

Gateway Load Balancer

エラスティックロードバランシング



Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

エラスティックロードバランシング: Gateway Load Balancer

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスはAmazon 以外の製品およびサービスに使用することはできま せん。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使 用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、 関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

Gateway Load Balancer とは?	. 1
Gateway Load Balancer の概要	1
アプライアンスベンダー	. 2
入門	2
料金	2
入門	3
概要	3
ルーティング	5
前提条件	6
ステップ 1: Gateway Load Balancer を作成する	6
ステップ 2: Gateway Load Balancer エンドポイントサービスを作成する	8
ステップ 3: Gateway Load Balancer エンドポイントを作成する	9
ステップ 4: ルーティングを設定する [,]	10
CLI を使用した開始方法	12
概要	12
ルーティング	5
前提条件	15
ステップ 1: Gateway Load Balancer を作成し、ターゲットを登録する	16
ステップ 2: Gateway Load Balancer エンドポイントを作成する	17
ステップ 3: ルーティングを設定する	18
Gateway Load Balancer	20
ロードバランサーの状態	20
IP アドレスタイプ	21
アベイラビリティーゾーン	22
アイドルタイムアウト	22
ロードバランサーの属性	23
ネットワーク ACL	23
非対称フロー	23
ネットワーク最大送信単位 (MTU)	23
ロードバランサーの作成	24
前提条件	24
ロードバランサーを作成する	24
重要な次のステップ	25
IP アドレスタイプを更新する	26

	ロードバランサー属性を編集する	26
	削除保護	26
	クロスゾーンロードバランサー	27
	ロードバランサーのタグ付け	28
	ロードバランサーの削除	. 29
	LCU 予約	30
	予約をリクエストする	31
	予約を更新または終了する	32
	予約をモニタリングする	. 32
リ	スナー	. 34
	リスナー属性	. 34
	リスナーターゲットグループの更新	. 34
	アイドルタイムアウトの更新	35
タ	ーゲットグループ	. 36
	ルーティング設定	36
	対象タイプ	37
	登録済みターゲット	. 38
	ターゲットグループの属性	38
	ターゲットグループの作成	39
	ヘルスチェックを設定する	40
	ヘルスチェックの設定	41
	ターゲットヘルスステータス	. 42
	ヘルスチェックの理由コード	. 44
	ターゲット障害シナリオ	. 45
	ターゲットのヘルスステータスをチェックする	. 45
	ヘルスチェックの設定の変更	. 46
	ターゲットグループ属性を編集する	. 46
	ターゲットフェイルオーバー	. 47
	登録解除の遅延	48
	フローの維持設定	. 49
	ターケットの登録	50
	考慮事項	51
	ターケットセキュリティクルーフ	51
	ネットリーク ACL	51
	イン人タン人 ID によるターケットの登録	52
	IP	. 52

53
53
54
56
57
57
61
61
64
64
64
65
66
. Ixviii

Gateway Load Balancer とは?

Elastic Load Balancing は、受信したトラフィックを複数のアベイラビリティーゾーンの複数のター ゲットに自動的に分散させます。登録されているターゲットの状態をモニタリングし、正常なター ゲットにのみトラフィックをルーティングします。Elastic Load Balancing は、受信トラフィックの 時間的な変化に応じて、ロードバランサーをスケーリングします。また、大半のワークロードに合わ せて自動的にスケーリングできます。

Elastic Load Balancing は、Application Load Balancer、Network Load Balancer、Gateway Load Balancer、Classic Load Balancer といったロードバランサーをサポートします。ニーズに最適なタ イプのロードバランサーを選択できます。このガイドでは、Gateway Load Balancer について説明 します。その他のロードバランサーの詳細については、「<u>Application Load Balancer ユーザーガイ</u> <u>ド</u>」、「<u>Network Load Balancer ユーザーガイド</u>」、および「<u>Classic Load Balancer ユーザーガイ</u> ド」を参照してください。

Gateway Load Balancer の概要

ゲートウェイロードバランサ-を使用すると、ファイアウォール、侵入検知および防止システム、 ディープパケットインスペクションシステムなどの仮想アプライアンスをデプロイ、スケーリング、 管理できます。透過的なネットワークゲートウェイ(つまり、すべてのトラフィックに対して単一の 入口と出口ポイント)を組み合わせて、トラフィックを分散しながら、仮想アプライアンスを需要に 応じてスケーリングします。

ゲートウェイロードバランサーは、開放型システム間相互接続 (OSI) モデルの第3層(ネットワー クレイヤー)で機能します。すべてのポートですべての IP パケットをリッスンし、リスナールー ルで指定されたターゲットグループにトラフィックを転送します。5 タプル (デフォルト)、3 タ プル、または2タプルを使用して、特定のターゲットアプライアンスへのフローの維持 を保持しま す。Gateway Load Balancer とその登録された仮想アプライアンスインスタンスは、ポート 6081 で GENEVE プロトコルを使用してアプリケーショントラフィックを交換します。

ゲートウェイロードバランサーは、ゲートウェイロードバランサーのエンドポイントを使用し て、VPC 境界を越えてトラフィックを安全に交換します。ゲートウェイロードバランサーエンドポ イントは、サービスプロバイダー VPC 内の仮想アプライアンスとサービスコンシューマー VPC 内 のアプリケーションサーバー間のプライベート接続を提供する VPC エンドポイントです。ゲート ウェイLoad Balancer は、仮想アプライアンスと同じ VPC にデプロイします。仮想アプライアンス は、ゲートウェイ Load Balancer ターゲットグループに登録します。 Gateway Load Balancer エンドポイントとの間で送受信されるトラフィックは、ルートテーブルを使用して設定されます。トラフィックは、サービスコンシューマー VPC から Gateway Load Balancer エンドポイントを経由してサービスプロバイダー VPC 内の Gateway Load Balancer に流れ、サー ビスコンシューマー VPC に戻ります。Gateway Load Balancer エンドポイントとアプリケーション サーバーは、別のサブネットに作成する必要があります。これにより、Gateway Load Balancer エン ドポイントをアプリケーションサブネットのルートテーブルのネクストホップとして構成できます。

詳細については、「AWS PrivateLink ガイド」の「<u>AWS PrivateLinkを通じて仮想アプライアンスに</u> アクセスする」を参照してください。

アプライアンスベンダー

アプライアンスベンダーのソフトウェアを選択して適格化する必要があります。ロードバランサーか らのトラフィックを検査または変更するには、アプライアンスソフトウェアを信頼する必要がありま す。Elastic Load Balancing パートナーとしてリストされているアプライアンスベンダーは、アプラ イアンスソフトウェアをと統合し、認定しています AWS。このリストのベンダーのアプライアンス ソフトウェアには、より高いレベルの信頼を置くことができます。ただし、 AWS は、これらのベン ダーのソフトウェアのセキュリティまたは信頼性を保証するものではありません。

入門

を使用して Gateway Load Balancer を作成するには AWS Management Console、「」を参照してく ださい<u>入門</u>。を使用して Gateway Load Balancer を作成するには AWS Command Line Interface、 「」を参照してくださいCLI を使用した開始方法。

料金

ロードバランサーについては、お客様が利用された分のみのお支払いとなります。詳細について は、<u>Elastic Load Balancing の料金表</u>を参照してください。

Gateway Load Balancer の使用開始方法

Gateway Load Balancer を使用すると、セキュリティアプライアンスなどのサードパーティー仮想ア プライアンスを簡単にデプロイ、スケーリング、管理できます。

このチュートリアルでは、Gateway Load Balancer と Gateway Load Balancer エンドポイントを使 用して検査システムを実装します。

内容

- 概要
- 前提条件
- ステップ 1: Gateway Load Balancer を作成する
- ステップ 2: Gateway Load Balancer エンドポイントサービスを作成する
- ステップ 3: Gateway Load Balancer エンドポイントを作成する
- ステップ 4: ルーティングを設定する

概要

Gateway Load Balancer エンドポイントは、サービスプロバイダー VPC 内の仮想アプライアンスと サービスコンシューマー VPC 内のアプリケーションサーバー間のプライベート接続を提供する VPC エンドポイントです。Gateway Load Balancer は、仮想アプライアンスと同じ VPC にデプロイされ ます。これらのアプライアンスは、Gateway Load Balancer のターゲットグループに登録されます。

アプリケーションサーバーはサービスコンシューマー VPC の 1 つのサブネット (宛先サブネット) で実行されますが、Gateway Load Balancer エンドポイントは同じ VPC の別のサブネットにあり ます。インターネットゲートウェイを経由してサービスコンシューマー VPC に入るすべてのトラ フィックは、まず、Gateway Load Balancer エンドポイントにルーティングされ、その後、送信先サ ブネットにルーティングされます。

同様に、アプリケーションサーバー (送信先サブネット) から出るすべてのトラフィック は、Gateway Load Balancer エンドポイントにルーティングされてから、インターネットにルーティ ングされます。次のネットワークの図は、Gateway Load Balancer エンドポイントがエンドポイント サービスへのアクセスにどのように使用されるのかを視覚的に示したものです。



下の番号付きの項目で、上記の図に示されている各要素がわかりやすく説明されています。

インターネットからアプリケーションへのトラフィック (青い矢印):

- トラフィックは、インターネットゲートウェイを介してサービスコンシューマー VPC に入ります。
- トラフィックは、入力ルーティングの結果として Gateway Load Balancer エンドポイントに送信されます。
- Gateway Load Balancer に送信されたトラフィックは、セキュリティアプライアンスの1つに 分散されます。
- 4. セキュリティアプライアンスによって検査されたトラフィックは Gateway Load Balancer エンドポイントに戻されます。
- 5. トラフィックはアプリケーションサーバー (宛先サブネット) に送信されます。

アプリケーションからインターネットへのトラフィック (オレンジの矢印):

 トラフィックは、アプリケーションサーバーのサブネットで設定されたデフォルトルートの結果 として、Gateway Load Balancer エンドポイントに送信されます。

- Gateway Load Balancer に送信されたトラフィックは、セキュリティアプライアンスの1つに 分散されます。
- セキュリティアプライアンスによって検査されたトラフィックは Gateway Load Balancer エンドポイントに戻されます。
- 4. トラフィックは、ルートテーブルの設定に基づいてインターネットゲートウェイに送信されま す。
- 5. トラフィックはインターネットにルーティングされます。

ルーティング

インターネットゲートウェイのルートテーブルには、アプリケーションサーバー宛てのトラフィック を Gateway Load Balancer エンドポイントにルーティングするエントリが必要です。Gateway Load Balancer エンドポイントを指定するには、VPC エンドポイントの ID を使用します。次の例は、 デュアルスタック設定のルートを示します。

デスティネーション	ターゲット
VPC IPv4 CIDR	ローカル
VPC IPv6 CIDR	ローカル
##### 1 IPv4 CIDR	vpc-endpoint-id
##### 1 IPv6 CIDR	vpc-endpoint-id

アプリケーションサーバーがあるサブネットのルートテーブルには、アプリケーションサーバーから のすべてのトラフィックを Gateway Load Balancer エンドポイントにルーティングするエントリが 必要です。

デスティネーション	ターゲット
VPC IPv4 CIDR	ローカル
VPC IPv6 CIDR	ローカル
0.0.0/0	vpc-endpoint-id

デスティネーション	ターゲット
::/0	vpc-endpoint-id

Gateway Load Balancer エンドポイントがあるサブネットのルートテーブルは、検査から返されるト ラフィックを最終的な送信先にルーティングする必要があります。インターネットを起点とするトラ フィックについては、ローカルルートによって、アプリケーションサーバーに確実に到達します。ア プリケーションサーバーを起点とするトラフィックに対して、すべてのトラフィックをインターネッ トゲートウェイにルーティングするエントリを追加します。

デスティネーション	ターゲット
VPC IPv4 CIDR	ローカル
VPC IPv6 CIDR	ローカル
0.0.0/0	internet-gateway-id
::/0	internet-gateway-id

前提条件

- サービスコンシューマー VPC に、アプリケーションサーバーを含むアベイラビリティーゾーンご とに少なくとも2つのサブネットがあることを確認します。1つのサブネットは Gateway Load Balancer エンドポイント用で、もう1つはアプリケーションサーバー用です。
- Gateway Load Balancer とターゲットは同じサブネットに配置できます。
- 別のアカウントから共有されているサブネットを使用して Gateway Load Balancer をデプロイす ることはできません。
- サービスプロバイダー VPC 内の各セキュリティアプライアンスサブネットで、少なくとも1つの セキュリティアプライアンスインスタンスを起動します。これらのインスタンスのセキュリティグ ループは、ポート 6081 で UDP トラフィックを許可する必要があります。

ステップ 1: Gateway Load Balancer を作成する

次の手順に従って、ロードバランサー、リスナー、ターゲットグループを作成します。

コンソールを使用して、ロードバランサー、リスナー、ターゲットグループを作成するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- 2. ナビゲーションペインの [Load Balancing] で、[Load Balancers] を選択します。
- 3. [ロードバランサーを作成]を選択します。
- 4. [Gateway Load Balancer] で、[Create] (作成) を選択します。
- 5. 基本的な設定
 - a. [ロードバランサー名] に、ロードバランサーの名前を入力します。
 - b. [IP アドレスタイプ] で、[IPv4] を選択して IPv4 アドレスのみをサポートするか、[デュアル スタック] を選択して IPv4 と IPv6 アドレスの両方をサポートします。
- 6. ネットワークマッピング
 - a. [VPC] では、サービスプロバイダー VPC を選択します。
 - b. [マッピング] で、セキュリティアプライアンスインスタンスを起動したすべてのアベイラビ
 リティーゾーン、およびアベイラビリティゾーンごとに1つのサブネットを選択します。
- 7. IP リスナーのルーティング
 - a. [デフォルトアクション] で、トラフィックを受信する既存のターゲットグループを選択しま す。このターゲットグループは GENEVE プロトコルを使用する必要があります。

