Elastic Load Balancing

Network Load Balancer

Elastic Load Balancing: Network Load Balancer

Table of Contents

Network Load Balancer とは

Elastic Load Balancing は、次のタイプのロードバランサーをサポートしています。Application Load Balancer、Network Load Balancer、および クラシックロードバランサー です。このガイドでは、Network 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、Application Load Balancer 用ユーザーガイドおよび クラシックロードバランサー 用ユーザーガイドを参照してください。

Network Load Balancer コンポーネント

ロードバランサーは、クライアントにとって単一の通信先として機能します。ロードバランサーは、受信トラフィックを Amazon EC2 インスタンスなどの複数のターゲットに分散します。これにより、アプリケーションの可用性が向上します。ロードバランサーに 1 つ以上のリスナーを追加できます。

リスナーは、構成したプロトコルとポートを使用してクライアントからの接続リクエストをチェックし、リクエストをターゲットグループに転送します。

各ターゲットグループは、指定された TCP プロトコルとポート番号を使用して、1 つ以上の登録済みのターゲット (EC2 インスタンスなど) にリクエストをルーティングできます。1 つのターゲットを複数のターゲットグループに登録できます。ターゲットグループ単位でヘルスチェックを設定できます。ヘルスチェックは、ロードバランサーのリスナールールに指定されたターゲットグループに登録されたすべてのターゲットで実行されます。

詳細については、次のドキュメントを参照してください。

- ロードバランサー (p. 10)
- リスナー (p. 17)
- ターゲットグループ (p. 24)

Network Load Balancer の概要

Network Load Balancer は、開放型システム間相互接続 (OSI) モデルの第 4 層で機能します。毎秒数百万のリクエストを処理できます。ロードバランサーは、接続リクエストを受信すると、デフォルトルールのターゲットグループからターゲットを選択します。リスナー構成で指定されたポート上の選択したターゲットへの TCP 接続を開こうとします。

ロードバランサー用のアベイラビリティーゾーンを有効にすると、Elastic Load Balancing はアベイラビリティーゾーンにロードバランサーノードを作成します。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、各ロードバランサーノードは、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「クロスゾーン負荷分散」を参照してください。

ロードバランサーで複数のアベイラビリティゾーンを有効にした場合、各ターゲットグループに、有効にされたアベイラビリティーゾーンごとに 1 つ以上のターゲットがあることを確認してください。これにより、アプリケーションの耐障害性が高まります。たとえば、1 つ以上のターゲットグループで 1 つのアベイラビリティーゾーン内に正常なターゲットがない場合、DNS から該当するサブネットの IP アドレスを削除しますが、他のアベイラビリティーゾーンのロードバランサーノードは、引き続きトラフィックをルーティングできます。クライアントが有効期限 (TTL) を守らず、DNS から削除された後でリクエストを IP アドレスに送信すると、そのリクエストは失敗します。

ロードバランサーノードは、プロトコル、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート、および TCP シーケンス番号に基づいて、フローハッシュアルゴリズムを使用してターゲットを選択します。クライアントからの TCP 接続のソースポートとシーケンス番号は異なり、別のターゲットにルーティングできます。各 TCP 接続は、接続中は単一のターゲットにルーティングされます。

Elastic Load Balancing は、有効にした各アベイラビリティーゾーンごとにネットワークインターフェイスを作成します。アベイラビリティーゾーンの各ロードバランサーノードは、このネットワークインターフェイスを使用して静的 IP アドレスを取得します。インターネット向けのロードバランサーを作成する場合は、必要に応じて 1 つの Elastic IP アドレスをサブネットごとに関連付けることができます。

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るように、ターゲットグループを構成できます。インスタンス ID を使用してターゲットを指定すると、クライアントの送信元 IP アドレスが保持され、アプリケーションに提供されます。ターゲットを IP アドレスで指定する場合、送信元 IP アドレスはロードーバランサノードのプライベート IP アドレスとなります。

アプリケーションへの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と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 は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。

登録済みのインスタンスのヘルス状態をモニタリングするために使用されるヘルスチェックを設定することで、ロードバランサーは正常なターゲットにのみリクエストを送信できます。

詳細については、Elastic Load Balancing ユーザーガイドの「Elastic Load Balancing の仕組み」を参照してください。

Classic Load Balancer からの移行のメリット

Classic Load Balancer に代わる Network Load Balancer の使用には、次のメリットがあります。

- 揮発性のワークロードを処理し、毎秒数百万のリクエストに対応できる能力。
- ロードバランサーの静的 IP アドレスのサポート。ロードバランサーで有効になっているサブネットごとに 1 つの Elastic IP アドレスを割り当てることもできます。
- ロードバランサーの VPC 外のターゲットを含め、IP アドレスによるターゲットの登録をサポート。
- 1 つの EC2 インスタンス上での複数のアプリケーションへのルーティングリクエストのサポート。複数のポートを使用して、各インスタンスまたは IP アドレスを同じターゲットグループに登録できます。
- コンテナ化されたアプリケーションのサポート。Amazon Elastic Container Service (Amazon ECS) は、タスクをスケジュールするときに未使用のポートを選択し、そのポートを使用するターゲットグループにタスクを登録できます。これにより、クラスターを効率的に使用することができます。
- 各サービスの個別のヘルスステータスのモニタリングのサポート。ヘルスチェックがターゲットグループレベルで定義され、多数の Amazon CloudWatch メトリクスがターゲットグループレベルで報告されます。ターゲットグループを Auto Scaling グループにアタッチすることで、各サービスをオンデマンドで動的にスケールすることができます。

各ロードバランサーの種類でサポートされている機能の詳細については、「Elastic Load Balancing 製品の比較」を参照してください。

開始方法

Network Load Balancer を作成するには、次のいずれかのチュートリアルに従います。

- Network Load Balancer の使用開始 (p. 4)

- チュートリアル: AWS CLI を使用して Network Load Balancer を作成する (p. 7)

料金表

詳細については、「Network Load Balancer 料金表」を参照してください。

Network Load Balancer の使用開始

このチュートリアルでは、ウェブベースインターフェイスである AWS マネジメントコンソールを使用して Network Load Balancer を実践的に説明します。最初の Network Load Balancer を作成するには、次のステップを完了します。

タスク

または、Application Load Balancer を作成するには、Application Load Balancer 用ユーザーガイドの「Application Load Balancer の開始方法」を参照してください。Classic Load Balancer を作成するには、クラシックロードバランサー 用ユーザーガイドの「Classic Load Balancer の作成」を参照してください。

開始する前に

- EC2 インスタンスに使用するアベイラビリティーゾーンを決定します。これらの各アベイラビリティーゾーンに少なくとも 1 つのパブリックサブネットがある Virtual Private Cloud (VPC) を設定します。これらのパブリックサブネットは、ロードバランサーを設定するために使用されます。その代わりに、これらのアベイラビリティーゾーンの他のサブネットで EC2 インスタンスを起動することができます。
- 各アベイラビリティーゾーンで少なくとも 1 つの EC2 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が、リスナーポート上のクライアントからの TCP アクセスと、VPC からのヘルスチェックリクエストを許可していることを確認します。詳細については、「ターゲットセキュリティグループ (p. 33)」を参照してください。

ステップ 1: ロードバランサーの種類の選択

Elastic Load Balancing は 3 種類のロードバランサーをサポートしています。このチュートリアルでは、Network Load Balancer を作成します。

Network Load Balancer を作成するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ナビゲーションバーで、ロードバランサーのリージョンを選択します。EC2 インスタンス用に使用したリージョンと同じリージョンを必ず選択してください。
3. ナビゲーションペインの [LOAD BALANCING] で [Load Balancers] を選択します。
4. [Create Load Balancer] を選択します。

5. [Network Load Balancer] の場合は、[作成] を選択します。

ステップ 2: ロードバランサーとリスナーの設定

[Configure Load Balancer] ページで、次の手順を完了します。

ロードバランサーとリスナーを設定するには

1. [Name] に、ロードバランサーの名前を入力します。

   Network Load Balancer の名前は、リージョンの Application Load Balancer および Network Load Balancer セット内で一意にする必要があります。最大 32 文字で、英数字とハイフンのみ使用できます。先頭と末尾にハイフンを使用することはできず、「internal-」で始めることはできません。
2. [Scheme] で、デフォルト値 [internet-facing] を保持します。
3. [Listeners] では、デフォルトを保持します。これは、ポート 80 で TCP トラフィックを受け付けるリスナーです。
4. [Availability Zones] で、EC2 インスタンスに使用する VPC を選択します。EC2 インスタンスの起動に使用した各アベイラビリティーゾーンについて、アベイラビリティーゾーンを選択し、そのアベイラビリティーゾーンのパブリックサブネットを選択します。

   インターネット向けのロードバランサーを作成する場合は、必要に応じて [Elastic IP] から Elastic IP アドレスを選択できますこれにより、ロードバランサーノードに静的 IPv4 アドレスが提供されます。
5. [Next: Configure Routing] を選択します。

ステップ 3: ターゲットグループの設定

リクエストルーティングで使用されるターゲットグループを作成します。リスナーのルールは、このターゲットグループ内の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。ロードバランサーは、ターゲットグループに定義されたヘルスチェック設定を使用してこのターゲットグループ内のターゲットの状態を確認します。[Configure Routing] ページで、次の手順を完了します。

ターゲットグループを設定するには

1. [Target group] で、デフォルトの [New target group] を保持します。
2. [Name] に、新しいターゲットグループの名前を入力します。
3. [プロトコル] は TCP、[ポート] は 80、[ターゲットの種類] はインスタンスで維持します。
4. [Health checks] は、デフォルトのプロトコルを保持します。
5. [Next: Register Targets] を選択します。

ステップ 4: ターゲットグループへのターゲットの登録

[Register Targets] ページで、次の手順を完了します。

ターゲットグループにターゲットを登録するには

1. [Instances] で、1 つ以上のインスタンスを選択します。
2. デフォルトポート 80 を保持し、[Add to registered] を選択します。

3. インスタンスの選択が完了したら、[Next: Review] を選択します。

ステップ 5: Load Balancer の作成とテスト

ロードバランサーを作成する前に、設定を確認します。ロードバランサーを作成した後で、EC2 インスタンスにトラフィックを送信するかどうかを検証します。

ロードバランサーを作成してテストするには

1. [Review] ページで、[Create] を選択します。
2. ロードバランサーが正常に作成されたことが通知されたら、[Close] を選択します。
3. ナビゲーションペインの [LOAD BALANCING] で [Target Groups] を選択します。
4. 新しく作成したターゲットグループを選択します。
5. [Targets] を選択して、インスタンスの準備ができていることを確認します。インスタンスのステータスが `initial` の場合、インスタンスがまだ登録の途中であるか、正常と見なされるのに必要なヘルスチェックの最小数に合格しなかったと考えられます。少なくとも 1 つのインスタンスのステータスが `healthy` であれば、ロードバランサーをテストできます。
6. ナビゲーションペインの [LOAD BALANCING] で [Load Balancers] を選択します。
7. 新しく作成したロードバランサーを選択します。
8. [Description] を選択し、ロードバランサーの DNS 名 (例: my-load-balancer-1234567890.us-west-2.elb.amazonaws.com) をコピーします。インターネットに接続したウェブブラウザのアドレスフィールドに DNS 名を貼り付けます。すべて適切な場合は、ブラウザにサーバーのデフォルトページが表示されます。

