pageTagResourcedans leRéférence de l'API AWS Global Accelerator.

Pour ajouter, modifier ou supprimer des balises dans Global Accelerator

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Sélectionnez l'accélérateur pour lequel vous souhaitez ajouter ou mettre à jour des balises.
3. DansTags (Balises)vous permet d'effectuer les actions suivantes :

   Ajouter une balise

   ChoisissezAjouter une balise, puis entrez une clé et, éventuellement, une valeur pour la balise.

   Modifier une balise

   Mettez à jour le texte pour une clé, une valeur ou les deux. Vous pouvez également effacer la valeur d'une balise, mais la clé est obligatoire.

   Supprimer une balise

   ChoisissezSupprimezSur la droite du champ de valeur.
4. Sélectionnez Save Changes.

Tarification d'AWS Global Accelerator

Avec AWS Global Accelerator Vous êtes facturé à un tarif horaire et aux frais de transfert de données pour chaque accélérateur de votre compte. Pour de plus amples informations, veuillez consulterTarification AWS Global Accelerator.

Mise en route d'AWS Global Accelerator

Ces didacticiels fournissent les étapes à suivre pour démarrer avec AWS Global Accelerator à l'aide de la console. Vous pouvez également utiliser les opérations d'API AWS Global Accelerator pour créer et personnaliser vos accélérateurs. À chaque étape de ce didacticiel, il y a un lien vers l'opération API correspondante pour terminer la tâche par programmation. (Lorsque vous configurez un accélérateur de routage personnalisé, vous devez utiliser l'API pour certaines étapes de configuration.) Pour plus d'informations sur l'utilisation des opérations AWS Global Accelerator, consultez leRéférence de l'API AWS Global Accelerator.

> **Tip**
>
> Pour découvrir comment utiliser Global Accelerator pour améliorer les performances et la disponibilité des applications Web, consultez l'atelier suivant : Atelier AWS Global Accelerator.

Global Accelerator est un service global qui prend en charge les points de terminaison dans plusieurs régions AWS répertoriées dans leTable des régions AWS.

Ce chapitre comprend deux didacticiels : un pour la création d'un accélérateur standard et un pour la création d'un accélérateur de routage personnalisé. Pour en savoir plus sur les deux types d'accélérateurs, consultezTravailler avec des accélérateurs standard dans AWS Global AcceleratorandTravailler avec des accélérateurs de routage personnalisés dans AWS Global Accelerator.

Rubriques

- Mise en route d'un accélérateur standard
- Mise en route d'un accélérateur de routage personnalisé

Mise en route d'un accélérateur standard

Cette section répertorie les étapes à suivre pour créer un accélérateur standard qui achemine le trafic vers un point de terminaison optimal

Tâches

Avant de commencer

Avant de créer un accélérateur, créez au moins une ressource que vous pouvez ajouter en tant que point de terminaison vers laquelle diriger le trafic. Par exemple, créez l'une des méthodes suivantes :

- Lancez au moins une instance Amazon EC2 à ajouter en tant que point de terminaison. Pour de plus amples informations, veuillez consulterCréez vos ressources EC2 et lancez votre instance EC2dans leGuide de l'utilisateur Amazon EC2 pour les instances Linux.
- Vous pouvez également créer un ou plusieurs équilibreurs de charge réseau ou des équilibreurs de charge d'application qui incluent des instances EC2. Pour de plus amples informations, veuillez consulterCréer un équilibreur de charge d'application Network Load Balancerdans leGuide de l'utilisateur des Network Load Balancers.

Lorsque vous créez une ressource à ajouter à Global Accelator, soyez conscient des points suivants :

- Lorsque vous ajoutez un Application Load Balancer interne ou un point de terminaison d'instance EC2 dans Global Accelerator, vous autorisez le trafic Internet à circuler directement vers et depuis le point de terminaison dans des clouds privés virtuels (VPC) en le ciblant dans un sous-réseau privé. Le VPC qui contient l'instance EC2 ou l'équilibreur de charge doit avoir unPasserelle Internetjoint à lui, pour indiquer que le VPC accepte le trafic Internet. Pour plus d'informations, consultez Connexions VPC sécurisées dans AWS Global Accelerator.
- Global Accelerator requiert que vos règles de routeur et de pare-feu autorisent le trafic entrant à partir des adresses IP associées aux vérificateurs d'intégrité de Route 53 pour effectuer des vérifications d'intégrité pour les points de terminaison d'instance EC2 ou d'adresse IP Elastic. Vous trouverez des informations sur les plages d'adresses IP associées aux vérificateurs d'état Amazon Route 53 dansVérifications de l'état de vos groupes cibledans leGuide du développeur Amazon Route 53.

Étape 1 : Créer un accélérateur

Pour créer votre accélérateur, entrez un nom.

> **Note**
>
> Pour effectuer cette tâche à l'aide d'une opération d'API au lieu de la console, consultezCreateAcceleratordans leRéférence de l'API AWS Global Accelerator.

Pour créer un accélérateur

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. ChoisissezCréer un accélérateur.
3. Fournissez un nom pour votre accélérateur.
4. Si vous le souhaitez, ajoutez une ou plusieurs balises pour faciliter l'identification de vos ressources Accelerator Global si vous le souhaitez.
5. Choisissez Suivant.

Étape 2 : Ajouter des écouteurs

Créez un écouteur pour traiter les connexions entrantes de vos utilisateurs vers Global Accelator.

> **Note**
>
> Pour effectuer cette tâche à l'aide d'une opération d'API au lieu de la console, consultezCreateListenerdans leRéférence de l'API AWS Global Accelerator.

Pour créer un écouteur

1. Dans la pageAjouter un écouteur, entrez les ports ou plages de ports que vous souhaitez associer au processus d'écoute. Les écouteurs prennent en charge les ports 1 à 65535.
2. Choisissez le ou les protocoles pour les ports que vous avez entrés.
3. Le cas échéant, choisissez d'activer l'affinité du client. L'affinité client pour un écouteur signifie que Global Accelerator garantit que les connexions d'une adresse IP source (client) spécifique

sont toujours acheminées vers le même point de terminaison. Pour activer ce comportement, dans la liste déroulante, choisissezIP Source.

La valeur par défaut estAucun, ce qui signifie que l'affinité du client n'est pas activée et que Global Accelerator distribue le trafic de manière égale entre les points de terminaison des groupes de points de terminaison pour l'écouteur.

Pour plus d'informations, consultez Affinité du client.

4. Choisissez éventuellementAjouter un écouteurpour ajouter un écouteur supplémentaire.
5. Lorsque vous avez fini d'ajouter les écouteurs, choisissezSuivant.

Étape 3 : Ajouter des groupes d'endpoints

Ajoutez un ou plusieurs groupes de points de terminaison, chacun étant associé à une région AWS spécifique.

> **Note**
>
> Pour effectuer cette tâche à l'aide d'une opération d'API au lieu de la console, consultezCreateEndPointGroupdans leRéférence de l'API AWS Global Accelerator.

Ajouter un groupe de points de terminaison

1. Dans la pageAjouter des groupes d'endpoints, dans la section correspondant à un écouteur, choisissez unRégiondans la liste déroulante.
2. Facultatif, pourCadran de trafic, entrez un nombre compris entre 0 et 100 pour définir un pourcentage de trafic pour ce groupe de points de terminaison. Le pourcentage est appliqué uniquement au trafic déjà dirigé vers ce groupe de points de terminaison, et non à l'ensemble du trafic d'écoute. Par défaut, la numérotation de trafic pour un groupe de points de terminaison est définie sur 100 (c'est-à-dire 100 %).
3. Le cas échéant, pour les valeurs de vérification de l'intégrité personnalisées, choisissezConfigurer les vérifications de l'état. Lorsque vous configurez les paramètres de vérification de l'intégrité, Global Accelerator utilise les paramètres pour les vérifications de l'état des points de terminaison d'instance EC2 et d'adresse IP Elastic. Pour les points de terminaison de l'Network Load Balancer et de l'équilibreur de charge d'application, Global Accelerator utilise les paramètres de vérification de l'état que vous avez déjà configurés pour les équilibreurs

de charge eux-mêmes. Pour plus d'informations, consultez Health check options (Options de vérification de l'état).

4. Choisissez éventuellementAjout d'un groupe de pointspour ajouter des groupes de points de terminaison supplémentaires pour cet écouteur ou d'autres écouteurs.
5. Choisissez Suivant.

Étape 4 : Ajouter des points de terminaison

Ajoutez un ou plusieurs points de terminaison associés à des groupes de points de terminaison spécifiques. Cette étape n'est pas obligatoire, mais aucun trafic n'est dirigé vers les points de terminaison d'une région, à moins que les points de terminaison ne soient inclus dans un groupe de points de terminaison.

> **Note**
>
> Si vous créez votre accélérateur par programme, vous ajoutez des points de terminaison dans le cadre de l'ajout de groupes de points de terminaison. Pour de plus amples informations, veuillez consulterCreateEndPointGroupdans leRéférence de l'API AWS Global Accelerator.

Ajouter des points de terminaison

1. Dans la pageCréer des points de terminaison, dans la section correspondant à un point de terminaison, choisissez unPoint de terminaison.
2. Facultatif, pourPoids, entrez un nombre compris entre 0 et 255 pour définir une pondération pour le trafic de routage vers ce point de terminaison. Lorsque vous ajoutez des poids aux points de terminaison, vous configurez Global Accelerator pour acheminer le trafic en fonction des proportions que vous spécifiez. Par défaut, tous les points de terminaison ont un poids de 128. Pour plus d'informations, consultez Pondérations des points de.
3. Si vous le souhaitez, pour un point de terminaison Application Load Balancer, sousPréserver l'adresse IP du client, sélectionnezPréserver l'adresse. Pour plus d'informations, consultez Conserver les adresses IP des clients dans AWS Global Accelerator.
4. Choisissez éventuellementAjouter un point de terminaisonpour ajouter d'autres points de terminaison.
5. Choisissez Suivant.

Après avoir choisiSuivant, sur le tableau de bord Global Accelerator, vous verrez un message indiquant que votre accélérateur est en cours. Lorsque le processus est terminé, l'état accélérateur dans le tableau de bord estActif.

Étape 5 : Testez votre accélérateur

Prenez des mesures pour tester votre accélérateur afin de vous assurer que le trafic est dirigé vers vos terminaux. Par exemple, exécutez une commande curl telle que la suivante, en remplaçant l'une des adresses IP statiques de votre accélérateur, pour afficher les régions AWS où les demandes sont traitées. Ceci est particulièrement utile si vous définissez des pondérations différentes pour les points de terminaison ou si vous réglez la numérotation du trafic sur les groupes de points de terminaison

