aws

開発者ガイド

AWS Global Accelerator

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Global Accelerator: 開発者ガイド

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、Amazon のものではない製品またはサービスと関連付けてはならず、また、お客様に混乱を招くような形や Amazon の信用を傷つけたり失わせたりする形で使用することはできません。Amazon が所有しない商標はすべてそれぞれの所有者に所属します。所有者は必ずしも Amazon と提携していたり、関連しているわけではありません。また、Amazon 後援を受けているとはかぎりません。

Table of Contents

AWS Global Accelerator

AWS Global Accelerator は、アクセラレーターを使用すると、ローカルおよびGlobal ユーザー向けのアプリケーションのパフォーマンスが向上します。選択したアクセラレーターのタイプに応じて、追加のメリットを得ることができます。

- 標準のアクセラレーターを使用すると、世界中のユーザーが使用するインターネットアプリケーションの可用性を向上できます。標準アクセラレータを使用すると、Global Accelerator は AWS グローバルネットワーク経由でクライアントに最も近いリージョンのエンドポイントにトラフィックを転送します。
- カスタムルーティングアクセラレータを使用すると、1 人以上のユーザーを複数の宛先の特定の宛先にマッピングできます。

グローバルアクセラレータは、複数の AWS リージョンのエンドポイントをサポートするグローバルサービスです。これらのエンドポイントは、AWS リージョン表。

デフォルトでは、グローバルアクセラレータには、アクセラレータに関連付けられた 2 つの静的 IP アドレスが用意されています。標準アクセラレータでは、グローバルアクセラレータが提供する IP アドレスを使用する代わりに、グローバルアクセラレータに持ち込む独自の IP アドレス範囲の IPv4 アドレスにこれらのエントリポイントを構成できます。静的 IP アドレスは、AWS エッジネットワークからのエニーキャストです。

> **Important**
>
> スタティック IP アドレスは、アクセラレータをディセーブルにしてトラフィックの受け入れやルーティングを行わなくても、存在している限り、アクセラレータに割り当てられたままになります。しかし、ときにdeleteアクセラレータを使用すると、割り当てられた静的 IP アドレスが失われるため、それらを使用してトラフィックをルーティングできなくなります。Global Accelerator でタグベースのアクセス許可などの IAM ポリシーを使用すると、アクセラレータを削除するアクセス許可を持つユーザーを制限できます。詳細については、「タグベースのポリシー」を参照してください。

標準アクセラレータの場合、Global Accelerator は AWS グローバルネットワークを使用して、正常性、クライアントの場所、および設定したポリシーに基づいて、最適なリージョンエンドポイントにトラフィックをルーティングします。これにより、アプリケーションの可用性が向上します。標準アクセラレータのエンドポイントは、ネットワークロードバランサー、アプリケーションロードバラン

サー、Amazon EC2 インスタンス、または 1 つの AWS リージョンまたは複数のリージョンにある Elastic IP アドレスです。このサービスは、正常性または構成の変更に即座に対応し、クライアントからのインターネットトラフィックが常に正常なエンドポイントに送信されるようにします。

カスタムルーティングアクセラレーターはVirtual Private Cloud (VPC) サブネットエンドポイントタイプのみをサポートし、そのサブネット内のプライベート IP アドレスにトラフィックをルーティングします。

Global Accelerator とその他のサービスが現在サポートされている AWS リージョンのリストについては、AWS リージョン表。

トピック

- AWS Global Accelerator
- AWS Global Accelerator
- アクセラレータの種類
- Global Accelerator エッジサーバーの場所と IP アドレス範囲
- AWS Global Accelerator
- AWS Global Accelerator
- AWS Global Accelerator
- AWS Global Accelerator でのタグ付け
- AWS Global Accelerator

AWS Global Accelerator

AWS Global Accelerator

静的 IP アドレス

Global Accelerator は、AWS エッジネットワークからエニーキャストされる 2 つの静的 IP アドレスのセットを提供します。Global Accelerator で使用するために自分の IP アドレス範囲を AWS (BYOIP) に追加した場合、代わりに、アクセラレーターの使用のために独自のプールから IP アドレスを割り当てることができます。詳細については、「AWS Global Accelerator で独自の IP アドレス (BYOIP) を使用する」を参照してください。

IP アドレスは、クライアントの単一の固定エントリポイントとして機能します。アプリケーション用に Elastic Load Balancing ロードバランサー、Amazon EC2 インスタンス、または Elastic IP

アドレスリソースがすでに設定されている場合は、Global Accelerator で標準アクセラレータに簡単に追加できます。これにより、グローバルアクセラレータは静的 IP アドレスを使用してリソースにアクセスできます。

スタティック IP アドレスは、アクセラレータをディセーブルにしてトラフィックの受け入れやルーティングを行わなくても、存在している限り、アクセラレータに割り当てられたままになります。しかし、ときにdeleteアクセラレータを使用すると、割り当てられた静的 IP アドレスが失われるため、それらを使用してトラフィックをルーティングできなくなります。Global Accelerator でタグベースのアクセス許可などの IAM ポリシーを使用すると、アクセラレータを削除するアクセス許可を持つユーザーを制限できます。詳細については、「タグベースのポリシー」を参照してください。

アクセラレーター

アクセラレータは、AWS グローバルネットワーク経由でエンドポイントにトラフィックを転送し、インターネットアプリケーションのパフォーマンスを向上させます。各アクセラレータには、1 つ以上のリスナーが含まれます。

アクセラレータには 2 つのタイプがあります。

- Aスタンダードアクセラレータは、ユーザーの場所、エンドポイントの正常性、設定するエンドポイントの重みなど、いくつかの要因に基づいて、トラフィックを最適な AWS エンドポイントに転送します。これにより、アプリケーションの可用性とパフォーマンスが向上します。エンドポイントは、ネットワークロードバランサー、アプリケーションロードバランサー、Amazon EC2 インスタンス、または Elastic IP アドレスです。
- Aカスタムログルーティングアクセラレータを使用すると、いくつかのユースケースで必要とされるように、アクセラレータの背後にある特定の EC2 宛先に複数のユーザーを決定的にルーティングできます。これを行うには、Global Accelerator が宛先にマッピングしたアクセラレータの一意の IP アドレスとポートにユーザを誘導します。

詳細については、「アクセラレータの種類」を参照してください。

DNS 名

Global Accelerator は、各アクセラレーターのデフォルトのドメインネームシステム (DNS) 名を割り当てます。これは`a1234567890abcdef.awsglobalaccelerator.com`で、グローバルアクセラレータが割り当てる、または独自の IP アドレス範囲から選択する静的 IP アドレスを指します。ユースケースに応じて、アクセラレータの静的 IP アドレスまたは DNS 名を使用してトラフィックをアクセラレータにルーティングしたり、独自のカスタムドメイン名を使用してトラフィックをルーティングするように DNS レコードを設定できます。

ネットワークゾーン

ネットワークゾーンは、一意の IP サブネットからアクセラレータの静的 IP アドレスをサービスします。AWS アベイラビリティーゾーンと同様に、ネットワークゾーンは、独自の物理インフラストラクチャセットを備えた独立したユニットです。アクセラレータを構成すると、デフォルトでは、グローバルアクセラレータによって 2 つの IPv4 アドレスが割り当てられます。特定のクライアントネットワークによる IP アドレスブロックまたはネットワークの中断により、ネットワークゾーンの 1 つの IP アドレスが使用できなくなった場合、クライアントアプリケーションは、別の分離されたネットワークゾーンから正常な静的 IP アドレスを再試行できます。

Listener

リスナーは、構成するポート (またはポート範囲) とプロトコル (またはプロトコル) に基づいて、クライアントからグローバルアクセラレータへの受信接続を処理します。リスナーは、TCP、UDP、または TCP と UDP の両方のプロトコルに対して構成できます。各リスナーには、1 つ以上のエンドポイントグループが関連付けられており、トラフィックはいずれかのグループのエンドポイントに転送されます。トラフィックを配信するリージョンを指定して、エンドポイントグループをリスナーに関連付けます。標準アクセラレータを使用すると、リスナーに関連付けられたエンドポイントグループ内の最適なエンドポイントにトラフィックが分散されます。

エンドポイントグループ

各エンドポイントグループは、特定の AWS リージョンに関連付けられています。エンドポイントグループには、リージョン内の 1 つ以上のエンドポイントが含まれます。標準アクセラレータを使用すると、エンドポイントグループに送信されるトラフィックの割合を増減できます。トラフィックダイヤル。トラフィックダイヤルを使用すると、パフォーマンステストやブルー/グリーンのデプロイテストを簡単に実行できます。たとえば、さまざまな AWS リージョンの新しいリリースなどです。

エンドポイント

エンドポイントは、グローバルアクセラレータがトラフィックを転送するリソースです。

標準アクセラレータのエンドポイントは、ネットワークロードバランサー、アプリケーションロードバランサー、EC2 インスタンス、または Elastic IP アドレスです。Application Load Balancer エンドポイントは、インターネットに接続したエンドポイントまたは内部エンドポイントです。標準アクセラレータのトラフィックは、エンドポイントの正常性と、エンドポイントの重みなどの選択した設定オプションに基づいてエンドポイントにルーティングされます。エンドポイントごとに、重みを設定できます。重みは、各エンドポイントにルーティングするトラ

フィックの割合を指定するために使用できる数値です。これは、リージョン内でパフォーマンステストを行う場合などに便利です。

カスタムルーティングアクセラレータのエンドポイントは、トラフィックの宛先である 1 つまたは複数の Amazon EC2 インスタンスを持つ仮想プライベートクラウド (VPC) サブネットです。

AWS Global Accelerator

AWS Global Accelerator によって提供される静的 IP アドレスは、クライアントの単一の固定エントリポイントとして機能します。Global Accelerator を使用してアクセラレータを設定する場合、静的 IP アドレスを 1 つ以上の AWS リージョンのリージョンエンドポイントに関連付けます。標準アクセラレータの場合、エンドポイントはネットワークロードバランサー、アプリケーションロードバランサー、Amazon EC2 インスタンス、または Elastic IP アドレスです。カスタムルーティングアクセラレータの場合、エンドポイントは 1 つ以上の EC2 インスタンスを持つ仮想プライベートクラウド (VPC) サブネットです。静的 IP アドレスは、ユーザーに最も近いエッジロケーションから AWS グローバルネットワークへの着信トラフィックを受け入れます。

> **Note**
>
> Global Accelerator で使用するために自分の IP アドレス範囲を AWS (BYOIP) に追加した場合、代わりに、アクセラレーターの使用のために独自のプールから静的 IP アドレスを割り当てることができます。詳細については、「AWS Global Accelerator で独自の IP アドレス (BYOIP) を使用する」を参照してください。

エッジロケーションから、アプリケーションのトラフィックは、設定したアクセラレータのタイプに基づいてルーティングされます。

- 標準アクセラレータの場合、トラフィックは、ユーザーの場所、エンドポイントの正常性、設定するエンドポイントの重みなど、いくつかの要因に基づいて、最適な AWS エンドポイントにルーティングされます。
- カスタムルーティングアクセラレータの場合、各クライアントは、指定した外部の静的 IP アドレスとリスナーポートに基づいて、VPC サブネット内の特定の Amazon EC2 インスタンスおよびポートにルーティングされます。

トラフィックは、十分に監視され、輻輳のない冗長な AWS グローバルネットワークを介してエンドポイントに送信されます。Global Accelerator は、トラフィックが AWS ネットワーク上にある時間

を最大化することで、トラフィックが常に最適なネットワークパスでルーティングされるようにします。

いくつかのエンドポイントタイプ (一部の AWS リージョンで) では、クライアントの IP アドレスを保持してアクセスするオプションがあります。次の 2 種類のエンドポイントでは、着信パケットでクライアントの送信元 IP アドレスを保持できます。アプリケーションロードバランサーと Amazon EC2 インスタンス グローバルアクセラレータは、Network Load Balancer および Elastic IP アドレスエンドポイントのクライアント IP アドレスの保持をサポートしていません。カスタムルーティングアクセラレータのエンドポイントには、常にクライアント IP アドレスが保持されます。

Global Accelerator は、AWS エッジロケーションのクライアントからの TCP 接続を終了し、ほぼ同時にエンドポイントとの新しい TCP 接続を確立します。これにより、クライアントの応答時間が短くなり (待ち時間が短くなり) 、スループットが向上します。

標準アクセラレータでは、Global Accelerator はすべてのエンドポイントの正常性を継続的に監視し、アクティブなエンドポイントが正常でないと判断すると、利用可能な別のエンドポイントへのトラフィックの転送を即座に開始します。これにより、AWS 上のアプリケーションの高可用性アーキテクチャを作成できます。Health チェックはカスタムルーティングアクセラレータでは使用されず、フェイルオーバーもありません。これは、トラフィックのルーティング先を指定するためです。

アクセラレータを追加すると、すでに設定済みのセキュリティグループと AWS WAF ルールは、アクセラレータを追加する前に動作し続けます。

グローバルトラフィックをきめ細かく制御する場合は、標準アクセラレータでエンドポイントの重みを設定できます。特定のエンドポイントグループへのトラフィックの割合を増加 (拡大) または減少 (縮小) できます。たとえば、パフォーマンステストやスタックのアップグレードなどです。

Global Accelerator を使用する場合は、次の点に注意してください。

- AWS Direct Connect は、パブリック仮想インターフェイス上で AWS Global Accelerator の IP アドレスプレフィックスをアドバタイズしません。AWS Direct Connect パブリック仮想インターフェイス経由でグローバルアクセラレータと通信するために使用する IP アドレスをアドバタイズしないことをお勧めします。AWS Direct Connect パブリック仮想インターフェイス経由でGlobal Accelerator との通信に使用する IP アドレスをアドバタイズすると、非対称のトラフィックフローが発生します。Global Accelerator へのトラフィックはインターネット経由でGlobal Accelerator に送信されますが、オンプレミスへのトラフィックは返されます。ネットワークは、AWS Direct Connect パブリック仮想インターフェイスを介して提供されます。
- Global Accelerator では、別の AWS アカウントに属するリソースをエンドポイントとして追加することはできません。

トピック

- AWS Global Accelerator
- AWS Global Accelerator
- トラフィックダイヤルとエンドポイントの重みによるトラフィックフロー管理
- AWS Global Accelerator

AWS Global Accelerator

AWS Global Accelerator は、その接続に適用されるアイドルタイムアウト期間を設定します。アイドルタイムアウト期間が経過するまでデータが送受信されなかった場合、Global Accelerator は接続を閉じます。接続を維持するには、アイドルタイムアウト期間が経過する前に、クライアントまたはエンドポイントが少なくとも 1 バイトのデータを送信する必要があります。

ネットワーク接続のグローバルアクセラレータアイドルタイムアウトは、接続の種類によって異なります。

- TCP 接続のタイムアウトは 340 秒です。
- UDP 接続のタイムアウトは 30 秒です。

Global Accelerator は、エンドポイントが正常でないとマークされている場合でも、アイドルタイムアウトに達するまでエンドポイントにトラフィックを誘導し続けます。Global Accelerator は、必要に応じて、新しい接続が開始されたときまたはアイドルタイムアウト後にのみ、新しいエンドポイントを選択します。

AWS Global Accelerator

Global Accelerator がアクセラレータに割り当てる静的 IP アドレス (標準アクセラレータの場合は、独自の IP アドレスプールから指定) を使用して、ユーザーの場所に関係なく、ユーザーのいる場所の近くにある AWS グローバルネットワークにインターネットトラフィックをルーティングします。標準アクセラレータの場合、アドレスを、ネットワークロードバランサー、アプリケーションロードバランサー、Amazon EC2 インスタンス、または 1 つの AWS リージョンまたは複数のリージョンで実行される Elastic IP アドレスに関連付けます。カスタムルーティングアクセラレータの場合、1 つ以上のリージョンの VPC サブネット内の EC2 宛先にトラフィックを誘導します。AWS グローバルネットワーク経由でトラフィックをルーティングすると、トラフィックがパブリックインターネット経由で複数のホップを取る必要がないため、可用性とパフォーマンスが向上します。静的 IP アド

レスを使用すると、受信アプリケーショントラフィックを複数の AWS リージョンの複数のエンドポイントリソースに分散することもできます。

さらに、静的 IP アドレスを使用すると、アプリケーションをより多くのリージョンに追加したり、リージョン間でアプリケーションを移行したりすることが容易になります。固定 IP アドレスを使用すると、ユーザーが変更を行う際に一貫した方法でアプリケーションに接続できるようになります。

必要に応じて、独自のカスタムドメイン名をアクセラレータの静的 IP アドレスに関連付けることができます。詳細については、「カスタムドメイントラフィックをアクセラレータにルーティングする」を参照してください。

グローバルアクセラレータは、独自の IP アドレス範囲を AWS に持ち込み、そのプールから静的 IP アドレスを指定しない限り、IP アドレスの Amazon プールから静的 IP アドレスを提供します。（詳しくは、AWS Global Accelerator で独自の IP アドレス (BYOIP) を使用する を参照してください）。コンソールでアクセラレータを作成するには、まず Global Accelerator に対して、アクセラレータの名前を入力するか、独自の固定 IP アドレスを選択して固定 IP アドレスをプロビジョニングするように指示します。アクセラレータを作成する手順については、AWS Global Accelerator の使用開始。

スタティック IP アドレスは、アクセラレータをディセーブルにしてトラフィックの受け入れやルーティングを行わなくても、存在している限り、アクセラレータに割り当てられたままになります。しかし、ときにdeleteアクセラレータを使用すると、割り当てられた静的 IP アドレスが失われるため、それらを使用してトラフィックをルーティングできなくなります。Global Accelerator でタグベースのアクセス許可などの IAM ポリシーを使用すると、アクセラレータを削除するアクセス許可を持つユーザーを制限できます。詳細については、「 タグベースのポリシー」を参照してください。

トラフィックダイヤルとエンドポイントの重みによるトラフィックフロー管理

AWS Global Accelerator が標準のアクセラレータを使用してエンドポイントにトラフィックを送信する方法をカスタマイズするには、次の 2 つの方法があります。

- トラフィックダイヤルを変更して、1 つ以上のエンドポイントグループのトラフィックを制限する
- グループのエンドポイントへのトラフィックの比率を変更するための重みを指定する

トラフィックダイヤルの仕組み

標準アクセラレータの各エンドポイントグループに対して、トラフィックダイヤルを設定して、エンドポイントグループに送信されるトラフィックの割合を制御できます。パーセンテージは、すべてのリスナートラフィックではなく、すでにエンドポイントグループにリダイレクトされているトラフィックにのみ適用されます。

トラフィックダイヤルは、エンドポイントグループが受け入れるトラフィックの部分を、そのエンドポイントグループ宛てのトラフィックの割合として制限します。たとえば、エンドポイントグループのトラフィックダイヤルをus-east-1を 50 (つまり 50%) に設定し、アクセラレータはそのエンドポイントグループに 100 人のユーザー要求を送信する場合、グループによって受け入れられる要求は 50 個だけです。アクセラレータは、残りの 50 個の要求を他のリージョンのエンドポイントグループに送信します。

詳細については、「トラフィックダイヤルによるトラフィックフローの調整」を参照してください。

重みの仕組み

標準アクセラレータの各エンドポイントに対して、重みを指定できます。重みは、アクセラレータが各エンドポイントにルーティングするトラフィックの割合を変更する数値です。これは、リージョン内でパフォーマンステストを行う場合などに便利です。

重みは、アクセラレータがエンドポイントに送信するトラフィックの割合を決定する値です。デフォルトでは、エンドポイントの重みは 128 です。つまり、重みの最大値 255 の半分です。

アクセラレータは、エンドポイントグループ内のエンドポイントの重みの合計を計算し、合計に対する各エンドポイントの重みの比率に基づいて、トラフィックをエンドポイントに転送します。重みの動作の例については、」エンドポイントウェイト。

トラフィックダイヤルと重み付けは、標準アクセラレータがさまざまな方法でトラフィックを処理する方法に影響します。

- トラフィックダイヤルは、エンドポイントグループ。トラフィックダイヤルを使用すると、近接性などの他の要因に基づいて、アクセラレータがすでにそのグループに転送したトラフィックを「ダイヤルダウン」することによって、グループに対するトラフィックの割合 (またはすべてのトラフィック) を切り取ることができます。
- 一方、ウェイトを使用して、個々のエンドポイントですエンドポイントグループ内の 重み付けは、エンドポイントグループ内のトラフィックを分割する方法を提供します。たとえば、重みを使用して、リージョン内の特定のエンドポイントのパフォーマンステストを実行できます。

> **Note**
>
> トラフィックのダイヤルと重み付けがフェールオーバーに与える影響の詳細については、「」を参照してください。正常でないエンドポイントのフェイルオーバー。

AWS Global Accelerator

標準アクセラレータの場合、AWS Global Accelerator は静的 IP アドレスに関連付けられているエンドポイントの正常性を自動的にチェックし、正常なエンドポイントにのみユーザートラフィックを送信します。

グローバルアクセラレータには、自動的に実行される既定のヘルスチェックが含まれていますが、チェックやその他のオプションのタイミングを構成できます。カスタムヘルスチェック設定を構成した場合、グローバルアクセラレータは、構成に応じて特定の方法でこれらの設定を使用します。これらの設定は、Amazon EC2 インスタンスまたは Elastic IP アドレスエンドポイント用のグローバルアクセラレータで設定するか、Elastic Load Balancing コンソールでネットワークロードバランサーまたはアプリケーションロードバランサーの設定を構成します。詳細については、「ヘルスチェックオプション」を参照してください。

エンドポイントを標準アクセラレータに追加する場合、トラフィックが送信される前に、正常であると見なされるヘルスチェックに合格する必要があります。Global Accelerator に、標準アクセラレータでトラフィックをルーティングする正常なエンドポイントがない場合、要求はすべてのエンドポイントにルーティングされます。

アクセラレータの種類

AWS Global Accelerator で使用できるアクセラレータには、次の 2 種類があります。標準アクセラレーターおよびカスタムルーティングアクセラレーター。どちらのタイプのアクセラレータも、パフォーマンスと安定性を向上させるために AWS グローバルネットワーク経由でトラフィックをルーティングしますが、それぞれ異なるアプリケーションニーズに合わせて設計されています。

標準アクセラレーター

標準アクセラレータを使用することで、アプリケーションロードバランサー、ネットワークロードバランサー、または Amazon EC2 インスタンスで実行されているアプリケーションの可用性とパフォーマンスを向上させることができます。標準アクセラレータを使用すると、グローバルアクセラレータは、地理的近接性とエンドポイントの正常性に基づいて、リージョンのエンドポイント間でクライアントトラフィックをルーティングします。また、トラフィックダイヤルやエ

ンドポイントの重みなどの制御に基づいて、クライアントトラフィックをエンドポイント間でシフトすることもできます。これは、青/緑のデプロイ、A/B テスト、マルチリージョンのデプロイなど、さまざまなユースケースで機能します。その他のユースケースについては、AWS Global Accelerator。

詳細については、「AWS Global Accelerator で標準アクセラレータを使用する」を参照してください。

カスタムルーティングアクセラレーター

カスタムルーティングアクセラレータは、カスタムアプリケーションロジックを使用して、1 人以上のユーザーを多数の宛先とポートに誘導し、グローバルアクセラレータのパフォーマンス上の利点を得たい場合に適しています。たとえば、VoIP アプリケーションで、複数の発信者を特定のメディアサーバに割り当てて、音声、ビデオ、およびメッセージングセッションを開始します。もう 1 つの例として、地理的位置、プレイヤーのスキル、ゲームモードなどの要素に基づいて、複数のプレイヤーをゲームサーバー上の 1 つのセッションに割り当てるオンラインリアルタイムゲームアプリケーションがあります。

詳細については、「AWS Global Accelerator でカスタムルーティングアクセラレータを使用する」を参照してください。

特定のニーズに基づいて、これらのタイプのアクセラレータのいずれかを作成して、顧客のトラフィックを加速します。

Global Accelerator エッジサーバーの場所と IP アドレス範囲

Global Accelerator エッジサーバーの場所の一覧については、AWS Global Accelerator は現在、どこにデプロイされていますか?「」セクションAWS Global Acceleratorページで.

AWS は、その現在の IP アドレス範囲を JSON 形式で公開します。現在の範囲を表示するには、ip-ranges.json。詳細については、「」を参照してください。AWS IP アドレスの範囲()Amazon Web Services 全般的なリファレンス。

AWS Global Accelerator エッジサーバーに関連付けられた IP アドレス範囲を見つけるには、`ip-ranges.json`次の文字列の「」。

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

次のグローバルアクセラレータエントリ`"region": "GLOBAL"`は、アクセラレータに割り当てられた静的 IP アドレスを参照します。1 つのエリアの Point of Presence (PoP) からのアクセラレータを

通過するトラフィックをフィルタリングする場合は、特定の地理的エリア (us-*またはeu-*。したがって、たとえば、us-*では、米国 (米国) の POP を通過するトラフィックのみが表示されます。

AWS Global Accelerator

AWS Global Accelerator を使用すると、さまざまな目標を達成するのに役立ちます。このセクションでは、グローバルアクセラレータを使用して二ーズを満たす方法を説明します。

アプリケーション使用率の向上のための拡張性

アプリケーションの使用量が増加すると、管理する必要がある IP アドレスとエンドポイントの数も増加します。グローバルアクセラレータを使用すると、ネットワークを拡大または縮小できます。これにより、ロードバランサーや Amazon EC2 インスタンスなどのリージョンリソースを 2 つの静的 IP アドレスに関連付けることができます。これらのアドレスは、クライアントアプリケーション、ファイアウォール、および DNS レコードに 1 回だけ許可リストに含めます。Global Accelerator を使用すると、クライアントアプリケーションの IP アドレスを更新しなくても、AWS リージョンのエンドポイントの追加や削除、青/緑のデプロイの実行、A/B テストを実行できます。これは、クライアントアプリケーションを頻繁に更新できないIoT、小売、メディア、自動車、ヘルスケアのユースケースに特に役立ちます。

レイテンシーに敏感なアプリケーション向けのアクセラレーション

特にゲーム、メディア、モバイルアプリ、財務などの多くのアプリケーションでは、優れたユーザーエクスペリエンスを実現するために、非常に低いレイテンシーを必要とします。ユーザーエクスペリエンスを向上させるために、Global Accelerator はユーザーのトラフィックをクライアントに最も近いアプリケーションエンドポイントに転送し、インターネットのレイテンシーとジッタを低減します。Global Accelerator は、エニーキャストを使用してトラフィックを最も近いエッジロケーションにルーティングし、AWS グローバルネットワーク経由で最も近いリージョンのエンドポイントにルーティングします。Global Acceleratorは、ネットワークパフォーマンスの変化に迅速に対応し、ユーザーのアプリケーションパフォーマンスを向上させます。

ディザスタリカバリとマルチリージョンの耐障害性

利用できるようにするには、ネットワークに依存できる必要があります。災害復旧、高可用性、低レイテンシー、コンプライアンスをサポートするために、複数の AWS リージョンでアプリケーションを実行している可能性があります。Global Accelerator は、プライマリの AWS リージョンでアプリケーションエンドポイントに障害が発生したことを検出すると、次に利用可能な AWS リージョンでアプリケーションエンドポイントへのトラフィックの再ルーティングを即座にトリガーします。

アプリケーションの保護

アプリケーションロードバランサーや Amazon EC2 インスタンスなどの AWS オリジンをパブリックインターネットトラフィックに公開すると、悪意のある攻撃が発生する可能性があります。Global Acceleratorは、2つの静的エントリポイントの後ろにオリジンをマスキングすることで、攻撃のリスクを低減します。AWS Shield による分散サービス妨害 (DDoS) 攻撃からデフォルトで保護されています。Global Accelerator は、プライベート IP アドレスを使用して Amazon Virtual Private Cloud とのピアリング接続を作成し、内部アプリケーションロードバランサーまたはプライベート EC2 インスタンスへの接続をパブリックインターネットから維持します。

VoIPまたはオンラインゲームアプリケーションのパフォーマンスを向上

カスタムルーティングアクセラレータを使用すると、VoIP やゲームアプリケーションに Global Accelerator のパフォーマンス上のメリットを活用できます。たとえば、1 つのゲームセッションに複数のプレイヤーを割り当てるオンラインゲームアプリケーションに Global Accelerator を使用できます。Global Accelerator を使用すると、マルチプレイヤーゲームや VoIP コールなどの特定のエンドポイントにユーザーをマッピングするカスタムロジックを必要とするアプリケーションのレイテンシーとジッタをグローバルに削減できます。1 つのアクセラレータを使用して、1 つまたは複数の AWS リージョンで実行されている数千の Amazon EC2 インスタンスにクライアントを接続できます。同時に、どの EC2 インスタンスおよびポートにどのクライアントを転送するかを完全に制御できます。

AWS Global Accelerator

AWS Global Accelerator 速度比較ツールを使用して、AWS リージョン間で直接インターネットダウンロードと比較したグローバルアクセラレータのダウンロード速度を確認できます。このツールを使用すると、Global Accelerator を使用してデータを転送するときに、ブラウザを使用してパフォーマンスの違いを確認できます。ダウンロードするファイルサイズを選択すると、異なるリージョンのアプリケーションロードバランサーからHTTPS/TCP 経由でファイルがブラウザにダウンロードされます。各リージョンについて、ダウンロード速度の直接比較が表示されます。

速度比較ツールにアクセスするには、次の URL をブラウザにコピーします。

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

> **Important**
>
> テストを複数回実行すると、結果が異なる場合があります。ダウンロード時間は、使用しているラストマイルネットワークの接続の品質、容量、距離など、Global Accelerator の外部要因によって異なります。

AWS Global Accelerator

AWS Global Accelerator の設定は、API または AWS Global Accelerator コンソールを使用して開始できます。Global Accelerator はグローバルサービスであるため、特定の AWS リージョンに関連付けられていません。Global Accelerator は、複数の AWS リージョンのエンドポイントをサポートするグローバルサービスですが、アクセラレーターを作成または更新するには、米国西部 (オレゴン) リージョンを指定する必要があります。

グローバルアクセラレータの使用を開始するには、次の一般的な手順を実行します。

1. 作成するアクセラレータのタイプを選択します。標準アクセラレータまたはカスタムルーティングアクセラレーター
2. グローバルアクセラレータの初期設定を構成します。 アクセラレータの名前を指定します。次に、指定したプロトコルとポート (またはポート範囲) に基づいて、クライアントからのインバウンド接続を処理するように 1 つ以上のリスナーを設定します。
3. アクセラレータのリージョナルエンドポイントグループを構成します。 リスナーに追加する 1 つ以上のリージョンエンドポイントグループを選択できます。リスナーは、エンドポイントグループに追加したエンドポイントにリクエストをルーティングします。

   標準アクセラレータの場合、グローバルアクセラレータは、各エンドポイントに定義されている正常性チェック設定を使用して、グループ内のエンドポイントの正常性を監視します。標準アクセラレータ内の各エンドポイントグループに対して、トラフィックダイヤルパーセンテージを使用して、エンドポイントグループが受け入れるトラフィックの割合を制御します。パーセンテージは、すべてのリスナートラフィックではなく、すでにエンドポイントグループにリダイレクトされているトラフィックにのみ適用されます。デフォルトでは、トラフィックダイヤルは、すべての地域のエンドポイントグループに対して 100% に設定されています。

   カスタムルーティングアクセラレータの場合、トラフィックは、トラフィックを受信するリスナーポートに基づいて、VPC サブネット内の特定の宛先に決定的にルーティングされます。

4. エンドポイントグループへのエンドポイントの追加 追加するエンドポイントは、アクセラレータのタイプによって異なります。
   - 標準アクセラレータの場合、ロードバランサーや EC2 インスタンスのエンドポイントなど、1 つ以上のリージョンリソースを各エンドポイントグループに追加できます。次に、エンドポイントの重みを設定することで、各エンドポイントにルーティングするトラフィックの量を決定できます。
   - カスタムルーティングアクセラレータの場合は、1 つ以上の仮想プライベートクラウド (VPC) サブネットを追加し、最大数千個の Amazon EC2 インスタンス宛先を設定します。

AWS Global Accelerator コンソールを使用して標準アクセラレータまたはカスタムルーティングアクセラレータを作成する方法の詳細については、」AWS Global Accelerator の使用開始。API オペレーションを使用するには、AWS Global Accelerator で使用できる一般的なアクションとAWS Global Accelerator。

AWS Global Accelerator でのタグ付け

タグは、AWS リソースを特定し、整理するのに使用する単語または語句 (メタデータ) です。各リソースには複数のタグを追加でき、各タグにはユーザーが定義したキーと値が含まれています。たとえば、キーが`environment`であり、値は`production`。追加したタグに基づいて、リソースを検索したりフィルタ処理したりできます。AWS Global Accelerator では、アクセラレータにタグを付けることができます。

Global Accelerator でタグを使用する便利な方法を示しています。

- タグを使用して、さまざまなカテゴリの請求情報を追跡する。これを行うには、アクセラレータまたは他の AWS リソース (ネットワークロードバランサー、アプリケーションロードバランサー、Amazon EC2 インスタンスなど) にタグを適用し、タグをアクティブにします。次に、AWS はアクティブなタグ別に利用量とコストを集計したカンマ区切り値 (CSV) ファイルとしてコスト配分レポートを作成します。自社のカテゴリ (たとえばコストセンター、アプリケーション名、所有者) を表すタグを適用すると、複数のサービスにわたってコストを分類することができます。詳細については、AWS 請求とコスト管理ユーザーガイドのコスト配分タグの使用を参照してください。
- タグを使用して、アクセラレーターにタグベースのアクセス許可を適用する。これを行うには、アクションを許可または禁止するタグとタグ値を指定する IAM ポリシーを作成します。詳細については、「 タグベースのポリシー」を参照してください。

使用規約とタグ付けに関する他のリソースへのリンクについては、AWS リソースのタグ付け()AWS 全般のリファレンス。タグの使用に関するヒントについては、タグ付けのベストプラクティス: AWS リソースのタグ付け戦略()AWS ホワイトペーパーブログ。

Global Accelerator でリソースに追加できるタグの最大数は、AWS Global Accelerator のクォータ。

タグを追加するには、AWS コンソール、AWS CLI、またはGlobal Accelerator API を使用できます。この章では、コンソールでタグ付けを使用する手順について説明します。CLI の例を含む AWS CLI およびグローバルアクセラレータ API を使用したタグの操作の詳細については、『AWS Global Accelerator API リファレンス:

- アクセラレータの作成
- TagResource
- UntagResource
- ListTagsForResource

グローバルアクセラレータでのタグ付けのサポート

AWS Global Accelerator は、アクセラレータのタグ付けをサポートしています。

Global Accelerator は、AWS Identity and Access Management (IAM) のタグベースのアクセスコントロール機能をサポートしています。詳細については、「 タグベースのポリシー」を参照してください。

Global Accelerator でタグを追加、編集、削除

次の手順では、Global Accelerator コンソールでアクセラレーターのタグを追加、編集、削除する方法について説明します。

> **Note**
>
> タグは、コンソール、AWS CLI、またはGlobal Accelerator API オペレーションを使用して追加または削除できます。CLI の例を含め、詳細については、「」TagResource()AWS Global Accelerator API リファレンス。

Global Accelerator でタグを追加、編集、または削除するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. タグを追加または更新するアクセラレーターを選択します。
3. 左タグセクションでは、以下のことができます。