ステップ 6: ロードバランサーの削除 (オプション)

ロードバランサー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。不要になったロードバランサーは削除できます。ロードバランサーが削除されると、ロードバランサーの課金も停止されます。ロードバランサーを削除しても、ロードバランサーに登録されたターゲットには影響を与えません。たとえば、EC2 インスタンスを実行し続けます。

ロードバランサーを削除するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
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て [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、削除する] を選択します。

チュートリアル: AWS CLI を使用して Network Load Balancer を作成する

このチュートリアルでは、AWS CLI を通じた Network Load Balancer の実践入門を示します。

開始する前に

- AWS CLI をインストールするか、Network 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は AWS CLI を現行バージョンに更新します。詳細については、AWS Command Line Interface ユーザーガイドの「AWS コマンドラインインターフェイスのインストール」を参照してください。
- EC2 インスタンスに使用するアベイラビリティーゾーンを決定します。これらの各アベイラビリティーゾーンに少なくとも 1 つのパブリックサブネットがある Virtual Private Cloud (VPC) を設定します。
- 各アベイラビリティーゾーンで少なくとも 1 つの EC2 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が、リスナーポート上のクライアントからの TCP アクセスと、VPC からのヘルスチェックリクエストを許可していることを確認します。詳細については、「ターゲットセキュリティグループ (p. 33)」を参照してください。

Load Balancer の作成

最初のロードバランサーを作成するには、次のステップを完了します。

ロードバランサーを作成するには

1. create-load-balancer コマンドを使用してロードバランサーを作成し、インスタンスを起動した各アベイラビリティーゾーンのパブリックサブネットを指定します。アベイラビリティーゾーンごとに 1 つだけサブネットを指定できます。

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
 subnet-12345678
```

出力には、次の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/net/my-load-
balancer/1234567890123456
```

2. ターゲットグループを指定し、EC2 インスタンスに使用したのと同じ VPC を指定するには、create-target-group コマンドを使用します。

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id
 vpc-12345678
```

出力には、次の形式の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/my-
targets/1234567890123456
```

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-12345678
 Id=i-23456789
```

4. 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するには、create-listener コマンドを使用します。

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --protocol TCP --port 80
  \
--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/net/my-load-
balancer/1234567890123456/1234567890123456
```

5. (オプション) この describe-target-health 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
```

ロードバランサーの Elastic IP アドレスを指定します。

Network Load Balancer を作成するときは、サブネットマッピングを使用して、サブネットごとに 1 つの Elastic IP アドレスを指定できます。

```
aws elbv2 create-load-balancer --name my-load-balancer --type network \
--subnet-mappings SubnetId=subnet-12345678,AllocationId=eipalloc-12345678
```

ポートの上書きを使用したターゲットの追加

1 つのインスタンスに複数のサービスを持つマイクロサービスアーキテクチャがある場合、各サービスは異なるポートで接続を受け入れます。毎回別のポートで、インスタンスをターゲットグループに複数回登録できます。

ポートの上書きを使用してターゲットを追加するには

1. ターゲットグループを作成するには、create-target-group コマンドを使用します。

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 \
--vpc-id vpc-12345678
```

2. 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。インスタンス ID はコンテナごとに同じですが、ポートは異なることに注意してください。

```
aws elbv2 register-targets --target-group-arn targetgroup-arn  \
--targets Id=i-12345678,Port=80 Id=i-12345678,Port=766
```

3. 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するには、create-listener コマンドを使用します。

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn \
--protocol TCP --port 80  \
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

ロードバランサーの削除

ロードバランサーとターゲットグループが必要なくなった場合は、次のように削除することができます。

```
aws elbv2 delete-load-balancer --load-balancer-arn loadbalancer-arn
aws elbv2 delete-target-group --target-group-arn targetgroup-arn
```

Network Load Balancer

ロードバランサーは、クライアントにとって単一の通信先として機能します。クライアントはロードバランサーにリクエストを送信し、ロードバランサーは 1 つ以上のアベイラビリティーゾーンにあるターゲット (EC2 インスタンスなど) にそれらのリクエストを送信します。

ロードバランサーを設定するには、ターゲットグループ (p. 24)を作成し、ターゲットグループにターゲットを登録します。有効な各アベイラビリティーゾーンに少なくとも 1 つの登録済みターゲットがあるようにする場合、ロードバランサーが最も効果的です。さらに、リスナー (p. 17)を作成してクライアントからの接続リクエストがないかチェックし、リクエストをクライアントからターゲットグループ内のターゲットにルーティングします。

Network Load Balancerは VPC ピアリング、AWS マネージド VPN、およびサードパーティーの VPN ソリューションを経由した接続をサポートします。

コンテンツ

ロードバランサーの状態

ロードバランサーの状態は次のいずれかです。

`provisioning`

ロードバランサーはセットアップ中です。

`active`

ロードバランサー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`

ロードバランサークラウドをセットアップできませんでした。

ロードバランサーの属性

ロードバランサーの属性は以下のとおりです。

`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: `false`。

`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: `false`。

アベイラビリティーゾーン

ロードバランサーを作成するときに、ロードバランサーの 1 つまたは複数のアベイラビリティーゾーンを有効にします。Network Load Balancer を作成した後で、アベイラビリティーゾーンを有効または無効にすることはできません。ロードバランサーで複数のアベイラビリティーゾーンを有効にすると、アプリケーションの耐障害性が向上します。

アベイラビリティゾーンを有効にする場合、このアベイラビリティゾーンから 1 つのサブネットを指定します。Elastic Load Balancing はアベイラビリティーゾーンにロードバランサーノードを作成し、サブネットのネットワークインターフェイスを作成します (「ELB net」で始まり、ロードバランサーの名前を含む記述)。アベイラビリティーゾーンの各ロードバランサーノードは、このネットワークインターフェイスを使用して静的 IP アドレスを取得します。このネットワークインターフェイスは表示できますが、変更することはできません。

インターネット向けのロードバランサーを作成する場合は、必要に応じて 1 つの Elastic IP アドレスをサブネットごとに関連付けることができます。ロードバランサーの作成後に、サブネットの Elastic IP アドレスを追加または変更することはできません。

要件

- 指定するサブネットには最低 8 個の利用可能な IP アドレスが必要です。
- 別の AWS アカウントと共有していたサブネットを指定することはできません。
- 制約のあるアベイラビリティゾーンにあるサブネットを指定することはできません。エラーメッセージは、「'network' タイプを使用したロードバランサーは az_name でサポートされていません」です。制約されていない別のアベイラビリティゾーンにあるサブネットを指定し、クロスゾーン負荷分散を使用して、制約されているアベイラビリティゾーンのターゲットにトラフィックを分散することはできます。

クロスゾーン負荷分散

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、各ロードバランサーノードは、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「クロスゾーン負荷分散」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. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
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ます。
4. [Description]、[Edit attributes] を選択します。
5. [ロードバランサー属性の編集] ページで、[クロスゾーン負荷分散] の [有効] を選択し、[保存] を選択します。

AWS CLI を使用してクロスゾーン負荷分散を有効にするには

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

削除保護

ロードバランサー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、ロードバランサーで削除保護が無効になっています。

ロードバランサーの削除保護を有効にした場合、ロードバランサー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. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
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ます。
4. [Description]、[Edit attributes] 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. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
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ます。
4. [Description]、[Edit attributes] を選択します。
5. [Edit load balancer attributes] ページで、[Enable delete protection] をクリアし、[Save] を選択します。

AWS CLI を使用して削除保護を有効または無効にするには

`deletion_protection.enabled` 属性を指定して modify-load-balancer-attributes コマンドを使用します。

接続のアイドルタイムアウト

クライアントがNetwork Load Balancerを通じて行うリクエストごとに、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の経過後にクライアントがデータを送信した場合、TCP RST 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。

Elastic Load Balancing はアイドルタイムアウト値を 350 秒に設定します。この値を変更することはできません。TCP リスナーのターゲットは、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。TCP キープアライブパケットは、TLS リスナーのターゲットではサポートされていません。

Network Load Balancer の作成

ロードバランサー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。

開始する前に、少なくとも 1 つのアベイラビリティーゾーンで EC2 インスタンスを起動してください。Virtual Private Cloud (VPC) で、これらの各アベイラビリティーゾーンに少なくとも 1 つのパブリックサブネットがあることを確認します。

AWS CLI を使用してロードバランサーを作成する方法については、「チュートリアル: AWS CLI を使用して Network Load Balancer を作成する (p. 7)」を参照してください。

AWS マネジメントコンソール を使用してロードバランサーを作成するには、以下のタスクを完了します。

タスク

- ステップ 1: ロードバランサーとリスナーを設定する (p. 5)
- ステップ 2: ターゲットグループを設定する (p. 5)
- ステップ 3: ターゲットグループへのターゲットの登録 (p. 14)
- ステップ 4: ロードバランサーを作成する (p. 14)

ステップ 1: ロードバランサーとリスナーを設定する

最初に、名前、ネットワーク、1 つ以上のリスナーなど、ロードバランサーの基本的な設定情報を指定します。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。これは、クライアントからロードバランサーへの接続用のプロトコルとポートを使用して設定します。サポートされるプロトコルとポートの詳細については、「リスナーの設定 (p. 17)」を参照してください。

ロードバランサーとリスナーを設定するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ナビゲーションペインの [LOAD BALANCING] で [Load Balancers] を選択します。
3. [Create Load Balancer] を選択します。
4. [Network Load Balancer] の場合は、[作成] を選択します。
5. [Name] に、ロードバランサーの名前を入力します。たとえば、**`my-nlb`** と指定します。
6. [スキーム] のインターネット向けロードバランサーは、クライアントからインターネット経由でリクエストをターゲットにルーティングします。内部ロードバランサーは、プライベート IP アドレスを使用してターゲットにリクエストをルーティングします。
7. [Listeners] のデフォルトは、ポート 80 で TCP トラフィックを受け付けるリスナーです。デフォルトのリスナー設定を保持する、プロトコルを変更する、またはポートを変更することができます。別のリスナーを追加するには、[Add] を選択します。
8. [Availability Zones] で、EC2 インスタンスに使用する VPC を選択します。EC2 インスタンスの起動に使用した各アベイラビリティーゾーンについて、アベイラビリティーゾーンを選択し、そのアベイラビリティーゾーンのパブリックサブネットを選択します。Elastic IP アドレスをサブネットに関連付けるには、[Elastic IP] から選択します。
9. [Next: Configure Routing] を選択します。

ステップ 2: ターゲットグループを設定する

EC2 インスタンスなどのターゲットをターゲットグループに登録できます。このステップで設定するターゲットグループは、リクエストをターゲットグループに転送するリスナールールで、ターゲットグループとして使用されます。詳細については、「Network Load Balancer のターゲットグループ (p. 24)」を参照してください。