ターゲットグループがない場合は、[ターゲットグループを作成] を選択します。ブラウザで 新しいタブが開きます。ターゲットタイプを選択し、ターゲットグループの名前を入力して GENEVE プロトコルを維持します。セキュリティアプライアンスインスタンスがある VPC を選択します。必要に応じてヘルスチェック設定を変更し、必要なタグを追加します。[次 へ] を選択します。ターゲットグループへのセキュリティアプライアンスインスタンスの登 録は、今すぐ行うか、この手順を完了した後に行うことができます。[ターゲットグループ の作成] を選択し、以前のブラウザタブに戻ります。

- b. (オプション)[リスナータグ]を展開し、必要なタグを追加します。
- 8. (オプション)[ロードバランサータグ]を展開し、必要なタグを追加します。
- 9. [ロードバランサーを作成]を選択します。

ステップ 2: Gateway Load Balancer エンドポイントサービスを作 成する

次の手順を使用して、Gateway Load Balancer を使用するエンドポイントサービスを作成します。

Gateway Load Balancer エンドポイントサービスを作成するには

- 1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
- 2. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
- 3. [エンドポイントサービスの作成]を選択し、以下の手順を実行します。
 - a. [Load balancer type] (ロードバランサーのタイプ) で、[Gateway] を選択します。
 - b. [Available load balancers] (使用可能なロードバランサー) で、お使いの Gateway Load Balancer を選択します。
 - c. [Require acceptance for endpoint] (エンドポイントの承諾が必要) で、[Acceptance required]
 (承諾が必要) を選択し、サービスへの接続リクエストを手動で承諾します。そうでない場合、これらのリクエストは自動的に受け入れられます。
 - d. [Supported IP address types] (サポートされている IP アドレスのタイプ) で、次のいずれか を実行します。
 - [IPv4] を選択 エンドポイントサービスが IPv4 リクエストを受け入れることができるようにします。
 - [IPv6]を選択 エンドポイントサービスが IPv6 リクエストを受け入れることができるようにします。
 - [IPv4] と [IPv6] を選択 エンドポイントサービスが IPv4 と IPv6 の両方のリクエストを 受け入れることができるようにします。
 - e. (オプション) タグを追加するには、[Add new tag] (新しいタグを追加) を選択し、タグキー とタグ値を入力します。
 - f. [作成]を選択します。サービス名を書き留めます。これはエンドポイントを作成するときに 必要になります。
- 新しいエンドポイントサービスを選択し、[アクション]、[プリンシパルを許可] の順に選択します。サービスへのエンドポイントの作成を許可されているサービスコンシューマーの ARN を入力します。サービスコンシューマーは、ユーザー、IAM ロール、または AWS アカウントです。 [プリンシパルを許可]を選択します。

ステップ 2: Gateway Load Balancer エンドポイントサービスを作成する

ステップ 3: Gateway Load Balancer エンドポイントを作成する

次の手順を使用して、Gateway Load Balancer エンドポイントサービスに接続する Gateway Load Balancer エンドポイントを作成します。Gateway Load Balancer エンドポイントにはゾーンが適用 されます。ゾーンごとに Gateway Load Balancer エンドポイントを 1 つ作成することをお勧めしま す。詳細については、「AWS PrivateLink ガイド」の「<u>AWS PrivateLinkを通じて仮想アプライアン</u> スにアクセスする」を参照してください。

Gateway Load Balancer エンドポイントを作成するには

- 1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
- 2. ナビゲーションペインで、[Endpoints] (エンドポイント) を選択します。
- 3. [エンドポイントの作成]を選択し、以下の手順を実行します。
 - a. [Service category] (サービスカテゴリ) で、[Other endpoint services] (その他のエンドポイン トサービス) を選択します。
 - b. 以前に書き留めたしたサービスの名前を [サービス名] に入力し、[確認] を選択します。
 - c. [VPC] では、サービスコンシューマー VPC を選択します。
 - d. [Subnets] (サブネット) で、Gateway Load Balancer エンドポイントのサブネットを選択します。

注: Gateway Load Balancer エンドポイントの作成時に選択できるサブネットは、各アベ イラビリティーゾーンで1つだけです。

- e. [IP address type] (IP アドレスのタイプ) で、次のオプションから選択します。
 - [IPv4] IPv4 アドレスをエンドポイントのネットワークインターフェイスに割り当てます。このオプションは、選択したすべてのサブネットに IPv4 アドレス範囲がある場合にのみサポートされます。
 - [IPv6] IPv6 アドレスをエンドポイントのネットワークインターフェイスに割り当てます。このオプションは、選択したすべてのサブネットが IPv6 のみのサブネットである場合にのみサポートされます。
 - [Dualstack] IPv4 と IPv6 の両方のアドレスをエンドポイントのネットワークインター フェイスに割り当てます。このオプションは、選択したすべてのサブネットに IPv4 と IPv6 の両方のアドレス範囲がある場合にのみサポートされます。
- f. (オプション) タグを追加するには、[Add new tag] (新しいタグを追加) を選択し、タグキー とタグ値を入力します。

g. [エンドポイントの作成]を選択します。初期ステータスはpending acceptance です。

エンドポイント接続リクエストを受け入れるには、次の手順を使用します。

- 1. ナビゲーションペインで、[Endpoint Services] (エンドポイントサービス) を選択します。
- 2. エンドポイントサービスを選択します。
- 3. [Endpoint connections] (エンドポイント接続) タブで、エンドポイント接続を選択します。
- 接続リクエストを承諾するには、[Actions] (アクション)、[Accept endpoint connection request] (エンドポイント接続リクエストを承諾)の順に選択します。確認を求められたら、accept と入 力し、[Accept] (承諾)を選択します。

ステップ 4: ルーティングを設定する

次のようにして、サービスコンシューマー VPC のルートテーブルを設定します。これにより、セ キュリティアプライアンスは、アプリケーションサーバー宛てのインバウンドトラフィックに対して セキュリティ検査を実行できます。

ルーティングを設定するには

- 1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
- 2. ナビゲーションペインで、[Route tables] (ルートテーブル) を選択します。
- 3. インターネットゲートウェイのルートテーブルを選択し、以下を実行します。
 - a. [アクション]、[ポリシーの編集]の順に選択します。
 - b. [Add Rule (ルートの追加)] を選択します。[Destination] (送信先) に、アプリケーションサー バーのサブネットの IPv4 CIDR ブロックを入力します。[Target] (ターゲット) で、VPC エ ンドポイントを選択します。
 - c. IPv6 をサポートしている場合は、[Add route] (ルートを追加) を選択します。[Destination] (送信先) に、アプリケーションサーバーのサブネットの IPv6 CIDR ブロックを入力しま す。[Target] (ターゲット) で、VPC エンドポイントを選択します。
 - d. [Save changes] (変更の保存) をクリックします。
- 4. アプリケーションサーバーを含むサブネットのルートテーブルを選択し、以下を実行します。
 - a. [アクション]、[ポリシーの編集]の順に選択します。

- b. [Add Rule (ルートの追加)] を選択します。[送信先] に「0.0.0.0/0」と入力しま す。[Target] (ターゲット) で、VPC エンドポイントを選択します。
- c. IPv6 をサポートしている場合は、[Add route] (ルートを追加) を選択します。[送信先] に 「**::/0**」と入力します。[Target] (ターゲット) で、VPC エンドポイントを選択します。
- d. [Save changes] (変更の保存) をクリックします。
- 5. Gateway Load Balancer エンドポイントを持つサブネットのルートテーブルを選択し、以下を実行します。
 - a. [アクション]、[ポリシーの編集] の順に選択します。
 - b. [Add Rule (ルートの追加)] を選択します。[送信先] に「**0.0.0.0/0**」と入力しま す。[Target] (ターゲット) で、インターネットゲートウェイを選択します。
 - c. IPv6 をサポートしている場合は、[Add route] (ルートを追加) を選択します。[送信先] に 「**::/0**」と入力します。[Target] (ターゲット) で、インターネットゲートウェイを選択し ます。
 - d. [Save changes] (変更の保存) をクリックします。

を使用した Gateway Load Balancer の開始方法 AWS CLI

Gateway Load Balancer を使用すると、セキュリティアプライアンスなどのサードパーティー仮想ア プライアンスを簡単にデプロイ、スケーリング、管理できます。

このチュートリアルでは、Gateway Load Balancer と Gateway Load Balancer エンドポイントを使用して検査システムを実装します。

内容

- <u>概要</u>
- 前提条件
- ステップ 1: Gateway Load Balancer を作成し、ターゲットを登録する
- ステップ 2: Gateway Load Balancer エンドポイントを作成する
- ステップ 3: ルーティングを設定する

概要

Gateway Load Balancer エンドポイントは、サービスプロバイダー VPC 内の仮想アプライアンスと サービスコンシューマー VPC 内のアプリケーションサーバー間のプライベート接続を提供する VPC エンドポイントです。Gateway Load Balancer は、仮想アプライアンスと同じ VPC にデプロイされ ます。これらのアプライアンスは、Gateway Load Balancer のターゲットグループに登録されます。

アプリケーションサーバーはサービスコンシューマー VPC の 1 つのサブネット (宛先サブネット) で実行されますが、Gateway Load Balancer エンドポイントは同じ VPC の別のサブネットにあり ます。インターネットゲートウェイを経由してサービスコンシューマー VPC に入るすべてのトラ フィックは、まず、Gateway Load Balancer エンドポイントにルーティングされ、その後、送信先サ ブネットにルーティングされます。

同様に、アプリケーションサーバー (送信先サブネット) から出るすべてのトラフィック は、Gateway Load Balancer エンドポイントにルーティングされてから、インターネットにルーティ ングされます。次のネットワークの図は、Gateway Load Balancer エンドポイントがエンドポイント サービスへのアクセスにどのように使用されるのかを視覚的に示したものです。



下の番号付きの項目で、上記の図に示されている各要素がわかりやすく説明されています。

インターネットからアプリケーションへのトラフィック (青い矢印):

- トラフィックは、インターネットゲートウェイを介してサービスコンシューマー VPC に入ります。
- トラフィックは、入力ルーティングの結果として Gateway Load Balancer エンドポイントに送信されます。
- Gateway Load Balancer に送信されたトラフィックは、セキュリティアプライアンスの1つに 分散されます。
- 4. セキュリティアプライアンスによって検査されたトラフィックは Gateway Load Balancer エンドポイントに戻されます。
- 5. トラフィックはアプリケーションサーバー (宛先サブネット) に送信されます。

アプリケーションからインターネットへのトラフィック (オレンジの矢印):

 トラフィックは、アプリケーションサーバーのサブネットで設定されたデフォルトルートの結果 として、Gateway Load Balancer エンドポイントに送信されます。

- Gateway Load Balancer に送信されたトラフィックは、セキュリティアプライアンスの1つに 分散されます。
- セキュリティアプライアンスによって検査されたトラフィックは Gateway Load Balancer エンドポイントに戻されます。
- 4. トラフィックは、ルートテーブルの設定に基づいてインターネットゲートウェイに送信されま す。
- 5. トラフィックはインターネットにルーティングされます。

ルーティング

インターネットゲートウェイのルートテーブルには、アプリケーションサーバー宛てのトラフィック を Gateway Load Balancer エンドポイントにルーティングするエントリが必要です。Gateway Load Balancer エンドポイントを指定するには、VPC エンドポイントの ID を使用します。次の例は、 デュアルスタック設定のルートを示します。

デスティネーション	ターゲット
VPC IPv4 CIDR	ローカル
VPC IPv6 CIDR	ローカル
##### 1 IPv4 CIDR	vpc-endpoint-id
##### 1 IPv6 CIDR	vpc-endpoint-id

アプリケーションサーバーがあるサブネットのルートテーブルには、アプリケーションサーバーから のすべてのトラフィックを Gateway Load Balancer エンドポイントにルーティングするエントリが 必要です。

デスティネーション	ターゲット
VPC IPv4 CIDR	ローカル
VPC IPv6 CIDR	ローカル
0.0.0/0	vpc-endpoint-id

デスティネーション	ターゲット
::/0	vpc-endpoint-id

Gateway Load Balancer エンドポイントがあるサブネットのルートテーブルは、検査から返されるト ラフィックを最終的な送信先にルーティングする必要があります。インターネットを起点とするトラ フィックについては、ローカルルートによって、アプリケーションサーバーに確実に到達します。ア プリケーションサーバーを起点とするトラフィックに対して、すべてのトラフィックをインターネッ トゲートウェイにルーティングするエントリを追加します。

デスティネーション	ターゲット
VPC IPv4 CIDR	ローカル
VPC IPv6 CIDR	ローカル
0.0.0/0	internet-gateway-id
::/0	internet-gateway-id

