aws

開発者ガイド

AWS Global Accelerator

AWS Global Accelerator: 開発者ガイド

Table of Contents

AWS Global Accelerator とは 1
コンポーネント 2
AWS リージョン 5
仕組み 7
仕組みの概要 9
アクセラレーターのタイプ 10
アイドルタイムアウト 11
グローバル静的 IP IP アドレス 11
ヘルスチェック 13
トラフィックダイヤルとエンドポイントの重み 13
ICMP レスポンスメッセージ 15
IP アドレスの範囲 16
ユースケース 16
速度比較ツール 18
開始方法 19
タグ付け 20
Global Accelerator でのタグ付けへのサポート 21
Global Accelerator でのタグの追加、編集、削除 21
料金 22
使用開始方法 23
標準アクセラレーターを作成する 24
開始する前に 24
ステップ 1: 標準アクセラレーターを作成する 25
ステップ 2: リスナーを追加する 25
ステップ 3: エンドポイントグループを追加する 26
ステップ 4: エンドポイントを追加する 27
ステップ 5: アクセラレーターをテストする 27
ステップ 6 (選択可能): アクセラレーターを削除する 28
カスタムルーティングアクセラレーターを作成する 29
開始する前に 29
ステップ 1: カスタムルーティングアクセラレーターを作成する 30
ステップ 2: リスナーを追加する 30
ステップ 3: エンドポイントグループを追加する 31
ステップ 4: VPC サブネットエンドポイントを追加する 32

ステップ 5 (選択可能): アクセラレーターを削除する 33
API アクション 34
標準アクセラレーターの使用 39
標準アクセラレーター 40
アクセラレーターを作成する 41
アクセラレーターを更新する 42
アクセラレーターを削除する 43
アクセラレーターを表示する 44
ロードバランサーの作成中に Global Accelerator を統合する 44
グローバルアドレスとリージョンアドレスを比較する 46
標準アクセラレーターのリスナー 47
リスナーを追加する 47
リスナーを編集する 48
リスナーを削除する 49
クライアントアフィニティの仕組み 49
標準アクセラレーターのエンドポイントグループ 50
エンドポイントグループを追加する 51
エンドポイントグループを編集する 52
エンドポイントグループを削除する 53
トラフィックダイヤルでトラフィックフローを調整する 53
リスナーポートを上書きする 55
ヘルスチェックアクセスを確保する 57
標準アクセラレーターのエンドポイント 59
エンドポイントの要件 61
エンドポイントを追加する 63
エンドポイントを編集する 64
エンドポイントを削除する 65
エンドポイントの重みの仕組み 66
異常なエンドポイントのフェイルオーバー 67
TCP 接続時間の遅延を回避する 68
カスタムルーティングアクセラレーターの使用 71
カスタムルーティングアクセラレーターの仕組み 72
カスタムルーティングの例 74
カスタムルーティングガイドライン 77
カスタムルーティングアクセラレーター。 80
カスタムルーティングアクセラレーターを作成する 81

カスタムルーティングアクセラレーターを編集する 81
カスタムルーティングアクセラレーターを表示する 82
カスタムルーティングアクセラレーターを削除する 82
カスタムルーティングアクセラレーターのリスナー 83
リスナーを追加する 84
リスナーを編集する 85
リスナーを削除する 86
カスタムルーティングアクセラレーターのエンドポイントグループ 86
エンドポイントグループを追加する 87
エンドポイントグループを編集する 88
エンドポイントグループを削除する 89
VPC サブネットエンドポイント 89
Amazon VPC サブネットエンドポイントを追加する 91
Amazon VPC サブネットエンドポイントを編集する 92
Amazon VPC サブネットエンドポイントを削除する 93
クロスアカウントアクセスの設定 95
クロスアカウントの仕組み 96
クロスアカウントアタッチメントを操作する 96
クロスアカウントアタッチメントを作成する 97
クロスアカウントアタッチメントを編集する 98
クロスアカウントアタッチメントを削除する 99
クロスアカウントリソースを操作する 99
クロスアカウント BYOIP アドレスを追加する 100
クロスアカウントエンドポイントを追加する 101
クロスアカウントエンドポイントを削除する 102
クロスアカウントリソースを特定する 102
所有者: クロスアカウントリソースを特定する 103
プリンシパル: クロスアカウントリソースを特定する 103
責任と権限 105
リソース所有者のアクセス許可 105
プリンシパルのアクセス許可 106
費用請求 106
クォータ 106
DNS アドレス指定とカスタムドメイン 108
DNS アドレス指定のサポート 108
カスタムドメイントラフィックをアクセラレーターにルーティングする 109

自分の IP アドレスを使用する ... 110
要件 ... 111
IP アドレス範囲の承認 ... 112
アドレス範囲のプロビジョニング ... 115
アドレス範囲をアドバタイズする ... 116
アドレス範囲のプロビジョニング解除 ... 118
アクセラレーターで BYOIP アドレスを使用する ... 118
IP アドレスを更新する ... 119
クライアント IP アドレスを保存する ... 122
ガイドラインと制限事項 ... 123
クライアント IP アドレスの保存に関する要件 ... 125
クライアント IP アドレスが保存される方法 ... 127
クライアント IP アドレスの保存の利点 ... 128
ENI とセキュリティのベストプラクティス ... 129
移行エンドポイント ... 132
エンドポイントの移行 ... 132
ログ記録とモニタリング ... 135
CloudWatch のモニタリング ... 136
Global Accelerator メトリクス ... 137
アクセラレーターのメトリクスディメンション ... 147
Global Accelerator TCP リセット問題のトラブルシューティング ... 149
Global Accelerator メトリクスの統計 ... 150
アクセラレーターの CloudWatch メトリクスを表示する ... 151
フローログ ... 153
フローログの有効化 ... 154
フローログレコードの処理 ... 154
Amazon S3 への発行 ... 155
ログファイルのタイミング ... 159
フローログレコードの構文 ... 160
CloudTrail ロギング ... 163
CloudTrail の Global Accelerator 情報 ... 163
イベント履歴での Global Accelerator イベントの表示 ... 164
Global Accelerator ログファイルエントリの概要 ... 164
セキュリティ ... 174
ID とアクセス管理 ... 175
対象者 ... 175

アイデンティティによる認証 176
ポリシーを使用したアクセス権の管理 180
Global Accelerator が IAM と連携する方法 182
アイデンティティベースポリシーの例 189
サービスリンクロール 194
AWS マネージドポリシー 197
タグベースのポリシー 201
トラブルシューティング 202
安全な VPC 接続 204
ログ記録とモニタリング 205
コンプライアンス検証 206
レジリエンス 207
インフラストラクチャセキュリティ 208
クォータ 210
一般的なクォータ 210
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 211
関連クォータ 212
関連情報 214
AWS Global Accelerator の API Reference と製品情報 214
サポート情報 214
AWS ブログウェブサイトからのヒント 215
ドキュメント履歴 216

AWS Global Accelerator とは

AWS Global Accelerator では、アクセラレーターを作成して、ローカルユーザーとグローバルユーザーのアプリケーションのパフォーマンスを向上させることができます。選択したアクセラレーターのタイプに応じて、追加の利点が得られます。

- 標準アクセラレーターを使用すると、世界中の視聴者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させることができます。標準アクセラレーターを使用すると、Global Accelerator は AWS グローバルネットワーク経由のトラフィックを、最も近いリージョンのエンドポイントからクライアントに送信します。
- カスタムルーティングアクセラレーターを使用すると、1 人以上のユーザーを多くの送信先間で特定の送信先にマッピングできます。

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。Global Accelerator やその他のサービスが特定の AWS リージョン で現在サポートされているかどうかを確認するには、「AWS リージョンサービスリスト」を参照してください。

デフォルトでは、Global Accelerator はアクセラレーターに関連付ける静的 IP アドレスを提供します。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。IPv4 の場合、Global Accelerator は 2 つの静的 IPv4 アドレスを提供します。デュアルスタックの場合、Global Accelerator は 2 つの IPv4 アドレスと 2 つの IPv6 アドレス、合計 4 つのグローバルの静的 IP アドレスを提供します。IPv4 の場合、Global Accelerator が提供するアドレスを使用する代わりに、Global Accelerator (BYOIP) に持ち込む独自の IP アドレス範囲から、これらのエントリポイントを IPv4 アドレスに設定できます。

> **Important**
>
> 静的 IP アドレスは、アクセラレーターを無効にし、トラフィックを受け入れたりルーティングしたりしなくなった場合でも、存在する限り、アクセラレーターに割り当てられたままになります。ただし、アクセラレーターを削除すると、そのアクセラレーターに割り当てられた静的 IP アドレスが失われるため、それ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 でのタグベースのアクセス許可などの IAM ポリシーを使用して、アクセラレーター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、「Global Accelerator を使用した ABAC」を参照してください。

標準アクセラレーターの場合、Global Accelerator は AWS グローバルネットワークを使用して、設定したヘルス、クライアントの場所、ポリシーに基づいてトラフィックを最適なリージョンエンドポイントにルーティングするため、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ーのエンドポイントは、Network Load Balancer、Application Load Balancer、Amazon EC2 インスタンス、AWS リージョン または 1 つ以上のリージョンにある Elastic IP アドレスのいずれかも可能です。

このサービスは、ヘルスや設定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ルーティングされるようにします。Global Accelerator は、サポートされているエンドポイントの ARC トラフィックリダイレクトも従い、ゾーンシフトまたはゾーンオートシフトにより、障害が発生する可能性のあるアベイラビリティーゾーンからのトラフィックを再ルーティングします。詳細については、「Amazon Application Recovery Controller (ARC) のマルチ AZ リカバリ」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は、Amazon VPC (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。

内容

- AWS Global Accelerator コンポーネント
- AWS Global Accelerator のための AWS リージョン の可用性
- AWS Global Accelerator の働き
- Global Accelerator エッジサーバーの場所と IP アドレス範囲
- AWS Global Accelerator ユースケースについて
- AWS Global Accelerator 速度比較ツール
- AWS Global Accelerator の開始方法
- AWS Global Accelerator でのタグ付け
- AWS Global Accelerator の料金

AWS Global Accelerator コンポーネント

AWS Global Accelerator のコンポーネントは以下のとおりです。

静的 IP アドレス

デフォルトでは、Global Accelerator はアクセラレーターに関連付ける静的 IP アドレスを提供します。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。IPv4 の場合、Global Accelerator は 2 つの静的 IPv4 アドレスを提供します。デュアルスタックの場合、Global Accelerator は 2 つの IPv4 アドレスと 2 つの IPv6 アドレス、合計 4 つのグローバルの静的 IP アドレスを提供します。Global Accelerator (IPv4 のみ) で使用する独自の IP アドレス範囲を AWS (BYOIP) にする場合は、代わりに、アクセラレータで使用する IPv4 アドレスを独自のプールから割り当てることができます。詳細については、「Global Accelerator の Bring your own IP (BYOIP)」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 の標準アクセラレーターにそれらを簡単に追加できます。これにより、Global Accelerator 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。Global Accelerator の静的 IP アドレスを使用して API Gateway にアクセスする場合は、次のブログ記事を参照してください:「Accessing an Amazon API Gateway via static IP addresses provided by AWS Global Accelerator」。

静的 IP アドレスは、アクセラレーターを無効にし、トラフィックを受け入れたりルーティングしたりしなくなった場合でも、存在する限り、アクセラレーターに割り当てられたままになります。ただし、アクセラレーターを削除すると、そのアクセラレーターに割り当てられた静的 IP アドレスが失われるため、それ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 では、タグベースのアクセス許可などの IAM ポリシーを使用して、アクセラレーター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、「Global Accelerator を使用した ABAC」を参照してください。

アクセラレーター

アクセラレーターは、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エンドポイントに送信します。各アクセラレーターには 1 つ以上のリスナーが含まれます。

アクセラレーターには 2 種類あります。

- 標準アクセラレーターは、ユーザーの場所、エンドポイントのヘルス、設定した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 エンドポイントに送信します。これは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。エンドポイントには、Network Load Balancer、Application Load Balancer、Amazon EC2 インスタンス、または Elastic IP アドレスを使用できます。

- カスタムルーティングアクセラレーターを使用すると、一部のユースケースで必要とされるように、複数のユーザーをアクセラレーターの背後にある特定の EC2 送信先に決定的にルーティングできます。これを行うには、Global Accelerator が送信先にマッピングしたアクセラレーターの一意の IP アドレスとポートをユーザーに指示します。カスタムルーティングアクセラレーターは、IP アドレスのデュアルスタックをサポートしていないことに注意してください。

詳細については、「アクセラレーターのタイプ」を参照してください。

[DNS 名]

Global Accelerator は、Global Accelerator が割り当てる静的 IP アドレス、または独自の IP アドレス範囲から選択する静的 IP アドレスを指す a1234567890abcdef.awsglobalaccelerator.com に似たデフォルトのドメインネームシステム (DNS) 名を各アクセラレーターに割り当てます。デュアルスタックアクセラレーターを使用している場合、Global Accelerator はデュアルスタックアクセラレーターの 4 つの静的 IP アドレスを指す a1234567890abcdef.dualstack.awsglobalaccelerator.com と同様のデュアルスタック DNS 名も割り当てます。

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 レコードを設定したりできます。詳細については、「AWS Global Accelerator での DNS アドレス指定のサポート」を参照してください。

ネットワークゾーン

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持つ分離されたユニットです。アクセラレーターを作成すると、Global Accelerator は一連の静的 IP アドレスを提供します。1 つのアクセラレーターに IPv4 IP アドレスタイプが 2 つ、またはデュアルスタックアクセラレーターに IPv4 つの静的 IP アドレス (2 つの IPv4 アドレスと 2 つの IPv6 アドレス) です。Global Accelerator は、各 IP アドレスファミリーの一意の IP サブネットから、ネットワークゾーンごとに 1 つの静的 IP アドレスを提供します。特定のクライアントネットワークによる IP アドレスの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他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、設定したポート (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 Global Accelerator へのインバウンド接続を処理します。リスナーは、TCP、UDP、または TCP プロトコルと UDP プロトコルの両方で設定できます。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、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。トラフィックを分散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ーを使用すると、トラフィックは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ーを使用すると、トラフィックダイヤルと呼ばれる設定を調整することで、エンドポイントグループに転送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を使用すると、パフォーマンステストやブルー/グリーンデプロイテストを簡単に実行できます。例えば、さまざまな AWS リージョン にわたる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、Global Accelerator がトラフィックを送信するリソースです。

標準アクセラレーターのエンドポイントは、Network Load Balancer、Application Load Balancer、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、内部またはインターネット接続を問いません。標準アクセラレーターのトラフィックは、エンドポイントのヘルスと、エンドポイントの重みなど、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実行する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ーのエンドポイントは、トラフィックの送信先である 1 つ以上の Amazon EC2 インスタンスを持つ Amazon VPC (VPC) サブネットです。

AWS Global Accelerator のための AWS リージョン の可用性

AWS Global Accelerator のリージョン別のサポートとサービスエンドポイントの詳細情報については、「Amazon Web Services General Reference」の「AWS Global Accelerator endpoints and quotas」を参照してください。

> **Note**
>
> AWS Global Accelerator はグローバルサービスです。ただし、リージョン別の Global Accelerator AWS CLI コマンドでは米国西部 (オレゴン) リージョンを指定 (つまり、--

region us-west-2 パラメータを指定) します。つまり、アクセラレーターのようなリソースを作成する際のことです。

Global Accelerator は現在、次の AWS リージョンで利用できます。アベイラビリティーゾーン (AZ) の例外が表示されます。

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
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 (ハイデラバード)	ap-south-2
アジアパシフィック (ジャカルタ)	ap-southeast-3
アジアパシフィック (メルボルン)	ap-southeast-4
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)

リージョン名	リージョン
カナダ西部 (カルガリー)	ca-west-1
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
欧州 (ミラノ)	eu-south-1
欧州 (パリ)	eu-west-3
欧州 (スペイン)	eu-south-2
欧州 (ストックホルム)	eu-north-1
欧州 (チューリッヒ)	eu-central-2
イスラエル (テルアビブ)	il-central-1
中東 (バーレーン)	me-south-1
中東 (アラブ首長国連邦)	me-central-1
南米 (サンパウロ)	sa-east-1

AWS Global Accelerator の働き

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。アクセラレーターを Global Accelerator で設定すると、静的 IP アドレスが 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られます。標準アクセラレーターの場合、エンドポイントは Network Load Balancer、Application Load Balancer、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ーの場合、エンドポイントは、1 つ以上の EC2 インスタンスを持つ Amazon VPC (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受信トラフィックを受け入れます。

> **Note**
>
> Global Accelerator で使用する独自の IP アドレス範囲を AWS (BYOIP) にする場合は、代わりに、アクセラレーターで使用する静的 IP アドレスを独自のプールから割り当てることができます。詳細については、「Global Accelerator の Bring your own IP (BYOIP)」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ー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ーの場合、トラフィックは、ユーザーの場所、AWS エンドポイントのヘルス、設定した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ーの場合、各クライアントは、指定した外部静的 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 インスタンスとポートにルーティングされます。

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

- エンドポイントの重みを上書きする： 特定の限られたシナリオでは、Global Accelerator は設定したエンドポイントの重みを上書きし、可用性を確保します。Global Accelerator が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ロードバランシングする場合、特定の状況では、クライアントトラフィックの可用性を維持するか、エンドポイントの重みに従うかを選択する必要があります。例えば、クライアントの IP アドレスが保存されているアクセラレーターでは、接続の衝突を避けるために Global Accelerator がエンドポイントの重み設定を上書きする必要があります。
- セキュリティグループとルール： アクセラレーターを追加すると、すでに設定したセキュリティグループと AWS WAF ルールは、アクセラレーターを追加する前と同じように動作し続けます。
- IP フラグメント化： インターネットやその他の大規模なネットワーク経由で送信されるときに、標準のイーサネットフレーム (1500 バイト以上) に収まるほど大きすぎる IP パケットは、中間ルーターによってフラグメント化され、個別に送信されます。クライアントとエンドポイントは、より小さな最大セグメントサイズ (MSS) を自動的にネゴシエートするため、TCP プロトコルには IP フラグメント化は必要ありません。ただし、UDP プロトコルには IP フラグメント化が必要です。パケットがフラグメント化されると、Global Accelerator は UDP フラグメントを設定された

エンドポイントに転送し、元の IP パケットを再アセンブルします。Global Accelerator は、AWS ネットワークでサポートされていないため、TCP フラグメントをエッジにドロップします。

トピック

- AWS Global Accelerator の仕組みの概要
- アクセラレーターのタイプ
- AWS Global Accelerator でのアイドルタイムアウトについて
- AWS Global Accelerator の静的 IP アドレスの使用
- Global Accelerator がヘルスチェックを使用する方法
- トラフィックダイヤルとエンドポイントの重みを使用してトラフィックフローを管理する方法
- ICMP レスポンスメッセージと AWS Global Accelerator

AWS Global Accelerator の仕組みの概要

トラフィックは、十分にモニタリングされ、輻輳のない冗長な AWS グローバルネットワーク経由でエンドポイントに移動します。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経由でルーティングされるようにします。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新しい TCP 接続を確立します。これにより、クライアントは応答時間が短縮され (レイテンシーが短縮) 、スループットが向上します。

Global Accelerator は、カスタムルーティングアクセラレーター上のエンドポイントのクライアント IP アドレスを常に保存します。標準アクセラレーターでは、一部のエンドポイントタイプのクライアント IP アドレスを保存してアクセスするオプションがあります。クライアント IP アドレスの保存サポートなど、Global Accelerator がサポートするエンドポイントタイプと設定の詳細については、アクセラレーターエンドポイントとして追加するリソースの要件 を参照してください。

標準アクセラレーターを使用すると、Global Accelerator 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、アクティブなエンドポイントが異常であると判断した場合、新しい接続のトラフィックを別の利用可能なエンドポイントに瞬時に送信し始めます。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。ヘルスチェックはカスタムルーティングアクセラレーターでは使用されず、トラフィックをルーティングする送信先を指定するためフェイルオーバーも行われません。

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ーでエンドポイントの重みを設定できます。さらに、Global Accelerator のトラフィックダイヤルを使用して、パフォーマン

ステストやスタックアップグレードなど、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減 (ダイヤルアップ) できます。

アクセラレーターのタイプ

AWS Global Accelerator で使用できるアクセラレーターには、標準アクセラレーターとカスタムルーティングアクセラレーターの 2 種類があります。どちらのタイプのアクセラレーターも、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ーを使用することで、Application Load Balancer、Network Load Balancer、または Amazon EC2 インスタンス上で稼働す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ーを使用すると、Global Accelerator は、地理的近接性とエンドポイントのヘルスに基づいて、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コントロールに基づいて、エンドポイント間でクライアントトラフィックをシフトすることもできます。これは、ブルー/グリーンデプロイ、A/B テスト、マルチリージョンデプロイなど、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 ユースケースについて を参照してください。

詳細については、「AWS Global Accelerator での標準アクセラレーターの使用」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ーは、独自のアプリケーションロジックを使用して、多数の送信先とポートの中から特定の送信先とポートに 1 人または複数のユーザーを送信したい場合に適しています。この場合でも、Global Accelerator のパフォーマンス向上の利点を得ることができます。1 つの例は、音声、ビデオ、メッセージングセッションを開始するために、特定のメディアサーバーに複数の発信者を割り当てる VoIP アプリケーションです。もう 1 つの例は、地理的位置、プレイヤースキル、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です。

> **Note**
>
> カスタムルーティングアクセラレーターは、IPv4 IP アドレスタイプのみをサポートします。

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ーの使用」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ーの 1 つを作成して、顧客のトラフィックを加速します。

AWS Global Accelerator でのアイドルタイムアウトについて

AWS Global Accelerator は、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。アイドルタイムアウト期間はカスタマイズできません。

接続のタイムアウトを防ぐために、Global Accelerator では、TCP 接続のタイムアウトウィンドウ内に、受信と送信の方向に少なくとも 1 バイトのデータを含むパケットを送信する必要があります。TCP キープアライブパケットを使用してオープン接続を維持することはできません。

ネットワーク接続のグローバルアクセラレーターのアイドルタイムアウトは、接続のタイプ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、エンドポイントが異常とマークされている場合やアクセラレーターから削除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、確立された接続のトラフィックをエンドポイントに転送し続けます。Global Accelerator は、必要に応じて、新しい接続が開始したとき、またはアイドルタイムアウトの後にのみ、新しいエンドポイントを選択します。

AWS Global Accelerator の静的 IP アドレスの使用

デフォルトでは、Global Accelerator はアクセラレーターに関連付けられた静的 IP アドレスを提供します。Global Accelerator がアクセラレーターに割り当てる静的 IP アドレス、または標準アクセラレーター用に独自の IP アドレスプールから指定する静的 IP アドレスを使用して、ユーザーの場所

に関係なく、ユーザーの近くの 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ーの場合、1 つまたは複数の AWS リージョン リージョンで実行される Network Load Balancer、Application Load Balancer、Amazon EC2 インスタンス、または Elastic IP アドレスにアドレスを関連付けます。カスタムルーティングアクセラレーターの場合、1 つ以上のリージョンの VPC サブネット内の EC2 送信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経由する必要がないため、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 で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、ユーザーは変更時にアプリケーションに一貫した方法で接続できます。

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ーの静的 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ーにルーティングする」を参照してください。

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。

IPv4 の場合、Global Accelerator は 2 つの静的 IPv4 アドレスを提供します。デュアルスタックの場合、Global Accelerator は 2 つの IPv4 アドレスと 2 つの IPv6 アドレス、合計 4 つのグローバルの静的 IP アドレスを提供します。Global Accelerator (IPv4 のみ) で使用する独自の IP アドレス範囲を AWS (BYOIP) にする場合は、代わりに、アクセラレータで使用する IPv4 アドレスを独自のプールから割り当てることができます。詳細については、「Global Accelerator の Bring your own IP (BYOIP)」を参照してください。

デュアルスタックのアクセラレーターの場合、Global Accelerator は同じ 2 つの /64 CIDR プレフィックスから IPv6 アドレスを割り当てます。これにより、ACL コントロールの許可リスト化と設定の手順を簡素化できます。

IPv4 IP アドレスタイプ用に設定された標準アクセラレーターに IPv4 専用のエンドポイントを追加できますが、デュアルスタックとして設定したアクセラレーターでは、デュアルスタックもサポートするエンドポイントのみを追加する必要があります。デュアルスタックアクセラレータでサポートされているエンドポイントの詳細については、「アクセラレーターエンドポイントとして追加するリソースの要件」を参照してください。

Global Accelerator は、独自の IP アドレス範囲を AWS にし、そのプールから静的 IP アドレスを指定しない限り、Amazon の IP アドレスプールから静的 IP アドレスを提供します。(詳細については、Global Accelerator の Bring your own IP (BYOIP) を参照してください)。コンソールでアクセラ

レーターを作成するには、最初のステップとして、アクセラレーターの名前を入力するか、独自の静的 IP アドレスを選択して静的 IP アドレスをプロビジョニングするように Global Accelerator に指示します。アクセラレーターを作成する手順については、AWS Global Accelerator の開始方法 を参照してください。

静的 IP アドレスは、アクセラレーターを無効にし、トラフィックを受け入れたりルーティングしたりしなくなった場合でも、存在する限り、アクセラレーターに割り当てられたままになります。ただし、アクセラレーターを削除すると、そのアクセラレーターに割り当てられた静的 IP アドレスが失われるため、それ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 では、タグベースのアクセス許可などの IAM ポリシーを使用して、アクセラレーター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、「Global Accelerator を使用した ABAC」を参照してください。

Global Accelerator がヘルスチェックを使用する方法

標準アクセラレーターの場合、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ヘルスを自動的にチェックし、ユーザートラフィックを正常なエンドポイントにのみ送信します。

Global Accelerator には、自動的に実行されるデフォルト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設定できます。カスタムヘルスチェック設定を行う場合、Global Accelerator は設定に応じて特定の方法でそれらの設定を使用します。これらの設定は、Global Accelerator for Amazon EC2 インスタンスまたは Elastic IP アドレスエンドポイントで設定するか、Network Load Balancer または Application Load Balancer の Elastic Load Balancing コンソールで設定することができます。詳細については、「アクセラレーターのヘルスチェックアクセスを確保する」を参照してください。

標準アクセラレーターにエンドポイントを追加する場合、トラフィックが転送される前に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ー内の に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、リクエストはすべてのエンドポイントにルーティングされます。

トラフィックダイヤルとエンドポイントの重みを使用してトラフィックフローを管理する方法

AWS Global Accelerator が標準アクセラレーター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方法は 2 つあります:

- 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

- グループ内のエンドポイントへのトラフィックの割合を変更する重みを指定する

トラフィックダイヤルの仕組み

標準アクセラレーター内のエンドポイントグループごとに、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制御するようにトラフィックダイヤルを設定できます。この割合は、リスナー全体の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向けら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一部を制限し、そのエンドポイントグループに転送されるトラフィックの割合で表します。例えば、us-east-1 でエンドポイントグループのトラフィックダイヤルを 50 (つまり 50%) に設定し、アクセラレーターがそのエンドポイントグループに 100 件のユーザーリクエストを指示する場合、グループが受け入れるリクエストは 50 件のみです。アクセラレーターは、残りの 50 件のリクエストを他のリージョンのエンドポイントグループにルーティングします。

詳細については、「トラフィックダイヤルを使用してリージョンへ送信するトラフィックフローを調整する」を参照してください。

重みの仕組み

標準アクセラレーター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、アクセラレーター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実行する場合などに便利です。

重みは、アクセラレーター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、重みの最大値の半分である 255 です。

アクセラレーターは、エンドポイントグループのエンドポイントの重みの合計を計算し、各エンドポイントの重みと合計の比率に基づいてトラフィックをエンドポイントに送信します。重みの仕組みの例については、エンドポイントの重みがトラフィックボリュームを管理する仕組み を参照してください。

トラフィックダイヤルと重みは、標準アクセラレーター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。

- エンドポイントグループのトラフィックダイヤルを設定します。トラフィックダイヤルを使用すると、アクセラレーターが既に送信したトラフィックを近接性などの他の要素に基づいて「ダイヤル

ダウン」することで、グループへのトラフィックの割合、またはすべてのトラフィックをカットできます。

- 一方、重みを使用して、エンドポイントグループ内の個々のエンドポイントの値を設定します。重みは、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。例えば、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。

トラフィックのダイヤルと重みがフェイルオーバーにどのように影響するかの詳細については、異常なエンドポイントに対するフェイルオーバーの仕組み を参照してください。

ICMP レスポンスメッセージと AWS Global Accelerator

`ICMP Packet Too Big` や `Fragmentation Needed` などの ICMP レスポンスメッセージは、インターネット上での可用性を確保するのに役立ちます。AWS Global Accelerator は、すべてのグローバル IP アドレスのエッジで ICMP エコーメッセージ (ping) に応答します。これらの ping はお客様のエンドポイントに転送されません。Global Accelerator でパフォーマンスを正確にテストするには、テストに詳細なプロトコルを使用します。

ここでは、ICMP がインターネットの可用性を確保する方法の概要を示します。ネットワーク接続の最大送信単位 (MTU) とは、接続を介して渡すことができる最大許容パケットサイズ (バイト単位) です。接続の MTU が大きいほど、より多くのデータを単一のパケットで渡すことができます。2 つのデバイス間のパス MTU を判断するために、パス MTU 検出 (PMTUD) が使用されます。パス MTU は、送信側ホストと受信側ホスト間のパスでサポートされている最大のパケットサイズです。2 つのホスト間でネットワーク内の MTU サイズに差がある場合、MTU より大きいパケットはドロップされ、パケットをドロップした受信ホストは送信者に ICMP メッセージで通知します。詳細については、「パス MTU 検出」を参照してください。

Global Accelerator のアクセラレーターで ICMP トラフィックをブロックすることはできません。すべての ICMP トラフィックをブロックすると、`ICMPv6 Packet Too Big (PTB)` (タイプ 2) や `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (タイプ 3、コード 4) などの ICMP メッセージも削除されます。これらのメッセージは、トラフィックが発信元ホストに正常に返すために必要です。次に、これらのメッセージがドロップされると、Global Accelerator 上に構築された TCP とプロトコルが、通常よりも小さな MTU を持つネットワーク上のクライアントからのトラフィックをドロップし、PMTUD が防止されます。

PMTUD を機能させるには、エンドポイントのセキュリティグループも ICMP トラフィックを許可する必要があります。特定のエンドユーザーネットワークに固有の可用性の問題がある場合は、エンドポイントセキュリティグループが ICMP トラフィックを許可していることを確認します。

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リストについては、「AWS Global Accelerator 機能」ページのグローバルエッジネットワークを参照してください。

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」ファイルをダウンロードします。詳細については、Amazon Web Services 全般のリファレンス の AWS IP アドレスの範囲をご参照ください。

`ip-ranges.json` ファイルを使用する前に、まず以下の情報を確認してください。

- 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` で次の文字列を検索します:

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

- `"region": "GLOBAL"` を含む Global Accelerator エントリは、アクセラレーターに割り当てられた静的 IP アドレスを指します。1 つのエリアの Point of Presence (POP) からのアクセラレーター経由のトラフィックをフィルタリングする場合は、`us-*` や `eu-*` などの特定の地理的エリアを含むエントリをフィルタリングします。したがって、例えば、`us-*` をフィルタリングすると、米国 (U.S.) POP を通過するトラフィックのみが表示されます。
- Global Accelerator は、クライアント IP アドレスの保存とネットワークアドレス変換 (NAT) の 2 つの方法でトラフィックをルーティングできます。トラフィックのルーティング方法によって、AWS WAF ルールを適用できるクライアント IP アドレスが決まります。クライアント IP アドレスの保存を使用する場合、AWS WAF ルールはクライアント IP アドレス、つまりサービスにアクセスするクライアントの IP アドレスをターゲットにします。NAT を使用すると、Global Accelerator がトラフィックのルーティングに使用するグローバル IP アドレスに AWS WAF ルールが適用されます。

AWS Global Accelerator ユースケースについて

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、そのユースケースをいくつか表示し、Global Accelerator を使用してニ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を高めるスケール

アプリケーション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。Global Accelerator を使用すると、ネットワークをスケールアップまたはスケールダ

ウンできます。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 IPv4 アドレスに関連付けたり、デュアルスタックの場合は 2 つの静的 IPv4 アドレスと 2 つの IPv6 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 レコードで 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 アドレスを更新することなく、AWS リージョン でエンドポイントを追加または削除したり、ブルー/グリーンデプロイを実行したり、A/B テストを実行したりできます。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、医療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の高速化

多くのアプリケーション、特にゲーム、メディア、モバイルアプリ、広告技術、財務などの分野では、優れたユーザーエクスペリエンスを実現するには、非常に低いレイテンシーが必要です。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誘導し、インターネットのレイテンシーとジッターを減らします。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すばやく対応して、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

ネットワークを利用できる必要があります。ディザスタリカバリ、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場合があります。Global Accelerator は、アプリケーションエンドポイントがプライマリ AWS リージョン で失敗していることを検出すると、次に利用可能な最も近い 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。

Global Accelerator が本質的に、また、サービスを使用するアプリケーションで耐障害性をサポートする方法の詳細については、「Maximising application resiliency with AWS Global Accelerator」というブログ記事を参照してください。

アプリケーションの保護

Application Load Balancer や Amazon EC2 インスタンスなどの AWS の元をパブリックインターネットトラフィックにさらすと、悪意のある攻撃の機会が発生します。Global Accelerator は、2 つの静的エントリポイントの背後にあるオリジンをマスキングすることで、攻撃のリスクを減らします。これらのエントリポイントは、AWS Shield による分散サービス拒否 (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 Application Load Balancer 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外に保存します。

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させる

カスタムルーティングアクセラレーターを使用すると、VoIP またはゲームアプリケーションに Global Accelerator のパフォーマンス上の利点を活用できます。例えば、Global Accelerator を使用して、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を作成できます。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ためにカスタムロジックを必要とするアプリケーションに対して、レイテンシーとジッターをグローバルに削減できます。1 つのアクセラレーターを使用して、クライアントを 1 つまたは複数の AWS リージョン で実行されている何千もの Amazon EC2 インスタンスに接続できます。同時に、どのクライアントがどの EC2 インスタンスとポートに送信されるかを完全に制御できます。

