AWS トランジットゲートウェイ

Amazon VPC

Amazon VPC: AWS トランジットゲートウェイ

Table of Contents

Amazon VPC Transit Gateway とは

Amazon VPC Transit Gateways は、仮想プライベートクラウド (VPCs) とオンプレミスネットワークを相互接続するために使用されるネットワークトランジットハブです。クラウドインフラストラクチャがグローバルに拡張されると、リージョン間ピアリングは AWS グローバルインフラストラクチャを使用してトランジットゲートウェイを接続できます。 AWS データセンター間のすべてのネットワークトラフィックは、物理層で自動的に暗号化されます。Amazon VPC Transit Gateways は Amazon Virtual Private Cloud (VPC) のサービスで、Amazon VPC コンソールの https://console.aws.amazon.com/vpc/home#vpc/ からアクセスできます。

詳細については、「AWS Transit Gateway」を参照してください。

Transit Gateway の概念

Transit Gateway の主要な概念を次に示します。

- アタッチメント — 次をアタッチできます。
  - 1 つ以上のVPCs
  - Connect SDWAN/サードパーティーのネットワークアプライアンス
  - AWS Direct Connect ゲートウェイ
  - 別のTransit Gateway とのピア接続
  - トランジットゲートウェイVPNへの接続
- トランジットゲートウェイの最大送信単位 (MTU) — ネットワーク接続の最大送信単位 (MTU) は、接続を通過できる最大許容パケットのサイズをバイト単位で表したものです。接続MTU の が大きいほど、1 つのパケットで渡すことができるデータが多くなります。Transit Gateway は、VPCs、、Transit Gateway Connect AWS Direct Connect、ピアリングアタッチメント (リージョン内、リージョン間、およびクラウドWANピアリングアタッチメント) 間のトラフィックに対して 8500 バイトMTUの をサポートします。VPN 接続経由MTUのトラフィックは、1500 バイトの を持つことができます。
- Transit Gateway ルートテーブル — Transit Gateway にはデフォルトのルートテーブルがあり、オプションで追加のルートテーブルを含めることができます。ルートテーブルには、パケットの宛先 IP アドレスに基づいてネクストホップを決定する動的ルートと静的ルートが含まれます。これらのルートのターゲットは、Transit Gateway のアタッチメントである場合があります。デフォルトでは、Transit Gateway アタッチメントはデフォルトの Transit Gateway ルートテーブルに関連付けられます。

- 関連付け — 各アタッチメントは、正確に 1 つのルートテーブルに関連付けられます。各アタッチメントは、正確に 1 つのルートテーブルに関連付けることができます。
- ルート伝達 — VPC、VPN接続、または Direct Connect ゲートウェイは、ルートをトランジットゲートウェイルートテーブルに動的に伝達できます。Connect アタッチメントでは、ルートはデフォルトで Transit Gateway ルートテーブルに伝達されます。ではVPC、トランジットゲートウェイにトラフィックを送信する静的ルートを作成する必要があります。VPN 接続では、ボーダーゲートウェイプロトコル () を使用して、ルートがトランジットゲートウェイからオンプレミスルーターに伝播されますBGP。Direct Connect ゲートウェイでは、許可されたプレフィックスはを使用してオンプレミスルーターに発信されますBGP。ピアリングアタッチメントでは、ピアリングアタッチメントをポイントする静的ルートをTransit Gateway のルートテーブルに作成する必要があります。

Transit Gateway の開始方法

次のリソースを使用して、Transit Gateway の作成と使用を支援します。

- Transit Gateway の動作
- トランジットゲートウェイの使用を開始する
- 設計のベストプラクティス

Transit Gateway の使用

次のインターフェイスのいずれかを使用して、Transit Gateway の作成、アクセス、管理を行うことができます。

- AWS Management Console — Transit Gateway へのアクセスに使用するウェブインターフェイスを提供します。
- AWS コマンドラインインターフェイス (AWS CLI) — Amazon を含む幅広い AWS のサービス用のコマンドを提供しVPC、Windows、macOS、Linux でサポートされています。詳細については、「AWS Command Line Interface」を参照してください。
- AWS SDKs — 言語固有のAPIオペレーションを提供し、署名の計算、リクエストの再試行処理、エラー処理など、接続の詳細の多くを処理します。詳細については、「」を参照してくださいAWS SDKs。
- クエリ API — HTTPSリクエストを使用して呼び出す低レベルのAPIアクションを提供します。クエリを使用することAPIは、Amazon にアクセスする最も直接的な方法ですがVPC、アプリケー

ションがリクエストに署名するためのハッシュの生成やエラーの処理など、低レベルの詳細を処理する必要があります。詳細については、「Amazon EC2APIリファレンス」を参照してください。

料金

Transit Gateway 上のアタッチメントごとに時間単位で課金され、Transit Gateway で処理されたトラフィック量に対して課金されます。詳細については、AWS Transit Gateway の料金を参照してください。

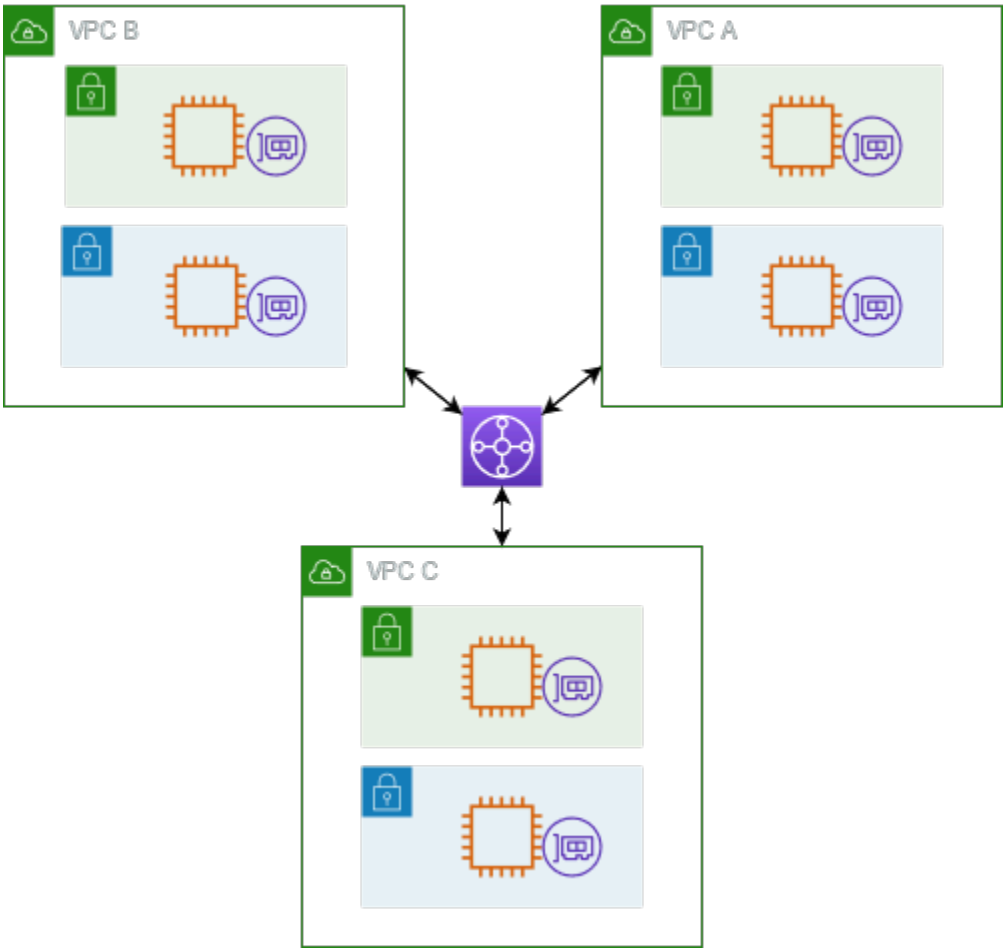
Amazon VPC Transit Gateway の仕組み

AWS Transit Gateway では、トランジットゲートウェイは、仮想プライベートクラウド (VPCs) とオンプレミスネットワーク間を流れるトラフィックのリージョン仮想ルーターとして機能します。Transit Gateway は、ネットワークトラフィックの量に基づいて伸縮自在にスケーリングされます。Transit Gateway を介したルーティングは、レイヤー 3 で動作します。レイヤー 3 では、送信先 IP アドレスに基づいて、パケットが特定のネクストホップ接続に送信されます。

トピック

アーキテクチャ図の例

次の図は、3 つのVPCアタッチメントを持つトランジットゲートウェイを示しています。これらそれぞれのルートテーブルVPCsには、ローカルルートと、他の 2 つ宛てのトラフィックをVPCsトランジットゲートウェイに送信するルートが含まれます。



以下は、前の図に示されているアタッチメントのデフォルト Transit Gateway のルートテーブルの例です。各 のCIDRブロックVPCはルートテーブルに伝播されます。したがって、各アタッチメントは他の 2 つのアタッチメントにパケットをルーティングできます。

デスティネーション	ターゲット	ルートタイプ
VPC A CIDR	*Attachment for VPC A*	伝播済み
VPC B CIDR	*Attachment for VPC B*	伝播済み
VPC C CIDR	*Attachment for VPC C*	伝播済み

リソースアタッチメント

Transit Gateway アタッチメントは、パケットの送信元と送信先の両方です。次のリソースを Transit Gateway にアタッチできます。

- 1 つ以上の VPCs. AWS Transit Gateway がVPCサブネット内に Elastic Network Interface をデプロイし、Transit Gateway が選択したサブネットとの間でトラフィックをルーティングするために使用します。各アベイラビリティーゾーンには、少なくとも 1 つのサブネットが必要です。これにより、そのゾーンのすべてのサブネットのリソースにトラフィックが到達できるようになります。アタッチメントの作成時に、サブネットが同じゾーン内で有効になっている場合にだけ、特定のアベイラビリティーゾーン内のリソースが Transit Gateway に到達できます。サブネットルートテーブルに Transit Gateway へのルートがある場合、トラフィックが Transit Gateway に転送されるのは、Transit Gateway のアタッチメントが同じアベイラビリティーゾーンのサブネットにある場合のみです。
- 1 つ以上のVPN接続
- 1 つ以上の AWS Direct Connect ゲートウェイ
- 1 つまたは複数の Transit Gateway Connect アタッチメント
- 1 つ以上の Transit Gateway ピアリング接続
- Transit Gateway アタッチメントは、パケットの送信元と送信先の両方です。

等コストマルチパスルーティング

AWS Transit Gateway は、ほとんどのアタッチメントで等コストマルチパス (ECMP) ルーティングをサポートしています。VPN アタッチメントの場合、トランジットゲートウェイを作成または変更するときに、コンソールを使用してECMPサポートを有効または無効にできます。他のすべてのアタッチメントタイプには、次のECMP制限が適用されます。

- VPC - CIDRブロックVPCは重複できないECMPため、 は をサポートしていません。例えば、10.1.0.0/16 VPC CIDR の と 1 秒の を同じ VPCを使用してトランジットゲートウェイCIDRにアタッチし、それらの間のトラフィックを負荷分散するようにルーティングを設定することはできません。
- VPN - VPN ECMP サポートオプションが無効になっている場合、トランジットゲートウェイは内部メトリクスを使用して、複数のパスでプレフィックスが等しい場合に優先パスを決定します。VPN アタッチメントの有効化または無効化の詳細については、ECMP「」を参照してくださいthe section called “Transit Gateway”。
- AWS Transit Gateway Connect - AWS Transit Gateway Connect アタッチメントは、 を自動的にサポートしますECMP。
- AWS Direct Connect Gateway - AWS Direct Connect Gateway アタッチメントは、ネットワークプレフィックス、プレフィックスの長さ、および AS_PATH がまったく同じ場合、複数の Direct Connect Gateway アタッチメントECMP間で自動的にサポートされます。

- トランジットゲートウェイピアリング - トランジットゲートウェイピアリングは、動的ルーティングをサポートしておらず、2 つの異なるターゲットに対して同じ静的ルートを設定できないECMPため、 をサポートしていません。

> **Note**
>
> - BGP マルチパス AS-Path relax はサポートされていないため、異なる自律システム番号 () ECMPで を使用することはできませんASNs。
> - ECMP は、異なるアタッチメントタイプ間ではサポートされていません。例えば、 VPNとVPC添付ファイルECMPの間で を有効にすることはできません。代わりに、Transit Gateway ルートが評価され、トラフィックは評価されたルートに従ってルーティングされます。詳細については、「the section called “ルートの評価順序”」を参照してください。
> - 単一の Direct Connect ゲートウェイは、複数のトランジット仮想インターフェイスECMPで をサポートします。したがって、 を利用するために複数のゲートウェイをセットアップして使用しないように、1 つの Direct Connect ゲートウェイのみをセットアップして使用することをお勧めしますECMP。Direct Connect ゲートウェイとパブリック仮想インターフェイスの詳細については、「パブリック仮想インターフェイスAWS から へのアクティブ/アクティブまたはアクティブ/パッシブ Direct Connect 接続を設定する方法」を参照してください。

アベイラビリティーゾーン

VPC をトランジットゲートウェイにアタッチするときは、トランジットゲートウェイがVPCサブネット内のリソースにトラフィックをルーティングするために使用する 1 つ以上のアベイラビリティーゾーンを有効にする必要があります。各アベイラビリティーゾーンを有効にするには、サブネットを 1 つだけ指定します。Transit Gateway は、サブネットから 1 つの IP アドレスを使用して、そのサブネット内にネットワークインターフェイスを配置します。アベイラビリティーゾーンを有効にすると、指定したサブネットやアベイラビリティーゾーンだけでなくVPC、 内のすべてのサブネットにトラフィックをルーティングできます。ただし、Transit Gateway アタッチメントが存在するアベイラビリティーゾーンにあるリソースのみ、Transit Gateway に到達できます。

送信先アタッチメントが存在しないアベイラビリティーゾーンからトラフィックが発信された場合、AWS Transit Gateway はそのトラフィックをアタッチメントが存在するランダムなアベイラビリティーゾーンに内部的にルーティングします。このタイプのクロスアベイラビリティーゾーントラフィックには、Transit Gateway の追加料金はかかりません。

高可用性を確保するために、複数のアベイラビリティーゾーンを有効にすることをお勧めします。

アプライアンスモードサポートの使用

でステートフルネットワークアプライアンスを設定する場合はVPC、アプライアンスが配置されているVPCアタッチメントのアプライアンスモードサポートを有効にできます。これにより、送信元と送信先間のトラフィックフローの存続期間中、トランジットゲートウェイはそのVPCアタッチメントに同じアベイラビリティーゾーンを使用します。また、そのゾーンにサブネットの関連付けがある限りVPC、トランジットゲートウェイは 内の任意のアベイラビリティーゾーンにトラフィックを送信できます。詳細については、「例: 共有サービスのアプライアンス VPC」を参照してください。

ルーティング

トランジットゲートウェイはIPv4、トランジットゲートウェイルートテーブルを使用してアタッチメント間で とIPv6パケットをルーティングします。これらのルートテーブルを設定して、アタッチされた VPCs、VPN接続、および Direct Connect ゲートウェイのルートテーブルからルートを伝達できます。静的ルートを Transit Gateway ルートテーブルに追加することもできます。パケットが 1 つのアタッチメントから送信されると、宛先 IP アドレスと一致するルートを使用して別のアタッチメントにルーティングされます。

Transit Gateway のピアリングアタッチメントでは、静的ルートだけがサポートされます。

ルーティングトピック

- ルートテーブル
- ルートテーブルの関連付け
- ルート伝達
- ピアリングアタッチメントのルート
- ルートの評価順序

ルートテーブル

Transit Gateway ではデフォルトのルートテーブルが自動的に使用されます。デフォルトでは、このルートテーブルはデフォルトの関連付けルートテーブルおよびデフォルトの伝達ルートテーブルです。または、ルート伝達とルートテーブルの関連付けを無効にした場合、 AWS は Transit Gateway のデフォルトルートテーブルを作成しません。

Transit Gateway に対して追加のルートテーブルを作成できます。これにより、アタッチメントのサブネットを分離できます。アタッチメントごとに 1 つのルートテーブルに関連付けることができます。アタッチメントでそのルートを 1 つ以上のルートテーブルに伝播できます。

ルートに一致するトラフィックを破棄する Transit Gateway ルートテーブルでは、ブラックホールルートを作成できます。

をトランジットゲートウェイVPCにアタッチするときは、トラフィックがトランジットゲートウェイを経由するように、サブネットルートテーブルにルートを追加する必要があります。詳細については、「Amazon ユーザーガイド」の「トランジットゲートウェイのルーティング」を参照してください。 VPC

ルートテーブルの関連付け

Transit Gateway アタッチメントを単一のルートテーブルに関連付けることができます。各ルートテーブルは、ゼロから多数のアタッチメントに関連付けられ、パケットを他のアタッチメントに転送できます。

ルート伝達

各アタッチメントには、1 つ以上の Transit Gateway ルートテーブルにインストールできるルートが付属しています。アタッチメントが Transit Gateway ルートテーブルに伝播されると、これらのルートはルートテーブルにインストールされます。アドバタイズされたルートをフィルタリングすることはできません。

VPC アタッチメントの場合、 のCIDRブロックVPCは Transit Gateway ルートテーブルに伝達されます。

アタッチメントまたは Direct Connect ゲートウェイVPNアタッチメントで動的ルーティングを使用する場合、オンプレミスルーターから学習したルートを 経由で任意のトランジットゲートウェイルートテーブルBGPに伝達できます。

動的ルーティングがVPNアタッチメントとともに使用されると、VPNアタッチメントに関連付けられたルートテーブル内のルートは、 を介してカスタマーゲートウェイにアドバタイズされますBGP。

Connect アタッチメントの場合、Connect アタッチメントに関連付けられたルートテーブル内のルートは、 VPC から で実行される SD WANアプライアンスなどのサードパーティーの仮想アプライアンスにアドバタイズされますBGP。

Direct Connect ゲートウェイアタッチメントの場合、許可されたプレフィックスインタラクションは、 からカスタマーネットワークにアドバタイズされるルートを制御します AWS。

静的ルートと伝達ルートが同じ送信先を持つ場合、静的ルートの優先度が高くなるため、伝達されたルートはルートテーブルに含まれません。静的ルートを削除すると、重複する伝達ルートがルートテーブルに含まれます。

ピアリングアタッチメントのルート

2 つの Transit Gateway をピアリングし、それらの間でトラフィックをルーティングできます。これを行うには、Transit Gateway にピアリングアタッチメントを作成し、ピアリング接続を行うピア Transit Gateway を指定します。次に、Transit Gateway ルートテーブルに静的ルートを作成し、トラフィックを Transit Gateway ピアリングアタッチメントにルーティングします。その後、ピアトランジットゲートウェイにルーティングされるトラフィックは、ピアトランジットゲートウェイの VPCおよび VPNアタッチメントにルーティングできます。

詳細については、「例: ピア接続 Transit Gateway 」を参照してください。

ルートの評価順序

Transit Gateway のルートは、次の順序で評価されます。

- 送信先アドレスの最も具体的なルート。
- 同じ を持つがCIDR、異なるアタッチメントタイプからのルートの場合、ルートの優先度は次のとおりです。
  - 静的ルート (Site-to-Site VPN 静的ルートなど)
  - プレフィックスリスト参照ルート
  - VPC伝播されたルート
  - Direct Connect ゲートウェイで伝播されたルート
  - Transit Gateway Connect で伝播されたルート
  - プライベート Direct Connect で伝播されたルートVPNを介した Site-to-Site
  - Site-toVPN-Site で伝播されたルート
  - Transit Gateway ピアリング伝達ルート (クラウド WAN)

一部のアタッチメントは、 経由のルートアドバタイズをサポートしていますBGP。同じ を持つルートCIDR、および同じアタッチメントタイプのルートの場合、ルートの優先度はBGP属性によって制御されます。

- AS パスの長さを短くする
- 低いMED値
- アタッチメントでサポートされている場合は、iBGP ルートよりも eBGP が推奨されます

> **Important**
>
> AWS は、上記の同じ 、アタッチメントタイプCIDR、およびBGP属性を持つルートの一貫したBGPルート優先順位を保証することはできません。

AWS Transit Gateway には優先ルートのみが表示されます。バックアップルートは、そのルートがアドバタイズされなくなった場合にのみ Transit Gateway ルートテーブルに表示されます。例えば、Direct Connect ゲートウェイおよび Site-to-Site を介して同じルートをアドバタイズする場合などですVPN。 AWS Transit Gateway は、優先ルートである Direct Connect ゲートウェイルートから受信したルートのみを表示します。バックアップルートVPNである Site-to-Site は、Direct Connect ゲートウェイがアドバタイズされなくなった場合にのみ表示されます。

VPC とトランジットゲートウェイのルートテーブルの違い

ルートテーブルの評価は、VPCルートテーブルとトランジットゲートウェイルートテーブルのどちらを使用しているかによって異なります。

次の例は、VPCルートテーブルを示しています。VPC ローカルルートが最優先され、次に最も具体的なルートが続きます。静的ルートと伝達されたルートの送信先が同じ場合は、静的ルートの方が優先度が高くなります。

送信先	ターゲット	優先度
10.0.0.0/16	ローカル	1
192.168.0.0/16	pcx-12345	2
172.31.0.0/16	vgw-12345 (静的) または tgw-12345 (静的)	2
172.31.0.0/16	vgw-12345 (伝播済み)	3
0.0.0.0/0	igw-12345	4

次の例は、トランジットゲートウェイルートテーブルを示しています。ゲートウェイアタッチメントを AWS Direct Connect VPNアタッチメントにする場合は、BGPVPN接続を使用してトランジットゲートウェイルートテーブルにルートを伝播します。

デスティネーション	アタッチメント (ターゲット)	リソースタイプ	ルートタイプ	優先度
10.0.0.0/16	tgw-attach-123 | vpc-1234	VPC	静的または伝播済み	1
192.168.0.0/16	tgw-attach-789 | vpn-5678	VPN	静的	2
172.31.0.0/16	tgw-attach-456 | dxgw_id	AWS Direct Connect ゲートウェイ	伝播済み	3
172.31.0.0/16	tgw-attach-789 | tgw-connect-peer-123	接続	伝播済み	4
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	伝播済み	5

トランジットゲートウェイシナリオの例

トランジットゲートウェイの一般的ユースケースは以下のとおりです。お客様のトランジットゲートウェイはこれらのユースケースに限定されません。

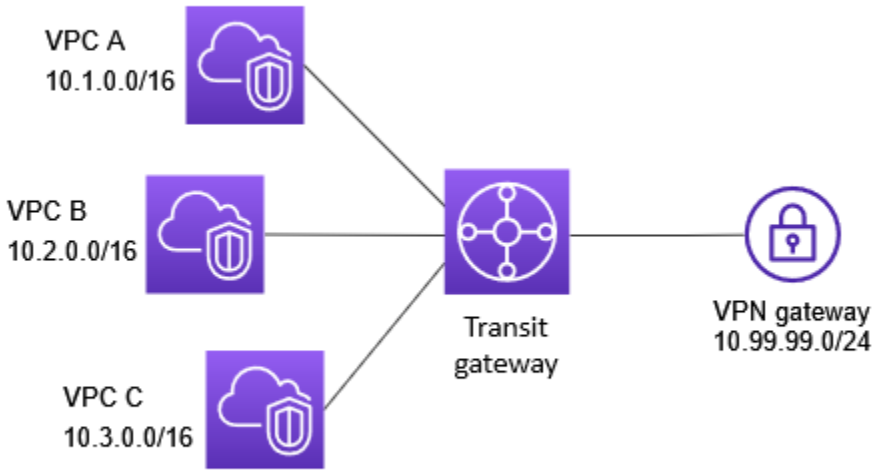
例: 集中型ルーター

トランジットゲートウェイは、、VPCs、 AWS Direct Connectおよび Site-to-Site のすべてのVPN接続を接続する集中型ルーターとして設定できます。このシナリオでは、アタッチメントはすべて、トランジットゲートウェイのデフォルトルートテーブルに関連付けられ、トランジットゲートウェイのデフォルトルートテーブルに伝播されます。そのため、アタッチメントはすべて、単純なレイヤー 3 IP ルーターとしてトランジットゲートウェイを提供しながら、パケットを相互にルーティングできます。

内容

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。このシナリオでは、トランジットゲートウェイに 3 つのVPCアタッチメントと 1 つの Site-to-Site VPNアタッチメントがあります。VPC A、VPCB、C VPC のサブネットからのパケットで、別の のサブネットVPCまたはVPN接続の宛先が最初にトランジットゲートウェイを経由します。



リソース

このシナリオでは、次のリソースを作成します。

- 3 つの VPCs。の作成の詳細についてはVPC、「Amazon ユーザーガイド」のVPC「 の作成」を参照してください。 VPC
- Transit Gateway。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
- トランジットゲートウェイ上の 3 つのVPCアタッチメント。詳細については、「the section called “VPC 添付ファイルを作成する”」を参照してください。

- トランジットゲートウェイ上の Site-to-Site VPNアタッチメント。各 のCIDRブロックはVPC、トランジットゲートウェイルートテーブルに伝播されます。VPN 接続が起動すると、BGPセッションが確立され、Site-to-Site VPN CIDR がトランジットゲートウェイルートテーブルに伝達され、 VPCCIDRsがカスタマーゲートウェイBGPテーブルに追加されます。詳細については、「the section called “への Transit Gateway アタッチメントを作成する VPN”」を参照してください。

  Site-to-Site VPN AWS Site-to-Site VPN ユーザーガイドで、カスタマーゲートウェイデバイスの要件を必ず確認してください。

ルーティング

各 VPCにはルートテーブルがあり、トランジットゲートウェイのルートテーブルがあります。

VPC ルートテーブル

各 には 2 つのエントリを持つルートテーブルVPCがあります。最初のエントリは、 のローカルIPv4ルーティングのデフォルトエントリVPCです。このエントリにより、この中のインスタンスは相互に通信VPCできるようになります。2 番目のエントリは、他のすべてのIPv4サブネットトラフィックをトランジットゲートウェイにルーティングします。次の表は、VPCA ルートを示しています。

デスティネーション	ターゲット
10.1.0.0/16	ローカル
0.0.0.0/0	tgw-id

転送ゲートウェイルートテーブル

以下は、前の図に示されているアタッチメントのデフォルトルートテーブルの例で、ルート伝播が有効になっています。

送信先	ターゲット	ルートタイプ
10.1.0.0/16	*Attachment for VPC A*	伝播済み
10.2.0.0/16	*Attachment for VPC B*	伝播済み

送信先	ターゲット	ルートタイプ
10.3.0.0/16	*Attachment for VPC C*	伝播済み
10.99.99.0/24	*Attachment for VPN connection*	伝播済み

カスタマーゲートウェイBGPテーブル

カスタマーゲートウェイBGPテーブルには、次の VPC が含まれますCIDRs。

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

例: 分離 VPCs

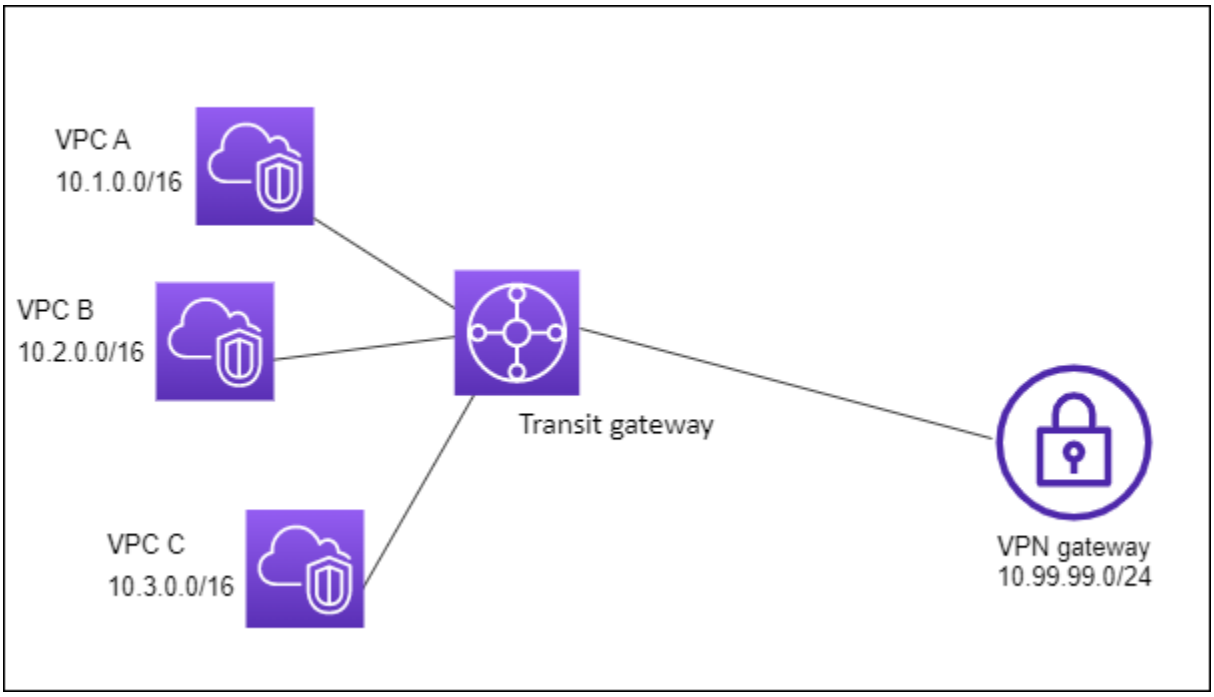
複数の独立したルーターとしてトランジットゲートウェイを設定することができます。これは複数のトランジットゲートウェイを使用するのと似ていますが、ルートとアタッチメントが変わる可能性がある場合に、より高い柔軟性を提供します。このシナリオでは、独立した各ルーターに単一のルートテーブルがあります。独立したルーターに関連付けられているすべてのアタッチメントは、伝播されてそのルートテーブルに関連付けられます。1 つの独立したルーターに関連付けられているアタッチメントは、相互にパケットをルーティングできますが、別の独立したルーターのアタッチメントにパケットをルーティングしたり、アタッチメントからパケットを受信したりすることはできません。

内容

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。VPC A、VPCB、C VPC からのパケットはトランジットゲートウェイにルーティングされます。インターネットを送信先とする VPC A、VPCB、C VPC のサブネットからのパケットは、まず Transit Gateway を経由し、次

に Site-to-Site VPN接続にルーティングします (送信先がそのネットワーク内にある場合) 。例えば、10.1.0.0 から 10.2.0.0 までVPCなど、別の のサブネットの送信先VPCを持つパケットは、トランジットゲートウェイを経由します。トランジットゲートウェイルートテーブルにサブネットのルートがないため、パケットはブロックされます。



リソース

このシナリオでは、次のリソースを作成します。

- 3 つの VPCs。の作成の詳細についてはVPC、「Amazon ユーザーガイド」のVPC「 の作成」を参照してください。 VPC
- Transit Gateway。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
- 3 つの のトランジットゲートウェイ上の 3 つのアタッチメントVPCs。詳細については、「the section called “VPC 添付ファイルを作成する”」を参照してください。
- トランジットゲートウェイ上の Site-to-Site VPNアタッチメント。詳細については、「the section called “への Transit Gateway アタッチメントを作成する VPN”」を参照してください。Site-to-Site VPN AWS Site-to-Site VPN ユーザーガイドで、カスタマーゲートウェイデバイスの要件を必ず確認してください。

VPN 接続が起動すると、BGPセッションが確立され、 VPN CIDR がトランジットゲートウェイルートテーブルに伝達され、 VPCCIDRsがカスタマーゲートウェイBGPテーブルに追加されます。

ルーティング

各 VPCにはルートテーブルがあり、トランジットゲートウェイには 2 つのルートテーブルがあります。1 つは 用VPCs、もう 1 つはVPN接続用です。

VPC A、VPCB、C VPC ルートテーブル

各 VPCには 2 つのエントリを持つルートテーブルがあります。最初のエントリは、 のローカルIPv4ルーティングのデフォルトエントリですVPC。このエントリにより、この中のインスタンスは相互に通信VPCできるようになります。2 番目のエントリは、他のすべてのIPv4サブネットトラフィックをトランジットゲートウェイにルーティングします。次の表は、VPCA ルートを示しています。

デスティネーション	ターゲット
10.1.0.0/16	ローカル
0.0.0.0/0	tgw-id

トランジットゲートウェイルートテーブル

このシナリオでは、 に 1 つのルートテーブルVPCsを使用し、VPN接続に 1 つのルートテーブルを使用します。

VPC アタッチメントは、VPNアタッチメントの伝播されたルートを持つ次のルートテーブルに関連付けられています。

デスティネーション	ターゲット	ルートタイプ
10.99.99.0/24	*Attachment for VPN connection*	伝播済み

VPN アタッチメントは、各VPCアタッチメントに伝播されたルートを持つ次のルートテーブルに関連付けられています。

デスティネーション	ターゲット	ルートタイプ

デスティネーション	ターゲット	ルートタイプ
10.1.0.0/16	*Attachment for VPC A*	伝播済み
10.2.0.0/16	*Attachment for VPC B*	伝播済み
10.3.0.0/16	*Attachment for VPC C*	伝播済み

トランジットゲートウェイルートテーブルでのルート伝播の詳細については、「Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルへのルート伝達を有効にする」を参照してください。

カスタマーゲートウェイBGPテーブル

カスタマーゲートウェイBGPテーブルには、次の VPC が含まれますCIDRs。

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

例: 共有サービスVPCsで分離

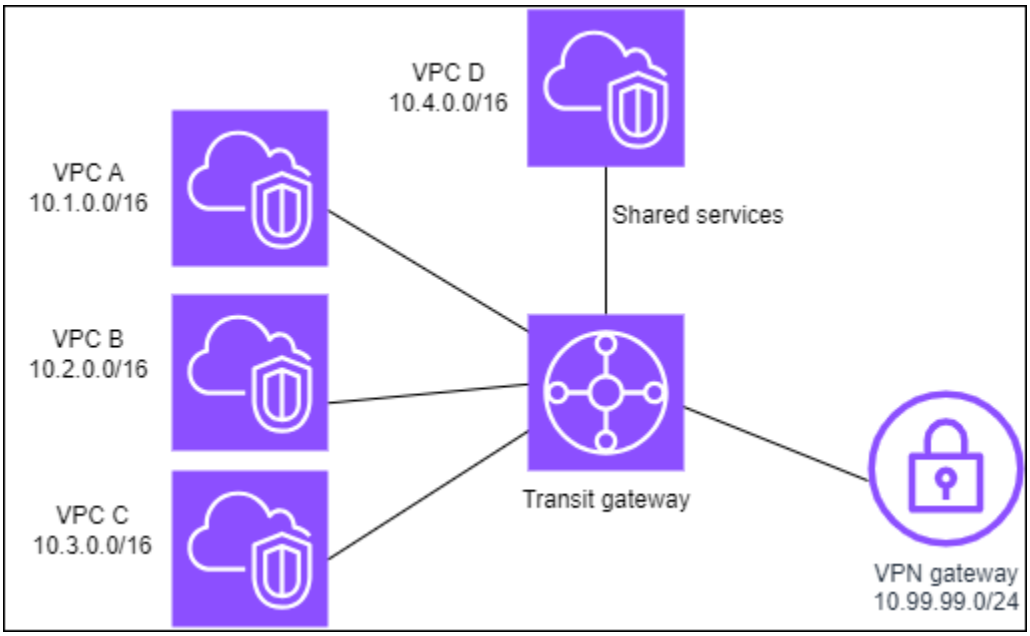
共有サービスを使用する複数の分離されたルーターとしてトランジットゲートウェイを設定できます。これは複数のトランジットゲートウェイを使用するのと似ていますが、ルートとアタッチメントが変わる可能性がある場合に、より高い柔軟性を提供します。このシナリオでは、独立した各ルーターに単一のルートテーブルがあります。独立したルーターに関連付けられているすべてのアタッチメントは、伝播されてそのルートテーブルに関連付けられます。1 つの独立したルーターに関連付けられているアタッチメントは、相互にパケットをルーティングできますが、別の独立したルーターのアタッチメントにパケットをルーティングしたり、アタッチメントからパケットを受信したりすることはできません。アタッチメントは、共有サービスとの間でパケットを送受信することができます。このシナリオは、分離する必要があるが、本番システムなどの共有サービスを使用する必要があるグループがある場合に使用できます。