ターゲットグループを設定するには

1. [Target group] で、デフォルトの [New target group] を保持します。
2. [Name] に、ターゲットグループの名前を入力します。
3. [Protocol] と [Port] を必要に応じて設定します。

4. [Target type] には、`instance` 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` を選択して IP アドレスでターゲットを指定します。
5. [Health checks] は、デフォルトのヘルスチェック設定のままにします。
6. [Next: Register Targets] を選択します。

ステップ 3: ターゲットグループへのターゲットの登録

EC2 インスタンスをターゲットグループのターゲットとして登録できます。

インスタンス ID でターゲットを登録するには

1. [Instances] で、1 つ以上のインスタンスを選択します。
2. デフォルトのインスタンスリスナーポートをそのまま使用するか、新しいインスタンスリスナーポートを入力し、[Add to registered] を選択します。
3. インスタンスの登録が完了したら、[Next: Review] を選択します。

IP アドレスでターゲットを登録するには

1. 各 IP アドレスを登録するには、次の操作を行います。
   a. [Network] で、IP アドレスがターゲットグループ VPC のサブネットからのものである場合は、VPC を選択します。それ以外の場合は、[Other private IP address] を選択します。
   b. [Availability Zone] で、アベイラビリティゾーンまたは [all] を選択します。これは、ターゲットが指定されたアベイラビリティゾーン内のロードバランサーノードからのトラフィックのみを受信するか、またはすべての有効なアベイラビリティゾーンからトラフィックを受信するかを決定します。このフィールドは、VPC から IP アドレスを登録している場合は表示されません。その場合は、アベイラビリティーゾーンが自動的に検出されます。
   c. [IP] にアドレスを入力します。
   d. [Port] にポートを入力します。
   e. [Add to list] を選択します。
2. IP アドレスのリストへの追加が完了したら、[Next: Review] を選択します。

ステップ 4: ロードバランサーを作成する

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ことを確認してから、ロードバランサーが EC2 インスタンスにトラフィックを送信することをテストできます。ロードバランサーの操作を終了したら、ロードバランサーを削除できます。詳細については、「Network Load Balancer の削除 (p. 15)」を参照してください。

ロードバランサーを作成するには

1. [Review] ページで、[Create] を選択します。
2. ロードバランサーが作成されたら、[Close] を選択します。
3. ナビゲーションペインの [LOAD BALANCING] で [Target Groups] を選択します。
4. 新しく作成したターゲットグループを選択します。
5. [Targets] を選択して、インスタンスの準備ができていることを確認します。インスタンスのステータスが `initial` の場合、インスタンスがまだ登録の途中であるか、正常と見なされるのに必要なヘルスチェックの最小数に合格しなかったと考えられます。少なくとも 1 つのインスタンスのステータスが正常であれば、ロードバランサーをテストできます。

Network Load Balancer のタグ

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、各ロードバランサー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、ロードバランサーからタグを削除できます。

制限

- 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。
- タグの名前または値に `aws:` プレフィックスは使用しないでください。このプレフィックスは AWS 用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ロードバランサーのタグを更新するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
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。[Key] と [Value] 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。

AWS CLI を使用してロードバランサーのタグを更新するには

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

Network Load Balancer の削除

ロードバランサー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。不要になったロードバランサーは削除できます。ロードバランサーが削除されると、ロードバランサーの課金も停止されます。

削除保護が有効になった場合、ロードバランサーを削除することはできません。詳細については、「削除保護 (p. 12)」を参照してください。

ロードバランサーを削除すると、そのリスナーも削除されます。ロードバランサーを削除しても、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、「ターゲットグループの削除 (p. 36)」を参照してください。

コンソールを使用してロードバランサーを削除するには

1. ロードバランサーをポイントするドメインの CNAME レコードが存在する場合は、新しい場所にポイントして DNS の変更が有効になってから、ロードバランサーを削除します。
2. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
3. ナビゲーションペインの [LOAD BALANCING] で [Load Balancers] を選択します。
4. ロードバランサーを選択します。
5. [Actions] で、[Delete] を選択します。
6. 確認を求めるメッセージが表示されたら、[はい、削除する] を選択します。

AWS CLI を使用してロードバランサーを削除するには

delete-load-balancer コマンドを使用します。

Network Load Balancer のリスナー

Network Load Balancer の使用を開始する前に、1 つ以上のリスナーを追加する必要があります。リスナーとは、設定したプロトコルとポートを使用して接続リクエストをチェックするプロセスです。リスナーに対して定義したルールは、ロードバランサーが 1 つ以上のターゲットグループ内のターゲットにリクエストをルーティングする方法を決定します。

詳細については、Elastic Load Balancing ユーザーガイドの「リクエストルーティング」を参照してください。

コンテンツ

リスナーの設定

リスナーは次のポートとプロトコルをサポートします。

- プロトコル: TCP、TLS
- ポート: 1 ~ 65535

アプリケーションがビジネスロジックに集中できるように、TLS リスナーを使用して、暗号化および復号の作業をロードバランサーに任せることができます。リスナープロトコルが TLS の場合は、リスナーに SSL サーバー証明書を 1 つだけデプロイする必要があります。詳細については、「Network Load Balancer の TLS リスナー (p. 18)」を参照してください。

リスナーで WebSockets が利用できます。

設定済みのリスナーに対するすべてのネットワークトラフィックが、意図されたトラフィックとして分類されます。設定済みのリスナーに一致しないネットワークトラフィックが、意図しないトラフィックとして分類されます。タイプ 3 以外の ICMP リクエストも、意図しないトラフィックと見なされます。Network Load Balancer は、意図しないトラフィックをターゲットに転送することなく削除します。意図しないトラフィックの一部となっている TCP データパケットは、TCP リセット (RST) で拒否されます。

リスナールール

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。このルールを更新するには、「Network Load Balancer のリスナーを更新する (p. 21)」を参照してください。

Network Load Balancer のリスナーを作成する

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。ロードバランサーを作成するときにリスナーを定義し、いつでもロードバランサーにリスナーを追加できます。

前提条件

- リスナールールのターゲットグループを指定する必要があります。詳細については、「Network Load Balancer のターゲットグループを作成するには (p. 28)」を参照してください。
- TLS リスナーの SSL 証明書を指定する必要があります。ターゲットにリクエストをルーティングする前に、ロードバランサーはこの証明書を使用して接続を終了し、クライアントからのリクエストを復号します。詳細については、「サーバー証明書 (p. 19)」を参照してください。

リスナーの追加

クライアントからロードバランサーへの接続用のプロトコルとポート、およびデフォルトのリスナールールのターゲットグループでリスナーを設定します。詳細については、「リスナーの設定 (p. 17)」を参照してください。

コンソールを使用してリスナーを追加するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
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. [リスナーの追加] を選択します。
5. [Protocol : port (プロトコル : ポート)] で、[TCP] または [TLS] を選択します。デフォルトポートのままにすることも、別のポートを入力することもできます。
6. [Default actions (デフォルトアクション)] で、[Add action (アクションの追加)]、[Forward to (転送先)] の順に選択し、利用可能なターゲットグループを選択します。
7. [TLS リスナー] [Security policy (セキュリティポリシー)] で、デフォルトのセキュリティポリシーを保持することをお勧めします。
8. [TLS リスナー] [Default SSL certificate (デフォルトの SSL 証明書)] で、次のいずれかを実行します。
   - AWS Certificate Manager を使用して証明書を作成またはインポートした場合は、[From ACM (ACM から)] を選択して、証明書を選択します。
   - IAM を使用して証明書をアップロードした場合は、[From IAM (IAM から)] を選択して、証明書を選択します。
9. [Save] を選択します。

AWS CLI を使用してリスナーを追加するには

リスナーを作成するには、create-listener コマンドを使用します。

Network Load Balancer の TLS リスナー

TLS リスナーごとにサーバー証明書を 1 つだけ指定する必要があります。ターゲットにリクエストを送信する前に、ロードバランサーはこの証明書を使用して接続を終了し、クライアントからのリクエストを復号します。

Elastic Load Balancing は、セキュリティポリシーと呼ばれる TLS ネゴシエーション設定を使用して、クライアントとロードバランサー間の TLS 接続をネゴシエートします。セキュリティポリシーはプロトコルと暗号の組み合わせです。プロトコルは、クライアントとサーバーの間の安全な接続を確立し、クライアントとロードバランサーの間で受け渡しされるすべてのデータのプライバシーを保証します。暗号とは、暗号化キーを使用してコード化されたメッセージを作成する暗号化アルゴリズムです。プロトコルは、複数の暗号を使用し、インターネットを介してデータを暗号化します。接続ネゴシエーションのプロセスで、クライアントとロードバランサーでは、それぞれサポートされる暗号とプロトコルのリストが優先される順に表示されます。サーバーのリストで最初にクライアントの暗号と一致した暗号が安全な接続用に選択されます。

Network Load Balancer ではクライアントまたはターゲット接続の TLS 再ネゴシエーションまたは TLS セッションの再開はサポートされていません。

サーバー証明書

ロードバランサーは X.509 証明書 (サーバー証明書) を使用します。証明書とは、認証機関 (CA) によって発行された識別用デジタル形式です。証明書には、認識用情報、有効期間、パブリックキー、シリアル番号と発行者のデジタル署名が含まれます。

ロードバランサーで使用する証明書を作成するときに、ドメイン名を指定する必要があります。

AWS Certificate Manager (ACM) を使用して、ロードバランサーの証明書を作成することをお勧めします。ACM は、Elastic Load Balancing と統合して、ロードバランサーに証明書をデプロイできます。詳細については、『AWS Certificate Manager ユーザーガイド』を参照してください。

また、TLS を使用して署名証明書リクエスト (CSR) を作成し、CA から CSR 署名を取得して証明書を発行して、ACM にこの証明書をインポートする、あるいは AWS Identity and Access Management (IAM) に証明書をアップロードすることもできます。詳細については、AWS Certificate Manager ユーザーガイドの「証明書のインポート」または IAM ユーザーガイドの「サーバー証明書の使用」を参照してください。

> Important
>
> 2048 ビットより大きい RSA キーまたは EC キーを持つ証明書を Network Load Balancer にインストールすることはできません。

セキュリティポリシー

フロントエンド接続に使用するセキュリティポリシーを選択できます。バックエンド接続には、常に `ELBSecurityPolicy-2016-08` セキュリティポリシーが使用されます。Network Load Balancer はカスタムセキュリティポリシーをサポートしていません。

Elastic Load Balancing に用意されている Network Load Balancer 用のセキュリティポリシーは次のとおりです。

- `ELBSecurityPolicy-2016-08`
- `ELBSecurityPolicy-FS-2018-06`
- `ELBSecurityPolicy-TLS-1-2-2017-01`
- `ELBSecurityPolicy-TLS-1-2-Ext-2018-06`
- `ELBSecurityPolicy-TLS-1-1-2017-01`
- `ELBSecurityPolicy-2015-05`
- `ELBSecurityPolicy-TLS-1-0-2015-04`