Exécutez une commande curl comme la suivante, en remplaçant l'une des adresses IP statiques de votre accélérateur, pour appeler l'adresse IP 100 fois, puis générer un compte de l'endroit où chaque requête a été traitée.

```
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 vous avez ajusté la numérotation de trafic sur n'importe quel groupe de points de terminaison, cette commande peut vous aider à confirmer que votre accélérateur dirige les pourcentages corrects de trafic vers différents groupes. Pour plus d'informations, consultez les exemples détaillés dans le billet de blog suivant,Gestion du trafic avec AWS Global Accelerator.

Étape 6 (facultatif) : Supprimez votre accélérateur

Si vous avez créé un accélérateur en tant que test ou si vous n'utilisez plus d'accélérateur, vous pouvez le supprimer. Sur la console, désactivez l'accélérateur, puis vous pouvez le supprimer. Vous n'avez pas besoin de supprimer les écouteurs et les groupes de points de terminaison de l'accélérateur.

Pour supprimer un accélérateur à l'aide d'une opération API à la place de la console, vous devez d'abord supprimer tous les écouteurs et groupes de points de terminaison associés à l'accélérateur et le désactiver. Pour plus d'informations, consultez le .DeleteAcceleratorOpération dans leRéférence de l'API AWS Global Accelerator.

Soyez conscient des éléments suivants lorsque vous supprimez des points de terminaison ou des groupes de points de terminaison, ou supprimez un accélérateur :

- Lorsque vous créez un accélérateur, Global Accelerator vous fournit un ensemble de deux adresses IP statiques. Les adresses IP sont assignées à votre accélérateur aussi longtemps qu'il existe, même si vous désactivez l'accélérateur et qu'il n'accepte plus ni achemine le trafic. Cependant, lorsque vousdeleteun accélérateur, vous perdez les adresses IP statiques qui sont assignées à l'accélérateur, de sorte que vous ne pouvez plus acheminer le trafic en les utilisant. Comme pratique exemplaire, assurez-vous que vous disposez des autorisations nécessaires pour éviter de supprimer par inadvertance des accélérateurs. Vous pouvez utiliser des stratégies IAM avec Global Accelerator, par exemple des autorisations basées sur des balises, pour limiter les utilisateurs disposant des autorisations pour supprimer un accélérateur. Pour plus d'informations, consultez Stratégies basées sur balises.
- Si vous mettez fin à une instance EC2 avant de la supprimer d'un groupe de points de terminaison dans Global Accelerator, puis que vous créez une autre instance avec la même adresse IP privée et que les vérifications d'intégrité passent, Global Accelerator achemine le trafic vers le nouveau point de terminaison. Si vous ne voulez pas que cela se produise, supprimez l'instance EC2 du groupe de points de terminaison avant de mettre fin à l'instance.

Pour supprimer un accélérateur

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Choisissez l'accélérateur que vous souhaitez supprimer.
3. Choisissez Modifier.
4. ChoisissezDésactiver l'accélérateur, puisEnregistrer.
5. Choisissez l'accélérateur que vous souhaitez supprimer.
6. ChoisissezSupprimer l'accélérateur.
7. Dans la boîte de dialogue de confirmation, choisissez Delete (Supprimer).

Mise en route d'un accélérateur de routage personnalisé

Cette section répertorie les étapes à suivre pour créer un accélérateur de routage personnalisé qui achemine le trafic de manière déterministe vers des destinations d'instance Amazon EC2 dans un point de terminaison de sous-réseau de cloud privé virtuel (VPC).

Tâches

- Avant de commencer

Avant de commencer

Avant de créer un accélérateur de routage personnalisé, créez une ressource que vous pouvez ajouter en tant que point de terminaison vers laquelle diriger le trafic. Un point de terminaison d'accélérateur de routage personnalisé doit être un sous-réseau de cloud privé virtuel (VPC), qui peut inclure plusieurs instances Amazon EC2. Pour obtenir des instructions sur la création des ressources, veuillez consulter les sections suivantes :

- Crée un sous-réseau VPC. Pour de plus amples informations, veuillez consulterCréation et configuration de votre VPCdans leGuide d'administration AWS Directory Service.
- Si vous le souhaitez, lancez une ou plusieurs instances Amazon EC2 dans votre VPC. Pour de plus amples informations, veuillez consulterCréez vos ressources EC2 et lancez votre instance EC2dans leGuide de l'utilisateur Amazon EC2 pour les instances Linux.

Lorsque vous créez une ressource à ajouter à Global Accelator, soyez conscient des points suivants :

- Lorsque vous ajoutez un point de terminaison d'instance EC2 dans Global Accelerator, vous activez le trafic Internet à circuler directement vers et depuis le point de terminaison dans des VPC en le ciblant dans un sous-réseau privé. Le VPC qui contient l'instance EC2 doit avoir unPasserelle Internetjoint à lui, pour indiquer que le VPC accepte le trafic Internet. Pour plus d'informations, consultez Connexions VPC sécurisées dans AWS Global Accelerator.

Étape 1 : Créer un accélérateur de routage personnalisé

> **Note**
>
> Pour effectuer cette tâche à l'aide d'une opération d'API au lieu de la console, consultezCreateCustomRoutingAcceleratordans leRéférence de l'API AWS Global Accelerator.

Pour créer un accélérateur

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Fournissez un nom pour votre accélérateur.
3. PourType d'accélérateur, sélectionnezRoutage personnalisé.
4. Si vous le souhaitez, ajoutez une ou plusieurs balises pour vous aider à identifier vos ressources d'accélérateur.
5. ChoisissezSuivantpour ajouter des écouteurs, des groupes de points de terminaison et des points de terminaison de sous-réseau VPC.

Étape 2 : Ajouter des écouteurs

Créez un écouteur pour traiter les connexions entrantes de vos utilisateurs vers Global Accelerator

La plage que vous spécifiez lorsque vous créez un écouteur définit le nombre de combinaisons d'adresses IP de port d'écoute et de destination que vous pouvez utiliser avec votre accélérateur de routage personnalisé. Pour une flexibilité maximale, nous vous recommandons de spécifier une large plage de ports. Chaque plage de ports d'écoute que vous spécifiez doit inclure au moins 16 ports.

> **Note**
>
> Pour effectuer cette tâche à l'aide d'une opération d'API au lieu de la console, consultezCreateCustomRoutinGlistenerdans leRéférence de l'API AWS Global Accelerator.

Pour créer un écouteur

1. Dans la pageAjouter un écouteur, entrez les ports ou plages de ports que vous souhaitez associer au processus d'écoute. Les écouteurs prennent en charge les ports 1 à 65535.
2. Choisissez le ou les protocoles pour les ports que vous avez entrés.
3. Choisissez éventuellementAjouter un écouteurpour ajouter un écouteur supplémentaire.
4. Lorsque vous avez fini d'ajouter les écouteurs, choisissezSuivant.

Étape 3 : Ajouter des groupes d'endpoints

Ajoutez un ou plusieurs groupes de points de terminaison, chacun étant associé à une région AWS spécifique. Pour chaque groupe de points de terminaison, spécifiez un ou plusieurs ensembles de plages de ports et de protocoles. Global Accelerator les utilise pour diriger le trafic vers les instances Amazon EC2 dans les sous-réseaux de la région.

Pour chaque plage de ports que vous fournissez, vous spécifiez également le protocole à utiliser : UDP, TCP, ou à la fois UDP et TCP.

> **Note**
>
> Pour effectuer cette tâche à l'aide d'une opération d'API au lieu de la console, consultezCreateCustomRoutingEndPointGroupdans leRéférence de l'API AWS Global Accelerator.

Ajouter un groupe de points de terminaison

1. Dans la pageAjouter des groupes d'endpoints, dans la section correspondant à un écouteur, choisissez unRégion.
2. PourJeux de ports et de protocoles, entrez les plages de ports et les protocoles pour vos instances Amazon EC2.

   - Saisissez unDepuis le portet unPort de destinationpour spécifier une plage de ports.
   - Pour chaque plage de ports, spécifiez le ou les protocoles correspondant à cette plage.

   La plage de ports ne doit pas nécessairement être un sous-ensemble de votre plage de ports d'écoute, mais il doit y avoir suffisamment de ports totaux dans la plage de ports d'écoute pour prendre en charge le nombre total de ports que vous spécifiez.
3. Choisissez Enregistrer.
4. Choisissez éventuellementAjout d'un groupe de pointspour ajouter des groupes de points de terminaison supplémentaires pour cet écouteur ou d'autres écouteurs.
5. Choisissez Suivant.

Étape 4 : Ajouter des points de terminaison de sous-réseau VPC

Ajoutez un ou plusieurs points de terminaison de sous-réseau de cloud privé virtuel (VPC) pour ce groupe de points de terminaison régionaux Les points de terminaison pour les accélérateurs de routage personnalisés définissent les sous-réseaux VPC qui peuvent recevoir du trafic via un accélérateur de routage personnalisé. Chaque sous-réseau peut contenir une ou plusieurs destinations d'instance Amazon EC2.

Lorsque vous ajoutez un point de terminaison de sous-réseau VPC, Global Accelerator génère de nouveaux mappages de ports que vous pouvez utiliser pour acheminer le trafic vers les adresses IP de l'instance EC2 de destination dans le sous-réseau. Ensuite, vous pouvez utiliser l'API Global Accelerator pour obtenir une liste statique de tous les mappages de ports pour le sous-réseau, et utiliser le mappage pour diriger le trafic de manière déterministe vers des instances EC2 spécifiques.

> **Note**
>
> Les étapes ci-dessous montrent comment ajouter des points de terminaison dans la console. Si vous créez votre accélérateur par programme, vous ajoutez des points de terminaison avec des groupes de points de terminaison. Pour de plus amples informations, veuillez consulterCreateCustomRoutingEndPointGroupdans leRéférence de l'API AWS Global Accelerator.

Ajouter des points de terminaison

1. Dans la pageAjouter des points de terminaison, dans la section du groupe de points de terminaison auquel vous souhaitez ajouter le point de terminaison, choisissez un ID de sous-réseau pourPoint de terminaison.
2. Si vous le souhaitez, effectuez l'une des opérations suivantes pour activer le trafic vers des destinations d'instance EC2 dans le sous-réseau :

   - Pour autoriser le trafic à être dirigé vers tous les points de terminaison et ports EC2 du sous-réseau, sélectionnezAutoriser tout le trafic
   - Pour autoriser le trafic vers des points de terminaison et des ports EC2 spécifiques sur le sous-réseau, sélectionnezAutoriser le trafic vers des adresses de socket de destination spécifiques. Spécifiez ensuite les adresses IP et les ports ou plages de ports à autoriser. Enfin, choisissezAutoriser ces destinations.

Par défaut, aucun trafic n'est autorisé pour les points de terminaison de sous-réseau. Si vous ne sélectionnez pas d'option permettant d'autoriser le trafic, le trafic est refusé vers toutes les destinations du sous-réseau.

> **Note**
>
> Si vous souhaitez activer le trafic vers des instances et des ports EC2 spécifiques dans le sous-réseau, vous pouvez le faire par programmation. Pour de plus amples informations, veuillez consulterAutoriser CustomRoutingTrafficdans leRéférence de l'API AWS Global Accelerator.

3. Choisissez Suivant.

Après avoir choisiSuivant, dans le tableau de bord Global Accelerator, vous verrez un message indiquant que votre accélérateur est en cours. Lorsque le processus est terminé, l'état accélérateur dans le tableau de bord estActif.

Étape 5 (facultatif) : Supprimez votre accélérateur

Si vous avez créé un accélérateur en tant que test ou si vous n'utilisez plus d'accélérateur, vous pouvez le supprimer. Sur la console, désactivez l'accélérateur, puis vous pouvez le supprimer. Vous n'avez pas besoin de supprimer les écouteurs et les groupes de points de terminaison de l'accélérateur.

Pour supprimer un accélérateur à l'aide d'une opération API à la place de la console, vous devez d'abord supprimer tous les écouteurs et groupes de points de terminaison associés à l'accélérateur et le désactiver. Pour plus d'informations, consultez le .DeleteCustomRoutingAcceleratorOpération dans leRéférence de l'API AWS Global Accelerator.

Soyez conscient des points suivants lorsque vous supprimez un accélérateur :

- Lorsque vous créez un accélérateur, Global Accelerator vous fournit un ensemble de deux adresses IP statiques. Les adresses IP sont assignées à votre accélérateur aussi longtemps qu'il existe, même si vous désactivez l'accélérateur et qu'il n'accepte plus ni achemine le trafic. Cependant, lorsque vousdeleteun accélérateur, vous perdez les adresses IP statiques qui sont assignées à l'accélérateur, de sorte que vous ne pouvez plus acheminer le trafic en les utilisant. Comme pratique exemplaire, assurez-vous que vous disposez des autorisations nécessaires

pour éviter de supprimer par inadvertance des accélérateurs. Vous pouvez utiliser des stratégies IAM telles que des autorisations basées sur des balises avec Global Accelerator pour limiter les utilisateurs disposant des autorisations pour supprimer un accélérateur. Pour plus d'informations, consultez Stratégies basées sur balises.

Pour supprimer un accélérateur

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Choisissez l'accélérateur que vous souhaitez supprimer.
3. Choisissez Modifier.
4. ChoisissezDésactiver l'accélérateur, puisEnregistrer.
5. Choisissez l'accélérateur que vous souhaitez supprimer.
6. ChoisissezSupprimer l'accélérateur.
7. Dans la boîte de dialogue de confirmation, choisissez Delete (Supprimer).

Actions courantes que vous pouvez utiliser avec AWS Global Accelerator

Cette section répertorie les actions AWS Global Accelerator courantes que vous pouvez utiliser avec les ressources Global Accelerator, avec des liens vers la documentation pertinente.

Actions à utiliser avec des ressources standard

Le tableau suivant répertorie les actions courantes de Global Accelerator que vous pouvez utiliser avec les accélérateurs standard Global Accelerator, avec des liens vers la documentation pertinente.

Action	Utilisation de la console Global Accelerator	Utilisation de l'API Global Accelerator
Créer un accélérateur standard	Voir Mise en route d'un accélérateur standard	Voir `CreateAccelerator`
Créer un écouteur d'un accélérateur standard	Voir Écouteurs pour les accélérateurs standard dans AWS Global Accelerator	Voir `CreateListener`
Créer un groupe de points de terminaison pour un accélérateur standard	Voir Groupes de points de terminaison pour les accélérateurs standard dans AWS Global Accelerator	Voir `CreateEndpointGroup`
Mettre à jour un accélérateur standard	Voir Accélérateurs standard dans AWS Global Accelerator	Voir `UpdateAccelerator`
Liste de vos accélérateurs	Voir Affichage de vos accélérateurs	Voir `ListAccelerator`
Obtenir toutes les informations sur un accélérateur	Voir Affichage de vos accélérateurs	Voir `DescribeAccelerator`
Supprimer un accélérateur	Voir Création ou mise à jour d'un accélérateur standard	Voir `DeleteAccelerator`

Actions à utiliser avec des ressources de routage personnalisées

Le tableau suivant répertorie les actions courantes de Global Accelerator que vous pouvez utiliser avec des accélérateurs de routage personnalisés, avec des liens vers la documentation pertinente.

Action	Utilisation de la console Global Accelerator	Utilisation de l'API Global Accelerator
Créer un accélérateur de routage personnalisé	Voir Mise en route d'un accélérateur de routage personnalisé	Voir `CreateCustomRoutingAccelerator`
Créer un écouteur d'un accélérateur de routage personnalisé	Voir Écouteurs pour les accélérateurs de routage personnalisés dans AWS Global Accelerator	Voir `CreateCustomRoutingListener`
Créer un groupe de points de terminaison d'un accélérateur de routage personnalisé	Voir Groupes de points de terminaison pour les accélérateurs de routage personnalisés dans AWS Global Accelerator	Voir `CreateCustomRoutingEndpointGroup`
Mettre à jour un accélérateur de routage personnalisé	Voir Accélérateurs de routage personnalisés dans AWS Global Accelerator	Voir `UpdateCustomRoutingAccelerator`
Liste de vos accélérateurs de routage personnalisés	Voir Affichage de vos accélérateurs de routage personnalisés	Voir `ListCustomRoutingAccelerator`
Obtenir toutes les informations sur un accélérateur de routage personnalisé	Voir Affichage de vos accélérateurs de routage personnalisés	Voir `DescribeCustomRoutingAccelerator`
Supprimer un accélérateur de routage personnalisé	Voir Création ou mise à jour d'un accélérateur de routage personnalisé	Voir `DeleteCustomRoutingAccelerator`

Action	Utilisation de la console Global Accelerator	Utilisation de l'API Global Accelerator
Obtenir le mappage de port statique d'un accélérateur de routage personnalisé	N/A	Voir `ListCustomRoutingPortMappings`
Autoriser tout le trafic de destination pour un sous-réseau dans un accélérateur de routage personnalisé	Voir Ajout, modification ou suppression d'un point de terminaison de sous-réseau VPC	Voir `AllowCustomRoutingTraffic`
Refuser tout le trafic de destination pour un sous-réseau dans un accélérateur de routage personnalisé	Voir Ajout, modification ou suppression d'un point de terminaison de sous-réseau VPC	Voir `DenyCustomRoutingTraffic`
Autoriser le trafic vers des destinations spécifiques dans un accélérateur de routage personnalisé	Voir Ajout, modification ou suppression d'un point de terminaison de sous-réseau VPC	Voir `AllowCustomRoutingTraffic`
Refuser le trafic vers des destinations spécifiques dans un accélérateur de routage personnalisé	Voir Ajout, modification ou suppression d'un point de terminaison de sous-réseau VPC	Voir `DenyCustomRoutingTraffic`

Travailler avec des accélérateurs standard dans AWS Global Accelerator

Ce chapitre contient des procédures et des recommandations pour la création d'accélérateurs standard dans AWS Global Accelerator. Avec un accélérateur standard, Global Accelerator choisit le point de terminaison sain le plus proche pour votre trafic.

Si vous souhaitez utiliser une logique d'application personnalisée pour diriger un ou plusieurs utilisateurs vers un point de terminaison spécifique parmi de nombreux points de terminaison, créez un accélérateur de routage personnalisé. Pour plus d'informations, consultez Travailler avec des accélérateurs de routage personnalisés dans AWS Global Accelerator.

Pour configurer un accélérateur standard, procédez comme suit :

1. Créez un accélérateur et choisissez l'option d'accélérateur standard.
2. Ajoutez un écouteur avec un ensemble spécifique de ports ou une plage de ports, et choisissez le protocole à accepter : TCP, UDP ou les deux.
3. Ajoutez un ou plusieurs groupes de points de terminaison, un pour chaque région AWS dans laquelle vous disposez de ressources de point de terminaison.
4. Ajoutez un ou plusieurs points de terminaison aux groupes de points de terminaison. Ce n'est pas obligatoire, mais le trafic ne sera pas routé si vous n'avez pas de points de terminaison. Les points de terminaison peuvent être des équilibreurs de charge réseau, des équilibreurs de charge d'application, des instances Amazon EC2 ou des adresses IP élastiques.

Les sections suivantes passent en revue l'utilisation des accélérateurs, des écouteurs, des groupes de points de terminaison et des points de terminaison standard.

Rubriques

Accélérateurs standard dans AWS Global Accelerator

AStandard AcceleratorDans AWS Global Accelerator, le trafic est dirigé vers des points de terminaison optimaux sur le réseau AWS Global Accelerator afin d'améliorer la disponibilité et les performances de vos applications Internet qui ont une audience mondiale. Chaque accélérateur comprend un ou plusieurs auditeurs. Un écouteur traite les connexions entrantes des clients vers Global Accelerator, en fonction du protocole (ou des protocoles) et du port (ou de la plage de ports) que vous configurez.

Lorsque vous créez un accélérateur, par défaut, Global Accelerator vous fournit un ensemble de deux adresses IP statiques. Si vous apportez votre propre plage d'adresses IP à AWS (BYOIP), vous pouvez attribuer à la place des adresses IP statiques de votre propre pool à utiliser avec votre accélérateur. Pour plus d'informations, consultez Fourniture de vos propres adresses IP (BYOIP) dans AWS Global Accelerator.

> **Important**
>
> Les adresses IP sont assignées à votre accélérateur aussi longtemps qu'il existe, même si vous désactivez l'accélérateur et qu'il n'accepte plus ni achemine le trafic. Cependant, lorsque vousdeleteun accélérateur, vous perdez les adresses IP statiques Global Accelerator qui sont assignées à l'accélérateur, de sorte que vous ne pouvez plus acheminer le trafic en les utilisant. Comme pratique exemplaire, assurez-vous que vous disposez des autorisations nécessaires pour éviter de supprimer par inadvertance des accélérateurs. Vous pouvez utiliser des stratégies IAM avec Global Accelerator, par exemple des autorisations basées sur des balises, pour limiter les utilisateurs disposant des autorisations pour supprimer un accélérateur. Pour plus d'informations, consultez Stratégies basées sur balises.

Cette section explique comment créer, modifier ou supprimer un accélérateur standard sur la console Global Accelerator. Si vous souhaitez utiliser les opérations API avec Global Accelerator, consultez le documentRéférence de l'API AWS Global Accelerator.

Rubriques

- Utilisation d'adresses IP statiques globales au lieu d'adresses IP statiques régionales

Création ou mise à jour d'un accélérateur standard

Cette section explique comment créer ou mettre à jour des accélérateurs standard sur la console. Pour travailler avec Global Accelerator par programmation, consultez laRéférence de l'API AWS Global Accelerator.

Pour créer un accélérateur standard

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. ChoisissezCréer un accélérateur.
3. Indiquez un nom pour votre accélérateur.
4. PourType d'accélérateur, sélectionnezStandard.
5. Si vous avez apporté vos propres plages d'adresses IP à AWS (BYOIP), vous pouvez spécifier une adresse IP statique pour votre accélérateur, une à partir de chaque pool d'adresses. Faites ce choix pour chacune des deux adresses IP statiques de votre accélérateur.

   - Pour chaque adresse IP statique, choisissez le pool d'adresses IP à utiliser.

     > **Note**
     >
     > Vous devez choisir un pool d'adresses IP différent pour chaque adresse IP statique. Cette restriction est due au fait que Global Accelerator affecte chaque plage d'adresses à une zone réseau différente, pour une haute disponibilité.

   - Si vous avez choisi votre propre pool d'adresses IP, choisissez également une adresse IP spécifique à partir du groupe. Si vous choisissez le pool d'adresses IP Amazon par défaut, Global Accelerator attribue une adresse IP spécifique à votre accélérateur.
6. Si vous le souhaitez, ajoutez une ou plusieurs balises pour vous aider à identifier vos ressources d'accélérateur.
7. ChoisissezSuivantpour ajouter des écouteurs, des groupes de points de terminaison et des points de terminaison.

Pour modifier un accélérateur standard

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la liste des accélérateurs, choisissez en un, puis choisissezModifier.
3. Dans la pageModifier l'accélérateur, apportez les modifications souhaitées. Par exemple, vous pouvez désactiver l'accélérateur pour qu'il n'accepte plus ou achemine le trafic, ou pour que vous puissiez le supprimer. Ou, si l'accélérateur est désactivé, vous pouvez l'activer.
4. Sélectionnez Save Changes.

Suppression d'un accélérateur

Si vous avez créé un accélérateur en tant que test ou si vous n'utilisez plus d'accélérateur, vous pouvez le supprimer. Sur la console, désactivez l'accélérateur, puis vous pouvez le supprimer. Vous n'avez pas besoin de supprimer les écouteurs et les groupes de points de terminaison de l'accélérateur.

Pour supprimer un accélérateur à l'aide d'une opération API au lieu de la console, vous devez d'abord supprimer tous les écouteurs et groupes de points de terminaison associés à l'accélérateur, puis le désactiver. Pour plus d'informations, consultez le .DeleteAcceleratordans leRéférence de l'API AWS Global Accelerator.

Pour désactiver un accélérateur

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la liste, choisissez un accélérateur que vous souhaitez désactiver.
3. Choisissez Modifier.
4. ChoisissezDésactiver l'accélérateur, puis choisissezEnregistrer.

Pour supprimer un accélérateur

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la liste, choisissez un accélérateur à supprimer.
3. Sélectionnez Delete.

> **Note**
>
> Si vous n'avez pas désactivé l'accélérateur,Supprimerest indisponible.

4. Dans la boîte de dialogue de confirmation, choisissez Delete (Supprimer).

> **Important**
>
> Lorsque vous supprimez un accélérateur, vous perdez les adresses IP statiques qui sont assignées à l'accélérateur, de sorte que vous ne pouvez plus acheminer le trafic en les utilisant.

Affichage de vos accélérateurs

Vous pouvez afficher les informations concernant vos accélérateurs sur la console. Pour voir les descriptions de vos accélérateurs par programme, consultezListAcceleratorsandDescribeAcceleratordans leRéférence de l'API AWS Global Accelerator.

Pour afficher des informations sur votre accélérateur

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Pour afficher des détails sur un accélérateur, dans la liste, choisissez un accélérateur, puis choisissezAfficher.

Ajouter un accélérateur lorsque vous créez un équilibreur de charge

Lorsque vous créez un Application Load Balancer dans AWS Management Console, vous pouvez le cas échéantAjouter un accélérateur. Elastic Load Balancing et Global Accelerator travaillent ensemble pour ajouter l'accélérateur de manière transparente. L'accélérateur est créé dans votre compte, avec l'équilibreur de charge comme point de terminaison. L'utilisation d'un accélérateur fournit des adresses IP statiques et améliore la disponibilité et les performances de vos applications.

> **Important**
>
> Pour créer un accélérateur, vous devez disposer des autorisations appropriées. Pour plus d'informations, consultez Autorisations requises pour l'accès à la console, la gestion de l'authentification et le contrôle d'accès.

Configurer et afficher votre accélérateur

Vous devez mettre à jour votre configuration DNS pour diriger le trafic vers les adresses IP statiques ou le nom DNS de l'accélérateur. Le trafic ne passera pas par l'accélérateur à votre équilibreur de charge tant que vos modifications de configuration ne seront pas terminées.

Après avoir créé votre équilibreur de charge en choisissant le module complémentaire Global Accelerator sur la console Amazon EC2, accédez à la pageServices intégrésPour afficher les adresses IP statiques et le nom DNS (Domain Name System) de votre accélérateur. Vous utilisez ces informations pour commencer à acheminer le trafic utilisateur vers l'équilibreur de charge sur le réseau global AWS. Pour plus d'informations sur le nom DNS attribué à votre accélérateur, consultez la sectionAdresses DNS et domaines personnalisés dans AWS Global Accelerator.

Vous pouvez visualiser et configurer votre accélérateur enNavigation vers Global AcceleratorDans AWS Management Console. Par exemple, vous pouvez voir les accélérateurs associés à votre compte ou ajouter des équilibreurs de charge supplémentaires à votre accélérateur. Pour plus d'informations, consultez Affichage de vos accélérateurs et Création ou mise à jour d'un accélérateur standard.

Tarification

Avec AWS Global Accelerator, vous ne payez que ce que vous utilisez. Vous êtes facturé à un tarif horaire et aux frais de transfert de données pour chaque accélérateur de votre compte. Pour de plus amples informations, veuillez consulterTarification AWS Global Accelerator.

Cessation d'utiliser l'accélérateur

Si vous souhaitez arrêter le routage du trafic via Global Accelerator vers votre équilibreur de charge, procédez comme suit :

1. Mettez à jour votre configuration DNS pour diriger votre trafic directement vers l'équilibreur de charge.

2. Supprimez l'équilibreur de charge de l'accélérateur. Pour de plus amples informations, veuillez consulterPour supprimer un point de terminaisonin[Ajout, modification ou suppression d'un point de terminaison standard](#).
3. Supprime l'accélérateur. Pour plus d'informations, consultez [Suppression d'un accélérateur](#).

Utilisation d'adresses IP statiques globales au lieu d'adresses IP statiques régionales

Si vous souhaitez utiliser une adresse IP statique devant une ressource AWS, telle qu'une instance Amazon EC2, vous disposez de plusieurs options. Par exemple, vous pouvez allouer une adresse IP Elastic, qui est une adresse IPv4 statique que vous pouvez associer à une instance Amazon EC2 ou une interface réseau dans une seule région AWS.

Si vous avez une audience mondiale, vous pouvez créer un accélérateur avec Global Accelerator pour obtenir deux adresses IP statiques globales qui sont annoncées à partir d'emplacements périphériques AWS dans le monde entier. Si vous disposez déjà de ressources AWS configurées pour vos applications, dans une ou plusieurs régions, y compris les instances Amazon EC2, les équilibreurs de charge réseau et les équilibreurs de charge d'application, vous pouvez facilement les ajouter à Global Accelerator pour les confronter avec des adresses IP statiques globales.

Choisir d'utiliser des adresses IP statiques globales provisionnées par Global Accelerator peut également améliorer la disponibilité et les performances de vos applications. Avec Global Accelerator, les adresses IP statiques acceptent le trafic entrant sur le réseau global AWS à partir de l'emplacement périphérique le plus proche de vos utilisateurs. Optimiser la durée du trafic sur le réseau AWS peut offrir une expérience client plus rapide et meilleure. Pour plus d'informations, consultez [Fonctionnement AWS Global Accelerator](#).

Vous pouvez ajouter un accélérateur à partir d'AWS Management Console ou à l'aide d'opérations API avec l'interface de ligne de commande AWS ou les kits SDK. Pour plus d'informations, consultez [Création ou mise à jour d'un accélérateur standard](#).

Notez les points suivants lorsque vous ajoutez un accélérateur :

- Les adresses IP statiques globales provisionnées par Global Accelerator vous restent assignées tant que votre accélérateur existe, même si vous désactivez l'accélérateur et qu'il n'accepte plus ni achemine le trafic. Toutefois, si vous supprimez un accélérateur, vous perdez les adresses IP statiques qui lui sont assignées. Pour plus d'informations, consultez [Suppression d'un accélérateur](#).

- Avec Global Accelerator, vous ne payez que ce que vous utilisez. Vous êtes facturé à un tarif horaire et aux frais de transfert de données pour chaque accélérateur de votre compte. Pour de plus amples informations, veuillez consulterTarification AWS Global Accelerator.

Écouteurs pour les accélérateurs standard dans AWS Global Accelerator

Avec AWS Global Accelerator, vous ajoutez des écouteurs qui traitent les connexions entrantes à partir de clients en fonction des ports et des protocoles que vous spécifiez. Les écouteurs prennent en charge les protocoles TCP, UDP ou TCP et UDP.

Vous définissez un écouteur standard lorsque vous créez votre accélérateur standard et vous pouvez ajouter des écouteurs supplémentaires à tout moment. Vous associez chaque écouteur à un ou plusieurs groupes de points de terminaison et vous associez chaque groupe de points de terminaison à une région AWS.

Rubriques

- Ajout, modification ou suppression d'un écouteur standard
- Affinité du client

Ajout, modification ou suppression d'un écouteur standard

Cette section explique comment utiliser les écouteurs sur la console AWS Global Accelerator. Pour effectuer ces tâches à l'aide d'une opération API au lieu de la console, consultez`CreateListener`,`UpdateListener`, et`DeleteListener`dans leRéférence de l'API AWS Global Accelerator.

Pour ajouter un écouteur

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. Choisissez Ajouter un écouteur.
4. Dans la pageAjout d'écouteur, entrez les ports ou plages de ports que vous souhaitez associer au processus d'écoute. Les écouteurs prennent en charge les ports 1 à 65535.
5. Choisissez le protocole pour les ports que vous avez entrés.

6. Le cas échéant, choisissez d'activer l'affinité du client. L'affinité client pour un écouteur signifie que Global Accelerator garantit que les connexions à partir d'une adresse IP source (client) spécifique sont toujours acheminées vers le même point de terminaison. Pour activer ce comportement, dans la liste déroulante, choisissezIP Source.

   La valeur par défaut estAucun, ce qui signifie que l'affinité du client n'est pas activée et que Global Accelerator distribue le trafic de manière égale entre les points de terminaison des groupes de points de terminaison pour l'écouteur.

   Pour plus d'informations, consultez Affinité du client.
7. Choisissez Ajouter un écouteur.

Pour modifier un écouteur standard

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. Choisissez un écouteur, puis puisModifier le écouteur.
4. Dans la pageModifier le écouteur, modifiez les ports, plages de ports ou protocoles que vous souhaitez associer au processus d'écoute.
5. Le cas échéant, choisissez d'activer l'affinité du client. L'affinité client pour un écouteur signifie que Global Accelerator garantit que les connexions à partir d'une adresse IP source (client) spécifique sont toujours acheminées vers le même point de terminaison. Pour activer ce comportement, dans la liste déroulante, choisissezIP Source.

   La valeur par défaut estAucun, ce qui signifie que l'affinité du client n'est pas activée et que Global Accelerator distribue le trafic de manière égale entre les points de terminaison des groupes de points de terminaison pour l'écouteur.

   Pour plus d'informations, consultez Affinité du client.
6. Choisissez Enregistrer.

Pour supprimer un écouteur

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. Choisissez un écouteur, puis puisSupprimez.

4. Dans la boîte de dialogue de confirmation, choisissezSupprimez.

Affinité du client

Si vous avez des applications avec état que vous utilisez avec un accélérateur standard, vous pouvez choisir que Global Accelerator dirige toutes les demandes d'un utilisateur à une adresse IP source (client) spécifique vers la même ressource de point de terminaison, afin de maintenir l'affinité du client.

Par défaut, l'affinité client pour un écouteur standard est définie surAucunet Global Accelerator distribuent le trafic de manière égale entre les points de terminaison des groupes de points de terminaison pour l'écouteur.

Global Accelerator utilise un algorithme de hachage à flux cohérent pour choisir le point de terminaison optimal pour la connexion d'un utilisateur. Si vous configurez l'affinité du client pour que votre ressource Global Accelerator soitAucun, Global Accelerator utilise les propriétés 5 tuples (adresse IP source, port source, adresse IP de destination, port de destination et protocole) pour sélectionner la valeur de hachage. Ensuite, il choisit le point de terminaison qui offre les meilleures performances. Si un client donné utilise des ports différents pour se connecter à Global Accelerator et que vous avez spécifié ce paramètre, Global Accelerator ne peut pas garantir que les connexions du client sont toujours acheminées vers le même point de terminaison.

Si vous souhaitez conserver l'affinité du client en acheminant un utilisateur spécifique (identifié par son adresse IP source) vers le même point de terminaison chaque fois qu'il se connecte, définissez l'affinité du client surIP Source. Lorsque vous spécifiez cette option, Global Accelerator utilise les propriétés 2 tuples (adresse IP source et adresse de destination) pour sélectionner la valeur de hachage et acheminer l'utilisateur vers le même point de terminaison chaque fois qu'il se connecte. Global Accelerator honore l'affinité du client après le groupe de points de terminaison que vous sélectionnez.

Groupes de points de terminaison pour les accélérateurs standard dans AWS Global Accelerator

Un groupe de points de terminaison achemine les demandes vers un ou plusieurs points de terminaison enregistrés dans AWS Global Accelerator. Lorsque vous ajoutez un écouteur dans un accélérateur standard, vous spécifiez les groupes de points de terminaison vers lesquels Global Accelerator doit diriger le trafic. Un groupe de points de terminaison et tous les points de terminaison

qu'il contient doivent se trouver dans une seule région AWS. Vous pouvez ajouter différents groupes de points de terminaison à des fins différentes, par exemple pour les tests de déploiement bleu/vert.

Global Accelerator dirige le trafic vers les groupes de points de terminaison dans les accélérateurs standard en fonction de l'emplacement du client et de l'intégrité du groupe de points de terminaison. Si vous le souhaitez, vous pouvez également définir le pourcentage de trafic à envoyer vers un groupe de points de terminaison. Pour ce faire, utilisez la numérotation de trafic pour augmenter ou réduire le trafic vers le groupe. Le pourcentage est appliqué uniquement au trafic que Global Accelerator dirige déjà vers le groupe de points de terminaison, et pas à tout le trafic qui arrive à un écouteur.

Vous pouvez définir les paramètres de vérification de l'état pour Global Accelerator pour chaque groupe de points de terminaison. En mettant à jour les paramètres de vérification de l'état, vous pouvez modifier vos exigences en matière d'interrogation et de vérification de l'intégrité des points de terminaison d'instance Amazon EC2 et d'adresse IP Elastic. Pour les points de terminaison de l'Network Load Balancer et de l'équilibreur de charge d'application, configurez les paramètres de vérification de l'état sur la console Elastic

Global Accelerator surveille en permanence l'état de tous les points de terminaison inclus dans un groupe de points de terminaison standard et achemine les demandes uniquement vers les points de terminaison actifs qui sont sains. S'il n'y a pas de points de terminaison sains vers lesquels acheminer le trafic, Global Accelerator achemine les demandes vers tous les points de terminaison.

Cette section explique comment utiliser les groupes de points de terminaison pour les accélérateurs standard sur la console AWS Global Accelerator. Si vous souhaitez utiliser des opérations d'API avec AWS Global Accelerator, consultez le documentRéférence de l'API AWS Global Accelerator.

Rubriques

Ajout, modification ou suppression d'un groupe de points de terminaison standard

Vous travaillez avec des groupes de points de terminaison sur la console AWS Global Accelerator ou à l'aide d'une opération d'API. Vous pouvez ajouter ou supprimer des points de terminaison d'un groupe de points de terminaison à tout moment.

Cette section décrit comment utiliser les groupes de points de terminaison standard sur la console AWS Global Accelerator. Si vous voulez utiliser des opérations d'API avec Global Accelerator, consultez le documentRéférence de l'API AWS Global Accelerator.

Pour ajouter un groupe de points de terminaison standard

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. DansÉcouteursSection, pourID d'écoute, choisissez l'ID du processus d'écoute auquel vous souhaitez ajouter un groupe de points de terminaison.
4. ChoisissezAjouter un groupe de points de termin.
5. Dans la section correspondant à un processus d'écoute, spécifiez une région pour le groupe de points de terminaison en sélectionnant une région dans la liste déroulante.
6. Facultatif, pourCadran de trafic, entrez un nombre compris entre 0 et 100 pour définir un pourcentage de trafic pour ce groupe de points de terminaison. Le pourcentage est appliqué uniquement au trafic qui est déjà dirigé vers ce groupe de points de terminaison, et non à l'ensemble du trafic d'écoute. Par défaut, la numérotation de trafic est définie sur 100.
7. Le cas échéant, pour remplacer le port d'écoute utilisé pour acheminer le trafic vers les points de terminaison et réacheminer le trafic vers des ports spécifiques sur vos points de terminaison, choisissezConfigurer les remplacements de port. Pour plus d'informations, consultez Remplacements de ports.
8. Si vous le souhaitez, pour spécifier des valeurs de contrôle d'intégrité personnalisées à appliquer aux points de terminaison d'instance EC2 et d'adresse IP Elastic, choisissezConfigurer les vérifications de l'état. Pour plus d'informations, consultez Health check options (Options de vérification de l'état).
9. Choisissez éventuellementAjouter un groupe de points de terminPour ajouter des groupes de points de terminaison supplémentaires pour cet écouteur ou d'autres écouteurs.
10. ChoisissezAjouter un groupe de points de termin.

Pour modifier un groupe de points de terminaison

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. DansÉcouteursSection, pourID d'écoute, choisissez l'ID du processus d'écoute auquel le groupe de points de terminaison est associé.
4. ChoisissezModification du groupe de points de termin.
5. Dans la pageModification du groupe de points de termin, modifiez la Région, ajustez le pourcentage de numérotation du trafic ou choisissezConfigurer les vérifications de l'étatPour modifier les paramètres de vérification de l'état.
6. Choisissez Enregistrer.

Pour supprimer un groupe de points de terminaison standard

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. DansÉcouteursSection, choisissez un écouteur, puis choisissezSupprimez.
4. DansGroupes de points de terminaisonSection, choisissez un groupe de points de terminaison, puis choisissezSupprimez.
5. Dans la boîte de dialogue de confirmation, choisissezSupprimez.

Réglage du flux de trafic avec les cadrans de trafic

Pour chaque groupe de points de terminaison standard, vous pouvez définir une numérotation de trafic pour contrôler le pourcentage de trafic qui est dirigé vers le groupe. Le pourcentage est appliqué uniquement au trafic qui est déjà dirigé vers le groupe de points de terminaison, et non à tout le trafic d'écoute.

Par défaut, la numérotation de trafic est définie sur 100 (c'est-à-dire 100 %) pour tous les groupes de points de terminaison régionaux dans un accélérateur. La molette de trafic vous permet d'effectuer facilement des tests de performances ou des tests de déploiement bleu/vert pour les nouvelles versions dans différentes régions AWS, par exemple.

Voici quelques exemples pour illustrer comment utiliser les cadrans de trafic pour modifier le flux de trafic en groupes de points de terminaison.

Mettre à niveau votre application par région

Si vous souhaitez mettre à niveau une application dans une région ou effectuer la maintenance, définissez d'abord la numérotation de trafic sur 0 pour couper le trafic de la région. Lorsque vous terminez le travail et que vous êtes prêt à remettre la région en service, réglez la numérotation de trafic à 100 pour composer le trafic de retour.

Mélanger le trafic entre deux régions

Cet exemple montre comment fonctionne le flux de trafic lorsque vous modifiez simultanément les cadrans de trafic pour deux groupes de points de terminaison régionaux. Supposons que vous disposez de deux groupes de points de terminaison pour votre accélérateur, l'un pour le`us-west-2`Région et une pour la`us-east-1`région : vous avez défini les cadrans de trafic à 50 % pour chaque groupe de points de terminaison.

Maintenant, disons que vous avez 100 demandes à venir à votre accélérateur, dont 50 de la côte Est des États-Unis et 50 de la côte Ouest. L'accélérateur dirige le trafic comme suit :

- Les 25 premières demandes sur chaque côte (50 demandes au total) sont traitées à partir de leur groupe de points de terminaison à proximité. Autrement dit, 25 demandes sont dirigées vers le groupe de points de terminaison dans`us-west-2`et 25 sont dirigés vers le groupe de points de terminaison dans`us-east-1`.
- Les 50 prochaines demandes sont adressées aux régions opposées. Autrement dit, les 25 prochaines demandes de la côte Est sont desservies par`us-west-2`, et les 25 prochaines demandes de la côte ouest sont desservies par`us-east-1`.

Le résultat dans ce scénario est que les deux groupes de points de terminaison servent la même quantité de trafic. Cependant, chacune reçoit un mélange de trafic des deux régions.

Remplacements de ports

Par défaut, un accélérateur achemine le trafic utilisateur vers les points de terminaison dans les régions AWS à l'aide des plages de protocole et de ports que vous spécifiez lorsque vous créez un écouteur. Par exemple, si vous définissez un écouteur qui accepte le trafic TCP sur les ports 80 et 443, l'accélérateur achemine le trafic vers ces ports sur un point de terminaison.

Toutefois, lorsque vous ajoutez ou mettez à jour un groupe de points de terminaison, vous pouvez remplacer le port d'écoute utilisé pour acheminer le trafic vers les points de terminaison. Par exemple, vous pouvez créer un remplacement de port dans lequel l'écouteur reçoit le trafic utilisateur

sur les ports 80 et 443, mais pour lequel votre accélérateur achemine ce trafic vers les ports 1080 et 1443, respectivement, sur les points de terminaison.

Les remplacements de ports peuvent vous aider à éviter les problèmes d'écoute sur les ports restreints. Il est plus sûr d'exécuter des applications qui ne nécessitent pas de privilèges de superutilisateur (root) sur vos terminaux. Toutefois, sous Linux et d'autres systèmes de type Unix, vous devez disposer des privilèges de superutilisateur pour écouter sur les ports restreints (ports TCP ou UDP inférieurs à 1024). En mappant un port restreint d'un écouteur à un port non restreint sur un point de terminaison, les remplacements de port vous permettent d'éviter ce problème. Vous pouvez accepter le trafic sur les ports restreints lors de l'exécution d'applications sans accès root sur vos terminaux derrière Global Accelerator. Par exemple, vous pouvez remplacer un port d'écoute 443 sur un port de point de terminaison 8443.

Pour chaque remplacement de port, vous spécifiez un port d'écoute qui accepte le trafic des utilisateurs et le port de point de terminaison vers lequel Global Accelerator acheminera ce trafic. Pour plus d'informations, consultez Ajout, modification ou suppression d'un groupe de points de terminaison standard.

Lorsque vous créez une substitution de port, gardez les éléments suivants à l'esprit.

- Les ports de point de terminaison ne peuvent pas chevaucher les plages de ports d'écoute. Les ports de point de terminaison que vous spécifiez dans un remplacement de port ne peuvent pas être inclus dans aucune des plages de ports d'écoute que vous avez configurées pour l'accélérateur. Par exemple, imaginez que vous avez deux écouteurs pour un accélérateur et que vous avez défini les plages de ports pour ces écouteurs comme 100-199 et 200-299, respectivement. Lorsque vous créez des remplacements de port, vous ne pouvez pas en définir un du port d'écoute 100 au port 210 du point de terminaison, par exemple, car le port de point de terminaison (210) est inclus dans une plage de ports d'écoute que vous avez définie (200-299).
- Pas de ports de point de terminaison dupliqués. Si un remplacement de port dans un accélérateur spécifie un port de point de terminaison, vous ne pouvez pas spécifier le même port de point de terminaison avec remplacement de port à partir d'un autre port d'écoute. Par exemple, vous ne pouvez pas spécifier un remplacement de port du port d'écoute 80 vers le port 90 du point de terminaison ainsi qu'un remplacement du port d'écoute 81 au port 90 du point de terminaison.
- La vérification Health continue d'utiliser le port d'origine. Si vous spécifiez un remplacement de port pour un port configuré en tant que port de vérification de l'état, la vérification de l'état utilise toujours le port d'origine, et non le port de remplacement. Par exemple, supposons que vous spécifiez des contrôles d'intégrité sur le port d'écoute 80 et que vous spécifiez également un remplacement de port du port d'écoute 80 vers le port 480 du point de terminaison. Les Health

l'état continuent d'utiliser le port 80 du point de terminaison. Toutefois, le trafic utilisateur qui passe par le port 80 va au port 480 sur le point de terminaison.

Ce comportement maintient la cohérence entre l'équilibreur de charge réseau, l'équilibreur de charge d'application, l'instance EC2 et les points de terminaison d'adresse IP Elastic. Étant donné que les équilibreurs de charge réseau et les équilibreurs de charge d'application ne mappent pas les ports de vérification de l'état à un autre port de point de terminaison lorsque vous spécifiez un remplacement de port dans Global Accelerator, il serait incohérent pour Global Accelerator de mapper les ports de vérification de l'état vers différents ports de point de terminaison pour l'instance EC2 et Elastic IP points de terminaison d'adresse.

- Les paramètres du groupe de sécurité doivent autoriser l'accès au port. Assurez-vous que vos groupes de sécurité autorisent l'arrivée du trafic aux ports de point de terminaison que vous avez désignés dans les remplacements de ports. Par exemple, si vous remplacez le port d'écoute 443 vers le port 1433 du point de terminaison, assurez-vous que toutes les restrictions de port définies dans votre groupe de sécurité pour cet Application Load Balancer ou le point de terminaison Amazon EC2 autorisent le trafic entrant sur le port 1433.

Health check options (Options de vérification de l'état)

AWS Global Accelerator envoie régulièrement des demandes aux points de terminaison standard pour tester leur état. Ces vérifications de l'état s'exécutent automatiquement. Les conseils pour déterminer l'intégrité de chaque point de terminaison et le calendrier des vérifications d'intégrité dépendent du type de ressource de point de terminaison.

> **Important**
>
> Global Accelerator requiert que vos règles de routeur et de pare-feu autorisent le trafic entrant à partir des adresses IP associées aux vérificateurs d'intégrité de Route 53 pour effectuer des vérifications d'intégrité pour les points de terminaison d'instance EC2 ou d'adresse IP Elastic. Vous trouverez des informations sur les plages d'adresses IP associées aux vérificateurs d'état Amazon Route 53 dansVérifications de l'état de vos groupes cibledans leGuide du développeur Amazon Route 53.

Vous pouvez configurer les options de vérification de l'état suivantes pour un groupe de points de terminaison. Si vous spécifiez des options de vérification de l'état, Global Accelerator utilise les

paramètres pour les vérifications d'intégrité d'instance EC2 ou d'adresse IP Elastic, mais pas pour les équilibreurs de charge réseau ou les équilibreurs de charge d'application.

- Pour les points de terminaison de l'équilibreur de charge d'application ou de l'équilibreur de charge réseau, vous configurez les vérifications de l'intégrité des ressources à l'aide des options de configuration Elastic Load Balancing Pour de plus amples informations, veuillez consulterVérifications de l'état de vos groupes cible. Les options de vérification de l'Health que vous choisissez dans Global Accelerator n'affectent pas les équilibreurs de charge d'application ou les équilibreurs de charge réseau que vous avez ajoutés en tant que points de terminaison.

  > **Note**
  >
  > Lorsque vous disposez d'un équilibreur de charge d'application ou d'un Network Load Balancer qui inclut plusieurs groupes cibles, Global Accelerator considère que le point de terminaison de l'équilibreur de charge est sain uniquement siEACHderrière l'équilibreur de charge a au moins une cible saine. Si un seul groupe cible pour l'équilibreur de charge n'a que des cibles insalubres, Global Accelerator considère que le point de terminaison est défectueux.

- Pour les points de terminaison d'instance EC2 ou d'adresse IP Elastic qui sont ajoutés à un écouteur configuré avec TCP, vous pouvez spécifier le port à utiliser pour les vérifications d'intégrité. Par défaut, si vous ne spécifiez pas de port pour les vérifications d'intégrité, Global Accelerator utilise le port d'écoute que vous avez spécifié pour votre accélérateur.
- Pour les points de terminaison d'instance EC2 ou d'adresse IP Elastic avec des écouteurs UDP, Global Accelerator utilise le port d'écoute et le protocole TCP pour les vérifications d'intégrité. Vous devez donc disposer d'un serveur TCP sur votre point de terminaison.

  > **Note**
  >
  > Assurez-vous de vérifier que le port que vous avez configuré pour le serveur TCP sur chaque point de terminaison est le même que le port que vous spécifiez pour la vérification de l'état dans Global Accelerator. Si les numéros de port ne sont pas les mêmes, ou si vous n'avez pas configuré de serveur TCP pour le point de terminaison, Global Accelerator marque le point de terminaison comme étant défectueux, quel que soit l'état du point de terminaison.

Port Health vérification de l'état

Port à utiliser lorsque Global Accelerator effectue des vérifications de l'état sur les points de terminaison faisant partie de ce groupe de points de terminaison.

> **Note**
>
> Vous ne pouvez pas définir de remplacement de port pour les ports de vérification de l'état.

Health check protocol (Protocole de vérification de l'état)

Protocole à utiliser lorsque Global Accelerator effectue des vérifications de l'état sur les points de terminaison faisant partie de ce groupe de points de terminaison.

InterHealth le de vérification de

Intervalle, en secondes, entre chaque vérification de l'état pour un point de terminaison.

Nombre de seuils

Le nombre de vérifications consécutives de l'état à partir duquel une cible défectueuse est considérée comme saine ou comme défectueuse.

Chaque écouteur achemine les demandes uniquement vers des points de terminaison sains. Après avoir ajouté un point de terminaison, il doit passer avec succès une vérification de l'état pour être considéré comme sain. Une fois que toutes les vérifications de l'état sont terminées, l'écouteur ferme la connexion qui a été établie pour la vérification de l'état.

Points de terminaison pour les accélérateurs standard dans AWS Global Accelerator

Les points de terminaison pour les accélérateurs standard dans AWS Global Accelerator peuvent être des équilibreurs de charge réseau, des équilibreurs de charge d'application, des instances Amazon EC2 ou des adresses IP Elastic. Avec des accélérateurs standard, une adresse IP statique sert de point de contact unique pour les clients et Global Accelerator répartit ensuite le trafic entrant sur des points de terminaison sains. Global Accelerator dirige le trafic vers les points de terminaison à l'aide

du port (ou plage de ports) que vous spécifiez pour l'écouteur auquel appartient le groupe de points de terminaison pour le point de terminaison.

Chaque groupe de points de terminaison peut avoir plusieurs points de terminaison. Vous pouvez ajouter chaque point de terminaison à plusieurs groupes de points de terminaison, mais les groupes de points de terminaison doivent être associés à différents écouteurs. Une ressource doit être valide et active lorsque vous l'ajoutez en tant que point de terminaison.

Global Accelerator surveille en permanence l'état de tous les points de terminaison inclus dans un groupe de points de terminaison standard. Il achemine le trafic uniquement vers les points de terminaison actifs qui sont sains. Si Global Accelerator ne dispose pas de points de terminaison sains vers lesquels acheminer le trafic, il achemine le trafic vers tous les points de terminaison.

Soyez conscient des points suivants pour des types spécifiques de points de terminaison standard Global Accelerator :

Points de terminaison d'équilibrage de charge

- Un point de terminaison d'Application Load Balancer peut être connecté à Internet ou interne. Un point de terminaison de l'équilibreur de charge réseau doit être connecté à Internet.

Points de terminaison d'instance Amazon EC2

- Un point de terminaison d'instance EC2 (pour les accélérateurs de routage standard et personnalisés) ne peut pas être l'un des types suivants : C1, CC1, CC2, CG1, CG1, CG2, CG2, CG2, CG1, G2, HI1, HS1, M1, M2, M3 ou T1.
- Les instances EC2 sont prises en charge en tant que points de terminaison dans certaines régions AWS uniquement. Pour obtenir une liste des régions prises en charge, consultez Régions AWS prises en charge pour la préservation des adresses IP des clients.
- Nous vous recommandons de supprimer une instance EC2 des groupes de points de terminaison Global Accelerator avant de mettre fin à l'instance. Si vous mettez fin à une instance EC2 avant de la supprimer d'un groupe de points de terminaison dans Global Accelerator, puis que vous créez une autre instance dans le même VPC avec la même adresse IP privée et que les vérifications d'intégrité passent, Global Accelerator achemine le trafic vers le nouveau point de terminaison.

Rubriques

- Ajout de points de terminaison avec préservation de l'adresse IP client
- Transition des points de terminaison pour utiliser la préservation des adresses IP du client

Ajout, modification ou suppression d'un point de terminaison standard

Vous ajoutez des points de terminaison aux groupes de points de terminaison afin que le trafic puisse être dirigé vers vos ressources. Vous pouvez modifier un point de terminaison standard pour modifier le poids du point de terminaison. Vous pouvez également supprimer un point de terminaison de votre accélérateur en le supprimant d'un groupe de points de terminaison. La suppression d'un point de terminaison n'affecte pas le point de terminaison lui-même, mais Global Accelerator ne peut plus diriger le trafic vers cette ressource.

Les points de terminaison dans Global Accelerator peuvent être des équilibreurs de charge réseau, des équilibreurs de charge d'application, des instances Amazon EC2 ou des adresses IP Elastic. Vous devez d'abord créer une de ces ressources, puis vous pouvez l'ajouter en tant que point de terminaison dans Global Accelerator. Une ressource doit être valide et active lorsque vous l'ajoutez en tant que point de terminaison.

Vous pouvez ajouter ou supprimer des points de terminaison des groupes de points de terminaison en fonction de l'utilisation. Par exemple, si la demande de votre application augmente, vous pouvez créer plus de ressources, puis ajouter d'autres points de terminaison à un ou plusieurs groupes de points de terminaison pour gérer l'augmentation du trafic. Global Accelerator commence à acheminer les demandes vers le point de terminaison dès que vous l'ajoutez et que le point de terminaison a passé avec succès les vérifications de l'état initiales. Vous pouvez gérer le trafic vers les points de terminaison en ajustant les pondérations sur un point de terminaison, afin d'envoyer proportionnellement plus ou moins de trafic vers le point de terminaison.

Si vous ajoutez un point de terminaison avec la préservation de l'adresse IP du client, consultez d'abord les informations dansRégions AWS prises en charge pour la préservation des adresses IP des clientsandConserver les adresses IP des clients dans AWS Global Accelerator.

Vous pouvez supprimer des points de terminaison de vos groupes de points de terminaison, par exemple, si vous avez besoin de desservir vos points de terminaison. La suppression d'un point de terminaison le retire du groupe de points de terminaison, mais n'affecte pas autrement le point de terminaison. Global Accelerator cesse de diriger le trafic vers un point de terminaison dès que vous le supprimez d'un groupe de points de terminaison. Le point de terminaison passe dans un état où il attend que toutes les demandes en cours soient terminées, de sorte qu'il n'y ait pas d'interruption

pour le trafic client en cours. Vous pouvez ajouter le point de terminaison au groupe de points de terminaison lorsque vous êtes prêt à reprendre la réception des demandes.

Cette section explique comment utiliser les points de terminaison sur la console AWS Global Accelerator. Si vous souhaitez utiliser des opérations d'API avec AWS Global Accelerator, consultez le documentRéférence d'API AWS Global Accelerator.

Pour ajouter un point de terminaison standard

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. DansÉcouteursSection, pourID de l'écouteur, choisissez l'ID d'un écouteur.
4. DansGroupes de point de terminaisonSection, pourID de groupe de points de termin, choisissez l'ID du groupe de points de terminaison auquel vous souhaitez ajouter un point de terminaison.
5. DansPoints de terminaisonSection, choisissezAjouter un point de terminaison.
6. Dans la pageAjouter des points de terminaison, choisissez une ressource dans la liste déroulante.

   Si vous ne disposez pas de ressources AWS, il n'y a pas d'éléments dans la liste. Pour continuer, créez des ressources AWS telles que des équilibreurs de charge, des instances Amazon EC2 ou des adresses IP Elastic. Revenez ensuite aux étapes ici et choisissez une ressource dans la liste.
7. Facultatif, pourPoids, entrez un nombre compris entre 0 et 255 pour définir une pondération pour le trafic de routage vers ce point de terminaison. Lorsque vous ajoutez des poids aux points de terminaison, vous configurez Global Accelerator pour acheminer le trafic dans les proportions que vous spécifiez. Par défaut, tous les points de terminaison ont un poids de 128. Pour plus d'informations, consultez Pondérations des points de.
8. Vous pouvez éventuellement activer la préservation de l'adresse IP du client pour un point de terminaison d'Application Load Balancer accessible sur Internet. UNDERPréserver l'adresse IP du client, sélectionnezPréserver l'adresse.

   Cette option est toujours sélectionnée pour l'Application Load Balancer interne et les points de terminaison d'instance EC2, et jamais sélectionnée pour les points de terminaison Network Load Balancer et Elastic IP Address. Pour plus d'informations, consultez Conserver les adresses IP des clients dans AWS Global Accelerator.

> **Note**
>
> Avant d'ajouter et de commencer à acheminer le trafic vers des points de terminaison qui conservent l'adresse IP du client, assurez-vous que toutes les configurations de sécurité requises, par exemple les groupes de sécurité, sont mises à jour pour inclure l'adresse IP du client utilisateur dans les listes autorisées.

9. Choisir Add endpoint (Ajouter un point de terminaison).

Pour modifier un point de terminaison standard

Vous pouvez modifier une configuration de point de terminaison pour modifier la pondération. Pour plus d'informations, consultez Pondérations des points de.

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. DansÉcouteursSection, pourID de l'écouteur, choisissez l'ID d'un écouteur.
4. DansGroupes de point de terminaisonSection, pourID de groupe de points de termin, choisissez l'ID du groupe de points de terminaison.
5. ChoisissezModification du point de terminaison.
6. Dans la pageModification du point de terminaison, effectuez des mises à jour et choisissezEnregistrer.

Pour supprimer un point de terminaison

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. DansÉcouteursSection, pourID de l'écouteur, choisissez l'ID d'un écouteur.
4. DansGroupes de point de terminaisonSection, pourID de groupe de points de termin, choisissez l'ID du groupe de points de terminaison.
5. ChoisissezSupprimer le point de terminaison.
6. Dans la boîte de dialogue de confirmation, choisissezSupprimez.

Pondérations des points de

Une pondération est une valeur qui détermine la proportion de trafic que Global Accelerator dirige vers un point de terminaison dans un accélérateur standard. Les points de terminaison peuvent être des équilibreurs de charge réseau, des équilibreurs de charge d'application, des instances Amazon EC2 ou des adresses IP élastiques. Global Accelerator calcule la somme des pondérations des points de terminaison d'un groupe de points de terminaison, puis dirige le trafic vers les points de terminaison en fonction du rapport entre le poids de chaque point de terminaison et le total.

Le routage pondéré vous permet de choisir la quantité de trafic acheminée vers une ressource dans un groupe de points de terminaison. Cela peut vous être utile de plusieurs façons, notamment l'équilibrage de charge et le test de nouvelles versions d'une application.

Fonctionnement des pondérations des points de terminaison

Pour utiliser des pondérations, vous attribuez à chaque point de terminaison dans un groupe de points de terminaison une pondération relative correspondant au volume de trafic que vous souhaitez lui envoyer. Par défaut, le poids d'un point de terminaison est 128, c'est-à-dire la moitié de la valeur maximale d'un poids, 255. Global Accelerator envoie le trafic vers un point de terminaison en fonction de la pondération attribuée à ce point par rapport au poids total des points de terminaison dans le groupe :

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

Par exemple, si vous souhaitez envoyer une petite partie de votre trafic vers un point de terminaison et que le reste soit acheminé vers un autre point de terminaison, vous pouvez spécifier des pondérations de 1 à 255. Le point de terminaison ayant une pondération de 1 obtient 1/256 du trafic (1/1+255) et l'autre point de terminaison obtient 255/256 (255/1+255). Vous pouvez progressivement modifier l'équilibre en changeant les pondérations. Si vous voulez que Global Accelerator cesse d'envoyer du trafic vers un point de terminaison, vous pouvez passer la pondération de cette ressource à 0.

Basculement sur incident pour les terminaux non sains

S'il n'y a pas de points de terminaison sains dans un groupe de points de terminaison dont la pondération est supérieure à zéro, Global Accelerator tente de basculer vers un point de terminaison sain dont la pondération est supérieure à zéro dans un autre groupe de points de terminaison. Pour ce basculement, Global Accelerator ignore le paramètre de numérotation du trafic. Ainsi, si, par

exemple, un groupe de points de terminaison a une numérotation de trafic définie sur zéro, Global Accelerator inclut toujours ce groupe de points de terminaison dans la tentative de basculement.

Si Global Accelerator ne trouve pas de point de terminaison sain avec une pondération supérieure à zéro après avoir essayé trois groupes de points de terminaison supplémentaires (c'est-à-dire trois régions AWS), il achemine le trafic vers un point de terminaison aléatoire dans le groupe de points de terminaison le plus proche du client. C'est, ilÉchec d'ouverture.

Remarques :

- Le groupe de points de terminaison choisi pour le basculement peut être un groupe dont la numérotation de trafic est définie à zéro.
- Le groupe de points de terminaison le plus proche peut ne pas être le groupe de points de terminaison original. En effet, Global Accelerator prend en compte les paramètres de numérotation de trafic de compte lorsqu'il choisit le groupe de points de terminaison d'origine.

Par exemple, supposons que votre configuration comporte deux points de terminaison, l'un sain et l'autre malsain, et que vous avez défini le poids de chacun d'entre eux sur une valeur supérieure à zéro. Dans ce cas, Global Accelerator achemine le trafic vers le point de terminaison sain. Cependant, dites maintenant que vous définissez le poids du seul point de terminaison sain sur zéro. Global Accelerator tente ensuite trois groupes de points de terminaison supplémentaires pour trouver un point de terminaison sain avec un poids supérieur à zéro. S'il n'en trouve pas, Global Accelerator achemine le trafic vers un point de terminaison aléatoire dans le groupe de points de terminaison le plus proche du client.

Ajout de points de terminaison avec préservation de l'adresse IP client

Une fonctionnalité que vous pouvez utiliser avec certains types de point de terminaison (dans certaines régions) estPréservation d'adresses IP du client. Avec cette fonctionnalité, vous préservez l'adresse IP source du client d'origine pour les paquets qui arrivent au point de terminaison. Vous pouvez utiliser cette fonctionnalité avec l'Application Load Balancer et les points de terminaison d'instance Amazon EC2. Les points de terminaison des accélérateurs de routage personnalisés ont toujours l'adresse IP du client conservée. Pour plus d'informations, consultez Conserver les adresses IP des clients dans AWS Global Accelerator.

Si vous avez l'intention d'utiliser la fonctionnalité de conservation des adresses IP du client, prenez en compte les points suivants lorsque vous ajoutez des points de terminaison à Global Accelerator :

Interfaces réseau Elastic

Pour prendre en charge la préservation des adresses IP des clients, Global Accelerator crée des interfaces réseau élastiques dans votre compte AWS, une pour chaque sous-réseau où un point de terminaison est présent. Pour plus d'informations sur le fonctionnement de Global Accelerator avec les interfaces réseau Elastic, consultezMeilleures pratiques pour la préservation des adresses IP des clients.

Points de terminaison dans les sous-réseaux privés

Vous pouvez cibler un Application Load Balancer ou une instance EC2 dans un sous-réseau privé à l'aide d'AWS Global Accelerator, mais vous devez disposer d'unPasserelle Internetattaché au VPC qui contient les points de terminaison. Pour plus d'informations, consultez Connexions VPC sécurisées dans AWS Global Accelerator.

Ajouter l'adresse IP du client à la liste autorisée

Avant d'ajouter et de commencer à acheminer le trafic vers des points de terminaison qui conservent l'adresse IP du client, assurez-vous que toutes les configurations de sécurité requises, par exemple les groupes de sécurité, sont mises à jour pour inclure l'adresse IP du client utilisateur dans la liste autorisée. Les listes de contrôle d'accès réseau (listes ACL) ne s'appliquent qu'au trafic sortant. Si vous devez filtrer le trafic entrant (entrant), vous devez utiliser des groupes de sécurité.

Configurer les listes de contrôle d'accès réseau (listes ACL)

Les listes d'accès réseau associées à vos sous-réseaux VPC s'appliquent au trafic de sortie (sortant) lorsque la préservation de l'adresse IP du client est activée sur votre accélérateur. Toutefois, pour que le trafic puisse quitter via Global Accelerator, vous devez configurer la liste ACL en tant que règle entrante et sortante.

Par exemple, pour permettre aux clients TCP et UDP utilisant un port source éphémère de se connecter à votre point de terminaison via Global Accelerator, associez le sous-réseau de votre point de terminaison à une liste ACL réseau qui autorise le trafic sortant destiné à un port TCP ou UDP éphémère (plage de ports 1024-65535, destination 0.0.0.0/0). De plus, créez une règle entrante correspondante (plage de ports 1024-65535, source 0.0.0.0/0).

> **Note**
>
> Le groupe de sécurité et les règles AWS WAF constituent un ensemble supplémentaire de fonctionnalités que vous pouvez appliquer pour protéger vos ressources. Par exemple,

les règles de groupe de sécurité entrantes associées à vos instances Amazon EC2 et aux équilibreurs de charge d'application vous permettent de contrôler les ports de destination auxquels les clients peuvent se connecter via Global Accelerator, tels que le port 80 pour HTTP ou le port 443 pour HTTPS. Notez que les groupes de sécurité d'instance Amazon EC2 s'appliquent à tout trafic qui arrive à vos instances, y compris le trafic provenant de Global Accelerator et toute adresse IP publique ou Elastic attribuée à votre instance. Il est recommandé d'utiliser des sous-réseaux privés si vous souhaitez vous assurer que le trafic est fourni uniquement par Global Accelerator. Assurez-vous également que les règles du groupe de sécurité entrant sont configurées de manière appropriée pour autoriser ou refuser correctement le trafic pour vos applications.

Transition des points de terminaison pour utiliser la préservation des adresses IP du client

Suivez les instructions de cette section pour faire passer un ou plusieurs points de terminaison de votre accélérateur vers des points de terminaison qui conservent l'adresse IP du client de l'utilisateur. Vous pouvez opter pour la transition d'un point de terminaison de l'Application Load Balancer ou d'un point de terminaison d'adresse IP Elastic vers un point de terminaison correspondant (un équilibreur de charge d'application ou une instance EC2) qui possède la préservation de l'adresse IP du client. Pour plus d'informations, consultez Conserver les adresses IP des clients dans AWS Global Accelerator.

Nous vous recommandons de passer lentement à l'utilisation de la préservation de l'adresse IP du client. Tout d'abord, ajoutez de nouveaux points de terminaison d'instance EC2 ou d'Application Load Balancer que vous activez pour conserver l'adresse IP du client. Ensuite, déplacez lentement le trafic des points de terminaison existants vers les nouveaux points de terminaison en configurant les pondérations sur les points de terminaison.

Important

Avant de commencer à acheminer le trafic vers des points de terminaison qui conservent l'adresse IP du client, assurez-vous que toutes les configurations dans lesquelles vous avez inclus les adresses IP du client Global Accelerator dans les listes autorisées sont mises à jour pour inclure l'adresse IP du client utilisateur à la place.

La préservation de l'adresse IP du client est disponible uniquement dans des régions AWS spécifiques. Pour plus d'informations, consultez Régions AWS prises en charge pour la préservation des adresses IP des clients.

Cette section explique comment utiliser les groupes de points de terminaison sur la console AWS Global Accelerator. Si vous voulez utiliser des opérations API avec Global Accelerator, consultez laRéférence d'API AWS Global Accelerator.

Après avoir déplacé une petite quantité de trafic vers le nouveau point de terminaison avec la préservation de l'adresse IP du client, testez pour vous assurer que votre configuration fonctionne comme vous le souhaitez. Augmentez ensuite progressivement la proportion de trafic vers le nouveau point de terminaison en ajustant les poids sur les points de terminaison correspondants.

Pour effectuer la transition vers des points de terminaison qui préservent les adresses IP des clients, commencez par suivre les étapes ci-dessous pour ajouter un nouveau point de terminaison et, pour les points de terminaison de l'Application Load Balancer sur Internet, activez la préservation des adresses IP du client. (L'option de conservation des adresses IP du client est toujours sélectionnée pour les équilibreurs de charge des applications internes et les instances EC2.)

Pour ajouter un point de terminaison avec la préservation de l'adresse IP du client

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. DansÉcouteursSection, choisissez un écouteur.
4. DansGroupe de points de terminaisonSection, choisissez un groupe de points de terminaison.
5. DansPoints de terminaisonSection, choisissezAjouter un point de terminaison.
6. Dans la pageAjouter des points de terminaison, dans laPoints de terminaison, choisissez un point de terminaison d'Application Load Balancer ou un point de terminaison d'instance EC2.
7. DansPoids, choisissez un nombre faible par rapport aux pondérations définies pour vos points de terminaison existants. Par exemple, si la pondération d'un Application Load Balancer correspondant est 255, vous pouvez entrer une pondération de 5 pour le nouvel équilibreur de charge d'application, pour commencer. Pour plus d'informations, consultez Pondérations des points de.
8. Pour un nouveau point de terminaison d'Application Load Balancer orienté vers l'extérieur, sousPréserver l'adresse IP du client, sélectionnezPréserver l'adresse. (Cette option est toujours sélectionnée pour les équilibreurs de charge d'application internes et les instances EC2.)
9. Sélectionnez Save Changes.

Ensuite, suivez les étapes ci-dessous pour modifier les points de terminaison existants correspondants (que vous remplacez par les nouveaux points de terminaison avec la préservation de l'adresse IP du client) afin de réduire les poids des points de terminaison existants afin de réduire le trafic vers eux.

Pour réduire le trafic des points de terminaison existants

1. Dans la pageGroupe de points de terminaison, choisissez un point de terminaison existant qui n'a pas de conservation de l'adresse IP du client.
2. Choisissez Modifier.
3. Dans la pageModification du point de terminaison, dans laPoids, entrez un nombre inférieur au nombre actuel. Par exemple, si le poids d'un point de terminaison existant est 255, vous pouvez entrer une pondération de 220 pour le nouveau point de terminaison (avec la préservation de l'adresse IP du client).
4. Sélectionnez Save Changes.

Une fois que vous avez testé une petite partie du trafic d'origine en définissant le poids du nouveau point de terminaison sur un nombre faible, vous pouvez faire passer lentement tout le trafic en continuant à ajuster les poids des points de terminaison d'origine et des nouveaux points de terminaison.

Par exemple, supposons que vous commenciez avec un Application Load Balancer existant avec une pondération définie sur 200, et que vous ajoutez un nouveau point de terminaison de l'équilibreur de charge d'application avec la préservation de l'adresse IP du client activée avec une pondération définie sur 5. Déplacez progressivement le trafic de l'équilibreur de charge d'application d'origine vers le nouvel Application Load Balancer en augmentant le poids du nouvel équilibreur de charge d'application et en diminuant le poids de l'équilibreur de charge d'application d'origine. Exemples :

- Poids d'origine 190/nouveau poids 10
- Poids d'origine 180/nouveau poids 20
- Poids original 170/nouveau poids 30, et ainsi de suite.

Lorsque vous avez réduit le poids à 0 pour le point de terminaison d'origine, tout le trafic (dans cet exemple de scénario) passe au nouveau point de terminaison de l'Application Load Balancer, qui inclut la préservation de l'adresse IP du client.

Si vous avez d'autres points de terminaison (équilibreurs de charge d'application ou instances EC2) que vous souhaitez effectuer une transition pour utiliser la préservation de l'adresse IP du client, répétez les étapes décrites dans cette section pour les faire passer.

Si vous devez rétablir votre configuration pour un point de terminaison afin que le trafic vers le point de terminaison ne conserve pas l'adresse IP du client, vous pouvez le faire à tout moment : augmenter le poids du point de terminaison quipasavoir la conservation de l'adresse IP du client à la valeur d'origine et diminuer le poids du point de terminaisonavecconservation de l'adresse IP du client à 0.

Travailler avec des accélérateurs de routage personnalisés dans AWS Global Accelerator

Ce chapitre contient des procédures et des recommandations pour la création d'accélérateurs de routage personnalisés dans AWS Global Accelerator. Un accélérateur de routage personnalisé vous permet d'utiliser la logique d'application pour mapper directement un ou plusieurs utilisateurs à une instance Amazon EC2 spécifique parmi de nombreuses destinations, tout en améliorant les performances du routage de votre trafic via Global Accelerator. Ceci est utile lorsque vous disposez d'une application qui nécessite un groupe d'utilisateurs pour interagir les uns avec les autres sur la même session exécutée sur une instance et un port EC2 spécifiques, telles que des applications de jeu ou des sessions VoIP (VoIP).

Les points de terminaison pour les accélérateurs de routage personnalisés doivent être des sous-réseaux de cloud privé virtuel (VPC), et un accélérateur de routage personnalisé peut uniquement acheminer le trafic vers des instances Amazon EC2 de ces sous-réseaux. Lorsque vous créez un accélérateur de routage personnalisé, vous pouvez inclure des milliers d'instances Amazon EC2 exécutées dans un ou plusieurs sous-réseaux VPC. Pour en savoir plus, consultez la section Fonctionnement des accélérateurs de routage personnalisés dans AWS Global Accelerator.

Si vous souhaitez que Global Accelerator choisisse automatiquement le point de terminaison sain le plus proche de vos clients, créez un accélérateur standard. Pour plus d'informations, consultez Travailler avec des accélérateurs standard dans AWS Global Accelerator.

Pour configurer l'accélérateur de routage personnalisé, procédez comme suit :

1. Passez en revue les directives et les exigences relatives à la création d'un accélérateur de routage personnalisé Voir Directives et restrictions pour les accélérateurs de routage personnalisés.
2. Créer un sous-réseau VPC Vous pouvez ajouter des instances EC2 au sous-réseau à tout moment après avoir ajouté le sous-réseau à Global Accelerator.
3. Créer un accélérateur et sélectionnez l'option d'un accélérateur de routage personnalisé
4. Ajoutez un écouteur et spécifiez une plage de ports pour que Global Accelerator puisse écouter. Assurez-vous d'inclure une large gamme avec suffisamment de ports pour que Global Accelerator puisse être mappé à toutes les destinations que vous prévoyez d'avoir. Ces ports sont distincts des ports de destination, que vous spécifiez à l'étape suivante. Pour plus d'informations sur les exigences de port d'écouteur, consultezDirectives et restrictions pour les accélérateurs de routage personnalisés.

5. Ajoutez un ou plusieurs groupes de points de terminaison pour les régions AWS dans lesquelles vous avez des sous-réseaux VPC. Pour chaque groupe de points de terminaison, procédez comme suit :
   - Plage de ports de point de terminaison, qui représente les ports sur vos instances EC2 de destination qui seront en mesure de recevoir du trafic.
   - Le protocole pour chaque plage de ports de destination : UDP, TCP, ou à la fois UDP et TCP.
6. Pour le sous-réseau de point de terminaison, sélectionnez un ID de sous-réseau. Vous pouvez ajouter plusieurs sous-réseaux dans chaque groupe de points de terminaison et les sous-réseaux peuvent avoir des tailles différentes (jusqu'à /17).

Les sections suivantes permettent d'utiliser des accélérateurs de routage, des écouteurs, des groupes de points de terminaison et des points de terminaison personnalisés.

Rubriques

Fonctionnement des accélérateurs de routage personnalisés dans AWS Global Accelerator

En utilisant un accélérateur de routage personnalisé dans AWS Global Accelerator, vous pouvez utiliser la logique d'application pour mapper directement un ou plusieurs utilisateurs vers une destination spécifique parmi de nombreuses destinations tout en profitant des avantages de performances de Global Accelerator. Un accélérateur de routage personnalisé mappe les plages de ports d'écoute aux destinations d'instance EC2 dans les sous-réseaux VPC (Virtual Private Cloud). Cela permet à Global Accelerator d'acheminer le trafic de manière déterministe vers une adresse IP privée Amazon EC2 et une destination de port spécifiques dans votre sous-réseau.

Par exemple, vous pouvez utiliser un accélérateur de routage personnalisé avec une application de jeu en ligne en temps réel dans laquelle vous affectez plusieurs joueurs à une seule session sur un serveur de jeu Amazon EC2 en fonction des facteurs que vous choisissez, tels que l'emplacement géographique, la compétence du joueur et le mode de jeu. Vous pouvez également disposer d'une application VoIP ou de médias sociaux qui affecte plusieurs utilisateurs à un serveur de médias spécifique pour les sessions de voix, de vidéo et de messagerie.

Votre application peut appeler une API Global Accelerator et recevoir un mappage statique complet des ports Global Accelerator et de leurs adresses IP de destination et ports associés. Vous pouvez enregistrer ce mappage statique, puis votre service de matchmaking l'utilise pour acheminer les utilisateurs vers des instances EC2 de destination spécifiques. Vous n'avez pas besoin d'effectuer de modifications de votre logiciel client pour commencer à utiliser Global Accelerator avec votre application.

Pour configurer un accélérateur de routage personnalisé, sélectionnez un point de terminaison de sous-réseau VPC. Ensuite, vous définissez une plage de ports de destination sur laquelle les connexions entrantes seront mappées, afin que votre logiciel puisse écouter sur le même ensemble de ports dans toutes les instances. Global Accelerator crée un mappage statique qui permet à votre service de matchmaking de traduire une adresse IP de destination et un numéro de port pour une session en une adresse IP externe et un port que vous donnez aux utilisateurs.

La pile réseau de votre application peut fonctionner sur un seul protocole de transport, ou vous pouvez utiliser UDP pour une livraison rapide et TCP pour une livraison fiable. Vous pouvez définir UDP, TCP ou UDP et TCP pour chaque plage de ports de destination, afin de vous offrir une flexibilité maximale sans devoir dupliquer votre configuration pour chaque protocole.

> **Note**
>
> Par défaut, toutes les destinations de sous-réseau VPC dans un accélérateur de routage personnalisé ne sont pas autorisées à recevoir du trafic. Ceci doit être sécurisé par défaut, et également pour vous donner un contrôle granulaire sur les destinations d'instance EC2 privées dans votre sous-réseau qui sont autorisées à recevoir du trafic. Vous pouvez autoriser ou refuser le trafic vers le sous-réseau ou vers des combinaisons d'adresses IP et de ports spécifiques (sockets de destination). Pour plus d'informations, consultez Ajout, modification ou suppression d'un point de terminaison de sous-réseau VPC. Vous pouvez également spécifier des destinations à l'aide de l'API Global Accelerator. Pour de plus amples informations, veuillez consulterAutoriser CustomRoutingTrafficandDenyCustomRoutingTraffic.

Exemple de fonctionnement du routage personnalisé dans Global Accelerator

Par exemple, supposons que vous souhaitiez prendre en charge 10 000 sessions où des groupes d'utilisateurs interagissent, telles que des sessions de jeu ou des sessions d'appel VoIP, sur 1 000 instances Amazon EC2 derrière Global Accelerator. Dans cet exemple, nous allons spécifier une plage de ports d'écoute de 10001—20040 et une plage de ports de destination de 81—90. Nous dirons que nous avons les quatre sous-réseaux VPC dans us-east-1 : subnet-1, subnet-2, subnet-3 et subnet-4.

Dans notre exemple de configuration, chaque sous-réseau VPC a une taille de bloc de /24, donc il peut prendre en charge 251 instances Amazon EC2. (Cinq adresses sont réservées et indisponibles à partir de chaque sous-réseau, et ces adresses ne sont pas mappées.) Chaque serveur exécuté sur chaque instance EC2 sert les 10 ports suivants, que nous avons spécifiés pour les ports de destination dans notre groupe de points de terminaison : 81-90. Cela signifie que nous avons 2510 ports (10 x 251) associés à chaque sous-réseau. Chaque port peut être associé à une session.

Étant donné que nous avons spécifié 10 ports de destination sur chaque instance EC2 de notre sous-réseau, Global Accelerator les associe en interne à 10 ports d'écoute que vous pouvez utiliser pour accéder aux instances EC2. Pour illustrer cela simplement, nous dirons qu'il existe un bloc de ports d'écoute qui commence par la première adresse IP du sous-réseau de point de terminaison pour le premier ensemble de 10, puis passe à l'adresse IP suivante pour le jeu suivant de 10 ports d'écoute.

> **Note**
>
> Le mappage n'est pas prévisible comme celui-ci, mais nous utilisons un mappage séquentiel ici pour aider à montrer comment fonctionne le mappage de port. Pour déterminer le mappage réel pour vos plages de ports d'écoute, utilisez les opérations API suivantes : ListCustomRoutingMappingsandListCustomRoutingPortMappingsByDestination.

Dans notre exemple, le premier port d'écoute est 10001. Ce port est associé à la première adresse IP de sous-réseau, 192.0.2.4, et au premier port EC2, 81. Le port d'écoute suivant, 10002, est associé à la première adresse IP de sous-réseau, 192.0.2.4, et au deuxième port EC2, 82. Le tableau suivant illustre comment cet exemple de mappage se poursuit jusqu'à la dernière adresse IP du premier sous-réseau VPC, puis à la première adresse IP du deuxième sous-réseau VPC.

Port d'écoute Global Accelerator	Sous-réseaux VPC	Port d'instance EC2
10001	192.0.2.4	81
10002	192.0.2.4	82
10003	192.0.2.4	83
10004	192.0.2.4	84
10005	192.0.2.4	85
10006	192.0.2.4	86
10007	192.0.2.4	87
10008	192.0.2.4	88
10009	192.0.2.4	89
10010	192.0.2.4	90
10011	192.0.2.5	81
10012	192.0.2.5	82
10013	192.0.2.5	83
10014	192.0.2.5	84
10015	192.0.2.5	85
10016	192.0.2.5	86
10017	192.0.2.5	87
10018	192.0.2.5	88
10019	192.0.2.5	89

Port d'écoute Global Accelerator	Sous-réseaux VPC	Port d'instance EC2
10020	192.0.2.5	90
...	...	...
12501	192.0.2.244	81
12502	192.0.2.244	82
12503	192.0.2.244	83
12504	192.0.2.244	84
12505	192.0.2.244	85
12506	192.0.2.244	86
12507	192.0.2.244	87
12508	192.0.2.244	88
12509	192.0.2.244	89
12510	192.0.2.244	90
12511	192.0.3.4	81
12512	192.0.3.4	82
12513	192.0.3.4	83
12514	192.0.3.4	84
12515	192.0.3.4	85
12516	192.0.3.4	86
12517	192.0.3.4	87
12518	192.0.3.4	88

Port d'écoute Global Accelerator	Sous-réseaux VPC	Port d'instance EC2
12519	192.0.3.4	89
12520	192.0.3.4	90

Directives et restrictions pour les accélérateurs de routage personnalisés

Lorsque vous créez et travaillez avec des accélérateurs de routage personnalisés dans AWS Global Accelerator, gardez à l'esprit les directives et restrictions suivantes.

Destinations d'instance Amazon EC2

- Les points de terminaison de sous-réseau de cloud public virtuel (VPC) d'un accélérateur de routage personnalisé Aucune autre ressource, telle que les équilibreurs de charge, n'est prise en charge pour l'accélérateur de routage personnalisé.

- Les types d'instances EC2 pris en charge par Global Accelerator sont répertoriés dansPoints de terminaison pour les accélérateurs standard dans AWS Global Accelerator.

Mappages de port

- Lorsque vous ajoutez un sous-réseau VPC, Global Accelerator crée un mappage de port statique des plages de ports d'écoute vers les plages de ports prises en charge par le sous-réseau. Le mappage de port d'un sous-réseau spécifique ne change jamais.

- Vous pouvez afficher la liste de mappages de port d'un accélérateur de routage personnalisé par programme Pour plus d'informations, consultez `ListCustomRoutingPortMappings`.

Taille de sous-réseau VPC

- Les sous-réseaux VPC que vous ajoutez à un accélérateur de routage personnalisé doivent être au minimum /28 et au maximum /17.

Plages de ports d'écoute

- Vous devez spécifier suffisamment de ports d'écoute, en spécifiant des plages de ports d'écoute, pour tenir compte du nombre de destinations incluses dans les sous-réseaux que vous prévoyez

d'ajouter à votre accélérateur de routage personnalisé. La plage que vous spécifiez lorsque vous créez un processus d'écoute détermine le nombre de combinaisons d'adresses IP de port d'écoute et de destination que vous pouvez utiliser avec votre accélérateur de routage personnalisé. Pour une flexibilité maximale et pour réduire la possibilité d'obtenir une erreur si vous n'avez pas assez de ports d'écoute disponibles, nous vous recommandons de spécifier une plage de ports étendue.

Global Accelerator alloue des plages de ports en blocs lorsque vous ajoutez un sous-réseau à un accélérateur de routage personnalisé. Nous vous recommandons d'allouer des plages de ports d'écoute linéairement et de les rendre suffisamment grandes pour prendre en charge le nombre de ports de destination que vous avez l'intention d'avoir. Autrement dit, le nombre de ports que vous devez allouer doit correspondre au moins à la taille du sous-réseau multipliée par le nombre de ports et de protocoles de destination (configurations de destination) que vous aurez dans le sous-réseau.

> **Note**
>
> L'algorithme utilisé par Global Accelerator pour allouer des mappages de ports peut nécessiter l'ajout de ports d'écoute supplémentaires, au-delà de ce total.

Après avoir créé un écouteur, vous pouvez le modifier pour ajouter des plages de ports supplémentaires et des protocoles associés, mais vous ne pouvez pas réduire les plages de ports existantes. Par exemple, si vous avez une plage de ports d'écoute comprise entre 5 000 et 10 000, vous ne pouvez pas modifier la plage de ports pour qu'elle soit de 5 000 à 10 000 et vous ne pouvez pas modifier la plage de ports pour qu'elle soit de 5 000 à 9 900.

Chaque plage de ports d'écoute doit inclure au moins 16 ports. Les écouteurs prennent en charge les ports 1 à 65535.

Plages de ports de destination

Vous spécifiez des plages de ports pour un accélérateur de routage personnalisé à deux endroits : les plages de ports que vous spécifiez lorsque vous ajoutez un écouteur et les plages de ports de destination et les protocoles que vous spécifiez pour un groupe de points de terminaison.

- Plages de ports d'écoute : Ports d'écoute sur les adresses IP statiques Global Accelerator auxquelles vos clients se connectent. Global Accelerator mappe chaque port à une adresse IP de destination unique et un port sur un sous-réseau VPC derrière l'accélérateur.

- Plages de ports de destination : Les ensembles de plages de ports de destination que vous spécifiez pour un groupe de points de terminaison (également appelés configurations de destination) sont les ports d'instance EC2 qui reçoivent du trafic. Pour recevoir du trafic sur les ports de destination, les groupes de sécurité associés à vos instances EC2 doivent autoriser le trafic sur eux.

Vérifications Health l'état et basculement

Global Accelerator n'effectue pas de contrôles d'intégrité pour les accélérateurs de routage personnalisés et ne fait pas de basculement vers des points de terminaison sains. Le trafic des accélérateurs de routage personnalisés est routé de manière déterministe, quel que soit l'état d'une ressource de destination.

Tout le trafic est refusé par défaut

Par défaut, le trafic dirigé via un accélérateur de routage personnalisé est refusé vers toutes les destinations de votre sous-réseau. Pour permettre aux instances de destination de recevoir du trafic, vous devez autoriser spécifiquement tout le trafic vers le sous-réseau ou, alternativement, autoriser le trafic vers des adresses IP d'instance spécifiques et des ports du sous-réseau.

La mise à jour d'un sous-réseau ou d'une destination spécifique pour autoriser ou refuser le trafic prend du temps à se propager sur Internet. Pour déterminer si une modification s'est propagée, vous pouvez appeler la méthode`DescribeCustomRoutingAccelerator`pour vérifier l'état de l'accélérateur. Pour de plus amples informations, veuillez consulterDescribeCustomRoutingAccelerator.

AWS CloudFormation n'est pas pris en charge

AWS CloudFormation n'est pas pris en charge pour les accélérateurs de routage personnalisés.

Accélérateurs de routage personnalisés dans AWS Global Accelerator

Aaccélérateur de routage personnalisédans AWS Global Accelerator vous permet d'utiliser une logique d'application personnalisée pour diriger un ou plusieurs utilisateurs vers une destination spécifique parmi de nombreuses destinations, tout en utilisant le réseau global AWS pour améliorer la disponibilité et les performances de votre application.

Un accélérateur de routage personnalisé achemine le trafic uniquement vers les ports sur les instances Amazon EC2 qui s'exécutent dans des sous-réseaux VPC (Virtual Private Cloud). Avec

un accélérateur de routage personnalisé, Global Accelerator n'achemine pas le trafic en fonction de la géoproximité ou de l'intégrité du point de terminaison. Pour en savoir plus, consultez la section Fonctionnement des accélérateurs de routage personnalisés dans AWS Global Accelerator.

Lorsque vous créez un accélérateur, par défaut, Global Accelerator vous fournit un ensemble de deux adresses IP statiques. Si vous apportez votre propre plage d'adresses IP à AWS (BYOIP), vous pouvez à la place attribuer des adresses IP statiques à partir de votre propre pool à utiliser avec votre accélérateur. Pour plus d'informations, consultez Fourniture de vos propres adresses IP (BYOIP) dans AWS Global Accelerator.

> **Important**
>
> Les adresses IP sont assignées à votre accélérateur aussi longtemps qu'il existe, même si vous désactivez l'accélérateur et qu'il n'accepte plus ni achemine le trafic. Cependant, lorsque vousdeleteun accélérateur, vous perdez les adresses IP statiques Global Accelerator qui sont assignées à l'accélérateur, de sorte que vous ne pouvez plus acheminer le trafic en les utilisant. En tant que meilleure pratique, assurez-vous que vous disposez des autorisations nécessaires pour éviter de supprimer par inadvertance des accélérateurs. Vous pouvez utiliser des stratégies IAM telles que des autorisations basées sur des balises avec Global Accelerator pour limiter les utilisateurs disposant des autorisations pour supprimer un accélérateur. Pour plus d'informations, consultez Stratégies basées sur balises.

Cette section explique comment créer, modifier ou supprimer un accélérateur de routage personnalisé sur la console Global Accelerator. Pour en savoir plus sur l'utilisation des opérations API avec Global Accelerator, consultez leRéférence de l'API AWS Global Accelerator.

Rubriques

- Création ou mise à jour d'un accélérateur de routage personnalisé
- Affichage de vos accélérateurs de routage personnalisés
- Suppression d'un accélérateur de routage personnalisé

Création ou mise à jour d'un accélérateur de routage personnalisé

Pour créer un accélérateur de routage personnalisé

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. ChoisissezCréer accélérateur.
3. Fournissez un nom pour votre accélérateur.
4. PourType d'accélérateur, sélectionnezRoutage personnalisé.
5. Si vous avez apporté votre propre plage d'adresses IP à AWS (BYOIP), vous pouvez spécifier des adresses IP statiques pour votre accélérateur à partir de ce pool d'adresses. Faites ce choix pour chacune des deux adresses IP statiques de votre accélérateur.
   - Pour chaque adresse IP statique, choisissez le pool d'adresses IP à utiliser.
   - Si vous avez choisi votre propre pool d'adresses IP, choisissez également une adresse IP spécifique à partir du groupe. Si vous avez choisi le pool d'adresses IP Amazon par défaut, Global Accelerator attribue une adresse IP spécifique à votre accélérateur.
6. Si vous le souhaitez, ajoutez une ou plusieurs balises pour vous aider à identifier vos ressources d'accélérateur.
7. ChoisissezSuivantpour accéder aux pages suivantes de l'Assistant pour ajouter des écouteurs, des groupes de points de terminaison et des points de terminaison de sous-réseau VPC.

Pour modifier un accélérateur de routage personnalisé

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la liste des accélérateurs de routage personnalisés, choisissez en un, puis choisissezModifier.
3. Dans la pageModifier l'accélérateur, apportez les modifications souhaitées. Par exemple, vous pouvez désactiver l'accélérateur afin de pouvoir le supprimer.
4. Choisissez Enregistrer.

Affichage de vos accélérateurs de routage personnalisés

Vous pouvez afficher les informations concernant vos accélérateurs de routage personnalisés sur la console. Pour voir les descriptions de vos accélérateurs de routage personnalisés par programme, voirListCustomRoutingAcceleratorandDescribeCustomRoutingAcceleratorDans la Référence d'API AWS Global Accelerator.

Pour afficher des informations sur vos accélérateurs de routage personnalisés

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Pour afficher les détails d'un accélérateur, choisissez un accélérateur, puis choisissezAfficher.

Suppression d'un accélérateur de routage personnalisé

Si vous avez créé un accélérateur de routage personnalisé en tant que test, ou si vous n'utilisez plus d'accélérateur, vous pouvez le supprimer. Sur la console, désactivez l'accélérateur, puis vous pouvez le supprimer. Vous n'avez pas besoin de supprimer les écouteurs et les groupes de points de terminaison de l'accélérateur.

Pour supprimer un accélérateur de routage personnalisé à l'aide d'une opération API au lieu de la console, vous devez d'abord supprimer tous les écouteurs et groupes de points de terminaison associés à l'accélérateur, puis le désactiver. Pour plus d'informations, consultez le .DeleteAcceleratorOpération dans leRéférence de l'API AWS Global Accelerator.

Pour désactiver un accélérateur de routage personnalisé

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la liste, choisissez l'accélérateur que vous souhaitez désactiver.
3. Choisissez Modifier.
4. ChoisissezDésactiver l'accélérateur, puis choisissezEnregistrer.

Pour supprimer un accélérateur de routage personnalisé

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.

2. Dans la liste, choisissez l'accélérateur que vous souhaitez supprimer.
3. Sélectionnez Delete.

> **Note**
>
> Si vous n'avez pas désactivé l'accélérateur,Supprimern'est pas disponible. Pour désactiver l'accélérateur, consultez la procédure précédente.

4. Dans la boîte de dialogue de confirmation, choisissez Delete (Supprimer).

> **Important**
>
> Lorsque vous supprimez un accélérateur, vous perdez les adresses IP statiques qui sont assignées à l'accélérateur, de sorte que vous ne pouvez plus acheminer le trafic en les utilisant.

Écouteurs pour les accélérateurs de routage personnalisés dans AWS Global Accelerator

Pour un accélérateur de routage personnalisé dans AWS Global Accelerator, vous configurez un écouteur qui spécifie une plage de ports d'écoute avec des protocoles associés que Global Accelerator mappe à des instances Amazon EC2 de destination spécifiques dans vos points de terminaison de sous-réseau VPC. Lorsque vous ajoutez un point de terminaison de sous-réseau VPC, Global Accelerator crée un mappage de port statique entre les plages de ports que vous définissez pour votre écouteur et les adresses IP et ports de destination dans le sous-réseau. Ensuite, vous pouvez utiliser le mappage de port pour spécifier vos adresses IP statiques d'accélérateur ainsi qu'un port d'écoute et un protocole pour diriger le trafic utilisateur vers des adresses IP d'instance Amazon EC2 de destination spécifiques et des ports dans votre sous-réseau VPC.

Vous définissez un écouteur lorsque vous créez votre accélérateur de routage personnalisé Chaque écouteur peut avoir un ou plusieurs groupes de points de terminaison, un pour chaque région AWS dans laquelle vous avez des points de terminaison de sous-réseau VPC. Un écouteur dans un accélérateur de routage personnalisé prend en charge les protocoles TCP et UDP. Vous spécifiez le ou les protocoles pour chaque plage de ports de destination que vous définissez : UDP, TCP, ou à la fois UDP et TCP.

Pour plus d'informations, consultez Fonctionnement des accélérateurs de routage personnalisés dans AWS Global Accelerator.

Ajout, modification ou suppression d'un écouteur de routage personnalisé

Cette section explique comment utiliser les écouteurs de routage personnalisés sur la console AWS Global Accelerator. Pour en savoir plus sur l'utilisation des opérations d'API avec AWS Global Accelerator, consultez laRéférence de l'API AWS Global Accelerator.

Ajout d'un écouteur d'un accélérateur de routage personnalisé

La plage que vous spécifiez lorsque vous créez un écouteur définit le nombre de combinaisons d'adresses IP de port d'écoute et de destination que vous pouvez utiliser avec votre accélérateur de routage personnalisé. Pour une flexibilité maximale, nous vous recommandons de spécifier une plage de ports étendue Chaque plage de ports d'écoute que vous spécifiez doit inclure au moins 16 ports.

> **Note**
>
> Après avoir créé un écouteur, vous pouvez le modifier pour ajouter des plages de ports supplémentaires et des protocoles associés, mais vous ne pouvez pas réduire les plages de ports existantes.

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur de routage personnalisé
3. Choisissez Ajouter un écouteur.
4. Dans la pageAjout d'un écouteur, entrez la plage de ports d'écouteur à associer à l'accélérateur.

   Les écouteurs prennent en charge les ports 1 à 65535. Pour une flexibilité maximale avec un accélérateur de routage personnalisé, nous vous recommandons de spécifier une plage de ports étendue.
5. Choisissez Ajouter un écouteur.

Pour modifier un écouteur d'un accélérateur de routage personnalisé

Lorsque vous modifiez un écouteur pour un accélérateur de routage personnalisé, sachez que vous pouvez ajouter des plages de ports supplémentaires et des protocoles associés, augmenter des

plages de ports existantes ou modifier des protocoles, mais vous ne pouvez pas réduire les plages de ports existantes.

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. Choisissez un écouteur, puis et.Éditer l'écouteur.
4. Dans la pageÉditer l'écouteur, apportez les modifications que vous souhaitez apporter aux plages de ports ou protocoles existants, ou ajoutez de nouvelles plages de ports.

   Sachez que vous ne pouvez pas diminuer la plage d'une plage de ports existante.
5. Choisissez Enregistrer.

Pour supprimer un écouteur

1. Ouvrez la console Global Accelerator àhttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. Choisissez un écouteur, puis et.Supprimez.
4. Dans la boîte de dialogue de confirmation, choisissezSupprimez.

Groupes de points de terminaison pour les accélérateurs de routage personnalisés dans AWS Global Accelerator

Avec un accélérateur de routage personnalisé dans AWS Global Accelerator, un groupe de points de terminaison définit les ports et protocoles sur lesquels les instances Amazon EC2 de vos sous-réseaux de cloud privé virtuel (VPC) acceptent le trafic.

Vous créez un groupe de points de terminaison pour votre accélérateur de routage personnalisé pour chaque région AWS dans laquelle se trouvent vos sous-réseaux VPC et vos instances EC2. Chaque groupe de points de terminaison d'un accélérateur de routage personnalisé peut avoir plusieurs points de terminaison de sous-réseau VPC. De même, vous pouvez ajouter chaque VPC à plusieurs groupes de points de terminaison, mais les groupes de points de terminaison doivent être associés à différents écouteurs.

Pour chaque groupe de points de terminaison, vous spécifiez un ensemble d'une ou plusieurs plages de ports comprenant les ports vers lesquels vous souhaitez diriger le trafic sur les instances EC2 de

la région. Pour chaque plage de ports de groupe de points de terminaison, spécifiez le protocole à utiliser : UDP, TCP, ou à la fois UDP et TCP. Cela vous offre une flexibilité maximale, sans avoir à dupliquer des ensembles de plages de ports pour chaque protocole. Par exemple, vous pouvez avoir un serveur de jeu avec un trafic de jeu fonctionnant sur UDP sur les ports 8080-8090 alors que vous avez également un serveur qui écoute les messages de chat sur TCP sur le port 80.

Pour en savoir plus, consultez la section Fonctionnement des accélérateurs de routage personnalisés dans AWS Global Accelerator.

Ajouter, modifier ou supprimer un groupe de points de terminaison d'un accélérateur de routage personnalisé

Vous travaillez avec un groupe de points de terminaison pour votre accélérateur de routage personnalisé sur la console AWS Global Accelerator ou à l'aide d'une opération API. Vous pouvez ajouter ou supprimer des points de terminaison de sous-réseau VPC d'un groupe de points de terminaison à tout moment.

Cette section explique comment utiliser des groupes de points de terminaison pour votre accélérateur de routage personnalisé sur la console AWS Global Accelerator. Pour en savoir plus sur l'utilisation des opérations API avec Global Accelerator, consultez laRéférence de l'API AWS Global Accelerator.

Pour ajouter un groupe de points de terminaison pour un accélérateur de routage personnalisé

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur de routage personnalisé
3. DansÉcouteursSection, pourID de l'écouteur, choisissez l'ID de l'écouteur auquel vous souhaitez ajouter un groupe de points de terminaison.
4. ChoisissezAjouter un groupe de points de termin.
5. Dans la section correspondant à un processus d'écoute, spécifiez une région pour le groupe de points de terminaison.
6. PourPorts et protocoles, entrez les plages de ports et les protocoles pour vos instances Amazon EC2.
   - Saisissez unDepuis le portet unPort dePour spécifier une plage de ports.
   - Pour chaque plage de ports, spécifiez le ou les protocoles correspondant à cette plage.

La plage de ports ne doit pas nécessairement être un sous-ensemble de votre plage de ports d'écoute, mais il doit y avoir suffisamment de ports totaux dans la plage de ports d'écoute pour prendre en charge le nombre total de ports que vous spécifiez pour les groupes de points de terminaison dans votre accélérateur de routage personnalisé.

7. Choisissez Enregistrer.
8. Choisissez éventuellementAjouter un groupe de points de terminPour ajouter des groupes de points de terminaison supplémentaires pour cet écouteur. Vous pouvez également choisir un autre écouteur et ajouter des groupes de points de terminaison.
9. ChoisissezAjouter un groupe de points de termin.

Pour modifier un groupe de points de terminaison d'un accélérateur de routage personnalisé

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur de routage personnalisé
3. DansÉcouteursSection, pourID de l'écouteur, choisissez l'ID de l'écouteur auquel le groupe de points de terminaison est associé.
4. ChoisissezModifier le groupe de points de termin.
5. Dans la pageModifier le groupe de points de termin, modifiez la région, la plage de ports ou le protocole d'une plage de ports.
6. Choisissez Enregistrer.

Pour supprimer un accélérateur de routage personnalisé

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur.
3. DansÉcouteurs, choisissez un écouteur, puis choisissezSupprimez.
4. DansGroupes de points de terminaison, choisissez un groupe de points de terminaison, puis choisissezSupprimez.
5. Dans la boîte de dialogue de confirmation, choisissezSupprimez.

Points de terminaison de sous-réseau VPC pour les accélérateurs de routage personnalisés dans AWS Global Accelerator

Les points de terminaison des accélérateurs de routage personnalisés sont des sous-réseaux de cloud privé virtuel (VPC) qui peuvent recevoir du trafic via un accélérateur. Chaque sous-réseau peut contenir une ou plusieurs destinations d'instance Amazon EC2. Lorsque vous ajoutez un point de terminaison de sous-réseau, Global Accelerator génère un nouveau mappage de port. Ensuite, vous pouvez utiliser l'API Global Accelerator pour obtenir une liste statique de tous les mappages de ports pour le sous-réseau, que vous pouvez utiliser pour acheminer le trafic vers les adresses IP d'instance EC2 de destination dans le sous-réseau. Pour de plus amples informations, veuillez consulterListCustomRoutingMappings.

Vous pouvez uniquement diriger le trafic vers des instances EC2 dans les sous-réseaux, pas d'autres ressources comme les équilibreurs de charge (contrairement aux accélérateurs standard). Les types d'instance EC2 pris en charge sont répertoriés dansPoints de terminaison pour les accélérateurs standard dans AWS Global Accelerator.

Pour en savoir plus, consultez la section Fonctionnement des accélérateurs de routage personnalisés dans AWS Global Accelerator.

Soyez conscient de ce qui suit lorsque vous ajoutez des sous-réseaux VPC pour votre accélérateur de routage personnalisé :

- Par défaut, le trafic dirigé par un accélérateur de routage personnalisé ne peut arriver à aucune destination de votre sous-réseau. Pour permettre aux instances de destination de recevoir du trafic, vous devez choisir d'autoriser tout le trafic vers le sous-réseau ou, alternativement, d'activer le trafic vers des adresses IP d'instance spécifiques et des ports (sockets de destination) dans le sous-réseau.

> **Important**
>
> La mise à jour d'un sous-réseau ou d'une destination spécifique pour autoriser ou refuser le trafic prend du temps à se propager sur Internet. Pour déterminer si une modification s'est propagée, vous pouvez appeler la méthode`DescribeCustomRoutingAccelerator`pour vérifier l'état de l'accélérateur. Pour de plus amples informations, veuillez consulterDescribeCustomRoutingAccelerator.

- Étant donné que les sous-réseaux VPC conservent l'adresse IP du client, vous devez examiner les informations de sécurité et de configuration pertinentes lorsque vous ajoutez des sous-réseaux en tant que points de terminaison pour les accélérateurs de routage personnalisés. Pour plus d'informations, consultez Ajout de points de terminaison avec préservation de l'adresse IP client.

Ajout, modification ou suppression d'un point de terminaison de sous-réseau VPC

Vous ajoutez des points de terminaison de sous-réseau de cloud privé virtuel (VPC) aux groupes de points de terminaison dans vos accélérateurs de routage personnalisés afin que vous puissiez diriger le trafic utilisateur vers les instances Amazon EC2 de destination dans le sous-réseau.

Lorsque vous ajoutez et supprimez des instances EC2 du sous-réseau, ou activez ou désactivez le trafic vers des destinations EC2, vous modifiez si ces destinations peuvent recevoir du trafic. Cependant, le mappage de port Global Accelerator ne change pas.

Pour autoriser le trafic vers certaines destinations du sous-réseau, mais pas toutes, entrez les adresses IP de chaque instance EC2 que vous souhaitez autoriser, ainsi que les ports de l'instance que vous souhaitez recevoir du trafic. Les adresses IP que vous spécifiez doivent être pour les instances EC2 du sous-réseau. Vous pouvez spécifier un port ou une plage de ports, à partir des ports qui sont mappés pour le sous-réseau.

Vous pouvez supprimer le sous-réseau VPC de votre accélérateur en le supprimant d'un groupe de points de terminaison. La suppression d'un sous-réseau n'affecte pas le sous-réseau lui-même, mais Global Accelerator ne peut plus diriger le trafic vers le sous-réseau ou vers les instances Amazon EC2 qu'il contient. En outre, Global Accelerator récupère le mappage des ports pour le sous-réseau VPC afin de les utiliser potentiellement pour les nouveaux sous-réseaux que vous ajoutez.

Les étapes de cette section expliquent comment ajouter, modifier ou supprimer des points de terminaison de sous-réseau VPC sur la console AWS Global Accelerator. Pour en savoir plus sur l'utilisation des opérations d'API avec AWS Global Accelerator, consultez laRéférence de l'API AWS Global Accelerator.

Pour ajouter un point de terminaison de sous-réseau VPC

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur de routage personnalisé

3. DansÉcouteursSection, pourID de l'écouteur, choisissez l'ID d'un écouteur.
4. DansGroupes de points de terminaisonSection, pourID de groupe de points de termin, choisissez l'ID du groupe de points de terminaison (région AWS) auquel vous souhaitez ajouter le point de terminaison de sous-réseau VPC.
5. DansPoints de terminaisonSection, choisissezAjouter un point de terminaison.
6. Dans la pageAjouter des points de terminaison, pourPoint de terminaison, choisissez un sous-réseau VPC.

   Si vous n'avez aucun VPC, il n'y a aucun élément dans la liste. Pour continuer, ajoutez au moins un VPC, puis revenez aux étapes ici et choisissez un VPC dans la liste.
7. Pour le point de terminaison de sous-réseau VPC que vous ajoutez, vous pouvez choisir d'autoriser ou de refuser le trafic vers toutes les destinations du sous-réseau, ou vous pouvez autoriser le trafic vers uniquement des instances et des ports EC2 spécifiques. La valeur par défaut est de refuser le trafic vers toutes les destinations du sous-réseau.
8. Choisir Add endpoint (Ajouter un point de terminaison).

Pour autoriser ou refuser le trafic vers des destinations spécifiques

Vous pouvez modifier le mappage des ports de sous-réseau VPC pour un point de terminaison afin d'autoriser ou de refuser le trafic vers des instances et des ports EC2 spécifiques (sockets de destination) dans un sous-réseau.

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur de routage personnalisé
3. DansÉcouteursSection, pourID de l'écouteur, choisissez l'ID d'un écouteur.
4. DansGroupes de points de terminaisonSection, pourID de groupe de points de termin, choisissez l'ID du groupe de points de terminaison (région AWS) du point de terminaison du sous-réseau VPC que vous souhaitez modifier.
5. Choisissez un sous-réseau de point de terminaison, puis choisissezView details (Afficher les détails).
6. Dans la pagePoint de terminaison, sousMappages de port, choisissez une adresse IP, puis choisissezModifier.
7. Entrez les ports pour lesquels vous souhaitez activer le trafic, puis choisissezAutoriser/ces destinations.

Pour autoriser ou refuser TOUT le trafic vers un sous-réseau

Vous pouvez mettre à jour un point de terminaison pour autoriser ou refuser le trafic vers toutes les destinations du sous-réseau VPC.

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur de routage personnalisé
3. DansÉcouteursSection, pourID de l'écouteur, choisissez l'ID d'un écouteur.
4. DansGroupes de points de terminaisonSection, pourID de groupe de points de termin, choisissez l'ID du groupe de points de terminaison (région AWS) du point de terminaison du sous-réseau VPC que vous souhaitez mettre à jour.
5. ChoisissezAutoriser/Refuser tout trafic.
6. Choisissez une option pour autoriser tout le trafic ou refuser tout le trafic, puis choisissezEnregistrer.

Pour supprimer un point de terminaison

1. Ouvrez la console Global Accelerator à l'adressehttps://console.aws.amazon.com/globalaccelerator/home.
2. Dans la pageAccélérateurs, choisissez un accélérateur de routage personnalisé
3. DansÉcouteursSection, pourID de l'écouteur, choisissez l'ID d'un écouteur.
4. DansGroupes de points de terminaisonSection, pourID de groupe de points de termin, choisissez l'ID du groupe de points de terminaison (région AWS) du point de terminaison du sous-réseau VPC que vous souhaitez supprimer.
5. ChoisissezSuppression de l'endpoint.
6. Dans la boîte de dialogue de confirmation, choisissezSupprimez.

Adresses DNS et domaines personnalisés dans AWS Global Accelerator

Ce chapitre explique comment AWS Global Accelerator effectue le routage DNS et inclut des informations sur l'utilisation d'un domaine personnalisé avec Global Accelerator.

Rubriques

Support des adressages DNS dans Global Accelerator

Lorsque vous créez un routage personnalisé ou un accélérateur standard, Global Accelerator fournit deux adresses IP statiques pour vous. Il affecte également un nom DNS (Domain Name System) par défaut à votre accélérateur, similaire à`a1234567890abcdef.awsglobalaccelerator.com`, qui pointe vers les adresses IP statiques. Les adresses IP statiques sont annoncées globalement en utilisant anycast depuis le réseau périphérique AWS vers vos points de terminaison. Vous pouvez utiliser les adresses IP statiques ou le nom DNS de votre accélérateur pour acheminer le trafic vers votre accélérateur. Les serveurs DNS et les résolveurs DNS utilisent un round robin pour résoudre le nom DNS d'un accélérateur, de sorte que le nom se résout en adresses IP statiques de l'accélérateur, renvoyées par Amazon Route 53 dans un ordre aléatoire. Les clients utilisent généralement la première adresse IP renvoyée.

> **Note**
>
> Global Accelerator crée deux enregistrements de pointeur (PTR) qui mappent les adresses IP statiques d'un accélérateur au nom DNS correspondant généré par Global Accelerator, pour prendre en charge la recherche DNS inverse. Cette zone est également appelée zone d'hébergement inversé. Sachez que le nom DNS généré par Global Accelerator n'est pas configurable et que vous ne pouvez pas créer d'enregistrements PTR pointant vers votre nom de domaine personnalisé. Global Accelerator ne crée pas non plus d'enregistrements PTR pour les adresses IP statiques à partir d'une plage d'adresses IP que vous apportez à AWS (BYOIP).

Router le trafic de domaine personnalisé vers votre accélérateur

Dans la plupart des scénarios, vous pouvez configurer le DNS pour utiliser votre nom de domaine personnalisé (tel que`www.example.com`) avec votre accélérateur, au lieu d'utiliser les adresses IP statiques assignées ou le nom DNS par défaut. Tout d'abord, à l'aide d'Amazon Route 53 ou d'un autre fournisseur DNS, créez un nom de domaine, puis ajoutez ou mettez à jour des enregistrements DNS avec vos adresses IP Global Accelerator. Vous pouvez également associer votre nom de domaine personnalisé au nom DNS de votre accélérateur. Terminez la configuration DNS et attendez que les modifications se propagent sur Internet. Maintenant, lorsqu'un client effectue une demande à l'aide de votre nom de domaine personnalisé, le serveur DNS résout les adresses IP, dans un ordre aléatoire, ou le nom DNS pour votre accélérateur.

Pour utiliser votre nom de domaine personnalisé avec Global Accelerator lorsque vous utilisez Route 53 comme service DNS, vous créez un enregistrement d'alias qui pointe votre nom de domaine personnalisé vers le nom DNS attribué à votre accélérateur. Un enregistrement d'alias est une extension d'Route 53 au DNS. Il est similaire à un enregistrement CNAME, mais vous pouvez créer un enregistrement d'alias pour le domaine racine, par exemple`example.com`, et pour les sous-domaines, tels que`www.example.com`. Pour de plus amples informations, veuillez consulterChoix entre des enregistrements avec ou sans aliasdans le Manuel du développeur Amazon Route 53.

Pour configurer Route 53 avec un enregistrement d'alias pour un accélérateur, suivez les instructions incluses dans la rubrique suivante : Cible d'aliasdans le Manuel du développeur Amazon Route 53. Pour afficher les informations relatives à Global Accelerator, faites défiler vers le bas sur leCible d'alias.

Fourniture de vos propres adresses IP (BYOIP) dans AWS Global Accelerator

AWS Global Accelerator utilise des adresses IP statiques comme points d'entrée pour vos accélérateurs. Ces adresses IP sont anycast à partir d'emplacements périphériques AWS. Par défaut, Global Accelerator fournit des adresses IP statiques à partir duPool d'adresses IP Amazon. Au lieu d'utiliser les adresses IP fournies par Global Accelerator, vous pouvez configurer ces points d'entrée pour qu'ils soient des adresses IPv4 à partir de vos propres plages d'adresses. Cette rubrique explique comment utiliser vos propres plages d'adresses IP avec Global Accelerator.

Vous pouvez fournir tout ou partie de vos plages d'adresses IPv4 publiques depuis votre réseau sur site vers votre compte AWS pour l'utiliser avec Global Accelerator. Les plages d'adresses vous appartiennent toujours, mais AWS les publie sur Internet.

Vous ne pouvez pas utiliser les adresses IP que vous apportez à AWS pour un service AWS avec un autre service. Les étapes de ce chapitre décrivent comment fournir votre propre plage d'adresses IP pour une utilisation dans AWS Global Accelerator uniquement. Pour connaître les étapes à suivre pour fournir votre propre plage d'adresses IP pour l'utiliser dans Amazon EC2, veuillez consulterFourniture de vos propres adresses IP (BYOIP)dans le Guide de l'utilisateur Amazon EC2.

> **⚠ Important**
>
> Vous devez cesser de publier votre plage d'adresses IP à partir d'autres emplacements avant de la publier via AWS. Si une plage d'adresses IP est multihomed (c'est-à-dire que la plage est annoncée par plusieurs fournisseurs de services en même temps), nous ne pouvons pas garantir que le trafic vers la plage d'adresses entrera dans notre réseau ou que votre flux de travail publicitaire BYOIP sera terminé avec succès.

Une fois que vous avez fourni une plage d'adresses dans AWS, elle s'affiche dans votre compte en tant que groupe d'adresses. Lorsque vous créez un accélérateur, vous pouvez lui attribuer une adresse IP de votre plage. Global Accelerator vous attribue une deuxième adresse IP statique à partir d'une plage d'adresses IP Amazon. Si vous apportez deux plages d'adresses IP à AWS, vous pouvez attribuer une adresse IP de chaque plage à votre accélérateur. Cette restriction est due au fait que Global Accelerator affecte chaque plage d'adresses à une zone réseau différente, pour une haute disponibilité.

Pour utiliser votre propre plage d'adresses IP avec Global Accelerator, consultez la configuration requise, puis suivez les étapes décrites dans cette rubrique.

Rubriques

Requirements

Vous pouvez ajouter jusqu'à deux plages d'adresses IP éligibles à AWS Global Accelerator par compte AWS.

Pour être éligible, votre plage d'adresses IP doit répondre aux exigences suivantes :

- La plage d'adresses IP doit être enregistrée auprès d'un des registres Internet régionaux (RIR) suivants : l'ARIN (American Registry for Internet Numbers), le RIPE (Réseaux IP Européens Network Coordination Centre) ou l'APNIC (Asia-Pacific Network Information Centre). La plage d'adresses doit être enregistrée auprès d'une entreprise ou d'une entité institutionnelle. Elle ne peut pas être enregistrée pour un individu.
- La plage d'adresses la plus spécifique que vous pouvez apporter est /24. Les 24 premiers bits de l'adresse IP spécifient le numéro de réseau. Par exemple, 198.51.100 est le numéro de réseau pour l'adresse IP 198.51.100.0.
- L'historique des adresses IP dans la plage d'adresses doit être propre. Autrement dit, ils ne peuvent pas avoir une mauvaise réputation ou être associés à un comportement malveillant. Nous nous réservons le droit de rejeter la plage d'adresses IP si nous enquêtons sur la réputation de la plage d'adresses IP et nous constatons qu'elle contient une adresse IP qui n'a pas d'historique propre.

En outre, nous exigeons les types ou statuts de réseau d'allocation et d'affectation suivants, selon l'endroit où vous avez enregistré votre plage d'adresses IP :

- ARIN :`Direct Allocation`and`Direct Assignment`Types de réseau
- MÛRS :`ALLOCATED PA`,`LEGACY`, et`ASSIGNED PI`États d'allocation
- APNIQUE :`ALLOCATED PORTABLE`and`ASSIGNED PORTABLE`États d'allocation

Préparez-vous à importer votre plage d'adresses IP dans votre compte AWS : Autorisation

Pour vous assurer que vous seul pouvez apporter votre espace d'adresse IP à Amazon, nous avons besoin de deux autorisations :

- Vous devez autoriser Amazon à annoncer la plage d'adresses IP.

- Vous devez fournir la preuve que vous possédez la plage d'adresses IP et que vous avez donc le pouvoir de la transmettre à AWS.

> **Note**
>
> Lorsque vous utilisez BYOIP pour apporter une plage d'adresses IP à AWS, vous ne pouvez pas transférer la propriété de cette plage d'adresses à un autre compte ou société pendant que nous la publions. Vous ne pouvez pas non plus transférer directement une plage d'adresses IP d'un compte AWS à un autre compte. Pour transférer la propriété ou transférer entre des comptes AWS, vous devez déprovisionner la plage d'adresses, puis le nouveau propriétaire doit suivre les étapes pour ajouter la plage d'adresses à son compte AWS.

Pour autoriser Amazon à annoncer la plage d'adresses IP, vous fournissez à Amazon un message d'autorisation signé. Utilisez une autorisation d'origine d'itinéraire (ROA) pour fournir cette autorisation. Un ROA est une instruction de chiffrement concernant les annonces de routage que vous créez via votre registre Internet régional (RIR). Une ROA contient la plage d'adresses IP, les numéros de système autonome (ASN) qui sont autorisés à publier la plage d'adresses IP et une date d'expiration. La ROA autorise Amazon à publier une plage d'adresses IP dans le cadre d'un système autonome spécifique.

Un ROA n'autorise pas votre compte AWS à importer la plage d'adresses IP dans AWS. Pour fournir cette autorisation, vous devez publier un certificat X.509 auto-signé dans les remarques RDAP (Registry Data Access Protocol) pour la plage d'adresses IP. Le certificat contient une clé publique utilisée par AWS pour vérifier la signature de contexte d'autorisation que vous fournissez. Il est recommandé de sécuriser la clé privée et de l'utiliser pour signer le message de contexte d'autorisation.

Les sections suivantes fournissent les étapes détaillées pour l'exécution de ces tâches d'autorisation. Les commandes de ces étapes sont prises en charge sous Linux. Si vous utilisez Windows, vous pouvez accéder auWSL (Windows Subsystem for Linux)pour exécuter des commandes Linux.

Étapes pour fournir l'autorisation

- Étape 1 : Créer un objet ROA
- Étape 2 : Créer un certificat X.509 auto-signé
- Étape 3 : Créer un message d'autorisation signé

Étape 1 : Créer un objet ROA

Créez un objet ROA pour autoriser Amazon ASN 16509 à publier votre plage d'adresses IP ainsi que les ASN qui sont actuellement autorisés à publier la plage d'adresses IP. Le ROA doit contenir l'adresse IP /24 que vous souhaitez fournir à AWS et vous devez définir la longueur maximale à /24.

Pour plus d'informations sur la création d'une demande ROA, consultez les sections suivantes, selon l'endroit où vous avez enregistré votre plage d'adresses IP :

- ARIN : Requests ROA
- MÛRS : Gestion des ROAS
- APNIQUE : Gestion d'itinéraires

Étape 2 : Créer un certificat X.509 auto-signé

Créez une key pair et un certificat X.509 auto-signé, et ajoutez le certificat à l'enregistrement RDAP de votre RIR. Les étapes suivantes expliquent comment exécuter ces tâches.

> **Note**
>
> La `.openssl`Dans ces étapes, OpenSSL version 1.0.2 ou ultérieure.

Pour créer et ajouter un certificat X.509

1. Générez une key pair RSA 2048 bits à l'aide de la commande suivante.

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

2. Créez un certificat public X.509 à partir de la key pair en utilisant la commande suivante.

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

   Dans cet exemple, le certificat expire dans 365 jours, après quoi il n'est plus fiable. Lorsque vous exécutez la commande, assurez-vous d'avoir défini le`-days`à la valeur souhaitée pour l'expiration correcte. Lorsque vous êtes invité à saisir d'autres informations, vous pouvez accepter les valeurs par défaut.

3. Mettez à jour l'enregistrement RDAP de votre RIR avec le certificat X.509 en utilisant les étapes suivantes, en fonction de votre RIR.

   1. Affichez votre certificat à l'aide de la commande suivante.

      ```
      cat publickey.cer
      ```

   2. Ajoutez le certificat en procédant comme suit :

      > **Important**
      >
      > Veillez à inclure le`-----BEGIN CERTIFICATE-----`and`-----END CERTIFICATE-----`À partir du certificat.

      - Pour l'ARIN, ajoutez le certificat dans le`Public Comments`Pour votre plage d'adresses IP.
      - Pour le RIPE, ajoutez le certificat sous la forme d'un nouveau`descr`pour votre plage d'adresses IP.
      - Pour APNIC, envoyez la clé publique par e-mail à`helpdesk@apnic.net`, le contact autorisé APNIC pour les adresses IP, pour demander qu'ils l'ajoutent manuellement à l'`remarks`champ.

Étape 3 : Créer un message d'autorisation signé

Créez le message d'autorisation signé pour permettre à Amazon d'annoncer votre plage d'adresses IP.

Le format du message est le suivant, où le`YYYYMMDD`date est la date d'expiration du message.

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

Pour créer le message d'autorisation signé

1. Crée un message d'autorisation en texte brut et stockez-le dans une variable nommée`text_message`, comme le montre l'exemple suivant. Remplacez le numéro de compte, la plage d'adresses IP et la date d'expiration de l'exemple par vos propres valeurs.

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

2. Signer le message d'autorisation dans`text_message`À l'aide de la key pair que vous avez créée dans la section précédente.
3. Stockage du message dans une variable nommée`signed_message`, comme le montre l'exemple suivant.