内容

- ルーティング

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。インターネットを送信先とする VPC A、VPCB、C VPC のサブネットからのパケットは、まずトランジットゲートウェイを経由し、次に Site-to-Site のカスタマーゲートウェイにルーティングしますVPN。A、VPCB、または VPC VPCC のサブネットから送信先が A、VPCB、または VPC VPCC のサブネットのパケットは、トランジットゲートウェイを経由します。トランジットゲートウェイルートテーブルにルートがないため、パケットはブロックされます。D を宛先ルートとする VPC A、VPCB、VPCC VPC からのパケットは、トランジットゲートウェイを経由し、その後 D VPC にルーティングされます。



リソース

このシナリオでは、次のリソースを作成します。

- 4 つの VPCs。の作成の詳細についてはVPC、「Amazon ユーザーガイド」のVPC「 の作成」を参照してください。 VPC
- トランジットゲートウェイ。詳細については、「トランジットゲートウェイを作成する」を参照してください。
- トランジットゲートウェイ上の 4 つのアタッチメント。 ごとに 1 つVPC。詳細については、「the section called “VPC 添付ファイルを作成する”」を参照してください。
- トランジットゲートウェイ上の Site-to-Site VPNアタッチメント。詳細については、「the section called “への Transit Gateway アタッチメントを作成する VPN”」を参照してください。

Site-to-Site VPN AWS Site-to-Site VPN ユーザーガイドで、カスタマーゲートウェイデバイスの要件を必ず確認してください。

VPN 接続が起動すると、BGPセッションが確立され、 VPN CIDR がトランジットゲートウェイルートテーブルに伝達され、 VPCCIDRsがカスタマーゲートウェイBGPテーブルに追加されます。

- 分離された各 VPCは、分離されたルートテーブルに関連付けられ、共有ルートテーブルに伝播されます。
- 各共有VPCサービスは共有ルートテーブルに関連付けられ、両方のルートテーブルに伝播されます。

ルーティング

各 VPCにはルートテーブルがあり、トランジットゲートウェイには 2 つのルートテーブルがあります。1 つは 用VPCs、もう 1 つはVPN接続と共有サービス用ですVPC。

VPC A、VPCB、VPCC、D VPC ルートテーブル

各 VPCには、2 つのエントリを持つルートテーブルがあります。最初のエントリは、 のローカルルーティングのデフォルトエントリVPCです。このエントリにより、この中のインスタンスは相互に通信VPCできるようになります。2 番目のエントリは、他のすべてのIPv4サブネットトラフィックをトランジットゲートウェイにルーティングします。

デスティネーション	ターゲット
10.1.0.0/16	ローカル
0.0.0.0/0	*transit gateway ID*

Transit Gateway ルートテーブル

このシナリオでは、 に 1 つのルートテーブルVPCsを使用し、VPN接続に 1 つのルートテーブルを使用します。

VPC A、B、および C アタッチメントは、次のルートテーブルに関連付けられています。このルートテーブルには、VPNアタッチメントの伝播されたルートとVPC、D のアタッチメントの伝播されたルートがあります。

デスティネーション	ターゲット	ルートタイプ
10.99.99.0/24	*Attachment for VPN connection*	伝播済み
10.4.0.0/16	*Attachment for VPC D*	伝播済み

VPN アタッチメントと共有サービス VPC (VPC D) アタッチメントは、次のルートテーブルに関連付けられます。ルートテーブルには、各VPCアタッチメントを指すエントリがあります。これにより、VPN接続 と共有サービス VPCsから への通信が可能になりますVPC。

デスティネーション	ターゲット	ルートタイプ
10.1.0.0/16	*Attachment for VPC A*	伝播済み
10.2.0.0/16	*Attachment for VPC B*	伝播済み
10.3.0.0/16	*Attachment for VPC C*	伝播済み

詳細については、「Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルへのルート伝達を有効にする」を参照してください。

カスタマーゲートウェイBGPテーブル

カスタマーゲートウェイBGPテーブルには、4 つすべての CIDRsの が含まれていますVPCs。

例: ピア接続 Transit Gateway

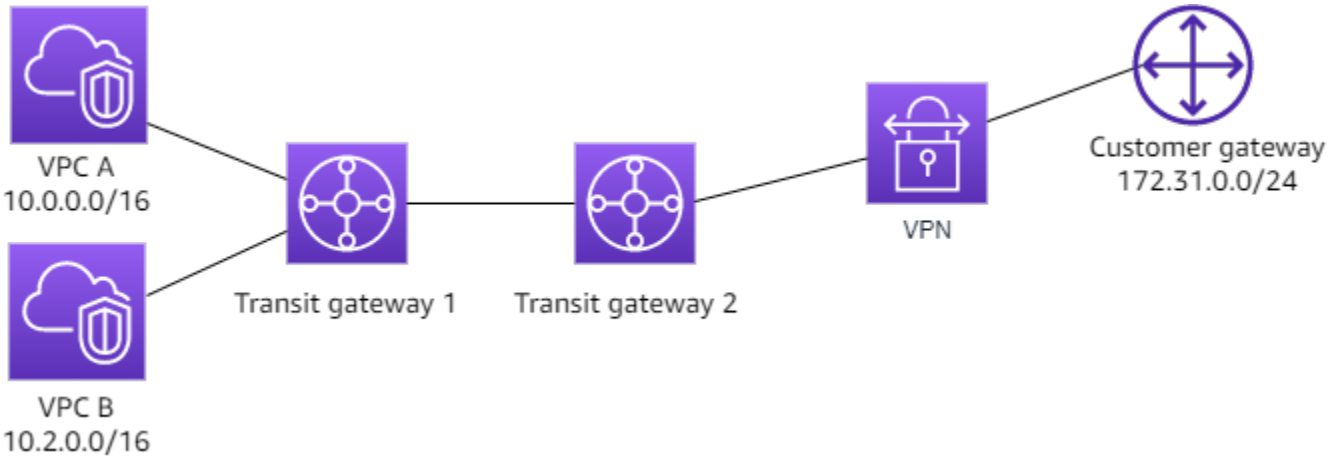
異なるリージョンで Transit Gateway 間に Transit Gateway ピアリング接続を作成できます。その後、各 Transit Gateway のアタッチメント間でトラフィックをルーティングできます。このシナリオでは、 VPCおよび VPNアタッチメントはトランジットゲートウェイのデフォルトルートテーブルに関連付けられ、トランジットゲートウェイのデフォルトルートテーブルに伝播されます。各 Transit Gateway のルートテーブルには、ゲートウェイのピアリングアタッチメントを指す静的ルートがあります。

内容

- リソース
- ルーティング

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。トランジットゲートウェイ 1 には 2 つのVPCアタッチメントがあり、トランジットゲートウェイ 2 には 1 つの Site-to-Site VPN アタッチメントがあります。インターネットを送信先とする VPC A と VPC B のサブネットからのパケットは、まずトランジットゲートウェイ 1 を経由し、次にトランジットゲートウェイ 2 を経由し、次にVPN接続にルーティングします。



リソース

このシナリオでは、次のリソースを作成します。

- 2 つの VPCs。の作成の詳細についてはVPC、「Amazon ユーザーガイド」のVPC「 の作成」を参照してください。 VPC
- 2 つの Transit Gateway。同じリージョン内に存在することも、異なるリージョン内に存在することもできます。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
- 最初のトランジットゲートウェイに 2 つのVPCアタッチメント。詳細については、「the section called “VPC 添付ファイルを作成する”」を参照してください。
- 2 番目のトランジットゲートウェイ上の Site-to-Site VPNアタッチメント。詳細については、「the section called “への Transit Gateway アタッチメントを作成する VPN”」を参照してください。Site-to-Site VPN AWS Site-to-Site VPN ユーザーガイドで、カスタマーゲートウェイデバイスの要件を必ず確認してください。

- 2 つのTransit Gateway 間のTransit Gateway ピアリングアタッチメント。詳細については、「Amazon Transit Gateway のVPCトランジットゲートウェイピアリングアタッチメント」を参照してください。

VPC アタッチメントを作成すると、各 CIDRsの がトランジットゲートウェイ VPC 1 のルートテーブルに伝播されます。VPN 接続が起動すると、次のアクションが発生します。

- BGP セッションが確立された
- Site-to-Site はトランジットゲートウェイ VPN CIDR 2 のルートテーブルに伝播されます。
- VPC CIDRs がカスタマーゲートウェイBGPテーブルに追加されます。

ルーティング

各 VPCにはルートテーブルがあり、各トランジットゲートウェイにはルートテーブルがあります。

VPC A および VPC B ルートテーブル

各 VPCには 2 つのエントリを持つルートテーブルがあります。最初のエントリは、 のローカルIPv4ルーティングのデフォルトエントリですVPC。このデフォルトエントリにより、この中のリソースは相互に通信VPCできるようになります。2 番目のエントリは、他のすべてのIPv4サブネットトラフィックをトランジットゲートウェイにルーティングします。次の表は、VPCA ルートを示しています。

デスティネーション	ターゲット
10.0.0.0/16	ローカル
0.0.0.0/0	tgw-1-id

Transit Gateway ルートテーブル

次に、ルート伝播が有効になっているTransit Gateway 1 のデフォルトルートテーブルの例を示します。

送信先	ターゲット	ルートタイプ

送信先	ターゲット	ルートタイプ
10.0.0.0/16	*Attachment ID for VPC A*	伝播済み
10.2.0.0/16	*Attachment ID for VPC B*	伝播済み
0.0.0.0/0	*Attachment ID for peering connection*	静的

次に、ルート伝播が有効になっているTransit Gateway 2 のデフォルトルートテーブルの例を示します。

送信先	ターゲット	ルートタイプ
172.31.0.0/24	*Attachment ID for VPN connection*	伝播済み
10.0.0.0/16	*Attachment ID for peering connection*	static
10.2.0.0/16	*Attachment ID for peering connection*	static

カスタマーゲートウェイBGPテーブル

カスタマーゲートウェイBGPテーブルには、次の VPC が含まれますCIDRs。

- 10.0.0.0/16
- 10.2.0.0/16

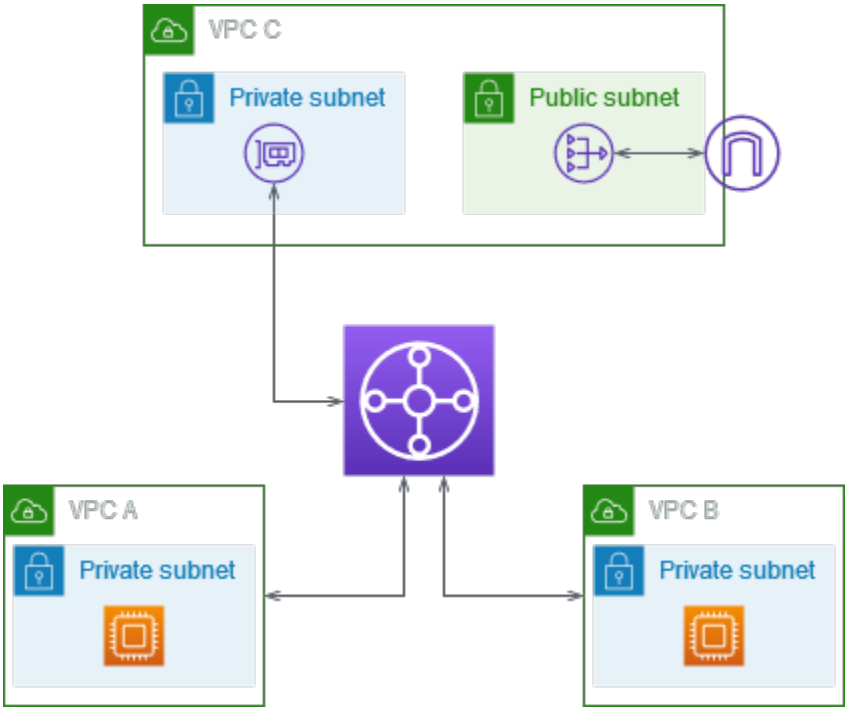
例: インターネットへの一元的な発信ルーティング

インターネットゲートウェイVPCのない から、ゲートウェイNATとインターネットゲートウェイを含む にアウトバウンドインターネットトラフィックをルーティングVPCするようにトランジットゲートウェイを設定できます。

内容

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。A と VPC B VPC には、アウトバウンドのみのインターネットアクセスを必要とするアプリケーションがあります。VPC C は、パブリックNATゲートウェイとインターネットゲートウェイ、およびVPCアタッチメントのプライベートサブネットを使用して設定します。すべてをVPCsトランジットゲートウェイに接続します。A と VPC B VPC からのアウトバウンドインターネットトラフィックがトランジットゲートウェイを C VPC に通過するようにルーティングを設定します。C VPC のNATゲートウェイは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します。



リソース

このシナリオでは、次のリソースを作成します。

- 重複しない IP アドレス範囲VPCsを持つ 3 つの 。詳細については、「Amazon ユーザーガイド」のVPC「 の作成」を参照してください。 VPC
- VPC A と VPC B には、それぞれEC2インスタンスを持つプライベートサブネットがあります。

- VPC C には次のものがあります。
  - にアタッチされたインターネットゲートウェイVPC。詳細については、「Amazon ユーザーガイド」の「インターネットゲートウェイの作成とアタッチ」を参照してください。 VPC
  - NAT ゲートウェイを持つパブリックサブネット。詳細については、「Amazon ユーザーガイド」のNAT「ゲートウェイの作成」を参照してください。 VPC
  - Transit Gateway アタッチメントのサブネット。プライベートサブネットは、パブリックサブネットと同じアベイラビリティーゾーンに設置する必要があります。
- 1 つのトランジットゲートウェイ。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
- トランジットゲートウェイ上の 3 つのVPCアタッチメント。各 のCIDRブロックはVPC、トランジットゲートウェイルートテーブルに伝播されます。詳細については、「the section called “VPC 添付ファイルを作成する”」を参照してください。VPC C の場合、プライベートサブネットを使用してアタッチメントを作成する必要があります。パブリックサブネットを使用してアタッチメントを作成すると、インスタンストラフィックはインターネットゲートウェイにルーティングされるものの、インターネットゲートウェイはそのトラフィックをドロップします。これは、インスタンスにパブリック IP アドレスがないためです アタッチメントをプライベートサブネットに配置すると、トラフィックはNATゲートウェイにルーティングされ、NATゲートウェイは Elastic IP アドレスをソース IP アドレスとして使用してトラフィックをインターネットゲートウェイに送信します。

ルーティング

各 のルートテーブルVPCとトランジットゲートウェイのルートテーブルがあります。

ルートテーブル

- VPC A のルートテーブル
- VPC B のルートテーブル
- C VPC のルートテーブル
- トランジットゲートウェイルートテーブル

VPC A のルートテーブル

ルートテーブルの例を次に示します。最初のエントリにより、 内のインスタンスが相互に通信VPCできるようになります。2 番目のエントリは、他のすべてのIPv4サブネットトラフィックをトランジットゲートウェイにルーティングします。

デスティネーション	ターゲット
VPC A CIDR	ローカル
0.0.0.0/0	*transit-gateway-id*

VPC B のルートテーブル

ルートテーブルの例を次に示します。最初のエントリにより、 内のインスタンスが相互に通信VPC できるようになります。2 番目のエントリは、他のすべてのIPv4サブネットトラフィックをトランジットゲートウェイにルーティングします。

デスティネーション	ターゲット
VPC B CIDR	ローカル
0.0.0.0/0	*transit-gateway-id*

C VPC のルートテーブル

インターネットNATゲートウェイにルートを追加して、ゲートウェイをパブリックサブネットとしてサブネットを設定します。もう一方のサブネットはプライベートサブネットのままにします。

パブリックサブネットのルートテーブルの例を次に示します。最初のエントリにより、 内のインスタンスが相互に通信VPCできるようになります。2 番目と 3 番目のエントリは、VPCA と VPC B のトラフィックをトランジットゲートウェイにルーティングします。残りのエントリは、他のすべてのIPv4サブネット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します。

デスティネーション	ターゲット
VPC C CIDR	ローカル
VPC A CIDR	*transit-gateway-id*
VPC B CIDR	*transit-gateway-id*

デスティネーション	ターゲット
0.0.0.0/0	*internet-gateway-id*

プライベートサブネットのルートテーブルの例を次に示します。最初のエントリにより、 内のインスタンスが相互に通信VPCできるようになります。2 番目のエントリは、他のすべてのIPv4サブネットトラフィックをNATゲートウェイにルーティングします。

デスティネーション	ターゲット
VPC C CIDR	ローカル
0.0.0.0/0	*nat-gateway-id*

トランジットゲートウェイルートテーブル

トランジットゲートウェイのルートテーブルの例を次に示します。各 のCIDRブロックはVPC、トランジットゲートウェイルートテーブルに伝播されます。静的ルートはアウトバウンドインターネットトラフィックを C VPC に送信します。オプションで、各 にブラックホールルートを追加することで、通信VPC間を防ぐことができますVPCCIDR。

CIDR	Attachment	ルートタイプ
VPC A CIDR	*Attachment for VPC A*	伝播済み
VPC B CIDR	*Attachment for VPC B*	伝播済み
VPC C CIDR	*Attachment for VPC C*	伝播済み
0.0.0.0/0	*Attachment for VPC C*	static

例: 共有サービスのアプライアンス VPC

アプライアンス (セキュリティアプライアンスなど) は、共有サービス で設定できますVPC。Transit Gateway アタッチメント間でルーティングされるすべてのトラフィックは、まず共有サービス のアプライアンスによって検査されますVPC。アプライアンスモードを有効にすると、トランジットゲートウェイは、フローハッシュアルゴリズムVPCを使用してアプライアンス 内の単一のネットワークインターフェイスを選択し、フローの存続期間中、トラフィックを に送信します。トランジットゲートウェイは、リターントラフィックに同じネットワークインターフェイスを使用します。これにより、双方向トラフィックは対称的にルーティングされ、フローの存続期間中、VPCアタッチメント内の同じアベイラビリティーゾーンを介してルーティングされます。アーキテクチャ内に複数のトランジットゲートウェイがある場合、各トランジットゲートウェイは独自のセッションアフィニティを維持し、各トランジットゲートウェイは異なるネットワークインターフェイスを選択できます。

フローの維持を保証するVPCには、1 つのトランジットゲートウェイのみをアプライアンスに接続する必要があります。複数のトランジットゲートウェイを単一のアプライアンスに接続しても、トランジットゲートウェイVPCはフロー状態情報を相互に共有しないため、フローの維持は保証されません。

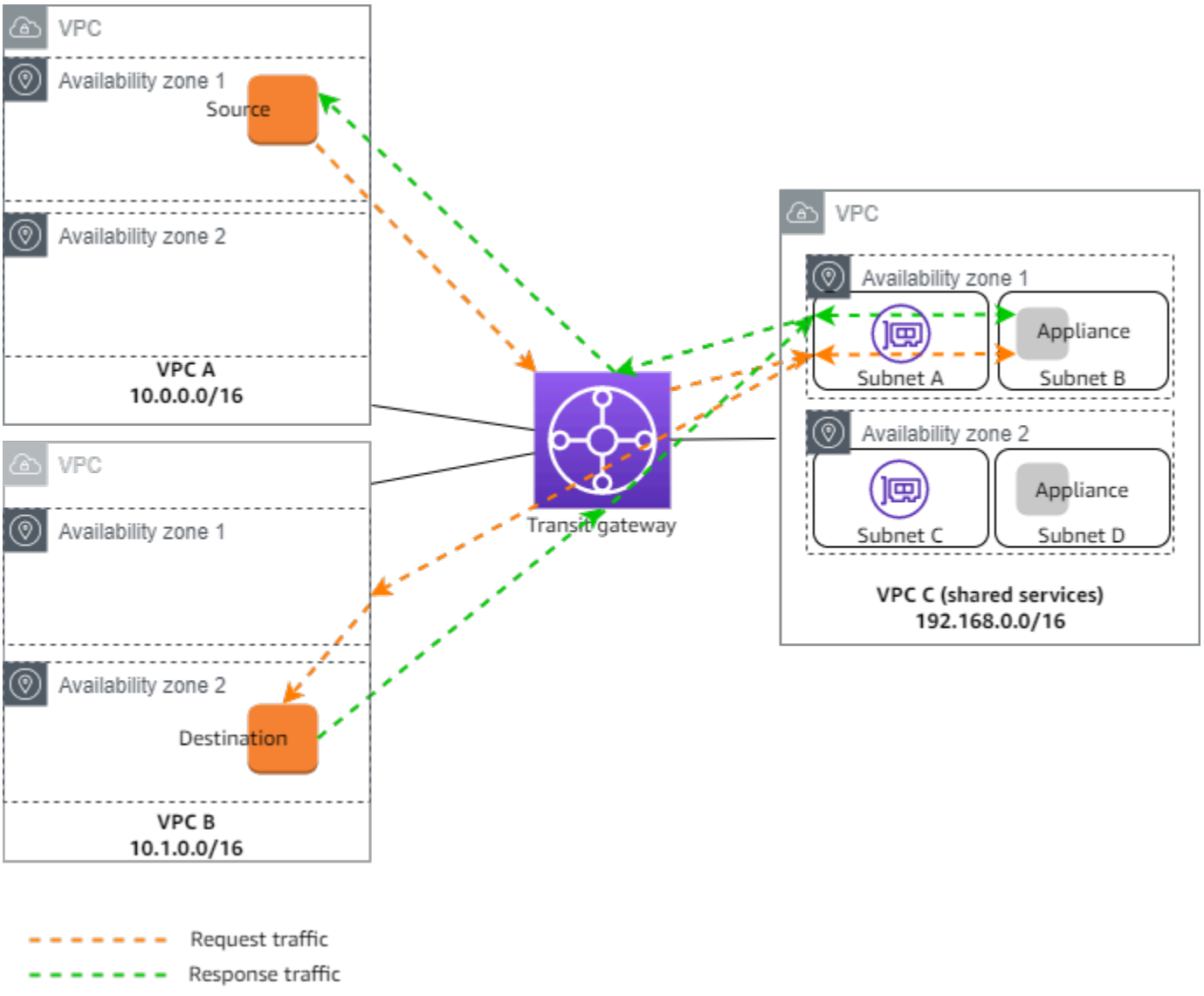
> **Important**
>
> - アプライアンスモードのトラフィックは、送信元トラフィックと送信先トラフィックが同じ Transit Gateway アタッチメントから一元管理された VPC (検査 VPC) に到達する限り、正しくルーティングされます。送信元と送信先が 2 つの異なる Transit Gateway アタッチメントにある場合、トラフィックがドロップされる可能性があります。一元化された がインターネットゲートウェイなどの別のゲートウェイからトラフィックVPCを受信し、検査後にそのトラフィックをトランジットゲートウェイアタッチメントに送信すると、トラフィックがドロップされる可能性があります。
> - 既存のアタッチメントでアプライアンスモードを有効にすると、アタッチメントがアベイラビリティーゾーンを流れる可能性があるため、そのアタッチメントの現在のルートに影響する可能性があります。アプライアンスモードが有効になっていない場合、トラフィックは発信元のアベイラビリティーゾーンに保持されます。

内容

- ルーティング

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。トランジットゲートウェイには 3 つのVPCアタッチメントがあります。VPC C は共有サービス ですVPC。A と VPC B VPC の間のトラフィックはトランジットゲートウェイにルーティングされ、検査のために C VPC のセキュリティアプライアンスにルーティングされてから、最終送信先にルーティングされます。アプライアンスはステートフルアプライアンスであるため、リクエストトラフィックとレスポンストラフィックの両方が検査されます。高可用性のために、VPCC の各アベイラビリティーゾーンにアプライアンスがあります。



このシナリオでは、次のリソースを作成します。

- 3 つの VPCs。の作成の詳細についてはVPC、Amazon Virtual Private Cloud ユーザーガイド VPC」の「 の作成」を参照してください。
- Transit Gateway。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
- 3 つのVPCアタッチメント - 各 に 1 つずつVPCs。詳細については、「the section called “VPC 添付ファイルを作成する”」を参照してください。

  VPC アタッチメントごとに、各アベイラビリティーゾーンにサブネットを指定します。共有サービス の場合VPC、これらはトラフィックがトランジットゲートウェイVPCから にルーティングされるサブネットです。前の例では、サブネット A と C です。

  VPC C のVPCアタッチメントでは、アプライアンスモードのサポートを有効にして、レスポンストラフィックがソーストラフィックと同じ C VPC のアベイラビリティーゾーンにルーティングされるようにします。

  Amazon VPCコンソールはアプライアンスモードをサポートしています。Amazon API、、VPC を使用してアプライアンスモード AWS SDK AWS CLI を有効にすることもできます AWS CloudFormation。例えば、 `--options ApplianceModeSupport=enable`を create-transit-gateway-vpc-attachment コマンドまたは modify-transit-gateway-vpc-attachment コマンドに追加します。

> **Note**
>
> アプライアンスモードでのフローの維持は、検査 に向かう送信元トラフィックと送信先トラフィックに対してのみ保証されますVPC。

ステートフルアプライアンスおよびアプライアンスモード

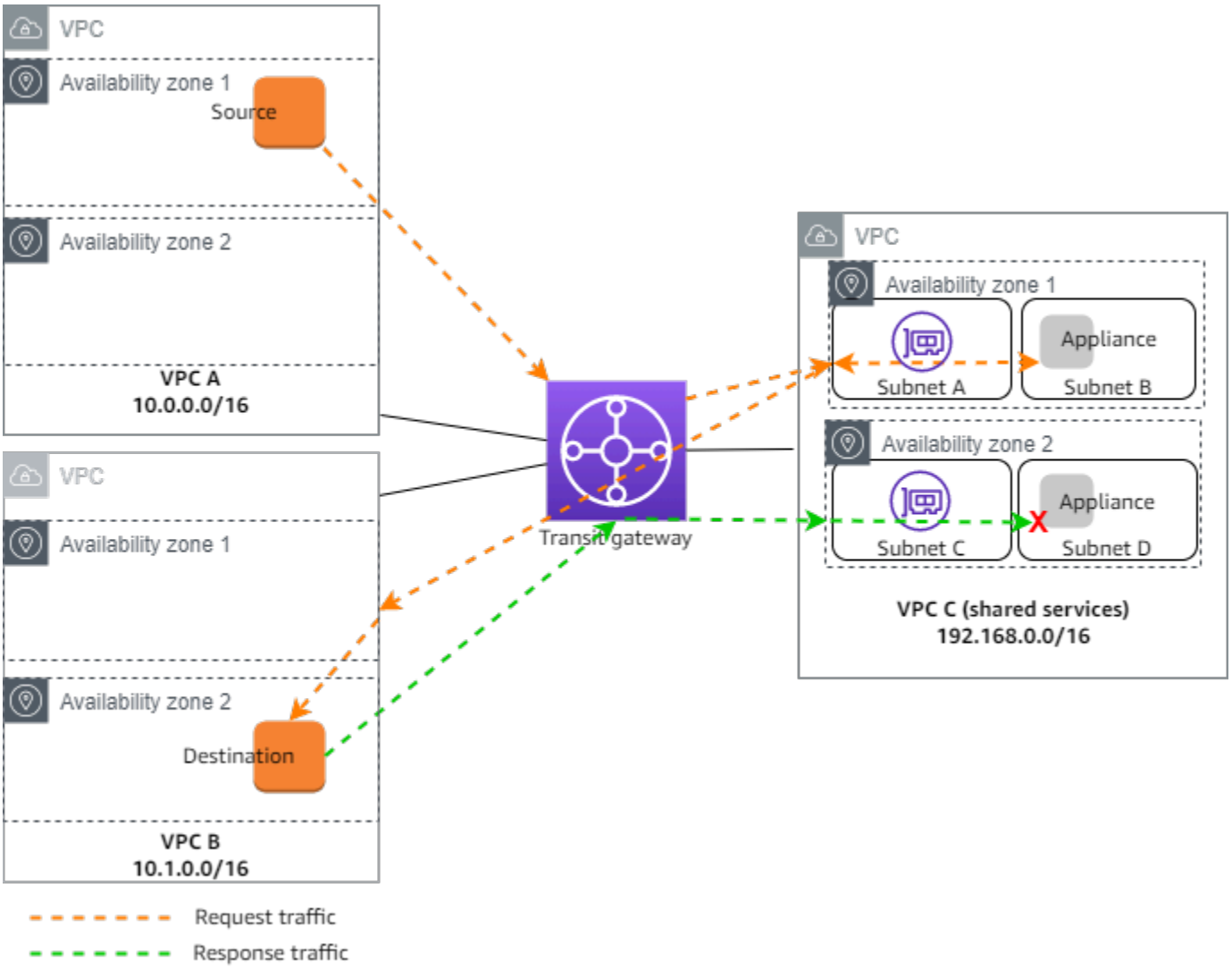
VPC アタッチメントが複数のアベイラビリティーゾーンにまたがり、ステートフル検査のために送信元ホストと送信先ホスト間のトラフィックを同じアプライアンス経由でルーティングする必要がある場合は、アプライアンスが配置されているVPCアタッチメントのアプライアンスモードサポートを有効にします。

詳細については、 AWS ブログの「一元化された検査アーキテクチャ」を参照してください。

アプライアンスモードが有効でない場合の動作

アプライアンスモードが有効になっていない場合、トランジットゲートウェイは、送信先に到達するまで、送信元のアベイラビリティーゾーン内のVPCアタッチメント間でルーティングされたトラフィックを保持しようとします。トラフィックは、アベイラビリティーゾーンに障害が発生した場合、またはそのアベイラビリティーゾーンにアタッチメントに関連付けられたサブネットがない場合にのみ、VPCアタッチメント間でアベイラビリティーゾーンを通過します。

次の図は、アプライアンスモードサポートが有効でない場合のトラフィックフローを示しています。VPC B のアベイラビリティーゾーン 2 から発信されるレスポンストラフィックは、トランジットゲートウェイによって VPC C の同じアベイラビリティーゾーンにルーティングされます。したがって、アベイラビリティーゾーン 2 のアプライアンスは VPC A のソースからの元のリクエストを認識しないため、トラフィックはドロップされます。



ルーティング

各 VPCには 1 つ以上のルートテーブルがあり、トランジットゲートウェイには 2 つのルートテーブルがあります。

VPC ルートテーブル

VPC A と VPC B

VPCs A と B には、2 つのエントリを持つルートテーブルがあります。最初のエントリは、 のローカルIPv4ルーティングのデフォルトエントリですVPC。このデフォルトエントリにより、この中のリソースは相互に通信VPCできるようになります。2 番目のエントリは、他のすべてのIPv4サブネットトラフィックをトランジットゲートウェイにルーティングします。VPC A のルートテーブルを次に示します。

デスティネーション	ターゲット
10.0.0.0/16	ローカル
0.0.0.0/0	tgw-id

VPC C

共有サービス VPC (VPC C) には、サブネットごとに異なるルートテーブルがあります。サブネット A はトランジットゲートウェイによって使用されます (VPCアタッチメントの作成時にこのサブネットを指定します) 。サブネット A のルートテーブルは、サブネット B のアプライアンスにすべてのトラフィックをルーティングします。

送信先	ターゲット
192.168.0.0/16	ローカル
0.0.0.0/0	appliance-eni-id

サブネット B (アプライアンスを含む) のルートテーブルは、トラフィックをトランジットゲートウェイにルーティングします。

送信先	ターゲット
192.168.0.0/16	ローカル
0.0.0.0/0	tgw-id

トランジットゲートウェイルートテーブル

このトランジットゲートウェイは、A と VPC B に 1 VPC つのルートテーブルを使用し、共有サービス VPC (VPC C) に 1 つのルートテーブルを使用します。

VPC A および VPC B アタッチメントは、次のルートテーブルに関連付けられています。ルートテーブルは、すべてのトラフィックを C VPC にルーティングします。

デスティネーション	ターゲット	ルートタイプ
0.0.0.0/0	*Attachment ID for VPC C*	static

C VPC アタッチメントは、次のルートテーブルに関連付けられています。トラフィックを VPC A と VPC B にルーティングします。

デスティネーション	ターゲット	ルートタイプ
10.0.0.0/16	*Attachment ID for VPC A*	伝播済み
10.1.0.0/16	*Attachment ID for VPC B*	伝播済み

Amazon VPC Transit Gateway の使用を開始する

以下のタスクは、Amazon VPC Transit Gateway のトランジットゲートウェイに慣れるのに役立ちます。このタスクでは、トランジットゲートウェイを作成し、そのトランジットゲートウェイVPCsを使用して の 2 つを接続する手順を説明します。

タスク

- 前提条件
- ステップ 1: トランジットゲートウェイを作成する
- ステップ 2: をトランジットゲートウェイVPCsにアタッチする
- ステップ 3: トランジットゲートウェイと の間にルートを追加する VPCs
- ステップ 4: トランジットゲートウェイをテストする
- ステップ 5: トランジットゲートウェイを削除する

前提条件

- トランジットゲートウェイを使用する簡単な例を示すには、同じリージョンVPCsに 2 つを作成します。は重複する を持つVPCsことはできませんCIDRs。各 で 1 つの Amazon EC2インスタンスを起動しますVPC。詳細については、「Amazon ユーザーガイド」のVPC「Amazon の開始方法VPC」を参照してください。
- 2 つの異なる を指す同一のルートを持つことはできませんVPCs。トランジットゲートウェイルートテーブルに同じルートが存在するVPC場合、トランジットゲートウェイはCIDRs新しくアタッチされた の を伝播しません。
- トランジットゲートウェイを処理するために必要なアクセス許可があることを確認してください。詳細については、「Amazon VPC Transit Gateway での Identity and Access Management 」を参照してください。
- 各ホストセキュリティグループにICMPルールを追加していない場合、ホスト間で ping を実行することはできません。詳細については、「Amazon ユーザーガイド」の「セキュリティグループの使用」を参照してください。 VPC

ステップ 1: トランジットゲートウェイを作成する

トランジットゲートウェイを作成すると、デフォルトのトランジットゲートウェイルートテーブルが作成され、それをデフォルトの関連付けルートテーブルおよびデフォルトの伝達ルートテーブルとして使用します。

