ユーザーガイド

AWS Direct Connect

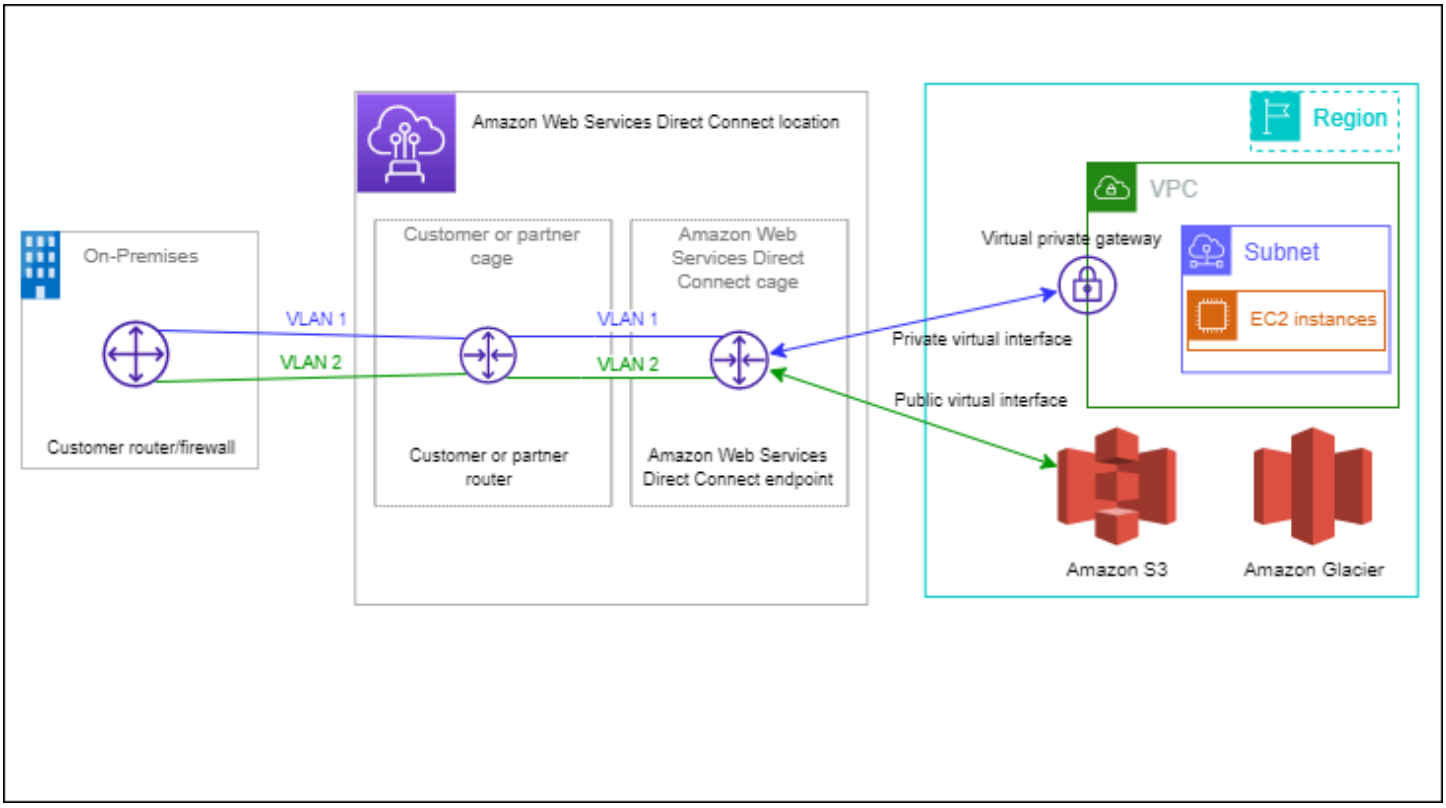
AWS Direct Connect: ユーザーガイド

Table of Contents

とは AWS Direct Connect

AWS Direct Connect は、標準のイーサネット光ファイバケーブルを介して内部ネットワークを AWS Direct Connect ロケーションにリンクします。ケーブルの一方の端はルーターに接続され、もう一方の端は AWS Direct Connect ルーターに接続されています。この接続を使用すると、パブリック AWS サービス (Amazon S3 など) または Amazon VPC への仮想インターフェイスを直接作成し、ネットワークパス内のインターネットサービスプロバイダーをバイパスできます。 AWS Direct Connect ロケーションは、関連付けられているリージョン AWS の へのアクセスを提供します。パブリックリージョンで単一の接続を使用するか、他のすべてのパブリックリージョンでパブリック AWS サービス AWS GovCloud (US) にアクセスできます。

次の図は、 が ネットワークと AWS Direct Connect 連携する方法の概要を示しています。



内容

- リモート AWS リージョンへのアクセス
- ルーティングポリシーと BGP コミュニティ

AWS Direct Connect コンポーネント

以下は、 に使用する主要なコンポーネントです AWS Direct Connect。

接続

AWS Direct Connect ロケーションに接続を作成して、オンプレミスから AWS リージョンへのネットワーク接続を確立します。詳細については、「AWS Direct Connect 接続」を参照してください。

仮想インターフェイス

AWS サービスへのアクセスを有効にする仮想インターフェイスを作成します。パブリックな仮想インターフェイスでは、Amazon S3 などのパブリックなサービスへのアクセスが可能です。プライベート仮想インターフェイスは、VPC へのアクセスを有効にします。詳細については、「AWS Direct Connect 仮想インターフェイス」および「仮想インターフェイスの前提条件」を参照してください。

ネットワークの要件

AWS Direct Connect ロケーション AWS Direct Connect で を使用するには、ネットワークが次のいずれかの条件を満たしている必要があります。

- ネットワークが既存の AWS Direct Connect ロケーションにコロケーションされている。利用可能な AWS Direct Connect ロケーションの詳細については、AWS 「Direct Connect 製品の詳細」を参照してください。
- AWS Direct Connect パートナーネットワーク (APN) のメンバーである AWS パートナーと連携している。詳細については、「AWS Direct Connect をサポートする APN パートナー」を参照してください。
- 独立系サービスプロバイダを利用して に接続する AWS Direct Connect

さらに、お客様のネットワークは以下の条件を満たしている必要があります。

- ネットワークでは、1 ギガビットイーサネットの場合は 1000BASE-LX (1310 nm) トランシーバー、10 ギガビットイーサネットの場合は 10GBASE-LR (1310 nm) トランシーバー、100 ギガ

ビットイーサネットの場合は 100GBASE-LR4 トランシーバーでシングルモードファイバーを使用する必要があります。

- ポート速度が 1 Gbps を超える接続では、ポートのオートネゴシエーションを無効にする必要があります。ただし、接続を提供する AWS Direct Connect エンドポイントによっては、1 Gbps 接続で自動ネゴシエーションを有効または無効にする必要がある場合があります。仮想インターフェイスがダウンしたままの場合は、レイヤー 2 (データリンク層) 問題のトラブルシューティング を参照してください。
- 802.1Q VLAN のカプセル化が、中間デバイスを含む接続全体でサポートされている必要があります。
- デバイスがボーダーゲートウェイプロトコル (BGP) と BGP MD5 認証をサポートしている必要があります。
- (省略可能) ご使用のネットワークで双方向フォワーディング検出 (BFD) プロトコルを設定できます。非同期 BFD は、 AWS Direct Connect 仮想インターフェイスごとに自動的に有効になります。Direct Connect 仮想インターフェイスに対して自動的に有効になりますが、お客様のルーターで設定するまでは利用可能になりません。詳細については、「Enable BFD for a Direct Connect connection」(Direct Connect 接続に対して BFD を有効にする) を参照してください。

AWS Direct Connect は、IPv4 と IPv6 の両方の通信プロトコルをサポートします。パブリック AWS サービスによって提供される IPv6 アドレスには、 AWS Direct Connect パブリック仮想インターフェイスからアクセスできます。

AWS Direct Connect は 1522 バイトまたは 9023 バイトのイーサーネットフレームサイズ (14 バイトイーサーネットヘッダー + 4 バイト VLAN タグ + IP データグラム用バイト + 4 バイト FCS) をリンクレイヤーでサポートします。使用するプライベート仮想インターフェイスの MTU を設定できます。詳細については、「プライベート仮想インターフェイスまたはトランジット仮想インターフェイスのネットワーク MTU の設定」を参照してください。

の料金 AWS Direct Connect

AWS Direct Connect には、ポート時間とアウトバウンドデータ転送の 2 つの請求要素があります。ポート時間料金は容量および接続のタイプ (専用接続あるいはホスト型接続) によって決定されます。

プライベートインターフェイスとトランジット仮想インターフェイスのデータ転送出力料金は、データ転送を担当する AWS アカウントに割り当てられます。マルチアカウントの AWS Direct Connect ゲートウェイを使用する際に追加料金はかかりません。

パブリックアドレス可能な AWS リソース (Amazon S3 バケット、Classic EC2 インスタンス、インターネットゲートウェイを通過する EC2 トラフィックなど) の場合、アウトバウンドトラフィックが同じ AWS 支払者アカウントが所有するパブリックプレフィックスを送信先とし、 AWS Direct Connect パブリック仮想インターフェイス AWS を介してアクティブにアドバタイズされている場合、データ転送アウト (DTO) の使用量は、 AWS Direct Connect データ転送レートでリソース所有者に対して計測されます。

詳細については、AWS Direct Connect の料金を参照してください。

AWS Direct Connect メンテナンス

AWS Direct Connect はフルマネージドサービスで、Direct Connect はサービスをサポートするハードウェアフリートで定期的にメンテナンスアクティビティを実行します。Direct Connect 接続はスタンドアロンのハードウェアデバイスにプロビジョニングされるため、 Amazon Virtual Private Cloud とオンプレミスインフラストラクチャとの間に回復力の高いネットワーク接続を作成できます。この機能を使用すると、信頼性、スケーラビリティ、コスト効率に優れた方法で AWS リソースにアクセスできます。詳細については、「AWS Direct Connect の回復性に関する推奨事項」を参照してください。

Direct Connect メンテナンスには、計画的なメンテナンスと緊急メンテナンスの 2 種類があります。

- 計画的なメンテナンス。計画的なメンテナンスは、可用性の向上と新機能の提供を目的に事前にスケジュールされます。このタイプのメンテナンスは、14 カレンダー日、7 カレンダー日、1 カレンダー日の 3 つの通知を提供するメンテナンスウィンドウ中にスケジュールされます。

  > **Note**
  >
  > 暦日には、営業日以外の日と現地の祝日が含まれます。

- 緊急メンテナンス。緊急メンテナンスは、サービスに影響する障害が発生し、サービスを復元するために AWS からの即時アクションが必要とされる場合に開始されます。このタイプのメンテナンスは事前に計画されません。影響を受けるお客様には、メンテナンスの 60 分前までに緊急メンテナンスの通知が届きます。

メンテナンス中にトラフィックを冗長な Direct Connect 接続に適切かつプロアクティブに移行するために「AWS Direct Connect の回復性に関する推奨事項」に従うことが推奨されます。また、冗長接続の回復性を定期的に積極的にテストして、フェイルオーバーが意図したとおりに機能することを検証することをお勧めします。the section called “AWS Direct Connect フェイルオーバーテスト” 機

能を使用すると、トラフィックが冗長な仮想インターフェイスの 1 つを介してルーティングされていることを確認できます。

計画的メンテナンスのキャンセルをリクエストする資格基準に関するガイダンスについては、「Direct Connect のメンテナンスイベントをキャンセルする方法を教えてください」を参照してください。

> **Note**
>
> 緊急メンテナンスリクエストはキャンセルできません。 AWS はすぐにサービスを復元する必要があります。

メンテナンスイベントの詳細については、「よくある質問」の「メンテナンスイベントAWS Direct Connect FAQs」を参照してください。

リモート AWS リージョンへのアクセス

パブリックリージョン、または AWS GovCloud (US) 内の AWS Direct Connect ロケーションは、その他すべてのパブリックリージョン (中国 (北京および寧夏) を除く) のパブリックサービスにアクセスできます。パブリックリージョン、または AWS GovCloud (US) 内の AWS Direct Connect 接続を、その他すべてのパブリックリージョン (中国 (北京と寧夏) を除く) にあるアカウントの VPC にアクセスするように設定することもできます。したがって、単一の AWS Direct Connect 接続を使用して、マルチリージョンサービスを構築できます。パブリック AWS サービスにアクセスするか、別のリージョンの VPC にアクセスするかに関係なく、すべてのネットワークトラフィックが AWS グローバルネットワークのバックボーンで保持されます。

リモートリージョンからの任意のデータ転送で、リージョンのデータ転送レートでの請求が行われます。データ転送の料金の詳細については、AWS Direct Connect ページの「料金」セクションを参照してください。

AWS Direct Connect 接続のルーティングポリシーおよびサポートされている BGP コミュニティの詳細については、「ルーティングポリシーと BGP コミュニティ」を参照してください。

リモートリージョンでのパブリックサービスへのアクセス

リモートリージョンのパブリックリソースにアクセスするには、パブリック仮想インターフェイスをセットアップし、ボーダーゲートウェイプロトコル (BGP) のセッションを設定する必要があります。詳細については、「AWS Direct Connect 仮想インターフェイス」を参照してください。

パブリック仮想インターフェイスを作成して、BGP セッションを確立したら、ルーターが他のパブリック AWS リージョンのルートを学習します。現在 AWS によってアドバタイズされているプレフィックスの詳細については、「Amazon Web Services 全般のリファレンス」の「AWS IP アドレスの範囲」を参照してください。

リモートリージョンの VPC へのアクセス

すべてのパブリックリージョンで、Direct Connect ゲートウェイを作成できます。ゲートウェイを使用すると、プライベート仮想インターフェイスを介して、AWS Direct Connect 接続を、異なるリージョンまたはトランジットゲートウェイに配置されたご自身のアカウントの VPC に接続できます。詳細については、「Direct Connect ゲートウェイの操作」を参照してください。

また、AWS Direct Connect 接続用のパブリック仮想インターフェイスを作成し、リモートリージョンのご自身の VPC への VPN 接続を確立することもできます。VPC への VPN 接続設定の詳細については、Amazon VPC ユーザーガイドの Scenarios for Using Amazon Virtual Private Cloud を参照してください。

ネットワークから Amazon VPC への接続オプション

次の設定を使用して、リモートネットワークを Amazon VPC 環境に接続できます。これらのオプションは、AWS リソースの既存のオンサイトサービスとの統合に役立ちます。

- Amazon Virtual Private Cloud Connectivity Options

ルーティングポリシーと BGP コミュニティ

AWS Direct Connect パブリック接続のインバウンド (オンプレミスのデータセンターから) とアウトバウンド (AWS 地域から) のルーティングポリシーを適用します。 AWS Direct Connect また、Amazon がアドバタイズするルートのボーダーゲートウェイプロトコル (BGP) コミュニティタグを使用して、ユーザーが Amazon にアドバタイズするルートに BGP コミュニティタグを適用できます。

パブリック仮想インターフェイスのルーティングポリシー

AWS を使用して公共サービスにアクセスする場合は、BGP AWS Direct Connect 経由でアドバタイズするパブリック IPv4 プレフィックスまたは IPv6 プレフィックスを指定する必要があります。

次のインバウンドルーティングポリシーが適用されます。

- パブリックプレフィックスを所有しており、それが適切な地域のインターネットレジストリに登録されている必要があります。
- トラフィックは Amazon パブリックプレフィックス宛である必要があります。接続間の推移的ルーティングはサポートされていません。
- AWS Direct Connect インバウンドパケットフィルタリングを実行して、トラフィックのソースがアドバタイズされたプレフィックスから発信されたものであることを検証します。

次のアウトバウンドルーティングポリシーが適用されます。

- AS_PATH と最長プレフィックス一致を使用してルーティングパスを決定します。 AWS AWS Direct Connect インターネットとパブリック仮想インターフェイスの両方に同じプレフィックスがアドバタイズされている場合を使用して、より具体的なルートをアドバタイズすることを推奨します。
- AWS Direct Connect AWS 利用可能な場合はすべてのローカルリージョンとリモートリージョンのプレフィックスをアドバタイズし、 AWS 利用可能な場合は他の非リージョンのポイントオブプレゼンス (PoP) (Route 53 など) からのオンネットプレフィックスを含めます。 CloudFront

> **Note**
>
> - AWS 中国リージョンの IP アドレス範囲 JSON ファイル ip-ranges.json に記載されているプレフィックスは、中国リージョンでのみアドバタイズされます。 AWS AWS
> - AWS 商業地域の IP アドレス範囲 JSON ファイル ip-ranges.json に記載されているプレフィックスは、商業地域でのみアドバタイズされます。 AWS AWS
>
> 詳細については、「AWS 全般のリファレンス」の「AWS IP アドレス範囲」を参照してください。

- AWS Direct Connect 最小パス長が 3 のプレフィックスをアドバタイズします。
- AWS Direct Connect すべてのパブリックプレフィックスを有名な BGP コミュニティにアドバタイズします。NO_EXPORT
- 2 つの異なるパブリック仮想インターフェイスを使用して 2 つの異なるリージョンから同じプレフィックスをアドバタイズし、両方とも BGP 属性が同じでプレフィックス長が最も長い場合、AWS アウトバウンドトラフィックのホームリージョンが優先されます。
- AWS Direct Connect 接続が複数ある場合は、同じパス属性を持つプレフィックスをアドバタイズすることで、インバウンドトラフィックの負荷分散を調整できます。

- によってアドバタイズされるプレフィックスは、 AWS Direct Connect 接続のネットワーク境界を越えてアドバタイズしてはなりません。たとえば、これらのプレフィックスは、任意のパブリックインターネットルーティングテーブルに含めることはできません。
- AWS Direct Connect Amazon ネットワーク内の顧客によってアドバタイズされたプレフィックスを保持します。パブリック VIF から学習したカスタマープレフィクスを、次のいずれかに再アドバタイズすることはありません。
  - 他のお客様 AWS Direct Connect
  - AWS グローバルネットワークとピアリングするネットワーク
  - Amazon のトランジットプロバイダー

パブリック仮想インターフェイス BGP コミュニティ

AWS Direct Connect スコープ BGP コミュニティタグをサポートし、パブリック仮想インターフェイス上のトラフィックの範囲 (地域またはグローバル) とルート優先度の制御に役立ちます。 AWS パブリックVIFから受信したすべてのルートを、あたかもNO_EXPORT BGPコミュニティタグでタグ付けされたかのように扱います。つまり、 AWS ネットワークだけがそのルーティング情報を使用するということです。

BGP コミュニティの範囲

BGP コミュニティタグを Amazon にアドバタイズするパブリックプレフィックスに適用して、Amazon のネットワーク内のどの程度の範囲にプレフィックスを伝達するか (ローカルの AWS リージョンのみ、大陸内のすべてのリージョン、すべてのパブリックリージョンなど) を示すことができます。

AWS リージョン コミュニティ

インバウンドルーティングポリシーの場合、プレフィックスには次の BGP コミュニティを使用できます。

- `7224:9100`—ローカル AWS リージョン
- `7224:9200`—すべて 1 AWS リージョン つの大陸用:
  - 北米全域
  - アジアパシフィック
  - 欧州、中東、アフリカ
- `7224:9300`—グローバル (すべてのパブリックリージョン) AWS

> **Note**
>
> コミュニティタグをまったく適用しない場合、 AWS プレフィックスはデフォルトですべてのパブリックリージョン (グローバル) にアドバタイズされます。
> 同じコミュニティでマークされ、同一の AS_PATH 属性を持つプレフィックスが、複数経路化の候補になります。

コミュニティ 7224:1 - 7224:65535 は AWS Direct Connectによって予約されています。

アウトバウンドルーティングポリシーでは、次の BGP AWS Direct Connect コミュニティをアドバタイズされたルートに適用します。

- 7224:8100 AWS AWS Direct Connect —ポイントオブプレゼンスが関連付けられているのと同じリージョンを起点とするルート。
- 7224:8200 AWS Direct Connect —プレゼンスポイントが関連付けられているのと同じ大陸を起点とするルート。
- タグなし-他の大陸を起点とするルート。

> **Note**
>
> AWS すべてのパブリックプレフィックスを受信するには、フィルタを適用しないでください。

AWS Direct Connect パブリック接続がサポートされていないコミュニティは削除されます。

NO_EXPORT BGP コミュニティ

アウトバウンドルーティングポリシーの場合、NO_EXPORT BGP コミュニティタグは、パブリック仮想インターフェイスでサポートされています。

AWS Direct Connect また、アドバタイズされた Amazon ルートに BGP コミュニティタグを提供します。 AWS Direct Connect AWS を使用して公共サービスにアクセスする場合は、これらのコミュニティタグに基づいてフィルタを作成できます。

パブリック仮想インターフェースでは、 AWS Direct Connect 顧客に広告を出すすべてのルートに NO_EXPORT コミュニティタグが付けられます。

プライベート仮想インターフェイスおよびトランジット仮想インターフェイスのルーティングポリシー

AWS Direct Connect AWS プライベートリソースへのアクセスに使用する場合は、BGP 経由でアドバタイズする IPv4 または IPv6 プレフィックスを指定する必要があります。これらのプレフィックスは、パブリックでもプライベートでもかまいません。

アドバタイズされたプレフィックスに基づいて、以下のアウトバウンドルーティングルールが適用されます。

- AWS 最も長いプレフィックス長を最初に評価します。 AWS 目的のルーティングパスがアクティブ/パッシブ接続用である場合は、複数の Direct Connect 仮想インターフェイスを使用してより具体的なルートをアドバタイズすることをお勧めします。詳細については、「最長プレフィックス一致によるハイブリッドネットワーク上のトラフィックへの影響」を参照してください。
- ローカルプリファレンスは、必要なルーティングパスがアクティブ/パッシブ接続用で、アドバタイズされるプレフィックス長が同じ場合に使用することをおすすめする BGP 属性です。この値は、—Medium AWS リージョン ローカルプリファレンスコミュニティ値を使用して、AWS Direct Connect 同じ関連付けを持つロケーションを優先するようにリージョンごとに設定されます`7224:7200`。ローカルリージョンが Direct Connect ロケーションに関連付けられていない場合は、低い値に設定されます。これが適用されるのは、ローカルプリファレンスコミュニティタグが割り当てられていない場合のみです。
- プレフィックスの長さとローカルプリファレンスが同じ場合は、AS_PATH length を使用してルーティングパスを決定できます。
- プレフィックス長、ローカルプリファレンス、AS_PATH が同じ場合は、Multi-Exit Deminator (MED) を使用してルーティングパスを決定できます。 AWS 評価時の優先度が低いため、MED 値の使用はお勧めしません。
- AWS プレフィックスの長さと BGP 属性が同じ場合、複数の中継仮想インターフェイスまたはプライベート仮想インターフェイス間で負荷分散されます。

プライベート仮想インターフェイスおよびトランジット仮想インターフェイスの BGP コミュニティ

が Direct Connect AWS リージョン のプライベートまたはトランジット仮想インターフェイスを介してオンプレミスの場所にトラフィックをルーティングする場合、Direct Connect AWS リージョン ロケーションに関連付けられているものが、等コストマルチパスルーティング (ECMP) を使用する機能に影響します。 AWS リージョン AWS リージョン デフォルトでは同じ関連付けのダイレクト

Connect ロケーションを優先します。Direct Connect AWS Direct ConnectAWS リージョン ロケーションの関連を特定するには、「ロケーション」を参照してください。

ローカルプリファレンスコミュニティタグが適用されていない場合、Direct Connect は、次のシナリオで、同じ長さ、AS_PATH 長、および MED 値を持つプレフィックスに対して、プライベートまたは中継仮想インターフェイス上の ECMP をサポートします。

- AWS リージョン 送信トラフィックには、同じコロケーション施設内であろうと異なるコロケーション施設内であろうと AWS リージョン、同じアソシエート内のロケーションからの仮想インターフェイスパスが 2 つ以上あります。
- AWS リージョン 送信トラフィックには、同じリージョンにない場所からの仮想インターフェイスパスが 2 つ以上あります。

詳細については、「AWS プライベートまたはトランジット仮想インターフェイスからのアクティブ/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。

> **Note**
>
> これは、オンプレミスの場所への、またはオンプレミスの場所からの ECMP には影響しません。 AWS リージョン

ルートプリファレンスを制御するために、Direct Connect はプライベート仮想インターフェイスとトランジット仮想インターフェイスのローカルプリファレンス BGP コミュニティタグをサポートしています。

BGP コミュニティのローカル優先設定

ローカル優先設定の BGP コミュニティタグを使用すると、ネットワークの着信トラフィックでロードバランシングやルート設定を実現できます。BGP セッション経由でアドバタイズするプレフィックスごとに、コミュニティタグを適用して、返されるトラフィックの関連付け済みパスの優先度を示すことができます。

サポートされているローカル優先設定の BGP コミュニティタグを次に示します。

- `7224:7100` - 優先設定: 低
- `7224:7200` - 優先設定: 中
- `7224:7300` - 優先設定: 高

ローカル優先設定 BGP コミュニティタグは相互に排他的です。 AWS Direct Connect AWS 同じリージョンまたは異なるリージョンをホームとする複数の接続 (アクティブ/アクティブ) 間でトラフィックを負荷分散するには、接続のプレフィックス全体に `7224:7200` (中程度の優先順位) などの同じコミュニティタグを適用します。接続の 1 つに障害が発生すると、ホームリージョンの関連付けに関係なく、残りのアクティブな接続全体で ECMP を使用してトラフィックの負荷分散が行われます。複数の AWS Direct Connect 接続 (アクティブ/パッシブ) でフェイルオーバーをサポートするには、プライマリまたはアクティブな仮想インターフェイスのプレフィックスに、優先設定が高いコミュニティタグを適用し、バックアップまたはパッシブな仮想インターフェイスのプレフィックスに低い優先設定を適用します。例えば、プライマリまたはアクティブな仮想インターフェイスの BGP コミュニティタグを `7224:7300` (高優先設定) に設定し、パッシブ仮想インターフェイスの BGP コミュニティタグを `7224:7100` (低優先設定) に設定します。

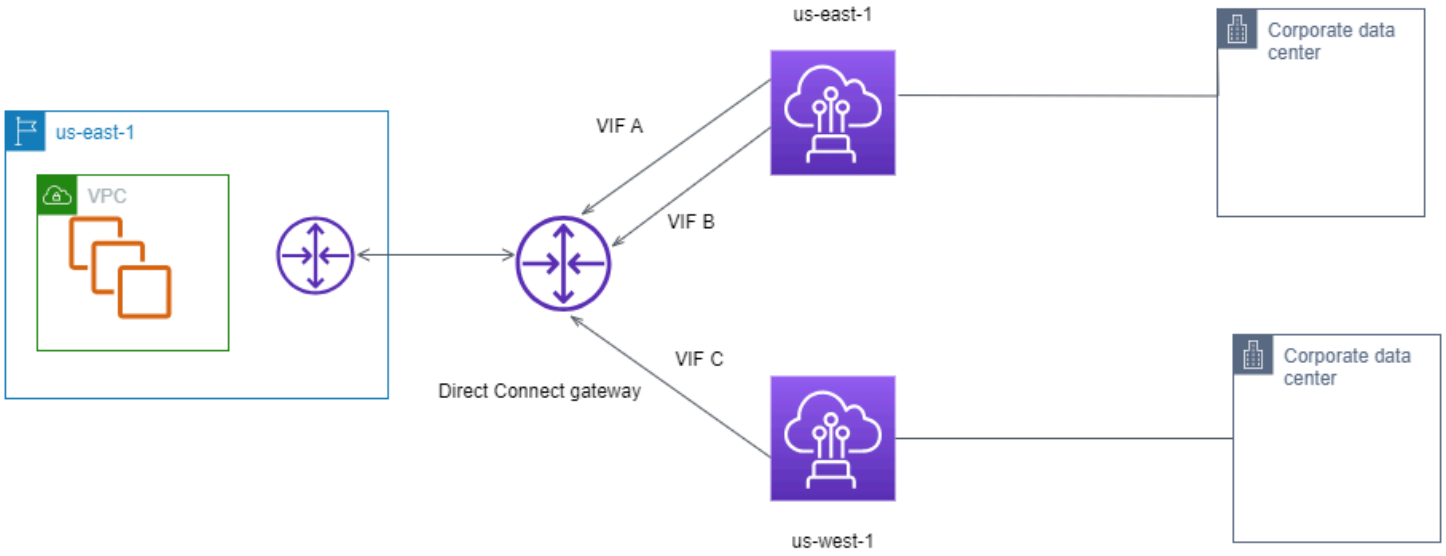
ローカル設定 BGP コミュニティタグは AS_PATH 属性の前に評価され、最も低い設定から最も高い設定の順に評価されます (最も高い設定が優先されます)。

プライベート仮想インターフェイスルーティングの例

AWS Direct Connect Location 1 のホームリージョンが VPC ホームリージョンと同じ設定を考えてみましょう。 AWS Direct Connect 別のリージョンに冗長ロケーションがあります。 AWS Direct Connect ロケーション 1 (us-east-1) から Direct Connect ゲートウェイまで 2 つのプライベート VIF (VIF A と VIF B) があります。 AWS Direct Connect ロケーション (us-west-1) からダイレクトConnect ゲートウェイへのプライベート VIF (VIF C) が 1 つあります。VIF A よりも前に VIF B AWS 経由でトラフィックをルーティングするには、VIF B の AS_PATH 属性を VIF A の AS_PATH 属性よりも短く設定します。

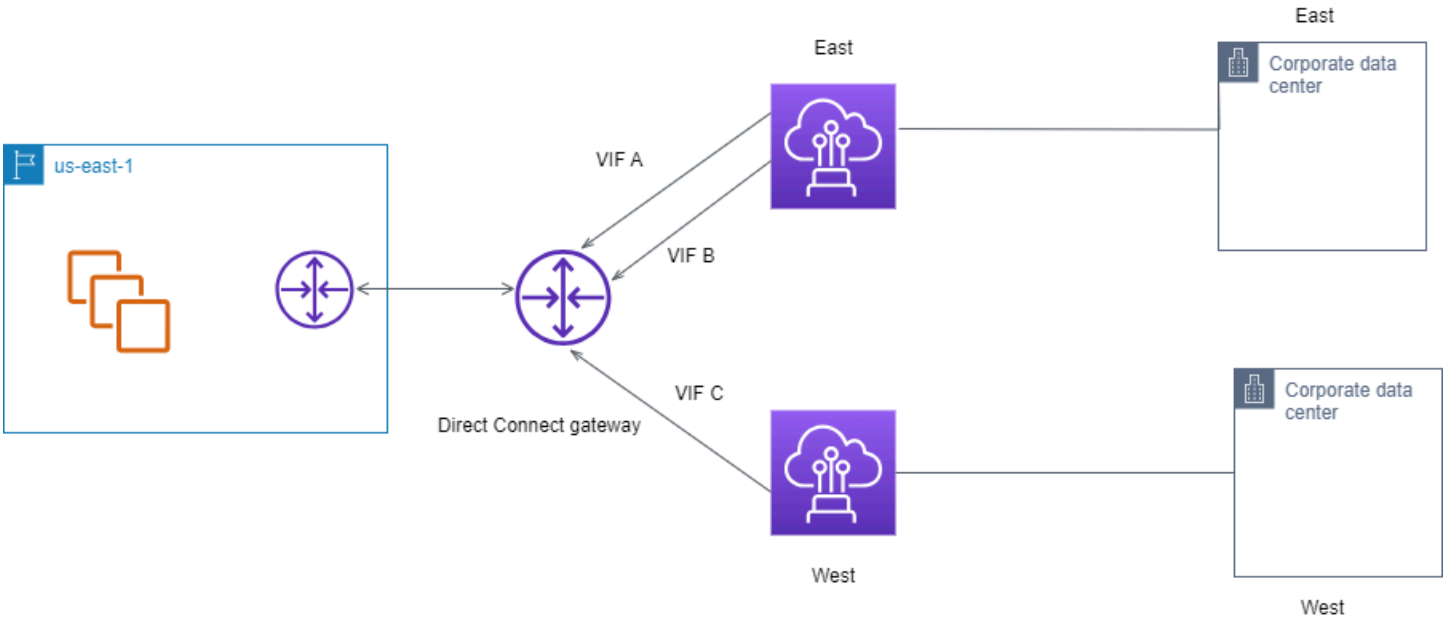
VIF の設定は次のとおりです。

- VIF A (us-east-1) は 172.16.0.0/16 をアドバタイズし、AS_PATH 属性は 65001、65001、65001
- VIF B (us-east-1) は 172.16.0.0/16 をアドバタイズし、AS_PATH 属性は 65001、65001
- VIF C (us-west-1) は 172.16.0.0/16 をアドバタイズし、AS_PATH 属性は 65001



VIF C の CIDR 範囲設定を変更すると、VIF C CIDR 範囲に含まれるルートには VIF C が使用されます。これは、VIF C のプレフィックス長が最も長いためです。

- VIF C (us-west-1) は 172.16.0.0/24 をアドバタイズし、AS_PATH 属性は 65001



Resiliency Toolkit AWS Direct Connect を使用して開始する

AWS は、Amazon Virtual Private Cloud (Amazon VPC) とオンプレミスインフラストラクチャ間の耐障害性の高いネットワーク接続を実現する機能を提供します。 AWS Direct Connect Resiliency Toolkit は、複数の障害耐性モデルを備えた接続ウィザードを提供します。これらのモデルは、SLA 目標を達成するための専用接続の数を決定し、注文するのに役立ちます。障害耐性モデルを選択すると、Resiliency Toolkit AWS Direct Connect が専用の接続順序付けプロセスをガイドします。回復性モデルは、複数の場所で適切な数の専用接続を確保するように設計されています。

AWS Direct Connect Resiliency Toolkit には次の利点があります。

- 適切な冗長 AWS Direct Connect 専用接続を決定してリクエストする方法に関するガイダンスを提供します。
- 複数の冗長専用接続の速度が同じになるようにします。
- 専用接続の名称を自動的に設定します。
- 既存の AWS アカウントがあり、既知の AWS Direct Connect パートナーを選択すると、専用接続が自動的に承認されます。授権書 (LOA) はすぐにダウンロードできます。
- 新規 AWS のお客様、または不明な (その他の) パートナーを選択した場合、専用接続承認のサポートチケットを自動的に作成します。
- 専用接続のリクエストに関する概要を提供します。これには達成可能な SLA や、リクエストした専用接続のポート時間コストが含まれます。
- Link Aggregation Group (LAG) を作成し、1 Gbps、10 Gbps または 100 Gbps 以外の速度を選択した場合は適切な数の専用接続を LAG に追加します。
- LAG の概要を提供します。これには、達成可能な専用接続 SLA や、LAG の一部としてリクエストされた専用接続ごとの合計ポート時間コストが含まれます。
- 同じ AWS Direct Connect デバイス上の専用接続を終了できないようにします。
- 構成の回復性をテストする方法を提供します。 AWS と連携して BGP ピア接続セッションを停止して、トラフィックがいずれかの冗長仮想インターフェイスにルーティングされることを確認します。詳細については、「the section called “AWS Direct Connect フェイルオーバーテスト”」を参照してください。
- 接続と仮想インターフェイスの Amazon CloudWatch メトリクスを提供します。詳細については、「モニタリング」を参照してください。

Resiliency Toolkit では、次の AWS Direct Connect 障害耐性モデルを使用できます。

- 最大回復性: このモデルは、99.99% の SLA を達成するための専用接続をリクエストする方法を提供します。これには、AWS Direct Connect サービスレベルアグリーメントに規定されている SLA 達成のためのすべての要件を満たす必要があります。
- 高い回復性: このモデルは、99.9% の SLA を達成するための専用接続をリクエストする方法を提供します。これには、AWS Direct Connect サービスレベルアグリーメントに規定されている SLA 達成のためのすべての要件を満たす必要があります。
- 開発とテスト: このモデルでは、1 つの場所にある個別のデバイスを終端とする別々の接続を使用して、クリティカルでないワークロードの開発とテストの回復性を実現できます。
- Classic このモデルは、既存の接続があり、それに接続を追加するユーザーが使用することを目的としています。このモデルでは SLA は提供されません。

ベストプラクティスは、 AWS Direct Connect 障害耐性ツールキットの接続ウィザードを使用して、SLA 目標を達成するための専用接続を注文することです。

障害耐性モデルを選択すると、Resiliency Toolkit AWS Direct Connect は次の手順を実行します。

- 専用接続数を選択する
- 接続容量と専用接続の場所を選択する
- 専用接続をリクエストする
- 専用接続を使用できる準備が整っていることを確認する
- 専用接続ごとに Letter of Authority (LOA-CFA) をダウンロードする
- 構成が回復性の要件を満たしていることの確認

前提条件

AWS Direct Connect は、シングルモードファイバーで次のポート速度をサポートします。1 ギガビットイーサネットの場合は 1000BASE-LX (1310 nm) トランシーバー、10 ギガビットイーサネットの場合は 10GBASE-LR (1310 nm) トランシーバー、100 ギガビットイーサネットの場合は 100GBASE-LR4。

AWS Direct Connect 接続は、次のいずれかの方法で設定できます。

モデル	帯域幅	方法
専用接続	1 Gbps、10 Gbps、100 Gbps	AWS Direct Connect パートナーまたはネットワークプロ

モデル	帯域幅	方法
		バイダーと協力して、データセンター、オフィス、またはコロケーション環境から AWS Direct Connect ロケーションにルーターを接続します。専用接続への接続を行うネットワークプロバイダーがAWS Direct Connect パートナーである必要はありません。 AWS Direct Connect の専用接続は、シングルモードファイバで 1 Gbps: 1000BASE-LX (1310 nm)、10 Gbps: 10GBASE-LR (1310 nm)、および 100 Gbps: 100GBASE-LR4 のポート速度をサポートします。
ホスト接続	50 Mbps、100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps、10 Gbps	パートナーAWS Direct Connect プログラムのパートナーと協力して、データセンター、オフィス、またはコロケーション環境から AWS Direct Connect ロケーションにルーターを接続します。 一部のパートナーのみがより大きな容量の接続を提供しています。

帯域幅 AWS Direct Connect が 1 Gbps 以上の への接続の場合は、ネットワークが次の要件を満たしていることを確認してください。

- ネットワークでは、1 ギガビットイーサネットの場合は 1000BASE-LX (1310 nm) トランシーバー、10 ギガビットイーサネットの場合は 10GBASE-LR (1310 nm) トランシーバー、100 ギガ

ビットイーサネットの場合は 100GBASE-LR4 トランシーバーでシングルモードファイバーを使用する必要があります。

- ポート速度が 1 Gbps を超える接続では、ポートのオートネゴシエーションを無効にする必要があります。ただし、接続を提供する AWS Direct Connect エンドポイントによっては、1 Gbps 接続で自動ネゴシエーションを有効または無効にする必要がある場合があります。仮想インターフェイスがダウンしたままの場合は、レイヤー 2 (データリンク層) 問題のトラブルシューティング を参照してください。
- 802.1Q VLAN のカプセル化が、中間デバイスを含む接続全体でサポートされている必要があります。
- デバイスがボーダーゲートウェイプロトコル (BGP) と BGP MD5 認証をサポートしている必要があります。
- (省略可能) ご使用のネットワークで双方向フォワーディング検出 (BFD) プロトコルを設定できます。非同期 BFD は、 AWS Direct Connect 仮想インターフェイスごとに自動的に有効になります。Direct Connect 仮想インターフェイスに対して自動的に有効になりますが、お客様のルーターで設定するまでは利用可能になりません。詳細については、「Enable BFD for a Direct Connect connection」(Direct Connect 接続に対して BFD を有効にする) を参照してください。