前提条件

- Gateway Load Balancer をサポートしていないバージョンを使用している場合 AWS CLI は、 をインストールする AWS CLI か、 の最新バージョンに更新します。詳細については、<u>AWS CLIユー</u>ザーガイドのAWS Command Line Interface のインストールを参照してください。
- サービスコンシューマー VPC に、アプリケーションサーバーを含むアベイラビリティーゾーンご とに少なくとも2つのサブネットがあることを確認します。1つのサブネットは Gateway Load Balancer エンドポイント用で、もう1つはアプリケーションサーバー用です。
- サービスプロバイダー VPC に、セキュリティアプライアンスインスタンスを含むアベイラビリ ティーゾーンごとに少なくとも2つのサブネットがあることを確認します。1つのサブネットは Gateway Load Balancer 用で、もう1つはインスタンス用です。
- サービスプロバイダー VPC 内の各セキュリティアプライアンスサブネットで、少なくとも1つの セキュリティアプライアンスインスタンスを起動します。これらのインスタンスのセキュリティグ ループは、ポート 6081 で UDP トラフィックを許可する必要があります。

ステップ 1: Gateway Load Balancer を作成し、ターゲットを登録 する

次の手順に従って、ロードバランサー、リスナー、およびターゲットグループを作成し、セキュリ ティアプライアンスインスタンスをターゲットとして登録します。

Gateway Load Balancer を作成し、ターゲットを登録するには

 <u>create-load-balancer</u> コマンドを使用して、gateway タイプのロードバランサーを作成します。 セキュリティアプライアンスインスタンスを起動したアベイラビリティーゾーンごとに1つの サブネットを指定できます。

aws elbv2 create-load-balancer --name my-load-balancer --type gateway -subnets provider-subnet-id

デフォルトでは、IPv4 アドレスのみがサポートされます。IPv4 と IPv6 の両方のアドレスをサ ポートするには、--ip-address-type dualstack オプションを追加します。

出力には、次の例に示されている形式でロードバランサーの Amazon リソースネーム (ARN) が 含まれます。

arn:aws:elasticloadbalancing:us-east-2:123456789012:loadbalancer/gwy/my-loadbalancer/1234567890123456

2. <u>create-target-group</u> コマンドを使用して、インスタンスを起動したサービスプロバイダー VPC を指定し、ターゲットグループを作成します。

aws elbv2 create-target-group --name my-targets --protocol GENEVE --port 6081 -vpc-id provider-vpc-id

出力には、次の形式でターゲットグループの ARN が含まれます。

arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/mytargets/0123456789012345

3. インスタンスをターゲットグループに登録するには、register-targets コマンドを使用します。

aws elbv2 register-targets --target-group-arn targetgroup-arn --targets
Id=i-1234567890abcdef0 Id=i-0abcdef1234567890

4. <u>create-listener</u> コマンドを使用して、ターゲットグループにリクエストを転送するデフォルト ルールを持つロードバランサーのリスナーを作成します。

aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --default-actions
Type=forward,TargetGroupArn=targetgroup-arn

出力には、次の形式のリスナーの ARN が含まれます。

arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/gwy/my-loadbalancer/1234567890123456/abc1234567890123

5. (オプション)次の <u>describe-target-health</u> コマンドを使用してターゲットグループの登録された ターゲットのヘルスステータスを確認できます。

aws elbv2 describe-target-health --target-group-arn targetgroup-arn

ステップ 2: Gateway Load Balancer エンドポイントを作成する

次の手順に従って、Gateway Load Balancer エンドポイントを作成します。Gateway Load Balancer エンドポイントにはゾーンが適用されます。ゾーンごとに Gateway Load Balancer エンドポイント を 1 つ作成することをお勧めします。詳細については、「<u>AWS PrivateLinkを通じて仮想アプライア</u> ンスにアクセスする」を参照してください。

Gateway Load Balancer エンドポイントを作成するには

 <u>create-vpc-endpoint-service-configuration</u> コマンドを使用して、Gateway Load Balancer を使用 するエンドポイントサービス設定を作成します。

aws ec2 create-vpc-endpoint-service-configuration --gateway-load-balancerarns loadbalancer-arn --no-acceptance-required

IPv4 と IPv6 の両方のアドレスをサポートするには、--supported-ip-address-types ipv4 ipv6 オプションを追加します。 出力には、サービス ID (例: vpce-svc-12345678901234567)、およびサービス名 (例: com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567) が含まれます。

 modify-vpc-endpoint-service-permissions コマンドを使用して、サービスコンシューマーが サービスへのエンドポイントを作成できるようにします。サービスコンシューマーは、ユー ザー、IAM ロール、または AWS アカウントです。次の の例では、指定された のアクセス許可 を追加します AWS アカウント。

aws ec2 modify-vpc-endpoint-service-permissions --service-id vpcesvc-12345678901234567 --add-allowed-principals arn:aws:iam::123456789012:root

 <u>create-vpc-endpoint</u> コマンドを使用して、サービス用の Gateway Load Balancer エンドポイン トを作成します。

aws ec2 create-vpc-endpoint --vpc-endpoint-type GatewayLoadBalancer --servicename com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567 --vpc-id consumer-vpcid --subnet-ids consumer-subnet-id

IPv4 と IPv6 の両方のアドレスをサポートするには、--ip-address-type dualstack オプ ションを追加します。

出力には、Gateway Load Balancer エンドポイントの ID (例: vpce-01234567890abcdef) が含ま れます。

ステップ 3: ルーティングを設定する

次のようにして、サービスコンシューマー VPC のルートテーブルを設定します。これにより、セ キュリティアプライアンスは、アプリケーションサーバー宛てのインバウンドトラフィックに対して セキュリティ検査を実行できます。

ルーティングを設定するには

 <u>create-route</u> コマンドを使用して、アプリケーションサーバー宛てのトラフィックを Gateway Load Balancer エンドポイントにルーティングするエントリをインターネットゲートウェイの ルートテーブルに追加します。

aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1
IPv4 CIDR --vpc-endpoint-id vpce-01234567890abcdef

IPv6 をサポートするには、次のルートを追加します。

aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1
IPv6 CIDR --vpc-endpoint-id vpce-01234567890abcdef

<u>create-route</u> コマンドを使用して、アプリケーションサーバーから Gateway Load Balancer エンドポイントにすべてのトラフィックをルーティングするエントリを、アプリケーションサーバーを持つサブネットのルートテーブルに追加します。

aws ec2 create-route --route-table-id application-rtb --destination-cidr-block
 0.0.0.0/0 --vpc-endpoint-id vpce-01234567890abcdef

IPv6 をサポートするには、次のルートを追加します。

aws ec2 create-route --route-table-id application-rtb --destination-cidr-block ::/0
 --vpc-endpoint-id vpce-01234567890abcdef

<u>create-route</u> コマンドを使用して、アプリケーションサーバーを起点とするすべてのトラフィックをインターネットゲートウェイにルーティングするエントリを、Gateway Load Balancer エンドポイントを持つサブネットのルートテーブルに追加します。

aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block 0.0.0.0/0 --gateway-id igw-01234567890abcdef

IPv6 をサポートするには、次のルートを追加します。

aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block ::/0 -gateway-id igw-01234567890abcdef

4. 各ゾーン内のアプリケーションサブネットのルートテーブルごとに繰り返します。

Gateway Load Balancer

Gateway Load Balancer を使用して、GENEVE プロトコルをサポートする仮想アプライアンスのフ リートをデプロイおよび管理します。

Gateway Load Balancer は、開放型システム間相互接続 (OSI) モデルの第3層で機能します。すべて のポートですべての IP パケットをリッスンし、ポート 6081 で GENEVE プロトコルを使用して、リ スナールールで指定されたターゲットグループにトラフィックを転送します。

リクエストの流れを中断することなく、ニーズの変化に応じてロードバランサーに対してターゲットの追加または削除を行うことができます。Elastic Load Balancing はアプリケーションへのトラフィックが時間の経過とともに変化するのに応じてロードバランサーをスケーリングします。Elastic Load Balancing では、大半のワークロードに合わせた自動的なスケーリングが可能です。

内容

- ロードバランサーの状態
- <u>IP アドレスタイプ</u>
- アベイラビリティーゾーン
- アイドルタイムアウト
- <u>ロードバランサーの属性</u>
- ネットワーク ACL
- <u>非対称フロー</u>
- ネットワーク最大送信単位 (MTU)
- ゲートウェイロードバランサーを作成
- Gateway Load Balancer の IP アドレスタイプを更新する
- Gateway Load Balancer の属性を編集する
- Gateway Load Balancer のタグ付け
- Gateway Load Balancer の削除
- Gateway Load Balancer のキャパシティ予約

ロードバランサーの状態

Gateway Load Balancer の状態は次のいずれかです。

provisioning

Gateway Load Balancer はセットアップ中です。

active

Gateway Load Balancer は完全にセットアップされており、トラフィックをルーティングする準 備ができています。

failed

Gateway Load Balancer をセットアップできませんでした。

IP アドレスタイプ

Gateway Load Balancer にアクセスするためにアプリケーションサーバーが使用できる IP アドレス の種類を設定できます。

Gateway Load Balancer は、次の IP アドレスタイプをサポートしています。

ipv4

IPv4 のみがサポートされます。

dualstack

IPv4 と IPv6 がサポートされます。

考慮事項

- ロードバランサーに指定する Virtual Private Cloud (VPC) とサブネットには、IPv6 CIDR ブロックが関連付けられている必要があります。
- サービスコンシューマー VPC のサブネットのルートテーブルは IPv6 トラフィックをルーティ ングする必要があり、これらのサブネットのネットワーク ACL は IPv6 トラフィックを許可す る必要があります。
- Gateway Load Balancer は、IPv4 と IPv6 の両方のクライアントトラフィックを IPv4 GENEVE ヘッダーでカプセル化してアプライアンスに送信します。アプライアンスは IPv4 と IPv6 の 両方のクライアントトラフィックを IPv4 GENEVE ヘッダーでカプセル化して Gateway Load Balancer に返します。

IP アドレスのタイプについては、「<u>Gateway Load Balancer の IP アドレスタイプを更新する</u>」を参 照してください。

アベイラビリティーゾーン

Gateway Load Balancer を作成するときは、1 つ以上のアベイラビリティーゾーンを有効にし、各 ゾーンに対応するサブネットを指定します。複数のアベイラビリティーゾーンを有効にすると、アベ イラビリティーゾーンが使用できなくなっても、ロードバランサーがトラフィックをルーティングし 続けることができます。指定するサブネットにはそれぞれ、最低 8 個の利用可能な IP アドレスが必 要です。サブネットは、ロードバランサーの作成後に削除できません。サブネットを削除するには、 新しいロードバランサーを作成する必要があります。

アイドルタイムアウト

Gateway Load Balancer を通じて行う TCP リクエストごとに、その接続の状態が追跡されます。ア イドルタイムアウトよりも長い時間、クライアントからもターゲットからもその接続経由でデータ が送信されない場合、接続は閉じられます。アイドルタイムアウト期間が経過した後、ロードバラン サーは次の TCP SYN を新しいフローと見なし、それを新しいターゲットにルーティングします。た だし、アイドルタイムアウト期間が経過した後に送信されるデータパケットは削除されます。

TCP フローのデフォルトのアイドルタイムアウト値は 350 秒ですが、60~6,000 秒の任意の値に更 新できます。クライアントまたはターゲットは TCP キープアライブパケットを使用して、アイドル タイムアウトをリセットできます。

<u> 維</u>持の制限

Gateway Load Balancer のアイドルタイムアウトは、5 タプルの維持を使用している場合に のみ更新できます。3 タプルまたは 2 タプルのスティクネスを使用する場合、デフォルトの アイドルタイムアウト値が使用されます。詳細については、<u>フローの維持設定</u>を参照してく ださい。

UDP はコネクションレスですが、ロードバランサーは送信元と宛先のIPアドレスとポートに基づい て UDP フロー状態を維持します。これにより、同じフローに属するパケットが一貫して同じター ゲットに一貫して同じターゲットに送信されます。アイドルタイムアウト期間が経過した後、ロード バランサーは着信 UDP パケットを新しいフローとみなし、それを新しいターゲットにルーティング します。Elastic Load Balancing は、UDP フローのアイドルタイムアウト値を 120 秒に設定します。 これは変更できません。

EC2 インスタンスは、リターンパスを確立するために、30 秒以内に新しいリクエストに応答する必要があります。

詳細については、「アイドルタイムアウトの更新」を参照してください。

ロードバランサーの属性

Gateway Load Balancer のロードバランサーの属性を以下に示します。

deletion_protection.enabled

削除保護が有効化されているかどうかを示します。デフォルトは false です。 load_balancing.cross_zone.enabled

クロスゾーン負荷分散が有効かどうかを示します。デフォルトは false です。

詳細については、「ロードバランサー属性を編集する」を参照してください。

ネットワーク ACL

アプリケーションサーバーと Gateway Load Balancer エンドポイントが同じサブネットにある場 合、アプリケーションサーバーから Gateway Load Balancer エンドポイントへのトラフィックにつ いて NACL ルールが評価されます。

非対称フロー

ロードバランサーが最初のフローパケットを処理し、応答フローパケットがロードバランサーを経由 しない場合、Gateway Load Balancer は非対称フローをサポートします。非対称ルーティングはネッ トワークのパフォーマンスを低下させる可能性があるため推奨されません。ロードバランサーが最 初のフローパケットを処理せず、応答フローパケットがロードバランサーを経由する場合、Gateway Load Balancer は非対称フローをサポートしません。

ネットワーク最大送信単位 (MTU)