AWS Global Accelerator 速度比較ツール

AWS Global Accelerator 速度比較ツールを使用して、AWS リージョン 全体の直接インターネットダウンロードと比較した Global Accelerator 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、ブラウザを使用して Global Accelerator を使用してデータを転送する際の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、ツールは異なるリージョンの Application Load Balancer から HTTPS/TCP 経由でブラウザにファイルをダウンロードします。リージョンごとに、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 の外部にある要素によって異なる場合があります。

AWS Global Accelerator の開始方法

API または AWS Global Accelerator コンソールを使用して AWS Global Accelerator を設定することで開始できます。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 にある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、アクセラレータの作成や更新を行うには、米国西部 (オレゴン) リージョンを指定する必要がある点に注意してください。

Global Accelerator の使用を開始するには、以下の一般的な手順に従います。

1. 作成するアクセラレーターのタイプを選択します: 標準アクセラレーターまたはカスタムルーティングアクセラレーター。
2. Global Accelerator の初期設定を行う: アクセラレーターの名前を指定し、アクセラレーターのタイプとアドレスタイプを選択します。
3. アクセラレーターに 1 つ以上のリスナーを設定する: リスナーは、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します。
4. アクセラレーターのリージョンエンドポイントグループを設定する: リスナーに追加するリージョンエンドポイントグループを 1 つ以上選択できます。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ーの場合、Global Accelerator は、各エンドポイントに定義されているヘルス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ヘルスをモニタリングします。標準アクセラレーターの各エンドポイントグループについて、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するようにトラフィックダイヤルの割合を設定できます。この割合は、すべてのリスナートラフィックではなく、エンドポイントグループに既に送信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リージョンエンドポイントグループで 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ーの場合、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。
5. エンドポイントグループにエンドポイントを追加する: 追加するエンドポイントは、アクセラレーターのタイプによって異なります。
   - 標準アクセラレーターでは、ロードバランサーや EC2 インスタンスエンドポイントなどの 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ーには、最大数千の Amazon EC2 インスタンスの送信先を持つ 1 つ以上の Amazon VPC (VPC) サブネットを追加します。

AWS Global Accelerator コンソールを使用して標準アクセラレーターまたはカスタムルーティングアクセラレーターを作成する方法の詳細については、AWS Global Accelerator の開始方法 を参照してください。API オペレーションを操作するには、AWS Global Accelerator の一般的な API アクション および「AWS Global Accelerator API リファレンス」を参照してください。

AWS Global Accelerator でのタグ付け

タグとは、AWS リソースを特定し、整理するのに使用できる単語または語句 (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。例えば、タグキーは「environment」、タグ値は「production」などです。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、アクセラレーターにタグを付けることができます。

以下の 2 つの例では、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、アクセラレーターやその他の AWS リソース (Network Load Balancer、Application Load Balancer、Amazon EC2 インスタンスなど) にタグを適用し、タグを有効にします。次に、AWS はコストクォータレポートをコンマ区切り値 (CSV ファイル) として生成し、使用量とコストがタグごとに集計されます。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 Billingユーザーガイド の [コスト配分タグの使用] をご参照ください。
- 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します。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、「Global Accelerator を使用した ABAC」を参照してください。

タグ付けに関する使用規則と他のリソースへのリンクについては、「AWS 全般のリファレンス」の「AWSリソースのタグ付け」を参照してください。タグの使用に関するヒントについては、「AWS Whitepapers」の「Tagging Best Practices: AWS Resource Tagging Strategy」を参照してください。

Global Accelerator でリソースに追加できるタグの最大数については、AWS Global Accelerator のクォータ を参照してください。

AWS コンソール、AWS CLI、または Global Accelerator API を使用して、タグを追加および更新できます。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。AWS CLI および Global Accelerator API を使用したタグの操作の詳細については、「AWS Global Accelerator API Reference」の以下のオペレーションを参照してください。

- CreateAccelerator
- CreateCrossAccountAttachment
- TagResource
- UntagResource
- ListTagsForResource

Global Accelerator でのタグ付けへのサポート

AWS Global Accelerator は、アクセラレーターとクロスアカウントアタッチメント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、「Global Accelerator を使用した ABAC」を参照してください。

Global Accelerator でのタグの追加、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にタグを追加、編集、削除する方法について説明します。

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タグを追加または削除できます。CLI の例などの詳細については、「AWS Global Accelerator API Reference」の「TagResource」を参照してください。

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

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. タグを追加または更新したいアクセラレーターを選択します。
3. [タグ] セクションで、次の操作を行います:

タグの追加

[タグの追加] を選択し、キーを入力し、必要に応じてタグの値を入力します。

タグの編集

キー、値またはその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

値フィールドの右側にある [削除] を選択します。

4. [Save changes] (変更の保存) をクリックします。

AWS Global Accelerator の料金

AWS Global Accelerator では、アカウントでプロビジョニングされる各アクセラレーター (有効または無効にかかわらず) に対して固定時間料金が請求され、アクセラレーターを通過する主要な方向のトラフィックの 1 時間ごとに、標準データ転送レートに加えて増分料金 が課金されます。増分率は、リクエストを処理する AWS リージョン (ソース) と、レスポンスが送られる AWS エッジロケーション (送信先) に依存します。通常、お客様はアプリケーションごとに 1 つのアクセラレーターを作成しますが、複雑なアプリケーションのお客様は、より多くのアクセラレーターが必要になる場合があります。

料金の詳細、送信元および送信先リージョン別の料金情報、料金の例については、「AWS Global Accelerator 料金」を参照してください。

AWS Global Accelerator の開始方法

この章では、AWS Global Accelerator の使用開始に役立つように、標準アクセラレーターとカスタムルーティングアクセラレーターを設定するためのチュートリアルを提供します。

Global Accelerator で作成できる 2 つのタイプのアクセラレーターの詳細については、AWS Global Accelerator での標準アクセラレーターの使用 および AWS Global Accelerator でのカスタムルーティングアクセラレーターの使用 を参照してください。

このチュートリアルでは、主に AWS マネジメントコンソール を使用する手順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ーを設定するときは、特定の設定手順に API を使用する必要があります。

> **Tip**
>
> Global Accelerator を使用してウェブ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、セルフペース型ワークショップ を参照してください: AWS Global Accelerator ワークショップ。

AWS Command Line Interface (AWS CLI) または AWS SDK で Global Accelerator 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。以下は、Global Accelerator API を操作するためのリソースです。

- API オペレーションのリストについては、「AWS Global Accelerator の一般的な API アクション」を参照してください。
- AWS Global Accelerator API オペレーションの操作の詳細については、「AWS Global Accelerator API Reference」を参照してください。

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。サポートされているリージョンは、AWS リージョンテーブルに一覧表示されています。

内容

- 標準アクセラレーターの使用を開始する
- カスタムルーティングアクセラレーターの使用を開始

標準アクセラレーターの使用を開始する

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ー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: 標準アクセラレーターを作成する
- ステップ 2: リスナーを追加する
- ステップ 3: エンドポイントグループを追加する
- ステップ 4: エンドポイントを追加する
- ステップ 5: アクセラレーターをテストする
- ステップ 6 (選択可能): アクセラレーターを削除する

開始する前に

アクセラレーターを作成する前に、トラフィックを送信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。例えば、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ため、Amazon EC2 インスタンスを少なくとも 1 つ起動します。詳細については、「Amazon EC2 ユーザーガイド」の「EC2 リソースの作成と EC2 インスタンスの起動」を参照してください。
- 必要に応じて、EC2 インスタンスを含む 1 つ以上の Network Load Balancer または Application Load Balancer を作成します。詳細については、「Network Load Balancer ユーザーガイド」の「Network Load Balancer の作成」を参照してください。

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

- Global Accelerator に内部 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と、プライベートサブネットでターゲットにすることで、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) のエンドポイントとの間で直接流れるようになります。ロードバランサーまたは EC2 インスタンスを含む VPC には、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す「インターネットゲートウェイ」がアタッチされている必要があります。詳細については、「AWS Global Accelerator での安全な 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、Amazon 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が 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できるようにする必要があります。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、「Amazon Route 53 デベロッパーガイド」の「 Amazon Route 53 サーバーの IP アドレス範囲」を参照してください。

ステップ 1: 標準アクセラレーターを作成する

標準アクセラレーターを作成するときは、Global Accelerator がアクセラレーターに割り当てる静的 IP アドレスに IPv4 またはデュアルスタックを選択できます。デュアルスタックは、IPv4 と IPv6 の両方の IP アドレスをサポートしています。

アクセラレーターを作成するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [アクセラレーターの作成] を選択します。
3. アクセラレーターの名前を指定します。
4. [Accelerator タイプ] には、[標準] を選択します。
5. [IP アドレスタイプ] で、[IPv4] または [デュアルスタック]を選択します。
6. 必要に応じて、Global Accelerator リソースの特定に役立つタグを 1 つ以上追加します。
7. [次へ] を選択します。

ステップ 2: リスナーを追加する

ユーザーから Global Accelerator へのインバウンド接続を処理するリスナーを作成します。

リスナーを作成するには

1. [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選択します。
3. 必要に応じて、クライアントアフィニティを有効にすることを選択します。リスナーに対するクライアントアフィニティとは、Global Accelerator が特定のソース (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ようにす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から [ソース IP] を選択します。

デフォルトは [None] です。つまり、クライアントアフィニティが有効になっていず、Global Accelerator はリスナーのエンドポイントグループ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、「Global Accelerator でのクライアントアフィニティの仕組み」を参照してください。

4. (選択可能) [リスナーを追加] を選択してその他のリスナーを追加します。
5. タグを追加した後、[次へ] を選択します。

ステップ 3: エンドポイントグループを追加する

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を追加するには

1. [エンドポイントグループの追加] ページで、リスナーのセクションで、ドロップダウンリストから [リージョン] 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 から 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。この割合は、すべてのリスナートラフィックにではなく、このエンドポイントグループに既に送信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、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については、「ヘルスチェックの設定」を選択します。ヘルスチェック設定を設定すると、Global Accelerator は EC2 インスタンスと 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 エンドポイントと Application Load Balancer エンドポイントの場合、Global Accelerator はロードバランサー自体に対して既に設定したヘルスチェック設定を使用します。詳細については、「アクセラレーターのヘルスチェックアクセスを確保する」を参照してください。
4. オプションで、[エンドポイントグループの追加] を選択して、このリスナーまたは他のリスナーにさらにエンドポイントグループを追加します。
5. [次へ] を選択します。

ステップ 4: エンドポイントを追加する

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。このステップ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へのトラフィックは送信されません。

エンドポイントを追加するには

1. [エンドポイントの作成] ページで、エンドポイントのセクションで[エンドポイント] を選択します。
2. 必要に応じて、[重み] に 0 から 255 の数字を入力し、このエンドポイントへのトラフィックをルーティングする際の重みを設定します。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、すべてのフィールドの重みは 128 です。詳細については、「エンドポイントの重みがトラフィックボリュームを管理する仕組み」を参照してください。
3. 必要に応じて、[クライアント IP アドレスの保存] で、[アドレスの保存] を選択します。(一部のエンドポイントタイプでは、このオプションが選択されており、クリアできません。) 詳細については、「AWS Global Accelerator でクライアント IP アドレスを保存する」を参照してください。
4. 必要に応じて、[エンドポイントの追加] を選択してエンドポイントを追加します。
5. [次へ] を選択します。

[次へ]を選択すると、Global Accelerator ダッシュボードに、アクセラレーターが進行中であることを示すメッセージが表示されます。プロセスが完了すると、ダッシュボードのアクセラレーターステータスは[アクティブ] になります。

ステップ 5: アクセラレーターをテストする

アクセラレーターをテストして、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。例えば、アクセラレーターの静的 IP アドレスの 1 つを置き換えて、リクエストが処理される AWS リージョンを表示するように、次のように curl コマンドを実行します。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したりする場合に特に役立ちます。