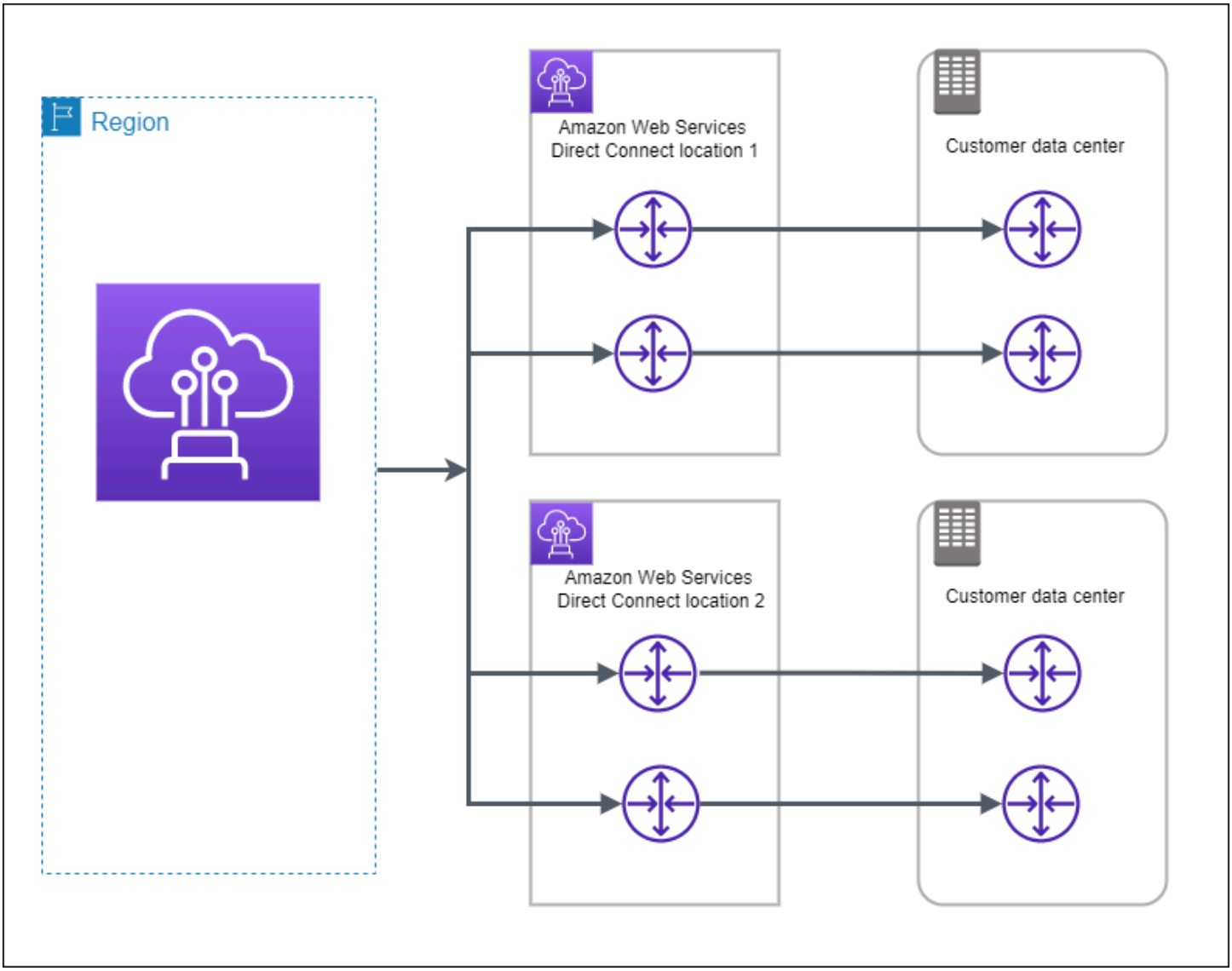
設定を開始する前に、次の情報が揃っていることを確認してください。

- 使用する回復性モデル。
- すべての接続の速度、場所、およびパートナー。

  速度は、1 つの接続分のみ必要です。

最大回復性

クリティカルなワークロードに対し、複数の場所にある別々のデバイスを終端とする別々の接続を使用することで最大限の回復性を実現できます (以下の図を参照)。このモデルは、デバイス、接続、ロケーション全体の障害に対する回復性を提供します。次の図は、各カスタマーデータセンターから同じ AWS Direct Connect 場所への両方の接続を示しています。必要に応じてお客様は、自身のデータセンターから異なるロケーションに向かう、別個の接続を持つこともできます。



次の手順は、Resiliency Toolkit AWS Direct Connect を使用して最大回復性モデルを設定する方法を示しています。

トピック

- ステップ 1: にサインアップする AWS
- ステップ 2: 回復性モデルを設定する
- ステップ 3: 仮想インターフェイスを作成する
- ステップ 4: 仮想インターフェイスの構成の回復性を確認する
- ステップ 5: 仮想インターフェイス接続を検証する

ステップ 1: にサインアップする AWS

を使用するには AWS Direct Connect、まだアカウントをお持ちでない場合は、 AWS アカウントが必要です。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [アカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「ルートユーザーとしてサインインする」を参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の AWS アカウント 「ルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 ユーザーガイド」の「デフォルト でユーザーアクセス IAM アイデンティティセンターディレクトリを設定するAWS IAM Identity Center 」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、「 AWS サインイン ユーザーガイド」の AWS 「 アクセスポータルへのサインイン」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの参加」を参照してください。

ステップ 2: 回復性モデルを設定する

最大回復性モデルを設定するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [接続] を選択し、[接続の作成] を選択します。
3. [Connection ordering type] の [Connection wizard] を選択します。
4. [回復性レベル] で、[最大回復性]、[Next (次へ)] の順に選択します。
5. [Configure connections (接続の構成)] ペインの [Connection settings (接続設定)] で、以下を実行します。

   a. [帯域幅] で、専用接続の帯域幅を選択します。

      この帯域幅は、作成されたすべての接続に適用されます。

   b. 最初のロケーションサービスプロバイダー では、専用接続に適した AWS Direct Connect ロケーションを選択します。

   c. 該当する場合は、[First Sub location] で、お客様、またはお客様のネットワークプロバイダに最も近いフロアを選択します。このオプションは、ロケーションで建物の複数のフロアに会議室 (MMR) がある場合のみ利用できます。

   d. [First location service provider] で [Other] を選択した場合は、[プロバイダーの名前] に、使用するパートナーの名前を入力します。

   e. 2 番目のロケーションサービスプロバイダー で、適切な AWS Direct Connect ロケーションを選択します。

   f. 該当する場合は、[Second Sub location] で、お客様、またはお客様のネットワークプロバイダに最も近いフロアを選択します。このオプションは、ロケーションで建物の複数のフロアに会議室 (MMR) がある場合のみ利用できます。

   g. [Second location service provider] で [Other] を選択した場合は、[プロバイダーの名前] に、使用するパートナーの名前を入力します。

   h. (オプション) タグを追加または削除します。

      [タグの追加] [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。

      [タグの削除] タグの横にある [タグの削除] を選択します。

6. [Next] を選択します。
7. 接続を確認し、[Continue] を選択します。

   LOA の準備ができたら [Download LOA] を選択し、[Continue] を選択します。

   がリクエストを確認し、接続用のポートをプロビジョニング AWS するまでに最大 72 時間かかる場合があります。この時間中、ユースケースまたは指定された場所に関する詳細情報のリクエストを含む E メールが送信される場合があります。E メールは、 にサインアップしたときに使用した E メールアドレスに送信されます AWS。7 日以内に応答する必要があり、応答しないと接続は削除されます。

ステップ 3: 仮想インターフェイスを作成する

プライベート仮想インターフェイスを作成して、VPC に接続することができます。または、パブリック仮想インターフェイスを作成して、VPC にないパブリック AWS サービスに接続することもできます。VPC へのプライベート仮想インターフェイスを作成するときは、接続する VPC ごとにプライベート仮想インターフェイスが必要です。たとえば、3 つの VPC に接続するには 3 つのプライベート仮想インターフェイスが必要です。

作業を開始する前に、次の情報が揃っていることを確認してください。

リソース	必要な情報
Connection	仮想インターフェイスを作成する AWS Direct Connect 接続またはリンク集約グループ (LAG)。
仮想インターフェイス名	仮想インターフェイスの名前。
仮想インターフェイス所有者	別の アカウントの仮想インターフェイスを作成する場合は、他の AWS アカウントのアカウント ID が必要です。
(プライベート仮想インターフェイスのみ) 接続	同じ AWS リージョンの VPC に接続するには、VPC の仮想プライベートゲートウェイが必要です。Amazon 側の BGP セッションのための ASN は、仮想プライベートゲートウェイから継承されます。仮想プライベートゲートウェイを作成するときに、独自のプライベート ASN を指定できます。そうでない場合は、Amazon によってデフォルトの ASN が指定されます。詳細については、Amazon VPC ユーザーガイドの Create a Virtual Private

リソース	必要な情報
	Gateway を参照してください。Direct Connect Gateway 経由で VPC に接続する場合は、Direct Connect Gateway が必要です。詳細については、「Direct Connect Gateway」を参照してください。
VLAN	仮想ローカルエリアネットワーク (VLAN) の、まだ接続で使用されていない一意のタグ。値は 1 ~ 4094 を指定する必要があります。またイーサネット 802.1Q 規格を満たしている必要があります。このタグは、 AWS Direct Connect 接続を通過するすべてのトラフィックに必要です。 ホスト接続がある場合、 AWS Direct Connect パートナーはこの値を提供します。仮想インターフェイス作成後に値を変更することはできません。

リソース	必要な情報

ピア IP アドレス	仮想インターフェイスは、IPv4 または IPv6 に対して 1 つの BGP ピアリングセッションをサポートできます。または両方に対して 1 つずつ BGP ピアリングセッションをサポートできます (デュアルスタック)。パブリック仮想インターフェイスの作成に Amazon プールからの Elastic IP (EIP) および Bring your own IP アドレス (BYOIP) を使用して作成しないでください。同じ仮想インターフェイスで同じ IP アドレスファミリに対して複数の BGP セッションを作成することはできません。BGP ピアセッションでは、仮想インターフェイスの両端に IP アドレス範囲が割り当てられます。
	
	• IPv4:
	  • (パブリック仮想インターフェイスのみ) お客様が所有している一意のパブリック IPv4 アドレスを指定する必要があります。以下のいずれかを指定できます。
	  • カスタマー所有 IPv4 CIDR
	
	これらは任意のパブリック IPs (顧客所有または が提供する AWS) にすることができますが、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、などの/31範囲を割り当てる場合は、ピア IP 203.0.113.0 にを203.0.113.0/31 、 AWS ピア IP 203.0.113.1 に を使用できます。または、 などの/24範囲を割り当てる場合は、ピア IP 198.51.100.10 に を198.51.100.0/24 、 AWS ピア IP 198.51.100.20 に を使用できます。
	  • AWS Direct Connect パートナーまたは ISP が所有する IP 範囲と LOA-CFA 認証
	  • AWSが提供する /31 CIDR。AWS Support に連絡して、パブリック IPv4 CIDR をリクエストします (リクエストにはユースケースを提供します)
	
	Note
	AWSが提供するパブリック IPv4 アドレスに対するすべてのリクエストを当社が受理できることを保証することはできません。

リソース	必要な情報
	• (プライベート仮想インターフェイスのみ) Amazon がプライベート IPv4 アドレスを自動的に生成できます。独自の CIDRs を指定してください。 AWS 例えば、ローカルネットワークから他の IP アドレスを指定しないでください。パブリック仮想インターフェイスと同様に、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、 などの/30範囲を割り当てる場合、ピア IP 192.168.0.1 には を192.168.0.0/30 、 AWS ピア IP 192.168.0.2 には を使用できます。 • IPv6: Amazon は /125 IPv6 CIDR を自動的に割り当てます。独自のピア IPv6 アドレスを指定することはできません。
アドレスファミリー	BGP ピアリングセッションが IPv4 と IPv6 のどちらを使用するか。
BGP 情報	• BGP セッションのお客様側のパブリックまたはプライベート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)。パブリック ASN を使用する場合は、お客様が所有者であることが必要です。プライベート ASN を使用している場合は、カスタム ASN 値を設定できます。16 ビット ASN では、値は 64512 から 65534 の範囲内である必要があります。32 ビット ASN では、値は 1 から 2,147,483,647 の範囲内である必要があります。パブリック仮想インターフェイス用のプライベート ASN を使用する場合、自律システム (AS) の前置は動作しません。 • AWS はデフォルトで MD5 を有効にします。この値を変更することはできません。 • MD5 BGP 認証キー。独自のキーを指定するか、Amazon で自動的に生成することができます。

リソース	必要な情報

(パブリック仮想インターフェイスのみ) アドバタイズするプレフィックス	BGP 経由でアドバタイズするパブリックの IPv4 ルートまたは IPv6 ルート。BGP を使用して少なくとも 1 つ (最大 1,000 個) のプレフィックスをアドバタイズする必要があります。
	• IPv4: IPv4 CIDR は、次のいずれか AWS Direct Connect に該当する場合、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs異なる AWS リージョンから取得されます。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• IPv6: /64 以下のプレフィックスの長さを指定します。
	• AWS Support に連絡することによって、既存のパブリック VIF にプレフィックスを追加し、それらをアドバタイズすることができます。サポートケースで、パブリック VIF に追加してアドバタイズしたい追加の CIDR プレフィックスのリストを提供してください。
	• Direct Connect パブリック仮想インターフェイスでは、任意のプレフィックス長を指定できます。IPv4 は /1 から /32 までのすべてをサポートし、IPv6 は /1 から /64 までのすべてをサポートする必要があります。

リソース	必要な情報
(プライベート仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェースの MTU を 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。ジャンボフレームは、 から伝播されたルートにのみ適用されます AWS Direct Connect。仮想プライベートゲートウェイを指すルートテーブルに静的ルートを追加する場合、静的ルートを介してルーティングされるトラフィックは 1500 MTU を使用して送信されます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでジャンボフレームを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが対応しているかどうかを確認します。
(トランジット仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェイスの MTU を 8500 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。Direct Connect では、最大 8500 MTU のジャンボフレームがサポートされます。Transit Gateway ルートテーブルで設定された静的なルートと伝播されたルートはジャンボフレームをサポートします。これには、VPC の静的なルートテーブルのエントリを持つ EC2 インスタンスから Transit Gateway アタッチメントへのものが含まれます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでジャンボフレームを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが対応しているかどうかを確認します。

お客様のパブリックプレフィックスまたは ASN が、ISP またはネットワークキャリアに属している場合には、当社からお客様に対し追加の情報がリクエストされます。これは、ネットワークプレフィックス/ASN をお客様が使用できることを確認する、会社の正式なレターヘッドを使用したドキュメント、または会社のドメイン名からの E メールとすることができます。

パブリック仮想インターフェイスを作成すると、 がリクエストを確認して承認 AWS するまでに最大 72 時間かかることがあります。

非 VPC サービスへのパブリック仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [パブリック] を選択します。
5. [Public Virtual Interface settings (仮想インターフェイス設定)] で以下を実行します。

   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

   c. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

   d. [BGP ASN] に、ゲートウェイ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) を入力します。

      有効な値は 1 ~ 2147483647 です。
6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

      - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
      - [Amazon ルーターのピア IP] に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

      [IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

   b. 独自の BGP キーを指定するには、使用する BGP MD5 キーを入力します。

      値が入力されない場合は、当社の側で自動的に BGP キーを生成します。

c. Amazon にプレフィックスを発行するには、[アドバタイズするプレフィックス] に、この仮想インターフェイスを介してルーティングされるトラフィックのルーティング先となる IPv4 CIDR アドレスをカンマで区切って入力します。

d. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

VPC へのプライベート仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [プライベート] を選択します。
5. [プライベート仮想インターフェイス設定] で以下を実行します。

a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

c. [ゲートウェイタイプ] で、[仮想プライベートゲートウェイ] または [Direct Connect ゲートウェイ] を選択します。

d. 仮想インターフェイス所有者 で、別の AWS アカウント を選択し、 AWS アカウントを入力します。

e. [仮想プライベートゲートウェイ] で、このインターフェイスに使用する仮想プライベートゲートウェイを選択します。

f. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

g. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

有効な値は 1 ~ 2,147,483,647 です。

6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

      - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
      - [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

      > **Important**
      >
      > IPv4 アドレス AWS の自動割り当てを許可すると、RFC 3927 に従って 169.254.0.0/16 IPv4 Link-Local から /29 CIDR が接続用に割り当てられます。VPC point-to-point AWS トラフィックの送信元および/または送信先としてカスタマールーターピア IP アドレスを使用する場合は、このオプションは推奨されません。代わりに、RFC 1918 または他のアドレスを使用して、アドレスを自分で指定する必要があります。
      >
      > - RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。
      > - RFC 3927 の詳細については、「IPv4 リンクローカルアドレスのダイナミック設定」を参照してください。

      [IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

   b. 最大送信単位 (MTU) を 1500 (デフォルト) から 9001 (ジャンボフレーム) に変更するには、[ジャンボ MTU (MTU サイズ 9001)] を選択します。

   c. （ オプション ）「 を有効にする SiteLink」で「有効」を選択して、Direct Connect のプレゼンスポイント間の直接接続を有効にします。

   d. (オプション) タグを追加または削除します。

      [タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

ステップ 4: 仮想インターフェイスの構成の回復性を確認する

AWS クラウドまたは Amazon VPC への仮想インターフェイスを確立したら、仮想インターフェイスのフェイルオーバーテストを実行して、設定が障害耐性要件を満たしていることを確認します。詳細については、「the section called “AWS Direct Connect フェイルオーバーテスト”」を参照してください。

ステップ 5: 仮想インターフェイス接続を検証する

AWS クラウドまたは Amazon VPC への仮想インターフェイスを確立したら、次の手順を使用して AWS Direct Connect 接続を検証できます。

AWS クラウドへの仮想インターフェイス接続を確認するには

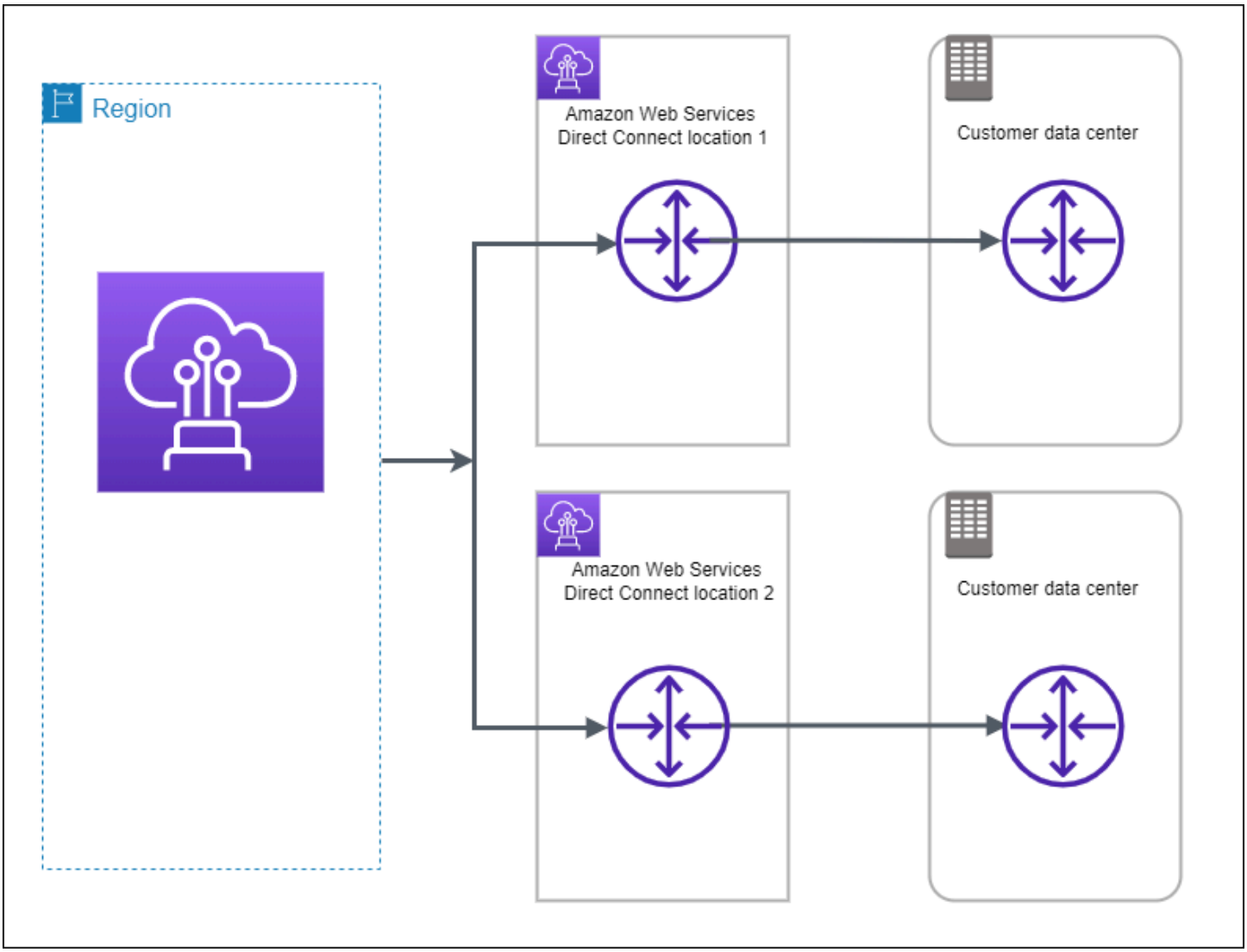
- を実行し`traceroute`、 AWS Direct Connect 識別子がネットワークトレースにあることを確認します。

Amazon VPC への仮想インターフェイス接続を検証するには

1. Amazon Linux AMI など Ping に応答する AMI を使用して、仮想プライベートゲートウェイにアタッチされている VPC に EC2 インスタンスを起動します。Amazon EC2 コンソールのインスタンス起動ウィザードを使用すれば、Amazon Linux AMI を [Quick Start (クイックスタート)] タブで使用することができます。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの起動」を参照してください。 Amazon EC2 インスタンスに関連付けられたセキュリティグループに、インバウンド ICMP トラフィックを許可するルール (ping リクエストの場合) が含まれていることを確認します。
2. インスタンスが実行中になった後、そのプライベート IPv4 アドレス (たとえば 10.0.0.4) を取得します。Amazon EC2 コンソールにインスタンスの詳細の一部としてアドレスが表示されます。
3. プライベート IPv4 アドレスに Ping を実行し、応答を確認します。

高い回復性

クリティカルなワークロードに対し、複数の場所につながる 2 つの単一接続を使用することで、高い回復性を実現できます (以下の図を参照)。このモデルは、ファイバーの切断やデバイスの障害に起因する接続障害に対し、回復性を提供します。また、ロケーション全体の障害を防ぐのに役立ちます。



次の手順は、Resiliency Toolkit AWS Direct Connect を使用して高回復性モデルを設定する方法を示しています。

トピック

- ステップ 1: にサインアップする AWS
- ステップ 2: 回復性モデルを設定する

- ステップ 3: 仮想インターフェイスを作成する
- ステップ 4: 仮想インターフェイスの構成の回復性を確認する
- ステップ 5: 仮想インターフェイス接続を検証する

ステップ 1: にサインアップする AWS

を使用するには AWS Direct Connect、まだアカウントをお持ちでない場合は、 AWS アカウントが必要です。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [アカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「ルートユーザーとしてサインインする」を参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の AWS アカウント 「ルートユーザーの仮想 MFA デバイスを有効にする (コンソール) 」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 ユーザーガイド」の「デフォルト でユーザーアクセスを設定する IAM アイデンティティセンターディレクトリAWS IAM Identity Center 」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、「 AWS サインイン ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの参加」を参照してください。

ステップ 2: 回復性モデルを設定する

高回復性モデルを設定するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [接続] を選択し、[接続の作成] を選択します。
3. [Connection ordering type] の [Connection wizard] を選択します。
4. [回復性レベル] で、[高い回復性]、[Next (次へ)] の順に選択します。
5. [Configure connections (接続の構成)] ペインの [Connection settings (接続設定)] で、以下を実行します。

   a. [帯域幅] で、接続の帯域幅を選択します。

      この帯域幅は、作成されたすべての接続に適用されます。

   b. 最初のロケーションサービスプロバイダー で、適切な AWS Direct Connect ロケーションを選択します。

   c. 該当する場合は、[First Sub location] で、お客様、またはお客様のネットワークプロバイダに最も近いフロアを選択します。このオプションは、ロケーションで建物の複数のフロアに会議室 (MMR) がある場合のみ利用できます。

   d. [First location service provider] で [Other] を選択した場合は、[プロバイダーの名前] に、使用するパートナーの名前を入力します。

   e. 2 番目のロケーションサービスプロバイダー で、適切な AWS Direct Connect ロケーションを選択します。

   f. 該当する場合は、[Second Sub location] で、お客様、またはお客様のネットワークプロバイダに最も近いフロアを選択します。このオプションは、ロケーションで建物の複数のフロアに会議室 (MMR) がある場合のみ利用できます。

g. [Second location service provider] で [Other] を選択した場合は、[プロバイダーの名前] に、使用するパートナーの名前を入力します。

h. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

6. [Next] を選択します。
7. 接続を確認し、[Continue] を選択します。

LOA の準備ができたら [Download LOA] を選択し、[Continue] を選択します。

がリクエストを確認し、接続用のポートをプロビジョニング AWS するまでに最大 72 時間かかる場合があります。この時間中、ユースケースまたは指定された場所に関する詳細情報のリクエストを含む E メールが送信される場合があります。E メールは、 にサインアップしたときに使用した E メールアドレスに送信されます AWS。7 日以内に応答する必要があり、応答しないと接続は削除されます。

ステップ 3: 仮想インターフェイスを作成する

プライベート仮想インターフェイスを作成して、VPC に接続することができます。または、パブリック仮想インターフェイスを作成して、VPC にないパブリック AWS サービスに接続することもできます。VPC へのプライベート仮想インターフェイスを作成するときは、接続する VPC ごとにプライベート仮想インターフェイスが必要です。たとえば、3 つの VPC に接続するには 3 つのプライベート仮想インターフェイスが必要です。

作業を開始する前に、次の情報が揃っていることを確認してください。

リソース	必要な情報
Connection	仮想インターフェイスを作成する AWS Direct Connect 接続またはリンク集約グループ (LAG)。
仮想インターフェイス名	仮想インターフェイスの名前。

リソース	必要な情報
仮想インターフェイス所有者	別の アカウントの仮想インターフェイスを作成する場合は、他の AWS アカウントのアカウント ID が必要です。
(プライベート仮想インターフェイスのみ) 接続	同じ AWS リージョンの VPC に接続するには、VPC の仮想プライベートゲートウェイが必要です。Amazon 側の BGP セッションのための ASN は、仮想プライベートゲートウェイから継承されます。仮想プライベートゲートウェイを作成するときに、独自のプライベート ASN を指定できます。そうでない場合は、Amazon によってデフォルトの ASN が指定されます。詳細については、Amazon VPC ユーザーガイドの Create a Virtual Private Gateway を参照してください。Direct Connect Gateway 経由で VPC に接続する場合は、Direct Connect Gateway が必要です。詳細については、「Direct Connect Gateway」を参照してください。
VLAN	仮想ローカルエリアネットワーク (VLAN) の、まだ接続で使用されていない一意のタグ。値は 1 ~ 4094 を指定する必要があります。またイーサネット 802.1Q 規格を満たしている必要があります。このタグは、 AWS Direct Connect 接続を通過するすべてのトラフィックに必要です。 ホスト接続がある場合、 AWS Direct Connect パートナーはこの値を提供します。仮想インターフェイス作成後に値を変更することはできません。

リソース	必要な情報

ピア IP アドレス	仮想インターフェイスは、IPv4 または IPv6 に対して 1 つの BGP ピアリングセッションをサポートできます。または両方に対して 1 つずつ BGP ピアリングセッションをサポートできます (デュアルスタック)。パブリック仮想インターフェイスの作成に Amazon プールからの Elastic IP (EIP) および Bring your own IP アドレス (BYOIP) を使用して作成しないでください。同じ仮想インターフェイスで同じ IP アドレスファミリに対して複数の BGP セッションを作成することはできません。BGP ピアセッションでは、仮想インターフェイスの両端に IP アドレス範囲が割り当てられます。
	
	• IPv4:
	  • (パブリック仮想インターフェイスのみ) お客様が所有している一意のパブリック IPv4 アドレスを指定する必要があります。以下のいずれかを指定できます。
	  • カスタマー所有 IPv4 CIDR
	
	これらは任意のパブリック IPs (顧客所有または が提供する AWS) にすることができますが、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、などの/31範囲を割り当てる場合は、ピア IP 203.0.113.0 にを203.0.113.0/31 、 AWS ピア IP 203.0.113.1 に を使用できます。または、 などの/24範囲を割り当てる場合は、ピア IP 198.51.100.10 に を198.51.100.0/24 、 AWS ピア IP 198.51.100.20 に を使用できます。
	  • AWS Direct Connect パートナーまたは ISP が所有する IP 範囲と LOA-CFA 認証
	  • AWSが提供する /31 CIDR。AWS Support に連絡して、パブリック IPv4 CIDR をリクエストします (リクエストにはユースケースを提供します)
	
	Note
	AWSが提供するパブリック IPv4 アドレスに対するすべてのリクエストを当社が処理できることを保証することはできません。

リソース	必要な情報
	• (プライベート仮想インターフェイスのみ) Amazon がプライベート IPv4 アドレスを自動的に生成できます。独自の CIDRs を指定してください。 AWS 例えば、ローカルネットワークから他の IP アドレスを指定しないでください。パブリック仮想インターフェイスと同様に、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、 などの/30範囲を割り当てる場合は、ピア IP 192.168.0.1 に を192.168.0.0/30 、 AWS ピア IP 192.168.0.2 に を使用できます。 • IPv6: Amazon は /125 IPv6 CIDR を自動的に割り当てます。独自のピア IPv6 アドレスを指定することはできません。
アドレスファミリー	BGP ピアリングセッションが IPv4 と IPv6 のどちらを使用するか。
BGP 情報	• BGP セッションのお客様側のパブリックまたはプライベート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)。パブリック ASN を使用する場合は、お客様が所有者であることが必要です。プライベート ASN を使用している場合は、カスタム ASN 値を設定できます。16 ビット ASN では、値は 64512 から 65534 の範囲内である必要があります。32 ビット ASN では、値は 1 から 2,147,483,647 の範囲内である必要があります。パブリック仮想インターフェイス用のプライベート ASN を使用する場合、自律システム (AS) の前置は動作しません。 • AWS はデフォルトで MD5 を有効にします。この値を変更することはできません。 • MD5 BGP 認証キー。独自のキーを指定するか、Amazon で自動的に生成することができます。

リソース	必要な情報

(パブリック仮想インターフェイスのみ) アドバタイズするプレフィックス	BGP 経由でアドバタイズするパブリックの IPv4 ルートまたは IPv6 ルート。BGP を使用して少なくとも 1 つ (最大 1,000 個) のプレフィックスをアドバタイズする必要があります。
	• IPv4: IPv4 CIDR は、次のいずれか AWS Direct Connect に該当する場合、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs異なる AWS リージョンから取得されます。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• IPv6: /64 以下のプレフィックスの長さを指定します。
	• AWS Support に連絡することによって、既存のパブリック VIF にプレフィックスを追加し、それらをアドバタイズすることができます。サポートケースで、パブリック VIF に追加してアドバタイズしたい追加の CIDR プレフィックスのリストを提供してください。
	• Direct Connect パブリック仮想インターフェイスでは、任意のプレフィックス長を指定できます。IPv4 は /1 から /32 までのすべてをサポートし、IPv6 は /1 から /64 までのすべてをサポートする必要があります。

リソース	必要な情報
(プライベート仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェースの MTU を 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。ジャンボフレームは、 から伝播されたルートにのみ適用されます AWS Direct Connect。仮想プライベートゲートウェイを指すルートテーブルに静的ルートを追加する場合、静的ルートを介してルーティングされるトラフィックは 1500 MTU を使用して送信されます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでジャンボフレームを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが使用可能かどうかを確認します。
(トランジット仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェイスの MTU を 8500 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。Direct Connect では、最大 8500 MTU のジャンボフレームがサポートされます。Transit Gateway ルートテーブルで設定された静的なルートと伝播されたルートはジャンボフレームをサポートします。これには、VPC の静的なルートテーブルのエントリを持つ EC2 インスタンスから Transit Gateway アタッチメントへのものが含まれます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでジャンボフレームを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが使用可能かどうかを確認します。

パブリックプレフィックスまたは ASNs が ISP またはネットワークキャリアに属している場合、 はユーザーに追加情報 AWS をリクエストします。これは、ネットワークプレフィックス/ASN をお客様が使用できることを確認する、会社の正式なレターヘッドを使用したドキュメント、または会社のドメイン名からの E メールとすることができます。

パブリック仮想インターフェイスを作成すると、 がリクエストを確認して承認 AWS するまでに最大 72 時間かかる場合があります。

非 VPC サービスへのパブリック仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [パブリック] を選択します。
5. [Public Virtual Interface settings (仮想インターフェイス設定)] で以下を実行します。

   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

   c. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

   d. [BGP ASN] に、ゲートウェイ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) を入力します。

      有効な値は 1 ~ 2147483647 です。
6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

      - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
      - [Amazon ルーターのピア IP] に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

      [IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

   b. 独自の BGP キーを指定するには、使用する BGP MD5 キーを入力します。

      値が入力されない場合は、当社の側で自動的に BGP キーを生成します。

c. Amazon にプレフィックスを発行するには、[アドバタイズするプレフィックス] に、この仮想インターフェイスを介してルーティングされるトラフィックのルーティング先となる IPv4 CIDR アドレスをカンマで区切って入力します。

d. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

VPC へのプライベート仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [プライベート] を選択します。
5. [プライベート仮想インターフェイス設定] で以下を実行します。

a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

c. [ゲートウェイタイプ] で、[仮想プライベートゲートウェイ] または [Direct Connect ゲートウェイ] を選択します。

d. 仮想インターフェイス所有者 で、別の AWS アカウント を選択し、 AWS アカウントを入力します。

e. [仮想プライベートゲートウェイ] で、このインターフェイスに使用する仮想プライベートゲートウェイを選択します。

f. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

g. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

有効な値は 1 ~ 2,147,483,647 です。

6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

      - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
      - [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

      > **Important**
      >
      > IPv4 アドレス AWS の自動割り当てを許可すると、RFC 3927 に従って 169.254.0.0/16 IPv4 Link-Local から /29 CIDR が接続用に割り当てられます。VPC point-to-point AWS トラフィックの送信元および/または送信先としてカスタマールーターピア IP アドレスを使用する場合は、このオプションは推奨されません。代わりに、RFC 1918 または他のアドレスを使用して、アドレスを自分で指定する必要があります。
      >
      > - RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。
      > - RFC 3927 の詳細については、「IPv4 リンクローカルアドレスのダイナミック設定」を参照してください。

      [IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

   b. 最大送信単位 (MTU) を 1500 (デフォルト) から 9001 (ジャンボフレーム) に変更するには、[ジャンボ MTU (MTU サイズ 9001)] を選択します。

   c. (オプション) の有効化 SiteLinkで、有効化 を選択して Direct Connect のプレゼンスポイント間の直接接続を有効にします。

   d. (オプション) タグを追加または削除します。

      [タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

ステップ 4: 仮想インターフェイスの構成の回復性を確認する

AWS クラウドまたは Amazon VPC への仮想インターフェイスを確立したら、仮想インターフェイスのフェイルオーバーテストを実行して、設定が障害耐性要件を満たしていることを確認します。詳細については、「the section called “AWS Direct Connect フェイルオーバーテスト”」を参照してください。

ステップ 5: 仮想インターフェイス接続を検証する

AWS クラウドまたは Amazon VPC への仮想インターフェイスを確立したら、次の手順を使用して AWS Direct Connect 接続を検証できます。

AWS クラウドへの仮想インターフェイス接続を確認するには

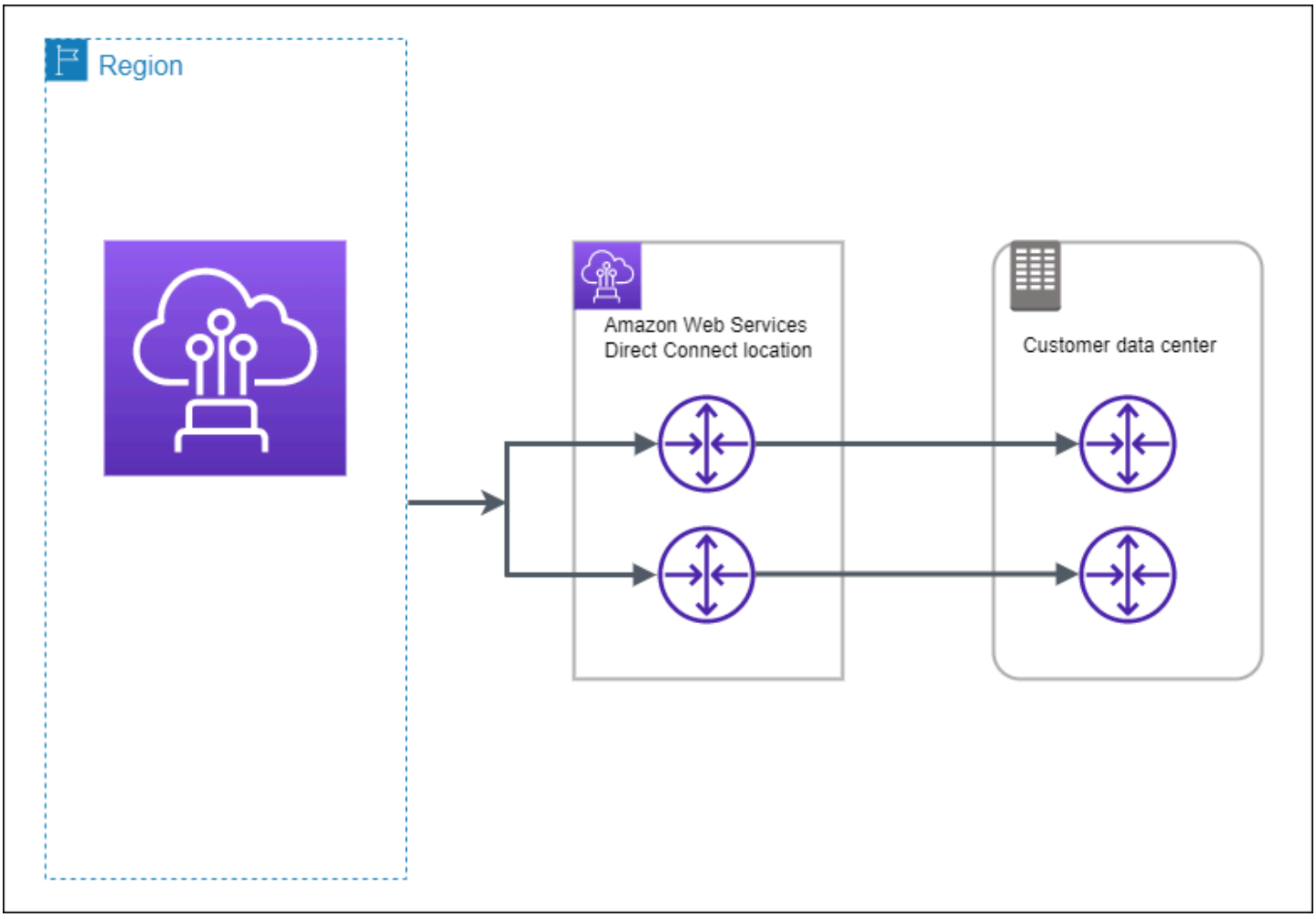
- を実行し`traceroute`、 AWS Direct Connect 識別子がネットワークトレースにあることを確認します。

Amazon VPC への仮想インターフェイス接続を検証するには

1. Amazon Linux AMI など Ping に応答する AMI を使用して、仮想プライベートゲートウェイにアタッチされている VPC に EC2 インスタンスを起動します。Amazon EC2 コンソールのインスタンス起動ウィザードを使用すれば、Amazon Linux AMI を [Quick Start (クイックスタート)] タブで使用することができます。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの起動」を参照してください。 Amazon EC2 インスタンスに関連付けられたセキュリティグループに、インバウンド ICMP トラフィックを許可するルール (ping リクエストの場合) が含まれていることを確認します。
2. インスタンスが実行中になった後、そのプライベート IPv4 アドレス (たとえば 10.0.0.4) を取得します。Amazon EC2 コンソールにインスタンスの詳細の一部としてアドレスが表示されます。
3. プライベート IPv4 アドレスに Ping を実行し、応答を確認します。

開発とテスト

クリティカルでないワークロードの開発とテストの回復性を実現するには、1 つの場所にある別々のデバイスを終端とする別々の接続を使用します (以下の図を参照)。このモデルは、デバイスの障害に対する回復性を提供しますが、ロケーションの障害に対する回復性は提供しません。



次の手順は、Resiliency Toolkit AWS Direct Connect を使用して開発およびテストの回復性モデルを設定する方法を示しています。

トピック

- ステップ 1: にサインアップする AWS
- ステップ 2: 回復性モデルを設定する
- ステップ 3: 仮想インターフェイスを作成する
- ステップ 4: 仮想インターフェイスの構成の回復性を確認する
- ステップ 5: 作成した仮想インターフェイスを検証する

ステップ 1: にサインアップする AWS

を使用するには AWS Direct Connect、アカウントをまだお持ちでない場合は、 AWS アカウントが必要です。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [アカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「ルートユーザーとしてサインインする」を参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の AWS アカウント 「ルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 ユーザーガイド」の「デフォルト でユーザーアクセス IAM アイデンティティセンターディレクトリを設定するAWS IAM Identity Center 」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、「 AWS サインイン ユーザーガイド」の AWS 「 アクセスポータルへのサインイン」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの参加」を参照してください。

ステップ 2: 回復性モデルを設定する

回復性モデルを設定するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [接続] を選択し、[接続の作成] を選択します。
3. [Connection ordering type] の [Connection wizard] を選択します。
4. [回復性レベル] で、[開発とテスト]、[Next (次へ)] の順に選択します。
5. [Configure connections (接続の構成)] ペインの [Connection settings (接続設定)] で、以下を実行します。

   a. [帯域幅] で、接続の帯域幅を選択します。

      この帯域幅は、作成されたすべての接続に適用されます。

   b. 最初のロケーションサービスプロバイダー で、適切な AWS Direct Connect ロケーションを選択します。

   c. 該当する場合は、[First Sub location] で、お客様、またはお客様のネットワークプロバイダに最も近いフロアを選択します。このオプションは、ロケーションで建物の複数のフロアに会議室 (MMR) がある場合のみ利用できます。

   d. [First location service provider] で [Other] を選択した場合は、[プロバイダーの名前] に、使用するパートナーの名前を入力します。

   e. (オプション) タグを追加または削除します。

      [タグの追加] [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。

      [タグの削除] タグの横にある [タグの削除] を選択します。
6. [Next] を選択します。
7. 接続を確認し、[Continue] を選択します。

   LOA の準備ができたら [Download LOA] を選択し、[Continue] を選択します。

   がリクエストを確認し、接続用のポートをプロビジョニング AWS するまでに最大 72 時間かかる場合があります。この時間中、ユースケースまたは指定された場所に関する詳細情報のリクエ

ストを含む E メールが送信される場合があります。E メールは、 にサインアップしたときに使用した E メールアドレスに送信されます AWS。7 日以内に応答する必要があり、応答しないと接続は削除されます。

ステップ 3: 仮想インターフェイスを作成する

AWS Direct Connect 接続の使用を開始するには、仮想インターフェイスを作成する必要があります。プライベート仮想インターフェイスを作成して、VPC に接続することができます。または、パブリック仮想インターフェイスを作成して、VPC にないパブリック AWS サービスに接続することもできます。VPC へのプライベート仮想インターフェイスを作成するときは、接続する VPC ごとにプライベート仮想インターフェイスが必要です。たとえば、3 つの VPC に接続するには 3 つのプライベート仮想インターフェイスが必要です。