最大送信単位 (MTU) は、ネットワーク上で送信できる最大データパケットサイズです。Gateway Load Balancer インターフェイス MTU は、最大 8,500 バイトのパケットをサポートします。8,500 バイトを超えるサイズのパケットが Gateway Load Balancer インターフェイスに到着した場合、そ のパケットはドロップされます。

Gateway Load Balancer は、IP トラフィックを GENEVE ヘッダーでカプセル化してアプライアン スに転送します。GENEVE カプセル化プロセスは、元のパケットに 68 バイトを追加します。した がって、最大 8,500 バイトのパケットをサポートするには、アプライアンスの MTU 設定が少なくと も 8,568 バイトのパケットをサポートしていることを確認します。

Gateway Load Balancer は、IP フラグメント化をサポートしていません。また、Gateway Load Balancer は「送信先に到達できません: フラグメント化が必要ですが、フラグメント化しないが設定 されています」というICMPメッセージを生成しません。このため、パス MTU 検出 (PMTUD) はサ ポートされていません。

ゲートウェイロードバランサーを作成

Gateway Load Balancer はクライアントからリクエストを受け取り、EC2 インスタンスなどのター ゲットグループのターゲット間でリクエストを割り当てます。

を使用して Gateway Load Balancer を作成するには AWS Management Console、次のタスクを実行 します。または、 を使用して Gateway Load Balancer を作成するには AWS CLI、「」を参照してく ださいCLI を使用した開始方法。

タスク

- 前提条件
- ロードバランサーを作成する
- 重要な次のステップ

前提条件

開始する前に、Gateway Load Balancer の仮想プライベートクラウド (VPC) について、ターゲッ トがある各アベイラビリティーゾーンに少なくとも 1 つのサブネットがあることを確認してくださ い。

ロードバランサーを作成する

次の手順に従って、Gateway Load Balancer を作成します。名前やIP アドレスの種類など、ロー ドバランサーの基本的な設定情報を指定します。次に、ネットワークに関する情報と、トラフィッ クをターゲットグループにルーティングするリスナーを指定します。Gateway Load Balancer には GENEVE プロトコルを使用するターゲットグループが必要です。

コンソールを使用してロードバランサーとリスナーを作成するには

1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。

- 2. ナビゲーションペインの [Load Balancing] で、[Load Balancers] を選択します。
- 3. [ロードバランサーを作成]を選択します。
- 4. [Gateway Load Balancer] で、[Create] (作成) を選択します。
- 5. 基本的な設定
 - a. [ロードバランサー名] に、ロードバランサーの名前を入力します。例えば、myglb。Gateway Load Balancer の名前は、リージョンのロードバランサーのセット内で一意 である必要があります。最大 32 文字で、英数字とハイフンのみを使用できます。先頭と末 尾にハイフンを使用することはできません。
 - b. [IP アドレスタイプ] で、[IPv4] を選択して IPv4 アドレスのみをサポートするか、[デュアル スタック] を選択して IPv4 と IPv6 アドレスの両方をサポートします。
- 6. ネットワークマッピング
 - a. [VPC] では、サービスプロバイダー VPC を選択します。
 - b. [Mappings] (マッピング) では、セキュリティアプライアンスインスタンスを起動したすべ てのアベイラビリティーゾーンと、対応するパブリックサブネットを選択します。
- 7. IP リスナーのルーティング
 - a. [デフォルトアクション] で、トラフィックを受信するターゲットグループを選択します。 ターゲットグループがない場合は、[ターゲットグループの作成] を選択します。詳細につい ては、「ターゲットグループの作成」を参照してください。
 - b. (オプション)[リスナータグ]を展開し、必要なタグを追加します。
- 8. (オプション) [ロードバランサータグ] を展開し、必要なタグを追加します。
- 9. 設定を確認し、[ロードバランサーの作成]を選択します。

重要な次のステップ

ロードバランサーを作成したら、EC2 インスタンスが最初のヘルスチェックに合格したかを検証し ます。ロードバランサーをテストするには、Gateway Load Balancer エンドポイントを作成し、ルー トテーブルを更新して Gateway Load Balancer エンドポイントをネクストホップにする必要があり ます。これらの設定は、Amazon VPC コンソールで設定します。詳細については、入門 のチュート リアルを参照してください。

Gateway Load Balancer の IP アドレスタイプを更新する

Gateway Load Balancer は、IPv4 アドレスのみを使用してロードバランサーと通信できるように設 定する、または IPv4 アドレスと IPv6 アドレスの両方 (デュアルスタック) を使用してロードバラン サーと通信できるように設定することができます。ロードバランサーは、ターゲットグループの IP アドレスのタイプに基づいてターゲットと通信します。詳細については、「<u>IP アドレスタイプ</u>」を 参照してください。

IP アドレスを更新するには、コンソールを使用して入力します。

- 1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
- 2. ナビゲーションペインの [ロードバランシング] で [ロードバランサー] を選択します。
- 3. ロードバランサーを選択します。
- 4. [Actions]、[Edit IP address type] を選択します。
- 5. [IP address type] で、[ipv4] を選択して IPv4 アドレスのみをサポートするか、[dualstack] を選 択して IPv4 と IPv6 アドレスの両方をサポートします。
- 6. [保存]を選択します。

を使用して IP アドレスタイプを更新するには AWS CLI

set-ip-address-type コマンドを使用します。

Gateway Load Balancer の属性を編集する

Gateway Load Balancer を作成したら、そのロードバランサー属性を編集できます。

ロードバランサーの属性

- 削除保護
- <u>クロスゾーンロードバランサー</u>

削除保護

Gateway Load Balancer が誤って削除されるのを防ぐため、削除保護を有効にできます。デフォルト では、削除保護は無効です。

Gateway Load Balancer の削除保護を有効にした場合、Gateway Load Balancer を削除する前に無効 にする必要があります。 コンソールを使用して削除保護を有効にするには

- 1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
- 2. ナビゲーションペインの [Load Balancing] で、[Load Balancers] を選択します。
- 3. Gateway Load Balancer を選択します。
- 4. [Actions] (アクション)、[Edit attributes] (属性の編集) を選択します。
- 5. [ロードバランサー属性の編集] ページで、[削除保護] の [有効] を選択し、[保存] を選択します。

コンソールを使用して削除保護を無効にするには

- 1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
- 2. ナビゲーションペインの [Load Balancing] で、[Load Balancers] を選択します。
- 3. Gateway Load Balancer を選択します。
- 4. [Actions] (アクション)、[Edit attributes] (属性の編集) を選択します。
- 5. [ロードバランサー属性の編集] ページで、[削除保護] の [有効] の選択を解除し、[保存] を選択し ます。

を使用して削除保護を有効または無効にするには AWS CLI

deletion_protection.enabled 属性を指定して <u>modify-load-balancer-attributes</u> コマンドを使用 します。

クロスゾーンロードバランサー

デフォルトでは、各ロードバランサーノードは、アベイラビリティーゾーン内の登録済みターゲット間でのみトラフィックを分散します。クロスゾーン負荷分散を有効にすると、各 Gateway Load Balancer ノードは、有効なすべてのアベイラビリティーゾーンの登録済みターゲットにトラフィックを分散します。詳細については、Elastic Load Balancing ユーザーガイドの<u>クロスゾーン負荷分</u> 散を参照してください。

コンソールを使用してクロスゾーン負荷分散を有効にするには

- 1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
- 2. ナビゲーションペインの [Load Balancing] で、[Load Balancers] を選択します。
- 3. Gateway Load Balancer を選択します。
- 4. [Actions] (アクション)、[Edit attributes] (属性の編集) を選択します。

5. [Edit load balancer attributes] (ロードバランサー属性の編集) ページで、[Cross-Zone Load Balancing] (クロスゾーン負荷分散) の [Enable] (有効) を選択し、[Save] (保存) を選択します。

を使用してクロスゾーン負荷分散を有効にするには AWS CLI

load_balancing.cross_zone.enabled 属性を指定して <u>modify-load-balancer-attributes</u> コマン ドを使用します。

Gateway Load Balancer のタグ付け

タグを使用すると、ロードバランサーを目的、所有者、環境などさまざまな方法で分類することがで きます。

各ロードバランサーに対して複数のタグを追加できます。タグキーは、各 Gateway Load Balancer で一意である必要があります。すでにロードバランサーに関連付けられているキーを持つタグを追加 すると、そのキーの値が更新されます。

タグが不要になったら、Gateway Load Balancer からタグを削除できます。

制限事項

- ・ リソースあたりのタグの最大数 50
- キーの最大長 127 文字 (Unicode)
- 値の最大長 255 文字 (Unicode)
- タグのキーと値は大文字と小文字が区別されます。使用できる文字は、UTF-8 で表現できる文字、スペース、および数字と、特殊文字 (+、-、=、.、_、:、/、@) です。ただし、先頭または未尾にはスペースを使用しないでください。
- タグ名または値に aws: プレフィックスを使用しないでください。このプレフィックスは AWS 使用のために予約されています。このプレフィックスが含まれるタグの名前または値は編集または削除できません。このプレフィックスを持つタグは、リソースあたりのタグ数の制限時には計算されません。

コンソールを使用して Gateway Load Balancer のタグを更新するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- 2. ナビゲーションペインの [Load Balancing] で、[Load Balancers] を選択します。
- 3. Gateway Load Balancer を選択します。

4. [Tags]、[Add/Edit Tags] を選択し、次のうち1つ以上を実行します。

- a. タグを更新するには、[Key] と [Value] の値を編集します。
- b. 新しいタグを追加するには、[Create Tag] を選択します。[キー] と [値] に値を入力します。
- c. タグを削除するには、タグの横にある削除アイコン (X)を選択します。
- 5. タグの更新を完了したら、[Save] を選択します。

を使用して Gateway Load Balancer のタグを更新するには AWS CLI

add-tags コマンドと remove-tags コマンドを使用します。

Gateway Load Balancer の削除

Gateway Load Balancer が利用可能になると、ロードバランサーの実行時間に応じて1時間ごと、 または1時間未満の時間について課金されます。不要になった Gateway Load Balancer は削除でき ます。Gateway Load Balancer が削除されると、Gateway Load Balancer の課金も停止されます。

別のサービスで使用中の Gateway Load Balancer は削除できません。例えば、Gateway Load Balancer が VPC エンドポイントサービスに関連付けられている場合、関連付けられた Gateway Load Balancer を削除するには、まずエンドポイントサービス設定を削除する必要があります。

Gateway Load Balancer を削除すると、そのリスナーも削除されます。Gateway Load Balancer を 削除しても、登録済みターゲットには影響を与えません。たとえば、EC2 インスタンスは実行を続 け、ターゲットグループに登録されたままです。ターゲットグループを削除するには、「<u>Gateway</u> Load Balancer のターゲットグループの削除」を参照してください。

コンソール を使用して Gateway Load Balancer を削除するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- 2. ナビゲーションペインの [Load Balancing] で、[Load Balancers] を選択します。
- 3. Gateway Load Balancer を選択します。
- 4. [Actions] で、[Delete] を選択します。
- 5. 確認を求めるメッセージが表示されたら、[Yes、Delete] を選択します。

を使用して Gateway Load Balancer を削除するには AWS CLI

delete-load-balancer コマンドを使用します。

Gateway Load Balancer のキャパシティ予約

ロードバランサーキャパシティーユニット (LCU) 予約では、ロードバランサーの静的最小キャパシ ティーを予約できます。Gateway Load Balancer は、検出されたワークロードをサポートし、容量の ニーズを満たすように自動的にスケーリングします。最小容量を設定すると、ロードバランサーは受 信したトラフィックに基づいてスケールアップまたはスケールダウンを続けますが、設定された最小 容量を下回ることも防止します。

以下の状況では LCU 予約の使用を検討してください。

- 突然の異常に高いトラフィックが発生し、イベント中にロードバランサーが突然のトラフィックス パイクをサポートできるようにしたいイベントが近づいています。
- ワークロードの性質上、短期間、予期しないスパイクトラフィックが発生している。
- 特定の開始時刻にサービスをオンボードまたは移行するようにロードバランサーを設定しており、
 自動スケーリングが有効になるのを待つのではなく、大容量から開始する必要があります。
- サービスレベルアグリーメントまたはコンプライアンス要件を満たすには、最小容量を維持する必要があります。
- ロードバランサー間でワークロードを移行していて、ソースのスケールに合わせて送信先を設定する場合。

必要な容量を見積もる

ロードバランサー用に予約する容量を決定するときは、負荷テストを実行するか、予想される今 後のトラフィックを表すワークロードの履歴データを確認することをお勧めします。Elastic Load Balancing コンソールを使用すると、レビューされたトラフィックに基づいて予約する必要がある容 量を見積もることができます。

または、CloudWatch メトリクス ProcessedBytes を参照して、適切な容量レベルを決定すること もできます。ロードバランサーの容量は LCUs で予約され、各 LCU は 2.2Mbps に等しくなりま す。PeakBytesPerSecond メトリクスを使用して、ロードバランサーの 1 分あたりのスループット トラフィックの最大数を表示し、そのスループットを LCUs に変換するには、2.2Mbps の変換レー トが 1 LCU になります。

参照するワークロードの履歴データがなく、負荷テストを実行できない場合は、LCU 予約計算ツー ルを使用して必要な容量を見積もることができます。LCU 予約計算ツールは、 AWS 観測された過 去のワークロードに基づいてデータを使用し、特定のワークロードを表していない場合があります。 詳細については、Load Balancerキャパシティユニット予約計算ツール」を参照してください。 LCU 予約のクォータ