アクセラレーターの静的 IP アドレスの 1 つを置き換えて、次のように curl コマンドを実行して IP アドレスを 100 回呼び出し、各リクエストが処理されたカウントを出力します。

```
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のトラフィックダイヤルを調整した場合、このコマンドは、アクセラレーターがトラフィックを正しい割合で異なるグループに送信していることを確認するのに役立ちます。詳細については、次のブログ記事の詳細な例、「Traffic management with AWS Global Accelerator」を参照してください。

ステップ 6 (選択可能): アクセラレーターを削除する

アクセラレーターをテストとして作成した場合、またはアクセラレーターを使用しなくなった場合は、削除できます。コンソールでアクセラレーターを無効にし、削除できます。アクセラレーター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。

コンソールの代わりに API オペレーションを使用してアクセラレーターを削除するには、まずアクセラレーター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、「AWS Global Accelerator API Reference」の「DeleteAccelerator」オペレーションを参照してください。

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

- アクセラレーターを作成すると、Global Accelerator は 2 つの静的 IP アドレスのセットを提供します。静的 IP アドレスは、アクセラレーターを無効にし、トラフィックを受け入れたりルーティングしたりしなくなった場合でも、存在する限り、アクセラレーターに割り当てられたままになります。ただし、アクセラレーターを削除すると、アクセラレーターに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。ベストプラクティスとして、アクセラレーター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 では、IAM ポリシーを使用して、例えばタグベースのアクセス許可を設定し、アクセラレータを削除する権限を持つユーザーを制限することができます。詳細については、「Global Accelerator を使用した ABAC」を参照してください。
- Global Accelerator の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、ヘルスチェックが合格した場合、Global Accelerator はトラフィックを新しいエンドポイントにルーティングします。そうしたくない場合は、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. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. 削除したいアクセラレーターを選択します。
3. [編集] を選択します。
4. [アクセラレーターの無効化] を選択し、[保存] を選択します。
5. 削除したいアクセラレーターを選択します。
6. [アクセラレーターの削除] を選択します。
7. 確認ダイアログボックスで、[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ーの使用を開始

このセクションでは、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の Amazon EC2 インスタンスの送信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ー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: カスタムルーティングアクセラレーターを作成する
- ステップ 2: リスナーを追加する
- ステップ 3: エンドポイントグループを追加する
- ステップ 4: エンドポイントを追加する
- ステップ 5 (選択可能): アクセラレーターを削除する

開始する前に

カスタムルーティングアクセラレーターを作成する前に、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ーエンドポイントは、複数の Amazon EC2 インスタンスを含めることができる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。これらのリソースの作成手順については、次の内容を参照してください。

- VPC またはサブネットを作成します。詳細については、「Directory Service 管理ガイド」の「VPC の作成と設定」を参照してください。

- 必要に応じて、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、「Amazon EC2 ユーザーガイド」の「EC2 リソースの作成と EC2 インスタンスの起動」を参照してください。

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

- Global Accelerator に EC2 インスタンスエンドポイントを追加すると、プライベートサブネットでターゲットにすることで、VPC 内のエンドポイントとの間でインターネットトラフィックを直接流れるようになります。EC2 インスタンスを含む VPC には、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すために、「インターネットゲートウェイ」がアタッチされている必要があります。詳細については、「AWS Global Accelerator での安全な VPC 接続」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を作成する前に、カスタムルーティングアクセラレーターのガイドラインと制限 で説明されているベストプラクティスを確認してください。

ステップ 1: カスタムルーティングアクセラレーターを作成する

アクセラレーターを作成するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. アクセラレーターの名前を指定します。
3. [Accelerator タイプ] の場合は、[カスタムルーティング] を選択します。
4. 必要に応じて、アクセラレーターリソースを識別するのに役立つタグを 1 つ以上追加します。
5. [次へ] を選択して、リスナー、エンドポイントグループ、VPC サブネットエンドポイントを追加します。

ステップ 2: リスナーを追加する

ユーザーから Global Accelerator へのインバウンド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は、カスタムルーティングアクセラレーターで使用できるリスナーポートと送信先 IP アドレスの組み合わせの数を定義します。最大限の柔軟性を得るには、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、少なくとも 16 ポートを含める必要があります。

リスナーを作成するには

1. [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選択します。
3. (選択可能) [リスナーを追加] を選択してその他のリスナーを追加します。
4. タグを追加した後、[次へ] を選択します。

ステップ 3: エンドポイントグループを追加する

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。Global Accelerator 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送信します。

指定したポート範囲ごとに、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。

エンドポイントグループを追加するには

1. [エンドポイントグループの追加] ページで、リスナーのセクションで [リージョン] を選択します。
2. [ポートとプロトコルセット] には、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。
   - [入力ポート] と [出力ポート] を入力して、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または複数のプロトコルを指定します。

   ポート範囲をリスナーポート範囲のサブセットにす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するのに十分な合計ポートが必要です。
3. [Save] を選択します。
4. オプションで、[エンドポイントグループの追加] を選択して、このリスナーまたは他のリスナーにさらにエンドポイントグループを追加します。
5. [次へ] を選択します。

ステップ 4: VPC サブネットエンドポイントを追加する

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ー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ー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 つ以上の Amazon EC2 インスタンスの送信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、サブネット内の送信先 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するために使用できる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送信できます。

エンドポイントを追加するには

1. [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、エンドポイントの [サブネット ID] を選択します。
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 インスタンスの送信先へのトラフィックを有効にします。

   - トラフィックをサブネット上のすべての EC2 エンドポイントとポートに誘導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] を選択します。
   - サブネット上の特定の EC2 エンドポイントとポートへのトラフィックを許可するには、[特定の送信先ソケットアドレスへのトラフィックを許可する] を選択します。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] を選択します。

   デフォルトでは、エンドポイントをサブネット化するため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送信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 インスタンスとポートへのトラフィックを有効にする場合は、プログラムで有効にできます。詳細については、「AWS Global Accelerator API Reference」の「AllowCustomRoutingTraffic」を参照してください。

3. [次へ] を選択します。

[次へ] を選択すると、Global Accelerator ダッシュボードに、アクセラレーターが進行中であることを示すメッセージが表示されます。プロセスが完了すると、ダッシュボードのアクセラレーターステータスは[アクティブ] になります。

ステップ 5 (選択可能): アクセラレーターを削除する

アクセラレーターをテストとして作成した場合、またはアクセラレーターを使用しなくなった場合は、削除できます。コンソールでアクセラレーターを無効にし、削除できます。アクセラレーター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。

コンソールの代わりに API オペレーションを使用してアクセラレーターを削除するには、まずアクセラレーター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、「AWS Global Accelerator API Reference」の「DeleteCustomRoutingAccelerator」を参照してください。

アクセラレーターを削除するときは、次の点に注意してください。

- アクセラレーターを作成すると、Global Accelerator は 2 つの静的 IP アドレスのセットを提供します。静的 IP アドレスは、アクセラレーターを無効にし、トラフィックを受け入れたりルーティングしたりしなくなった場合でも、存在する限り、アクセラレーターに割り当てられたままになります。ただし、アクセラレーターを削除すると、アクセラレーターに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。ベストプラクティスとして、アクセラレーター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 では、タグベースのアクセス許可などの IAM ポリシーを使用して、アクセラレーター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、「Global Accelerator を使用した ABAC」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. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. 削除したいアクセラレーターを選択します。
3. [編集] を選択します。
4. [アクセラレーターの無効化] を選択し、[保存] を選択します。
5. 削除したいアクセラレーターを選択します。
6. [アクセラレーターの削除] を選択します。
7. 確認ダイアログボックスで、[削除] を選択します。

AWS Global Accelerator の一般的な API アクション

このセクションでは、Global Accelerator リソースで使用できる一般的な AWS Global Accelerator アクションを、関連するドキュメントへのリンクとともに一覧表示します。

標準アクセラレーターで使用するアクション

次の表に、標準アクセラレーターで使用できる一般的な 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。

アクション	Global Accelerator コンソールの使用	Global Accelerator API の使用
標準アクセラレーターを作成する	「標準アクセラレーターの使用を開始する」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ーのリスナーを作成する	「AWS Global Accelerator の標準アクセラレーターのリスナー」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ー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ー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ーを更新する	「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。
エンドポイントグループを更新する	「標準エンドポイントグループを追加する」を参照してください。	「UpdateEndpointGroup 」を参照してください。
エンドポイントを追加する	「標準エンドポイントを追加する」を参照してください。	「AddEndpoints 」を参照してください。

アクション	Global Accelerator コンソールの使用	Global Accelerator API の使用
エンドポイントを削除する	「標準エンドポイントを追加する」を参照してください。	「RemoveEndpoints 」を参照してください。
標準アクセラレーターの一覧表示	「アクセラレーターを表示する」を参照してください。	「ListAccelerator 」を参照してください。
アクセラレーターに関する情報を獲得する	「アクセラレーターを表示する」を参照してください。	「DescribeAccelerator 」を参照してください。
アクセラレーターを削除する	「アクセラレーターを作成する」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アクセラレーター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ーで使用できる一般的な 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。

アクション	Global Accelerator コンソールの使用	Global Accelerator API の使用
カスタムルーティングアクセラレーターを作成する	「カスタムルーティングアクセラレーターの使用を開始」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ーのリスナーを作成する	「Global Accelerator のカスタムルーティングアクセラレーターのリスナー」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ーのエンドポイントグループを作成する	「Global Accelerator のカスタムルーティングアクセラレーター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。

アクション	Global Accelerator コンソールの使用	Global Accelerator API の使用
カスタムルーティングアクセラレーターを更新する	「AWS Global Accelerator のカスタムルーティングアクセラレーター」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ーの一覧表示	「Global Accelerator でカスタムルーティングアクセラレーターを表示する」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ーに関するすべての情報を取得する	「Global Accelerator でカスタムルーティングアクセラレーターを表示する」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ーを削除する	「Global Accelerator でカスタムルーティングアクセラレーターを作成する」を参照してください。	「DeleteCustomRoutingAccelerator 」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ー内のサブネットのすべての送信先トラフィックを許可する	「カスタムルーティングアクセラレーターの VPC サブネットエンドポイントを追加する」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ー内のサブネットのすべての送信先トラフィックを拒否する	「カスタムルーティングアクセラレーターの VPC サブネットエンドポイントを追加する」を参照してください。	「DenyCustomRoutingTraffic 」を参照してください。

アクション	Global Accelerator コンソールの使用	Global Accelerator API の使用
カスタムルーティングアクセラレーター内の特定の送信先へのトラフィックを許可する	「カスタムルーティングアクセラレーターの VPC サブネットエンドポイントを追加する」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ー内の特定の送信先へのトラフィックを拒否する	「カスタムルーティングアクセラレーターの VPC サブネットエンドポイントを追加する」を参照してください。	「DenyCustomRoutingTraffic 」を参照してください。

Global Accelerator でのクロスアカウントサポートで使用するアクション

次の表に、Global Accelerator のクロスアカウントサポートで使用できる一般的な 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。

アクション	Global Accelerator コンソールの使用	Global Accelerator API の使用
クロスアカウントアタッチメントを作成する	「AWS Global Accelerator でクロスアカウントアタッチメントを作成する」を参照してください。	「CreateCrossAccountAttachment 」を参照してください。
クロスアカウントアタッチメントを削除する	「AWS Global Accelerator でクロスアカウントアタッチメントを作成する」を参照してください。	「DeleteCrossAccountAttachment 」を参照してください。
クロスアカウントアタッチメントでの情報を記述する	「Global Accelerator でクロスアカウントリソースを特定する」を参照してください。	「DescribeCrossAccountAttachment 」を参照してください。

アクション	Global Accelerator コンソールの使用	Global Accelerator API の使用
アカウントのクロスアカウントアタッチメントを一覧表示する	「Global Accelerator でクロスアカウントリソースを特定する」を参照してください。	「ListCrossAccountAttachments」を参照してください。
クロスアカウントアタッチメントを更新する	「AWS Global Accelerator でクロスアカウントアタッチメントを作成する」を参照してください。	「UpdateCrossAccountAttachment」を参照してください。

AWS Global Accelerator での標準アクセラレーターの使用

この章には、アクセラレーター、リスナー、エンドポイントグループ、エンドポイントの設定など、AWS Global Accelerator で標準アクセラレーターを作成するための手順と推奨事項が含まれています。標準アクセラレーターを使用すると、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間で特定のエンドポイントに送信する場合は、カスタムルーティングアクセラレーターを作成します。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ーの使用」を参照してください。

標準アクセラレーターを設定するには、以下を実行します。

1. アクセラレーターを作成し、標準アクセラレーターオプションを選択します。
2. [アドレスタイプ] で、[IPv4] または [デュアルスタック] を選択します。
3. 必要に応じて、Bring Your Own IP アドレスを使用する静的 IP アドレスを設定します。
4. 特定のポートまたはポート範囲のセット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 または UDP。
5. エンドポイントリソースがある各 AWS リージョン に対して、1 つ以上のエンドポイントグループを追加します。
6. エンドポイントグループに 1 つ以上のエンドポイントを追加します。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。エンドポイントのタイプおよび要件については、??? を参照してください。

以下のセクションでは、リスナー、エンドポイントグループ、エンドポイントなど、標準アクセラレーターとそのコンポーネントを追加、削除、設定する手順について説明します。

トピック

- AWS Global Accelerator の標準アクセラレーター
- AWS Global Accelerator の標準アクセラレーターのリスナー
- AWS Global Accelerator の標準アクセラレーターのエンドポイントグループ
- AWS Global Accelerator の標準アクセラレーターのエンドポイント

AWS Global Accelerator の標準アクセラレーター

AWS Global Accelerator の標準アクセラレーターは、AWS グローバルネットワーク経由のトラフィックを、指定された AWS リージョン に含まれるエンドポイントに送信します。各アクセラレーターには 1 つ以上のリスナーが含まれます。リスナーは、設定したプロトコル (または複数のプロトコル) 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 Global Accelerator へのインバウンド接続を処理します。

標準アクセラレーターの場合、Global Accelerator は、設定したヘルス、クライアントの場所、ポリシーに基づいてトラフィックを最適なリージョンエンドポイントに誘導し、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ーのエンドポイントは、Network Load Balancer、Application Load Balancer、Amazon EC2 インスタンス、AWS リージョン または 1 つ以上のリージョンにある Elastic IP アドレスのいずれかも可能です。

> **Important**
>
> デフォルトでは、Global Accelerator は、アクセラレーターに関連される静的 IP アドレスを提供します。IP アドレスは、アクセラレーターを無効にし、トラフィックを受け入れなくなったりルーティングしたりした場合でも、存在する限り、アクセラレーターに割り当てられます。ただし、アクセラレーターを削除すると、アクセラレーターに割り当てられた Global Accelerator 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することができなくなります。ベストプラクティスとして、アクセラレーター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 では、IAM ポリシーを使用して、例えばタグベースのアクセス許可を設定し、アクセラレータを削除する権限を持つユーザーを制限することができます。詳細については、「Global Accelerator を使用した ABAC」を参照してください。

このセクションでは、Global Accelerator コンソールで標準アクセラレーターを操作する手順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 Reference」を参照してください。

内容

- アクセラレーターを作成する
- アクセラレーターを更新する
- アクセラレーターを削除する
- アクセラレーターを表示する

- ロードバランサーを作成するときにアクセラレーターを追加する
- グローバルの静的 IP アドレスとリージョンの静的 IP アドレスの使用を比較する

アクセラレーターを作成する

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する方法について説明します。Global Accelerator をプログラムで操作するには、「AWS Global Accelerator API Reference」を参照してください。

標準アクセラレーターを作成するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [アクセラレーターの作成] を選択します。
3. アクセラレーターの名前を指定します。
4. [アクセラレータのタイプ] には、[標準] を選択します。
5. [IP アドレスタイプ] で、[IPv4] または [デュアルスタック] を選択します。
6. 必要に応じて、独自の IP アドレス範囲を AWS (BYOIP) にした場合は、各アドレスプールから 1 つずつ、アクセラレータの静的 IP アドレスを指定できます。アクセラレーターの 2 つの静的 IP アドレスのそれぞれに対して、この選択を行います。

   - 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**
     >
     > 静的 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、Global Accelerator が高可用性のために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。

   - 独自の 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すると、Global Accelerator は特定の IP アドレスをアクセラレーターに割り当てます。

   BYOIP で静的 IP アドレスを指定または更新するための要件の詳細については、「Requirements when you update an accelerator to change the IP address.」を参照してください。

7. 必要に応じて、アクセラレーターリソースを識別するのに役立つタグを 1 つ以上追加します。
8. [次へ] を選択して、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。

アクセラレーターを更新する

このセクションでは、コンソールで標準アクセラレータを更新する方法について説明します。Global Accelerator をプログラムで操作するには、「AWS Global Accelerator API Reference」を参照してください。

標準アクセラレーターを更新するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. アクセラレーターのリストで 1 つを選択し、[編集] を選択します。
3. [アクセラレーターの編集] ページで、次のような変更を行います。
   - アクセラレーターの名前を変更します。
   - アクセラレーターを無効にして、トラフィックを受け付けたりルーティングしたりしないようにするか、削除できるようにします。
   - アクセラレーターが無効になっている場合は有効にします。
   - IP アドレスタイプを更新します。IPv4 に設定されている場合は、デュアルスタックに変更します。または、デュアルスタックの場合は IPv4 に変更します。
   - タグを更新します。
4. [Save changes] (変更の保存) をクリックします。

アクセラレーターを無効にする場合は、次の点に注意してください:

- Global Accelerator の静的 IP アドレスは、アクセラレーターを無効にしても、アクセラレーターに割り当てられたままになり、トラフィックの受け入れやルーティングができなくなります。アクセラレーターが存在する限り、アクセラレーターと同じ静的 IP アドレスを保持します。
- ただし、アクセラレーターを削除すると、アクセラレーターに割り当てられた Global Accelerator の静的 IP アドレスが失われます。その時点で、アドレスを使用してトラフィックをルーティングすることはできなくなります。

IP アドレスタイプを変更する場合は、次の点に注意してください:

- デュアルスタックエンドポイントを持つアクセラレーターのみをデュアルスタックの IP アドレスタイプに変更できます。
- アクセラレータの IP アドレスタイプをデュアルスタックから IPv4 に変更すると、Global Accelerator はアクセラレータに割り当てられた IPv6 IP アドレスを保存します。つまり、アクセラレーターの IP アドレスタイプをデュアルスタックに戻すと、元の静的 IPv6 IP アドレスがアクセラレーターに復元されます。

アクセラレータの他の機能、例えばエンドポイントの追加や削除、トラフィックダイヤルの更新、エンドポイントの重みの調整を変更したい場合は、以下のような関連トピックを取り扱う該当セクションを参照してください:

- 標準リスナーを追加する
- 標準エンドポイントグループを追加する
- 標準エンドポイントを追加する

アクセラレーターを削除する

アクセラレーターをテストとして作成した場合、またはアクセラレーターを使用しなくなった場合は、削除できます。コンソールでアクセラレーターを無効にし、削除できます。アクセラレーター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。

コンソールの代わりに API オペレーション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、「AWS Global Accelerator API Reference」の「DeleteAccelerator」オペレーションを参照してください。

アクセラレータを無効にするには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. リストで、無効にしたいアクセラレーターを選択します。
3. [編集] を選択します。
4. [アクセラレーターの無効化] を選択し、[保存] を選択します。

アクセラレーターを削除するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. リストで、削除したい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にしていない場合、[削除] は選択できません。

4. 確認ダイアログボックスで、[削除] を選択します。

> **Important**
>
> アクセラレーターを削除すると、アクセラレータに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。

アクセラレーターを表示する

アクセラレーターに関する情報は、コンソールで表示できます。プログラムを使用したアクセラレーターの説明を確認するには、「AWS Global Accelerator API Reference」の「ListAccelerators」と「DescribeAccelerator」を参照してください。

アクセラレーターに関する情報を表示するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. アクセラレーターの詳細を表示するには、リストでアクセラレーターを選択し、[表示] を選択します。

ロードバランサーを作成するとき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 または Network Load Balancer を作成する場合、必要に応じて「同時にアクセラレーターを追加できます」。Elastic Load Balancing と Global Accelerator は連携して、アクセラレーターを透過的に追加します。アクセラレーターは、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。(アクセラレーターの詳細については、AWS Global Accelerator とは を参照してください。)

> **Important**
>
> アクセラレーターを作成するには、適切なアクセス許可が必要です。詳細については、「AWS Global Accelerator のアイデンティティベースのポリシー」を参照してください。

アクセラレーターの設定と表示

DNS 設定を更新して、トラフィックをアクセラレーターの静的 IP アドレスまたは DNS 名に誘導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、アクセラレーターをロードバランサーに通過しません。

Amazon EC2 コンソールで Global Accelerator アドオンを選択してロードバランサーを作成した後、[統合サービス] タブに移動して、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) 名を確認します。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 の DNS アドレス指定とカスタムドメイン を参照してください。

AWS マネジメントコンソール で「Global Accelerator に移動」することで、アクセラレーターを表示および設定できます。例えば、アカウントに関連付けられているアクセラレーターを表示したり、アクセラレーター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、アクセラレーターを表示するおよびアクセラレーターを作成するを参照してください。

料金

AWS Global Accelerator では、お客様が利用された分のみのお支払いとなります。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、AWS Global Accelerator 料金を参照してください。

アクセラレーターの使用を停止する

Global Accelerator を通じてロードバランサーへのトラフィックルーティングを停止しようとする場合は、以下を実行します。

1. DNS 設定を更新して、トラフィックをロードバランサーに直接向けます。

2. アクセラレーターからロードバランサーを削除します。詳細については、標準エンドポイントを追加する の「エンドポイントを削除するには」を参照してください。
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。

グローバルの静的 IP アドレスとリージョンの静的 IP アドレスの使用を比較する

Amazon EC2 インスタンスなどの AWS リソースの前で静的 IP アドレスを使用する場合は、いくつかのオプションが利用できます。例えば、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 または IPv6 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、世界中の AWS エッジロケーションから発表されたグローバルの静的アドレスを取得できます。IPv4 の場合、Global Accelerator はグローバルの静的 IPv4 アドレスを 2 つ提供します。デュアルスタックの場合、Global Accelerator は 2 つの IPv4 アドレスと 2 つの IPv6 アドレス、合計 4 つのグローバルの静的 IP アドレスを提供します。Amazon EC2 インスタンス、Network Load Balancer、Application Load Balancer などの 1 つ以上のリージョンで、アプリケーション用に既に AWS リソースが設定されている場合は、それらを簡単に Global Accelerator に追加して、グローバルの静的 IP アドレスで事前処理できます。詳細については、「アクセラレーターエンドポイントとして追加するリソースの要件」を参照してください。

Global Accelerator によってプロビジョニングされたグローバルの静的 IP アドレスを使用することを選択すると、アプリケーションの可用性とパフォーマンスも向上します。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受信トラフィックを受け入れます。トラフィックが AWS ネットワーク上に存在する時間を最大化することで、カスタマーエクスペリエンスを迅速かつ向上させることができます。詳細については、「AWS Global Accelerator の働き」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 から追加するか、AWS CLI または SDK を使用して API 操作で追加できます。詳細については、「アクセラレーターを作成する」を参照してください。

アクセラレーターを追加する際に、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たグローバルの静的 IP アドレスは、アクセラレーターを無効にし、トラフィックを受け入れたりルーティングしたりしなくなった場合でも、

アクセラレーターが存在する限り、ユーザーに割り当てられます。ただし、アクセラレーターを削除すると、アクセラレーターに割り当てられた静的 IP アドレスが失われます。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、使用した分に対してのみ料金が発生します。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、AWS Global Accelerator 料金を参照してください。

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

AWS Global Accelerator では、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します。リスナーは、TCP プロトコルと UDP 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、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。

必要に応じて、リスナーのクライアントアフィニティを設定できます。クライアントアフィニティにより、Global Accelerator は特定のソース (クライアント) IP アドレスのユーザーからのすべてのリクエストを同じエンドポイントリソースにルーティングします。このオプションを選択すると、ユーザーのクライアントアフィニティが維持されます。

内容

- 標準リスナーを追加する
- 標準リスナーを編集する
- 標準リスナーを削除する
- Global Accelerator でのクライアントアフィニティの仕組み

標準リスナーを追加する

このセクションでは、AWS Global Accelerator コンソールで標準リスナーを作成する手順について説明します。コンソールの代わりに API オペレーションを使用してこのタスクを完了するには、「AWS Global Accelerator API Reference」の「`CreateListener`」を参照してください。

リスナーを追加するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [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. 必要に応じて、クライアントアフィニティを有効にすることを選択します。リスナーに対するクライアントアフィニティとは、Global Accelerator が特定のソース (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ようにす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から [ソース IP] を選択します。

   デフォルトは [None] です。つまり、クライアントアフィニティが有効になっていず、Global Accelerator はリスナーのエンドポイントグループ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、「Global Accelerator でのクライアントアフィニティの仕組み」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

このセクションでは、AWS Global Accelerator コンソールで標準リスナーを編集する手順について説明します。コンソールの代わりに API オペレーションを使用してこのタスクを完了するには、「AWS Global Accelerator API Reference」の「`UpdateListener`」を参照してください。

標準リスナーを編集するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [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、[リスナーの編集] を選択します。
4. [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. 必要に応じて、クライアントアフィニティを有効にすることを選択します。リスナーに対するクライアントアフィニティとは、Global Accelerator が特定のソース (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ようにす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から [ソース IP] を選択します。

   デフォルトは [None] です。つまり、クライアントアフィニティが有効になっていず、Global Accelerator はリスナーのエンドポイントグループ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、「Global Accelerator でのクライアントアフィニティの仕組み」を参照してください。
6. [Save] を選択します。

標準リスナーを削除する

このセクションでは、AWS Global Accelerator コンソールで標準リスナーを削除する手順について説明します。コンソールの代わりに API オペレーションを使用してこのタスクを完了するには、「AWS Global Accelerator API Reference」の「`DeleteListener`」を参照してください。

リスナーを削除するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [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、[削除] を選択します。
4. 確認ダイアログボックスで、[削除] を選択します。

Global Accelerator でのクライアントアフィニティの仕組み

標準アクセラレーター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、Global Accelerator が特定のソース (クライアント) IP アドレスのユーザーからのすべてのリクエストを同じエンドポイントリソースに送信するようにクライアントアフィニティを設定できます。このオプションを選択すると、ユーザーのクライアントアフィニティが維持されます。

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] に設定され、Global Accelerator はリスナーのエンドポイントグループ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。Global Accelerator リソースのクライアントアフィニティを [なし] に設定すると、Global Accelerator はソース IP、ソースポート、送信先 IP、送信先ポート、プロトコルの 5 つのタプルプロパティ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異なるポートを使用して Global Accelerator に接続し、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が常に同じエンドポイントにルーティングされるようにすることはできません。

接続するたびに、ソース IP アドレスで識別される特定のユーザー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 [ソース IP] に設定します。このオプションを指定すると、Global Accelerator はソース IP と送信先 IP の 2 つのタプルプロパティ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。さらに、Global Accelerator は、同じソース IP アドレスを持つすべての接続を同じエンドポイントグループにルーティングすることで、クライアントアフィニティを尊重します。

場合によっては、インターネットトラフィックルーティングの変動によって発生するネットワークメンテナンスや中断により、クライアントトラフィックが異なる Global Accelerator エッジロケーションに移行する可能性があります。この場合、クライアントトラフィックを提供するエッジロケーションが別の AWS リージョンを優先する場合、クライアントアフィニティは維持されません。

さらに、アクセラレーターでエンドポイントの重みを設定すると、特定の限られたシナリオでは、可用性を確保するために Global Accelerator がそれらの重みをオーバーライドすることに注意してください。Global Accelerator が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ロードバランシングする場合、特定の状況では、クライアントトラフィックの可用性を維持するか、エンドポイントの重みに従うかを選択する必要があります。例えば、クライアントの IP アドレスが保存されているアクセラレーターでは、接続の衝突を避けるために Global Accelerator がエンドポイントの重み設定を上書きする必要があります。

AWS Global Accelerator の標準アクセラレーター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 で登録された 1 つ以上の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ーにリスナーを追加するときは、Global Accelerator がトラフィックを送信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 リージョンにある必要があります。ブルー/グリーンデプロイテストなど、さまざまな目的でさまざまな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状態に基づいて、標準アクセラレーターのエンドポイントグループにトラフィックをルーティングします。必要があれば、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。これを行うには、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 (ダイヤルアップ) または削減 (ダイヤルダウン) します。この割合は、Global Accelerator がエンドポイントグループに既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。

Global Accelerator のヘルスチェック設定は、エンドポイントグループごとに定義できます。ヘルスチェック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状態をポーリングおよび検証するための要件を変更できます。Network Load Balancer および Application Load Balancer 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行います。

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状態を継続的にモニタリングし、正常なアクティブなエンドポイントにのみリクエストをルーティングします。詳細については アクセラレーターのヘルスチェックアクセスを確保する を参照してください。正常なエンドポイントがない場合、Global Accelerator はリクエストをすべてのエンドポイントに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ー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。Global Accelerator で API オペレーションを使用する場合は、「AWS Global Accelerator API Reference」を参照してください。

内容

- 標準エンドポイントグループを追加する
- 標準エンドポイントグループを編集する
- 標準エンドポイントグループを削除する
- トラフィックダイヤルを使用してリージョンへ送信するトラフィックフローを調整する
- 制限されたポートまたは接続コリジョンのリスナーポートを上書きする
- アクセラレーターのヘルスチェックアクセスを確保する

標準エンドポイントグループを追加する

AWS Global Accelerator コンソールで、または API オペレーションを使用してエンドポイントグループを操作します。エンドポイントグループからのエンドポイントをいつでも追加または削除できます。

このセクションでは、AWS Global Accelerator コンソールで標準エンドポイントグループを追加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 API Reference」を参照してください。

標準エンドポイントグループを追加するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [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] 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. [エンドポイントの追加] を選択します。
5. リスナーのセクションで、ドロップダウンリストから 1 つを選択して、エンドポイントグループのリージョンを指定します。
6. 必要に応じて、[トラフィックダイヤル] に 0 から 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。この割合は、このエンドポイントグループに既に送信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し、エンドポイント上の特定のポートにトラフィックを再ルーティングするために使用されるリスナーポートをオーバーライドするには、[ポートオーバーライドの設定] を選択します。詳細については、「制限されたポートまたは接続コリジョンのリスナーポートを上書きする」を参照してください。
8. 必要に応じて、EC2 インスタンスと 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、[ヘルスチェックの設定] を選択します。詳細については、「アクセラレーターのヘルスチェックアクセスを確保する」を参照してください。
9. オプションで、[エンドポイントグループの追加] を選択して、このリスナーまたは他のリスナーにさらにエンドポイントグループを追加します。
10. [エンドポイントの追加] を選択します。

標準エンドポイントグループを編集する

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編集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 API Reference」を参照してください。

エンドポイントグループを編集するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [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] 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. [エンドポイントグループの編集] を選択します。
5. [エンドポイントグループの編集] 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、[ヘルスチェックの設定] を選択してヘルスチェック設定を変更します。
6. [Save] を選択します。

標準エンドポイントグループを削除する

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 API Reference」を参照してください。

標準エンドポイントグループを削除するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [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] タブで、リスナーを選択します。
4. [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んだ後、[削除] を選択します。
5. 確認ダイアログボックスで、[削除] を選択します。

トラフィックダイヤルを使用してリージョンへ送信するトラフィックフローを調整する

標準エンドポイントグループごとに、エンドポイントグループ (AWS リージョン) に送信されるトラフィックの割合を制御するようにトラフィックダイヤルを設定できます。この割合は、リスナー全体の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向けら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を変更すると、更新された設定は新しい接続にのみ適用されることを注意してください。現在のトラフィックフローを調整するために、既存の接続は終了する必要はありません。

デフォルトでは、トラフィックダイヤルはアクセラレーター内のすべてのリージョンエンドポイントグループで 100 (つまり 100%) に設定されています。トラフィックダイヤルを使用することで、さまざまな AWS リージョンにわたる新しいリリースのパフォーマンステストやブルー/グリーンデプロイテストなどを簡単に実行できます。

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を説明する例をいくつか示します。

リージョン別にアプリケーションをアップグレードする

リージョン内のアプリケーションをアップグレードしたり、メンテナンスを行ったりする場合は、まずトラフィックダイヤルを 0 に設定して、リージョンへのトラフィックを遮断します。作業を完了し、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、トラフィックを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

この例では、2 つのリージョン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するときに、トラフィックフローがどのように機能するかを示します。アクセラレーターには 2 つのエンドポイントグループがあると仮定します。1 つは us-west-2 リージョン用、もう 1 つは us-east-1 リージョン用で、その場合、トラフィックダイヤルはエンドポイントグループごとに 50% に設定されています。

次に、アクセラレーターへのリクエストが 100 件あり、そのうち 50 件が米国東部から、50 件が米国西部から送信されると仮定します。アクセラレーターは、次のようにトラフィックを送信します:

- 両方の最初の 25 件のリクエスト (合計 50 件のリクエスト) は、近くのエンドポイントグループから処理されます。つまり、25 件のリクエストが us-west-2 のエンドポイントグループに送信され、他の 25 件が us-east-1 のエンドポイントグループに送信されます。
- 次の 50 件のリクエストは、向こう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 件のリクエストは us-west-2 によって処理され、西海岸からの次の 25 件のリクエストは us-east-1 によって処理されます。

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ています。ただし、それぞれのエンドポイントは両方のリージョンからのトラフィックを混同して受信します。

ロード共有のマルチリージョンアーキテクチャ

トラフィックダイヤルとエンドポイントの重みを設定して、複雑なシナリオを実装し、アプリケーションエンドポイント間のロード共有を設定することもできます。これらの Global Accelerator 機能を使用すると、アクティブ/アクティブ設定やアクティブ/スタンバイ設定などのマルチリージョンアーキテクチャでアプリケーションをデプロイして実行できます。詳細な情報と具体的な例については、次のブログ記事を参照してください: Deploying multi-Region applications in AWS using AWS Global Accelerator

制限されたポートまたは接続コリジョンのリスナーポートを上書きする

デフォルトでは、アクセラレーターは、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 リージョン内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。例えば、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、アクセラレーターはエンドポイント上のそれらのポートにトラフィックをルーティングします。

ただし、エンドポイントグループを追加または更新するときに、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。

ポートの上書きを使用する利点の 1 つは、Global Accelerator で断続的な接続問題を引き起こし、特定のシナリオで TCP 接続時間の遅延が発生する可能性がある接続の衝突を回避できることです。これらの衝突は、ユーザーが (同じソース IP とソースポートを使用して) Global Accelerator のリソースにアクセスするときに発生する可能性があります。アクセラレーターでポート上書きを設定することで、衝突を防ぎ、遅延を回避できます。詳細については、「TCP 接続時間の遅延につながる接続の衝突を回避する方法」を参照してください。

ポートを上書きすると、制限されたポートでリッスンする際の問題を回避することもできます。エンドポイントでスーパーユーザー (ルート) 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 やその他の UNIX 系システムでは、制限されたポート (1024 未満の TCP または UDP ポート) でリッスンするには、スーパーユーザ権限が必要です。リスナーの制限付きのポートをエンドポイントの制限のないポートにマッピングすることで、この問題を回避できます。Global Accelerator の後ろにあるエンドポイントでルートアクセスなしでアプリケーションを実行している間、制限されたポートでトラフィックを受け入れることができます。例えば、リスナーポート 443 をエンドポイントポート 8443 に上書きすることができます。

ポートオーバーライドごとに、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を追加する」を参照してください。

ポートの上書きを作成する際は、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の範囲と重複することはできません。ポート上書きで指定したエンドポイントポートは、アクセラレーター用に設定したリスナーポートの範囲に含めることはできません。例えば、アクセラレーターのリスナーが 2 人いて、それらのリスナーのポート範囲をそれぞれ 100 ~ 199 と 200 ~ 299 と定義したと仮定します。ポート上書きを作成する場合、例えば、エンドポイントポート (210) が定義したリスナーポート範囲 (200 ~ 299) に含まれているため、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。
- エンドポイントポートが重複していません。アクセラレーターの 1 つのポート上書きでエンドポイントポートを指定している場合、別のリスナーポートからのポート上書き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。例えば、リスナーポート 80 からエンドポイントポート 90 へのポート上書きと、リスナーポート 81 からエンドポイントポート 90 への上書きを指定することはできません。
- ヘルスチェックは引き続き元のポートを使用します。ヘルスチェックポートとして設定されたポートにポート上書きを指定しても、ヘルスチェックは上書きポートではなく元のポートを使用します。例えば、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 へのポート上書きも指定すると仮定します。ヘルスチェックは、エンドポイントポート 80 が引き続き使用します。ただし、ポート 80 経由で着信するユーザートラフィックは、エンドポイントのポート 480 に送信されます。

  この動作は、Network Load Balancer、Application Load Balancer、EC2 インスタンス、および Elastic IP アドレスエンドポイント間の整合性を維持します。Network Load Balancer と Application Load Balancer は、Global Accelerator でポート上書きを指定したときに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 が EC2 インスタンスと Elastic IP アドレスエンドポイントの異なる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一貫性がありません。
- セキュリティグループ設定では、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着信を許可していることを確認します。例えば、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で、ポート 1433 のインバウンドトラフィックが許可されていることを確認してください。

アクセラレーターのヘルスチェックアクセスを確保する

標準アクセラレーターの各リスナーは、正常、およびアクティブなエンドポイントにのみリクエストをルーティングします。エンドポイントを追加する場合、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。AWS Global Accelerator は、ステータスをテストするために、定期的に標準アクセラレーターのすべてのエンドポイントにヘルスチェックリクエストを送信します。Global Accelerator は、これらの定期的なヘルスチェックを自動的に実行します。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。

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 は受信クライアントリクエストをエンドポイントグループ内のすべてのエンドポイントにルーティングします。詳細については、「異常なエンドポイントに対するフェイルオーバーの仕組み」を参照してください。

ヘルスチェックの仕組みの詳細とヘルスチェックの使用に関するガイダンスは、エンドポイントリソースのタイプによって異なります。このトピックでは、Global Accelerator でヘルスチェックオプションを更新する手順 (EC2 インスタンスまたは Elastic IP アドレスエンドポイントに適用) など、さまざまなエンドポイントタイプのヘルスチェックを操作する方法について説明します。

アクセラレーターのヘルスチェックアクセスを確保する

EC2 インスタンスまたは Elastic IP アドレスエンドポイントでヘルスチェックへのアクセスが正常に完了するようにするには、ルーターとファイアウォールのルールで Amazon 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が許可されていることを確認してください。Route 53 ヘルスチェッカーに関連する IP アドレス範囲のリストを確認するには、「Amazon Route 53 デベロッパーガイド」の「Route 53 サーバーの IP アドレス範囲」を参照してください。

Global Accelerator のヘルスチェックは、Route 53 のヘルスチェックのトラフィックを受信することで機能し、エンドポイントグループの設定されたヘルスチェックポートに転送されます。通常、ヘルスチェック用に設定されたポートはリスナー設定と一致します。代わりにヘルスチェック用に別のポートを設定する場合は、セキュリティグループ設定を確認して、ポートでパブリックトラフィックを許可していないことを確認します。

例えば、リスナーがポート 80 で設定されている場合、ヘルスチェックポートも 80 です。ポート 83 などの別のポートでヘルスポートを設定する場合は、Route 53 ヘルスチェックの IP アドレス範囲内の IP アドレスからのトラフィックのみポート 83 でのトラフィックを許可するようにセキュリティグループを設定してください。

異なるエンドポイントタイプのヘルスチェックガイダンス

アクセラレーターのエンドポイントタイプごとに指定するヘルスチェックに関するガイドラインについては、このセクションの情報を参照してください。

さらに、HTTP ワークロードを使用するエンドポイントに対して選択したヘルスチェックがアプリケーションの全体的な状態を表し、前述のセクションで説明されているヘルスチェックへのアクセスを確実にするためのガイダンスに従っていることを確認してください。「ヘルスチェックのセキュリティとアクセスを確保します」。

以下のガイドラインは、指定された各エンドポイントタイプに適用されます:

- Network Load Balancer または Application Load Balancer エンドポイントの場合、次の点に注意してください:
  - Global Accelerator で選択した「ヘルスチェックオプション」は、エンドポイントとして追加した Network Load Balancer または Application Load Balancer には影響しません。つまり、Global Accelerator で指定したヘルスチェックオプションは、Amazon EC2 および Elastic IP アドレスのヘルスチェックに使用されますが、ロードバランサーエンドポイントのヘルスチェックには使用されません。

    ロードバランサーエンドポイントの場合は、Elastic Load Balancing 設定オプションを使用してヘルスチェックを設定します。詳細については、「ターゲットグループのヘルスチェック」を参照してください。
  - Global Accelerator は、少なくとも 1 つの正常なアベイラビリティーゾーンがある場合、Network Load Balancer または Application Load Balancer の状態を正常と見なします。アベイラビリティーゾーン内のすべてのロードバランサーターゲットグループが正常である場合、アベイラビリティーゾーンは正常です。詳細については、「ターゲットグループのヘルスチェック」を参照してください。
- 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、次の点に注意してください:
  - EC2 インスタンスまたは Elastic IP アドレスエンドポイントを TCP で設定されたリスナーに追加するときは、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、ヘルスチェックのポートを指定しない場合、Global Accelerator はアクセラレーターに指定したリスナーポートを使用します。
  - UDP リスナーでこれらのエンドポイントタイプを追加すると、Global Accelerator はリスナーポートと TCP プロトコルをヘルスチェックに使用するため、エンドポイントに TCP サーバーが必要です。

各エンドポイントの TCP サーバー用に設定したポートが、Global Accelerator でヘルスチェックに指定したポートと同じであることを確認します。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状態に関係なく、エンドポイントを異常としてマークします。

- 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用にポートを設定するときは、「セキュリティとアクセスに関するガイダンス」に従ってください。

ヘルスチェックオプションを設定する

アクセラレーターのヘルスチェックオプションを設定するには、アクセラレーターを作成するとき、またはエンドポイントグループを編集するときに、次のオプションを 1 つ以上指定します。

エンドポイントグループに次のヘルスチェックオプションを追加できます。

ヘルスチェックポート

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。

ヘルスチェックポートのポート上書きを設定できないことに注意してください。

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。

ヘルスチェック間隔

エンドポイントの各ヘルスチェック間の秒単位の間隔。

しきい値数

非正常なインスタンスが正常である、またはその逆と見なすまでに必要なヘルスチェックの連続回数。

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

AWS Global Accelerator の標準アクセラレーターのエンドポイントは、Network Load Balancer、Application Load Balancer、Amazon EC2 インスタンス、または Elastic IP アドレスで

す。AWS Global Accelerator では、静的 IP アドレスはクライアントへの単一の連絡先として機能し、標準のアクセラレーターを使用すると、Global Accelerator は正常なエンドポイントに着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するリスナーに指定したポート (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ルーティングします。

各エンドポイントグループには複数のエンドポイントを含める可能性があります。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。

> **Important**
>
> デュアルスタックとして設定するアクセラレーター (つまり、IPv4 および IPv6 をサポートするアクセラレーター) では、デュアルスタックもサポートするエンドポイントのみを追加する必要があります。Network Load Balancer、Application Load Balancer、Amazon EC2 インスタンスは、デュアルスタックエンドポイントとして追加できます。

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状態を継続的にモニタリングします。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 にトラフィックをルーティングする正常なエンドポイントがない場合、トラフィックは AWS リージョン 内のすべてのエンドポイントにルーティングされます。

内容

- アクセラレーターエンドポイントとして追加するリソースの要件
- 標準エンドポイントを追加する
- 標準エンドポイントを編集する
- 標準エンドポイントを削除する
- エンドポイントの重みがトラフィックボリュームを管理する仕組み
- 異常なエンドポイントに対するフェイルオーバーの仕組み
- TCP 接続時間の遅延につながる接続の衝突を回避する方法

アクセラレーターエンドポイントとして追加するリソースの要件

AWS Global Accelerator の標準アクセラレーターのエンドポイントとして追加できるさまざまなタイプのリソースには、以下の要件と制限があります。

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する場合は、追加の要件に注意する必要があります。詳細については、「クライアント IP アドレスの保存による移行エンドポイント」を参照してください。

注: アクセラレーターの背後にあるエンドポイントとして追加したリソースを終了または削除する前に、Global Accelerator エンドポイントグループからエンドポイントを削除することを推奨します。

Application Load Balancer エンドポイント

- Application Load Balancer エンドポイントは、内部またはインターネット接続を問いません。
- デュアルスタック Application Load Balancer はエンドポイントとして追加できます。
- Global Accelerator は、AWS リージョン 内で実行される Application Load Balancer のみをサポートします。Global Accelerator は、ローカルゾーンのエンドポイントとして実行される Application Load Balancer をサポートしていません。

Network Load Balancer エンドポイント

- Network Load Balancer のエンドポイントは、内部またはインターネット接続を問いません。
- デュアルスタック Network Load Balancer をエンドポイントとして追加できますが、いくつかの制限があります:
  - デュアルスタックアクセラレーターの場合、デュアルスタック Network Load Balancer を追加すると、Network Load Balancer にはターゲットタイプが `ip` のターゲットグループ、またはターゲットタイプが `instance` および IP アドレスタイプが `ipv6` のターゲットグループを持つことはできません。
  - IPv4 アクセラレーターの場合、デュアルスタック Network Load Balancer を追加すると、Global Accelerator でエンドポイントのクライアント IP アドレスの保存を有効にすることはできません。
- Global Accelerator は、AWS リージョン 内で実行される Network Load Balancer のみをサポートします。Global Accelerator は、ローカルゾーンでエンドポイントとして動作する Network Load Balancer をサポートしていません。
- Network Load Balancer エンドポイントでは、接続の衝突を避けるためにロードバランサーのクロスゾーントラフィックを無効にすることをお勧めします。これにより、TCP 接続時間が長くなる可能性があります。詳細については、「TCP 接続時間の遅延につながる接続の衝突を回避する方法」を参照してください。

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
  は、C1、CC1、CC2、CG1、CG2、CR1、CS1、G1、G2、HI1、HS1、M1、M2、M3、または T1 のいずれかにすることはできません。
- EC2 インスタンスは、特定の AWS リージョン のエンドポイントとしてサポートされています。詳細については、「AWS Global Accelerator のための AWS リージョン の可用性」を参照してください。

  Global Accelerator は、AWS リージョン 内の EC2 インスタンスのみをサポートします。Global Accelerator は、ローカルゾーンのエンドポイントとして Elastic IP アドレスへのルーティングをサポートしていません。
- 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 の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 アドレスを持つ同じ VPC に別のインスタンスを作成し、ヘルスチェックが合格すると、Global Accelerator はトラフィックを新しいエンドポイントにルーティングします。
- デュアルスタック EC2 インスタンスはエンドポイントとして追加できます。ただし、当インスタンスにはプライマリ IPv6 Elastic Network Interface (ENI) がアタッチされている必要があります。詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「ネットワークインターフェースの動作」を参照してください。

Elastic IP アドレス

- デュアルスタックの Elastic IP アドレスをエンドポイントとして追加することはできません。

すべてのエンドポイントについて、Global Accelerator の背後にあるリソースをエンドポイントとして設定する場合、同じエンドポイントにインターネット経由で直接トラフィックを送信しないことを推奨します。直接トラフィックを送信すると、接続の衝突問題が発生する可能性があります。

さらに、クロスアカウントサポートを設定しない限り、アクセラレーターのエンドポイントとして追加するリソースとアクセラレーター自体は同じアカウントによって所有される必要があることに注意してください。ただし、ロードバランサーエンドポイントの後ろにあるターゲットインスタンスは、異なるアカウントによって所有できます。このシナリオでは、ターゲットインスタンスを所有するアカウントには、ロードバランサーとアクセラレーターを所有するアカウントが所有するサブネットにアクセスするアクセス許可を付与する必要があります。詳細については、「Global Accelerator でクロスアカウントアクセスを設定する」を参照してください。

標準エンドポイントを追加する

エンドポイントグループにエンドポイントを追加して、トラフィックをリソースに誘導できるようにします。標準エンドポイントを編集することで、エンドポイントの重みを変更できます。または、エンドポイントをエンドポイントグループから削除することで、アクセラレーター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 はそのリソースにトラフィックを送信できなくなります。

まずリソースを作成し、Global Accelerator 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。Global Accelerator がサポートするエンドポイントタイプと設定の詳細については、アクセラレーターエンドポイントとして追加するリソースの要件 を参照してください。

エンドポイントグループでエンドポイントを追加または削除する理由の 1 つは使用状況です。例えば、アプリケーションに対する需要が増加すると、より多くのリソースを作成できます。次に、1 つ以上のエンドポイントグループに複数の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、リクエストを追加し、エンドポイントが最初のヘルスチェックに合格するとすぐに、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ます。

エンドポイントの重みを調整してエンドポイントへのトラフィックを管理し、エンドポイントへのトラフィックを比例的に増減させることができます。詳細については、「エンドポイントの重みがトラフィックボリュームを管理する仕組み」を参照してください。

注: クライアント IP アドレスの保存でエンドポイントを追加しようとする場合は、まず AWS Global Accelerator でクライアント IP アドレスを保存する の情報を確認してください。

このセクションでは、AWS Global Accelerator コンソールにエンドポイントを追加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 Reference」を参照してください。

標準エンドポイントを追加するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [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] セクションの [リスナー ID] で、リスナーの ID を選択します。
4. [エンドポイントグループ] セクションの[エンドポイントグループ ID] 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 ID を選択します。
5. [編集] を選択します。

6. [エンドポイント] セクションで、[エンドポイントの追加] を選択します。
7. [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は、リストにアイテムはありません。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、ここにある手順に戻り、リストからリソースを選択します。

   > **Note**
   >
   > デュアルスタックアクセラレーターがある場合は、デュアルスタックエンドポイントを追加する必要があります。Network Load Balancer、Application Load Balancer、Amazon EC2 インスタンスは、デュアルスタックエンドポイントとして追加できます。

8. 必要に応じて、[重み] に 0 から 255 の数字を入力し、このエンドポイントへのトラフィックをルーティングする際の重みを設定します。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、すべてのフィールドの重みは 128 です。詳細については、「エンドポイントの重みがトラフィックボリュームを管理する仕組み」を参照してください。
9. 必要に応じて、エンドポイントのクライアント IP アドレスの保存を有効にします。[クライアント IP アドレスの保存] で、[アドレスの保存] を選択します。詳細については、「AWS Global Accelerator でクライアント IP アドレスを保存する」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に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、必要なセキュリティ設定がすべて更新され、許可リストにユーザークライアント IP アドレスが含まれていることを確認してください。

10. [Add endpoint] (エンドポイントの追加) を選択します。

標準エンドポイントを編集する

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編集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 Reference」を参照してください。

標準エンドポイントを編集するには

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、「エンドポイントの重みがトラフィックボリュームを管理する仕組み」を参照してください。

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [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] セクションの [リスナー ID] で、リスナーの ID を選択します。
4. [エンドポイントグループ] セクションの [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. [エンドポイントの編集] を選択します。
6. [エンドポイントの編集] ページで更新を行い、[保存] を選択します。

標準エンドポイントを削除する

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削除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 Reference」を参照してください。

エンドポイントをサービス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。エンドポイントが削除されるとき、エンドポイントグループから削除されますが、それ以外の場合はエンドポイントには影響しません。Global Accelerator は、エンドポイントグループから削除すると、エンドポイントへのトラフィックの送信をすぐに停止します。エンドポイントは、現在のすべてのリクエストが完了するまで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たら、エンドポイントをエンドポイントグループに戻すことができます。

注: アクセラレーターの背後にあるエンドポイントとして追加したリソースを終了または削除する前に、Global Accelerator エンドポイントグループからエンドポイントを削除することを推奨します。

エンドポイントを削除するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [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] セクションの [リスナー ID] で、リスナーの ID を選択します。

4. [エンドポイントグループ] セクションの [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. [エンドポイントの削除] を選択します。
6. 確認ダイアログボックスで、[削除] を選択します。

エンドポイントの重みがトラフィックボリュームを管理する仕組み

加重ルーティングでは、エンドポイントグループ内の特定のリソース (エンドポイント) 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、ロードバランシングやアプリケーションの新しいバージョンのテストなど、いくつかの方法で役立ちます。

重みは、Global Accelerator が標準アクセラレーターのエンドポイントに向けるトラフィックの割合を決定するために設定できる値です。エンドポイントには、Network Load Balancer、Application Load Balancer、Amazon EC2 インスタンス、または Elastic IP アドレスを使用できます。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、各エンドポイントの重みと合計の比率に基づいてトラフィックをエンドポイントに送信します。デフォルトでは、エンドポイントの重みは 128 に設定されています。これは最大値の 255 の半分です。

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量に対応する相対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、重みの最大値の半分である 255 です。Global Accelerator は、グループ内のすべてのエンドポイントの合計重みに比例して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:

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

例えば、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、重みをそれぞれ 1 と 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、他のエンドポイントは 255/256 (255/1+255) を取得します。重みを変更することで、トラフィックボリュームのバランスを各エンドポイントに段階的に変更できます。エンドポイントへのトラフィック送信を停止するには、リソースの重みを 0 に変更します。

アクセラレーターでエンドポイントの重みを設定しても、特定の限定されたシナリオでは、Global Accelerator がそれらの重みを上書きして可用性を確保することに注意してください。つまり、Global Accelerator が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ロードバランシングする場合、特定の状況では、クライアントトラフィックの可用性を維持するか、エンドポ

イントの重みに従うかを選択する必要があります。例えば、クライアントの IP アドレスが保存されているアクセラレーターでは、接続の衝突を避けるために Global Accelerator がエンドポイントの重み設定を上書きする必要があります。

異常なエンドポイントに対するフェイルオーバーの仕組み

エンドポイントグループに重みが 0 より大きい正常なエンドポイントがない場合、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にフェイルオーバーしようとします。このフェイルオーバーにおいて、Global Accelerator はトラフィックダイヤルの設定を無視することに注意してください。したがって、例えば、エンドポイントグループでトラフィックダイヤルが 0 に設定されている場合、Global Accelerator はフェイルオーバーの試行にそのエンドポイントグループを含めます。

Global Accelerator は、最も近い 3 つのエンドポイントグループ (つまり AWS リージョン) を試した後に重みが 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、クライアントに最も近いエンドポイントグループ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。つまり、[開くのに失敗] します。

次の点に注意してください。

- フェイ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ある場合があります。
- 最も近いエンドポイントグループは、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、アカウントのトラフィックダイヤル設定を考慮するためです。

例えば、2 つのエンドポイントがあり、1 つは正常でもう 1 つは異常で、それぞれの重みを 0 より大きい値に設定していると仮定します。この場合、Global Accelerator は正常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。ただし、唯一の正常なエンドポイントの重みを 0 に設定すると仮定します。次に、Global Accelerator は 3 つの追加のエンドポイントグループを試行して、重みが 0 より大きい正常なエンドポイントを見つけます。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のランダムエンドポイントにトラフィックをルーティングします。

回復を行うと、つまりリージョンが再び正常になると、Global Accelerator は通常のルーティング動作に戻ります。つまり、通常、ルーティングは正常なエンドポイントに戻り、約 30 秒ほどでゼロに設定されないトラフィックダイヤルが使用されます。ただし、確立されたアクティブな接続は移動されないことに注意してください。接続がクライアントまたはサーバーによってリセットされるまで、

またはクライアントが新しい接続を行うまで、ゼロウェイトリージョンにルーティングされ続けます。

TCP 接続時間の遅延につながる接続の衝突を回避する方法

断続的な接続の問題は、AWS Global Accelerator の接続の衝突によって発生する可能性があります。これは、ユーザー (同じ送信元 IP と送信元ポートを持つ) が特定のシナリオで Global Accelerator のリソースにアクセスする場合に発生する可能性があります。衝突により、アクセラレーターを通過するトラフィックの TCP 接続時間が遅延する可能性があります。

これらの遅延を回避するには、アクセラレーターをポート上書きで設定します。これは、Global Accelerator の機能で、着信トラフィックをアクセラレーターエンドポイントの別の送信先ポートにルーティングできます。このセクションのガイダンスに従って、ポートオーバーライドを使用して接続の衝突を防ぎ、TCP 接続時間の遅延を防ぐ方法について説明します。

接続の衝突を引き起こす可能性のあるシナリオ

Global Accelerator には、接続の衝突や TCP 接続時間の遅延につながる可能性のあるシナリオが 3 つあります。

- 複数のアクセラレーターを持つエンドポイントと同じリソースを設定します。
- Global Accelerator の後ろにあるエンドポイントとしてリソースを設定し、インターネット経由でエンドユーザーから同じリソースにトラフィックを直接送信することもできます。
- クロスゾーントラフィック用に Network Load Balancer エンドポイントを設定します。

Network Load Balancer エンドポイントの場合、接続の衝突を避けるために、ロードバランサーのクロスゾーントラフィックを無効にすることをお勧めします。詳細については、「Network Load Balancer ユーザーガイド」の「TCP 接続の遅延」を参照してください。

その他のシナリオでは、衝突を防ぐために、エンドポイントグループでポート上書き機能を使用することをお勧めします。ポート上書きを使用すると、Global Accelerator リスナーポートをエンドポイントリソースの異なる宛先ポート番号にマッピングできます。リスナーポートは、デフォルトでエンドポイントリソースで同じポート番号を使用します。ポート上書きを使用すると、アクセラレーターは同じユーザー (ソース IP とソースポートを使用) から同じエンドポイントにトラフィックをルーティングできますが、異なる送信先ポート番号を使用することで、衝突を回避できます。

次のセクションでは、接続の衝突を避けるためにポート上書きを設定する方法の各シナリオの具体的な例を示します。ポート上書きの設定の詳細については、制限されたポートまたは接続コリジョンのリスナーポートを上書きする を参照してください。

ポート上書きを使用して接続の衝突を防ぐ方法

デフォルトでは、アクセラレーターは、リスナーの作成時に指定したのと同じプロトコルと同じ送信先ポート範囲を使用して、AWS リージョン でユーザートラフィックをエンドポイントにルーティングします。ただし、オプションでリスナーポートのポート番号マッピングを上書きすることもできます。つまり、リスナーポート番号をマッピングして、エンドポイント上の別の送信先ポート番号にトラフィックをルーティングできます。

例えば、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、デフォルトでアクセラレータはエンドポイント上の同じポート 80 と 443 にトラフィックをルーティングします。ただし、ポートオーバーライド機能を使用すると、アクセラレーターはこれらのポートに着信するトラフィックを、8080 や 8443 などのエンドポイントの異なるポートにルーティングできます。

同じリソースが設定されている 2 つ (またはそれ以上) のアクセラレーターでリスナーに異なるポートマッピングを作成することで、アクセラレーターごとに別々の送信先ポート番号を使用し、衝突を回避できます。

例えば、Accelerator-A と Accelerator-B があり、それぞれに TCP とポート 443 用のリスナーが設定されていると仮定します。Accelerator-A のリスナーがポート 443 を 8443 にマッピングし、Accelerator-B のリスナーがポート 443 を 9443 にマッピングするようにポート上書きを設定できます。次に、例えば、ポート 8443 と 9443 の両方をリッスンするように Application Load Balancer エンドポイント ALB-1234 を設定します。その後、同じユーザー IP アドレスからポート 443 (両方のアクセラレーターのリスナー) に着信するトラフィックは ALB-1234 に到着し、接続の衝突や TCP 接続時間の遅延は発生しません。

この例のトラフィックパスを次に示します:

```
Accelerator-A [listener: tcp,443] # Endpoint-Group [port-override:
443#8443] # ALB-1234 (listener: HTTPS,8443)

Accelerator-B [listener: tcp,443] # Endpoint-Group [port-override:
443#9443] # ALB-1234 (listener: HTTPS,9443)
```

同様の方法でポート上書きを使用すると、アクセラレーターのリスナーポート番号のデフォルトマッピングを上書きすることで、直接ユーザートラフィックとアクセラレーターの両方からアクセスされるリソースの接続の衝突を防ぐことができます。このシナリオでの衝突を防ぐには、以下を実行します:

1. リソースが直接トラフィックをリッスンするポートを決定します。

2. アクセラレーターのリスナーを設定してデフォルトのポートを上書きし、リソースのリスナーを設定してそのポートでアクセラレータートラフィックをリッスンします。

例えば、アクセラレーターがポート 443 をポート 8443 にマッピングするためのリスナーのポートオーバーライドを設定できます。これで、例えば、ポート 8443 でアクセラレータトラフィックをリッスンし、ポート 443 で直接トラフィックをリッスンするように Application Load Balancer エンドポイントを設定できます。この設定では、同じユーザーの IP アドレスからのトラフィックに対する Application Load Balancer の接続の衝突を回避できます。

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

この章では、AWS Global Accelerator のカスタムルーティングアクセラレーターの仕組みと、カスタムルーティングアクセラレーターのアクセラレーター、リスナー、エンドポイントグループ、VPC サブネットエンドポイントを設定する方法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ーを使用すると、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くの送信先間で特定の Amazon EC2 インスタンスに直接マッピングできます。また、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が向上します。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 インスタンスと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ーのエンドポイントは Amazon VPC (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ーは、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ーを作成する場合、1 つまたは複数の 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、「Global Accelerator でのカスタムルーティングアクセラレーターの仕組み」を参照してください。

> **Note**
>
> 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ーを作成します。詳細については、「AWS Global Accelerator での標準アクセラレーターの使用」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を設定するには、以下を実行します。

1. カスタムルーティングアクセラレーターを作成するためのガイドラインと要件を確認してください。「カスタムルーティングアクセラレーターのガイドラインと制限」を参照してください。
2. VPC またはサブネットを作成します。Global Accelerator にサブネットを追加した後は、いつでも EC2 インスタンスをサブネットに追加できます。
3. Global Accelerator でアクセラレーターを作成します。カスタムルーティングアクセラレーターのオプションを選択します。

4. Global Accelerator がリッスンするポートの範囲を指定するリスナーを追加します。Global Accelerator が想定されるすべての送信先にマッピングするための十分なポートを持つ広い範囲を含めてください。これらのポートは、次のステップで指定する送信先ポートとは異なります。リスナーポートの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ーのガイドラインと制限 を参照してください。
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ごとに以下を指定します。
   - エンドポイントポート範囲。トラフィックを受信できる送信先 EC2 インスタンスのポートを表します。
   - 各送信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で、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。

以下のセクションでは、カスタムルーティングアクセラレーターの仕組みについて説明し、リスナー、エンドポイントグループ、VPC サブネットエンドポイントなどのカスタムルーティングアクセラレーターとそのコンポーネントを作成および操作する手順を示します。

トピック

- Global Accelerator でのカスタムルーティングアクセラレーターの仕組み
- Global Accelerator でのカスタムルーティングの仕組みの例
- カスタムルーティングアクセラレーターのガイドラインと制限
- AWS Global Accelerator のカスタムルーティングアクセラレーター
- Global Accelerator のカスタムルーティングアクセラレーターのリスナー
- Global Accelerator のカスタムルーティングアクセラレーターのエンドポイントグループ
- Global Accelerator のカスタムルーティングアクセラレーター用 Amazon VPC サブネットエンドポイント

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

AWS Global Accelerator でカスタムルーティングアクセラレーターを使用すると、アプリケーションロジックを使用して、Global Accelerator のパフォーマンス上の利点を得ながら、1 人以上のユーザーを多くの送信先間で特定の送信先に直接マッピングできます。カスタムルーティングアクセラ

レーターは、リスナーポート範囲を Amazon VPC (VPC) サブネットの EC2 インスタンス送信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 アドレスとポート送信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、地理的位置、プレイヤースキル、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オンラインリアルタイムゲームアプリケーションでカスタムルーティングアクセラレーターを使用できます。または、音声、ビデオ、メッセージングセッション用に、特定のメディアサーバーに複数のユーザーを割り当てる VoIP またはソーシャルメディアアプリケーションがある場合があります。

アプリケーションは Global Accelerator API を呼び出し、Global Accelerator ポートと、関連する送信先 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。静的マッピングを保存し、マッチメーキングサービスがそれを使用して特定の送信先 EC2 インスタンスにユーザーをルーティングできます。アプリケーションで Global Accelerator の使用を開始するために、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ーを設定するには、VPC サブネットエンドポイントを選択します。次に、受信接続がマッピングされる送信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をリッスンできるようにします。Global Accelerator は、マッチメーキングサービスがセッションの送信先 IP アドレスとポート番号を、ユーザーに付与する外部 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で動作するか、UDP を使用して高速配信を行い、TCP を使用して信頼性の高い配信を行うことができます。送信先ポート範囲ごとに UDP、TCP、または UDP と TCP の両方を設定することで、各プロトコルの設定を複製することなく、最大限の柔軟性を実現できます。

> **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ー内のすべての VPC サブネット送信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セキュリティを確保するとともに、サブネット内のプライベートな EC2 インスタンスのうち、どの送信先がトラフィックを受信できるかを細かく制御するためのものです。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 (送信先ソケット) 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、「カスタムルーティングアクセラレーターの VPC サブネットエンドポイントを追加する」を参照してください。Global Accelerator API を使用して送信先を指定することもできます。詳細については、「AllowCustomRoutingTraffic」および「DenyCustomRoutingTraffic」を参照してください。

Global Accelerator でのカスタムルーティングの仕組みの例

例えば、Global Accelerator の後ろにある 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のユーザーのグループがやり取りする 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、リスナーポートの範囲を 10001 ~ 20040 に指定し、送信先ポートの範囲を 81 ~ 90 に指定します。us-east-1 には、subnet-1、subnet-2、subnet-3、subnet-4 の 4 つの VPC サブネットがあると仮定します。

この例では、各 VPC サブネットのブロックサイズは /24 であるため、251 個の Amazon EC2 インスタンスをサポートできます。(各サブネットから 5 つのアドレスが予約されており、使用できません。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には、エンドポイントグループの送信先ポートに指定した 81 ~ 90 個のポートが 10 個あります。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 個の送信先ポートを指定しているため、Global Accelerator は EC2 インスタンスへのアクセスに使用できる 10 個のリスナーポートを内部的に関連付けます。簡単に説明すると、リスナーポートのブロックがあり、最初の 10 個のセットはエンドポイントサブネットの最初の IP アドレスから始まり、次の 10 個のリスナーポートのセットには次の IP アドレスが割り当てられるという仕組みです。

> **Note**
>
> マッピングは実際にはこのように予測できませんが、ここではポートマッピングの仕組みを示すためにシーケンシャルマッピングを使用しています。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、「ListCustomRoutingPortMappings」および「ListCustomRoutingPortMappingsByDestination」API オペレーションを使用します。

この例では、最初のリスナーポートは 10001 です。そのポートは、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 に関連付けられています。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 に関連付けられています。次の表は、このマッピング例が最初の VPC サブネットの最後の IP アドレスを経由し、2 番目の VPC サブネットの最初の IP アドレスに続く方法を示しています。

Global Accelerator リスナーポート	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
10006	192.0.2.4	86
10007	192.0.2.4	87
10008	192.0.2.4	88
10009	192.0.2.4	89
10010	192.0.2.4	90
10011	192.0.2.5	81
10012	192.0.2.5	82
10013	192.0.2.5	83
10014	192.0.2.5	84
10015	192.0.2.5	85
10016	192.0.2.5	86
10017	192.0.2.5	87
10018	192.0.2.5	88
10019	192.0.2.5	89

Global Accelerator リスナーポート	VPC サブネット	EC2 インスタンスポート
10020	192.0.2.5	90
...	...	...
12501	192.0.2.244	81
12502	192.0.2.244	82
12503	192.0.2.244	83
12504	192.0.2.244	84
12505	192.0.2.244	85
12506	192.0.2.244	86
12507	192.0.2.244	87
12508	192.0.2.244	88
12509	192.0.2.244	89
12510	192.0.2.244	90
12511	192.0.3.4	81
12512	192.0.3.4	82
12513	192.0.3.4	83
12514	192.0.3.4	84
12515	192.0.3.4	85
12516	192.0.3.4	86
12517	192.0.3.4	87
12518	192.0.3.4	88

Global Accelerator リスナーポート	VPC サブネット	EC2 インスタンスポート
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ーのガイドラインと制限

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に注意してください。

サポートされているエンドポイントの送信先

カスタムルーティングアクセラレーター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。ロードバランサー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ーではサポートされていません。Global Accelerator でサポートされている EC2 インスタンスのタイプは、AWS Global Accelerator の標準アクセラレーターのエンドポイント に記載されています。

カスタムルーティングアクセラレーターを使用すると、Global Accelerator は VPC サブネット上の Amazon EC2 インスタンス上のプライベート IP エンドポイントにのみトラフィックをルーティングできます。ただし、カスタムルーティングを使用しようとするゲームのお客様は、ステートフルセッションに接続する必要がある場合があります。そのためには、お客様が Amazon Elastic Kubernetes Service (EKS) でゲームサーバーを実行すると同時に、特定のコンテナでホストされたセッションは Kubernetes ポッド内で実行されます。

このシナリオでカスタムルーティングを使用するには、エンドポイントが存在するサブネットごとに Global Accelerator が作成する Elastic Network Interface (ENI) を介して Kubernetes ポッドにトラフィックを送信するように VPC-CNI プラグインを設定できます。これは、EKS でカスタムルーティングアクセラレーターを使用する方法です。Amazon Elastic Container Service (ECS) でカスタムルーティングアクセラレーターを使用するとき、同じ設定は機能します。詳細については、次のブログ記事:「AWS Global Accelerator Custom Routing with Amazon Elastic Kubernetes Service」で提供されている詳細な手順を参照してください。

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の静的ポートマッピングをサブネットでサポートされているポート範囲に作成します。特定のサブネットのポートマッピングは一切変更されません。

カスタムルーティングアクセラレーターのポートマッピングリスト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 のサブネットサイズ

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

IP アドレスタイプ

カスタムルーティングアクセラレーターは、IPv4 IP アドレスタイプのみをサポートします。

リスナーポート範囲

カスタムルーティングアクセラレーターに追加しようとするサブネットに含まれる送信先の数に対応するために、リスナーポートの範囲を指定して、十分なリスナーポートを指定する必要があります。リスナーを作成する際に指定する範囲は、カスタムルーティングアクセラレーターで使用できるリスナーポートと送信先 IP アドレスの組み合わせの数を決定します。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発生す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。

Global Accelerator は、カスタムルーティングアクセラレーターにサブネットを追加するときに、ポート範囲をブロックに割り当てます。リスナーポート範囲を線形に割り当て、使用する送信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、少なくともサブネットサイズに、サブネット内の送信先ポートとプロトコル (送信先設定) の数を掛けたものでなければなりません。

> **Note**
>
> Global Accelerator 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ら、それを編集してポート範囲と関連付けられたプロトコルを追加できますが、既存のポート範囲を小さくすることはできません。例えば、リスナーポートの範囲が 5,000 ~ 10,000 の場合、その範囲を 5,900 ~ 10,000 や 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、少なくとも 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。

送信先ポートの範囲。

カスタムルーティングアクセラレーターのポート範囲を指定する場所は 2 つあります。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送信先ポート範囲とプロトコルです。

- リスナーポート範囲: クライアントが接続する Global Accelerator 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ーの背後にある VPC サブネット上の一意の送信先 IP アドレスとポートにマッピングします。
- 送信先ポート範囲: エンドポイントグループに指定する送信先ポート範囲のセット (送信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。送信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ているセキュリティグループでそれらのポートへのトラフィックを許可する必要があります。

ヘルスチェックとフェイルオーバー

Global Accelerator は、カスタムルーティングアクセラレーターのヘルスチェックを実行せず、正常なエンドポイントにフェイ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ーのトラフィックは、送信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。

すべてのトラフィックはデフォルトで拒否される

デフォルトでは、カスタムルーティングアクセラレーターを介して送信されるトラフィックは、サブネット内のすべての送信先に拒否されます。送信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具体的に許可するか、または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送信先を更新してトラフィックを許可または拒否するには、インターネット全体に伝播するまでに時間がかかります。変更が伝播されたかどうかを判断するには、`DescribeCustomRoutingAccelerator` API アクションを呼び出してアクセラレーターのステータスを確認できます。詳細については、「DescribeCustomRoutingAccelerator」を参照してください。

CloudFormation はサポートされていない

CloudFormation は、カスタムルーティングアクセラレーター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ー

AWS Global Accelerator の「カスタムルーティングアクセラレーター」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、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ながら、1 人以上のユーザーを多くの送信先の間で特定の送信先に誘導できます。

カスタムルーティングアクセラレーターは、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ーを使用する場合、Global Accelerator はエンドポイントの地理的近接度やヘルス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、「Global Accelerator でのカスタムルーティングアクセラレーターの仕組み」を参照してください。

アクセラレーターを作成すると、デフォルトで Global Accelerator は 2 つの静的 IPv4 アドレスのセットを提供します。カスタムルーティングアクセラレーターは、IPv4 IP アドレスタイプのみをサポートします。独自の IP アドレス範囲を AWS (BYOIP) にすると、アクセラレータで使用する静的 IPv4 アドレスを独自のプールから割り当てることができます。詳細については、「Global Accelerator の Bring your own IP (BYOIP)」を参照してください。

> **Important**
>
> 静的 IP アドレスは、アクセラレーターを無効にし、トラフィックを受け入れたりルーティングしたりしなくなった場合でも、存在する限り、アクセラレーターに割り当てられたままになります。ただし、アクセラレーターを削除すると、アクセラレーターに割り当てられた Global Accelerator 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することができなくなります。ベストプラクティスとして、アクセラレーター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 では、タグベースのアクセス許可などの IAM ポリシーを使用して、アクセラレーター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、「Global Accelerator を使用した ABAC」を参照してください。

このセクションでは、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ーを操作する方法について説明します。Global Accelerator での API 操作の使用については、「AWS Global Accelerator API Reference」を参照してください。

内容

- Global Accelerator でカスタムルーティングアクセラレーターを作成する
- Global Accelerator でカスタムルーティングアクセラレーターを編集する
- Global Accelerator でカスタムルーティングアクセラレーターを表示する
- Global Accelerator でカスタムルーティングアクセラレーターを削除する

Global Accelerator でカスタムルーティングアクセラレーターを作成する

このセクションでは、コンソールでカスタムアクセラレーターを作成する手順について説明します。Global Accelerator をプログラムで操作するには、「AWS Global Accelerator API Reference」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を作成するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [アクセラレーターの作成] を選択します。
3. アクセラレーターの名前を指定します。
4. [アクセラレータのタイプ] の場合は、[カスタムルーティング] を選択します。
5. 必要に応じて、独自の IP アドレス範囲を AWS (BYOIP) にした場合は、そのアドレスプールからアクセラレーターの静的 IP アドレスを指定できます。アクセラレーターの 2 つの静的 IP アドレスのそれぞれに対して、この選択を行います。
   - 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。
   - 独自の 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ーに割り当てます。
6. 必要に応じて、アクセラレーターリソースを識別するのに役立つタグを 1 つ以上追加します。
7. [次へ] を選択してウィザードの次のページに移動し、リスナー、エンドポイントグループ、VPC サブネットエンドポイントを追加します。

Global Accelerator でカスタムルーティングアクセラレーターを編集する

このセクションでは、コンソールでカスタムアクセラレーターを更新する手順について説明します。Global Accelerator をプログラムで操作するには、「AWS Global Accelerator API Reference」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を編集するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. カスタムルーティングアクセラレーターのリストで、1 つを選択し、[編集] を選択します。
3. [アクセラレーターの編集] ページで、必要な変更を行います。例えば、アクセラレーターを削除できるように無効にします。
4. [Save] を選択します。

Global Accelerator でカスタムルーティングアクセラレーターを表示する

このセクションでは、コンソールでカスタムルーティングアクセラレーターに関する情報を表示する手順について説明します。プログラムでカスタムルーティングアクセラレータの説明を確認するには、「AWS Global Accelerator API Reference」の「ListCustomRoutingAccelerator」と「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ーに関する情報を表示するには

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. アクセラレーターの詳細を確認するには、アクセラレーターを選択し、[表示] を選択します。

Global Accelerator でカスタムルーティングアクセラレーターを削除する

カスタムルーティングアクセラレーターをテストとして作成した場合、またはアクセラレーターを使用しなくなった場合は、削除できます。コンソールでアクセラレーターを無効にし、削除できます。アクセラレーター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。

コンソールの代わりに API オペレーションを使用してカスタムルーティングアクセラレーターを削除するには、まずアクセラレーター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、「AWS Global Accelerator API Reference」の「DeleteAccelerator」オペレーション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を無効にするには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。

2. リストで、無効にしたいアクセラレーターを選択します。
3. [編集] を選択します。
4. [アクセラレーターの無効化] を選択し、[保存] を選択します。

カスタムルーティングアクセラレーターを削除するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. リストで、削除したい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にしていない場合、[削除] は選択できません。アクセラレーターを無効にするには、前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、[削除] を選択します。

> **Important**
>
> アクセラレーターを削除すると、アクセラレータに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 のカスタムルーティングアクセラレーターのリスナー

AWS Global Accelerator のカスタムルーティングアクセラレーターの場合、Global Accelerator が VPC サブネットエンドポイント内の特定の送信先 Amazon EC2 インスタンスにマッピングする関連プロトコルを持つリスナーポートの範囲を指定するリスナーを設定します。VPC サブネットエンドポイントを追加すると、Global Accelerator はリスナーに定義したポート範囲とサブネット内の送信先 IP アドレスとポートの間に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とプロトコルとともに指定し、ユーザートラフィックを VPC サブネット内の特定の送信先 Amazon EC2 インスタンス IP アドレスとポートに送信できます。

カスタムルーティングアクセラレーター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存在する AWS リージョンごとに 1 つ以上のエンドポイントグループを含めることができます。カスタムルーティングアクセラレーターのリスナーは、TCP プロトコルと UDP プロトコルの両方をサポートします。UDP、TCP、または UDP と TCP の両方を定義する送信先ポート範囲ごとにプロトコルまたは複数のプロトコルを指定します。

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

内容

- Global Accelerator でカスタムルーティングアクセラレーターのリスナーを追加する
- Global Accelerator でカスタムルーティングアクセラレーターのリスナーを編集する
- Global Accelerator でカスタムルーティングアクセラレーターのリスナーを削除する

Global Accelerator でカスタムルーティングアクセラレーターのリスナーを追加する

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ーのリスナーを追加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 Reference」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は、カスタムルーティングアクセラレーターで使用できるリスナーポートと送信先 IP アドレスの組み合わせの数を定義します。最大限の柔軟性を得るには、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、少なくとも 16 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ら、それを編集してポート範囲と関連付けられたプロトコルを追加できますが、既存のポート範囲を小さくすることはできません。

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。

2. [アクセラレーター] 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ーで最大限の柔軟性を得るには、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。

Global Accelerator でカスタムルーティングアクセラレーターのリスナーを編集する

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ーのリスナーを編集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 Reference」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のリスナーを編集するには

カスタムルーティングアクセラレーターのリスナーを編集するときは、さらにポート範囲と関連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、プロトコルを変更したりすることはできますが、既存のポート範囲をこと小さくすることはできません。

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. [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、[リスナーの編集] を選択します。
4. [リスナーを編集する] ページで、既存のポート範囲またはプロトコルを変更するか、新しいポート範囲を追加します。

   既存のポート範囲を小さくすることはできません。
5. [Save] を選択します。

Global Accelerator でカスタムルーティングアクセラレーターのリスナーを削除する

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ーのリスナーを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 Reference」を参照してください。

リスナーを削除するには

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. [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、[削除] を選択します。
4. 確認ダイアログボックスで、[削除] を選択します。

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

AWS Global Accelerator でカスタムルーティングアクセラレーターを使用すると、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) サブネット内の送信先 Amazon EC2 インスタンスがトラフィックを受け入れるポートとプロトコルを定義します。

カスタムルーティングアクセラレーターのエンドポイントグループは、VPC サブネットと EC2 インスタンスが配置されている各 AWS リージョン に対して作成します。カスタムルーティングアクセラレーターの各エンドポイントグループには、複数の VPC サブネットエンドポイントを含めることができます。同様に、各 VPC を複数のエンドポイントグループに追加できますが、エンドポイントグループは異なるリスナーと関連される必要があります。

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のポート範囲ごとに、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、各プロトコルの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。例えば、ポート 8080-8090 を使用し、UDP 経由でゲームトラフィックが実行されているゲームサーバーがあれば、ポート 80 を使用して TCP 経由でチャットメッセージを聞いているサーバーもあります。

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

内容

- Global Accelerator でカスタムルーティングアクセラレーターのエンドポイントグループを追加する
- Global Accelerator でカスタムルーティングアクセラレーターのエンドポイントグループを編集する
- Global Accelerator でカスタムルーティングアクセラレーターのエンドポイントグループを削除する

Global Accelerator でカスタムルーティングアクセラレーターのエンドポイントグループを追加する

AWS Global Accelerator コンソールで、または API オペレーションを使用して、カスタムルーティングアクセラレーターのエンドポイントグループを操作します。エンドポイントグループからいつでも VPC サブネットエンドポイントを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ーのエンドポイントグループを作成する方法について説明します。Global Accelerator での API 操作の使用については、「AWS Global Accelerator API Reference」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のエンドポイントグループを追加するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [アクセラレーター] 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] 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. [エンドポイントの追加] を選択します。
5. リスナーのセクションで、エンドポイントグループ用のリージョンを指定します。
6. [ポートとプロトコルセット] には、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。
   - [入力ポート] と [出力ポート] を入力して、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または複数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ーのエンドポイントグループに指定したポートの合計数をサポートするのに十分な合計ポートがリスナーポート範囲にある必要があります。

7. [Save] を選択します。
8. 必要に応じて、[エンドポイントグループの追加] を選択して、このリスナーに追加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. [エンドポイントの追加] を選択します。

Global Accelerator でカスタムルーティングアクセラレーターのエンドポイントグループを編集する

AWS Global Accelerator コンソールで、または API オペレーションを使用して、カスタムルーティングアクセラレーターのエンドポイントグループを操作します。エンドポイントグループからいつでも VPC サブネットエンドポイントを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ーのエンドポイントグループを編集する方法について説明します。Global Accelerator での API 操作の使用については、「AWS Global Accelerator API Reference」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のエンドポイントグループを編集するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [アクセラレーター] 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] 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. [エンドポイントグループの編集] を選択します。
5. [エンドポイントグループの編集] ページで、リージョン、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。

Global Accelerator でカスタムルーティングアクセラレーターのエンドポイントグループを削除する

AWS Global Accelerator コンソールで、または API オペレーションを使用して、カスタムルーティングアクセラレーターのエンドポイントグループを操作します。

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ーのエンドポイントグループを削除する方法について説明します。Global Accelerator での API 操作の使用については、「AWS Global Accelerator API Reference」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を削除するには

1. https://us-west-2.console.aws.amazon.com/globalaccelerator/home#GlobalAcceleratorHome: で Global Accelerator コンソールを開きます。
2. [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] セクションでリスナーを選択し、[削除] を選択します。
4. [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んだ後、[削除] を選択します。
5. 確認ダイアログボックスで、[削除] を選択します。

Global Accelerator のカスタムルーティングアクセラレーター用 Amazon 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ーのエンドポイントは、アクセラレーターを介してトラフィックを受信できる Amazon Virtual Private Cloud (VPC) サブネットです。各サブネットには、1 つ以上の Amazon EC2 インスタンスの送信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、Global Accelerator 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。これを使用して、サブネット内の送信先 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、「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ーに VPC サブネットと送信先を追加するときは、次の点に注意してください:

- トラフィックをサブネット内の EC2 インスタンスにのみ送信できます。ロードバランサー (標準アクセラレーターとは対照的) などの他のリソースには送信できません。

- サブネットエンドポイントの EC2 インスタンスの送信先は、C1、CC1、CC2、CG1、CG2、CR1、CS1、G1、G2、HI1、HS1、M1、M2、M3、または T1 のいずれかにすることはできません。
- デフォルトでは、カスタムルーティングアクセラレーターを介して送信されるトラフィックは、サブネット内の送信先に到達できません。送信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 (送信先ソケット) へのトラフィックを有効にするかを選択する必要があります。

> **Important**
>
> サブネットまたは特定の送信先を更新してトラフィックを許可または拒否するには、インターネット全体に伝播するまでに時間がかかります。変更が伝播され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できます。詳細については、「DescribeCustomRoutingAccelerator」を参照してください。

- VPC サブネットはクライアント IP アドレスを保持するため、カスタムルーティングアクセラレーターのエンドポイントとしてサブネットを追加するときは、関連するセキュリティと設定情報を確認してください。詳細については、「クライアント IP アドレスが保存されているエンドポイントの要件」を参照してください。
- Global Accelerator の後ろにあるエンドポイントとしてリソースを設定する場合、インターネット経由で同じエンドポイントにトラフィックを直接送信しないことをお勧めします。直接トラフィックを送信すると、接続の衝突問題が発生する可能性があります。

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

内容

- カスタムルーティングアクセラレーターの VPC サブネットエンドポイントを追加する
- カスタムルーティングアクセラレーターの VPC サブネットエンドポイントを編集する
- カスタムルーティングアクセラレーターの VPC サブネットエンドポイントを削除する

カスタムルーティングアクセラレーターの VPC サブネットエンドポイントを追加する

Amazon Virtual Private Cloud (VPC) サブネットエンドポイントをカスタムルーティングアクセラレーターのエンドポイントグループに追加して、サブネット内の送信先 Amazon EC2 インスタンスにユーザートラフィックを送信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・削除したり、EC2 の宛先へのトラフィックを有効・無効にすることで、それらの宛先がトラフィックを受信できるかどうかが変わります。ただし、Global Accelerator 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だけの送信先へのトラフィックを許可するには、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。

VPC サブネットをアクセラレーターから削除するには、エンドポイントグループから削除します。サブネットを削除してもサブネット自体には影響はありませんが、Global Accelerator はそのサブネットやその中の Amazon EC2 インスタンスにトラフィックを送信することができなくなります。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 コンソールに VPC サブネットエンドポイントを追加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 Reference」を参照してください。

VPC サブネットエンドポイントを追加するには

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. [アクセラレーター] 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] セクションの [リスナー ID] で、リスナーの ID を選択します。
4. [エンドポイントグループ] セクションの [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. [エンドポイント] セクションで、[エンドポイントの追加] を選択します。
6. [エンドポイントの追加] ページで、[エンドポイント] で VPC サブネットを選択します。

VPC がない場合は、リストにアイテムはありません。続行するには、少なくとも 1 つの VPC を追加し、ここでステップに戻り、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では、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 インスタンスとポートへのトラフィックのみを許可することができます。デフォルトでは、サブネット内のすべての送信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。

カスタムルーティングアクセラレーターの VPC サブネットエンドポイントを編集する

カスタムルーティングアクセラレーター用の Amazon Virtual Private Cloud (VPC) サブネットエンドポイントを編集することで、ユーザートラフィックの送信先を変更したり、サブネット内のすべての送信先へのトラフィックを許可または拒否したりすることができます。

サブネットに EC2 インスタンスを追加・削除したり、EC2 の宛先へのトラフィックを有効・無効にすることで、それらの宛先がトラフィックを受信できるかどうかが変わります。ただし、Global Accelerator ポートマッピングは変更されません。

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編集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 Reference」を参照してください。

特定の送信先へのトラフィックを許可または拒否するには

VPC エンドポイントのサブネットポートマッピングを編集することで、特定のサブネット内の 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. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. [アクセラレーター] 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] セクションの [リスナー ID] で、リスナーの ID を選択します。
4. [エンドポイントグループ] セクションの[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. エンドポイントサブネットを選択し、[詳細の表示] を選択します。
6. [エンドポイント] ページで、[ポートマッピング] で IP アドレスを選択し、[編集] を選択します。

7. トラフィックを有効にするポートを入力し、[これらの送信先を許可する] を選択します。

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送信先へのトラフィックを許可または拒否できます。

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. [アクセラレーター] 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] セクションの [リスナー ID] で、リスナーの ID を選択します。
4. [エンドポイントグループ] セクションの[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. [すべてのトラフィックを許可/拒否] を選択します。
6. オプションを選択して、すべてのトラフィックを許可するか、またはすべてのトラフィックを拒否し、[保存] を選択します。

カスタムルーティングアクセラレーターの VPC サブネットエンドポイントを削除する

Amazon Virtual Private Cloud (VPC) サブネットエンドポイントをカスタムルーティングアクセラレーターから削除して、ユーザートラフィックがサブネット内の送信先 Amazon EC2 インスタンスに移動しないようにすることができます。

このセクション内の手順では、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 Reference」を参照してください。

エンドポイントを削除するには

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. [アクセラレーター] 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] セクションの [リスナー ID] で、リスナーの ID を選択します。
4. [エンドポイントグループ] セクションの [エンドポイントグループ ID] で、削除したい 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. [エンドポイントの削除] を選択します。
6. 確認ダイアログボックスで、[削除] を選択します。

Global Accelerator でクロスアカウントアクセスを設定する

クロスアカウントサポートを使用すると、複数のアカウントのリソースにアクセスするアプリケーションの固定エントリポイントとして AWS Global Accelerator を使用するか、共有 CIDR ブロックからアクセラレータの IP アドレスを選択できます。クロスアカウントアクセス許可を使用して、異なるアカウントのリソースへのアクセスを許可するのが AWS ベストプラクティスです。Bring-Your-Own-IP (BYOIP) アドレスの CIDR ブロックのクロスアカウントサポートにより、組織内の異なるアカウントのアクセラレーターに同じアドレスプールを使用できます。また、アプリケーションへのインターネットアクセスを制御する 1 つのアカウントで AWS リソースを整理することもできます。これにより、モニタリングとセキュリティを簡素化し、インバウンド接続を可視化できます。

Global Accelerator でのクロスアカウントサポートでは、以下を実行できます:

- Network Load Balancer などのエンドポイントを他のアカウントからアクセラレーターに追加します。
- IP アドレスに BYOIP アドレスプールを選択し、異なるアカウントのアクセラレーターにプールから IP アドレスを選択します。BYOIP アドレスプールを共有することで、同じ CIDR ブロックからより多くのアドレスを使用できるため、必要な CIDR ブロックの数を減らすことができます。

Global Accelerator コンソールでクロスアカウントアタッチメントとリソースを操作するか、AWS Command Line Interface (AWS CLI) または AWS SDK で Global Accelerator API オペレーションを使用します。例えば、プリンシパルとして、「UpdateEndpoints」オペレーションを使用して、クロスアカウントリソースをアクセラレーターのエンドポイントとして追加できます。API オペレーションを使用する場合は、クロスアカウントアタッチメント ARN とエンドポイント ID を指定します。詳細については、「AWS Global Accelerator API Reference ガイド」を参照してください。

内容

- Global Accelerator でのクロスアカウントの仕組み
- Global Accelerator でクロスアカウントアタッチメントを操作する
- Global Accelerator でクロスアカウントリソースを操作する
- Global Accelerator でクロスアカウントリソースを特定する
- Global Accelerator のクロスアカウントリソースの責任とアクセス許可
- Global Accelerator のクロスアカウントリソースの請求コスト
- Global Accelerator のクロスアカウントリソースのクォータ

Global Accelerator でのクロスアカウントの仕組み

Global Accelerator でのクロスアカウントサポートにより、リソース所有者は、リソースが他のアカウントが所有するアクセラレーターと共有されているかどうかを制御します。リソースのリソース共有を有効にするには、リソース所有者として Global Accelerator クロスアカウントアタッチメントを作成し、アカウント内のリソースを別のアカウントによってアクセラレーターに追加することを許可します。

Global Accelerator でクロスアカウントアタッチメントを作成します。アタッチメントには、共有するリソースと、リソースの使用が許可されているプリンシパル (他のアカウントまたは特定のアクセラレーター ARN) が一覧表示されます。リソースには、アクセラレータのエンドポイントグループにエンドポイントとして追加する Network Load Balancer のような AWS リソースや、Bring-Your-Own-IP (BYOIP) アドレスのプロセスを通じて Global Accelerator に持ち込んだ IP アドレス範囲が含まれます。

> **Important**
>
> BYOIP IP アドレス範囲をクロスアカウントアタッチメントに追加してプリンシパルと共有する前に、アドレス範囲をプロビジョニングしてアドバタイズするプロセスを完了する必要があります。詳細については、「Global Accelerator の Bring your own IP (BYOIP)」を参照してください。

リソース所有者としてアタッチメントを作成した後、アタッチメントにリストされているプリンシパルは、アタッチメントにリストされているリソースを操作できます。つまり、リストされているエンドポイント AWS リソースとして追加したり、リストされている CIDR プレフィックスから BYOIP アドレスを静的 IP アドレスとして選択したりできます。プリンシパルがアクセラレーターにクロスアカウントリソースを追加する場合は、リソースを使用するアクセス許可を持つプリンシパルとしてそれらを許可するクロスアカウントアタッチメントを指定する必要があります。

Global Accelerator でクロスアカウントアタッチメントを操作する

誰かが別のアカウントからリソースをアクセラレーターのエンドポイントまたは BYOIP アドレスとして追加できるようにするには、リソースの所有者が Global Accelerator でクロスアカウントアタッチメントを作成する必要があります。アタッチメントでは、リソース所有者は、プリンシパルがアクセラレーターに追加できる特定のリソースとともに、リソースを追加できる 1 つ以上のアクセラレーターまたはアカウントを指定します。

リソース所有者は、クロスアカウントアタッチメントでリソースを指定するには、AWS アカウント内のリソースを所有する必要があることに注意してください。つまり、リソースはあなたのアカウント内で割り当てまたはプロビジョニングされている必要があります。共有サブネットのようにあなたと共有されたリソースを指定することはできません。

内容

- AWS Global Accelerator でクロスアカウントアタッチメントを作成する
- AWS Global Accelerator でクロスアカウントアタッチメントを編集する
- Global Accelerator でクロスアカウントアタッチメントを削除する

AWS Global Accelerator でクロスアカウントアタッチメントを作成する

このセクションの手順に従って、AWS Global Accelerator コンソールを使用してクロスアカウントアタッチメントを作成します。

このセクションでは、AWS Global Accelerator コンソールを使用してクロスアカウントアタッチメントを作成する方法について説明します。Global Accelerator での API 操作の使用については、「AWS Global Accelerator API Reference」を参照してください。

クロスアカウントアタッチメントを作成するには

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. [クロスアカウントアタッチメントの作成] を選択します。
3. [クロスアカウントアタッチメントの作成] ページで、アタッチメントの名前を入力します。
4. リソースの追加を許可するアクセラレーターの AWS アカウント、ARN、またはその両方を追加します。
5. 使用を許可するリソースを選択します。例えば、エンドポイントとして追加できるリソースを追加するには、リソースごとに AWS リージョン を選択します。次に、ドロップダウンメニューから、追加するエンドポイントタイプ (リソースタイプ) とエンドポイント (リソース) を選択します。
6. [アタッチメントの作成] を選択します。

注: アタッチメントのリストに新しいクロスアカウントアタッチメントを表示するには、[クロスアカウントアタッチメント] ページを更新します。

AWS Global Accelerator でクロスアカウントアタッチメントを編集する

このセクションの手順に従って、AWS Global Accelerator コンソールを使用してクロスアカウントアタッチメントを編集します。

このセクションでは、AWS Global Accelerator コンソールを使用してクロスアカウントアタッチメントを編集する方法について説明します。Global Accelerator での API 操作の使用については、「AWS Global Accelerator API Reference」を参照してください。

クロスアカウントアタッチメントを編集して、プリンシパルまたはリソースを追加または削除したり、アタッチメントの名前を変更したり、アタッチメントを削除したりできます。

プリンシパルやリソースを削除する場合、または添付ファイルを削除する場合は、次の点に注意してください:

- プリンシパルまたは CIDR をアタッチメントから削除するには、プリンシパルはまず、それらを使用するすべてのアクセラレーターから共有 IP アドレスを削除する必要があります。次に、プリンシパル、または CIDR をアタッチメントから削除できます。
- 共有 IP アドレスを削除したり、プリンシパルが共有 CIDR にアクセスするための承認を添付ファイルから削除したりする前に、CIDR の共有 IP アドレスを現在アクセラレーターで使用してはいけません。
- プリンシパルが 1 つ以上の共有エンドポイントを追加できるようにするクロスアカウントアタッチメントからプリンシパルを削除すると、Global Accelerator は、アタッチメントに記載されているクロスアカウントリソースに対してそのアクセス許可を使用するアクセラレータからそれらのクロスアカウントエンドポイントを削除します。
- クロスアカウントアタッチメントからエンドポイントリソースを削除すると、Global Accelerator は、アタッチメントのアクセス許可に基づいて、クロスアカウントエンドポイントがエンドポイントとして追加されたアクセラレーターからクロスアカウントエンドポイントを削除します。
- クロスアカウントアタッチメントを削除すると、Global Accelerator は、アタッチメントのアクセス許可に基づいてリソースがエンドポイントとして追加されたすべてのアクセラレーターから、アタッチメントにリストされているすべてのクロスアカウントエンドポイントを削除します。
- プリンシパルまたはリソースを含むクロスアカウントアタッチメントが複数ある場合、Global Accelerator は既存のアタッチメントが提供するアクセスを引き続き許可します。例えば、1 つの添付ファイルからプリンシパルを削除しても、プリンシパルに 2 番目の添付ファイルによって付与されたリソースにアクセスするアクセス許可が依然としてある場合、Global Accelerator は引き続き、プリンシパルにクロスアカウントリソースへのアクセスを許可します。

クロスアカウントアタッチメントを編集するには

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. [クロスアカウントアタッチメント] を選択します。
3. 更新したいクロスアカウントアタッチメントを選択し、[編集] を選択します。
4. アタッチメントを変更して、必要な変更を行います。例えば、プリンシパルの追加または削除、アタッチメントの名前の変更、リソースの追加または削除を行うことができます。
5. [Save changes] (変更の保存) をクリックします。

Global Accelerator でクロスアカウントアタッチメントを削除する

このセクションの手順に従って、AWS Global Accelerator コンソールを使用してクロスアカウントアタッチメントを削除します。

このセクションでは、AWS Global Accelerator コンソールを使用してクロスアカウントアタッチメントを削除する方法について説明します。Global Accelerator での API 操作の使用については、「AWS Global Accelerator API Reference」を参照してください。

クロスアカウントアタッチメントを削除するには

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. [クロスアカウントアタッチメント] を選択します。
3. クロスアカウントアタッチメントを選択し、[削除] を選択します。
4. ダイアログボックスでテキストボックスに [削除] と入力し、クロスアカウントアタッチメントを削除することを確認します。
5. [Delete] (削除) をクリックします。

Global Accelerator でクロスアカウントリソースを操作する

アカウント、またはアクセス許可を持つアクセラレーターが、AWS Global Accelerator のクロスアカウントアタッチメントでプリンシパルとして指定されている場合は、別のアカウントから共有されているリソースを使用できます。

例えば、アクセラレーターの作成時に Bring-Your-Own-IP (BYOIP) アドレスを静的 IP アドレスとして持ち込むか、アクセラレーターのアクセラレーターエンドポイントグループにエンドポイントを追加することができます。追加できるリソースは、添付ファイルにも指定する必要があります。

以下のセクションでは、Global Accelerator でクロスアカウントアタッチメントを追加または削除する手順について説明します。

内容

- Global Accelerator にクロスアカウント BYOIP アドレスを追加する
- AWS Global Accelerator でクロスアカウントエンドポイントを追加する
- Global Accelerator でクロスアカウントエンドポイントを削除する

Global Accelerator にクロスアカウント BYOIP アドレスを追加する

このセクションのステップに従って、Global Accelerator コンソールを使用して、クロスアカウント持ち込みの Bring-Your-Own-IP (BYOIP) ID アドレスを設定します。

このセクションでは、AWS Global Accelerator コンソールを使用して BYOIP IP アドレスを使用する方法について説明します。Global Accelerator での API 操作の使用については、「AWS Global Accelerator API Reference」を参照してください。

アクセラレーターに使用する BYOIP アドレスは変更できますが、いくつかの制限が適用されます。詳細については、「アクセラレーターを更新して IP アドレスを変更する方法」を参照してください。

クロスアカウント BYOIP IP アドレスを使用するには

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. [アクセラレーターの作成] を選択します。
3. アクセラレーターの名前を指定します。
4. [アクセラレータータイプ] を選択します。
5. [IP アドレスの種類] には [IPv4] を選択します。
6. [クロスアカウント用に承認された CIDR から静的 IP アドレスを使用する] チェックボックスを選択します。
7. プリンシパルとしてユーザーを指定し、共有されている BYOIP アドレスブロックを含むクロスアカウントアタッチメントの所有者のアカウント ID を選択します。

アドレスを選択するアカウントを 1 つ選択する必要があるため、アクセラレータを作成するときに 2 つの BYOIP IP アドレスを選択した場合、IP アドレスは同じ所有者に属し、同じクロスアカウントアタッチメントで承認されている必要があります。

8. アクセラレーターの静的 IP アドレスを 1 つまたは両方指定します。

   - 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**
     >
     > 静的 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、Global Accelerator が高可用性のために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。

   - 独自の 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すると、Global Accelerator は特定の IP アドレスをアクセラレーターに割り当てます。

9. 必要に応じて、アクセラレーターリソースを識別するのに役立つタグを 1 つ以上追加します。

10. [次へ] を選択して、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。

AWS Global Accelerator でクロスアカウントエンドポイントを追加する

このセクションのステップに従って、Global Accelerator コンソールを使用してクロスアカウントエンドポイントを追加します。

このセクションでは、AWS Global Accelerator コンソールを使用してクロスアカウントエンドポイントを追加する方法について説明します。Global Accelerator での API 操作の使用については、「AWS Global Accelerator API Reference」を参照してください。

クロスアカウントエンドポイントを追加するには

1. アクセラレーターを作成または更新するときは、[エンドポイント] セクションで [エンドポイントの追加] を選択します。
2. [エンドポイントの追加] ページで、[クロスアカウントアタッチメントで指定されたリソースを追加する] を選択します。
3. ドロップダウンメニューで、自分またはアクセラレーターをプリンシパルとして含むクロスアカウントアタッチメントを作成した AWS アカウント を選択します。

4. [エンドポイントタイプ] で、追加するリソースのタイプを選択します。

   クロスアカウントアタッチメントに含まれるリソースタイプのみがドロップダウンメニューに表示されることに注意してください。

5. [エンドポイント] で、追加するリソースを選択します。

   クロスアカウントアタッチメントに含まれるリソースのみがドロップダウンメニューに表示されることに注意してください。クロスアカウントアタッチメントで有効になっていないリソースを表示するには、[クロスアカウントアタッチメントで指定されたリソースを追加する] チェックボックスを選択します。

Global Accelerator でクロスアカウントエンドポイントを削除する

このセクションのステップに従って、Global Accelerator コンソールを使用してクロスアカウントエンドポイントを削除します。

このセクションでは、AWS Global Accelerator コンソールを使用してクロスアカウントエンドポイントを削除する方法について説明します。Global Accelerator での API 操作の使用については、「AWS Global Accelerator API Reference」を参照してください。

クロスアカウントエンドポイントを削除するには

1. アクセラレータを作成または更新するときは、[エンドポイントグループ] の詳細ページで、削除したいエンドポイントを選択します。
2. [削除] を選択します。

Global Accelerator でクロスアカウントリソースを特定する

リソース所有者とプリンシパルは、AWS Global Accelerator コンソールを使用するか、Global Accelerator オペレーションで AWS CLI を使用して共有リソースを識別できます。例えば、次のオペレーションを実行できます。

- 所有者は、クロスアカウントアタッチメントのリストを表示し、各アタッチメントのプリンシパルとリソースを表示できます。
- プリンシパルとして、リストされているすべてのクロスアカウントアタッチメントを表示し、特定のアタッチメントのアクセラレーターのエンドポイントまたは IP アドレス範囲として追加できるリソースを一覧表示できます。

API オペレーションを使用してクロスアカウントアタッチメントと共有リソースを表示する方法の詳細については、「AWS Global Accelerator API Reference ガイド」を参照してください。

所有者として: Global Accelerator でクロスアカウントリソースを特定する

所有者として、クロスアカウントアタッチメントを AWS マネジメントコンソール で表示することも、Global Accelerator API オペレーションで AWS Command Line Interface を使用して表示することもできます。

クロスアカウントアタッチメントを表示するには

- Global Accelerator コンソールで、[クロスアカウントアタッチメント] を選択します。

クロスアカウントアタッチメントに含まれる情報を表示するには

1. Global Accelerator コンソールの [クロスアカウントアタッチメント] ページでアタッチメントを選択し、[詳細を表示する] を選択します。

   -または-

2. 例えば、AWS Command Line Interface を使用することで API オペレーション「ListCrossAccountResources」を使用します。このオペレーションは、アカウント内のすべての添付ファイルで、すべてのリソースの一意のアタッチメントとリソースのペアのリストを返します。

   例えば、クロスアカウントアタッチメントが 2 つあり、1 つ目が 2 つのエンドポイントと CIDR ブロックを含み、2 つ目が 3 つのエンドポイントを含む場合、`ListCrossAccountResources` はアタッチメントリソースペア attachment1-endpoint1、Attachment1-endpoint2、attachment1-CIDR 、Attachment2-endpoint3、Attachment2-endpoint4、および Attachment2-endpoint5 の 6 つを返します。

プリンシパルとして: Global Accelerator でクロスアカウントリソースを特定する

プリンシパルとして、クロスアカウントアタッチメントによってリソースをエンドポイントとしてアクセラレーターに追加する権限が付与された後、リソースをエンドポイントとして追加する前に実行する追加のアクションはありません。

自分がプリンシパルとして記載されているクロスアカウントアタッチメントを作成した AWS アカウント を確認できます。また、各アカウントが作成した添付ファイルで指定されたリソースも確認できます。このリソースは、アクセラレーターのエンドポイントまたは IP アドレス範囲として追加できます。

プリンシパルとしてリストされているクロスアカウントアタッチメントを作成したアカウントを表示するには

1. Global Accelerator コンソールで、アクセラレーターの [エンドポイントの詳細] ページで、[エンドポイントの追加] を選択します。
2. [エンドポイントの追加] ページで、[クロスアカウントアタッチメントで指定されたリソースを追加する] を選択します。
3. [クロスアカウントアタッチメント所有者のアカウント ID を選択する] のドロップダウンメニューで、クロスアカウントアタッチメントでアクセス許可を付与するアカウントを表示して、アクセラレーターにリソースを追加します。

各アカウントが作成したアタッチメントで指定されたエンドポイントリソースを表示するには

1. Global Accelerator コンソールで、アクセラレーターの [エンドポイントの詳細] ページで、[エンドポイントの追加] を選択します。
2. [エンドポイントの追加] ページで、[クロスアカウントアタッチメントで指定されたリソースを追加する] を選択します。
3. ドロップダウンメニューで、クロスアカウントアタッチメントでアクセス許可を付与するアカウントを選択して、アクセラレーターにリソースを追加します。
4. [エンドポイントタイプ] では、リソースのタイプを選択します。

   クロスアカウントアタッチメントに含まれるリソースタイプのみがドロップダウンメニューに表示されることに注意してください。
5. [エンドポイント] ドロップダウンメニューには、リソースのリストが表示されます。これらは、特定のリソースタイプに対して、エンドポイントとして追加するクロスアカウントアタッチメントを作成したアカウントによって承認されるリソースです。
6. 別のアカウントによって作成されたクロスアカウントアタッチメントで指定された追加できるリソースを確認するには、次の操作を行います。[クロスアカウントアタッチメント所有者のアカウント ID を選択する] のドロップダウンメニューで、別の AWS アカウント を選択します。

アカウントが作成した添付ファイルで指定された IP アドレスリソースを表示するには

1. Global Accelerator コンソールで、[アクセラレーターの作成] を選択します。
2. [名前の入力] ページで、IP アドレスタイプで [IPv4] を選択します。
3. IP アドレスプールの選択で、[クロスアカウントアタッチメントで指定された共有 IP アドレスプールを使用する] を選択します。
4. クロスアカウントアタッチメントでアクセス許可を付与するアカウントを選択して、共有 IP アドレスプールから IP アドレスを選択します。
5. [IP アドレスプール] の場合、ドロップダウンリストから共有 IP アドレスプールを表示できます。

   使用できるクロスアカウントアタッチメントに含まれる共有 IP アドレスプールのみがドロップダウンメニューに表示されることに注意してください。

Global Accelerator のクロスアカウントリソースの責任とアクセス許可

以下のセクションでは、リソース所有者として、または AWS Global Accelerator でのクロスアカウントアクセスのプリンシパルとして持っているアクセス許可を一覧表示します。

リソース所有者のアクセス許可

リソース所有者として、プリンシパルが AWS アカウント からアクセラレーターまたは特定のアクセラレーターにリソースを追加することを承認した場合、プリンシパルはクロスアカウントアタッチメントにリストしたリソースを追加できます。

リソース所有者は、リソースの作成、管理、削除を担当します。アクセラレーターでリソースを追加または削除することはできません。ただし、権限を付与されたロールがある場合は除きます。

アクセラレーターがあり、クロスアカウントリソースを追加または削除する必要がある場合、プリンシパルはリソースへのアクセス許可を持つロールを IAM に設定し、そのロールにアカウントを追加できます。

クロスアカウントアタッチメントでプリンシパルまたはリソースを追加または削除して、所有しているリソースがアクセラレーターのエンドポイントまたは共有 IP アドレスプールとして使用されているかどうかを管理できます。

プリンシパルのアクセス許可

一般的に、プリンシパルは、アタッチメントがアクセス許可を付与するアクセラレーターのクロスアカウントアタッチメントにリストされているリソースを追加できます。アクセス許可を持つクロスアカウントリソースでは、BYOIP アドレスプールからエンドポイントを表示、追加、または削除したり、共有 IP アドレスを選択したりすることしかできません。

プリンシパルには以下が適用されます:

- プリンシパルは、クロスアカウントアタッチメントでアクセス許可が付与されたアクセラレーターのエンドポイントまたは共有 IP アドレスプールとしてのみ、リソースを表示、追加、または削除できます。
- プリンシパルは、自分自身が所有するロードバランサーなどのリソースのみ変更できます。リソースはリソース所有者に属するため、クロスアカウントアタッチメントで指定されたリソースを変更することはできません。

プリンシパルは実際のクロスアカウントリソースを変更することはできませんが、クロスアカウントアタッチメントに基づいて、リソース所有者はリソースへのアクセス許可を提供する IAM ロールを作成できます。その後、所有者はプリンシパルにロールを引き受ける許可を付与できます。これにより、プリンシパルはリソースにアクセスし、所有者がロールのアクセス許可で指定した方法で使用できるようになります。

Global Accelerator のクロスアカウントリソースの請求コスト

AWS Global Accelerator のアクセラレーターの所有者には、アクセラレーターに関連するコストが請求されます。アクセラレーター所有者またはリソース所有者の場合、クロスアカウントリソースをエンドポイントとして追加したり、アクセラレーターに独自の IP アドレス (BYOIP) プールを持ち込むために追加コストはかかりません。

料金の詳細については、「AWS Global Accelerator の料金」を参照してください。

Global Accelerator のクロスアカウントリソースのクォータ

以下の内容は、AWS Global Accelerator でクロスアカウントアタッチメントとクロスアカウントリソースを使用する場合に適用されます:

- クロスアカウントアクセス許可を持つすべてのプリンシパルによって追加されたリソースを含む、アクセラレーターのエンドポイントとして追加されたすべてのクロスアカウントリソースおよびその他のリソースは、アクセラレーターの有効なクォータに計算されます。
- アクセラレーターのクォータはプリンシパルに適用されます。
- Global Accelerator のクロスアカウントアタッチメントのクォータは、リソース所有者に適用されます。

クォータの詳細については、「AWS Global Accelerator のクォータ」を参照してください。

AWS Global Accelerator 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と、Global Accelerator でのカスタムドメインの使用に関する情報について説明します。また、Global Accelerator のアクセラレーターで使用する独自の IP (BYOIP) アドレスの持ち込みを設定する手順も含まれています。

- DNS アドレス指定: アクセラレータを作成すると、Global Accelerator はデフォルトのドメインネームシステム (DNS) 名をアクセラレータに割り当てます。
- カスタムドメイン名: 割り当てられた静的 IP アドレスやデフォルトの DNS 名を使用する代わりに、アクセラレータでカスタムドメイン名 (`www.example.com` など) を使用するように DNS を設定できます。
- BYOIP IP アドレス : Global Accelerator が割り当てる静的 IP アドレスの代わりに、または一緒に、独自の IP アドレスを AWS に持ち込んでアクセラレーターに追加できます。

内容

- AWS Global Accelerator での DNS アドレス指定のサポート
- カスタムドメイントラフィックをアクセラレーターにルーティングする
- Global Accelerator の Bring your own IP (BYOIP)

AWS Global Accelerator での DNS アドレス指定のサポート

IPv4 IP アドレスタイプでアクセラレータを作成すると、Global Accelerator は 2 つの静的 IPv4 アドレスをプロビジョニングします。また、`a1234567890abcdef.awsglobalaccelerator.com` と同様に、静的 IP アドレスを指すデフォルトのドメインネームシステム (DNS) 名をアクセラレータに割り当てます。

デュアルスタック IP アドレスタイプのアクセラレーターの場合、Global Accelerator は 2 つの静的 IPv4 アドレスと 2 つの静的 IPv6 アドレスの合計 4 つのアドレスを提供します。Global Accelerator は、A レコードと 4 つの IP アドレスすべてを指す AAAA レコードの両方を指す新しい DNS 名を作成します。新しい DNS レコードにより、Global Accelerator は、デュアルスタックではない元の DNS レコードを現在参照しているクライアントに影響を与えることなく、アクセラレーターをデュアルスタックにアップグレードできます。デュアルスタック IP アドレスを持つアクセラレーターの DNS 名の例を次に示します: `a1234567890abcdef.dualstack.awsglobalaccelerator.com`

静的アドレスは、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。アクセラレーターの静的アドレスまたは DNS 名を使用して、トラフィックをアクセラレーター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 DNS」プロセスを使用してアクセラレーターの DNS 名を解決するため、名前はアクセラレーターの静的 IP アドレスに解決され、Amazon Route 53 によってランダムに返されます。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**
>
> アクセラレーターに関連付けられた IPv4 および IPv6 アドレスごとに、Global Accelerator は、アクセラレーターの静的 IP アドレスを Global Accelerator によって生成された対応する DNS 名にマッピングするポインター (PTR) レコードを作成し、リバース DNS ルックアップをサポートします。これはリバースホストゾーンとも呼ばれます。Global Accelerator が生成する DNS 名は設定できず、カスタムドメイン名を指定する PTR レコードを作成できないことに注意してください。Global Accelerator は、AWS (BYOIP) に持ち込む IP アドレス範囲から静的 IP アドレスの PTR レコードも作成しません。

カスタムドメイントラフィックをアクセラレーターにルーティングする

ほとんどのシナリオでは、割り当てられた静的 IP アドレスやデフォルトの DNS 名を使用する代わりに、アクセラレーターでカスタムドメイン名 (`www.example.com` など) を使用するように DNS を設定できます。まず、Amazon Route 53 または他の DNS プロバイダーを使用してドメイン名を作成し、Global Accelerator 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ーの DNS 名に関連付けることもできます。DNS 設定を完了し、インターネット経由で変更が伝達されるのを待ちます。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行うと、DNS サーバーはそれを IP アドレス、ランダムな順序、またはアクセラレーターの 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 Global Accelerator 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ーに割り当てられた DNS 名にポイントするエイリアスレコードを作成します。エイリアスレコードは、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) とサブドメイン (`www.example.com` など) の両方にエイリアスレコードを作成できます。詳細については、「Amazon Route 53 デベロッパーガイド」の「エイリアスリソースレコードセットと非エイリアスリソースレコードセットの選択」を参照してください。

アクセラレーターのエイリアスレコードで Route 53 を設定するには、Amazon Route 53 デベロッパーガイドの次のトピック:「エイリアスターゲット」に含まれるガイダンスに従います。Global Accelerator の情報を表示するには、[エイリアスターゲット] ページを下にスクロールします。

Global Accelerator の Bring your own IP (BYOIP)

すべての公開 IPv4 アドレス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 アカウントに導入し、AWS Global Accelerator と使い合わせます。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。IPv6 を使用した BYOIP は現在サポートされていません。

Global Accelerator は、アクセラレーター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、Global Accelerator は Amazon IP アドレスプールから静的 IP アドレスを提供します。Global Accelerator が提供する IP アドレスを使用する代わりに、これらのエントリポイントを独自のアドレス範囲から IPv4 アドレスに設定できます。このトピックでは、Global Accelerator で独自の IP アドレス範囲を使用する方法について説明します。

AWS に持ち込んだ IP アドレスはを、1 つの AWS サービスで使用した場合、他のサービスでは使用できません。この章内の手順ップでは、独自の IP アドレス範囲を AWS Global Accelerator でのみ使用する方法について説明します。Amazon EC2 での使用のために独自の IP アドレスの導入の手順については、「Amazon EC2 ユーザーガイド」の「Bring your own IP (BYOIP) を使用する」を参照してください。

> **Important**
>
> AWS を介して IP アドレス範囲をアドバタイズする前に、他の場所からの IP アドレス範囲のアドバタイズ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 (つまり、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ている) 場合、そのアドレス範囲へのトラフィックが当社のネットワークに入ることや、BYOIP アドバタイズのワークフローが正常に完了することを保証できません。

アドレス範囲を AWS に導入すると、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。アクセラレーターを作成するときは、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。Global Accelerator 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。2 つの IP アドレス範囲を AWS に持ち込む場合、各範囲から 1 つの IP アドレスをアクセラレー

ターに割り当てることができます。この制限は、Global Accelerator が高可用性のために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。

Global Accelerator で独自の IP アドレス範囲を使用するには、要件を確認し、このトピックで説明されているステップに従います。

内容

- 要件
- AWS アカウントに IP アドレス範囲を持ち込むために準備する
- Global Accelerator で使用するためのアドレス範囲をプロビジョニングする
- AWS を通じてアドレス範囲をアドバタイズする
- アドレス範囲のプロビジョニング解除
- Global Accelerator のアクセラレーターで BYOIP アドレスを使用する
- アクセラレーターを更新して IP アドレスを変更する

要件

アカウント AWS ごとに最大 2 つの対象となる IP アドレス範囲を AWS Global Accelerator にすることができます。

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 アドレス範囲は以下の地域インターネットレジストリ (RIR、Regional Internet Registry) に登録する必要があります: American Registry for Internet Numbers (ARIN)、Réseaux IP Européens Network Coordination Centre (RIPE)、または Asia-Pacific Network Information Centre (APNIC)。アドレス範囲は、企業または機関エンティティに登録する必要があります。個人に登録することはできません。
- 導入できる唯一のアドレス範囲は /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。例えば、198.51.100 は IP アドレス 198.51.100.0 のネットワーク番号です。
- アドレス範囲内の IP アドレスには、消去履歴が含まれている必要があります。つまり、評判が悪くなったり、悪意のある動作に関連付けられたりすることはできません。IP アドレス範囲の評判を調査し、クリーンな履歴がない IP アドレスが含まれていることが判明した場合、IP アドレス範囲を拒否する権利を保留します。

また、IP アドレス範囲を登録した場所に応じて、次の割り当てネットワークタイプと割り当てネットワークステータスが必要です:

- ARIN: `Direct Allocation` および `Direct Assignment` ネットワークタイプ
- RIPE: `ALLOCATED PA`、`LEGACY`、および `ASSIGNED PI` 割り当てステータス
- APNIC: `ALLOCATED PORTABLE` および `ASSIGNED PORTABLE` クォータステータス

AWS アカウントに IP アドレス範囲を持ち込むために準備する

あなたのみが自分の IP アドレススペースを Amazon に持ち込めるようにするため、次の 2 つの認証が必要です。

- Amazon が IP アドレス範囲をアドバタイズすることを許可する必要があります。
- IP アドレス範囲を所有していることの証明を提供し、AWS に持ち込む権限を持っている必要があります。

> **Note**
>
> BYOIP を使用して IP アドレス範囲を AWS にする場合、そのアドレス範囲の所有権を別のアカウントまたは会社に移管することはできません。また、IP アドレス範囲をある AWS アカウントから別のアカウントに直接移管することはできません。所有権を移管したり、AWS アカウント間で移管したりするには、アドレス範囲のプロビジョニングを解除し、新しい所有者が自分の AWS アカウントにアドレス範囲を追加するステップに従う必要があります。

Amazon に IP アドレス範囲のアドバタイズを許可するには、署名付き認証メッセージを Amazon に提供します。Route Origin Authorization (ROA) を使用して、この承認を提供します。ROA は、利用している地域インターネットレジストリ (RIR) を介して作成できる、経路広告に関する電子署名付き証明書です。ROA には、IP アドレス範囲、その IP アドレス範囲を公開することを許可された AS 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) で IP アドレス範囲をアドバタイズすることを許可します。

ROA はその 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するわけではありません。この認証を提供するには、IP アドレス範囲の Registry Data Access Protocol (RDAP) リマークスで自己署名の 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可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、これらの手順を完了するための詳細な手順について説明します。これらの手順のコマンドは、Linux でサポートされています。Windows を使用する場合、「Windows Subsystem for Linux」をアクセスして、Linux コマンドを実行できます。

認証を提供する手順

- ステップ 1: ROA オブジェクトを作成する
- ステップ 2: 自己署名の 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

IP アドレス範囲をアドバタイズするために Amazon ASN 16509 を承認し、また、IP アドレス範囲をアドバタイズすることが現在許可されている ASN も承認するために、ROA オブジェクトを作成します。ROA には、AWS に持ち込む /24 IP アドレスが含まれ、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、以下のセクションを参照してください:

- ARIN: ROA のリクエスト数
- RIPE: ROA の管理
- APNIC: 経路管理

ステップ 2: 自己署名の X.509 証明書を作成する

キーペアと自己署名の 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。次の手順では、これらのタスクを実行する方法を説明します。

> **Note**
>
> これらの手順での `openssl` コマンドには、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 ビットのキーペアを生成します。

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

2. 次のコマンドを使用してキーペアからパブリック 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きは、正しい有効期限の希望値に –days オプションを設定してください。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、RIR の RDAP レコードを X.509 証明書で更新します。

   1. 次のコマンドを実行して、証明書を表示します。