```
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")
```

Mise en service de la plage d'adresses pour une utilisation avec AWS Global Accelerator

Lorsque vous mettez en service une plage d'adresses pour une utilisation avec AWS, vous confirmez que vous êtes propriétaire de la plage d'adresses et vous autorisez Amazon à la publier. Nous vérifierons que vous possédez la plage d'adresses.

Vous devez provisionner votre plage d'adresses à l'aide des opérations de l'API CLI ou Global Accelerator. Cette fonctionnalité n'est pas disponible dans la console AWS.

Pour allouer la plage d'adresses, utilisez leProvisionByoipCidrLa commande. La `.--cidr-authorization-context`utilise les variables que vous avez créées dans la section précédente, pas le message ROA.

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

Voici un exemple de provisionnement d'une plage d'adresses.

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

La mise en service d'une plage d'adresses est une opération asynchrone, de sorte que l'appel est immédiatement renvoyé. Cependant, la plage d'adresses n'est pas prête à être utilisée tant que son état ne change pas de`PENDING_PROVISIONING`sur`READY`. Le processus d'allocation peut durer jusqu'à 3 semaines. Pour surveiller l'état des plages d'adresses que vous allouez, utilisez l'ListByoipCIDRSCommande de l' :

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

Pour afficher la liste des états d'une plage d'adresses IP, voirparoiPCIDR.

Lorsque votre plage d'adresses IP est provisionnée, l'option`State`Retourné par`list-byoip-cidrs`est`READY`. Exemples :

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

Publication de la plage d'adresses via AWS

Une fois que la plage d'adresses est mise en service, elle est prête à être publiée. Vous devez publier la plage d'adresses exacte que vous avez mise en service. Vous ne pouvez pas publier seulement une portion de la plage d'adresses mise en service. En outre, vous devez cesser de publier votre plage d'adresses IP à partir d'autres emplacements avant de la publier via AWS.

Vous devez annoncer (ou arrêter la publicité) votre plage d'adresses à l'aide des opérations CLI ou de l'API Global Accelerator. Cette fonctionnalité n'est pas disponible dans la console AWS.

> **Important**
>
> Assurez-vous que votre plage d'adresses IP est annoncée par AWS avant d'utiliser une adresse IP de votre pool avec Global Accelerator.

Pour publier la plage d'adresses, utilisez lePublicitéparOIPCIDRLa commande.

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

Voici un exemple de demande à Global Accelerator d'annoncer une plage d'adresses.

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

Pour surveiller l'état des plages d'adresses que vous avez publiées, utilisez l'ListByoipCIDRSLa commande.

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

Lorsque votre plage d'adresses IP est annoncée, le`State`Retourné par`list-byoip-cidrs`est`ADVERTISING`. Exemples :

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

Pour arrêter la publication de la plage d'adresses, utilisez le`withdraw-byoip-cidr`La commande.

> **Important**
>
> Pour arrêter la publicité de votre plage d'adresses, vous devez d'abord supprimer tous les accélérateurs dotés d'adresses IP statiques qui sont alloués du pool d'adresses. Pour supprimer un accélérateur à l'aide de la console ou d'opérations API, consultezSuppression d'un accélérateur.

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

Voici un exemple de demande à Global Accelerator de retirer une plage d'adresses.

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

Mise hors service de la plage d'adresses

Pour cesser d'utiliser votre plage d'adresses avec AWS, vous devez d'abord supprimer tous les accélérateurs qui ont des adresses IP statiques qui sont allouées à partir du groupe d'adresses et vous cessez la publication de votre plage d'adresses. Une fois ces étapes terminées, vous pouvez désactiver la plage d'adresses.

Vous devez arrêter la publicité et déprovisionner votre plage d'adresses à l'aide des opérations CLI ou de l'API Global Accelerator. Cette fonctionnalité n'est pas disponible dans la console AWS.

Étape 1 : Supprimez tous les accélérateurs associés.Pour supprimer un accélérateur à l'aide de la console ou d'opérations API, consultezSuppression d'un accélérateur.

Étape 2. Cessez la publication de la plage d'adresses. Pour arrêter la publication de la plage, utilisez leRetrait par OIPCIDRLa commande.

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

Étape 3. Mise hors service de la plage d'adresses. Pour déprovisionner la plage, utilisez la commande suivanteDéprovisionByOIPCIDRLa commande.

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

Créez un accélérateur avec vos adresses IP

Vous pouvez maintenant créer un accélérateur avec vos adresses IP. Si vous avez apporté une plage d'adresses à AWS, vous pouvez attribuer une adresse IP à votre accélérateur. Si vous avez apporté deux plages d'adresses, vous pouvez attribuer une adresse IP de chaque plage d'adresses à votre accélérateur.

Vous avez plusieurs options pour créer un accélérateur à l'aide de vos propres adresses IP pour les adresses IP statiques :

- Utilisez la console Global Accelerator pour créer un accélérateur. Pour plus d'informations, consultez Création ou mise à jour d'un accélérateur standard et Création ou mise à jour d'un accélérateur de routage personnalisé.

- Utilisez l'API Global Accelerator pour créer un accélérateur. Pour plus d'informations, y compris des exemples d'utilisation de l'interface de ligne de commande, consultezCreateAcceleratorandCreateCustomRoutingAcceleratordans la Référence d'API AWS Global Accelerator.

Conserver les adresses IP des clients dans AWS Global Accelerator

Vos options de conservation et d'accès à l'adresse IP du client pour AWS Global Accelerator dépendent des points de terminaison que vous avez configurés avec votre accélérateur. Il existe deux types de points de terminaison qui peuvent conserver l'adresse IP source du client dans les paquets entrants : Équilibreurs de charge des applications et instances Amazon EC2.

- Lorsque vous utilisez un Application Load Balancer sur Internet comme point de terminaison avec Global Accelerator, la préservation des adresses IP du client est activée par défaut pour les nouveaux accélérateurs. Cela signifie que l'adresse IP source du client d'origine est conservée pour les paquets qui arrivent à l'équilibreur de charge. Vous pouvez choisir de désactiver l'option lorsque vous créez l'accélérateur ou en modifiant l'accélérateur ultérieurement.
- Lorsque vous utilisez un Application Load Balancer interne ou une instance EC2 avec Global Accelerator, la conservation de l'adresse IP du client est toujours activée sur le point de terminaison.

> **Note**
>
> Global Accelerator ne prend pas en charge la préservation des adresses IP des clients pour les points de terminaison de l'Network Load Balancer et des adresses IP Elastic

Lorsque vous prévoyez d'ajouter la préservation d'adresse IP du client, soyez conscient de ce qui suit :

- Avant d'ajouter et de commencer à acheminer le trafic vers des points de terminaison qui conservent l'adresse IP du client, assurez-vous que toutes les configurations de sécurité requises, par exemple les groupes de sécurité, sont mises à jour pour inclure l'adresse IP du client utilisateur dans les listes autorisées.
- La préservation des adresses IP du client est prise en charge uniquement dans des régions AWS spécifiques. Pour plus d'informations, consultez Régions AWS prises en charge pour la préservation des adresses IP des clients.

Rubriques

Comment activer la préservation de l'adresse IP du client

Lorsque vous créez un nouvel accélérateur, la préservation des adresses IP du client est activée, par défaut, pour les points de terminaison pris en charge.

Tenez compte des points suivants :

- Les équilibreurs de charge des applications internes et les instances EC2 ont toujours activé la préservation de l'adresse IP du client. Vous ne pouvez pas désactiver l'option pour ces points de terminaison.
- Lorsque vous utilisez la console AWS pour créer un nouvel accélérateur, l'option de préservation des adresses IP du client est activée par défaut pour les points de terminaison de l'Application Load Balancer. Vous pouvez désactiver cette option à tout moment si vous ne souhaitez pas conserver l'adresse IP du client pour un point de terminaison de l'Application Load Balancer sur Internet.
- Lorsque vous utilisez l'interface de ligne de commande AWS ou une action API pour créer un nouvel accélérateur et que vous ne spécifiez pas l'option de préservation des adresses IP du client, les points de terminaison de l'Application Load Balancer accessibles sur Internet ont la conservation des adresses IP du client activée par défaut.
- Global Accelerator ne prend pas en charge la préservation des adresses IP des clients pour les points de terminaison de l'Network Load Balancer et des adresses IP Elastic

Pour les accélérateurs existants, vous pouvez transférer des points de terminaison sans conservation d'adresse IP du client vers des points de terminaison qui conservent l'adresse IP du client. Les points de terminaison de l'Application Load Balancer existants peuvent être migrés vers de nouveaux points de terminaison d'équilibreur de charge d'application, et les points de terminaison d'adresse IP Elastic existants peuvent être transférés vers des points de terminaison d'instance EC2. (Les points de terminaison de l'Network Load Balancer ne prennent pas en charge la préservation des adresses IP du client.) Pour passer aux nouveaux points de terminaison, nous vous recommandons de déplacer

lentement le trafic d'un point de terminaison existant vers un nouveau point de terminaison disposant de la préservation de l'adresse IP du client en procédant comme suit :

- Pour les points de terminaison de l'Application Load Balancer existants, ajoutez d'abord à Global Accelerator un point de terminaison d'Application Load Balancer en double qui cible les mêmes backends et, s'il s'agit d'un équilibreur de charge d'application orienté sur Internet, activez la préservation de l'adresse IP du client pour celui-ci. Réglez ensuite les poids sur les terminaux pour déplacer lentement le trafic de l'équilibreur de charge quipasque la préservation de l'adresse IP du client soit activée sur l'équilibreur de chargeavecLa préservation de l'adresse IP du client.
- Pour un point de terminaison d'adresse IP Elastic existant, vous pouvez déplacer le trafic vers un point de terminaison d'instance EC2 avec la préservation de l'adresse IP du client. Ajoutez d'abord un point de terminaison d'instance EC2 à Global Accelerator, puis ajustez les pondérations sur les points de terminaison pour déplacer lentement le trafic du point de terminaison d'adresse IP Elastic vers le point de terminaison d'instance EC2.

Pour obtenir des conseils pas à pas sur la transition, veuillez consulter.Transition des points de terminaison pour utiliser la préservation des adresses IP du client.

Avantages de la préservation des adresses IP du client

Pour les points de terminaison pour lesquels la conservation de l'adresse IP du client n'est pas activée, les adresses IP utilisées par le service Global Accelerator sur le réseau de périphérie remplacent l'adresse IP de l'utilisateur demandeur comme adresse source dans les paquets d'arrivée. Les informations de connexion du client d'origine, telles que l'adresse IP du client et le port du client, ne sont pas conservées lorsque le trafic se déplace vers les systèmes derrière un accélérateur. Cela fonctionne bien pour de nombreuses applications, en particulier celles qui sont disponibles pour tous les utilisateurs tels que les sites Web publics.

Toutefois, pour d'autres applications, vous pouvez accéder à l'adresse IP du client d'origine en utilisant des points de terminaison avec la préservation de l'adresse IP du client. Par exemple, lorsque vous disposez de l'adresse IP du client, vous pouvez collecter des statistiques basées sur les adresses IP du client. Vous pouvez également utiliser des filtres basés sur l'adresse IP tels queLes groupes de sécurité sur les équilibreurs de charge d'applicationpour filtrer le trafic. Vous pouvez appliquer une logique spécifique à l'adresse IP d'un utilisateur dans vos applications qui s'exécutent sur les serveurs de niveau Web derrière ce point de terminaison de l'équilibreur de charge d'application à l'aide de la méthode`X-Forwarded-For`, qui contient les informations d'adresse IP du client d'origine. Vous pouvez également utiliser la préservation des adresses IP du

client dans les règles de groupe de sécurité des groupes de sécurité associés à votre Application Load Balancer. Pour plus d'informations, consultez Comment l'adresse IP du client est conservée dans AWS Global Accelerator. Pour les points de terminaison d'instance EC2, l'adresse IP du client d'origine est conservée.

Pour les points de terminaison qui n'ont pas de conservation de l'adresse IP du client, vous pouvez filtrer l'adresse IP source utilisée par Global Accelerator lorsqu'il transfère le trafic à partir de la périphérie. Vous pouvez afficher des informations sur les adresses IP source (qui sont également des adresses IP clientes, lorsque la conservation de l'adresse IP du client est activée) des paquets entrants en consultant vos journaux de flux Global Accelerator. Pour plus d'informations, consultez Plages d'adresses IP et d'emplacements des serveurs périphériques Global Accelator et Journaux de flux dans AWS Global Accelerator.

Comment l'adresse IP du client est conservée dans AWS Global Accelerator

AWS Global Accelerator conserve l'adresse IP source du client différemment pour les instances Amazon EC2 et les équilibreurs de charge d'application :

- Pour un point de terminaison d'instance EC2, l'adresse IP du client est conservée pour tout le trafic.
- Pour un point de terminaison de l'Application Load Balancer avec la préservation de l'adresse IP du client, Global Accelerator travaille en collaboration avec l'Application Load Balancer pour fournir un`X-Forwarded`En-tête,`X-Forwarded-For`, qui inclut l'adresse IP du client d'origine afin que votre niveau Web puisse y accéder.

Les demandes HTTP et les réponses HTTP utilisent des champs d'en-tête pour envoyer des informations concernant les messages HTTP. Les champs d'en-tête sont des paires nom-valeur dont les noms et les valeurs sont séparés par un signe deux points, et qui sont séparées entre elles par un retour chariot (CR) et un saut de ligne (LF). Un ensemble standard de champs d'en-tête HTTP est défini dans la section du RFC 2616concernant les en-têtes HTTPEn-têtes de message. Des en-têtes HTTP non standard couramment utilisés par les applications sont également disponibles. Certains des en-têtes HTTP non standard ont un`X-Forwarded`prefix.

Étant donné qu'un Application Load Balancer met fin aux connexions TCP entrantes et crée de nouvelles connexions à vos cibles principales, il ne conserve pas les adresses IP du client jusqu'à votre code cible (telles que les instances, les conteneurs ou le code Lambda). L'adresse IP source que vos cibles voient dans le paquet TCP est l'adresse IP de l'équilibreur de charge d'application.

Toutefois, un équilibreur de charge d'application conserve l'adresse IP du client d'origine en la supprimant de l'adresse de réponse du paquet d'origine et en l'insérant dans un en-tête HTTP avant d'envoyer la requête à votre serveur principal via une nouvelle connexion TCP.

La .`X-Forwarded-For`est formaté comme ceci :

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

L'exemple suivant illustre un`X-Forwarded-For`En-tête de demande pour un client avec l'adresse IP 203.0.113.7.

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

Meilleures pratiques pour la préservation des adresses IP des clients

Lorsque vous utilisez la préservation des adresses IP du client dans AWS Global Accelerator, gardez à l'esprit les informations et les meilleures pratiques de cette section pour les interfaces réseau élastiques et les groupes de sécurité.

Pour prendre en charge la préservation des adresses IP des clients, Global Accelerator crée des interfaces réseau élastiques dans votre compte AWS, une pour chaque sous-réseau où un point de terminaison est présent. Une interface réseau élastique est un composant réseau logique dans un VPC qui représente une carte réseau virtuelle. Global Accelerator utilise ces interfaces réseau élastiques pour acheminer le trafic vers les points de terminaison configurés derrière un accélérateur. Les points de terminaison pris en charge pour le routage du trafic de cette façon sont les équilibreurs de charge d'application (internes et Internet) et les instances Amazon EC2.

> **Note**
>
> Lorsque vous ajoutez un Application Load Balancer interne ou un point de terminaison d'instance EC2 dans Global Accelerator, vous autorisez le trafic Internet à circuler directement vers et depuis le point de terminaison dans Virtual Private Clouds (VPC) en le ciblant dans un sous-réseau privé. Pour plus d'informations, consultez Connexions VPC sécurisées dans AWS Global Accelerator.

Comment Global Accelerator utilise les interfaces réseau élastiques

Lorsque vous avez un équilibreur de charge d'application avec la conservation de l'adresse IP du client activée, le nombre de sous-réseaux dans lesquels se trouve l'équilibreur de charge détermine le nombre d'interfaces réseau élastiques que Global Accelerator crée dans votre compte. Global Accelerator crée une elastic network interface pour chaque sous-réseau qui comporte au moins une elastic network interface de l'Application Load Balancer qui est orientée par un accélérateur dans votre compte.

Les exemples suivants illustrent comment cela fonctionne :

- Exemple 1 : Si un équilibreur de charge d'application possède des interfaces réseau élastiques dans le sous-réseau A et le sous-réseau B, puis que vous ajoutez l'équilibreur de charge comme point de terminaison d'accélérateur, Global Accelerator crée deux interfaces réseau élastiques, une dans chaque sous-réseau.
- Exemple 2 : Si vous ajoutez, par exemple, un ALB1 qui a des interfaces réseau élastiques dans SubNETA et SubNetB à Accelerator1, puis ajoutez un ALB2 avec des interfaces réseau élastiques dans le sous-réseau A et le sous-réseau B à Accelerator2, Global Accelerator ne crée que deux interfaces réseau élastiques : une dans SubNETA et une dans SubNetB.
- Exemple 3 : Si vous ajoutez un ALB1 qui a des interfaces réseau élastiques dans SubNETA et SubNetB à Accelerator1, puis ajoutez un ALB2 avec des interfaces réseau élastiques dans SubNETA et SubNetC à Accelerator2, Global Accelerator crée trois interfaces réseau élastiques : une dans SubNETA, une dans SubNetB et une dans SubNetC. L'elastic network interface de SubNETA fournit le trafic activé pour Accelerator1 et Accelerator2.

Comme indiqué dans l'exemple 3, les interfaces réseau élastiques sont réutilisées entre les accélérateurs si les points de terminaison du même sous-réseau sont placés derrière plusieurs accélérateurs.

Les interfaces réseau élastiques logiques créées par Global Accelerator ne représentent pas un hôte unique, un goulot d'étranglement de débit ou un point de défaillance unique. Comme d'autres services AWS qui apparaissent sous la forme d'une elastic network interface unique dans une zone de disponibilité ou un sous-réseau, des services tels qu'une passerelle de traduction d'adresses réseau (NAT) ou un équilibrage de charge réseau, Global Accelerator est implémenté en tant que service hautement disponible à échelle horizontale.

Évaluez le nombre de sous-réseaux utilisés par les points de terminaison dans vos accélérateurs pour déterminer le nombre d'interfaces réseau élastiques que Global Accelerator créera. Avant

de créer un accélérateur, assurez-vous que vous disposez d'une capacité d'espace d'adressage IP suffisante pour les interfaces réseau élastiques requises, au moins une adresse IP libre par sous-réseau concerné. Si vous n'avez pas assez d'espace d'adressage IP libre, vous devez créer ou utiliser un sous-réseau disposant d'un espace d'adressage IP suffisant pour votre Application Load Balancer et les interfaces réseau élastiques Global Accelerator associées.

Lorsque Global Accelerator détermine qu'aucune elastic network interface n'est utilisée par aucun des points de terminaison des accélérateurs de votre compte, Global Accelerator supprime l'interface.

Groupes de sécurité créés par Global Accelerator

Consultez les informations et les meilleures pratiques suivantes lorsque vous travaillez avec Global Accelerator et des groupes de sécurité.

- Global Accelerator crée des groupes de sécurité associés à ses interfaces réseau élastiques. Bien que le système ne vous empêche pas de le faire, vous ne devez pas modifier les paramètres du groupe de sécurité pour ces groupes.
- Global Accelerator ne supprime pas les groupes de sécurité qu'il crée. Toutefois, Global Accelerator supprime une elastic network interface si elle n'est utilisée par aucun des points de terminaison des accélérateurs de votre compte.
- Vous pouvez utiliser les groupes de sécurité créés par Global Accelerator comme groupe source dans d'autres groupes de sécurité que vous maintenez à jour, mais Global Accelerator transfère uniquement le trafic vers les cibles que vous spécifiez dans votre VPC.
- Si vous modifiez les règles de groupe de sécurité créées par Global Accelerator, le point de terminaison peut devenir défectueux. Dans ce cas, contactezAWS SupportPour obtenir de l'aide.
- Global Accelerator crée un groupe de sécurité spécifique pour chaque VPC. Les interfaces réseau élastiques créées pour les points de terminaison d'un VPC spécifique utilisent toutes le même groupe de sécurité, quel que soit le sous-réseau auquel une elastic network interface est associée.

Régions AWS prises en charge pour la préservation des adresses IP des clients

Vous pouvez activer la préservation des adresses IP du client pour AWS Global Accelerator dans les régions AWS suivantes.

Nom de la région	Région
US East (Ohio)	`us-east-2`
US East (N. Virginia)	`us-east-1`
US West (N. California)	`us-west-1 (except AZ usw1-az2)`
US West (Oregon)	`us-west-2`
Africa (Cape Town)	`af-south-1`
Asia Pacific (Hong Kong)	`ap-east-1`
Asia Pacific (Mumbai)	`ap-south-1`
Asia Pacific (Osaka)	`ap-northeast-3`
Asia Pacific (Singapore)	`ap-southeast-1`
Asia Pacific (Sydney)	`ap-southeast-2`
Asia Pacific (Tokyo)	`ap-northeast-1 (except AZ apne1-az3)`
Asia Pacific (Seoul)	`ap-northeast-2`
Canada (Central)	`ca-central-1 (except AZ cac1-az3)`
Europe (Frankfurt)	`eu-central-1`
Europe (Ireland)	`eu-west-1`
Europe (London)	`eu-west-2`
Europe (Milan)	`eu-south-1`
Europe (Paris)	`eu-west-3`
Europe (Stockholm)	`eu-north-1`

Nom de la région	Région
Middle East (Bahrain)	`me-south-1`
South America (São Paulo)	`sa-east-1`

Journalisation et surveillance dans

Vous pouvez utiliser les journaux de flux et AWS CloudTrail pour surveiller votre accélérateur dans AWS Global Accelerator, analyser les modèles de trafic et résoudre les problèmes liés à vos points de terminaison et vos points de terminaison.

Rubriques

- Journaux de flux dans AWS Global Accelerator
- Utilisation d'Amazon CloudWatch avec AWS Global Accelerator
- Utilisation d'AWS CloudTrail pour journaliser les appels d'API AWS Global Accelerator

Journaux de flux dans AWS Global Accelerator

Les journaux de flux vous permettent de capturer des informations sur le trafic d'adresses IP entrant et sortant dans les interfaces réseau dans votre accélérateur dans AWS Global Accelerator. Les données du journal de flux sont publiées dans Amazon S3, où vous pouvez récupérer et afficher vos données après que vous avez créé un journal de flux.

Les journaux de flux peuvent vous aider pour de nombreuses tâches. Par exemple, vous pouvez déterminer pourquoi un trafic spécifique n'atteint pas un point de terminaison, ce qui vous aide à diagnostiquer des règles de groupe de sécurité trop restrictives. Vous pouvez également utiliser les journaux de flux comme outil de sécurité pour surveiller le trafic qui atteint vos points de terminaison.

Un enregistrement de journal de flux représente un flux de réseau dans votre journal de flux. Chaque enregistrement capture le flux de réseau pour un 5-uplet spécifique, pour une fenêtre de capture spécifique. Un 5-uplet est un ensemble de cinq valeurs différentes qui spécifient la source, la destination et un protocole pour un flux IP. La fenêtre de capture correspond à la durée pendant laquelle le service de journaux de flux regroupe les données avant de publier les enregistrements de journaux de flux. La fenêtre de capture dure environ 10 secondes, mais elle peut aller jusqu'à 1 minute.

Des frais de CloudWatch Logs s'appliquent lors de l'utilisation de journaux de flux, même lorsque les journaux sont publiés directement dans Amazon S3. Pour de plus amples informations, veuillez consulterLivrer les journaux à S3àTarification Amazon CloudWatch.

Rubriques

Publication des journaux de flux sur Amazon S3

Les journaux de flux pour AWS Global Accelerator sont publiés dans Amazon S3 dans un compartiment S3 existant que vous spécifiez. Les enregistrements de journaux de flux sont publiés dans une série d'objets de fichier journal qui sont stockés dans le compartiment.

Pour créer un compartiment Amazon S3 à utiliser avec les journaux de flux, reportez-vous à Créer un compartiment dans leGuide de démarrage Amazon Simple Storage Service.

Fichiers journaux de flux

Les journaux de flux collectent les enregistrements de journal de flux, les consolident dans des fichiers journaux, puis publient ceux-ci dans le compartiment Amazon S3 à intervalles de 5 minutes. Chaque fichier journal contient des enregistrements de journaux de flux pour le trafic de l'adresse IP enregistré au cours des cinq dernières minutes.

La taille maximale d'un fichier journal est de 75 Mo. Si le fichier journal atteint la limite maximale de taille au cours de la période de 5 minutes, le journal de flux cesse de lui ajouter des enregistrements de journaux de flux, le publie dans le compartiment Amazon S3, puis crée un nouveau fichier journal.

Les fichiers journaux sont enregistrés dans le compartiment Amazon S3 indiqué à l'aide d'une structure de dossiers qui est déterminée par l'ID du journal de flux, sa région et sa date de création. La structure de dossiers du compartiment utilise le format suivant :

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

De même, le nom du fichier journal est déterminé par son ID, sa région, ainsi que la date et l'heure de sa création. Les noms de fichier utilisent le format suivant :