作業を開始する前に、次の情報が揃っていることを確認してください。

リソース	必要な情報
Connection	仮想インターフェイスを作成する AWS Direct Connect 接続またはリンク集約グループ (LAG)。
仮想インターフェイス名	仮想インターフェイスの名前。
仮想インターフェイス所有者	別の アカウントの仮想インターフェイスを作成する場合は、他の AWS アカウントのアカウント ID が必要です。
(プライベート仮想インターフェイスのみ) 接続	同じ AWS リージョンの VPC に接続するには、VPC の仮想プライベートゲートウェイが必要です。Amazon 側の BGP セッションのための ASN は、仮想プライベートゲートウェイから継承されます。仮想プライベートゲートウェイを作成するときに、独自のプライベート ASN を指定できます。そうでない場合は、Amazon によってデフォルトの ASN が指定されます。詳細については、Amazon VPC ユーザーガイドの Create a Virtual Private Gateway を参照してください。Direct Connect Gateway 経由で VPC に接続する場合は、Direct Connect Gateway が必要です。詳細については、「Direct Connect Gateway」を参照してください。
VLAN	仮想ローカルエリアネットワーク (VLAN) の、まだ接続で使用されていない一意のタグ。値は 1 ~ 4094 を指定する必要があります。またイーサネッ

リソース	必要な情報
	ト 802.1Q 規格を満たしている必要があります。このタグは、 AWS Direct Connect 接続を通過するすべてのトラフィックに必要です。 ホスト接続がある場合、 AWS Direct Connect パートナーはこの値を提供します。仮想インターフェイス作成後に値を変更することはできません。

リソース	必要な情報

ピア IP アドレス	仮想インターフェイスは、IPv4 または IPv6 に対して 1 つの BGP ピアリングセッションをサポートできます。または両方に対して 1 つずつ BGP ピアリングセッションをサポートできます (デュアルスタック)。パブリック仮想インターフェイスの作成に Amazon プールからの Elastic IP (EIP) および Bring your own IP アドレス (BYOIP) を使用して作成しないでください。同じ仮想インターフェイスで同じ IP アドレスファミリに対して複数の BGP セッションを作成することはできません。BGP ピアセッションでは、仮想インターフェイスの両端に IP アドレス範囲が割り当てられます。
	
	• IPv4:
	  • (パブリック仮想インターフェイスのみ) お客様が所有している一意のパブリック IPv4 アドレスを指定する必要があります。以下のいずれかを指定できます。
	  • カスタマー所有 IPv4 CIDR
	
	これらは任意のパブリック IPs (顧客所有または が提供する AWS) にすることができますが、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、などの/31範囲を割り当てる場合は、ピア IP 203.0.113.0 にを203.0.113.0/31 、 AWS ピア IP 203.0.113.1 に を使用できます。または、 などの/24範囲を割り当てる場合は、ピア IP 198.51.100.10 に を198.51.100.0/24 、 AWS ピア IP 198.51.100.20 に を使用できます。
	  • AWS Direct Connect パートナーまたは ISP が所有する IP 範囲と LOA-CFA 認証
	  • AWSが提供する /31 CIDR。AWS Support に連絡して、パブリック IPv4 CIDR をリクエストします (リクエストにはユースケースを提供します)
	
	Note
	AWSが提供するパブリック IPv4 アドレスに対するすべてのリクエストを当社が処理できることを保証することはできません。

リソース	必要な情報
	• (プライベート仮想インターフェイスのみ) Amazon がプライベート IPv4 アドレスを自動的に生成できます。独自の CIDRs を指定してください。 AWS 例えば、ローカルネットワークから他の IP アドレスを指定しないでください。パブリック仮想インターフェイスと同様に、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、 などの/30範囲を割り当てる場合は、ピア IP 192.168.0.1 に を192.168.0.0/30 、 AWS ピア IP 192.168.0.2 に を使用できます。 • IPv6: Amazon は /125 IPv6 CIDR を自動的に割り当てます。独自のピア IPv6 アドレスを指定することはできません。
アドレスファミリー	BGP ピアリングセッションが IPv4 と IPv6 のどちらを使用するか。
BGP 情報	• BGP セッションのお客様側のパブリックまたはプライベート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)。パブリック ASN を使用する場合は、お客様が所有者であることが必要です。プライベート ASN を使用している場合は、カスタム ASN 値を設定できます。16 ビット ASN では、値は 64512 から 65534 の範囲内である必要があります。32 ビット ASN では、値は 1 から 2,147,483,647 の範囲内である必要があります。パブリック仮想インターフェイス用のプライベート ASN を使用する場合、自律システム (AS) の前置は動作しません。 • AWS はデフォルトで MD5 を有効にします。この値を変更することはできません。 • MD5 BGP 認証キー。独自のキーを指定するか、Amazon で自動的に生成することができます。

リソース	必要な情報

(パブリック仮想インターフェイスのみ) アドバタイズするプレフィックス	BGP 経由でアドバタイズするパブリックの IPv4 ルートまたは IPv6 ルート。BGP を使用して少なくとも 1 つ (最大 1,000 個) のプレフィックスをアドバタイズする必要があります。
	• IPv4: IPv4 CIDR は、次のいずれか AWS Direct Connect に該当する場合、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs異なる AWS リージョンから取得されます。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• IPv6: /64 以下のプレフィックスの長さを指定します。
	• AWS Support に連絡することによって、既存のパブリック VIF にプレフィックスを追加し、それらをアドバタイズすることができます。サポートケースで、パブリック VIF に追加してアドバタイズしたい追加の CIDR プレフィックスのリストを提供してください。
	• Direct Connect パブリック仮想インターフェイスでは、任意のプレフィックス長を指定できます。IPv4 は /1 から /32 までのすべてをサポートし、IPv6 は /1 から /64 までのすべてをサポートする必要があります。

リソース	必要な情報
(プライベート仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェースの MTU を 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。ジャンボフレームは、 から伝播されたルートにのみ適用されます AWS Direct Connect。仮想プライベートゲートウェイを指すルートテーブルに静的ルートを追加する場合、静的ルートを介してルーティングされるトラフィックは 1500 MTU を使用して送信されます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでジャンボフレームを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが対応しているかどうかを確認します。
(トランジット仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェイスの MTU を 8500 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。Direct Connect では、最大 8500 MTU のジャンボフレームがサポートされます。Transit Gateway ルートテーブルで設定された静的なルートと伝播されたルートはジャンボフレームをサポートします。これには、VPC の静的なルートテーブルのエントリを持つ EC2 インスタンスから Transit Gateway アタッチメントへのものが含まれます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでジャンボフレームを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが使用可能かどうかを確認します。

お客様のパブリックプレフィックスまたは ASN が、ISP またはネットワークキャリアに属している場合には、当社からお客様に対し追加の情報がリクエストされます。これは、ネットワークプレフィックス/ASN をお客様が使用できることを確認する、会社の正式なレターヘッドを使用したドキュメント、または会社のドメイン名からの E メールとすることができます。

パブリック仮想インターフェイスを作成する場合、 AWS がリクエストを確認し、承認するまでに最大 72 時間かかる場合があります。

非 VPC サービスへのパブリック仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [パブリック] を選択します。
5. [Public Virtual Interface settings (仮想インターフェイス設定)] で以下を実行します。

   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

   c. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

   d. [BGP ASN] に、ゲートウェイ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) を入力します。

      有効な値は 1 ~ 2147483647 です。
6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

      - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
      - [Amazon ルーターのピア IP] に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

      [IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

   b. 独自の BGP キーを指定するには、使用する BGP MD5 キーを入力します。

      値が入力されない場合は、当社の側で自動的に BGP キーを生成します。

c. Amazon にプレフィックスを発行するには、[アドバタイズするプレフィックス] に、この仮想インターフェイスを介してルーティングされるトラフィックのルーティング先となる IPv4 CIDR アドレスをカンマで区切って入力します。

d. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

VPC へのプライベート仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [プライベート] を選択します。
5. [プライベート仮想インターフェイス設定] で以下を実行します。

a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

c. [ゲートウェイタイプ] で、[仮想プライベートゲートウェイ] または [Direct Connect ゲートウェイ] を選択します。

d. 仮想インターフェイス所有者 で、別の AWS アカウント を選択し、 AWS アカウントを入力します。

e. [仮想プライベートゲートウェイ] で、このインターフェイスに使用する仮想プライベートゲートウェイを選択します。

f. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

g. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

有効な値は 1 ~ 2,147,483,647 です。

6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

      - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
      - [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

      > **Important**
      >
      > IPv4 アドレス AWS の自動割り当てを許可すると、RFC 3927 に従って 169.254.0.0/16 IPv4 Link-Local から /29 CIDR が接続用に割り当てられます。VPC point-to-point AWS トラフィックの送信元および/または送信先としてカスタマールーターピア IP アドレスを使用する場合は、このオプションは推奨されません。代わりに、RFC 1918 または他のアドレスを使用して、アドレスを自分で指定する必要があります。
      >
      > - RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。
      > - RFC 3927 の詳細については、「IPv4 リンクローカルアドレスのダイナミック設定」を参照してください。

      [IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

   b. 最大送信単位 (MTU) を 1500 (デフォルト) から 9001 (ジャンボフレーム) に変更するには、[ジャンボ MTU (MTU サイズ 9001)] を選択します。

   c. （ オプション ）「 を有効にする SiteLink」で「有効」を選択して、Direct Connect のプレゼンスポイント間の直接接続を有効にします。

   d. (オプション) タグを追加または削除します。

      [タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

ステップ 4: 仮想インターフェイスの構成の回復性を確認する

AWS クラウドまたは Amazon VPC への仮想インターフェイスを確立したら、仮想インターフェイスのフェイルオーバーテストを実行して、設定が障害耐性要件を満たしていることを確認します。詳細については、「the section called “AWS Direct Connect フェイルオーバーテスト”」を参照してください。

ステップ 5: 作成した仮想インターフェイスを検証する

AWS クラウドまたは Amazon VPC への仮想インターフェイスを確立したら、次の手順を使用して AWS Direct Connect 接続を検証できます。

AWS クラウドへの仮想インターフェイス接続を確認するには

- を実行し`traceroute`、 AWS Direct Connect 識別子がネットワークトレースにあることを確認します。

Amazon VPC への仮想インターフェイス接続を検証するには

1. Amazon Linux AMI など Ping に応答する AMI を使用して、仮想プライベートゲートウェイにアタッチされている VPC に EC2 インスタンスを起動します。Amazon EC2 コンソールのインスタンス起動ウィザードを使用すれば、Amazon Linux AMI を [Quick Start (クイックスタート)] タブで使用することができます。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの起動」を参照してください。 Amazon EC2 インスタンスに関連付けられたセキュリティグループに、インバウンド ICMP トラフィックを許可するルール (ping リクエストの場合) が含まれていることを確認します。
2. インスタンスが実行中になった後、そのプライベート IPv4 アドレス (たとえば 10.0.0.4) を取得します。Amazon EC2 コンソールにインスタンスの詳細の一部としてアドレスが表示されます。
3. プライベート IPv4 アドレスに Ping を実行し、応答を確認します。

Classic

既存の接続がある場合は、[Classic] を選択します。

次の手順では、 AWS Direct Connect 接続をセットアップするための一般的なシナリオを示しています。

内容

前提条件

ポート速度 AWS Direct Connect が 1 Gbps 以上の への接続では、ネットワークが次の要件を満たしていることを確認します。

- ネットワークでは、1 ギガビットイーサネットの場合は 1000BASE-LX (1310 nm) トランシーバー、10 ギガビットイーサネットの場合は 10GBASE-LR (1310 nm) トランシーバー、100 ギガビットイーサネットの場合は 100GBASE-LR4 トランシーバーでシングルモードファイバーを使用する必要があります。
- ポート速度が 1 Gbps を超える接続では、ポートのオートネゴシエーションを無効にする必要があります。ただし、接続を提供する AWS Direct Connect エンドポイントによっては、1 Gbps 接続で自動ネゴシエーションを有効または無効にする必要がある場合があります。仮想インターフェイスがダウンしたままの場合は、レイヤー 2 (データリンク層) 問題のトラブルシューティング を参照してください。
- 802.1Q VLAN のカプセル化が、中間デバイスを含む接続全体でサポートされている必要があります。
- デバイスがボーダーゲートウェイプロトコル (BGP) と BGP MD5 認証をサポートしている必要があります。

- (省略可能) ご使用のネットワークで双方向フォワーディング検出 (BFD) プロトコルを設定できます。非同期 BFD は、 AWS Direct Connect 仮想インターフェイスごとに自動的に有効になります。Direct Connect 仮想インターフェイスに対して自動的に有効になりますが、お客様のルーターで設定するまでは利用可能になりません。詳細については、「Enable BFD for a Direct Connect connection」(Direct Connect 接続に対して BFD を有効にする) を参照してください。

ステップ 1: にサインアップする AWS

を使用するには AWS Direct Connect、まだアカウントをお持ちでない場合は、アカウントが必要です。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [アカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「ルートユーザーとしてサインインする」を参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の AWS アカウント 「ルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 ユーザーガイド」の「デフォルト でユーザーアクセスを設定する IAM アイデンティティセンターディレクトリAWS IAM Identity Center 」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、「 AWS サインイン ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの参加」を参照してください。

ステップ 2: AWS Direct Connect 専用接続をリクエストする

専用接続の場合は、 AWS Direct Connect コンソールを使用して接続リクエストを送信できます。ホスト接続の場合は、 AWS Direct Connect パートナーと協力してホスト接続をリクエストします。次の情報があることを確認します。

- 必要なポートスピード。接続リクエストの作成後にポート速度を変更することはできません。
- 接続を終了する AWS Direct Connect 場所。

> **Note**
>
> AWS Direct Connect コンソールを使用してホスト接続をリクエストすることはできません。代わりに、ホスト接続を作成できる AWS Direct Connect パートナーに連絡して、受け入れてください。次の手順をスキップして「 ホスト接続の許可」に進みます。

新しい AWS Direct Connect 接続を作成するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [接続] を選択し、[接続の作成] を選択します。
3. [Classic] を選択します。
4. [接続の作成] ペインの [Connection settings (接続の設定)] で、以下を実行します。

   a. [名前] に、接続の名前を入力します。

   b. [Location (場所)] で、適切な AWS Direct Connect の場所を選択します。

c. 該当する場合は、[サブロケーション] で、お客様、またはお客様のネットワークプロバイダーに最も近いフロアを選択します。このオプションは、ロケーションで建物の複数のフロアに会議室 (MMR) がある場合のみ該当します。

d. [ポートスピード] で接続帯域幅を選択します。

e. オンプレミス では、この接続を使用してデータセンターに接続するときに、 AWS Direct Connect パートナー経由で接続を選択します。

f. サービスプロバイダー で、 AWS Direct Connect パートナーを選択します。リストにないパートナーを使用する場合は、[Other] を選択します。

g. [サービスプロバイダー] で [Other] を選択した場合は、[プロバイダーの名前] に、使用するパートナーの名前を入力します。

h. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

5. [接続の作成] を選択します。

がリクエストを確認し、接続用のポートをプロビジョニング AWS するまでに最大 72 時間かかる場合があります。この時間中、ユースケースまたは指定された場所に関する詳細情報のリクエストを含む E メールが送信される場合があります。E メールは、 にサインアップしたときに使用した E メールアドレスに送信されます AWS。7 日以内に応答する必要があり、応答しないと接続は削除されます。

詳細については、「AWS Direct Connect 接続」を参照してください。

ホスト接続の許可

仮想インターフェイスを作成する前に、 AWS Direct Connect コンソールでホスト接続を受け入れる必要があります。このステップは、ホスト接続にのみ適用されます。

ホスト仮想インターフェイスを承諾するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Connections (接続)] を選択します。

3. ホスト接続を選択し、[承諾] を選択します。

   [Accept (承諾)] を選択します。

(専用接続) ステップ 3: LOA-CFA をダウンロードする

接続がリクエストされると、当社は、Letter of Authorization and Connecting Facility Assignment (LOA-CFA) をダウンロード可能にするか、追加情報をリクエストする E メールを送信します。LOA-CFA は、 に接続するための認可であり AWS、ネットワーク間接続 (クロスコネクト) を確立するには、コロケーションプロバイダーまたはネットワークプロバイダーが必要とするものです。

LOA-CFA のダウンロード方法

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Connections (接続)] を選択します。
3. 接続を選択したら、[View Details (詳細の表示)] を選択します。
4. [Download LOA-CFA] を選択します。

   LOA-CFA が PDF ファイルとしてコンピュータにダウンロードされます。

   > **Note**
   >
   > リンクが有効になっていない場合、LOA-CFA がまだダウンロード可能になっていません。追加情報のリクエストメールを確認します。それでもダウンロードできない、または 72 時間経過してもメールが届かない場合は、AWS Support にお問い合わせください。

5. LOA-CFA をダウンロードしたら、次のいずれかを実行します。

   - AWS Direct Connect パートナーまたはネットワークプロバイダーと連携している場合は、ロケーションでクロスコネクトを注文できるように LOA-CFA を送信します AWS Direct Connect 。メンバーまたはプロバイダがクロスコネクトをお客様に代わって注文できない場合は、直接コロケーションプロバイダにお問い合わせください。
   - AWS Direct Connect ロケーションに機器がある場合は、コロケーションプロバイダーに連絡してクロスネットワーク接続をリクエストしてください。お客様はコロケーションプロバイダーの顧客である必要があります。また、 AWS ルーターへの接続を許可する LOA-CFA と、ネットワークに接続するために必要な情報も提示する必要があります。

AWS Direct Connect 複数のサイト (Equinix DC1-DC6 や DC10-DC11 など) としてリストされているロケーションは、キャンパスとして設定されます。お客様またはネットワークプロバイダの機器がこれらのいずれかのサイトに配置されている場合は、キャンパスの別の建物に存在している場合でも、割り当てられたポートへのクロスコネクトをリクエストできます。

> **Important**
>
> キャンパスは単一の AWS Direct Connect 場所として扱われます。高可用性を実現するために、別の AWS Direct Connect ロケーションへの接続を設定します。

お客様またはネットワークプロバイダーに、物理的な接続の確立に関する問題が発生した場合は、「レイヤー 1 (物理層) 問題のトラブルシューティング」を参照してください。

ステップ 4: 仮想インターフェイスを作成する

AWS Direct Connect 接続の使用を開始するには、仮想インターフェイスを作成する必要があります。プライベート仮想インターフェイスを作成して、VPC に接続することができます。または、パブリック仮想インターフェイスを作成して、VPC にないパブリック AWS サービスに接続することもできます。VPC へのプライベート仮想インターフェイスを作成するときは、接続する VPC ごとにプライベート仮想インターフェイスが必要です。たとえば、3 つの VPC に接続するには 3 つのプライベート仮想インターフェイスが必要です。

作業を開始する前に、次の情報が揃っていることを確認してください。

リソース	必要な情報
Connection	仮想インターフェイスを作成する AWS Direct Connect 接続またはリンク集約グループ (LAG)。
仮想インターフェイス名	仮想インターフェイスの名前。
仮想インターフェイス所有者	別の アカウントの仮想インターフェイスを作成する場合は、他の AWS アカウントのアカウント ID が必要です。
(プライベート仮想インターフェイスのみ) 接続	同じ AWS リージョンの VPC に接続するには、VPC の仮想プライベートゲートウェイが必要です。Amazon 側の BGP セッションのための ASN は、仮想プライベートゲートウェイから継承されます。仮想プライベートゲー

リソース	必要な情報
	トウェイを作成するときに、独自のプライベート ASN を指定できます。そうでない場合は、Amazon によってデフォルトの ASN が指定されます。詳細については、Amazon VPC ユーザーガイドの Create a Virtual Private Gateway を参照してください。Direct Connect Gateway 経由で VPC に接続する場合は、Direct Connect Gateway が必要です。詳細については、「Direct Connect Gateway」を参照してください。
VLAN	仮想ローカルエリアネットワーク (VLAN) の、まだ接続で使用されていない一意のタグ。値は 1 ~ 4094 を指定する必要があります。またイーサネット 802.1Q 規格を満たしている必要があります。このタグは、 AWS Direct Connect 接続を通過するすべてのトラフィックに必要です。 ホスト接続がある場合、 AWS Direct Connect パートナーはこの値を提供します。仮想インターフェイス作成後に値を変更することはできません。

リソース	必要な情報

ピア IP アドレス	仮想インターフェイスは、IPv4 または IPv6 に対して 1 つの BGP ピアリングセッションをサポートできます。または両方に対して 1 つずつ BGP ピアリングセッションをサポートできます (デュアルスタック)。パブリック仮想インターフェイスの作成に Amazon プールからの Elastic IP (EIP) および Bring your own IP アドレス (BYOIP) を使用して作成しないでください。同じ仮想インターフェイスで同じ IP アドレスファミリに対して複数の BGP セッションを作成することはできません。BGP ピアセッションでは、仮想インターフェイスの両端に IP アドレス範囲が割り当てられます。
	
	• IPv4:
	  • (パブリック仮想インターフェイスのみ) お客様が所有している一意のパブリック IPv4 アドレスを指定する必要があります。以下のいずれかを指定できます。
	  • カスタマー所有 IPv4 CIDR
	
	これらは任意のパブリック IPs (顧客所有または が提供する AWS) にすることができますが、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、などの/31範囲を割り当てる場合は、ピア IP 203.0.113.0 にを203.0.113.0/31 、 AWS ピア IP 203.0.113.1 に を使用できます。または、 などの/24範囲を割り当てる場合は、ピア IP 198.51.100.10 に を198.51.100.0/24 、 AWS ピア IP 198.51.100.20 に を使用できます。
	  • AWS Direct Connect パートナーまたは ISP が所有する IP 範囲と LOA-CFA 認証
	  • AWSが提供する /31 CIDR。AWS Support に連絡して、パブリック IPv4 CIDR をリクエストします (リクエストにはユースケースを提供します)
	
	Note
	AWSが提供するパブリック IPv4 アドレスに対するすべてのリクエストを当社が受理できることを保証することはできません。

リソース	必要な情報
	• (プライベート仮想インターフェイスのみ) Amazon がプライベート IPv4 アドレスを自動的に生成できます。独自の CIDRs を指定してください。 AWS 例えば、ローカルネットワークから他の IP アドレスを指定しないでください。パブリック仮想インターフェイスと同様に、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、 などの/30範囲を割り当てる場合、ピア IP 192.168.0.1 には を192.168.0.0/30 、 AWS ピア IP 192.168.0.2 には を使用できます。 • IPv6: Amazon は /125 IPv6 CIDR を自動的に割り当てます。独自のピア IPv6 アドレスを指定することはできません。
アドレスファミリー	BGP ピアリングセッションが IPv4 と IPv6 のどちらを使用するか。
BGP 情報	• BGP セッションのお客様側のパブリックまたはプライベート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)。パブリック ASN を使用する場合は、お客様が所有者であることが必要です。プライベート ASN を使用している場合は、カスタム ASN 値を設定できます。16 ビット ASN では、値は 64512 から 65534 の範囲内である必要があります。32 ビット ASN では、値は 1 から 2,147,483,647 の範囲内である必要があります。パブリック仮想インターフェイス用のプライベート ASN を使用する場合、自律システム (AS) の前置は動作しません。 • AWS はデフォルトで MD5 を有効にします。この値を変更することはできません。 • MD5 BGP 認証キー。独自のキーを指定するか、Amazon で自動的に生成することができます。

リソース	必要な情報

(パブリック仮想インターフェイスのみ) アドバタイズするプレフィックス	BGP 経由でアドバタイズするパブリックの IPv4 ルートまたは IPv6 ルート。BGP を使用して少なくとも 1 つ (最大 1,000 個) のプレフィックスをアドバタイズする必要があります。
	• IPv4: IPv4 CIDR は、次のいずれか AWS Direct Connect に該当する場合、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs異なる AWS リージョンから取得されます。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• IPv6: /64 以下のプレフィックスの長さを指定します。
	• AWS Support に連絡することによって、既存のパブリック VIF にプレフィックスを追加し、それらをアドバタイズすることができます。サポートケースで、パブリック VIF に追加してアドバタイズしたい追加の CIDR プレフィックスのリストを提供してください。
	• Direct Connect パブリック仮想インターフェイスでは、任意のプレフィックス長を指定できます。IPv4 は /1 から /32 までのすべてをサポートし、IPv6 は /1 から /64 までのすべてをサポートする必要があります。

リソース	必要な情報
(プライベート仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェースの MTU を 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。ジャンボフレームは、 から伝播されたルートにのみ適用されます AWS Direct Connect。仮想プライベートゲートウェイを指すルートテーブルに静的ルートを追加する場合、静的ルートを介してルーティングされるトラフィックは 1500 MTU を使用して送信されます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでそれを選択し、仮想インターフェイスの一般的な設定ページで使用可能なジャンボフレームを見つけます。
(トランジット仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェイスの MTU を 8500 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。Direct Connect では、最大 8500 MTU のジャンボフレームがサポートされます。Transit Gateway ルートテーブルで設定された静的なルートと伝播されたルートはジャンボフレームをサポートします。これには、VPC の静的なルートテーブルのエントリを持つ EC2 インスタンスから Transit Gateway アタッチメントへのものが含まれます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでジャンボフレームを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが対応しているかどうかを確認します。

パブリックプレフィックスまたは ASN が ISP またはネットワークキャリアに属している場合、当社はお客様に追加情報をリクエストします。これは、ネットワークプレフィックス/ASN をお客様が使用できることを確認する、会社の正式なレターヘッドを使用したドキュメント、または会社のドメイン名からの E メールとすることができます。

プライベート仮想インターフェイスとパブリック仮想インターフェイスで、ネットワーク接続の最大送信単位 (MTU) とは、接続を介して渡すことができる最大許容パケットサイズ (バイト単位) です。仮想プライベートインターフェイスの MTU では、1500 あるいは 9001 (ジャンボフレーム) のどちらでも使用できます。トランジット仮想プライベートインターフェイスの MTU では、1500 あるいは 8500 (ジャンボフレーム) のどちらでも使用できます。インターフェイスの作成時あるいは作成後の更新時に、MTU を指定できます。仮想インターフェイスの MTU を8500 (ジャンボフレーム) または 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでそれを選択し、概要タブでジャンボフレーム機能を見つけます。

パブリック仮想インターフェイスを作成すると、 がリクエストを確認して承認 AWS するまでに最大 72 時間かかることがあります。

非 VPC サービスへのパブリック仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [パブリック] を選択します。
5. [Public Virtual Interface settings (仮想インターフェイス設定)] で以下を実行します。

   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

   c. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

   d. [BGP ASN] に、新しい仮想インターフェイスのオンプレミスピアルーターのボーダーゲートウェイプロトコル自律システム番号を入力します。

      有効な値は 1 ~ 2147483647 です。
6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

- これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
- [Amazon ルーターのピア IP] に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

[IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

b. 独自の BGP キーを指定するには、使用する BGP MD5 キーを入力します。

値が入力されない場合は、当社の側で自動的に BGP キーを生成します。

c. Amazon にプレフィックスを発行するには、[アドバタイズするプレフィックス] に、この仮想インターフェイスを介してルーティングされるトラフィックのルーティング先となる IPv4 CIDR アドレスをカンマで区切って入力します。

d. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

VPC へのプライベート仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [プライベート] を選択します。
5. [プライベート仮想インターフェイス設定] で以下を実行します。

a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

c. [ゲートウェイタイプ] で、[仮想プライベートゲートウェイ] または [Direct Connect ゲートウェイ] を選択します。

d. 仮想インターフェイス所有者 で、別の AWS アカウント を選択し、 AWS アカウントを入力します。

e. [仮想プライベートゲートウェイ] で、このインターフェイスに使用する仮想プライベートゲートウェイを選択します。

f. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

g. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

有効な値は 1 ~ 2,147,483,647 です。

6. [追加設定] で、以下を実行します。

a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

[IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

- これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
- [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

> **Important**
>
> IPv4 アドレス AWS の自動割り当てを許可すると、RFC 3927 に従って 169.254.0.0/16 IPv4 Link-Local から /29 CIDR が接続用に割り当てられます。VPC point-to-point AWS トラフィックの送信元および/または送信先としてカスタマールーターピア IP アドレスを使用する場合は、このオプションは推奨されません。代わりに、RFC 1918 または他のアドレスを使用して、アドレスを自分で指定する必要があります。
>
> - RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。
> - RFC 3927 の詳細については、「IPv4 リンクローカルアドレスのダイナミック設定」を参照してください。

[IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

b. 最大送信単位 (MTU) を 1500 (デフォルト) から 9001 (ジャンボフレーム) に変更するには、[ジャンボ MTU (MTU サイズ 9001)] を選択します。

c. (オプション) の有効化 SiteLinkで、有効化 を選択して Direct Connect のプレゼンスポイント間の直接接続を有効にします。

d. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。
8. パブリック VIF 接続に使用するネットワークをアドバタイズするには、BGP デバイスを使用する必要があります。

ステップ 5: ルーター設定をダウンロードする

AWS Direct Connect 接続用の仮想インターフェイスを作成したら、ルーター設定ファイルをダウンロードできます。このファイルには、プライベートまたはパブリック仮想インターフェイスで使用する、ルーターを設定するために必要なコマンドが含まれています。

ルーター設定をダウンロードするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. 接続を選択したら、[View Details (詳細の表示)] を選択します。
4. [ルーター設定をダウンロードする] を選択します。
5. [ルーター設定をダウンロードする] で、次を実行します。

   a. [Vendor] で、ルーターの製造元を選択します。

   b. [Platform] で、ルーターのモデルを選択します。

c. [Software] で、ルーターのソフトウェアのバージョンを選択します。

6. [ダウンロード] を選択してから、ルーターに対応する適切な設定を使用して AWS Direct Connectに接続できることを確認します。

設定ファイルの例については、「ルーター設定ファイルの例」を参照してください。

ルーターを設定した後は、仮想インターフェイスのステータスは UP になります。仮想インターフェイスがダウンしたままで、 AWS Direct Connect デバイスのピア IP アドレスに ping を実行できない場合は、「」を参照してくださいレイヤー 2 (データリンク層) 問題のトラブルシューティング。ピア IP アドレスに対して ping を送信できる場合は、「レイヤー 3/4 (ネットワーク層/トランスポート層) 問題のトラブルシューティング」を参照してください。BGP ピア接続セッションが確立されたが、トラフィックをルーティングできない場合は、「ルーティング問題のトラブルシューティング」を参照してください。

ステップ 6: 作成した仮想インターフェイスを検証する

AWS クラウドまたは Amazon VPC への仮想インターフェイスを確立したら、次の手順を使用して AWS Direct Connect 接続を検証できます。

AWS クラウドへの仮想インターフェイス接続を確認するには

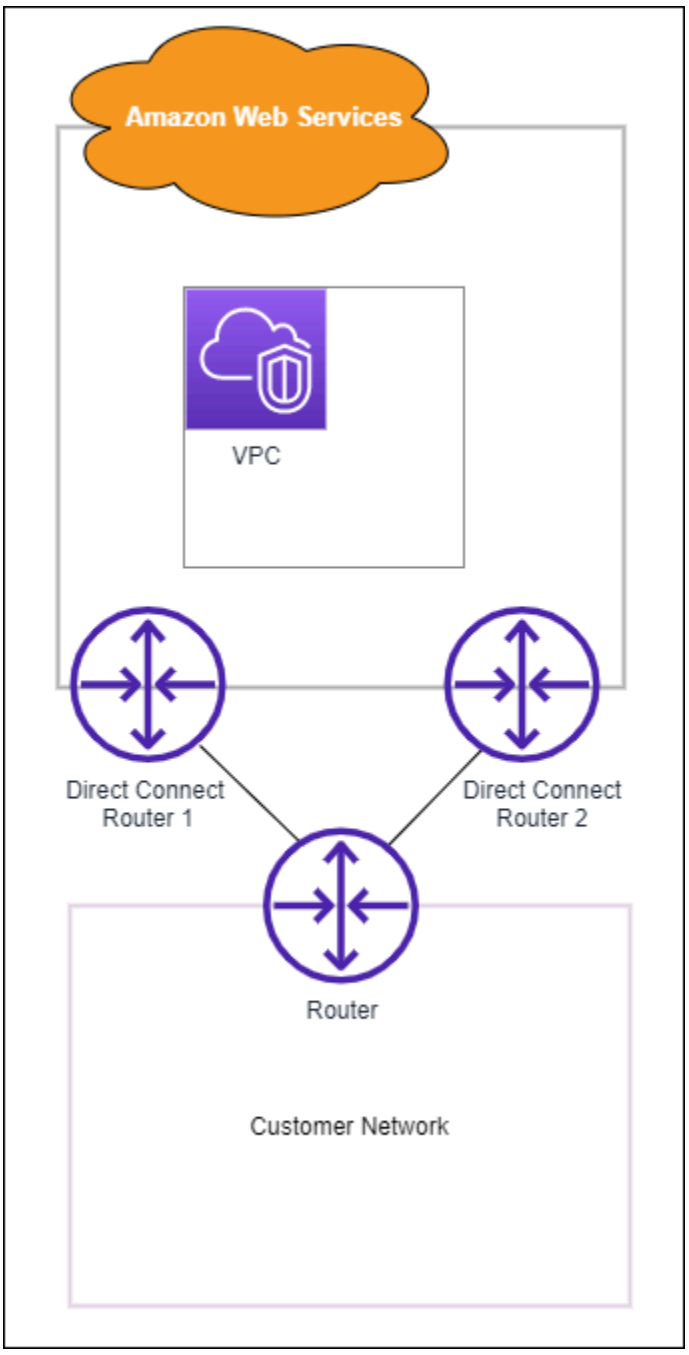
- を実行し`traceroute`、 AWS Direct Connect 識別子がネットワークトレースにあることを確認します。

Amazon VPC への仮想インターフェイス接続を検証するには

1. Amazon Linux AMI など Ping に応答する AMI を使用して、仮想プライベートゲートウェイにアタッチされている VPC に EC2 インスタンスを起動します。Amazon EC2 コンソールのインスタンス起動ウィザードを使用すれば、Amazon Linux AMI を [Quick Start (クイックスタート)] タブで使用することができます。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの起動」を参照してください。 Amazon EC2 インスタンスに関連付けられたセキュリティグループに、インバウンド ICMP トラフィックを許可するルール (ping リクエストの場合) が含まれていることを確認します。
2. インスタンスが実行中になった後、そのプライベート IPv4 アドレス (たとえば 10.0.0.4) を取得します。Amazon EC2 コンソールにインスタンスの詳細の一部としてアドレスが表示されます。
3. プライベート IPv4 アドレスに Ping を実行し、応答を確認します。

(推奨) ステップ 7: 冗長接続を設定する

フェイルオーバーを実現するには、次の図に示すように AWS、 への 2 つの専用接続をリクエストして設定することをお勧めします。これらの接続は、お客様のネットワーク内の 1 台もしくは 2 台のルーターを終端とすることができます。



2 本の専用接続をプロビジョニングする際の設定は、以下からどちらかを選びます。

- アクティブ/アクティブ (BGP マルチパス)。これは、両方の接続がアクティブであるデフォルト設定です。 は、同じ場所内の複数の仮想インターフェイスへのマルチパス AWS Direct Connect をサポートし、トラフィックはフローに基づいてインターフェイス間でロード共有されます。一方の接続が使用できなくなった場合、すべてのトラフィックが他方の接続のネットワーク経由でルーティングされます。
- アクティブ/パッシブ (フェイルオーバー)。一方の接続がトラフィックを処理し、他方はスタンバイ状態となります。アクティブな接続が使用できなくなった場合、すべてのトラフィックがパッシブ接続を介してルーティングされます。AS パスに、パッシブリンクとなるいずれかのリンクのルートを付加する必要があります。

どちらの接続設定でも冗長性には影響ありませんが、これら 2 本の接続でのデータのルーティングポリシーが変わってきます。推奨設定はアクティブ/アクティブです。

冗長性を確保するために VPN 接続を使用する場合は、ヘルスチェックとフェイルオーバーメカニズムを確実に実装してください。以下のいずれかの設定を使用する場合は、新しいネットワークインターフェイスにルーティングするようにルートテーブルのルーティングを確認する必要があります。

- ルーティングには独自のインスタンスを使用します。たとえば、インスタンスがファイアウォールなどです。
- VPN 接続を終了する独自のインスタンスを使用します。

高可用性を実現するには、さまざまな AWS Direct Connect 場所への接続を設定することを強くお勧めします。

障害 AWS Direct Connect 耐性の詳細については、AWS Direct Connect 「Resiliency Recommendations」を参照してください。

AWS Direct Connect フェイルオーバーテスト

AWS Direct Connect Resiliency Toolkit の回復性モデルは、複数の場所で適切な数の仮想インターフェイス接続を確保するように設計されています。ウィザードの完了後、トラフィックが冗長仮想インターフェイスの 1 つにルーティングされ、回復性要件を満たすことを確認するため、AWS Direct Connect Resiliency Toolkit のフェイルオーバーテストを使用して BGP ピア接続セッションを停止します。

このテストを使用して、仮想インターフェイスがサービス停止状態のときに、トラフィックが冗長仮想インターフェイスを介してルーティングされることを確認します。テストを開始するには、仮想イ

ンターフェイス、BGP ピア接続セッション、テストの実行時間を選択します。AWS は、選択された仮想インターフェイス BGP ピア接続セッションを停止状態にします。インターフェイスがこの状態のとき、トラフィックは冗長仮想インターフェイスを通過する必要があります。構成に適切な冗長接続が含まれていない場合、BGP ピア接続セッションは失敗し、トラフィックはルーティングされません。テストが完了するか、手動でテストを停止すると、AWS は BGP セッションを復元します。テストが完了したら、AWS Direct Connect Resiliency Toolkit を使用して設定を調整できます。

> **Note**
>
> この機能は、メンテナンス中またはメンテナンス後に BGP セッションが途中で復元される可能性があるため、Direct Connect メンテナンス期間中には使用しないでください。

テスト履歴

AWS は、365 日後にテスト履歴を削除します。テスト履歴には、すべての BGP ピアで実行されたテストのステータスが含まれます。履歴には、テストされた BGP ピア接続セッション、開始時刻と終了時刻、テストステータスが含まれます。テストステータスは次のいずれかの値です。

- In progress (進行中) - テストは現在実行中です。
- Completed (完了) - 指定した時間、テストが実行されました。
- Canclled (キャンセル済み) - 指定した時間より前に、テストがキャンセルされました。
- Failed (失敗) - 指定した期間、テストが実行されませんでした。このスタータスになると、ルーターに問題がある可能性があります。

詳細については、「the section called “仮想インターフェイスのフェイルオーバーテスト履歴の表示”」を参照してください。

検証のアクセス許可

フェイルオーバーテストを実行するアクセス許可のある唯一のアカウントは、仮想インターフェイスを所有するアカウントです。このアカウントの所有者は AWS CloudTrail から、テストが仮想インターフェイスで実行されたという通知を受け取ります。

仮想インターフェイスのフェイルオーバーテストの開始

仮想インターフェイスのフェイルオーバーテストは AWS Direct Connect コンソールまたは AWS CLI を使用して開始できます。

AWS Direct Connect コンソールから仮想インターフェイスのフェイルオーバーテストを開始するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. [Virtual interfaces (仮想インターフェイス)] を選択します。
3. 仮想インターフェイスを選択し、[Actions (アクション)]、[Bring down BGP (BGP の停止)] の順に選択します。

   テストは、パブリック、プライベート、またはトランジット仮想インターフェイスで実行できます。
4. [Start failure test (障害テストの開始)] ダイアログボックスで、以下の操作を行います。

   a. [Peerings to bring down to test (ピア接続を停止してテストする)] で、テストするピア接続セッション (IPv4 など) を選択します。

   b. [Test maximum time (テストの最大時間)] で、テストを継続する分数を入力します。

      最大値は 4,320 分 (72 時間) です。

      デフォルト値は 180 分 (3 時間) です。

   c. [To confirm test (テストを確認するには)] で、「Confirm」と入力します。

   d. [Confirm (確認)] を選択します。

   BGP ピア接続セッションは DOWN (停止) 状態になります。トラフィックを送信して、サービス停止が起こらないことを確認できます。必要に応じて、テストをすぐに停止できます。

AWS CLI を使用して仮想インターフェイスのフェイルオーバーテストを開始するには

を使用しますStartBgpFailoverTest。

仮想インターフェイスのフェイルオーバーテスト履歴の表示

仮想インターフェイスのフェイルオーバーテスト履歴は、AWS Direct Connect コンソールまたは AWS CLI を使用して表示できます。

AWS Direct Connect コンソールから仮想インターフェイスのフェイルオーバーテスト履歴を表示するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. [Virtual interfaces (仮想インターフェイス)] を選択します。
3. 仮想インターフェイスを選択したら、[View details (詳細の表示)] を選択します。
4. [Test history (テスト履歴)] を選択します。

   コンソールには、仮想インターフェイスで実行した仮想インターフェイステストが表示されます。
5. 特定のテストの詳細を表示するには、テスト ID を選択します。

AWS CLI を使用して仮想インターフェイスのフェイルオーバーテスト履歴を表示するには

を使用しますListVirtualInterfaceTestHistory。

仮想インターフェイスのフェイルオーバーテストの停止

仮想インターフェイスのフェイルオーバーテストは、AWS Direct Connect コンソールまたは AWS CLI を使用して停止できます。

AWS Direct Connect コンソールから仮想インターフェイスのフェイルオーバーテストを停止するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. [Virtual interfaces (仮想インターフェイス)] を選択します。
3. 仮想インターフェイスを選択し、[Actions (アクション)]、[Cancel test (テストのキャンセル)] の順に選択します。
4. [Confirm (確認)] を選択します。