```
cat publickey.cer
```

   2. 以前に作成した証明書を、RIR の RDAP レコードに追加します。エンコードされた部分の前後の `-----BEGIN CERTIFICATE-----` および `-----END CERTIFICATE-----` 文字列を、必ず含めます。このコンテンツはすべて、長い 1 行にする必要があります。RDAP を更新する手順は、ご使用の RIR によって異なります。

      - ARIN の場合は、Account Manager ポータルを使用して、アドレス範囲を表す「ネットワーク情報」オブジェクトの「パブリックコメント」セクションに証明書を追加してください。組織の [comments] セクションには追加しないでください。
      - RIPE の場合は、証明書を新しい「descr」フィールドとして、アドレス範囲を表す「inetnum」または「inet6num」オブジェクトに追加します。これらは通常、RIPE Database ポータルの「マイリソース」セクションにあります。組織の [コメント] セクションや上記オブジェクトの「備考」フィールドには追加しないでください。
      - APNIC の場合は、証明書を電子メールで helpdesk@apnic.net に送信し、アドレス範囲の "remarks" フィールドに手動で追加します。APNIC の IP アドレスに関する正規連絡先に電子メールを送信します。

   以下のプロビジョニング段階が完了したら、RIR の記録から証明書を削除できます。

ステップ 3: 署名付き認可メッセージを作成する

Amazon が IP アドレス範囲をアドバタイズできるようにする署名付き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。日付 YYYYMMDD はメッセージの有効期限日になります。

```
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. 次に例を示すように、プレーンテキストの認可メッセージを作成し、text_message という名前の変数に保存します。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. 前のセクションで作成したキーペア text_message を使用して、認証メッセージに署名します。
3. 次の例に示すように、メッセージを signed_message という名前の変数に保存します。

   ```
   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")
   ```

Global Accelerator で使用するための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 による当該範囲のアドバタイズを承認します。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 Global Accelerator API オペレーション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、次の ProvisionByoipCidr コマンドを使用します。--cidr-authorization-context パラメータでは、以前に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 --region us-west-2 provision-byoip-cidr --cidr address-range --
cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

アドレス範囲をプロビジョニングする例を次に示します。

```
aws globalaccelerator --region us-west-2 provision-byoip-cidr
    --cidr 203.0.113.0/24
    --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操作であるため、呼び出しはすぐに返されます。ただし、アドレス範囲は、状態が PENDING_PROVISIONING から READY に変わるまで使用できません。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モニタリングするには、次の ListByoipCidrs コマンドを使用します:

```
aws globalaccelerator --region us-west-2 list-byoip-cidrs
```

IP アドレス範囲の状態のリストを確認するには、「ByoipCidr」を参照してください。

IP アドレス範囲がプロビジョニングされると、list-byoip-cidrs によって返される State は READY です。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 を介して IP アドレス範囲をアドバタイズする前に、他の場所からの IP アドレス範囲のアドバタイズを停止する必要があります。

CLI または Global Accelerator API オペレーションを使用して、アドレス範囲をアドバタイズ (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、以下の「advertise-byoip-cidr」コマンドを使用します。