トランジットゲートウェイを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. リージョンセレクタで、 の作成時に使用したリージョンを選択しますVPCs。
3. ナビゲーションペインで [Transit Gateways] を選択します。
4. [Transit Gateway の作成] を選択します。
5. (オプション) [名前タグ] に、トランジットゲートウェイの名前を入力します。これにより、キーとして「Name」、値として指定した名前を持つタグが作成されます。
6. (オプション) [説明] に、トランジットゲートウェイの説明を入力します。
7. 「トランジットゲートウェイの設定」セクションで、次の操作を行います。

    1. Amazon 側の自律システム番号 (ASN) には、トランジットゲートウェイASNのプライベートを入力します。これは、ボーダーゲートウェイプロトコル (BGP) セッションの ASN AWS 側である必要があります。

        16 ビット の場合、範囲は 64512 ~ 65534 ですASNs。

        32 ビット の場合、範囲は 4200000000 ~ 4294967294 ですASNs。

        マルチリージョンデプロイの場合は、各トランジットゲートウェイASNに一意の を使用することをお勧めします。
    2. (オプション) 次のいずれかを有効にするかどうかを選択します。
        - このトランジットゲートウェイにアVPCsタッチされた DNSのサポート。
        - VPN ECMP は、トランジットゲートウェイにアタッチされたVPN接続をサポートします。
        - デフォルトのルートテーブルの関連付け。トランジットゲートウェイアタッチメントをこのトランジットゲートウェイのデフォルトルートテーブルに自動的に関連付けます。
        - デフォルトのルートテーブル伝達 。これにより、ルートテーブルアタッチメントがこのトランジットゲートウェイのデフォルトルートテーブルに自動的に伝達されます。
        - マルチキャストは をサポートします。これにより、このトランジットゲートウェイでマルチキャストドメインを作成できます。

8. （オプション) C onfigure-cross-account 共有オプションセクションで、共有アタッチメント を自動で受け入れるかどうかを選択します。有効にすると、添付ファイルは自動的に受け入れられます。それ以外の場合は、添付ファイルリクエストを承諾または拒否する必要があります。
9. （オプション)「トランジットゲートウェイCIDRブロック」セクションで、IPv4アドレスにサイズ /24 CIDRブロック以上、またはIPv6アドレスCIDRにサイズ /64 ブロック以上を追加します。169.254.0.0/16 範囲のアドレス、およびVPCアタッチメントとオンプレミスネットワークのアドレスと重複するアドレスを除き、任意のパブリックまたはプライベート IP アドレス範囲を関連付けることができます。

   > **Note**
   >
   > トランジットゲートウェイCIDRブロックは、Connect (GRE) アタッチメントまたは PrivateIP を設定する場合に使用されますVPNs。Transit Gateway は、この範囲のトンネルエンドポイント (GRE/PrivateIPVPN) IPsに を割り当てます。

10. （オプション) このトランジットゲートウェイにキーと値のタグを追加して、識別しやすくします。

    1. 新しいタブを追加 を選択します。
    2. [キー] の名前と関連する [値] を入力します。
    3. 新しいタグを追加 を選択してタグを追加するか、次のステップに進みます。
11. [Transit Gateway の作成] を選択します。ゲートウェイが作成されると、トランジットゲートウェイの初期状態は `pending` になります。

ステップ 2: をトランジットゲートウェイVPCsにアタッチする

アタッチメントの作成に進む前に、前のセクションで作成したトランジットゲートウェイが使用可能として表示されるまで待ちます。ごとに添付ファイルを作成しますVPC。

「」で説明されているようにVPCs、それぞれに 2 つの を作成し、EC2インスタンスを起動したことを確認します前提条件。

へのトランジットゲートウェイアタッチメントを作成する VPC

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. [Transit Gateway アタッチメントの作成] を選択します。

4. (オプション) [名前タグ] にアタッチメントの名前を入力します。
5. [Transit Gateway ID] で、アタッチメントに使用するトランジットゲートウェイを選択します。
6. 添付ファイルタイプ で、 を選択しますVPC。
7. DNS サポートを有効にするかどうかを選択します。この演習では、IPv6サポート を有効にしないでください。
8. VPC ID には、トランジットゲートウェイにVPCアタッチする を選択します。
9. サブネット IDsで、トラフィックをルーティングするためにトランジットゲートウェイが使用するアベイラビリティーゾーンごとに 1 つのサブネットを選択します。少なくとも 1 つのサブネットを選択する必要があります。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選択できます。
10. [Transit Gateway アタッチメントの作成] を選択します。

各アタッチメントは常に 1 つのルートテーブルに関連付けられています。ルートテーブルは、ゼロから多数のアタッチメントに関連付けることができます。設定するルートを決定するには、トランジットゲートウェイのユースケースを決定し、ルートを設定します。詳細については、「the section called “トランジットゲートウェイシナリオの例”」を参照してください。

ステップ 3: トランジットゲートウェイと の間にルートを追加する VPCs

ルートテーブルには、パケットの送信先 IP アドレスVPCsに基づいて、関連付けられた のネクストホップを決定する動的ルートと静的ルートが含まれます。非ローカルルートの送信先とトランジットゲートウェイのアタッチメント ID のターゲットを持つルートを設定します。詳細については、「Amazon ユーザーガイド」の「トランジットゲートウェイのルーティング」を参照してください。VPC

ルートをVPCルートテーブルに追加するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[ルートテーブル] を選択します。
3. に関連付けられているルートテーブルを選択しますVPC。
4. [ルート] タブを選択し、[ルート編集] を選択します。
5. [ルート追加] を選択します。

6. [送信先] 列に、送信先の IP アドレス範囲を入力します。ターゲットでは、トランジットゲートウェイを選択してから、トランジットゲートウェイ ID を選択します。
7. [Save changes] (変更の保存) をクリックします。

ステップ 4: トランジットゲートウェイをテストする

トランジットゲートウェイが正常に作成されたことを確認するには、各 の Amazon EC2インスタンスに接続しVPC、それらの間で ping コマンドなどのデータを送信します。詳細については、「Linux インスタンスへの接続」または「Windows インスタンスへの接続」を参照してください。

ステップ 5: トランジットゲートウェイを削除する

不要になったトランジットゲートウェイは削除できます。

リソースのアタッチメントがあるトランジットゲートウェイは削除できません。アタッチメント付きのトランジットゲートウェイを削除しようとすると、トランジットゲートウェイを削除する前に、まずそれらのアタッチメントを削除するように求められます。トランジットゲートウェイが削除されるとすぐに、そのゲートウェイに対する課金は停止します。

トランジットゲートウェイを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateways] を選択します。
3. トランジットゲートウェイを選択し、[アクション]、[トランジットゲートウェイの削除] を選択します。
4. 「**`delete`**」と入力し、[削除] を選択します。

   [Transit gateways] ページのトランジット ゲートウェイの State は [Deleting] です。削除すると、トランジットゲートウェイはページから削除されます。

Amazon VPC Transit Gateway の設計のベストプラクティス

Transit Gateway 設計に関するベストプラクティスは次のとおりです:

- トランジットゲートウェイVPCアタッチメントごとに個別のサブネットを使用します。サブネットごとに、 CIDRなどの小さな を使用して/28、EC2リソースのアドレスを増やします。別のサブネットを使用する場合は、次の項目を設定できます:
  - トランジットゲートウェイサブネットACLsに関連付けられたインバウンドネットワークとアウトバウンドネットワークを開いたままにします。
  - トラフィックフローに応じて、ネットワークACLsをワークロードサブネットに適用できます。
- 1 つのネットワークACLを作成し、トランジットゲートウェイに関連付けられているすべてのサブネットに関連付けます。インバウンド方向とアウトバウンド方向の両方でネットワークをACL開いたままにします。
- ネットワーク設計で複数のVPCルートテーブル (複数のゲートウェイを介してトラフィックをルーティングVPCするミドルボックスなど) が必要でない限り、同じVPCルートテーブルをトランジットNATゲートウェイに関連付けられているすべてのサブネットに関連付けます。
- ボーダーゲートウェイプロトコル (BGP) Site-to-Site VPN接続を使用します。接続用のカスタマーゲートウェイデバイスまたはファイアウォールがマルチパスをサポートしている場合は、機能を有効にします。
- AWS Direct Connect ゲートウェイアタッチメントと BGP Site-to-Site VPNアタッチメントのルート伝達を有効にします。
- VPC ピアリングからトランジットゲートウェイの使用に移行する場合。VPC ピアリングとトランジットゲートウェイMTUのサイズが一致しない場合、非対称トラフィックの一部のパケットがドロップされる可能性があります。サイズの不一致によるジャンボパケットのドロップを避けるため、両方VPCsを同時に更新します。
- 設計上、Transit Gateway は可用性が高いため、高可用性を得るためにTransit Gateway を追加する必要はありません。
- 設計で複数のTransit Gateway ルートテーブルが必要でない限り、Transit Gateway ルートテーブルの数を制限します。
- 冗長性を確保するには、災害対策用に各リージョンで 1 つの Transit Gateway を使用します。
- 複数のトランジットゲートウェイを使用するデプロイでは、トランジットゲートウェイごとに一意の自律システム番号 (ASN) を使用することをお勧めします。リージョン間のピアリングも使用できます。詳細については、「リージョン AWS Transit Gateway 間ピアリングを使用してグローバルネットワークを構築する」を参照してください。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイを操作する

Amazon VPCコンソールまたは を使用して、トランジットゲートウェイを操作できます AWS CLI。

トピック

共有トランジットゲートウェイ

AWS Resource Access Manager (RAM) を使用して、アカウント間または の組織全体でVPCアタッチメントのトランジットゲートウェイを共有できます AWS Organizations。RAM を有効にし、リソースを組織と共有する必要があります。詳細については、「AWS RAM ユーザーガイド」の「AWS Organizationsでリソース共有を有効にする」を参照してください。

考慮事項

AWS Resource Access Manager (RAM) を使用して、アカウント間または の組織全体でVPCアタッチメントのトランジットゲートウェイを共有できます AWS Organizations。RAM を有効にし、リソースを組織と共有する必要があります。詳細については、「AWS RAM ユーザーガイド」の「AWS Organizationsでリソース共有を有効にする」を参照してください。

トランジットゲートウェイを共有する場合は、以下の点を考慮してください。

- AWS Site-to-Site VPN アタッチメントは、トランジットゲートウェイを所有するのと同じ AWS アカウントで作成する必要があります。
- Direct Connect ゲートウェイへのアタッチメントは、トランジットゲートウェイの関連付けを使用し、Direct Connect ゲートウェイと同じ AWS アカウント、または Direct Connect ゲートウェイとは異なるアカウントにある場合があります。

デフォルトでは、ユーザーには AWS RAM リソースを作成または変更するアクセス許可はありません。ユーザーがリソースを作成または変更し、タスクを実行できるようにするには、特定のリソースとAPIアクションを使用するアクセス許可を付与するIAMポリシーを作成する必要があります。次に、これらのアクセス許可を必要とするIAMユーザーまたはグループに、これらのポリシーをアタッチします。

リソース所有者のみ次のオペレーションを実行できます。

- リソース共有を作成します。
- リソース共有を更新します。
- リソース共有を表示します。
- アカウントによって共有されているリソースをすべてのリソース共有間で表示できます。
- すべてのリソース共有で、リソースを共有しているプリンシパルを表示します。お客様の共有相手のプリンシパルを表示することで、お客様の共有リソースにアクセスできるプリンシパルを判別できます。
- リソース共有を削除します。
- すべてのトランジットゲートウェイ、トランジットゲートウェイアタッチメント、およびトランジットゲートウェイルートテーブル を実行しますAPIs。

共有されているリソース上で次のオペレーションを実行することができます。

- リソースの共有の招待を承認または拒否します。
- リソース共有を表示します。
- お客様がアクセスできる共有リソースを表示します。
- リソースを共有しているすべてのプリンシパルのリストを表示します。共有されているリソースおよびリソース共有を確認することができます。
- を実行できますDescribeTransitGatewaysAPI。

- 添付ファイルを作成および記述APIsする を実行します。たとえばDescribeTransitGatewayVpcAttachments、CreateTransitGatewayVpcAttachmentと を で実行しますVPCs。
- リソース共有を終了します。

Transit Gateway が共有されている場合、Transit Gateway ルートテーブルまたは Transit Gateway ルートテーブルの伝達および関連付けを作成、変更、削除することはできません。

トランジットゲートウェイを作成した場合、トランジットゲートウェイは自分のアカウントにマップされているアベイラビリティーゾーンに作成され、他のアカウントからは独立しています。トランジットゲートウェイおよびアタッチメントエンティティが異なるアカウントにある場合、アベイラビリティーゾーン ID を使用してアベイラビリティーゾーンを一意に一貫して識別します。例えば、use1-az1 は us-east-1 リージョンの AZ ID であり、すべての AWS アカウントの同じ場所にマッピングされます。

トランジットゲートウェイの共有解除

共有所有者がトランジットゲートウェイの共有を解除する場合、次のルールが適用されます。

- トランジットゲートウェイアタッチメントは、機能し続けます。
- 共有アカウントでトランジットゲートウェイを示すことはできません。
- トランジットゲートウェイの所有者および共有所有者は、トランジットゲートウェイアタッチメントを削除できます。

トランジットゲートウェイが別の AWS アカウントと共有解除された場合、またはトランジットゲートウェイが共有されている AWS アカウントが組織から削除された場合、トランジットゲートウェイ自体は影響を受けません。

共有サブネット

VPC 所有者は、共有VPCサブネットにトランジットゲートウェイをアタッチできます。参加者はできません。参加者のリソースからのトラフィックは、VPC所有者が共有VPCサブネットに設定したルートに応じて、アタッチメントを使用できます。

詳細については、「Amazon ユーザーガイド」の「 を他のアカウントVPCと共有する」を参照してください。 VPC

Amazon Transit Gateway のVPCトランジットゲートウェイ

トランジットゲートウェイを使用すると、 VPCsおよび VPN接続をアタッチし、それらの間でトラフィックをルーティングできます。トランジットゲートウェイは 間で動作し AWS アカウント、AWS RAM を使用してトランジットゲートウェイを他の アカウントと共有できます。トランジットゲートウェイを別の と共有すると AWS アカウント、アカウント所有者はトランジットゲートウェイVPCsに をアタッチできます。どちらのアカウントのユーザーも、アタッチメントをいつでも削除できます。

トランジットゲートウェイでマルチキャストを有効にし、ドメインに関連付けるVPC添付ファイルを介してマルチキャストトラフィックをマルチキャストソースからマルチキャストグループメンバーに送信できるようにするトランジットゲートウェイマルチキャストドメインを作成できます。

各 VPCまたは VPNアタッチメントは、単一のルートテーブルに関連付けられます。そのルートテーブルは、そのリソースアタッチメントから来るトラフィックのネクストホップを決定します。トランジットゲートウェイ内のルートテーブルでは、 IPv4ターゲットと IPv6CIDRsターゲットの両方を使用できます。ターゲットは VPCsおよび VPN接続です。をアタッチするか、トランジットゲートウェイでVPN接続VPCを作成すると、アタッチメントはトランジットゲートウェイのデフォルトルートテーブルに関連付けられます。

トランジットゲートウェイ内に追加のルートテーブルを作成し、 VPCまたは のVPN関連付けをこれらのルートテーブルに変更できます。これにより、ネットワークをセグメント化することができます。例えば、開発を 1 つのルートテーブルVPCsに、本番稼働を別のルートテーブルVPCsに関連付けることができます。これにより、従来のネットワークの仮想ルーティングや転送 (VRFs) と同様の分離されたネットワークをトランジットゲートウェイ内に作成できます。

トランジットゲートウェイは、アタッチされた とVPN接続間の動的VPCsルーティングと静的ルーティングをサポートします。各アタッチメントのルートの伝播は有効または無効にできます。Transit Gateway ピアリングアタッチメントは、静的ルーティングのみをサポートします。トランジットゲートウェイのルートテーブルをピアリングアタッチメントにポイントして、ピアリングされたトランジットゲートウェイ間でトラフィックをルーティングできます。

オプションで、1 つ以上の IPv4 または IPv6CIDRブロックをトランジットゲートウェイに関連付けることができます。Transit Gateway Connect アタッチメント の Transit Gateway Connect ピアを確立するときに、 CIDRブロックから IP アドレスを指定します。範囲内のアドレス、およびVPCアタッチメントやオンプレミスネットワークのアドレスと重複する`169.254.0.0/16`範囲を除き、パブリックまたはプライベートの IP アドレス範囲を関連付けることができます。IPv4 および IPv6CIDRブロックの詳細については、「Amazon VPC ユーザーガイド」のVPCs「 およびサブネット」を参照してください。

タスク

- Amazon VPC Transit Gateway を使用してトランジットゲートウェイを作成する
- Amazon VPC Transit Gateway を使用してトランジットゲートウェイ情報を表示する
- Amazon VPC Transit Gateway を使用してトランジットゲートウェイのタグを追加または編集する
- Amazon VPC Transit Gateway を使用してトランジットゲートウェイを変更する
- Amazon VPC Transit Gateway を使用してリソース共有を受け入れる
- Amazon VPC Transit Gateway を使用して共有アタッチメントを受け入れる
- Amazon VPC Transit Gateway を使用してトランジットゲートウェイを削除する

Amazon VPC Transit Gateway を使用してトランジットゲートウェイを作成する

Transit Gateway を作成すると、デフォルトの Transit Gateway ルートテーブルが作成され、それをデフォルトの関連付けルートテーブルおよびデフォルトの伝達ルートテーブルとして使用します。デフォルトの Transit Gateway ルートテーブルを作成しない場合は、後で作成できます。ルートおよびルートテーブルについての詳細は、「???」を参照してください。

コンソールを使用して Transit Gateway を作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateways] を選択します。
3. [Transit Gateway の作成] を選択します。
4. オプションで、[名前タグ] に Transit Gateway の名前を入力します。名前タグを使用すると、ゲートウェイのリストから特定のゲートウェイを識別しやすくなります。[名前タグ] を追加すると、[名前] というキーと、入力した値と同じ値のタグが作成されます。
5. オプションで、[説明] に、Transit Gateway の説明を入力します。
6. Amazon 側の自律システム番号 (ASN) の場合、デフォルト値のままにしておくと、デフォルトを使用するか、トランジットゲートウェイASNのプライベートASNを入力します。これは、ボーダーゲートウェイプロトコル (BGP) セッションの ASN AWS 側である必要があります。

   16 ビット の場合、範囲は 64512 ~ 65534 ですASNs。

   32 ビット の場合、範囲は 4200000000 ~ 4294967294 ですASNs。

マルチリージョンデプロイの場合は、各トランジットゲートウェイASNに一意の を使用することをお勧めします。

7. DNS をサポートするには、トランジットゲートウェイVPCにアVPCタッチされた別の のインスタンスからクエリを実行するときに、パブリックIPv4DNSホスト名をプライベートIPv4アドレスに解決するために が必要な場合は、このオプションを選択します。
8. VPN ECMP サポートについては、VPNトンネル間で等コストマルチパス (ECMP) ルーティングのサポートが必要な場合は、このオプションを選択します。接続が同じ をアドバタイズする場合CIDRs、トラフィックはそれらの間で均等に分散されます。

   このオプションを選択すると、アドバタイズされる BGP ASN、AS パスなどのBGP属性は同じである必要があります。

   > **Note**
   >
   > を使用するにはECMP、動的ルーティングを使用するVPN接続を作成する必要があります。VPN 静的ルーティングを使用する 接続は をサポートしていませんECMP。

9. [デフォルトルートテーブルの関連付け]で、Transit Gateway アタッチメントを Transit Gateway のデフォルトルートテーブルに自動的に関連付けるには、このオプションを選択します。
10. [デフォルトルートテーブルの伝播] で、Transit Gateway アタッチメントを Transit Gateway のデフォルトルートテーブルに自動的に伝達するには、このオプションを選択します。
11. (オプション) トランジットゲートウェイをマルチキャストトラフィックのルーターとして使用するには、[マルチキャストのサポート] を選択します。
12. (オプション) C onfigure-cross-account 共有オプションセクションで、共有アタッチメント を自動で受け入れるかどうかを選択します。有効にすると、添付ファイルは自動的に受け入れられます。それ以外の場合は、添付ファイルリクエストを承諾または拒否する必要があります。

    [共有アタッチメントを自動的に受け入れる]で、このオプションを選択して、アカウント間のアタッチメントを自動的に受け入れます。
13. (オプション) トランジットゲートウェイCIDRブロック には、トランジットゲートウェイに 1 つ以上の IPv4 または IPv6CIDRブロックを指定します。

    にはサイズ /24 CIDRブロック以上 (例: /23 または /22)IPv4、 にはサイズ /64 CIDRブロック以上 (例: /63 または /62) を指定できますIPv6。169.254.0.0/16 範囲のアドレス、およびVPCアタッチメントとオンプレミスネットワークのアドレスと重複するアドレスを除き、任意のパブリックまたはプライベート IP アドレス範囲を関連付けることができます。

> **Note**
>
> トランジットゲートウェイCIDRブロックは、Connect (GRE) アタッチメントまたは PrivateIP を設定する場合に使用されますVPNs。Transit Gateway は、この範囲のトンネルエンドポイント (GRE/PrivateIPVPN) IPsに を割り当てます。

14. [Transit Gateway の作成] を選択します。

を使用してトランジットゲートウェイを作成するには AWS CLI

create-transit-gateway コマンドを使用します。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイ情報を表示する

トランジットゲートウェイのいずれかを表示します。

コンソールを使用してトランジットゲートウェイを表示するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、トランジットゲートウェイ を選択します。トランジットゲートウェイの詳細がページ上のゲートウェイのリストの下に表示されます。

を使用してトランジットゲートウェイを表示するには AWS CLI

describe-transit-gateway コマンドを使用します。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイのタグを追加または編集する

目的、所有者、環境などに応じて、タグを整理して識別しやすくするために、リソースにタグを追加します。各 Transit Gateway に対して複数のタグを追加できます。タグキーは、各 Transit Gateway で一意である必要があります。すでに Transit Gateway 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。詳細については、「Amazon EC2リソースのタグ付け」を参照してください。

コンソールを使用して Transit Gateway にタグを追加する

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateways] を選択します。
3. タグを追加または編集するトランジットゲートウェイを選択します。
4. ページ下部の [タグ] タブをクリックします。
5. [Manage tags (タグの管理)] を選択します。
6. 新しいタグを追加を選択します。
7. タグの [キー] と [値] を入力します。
8. [Save] を選択します。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイを変更する

Transit Gateway の設定オプションを変更できます。Transit Gateway を変更すると、変更されたオプションは新しい Transit Gateway アタッチメントにのみ適用されます。既存の Transit Gateway アタッチメントは変更されず、サービスの中断も見られません。

共有されている Transit Gateway を変更することはできません。

Connect ピア に現在使用されている IP アドレスがある場合は、トランジットゲートウェイのCIDR ブロックを削除することはできません。

Transit Gateway を変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway] を選択します。
3. 変更するTransit Gatewayを選択します。
4. アクション、Transit Gateway の変更を選択します。
5. 必要に応じてオプションを変更し、[トランジットゲートウェイの変更] をクリックします。

を使用してトランジットゲートウェイを変更するには AWS CLI

modify-transit-gateway コマンドを使用します。

Amazon VPC Transit Gateway を使用してリソース共有を受け入れる

ユーザーがリソース共有に追加された場合は、リソース共有に参加するための招待状を受け取ります。共有リソースにアクセスする前に、リソース共有を受け入れる必要があります。

リソース共有を受け入れるには

1. で AWS RAM コンソールを開きますhttps://console.aws.amazon.com/ram/。
2. ナビゲーションペインで、[自分と共有]、[リソース共有] の順に選択します。
3. リソース共有を選択します。
4. [リソース共有を受け入れる] を選択します。
5. 共有トランジットゲートウェイを表示するには、Amazon コンソールでトランジットゲートウェイページを開きます。 VPC

Amazon VPC Transit Gateway を使用して共有アタッチメントを受け入れる

トランジットゲートウェイの作成時に共有アタッチメントの自動承諾機能を有効にしなかった場合は、Amazon VPC コンソールまたは を使用して、クロスアカウント (共有) アタッチメントを手動で承諾する必要があります AWS CLI。

共有アタッチメントを手動で受け入れるには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. 承認保留中の Transit Gateway アタッチメントを選択します。
4. アクション、Transit Gateway アタッチメントを受け入れるを選択します。

を使用して共有アタッチメントを受け入れるには AWS CLI

accept-transit-gateway-vpc-attachment コマンドを使用します。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイを削除する

既存のアタッチメントを含む Transit Gateway を削除することはできません。Transit Gateway を削除する前に、すべてのアタッチメントを削除する必要があります。

コンソールを使用して Transit Gateway を削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. 削除する Transit Gateway を選択します。
3. アクション,Transit Gateway の削除を選択します。「**delete**」と入力して、[Delete (削除)] を選択して削除を確認します。

を使用してトランジットゲートウェイを削除するには AWS CLI

delete-transit-gateway コマンドを使用します。

Amazon VPC Transit Gateway の Amazon VPCアタッチメント

をトランジットゲートウェイVPCにアタッチするときは、トラフィックをルーティングするためにトランジットゲートウェイが使用する各アベイラビリティーゾーンから 1 つのサブネットを指定する必要があります。1 つのアベイラビリティーゾーンから 1 つのサブネットを指定すると、そのアベイラビリティーゾーン内のすべてのサブネットのリソースにトラフィックが到達できるようになります。

制限

- をトランジットゲートウェイVPCにアタッチすると、トランジットゲートウェイアタッチメントがないアベイラビリティーゾーン内のリソースはトランジットゲートウェイに到達できません。Transit Gateway へのルートがサブネットルートテーブルにある場合、トラフィックが Transit Gateway に転送されるのは、Transit Gateway のアタッチメントが同じアベイラビリティーゾーンのサブネットにある場合のみです。
- トランジットゲートウェイにアVPCタッチされた のリソースは、同じトランジットゲートウェイにもアタッチVPCされている別の のセキュリティグループにアクセスできません。
- Transit Gateway は、Amazon Route 53 のプライベートホストゾーンを使用してVPCsセットアップされたアタッチされたカスタムDNS名のDNS解決をサポートしていません。トランジットゲー

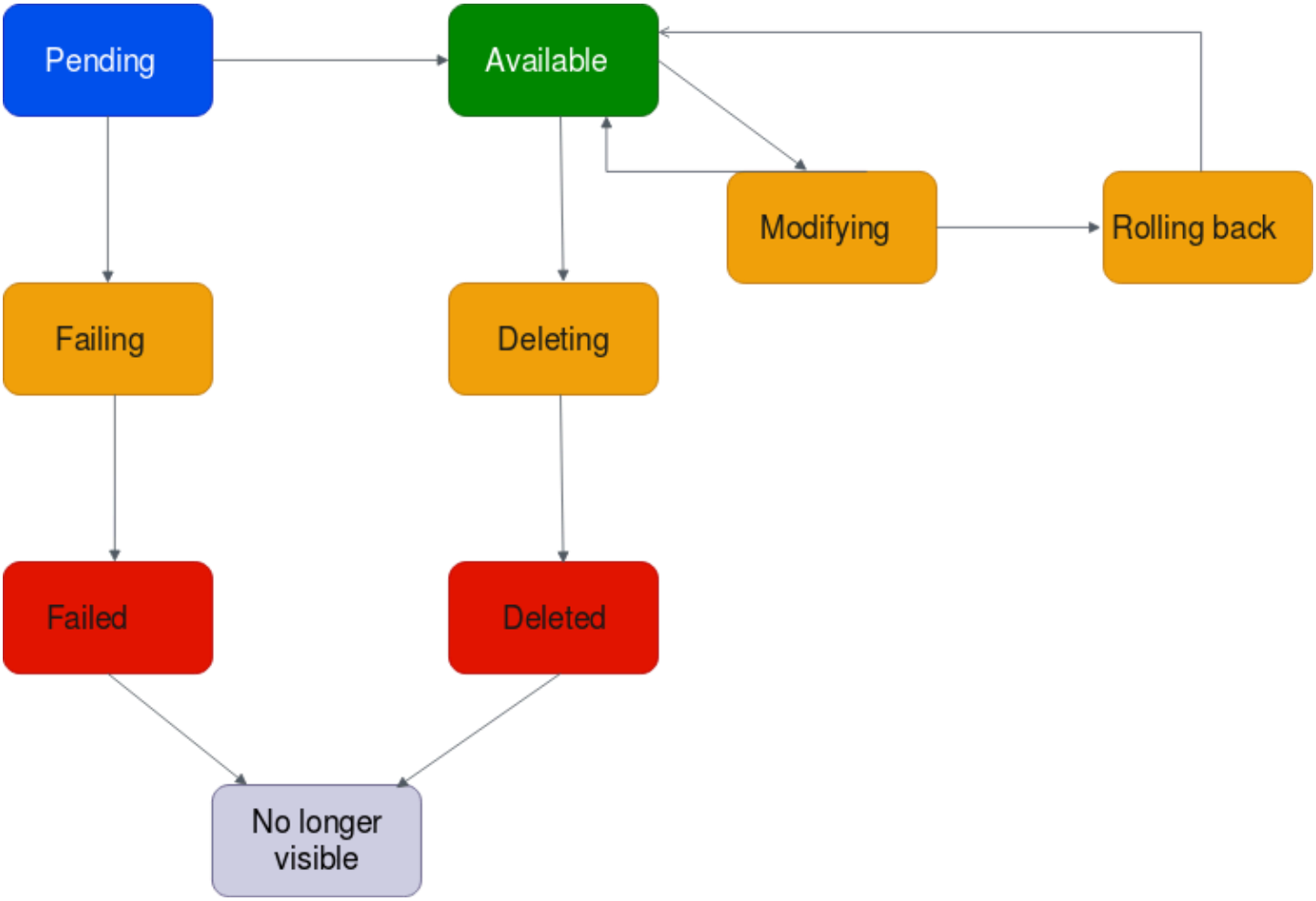
トウェイにアVPCsタッチされたすべての のプライベートホストゾーンの名前解決を設定するには、「Amazon Route 53 と AWS Transit Gateway によるハイブリッドクラウドの集中DNS管理」を参照してください。

- トランジットゲートウェイは、同じ VPCsを持つ 間のルーティングをサポートしていません CIDRs。VPC をトランジットゲートウェイにアタッチし、その CIDRがトランジットゲートウェイに既にアタッチVPCされている別の の と同じである場合、新しくアタッチされた CIDRのルート VPCはトランジットゲートウェイのルートテーブルに伝達されません。
- ローカルゾーンに存在するVPCサブネットのアタッチメントを作成することはできません。ただし、ローカルゾーンのサブネットを、親アベイラビリティーゾーンを介して Transit Gateway に接続できるようにネットワークを設定することが可能です。詳細については、「ローカルゾーンのサブネットを Transit Gateway に接続する」を参照してください。
- IPv6専用サブネットを使用してトランジットゲートウェイアタッチメントを作成することはできません。トランジットゲートウェイアタッチメントサブネットはIPv4アドレスもサポートする必要があります。
- トランジットゲートウェイをルートテーブルに追加するには、トランジットゲートウェイに少なくとも 1 つのVPCアタッチメントが必要です。

VPC アタッチメントのライフサイクル

VPC アタッチメントは、リクエストが開始されたときからさまざまな段階を経ます。各ステージで実行できるアクションがあり、ライフサイクルの最後に、VPC添付ファイルは および APIまたはコマンドライン出力に一定期間表示されます Amazon Virtual Private Cloud Console 。

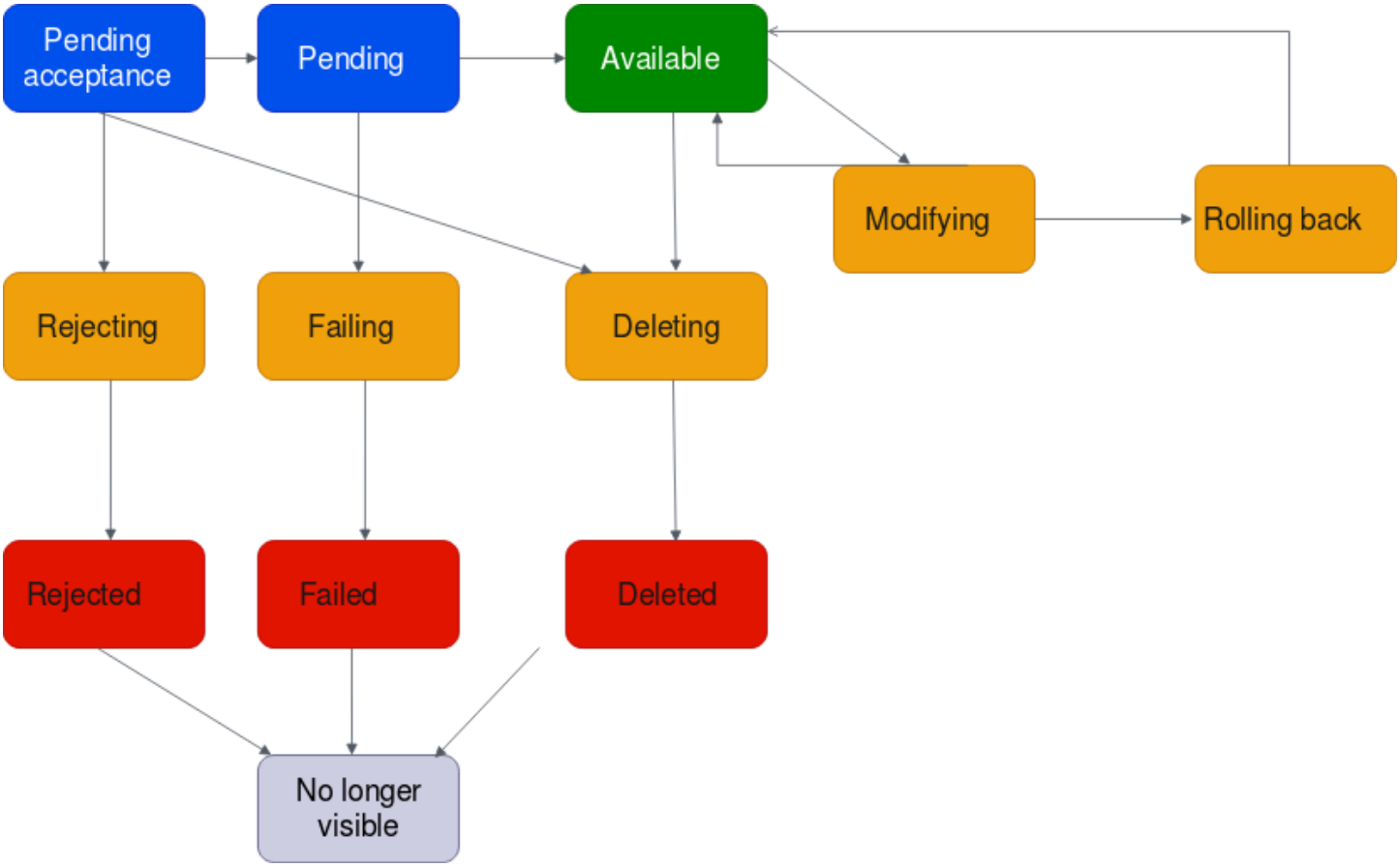
次の図は、単一のアカウント設定、または [共有アタッチメントを自動承諾] がオンになっているクロスアカウント設定で、アタッチメントが経る可能性のある状態を示しています。