一般的な使用には `ELBSecurityPolicy-2016-08` ポリシーをお勧めします。Forward Secrecy (FS) を必要とする場合は、`ELBSecurityPolicy-FS-2018-06` ポリシーを使用できます。`ELBSecurityPolicy-TLS` ポリシーの 1 つを使用して、特定の TLS プロトコルバージョンを無効に

する必要があるコンプライアンスおよびセキュリティ標準を満たすか、廃止された暗号を必要とするレガシークライアントをサポートできます。TLS バージョン 1.0 を必要とするのは、一部のインターネットクライアントのみです。ロードバランサーへのリクエストの TLS プロトコルバージョンを表示するには、ロードバランサーのアクセスログ記録を有効にして、アクセスログを調べます。詳細については、「アクセスログ (p. 41)」を参照してください。

次の表は、Network Load Balancer に定義されたセキュリティポリシーについて示しています。

セキュリティポリシー	2016-08 *	FS-2018-0	TLS-1-2	TLS-1-2-Ext	TLS-1-1	TLS-1-0 †
TLS Protocols						
Protocol-TLSv1	♦	♦				♦
Protocol-TLSv1.1	♦	♦			♦	♦
Protocol-TLSv1.2	♦	♦	♦	♦	♦	♦
TLS Ciphers						
ECDHE-ECDSA-AES128- GCM-SHA256	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES128- GCM-SHA256	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA256	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES128-SHA256	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA	♦	♦		♦	♦	♦
ECDHE-RSA-AES128-SHA	♦	♦		♦	♦	♦
ECDHE-ECDSA-AES256- GCM-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES256- GCM-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES256-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA	♦	♦		♦	♦	♦
ECDHE-ECDSA-AES256-SHA	♦	♦		♦	♦	♦
AES128-GCM-SHA256	♦		♦	♦	♦	♦
AES128-SHA256	♦		♦	♦	♦	♦
AES128-SHA	♦			♦	♦	♦
AES256-GCM-SHA384	♦		♦	♦	♦	♦
AES256-SHA256	♦		♦	♦	♦	♦
AES256-SHA	♦			♦	♦	♦
DES-CBC3-SHA						♦

* `ELBSecurityPolicy-2016-08` および `ELBSecurityPolicy-2015-05` のセキュリティポリシーは同じです。

† DES-CBC3-SHA 暗号 (弱い暗号) を必要とするレガシークライアントをサポートする必要がない限り、このセキュリティポリシーは使用しないでください。

AWS CLI を使用して、ロードバランサーのセキュリティポリシーの設定を表示するには、describe-ssl-policies コマンドを使用します。

セキュリティポリシーの更新

TLS リスナーを作成するときに、ニーズを満たすセキュリティポリシーを選択できます。新しいセキュリティのポリシーを追加したら、TLS リスナーを更新して新しいセキュリティポリシーを使用できます。Network Load Balancer はカスタムセキュリティポリシーをサポートしていません。

コンソールを使用してセキュリティポリシーを更新するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
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. TLS リスナーのチェックボックスをオンにして、[編集] を選択します。
5. [Security policy (セキュリティポリシー)] で、セキュリティポリシーを選択します。
6. [Update] を選択します。

AWS CLI を使用してセキュリティポリシーを更新するには

modify-listener コマンドを使用します。

Network Load Balancer のリスナーを更新する

リスナーポート、リスナープロトコル、またはデフォルトのリスナールールを更新できます。

デフォルトリスナールールは、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。

TCP から TLS にプロトコルを変更した場合、セキュリティポリシーとサーバー証明書を指定する必要があります。TLS から TCP にプロトコルを変更した場合、セキュリティポリシーとサーバー証明書は削除されます。

コンソールを使用してリスナーを更新するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
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. リスナーのチェックボックスをオンにしてから、[編集] を選択します。
5. (オプション) [プロトコル : ポート] の指定された値を変更します。
6. (オプション) 鉛筆アイコンをクリックし、[デフォルトアクション] の別のターゲットグループを選択します。
7. [Update] を選択します。

AWS CLI を使用してリスナーを更新するには

modify-listener コマンドを使用します。

サーバー証明書の更新

TLS リスナーを作成するときは、デフォルトの証明書を指定します。

各証明書には有効期間が記載されています。有効期間が終わる前に、証明書を更新するか、置き換える必要があります。証明書を更新または置き換えしても、ロードバランサーノードが受信し、正常なターゲットへのルーティングを保留中の未処理のリクエストには影響しません。証明書更新後、新しいリクエストは更新された証明書を使用します。証明書置き換え後、新しいリクエストは新しい証明書を使用します。

証明書の更新と置き換えは次のとおりに管理できます。

- AWS Certificate Manager が提供し、ロードバランサーにデプロイされた証明書は、自動的に更新できます。ACM は期限切れになる前に証明書を更新しようとします。詳細については、AWS Certificate Manager ユーザーガイド の管理された更新を参照してください。
- 証明書を ACM にインポートした場合は、証明書の有効期限をモニタリングし、期限切れ前に更新する必要があります。詳細については、AWS Certificate Manager ユーザーガイドの「証明書のインポート」を参照してください。
- IAM に証明書をインポートし、まもなく期限切れになる場合は、新しい証明書を作成し、この新しい証明書を ACM または IAM にインポートします。ロードバランサーにこの新しい証明書を追加し、期限切れの証明書をロードバランサーから削除します。

制限

2048 ビットより大きい RSA キーまたは EC キーを持つ証明書を Network Load Balancer にインストールすることはできません。

デフォルトの証明書の置き換え

次の手順でリスナーのデフォルトの証明書を置き換えできます。

コンソールを使用してデフォルトの証明書を変更するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
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. リスナーのチェックボックスを選択して、[編集] を選択します。
5. [Default SSL certificate (デフォルトの SSL 証明書)] で、次のいずれかを実行します。
   - AWS Certificate Manager を使用して証明書を作成またはインポートした場合は、[From ACM (ACM から)] を選択して、証明書を選択します。
   - IAM を使用して証明書をアップロードした場合は、[From IAM (IAM から)] を選択して、証明書を選択します。
6. [Update] を選択します。

AWS CLI を使用してデフォルトの証明書を変更するには

modify-listener コマンドを使用します。

Network Load Balancer のリスナーを削除する

リスナーの削除はいつでも行うことができます。

コンソールを使用してリスナーを削除するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
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。リスナーのチェックボックスをオンにして、[削除] 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、削除する] を選択します。

AWS CLI を使用してリスナーを削除するには

delete-listener コマンドを使用します。

Network 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。各リスナーのルールを作成するときに、ターゲットグループと条件を指定します。ルールの条件が満たされると、トラフィックが該当する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。たとえば、一般的なリクエスト用に 1 つのターゲットグループを作成し、アプリケーションのマイクロサービスへのリクエスト用に別のターゲットグループを作成できます。詳細については、「Network Load Balancer コンポーネント (p. 1)」を参照してください。

ロードバランサー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。リスナーのルールでターゲットグループを指定すると、ロードバランサーは、ロードバランサー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。ロードバランサーは、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。

コンテンツ

ルーティング設定

デフォルトでは、ロードバランサーはターゲットグループの作成時に指定したプロトコルとポート番号を使用して、リクエストをターゲットにルーティングします。または、ターゲットグループへの登録時にターゲットへのトラフィックのルーティングに使用されるポートを上書きすることもできます。

Network Load Balancer のターゲットグループでは、次のプロトコルとポートがサポートされています。

- プロトコル: TCP、TLS
- ポート: 1 ~ 65535

ターゲットの種類

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
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

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。

これらのサポートされている CIDR ブロックを使用すると、ClassicLink インスタンス、IP アドレスとポート (たとえば、データベース) でアドレス指定できる AWS リソース、AWS Direct Connect を介して AWS にリンクされたオンプレミスリソース、またはソフトウェア VPN 接続をターゲットグループに登録できます。

ターゲットの種類が `ip` である場合、ロードバランサーは一意の各ターゲット (IP アドレスとポート) に対して 55,000 の同時接続または 1 分あたり約 55,000 の接続をサポートできます。これらの接続数を超えた場合、ポート割り当てエラーが発生する可能性が高くなります。ポート割り当てエラーが発生した場合は、ターゲットグループにさらに多くのターゲットを追加します。

Network Load Balancer は `lambda` ターゲットタイプをサポートしていません。Application Load Balancer のみが `lambda` ターゲットタイプをサポートしています。詳細については、Application Load Balancer 用ユーザーガイドの「ターゲットとしての Lambda 関数」を参照してください。

リクエストのルーティングと IP アドレス

インスタンス ID を使用してターゲットを指定すると、トラフィックはインスタンスのプライマリネットワークインターフェイスで指定されたプライマリプライベート IP アドレスを使用して、インスタンスにルーティングされます。IP アドレスを使用してターゲットを指定する場合は、1 つまたは複数のネットワークインターフェイスからのプライベート IP アドレスを使用して、トラフィックをインスタンスにルーティングできます。これにより、インスタンスの複数のアプリケーションが同じポートを使用できるようになります。各ネットワークインターフェイスは独自のセキュリティグループを持つことができます。

送信元 IP の保持

インスタンス ID を使用してターゲットを指定すると、クライアントの送信元 IP アドレスが保持され、アプリケーションに提供されます。

ターゲットを IP アドレスで指定する場合、送信元 IP アドレスはロードバランサノードのプライベート IP アドレスとなります。クライアントの IP アドレスが必要な場合は、Proxy Protocol を有効にし、Proxy Protocol ヘッダーからクライアント IP アドレスを取得します。

Network Load Balancer に登録されているインスタンスでマイクロサービスを使用している場合、ロードバランサーを使用してインスタンス間の通信を提供することはできません。ただし、ロードバランサーがインターネット向けであるか、インスタンスが IP アドレスによって登録されている場合は除きま

す。詳細については、「ターゲットからそのロードバランサーへのリクエストが接続タイムアウトになる (p. 50)」を参照してください。

登録済みターゲット

ロードバランサーは、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、ロードバランサー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。異なるポートを使用して、各 EC2 インスタンスまたは IP アドレスを同じターゲットグループに複数回登録できます。これにより、ロードバランサーはリクエストをマイクロサービスにルーティングできます。

アプリケーションの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。ロードバランサーは、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。

アプリケーションの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、ロードバランサー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。

インスタンス ID でターゲットを登録する場合は、Auto Scaling グループでロードバランサーを使用できます。Auto Scaling グループにターゲットグループをアタッチすると、ターゲットの起動時に Auto Scaling によりターゲットグループにターゲットが登録されます。詳細については、『Amazon EC2 Auto Scaling ユーザーガイド』の「Auto Scaling グループにロードバランサーをアタッチする」を参照してください。

制限

- インスタンス ID がC1、CC1、CC2、CG1、CG2、CR1、G1、G2、HI1、HS1、M1、M2、M3、および T1 のインスタンス ID でインスタンスを登録することはできません。IP アドレスで、これらの種類のインスタンスを登録することができます。
- ピア接続 VPC 内のインスタンスをインスタンス ID で登録することはできません。IP アドレスで登録する必要があります。