```
aws globalaccelerator --region us-west-2 advertise-byoip-cidr --cidr address-range
```

以下は、アドレス範囲をアドバタイズするように Global Accelerator にリクエストする例です。

```
aws globalaccelerator --region us-west-2 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モニタリングするには、次の「ListByoipCidrs」コマンドを使用します。

```
aws globalaccelerator --region us-west-2 list-byoip-cidrs
```

IP アドレス範囲がアドバタイズされると、`list-byoip-cidrs` によって返される `State` は `ADVERTISING` です。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 `withdraw-byoip-cidr` コマンドを使用します。

> **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 オペレーションを使用してアクセラレーターを削除するには、アクセラレーターを削除する を参照してください。

```
aws globalaccelerator --region us-west-2 withdraw-byoip-cidr --cidr address-range
```

以下は、Global Accelerator にアドレス範囲の取り消しをリクエストする例です。

```
aws globalaccelerator --region us-west-2 withdraw-byoip-cidr
    --cidr 203.0.113.0/24
```

アドレス範囲のプロビジョニング解除

AWS での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ーを削除し、アドレス範囲のアドバタイズを停止する必要があります。これらのステップを完了したら、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 Global Accelerator API オペレーションを使用して、アドレス範囲の広告を停止し、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ーを削除します。コンソールまたは API オペレーションを使用してアクセラレーターを削除するには、アクセラレーターを削除する を参照してください。

Step 2. アドレス範囲のアドバタイズを停止します。アドレス範囲の公開を停止するには、以下の「WithdrawByoipCidr」コマンドを使用します。

```
aws globalaccelerator --region us-west-2 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。アドレス範囲のプロビジョニングを解除するには、以下の「DeprovisionByoipCidr」コマンドを使用します。

```
aws globalaccelerator --region us-west-2 deprovision-byoip-cidr --cidr address-range
```

Global Accelerator のアクセラレーターで BYOIP アドレスを使用する

BYOIP でアドレス範囲を追加するステップを完了したら、BYOIP IP アドレスを使用してアクセラレーターを作成するか、既存のアクセラレーターで BYOIP IP アドレスを使用できます。1 つのアドレス範囲を AWS に持ち込んだ場合は、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持ち込んだ場合は、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ーに割り当てることができます。

既存のアクセラレーターを更新して、1 つ以上の BYOIP IP アドレスを使用することもできます。詳細については、「アクセラレーターを更新して IP アドレスを変更する」を参照してください。

もう 1 つのオプションは、共有 BYOIP アドレスを使用することです。別のアカウントから 1 つ以上の追加の CIDR アドレスが共有されている場合は、1 つまたは両方の BYOIP IP アドレスを選択したときに、共有 BYOIP CIDR から選択できます。2 つの共有 BYOIP アドレスを使用する場合は、どちらも同じアカウントが所有する CIDR から取得する必要があります。詳細については、「Global Accelerator でクロスアカウントアクセスを設定する」を参照してください。

静的 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ーを作成するためのオプションがいくつかあります。

- Global Accelerator コンソールを使用してアクセラレーターを作成します。詳細については、次を参照してください:
  - アクセラレーターを作成する
  - Global Accelerator でカスタムルーティングアクセラレーターを作成する
  - AWS Global Accelerator でクロスアカウントエンドポイントを追加する
- Global Accelerator API を使用してアクセラレーターを作成します。CLI の使用例などの詳細については、AWS Global Accelerator API Reference の以下内容を参照してください。
  - CreateAccelerator
  - CreateCustomRoutingAccelerator

アクセラレーターを更新して IP アドレスを変更する

BYOIP アドレスを AWS Global Accelerator のアクセラレーターの静的 IP アドレスとして割り当てた後、後でアクセラレーターを更新して、アドレス範囲とは異なる IP アドレスを使用できます。また、独自の IP アドレスを使用するアクセラレーターを更新して、AWS Global Accelerator が提供する IP アドレスを使用することもできます。

Amazon 所有の静的 IP アドレスを変更したら、元の静的 IP アドレスに戻すことができますが、変更してから 10 日以内に元に戻す必要があります。10 日後、元の静的 IP アドレスは Amazon IP アドレスプールに返され、再利用されます。その後、アクセラレーターを更新して BYOIP アドレスを Global Accelerator が割り当てた IP アドレスに変更すると、Amazon IP アドレスプールから新しい IP アドレスが割り当てられます。IP アドレスの復元の詳細については、「静的 IP アドレス変更の復元」を参照してください。

以下のセクションでは、Global Accelerator で Bring your own IP (BYOIP) を持ち込む際に IP アドレスを変更する方法と、静的 IP アドレスを変更するときに知っておくべき要件と事項について説明します。

アクセラレーターを更新して IP アドレスを変更する方法

アクセラレーターの IP アドレスを変更するには、アクセラレーターを編集してから、[IP アドレス] で新しい IP アドレスを選択します。独自の BYOIP アドレスプールまたは Amazon IP アドレスプールからアドレスを選択できるかどうかのオプションは、アクセラレーターが静的 IP アドレスに対して既に持っているもの、およびその他の要因によって異なります。

開始する前に、アクセラレーターの静的 IP アドレスを変更する際に「注意すべき要件と事項」を確認してください。

以下のトピックでは、アクセラレーターを更新する手順について説明します。

- Global Accelerator コンソールを使用してアクセラレーターを更新します。詳細については、次を参照してください:
  - アクセラレーターを更新する
  - Global Accelerator でカスタムルーティングアクセラレーターを編集する
- Global Accelerator API を使用してアクセラレーターを更新します。CLI の使用例などの詳細については、AWS Global Accelerator API Reference の以下内容を参照してください。
  - UpdateAccelerator
  - UpdateCustomRoutingAccelerator

IP アドレスを変更するためにアクセラレーターを更新する場合の要件

アクセラレーターを更新して 1 つまたは両方の静的 IP アドレスを変更する場合は、次の点に注意してください。

- 標準アクセラレーターとカスタムルーティングアクセラレーターの両方の BYOIP アドレスを変更できます。1 つまたは 2 つの BYOIP アドレスを持つアクセラレーターを作成した後、そのアクセラレーターには常に少なくとも 1 つの BYOIP アドレスが必要です。ただし、アクセラレーターを更新して、1 つまたは両方の静的 IP アドレスを変更して BYOIP アドレスを使用したり、BYOIP アドレスを変更したりできます。
- 2 つの BYOIP 静的 IP アドレスを持つアクセラレーターがある場合、Global Accelerator によって割り当てられた静的 IP アドレスを使用するように変更できるのは、そのうちの 1 つのみです。アクセラレーターの BYOIP 静的 IP アドレスを Global Accelerator が割り当てた静的 IP アドレスに変更するには、次の点に注意してください。
  - アドレスを元の Global Accelerator 静的 IP アドレスのいずれかに戻すことができるのは、BYOIP アドレスに変更してから 10 日以内に変更した場合のみです。10 日後、元の静的 IP

アドレスは Global Accelerator IP アドレスプールに返され、再利用されます。その後、アクセラレーターを更新して BYOIP アドレスを Global Accelerator が割り当てた IP アドレスに変更すると、Global Accelerator IP アドレスプールから新しい IP アドレスが割り当てられます。

  - 代わりに Global Accelerator の静的 IP アドレスを使用するように両方の BYOIP 静的 IP アドレスを変更することはできません。Global Accelerator によって割り当てられた 2 つの静的 IP アドレスをアクセラレーターで使用するには、新しいアクセラレーターを作成します。
- 2 つの BYOIP アドレスを使用しているアクセラレーターがある場合は、どちらかを別の BYOIP アドレスに変更できます。ただし、アクセラレーターの作成時に BYOIP アドレスを追加する場合と同じ制限が適用されます。例えば、2 つの異なる BYOIP アドレスを使用するようにアクセラレーターを更新する場合、アドレスは Global Accelerator に追加した異なる BYOIP アドレス範囲のものでなければなりません。
- クロスアカウント BYOIP アドレスを設定している場合、アクセラレーターの静的 IP アドレスを更新するときに、クロスアカウントアドレスを使用できます。
- 特定のシナリオでは、BYOIP アドレスを更新するときに、Global Accelerator が更新を正常に完了できるように Amazon 静的 IP アドレスを変更する必要がある場合があります。Amazon 静的 IP アドレスは以下の場合にのみ影響を受ける可能性があります：1) アクセラレーターの BYOIP 静的 IPv4 アドレスを更新して別のアカウント (クロスアカウント BYOIP アドレス) の BYOIP アドレスを使用するようにし、2) アクセラレーターの 2 番目の静的 IP アドレスが Amazon プールのものである。

  Amazon 静的 IP アドレスを変更したくない場合は、更新から 10 日が経過していない場合にのみ、以前の Amazon IP アドレスに戻すことができます。変更を元に戻すと、アクセラレーターの元の Amazon IP アドレスが復元されます。ただし、10 日が経過すると、Amazon IP アドレスは使用可能な IP アドレスプールにリリースされ、復元できなくなります。

静的 IP アドレスの変更を元に戻す

アクセラレーターの元の Amazon IP アドレスに戻すには、次の手順を実行します。

- アクセラレーターを、新しいアドレスに変更した元の BYOIP 静的 IP アドレスで更新します。

この更新を行うと、Global Accelerator は元の Amazon 静的 IP アドレスも復元します。

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

AWS Global Accelerator のクライアント IP アドレスを保存およびアクセスする方法は、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。クライアント IP アドレスの保存を有効にすると、ロードバランサーに到着するパケットに対して、元のクライアントのソース IP アドレスが保存されます。

カスタムルーティングアクセラレーターのエンドポイントでは、常にクライアント IP アドレスが保存されます。受信パケットでクライアントのソース IP アドレスを保存できる標準アクセラレーターのエンドポイントには、Application Load Balancer、Amazon EC2 インスタンス、およびセキュリティグループを使用する Network Load Balancer の 3 つのタイプがあります。クライアント IP アドレスの保存を伴うエンドポイントとして追加する特定のリソースには、要件と制限があります。詳細については、「クライアント IP アドレスの保存による移行エンドポイント」を参照してください。

Global Accelerator は、次のエンドポイントタイプのクライアント IP アドレスの保存をサポートしていないことに注意してください。

- セキュリティグループなしの Network Load Balancer
- Elastic IP アドレス

エンドポイント要件の詳細については、アクセラレーターエンドポイントとして追加するリソースの要件 を参照してください。

内容

- Global Accelerator でのクライアント IP アドレスの保存に関するガイドラインと制限事項
- クライアント IP アドレスが保存されているエンドポイントの要件
- AWS Global Accelerator でクライアント IP アドレスが保存される方法
- クライアント IP アドレスの保存の利点
- クライアント IP アドレスを保存する ENI とセキュリティグループのベストプラクティス
- クライアント IP アドレスの保存による移行エンドポイント

Global Accelerator でのクライアント IP アドレスの保存に関するガイドラインと制限事項

AWS Global Accelerator でクライアント IP アドレスの保存を準備して使用するときは、次のガイドラインと制限に注意してください。

クライアント IP アドレスの保存を追加する場合は、次の点に注意してください。

- クライアント IP アドレスを保存するエンドポイントに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、必要なセキュリティ設定がすべて更新され、許可リストにユーザークライアント IP アドレスが含まれていることを確認してください。
- Global Accelerator の IP アドレスではなく、AWS WAF にクライアント IP アドレスが表示される場合があります。クライアント IP アドレスは、Global Accelerator でクライアント IP アドレスの保存を設定し、Application Load Balancer への接続が Global Accelerator からのものでない場合に AWS WAF を有効にしてブロックする場合に AWS WAF に表示されます。
- クライアント IP アドレスの保存は、Global Accelerator がサポートされているすべての AWS リージョン で利用可能です。サポートされているリージョンのリストについては「AWS Global Accelerator のための AWS リージョン の可用性」を参照してください。

新しいアクセラレーターを作成すると、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。クライアント IP アドレス保存のデフォルト設定は、エンドポイントのタイプによって異なります:

- Global Accelerator でインターネット向け Application Load Balancer をエンドポイントとして使用すると、新しいアクセラレーターのクライアント IP アドレスの保存がデフォルトで有効になります。このオプションは、アクセラレータを作成する際に無効化するか、後からアクセラレーターを編集して無効化することができます。
- Global Accelerator で内部 Application Load Balancer または EC2 インスタンスを使用する場合、エンドポイントは常にクライアント IP アドレスの保存が有効になっています。
- Global Accelerator でセキュリティグループを使用した Network Load Balancer をエンドポイントとして追加する場合、クライアント IP アドレスの保存はデフォルトでは有効になっていません。

以下の点に注意してください。

- 内部 Application Load Balancer および EC2 インスタンスでは、常にクライアント IP アドレスの保存が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ーを作成すると、Application Load Balancer エンドポイントのクライアント IP アドレスの保存オプションがデフォルトで有効になります。このオプションは、セキュリティグループエンドポイントを持つ Network Load Balancer ではデフォルトで有効になっていません。これらのエンドポイントのクライアント IP アドレス保存のオプションは、追加後いつでも更新できます。
- 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ーを作成し、クライアント IP アドレスの保存オプションを指定しない場合、クライアント IP アドレスの保存のデフォルト設定は次のとおりです。
  - インターネット向け Application Load Balancer エンドポイントでは、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っています。
  - セキュリティグループエンドポイントを持つ Network Load Balancer では、クライアント IP アドレスの保存はデフォルトでは有効になっていません。

既存のアクセラレーターでは、クライアント IP アドレスを保存せずにエンドポイントを、クライアント IP アドレスを保存するエンドポイントに移行できます。例えば、既存の Application Load Balancer エンドポイントを新しい Application Load Balancer エンドポイントに移行できます。新しいエンドポイントへの移行に際しては、以下の手順を実行することで、既存のエンドポイントからクライアント IP アドレスの保存を有効にした新しいエンドポイントへ、トラフィックを徐々に移動させることをお勧めします:

- セキュリティグループエンドポイントを持つ既存の Application Load Balancer または Network Load Balancer の場合は、まず、同じバックエンドをターゲットとする重複ロードバランサーエンドポイントを Global Accelerator に追加し、クライアント IP アドレスの保存が有効になっていることを確認します。次に、エンドポイントの重みを調整し、クライアント IP アドレスの保存が有効になっていないロードバランサーから、クライアント IP アドレスの保存が有効なロードバランサーへトラフィックを徐々に移動させます。
- 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 アドレスの保存により、トラフィックを EC2 インスタンスエンドポイントに移動できます。まず 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徐々に移動させます。

詳しい移行ガイダンスについては、クライアント IP アドレスの保存を使用するエンドポイントの移行 を参照してください。

クライアント IP アドレスが保存されているエンドポイントの要件

クライアント IP アドレスの保存で使用できるエンドポイントタイプには、特定の要件があります。> この機能は、このセクションで説明する追加要件に従って、Application Load Balancer、セキュリティグループを持つ Network Load Balancer、Amazon EC2 インスタンスである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ーのエンドポイントでは、常にクライアント IP アドレスが保存されます。

このセクションでは、クライアント IP アドレスの保存を有効にして追加するエンドポイントに固有の情報を提供します。全体的なエンドポイント要件の詳細については、アクセラレーターエンドポイントとして追加するリソースの要件 を参照してください。

さらに、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の詳細については、クライアント IP アドレスを保存する ENI とセキュリティグループのベストプラクティス を参照してください。

クライアント IP アドレスの保存機能を使用する場合は、Global Accelerator のエンドポイントの全体的な要件に加えて、Global Accelerator にエンドポイントを追加するときに以下の点に注意してください。

Elastic IP アドレス

Global Accelerator の Elastic IP アドレスエンドポイントでは、クライアント IP アドレスの保存はサポートされていません。

Network Load Balancer エンドポイント

Network Load Balancer リソースを Global Accelerator にエンドポイントとして追加するときにクライアント IP アドレスの保存を有効にする場合は、クライアント IP アドレスの保存は以下ではサポートされていないことに注意してください。

- セキュリティグループなしの Network Load Balancer
- TLS リスナーがアタッチされたセキュリティグループを使用する
- EC2 ターゲットへの IPv4 から IPv6 への NAT 変換を実行するセキュリティグループを使用する Network Load Balancer

さらに、Network Load Balancer では、ターゲットが Network Load Balancer と同じ VPC にある場合にのみ、クライアント IP アドレスの保存がサポートされます。トラフィックは、Network Load Balancer からターゲットに直接流れる必要があります。

Elastic Network Interface

クライアント IP アドレスの保存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 Network Interface を作成します。Global Accelerator がElastic Network Interface と連携する方法の詳細については、クライアント IP アドレスを保存する ENI とセキュリティグループのベストプラクティス を参照してください。

プライベートサブネット内のエンドポイント

Global Accelerator を使用して、プライベートサブネット内の Application Load Balancer 、Network Load Balancer 、または EC2 インスタンスをターゲットにできますが、エンドポイントを含む VPC に「インターネットゲートウェイ」がアタッチされている必要があります。詳細については、「AWS Global Accelerator での安全な VPC 接続」を参照してください。

ベストプラクティスとして、トラフィックを Global Accelerator のみで配信したい場合は、プライベートサブネットを使用することをお勧めします。また、インバウンドセキュリティグループルールが、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 IP アドレスを許可リストに追加する

クライアント IP アドレスを保存するエンドポイントを追加し、トラフィックのルーティングを開始する前に確認してください。必要なすべてのセキュリティ設定 (例: セキュリティグループ) が、ユーザークライアントの IP アドレスを許可リストに含めるよう更新されていることを確認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) は、送信 (アウトバウンド) トラフィックにのみ適用されます。受信 (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) を設定する

VPC サブネットに関連付けられたネットワーク ACL は、アクセラレーターでクライアント IP アドレスの保存が有効になっている場合、送信 (アウトバウンド) トラフィックに適用されます。ただし、トラフィックを Global Accelerator 経由で終了できるようにするには、ACL をインバウンドルールとアウトバウンドルールの両方として設定する必要があります。

例えば、エフェメラルソースポートを使用して TCP および 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、エフェメラル 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、ソース 0.0.0.0/0) を作成します。

セキュリティグループと WAF については、次の点に注意してください:

- 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。例えば、Amazon EC2 インスタンスと Application Load Balancer 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 Global Accelerator を介して接続できる送信先ポートを制御できます。例えば、HTTP の場合はポート 80、HTTPS の場合はポート 443 などです。
- Amazon EC2 インスタンス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。

AWS Global Accelerator でクライアント IP アドレスが保存される方法

AWS Global Accelerator は、Amazon EC2 インスタンス、Network Load Balancer、Application Load Balancer でクライアントのソース IP アドレスを次のように保存します:

- EC2 インスタンスエンドポイントの場合、すべてのトラフィックのクライアント IP アドレスは保存されます。
- クライアント IP アドレスが保存されている Network Load Balancer エンドポイントの場合、Global Accelerator は Network Load Balancer と連携して、元のクライアントの IP アドレスをパケットの IP ヘッダーに含めて、アプリケーションがアクセスできるようにします。
- クライアント IP アドレスが保存されている Application Load Balancer エンドポイントの場合、Global Accelerator は Application Load Balancer と連携して、ウェブ層がアクセスできるように `X-Forwarded-For`、元のクライアントの IP アドレスを含む `X-Forwarded` ヘッダーを提供します。

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は、「メッセージヘッダー」RFC 2616 で定義されています。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 というプレフィックスが付いている場合があります。

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、ターゲットコード (インスタンス、コンテナ、Lambda コードなど) までのクライアント IP アドレスは保存されません。ターゲットが TCP パケットに表示される送信元 IP アドレスは、Application Load Balancer の IP アドレスです。ただし、Application Load Balancer は、元のパケットの返信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 接続を介してリクエストをバックエンドに送信することで、元のクライアント IP アドレスを保存します。

X-Forwarded-For リクエストヘッダーの形式は次のとおりです:

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

以下に、IP アドレスが 203.0.113.7 であるクライアントの X-Forwarded-For リクエストヘッダーの例を示します。

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

次の例は、IPv6 アドレスが 2001:DB8::21f:5bff:febf:ce22:8a2e であるクライアントの X-Forwarded-For リクエストヘッダーを示しています。

```
X-Forwarded-For: 2001:DB8::21f:5bff:febf:ce22:8a2e
```

クライアント IP アドレスの保存の利点

Global Accelerator では、特定のエンドポイントのクライアント IP アドレスの保存を設定できます。AWS Global Accelerator で設定するアプリケーションによっては、クライアント IP アドレスの保存に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場合があります。

例えば、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を収集できます。「Application Load Balancer のセキュリティグループ」などの IP アドレスベースのフィルターを使用して、トラフィックをフィルタリングすることもできます。元のクライアント IP アドレス情報を含むロードバランサーの X-Forwarded-For ヘッダーを使用して、Application Load Balancer エンドポイントの背後にあるウェブ層サーバーで実行されるアプリケーション内のユーザーの IP アドレスに固有のロジックを適用できます。Application Load Balancer または Network Load Balancer に関連付けられている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 IP アドレスの保存を使用することもできます。詳細については、「AWS Global Accelerator でクライアント IP アドレスが保存される方法」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 アドレスは保存されます。

クライアント IP アドレスの保存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で Global Accelerator サービスが使用する IP アドレスは、リクエスト元のユーザーの IP アドレスを到着パケットの送信元アドレスに置き換えます。元のクライアントの IP アドレスやクライアントのポートなどの接続情報は、トラフィックがアクセラレーターの背後にあるシステムに移動するため、保存されません。これは、多くのアプリケーション、特にパブリックウェブ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に適しています。

クライアント IP アドレスの保存がないエンドポイントの場合、エッジからトラフィックを転送するときに Global Accelerator が使用する送信元 IP アドレスをフィルタリングできます。Global Accelerator フローログを確認することで、受信パケットの送信元 IP アドレス (クライアント IP アドレスの保存が有効になっている場合はクライアント IP アドレスでもあります) に関する情報を確認できます。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 フローログインの設定と使用を参照してください。

クライアント IP アドレスを保存する ENI とセキュリティグループのベストプラクティス

AWS Global Accelerator でクライアント IP アドレスの保存を使用する場合は、このセクションの Elastic Network Interface (ENI) とセキュリティグループの情報とベストプラクティスに注意してください。

クライアント IP アドレスの保存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 Network Interface 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、これらのエラスティックネットワークインターフェイスを使用して、アクセラレーターの後ろに設定されたエンドポイントにトラフィックをルーティングします。この方法で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、Application Load Balancer (内部およびインターネット向け) 、セキュリティグループを持つ Network Load Balancer、Amazon EC2 インスタンスです。

> **Note**
>
> Global Accelerator に内部 Application Load Balancer や EC2 インスタンスの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内でターゲットとすることで、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流れるようにします。詳細については、「AWS Global Accelerator での安全な VPC 接続」を参照してください。

Global Accelerator がエラスティックネットワークインターフェイスを使用する方法

クライアント IP アドレスの保存が有効になっている Application Load Balancer または Network Load Balancer のエンドポイントを使用する場合、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 がアカウント内に作成する Elastic Network Interface の数が決定されます。Global Accelerator は、Application Load Balancer または Network Load Balancer の 1 つ以上の Elastic Network Interface を持つサブネットごとに 1 つの Elastic Network Interface を作成し、アカウント内のアクセラレーターが先頭に立っています。

次の例は、この仕組みを示しています。

- 例 1: Application Load Balancer にサブネット A とサブネット B に Elastic Network Interface 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を作成します。
- 例 2: 例えば、subnetA とsubnetB に Elastic Network Interface を持つ ALB1 を Accelerator1 に追加し、サブネット A とサブネット B に Elastic Network Interface を使用する ALB2 を Accelerator2 に追加すると、Global Accelerator は 2 つの Elastic Network Interface のみを作成します。1 つは subnetA に、もう 1 つは subnetB に作成します。
- 例 3: subnetA と subnetB に Elastic Network Interface を持つ ALB1 を Accelerator1 に追加し、subnetA と subnetC に Elastic Network Interface を持つ ALB2 を Accelerator2 に追加すると、Global Accelerator は 3 つの Elastic Network Interface を作成します。1 つは subnetA、もう 1 つは subnetB、もう 1 つは subnetC です。subnetA の Elastic Network Interface は、Accelerator1 と Accelerator2 の両方のトラフィックを配信します。

例 3 に示すように、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ーの後ろに配置される場合、エラスティックネットワークインターフェイスはアクセラレーター間で再利用されます。

Global Accelerator が作成する論理的な Elastic Network Interface は、単一のホスト、スループットのボトルネック、または単一の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内の単一の Elastic Network Interface として表示される他の AWS サービスと同様に、ネットワークアドレス変換 (NAT) ゲートウェイや Network Load Balancer などのサービス

と同様に、Global Accelerator は水平方向にスケールされた高可用性サービスとして実装されます。

アクセラレーターのエンドポイントが使用するサブネットの数を評価し、Global Accelerator が作成する Elastic Network Interface の数を決定します。アクセラレーターを作成する前に、必要なエラスティックネットワークインターフェイスの IP アドレススペース容量が十分であることを確認してください。つまり、関連するサブネットごとに少なくとも 1 つの空き IP アドレスです。十分な空き IP アドレス領域がない場合は、Application Load Balancer または Network Load Balancer および関連する Global Accelerator の Elastic Network Interface に十分な空き IP アドレス領域を持つ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ーのエンドポイントで Elastic Network Interface が使用されていないと判断した場合、Global Accelerator はインターフェイスを削除します。

Global Accelerator によって作成されたセキュリティグループ

Global Accelerator およびセキュリティグループを使用する際は、以下の情報とベストプラクティスを確認してください。

- Global Accelerator によって作成されたセキュリティグループは、維持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 によって作成されたセキュリティグループルールを変更すると、エンドポイントが異常になる可能性があります。その場合は、「AWS サポート」にお問い合わせください。
- Global Accelerator 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 Network Interface はすべて、Elastic Network Interface がどのサブネットに関連付けられているかに関係なく、同じセキュリティグループを使用します。

> **Important**
>
> Global Accelerator は、Elastic Network Interface 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。システムはこれを行うことを妨げませんが、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。

クライアント IP アドレスの保存による移行エンドポイント

アクセラレーターのエンドポイントにクライアント IP アドレスの保存をまだ設定していない場合は、このセクションのガイダンスに従って、1 つ以上のエンドポイントを追加し、ユーザーのクライアント IP アドレスを保存するエンドポイントに移行します。Application Load Balancer 、セキュリティグループを備えた Network Load Balancer、または Elastic IP アドレスエンドポイントを、クライアント IP アドレスが保存されている対応するロードバランサーエンドポイントまたは EC2 インスタンスエンドポイントに移行するように選択できます。

このセクションでは、AWS Global Accelerator コンソールを使用してエンドポイントを追加および移行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 API Reference」を参照してください。

クライアント IP アドレスの保存を使用するエンドポイントの移行

エンドポイントをクライアントの IP アドレスの保存にゆっくり移行することをお勧めします。

- 新しいエンドポイントを追加する: まず、クライアント IP アドレスを保存するために有効にする新しいロードバランサーまたは EC2 インスタンスエンドポイントを Global Accelerator に追加します。
- トラフィックをゆっくり増やす: 次に、エンドポイントの重みを設定して、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徐々に移動します。
- 進めながらテストを行う: クライアントの IP アドレスを保存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ら、設定が期待どおりに機能してい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ゆっくり増やします。

エンドポイントを移行するには、以下のセクションの手順に従ってください。

クライアント IP アドレスの保存は、Global Accelerator がサポートされているすべての AWS リージョン で利用可能です。サポートされているリージョンのリストについては「AWS Global Accelerator のための AWS リージョン の可用性」を参照してください。

> **Important**
>
> クライアント IP アドレスを保存するエンドポイントにトラフィックをルーティングする前に、Global Accelerator のクライアント IP アドレスを許可リストに含めたすべての設定を、ユーザーのクライアント IP アドレスを含めるように更新してください。

クライアント IP アドレスの保存でエンドポイントを追加するには

1. https://console.aws.amazon.com/globalaccelerator/home で Global Accelerator コンソールを開きます。
2. アクセラレーターページで、アクセラレータを選択します。
3. [リスナー] タブで、リスナーを選択します。
4. [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. [エンドポイント] セクションで、[エンドポイントの追加] を選択します。
6. [エンドポイントの追加] ページで、[エンドポイント] ドロップダウンメニューで、クライアント IP アドレスの保存をサポートするエンドポイントを選択します。
7. [重み] 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。例えば、対応する Application Load Balancer の重みが 255 の場合、新しい Application Load Balancer の重みに 5 を入力して開始できます。詳細については、「エンドポイントの重みがトラフィックボリュームを管理する仕組み」を参照してください。
8. 必要に応じて、[クライアント IP アドレスの保存] で、[アドレスの保存] を選択します。
9. [Save changes] (変更の保存) をクリックします。

次に、以下の手順に従って、対応する既存のエンドポイント (クライアント IP アドレスの保存で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. [エンドポイントグループ] ページで、クライアント IP アドレスの保存がない既存のエンドポイントを選択します。
2. [編集] を選択します。

3. [エンドポイントの編集] ページの [重み] 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。例えば、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に重みを 220 と入力できます (クライアント IP アドレスの保存あり) 。
4. [Save changes] (変更の保存) をクリックします。

新しいエンドポイントの重みを低い数に設定して元のトラフィックのわずかな部分でテストした後、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。

例えば、重みを 200 に設定した既存の Application Load Balancer から開始し、重みを 5 に設定したクライアント IP アドレスの保存が有効になっている新しい Application Load Balancer エンドポイントを追加すると仮定します。新しい Application Load Balancer の重みを増やし、元の Application Load Balancer Load Balancer の重みを減らすことで、トラフィックを元の Application Load Balancer から新しい Application Load Balancer にゆっくり移行します。例:

- 元の重み 190/新しい重み 10
- 元の重み 180/新しい重み 20
- 元の重み 170/新しい重み 30 など。

元のエンドポイントの重みを 0 に減らすと、すべてのトラフィック (この例のシナリオ) は、クライアント IP アドレスの保存を含む新しい Application Load Balancer エンドポイントに送信されます。

クライアント IP アドレスの保存を使用するように移行する追加のエンドポイントである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 アドレスを保存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。クライアント IP アドレスの保存がないエンドポイントの重みを元の値に増やし、クライアント IP アドレスの保存があるエンドポイントの重みを 0 に減らします。

AWS Global Accelerator でのログ記録とモニタリング

Amazon CloudWatch 、フローログ、および AWS CloudTrail を使用して、AWS Global Accelerator でアクセラレーターをモニタリングできます。例えば、リスナーとエンドポイントに関する問題のトラブルシューティング、トラフィックパターンの分析、監査に必要な情報の取得を行うことができます。

これらのログ記録とモニタリングメソッドは、ある程度重複する可能性があります。以下は、各メソッドの一般的な用途です。

- CloudWatch メトリクスは、追加のセットアップなしでリアルタイムの情報を提供し、セットアップのトラブルシューティングに役立ちます。また、本番稼働時に問題が発生した場合などに警告するアラームを作成することもできます。
- フローログは、アクセラレーターに入ってクライアントに戻るトラフィックに関する詳細情報を提供します。フローログは、到達可能性に関する問題のトラブルシューティングや、包括的な監査のための情報の提供に役立ちます。(フローログには Amazon S3 ストレージの設定と使用が必要であることに注意してください。)
- CloudTrail は、Global Accelerator API を呼び出すアクションを自動的に追跡します。これは、監査などに役立ちます。

> **Note**
>
> 米国西部 (オレゴン) リージョンの Global Accelerator に関する CloudWatch メトリクスとログは、両方ともコンソール上または AWS CLI の使用時に表示する必要があります。AWS CLI を使用するときは、`--region us-west-2` のパラメータを含めて、コマンドに米国西部 (オレゴン) リージョンを指定します。

トピック

- Amazon CloudWatch と AWS Global Accelerator の併用
- AWS Global Accelerator フローログインの設定と使用
- AWS CloudTrail を使用して AWS Global Accelerator API コールをログに記録する

Amazon CloudWatch と AWS Global Accelerator の併用

AWS Global Accelerator は、アクセラレーターのデータポイントを Amazon CloudWatch に公開します。CloudWatch では、それらのデータポイントについての統計を、(メトリクスと呼ばれる) 順序付けられた時系列データのセットとして取得できます。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。例えば、アクセラレーターを通じて、トラフィックを指定した期間内でモニタリングできます。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。

> **Note**
>
> 米国西部 (オレゴン) リージョンの Global Accelerator に関する CloudWatch メトリクスとログは、両方ともコンソール上または AWS CLI の使用時に表示する必要があります。AWS CLI を使用するときは、`--region us-west-2` のパラメータを含めて、コマンドに米国西部 (オレゴン) リージョンを指定します。

メトリクスを使用して、最初の Global Accelerator のセットアップをトラブルシューティングし、トラフィックがエンドポイントに到着し、レスポンスが返るかどうかを判断するのに役立ちます。自動的にログに記録される CloudWatch メトリクスを表示して、トラフィックが Network Load Balancer などのエンドポイントに届いているかどうかを確認します。Global Accelerator からエンドポイントへのアウトバウンド、Global Accelerator からクライアントへのバック、ロードバランサーなどのエンドポイントについても同じメトリクスが必要です。Global Accelerator から流れ込むが、バックアウトしないトラフィック、またはロードバランサーに到達しないトラフィックは、設定でトラフィックが想定ポートを通過することを許可し、セキュリティグループ設定でアクセスを許可することを確認する必要がある可能性があります。

メトリクスを使用して、システムが予定通りにに実行されていることを確認できます。例えば、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) を実行することができます。

リクエストがアクセラレーターを経由する場合のみ、Global Accelerator はメトリクスを CloudWatch に報告します。アクセラレーターを経由するリクエストがある場合、Global Accelerator は 60 秒間隔でメトリクスを測定し、送信します。アクセラレーター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。

内容

- Global Accelerator メトリクス
- アクセラレーターのメトリクスディメンション
- Global Accelerator TCP リセット問題のトラブルシューティング
- Global Accelerator メトリクスの統計
- アクセラレーターの CloudWatch メトリクスを表示する

Global Accelerator 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
ActiveFlowCount	Global Accelerator のアクセラレーターのクライアントからエンドポイントへの並行 TCP および UDP 接続の合計数。TCP 接続はアクセラレーターで終了したため、ターゲットへの TCP 接続を開いているクライアントは単一のフローとして計算されます。 このメトリクスを使用して、エンドポイントにアクセスしているアクティブなユーザー (接続数) の数をよりよく理解したり、トラフィックを処理するためにリソースをスケーリングする必要があるかどうかを判断したりできます。 報告基準: 設定および有効化されているアクセラレーターについて報告されます。 統計: 使用できる統計は Sum のみです。 ディメンション • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress

メトリクス	説明
Flows_Dropped_No_Endpoint_Found	IPv6 エンドポイントが利用できなかったためにドロップされた TCP IPv6 パケットフローの合計数。これは、デュアルスタック IP アドレスタイプのアクセラレーターがあり、アクセラレーターのエンドポイントの IP アドレスタイプを IPv4 に変更した場合などに発生する可能性があります。 報告基準: 次のいずれかが発生した場合に IPv6 トラフィックを受信しているデュアルスタック IP アドレスタイプのアクセラレーターについて報告されます。 • トラフィックを処理する IPv6 エンドポイントを持つアクセラレーターが 0 メトリクスをレポートする • エンドポイントの設定ミスがあるアクセラレーターは、フローの合計ドロップ数を報告します 統計: 使用できる統計は Sum のみです。 ディメンション • Accelerator • Accelerator, Listener • Accelerator, AcceleratorIPAddress

メトリクス	説明
HealthyEndpointCount	正常と見なされるエンドポイントの合計数。Global Accelerator は、標準アクセラレーターのエンドポイントのステータスを定期的にチェックします。これらのヘルスチェックは自動的に実行されます。これらのヘルスチェックの実行方法とタイミングは、エンドポイントのタイプとエンドポイントのヘルスチェックオプションによって異なります。詳細については、「アクセラレーターのヘルスチェックアクセスを確保する」を参照してください。 報告基準: 設定および有効化されているアクセラレーターについて報告されます。 統計値: 最も有用な統計値は Minimum および Maximum です。 ディメンション • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup

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 と 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: 使用できる統計は Sum のみです。 ディメンション • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress • Accelerator, NetworkProtocol

メトリクス	説明
ProcessedBytesIn	TCP/IP ヘッダーを含む、アクセラレーターによって処理された受信バイトの合計数。この数には、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: 使用できる統計は Sum のみです。 ディメンション • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress • Accelerator, NetworkProtocol

メトリクス	説明
ProcessedBytesOut	TCP/IP ヘッダーを含む、アクセラレーター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: 使用できる統計は Sum のみです。 ディメンション • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress • Accelerator, NetworkProtocol

メトリクス	説明
PacketsProcessed	ヘルスチェックトラフィックを含むエンドポイントとの間で送信および受信されるトラフィックを含む、アクセラレーターに対して Global Accelerator によって処理されたパケットの合計数。このメトリクスは、特定の期間内にトラフィックボリュームのきじゅんを設定するのに役立ちます。 報告基準: 設定および有効化されているアクセラレーターについて報告されます。 統計: 使用できる統計は Sum のみです。 ディメンション • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress

メトリクス	説明
UnhealthyEndpointCount	異常とみなされるエンドポイントの数。Global Accelerator は、標準アクセラレーターのエンドポイントのステータスを定期的にチェックします。これらのヘルスチェックは自動的に実行されます。これらのヘルスチェックの実行方法とタイミングは、エンドポイントのタイプとエンドポイントのヘルスチェックオプションによって異なります。詳細については、「アクセラレーターのヘルスチェックアクセスを確保する」を参照してください。 報告基準: 設定および有効化されているアクセラレーターについて報告されます。 統計値: 最も有用な統計値は Minimum および Maximum です。 ディメンション • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup

メトリクス	説明
TCP_AGA_Reset_Count	AWS Global Accelerator (「AGA」) によって生成されたリセット (RST) パケットの合計数。このメトリクスを使用すると、Global Accelerator がクライアント接続を終了し、クライアントエンドポイントにリセットを送信しているかどうかを確認できます。 Global Accelerator によって生成された TCP RST の評価とトラブルシューティングの詳細については、Global Accelerator TCP リセット問題のトラブルシューティング を参照してください。 報告基準: トラフィックがあり、値がゼロ以外の場合に報告されます。 統計: 使用できる統計は Sum のみです。 ディメンション • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, AcceleratorIPAddress

メトリクス	説明
TCP_Client_Reset_Count	クライアントからエンドポイントに送信されたリセット (RST) パケットの合計数。このメトリクスを使用すると、クライアントが Global Accelerator との接続を開いたままにできるかどうか、または接続が予期せず早期にリセットされるかどうかを判断できます。これは、最初に Global Accelerator を設定する場合や、接続のリセットを作成するクライアントに変更を加えるときに可視化するために便利です。 Global Accelerator によって生成された TCP RST の評価とトラブルシューティングの詳細については、Global Accelerator TCP リセット問題のトラブルシューティング を参照してください。 報告基準: トラフィックがあり、値がゼロ以外の場合に報告されます。 統計: 使用できる統計は Sum のみです。 ディメンション • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, AcceleratorIPAddress

メトリクス	説明
TCP_Endpoint_Reset_Count	エンドポイントからクライアントに送信されたリセット (RST) パケットの合計数。このメトリクスを使用すると、クライアントエンドポイントが過負荷になっている時期を判断するのに役立ちます。 Global Accelerator によって生成された TCP RST の評価とトラブルシューティングの詳細については、Global Accelerator TCP リセット問題のトラブルシューティング を参照してください。 報告基準: トラフィックがあり、値がゼロ以外の場合に報告されます。 統計: 使用できる統計は Sum のみです。 ディメンション • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, AcceleratorIPAddress

アクセラレーターのメトリクスディメンション

アクセラレーター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できます。

ディメンション	説明
Accelerator	アクセラレーターによってメトリクスデータをフィルタリングします。アクセラレーター ID (アクセラレータ ARN の最後の部分) でアクセラレーターを指定します。例えば、ARN は arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh とする場合、次の値を指定します: **1234abcd-abcd-1234-abcd-1234abcdefgh** 。

ディメンション	説明
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 の最終部分) によってリスナーを指定します。例えば、ARN は `arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123wxyz` とする場合、次の値を指定します: **0123wxyz**。
EndpointGroup	エンドポイントグループによってメトリクスデータをフィルタリングします。AWS リージョンによってエンドポイントグループを指定します。例えば、**us-east-1** (すべて小文字)。
SourceRegion	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領域であるソースリージョンによってメトリクスデータをフィルタリングします。ソースリージョンは次のいずれかです: • 北米 – 米国およびカナダ • EU – ヨーロッパ • AP – アジア太平洋* • 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 * 韓国とインドを除く

ディメンション	説明
DestinationEdge	クライアントトラフィックに対応する AWS エッジロケーションの地理的な地域である送信先エッジによってメトリックデータをフィルタリングします。送信先エッジは、次のいずれかです: • 北米 – 米国およびカナダ • EU – ヨーロッパ • AP – アジア太平洋* • 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 * 韓国とインドを除く
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	アクセラレーターの IP アドレス、つまりアクセラレーターに割り当てられた静的 IP アドレスの 1 つでメトリクスデータをフィルタリングします。

Global Accelerator TCP リセット問題のトラブルシューティング

各アクセラレーターは、Global Accelerator から生成および送信された TCP リセット (TCP RST) の数を報告します。Global Accelerator が TCP リセットを送信する一般的な理由は次のとおりです:

- Global Accelerator は、クライアントまたはエンドポイントが FIN ハンドシェイクまたはリセットを使用して接続を閉じると、TCP 接続を閉じたものとしてマークします。クライアントまたはエンドポイントが閉じた TCP 接続でデータパケットを送信すると、Global Accelerator は TCP リセットを生成して、接続が閉じられ、トラフィックを受け入れることができないことを示します。

- アイドルタイムアウト期間の経過後にクライアントまたはエンドポイントがデータを送信した場合、Global Accelerator からの TCP リセットパケットを受信して、接続が無効になったことを示します。
- TCP ハンドシェイク中にクライアントまたはエンドポイントとの接続を構築中に Global Accelerator が予期しないパケットを受信すると、Global Accelerator は TCP リセットを生成します。

アクセラレーターの AGA_Reset_Count メトリクスが安定している場合、クライアントまたはエンドポイントがデータを Global Accelerator に閉じた接続または期限切れの接続に送信したためです。

もし AGA_Reset_Count メトリクスに急激な増加が見られ、それがエンドポイント側の関連メトリクスの変化 (例えば、スケールアップ、スケールダウン、または非正常なエンドポイント) と一致する場合、エンドポイントが到達不能になり、Global Accelerator の TCP リセットがトリガーされた可能性があります。この問題の調査については、AWS サポートにお問い合わせください。

Global Accelerator メトリクスの統計

CloudWatch では、Global Accelerator で発行されたメトリクスのデータポイントに基づいた統計が提供されます。統計とは、指定された期間のメトリクスデータを集計したものです。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。例えば、ヨーロッパの AWS エッジロケーションからバイトが提供されるアクセラレーターに対して処理されたバイトをリクエストできます (送信先エッジは「EU」です) 。

以下は、役に立つメトリクス/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ー IP アドレスごとにサービスされるトラフィック量 (ProcessedBytesOut など) を表示して、DNS 設定が正しいことを確認します。
- ユーザートラフィックの地理的分布を表示し、ローカル (北米から北米など) またはグローバル (オーストラリアやインドから北米など) のトラフィックの量をモニタリングします。これを決定するには、ディメンション DestinationEdge と SourceRegion を特定の値に設定して、ProcessedBytesIn または ProcessedBytesOut のメトリクスを表示します。
- アクセラレーター全体の異常なエンドポイントの数を表示し、それらが属するエンドポイントグループを決定します。エンドポイントグループが多数ある場合、これは特に問題が発生しているエンドポイントを持つエンドポイントグループをすばやく見つけるのに役立ちます。これを決定するには、ディメンション Accelerator、Listener、EndpointGroup を使用して、メトリクス UnhealthyEndpointCount を表示します。

アクセラレーターの CloudWatch メトリクスを表示する

アクセラレーターに関する CloudWatch メトリクスを表示するときは、CloudWatch コンソールまたは AWS CLI を使用します。コンソールでは、メトリクスはモニタリンググラフのように表示されます。アクセラレーターがアクティブでリクエストを受信しているときにのみ、モニタリング用のグラフにデータポイントが表示されます。

米国西部 (オレゴン) リージョンの Global Accelerator に関する CloudWatch メトリクスは、両方ともコンソール上または AWS CLI の使用時に表示する必要があります。AWS CLI を使用するときは、`--region us-west-2` のパラメータを含めて、コマンドに米国西部 (オレゴン) リージョンを指定します。

CloudWatch コンソールを使用してメトリクスを表示するには、Amazon CloudWatch ユーザーガイドの手順に従って GlobalAccelerator ネームスペースを選択します。詳細について、「利用可能なメトリクスを表示する」を参照してください。

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 get-metric-statistics コマンドを使用して、指定されたメトリクスとディメンションの統計情報を取得します。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。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) 送信先エッジからサービスを提供するアクセラレーターの 1 分あたりの合計処理バイト数を一覧表示します。