```
aws_account_id_globalaccelerator_accelerator_id_flow_log_id_timestamp_hash.log.gz
```

Notez ce qui suit à propos de la structure des dossiers et des noms de fichiers pour les fichiers journaux :

- L'horodatage utilise le format YYYYMMDDTHHmmZ.
- Si vous spécifiez une barre oblique (/) pour le préfixe du compartiment S3, la structure du dossier du compartiment du fichier journal inclut une double barre oblique (//), comme suit :

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

L'exemple suivant montre la structure de dossiers et le nom d'un fichier journal pour un flux créé par le compte AWS123456789012pour un accélérateur avec un ID de1234abcd-abcd-1234-abcd-1234abcdefgh, le 23 novembre 2018 à 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 fichier journal de flux unique contient des entrées entrelacées avec plusieurs enregistrements de 5 tuples, c'est-à-direclient_ip,client_port,accelerator_ip,accelerator_port,protocol. Pour afficher tous les fichiers journaux de flux de votre accélérateur, recherchez les entrées agrégées par leaccelerator_idet vos recettesaccount_id.

Rôles IAM pour la publication des journaux de flux sur Amazon S3

Un mandataire IAM tel qu'un utilisateur IAM doit disposer d'autorisations suffisantes pour publier des journaux de flux dans le compartiment Amazon S3. La stratégie IAM doit inclure les autorisations suivantes :

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

Autorisations du compartiment Amazon S3 pour les journaux de flux

Les compartiments Amazon S3 et les objets qu'ils contiennent sont confidentiels par défaut. Seul le propriétaire du compartiment peut accéder au compartiment et aux objets qui sont stockés dedans. Le propriétaire du compartiment peut toutefois accorder des autorisations d'accès à d'autres ressources et à d'autres utilisateurs en créant une stratégie d'accès.

Si l'utilisateur qui crée le journal de flux est le propriétaire du compartiment, le service attache automatiquement la stratégie suivante au compartiment pour donner au journal de flux l'autorisation de publier des journaux dans ce compartiment :