   タグの追加

   選択タグの追加をクリックし、タグのキーと、オプションで値を入力します。

   タグの編集

   キー、値、または両方のテキストを更新します。タグの値をクリアすることもできますが、キーが必要です。

   タグの削除

   選択を削除します。値フィールドの右側にある。
4. [Save changes] を選択します。

AWS Global Accelerator

AWS Global Accelerator では、利用した分のみ料金が発生します。アカウント内の各アクセラレーターの時間単位の料金とデータ転送料金が課金されます。詳細については、「」を参照してください。AWS Global Accelerator。

AWS Global Accelerator の使用開始

このチュートリアルでは、コンソールを使用して AWS Global Accelerator を開始するための手順について説明します。AWS グローバルアクセラレーター API オペレーションを使用して、アクセラレーターを作成およびカスタマイズすることもできます。このチュートリアルの各ステップでは、プログラムによってタスクを完了するための対応する API 操作へのリンクがあります。(カスタムルーティングアクセラレータを設定する場合、特定の構成手順で API を使用する必要があります)。AWS Global Accelerator API オペレーションに関する詳細については、「」AWS Global Accelerator。

> **Tip**
>
> Global Accelerator を使用して Web アプリケーションのパフォーマンスと可用性を向上させる方法については、次のセルフペースワークショップを参照してください。AWS Global Accelerator ワークショップ。

グローバルアクセラレータは、複数の AWS リージョンのエンドポイントをサポートするグローバルサービスです。これらのエンドポイントは、AWS リージョン表。

この章には 2 つのチュートリアルがあります。1 つは標準アクセラレータの作成用で、もう 1 つはカスタムルーティングアクセラレータの作成用です。2 種類のアクセラレータの詳細については、」AWS Global Accelerator で標準アクセラレータを使用するおよびAWS Global Accelerator でカスタムルーティングアクセラレータを使用する。

トピック

- 標準アクセラレータの開始方法
- カスタムルーティングアクセラレータの開始方法

標準アクセラレータの開始方法

このセクションでは、トラフィックを最適なエンドポイントにルーティングする標準アクセラレータを作成する手順について説明します。

タスク

- 開始する前に

- ステップ 1: アクセラレーターの作成
- ステップ 2: リスナーの追加
- ステップ 3: エンドポイントグループを追加します。
- ステップ 4: エンドポイントの追加
- ステップ 5: アクセラレーターのテスト
- ステップ6 (オプション) : アクセラレーターの削除

開始する前に

アクセラレータを作成する前に、トラフィックを誘導するエンドポイントとして追加できるリソースを少なくとも 1 つ作成します。たとえば、次のいずれかを作成します。

- エンドポイントとして追加する Amazon EC2 インスタンスを少なくとも 1 つ起動する。詳細については、「」を参照してください。EC2 リソースを作成し、EC2 インスタンスを起動します。()Linux インスタンス用 Amazon EC2 ユーザーガイド。
- オプションで、EC2 インスタンスを含む 1 つ以上のネットワークロードバランサーまたはアプリケーションロードバランサーを作成します。詳細については、「」を参照してください。ネットワークロードバランサーApplication Load Balancer を作成する()Network Load Balancer のユーザーガイド。

Global Accelerator に追加するリソースを作成する場合は、次の点に注意してください。

- Global Accelerator で内部Application Load Balancer または EC2 インスタンスエンドポイントを追加する場合、プライベートサブネットでターゲットを設定することで、インターネットトラフィックが仮想プライベートクラウド (VPC) のエンドポイントに直接送受信されるようにします。ロードバランサーまたは EC2 インスタンスを含む VPC には、インターネットゲートウェイをアタッチして、VPC がインターネットトラフィックを受け入れることを示します。詳細については、「AWS Global Accelerator でのセキュアな VPC 接続」を参照してください。
- Global Accelerator では、ルーターとファイアウォールのルールで、Route 53 ヘルスチェッカーに関連付けられた IP アドレスからのインバウンドトラフィックを許可し、EC2 インスタンスまたは Elastic IP アドレスエンドポイントのヘルスチェックを完了する必要があります。Amazon Route 53 ヘルスチェッカーに関連付けられた IP アドレス範囲に関する情報は、ターゲットグループのヘルスチェック()Amazon Route 53 開発者ガイド。

ステップ 1: アクセラレーターの作成

アクセラレータを作成するには、名前を入力します。

> **Note**
>
> コンソールではなく API オペレーションを使用してこのタスクを実行するには、以下を参照してください。アクセラレータの作成()AWS Global Accelerator。

アクセラレーターを作成するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. 選択アクセラレーターの作成。
3. アクセラレータの名前を指定します。
4. オプションで、1 つ以上のタグを追加するとグローバルアクセラレータリソースを識別するのに役立ちます。
5. [Next] を選択します。

ステップ 2: リスナーの追加

ユーザーからGlobal Accelerator への着信接続を処理するリスナーを作成します。

> **Note**
>
> コンソールではなく API オペレーションを使用してこのタスクを実行するには、以下を参照してください。CreateListener()AWS Global Accelerator。

リスナーを作成するには

1. リポジトリの []リスナーの追加ページで、リスナーに関連付けるポートまたはポート範囲を入力します。リスナーは、ポート 1 ~ 65535 をサポートします。
2. 入力したポートのプロトコルを 1 つまたは複数選択します。
3. オプションで、クライアントのアフィニティを有効にするかどうかを選択します。リスナーのクライアントアフィニティとは、Global Accelerator によって、特定のソース (クライアント) IP ア

ドレスからの接続が常に同じエンドポイントにルーティングされることを意味します。この動作を有効にするには、ドロップダウンリストで、[] を選択します。送信元 IP。

デフォルトは です。なしです。つまり、クライアントアフィニティが有効にならず、Global Accelerator はリスナーのエンドポイントグループ内のエンドポイント間でトラフィックを均等に分散します。

詳細については、「クライアントのアフィニティ」を参照してください。

4. 必要に応じて、[] を選択しますリスナーの追加をクリックして、追加のリスナーを追加します。
5. リスナーの追加が完了したら、[] を選択します。次。

ステップ 3: エンドポイントグループを追加します。

1 つ以上のエンドポイントグループを追加します。各エンドポイントグループは、特定の AWS リージョンに関連付けられます。

> **Note**
>
> コンソールではなく API オペレーションを使用してこのタスクを実行するには、以下を参照してください。エンドポイントグループを作成()AWS Global Accelerator。

エンドポイントグループを追加するには

1. リポジトリの []エンドポイントグループを追加します。ページのリスナーのセクションで、リージョンドロップダウンリストから [] を選択します。
2. 必要に応じて、トラフィックダイヤルに、0 ~ 100 の数値を入力して、このエンドポイントグループのトラフィックの割合を設定します。パーセンテージは、このエンドポイントグループにすでに転送されているトラフィックだけに適用され、すべてのリスナートラフィックには適用されません。デフォルトでは、エンドポイントグループのトラフィックダイヤルは 100 (つまり 100%) に設定されています。
3. 必要に応じて、カスタムヘルスチェック値の場合は、ヘルスチェックを設定する。ヘルスチェック設定を構成すると、Global Accelerator は EC2 インスタンスおよび Elastic IP アドレスエンドポイントのヘルスチェックの設定を使用します。Network Load Balancer およびApplication Load Balancer エンドポイントの場合、グローバルアクセラレータは、ロードバランサ自体に対して既に構成されている状態チェック設定を使用します。詳細については、「ヘルスチェックオプション」を参照してください。

4. 必要に応じて、[] を選択しますエンドポイントグループを追加します。このリスナーまたは他のリスナーのエンドポイントグループを追加します。
5. [Next] を選択します。

ステップ 4: エンドポイントの追加

特定のエンドポイントグループに関連付けられている 1 つ以上のエンドポイントを追加します。この手順は必須ではありませんが、エンドポイントがエンドポイントグループに含まれていない限り、リージョン内のエンドポイントにはトラフィックが送信されません。

> **Note**
>
> アクセラレータをプログラムで作成する場合は、エンドポイントグループの追加の一部としてエンドポイントを追加します。詳細については、「」を参照してください。エンドポイントグループを作成()AWS Global Accelerator。

エンドポイントを追加するには

1. リポジトリの []エンドポイントの作成ページのエンドポイントのセクションで、エンドポイント。
2. 必要に応じて、重量に、0 ~ 255 の数値を入力して、このエンドポイントにトラフィックをルーティングする重みを設定します。エンドポイントに重みを追加する場合、指定した比率に基づいてトラフィックがルーティングされるように Global Accelerator を構成します。デフォルトでは、すべてのエンドポイントの重みは 128 です。詳細については、「エンドポイントウェイト」を参照してください。
3. オプションで、Application Load Balancer エンドポイントの場合は、[]クライアントIPアドレスの保持] を選択してから、アドレスの保持。詳細については、「AWS Global Accelerator でクライアント IP アドレスを保持する」を参照してください。
4. 必要に応じて、[] を選択しますエンドポイントを追加します。をクリックして、さらにエンドポイントを追加します。
5. [Next] を選択します。

あなたが選択した後次をクリックすると、グローバルアクセラレータダッシュボードに、アクセラレータが進行中であるというメッセージが表示されます。プロセスが完了すると、ダッシュボード内のアクセラレーターステータスはアクティブ。

ステップ 5: アクセラレーターのテスト

アクセラレータをテストし、トラフィックがエンドポイントに転送されていることを確認します。たとえば、以下のような curl コマンドを実行し、アクセラレータの静的 IP アドレスのいずれかを置き換えて、リクエストが処理される AWS リージョンを表示します。これは、エンドポイントに異なる重みを設定したり、エンドポイントグループのトラフィックダイヤルを調整する場合に特に役立ちます。

次のような curl コマンドを実行し、アクセラレータの静的 IP アドレスのいずれかを置き換えて、IP アドレスを 100 回呼び出して、各要求が処理された場所の数を出力します。

```
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;
```

エンドポイントグループでトラフィックダイヤルを調整した場合、このコマンドを使用すると、アクセラレータがトラフィックの正しい割合を異なるグループに送信していることを確認できます。詳細については、次のブログ投稿の詳細例を参照してください。AWS Global Accelerator。

ステップ6 (オプション) : アクセラレーターの削除

テストとしてアクセラレータを作成した場合、またはアクセラレータを使用しなくなった場合は、そのアクセラレータを削除できます。コンソールで、アクセラレータを無効にして、削除できます。アクセラレータからリスナーとエンドポイントグループを削除する必要はありません。

コンソールではなく API 操作を使用してアクセラレータを削除するには、まず、アクセラレータに関連付けられているすべてのリスナーとエンドポイントグループを削除し、無効にする必要があります。詳細については、「」を参照してください。アクセラレータの削除オペレーションをAWS Global Accelerator。

エンドポイントまたはエンドポイントグループを削除する場合、またはアクセラレータを削除する場合は、次の点に注意してください。

- アクセラレータを作成すると、グローバルアクセラレータは 2 つの固定 IP アドレスのセットを提供します。IP アドレスは、アクセラレータを無効にしてトラフィックの受け入れやルーティングを行わなくても、存在している限り、アクセラレータに割り当てられます。しかし、ときにdeleteアクセラレータを使用すると、アクセラレータに割り当てられている静的 IP アドレスが失われるため、それらを使用してトラフィックをルーティングできなくなります。ベストプラクティスとして、アクセラレータを誤って削除しないように、アクセス許可があることを確認してく

ださい。タグベースのアクセス権限など、グローバルアクセラレータで IAM ポリシーを使用すると、アクセラレータを削除するアクセス権限を持つユーザーを制限できます。詳細については、「タグベースのポリシー」を参照してください。

- Global Accelerator でエンドポイントグループから削除する前に EC2 インスタンスを終了し、同じプライベート IP アドレスを持つ別のインスタンスを作成し、ヘルスチェックに合格すると、Global Accelerator は新しいエンドポイントにトラフィックをルーティングします。これを回避するには、インスタンスを終了する前にエンドポイントグループから EC2 インスタンスを削除します。

アクセラレーターを削除するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. 削除するアクセラレータを選択します。
3. [Edit] を選択します。
4. 選択アクセラレーターを無効にする] を選択してから、[保存。
5. 削除するアクセラレータを選択します。
6. 選択アクセラレーターの削除。
7. 確認ダイアログボックスで、[Delete (削除)] を選択します。

カスタムルーティングアクセラレータの開始方法

このセクションでは、Virtual Private Cloud (VPC) サブネットエンドポイントの Amazon EC2 インスタンスの宛先にトラフィックを決定的にルーティングするカスタムルーティングアクセラレータを作成するステップについて説明します。

タスク

- 開始する前に
- ステップ 1: カスタムルーティングアクセラレータを作成する
- ステップ 2: リスナーの追加
- ステップ 3: エンドポイントグループを追加します。
- ステップ 4: エンドポイントの追加
- ステップ5 (オプション) : アクセラレーターの削除

開始する前に

カスタムルーティングアクセラレータを作成する前に、トラフィックを誘導するエンドポイントとして追加できるリソースを作成します。カスタムルーティングアクセラレータエンドポイントは仮想プライベートクラウド (VPC) サブネットである必要があります。仮想プライベートクラウドには複数の Amazon EC2 インスタンスを含めることができます。リソースを作成する手順については、以下を参照してください。

- VPC サブネットを作成します。詳細については、「」を参照してください。VPC の作成と設定()AWS Directory Service の管理ガイド。
- オプションで、VPC で 1 つ以上の Amazon EC2 インスタンスを起動します。詳細については、「」を参照してください。EC2 リソースを作成し、EC2 インスタンスを起動します。()Linux インスタンス用 Amazon EC2 ユーザーガイド。

Global Accelerator に追加するリソースを作成する場合は、次の点に注意してください。

- Global Accelerator で EC2 インスタンスエンドポイントを追加する場合、プライベートサブネットでターゲット設定することで、インターネットトラフィックが VPC のエンドポイントに直接送受信されるようにします。EC2 インスタンスを含む VPC には、インターネットゲートウェイをアタッチして、VPC がインターネットトラフィックを受け入れることを示します。詳細については、「AWS Global Accelerator でのセキュアな VPC 接続」を参照してください。

ステップ 1: カスタムルーティングアクセラレータを作成する

> **Note**
>
> コンソールではなく API オペレーションを使用してこのタスクを実行するには、以下を参照してください。カスタムルーティングアクセラレータの作成()AWS Global Accelerator。

アクセラレーターを作成するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. アクセラレータの名前を指定します。
3. を使用する場合アクセラレーターの種類] を選択してから、カスタムルーティング。

4. オプションで、1 つ以上のタグを追加して、アクセラレーター
5. 選択次をクリックして、リスナー、エンドポイントグループ、および VPC サブネットエンドポイントを追加します。

ステップ 2: リスナーの追加

ユーザーからグローバルアクセラレータへの着信接続を処理するリスナーを作成します。

リスナーの作成時に指定する範囲によって、カスタムルーティングアクセラレータで使用できるリスナーポートと宛先 IP アドレスの組み合わせの数が定義されます。柔軟性を最大限に高めるために、大きなポート範囲を指定することをお勧めします。指定する各リスナーポート範囲には、最低 16 個のポートを含める必要があります。

> **Note**
>
> コンソールではなく API オペレーションを使用してこのタスクを実行するには、以下を参照してください。カスタムルーティングリスナーの作成()AWS Global Accelerator。

リスナーを作成するには

1. リポジトリの []リスナーの追加ページで、リスナーに関連付けるポートまたはポート範囲を入力します。リスナーは、ポート 1 ~ 65535 をサポートします。
2. 入力したポートのプロトコルを 1 つまたは複数選択します。
3. 必要に応じて、[] を選択しますリスナーの追加をクリックして、追加のリスナーを追加します。
4. リスナーの追加が完了したら、[] を選択します。次。

ステップ 3: エンドポイントグループを追加します。

1 つ以上のエンドポイントグループを追加します。各エンドポイントグループは、特定の AWS リージョンに関連付けられます。エンドポイントグループごとに、ポート範囲とプロトコルのセットを 1 つ以上指定します。グローバルアクセラレータは、これらを使用して、リージョンのサブネット内の Amazon EC2 インスタンスにトラフィックを誘導します。

指定するポート範囲ごとに、使用するプロトコルも指定します。UDP、TCP、または UDP と TCP の両方。

> **Note**
>
> コンソールではなく API オペレーションを使用してこのタスクを実行するには、以下を参照してください。カスタムルーティングエンドポイントグループの作成()AWS Global Accelerator。

エンドポイントグループを追加するには

1. リポジトリの []エンドポイントグループを追加します。ページのリスナーのセクションで、リージョン。
2. を使用する場合ポートとプロトコルセットで、Amazon EC2 インスタンスのポート範囲とプロトコルを入力します。
   - 「」と入力します。ポートからと[宛先]ポートの範囲を指定します。
   - ポート範囲ごとに、その範囲のプロトコルを指定します。

   ポート範囲はリスナー・ポート範囲のサブセットである必要はありませんが、リスナー・ポート範囲には、指定したポートの合計数をサポートできる十分な合計ポートが必要です。
3. [Save] を選択します。
4. 必要に応じて、[] を選択しますエンドポイントグループを追加します。このリスナーまたは他のリスナーのエンドポイントグループを追加します。
5. [Next] を選択します。

ステップ 4: VPC サブネットエンドポイントの追加

このリージョンエンドポイントグループに、1 つ以上の仮想プライベートクラウド (VPC) サブネットエンドポイントを追加します。カスタムルーティングアクセラレータのエンドポイントは、カスタムルーティングアクセラレータを介してトラフィックを受信できる VPC サブネットを定義します。各サブネットには、1 つまたは複数の Amazon EC2 インスタンスの宛先を含めることができます。

VPC サブネットエンドポイントを追加すると、Global Accelerator は新しいポートマッピングを生成します。このマッピングを使用して、サブネット内の宛先 EC2 インスタンスの IP アドレスにトラフィックをルーティングできます。次に、Global Accelerator API を使用して、サブネットのすべてのポートマッピングの静的リストを取得し、マッピングを使用して特定の EC2 インスタンスにトラフィックを決定的に誘導できます。

> **Note**
>
> 次の手順は、コンソールにエンドポイントを追加する方法を示しています。アクセラレータをプログラムで作成している場合は、エンドポイントグループを使用してエンドポイントを追加します。詳細については、「」を参照してください。カスタムルーティングエンドポイントグループの作成()AWS Global Accelerator。

エンドポイントを追加するには

1. リポジトリの []エンドポイントの追加ページで、エンドポイントを追加するエンドポイントグループのセクションで、エンドポイント。
2. 必要に応じて、次のいずれかを実行して、サブネット内の EC2 インスタンスの宛先へのトラフィックを有効にします。

   - サブネット上のすべての EC2 エンドポイントとポートにトラフィックを転送できるようにするには、すべてのトラフィックを許可する
   - サブネット上の特定の EC2 エンドポイントおよびポートへのトラフィックを許可するには、特定の宛先ソケットアドレスへのトラフィックを許可する。次に、許可する IP アドレスとポートまたはポート範囲を指定します。最後に、[これらの送信先を許可する。

   デフォルトでは、サブネットエンドポイントへのトラフィックは許可されません。トラフィックを許可するオプションを選択しない場合、サブネット内のすべての宛先へのトラフィックは拒否されます。

   > **Note**
   >
   > サブネット内の特定の EC2 インスタンスおよびポートへのトラフィックを有効にする場合は、プログラムで実行できます。詳細については、「」を参照してください。カスタムルーティングトラフィックの許可()AWS Global Accelerator。

3. [Next] を選択します。

あなたが選択した後次のグローバルアクセラレータのダッシュボードには、アクセラレータが進行中であるというメッセージが表示されます。プロセスが完了すると、ダッシュボード内のアクセラレーターステータスはアクティブ。

ステップ5 (オプション) : アクセラレーターの削除

テストとしてアクセラレータを作成した場合、またはアクセラレータを使用しなくなった場合は、そのアクセラレータを削除できます。コンソールで、アクセラレータを無効にして、削除できます。アクセラレータからリスナーとエンドポイントグループを削除する必要はありません。

コンソールではなく API 操作を使用してアクセラレータを削除するには、まず、アクセラレータに関連付けられているすべてのリスナーとエンドポイントグループを削除し、無効にする必要があります。詳細については、「」を参照してください。カスタムルーティングアクセラレータの削除オペレーションをAWS Global Accelerator。

アクセラレータを削除するときは、次の点に注意してください。

- アクセラレータを作成すると、グローバルアクセラレータは 2 つの固定 IP アドレスのセットを提供します。IP アドレスは、アクセラレータを無効にしてトラフィックの受け入れやルーティングを行わなくても、存在している限り、アクセラレータに割り当てられます。しかし、ときにdeleteアクセラレータを使用すると、アクセラレータに割り当てられている静的 IP アドレスが失われるため、それらを使用してトラフィックをルーティングできなくなります。ベストプラクティスとして、アクセラレータを誤って削除しないように、アクセス許可があることを確認してください。Global Accelerator でタグベースのアクセス許可などの IAM ポリシーを使用すると、アクセラレータを削除するアクセス許可を持つユーザーを制限できます。詳細については、「 タグベースのポリシー」を参照してください。

アクセラレーターを削除するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. 削除するアクセラレータを選択します。
3. [Edit] を選択します。
4. 選択アクセラレーターを無効にする] を選択してから、[保存。
5. 削除するアクセラレータを選択します。
6. 選択アクセラレーターの削除。
7. 確認ダイアログボックスで、[Delete (削除)] を選択します。

AWS Global Accelerator で使用できる一般的なアクション

このセクションでは、グローバルアクセラレータリソースで使用できる一般的な AWS Global Accelerator アクションと、関連するドキュメントへのリンクを示します。

標準リソースで使用するアクション

次の表に、グローバルアクセラレータの標準アクセラレータで使用できる一般的なグローバルアクセラレータアクションと、関連ドキュメントへのリンクを示します。

アクション	グローバルアクセラレータコンソールの使用	グローバルアクセラレーターのAPIを使用する
標準アクセラレータを作成する	「標準アクセラレータの開始方法」を参照してください。	「CreateAccelerator 」を参照してください。
標準アクセラレータのリスナーを作成する	「AWS Global Accelerator の標準アクセラレータのリスナー」を参照してください。	「CreateListener 」を参照してください。
標準アクセラレータのエンドポイントグループを作成する	「AWS Global Accelerator の標準アクセラレータのエンドポイントグループ」を参照してください。	「CreateEndpointGroup 」を参照してください。
標準アクセラレータを更新する	「AWS Global Accelerator の標準アクセラレーター」を参照してください。	「UpdateAccelerator 」を参照してください。
アクセラレータの一覧表示	「アクセラレータの表示」を参照してください。	「ListAccelerator 」を参照してください。
アクセラレータに関するすべての情報を取得する	「アクセラレータの表示」を参照してください。	「DescribeAccelerator 」を参照してください。
アクセラレーターの削除	「標準アクセラレータの作成または更新」を参照してください。	「DeleteAccelerator 」を参照してください。

カスタムルーティングリソースで使用するアクション

次の表に、カスタムルーティングアクセラレータで使用できる一般的なグローバルアクセラレータアクションと、関連ドキュメントへのリンクを示します。

アクション	グローバルアクセラレータコンソールの使用	グローバルアクセラレーターのAPIを使用する
カスタムルーティングアクセラレータを作成する	「カスタムルーティングアクセラレータの開始方法」を参照してください。	「CreateCustomRoutingAccelerator」を参照してください。
カスタムルーティングアクセラレータのリスナーを作成する	「AWS Global Accelerator のカスタムルーティングアクセラレータのリスナー」を参照してください。	「CreateCustomRoutingListener」を参照してください。
カスタムルーティングアクセラレータのエンドポイントグループを作成する	「AWS Global Accelerator のカスタムルーティングアクセラレータのエンドポイントグループ」を参照してください。	「CreateCustomRoutingEndpointGroup」を参照してください。
カスタムルーティングアクセラレータを更新する	「AWS Global Accelerator のカスタムルーティングアクセラレータ」を参照してください。	「UpdateCustomRoutingAccelerator」を参照してください。
カスタムルーティングアクセラレータを一覧表示する	「カスタムルーティングアクセラレータの表示」を参照してください。	「ListCustomRoutingAccelerator」を参照してください。
カスタムルーティングアクセラレータに関するすべての情報を取得する	「カスタムルーティングアクセラレータの表示」を参照してください。	「DescribeCustomRoutingAccelerator」を参照してください。
カスタムルーティングアクセラレータを削除する	「カスタムルーティングアクセラレータの作成または更新」を参照してください。	「DeleteCustomRoutingAccelerator」を参照してください。

アクション	グローバルアクセラレータコンソールの使用	グローバルアクセラレーターのAPIを使用する
カスタムルーティングアクセラレータの静的ポートマッピングを取得する	該当なし	「ListCustomRoutingPortMappings」を参照してください。
カスタムルーティングアクセラレータでサブネットのすべての宛先トラフィックを許可する	「VPC サブネットエンドポイントの追加、編集、削除」を参照してください。	「AllowCustomRoutingTraffic」を参照してください。
カスタムルーティングアクセラレータでサブネットのすべての宛先トラフィックを拒否する	「VPC サブネットエンドポイントの追加、編集、削除」を参照してください。	「DenyCustomRoutingTraffic」を参照してください。
カスタムルーティングアクセラレータで特定の宛先へのトラフィックを許可する	「VPC サブネットエンドポイントの追加、編集、削除」を参照してください。	「AllowCustomRoutingTraffic」を参照してください。
カスタムルーティングアクセラレータで特定の宛先へのトラフィックを拒否する	「VPC サブネットエンドポイントの追加、編集、削除」を参照してください。	「DenyCustomRoutingTraffic」を参照してください。

AWS Global Accelerator で標準アクセラレータを使用する

この章では、AWS Global Accelerator で標準アクセラレータを作成するための手順と推奨事項について説明します。標準アクセラレータを使用すると、Global Accelerator はトラフィックに最も近い正常なエンドポイントを選択します。

代わりに、カスタムアプリケーションロジックを使用して、1 人以上のユーザーを多数のエンドポイントの特定のエンドポイントに誘導する場合は、カスタムルーティングアクセラレータを作成します。詳細については、「AWS Global Accelerator でカスタムルーティングアクセラレータを使用する」を参照してください。

標準アクセラレータを設定するには、次を実行します。

1. アクセラレータを作成し、標準のアクセラレータオプションを選択します。
2. 特定のポートまたはポート範囲を持つリスナーを追加し、受け入れるプロトコルを選択します。TCP、UDP、またはその両方
3. エンドポイントリソースがある AWS リージョンごとに 1 つずつ、1 つ以上のエンドポイントグループを追加します。
4. 1 つまたは複数のエンドポイントをエンドポイントグループに追加します。これは必須ではありませんが、エンドポイントがない場合、トラフィックはルーティングされません。エンドポイントは、ネットワークロードバランサー、アプリケーションロードバランサー、Amazon EC2 インスタンス、または Elastic IP アドレスです。

次のセクションでは、標準アクセラレータ、リスナー、エンドポイントグループ、およびエンドポイントを操作します。

トピック

AWS Global Accelerator の標準アクセラレーター

A標準アクセラレーターAWS Global Accelerator では、AWS Global Accelerator の最適なエンドポイントにトラフィックを転送し、世界中のユーザーを持つインターネットアプリケーションの可用性とパフォーマンスを向上させます。各アクセラレータには、1 つ以上のリスナーが含まれます。リスナーは、構成するプロトコル (1 つまたは複数) とポート (またはポート範囲) に基づいて、クライアントからグローバルアクセラレータへの受信接続を処理します。

アクセラレータを作成すると、デフォルトでは、グローバルアクセラレータは 2 つの固定 IP アドレスのセットを提供します。AWS (BYOIP) に自分の IP アドレス範囲を設定するには (BYOIP)、代わりに、アクセラレーターで使用するために独自のプールから静的 IP アドレスを割り当てることができます。詳細については、「AWS Global Accelerator で独自の IP アドレス (BYOIP) を使用する」を参照してください。

> **Important**
>
> IP アドレスは、アクセラレータを無効にしてトラフィックの受け入れやルーティングを行わなくても、存在している限り、アクセラレータに割り当てられます。しかし、ときにdeleteアクセラレータを使用すると、アクセラレータに割り当てられているグローバルアクセラレータの静的 IP アドレスが失われるため、それらを使用してトラフィックをルーティングできなくなります。ベストプラクティスとして、アクセラレータを誤って削除しないように、アクセス許可があることを確認してください。タグベースのアクセス権限など、グローバルアクセラレータで IAM ポリシーを使用すると、アクセラレータを削除するアクセス権限を持つユーザーを制限できます。詳細については、「 タグベースのポリシー」を参照してください。

このセクションでは、グローバルアクセラレータコンソールで標準アクセラレータを作成、編集、または削除する方法について説明します。Global Accelerator で API オペレーションを使用する場合は、AWS Global Accelerator。

トピック

- 標準アクセラレータの作成または更新
- アクセラレーターを削除する
- アクセラレータの表示
- ロードバランサーの作成時にアクセラレーターを追加する

- 地域の静的 IP アドレスの代わりにグローバル静的 IP アドレスの使用

標準アクセラレータの作成または更新

このセクションでは、コンソールで標準アクセラレーターを作成または更新する方法について説明します。グローバルアクセラレータをプログラムで操作するには、AWS Global Accelerator。

標準アクセラレーターを作成するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. 選択アクセラレーターを作成します。。
3. アクセラレーターの名前を入力します。
4. を使用する場合アクセラレーターのタイプで、[]Standard。
5. オプションで、独自の IP アドレス範囲を AWS (BYOIP) に持ち込んだ場合、アクセラレータの静的 IP アドレスを各アドレスプールから 1 つ指定できます。この選択は、アクセラレータの 2 つの固定 IP アドレスのそれぞれに対して行います。

   - 静的 IP アドレスごとに、使用する IP アドレスプールを選択します。

     > **Note**
     >
     > 固定 IP アドレスごとに異なる IP アドレスプールを選択する必要があります。この制限は、高可用性を実現するために、グローバルアクセラレータが各アドレス範囲を別のネットワークゾーンに割り当てるためです。

   - 自分の IP アドレスプールを選択した場合は、プールから特定の IP アドレスも選択します。デフォルトの Amazon IP アドレスプールを選択した場合、Global Accelerator は特定の IP アドレスをアクセラレータに割り当てます。
6. アクセラレーターのリソースを識別できるように、必要に応じて 1 つ以上のタグを追加します。
7. 選択次を使用して、リスナー、エンドポイントグループ、エンドポイントを追加します。

標準アクセラレータを編集するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。

2. アクセラレーターの一覧で、1 つを選択し、[]編集。
3. リポジトリの []アクセラレーターの編集ページで、必要な変更を加えます。たとえば、アクセラレータを無効にして、トラフィックの受け入れやルーティングを行わなくなったり、削除したりできます。または、アクセラレータが無効になっている場合は、有効にすることができます。
4. [Save changes] を選択します。

アクセラレーターを削除する

テストとしてアクセラレータを作成した場合、またはアクセラレータを使用しなくなった場合は、そのアクセラレータを削除できます。コンソールで、アクセラレータを無効にして、削除できます。アクセラレータからリスナーとエンドポイントグループを削除する必要はありません。

コンソールではなく API 操作を使用してアクセラレータを削除するには、まずアクセラレータに関連付けられているすべてのリスナーとエンドポイントグループを削除してから無効にする必要があります。詳細については、「」を参照してください。アクセラレータの削除オペレーションでAWS Global Accelerator。

アクセラレーターを無効にするには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. 一覧で、無効にするアクセラレーターを選択します。
3. [Edit] を選択します。
4. 選択アクセラレーターを無効にする[] を選択してから、[保存。

アクセラレーターを削除するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. [] リストで、削除するアクセラレーターを選択します。
3. [削除] を選択します。

> **Note**
>
> アクセラレーターを無効化していない場合は、削除は使用不可です。

4. 確認ダイアログボックスで、[Delete (削除)] を選択します。

> **Important**
>
> アクセラレータを削除すると、アクセラレータに割り当てられている静的 IP アドレスが失われるため、それらを使用してトラフィックをルーティングできなくなります。

アクセラレータの表示

コンソールで、アクセラレーターに関する情報を表示できます。アクセラレータの説明をプログラムで表示するには、リストアクセラレータおよびDescribeAccelerator()AWS Global Accelerator。

アクセラレーターに関する情報を表示するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. アクセラレータの詳細を表示するには、一覧でアクセラレータを選択し、表示。

ロードバランサーの作成時にアクセラレーターを追加する

AWS マネジメントコンソールでApplication Load Balancer を作成する場合は、必要に応じてアクセラレーターを同時に追加。Elastic Load Balancing とグローバルアクセラレータが連携して、アクセラレータを透過的に追加します。アクセラレータは、ロードバランサーをエンドポイントとしてアカウント内に作成されます。アクセラレーターを使用すると、静的 IP アドレスが提供され、アプリケーションの可用性とパフォーマンスが向上します。

> **Important**
>
> アクセラレーターを作成するには、適切なアクセス権限が必要です。詳細については、「コンソールアクセス、認証管理、アクセス制御に必要な権限」を参照してください。

アクセラレータの設定と表示

アクセラレータの静的 IP アドレスまたは DNS 名にトラフィックを転送するには、DNS 設定を更新する必要があります。トラフィックは、設定の変更が完了するまで、アクセラレータを介してロードバランサーに送信されません。

Amazon EC2 コンソールでグローバルアクセラレータアドオンを選択してロードバランサーを作成したら、統合サービス[] タブをクリックして、アクセラレーターの静的 IP アドレスとドメインネームシステム (DNS) 名を表示します。この情報を使用して、AWS グローバルネットワーク経由でロードバランサーへのユーザートラフィックのルーティングを開始します。アクセラレーターに割り当てられた DNS 名の詳細については、」AWS Global Accelerator での DNS アドレス指定とカスタムドメイン。

アクセラレータを表示および構成するには、Global Accelerator へのAWS マネジメントコンソールで AWS マネジメントコンソール. たとえば、アカウントに関連付けられているアクセラレータを表示したり、アクセラレータにロードバランサーを追加したりできます。詳細については、「アクセラレータの表示」および「 標準アクセラレータの作成または更新」を参照してください。

料金表

AWS Global Accelerator では、ご利用分のみがお支払いの対象になります。アカウント内のアクセラレーターごとに、時間単位の料金とデータ転送料金が課金されます。詳細については、「」を参照してください。AWS Global Accelerator。

アクセラレーターの使用を停止します。

Global Accelerator 経由のロードバランサーへのトラフィックのルーティングを停止するには、次の手順を実行します。

1. DNS 設定を更新して、トラフィックがロードバランサーに直接ポイントされるようにします。
2. アクセラレータからロードバランサーを削除します。詳細については、「」を参照してください。エンドポイントを削除するにはが標準エンドポイントの追加、編集、削除。
3. アクセラレーターを削除します。詳細については、「 アクセラレーターを削除する」を参照してください。

地域の静的 IP アドレスの代わりにグローバル静的 IP アドレスの使用

Amazon EC2 インスタンスなどの AWS リソースの前に静的 IP アドレスを使用する場合は、いくつかのオプションがあります。たとえば、Elastic IP アドレスを割り当てることができます。これは、単一の AWS リージョン内の Amazon EC2 インスタンスまたはネットワークインターフェイスに関連付けることができる静的 IPv4 アドレスです。

グローバルオーディエンスがいる場合は、Global Accelerator を使用してアクセラレーターを作成して、世界中の AWS エッジロケーションからアナウンスされる 2 つのグローバル静的 IP アドレス

を取得できます。Amazon EC2 インスタンス、ネットワークロードバランサー、アプリケーションロードバランサーなど、1 つ以上のリージョンでアプリケーション用に AWS リソースがすでに設定されている場合は、それらをグローバルアクセラレータに簡単に追加して、グローバル静的 IP アドレスを持つことができます。