```
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
```

以下は、コマンドからの出力例です。

```
{
    "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 Global Accelerator フローログインの設定と使用

フローログにより、AWS Global Accelerator のアクセラレーター内のネットワークインターフェイス間で送信される 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 にパブリッシュされ、フローログを獲得した後、そこでデータを取得して表示できます。

> **Note**
>
> 米国西部 (オレゴン) リージョンの Global Accelerator に関する CloudWatch メトリクスとログは、両方ともコンソール上または AWS CLI の使用時に表示する必要があります。AWS CLI を使用するときは、`--region us-west-2` のパラメータを含めて、コマンドに米国西部 (オレゴン) リージョンを指定します。

フローログは、以下のような数多くのタスクに役立ちます。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原因のトラブルシューティングに役立ちます。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。また、セキュリティツールとしてフローツールを使用し、エンドポイントに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 のフローの送信元、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最大 1 分間です。つまり、ログは 1 分ごとに発行される頻度は高くなりますが、少なくとも 1 分ごとに発行されます。

CloudWatch Logs の料金は、ログが Amazon S3 に直接発行されている場合でも、フローログを使用する際に適用されます。詳細については、[ログ] タブの「Amazon CloudWatch 料金表」で提供されたログを参照してください。

> **Tip**
>
> Amazon Athena と Amazon QuickSight を Global Accelerator フローログデータと共に使用すると、アプリケーションの到達可能性に関する問題のトラブルシューティング、セキュリティの脆弱性の特定、ユーザーがアプリケーションにアクセスする方法の概要を把握できます。詳細については、次の AWS ブログ記事を参照してください:「Analyzing and visualizing AWS Global Accelerator flow logs using Amazon Athena and Amazon QuickSight」。

内容

- フローログを Amazon S3 に発行できるようにする
- Amazon S3 でのフローログレコードの処理
- 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 に発行できるようにする

AWS Global Accelerator でフローログを有効にするには、この手順内のステップに従います。この章のその他のセクションでは、フローログを発行してアクセスできるように、Amazon S3 バケットを設定し、アクセス許可を設定する手順について説明します。

AWS Global Accelerator でフローログを有効にするには

1. AWS アカウントのフローログ用に Amazon S3 バケットを作成します。
2. フローログを有効にする 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 IAM ロール」を参照してください。
3. ログファイルに使用したい 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。

フローログを Amazon S3 に発行する

Amazon S3 に発行される AWS Global Accelerator のフローログは、指定される既存の S3 バケットに発行されます。フローログレコードが、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 バケットの作成方法については、「Amazon Simple Storage Service ユーザーガイド」の「最初の S3 バケットの作成」を参照してください。

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。つまり、ログファイルは 5 分ごとに書き込まれ、各ログファイルには、過去 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、ログファイルのファイル名は、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、2018 年 11 月 23 日 00:05 UTC に AWS アカウントが 123456789012 アクセラレーター (ID: 1234abcd-abcd-1234-abcd-1234abcdefgh) 用に作成したフローログのフォルダ構造とファイル名を示しています:

```
amzn-s3-demo-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、5 タプルのレコードを含むインターリーブされたエントリが含まれます。つまり:
client_ip、client_port、accelerator_ip、accelerator_port、protocol。アクセラレーターのすべてのフローログファイルを表示するには、accelerator_id と account_id によって集計されたエントリを探します。

フローログを Amazon S3 に発行する IAM ロール

フローログを Amazon S3 バケットに発行するには、IAM プリンシパル (例: IAM ロールまたはユーザー) に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 バケットとそれに含まれてい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許可を付与することができます。

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る場合、そのバケットにログを発行する許可をフローログに付与するため、サービスは次のポリシーを自動的にバケットにアタッチします。

```
{
    "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述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、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 コンソールを使用したバケットポリシーの追加」を参照してください。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 Resource ポリシーステートメントに AWSLogDeliveryWrite エレメントエントリを追加します。

例えば、次のバケットポリシーでは、AWS アカウント 123123123123 および 456456456456 に、log-bucket という名前のバケットの flow-logs という名前のフォルダに、フローログの発行を許可します。

```
{
    "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**
>
> 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に `AWSLogDeliveryAclCheck` および `AWSLogDeliveryWrite` アクセス許可を付与することをお勧めします。

SSE-KMS バケットで使用するために必要な 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 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、許可を持ちません。ログ配信アカウントには、`READ` および `WRITE` 許可があります。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

ログファイル配信のタイミング

AWS Global Accelerator は、設定されたアクセラレーターのログファイルを 1 時間に最大数回配信します。一般的に、ログファイルには、一定期間内にアクセラレーター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、ログに書き込まれたイベントの発生から 1 時間以内に Amazon S3 バケットに配信します。ある期間のログファイ

ルエントリの一部またはすべてが、最大で 24 時間遅れることもあります。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、アクセラレーターの情報を集約します。

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を書き出し始めます。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対してユーザーによる接続がなければ、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 は含まれません。vpc_id を含むバージョン 2.0 形式は、Global Accelerator がクライアント IP アドレスが保持されているエンドポイントにトラフィックを送信すると生成されます。

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	フローログバージョン。
aws_account_id	フローログの AWS アカウント ID。

フィールド	説明
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	送信元の IPv4 または IPv6 アドレス。
client_port	ソースポート。
accelerator_ip	アクセラレーターの IP アドレス。
accelerator_port	アクセラレーターのポート。
endpoint_ip	トラフィックの送信先 IP アドレスとポート。
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 または IPv6。
packets	キャプチャウィンドウ中に転送されたパケットの数。パケット数が 0 (ゼロ) の場合、フローは存続していますが、キャプチャウィンドウ中にその方向にパケットは見られませんでした。
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。この値は現在、常に ACCEPT です。

フィールド	説明
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。 • 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。
globalaccelerator_source_ip	Global Accelerator ネットワークインターフェイスで使用される IP アドレス。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、この値は - (ハイフン) に設定されます。 詳細については、「AWS Global Accelerator でクライアント IP アドレスを保存する」を参照してください。
globalaccelerator_source_port	Global Accelerator ネットワークインターフェイスで使用されるポート。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、この値は 0 (ゼロ) に設定されます。 詳細については、「AWS Global Accelerator でクライアント IP アドレスを保存する」を参照してください。
endpoint_region	エンドポイントが配置されている 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 (プレゼンスポイント)。各エッジロケーションには、3 文字コードと、割り当てられた任意の数字が存在します (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。Global Accelerator ネットワーク (INGRESS) に入るトラフィック、またはクライアント (EGRESS) に戻るトラフィックを示します。

フィールド	説明
vpc_id	VPC 識別子。Global Accelerator がクライアント IP アドレスが保持されているエンドポイントにトラフィックを送信する場合、バージョン 2.0 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適用しない場合、レコードでそのエントリには「-」記号が表示されます。

AWS CloudTrail を使用して AWS Global Accelerator API コールをログに記録する

AWS Global Accelerator は、Global Accelerator 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を記録するサービスである AWS CloudTrail と統合されています。CloudTrail は、Global Accelerator コンソールからの呼び出しや Global Accelerator API へのコード呼び出しを含むすべての 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 [イベント履歴] で最新のイベントを表示できます。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail の Global Accelerator 情報

AWS アカウントを作成すると、そのアカウントに対して CloudTrail が有効になります。アクティビティが Global Accelerator で発生すると、そのアクティビティは [イベント履歴] の他の AWS サービスのイベントとともに、CloudTrail イベントにレコードされます。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。

AWS アカウントのイベント (Global Accelerator のイベントを含む) を継続的に記録するには、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、コンソールで追跡を作成するときに、追跡がすべてのリージョンに適用されます。証跡は 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をログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、以下の各トピックを参照してください。

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- 「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 によってログに記録され、「AWS Global Accelerator API Reference」に記録されます。例えば、`CreateAccelerator`、`ListAccelerators`、および `UpdateAccelerator` オペレーションへの呼び出しによって CloudTrail ログファイルにエントリが生成されます。

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。アイデンティティ情報から以下を判断することができます。

- リクエストが、ルートと AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか
- リクエストの送信に使用された一時的なセキュリティ認証情報に、ロールとフェデレーティッドユーザーのどちらが使用されたか
- リクエストが、別の AWS のサービスによって送信されたかどうか

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

イベント履歴での Global Accelerator イベントの表示

CloudTrail では、[イベント履歴] に最近のイベントが表示されます。Global Accelerator API リクエストのイベントを表示するには、コンソールの上部にあるリージョンセレクターで [米国西部 (オレゴン)] を指定する必要があります。詳細については、「AWS CloudTrail ユーザーガイド」の「Viewing events with CloudTrail event history」(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 ログファイルエントリの概要

「トレイル」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。CloudTrail ログファイルは、パブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序では表示されません。

以下の例では、次の 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ーを一覧表示する: eventName は ListAccelerators です。
- リスナーの作成: eventName は CreateListener です。
- リスナーの更新: eventName は UpdateListener です。
- リスナーの説明: eventName は DescribeListener です。
- アカウントのリスナーを一覧表示する: eventName は ListListeners です。
- リスナーの削除: eventName は DeleteListener です。


```
{
  "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": [
            {
              "ipAddressFamily": "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 のセキュリティ

AWS でのクラウドセキュリティは最優先事項です。AWS のユーザーは、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を利用できます。

セキュリティは、AWS とユーザーの間の責任共有です。責任共有モデルでは、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 は、ユーザーが安全に使用できるサービスも提供します。AWSコンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。AWS Global Accelerator に適用されるコンプライアンス プログラムについては、「AWS Services in Scope by Compliance Program」 を参照してください。
- クラウド内のセキュリティ - ユーザーの責任は、使用する AWS サービスに応じて異なります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Global Accelerator 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、セキュリティおよびコンプライアンスの目的を達成するために Global Accelerator を設定する方法を示します。Global Accelerator リソースのモニタリングやセキュリティ確保に役立つ他の AWS のサービスの使用方法についても学習します。

内容

- AWS Global Accelerator 管理用の Identity and Access Management
- AWS Global Accelerator での安全な VPC 接続
- AWS Global Accelerator でのログ記録とモニタリング
- AWS Global Accelerator のコンプライアンス検証
- AWS Global Accelerator の耐障害性
- AWS Global Accelerator 内のインフラストラクチャセキュリティ

AWS Global Accelerator 管理用の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御するために役立つ AWS のサービスです。IAM 管理者は、誰を認証 (サインイン) し、誰に Global Accelerator リソースの使用を許可する (アクセス許可を持たせる) かをコントロールします。IAM は、追加費用なしで使用できる AWS のサービス です。

内容

- 対象者
- アイデンティティによる認証
- ポリシーを使用したアクセス権の管理
- AWS Global Accelerator が IAM と連携する方法
- AWS Global Accelerator のアイデンティティベースのポリシー
- AWS Global Accelerator 用のサービスにリンクされたロール
- AWS の AWS Global Accelerator マネージドポリシー
- AWS Global Accelerator でのタグベースのポリシーの使用
- AWS Global Accelerator アイデンティティとアクセスのトラブルシューティング

対象者

AWS Identity and Access Management (IAM) の用途は、Global Accelerator で行う作業によって異なります。

サービスユーザー – Global Accelerator サービスを使用してジョブを実行する場合は、必要な認証情報とアクセス許可を管理者が提供します。さらに多くの Global Accelerator 機能を使用して作業を実行するとき、追加のアクセス許可が必要になる場合があります。アクセスの管理方法を理解すると、管理者から適切な権限をリクエストするのに役に立ちます。Global Accelerator の機能にアクセスできない場合は、AWS Global Accelerator アイデンティティとアクセスのトラブルシューティング を参照してください。

サービス管理者 – 社内の Global Accelerator リソースを担当している場合は、通常、Global Accelerator に完全にアクセスすることができます。サービスを利用するユーザーがどの Global

Accelerator 機能やリソースにアクセスできるかを決めるのは、管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。自社で Global Accelerator で IAM を使用する方法の詳細については、AWS Global Accelerator が IAM と連携する方法 を参照ください。

IAM 管理者 – IAM 管理者は、Global Accelerator へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる Global Accelerator アイデンティティベースのポリシーの例を表示するには、AWS Global Accelerator のアイデンティティベースのポリシー を参照してください。

アイデンティティによる認証

認証とは、アイデンティティ認証情報を使用して AWSにサインインする方法です。ユーザーは、AWS アカウントのルートユーザー、IAM ユーザーとして、または IAM ロールを引き受けることによって、認証される (AWSにサインインする) 必要があります。

ID ソースから提供された認証情報を使用して、フェデレーティッドアイデンティティとして AWS にサインインできます。AWS IAM アイデンティティセンターフェデレーティッドアイデンティティの例としては、(IAM アイデンティティセンター) ユーザー、貴社のシングルサインオン認証、Google または Facebook の認証情報などがあります。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して AWSにアクセスする場合、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、AWS マネジメントコンソールまたは AWS アクセスポータルにサインインできます。AWS へのサインインの詳細については、AWS サインインユーザーガイドの「AWS アカウントにサインインする方法」を参照してください。

プログラムを使用して AWS にアクセスする場合、AWSは Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) を提供し、認証情報を使用してリクエストに暗号で署名します。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。リクエストに自分で署名する場合の推奨方法については、「IAM ユーザーガイド」の「API リクエストに対する AWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、AWS は、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用することをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM の AWS 多要素認証」を参照してください。

AWS アカウントのルートユーザー

AWS アカウントを作成する場合は、このアカウントのすべての AWS のサービスとリソースに対して完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。このアイデンティティは AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることによってアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。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の完全なリストについては、IAM ユーザーガイドのルートユーザー認証情報が必要なタスクを参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに対し、ID プロバイダーとのフェデレーションを使用して、一時的な認証情報の使用により、AWS のサービスにアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダ、Directory Service、Identity Center ディレクトリのユーザーか、または ID ソースから提供された認証情報を使用して AWS のサービス にアクセスするユーザーです。フェデレーティッド ID が AWS アカウント にアクセスすると、ロールが継承され、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、AWS IAM アイデンティティセンターを使用することをお勧めします。IAM アイデンティティセンター でユーザーとグループを作成するか、すべての AWS アカウント とアプリケーションで使用するために、独自の ID ソースで一連のユーザーとグループに接続して同期することもできます。IAM Identity Center の詳細については、「AWS IAM アイデンティティセンターユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたは 1 つのアプリケーションに対して特定の許可を持つ AWS アカウント 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイドの長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションするを参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdminsという名前のグループを設定して、そのグループにIAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーション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。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定の許可を持つ、AWS アカウント内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。AWS マネジメントコンソールで IAM ロールを一時的に引き受けるには、ユーザーから IAM ロールに切り替える (コンソール) ことができます。ロールを引き受けるには、AWS CLIまたは AWS API オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM アイデンティティセンターユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- 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、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。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。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、

「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

- クロスサービスアクセス権 - 一部の AWS のサービスでは、他の AWS のサービスの機能を使用します。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、AWS のサービスを呼び出すプリンシパルの権限を、AWS のサービスのリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエストを行います。FAS リクエストは、サービスが、完了するために他の AWS のサービス またはリソースとのやりとりを必要とするリクエストを受け取ったときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。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、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - 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、AWS のサービスにリンクされたサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション - EC2 インスタンスで実行され、AWS CLIまたは AWS API 要求を行っ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 ロールを使用できます。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、インスタンスに添付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的な認証情報を取得できます。詳細については、IAM ユーザーガイドのAmazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与するを参照してください。

ポリシーを使用したアクセス権の管理

AWS でアクセスを制御するには、ポリシーを作成して AWS ID またはリソースにアタッチします。ポリシーは AWS のオブジェクトであり、アイデ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、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシーを評価します。ポリシーでの権限により、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。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、IAM ユーザーガイドのJSON ポリシー概要を参照してください。

管理者は AWSJSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole`アクションを許可するポリシーがあるとします。このポリシーがあるユーザーは、AWS マネジメントコンソール、AWS CLI、または AWS API からロール情報を取得できます。

アイデンティティベースポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれます。マネージドポリシーは、AWS アカウント内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロンポリシーです。マネージドポリシーには、AWS マネージドポリシーとカスタマー管理ポリシーがあります。管理ポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

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、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーションユーザー、または AWS のサービス を含めることができます。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは IAM の AWSマネージドポリシーは使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、AWS WAF、および Amazon VPC は、ACL をサポートするサービスの例です。ACL の詳細については、Amazon Simple Storage Service デベロッパーガイドのアクセスコントロールリスト (ACL) の概要を参照してください。

その他のポリシータイプ

AWS では、他の一般的ではないポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、IAM ユーザーガイドのIAM エンティティのアクセス許可の境界を参照してください。
- サービスコントロールポリシー (SCP) - SCP は、AWS Organizationsで組織や組織単位 (OU) の最大許可を指定する JSON ポリシーです。AWS Organizationsは、顧客のビジネスが所有する複数の

AWS アカウント をグループ化し、一元的に管理するサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP はメンバーアカウントのエンティティに対する権限を制限します (各 AWS アカウントのルートユーザー など)。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、IAM ユーザーガイドのセッションポリシーを参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関連するとき、リクエストを許可するかどうかを AWS が決定する方法の詳細については、IAM ユーザーガイドのポリシーの評価ロジックを参照してください。

AWS Global Accelerator が IAM と連携する方法

IAM を使用して Global Accelerator へのアクセスを管理する前に、Global Accelerator で利用できる IAM の機能について学びます。

AWS のサービスが大部分の IAM 機能と連動する方法に関する同様の概要のビューを表示するテーブルを確認するには、「IAM ユーザーガイド」の「IAM と連携する AWS のサービス」を参照してください。

AWS Global Accelerator で使用できる IAM の機能

IAM の機能	Global Accelerator へのサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり

IAM の機能	Global Accelerator へのサポート
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	はい
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	あり
プリンシパル権限	あり
サービスロール	いいえ
サービスリンクロール	可能

Global Accelerator のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。ID ベースのポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、IAM ユーザーガイドのIAM JSON ポリシーの要素のリファレンスを参照してください。

Global Accelerator アイデンティティベースのポリシーの例は、AWS Global Accelerator のアイデンティティベースのポリシー を参照してください。

Global Accelerator でのリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。

Global Accelerator のポリシーアクション

ポリシーアクションのサポート: あり

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーの`Action`要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

Global Accelerator アクションのリストを確認するには、「サービス認証リファレンス」の「Actions defined by AWS Global Accelerator」を参照してください。

Global Accelerator のポリシーアクションは、アクションの前に以下のプレフィックスを使用します:

```
aws-globalaccelerator
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "aws-globalaccelerator:action1",
      "aws-globalaccelerator:action2"
         ]
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、`Describe` という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

```
"Action": "aws-globalaccelerator:Describe*"
```

Global Accelerator アイデンティティベースのポリシーの例は、AWS Global Accelerator のアイデンティティベースのポリシー を参照してください。

Global Accelerator のポリシーリソース

ポリシーリソースのサポート: あり

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

「サービス認証リファレンス」では、Internet Monitor に関連する次の情報を確認できます。

- Global Accelerator リソースタイプとその ARN のリストについて、「AWS Global Accelerator で定義されるリソース」を参照してください。
- どのアクションで各リソースの ARN を指定できるかについては、「AWS Global Accelerator で定義されるアクション」を参照してください。

Global Accelerator アイデンティティベースのポリシーの例は、AWS Global Accelerator のアイデンティティベースのポリシー を参照してください。

Global Accelerator のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、AWSでは AND 論理演算子を使用してそれらを評価します。単一の条件キーに複数の値を指定する場合、AWS では OR 論理演算子を使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、IAM ユーザーガイドのIAM ポリシーの要素: 変数およびタグを参照してください。

AWS はグローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイド の「AWS グローバル条件コンテキストキー」を参照してください。

アカウント管理条件キーのリストを確認するには、「サービス認可リファレンス」の「AWS Global Accelerator の条件キー」を参照してください。どのアクションおよびリソースと条件キー組み合わせてを使用できるかについては、「AWS Global Accelerator で定義されるアクション」を参照してください。

Global Accelerator アイデンティティベースのポリシーの例は、AWS Global Accelerator のアイデンティティベースのポリシー を参照してください。

Global Accelerator における ACL

ACL のサポート: あり

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Global Accelerator を使用した ABAC

ABAC (ポリシー内のタグ) のサポート: 一部

Global Accelerator は、ポリシーのタグを部分的にサポートしています。リソースの 1 つであるアクセラレーターのタグ付けをサポートしています。ポリシーステートメント条件でのタグの使用、お

よびリソースのタグに基づいてリソースへのアクセスを制限するためのポリシーの例を表示するには、AWS Global Accelerator でのタグベースのポリシーの使用 を参照してください。

Global Accelerator の詳細については、AWS Global Accelerator でのタグ付け を参照してください。

ポリシーにおけるタグの使用の詳細については、次の情報を確認してください。

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。AWS では、属性は タグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール)、および多数の AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可で属性に基づいてアクセス許可を定義する」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、IAM ユーザーガイドの属性に基づくアクセスコントロール (ABAC) を使用するを参照してください。

Global Accelerator での一時的認証情報の使用

一時的な認証情報のサポート: あり

AWS のサービス には、一時的な認証情報を使用してサインインしても機能しないものがあります。一時的な認証情報を利用できる AWS のサービス を含めた詳細情報については、「IAM ユーザーガイド」の「IAM と連携する」AWS のサービスを参照してください。

ユーザー名とパスワード以外の方法で AWS マネジメントコンソール にサインインする場合は、一時的な認証情報を使用していることになります。例えば、会社のシングルサインオン (SSO) リンクを使用して AWS にアクセスすると、そのプロセスは自動的に一時認証情報を作成します。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が

自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時認証情報は、AWS CLIまたは AWS API を使用して手動で作成できます。作成後、一時認証情報を使用して AWS にアクセスできるようになります。AWSは、長期的なアクセスキーを使用する代わりに、一時認証情報を動的に生成することをお勧めします。詳細については、IAM の一時的セキュリティ認証情報を参照してください。

Global Accelerator のクロスサービスプリンシパル許可

転送アクセスセッション (FAS) のサポート: あり

IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルとみなされます。一部のサービスを使用する際に、アクションを実行してから、別のサービスの別のアクションを開始することがあります。FAS は、AWS のサービスを呼び出すプリンシパルの権限を、AWS のサービスのリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエストを行います。FAS リクエストは、サービスが、完了するために他の AWS のサービス またはリソースとのやりとりを必要とするリクエストを受け取ったときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Global Accelerator のサービスロール

サービスロールのサポート: なし

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。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、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

Global Accelerator のサービスリンクロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、AWS のサービスにリンクされているサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント 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。

Global Accelerator のサービスリンクロールの詳細については、AWS Global Accelerator 用のサービスにリンクされたロール を参照してください。

AWS のサービスリンクロール全般の作成または管理の詳細については、「IAM と提携する AWS のサービス」を参照してください。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、はい リンクを選択します。

AWS Global Accelerator のアイデンティティベースのポリシー

デフォルトでは、ユーザーおよびロールには Global Accelerator リソースを作成または変更するアクセス許可がありません。また、AWS マネジメントコンソール、AWS Command Line Interface (AWS CLI)、または AWS API を使用してタスクを実行することもできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して IAM ID ベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

Global Accelerator が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「サービス認可リファレンス」の「AWS Global Accelerator のアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーのベストプラクティス
- Global Accelerator アクセラレーターの作成
- Global Accelerator コンソールの使用
- Global Accelerator API アクションの使用
- 自分の権限の表示をユーザーに許可する

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰が Global Accelerator リソースを作成し、これにアクセスし、これを削除できるかを決定します。これらのアクションを実行すると、AWS アカウント に料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS マネージドポリシーを使用して開始し、最小特権の許可に移行する – ユーザーとワークロードへの許可の付与を開始するには、多くの一般的なユースケースのために許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケースに応じた AWS カスタマー管理ポリシーを定義することで、許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWSマネージドポリシー」または「ジョブ機能の AWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイドのIAM でのポリシーとアクセス許可を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。また、CloudFormation などの特定の AWS のサービス を介して使用する場合、条件を使用してサービスアクションへのアクセスを許可することもできます。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素:条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。
- 多要素認証 (MFA) を要求する – AWS アカウント で IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイドのIAM でのセキュリティのベストプラクティスを参照してください。

Global Accelerator アクセラレーターの作成

AWS Global Accelerator アクセラレーターを作成するには、ユーザーに Global Accelerator に関連付けられているサービスリンクロールを作成するアクセス許可が必要です。

ユーザーに Global Accelerator でアクセラレーターを作成するための正しいアクセス許可を付与するには、次のようなポリシーをユーザーにアタッチします。

> **Note**
>
> 次のポリシーよりも制限の厳しい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、制限の厳しいポリシーを持つユーザーはアクセラレーターを作成できなくなります。