アカウントには LCUs。詳細については、「<u>the section called "Load Balancerのキャパシティーユ</u> ニット"」を参照してください。

Gateway Load Balancer のLoad Balancerキャパシティユニット予約をリク エストする

LCU 予約を使用する前に、以下を確認してください。

- LCU 予約は、Gateway Load Balancer のスループットキャパシティの予約のみをサポートします。LCU 予約をリクエストするときは、1 LCUs の変換レートを使用して容量のニーズを Mbps から LCU に変換します。
- キャパシティはリージョンレベルで予約され、アベイラビリティーゾーン間で均等に分散されます。LCU予約を有効にする前に、各アベイラビリティーゾーンに十分に均等に分散されたター ゲットがあることを確認します。
- LCU 予約リクエストは先着順で受理され、その時点でゾーンで使用可能な容量によって異なります。通常、ほとんどのリクエストは1時間以内に受理されますが、最大数時間かかる場合があります。
- 既存の予約を更新するには、前のリクエストをプロビジョニングするか、失敗する必要があります。リザーブドキャパシティは必要な回数だけ増やすことができますが、リザーブドキャパシティは1日に2回しか減らせません。

LCU 予約をリクエストする

この手順のステップでは、ロードバランサーで LCU 予約をリクエストする方法について説明しま す。

コンソールを使用して LCU 予約をリクエストするには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- 2. ナビゲーションペインで、[ロードバランサー] を選択します。
- 3. ロードバランサー名を選択します。
- 4. キャパシティタブで、LCU 予約の編集を選択します。
- 5. 履歴参照ベースの見積りを選択し、ドロップダウンリストからロードバランサーを選択します。
- 6. 参照期間を選択して、推奨されるリザーブド LCU レベルを表示します。
- 過去のリファレンスワークロードがない場合は、手動見積りを選択し、予約する LCUsの数を入 力できます。
- 8. [保存]を選択します。

を使用して LCU 予約をリクエストするには AWS CLI

modify-capacity-reservation コマンドを使用します。

Gateway Load Balancer のLoad Balancerバランサーキャパシティユニット 予約を更新または終了する

LCU 予約を更新または終了する

この手順のステップでは、ロードバランサーの LCU 予約を更新または終了する方法について説明し ます。

コンソールを使用して LCU 予約を更新または終了するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- 2. ナビゲーションペインで、[ロードバランサー] を選択します。
- 3. ロードバランサー名を選択します。
- 4. キャパシティタブで、予約のステータスがプロビジョニングされていることを確認します。
 - a. LCU 予約を更新するには、LCU 予約の編集を選択します。
 - b. LCU 予約を終了するには、キャパシティのキャンセルを選択します。

を使用して LCU 予約を更新または終了するには AWS CLI

modify-capacity-reservation コマンドを使用します。

Gateway Load Balancer のLoad Balancerキャパシティユニットの予約をモ ニタリングする

予約ステータス

LCU 予約には 4 つのステータスがあります。

• 保留中 - プロビジョニング中の予約を示します。

プロビジョニング済み - リザーブドキャパシティーが使用可能であることを示します。

- failed その時点でリクエストを完了できないことを示します。
- ・ 再調整 アベイラビリティーゾーンが追加され、ロードバランサーが容量を再調整していることを示します。

リザーブド LCU

予約済み LCU 使用率を決定するには、1 分あたりの PeakBytesPerSecond メトリクスを 1 時間あた りの Sum(ReservedLCUs) と比較します。1 分あたりのバイト数を 1 時間あたりの LCU に変換する には、 (1 分あたりのバイト数)*8/60/ (10^6)/2.2 を使用します。

リザーブドキャパシティをモニタリングする

このプロセスのステップでは、ロードバランサーの LCU 予約のステータスを確認する方法について 説明します。

コンソールを使用して LCU 予約のステータスを表示するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- 2. ナビゲーションペインで、[ロードバランサー] を選択します。
- 3. ロードバランサー名を選択します。
- 4. キャパシティタブでは、予約ステータスとリザーブド LCU 値を表示できます。

を使用して LCU 予約のステータスをモニタリングするには AWS CLI

describe-capacity-reservation コマンドを使用します。

Gateway Load Balancer のリスナー

Gateway Load Balancer を作成するときに、リスナーを追加します。リスナーとは接続リクエストを チェックするプロセスです。

Gateway Load Balancer のリスナーは、すべてのポートですべての IP パケットをリッスンしま す。Gateway Load Balancer のリスナーを作成するときに、プロトコルまたはポートを指定すること はできません。

リスナーを作成するときは、ルーティングリクエストのルールを指定します。このルールは、指定さ れたターゲットグループにリクエストを転送します。リスナールールを更新して、リクエストを別の ターゲットグループに転送できます。

リスナー属性

Gateway Load Balancer のリスナー属性を以下に示します。

tcp.idle_timeout.seconds

TCP アイドルタイムアウト値 (秒単位)。有効な範囲は 60~6,000 秒です。デフォルト値は 350 秒です。

詳細については、「アイドルタイムアウトの更新」を参照してください。

Gateway Load Balancer のターゲットグループの更新

リスナーを作成するときは、ルーティングリクエストのルールを指定します。このルールは、指定さ れたターゲットグループにリクエストを転送します。リスナールールを更新して、リクエストを別の ターゲットグループに転送できます。

コンソールを使用してリスナーを更新するには

- 1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
- 2. ナビゲーションペインの [Load Balancing] で、[Load Balancers] を選択します。
- 3. ロードバランサーを選択し、[Listeners] を選択します。
- 4. [Edit listener] (リスナーの編集) を選択します。

- 5. [Forwarding to target group] (ターゲットグループに転送) で、ターゲットグループを選択します。
- 6. [Save]を選択します。

を使用してリスナーを更新するには AWS CLI

modify-listener コマンドを使用します。

Gateway Load Balancer リスナーの TCP アイドルタイムアウトの 更新

Gateway Load Balancer を通じて行う TCP リクエストごとに、その接続の状態が追跡されます。ア イドルタイムアウトよりも長い時間、クライアントからもターゲットからもその接続経由でデータ が送信されない場合、接続は閉じられます。TCP フローのデフォルトのアイドルタイムアウト値は 350 秒ですが、60~6,000 秒の任意の値に更新できます。

コンソールを使用して TCP アイドルタイムアウトを更新するには

- 1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
- 2. ナビゲーションペインの [Load Balancing] で、[Load Balancers] を選択します。
- 3. Gateway Load Balancer を選択します。
- 4. リスナータブで [アクション]、[リスナーの詳細を表示] を選択します。
- 5. リスナーの詳細ページの [属性] タブで [編集] を選択します。
- 6. [リスナー属性の編集] ページの [リスナー属性] セクションで [TCP アイドルタイムアウト] の値 を入力します。
- 7. [変更を保存]を選択します。

を使用して TCP アイドルタイムアウトを更新するには AWS CLI

tcp.idle_timeout.seconds 属性を指定して modify-listener-attributes コマンドを使用します。

Gateway Load Balancer のターゲットグループ

各ターゲットグループは、1 つ以上の登録されているターゲットにリクエストをルーティングするた めに使用されます。リスナーを作成するときは、デフォルトアクションのターゲットグループを指定 します。トラフィックは、リスナールールで指定されたターゲットグループに転送されます。さまざ まなタイプのリクエストに応じて別のターゲットグループを作成できます。

Gateway Load Balancer のヘルスチェック設定は、ターゲットグループ単位で定義します。各ター ゲットグループはデフォルトのヘルスチェック設定を使用します。ただし、ターゲットグループを作 成したときや、後で変更したときに上書きした場合を除きます。リスナールールでターゲットグルー プを指定すると、Gateway Load Balancer は、Gateway Load Balancer で有効なアベイラビリティー ゾーンにある、ターゲットグループに登録されたすべてのターゲットの状態を継続的にモニタリン グします。Gateway Load Balancer は、正常な登録済みターゲットにリクエストをルーティングしま す。詳細については、「<u>Gateway Load Balancer ターゲットグループのヘルスチェック</u>」を参照して ください。

目次

- ルーティング設定
- 対象タイプ
- 登録済みターゲット
- ターゲットグループの属性
- Gateway Load Balancer のターゲットグループの作成
- Gateway Load Balancer ターゲットグループのヘルスチェック
- Gateway Load Balancer のターゲットグループ属性を編集する
- Gateway Load Balancer のターゲットを登録する
- Gateway Load Balancer のターゲットグループのタグ付け
- Gateway Load Balancer のターゲットグループの削除

ルーティング設定

Gateway Load Balancer のターゲットグループは、次のプロトコルとポートをサポートします。

- ・ プロトコル: GENEVE
- ・ポート: 6081

Gateway Load Balancer は、GENEVE を使用して元のパケットをカプセル化します。GENEVE ヘッ ダーは、オプションクラス 0x0108 を使用して、Type-Length-Value (TLV) 形式を使用して情報を保 存します。アプライアンスは、元のパケットを処理するために TLV ペアをカプセル化解除する必要 があります。詳細については、次のブログ記事<u>「アプライアンスを Gateway Load Balancer と統合</u> する」を参照してください。

対象タイプ

ターゲットグループを作成するときは、そのターゲットの種類を指定します。ターゲットの種類は、 ターゲットの指定方法を決定します。ターゲットグループを作成した後で、ターゲットの種類を変更 することはできません。

可能なターゲットの種類は次のとおりです。

instance

インスタンス ID で指定されたターゲット。

ip

IP アドレスで指定されたターゲット。

ターゲットの種類が ip の場合、次のいずれかの CIDR ブロックから IP アドレスを指定できます。

- ターゲットグループの VPC のサブネット
- 10.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

A Important

パブリックにルーティング可能な IP アドレスは指定できません。

登録済みターゲット

Gateway Load Balancer は、クライアントにとって単一の通信先として機能し、正常な登録済みター ゲットに受信トラフィックを分散します。各ターゲットグループでは、Gateway Load Balancer が有 効になっている各アベイラビリティーゾーンで少なくとも1つのターゲットが登録されている必要 があります。各ターゲットは、1つ以上のターゲットグループに登録できます。

需要が高まった場合、需要に対処するため、1 つまたは複数のターゲット グループに追加のター ゲットを登録できます。Gateway Load Balancer は、登録プロセスが完了するとすぐに、新しく登録 したターゲットへのトラフィックのルーティングを開始します。

需要が低下した場合や、ターゲットを保守する必要がある場合、ターゲットグループからターゲット を登録解除することができます。ターゲットを登録解除するとターゲットグループから削除されます が、ターゲットにそれ以外の影響は及びません。登録解除するとすぐに、Gateway Load Balancer は ターゲットへのトラフィックのルーティングを停止します。ターゲットは、未処理のリクエストが完 了するまで draining 状態になります。トラフィックの受信を再開する準備ができると、ターゲッ トをターゲットグループに再度登録することができます。

ターゲットグループの属性

ターゲットグループでは次の属性を使用できます。

deregistration_delay.timeout_seconds

登録解除するターゲットの状態が draining から unused に変わるのを Elastic Load Balancing が待機する時間。範囲は 0 ~ 3600 秒です。デフォルト値は 300 秒です。

stickiness.enabled

設定可能なフローの維持がターゲットグループで有効化されているかどうかを示します。使用で きる値は、true または false です。デフォルトは False です。属性が false に設定されてい る場合、5 tuple が使用されます。

stickiness.type

フローの維持設定タイプを示します。Gateway Load Balancers に関連付けられているターゲット グループに指定できる値は次のとおりです。

- source_ip_dest_ip
- source_ip_dest_ip_proto

target_failover.on_deregistration

ターゲットの登録が解除されたときに、Gateway Load Balancer が既存のフ ローをどのように処理するかを示します。指定できる値は rebalance およ び no_rebalance です。デフォルトは no_rebalance です。2 つの属性 (target_failover.on_deregistrationとtarget_failover.on_unhealthy)を個別に 設定することはできません。両方の属性に設定する値は同じである必要があります。

target_failover.on_unhealthy

ターゲットに異常がある場合に、Gateway Load Balancer が既存のフロー をどのように処理するかを示します。指定できる値は rebalance およ び no_rebalance です。デフォルトは no_rebalance です。2 つの属性 (target_failover.on_deregistrationとtarget_failover.on_unhealthy) を個別に 設定することはできません。両方の属性に設定する値は同じである必要があります。

詳細については、「ターゲットグループ属性を編集する」を参照してください。

Gateway Load Balancer のターゲットグループの作成

ターゲットグループを使用して、Gateway Load Balancer のターゲットを登録します。

トラフィックをターゲットグループ内のターゲットにルーティングするには、リスナーを作成し、リ スナーのデフォルトアクションでターゲットグループを指定します。詳細については、「<u>リスナー</u>」 を参照してください。

ターゲットグループのタグはいつでも追加または削除できます。詳細については、「<u>ターゲットの登</u> 録」を参照してください。ターゲットグループのヘルスチェック設定を変更することもできます。詳 細については、「ヘルスチェックの設定の変更」を参照してください。

コンソールを使用してターゲットグループを作成するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- 2. ナビゲーションペインの [ロードバランシング] で [ターゲットグループ] を選択します。
- 3. [Create target group] を選択します。
- 基本的な設定