Global Accelerator によってプロビジョニングされたグローバル静的 IP アドレスの使用を選択すると、アプリケーションの可用性とパフォーマンスが向上します。Global Accelerator を使用すると、静的 IP アドレスは、ユーザーに最も近いエッジロケーションから AWS グローバルネットワークへの着信トラフィックを受け入れます。トラフィックが AWS ネットワーク上にある時間を最大化することで、より速く、より優れたカスタマーエクスペリエンスを提供できます。詳細については、「AWS Global Accelerator 」を参照してください。

アクセラレータは、AWS マネジメントコンソールから、または AWS CLI または SDK で API オペレーションを使用して追加できます。詳細については、「 標準アクセラレータの作成または更新」を参照してください。

アクセラレーターを追加するときは、次の点に注意してください。

- Global Accelerator によってプロビジョニングされるグローバル静的 IP アドレスは、アクセラレータが存在する限り、アクセラレータを無効にしてトラフィックの受け入れやルーティングを行わなくても、割り当てられます。ただし、アクセラレータを削除すると、アクセラレータに割り当てられている静的 IP アドレスは失われます。詳細については、「 アクセラレーターを削除する」を参照してください。
- Global Accelerator では、ご利用分のみがお支払いの対象になります。アカウント内のアクセラレーターごとに、時間単位の料金とデータ転送料金が課金されます。詳細については、「」を参照してください。AWS Global Accelerator。

AWS Global Accelerator の標準アクセラレータのリスナー

AWS Global Accelerator を使用すると、指定したポートとプロトコルに基づいてクライアントからのインバウンド接続を処理するリスナーを追加できます。リスナーは、TCP、UDP、または TCP と UDP の両方のプロトコルをサポートします。

標準アクセラレーターを作成するときに標準リスナーを定義し、いつでもリスナーを追加できます。各リスナーを 1 つ以上のエンドポイントグループに関連付けて、各エンドポイントグループを 1 つの AWS リージョンに関連付けます。

トピック

標準リスナーの追加、編集、削除

このセクションでは、AWS Global Accelerator コンソールでリスナーを操作する方法について説明します。コンソールではなく API 操作を使用してこれらのタスクを実行するには、`CreateListener`,`UpdateListener`, および`DeleteListener`()AWS Global Accelerator API リファレンス。

リスナーを追加するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレーター[] ページで、アクセラレーターを選択します。
3. [リスナーの追加] を選択します。
4. リポジトリの []リスナーの追加ページで、リスナーに関連付けるポートまたはポート範囲を入力します。リスナーは、ポート 1 ~ 65535 をサポートします。
5. 入力したポートのプロトコルを選択します。
6. オプションで、クライアントのアフィニティを有効にするかどうかを選択します。リスナーのクライアントアフィニティとは、Global Accelerator によって、特定のソース (クライアント) IP アドレスからの接続が常に同じエンドポイントにルーティングされることを意味します。この動作を有効にするには、ドロップダウンリストで [] を選択します。送信元 IP。

   デフォルトは です。なしです。つまり、クライアントアフィニティが有効にならず、Global Accelerator はリスナーのエンドポイントグループ内のエンドポイント間でトラフィックを均等に分散します。

   詳細については、「クライアントのアフィニティ」を参照してください。
7. [リスナーの追加] を選択します。

標準リスナーを編集するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレーター[] ページで、アクセラレーターを選択します。

3. リスナーを選択し、[] メニューから [] を選択します。リスナーの編集。
4. リポジトリの []リスナーの編集ページで、リスナーに関連付けるポート、ポート範囲、またはプロトコルを変更します。
5. オプションで、クライアントのアフィニティを有効にするかどうかを選択します。リスナーのクライアントアフィニティとは、Global Accelerator によって、特定のソース (クライアント) IP アドレスからの接続が常に同じエンドポイントにルーティングされることを意味します。この動作を有効にするには、ドロップダウンリストで [] を選択します。送信元 IP。

   デフォルトは です。なしです。つまり、クライアントアフィニティが有効にならず、Global Accelerator はリスナーのエンドポイントグループ内のエンドポイント間でトラフィックを均等に分散します。

   詳細については、「クライアントのアフィニティ」を参照してください。
6. [Save] を選択します。

リスナーを削除するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレーター[] ページで、アクセラレーターを選択します。
3. リスナーを選択し、[] メニューから [] を選択します。を削除します。。
4. 確認ダイアログボックスで、[を削除します。。

クライアントのアフィニティ

標準アクセラレータで使用するステートフルアプリケーションがある場合は、グローバルアクセラレータを使用して、特定のソース (クライアント) IP アドレスのユーザーからのすべての要求を同じエンドポイントリソースに転送して、クライアントの親和性を維持するように選択できます。

デフォルトでは、標準リスナーのクライアントアフィニティはなしと Global Accelerator は、リスナーのエンドポイントグループ内のエンドポイント間でトラフィックを均等に分散します。

Global Accelerator は、一貫したフローのハッシュ生成アルゴリズムを使用して、ユーザーの接続に最適なエンドポイントを選択します。グローバルアクセラレータリソースのクライアントアフィニティをなしGlobal Accelerator は、5 タプルプロパティ (送信元 IP、送信元ポート、送信先 IP、送信先ポート、およびプロトコル) を使用してハッシュ値を選択します。次に、最高のパフォーマ

ンスを提供するエンドポイントを選択します。特定のクライアントが別のポートを使用して Global Accelerator に接続する場合、この設定を指定した場合、Global Accelerator は、クライアントからの接続は常に同じエンドポイントにルーティングされるとは限りません。

接続するたびに、特定のユーザー (送信元 IP アドレスで識別される) を同じエンドポイントにルーティングしてクライアントアフィニティを維持する場合は、クライアントアフィニティを送信元 IP。このオプションを指定すると、Global Accelerator は、2 タプルプロパティ (送信元 IP と送信先 IP) を使用してハッシュ値を選択し、接続するたびに同じエンドポイントにユーザーをルーティングします。グローバルアクセラレータは、選択したエンドポイントグループの後にクライアントアフィニティを適用します。

AWS Global Accelerator の標準アクセラレータのエンドポイントグループ

エンドポイントグループは、AWS Global Accelerator で 1 つ以上の登録されたエンドポイントにリクエストをルーティングします。標準アクセラレータにリスナーを追加する場合、Global Accelerator のトラフィックを転送するエンドポイントグループを指定します。エンドポイントグループとその中のすべてのエンドポイントは、1 つの AWS リージョンに存在する必要があります。ブルー/グリーンのデプロイメントテストなど、目的に応じて、異なるエンドポイントグループを追加できます。

Global Accelerator は、クライアントの場所とエンドポイントグループの正常性に基づいて、標準アクセラレータのエンドポイントグループにトラフィックを転送します。必要に応じて、エンドポイントグループに送信するトラフィックの割合を設定することもできます。トラフィックダイヤルを使用してグループへのトラフィックを増加 (拡大) または減少 (縮小) するには、トラフィックダイヤルを使用します。この割合は、Global Accelerator がすでにエンドポイントグループに送信しているトラフィックにのみ適用されます。リスナーに送信されるすべてのトラフィックには適用されません。

各エンドポイントグループのグローバルアクセラレータのヘルスチェック設定を定義できます。ヘルスチェックの設定を更新することで、Amazon EC2 インスタンスと Elastic IP アドレスエンドポイントのポーリングと正常性の検証の要件を変更できます。ネットワークロードバランサーおよび Application Load Balancer サーのエンドポイントの場合、Elastic Load Balancing コンソールでヘルスチェック設定を構成します。

Global Accelerator は、標準エンドポイントグループに含まれるすべてのエンドポイントの正常性を継続的に監視し、正常なアクティブなエンドポイントにのみ要求をルーティングします。トラフィックをルーティングする正常なエンドポイントがない場合、Global Accelerator はすべてのエンドポイントに要求をルーティングします。

このセクションでは、AWS Global Accelerator コンソールで標準アクセラレータのエンドポイントグループを操作する方法について説明します。AWS Global Accelerator で API オペレーションを使用する場合は、AWS Global Accelerator API リファレンス。

トピック

- 標準エンドポイントグループの追加、編集、削除
- トラフィックダイヤルによるトラフィックフローの調整
- ポートの上書き
- ヘルスチェックオプション

標準エンドポイントグループの追加、編集、削除

エンドポイントグループは、AWS Global Accelerator コンソールまたは API オペレーションを使用して操作します。エンドポイントグループへのエンドポイントの追加または削除は随時行うことができます。

このセクションでは、AWS Global Accelerator コンソールで標準エンドポイントグループを操作する方法について説明します。Global Accelerator で API 操作を使用する場合は、AWS Global Accelerator API リファレンス。

標準のエンドポイントグループを追加するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレーター[] ページで、[] を選択します。
3. 左リスナーセクションのリスナーIDで、エンドポイントグループを追加するリスナーの ID を選択します。
4. 選択エンドポイントグループを追加します。。
5. リスナーのセクションで、ドロップダウンリストからエンドポイントグループの Region を選択して、エンドポイントグループの Region を指定します。
6. 必要に応じて、トラフィックダイヤルに、0 ~ 100 の数値を入力して、このエンドポイントグループのトラフィックの割合を設定します。パーセンテージは、このエンドポイントグループにすでに転送されているトラフィックにのみ適用され、すべてのリスナートラフィックには適用されません。デフォルトでは、トラフィックダイヤルは 100 に設定されています。

7. 必要に応じて、トラフィックをエンドポイントにルーティングするために使用するリスナーポートを上書きし、トラフィックをエンドポイントの特定のポートに再ルーティングするには、ポートオーバーライドを構成する。詳細については、「ポートの上書き」を参照してください。
8. オプションで、EC2 インスタンスおよび Elastic IP アドレスエンドポイントに適用するカスタムヘルスチェック値を指定するには、ヘルスチェックを設定する。詳細については、「ヘルスチェックオプション」を参照してください。
9. 必要に応じて [] を選択します。エンドポイントグループを追加します。を使用して、このリスナーまたは他のリスナーのエンドポイントグループを追加します。
10. 選択エンドポイントグループを追加します。。

エンドポイントグループを編集するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレーター[] ページで、[] を選択します。
3. 左リスナーセクションのリスナーIDで、エンドポイントグループが関連付けられているリスナーの ID を選択します。
4. 選択エンドポイントグループを編集します。。
5. リポジトリの []エンドポイントグループを編集します。ページで、[リージョン] を変更するか、トラフィックダイヤルの割合を調整するか、ヘルスチェックを設定するヘルスチェック設定を変更します。
6. [Save] を選択します。

標準のエンドポイントグループを削除するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレーター[] ページで、[] を選択します。
3. 左リスナーセクションでリスナーを選択し、[] メニューから [] を選択します。を削除します。。
4. 左エンドポイントグループセクションでエンドポイントグループを選択し、[] メニューから [] を選択します。を削除します。。
5. 確認ダイアログボックスで、[] を選択します。を削除します。。

トラフィックダイヤルによるトラフィックフローの調整

標準エンドポイントグループごとに、トラフィックダイヤルを設定して、グループに送信されるトラフィックの割合を制御できます。パーセンテージは、すべてのリスナートラフィックではなく、すでにエンドポイントグループにリダイレクトされているトラフィックにのみ適用されます。

デフォルトでは、アクセラレータ内のすべてのリージョンエンドポイントグループに対して、トラフィックダイヤルは 100 (つまり 100%) に設定されます。トラフィックダイヤルを使用すると、パフォーマンステストやブルー/グリーンのデプロイテストをさまざまな AWS リージョンで簡単に行うことができます。

次に、トラフィックダイヤルを使用してトラフィックフローをエンドポイントグループに変更する方法の例をいくつか示します。

地域別にアプリケーションをアップグレードする

リージョンのアプリケーションをアップグレードする場合、またはメンテナンスを行う場合は、まずトラフィックダイヤルを 0 に設定して、リージョンのトラフィックを遮断します。作業が完了し、リージョンをサービスに戻す準備ができたら、トラフィックダイヤルを100に調整して、トラフィックにダイヤルアップします。

2 つのリージョン間でトラフィックを混在させる

次に、2 つのリージョナルエンドポイントグループのトラフィックダイヤルを同時に変更した場合のトラフィックフローの仕組みの例を示します。アクセラレータ用に 2 つのエンドポイントグループがあるとします。1 つはus-west-2リージョンと 1 つのus-east-1地域：各エンドポイントグループのトラフィックダイヤルを 50% に設定しました。

さて、あなたのアクセラレータに100件の要求があり、米国東海岸から50件、西海岸から50件の要求があるとします。アクセラレータは、トラフィックを次のように指示します。

- 各海岸の最初の 25 リクエスト (合計 50 リクエスト) は、近くのエンドポイントグループから配信されます。つまり、25 のリクエストはus-west-2および 25 は、us-east-1。
- 次の 50 件のリクエストは、反対側のリージョンに送信されます。つまり、東海岸からの次の25のリクエストはus-west-2、西海岸からの次の25件のリクエストはus-east-1。

このシナリオでは、両方のエンドポイントグループが同じ量のトラフィックを処理します。ただし、各リージョンは、両方のリージョンからトラフィックの混在を受信します。

ポートの上書き

デフォルトでは、アクセラレータは、リスナーの作成時に指定したプロトコルとポート範囲を使用して、AWS リージョンのエンドポイントにユーザートラフィックをルーティングします。たとえば、ポート 80 と 443 で TCP トラフィックを受け入れるリスナーを定義すると、アクセラレータはエンドポイント上のこれらのポートにトラフィックをルーティングします。

エンドポイントグループを追加または更新する場合、エンドポイントへのトラフィックのルーティングに使用されるリスナーポートを上書きすることもできます。例えば、リスナーがポート 80 と 443 でユーザトラフィックを受信し、アクセラレーターがそのトラフィックをエンドポイント上のポート 1080 と 1443 にそれぞれルーティングする、ポートオーバーライドを作成できます。

ポートの上書きは、制限付きポートでのリスニングに関する問題を回避するのに役立ちます。エンドポイントでスーパーユーザー (root) 権限を必要としないアプリケーションを実行する方が安全です。ただし、Linux や他のUnix系システムでは、制限付きポート (1024 未満の TCP または UDP ポート) でリッスンするには、スーパーユーザー権限が必要です。リスナー上の制限付きポートをエンドポイント上の制限付きポートにマッピングすることで、ポートオーバーライドによりこの問題を回避できます。Global Accelerator の背後にあるエンドポイントで root アクセスなしでアプリケーションを実行しているときに、制限付きポートでトラフィックを受け入れることができます。たとえば、リスナーポート 443 をエンドポイントポート 8443 に上書きできます。

ポートの上書きごとに、ユーザーからのトラフィックを受け入れるリスナーポートと、Global Accelerator がそのトラフィックをルーティングするエンドポイントポートを指定します。詳細については、「標準エンドポイントグループの追加、編集、削除」を参照してください。

ポートの上書きを作成する場合、次の点に注意してください。

- エンドポイントポートはリスナーポート範囲と重複できません。 ポートオーバーライドで指定したエンドポイントポートは、アクセラレータに対して構成したリスナーポート範囲には含めることはできません。たとえば、アクセラレータに 2 つのリスナーがあり、それらのリスナーのポート範囲をそれぞれ100-199 と 200-299 として定義したとします。ポートオーバーライドを作成する場合、リスナーポート 100 からエンドポイントポート 210 まで定義することはできません。たとえば、エンドポイントポート (210) は、定義したリスナーポート範囲 (200 ~ 299) に含まれているためです。
- 重複するエンドポイントポートはありません。 アクセラレータの 1 つのポートオーバーライドでエンドポイントポートが指定されている場合、別のリスナーポートからのポートオーバーライドで同じエンドポイントポートを指定することはできません。たとえば、リスナーポート 80 からエンドポイントポート 90 へのポートオーバーライドと、リスナーポート 81 からエンドポイントポート 90 へのオーバーライドを指定することはできません。

- Health チェックは元のポートを引き続き使用します。 ヘルスチェックポートとして設定されているポートにポートオーバーライドを指定しても、ヘルスチェックではオーバーライドポートではなく元のポートが使用されます。たとえば、リスナーポート 80 でヘルスチェックを指定し、リスナーポート 80 からエンドポイントポート 480 へのポートオーバーライドも指定するとします。Health チェックは引き続きエンドポイントポート 80 を使用します。ただし、ポート 80 を介して着信するユーザトラフィックは、エンドポイントのポート 480 に送信されます。

  この動作は、ネットワークロードバランサー、Application Load Balancer サー、EC2 インスタンス、Elastic IP アドレスのエンドポイント間で一貫性を維持します。Global Accelerator でポートオーバーライドを指定する場合、ネットワークロードバランサーとアプリケーションロードバランサーはヘルスチェックポートを別のエンドポイントポートにマッピングしないため、Global Accelerator では EC2 インスタンスと Elastic IP の別のエンドポイントポートにヘルスチェックポートをマッピングすることは矛盾します。アドレスエンドポイント。
- セキュリティグループの設定では、ポートアクセスを許可する必要があります。 セキュリティグループがポートの上書きで指定したエンドポイントポートへのトラフィックの到着を許可していることを確認します。たとえば、リスナーポート 443 をエンドポイントポート 1433 に上書きする場合は、そのApplication Load Balancer または Amazon EC2 エンドポイントのセキュリティグループに設定されているポート制限がポート 1433 のインバウンドトラフィックを許可していることを確認します。

ヘルスチェックオプション

AWS Global Accelerator は、ステータスをテストするため、標準エンドポイントに定期的にリクエストを送信します。これらのヘルスチェックは自動的に実行されます。各エンドポイントの正常性と正常性チェックのタイミングを判断するためのガイダンスは、エンドポイントリソースの種類によって異なります。

> **Important**
>
> Global Accelerator では、ルーターとファイアウォールのルールで、Route 53 ヘルスチェッカーに関連付けられた IP アドレスからのインバウンドトラフィックを許可し、EC2 インスタンスまたは Elastic IP アドレスエンドポイントのヘルスチェックを完了する必要があります。Amazon Route 53 ヘルスチェッカーに関連付けられた IP アドレス範囲に関する情報は、ターゲットグループのヘルスチェック()Amazon Route 53 開発者ガイド。

エンドポイントグループに対して次のヘルスチェックオプションを設定できます。ヘルスチェックオプションを指定すると、Global Accelerator は EC2 インスタンスまたは Elastic IP アドレスのヘルスチェックの設定を使用しますが、ネットワークロードバランサーやアプリケーションロードバランサーには使用しません。

- アプリケーションロードバランサーまたはNetwork Load Balancer のエンドポイントの場合、Elastic Load Balancing 設定オプションを使用して、リソースのヘルスチェックを設定します。詳細については、「」を参照してください。ターゲットグループのヘルスチェック。グローバルアクセラレータで選択したHealth チェックオプションは、エンドポイントとして追加したアプリケーションロードバランサーまたはネットワークロードバランサーには影響しません。

  > **Note**
  >
  > 複数のターゲットグループを含むApplication Load Balancer またはNetwork Load Balancer がある場合、Global Accelerator はロードバランサのエンドポイントが正常であると見なすのは各ターゲットグループには、少なくとも 1 つの正常なターゲットがあります。ロードバランサーの 1 つのターゲットグループに異常なターゲットしか存在しない場合、Global Accelerator はエンドポイントを異常であると見なします。

- TCP で設定されたリスナーに追加される EC2 インスタンスまたは Elastic IP アドレスエンドポイントの場合、ヘルスチェックに使用するポートを指定できます。デフォルトでは、ヘルスチェック用にポートを指定しない場合、Global Accelerator はアクセラレータ用に指定したリスナーポートを使用します。
- UDP リスナーを持つ EC2 インスタンスまたは Elastic IP アドレスエンドポイントの場合、Global Accelerator はヘルスチェックにリスナーポートと TCP プロトコルを使用するため、エンドポイントに TCP サーバーが必要です。

  > **Note**
  >
  > 各エンドポイントの TCP サーバー用に構成したポートが、グローバルアクセラレータの正常性チェック用に指定したポートと同じであることを確認してください。ポート番号が同じでない場合、またはエンドポイントに TCP サーバーを設定していない場合、Global Accelerator は、エンドポイントの正常性に関係なく、エンドポイントを異常としてマークします。

Health チェックポート

Global Accelerator がこのエンドポイントグループの一部であるエンドポイントでヘルスチェックを実行するときに使用するポート。

> **Note**
>
> ヘルスチェックポートのポートオーバーライドを設定することはできません。

ヘルスチェックプロトコル

Global Accelerator がこのエンドポイントグループの一部であるエンドポイントでヘルスチェックを実行するときに使用するプロトコル。

Health チェック間隔

エンドポイントの各ヘルスチェック間隔 (秒)。

しきい値のカウント

異常なターゲットが正常または非正常であると見なされるまでに必要なヘルスチェックの連続回数。

各リスナーは、正常なエンドポイントにのみ要求をルーティングします。エンドポイントを追加した後、正常と見なされるにはヘルスチェックに合格する必要があります。各ヘルスチェックが完了すると、リスナーはヘルスチェック用に確立された接続を終了します。

AWS Global Accelerator の標準アクセラレータのエンドポイント

AWS Global Accelerator の標準アクセラレータのエンドポイントは、ネットワークロードバランサー、アプリケーションロードバランサー、Amazon EC2 インスタンス、または Elastic IP アドレスです。標準アクセラレータの場合、静的 IP アドレスはクライアントにとって単一の通信先として機能し、Global Accelerator は正常なエンドポイントに受信トラフィックを分散します。Global Accelerator は、エンドポイントのエンドポイントグループが属しているリスナーに対して指定したポート (またはポート範囲) を使用して、トラフィックをエンドポイントに転送します。

エンドポイントグループは複数のエンドポイントを持つことができます。各エンドポイントを複数のエンドポイントグループに追加できますが、エンドポイントグループは異なるリスナーに関連付ける必要があります。リソースは、エンドポイントとして追加するときに、有効かつアクティブである必要があります。

Global Accelerator は、標準エンドポイントグループに含まれるすべてのエンドポイントの正常性を継続的に監視します。トラフィックは、正常なアクティブなエンドポイントにのみルーティングされます。Global Accelerator にトラフィックのルーティング先となる正常なエンドポイントがない場合、トラフィックはすべてのエンドポイントにルーティングされます。

特定の種類のグローバルアクセラレータ標準エンドポイントについては、次の点に注意してください。

ロードバランサーエンドポイント

- Application Load Balancer エンドポイントは、インターネットに接続することも、内部を問いません。Network Load Balancer のエンドポイントは、インターネットに接続されている必要があります。

Amazon EC2 インスタンスエンドポイント

- EC2 インスタンスエンドポイント (標準ルーティングアクセラレータとカスタムルーティングアクセラレータの両方) は、次のタイプのいずれかにできません。C1、CC1、CC2、CG2、CR1、CR2、CR2、G2、HI1、HI1、HI1、HI1、HI1、HI1、HI1、HI1、H
- EC2 インスタンスは、一部の AWS リージョンでのみエンドポイントとしてサポートされています。サポートされているリージョンのリストについては「クライアント IP アドレスの保持でサポートされる AWS リージョン」を参照してください。
- インスタンスを終了する前に、Global Accelerator エンドポイントグループから EC2 インスタンスを削除することをお勧めします。Global Accelerator でエンドポイントグループから削除する前に EC2 インスタンスを終了した後、同じ VPC 内に同じプライベート IP アドレスを持つ別のインスタンスを作成し、ヘルスチェックに合格すると、Global Accelerator は新しいエンドポイントにトラフィックをルーティングします。

トピック

標準エンドポイントの追加、編集、削除

トラフィックをリソースに転送できるように、エンドポイントをエンドポイントグループに追加します。標準の終点を編集して、終点の重みを変更できます。または、エンドポイントグループからエン

ドポイントを削除して、アクセラレータからエンドポイントを削除することもできます。エンドポイントを削除しても、エンドポイント自体には影響しませんが、Global Accelerator はトラフィックをそのリソースに転送できなくなりました。

Global Accelerator のエンドポイントは、ネットワークロードバランサー、アプリケーションロードバランサー、Amazon EC2 インスタンス、または Elastic IP アドレスです。最初にこれらのリソースの 1 つを作成してから、グローバルアクセラレータでエンドポイントとして追加できます。リソースは、エンドポイントとして追加するときに、有効かつアクティブである必要があります。

使用状況に基づいて、エンドポイントグループにエンドポイントを追加または削除できます。たとえば、アプリケーションの需要が増えた場合は、より多くのリソースを作成し、1 つ以上のエンドポイントグループにエンドポイントを追加して、増加したトラフィックを処理できます。Global Accelerator は、リクエストを追加するとすぐに、エンドポイントへのリクエストのルーティングを開始し、エンドポイントは最初のヘルスチェックに合格します。エンドポイントへのトラフィックを管理するには、エンドポイントの重みを調整して、多かれ少なかれトラフィックをエンドポイントに送信します。

クライアントの IP アドレスを保持するエンドポイントを追加する場合は、まずクライアント IP アドレスの保持でサポートされる AWS リージョンおよびAWS Global Accelerator でクライアント IP アドレスを保持する。

エンドポイントにサービスを提供する必要がある場合など、エンドポイントグループからエンドポイントを削除できます。エンドポイントを削除するとエンドポイントグループから除外されますが、エンドポイントにそれ以外の影響は及びません。グローバルアクセラレータは、エンドポイントグループから削除するとすぐに、エンドポイントへのトラフィックの送信を停止します。エンドポイントは、現在のすべての要求が完了するのを待機する状態になり、進行中のクライアントトラフィックが中断されることはありません。リクエストの受信を再開する準備ができると、エンドポイントグループにエンドポイントを追加し直すことができます。

このセクションでは、AWS Global Accelerator コンソールでエンドポイントを操作する方法について説明します。AWS Global Accelerator で API オペレーションを使用する場合は、「」を参照してください。AWS Global Accelerator API リファレンス。

標準のエンドポイントを追加するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレーター[] ページで、アクセラレーターを選択します。
3. 左リスナーセクションに追加します。リスナーIDで、リスナーの ID を選択します。

4. 左エンドポイントグループセクションに追加します。エンドポイントグループ IDエンドポイントの追加先となるエンドポイントグループの ID を選択します。
5. 左エンドポイントセクションで [] を選択します。エンドポイントの追加。
6. リポジトリの []エンドポイントの追加[] ページで、ドロップダウンリストからリソースを選択します。

   AWS リソースがない場合、リストには項目がありません。続行するには、ロードバランサー、Amazon EC2 インスタンス、Elastic IP アドレスなどの AWS リソースを作成します。次に、この手順に戻り、リストからリソースを選択します。
7. オプションで、重量に、0 ~ 255 の数値を入力して、このエンドポイントにトラフィックをルーティングする重みを設定します。エンドポイントに重みを追加する場合、指定した比率に基づいてトラフィックがルーティングされるように Global Accelerator を設定します。デフォルトでは、すべてのエンドポイントの重みは 128 です。詳細については、「エンドポイントウェイト」を参照してください。
8. 必要に応じて、インターネットに接続しているApplication Load Balancer エンドポイントでクライアント IP アドレスの保存を有効にします。[]クライアント IP アドレスを保持する[] で、アドレスの保持。

   このオプションは、内部Application Load Balancer と EC2 インスタンスエンドポイントでは常に選択され、Network Load Balancer と Elastic IP アドレスエンドポイントでは選択されません。詳細については、「AWS Global Accelerator でクライアント IP アドレスを保持する」を参照してください。

   > **Note**
   >
   > クライアント IP アドレスを保持するエンドポイントへのトラフィックを追加してルーティングを開始する前に、セキュリティグループなどの必要なすべてのセキュリティ構成が更新され、許可リストにユーザークライアント IP アドレスが含まれることを確認します。
9. [Add endpoint] (エンドポイントの追加) を選択します。

標準の端点を編集するには

エンドポイント設定を編集して、重みを変更できます。詳細については、「エンドポイントウェイト」を参照してください。

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレーター[] ページで、アクセラレーターを選択します。
3. 左リスナーセクションに追加します。リスナーIDで、リスナーの ID を選択します。
4. 左エンドポイントグループセクションに追加します。エンドポイントグループ ID[] で、エンドポイントグループの ID を選択します。
5. 選択エンドポイントの編集。
6. リポジトリの []エンドポイントの編集[] ページで更新を行い、[] を選択します。保存。

エンドポイントを削除するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレーター[] ページで、アクセラレーターを選択します。
3. 左リスナーセクションに追加します。リスナーIDで、リスナーの ID を選択します。
4. 左エンドポイントグループセクションに追加します。エンドポイントグループ ID[] で、エンドポイントグループの ID を選択します。
5. 選択エンドポイントの削除。
6. 確認ダイアログボックスで、[] を選択します。を削除します。。

エンドポイントウェイト

重みは、Global Accelerator が標準アクセラレータのエンドポイントに送信するトラフィックの割合を決定する値です。エンドポイントは、ネットワークロードバランサー、アプリケーションロードバランサー、Amazon EC2 インスタンス、または Elastic IP アドレスです。Global Accelerator は、エンドポイントグループ内のエンドポイントの重みの合計を計算し、合計に対する各エンドポイントの重みの比率に基づいてトラフィックをエンドポイントに転送します。

重み付けルーティングでは、エンドポイントグループ内のリソースにルーティングされるトラフィックの量を選択できます。これは、負荷分散や新しいバージョンのアプリケーションのテストなど、いくつかの点で有用です。

エンドポイントの重みの仕組み

重みを使用するには、エンドポイントグループ内の各エンドポイントに送信するトラフィックの数に対応する相対的な重みを割り当てます。デフォルトでは、エンドポイントの重みは 128 です。つま

り、重みの最大値 255 の半分です。グループ内のすべてのエンドポイントの重みの合計に対する割合として、Global Accelerator は割り当てた重みに基づいてエンドポイントにトラフィックを送信します。

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

たとえば、トラフィックのごく一部を 1 つのエンドポイントに送信し、残りを別のエンドポイントに送信する場合、重みとして 1 つ 255 を指定します。重みが 1 のエンドポイントは、トラフィックの 1/256 (1/1+255) を、もう一方のエンドポイントは 255/256 (255/1+255) を取得します。重みを変更するとバランスは徐々に変更できます。エンドポイントへのトラフィックの送信を停止するには、Global Accelerator でリソースの重みを 0 に変更します。

正常でないエンドポイントのフェイルオーバー

重みが 0 より大きい正常なエンドポイントがエンドポイントグループに存在しない場合、Global Accelerator は、別のエンドポイントグループの重みが 0 より大きい正常なエンドポイントへのフェールオーバーを試みます。このフェールオーバーでは、グローバルアクセラレータはトラフィックダイヤル設定を無視します。したがって、たとえば、エンドポイントグループのトラフィックダイヤルが 0 に設定されている場合、Global Accelerator はそのエンドポイントグループをフェールオーバーの試行に含めます。

Global Accelerator が 3 つのエンドポイントグループ (つまり 3 つの AWS リージョン) を試しても、重みが 0 より大きい正常なエンドポイントを見つけられない場合、トラフィックは、クライアントに最も近いエンドポイントグループ内のランダムなエンドポイントにルーティングされます。つまり、それオープンに失敗する。

次の点に注意してください。

- フェールオーバー用に選択されたエンドポイントグループは、トラフィックダイヤルが 0 に設定されているエンドポイントグループです。
- 最も近いエンドポイントグループが元のエンドポイントグループではない可能性があります。これは、Global Accelerator が元のエンドポイントグループを選択するときに、アカウントトラフィックダイヤル設定を考慮するためです。

たとえば、構成に 2 つのエンドポイントがあり、1 つが正常なエンドポイントと正常でないエンドポイントがあり、それぞれの重みを 0 より大きい値に設定したとします。この場合、グローバルアクセラレータはトラフィックを正常なエンドポイントにルーティングします。ただし、ここで、唯一の正常なエンドポイントの重みをゼロに設定するとします。次に、Global Accelerator は、3 つの追

加のエンドポイントグループを試み、重みが 0 より大きい正常なエンドポイントを検出します。トラフィックが見つからない場合、Global Accelerator は、クライアントに最も近いエンドポイントグループ内のランダムなエンドポイントにトラフィックをルーティングします。

クライアントの IP アドレスを保持するエンドポイントの追加

一部のエンドポイントタイプ (一部の地域) で使用できる機能は、クライアント IP アドレスの保持。この機能を使用すると、エンドポイントに到着したパケットについて、元のクライアントの送信元 IP アドレスを保持できます。この機能は、Application Load Balancer および Amazon EC2 インスタンスエンドポイントで使用できます。カスタムルーティングアクセラレータのエンドポイントには、常にクライアント IP アドレスが保持されます。詳細については、「AWS Global Accelerator でクライアント IP アドレスを保持する」を参照してください。

クライアントの IP アドレス保持機能を使用する場合は、グローバルアクセラレータにエンドポイントを追加するときに、次の点に注意してください。

Elastic Network Interface

クライアントの IP アドレスの保持をサポートするために、Global Accelerator は、エンドポイントが存在するサブネットごとに 1 つずつ、AWS アカウントに Elastic ネットワークインターフェイスを作成します。Elastic Network Interfaces で Global Accelerator を操作する方法については、クライアント IP アドレスの保存に関するベストプラクティス。

プライベートサブネット内のエンドポイント

AWS Global Accelerator を使用して、プライベートサブネット内のApplication Load Balancer または EC2 インスタンスをターゲットにすることができますが、インターネットゲートウェイエンドポイントを含む VPC にアタッチされます。詳細については、「AWS Global Accelerator でのセキュアな VPC 接続」を参照してください。

許可リストにクライアント IP アドレスを追加します。

クライアント IP アドレスを保持するエンドポイントへのトラフィックを追加してルーティングを開始する前に、セキュリティグループなどの必要なセキュリティ構成がすべて更新され、許可リストにユーザークライアント IP アドレスが含まれることを確認します。Network Access Control List (ACL) は、出力 (発信) トラフィックにのみ適用されます。入力 (インバウンド) トラフィックをフィルタリングする必要がある場合は、セキュリティグループを使用する必要があります。

ネットワークアクセスコントロールリスト (ACL) の設定

アクセラレータでクライアント IP アドレスの保存が有効になっている場合、VPC サブネットに関連付けられたネットワーク ACL は出力 (アウトバウンド) トラフィックに適用されます。ただ

し、グローバルアクセラレータを介してトラフィックを終了できるようにするには、ACL をインバウンドおよびアウトバウンドの両方のルールとして設定する必要があります。

たとえば、エフェメラル送信元ポートを使用する TCP クライアントと UDP クライアントが Global Accelerator を介してエンドポイントに接続できるようにするには、エンドポイントのサブネットを、一時的な TCP または UDP ポート (ポート範囲 1024-65535、宛先 0.0.0.0/0) 宛てのアウトバウンドトラフィックを許可するネットワーク ACL に関連付けます。さらに、一致するインバウンドルール (ポート範囲 1024-65535、送信元 0.0.0.0/0) を作成します。

> **Note**
>
> セキュリティグループと AWS WAF ルールは、リソースを保護するために適用できる追加の機能セットです。たとえば、Amazon EC2 インスタンスおよびアプリケーションロードバランサーに関連付けられたインバウンドセキュリティグループルールを使用すると、クライアントがグローバルアクセラレータを介して接続できる宛先ポート (HTTP の場合はポート 80、HTTPS の場合はポート 443 など) を制御できます。Amazon EC2 インスタンスセキュリティグループは、インスタンスに到着するすべてのトラフィックに適用されます。これには、Global Accelerator からのトラフィックや、インスタンスに割り当てられているパブリック IP アドレスまたは Elastic IP アドレスが含まれます。ベストプラクティスとして、トラフィックがGlobal Acceleratorによってのみ配信されるようにするには、プライベートサブネットを使用します。また、アプリケーションのトラフィックを正しく許可または拒否するように、インバウンドセキュリティグループルールが適切に設定されていることを確認してください。