```
{
      "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*"
    }
```

Global Accelerator コンソールの使用

AWS Global Accelerator コンソールにアクセスするには、最小限の許可が必要です。これらのアクセス許可により、AWS アカウント の Global Accelerator リソースの一覧と詳細を表示する必要があります。最小限必要なアクセス許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) ではコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソール権限を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスを許可します。

ユーザーとロールが引き続き Global Accelerator コンソールを使用できるようにするには、エンティティに `GlobalAcceleratorReadOnlyAccess` または `GlobalAcceleratorFullAccess` AWS 管理ポリシーもアタッチします。

ユーザーがコンソールで情報を表示するか、`List*` または `Describe*` オペレーションを使用する API を AWS Command Line Interface に呼び出すだけでよい場合は、最初のポリシー `GlobalAcceleratorReadOnlyAccess` をアタッチします。

アクセラレーターの作成や更新が必要なユーザーには、2 つ目のポリシーである `GlobalAcceleratorFullAccess` をアタッチします。フルアクセスポリシーには、Global Accelerator のフルアクセス許可と、Amazon EC2 および Elastic Load Balancing のアクセス許可の説明が含まれています。

> **Note**
>
> Amazon EC2 および Elastic Load Balancing に必要なアクセス許可を含まない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なくなります。

詳細については、「IAM ユーザーガイド」の Global Accelerator「AWS マネージドポリシーのページ」または「ユーザーへのアクセス許可の追加」を参照してください。

Global Accelerator API アクションの使用

AWS Global Accelerator 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、Global Accelerator 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。

例えば、次のポリシーは、ユーザーが `CreateAccelerator` アクションを実行して、AWS アカウントのアクセラレーターをプログラム的に作成できるようにします。

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

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

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI か AWS API を使用してプログラム的に、このアクションを完了する権限が含まれています。

```
{
    "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": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

AWS Global Accelerator 用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)「サービスリンクロール」を使用します。サービスリンクロールは、Global Accelerator に直接リンクされた一意のタイプの IAM ロールです。サービスリンクロールは Global Accelerator によって事前に定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なアクセス許可がすべて含まれています。

サービスリンクロールを使用することで、必要なアクセス権限を手動で追加する必要がなくなるため、Global Accelerator の設定が簡単になります。Global Accelerator は、サービスリンクロールのアクセス許可を定義します。特に定義されている場合を除き、Global Accelerator のみがその ロールを引き受けることができます。定義されるアクセス許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールを削除するには、まずその関連リソースを削除します。これにより、リソースにアクセスするための許可を意図せず削除することが防止され、Global Accelerator 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する他のサービスについては、「IAM と連動する AWS サービス」を参照し、[Service-linked roles] (サービスにリンクされたロール) の列内で [Yes] (はい) と表記されたサービスを確認してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、はいリンクを選択します。

Global Accelerator サービスリンクロールのアクセス許可

AWS Global Accelerator は、AWSServiceRoleForGlobalAccelerator という名前のサービスリンクロールを使用します。このロールにより、Global Accelerator はアカウント内のロードバランサーやその他のエンドポイントなどのリソースにアクセスして、Global Accelerator と連携するように設定されたリソースのみを追加できるようになります。AWSServiceRoleForGlobalAccelerator ロールを使用すると、Global Accelerator はクライアント 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もできます。

Global Accelerator は、Global Accelerator 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になると、AWSServiceRoleForGlobalAccelerator という名前のロールを自動的に作成します。Global Accelerator でアクセラレーターを使用するには、このロールが必要です。AWSServiceRoleForLambdaReplicator 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のアクセス許可

Global Accelerator は、AWSServiceRoleForGlobalAccelerator という名前のサービスリンクロールを使用して、リソースと設定にアクセスして準備状況を確認します。このサービスリンクロールは、マネージドポリシーである `AWSGlobalAcceleratorSLRPolicy` を使用します。

AWSServiceRoleForGlobalAccelerator サービスリンクロールは、次のサービスを信頼してロールを引き受けます:

- `globalaccelerator.amazonaws.com`

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AWSGlobalAcceleratorSLRPolicy」を参照してください。

IAM エンティティ (ユーザー、グループ、ロールなど) で Global Accelerator のサービスリンクロールを削除できるように、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、「IAM ユーザーガイド」の「サービスリンクロールの許可」を参照してください。

Global Accelerator のサービスリンクロールの作成

Global Accelerator のサービスリンクロールを手動で作成する必要はありません。サービスは、アクセラレーターを初めて作成するときに自動的にロールを作成します。Global Accelerator リソースを削除し、サービスリンクロールを削除する場合、新しいアクセラレータを作成する時、サービスによってロールが再度自動的に作成されます。

Global Accelerator のサービスリンクロールの編集

Global Accelerator では、サービスリンクロール AWSServiceRoleForGlobalAccelerator を編集できません。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、IAM ユーザーガイドの「サービスにリンクされたロールの編集」を参照してください。

Global Accelerator のサービスリンクロールの削除

Global Accelerator が不要になった場合は、サービスリンク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 Global Accelerator リソースをクリーンアップする必要があります。

アクセラレーターを無効にして削除した後、サービスリンクロールを削除できます。アクセラレーターの削除の詳細については、アクセラレーターを作成する を参照してください。

> **Note**
>
> アクセラレーターを無効にして削除しても Global Accelerator の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が失敗する可能性があります。その場合は、数分待ってからサービスリンクロールの削除手順をもう一度試してください。

AWSServiceRoleForGlobalAccelerator サービスリンク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 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] (はい、削除する) 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モニタリングします。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、 IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

Global Accelerator サービスリンクロールのポリシーの更新

`AWSGlobalAcceleratorSLRPolicy` の更新について、Global Accelerator サービスリンクロールの AWS マネージドポリシーの更新については、「AWS マネージドポリシーの更新表」を参照してください。AWS Global Accelerator ドキュメント履歴 ページで、自動 RSS アラートにサブスクライブすることもできます。

AWS の AWS Global Accelerator マネージドポリシー

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースで権限を提供できるように設計されているため、ユーザー、グループ、ロールへの権限の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることにご注意ください。AWSのすべてのお客様が使用できるようになるのを避けるためです。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS マネージドポリシーで定義したアクセス権限は変更できません。AWS が AWS マネージドポリシーに定義されている権限を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービス を起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS 管理ポリシー」を参照してください。

AWS マネージドポリシー: AWSServiceRoleForGlobalAccelerator

IAM エンティティに `AWSServiceRoleForGlobalAccelerator` をアタッチすることはできません。このポリシーはサービスリンクロールにアタッチします。AWS Global Accelerator による AWS の (Global Accelerator が使用または管理する) サービスおよびリソースへのアクセスを許可します。詳細については、「AWS Global Accelerator 用のサービスにリンクされたロール」を参照してください。

AWS マネージドポリシー: GlobalAcceleratorReadOnlyAccess

IAM エンティティに `GlobalAcceleratorReadOnlyAccess` をアタッチできます。このポリシーは、Global Accelerator でアクセラレーターを操作するためのアクションへの読み取り専用アクセスを許可します。これは、コンソールで情報を表示したり、`List*` または `Describe*` オペレーションを使用して AWS Command Line Interface または API を呼び出すだけで済むユーザーに役立ちます。

このポリシーのアクセス許可を表示するには、「AWS マネージドポリシーリファレンス」の「GlobalAcceleratorReadOnlyAccess」を参照してください。

AWS マネージドポリシー: GlobalAcceleratorFullAccess

IAM エンティティに `GlobalAcceleratorFullAccess` をアタッチできます。このポリシーは、Global Accelerator でアクセラレーターを操作するためのアクションへのフルアクセスを許可します。これを、Global Accelerator アクションへの完全なアクセス権を必要とする IAM ユーザーとその他プリンシパルにアタッチします。

> **Note**
>
> Amazon EC2 および Elastic Load Balancing に必要なアクセス許可を含まない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なくなります。

このポリシーのアクセス許可を表示するには、「AWS マネージドポリシーリファレンス」の「GlobalAcceleratorFullAccess」を参照してください。

AWS マネージドポリシーに対する Global Accelerator の更新

Global Accelerator の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページの変更を自動通知するには、Global Accelerator の「ドキュメントの履歴」ページで RSS フィードをサブスクライブします。

変更	説明	日付
AWSGlobalAcceleratorSLRPolicy – ポリシーの更新	Global Accelerator は、ロードバランサーのターゲットグループを記述する新しいアクセス許可を追加しました。 Global Accelerator は `elasticloadbalancing:DescribeTargetGroups` を使用して、ターゲットタイプ `ip` のロードバランサーを識別します。このターゲットタイプは、Global Accelerator のデュアルスタッ	2023 年 10 月 20 日

変更	説明	日付
	クロードバランサーエンドポイントでサポートされていません。	
AWSGlobalAcceleratorSLRPolicy – ポリシーの更新	Global Accelerator は、ロードバランサーのリスナーを記述し、EC2 インスタンスのアドレスを記述する新しいアクセス許可を追加しました。 Global Accelerator は `elasticloadbalancing:DescribeListeners` を使用して、リスナー設定に基づいてロードバランサーのリスナー管理の決定をサポートします。 Global Accelerator は、`ec2:DescribeAddresses` を使用して Elastic IP アドレスエンドポイントをアクセラレーターに追加します。	2023 年 5 月 23 日

変更	説明	日付
AWSGlobalAcceleratorSLRPolicy – ポリシーの更新	Global Accelerator は、IPv6 アドレスをサポートする新しいアクセス許可を追加しました。 Global Accelerator は `ec2:AssignIpv6Addresses` を使用して、IPv6 トラフィックを送受信するための IPv6 アドレスを使用してカスタマーサブネット上の Global Accelerator ENI IPv6 を更新し、不要になったときに `UnassignIpv6Addresses` を使用して IPv6 アドレスを削除します。	2021 年 11 月 15 日
AWSGlobalAcceleratorSLRPolicy – ポリシーの更新	Global Accelerator は、Global Accelerator がエラーを診断するのに役立つ新しいアクセス許可を追加しました。 Global Accelerator は `ec2:DescribeRegions` を使用して、顧客がいる AWS リージョンを決定します。これにより、Global Accelerator は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
Global Accelerator が変更の追跡を開始する	Global Accelerator が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 5 月 18 日

AWS Global Accelerator でのタグベースのポリシーの使用

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。ただし、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。リソース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。特定のタグを使用する任意のリソースへのアクセスを一括して付与できます。このタグは、リソースを作成するとき、または後でリソースを更新することで、関連するリソースに繰り返し適用できます。

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ひとつの方法です。タグは、リソースにアタッチするか、タグ付けをサポートするサービスへのリクエストに渡すことができます。Global Accelerator では、アクセラレーターのみがタグを含めることができます。Global Accelerator のタグ付けの詳細については、AWS Global Accelerator でのタグ付け を参照してください。

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コントロールできます。

- 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ー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。

たとえば、AWS `GlobalAcceleratorFullAccess` マネージドポリシーは、任意のリソースに対して Global Accelerator アクションを実行するための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実稼働環境アクセラレーターで Global Accelerator アクションを実行するアクセス許可を拒否します。お客様の管理者は、権限のない IAM ユーザーには、マネージドユーザーポリシーに加えて、この IAM ポリシーを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"
                }
            }
        }
    ]
}
```

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 ユーザーガイド」の「IAM タグを使用したアクセスコントロール」を参照してください。

AWS Global Accelerator アイデンティティとアクセスのトラブルシューティング

次の情報は、Global Accelerator と IAM の使用に伴い発生する可能性のある、一般的な問題の診断や修復に役立ちます。

トピック

- Global Accelerator でのアクションの実行を認可されていない
- iam:PassRole を実行する権限がありません
- 自分の AWS アカウント 以外のユーザーに Global Accelerator リソースへのアクセスを許可したい

Global Accelerator でのアクションの実行を認可されていない

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なaws-globalaccelerator:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: aws-
globalaccelerator:GetWidget on resource: my-example-widget
```

この場合、aws-globalaccelerator:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Global Accelerator にロールを渡せるようにする必要があります。

一部の AWS のサービスでは、新しいサービスロールやサービスリンクロールを作成せずに、既存のロールをサービスに渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して Global Accelerator でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

自分の AWS アカウント 以外のユーザーに Global Accelerator リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください。

- Global Accelerator でこれらの機能がサポートされるかどうかを確認するには、AWS Global Accelerator が IAM と連携する方法 を参照してください。
- 所有している AWS アカウント 全体のリソースへのアクセス権を提供する方法については、IAM ユーザーガイドの所有している別の AWS アカウント アカウントへのアクセス権を IAM ユーザーに提供を参照してください。
- サードパーティーの AWS アカウント にリソースへのアクセス権を提供する方法については、「IAM ユーザーガイド」の「サードパーティが所有する AWS アカウント へのアクセス権を付与する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

AWS Global Accelerator での安全な VPC 接続

AWS Global Accelerator に Network Load Balancer、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と、プライベートサブネットでターゲットにして、仮想プライベートクラウド (VPC) のエンドポイントとの間でインターネットトラフィックを直接送信できるようになります。ロードバランサーまたは EC2 インスタンスを含む VPC には、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す「インターネットゲートウェイ」がアタッチされている必要があります。ただし、ロードバランサーまたは EC2 インスタンスに公開 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は必要ありません。

これは一般的なインターネットゲートウェイのユースケースとは異なり、VPC 内のインスタンスまたはロードバランサーにインターネットトラフィックを送信しるためには、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です。ターゲットの伸縮性のある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 (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、インターネットトラフィックに Global Accelerator を使用すると、Global Accelerator は一般的なインターネットルートをオーバーライドし、Global Accelerator 経由で到着するすべての論理接続もインターネットゲートウェイではなく Global Accelerator 経由で返されます。

> **Note**
>
> Amazon EC2 インスタンスにパブリック IP アドレスとパブリックサブネットを使用すること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。
> ENI、セキュリティグループや Global Acceleratorの動作の詳細について、「クライアント IP アドレスが保存されているエンドポイントの要件」を参照してください。

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、この情報に注意してください。VPC へのインターネットアクセスの制御の詳細については、この「サービスコントロールポリシーの例」を参照してください。

AWS Global Accelerator でのログ記録とモニタリング

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のモニタリングデータを収集する必要があります。AWS は、Global Accelerator リソースとアクティビティをモニタリングし、潜在的なインシデントに対応するための複数のツールを提供します。

Global Accelerator は、ログ記録と追跡のための次の 3 つの主要な方法を提供します:

Amazon CloudWatch メトリクスおよびアラーム

CloudWatch を使用することで、AWS リソースと、AWS で実行している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。アクセラレーターがデプロイされるとすぐに、CloudWatch は Global Accelerator のメトリクスの収集と追跡を開始します。メトリクスとは、トラフィックが流れていることを確認するために表示したり、時間の経過とともに測定できる変数のことです。

例えば、メトリクスを使用して、トラフィックが Global Accelerator を介してエンドポイントに流れていることを検証し、クライアントにバックアウトし、問題のトラブルシューティングに役立てることができます。また、メトリクスを監視し、それが、一定期間しきい値を超過したときに通知を送信する、またはモニタリングしているリソースを自動的に変更するアラームを作成できます。

詳細については、「Amazon CloudWatch と AWS Global Accelerator の併用」を参照してください。

Global Accelerator フローのログ

サーバーフローログは、Global Accelerator で設定したログで、アクセラレーターを介してエンドポイントに通過す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、セキュリティ監査やアクセス監査など、多くのアプリケーションに役立ちます。詳細については、「AWS Global Accelerator フローログインの設定と使用」を参照してください。

AWS CloudTrail ログ

CloudTrail は、Global Accelerator 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、Global Accelerator コンソールからの呼び出しや Global Accelerator API へのコード呼び出しを含むすべての 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 を使用して AWS Global Accelerator API コールをログに記録する」を参照してください。

AWS Global Accelerator のコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの対象であるかどうかを確認するには、コンプライアンスプログラムによる対象範囲内の AWS のサービス のサービスをご覧いただき、関心のあるコンプライアンスプログラムを選択してください。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。

AWS Artifact を使用して、サードパーティーの監査レポートをダウンロードできます。詳細については、「AWS Artifact でレポートをダウンロードする」「」を参照してください。

AWS のサービス を使用する際のユーザーのコンプライアンス責任は、ユーザーのデータの機密性や貴社のコンプライアンス目的、適用される法律および規制によって決まります。AWS では、コンプライアンスに役立つ次のリソースを提供しています。

- セキュリティと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 にデプロイするためのステップを示します。
- Amazon Web Services での HIPAA のセキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法を説明しています。

> **Note**
>
> すべての AWS のサービスが HIPAA 適格であるわけではありません。詳細については、HIPAA 対応サービスのリファレンスを参照してください。

- 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、顧客の業界と拠点に適用されるものである場合があります。
- AWS Customer Compliance Guide — コンプライアンスの観点から見た責任共有モデルを理解できます。このガイドは、AWS のサービスを保護するためのベストプラクティスを要約したものであり、複数のフレームワーク (米国標準技術研究所 (NIST)、ペイメントカード業界セキュリティ標準評議会 (PCI)、国際標準化機構 (ISO) など) にわたるセキュリティ統制へのガイダンスがまとめられています。
- 「AWS Config デベロッパーガイド」の「ルールでのリソースの評価」 - AWS Config サービスは、自社のプラクティス、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 Security Hub CSPM – この AWS のサービス は、AWS 内のセキュリティ状態の包括的なビューを提供します。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – この AWS のサービスは、環境をモニタリングして、疑わしいアクティビティや悪意のあるアクティビティがないか調べることで、AWS アカウント、ワークロード、コンテナ、データに対する潜在的な脅威を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager - この AWS のサービスは、AWS の使用状況を継続的に監査して、リスクの管理方法や、規制および業界標準へのコンプライアンスの管理方法を簡素化するために役立ちます。

AWS Global Accelerator の耐障害性

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ています。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し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せずに、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、およびスケーラビリティが優れています。

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、データの耐障害性をサポートする以下の機能も用意されています。

- AWS の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持つ分離されたユニットです。アクセラレーターを作成すると、Global Accelerator は一連の IPv4 静的 IP アドレスを提供します。1 つのアクセラレーターに IPv4 IP アドレスタイプが 2 つ、またはデュアルスタックアクセラレーターに静的 IP アドレスが 4 つ (2 つの IPv4 アドレスと 2 つの IPv6 アドレス) です。Global Accelerator は、各 IP アドレスファミリーの一意の IP サブネットから、ネットワークゾーンごとに 1 つの静的 IP アドレスを提供します。特定のクライアントネットワークによる IP アドレスの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他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。
- Global Accelerator は、すべてのエンドポイントの状態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異常であると判断された場合、Global Accelerator はすぐにトラフィックを別の利用可能なエンドポイントに誘導し始めます。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 Accelerator 内のインフラストラクチャセキュリティ

マネージドサービスである AWS Global Accelerator は AWS グローバルネットワークセキュリティで保護されています。AWSセキュリティサービスと AWS がインフラストラクチャを保護する方法については、「AWSクラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、セキュリティの柱 - AWS Well-Architected Frameworkのインフラストラクチャ保護を参照してください。

AWS 公開 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。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2 は必須で TLS 1.3 がお勧めです。

- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストには、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 ServiceAWS 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 に関連する制限とも呼ばれる特定のクォータがあります。

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、調整可能なクォータの引き上げをリクエストできます。

Service Quotas コンソールで Global Accelerator のサービス制限を管理し、クォータの引き上げをリクエストするには、米国東部 (バージニア北部) (us-east-1) リージョンにいる必要があります。Global Accelerator のサービスクォータは、AWS グローバルサービスクォータが定義されている米国東部 (バージニア北部) リージョンで管理されます。他の AWS リージョン では、Global Accelerator のクォータは表示されず、クォータを変更することはできません。ただし、すべての Global Accelerator API オペレーションは、米国西部 (オレゴン) (us-west-2) リージョンで実行する必要があります。

トピック

- 一般的なクォータ
- 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
- 関連クォータ

一般的なクォータ

Global Accelerator の全体的なクォータは次のとおりです。

エンティティ	クォータ
AWS アカウントあたりの標準アクセラレーター	20 クォータの引き上げをリクエストできます。
AWS アカウントごとのカスタムルーティングアクセラレーター	10 クォータの引き上げをリクエストできます。
アクセラレーターあたりのリスナー	10

エンティティ	クォータ
	クォータの引き上げをリクエストできます。
すべてのリスナーにわたるアクセラレーターあたりのエンドポイントグループ	42
Global Accelerator がすべてのリスナーとエンドポイントグループで指すことができる AWS リージョン	42 アクセラレーターにリスナーが 1 つある場合は、アクセラレーターのエンドポイントグループ設定を使用して、Global Accelerator がサポートするすべてのリージョンを指すことができます。 エンドポイントグループを使用してアクセラレーターで参照できるリージョンの最大数は、リスナーの数が増えるにつれて比例的に減少することに注意してください。(リスナーの合計数) x (エンドポイントグループの数) は 42 を超えることはできません。
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あたりのポートのオーバーライド	10 クォータの引き上げをリクエストできます。
クロスアカウントアタッチメントあたりのプリンシパル	10 クォータの引き上げをリクエストできます。
クロスアカウントアタッチメントあたりのリソース	500

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

以下は、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 Global Accelerator クォータです。

エンティティ	説明	クォータ
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
Application Load Balancer のみを使用するエンドポイントグループ	Application Load Balancer 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
Network Load Balancer のみを使用するエンドポイントグループ	Network Load Balancer 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 クォータの引き上げをリクエストできます。
Amazon EC2 インスタンスのみを使用するエンドポイントグループ	EC2 インスタンス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 クォータの引き上げをリクエストできます。
Elastic IP アドレスのみを使用するエンドポイントグループ	Elastic IP アドレスエンドポイントのみを含むエンドポイントグループの Elastic IP アドレスの数。	10 クォータの引き上げをリクエストできます。
Amazon Virtual Private Cloud サブネットのみを使用するエンドポイントグループ	VPC 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 クォータの引き上げをリクエストできます。

関連クォータ

Global Accelerator のクォータに加えて、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、次を参照してください:

- 「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスクォータ」。
- 「Amazon EC2 ユーザーガイド」の「Amazon EC2 サービスクォータ」

- 詳細については、「Network Load Balancers ユーザーガイド」の「Network Load Balancer のクォータ」を参照してください。
- 「Application Load Balancer ユーザーガイド」の「Application Load Balancer のクオータ」。
- 「Amazon VPC ユーザーガイド」の「Amazon VPC ユーザーガイド」。

AWS Global Accelerator 関連情報

ここに列挙されている情報とリソースは Global Accelerator に対する理解を深めるのに役立ちます。

トピック

- AWS Global Accelerator の API Reference と製品情報
- サポート情報
- AWS ブログウェブサイトからのヒント

AWS Global Accelerator の API Reference と製品情報

このサービスを利用する際に役立つ関連リソースは次のとおりです。

- AWS Global Accelerator API Reference – API のアクション、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あります。
- Global Accelerator の最新情報 – Global Accelerator の新機能や最近追加されたエッジロケーションに関するお知らせ。
- AWS Global Accelerator 製品情報 – に関する情報の基本となるウェブページ。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、その他のトピックに関する詳細情報です。

サポート情報

Global Accelerator のサポートは、いくつかの形式で利用可能です。

- ディスカッションフォーラム – 開発者のためのコミュニティベースのフォーラムです。Global Accelerator に関連する技術的な質問についてディスカッションできます。
- 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 とヘルスチェックの結果に関する情報がまとめられていて、ディスカッションフォーラム、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 Discussion Forums またはサポート用のリンクをご利用ください。

AWS ブログウェブサイトからのヒント

AWS ブログウェブサイトには、Global Accelerator に関する以下のブログ記事など、AWS サービスの使用に役立つ投稿が多数あります。

- AWS Global Accelerator を使用してアプリケーションのパフォーマンスを向上させる
- AWS Global Accelerator を使用したデプロイのベストプラクティス
- AWS Global Accelerator のクロスアカウントサポートの発表
- AWS Global Accelerator が提供した静的 IP アドレスを介した Amazon API Gateway へのアクセス
- AWS Global Accelerator Amazon Elastic Kubernetes Service を使用したカスタムルーティング
- AWS で AWS Global Accelerator を使用したマルチリージョンアプリケーションのデプロイ
- AWS Global Accelerator でアプリケーションの耐障害性を最大化する
- AWS Global Accelerator で Small を開始する
- AWS Global Accelerator で行うトラフィック管理
- Amazon Athena および Amazon QuickSight を使用した AWS Global Accelerator フローログの分析と可視化

AWS Global Accelerator ブログの完全なリストについては、AWS ブログ投稿の Networking & Content Delivery カテゴリの「AWS Global Accelerator」を参照してください。

ドキュメント履歴

以下の表は、AWS Global Accelerator の重要な変更点をまとめたものです。

- API バージョン: 最新
- ドキュメント最新更新日: 2024 年 3 月 27 日

変更	説明	日付
BYOIP のクロスアカウントのサポートを追加する	Global Accelerator は、アクセラレータエンドポイントの問題をより簡単に検出するために使用できる 5 つの追加の CloudWatch メトリクスをサポートするようになりました。詳細については、「AWS Global Accelerator で Amazon CloudWatch アラームを使用する」を参照してください。	2024 年 3 月 27 日
BYOIP のクロスアカウントのサポートを追加する	Global Accelerator では、AWS アカウント間で Bring-Your-Own-IP (BYOIP) アドレスの持ち込みがサポートされるようになりました。詳細については、「AWS Global Accelerator のクロスアカウントアタッチメントとリソースの使用」を参照してください。	2024 年 3 月 25 日
Network Load Balancer のデュアルスタックのサポートを追加	Global Accelerator は、標準アクセラレーターへのデュアルスタック Network Load Balancer の追加をサポートするようになりました。詳細	2023 年 11 月 2 日

変更	説明	日付
	については、「AWS Global Accelerator のアクセラレーターのエンドポイント要件」を参照してください。	
クロスアカウントへのサポートを追加する	Global Accelerator は、アクセラレーターへのクロスアカウントリソースの追加をサポートするようになりました。クロスアカウントリソースのアクセス許可を追加するには、Global Accelerator でクロスアカウントアタッチメントを作成します。詳細については、「AWS Global Accelerator のクロスアカウントアタッチメントとエンドポイントの使用」を参照してください。	2023 年 11 月 1 日
4 つの AWS リージョン でサポートを追加する	Global Accelerator では以下の AWS リージョン におけるサポートが追加されました: アジアパシフィック (メルボルン)、欧州 (スペイン)、欧州 (チューリッヒ)、およびイスラエル (テルアビブ)。詳細については、「AWS リージョンでの AWS Global Accelerator の可用性」を参照してください。	2023 年 9 月 26 日

変更	説明	日付
サービスリンクロールを更新	サービスに新しいアクセス許可 `elasticloadbalancing:DescribeTargetGroups` を追加します。Global Accelerator は、ターゲットタイプとして識別するためのアクセス許可を使用しますが、これは Global Accelerator におけるデュアルスタックロードバランサーエンドポイントでサポートされていないターゲットタイプ `ip` です。詳細については、「AWS Global Accelerator のサービスリンクロール」を参照してください。	2023 年 9 月 12 日
Network Load Balancer のクライアント IP アドレスの保存のサポートを追加	Global Accelerator は、セキュリティグループを使用して Network Load Balancer のクライアント IP アドレスの保存を有効にすることをサポートするようになりました。詳細については、「クライアント IP アドレスの保存によるエンドポイントの追加または更新」を参照してください。	2023 年 8 月 22 日

変更	説明	日付
EC2 インスタンスの IPv6 サポートを追加する	Global Accelerator は、デュアルスタックアクセラレーターへの Amazon EC2 インスタンスの追加をサポートし、EC2 エンドポイントへの IPv4 トラフィックと IPv6 トラフィックの両方を有効にするようになりました。サポートされているエンドポイントタイプのフルリストと詳細については、「AWS Global Accelerator の標準アクセラレーターのエンドポイント」を参照してください。	2023 年 8 月 8 日
新しいリージョンを追加した	Global Accelerator がアジアパシフィック (ジャカルタ) をサポートするようになりました。サポートされているリージョンの完全なリストについては、「AWS リージョン での AWS Global Accelerator の可用性」を参照してください。	2023 年 6 月 15 日
2 つの新しいリージョンを追加した	Global Accelerator が、アジアパシフィック (ハイデラバード) と中東 (UAE) をサポートするようになりました。サポートされているリージョンの完全なリストについては、「AWS リージョン での AWS Global Accelerator の可用性」を参照してください。	2023 年 5 月 23 日

変更	説明	日付
サービスリンクロールを更新	Global Accelerator のサービスリンクロールに新しいアクセス許可 `elasticloadbalancing:DescribeListeners` と `ec2:DescribeAddresses` を追加し、リスナー設定に基づいてロードバランサーのリスナー管理の意思決定を行い、アクセラレーターに Elastic IP アドレスエンドポイントを追加します。詳細については、「AWS Global Accelerator のサービスリンクロール」を参照してください。	2023 年 5 月 23 日
カスタムルーティングアクセラレータークォータを追加する	カスタムルーティングアクセラレータークォータを追加します。Global Accelerator には、標準アクセラレーターのクォータもあります。詳細については、「AWS Global Accelerator のクォータ」を参照してください。	2023 年 2 月 13 日
ガイドの IAM ガイダンスを更新します	IAM ベストプラクティスに沿ってガイドを更新しました。詳細については、「IAM のセキュリティのベストプラクティス」を参照してください。	2023 年 2 月 10 日

変更	説明	日付
AddEndpoints および RemoveEndpoints の更新	Global Accelerator は、新しい AddEndpoints および RemoveEndpoints API オペレーションを使用することで、UpdateEndpointGroup API オペレーションを使用せずにエンドポイントを個別に追加および削除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/global-accelerator-actions.html」を参照してください。	2022 年 10 月 20 日
デュアルスタックアクセラレーターの更新	Global Accelerator がデュアルスタックアクセラレーターをサポートするようになりました。IPv4 の場合、Global Accelerator は 2 つの静的 IPv4 アドレスを提供します。デュアルスタックの場合、Global Accelerator は 2 つの IPv4 アドレスと 2 つの IPv6 アドレス、合計 4 つのグローバルの静的 IP アドレスを提供します。詳細については、「https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html」を参照してください。	2022 年 7 月 27 日

変更	説明	日付
Global Accelerator の既存のサービスリンクロールの更新	Global Accelerator は、IPv6 アドレスをサポートする新しいアクセス許可 `ec2:AssignIpv6Addresses` と `ec2:UnassignIpv6Addresses` を追加しました。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 11 月 2 日
新しい CloudWatch メトリクスを追加した	Global Accelerator は、2 つの新しい CloudWatch メトリクスを追加した。詳細については、「https://docs.aws.amazon.com/global-accelerator/latest/dg/cloudwatch-monitoring.html」を参照してください。	2021 年 10 月 28 日
フローログキャプチャウィンドウの更新	Global Accelerator は、フローログキャプチャウィンドウを 10 秒から 60 秒に拡張しました。詳細については、「https://docs.aws.amazon.com/global-accelerator/latest/dg/monitoring-global-accelerator.flow-logs.html」を参照してください。	2021 年 7 月 30 日

変更	説明	日付
Global Accelerator の既存のサービスリンクロールの更新	Global Accelerator は、エラーの診断に役立つ AWS リージョン情報を取得できるようにする新しいアクセス許可 `ec2:DescribeRegions` を追加しました。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ーを追加した	Global Accelerator は、新しいタイプの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ーを導入しました。カスタムルーティングアクセラレーターは、独自のアプリケーションロジックを使用して、多数の送信先とポートの中から特定の送信先とポートに 1 人または複数のユーザーを送信したい場合に適しています。この場合でも、Global Accelerator のパフォーマンス向上の利点を得ることができます。詳細については、「https://docs.aws.amazon.com/global-accelerator/latest/dg/work-with-custom-routing-accelerators.html」を参照してください。	2020 年 12 月 9 日

変更	説明	日付
ポート上書きへのサポートを追加した	Global Accelerator では、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されるリスナーポートの上書きがサポートされるようになりました。これにより、トラフィックをエンドポイント上の特定のポートに再ルーティングできます。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を追加した	Global Accelerator がアフリカ (ケープタウン) と欧州 (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
タグ付けと BYOIP	このリリースでは、アクセラレーターにタグを追加し、独自の IP アドレスを AWS Global Accelerator (BYOIP) に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
セキュリティ章が追加されました。	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 名へのサポート	AWS Global Accelerator では、サポートされている AWS リージョンへの 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、Global Accelerator は、アクセラレーターの静的 IP アドレスにマッピングされたデフォルトの 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
Application Load Balancer のクライアント IP アドレスの保存	これで、サポートされている AWS リージョンで Application Load Balancer 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 デベロッパーガイドには、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るアクセラレーターであるネットワークレイヤートラフィックマネージャーの設定と使用に関する情報が記載されています。	2018 年 11 月 26 日