ターゲットグループの属性

ターゲット グループの属性は次のとおりです。

`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 が待機する時間の長さです。範囲は 0 ~ 3600 秒です。デフォルト値は 300 秒です。

`proxy_protocol_v2.enabled`

Proxy Protocol バージョン 2 が有効になっているかどうかを示します。Proxy Protocol は、デフォルトで無効になっています。

登録解除の遅延

Elastic Load Balancing は、登録解除するインスタンスへのリクエストの送信を停止します。Connection Drainingを行うと、既存の接続が終了する前に未処理のリクエストが完了します。登録解除するターゲッ

トの初期状態は `draining` です。デフォルトでは、登録解除するターゲット状態は 300 秒後に `unused` に変化します。状態が `unused` に変わるのを Elastic Load Balancing が待機する時間の長さを変更するには、登録解除の遅延値を更新します。リクエストを確実に完了するには、120 秒以上の値を指定することをお勧めします。

コンソールを使用して登録解除の遅延値を更新するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ナビゲーションペインの [LOAD BALANCING] で [Target Groups] を選択します。
3. ターゲットグループを選択します。
4. [Description]、[Edit attributes] を選択します。
5. 必要に応じて [Deregistration delay] の値を変更し、[Save] を選択します。

AWS CLI を使用して登録解除の遅延値を更新するには

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

Proxy Protocol

Network Load Balancer は、Proxy Protocol バージョン 2 を使用して、送信元と送信先などの追加の接続情報を送信します。Proxy Protocol バージョン 2 は、Proxy Protocol ヘッダーのバイナリエンコードを提供します。ロードバランサーは TCP データにプロキシプロトコルヘッダーを付加します。既存のデータは破棄または上書きされません。これには、ネットワークパスのクライアントまたは他のプロキシ、ロードバランサー、またはサーバーによって送信されたプロキシプロトコルヘッダーが含まれます。したがって、複数のプロキシプロトコルヘッダーを受け取ることができます。また、Network Load Balancer の外部のターゲットへの別のネットワークパスが存在する場合、最初のプロキシプロトコルヘッダーは、Network Load Balancer からのものでない可能性があります。

ターゲットを IP アドレスで指定する場合、アプリケーションに提供される送信元 IP アドレスはロードバランサーノードのプライベート IP アドレスとなります。アプリケーションでクライアントの IP アドレスが必要な場合は、Proxy Protocol を有効にし、Proxy Protocol ヘッダーからクライアント IP アドレスを取得します。

インスタンス ID でターゲットを指定すると、アプリケーションに提供される送信元 IP アドレスは、クライアントの IP アドレスになります。ただし、必要に応じて Proxy Protocol を有効にし、Proxy Protocol ヘッダーからクライアント IP アドレスを取得できます。

ヘルスチェックの接続

Proxy Protocol を有効にした後、Proxy Protocol ヘッダーも、ロードバランサーからのヘルスチェック接続に含まれます。ただし、ヘルスチェック接続では、クライアント接続情報は Proxy Protocol ヘッダーでは送信されません。

VPC エンドポイントサービス

VPC エンドポイントを通じたサービスコンシューマーからのトラフィックの場合、アプリケーションに提供される送信元の IP アドレスは、ロードバランサーノードのプライベート IP アドレスです。アプリケーションでサービスコンシューマーの IP アドレスが必要な場合は、Proxy Protocol を有効にし、Proxy Protocol ヘッダーからその IP アドレスを取得します。

Proxy Protocol ヘッダーには、エンドポイントの ID も含まれています。この情報は、次のようにカスタム Type-Length-Value (TLV) ベクトルを使用してエンコードされます。

フィールド	長さ (オクテット単位)	説明
タイプ	1	PP2_TYPE_AWS (0xEA)
長さ。	2	値の長さ
値	1	PP2_SUBTYPE_AWS_VPCE_ID (0x01)
	変数 (値の長さから 1 を引いた値)	エンドポイントの ID

TLV タイプ 0xEA を解析する例については、https://github.com/aws/elastic-load-balancing-tools/tree/master/proprot を参照してください。

Proxy Protocol の有効化

ターゲットグループで Proxy Protocol を有効にする前に、アプリケーションが Proxy Protocol v2 ヘッダーを予期し、解析できることを確認します。それ以外の場合、アプリケーションは失敗する可能性があります。詳細については、「Proxy Protocol バージョン 1 および 2」を参照してください。

コンソールを使用して Proxy Protocol を有効化するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ナビゲーションペインの [LOAD BALANCING] で [Target Groups] を選択します。
3. ターゲットグループを選択します。
4. [Description]、[Edit attributes] を選択します。
5. [Enable proxy protocol v2] を選択し、[Save] を選択します。

AWS CLI を使用して Proxy Protocol を有効化するには

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

Network Load Balancer のターゲットグループを作成するには

ターゲットグループに Network Load Balancer のターゲットを登録します。デフォルトでは、ロードバランサーはターゲットグループに指定したポートとプロトコルを使用して登録済みターゲットにリクエストを送信します。ターゲットグループに各ターゲットを登録するときに、このポートを上書きできます。

ターゲットグループを作成すると、タグを追加できます。

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、「リスナールール (p. 17)」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、「ターゲットグループへのターゲットの登録 (p. 33)」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、「ターゲットグループのヘルスチェック設定を変更する (p. 32)」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. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。

2. ナビゲーションペインの [LOAD BALANCING] で [Target Groups] を選択します。
3. [Create target group] を選択します。
4. [Target group name] で、ターゲットグループの名前を入力します。
5. [プロトコル] で、[TCP] または [TLS] を選択します。
6. (オプション) [Port] で、必要に応じてデフォルト値を変更します。
7. [Target type] には、`instance` 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` を選択して IP アドレスでターゲットを指定します。
8. [VPC] で、Virtual Private Cloud (VPC) を選択します。
9. (オプション) [Health check settings] と [Advanced health check settings] で、必要に応じてデフォルト設定を変更します。[Create] を選択します。
10. (オプション) 次のように 1 つ以上のタグを追加します。
    a. 新しく作成したターゲットグループを選択します。
    b. [Tags]、[Add/Edit Tags] を選択します。
    c. [Add/Edit Tags] ページで、追加したタグごとに [Create Tag] を選択し、タグキーとタグの値を指定します。タグの追加を完了したら、[Save] を選択します。
11. (オプション) ターゲットグループにターゲットを追加する方法については、「ターゲットグループへのターゲットの登録 (p. 33)」を参照してください。

AWS CLI を使用してターゲットグループを作成するには

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

ターゲットグループのヘルスチェック

Network Load Balancer はアクティブおよびパッシブヘルスチェックを使用して、ターゲットがリクエストを処理できるかどうかを判断します。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リクエストをルーティングします。クロスゾーン負荷分散を有効にすると、各ロードバランサーノードは、有効なすべてのアベイラビリティーゾーンの正常な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、「クロスゾーン負荷分散 (p. 11)」を参照してください。

アクティブなヘルスチェックを使用すると、ロードバランサーは、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。各ロードバランサーノードは、ターゲットが登録されているターゲットグループのヘルスチェック設定を使用して、各ターゲットの状態を確認します。各ヘルスチェックが完了すると、ロードバランサーノードはヘルスチェック用に確立された接続を終了します。

パッシブのヘルスチェックでは、ロードバランサーはターゲットの接続への応答状態を確認します。パッシブのヘルスチェックでは、ロードバランサーはアクティブのヘルスチェックで異常が報告される前に異常なターゲットを検出できます。パッシブなヘルスチェックは無効、設定、または監視することはできません。

1 つ以上のターゲットグループで、有効にされたアベイラビリティゾーン内に正常なターゲットがない場合、DNS から該当するサブネットの IP アドレスを削除し、そのアベイラビリティーゾーンのターゲットにリクエストをルーティングできないようにします。各ターゲットグループで正常なターゲットがあるアベイラビリティーゾーンがない場合、リクエストはすべての有効なアベイラビリティーゾーンのターゲットにルーティングされます。

TLS リスナーを Network Load Balancer に追加すると、リスナーの接続テストが実行されます。TLS の終了では TCP 接続も終了され、新しい TCP 接続がロードバランサーとターゲット間で確立されます。したがって、TLS リスナーに登録されたターゲットに対してロードバランサーからこのテスト用に送信された

TCP ping が表示される場合があります。これらの TCP ping は識別できます。Network Load Balancer のソース IP アドレスがあり、接続にデータパケットは含まれていないためです。

ヘルスチェックの設定

次の設定を使用して、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。ロードバランサーは、指定されたポート、プロトコル、および ping パスを使用して、HealthCheckIntervalSeconds 秒ごとに、登録された各ターゲットにヘルスチェックリクエストを送信します。次に、ターゲットが応答タイムアウト期間内に応答するのを待ちます。ヘルスチェックが連続して失敗した応答の数のしきい値を超えると、ロードバランサーはターゲットをサービス停止中の状態にします。ヘルスチェックが連続して成功した応答の数のしきい値を超えると、ロードバランサーはターゲットをサービス提供中の状態に戻します。

設定	説明
HealthCheckProtocol	ターゲットでヘルスチェックを実行するときにロードバランサーが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 プロトコルです。
HealthCheckPort	ターゲットでヘルスチェックを実行するときにロードバランサーが使用するポート。デフォルトでは、ターゲットがロードバランサーからトラフィックを受信するポートが使用されます。
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 ping 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)。これは、TCP および HTTPS ヘルスチェックの場合は 10 秒、HTTP ヘルスチェックの場合は 6 秒です。
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)。この値は 10 秒または 30 秒となります。デフォルト値は 30 秒です。 **Important** Network 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。そのため、ターゲットは設定されているヘルスチェック数よりも多くのヘルスチェックを受ける場合があります。HTTP ヘルスチェックを使用している場合にターゲットへの影響を軽減するには、静的 HTML ファイルなどより単純な送信先をターゲットで使用するか、TCP ヘルスチェックに切り替えます。
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 3 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。この

設定	説明
	値は正常なしきい値カウントと同じでなければなりません。
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

ロードバランサー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。

値	説明
`initial`	ロードバランサーは、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。
`healthy`	ターゲットは正常です。
`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。
`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ません。または、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ります。
`draining`	ターゲットは登録解除中で、Connection Draining中です。

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、コンソールではツールヒントで同じ説明が表示されます。`Elb` で始まる理由コードはロードバランサー側で発生し、`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`	進行中の最初のヘルスチェック
`Elb.InternalError`	内部エラーのため、ヘルスチェックが失敗しました
`Elb.RegistrationInProgress`	ターゲットの登録中です
`Target.DeregistrationInProgress`	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

理由コード	説明
	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.NotInUse`	ターゲットグループは、ロードバランサー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 ロードバランサー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
`Target.ResponseCodeMismatch`	次のコードでヘルスチェックに失敗しました: [code]
`Target.Timeout`	リクエストがタイムアウトしました