クライアントの IP アドレス保持を使用するようにエンドポイントを移行する

このセクションのガイダンスに従って、アクセラレータ内の 1 つ以上のエンドポイントをユーザーのクライアント IP アドレスを保持するエンドポイントに移行します。必要に応じて、Application Load Balancer エンドポイントまたは Elastic IP アドレスエンドポイントを、クライアント IP アドレスを保持する対応するエンドポイント (アプリケーションロードバランサーまたは EC2 インスタンス) に移行するように選択できます。詳細については、「AWS Global Accelerator でクライアント IP アドレスを保持する」を参照してください。

クライアントの IP アドレスの保存にゆっくりと移行することをお勧めします。まず、クライアント IP アドレスを保持できるようにする、新しいApplication Load Balancer または EC2 インスタンスの

エンドポイントを追加します。次に、エンドポイントに重みを設定して、既存のエンドポイントから新しいエンドポイントにトラフィックをゆっくりと移動します。

> **Important**
>
> クライアント IP アドレスを保持するエンドポイントへのトラフィックのルーティングを開始する前に、グローバルアクセラレータクライアント IP アドレスを許可リストに含めたすべての構成が、代わりにユーザークライアント IP アドレスが含まれるように更新されていることを確認します。

クライアント IP アドレスの保存は、特定の AWS リージョンでのみ利用できます。詳細については、「クライアント IP アドレスの保持でサポートされる AWS リージョン」を参照してください。

このセクションでは、AWS Global Accelerator コンソールでエンドポイントグループの操作方法について説明します。Global Accelerator で API オペレーションを使用する場合は、AWS Global Accelerator API リファレンス。

クライアント IP アドレスを保持して新しいエンドポイントに少量のトラフィックを移動した後、構成が想定どおりに機能することをテストします。次に、対応するエンドポイントの重みを調整して、新しいエンドポイントへのトラフィックの割合を徐々に増やします。

クライアント IP アドレスを保持するエンドポイントに移行するには、まず、次の手順に従って新しいエンドポイントを追加し、インターネットに直接接続する Application Load Balancer エンドポイントの場合は、クライアント IP アドレスの保持を有効にします。（クライアントの IP アドレス保持オプションは、内部アプリケーションロードバランサーと EC2 インスタンスに対して常に選択されます）。

クライアントの IP アドレスを保持するエンドポイントを追加するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレーター[] ページで、アクセラレーターを選択します。
3. 左リスナー[] セクションで、リスナーを選択します。
4. 左エンドポイントグループ[] セクションで、エンドポイントグループを選択します。
5. 左エンドポイントセクションで [] を選択します。エンドポイントの追加。

6. リポジトリの []エンドポイントの追加[] ページで次の操作を行います。エンドポイントドロップダウンリストで、Application Load Balancer エンドポイントまたは EC2 インスタンスエンドポイントを選択します。
7. 左重量フィールドで、既存のエンドポイントに設定されている重みと比較して小さい数値を選択します。たとえば、対応するApplication Load Balancer の重みが 255 の場合、新しいアプリケーションロードバランサーの重みとして 5 を入力します。詳細については、「エンドポイントウェイト」を参照してください。
8. 新しい外部向けApplication Load Balancer エンドポイントの場合は、クライアント IP アドレスを保持する[] で、アドレスの保持。(このオプションは、内部アプリケーションロードバランサーおよび EC2 インスタンスに対して常に選択されます)。
9. [Save changes] を選択します。

次に、次の手順に従って、対応する既存のエンドポイント (クライアント IP アドレスを保持する新しいエンドポイントに置き換える) を編集し、既存のエンドポイントの重みを減らして、それらのエンドポイントへのトラフィックを減らします。

既存のエンドポイントのトラフィックを減らすには

1. リポジトリの []エンドポイントグループページで、クライアント IP アドレスを保持していない既存のエンドポイントを選択します。
2. [Edit] を選択します。
3. リポジトリの []エンドポイントの編集[] ページで次の操作を行います。重量フィールドに、現在の数値よりも小さい数値を入力します。たとえば、既存のエンドポイントの重みが 255 の場合、新しいエンドポイントの重みとして 220 を入力できます (クライアント IP アドレスを保持する場合)。
4. [Save changes] を選択します。

新しいエンドポイントの重みを小さい値に設定して、元のトラフィックのごく一部をテストした後、元のエンドポイントと新しいエンドポイントの重みを調整し続けることで、すべてのトラフィックをゆっくりと移行できます。

たとえば、加重が 200 に設定された既存のApplication Load Balancer から開始し、加重が 5 に設定されたクライアント IP アドレスの保持を有効にした新しいApplication Load Balancer エンドポイントを追加するとします。新しいApplication Load Balancer の重みを増やし、元のApplication Load Balancer の重みを減らして、元のアプリケーションロードバランサーから新しいアプリケーションロードバランサーにトラフィックを徐々にシフトします。例:

- 元重量190/新重量10
- 元の重量180/新しい重量20
- 元重量170/新重量30など。

元のエンドポイントの重みを 0 に減らした場合、（この例の場合）すべてのトラフィックは、クライアントの IP アドレスの保持を含む新しい Application Load Balancer エンドポイントに送信されます。

クライアント IP アドレスの保持を使用するように移行する追加のエンドポイント（アプリケーションロードバランサーまたは EC2 インスタンス）がある場合は、このセクションの手順を繰り返して移行します。

エンドポイントへのトラフィックがクライアント IP アドレスを保持しないようにエンドポイントの設定を元に戻す必要がある場合は、いつでもこれを行うことができます。ないクライアントの IP アドレスを元の値に保持し、エンドポイントの重みを減らすをクライアントの IP アドレスの保存を 0 に設定します。

AWS Global Accelerator でカスタムルーティングアクセラレータを使用する

この章では、AWS Global Accelerator でカスタムルーティングアクセラレータを作成するための手順と推奨事項について説明します。カスタムルーティングアクセラレータを使用すると、アプリケーションロジックを使用して、1 人以上のユーザーを多数の宛先間で特定の Amazon EC2 インスタンスに直接マッピングできます。同時に、Global Accelerator を介してトラフィックをルーティングするパフォーマンスの向上も実現できます。これは、ゲームアプリケーションや Voice over IP（VoIP）セッションなど、特定の EC2 インスタンスおよびポートで実行されている同じセッションでユーザーのグループが相互にやり取りする必要があるアプリケーションがある場合に便利です。

カスタムルーティングアクセラレータのエンドポイントは、仮想プライベートクラウド（VPC）サブネットである必要があります。カスタムルーティングアクセラレータは、それらのサブネット内の Amazon EC2 インスタンスにのみトラフィックをルーティングできます。カスタムルーティングアクセラレータを作成する場合、単一または複数の VPC サブネットで実行されている数千の Amazon EC2 インスタンスを含めることができます。詳細については、「AWS Global Accelerator でのカスタムルーティングアクセラレータの仕組み」を参照してください。

代わりに、Global Accelerator でクライアントに最も近い正常なエンドポイントを自動的に選択する場合は、標準アクセラレータを作成します。詳細については、「AWS Global Accelerator で標準アクセラレータを使用する」を参照してください。

カスタムルーティングアクセラレータを設定するには、以下の操作を実行します。

1. カスタムルーティングアクセラレータを作成するためのガイドラインと要件を確認します。「カスタムルーティングアクセラレータのガイドラインと制約事項」を参照してください。
2. VPC サブネットを作成します。サブネットを Global Accelerator に追加した後は、いつでもサブネットに EC2 インスタンスを追加できます。
3. アクセラレータを作成し、カスタムルーティングアクセラレータのオプションを選択します。
4. リスナーを追加し、グローバルアクセラレータがリッスンするポートの範囲を指定します。Global Accelerator が想定されるすべての宛先にマップするのに十分なポートがある範囲があることを確認してください。これらのポートは、次の手順で指定する宛先ポートとは異なります。リスナーポート要件の詳細については、カスタムルーティングアクセラレータのガイドラインと制約事項。
5. VPC サブネットがある AWS リージョンに 1 つ以上のエンドポイントグループを追加します。エンドポイントグループに対して以下を指定します。

- エンドポイントポート範囲。トラフィックを受信できる宛先 EC2 インスタンスのポートを表します。
- 各宛先ポート範囲のプロトコル：UDP、TCP、または UDP と TCP の両方。

6. エンドポイントサブネットの場合は、サブネット ID を選択します。各エンドポイントグループに複数のサブネットを追加でき、サブネットのサイズは異なる（最大/17）ことができます。

次のセクションでは、カスタムルーティングアクセラレータ、リスナー、エンドポイントグループ、およびエンドポイントの操作手順について説明します。

トピック

- AWS Global Accelerator でのカスタムルーティングアクセラレータの仕組み
- カスタムルーティングアクセラレータのガイドラインと制約事項
- AWS Global Accelerator のカスタムルーティングアクセラレータ
- AWS Global Accelerator のカスタムルーティングアクセラレータのリスナー
- AWS Global Accelerator のカスタムルーティングアクセラレータのエンドポイントグループ
- AWS Global Accelerator のカスタムルーティングアクセラレータ用の VPC サブネットエンドポイント

AWS Global Accelerator でのカスタムルーティングアクセラレータの仕組み

AWS Global Accelerator でカスタムルーティングアクセラレータを使用すると、アプリケーションロジックを使用して、1 人以上のユーザーを多数の宛先間で特定の宛先に直接マッピングできます。同時に、Global Accelerator のパフォーマンス上の利点も得られます。カスタムルーティングアクセラレータは、リスナーポート範囲を仮想プライベートクラウド（VPC）サブネット内の EC2 インスタンスの宛先にマッピングします。これにより、Global Accelerator は、サブネット内の特定の Amazon EC2 プライベート IP アドレスとポート宛先にトラフィックを決定的にルーティングできます。

例えば、カスタムルーティングアクセラレータをオンラインリアルタイムゲームアプリケーションで使用できます。このアプリケーションでは、地理的位置、プレイヤーのスキル、ゲームモードなど、選択した要素に基づいて、Amazon EC2 ゲームサーバー上の 1 つのセッションに複数のプレイヤーを割り当てることができます。または、VoIP またはソーシャルメディアアプリケーションを使用し

て、ボイス、ビデオ、およびメッセージングセッション用に特定のメディアサーバに複数のユーザを割り当てることができます。

アプリケーションは、グローバルアクセラレータ API を呼び出し、グローバルアクセラレータポートとそれに関連する宛先 IP アドレスとポートの完全な静的マッピングを受信できます。その静的マッピングを保存すると、マッチメイキングサービスでそのマッピングを使用してユーザーを特定の宛先 EC2 インスタンスにルーティングできます。Global Accelerator (Global Accelerator) をアプリケーションで使用するためにクライアントソフトウェアを変更する必要はありません。

カスタムルーティングアクセラレータを設定するには、VPC サブネットエンドポイントを選択します。次に、着信接続がマッピングされる宛先ポート範囲を定義して、ソフトウェアがすべてのインスタンスで同じポートセットでリッスンできるようにします。Global Accelerator は、マッチメイキングサービスが、セッションの宛先 IP アドレスとポート番号を、ユーザーに提供する外部 IP アドレスとポートに変換できるようにする静的マッピングを作成します。

アプリケーションのネットワークスタックは、単一のトランスポートプロトコル上で動作する場合もあれば、UDP を高速配信に使用し、TCP を信頼性の高い配信に使用する場合もあります。宛先ポート範囲ごとに UDP、TCP、または UDP と TCP の両方を設定できます。これにより、プロトコルごとに設定を複製することなく、最大限の柔軟性が得られます。

> **Note**
>
> デフォルトでは、カスタムルーティングアクセラレータ内のすべての VPC サブネット宛先はトラフィックを受信できません。これはデフォルトで安全であり、サブネット内のどのプライベート EC2 インスタンスの宛先がトラフィックの受信を許可するかをきめ細かく制御するためです。サブネット、または特定の IP アドレスとポートの組み合わせ (宛先ソケット) へのトラフィックを許可または拒否できます。詳細については、「VPC サブネットエンドポイントの追加、編集、削除」を参照してください。グローバルアクセラレータ API を使用して宛先を指定することもできます。詳細については、「」を参照してください。カスタムルーティングトラフィックの許可およびデニーカスタムルーティングトラフィック。

グローバルアクセラレータでのカスタムルーティングの機能の例

例として、Global Accelerator の背後にある 1,000 個の Amazon EC2 インスタンスで、ゲームセッションや VoIP コールセッションなど、ユーザーのグループが対話する 10,000 個のセッションをサポートするとします。この例では、リスナーポート範囲を 10001 ~ 20040、宛先ポート範囲を 81 ~ 90 に指定します。us-east-1 には、サブネット-1、サブネット 2、サブネット 3、サブネット 4 の VPC サブネットがあるとします。

この例の設定では、各 VPC サブネットのブロックサイズは /24 であるため、251 の Amazon EC2 インスタンスをサポートできます。(5 つのアドレスが予約され、各サブネットからは使用できず、これらのアドレスはマッピングされません)。各 EC2 インスタンスで実行されている各サーバーは、エンドポイントグループの宛先ポートに指定した、次の 10 個のポートを提供します。81-90か つまり、各サブネットには 2510 個のポート (10 x 251) が関連付けられています。各ポートは、セッションに関連付けることができます。

サブネット内の各 EC2 インスタンスに 10 個の宛先ポートを指定したため、Global Accelerator は内部的に 10 個のリスナーポートに関連付けて、EC2 インスタンスへのアクセスに使用できます。これを簡単に説明するために、最初のセットの 10 のエンドポイントサブネットの最初の IP アドレスで始まり、次に 10 のリスナーポートの次の IP アドレスに移動するリスナーポートのブロックがあるとします。

> **Note**
>
> マッピングは実際にはこのように予測できませんが、ここでは順次マッピングを使用して、ポートマッピングがどのように機能するかを示します。リスナーポート範囲の実際のマッピングを決定するには、次の API 操作を使用します。リストカスタムルーティングポートマッピングおよびリストカスタムルーティングポートマッピング宛先別。

この例では、最初のリスナーポートは 10001 です。このポートは、最初のサブネット IP アドレス 192.0.2.4、および最初の EC2 ポート 81 に関連付けられます。次のリスナーポート 10002 は、最初のサブネット IP アドレス 192.0.2.4、2 番目の EC2 ポート 82 に関連付けられます。次の表は、この例のマッピングが、最初の VPC サブネットの最後の IP アドレスから継続され、次に 2 番目の VPC サブネットの最初の IP アドレスまで継続される様子を示しています。

Global Accelerator	VPC サブネット	EC2 インスタンス ポート
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

Global Accelerator	VPC サブネット	EC2 インスタンスポート
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
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

Global Accelerator	VPC サブネット	EC2 インスタンスポート
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
12519	192.0.3.4	89
12520	192.0.3.4	90

カスタムルーティングアクセラレータのガイドラインと制約事項

AWS Global Accelerator でカスタムルーティングアクセラレーターを作成して操作する場合は、次のガイドラインと制限事項に留意してください。

Amazon EC2 インスタンスの送信先

カスタムルーティングアクセラレータの仮想パブリッククラウド (VPC) サブネットエンドポイントには、EC2 インスタンスのみを含めることができます。ロードバランサなどの他のリソースは、カスタムルーティングアクセラレータではサポートされていません。

グローバルアクセラレータでサポートされる EC2 インスタンスのタイプについては、AWS Global Accelerator の標準アクセラレータのエンドポイント。

ポートマッピング

VPC サブネットを追加すると、Global Accelerator は、リスナーポート範囲とサブネットでサポートされているポート範囲との静的ポートマッピングを作成します。特定のサブネットのポートマッピングは変更されません。

カスタムルーティングアクセラレータのポートマッピング一覧をプログラムで表示できます。詳細については、「`ListCustomRoutingPortMappings`」を参照してください。

VPC サブネットサイズ

カスタムルーティングアクセラレータに追加する VPC サブネットは、最小 /28、最大 /17 である必要があります。

リスナーポートの範囲

カスタムルーティングアクセラレータに追加するサブネットに含まれる宛先数に対応できるように、リスナーポート範囲を指定して、十分なリスナーポートを指定する必要があります。リスナーの作成時に指定する範囲によって、カスタムルーティングアクセラレータで使用できるリスナーポートと宛先 IP アドレスの組み合わせの数が決まります。柔軟性を最大限に高め、十分なリスナーポートがないというエラーが表示される可能性を減らすために、大きなポート範囲を指定することをお勧めします。

グローバルアクセラレータは、サブネットをカスタムルーティングアクセラレータに追加するときに、ブロック単位でポート範囲を割り当てます。リスナーポート範囲を直線的に割り当てて、その範囲を必要な宛先ポートの数をサポートするのに十分な大きさにすることをお勧めします。つまり、割り当てるポートの数は、サブネットのサイズに、サブネット内の宛先ポートおよびプロトコル（宛先設定）の数を掛けたものでなければなりません。

> **Note**
>
> グローバルアクセラレータがポートマッピングの割り当てに使用するアルゴリズムでは、この合計を超えるリスナーポートを追加する必要がある場合があります。

リスナーを作成した後、リスナーを編集して追加のポート範囲と関連プロトコルを追加することはできますが、既存のポート範囲を小さくすることはできません。たとえば、リスナーポート範囲が 5,000 ~ 10,000 の場合、ポート範囲を 5900 ~ 10,000 に変更することはできません。また、ポート範囲を 5,000 ~ 9,900 に変更することはできません。

各リスナーポート範囲には、最低 16 個のポートを含める必要があります。リスナーは、ポート 1 ~ 65535 をサポートします。

発信先ポートの範囲

カスタムルーティングアクセラレータのポート範囲を指定するには、2 つの場所があります。1 つは、リスナーを追加するときに指定するポート範囲と、エンドポイントグループに指定する宛先ポート範囲とプロトコルです。

- リスナーポートの範囲: クライアントが接続するグローバルアクセラレータの静的 IP アドレスのリスナーポート。Global Accelerator は、各ポートをアクセラレータの背後にある VPC サブネット上の一意の宛先 IP アドレスおよびポートにマッピングします。
- 発信先ポートの範囲: エンドポイントグループに対して指定する宛先ポート範囲のセット (宛先設定とも呼ばれます) は、トラフィックを受信する EC2 インスタンスポートです。宛先ポートでトラフィックを受信するには、EC2 インスタンスに関連付けられたセキュリティグループでトラフィックを許可する必要があります。

Health チェックとフェイルオーバー

グローバルアクセラレータは、カスタムルーティングアクセラレータの健全性チェックを実行せず、正常なエンドポイントにフェールオーバーしません。カスタムルーティングアクセラレータのトラフィックは、宛先リソースの状態に関係なく、決定的にルーティングされます。

デフォルトでは、すべてのトラフィックが拒否されます

デフォルトでは、カスタムルーティングアクセラレータを介して送られるトラフィックは、サブネット内のすべての宛先に対して拒否されます。宛先インスタンスがトラフィックを受信できるようにするには、サブネットへのすべてのトラフィックを明示的に許可するか、サブネット内の特定のインスタンス IP アドレスとポートへのトラフィックを許可する必要があります。

サブネットまたは特定の宛先を更新してトラフィックを許可または拒否すると、インターネット経由で伝播するまでに時間がかかります。変更が伝播したかどうかを判断するには、`DescribeCustomRoutingAccelerator`API アクションを使用して、アクセラレータのステータスを確認します。詳細については、「」を参照してください。DescribeCustomルーティングアクセラレータ。

AWS CloudFormation はサポートされていません

AWS CloudFormation は、カスタムルーティングアクセラレータではサポートされていません。

AWS Global Accelerator のカスタムルーティングアクセラレータ

Aカスタムルーティングアクセラレータを使用すると、カスタムアプリケーションロジックを使用して、1 人以上のユーザーを多数の宛先の中から特定の宛先に誘導し、AWS グローバルネットワークを使用してアプリケーションの可用性とパフォーマンスを向上させることができます。

カスタムルーティングアクセラレータは、仮想プライベートクラウド (VPC) サブネットで実行されている Amazon EC2 インスタンスのポートにのみトラフィックをルーティングします。カスタムルーティングアクセラレータを使用すると、Global Accelerator はエンドポイントの地理近接性または正常性に基づいてトラフィックをルーティングしません。詳細については、「AWS Global Accelerator でのカスタムルーティングアクセラレータの仕組み」を参照してください。

アクセラレータを作成すると、デフォルトでは、グローバルアクセラレータは 2 つの固定 IP アドレスのセットを提供します。AWS に自分の IP アドレス範囲を使用する場合は (BYOIP)、代わりに、独自のプールから静的 IP アドレスをアクセラレーターで使用するように静的 IP アドレスを割り当てることができます。詳細については、「AWS Global Accelerator で独自の IP アドレス (BYOIP) を使用する」を参照してください。

> **Important**
>
> IP アドレスは、アクセラレータを無効にしてトラフィックの受け入れやルーティングを行わなくても、存在している限り、アクセラレータに割り当てられます。しかし、ときにdeleteアクセラレータを使用すると、アクセラレータに割り当てられているグローバルアクセラレータの静的 IP アドレスが失われるため、それらを使用してトラフィックをルーティングできなくなります。ベストプラクティスとして、アクセラレータを誤って削除しないように、アクセス許可があることを確認してください。Global Accelerator でタグベースのアクセス許可などの IAM ポリシーを使用すると、アクセラレータを削除するアクセス許可を持つユーザーを制限できます。詳細については、「 タグベースのポリシー」を参照してください。

このセクションでは、グローバルアクセラレータコンソールでカスタムルーティングアクセラレータを作成、編集、または削除する方法について説明します。グローバルアクセラレータでの API 操作の使用方法については、AWS Global Accelerator API リファレンス。

トピック

カスタムルーティングアクセラレータの作成または更新

カスタムルーティングアクセラレータを作成するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. 選択アクセラレーターの作成。
3. アクセラレーターの名前を指定します。
4. を使用する場合アクセラレーターのタイプ[] で、カスタムログルーティング。
5. オプションで、独自の IP アドレス範囲を AWS (BYOIP) に持ち込んだ場合は、そのアドレスプールからアクセラレータの静的 IP アドレスを指定できます。この選択は、アクセラレータの 2 つの固定 IP アドレスのそれぞれに対して行います。
   - 静的 IP アドレスごとに、使用する IP アドレスプールを選択します。
   - 自分の IP アドレスプールを選択した場合は、プールから特定の IP アドレスも選択します。デフォルトの Amazon IP アドレスプールを選択した場合、グローバルアクセラレータは特定の IP アドレスをアクセラレータに割り当てます。
6. 必要に応じて、アクセラレーターのリソースを識別できるように、1 つ以上のタグを追加します。
7. 選択次をクリックして、ウィザードの次のページに移動して、リスナー、エンドポイントグループ、および VPC サブネットエンドポイントを追加します。

カスタムルーティングアクセラレータを編集するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. カスタムルーティングアクセラレータのリストで、1 つを選択し、編集。
3. リポジトリの []アクセラレーターの編集ページで、必要な変更を加えます。たとえば、アクセラレータを無効にして削除することができます。

4. [Save] を選択します。

カスタムルーティングアクセラレータの表示

カスタムルーティングアクセラレータに関する情報は、コンソールで表示できます。カスタムルーティングアクセラレータの説明をプログラムで表示するには、」リストカスタムルーティングアクセラレータおよび記述カスタムルーティングアクセラレータAWS Global Accelerator API リファレンスの

カスタムルーティングアクセラレータの情報を表示するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. アクセラレーターの詳細を表示するには、アクセラレーターの選択後、[表示。

カスタムルーティングアクセラレータの削除

テストとしてカスタムルーティングアクセラレータを作成した場合、またはアクセラレータを使用しなくなった場合は、そのアクセラレータを削除できます。コンソールで、アクセラレータを無効にして、削除できます。アクセラレータからリスナーとエンドポイントグループを削除する必要はありません。

コンソールではなく API 操作を使用してカスタムルーティングアクセラレータを削除するには、まずアクセラレータに関連付けられているすべてのリスナーとエンドポイントグループを削除してから無効にする必要があります。詳細については、「」を参照してください。アクセラレータの削除オペレーションでAWS Global Accelerator API リファレンス。

カスタムルーティングアクセラレータを無効にするには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. 一覧で、無効にするアクセラレータを選択します。
3. [Edit] を選択します。
4. 選択アクセラレータを無効にする[] を選択してから、[保存。

カスタムルーティングアクセラレータを削除するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. 一覧で、削除するアクセラレータを選択します。
3. [削除] を選択します。

> **Note**
>
> アクセラレーターの無効化を行っていない場合は、削除は使用不可です。アクセラレータを無効にするには、前述の手順を参照してください。

4. 確認ダイアログボックスで、[Delete (削除)] を選択します。

> **Important**
>
> アクセラレータを削除すると、アクセラレータに割り当てられている静的 IP アドレスが失われるため、それらを使用してトラフィックをルーティングできなくなります。

AWS Global Accelerator のカスタムルーティングアクセラレータのリスナー

AWS Global Accelerator のカスタムルーティングアクセラレータでは、リスナーポートの範囲を指定し、Global Accelerator が VPC サブネットエンドポイントの特定の宛先 Amazon EC2 インスタンスにマッピングする関連付けられたプロトコルを指定します。VPC サブネットエンドポイントを追加すると、Global Accelerator は、リスナーに対して定義したポート範囲と、サブネット内の宛先 IP アドレスとポートの間の静的ポートマッピングを作成します。次に、ポートマッピングを使用して、アクセラレータの静的 IP アドレスをリスナーポートおよびプロトコルとともに指定し、ユーザートラフィックを VPC サブネットの特定の宛先の Amazon EC2 インスタンスの IP アドレスおよびポートに転送できます。

カスタムルーティングアクセラレータを作成するときにリスナーを定義し、いつでもリスナーを追加できます。各リスナーには、VPC サブネットエンドポイントがある AWS リージョンごとに 1 つずつ、1 つ以上のエンドポイントグループを設定できます。カスタムルーティングアクセラレータのリスナーは、TCP プロトコルと UDP プロトコルの両方をサポートします。定義する宛先ポート範囲ごとに、プロトコルを指定します。UDP、TCP、または UDP と TCP の両方。

詳細については、「AWS Global Accelerator でのカスタムルーティングアクセラレータの仕組み」を参照してください。

カスタム・ルーティング・リスナーの追加、編集、削除

このセクションでは、AWS Global Accelerator コンソールでカスタムルーティングリスナーを操作する方法について説明します。AWS Global Accelerator での API オペレーションの使用については、AWS Global Accelerator API リファレンス。

カスタムルーティングアクセラレータのリスナーを追加するには

リスナーの作成時に指定する範囲によって、カスタムルーティングアクセラレータで使用できるリスナーポートと宛先 IP アドレスの組み合わせの数が定義されます。柔軟性を最大限に高めるために、大きなポート範囲を指定することをお勧めします。指定する各リスナーポート範囲には、最低 16 個のポートを含める必要があります。

> **Note**
>
> リスナーを作成した後、リスナーを編集して追加のポート範囲と関連プロトコルを追加することはできますが、既存のポート範囲を小さくすることはできません。

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレータ[] ページで、カスタムルーティングアクセラレーターを選択します。
3. [リスナーの追加] を選択します。
4. リポジトリの []リスナーの追加[] ページで、アクセラレーターに関連付けるリスナーのポート範囲を入力します。

   リスナーはポート1～65535をサポートします。カスタムルーティングアクセラレータで最大限の柔軟性を実現するために、大きなポート範囲を指定することをお勧めします。
5. [リスナーの追加] を選択します。

カスタムルーティングアクセラレータのリスナーを編集する手順は、次のとおりです。

カスタムルーティングアクセラレータのリスナーを編集する場合、追加のポート範囲および関連付けられたプロトコルを追加したり、既存のポート範囲を増やしたり、プロトコルを変更することはできますが、既存のポート範囲を小さくすることはできません。

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレータ[] ページで、アクセラレーターを選択します。
3. リスナーを選択し、[] を選択します。リスナーの編集。
4. リポジトリの []リスナーの編集ページで、既存のポート範囲またはプロトコルに変更を加えるか、新しいポート範囲を追加します。

   既存のポート範囲の範囲は小さくできないことに注意してください。
5. [Save] を選択します。

リスナーを削除するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレータ[] ページで、アクセラレーターを選択します。
3. リスナーを選択し、[] を選択します。を削除します。。
4. 確認ダイアログボックスで、[] を選択します。を削除します。。

AWS Global Accelerator のカスタムルーティングアクセラレータのエンドポイントグループ

AWS Global Accelerator のカスタムルーティングアクセラレータを使用すると、エンドポイントグループは、仮想プライベートクラウド（VPC）サブネット内の Amazon EC2 インスタンスを宛先とするポートとプロトコルを定義します。

VPC サブネットと EC2 インスタンスが配置されている AWS リージョンごとに、カスタムルーティングアクセラレータのエンドポイントグループを作成します。カスタムルーティングアクセラレータの各エンドポイントグループは、複数の VPC サブネットエンドポイントを持つことができます。同様に、各 VPC を複数のエンドポイントグループに追加することもできますが、エンドポイントグループは異なるリスナーに関連付ける必要があります。

エンドポイントグループごとに、リージョンの EC2 インスタンスでトラフィックを誘導するポートを含む 1 つ以上のポート範囲のセットを指定します。エンドポイントグループポート範囲ごとに、使用するプロトコルを指定します。UDP、TCP、または UDP と TCP の両方 これにより、プロトコルごとにポート範囲のセットを複製することなく、最大限の柔軟性が得られます。たとえば、ゲームトラフィックがポート 8080-8090 で UDP で実行されているゲームサーバーがある一方で、ポート 80 で TCP 経由でチャットメッセージをリッスンしているサーバーがあるとします。

詳細については、「AWS Global Accelerator でのカスタムルーティングアクセラレータの仕組み」を参照してください。

カスタムルーティングアクセラレータのエンドポイントグループの追加、編集、または削除します。

カスタムルーティングアクセラレータのエンドポイントグループは、AWS Global Accelerator コンソールまたは API オペレーションを使用して操作します。エンドポイントグループから VPC サブネットエンドポイントは随時追加または削除できます。

このセクションでは、AWS Global Accelerator コンソールでカスタムルーティングアクセラレータのエンドポイントグループを操作する方法について説明します。グローバルアクセラレータでの API 操作の使用方法については、AWS Global Accelerator API リファレンス。

カスタムルーティングアクセラレータのエンドポイントグループを追加するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレータ[] ページで、カスタムルーティングアクセラレータを選択します。
3. 左リスナーセクションのリスナーIDで、エンドポイントグループを追加する先となるリスナーの ID を選択します。
4. 選択エンドポイントグループの追加。
5. リスナーのセクションで、エンドポイントグループの Region を指定します。
6. を使用する場合ポートとプロトコルセットで、Amazon EC2 インスタンスのポート範囲とプロトコルを入力します。
   - と入力します。ポートからと[ポート]ポートの範囲を指定します。
   - ポート範囲ごとに、その範囲のプロトコルを指定します。

ポート範囲はリスナーポート範囲のサブセットである必要はありませんが、カスタムルーティングアクセラレータでエンドポイントグループに指定したポートの総数をサポートできるだけの十分な合計ポートがリスナーポート範囲内に存在する必要があります。

7. [Save] を選択します。
8. 必要に応じて、[] を選択しますエンドポイントグループの追加このリスナーのエンドポイントグループを追加します。別のリスナーを選択し、エンドポイントグループを追加することもできます。
9. 選択エンドポイントグループの追加。

カスタムルーティングアクセラレータのエンドポイントグループを編集するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレータ[] ページで、カスタムルーティングアクセラレータを選択します。
3. 左リスナーセクションのリスナーIDで、エンドポイントグループが関連付けられているリスナーのIDを選択します。
4. 選択エンドポイントグループの編集。
5. リポジトリの []エンドポイントグループの編集ページで、地域、ポートの範囲、またはポートの範囲のプロトコルを変更します。
6. [Save] を選択します。

カスタムルーティングアクセラレータを削除するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレータ[] ページで、アクセラレーターを選択します。
3. 左リスナーセクションで、リスナーを選択し、[] を選択してから [] を選択します。を削除します。。
4. 左エンドポイントグループセクションで、エンドポイントグループを選択し、[] を選択してから [] を選択します。を削除します。。
5. 確認ダイアログボックスで、[] を選択します。を削除します。。

AWS Global Accelerator のカスタムルーティングアクセラレータ用の VPC サブネットエンドポイント

カスタムルーティングアクセラレータのエンドポイントは、アクセラレータを介してトラフィックを受信できる仮想プライベートクラウド（VPC）サブネットです。各サブネットには、1 つまたは複数の Amazon EC2 インスタンスの宛先を含めることができます。サブネットエンドポイントを追加すると、グローバルアクセラレータは新しいポートマッピングを生成します。次に、Global Accelerator API を使用して、サブネットのすべてのポートマッピングの静的リストを取得できます。このリストを使用して、サブネット内の宛先 EC2 インスタンス IP アドレスにトラフィックをルーティングできます。詳細については、「」を参照してください。リストカスタムルーティングポートマッピング。

トラフィックは、サブネット内の EC2 インスタンスにのみ転送できます。ロードバランサーなどの他のリソースには転送できません（標準アクセラレータとは対照的に）。サポートされている EC2 インスタンスタイプについては、AWS Global Accelerator の標準アクセラレータのエンドポイント。

詳細については、「AWS Global Accelerator でのカスタムルーティングアクセラレータの仕組み」を参照してください。

カスタムルーティングアクセラレータに VPC サブネットを追加するときは、次の点に注意してください。

- デフォルトでは、カスタムルーティングアクセラレータを経由するトラフィックは、サブネット内のどの宛先にも到着できません。宛先インスタンスがトラフィックを受信できるようにするには、サブネットへのすべてのトラフィックを許可するか、サブネット内の特定のインスタンス IP アドレスとポート（宛先ソケット）へのトラフィックを有効にする必要があります。

  > **Important**
  >
  > サブネットまたは特定の宛先を更新してトラフィックを許可または拒否すると、インターネット経由で伝播するまでに時間がかかります。変更が伝播したかどうかを判断するには、`DescribeCustomRoutingAcceleratorAPI` アクションを使用して、アクセラレータのステータスを確認します。詳細については、「」を参照してください。DescribeCustomルーティングアクセラレータ。

- VPC サブネットはクライアントの IP アドレスを保持するため、サブネットをカスタムルーティングアクセラレータのエンドポイントとして追加するときは、関連するセキュリティおよび設定情報

を確認する必要があります。詳細については、「クライアントの IP アドレスを保持するエンドポイントの追加」を参照してください。

VPC サブネットエンドポイントの追加、編集、削除

カスタムルーティングアクセラレータのエンドポイントグループに仮想プライベートクラウド（VPC）サブネットエンドポイントを追加して、サブネット内の送信先の Amazon EC2 インスタンスにユーザートラフィックを誘導できるようにします。

サブネットに EC2 インスタンスを追加および削除する場合、または EC2 宛先へのトラフィックを有効または無効にする場合は、それらの宛先がトラフィックを受信できるかどうかを変更します。ただし、グローバルアクセラレータポートマッピングは変更されません。

サブネット内の一部の宛先へのトラフィックを許可する（すべてではなく）には、許可する各 EC2 インスタンスの IP アドレスと、トラフィックを受信するインスタンス上のポートを入力します。指定する IP アドレスは、サブネット内の EC2 インスタンス用である必要があります。サブネットにマッピングされているポートから、ポートまたはポートの範囲を指定できます。