AWS は BGP ピア接続セッションを復元します。テスト履歴では、テストに「cancelled (キャンセル済み)」が表示されます。

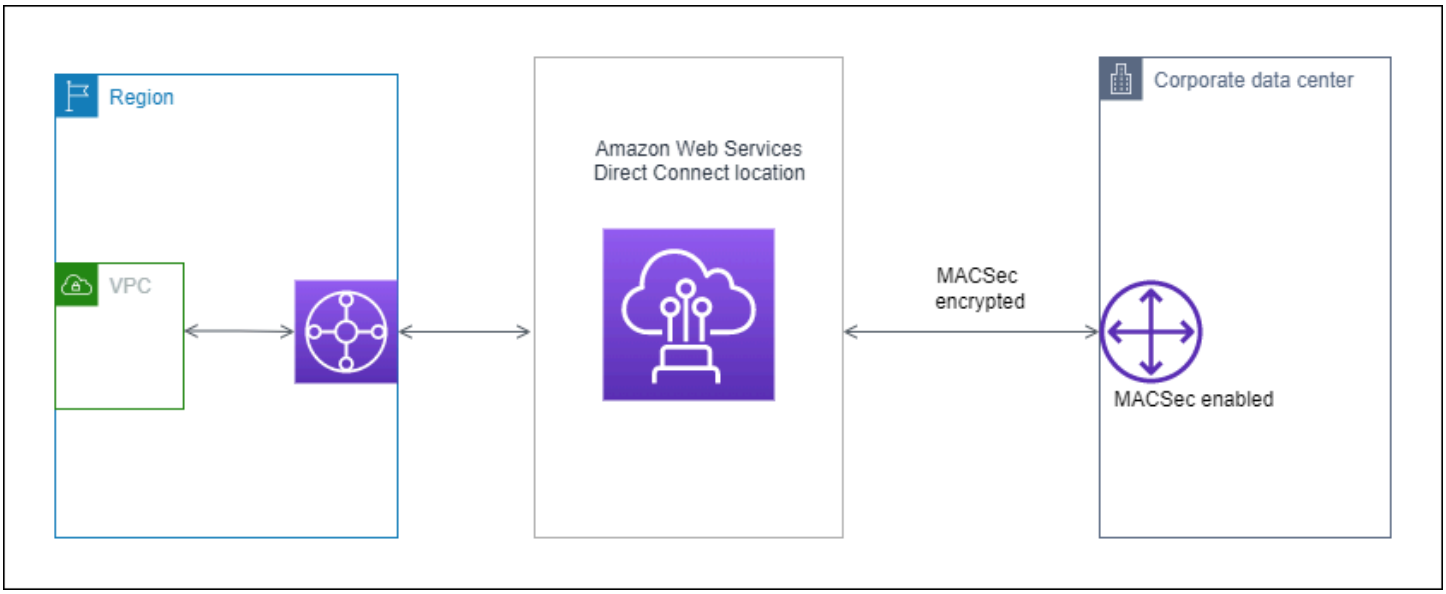
AWS CLI を使用して仮想インターフェイスのフェイルオーバーテストを停止するには

を使用しますStopBgpFailoverTest。

MAC セキュリティ

MAC Security (MACsec) は IEEE 標準の 1 つです。データの機密性、データの整合性、およびデータオリジンの信頼性を定義しています。MACSec は、 へのクロスコネクトを介してレイヤー 2 point-to-point 暗号化を提供します AWS。MACSec は 2 つのレイヤー 3 ルーター間でレイヤー 2 で動作し、レイヤー 2 ドメインで暗号化を提供します。データセンターやリージョンと相互接続する AWS グローバルネットワークを流れるすべてのデータは、データセンターを離れる前に物理レイヤーで自動的に暗号化されます。

次の図では、専用接続とオンプレミスのリソースの両方が MacSec をサポートしている必要があります。データセンターとの間にある、専用接続を通過するレイヤ 2 トラフィックは暗号化されます。



MACsec の概念

MACsec の主な概念は次のとおりです。

- MAC Security (MACsec) — IEEE 802.1 レイヤー 2 標準の 1 つで、データの機密性、データの整合性、およびデータオリジンの信頼性を定義しています。このプロトコルの詳細については、「802.1AE: MAC Security (MACsec)」を参照してください。
- MACsec シークレットキー — お客様のオンプレミスルーターと AWS Direct Connect ロケーションの接続ポート間の MACsec 接続を確立する事前共有キー。キーは、 に提供 AWS し、デバイスでプロビジョニングした CKN/CAK ペアを使用して、接続の最後にデバイスによって生成されます。

- 接続キー名 (CKN) と接続関連付けキー (CAK) — これらの値はペアとして、MACsec シークレットキーを生成するために使用されます。ペア値を生成して AWS Direct Connect 接続に関連付け、AWS Direct Connect 接続の最後にエッジデバイスにプロビジョニングします。

サポートされている接続

MACSec は専用接続の上で使用可能です。MACsec をサポートする接続の注文方法については、AWS Direct Connect を参照してください。

専用接続での MacSec の使用開始

以下のタスクは、 AWS Direct Connect 専用接続の MACsec に慣れるのに役立ちます。MACsec の使用に追加料金はかかりません。

専用接続で MACsec を設定する前に、次の点に注意してください。

- MACsec は、選択された POP (Point Of Presence) での 10 Gbps および 100 Gbps の専用 Direct Connect 接続でサポートされます。これらの接続では、次の MACsec 暗号スイートがサポートされています。
  - 10Gbps の接続の場合、GCM-AES-256 および GCM-AES-XPN-256。
  - 100 Gbps の接続の場合、GCM-AES-XPN-256。
- 256 ビットの MACsec キーのみがサポートされています。
- 100Gbps の接続には拡張パケット番号付け (XPN) が必要です。10Gbps の接続の場合、Direct Connect は GCM-AES-256 と GCM-AES-XPN-256 の両方をサポートします。100 Gbps の専用接続などの高速接続では、MACsec の元の 32 ビットパケット番号空間がすぐに使い果たす可能性があるため、新しい接続アソシエーションを確立するために暗号化キーを数分ごとにローテーションする必要があります。このような状況を回避するため、IEEE Std 802.1AEbw -2013 の会社では、パケット番号が拡張され、番号付けスペースが 64 ビットに増加し、キーローテーションのタイムライン要件が軽減されました。
- Secure Channel Identifier (SCI) は必須であり、オンにする必要があります。この設定は調整できません。
- IEEE 802.1Q (Dot1q/VLAN) タグ offset/dot1 q-in-clear は、暗号化されたペイロードの外部での VLAN タグの移動ではサポートされていません。

Direct Connect と MACsec の詳細については、よくある質問の「MACsecAWS Direct Connect FAQs」セクションを参照してください。

トピック

MacSec の前提条件

専用接続で MACSec の設定を行う前に、以下のタスクを完了してください。

- MACsec シークレットキー用の CKN/CAK ペアを作成します。

  このペアの作成には、公開された標準ツールが使用できます。作成するペアは、the section called “ステップ 4: オンプレミスのルーターを設定する” で指定された要件を満たしている必要があります。
- 接続の末端には、MacSec をサポートする適切なデバイスが設置されている必要があります。
- Secure Channel Identifier (SCI) をオンにする必要があります。
- 256 ビットの MACsec キーのみがサポートされており、最新の高度なデータ保護を提供します。

サービスにリンクされたロール

AWS Direct Connect は AWS Identity and Access Management (IAM) 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は、 に直接リンクされた一意のタイプの IAM ロールです AWS Direct Connect。サービスにリンクされたロールは、 によって事前定義 AWS Direct Connect されており、ユーザーに代わってサービスから他の AWS のサービスを呼び出す必要のあるアクセス許可がすべて含まれています。サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、 の設定 AWS Direct Connect が簡単になります。は、サービスにリンクされたロールのアクセス許可 AWS Direct Connect を定義し、特に定義されて

いる場合を除き、 のみがそのロールを引き受け AWS Direct Connect ることができます。定義されるアクセス許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。詳細については、「the section called “サービスリンクロール”」を参照してください。

MACSec の事前共有 CKN/CAK キーに関する考慮事項

AWS Direct Connect は、接続または LAGs に関連付ける事前共有キーに AWS マネージド CMK を使用します。 CMKs Secrets Manager は、Secrets Manager のルートキーが暗号化するシークレットとして、事前共有された CKN と CAK のペアを保存します。詳細については、AWS Key Management Service デベロッパーガイドの「AWS 管理の CMK」を参照してください。

保存されているキーは設計上読み取り専用ですが、 AWS Secrets Manager コンソールまたは API を使用して、7 日から 30 日の削除をスケジュールできます。削除をスケジュールすると、CKN を読み取ることができなくなるため、ネットワーク接続に影響が生じる場合があります。この場合、次のルールが適用されます。

- 接続が保留状態の場合は、その接続での CKN の関連付けを解除します。
- 接続が使用可能な状態の場合は、接続の所有者に電子メールで通知します。所有者が 30日以内に何らかの措置を講じなかった場合は、対象の CKN の接続との関連付けが当社により解除されます。

接続から最後の CKN の関連付けを解除した際に、接続の暗号化モードが「must encrypt」に設定されている場合は、モードを「should_encrypt」に設定して突然のパケット損失を防ぎます。

ステップ 1: 接続を作成する

MACsec の使用を開始するには、専用接続を作成する際に、この機能をオンにする必要があります。詳細については、「the section called “接続ウィザードを使用して接続を作成する”」を参照してください。

(オプション) ステップ 2: Link Aggregation Group (LAG) を作成する

冗長性のために複数の接続を使用する場合は、MACsec をサポートする LAG を作成できます。詳細については、「the section called “MacSec に関する考慮事項”」および「the section called “LAG を作成する”」を参照してください。

ステップ 3: CKN/CAK を、接続または LAG に関連付ける

MACsec をサポートする接続または LAG の作成後は、CKN/CAK をその接続に関連付ける必要があります。詳細については、以下のいずれかを参照してください。

- the section called “MACSec CKN/CAK を接続に関連付ける”
- the section called “MACSec CKN/CAK と LAG を関連付ける”

ステップ 4: オンプレミスのルーターを設定する

MACsec シークレットキーを使用するように、オンプレミスのルーターを更新します。オンプレミスルーターと AWS Direct Connect ロケーションの MACsec シークレットキーは一致する必要があります。詳細については、「the section called “ルーター設定ファイルをダウンロードする”」を参照してください。

(オプション) ステップ 5 : CKN/CAK と接続または LAG 間での関連付けを解除する

接続または LAG と MACsec キーとの間の関連付けを解除する方法に関しては、次のいずれかを参照してください。

- the section called “MACsec シークレットキーと接続の間の関連付けを解除する”
- the section called “MACsec シークレットキーと LAG の間の関連付けを解除する”

AWS Direct Connect 接続

AWS Direct Connect では、ネットワークといずれかの AWS Direct Connect ロケーションとの間に専用のネットワーク接続を確立できます。

接続には 2 種類あります。

- 専用接続: 単一のお客様に関連付けられた物理イーサーネット接続。お客様は、 AWS Direct Connect コンソール、 CLI、または API を使用して専用接続をリクエストできます。詳細については、「the section called “専用接続”」を参照してください。
- ホスト接続: AWS Direct Connect パートナーがお客様に代わってプロビジョニングする物理イーサネット接続。お客様は、この接続をプロビジョニングする AWS Direct Connect パートナープログラムのパートナーに連絡することで、ホスト接続をリクエストします。詳細については、「the section called “ホスト接続”」を参照してください。

専用接続

AWS Direct Connect 専用接続を作成するには、次の情報が必要です。

AWS Direct Connect location

パートナープログラムの AWS Direct Connect パートナーと協力して、 AWS Direct Connect ロケーションとデータセンター、オフィス、またはコロケーション環境との間にネットワーク回線を確立します。また、ロケーションと同じ施設内にコロケーションスペースを提供するのにも役立ちます。詳細については、「AWS Direct Connectをサポートしている APN パートナー」を参照してください。

Port speed

指定できる値は 1 Gbps、10 Gbps、および 100 Gbps です。

接続リクエストの作成後にポート速度を変更することはできません。ポート速度を変更するには、新しい接続を作成し、設定する必要があります。

接続ウィザードを使用して接続を作成することも、Classic 接続を作成することもできます。接続ウィザードを使用すると、回復性に関する推奨事項を使用して接続を設定できます。接続を初めて設定する場合、このウィザードの使用をお勧めします。必要に応じて、 Classic を使用して接

続 を作成できます one-at-a-time。既存のセットアップがすでにあり、それに接続を追加する場合は、Classic をお勧めします。スタンドアロン接続を作成するか、アカウントの LAG に関連付ける接続を作成できます。LAG と接続を関連付ける場合、LAG で指定されたものと同じポート速度と場所で作成されます。

当社は、お客様から接続のリクエストを受け取った後、Letter of Authorization and Connecting Facility Assignment (設備の接続割り当て書ならびに承認書 = LOA-CFA) をダウンロード可能にするか、追加情報を求めるメールを返信します。追加情報のリクエストを受け取った場合は、7 日以内に応答する必要があります。応答しないと接続は削除されます。LOA-CFA は、 に接続するための認可であり AWS、クロスコネクトを注文するためにネットワークプロバイダーが必要とするものです。AWS Direct Connect ロケーションに機器がない場合は、そこで自分でクロスコネクトを注文することはできません。

次のオペレーションが専用接続で利用できます。

- the section called “接続ウィザードを使用して接続を作成する”
- the section called “Classic 接続を作成する”
- the section called “接続の詳細を表示する”
- the section called “接続を更新する”
- the section called “MACSec CKN/CAK を接続に関連付ける”
- the section called “MACsec シークレットキーと接続の間の関連付けを解除する”
- the section called “複数の接続を削除”

専用接続を Link Aggregation Group (LAG) に追加すると、複数の接続を単一の接続として扱うことができます。詳細については、接続を LAG に関連付ける を参照してください。

接続の確立後、パブリックおよびプライベートの AWS リソースに接続するための仮想インターフェイスを作成します。詳細については、「AWS Direct Connect 仮想インターフェイス」を参照してください。

AWS Direct Connect ロケーションに機器がない場合は、まず AWS Direct Connect パートナープログラムの AWS Direct Connect パートナーにお問い合わせください。詳細については、「AWS Direct Connectをサポートしている APN パートナー」を参照してください。

MAC セキュリティ (MACsec) を使用する接続を作成する場合は、その作業を開始する前に、接続の前提条件をご確認ください。詳細については、「the section called “MacSec の前提条件 ”」を参照してください。

接続ウィザードを使用して接続を作成する

このセクションでは、接続ウィザードを使用して接続を作成する方法について説明します。Classic 接続を作成する場合、the section called “ステップ 2: AWS Direct Connect 専用接続をリクエストする” の手順をご覧ください。

接続ウィザードの接続を作成するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [接続] を選択し、[接続の作成] を選択します。
3. [接続の作成] ページの [接続順序タイプ] で、[接続ウィザード] を選択します。
4. ネットワーク接続の [回復性レベル] を選択します。回復性レベルは次のいずれかを指定できます。

   - 最大回復性
   - 高い回復性
   - 開発とテスト

   これらの回復性レベルの説明と詳細については、Resiliency Toolkit AWS Direct Connect を使用して開始する を参照してください。
5. [次へ] をクリックします。
6. [接続の構成] ページで、次の詳細情報を入力します。

   a. [帯域幅] ドロップダウンリストから、接続に必要な帯域幅を選択します。1 Gbps から 100 Gbps までの範囲で設定できます。

   b. ロケーション で適切な AWS Direct Connect ロケーションを選択し、最初のロケーション サービスプロバイダー を選択し、このロケーションで接続を提供するサービスプロバイダーを選択します。

   c. 2 番目の場所 では、2 番目の場所で適切な を選択し、2 番目の場所サービスプロバイダーを選択し、この 2 番目の場所で接続を提供するサービスプロバイダーを選択します。 AWS Direct Connect

   d. (オプション) MAC セキュリティ (MACsec) を使用する接続を設定します。[その他の設定] で、[MACSec 対応ポートをリクエストする] をクリックします。

      MACSec は専用接続でのみ使用が可能です。

e. (オプション) [タグを追加] を選択してキーと値のペアを追加すると、この接続をさらに識別しやすくなります。

- [キー] にはキー名を入力します。
- [値] にキー値を入力します。

既存のタグを削除するには、タグを選択し、[タグの削除] を選択します。タグを空にすることはできません。

7. [次へ] をクリックします。
8. [確認と作成] ページで、接続を確認します。このページには、ポート使用量の推定コストと追加のデータ転送料金も表示されます。
9. [作成] を選択します。
10. Letter of Authorization and Connecting Facility Assignment (LOA-CFA) をダウンロードします。詳細については、the section called “LOA-CFA をダウンロードする” を参照してください。

以下のいずれかのコマンドを使用します。

- create-connection (AWS CLI)
- CreateConnection (AWS Direct Connect API)

Classic 接続を作成する

専用接続の場合は、 AWS Direct Connect コンソールを使用して接続リクエストを送信できます。ホスト接続の場合は、 AWS Direct Connect パートナーと協力してホスト接続をリクエストします。次の情報があることを確認します。

- 必要なポートスピード。専用接続では、接続リクエストの作成後にポート速度を変更することはできません。ホスト接続の場合、 AWS Direct Connect パートナーは速度を変更できます。
- 接続を終了する AWS Direct Connect 場所。

> **Note**
>
> AWS Direct Connect コンソールを使用してホスト接続をリクエストすることはできません。代わりに、ホスト接続を作成できる AWS Direct Connect パートナーに連絡して、受け入れてください。次の手順をスキップして「ホスト接続の許可」に進みます。

新しい AWS Direct Connect 接続を作成するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. [AWS Direct Connect] 画面の [Get started (使用開始)] で、[接続の作成] を選択します。
3. [Classic] を選択します。
4. [名前] に、接続の名前を入力します。
5. [Location (場所)] で、適切な AWS Direct Connect の場所を選択します。
6. 該当する場合は、[サブロケーション] で、お客様、またはお客様のネットワークプロバイダーに最も近いフロアを選択します。このオプションは、ロケーションで建物の複数のフロアに会議室 (MMR) がある場合のみ該当します。
7. [ポートスピード] で接続帯域幅を選択します。
8. この接続を使用してデータセンターに接続する場合は、[On-premises] (オンプレミス) で、[Connect through an AWS Direct Connect partner] (パートナー経由で接続する) を選択します。
9. サービスプロバイダー で、 AWS Direct Connect パートナーを選択します。リストにないパートナーを使用する場合は、[Other] を選択します。
10. [サービスプロバイダー] で [Other] を選択した場合は、[プロバイダーの名前] に、使用するパートナーの名前を入力します。
11. (オプション) [タグを追加] を選択してキーと値のペアを追加すると、この接続をさらに識別しやすくなります。

    - [キー] にはキー名を入力します。
    - [値] にキー値を入力します。

    既存のタグを削除するには、タグを選択し、[タグの削除] を選択します。タグを空にすることはできません。
12. [接続の作成] を選択します。

がリクエストを確認し、接続用のポートをプロビジョニング AWS するまでに最大 72 時間かかる場合があります。この時間中、ユースケースまたは指定された場所に関する詳細情報のリクエストを含む E メールが送信される場合があります。E メールは、 にサインアップしたときに使用した E メールアドレスに送信されます AWS。7 日以内に応答する必要があり、応答しないと接続は削除されます。

詳細については、「AWS Direct Connect 接続」を参照してください。

LOA-CFA をダウンロードする

当社側で、お客様からの接続リクエストが処理されると、LOA-CFA のダウンロードが可能になります。リンクが有効になっていない場合、LOA-CFA がまだダウンロード可能になっていません。情報のリクエストメールを確認します。

請求は、ポートがアクティブになったとき、または LOA が発行されてから 90 日が経過したときのいずれか早い時点で自動的に開始されます。アクティベーションの前、または LOA が発行されてから 90 日以内にポートを削除することで、請求を回避することができます。

90 日が経過しても接続が行われておらず、LOA-CFA が発行されてない場合は、ポートが 10 日後に削除されることを警告する E メールが送信されます。10 日の追加期間内にポートをアクティブにしなかった場合、ポートは自動的に削除され、ポート作成プロセスを再度開始する必要が生じます。

> **Note**
>
> 料金の詳細については、「AWS Direct Connect 料金」を参照してください。LOA-CFA を再発行した後に接続が必要なくなった場合は、お客様ご自身で接続を削除する必要があります。詳細については、「複数の接続を削除」を参照してください。

Console

LOA-CFA のダウンロード方法

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Connections (接続)] を選択します。
3. 接続を選択したら、[詳細の表示] をクリックします。
4. [Download LOA-CFA] を選択します。

> **Note**
>
> リンクが有効になっていない場合、LOA-CFA がまだダウンロード可能になっていません。追加情報を要求するサポートケースが作成されます。リクエストに応答し、リクエストが処理されると、LOA-CFA をダウンロードできるようになります。それでもダウンロードできない場合は、AWS サポートにお問い合わせください。

5. LOA-CFA をネットワークプロバイダーまたはコロケーションプロバイダーに送信し、クロスコネクトを代行注文できるようにします。連絡方法はコロケーションプロバイダにより異なります。詳細については、「AWS Direct Connect ロケーションでのクロスコネクトのリクエスト」を参照してください。

Command line

コマンドラインまたは API を使用して LOA-CFA をダウンロードするには

- describe-loa (AWS CLI)
- DescribeLoa (AWS Direct Connect API)

接続を更新する

次の接続属性を更新できます。

- コレクションの名前。
- 接続で使用する MACsec 暗号化モード。

> **Note**
> MACSec は専用接続でのみ使用が可能です。

有効な値は以下のとおりです。

- `should_encrypt`
- `must_encrypt`

  暗号化モードをこの値に設定した場合、暗号化がダウンすると接続もダウンします。
- `no_encrypt`

Console

接続を更新するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。

2. ナビゲーションペインで [Connections (接続)] を選択します。
3. 接続を選択した後、[編集] をクリックします。
4. 接続を変更するには

   [名前の変更] [名前] に新しい接続名を入力します。

   [タグの追加] [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。

   [タグの削除] タグの横にある [タグの削除] を選択します。
5. [接続の編集] を選択します。

Command line

コマンドラインを使用してタグを追加または削除するには

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

コマンドラインまたは API を使用して接続を更新するには

- update-connection (AWS CLI)
- UpdateConnection (AWS Direct Connect API)

MACSec CKN/CAK を接続に関連付ける

MACsec をサポートする接続を作成した後に、CKN/CAK をその接続に関連付けることができます。

> **Note**
>
> 接続に関連付けされた後の MACsec のシークレットキーは変更できません。キーを変更する必要がある場合は、そのキーと接続との関連付けを解除した上で、新しいキーを接続に関連付けます。関連付けの解除については、「the section called “MACsec シークレットキーと接続の間の関連付けを解除する”」を参照してください。

Console

MACsec キーを接続に関連付けるには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. 左のペインで、[接続] を選択します。
3. 接続を選択したら、[詳細の表示] をクリックします。
4. [キーの関連付け] をクリックします。
5. MACsec キーを入力します。

   [CAK/CKN ペアの使用]: [キーペア] を選択し次の操作を行います。

   - [接続関連付けキー (CAK)] に、使用する CAK を入力します。
   - [接続関連付けキー名 (CKN)] に、使用する CKN を入力します。

   [シークレットの使用] : [既存のシークレットマネージャのシークレット] を選択し、[シークレット] で MACSec シークレットキーを選択します。
6. [キーの関連付け] をクリックします。

Command line

MACsec キーを接続に関連付けるには

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey (AWS Direct Connect API)

MACsec シークレットキーと接続の間の関連付けを解除する

接続と MACsec キーの間の関連付けは解除することが可能です。

Console

接続と MACsec キー間の関連付けを解除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。

2.
3. 左のペインで、[接続] を選択します。
4. 接続を選択したら、[詳細の表示] をクリックします。
5. 解除する MacSec シークレットを選択し、[キーの関連付けを解除する] をクリックします。
6. 確認ダイアログボックスで、disassociate と入力し、[関連付けを解除] をクリックします。

Command line

接続と MACsec キー間の関連付けを解除するには

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey (AWS Direct Connect API)

ホスト接続

AWS Direct Connect ホスト接続を作成するには、次の情報が必要です。

AWS Direct Connect location

AWS Direct Connect パートナープログラムの AWS Direct Connect パートナーと協力して、AWS Direct Connect ロケーションとデータセンター、オフィス、またはコロケーション環境との間にネットワーク回線を確立します。また、ロケーションと同じ施設内にコロケーションスペースを提供するのにも役立ちます。詳細については、「AWS Direct Connect Delivery Partners」(デリバリーパートナー) を参照してください。

> **Note**
>
> AWS Direct Connect コンソールからホスト接続をリクエストすることはできません。ただし、 AWS Direct Connect パートナーはホスト接続を作成して設定できます。接続が設定されたら、 コンソールの [Connections] (接続) ペインに接続が表示されます。
> ホスト接続を使用する前に同意する必要があります。詳細については、「the section called “ホスト接続を受け入れる”」を参照してください。

Port speed

ホスト接続の場合、指定できる値は 50 Mbps、100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps、10 Gbps、25 Gbps です。特定の要件を満たす AWS Direct Connect パートナーのみが、1 Gbps、2 Gbps、5 Gbps、10 Gbps、または 25 Gbps のホスト接続を作成できることに注意してください。25 Gbps の接続は、100 Gbps のポート速度が利用可能な Direct Connect ロケーションでのみ使用できます。

次の点に注意してください。

- 接続ポートの速度は、 AWS Direct Connect パートナーによってのみ変更できます。既存のホスト接続の帯域幅をアップグレードまたはダウングレードするために、接続を削除して再作成する必要がなくなりました。ポート速度を変更するには、ホスト接続を管理する AWS Direct Connect パートナーにお問い合わせください。
- AWS はホスト接続でトラフィックポリシーを使用します。つまり、トラフィックレートが設定された最大レートに達すると、過剰なトラフィックがドロップされます。これにより、高バーストトラフィックのスループットは、非バーストトラフィックよりも低くなる可能性があります。
- ジャンボフレームは、 AWS Direct Connect ホスト親接続で最初に有効になっている場合にのみ接続で有効にできます。ジャンボフレームがその親接続で有効になっていない場合、どの接続でも有効にすることはできません。

ホスト接続をリクエストして承認すると、次のコンソール操作が可能になります。

- the section called “接続の詳細を表示する”
- the section called “接続を更新する”
- the section called “複数の接続を削除”

接続の同意したら、パブリックおよびプライベート AWS リソースに接続するための仮想インターフェイスを作成します。詳細については、「AWS Direct Connect 仮想インターフェイス」を参照してください。

ホスト接続を受け入れる

ホスト接続の購入に関心がある場合は、 AWS Direct Connect パートナープログラムの AWS Direct Connect パートナーに連絡する必要があります。パートナーがお客様の接続をプロビジョニングしま

す。接続を設定されたら、 AWS Direct Connect コンソールの [Connections] ペインに接続が表示されます。

ホスト接続を使用する前に接続を受け入れる必要があります。

Console

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Connections (接続)] を選択します。
3. ホスト接続を選択したら、[詳細の表示] を選択します。
4. 確認のチェックボックスをオンにし、[同意する] を選択します。

Command line

コマンドラインまたは API を使用して接続を説明するには

- confirm-connection (AWS CLI)
- ConfirmConnection (AWS Direct Connect API)

接続の詳細を表示する

接続の現在のステータスを表示できます。接続 ID (たとえば、dxcon-12nikabc) を表示し、受信またはダウンロードした LOA-CFA の接続 ID との一致を確認することもできます。

接続のモニタリングの詳細については、「モニタリング」を参照してください。

Console

接続の詳細情報を表示するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. 左のペインで、[接続] を選択します。
3. 接続を選択したら、[詳細の表示] をクリックします。

Command line

コマンドラインまたは API を使用して接続を記述するには

- describe-connections (AWS CLI)
- DescribeConnections (AWS Direct Connect API)

複数の接続を削除

接続を削除できるのは、その接続に仮想インターフェイスが 1 つもアタッチされていない場合に限られます。接続を削除すると、この接続のポート時間料金はすべて停止しますが、クロスコネクト料金またはネットワーク回線料金が発生する場合があります (以下を参照) 。 AWS Direct Connect データ転送料金は仮想インターフェイスに関連付けられます。仮想インターフェイスの削除方法の詳細については、「仮想インターフェースを削除する」を参照してください。

接続を削除する前に、クロスアカウント情報が含まれる接続の LOA をダウンロードし、回線停止についての関連情報を入手してください。接続 LOA をダウンロードする手順については、「the section called “LOA-CFA をダウンロードする”」を参照してください。

接続を削除すると、該当する AWS パッチパネルから光ファイバクロスコネクトケーブルを削除して、Direct Connect ルーターからネットワークデバイスを切断するようにコロケーションプロバイダーに AWS 指示します。ただし、クロスコネクトケーブルがまだネットワークデバイスに接続されている可能性があるため、コロケーションプロバイダーまたは回線プロバイダーがクロスコネクト料金またはネットワーク回線料金を請求する場合があります。これらのクロスコネクト料金は Direct Connect とは無関係であり、LOAの情報を使用してコロケーションプロバイダーまたは回線プロバイダーによりキャンセルされなければなりません。

接続が Link Aggregation Group (LAG) の一部である場合、接続を削除すると LAG で使用できる接続の最小数の設定を下回るときは、この操作を行うことはできません。

Console

接続を削除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Connections (接続)] を選択します。
3. 接続を選択し、[Delete (削除)] を選択します。

4. [Delete (削除)] の確認ダイアログボックスで、[Delete (削除)] を選択します。

Command line

コマンドラインまたは API を使用して 接続を削除するには

- delete-connection (AWS CLI)
- DeleteConnection (AWS Direct Connect API)

AWS Direct Connect ロケーションでのクロスコネクトのリクエスト

Letter of Authorization and Connecting Facility Assignment (LOA-CFA) をダウンロードしたら、クロスネットワーク接続 (別名クロスコネクト) を完了する必要があります。 AWS Direct Connect ロケーションに既に機器がある場合は、適切なプロバイダーに連絡してクロスコネクトを完了してください。プロバイダごとの手順については、以下の表を参照してください。クロスコネクトの価格設定については、プロバイダにお問い合わせください。クロスコネクトを確立したら、 AWS Direct Connect コンソールを使用して仮想インターフェイスを作成することができます。

一部のロケーションは、キャンパスとして設定されます。各ロケーションで利用可能な速度などの詳細については、「AWS Direct Connect ロケーション」を参照してください。

AWS Direct Connect ロケーションにまだ機器がない場合は、 AWS パートナーネットワーク (APN) のパートナーの 1 人と協力して作業できます。 AWS Direct Connect ロケーションに接続するのに役立ちます。詳細については、「 をサポートする APN パートナー AWS Direct Connect」を参照してください。クロスコネクトのリクエストを迅速に行うには、選択したプロバイダと LOA-CFA を共有してください。

AWS Direct Connect 接続は、他のリージョンのリソースへのアクセスを提供できます。詳細については、「リモート AWS リージョンへのアクセス」を参照してください。

> **Note**
>
> クロスコネクトが 90 日以内に完了しない場合は、LOA-CFA が付与した権利は無効になります。有効期限が切れた LOA-CFA を更新するには、 AWS Direct Connect コンソールから再度ダウンロードできます。詳細については、「LOA-CFA をダウンロードする」を参照してください。

コロケーション

- 米国東部 (オハイオ)
- 米国東部 (バージニア北部)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)

- アフリカ (ケープタウン)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- カナダ (中部)
- 中国 (北京)
- 中国 (寧夏)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ミラノ)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 欧州 (ストックホルム)
- 欧州 (チューリッヒ)
- イスラエル (テルアビブ)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)
- 南米 (サンパウロ)
- AWS GovCloud （ 米国東部 ）
- AWS GovCloud （ 米国西部 ）

米国東部 (オハイオ)

ロケーション	接続をリクエストする方法
Cologix COL2、コロンバス	Cologix へのお問い合わせは、sales@cologix.com までご連絡ください。

ロケーション	接続をリクエストする方法
Cologix MIN3、ミネアポリス	Cologix へのお問い合わせは、sales@cologix.com までご連絡ください。
CyrusOne West III、イメージング	カスタマーポータル を使用して、リクエストを送信します。
Equinix CH2、シカゴ	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
QTS、シカゴ	QTS へのお問い合わせは、AConnect@qtsdatacenters.com までご連絡ください。
Netrality Data Centers、1102 Grand、カンザスシティ	Netrality データセンターへのお問い合わせは、support@netrality.com までご連絡ください。

米国東部 (バージニア北部)

ロケーション	接続をリクエストする方法
165 Halsey Street、ニューアーク	operations@165halsey.com にお問い合わせください。
CoreSite 32k、ニューヨーク	CoreSite カスタマーポータル を使用して注文を行います。フォームに記入したら、注文の内容が正しいことを確認してから、ウェブサイトを使用して注文を承認してください。
CoreSite VA1-VA2、復元	CoreSite カスタマーポータル で注文を行います。フォームに記入したら、注文の内容が正しいことを確認してから、ウェブサイトを使用して注文を承認してください。
Digital Realty ATL1 &ATL2、イメージング	Digital Realty へのお問い合わせは、amazon.orders@digitalrealty.com までご連絡ください。
デジタル Realty IAD38、アッシュバーン	Digital Realty へのお問い合わせは、amazon.orders@digitalrealty.com までご連絡ください。

ロケーション	接続をリクエストする方法
Equinix DC1-DC6 および DC10-D12、アッシュバーン	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix DAA1-DC3 & DC6、ダラス	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix MI1、マイアミ	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix NY5、セコカウス	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
KIO Networks QRO1、ケレタロ、MX	KIO Networks にお問い合わせください。
Markley、One Summer Street、ボストン	現在のお客様の場合は、カスタマーポータル を使用してリクエストを作成します。新しいクエリは、sales@markleygroup.com までご連絡ください。
Netrality データセンター、第 2 フロア MMR、バージニア	Netrality データセンターへのお問い合わせは、support@netrality.com までご連絡ください。
QTS ATL1、イメージング	QTS へのお問い合わせは、AConnect@qtsdatacenters.com までご連絡ください。

米国西部 (北カリフォルニア)

ロケーション	接続をリクエストする方法
CoreSite、LA1、ロサンゼルス	CoreSite カスタマーポータル を使用して注文を行います。フォームに記入したら、注文の内容が正しいことを確認してから、ウェブサイトを使用して注文を承認してください。
CoreSite SV2、ミリタス	CoreSite カスタマーポータル を使用して注文を行います。フォームに記入したら、注文の内容が正しいことを確認してから、ウェブサイトを使用して注文を承認してください。

ロケーション	接続をリクエストする方法
CoreSite SV4、サンタプララ	CoreSite カスタマーポータル を使用して注文を行います。フォームに記入したら、注文内容が正確かどうかを確認し、MyCoreSite ウェブサイトを使用して承認します。
EdgeConneX、フェニックス	EdgeOS カスタマーポータル を使用して、発注してください。フォームを送信すると、EdgeConneX は承認のためにサービス注文フォームを提供します。質問は cloudaccess@edgeconnex.com に送ることができます。
Equinix LA3、エルスグンド	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix SV1 & SV5、サンノゼ	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
PhoenixNAP、フェニックス	phoenixNAP Provisioning へのお問い合わせは、provisioning@phoenixnap.com までご連絡ください。

米国西部 (オレゴン)

ロケーション	接続をリクエストする方法
CoreSite DE1、デンバー	CoreSite カスタマーポータル を使用して注文を行います。フォームに記入したら、注文の内容が正しいことを確認してから、ウェブサイトを使用して注文を承認してください。
Digital Realty SEA10、シアトル、Westin Building	Digital Realty へのお問い合わせは、amazon.orders@digitalrealty.com までご連絡ください。
EdgeConneX、ポートランド	EdgeOS カスタマーポータル を使用して、発注してください。フォームを送信すると、 EdgeConneX は承認のためにサービス注文フォームを提供します。質問は cloudaccess@edgeconnex.com に送ることができます。

ロケーション	接続をリクエストする方法
Equinix SE2、シアトル	Equinix へのお問い合わせは、support@equinix.com をご利用ください。
Pittock Block、ポートランド	E メール crossconnect@pittock.com あるいは電話番号 +1 503 226 6777 からリクエストを送信してください。
Switch SUPERNAP 8、ラスベガス	Switch SUPERNAP へのお問い合わせは、orders@supernap.com までご連絡ください。
TierPoint シアトル	sales@tierpoint.com TierPoint にお問い合わせください。

アフリカ (ケープタウン)

ロケーション	接続をリクエストする方法
Cape Town Internet Exchange/ Teraco Data Centres	Teraco へのお問い合わせは、support@teraco.co.za (Teraco の既存のお客様用) あるいは connect@teraco.co.za (新規のお客様用) までご連絡ください。
Teraco JB1、ヨハネスブルグ、南アフリカ	Teraco へのお問い合わせは、support@teraco.co.za (Teraco の既存のお客様用) あるいは connect@teraco.co.za (新規のお客様用) までご連絡ください。

アジアパシフィック (ジャカルタ)

ロケーション	接続をリクエストする方法
DCI JK3、ジャカルタ	DCI インドネシア (jessie.w@dci-indonesia.com.com) に問い合わせる。
NTT 2 データセンター、ジャカルタ	NTT (tps.cms.presales@global.ntt) に問い合わせる。

アジアパシフィック（ムンバイ）

ロケーション	接続をリクエストする方法
Equinix、ムンバイ	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
NetMagic DC2、フクストール	NetMagic Sales and Marketing への通話料無料は、18001033130 または marketing@netmagicsolutions.com までご連絡ください。
Sify Rabale、ムンバイ	Sify へのお問い合わせは、aws.directconnect@sifycorp.com までご連絡ください。
STT デリー DC 2、デリー	enquiry.AWSDX@sttelemediagdc.in で STT にお問い合わせください。
STT GDC Pvt. Ltd。VSB、チェンナイ	enquiry.AWSDX@sttelemediagdc.in で STT にお問い合わせください。
STT ハイデラバード DC 1、ハイデラバード	enquiry.AWSDX@sttelemediagdc.in で STT にお問い合わせください。

アジアパシフィック（ソウル）

ロケーション	接続をリクエストする方法
Digital Realty ICN1、ソウル	Digital Realty へのお問い合わせは、amazon.orders@digitalrealty.com までご連絡ください。
KINX ガサンデータセンター、ソウル	KINX へのお問い合わせは、sales@kinx.net までご連絡ください。
LG U+ Pyeong-Chon Mega Center、ソウル	LOA ドキュメントを kidcadmin@lguplus.co.kr および center8@kidc.net に送信してください。

アジアパシフィック（シンガポール）

ロケーション	接続をリクエストする方法
Equinix HK1、Tsuen Wan N.T.、香港特別行政区	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix SG2、シンガポール	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
グローバルスイッチ、シンガポール	Global Switch へのお問い合わせは、salessingapore@globalswitch.com までご連絡ください。
GPX、ムンバイ	GPX (Equinix) へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
iAdvantage Mega-i、香港	iAdvantage へのお問い合わせは、cs@iadvantage.net をご利用いただくか、iAdvantage Cabling Order e-Form を使用して発注してください。
Menara AIMS、クアラルンプール	既存の AIMS のお客様は、エンジニアリングワークオーダーリクエストフォームに記入し、カスタマーサービスポータルを使用して、X-Connect 注文をリクエストすることができます。リクエストを送信する際に問題がある場合は、service.delivery@aims.com.my にお問い合わせください。
TCC データセンター、バンコク	TCC テクノロジー株式会社（gateway.ne@tcc-technology.com）にお問い合わせください。

アジアパシフィック（シドニー）

ロケーション	接続をリクエストする方法
CDCTAKe 2、Canberra	CDC カスタマーポータル でカスタマーポータルにログインします。

ロケーション	接続をリクエストする方法
Datacom DH6、アックランド	Datacom TAK – アッカーランド で Datacom にお問い合わせください。
Equinix ME2、メルボルン	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix SY3、シドニー	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Global Switch、シドニー	Global Switch へのお問い合わせは、salessydney@globalswitch.com までご連絡ください。
NEXTDC C1、キャンベラ	NEXTDC へのお問い合わせは、nxtops@nextdc.com までご連絡ください。
NEXTDC M1、メルボルン	NEXTDC へのお問い合わせは、nxtops@nextdc.com までご連絡ください。
NEXTDC P1、パース	NEXTDC へのお問い合わせは、nxtops@nextdc.com までご連絡ください。
NEXTDC S2、シドニー	NEXTDC へのお問い合わせは、nxtops@nextdc.com までご連絡ください。

アジアパシフィック (東京)

ロケーション	接続をリクエストする方法
アット東京中央データセンター、東京	AT TOKYO (at-sales@attokyo.co.jp) にお問い合わせください。
Chief Telecom LY、台北	Chief Telecom へのお問い合わせは、vicky_chan@chief.com.tw までご連絡ください。
Chunghwa Telecom、台北	CHT Taipei IDC NOC へのお問い合わせは、taipei_idc@cht.com.tw までご連絡ください。

ロケーション	接続をリクエストする方法
Equinix OS1、大阪	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix TY2、東京	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
NEC 印西、印西	NEC 印西へのお問い合わせは、connection_support@ices.jp.nec.comまでご連絡ください。

カナダ（中部）

ロケーション	接続をリクエストする方法
Allied 250 Front St W、トロント	driches@alliedreit.com までお問い合わせください。
Cologix MTL3、モントリオール	Cologix へのお問い合わせは、sales@cologix.com までご連絡ください。
Cologix VAN2、バンクーバー	Cologix へのお問い合わせは、sales@cologix.com までご連絡ください。
eStruxture、モントリオール	eStruxture へのお問い合わせは、 directconnect@estruxture.com までご連絡ください。