- 保留中: VPCアタッチメントのリクエストが開始され、プロビジョニングプロセス中です。この段階では、アタッチメントは失敗するか、または `available` になる場合があります。
- 失敗： VPC添付ファイルのリクエストが失敗しています。この段階では、VPC添付ファイルは になりますfailed。
- 失敗： VPC添付ファイルのリクエストが失敗しました。この状態では、削除できません。失敗したVPCアタッチメントは 2 時間表示され、その後表示されなくなります。
- 使用可能な : VPCアタッチメントが使用可能で、トラフィックが VPCとトランジットゲートウェイの間で流れる可能性があります。この段階では、アタッチメントは `modifying` または `deleting` になる場合があります。
- の削除: 削除中のVPC添付ファイル。この段階では、アタッチメントは `deleted` になる場合があります。
- 削除済み： `available`VPC添付ファイルが削除されました。この状態にある間は、VPCアタッチメントを変更することはできません。VPC 添付ファイルは 2 時間表示され、その後表示されなくなります。

- の変更: VPC添付ファイルのプロパティを変更するリクエストが行われました。この段階では、アタッチメントは `available` または `rolling back` になる場合があります。
- ロールバック: VPCアタッチメント変更リクエストを完了できず、システムは行われた変更を元に戻しています。この段階では、アタッチメントは `available` になる場合があります。

次の図は、[Auto accept shared attachments] (共有アタッチメントを自動承諾) がオフになっているクロスアカウント設定で、アタッチメントが経る可能性のある状態を示しています。



- Pending-acceptance : VPCアタッチメントリクエストは承認を待っています。この段階では、アタッチメントは `pending`、`rejecting`、または `deleting` になる場合があります。
- 拒否中: 拒否中のVPC添付ファイル。この段階では、アタッチメントは `rejected` になる場合があります。
- 拒否済み： `pending acceptance`VPC添付ファイルが拒否されました。この状態にある間は、VPCアタッチメントを変更することはできません。VPC 添付ファイルは 2 時間表示され、その後表示されなくなります。
- 保留中: VPCアタッチメントが受け入れられ、プロビジョニングプロセス中です。この段階では、アタッチメントは失敗するか、または `available` になる場合があります。

- 失敗： VPC添付ファイルのリクエストが失敗しています。この段階では、VPC添付ファイルは になりますfailed。
- 失敗： VPCアタッチメントのリクエストが失敗しました。この状態では、削除できません。失敗したVPCアタッチメントは 2 時間表示され、その後表示されなくなります。
- 使用可能な : VPCアタッチメントが使用可能で、トラフィックが VPCとトランジットゲートウェイの間で流れる可能性があります。この段階では、アタッチメントは modifying または deleting になる場合があります。
- の削除: 削除中のVPC添付ファイル。この段階では、アタッチメントは deleted になる場合があります。
- 削除済み： availableまたは pending acceptanceVPCアタッチメントが削除されました。この状態にある間は、VPCアタッチメントを変更することはできません。VPC 添付ファイルは 2 時間表示され、その後表示されなくなります。
- の変更: VPC添付ファイルのプロパティを変更するリクエストが行われました。この段階では、アタッチメントは available または rolling back になる場合があります。
- ロールバック: VPCアタッチメント変更リクエストを完了できず、システムは行われた変更を元に戻しています。この段階では、アタッチメントは available になる場合があります。

タスク

- Amazon VPC Transit Gateway を使用してVPCアタッチメントを作成する
- Amazon VPC Transit Gateway を使用してVPCアタッチメントを変更する
- Amazon VPC Transit Gateway を使用してVPCアタッチメントタグを変更する
- Amazon VPC Transit Gateway を使用してVPCアタッチメントを表示する
- Amazon VPC Transit Gateway を使用してVPCアタッチメントを削除する
- Amazon VPC Transit Gateways VPCアタッチメント作成のトラブルシューティング

Amazon VPC Transit Gateway を使用してVPCアタッチメントを作成する

コンソールを使用してVPCアタッチメントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. [Transit Gateway アタッチメントの作成] を選択します。
4. オプションで、[名前タグ] に Transit Gateway アタッチメントの名前を入力します。

5. [Transit Gateway ID] で、アタッチメントの Transit Gateway を選択します。所有している Transit Gateway 、または自分と共有されたTransit Gateway を選択できます。
6. 添付ファイルタイプ で、 を選択しますVPC。
7. サポート、DNSサポート、アプライアンスモードIPv6のサポートを有効にするかどうかを選択します。

   アプライアンスモードを選択した場合、送信元と送信先の間のトラフィックフローは、そのフローの存続期間中、VPCアタッチメントに同じアベイラビリティーゾーンを使用します。
8. VPC ID には、トランジットゲートウェイにVPCアタッチする を選択します。

   これには、少なくとも 1 つのサブネットが関連付けられているVPC必要があります。
9. サブネット IDsで、トラフィックをルーティングするためにトランジットゲートウェイが使用するアベイラビリティーゾーンごとに 1 つのサブネットを選択します。少なくとも 1 つのサブネットを選択する必要があります。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選択できます。
10. [Transit Gateway アタッチメントの作成] を選択します。

を使用してVPC添付ファイルを作成するには AWS CLI

create-transit-gateway-vpc-attachment コマンドを使用します。

Amazon VPC Transit Gateway を使用してVPCアタッチメントを変更する

コンソールを使用してVPC添付ファイルを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. VPC アタッチメントを選択し、アクション、トランジットゲートウェイアタッチメントの変更を選択します。
4. 次のいずれかを有効または無効にします。

   - DNS サポート
   - IPv6 サポート
   - アプライアンスモードのサポート
5. アタッチメントからサブネットを追加または削除するには、追加または削除するサブネット ID のチェックボックスを選択またはオフにします。

> **Note**
>
> VPC アタッチメントサブネットを追加または変更すると、アタッチメントが変更状態にある間、データトラフィックに影響する可能性があります。

6. Transit Gateway のアタッチメントの変更を選択します。

を使用してVPC添付ファイルを変更するには AWS CLI

modify-transit-gateway-vpc-attachment コマンドを使用します。

Amazon VPC Transit Gateway を使用してVPCアタッチメントタグを変更する

コンソールを使用してVPCアタッチメントタグを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. VPC アタッチメントを選択し、アクション、タグの管理 を選択します。
4. [タグの追加] [新しいタグの追加] を選択して、以下を実行します。
   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。
5. [Remove a tag (タグの削除)] タグの横にある [削除] を選択します。
6. [Save] を選択します。

   VPC アタッチメントタグは、コンソールを使用してのみ変更できます。

Amazon VPC Transit Gateway を使用してVPCアタッチメントを表示する

コンソールを使用してVPC添付ファイルを表示するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. リソースタイプ列で、 を探しますVPC。これらはVPC添付ファイルです。

4. 詳細を表示するには、アタッチメントを選択します。

を使用してVPC添付ファイルを表示するには AWS CLI

describe-transit-gateway-vpc-attachments コマンドを使用します。

Amazon VPC Transit Gateway を使用してVPCアタッチメントを削除する

コンソールを使用してVPC添付ファイルを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. VPC 添付ファイルを選択します。
4. アクション、Transit Gateway のアタッチメントの削除を選択します。
5. 確認を求めるメッセージが表示されたら、「**delete**」と入力し、[削除] を選択します。

を使用してVPC添付ファイルを削除するには AWS CLI

delete-transit-gateway-vpc-attachment コマンドを使用します。

Amazon VPC Transit Gateways VPCアタッチメント作成のトラブルシューティング

次のトピックは、VPC添付ファイルの作成時に発生する可能性のある問題のトラブルシューティングに役立ちます。

問題

VPC 添付ファイルが失敗しました。

原因

原因は、次のいずれかである可能性があります。

1. VPC アタッチメントを作成しているユーザーには、サービスにリンクされたロールを作成するための正しいアクセス許可がありません。
2. IAM リクエストが多すぎるため、スロットリングの問題があります。例えば、 AWS CloudFormation を使用してアクセス許可とロールを作成しています。

3. サービスにリンクされたロールがアカウントにあり、サービスにリンクされたロールが変更されました。
4. トランジットゲートウェイは `available` 状態にありません。

ソリューション

原因に応じて、次をお試しください。

1. サービスにリンクされたロールを作成するための適切なアクセス権限がユーザーに付与されていることを確認します。詳細については、「 ユーザーガイド」の「サービスにリンクされたロールのアクセス許可IAM」を参照してください。ユーザーがアクセス許可を取得したら、VPC添付ファイルを作成します。
2. コンソールまたは を使用してVPCアタッチメントを手動で作成しますAPI。詳細については、「the section called “VPC 添付ファイルを作成する”」を参照してください。
3. サービスにリンクされたロールに正しいアクセス権限があることを確認します。詳細については、「the section called “Transit Gateway”」を参照してください。
4. トランジットゲートウェイが `available` 状態であることを確認します。詳細については、「the section called “トランジットゲートウェイを表示する”」を参照してください。

Amazon VPC Transit Gateway の Site-to-Site VPNアタッチメント

トランジットゲートウェイVPNに接続をアタッチするには、カスタマーゲートウェイを指定する必要があります。VPN カスタマーゲートウェイには特定の要件があります。ゲートウェイ設定ファイルの例など、カスタマーゲートウェイデバイスの要件の詳細については、「 AWS Site-to-Site VPN ユーザーガイド」の「カスタマーゲートウェイデバイスの要件」を参照してください。

静的 の場合VPNs、静的ルートをトランジットゲートウェイルートテーブルに追加する必要があります。VPN アタッチメントをターゲットとするトランジットゲートウェイルートテーブルの静的ルートは、Site-to-Site によってフィルタリングされません。VPNこれにより、 BGPベースの を使用するときに意図しないアウトバウンドトラフィックフローが許可される可能性があるためですVPN。トランジットゲートウェイルートテーブルに静的ルートを追加する手順については、「」を参照してください静的ルートを作成する。

Amazon VPCコンソールまたは を使用して、トランジットゲートウェイの Site-to-Site VPNアタッチメントを作成、表示、または削除できます AWS CLI。

タスク

- Amazon VPC Transit Gateway VPNを使用して へのトランジットゲートウェイアタッチメントを作成する
- Amazon VPC Transit Gateway を使用してVPNアタッチメントを表示する
- Amazon VPC Transit Gateway を使用してVPNアタッチメントを削除する

Amazon VPC Transit Gateway VPNを使用して へのトランジットゲートウェイアタッチメントを作成する

コンソールを使用してVPNアタッチメントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. [Transit Gateway アタッチメントの作成] を選択します。
4. [Transit Gateway ID] で、アタッチメントの Transit Gateway を選択します。所有している Transit Gateway を選択できます。
5. 添付ファイルタイプ で、 を選択しますVPN。
6. [カスタマーゲートウェイ] で、以下のいずれかを実行します。
   - 既存のカスタマーゲートウェイを使用するには、[Existing (既存)] を選択してから、使用するゲートウェイを選択します。

     カスタマーゲートウェイがNATトラバーサル (NAT-TNAT) が有効になっているネットワークアドレス変換 () デバイスの内側にある場合は、NATデバイスのパブリック IP アドレスを使用し、ファイアウォールルールを調整してUDPポート 4500 のブロックを解除します。
   - カスタマーゲートウェイを作成するには、新規 を選択し、IP アドレス に静的パブリック IP アドレス と BGP ASNを入力します。

     [ルーティング] オプションで、[動的] と [静的] のどちらを使用するかを選択します。詳細については、「 ユーザーガイド」の「Site-to-Site VPNルーティングオプションAWS Site-to-Site VPN 」を参照してください。
7. トンネルオプション には、トンネルCIDRの範囲と事前共有キーを入力します。詳細については、「Site-to-Site VPNアーキテクチャ」を参照してください。
8. [Transit Gateway アタッチメントの作成] を選択します。

を使用してVPN添付ファイルを作成するには AWS CLI

create-vpn-connection コマンドを使用します。

Amazon VPC Transit Gateway を使用してVPNアタッチメントを表示する

コンソールを使用してVPN添付ファイルを表示するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. リソースタイプ列で、 を探しますVPN。これらはVPN添付ファイルです。
4. アタッチメントを選択して、詳細を表示したりタグを追加したりします。

を使用してVPN添付ファイルを表示するには AWS CLI

describe-transit-gateway-attachments コマンドを使用します。

Amazon VPC Transit Gateway を使用してVPNアタッチメントを削除する

コンソールを使用してVPN添付ファイルを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. VPN 添付ファイルを選択します。
4. VPN 接続のリソース ID を選択して、VPN接続ページに移動します。
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、[削除] を選択します。

を使用してVPN添付ファイルを削除するには AWS CLI

delete-vpn-connection コマンドを使用します。

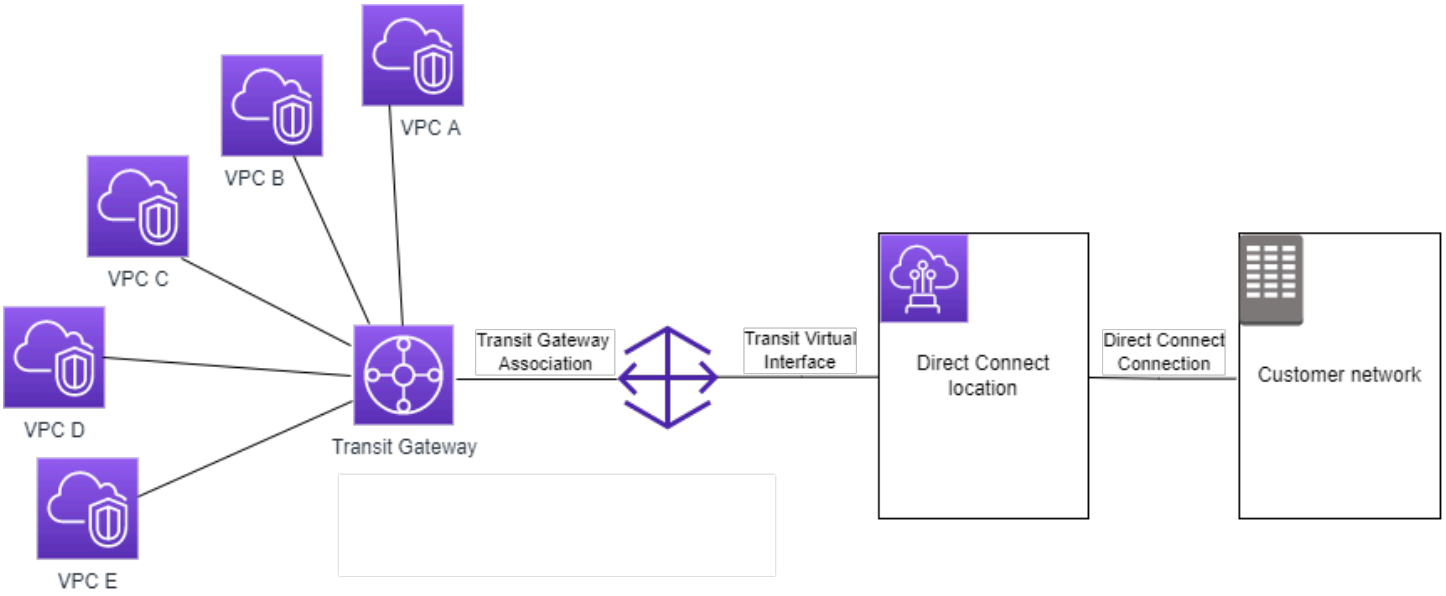
Amazon Transit Gateway の Direct Connect ゲートウェイへのVPC トランジットゲートウェイアタッチメント

トランジットゲートウェイで Direct Connect ゲートウェイアタッチメントを操作します。この設定には次のような利点があります。以下を実行できます。

- 同じ リージョンにある複数の VPCsまたは VPNs の 1 つの接続を管理します。

- プレフィックスをオンプレミスからオンプレミスへ、 AWS またはオンプレミスからオンプレミス AWS へアドバタイズします。

次の図は、Direct Connect ゲートウェイを使用して、すべての がVPCs使用できる Direct Connect 接続への単一の接続を作成する方法を示しています。



このソリューションには、次のコンポーネントが必要です。

- トランジットゲートウェイ。
- Direct Connect ゲートウェイ
- Direct Connect ゲートウェイと Transit Gateway の間の関連付け。
- トランジット仮想インターフェイスを使用して、Direct Connect ゲートウェイにトランジットゲートウェイをアタッチします。

トランジットゲートウェイを使用した Direct Connect ゲートウェイの設定の詳細については、AWS Direct Connect ユーザーガイドの「トランジットゲートウェイの関連付け」を参照してください。

Amazon Transit Gateway のVPCトランジットゲートウェイピアリングアタッチメント

リージョン内とリージョン間のトランジットゲートウェイの両方をピアリングし、 IPv4および トラフィックを含むトラフィックをそれらのIPv6間でルーティングできます。これを行うには、Transit Gateway にピアリングアタッチメントを作成し、Transit Gateway を指定します。ピアトランジット

ゲートウェイは アカウントにある必要があります。ピアリングアタッチメントは、ユーザーと共有される可能性のあるトランジットゲートウェイでは使用できません。

ピアリングアタッチメントリクエストを作成した後、ピアTransit Gateway（アクセプタTransit Gateway とも呼ばれる）の所有者がリクエストを受け入れる必要があります。Transit Gateway 間でトラフィックをルーティングするには、Transit Gateway のピアリングアタッチメントをポイントする静的ルートをTransit Gateway のルートテーブルに追加します。

将来のルート伝達機能を利用するには、ピアリングされたトランジットゲートウェイASNsごとに一意の を使用することをお勧めします。

トランジットゲートウェイピアリングでは、 Amazon Route 53 Resolver 別のリージョンの を使用して、トランジットゲートウェイピアリングアタッチメントの両側VPCsにあるプライベートIPv4アドレスへのパブリックホスト名またはプライベートIPv4DNSホスト名の解決をサポートしていません。Route 53 リゾルバーの詳細については、「Amazon Route 53 デベロッパーガイド」の「Route 53 Resolver の使用開始」を参照してください。

リージョン間ゲートウェイピアリングは、VPCピアリングと同じネットワークインフラストラクチャを使用します。したがって、トラフィックは、リージョン間を移動する仮想ネットワークレイヤーで AES-256 暗号化を使用して暗号化されます。また、トラフィックは、 の物理的な制御の範囲外にあるネットワークリンクを通過するときに、物理レイヤーで AES-256 暗号化を使用して暗号化されます AWS。その結果、トラフィックは の物理的な制御の外部にあるネットワークリンクで二重に暗号化されます AWS。同じリージョン内では、トラフィックは、 AWSの物理的な制御の外部にあるネットワークリンクを通過する場合にのみ、物理レイヤーで暗号化されます。

どのリージョンがトランジットゲートウェイピアリングアタッチメントをサポートしているかについては、AWS 「トランジットゲートウェイFAQs」を参照してください。

オプトイン AWS リージョンに関する考慮事項

オプトインリージョンの境界を越えて Transit Gateway をピアリングできます。これらのリージョンの詳細とオプトイン方法については、「」のAWS 「リージョンの管理」を参照してくださいAmazon Web Services 全般のリファレンス。これらのリージョンで Transit Gateway ピアリングを使用する場合は、次の点を考慮に入れてください。

- ピアリングアタッチメントを受け入れるアカウントがそのリージョンにオプトインされている限り、オプトインリージョンにピアリングできます。
- リージョンのオプトインステータスに関係なく、 はピアリングアタッチメントを受け入れるアカウントと次のアカウントデータ AWS を共有します。

  - AWS アカウント ID
  - 転送ゲートウェイ ID
  - リージョンコード
- Transit Gateway のアタッチメントを削除すると、上記のアカウントデータが削除されます。
- リージョンをオプトアウトする前に、Transit Gateway ピアリングのアタッチメントを削除することを推奨します。ピアリングアタッチメントを削除しないと、トラフィックがアタッチメントを通過し続け、引き続き課金される可能性があります。アタッチメントを削除しない場合は、オプトインし直し、アタッチメントを削除できます。
- 一般に、Transit Gateway には送信者支払いモデルがあります。オプトイン境界を越えて Transit Gateway ピアリングアタッチメントを使用すると、アタッチメントを受け入れるリージョン (オプトインしていないリージョンを含む) で料金が発生する可能性があります。詳細については、AWS Transit Gateway の料金を参照してください。

タスク

- Amazon VPC Transit Gateway を使用してピアリングアタッチメントを作成する
- Amazon VPC Transit Gateway を使用してピアリングアタッチメントリクエストを承諾または拒否する
- Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルにルートを追加する
- Amazon VPC Transit Gateway を使用してピアリングアタッチメントを削除する

Amazon VPC Transit Gateway を使用してピアリングアタッチメントを作成する

開始する前に、アタッチするTransit Gateway の ID があることを確認します。トランジットゲートウェイが別の にある場合は AWS アカウント、トランジットゲートウェイの所有者の AWS アカウント ID があることを確認してください。

ピアリングアタッチメントを作成した後、アクセプタTransit Gateway の所有者はアタッチメントリクエストを受け入れる必要があります。

コンソールを使用して、ピアリングアタッチメントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。

2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. [Transit Gateway アタッチメントの作成] を選択します。
4. [Transit Gateway ID] で、アタッチメントの Transit Gateway を選択します。所有している Transit Gateway を選択できます。自分と共有されているトランジットゲートウェイは、ピアリングに使用できません。
5. [アタッチメントの種類] で、[ピア接続] を選択します。
6. 必要に応じて、アタッチメントの名前タグを入力します。
7. [アカウント] で、次のいずれかを実行します。
   - Transit Gateway がアカウントにある場合は、[マイアカウント] を選択します。
   - トランジットゲートウェイが異なる にある場合は AWS アカウント、その他のアカウント を選択します。[アカウント ID] に AWS アカウント ID を入力します。
8. [リージョン] で、Transit Gateway があるリージョンを選択します。
9. [Transit Gateway ID (アクセプタ)] に、アタッチする Transit Gateway の ID を入力します。
10. [Transit Gateway アタッチメントの作成] を選択します。

を使用してピアリングアタッチメントを作成するには AWS CLI

create-transit-gateway-peering-attachment コマンドを使用します。

Amazon VPC Transit Gateway を使用してピアリングアタッチメントリクエストを承諾または拒否する

ピアリングアタッチメントをアクティブにするには、アクセプタ Transit Gateway の所有者がピアリングアタッチメントリクエストを受け入れる必要があります。これは、両方の Transit Gateway が同じアカウントにある場合でも必要です。ピアリングアタッチメントは `pendingAcceptance` 状態である必要があります。アクセプタ Transit Gateway が配置されているリージョンからのピアリングアタッチメントリクエストを受け入れます。

または、受信した VPC ピア接続リクエストで `pendingAcceptance` 状態にあるものを拒否できます。アクセプタ Transit Gateway があるリージョンからのリクエストを拒否する必要があります。

コンソールを使用して、ピアリングアタッチメントリクエストを受け入れるには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。

3. 承認保留中の Transit Gateway ピアリングアタッチメントを選択します。
4. アクション、Transit Gateway アタッチメントを受け入れるを選択します。
5. 静的ルートを Transit Gateway のルートテーブルに追加します。詳細については、「the section called “静的ルートを作成する”」を参照してください。

コンソールを使用して、ピアリングアタッチメントリクエストを拒否するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. 承認保留中の Transit Gateway ピアリングアタッチメントを選択します。
4. アクション、Transit Gateway アタッチメントを拒否するを選択します。

を使用してピアリングアタッチメントを承諾または拒否するには AWS CLI

accept-transit-gateway-peering-attachment コマンドと reject-transit-gateway-peering-attachment コマンドを使用します。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルにルートを追加する

ピアリングされた Transit Gateway 間でトラフィックをルーティングするには、Transit Gateway のピアリングアタッチメントをポイントする静的ルートを Transit Gateway のルートテーブルに追加する必要があります。アクセプタTransit Gateway の所有者も、Transit Gateway ルートテーブルに静的ルートを追加する必要があります。

コンソールを使用して静的ルートを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートを作成するルートテーブルを選択します。
4. [アクション]、[静的ルートの作成] の順に選択します。
5. 静的ルートの作成ページで、ルートを作成するCIDRブロックを入力します。例えば、ピアトランジットゲートウェイにアタッチVPCされている のCIDRブロックを指定します。
6. ルートのピアリングアタッチメントを選択します。
7. [静的ルートの作成] を選択します。

を使用して静的ルートを作成するには AWS CLI

create-transit-gateway-route コマンドを使用します。

> **Important**
>
> ルートを作成したら、Transit Gateway ルートテーブルをTransit Gateway ピアリングアタッチメントに関連付けます。詳細については、「the section called “Transit Gateway ルートテーブルの関連付け”」を参照してください。

Amazon VPC Transit Gateway を使用してピアリングアタッチメントを削除する

Transit Gateway ピアリングアタッチメントを削除できます。いずれかの Transit Gateway の所有者は、アタッチメントを削除できます。

コンソールを使用して、ピアリングアタッチメントを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. Transit Gateway ピアリングアタッチメントを選択します。
4. アクション,Transit Gateway のアタッチメントの削除を選択します。
5. 「**delete**」と入力し、[Delete (削除)] を選択します。

を使用してピアリングアタッチメントを削除するには AWS CLI

delete-transit-gateway-peering-attachment コマンドを使用します。

Amazon Transit Gateway の Transit Gateway Connect アタッチメントと Transit Gateway Connect VPC ピア

Transit Gateway Connect アタッチメントを作成して、トランジットゲートウェイと で実行されているサードパーティーの仮想アプライアンス (SD アプライアンスなど) WAN間の接続を確立できますVPC。Connect アタッチメントは、高性能な汎用ルーティングカプセル化 (GRE) トンネルプロトコルと動的ルーティング用のボーダーゲートウェイプロトコル (BGP) をサポートしています。Connect アタッチメントを作成したら、Connect アタッチメントに 1 つ以上のGREトンネル

(Transit Gateway Connect ピア とも呼ばれます) を作成して、Transit Gateway とサードパーティーアプライアンスを接続できます。ルーティング情報を交換するために、GREトンネルを介して 2 つのBGPセッションを確立します。

> **Important**
>
> Transit Gateway Connect ピアは、 マネージドインフラストラクチャで終了する 2 AWSつのBGPピアリングセッションで構成されます。2 つのBGPピアリングセッションはルーティングプレーンの冗長性を提供するため、1 つのBGPピアリングセッションが失われてもルーティングオペレーションには影響しません。両方のBGPセッションから受信したルーティング情報は、指定された Connect ピアに対して累積されます。2 つのBGPピアリングセッションは、定期的なメンテナンス、パッチ適用、ハードウェアのアップグレード、交換などのインフラストラクチャオペレーションからも AWS 保護します。Connect ピアが冗長性のために設定された推奨デュアルBGPピアリングセッションなしで動作している場合、AWS インフラストラクチャのオペレーション中に一時的に接続が失われる可能性があります。Connect ピアで両方のBGPピアリングセッションを設定することを強くお勧めします。アプライアンス側で高可用性をサポートするように複数の Connect ピアを設定している場合は、各 Connect ピアで両方のBGPピアリングセッションを設定することをお勧めします。

Connect アタッチメントは、既存のアタッチメントVPCまたは Direct Connect アタッチメントを基盤となるトランスポートメカニズムとして使用します。これは、トランスポートアタッチメントと呼ばれます。トランジットゲートウェイは、サードパーティーアプライアンスからの一致したGREパケットを Connect アタッチメントからのトラフィックとして識別します。送信元または送信先情報が正しくないパケットを含む他のGREパケットは、トランスポートアタッチメントからのトラフィックとして扱われます。

> **Note**
>
> Direct Connect アタッチメントをトランスポートメカニズムとして使用するには、まず Direct Connect を AWS Transit Gateway と統合する必要があります。この統合を作成する手順については、「 SD-WAN デバイスを AWS Transit Gateway と と統合 AWS Direct Connectする」を参照してください。

Connect ピア

Connect ピア (GRE トンネル) は、次のコンポーネントで構成されます。

ブロック内 CIDR (BGP アドレス)

BGP ピアリングに使用される内部 IP アドレス。169.254.0.0/16 の範囲から /29 CIDRブロックを指定する必要がありますIPv4。オプションで、 fd00::/8の範囲から /125 CIDRブロックを指定できますIPv6。次のCIDRブロックは予約されており、使用できません。

- 169.254.0.0/29
- 169.254.1.0/29
- 169.254.2.0/29
- 169.254.3.0/29
- 169.254.4.0/29
- 169.254.5.0/29
- 169.254.169.248/29

アプライアンスの IPv4範囲から最初のアドレスを BGP IP アドレスとして設定する必要があります。を使用する場合IPv6、内部CIDRブロックが fd00::/125 の場合、アプライアンスのトンネルインターフェイスでこの範囲 (fd00::1) の最初のアドレスを設定する必要があります。

BGP アドレスは、トランジットゲートウェイ上のすべてのトンネルで一意である必要があります。

ピア IP アドレス

Connect ピアのアプライアンス側のピア IP アドレス (GRE外部 IP アドレス) 。これは任意の IP アドレスにすることができます。IP アドレスは IPv4または IPv6 アドレスにすることができますが、トランジットゲートウェイアドレスと同じ IP アドレスファミリーである必要があります。

トランジットゲートウェイアドレス

Connect ピアのトランジットゲートウェイ側のピア IP アドレス (GRE外部 IP アドレス) 。IP アドレスはトランジットゲートウェイCIDRブロックから指定する必要があり、トランジットゲートウェイの Connect アタッチメント全体で一意である必要があります。IP アドレスを指定しない場合、トランジットゲートウェイCIDRブロックから最初に使用可能なアドレスが使用されます。

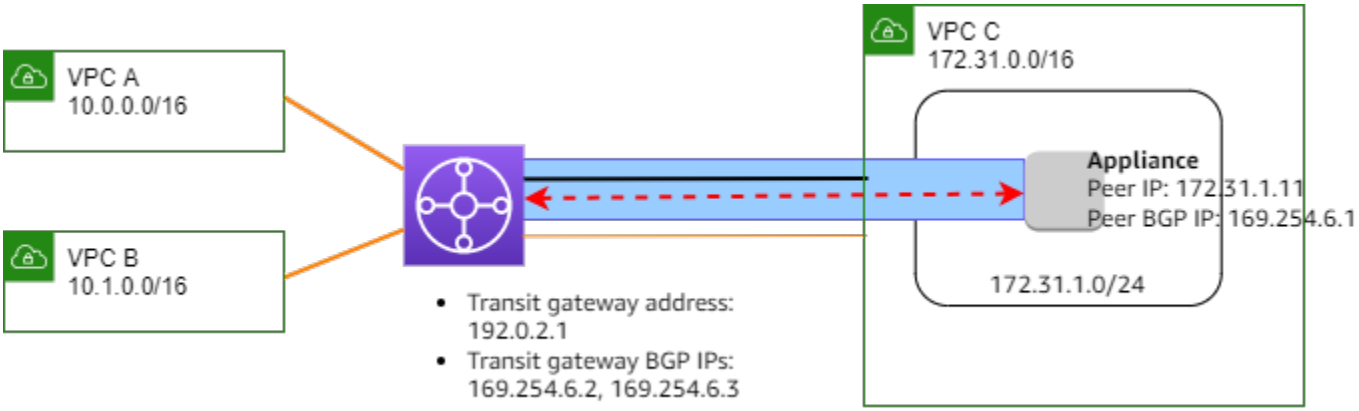
トランジットゲートウェイCIDRブロックは、トランジットゲートウェイを作成または変更するときに追加できます。

IP アドレスは IPv4または IPv6 アドレスにすることができますが、ピア IP アドレスと同じ IP アドレスファミリーである必要があります。

ピア IP アドレスとトランジットゲートウェイアドレスは、GREトンネルを一意に識別するために使用されます。複数のトンネル全体でいずれかのアドレスを再利用することはできますが、同じトンネル内で両方を再利用することはできません。

BGP ピアリング用の Transit Gateway Connect は、マルチプロトコル BGP (MP-BGP) のみをサポートします。Unicast IPv4 のBGPセッションを確立するために IPv6 Unicast アドレス指定も必要です。GRE 外部 IP IPv6 アドレスには、 IPv4と アドレスの両方を使用できます。

次の例は、トランジットゲートウェイと のアプライアンス間の Connect アタッチメントを示していますVPC。



図のコンポーネント	説明
	VPC 添付ファイル
	Connect アタッチメント
	GRE トンネル (Connect ピア)
	BGP ピアリングセッション

前の例では、Connect アタッチメントが既存のVPCアタッチメント (トランスポートアタッチメント) に作成されます。Connect アタッチメントに Connect ピアが作成され、 のアプライアンスへの接続が確立されますVPC。トランジットゲートウェイのアドレスは で192.0.2.1、BGPアドレスの範囲は です169.254.6.0/29。範囲 (169.254.6.1) の最初の IP アドレスは、アプライアンスでピア BGP IP アドレスとして設定されます。

VPC C のサブネットルートテーブルには、トランジットゲートウェイCIDRブロック宛てのトラフィックをトランジットゲートウェイにポイントするルートがあります。

デスティネーション	ターゲット
172.31.0.0/16	ローカル
192.0.2.0/24	tgw-id

要件と考慮事項

Connect アタッチメントの要件と考慮事項は次のとおりです。

- Connect アタッチメントをサポートするリージョンについては、AWS「トランジットゲートウェイFAQ」を参照してください。
- サードパーティーアプライアンスは、Connect アタッチメントを使用してトランジットゲートウェイとの間でGREトンネル経由でトラフィックを送受信するように設定する必要があります。
- 動的ルートの更新とヘルスチェックBGPに使用するようにサードパーティーアプライアンスを設定する必要があります。
- 次のタイプの BGPがサポートされています。
  - 外部 BGP (e BGP): トランジットゲートウェイとは異なる自律システムにあるルーターへの接続に使用されます。e を使用する場合はBGP、ebgp-multihop を time-to-live （ TTL) 値 2 で設定する必要があります。
  - インテリア BGP (i BGP): トランジットゲートウェイと同じ自律システムにあるルーターへの接続に使用されます。トランジットゲートウェイは、ルートが eBGP ピアから発信され、設定されている next-hop-self必要がある場合を除き、iBGP ピア (サードパーティーアプライアンス) からルートをインストールしません。iBGP ピアリングを介してサードパーティーアプライアンスによってアドバタイズされるルートには、 が必要ですASN。
  - MP-BGP (のマルチプロトコル拡張BGP): IPv4や IPv6 アドレスファミリーなど、複数のプロトコルタイプをサポートするために使用されます。
- デフォルトのBGPキープアライブタイムアウトは 10 秒、デフォルトのホールドタイマーは 30 秒です。
- IPv6 BGP ピアリングはサポートされていません。 IPv4ベースのBGPピアリングのみがサポートされています。IPv6 プレフィックスは、MP- を使用してIPv4BGPピアリングを介して交換されますBGP。

- 双方向転送検出 (BFD) はサポートされていません。
- BGP 正常な再起動はサポートされていません。
- トランジットゲートウェイピアを作成するときにピアASN番号を指定しない場合、トランジットゲートウェイASN番号が選択されます。つまり、アプライアンスとトランジットゲートウェイは、i を実行する同じ自律システムに置かれますBGP。
- 2 つの Connect ピアがある場合、BGPAS-PATH 属性を使用する Connect ピアが優先ルートです。