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. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ナビゲーションペインの [LOAD BALANCING] で [Target Groups] を選択します。
3. ターゲットグループを選択します。
4. [Targets] を選択し、[Status] 列の各ターゲットのステータスを表示します。ステータスの値が `Healthy` 以外の場合は、詳細についてツールヒントを参照してください。

AWS CLI 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

describe-target-health 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。

ターゲットグループのヘルスチェック設定を変更する

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。ターゲットグループのプロトコルが TCP である場合、ヘルスチェックプロトコル、間隔、タイムアウト、または成功コードを変更できません。

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. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ナビゲーションペインの [LOAD BALANCING] で [Target Groups] を選択します。
3. ターゲットグループを選択します。
4. [Health checks]、[Edit] を選択します。
5. [Edit target group] ページで、必要に応じて設定を変更し、[Save] を選択します。

AWS CLI 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

modify-target-group コマンドを使用します。

ターゲットグループへのターゲットの登録

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。各ターゲットグループでは、ロードバランサー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。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。詳細については、「Network Load Balancer のターゲットグループ (p. 24)」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。ターゲットがリクエストを処理する準備ができたら、ターゲットグループに登録します。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、ロードバランサー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。

登録済みターゲットの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登録解除できます。登録解除するとすぐに、ロードバランサーはターゲットへのリクエストのルーティングを停止します。ターゲットがリクエストを受信する準備ができたら、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。

インスタンス ID でターゲットを登録する場合は、Auto Scaling グループでロードバランサーを使用できます。Auto Scaling グループにターゲット・グループを接続し、そのグループがスケールアウトすると、Auto Scaling グループによって起動されたインスタンスが自動的にターゲットグループに登録されます。Auto Scaling グループからロードバランサーをデタッチした場合、インスタンスはターゲットグループから自動的に登録解除されます。詳細については、Amazon EC2 Auto Scaling ユーザーガイドの「Auto Scaling グループにロードバランサーをアタッチする」を参照してください。

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がリスナーポートとヘルスチェックポートの両方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。

制限

- Network Load Balancer には関連する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。
- ターゲットのセキュリティグループで、クライアント用のセキュリティグループを使用して、ロードバランサーを通じてクライアントからターゲットにトラフィックを許可することはできません。代わりに、ターゲットセキュリティグループでクライアント CIDR ブロックを使用します。

推奨ルール

Inbound		
Source	Port Range	Comment
`###### IP ####`	*`##########`*	インスタンスリスナーポートでクライアントからのトラフィックを許可します。
`VPC CIDR`	*`#######`*	ヘルスチェックポートでロードバランサーからのトラフィックを許可する

VPC CIDR 全体へのアクセスを許可しない場合は、ロードバランサーノードが使用するプライベート IP アドレスへのアクセスを許可できます。ロードバランサーのサブネットあたり 1 つの IP アドレスがあります。これらのアドレスを見つけるには、次の手順を使用します。

ホワイトリストにプライベート IP アドレスを見つけるには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ナビゲーションペインで、[Network Interfaces] を選択します。
3. 検索フィールドに Network Load Balancer の名前を入力します。ロードバランサーのサブネットあたり 1 つのネットワークインターフェイスがあります。
4. 各ネットワークインターフェイスの [Details (詳細)] タブで、[プライマリプライベート IPv4] からアドレスをコピーします。

ネットワーク ACL

VPC のデフォルトネットワークアクセスコントロールリスト (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が許可されます。カスタムネットワーク ACL を作成する場合、リスナーポート、ヘルスチェックポート、および一時ポート (1024-65535) で、ロードバランサーとインスタンスの双方向の通信を許可する必要があります。

ターゲットの登録または登録解除

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、「ターゲットの種類 (p. 24)」を参照してください。

制限

- インスタンス ID がC1、CC1、CC2、CG1、CG2、CR1、G1、G2、HI1、HS1、M1、M2、M3、および T1 のインスタンス ID でインスタンスを登録することはできません。IP アドレスで、これらの種類のインスタンスを登録することができます。
- ピア接続 VPC 内のインスタンスをインスタンス ID で登録することはできません。IP アドレスで登録する必要があります。

コンテンツ

インスタンス ID によるターゲットの登録または登録解除

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。

インスタンス ID でターゲットを登録または登録解除するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ナビゲーションペインの [LOAD BALANCING] で [Target Groups] を選択します。
3. ターゲットグループを選択します。
4. [Targets]、[Edit] の順に選択します。
5. (オプション) [Registered instances] で、登録解除するインスタンスを選択して [Remove] を選択します。

6. (オプション) [Instances] で、登録する実行中のインスタンスを選択し、必要に応じてデフォルトインスタンスポートを変更して、[Add to registered] を選択します。
7. [Save] を選択します。

IP アドレスによるターゲットの登録または登録解除

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
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

IPアドレスでターゲットを登録または登録解除するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ナビゲーションペインの [LOAD BALANCING] で [Target Groups] を選択します。
3. ターゲットグループを選択し、[Targets]、[Edit] の順に選択します。
4. IP アドレスを登録するには、メニューバーの [Register targets] アイコン (プラス記号) を選択します。各 IP アドレスに対して、ネットワーク、アベイラビリティゾーン、IP アドレス、およびポートを指定し、[Add to list] を選択します。アドレスの指定が終了したら、[Register] を選択します。
5. IP アドレスを登録解除するには、メニューバーの [Deregister targets] アイコン (マイナス記号) を選択します。登録済みの IP アドレスが多い場合は、フィルタを追加したりソート順を変更したりすると便利です。IP アドレスを選択し、[Deregister] を選択します。
6. この画面から抜けるには、メニューバーの [Back to target group] (戻るボタン) を選択します。

AWS CLI を使用してターゲットを登録または登録解除する

ターゲットを追加するには register-targets コマンドを使用し、ターゲットを削除するには deregister-targets コマンドを使用します。

ターゲットグループのタグ

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

- 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)

- タグのキーと値で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。
- タグの名前または値に `aws:` プレフィックスは使用しないでください。このプレフィックスは AWS 用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. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ナビゲーションペインの [LOAD BALANCING] で [Target Groups] を選択します。
3. ターゲットグループを選択します。
4. [Tags] タブで、[Add/Edit Tags] を選択し、次のうち 1 つ以上を選択します。
   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、[Key] と [Value] の値を入力します。
   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。

AWS CLI を使用してターゲットグループのタグを更新するには

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

ターゲットグループの削除

どのアクションからも参照されていない場合、ターゲットグループを削除できます。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。EC2 インスタンスが必要なくなった場合、インスタンスを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. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ナビゲーションペインの [LOAD BALANCING] で [Target Groups] 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、[Yes] を選択します。

AWS CLI を使用してターゲットグループを削除するには

delete-target-group コマンドを使用します。

Network Load Balancer を監視する

次の機能を使用して、ロードバランサーの監視、トラフィックパターンの分析、ロードバランサーとターゲットに関する問題の解決を実行できます。

CloudWatch メトリクス

Amazon CloudWatch を使用して、ロードバランサー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、「Network Load Balancer の CloudWatch メトリクス (p. 37)」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、Network 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「VPC フローログ」を参照してください。

ロードバランサー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。ロードバランサーのサブネットあたり 1 つのネットワークインターフェイスがあります。Network 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ロードバランサーの名前を探します。

Network 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ロードバランサー間のフロントエンド接続で、もう 1 つはロードバランサー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、ロードバランサーサブネットのネットワーク ACL で許可される場合、ロードバランサー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。

アクセスログ

アクセスログを使用して、ロードバランサーに送信される TLS リクエストについて、詳細情報を収集できます。ログファイルは Amazon S3 に保存されます。これらのアクセスログを使用して、トラフィックパターンの分析や、ターゲットの問題のトラブルシューティングを行うことができます。詳細については、「Network Load Balancer のアクセスログ (p. 41)」を参照してください。

CloudTrail ログ

AWS CloudTrail を使用して、Elastic Load Balancing API に対して行われた呼び出しに関する詳細情報をキャプチャし、Amazon S3 でログファイルとして保存できます。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、「AWS CloudTrail を使用した Network Load Balancer の API コールのログ記録 (p. 45)」を参照してください。

Network Load Balancer の CloudWatch メトリクス

Elastic Load Balancing は、ロードバランサーとターゲットに関するデータポイントを Amazon CloudWatch に発行します。CloudWatch を使用すると、それらのデータポイントについての統計を、順序

付けられた時系列データのセット (メトリクスと呼ばれる) 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。たとえば、指定した期間中のロードバランサーの正常なターゲットの合計数を監視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。たとえば、メトリクスが許容範囲外になる場合、CloudWatch アラームを作成して、指定されたメトリクスを監視し、アクション (E メールアドレスに通知を送信するなど) を開始することができます。

Elastic Load Balancing は、リクエストがロードバランサーを経由する場合のみ、メトリクスを CloudWatch に報告します。ロードバランサーを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。ロードバランサ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。

コンテンツ

Network Load Balancerメトリクス

`AWS/NetworkELB` 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。このメトリクスには、SYN_SENT 状態と ESTABLISHED 状態の接続が含まれます。TCP 接続はロードバランサで終了しないため、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カウントされます。 統計: 最も有用な統計は `Average`、`Maximum`、および `Minimum` です。
`ActiveFlowCount_TLS`	クライアントからターゲットへの同時 TLS フロー (または接続) の合計数。このメトリクスには、ESTABLISHED 状態の接続のみが含まれます。 統計: 最も有用な統計は `Average`、`Maximum`、および `Minimum` です。
`ClientTLSNegotiationErrorCount`	クライアントと TLS リスナー間でネゴシエーション中に失敗した TLS ハンドシェイクの合計数。 統計: 最も有用な統計は `Sum` です。
`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、「Elastic Load Balancing 料金表」を参照してください。
`HealthyHostCount`	正常と見なされるターゲットの数。 Statistics: 最も有用な統計は `Maximum` および `Minimum` です。

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。 統計: 最も有用な統計は Sum です。
NewFlowCount_TLS	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 TLS フロー (または接続) の合計数。 統計: 最も有用な統計は Sum です。
ProcessedBytes	TCP/IP ヘッダーを含む、ロードバランサーによって処理された合計バイト数。 統計: 最も有用な統計は Sum です。
ProcessedBytes_TLS	TLS リスナーによって処理される総バイト数。 統計: 最も有用な統計は Sum です。
TargetTLSNegotiationErrorCount	TLS リスナーとターゲット間でネゴシエーション中に失敗した TLS ハンドシェイクの合計数。 統計: 最も有用な統計は Sum です。
TCP_Client_Reset_Count	クライアントからターゲットに送信されたリセット (RST) パケットの合計数。これらのリセットは、クライアントによって生成され、ロードバランサーによって転送されます。 統計: 最も有用な統計は Sum です。
TCP_ELB_Reset_Count	ロードバランサーによって生成されたリセット (RST) パケットの合計数。 統計: 最も有用な統計は Sum です。
TCP_Target_Reset_Count	ターゲッ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。これらのリセットは、ターゲットによって生成され、ロードバランサーによって転送されます。 統計: 最も有用な統計は Sum です。
UnHealthyHostCount	異常と見なされるターゲットの数。 Statistics: 最も有用な統計は Maximum および Minimum です。