中国 (北京)

ロケーション	接続をリクエストする方法
CIDS Jiachuang IDC、北京	dx-order@sinnet.com.cn までお問い合わせください。
Sinnet Jiuxianqiao IDC、北京	dx-order@sinnet.com.cn までお問い合わせください。

ロケーション	接続をリクエストする方法
GDS No. 3 データセンター、上海	dx@nwcdcloud.cn までお問い合わせください。
GDS No. 3 データセンター、深川	dx@nwcdcloud.cn までお問い合わせください。

中国 (寧夏)

ロケーション	接続をリクエストする方法
Industrial Park IDC、寧夏	dx@nwcdcloud.cn までお問い合わせください。
Shapotou IDC、寧夏	dx@nwcdcloud.cn までお問い合わせください。

欧州 (フランクフルト)

ロケーション	接続をリクエストする方法
CE Colo、プラハ、チェコ共和国	CE Colo へのお問い合わせは、info@cecolo.com までご連絡ください。
DigiPlex Ulven、オスロ、ノルウェー	helpme@digiplex.com DigiPlex にお問い合わせください。
Equinix AM3、アムステルダム、オランダ	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix FR5、フランクフルト	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix HE6、ヘルシンキ	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。

ロケーション	接続をリクエストする方法
Equinix MU1、ミュンヘン	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix WA1、ワルシャワ	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Interxion AMS7、アムステルダム	Interxion へのお問い合わせは、customer.services@interxion.com までご連絡ください。
Interxion CPH2、コペンハーゲン	Interxion へのお問い合わせは、customer.services@interxion.com までご連絡ください。
Interxion FRA6、フランクフルト	Interxion へのお問い合わせは、customer.services@interxion.com までご連絡ください。
Interxion MAD2、マドリード	Interxion へのお問い合わせは、customer.services@interxion.com までご連絡ください。
Interxion VIE2、ウィーン	Interxion へのお問い合わせは、customer.services@interxion.com までご連絡ください。
Interxion ZUR1、チューリッヒ	Interxion へのお問い合わせは、customer.services@interxion.com までご連絡ください。
IPB、ベルリン	IPB へのお問い合わせは、kontakt@ipb.de までご連絡ください。
Equinix ITConic、MD2、マドリード	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。

欧州 (アイルランド)

ロケーション	接続をリクエストする方法
Digital Realty (英国)、ドックランズ	Digital Realty (UK) へのお問い合わせは、amazon.orders@digitalrealty.com までご連絡ください。

ロケーション	接続をリクエストする方法
Eircom Clonshaugh	Eircom へのお問い合わせは、awsorders@eircom.ie までご連絡ください。
Equinix DX1、ダブリン	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix LD5、ロンドン (スラウ)	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Interxion DUB2、ダブリン	Interxion へのお問い合わせは、customer.services@interxion.com までご連絡ください。
Interxion MRS1、マルセイユ	Interxion へのお問い合わせは、customer.services@interxion.com までご連絡ください。

欧州 (ミラノ)

ロケーション	接続をリクエストする方法
CDLAN srl Via Caldera 21, Milano	CDLAN (sales@cdlan.it) までお問い合わせください。
Equinix、ML2、ミラノ、イタリア	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。

欧州 (ロンドン)

ロケーション	接続をリクエストする方法
Digital Realty (英国)、ドックランズ	Digital Realty (UK) へのお問い合わせは、amazon.orders@digitalrealty.com までご連絡ください。
Equinix LD5、ロンドン (スラウ)	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。

ロケーション	接続をリクエストする方法
Equinix MA3、マンチェスター	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Telehouse West、ロンドン	Telehouse UK へのお問い合わせは、sales.support@uk.telehouse.net までご連絡ください。

欧州 (パリ)

ロケーション	接続をリクエストする方法
Equinix PA3、パリ	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Interxion PAR7、パリ	Interxion へのお問い合わせは、customer.services@interxion.com までご連絡ください。
テレハウスボルテール、パリ	お問い合わせページを使用して Telehouse Patch Voltaire https://www.telehouse.net/contact-telehouse/にお問い合わせください。

欧州 (ストックホルム)

ロケーション	接続をリクエストする方法
Interxion STO1、ストックホルム	Interxion へのお問い合わせは、customer.services@interxion.com までご連絡ください。

欧州 (チューリッヒ)

ロケーション	接続をリクエストする方法
Equinix ZRH51、オーベレンクシュトリンゲン、スイス	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。

イスラエル (テルアビブ)

ロケーション	接続をリクエストする方法
MedOne、ハイファ	support@Medone.co.il MedOne へのお問い合わせ
EdgeConnex、ヘルツリヤ語	info@edgeconnecx.com EdgeConnect へのお問い合わせ

中東 (バーレーン)

ロケーション	接続をリクエストする方法
AWS バーレーン DC53、マナマ	接続を完了するには、現地のネットワークプロバイダーパートナーと連携して接続を確立します。次に、ネットワークプロバイダーから にAWS サポートセンター AWS 経由で認証書 (LOA) を提供します。 はこの場所でクロスコネクト AWS を完了します。
AWS バーレーン DC52、マナマ	接続を完了するには、現地のネットワークプロバイダーパートナーと連携して接続を確立します。次に、ネットワークプロバイダーから にAWS サポートセンター AWS 経由で認証書 (LOA) を提供します。 はこの場所でクロスコネクト AWS を完了します。

中東 (アラブ首長国連邦)

ロケーション	接続をリクエストする方法
Equinix DX1、ドバイ、アラブ首長国連邦	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Etisalat SmartHub データセンター、アラブ首長国連邦フジャイラ	Etisalat SmartHub データセンターへのお問い合わせは、IntlSales-C&WS@etisalat.ae までご連絡ください。

南米 (サンパウロ)

ロケーション	接続をリクエストする方法
Equinix RJ2、リオデジャネイロ	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Equinix SP4、サンパウロ	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。
Tivit	Tivit へのお問い合わせは、aws@tivit.com.br までご連絡ください。

AWS GovCloud （ 米国東部 ）

このリージョンで接続を注文することはできません。

AWS GovCloud （ 米国西部 ）

ロケーション	接続をリクエストする方法
Equinix SV5、サンノゼ	Equinix へのお問い合わせは、awsdealreg@equinix.com までご連絡ください。

AWS Direct Connect 仮想インターフェイス

接続の使用 AWS Direct Connect を開始するには、次のいずれかの仮想インターフェイス (VIFsを作成する必要があります。

- プライベート仮想インターフェイス: プライベート IP アドレスを使って Amazon VPC にアクセスするには、プライベート仮想インターフェイスを使用する必要があります。
- パブリック仮想インターフェイス: パブリック仮想インターフェイスは、 AWS パブリック IP アドレスを使用してすべてのパブリックサービスにアクセスできます。
- トランジット仮想インターフェイス: Direct Connect ゲートウェイに関連付けられた 1 つまたは複数の Amazon VPC Transit Gateway にアクセスするには、トランジット仮想インターフェイスを使用する必要があります。トランジット仮想インターフェイスは、任意の速度の AWS Direct Connect 専用接続またはホスト接続で使用できます。Direct Connect ゲートウェイの設定については、「the section called “Direct Connect ゲートウェイ”」を参照してください。

IPv6 アドレスを使用して他の AWS サービスに接続するには、サービスドキュメントで IPv6 アドレス指定がサポートされていることを確認します。

パブリック仮想インターフェイスプレフィックス広告ルール

VPCsまたは他の AWS サービスに到達できるように、適切な Amazon プレフィックスをお客様にアドバタイズします。この接続を介して、Amazon EC2、Amazon S3、 など、すべての AWS プレフィックスにアクセスできます。 Amazon.com Amazon 以外のプレフィックスにアクセスできません。によってアドバタイズされるプレフィックスの現在のリストについては AWS、AWS 「」の「IP アドレス範囲 AWS 」を参照してくださいAmazon Web Services 全般のリファレンス。 AWS Direct Connect パブリック仮想インターフェイスを介して受信したカスタマープレフィックスを他のカスタマーに再アドバタイズすることはありません。パブリック仮想インターフェイスとルーティングポリシーの詳細については、「the section called “パブリック仮想インターフェイスのルーティングポリシー”」を参照してください。

> **Note**
>
> ファイアウォールフィルタ (パケットの送信元/送信先アドレスに基づいて) を使用して、一部のプレフィックスに出入りするトラフィックを制御することをお勧めします。プレフィックスフィルタ (ルートマップ) を使用している場合は、正確に一致するかそれより長いプレフィックスを受け入れるようにしてください。からアドバタイズされるプレフィックス

AWS Direct Connect は集計され、プレフィックスフィルターで定義されているプレフィックスとは異なる場合があります。

ホスト型仮想インターフェイス

別のアカウントと AWS Direct Connect の接続を使用するには、そのアカウントのホスト仮想インターフェイスを作成します。他のアカウントの所有者は、利用を開始するためにはホスト仮想インターフェイスを受け入れる必要があります。ホスト仮想インターフェイスは、標準仮想インターフェイスと同様に機能し、パブリックリソースまたは VPC に接続できます。

トランジット仮想インターフェイスは任意の速度の Direct Connect 専用接続またはホスト接続で使用できます。ホスト接続でサポートされる仮想インターフェイスは 1 つのみです。

仮想インターフェイスを作成するには、次の情報が必要です。

リソース	必要な情報
Connection	仮想インターフェイスを作成する AWS Direct Connect 接続またはリンク集約グループ (LAG)。
仮想インターフェイス名	仮想インターフェイスの名前。
仮想インターフェイス所有者	別の アカウントの仮想インターフェイスを作成する場合は、他の AWS アカウントのアカウント ID が必要です。
(プライベート仮想インターフェイスのみ) 接続	同じ AWS リージョンの VPC に接続するには、VPC の仮想プライベートゲートウェイが必要です。Amazon 側の BGP セッションのための ASN は、仮想プライベートゲートウェイから継承されます。仮想プライベートゲートウェイを作成するときに、独自のプライベート ASN を指定できます。そうでない場合は、Amazon によってデフォルトの ASN が指定されます。詳細については、Amazon VPC ユーザーガイドの Create a Virtual Private Gateway を参照してください。Direct Connect Gateway 経由で VPC に接続する場合は、Direct Connect Gateway が必要です。詳細については、「Direct Connect Gateway」を参照してください。
VLAN	仮想ローカルエリアネットワーク (VLAN) の、まだ接続で使用されていない一意のタグ。値は 1 ~ 4094 を指定する必要があります。またイーサネッ

リソース	必要な情報
	ト 802.1Q 規格を満たしている必要があります。このタグは、 AWS Direct Connect 接続を通過するすべてのトラフィックに必要です。 ホスト接続がある場合、 AWS Direct Connect パートナーはこの値を提供します。仮想インターフェイス作成後に値を変更することはできません。

リソース	必要な情報

ピア IP アドレス	仮想インターフェイスは、IPv4 または IPv6 に対して 1 つの BGP ピアリングセッションをサポートできます。または両方に対して 1 つずつ BGP ピアリングセッションをサポートできます (デュアルスタック)。パブリック仮想インターフェイスの作成に Amazon プールからの Elastic IP (EIP) および Bring your own IP アドレス (BYOIP) を使用して作成しないでください。同じ仮想インターフェイスで同じ IP アドレスファミリに対して複数の BGP セッションを作成することはできません。BGP ピアセッションでは、仮想インターフェイスの両端に IP アドレス範囲が割り当てられます。
	
	• IPv4:
	  • (パブリック仮想インターフェイスのみ) お客様が所有している一意のパブリック IPv4 アドレスを指定する必要があります。以下のいずれかを指定できます。
	  • カスタマー所有 IPv4 CIDR
	
	これらは任意のパブリック IPs (顧客所有または が提供する AWS) にすることができますが、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、などの/31範囲を割り当てる場合は、ピア IP 203.0.113.0 にを203.0.113.0/31 、 AWS ピア IP 203.0.113.1 に を使用できます。または、 などの/24範囲を割り当てる場合は、ピア IP 198.51.100.10 に を198.51.100.0/24 、 AWS ピア IP 198.51.100.20 に を使用できます。
	  • AWS Direct Connect パートナーまたは ISP が所有する IP 範囲と LOA-CFA 認証
	  • AWSが提供する /31 CIDR。AWS Support に連絡して、パブリック IPv4 CIDR をリクエストします (リクエストにはユースケースを提供します)
	
	Note
	AWSが提供するパブリック IPv4 アドレスに対するすべてのリクエストを当社が処理できることを保証することはできません。

リソース	必要な情報
	• (プライベート仮想インターフェイスのみ) Amazon がプライベート IPv4 アドレスを自動的に生成できます。独自の CIDRs を指定してください。 AWS 例えば、ローカルネットワークから他の IP アドレスを指定しないでください。パブリック仮想インターフェイスと同様に、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、 などの/30範囲を割り当てる場合は、ピア IP 192.168.0.1 に を192.168.0.0/30 、 AWS ピア IP 192.168.0.2 に を使用できます。 • IPv6: Amazon は /125 IPv6 CIDR を自動的に割り当てます。独自のピア IPv6 アドレスを指定することはできません。
アドレスファミリー	BGP ピアリングセッションが IPv4 と IPv6 のどちらを使用するか。
BGP 情報	• BGP セッションのお客様側のパブリックまたはプライベート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)。パブリック ASN を使用する場合は、お客様が所有者であることが必要です。プライベート ASN を使用している場合は、カスタム ASN 値を設定できます。16 ビット ASN では、値は 64512 から 65534 の範囲内である必要があります。32 ビット ASN では、値は 1 から 2,147,483,647 の範囲内である必要があります。パブリック仮想インターフェイス用のプライベート ASN を使用する場合、自律システム (AS) の前置は動作しません。 • AWS はデフォルトで MD5 を有効にします。この値を変更することはできません。 • MD5 BGP 認証キー。独自のキーを指定するか、Amazon で自動的に生成することができます。

リソース	必要な情報

(パブリック仮想インターフェイスのみ) アドバタイズするプレフィックス	BGP 経由でアドバタイズするパブリックの IPv4 ルートまたは IPv6 ルート。BGP を使用して少なくとも 1 つ (最大 1,000 個) のプレフィックスをアドバタイズする必要があります。
	• IPv4: IPv4 CIDR は、次のいずれか AWS Direct Connect に該当する場合、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs異なる AWS リージョンから取得されます。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• IPv6: /64 以下のプレフィックスの長さを指定します。
	• AWS Support に連絡することによって、既存のパブリック VIF にプレフィックスを追加し、それらをアドバタイズすることができます。サポートケースで、パブリック VIF に追加してアドバタイズしたい追加の CIDR プレフィックスのリストを提供してください。
	• Direct Connect パブリック仮想インターフェイスでは、任意のプレフィックス長を指定できます。IPv4 は /1 から /32 までのすべてをサポートし、IPv6 は /1 から /64 までのすべてをサポートする必要があります。

リソース	必要な情報
(プライベート仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェースの MTU を 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。ジャンボフレームは、 から伝播されたルートにのみ適用されます AWS Direct Connect。仮想プライベートゲートウェイを指すルートテーブルに静的ルートを追加する場合、静的ルートを介してルーティングされるトラフィックは 1500 MTU を使用して送信されます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでジャンボフレームを選択し、仮想インターフェイスの一般的な設定ページで使用可能なジャンボフレームを見つけます。
(トランジット仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェイスの MTU を 8500 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。Direct Connect では、最大 8500 MTU のジャンボフレームがサポートされます。Transit Gateway ルートテーブルで設定された静的なルートと伝播されたルートはジャンボフレームをサポートします。これには、VPC の静的なルートテーブルのエントリを持つ EC2 インスタンスから Transit Gateway アタッチメントへのものが含まれます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでジャンボフレームを選択し、仮想インターフェイスの一般的な設定ページで使用可能なジャンボフレームを見つけます。

SiteLink

プライベート仮想インターフェイスまたはトランジット仮想インターフェイスを作成する場合は、を使用できます SiteLink。

SiteLink は、仮想プライベートインターフェイス用のオプションの Direct Connect 機能で、 AWS ネットワーク上で使用可能な最短パスを使用して、同じ AWS パーティション内の任意の 2 つの Direct Connect のプレゼンスポイント (PoPs) 間の接続を可能にします。これにより、トラフィックをリージョン経由でルーティングすることなく、 AWS グローバルネットワークを介してオンプレミスネットワークに接続できます。詳細については、「 の紹介 AWS Direct Connect SiteLink SiteLink 」を参照してください。

> **Note**
>
> SiteLink は、 AWS GovCloud (US) および中国リージョンでは使用できません。

の使用には別途料金が発生します SiteLink。詳細については、AWS Direct Connect の料金を参照してください。

SiteLink は、すべての仮想インターフェイスタイプをサポートしているわけではありません。以下の表には、インターフェイスの種類と、サポートされるかどうかが記載されています。

仮想インターフェイスのタイプ	サポート対象/サポート対象外
トランジット仮想インターフェイス	サポート
仮想ゲートウェイを使用して Direct Connect ゲートウェイにアタッチされたプライベート仮想インターフェイス	サポート
仮想ゲートウェイまたはトランジットゲートウェイに関連付けられていない Direct Connect ゲートウェイにアタッチされたプライベート仮想インターフェイス	サポート

仮想インターフェイスのタイプ	サポート対象/サポート対象外
仮想ゲートウェイにアタッチされたプライベート仮想インターフェイス	サポートされていません
パブリック仮想インターフェイス	サポートされていません

SiteLink 有効な仮想インターフェイスを介した AWS リージョン（ 仮想ゲートウェイまたはトランジットゲートウェイ) からオンプレミスの場所へのトラフィックのトラフィックルーティング動作は、 AWS パスの先頭にあるデフォルトの Direct Connect 仮想インターフェイス動作とは若干異なります。を有効にすると、 SiteLinkの仮想インターフェイスは、関連付けられたリージョンに関係なく、Direct Connect の場所からの AS パスの長さが小さい BGP パスを AWS リージョン 優先します。例えば、Direct Connect の場所ごとに、関連するリージョンがアドバタイズされます。 SiteLink が無効になっている場合、仮想ゲートウェイまたはトランジットゲートウェイからのトラフィックは、異なるリージョンに関連付けられた Direct Connect ロケーションからのルーターが AS パスの長さが短いパスをアドバタイズする場合でも AWS リージョン、その に関連付けられた Direct Connect ロケーションをデフォルトで優先します。仮想ゲートウェイまたはトランジットゲートウェイは、引き続き Direct Connect ロケーションからのパスを、関連する AWS リージョンよりも優先します。

SiteLink は、仮想インターフェイスのタイプに応じて、8500 または 9001 の最大ジャンボフレーム MTU サイズをサポートします。詳細については、「the section called “プライベート仮想インターフェイスまたはトランジット仮想インターフェイスのネットワーク MTU の設定”」を参照してください。

仮想インターフェイスの前提条件

仮想インターフェイスを作成する前に、以下を実行します。

- 接続を作成します。詳細については、「the section called “接続ウィザードを使用して接続を作成する”」を参照してください。
- 単一のものとして扱う複数の接続がある場合には、Link Aggregation Group (LAG) を作成します。詳細については、接続を LAG に関連付ける を参照してください。

仮想インターフェイスを作成するには、次の情報が必要です。

リソース	必要な情報
Connection	仮想インターフェイスを作成する AWS Direct Connect 接続またはリンク集約グループ (LAG)。
仮想インターフェイス名	仮想インターフェイスの名前。
仮想インターフェイス所有者	別の アカウントの仮想インターフェイスを作成する場合は、他の AWS アカウントのアカウント ID が必要です。
(プライベート仮想インターフェイスのみ) 接続	同じ AWS リージョンの VPC に接続するには、VPC の仮想プライベートゲートウェイが必要です。Amazon 側の BGP セッションのための ASN は、仮想プライベートゲートウェイから継承されます。仮想プライベートゲートウェイを作成するときに、独自のプライベート ASN を指定できます。そうでない場合は、Amazon によってデフォルトの ASN が指定されます。詳細については、Amazon VPC ユーザーガイドの Create a Virtual Private Gateway を参照してください。Direct Connect Gateway 経由で VPC に接続する場合は、Direct Connect Gateway が必要です。詳細については、「Direct Connect Gateway」を参照してください。
VLAN	仮想ローカルエリアネットワーク (VLAN) の、まだ接続で使用されていない一意のタグ。値は 1 ~ 4094 を指定する必要があります。またイーサネット 802.1Q 規格を満たしている必要があります。このタグは、 AWS Direct Connect 接続を通過するすべてのトラフィックに必要です。 ホスト接続がある場合、 AWS Direct Connect パートナーはこの値を提供します。仮想インターフェイス作成後に値を変更することはできません。
ピア IP アドレス	仮想インターフェイスは、IPv4 または IPv6 に対して 1 つの BGP ピアリングセッションをサポートできます。または両方に対して 1 つずつ BGP ピアリングセッションをサポートできます (デュアルスタック)。パブリック仮想インターフェイスの作成に Amazon プールからの Elastic IP (EIP) および Bring your own IP アドレス (BYOIP) を使用して作成しないでください。同じ仮想インターフェイスで同じ IP アドレスファミリに対して複数の BGP セッショ

リソース	必要な情報

	ンを作成することはできません。BGP ピアセッションでは、仮想インターフェイスの両端に IP アドレス範囲が割り当てられます。
	
	• IPv4:
	  • (パブリック仮想インターフェイスのみ) お客様が所有している一意のパブリック IPv4 アドレスを指定する必要があります。以下のいずれかを指定できます。
	  • カスタマー所有 IPv4 CIDR
	
	これらは任意のパブリック IPs (顧客所有または が提供する AWS) にすることができますが、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、などの/31範囲を割り当てる場合は、ピア IP 203.0.113.0 にを203.0.113.0/31 、 AWS ピア IP 203.0.113.1 に を使用できます。または、 などの/24範囲を割り当てる場合は、ピア IP 198.51.100.10 に を198.51.100.0/24 、 AWS ピア IP 198.51.100.20 に を使用できます。
	  • AWS Direct Connect パートナーまたは ISP が所有する IP 範囲と LOA-CFA 認証
	  • AWSが提供する /31 CIDR。AWS Support に連絡して、パブリック IPv4 CIDR をリクエストします (リクエストにはユースケースを提供します)
	
	Note
	AWSが提供するパブリック IPv4 アドレスに対するすべてのリクエストを当社が処理できることを保証することはできません。
	  • (プライベート仮想インターフェイスのみ) Amazon がプライベート IPv4 アドレスを自動的に生成できます。独自の CIDRs を指定してください。 AWS 例えば、ローカルネットワークから他の IP アドレスを指定しないでください。パブリック仮想インターフェイスと同様に、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。例えば、 などの/30範囲を割り当てる場合は、ピア IP

リソース	必要な情報
	192.168.0.1 に を192.168.0.0/30 、 AWS ピア IP 192.168.0.2 に を使用できます。 • IPv6: Amazon は /125 IPv6 CIDR を自動的に割り当てます。独自のピア IPv6 アドレスを指定することはできません。
アドレスファミリー	BGP ピアリングセッションが IPv4 と IPv6 のどちらを使用するか。
BGP 情報	• BGP セッションのお客様側のパブリックまたはプライベート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)。パブリック ASN を使用する場合は、お客様が所有者であることが必要です。プライベート ASN を使用している場合は、カスタム ASN 値を設定できます。16 ビット ASN では、値は 64512 から 65534 の範囲内である必要があります。32 ビット ASN では、値は 1 から 2,147,483,647 の範囲内である必要があります。パブリック仮想インターフェイス用のプライベート ASN を使用する場合、自律システム (AS) の前置は動作しません。 • AWS はデフォルトで MD5 を有効にします。この値を変更することはできません。 • MD5 BGP 認証キー。独自のキーを指定するか、Amazon で自動的に生成することができます。

リソース	必要な情報

(パブリック仮想インターフェイスのみ) アドバタイズするプレフィックス	BGP 経由でアドバタイズするパブリックの IPv4 ルートまたは IPv6 ルート。BGP を使用して少なくとも 1 つ (最大 1,000 個) のプレフィックスをアドバタイズする必要があります。
	• IPv4: IPv4 CIDR は、次のいずれか AWS Direct Connect に該当する場合、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs異なる AWS リージョンから取得されます。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• IPv6: /64 以下のプレフィックスの長さを指定します。
	• AWS Support に連絡することによって、既存のパブリック VIF にプレフィックスを追加し、それらをアドバタイズすることができます。サポートケースで、パブリック VIF に追加してアドバタイズしたい追加の CIDR プレフィックスのリストを提供してください。
	• Direct Connect パブリック仮想インターフェイスでは、任意のプレフィックス長を指定できます。IPv4 は /1 から /32 までのすべてをサポートし、IPv6 は /1 から /64 までのすべてをサポートする必要があります。

リソース	必要な情報
(プライベート仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェースの MTU を 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。ジャンボフレームは、 から伝播されたルートにのみ適用されます AWS Direct Connect。仮想プライベートゲートウェイを指すルートテーブルに静的ルートを追加する場合、静的ルートを介してルーティングされるトラフィックは 1500 MTU を使用して送信されます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでジャンボフレームを選択し、仮想インターフェイスの一般的な設定ページで使用可能なジャンボフレームを見つけます。
(トランジット仮想インターフェイスのみ) Jumbo Frames	経由のパケットの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェイスの MTU を 8500 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。Direct Connect では、最大 8500 MTU のジャンボフレームがサポートされます。Transit Gateway ルートテーブルで設定された静的なルートと伝播されたルートはジャンボフレームをサポートします。これには、VPC の静的なルートテーブルのエントリを持つ EC2 インスタンスから Transit Gateway アタッチメントへのものが含まれます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでジャンボフレームを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが対応しているかどうかを確認します。

仮想インターフェイスを作成するときに、仮想インターフェイスを所有するアカウントを指定できます。自分の AWS アカウントではないアカウントを選択すると、次のルールが適用されます。

- プライベート VIF およびトランジット VIF の場合、アカウントは仮想インターフェイスおよび仮想プライベートゲートウェイ/Direct Connect ゲートウェイの宛先に適用されます。

- パブリック VIF の場合、アカウントは仮想インターフェイスの課金に使用されます。Data Transfer Out (DTO) の使用量は、 AWS Direct Connect データ転送レートでリソース所有者に対して計測されます。

> **Note**
>
> 31 ビットプレフィックスは、すべての Direct Connect 仮想インターフェイスタイプでサポートされています。詳細については、「RFC 3021: Using 31-Bit Prefixes on IPv4 Point-to-Point Links」(RFC 3021: IPv4 ポイントツーポイントリンクでの 31 ビットプレフィックスの使用) を参照してください。

仮想インターフェイスを作成する

トランジットゲートウェイに接続するにはトランジット仮想インターフェイスを、パブリックリソース (非 VPC サービス) に接続するにはパブリック仮想インターフェイスを、VPC に接続するにはプライベート仮想インターフェイスを作成できます。

内のアカウント AWS Organizations、または とは異なるアカウントの仮想インターフェイスを作成するには、ホスト AWS Organizations された仮想インターフェイスを作成します。詳細については、「the section called “ホスト仮想インターフェイスを作成する”」を参照してください。

前提条件

作業を開始する前に、「仮想インターフェイスの前提条件」の情報を参照済みであることを確認してください。

パブリック仮想インターフェイスを作成する

パブリック仮想インターフェイスを作成する場合、そのリクエストが当社により確認され承認されるまでに、最大 72 時間かかる場合があります。

パブリック仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。

4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [パブリック] を選択します。
5. [Public Virtual Interface settings (仮想インターフェイス設定)] で以下を実行します。
   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。
   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。
   c. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。
   d. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

      有効な値は 1 ~ 2147483647 です。
6. [追加設定] で、以下を実行します。
   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

      - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
      - [Amazon ルーターのピア IP] に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

      [IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。
   b. 独自の BGP キーを指定するには、使用する BGP MD5 キーを入力します。

      値が入力されない場合は、当社の側で自動的に BGP キーを生成します。独自のキーを提供した、または当社がキーを生成した場合は、その値が [Virtual interfaces] (仮想インターフェイス) の仮想インターフェイスの詳細ページにある [BGP authentication key] (BGP 認証キー) 列に表示されます。
   c. Amazon にプレフィックスを発行するには、[アドバタイズするプレフィックス] に、この仮想インターフェイスを介してルーティングされるトラフィックのルーティング先となる IPv4 CIDR アドレスをカンマで区切って入力します。

> **Important**
>
> AWS Support に連絡することによって、既存のパブリック VIF にプレフィックスを追加し、それらをアドバタイズすることができます。サポートケースで、パブリック VIF に追加してアドバタイズしたい追加の CIDR プレフィックスのリストを提供してください。

d. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。
8. デバイス用のルーターの設定をダウンロードします。詳細については、「ルーター設定ファイルをダウンロードする」を参照してください。

コマンドラインまたは API を使用してパブリック仮想インターフェイスを作成するには

- create-public-virtual-interface (AWS CLI)
- CreatePublicVirtualInterface (AWS Direct Connect API)

プライベート仮想インターフェイスを作成する

プライベート仮想インターフェイスは、 AWS Direct Connect 接続と同じリージョンの仮想プライベートゲートウェイにプロビジョニングできます。 AWS Direct Connect ゲートウェイへのプライベート仮想インターフェイスのプロビジョニングの詳細については、「」を参照してくださいDirect Connect ゲートウェイの操作。

VPC の作成に VPC ウィザードを使用する場合、ルートの伝播が自動的に有効になります。ルートの伝播により、ルートが自動的に VPC のルートテーブルに入力されます。必要に応じて、ルートの伝播を無効にすることができます。詳細については、Amazon VPC ユーザーガイドの Enable Route Propagation in Your Route Table を参照してください。

ネットワーク接続の最大送信単位 (MTU) とは、接続を介して渡すことができる最大許容パケットサイズ (バイト単位) です。仮想プライベートインターフェイスの MTU では、1500 あるいは 9001 (ジャンボフレーム) のどちらでも使用できます。トランジット仮想プライベートインターフェイスの MTU では、1500 あるいは 8500 (ジャンボフレーム) のどちらでも使用できます。インターフェイスの作成時あるいは作成後の更新時に、MTU を指定できます。仮想インターフェイスの MTU を8500 (ジャンボフレーム) または 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。接続あるいは仮想インターフェイスがジャンボフレームをサポートしているかを確認するには、 AWS Direct Connect コンソールを選択して [概要] タブで [ジャンボフレーム対応] を見つけます。

VPC へのプライベート仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] で [プライベート] を選択します。
5. [プライベート仮想インターフェイス設定] で以下を実行します。

   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

   c. 仮想インターフェイスの所有者 で、仮想インターフェイスがアカウント用 AWS である場合はマイ AWS アカウントを選択します。

   d. [Direct Connect ゲートウェイ] の場合、[Direct Connect ゲートウェイ] を選択します。

   e. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

   f. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

      有効な値は 1 ~ 2,147,483,647 です。

6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

- これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
- [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

> **Important**
>
> IPv4 アドレス AWS の自動割り当てを許可すると、RFC 3927 に従って 169.254.0.0/16 IPv4 Link-Local から /29 CIDR が接続用に割り当てられます。VPC point-to-point AWS トラフィックの送信元および/または送信先としてカスタマールーターピア IP アドレスを使用する場合は、このオプションは推奨されません。代わりに、RFC 1918 または他のアドレス (RFC 1918 以外) を使用して、アドレスを自分で指定する必要があります。
>
> - RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。
> - RFC 3927 の詳細については、「IPv4 リンクローカルアドレスのダイナミック設定」を参照してください。

[IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

b. 最大送信単位 (MTU) を 1500 (デフォルト) から 9001 (ジャンボフレーム) に変更するには、[ジャンボ MTU (MTU サイズ 9001)] を選択します。

c. (オプション) の有効化 SiteLinkで、有効化 を選択して Direct Connect のプレゼンスポイント間の直接接続を有効にします。

d. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。
8. デバイス用のルーターの設定をダウンロードします。詳細については、「ルーター設定ファイルをダウンロードする」を参照してください。

コマンドラインまたは API を使用してプライベート仮想インターフェイスを作成するには

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface (AWS Direct Connect API)

Direct Connect ゲートウェイと接続するトランジット仮想インターフェイスを作成する

AWS Direct Connect 接続をトランジットゲートウェイに接続するには、接続用のトランジットインターフェイスを作成する必要があります。接続先の Direct Connect ゲートウェイを指定します。

ネットワーク接続の最大送信単位 (MTU) とは、接続を介して渡すことができる最大許容パケットサイズ (バイト単位) です。仮想プライベートインターフェイスの MTU では、1500 あるいは 9001 (ジャンボフレーム) のどちらでも使用できます。トランジット仮想プライベートインターフェイスの MTU では、1500 あるいは 8500 (ジャンボフレーム) のどちらでも使用できます。インターフェイスの作成時あるいは作成後の更新時に、MTU を指定できます。仮想インターフェイスの MTU を8500 (ジャンボフレーム) または 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。接続あるいは仮想インターフェイスがジャンボフレームをサポートしているかを確認するには、 AWS Direct Connect コンソールを選択して [概要] タブで [ジャンボフレーム対応] を見つけます。

> **Important**
>
> Transit Gateway を 1 つ以上の Direct Connect ゲートウェイに関連付ける場合、Transit Gateway およびその Direct Connect ゲートウェイで使用される自律システム番号 (ASN) は異なる値である必要があります。たとえば、Transit Gateway と Direct Connect ゲートウェイの両方にデフォルトの ASN 64512 を使用すると、関連付けのリクエストは失敗します。

Direct Connect ゲートウェイへのトランジット仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。

4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [Transit (トランジット)] を選択します。
5. [Transit virtual interface settings (トランジット仮想インターフェイス設定)] で以下を実行します。

   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

   c. 仮想インターフェイスの所有者 で、仮想インターフェイスがアカウント用 AWS である場合はマイ AWS アカウントを選択します。

   d. [Direct Connect ゲートウェイ] の場合、[Direct Connect ゲートウェイ] を選択します。

   e. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

   f. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

      有効な値は 1 ~ 2,147,483,647 です。
6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

      - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
      - [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

      > **Important**
      >
      > IPv4 アドレス AWS の自動割り当てを許可すると、RFC 3927 に従って 169.254.0.0/16 IPv4 Link-Local から /29 CIDR が接続用に割り当てられます。VPC point-to-point AWS トラフィックの送信元および/または送信先としてカスタマールーターピア IP アドレスを使用する場合は、このオプションは推奨されません。代わりに、RFC 1918 または他のアドレス (RFC 1918 以外) を使用して、アドレスを自分で指定する必要があります。
      >
      > - RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。

- RFC 3927 の詳細については、「IPv4 リンクローカルアドレスのダイナミック設定」を参照してください。

[IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

b. 最大送信単位 (MTU) を 1500 (デフォルト) から 8500 (ジャンボフレーム) に変更するには、[ジャンボ MTU (MTU サイズ 8500)] を選択します。

c. (オプション) の有効化 SiteLinkで、有効化 を選択して Direct Connect のプレゼンスポイント間の直接接続を有効にします。

d. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

仮想インターフェイスを作成したら、デバイス用のルーター設定をダウンロードできます。詳細については、「ルーター設定ファイルをダウンロードする」を参照してください。

コマンドラインまたは API を使用してトランジット仮想インターフェイスを作成するには

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface (AWS Direct Connect API)

コマンドラインまたは API を使用して、Direct Connect ゲートウェイにアタッチされた仮想インターフェイスを表示するには

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGateway添付ファイル (AWS Direct Connect API)

ルーター設定ファイルをダウンロードする

仮想インターフェイスを作成してインターフェイスの状態がアップになったら、ルーターのルーター設定ファイルをダウンロードできます。

MACSec をオンにした仮想インターフェイスに次のいずれかのルータを使用すると、そのルータの設定ファイルが自動的に作成されます。

- NX-OS 9.3 以降のソフトウェアを実行している Cisco Nexus 9K+ シリーズスイッチ
- JunOS 9.5 以降のソフトウェアを実行しているジュニパーネットワークス M/MX シリーズルータ

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. 仮想インターフェイスを選択したら、[View details (詳細の表示)] を選択します。
4. [ルーター設定をダウンロードする] を選択します。
5. [ルーター設定をダウンロードする] で、次を実行します。
   a. [Vendor] で、ルーターの製造元を選択します。
   b. [Platform] で、ルーターのモデルを選択します。
   c. [Software] で、ルーターのソフトウェアのバージョンを選択します。
6. [ダウンロード] を選択してから、ルーターに対応する適切な設定を使用して AWS Direct Connectに接続できることを確認します。

MacSec に関する考慮事項

ご使用のルータで MACsec の使用を手動で設定する必要がある場合は、次の表のガイドラインを参照してください。

Parameter	説明
CKN の長さ	これは 16 進数 (0～9、A～F) を表す 64 文字の文字列です。クロスプラットフォームの互換性を最大化するために、文字数をすべて使用してください。
CAK の長さ	これは 16 進数 (0～9、A～F) を表す 64 文字の文字列です。クロスプラットフォームの互換性を最大化するために、文字数をすべて使用してください。

Parameter	説明
暗号アルゴリズム	AES_256_CMAC
SAK 暗号スイート	• 100 Gbps の接続の場合: GCM_AES_XPN_256 • 10 Gbps の接続の場合: GCM_AES_XPN_256 または GCM_AES _256
キー暗号スイート	16
機密性オフセット	0
ICVインジケータ	いいえ
SAK キー再生成時間	PN ロールオーバー >

仮想インターフェイスの詳細を表示する

仮想インターフェイスの現在のステータスを表示できます。詳細は次のとおりです。

- 接続状態
- 名前
- 場所
- VLAN
- BGP の詳細
- ピア IP アドレス

仮想インターフェイスに関する詳細を表示するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. 左側のペインで、[仮想インターフェイス] を選択します。
3. 仮想インターフェイスを選択したら、[View details (詳細の表示)] を選択します。

コマンドラインまたは API を使用して仮想インターフェイスを説明するには

- describe-virtual-interfaces (AWS CLI)
- DescribeVirtualインターフェイス (AWS Direct Connect API)

BGP ピアを追加もしくは削除する

IPv4 または IPv6 BGP ピアセッションを仮想インターフェイスに追加または削除します。

仮想インターフェースは、単一の IPv4 BGP ピアリングセッションと単一の IPv6 BGP ピアリングセッションをサポートできます。

IPv6 BGP ピアリングセッションに独自のピア IPv6 アドレスを指定することはできません。Amazon は /125 IPv6 CIDR を自動的に割り当てます。

マルチプロトコル BGP はサポートされていません。IPv4 と IPv6 は、仮想インターフェイスのデュアルスタックモードで動作します。

AWS はデフォルトで MD5 を有効にします。この値を変更することはできません。

BGP ピアを追加する

以下の手順に従って BGP ピアを追加します。

BGP ピアを追加するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. 仮想インターフェイスを選択したら、[View details (詳細の表示)] を選択します。

4. [ピア接続の追加] を選択します。
5. (プライベート仮想インターフェイス) IPv4 BGP ピアを追加するには、以下を実行します。
   - [IPv4] を選択します。
   - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。[Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。
6. (パブリック仮想インターフェイス) IPv4 BGP ピアを追加するには、以下を実行します。
   - [ルーターのピア IP] に、トラフィックの送信先となる IPv4 CIDR アドレスを入力します。
   - [Amazon ルーターのピア IP] に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

   > **Important**
   >
   > IP アドレス AWS の自動割り当てを許可すると、169.254.0.0/16. から /29 CIDR AWS が割り当てられるため、カスタマールーターピア IP アドレスをトラフィックの送信元と送信先として使用する場合は、このオプションは推奨されません。代わりに、RFC 1918 または他のアドレスを使用して、アドレスを自分で指定する必要があります。RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。
7. (プライベートまたはパブリックの仮想インターフェイス) IPv6 BGP ピアを追加するには、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。
8. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

   パブリック仮想インターフェースの場合、ASN はプライベートであるか、仮想インターフェースの許可リストに登録済みであることが必要です。

   有効な値は 1 ~ 2147483647 です。

   値を入力しない場合は、自動的に値が割り当てられます。
9. 独自の BGP キーを指定するには、[BGP 認証キー] に使用する BGP MD5 キーを入力します。
10. [ピア接続の追加] を選択します。

コマンドラインまたは API を使用して BGP ピアを作成するには

- create-bgp-peer (AWS CLI)
- CreateBGPPeer (AWS Direct Connect API)

BGP ピアを削除する

仮想インターフェイスに IPv4 と IPv6 の両方のピアリングセッションがある場合は、一方の BGP ピアリングセッションを削除できます (両方を削除することはできません)。

BGP ピアを削除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. 仮想インターフェイスを選択したら、[View details (詳細の表示)] を選択します。
4. [Peerings (ピア)] で削除するピアを選択したら、[Delete (削除)] を選択します。
5. [Remove peering from virtual interface (仮想インターフェイスからピアを削除する)] ダイアログボックスで、[Delete (削除)] を選択します。

コマンドラインまたは API を使用して BGP ピアを削除するには

- delete-bgp-peer (AWS CLI)
- DeleteBGPPeer (AWS Direct Connect API)

プライベート仮想インターフェイスまたはトランジット仮想インターフェイスのネットワーク MTU の設定

AWS Direct Connect は、リンクレイヤーで 1522 バイトまたは 9023 バイト (14 バイトのイーサネットヘッダー + 4 バイトの VLAN タグ + IP データグラムのバイト + 4 バイトの FCS) のイーサネットフレームサイズをサポートします。

ネットワーク接続の最大送信単位 (MTU) とは、接続を介して渡すことができる最大許容パケットサイズ (バイト単位) です。仮想プライベートインターフェイスの MTU では、1500 あるいは 9001 (ジャンボフレーム) のどちらでも使用できます。トランジット仮想プライベートインターフェイスの