  複数のアプライアンス間で等コストマルチパス (ECMP) ルーティングを使用するには、同じ BGP ASPATH- 属性を持つトランジットゲートウェイに同じプレフィックスをアドバタイズするようにアプライアンスを設定する必要があります。トランジットゲートウェイが使用可能なすべてのECMPパスを選択するには、AS PATHと自律システム番号 (ASN) が一致している必要があります。トランジットゲートウェイは、同じ Connect アタッチメントの Connect ピアECMP間、または同じトランジットゲートウェイ上の Connect アタッチメント間で を使用できます。Transit Gateway は、1 つのBGPピアが確立する両方の冗長ピアリングECMP間で を使用することはできません。
- Connect アタッチメントでは、ルートはデフォルトで Transit Gateway ルートテーブルに伝達されます。
- 静的ルートはサポートされていません。
- サードパーティーアプライアンスの外部インターフェイス (トンネルソース) 最大送信単位 (MTU) が、
  - がGREトンネルインターフェイスMTUの と一致する、または
  - は、GREトンネルインターフェイスのものよりも大きくなければなりません。

タスク

- Amazon VPC Transit Gateway を使用して Connect アタッチメントを作成する
- Amazon VPC Transit Gateway を使用して Connect ピアを作成する
- Amazon VPC Transit Gateway を使用して Connect アタッチメントと Connect ピアを表示する
- Amazon VPC Transit Gateway を使用して Connect アタッチメントと Connect ピアタグを変更する
- Amazon VPC Transit Gateway を使用して Connect ピアを削除する
- Amazon VPC Transit Gateway を使用して Connect アタッチメントを削除する

Amazon VPC Transit Gateway を使用して Connect アタッチメントを作成する

Connect アタッチメントを作成するには、トランスポートアタッチメントとして既存のアタッチメントを指定する必要があります。VPC アタッチメントまたは Direct Connect アタッチメントをトランスポートアタッチメントとして指定できます。

コンソールを使用して Connect アタッチメントを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. [Transit Gateway アタッチメントの作成] を選択します。
4. (オプション) [名前タグ] でアタッチメントの名前タグを指定します。
5. [Transit Gateway ID] で、アタッチメントのトランジットゲートウェイを選択します。
6. [アタッチメントタイプ] で、[接続] を選択します。
7. [トランスポートアタッチメント ID] で、既存のアタッチメント の ID を選択します。
8. [Transit Gateway アタッチメントの作成] を選択します。

を使用して Connect アタッチメントを作成するには AWS CLI

create-transit-gateway-connect コマンドを使用します。

Amazon VPC Transit Gateway を使用して Connect ピアを作成する

既存の Connect アタッチメントの Connect ピア (GRE トンネル) を作成できます。開始する前に、トランジットゲートウェイCIDRブロックが設定されていることを確認してください。トランジットゲートウェイCIDRブロックは、トランジットゲートウェイを作成または変更するときに設定できます。

Connect ピアを作成するときは、Connect ピアのアプライアンス側でGRE外部 IP アドレスを指定する必要があります。

コンソールを使用して Connect ピアを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。

3. Connect アタッチメントを選択し、[アクション] 、[Connect ピアを作成] の順に選択します。
4. (オプション) [名前タグ] に、Connect ピアの名前タグを指定します。
5. （ オプション) トランジットゲートウェイGREアドレス で、トランジットゲートウェイのGRE外部 IP アドレスを指定します。デフォルトでは、トランジットゲートウェイCIDRブロックから最初に使用可能なアドレスが使用されます。
6. ピアGREアドレス には、Connect ピアのアプライアンス側のGRE外部 IP アドレスを指定します。
7. BGP 内部CIDRブロック IPv4には、BGPピアリングに使用される内部IPv4アドレスの範囲を指定します。`169.254.0.0/16` 範囲から /29 CIDRブロックを指定します。
8. （ オプション) BGP内部CIDRブロック IPv6で、BGPピアリングに使用される内部IPv6アドレスの範囲を指定します。`fd00::/8` 範囲から /125 CIDRブロックを指定します。
9. （ オプション) ピア でASN、アプライアンスのボーダーゲートウェイプロトコル (BGP) 自律システム番号 (ASN) を指定します。ネットワークASNに割り当てられた既存の を使用できます。プライベート がない場合は、64512 ~ 65534 (16 ビットASN) または 4200000000 ~ 4294967294 (32 ビットASN) の範囲ASNのプライベート を使用できます。

   デフォルトはトランジットゲートウェイASNと同じです。ピアASNをトランジットゲートウェイ ASN (e BGP) とは異なるように設定する場合は、 time-to-live （ TTL) 値を 2 に設定する必要があります。
10. 選択接続ピアの作成を選択します。

を使用して Connect ピアを作成するには AWS CLI

create-transit-gateway-connect-peer コマンドを使用します。

Amazon VPC Transit Gateway を使用して Connect アタッチメントと Connect ピアを表示する

Connect アタッチメントと Connect ピアを表示します。

コンソールを使用して Connect アタッチメントと Connect ピアを表示するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. Connect アタッチメントを選択します。
4. アタッチメントの Connect ピアを表示するには、[Connect ピア] タブを選択します。

を使用して Connect アタッチメントと Connect ピアを表示するには AWS CLI

describe-transit-gateway-connects および describe-transit-gateway-connectピアコマンドを使用します。

Amazon VPC Transit Gateway を使用して Connect アタッチメントと Connect ピアタグを変更する

Connect アタッチメントのタグを変更できます。

コンソールを使用して Connect アタッチメントタグを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. 接続 アタッチメントを選択後、[アクション]、[タグの管理] の順に選択します。
4. タグを追加するには、新しいタグを追加を選択し、キー名とキーバリューを指定します。
5. タグを削除するには、[削除] を選択します。
6. [保存] を選択します。

Connect ピアのタグは変更できます。

コンソールを使用して Connect ピアのタグを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. 接続 アタッチメントを選択し、[接続 ピア] を選択します。
4. Connect ピアを選択後、[アクション]、[タグの管理] の順に選択します。
5. タグを追加するには、新しいタグを追加を選択し、キー名とキーバリューを指定します。
6. タグを削除するには、[削除] を選択します。
7. [Save] を選択します。

AWS CLIを使用して Connect アタッチメントおよび Connect ピアのタグを変更するには

create-tags および delete-tags コマンドを使用します。

Amazon VPC Transit Gateway を使用して Connect ピアを削除する

Connect ピアが不要になった場合には、それを削除することができます。

コンソールを使用して Connect ピアを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. Connect アタッチメントを選択します。
4. [Connect ピア] タブで、Connect ピアを選択し、[アクション]、[Connect ピアを削除] の順に選択します。

を使用して Connect ピアを削除するには AWS CLI

delete-transit-gateway-connect-peer コマンドを使用します。

Amazon VPC Transit Gateway を使用して Connect アタッチメントを削除する

Connect アタッチメントが不要になった場合は、削除できます。まず、アタッチメントの Connect ピアをすべて削除する必要があります。

コンソールを使用して Connect アタッチメントを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. Connect アタッチメントを選択後、[アクション]、[Transit Gateway アタッチメントの削除]を選択します。
4. 「**`delete`**」と入力し、[削除] を選択します。

を使用して Connect アタッチメントを削除するには AWS CLI

delete-transit-gateway-connect コマンドを使用します。

Amazon Transit Gateway のVPCトランジットゲートウェイルートテーブル

Transit Gateway ルートテーブルを使用して、Transit Gateway アタッチメントのルーティングを設定します。

プレフィックスリスト参照

トランジットゲートウェイルートテーブルでプレフィックスリストを参照できます。プレフィックスリストは、ユーザーが定義して管理する 1 つ以上のCIDRブロックエントリのセットです。プレフィックスリストを使用すると、ネットワークトラフィックをルーティングするためにリソースで参照する IP アドレスの管理を簡素化できます。例えば、複数の Transit Gateway ルートテーブル CIDRsで同じ送信先を頻繁に指定する場合、各ルートテーブルCIDRsで同じ を繰り返し参照するのではなく、1 つのプレフィックスリストCIDRsでそれらの送信先を管理できます。送信先CIDRブロックを削除する必要がある場合は、影響を受けるすべてのルートテーブルからルートを削除する代わりに、プレフィックスリストからそのエントリを削除できます。

Transit Gateway ルートテーブルにプレフィックスリストリファレンスを作成すると、プレフィックスリストの各エントリは、Transit Gateway ルートテーブルにルートとして表示されます。

プレフィックスリストの詳細については、「Amazon VPC ユーザーガイド」の「プレフィックスリスト」を参照してください。

タスク

- Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルを作成する
- Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルを表示する
- Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルを関連付ける
- Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルの関連付けを削除する
- Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルへのルート伝達を有効にする
- Amazon VPC Transit Gateway を使用したルート伝達の無効化
- Amazon VPC Transit Gateway を使用して静的ルートを作成する
- Amazon VPC Transit Gateway を使用して静的ルートを削除する
- Amazon VPC Transit Gateway を使用して静的ルートを置き換える

- Amazon VPC Transit Gateway を使用してルートテーブルを Amazon S3 にエクスポートする
- Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルを削除する
- Amazon VPC Transit Gateway を使用してルートテーブルプレフィックスリストリファレンスを作成する
- Amazon VPC Transit Gateway を使用してプレフィックスリスト参照を表示する
- Amazon VPC Transit Gateway を使用してプレフィックスリストリファレンスを変更する
- Amazon VPC Transit Gateway を使用してプレフィックスリストリファレンスを削除する

Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルを作成する

コンソールを使用して Transit Gateway ルートテーブルを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. [Transit Gateway ルートテーブルの作成] を選択します。
4. (オプション) [名前タグ] に、トランジットゲートウェイルートテーブルの名前を入力します。これにより、タグキー「名前」を持つタグが作成されます。タグ値は指定した名前です。
5. [Transit Gateway ID] で、ルートテーブルの Transit Gateway を選択します。
6. [Transit Gateway ルートテーブルの作成] を選択します。

を使用してトランジットゲートウェイルートテーブルを作成するには AWS CLI

create-transit-gateway-route-table コマンドを使用します。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルを表示する

コンソールを使用して Transit Gateway ルートテーブルを表示するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. (オプション) 特定のルートテーブルまたはテーブルのセットを検索するには、フィルターフィールドに名前、キーワード、または属性の全部または一部を入力します。

4. ルートテーブルのチェックボックスをオンにするか、ID を選択して、関連付け、伝達、ルート、タグに関する情報を表示します。

を使用してトランジットゲートウェイルートテーブルを表示するには AWS CLI

describe-transit-gateway-route-tables コマンドを使用します。

を使用してトランジットゲートウェイルートテーブルのルートを表示するには AWS CLI

search-transit-gateway-routes コマンドを使用します。

を使用してトランジットゲートウェイルートテーブルのルート伝達を表示するには AWS CLI

get-transit-gateway-route-table-propagations コマンドを使用します。

を使用してトランジットゲートウェイルートテーブルの関連付けを表示するには AWS CLI

get-transit-gateway-route-table-associations コマンドを使用します。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルを関連付ける

Transit Gateway ルートテーブルを、Transit Gateway アタッチメントに関連付けることができます。

コンソールを使用して Transit Gateway ルートテーブルを関連付けるには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートテーブルを選択します。
4. ページ下部で、[Associations (関連付け)] タブを選択します。
5. [関連付けの作成] を選択します。
6. 関連付けるアタッチメントを選択してから、[Create association (関連付けの作成)] を選択します。

を使用してトランジットゲートウェイルートテーブルを関連付けるには AWS CLI

associate-transit-gateway-route-table コマンドを使用します。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルの関連付けを削除する

Transit Gateway アタッチメントから Transit Gateway ルートテーブルの関連付けを解除できます。

コンソールを使用して Transit Gateway ルートテーブルの関連付けを解除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートテーブルを選択します。
4. ページ下部で、[Associations (関連付け)] タブを選択します。
5. 関連付けを解除するアタッチメントを選択してから、[Delete association (関連付けの解除)] 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、[Delete association (関連付けの解除)] を選択します。

を使用してトランジットゲートウェイルートテーブルの関連付けを解除するには AWS CLI

disassociate-transit-gateway-route-table コマンドを使用します。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルへのルート伝達を有効にする

ルート伝達を使用して、アタッチメントからルートテーブルへのルートを追加します。

Transit Gateway アタッチメントルートテーブルにルートを伝達するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. 伝播を作成するルートテーブルを選択します。
4. [Actions (アクション)]、[Create propagation (伝播の作成)] の順に選択します。
5. [Create propagation (伝播の作成)]ページで、アタッチメントを選択します。
6. 伝播の作成] を選択します。

を使用してルート伝達を有効にするには AWS CLI

enable-transit-gateway-route-table-propagation コマンドを使用します。

Amazon VPC Transit Gateway を使用したルート伝達の無効化

ルートテーブルアタッチメントからルート伝達を削除します。

コンソールを使用してルート伝達を無効にするには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. 伝播を削除するルートテーブルを選択します。
4. ページ下部で、[Propagations (伝播)] タブを選択します。
5. アタッチメントを選択し、次に[Delete propagation (伝播の削除)] 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、[Delete propagation (伝播の削除)] を選択します。

を使用してルート伝達を無効にするには AWS CLI

disable-transit-gateway-route-table-propagation コマンドを使用します。

Amazon VPC Transit Gateway を使用して静的ルートを作成する

VPC、VPN、または Transit Gateway ピアリングアタッチメントの静的ルートを作成するか、ルートに一致するトラフィックを削除するブラックホールルートを作成できます。

VPN アタッチメントをターゲットとするトランジットゲートウェイルートテーブルの静的ルートは、Site-to-Site によってフィルタリングされませんVPN。これにより、 BGPベースの を使用するときに、意図しないアウトバウンドトラフィックフローが発生する可能性がありますVPN。

コンソールを使用して静的ルートを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートを作成するルートテーブルを選択します。
4. [アクション]、[静的ルートの作成] の順に選択します。
5. 静的ルートの作成ページで、ルートを作成するCIDRブロックを入力し、アクティブ を選択します。
6. ルートのアタッチメントを選択します。
7. [静的ルートの作成] を選択します。

コンソールを使用してブラックホールルートを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートを作成するルートテーブルを選択します。
4. [アクション]、[静的ルートの作成] の順に選択します。
5. 「静的ルートの作成」ページで、ルートを作成するCIDRブロックを入力し、「ブラックホール」を選択します。
6. [静的ルートの作成] を選択します。

を使用して静的ルートまたはブラックホールルートを作成するには AWS CLI

create-transit-gateway-route コマンドを使用します。

Amazon VPC Transit Gateway を使用して静的ルートを削除する

トランジットゲートウェイルートテーブルから静的ルートを削除します。

コンソールを使用して静的ルートを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートを削除するルートテーブルを選択し、[ルート] を選択します。
4. 削除するルートを選択します。
5. 選択静的ルートを削除する。
6. 確認ボックスで [静的ルートの削除] を選択します。

を使用して静的ルートを削除するには AWS CLI

delete-transit-gateway-route コマンドを使用します。

Amazon VPC Transit Gateway を使用して静的ルートを置き換える

トランジットゲートウェイルートテーブルの静的ルートを別の静的ルートに置き換えます。

コンソールを使用してスタティックルートを置き換えるには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。

2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートテーブルで置換するルートを選択します。
4. 詳細セクションで、[ルート] タブを選択します。
5. [アクション]、[スタティックルートの置換] を選択します。
6. [タイプ] では、[アクティブ] または [ブラックホール] を選択します。
7. [アタッチメントの選択] ドロップダウンから、ルートテーブル内の現在のゲートウェイを置き換えるトランジットゲートウェイを選択します。
8. [スタティックルートの置換] を選択します。

を使用して静的ルートを置き換えるには AWS CLI

replace-transit-gateway-route コマンドを使用します。

Amazon VPC Transit Gateway を使用してルートテーブルを Amazon S3 にエクスポートする

Transit Gateway のルートテーブルのルートを Amazon S3 バケットにエクスポートできます。ルートは、JSONファイル内の指定された Amazon S3 バケットに保存されます。

コンソールを使用して Transit Gateway ルートテーブルをエクスポートするには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. エクスポートするルートを含むルートテーブルを選択します。
4. [Actions (アクション)]、[Export routes (ルートのエクスポート)] を選択します。
5. [Export routes (ルートのエクスポート)] ページの [S3 bucket name (S3バケット名)]に、S3 バケットの名前を入力します。
6. エクスポートされたルートをフィルタリングするには、ページの [フィルター] セクションでフィルターパラメータを指定します。
7. [Export routes (ルートのエクスポート)] を選択します。

エクスポートされたルートにアクセスするには、 で Amazon S3 コンソールを開きhttps://console.aws.amazon.com/s3/、指定したバケットに移動します。ファイル名には、 AWS アカウント AWS ID、リージョン、ルートテーブル ID、タイムスタンプが含まれます。ファイルを選択し、[ダ

ウンロード] を選択します。以下は、VPC添付ファイルの 2 つの伝播されたルートに関する情報を含むJSONファイルの例です。

```
{
  "filter": [
    {
      "name": "route-search.subnet-of-match",
      "values": [
        "0.0.0.0/0",
        "::/0"
      ]
    }
  ],
  "routes": [
    {
      "destinationCidrBlock": "10.0.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-0123456abcd123456",
          "transitGatewayAttachmentId": "tgw-attach-1122334455aabbcc1",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    },
    {
      "destinationCidrBlock": "10.2.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-abcabc123123abca",
          "transitGatewayAttachmentId": "tgw-attach-6677889900aabbcc7",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    }
  ]
}
```

Amazon VPC Transit Gateway を使用してトランジットゲートウェイルートテーブルを削除する

コンソールを使用して Transit Gateway ルートテーブルを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. 削除するルートテーブルを選択します。
4. アクション、Transit Gateway ルートテーブルの削除を選択します。
5. **`delete`** と入力して、[Delete (削除)] を選択して削除を確認します。

を使用してトランジットゲートウェイルートテーブルを削除するには AWS CLI

delete-transit-gateway-route-table コマンドを使用します。

Amazon VPC Transit Gateway を使用してルートテーブルプレフィックスリストリファレンスを作成する

Transit Gateway ルートテーブルにプレフィックスリストへの参照を作成できます。

コンソールを使用してプレフィックスリストリファレンスを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル}] をクリックします。
3. Transit Gateway ルートテーブルを選択します。
4. [アクション]、[プレフィックスリスト参照を作成] の順にクリックします。
5. [プレフィックスリスト ID] で、プレフィックスリストの ID を選択します。
6. を使用する場合タイプで、このプレフィクスリストへのトラフィックを許可するかどうかを選択します (アクティブ) またはドロップ (ブラックホール)。
7. [Transit Gateway アタッチメント ID] で、トラフィックをルーティングする先のアタッチメントの ID を選択します。
8. [プレフィックスリスト参照を作成] をクリックします。

を使用してプレフィックスリストリファレンスを作成するには AWS CLI

create-transit-gateway-prefix-list-reference コマンドを使用します。

Amazon VPC Transit Gateway を使用してプレフィックスリスト参照を表示する

トランジットゲートウェイルートテーブルのプレフィックスリスト参照を表示します。プレフィックスリストの各エントリを、Transit Gateway ルートテーブルに個別のルートとして表示することもできます。プレフィックスリストルートのルートタイプは `propagated` です。

コンソールを使用してプレフィックスリストリファレンスを表示するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル}] をクリックします。
3. Transit Gateway ルートテーブルを選択します。
4. 下部のペインで、[プレフィックスリストリファレンス] をクリックします。プレフィックスリストリファレンスが一覧表示されます。
5. [ルート] をクリックします。プレフィックスリストの各エントリが、ルートテーブルにルートとして表示されます。

を使用してプレフィックスリストリファレンスを表示するには AWS CLI

get-transit-gateway-prefix-list-references コマンドを使用します。

Amazon VPC Transit Gateway を使用してプレフィックスリストリファレンスを変更する

プレフィックスリストリファレンスを変更するには、トラフィックのルーティング先のアタッチメントを変更します。または、ルートに一致するトラフィックを削除するかどうかを指定します。

プレフィックスリストの各ルートを [ルート] タブで変更することはできません。プレフィックスリストのエントリを変更するには、[マネージドプレフィックスリスト] 画面を使用します。詳細については、「Amazon VPC ユーザーガイド」の「プレフィックスリストの変更」を参照してください。

コンソールを使用してプレフィックスリストリファレンスを変更するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル}] をクリックします。
3. Transit Gateway ルートテーブルを選択します。

4. 下部のペインで、[プレフィックスリストリファレンス] をクリックします。
5. プレフィックスリストリファレンスを選択し、[リファレンスの変更] をクリックします。
6. を使用する場合タイプで、このプレフィクスリストへのトラフィックを許可するかどうかを選択します (アクティブ) またはドロップ (ブラックホール)。
7. [Transit Gateway アタッチメント ID] で、トラフィックをルーティングする先のアタッチメントの ID を選択します。
8. [プレフィックスリスト参照の変更] をクリックします。

を使用してプレフィックスリストリファレンスを変更するには AWS CLI

modify-transit-gateway-prefix-list-reference コマンドを使用します。

Amazon VPC Transit Gateway を使用してプレフィックスリストリファレンスを削除する

プレフィックスリストリファレンスが不要になった場合は、Transit Gateway ルートテーブルから削除できます。参照を削除しても、プレフィックスリストは削除されません。

コンソールを使用してプレフィックスリストリファレンスを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway ルートテーブル}] をクリックします。
3. Transit Gateway ルートテーブルを選択します。
4. プレフィックスリストリファレンスを選択し、[リファレンスの削除] をクリックします。
5. [リファレンスの削除] を選択します。

を使用してプレフィックスリストリファレンスを変更するには AWS CLI

delete-transit-gateway-prefix-list-reference コマンドを使用します。

Amazon Transit Gateway のVPCトランジットゲートウェイポリシーテーブル

トランジットゲートウェイの動的ルーティングは、ポリシーテーブルを使用して AWS 、 クラウド のネットワークトラフィックをルーティングしますWAN。このテーブルには、ポリシー属性に

よってネットワークトラフィックを照合するためのポリシールールが含まれ、ルールに一致するトラフィックがターゲットルートテーブルにマッピングされます。

Transit Gateway に動的ルーティングを使用して、ルーティングおよび到達可能性の情報をピアリングされた Transit Gateway と自動的に情報交換できます。静的ルートとは異なり、パスの障害や輻輳などのネットワーク状態に基づいて、別のパスを経由してトラフィックをルーティングできます。また、動的ルーティングは、ネットワークの侵害や侵入が発生した場合にトラフィックを簡単に再ルーティングできるという点で、セキュリティの強化につながります。

> **Note**
>
> 現在、トランジットゲートウェイポリシーテーブルは、トランジットゲートウェイピアリング接続を作成するWANときに クラウドでのみサポートされています。ピアリング接続を作成するときに、そのテーブルを接続に関連付けることができます。その後、アソシエーションはポリシールールを自動的にテーブルに入力します。
> クラウドでのピアリング接続の詳細についてはWAN、 クラウドAWS WANユーザーガイドの「ピアリング」を参照してください。

タスク

- Amazon VPC Transit Gateway を使用してトランジットゲートウェイポリシーテーブルを作成する
- Amazon VPC Transit Gateway を使用してトランジットゲートウェイポリシーテーブルを削除する

Amazon VPC Transit Gateway を使用してトランジットゲートウェイポリシーテーブルを作成する

コンソールを使用して Transit Gateway ポリシーテーブルを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit gateway policy table] (Transit Gateway ポリシーテーブル) を選択します。
3. [Create transit gateway policy table] (Transit Gateway ポリシーテーブルの作成) を選択します。
4. (オプション) [Name tag] (名前タグ) に、Transit Gateway ポリシーテーブルの名前を入力します。これによりタグが作成され、タグの値は指定した名前になります。
5. [Transit gateway ID] (Transit Gateway の ID) で、ポリシーテーブルの Transit Gateway を選択します。

6. [Create transit gateway policy table] (Transit Gateway ポリシーテーブルの作成) を選択します。

を使用してトランジットゲートウェイポリシーテーブルを作成するには AWS CLI

create-transit-gateway-policy-table コマンドを使用します。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイポリシーテーブルを削除する

Transit Gateway ポリシーテーブルを削除します。テーブルが削除されると、そのテーブル内のすべてのポリシールールが削除されます。

コンソールを使用して Transit Gateway ポリシーテーブルを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit gateway policy tables] (Transit Gateway ポリシーテーブル) を選択します。
3. 削除する Transit Gateway ポリシーテーブルを選択します。
4. [Actions] (アクション) を選択してから、[Delete policy table] (ポリシーテーブルの削除) を選択します。
5. テーブルを削除することを確認します。

を使用してトランジットゲートウェイポリシーテーブルを削除するには AWS CLI

delete-transit-gateway-policy-table コマンドを使用します。

Amazon VPC Transit Gateway のマルチキャスト

マルチキャストは、単一のデータストリームを複数の受信コンピュータに同時に配信するために使用される通信プロトコルです。Transit Gateway は、アタッチされた のサブネット間のマルチキャストトラフィックのルーティングをサポートしVPCs、複数の受信インスタンス宛てのトラフィックを送信するインスタンスのマルチキャストルーターとして機能します。

トピック

- マルチキャストの概念
- 考慮事項

- マルチキャストのルーティング
- Amazon VPC Transit Gateway のマルチキャストドメイン
- Amazon VPC Transit Gateway の共有マルチキャストドメイン
- Amazon VPC Transit Gateway を使用してマルチキャストグループにソースを登録する
- Amazon VPC Transit Gateway を使用してマルチキャストグループにメンバーを登録する
- Amazon VPC Transit Gateway を使用してマルチキャストグループからソースを登録解除する
- Amazon VPC Transit Gateway を使用してマルチキャストグループからメンバーを登録解除する
- Amazon VPC Transit Gateway を使用してマルチキャストグループを表示する
- Amazon VPC Transit Gateway で Windows Server のマルチキャストを設定する
- 例: Amazon VPC Transit Gateway を使用してIGMP設定を管理する
- 例: Amazon VPC Transit Gateway を使用した静的ソース設定の管理
- 例: Amazon VPC Transit Gateway での静的グループメンバー設定の管理

マルチキャストの概念

マルチキャストの主な概念は次のとおりです。

- マルチキャストドメイン — 異なるドメインへのマルチキャストネットワークのセグメント化が可能になり、Transit Gateway が複数のマルチキャストルーターとして機能するようになります。サブネットレベルでマルチキャストドメインのメンバーシップを定義します。
- マルチキャストグループ — 同じマルチキャストトラフィックを送受信するホストセットを識別します。マルチキャストグループは、グループ IP アドレスによって識別されます。マルチキャストグループのメンバーシップは、EC2インスタンスにアタッチされた個々の Elastic Network Interface によって定義されます。
- インターネットグループ管理プロトコル (IGMP) — ホストとルーターがマルチキャストグループメンバーシップを動的に管理できるようにするインターネットプロトコル。IGMP マルチキャストドメインには、IGMPプロトコルを使用してメッセージを結合、終了、送信するホストが含まれています。 は、IGMPv2プロトコルと、 IGMP および静的 (APIベース) グループメンバーシップマルチキャストドメインの両方 AWS をサポートします。

- マルチキャストソース — マルチキャストトラフィックを送信するように静的に設定された、サポートされているEC2インスタンスに関連付けられた Elastic Network Interface。マルチキャスト送信元は、静的な送信元の設定のみに適用されます。

静的ソースマルチキャストドメインには、メッセージを結合、終了、送信するためにIGMPプロトコルを使用しないホストが含まれています。を使用して AWS CLI 、ソースメンバーとグループメンバーを追加します。静的に追加された送信元は、マルチキャストトラフィックを送信し、メンバーはマルチキャストトラフィックを受信します。

- マルチキャストグループメンバー — マルチキャストトラフィックを受信するサポートされているEC2インスタンスに関連付けられた Elastic Network Interface。マルチキャストグループには複数のグループメンバーがあります。静的な送信元のグループメンバーシップの設定では、マルチキャストグループメンバーはトラフィックだけを受信できます。IGMP グループ設定では、メンバーはトラフィックを送受信できます。

考慮事項

- サポートされているリージョンの詳細については、AWS 「トランジットゲートウェイFAQs」を参照してください。
- マルチキャストをサポートするには、新しいTransit Gateway を作成する必要があります。
- マルチキャストグループのメンバーシップは、、 AWS CLI、 Amazon Virtual Private Cloud Console または を使用して管理されますIGMP。
- マルチキャストドメインに存在するサブネットは 1 つだけです。
- Nitro 以外のインスタンスを使用する場合は、送信元/送信先チェックボックスを無効にする必要があります。チェックを無効にする方法については、「Amazon ユーザーガイド」の「送信元または送信先のチェックの変更」を参照してください。 EC2
- ニトロ以外のインスタンスをマルチキャスト送信元にすることはできません。
- マルチキャストルーティングは AWS Direct Connect、、Site-to-SiteVPN、ピアリングアタッチメント、または Transit Gateway Connect アタッチメントではサポートされていません。
- Transit Gateway は、マルチキャストパケットのフラグメント化をサポートしていません。フラグメント化されたマルチキャストパケットはドロップされます。詳細については、「最大送信単位 (MTU) 」を参照してください。
- 起動時に、IGMPホストはマルチキャストグループに参加するために複数のIGMPJOINメッセージを送信します (通常は 2～3 回の再試行) 。万一、すべてのIGMPJOINメッセージが紛失した場合、ホストは Transit Gateway マルチキャストグループの一部にはなりません。このようなシナリオでは、アプリケーション固有の方法を使用してホストからIGMPJOINメッセージを再トリガーする必要があります。

- グループメンバーシップは、トランジットゲートウェイによるIGMPv2JOINメッセージの受信で始まり、IGMPv2LEAVEメッセージの受信で終わります。Transit Gateway は、グループに正常に参加したホストを追跡します。クラウドマルチキャストルーターとして、トランジットゲートウェイは 2 分ごとにすべてのメンバーにIGMPv2QUERYメッセージを発行します。各メンバーは応答としてIGMPv2JOINメッセージを送信します。これは、メンバーがメンバーシップを更新する方法です。メンバーが 3 つの連続するクエリに応答できない場合、Transit Gateway は、参加したすべてのグループからこのメンバーシップを削除します。ただし、メンバーを to-be-queried リストから完全に削除するまで、このメンバーにクエリを送信し続けます。明示的なIGMPv2LEAVEメッセージは、ホストを他のマルチキャスト処理から即時かつ完全に削除します。
- Transit Gateway は、グループに正常に参加したホストを追跡します。トランジットゲートウェイが停止した場合、トランジットゲートウェイは最後に成功したIGMPJOINメッセージから 7 分 (420 秒) の間、ホストにマルチキャストデータを送信し続けます。Transit Gateway は、最大 12 時間、またはホストからIGMPLEAVEメッセージを受信するまで、メンバーシップクエリをホストに送信し続けます。
- トランジットゲートウェイは、マルチキャストグループのメンバーシップを追跡IGMPできるように、メンバーシップクエリパケットをすべてのメンバーに送信します。これらのIGMPクエリパケットの送信元 IP は 0.0.0.0/32 で、送信先 IP は 224.0.0.1/32 で、プロトコルは 2 です。IGMP ホスト (インスタンス) のセキュリティグループ設定と、ホストサブネット上のすべてのACLs設定で、これらのIGMPプロトコルメッセージを許可する必要があります。
- マルチキャストの送信元と送信先が同じ にある場合VPC、セキュリティグループ参照を使用して、送信元のセキュリティグループからのトラフィックを受け入れるように送信先セキュリティグループを設定することはできません。
- 静的マルチキャストグループとソースの場合、Amazon VPC Transit Gateway は、存在しない の静的グループとソースを自動的に削除ENIsします。これは、アカウントENIsで記述する Transit Gateway サービスにリンクされたロールを定期的に引き受けることによって実行されます。
- 静的マルチキャストのみが をサポートしますIPv6。動的マルチキャストはそうではありません。

マルチキャストのルーティング

トランジットゲートウェイは、マルチキャストを有効にすると、マルチキャストルーターとして動作します。サブネットをマルチキャストドメインに追加すると、そのマルチキャストドメインに関連付けられたトランジットゲートウェイにすべてのマルチキャストトラフィックが送信されます。

ネットワーク ACLs

ネットワークACLルールはサブネットレベルで動作します。トランジットゲートウェイはサブネットの外部に存在するため、マルチキャストトラフィックに適用されます。詳細については、「Amazon ユーザーガイド」の「ネットワークACLs」を参照してください。 VPC

インターネットグループ管理プロトコル (IGMP) マルチキャストトラフィックの場合、最小インバウンドルールは次のとおりです。リモートホストは、マルチキャストトラフィックを送信するホストです。

タイプ	プロトコル	送信元	説明
カスタムプロトコル	IGMP(2)	0.0.0.0/32	IGMP クエリ
カスタムUDPプロトコル	UDP	リモートホストの IP アドレス	着信マルチキャストトラフィック

の最小アウトバウンドルールは次のとおりですIGMP。

タイプ	プロトコル	送信先	説明
カスタムプロトコル	IGMP(2)	224.0.0.2/32	IGMP 退出
カスタムプロトコル	IGMP(2)	マルチキャストグループの IP アドレス	IGMP 参加
カスタムUDPプロトコル	UDP	マルチキャストグループの IP アドレス	アウトバウンドマルチキャストトラフィック

セキュリティグループ

セキュリティグループルールは、インスタンスレベルで動作します。これらのトラフィックは、インバウンドマルチキャストトラフィックとアウトバウンドマルチキャストトラフィックの両方に適用できます。動作は、ユニキャストトラフィックと同じです。すべてのグループメンバーインスタンスで、グループソースからのインバウンドトラフィックを許可する必要があります。詳細については、「Amazon ユーザーガイド」の「セキュリティグループ」を参照してください。 VPC

IGMP マルチキャストトラフィックの場合、少なくとも次のインバウンドルールが必要です。リモートホストは、マルチキャストトラフィックを送信するホストです。UDP インバウンドルールのソースとしてセキュリティグループを指定することはできません。

タイプ	プロトコル	送信元	説明
カスタムプロトコル	2	0.0.0.0/32	IGMP クエリ
カスタムUDPプロトコル	UDP	リモートホストの IP アドレス	着信マルチキャストトラフィック

IGMP マルチキャストトラフィックの場合、少なくとも次のアウトバウンドルールが必要です。

タイプ	プロトコル	送信先	説明
カスタムプロトコル	2	224.0.0.2/32	IGMP 退出
カスタムプロトコル	2	マルチキャストグループの IP アドレス	IGMP 参加
カスタムUDPプロトコル	UDP	マルチキャストグループの IP アドレス	アウトバウンドマルチキャストトラフィック

Amazon VPC Transit Gateway のマルチキャストドメイン

マルチキャストドメインを使用すると、マルチキャストネットワークを異なるドメインにセグメント化できます。トランジットゲートウェイでマルチキャストの使用を開始するには、マルチキャストドメインを作成し、サブネットをドメインに関連付けます。