- a. [Choose a target type] (ターゲットタイプの選択) で、[Instances] (インスタンス) を選択し てインスタンス ID でターゲットを指定するか、[IP addresses] (IP アドレス) を選択して IP アドレスでターゲットを指定します。
- b. [ターゲットグループ名]に、ターゲットグループの名前を入力します。この名前はリージョンごと、アカウントごとに一意である必要があり、最大 32 文字の英数字またはハイフンのみを使用する必要があり、先頭と末尾にハイフンを使用することはできません。
- c. [プロトコル] が GENEVE であること、および [ポート] が 6081 であることを確認します。 その他のプロトコルとポートはサポートされていません。
- d. [VPC] で、ターゲットグループに含めるセキュリティアプライアンスインスタンスがある仮
 想プライベートクラウド (VPC) を選択します。
- (オプション) [ヘルスチェック] で、必要に応じて設定と詳細設定を変更します。ヘルスチェックが [異常なしきい値] のカウントを連続して超えると、ロードバランサーはターゲットを停止中の状態にします。ヘルスチェックが [正常なしきい値] のカウントを連続して超えると、ロードバランサーはターゲットを稼働状態に戻します。詳細については、「Gateway Load Balancer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。
- 6. (オプション) [タグ] を展開し、必要なタグを追加します。
- 7. [次へ]を選択します。
- 8. [ターゲットの登録] で、次のように 1 つ以上のターゲットを追加します。
 - ターゲットタイプがインスタンスである場合は、1つ以上のインスタンスを選択し、1つ以上のポートを入力して、[保留中として以下を含める]を選択します。
 - ターゲットタイプが IP アドレスの場合は、ネットワークを選択し、IP アドレスとポートを 入力して、[保留中として以下を含める]を選択します。
- 9. [Create target group] を選択します。

を使用してターゲットグループを作成するには AWS CLI

ターゲットグループを作成するには <u>create-target-group</u> コマンド、ターゲットグループにタグを付けるには <u>add-tags</u> コマンド、ターゲットを追加するには <u>register-targets</u> コマンドを使用します。

Gateway Load Balancer ターゲットグループのヘルスチェック

ターゲットを1つ以上のターゲットグループに登録します。登録プロセスが完了するとすぐ に、Gateway Load Balancer は新たに登録されたターゲットへのトラフィックのルーティングを開始 します。登録プロセスが完了し、ヘルスチェックが開始されるまで数分かかることがあります。 Gateway Load Balancer は、登録された各ターゲットに定期的にリクエストを送信してそのステータ スを確認します。各ヘルスチェックが完了すると、Gateway Load Balancer はヘルスチェック用に確 立された接続を終了します。

ヘルスチェックの設定

以下の設定を使用して、ターゲットグループのターゲットのアクティブなヘルスチェックを設定 します。ヘルスチェックが UnhealthyThresholdCount 連続失敗数として指定された値を超える と、Gateway Load Balancer はターゲットをサービス停止中の状態にします。ヘルスチェックが HealthyThresholdCount 連続成功数として指定された値を超えると、Gateway Load Balancer はター ゲットを実行中の状態に戻します。

設定	説明
HealthCheckProtocol	ターゲットに対してヘルスチェックを実行す るときにロードバランサーで使用するプロトコ ル。使用可能なプロトコルは HTTP、HTTPS、お よび TCP です。デフォルトは TCP です。
HealthCheckPort	ターゲットでヘルスチェックを実行するときに Gateway Load Balancer が使用するポート。範 囲は1~ 65535 です。デフォルトは 80 です。
HealthCheckPath	[HTTP/HTTPS ヘルスチェック] ヘルスチェッ クのターゲットの送信先であるヘルスチェック パス。デフォルトは / です。
HealthCheckTimeoutSeconds	ヘルスチェックを失敗と見なす、ターゲットか らレスポンスがない時間 (秒単位)。範囲は2~ 120 です。デフォルトは5です。
HealthCheckIntervalSeconds	個々のターゲットのヘルスチェックの概算間隔 (秒単位)。範囲は 5 ~ 300 です。デフォルト値 は 10 秒です。この値は、HealthCheckTimeout Seconds 以上にする必要があります。

設定	説明
	▲ Important Gateway Load Balancer のヘルス チェックは分散され、コンセンサスメ カニズムを使用してターゲットのヘル スを判断します。このため、ターゲッ トアプライアンスでは、設定された時 間間隔内に複数のヘルスチェックを受 け取ることが考えられます。
HealthyThresholdCount	非正常なインスタンスが正常であると見なすま でに必要なヘルスチェックの連続成功回数。範 囲は 2~10 です。デフォルトは 5 です。
UnhealthyThresholdCount	非正常なインスタンスが非正常であると見なす までに必要なヘルスチェックの連続失敗回数。 範囲は 2~10 です。デフォルトは 2 です。
マッチャー	[HTTP/HTTPS ヘルスチェック] ターゲットか らの正常なレスポンスを確認するために使用す る HTTP コード。この値は、200 ~ 399 であ る必要があります。

ターゲットヘルスステータス

Gateway Load Balancer がターゲットにヘルスチェックリクエストを送信する前に、ターゲットグ ループに登録し、リスナールールでターゲットグループを指定して、ターゲットのアベイラビリ ティーゾーンがロードバランサーに対して有効になっていることを確認する必要があります。

次の表は、登録されたターゲットのヘルスステータスの可能値を示しています。

值	説明
initial	Gateway Load Balancer は、ターゲットを登録中か、 ターゲットで最初のヘルスチェックを実行中です。

值	説明	
	関連する理由コード:Elb.RegistrationIn Progress Elb.InitialHealthChecking	
healthy	ターゲットは正常です。	
	関連する理由コード:なし	
unhealthy	ターゲットはヘルスチェックに応答しなかったか、ヘル スチェックに合格しませんでした。	
	関連する理由コード : Target.FailedHealt hChecks	
unused	ターゲットがターゲットグループに登録されていない か、ターゲットグループがロードバランサーのリスナー ルールで使用されていないか、ロードバランサーに対し て有効ではないアベイラビリティーゾーンにターゲット があるか、ターゲットが停止または終了状態にありま す。 関連する理由コード:Target.NotRegistered Target.NotInUse Target.InvalidState Target.IpUnusable	
draining	ターゲットは登録解除中で、Connection Draining 中で す。	
	関連する理由コード:Target.Deregistrat ionInProgress	
unavailable	ターゲットヘルスは使用できません。	
	関連する理由コード:Elb.InternalError	

ヘルスチェックの理由コード

ターゲットのステータスが Healthy 以外の値の場合、API は問題の理由コードと説明を返し、コンソールで同じ説明が表示されます。Elb で始まる理由コードは Gateway Load Balancer 側で発生し、Target で始まる理由コードはターゲット側で発生します。

理由コード	説明
Elb.InitialHealthChecking	最初のヘルスチェックが進行中です
Elb.InternalError	内部エラーのため、ヘルスチェックに失敗しました
Elb.RegistrationIn Progress	ターゲットの登録中です
Target.Deregistrat ionInProgress	ターゲットの登録解除中です
Target.FailedHealthChecks	ヘルスチェックに失敗しました
Target.InvalidState	ターゲットが停止状態にあります
	ターゲットは終了状態にあります
	ターゲットは終了状態か、または停止状態にあります
	ターゲットは無効な状態にあります
Target.IpUnusable	IP アドレスはロードバランサーによって使用されている ので、ターゲットとして使用できません
Target.NotInUse	ターゲットグループは、Gateway Load Balancer からト ラフィックを受信するように設定されていません
	Gateway Load Balancer が有効になっていないアベイラ ビリティーゾーンにターゲットがあります
Target.NotRegistered	ターゲットはターゲットグループに登録されていません

Gateway Load Balancer ターゲット障害シナリオ

既存のフロー: デフォルトでは、ターゲットのヘルスや登録のステータスにかかわらず、フローがタ イムアウトまたはリセットされない限り、既存のフローは常に同じターゲットに移動します。この アプローチにより、Connection Draining が容易になります。また、CPU 使用率が高いため、ヘルス チェックに応答できないことがあるサードパーティーのファイアウォールに対応できます。詳細につ いては、「Target failover」を参照してください。

新しいフロー: 新しいフローが正常なターゲットに送信されます。フローのロードバランシングの決 定が行われると、Gateway Load Balancer は、そのターゲットが異常になったり、他のターゲットが 正常になったりした場合でも、同じターゲットにフローを送信します。

すべてのターゲットが異常な場合、Gateway Load Balancer はターゲットをランダムに選択し、リ セットされるかタイムアウトするまで、フローの存続期間中、そのターゲットにトラフィックを転送 します。トラフィックは異常なターゲットに転送されるため、トラフィックはそのターゲットが再び 正常になるまでドロップされます。

TLS 1.3: ターゲットグループが HTTPS ヘルスチェックで構成されている場合、登録されたターゲットが TLS 1.3 のみをサポートしている場合にはそのターゲットはヘルスチェックに失敗します。これらのターゲットは、TLS 1.2 などの以前のバージョンの TLS をサポートしている必要があります。

クロスゾーン負荷分散: デフォルトでは、アベイラビリティーゾーン間のロードバランシングは無 効になっています。ゾーン間のロードバランシングが有効になっている場合、各 Gateway Load Balancer はすべてのアベイラビリティーゾーン内のすべてのターゲットを認識でき、ゾーンに関係 なく、それらはすべて同じように処理されます。

ロードバランシングとヘルスチェックの決定は、ゾーン間で常に独立しています。ゾーン間のロード バランシングが有効になっている場合でも、既存のフローと新しいフローの動作は上記と同じです。 詳細については、Elastic Load Balancing ユーザーガイドの<u>クロスゾーン負荷分散</u>を参照してくださ い。

ターゲットのヘルスステータスをチェックする

ターゲットグループに登録されたターゲットのヘルスステータスをチェックできます。

コンソールを使用してターゲットのヘルスステータスをチェックするには

- 1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
- 2. ナビゲーションペインの [ロードバランシング] で [ターゲットグループ] を選択します。

- 3. ターゲットグループの名前を選択して、その詳細ページを開きます。
- 4. [ターゲット] タブの [ステータス] 列は、各ターゲットのステータスを示します。
- 5. ターゲットのステータスの値が Healthy 以外の場合は、[ステータスの詳細] 列に詳細情報が表示されます。

を使用してターゲットの状態を確認するには AWS CLI

<u>describe-target-health</u> コマンドを使用します。このコマンドの出力にはターゲットのヘルス状態が含 まれます。ステータスの値が Healthy 以外の場合は、理由コードも含まれています。

異常なターゲットに関する E メール通知を受信するには

CloudWatch アラームを使用して、異常なターゲットに関する詳細を送信する Lambda 関数をトリ ガーします。ステップバイステップの手順については、ブログ投稿「<u>ロードバランサーの異常なター</u> ゲットを特定する」を参照してください。

ヘルスチェックの設定の変更

ターゲットグループのヘルスチェック設定の一部を変更できます。

コンソールを使用してターゲットグループのヘルスチェック設定を変更するには

- 1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
- 2. ナビゲーションペインの [ロードバランシング] で [ターゲットグループ] を選択します。
- 3. ターゲットグループの名前を選択して、その詳細ページを開きます。
- 4. [グループの詳細] タブの [ヘルスチェックの設定] セクションで、[編集] を選択します。
- 5. [ヘルスチェックの編集の設定] ページで、必要に応じて設定を変更し、[変更内容の保存] を選択 します。

を使用してターゲットグループのヘルスチェック設定を変更するには AWS CLI

modify-target-group コマンドを使用します。

Gateway Load Balancer のターゲットグループ属性を編集する

Gateway Load Balancer のターゲットグループを作成したら、そのターゲットグループ属性を編集できます。

ターゲットグループの属性

- ターゲットフェイルオーバー
- 登録解除の遅延
- フローの維持設定

ターゲットフェイルオーバー

ターゲットフェイルオーバーでは、ターゲットに異常が発生したとき、またはターゲットの登録が解除されたときに、Gateway Load Balancer が既存のトラフィックフローをどのように処理するかを指定します。デフォルトでは、Gateway Load Balancer は、ターゲットに障害が発生した場合や登録が解除された場合でも既存のフローを同じターゲットに引き続き送信します。これらのフローは、再ハッシュする (rebalance) か、デフォルト状態のままにする (no_rebalance) ことで管理できます。

再分散なし:

Gateway Load Balancer は、障害が発生したターゲットまたはドレインされたターゲットに既存 のフローを引き続き送信します。Gateway Load Balancer がターゲットに到達できない場合、ト ラフィックは削除されます。

ただし、新しいフローは正常なターゲットに送信されます。これがデフォルトの動作です。 再分散:

Gateway Load Balancer は既存のフローを再ハッシュし、登録解除遅延タイムアウト後に正常な ターゲットに送信します。

登録解除されたターゲットの場合、フェイルオーバーまでの最小時間は登録解除の遅延に応じて 異なります。ターゲットは、登録解除の遅延が完了するまで登録解除済みとしてマークされませ ん。