Network Load Balancer のメトリクスディメンション

ロードバランサー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
AvailabilityZone	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	ロードバランサーでメトリクスデータをフィルタリングします。 ロードバランサーを次のように指定します。net/ロードバランサー名/1234567890123456 (ロードバランサー ARN の最後の部分)。

ディメンション	説明
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)。

Network Load Balancer メトリクスの統計

CloudWatch では、Elastic Load Balancing で発行されたメトリクスのデータポイントに基づいて統計が提供されます。統計とは、メトリクスデータを指定した期間で集約したものです。統計を要求した場合、返されるデータストリームはメトリクス名とディメンションによって識別されます。ディメンションは、メトリクスを一意に識別する名前/値のペアです。たとえば、特定のアベイラビリティーゾーンで起動されたロードバランサーの配下のすべての正常な EC2 インスタンスの統計をリクエストできます。

Maximum および Minimum の統計は、各サンプリングウィンドウの個別のロードバランサーノードから報告されるデータポイントの最小値と最大値を反映します。HealthyHostCount の最大値の増加は、UnHealthyHostCount の最小値の減少に対応します。したがって、HealthyHostCount の最大値または UnHealthyHostCount の最小値のいずれかを使用して Network Load Balancer をモニタリングすることをお勧めします。

Sum 統計は、すべてのロードバランサーノードにおける集計値です。メトリクスには期間あたり複数のレポートが含まれているため、Sum はすべてのロードバランサーノードで集計されたメトリクスのみに適用されます。

SampleCount 統計は測定されたサンプルの数です。メトリクスはサンプリング間隔とイベントに基づいて集計されるため、通常、この統計は有用ではありません。たとえば、HealthyHostCount の SampleCount は、正常なホストの数ではなく各ロードバランサーノードが報告するサンプル数に基づいています。

ロードバランサーの CloudWatch メトリクスを表示する

Amazon EC2 コンソールを使用して、ロードバランサーに関する 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。ロードバランサ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。

または、CloudWatch コンソールを使用してロードバランサーのメトリクスを表示できます。

Amazon EC2 コンソールを使用してメトリクスを表示するには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. 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。
3. ロードバランサー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、[Load Balancers] を選択します。
   b. ロードバランサーを選択し、[Monitoring] 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. https://console.aws.amazon.com/cloudwatch/にある CloudWatch コンソールを開きます。
2. ナビゲーションペインで メトリクスを選択します。
3. [NetworkELB] 名前空間を選択します。
4. (オプション) すべてのディメンションでメトリクスを表示するには、検索フィールドに名称を入力します。

AWS CLI を使用してメトリクスを表示するには

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

```
aws cloudwatch list-metrics --namespace AWS/NetworkELB
```

AWS CLI を使用してメトリクスの統計を取得するには

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/NetworkELB \
--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
```

出力例を次に示します。

```
{
    "Datapoints": [
        {
            "Timestamp": "2017-04-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2017-04-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

Network Load Balancer のアクセスログ

Elastic Load Balancing は、Network Load Balancer に送信される TLS リクエストについて、詳細情報を収集するアクセスログを提供します。これらのアクセスログを使用して、トラフィックパターンの分析や、問題のトラブルシューティングを行うことができます。

Important

アクセスログが作成されるのは、ロードバランサーに TLS リスナーがあり、TLS リクエストに関する情報のみを含む場合のみです。

アクセスログの作成は、Elastic Load Balancing のオプション機能であり、デフォルトでは無効化されています。ロードバランサーのアクセスログの作成を有効にすると、Elastic Load Balancing はログを圧縮ファイルとしてキャプチャし、指定した Amazon S3 バケット内に保存します。アクセスログの作成はいつでも無効にできます。

S3 バケットに対して、Amazon S3 管理の暗号化キーによるサーバー側の暗号化 (SSE-S3) を有効にした場合、各アクセスログファイルは、S3 バケットに保存される前に自動的に暗号化され、アクセス時に復号されます。暗号化あるいは復号化されたログファイルにアクセスする方法に違いがないため、特別なアクションを実行する必要はありません。各ログファイルは、一意のキーで暗号化されます。この一意のキー自体が、定期的に更新されるマスターキーで更新されます。詳細については、Amazon Simple Storage Service 開発者ガイドの「Amazon S3 で管理された暗号化キーによるサーバー側の暗号化 (SSE-S3) を使用したデータの保護」を参照してください。

アクセスログに対する追加料金はありません。Amazon S3 のストレージコストは発生しますが、Amazon S3 にログファイルを送信するために Elastic Load Balancing が使用する帯域については料金は発生しません。ストレージコストの詳細については、Amazon S3 料金表を参照してください。

アクセスログファイル

Elastic Load Balancing は各ロードバランサーノードのログファイルを 5 分ごとに発行します。ログ配信には結果整合性があります。ロードバランサーでは、同じ期間について複数のログが発行されることがあります。これは通常、サイトに高トラフィックがある場合に発生します。

アクセスログのファイル名には次の形式を使用します。

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_load-balancer-id_end-time_random-string.log.gz
```

bucket

S3 バケットの名前。

プレフィックス

バケットのプレフィックス (論理階層)。プレフィックスを指定しない場合、ログはバケットのルートレベルに配置されます。

aws-account-id

所有者の AWS アカウント ID。

リージョン

ロードバランサーおよび S3 バケットのリージョン。

yyyy/mm/dd

ログが配信された日付。

load-balancer-id

ロードバランサーのリソース ID。リソース ID にスラッシュ (/) が含まれている場合、ピリオド (.) に置換されます。

end-time

ログ作成の間隔が終了した日時。たとえば、終了時間 20181220T2340Z には、23:35 ~ 23:40 に行われたリクエストのエントリが含まれます。

random-string

システムによって生成されたランダム文字列。

ログファイルは無期限に保管できますが、ログファイルを自動的にアーカイブまたは削除するように Amazon S3 ライフサイクルルールを定義することもできます。詳細については、Amazon Simple Storage Service 開発者ガイド の「オブジェクトのライフサイクル管理」を参照してください。

アクセスログのエントリ

次の表は、アクセスログのエントリのフィールドを順に示しています。すべてのフィールドはスペースで区切られています。新しいフィールドが導入されると、ログエントリの最後に追加されます。ログファイルの処理中に、予期していなかったログエントリの最後のフィールドは無視する必要があります。

フィールド	説明
type	リスナーの種類。サポートされる値は `tls` です。
バージョン	ログエントリのバージョン。サポートされているバージョンは 1.0 です。
timestamp	TLS 接続の最後に記録されたタイムスタンプ (ISO 8601 形式)。
elb	ロードバランサーのリソース ID。
リスナー	接続の TLS リスナーのリソース ID。
client:port	クライアントの IP アドレスとポート。
listener:port	リスナーの IP アドレスとポート。
connection_time	接続が完了するまでの合計時間 (開始から終了まで) (ミリ秒単位)。
tls_handshake_time	TCP 接続が確立された後に TLS ハンドシェイクが完了するまでの合計時間 (クライアント側の遅延時間を含む) (ミリ秒単位)。この時間は connection_time フィールドに含まれています。
received_bytes	クライアントからロードバランサーによって受信されたバイト数 (復号後)。
sent_bytes	ロードバランサーからクライアントに送信されたバイト数 (復号前)。
incoming_tls_alert	クライアントからロードバランサーによって受信された TLS アラートの整数値 (存在する場合)。それ以外の場合、この値は - に設定されます。
chosen_cert_arn	クライアントに提供された証明書の ARN。有効なクライアント hello メッセージが送信されない場合、この値は - に設定されます。
chosen_cert_serial	将来の利用のために予約されています。この値は常に - に設定されます。
tls_cipher	クライアントとネゴシエートされた暗号スイート (OpenSSL 形式)。TLS ネゴシエーションが完了しない場合、この値は - に設定されます。
tls_protocol_version	クライアントとネゴシエートされた TLS プロトコル (文字列形式)。指定できる値は、tlsv10、tlsv11、および tlsv12 です。TLS ネゴシエーションが完了しない場合、この値は - に設定されます。
tls_named_group	将来の利用のために予約されています。この値は常に - に設定されます。
domain_name	クライアント hello メッセージの server_name 拡張機能の値。この値は URL でエンコードされます。有効なクライアント hello メッセージが送信されない場合、または拡張機能が存在しない場合、この値は - に設定されます。

ログエントリの例

ログエントリの例を示します。読みやすくするためだけの目的で、テキストは複数の行に表示されています。

```
tls 1.0 2018-12-20T02:59:40 net/my-network-loadbalancer/c6e77e28c25b2234 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
```

バケットの要件

アクセスログの作成を有効にするときは、アクセスログの S3 バケットを指定する必要があります。バケットは、ロードバランサーを所有するアカウントとは別のアカウントが所有するものでもかまいません。バケットは、次の要件を満たしている必要があります。

要件

- バケットは、ロードバランサーと同じリージョンに配置されている必要があります。
- このバケットには、バケットにアクセスログを書き込む許可を付与するバケットポリシーが必要です。バケットポリシーは、バケットのアクセス許可を定義するためにアクセスポリシー言語で記述された JSON ステートメントのコレクションです。ポリシーの例を次に示します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": [ "delivery.logs.amazonaws.com" ]
      },
      "Action": [ "s3:PutObject" ],
      "Resource": "arn:aws:s3:::bucket_name/prefix/AWSLogs/123456789012/*",
      "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"
    }
  ]
}
```

アクセスログ記録を有効または無効にします。

ロードバランサーのアクセスログの作成を有効にする場合は、ロードバランサーがログを保存する S3; バケットの名前を指定する必要があります。詳細については、「バケットの要件 (p. 44)」を参照してください。

コンソールを使用してアクセスログ記録を有効または無効にするには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。

2. ナビゲーションペインで、[Load Balancers] を選択します。
3. ロードバランサーを選択します。
4. [Description] タブで、[Edit attributes] を選択します。
5. [Edit load balancer attributes] ページで、以下を実行します。
   a. [Enable access logs] を選択します。
   b. [S3 location] に、プレフィックスを含めて S3 バケットの名前を入力します (たとえば `my-loadbalancer-logs/my-app`)。既存のバケットの名前や新しいバケットの名前を指定できます。既存のバケットを指定する場合は、このバケットを所有していること、および必要なバケットポリシーを設定したことを確認します。
   c. [Save] を選択します。

AWS CLI を使用してアクセスログの作成を有効にするには

modify-load-balancer-attributes コマンドを使用します。

アクセスログファイルの処理

アクセス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ファイルを開くと、ファイルは解凍され、情報が表示されます。ファイルをダウンロードする場合、情報を表示するには解凍する必要があります。

ウェブサイトの需要が大きい場合は、ロードバランサーによって数 GB のデータ量のログファイルが生成されることがあります。このような大容量のデータは、行単位で処理できない場合があります。このため、場合によっては、並列処理ソリューションを提供する分析ツールを使用する必要があります。たとえば、次の分析ツールを使用するとアクセスログの分析と処理を行うことができます。