```
{
    "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 l'utilisateur qui crée le journal de flux n'est pas le propriétaire du compartiment ou ne dispose pas des autorisations `GetBucketPolicy` et `PutBucketPolicy` pour le compartiment, la création du journal de flux échoue. Dans ce cas, le propriétaire du compartiment doit ajouter manuellement la stratégie précédente au compartiment et indiquer l'ID de compte AWS du créateur du journal de flux. Pour de plus amples informations, veuillez consulterComment ajouter une stratégie de compartiment S3 ?dans leGuide de mise en route Amazon Simple Storage Service. Si le compartiment reçoit des journaux de flux de plusieurs comptes, ajoutez une entrée d'élément `Resource` à la déclaration de stratégie `AWSLogDeliveryWrite` pour chaque compte.

Par exemple, la stratégie de compartiment suivante permet aux comptes AWS 123123123 et 456456456456456456 de publier des journaux de flux dans un dossier nomméflow-logsdans un compartiment nommélog-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**
>
> Nous vous recommandons d'accorder le`AWSLogDeliveryAclCheck`and`AWSLogDeliveryWrite`au principal du service de remise des journaux plutôt qu'à des ARN de compte AWS individuels.

Stratégie de clé CMK obligatoire à utiliser avec les compartiments SSE-KMS

Si vous avez activé le chiffrement côté serveur (SSE) pour votre compartiment Amazon S3 à l'aide de clés gérées par AWS KMS (SSE-KMS) avec une clé principale client gérée par le client (CMK), vous devez ajouter ce qui suit à la stratégie de clé pour votre CMK de sorte que les journaux de flux puissent écrire des fichiers journaux dans le compartiment :

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

Autorisations pour les fichiers journaux Amazon S3

Outre les stratégies de compartiment obligatoires, Amazon S3 utilise des listes de contrôle d'accès (ACL) afin de gérer l'accès aux fichiers journaux créés par un journal de flux. Par défaut, le propriétaire du compartiment dispose d'autorisations `FULL_CONTROL` sur chaque fichier journal. Si le propriétaire de la livraison des journaux n'est pas le propriétaire du compartiment, il ne dispose d'aucune autorisation. Le compte de livraison des journaux possède les autorisations `READ` et `WRITE`.

Pour de plus amples informations, veuillez consulterPrésentation de la liste de contrôle d'accès (ACL)dans leGuide de mise en route Amazon Simple Storage Service.

Activer la publication des journaux de flux sur Amazon S3

Pour activer les journaux de flux dans AWS Global Accelerator, suivez les étapes de cette procédure.

Pour activer les journaux de flux dans AWS Global Accelerator

1. Créez un compartiment Amazon S3 pour vos journaux de flux dans votre compte AWS.
2. Ajoutez la stratégie IAM requise pour l'utilisateur AWS qui active les journaux de flux. Pour plus d'informations, consultez Rôles IAM pour la publication des journaux de flux sur Amazon S3.
3. Exécutez la commande AWS CLI suivante, avec le nom du compartiment Amazon S3 et le préfixe que vous souhaitez utiliser pour vos fichiers journaux :

```
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
```

Traitement des enregistrements de journal de flux dans Amazon S3

Les fichiers journaux sont compressés. Si vous ouvrez les fichiers journaux à l'aide de la console Amazon S3, ils sont décompressés et les enregistrements de journal de flux s'affichent. Si vous téléchargez les fichiers, vous devez les décompresser pour afficher les enregistrements de journaux de flux.

Délai de distribution des fichiers journaux

AWS Global Accelerator distribue les fichiers journaux de votre accélérateur configuré jusqu'à plusieurs fois par heure. En général, un fichier journal contient des informations sur les demandes que votre accélérateur a reçues pendant une période donnée. Global Accelerator livre généralement le fichier journal correspondant à cette période à votre compartiment Amazon S3 dans l'heure qui suit les événements figurant dans le journal. Une partie ou la totalité des entrées d'un fichier journal d'une période peut parfois être retardé de 24 heures au plus. Lorsque les entrées des journaux

sont retardées, Global Accelerator les enregistre dans un fichier journal dont le nom inclut la date et l'heure de la période auxquelles les demandes se sont produites, et non la date et l'heure auxquelles le fichier a été livré.

Lors de la création d'un fichier journal, Global Accelerator consolide les informations de votre accélérateur à partir de tous les emplacements périphériques ayant reçu les demandes pendant la période couverte par le fichier journal.

Global Accelerator commence à livrer les fichiers journaux de façon fiable quatre heures environ après que vous avez activé la journalisation. Vous pourriez obtenir quelques fichiers journaux avant ce moment-là.

> **Note**
>
> Si aucun utilisateur ne se connecte à votre accélérateur pendant la période, vous ne recevez aucun fichier journal pour cette dernière.