異常のあるターゲットの場合、フェイルオーバーまでの最小時間は、ターゲットグループのヘル スチェック設定 (間隔時間のしきい値) に応じて異なります。これは、ターゲットが異常としてフ ラグが設定されるまでの最小時間です。この時間が過ぎると、Gateway Load Balancer が正常な ターゲットに新しいフローを再ルーティングするまでに、追加の伝播時間と TCP 再送信バック オフのために数分かかる場合があります。 コンソールを使用してターゲットフェイルオーバー属性を更新するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- 2. ナビゲーションペインの [Load Balancing (ロードバランシング)] で [Target Groups (ターゲットグループ)]を選択します。
- 3. ターゲットグループの名前を選択して、その詳細ページを開きます。
- 4. [グループの詳細] ページの [属性] セクションで、[編集] を選択します。
- 5. [属性の編集] ページで [ターゲットフェイルオーバー] の値を変更します。
- 6. [Save changes] (変更の保存) をクリックします。

を使用してターゲットフェイルオーバー属性を更新するには AWS CLI

次のキーと値のペアで modify-target-group-attributes コマンドを使用します。

- キー = target_failover.on_deregistration および値 = no_rebalance (デフォルト) また は rebalance
- キー = target_failover.on_unhealthy および値 = no_rebalance (デフォルト) または rebalance

Note

両方の属性 (target_failover.on_deregistration と target_failover.on_unhealthy) は同じ値である必要があります。

登録解除の遅延

ターゲットの登録を解除すると、Gateway Load Balancer は、そのターゲットへのフローを次のよう に管理します。

新しいフロー

Gateway Load Balancer は、新しいフローの送信を停止します。 既存のフロー

Gateway Load Balancer は、プロトコルに基づいて既存のフローを処理します。

• TCP: 350 秒以上アイドル状態の場合、既存のフローは閉じられます。

• その他のプロトコル: 120 秒以上アイドル状態の場合、既存のフローは閉じられます。

既存のフローをドレインするために、ターゲットグループのフロー再分散を有効にすることができま す。詳細については、「the section called "ターゲットフェイルオーバー"」を参照してください。

登録解除されたターゲットは、タイムアウトが期限切れになるまで、draining 状態であることを 示します。登録解除遅延のタイムアウトの期限が切れると、ターゲットは unused 状態に移行しま す。

コンソールを使用して登録解除の遅延属性を更新するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- 2. ナビゲーションペインの [Load Balancing (ロードバランシング)] で [Target Groups (ターゲットグループ)] を選択します。
- 3. ターゲットグループの名前を選択して、その詳細ページを開きます。
- 4. [グループの詳細] ページの [属性] セクションで、[編集] を選択します。
- 5. [属性の編集]ページで、必要に応じて [登録解除の遅延]の値を変更します。
- 6. [Save changes] (変更の保存) をクリックします。

を使用して登録解除遅延属性を更新するには AWS CLI

modify-target-group-attributes コマンドを使用します。

フローの維持設定

デフォルトでは、Gateway Load Balancer は 5 タプルを使用して、特定のターゲットアプライアン スへのフローの持続性を維持します (TCP/UDP フローの場合)。5 タプルには、送信元 IP、送信元 ポート、送信先 IP、送信先ポート、およびトランスポートプロトコルが含まれます。維持の種類属 性を使用してデフォルト (5 タプル) を変更し、3 タプル (送信元 IP、送信先 IP、トランスポートプロ トコル)または 2 タプル (送信元 IP と送信先 IP) を選択できます。

フローの維持設定に関する考慮事項

- フローの維持設定はターゲットグループレベルで設定および適用され、ターゲットグループに送信 されるすべてのトラフィックに適用されます。
- 2 タプルおよび 3 タプルのフローの維持は、AWS Transit Gateway アプライアンスモード が有効な場合はサポートされません。でアプライアンスモードを使用するには AWS Transit Gateway、Gateway Load Balancer で 5 タプルフローの維持を使用します。

 フローの維持設定では接続とフローの分散が不均一になり、ターゲットの可用性に影響することが あります。ターゲットグループの維持タイプを変更する前に、既存のすべてのフローを終了または ドレインすることをお勧めします。

コンソールを使用してフローの維持属性を更新するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- 2. ナビゲーションペインの [Load Balancing (ロードバランシング)] で [Target Groups (ターゲットグループ)] を選択します。
- 3. ターゲットグループの名前を選択して、その詳細ページを開きます。
- 4. [グループの詳細] ページの [属性] セクションで、[編集] を選択します。
- 5. [属性の編集] ページで [維持設定] の値を変更します。
- 6. [Save changes] (変更の保存) をクリックします。

を使用してフロー維持属性を更新するには AWS CLI

stickiness.enabled および stickiness.type のターゲットグループ属性を指定して <u>modify-</u> target-group-attributes コマンドを使用します。

Gateway Load Balancer のターゲットを登録する

ターゲットがリクエストを処理する準備ができたら、そのターゲットを1つ以上のターゲットグ ループに登録します。インスタンス ID または IP アドレスでターゲットを登録できます。登録処理 が完了し、ターゲットが最初のヘルスチェックに合格するとすぐに、Gateway Load Balancer はター ゲットへのリクエストのルーティングを開始します。登録プロセスが完了し、ヘルスチェックが開 始されるまで数分かかることがあります。詳細については、「<u>Gateway Load Balancer ターゲットグ</u> ループのヘルスチェック」を参照してください。

現在登録されているターゲットの需要が上昇した場合、需要に対応するために追加ターゲットを登録 できます。登録されたターゲットの需要が減少した場合は、ターゲットグループからターゲットの登 録を解除できます。登録解除プロセスが完了し、Gateway Load Balancer がターゲットへのリクエス トのルーティングを停止するまで数分かかることがあります。その後需要が増加した場合は、登録解 除したターゲットをターゲットグループに再度登録できます。ターゲットをサービスする必要がある 場合は、そのターゲットを登録解除し、サービスの完了時に再度登録できます。

内容

- 考慮事項
- ターゲットセキュリティグループ
- ・ ネットワーク ACL
- インスタンス ID によるターゲットの登録
- IP アドレスによるターゲットの登録
- ターゲットの登録解除

考慮事項

- 各ターゲットグループでは、Gateway Load Balancer が有効になっている各アベイラビリティー ゾーンで少なくとも1つのターゲットが登録されている必要があります。
- ターゲットグループのターゲットの種類により、ターゲットグループにターゲットを登録する方法 が決定されます。詳細については、「対象タイプ」を参照してください。
- リージョン間 VPC ピアリング全体でターゲットを登録することはできません。
- リージョン内 VPC ピアリング全体でインスタンス ID でインスタンスを登録することはできませんが、IP アドレスで登録することはできます。

ターゲットセキュリティグループ

EC2 インスタンスをターゲットとして登録する場合は、これらのインスタンスのセキュリティグ ループのインバウンドトラフィックとアウトバウンドトラフィックがポート 6081 で許可されている ことを確認する必要があります。

Gateway Load Balancer には関連付けられたセキュリティグループがありません。したがって、ター ゲットのセキュリティグループは、ロードバランサーからのトラフィックを許可するために IP アド レスを使用する必要があります。

ネットワーク ACL

EC2 インスタンスをターゲットとして登録する場合は、インスタンスのサブネットのアクセスコン トロールリスト (ACL) をチェックして、ポート 6081 でトラフィックを許可していることを確認する 必要があります。VPC のデフォルトのネットワーク ACL では、すべてのインバウンドトラフィック とアウトバウンドトラフィックを許可します。カスタムネットワーク ACL を作成する場合は、適切 なトラフィックを許可していることを確認してください。

インスタンス ID によるターゲットの登録

インスタンスの登録時の状態は running である必要があります。

コンソールを使用してインスタンス ID でターゲットを登録するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- ナビゲーションペインの [Load Balancing (ロードバランシング)]で [Target Groups (ターゲットグループ)]を選択します。
- 3. ターゲットグループの名前を選択して、その詳細ページを開きます。
- 4. [ターゲット] タブで、[ターゲットの登録] を選択します。
- 5. インスタンスを選択し、[保留中として以下を含める]を選択します。
- 6. インスタンスの追加が完了したら、[保留中のターゲットの登録]を選択します。

を使用してインスタンス ID でターゲットを登録するには AWS CLI

インスタンスの ID で register-targets コマンドを使用します。

IP アドレスによるターゲットの登録

登録する IP アドレスは、次のいずれかの CIDR ブロックからのものである必要があります。

- ターゲットグループの VPC のサブネット
- 10.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

コンソールを使用して IP アドレスでターゲットを登録するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- ナビゲーションペインの [Load Balancing (ロードバランシング)]で [Target Groups (ターゲットグループ)]を選択します。
- 3. ターゲットグループの名前を選択して、その詳細ページを開きます。
- 4. [ターゲット] タブで、[ターゲットの登録] を選択します。

5. ネットワーク、IP アドレス、ポートを選択し、[保留中として以下を含める] を選択します。

6. アドレスの指定が終了したら、[保留中のターゲットの登録]を選択します。

を使用して IP アドレスでターゲットを登録するには AWS CLI

register-targets コマンドをターゲットの IP アドレスとともに使用します。

ターゲットの登録解除

ターゲットを登録解除すると、Elastic Load Balancing は未処理のリクエストが完了するまで待機し ます。これは、Connection Drainingと呼ばれます。Connection Drainingの進行中、ターゲットのス テータスは draining です。登録解除が完了すると、ターゲットのステータスは unused に変わり ます。詳細については、「登録解除の遅延」を参照してください。

コンソールを使用してターゲットを登録解除するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- ナビゲーションペインの [Load Balancing (ロードバランシング)]で [Target Groups (ターゲットグループ)]を選択します。
- 3. ターゲットグループの名前を選択して、その詳細ページを開きます。
- 4. [Targets] タブを選択します。
- 5. ターゲットを選択し、[登録解除]を選択します。

を使用してターゲットの登録を解除するには AWS CLI

deregister-targets コマンドを使用して、ターゲットを削除します。

Gateway Load Balancer のターゲットグループのタグ付け

タグを使用すると、ターゲットグループを目的、所有者、環境などさまざまな方法で分類することが できます。

各ターゲットグループに対して複数のタグを追加できます。タグキーは、各ターゲットグループで一 意である必要があります。すでにターゲットグループに関連付けられているキーを持つタグを追加す ると、そのキーの値が更新されます。

不要になったタグは、削除することができます。

制限事項

- ・ リソースあたりのタグの最大数 50
- キーの最大長 127 文字 (Unicode)
- 値の最大長 255 文字 (Unicode)
- タグのキーと値は大文字と小文字が区別されます。使用できる文字は、UTF-8 で表現できる文字、スペース、および数字と、特殊文字 (+、-、=、.、_、:、/、@) です。ただし、先頭または末尾にはスペースを使用しないでください。
- タグ名または値に aws: プレフィックスを使用しないでください。このプレフィックスは AWS 使用のために予約されています。このプレフィックスが含まれるタグの名前または値は編集または削除できません。このプレフィックスを持つタグは、リソースあたりのタグ数の制限時には計算されません。

コンソールを使用してターゲットグループのタグを更新するには

- 1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
- 2. ナビゲーションペインの [Load Balancing (ロードバランシング)] で [Target Groups (ターゲットグループ)]を選択します。
- 3. ターゲットグループの名前を選択して、その詳細ページを開きます。
- 4. [タグ] タブで、[タグの管理] を選択し、次の1つ以上の操作を行います。
 - a. タグを更新するには、[キー] と [値] に新しい値を入力します。
 - b. タグを追加するには、[タグの追加]を選択し、[キー] と [値] に値を入力します。
 - c. タグを削除するには、タグの横にある [削除] を選択します。
- 5. タグの更新を完了したら、[変更内容の保存]を選択します。

を使用してターゲットグループのタグを更新するには AWS CLI

add-tags コマンドと remove-tags コマンドを使用します。

Gateway Load Balancer のターゲットグループの削除

ターゲットグループがリスナールールの転送アクションによって参照されていない場合は、これを削除できます。ターゲットグループを削除しても、ターゲットグループに登録されたターゲットには影響が及びません。登録済み EC2 インスタンスが必要なくなった場合は停止または終了できます。

コンソールを使用してターゲットグループを削除するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- 2. ナビゲーションペインの [ロードバランシング] で [ターゲットグループ] を選択します。
- 3. ターゲットグループを選択し、[Actions]、[Delete] を選択します。
- 4. 確認を求めるメッセージが表示されたら、[はい、削除します]を選択します。

を使用してターゲットグループを削除するには AWS CLI

delete-target-group コマンドを使用します。

Gateway Load Balancer のモニタリング

次の機能を使用して、Gateway Load Balancer のモニタリング、トラフィックパターンの分析、問題 の解決を行えます。ただし、Gateway Load Balancer はフローを終了しない透過レイヤー 3 のロー ドバランサーであるため、アクセスログは生成されません。アクセスログを受信するには、ファイア ウォール、IDS/IPS、セキュリティアプライアンスなど、Gateway Load Balancer ターゲットアプラ イアンスでアクセスログを有効にする必要があります。さらに、Gateway Load Balancer で VPC フ ローログを有効にすることもできます。

CloudWatch メトリクス

Amazon CloudWatch を使用して、Gateway Load Balancer とターゲットのデータポイントに関 する統計情報を、メトリクスと呼ばれる時系列データの時間順のセットとして取得できます。こ れらのメトリクスを使用して、システムが正常に実行されていることを確認できます。詳細につ いては、「<u>Gateway Load Balancer の CloudWatch メトリクス</u>」を参照してください。

VPC フローログ

VPC フローログを使用して、Gateway Load Balancer との間で送受信されるトラフィックに関 する詳細情報を取得できます。詳細については、Amazon VPC ユーザーガイドの <u>VPC フローロ</u> グを参照してください。