マルチキャストドメイン属性

次の表は、マルチキャストドメイン属性の詳細を示しています。両方の属性を同時に有効にすることはできません。

属性	説明
`Igmpv2Support` (AWS CLI) IGMPv2 サポート (コンソール)	この属性は、グループメンバーがマルチキャストグループの参加または脱退を行う方法を決定します。 この属性が無効の場合は、ドメインにグループメンバーを手動で追加する必要があります。 少なくとも 1 人のメンバーがIGMPプロトコルを使用している場合は、この属性を有効にします。メンバーは、次のいずれかの方法でマルチキャストグループに参加します。 • をサポートするメンバーは、 `JOIN`および `LEAVE` メッセージIGMPを使用します。 • サポートされていないメンバーは、Amazon VPCコンソールまたは を使用してグループに追加または削除IGMPする必要があります AWS CLI。 マルチキャストグループメンバーを登録する場合は、登録を解除する必要があります。トランジットゲートウェイは、手動で追加されたグループメンバーによって送信されたIGMPLEAVEメッセージを無視します。
`StaticSourcesSupport` (AWS CLI) 静的ソースサポート(コンソール)	この属性は、グループに静的なマルチキャスト送信元があるかどうかを決定します。 この属性が有効になっている場合は、register-transit-gateway-multicast-group-sources を使用してマルチキャストドメインのソースを追加する必要があります。マルチキャストトラフィックを送信できるのは、マルチキャスト送信元のみです。 この属性を無効にした場合、指定されたマルチキャスト送信元はありません。マルチキャストドメインに関連付けられたサブネットにあるインスタンスはすべて、マルチキャストトラフィックを送信でき、グループメンバーはマルチキャストトラフィックを受信します。

Amazon VPC Transit Gateway を使用してIGMPマルチキャストドメインを作成する

まだ確認していない場合は、使用可能なマルチキャストドメイン属性を確認します。詳細については、「the section called “マルチキャストドメイン”」を参照してください。

コンソールを使用してIGMPマルチキャストドメインを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. [Transit Gateway マルチキャストドメインの作成] をクリックします。
4. [名前タグ] に、ドメインの名前を入力します。
5. [トランジットゲートウェイ ID] で、マルチキャストトラフィックを処理するトランジットゲートウェイを選択します。
6. IGMPv2 をサポートするには、チェックボックスをオンにします。
7. 静的ソースが をサポートしている場合は、チェックボックスをオフにします。
8. このマルチキャストドメインについてクロスアカウントサブネットの関連付けを自動的に受け入れるには、[Auto accept shared associations] (共有されている関連付けを自動的に受け入れる) を選択します。
9. [Transit Gateway マルチキャストドメインの作成] をクリックします。

を使用してIGMPマルチキャストドメインを作成するには AWS CLI

create-transit-gateway-multicast-domain コマンドを使用します。

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=disable,Igmpv2Support=enable
```

Amazon VPC Transit Gateway を使用して静的ソースマルチキャストドメインを作成する

まだ確認していない場合は、使用可能なマルチキャストドメイン属性を確認します。詳細については、「the section called “マルチキャストドメイン”」を参照してください。

コンソールを使用して静的なマルチキャストドメインを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。

2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. [Transit Gateway マルチキャストドメインの作成] をクリックします。
4. [Name tag] (名前タグ) に、ドメインを識別する名前を入力します。
5. [トランジットゲートウェイ ID] で、マルチキャストトラフィックを処理するトランジットゲートウェイを選択します。
6. IGMPv2 をサポートするには、チェックボックスをオフにします。
7. 静的ソースが をサポートしている場合は、チェックボックスをオンにします。
8. このマルチキャストドメインについてクロスアカウントサブネットの関連付けを自動的に受け入れるには、[Auto accept shared associations] (共有されている関連付けを自動的に受け入れる) を選択します。
9. [Transit Gateway マルチキャストドメインの作成] をクリックします。

を使用して静的マルチキャストドメインを作成するには AWS CLI

create-transit-gateway-multicast-domain コマンドを使用します。

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=enable,Igmpv2Support=disable
```

Amazon VPC Transit Gateway を使用してVPCアタッチメントとサブネットをマルチキャストドメインに関連付ける

VPC アタッチメントをマルチキャストドメインに関連付けるには、次の手順に従います。関連付けを作成するときに、マルチキャストドメインに含めるサブネットを選択できます。

開始する前に、トランジットゲートウェイにVPCアタッチメントを作成する必要があります。詳細については、「Amazon VPC Transit Gateway の Amazon VPCアタッチメント」を参照してください。

コンソールを使用してVPCアタッチメントをマルチキャストドメインに関連付けるには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択し、[Actions] (アクション)、[Create association] (関連付けの作成) の順に選択します。
4. 関連付ける添付ファイルを選択で、トランジットゲートウェイアタッチメントを選択します。

5. [Choose subnets to associate] (関連付けるサブネットを選択する) で、マルチキャストドメインに含めるサブネットを選択します。
6. [関連付けの作成] を選択します。

を使用してVPCアタッチメントをマルチキャストドメインに関連付けるには AWS CLI

associate-transit-gateway-multicast-domain コマンドを使用します。

Amazon VPC Transit Gateway を使用してマルチキャストドメインからサブネットの関連付けを解除する

サブネットとマルチキャストドメインの関連付けを解除するには、次の手順を実行します。

コンソールを使用して、サブネットの関連付けを解除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [Associations (関連付け)] タブを選択します。
5. サブネットに続いて、アクション、関連付けを削除の順に選択します。

を使用してサブネットの関連付けを解除するには AWS CLI

disassociate-transit-gateway-multicast-domain コマンドを使用します。

Amazon VPC Transit Gateway を使用してマルチキャストドメインの関連付けを表示する

マルチキャストドメインを表示して、それらが使用可能であり、適切なサブネットとアタッチメントが含まれていることを確認します。

コンソールを使用してマルチキャストドメインを表示するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [Associations (関連付け)] タブを選択します。

を使用してマルチキャストドメインを表示するには AWS CLI

describe-transit-gateway-multicast-domains コマンドを使用します。

Amazon VPC Transit Gateway を使用してマルチキャストドメインにタグを追加する

目的、所有者、環境などに応じて、タグを整理して識別しやすくするために、リソースにタグを追加します。各マルチキャストドメインに複数のタグを追加できます。タグキーは、マルチキャストドメインごとに一意である必要があります。既にマルチキャストドメイン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。詳細については、「Amazon EC2リソースのタグ付け」を参照してください。

コンソールを使用してマルチキャストドメインにタグを追加するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [Actions] (アクション)、[Manage tags] (タグの管理) を選択します。
5. タグごとに、[Add new tag] (新しいタグの追加)を選択し、キーの名前と値を入力します。
6. [Save] を選択します。

を使用してマルチキャストドメインにタグを追加するには AWS CLI

create-tags コマンドを使用します。

Amazon VPC Transit Gateway を使用してマルチキャストドメインを削除する

マルチキャストドメインを削除するには、次の手順に従います。

コンソールを使用してマルチキャストドメインを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択し、[Actions] (アクション)、[Delete multicast domain] (マルチキャストドメインの削除) の順に選択します。
4. 確認を求められたら、**delete**と入力し、[削除] を選択します。

を使用してマルチキャストドメインを削除するには AWS CLI

delete-transit-gateway-multicast-domain コマンドを使用します。

Amazon VPC Transit Gateway の共有マルチキャストドメイン

マルチキャストドメイン共有を使用すると、マルチキャストドメイン所有者は、その組織内の AWS アカウント、または AWS Organizations内の組織全体とドメインを共有できます。マルチキャストドメイン所有者は、マルチキャストドメインを一元的に作成および管理できます。共有されると、これらのユーザーは共有マルチキャストドメインで次の操作を実行できます。

- マルチキャストドメイン内のグループメンバーまたはグループソースを登録および登録解除する
- サブネットをマルチキャストドメインに関連付けたり、サブネットとマルチキャストドメインとの関連付けを解除したりする

マルチキャストドメイン所有者は、マルチキャストドメインを次のユーザーと共有できます。

- AWS 組織内または 内の組織全体の アカウント AWS Organizations
- の組織内の組織単位 AWS Organizations
- の組織全体 AWS Organizations
- AWS の外部にある アカウント AWS Organizations。

  マルチキャストドメインを Organization 外の AWS アカウントと共有するには、 を使用してリソース共有を作成し AWS Resource Access Manager、マルチキャストドメインを共有するプリンシパルを選択するときに、任意のユーザーとの共有を許可するを選択する必要があります。リソース共有の作成の詳細については、AWS RAM ユーザーガイドの「AWS RAMでのリソース共有の作成」を参照してください。

内容

- Amazon VPC Transit Gateway を使用して共有マルチキャストドメインを特定する

マルチキャストドメインを共有するための前提条件

- マルチキャストドメインを共有するには、 AWS アカウント内でそのドメインを所有している必要があります。自身が共有を受けているマルチキャストドメインは共有できません。
- マルチキャストドメインを の組織または組織単位と共有するには AWS Organizations、 との共有を有効にする必要があります AWS Organizations。詳細については、AWS RAM ユーザーガイドの「Enable Sharing with AWS Organizations」を参照してください。

関連サービス

マルチキャストドメイン共有は AWS Resource Access Manager () と統合されますAWS RAM。AWS RAM は、任意の AWS アカウントまたは を通じて AWS リソースを共有できるようにするサービスです AWS Organizations。 AWS RAMを使用した リソース共有。これにより、自身が所有するリソースを共有できます。リソース共有は、共有するリソースと、共有するユーザーを指定します。コンシューマーは、個々の AWS アカウント、組織単位、または の組織全体にすることができます AWS Organizations。

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

共有マルチキャストドメインのアクセス許可

所有者のアクセス許可

所有者は、マルチキャストドメインと、ドメインに登録または関連付けたメンバーとアタッチメントの管理に責任を負います。所有者は、いつでも共有アクセスを変更または取り消すことができます。AWS Organizations を使用して、コンシューマーが共有マルチキャストドメインで作成するリソースを表示、変更、削除できます。

コンシューマーのアクセス許可

共有マルチキャストドメインのユーザーは、作成したマルチキャストドメインと同じ方法で、共有マルチキャストドメインに対して次の操作を実行できます。

- マルチキャストドメイン内のグループメンバーまたはグループソースを登録および登録解除する
- サブネットをマルチキャストドメインに関連付けたり、サブネットとマルチキャストドメインとの関連付けを解除したりする

コンシューマーは、共有マルチキャストドメイン上に作成するリソースの管理に責任を負います。

お客様は、他のコンシューマーまたはマルチキャストドメイン所有者が所有するリソースを表示または変更することはできません。また、それらの者と共有されているマルチキャストドメインを変更することもできません。

請求と使用量測定

所有者またはコンシューマーのマルチキャストドメインを共有するための追加料金は発生しません。

クォータ

共有マルチキャストドメインは、所有者と共有ユーザーのマルチキャストドメインクォータにカウントされます。

Amazon VPC Transit Gateway のアベイラビリティーゾーン間でリソースを共有する

リソースがリージョンのアベイラビリティーゾーンに分散されるように、Amazon VPC Transit Gateway は アベイラビリティーゾーンを各アカウントの名前に個別にマッピングします。このため、アカウントが異なると、アベイラビリティーゾーンの命名方法が異なる場合があります。例えば、us-east-1a AWS アカウントのアベイラビリティーゾーンの場所が別の AWS アカウントus-east-1aの場所と同じでない場合があります。

自己のアカウントを基準にしてマルチキャストドメインの場所を特定するには、アベイラビリティーゾーン ID (AZ ID) を使用する必要があります。AZ ID は、すべての AWS アカウントでアベイラビリティーゾーンの一意で一貫性のある識別子です。例えば、 use1-az1はus-east-1リージョンの AZ ID であり、すべての AWS アカウントで同じ場所です。

アカウントのIDsアベイラビリティーゾーンの AZ を表示するには

1. https://console.aws.amazon.com/ram で AWS RAM コンソールを開きます。
2. 現在のリージョンIDsの AZ は、画面の右側にある AZ ID パネルに表示されます。

Amazon VPC Transit Gateway を使用してマルチキャストドメインを共有する

所有者がマルチキャストドメインを共有する場合、次の操作を実行できます。

- グループメンバーまたはグループソースを登録および登録解除する
- サブネットの関連付けおよび関連付けの解除を行う

> **Note**
>
> マルチキャストドメインを共有するには、そのマルチキャストドメインをリソース共有に追加する必要があります。リソース共有は、 AWS アカウント間で AWS RAM リソースを共有できる リソースです。リソース共有では、共有対象のリソースと、共有先のコンシューマーを指定します。を使用してマルチキャストドメインを共有する場合は Amazon Virtual Private Cloud Console、既存のリソース共有に追加します。マルチキャストドメインを新しいリソース共有に追加するには、最初にAWS RAM コンソールを使用してリソース共有を作成する必要があります。
>
> ユーザーが の組織に属 AWS Organizations していて、組織内での共有が有効になっている場合、組織内のコンシューマーには共有マルチキャストドメインへのアクセス許可が自動的に付与されます。それ以外の場合、コンシューマーはリソース共有への参加の招待を受け取り、その招待を受け入れた後で、共有マルチキャストドメインへのアクセス許可が付与されます。

Amazon Virtual Private Cloud コンソール、 AWS RAM コンソール、または を使用して、所有しているマルチキャストドメインを共有できます AWS CLI。

*Amazon Virtual Private Cloud Consoleを使用して所有しているマルチキャストドメインを共有するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Multicast Domains] (マルチキャストドメイン) を選択します。
3. マルチキャストドメインを選択し、[Actions] (アクション)、[Share multicast domain] (マルチキャストドメインの共有) の順に選択します。
4. リソース共有を選択してから、[Share multicast domain] (マルチキャストドメインの共有) を選択します。

AWS RAM コンソールを使用して所有しているマルチキャストドメインを共有するには

「AWS RAM ユーザーガイド 」の「リソース共有の作成」を参照してください。

を使用して所有しているマルチキャストドメインを共有するには AWS CLI

create-resource-share コマンドを使用します。

Amazon VPC Transit Gateway を使用して共有マルチキャストドメインの共有を解除する

共有マルチキャストドメインの共有が解除されると、コンシューマーマルチキャストドメインリソースについて次の事項が生じます。

- コンシューマーサブネットは、マルチキャストドメインとの関連付けが解除されます。サブネットは、コンシューマーアカウントに残ります。
- コンシューマーグループソースおよびグループメンバーは、マルチキャストドメインとの関連付けが解除され、コンシューマーアカウントから削除されます。

マルチキャストドメインの共有を解除するには、リソース共有からそのマルチキャストドメインを削除する必要があります。これは、 AWS RAM コンソールまたは から実行できます AWS CLI。

自己所有の共有マルチキャストドメインを共有解除するには、それをリソース共有から削除する必要があります。これは、、 AWS RAM コンソール Amazon Virtual Private Cloud、または を使用して実行できます AWS CLI。

*Amazon Virtual Private Cloud Consoleを使用して所有している共有マルチキャストドメインの共有を解除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Multicast Domains] (マルチキャストドメイン) を選択します。
3. マルチキャストドメインを選択し、[Actions] (アクション)、[Stop sharing] (共有を停止) の順に選択します。

AWS RAM コンソールを使用して所有している共有マルチキャストドメインの共有を解除するには

「AWS RAM ユーザーガイド」の「リソース共有の更新」を参照してください。

を使用して、所有している共有マルチキャストドメインの共有を解除するには AWS CLI

disassociate-resource-share コマンドを使用します。

Amazon VPC Transit Gateway を使用して共有マルチキャストドメインを特定する

所有者とコンシューマーは、 Amazon Virtual Private Cloud と を使用して共有マルチキャストドメインを識別できます。 AWS CLI

*Amazon Virtual Private Cloud Consoleを使用して共有マルチキャストドメインを識別するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Multicast Domains] (マルチキャストドメイン) を選択します。
3. マルチキャストドメインを選択します。
4. 「マルチキャストドメイン詳細の転送」ページで、所有者 ID を表示してマルチキャストドメインの AWS アカウント ID を識別します。

を使用して共有マルチキャストドメインを識別するには AWS CLI

describe-transit-gateway-multicast-domains コマンドを使用します。コマンドは、所有しているマルチキャストドメインと、共有されているマルチキャストドメインを返します。 は、マルチキャストドメイン所有者の AWS アカウント ID `OwnerId`を示します。

Amazon VPC Transit Gateway を使用してマルチキャストグループにソースを登録する

> **Note**
>
> この手順は、[Static sources support] (静的な送信元のサポート) 属性を [enable] (有効) に設定している場合にのみ必要です。

次の手順に従って、ソースをマルチキャストグループに登録します。ソースは、マルチキャストトラフィックを送信するネットワークインターフェイスです。

ソースを追加する前に、次の情報が必要です。

- マルチキャストドメインの ID
- ソースIDsのネットワークインターフェイスの
- マルチキャストグループの IP アドレス

コンソールを使用して、ソースを登録するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。

3. マルチキャストドメインを選択し、[Actions] (アクション)、[Add group sources] (グループソースの追加) の順に選択します。
4. グループ IP アドレス には、マルチキャストドメインに割り当てる IPv4 CIDR ブロックまたは IPv6CIDRブロックを入力します。
5. [Choose network interfaces (ネットワークインターフェイスの選択)] で、マルチキャスト送信者のネットワークインターフェイスを選択します。
6. 「ソースを追加」 を選択します。

を使用してソースを登録するには AWS CLI

register-transit-gateway-multicast-group-sources コマンドを使用します。

Amazon VPC Transit Gateway を使用してマルチキャストグループにメンバーを登録する

グループメンバーをマルチキャストグループに登録するには、次の手順を実行します。

メンバーを追加する前に、次の情報が必要です。

- マルチキャストドメインの ID
- グループメンバーIDsのネットワークインターフェイスの
- マルチキャストグループの IP アドレス

コンソールを使用して、メンバーを登録するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択し、[Actions] (アクション)、[Add group members] (グループメンバーの追加) の順に選択します。
4. グループ IP アドレス には、マルチキャストドメインに割り当てる IPv4 CIDR ブロックまたは IPv6CIDRブロックを入力します。
5. [Choose network interfaces (ネットワークインターフェイスの選択)] で、マルチキャスト受信者のネットワークインターフェイスを選択します。
6. [Add members (メンバーの追加)] を選択します。

を使用してメンバーを登録するには AWS CLI

register-transit-gateway-multicast-group-members コマンドを使用します。

Amazon VPC Transit Gateway を使用してマルチキャストグループからソースを登録解除する

マルチキャストグループに手動で送信元を追加していない限り、この手順を実行する必要はありません。

コンソールを使用して、ソースを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [グループ] タブを選択します。
5. ソースを選択し、[Remove source (ソースを削除)] を選択します。

を使用してソースを削除するには AWS CLI

deregister-transit-gateway-multicast-group-sources コマンドを使用します。

Amazon VPC Transit Gateway を使用してマルチキャストグループからメンバーを登録解除する

マルチキャストグループに手動でメンバーを追加していない限り、この手順を実行する必要はありません。

コンソールを使用して、メンバーの登録を解除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [グループ] タブを選択します。
5. メンバーを選択し、[Remove member (メンバーの削除)] を選択します。

を使用してメンバーの登録を解除するには AWS CLI

deregister-transit-gateway-multicast-group-members コマンドを使用します。

Amazon VPC Transit Gateway を使用してマルチキャストグループを表示する

マルチキャストグループに関する情報を表示して、メンバーがIGMPv2プロトコルを使用して検出されたことを確認できます。メンバータイプ (コンソール内) 、または MemberType (内 AWS CLI) は、プロトコルを持つメンバー AWS が検出されIGMPると表示されます。

コンソールを使用して、マルチキャストグループを表示するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [グループ] タブを選択します。

を使用してマルチキャストグループを表示するには AWS CLI

search-transit-gateway-multicast-groups コマンドを使用します。

次の例は、IGMPプロトコルがマルチキャストグループメンバーを検出したことを示しています。

```
aws ec2 search-transit-gateway-multicast-groups --transit-gateway-multicast-domain tgw-mcast-domain-000fb24d04EXAMPLE
{
    "MulticastGroups": [
        {
            "GroupIpAddress": "224.0.1.0",
            "TransitGatewayAttachmentId": "tgw-attach-0372e72386EXAMPLE",
            "SubnetId": "subnet-0187aff814EXAMPLE",
            "ResourceId": "vpc-0065acced4EXAMPLE",
            "ResourceType": "vpc",
            "NetworkInterfaceId": "eni-03847706f6EXAMPLE",
            "MemberType": "igmp"
        }
    ]
}
```

Amazon VPC Transit Gateway で Windows Server のマルチキャストを設定する

Windows Server 2019 または 2022 上の Transit Gateway と連携するようにマルチキャストを設定する場合は、追加の手順を実行する必要があります。これをセットアップするには、 を使用し PowerShell、次のコマンドを実行する必要があります。

を使用して Windows Server のマルチキャストを設定するには PowerShell

1. TCP/IP スタックIGMPv2IGMPv3の代わりに を使用するように Windows Server を変更します。

   ```
   PS C:\> New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services
   \Tcpip\Parameters -Name IGMPVersion -PropertyType DWord -Value 3
   ```

   > **Note**
   >
   > `New-ItemProperty` は、 IGMPバージョンを指定するプロパティインデックスです。v2 IGMP はマルチキャストでサポートされているバージョンであるため、 プロパティは `Value`である必要があります3。Windows レジストリを編集する代わりに、次のコマンドを実行してIGMPバージョンを 2 に設定できます。
   > `Set-NetIPv4Protocol -IGMPVersion Version2`

2. Windows Firewall は、デフォルトでほとんどのUDPトラフィックを削除します。まず、どの接続プロファイルがマルチキャストに使用されているかを確認する必要があります。

   ```
   PS C:\> Get-NetConnectionProfile | Select-Object NetworkCategory

   NetworkCategory
   ---------------
            Public
   ```

3. 前のステップから接続プロファイルを更新して、必要なUDPポート (複数可) へのアクセスを許可します。

   ```
   PS C:\> Set-NetFirewallProfile -Profile Public -Enabled False
   ```

4. EC2 インスタンスを再起動します。
5. マルチキャストアプリケーションをテストして、トラフィックのフローが予期したとおりのものであることを確認します。

例: Amazon VPC Transit Gateway を使用してIGMP設定を管理する

この例では、マルチキャストトラフィックに IGMPプロトコルを使用するホストを少なくとも 1 つ示しています。 は、インスタンスからIGMP`JOIN`メッセージを受信すると、マルチキャストグループ AWS を自動的に作成し、インスタンスをこのグループのメンバーとして追加します。を使用して、非IGMPホストをメンバーとしてグループに静的に追加することもできます AWS CLI。マルチキャストドメインに関連付けられたサブネットにあるインスタンスはすべて、トラフィックを送信でき、グループメンバーはマルチキャストトラフィックを受信します。

設定を完了するには、次の手順を実行します。

1. を作成しますVPC。の作成の詳細についてはVPCs、「Amazon ユーザーガイド」の「 VPCの作成」を参照してください。 VPC
2. VPC にサブネットを作成します。サブネットの作成の詳細については、「Amazon VPC ユーザーガイド」の「 でのサブネットVPCの作成」を参照してください。
3. マルチキャストトラフィック用に設定されたトランジットゲートウェイを作成します。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
4. VPC 添付ファイルを作成します。詳細については、「the section called “VPC 添付ファイルを作成する”」を参照してください。
5. IGMP サポート用に設定されたマルチキャストドメインを作成します。詳細については、「the section called “IGMP マルチキャストドメインを作成する”」を参照してください。

   以下の設定を使用します。

   - IGMPv2 サポートを有効にします。
   - 静的ソースサポートを無効にします。
6. トランジットゲートウェイVPCアタッチメントのサブネットとマルチキャストドメインの間に関連付けを作成します。詳細については、「the section called “VPC アタッチメントとサブネットをマルチキャストドメインに関連付ける”」を参照してください。
7. のデフォルトIGMPバージョンは EC2ですIGMPv3。すべてのIGMPグループメンバーのバージョンを変更する必要があります。以下のコマンドを実行できます。

   ```
   sudo sysctl net.ipv4.conf.eth0.force_igmp_version=2
   ```
8. IGMP プロトコルを使用しないメンバーをマルチキャストグループに追加します。詳細については、「the section called “マルチキャストグループにメンバーを登録する”」を参照してください。

例: Amazon VPC Transit Gateway を使用した静的ソース設定の管理

この例では、マルチキャストソースをグループに静的に追加します。ホストは、IGMPプロトコルを使用してマルチキャストグループに参加または退出しません。マルチキャストトラフィックを受信するグループメンバーを静的に追加する必要があります。

設定を完了するには、次の手順を実行します。

1. を作成しますVPC。の作成の詳細についてはVPCs、「Amazon ユーザーガイド」の「 VPCの作成」を参照してください。 VPC
2. VPC にサブネットを作成します。サブネットの作成の詳細については、「Amazon VPC ユーザーガイド」の「 でのサブネットVPCの作成」を参照してください。
3. マルチキャストトラフィック用に設定されたトランジットゲートウェイを作成します。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
4. VPC 添付ファイルを作成します。詳細については、「the section called “VPC 添付ファイルを作成する”」を参照してください。
5. サポートなしで設定されたマルチキャストドメインを作成しIGMP、ソースを静的に追加するためのサポートを作成します。詳細については、「the section called “静的ソースマルチキャストドメインを作成する”」を参照してください。

   以下の設定を使用します。

   - IGMPv2 サポート を無効にします。
   - 手動で送信元を追加するには、[Static sources support] (静的な送信元のサポート) を有効にします。

     属性が有効になっている場合、マルチキャストトラフィックを送信できる唯一のリソースは送信元です。その他の場合は、マルチキャストドメインに関連付けられたサブネットにあるインスタンスはすべて、マルチキャストトラフィックを送信でき、グループメンバーはマルチキャストトラフィックを受信します。
6. トランジットゲートウェイVPCアタッチメントのサブネットとマルチキャストドメインの間に関連付けを作成します。詳細については、「the section called “VPC アタッチメントとサブネットをマルチキャストドメインに関連付ける”」を参照してください。
7. [Static sources support] (静的な送信元のサポート) を有効にした場合は、送信元をマルチキャストグループに追加します。詳細については、「the section called “マルチキャストグループにソースを登録する”」を参照してください。

8. メンバーをマルチキャストグループに追加します。詳細については、「the section called “マルチキャストグループにメンバーを登録する”」を参照してください。

例: Amazon VPC Transit Gateway での静的グループメンバー設定の管理

この例では、マルチキャストメンバーをグループに静的に追加する方法を示します。ホストは、IGMPプロトコルを使用してマルチキャストグループに参加または退出することはできません。マルチキャストドメインに関連付けられたサブネットにあるインスタンスはすべて、マルチキャストトラフィックを送信でき、グループメンバーはマルチキャストトラフィックを受信します。

設定を完了するには、次の手順を実行します。

1. を作成しますVPC。の作成の詳細についてはVPCs、「Amazon ユーザーガイド」の「 VPCの作成」を参照してください。 VPC
2. VPC にサブネットを作成します。サブネットの作成の詳細については、「Amazon VPC ユーザーガイド」の「 でのサブネットVPCの作成」を参照してください。
3. マルチキャストトラフィック用に設定されたトランジットゲートウェイを作成します。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
4. VPC 添付ファイルを作成します。詳細については、「the section called “VPC 添付ファイルを作成する”」を参照してください。
5. サポートなしで設定されたマルチキャストドメインを作成しIGMP、ソースを静的に追加するためのサポートを作成します。詳細については、「the section called “静的ソースマルチキャストドメインを作成する”」を参照してください。

   以下の設定を使用します。

   - IGMPv2 サポート を無効にします。
   - 静的ソースサポートを無効にします。
6. トランジットゲートウェイVPCアタッチメントのサブネットとマルチキャストドメイン間の関連付けを作成します。詳細については、「the section called “VPC アタッチメントとサブネットをマルチキャストドメインに関連付ける”」を参照してください。
7. メンバーをマルチキャストグループに追加します。詳細については、「the section called “マルチキャストグループにメンバーを登録する”」を参照してください。

Amazon VPC Transit Gateway フローログ

トランジットゲートウェイフローログは、トランジットゲートウェイとの間で送受信される IP VPC トラフィックに関する情報をキャプチャできる Amazon Transit Gateway の機能です。フローログデータは、Amazon CloudWatch Logs、Amazon S3、または Firehose に発行できます。フローログを作成したら、選択した送信先でそのデータを取得して表示できます。フローログデータはネットワークトラフィックのパスの外で収集されるため、ネットワークのスループットやレイテンシーには影響しません。ネットワークパフォーマンスに影響を与えるリスクなしに、フローログを作成または削除できます。Transit Gateway フローログは、「the section called “Transit Gateway Flow Log のレコード”」で説明されている Transit Gateway のみに関連する情報をキャプチャします。のネットワークインターフェイスとの間で送受信される IP トラフィックに関する情報をキャプチャする場合はVPCs、VPCフローログを使用します。詳細については、「Amazon VPCユーザーガイド」のVPC「フローログを使用した IP トラフィックのログ記録」を参照してください。

> **Note**
>
> トランジットゲートウェイフローログを作成するには、トランジットゲートウェイの所有者である必要があります。所有者でない場合は、トランジットゲートウェイの所有者からアクセス許可を付与する必要があります。

モニタリングされる Transit Gateway のフローログデータは、フローログレコードとして記録されます。これは、トラフィックフローについて説明するフィールドで構成されるログイベントです。詳細については、「Transit Gateway Flow Log のレコード」を参照してください。

フローログを作成するには、以下の内容を指定します。

- フローログを作成するリソース
- フローログデータを発行する送信先

フローログを作成後、データ収集と選択された送信先へのデータ発行が開始されるまでに数分かかる場合があります。フローログで、Transit Gateway のリアルタイムのログストリームはキャプチャされません。詳細については、「Amazon VPC Transit Gateway フローログを作成する」を参照してください。

フローログにタグを適用できます。タグはそれぞれ、1 つのキーとオプションの 1 つの値で構成されており、どちらもお客様側が定義します。タグは、目的や所有者などによって、フローログを整理するのに役立ちます。

フローログが不要になった場合には、それを削除することができます。フローログを削除すると、リソースのフローログサービスは無効になり、新しいフローログレコードは作成されず、 CloudWatch ログまたは Amazon S3 に発行されません。フローログを削除しても、トランジットゲートウェイの既存のフローログレコードまたはログストリーム (CloudWatch ログの場合) またはログファイルオブジェクト (Amazon S3 の場合) は削除されません。既存のログストリームを削除するには、 CloudWatch ログコンソールを使用します。既存のログファイルオブジェクトを削除するには、Amazon S3 コンソールを使用します。フローログを削除した後で、データの収集が中止するまでに数分かかる場合があります。詳細については、「Amazon VPC Transit Gateways フローログレコードを削除する」を参照してください。

制限事項

Transit Gateway フローログには、次の制限が適用されます。

- マルチキャストトラフィックはサポートされていません。
- Connect アタッチメントはサポートされていません。すべての Connect フローログはトランスポートアタッチメントの下に表示されるため、トランジットゲートウェイまたは Connect トランスポートアタッチメントで有効にする必要があります。

Transit Gateway Flow Log のレコード

フローログレコードは、Transit Gateway のネットワークフローを表します。各レコードは、スペースで区切られたフィールドから成る文字列です。送信元、送信先、プロトコルなど、レコードにはトラフィックフローのさまざまなコンポーネントの値が含まれています。

フローログを作成するときは、フローログレコードのデフォルトの形式を使用するか、カスタム形式を指定できます。

内容

デフォルトの形式

デフォルトの形式では、フローログレコードには、使用可能なフィールドテーブルに表示される順序でバージョン 2 から 6 のフィールドが含まれます 。デフォルトの形式をカスタマイズまたは変更することはできません。使用可能なすべてのフィールドまたはフィールドの異なるサブセットをキャプチャするには、代わりにカスタム形式を指定します。

カスタム形式

カスタム形式を使用して、フローログレコードに含めるフィールドと順序を指定します。これにより、ニーズに合ったフローログを作成し、関連のないフィールドを省略できます。カスタム形式を使用すると、発行されたフローログから特定の情報を抽出する別個のプロセスが不要になります。使用可能なフローログフィールドは任意の数指定できますが、少なくとも 1 つ指定する必要があります。

使用可能なフィールド

次の表に、Transit Gateway フローログレコードの使用可能なすべてのフィールドを示します。Version 列には、フィールドが導入されたバージョンが表示されます。

Amazon S3 にフローログデータを公開する場合、フィールドのデータ型はフローログ形式によって異なります。形式がプレーンテキストの場合、すべてのフィールドは STRING 形式です。形式が Parquet の場合は、フィールドのデータ型の表を参照してください。

フィールドが特定のレコードに該当しないか、特定のレコードに対して計算できなかった場合、レコードでそのエントリには「-」記号が表示されます。パケットヘッダーから直接取得されないメタデータフィールドは、ベストエフォート近似値であり、値が欠落しているか、不正確である可能性があります。

フィールド	説明	Version
version	フィールドが導入されたバージョンを示します。デフォルトの形式には、すべてのバージョン 2 フィールドが含まれ、順番はテーブルと同じです。 Parquet データ型： INT_32	2
resource-type	サブスクリプションが作成されるリソースのタイプ。Transit Gateway フローログの場合、これは になりますTransitGateway。	6

フィールド	説明	Version
	Parquet データ型： STRING	
account-id	ソーストランジットゲートウェイの所有者の AWS アカウント ID。 Parquet データ型： STRING	2
tgw-id	トラフィックが記録される Transit Gateway の ID。 Parquet データ型: STRING	6
tgw-attachment-id	トラフィックが記録される Transit Gateway アタッチメントの ID。 Parquet データ型: STRING	6
tgw-src-vpc-account-id	ソースVPCトラフィックの AWS アカウント ID。 Parquet データ型： STRING	6
tgw-dst-vpc-account-id	送信先VPCトラフィックの AWS アカウント ID。 Parquet データ型： STRING	6
tgw-src-vpc-id	トランジットゲートウェイVPCのソースの ID Parquet データ型： STRING	6
tgw-dst-vpc-id	トランジットゲートウェイVPCの送信先の ID。 Parquet データ型： STRING	6
tgw-src-subnet-id	Transit Gateway 送信元トラフィックのサブネットの ID。 Parquet データ型： STRING	6
tgw-dst-subnet-id	Transit Gateway 送信先トラフィックのサブネットの ID。 Parquet データ型： STRING	6

フィールド	説明	Version
tgw-src-eni	フローのソーストランジットゲートウェイアタッチメントENIのID。 Parquet データ型： STRING	6
tgw-dst-eni	フローの送信先トランジットゲートウェイENIアタッチメントのID。 Parquet データ型： STRING	6
tgw-src-az-id	トラフィックが記録される Transit Gateway を含むアベイラビリティーゾーンの ID。トラフィックがサブロケーションからの場合、レコードにはこのフィールドに「-」記号が表示されます。 Parquet データ型： STRING	6
tgw-dst-az-id	トラフィックが記録される送信先 Transit Gateway を含むアベイラビリティーゾーンの ID。 Parquet データ型： STRING	6
tgw-pair-attachment-id	フローの方向に応じて、これはフローの出力または入力のアタッチメント ID になります。 Parquet データ型： STRING	6
srcaddr	受信トラフィックの送信元アドレス。 Parquet データ型: STRING	2
dstaddr	送信トラフィックの送信先アドレス。 Parquet データ型: STRING	2
srcport	トラフィックの送信元ポート。 Parquet データ型: INT_32	2