Syntaxe des enregistrements de journaux de flux

Un enregistrement de journal de flux est une chaîne d'éléments séparés par un espace, dont le format est le suivant :

```
<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>
```

Le format Version 1.0 n'inclut pas l'identifiant VPC,`vpc_id`. Le format de la version 2.0, qui inclut`vpc_id`, est généré lorsque Global Accelerator envoie du trafic vers un point de terminaison avec la préservation de l'adresse IP du client.

Le tableau suivant décrit les champs d'un enregistrement de journal de flux.

Champ	Description
`version`	Version des journaux de flux.

Champ	Description
`aws_account_id`	ID de compte AWS pour le journal de flux
`accelerator_id`	ID de l'accélérateur pour lequel le trafic est enregistré.
`client_ip`	Adresse IPv4 source.
`client_port`	Port source.
`accelerator_ip`	Adresse IP de l'accélérateur.
`accelerator_port`	Le port de l'accélérateur.
`endpoint_ip`	Adresse IP de destination du trafic
`endpoint_port`	Port de destination du trafic
`protocol`	Numéro de protocole IANA du trafic (pour plus d'informations, consultez la page Assigned Internet Protocol Numbers).
`ip_address_type`	IPv4.
`packets`	Nombre de paquets transférés au cours de la fenêtre de capture
`bytes`	Nombre d'octets transférés au cours de la fenêtre de capture
`start_time`	Heure de début de la fenêtre de capture, en secondes Unix
`end_time`	Heure de fin de la fenêtre de capture, en secondes Unix

Champ	Description
`action`	Action associée au trafic : • `ACCEPT` : le trafic enregistré a été autorisé par les groupes de sécurité ou les listes ACL réseau. La valeur est actuellement toujours ACCEPTER.
`log-status`	Statut de journalisation du journal de flux : • `OK` : les données sont consignées normalement dans les destinations choisies. • `NODATA` : il n'y a eu aucun trafic réseau depuis ou vers l'interface réseau pendant la fenêtre de capture. • `SKIPDATA` : certains enregistrements de journaux de flux ont été ignorés pendant la fenêtre de capture. Cela peut être dû à une contrainte de capacité interne ou à une erreur interne.
`globalaccelerator_source_ip`	Adresse IP utilisée par l'interface réseau Global Accelerator.
`globalaccelerator_source_port`	Port utilisé par l'interface réseau Global Accelerator.
`endpoint_region`	Région AWS dans laquelle se trouve le point de terminaison.
`globalaccelerator_region`	Emplacement périphérique (point de présence) ayant servi la demande. Chaque emplacement périphérique dispose d'un code à trois lettres et d'un numéro attribué arbitrairement (par exemple, DFW3). Le code sur trois lettres correspond généralement au code IATA (International Air Transport Association) d'un aéroport proche de l'emplacement périphérique. (Ces abréviations peuvent changer à l'avenir.)

Champ	Description
`direction`	La direction de la circulation. Indique le trafic entrant dans le réseau Global Accelerator (`INGRESS`) ou retourner au client (`EGRESS`).
`vpc_id`	Identificateur du VPC. Inclus dans les journaux de flux de la version 2.0 lorsque Global Accelerator envoie du trafic vers un point de terminaison avec la préservation de l'adresse IP du client

Si un champ ne s'applique pas à un enregistrement spécifique, ce dernier affiche le symbole « - » pour cette entrée.

Utilisation d'Amazon CloudWatch avec AWS Global Accelerator

AWS Global Accelerator publie des points de données vers Amazon CloudWatch pour vos accélérateurs. CloudWatch vous permet de récupérer des statistiques sur ces points de données sous la forme d'un ensemble classé de données en séries chronologiques, appeléesMétriques. Considérez une métrique comme une variable à surveiller, et les points de données comme les valeurs de cette variable au fil du temps. Par exemple, vous pouvez surveiller le trafic via un accélérateur sur une période spécifiée. Un horodatage et une unité de mesure facultative sont associés à chaque point de données.

Vous pouvez utiliser les métriques pour vérifier que le système fonctionne comme prévu. Par exemple, vous pouvez créer une alarme CloudWatch pour surveiller une métrique spécifiée et initier une action (par exemple, l'envoi d'une notification à une adresse e-mail) si la métrique sort de ce que vous considérez comme une plage acceptable.

Global Accelerator ne signale des métriques à CloudWatch que lorsque les demandes passent par l'accélérateur. Si les demandes passent par l'accélérateur, Global Accelerator mesure et envoie ses métriques par intervalles de 60 secondes. Si aucune demande ne passe par l'accélérateur ou s'il n'existe pas de données pour une métrique, cette dernière n'est pas présentée.

Pour plus d’informations, consultez le Guide de l'utilisateur Amazon CloudWatch.

Sommaire

- Statistiques relatives aux métriques Global Accelerator
- Affichez les métriques CloudWatch pour vos accélérateurs

Métriques Global Accelerator

L'espace de noms `AWS/GlobalAccelerator` inclut les métriques suivantes.

Métrique	Description
`NewFlowCount`	Nombre total de nouveaux flux (ou connexions) TCP et UDP établis entre les clients et les points de terminaison pendant la période. Critères : Il existe une valeur différente de zéro. Statistiques : La seule statistique utile est`Sum`. Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`
`ProcessedBytesIn`	Nombre total d'octets entrants traités par l'accélérateur, y compris les en-têtes TCP/IP. Ce nombre inclut tout le trafic vers les terminaux. Critères : Il existe une valeur différente de zéro. Statistiques : La seule statistique utile est`Sum`. Dimensions • `Accelerator` • `Accelerator, Listener`

Métrique	Description
	• Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress
ProcessedBytesOut	Nombre total d'octets sortants traités par l'accélérateur, y compris les en-têtes TCP/IP. Ce nombre inclut le trafic depuis les terminaux, moins le trafic lié à la vérification de l'état. Critères : Il existe une valeur différente de zéro. Statistiques : La seule statistique utile estSum. Dimensions • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress

Dimensions métriques pour les

Pour filtrer les métriques pour votre accélérateur, utilisez les dimensions suivantes.

Dimension	Description
Accelerator	Filtre les données des métriques par accélérateur. Spécifiez l'accélérateur par l'identifiant de l'accélérateur (la dernière partie de l'ARN de l'accélérateur). Par exemple, si l'ARN estarn:aws:globalaccelerator::012345678901:accelerator/1234abcd-

Dimension	Description
	`abcd-1234-abcd-1234abcdefgh` , vous spécifiez ce qui suit :**`1234abcd-abcd-1234-abcd-1234abcdefgh`** .
`Listener`	Filtre les données des métriques par écouteur. Spécifiez le processus d'écoute par l'identifiant de l'écouteur (la dernière partie de l'ARN de l'écouteur). Par exemple, si l'ARN est`arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123wxyz` , vous spécifiez ce qui suit :**`0123wxyz`**.
`EndpointGroup`	Filtre les données des métriques par groupe de points de terminaison. Spécifiez le groupe de points de terminaison par la région AWS, par exemple**`us-east-1`** (toutes minuscules).
`SourceRegion`	Filtre les données de mesure par région source, c'est-à-dire la zone géographique des régions AWS où les points de terminaison de votre application s'exécutent. La région source est l'une des suivantes : • NA — États-Unis et Canada • EU — Europe • AP — Asie-Pacifique* • KR — Corée du Sud • IN — Inde • AU — Australie • ME — Moyen-Orient • SA — Amérique du Sud *Excluant la Corée du Sud et l'Inde

Dimension	Description
`DestinationEdge`	Filtre les données de mesure par limite de destination, qui correspond à la zone géographique des emplacements périphériques AWS qui desservent votre trafic client. L'extrémité de destination est l'une des suivantes : • NA — États-Unis et Canada • EU — Europe • AP — Asie-Pacifique* • KR — Corée du Sud • IN — Inde • AU — Australie • ME — Moyen-Orient • SA — Amérique du Sud • ZA — Afrique du Sud *Excluant la Corée du Sud et l'Inde
`TransportProtocol`	Filtre les données des métriques par protocole de transport : UDP ou TCP.
`AcceleratorIPAddress`	Filtre les données des métriques par l'adresse IP de l'accélérateur : c'est-à-dire l'une des adresses IP statiques attribuées à un accélérateur.

Statistiques relatives aux métriques Global Accelerator

CloudWatch fournit des statistiques basées sur les points de données métriques publiés par Global Accelerator. Les statistiques sont des regroupements de données de métrique sur une période donnée. Lorsque vous demandez des statistiques, le flux de données renvoyé est identifié par le nom et la dimension de la métrique. Une dimension est une paire nom/valeur qui identifie une métrique de manière unique. Par exemple, vous pouvez demander aux octets traités de sortir pour un accélérateur où les octets sont servis à partir d'emplacements périphériques AWS en Europe (le bord de destination est « UE »).

Voici des exemples de combinaisons métriques/dimensions que vous pourriez trouver utiles :

- Affichez le volume de trafic servi (tel que ProcessedBytesOut) par chacune de vos deux adresses IP d'accélérateur pour vérifier que votre configuration DNS est correcte.
- Visualisez la répartition géographique de votre trafic d'utilisateurs et surveillez la quantité de trafic local (par exemple, Amérique du Nord vers l'Amérique du Nord) ou mondial (par exemple, Australie ou Inde vers l'Amérique du Nord). Pour déterminer cela, affichez les mesures ProcessedBytesIn ou ProcessedBytesOut avec les dimensions DestinationEdge et SourceRegion définies sur des valeurs spécifiques.

Affichez les métriques CloudWatch pour vos accélérateurs

Vous pouvez afficher les métriques CloudWatch pour vos accélérateurs à l'aide de la console CloudWatch ou de l'interface de ligne de commande AWS. Dans la console, les métriques s'affichent sous forme de graphiques de surveillance. Les graphiques de surveillance affichent des points de données uniquement si l'accélérateur est actif et reçoit des demandes.

Vous devez afficher les métriques CloudWatch pour Global Accelerator dans la région USA West (Oregon), à la fois dans la console ou lors de l'utilisation de l'AWS CLI. Lorsque vous utilisez l'interface de ligne de commande AWS, spécifiez la région USA Ouest (Oregon) pour votre commande en incluant le paramètre suivant :`--region us-west-2`.

Pour afficher des métriques à l'aide de la console CloudWatch

1. Ouvrez la console CloudWatchhttps://us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2.
2. Dans le panneau de navigation, choisissez Métriques.
3. Sélectionnez laGlobalAcceleratorEspace de noms.
4. (Facultatif) Pour afficher une métrique pour toutes les dimensions, saisissez son nom dans le champ de recherche.

Pour afficher les métriques à l'aide de l'interface de ligne de commande AWS

Utilisez la commande list-metrics suivante pour répertorier les métriques disponibles :

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

Pour obtenir les statistiques pour une métrique à l'aide de l'AWS CLI

Utilisez le suivantget-metric-pour obtenir des statistiques pour une métrique et une dimension spécifiées. Remarque : CloudWatch traite chaque combinaison de dimensions unique comme une métrique distincte. Vous ne pouvez pas récupérer de statistiques à l'aide de combinaisons de dimensions qui n'ont pas été spécifiquement publiées. Vous devez spécifier les mêmes dimensions que celles utilisées lorsque les mesures ont été créées.

L'exemple suivant répertorie le nombre total d'octets traités en, par minute, pour votre accélérateur desservant à partir de la périphérie de destination Amérique du Nord (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
```

Voici un exemple de sortie de la commande :

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


Utilisation d'AWS CloudTrail pour journaliser les appels d'API AWS Global Accelerator

AWS Global Accelerator est intégré à AWS CloudTrail, service qui enregistre les actions effectuées par un utilisateur, un rôle ou un service AWS dans Global Accelerator. CloudTrail capture tous les appels d'API pour Global Accelerator en tant qu'événements, y compris les appels émis par la console Global Accelerator et les appels de code transmis à l'API Global Accelerator. Si vous créez un journal de suivi, vous pouvez activer la livraison continue des événements CloudTrail dans un compartiment Amazon S3, y compris les événements pour Global Accelerator. Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements).

Pour en savoir plus sur CloudTrail, consultez AWS CloudTrail User Guide.

Informations Global Accelerator dans CloudTrail

CloudTrail est activé sur votre compte AWS lorsque vous créez le compte. Quand une activité a lieu dans Global Accelerator, cette activité est enregistrée dans un événement CloudTrail avec d'autres événements de services AWS dansHistorique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour plus d'informations, consultez Affichage des événements avec l'historique des événements CloudTrail .

Pour un enregistrement continu des événements dans votre compte AWS, y compris les événements pour Global Accelerator, créez un journal de suivi. Un journal de suivi permet à CloudTrail de livrer les fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions. Le journal de suivi consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et agir sur celles-ci. Pour plus d'informations, consultez les rubriques suivantes :

- Présentation de la création d'un journal de suivi
- Intégrations et services pris en charge par CloudTrail
- Configuration des Notifications de Amazon SNS pour CloudTrail
- Réception de fichiers journaux CloudTrail de plusieurs régions et Réception de fichiers journaux CloudTrail de plusieurs comptes

Toutes les actions Global Accelerator sont enregistrées par CloudTrail et sont documentées dans la section de suiviRéférence de l'API AWS Global Accelerator. Par exemple, les appels aux`CreateAccelerator`,`ListAccelerators`and`UpdateAccelerator`génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée du journal contient des informations sur la personne qui a généré la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou IAM
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la requête a été effectuée par un autre service AWS

Pour plus d'informations, consultez la section Élément userIdentity CloudTrail.

Présentation des entrées du fichier journal Global Accelerator

Un journal de suivi est une configuration qui permet la livraison d'événements sous forme de fichiers journaux vers un compartiment Amazon S3 que vous spécifiez. Le fichier journal CloudTrail au format JSON peut contenir une ou plusieurs entrées de journal. Une entrée de journal représente une demande individuelle à partir d'une source quelconque et comprend des informations sur l'action demandée, y compris sur tous les paramètres, sur la date et l'heure de l'action, etc. Les entrées de journal ne suivent aucun ordre précis ; il ne s'agit pas d'une série ordonnée retraçant les appels aux API publics.

L'exemple suivant montre une entrée de journal CloudTrail qui inclut ces actions Global Accelerator :

- Liste des accélérateurs d'un compte :`eventNameestListAccelerators`.
- Création d'un écouteur :`eventNameestCreateListener`.
- Mette à jour un écouteur :`eventNameestUpdateListener`.
- Description d'un écouteur :`eventNameestDescribeListener`.
- Liste des auditeurs d'un compte :`eventNameestListListeners`.
- Supprimer un écouteur :`eventNameestDeleteListener`.


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

Sécurité AWS Global Accelerator

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous-même. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité dans le cloud : AWS est responsable de la protection de l'infrastructure qui exécute les services AWS dans le Cloud AWS. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. L'efficacité de notre sécurité est régulièrement testée et vérifiée par des auditeurs tiers dans le cadre des programmes de conformité AWS. Pour de plus amples informations sur les programmes de conformité qui s'appliquent à Global Accelerator, consultezServices AWS concernés par le programme de conformité.
- Sécurité dans le cloud – Votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation, et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Global Accelerator. Les rubriques suivantes vous montrent comment configurer Global Accelerator pour qu'elle réponde à vos objectifs de sécurité.

Rubriques

Identity and Access Management pour AWS Global Accelerator

AWS Identity and Access Management (IAM) est un service AWS qui permet à un administrateur de contrôler, en toute sécurité, l'accès aux ressources AWS, y compris aux ressources AWS

Global Accelerator. Les administrateurs utilisent IAM pour contrôler qui estAuthentifié(connecté) etAuthorized(dispose d'autorisations) pour utiliser les ressources Global Accelerator. IAM est une fonction incluse gratuitement dans votre compte AWS.

> **Important**
>
> Si vous n'êtes pas familiarisé avec IAM, passez en revue les informations d'introduction fournies sur cette page, puis consultezMise en route d'IAM. Si vous le souhaitez, vous pouvez en savoir plus sur l'authentification et le contrôle d'accès en consultantEn quoi consiste l'authentification ?,Qu'est-ce que le contrôle d'accès ?, etEn quoi consistent les stratégies ?.

Rubriques

- Concepts et modalités d'
- Autorisations requises pour l'accès à la console, la gestion de l'authentification et le contrôle d'accès
- Comprendre comment Global Accelerator fonctionne avec IAM
- Résolution des problèmes d'authentification et de contrôle d'accès

Concepts et modalités d'

AuthentificationPour vous connecter à AWS, vous devez utiliser l'un des éléments suivants : informations d'identification utilisateur racine (non recommandé), informations d'identification utilisateur IAM ou informations d'identification temporaires à l'aide de rôles IAM. Pour en savoir plus sur ces entités, consultez En quoi consiste l'authentification ?.

Contrôle d'accès— Les administrateurs AWS utilisent des stratégies pour contrôler l'accès aux ressources AWS, comme des accélérateurs dans Global Accelerator. Pour en savoir plus, consultez Qu'est-ce que le contrôle d'accès ? et En quoi consistent les stratégies ?.

> **Important**
>
> Toutes les ressources d'un compte appartiennent à ce compte, indépendamment de la personne qui a créé ces ressources. Vous devez recevoir une autorisation d'accès pour créer une ressource. Cependant, le simple fait que vous avez créé une ressource ne signifie pas que vous disposez automatiquement d'un accès complet à cette ressource. Un administrateur

doit accorder explicitement des autorisations pour chaque action que vous souhaitez effectuer. Cet administrateur peut aussi révoquer vos autorisations à tout moment.

Pour vous aider à comprendre les notions de base du fonctionnement d'IAM, parcourez la terminologie suivante :

Ressources

Les services AWS, comme Global Accelerator et IAM, incluent généralement des objets appelés ressources. Dans la plupart des cas, vous pouvez créer, gérer et supprimer ces ressources à partir du service. Les ressources IAM incluent des utilisateurs, des groupes, des rôles et des stratégies :

Users

Un utilisateur IAM représente la personne ou l'application qui utilise ses informations d'identification pour interagir avec AWS. Un utilisateur possède un nom et un mot de passe, avec lesquels il se connecte à AWS Management Console et jusqu'à deux clés d'accès qui peuvent être utilisées avec l'interface de ligne de commande AWS ou l'API AWS.

Groupes

Un groupe IAM est un ensemble d'utilisateurs IAM. Les administrateurs peuvent utiliser les groupes pour spécifier des autorisations aux utilisateurs qui en sont membres. Cela permet à un administrateur de gérer plus facilement les autorisations de plusieurs utilisateurs.

Roles

Un rôle IAM n'est associé à aucune information d'identification à long terme (mot de passe ou clés d'accès). Un rôle peut être endossé par tout utilisateur qui en a besoin et dispose des autorisations requises. Un utilisateur IAM peut assumer un rôle pour accepter différentes autorisations temporaires concernant un tâche spécifique. Les utilisateurs fédérés peuvent endosser un rôle à l'aide d'un fournisseur d'identité externe qui est mappé au rôle. Certains services AWS peuvent supposer unRôle de servicepour accéder aux ressources AWS en votre nom.

Policies

Les stratégies sont des documents JSON qui définissent les autorisations pour l'objet auquel elles sont attachées. AWS prend en chargeStratégies basées sur l'identitéque vous attachez aux identités (utilisateurs, groupes ou rôles). Certains services AWS vous permettent de

joindreStratégies basées sur les ressourcesAux ressources afin de contrôler les actions effectuées par un détenteur (personne ou application) sur cette ressource. Global Accelerator ne prend pas en charge les stratégies basées sur les ressource.

Identités

Identités sont des ressources IAM pour lesquelles vous pouvez définir des autorisations. Ces objets incluent les utilisateurs, les groupes et les rôles.

Entités

Les entités sont des ressources IAM que vous utilisez pour l'authentification. Ces objets incluent les utilisateurs et les rôles.

Mandataires

Dans AWS, un mandataire est une personne ou une application qui utilise une entité pour se connecter et adresser des demandes à AWS. En tant que détenteur, vous pouvez utiliser AWS Management Console, l'interface de ligne de commande AWS ou l'API AWS pour effectuer une opération (telle que la suppression d'un accélérateur). Cela crée une demande pour cette opération. Votre demande spécifie l'action, la ressource, le détenteur, le détenteur du compte et toutes les informations supplémentaires relatives à la demande. Toutes ces informations fournissent à AWScontextpour votre demande de. AWS recherche toutes les stratégies qui s'appliquent au contexte de votre demande. AWS autorise la demande uniquement si chaque partie de celle-ci est autorisée par les stratégies.

Pour afficher un schéma du processus d'authentification et de contrôle d'accès, consultezComprendre le fonctionnement d'IAMdans leGuide de l'utilisateur IAM. Pour obtenir des détails sur la façon dont AWS détermine si une demande est autorisée, consultezLogique d'évaluation des stratégiesdans leGuide de l'utilisateur IAM.

Autorisations requises pour l'accès à la console, la gestion de l'authentification et le contrôle d'accès

Pour utiliser Global Accelerator ou pour gérer l'autorisation et le contrôle d'accès pour vous-même ou pour d'autres, vous devez disposer des autorisations appropriées.

Autorisations requises pour créer un accélérateur Global Accelerator

Pour créer un accélérateur AWS Global Accelerator, les utilisateurs doivent être autorisés à créer des rôles liés au service qui sont associés à Global Accelerator.

Pour vous assurer que les utilisateurs disposent des autorisations appropriées pour créer des accélérateurs dans Global Accelerator, associez à l'utilisateur une stratégie telle que la suivante.

> **Note**
>
> Si vous créez une stratégie d'autorisations basée sur l'identité qui est plus restrictive, les utilisateurs dotés de cette stratégie ne pourront pas créer d'accélérateur.

```
{
      "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*"
    }
```

Autorisations requises pour utiliser la console Global Accelerator

Pour accéder à AWS Global Accelerator Console, vous devez disposer d'un ensemble minimal d'autorisations qui vous permet de répertorier et de consulter les informations détaillées relatives aux ressources Global Accelerator de votre compte AWS. Si vous créez une stratégie d'autorisation basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités tributaires de cette stratégie.

Pour garantir que ces entités pourront continuer à utiliser la console Global Accelerator ou les actions API, attachez également l'une des stratégies gérées par AWS à l'utilisateur, comme expliqué dansCréation de stratégies dans l'onglet JSON :

```
        GlobalAcceleratorReadOnlyAccess
        GlobalAcceleratorFullAccess
```

Joindre la première politique,`GlobalAcceleratorReadOnlyAccess`, si les utilisateurs n'ont besoin que d'afficher des informations dans la console ou d'effectuer des appels vers l'interface de ligne de commande AWS ou l'API qui utilisent`List*`ou`Describe*`.

Joindre la deuxième politique,`GlobalAcceleratorFullAccess`, aux utilisateurs qui ont besoin de créer ou de mettre à jour des accélérateurs. La politique d'accès complet inclutFULLpour Global Accelerator ainsi quedescribepour Amazon EC2 et Elastic Load Balancing.

> **Note**
>
> Si vous créez une stratégie d'autorisations basée sur l'identité qui n'inclut pas les autorisations requises pour Amazon EC2 et Elastic Load Balancing, les utilisateurs avec cette stratégie ne pourront pas ajouter des ressources Amazon EC2 et Elastic Load Balancing aux accélérateurs.

Voici la politique d'accès complet :

```
{
    "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/*"
            ]
        }
    ]
}
```

Autorisations requises pour la gestion de l'authentification

Pour gérer vos propres informations d'identification, telles que votre mot de passe, vos clés d'accès et vos périphériques d'authentification multi-facteurs (MFA), votre administrateur doit vous accorder les autorisations requises. Pour consulter la stratégie sous-tendant ces autorisations, consultez Autorise les utilisateurs à gérer eux-mêmes leurs informations d'identification.

En tant qu'administrateur AWS, vous avez besoin d'un accès total à IAM afin que vous puissiez créer et gérer des utilisateurs, des groupes, des rôles et des stratégies. Vous devez utiliser les balisesAdministratorAccessStratégie gérée par AWS qui inclut un accès complet à l'ensemble d'AWS. Cette stratégie n'autorise pas l'accès à la console AWS Billing and Cost Management, ni les tâches nécessitant des informations d'identification utilisateur racine du compte AWS. Pour de plus amples informations, veuillez consulterTâches AWS nécessitant des informations d'identification d'utilisateur racine du compte AWSdans leRéférences générales AWS.

> **Warning**
>
> Seul un utilisateur administrateur doit avoir un accès complet à AWS. Toute personne disposant de cette stratégie est autorisée à gérer entièrement l'authentification et le contrôle d'accès, en plus de pouvoir modifier chaque ressource dans AWS. Pour savoir comment créer cet utilisateur, consultez Créez votre utilisateur administrateur IAM.

Autorisations requises pour le contrôle d'accès

Si votre administrateur vous a fourni des informations d'identification d'utilisateur IAM, il a attaché des stratégies votre utilisateur IAM pour contrôler les ressources auxquelles vous avez accès. Pour afficher les stratégies attachées à votre identité d'utilisateur dans AWS Management Console, vous devez disposer des autorisations suivantes :

```
{
    "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 vous avez besoin d'autorisations supplémentaires, demandez à votre administrateur de mettre à jour vos stratégies pour vous permettre d'accéder aux actions nécessaires.

Comprendre comment Global Accelerator fonctionne avec IAM

Les services peuvent fonctionner avec IAM de différentes manières :

Actions

Global Accelerator prend en charge l'utilisation d'actions dans une stratégie. Cela permet à un administrateur de contrôler si une entité peut effectuer une opération dans Global Accelerator. Par exemple, pour permettre à une entité d'appeler le`GetPolicy`AWS afficher une stratégie, un administrateur doit attacher une stratégie qui autorise le`iam:GetPolicy`action.

L'exemple de stratégie qui suit permet à un utilisateur d'effectuer le`CreateAccelerator`pour créer par programme un accélérateur pour votre compte AWS :

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

```
            ],
            "Resource":"*"
        }
    ]
}
```

Autorisations de niveau ressource

Global Accelerator prend en charge les autorisations au niveau des ressources. Les autorisations au niveau des ressources vous permettent d'utiliser les ARN pour spécifier des ressources spécifiques dans la stratégie.

Stratégies basées sur les ressources

Global Accelerator ne prend pas en charge les stratégies basées sur les ressource. Avec les stratégies basées sur les ressources, vous pouvez attacher une stratégie à une ressource du service. Les stratégies basées sur les ressources comprennent un`Principal`élément pour spécifier les identités IAM qui peuvent accéder à cette ressource.

Autorisation basée sur les balises

Global Accelerator prend en charge les balises basées sur l'autorisation. Cette fonction vous permet d'utiliser des balises de ressource dans la condition d'une stratégie.

Informations d'identification temporaires

Global Accelerator prend en charge l'identification temporaire. Avec les informations d'identification temporaires, vous pouvez vous connecter à l'aide de la fédération, endosser un rôle IAM ou endosser un rôle entre comptes. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d'API AWS STS comme`AssumeRole`ou`GetFederationToken`.

Rôles liés à un service

Global Accelerator prend en charge les rôles liés à un service. Cette fonction permet à un service d'endosser un rôle lié à un service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Rôles de service

Global Accelerator ne prend pas en charge les rôles de service. Cette fonctionnalité permet à un service d'endosser un rôle de service en votre nom. Ce rôle autorise le service à accéder

à des ressources d'autres services pour effectuer une action en votre nom. Les rôles de service s'affichent dans votre compte IAM et sont la propriété du compte. Cela signifie qu'un administrateur IAM peut modifier les autorisations associées à ce rôle. Toutefois, cela peut perturber le bon fonctionnement du service.

Résolution des problèmes d'authentification et de contrôle d'accès

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec IAM.

Rubriques

- Je ne suis pas autorisé à exécuter une action dans Global Accelerator
- Je suis un administrateur et je veux autoriser d'autres utilisateurs à accéder à Global Accelerator
- Je veux comprendre IAM sans devenir un expert

Je ne suis pas autorisé à exécuter une action dans Global Accelerator

Si AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter l'administrateur qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple suivant se produit lorsqu'un utilisateur IAM nommémy-user-nametente d'utiliser la console pour effectuerglobalaccelerator:CreateAcceleratormais n'a pas d'autorisations :

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

Dans ce cas, demandez à votre administrateur de mettre à jour vos stratégies pour vous permettre d'accéder à l'my-example-acceleratorà l'aide de l'outilaws-globalaccelerator:CreateAcceleratoraction.

Je suis un administrateur et je veux autoriser d'autres utilisateurs à accéder à Global Accelerator

Pour permettre à d'autres utilisateurs d'accéder à Global Accelerator, vous devez créer une entité IAM (utilisateur ou rôle) pour la personne ou l'application nécessitant un accès. Ils utiliseront les informations d'identification de cette entité pour accéder à AWS. Vous devez ensuite associer une stratégie à l'entité qui leur accorde les autorisations appropriées dans Global Accelerator.

Pour démarrer immédiatement, consultez Mise en route d'IAM.

Je veux comprendre IAM sans devenir un expert

Pour en savoir plus sur les conditions, les concepts et les procédures IAM, consultez les rubriques suivantes :

- En quoi consiste l'authentification ?
- Qu'est-ce que le contrôle d'accès ?
- En quoi consistent les stratégies ?

Stratégies basées sur balises

Lorsque vous concevez des stratégies IAM, vous pouvez définir des autorisations granulaires en accordant l'accès à des ressources spécifiques. Au fur et à mesure que le nombre de ressources que vous gérez s'accroît, cette tâche devient plus difficile. Le balisage des accélérateurs et l'utilisation de balises dans les déclarations de stratégie peuvent rendre cette tâche plus facile. Vous accordez l'accès en bloc à tout accélérateur doté d'une balise spécifique. Puis, vous appliquez cette balise à plusieurs reprises aux accélérateurs correspondants, lorsque vous créez l'accélérateur ou en mettant à jour l'accélérateur ultérieurement.

> **Note**
>
> L'utilisation des balises dans les conditions est un moyen de contrôler l'accès aux ressources et demandes. Pour plus d'informations sur le balisage dans Global Accelerator, consultezBalisage dans AWS Global Accelerator.

Les balises peuvent être attachées à une ressource ou transmises dans la demande aux services qui prennent en charge le balisage. Dans Global Accelerator, seuls les accélérateurs peuvent inclure des balises. Lorsque vous créez une stratégie IAM, vous pouvez utiliser des clés de condition de balise pour contrôler :

- quels utilisateurs peuvent effectuer des actions sur un accélérateur, en fonction des balises qu'il possède déjà ;
- quelles balises peuvent être transmises dans une demande d'action ;
- si des clés de balise spécifiques peuvent être utilisées dans une demande.

Pour connaître la syntaxe complète et la sémantique des clés de condition de balise, consultezContrôle des accès à l'aide de balises IAMdans leGuide de l'utilisateur IAM.

Par exemple, l'accélérateur global`GlobalAcceleratorFullAccess`Stratégie utilisateur gérée fournit aux utilisateurs les autorisations complètes nécessaires pour effectuer une action globale Accelerator sur une ressource. La stratégie suivante refuse aux utilisateurs non autorisés l'autorisation d'effectuer une action d'accélérateur mondial sur lesProductionAccélérateurs. L'administrateur d'un client peut attacher cette stratégie IAM aux utilisateurs IAM non autorisés et à la stratégie d'utilisateur gérée.

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

Rôle lié à un service pour Global Accelerator

AWS Global Accelerator utilise un AWS Identity and Access Management (IAM)Rôle lié à un service. Un rôle lié à un service est un type unique de rôle IAM lié directement à un service. Les rôles liés

à un service sont prédéfinis par le service et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom.

Global Accelerator utilise le rôle lié à un service IAM suivant :

- AWSServiceRoleForGlobalAccelerator : Global Accelerator utilise ce rôle pour permettre à Global Accelerator de créer et de gérer les ressources nécessaires à la préservation des adresses IP du client.

Global Accelerator crée automatiquement un rôle nommé AWSServiceRoleForGlobalAccelerator lorsque le rôle est nécessaire pour prendre en charge une opération API Global Accelerator. Le rôle AWSServiceRoleForGlobalAccelerator permet à Global Accelerator de créer et de gérer les ressources nécessaires à la préservation des adresses IP du client. Ce rôle est requis pour utiliser des accélérateurs dans Global Accelerator. L'ARN du rôle AWSServiceRoleForGlobalAccelerator se présente sous la forme suivante :

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

Un rôle lié à un service simplifie la configuration et l'utilisation de l'accélérateur mondial, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Global Accelerator définit les autorisations de son rôle lié un service et seul l'Accélérateur mondial peut endosser ces rôles. Les autorisations définies comprennent la stratégie d'approbation et la stratégie d'autorisations. La stratégie d'autorisations ne peut pas être attachée à une autre entité IAM.

Vous devez supprimer toute ressource Global Accelerator associée pour pouvoir supprimer un rôle lié à un service. Cela vous aide à protéger vos ressources Global Accelator en assurant que vous ne supprimez pas un rôle lié à un service qui est toujours exigé pour accéder aux ressources actives.

Pour de plus amples informations sur les autres services qui prennent en charge les rôles liés à un service, veuillez consulter Services AWS qui fonctionnent avec IAM et recherchez les services qui comportent Oui dans la colonne Rôle lié à un service.

Autorisations des rôles liés à un service pour Global Accelerator

Global Accelerator utilise un rôle lié à un service nomméAWSServiceRoleForGlobalAccelerator. Les sections suivantes décrivent comment gérer les autorisations pour le rôle.

Autorisations de rôles liés à un service

Ce rôle lié au service permet à Global Accelerator de gérer les interfaces réseau Elastic EC2 et les groupes de sécurité, et de vous aider à diagnostiquer les erreurs.