Gateway Load Balancer の各ネットワークインターフェイスのフローログを作成します。サブ ネットあたり 1 つのネットワークインターフェイスがあります。Gateway Load Balancer のネッ トワークインターフェイスを特定するには、ネットワークインターフェイスの説明フィールドで Gateway Load Balancer の名前を探します。

Gateway Load Balancer を通じて、各接続に2つのエントリがあります。1つはクライアントと Gateway Load Balancer 間のフロントエンド接続で、もう1つは Gateway Load Balancer とター ゲットとの間のバックエンド接続です。ターゲットがインスタンス ID で登録されている場合、 接続はクライアントからの接続としてインスタンスに表示されます。インスタンスのセキュリ ティグループで、クライアントからの接続が許可されないが、サブネットのネットワーク ACL で許可される場合、Gateway Load Balancer のネットワークインターフェイスのログにはフロン トエンドおよびバックエンド接続に対して「ACCEPT OK」と表示され、インスタンスのネット ワークインターフェイスのログには接続に対して「REJECT OK」と表示されます。

CloudTrail ログ

AWS CloudTrail を使用して、Elastic Load Balancing API に対する呼び出しに関する詳細情報を キャプチャし、ログファイルとして Amazon S3 に保存できます。これらの CloudTrail ログを使 用して、行われた呼び出し、呼び出し元のソース IP アドレス、呼び出し元、呼び出し時間などを 判断できます。詳細については、「<u>Log API calls for Elastic Load Balancing using CloudTrail</u>」を 参照してください。

Gateway Load Balancer の CloudWatch メトリクス

Elastic Load Balancing は、Gateway Load Balancer とターゲットのデータポイントを Amazon CloudWatch に発行します。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、指定 した期間中の Gateway Load Balancer の正常なターゲットの合計数をモニタリングすることができ ます。各データポイントには、タイムスタンプと、オプションの測定単位が関連付けられています。

メトリクスを使用して、システムが正常に実行されていることを確認できます。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モニタリング し、アクション (E メールアドレスに通知を送信するなど) を開始することができます。

Elastic Load Balancing は、Gateway Load Balancer 経由でリクエストが伝達される場合にのみ、 メトリクスを CloudWatch にレポートします。経由するリクエストがある場合、Elastic Load Balancing は 60 秒間隔でメトリクスを測定し、送信します。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

- Gateway Load Balancer のメトリクス
- Gateway Load Balancer のメトリクスディメンション
- Gateway Load Balancer の CloudWatch メトリクスの表示

Gateway Load Balancer のメトリクス

AWS/GatewayELB 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	クライアントからターゲットへの同時フロー (または接続) の合計 数。

メトリクス	説明		
	レポート条件: ゼロ以外の値がある		
	統計値:最も有用な統計値は Average、Maximum、および Minimum です。		
	ディメンション		
	LoadBalancerAvailabilityZone ,LoadBalancer		
ConsumedLCUs	ロードバランサーが使用するロードバランサーキャパシティーユ ニット (LCU) の数です。1 時間当たりで使用する LCU 数の料金をお 支払いいただきます。 詳細については、 <u>Elastic Load Balancing の料</u> <u>金表</u> を参照してください。		
	レポート条件: 常に報告される		
	統計: All		
	ディメンション		
	• LoadBalancer		
HealthyHostCount	正常と見なされるターゲットの数。		
	レポート条件: ヘルスチェックが有効になっている場合にレポートさ れます		
	統計値: 最も有用な統計値は Maximum および Minimum です。		
	ディメンション		
	LoadBalancer , TargetGroupAvailabilityZone , LoadBalancer , TargetGroup		

メトリクス	説明	
NewFlowCount	期間内にクライアントからターゲットに確立された新しいフロー (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: 最も有用な統計は Sum です。	
	ディメンション	
	• LoadBalancer	
	 AvailabilityZone ,LoadBalancer 	
PeakBytesPerSecond	サンプリングウィンドウ中に 10 秒ごとに計算される、1 秒あたりに 処理される最大平均バイト数。このメトリクスにはヘルスチェック トラフィックは含まれません。	
	レポート条件: 常に報告される	
	統計:最も有用な統計は Maximum です。	
	ディメンション	
	• LoadBalancer	
	 AvailabilityZone ,LoadBalancer 	
PeakPacketsPerSeco nd	サンプリングウィンドウの間に 10 秒間隔で計算される最大パケット レートの平均値 (1 秒あたりの処理パケット数)。このメトリクスに は、ヘルスチェックトラフィックが含まれます。	
	レポート条件: 常に報告される	
	統計:最も有用な統計は Maximum です。	
	ディメンション	
	• LoadBalancer	
	 AvailabilityZone ,LoadBalancer 	

メトリクス	説明
ProcessedBytes	ロードバランサーによって処理される総バイト数。この数には、ヘ ルスチェックトラフィックを除く、ターゲットとの間のトラフィッ クが含まれます。
	レポート条件: ゼロ以外の値がある
	統計: 最も有用な統計は Sum です。
	ディメンション
	• LoadBalancer
	 AvailabilityZone ,LoadBalancer
RejectedFlowCount	ロードバランサーによって拒否されたフロー (または接続) の合計 数。
	レポート条件: 常に報告される。
	統計値: 最も有用な統計値は Average、Maximum、および Minimum です。
	ディメンション
	• LoadBalancer
	 AvailabilityZone ,LoadBalancer
RejectedFlowCount_ TCP	ロードバランサーによって拒否された TCP フロー (または接続) の 数。
	レポート条件: ゼロ以外の値がある。
	統計: 最も有用な統計は Sum です。
	ディメンション
	• LoadBalancer
	 AvailabilityZone , LoadBalancer

メトリクス	説明		
UnHealthyHostCount	異常と見なされるターゲットの数。		
	レポート条件: ヘルスチェックが有効になっている場合にレポートさ れます		
	統計値: 最も有用な統計値は Maximum および Minimum です。		
	ディメンション		
	LoadBalancer , TargetGroupAvailabilityZone , LoadBalancer , TargetGroup		

Gateway Load Balancer のメトリクスディメンション

Gateway Load Balancer のメトリクスを絞り込むには、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
Availabil ityZone	アベイラビリティーゾーン別にメトリクスデータをフィルタリングしま す。
LoadBalancer	Gateway Load Balancer でメトリクスデータをフィルタリングしま す。Gateway Load Balancer を次のように指定します: gateway/load- balancer-name/1234567890123456 (ARN の最後の部分)。
TargetGroup	ターゲットグループでメトリクスデータをフィルタリングします。ター ゲットグループを次のように指定します。targetgroup/ターゲットグルー プ名/1234567890123456 (ターゲットグループ ARN の最後の部分)。

Gateway Load Balancer の CloudWatch メトリクスの表示

Amazon EC2 コンソールを使用して、Gateway Load Balancer に関する CloudWatch メトリクスを 表示できます。これらのメトリクスは、モニタリング用のグラフのように表示されます。Gateway Load Balancer 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。 別の方法として、Gateway Load Balancer のメトリクスの表示に、CloudWatch コンソールを使用す ることもできます。

コンソールを使用してメトリクスを表示するには

- 1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
- ターゲットグループによってフィルタリングされたメトリクスを表示するには、以下の作業を実行します。
 - a. ナビゲーションペインで、[Target Groups] を選択します。
 - b. ターゲットグループを選択し、[Monitoring] を選択します。
 - c. (オプション) 結果を時間でフィルタリングするには、[Showing data for] から時間範囲を選 択します。
 - d. 1 つのメトリクスの大きいビューを取得するには、グラフを選択します。
- Gateway Load Balancer でフィルタリングされたメトリクスを表示するには、以下の操作を実行します。
 - a. ナビゲーションペインで、[ロードバランサー]を選択します。
 - b. Gateway Load Balancer を選択し、[Monitoring] (モニタリング) タブを選択します。
 - c. (オプション) 結果を時間でフィルタリングするには、[Showing data for] から時間範囲を選 択します。
 - d. 1 つのメトリクスの大きいビューを取得するには、グラフを選択します。

CloudWatch コンソールを使用してメトリクスを表示するには

- 1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
- 2. ナビゲーションペインで [Metrics (メトリクス)] を選択してください。
- 3. GatewayELB 名前空間を選択します。
- (オプション) すべてのディメンションでメトリクスを表示するには、検索フィールドに名称を入力します。

を使用してメトリクスを表示するには AWS CLI

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

aws cloudwatch list-metrics --namespace AWS/GatewayELB

を使用してメトリクスの統計を取得するには AWS CLI

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。特に発行されていないディメンションの組み合わせを使用した統計を取得 することはできません。メトリクス作成時に使用した同じディメンションを指定する必要がありま す。

```
aws cloudwatch get-metric-statistics --namespace AWS/GatewayELB \
--metric-name UnHealthyHostCount --statistics Average --period 3600 \
--dimensions Name=LoadBalancer,Value=net/my-load-balancer/50dc6c495c0c9188 \
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \
--start-time 2017-04-18T00:00:00Z --end-time 2017-04-21T00:00:00Z
```

以下は出力例です。

```
{
    "Datapoints": [
        {
             "Timestamp": "2020-12-18T22:00:00Z",
             "Average": 0.0,
             "Unit": "Count"
        },
        {
             "Timestamp": "2020-12-18T04:00:00Z",
             "Average": 0.0,
             "Unit": "Count"
        },
        . . .
    ],
    "Label": "UnHealthyHostCount"
}
```

Gateway Load Balancers のクォータ

AWS アカウントには、 AWS サービスごとに、以前は制限と呼ばれていたデフォルトのクォータが あります。特に明記されていない限り、クォータは地域固有です。一部のクォータについては引き上 げをリクエストできますが、その他のクォータについては引き上げることはできません。

クォータの引き上げをリクエストするには、「Service Quotas ユーザーガイド」の「<u>クォータ</u> <u>引き上げリクエスト</u>」を参照してください。Service Quotas でクォータがまだ利用できない場合 は、サービスクォータの引き上げをリクエストしてください。

クォータ

- ロードバランサー
- ターゲットグループ
- Load Balancerのキャパシティーユニット

ロードバランサー

AWS アカウントには、Gateway Load Balancer に関連する次のクォータがあります。

名前	デフォルト	引き上げ可能
リージョンあたりの Gateway Load Balancer	100	はい
VPC あたりの Gateway Load Balancer	100	はい
VPC あたりの Gateway Load Balancer ENI 数	300 *	はい
Gateway Load Balancer あたりのリスナー数	1	いいえ

* それぞれの Gateway Load Balancer は、ゾーンごとに 1 つのネットワークインターフェイスを使用 します。

ターゲットグループ

次のクォータはターゲットグループ用です。

名前	デフォルト	引き上げ可能
リージョンあたりの GENEVE ターゲットグループ 数	100	はい
ターゲットグループあたりのターゲット	1,000	はい
GENEVE ターゲットグループあたりのアベイラビリ ティーゾーンあたりのターゲット数	300	いいえ
Gateway Load Balancer あたりのアベイラビリ ティーゾーンあたりのターゲット数	300	いいえ
Gateway Load Balancer あたりのターゲット数	300	いいえ

Load Balancerのキャパシティーユニット

次のクォータは、Load Balancerキャパシティーユニット (LCUs。

名前	デフォルト	引き上げ可能
リージョンあたりのリザーブドゲートウェイLoad Balancerキャパシティーユニット (LCU)	0	<u>あり</u>

Gateway Load Balancer のドキュメント履歴

次の表に、Gateway Load Balancer のリリース情報を示します。

変更	説明	日付
<u>キャパシティーユニットの予</u> 約	このリリースでは、ロードバ ランサーの最小容量を設定 するサポートが追加されまし た。	2025 年 4 月 10 日
<u>IPv6 サポート</u>	IPv4 と IPv6 の両方のアド レスをサポートするように Gateway Load Balancer を設 定できます。	2022 年 12 月 12 日
<u>フローの再調整</u>	このリリースでは、ターゲッ トが失敗または登録解除さ れた場合の Gateway Load Balancer のフロー処理動作を 定義するサポートが追加され ました。	2022 年 10 月 13 日
<u>設定可能なフロースの維持</u>	特定のターゲットアプライア ンスへのフローの維持設定を 保持するハッシュを設定でき ます。	2022 年 8 月 25 日
<u>新しいリージョンで利用可能</u>	このリリースでは、 AWS GovCloud (US) リージョンで Gateway Load Balancer のサ ポートが追加されました。	2021 年 6 月 17 日
<u>新しいリージョンで利用可能</u>	このリリースでは、カナダ (中 部)、アジアパシフィック (ソ ウル)、アジアパシフィック (大阪) リージョンの Gateway	2021 年 3 月 31 日

Load Balancer のサポートが追 加されました。

このリリースでは、米国西部 2021年3月19日 新しいリージョンで利用可能 (北カリフォルニア)、欧州 (ロ ンドン)、欧州 (パリ)、欧州 (ミラノ)、アフリカ (ケープ タウン)、中東 (バーレーン)、 アジアパシフィック (香港)、 アジアパシフィック (シンガ ポール)、およびアジアパシフ ィック (ムンバイ) リージョン σ Gateway Load Balancer σ サポートが追加されました。 初回リリース このリリースの Elastic Load 2020年11月10日 Balancing では、Gateway Load Balancer が導入されてい ます。
翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛 盾がある場合、英語版が優先します。