MTU では、1500 あるいは 8500 (ジャンボフレーム) のどちらでも使用できます。インターフェイスの作成時あるいは作成後の更新時に、MTU を指定できます。仮想インターフェイスの MTU を8500 (ジャンボフレーム) または 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでそれを選択し、概要タブでジャンボフレーム機能を見つけます。

プライベート仮想インターフェイスまたはトランジット仮想インターフェイスに対してジャンボフレームを有効にすると、インターフェイスを関連付けることができるのはジャンボフレーム対応の接続または LAG のみになります。ジャンボフレームは、仮想プライベートゲートウェイもしくは Direct Connect ゲートウェイにアタッチされたプライベート仮想インターフェイス、または Direct Connect ゲートウェイにアタッチされたトランジット仮想インターフェイスでサポートされます。同じルートをアドバタイズするものの使用する MTU 値が異なる 2 つのプライベート仮想インターフェイスがある場合、または同じルートをアドバタイズする Site-to-Site VPN がある場合には、1500 MTU が使用されます。

> **Important**
>
> ジャンボフレームは、 経由の伝播されたルート AWS Direct Connect とトランジットゲートウェイ経由の静的ルートにのみ適用されます。トランジットゲートウェイ上のジャンボフレームによってサポートされるのは、8500 バイトのみです。
> EC2 インスタンスでジャンボフレームがサポートされていない場合、ジャンボフレームは Direct Connect からドロップされます。C1、CC1、T1 と M1 を除くすべての EC2 インスタンスタイプは、ジャンボフレームをサポートしています。詳細については、「Amazon EC2 ユーザーガイド」の「EC2 インスタンスのネットワーク最大送信単位 (MTU)」を参照してください。 Amazon EC2
> ホスト接続の場合、ジャンボフレームは Direct Connect のホスト親接続で最初に有効になっている場合にのみ有効にできます。ジャンボフレームがその親接続で有効になっていない場合、どの接続でも有効にすることはできません。

プライベート仮想インターフェイスの MTU を設定するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。

3. 仮想インターフェイスを選択し、[編集] を選択します。
4. [ジャンボ MTU (MTU サイズ 9001)] または [ジャンボ MTU (MTU サイズ 8500)] で [有効] を選択します。
5. [確認] で [I understand the selected connection(s) will go down for a brief period (選択された接続は短時間停止することを理解しています)] を選択します。更新が完了するまでの仮想インターフェイスのステータスは、`pending` です。

コマンドラインまたは API を使用してプライベート仮想インターフェイスの MTU を設定するには

- update-virtual-interface-attributes (AWS CLI)
- UpdateVirtualInterfaceAttributes (AWS Direct Connect API)

仮想インターフェイスタグを追加または削除する

タグは仮想インターフェイスを識別する方法を提供します。仮想インターフェイスのアカウント所有者である場合は、タグを追加または削除できます。

仮想インターフェイスタグを追加または削除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. 仮想インターフェイスを選択し、[編集] を選択します。
4. タグを追加または削除します。

   [タグの追加] [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。

   [タグの削除] タグの横にある [タグの削除] を選択します。
5. [Edit virtual interface (仮想インターフェイスの編集)] を選択します。

コマンドラインを使用してタグを追加または削除するには

- tag-resource (AWS CLI)

- untag-resource (AWS CLI)

仮想インターフェースを削除する

1 つ以上の仮想インターフェイスを削除します。接続を削除するには、接続の仮想インターフェイスを削除する必要があります。仮想インターフェイスを削除すると、仮想インターフェイスに関連する AWS Direct Connect データ転送料金が停止します。

仮想インターフェイスを削除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. 左側のペインで、[仮想インターフェイス] を選択します。
3. 仮想インターフェイスを選択し、[Delete (削除)] を選択します。
4. [Delete (削除)] の確認ダイアログボックスで、[Delete (削除)] を選択します。

仮想インターフェイスを削除するには、コマンドラインまたは API を使用します

- delete-virtual-interface (AWS CLI)
- DeleteVirtualインターフェイス (AWS Direct Connect API)

ホスト仮想インターフェイスを作成する

パブリック、トランジット、またはプライベートのホスト仮想インターフェイスを作成できます。作業を開始する前に、「仮想インターフェイスの前提条件」の情報を参照済みであることを確認してください。

ホストされたプライベート仮想インターフェイスを作成する

ホストされたプライベート仮想インターフェイスを作成するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。

4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [プライベート] を選択します。
5. [プライベート仮想インターフェイス設定] で以下を実行します。

   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

   c. [Virtual interface owner] (仮想インターフェイスの所有者) で [Another AWS account] (別の アカウント) を選択してから、[Virtual interface owner] (仮想インターフェイスの所有者) にアカウントの ID を入力してこの仮想インターフェイスを所有します。

   d. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

   e. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

      有効な値は 1 ~ 2147483647 です。
6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

      - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
      - [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

      > **Important**
      >
      > IP アドレス AWS の自動割り当てを許可すると、169.254.0.0/16. から /29 CIDR AWS が割り当てられるため、カスタマールーターピア IP アドレスをトラフィックの送信元と送信先として使用する場合は、このオプションは推奨されません。代わりに、RFC 1918 または他のアドレス (RFC 1918 以外) を使用して、アドレスを自分で指定する必要があります。RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。

      [IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

b. 最大送信単位 (MTU) を 1500 (デフォルト) から 9001 (ジャンボフレーム) に変更するには、[ジャンボ MTU (MTU サイズ 9001)] を選択します。

c. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. ホスト仮想インターフェイスが他の AWS アカウントの所有者によって承諾されたら、ルーター設定ファイルをダウンロードできます。

コマンドラインまたは API を使用してホストされたプライベート仮想インターフェイスを作成するには

- allocate-private-virtual-interface (AWS CLI)
- AllocatePrivateVirtualInterface (AWS Direct Connect API)

ホストされたパブリック仮想インターフェイスを作成する

ホストされたパブリック仮想インターフェイスを作成するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [パブリック] を選択します。
5. [パブリック仮想インターフェイス設定] で以下を実行します。

a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

c. 仮想インターフェイス所有者 で別の AWS アカウント を選択し、仮想インターフェイス所有者 で、この仮想インターフェイスを所有するアカウントの ID を入力します。

d. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

e. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

有効な値は 1 ~ 2147483647 です。

6. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

[IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

- これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
- [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

> **Important**
>
> IP アドレス AWS の自動割り当てを許可すると、169.254.0.0/16. から /29 CIDR AWS が割り当てられるため、カスタマールーターピア IP アドレスをトラフィックの送信元と送信先として使用する場合は、このオプションは推奨されません。代わりに、RFC 1918 または他のアドレスを使用して、アドレスを自分で指定する必要があります。RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。

[IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

7. Amazon にプレフィックスを発行するには、[アドバタイズするプレフィックス] に、この仮想インターフェイスを介してルーティングされるトラフィックのルーティング先となる IPv4 CIDR アドレスをカンマで区切って入力します。
8. 独自のキーを使用して BGP セッションを認証するには、[追加設定] の [BGP 認証キー] にキーを入力します。

値が入力されない場合は、当社側で自動的に BGP キーが生成されます。

9. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

10. [仮想インターフェイスの作成] を選択します。
11. ホスト仮想インターフェイスが他の AWS アカウントの所有者によって承諾されたら、ルーター設定ファイルをダウンロードできます。

コマンドラインまたは API を使用してホストされたパブリック仮想インターフェイスを作成するには

- allocate-public-virtual-interface (AWS CLI)
- AllocatePublicVirtualInterface (AWS Direct Connect API)

ホストされたトランジット仮想インターフェイスを作成する

ホストされたトランジット仮想インターフェイスを作成するには

> **Important**
>
> Transit Gateway を 1 つ以上の Direct Connect ゲートウェイに関連付ける場合、Transit Gateway およびその Direct Connect ゲートウェイで使用される自律システム番号 (ASN) は異なる値である必要があります。たとえば、Transit Gateway と Direct Connect ゲートウェイの両方にデフォルトの ASN 64512 を使用すると、関連付けのリクエストは失敗します。

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [Transit (トランジット)] を選択します。
5. [Transit virtual interface settings (トランジット仮想インターフェイス設定)] で以下を実行します。

   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

c. 仮想インターフェイス所有者 で別の AWS アカウント を選択し、仮想インターフェイス所有者 で、この仮想インターフェイスを所有するアカウントの ID を入力します。

d. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

e. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

有効な値は 1 ~ 2147483647 です。

6. [追加設定] で、以下を実行します。

a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

[IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

- これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
- [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

> **Important**
>
> IP アドレス AWS の自動割り当てを許可すると、169.254.0.0/16. から /29 CIDR AWS が割り当てられるため、カスタマールーターピア IP アドレスをトラフィックの送信元と送信先として使用する場合は、このオプションは推奨されません。代わりに、RFC 1918 または他のアドレスを使用して、アドレスを自分で指定する必要があります。RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。

[IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

b. 最大送信単位 (MTU) を 1500 (デフォルト) から 8500 (ジャンボフレーム) に変更するには、[ジャンボ MTU (MTU サイズ 8500)] を選択します。

c. (オプション) タグを追加します。次の作業を行います。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。
8. ホスト仮想インターフェイスが他の AWS アカウントの所有者によって承諾されたら、ルーター設定ファイルをダウンロードできます。

コマンドラインまたは API を使用してホストされたトランジット仮想インターフェイスを作成するには

- allocate-transit-virtual-interface (AWS CLI)
- AllocateTransitVirtualInterface (AWS Direct Connect API)

ホスト仮想インターフェイスを承諾する

ホスト仮想インターフェイスを使用する前に、仮想インターフェイスを承諾する必要があります。プライベート仮想インターフェイスの場合は、既存の仮想プライベートゲートウェイまたは Direct Connect Gateway も必要です。トランジット仮想インターフェイスの場合は、既存の仮想プライベートゲートウェイまたは Direct Connect ゲートウェイが必要です。

ホスト仮想インターフェイスを承諾するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. 仮想インターフェイスを選択したら、[View details (詳細の表示)] を選択します。
4. [承諾] を選択します。
5. これは、プライベート仮想インターフェイスおよびトランジット仮想インターフェイスに適用されます。

   (トランジット仮想インターフェイス) [仮想インターフェイスの承諾] ダイアログボックスで、Direct Connect ゲートウェイを選択して、[仮想インターフェイスの承諾] を選択します。

   (プライベート仮想インターフェイス) [仮想インターフェイスの承諾] ダイアログボックスで、仮想プライベートゲートウェイまたは Direct Connect ゲートウェイを選択して、[仮想インターフェイスの承諾] を選択します。

6. ホスト仮想インターフェイスを承諾すると、 AWS Direct Connect 接続の所有者はルーター設定ファイルをダウンロードすることができます。[ルーター設定をダウンロードする] オプションは、ホストされた仮想インターフェイスを承諾するアカウントでは利用できません。

コマンドラインまたは API を使用して、ホストされたプライベート仮想インターフェイスを承諾するには

- confirm-private-virtual-interface (AWS CLI)
- ConfirmPrivateVirtualInterface (AWS Direct Connect API)

コマンドラインまたは API を使用して、ホストされたパブリック仮想インターフェイスを承諾するには

- confirm-public-virtual-interface (AWS CLI)
- ConfirmPublicVirtualInterface (AWS Direct Connect API)

コマンドラインまたは API を使用して、ホストされたトランジット仮想インターフェイスを承諾するには

- confirm-transit-virtual-interface (AWS CLI)
- ConfirmTransitVirtualInterface (AWS Direct Connect API)

仮想インターフェイスを移行する

この手順は、次のいずれかの仮想インターフェイス移行オペレーションを実行する場合に使用します。

- 接続に関連付けられた既存の仮想インターフェイスを別の LAG に移行する。
- 既存の LAG に関連付けられた既存の仮想インターフェイスを新しい LAG に移行する。
- 接続に関連付けられた既存の仮想インターフェイスを別の接続に移行する。

> **Note**
>
> - 仮想インターフェイスを同じリージョン内の新しい接続に移行することはできますが、あるリージョンから別のリージョンに移行することはできません。既存の仮想インターフェ

イスを新しい接続に移行または関連付けると、これらの仮想インターフェイスに関連付けられている設定パラメータは同じになります。これを回避するには、接続で事前に設定してから、BGP 設定を更新します。

- 1 つのホスト接続から別のホスト接続に VIF を移行することはできません。VLAN ID は一意であるため、このようにして VIF を移行すると、VLAN が一致しないことを意味します。接続または VIF を削除してから、接続と VIF の両方で同じ VLAN を使用して再作成する必要があります。

Important

仮想インターフェイスが短い期間、ダウンします。メンテナンス期間中にこの手順を実行することをお勧めします。

仮想インターフェイスを移行するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. 仮想インターフェイスを選択し、[編集] を選択します。
4. [接続] で、LAG または接続を選択します。
5. [Edit virtual interface (仮想インターフェイスの編集)] を選択します。

仮想インターフェイスを移行するには、コマンドラインまたは API を使用します

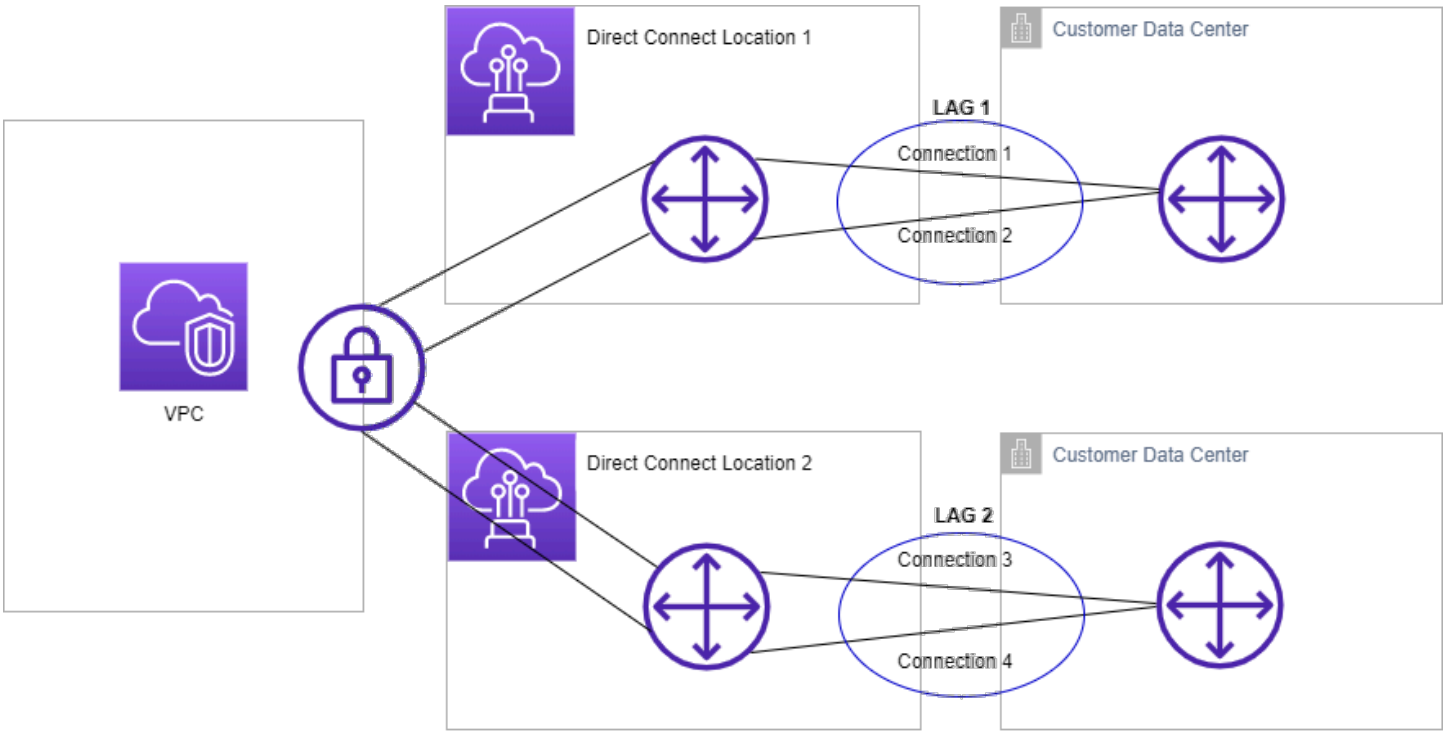
- associate-virtual-interface (AWS CLI)
- AssociateVirtualインターフェイス (AWS Direct Connect API)

Link Aggregation Group (LAG)

複数の接続を使用して、利用できる帯域幅を増やすことができます。Link Aggregation Group (LAG) は、Link Aggregation Control Protocol (LACP) を使用して、1 つの AWS Direct Connect エンドポイントに複数の接続を集約し、それらを 1 つのマネージド型接続として扱うことを可能にする論理インターフェイスです。LAG 設定はグループ内のすべての接続に適用されるため、LAG は設定を合理化します。

> **Note**
>
> AWS はマルチシャーシ LAG (MLAG) をサポートしません。

次の図では、各ロケーションに 2 つずつ、合計 4 つの接続があります。同じAWSデバイスおよび同じ場所を終了する接続の LAG を作成し、設定と管理に 4 つの接続の代わりに 2 つの LAGsを使用できます。



既存の接続から LAG を作成するか、新しい接続をプロビジョニングできます。LAG を作成したら、既存の接続 (スタンドアロンか別の LAG の一部であるかどうかを問わず) を LAG に関連付けることができます。

以下のルールが適用されます。

- すべての接続は専用接続でなければならず、ポートスピードが 1 Gbps、10 Gbps または 100 Gbps であることが必要です。
- LAG のすべての接続では、同じ帯域幅を使用する必要があります。
- LAG では、100G のポートスピードで最大 2 つの 接続、または 100G 未満で最大 4 つの接続を使用できます。LAG の各接続はリージョンの全体的な接続制限の対象になります。
- LAG のすべての接続は、同じ AWS Direct Connect エンドポイントで終了する必要があります。
- LAGは、パブリック、プライベート、トランジットのすべての仮想インターフェースタイプでサポートされています。

LAG の作成時に、新しい物理接続ごとに Letter of Authorization and Connecting Facility Assignment (LOA-CFA) を AWS Direct Connect コンソールからダウンロードできます。詳細については、「LOA-CFA をダウンロードする」を参照してください。

すべての LAG には、LAG 自体が機能するために使用できる必要がある、LAG での接続の最小数を決定する属性があります。新しい LAG では、この属性はデフォルトで 0 に設定されます。LAG を更新して別の値を指定できます。その場合、使用できる接続の数がこのしきい値を下回ると、LAG 全体が機能しなくなります。この属性を使用して、その他の接続の過度の使用を防ぐことができます。

LAG のすべての接続はアクティブ/アクティブモードで実行されます。

> **Note**
>
> LAG を作成するか、複数の接続を LAG と関連付ける場合、特定の AWS Direct Connect エンドポイントで十分な数のポートが使用可能であることは保証されません。

MacSec に関する考慮事項

LAG で MACsec を設定する場合は、次の点を考慮してください。

- 既存の接続から LAG を作成すると、すべての MACsec キーと接続との関連付けが解除されます。その後に、LAG に接続が追加され、LAG の MACSec キーがその接続に関連付けられます。
- 既存の接続を LAG に関連付けると、現在LAG に関連付けられている MacSec キーも、その接続に関連付けられます。したがって、接続から MACsec キーの関連付けを解除し、接続を LAG に追加した上で、LAG MACSec キーを接続に関連付けしています。

LAG を作成する

新しい接続をプロビジョニングするか、既存の接続を集約して LAG を作成できます。

リージョンに対する全体的な接続の制限を超える場合、新しい接続で LAG を作成することはできません。

既存の接続から LAG を作成するには、それらの接続が同じ AWS デバイス上にあり (同じ AWS Direct Connect エンドポイントで終端する)、同じ帯域幅を使用する必要があります。接続を削除することにより、元の LAG で使用できる接続の最小数の設定を下回る場合、既存の LAG から接続を移行することはできません。

> **Important**
>
> 既存の接続では、LAG の作成中に AWS への接続が中断されます。

Create a LAG with new connections using the console

新しい接続で LAG を作成するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. [Create LAG] を選択します。
4. [Lag creation type (LAG 作成タイプ)] で [新しい接続のリクエスト] を選択し、次の情報を入力します。

   - [LAG name (LAG 名)]: LAG の名前。
   - [Location (場所)]: LAG の場所。
   - [ポートスピード]: 接続のポートスピード。
   - [Number of new connections (新しい接続の数)]: 作成する新しい接続の数。ポート速度が 1G または 10G の場合は最大 4 つの接続が可能です。ポート速度が 100G の場合は最大 2 つの接続が可能です。
   - (オプション) MAC セキュリティ (MACsec) を使用する接続を設定します。[その他の設定] で、[MACSec 対応ポートをリクエストする] をクリックします。

     MACSec は専用接続でのみ使用が可能です。

- (オプション) タグを追加または削除します。

  [タグの追加] [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。

  [タグの削除] タグの横にある [タグの削除] を選択します。

5. [Create LAG] を選択します。

Create a LAG with existing connections using the console

既存の接続から LAG を作成するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. [Create LAG] を選択します。
4. [Lag creation type (LAG 作成タイプ)] で [既存の接続を使用] を選択し、次の情報を入力します。

   - [LAG name (LAG 名)]: LAG の名前。
   - [既存の接続]: LAG に使用する Direct Connect 接続。
   - (オプション) [新しい接続の数]: 作成する新しい接続の数。ポート速度が 1G または 10G の場合は最大 4 つの接続が可能です。ポート速度が 100G の場合は最大 2 つの接続が可能です。
   - [最小リンク数]: LAG 自体が機能するために使用できる必要がある接続の最小数。値を指定しない場合は、デフォルト値 0 が割り当てられます。
5. (オプション) タグを追加または削除します。

   [タグの追加] [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。

   [タグの削除] タグの横にある [タグの削除] を選択します。
6. [Create LAG] を選択します。

Command line

コマンドラインまたは API を使用して LAG を作成するには

- create-lag (AWS CLI)
- CreateLag (AWS Direct Connect API)

コマンドラインまたは API を使用して LAG を記述するには

- describe-lags (AWS CLI)
- DescribeLags (AWS Direct Connect API)

コマンドラインまたは API を使用して LOA-CFA をダウンロードするには

- describe-loa (AWS CLI)
- DescribeLoa (AWS Direct Connect API)

LAG を作成したら、この LAG に接続を関連付けたり、その関連付けを解除したりできます。詳細については、「接続を LAG に関連付ける」および「LAG から接続の関連付けを解除する」を参照してください。

LAG の詳細を表示する

LAG を作成したら、その詳細を表示できるようになります。

Console

LAG に関する情報を表示するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択したら、[View details (詳細の表示)] を選択します。
4. ID および接続が終端する AWS Direct Connect エンドポイントなどの LAG に関する情報を表示できます。

Command line

コマンドラインまたは API を使用して LAG に関する情報を表示するには

- describe-lags (AWS CLI)
- DescribeLags (AWS Direct Connect API)

LAG を更新する

次の Link Aggregation Group (LAG) 属性が更新できます。

- LAG の名前。
- LAG 自体が機能するために使用する必要がある、接続の最小数を指定する値。
- LAG の MACsec 暗号化モード。

  MACSec は専用接続でのみ使用が可能です。

  AWS は、LAG の構成部分である各接続にこの値を割り当てます。

  有効な値は以下のとおりです。

  - `should_encrypt`
  - `must_encrypt`

    暗号化モードにこの値を設定した場合は、暗号化がダウンした際に接続もダウンします。
  - `no_encrypt`
- タグ。

> **Note**
>
> 使用できる接続の最小数のしきい値を調整する場合は、新しい値によって LAG がこのしきい値を下回り、機能しなくなることがないようにしてください。

Console

LAG を更新するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択し、その後で [編集] をクリックします。
4. LAG の変更

   [名前の変更] [LAG 名] に新しい LAG 名を入力します。

   [接続最小数の調整]: [最小リンク数] に、使用可能な状態にする接続の最小数を入力します。

   [タグの追加] [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。

   [タグの削除] タグの横にある [タグの削除] を選択します。
5. [Edit LAG (LAG の編集)] を選択します。

Command line

コマンドラインまたは API を使用して LAG を更新するには

- update-lag (AWS CLI)
- UpdateLag (AWS Direct Connect API)

コマンドラインを使用してタグを追加または削除するには

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

接続を LAG に関連付ける

既存の接続を LAG に関連付けることができます。接続は、スタンドアロンであっても、別の LAG の一部であってもかまいません。また、同じ AWS デバイス上にあり、LAG と同じ帯域幅を使用し

ている必要があります。接続が既に別の LAG と関連付けられていて、接続を削除すると、元の LAG で使用できる接続の最小数のしきい値を下回る場合、もう一度関連付けることはできません。

LAG に接続を関連付けると、その仮想インターフェイスは自動的に LAG にもう一度関連付けられます。

> **Important**
>
> この関連付け処理中は、この接続経由での AWS への接続が中断されます。

Console

接続を LAG と関連付けるには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択した上で、[詳細の表示] をクリックします。
4. [接続] で [接続の関連付け] を選択します。
5. [接続] では、LAG を使用する Direct Connect 接続を選択します。
6. [接続の関連付け] を選択します。

Command line

コマンドラインまたは API を使用して接続を関連付けるには

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag (AWS Direct Connect API)

LAG から接続の関連付けを解除する

接続をスタンドアロンに変換するには、LAG から関連付けを解除します。これにより LAG で使用できる接続の最小数のしきい値を下回る場合、接続の関連付けを解除することはできません。

LAG から接続の関連付けを解除しても、仮想インターフェイスは自動的に関連付けが解除されません。

> **Important**
>
> 関連付けの解除中は、AWS への接続が切断されます。

Console

LAG から接続の関連付けを解除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. 左側のペインで、[LAG] を選択します。
3. LAG を選択した上で、[詳細の表示] をクリックします。
4. [接続] で利用できる接続のリストかた接続を選択したら、[関連付け解除] を選択します。
5. 確認ダイアログボックスで、[関連付け解除] を選択します。

Command line

コマンドラインまたは API を使用して接続の関連付けを解除するには

- disassociate-connection-from-lag (AWS CLI)
- DisassociateConnectionFromLag (AWS Direct Connect API)

MACSec CKN/CAK と LAG を関連付ける

MACsec をサポートする LAG の作成が完了すると、CKN/CAK を接続に関連付けることが可能になります。

> **Note**
>
> LAG に関連付けた後の MACsec シークレットキーは、変更することはできません。キーを変更する必要がある場合は、そのキーと接続との関連付けを解除した上で、新しいキーを接続に関連付けます。関連付けの解除については、「the section called “MACsec シークレットキーと LAG の間の関連付けを解除する”」を参照してください。

Console

MACsec キーと LAG を関連付けるには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択したら、[View details (詳細の表示)] を選択します。
4. [キーの関連付け] をクリックします。
5. MACsec キーを入力します。

   [CAK/CKN ペアの使用]: [キーペア] を選択し次の操作を行います。

   - [接続関連付けキー (CAK)] に、使用する CAK を入力します。
   - [接続関連付けキー名 (CKN)] に、使用する CKN を入力します。

   [シークレットの使用] : [既存のシークレットマネージャのシークレット] を選択し、[シークレット] で MACSec シークレットキーを選択します。
6. [キーの関連付け] をクリックします。

Command line

MACsec キーと LAG を関連付けるには

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey (AWS Direct Connect API)

MACsec シークレットキーと LAG の間の関連付けを解除する

LAG キーと MACsec キーの関連付けは、解除することができます。

Console

LAG キーと MACsec キー間の関連付けを解除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。

2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択したら、[View details (詳細の表示)] を選択します。
4. 解除する MacSec シークレットを選択し、[キーの関連付けを解除する] をクリックします。
5. 確認ダイアログボックスで、disassociate と入力し、[関連付けを解除] をクリックします。

Command line

LAG キーと MACsec キー間の関連付けを解除するには

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey (AWS Direct Connect API)

LAG を削除する

LAG が不要になると、これを削除できます。関連付けられた仮想インターフェイスがある LAG は削除できません。まず仮想インターフェイスを削除するか、または別の LAG あるいは接続にこれを関連付けます。LAG を削除しても、LAG の接続は削除されません。手動で接続を削除する必要があります。詳細については、「複数の接続を削除」を参照してください。

Console

LAG を削除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択し、[削除] をクリックします。
4. 確認ダイアログボックスで、[Delete (削除)] を選択します。

Command line

コマンドラインまたは API を使用して LAG を削除するには

- delete-lag (AWS CLI)
- DeleteLag (AWS Direct Connect API)

Direct Connect ゲートウェイの操作

Amazon VPC AWS Direct Connect コンソールまたはを使用してゲートウェイを操作できます。
AWS CLI

コンテンツ

Direct Connect ゲートウェイ

AWS Direct Connect ゲートウェイを使用して VPC を接続します。 AWS Direct Connect ゲートウェイは、次のいずれかのゲートウェイに関連付けます。

- 同一リージョン内に複数の VPC がある場合は Transit Gateway
- 仮想プライベートゲートウェイ

仮想プライベートゲートウェイを使用して、ローカルゾーンを拡張することもできます。この設定により、ローカルゾーンに関連付けられた VPC が Direct Connect ゲートウェイに接続できるようになります。Direct Connect ゲートウェイは、リージョン内の Direct Connect ロケーションに接続します。オンプレミスのデータセンターには、Direct Connect ロケーションへの Direct Connect 接続があります。詳細については、Amazon VPC ユーザーガイド の Accessing Local Zones using a Direct Connect gateway を参照してください。

Direct Connect ゲートウェイはグローバルに利用可能なリソースです。Direct Connect ゲートウェイを使用して、世界中のリージョン内の VPC に接続できます。 AWS GovCloud (US) AWS これには中国リージョンが含まれますが、含まれません。

現在、親アベイラビリティーゾーンをバイパスしている VPC で Direct Connect を使用しているお客様は、Direct Connect 接続または仮想インターフェイスを移行できません。

以下は、Direct Connect ゲートウェイを使用できるシナリオを説明しています。

Direct Connect ゲートウェイでは、同じ Direct Connect ゲートウェイ上にあるゲートウェイの関連付けが相互にトラフィックを送信することはできません (たとえば、仮想プライベートゲートウェイ

から別の仮想プライベートゲートウェイへ)。2021 年 11 月に実装されたこのルールの例外は、スーパーネットが、同じ Direct Connect ゲートウェイおよび同じ仮想インターフェイス上に関連付けられている接続された仮想プライベートゲートウェイ (VGW) を持つ 2 つ以上の VPC にわたってアドバタイズされる場合です。この場合、VPC は Direct Connect エンドポイントを介して互いに通信できます。例えば、Direct Connect ゲートウェイ (10.0.0.0/24 および 10.0.1.0/24 など) に接続された VPC と重複するスーパーネット (10.0.0.0/8 または 0.0.0.0/0 など) をアドバタイズし、同じ仮想インターフェイス上で、オンプレミスネットワークから VPC は相互に通信できます。

Direct Connect ゲートウェイ内の VPC 間通信をブロックする場合は、次の手順を実行します。

1. VPC 内のインスタンスおよびその他のリソースにセキュリティグループを設定し、VPC 間のトラフィックをブロックします。また、これを VPC のデフォルトのセキュリティグループの一部として使用します。
2. VPC と重複するオンプレミスネットワークからスーパーネットをアドバタイズすることは避けてください。代わりに、VPC と重複しないオンプレミスネットワークからのより具体的なルートをアドバタイズできます。
3. 複数の VPC に同じ Direct Connect Gateway を使用する代わりに、オンプレミスネットワークに接続する VPC ごとに 1 つの Direct Connect ゲートウェイをプロビジョニングします。例えば、開発用および本番用 VPC に単一の Direct Connect ゲートウェイを使用する代わりに、これらの VPC ごとに個別のダイレクトConnect ゲートウェイを使用します。

Direct Connect ゲートウェイは、1 つのゲートウェイの関連付けからゲートウェイの関連付け自体へのトラフィックの送信を禁止しません (ゲートウェイ関連付けからのプレフィックスを含むオンプレミスのスーパーネットルートがある場合など)。同じ Direct Connect ゲートウェイに関連付けられたトランジットゲートウェイに複数の VPC が接続されている設定がある場合、VPC は通信できます。VPC が通信しないようにするには、ブラックホールオプションが設定されている VPC アタッチメントにルートテーブルを関連付けます。

以下は、Direct Connect ゲートウェイを使用できるシナリオを説明しています。

シナリオ

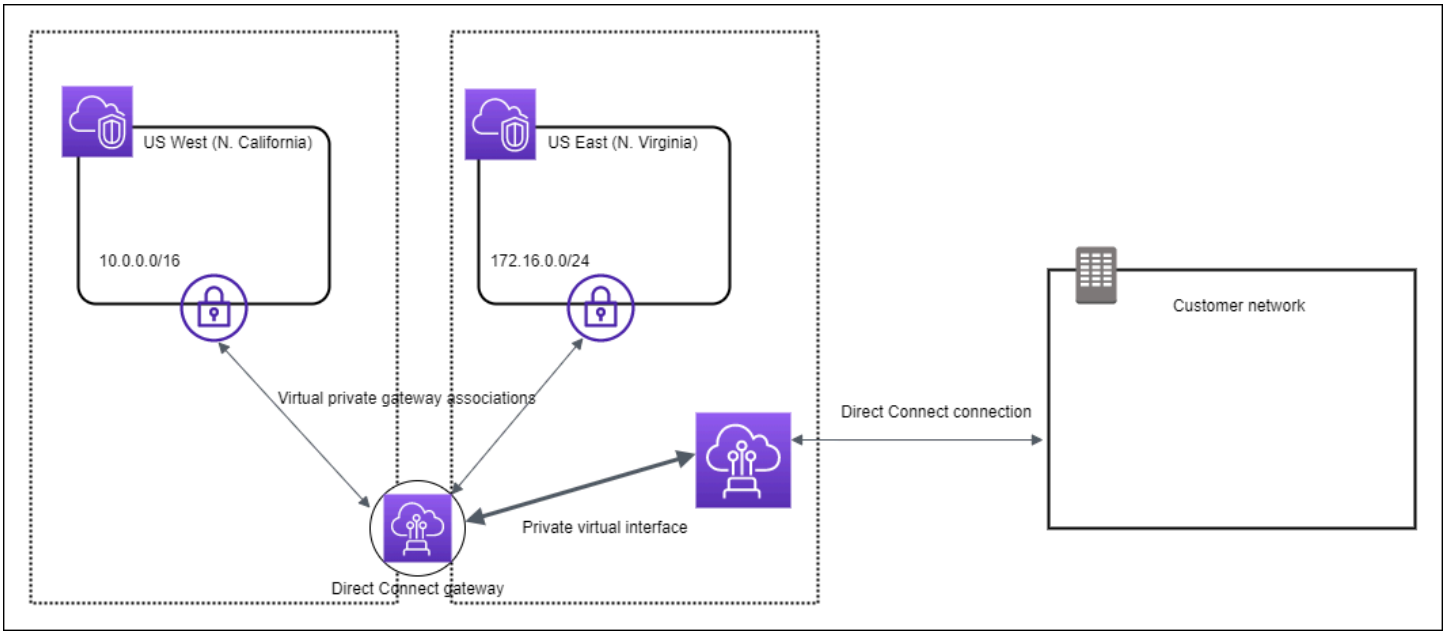
- 仮想プライベートゲートウェイの関連付け
- アカウント間の仮想プライベートゲートウェイの関連付け
- トランジットゲートウェイの関連付け
- アカウント間のトランジットゲートウェイの関連付け
- Direct Connect ゲートウェイの作成

- Direct Connect Gateway の削除
- 仮想プライベートゲートウェイから Direct Connect ゲートウェイへの移行

仮想プライベートゲートウェイの関連付け

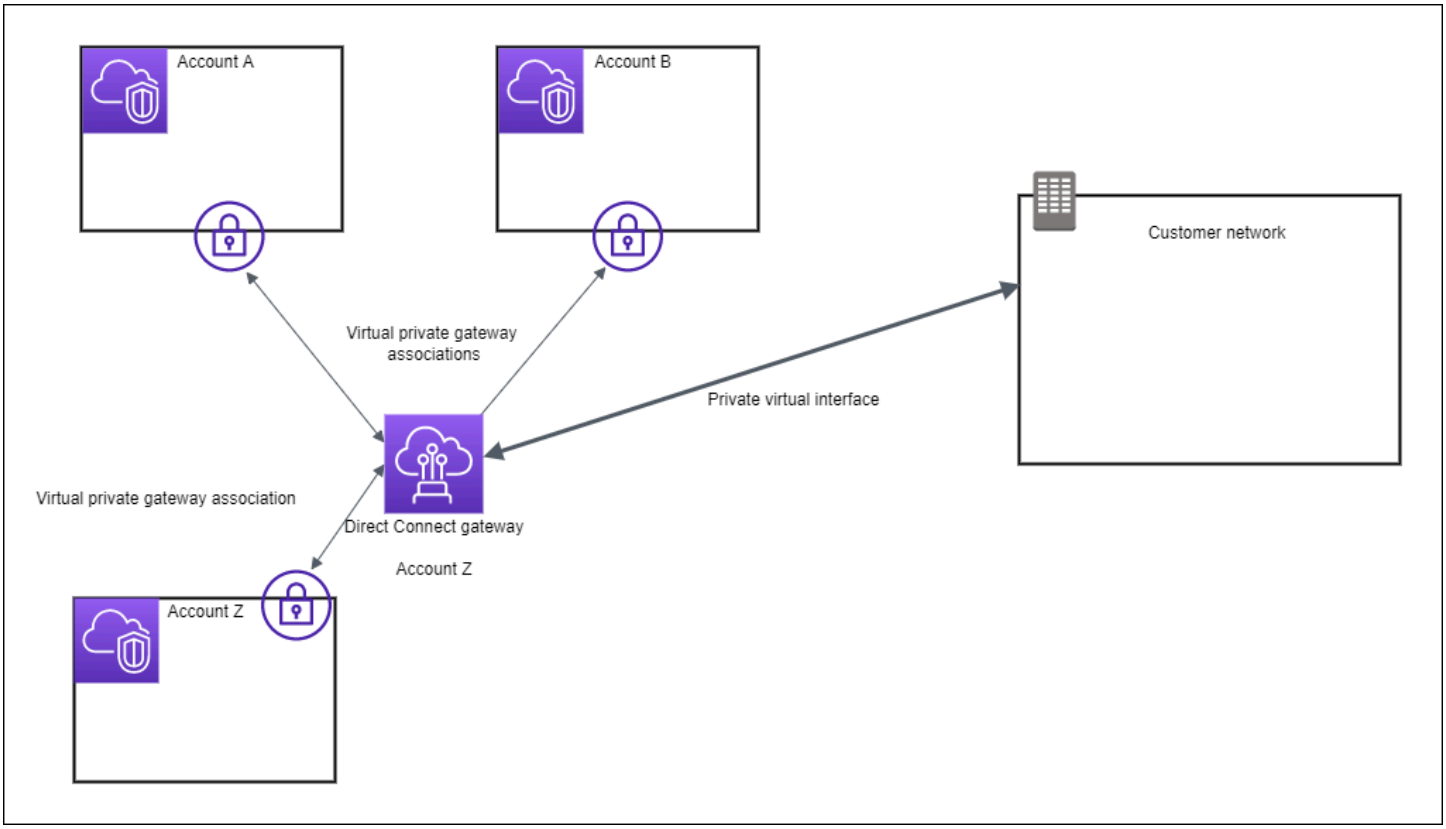
次の図では、Direct Connect ゲートウェイが米国東部 (バージニア北部) リージョンの AWS Direct Connect 接続を使用して、米国東部 (バージニア北部) と米国西部 (北カリフォルニア) の両リージョンにあるアカウント内の VPC へのアクセスを可能にします。

各 VPC には、仮想プライベートゲートウェイの関連付けを使用して Direct Connect ゲートウェイに接続する仮想プライベートゲートウェイがあります。Direct Connect ゲートウェイは、 AWS Direct Connect ロケーションへの接続にプライベート仮想インターフェイスを使用します。ロケーションからお客様のデータセンターへの AWS Direct Connect 接続があります。