フィールド	説明	Version
dstport	トラフィックの送信先ポート。 Parquet データ型: INT_32	2
protocol	トラフィックのIANAプロトコル番号。詳細については、「割り当てられたインターネットプロトコル番号」を参照してください。 Parquet データ型: INT_64	2
packets	フロー中に転送されたパケットの数。 Parquet データ型 : INT_64	2
bytes	フロー中に転送されたバイト数。 Parquet データ型: INT_64	2
start	集約間隔内にフローの最初のパケットが受信された時間 (UNIX 秒)。これは、パケットが Transit Gateway 上で送信または受信されてから最大 60 秒になる場合があります。 Parquet データ型: INT_64	2
end	集約間隔内にフローの最後のパケットが受信された時間 (UNIX 秒)。これは、パケットが Transit Gateway 上で送信または受信されてから最大 60 秒になる場合があります。 Parquet データ型: INT_64	2

フィールド	説明	Version
log-status	フローログのステータス。 • OK — データは選択された送信先に正常にログ記録されます。 • NODATA — 集約間隔中に、ネットワークインターフェイスとの間で送受信されるネットワークトラフィックはありませんでした。 • SKIPDATA — 一部のフローログレコードは、集約間隔中にスキップされました。これは、内部的なキャパシティー制限、または内部エラーが原因である可能性があります。 Parquet データ型： STRING	2
type	トラフィックの種類。指定できる値は IPv4 | IPv6 | ですEFA。詳細については、「Amazon ユーザーガイド」の「Elastic Fabric Adapter」を参照してください。 EC2 Parquet データ型： STRING	3
packets-lost-no-route	ルートが指定されていないためにパケットが失われました。 Parquet データ型: INT_64	6
packets-lost-blackhole	ブラックホールのためにパケットが失われました。 Parquet データ型: INT_64	6
packets-lost-mtu-exceeded	サイズが を超えたためにパケットが失われましたMTU。 Parquet データ型： INT_64	6
packets-lost-ttl-expired	の有効期限が切れたためにパケットが失われました time-to-live。 Parquet データ型： INT_64	6

フィールド	説明	Version
tcp-flags	次のTCPフラグのビットマスク値。 • FIN — 1 • SYN — 2 • RST — 4 • PSH — 8 • ACK — 16 • SYN-ACK — 18 • URG — 32 **Important** フローログエントリがACKパケットのみで構成されている場合、フラグ値は 16 ではなく 0 です。 TCP フラグに関する一般的な情報 (、FIN、 などのフラグの意味などACK) についてはSYN、Wikipedia のTCP「セグメント構造」を参照してください。 TCP フラグは、集計間隔中に OR で指定できます。短い接続の場合、フラグはフローログレコードの同じ行に設定されます。例えば、 SYN-ACK と には 19FIN、 と には 3 SYNですFIN。 Parquet データ型： INT_32	3
region	トラフィックが記録される Transit Gateway を含むリージョン。 Parquet データ型： STRING	4
flow-direction	トラフィックがキャプチャされるインターフェイスに対するフローの方向。指定できる値は次のとおりです: ingress | egress。 Parquet データ型： STRING	5

フィールド	説明	Version
pkt-src-aws-service	送信元 IP アドレスが サービスのものである場合の、 の IP アドレス範囲のサブセットの名前。 srcaddr AWS 指定可能な値は次のとおりです:AMAZON |AMAZON_APPFLOW |AMAZON_CONNECT |API_GATEWAY |CHIME_MEETINGS |CHIME_VOICECONNECTOR |CLOUD9 |CLOUDFRONT |CODEBUILD |DYNAMODB |EBS |EC2 |EC2_INSTANCE_CONNECT |GLOBALACCELERATOR |KINESIS_VIDEO_STREAMS |ROUTE53 |ROUTE53_HEALTHCHECKS |ROUTE53_HEALTHCHECKS_PUBLISHING |ROUTE53_RESOLVER |S3 |WORKSPACES_GATEWAYS。 Parquet データ型： STRING	5
pkt-dst-aws-service	送信先 IP アドレスが AWS サービスのものである場合、 dstaddr フィールドの IP アドレス範囲のサブセットの名前。可能な値の一覧については、pkt-src-aws-service フィールドをご参照ください。 Parquet データ型： STRING	5

フローログの使用の管理

デフォルトでは、 ユーザーにはフローログを使用するためのアクセス許可がありません。フローログを作成、説明、削除するアクセス権限をユーザーに付与するユーザーポリシーを作成できます。詳細については、「Amazon リファレンス」の「Amazon EC2リソースに必要なアクセス許可をIAMユーザーに付与する」を参照してください。 EC2 API

フローログを作成、説明、削除する完全なアクセス許可をユーザーに付与するポリシー例を次に示します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
```

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

CloudWatch Logs または Amazon S3 のどちらに発行するかに応じて、追加のIAMロールとアクセス許可の設定が必要です。詳細については、「Amazon Logs の Transit Gateway フロー CloudWatch ログレコード」および「 Amazon S3 のトランジットゲートウェイフローログレコード 」を参照してください。

Transit Gateway Flow Logs の料金

Transit Gateway フローログを発行すると、提供されたログに対するデータインジェスト料金とアーカイブ料金が適用されます。発行されたログを発行する際の料金の詳細については、Amazon CloudWatch 料金表 を開き、次に有料階層 でログ を選択し、発行されたログ を見つけます。

Amazon VPC Transit Gateways フローログの IAMロールを作成または更新する

既存のロールを更新するか、次の手順を使用して、 AWS Identity and Access Management コンソールを使用してフローログで使用する新しいロールを作成できます。

フローログの IAMロールを作成するには

1. でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. ナビゲーションペインで [ロール]、[ロールの作成] の順に選択します。
3. 信頼できるエンティティの種類の選択 で、AWS サービス を選択します。ユースケース で、 を選択しますEC2。[Next (次へ)] を選択します。
4. [アクセス権限を追加] ページで、[次へ: レビュー] を選択し、オプションでタグを追加します。[Next (次へ)] を選択します。
5. 名前、確認、作成ページで、ロールの名前を入力し、オプションで説明を入力します。[ロールの作成] を選択します。
6. ロールの名前を選択します。アクセス許可の追加 で、インラインポリシーの作成 を選択し、JSONタブを選択します。
7. 「IAM フローログを CloudWatch ログに発行するための ロール」から最初のポリシーをコピーして、ウィンドウに貼り付けます。[ポリシーの確認] を選択します。

8. ポリシーの名前を入力し、[ポリシーの作成] を選択します。
9. ロールの名前を選択します。[信頼関係] で、[信頼関係の編集] を選択します。既存のポリシードキュメントで、サービスを ec2.amazonaws.com から vpc-flow-logs.amazonaws.com に変更します。[信頼ポリシーの更新] を選択します。
10. 概要ページで、ロールARNの を書き留めます。これは、フローログを作成するARNときに必要になります。

Amazon Logs の Transit Gateway フロー CloudWatch ログレコード

フローログは、フローログデータを Amazon に直接発行できます CloudWatch。

CloudWatch Logs に発行されると、フローログデータはロググループに発行され、各トランジットゲートウェイにはロググループに一意のログストリームがあります。ログストリームにはフローログレコードが含まれます。同じロググループにデータを公開する複数のフローログを作成できます。同じ Transit Gateway が同じロググループの 1 つまたは複数のフローログに存在する場合、1 つの組み合わされたログストリームがあります。1 つのフローログで、拒否されたトラフィックをキャプチャし、別のフローログで、許可されたトラフィックをキャプチャするよう指定した場合、組み合わされたログストリームですべてのトラフィックがキャプチャされます。

フローログを CloudWatch Logs に発行すると、提供されたログのデータ取り込み料金とアーカイブ料金が適用されます。詳細については、「Amazon CloudWatch の料金」を参照してください。

CloudWatch Logs のタイムスタンプフィールドは、フローログレコードにキャプチャされた開始時刻に対応します。ingestionTime フィールドには、フローログレコードが CloudWatch Logs によって受信された日時が表示されます。タイムスタンプは、フローログレコードでキャプチャされた終了時刻より後になります。

CloudWatch ログの詳細については、「Amazon Logs ユーザーガイド」の CloudWatch 「ログに送信されたログ」を参照してください。 CloudWatch

内容

- IAM フローログを CloudWatch ログに発行するための ロール
- IAM ユーザーがロールを渡すためのアクセス許可
- に発行する Transit Gateways フローログレコードを作成する Amazon CloudWatch Logs
- Amazon で Transit Gateway Flow Logs レコードを表示する CloudWatch

- Amazon Logs で Transit Gateway フロー CloudWatch ログレコードを処理する

IAM フローログを CloudWatch ログに発行するための ロール

フローログに関連付けられているIAMロールには、 CloudWatch Logs で指定されたロググループにフローログを発行するための十分なアクセス許可が必要です。IAM ロールは に属している必要があります AWS アカウント。

IAM ロールにアタッチされているIAMポリシーには、少なくとも次のアクセス許可が含まれている必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

フローログサービスがロールを引き受けることができる信頼関係がロールにあることも確認します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

Confused Deputy Problem (混乱した使節の問題) から自分を守るために、aws:SourceAccount および aws:SourceArn の条件キーを使用することをお勧めします。例えば、前述の信頼ポリシーに次の条件ブロックを追加できます。ソースアカウントはフローログの所有者であり、ソースARNはフローログ ですARN。フローログ ID がわからない場合は、 のその部分をワイルドカード (*) ARNに置き換え、フローログを作成した後にポリシーを更新できます。

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

IAM ユーザーがロールを渡すためのアクセス許可

ユーザーは、フローログに関連付けられているIAMロールに対して iam:PassRoleアクションを使用するアクセス許可も必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

に発行する Transit Gateways フローログレコードを作成する Amazon CloudWatch Logs

Transit Gateway のフローログを作成できます。IAM ユーザーとしてこれらのステップを実行する場合は、 iam:PassRoleアクションを使用するアクセス許可があることを確認してください。詳細については、「IAM ユーザーがロールを渡すためのアクセス許可」を参照してください。

コンソールを使用して Transit Gateway フローログを作成するには

1. にサインイン AWS Management Console し、 で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Transit Gateway] を選択します。
3. 1 つ以上のトランジットゲートウェイのチェックボックスを選択し、アクション 、フローログの作成 を選択します。
4. 送信先 で、ログに送信 CloudWatch を選択します。
5. [送信先ロググループ] で、現在の送信先ロググループの名前を選択します。

   > **Note**
   >
   > 送信先ロググループがまだ存在しない場合は、このフィールドに新しい名前を入力すると、新しい送信先ロググループが作成されます。

6. IAM ロール には、ログを CloudWatch Logs に発行する権限を持つロールの名前を指定します。
7. [Lログレコードの形式] で、フローログレコードの形式を選択します。
   - デフォルトの形式を使用するには、[AWS のデフォルト形式] を選択します。
   - カスタム形式を使用するには、[カスタム形式] を選択し、[ログ形式] からフィールドを選択します。
8. (オプション) フローログにタグを適用するには、[新規タグを追加] を選択します。
9. [フローログの作成] を選択します。

コマンドラインを使用してフローログを作成するには

以下のいずれかのコマンドを使用します。

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs (Amazon EC2 クエリ API)

次の AWS CLI 例では、トランジットゲートウェイ情報をキャプチャするフローログを作成します。フローログは、IAMロール を使用してmy-flow-logs、アカウント 123456789101 の CloudWatch というログのロググループに配信されますpublishFlowLogs。

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-1a2b3c4d --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

Amazon で Transit Gateway Flow Logs レコードを表示する CloudWatch

選択した送信先タイプに応じて、 CloudWatch ログコンソールまたは Amazon S3 コンソールを使用してフローログレコードを表示できます。フローログを作成してからコンソールに表示されるまでに、数分かかる場合があります。

CloudWatch Logs に発行されたフローログレコードを表示するには

1. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
2. ナビゲーションペインで、[ログ] を選択し、フローログを含むロググループを選択します。各 Transit Gateway のログストリームのリストが表示されます。
3. フローログレコードを表示する Transit Gateway の ID を含むログストリームを選択します。詳細については、「Transit Gateway Flow Log のレコード」を参照してください。

Amazon Logs で Transit Gateway フロー CloudWatch ログレコードを処理する

Logs によって収集された他のログイベントと同様に、フロー CloudWatch ログレコードを操作できます。ログデータとメトリクスフィルターのモニタリングの詳細については、「Amazon ユーザーガイド」の「ログデータの検索とフィルタリング」を参照してください。 CloudWatch

例: フローログの CloudWatch メトリクスフィルターとアラームを作成する

この例では、tgw-123abc456bca のフローログがあります。1 時間以内にTCPポート 22 (SSH) 経由でインスタンスに接続しようとして 10 回以上拒否された場合に警告するアラームを作成するとします。最初に、アラームを作成するトラフィックのパターンと一致するメトリクスフィルターを作成する必要があります。次に、メトリクスフィルターのアラームを作成できます。

拒否されたSSHトラフィックのメトリクスフィルターを作成し、フィルターのアラームを作成するには

1. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
2. ナビゲーションペインで、[ログ]、[ロググループ] の順に選択します。

3. ロググループのチェックボックスを選択し、アクション、メトリクスフィルターの作成 を選択します。
4. [フィルターパターン] で、次のように入力します。

```
[version, resource_type, account_id,tgw_id="tgw-123abc456bca”, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= "10.0.0.1", dstaddr,
 srcport=“80”, dstport, protocol=“6”, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

5. [テストするログデータの選択] で、Transit Gateway のログストリームを選択します。(オプション) フィルターパターンと一致するログデータの行を表示するには、[テストパターン] を選択します。準備ができたら、[次へ] を選択します。
6. フィルター名、メトリクス名前空間、およびメトリック名を入力します。メトリクス値の設定を「**1**」にします。完了したら、[次へ] を選択し、その後 [メトリクスフィルターの作成] を選択します。
7. ナビゲーションペインで、[アラーム]、[すべてのアラーム] の順に選択します。
8. [アラームの作成] を選択します。
9. 作成したメトリクスフィルターの名前空間を選択します。

   新しいメトリクスがコンソールに表示されるまでに数分かかる場合があります。
10. 作成したメトリクス名を選択し、その後 [メトリクスの選択] を選択します。
11. アラームを以下のように設定して、[次へ] をクリックします。

    - [統計] で、[合計] を選択します。これにより、指定された期間のデータポイントの総数をキャプチャしていることを確認できます。
    - [期間] で、[1 時間] を選択します。
    - [随時] で、[以上] を選択し、しきい値は「**10**」と入力します。
    - [追加設定]、[警告を出すデータポイント数] はデフォルトの「**1**」のままにしておきます。
12. 通知 で、既存のSNSトピックを選択するか、新しいトピックを作成 を選択して新しいトピックを作成します。[Next (次へ)] を選択します。
13. 次のページで、アラームの名前と説明を入力し、[次へ] を選択します。
14. アラームの設定が終わったら、[アラームを作成] を選択します。

Amazon S3 のトランジットゲートウェイフローログレコード

フローログはフローログデータを Amazon S3 に発行できます。

Amazon S3 に発行した場合、フローログデータは、指定する既存の Amazon S3 バケットに発行されます。モニタリングされるすべての Transit Gateway のフローログレコードが、バケットに保存された一連のログファイルオブジェクトに発行されます。

フローログを Amazon S3 に発行すると、 Amazon CloudWatch データインジェスト料金とアーカイブ料金が によって提供されるログに適用されます。発行されたログの CloudWatch 料金の詳細については、Amazon CloudWatch の料金 を開き、ログ を選択してから、発行されたログ を見つけます。

フローログに使用する Amazon S3 バケットの作成方法については、Amazon Simple Storage Service ユーザーガイドの「バケットの作成」を参照してください。

複数のアカウントログの詳細については、「AWS ソリューションライブラリの中央ロギング」を参照してください。

CloudWatch ログの詳細については、Amazon S3 に送信された CloudWatch ログ」を参照してください。

内容

フローログファイル

VPC フローログは、フローログレコードを収集し、ログファイルに統合してから、ログファイルを 5 分間隔で Amazon S3 バケットに発行する機能です。各ログファイルには、前の 5 分間に記録された IP トラフィックのフローログレコードが含まれています。

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

Amazon S3 では、フローログファイルの [最終更新日時] フィールドに、ファイルが Amazon S3 バケットにアップロードされた日時が表示されます。これは、ファイル名のタイムスタンプより後で、Amazon S3 バケットにファイルをアップロードするのにかかった時間によって異なります。

ログファイル形式

ログファイルに指定できる形式は次のとおりです。各ファイルは 1 つの Gzip ファイルに圧縮されます。

- [Text] - プレーンテキスト。これがデフォルトの形式です。
- [Parquet] - Apache Parquet は列指向データ形式です。Parquet 形式のデータに対するクエリは、プレーンテキストのデータに対するクエリに比べて 10 ~ 100 倍高速です。Gzip 圧縮を使用した Parquet 形式のデータは、Gzip 圧縮を使用したプレーンテキストよりもストレージスペースが 20% 少なくなります。

ログファイルオプション

オプションで、次のオプションを指定できます。

- [Hive-compatible S3 prefixes] - Hive 互換ツールにパーティションをインポートする代わりに、Hive 互換プレフィックスを有効にします。クエリを実行する前に、[MSCK REPAIR TABLE] コマンドを使用します。
- [Hourly partitions] - 大量のログがあり、通常は特定の時間にクエリをターゲットにしている場合、ログを時間単位で分割することで、より高速な結果が得られ、クエリコストを節約できます。

ログファイル S3 バケット構造

ログファイルでは、フローログの ID、リージョン、作成日、および送信先オプションに基づくフォルダ構造を使用して、指定された Amazon S3 バケットに保存されます。

デフォルトでは、ファイルは次の場所に配信されます。

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Hive 互換の S3 プレフィックスを有効にすると、ファイルは次の場所に配信されます。

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-region=region/year=year/month=month/day=day/
```

時間単位のパーティションを有効にすると、ファイルは次の場所に配信されます。

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

Hive 互換パーティションを有効にして 1 時間あたりのフローログをパーティション化すると、ファイルは次の場所に配信されます。

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-region=region/year=year/month=month/day=day/hour=hour/
```

ログファイル名

ログファイルのファイル名は、フローログ ID、リージョン、および作成日時に基づきます。ファイル名は、次の形式です。

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

以下は、us-east-1 リージョンで June 20, 2018 の 16:20 UTC に、リソースに対して AWS アカウント「123456789012」で作成されたフローログのログファイルの例です。ファイルには、終了時刻が 16:20:00 から 16:24:59 の間のフローログレコードが含まれます。

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

IAM Amazon S3 にフローログを発行するIAMプリンシパルの ポリシー Amazon S3

フローログを作成するIAMプリンシパルには、フローログを送信先 Amazon S3 バケットに発行するために必要な次のアクセス許可が必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
        ],
      "Resource": "*"
    }
  ]
}
```

フローログのための Amazon S3 バケットのアクセス許可

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

フローログを作成するユーザーがバケットを所有し、そのバケットに PutBucketPolicy および GetBucketPolicy 許可を持っている場合、次のポリシーが自動的にそのバケットにアタッチされます。このポリシーは、バケットにアタッチされている既存のポリシーを上書きします。

それ以外の場合は、バケット所有者が、フローログ作成者の AWS アカウント ID を指定して、このポリシーをバケットに追加しなければ、フローログの作成は失敗します。詳細については、Amazon Simple Storage Service ユーザーガイドのバケットポリシーの使用を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "my-s3-arn",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
```

```
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": ["s3:GetBucketAcl", "s3:ListBucket"],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        }
    ]
}
```

にARN指定する *my-s3-arn* は、Hive 互換の S3 プレフィックスを使用するかどうかによって異なります。

- デフォルトのプレフィックス

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- Hive 互換の S3 プレフィックス

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

ベストプラクティスとして、個々の ではなく、ログ配信サービスプリンシパルにこれらのアクセス許可を付与することをお勧めします AWS アカウント ARNs。また、aws:SourceAccount および aws:SourceArn 条件キーを使用して、混乱した使節の問題から保護することもベストプラクティスです。ソースアカウントはフローログの所有者であり、ソースARNはログサービスのワイルドカード (*) ARNです。

- で使用するために必要なキーポリシー SSEKMS

Amazon S3 バケット内のデータを保護するには、Amazon SS3-Managedキーによるサーバー側の暗号化 (SSE-S3) またはKMSキーによるサーバー側の暗号化 (-) のいずれかを有効にしますSSEKMS。詳細については、Amazon S3 ユーザーガイドの「サーバー側の暗号化を使用したデータの保護」をご参照ください。

SSE- ではKMS、 AWS マネージドキーまたはカスタマーマネージドキーを使用できます。 AWS マネージドキーでは、クロスアカウント配信を使用できません。フローログはログ配信アカウントから配信されるため、クロスアカウント配信のアクセス権を付与する必要があります。S3 バケットへのクロスアカウントアクセスを許可するには、カスタマーマネージドキーを使用し、バケット暗号化を有効にするときにカスタマーマネージドキーの Amazon リソースネーム (ARN) を指定します。詳細については、Amazon S3 ユーザーガイドの「AWS KMSによるサーバー側の暗号化の指定」をご参照ください。

カスタマーマネージドキーで SSE-KMS を使用する場合は、VPCフローログが S3 バケットに書き込めるように、キーのキーポリシーに (S3 バケットのバケットポリシーではなく) 以下を追加する必要があります。

```
{
    "Sid": "Allow Transit Gateway Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
   "Action": [
       "kms:Encrypt",
       "kms:Decrypt",
       "kms:ReEncrypt*",
       "kms:GenerateDataKey*",
       "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

Amazon S3 ログファイルのアクセス許可

必要なバケットポリシーに加えて、Amazon S3 はアクセスコントロールリスト (ACLs) を使用して、フローログによって作成されたログファイルへのアクセスを管理します。デフォルトでは、バ

ケット所有者が各ログファイルで FULL_CONTROL 許可を持ちます。ログ配信の所有者 (バケット所有者とは異なる場合) は、許可を持ちません。ログ配信アカウントには、READ および WRITE 許可があります。詳細については、Amazon Simple Storage Service ユーザーガイドの「アクセスコントロールリスト (ACL) の概要」を参照してください。

Amazon S3 の Transit Gateway Flow Logs ソースアカウントロールを作成する

ソースアカウントから、 AWS Identity and Access Management コンソールでソースロールを作成します。

ソースアカウントロールを作成するには

1. にサインイン AWS Management Console し、 でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. ナビゲーションペインで、ポリシー を選択します。
3. [ポリシーの作成] を選択します。
4. [ポリシーの作成] ページで、次の操作を行います。
   1. を選択しますJSON。
   2. このウィンドウのコンテンツを、このセクションの冒頭にあるアクセス許可ポリシーに置き換えてください。
   3. [次へ: タグ]、[次へ: 確認] の順に選択します。
   4. ポリシーの名前と説明 (省略可能) を入力し、[ポリシーの作成] を選択します。
5. ナビゲーションペインで [ロール] を選択します。
6. [Create role] を選択します。
7. [信頼されたエンティティのタイプ] には、[カスタム信頼ポリシー] を選択します。[カスタム信頼ポリシー] で、"Principal": {}, を次のように置き換え、ログ配信サービスを指定します。[Next (次へ)] を選択します。

   ```
   "Principal": {
      "Service": "delivery.logs.amazonaws.com"
   },
   ```

8. [Add permissions] (アクセス許可の追加) ページで、この手順で先ほど作成したポリシーの横にあるチェックボックスを選択し、[Next] (次へ) を選択します。
9. ロールの名前を入力し、オプションで説明を入力します。

10. [ロールの作成] を選択します。

Amazon S3 に発行する Transit Gateway フローログレコードを作成する

Amazon S3 バケットを作成して設定した後は、Transit Gateway のフローログを作成できます。

コンソールを使用して Amazon S3 に発行される Transit Gateway フローログを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Transit Gateways]、[Transit Gateway アタッチメント] の順に選択します。
3. 1 つまたは複数の Transit Gateway または Transit Gateway アタッチメントのチェックボックスを選択します。
4. [アクション]、[フローログの作成] を選択します。
5. フローログ設定を構成します。詳細については、「フローログ設定を構成するには」を参照してください。

コンソールを使用してフローログ設定を構成するには

1. [送信先] で、[S3 バケットへの送信] を選択します。
2. S3 バケット にはARN、既存の Amazon S3 バケットの Amazon リソースネーム (ARN) を指定します。 Amazon S3 オプションで、サブフォルダを含めることができます。例えば、 という名前のバケットmy-logsで という名前のサブフォルダを指定するにはmy-bucket、次の を使用しますARN。

   ```
   arn:aws::s3:::my-bucket/my-logs/
   ```

   AWSLogs は予約語であるため、バケットでサブフォルダ名として使用することはできません。

   バケットを所有している場合は、リソースポリシーが自動的に作成され、バケットにアタッチされます。詳細については、「フローログのための Amazon S3 バケットのアクセス許可」を参照してください。
3. [ログレコード形式] で、フローログレコードの形式を指定します。

   - デフォルトのフローログレコード形式を使用するには、[AWS のデフォルト形式] を選択します。

- カスタム形式を作成するには、[カスタム形式] を選択します。[ログの形式] で、フローログレコードに含めるフィールドを選択します。

4. [ログファイル形式] で、ログファイルの形式を指定します。

   - [Text] - プレーンテキスト。これがデフォルトの形式です。
   - [Parquet] - Apache Parquet は列指向データ形式です。Parquet 形式のデータに対するクエリは、プレーンテキストのデータに対するクエリに比べて 10 ~ 100 倍高速です。Gzip 圧縮を使用した Parquet 形式のデータは、Gzip 圧縮を使用したプレーンテキストよりもストレージスペースが 20% 少なくなります。

5. (オプション) Hive 互換の S3 プレフィックスを使用するには、[Hive-compatible S3 prefix]、[有効化] を選択します。
6. (オプション) 1 時間あたりのフローログを分割するには、[Every 1 hour (60 mins)] を選択します。
7. (オプション) フローログにタグを追加するには、[新しいタグを追加] を選択し、タグのキーと値を指定します。
8. [フローログの作成] を選択します。

コマンドラインツールを使用して Amazon S3 に発行されるフローログを作成するには

以下のいずれかのコマンドを使用します。

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs (Amazon EC2 クエリ API)

次の AWS CLI 例では、 のすべてのトランジットゲートウェイトラフィックをキャプチャするフローログを作成しVPCtgw-00112233344556677、フローログを という Amazon S3 バケットに配信しますflow-log-bucket。--log-format パラメータにより、フローログレコードのカスタム形式が指定されます。

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-00112233344556677 --log-destination-type s3 --log-destination arn:aws:s3:::flow-
log-bucket/my-custom-flow-logs/'
```

Amazon S3 で Transit Gateway フローログレコードを表示する

Amazon S3 に対して発行されたフローログレコードを表示するには

1. で Amazon S3 コンソールを開きますhttps://console.aws.amazon.com/s3/。
2. [バケット名] で、フローログを発行するバケットを選択します。
3. 名前 で、ログファイルの横にあるチェックボックスをオンにします。オブジェクトの概要パネルで、[ダウンロード] を選択します。

Amazon S3 で処理されたフローログレコード

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

Amazon Data Firehose の Transit Gateway フローログレコード

トピック

- クロスアカウント配信のための IAM ロール
- Amazon Data Firehose の Transit Gateway Flow Logs ソースアカウントロールを作成する
- Amazon Data Firehose の Transit Gateway Flow Logs 送信先アカウントロールを作成する
- Amazon Data Firehose に発行する Transit Gateway フローログレコードを作成する

フローログは、フローログデータを Firehose に直接発行できます。フローログの発行先は、リソースモニターと同じアカウント、または別のアカウントを選択できます。

前提条件

Firehose に発行する場合、フローログデータはプレーンテキスト形式で Firehose 配信ストリームに発行されます。まず、Firehose 配信ストリームを作成しておく必要があります。配信ストリームを作成する手順については、「Amazon Data Firehose デベロッパーガイド」の「Amazon Data Firehose 配信ストリームの作成」を参照してください。

料金表

標準の取り込み料金と配信料金が適用されます。詳細については、Amazon CloudWatch 料金表 を開き、ログ を選択して、提供されたログ を見つけます。

クロスアカウント配信のための IAM ロール

Kinesis Data Firehose に発行する場合、監視するリソースと同じアカウント (ソースアカウント) または別のアカウント (送信先アカウント) にある配信ストリームを選択できます。Firehose へのフローログのクロスアカウント配信を有効にするには、ソースアカウントに IAMロールを作成し、宛先アカウントに IAMロールを作成する必要があります。

ロール

- ソースアカウントロール
- 送信先アカウントロール

ソースアカウントロール

ソースアカウントで、次のアクセス許可を付与するロールを作成します。この例のロールの名前は mySourceRole ですが、このロールには別の名前を選択できます。最後のステートメントにより、送信先アカウントのロールがこのロールを引き受けることができるようになります。条件ステートメントにより、このロールは指定されたリソースを監視する場合に限り、ログ配信サービスだけに渡されます。ポリシーを作成するときは、 条件キー を使用してモニタリングする 、VPCsネットワークインターフェイス、またはサブネットを指定しますiam:AssociatedResourceARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
          "StringEquals": {
              "iam:PassedToService": "delivery.logs.amazonaws.com"
          },
          "StringLike": {
              "iam:AssociatedResourceARN": [
                  "arn:aws:ec2:region:source-account:transit-gateway/
tgw-0fb8421e2da853bf"
              ]
          }
      }
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
          "logs:CreateLogDelivery",
          "logs:DeleteLogDelivery",
          "logs:ListLogDeliveries",
          "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}
```

このロールに以下の信頼ポリシーがあることを確認します。これにより、ログ配信サービスがロールを引き受けることができます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

送信先アカウントロール

送信先アカウントで、 で始まる名前のロールを作成しますAWSLogDeliveryFirehoseCrossAccountRole。このロールには、以下のアクセス許可が必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

このロールに次の信頼ポリシーがあることを確認します。これにより、ソースアカウントで作成したロールがこのロールを引き受けることができます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Amazon Data Firehose の Transit Gateway Flow Logs ソースアカウントロールを作成する

ソースアカウントから、 AWS Identity and Access Management コンソールでソースロールを作成します。

ソースアカウントロールを作成するには

1. にサインイン AWS Management Console し、 でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. ナビゲーションペインで、ポリシー を選択します。
3. [ポリシーの作成] を選択します。
4. [ポリシーの作成] ページで、次の操作を行います。

1. を選択しますJSON。
2. このウィンドウのコンテンツを、このセクションの冒頭にあるアクセス許可ポリシーに置き換えてください。
3. [次へ: タグ]、[次へ: 確認] の順に選択します。
4. ポリシーの名前と説明 (省略可能) を入力し、[ポリシーの作成] を選択します。

5. ナビゲーションペインで [ロール] を選択します。
6. [Create role] を選択します。
7. [信頼されたエンティティのタイプ] には、[カスタム信頼ポリシー] を選択します。[カスタム信頼ポリシー] で、`"Principal": {},` を次のように置き換え、ログ配信サービスを指定します。[Next (次へ)] を選択します。

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. [Add permissions] (アクセス許可の追加) ページで、この手順で先ほど作成したポリシーの横にあるチェックボックスを選択し、[Next] (次へ) を選択します。
9. ロールの名前を入力し、オプションで説明を入力します。
10. [ロールの作成] を選択します。

Amazon Data Firehose の Transit Gateway Flow Logs 送信先アカウントロールを作成する

送信先アカウントから、 AWS Identity and Access Management コンソールで送信先ロールを作成します。

送信先アカウントロールを作成するには

1. にサインイン AWS Management Console し、 でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
2. ナビゲーションペインで、ポリシー を選択します。
3. [ポリシーの作成] を選択します。
4. [ポリシーの作成] ページで、次の操作を行います。

    1. を選択しますJSON。

2. このウィンドウのコンテンツを、このセクションの冒頭にあるアクセス許可ポリシーに置き換えてください。
3. [次へ: タグ]、[次へ: 確認] の順に選択します。
4. で始まるポリシーの名前を入力しAWSLogDeliveryFirehoseCrossAccountRole、ポリシーの作成 を選択します。

5. ナビゲーションペインで [ロール] を選択します。
6. [Create role] を選択します。
7. [信頼されたエンティティのタイプ] には、[カスタム信頼ポリシー] を選択します。[カスタム信頼ポリシー] で、`"Principal": {},` を次のように置き換え、ログ配信サービスを指定します。[Next (次へ)] を選択します。

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. [Add permissions] (アクセス許可の追加) ページで、この手順で先ほど作成したポリシーの横にあるチェックボックスを選択し、[Next] (次へ) を選択します。
9. ロールの名前を入力し、オプションで説明を入力します。
10. [ロールの作成] を選択します。

Amazon Data Firehose に発行する Transit Gateway フローログレコードを作成する

コンソールを使用して Firehose に発行する Transit Gateway フローログを作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Transit Gateways]、[Transit Gateway アタッチメント] の順に選択します。
3. 1 つまたは複数の Transit Gateway または Transit Gateway アタッチメントのチェックボックスを選択します。
4. [アクション]、[フローログの作成] を選択します。
5. [送信先] には、[Firehose 配信システム] への送信を選択します。
6. Firehose 配信ストリーム ARNで、フローログを発行する配信ARNストリームの を選択します。
7. [ログレコード形式] で、フローログレコードの形式を指定します。

- デフォルトのフローログレコード形式を使用するには、[AWS のデフォルト形式] を選択します。
- カスタム形式を作成するには、[カスタム形式] を選択します。[ログの形式] で、フローログレコードに含めるフィールドを選択します。

8. (オプション) フローログにタグを追加するには、[新しいタグを追加] を選択し、タグのキーと値を指定します。
9. [フローログの作成] を選択します。

コマンドラインツールを使用して Firehose に発行するフローログを作成するには

以下のいずれかのコマンドを使用します。

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs (Amazon EC2 クエリ API)

次の AWS CLI例では、トランジットゲートウェイ情報をキャプチャするフローログを作成し、指定された Firehose 配信ストリームにフローログを配信します。

```
aws ec2 create-flow-logs \
                --resource-type TransitGateway \
                --resource-ids tgw-1a2b3c4d \
                --log-destination-type kinesis-data-firehose \
                --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream
```

次の AWS CLI例では、トランジットゲートウェイ情報をキャプチャするフローログを作成し、フローログをソースアカウントとは異なる Firehose 配信ストリームに配信します。

```
aws ec2 create-flow-logs  \
  --resource-type TransitGateway \
  --resource-ids gw-1a2b3c4d \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
```

```
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

Amazon VPC Transit Gateway フローログを作成する

データを CloudWatch Logs、Amazon S3、または Amazon Data Firehose に発行できるトランジットゲートウェイのフローログを作成できます。

詳細については、次を参照してください。

- に発行する Transit Gateways フローログレコードを作成する Amazon CloudWatch Logs
- Amazon S3 に発行する Transit Gateway フローログレコードを作成する
- Amazon Data Firehose に発行する Transit Gateway フローログレコードを作成する