エンドポイントグループから VPC サブネットを削除することで、アクセラレータから VPC サブネットを削除できます。サブネットを削除しても、サブネット自体には影響しませんが、Global Accelerator はサブネットまたはそのサブネット内の Amazon EC2 インスタンスにトラフィックを誘導できなくなりました。さらに、Global Accelerator は VPC サブネットのポートマッピングを再利用して、追加した新しいサブネットにポートマッピングを使用する可能性があります。

このセクションのステップでは、AWS Global Accelerator コンソールで VPC サブネットエンドポイントを追加、編集、または削除する方法について説明します。AWS Global Accelerator での API オペレーションの使用については、AWS Global Accelerator API リファレンス。

VPC サブネットエンドポイントを追加するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレータページで、カスタムルーティングアクセラレータを選択します。
3. 左リスナーセクションに追加します。リスナーIDで、リスナーの ID を選択します。
4. 左エンドポイントグループセクションに追加します。エンドポイントグループ IDで、VPC サブネットエンドポイントを追加するエンドポイントグループ（AWS リージョン）の ID を選択します。
5. 左エンドポイントセクションで、[エンドポイントの追加。

6. リポジトリの []エンドポイントの追加ページに追加します。エンドポイントで、VPC サブネットを選択します。

   VPC がない場合、一覧に項目はありません。続行するには、VPC を少なくとも 1 つ追加してから、次の手順に戻り、リストから VPC を選択します。
7. 追加する VPC サブネットエンドポイントの場合、サブネット内のすべての宛先へのトラフィックを許可または拒否するか、特定の EC2 インスタンスおよびポートへのトラフィックのみを許可するかを選択できます。デフォルトでは、サブネット内のすべての宛先へのトラフィックを拒否します。
8. [Add endpoint] (エンドポイントの追加) を選択します。

特定の宛先へのトラフィックを許可または拒否するには

エンドポイントの VPC サブネットポートマッピングを編集して、サブネット内の特定の EC2 インスタンスおよびポート (宛先ソケット) へのトラフィックを許可または拒否できます。

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレータページで、カスタムルーティングアクセラレータを選択します。
3. 左リスナーセクションに追加します。リスナーIDで、リスナーの ID を選択します。
4. 左エンドポイントグループセクションに追加します。エンドポイントグループ IDで、編集する VPC サブネットエンドポイントのエンドポイントグループ (AWS リージョン) の ID を選択します。
5. エンドポイントのサブネットを選択し、[詳細を表示。
6. リポジトリの []エンドポイントページの下にあるポートマッピング[IP] を選択して、[IP] を選択します。編集。
7. トラフィックを有効にするポートを入力し、[] を選択します。これらの送信先の許可。

サブネットへのすべてのトラフィックを許可または拒否するには

エンドポイントを更新して、VPC サブネット内のすべての宛先へのトラフィックを許可または拒否できます。

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレータページで、カスタムルーティングアクセラレータを選択します。

3. 左リスナーセクションに追加します。リスナーIDで、リスナーの ID を選択します。
4. 左エンドポイントグループセクションに追加します。エンドポイントグループ IDで、更新する VPC サブネットエンドポイントのエンドポイントグループ（AWS リージョン）の ID を選択します。
5. 選択すべてのトラフィックを許可/拒否。
6. すべてのトラフィックを許可するか、すべてのトラフィックを拒否するオプションを選択し、保存。

エンドポイントを削除するには

1. グローバルアクセラレータコンソール (https://console.aws.amazon.com/globalaccelerator/home。
2. リポジトリの []アクセラレータページで、カスタムルーティングアクセラレータを選択します。
3. 左リスナーセクションに追加します。リスナーIDで、リスナーの ID を選択します。
4. 左エンドポイントグループセクションに追加します。エンドポイントグループ IDで、削除する VPC サブネットエンドポイントのエンドポイントグループ（AWS リージョン）の ID を選択します。
5. 選択エンドポイントの削除。
6. 確認ダイアログボックスで、[を削除します。。

AWS Global Accelerator での DNS アドレス指定とカスタムドメイン

この章では、AWS Global Accelerator が DNS ルーティングを行う方法について説明し、グローバルアクセラレータでカスタムドメインを使用する方法について説明します。

トピック

グローバルアクセラレータでの DNS アドレッシングのSupport

カスタムルーティングまたは標準アクセラレータを作成すると、グローバルアクセラレータによって 2 つの静的 IP アドレスがプロビジョニングされます。また、アクセラレータにデフォルトのドメインネームシステム (DNS) 名を割り当てます。`a1234567890abcdef.awsglobalaccelerator.com`で、静的 IP アドレスを指します。静的 IP アドレスは、AWS エッジネットワークからエンドポイントへのエニーキャストを使用してグローバルにアドバタイズされます。アクセラレータの静的 IP アドレスまたは DNS 名を使用して、トラフィックをアクセラレータにルーティングできます。DNS サーバーと DNS リゾルバーは、ラウンドロビンを使用してアクセラレータの DNS 名を解決します。そのため、名前は Amazon Route 53 からランダムな順序で返されたアクセラレータの静的 IP アドレスに解決されます。クライアントは通常、返される最初の IP アドレスを使用します。

> **Note**
>
> グローバルアクセラレータは、DNS 逆引き参照をサポートするために、アクセラレータの静的 IP アドレスをグローバルアクセラレータによって生成された対応する DNS 名にマップする 2 つのポインタ (PTR) レコードを作成します。これは、リバースホストゾーンとも呼ばれます。グローバルアクセラレータによって生成される DNS 名は構成できません。また、カスタムドメイン名を参照する PTR レコードを作成できないことに注意してください。また、グローバルアクセラレータは、AWS に持ち込む IP アドレス範囲 (BYOIP) から静的 IP アドレスの PTR レコードを作成しません。

カスタムドメイントラフィックをアクセラレータにルーティングする

ほとんどのシナリオでは、カスタムドメイン名 (www.example.com) を、割り当てられた静的 IP アドレスまたはデフォルトの DNS 名を使用する代わりに、アクセラレータに置き換えます。まず、Amazon Route 53 または別の DNS プロバイダーを使用してドメイン名を作成し、グローバルアクセラレータ IP アドレスを使用して DNS レコードを追加または更新します。または、カスタムドメイン名をアクセラレータの DNS 名に関連付けることもできます。DNS 構成を完了し、変更がインターネット上に反映されるまで待ちます。これで、クライアントがカスタムドメイン名を使用してリクエストを生成すると、DNS サーバーがランダムに IP アドレス、またはアクセラレータの DNS 名に解決します。

Route 53 を DNS サービスとして使用するときにグローバルアクセラレータでカスタムドメイン名を使用するには、カスタムドメイン名をアクセラレータに割り当てられた DNS 名を指すエイリアスレコードを作成します。エイリアスレコードとは、DNS への Route 53 拡張です。CNAME レコードに似ていますが、ルートドメイン (example.comなどのサブドメインの場合、www.example.com。詳細については、「」を参照してください。エイリアスレコードと非エイリアスレコードの選択『Amazon 53 デベロッパーガイド』にあります。

アクセラレータのエイリアスレコードを使用して Route 53 を設定するには、次のトピックに含まれるガイダンスに従います。エイリアス先『Amazon 53 デベロッパーガイド』にあります。グローバルアクセラレータの情報を表示するには、エイリアス先ページで.

AWS Global Accelerator で独自の IP アドレス (BYOIP) を使用する

AWS Global Accelerator は、アクセラレータのエントリポイントとして静的 IP アドレスを使用します。これらの IP アドレスは、AWS エッジロケーションからのエニーキャストです。デフォルトでは、グローバルアクセラレータは、Amazon IP アドレスプール。グローバルアクセラレータが提供する IP アドレスを使用する代わりに、独自のアドレス範囲の IPv4 アドレスにこれらのエントリポイントを構成できます。このトピックは、独自の IP アドレス範囲を使用してグローバルアクセラレータを使用する方法について説明します。

すべての公開 IPv4 アドレスの範囲の一部またはすべてをオンプレミスのネットワークから AWS アカウントに導入できます。Global Accelerator で使用できます。引き続きアドレス範囲を所有できますが、AWS はこれをインターネット上でアドバタイズします。

AWS に持ち込む IP アドレスを、別の AWS サービスで使用することはできません。この章のステップでは、AWS Global Accelerator でのみ使用するために独自の IP アドレス範囲を使用する方法につ

いて説明します。Amazon EC2 で使用するために独自の IP アドレス範囲を使用するステップについては、自分の IP アドレスを使用する (BYOIP)Amazon EC2 ユーザーガイドを参照してください。

> **Important**
>
> AWS から公開する前に、IP アドレス範囲を他の場所からの公開を停止する必要があります。IP アドレス範囲がマルチホームである場合 (つまり、範囲が複数のサービスプロバイダーによって同時にアドバタイズされる)、アドレス範囲へのトラフィックがネットワークに入ることや、BYOIP 広告ワークフローが正常に完了することを保証することはできません。

アドレス範囲を AWS に設定すると、そのアドレス範囲はアドレスプールとしてアカウントに表示されます。アクセラレータを作成するときに、範囲から 1 つの IP アドレスを割り当てることができます。グローバルアクセラレータは、Amazon IP アドレス範囲から 2 番目の静的 IP アドレスを割り当てます。AWS に 2 つの IP アドレス範囲を設定する場合は、各範囲から 1 つの IP アドレスをアクセラレータに割り当てることができます。この制限は、高可用性を実現するために、グローバルアクセラレータが各アドレス範囲を別のネットワークゾーンに割り当てるためです。

グローバルアクセラレータで独自の IP アドレス範囲を使用するには、要件を確認し、このトピックに記載されている手順に従います。

トピック

Requirements

AWS アカウントごとに最大 2 つの IP アドレス範囲を AWS Global Accelerator に追加できます。

資格を得るには、IP アドレス範囲が以下の要件を満たしている必要があります。

- IP アドレス範囲は、American Registry for Internet Numbers (ARIN)、Réseaux IP Européens Network Coordination Centre (RIPE) または Asia-Pacific Network Information Centre (APNIC) のいずれかに登録している必要があります。アドレス範囲は、事業体または機関エンティティについて登録する必要があります。個人については登録を受けられない場合があります。
- 取得できる最も具体的なアドレス範囲は /24 です。IP アドレスの最初の 24 ビットは、ネットワーク番号を指定します。たとえば、198.100 は IP アドレス 198.100 です。IP アドレスは 198.100 です。
- アドレス範囲内の IP アドレスは、履歴が汚れていない必要があります。つまり、評判が悪かったり、悪意のある行動に関連したりすることはできません。当社は、IP アドレス範囲の評価を調査し、そのアドレスにクリーンな履歴がない IP アドレスが含まれていることを発見した場合、当該範囲を拒否する権利を留保する権利を留保する権利を留保します。

また、IP アドレスの範囲を登録した場所に応じて、次の割り当てと割り当てのネットワークタイプまたはステータスが必要です。

- アリン:`Direct Allocation`および`Direct Assignment`ネットワークタイプ
- 熟した:`ALLOCATED PA`,`LEGACY`, および`ASSIGNED PI`割当てステータス
- APNIC:`ALLOCATED PORTABLE`および`ASSIGNED PORTABLE`割当てステータス

AWS アカウントに IP アドレス範囲を持ち込むための準備: 承認

お客様のみが IP アドレス空間を Amazon に持ち込めるようにするには、次の 2 つの認証が必要です。

- IP アドレス範囲をアドバタイズするには、Amazon の認証が必要です。
- IP アドレス範囲を所有しており、AWS に持ち込む権限があることの証明を提出する必要があります。

> **Note**
>
> BYOIP を使用して IP アドレス範囲を AWS に持ち込む場合、そのアドレス範囲の所有権を別のアカウントや会社に譲渡することはできません。また、ある AWS アカウントから別のアカウントに IP アドレス範囲を直接転送することもできません。所有権を譲渡したり、AWS アカウント間で譲渡したりするには、アドレス範囲のプロビジョニングを解除

する必要があります。その後、新しい所有者は手順に従って、アドレス範囲を AWS アカウントに追加する必要があります。

Amazon に IP アドレス範囲の宣伝を許可するには、署名付き認証メッセージを Amazon に提供します。この許可を提供するには、ルート発信元認可 (ROA) を使用します。ROA は、地域インターネットレジストリ (RIR) から作成するルート通知に関する暗号化ステートメントです。ROA には、IP アドレス範囲、IP アドレス範囲を公開することを許可された自律システム番号 (ASN)、および有効期限が含まれています。ROA は Amazon が特定の自律システム (AS) の IP アドレス範囲を公開することを承認します。

ROA は、AWS アカウントに対して IP アドレス範囲を AWS に持ち込むことを承認しません。この承認を実行するには、IP アドレス範囲について Registry Data Access Protocol (RDAP) の注釈で自己署名付きの X.509 証明書を発行する必要があります。証明書にはパブリックキーが含まれており、AWS はこれを使用してお客様が提供する認証コンテキスト署名を確認します。プライベートキーを安全に管理し、これを使用して認可コンテキストメッセージに署名してください。

以下のセクションでは、これらの認可タスクを完了するための詳細なステップについて説明します。これらのステップのコマンドは、Linux でサポートされています。Windows を使用している場合は、Windows Subsystem for Linuxを使用して Linux コマンドを実行します。

承認を提供する手順

- ステップ 1: ROA オブジェクトを作成する
- ステップ 2: 自己署名 X.509 証明書を作成する
- ステップ 3: 署名付き認可メッセージを作成する

ステップ 1: ROA オブジェクトを作成する

ROA オブジェクトを作成して、Amazon ASN 16509 に対して IP アドレス範囲および IP アドレス範囲を公開することが現在承認されている ASNを承認します。ROA には AWS に持ち込む /24 IP アドレスが含まれている必要があります。また、最大長を /24 に設定する必要があります。

ROA リクエストの作成の詳細については、IP アドレス範囲を登録した場所に応じて、次のセクションを参照してください。

- アリン: ROA のリクエスト数
- 熟した: ROA の管理

- APNIC: ルート管理

ステップ 2: 自己署名 X.509 証明書を作成する

key pair と自己署名 X.509 証明書を作成し、RIR の RDAP レコードに証明書を追加します。以下のステップでは、これらのタスクを実行する方法を説明します。

> **Note**
>
> -opensslコマンドを使用するには、OpenSSL バージョン 1.0.2 以降が必要です。

X.509 証明書を作成して追加するには

1. 次のコマンドを使用して、RSA 2048 ビットのkey pair を生成します。

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

2. 次のコマンドを使用して、key pair からパブリック X.509 証明書を作成します。

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

   この例では、証明書は 365 日で期限切れになり、それ以降は信頼されません。コマンドを実行すると、設定することを確認します。-daysオプションを、適切な有効期限の希望の値に設定します。その他の情報の入力を求められたら、デフォルト値をそのまま使用します。

3. RIR に応じて、次の手順を使用して X.509 証明書を使用して RIR の RDAP レコードを更新します。

   1. 次のコマンドを使用して、証明書を表示します。

      ```
      cat publickey.cer
      ```

   2. 次の手順を実行して、証明書を追加します。

      > **Important**
      >
      > 必ず含まれていることを確認してください-----BEGIN CERTIFICATE-----および-----END CERTIFICATE-----証明書から。

- ARIN の場合は、証明書をPublic Commentsセクションに IP アドレス範囲を入力します。
- RIPE の場合は、証明書を新しいdescrフィールドに IP アドレス範囲を入力します。
- APNIC の場合は、電子メールで公開鍵をhelpdesk@apnic.netAPNIC の IP アドレスに関する正規連絡先に公開して、手動でその IP アドレスをremarksfields。

ステップ 3: 署名付き認可メッセージを作成する

Amazon がお客様の IP アドレス範囲をアドバタイズできるように、署名された認証メッセージを作成します。

メッセージの形式は以下のとおりですが、ここでYYYYMMDDdate はメッセージの有効期限です。

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

署名付き認可メッセージを作成するには

1. プレーンテキストの認可メッセージを作成し、という名前の変数に保存します。text_message、次の例が示すように。サンプルのアカウント番号、IP アドレス範囲、および有効期限を独自の値に置き換えます。

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

2. 認証メッセージに署名するtext_message前のセクションで作成した key pair を使用します。
3. メッセージをという名前の変数に保存するsigned_message、次の例が示すように。

   ```
   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")
   ```

AWS Global Accelerator で使用するためにアドレス範囲をプロビジョニングする

AWS で使用するアドレス範囲をプロビジョニングする場合は、当該範囲の所有者であることを証明し、Amazon による当該範囲の公開を承認します。アドレス範囲を所有していることを確認します。

CLI またはグローバルアクセラレータ API 操作を使用して、アドレス範囲をプロビジョニングする必要があります。この機能は、AWS コンソールでは使用できません。

アドレス範囲をプロビジョニングするには、以下を使用します。ProvisionbyoIPcIDRコマンド。`--cidr-authorization-context`パラメーターは、前のセクションで作成した変数を使用します。ROA メッセージではありません。

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

次に、アドレス範囲のプロビジョニングの例を示します。

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

アドレス範囲のプロビジョニングは非同期オペレーションであるため、呼び出しはすぐに戻ります。ただし、アドレス範囲はその状態が`PENDING_PROVISIONING`~`READY`。プロビジョニングプロセスの完了までには最大で 3 週間かかることがあります。プロビジョニングしたアドレス範囲の状態を監視するには、以下のコマンドを使用します。リストByoIPCIDRSコマンド:

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

IP アドレス範囲の状態の一覧については、」ByoIPcIDR。

IP アドレス範囲がプロビジョニングされると、`State`によって返される`list-byoip-cidrs`、`READY`。例:

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

AWS を通じてアドレス範囲をアドバタイズする

アドレス範囲をプロビジョニングすると、公開することができるようになります。プロビジョンした正確なアドレス範囲をアドバタイズする必要があります。プロビジョンしたアドレス範囲の一部のみアドバタイズすることはできません。さらに、AWS から公開する前に、IP アドレス範囲を他の場所からの公開を停止する必要があります。

CLI またはグローバルアクセラレータ API 操作を使用して、アドレス範囲をアドバタイズする (またはアドバタイズを停止する) 必要があります。この機能は、AWS コンソールでは使用できません。

> **Important**
>
> Global Accelerator でプールの IP アドレスを使用する前に、IP アドレス範囲が AWS によってアドバタイズされていることを確認してください。

アドレス範囲を公開するには、以下を使用します。アドバタイズByoIPcIDRコマンド。

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

次に、グローバルアクセラレータにアドレス範囲のアドバタイズを要求する例を示します。

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

アドバタイズしたアドレス範囲の状態を監視するには、以下のコマンドを使用します。リストByoIPCIDRSコマンド。

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

IP アドレス範囲がアドバタイズされると、Stateによって返されるlist-byoip-cidrs、ADVERTISING。例:

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

```
        }
    ]
}
```

アドレス範囲の公開を停止するには、以下のコマンドを使用します。withdraw-byoip-cidrコマンド。

> **Important**
>
> アドレス範囲のアドバタイズを停止するには、まず、アドレスプールから割り当てられた静的 IP アドレスを持つアクセラレータを削除する必要があります。コンソールまたは API 操作を使用してアクセラレータを削除するには、 アクセラレーターを削除する。

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

以下は、グローバルアクセラレータにアドレス範囲を取り下げるように要求する例です。

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

アドレス範囲のプロビジョニング解除

AWS でアドレス範囲の使用を停止するには、まず、アドレスプールから割り当てられた静的 IP アドレスを持つアクセラレータを削除して、アドレス範囲の公開を停止する必要があります。これらの手順を完了したら、アドレス範囲のプロビジョニングを解除できます。

CLI またはグローバルアクセラレータ API 操作を使用して、アドバタイズを停止し、アドレス範囲のプロビジョニングを解除する必要があります。この機能は、AWS コンソールでは使用できません。

ステップ 1: 関連するアクセラレータを削除します。コンソールまたは API 操作を使用してアクセラレータを削除するには、 アクセラレーターを削除する。

ステップ 2. アドレス範囲の公開を停止します。範囲の公開を停止するには、以下のコマンドを使用します。引き出しYoIPcIDRコマンド。

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

ステップ 3. アドレス範囲のプロビジョニング解除。範囲をプロビジョニング解除するには、次のDEProvisionbyoIPcIDRコマンド。

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

あなたの IP アドレスでアクセラレータを作成します。

これで、IP アドレスでアクセラレータを作成できます。AWS に 1 つのアドレス範囲を設定した場合は、アクセラレータに 1 つの IP アドレスを割り当てることができます。2 つのアドレス範囲を設定した場合は、各アドレス範囲から 1 つの IP アドレスをアクセラレータに割り当てることができます。

固定 IP アドレスに独自の IP アドレスを使用してアクセラレータを作成するには、いくつかのオプションがあります。

- グローバルアクセラレータコンソールを使用して、アクセラレータを作成します。 詳細については、「 標準アクセラレータの作成または更新」および「 カスタムルーティングアクセラレータの作成または更新」を参照してください。
- グローバルアクセラレータ API を使用して、アクセラレータを作成します。 CLI の使用例など、詳細については、」アクセラレータの作成およびカスタムルーティングアクセラレータの作成AWS Global Accelerator 詳細については、

AWS Global Accelerator でクライアント IP アドレスを保持する

AWS Global Accelerator のクライアント IP アドレスを保持およびアクセスするためのオプションは、アクセラレータで設定したエンドポイントによって異なります。着信パケットでクライアントの送信元 IP アドレスを保持できるエンドポイントには、次の 2 種類があります。Application Load Balancer と Amazon EC2 インスタンス。

- グローバルアクセラレータのエンドポイントとしてインターネットに直接接続するApplication Load Balancer を使用する場合、クライアントの IP アドレスの保存は新しいアクセラレータに対してデフォルトで有効になります。つまり、元のクライアントの送信元 IP アドレスは、ロードバランサに到着したパケットに対して保持されます。アクセラレータを作成するとき、または後でアクセラレータを編集することによって、このオプションを無効にすることができます。
- 内部Application Load Balancer または EC2 インスタンスを Global Accelerator とともに使用する場合、エンドポイントでは常にクライアント IP アドレスの保持が有効になります。

> **Note**
>
> グローバルアクセラレータは、Network Load Balancer および Elastic IP アドレスエンドポイントのクライアントの IP アドレスの保持をサポートしていません。

クライアントの IP アドレス保持を追加する場合は、以下について注意してください。

- クライアント IP アドレスを保持するエンドポイントへのトラフィックを追加してルーティングを開始する前に、セキュリティグループなどの必要なすべてのセキュリティ構成が更新され、許可リストにユーザークライアント IP アドレスが含まれることを確認します。
- クライアント IP アドレスの保持は、特定の AWS リージョンでのみサポートされます。詳細については、「クライアント IP アドレスの保持でサポートされる AWS リージョン」を参照してください。

トピック

- クライアントの IP アドレスの保存を有効にする方法
- クライアントの IP アドレス保持の利点

- クライアントの IP アドレスが AWS Global Accelerator で保持される方法
- クライアント IP アドレスの保存に関するベストプラクティス
- クライアント IP アドレスの保持でサポートされる AWS リージョン

クライアントの IP アドレスの保存を有効にする方法

新しいアクセラレータを作成すると、サポートされているエンドポイントに対して、クライアント IP アドレスの保存がデフォルトで有効になります。

以下の点に注意してください。

- 内部アプリケーションロードバランサーと EC2 インスタンスでは、クライアント IP アドレスの保持が常に有効になっています。これらのエンドポイントのオプションを無効にすることはできません。
- AWS コンソールを使用して新しいアクセラレータを作成する場合、Application Load Balancer エンドポイントに対してクライアントの IP アドレスを保持するオプションがデフォルトで有効になります。インターネットに接続するApplication Load Balancer エンドポイントでクライアント IP アドレスを保持したくない場合は、このオプションをいつでも無効にすることができます。
- AWS CLI または API アクションを使用して新しいアクセラレータを作成し、クライアント IP アドレスを保持するオプションを指定しない場合、インターネットに直接接続するApplication Load Balancer エンドポイントでは、デフォルトでクライアント IP アドレスの保持が有効になります。
- グローバルアクセラレータは、Network Load Balancer および Elastic IP アドレスエンドポイントのクライアントの IP アドレスの保持をサポートしていません。

既存のアクセラレータでは、クライアント IP アドレスを保持しないエンドポイントを、クライアント IP アドレスを保持するエンドポイントに移行できます。既存のApplication Load Balancer のエンドポイントは、新しいApplication Load Balancer のエンドポイントに移行でき、既存の Elastic IP アドレスエンドポイントは EC2 インスタンスエンドポイントに移行できます。（Network Load Balancer のエンドポイントは、クライアントの IP アドレスの保存をサポートしていません）。新しいエンドポイントに移行するには、次の手順を実行して、既存のエンドポイントからクライアント IP アドレスを保持する新しいエンドポイントにトラフィックをゆっくりと移動することをお勧めします。

- 既存のApplication Load Balancer エンドポイントの場合、最初に Global Accelerator に、同じバックエンドをターゲットとする重複するApplication Load Balancer エンドポイントを追加し、インターネットに接続するApplication Load Balancer の場合は、クライアント IP アドレスの保持を有

効にします。次に、エンドポイントの重みを調整して、ないロードバランサーに対してクライアントの IP アドレスの保持を有効にしているをクライアント IP アドレスの保持

- 既存の Elastic IP アドレスエンドポイントの場合、クライアント IP アドレスを保持して EC2 インスタンスエンドポイントにトラフィックを移動できます。最初に EC2 インスタンスエンドポイントを Global Accelerator に追加し、エンドポイントの重みを調整して、Elastic IP アドレスエンドポイントから EC2 インスタンスエンドポイントにトラフィックをゆっくりと移動します。

手順については、クライアントの IP アドレス保持を使用するようにエンドポイントを移行する。

クライアントの IP アドレス保持の利点

クライアントの IP アドレスの保持が有効になっていないエンドポイントの場合、エッジネットワークの Global Accelerator サービスによって使用される IP アドレスが、着信パケットの送信元アドレスとして要求しているユーザーの IP アドレスに置き換えられます。元のクライアントの接続情報（クライアントの IP アドレスやクライアントのポートなど）は、トラフィックがアクセラレータの背後にあるシステムに転送されるときに保持されません。これは、多くのアプリケーション、特にパブリックWebサイトなどのすべてのユーザーが利用できるアプリケーションでは正常に動作します。

ただし、他のアプリケーションでは、クライアント IP アドレスを保持するエンドポイントを使用して、元のクライアント IP アドレスにアクセスすることもできます。たとえば、クライアント IP アドレスがある場合、クライアント IP アドレスに基づいて統計情報を収集できます。IP アドレスベースのフィルターを使用することもできます。Application Load Balancerを使用してトラフィックをフィルタリングします。その Application Load Balancer エンドポイントの背後にある Web 層サーバーで実行されるアプリケーションで、ユーザーの IP アドレスに固有のロジックを適用するには、ロードバランサーの`X-Forwarded-For`ヘッダーには、元のクライアント IP アドレス情報が含まれています。Application Load Balancer に関連付けられたセキュリティグループのセキュリティグループルールで、クライアントの IP アドレスの保持を使用することもできます。詳細については、「クライアントの IP アドレスが AWS Global Accelerator で保持される方法」を参照してください。EC2 インスタンスエンドポイントの場合、元のクライアント IP アドレスは保持されます。

クライアント IP アドレスを保持していないエンドポイントの場合、Global Accelerator がエッジからトラフィックを転送するときに使用する送信元 IP アドレスをフィルタリングできます。グローバルアクセラレータフローログを確認することで、着信パケットの送信元 IP アドレス（クライアント IP アドレスの保持が有効な場合はクライアント IP アドレスでもあります）に関する情報を表示できます。詳細については、「Global Accelerator エッジサーバーの場所と IP アドレス範囲」および「AWS Global Accelerator のフロー」を参照してください。

クライアントの IP アドレスが AWS Global Accelerator で保持される方法

AWS Global Accelerator は、Amazon EC2 インスタンスおよびアプリケーションロードバランサーに対して、クライアントのソース IP アドレスを異なる方法で保持します。

- EC2 インスタンスエンドポイントの場合、クライアントの IP アドレスはすべてのトラフィックに対して保持されます。
- クライアントの IP アドレスを保持するApplication Load Balancer エンドポイントの場合、Global Accelerator はApplication Load Balancer と連携して、X-Forwardedヘッダー`X-Forwarded-For`には、元のクライアントの IP アドレスが含まれ、Web 層がそのクライアントにアクセスできるようにします。

HTTP リクエストと HTTP レスポンスは、ヘッダーフィールドを使用して HTTP メッセージに関する情報を送信します。ヘッダーフィールドはコロンで区切られた名前と値のペアであり、キャリッジリターン (CR) とラインフィード (LF) で区切ります。HTTP ヘッダーフィールドの標準セットが RFC 2616 のメッセージヘッダー。アプリケーションで広く使用されている標準以外の HTTP ヘッダーもあります。標準以外の HTTP ヘッダーには、`X-Forwarded`prefix.

Application Load Balancer は着信 TCP 接続を終了し、バックエンドターゲットへの新しい接続を作成するため、クライアントの IP アドレスはターゲットコード (インスタンス、コンテナー、Lambda コードなど) まで保持されません。ターゲットが TCP パケットで認識する送信元 IP アドレスは、Application Load Balancer の IP アドレスです。ただし、Application Load Balancer は、元のクライアント IP アドレスを元のパケットの応答アドレスから削除し、HTTP ヘッダーに挿入してから、新しい TCP 接続を介してバックエンドに要求を送信することによって、元のクライアント IP アドレスを保持します。

-`X-Forwarded-For`リクエストヘッダーは次のようにフォーマットされます。

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

次の例は、`X-Forwarded-For`リクエストヘッダーに、IP アドレスが 203.0.113.7 であるクライアントの

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

クライアント IP アドレスの保存に関するベストプラクティス

AWS Global Accelerator でクライアント IP アドレスの保持を使用する場合は、このセクションのエラスティックネットワークインターフェイスとセキュリティグループに関する情報とベストプラクティスに留意してください。

クライアントの IP アドレスの保持をサポートするために、Global Accelerator は、エンドポイントが存在するサブネットごとに 1 つずつ、AWS アカウントに Elastic ネットワークインターフェイスを作成します。Elastic Network Interface は、仮想ネットワークカードを表す VPC 内の論理ネットワーキングコンポーネントです。Global Accelerator は、これらの Elastic ネットワークインターフェイスを使用して、アクセラレータの背後にあるエンドポイントにトラフィックをルーティング このようにトラフィックをルーティングするためにサポートされているエンドポイントは、アプリケーションロードバランサー (内部およびインターネットに接続) と Amazon EC2 インスタンスです。

> **Note**
>
> Global Accelerator で内部Application Load Balancer または EC2 インスタンスエンドポイントを追加する場合、プライベートサブネットでターゲットを設定することで、インターネットトラフィックが Virtual Private Cloud (VPC; 仮想プライベートクラウド) のエンドポイントに直接送受信されるようにします。詳細については、「AWS Global Accelerator でのセキュアな VPC 接続」を参照してください。

グローバルアクセラレータによるエラスティックネットワークインターフェイスの使用方法

クライアントの IP アドレスの保持を有効にしたApplication Load Balancer がある場合、ロードバランサーが存在するサブネットの数によって、Global Accelerator がアカウントに作成する Elastic ネットワークインターフェイスの数が決まります。Global Accelerator は、アカウント内のアクセラレータの前にあるApplication Load Balancer のエラスティックネットワークインターフェイスを少なくとも 1 つ持つサブネットごとに 1 つのエラスティックネットワークインターフェイスを作成します。

以下の例では、このしくみを示しています。

- 例 1: Application Load Balancer のサブネット A とサブネット B にエラスティックネットワークインターフェイスがあり、ロードバランサーをアクセラレータエンドポイントとして追加すると、Global Accelerator は各サブネットに 1 つずつ、2 つのエラスティックネットワークインターフェイスが作成されます。

- 例 2: たとえば、サブネット A と SubnetB にエラスティックネットワークインターフェイスを持つ ALB1 を Accelerator1 に追加し、サブネット A にエラスティックネットワークインターフェイスを持つ ALB2 を Accelerator2 に追加すると、グローバルアクセラレータは、サブネット A に 1 つ、サブネット B に 1 つずつ、エラスティックネットワークインターフェイスを 2 つだけ作成します。
- 例 3: SubnetA および SubnetB にエラスティックネットワークインターフェイスを持つ ALB1 を Accelerator1 に追加し、SubnetA および SubnetC にエラスティックネットワークインターフェイスを持つ ALB2 を Accelerator2 に追加すると、グローバルアクセラレータは 3 つのエラスティックネットワークインターフェイス (SubnetA に 1 つ、SubnetB に 1 つ、SubnetC に 1 つ) を作成します。SubnetA のelastic network interface は、アクセラレータ 1 とアクセラレータ 2 の両方にトラフィックを配信します。

例 3 に示すように、エラスティックネットワークインターフェイスは、同じサブネット内のエンドポイントが複数のアクセラレータの背後に配置されている場合、アクセラレータ間で再利用されます。

Global Accelerator が作成する論理エラスティックネットワークインターフェイスは、単一のホスト、スループットのボトルネック、または単一障害点を表すものではありません。アベイラビリティーゾーンまたはサブネットで単一のelastic network interface として表示される他の AWS サービス (ネットワークアドレス変換 (NAT) ゲートウェイやネットワーク負荷バランサーなどのサービス) と同様に、Global Accelerator は水平方向に拡張され、可用性の高いサービスとして実装されます。

アクセラレータのエンドポイントで使用されるサブネットの数を評価して、Global Accelerator が作成する Elastic ネットワークインターフェイスの数を決定します。アクセラレータを作成する前に、必要な Elastic ネットワークインターフェイスに十分な IP アドレス空間容量 (関連するサブネットごとに少なくとも 1 つの空き IP アドレス) があることを確認してください。十分な空きの IP アドレス領域がない場合は、Application Load Balancer および関連する Global Accelerator Elastic ネットワークインターフェイスに十分な空きの IP アドレス領域があるサブネットを作成または使用する必要があります。

Global Accelerator が、アカウントのアクセラレータのエンドポイントでelastic network interface が使用されていないと判断すると、Global Accelerator はインターフェイスを削除します。

グローバルアクセラレータによって作成されたセキュリティグループ

グローバルアクセラレータとセキュリティグループを使用する場合は、次の情報とベストプラクティスを確認してください。

- Global Accelerator は、Elastic Network インターフェイスに関連付けられているセキュリティグループを作成します。システムによって禁止されるわけではありませんが、これらのグループのセキュリティグループ設定を編集しないでください。
- グローバルアクセラレータは、作成したセキュリティグループを削除しません。ただし、Global Accelerator では、アカウントのアクセラレータのエンドポイントでelastic network interface が使用されていない場合、エラスティックネットワークインターフェイスは削除されます。
- Global Accelerator によって作成されたセキュリティグループは、保守する他のセキュリティグループのソースグループとして使用できますが、Global Accelerator は VPC で指定したターゲットにのみトラフィックを転送します。
- Global Accelerator で作成されたセキュリティグループのルールを変更すると、エンドポイントが異常になることがあります。その場合は、AWS サポート詳細については、
- グローバルアクセラレータは、VPC ごとに特定のセキュリティグループを作成します。特定の VPC 内のエンドポイント用に作成された Elastic ネットワークインターフェイスは、elastic network interface が関連付けられているサブネットに関係なく、すべて同じセキュリティグループを使用します。