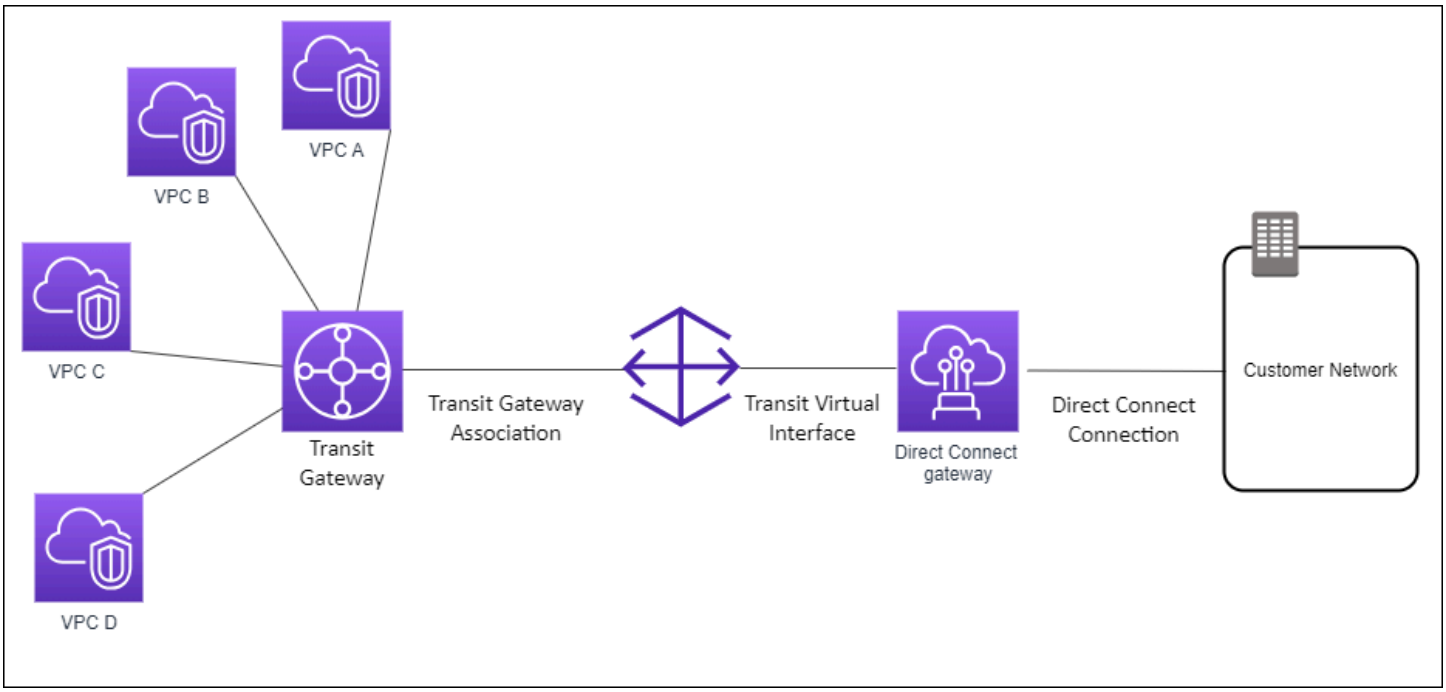
アカウント間の仮想プライベートゲートウェイの関連付け

Direct Connect ゲートウェイを所有している Direct Connect 所有者 (アカウント Z) のシナリオを考えてみます。アカウント A とアカウント B は Direct Connect ゲートウェイの使用を希望しています。アカウント A とアカウント B はそれぞれ、関連付け提案をアカウント Z に送信します。アカウント Z はこの関連付け提案を承諾し、必要に応じて、アカウント A の仮想プライベートゲートウェイまたはアカウント B の仮想プライベートゲートウェイから許可されるプレフィックスを更新します。アカウント Z が提案を承諾すると、アカウント A とアカウント B はそれぞれの仮想プライベートゲートウェイから Direct Connect ゲートウェイにトラフィックをルートできるようになります。また、アカウント Z はゲートウェイを所有しているため、顧客へのルーティングを所有します。



トランジットゲートウェイの関連付け

次の図は、Direct Connect ゲートウェイによって、すべての VPC が使用できる Direct Connect 接続に 1 つ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。

- VPC アタッチメントを持つ Transit Gateway。
- 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。
- Direct Connect ゲートウェイにアタッチされたトランジット仮想インターフェイス。

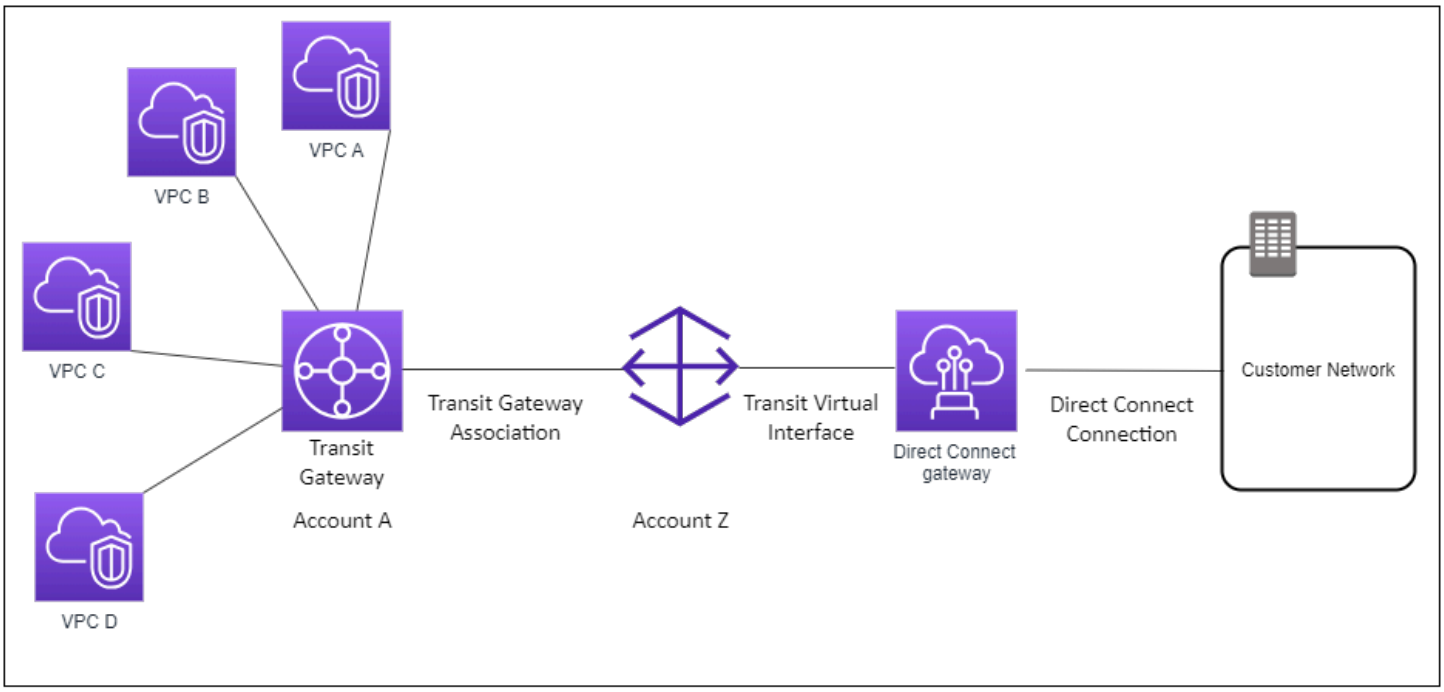
この設定には次のような利点があります。以下を実行できます。

- 同じリージョンにある複数の VPN または VPC に対して 1 つの接続を管理する。
- プレフィックスをオンプレミスへ、 AWS またはオンプレミス間でアドバタイズします。 AWS

Transit Gateways の詳細については、Amazon VPC Transit Gateways ガイドの Working with Transit Gateways を参照してください。

アカウント間のトランジットゲートウェイの関連付け

Direct Connect ゲートウェイを所有している Direct Connect 所有者 (アカウント Z) のシナリオを考えてみます。アカウント A が Transit Gateway を所有していて、Direct Connect ゲートウェイを使用したいと考えています。アカウント Z は関連付け提案を受け入れ、オプションで、アカウント A の Transit Gateway から許可されるプレフィックスを更新できます。アカウント Z が提案を受け入れた後で、Transit Gateway にアタッチされた VPC は、Transit Gateway から Direct Connect ゲートウェイにトラフィックをルーティングできます。また、アカウント Z はゲートウェイを所有しているため、顧客へのルーティングを所有します。



コンテンツ

Direct Connect ゲートウェイの作成

Direct Connect ゲートウェイは、すべてのサポートされているリージョンで作成できます。

Direct Connect ゲートウェイを作成するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Direct Connect Gateway] を選択します。
3. [Direct Connect Gateway の作成] を作成します。
4. 次の情報を指定し、[Create Direct Connect gateway (Direct Connect ゲートウェイの作成)] を選択します。
   - 名前: Direct Connect ゲートウェイを識別するのに役立つ名前を入力します。

- Amazon 側の ASN: Amazon 側の BGP セッションのための ASN を指定します。ASN は、64,512 ~ 65,534 または 4,200,000,000 ~ 4,294,967,294 の範囲内で指定する必要があります。
- [仮想プライベートゲートウェイ]: 仮想プライベートゲートウェイを関連付けるには、仮想プライベートインターフェイスを選択します。

コマンドラインまたは API を使用して Direct Connect ゲートウェイを作成するには

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway(AWS Direct Connect API)

Direct Connect Gateway の削除

Direct Connect ゲートウェイ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。最初に、すべての関連付け済み仮想プライベートゲートウェイの関連付けを解除し、アタッチ済みプライベート仮想インターフェイスを削除する必要があります。

Direct Connect ゲートウェイを削除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Direct Connect Gateway] を選択します。
3. ゲートウェイを選択し、[Delete (削除)] を選択します。

コマンドラインまたは API を使用して Direct Connect ゲートウェイを削除するには

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway(AWS Direct Connect API)

仮想プライベートゲートウェイから Direct Connect ゲートウェイへの移行

仮想インターフェイスにアタッチされた仮想プライベートゲートウェイがあり、Direct Connect ゲートウェイに移行する場合は、以下の手順を実行します。

Direct Connect ゲートウェイに移行するには

1. Direct Connect ゲートウェイを作成します。詳細については、「the section called “Direct Connect ゲートウェイの作成”」を参照してください。
2. Direct Connect ゲートウェイの仮想インターフェイスを作成します。詳細については、「the section called “仮想インターフェイスを作成する”」を参照してください。
3. 仮想プライベートゲートウェイを Direct Connect ゲートウェイに関連付けます。詳細については、「the section called “仮想プライベートゲートウェイの関連付けと関連付けの解除”」を参照してください。
4. 仮想プライベートゲートウェイに関連付けられた仮想インターフェイスを削除します。詳細については、「the section called “仮想インターフェースを削除する”」を参照してください。

仮想プライベートゲートウェイの関連付け

AWS Direct Connect ゲートウェイを使用すると、プライベート仮想インターフェイスを介して、AWS Direct Connect 接続を、同じリージョンまたは異なるリージョンに配置されたアカウントの 1 つ以上の VPC に接続できます。Direct Connect Gateway を VPC の仮想プライベートゲートウェイに関連付けます。次に、Direct Connect AWS Direct Connect ゲートウェイに接続するためのプライベート仮想インターフェイスを作成します。複数のプライベート仮想インターフェイスを、Direct Connect ゲートウェイにアタッチできます。

仮想プライベートゲートウェイの関連付けには、次の規則が適用されます。

- 仮想ゲートウェイを Direct Connect ゲートウェイに関連付けるまで、ルート伝達を有効にしないでください。ゲートウェイを関連付ける前にルートの伝達を有効にすると、ルートが正しく伝播されない可能性があります。
- Direct Connect ゲートウェイの作成および使用には制限があります。詳細については、「クォータ」を参照してください。
- Direct Connect ゲートウェイが既にトランジットゲートウェイに関連付けられている場合、Direct Connect ゲートウェイを仮想プライベートゲートウェイにアタッチすることはできません。
- Direct Connect ゲートウェイを介して接続する VPC には重複する CIDR ブロックを設定できません。Direct Connect ゲートウェイに関連付けられた VPC に IPv4 CIDR ブロックを追加する場合は、その CIDR ブロックが、他の関連付け済み VPC の既存の CIDR ブロックと重複しないことを確認してください。詳細については、Amazon VPC ユーザーガイドの「IPv4 CIDR ブロックの VPC への追加」を参照してください。
- Direct Connect ゲートウェイへのパブリック仮想インターフェイスを作成することはできません。

- Direct Connect ゲートウェイは、アタッチされたプライベート仮想インターフェイスと関連付けられた仮想プライベートゲートウェイ間の通信のみをサポートし、別のプライベートゲートウェイへの仮想プライベートゲートウェイを有効にする場合があります。次のトラフィックはサポートされていません。
  - 単一の Direct Connect ゲートウェイに関連付けられた VPC 間の直接的な通信。これには、単一の Direct Connect ゲートウェイを介したオンプレミスネットワーク経由のヘアピンを使用した 1 つの VPC から別の VPC へのトラフィックが含まれます。
  - 単一の Direct Connect ゲートウェイにアタッチされた仮想インターフェイス間の直接的な通信。
  - 単一の Direct Connect ゲートウェイにアタッチされた仮想インターフェイスと、同じ Direct Connect ゲートウェイに関連付けられた仮想プライベートゲートウェイの VPN 接続との間の直接的な通信。
- 仮想プライベートゲートウェイを、複数の Direct Connect ゲートウェイに関連付けることはできません。また、プライベート仮想インターフェイスを、複数の Direct Connect ゲートウェイにアタッチすることはできません。
- Direct Connect ゲートウェイに関連付けた仮想プライベートゲートウェイを、VPC にアタッチする必要があります。
- 仮想プライベートゲートウェイの関連付け提案は作成から 7 日後に有効期限が切れます。
- 受諾された仮想プライベートゲートウェイの提案、または削除された仮想プライベートゲートウェイの提案は、3 日間表示されたままとなります。
- 仮想プライベートゲートウェイは Direct Connect ゲートウェイに関連付けられ、仮想インターフェイスにアタッチすることもできます。
- VPC から仮想プライベートゲートウェイをデタッチすると、仮想プライベートゲートウェイと Direct Connect ゲートウェイの関連付けも解除されます。

同じリージョンの VPC AWS Direct Connect にのみ接続を接続するには、Direct Connect ゲートウェイを作成できます。または、プライベート仮想インターフェイスを作成し、VPCの仮想プライベートゲートウェイにアタッチすることもできます。詳細については、「」プライベート仮想インターフェイスを作成する と「VPN CloudHub」を参照してください。

別のアカウントの VPC AWS Direct Connect との接続を使用するには、そのアカウント用のホスト型プライベート仮想インターフェイスを作成できます。他のアカウントの所有者は、ホスト仮想インターフェイスを受け入れると、アカウントの仮想プライベートゲートウェイまたは Direct Connect ゲートウェイにそのインターフェイスをアタッチすることを選択できます。詳細については、「AWS Direct Connect 仮想インターフェイス」を参照してください。

目次

仮想プライベートゲートウェイの使用

仮想プライベートゲートウェイは、接続する VPC にアタッチされている必要があります。

> **Note**
>
> Direct Connect Gateway の仮想プライベートゲートウェイと動的 VPN 接続を使用する計画の場合は、仮想プライベートゲートウェイで、ASN を VPN 接続に必要な値に変更します。それ以外の場合、仮想プライベートゲートウェイの ASN は許可されている任意の値に設定することができます。Direct Connect Gateway は、接続されているすべての VPC を、それに割り当てられている ASN 経由でアドバタイズします。

仮想プライベートゲートウェイを作成した後は、VPC にアタッチする必要があります。

仮想プライベートゲートウェイを作成して VPC にアタッチするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [仮想プライベートゲートウェイ] を選択してから、[仮想プライベートゲートウェイの作成] を選択します。
3. (オプション) 仮想プライベートゲートウェイの名前を入力します。これにより、Name というキーと指定した値を含むタグが作成されます。
4. [ASN] では、デフォルトの Amazon ASN を使用するためにデフォルトの選択のままにします。それ以外の場合は、[カスタム ASN] を選択して値を入力します。16 ビット ASN では、値は 64512 から 65534 の範囲内である必要があります。32 ビット ASN では、値は 4200000000 から 4294967294 の範囲内である必要があります。
5. [Create Virtual Private Gateway] を選択します。
6. 作成した仮想プライベートゲートウェイを選択した後、[Actions]、[Attach to VPC] を選択します。

7. リストから VPC を選択し、[Yes, Attach] を選択します。

コマンドラインまたは API を使用して仮想プライベートゲートウェイを作成するには

- CreateVpnGateway(Amazon EC2 クエリ API)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

コマンドラインまたは API を使用して仮想プライベートゲートウェイを VPC にアタッチするには

- AttachVpnGateway(Amazon EC2 クエリ API)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

仮想プライベートゲートウェイの関連付けと関連付けの解除

仮想プライベートゲートウェイと Direct Connect ゲートウェイを関連付けたり、関連付けを解除したりできます。仮想プライベートゲートウェイのアカウント所有者がこうした操作を実行します。

仮想プライベートゲートウェイを関連付けるには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Direct Connect ゲートウェイ] を選択し、Direct Connect ゲートウェイを選択します。
3. [詳細を表示] を選択します。
4. [ゲートウェイの関連付け]、[ゲートウェイを関連付ける] の順に選択します。
5. [ゲートウェイ] で、関連する仮想プライベートゲートウェイを選択したら、[Associate gateway (ゲートウェイを関連付ける)] を選択します。

[Gateway associations (ゲートウェイの関連付け)] を選択すると、Direct Connect ゲートウェイに関連付けられたすべての仮想プライベートゲートウェイを表示できます。

仮想プライベートゲートウェイの関連付けを解除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Direct Connect Gateway] を選択し、Direct Connect ゲートウェイを選択します。
3. [View details] を選択します。
4. [Gateway associations (ゲートウェイの関連付け)] を選択し、仮想プライベートゲートウェイを選択します。
5. [関連付け解除] を選択します。

コマンドラインまたは API を使用して仮想プライベートゲートウェイを関連付けるには

- create-direct-connect-gateway-アソシエーション ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

コマンドラインまたは API を使用して、Direct Connect ゲートウェイに関連付けられた仮想プライベートゲートウェイを表示するには

- describe-direct-connect-gateway-アソシエーション ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

コマンドラインまたは API を使用して仮想プライベートゲートウェイの関連付けを解除するには

- delete-direct-connect-gateway-アソシエーション ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

Direct Connect ゲートウェイへのプライベート仮想インターフェイスの作成

AWS Direct Connect 接続をリモート VPC に接続するには、接続用のプライベート仮想インターフェイスを作成する必要があります。接続先の Direct Connect ゲートウェイを指定します。

> **Note**
>
> ホストされたプライベート仮想インターフェイスを受け入れる場合は、アカウントの Direct Connect ゲートウェイに関連付けることができます。詳細については、「ホスト仮想インターフェイスを承諾する」を参照してください。

Direct Connect ゲートウェイへのプライベート仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] で [プライベート] を選択します。
5. [プライベート仮想インターフェイス設定] で以下を実行します。

   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

   c. 仮想インターフェースオーナーの場合、 AWS 仮想インターフェースが自分のアカウント用であれば、[My AWS account] を選択します。

   d. [Direct Connect ゲートウェイ] の場合、[Direct Connect ゲートウェイ] を選択します。

   e. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

   f. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

      有効な値は 1～2,147,483,647 です。
6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

      - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
      - [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

> **Important**
>
> AWS IPv4アドレスの自動割り当てを許可すると、接続に関するRFC 3927に従って、169.254.0.0/16 IPv4リンクローカルから/29 CIDRが割り当てられます。 point-to-point AWS カスタマールーターのピアIPアドレスを VPC トラフィックの送信元または宛先として使用する場合は、このオプションはお勧めしません。代わりに、RFC 1918 または他のアドレス (RFC 1918 以外) を使用して、アドレスを自分で指定する必要があります。
>
> - RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。
> - RFC 3927 の詳細については、「IPv4 リンクローカルアドレスのダイナミック設定」を参照してください。

[IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

b. 最大送信単位 (MTU) を 1500 (デフォルト) から 9001 (ジャンボフレーム) に変更するには、[ジャンボ MTU (MTU サイズ 9001)] を選択します。

c. (オプション) [有効化] で [有効] を選択し SiteLink、Direct Connect のポイントオブプレゼンス間の直接接続を有効にします。

d. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

仮想インターフェイスを作成したら、デバイス用のルーター設定をダウンロードできます。詳細については、「ルーター設定ファイルをダウンロードする」を参照してください。

コマンドラインまたは API を使用してプライベート仮想インターフェイスを作成するには

- create-private-virtual-interface (AWS CLI)

- CreatePrivateVirtualInterface(AWS Direct Connect API)

コマンドラインまたは API を使用して、Direct Connect ゲートウェイにアタッチされた仮想インターフェイスを表示するには

- describe-direct-connect-gateway-添付ファイル ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

アカウント間で仮想プライベートゲートウェイを関連付ける

Direct Connect ゲートウェイは、 AWS 任意のアカウントが所有する仮想プライベートゲートウェイに関連付けることができます。Direct Connect ゲートウェイは、既存のゲートウェイにすることも、新しいゲートウェイを作成することもできます。仮想プライベートゲートウェイの所有者は関連付け提案を作成し、Direct Connect ゲートウェイの所有者はこの関連付け提案を承諾する必要があります。

関連付け提案には、仮想プライベートゲートウェイから許可されるプレフィックスを含めることができます。Direct Connect ゲートウェイの所有者は、関連付け提案でリクエストされたプレフィックスを必要に応じて上書きできます。

許可されたプレフィックス

仮想プライベートゲートウェイを Direct Connect ゲートウェイに関連付ける場合、Amazon VPC プレフィックスのリストを指定して、Direct Connect ゲートウェイをアドバタイズします。プレフィックスリストは、同じ CIDR またはより小さな CIDR が Direct Connect ゲートウェイにアドバタイズされることを許可するフィルタとして機能します。仮想プライベートゲートウェイでは VPC CIDR 全体をプロビジョニングするため、VPC CIDR と同じあるいはより広い範囲の [許可されたプレフィックス] を設定する必要があります。

VPC CIDR が 10.0.0.0/16 のケースを考えてみます。[許可されたプレフィックス] は、10.0.0.0/16 (VPC CIDR 値) あるいは 10.0.0.0/15 (VPC CIDR よりも広い範囲の値) で設定できます。

Direct Connect を介してアドバタイズされたネットワークプレフィックス内の仮想インターフェイスは、同じリージョン内ではなく、リージョンをまたがるトランジットゲートウェイにのみ伝達されます。許可されたプレフィックスと、仮想プライベートゲートウェイおよび Transit Gateway のやり取りの詳細については、the section called “許可されたプレフィックスのインタラクション” を参照してください。

タスク

- 関連付け提案を作成する
- 関連付け提案の承諾または拒否
- 関連付けに許可されたプレフィックスを更新する
- 関連付け提案を削除する

関連付け提案を作成する

仮想プライベートゲートウェイを所有している場合、関連付け提案を作成する必要があります。仮想プライベートゲートウェイは、 AWS アカウントの VPC にアタッチする必要があります。Direct Connect ゲートウェイの所有者は、Direct Connect ゲートウェイの ID AWS とそのアカウントの ID を共有する必要があります。提案を作成したら、Direct Connect ゲートウェイの所有者は、 を介したオンプレミスネットワークへのアクセスを取得するためにこの提案を承諾する必要があります AWS Direct Connect

関連付け提案を作成するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Virtual private gateways (仮想プライベートゲートウェイ)] を選択し、仮想プライベートゲートウェイを選びます。
3. [View details] を選択します。
4. [Direct Connect gateway associations (Direct Connect ゲートウェイの関連付け)] を選択し、[Associate Direct Connect gateway (Direct Connect ゲートウェイを関連付ける)] を選びます。
5. [Association account type (関連付けアカウントのタイプ)] の [アカウント所有者] で、[別のアカウント] を選択します。
6. [Direct Connect gateway owner] (Direct Connect ゲートウェイの所有者) に、Direct Connect ゲートウェイを所有している AWS アカウントの ID を入力します。
7. [Association settings (関連付け設定)] で、以下を実行します。

   a. [Direct Connect gateway ID] で、Direct Connect ゲートウェイの ID を入力します。

   b. Direct Connect ゲートウェイ所有者には、アソシエーションの Direct Connect AWS ゲートウェイを所有するアカウントの ID を入力します。

   c. (オプション) 仮想プライベートゲートウェイから許可されるプレフィックスのリストを指定するには、[許可されたプレフィックス] にプレフィックスを追加します。プレフィックスは、カンマを使用して区切るか、1 行ずつ入力します。

8. [Associate Direct Connect gateway (Direct Connect ゲートウェイの関連付け)] を選択します。

コマンドラインまたは API を使用して関連付け提案を作成するには

- create-direct-connect-gateway-アソシエーションプロポーザル ()AWS CLI
- CreateDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

関連付け提案の承諾または拒否

Direct Connect ゲートウェイを所有している場合、関連付けを作成するために関連付け提案を承諾する必要があります。それ以外の場合は、関連付け提案を拒否できます。

関連付け提案を承諾するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Direct Connect Gateway] を選択します。
3. 保留中の提案がある Direct Connect ゲートウェイを選択し、[詳細を表示] を選びます。
4. [Pending proposals (保留中の提案)] タブで提案を選択し、[提案を許可] を選びます。
5. (オプション) 仮想プライベートゲートウェイから許可されるプレフィックスのリストを指定するには、[許可されたプレフィックス] にプレフィックスを追加します。プレフィックスは、カンマを使用して区切るか、1 行ずつ入力します。
6. [提案を許可] を選択します。

関連付け提案を拒否するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Direct Connect Gateway] を選択します。
3. 保留中の提案がある Direct Connect ゲートウェイを選択し、[詳細を表示] を選びます。
4. [Pending proposals (保留中の提案)] タブで仮想プライベートゲートウェイを選択し、[提案を拒否] を選びます。
5. [提案を拒否] のダイアログボックスで Delete (削除) と入力し、[提案を拒否] を選択します。

コマンドラインまたは API を使用して関連付け提案を表示するには

- describe-direct-connect-gateway-アソシエーション-プロポーザル ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposalsAWS Direct Connect (API)

コマンドラインまたは API を使用して関連付け提案を承諾するには

- accept-direct-connect-gateway-アソシエーション-プロポーザル ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

コマンドラインまたは API を使用して関連付け提案を拒否するには

- delete-direct-connect-gateway-アソシエーション-プロポーザル ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

関連付けに許可されたプレフィックスを更新する

Direct Connect ゲートウェイを介した仮想プライベートゲートウェイから許可されるプレフィックスを更新できます。

仮想プライベートゲートウェイを所有している場合、同じ Direct Connect ゲートウェイに許可するプレフィックスを指定して新しい関連付け提案を作成します。

Direct Connect ゲートウェイを所有している場合、関連付け提案を承諾するときに許可されたプレフィックスを更新できます。また、次に示すように、既存の関連付けに許可されたプレフィックスを更新できます。

コマンドラインまたは API を使用して、既存の関連付けに許可されたプレフィックスを更新するには

- update-direct-connect-gateway-アソシエーション ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

関連付け提案を削除する

仮想プライベートゲートウェイの所有者は、Direct Connect ゲートウェイの関連付け提案がまだ承諾の保留中である場合に、この提案を削除できます。関連付け提案の承諾後はこれを削除することはできませんが、Direct Connect ゲートウェイから仮想プライベートゲートウェイの関連付けを解除する

ことができます。詳細については、「the section called “仮想プライベートゲートウェイの関連付けと関連付けの解除”」を参照してください。

関連付け提案を削除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Virtual private gateways (仮想プライベートゲートウェイ)] を選択し、仮想プライベートゲートウェイを選びます。
3. [View details] を選択します。
4. [Pending Direct Connect gateway associations (保留中の Direct Connect ゲートウェイの関連付け)] を選択し、関連付けを選び、[Delete (削除)] を選択します。
5. [Delete association proposal (関連付け提案の削除)] のダイアログボックスで Delete (削除) と入力し、[Delete (削除)] を選択します。

コマンドラインまたは API を使用して、保留中の関連付け提案を削除するには

- delete-direct-connect-gateway-アソシエーション-プロポーザル ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

トランジットゲートウェイの関連付け

Transit Gateway にアタッチされた VPC または VPN へのトランジット仮想インターフェイス経由で AWS Direct Connect 接続に接続するには、AWS Direct Connect ゲートウェイを使用できます。Direct Connect ゲートウェイを Transit Gateway に関連付けます。次に、Direct Connect AWS Direct Connect ゲートウェイに接続するためのトランジット仮想インターフェイスを作成します。

以下のルールが Transit Gateway の関連付けに適用されます。

- Direct Connect ゲートウェイが既に仮想プライベートゲートウェイに関連付けられている場合、または仮想プライベートインターフェイスにアタッチされている場合は、Direct Connect ゲートウェイを Transit Gateway にアタッチすることはできません。
- Direct Connect ゲートウェイの作成および使用には制限があります。詳細については、「クォータ」を参照してください。
- Direct Connect ゲートウェイは、アタッチされたトランジット仮想インターフェイスと、関連する Transit Gateway の間の通信をサポートします。

- 異なるリージョンにある複数の Transit Gateway に接続する場合は、それぞれの Transit Gateway に一意の ASN を使用します。
- Direct Connect を介してアドバタイズされたネットワークプレフィックス内の仮想インターフェイスは、リージョン間のトランジットゲートウェイにのみ伝播され、同じリージョン内では伝達されません

トランジットゲートウェイの関連付けと関連付け解除

Transit Gateway を関連付けるには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Direct Connect Gateway] を選択し、Direct Connect ゲートウェイを選択します。
3. [View details] を選択します。
4. [Gateways associations (ゲートウェイの関連付け)]、[Associate gateway (ゲートウェイを関連付ける)] の順に選択します。
5. [Gateways (ゲートウェイ)] で、Transit Gateway を選択して関連付けます。
6. [許可されたプレフィックス] に、Direct Connect ゲートウェイがオンプレミスのデータセンターにアドバタイズするプレフィックス (カンマ区切りまたは改行) を入力します。許可されたプレフィックスの詳細については、「the section called “許可されたプレフィックスのインタラクション”」を参照してください。
7. [Associate gateway (ゲートウェイを関連付ける)] を選択します

[Gateway associations (ゲートウェイの関連付け)] を選択すると、Direct Connect ゲートウェイに関連付けられたすべてのゲートウェイを表示できます。

Transit Gateway の関連付けを解除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Direct Connect ゲートウェイ] を選択し、Direct Connect ゲートウェイを選択します。
3. [View details] を選択します。

4. [Gateway associations (ゲートウェイの関連付け)] を選択し、トランジットゲートウェイを選択します。
5. [関連付け解除] を選択します。

トランジットゲートウェイの許可されたプレフィックスを更新する

トランジットゲートウェイの許可されたプレフィックスを追加または削除することができます。

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Direct Connect gateways] (Direct Connect ゲートウェイ) をクリックしてから、許可されたプレフィックスの追加または削除を行う Direct Connect ゲートウェイを選択します。
3. [Gateway associations] (ゲートウェイの関連付け) タブを選択します。
4. 変更するゲートウェイを選択してから、[Edit] (編集) をクリックします。
5. [Allowed prefixes] (許可されたプレフィックス) に、Direct Connect ゲートウェイがオンプレミスのデータセンターにアドバタイズするプレフィックスを入力します。プレフィックスが複数ある場合は、各プレフィックスをカンマで区切るか、各プレフィックスを新しい行で指定します。追加するプレフィックスは、すべての仮想プライベートゲートウェイの Amazon VPC CIDR と一致する必要があります。許可されたプレフィックスの詳細については、「the section called “許可されたプレフィックスのインタラクション”」を参照してください。
6. [Edit association] を選択します。

   [Gateway association] (ゲートウェイの関連付け) セクションの [State] (状態) に [updating] (更新中) が表示されます。完了したら、[State] (状態) が [associated] (関連付け完了) に変わります。
7. [Disassociate] (関連付け解除) を選択します。
8. [Disassociate] (関連付けを解除する) を再度選択して、ゲートウェイの関連付けの削除を確認します。

   [Gateway association] (ゲートウェイの関連付け) セクションの [State] (状態) に [disassociating] (関連付けを解除中) が表示されます。完了すると、確認メッセージが表示され、ゲートウェイがセクションから削除されます。この処理は、完了まで数分、またはそれ以上かかる場合があります。

コマンドラインまたは API を使用して Transit Gateway を関連付けるには

- create-direct-connect-gateway-アソシエーション ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

コマンドラインまたは API を使用して、Direct Connect ゲートウェイに関連付けられた Transit Gateway を表示するには

- describe-direct-connect-gateway-アソシエーション ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

コマンドラインまたは API を使用して Transit Gateway の関連付けを解除するには

- delete-direct-connect-gateway-アソシエーション ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

コマンドラインまたは API を使用してトランジットゲートウェイの許可されたプレフィックスを更新する

- update-direct-connect-gateway-アソシエーション ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Direct Connect ゲートウェイへのトランジット仮想インターフェイスの作成

AWS Direct Connect 接続をトランジットゲートウェイに接続するには、接続用のトランジットインターフェースを作成する必要があります。接続先の Direct Connect ゲートウェイを指定します。

> **Important**
>
> Transit Gateway を 1 つ以上の Direct Connect ゲートウェイに関連付ける場合、Transit Gateway およびその Direct Connect ゲートウェイで使用される自律システム番号 (ASN) は異なる値である必要があります。たとえば、Transit Gateway と Direct Connect ゲートウェイの両方にデフォルトの ASN 64512 を使用すると、関連付けのリクエストは失敗します。

Direct Connect ゲートウェイへのトランジット仮想インターフェイスをプロビジョニングするには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [Transit (トランジット)] を選択します。
5. [Transit virtual interface settings (トランジット仮想インターフェイス設定)] で以下を実行します。

   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。

   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。

   c. 仮想インターフェースオーナーの場合、 AWS 仮想インターフェースが自分のアカウント用であれば、「My AWS account」を選択します。

   d. [Direct Connect ゲートウェイ] の場合、[Direct Connect ゲートウェイ] を選択します。

   e. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。

   f. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

      有効な値は 1 ~ 2,147,483,647 です。

6. [追加設定] で、以下を実行します。

   a. IPv4 BGP あるいは an IPv6 ピアを設定するには、以下を実行します。

      [IPv4] IPv4 BGP ピアを設定する場合は、[IPv4] を選択し、以下のいずれかを実行します。

      - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。
      - [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

      > **Important**
      >
      > AWS IPv4アドレスの自動割り当てを許可すると、接続に関するRFC 3927に従って、169.254.0.0/16 IPv4リンクローカルから/29 CIDRが割り当てられます。 point-to-point AWS カスタマールーターのピアIPアドレスを VPC トラフィックの送信

元または宛先として使用する場合は、このオプションはお勧めしません。代わりに、RFC 1918 または他のアドレス (RFC 1918 以外) を使用して、アドレスを自分で指定する必要があります。

- RFC 1918 の詳細については、「プライベートインターネットのアドレス割り当て」を参照してください。
- RFC 3927 の詳細については、「IPv4 リンクローカルアドレスのダイナミック設定」を参照してください。

[IPv6] IPv6 BGP ピアを設定する場合は、[IPv6] を選択します。ピア IPv6 アドレスは、Amazon の IPv6 アドレスのプールから自動的に割り当てられます。独自の IPv6 アドレスを指定することはできません。

b. 最大送信単位 (MTU) を 1500 (デフォルト) から 8500 (ジャンボフレーム) に変更するには、[ジャンボ MTU (MTU サイズ 8500)] を選択します。

c. (オプション) [有効化] で [有効] を選択し SiteLink、Direct Connect のポイントオブプレゼンス間の直接接続を有効にします。

d. (オプション) タグを追加または削除します。

[タグの追加] [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。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

仮想インターフェイスを作成したら、デバイス用のルーター設定をダウンロードできます。詳細については、「ルーター設定ファイルをダウンロードする」を参照してください。

コマンドラインまたは API を使用してトランジット仮想インターフェイスを作成するには

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS Direct Connect API)

コマンドラインまたは API を使用して、Direct Connect ゲートウェイにアタッチされた仮想インターフェイスを表示するには

- describe-direct-connect-gateway-添付ファイル ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

アカウント間のトランジットゲートウェイの関連付け

既存の Direct Connect ゲートウェイまたは新しい Direct Connect ゲートウェイを、 AWS 任意のアカウントが所有する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 の所有者が関連付け提案を作成し、Direct Connect ゲートウェイの所有者がこの関連付け提案を承諾する必要があります。

関連付け提案には、Transit Gateway から許可されるプレフィックスを含めることができます。Direct Connect ゲートウェイの所有者は、関連付け提案でリクエストされたプレフィックスを必要に応じて上書きできます。

許可されたプレフィックス

Transit Gateway の関連付けの場合、許可されたプレフィックスリストを Direct Connect ゲートウェイでプロビジョニングします。このリストは、トランジットゲートウェイに接続されている VPC に CIDR が割り当てられていない場合でも、オンプレミスからトランジットゲートウェイへのトラフィックのルーティングに使用されます。 AWS Direct Connect ゲートウェイのプレフィックスにより、Direct Connect ゲートウェイからのプレフィックスリストの送信が許可され、オンプレミスネットワークにアドバタイズされます。許可されたプレフィックスが Transit Gateway および仮想プライベートゲートウェイを操作する方法については、the section called “許可されたプレフィックスのインタラクション” を参照してください。

タスク

- トランジットゲートウェイの関連付け提案の作成
- トランジットゲートウェイの関連付け提案の受諾または拒否
- トランジットゲートウェイの関連付けの許可されたプレフィックスの更新
- トランジットゲートウェイの関連付け提案の削除

トランジットゲートウェイの関連付け提案の作成

Transit Gateway を所有している場合は、関連付け提案を作成する必要があります。トランジットゲートウェイは、 AWS アカウントの VPC または VPN に接続する必要があります。Direct Connect ゲートウェイの所有者は、Direct Connect ゲートウェイの ID とその AWS アカウントの ID を共有する必要があります。提案を作成したら、Direct Connect ゲートウェイの所有者は、 を介したオンプレミスネットワークへのアクセスを取得するためにこの提案を承諾する必要があります AWS Direct Connect

関連付け提案を作成するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Transit Gateways (トランジットゲートウェイ)] を選択し、トランジットゲートウェイを選択します。
3. [View details] を選択します。
4. [Direct Connect gateway associations (Direct Connect ゲートウェイの関連付け)] を選択し、[Associate Direct Connect gateway (Direct Connect ゲートウェイを関連付ける)] を選びます。
5. [Association account type (関連付けアカウントのタイプ)] の [アカウント所有者] で、[別のアカウント] を選択します。
6. [Direct Connect gateway owner] (Direct Connect ゲートウェイの所有者) に、Direct Connect ゲートウェイを所有しているアカウントの ID を入力します。
7. [Association settings (関連付け設定)] で、以下を実行します。

   a. [Direct Connect gateway ID] で、Direct Connect ゲートウェイの ID を入力します。

   b. [仮想インターフェイス所有者] に、関連付ける仮想インターフェイスを所有しているアカウントの ID を入力します。

   c. (オプション) Transit Gateway から許可されるプレフィックスのリストを指定するには、[Allowed prefixes (許可されたプレフィックス)] にプレフィックスを追加します。プレフィックスは、カンマを使用して区切るか、1 行ずつ入力します。
8. [Associate Direct Connect gateway (Direct Connect ゲートウェイの関連付け)] を選択します。

コマンドラインまたは API を使用して関連付け提案を作成するには

- create-direct-connect-gateway-アソシエーションプロポーザル ()AWS CLI
- CreateDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

トランジットゲートウェイの関連付け提案の受諾または拒否

Direct Connect ゲートウェイを所有している場合、関連付けを作成するために関連付け提案を承諾する必要があります。関連付け提案を拒否することもできます。

関連付け提案を承諾するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Direct Connect Gateway] を選択します。
3. 保留中の提案がある Direct Connect ゲートウェイを選択し、[詳細を表示] を選びます。
4. [Pending proposals (保留中の提案)] タブで提案を選択し、[提案を許可] を選びます。
5. (オプション) Transit Gateway から許可されるプレフィックスのリストを指定するには、[Allowed prefixes (許可されたプレフィックス)] にプレフィックスを追加します。プレフィックスは、カンマを使用して区切るか、1 行ずつ入力します。
6. [提案を許可] を選択します。

関連付け提案を拒否するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Direct Connect Gateway] を選択します。
3. 保留中の提案がある Direct Connect ゲートウェイを選択し、[詳細を表示] を選びます。
4. [Pending proposals (保留中の提案)] タブでトランジットゲートウェイを選択し、[提案を拒否] を選択します。
5. [提案を拒否] のダイアログボックスで「Delete (削除)」と入力し、[提案を拒否] を選択します。

コマンドラインまたは API を使用して関連付け提案を表示するには

- describe-direct-connect-gateway-アソシエーション-プロポーザル ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposalsAWS Direct Connect (API)

コマンドラインまたは API を使用して関連付け提案を承諾するには

- accept-direct-connect-gateway-アソシエーション-プロポーザル ()AWS CLI

- AcceptDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

コマンドラインまたは API を使用して関連付け提案を拒否するには

- delete-direct-connect-gateway-アソシエーション-プロポーザル ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

トランジットゲートウェイの関連付けの許可されたプレフィックスの更新

Direct Connect ゲートウェイを介して、Transit Gateway から許可されたプレフィックスから更新できます。

Transit Gateway を所有している場合、許可するプレフィックスを指定して、同じ Direct Connect ゲートウェイおよび仮想プライベートゲートウェイ用に新しい関連付け提案を作成します。

Direct Connect ゲートウェイを所有している場合、関連付け提案を承諾するときに許可されたプレフィックスを更新できます。また、次に示すように、既存の関連付けに許可されたプレフィックスを更新できます。

コマンドラインまたは API を使用して、既存の関連付けに許可されたプレフィックスを更新するには

- update-direct-connect-gateway-アソシエーション ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

トランジットゲートウェイの関連付け提案の削除

Transit Gateway の所有者は、Direct Connect ゲートウェイの関連付け提案がまだ承諾の保留中である場合に、この提案を削除できます。関連付け提案の承諾後はこれを削除することはできませんが、Direct Connect ゲートウェイからトランジットゲートウェイの関連付けを解除することができます。詳細については、「the section called “トランジットゲートウェイの関連付け提案の作成”」を参照してください。

関連付け提案を削除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。

2. ナビゲーションペインで、[Transit Gateways (トランジットゲートウェイ)] を選択し、トランジットゲートウェイを選択します。
3. [View details] を選択します。
4. [Pending gateway associations (保留中のゲートウェイの関連付け)] を選択し、関連付けを選び、[Delete (削除)] を選択します。
5. [Delete association proposal (関連付け提案の削除)] のダイアログボックスで「Delete (削除)」と入力し、[Delete (削除)] を選択します。