APIs または を使用して Amazon VPC Transit Gateways フローログを作成および管理する CLI

このページで説明されているタスクは、 APIまたは コマンドラインを使用して実行できます。

`CreateFlowLogs` API または を使用する場合、次の制限が適用されます`create-flow-logs`CLI。

- `--resource-ids` の最大制約は、`TransitGateway` または `TransitGatewayAttachment` リソースタイプが 25 です。
- `--traffic-type` はデフォルトでは必須フィールドではありません。これを Transit Gateway リソースタイプに指定すると、エラーが返されます。この制限は Transit Gateway リソースタイプにのみ適用されます。
- `--max-aggregation-interval` には、`60` のデフォルトの値があります。これは、Transit Gateway リソースタイプで唯一受け入れられる値です。他の値を渡そうとすると、エラーが返されます。この制限は Transit Gateway リソースタイプにのみ適用されます。
- `--resource-type` で、`TransitGateway` と `TransitGatewayAttachment` の 2 つの新しいリソースタイプがサポートされています。
- 含めるフィールドを設定しない場合、`--log-format` には Transit Gateway リソースタイプのすべてのログフィールドが含まれます。これは、Transit Gateway リソースタイプにのみ適用されます。

フローログの作成

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)
- CreateFlowLogs (Amazon EC2 クエリ API)

フローログの説明

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)
- DescribeFlowLogs (Amazon EC2 クエリ API)

フローログレコード (ログイベント) の表示

- get-log-events (AWS CLI)
- Get-CWLLogEvent (AWS Tools for Windows PowerShell)
- GetLogEvents (CloudWatch API)

フローログの削除

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlowLogs (Amazon EC2 クエリ API)

Amazon VPC Transit Gateways フローログレコードを表示する

Amazon 経由でトランジットゲートウェイフローログに関する情報を表示しますVPC。リソースを選択すると、そのリソースのすべてのフローログが一覧表示されます。表示される情報には、フローログの ID、フローログの設定、およびフローログのステータスに関する情報が含まれます。

Transit Gateway のフローログに関する情報を表示するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Transit Gateways]、[Transit Gateway アタッチメント] の順に選択します。

3. Transit Gateway または Transit Gateway アタッチメントを選択し、[フローログの削除] を選択します。フローログに関する情報がタブに表示されます。[送信先タイプ] 列は、フローログを発行する送信先を示します。

Amazon VPC Transit Gateway フローログタグの管理

Amazon EC2および Amazon VPCコンソールで、フローログのタグを追加または削除できます。

Transit Gateway フローログのタグを追加または削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Transit Gateways]、[Transit Gateway アタッチメント] の順に選択します。
3. Transit Gateway または Transit Gateway アタッチメントを選択します。
4. 必要なフローログの [タグの管理] を選択します。
5. 新しいタグを追加するには、[タグの作成] を選択します。タグを削除するには、削除アイコンを選択します (x)。
6. [Save] を選択します。

Amazon VPC Transit Gateways フローログレコードの検索

Logs コンソールを使用して、 CloudWatch ログに発行されるフロー CloudWatch ログレコードを検索できます。メトリクスフィルターを使用すると、フローログレコードをフィルタリングできます。フローログレコードはスペースで区切られます。

Logs コンソールを使用してフロー CloudWatch ログレコードを検索するには

1. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
2. ナビゲーションペインで、[ログ]、[ロググループ] の順に選択します。
3. フローログを含むロググループを選択します。各 Transit Gateway のログストリームのリストが表示されます。
4. 検索する Transit Gateway がわかっている場合は、個々のログストリームを選択します。または、[ロググループの検索] を選択して、ロググループ全体を検索します。ロググループに多数の Transit Gateway がある場合、または選択した時間範囲によっては、この処理に時間がかかる場合があります。

5. [イベントをフィルター] で、次の文字列を入力します。これは、フローログレコードで デフォルトの形式が使用されていることを前提としています。

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport,
 protocol, packets, bytes,start,end, log_status, type,packets_lost_no_route,
 packets_lost_blackhole, packets_lost_mtu_exceeded, packets_lost_ttl_expired,
 tcp_flags,region, flow_direction, pkt_src_aws_service, pkt_dst_aws_service]
```

6. 必要に応じてフィールドの値を指定して、フィルターを変更します。次の例では、特定の送信元 IP アドレスでフィルタリングします。

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.0.1, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.2.*, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

次の例では、Transit Gateway ID tgw-123abc456bca、宛先ポート、およびバイト数でフィルタリングします。

```
[version, resource_type, account_id,tgw_id=tgw-123abc456bca, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport =
 80 || dstport = 8080, protocol, packets, bytes >= 500,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
```

```
packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
pkt_dst_aws_service]
```

Amazon VPC Transit Gateways フローログレコードを削除する

Amazon VPCコンソールを使用して、トランジットゲートウェイフローログを削除できます。

これらの手順では、リソースのフローログサービスが無効になります。フローログを削除しても、Amazon S3 の CloudWatch ログまたはログファイルから既存のログストリームは削除されません。既存のフローログデータは、それぞれのサービスのコンソールを使用して削除する必要があります。さらに、 が Amazon S3 に発行するフローログを削除しても、バケットポリシーとログファイルのアクセスコントロールリスト () は削除されませんACLs。

Transit Gateway のフローログを削除するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで、[Transit Gateway] を選択します。
3. [Transit Gateway ID] を選択します。
4. [フローログ] セクションで、削除するフローログを選択します。
5. [アクション] を選択してから、[フローログの削除] を選択します。
6. [削除] を選択してフローを削除することを確認します。

Amazon VPC Transit Gateway を使用してトランジットゲートウェイをモニタリングする

Transit Gateway をモニタリングするには、次の機能を使用して、トラフィックパターンの分析や Transit Gateway のトラブルシューティングを行います。

CloudWatch メトリクス

Amazon を使用して CloudWatch 、トランジットゲートウェイのデータポイントに関する統計を、メトリクス と呼ばれる時系列データの順序付けられた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、「CloudWatch Amazon VPC Transit Gateway の メトリクス」を参照してください。

Transit Gateway Flow Logs

Transit Gateway Flow Logs を使用して、Transit Gateway のネットワーク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、「Transit Gateway Flow Logs 」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、トランジットゲートウェイにアタッチされている との間で送受信 VPCsされるトラフィックに関する詳細情報をキャプチャできます。詳細については、「Amazon VPCユーザーガイドVPC」の「フローログ」を参照してください。

CloudTrail ログ

を使用して AWS CloudTrail 、トランジットゲートウェイ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API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、どの呼び出しが行われたか、呼び出し元の送信元 IP アドレス、呼び出し者、呼び出し日時などを判断できます。詳細については、「Amazon VPC Transit Gateways が をAPI呼び出す AWS CloudTrail」を参照してください。

CloudWatch Network Manager を使用したイベント

を使用してイベント AWS Network Manager を に転送し CloudWatch、それらのイベントをターゲット関数またはストリームにルーティングできます。Network Manager は、トポロジーの変更、ルーティングの更新、ステータスの更新に関するイベントを生成します。これらはすべて、Transit Ggateway の変更を確認するために使用できます。詳細については、「Global Networks for Transit Gateways ユーザーガイド」の CloudWatch 「イベントによるグローバルネットワークのモニタリング」を参照してください。 AWS

CloudWatch Amazon VPC Transit Gateway の メトリクス

Amazon VPC は、トランジットゲートウェイとトランジットゲートウェイアタッチメントのデータポイントを Amazon に発行 CloudWatch します。 CloudWatch を使用すると、これらのデータポイントに関する統計を、メトリクス と呼ばれる時系列データの順序付けられた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。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、指定したメトリクスをモニタリングする CloudWatch アラームを作成し、メトリクスが許容範囲外になった場合にアクション (E メールアドレスへの通知の送信など) を開始できます。

Amazon はメトリクスVPCを測定し、60 秒間隔で CloudWatch に送信します。

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

内容

Transit Gateway メトリクス

AWS/TransitGateway 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
BytesDropCountBlackhole	blackhole ルートと一致したためにドロップされたバイトの数。
BytesDropCountNoRoute	ルートと一致しなかったためにドロップされたバイトの数。
BytesIn	Transit Gateway あたりの受信バイト数。
BytesOut	Transit Gateway からの送信バイト数。
PacketsIn	Transit Gateway によって受信されたパケットの数。

メトリクス	説明
PacketsOut	Transit Gateway によって送信されたパケットの数。
PacketDropCountBlackhole	blackhole ルートと一致したためにドロップされたパケットの数。
PacketDropCountNoRoute	ルートと一致しなかったためにドロップされたパケットの数。

アタッチメントレベルのメトリクス

Transit Gateway アタッチメントでは、次のメトリクスを使用できます。すべてのアタッチメントメトリクスは、Transit Gateway 所有者のアカウントに発行されます。すべてのアタッチメントメトリクスは、 所有者のアカウントに公開されます。アタッチメントの所有者は、自分のアタッチメントのメトリクスのみを表示できます。サポートされているアタッチメントタイプの詳細については、「the section called “リソースアタッチメント”」を参照してください。

メトリクス	説明
BytesDropCountBlackhole	Transit Gateway アタッチメント上の blackhole ルートに一致したためにドロップされたバイトの数。
BytesDropCountNoRoute	Transit Gateway アタッチメント上のルートと一致しなかったためにドロップされたバイトの数。
BytesIn	Transit Gateway によってアタッチメントから受信されたバイト数。
BytesOut	Transit Gateway からアタッチメントに送信されたバイト数。
PacketsIn	Transit Gateway によってアタッチメントから受信されたパケット数。
PacketsOut	Transit Gateway によってアタッチメントに送信されたパケットの数。
PacketDropCountBlackhole	Transit Gateway アタッチメント上の blackhole ルートに一致したためにドロップされたパケットの数。

メトリクス	説明
PacketDropCountNoRoute	Transit Gateway アタッチメント上のルートと一致しなかったためにドロップされたパケットの数。

Transit Gateway のメトリクスディメンション

Transit Gateway のメトリクスをフィルタリングするには、次のディメンションを使用します。

ディメンション	説明
TransitGateway	Transit Gateway によってメトリクスデータをフィルタリングします。
TransitGatewayAttachment	Transit Gateway アタッチメントによってメトリクスデータをフィルタリングします。

Amazon VPC Transit Gateways が をAPI呼び出す AWS CloudTrail

AWS CloudTrail は、ユーザー、ロール、または AWS のサービスによって実行されたアクションを記録するサービスです。 は、すべての Transit Gateway API呼び出しをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、 からの呼び出し AWS Management Console と、トランジットゲートウェイAPIオペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、トランジットゲートウェイの CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴 で最新のイベントを表示できます。によって収集された情報を使用して CloudTrail、トランジットゲートウェイ に対して行われたリクエストAPI、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

トランジットゲートウェイ の詳細についてはAPIs、「Amazon EC2APIリファレンス」のAWS 「トランジットゲートウェイアクション」を参照してください。

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

のトランジットゲートウェイ情報 CloudTrail

CloudTrail AWS アカウントを作成すると、 がアカウントで有効になります。トランジットゲートウェイ を介してアクティビティが発生するとAPI、そのアクティビティは CloudTrail イベント履歴の他の AWS サービスイベントとともにイベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「イベント履歴を使用した CloudTrail イベントの表示」を参照してください。

トランジットゲートウェイ 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API、証跡を作成します。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、すべての リージョンに証跡が適用されます。証跡は、 AWS パーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、 CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように、他の AWS サービスを設定できます。詳細については、AWS CloudTrail ユーザーガイドで次を参照してください。

- 証跡の作成のための概要
- CloudTrail サポートされているサービスと統合
- の Amazon SNS Notifications の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

Transit Gateway アクションへのすべての呼び出しは、 によってログに記録されます CloudTrail。例えば、 `CreateTransitGateway`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、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストがルート認証情報と AWS Identity and Access Management ユーザー認証情報のどちらを使用して行われたか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

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

Transit Gateway のログファイルエントリを理解する

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ようにする設定です。 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。イベントは任意のソース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、リクエストパラメータ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。

ログファイルには、トランジットゲートウェイAPI呼び出しだけでなく、 AWS アカウントのすべてのAPI呼び出しのイベントが含まれます。トランジットゲートウェイへの呼び出しは、値 を持つeventSource要素をチェックAPIすることで見つけることができますec2.amazonaws.com。CreateTransitGateway 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。

コンソールを使用してトランジットゲートウェイAPIを作成したユーザーのトランジットゲートウェイの CloudTrail ログレコードの例を次に示します。userAgent 要素を使用してコンソールを特定できます。リクエストされたAPI呼び出しは、 eventName要素を使用して識別できます。ユーザーに関する情報 (Alice) は userIdentity 要素で確認できます。

Example 例： CreateTransitGateway

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2018-11-15T05:25:50Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateTransitGateway",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.ec2.amazonaws.com",
    "requestParameters": {
        "CreateTransitGatewayRequest": {
            "Options": {
                "DefaultRouteTablePropagation": "enable",
                "AutoAcceptSharedAttachments": "disable",
```

```
                "DefaultRouteTableAssociation": "enable",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable"
            },
            "TagSpecification": {
                "ResourceType": "transit-gateway",
                "tag": 1,
                "Tag": {
                    "Value": "my-tgw",
                    "tag": 1,
                    "Key": "Name"
                }
            }
        }
    },
    "responseElements": {
        "CreateTransitGatewayResponse": {
            "xmlns": "http://ec2.amazonaws.com/doc/2016-11-15/",
            "requestId": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
            "transitGateway": {
                "tagSet": {
                    "item": {
                        "value": "my-tgw",
                        "key": "Name"
                    }
                },
                "creationTime": "2018-11-15T05:25:50.000Z",
                "transitGatewayId": "tgw-0a13743bd6c1f5fcb",
                "options": {
                    "propagationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a",
                    "amazonSideAsn": 64512,
                    "defaultRouteTablePropagation": "enable",
                    "vpnEcmpSupport": "enable",
                    "autoAcceptSharedAttachments": "disable",
                    "defaultRouteTableAssociation": "enable",
                    "dnsSupport": "enable",
                    "associationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a"
                },
                "state": "pending",
                "ownerId": 123456789012
            }
        }
    },
    "requestID": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
```

```
    "eventID": "e8fa575f-4964-4ab9-8ca4-6b5b4EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Amazon VPC Transit Gateway での Identity and Access Management

AWS は、セキュリティ認証情報を使用してユーザーを識別し、 AWS リソースへのアクセスを許可します。 AWS Identity and Access Management （ IAM) の機能を使用すると、他のユーザー、サービス、およびアプリケーションが、セキュリティ認証情報を共有せずに、 AWS リソースを完全または限定的な方法で使用できるようになります。

デフォルトでは、IAMユーザーには AWS リソースを作成、表示、または変更するアクセス許可はありません。ユーザーがトランジットゲートウェイなどのリソースにアクセスしたり、タスクを実行したりできるようにするには、必要な特定のリソースとAPIアクションを使用するアクセス許可をユーザーに付与する IAMポリシーを作成し、そのユーザーが属するグループにポリシーをアタッチする必要があります。ポリシーをユーザーまたはユーザーのグループにアタッチする場合、ポリシーによって特定リソースの特定タスクを実行するユーザーの権限が許可または拒否されます。

トランジットゲートウェイを使用するには、次のいずれかの AWS マネージドポリシーがニーズを満たす場合があります。

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

Transit Gateway を管理するためのポリシー例

トランジットゲートウェイを使用するためのIAMポリシーの例を次に示します。

必要なタグを持つ Transit Gateway を作成する

以下の例で、ユーザーは Transit Gateway を作成できるようになります。`aws:RequestTag` 条件キーでは、ユーザーは Transit Gateway をタグ `stack=prod` にタグ付けすることが求められます。`aws:TagKeys` 条件キーは、`ForAllValues` 修飾子を使用し、キー `stack` のみがリクエストで許可されることを指定します (他のタグは指定できません) 。ユーザーが Transit Gateway の作成時にこの指定のタグを渡さない場合、またはタグを指定しない場合、リクエストは却下されます。

2 番目のステートメントは、`ec2:CreateAction` 条件キーを使用して、ユーザーが `CreateTransitGateway` のコンテキストでみタグを使用できるようにします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedTGWs",
            "Effect": "Allow",
            "Action": "ec2:CreateTransitGateway",
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stack": "prod"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "stack"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateTransitGateway"
                }
            }
        }
    ]
}
```

Transit Gateway ルートテーブルの操作

以下の例では、ユーザーが特定の Transit Gateway のみ（`tgw-11223344556677889`）に対して Transit Gateway ルートテーブルを作成および削除できるようにします。ユーザーは、任意の Transit Gateway のルートテーブルでルートの作成や置き換えができますが、タグ `network=new-york-office` の付いたアタッチメントに対してのみ可能です。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayRouteTable"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:transit-gateway/tgw-11223344556677889",
                "arn:aws:ec2:*:*:transit-gateway-route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-attachment/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/network": "new-york-office"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-route-table/*"
        }
    ]
}
```

Amazon VPC Transit Gateway でトランジットゲートウェイのサービスにリンクされたロールを使用する

Amazon VPCは、ユーザーに代わって他の AWS のサービスを呼び出すために必要なアクセス許可に、サービスにリンクされたロールを使用します。詳細については、「 ユーザーガイド」の「サービスにリンクされたロールの使用IAM」を参照してください。

Transit Gateway サービスにリンクされたロール

Amazon VPCは、トランジットゲートウェイを使用するときに、ユーザーに代わって他の AWS サービスを呼び出すために必要なアクセス許可として、サービスにリンクされたロールを使用します。

サービスにリンクされたロールによって付与されるアクセス許可

Amazon VPCは、トランジットゲートウェイを操作するときに、 という名前のサービスにリンクされたロールAWSServiceRoleForVPCTransitGatewayを使用して、ユーザーに代わって次のアクションを呼び出します。

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:AssignIpv6Addresses`
- `ec2:UnAssignIpv6Addresses`

AWSServiceRoleForVPCTransitGateway ロールは、次のサービスを信頼してロールを引き受けます。

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGateway は マネージドポリシー を使用しますAWSVPCTransitGatewayServiceRolePolicy。

IAM エンティティ (ユーザー、グループ、ロールなど) がサービスにリンクされたロールを作成、編集、または削除できるようにするには、アクセス許可を設定する必要があります。詳細について

は、「 ユーザーガイド」の「サービスにリンクされたロールのアクセス許可IAM」を参照してください。

サービスにリンクされたロールの作成

AWSServiceRoleForVPCTransitGateway ロールを手動で作成する必要はありません。Amazon VPC は、アカウントVPC内の をトランジットゲートウェイにアタッチするときに、このロールを作成します。

Amazon がユーザーに代わってサービスにリンクされたロールVPCを作成するには、必要なアクセス許可が必要です。詳細については、「 ユーザーガイド」の「サービスにリンクされたロールのアクセス許可IAM」を参照してください。

サービスにリンクされたロールを編集する

AWSServiceRoleForVPCTransitGateway を使用して の説明を編集できますIAM。詳細については、「 IAMユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

サービスにリンクされたロールを削除する

トランジットゲートウェイを使用する必要がなくなった場合は、 を削除することをお勧めしますAWSServiceRoleForVPCTransitGateway。

このサービスにリンクされたロールは、 AWS アカウント内のすべての Transit Gateway VPCアタッチメントを削除した後にのみ削除できます。これにより、VPC添付ファイルへのアクセス許可を誤って削除することがなくなります。

IAM コンソール、、または IAM を使用してCLI、サービスにリンクされたロールIAMAPIを削除できます。詳細については、「 ユーザーガイド」の「サービスにリンクされたロールの削除IAM」を参照してください。

アカウント内の をトランジットゲートウェイVPCにアタッチするとAWSServiceRoleForVPCTransitGateway、 を削除すると、Amazon によってロールが再度VPC作成されます。

AWS Amazon Transit Gateway のトランジットゲートウェイの VPC マネージドポリシー

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) が更新されます。 AWS サービス は、新しい AWS が起動されたとき、または既存のサービスで新しいAPIオペレーションが使用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については、「 ユーザーガイド」の「 AWS 管理ポリシーIAM」を参照してください。

トランジットゲートウェイを使用するには、次のいずれかの AWS マネージドポリシーがニーズを満たす場合があります。

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS マネージドポリシー： AWSVPCTransitGatewayServiceRolePolicy

このポリシーはロール にアタッチされますAWSServiceRoleForVPCTransitGateway。これにより、Amazon VPC はトランジットゲートウェイアタッチメントのリソースを作成および管理できます。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSVPCTransitGatewayServiceRolePolicy」の「」を参照してください。 AWS

AWS 管理ポリシーへのトランジットゲートウェイの更新

Amazon が 2021 年 3 月にこれらの変更の追跡VPCを開始した以降の、トランジットゲートウェイの AWS マネージドポリシーの更新に関する詳細を表示します。

変更	説明	日付
Amazon が変更の追跡VPCを開始しました	Amazon が AWS マネージドポリシーの変更の追跡VPCを開始しました。	2021 年 3 月 1 日

Amazon VPC Transit Gateway のACLsトランジットゲートウェイ用のネットワーク

ネットワークアクセスコントロールリスト (NACL) は、オプションのセキュリティレイヤーです。

ネットワークアクセスコントロールリスト (NACL) ルールは、シナリオに応じて異なる方法で適用されます。

- the section called “EC2 インスタンスとトランジットゲートウェイの関連付けに同じサブネット”
- the section called “EC2 インスタンスとトランジットゲートウェイの関連付け用の異なるサブネット”

EC2 インスタンスとトランジットゲートウェイの関連付けに同じサブネット

同じサブネットにEC2インスタンスとトランジットゲートウェイの関連付けがある設定を考えてみましょう。EC2 インスタンスからトランジットゲートウェイへのトラフィックと、トランジットゲートウェイからインスタンスへのトラフィックの両方に同じネットワークACLが使用されます。

NACL ルールは、インスタンスからトランジットゲートウェイへのトラフィックに次のように適用されます。

- アウトバウンドルールでは、評価に送信先 IP アドレスを使用します。
- インバウンドルールでは、評価に送信元 IP アドレスを使用します。

NACL ルールは、トランジットゲートウェイからインスタンスへのトラフィックに次のように適用されます。

- アウトバウンドルールは評価されません。
- インバウンドルールは評価されません。

EC2 インスタンスとトランジットゲートウェイの関連付け用の異なるサブネット

あるサブネットにEC2インスタンスがあり、別のサブネットにトランジットゲートウェイの関連付けがあり、各サブネットが異なるネットワーク に関連付けられている設定を考えてみましょうACL。

ネットワークACLルールは、EC2インスタンスサブネットに次のように適用されます。

- アウトバウンドルールでは、送信先 IP アドレスを使用して、インスタンスから Transit Gateway へのトラフィックを評価します。
- インバウンドルールでは、送信元 IP アドレスを使用して、Transit Gateway からインスタンスへのトラフィックを評価します。

NACL ルールは、トランジットゲートウェイサブネットに次のように適用されます。

- アウトバウンドルールでは、送信先 IP アドレスを使用して、Transit Gateway からインスタンスへのトラフィックを評価します。
- アウトバウンドルールは、インスタンスから Transit Gateway へのトラフィックの評価には使用されません。
- インバウンドルールでは、送信元 IP アドレスを使用して、インスタンスから Transit Gateway へのトラフィックを評価します。
- インバウンドルールは、Transit Gateway からインスタンスへのトラフィックの評価には使用されません。

ベストプラクティス

トランジットゲートウェイVPCアタッチメントごとに個別のサブネットを使用します。サブネットごとに、/28 CIDRなどの小さな を使用して、EC2リソースのアドレスを増やします。別のサブネットを使用する場合は、次の項目を設定できます:

- トランジットゲートウェイサブネットNACLに関連付けられているインバウンドとアウトバウンドを開いたままにします。
- トラフィックフローに応じて、ワークロードサブネットNACLsに適用できます。

VPC アタッチメントの仕組みの詳細については、「」を参照してくださいthe section called “リソースアタッチメント”。

Amazon VPC Transit Gateway のクォータ

には、トランジットゲートウェイに関連する次のクォータ (以前 AWS アカウント は制限 と呼ばれていました) 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。

Service Quotas コンソールには、アカウントのクォータに関する情報が表示されます。Service Quotas コンソールを使用して、デフォルトのサービスクォータを表示したり、調整可能なクォータのクォータの引き上げをリクエストしたりすることができます。詳細については、「Service Quotas ユーザーガイド」の「クォータ引き上げのリクエスト」を参照してください。

調整可能なクォータが Service Quotas でまだ使用できる状態になっていない場合は、サポートケースを開くことができます。

全般

名前	デフォルト	引き上げ可能
アカウントあたりの Transit Gateway	5	はい
CIDR トランジットゲートウェイあたりの ブロック	5	なし

CIDR ブロックは the section called “Connect アタッチメントおよび Connect ピア”機能で使用されます。

ルーティング

名前	デフォルト	引き上げ可能
Transit Gateway あたりの Transit Gateway ルートテーブル	20	はい
1 つの Transit Gateway のすべてのルートテーブルにわたるすべてのルート (動的ルートと静的ルート) の合計数	10,000	はい

名前	デフォルト	引き上げ可能
仮想ルーターアプライアンスから Connect ピアにアドバタイズされるダイナミックルート	1,000	あり
Transit Gateway 上の Connect ピアから仮想ルーターアプライアンスへのアドバタイズされたルート	5,000	いいえ
単一のアタッチメントへのプレフィックスの静的ルートの数	1	いいえ

アドバタイズされたルートは、接続 アタッチメントに関連付けられているルートテーブルから取得されます。

Transit Gateway アタッチメント

トランジットゲートウェイは、同じ に複数のVPCアタッチメントを持つことはできませんVPC。

名前	デフォルト	引き上げ可能
Transit Gateway あたりのアタッチメント	5,000	なし
あたりのトランジットゲートウェイ VPC	5	いいえ
Transit Gateway あたりのピアアタッチメント	50	はい
Transit Gateway あたりの保留中のピアリングアタッチメント	10	はい
2 つのトランジットゲートウェイ間、または 1 つのトランジットゲートウェイと クラウド WANコアネットワークエッジ間のピアリングアタッチメント (CNE)	1	なし
Connect アタッチメントあたりの Connect ピア (GRE トンネル)	4	なし

[帯域幅]

Site-to-Site VPN接続を通じて実現される帯域幅に影響を与える要因は多数あります。これには、パケットサイズ、トラフィックミックス (TCP/UDP) 、中間ネットワーク上のシェーピングポリシーまたはスロットリングポリシー、インターネットの気象状況、特定のアプリケーション要件が含まれますが、これらに限定されません。VPC アタッチメント、 AWS Direct Connect ゲートウェイ、またはピアリング接続されたトランジットゲートウェイアタッチメントの場合、デフォルト値を超える追加の帯域幅を提供しようとします。

名前	デフォルト	引き上げ可能
アベイラビリティーゾーンあたりのVPCアタッチメントあたりの帯域幅	最大 100 Gbps	詳細については、ソリューションアーキテクト (SA) またはテクニカルアカウントマネージャー (TAM) にお問い合わせください。
アベイラビリティーゾーンあたりのトランジットゲートウェイVPCアタッチメントあたりの 1 秒あたりのパケット数	最大 7,500,000	詳細については、ソリューションアーキテクト (SA) またはテクニカルアカウントマネージャー (TAM) にお問い合わせください。
リージョン内の利用可能なアベイラビリティーゾーンあたりの AWS Direct Connect ゲートウェイまたはピア接続の帯域幅	最大 100 Gbps	詳細については、ソリューションアーキテクト (SA) またはテクニカルアカウントマネージャー (TAM) にお問い合わせください。
リージョン内の利用可能なアベイラビリティーゾーンごとのトランジットゲートウェイアタッチメント (AWS Direct Connect およびピアリ	最大 7,500,000	詳細については、ソリューションアーキテクト (SA) またはテ

名前	デフォルト	引き上げ可能
ングアタッチメント) あたりの 1 秒あたりのパケット数		クニカルアカウントマネージャー (TAM) にお問い合わせください。
VPN トンネルあたりの最大帯域幅	最大 1.25 Gbps	なし
VPN トンネルあたりの 1 秒あたりの最大パケット数	最大 140,000	なし
Connect アタッチメントあたりの Connect ピア (GRE トンネル) あたりの最大帯域幅	最大 5 Gbps	いいえ
Connect ピアあたりの 1 秒あたりの最大パケット数	最大 300,000	なし

同一コストのマルチパスルーティング (ECMP) を使用すると、複数のVPNトンネルを集約することでVPN帯域幅を増やすことができます。を使用するにはECMP、動的ルーティング用にVPN接続を設定する必要があります。ECMP は、静的ルーティングを使用するVPN接続ではサポートされていません。

基盤となるトランスポート (または) アタッチメントが必要な帯域幅をサポートしている限り、Connect アタッチメントごとに最大 4 つの Connect ピアを作成できます (VPCConnect アタッチメントごとに最大 20 Gbps の合計帯域幅 AWS Direct Connect) 。を使用してECMP、同じ Connect アタッチメントの複数の Connect ピア間、または同じトランジットゲートウェイ上の複数の Connect アタッチメント間で水平にスケーリングすることで、より高い帯域幅を得ることができます。トランジットゲートウェイは、同じ Connect BGPピアのピアリングECMP間で を使用することはできません。

AWS Direct Connect ゲートウェイ

名前	デフォルト	引き上げ可能
AWS Direct Connect トランジットゲートウェイあたりのゲートウェイ	20	なし

名前	デフォルト	引き上げ可能
ゲートウェイあたりのトランジット AWS Direct Connect ゲートウェイ	6	なし

最大送信単位 (MTU)

- ネットワーク接続MTUの は、接続を介して渡すことができる最大許容パケットのサイズをバイト単位で表したものです。接続MTUの が大きいほど、1 つのパケットで渡すことができるデータが多くなります。トランジットゲートウェイは、VPCs、、Transit Gateway Connect AWS Direct Connect、ピアリングアタッチメント (リージョン内、リージョン間、およびクラウドWANピアリングアタッチメント) 間のトラフィックに対して 8500 バイトMTUの をサポートします。VPN接続経由MTUのトラフィックは 1500 バイトの を持つことができます VPN接続経由MTUのトラフィックは 1500 バイトの を持つことができます。
- VPC ピアリングからトランジットゲートウェイを使用するように移行する場合、VPCピアリングとトランジットゲートウェイMTUのサイズが一致しないと、非対称トラフィックパケットがドロップされる可能性があります。サイズが一致しないためにジャンボパケットがドロップされないように、両方VPCsを同時に更新します。
- Transit Gateway に到達したサイズが 8500 バイトを超えるパケットはドロップされます。
- トランジットゲートウェイは、ICMPv4パケットの FRAG_NEEDED またはICMPv6パケットの Packet Too Big (PTB) を生成しません。したがって、パスMTU検出 (PMTUD) はサポートされていません。
- トランジットゲートウェイは、すべてのパケットに対して最大セグメントサイズ (MSS) クランプを適用します。詳細については、「」を参照してくださいRFC879。
- の Site-to-Site VPN クォータの詳細についてはMTU、 ユーザーガイドの「最大送信単位 (MTU) AWS Site-to-Site VPN 」を参照してください。

マルチキャスト

名前	デフォルト	引き上げ可能
Transit Gateway あたりのマルチキャストドメイン	20	はい

名前	デフォルト	引き上げ可能
Transit Gateway あたりのマルチキャストネットワークインターフェイス	10,000	はい
あたりのマルチキャストドメインの関連付け VPC	20	はい
Transit Gateway マルチキャストグループあたりの送信元	1	はい
トランジットゲートウェイあたりの静的およびIGMPv2マルチキャストグループのメンバーとソース	10,000	なし
Transit Gateway IGMPv2 マルチキャストグループあたりの静的およびマルチキャストグループメンバー	100	いいえ
フローあたりの最大マルチキャストスループット	1 Gbps	いいえ
アベイラビリティーゾーンあたりの最大集約マルチキャストスループット	20 Gbps	なし

AWS ネットワークマネージャー

名前	デフォルト	引き上げ可能
あたりのグローバルネットワーク AWS アカウント	5	はい
グローバルネットワークあたりのデバイス数	200	はい
グローバルネットワークあたりのリンク数	200	はい
グローバルネットワークあたりのサイト数	200	はい

名前	デフォルト	引き上げ可能
グローバルネットワークあたりの接続数	500	いいえ

その他のクォータリソース

詳細については、次を参照してください。

- AWS Site-to-Site VPN ユーザーガイドVPNの Site-to-Site クォータ
- 「Amazon VPC ユーザーガイド」の「Amazon クォータVPC」
- AWS Direct Connect ユーザーガイド の AWS Direct Connect クォータ

Transit Gateway のドキュメント履歴

次の表は、Transit Gateway の各リリースの説明です。

変更	説明	日付
AWS Transit Gateway クォータ	帯域幅の制限が追加されました。	2023 年 8 月 14 日
AWS トランジットゲートウェイフローログ	Transit Gateway Flow Logs が Transit Gateway でサポートされるようになり、Transit Gateway 間のネットワークトラフィックをモニタリングしログ記録できるようになりました。	2022 年 7 月 14 日
Transit Gateway ポリシーテーブル	ポリシーテーブルを使用して、Transit Gateway 用の動的ルーティングを設定し、ルーティングおよび到達可能性の情報をピアリングされた Transit Gateway と自動的に交換できるようにします。	2022 年 7 月 13 日
Network Manager ユーザーガイド	Network Manager のガイドは単体のものが作成されたため、「AWS Transit Gateway ユーザーガイド」には含まれなくなりました。	2021 年 12 月 2 日
添付のピアリング	同じリージョンの Transit Gateway と、ピアリング接続を構築することが可能です。	2021 年 12 月 1 日
Transit Gateway 接続	トランジットゲートウェイと で実行されているサードパーティーの仮想アプライア	2020 年 12 月 10 日

	ンス間の接続を確立できます VPC。	
アプライアンスモード	VPC アタッチメントでアプライアンスモードを有効にして、双方向トラフィックがアタッチメントの同じアベイラビリティーゾーンを通過するようにすることができます。	2020 年 10 月 29 日
プレフィックスリスト参照	Transit Gateway ルートテーブルでプレフィックスリストを参照できます。	2020 年 8 月 24 日
Transit Gateway の変更	Transit Gateway の設定オプションを変更できます。	2020 年 8 月 24 日
CloudWatch トランジットゲートウェイアタッチメントの メトリクス	個々の Transit Gateway アタッチメントの CloudWatch メトリクスを表示できます。	2020 年 7 月 6 日
Network Manager ルートアナライザー	グローバルネットワーク内のトランジットゲートウェイルートテーブルのルートを分析できます。	2020 年 5 月 4 日
添付のピアリング	別のリージョンの Transit Gateway と、ピアリング接続を構築することが可能です。	2019 年 12 月 3 日

マルチキャストサポート	Transit Gateway は、アタッチされた のサブネット間のマルチキャストトラフィックのルーティングをサポートし、複数の受信インスタンス宛てのトラフィックを送信するインスタンスのマルチキャストルーターVPCsとして機能します。	2019 年 12 月 3 日
AWS Network Manager	Transit Gateway を中心に構築されたグローバルネットワークの視覚化およびモニタリングができます。	2019 年 12 月 3 日
AWS Direct Connect のサポート	AWS Direct Connect ゲートウェイを使用して、トランジット仮想インターフェイス経由で AWS Direct Connect に接続VPCsしたり、トランジットゲートウェイにアVPNsタッチしたりできます。	2019 年 3 月 27 日
初回リリース	このリリースでは、Transit Gateway が導入されました。	2018 年 11 月 26 日

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。