Le rôle lié à un service AWSServiceRoleForGlobalAccelerator approuve le service suivant pour assumer le rôle :

- `globalaccelerator.amazonaws.com`

La stratégie d'autorisations liée au rôle permet à Global Accelerator d'effectuer les actions suivantes sur les ressources spécifiées, comme indiqué dans la stratégie :

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

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

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, groupe ou rôle) de supprimer le rôle lié à un service Global Accelerator. Pour de plus amples informations, veuillez consulter Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM

Création du rôle lié à un service pour Global Accelerator

Vous ne créez pas manuellement le rôle lié à un service pour Global Accelerator. Le service crée le rôle pour vous automatiquement la première fois que vous créez un accélérateur. Si vous supprimez vos ressources Global Accelator et supprimez le rôle lié à un service, le service crée de nouveau automatiquement le rôle lorsque vous créez un nouvel accélérateur.

Modification du rôle lié à un service Global Accelerator

Global Accelerator ne vous permet pas de modifier le rôle lié à un service AWSServiceRoleForGlobalAccelerator. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent y faire référence. Néanmoins, vous pouvez modifier la description d'un rôle à l'aide d'IAM. Pour de plus amples informations, veuillez consulter Modification d'un rôle lié à un service dans le Guide de l’utilisateur IAM.

Suppression du rôle lié à un service Global Accelerator

Si vous n'avez plus besoin d'utiliser Global Accelerator, nous vous recommandons de supprimer le rôle lié à un service. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources Global Accelerator dans votre compte pour pouvoir supprimer manuellement les rôles.

Une fois que vous avez désactivé et supprimé vos accélérateurs, vous pouvez supprimer le rôle lié à un service. Pour plus d'informations sur la suppression des accélérateurs, consultezCréation ou mise à jour d'un accélérateur standard.

> **Note**
>
> Si vous avez désactivé et supprimé vos accélérateurs mais que Global Accelator n'a pas terminé la mise à jour, la suppression du rôle lié à un service peut échouer. Si cela se produit, patientez quelques minutes, puis réessayez.

Pour supprimer manuellement le rôle lié au service AWSServiceRoleForGlobalAccelerator

1. Connectez-vous à AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de la console IAM, choisissez Rôles. Cochez ensuite la case en regard du nom du rôle que vous souhaitez supprimer, sans sélectionner le nom ou la ligne.
3. Pour les actions sur les Rôle en haut de la page, sélectionnez Supprimer.
4. Dans la boîte de dialogue de confirmation, vérifiez les dernières données consultées dans le service. Elles indiquent quels rôles, parmi ceux sélectionnés, ont accédé en dernier à un service AWS. Cela vous permet de confirmer si le rôle est actif actuellement. Si vous souhaitez continuer, sélectionnez Oui, supprimer pour lancer la tâche de suppression du rôle.
5. Consultez les notifications de la console IAM pour surveiller la progression de la suppression du rôle lié à un service. Dans la mesure où la suppression du rôle lié à un service IAM est asynchrone, une fois que vous soumettez le rôle afin qu'il soit supprimé, la suppression peut réussir ou échouer. Pour de plus amples informations, veuillez consulter Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Mises à jour du rôle lié au service Global Accelerator (stratégie gérée par AWS)

Consultez les détails sur les mises à jour du rôle lié au service depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques sur les modifications apportées à cette page, abonnez-vous au flux RSS sur AWS Global AcceleratorHistorique du document.

Modification	Description	Date
AWSServiceRoleForGlobalAccelerator— Stratégie mise à jour	Global Accelerator a ajouté une nouvelle autorisation pour aider Global Accelerator à diagnostiquer les erreurs. Global Accelerator utiliseec2:DescribeRegions pour déterminer la région AWS dans laquelle se trouve un client, ce qui peut aider Global Accelerator à résoudre les erreurs.	18 mai 2021
Global Accelerator a commencé à suivre les modifications	Global Accelerator a commencé à suivre les modifications de ses stratégies gérées par AWS.	18 mai 2021

Régions prises en charge pour les rôles liés à un service Global Accelerator

Global Accelerator prend en charge l'utilisation des rôles liés à un service dans les régions AWS où Global Accelerator est pris en charge.

Pour obtenir la liste des régions AWS dans lesquelles Global Accelerator et d'autres services sont actuellement pris en charge, consultez laTable des régions AWS.

Présentation de l'accès et de l'authentification

Si vous découvrez IAM, lisez les rubriques suivantes pour démarrer avec l'autorisation et l'accès dans AWS.

Rubriques

En quoi consiste l'authentification ?

L'authentification correspond au processus par lequel vous vous vous connectez à AWS via vos informations d'identification.

> **Note**
>
> Pour démarrer rapidement, vous pouvez ignorer cette section. Tout d'abord, prenez connaissance des informations d'introduction surIdentity and Access Management pour AWS Global Accelerator, puis consultezMise en route d'IAM.

En tant que mandataire, vous devezAuthentifié(connecté à AWS) à l'aide d'une entité (utilisateur racine, utilisateur IAM ou rôle IAM) pour envoyer une demande à AWS. Un utilisateur IAM peut disposer d'informations d'identification à long terme, comme un nom d'utilisateur et un mot de passe ou un ensemble de clés d'accès. Lorsque vous endossez un rôle IAM, vous recevez des informations d'identification de sécurité temporaires.

Pour vous authentifier à partir de AWS Management Console en tant qu'utilisateur, vous devez vous connecter à l'aide de votre nom d'utilisateur et de votre mot de passe. Pour vous authentifier à partir de l'interface de ligne de commande AWS ou de l'API AWS, vous devez fournir votre clé d'accès et votre clé secrète ou des informations d'identification temporaires. AWS fournit un kit de développement logiciel (SDK) et des outils de CLI pour signer de façon cryptographique votre demande à l'aide de vos informations Si vous n'utilisez pas les outils AWS, vous devez signer la demande vous-même. Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être également fournir des informations de sécurité supplémentaires. Par exemple, AWS vous

recommande d'utiliser l'authentification multi-facteurs (MFA) pour améliorer la sécurité de votre compte.

En tant que mandataire, vous pouvez vous connecter à AWS à l'aide des entités suivantes (utilisateurs ou rôles) :

Utilisateur racine d'un compte AWS

Lorsque vous créez un compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les services et ressources AWS du compte. Cette identité est appelée utilisateur racine du compte AWS et elle est accessible après connexion à l'aide de l'adresse e-mail et du mot de passe utilisés pour la création du compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Respectez plutôt la bonne pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier utilisateur IAM. Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les uniquement pour effectuer certaines tâches de gestion des comptes et des services.

Utilisateur IAM

UnUtilisateur IAMest une entité au sein de votre compte AWS qui dispose d'autorisations spécifiques. prend en charge Global AccelerSignature Version 4, protocole permettant l'authentification des demandes d'API entrantes. Pour de plus amples informations sur l'authentification des demandes, veuillez consulter Processus de signature Signature Version 4 dans les Références générales AWS.

Rôle IAM

UnRôle IAMest une identité IAM que vous pouvez créer dans votre compte et qui dispose d'autorisations spécifiques. Un rôle IAM est similaire à un utilisateur IAM, car il s'agit d'une identité AWS avec des stratégies d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire dans AWS. En revanche, au lieu d'être associé de manière unique à une personne, un rôle est conçu pour être assumé par tout utilisateur qui en a besoin. En outre, un rôle ne dispose pas d'informations d'identification standard à long-terme comme un mot de passe ou des clés d'accès associées. Au lieu de cela, lorsque vous adoptez un rôle, il vous fournit des informations d'identification de sécurité temporaires pour votre session de rôle. Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

Accès d'utilisateurs fédérés

Au lieu de créer un utilisateur IAM, vous pouvez utiliser des identités existantes provenant d'AWS Directory Service, de votre annuaire utilisateur d'entreprise ou d'un fournisseur

d'identités web. Ces derniers sont appelés utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé par le biais d'un fournisseur d'identité. Pour de plus amples informations sur les utilisateurs fédérés, veuillez consulter Utilisateurs fédérés et rôles dans le Guide de l'utilisateur IAM.

Autorisations utilisateur temporaires

Un utilisateur IAM peut assumer un rôle temporaire pour accepter différentes autorisations différentes concernant un tâche spécifique.

Permettre l'accès entre comptes

Vous pouvez utiliser un rôle IAM pour permettre à un mandataire de confiance d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès entre plusieurs comptes. Toutefois, certains services AWS vous permettent d'attacher une stratégie directement à une ressource (au lieu d'utiliser un rôle en tant que proxy). Global Accelerator ne prend pas en charge ces stratégies basées sur les ressource. Pour plus d'informations sur le choix d'une stratégie basée sur un rôle ou sur une stratégie pour autoriser l'accès entre comptes, consultez Contrôle de l'accès aux mandataires sur un compte différent.

Accès d'un service AWS

Un rôle de service est unRôle IAMqu'un service assume pour effectuer des actions en votre nom. Les rôles de service fournissent un accès uniquement au sein de votre compte et ne peuvent pas être utilisés pour accorder l'accès à des services dans d'autres comptes. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus de plus amples informations, veuillez consulter Création d'un rôle pour la délégation d'autorisations à un service AWS dans le Guide de l'utilisateur IAM.

Applications qui s'exécutent sur Amazon EC2

Vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications s'exécutant sur une instance EC2 et effectuant des demandes par l'interface de ligne de commande ou par des API AWS. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour de plus amples informations, veuillez consulter Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Qu'est-ce que le contrôle d'accès ?

Une fois que vous êtes connecté (authentifié) à AWS, votre accès aux ressources et opérations AWS est régi par des stratégies. Le contrôle d'accès est également connu sous le nom d'autorisation.

> **Note**
>
> Pour démarrer rapidement, vous pouvez ignorer cette page. Tout d'abord, prenez connaissance des informations d'introduction surIdentity and Access Management pour AWS Global Accelerator, puis consultezMise en route d'IAM.

Au cours de l'autorisation, AWS utilise les valeurs de lacontexte de la demandepour vérifier les stratégies applicables à cette dernière. Ensuite, il utilise les stratégies pour déterminer s'il autorise ou refuse la demande. La plupart des stratégies sont stockées dans AWS sous forme de documents JSON et spécifient les autorisations accordées ou refusées aux mandataires. Pour plus d'informations sur la structure et le contenu des documents de stratégie JSON, consultez En quoi consistent les stratégies ?.

Les stratégies permettent à un administrateur de spécifier qui a accès aux ressources AWS et les actions pouvant être exécutées sur ces ressources. Chaque entité IAM (utilisateur ou rôle) démarre sans autorisation. En d'autres termes, par défaut, les utilisateurs ne peuvent rien faire, pas même afficher leurs propres clés d'accès. Pour autoriser un utilisateur à effectuer une opération, un administrateur doit associer une stratégie d'autorisations à ce dernier. Il peut également ajouter l'utilisateur à un groupe disposant des autorisations prévues. Lorsqu'un administrateur accorde des autorisations à un groupe, tous les utilisateurs de ce groupe obtiennent ces autorisations.

Vous possédez peut-être des informations d'identification valides pour authentifier vos demandes, mais vous ne pouvez pas créer de ressources AWS Global Accelerator ni y accéder, à moins qu'un administrateur vous ait accordé les autorisations requises. Par exemple, vous devez disposer d'autorisations explicites pour créer un accélérateur AWS Global Accelerator.

En tant qu'administrateur, vous pouvez rédiger une stratégie pour contrôler l'accès à ce qui suit :

- Mandataires— Contrôle de ce que la personne ou l'application à l'origine de la demande (leprincipal) est autorisé à faire.
- Identités IAM— Contrôlez à quelles identités IAM (groupes, utilisateurs et rôles) il est possible d'accéder et comment y accéder.

- Stratégies IAMContrôlez qui peut créer, modifier et supprimer les stratégies gérées par les clients, et qui peut attacher et détacher toutes les stratégies gérées.
- Ressources AWS— Contrôle qui a accès aux ressources à l'aide d'une stratégie basée sur les identités ou sur les ressources.
- Comptes AWS— Contrôlez si une demande est autorisée uniquement pour les membres d'un compte spécifique.

Contrôle de l'accès pour les mandataires

Les stratégies d'autorisation contrôlent ce que vous, en tant que mandataire, êtes autorisé à faire. Un administrateur doit associer une stratégie d'autorisation basée sur une identité à l'identité (utilisateur, groupe ou rôle) qui fournit vos autorisations. Les stratégies d'autorisation autorisent ou refusent l'accès à AWS. Les administrateurs peuvent également définir une limite d'autorisations pour une entité IAM (utilisateur ou rôle) afin de déterminer le nombre maximum d'autorisations qu'une entité peut détenir. Les limites d'autorisations constituent une fonctionnalité IAM avancée. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des identités IAM dans le Guide de l'utilisateur IAM.

Pour plus d'informations et obtenir un exemple de la façon de contrôler l'accès AWS pour les mandataires, consultezContrôle de l'accès pour les mandatairesdans leGuide de l'utilisateur IAM.

Contrôle de l'accès aux identités

Les administrateurs contrôlent vos opérations sur une identité IAM (utilisateur, groupe ou rôle) en créant une stratégie qui limite les opérations susceptibles d'être effectuées sur une identité ou les autorisations d'accès. Ensuite, ils attachent cette stratégie à l'identité qui fournit vos autorisations.

Par exemple, un administrateur peut vous permettre de réinitialiser le mot de passe pour trois utilisateurs spécifiques. Pour ce faire, associez à votre utilisateur IAM une stratégie qui vous permet de réinitialiser le mot de passe uniquement pour vous-même et pour les utilisateurs disposant de l'ARN des trois utilisateurs spécifiés. Cela vous permet de réinitialiser le mot de passe des membres de votre équipe, mais pas celui des autres utilisateurs IAM.

Pour plus d'informations et pour obtenir un exemple d'utilisation d'une stratégie pour contrôler l'accès AWS aux identités, consultezContrôle de l'accès aux identitésdans leGuide de l'utilisateur IAM.

Contrôle de l'accès aux stratégies

Les administrateurs peuvent contrôler les personnes autorisées à créer, modifier et supprimer les stratégies gérées par les clients, et celles autorisées à attacher et détacher toutes les stratégies gérées. Lorsque vous examinez une stratégie, vous pouvez consulter le récapitulatif de la stratégie, lequel inclut un récapitulatif du niveau d'accès pour chaque service de cette stratégie. AWS classe chaque action de service dans l'une des quatreNiveau d'accèsen fonction de ce que chaque action fait :`List`,`Read`,`Write`, ou`Permissions management`. Vous pouvez utiliser ces niveaux d'accès pour déterminer les actions à inclure dans vos stratégies. Pour de plus amples informations, veuillez consulterPrésentation des récapitulatifs de niveau d'accès au sein des récapitulatifs de stratégiesdans leGuide de l'utilisateur IAM.

> **Warning**
>
> Vous devez limiter`Permissions Management`Autorisations au niveau de l'accès dans votre compte. Dans le cas contraire, les membres de votre compte peuvent créer des stratégies pour eux-mêmes avec plus d'autorisations qu'ils ne devraient en avoir. Ou ils peuvent créer des utilisateurs distincts disposant d'un accès complet à AWS.

Pour plus d'informations et obtenir un exemple de la façon de contrôler l'accès AWS aux stratégies, consultezContrôle de l'accès aux stratégiesdans leGuide de l'utilisateur IAM.

Contrôle de l'accès aux ressources

Les administrateurs peuvent contrôler l'accès aux ressources à l'aide d'une stratégie basée sur les identités ou sur les ressources. Dans le cadre d'une stratégie basée sur les identités, vous attachez la stratégie à une identité et vous spécifiez à quelles ressources cette identité peut accéder. Dans le cadre d'une stratégie basée sur les ressources, vous attachez une stratégie à la ressource que vous souhaitez contrôler. Dans la stratégie, vous spécifiez quels mandataires peuvent accéder à cette ressource.

Pour de plus amples informations, veuillez consulterContrôle de l'accès aux ressourcesdans leGuide de l'utilisateur IAM.

Les créateurs de ressources n'ont pas automatiquement les autorisations

Toutes les ressources d'un compte appartiennent à ce compte, indépendamment de la personne qui a créé ces ressources. L'utilisateur racine du compte AWS est le propriétaire du compte et, par conséquent,a l'autorisation d'effectuer une action sur une ressource du compte.

> **Important**
>
> Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Au lieu de cela, suivez leMeilleure pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier utilisateur IAM. Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les uniquement pour effectuer certaines tâches de gestion des comptes et des services. Pour afficher les tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur racine, consultezTâches AWS nécessitant un utilisateur racine.

Les entités (utilisateurs ou rôles) du compte AWS doivent obtenir un accès pour créer une ressource. Cependant, le simple fait qu'ils créent une ressource ne signifie pas qu'ils disposent automatiquement d'un accès complet à cette ressource. Les administrateurs doivent accorder explicitement ces autorisations lors de chaque action. En outre, les administrateurs peuvent révoquer ces autorisations à tout moment, tant qu'ils disposent d'un accès pour gérer les autorisations relatives aux utilisateurs et aux rôles.

Contrôle de l'accès aux mandataires sur un compte différent

Les administrateurs peuvent utiliser des stratégies AWS basées sur les ressources, des rôles entre comptes IAM ou le service AWS Organizations pour permettre aux mandataires d'un autre compte d'accéder aux ressources de votre compte.

Pour certains services AWS, les administrateurs peuvent accorder un accès entre comptes à vos ressources. Pour cela, un administrateur attache une stratégie directement à la ressource qu'il souhaite partager, au lieu d'utiliser un rôle en tant que proxy. Si le service prend en charge ce type de stratégie, la ressource partagée par l'administrateur doit également prendre en charge les stratégies basées sur une ressource. Contrairement à une stratégie basée sur un utilisateur, une stratégie basée sur une ressource spécifie qui (sous forme de liste de numéros d'ID de compte AWS) peut accéder à cette ressource. Global Accelerator ne prend pas en charge les stratégies basées sur les ressource.

L'accès entre comptes avec une stratégie basée sur les ressources présente certains avantages comparée à un rôle. Avec une ressource accessible via une stratégie basée sur une ressource, le mandataire (personne ou application) continue d'utiliser le compte approuvé sans devoir renoncer à ses autorisations d'utilisateur au profit des autorisations de rôle. En d'autres termes, le mandataire a en même temps accès aux ressources du compte approuvé et du compte d'approbation. Cela

est utile pour les tâches de copie d'informations d'un compte à un autre. Pour plus d'informations sur l'utilisation des rôles entre comptes, consultezFournissez l'accès à un utilisateur IAM à un autre compte AWS vous appartenantdans leGuide de l'utilisateur IAM.

AWS Organizations (Organisations AWS) offre une gestion basée sur une stratégie pour plusieurs comptes AWS vous appartenant. Grâce à Organizations, vous pouvez créer des groupes de comptes, automatiser la création de compte et appliquer et gérer des stratégies pour ces groupes. Organizations vous permettent de gérer, de manière centralisée, les stratégies de plusieurs comptes, sans avoir besoin de scripts personnalisés et de processus manuels. Grâce AWS Organizations, vous pouvez créer des politiques de contrôles de services (SCP) qui régissent un service de manière centralisée sur plusieurs comptes AWS. Pour de plus amples informations, veuillez consulterQu'est-ce qu'AWS Organizations ?dans leGuide de l'utilisateur AWS Organizations.

En quoi consistent les stratégies ?

Vous pouvez contrôler l'accès dans AWS en créant des stratégies et en les attachant à des identités IAM ou à des ressources AWS.

> **Note**
>
> Pour démarrer rapidement, vous pouvez ignorer cette page. Tout d'abord, prenez connaissance des informations d'introduction surIdentity and Access Management pour AWS Global Accelerator, puis consultezMise en route d'IAM.

Une stratégie est un objet dans AWS qui, lorsqu'attaché à une identité ou à une ressource, définit ses autorisations. AWS évalue ces stratégies lorsqu'un mandataire, tel qu'un utilisateur, envoie une requête. Les autorisations dans les stratégies déterminent si la demande est autorisée ou refusée. La plupart des stratégies sont stockées dans AWS en tant que documents JSON.

Les stratégies IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, si une stratégie autorise leGetUserL'action, un utilisateur disposant de cette stratégie peut obtenir des informations utilisateur à partir d'AWS Management Console, de l'interface de ligne de commande AWS ou de l'API AWS. Lorsque vous créez un utilisateur IAM, vous pouvez le configurer pour qu'il autorise la console ou un accès par programme. L'utilisateur IAM peut se connecter à la console à l'aide d'un nom d'utilisateur et d'un mot de passe. Ou il peut utiliser des clés d'accès avec l'interface de ligne de commande ou l'API.

Les types de stratégie suivants, répertoriés par ordre de fréquence, peuvent affecter l'autorisation d'une demande. Pour plus d'informations, consultez .Types de stratégiedans leGuide de l'utilisateur IAM.

Stratégies basées sur l'identité

Vous pouvez attacher des stratégies gérées et en ligne à des identités IAM (utilisateurs, groupes auxquels appartiennent des utilisateurs et rôles).

Stratégies basées sur les ressources

Vous pouvez attacher des stratégies en ligne aux ressources de certains services AWS. Les exemples les plus courants de stratégies basées sur les ressources sont les stratégies de compartiment Amazon S3 et les stratégies d'approbation de rôle IAM. Global Accelerator ne prend pas en charge les stratégies basées sur les ressource.

Organizations SCP

Vous pouvez utiliser une stratégie de contrôle de service (SCP) pour appliquer une limite d'autorisations à une organisation ou à une unité d'organisation AWS Organizations. Ces autorisations sont appliquées à toutes les entités des comptes membres.

Listes de contrôle d'accès (ACL)

Vous pouvez utiliser des listes de contrôle d'accès pour contrôler les mandataires pouvant accéder à une ressource. Les listes de contrôle d'accès sont semblables aux stratégies basées sur les ressources, bien qu'elles soient le seul type de stratégie qui n'utilise pas la structure d'un document de stratégie JSON. Global Accelerator prend en charge les listes de contrôle d'accès.

Ces types de stratégie peuvent être classées par stratégies d'autorisations ou limites d'autorisations.

Stratégies d'autorisations

Vous pouvez attacher des stratégies d'autorisation à une ressource dans AWS pour définir les autorisations de cet objet. Dans un seul compte, AWS évalue l'ensemble des stratégies d'autorisations. Les stratégies d'autorisations sont les plus courantes. Vous pouvez utiliser les types de stratégie suivants en tant que stratégies d'autorisations :

Stratégies basées sur l'identité

Lorsque vous attachez une stratégie gérée ou en ligne à un utilisateur, groupe ou rôle IAM, la stratégie définit les autorisations pour cette entité.

Stratégies basées sur les ressources

Lorsque vous attachez un document de stratégie JSON à une ressource, vous définissez les autorisations pour cette ressource. Le service doit prendre en charge les stratégies basées sur les ressources.

Listes de contrôle d'accès (ACL)

Lorsque vous attachez une liste de contrôle d'accès à une ressource, vous définissez une liste de mandataires disposant d'une autorisation pour accéder à cette ressource. La ressource doit prendre en charge les listes de contrôle d'accès.

Limites d'autorisations

Vous pouvez utiliser les stratégies pour définir la limite d'autorisations d'une entité (utilisateur ou rôle). Une limite d'autorisations contrôle les autorisations maximum dont une entité peut disposer. Les limites d'autorisations constituent une fonctionnalité AWS avancée. Lorsque plusieurs limites d'autorisations s'appliquent à une demande, AWS évalue séparément chaque limite d'autorisations. Vous pouvez appliquer une limite d'autorisations dans les cas suivants :

Organisations

Vous pouvez utiliser une stratégie de contrôle de service (SCP) pour appliquer une limite d'autorisations à une organisation ou à une unité d'organisation AWS Organizations.

Utilisateurs ou rôles IAM

Vous pouvez utiliser une stratégie gérée pour la limite d'autorisations d'un utilisateur ou d'un rôle. Pour de plus amples informations, veuillez consulterLimites d'autorisations pour les entités IAMdans leGuide de l'utilisateur IAM.

Rubriques

- Stratégies basées sur l'identité
- Stratégies basées sur les ressources
- Classification des niveaux d'accès aux politiques

Stratégies basées sur l'identité

Vous pouvez attacher des stratégies à des identités IAM. Par exemple, vous pouvez effectuer les opérations suivantes :

Attacher une stratégie d'autorisation à un utilisateur ou à un groupe de votre compte

Pour accorder à un utilisateur les autorisations lui permettant de créer une ressource AWS Global Accelerator, telle qu'un accélérateur, vous pouvez attacher une stratégie d'autorisations à un utilisateur ou à un groupe auquel l'utilisateur appartient.

Attacher une stratégie d'autorisation à un rôle (accorder des autorisations entre comptes)

Vous pouvez attacher une stratégie d'autorisation basée sur une identité à un rôle IAM pour accorder des autorisations entre comptes. Par exemple, l'administrateur dans le compte A peut créer un rôle pour accorder des autorisations entre comptes à un autre compte AWS (par exemple, le compte B) ou à un service AWS comme suit :

1. L'administrateur du Compte A crée un rôle IAM et attache une stratégie d'autorisation à ce rôle qui accorde des autorisations sur les ressources dans le compte A.
2. L'administrateur du compte A lie une stratégie d'approbation au rôle identifiant le compte B comme mandataire pouvant assumer ce rôle.
3. L'administrateur du compte B peut alors déléguer des autorisations pour assumer le rôle à tous les utilisateurs figurant dans le compte B. Les utilisateurs du compte B sont ainsi autorisés à créer des ressources ou à y accéder dans le compte A. Le mandataire dans la stratégie d'approbation peut également être un mandataire de service AWS si vous souhaitez accorder à un service AWS des autorisations pour assumer ce rôle.

Pour plus d'informations sur l'utilisation d'IAM pour déléguer des autorisations, consultezGestion des accèsdans leGuide de l'utilisateur IAM.

Pour de plus amples informations sur les utilisateurs, les groupes, les rôles et les autorisations, veuillez consulter Identités (utilisateurs, groupes et rôles) dans le Guide de l'utilisateur IAM.

Voici deux exemples de stratégies que vous pouvez utiliser avec Global Accelerator. Le premier exemple de stratégie accorde à un utilisateur un accès programmatique à toutes les actions List et Descrive pour les accélérateurs de votre compte AWS :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "globalaccelerator:List*",
                "globalaccelerator:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

L'exemple suivant accorde un accès programmatique au`ListAccelerators`fonctionnements :

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

Stratégies basées sur les ressources

Les stratégies basées sur les ressources sont des documents de stratégie JSON que vous attachez à une ressource. Ces stratégies vous permettent de spécifier les actions qu'un mandataire spécifique peut effectuer sur cette ressource et dans quelles conditions. La stratégie basée sur les ressource la plus courante est pour un compartiment Amazon S3. Les stratégies basées sur les ressources sont des stratégies en ligne qui existent uniquement au niveau de la ressource. Il ne s'agit pas de stratégies gérées basées sur les ressources.

Attribuer des autorisations aux membres d'autres comptes AWS à l'aide d'une stratégie basée sur une ressource présente des avantages par rapport à un rôle IAM. Pour de plus amples informations, veuillez consulter Différence entre les rôles IAM et les stratégies basées sur les ressources dans le Guide de l’utilisateur IAM.

Classification des niveaux d'accès aux politiques

Dans la console IAM, les actions sont regroupés grâce aux classification par niveau d'accès suivantes :

List

Fournit l'autorisation de répertorier les ressources au sein du service afin de déterminer si un objet existe. Les actions associées à ce niveau d'accès peuvent répertorier les objets mais ne peuvent pas voir le contenu d'une ressource. La plupart des actions possédant le niveau d'accès Liste ne peuvent pas être effectuées sur une ressource spécifique. Lorsque vous créez une déclaration de stratégie avec ces actions, vous devez spécifier toutes les ressources ("*").

Lisez

Fournit l'autorisation de lire le contenu et les attributs de ressources dans le service, mais pas de les modifier. Par exemple, les opérations Amazon S3`GetObject`and`GetBucketLocation`ont les balisesLisezNiveau d'accès.

Écrire

Fournit l'autorisation de créer, supprimer ou modifier des ressources du service. Par exemple, les opérations Amazon S3`CreateBucket`,`DeleteBucket`, et`PutObject`ont les balisesÉcrireNiveau d'accès.

Gestion des autorisations

Fournit l'autorisation d'octroyer ou de modifier des autorisations de ressource dans le service. Par exemple, la plupart des actions de stratégie IAM et AWS Organizations sont associées à l'Gestion des autorisationsNiveau d'accès.

> **Tip**
>
> Afin d'améliorer la sécurité de votre compte AWS, nous vous conseillons de restreindre ou de surveiller régulièrement les stratégies dotées de laGestion des autorisationsclassification au niveau de l'accès.

Balisage

Fournit l'autorisation de créer, supprimer ou modifier des balises qui sont attachées à une ressource dans le service. Par exemple, Amazon EC2`CreateTags`and`DeleteTags`ont la propriétéBalisageNiveau d'accès.

Mise en route d'IAM

AWS Identity and Access Management (IAM) est un service AWS qui vous permet de gérer l'accès aux services et aux ressources en toute sécurité. IAM est une fonction de votre compte AWS proposée gratuitement.

> **Note**
>
> Avant de commencer avec IAM, vérifiez les informations d'introduction surIdentity and Access Management pour AWS Global Accelerator.

Lorsque vous créez un compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les services et ressources AWS du compte. Cette identité est appelée utilisateur racine du compte AWS et elle est accessible après connexion à l'aide de l'adresse e-mail et du mot de passe utilisés pour la création du compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Respectez plutôt la bonne pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier utilisateur IAM. Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les uniquement pour effectuer certaines tâches de gestion des comptes et des services.

Créez votre utilisateur administrateur IAM

Pour créer un administrateur pour vous-même et ajouter l'utilisateur à un groupe d'administrateurs (console)

1. Connectez-vous à la IAM console (Console IAM) en tant que propriétaire du compte en choisissant Root user (Utilisateur racine) et en entrant l'adresse e-mail de votre compte AWS. Sur la page suivante, saisissez votre mot de passe.

   > **Note**
   >
   > Nous vous recommandons vivement de respecter la bonne pratique qui consiste à avoir recours à l'**`Administrator`**Utilisateur IAM qui suit et verrouille en sécurité les informations d'identification de l'utilisateur racine. Connectez-vous en tant qu'utilisateur racine pour effectuer certaines tâches de gestion des comptes et des services.

2. Dans le panneau de navigation, choisissez Utilisateurs, puis Add user (Ajouter un utilisateur).

3. Dans User name (Nom d'utilisateur), entrez **`Administrator`**.
4. Activez la case à cocher en regard de l'accès à AWS Management Console. Puis, sélectionnez Mot de passe personnalisé, et saisissez votre nouveau mot de passe dans la zone de texte.
5. Par défaut, AWS oblige le nouvel utilisateur à créer un nouveau mot de passe lors de sa première connexion. Décochez la case en regard de User must create a new password at next sign-in (L'utilisateur doit créer un nouveau mot de passe à sa prochaine connexion) pour autoriser le nouvel utilisateur à réinitialiser son mot de passe une fois qu'il s'est connecté.
6. ChoisissezSuivant: Autorisations.
7. Sous Set permissions (Accorder des autorisations), choisissez Add user to group (Ajouter un utilisateur au groupe).
8. Choisissez Create group.
9. Dans la boîte de dialogue Create group (Créer un groupe), pour Group name (Nom du groupe), tapez **`Administrators`**.
10. ChoisissezStratégies de filtre, puis sélectionnezGestion d'AWS - fonction de travailpour filtrer le contenu de la table.
11. Dans la liste des stratégies, cochez la case AdministratorAccess. Choisissez ensuite Create group.

    > **Note**
    >
    > Vous devez activer l'accès de l'utilisateur et du rôle IAM à la facturation avant de pouvoir utiliser les autorisations `AdministratorAccess` pour accéder à la console AWS Billing and Cost Management. Pour ce faire, suivez les instructions de l'étape 1 du didacticiel portant sur comment déléguer l'accès à la console de facturation.

12. De retour dans la liste des groupes, activez la case à cocher du nouveau groupe. Choisissez Refresh si nécessaire pour afficher le groupe dans la liste.
13. ChoisissezSuivant: Tags (Balises).
14. (Facultatif) Ajoutez des métadonnées à l'utilisateur en associant les balises sous forme de paires clé-valeur. Pour de plus amples informations sur l'utilisation des balises dans IAM, veuillez consulter Balisage des utilisateurs et des rôles IAM dans le Guide de l'utilisateur IAM.
15. ChoisissezSuivant: VérificationPour afficher la liste des appartenances de groupe à ajouter au nouvel utilisateur. Une fois que vous êtes prêt à continuer, choisissez Create user.

Vous pouvez utiliser ce même processus pour créer d'autres groupes et utilisateurs et pour accorder l'accès aux ressources de votre compte AWS à vos utilisateurs. Pour en savoir plus sur l'utilisation des stratégies permettant de limiter les autorisations d'accès des utilisateurs à certaines ressources AWS, veuillez consulter Gestion des accès et Exemples de stratégies.

Création d'utilisateurs délégués pour Global Accelerator

Pour prendre en charge plusieurs utilisateurs dans votre compte AWS, vous devez déléguer l'autorisation pour permettre à d'autres personnes d'effectuer uniquement les actions que vous souhaitez autoriser. Pour ce faire, créez un groupe IAM avec les autorisations dont ces personnes ont besoin, puis ajoutez les utilisateurs IAM aux groupes nécessaires à mesure que vous les créez. Vous pouvez utiliser cette procédure pour configurer les groupes, les utilisateurs et les autorisations pour l'ensemble de votre compte AWS. Cette solution est mieux utilisé par les petites et moyennes entreprises où un administrateur AWS peut gérer manuellement les utilisateurs et les groupes. Pour les grandes organisations, vous pouvez utiliserRôles IAM personnalisés,fédération, ouAuthentification unique.