クライアント IP アドレスの保持でサポートされる AWS リージョン

以下の AWS リージョンで AWS Global Accelerator のクライアント IP アドレスの保持を有効にできます。

リージョン名	リージョン
米国東部 (オハイオ)	`us-east-2`
米国東部 (バージニア北部)	`us-east-1`
米国西部 (北カリフォルニア)	`us-west-1 (except AZ usw1-az2)`
米国西部 (オレゴン)	`us-west-2`
アフリカ (ケープタウン)	`af-south-1`
アジアパシフィック (香港)	`ap-east-1`

リージョン名	リージョン
アジアパシフィック (ムンバイ)	ap-south-1
アジアパシフィック (大阪)	ap-northeast-3
アジアパシフィック (シンガポール)	ap-southeast-1
アジアパシフィック (シドニー)	ap-southeast-2
アジアパシフィック (東京)	ap-northeast-1 (except AZ apne1-az3)
アジアパシフィック (ソウル)	ap-northeast-2
カナダ (中部)	ca-central-1 (except AZ cac1-az3)
欧州 (フランクフルト)	eu-central-1
欧州 (アイルランド)	eu-west-1
欧州 (ロンドン)	eu-west-2
ヨーロッパ (ミラノ)	eu-south-1
欧州 (パリ)	eu-west-3
欧州 (ストックホルム)	eu-north-1
中東 (バーレーン)	me-south-1
南米 (サンパウロ)	sa-east-1

AWS Global Accelerator でのロギングとモニタリング

フローログとAWS CloudTrail を使用して、AWS Global Accelerator でアクセラレータをモニタリングするには、トラフィックパターンの分析やリスナーとエンドポイントのトラブルシューティングを行います。

トピック

- AWS Global Accelerator のフロー
- AWS Global Accelerator での Amazon CloudWatch の使用
- AWS CloudTrail を使用した AWS Global Accelerator API コールのログ記録

AWS Global Accelerator のフロー

フローログにより、AWS Global Accelerator のアクセラレーターで、ネットワークインターフェイスとの間で行き来する IP アドレスに関する情報を取得できるようになります。フローログデータは Amazon S3 に発行され、フローログを作成した後にデータを取得して表示できます。

フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがエンドポイントに到達していない場合のトラブルシューティングを行うことができます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。フローログをセキュリティツールとして使用し、エンドポイントに到達しているトラフィックをモニタリングすることができます。

フローログレコードは、フローログのネットワークの流れを表します。各レコードでは、特定のキャプチャウィンドウで特定の 5 タプルのネットワークフローがキャプチャされます。5 タプルとは、IP フローの送信元、送信先、およびプロトコルを指定する 5 セットの異なる値のことです。キャプチャウィンドウは、フローログレコードを発行する前にフローログサービスがデータを集計する期間です。キャプチャウィンドウは約 10 秒ですが、最長 1 分かかる場合があります。

CloudWatch Logs の料金は、ログが Amazon S3 に直接発行された場合でも、フローログを使用するときに適用されます。詳細については、「」を参照してください。S3 へのログの配信atAmazon CloudWatch の料金。

トピック

- フローログを Amazon S3 に発行する
- ログファイル配信のタイミング
- フローログレコードの構文

フローログを Amazon S3 に発行する

AWS Global Accelerator のフローログは、指定する既存の S3 バケットに Amazon S3 に発行されます。フローログレコードは、バケットに保存された一連のログファイルオブジェクトに発行されます。

フローログに使用する Amazon S3 バケットを作成するには、バケットの作成()Amazon Simple Storage Service 入門ガイド。

フローログファイル

フローログは、フローログレコードを収集し、ログファイルに統合して、5 分間隔でログファイルを Amazon S3 バケットに発行します。各ログファイルには、前の 5 分間に記録された IP アドレストラフィックのフローログレコードが含まれています。

ログファイルの最大ファイルサイズは 75 MB です。ログファイルが 5 分以内にファイルサイズの上限に達した場合、フローログはフローログレコードの追加を停止し、Amazon S3 バケットに発行してから、新しいログファイルを作成します。

ログファイルでは、フローログの ID、リージョン、および作成日によって決定されるフォルダ構造を使用して、指定された Amazon S3 バケットに保存されます。バケットフォルダ構造では次の形式が使用されます。

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

同様に、ログファイル名は、フローログの ID、リージョン、および作成日時によって決定されます。ファイル名は、次の形式です。

```
aws_account_id_globalaccelerator_accelerator_id_flow_log_id_timestamp_hash.log.gz
```

ログファイルのフォルダとファイル名の構造については、次の点に注意してください。

- タイムスタンプは、YYYYMMDDTHHmmZ 形式を使用します。
- S3 バケットプレフィックスにスラッシュ (/) を指定すると、ログファイルのバケットフォルダ構造には、次のような二重スラッシュ (//) が含まれます。

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

次の例は、AWS アカウントで作成されたフローログのフォルダ構造とログファイルの名前を示しています。123456789012のIDを持つアクセラレータの場合1234abcd-abcd-1234-abcd-1234abcdefgh、2018年11月23日 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
```

1 つのフローログファイルには、複数の 5 タプルレコードを含むインターリーブエントリが含まれています。client_ip,client_port,accelerator_ip,accelerator_port,protocol。アクセラレータのすべてのフローログファイルを表示するには、accelerator_idおよびaccount_id。

フローログを Amazon S3 に発行するための IAM ロール

IAM ユーザーなどの IAM プリンシパル (例:IAM ユーザー) には、フローログを Amazon S3 バケットに発行するための十分なアクセス許可が付与されている必要があります。IAM ポリシーには以下のアクセス許可が含まれています。

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

フローログのための Amazon S3 バケットのアクセス許可

デフォルトでは、Amazon S3 バケットとそのバケットに含まれるオブジェクトはプライベートです。バケット所有者のみが、そのバケットとそれに含まれているオブジェクトにアクセスできます。ただし、バケット所有者は、アクセスポリシーを記述することで他のリソースおよびユーザーにアクセス権限を付与することができます。

フローログを作成するユーザーがバケットを所有している場合、サービスはバケットにログを発行するアクセス権限をフローログに付与するため、次のポリシーが自動的にバケットにアタッチされます。

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

フローログを作成しているユーザーがバケットを所有していないか、バケットに対する GetBucketPolicy および PutBucketPolicy アクセス権限がない場合、フローログの作成は失敗します。この場合、バケット所有者は、バケットに手動で前のポリシーを追加して、フローログ作成者の AWS アカウント ID を指定する必要があります。詳細については、「」を参照してください。S3 バケットポリシーを追加する方法()Amazon Simple Storage Service 入門ガイド。バケットが複数のアカウントからフローログを受け取る場合は、各アカウントの AWSLogDeliveryWrite ポリシーステートメントに Resource エレメントエントリを追加します。

たとえば、次のバケットポリシーでは、AWS アカウント 123123123 および 456456456456456 に、フローログをflow-logsという名前のバケットでlog-bucket:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": [
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/123123123123/*",
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/456456456456/*"
             ],
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-
control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::log-bucket"
        }
    ]
}
```

> **Note**
>
> 付与することをお勧めしますAWSLogDeliveryAclCheckおよびAWSLogDeliveryWriteアクセス許可を、個々の AWS アカウント ARN ではなく、ログ配信サービスプリンシパル。

SSE-KMS バケットに使用する必須の CMK キーポリシー

AWS KMS で管理されたキー (SSE-KMS) とカスタマー管理のカスタマーマスターキー (CMK) を使用して Amazon S3 バケットでサーバー側の暗号化を有効にしている場合、CMK のキーポリシーに以下を追加して、フローログがバケットにログファイルを書き込めるようにする必要があります。

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

Amazon S3 ログファイルのアクセス許可

Amazon S3 は、必須のバケットポリシーに加えて、アクセスコントロールリスト (ACL) を使用して、フローログによって作成されたログファイルへのアクセスを管理します。デフォルトでは、バケット所有者が各ログファイルで FULL_CONTROL 権限を持ちます。ログ配信の所有者 (バケット所有者とは異なる場合) は、アクセス権限を持ちません。ログ配信アカウントには、READ および WRITE アクセス権限があります。詳細については、「」を参照してください。アクセスコントロールリスト (ACL) の概要()Amazon Simple Storage Service 入門ガイド。

フローログを Amazon S3 に発行する

AWS Global Accelerator でフローログを有効にするには、この手順のステップに従います。

AWS Global Accelerator でフローログを有効にするには

1. フローログ用の Amazon S3 バケットを AWS アカウントに作成します。

2. フローログを有効にしている AWS ユーザーに必要な IAM ポリシーを追加します。詳細については、「フローログを Amazon S3 に発行するための IAM ロール」を参照してください。
3. ログファイルに使用する Amazon S3 バケット名とプレフィックスを使用して、次の AWS CLI コマンドを実行します。

```
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
```

Amazon S3 でのフローログレコードの処理

ログファイルは圧縮されます。Amazon S3 コンソールを使用してログファイルを開くと、ファイルは解凍され、フローログレコードが表示されます。ファイルをダウンロードする場合、フローログレコードを表示するには解凍する必要があります。

ログファイル配信のタイミング

AWS Global Accelerator は、設定したアクセラレーターのログファイルを 1 時間に最大で数回配信します。一般に、ログファイルには、一定期間内にアクセラレータが受信したリクエストに関する情報が含まれています。Global Accelerator は通常、その期間のログファイルを、ログに記録されたイベントから 1 時間以内に Amazon S3 バケットに配信します。一定期間におけるログファイルエントリの一部またはすべてが、最長 24 時間遅れることがあります。ログエントリが遅れた場合、Global Accelerator はこれらをログファイルに保存します。そのファイル名には、ファイルが配信された日時ではなく、リクエストが発生した期間の日時が含められます。

Global Accelerator は、ログファイルを作成する場合、ログファイルに対応する期間中にリクエストを受信したすべてのエッジロケーションから、アクセラレーターに関する情報を集約します。

Global Accelerator は、ロギングが有効化し 4 時間後ほどから確実にログファイル配信を開始します。この時間以前にも少しのログファイルを取得できる場合もあります。

> **Note**
>
> 期間中にアクセラレーターに接続したユーザーがいない場合、その期間のログファイルは配信されません。

フローログレコードの構文

フローログレコードはスペース区切りの文字列で、以下の形式です。

```
<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>
```

バージョン 1.0 形式には、VPC 識別子、vpc_id。バージョン 2.0 形式。これにはvpc_idは、Global Accelerator がクライアントの IP アドレスを保持するエンドポイントにトラフィックを送信するときに生成されます。

次の表は、フローログレコードのフィールドについて説明しています。

フィールド	説明
version	フローログのバージョン。
aws_account_id	フローログの AWS アカウント ID。
accelerator_id	トラフィックが記録されるアクセラレーターの ID。
client_ip	送信元 IPv4 アドレス。
client_port	送信元ポート。
accelerator_ip	アクセラレーターの IP アドレス。

フィールド	説明
accelerator_port	アクセラレータのポート
endpoint_ip	トラフィックの送信先 IP アドレス。
endpoint_port	トラフィックの送信先ポート。
protocol	トラフィックの IANA プロトコル番号。詳細については、「割り当てられたインターネットプロトコル番号」を参照してください。
ip_address_type	IPv4。
packets	キャプチャウィンドウ中に転送されたパケットの数。
bytes	キャプチャウィンドウ中に転送されたバイト数。
start_time	キャプチャウィンドウの開始時刻 (Unix 時間)。
end_time	キャプチャウィンドウの終了時刻 (Unix 時間)。
action	トラフィックに関連付けられたアクション: • ACCEPT: 記録されたトラフィックは、セキュリティグループまたはネットワーク ACL で許可されています。値は現在、常に ACCEPT です。
log-status	フローログのロギングステータス。 • OK: データは選択された送信先に正常に記録されます。 • NODATA: キャプチャウィンドウ中にネットワークインターフェイスとの間で行き来するネットワークトラフィックはありませんでした。 • SKIPDATA: 一部のフローログレコードはキャプチャウィンドウ中にスキップされました。これは、内部的なキャパシティー制限、または内部エラーが原因である可能性があります。

フィールド	説明
globalaccelerator_source_ip	グローバルアクセラレータネットワークインターフェイスによって使用される IP アドレス。
globalaccelerator_source_port	グローバルアクセラレータネットワークインターフェイスで使用されるポート。
endpoint_region	エンドポイントがある AWS リージョン。
globalaccelerator_region	リクエストを処理したエッジロケーション (ポイントオブプレゼンス)。各エッジロケーションは、3 文字コードと、任意に割り当てられた数字を持っています (例:DFW3)。通常、この 3 文字コードは、エッジロケーションの近くにある空港の、国際航空運送協会の空港コードに対応します。 (これらの略語は今後変更される可能性があります)。
direction	トラフィックの方向。グローバルアクセラレータネットワークに入ってくるトラフィックを示します (INGRESS)、またはクライアントに戻る (EGRESS).
vpc_id	VPC 識別子。グローバルアクセラレータがクライアントの IP アドレスを保持してエンドポイントにトラフィックを送信するときに、バージョン 2.0 のフローログに含まれます。

フィールドが特定のレコードに該当しない場合、レコードにはそのエントリに対して「-」記号が表示されます。

AWS Global Accelerator での Amazon CloudWatch の使用

AWS Global Accelerator は、アクセラレータ用のデータポイントを Amazon CloudWatch に発行します。CloudWatch を使用すると、それらのデータポイントについての統計を、順序付けられた時系列データのセット (のメトリクス。メトリクスは監視対象の変数、データポイントは時間の経過と共に変わる変数の値と考えることができます。たとえば、指定した期間中のアクセラレータを経由するトラフィックを監視できます。各データポイントには、タイムスタンプと、オプションの測定単位が関連付けられています。

メトリクスを使用して、システムが正常に実行されていることを確認できます。たとえば、メトリクスが許容範囲外になる場合、CloudWatch アラームを作成して、指定されたメトリクスを監視し、アクション (E メールアドレスに通知を送信するなど) を開始することができます。

Global Accelerator は、リクエストがアクセラレータを経由する場合のみ、メトリクスをCloudWatch に報告します リクエストがアクセラレータを経由する場合、Global Accelerator は 60 秒間隔でメトリクスを測定し、送信します。アクセラレータを経由するリクエストがないか、メトリクスのデータがない場合、メトリクスは報告されません。

詳細については、Amazon CloudWatch ユーザーガイドを参照してください。

コンテンツ

グローバルアクセラレータメトリクス

AWS/GlobalAccelerator 名前空間には、次のメトリクスが含まれます。

メトリクス	説明
NewFlowCount	期間内にクライアントからエンドポイントに確立された新しい TCP および UDP フロー (または接続) の合計数。 レポート条件: ゼロ以外の値がある。 統計: 唯一の有用な統計はSum。 Dimensions • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge

メトリクス	説明
	• Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress
ProcessedBytesIn	TCP/IP ヘッダーを含む、アクセラレータによって処理された受信バイトの合計数。このカウントには、エンドポイントへのすべてのトラフィックが含まれます。 レポート条件: ゼロ以外の値がある。 統計: 唯一の有用な統計はSum。 Dimensions • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress

メトリクス	説明
ProcessedBytesOut	TCP/IP ヘッダーを含む、アクセラレータによって処理された送信バイトの合計数。この数には、エンドポイントからのトラフィックからヘルスチェックトラフィックを引いたものが含まれます。 レポート条件: ゼロ以外の値がある。 統計: 唯一の有用な統計はSum。 Dimensions • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress

アクセラレータのメトリクスディメンション

アクセラレータのメトリクスをフィルタするには、次のディメンションを使用してください。

ディメンション	説明
Accelerator	アクセラレータによってメトリクスデータをフィルタリングします。アクセラレータ ID (アクセラレータ ARN の最後の部分) でアクセラレータを指定します。たとえば、ARN がarn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh で、以下を指定します。**1234abcd-abcd-1234-abcd-1234abcdefgh** 。
Listener	リスナーによってメトリクスデータをフィルタリングします。リスナー ID (リスナー ARN の最後の部分) でリスナーを指定します。たとえば、ARN がarn:aws:globalaccelerator::

ディメンション	説明
	012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123wxyz で、以下を指定します。**0123wxyz**。
EndpointGroup	エンドポイントグループでメトリクスデータをフィルタリングします。AWS リージョンでエンドポイントグループを指定します (例:**us-east-1** (すべて小文字) です。
SourceRegion	ソースリージョンでメトリックスデータをフィルタリングします。ソースリージョンとは、アプリケーションエンドポイントが実行されている AWS リージョンの地理的エリアです。ソースリージョンは以下のいずれかです。 • NA — 米国およびカナダ • EU — ヨーロッパ • AP — アジア太平洋地域* • KR — 韓国 • IN — インド • AU — オーストラリア • ME — 中東 • SA — 南米 ※韓国、インドを除く

ディメンション	説明
DestinationEdge	メトリックスデータを宛先エッジでフィルタリングします。宛先エッジとは、クライアントのトラフィックを処理する AWS エッジロケーションの地理的エリアです。送信先エッジは以下のいずれかです。 • NA — 米国およびカナダ • EU — ヨーロッパ • AP — アジア太平洋地域* • KR — 韓国 • IN — インド • AU — オーストラリア • ME — 中東 • SA — 南米 • ZA — 南アフリカ ※韓国、インドを除く
TransportProtocol	トランスポートプロトコルによってメトリクスデータをフィルタリングします。UDP または TCP。
AcceleratorIPAddress	アクセラレータの IP アドレス (アクセラレータに割り当てられた静的 IP アドレスの 1 つ) によってメトリクスデータをフィルタリングします。

グローバルアクセラレータメトリクスの統計

CloudWatch は、Global Accelerator によって発行されたメトリクスのデータポイントに基づいて統計を提供します。統計とは、メトリクスデータを指定した期間で集約したものです。統計を要求した場合、返されるデータストリームはメトリクス名とディメンションによって識別されます。ディメンションは、メトリクスを一意に識別する名前/値のペアです。たとえば、ヨーロッパの AWS エッジロケーション (宛先エッジは「EU」) からバイトが供給されるアクセラレータに対して、処理されたバイトをリクエストできます。

以下は、有用と思われるメトリック/ディメンションの組み合わせの例です。

- 2 つのアクセラレータ IP アドレスのそれぞれによって処理されるトラフィックの量（ProcessedBytesOut など）を表示し、DNS 構成が正しいことを確認します。
- ユーザトラフィックの地理的分布を表示し、ローカル（北米から北米）またはグローバル（オーストラリアまたはインドから北米）の量を監視します。これを判断するには、DestinationEdge ディメンションと SourceRegion ディメンションが特定の値に設定されている場合に ProcessedBytesIn メトリックまたは ProcessedBytesOut メトリックスを表示します。

アクセラレータの CloudWatch メトリクスを表示します。

CloudWatch コンソールまたは AWS CLI を使用して、アクセラレータの CloudWatch メトリクスを表示できます。コンソールには、メトリクスがモニタリング用のグラフとして表示されます。モニタリング用のグラフには、アクセラレータがアクティブでリクエストを受信している場合のみ、データポイントが表示されます。

コンソールまたは AWS CLI を使用する場合、米国西部（オレゴン）リージョンで、Global Accelerator の CloudWatch メトリクスを表示する必要があります。AWS CLI を使用する場合は、以下のパラメータを指定して、コマンドに米国西部（オレゴン）リージョンを指定します。`--region us-west-2`。

CloudWatch コンソールを使用してメトリクスを表示するには

1. CloudWatch コンソールをhttps://us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2。
2. ナビゲーションペインで メトリクスを選択します。
3. 選択GlobalAccelerator名前空間.
4. (オプション) すべてのディメンションでメトリクスを表示するには、検索フィールドに名称を入力します。

AWS CLI を使用してメトリクスを表示するには

使用可能なメトリクスを表示するには、次の list-metrics コマンドを使用します。

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

AWS CLI を使用してメトリクスの統計を取得するには

以下のを使用します。メトリクス統計を取得コマンドを使用すると、指定したメトリクスとディメンションの統計を取得できます。CloudWatch は、ディメンションの一意の組み合わせをそれぞれ別のメトリクスとして扱うことに注意してください。特に発行されていないディメンションの組み合わせを使用した統計を取得することはできません。メトリクス作成時に使用した同じディメンションを指定する必要があります。

次の例では、北米 (NA) 宛先エッジから処理されるアクセラレータの 1 分あたりの合計処理バイト数をリストします。

```
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
```

コマンドからの出力例を次に示します。

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


AWS CloudTrail を使用した AWS Global Accelerator API コールのログ記録

AWS Global Accelerator は、AWS CloudTrail と統合されます。AWS CloudTrail は、Global Accelerator のユーザー、ロール、または AWS のサービスで実行されたアクションのレコードを提供するサービスです。CloudTrail は、グローバルアクセラレーターコンソールからのコールや、グローバルアクセラレーター API へのコード呼び出しを含む、グローバルアクセラレーターのすべての API コールをイベントとしてキャプチャします。証跡を作成する場合は、Global Accelerator のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示できます。

CloudTrail に関する詳細は、AWS CloudTrail ユーザーガイドを参照してください。

CloudTrail のグローバルアクセラレーター情報

CloudTrail は、アカウント作成時に AWS アカウントで有効になります。Global Accelerator で CloudTrail が発生すると、そのアクティビティはイベント履歴。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

Global Accelerator のイベントなど、AWS アカウントのイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべてのリージョンに適用されます。証跡では、AWS パーティションのすべてのリージョンからのイベントがログに記録され、指定した Amazon S3 バケットにログファイルが配信されます。さらに、その他の AWS サービスを設定して、CloudTrail ログで収集されたデータをより詳細に分析し、それに基づく対応を行うことができます。詳細については、以下のトピックを参照してください。

- 証跡を作成するための概要
- CloudTrail のサポート対象サービスと統合
- Amazon SNS の CloudTrail 通知の設定
- 「複数のリージョンから CloudTrail ログファイルを受け取る」および「複数のアカウントから CloudTrail ログファイルを受け取る」

すべてのGlobal Accelerator アクションは CloudTrail によって記録され、AWS Global Accelerator API リファレンス。たとえば、`CreateAccelerator`,`ListAccelerators`および`UpdateAccelerator`オペレーションは、CloudTrail ログファイルにエントリを生成します。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。この ID 情報は以下のことを確認するのに役立ちます。

- リクエストが、ルートと IAM ユーザー認証情報のどちらを使用して送信されたか
- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか
- リクエストが AWS の別のサービスによって生成されたかどうか

詳細については、「CloudTrail userIdentity エレメント」を参照してください。

グローバルアクセラレーターログファイルエントリの概要

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。JSON 形式の各 CloudTrail ログファイルには、1 つ以上のログエントリを含めることができます。各ログエントリは任意の送信元からの単一のリクエストを表し、パラメータやアクションの日時など、リクエストされたアクションに関する情報を含みます。ログエントリは、特定の順序で生成されるわけではなく、API 呼び出しのスタックトレース順に並んではいません。

以下の例は、これらのGlobal Accelerator アクションを含む CloudTrail ログエントリを示しています。

- アカウントのアクセラレータの一覧表示:eventName、ListAccelerators。
- リスナーの作成eventName、CreateListener。
- リスナーの更新eventName、UpdateListener。
- リスナーの説明eventName、DescribeListener。
- アカウントのリスナーを一覧表示します。eventName、ListListeners。
- リスナーの削除eventName、DeleteListener。


```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
```

```
        }
      }
    },
    "eventTime": "2018-11-17T21:03:14Z",
    "eventSource": "globalaccelerator.amazonaws.com",
    "eventName": "ListAccelerators",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.50",
    "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "083cae81-28ab-4a66-862f-096e1example",
    "eventID": "fe8b1c13-8757-4c73-b842-fe2a3example",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "A1B2C3D4E5F6G7EXAMPLE",
      "arn": "arn:aws:iam::111122223333:user/smithj",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "attributes": {
          "mfaAuthenticated": "false",
          "creationDate": "2018-11-17T21:02:36Z"
        },
        "sessionIssuer": {
          "type": "Role",
          "principalId": "A1B2C3D4E5F6G7EXAMPLE",
          "arn": "arn:aws:iam::111122223333:user/smithj",
          "accountId": "111122223333",
          "userName": "smithj"
        }
      }
    },
    "eventTime": "2018-11-17T21:04:49Z",
    "eventSource": "globalaccelerator.amazonaws.com",
    "eventName": "CreateListener",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.50",
    "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
```

```
      "requestParameters": {
        "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample",
        "portRanges": [
          {
            "fromPort": 80,
            "toPort": 80
          }
        ],
        "protocol": "TCP"
      },
      "responseElements": {
        "listener": {
          "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
          "portRanges": [
            {
              "fromPort": 80,
              "toPort": 80
            }
          ],
          "protocol": "TCP",
          "clientAffinity": "NONE"
        }
      },
      "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
      "eventID": "9cab44ef-0777-41e6-838f-f249example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
```

```
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:03:52Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "CreateAccelerator",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "name": "cloudTrailTest"
      },
      "responseElements": {
        "accelerator": {
          "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample",
          "name": "cloudTrailTest",
          "ipAddressType": "IPV4",
          "enabled": true,
          "ipSets": [
            {
              "ipFamily": "IPv4",
              "ipAddresses": [
                "192.0.2.213",
                "192.0.2.200"
              ]
            }
          ],
          "status": "IN_PROGRESS",
          "createdTime": "Nov 17, 2018 9:03:52 PM",
          "lastModifiedTime": "Nov 17, 2018 9:03:52 PM"
        }
      },
      "requestID": "d2d7f300-2f0b-4bda-aa2d-e67d6e4example",
      "eventID": "11f9a762-8c00-4fcc-80f9-848a29example",
      "eventType": "AwsApiCall",
```

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

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

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

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

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

AWS Global Accelerator

クラウドセキュリティは AWS の最優先事項です。AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティは、AWS とお客様の間の共有責任です。共有責任モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS は、AWS クラウドで AWS のサービスを実行するインフラストラクチャを保護する責任を担います。また、AWS では安全に使用できるサービスも用意されています。AWS のセキュリティの有効性は、AWS コンプライアンスプログラムの一環として、第三者の監査機関により定期的にテストおよび検証されています。グローバルアクセラレーターに適用されるコンプライアンスプログラムの詳細については、」コンプライアンスプログラムによる AWS 対象範囲内のサービス。
- クラウド内のセキュリティ – お客様の責任はお客様が使用する AWS のサービスによって決まります。また、お客様は、お客様のデータの機密性、組織の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、グローバル· アクセラレーターを使用する際に、責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティ目的を達成するためにグローバルアクセラレータを設定する方法を示します。

トピック

AWS Global Accelerator の ID とアクセス管理

AWS Identity and Access Management (IAM) は、AWS Global Accelerator リソースを含む AWS リソースへのアクセスを管理者が安全に制御するために役立つ AWS のサービスです。管理者は IAM

を使用してユーザーを制御する認証済み(サインイン) と承認済み(権限を持つ) がグローバルアクセラレータリソースを使用できるようにします。IAM は追加料金なしで、AWS アカウントに含まれている機能です。

> **Important**
>
> IAM に慣れていない場合は、このページの入門情報を確認し、次に「」を参照してください。IAM の使用開始。必要に応じて、認証とアクセスコントロールの詳細については、認証とは,アクセス制御とは, およびポリシーとは。

トピック

- 概念と用語
- コンソールアクセス、認証管理、アクセス制御に必要な権限
- グローバルアクセラレータと IAM との連携の理解
- 認証とアクセスコントロールのトラブルシューティング

概念と用語

認証— AWS にサインインするには、ルートユーザー認証情報 (非推奨)、IAM ユーザー認証情報 (推奨)、または IAM ロールによる一時的認証情報のいずれかを使用する必要があります。これらのエンティティの詳細については、「認証とは」を参照してください。

アクセスコントロール— AWS 管理者は、ポリシーを使用してグローバルアクセラレーターなどの AWS リソースへのアクセスをコントロールします。詳細については、「アクセス制御とは」と「ポリシーとは」を参照してください。

> **Important**
>
> アカウントのすべてのリソースは、その作成者を問わず、アカウントが所有します。リソースを作成するには、アクセス許可が必要です。ただし、リソースを作成しても、そのリソースへのフルアクセスが自動的に許可されるわけではありません。実行するアクションごとに、管理者から明示的にアクセス許可を得る必要があります。管理者は、アクセス許可を随時取り消すこともできます。

IAM の基本的な仕組みを理解するために、以下の用語に精通してください。

リソース

グローバルアクセラレーターや IAM などの AWS のサービスには、通常リソースと呼ばれるオブジェクトが含まれています。ほとんどの場合、サービスでこれらのリソースを作成、管理、および削除できます。IAM リソースには、ユーザー、グループ、ロール、およびポリシーが含まれます。

ユーザー

IAM ユーザーは、認証情報を使用して AWS を操作する人またはアプリケーションです。ユーザーは、AWS マネジメントコンソールにサインインするための名前とパスワード、AWS CLI または AWS API で使用できる最大 2 つのアクセスキーで構成されます。

グループ

IAM グループは、IAM ユーザーのコレクションです。管理者は、グループを使用してメンバーユーザーのアクセス許可を指定できます。これにより、管理者は複数のユーザーのアクセス許可を簡単に管理できます。

ロール

IAM ロールには長期の認証情報 (パスワードやアクセスキー) を関連付けることはできません。どのユーザーでも、アクセス許可があれば、ロールを引き受けることができます。IAM ユーザーは、ロールを引き受けることで、一時的に特定のタスクに対して異なるアクセス許可を取得することができます。フェデレーティッドユーザーは、ロールにマッピングされている外部の ID プロバイダーを使用してロールを引き受けることができます。一部の AWS サービスは、サービスロールお客様の代わりに AWS リソースにアクセスします。

ポリシー

ポリシーは JSON ドキュメントであり、アタッチ先のオブジェクトのアクセス許可を定義します。AWS サポートアイデンティティベースのポリシーアイデンティティ (ユーザー、グループ、またはロール) にアタッチする。一部の AWS サービスでは、リソースベースのポリシーリソースに追加して、プリンシパル (人またはアプリケーション) がそのリソースに対して何ができるかをコントロールできます。グローバルアクセラレータでは、リソースベースのポリシーはサポートされていません。

ID

アイデンティティは、アクセス許可を定義できる IAM リソースです。ユーザー、グループ、およびロールなどがあります。

エンティティ

エンティティは、認証に使用する IAM リソースです。ユーザーやロールなどがあります。

プリンシパル

AWS では、プリンシパルとは、エンティティを使用して AWS にサインインしてリクエストを行う人またはアプリケーションです。プリンシパルは、AWS マネジメントコンソール、AWS CLI、または AWS API を使用してオペレーション (アクセラレーターの削除など) を実行できます。これに伴って、そのオペレーションに対するリクエストが作成されます。リクエストでは、アクション、リソース、プリンシパル、プリンシパルアカウント、その他リクエストに関する情報を指定します。これらのすべての情報により AWS は、contextリクエストをお受けください。AWS は、リクエストのコンテキストに該当するすべてのポリシーをチェックします。AWS は、リクエストの各部分がポリシーで許可されている場合のみ、リクエストを許可します。

認証とアクセスコントロールプロセスの図を表示するには、」IAM の機能について()IAM ユーザーガイド。AWS でリクエストの許可を決定する方法の詳細については、「」を参照してください。ポリシーの評価論理()IAM ユーザーガイド。

コンソールアクセス、認証管理、アクセス制御に必要な権限

グローバルアクセラレーターを使用したり、自分や他のユーザーの認証とアクセスコントロールを管理したりするには、適切なアクセス許可を持っている必要があります。

グローバルアクセラレータアクセラレータの作成に必要なアクセス許可

AWS Global Accelerator アクセラレータを作成するには、グローバルアクセラレータに関連付けられたサービスリンクロールを作成する権限が必要です。

Global Accelerator でアクセラレータを作成するための適切なアクセス許可をユーザーに付与するには、次のようなポリシーをユーザーにアタッチします。

> **Note**
>
> より制限された ID ベースのアクセス許可ポリシーを作成している場合、そのポリシーを使用するユーザーはアクセラレーターを作成できません。

```
{
      "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*"
    }
```

グローバルアクセラレータコンソールの使用に必要なアクセス許可

AWS Global Accelerator コンソールにアクセスするには、AWS アカウントのグローバルアクセラレータリソースに関する詳細を表示して確認するための最低限のアクセス許可が必要です。最小限必要なアクセス許可よりも制限されたアイデンティティベースのアクセス許可ポリシーを作成すると、そのポリシーをアタッチしたエンティティに対してはコンソールが意図したとおりに機能しません。

これらのエンティティが Global Accelerator コンソールまたは API アクションを使用できるように、次の AWS 管理ポリシーもアタッチします (「」を参照)。[JSON] タブでのポリシーの作成:

```
        GlobalAcceleratorReadOnlyAccess
        GlobalAcceleratorFullAccess
```

最初のポリシーGlobalAcceleratorReadOnlyAccess、ユーザーがコンソールで情報を表示するか、AWS CLI またはList*またはDescribe*オペレーション.

2 番目のポリシーGlobalAcceleratorFullAccess、アクセラレータを作成または更新する必要があるユーザーに適用されます。フルアクセスポリシーには、FULLグローバルアクセラレータのアクセス許可説明Amazon EC2 および Elastic Load Balancing の権限を付与します。

> **Note**
>
> Amazon EC2 および Elastic Load Balancing に必要なアクセス権限を含まないアイデンティティベースのアクセス権限ポリシーを作成した場合、そのポリシーを持つユーザーは

Amazon EC2 および Elastic Load Balancing リソースをアクセラレーターに追加できません。

以下は、フルアクセスポリシーです。

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

認証管理に必要な権限

自分の認証情報 (パスワード、アクセスキー、多要素認証 (MFA) デバイスなど) を管理するには、管理者から必要なアクセス許可を取得する必要があります。これらのアクセス許可が含まれているポリシーを表示するには、「ユーザーに資格情報の自己管理を許可する」を参照してください。

AWS 管理者は、IAM でユーザー、グループ、ロール、ポリシーを管理するために IAM へのフルアクセスが必要です。前提条件AdministratorAccessすべての AWS へのフルアクセスを含む AWS 管理ポリシー。このポリシーは、AWS Billing and Cost Management コンソールへのアクセスを許可しません。また、AWS アカウントのルートユーザー認証情報を必要とするタスクを許可しません。詳細については、「」を参照してください。AWS アカウントのルートユーザーの認証を必要とする AWS タスク()AWS 全般のリファレンス。

> **Warning**
>
> AWS へのフルアクセスを持つのは、管理者ユーザーに限ります。このポリシーをアタッチされたユーザーは、すべて、認証とアクセスコントロールを完全に管理するアクセス許可と、AWS のすべてのリソースを変更するアクセス許可を付与されます。このユーザーを作成する方法については、「IAM 管理者ユーザーを作成します。」を参照してください。

アクセス制御に必要な権限

管理者から IAM ユーザー認証情報が提供されている場合は、アクセスできるリソースをコントロールするためのポリシーが IAM ユーザーにアタッチされています。AWS Management Console でユーザー ID にアタッチされているポリシーを表示するには、以下のアクセス許可が必要です。

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

追加のアクセス許可が必要な場合は、管理者に依頼し、ポリシーを更新して必要なアクションへのアクセスを許可してもらいます。

グローバルアクセラレータと IAM との連携の理解

サービスでは IAM と連携できます。

アクション

グローバルアクセラレータは、ポリシーでのアクションの使用をサポートしています。これにより、管理者は、グローバルアクセラレータでオペレーションを実行することをエンティティに許可するかどうかをコントロールできます。たとえば、エンティティがGetPolicyAWS API オペレーションを使用してポリシーを表示する場合、管理者はiam:GetPolicyaction.