- Amazon Athena は、標準 SQL を使用して Amazon S3 のデータの分析を簡易化するインタラクティブなクエリサービスです。詳細については、Amazon Athena ユーザーガイドの「Network Load Balancer ログのクエリ」を参照してください。
- Loggly
- Splunk
- Sumo Logic

AWS CloudTrail を使用した Network Load Balancer の API コールのログ記録

Elastic Load Balancing は、AWS CloudTrail と統合されています。このサービスは、Elastic Load Balancing でユーザーやロール、または AWS 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す。CloudTrail は、Elastic Load Balancing のすべての API コールをイベントとしてキャプチャします。キャプチャされたコールには、AWS マネジメントコンソール からのコールと、Elastic Load Balancing API オペレーションへのコードコールが含まれます。証跡を作成する場合は、Elastic Load Balancing 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化にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示できます。CloudTrail によって収集された情報を使用して、リクエストの作成元の IP アドレス、リクエストの実行者、リクエストの実行日時などの詳細を調べて、Elastic Load Balancing に対してどのようなリクエストが行われたかを判断できます。

CloudTrail の詳細については、『AWS CloudTrail User Guide』を参照してください。

CloudTrail 内の Elastic Load Balancing 情報

CloudTrail は、アカウント作成時に AWS アカウントで有効になります。Elastic Load Balancing でアクティビティが発生すると、そのアクティビティは [Event history (イベント履歴)] の AWS の他のサービスのイベントとともに CloudTrail イベントに記録されます。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。

Elastic Load Balancingのイベントなど、AWS アカウントのイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで作成した証跡がすべての AWS リージョンに適用されます。証跡では、AWS パーティションのすべてのリージョンからのイベントがログに記録され、指定した Amazon S3 バケットにログファイルが配信されます。さらに、より詳細な分析と AWS ログで収集されたデータに基づいた行動のためにその他の CloudTrail サービスを設定できます。詳細については、以下を参照してください。

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

Network Load Balancer のすべての Elastic Load Balancing アクションは CloudTrail でログが作成され、Elastic Load Balancing API リファレンスバージョン 2015-12-01 に記録されます。たとえば、`CreateLoadBalancer` と `DeleteLoadBalancer` の各アクションを呼び出すと、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。この ID 情報は以下のことを確認するのに役立ちます。

- リクエストが、ルートまたは 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どうか。
- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか.
- リクエストが、別の AWS 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 要素」を参照してください。

Elastic Load Balancing ログファイルエントリの概要

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できる設定です。CloudTrail ログファイルには、1 つ以上のログエントリが含まれます。イベントは任意の送信元からの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメーターなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API コール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。

このログファイルには、Elastic Load Balancing API コールだけでなく、ご使用の AWS アカウントに関するすべての AWS API 呼び出しに関するイベントが含まれます。`elasticloadbalancing.amazonaws.com` の値を使用して `eventSource` 要素を確認することで、Elastic Load Balancing API に対するコールを見つけることができます。`CreateLoadBalancer` などの特定のアクションのレコードを表示するには、アクション名で `eventName` 要素を確認します。

次の例は、AWS CLI を使用して Network Load Balancer を作成後に削除したユーザーの Elastic Load Balancing に関する CloudTrail ログレコードを示しています。`userAgent` 要素を使用して CLI を特定できます。`eventName` 要素を使用して、リクエストされた API コールを特定できます。ユーザーに関する情報 (`Alice`) は `userIdentity` 要素で確認できます。

Example 例: CreateLoadBalancer


```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-8360a9e7","subnet-b7d581c0"],
        "securityGroups": ["sg-5943793c"],
        "name": "my-load-balancer",
        "scheme": "internet-facing",
        "type": "network"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "network",
            "ipAddressType": "ipv4",
            "loadBalancerName": "my-load-balancer",
            "vpcId": "vpc-3ac0fb5f",
            "securityGroups": ["sg-5943793c"],
            "state": {"code":"provisioning"},
            "availabilityZones": [
               {"subnetId":"subnet-8360a9e7","zoneName":"us-west-2a"},
               {"subnetId":"subnet-b7d581c0","zoneName":"us-west-2b"}
            ],
            "dNSName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
            "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
            "createdTime": "Apr 11, 2016 5:23:50 PM",
            "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0",
            "scheme": "internet-facing"
        }]
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```


Example 例: DeleteLoadBalancer


```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
```

```
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0"
    },
    "responseElements": null,
    "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
    "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Network Load Balancer のトラブルシューティング

以下の情報は、Network Load Balancer の問題のトラブルシューティングに役立ちます。

登録されたターゲットが実行中でない

ターゲットが `InService` 状態になるまでに予想以上に時間がかかっている場合、ヘルスチェックに合格していない可能性があります。ターゲットは、ヘルスチェックに合格するまで実行されません。詳細については、「ターゲットグループのヘルスチェック (p. 29)」を参照してください。

インスタンスがヘルスチェックに合格していないことを確認したら、以下についてチェックします。

セキュリティグループでトラフィックが許可されていない

インスタンスに関連付けられたセキュリティグループでは、ヘルスチェックポートとヘルスチェックプロトコルを使用してロードバランサーからのトラフィックを許可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) ではトラフィックが許可されない

インスタンスのサブネットに関連付けられたネットワーク ACL では、ヘルスチェックポートでインバウンドトラフィックを許可し、一時ポート (1024-65535) でアウトバウンドトラフィックを許可する必要があります。ロードバランサーノードのサブネットに関連付けられたネットワーク ACL では、一時ポートでインバウンドトラフィックを許可し、ヘルスチェックおよび一時ポートでアウトバウンドトラフィックを許可する必要があります。

リクエストがターゲットにルーティングされない

以下を確認します。

セキュリティグループでトラフィックが許可されていない

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は、リスナーポートからクライアント IP アドレス (ターゲットがインスタンス ID で指定されている場合) またはロードバランサーノード (ターゲットが IP アドレスで指定されている場合) へのトラフィックが許可されている必要があります。

ネットワークアクセスコントロールリスト (ACL) ではトラフィックが許可されない

VPC のサブネットに関連付けられているネットワーク ACL では、リスナーポートでロードバランサーとターゲットの双方向の通信が許可されている必要があります。

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る

ターゲットをアベイラビリティーゾーンに登録したが、アベイラビリティーゾーンを有効にしていない場合、登録したターゲットはロードバランサーからのトラフィックを受信しません。

インスタンスがピア接続 VPC にある

ピア接続 VPC 内にあるインスタンスは、インスタンス ID ではなく、IP アドレスでロードバランサーに登録する必要があります。

ターゲットが受け取るヘルスチェックリクエストが想定よりも多い

Network 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。そのため、ターゲットは `HealthCheckIntervalSeconds` 設定で設定されているヘルスチェック数よりも多くのヘルスチェックを受ける場合があります。

ターゲットが受け取るヘルスチェックリクエストが想定よりも少ない

`net.ipv4.tcp_tw_recycle` が有効化されているかどうかを確認します。この設定は、ロードバランサーに関する問題が発生することが判っています。`net.ipv4.tcp_tw_reuse` 設定の方が安全であると見なされています。

異常なターゲットがロードバランサーからリクエストを受信する

ロードバランサーに対して少なくとも 1 つの正常な登録済みターゲットがある場合、ロードバランサーは正常な登録済みターゲットにのみリクエストをルーティングします。異常な登録済みターゲットのみがある場合、ロードバランサーはすべての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。

ターゲットからそのロードバランサーへのリクエストが接続タイムアウトになる

インスタンス ID でターゲットが登録されている内部ロードバランサーがあるかどうかを確認します。内部ロードバランサーはヘアピニングまたはループバックをサポートしていません。インスタンス ID でターゲットを登録すると、クライアントの送信元 IP アドレスが維持されます。インスタンスが、インスタンス ID で登録されている内部ロードバランサーのクライアントである場合、リクエストが別のインスタンスにルーティングされる場合のみ接続が成功します。それ以外の場合は、送信元と送信先の IP アドレスが同じであるため、接続がタイムアウトします。

インスタンスが、それが登録されているロードバランサーにリクエストを送信する必要がある場合は、次のいずれかを実行します。

- インスタンス ID ではなく IP アドレスでインスタンスを登録するAmazon Elastic Container Service を使用している場合は、タスクで `awsvpc` ネットワークモードを使用して、ターゲットグループが IP アドレスで登録されるようにします。
- 通信する必要があるコンテナが異なるコンテナインスタンスにあることを確認します。
- インターネット向けロードバランサーを使用します。

Network Load Balancer にターゲットを移動する際にパフォーマンスが低下する

クラシックロードバランサー と Application Load Balancer はどちらも接続の多重化を使用しますが、Network Load Balancer は使用しません。したがって、ターゲットは Network Load Balancer の背後で複数の TCP 接続を受け取ることができます。必ず、ターゲットが受信する可能性のある接続リクエストのボリュームを処理できるようにしてください。

AWS PrivateLink を介した接続のポート割り当てエラー

Network 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、ロードバランサーは一意の各ターゲット (IP アドレスとポート) に対して 55,000 の同時接続または 1 分あたり約 55,000 の接続をサポートできます。これらの接続数を超えた場合、ポート割り当てエラーが発生する可能性が高くなります。ポート割り当てエラーを修正するには、ターゲットグループにさらに多くのターゲットを追加します。

Network Load Balancer の制限

Network Load Balancer の現在の制限を表示するには、Amazon EC2 コンソールの [制限] ページ、または describe-account-limits (AWS CLI) コマンドを使用します。制限の緩和をリクエストするには、Elastic Load Balancing 制限フォームを使用します。

AWS アカウントに Network Load Balancer に関連した以下の制限があります。

リージョンの制限

- リージョンごとの Network Load Balancer: 20
- リージョンあたりのターゲットグループの数: 3000 *

ロードバランサーの制限

- ロードバランサーあたりのリスナーの数: 50
- ロードバランサーあたりのアベイラビリティーゾーンあたりのサブネット: 1
- [クロスゾーン負荷分散無効] ロードバランサー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: 500
- [クロスゾーン負荷分散有効] ロードバランサーあたりのターゲット: 500
- ターゲットグループあたりのロードバランサーの数: 1

* この制限は、Application Load Balancer および Network Load Balancer のターゲットグループによって共有されます。

Network Load Balancer のドキュメント履歴

次の表では、Network Load Balancer のリリースを説明しています。

update-history-change	update-history-description	update-history-date
TLS プロトコル	このリリースでは、TLS プロトコルのサポートが追加されました。	January 24, 2019
クロスゾーン負荷分散 (p. 53)	このリリースでは、クロスゾーン負荷分散を有効にするためのサポートを追加しています。	February 22, 2018
Proxy Protocol	このリリースでは、Proxy Protocol を有効にするためのサポートが追加されます。	November 17, 2017
IP アドレスをターゲットに設定	このリリースでは、IP アドレスをターゲットとして登録する機能のサポートを追加しています。	September 21, 2017
新しい種類のロードバランサー (p. 53)	このリリースの Elastic Load Balancing では Network Load Balancer を導入しています。	September 7, 2017