Dans la procédure suivante, vous allez créer trois utilisateurs nommés**arnav**,**carlos**, et**martha**et joindre une stratégie qui accorde l'autorisation de créer un accélérateur nommé**my-example-accelerator**, mais seulement dans les 30 prochains jours. Vous pouvez utiliser les étapes fournies ici pour ajouter des utilisateurs possédant des autorisations différentes.

Pour créer un utilisateur délégué pour une autre personne (console)

1. Connectez-vous à AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Users (Utilisateurs), puis Add user (Ajouter un utilisateur).
3. Dans User name (Nom d'utilisateur), entrez **arnav**.
4. Choisissez Add another user (Ajouter un autre utilisateur) et saisissez **carlos** pour le deuxième utilisateur. Choisissez ensuite Add another user (Ajouter un autre utilisateur) et saisissez **martha** pour le troisième utilisateur.
5. Activez la case à cocher près deAccès AWS Management Console, puis sélectionnezMot de passe généré automatiquement.
6. Décochez la case en regard de L'utilisateur doit créer un nouveau mot de passe à sa prochaine connexion pour autoriser le nouvel utilisateur à réinitialiser son mot de passe une fois qu'il s'est connecté.

7. ChoisissezSuivant: Autorisations.
8. Choisissez Attacher directement les stratégies existantes. Vous allez créer une nouvelle stratégie gérée pour les utilisateurs.
9. Choisissez Créer une stratégie.

   L'assistant Create policy (Créer la stratégie) s'ouvre dans un nouvel onglet ou une nouvelle fenêtre du navigateur.
10. Dans l'onglet Éditeur visuel, sélectionnez Choose a service (Choisir un service). Choisissez Global Accelerator. Vous pouvez utiliser le menu Filtre ou la zone de recherche en haut de l'écran pour limiter les résultats dans la liste des services.

    La .Servicese ferme et la sectionActionss'ouvre automatiquement.
11. Choisissez les actions de l'accélérateur global que vous souhaitez autoriser.
    Par exemple, pour accorder l'autorisation de créer un accélérateur, entrez**`globalaccelerator:CreateAccelerator`**dans leAction de filtre. Lorsque la liste des actions Global Accelerator est filtrée, sélectionnez la case à cocher en regard de**`globalaccelerator:CreateAccelerator`**.

    Les actions Global Accelerator sont regroupées par classification de niveau d'accès pour vous permettre de rapidement déterminer le niveau d'accès que chaque action fournit. Pour plus d'informations, consultez Classification des niveaux d'accès aux politiques.
12. Si les actions choisies au cours des étapes précédentes ne prennent pas en charge le choix de ressources spécifiques, alorsToutes les ressourcesest sélectionné pour vous. Dans ce cas, vous ne pouvez pas modifier cette section.

    Si vous avez choisi une ou plusieurs actions qui prennent en charge les autorisations de niveau ressource, l'éditeur visuel affiche la liste de ces types de ressource dans la section Resources (Ressources). ChoisissezVous avez choisi des actions qui requièrent la propriétéAccélérateurType de ressourcePour choisir si vous souhaitez saisir un accélérateur spécifique pour votre stratégie.
13. Si vous souhaitez autoriser l'action `globalaccelerator:CreateAccelerator` pour toutes les ressources, choisissez All resources (Toutes les ressources).

    Si vous souhaitez spécifier une ressource, choisissez Add ARN (Ajouter un ARN). Spécifiez la région ou l'ID du compte (ou l'ID du compte) (ou choisissezAny), puis entrez**`my-example-accelerator`**pour la ressource. Choisissez ensuite Ajouter.

14. Choisissez Specify request conditions (optional) (Spécifier des conditions de demande (facultatif)).
15. ChoisissezAjouter une conditionpour accorder l'autorisation de créer un accélérateurdans les 7 jours. Supposez que la date du jour est le 1er janvier 2019.
16. Pour Condition Key (Clé de condition), choisissez aws : CurrentTime. Cette clé de condition vérifie la date et l'heure à laquelle l'utilisateur effectue la demande. Il renvoie la valeur true (et par conséquent autorise l'action **`globalaccelerator:CreateAccelerator`** uniquement si la date et l'heure sont comprise dans la plage spécifiée.
17. PourQualificateur, conservez la valeur par défaut.
18. Pour spécifier le début de la plage de dates et de temps autorisée, pour Operator (Opérateur), choisissez DateGreaterThan. Pour Value (Valeur), entrez **`2019-01-01T00:00:00Z`**.
19. Choisissez Add (Ajouter) pour enregistrer votre condition.
20. Choisissez Add another condition (Ajouter une condition) pour spécifier la date finale.
21. Suivez les étapes similaires pour spécifier la fin de la plage de dates et de temps autorisée. Pour Condition Key (Clé de condition), choisissez aws : CurrentTime. Pour Operator (Opérateur), choisissez DateLessThan. Pour Value (Valeur), entrez **`2019-01-06T23:59:59Z`**, sept jours après la première date. Choisissez ensuite Add (Ajouter) pour enregistrer votre condition.
22. (Facultatif) Pour afficher le document de stratégie JSON pour la stratégie que vous créez, choisissez l'optionJSON. Vous pouvez basculer à tout moment entre les onglets Éditeur visuel et JSON. Toutefois, si vous apportez des modifications ou choisissezExaminer une stratégiedans leVisual editor (Éditeur visuel), IAM peut restructurer votre stratégie pour optimiser son affichage dans l'éditeur visuel. Pour de plus amples informations, veuillez consulterRestructuration de stratégiedans leGuide de l'utilisateur IAM.
23. Lorsque vous avez terminé, choisissez Examiner une stratégie.
24. Dans la pageExaminer une stratégie, pourNom, saisissez**`globalaccelerator:CreateAcceleratorPolicy`**. Pour Description, entrez **`Policy to grants permission to create an accelerator`**. Passez en revue le récapitulatif de stratégie pour vous assurer que vous avez accordé les autorisations souhaitées, puis choisissez Créer une stratégie pour enregistrer votre nouvelle stratégie.
25. Revenez à l'onglet ou à la fenêtre initial(e) et actualisez votre liste de stratégies.
26. Dans la zone de recherche, entrez **`globalaccelerator:CreateAcceleratorPolicy`**. Cochez la case en regard de la nouvelle stratégie. Choisissez ensuite Next Step.
27. ChoisissezSuivant: Vérificationpour afficher vos nouveaux utilisateurs. Une fois que vous êtes prêt à continuer, choisissez Créer un utilisateur.

28. Téléchargez ou copiez les mots de passe de vos nouveaux utilisateurs et proposez-les aux utilisateurs en toute sécurité. Séparément, fournissez à vos utilisateurs unlien vers la page de votre console utilisateur IAMet les noms d'utilisateur que vous venez de créer.

Autorise les utilisateurs à gérer eux-mêmes leurs informations d'identification

Pour configurer l'authentification MFA, vous devez avoir accès physique au matériel sur lequel le périphérique MFA virtuel de l'utilisateur est hébergé. Par exemple, vous pouvez configurer le MFA pour un utilisateur qui utilisera un appareil MFA virtuel s'exécutant sur un smartphone. Dans ce cas, vous devez avoir le smartphone à proximité afin de finaliser l'assistant. De ce fait, vous pouvez préférer laisser les utilisateurs configurer et gérer leurs propres périphériques MFA virtuels. Dans ce cas, vous devez accorder aux utilisateurs les autorisations nécessaires pour effectuer les actions IAM nécessaires.

Pour créer une stratégie permettant la gestion automatique d'informations d'identification (console)

1. Connectez-vous à AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, choisissez Stratégies, puis Créer une stratégie.
3. Choisissez l'onglet JSON et copiez le texte du document de stratégie JSON suivant. Collez ce texte dans la zone de texte JSON.

> **Important**
>
> Cet exemple de stratégie n'autorise pas les utilisateurs à réinitialiser leur mot de passe lors de leur connexion. Les nouveaux utilisateurs et les utilisateurs ayant un mot de passe qui a expiré peuvent essayer de le faire. Vous pouvez autoriser cette opération en ajoutant `iam:ChangePassword` et `iam:CreateLoginProfile` à l'instruction `BlockMostAccessUnlessSignedInWithMFA`. Cependant, IAM ne le recommande pas.

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

A quoi sert cette stratégie ?

- La .`AllowAllUsersToListAccounts`permet à l'utilisateur de consulter des informations de base concernant le compte et ses utilisateurs dans la console IAM. Ces autorisations doivent se trouver dans leur propre instruction, car elles ne prennent pas en charge ou n'ont pas besoin de spécifier d'ARN de ressource particulier et spécifient à la place `"Resource" : "*"`.
- La .`AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation`L'instruction permet à l'utilisateur de gérer ses propres informations d'utilisateur, de mot de passe, de clés d'accès, de certificats de signature, de clés publiques SSH et de MFA dans la console IAM. Elle permet également aux utilisateurs de se connecter pour la première fois si un administrateur leur demande de définir un mot de passe initial. L'ARN de ressource limite l'utilisation de ces autorisations uniquement à l'entité IAM appartenant à l'utilisateur.
- L'instruction `AllowIndividualUserToViewAndManageTheirOwnMFA` permet à l'utilisateur d'afficher ou gérer son périphérique MFA. Notez que les ARN de ressource de cette instruction autorisent uniquement l'accès à un périphérique MFA ou un utilisateur dont le nom est strictement identique à celui de l'utilisateur actuellement connecté. Les utilisateurs ne peuvent pas créer ou modifier un périphérique MFA autre que le leur.
- L'instruction `AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA` permet à l'utilisateur de désactiver uniquement son propre périphérique MFA et uniquement s'il s'est connecté à l'aide de MFA. Ceci permet d'éviter que d'autres personnes disposant seulement des clés d'accès (et non du périphérique MFA) ne désactivent le périphérique MFA et n'accèdent au compte.
- La .`BlockMostAccessUnlessSignedInWithMFA`utilise une combinaison de`"Deny"`and`"NotAction"`pour refuser l'accès à toutes les actions sauf quelques actions dans IAM et d'autres services AWSifl'utilisateur n'est pas connecté avec MFA. Pour plus d'informations sur la logique de cette instruction, consultezNotAction avec Denydans leGuide de l'utilisateur IAM. Si l'utilisateur s'est connecté à l'aide de MFA, le test `"Condition"` échoue et la dernière instruction « deny » n'a aucun effet ; les autres stratégies ou instructions

pour l'utilisateur déterminent les autorisations de ce dernier. Cette instruction garantit que lorsque l'utilisateur ne s'est pas connecté avec MFA, celui-ci ne peut exécuter que les actions répertoriées et uniquement si une autre instruction ou stratégie accorde l'accès à ces actions.

La version `...IfExists` de l'opérateur `Bool` permet de s'assurer que si la clé `aws:MultiFactorAuthPresent` est manquante, la condition renvoie la valeur true. Cela signifie qu'un utilisateur qui accède à une API avec des informations d'identification à long terme, comme une clé d'accès, se voit refuser l'accès aux opérations d'API non IAM.

4. Lorsque vous avez terminé, choisissez Examiner une stratégie.
5. Sur la page Review (Vérification), tapez **`Force_MFA`** pour le nom de la stratégie. Pour la description de la stratégie, saisissez**`This policy allows users to manage their own passwords and MFA devices but nothing else unless they authenticate with MFA.`**Examiner la stratégieRécapitulatifPour afficher les autorisations accordées par votre stratégie, puis choisissezCréer une stratégiepour sauvegarder votre travail.

   La nouvelle stratégie s'affiche dans la liste des stratégies gérées et est prête à être attachée.

Pour attacher la stratégie à un utilisateur (console)

1. Dans le volet de navigation, sélectionnez Users.
2. Choisissez le nom (et non pas la case à cocher correspondante) de l'utilisateur que vous voulez modifier.
3. Sous l'onglet Autorisations, choisissez Ajouter des autorisations.
4. Choisissez Attacher directement les stratégies existantes.
5. Dans la zone de recherche, saisissez **`Force`**, puis cochez la case située en regard de Force_MFA dans la liste. Ensuite, sélectionnez Next (Suivant). Vérification.
6. Vérifiez vos modifications et choisissez Ajouter des autorisations.

Activer MFA pour votre utilisateur IAM

Pour plus de sécurité, nous recommandons à tous les utilisateurs IAM de configurer l'authentification multi-facteurs (Multi-Factor Authentication, MFA) pour mieux protéger vos ressources Global Accelerator. L'authentification MFA ajoute une couche de sécurité supplémentaire, car elle exige que les utilisateurs fournissent une authentification unique à partir d'un périphérique MFA pris en charge par AWS, en plus de leurs informations d'identification de connexion classiques. Le périphérique AWS MFA le plus sécurisé est la clé de sécurité U2F. Si votre société possède déjà des périphérique

U2F, nous vous recommandons d'activer ces périphériques pour AWS. Dans le cas contraire, vous devez acheter un périphérique pour chacun de vos utilisateurs et attendre de recevoir le matériel. Pour de plus amples informations, veuillez consulterActivation d'une clé de sécurité U2Fdans leGuide de l'utilisateur IAM.

Si vous n'avez pas déjà un périphérique U2F, vous pouvez démarrer rapidement et à moindre coût en activant un périphérique MFA virtuel. Cela nécessite que vous installiez une application logicielle sur un téléphone ou un autre appareil mobile. Le périphérique génère un code numérique à six chiffres basé sur un algorithme de mot de passe unique synchronisé. Lorsque l'utilisateur se connecte à AWS, il est invité à entrer un code à partir de l'appareil. Chaque périphérique MFA virtuel attribué à un utilisateur doit être unique. Un utilisateur ne peut pas saisir un code à partir du périphérique MFA virtuel d'un autre utilisateur pour s'authentifier. Pour obtenir une liste des applications que vous pouvez utiliser comme appareils MFA virtuels, consultez Multi-Factor Authentication.

> **Note**
>
> Pour configurer l'authentification MFA d'un utilisateur IAM, vous devez avoir un accès physique au périphérique mobile sur lequel le périphérique MFA virtuel de l'utilisateur est hébergé.

Pour activer un périphérique MFA virtuel pour un utilisateur IAM (console)

1. Connectez-vous à AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sélectionnez Users.
3. Dans la liste Nom d'utilisateur, choisissez le nom utilisateur MFA prévu.
4. Choisissez l'onglet Informations d'identification de sécurité. En regard de Assigned MFA device (Appareil MFA affecté), choisissez Manage (Gérer).
5. Dans l'assistant Gérer l'appareil MFA, choisissez Appareil MFA virtuel, puis Continuer.

   IAM génère et affiche les informations de configuration du périphérique MFA virtuel, notamment un graphique de code QR. Le graphique est une représentation de la clé de configuration secrète que l'on peut saisir manuellement sur des périphériques qui ne prennent pas en charge les codes QR.
6. Ouvrez votre application MFA virtuelle.

Pour obtenir une liste des applications que vous pouvez utiliser pour héberger des périphériques MFA virtuels, consultez Authentification multi-facteurs. Si l'application MFA virtuelle prend en charge plusieurs comptes (plusieurs périphériques MFA virtuels), choisissez l'option permettant de créer un compte (un nouveau périphérique MFA virtuel).

7. Déterminez si l'application MFA prend en charge les codes QR, puis effectuez l'une des actions suivantes :

   - Dans l'assistant, choisissez Show QR code (Afficher le code QR), puis utiliser l'application pour analyser le code QR. Par exemple, vous pouvez choisir l'icône de caméra ou une option similaire à Scan code, puis utiliser la caméra du périphérique pour analyser le code.
   - Dans l'assistant Gérer le périphérique MFA, choisissez Afficher la clé secrète pour la configuration manuelle, puis saisissez la clé secrète dans votre application MFA.

   Une fois que vous avez terminé, le périphérique MFA virtuel commence à générer des mots de passe uniques.

8. Dans l'assistant Gérer l'appareil MFA, dans la zone MFA Code 1 (Code MFA 1), saisissez le mot de passe unique qui s'affiche actuellement sur le périphérique MFA virtuel. Attendez jusqu'à 30 secondes pour que le périphérique génère un nouveau mot de passe unique. Saisissez ensuite le second mot de passe unique dans la zone MFA Code 2 (Code MFA 2). Choisissez Assign MFA (Affecter le MFA).

   > **Important**
   >
   > Envoyez votre demande immédiatement après avoir généré les codes. Si vous générez les codes puis attendez trop longtemps avant d'envoyer la demande, le périphérique MFA s'associe avec succès à l'utilisateur mais est désynchronisé. En effet, les TOTP (Time-based One-Time Passwords ou mots de passe à usage unique à durée limitée) expirent après une courte période. Dans ce cas, vous pouvez resynchroniser le périphérique. Pour de plus amples informations, veuillez consulterResynchronisation de périphériques MFA virtuels et matérielsdans leGuide de l'utilisateur IAM.

   L'appareil MFA virtuel est maintenant prêt à être utilisé avec AWS.

Connexions VPC sécurisées dans AWS Global Accelerator

Lorsque vous ajoutez un Application Load Balancer interne ou un point de terminaison d'instance Amazon EC2 dans AWS Global Accelerator, vous activez le trafic Internet pour circuler directement vers et depuis le point de terminaison dans les Clouds privés virtuels (VPC) en le ciblant dans un sous-réseau privé. Le VPC qui contient l'équilibreur de charge ou l'instance EC2 doit avoir unPasserelle Internetjoint à lui, pour indiquer que le VPC accepte le trafic Internet. Cependant, vous n'avez pas besoin d'adresses IP publiques sur l'équilibreur de charge ou l'instance EC2. Vous n'avez pas non plus besoin d'une route de passerelle Internet associée pour le sous-réseau.

Ceci est différent du cas d'utilisation de la passerelle Internet typique dans lequel les adresses IP publiques et les routes de passerelle Internet sont nécessaires pour que le trafic Internet circule vers des instances ou des équilibreurs de charge dans un VPC. Même si les interfaces réseau élastiques de vos cibles sont présentes dans un sous-réseau public (c'est-à-dire, un sous-réseau avec une route de passerelle Internet), lorsque vous utilisez Global Accelerator pour le trafic Internet, Global Accelerator remplace la route Internet typique et toutes les connexions logiques qui arrivent via le Accélérateur revient également via Global Accelerator plutôt que via la passerelle Internet.

> **Note**
>
> L'utilisation d'adresses IP publiques et l'utilisation d'un sous-réseau public pour vos instances Amazon EC2 ne sont pas typiques, bien qu'il soit possible de configurer votre configuration avec elles. Les groupes de sécurité s'appliquent à tout trafic qui arrive à vos instances, y compris le trafic provenant de Global Accelerator et toute adresse IP publique ou Elastic attribuée à votre instance ENI. Utilisez des sous-réseaux privés pour vous assurer que le trafic est fourni uniquement par Global Accelerator.

Gardez ces informations à l'esprit lors de la prise en compte des problèmes de périmètre réseau et de la configuration des privilèges IAM liés à la gestion de l'accès Internet. Pour en savoir plus sur le contrôle de l'accès à Internet à votre VPC, consultez cetExemple de stratégie de contrôle de service.

Journalisation et surveillance dans AWS Global Accelerator

La surveillance est un élément important permettant d'assurer la disponibilité et les performances de Global Accelerator et de vos solutions AWS. Vous devez recueillir les données de surveillance de toutes les parties de votre solution AWS de telle sorte que vous puissiez déboguer plus facilement

une éventuelle défaillance à plusieurs points. AWS fournit plusieurs outils pour surveiller vos ressources et vos activités Global Accelator et répondre aux éventuels incidents.

Journaux de flux AWS Global Accelerator

Les journaux de flux de serveur fournissent des enregistrements détaillés sur le trafic qui circule à travers un accélérateur vers un point de terminaison. Les journaux de flux de serveur sont utiles pour de nombreuses applications. Par exemple, les informations des journaux de flux peuvent s'avérer utiles en cas d'audit de sécurité ou d'audit des accès. Pour plus d'informations, consultez Journaux de flux dans AWS Global Accelerator.

Métriques et alarmes Amazon CloudWatch

CloudWatch vous permet de surveiller en temps réel vos ressources AWS et les applications que vous exécutez sur AWS. CloudWatch collecte et suit les mesures, qui sont des variables que vous mesurez au fil du temps. Vous pouvez créer des alarmes pour surveiller des métriques spécifiques, puis envoyer des notifications ou apporter automatiquement des modifications aux ressources surveillées, lorsque la mesure dépasse un certain seuil pendant une période donnée. Pour plus d'informations, consultez Utilisation d'Amazon CloudWatch avec AWS Global Accelerator.

Journaux CloudTrail AWS

CloudTrail fournit un enregistrement des actions réalisées par un utilisateur, un rôle ou un service AWS dans Global Accelerator. CloudTrail capture tous les appels d'API pour Global Accelator sous forme d'événements, y compris les appels émis par la console Global Accelerator et les appels de code transmis à l'API Global Accelerator. Pour plus d'informations, consultez Utilisation d'AWS CloudTrail pour journaliser les appels d'API AWS Global Accelerator.

Validation de conformité pour AWS Global Accelerator

Des auditeurs tiers évaluent la sécurité et la conformité d'AWS Global Accelerator dans le cadre de plusieurs programmes de conformité AWS. Il s'agit notamment des certifications SOC, PCI, HIPAA, GDPR, ISO et ENS High.

Pour obtenir la liste des services AWS, notamment Global Accelerator, dans le cadre de programmes de conformité spécifiques, consultezServices AWS concernés par le programme de conformité. Pour obtenir des renseignements généraux, consultez Programmes de conformitéAWS .

Vous pouvez télécharger les rapports d'audit tiers avec AWS Artifact. Pour de plus amples informations, veuillez consulterTéléchargement des rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation de Global Accelerator est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables. AWS fournit les ressources suivantes pour faciliter la conformité :

- Guides de démarrage rapide de la sécurité et de la conformité – Ces guides de déploiement proposent des considérations architecturales et fournissent des étapes pour déployer des environnements de référence centrés sur la sécurité et la conformité sur AWS.
- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA – Le livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications conformes à la loi HIPAA.
- Ressources de conformité AWS – Cet ensemble de manuels et de guides peut s'appliquer à votre secteur et à votre emplacement.
- Évaluation des ressources à l'aide de règles dans le Manuel du développeur AWS Config : le service évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub – Ce service AWS fournit une vue complète de votre état de sécurité au sein d'AWS qui vous permet de vérifier votre conformité aux normes du secteur et aux bonnes pratiques de sécurité.

Résilience dans AWS Global Accelerator

L'infrastructure mondiale d'AWS repose sur des régions et des zones de disponibilité AWS. Les régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les régions et les zones de disponibilité AWS, consultez Infrastructure mondiale AWS.

Outre la prise en charge de l'infrastructure mondiale AWS, Global Accelator propose les fonctionnalités suivantes qui contribuent à la prise en charge de la résilience des données :

- Une zone réseau dessert les adresses IP statiques de votre accélérateur à partir d'un sous-réseau IP unique. À l'instar d'une zone de disponibilité AWS, une zone réseau est une unité isolée dotée de son propre ensemble d'infrastructure physique. Lorsque vous configurez un accélérateur, Global Accelerator lui alloue deux adresses IPv4. Si une adresse IP d'une zone réseau devient indisponible en raison du blocage de l'adresse IP par certains réseaux clients, ou en raison de perturbations du réseau, les applications clientes peuvent réessayer sur l'adresse IP statique saine de l'autre zone réseau isolée.
- Global Accelerator surveille en permanence l'état de tous les terminaux. Lorsqu'il détermine qu'un point de terminaison actif est défectueux, Global Accelerator commence instantanément à diriger le trafic vers un autre point de terminaison disponible. Cela vous permet de créer une architecture haute disponibilité pour vos applications sur AWS.

Sécurité de l'infrastructure dans AWS Global Accelerator

En tant que service géré, AWS Global Accelerator est protégé par les procédures de sécurité du réseau mondial AWS qui sont décrites dans laAmazon Web Services : Présentation des processus de sécuritéLivre blanc.

Vous pouvez utiliser AWS appels d'API publiés pour accéder à Global Accelerator via le réseau. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.0 ou version ultérieure. Nous recommandons TLS 1.2 ou version ultérieure. Les clients doivent également prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) La plupart des systèmes modernes telles que Java 7 et versions ultérieures prennent en charge ces modes. En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un mandataire IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Quotas pour AWS Global Accelerator

Votre compte AWS dispose de quotas spécifiques, également appelés limites, pour AWS Global Accelerator.

La console Service Quotas fournit des informations sur les quotas Global Accelerator. En plus de visualiser les quotas par défaut, vous pouvez utiliser la console Service Quotas pourdemander des augmentations de quotapour les quotas ajustables. Notez que vous devez être dans US East (Virginie du Nord) lorsque vous demandez des augmentations de quota pour Global Accelerator.

Rubriques

Quotas généraux

Voici les quotas globaux pour Global Accelerator.

Entité	Quota
Accélérateurs par compte AWS	20 Vous pouvez.Demande d'augmentation de quota.
Écouteurs par accélérateur	10 Vous pouvez.Demande d'augmentation de quota.
Plages de ports par écouteur	10
Remplacements de port par groupe de points de terminaison	10 Vous pouvez.Demande d'augmentation de quota.

Quotas pour les terminaux par groupe de points de terminaison

Voici les quotas Global Accelerator qui s'appliquent au nombre de points de terminaison dans les groupes de points de terminaison.

Entité	Description	Quota
Groupes de points de terminaison avec plusieurs types de point de terminaison	Nombre de points de terminaison dans un groupe de points de terminaison contenant plus d'un type de point de terminaison.	10
Groupes de points de terminaison avec uniquement des équilibreurs de charge d'application	Nombre d'équilibreurs de charge d'application dans un groupe de points de terminaison contenant uniquement les points de terminaison de l'Application Load Balancer.	10
Groupes de points de terminaison avec uniquement des équilibreurs de charge réseau	Nombre d'équilibreurs de charge réseau dans un groupe de points de terminaison contenant uniquement les points de terminaison de l'Network Load Balancer.	10
Groupes de points de terminaison avec uniquement des instances Amazon EC2	Nombre d'instances EC2 dans un groupe de points de terminaison contenant uniquement des points de terminaison d'instance EC2.	10 Vous pouvez.Demande d'augmentation de quota.
Groupes de points de terminaison avec uniquement des adresses IP élastiques	Nombre d'adresses IP Elastic dans un groupe de points de terminaison contenant uniquement des points de terminaison d'adresse IP Elastic.	10 Vous pouvez.Demande d'augmentation de quota.
Groupes de points de terminaison avec uniquement des sous-réseaux Amazon Virtual Private Cloud	Nombre de sous-réseaux Amazon VPC dans un groupe de points de terminaison contenant uniquement des points de terminaison de sous-réseau.	10 Vous pouvez.Demande d'augmentation de quota.

Quotas connexes

En plus des quotas dans Global Accelerator, il y a des quotas qui s'appliquent aux ressources que vous utilisez en tant que points de terminaison pour un programme d'accélération. Pour plus d'informations, consultez les ressources suivantes :

- Quotas élastiques d'adressesdans leGuide de l'utilisateur Amazon EC2.
- Quotas de service Amazon EC2dans leGuide de l'utilisateur Amazon EC2.
- Quotas pour vos équilibreurs de charge du réseaudans leGuide de l'utilisateur des Network Load Balancers.
- Quotas pour vos équilibreurs de charge d'applicationdans leGuide de l'utilisateur des équilibreurs de charge d'application.
- Quotas Amazon VPCdans leGuide de l'utilisateur Amazon VPC.

Informations relatives à AWS Global Accelerator

Les informations et les ressources indiquées ici peuvent vous aider à en savoir plus sur Global Accelerator.

Rubriques

- Documentation AWS Global Accelerator
- Obtention de support
- Conseils du blog Amazon Web Services

Documentation AWS Global Accelerator

Les ressources connexes suivantes peuvent s'avérer utiles lors de l'utilisation de ce service.

- Référence d'API AWS Global Accelerator— Fournit une description complète des actions, paramètres et types de données API, ainsi qu'une liste des erreurs renvoyées par le service.
- Informations sur le produit AWS Global Accelerator— Page web principale pour des informations sur Global Accelerator, y compris sur les fonctions et la tarification.
- Conditions d'utilisation— Informations détaillées sur nos copyrights et marque de commerce, sur votre compte, votre licence et votre accès au site, et sur d'autres sujets.

Obtention de support

La prise en charge de Global Accelerator est disponible sous plusieurs formes.

- Forums de discussion— Un forum communautaire qui permet aux développeurs d'échanger à propos de questions techniques liées à Global Accelerator.
- Centre AWS Support – Ce site regroupe les informations sur vos dossiers de support récents et les résultats d'AWS Trusted Advisor ainsi que des vérifications d'état. Il fournit également des liens vers les forums de discussion, les questions fréquentes (FAQ) techniques, le tableau de bord de l'état des services et les informations sur les plans de support AWS.
- Informations sur AWS Premium Support – La page web de présentation d'AWS Premium Support représente un canal d'assistance individuelle rapide visant à vous permettre de construire et d'exécuter facilement vos applications sur les services d'infrastructure AWS.

- Contactez-nous – Liens pour les questions sur votre compte ou votre facturation. Pour les questions techniques, veuillez utiliser les forums de discussion ou les liens de support ci-dessus.

Conseils du blog Amazon Web Services

Le blog AWS contient divers billets pour vous aider à utiliser les services AWS. Par exemple, consultez les billets suivants sur Global Accelerator :

- AWS Global Accelerator pour la disponibilité et les performances
- Gestion du trafic avec AWS Global Accelerator
- Analyse et visualisation des journaux de flux AWS Global Accelerator à l'aide d'Amazon Athenaet d'Amazon QuickSight

Pour obtenir la liste complète des blogs AWS Global Accelerator, consultezAWS Global Acceleratordans la catégorie Mise en réseau et diffusion de contenu des articles de blog AWS.

Historique du document

Les entrées suivantes décrivent les modifications importantes apportées à la documentation AWS Global Accelerator.

- Version de l'API : dernière en date
- Mise à jour de la documentation : 9 décembre 2020

Modification	Description	Date
Mise à jour du rôle lié au service existant de Global Accelerator	Global Accelerator a ajouté une nouvelle autorisation,`ec2:DescribeRegions` , pour permettre à Global Accelerator d'obtenir des informations sur la région AWS pour aider à diagnostiquer les erreurs. Pour plus d'informations, consultez https://docs.aws.amazon.com/global-accelerator/latest/dg/security-iam-awsmanpol-updates.html.	7 mai 2021
Accélérateurs de routage personnalisés ajoutés	Global Accelerator a introduit un nouveau type d'accélérateurs de routage personnalisés d'accélérateur. Les accélérateurs de routage personnalisés fonctionnent bien pour les scénarios dans lesquels vous souhaitez utiliser une logique d'application personnalisée pour diriger un ou plusieurs utilisateurs vers une destination et	9 décembre 2020

Modification	Description	Date
	un port spécifiques parmi d'autres, tout en profitant des avantages de performances de Global Accelerator. Pour plus d'informations, consultez https://docs.aws.amazon.com/global-accelerator/latest/dg/work-with-custom-routing-accelerators.html.	
Prise en charge des remplacements de port ajoutés	Global Accelerator prend désormais en charge le remplacement du port d'écoute utilisé pour acheminer le trafic vers des points de terminaison afin que vous puissiez réacheminer le trafic vers des ports spécifiques sur vos points de terminaison. Pour plus d'informations, consultez https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-port-override.html.	21 octobre 2020
Ajout de deux nouvelles régions	Global Accelerator prend maintenant en charge l'Afrique (Le Cap) et l'Europe (Milan). Pour plus d'informations, consultez https://docs.aws.amazon.com/global-accelerator/latest/dg/preserve-client-ip-address.regions.html.	20 mai 2020

Modification	Description	Date
Marquage et BYOIP	Cette version ajoute la prise en charge de l'ajout de balises aux accélérateurs et de l'ajout de votre propre adresse IP à AWS Global Accelerator (BYOIP). Pour plus d'informations, consultez https://docs.aws.amazon.com/global-accelerator/latest/dg/tagging-in-global-accelerator.html et https://docs.aws.amazon.com/global-accelerator/latest/dg/using-byoip.html.	27 février 2020
Mise à jour du chapitre Sécurité	Ajout de contenu pour la conformité, la résilience et la sécurité de l'infrastructure. Pour plus d'informations, consultez https://docs.aws.amazon.com/global-accelerator/latest/dg/security.html.	20 décembre 2019

Modification	Description	Date
Support des instances EC2 et du nom DNS par défaut	AWS Global Accelerator prend désormais en charge l'ajout d'instances EC2 dans les régions AWS prises en charge. En outre, Global Accelerator crée un nom DNS par défaut qui est mappé aux adresses IP statiques de votre accélérateur. Pour plus d'informations, consultez https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html et https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.html#about-accelerators.dns-addressing.	29 octobre 2019
Conservation des adresses IP du client pour les équilibreurs de charge d'application	Vous pouvez désormais choisir qu'AWS Global Accelerator conserve l'adresse IP du client pour les équilibreurs de charge d'application dans les régions AWS prises en charge. Pour plus d'informations, consultez https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html.	28 août 2019

Modification	Description	Date
Publication du service AWS Global Accelerator	Le Guide du développeur AWS Global Accelerator fournit des informations sur la configuration et l'utilisation d'accélérateurs (gestionnaires de trafic de couche réseau) qui améliorent la disponibilité et les performances de vos applications Internet ayant une audience mondiale.	26 novembre 2018

Glossaire AWS

Pour connaître la terminologie AWS la plus récente, veuillez consulter le Glossaire AWS dans les Références générales AWS.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.