以下のポリシー例では、ユーザーがCreateAcceleratorオペレーションを使用して、AWS アカウントのアクセラレータをプログラムで作成します。

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

リソースレベルのアクセス許可

グローバルアクセラレータは、リソースレベルのアクセス許可をサポートします。リソースレベルのアクセス許可では、ARN を使用してポリシーで個々のリソースを指定できます。

リソースベースのポリシー

グローバルアクセラレータでは、リソースベースのポリシーはサポートされていません。リソースベースのポリシーでは、サービス内のリソースにポリシーをアタッチできます。リソースベースのポリシーには、Principal要素を使用して、リソースにアクセスできる IAM ID を指定します。

タグに基づいた承認

グローバルアクセラレータは、認証ベースのタグをサポートします。この機能により、ポリシーの条件でリソースタグを使用できます。

一時認証情報

Global Acceleratorer は、一時的な認証情報を使用して、フェデレーションを使用してサインインし、IAM ロールを引き受ける、またはクロスアカウントロールを引き受けることができます。一時的なセキュリティ認証情報を取得するには、AWS STS API オペレーションを呼び出します。AssumeRoleまたはGetFederationToken。

サービスにリンクされたロール

グローバルアクセラレータは、サービスにリンクされたロールをサポートします。この機能では、サービスにリンクされたロールをユーザーに代わって引き受けることをサービスに許可します。このロールにより、サービスはユーザーに代わって他のサービスのリソースにアクセスし、アクションを実行できます。サービスにリンクされたロールは、IAM アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスロール

グローバルアクセラレータでは、サービスロールはサポートされていません。この機能では、サービスのロールをユーザーに代わって引き受けることをサービスに許可します。このロールにより、サービスはユーザーに代わって他のサービスのリソースにアクセスし、アクションを実行できます。サービスロールは、IAM アカウントに表示され、サービスによって所有されます。つまり、IAM 管理者は、このロールのアクセス許可を変更できます。ただし、これにより、サービスの機能が損なわれる場合があります。

認証とアクセスコントロールのトラブルシューティング

次の情報は、IAM の使用時に発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- グローバルアクセラレータでアクションを実行する権限がない
- 管理者としてグローバルアクセラレータへのアクセスを他のユーザーに許可したい
- IAMは専門家にならずに理解したい

グローバルアクセラレータでアクションを実行する権限がない

AWS マネジメントコンソールから、アクションを実行する権限がないと通知された場合、ユーザー名とパスワードの提供元の管理者に問い合わせる必要があります。

以下の例は、IAM ユーザーの名前がmy-user-nameはコンソールを使用してglobalaccelerator:CreateAcceleratorアクションがありますが、アクセス許可はありません。

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

この場合、管理者に依頼し、ポリシーを更新してアクセスを許可してもらいます。my-example-acceleratorリソースを使用してaws-globalaccelerator:CreateAcceleratoraction.

管理者としてグローバルアクセラレータへのアクセスを他のユーザーに許可したい

グローバルアクセラレーターへのアクセスを他のユーザーに許可するには、アクセスを必要とする人またはアプリケーションの IAM エンティティ (ユーザーまたはロール) を作成する必要があります。ユーザーは、このエンティティの認証情報を使用して AWS にアクセスします。次に、グローバルアクセラレータの適切なアクセス許可を付与するポリシーを、そのエンティティにアタッチする必要があります。

すぐに開始するには、「IAM の使用開始」を参照してください。

IAMは専門家にならずに理解したい

IAM の用語、概念、および手順の詳細については、以下のトピックを参照してください。

- 認証とは
- アクセス制御とは
- ポリシーとは

タグベースのポリシー

IAM ポリシーの設計時に特定のリソースへのアクセスを許可することで、詳細なアクセス許可を設定できます。管理するリソースの数が増えるに従って、このタスクはより困難になります。アクセラレータにタグ付けしてポリシーステートメント条件でタグを使用することにより、このタスクをより容易にすることができます。特定のタグを使用して任意のアクセラレータにアクセス権を一括して付与します。次に、アクセラレーターを作成するとき、または後でアクセラレーターを更新することによって、このタグを関連するアクセラレーターに繰り返し適用します。

> **Note**
>
> 条件内でタグを使用することは、リソースとリクエストへのアクセスをコントロールする 1 つの方法です。グローバルアクセラレータでのタグ付けについては、」AWS Global Accelerator でのタグ付け。

タグは、リソースにアタッチするか、リクエストでタグ付けをサポートするサービスに渡すことができます。グローバルアクセラレータでは、タグを含めることができるのはアクセラレータだけです。IAM ポリシーを作成するときに、タグ条件キーを使用して以下を制御できます。

- 既にあるタグに基づいて、どのユーザーがアクセラレータに対してアクションを実行できるか。
- アクションのリクエストで渡すことができるタグ。
- リクエストで特定のタグキーを使用できるかどうか。

タグ条件キーの完全な構文とセマンティクスについては、IAM タグを使用してアクセスを制御する()IAM ユーザーガイド。

たとえば、グローバルアクセラレータGlobalAcceleratorFullAccess管理ユーザーポリシーは、すべてのリソースに対して任意の Global Accelerator アクションを実行する無制限のアクセス許可をユーザーに付与します。次のポリシーは、この権限を制限し、認証されていないユーザーに対して生産アクセラレーター. お客様の管理者は、管理されたユーザーポリシーに加えて、この IAM ポリシーを未認可の IAM ユーザーにアタッチする必要があります。

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

グローバルアクセラレータのサービスにリンクされたロール

AWS Global Accelerator は、AWS Identity and Access Management (IAM) を使用します。サービスにリンクされたロール。サービスにリンクされたロールは、サービスに直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、サービスによって事前定義されており、お客様の代わりにサービスから他の AWS サービスを呼び出す必要のあるアクセス許可がすべて含まれています。

グローバルアクセラレータは、以下の IAM サービスにリンクされたロールを使用します。

- AWSserviceRoleforGlobalアクセラレータ：グローバルアクセラレータは、このロールを使用して、グローバルアクセラレータがクライアントの IP アドレスの保存に必要なリソースを作成および管理できるようにします。

グローバルアクセラレータは、グローバルアクセラレータ API オペレーションをサポートするためにロールが最初に必要なときに、AWSServiceRoleForGlobalAccelerator という名前のロールを自動的に作成します。AWSServiceRoleForGlobalAccelerator ロールを使用すると、グローバルアクセラレータは、クライアントの IP アドレスの保存に必要なリソースを作成および管理することができます。この役割は、グローバルアクセラレータでアクセラレータを使用する場合に必要です。AWSServiceRoleForGlobalAccelerator ロールの ARN は次のようになります。

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

サービスにリンクされたロールを使用することで、必要なアクセス許可を手動で追加する必要がなくなるため、グローバルアクセラレーターの設定や使用が簡単になります。グローバルアクセラレーターはそのサービスにリンクされたロールのアクセス許可を定義し、グローバルアクセラレーターのみがそのロールを引き受けることができます。定義されたアクセス権限には、信頼ポリシーとアクセ

ス権限ポリシーが含まれます。アクセス権限ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールを削除する前に、それらのロールに関連付けられているグローバルアクセラレータリソースを削除する必要があります。このようにして、アクティブなリソースにアクセスするためにまだ必要な、サービスにリンクされたロールが削除されないようにすることで、グローバルアクセラレータリソースが保護されます。

サービスにリンクされたロールをサポートしているその他のサービスの詳細については、」IAM と連携する AWS のサービスを持っているサービスを探しますはい()サービスにリンクされたロール列でロードバランサーの ID をクリックします。

グローバルアクセラレータのサービスにリンクされたロールのアクセス許可

グローバルアクセラレータは、AWSserviceRoleforGlobalアクセラレータ。以下のセクションでは、ロールのアクセス許可を説明します。

サービスにリンクされたロールのアクセス許可

このサービスリンクロールにより、Global Accelerator は EC2 Elastic Network インターフェイスとセキュリティグループを管理し、エラーの診断に役立ちます。

AWSServiceRoleForGlobalAccelerForGlobalAcceleroleForGlobalAcceleroleFor

- `globalaccelerator.amazonaws.com`

ロールのアクセス許可ポリシーでは、ポリシーに示すように、グローバルアクセラレーターは、指定されたリソースで次のアクションを完了することができます。

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

グローバルアクセラレーターサービスにリンクされたロールの削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「」を参照してください。サービスにリンクされたロールのアクセス権限()IAM ユーザーガイド。

グローバルアクセラレータのサービスにリンクされたロールの作成

グローバルアクセラレータのサービスにリンクされたロールを手動で作成する必要はありません。アクセラレータを初めて作成すると、サービスによってロールが自動的に作成されます。グローバルアクセラレータリソースを削除し、サービスにリンクされたロールを削除した場合、新しいアクセラレータを作成すると、サービスは再び自動的にロールを作成します。

グローバルアクセラレータのサービスにリンクされたロールを編集する

グローバルアクセラレーターでは、AWSServiceRoleForGlobalAcceleroleForGlobalAcceleroleサービス サービスによってサービスにリンクされたロールが作成された後は、多くのエンティティでそのロールが参照されるため、そのロール名は変更できません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「」を参照してください。サービスにリンクされたロールの編集()IAM ユーザーガイド。

グローバルアクセラレータのサービスにリンクされたロールの削除

グローバルアクセラレータを使用する必要がなくなった場合は、サービスにリンクされたロールを削除することをお勧めします。そうすることで、アクティブにモニタリングやメンテナンスがされていない不要なエンティティがなくなります。ただし、ロールを手動で削除する前に、アカウントのグローバルアクセラレーターリソースをクリーンアップする必要があります。

アクセラレータを無効にして削除したら、サービスにリンクされたロールを削除できます。アクセラレータの削除の詳細については、」 標準アクセラレータの作成または更新。

> **Note**
>
> アクセラレーターを無効にして削除しても、グローバルアクセラレーターによる更新が完了していない場合、サービスにリンクされたロールの削除は失敗することがあります。発生した場合は、数分待ってから、サービスにリンクされたロールの削除手順をもう一度試してください。

AWSServiceRoleForGlobalAccelerator サービスにリンクされたロールを手動で削除するには

1. AWS マネジメントコンソールにサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM コンソールのナビゲーションペインで [ロール] を選択します。ロール名または行そのものではなく、削除するロール名の横にあるチェックボックスをオンにします。

3. ページ上部にある [ロールのアクション] で [ロールの削除] を選択します。
4. 確認ダイアログボックスで、サービスの最終アクセス時間データを確認します。これは、選択したそれぞれのロールの AWS のサービスへの最終アクセス時間を示します。これは、そのロールが現在アクティブであるかどうかを確認するのに役立ちます。先に進む場合は、[Yes, Delete] を選択し、削除するサービスにリンクされたロールを送信します。
5. IAM コンソール通知を見て、サービスにリンクされたロールの削除の進行状況を監視します。IAM サービスにリンクされたロールの削除は非同期であるため、削除するロールを送信すると、削除タスクは成功または失敗する可能性があります。詳細については、「」を参照してください。サービスにリンクされたロールの削除()IAM ユーザーガイド。

グローバルアクセラレータサービスリンクロール（AWS 管理ポリシー）の更新

このサービスがこれらの変更の追跡を開始してから、のサービスリンクロールの更新に関する詳細を表示します。このページの変更に関する自動アラートについては、AWS Global Accelerator の RSS フィードを購読してくださいドキュメント履歴ページで.

変更	説明	日付
AWSserviceRoleforGlobalアクセラレータ— ポリシーの更新	グローバルアクセラレータは、グローバルアクセラレータでエラーを診断するための新しいアクセス許可を追加しました。 グローバルアクセラレータはec2:DescribeRegions を使用して、お客様がいるAWS リージョンを特定します。これは、Global Accelerator がエラーのトラブルシューティングに役立ちます。	2021年5月18日
グローバルアクセラレータが変更の追跡を開始しました	Global Accelerator が AWS 管理ポリシーの変更の追跡を開始しました。	2021年5月18日

グローバルアクセラレータサービスにリンクされたロールでサポートされているリージョン

グローバルアクセラレータは、グローバルアクセラレータがサポートされている AWS リージョンで、サービスにリンクされたロールの使用をサポートします。

グローバルアクセラレーターやその他のサービスが現在サポートされている AWS リージョンのリストについては、AWS リージョン表。

アクセスと認証の概要

IAM を初めて使用する場合は、以下のトピックを読んで AWS の認証とアクセスを開始してください。

トピック

- 認証とは
- アクセス制御とは
- ポリシーとは
- IAM の使用開始

認証とは

認証は、認証情報を使用して AWS にサインインする方法です。

> **Note**
>
> すぐに開始するには、このセクションを無視できます。最初に、「」の基本情報に目を通してください。AWS Global Accelerator の ID とアクセス管理「」および「」を参照してください。IAM の使用開始。

プリンシパルとして、あなたは認証済み(AWS にサインイン)。エンティティー (ルートユーザー、IAM ユーザー、IAM ロール) を使用して AWS にリクエストを送信します。IAM ユーザーは、ユーザー名とパスワード、アクセスキーのセットなど、長期的な認証情報を持つことができます。IAM ロールを引き受けると、一時的なセキュリティ認証情報が付与されます。

AWS Management Console からユーザーとして認証するには、ユーザー名とパスワードを使用してサインインする必要があります。AWS CLI または AWS API から認証するには、アクセスキーと

シークレットキー、または一時的な認証情報を指定する必要があります。AWS では、SDK と CLI ツールを提供して、お客様の認証情報を使用して、リクエストに暗号で署名できます。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。使用する認証方法を問わず、追加のセキュリティ情報の提供を要求される場合もあります。たとえば、AWS では Multi-Factor Authentication (MFA) を使用してアカウントのセキュリティを高めることを推奨しています。

プリンシパルとして、以下のエンティティ (ユーザーまたはロール) を使用して AWS にサインインできます。

AWS アカウントのルートユーザー

AWS アカウントを初めて作成する場合は、すべての AWS のサービスとリソースに対して完全なアクセス権限を持つシングルサインイン ID で始めます。このアイデンティティは root ユーザーと呼ばれ、AWS アカウントの作成に使用したメールアドレスとパスワードでのサインインによりアクセスされます。強くお勧めしているのは、日常的なタスクには、それが管理者タスクであっても、root ユーザーを使用しないことです。代わりに、最初の IAM ユーザーを作成するためにのみ、ルートユーザーを使用するというベストプラクティスに従います。その後、ルートユーザーの認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。

IAM ユーザー

あんIAM ユーザーは、特定のアクセス許可を持つ、AWS アカウント内のエンティティです。グローバルアクセラレーター署名バージョン 4では、インバウンド API リクエストを認証するためのプロトコルです。リクエストの認証については、「」を参照してください。署名バージョン 4 署名プロセス()AWS 全般のリファレンス。

IAM ロール

あんIAM ロールは、特定のアクセス権限を持ち、アカウントで作成できる IAM アイデンティティです。IAM ロールは、AWS でできることとできないことを決定するのが、アクセス許可ポリシーを伴う AWS アイデンティティであるという点で IAM ユーザーと似ています。ただし、ユーザーは 1 人の特定の人に一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。また、ロールには標準の長期認証情報 (パスワードやアクセスキーなど) も関連付けられません。代わりに、ロールを引き受けると、ロールセッション用の一時的なセキュリティ認証情報が提供されます。IAM ロールと一時的な認証情報は、次の状況で役立ちます。

フェデレーティッドユーザーアクセス

IAM ユーザーを作成するのではなく、AWS Directory Service、エンタープライズユーザーディレクトリ、またはウェブアイデンティティプロバイダーの既存のアイデンティティを

使用することもできます。このようなユーザーはフェデレーティッドユーザーと呼ばれます。AWS では、ID プロバイダーを通じてアクセスがリクエストされたとき、フェデレーティッドユーザーにロールを割り当てます。フェデレーティッドユーザーの詳細については、」フェデレーティッドユーザーとロール()IAM ユーザーガイド。

一時的なユーザー権限

IAM ユーザーは、ロールを引き受けることで、一時的に特定のタスクに対して異なるアクセス許可を取得することができます。

クロスアカウントアクセス

IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを別のアカウントの信頼済みプリンシパルに許可できます。ロールは、クロスアカウントアクセスを許可する主な方法です。ただし、一部の AWS のサービスでは、(ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできます。グローバルアクセラレータでは、これらのリソースベースのポリシーはサポートされていません。ロールとリソースベースのポリシーのいずれを使用してクロスアカウントアクセスを許可するかの詳細については、「別のアカウント内のプリンシパルに対するアクセスコントロール」を参照してください。

AWS サービスへのアクセス

サービスロールとはIAM ロールサービスがお客様に代わってアクションを実行すると引き受けること。サービスロールは、お客様のアカウント内のみでアクセスを提供します。他のアカウントのサービスへのアクセス権を付与するためにサービスロールを使用することはできません。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「」を参照してください。AWS のサービスにアクセス許可を委任するロールの作成()IAM ユーザーガイド。

Amazon EC2 で実行中のアプリケーション

EC2 インスタンスで実行され、AWS CLI または AWS API リクエストを作成しているアプリケーションの一時的な認証情報を管理するには、IAM ロールを使用します。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時認証情報を取得することができます。詳細については、「」を参照してください。IAM ロールを使用して、Amazon EC2 インスタンスで実行されるアプリケーションにアクセス許可を付与する()IAM ユーザーガイド。

アクセス制御とは

AWS にサインイン (認証) した後では、AWS リソースおよびオペレーションへのアクセスはポリシーによって管理されます。アクセスコントロールは承認とも呼ばれます。

> **Note**
>
> すぐに開始するには、このページを無視できます。最初に、「」の基本情報に目を通してください。AWS Global Accelerator の ID とアクセス管理「」および「」を参照してください。IAM の使用開始。

承認中、AWS はリクエストのコンテキスト該当するポリシーを確認します。次に、ポリシーを使用してリクエストの許可または拒否を決定します。大半のポリシーは JSON ドキュメントとして AWS に保存され、プリンシパルに対して許可または拒否するアクセス許可を指定します。JSON ポリシードキュメントの構造と内容の詳細については、「ポリシーとは」を参照してください。

ポリシーにより、管理者は AWS リソースへのアクセスを許可するユーザーと、これらのリソースで実行できるアクションを指定できます。すべての IAM エンティティ (ユーザーまたはロール) は、アクセス許可のない状態からスタートします。言い換えると、デフォルト設定では、ユーザーは何もできず、そのユーザーのアクセスキーを参照することすらできません。何かを実行するアクセス許可をユーザーに付与するには、管理者がユーザーにアクセス許可ポリシーをアタッチする必要があります。または、必要なアクセス許可がアタッチ済みであるグループにユーザーを追加できます。次に、管理者がグループにアクセス許可を付与すると、そのアクセス許可はグループ内のすべてのユーザーに付与されます。

リクエストを認証できる有効な認証情報がある場合でも、管理者からアクセス許可が付与されない限り、AWS Global Accelerator リソースを作成したり、これらのリソースにアクセスしたりすることはできません。たとえば AWS Global Accelerator を作成するには、そのための明示的なアクセス許可が必要です。

管理者は、以下へのアクセスをコントロールするポリシーを作成できます。

- プリンシパル— リクエストを行っているユーザーまたはアプリケーションを制御する (プリンシパル) が許可されています。
- IAM ID— どの IAM アイデンティティ (グループ、ユーザー、ロール) にどのようにアクセスできるかをコントロールします。
- IAM ポリシー : だれがカスタマー管理ポリシーを作成、編集、削除でき、だれがすべての管理ポリシーをアタッチおよびデタッチできるかをコントロールします。

- AWS リソース— アイデンティティベースのポリシーまたはリソースベースのポリシーを使用してだれがリソースにアクセスできるかをコントロールできます。
- AWS アカウント— リクエストを特定のアカウントのメンバーにのみ許可するかどうかをコントロールします。

プリンシパルへのアクセスの制御

アクセス許可ポリシーは、プリンシパルに実行することを許可する操作をコントロールします。管理者は、アクセス許可を付与するアイデンティティ (ユーザー、グループ、またはロール) に対して、アイデンティティベースのアクセス許可ポリシーをアタッチする必要があります。アクセス許可ポリシーでは、AWS へのアクセスを許可または拒否します。管理者は、IAM エンティティ (ユーザーまたはロール) のアクセス許可の境界を設定して、エンティティに許可されるアクセス許可の上限を定義することもできます。アクセス許可の境界は IAM のアドバンスド機能です。アクセス許可の境界の詳細については、」IAM ID のアクセス許可の境界()IAM ユーザーガイド。

プリンシパルの AWS アクセスを制御する方法の詳細と例については、プリンシパルへのアクセスの制御()IAM ユーザーガイド。

ID へのアクセスの制御

管理者は、IAM アイデンティティ (ユーザー、グループ、ロール) に対して実行できる操作や、アイデンティティにアクセスできるユーザーを制限するポリシーを作成して、IAM アイデンティティ (ユーザーまたはグループ) に対して実行できる操作を制御します。次に、このポリシーを、アクセス許可を付与するアイデンティティにアタッチします。

たとえば、管理者は、特定の 3 ユーザーのパスワードをリセットすることを許可できます。これを行うには、IAM ユーザーにポリシーをアタッチします。このポリシーにより、ユーザー自身と特定の 3 ユーザーの ARN を持つユーザーのパスワードに限り、リセットすることを許可します。これにより、チームメンバーのパスワードはリセットできますが、他の IAM ユーザーのパスワードはリセットできません。

ポリシーを使用して ID への AWS アクセスを制御する方法の詳細と例については、」ID へのアクセスの制御()IAM ユーザーガイド。

ポリシーへのアクセスの制御

管理者は、だれがカスタマー管理ポリシーを作成、編集、削除でき、だれがすべての管理ポリシーをアタッチおよびデタッチできるかをコントロールできます。ポリシーを確認する場合、そのポリシー内の各サービスのアクセスレベルの要約を含むポリシー概要を表示できます。AWS は、各

サービスアクションを 4 つの 1 つに分類します。アクセスレベル各アクションが何をするかに基づいて：List,Read,Write, またはPermissions management。これらのアクセスレベルを使用して、ポリシーに含めるアクションを判断できます。詳細については、「」を参照してください。ポリシー概要内のアクセスレベルの概要について()IAM ユーザーガイド。

> **Warning**
>
> 制限する必要がありますPermissions Managementアカウントのアクセスレベルのアクセス権限。制限しないと、アカウントのメンバーは各自のポリシーを作成するときに必要以上のアクセス許可を使用できるようになります。または、AWS へのフルアクセスを使用して個別のユーザーを作成できます。

ポリシーへの AWS アクセスを制御する方法の詳細と例については、」ポリシーへのアクセスの制御()IAM ユーザーガイド。

のリソースへのアクセスの制御

管理者は、アイデンティティベースのポリシーまたはリソースベースのポリシーを使用してリソースへのアクセスをコントロールできます。アイデンティティベースのポリシーでは、ポリシーをアイデンティティにアタッチし、そのアイデンティティがアクセスできるリソースを指定します。リソースベースのポリシーでは、制御するリソースにポリシーをアタッチします。ポリシーでは、リソースにアクセスできるプリンシパルを指定します。

詳細については、「」を参照してください。リソースへのアクセスコントロール()IAM ユーザーガイド。

リソース作成者は自動的に権限を持たない

アカウントのすべてのリソースは、その作成者を問わず、アカウントが所有します。AWS アカウントのルートユーザーはアカウント所有者であるため、アカウント内のリソースに対して任意のアクションを実行するアクセス許可を持ちます。

> **Important**
>
> 強くお勧めしているのは、日常的なタスクには、それが管理者タスクであっても、root ユーザーを使用しないことです。代わりに、最初の IAM ユーザーを作成するためにのみ、ルートユーザーを使用するというベストプラクティスです。。その後、ルートユーザーの認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タス

クのみを実行します。ルートユーザーとしてサインインする必要があるタスクを確認するには、」root ユーザーを必要とする AWS タスク。

AWS アカウントのエンティティ (ユーザーまたはロール) には、リソースを作成するためのアクセス権を付与する必要があります。しかし、リソースを作成しても、そのリソースへのフルアクセスが自動的に許可されるわけではありません。管理者は、アクションごとに明示的にアクセス許可を付与する必要があります。さらに、管理者はユーザーやロールのアクセス許可を管理するアクセス許可を持っている限り、アクセス許可をいつでも取り消すことができます。

別のアカウント内のプリンシパルに対するアクセスコントロール

管理者は、AWS リソースベースのポリシー、IAM クロスアカウントロール、または AWS Organizations サービスを使用して、別のアカウントのプリンシパルがアカウントのリソースにアクセスすることを許可できます。

一部の AWS サービスでは、管理者は、リソースに対するクロスアカウントアクセス許可を付与できます。これを行うには、プロキシとしてロールを使用する代わりに、共有するリソースに直接ポリシーをアタッチします。このポリシータイプをサービスでサポートしている場合、管理者が共有するリソースもリソースベースのポリシーをサポートしている必要があります。ユーザーベースのポリシーとは異なり、リソースベースのポリシーでは、だれがリソースにアクセスできるかを AWS アカウント ID 番号のリストの形式で指定します。グローバルアクセラレータでは、リソースベースのポリシーはサポートされていません。

クロスアカウントアクセスには、ロールを使うよりも、リソースベースのポリシーを使うほうがいくつかの点で有利です。リソースベースのポリシーによってリソースにアクセスする場合、プリンシパル (人またはアプリケーション) は依然として信頼されたアカウントで作業を行います。ロールのアクセス許可を取得する代わりに自身のアクセス許可が無効になることはありません。つまり、プリンシパルは、信頼される側のアカウントおよび信頼する側のアカウントの両方で、同時にリソースへのアクセス権を保持します。これは、2 つのアカウント間で情報をコピーする場合などに便利です。クロスアカウントロールの使用の詳細については、「」を参照してください。所有している別の AWS アカウントへのアクセス権を IAM ユーザーに提供()IAM ユーザーガイド。

AWS Organizations では、ユーザーが所有している複数の AWS アカウントに対してポリシーベースの管理を提供します。Organizations では、アカウントのグループを作成し、アカウントの作成を自動化して、これらのグループにポリシーを適用して管理することができます。Organizations では、カスタムスクリプトや手動プロセスを必要とすることなく、複数のアカウントをまたいでポリシーを一元管理できます。AWS Organizations を使用して、AWS アカウントをまたいで AWS サービスの

使用を一元管理するサービスコントロールポリシー (SCP) を作成できます。詳細については、「」を参照してください。AWS Organizations とは何ですか?()AWS Organizations ユーザーガイド。

ポリシーとは

AWS でアクセスを制御するには、ポリシーを作成して IAM のアイデンティティや AWS のリソースにアタッチします。

> **Note**
>
> すぐに開始するには、このページを無視できます。最初に、「」の基本情報に目を通してください。AWS Global Accelerator の ID とアクセス管理「」および「」を参照してください。IAM の使用開始。

ポリシーは AWS のオブジェクトであり、エンティティやリソースに関連付けて、これらのアクセス許可を定義します。AWS は、ユーザーなどのプリンシパルがリクエストを行ったときに、それらのポリシーを評価します。ポリシーでのアクセス許可により、リクエストが許可されるか拒否されるかが決まります。大半のポリシーは JSON ドキュメントとして AWS に保存されます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションのアクセス許可を定義します。たとえば、ポリシーでGetUserアクションを適用している場合、そのポリシーをアタッチされたユーザーは AWS マネジメントコンソール、AWS CLI、または AWS API からユーザー情報を取得することができます。IAM ユーザーを作成したら、コンソールまたはプログラムによるアクセスを許可するようにユーザーを設定できます。IAM ユーザーは、ユーザー名とパスワードを使用してコンソールにサインインできます。または、アクセスキーを使用して CLI または API を操作できます。

以下のポリシータイプ (頻度順) は、リクエストが承認されるかどうかに影響する場合があります。詳細については、「」を参照してください。ポリシータイプ()IAM ユーザーガイド。

アイデンティティベースのポリシー

マネージドポリシーとインラインポリシーを IAM アイデンティティ (ユーザー、ユーザーの所属グループ、およびロール) にアタッチできます。

リソースベースのポリシー

一部の AWS サービスのリソースにインラインポリシーをアタッチできます。リソースベースのポリシーとして最も一般的な例は、Amazon S3 バケットポリシーと IAM ロールの信頼ポリシーです。グローバルアクセラレータでは、リソースベースのポリシーはサポートされていません。

Organizations SCP

AWS Organizations サービスコントロールポリシー (SCP) を使用して、AWS 組織の組織または組織単位 (OU) に権限の境界を適用できます。これらのアクセス許可は、メンバーアカウント内のすべてのエンティティに適用されます。

アクセスコントロールリスト (ACL)

ACL を使用して、リソースにアクセスできるプリンシパルをコントロールできます。ACL は、リソースベースのポリシーと似ていますが、JSON ポリシードキュメント構造を使用しない唯一のポリシータイプです。グローバルアクセラレータは ACL をサポートしている OR をサポートしていません。

これらのポリシータイプは、アクセス許可ポリシーまたはアクセス許可の境界として分類できます。

アクセス許可ポリシー

アクセス許可ポリシーを AWS のリソースにアタッチして、そのオブジェクトのアクセス許可を定義できます。AWS では、1 つのアカウント内のすべてのアクセス許可ポリシーがまとめて評価されます。アクセス許可ポリシーは、最も一般的なポリシーです。アクセス許可ポリシーとして、以下のポリシータイプを使用できます。

アイデンティティベースのポリシー

管理ポリシーまたはインラインポリシーを IAM ユーザー、グループ、またはロールにアタッチすると、そのエンティティのアクセス許可がポリシーで定義されます。

リソースベースのポリシー

JSON ポリシードキュメントをリソースにアタッチするときに、そのリソースのアクセス許可を定義します。サービスでリソースベースのポリシーをサポートしている必要があります。

アクセスコントロールリスト (ACL)

リソースに ACL をアタッチするときに、そのリソースにアクセスする権限を持つプリンシパルのリストを定義します。リソースで ACL をサポートしている必要があります。

アクセス許可の境界

ポリシーを使用して、エンティティ (ユーザーまたはロール) のアクセス許可の境界を定義できます。アクセス許可の境界では、エンティティに付与できるアクセス許可の上限をコントロールします。アクセス許可の境界は AWS のアドバンスド機能です。複数のアクセス許可の境界がリク

エストに適用される場合、AWS は各アクセス許可の境界を個別に評価します。アクセス許可の境界は以下の状況で適用できます。

Organizations

AWS Organizations サービスコントロールポリシー (SCP) を使用して、AWS 組織の組織または組織単位 (OU) にアクセス許可の境界を適用できます。

IAM ユーザーまたはロール

ユーザーまたはロールのアクセス許可の境界として管理ポリシーを使用できます。詳細については、「」を参照してください。IAM エンティティのアクセス許可の境界()IAM ユーザーガイド。

トピック

- アイデンティティベースのポリシー
- リソースベースのポリシー
- ポリシーアクセスレベルの分類

アイデンティティベースのポリシー

ポリシーを IAM アイデンティティにアタッチできます。たとえば、次の操作を実行できます。

アカウントのユーザーまたはグループにアクセス権限ポリシーをアタッチする

AWS Global Accelerator リソースを作成するアクセス許可を付与するために、ユーザーまたはユーザーが所属するグループにアクセス許可ポリシーをアタッチできます。

ロールにアクセス権限ポリシーをアタッチする (クロスアカウントアクセス権限を付与する)

アイデンティティベースのアクセス権限ポリシーを IAM ロールにアタッチして、クロスアカウントアクセス権限を付与できます。たとえば、アカウント A の管理者は、次のように他のまたは AWS にクロスアカウントのアクセス権限を別の AWS アカウント (アカウント B) または AWS サービスに付与するロールを作成することができます。

1. アカウント A の管理者は、IAM ロールを作成して、アカウント A のリソースに権限を付与するロールに権限ポリシーをアタッチします。
2. アカウント A の管理者は、アカウント B をそのロールを引き受けるプリンシパルとして識別するロールに、信頼ポリシーをアタッチします。
3. アカウント B の管理者は、アカウント B のユーザーにロールを引き受ける権限を委任できるようになります。これにより、アカウント B のユーザーにアカウント A のリソースの作成と

アクセスが許可されます。AWS サービスのアクセス権限を付与してロールを引き受けさせたい場合は、信頼ポリシー内のプリンシパルも、AWS サービスのプリンシパルとなることができます。

IAM を使用したアクセス許可の委任の詳細については、「」を参照してください。アクセス管理()IAM ユーザーガイド。

ユーザー、グループ、ロール、アクセス許可の詳細については、IAM ユーザーガイドの「アイデンティティ (ユーザー、グループ、ロール)」を参照してください。

以下に、グローバルアクセラレータで使用できるポリシーの例を 2 つ示します。最初のサンプルポリシーでは、AWS アカウントのアクセラレータに対するすべての List アクションと Describe アクションへのプログラムによるアクセスをユーザーに付与します。

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

次の例では、へのプログラムによるアクセスを許可します。ListAcceleratorsオペレーション:

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

```
}
```

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチする JSON ポリシードキュメントです。これらのポリシーでは、指定されたプリンシパルがリソースに対して実行できるアクションと実行条件を指定できます。最も一般的なリソースベースのポリシーは、Amazon S3 バケットです。リソースベースのポリシーは、リソース固有のインラインポリシーです。マネージド型のリソースベースのポリシーはありません。

リソースベースのポリシーを使用して他の AWS アカウントのメンバーにアクセス許可を付与することは、IAM ロールに比べて、いくつかの利点があります。詳細については、「」を参照してください。IAM ロールとリソースベースのポリシーとの相違点()IAM ユーザーガイド。

ポリシーアクセスレベルの分類

IAM コンソールでは、アクションが以下のアクセスレベルの分類に従ってグループ分けされます。

リスト

サービス内のリソースを一覧表示し、オブジェクトの存在を判断するアクセス許可を提供します。このレベルのアクセス権を持つアクションはオブジェクトをリストできますが、リソースのコンテンツは表示されません。List アクセスレベルの大半のアクションは、特定のリソースに対しては実行できません。これらのアクションを使用してポリシーステートメントを作成する場合は、[All resources (すべてのリソース)] ("*") を指定する必要があります。

Read

サービス内のリソースのコンテンツと属性を読み取るアクセス許可を提供します。ただし、編集するアクセス許可はありません。たとえば、Amazon S3 オペレーション`GetObject`および`GetBucketLocation`前提条件Readアクセスレベル.

書き込み

サービス内のリソースを作成、削除、または変更するためのアクセス許可を提供します。たとえば、Amazon S3 オペレーション`CreateBucket`,`DeleteBucket`, および`PutObject`前提条件書き込みアクセスレベル.

アクセス権限の管理

サービス内のリソースに対するアクセス許可を付与または変更するためのアクセス許可を提供します。たとえば、ほとんどの IAM および AWS Organizations ポリシーアクションには、アクセス権限の管理アクセスレベル.

> **Tip**
>
> AWS アカウントのセキュリティを強化するには、ポリシーを制限したり定期的にモニタリングします。アクセス権限の管理アクセスレベルの分類

タグ付け

サービス内のリソースにアタッチされているタグを作成、削除、または変更するアクセス許可を提供します。たとえば、Amazon EC2`CreateTags`および`DeleteTags`オペレーションにはタグ付けアクセスレベル.

IAM の使用開始

AWS Identity and Access Management (IAM) は、サービスおよびリソースへのアクセスを安全に管理するための AWS のサービスです。IAM は追加料金なしで提供している AWS アカウントの機能です。

> **Note**
>
> IAM を開始する前に、「」で基本的な情報に目を通してください。AWS Global Accelerator の ID とアクセス管理。

AWS アカウントを初めて作成する場合は、すべての AWS のサービスとリソースに対して完全なアクセス権限を持つシングルサインイン ID で始めます。このアイデンティティは root ユーザーと呼ばれ、AWS アカウントの作成に使用したメールアドレスとパスワードでのサインインによりアクセスされます。強くお勧めしているのは、日常的なタスクには、それが管理者タスクであっても、root ユーザーを使用しないことです。代わりに、最初の IAM ユーザーを作成するためにのみ、ルートユーザーを使用するというベストプラクティスに従います。その後、ルートユーザーの認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。

IAM 管理者ユーザーを作成します。

自分用の管理者ユーザーを作成し、そのユーザーを管理者グループに追加するには (コンソール)

1. サインインします。IAM コンソールを選択して、アカウントの所有者としてルートユーザーをクリックし、AWS アカウントの E メールアドレスを入力します。次のページでパスワードを入力します。

   > **Note**
   >
   > 強くお勧めします、使用するためのベストプラクティスに従います。**Administrator**ルートユーザー認証情報を追跡し、安全な場所に保管する IAM ユーザー。ルートユーザーとしてのサインインは、いくつかのアカウントとサービスの管理タスクの実行にのみ使用してください。

2. ナビゲーションペインで [Users]、[Add user] の順に選択します。
3. [ユーザー名] に「**Administrator**」と入力します。
4. [AWS Management Console access (AWS マネジメントコンソールへのアクセス)] の横にあるチェックボックスをオンにします。[Custom password (カスタムパスワード)] を選択し、その後テキストボックスに新しいパスワードを入力します。
5. (オプション) デフォルトでは、AWS は新しいユーザーの初回のサインイン時に新しいパスワードの作成を要求します。必要に応じて [User must create a new password at next sign-in (ユーザーは次回のサインイン時に新しいパスワードを作成する必要がある)] のチェックボックスをオフにして、新しいユーザーがサインインしてからパスワードをリセットできるようにできます。
6. 選択次へ: アクセス許可。
7. [Set permissions (アクセス許可の設定)] で、[Add user to group (ユーザーをグループに追加)] を選択します。
8. [Create group] を選択します。
9. [グループの作成] ダイアログボックスで、[グループ名] に「**Administrators**」と入力します。
10. 選択フィルタポリシーの適用[]、[] の順に選択します。AWS マネージド-ジョブ機能をクリックして、テーブルの内容をフィルタリングします。
11. ポリシーリストで、[AdministratorAccess] のチェックボックスをオンにします。次に、[Create group] を選択します。

> **Note**
>
> `AdministratorAccess` アクセス許可を使用して AWS の請求およびコスト管理コンソールにアクセスするには、IAM ユーザーと IAM ロールの請求情報へのアクセスを有効にする必要があります。これを行うには、請求コンソールへのアクセスの委任に関するチュートリアルのステップ 1 の手順に従ってください。

12. グループのリストに戻り、新しいグループのチェックボックスをオンにします。必要に応じて [Refresh] を選択し、リスト内のグループを表示します。
13. 選択次へ: タグ。
14. (オプション) タグをキー - 値のペアとしてアタッチして、メタデータをユーザーに追加します。IAM におけるタグの使用の詳細については、「」を参照してください。IAM エンティティのタグ付け()IAM ユーザーガイド。
15. 選択次へ: 確認をクリックして、新しいユーザーに追加するグループメンバーシップのリストを表示します。続行する準備ができたら、[Create user] を選択します。

このプロセスを繰り返して新しいグループとユーザーを作成して、AWS アカウントのリソースへのアクセス許可をユーザーに付与できます。ポリシーを使用して特定の AWS のリソースへのユーザーのアクセス許可を制限する方法については、「AWS リソースのアクセス管理」と「IAM アイデンティティベースのポリシーの例」を参照してください。

Global Accelerator の委任ユーザーの作成

AWS アカウントで複数のユーザーをサポートするには、許可するアクションのみ他のユーザーが実行できるようにアクセス許可を委任する必要があります。そのためには、それらのユーザーが必要なアクセス許可を持つ IAM グループを作成し、ユーザーの作成時に必要なグループに追加します。このプロセスを使用して、AWS アカウント全体のグループ、ユーザー、およびアクセス許可を設定できます。このソリューションは、AWS 管理者が手動でユーザーやグループを管理する中小企業で最もよく使用されます。大規模な組織では、カスタム IAM ロール,フェデレーション, またはシングルサインオン。

以下の手順では、という名前のユーザーを 3 つ作成します。**arnav**,**carlos**, および**martha**という名前のアクセラレータを作成するアクセス許可を付与するポリシーをアタッチします。**my-example-accelerator**しかし、次の30日以内のみ。以下に示す手順を使用して、さまざまなアクセス許可を持つユーザーを追加できます。

委任ユーザーを作成するには (コンソール)

1. AWS マネジメントコンソールにサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [ユーザー]、[ユーザーの追加] の順に選択します。
3. [ユーザー名] に「**arnav**」と入力します。
4. [別のユーザーの追加] を選択し、2 番目のユーザーの名前として「**carlos**」と入力します。さらに [別のユーザーの追加] を選択し、3 番目のユーザーの名前として「**martha**」と入力します。
5. [] のチェックボックスをオンにします。AWS マネジメントコンソールへのアクセス[]、[] の順に選択します。自動生成されたパスワード。
6. 新しいユーザーがサインインしてからパスワードをリセットできるようにするには、必要に応じて [User must create a new password at next sign-in (ユーザーは次回のサインイン時に新しいパスワードを作成する必要がある)] のチェックボックスをオフにします。
7. 選択次へ: アクセス許可。
8. [Attach existing policies directly] を選択します。ユーザーの新しい管理ポリシーを作成します。
9. [Create policy] を選択します。

   [ポリシーの作成] ウィザードが新しいタブまたはブラウザウィンドウで開きます。
10. [Visual editor (ビジュアルエディタ)] タブで、[Choose a service (サービスの選択)] を選択します。[Global Accelerator 上部の検索ボックスを使用して、サービスのリストの結果を制限することができます。

    -サービスセクションが閉じ、アクションセクションが自動的に開きます。
11. 許可する [グローバルアクセラレータ] アクションを選択します。たとえば、アクセラレータを作成するアクセス許可を付与するには、**globalaccelerator:CreateAccelerator**()アクションをフィルタする[] テキストボックス。グローバルアクセラレータアクションのリストがフィルタ処理されたら、[**globalaccelerator:CreateAccelerator**。

    グローバルアクセラレータのアクションは、アクセスレベルの分類別にグループ化され、各アクションが提供するアクセスのレベルをすばやく簡単に判断できます。詳細については、「ポリシーアクセスレベルの分類」を参照してください。
12. 前の手順で選択したアクションが特定のリソースの選択をサポートしていない場合は、すべてのリソースが選択されます。その場合、このセクションを編集することはできません。

リソースレベルのアクセス許可をサポートするアクションを 1 つ以上選択すると、これらのリソースタイプがビジュアルエディタの [Resources (リソース)] セクションに一覧表示されます。選択必要なアクションを選択したアクセラレーターリソースタイプをクリックして、ポリシーに特定のアクセラレータを入力するかどうかを選択します。

13. すべてのリソースに対する `globalaccelerator:CreateAccelerator` アクションを許可する場合は、[All resources (すべてのリソース)] を選択します。

    リソースを指定する場合は、[Add ARN (ARN の追加)] を選択します。リージョンとアカウント ID (またはアカウント ID) を指定します (または [すべて) と入力し、**`my-example-accelerator`**リソースに関して以下の操作を行います。次に、[Add (追加)] を選択します。
14. [Specify request conditions (optional) (リクエスト条件の指定 (省略可能))] を選択します。
15. 選択条件の追加アクセラレーターを作成するアクセス許可を付与します。以後 7 日間以内にします。今日の日付が 2019 年 1 月 1 日であるとします。
16. [Condition Key (条件キー)] で、[aws:CurrentTime] を選択します。この条件キーでは、ユーザーによるリクエストの日時をチェックします。日時が指定した範囲内にある場合に限り、true が返されます (したがって、**`globalaccelerator:CreateAccelerator`** アクションが許可されます)。
17. を使用する場合Qualifierデフォルト値のままにします。
18. 許可された日時範囲の開始を指定するには、[Operator (演算子)] の [DateGreaterThan] を選択します。次に、[Value (値)] に「**`2019-01-01T00:00:00Z`**」と入力します。
19. [Add (追加)] を選択して条件を保存します。
20. [Add another condition (別の条件の追加)] を選択して終了日を指定します。
21. 同様のステップに従って、許可された日時範囲の終了を指定します。[Condition Key (条件キー)] で、[aws:CurrentTime] を選択します。[Operator (演算子)] で、[DateLessThan] を選択します。[Value (値)] に、最初の日から 7 日後の日付である「**`2019-01-06T23:59:59Z`**」を入力します。次に [Add (追加)] を選択して条件を保存します。
22. (省略可能) 作成するポリシーの JSON ポリシードキュメントを表示するには、JSONタブ. いつでも [Visual editor (ビジュアルエディタ)] タブと [JSON] タブを切り替えることができます。ただし、変更を加えたり、ポリシーの確認()Visual editor (ビジュアルエディタ)タブで、IAM はポリシーを再構成してビジュアルエディタに合わせて最適化することがあります。詳細については、「」を参照してください。ポリシーの再構成()IAM ユーザーガイド。
23. 完了したら、[ポリシーの確認] を選択します。
24. リポジトリの []ポリシーの確認ページ、名前に、**`globalaccelerator:CreateAcceleratorPolicy`**。[説明] に「**`Policy to`**

grants permission to create an accelerator」と入力します。ポリシー概要を確認して、目的のアクセス許可を付与していることを確認し、[ポリシーの作成] を選択して新しいポリシーを保存します。

25. 元のタブまたはウィンドウに戻り、ポリシーのリストを更新します。
26. 検索ボックスに「**globalaccelerator:CreateAcceleratorPolicy**」と入力します。新しいポリシーの横のチェックボックスをオンにします。その後、[Next Step] を選択します。
27. 選択次へ: 確認で新しいユーザーをプレビューします。続行する準備ができたら、[ユーザーの作成] を選択します。
28. 新しいユーザーのパスワードをダウンロードまたはコピーし、安全にユーザーに配布します。別に、ユーザーにIAM ユーザーコンソールページへのリンクと、作成したユーザー名を入力します。

ユーザーに資格情報の自己管理を許可する

MFA を設定するには、ユーザーの仮想 MFA デバイスをホストするハードウェアに物理的にアクセスできる必要があります。たとえば、スマートフォンで実行される仮想 MFA デバイスを使用するユーザー用に MFA を設定するとします。その場合、ウィザードを完了するには、そのスマートフォンを利用できる必要があります。このため、ユーザーが自分の仮想 MFA デバイスを構成して管理できるようにすることをお勧めします。その場合、必要な IAM アクションを実行するアクセス許可をユーザーに付与する必要があります。

認証情報の自己管理を許可するポリシーを作成するには (コンソール)

1. AWS マネジメントコンソールにサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、[ポリシー]、 [ポリシーの作成] の順に選択します。
3. [JSON] タブを選択し、以下の JSON ポリシードキュメントからテキストをコピーします。このテキストを [JSON] ボックスに貼り付けます。

> **Important**
>
> 次のポリシー例では、サインイン時のパスワードのリセットをユーザーに許可しません。新しいユーザーおよびパスワードの期限が切れているユーザーは、これを行う場合があります。この操作を許可するには、`iam:ChangePassword` と `iam:CreateLoginProfile` をステートメント

BlockMostAccessUnlessSignedInWithMFA に追加します。ただし、IAM ではこのようなアクセス許可をお勧めしません。

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

このポリシーで行うこと

- -AllowAllUsersToListAccountsステートメントにより、ユーザーはアカウントとそのユーザーに関する基本情報を IAM コンソールで表示できます。この 3 つのアクセス許可は独自のステートメントにある必要があります。これは、アクセス許可が特定のリソース ARN の指定をサポートせず、また指定する必要もなく、その代わりに "Resource" : "*" を指定するためです。
- -AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformationステートメントにより、ユーザーは自分のユーザー、パスワード、アクセスキー、署名証明書、SSH パブリックキー、および MFA 情報を IAM コンソールで管理できます。また、これにより、ユーザーは管理者から初回パスワードの設定を求められたときに初めてサインインを許可されます。リソース ARN は、これらのアクセス許可の使用をユーザー独自の IAM ユーザーエンティティにのみ制限します。
- AllowIndividualUserToViewAndManageTheirOwnMFA ステートメントでは、ユーザーが各自の MFA デバイスを表示または管理できます。このステートメントのリソース ARN は、現在サインインしているユーザーと名前が一致するユーザーや MFA デバイスにのみアクセスを許可することに注意してください。ユーザーは、各自の MFA デバイス以外の MFA デバイスを作成または変更することはできません。
- AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA ステートメントでは、MFA を使用してユーザーがサインインした場合に限り、ユーザーが各自の MFA

デバイスのみを無効化できます。これにより、他者がアクセスキー (MFA デバイスではなく) のみを使用して MFA デバイスを無効化したり、アカウントにアクセスしたりできなくなります。

- -BlockMostAccessUnlessSignedInWithMFAステートメントは、"Deny"および"NotAction"を使用して、IAM およびその他の AWS サービスのいくつかのアクションを除くすべてのアクションへのアクセスを拒否します。ifユーザーは MFA でサインインしていません。このステートメントのロジックの詳細については、「」を参照してください。Deny での NotAction の使用()IAM ユーザーガイド。ユーザーが MFA でサインインしている場合、"Condition" テストは失敗し、最後の "deny" ステートメントは無効になります。ユーザーのアクセス許可は、ユーザー用の他のポリシーやステートメントで決定されます。このステートメントにより、ユーザーが MFA でサインインしていない場合、ユーザーが実行できるのは表示されたアクションのみで、これらのアクションへのアクセスが別のステートメントやポリシーで許可されている場合に限られます。

  ...IfExists バージョンの Bool 演算子により、aws:MultiFactorAuthPresent キーが見つからない場合、条件は必ず true を返します。つまり、アクセスキーなどの長期認証情報を使用して API にアクセスするユーザーは以外の IAM API オペレーションへのアクセスを拒否されます。

4. 完了したら、[ポリシーの確認] を選択します。
5. [確認] ページで、ポリシー名として「**Force_MFA**」と入力します。ポリシーの説明には、次のように入力します。**This policy allows users to manage their own passwords and MFA devices but nothing else unless they authenticate with MFA.**ポリシーの確認概要ポリシーによって付与されたアクセス許可を確認し、[ポリシーの作成[] をクリックして作業内容を保存します。

   新しいポリシーが管理ポリシーの一覧に表示され、アタッチの準備ができます。

ポリシーをユーザーにアタッチするには (コンソール)

1. ナビゲーションペインで [Users] を選択します。
2. 編集するユーザーの名前 (チェックボックスではなく) を選択します。
3. [Permissions] タブで、[Add permissions] を選択します。
4. [Attach existing policies directly] を選択します。
5. 検索ボックスに「**Force**」と入力し、リストの [Force_MFA] の横にあるチェックボックスをオンにします。続いて、[次へ] を選択します。確認。

6. 変更内容を確認し、[Add permissions (アクセス許可の追加)] を選択します。

IAM ユーザーに対して MFA を有効化する

セキュリティを強化するために、グローバルアクセラレーターのリソースを保護するために、すべての IAM ユーザーが多要素認証 (MFA) を設定することをお勧めします。MFA では、さらなるセキュリティが追加されます。ユーザーは、通常のサインイン認証情報に加えて、AWS でサポートされている MFA デバイスから一意の認証情報を提供することを求められるためです。最も安全な AWS MFA デバイスは U2F セキュリティキーです。貴社にすでに U2F デバイスがある場合は、これらのデバイスを AWS 用に有効にしてください。それ以外の場合は、ユーザーごとにデバイスを購入し、ハードウェアが到着するまで待つ必要があります。詳細については、「」を参照してください。U2F セキュリティキーのイネーブル化()IAM ユーザーガイド。

U2F デバイスがまだない場合は、仮想 MFA デバイスを有効にすることで迅速に低コストで開始できます。これには、ソフトウェアアプリケーションを既存の電話や他のモバイルデバイスにインストールする必要があります。このデバイスは、時間同期されるワンタイムパスワードアルゴリズムに基づいて 6 桁の数値コードを生成します。ユーザーが AWS にサインインすると、デバイスからコードを入力するよう求められます。ユーザーに割り当てられた各仮想 MFA デバイスは一意であることが必要です。ユーザーは、別のユーザーの仮想 MFA デバイスからコードを入力して認証することはできません。仮想 MFA デバイスとして使用できるサポートされるアプリケーションのリストについては、「多要素認証」を参照してください。

> **Note**
>
> IAM ユーザーの MFA を設定するには、ユーザーの仮想 MFA デバイスをホストするモバイルデバイスに物理的にアクセスできる必要があります。

IAM ユーザーの仮想 MFA デバイスを有効にするには (コンソール)

1. AWS マネジメントコンソールにサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [Users] を選択します。
3. [ユーザー名] リストから対象の MFA ユーザーの名前を選択します。
4. [Security credentials] タブを選択します。[Assigned MFA device (割り当て済み MFA デバイス)] の横で、[管理] を選択します。

5. [MFA デバイスの管理] ウィザードで、[仮想 MFA デバイス]、[Continue (続行)] の順に選択します。

   IAM は QR コードを含む仮想 MFA デバイスの設定情報を生成して表示します。図は、QR コードに対応していないデバイスでの手動入力に利用できる「シークレット設定キー」を示しています。

6. 仮想 MFA アプリを開きます。

   仮想 MFA デバイスをホストするために使用できるアプリケーションのリストについては、「多要素認証」を参照してください。仮想 MFA アプリが複数のアカウント (複数の仮想 MFA デバイス) をサポートしている場合は、新しいアカウント (新しい仮想 MFA デバイス) を作成するオプションを選択します。

7. MFA アプリが QR コードをサポートしているかどうかを確認してから、次のいずれかを実行します。

   - ウィザードから [Show QR code (QR コードの表示)] を選択し、アプリを使用して QR コードをスキャンします。たとえば、カメラアイコンまたは [Scan code (スキャンコード)] に似たオプションを選択し、デバイスのカメラを使用してコードをスキャンします。
   - [MFA デバイスの管理] ウィザードで [Show secret key (シークレットキーの表示)] を選択し、MFA アプリにシークレットキーを入力します。

   これで仮想 MFA デバイスはワンタイムパスワードの生成を開始します。

8. [MFA デバイスの管理] ウィザードの [MFA Code 1 (MFA コード 1)] ボックスに、現在仮想 MFA デバイスに表示されているワンタイムパスワードを入力します。デバイスが新しいワンタイムパススワードを生成するまで待ちます (最長 30 秒)。生成されたら [MFA Code 2 (MFA コード 2)] ボックスに 2 つ目のワンタイムパススワードを入力します。[Assign MFA (MFA の割り当て)] を選択します。

> **Important**
>
> コードを生成したら、即時にリクエストを送信します。コードを生成した後にリクエストを送信するまで時間がかかりすぎる場合、MFA デバイスはユーザーとは正常に関連付けられますが、その MFA デバイスは同期されません。これは、時刻ベースのワンタイムパスワード (TOTP) の有効期間が短いために起こります。その場合は、デバイスの再同期ができます。詳細については、「」を参照してください。仮想デバイスとハードウェア MFA デバイスの再同期()IAM ユーザーガイド。

これで仮想 MFA デバイスを AWS で使用できます。

AWS Global Accelerator でのセキュアな VPC 接続

AWS Global Accelerator で内部Application Load Balancer または Amazon EC2 インスタンスエンドポイントを追加する場合、プライベートサブネットでターゲットを設定することで、インターネットトラフィックが仮想プライベートクラウド (VPC) 内のエンドポイントに直接送受信されるようにします。ロードバランサーまたは EC2 インスタンスを含む VPC には、インターネットゲートウェイをアタッチして、VPC がインターネットトラフィックを受け入れることを示します。ただし、ロードバランサーや EC2 インスタンスにはパブリック IP アドレスは必要ありません。また、サブネットに関連付けられたインターネットゲートウェイルートも必要ありません。

これは、インターネットトラフィックが VPC 内のインスタンスまたはロードバランサーに流れるためにパブリック IP アドレスとインターネットゲートウェイルートの両方が必要となる一般的なインターネットゲートウェイユースケースとは異なります。ターゲットのエラスティックネットワークインターフェイスがパブリックサブネット (つまり、インターネットゲートウェイルートを持つサブネット) に存在する場合でも、グローバルアクセラレータをインターネットトラフィックに使用すると、グローバルアクセラレータは、通常のインターネットルートと、グローバルアクセラレータは、インターネットゲートウェイではなく、グローバルアクセラレータを介して戻ります。

> **Note**
>
> パブリック IP アドレスと Amazon EC2 インスタンスのパブリックサブネットの使用は一般的ではありませんが、それらを使用して設定することは可能です。セキュリティグループは、Global Accelerator からのトラフィックや、インスタンス ENI に割り当てられたパブリック IP アドレスまたは Elastic IP アドレスなど、インスタンスに到着するすべてのトラフィックに適用されます。プライベートサブネットを使用して、トラフィックがGlobal Acceleratorによってのみ配信されるようにします。

ネットワーク境界の問題を検討し、インターネットアクセス管理に関連する IAM 権限を設定するときは、この情報を念頭に置いてください。VPC へのインターネットアクセスの制御方法については、この「」を参照してください。サービスコントロールポリシーの例。

AWS Global Accelerator でのログ記録

モニタリングは、Global Accelerator および AWS ソリューションの可用性とパフォーマンスを維持する上で重要な役割を果たします。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。AWS には、グローバルアクセラレーターのリソースとアクティビティをモニタリングして、起こり得るインシデントに対応するためのツールがいくつか用意されています。

AWS Global Accelerator

サーバフローログは、アクセラレータを経由してエンドポイントに流れるトラフィックに関する詳細なレコードを提供します。サーバーフローログは、多くのアプリケーションに役立ちます。たとえば、フローログ情報は、セキュリティとアクセスの監査に役立ちます。詳細については、「AWS Global Accelerator のフロー」を参照してください。

Amazon CloudWatch メトリックスとアラーム

CloudWatch を使用して、AWS で実行される AWS リソースやアプリケーションをリアルタイムでモニタリングできます。CloudWatch はメトリックスを収集し、追跡します。メトリックスは、時間の経過とともに測定する変数です。特定のメトリクスを監視し、メトリクスが一定期間一定のしきい値を超過したときに通知を送信したり、モニタリングしているリソースを自動的に変更したりするアラームを作成できます。詳細については、「AWS Global Accelerator での Amazon CloudWatch の使用」を参照してください。

AWS CloudTrail ログ

CloudTrail は、グローバルアクセラレータのユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供します。CloudTrail は、グローバルアクセラレータコンソールからのコールや、グローバルアクセラレータ API へのコード呼び出しを含む、グローバルアクセラレータのすべての API コールをイベントとしてキャプチャします。詳細については、「AWS CloudTrail を使用した AWS Global Accelerator API コールのログ記録」を参照してください。

AWS Global Accelerator のコンプライアン

サードパーティーの監査者は、さまざまな AWS コンプライアンスプログラムの一環として AWS Global Accelerator のセキュリティとコンプライアンスを評価します。このプログラムには、SOC、PCI、HIPAA、GDPR、ISO、ENS High が含まれます。

グローバルアクセラレータを含む AWS のサービスのリストについては、「」を参照してください。コンプライアンスプログラムによる AWS 対象範囲内のサービス。一般的な情報については、「AWS コンプライアンスプログラム」を参照してください。

サードパーティーの監査報告書は、AWS Artifact を使用してダウンロードすることができます。詳細については、「」を参照してください。AWS Artifact のレポートのダウンロード。

Global Acceleratorを使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性や貴社のコンプライアンス目標、および適用される法律および規制によって決定されます。AWS では、コンプライアンスに役立つ以下のリソースを提供しています。

- セキュリティおよびコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境を AWS でデプロイするための手順を説明します。
- HIPAA のセキュリティとコンプライアンスに関するホワイトペーパーを作成する – このホワイトペーパーでは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法について説明します。
- AWS コンプライアンスのリソース – このワークブックおよびガイドのコレクションは、お客様の業界や場所に適用される場合があります。
- ルールでのリソースの評価()AWS Config 開発者ガイド— AWS Config サービスは、自社プラクティス、業界ガイドライン、および規制に対するリソースの設定の準拠状態を評価します。
- AWS セキュリティハブ – この AWS サービスでは、AWS 内のセキュリティ状態を包括的に表示しており、セキュリティ業界の標準およびベストプラクティスへの準拠を確認するのに役立ちます。

AWS Global Accelerator の復元性

AWS のグローバルインフラストラクチャは AWS リージョンとアベイラビリティーゾーンを中心として構築されます。AWS リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立· 隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、および拡張性が優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

AWS グローバルインフラストラクチャのサポートに加えて、Global Accelerator には、データの耐障害性のサポートに役立つ次の機能があります。

- ネットワークゾーンは、一意の IP サブネットからアクセラレータの静的 IP アドレスをサービスを提供します。AWS アベイラビリティーゾーンと同様に、ネットワークゾーンは、独自の物理インフラストラクチャセットを備えた独立したユニットです。アクセラレータを構成すると、グローバルアクセラレータは 2 つの IPv4 アドレスを割り当てます。特定のクライアントネットワークによる IP アドレスブロックまたはネットワークの中断が原因で、ネットワークゾーンの 1 つの IP アドレスが使用できなくなった場合、クライアントアプリケーションは、別の分離されたネットワークゾーンから正常な静的 IP アドレスを再試行できます。
- グローバルアクセラレータは、すべてのエンドポイントの正常性を継続的にモニタリングします。アクティブなエンドポイントが正常でないと判断すると、Global Accelerator は、使用可能な別のエンドポイントへのトラフィックの転送を即座に開始します。これにより、AWS 上のアプリケーションの高可用性アーキテクチャを作成できます。

AWS Global Acceleratorer

マネージド型サービスである AWS Global Accelerator は、に記載されている AWS グローバルネットワークのセキュリティ手順で保護されています。Amazon Web Services: セキュリティプロセスの概要ホワイトペーパー.

AWS が公開した API コールを使用して、ネットワーク経由で Global Accelerator にアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。また、リクエストは、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

AWS Global Accelerator のクォータ

AWS アカウントには、AWS Global Accelerator に関連する、特定のクォータ (制限とも呼ばれます) があります。

Service Quotas コンソールには、Global Accelerator のクォータに関する情報が表示されます。デフォルトのクォータの表示に加えて、Service Quotas コンソールを使用して要求クォータの増加調整可能なクォータ用。グローバルアクセラレータのクォータ増加を要求する場合は、米国東部 (バージニア北部) にいる必要があります。

トピック

一般的なクォータ

グローバルアクセラレータの全体的なクォータを次に示します。

エンティティ	Quota
AWS アカウントあたりのアクセラレーターの数	20 以下の操作を実行できます。クォータ引き上げのリクエスト。
アクセラレーターのリスナー	10 以下の操作を実行できます。クォータ引き上げのリクエスト。
リスナーあたりのポート範囲	10
エンドポイントグループごとのポートオーバーライド	10 以下の操作を実行できます。クォータ引き上げのリクエスト。

エンドポイントグループあたりのエンドポイントのクォータ

エンドポイントグループのエンドポイント数に適用されるグローバルアクセラレータクォータを次に示します。

エンティティ	説明	Quota
複数のエンドポイントタイプを持つエンドポイントグループ	複数のエンドポイントタイプを含むエンドポイントグループ内のエンドポイントの数。	10
アプリケーションロードバランサーのみを使用したエンドポイントグループ	アプリケーションロードバランサーのエンドポイントのみを含むエンドポイントグループ内のApplication Load Balancer の数。	10
ネットワークロードバランサーのみを使用したエンドポイントグループ	ネットワークロードバランサーのエンドポイントのみを含むエンドポイントグループ内のNetwork Load Balancer の数。	10
Amazon EC2 インスタンスのみを持つエンドポイントグループ	EC2 インスタンスのエンドポイントのみを含むエンドポイントグループの EC2 インスタンスの数。	10 以下の操作を実行できます。クォータ引き上げのリクエスト。
Elastic IP アドレスのみを持つエンドポイントグループ	Elastic IP アドレスのエンドポイントのみを含むエンドポイントグループ内の Elastic IP アドレスの数。	10 以下の操作を実行できます。クォータ引き上げのリクエスト。
Amazon Virtual Private Cloud サブネットのみを持つエンドポイントグループ	サブネットエンドポイントのみを含むエンドポイントグループ内の Amazon VPC サブネットの数。	10 以下の操作を実行できます。クォータ引き上げのリクエスト。

関連するクォータ

Global Accelerator には、クォータに加えて、アクセラレーターのエンドポイントとして使用するリソースに適用されるクォータがあります。詳細については、以下を参照してください。

- Elastic IP アドレスのクォータ()Amazon EC2 ユーザーガイド。
- Amazon EC2 サービスクォータについて()Amazon EC2 ユーザーガイド。
- Network Load Balancer のクォータ()Network Load Balancer のユーザーガイド。
- Application Load Balancer のクォータ()Application Load Balancer のユーザーガイド。
- Amazon VPC クォータ()Amazon VPC ユーザーガイド。

AWS Global Accelerator

ここに列挙されている情報とリソースは Global Accelerator について理解を深めるのに役立ちます。

トピック

- AWS Global Accelerator
- サポート情報
- アマゾン ウェブ サービスブログからのヒント

AWS Global Accelerator

このサービスを利用する際に役立つ関連リソースは以下の通りです。

- AWS Global Accelerator API リファレンスAPI アクション、パラメータ、データ型について詳しく説明します。サービスから返されるエラーのリストも含まれています。
- AWS Global Accelerator— Global Accelerator に関する情報の基本となるウェブページで、このサービスの特徴や料金表も掲載されています。
- 利用規約当社の著作権、商標、お客様のアカウント、ライセンス、サイトへのアクセス、およびその他のトピックに関する詳細情報です。

サポート情報

グローバルアクセラレータSupport は、いくつかの形式で提供されています。

- ディスカッションフォーラム開発者が Global Accelerator に関する技術的な質問についてディスカッションできる、コミュニティベースのフォーラムです。
- AWS サポートセンター – このサイトでは、お客様の最近のサポートケース、AWS Trusted Advisor の助言とヘルスチェックの結果に関する情報がひとつにまとめられていて、フォーラム、技術上のよくある質問、サービスヘルスダッシュボード、および AWS サポートプランに関する情報へのリンクも掲載されています。
- AWS プレミアムサポート情報 – 1 対 1 での迅速な対応を行うサポートチャネルである AWS プレミアムサポートに関する情報のメインウェブページです。プレミアムサポートは、AWS インフラストラクチャサービスでのアプリケーションの構築および実行を支援します。

- お問い合わせ – 請求やアカウントに関するお問い合わせ用のリンクです。技術的な質問の場合は、上記のディスカッションフォーラムまたはサポートリンクをご利用ください。

アマゾン ウェブ サービスブログからのヒント

AWS ブログには、AWS サービスの利用に役立つ投稿が数多くあります。たとえば、Global Accelerator に関する次のブログ投稿を参照してください。

- 可用性とパフォーマンスのための AWS Global Accelerator
- AWS Global Accelerator
- Amazon アテネと Amazon QuickSight を使用した AWS Global Accelerator フローログの分析と視覚化

AWS Global Accelerator ブログの詳細なリストについては、「」を参照してください。AWS Global AcceleratorAWS ブログ投稿の [ネットワークとコンテンツ配信] カテゴリにあります。

ドキュメント履歴

以下の表は、AWS Global Accelerator の重要な変更点を基にしたものです。

- API バージョン: 最新
- ドキュメントの最終更新: 2020 年 12 月 9 日

変更	説明	日付
グローバルアクセラレータの既存のサービスリンクロールへの更新	グローバルアクセラレータは、新しいアクセス許可`ec2:DescribeRegions` を使用して、グローバルアクセラレータが AWS リージョン情報を取得して、エラーの診断に役立てることができます。詳細については、「https://docs.aws.amazon.com/global-accelerator/latest/dg/security-iam-awsmanpol-updates.html」を参照してください。	2021 年 5 月 7 日
カスタムルーティングアクセラレータを追加	グローバルアクセラレータは、新しいタイプのアクセラレータカスタムルーティングアクセラレータを導入しました。カスタムルーティングアクセラレータは、カスタムアプリケーションロジックを使用して、1 人以上のユーザーを多数の宛先とポートに誘導し、グローバルアクセラレータのパフォーマンス上の利点を得たい場合に適しています。詳細については、	2020 年 12 月 9 日

変更	説明	日付
	「https://docs.aws.amazon.com/global-accelerator/latest/dg/work-with-custom-routing-accelerators.html」を参照してください。	
ポート上書きサポートを追加	Global Accelerator では、エンドポイントへのトラフィックのルーティングに使用されるリスナーポートのオーバーライドがサポートされ、エンドポイントの特定のポートにトラフィックを再ルーティングできるようになりました。詳細については、「https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-port-override.html」を参照してください。	2020 年 10 月 21 日
2 つの新しいリージョンが追加されました。	Global Accelerator がアフリカ (ケープタウン) および EU (ミラノ) をサポートするようになりました。詳細については、「https://docs.aws.amazon.com/global-accelerator/latest/dg/preserve-client-ip-address.regions.html」を参照してください。	2020 年 5 月 20 日

変更	説明	日付
タグ付けおよび BYOIP	このリリースでは、アクセラレーターにタグを追加し、AWS Global Accelerator レーター（BYOIP）に独自の IP アドレスを持ち込むためのサポートが追加されました。詳細については、「https://docs.aws.amazon.com/global-accelerator/latest/dg/tagging-in-global-accelerator.html」および「https://docs.aws.amazon.com/global-accelerator/latest/dg/using-byoip.html」を参照してください。	2020 年 2 月 27 日
セキュリティを更新しました。	コンプライアンス、耐障害性、インフラストラクチャのセキュリティに関するコンテンツを追加しました。詳細については、「https://docs.aws.amazon.com/global-accelerator/latest/dg/security.html」を参照してください。	2019 年 12 月 20 日

変更	説明	日付
EC2 インスタンスとデフォルトの DNS 名のSupport	AWS Global Accelerator では、サポート対象の AWS リージョンでの EC2 インスタンスの追加がサポートされるようになりました。さらに、グローバルアクセラレータは、アクセラレータの静的 IP アドレスにマップされる既定の DNS 名を作成します。詳細については、「https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html」および「https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.html#about-accelerators.dns-addressing」を参照してください。	2019 年 10 月 29 日
アプリケーションロードバランサのクライアント IP アドレスの保持	サポート対象の AWS リージョンで、アプリケーションロードバランサーのクライアント IP アドレスを AWS Global Accelerator で保持するように選択できるようになりました。詳細については、「https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html」を参照してください。	2019 年 8 月 28 日

変更	説明	日付
AWS Global Accelerator サービスのリリース	AWS Global Accelerator 開発者ガイドには、ネットワーク層トラフィックマネージャというアクセラレータの設定および使用に関する情報が含まれています。このアクセラレータは、グローバルオーディエンスを持つインターネットアプリケーションの可用性とパフォーマンスを向上させます。	2018 年 11 月 26 日

AWS の用語集

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

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。