コマンドラインまたは API を使用して、保留中の関連付け提案を削除するには

- delete-direct-connect-gateway-アソシエーション-プロポーザル ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposalAWS Direct Connect (API)

許可されたプレフィックスのインタラクション

許可されたプレフィックスが Transit Gateway や仮想プライベートゲートウェイとやり取りする方法について説明します。詳細については、「the section called “ルーティングポリシーと BGP コミュニティ”」を参照してください。

仮想プライベートゲートウェイの関連付け

プレフィックスリスト (IPv4 と IPv6) は、同じ CIDR またはより小さな範囲の CIDR が Direct Connect ゲートウェイにアドバタイズされることを許可するフィルタとして機能します。プレフィックスは、VPC CIDR ブロックと同じ範囲またはより広い範囲に設定する必要があります。

> **Note**
>
> 許可リストはフィルタとしてのみ機能し、関連付けられた VPC CIDR のみがカスタマーゲートウェイにアドバタイズされます。

CIDR 10.0.0.0/16 が仮想プライベートゲートウェイにアタッチされた VPC があるシナリオを考えてみます。

- 許可されたプレフィックスリストが 22.0.0.0/24 に設定されている場合、ルートは受け取りません。これは、22.0.0.0/24 が 10.0.0.0/16 と同じあるいはより広くないためです。

- 許可されたプレフィックスリストが 10.0.0.0/24 に設定されている場合、ルートは受け取りません。これは、10.0.0.0/24 が 10.0.0.0/16 と同じでないためです。
- 許可されたプレフィックスリストが 10.0.0.0/15 に設定されている場合、10.0.0.0/16 は受け取ります。これは、IP アドレスが 10.0.0.0/16 より広いためです。

許可されたプレフィックスを削除または追加しても、そのプレフィックスを使用しないトラフィックは影響を受けません。更新中、ステータスは `associated` から `updating` に変化します。既存のプレフィックスを変更すると、そのプレフィックスを使用するトラフィックだけが遅延する可能性があります。

トランジットゲートウェイの関連付け

Transit Gateway の関連付けの場合、許可されたプレフィックスリストを Direct Connect ゲートウェイでプロビジョニングします。このリストは、Transit Gateway にアタッチされた VPC に割り当てられた CIDR がない場合でも、Direct Connect ゲートウェイとの間のオンプレミストラフィックを Transit Gateway にルーティングします。使用可能なプレフィックスは、ゲートウェイのタイプによって動作が異なります。

- トランジットゲートウェイアソシエーションでは、入力された許可されたプレフィックスのみがオンプレミスにアドバタイズされます。これらは Direct Connect ゲートウェイ ASN から発信されたものとして表示されます。
- 仮想プライベートゲートウェイの場合、入力された許可されたプレフィックスは、同じまたはより小さい CIDR を許可するフィルターの役割を果たします。

CIDR 10.0.0.0/16 が Transit Gateway にアタッチされた VPC があるシナリオについて考えてみます。

- 許可されたプレフィックスリストが 22.0.0.0/24 に設定されている場合、トランジット仮想インターフェイスで BGP 経由で 22.0.0.0/24 を受信します。許可されたプレフィックスリスト内のプレフィクスを直接プロビジョニングするため、10.0.0.0/16 は受信しません。
- 許可されたプレフィックスリストが 10.0.0.0/24 に設定されている場合、トランジット仮想インターフェイスで BGP 経由で 10.0.0.0/24 を受信します。許可されたプレフィックスリスト内のプレフィクスを直接プロビジョニングするため、10.0.0.0/16 は受信しません。
- 許可されたプレフィックスリストが 10.0.0.0/8 に設定されている場合、トランジット仮想インターフェイスで BGP 経由で 10.0.0.0/8 を受信します。

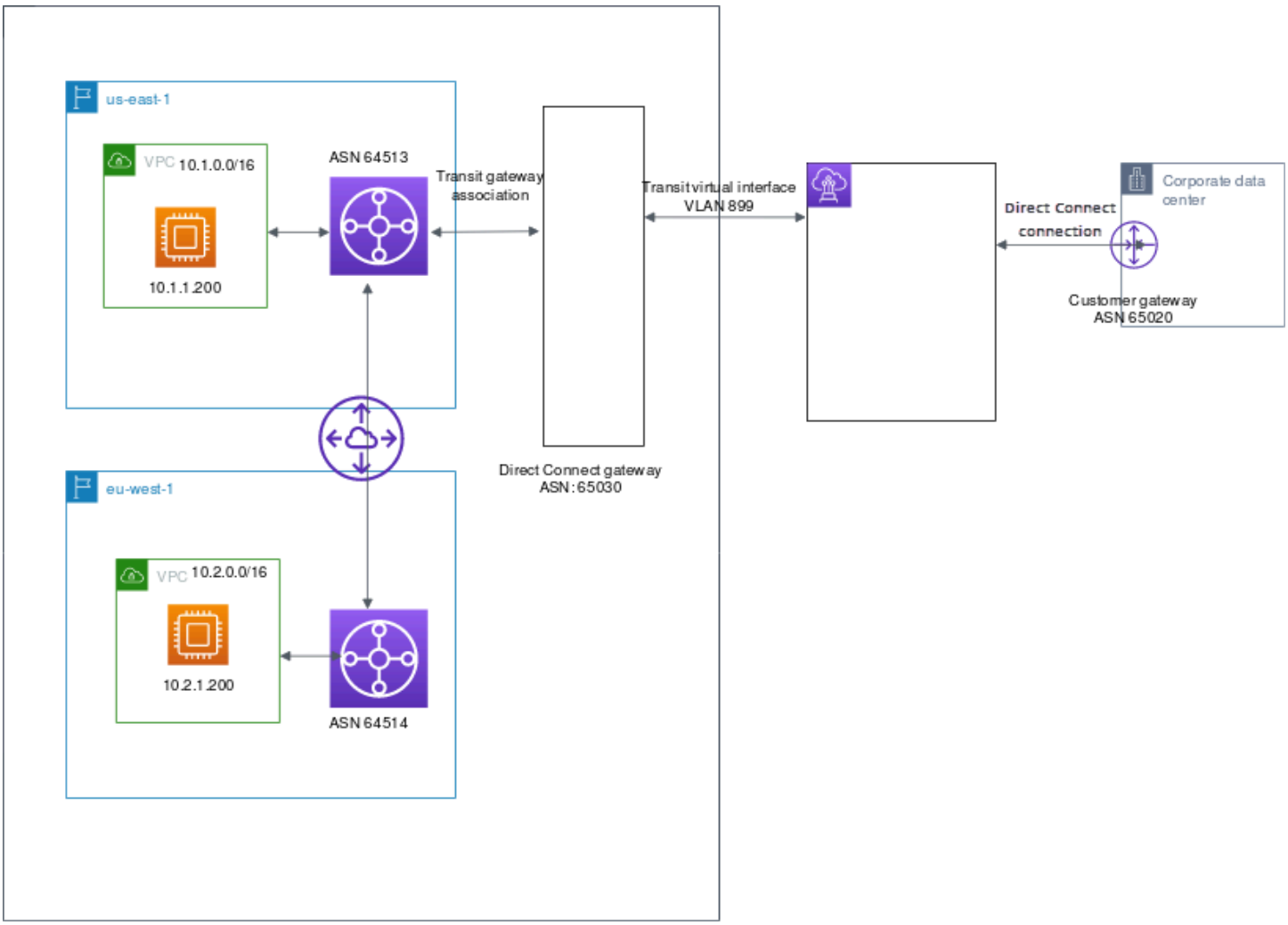
複数のトランジットゲートウェイが Direct Connect ゲートウェイに関連付けられている場合、許可されるプレフィックスの重複は許可されません。例えば、許可されたプレフィックスリストに 10.1.0.0/16 を含むトランジットゲートウェイがあり、許可されたプレフィックスリストが 10.2.0.0/16 と 0.0.0.0/0 を含む 2 番目のトランジットゲートウェイがある場合、2 番目のトランジットゲートウェイからの関連付けを 0.0.0.0/0 に設定することはできません。0.0.0.0/0 にはすべての IPv4 ネットワークが含まれるため、複数のトランジットゲートウェイが Direct Connect ゲートウェイに関連付けられている場合、0.0.0.0/0 を設定することはできません。許可されたルートが Direct Connect ゲートウェイの 1 つ以上の既存の許可ルートと重複していることを示すエラーが返されます。

許可されたプレフィックスを削除または追加しても、そのプレフィックスを使用しないトラフィックは影響を受けません。更新中、ステータスは `associated` から `updating` に変化します。既存のプレフィックスを変更すると、そのプレフィックスを使用するトラフィックだけが遅延する可能性があります。

例: トランジットゲートウェイの構成でプレフィックスを許可する

企業のデータセンターにアクセスする必要があるインスタンスが 2 つの異なる AWS リージョンにある構成を考えてみます。この構成には、次のリソースを使用します。

- 各リージョン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ピアリング接続。
- Direct Connect ゲートウェイ。
- トランジットゲートウェイ (us-east-1 のゲートウェイ) と Direct Connect ゲートウェイの間のトランジットゲートウェイの関連付け。
- オンプレミスの口ケーションと AWS Direct Connect 口ケーションからのトランジット仮想インターフェイス。



リソースに対して次のオプションを設定します。

- Direct Connect ゲートウェイ: ASN を 65030 に設定します。詳細については、「the section called “Direct Connect ゲートウェイの作成”」を参照してください。
- トランジット仮想インターフェイス: VLAN を 899、ASN を 65020 に設定します。詳細については、「the section called “Direct Connect ゲートウェイと接続するトランジット仮想インターフェイスを作成する”」を参照してください。
- Direct Connect ゲートウェイとトランジットゲートウェイの関連付け: 許可するプレフィックスを 10.0.0.0/8 に設定します。

  この CIDR ブロックは、両方の VPC CIDR ブロックをカバーします。詳細については、「the section called “トランジットゲートウェイの関連付けと関連付け解除”」を参照してください。
- VPC ルート: 10.2.0.0 VPC からのトラフィックをルーティングするには、VPC ルートテーブルにルートを作成します。宛先が 0.0.0.0/0 で、トランジットゲートウェイ ID がターゲットになりま

す。トランジットゲートウェイへのルーティングの詳細については、Amazon VPC ユーザーガイドの Routing for a transit gateway を参照してください。

AWS Direct Connect リソースのタグ付け

タグは、リソースの所有者が自分の AWS Direct Connect リソースに割り当てるラベルです。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。タグを使用すると、AWS Direct Connect リソースを用途、環境などのさまざまな方法で分類できます。これは、同じタイプのリソースが多数ある場合に役立ちます。割り当てたタグに基づいて特定のリソースをすばやく識別できます。

たとえば、リージョンの異なる場所に 2 つの AWS Direct Connect 接続がある場合。接続 dxcon-11aa22bb は接続のための本稼働トラフィックとなり、仮想インターフェース dxvif-33cc44dd に関連付けられます。接続 dxcon-abcabcab は冗長性(バックアップ)接続となり、仮想インターフェイス dxvif-12312312 に関連付けられます。接続と仮想インターフェイスに次のようなタグ付けをして、識別に役立たせることもできます。

[Resource ID (リソース ID)]	タグキー	タグ値
dxcon-11aa22bb	目的	本番稼働用
	場所	アムステルダム
dxvif-33cc44dd	目的	本番稼働用
dxcon-abcabcab	目的	バックアップ
	場所	フランクフルト
dxvif-12312312	目的	バックアップ

ニーズを満たす一連のタグキーをリソースタイプごとに考案されることをお勧めします。一貫性のあるタグキーセットを使用することで、リソースの管理が容易になります。タグには、AWS Direct Connect に関連する意味はなく、完全に文字列として解釈されます。また、タグは自動的にリソースに割り当てられます。タグのキーと値は編集でき、タグはリソースからいつでも削除できます。タグの値を空の文字列に設定することはできますが、タグの値を null に設定することはできません。特定のリソースについて既存のタグと同じキーを持つタグを追加した場合、以前の値は新しい値によって上書きされます。リソースを削除すると、リソースのタグも削除されます。

次の AWS Direct Connect リソースは、AWS Direct Connect コンソール、AWS Direct Connect API、AWS CLI、AWS Tools for Windows PowerShell、または AWS SDK を使用してタグ付けできま

す。このようなツールを使用してタグを管理する場合、リソースに Amazon リソースネーム (ARN) を指定する必要があります。ARN の詳細については、「Amazon Web Services 全般のリファレンス」の「Amazon リソースネーム (ARN)」を参照してください。

リソース	タグをサポート	作成時のタグをサポート	アクセスとリソースの割り当てを制御するタグをサポート	コスト配分をサポート
接続	はい	はい	はい	はい
仮想インターフェイス	はい	はい	はい	いいえ
Link aggregation groups (LAG)	はい	はい	はい	はい
相互接続	はい	はい	はい	はい
Direct Connect ゲートウェイ	いいえ	いいえ	いいえ	いいえ

タグの制限

タグには以下のルールや制限があります。

- リソースあたりのタグの最大数: 50
- キーの最大長: 128 文字 (Unicode)
- 値の最大長: 265 文字 (Unicode)
- タグのキーと値は大文字と小文字が区別されます。
- aws: プレフィックスは AWS の使用のために予約されています。タグに aws: というプレフィックスが付いたタグキーがある場合、タグのキーまたは値を編集、削除することはできません。aws: プレフィックスが付いたタグキーを持つタグは、リソースあたりのタグ数の制限に数えられません。
- 使用できる文字は、UTF-8 で表現できる文字、スペース、および数字と、特殊文字 (+、-、=、.、_、:、/、@) です。

- タグを追加または削除できるのは、リソースの所有者のみです。たとえば、ホスト接続がある場合、パートナーはタグを追加、削除、または表示することはできません。
- コスト配分タグは、接続、相互接続、および LAG に対してのみサポートされています。コスト管理にタグを使用する方法については、AWS Billing and Cost Management ユーザーガイドの「コスト配分タグの使用」を参照してください。

CLI または API でのタグの操作

リソースのタグの追加、更新、リスト表示、および削除には、次を使用します。

タスク	API	CLI
1 つ以上のタグを追加、または上書きします。	TagResource	タグリソース
1 つ以上のタグを削除します。	UntagResource	タグなしリソース
1 つ以上のタグを記述します。	DescribeTags	describe-tags

例

tag-resource コマンドを使用して、接続 dxcon-11aa22bb にタグ付けします。

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

describe-tags コマンドを使用して、接続 dxcon-11aa22bb のタグを示します。

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb
```

untag-resource コマンドを使用して、接続 dxcon-11aa22bb からタグを削除します。

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

AWS Direct Connect でのセキュリティ

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

セキュリティは、AWS と顧客の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ - AWS は、AWS クラウドで AWS のサービスを実行するインフラストラクチャを保護する責任を負います。また、AWS は、使用するサービスを安全に提供します。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。AWS Direct Connect に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」を参照してください。
- クラウド内のセキュリティ - ユーザーの責任は、使用する AWS のサービスに応じて異なります。また、お客様は、データの機密性、お客様の会社の要件、および適用される法律および規制など、その他の要因についても責任を負います。

このドキュメントは、AWS Direct Connect を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。次のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために AWS Direct Connect を設定する方法を示します。また、AWS リソースのモニタリングや保護に役立つ、他の AWS Direct Connect のサービスの使用方法についても説明します。

トピック

AWS Direct Connect でのデータ保護

AWS 責任共有モデルは、AWS Direct Connect でのデータ保護に適用されます。このモデルで説明されているように、AWS は、AWS クラウド のすべてを実行するグローバルインフラストラクチャを保護するがあります。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、「AWS セキュリティブログ」に投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データを保護するため、AWS アカウント の認証情報を保護し、AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーをセットアップすることをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみを各ユーザーに付与できます。また、次の方法でデータを保護することをおすすめします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須です。TLS 1.3 が推奨されます。
- AWS CloudTrail で API とユーザーアクティビティロギングをセットアップします。
- AWS のサービス内でデフォルトである、すべてのセキュリティ管理に加え、AWS の暗号化ソリューションを使用します。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API により AWS にアクセスするときに FIPS 140-2 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、AWS CLI、または AWS SDK で AWS Direct Connect または他の AWS のサービス を使用する場合も同様です。タグ、または名前に使用される自由形式のテキストフィールドに入力されるデータは、請求または診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

データ保護の詳細については AWS 責任共有モデルと AWS セキュリティブログ GDPR の GDPR ブログ投稿を参照してください。

トピック

- AWS Direct Connect のネットワーク間トラフィックプライバシー
- AWS Direct Connectでの暗号化

AWS Direct Connect のネットワーク間トラフィックプライバシー

サービスとオンプレミスのクライアントおよびアプリケーションとの間のトラフィック

プライベートネットワークと との間には 2 つの接続オプションがありますAWS

- AWS Site-to-Site VPN への関連付け。詳細については、「the section called “インフラストラクチャセキュリティ”」を参照してください。
- VPC への関連付け。詳細については、「the section called “仮想プライベートゲートウェイの関連付け”」および「the section called “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。

同じリージョン内の AWS リソース間のトラフィック

2 つの接続オプションがあります。

- AWS Site-to-Site VPN への関連付け。詳細については、「the section called “インフラストラクチャセキュリティ”」を参照してください。
- VPC への関連付け。詳細については、the section called “仮想プライベートゲートウェイの関連付け” および the section called “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。

AWS Direct Connectでの暗号化

AWS Direct Connect は、デフォルトで転送中のトラフィックを暗号化しません。を通過する転送中のデータを暗号化するには AWS Direct Connect、そのサービスの転送暗号化オプションを使用する必要があります。EC2 インスタンストラフィックの暗号化の詳細については、Amazon EC2 ユーザーガイド」の「転送中の暗号化」を参照してください。

AWS Direct Connect および では AWS Site-to-Site VPN、1 つ以上の AWS Direct Connect 専用ネットワーク接続を Amazon VPC VPN と組み合わせることができます。この組み合わせにより、IPsec で暗号化されたプライベート接続が提供されます。これにより、ネットワークコストが削減され、帯域幅のスループットが向上し、インターネットベースの VPN 接続よりも一貫性のあるネットワーク

体験が提供されます。詳細については、Amazon VPC から Amazon VPC への接続オプションを参照してください。

MAC Security (MACsec) は IEEE 標準の 1 つです。データの機密性、データの整合性、およびデータオリジンの信頼性を定義しています。MACsec をサポートする AWS Direct Connect 接続を使用して、企業のデータセンターから AWS Direct Connect の場所にデータを暗号化できます。詳細については、「MAC セキュリティ」を参照してください。

Direct Connect のための Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御するために役立つ AWS のサービスです。IAM 管理者は、誰を認証 (サインイン) し、誰に Direct Connect リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加費用なしで使用できる AWS のサービスです。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、Direct Connect で行う作業に応じて異なります。

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

サービス管理者 – 社内の Direct Connect リソースを担当している場合は、通常、Direct Connect へのフルアクセスがあります。サービスのユーザーがどの Direct Connect 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を確認して、IAM の基本概念を理解してください。会社で Direct Connect を使用して IAM を利用する方法の詳細については、Direct Connect が IAM と連携する仕組み を参照してください。

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

アイデンティティを使用した認証

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

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

ユーザーのタイプに応じて、AWS Management Console または AWS アクセスポータルにサインインできます。AWS へのサインインの詳細については、『AWS サインイン ユーザーガイド』の「AWS アカウント にサインインする方法」を参照してください。

プログラムで AWS にアクセスする場合、AWS は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) を提供し、認証情報でリクエストに暗号で署名します。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに署名する推奨方法の使用については、『IAM ユーザーガイド』の「AWS API リクエストの署名」を参照してください。

使用する認証方法を問わず、追加のセキュリティ情報の提供が求められる場合もあります。例えば、AWS では、アカウントのセキュリティ強化のために多要素認証 (MFA) の使用をお勧めしています。詳細については、『AWS IAM Identity Center ユーザーガイド』の「Multi-factor authentication (多要素認証)」 および『IAM ユーザーガイド』の「AWS での多要素認証 (MFA) の使用」を参照してください。

AWS アカウントのルートユーザー

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

フェデレーティッド ID

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

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

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

IAM ユーザーとグループ

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

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

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、『IAM ユーザーガイド』の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定の権限を持つ、AWS アカウント 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロールを切り替えることによって、AWS Management Console で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、『IAM ユーザーガイド』の「IAM ロールの使用」を参照してください。

一時的な認証情報を持った IAM ロールは、以下の状況で役立ちます。

- フェデレーティッドユーザーアクセス – フェデレーティッドアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーティッドアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、『IAM ユーザーガイド』の「Creating a role for a third-party Identity Provider (サードパーティーアイデンティティプロバイダー向けロールの作成)」を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、『AWS IAM Identity Center ユーザーガイド』の「権限セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の AWS のサービスでは、(ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできま

す。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

- クロスサービスアクセス - 一部の AWS のサービスでは、他の AWS のサービスの機能を使用します。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの権限、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS、Forward Access Session) – IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルと見なされます。一部のサービスを使用する際に、あるアクションを実行することで、別のサービスの別のアクションが開始されることがあります。FAS は、AWS のサービスを呼び出すプリンシパルのアクセス許可を使用し、リクエスト元の AWS のサービスと組み合わせて、ダウンストリームサービスにリクエストを行います。FAS リクエストは、完了するために他の AWS のサービスまたはリソースとのやり取りを必要とするリクエストをサービスが受信した場合にのみ作成されます。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、『IAM ユーザーガイド』の「AWS のサービス に権限を委任するロールの作成」を参照してください。
  - サービスリンクロール - サービスリンクロールは、AWS のサービス にリンクされたサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスリンクロールは、AWS アカウント に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールの権限を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション - EC2 インスタンスで実行され、AWS CLI または AWS API 要求を行っているアプリケーションの一時的な認証情報を管理するには、IAM ロールを使用できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスに添付されたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、『IAM ユーザーガイド』の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、『IAM ユーザーガイド』の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」を参照してください。

ポリシーを使用したアクセス権の管理

AWS でアクセス権を管理するには、ポリシーを作成して AWS アイデンティティまたはリソースにアタッチします。ポリシーは AWS のオブジェクトであり、アイデンティティやリソースに関連付けて、これらの権限を定義します。AWS は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。大半のポリシーは JSON ドキュメントとして AWSに保存されます。JSON ポリシードキュメントの構造と内容の詳細については、『IAM ユーザーガイド』の「JSON ポリシー概要」を参照してください。

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

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

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

アイデンティティベースポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件を制御します。アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

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

リソースベースのポリシー

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

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

アクセスコントロールリスト (ACL)

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

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

その他のポリシータイプ

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

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

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

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

複数のポリシータイプ

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

Direct Connect が IAM と連携する仕組み

IAM を使用して Direct Connect へのアクセスを管理する前に、Direct Connect で使用できる IAM 機能について理解しておく必要があります。

Direct Connect で使用できる IAM 機能

IAM の機能	Direct Connect のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	いいえ
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	なし

IAM の機能	Direct Connect のサポート
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	あり
プリンシパル権限	あり
サービスロール	あり
サービスリンクロール	いいえ

大部分の IAM 機能が Direct Connect および AWS のその他のサービスでどのように機能するかに関するおおまかな説明については、「IAM ユーザーガイド」の「IAM と連携する AWS のサービス」を参照してください。

Direct Connect のアイデンティティベースのポリシー

アイデンティティベースポリシーをサポートする	あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件を制御します。アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

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

Direct Connect アイデンティティベースのポリシーの例

Direct Connect アイデンティティベースのポリシーの例については、Direct Connect アイデンティティベースのポリシーの例 を参照してください。

Direct Connect リソースベースのポリシー

リソースベースのポリシーのサポート	なし

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

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる AWS アカウント にある場合、信頼できるアカウントの IAM 管理者は、リソースにアクセスするための権限をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーを追加する必要はありません。詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Direct Connect のポリシーアクション

ポリシーアクションに対するサポート	あり

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

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

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

Direct Connect アクションの一覧は、「サービス認可リファレンス」の「AWS Direct Connect で定義されるアクション」でご覧いただけます。

Direct Connect のポリシーアクションでは、アクションの前に次のプレフィックスを使用します。

```
Direct Connect
```

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

```
"Action": [
      "Direct Connect:action1",
      "Direct Connect:action2"
         ]
```

Direct Connect のポリシーリソース

ポリシーリソースに対するサポート	あり

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

JSON ポリシーの Resource 要素は、アクションが適用される 1 つ以上のオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの権限と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Direct Connect リソースタイプとその ARN のリストを表示するには、「AWS Direct Connect API リファレンス」の 「Direct Connect で定義されるリソースタイプ」を参照してください。どのアク

ションで各リソースの ARN を指定できるかについては、「Direct Connect で定義されるアクション」を参照してください。

Direct Connect アイデンティティベースのポリシーの例については、Direct Connect アイデンティティベースのポリシーの例 を参照してください。

Direct Connect リソースベースのポリシーの例については、タグベースの条件を使用した Direct Connect アイデンティティベースのポリシーの例 を参照してください。

Direct Connect のポリシー条件キー

サービス固有のポリシー条件キーのサポート	はい

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

`Condition` 要素 (または `Condition` ブロック) を使用すると、ステートメントが有効になる条件を指定できます。`Condition` 要素はオプションです。equal や less than などの条件演算子を使用して条件式を作成することによって、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の `Condition` 要素を指定するか、1 つの `Condition` 要素に複数のキーを指定すると、AWS は `AND` 論理演算子を使用してそれらを評価します。単一の条件キーに複数の値を指定すると、AWS は `OR` 論理演算子を使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、『IAM ユーザーガイド』の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS はグローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」の「AWS グローバル条件コンテキストキー」を参照してください。

Direct Connect 条件キーのリストを確認するには、「AWS Direct Connect API リファレンス」の「Direct Connect の条件キー」を参照してください。条件キーを使用できるアクションおよびリソースについては、「サービス認可リファレンス」の「AWS Direct Connect のアクション、リソース、および条件キー」を参照してください。

Direct Connect アイデンティティベースのポリシーの例については、Direct Connect アイデンティティベースのポリシーの例 を参照してください。

Direct Connect の ACL

ACL のサポート	なし

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

Direct Connect で使用できる ABAC

ABAC (ポリシー内のタグ) のサポート	部分的

属性ベースのアクセスコントロール (ABAC) は、属性に基づいて権限を定義する認可戦略です。AWS では、これらの属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール)、および多数の AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合に操作を許可するように ABAC ポリシーを設計します。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの Condition 要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーのすべてをサポートする場合、そのサービスでのサポート状況の値は「はい」になります。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、『IAM ユーザーガイド』の「ABAC とは?」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、『IAM ユーザーガイド』の「属性に基づくアクセスコントロール (ABAC) を使用する」を参照してください。

Direct Connect での一時的な認証情報の使用

一時的な認証情報のサポート	あり

AWS のサービス には、一時的な認証情報を使用してサインインしても機能しないものがあります。一時的な認証情報で機能する AWS のサービスなどの詳細については、「IAM ユーザーガイド」の「IAM と連携する AWS のサービス」を参照してください。

ユーザー名とパスワード以外の方法で AWS Management Console にサインインする場合は、一時的な認証情報を使用していることになります。例えば、会社の Single Sign-On (SSO) リンクを使用して AWS にアクセスすると、そのプロセスは自動的に一時認証情報を作成します。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、『IAM ユーザーガイド』の「ロールへの切り替え (コンソール)」を参照してください。

一時認証情報は、AWS CLI または AWS API を使用して手動で作成できます。作成後、一時的な認証情報を使用して AWS にアクセスできるようになります。AWS は、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「IAM の一時的なセキュリティ認証情報」を参照してください。

Direct Connect のクロスサービスプリンシパル許可

フォワードアクセスセッション (FAS) をサポート	はい

IAM ユーザーまたはロールを使用して AWSでアクションを実行するユーザーは、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行してから、別のサービスの別のアクションを開始することがあります。FAS は、AWS のサービスを呼び出すプリンシパルのアクセス許可を使用し、リクエスト元の AWS のサービスと組み合わせて、ダウンストリームサービスにリクエストを行います。FAS リクエストは、完了するために他の AWS のサービスまたはリソースとのやり取りを必要とするリクエストをサービスが受信した場合にのみ作成されます。この場合、両方のアクションを実行するための権限が必要です。FASリクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Direct Connect のサービスロール

サービスロールに対するサポート	あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、『IAM ユーザーガイド』の「AWS のサービス に権限を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールの許可を変更すると、Direct Connect の機能が損なわれる可能性があります。Direct Connect が指示する場合以外は、サービスロールを編集しないでください。

Direct Connect のサービスにリンクされたロールの使用

サービスにリンクされたロールのサポート	いいえ

サービスリンクロールは、AWS のサービスにリンクされているサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスリンクロールは、AWS アカウント に表示され、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携する AWS のサービス」を参照してください。表の中から、「サービスにリンクされたロール」列が「Yes」になっているサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

Direct Connect アイデンティティベースのポリシーの例

デフォルトでは、ユーザーおよびロールには、Direct Connect リソースを作成または変更するアクセス許可がありません。また、AWS Management Console、AWS Command Line Interface (AWS CLI)、または AWS API を使用してタスクを実行することもできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。そ

の後、管理者がロールに IAM ポリシーを追加すると、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

Direct Connect が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「サービス認証リファレンス」の「Direct Connect のアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーのベストプラクティス
- Direct Connect のアクション、リソース、および条件
- Direct Connect コンソールの使用
- ユーザーが自分の許可を表示できるようにする
- AWS Direct Connect への読み取り専用アクセス
- AWS Direct Connect へのフルアクセス
- タグベースの条件を使用した Direct Connect アイデンティティベースのポリシーの例

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Direct Connect リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、AWS アカウント に料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS マネージドポリシーを使用して開始し、最小特権の権限に移行する – ユーザーとワークロードへの権限の付与を開始するには、多くの一般的なユースケースのために権限を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケースに応じた AWS カスタマーマネージドポリシーを定義することで、権限をさらに減らすことをお勧めします。詳細については、『IAM ユーザーガイド』の「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定

義します。これは、最小特権権限とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、『IAM ユーザーガイド』の「IAM でのポリシーと権限」を参照してください。

- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。また、AWS CloudFormation などの特定の AWS のサービス を介して使用する場合、条件を使用してサービスアクションへのアクセスを許可することもできます。詳細については、『IAM ユーザーガイド』の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、『IAM ユーザーガイド』の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) を要求する - AWS アカウント内の IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、『IAM ユーザーガイド』の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、『IAM ユーザーガイド』の「IAM でのセキュリティのベストプラクティス」を参照してください。

Direct Connect のアクション、リソース、および条件

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。Direct Connect は、特定のアクション、リソース、および条件キーをサポートしています。JSON ポリシーで使用するすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素のリファレンス」を参照してください。

アクション

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

JSON ポリシーの`Action`要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのない権限のみのアクションなど、いくつかの例外があ

ります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

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

Direct Connect のポリシーアクションでは、アクションの前にプレフィックス `directconnect:` を使用します。たとえば、 Amazon EC2 `DescribeVpnGateways` API オペレーションで Amazon EC2 インスタンスを実行するためのアクセス許可をユーザーに付与するには、ポリシーに `ec2:DescribeVpnGateways` アクションを含めます。ポリシーステートメントには、`Action` または `NotAction` エレメントを含める必要があります。Direct Connect は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

次のポリシーの例では、AWS Direct Connect に読み取りアクセス権限が付与されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

次のポリシーの例では、AWS Direct Connect にフルアクセス権限が付与されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Direct Connect アクションのリストを確認するには、「IAM ユーザーガイド」の「Direct Connect で定義されるアクション」を参照してください。

リソース

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

JSON ポリシーの `Resource` 要素は、アクションが適用される 1 つ以上のオブジェクトを指定します。ステートメントには、`Resource` または `NotResource` 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの権限と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルのアクセス許可をサポートしないアクションの場合は、ワイルドカード (*) を使用して、ステートメントがすべてのリソースに適用されることを示します。

```
"Resource": "*"
```

Direct Connect では、次の ARN を使用します。

Direct Connect リソース ARN

リソースタイプ	ARN
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`

リソースタイプ	ARN
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`

ARN の形式の詳細については、「Amazon リソースネーム (ARN) と AWS サービスの名前空間」を参照してください。

たとえば、ステートメントで dxcon-11aa22bb インターフェイスを指定するには、次の ARN を使用します。

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

特定のアカウントに属するすべての仮想インスタンスを指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

リソースの作成など、一部の Direct Connect アクションは、特定のリソースで実行できません。このような場合は、ワイルドカード (*) を使用する必要があります。

```
"Resource": "*"
```

Direct Connect のリソースタイプとその ARN のリストを確認するには、「IAM ユーザーガイド」の「AWS Direct Connect で定義されるリソースタイプ」を参照してください。各リソースの ARN を指定することができるかアクションについては、「 SERVICE-ACTIONS-URL;」を参照してください。

条件キー

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

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効になる条件を指定できます。Condition 要素はオプションです。equal や less than などの条件演算子を使用して条件式を作成することによって、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、AWS は AND 論理演算子を使用してそれらを評価します。単一の条件キーに複数の値を指定すると、AWS は OR 論理演算子を使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、『IAM ユーザーガイド』の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS はグローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドの「AWS グローバル条件コンテキストキー」を参照してください。

Direct Connect は独自の条件キーを定義し、一部のグローバル条件キーの使用をサポートしています。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドの「AWS グローバル条件コンテキストキー」を参照してください。

タグリソースには条件キーが使用できます。詳細については、「例: 特定のリージョンへのアクセスの制限」を参照してください。

Direct Connect 条件キーのリストを確認するには、「IAM ユーザーガイド」の「Direct Connect の条件キー」を参照してください。条件キーを使用できるアクションおよびリソースについては、「SERVICE-ACTIONS-URL;」を参照してください。

Direct Connect コンソールの使用

Direct Connect コンソールにアクセスするには、最小限のアクセス許可が必要です。これらのアクセス許可により、AWS アカウントの Direct Connect リソースの詳細をリストして表示することが可能になります。最小限必要なアクセス許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

これらのエンティティが引き続き Direct Connect コンソールを使用できるようにするには、エンティティに次の AWS 管理ポリシーもアタッチします。詳細については、IAM ユーザーガイドのユーザーへのアクセス許可の追加を参照してください。

```
directconnect
```

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソール許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーが自分の許可を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI か AWS API を使用してプログラム的に、このアクションを完了するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

AWS Direct Connect への読み取り専用アクセス

次のポリシーの例では、AWS Direct Connect に読み取りアクセス権限が付与されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Direct Connect へのフルアクセス

次のポリシーの例では、AWS Direct Connect にフルアクセス権限が付与されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

タグベースの条件を使用した Direct Connect アイデンティティベースのポリシーの例

リソースおよびリクエストへのアクセスを制御するには、タグキーの条件を使用します。また、IAM ポリシーで条件を使用して、リソースまたはリクエストで特定のタグキーを使用できるかどうかを制御することもできます。

IAM ポリシーでタグを使用する方法については、「IAM ユーザーガイド」の「タグを使用してアクセスを制御する」を参照してください。

タグに基づく Direct Connect 仮想インターフェイスの関連付け

次の例は、タグに環境キーと preprod または production 値が含まれている場合にのみ、仮想インターフェイスを関連付けることを許可するポリシーを作成する方法を示しています。

```
    {
   "Version": "2012-10-17",
   "Statement": [
     {
       "Effect": "Allow",
       "Action": [
         "directconnect:AssociateVirtualInterface"
       ],
       "Resource": "arn:aws:directconnect:*:*:dxvif/*",
       "Condition": {
         "StringEquals": {
           "aws:ResourceTag/environment": [
             "preprod",
             "production"
           ]
         }
       }
     },
     {
       "Effect": "Allow",
       "Action": "directconnect:DescribeVirtualInterfaces",
       "Resource": "*"
     }
   ]
 }
```

タグに基づくリクエストへのアクセスの制御

IAM ポリシーで条件を使用して、AWS リソースをタグ付けするリクエストで渡すことができるタグのキーバリューペアを制御することができます。次の例は、タグに環境キーと preprod または production の値が含まれている場合にのみ、AWS Direct Connect TagResource アクションを使用してタグを仮想インターフェイスにアタッチできるようにするポリシーを作成する方法を示しています。ベストプラクティスとして、ForAllValues 修飾子を aws:TagKeys 条件キーとともに使用して、リクエストでキー環境のみが許可されることを示します。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "directconnect:TagResource",
        "Resource": "arn:aws:directconnect:*:*:dxvif/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/environment": [
                    "preprod",
                    "production"
                ]
            },
            "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
        }
    }
}
```

タグキーの制御

IAM ポリシーで条件を使用して、リソースまたはリクエストで特定のタグキーを使用できるかどうか制御できます。

次の例は、タグキー環境のみを使用して、リソースにタグを付けることを許可するポリシーを作成する方法を示しています。

```
 {
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "directconnect:TagResource",
    "Resource": "*",
```

```
        "Condition": {
          "ForAllValues:StringEquals": {
            "aws:TagKeys": [
              "environment"
            ]
          }
        }
      }
    }
```

AWS Direct Connect のサービスリンクロール

AWS Direct Connect は AWS Identity and Access Management (IAM) サービスリンクロールを使用します。サービスにリンクされたロールは、AWS Direct Connect に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、AWS Direct Connect による事前定義済みのロールであり、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべての許可を備えています。

サービスリンクロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、AWS Direct Connect の設定が簡単になります。AWS Direct Connect は、このサービスリンクロールのアクセス許可を定義します。特に定義されている場合を除き、AWS Direct Connect のみがそのロールを引き受けることができます。定義される許可は、信頼ポリシーと許可ポリシーに含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールを削除するには、まずその関連リソースを削除します。これにより、リソースへの意図しないアクセスによるアクセス許可の削除が防止され、AWS Direct Connect リソースは保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携する AWS のサービス」を参照して、[Service-Linked Role] (サービスにリンクされたロール)列で [Yes] (はい) のあるサービスを探してください。そのサービスに関するサービスにリンクされたロールのドキュメントを表示するには、リンクが設定されている [Yes] (はい) を選択します。

AWS Direct Connect のサービスにリンクされたロールの許可

AWS Direct Connect は、`AWSServiceRoleForDirectConnect` という名前のサービスリンクロールを使用します。これは、AWS Direct Connect が、AWS Secrets Manager に保存されている MACSec シークレットをユーザーに代わって取得できるようにします。

`AWSServiceRoleForDirectConnect` サービスにリンクされたロールは、ロールの引き受けについて以下のサービスを信頼します。

- directconnect.amazonaws.com

AWSServiceRoleForDirectConnect サービスにリンクされたロールは、マネージドポリシーである AWSDirectConnectServiceRolePolicy を使用します。

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、許可を設定する必要があります。AWSServiceRoleForDirectConnect サービスリンクロールが適切に作成されるようにするには、AWS Direct Connect で使用する IAM アイデンティティに必要な許可が付与されている必要があります。必要な許可を付与するには、次のポリシーを IAM アイデンティティにアタッチします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "directconnect.amazonaws.com"
                }
            },
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:GetRole",
            "Effect": "Allow",
            "Resource": "*"
       }
    ]
}
```

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アクセス許可」を参照してください。

AWS Direct Connect のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。AWS Direct Connect がユーザーに代わってサービスリンクロールを作成します。associate-mac-sec-key コマンドを実行すると、AWS は、AWS Direct Connect が AWS Management Console、AWS CLI、または AWS API を

使用して、AWS Secrets Manager に保存されている MACsec シークレットをユーザーに代わって取得できるようにするサービスリンクロールを作成します。

> **Important**
>
> このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。詳細については、「IAM アカウントに表示される新しいロール」を参照してください。

このサービスにリンクされたロールを削除した後で再度作成する必要が生じた場合にも、アカウントでのロールの再作成は同様な方法で行えます。サービスにリンクされたロールが、AWS Direct Connect により自動的に作成されます。

IAM コンソールを使用して、AWS Direct Connect ユースケースでのサービスリンクロールを作成することもできます。AWS CLI または AWS API で、サービスにリンクされたロールをサービス名 (`directconnect.amazonaws.com`) で作成します。詳細については、IAM ユーザーガイドの「サービスリンクロールの作成」を参照してください。このサービスにリンクされたロールを削除する場合、この同じプロセスを使用して、もう一度ロールを作成できます。

のサービスにリンクされたロールの編集AWS Direct Connect

AWS Direct Connect では、`AWSServiceRoleForDirectConnect` のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、IAM ユーザーガイドの「サービスリンクロールの編集」を参照してください。

AWS Direct Connect のサービスにリンクされたロールの削除

`AWSServiceRoleForDirectConnect` ロールを手動で削除する必要はありません。サービスリンクロールを削除するときは、AWS Secrets Manager ウェブサービスに保存されているすべての関連リソースを削除する必要があります。AWS Management Console、AWS CLI、 AWS API、または AWS Direct Connect がユーザーに代わってリソースをクリーンアップし、サービスリンクロールを削除します。

サービスリンクロールは、IAM コンソールを使用して削除することもできます。これを実行するには、まずサービスリンクロールのリソースをクリーンアップする必要があります。その後、サービスリンクロールを手動で削除することができます。

> **Note**
>
> リソースの削除試行時に AWS Direct Connect サービスがサービスリンクロールを使用している場合は、削除が失敗する可能性があります。失敗した場合は、数分待ってから操作を再試行してください。

`AWSServiceRoleForDirectConnect` で使用されている AWS Direct Connect リソースを削除するには

1. すべての MACsec キーと接続間の関連付けを削除します。詳細については、「the section called “MACsec シークレットキーと接続の間の関連付けを解除する”」を参照してください
2. すべての MACsec キーと LAG 間の関連付けを削除します。詳細については、「the section called “MACsec シークレットキーと LAG の間の関連付けを解除する”」を参照してください

IAM を使用してサービスリンクロールを手動で削除するには

IAM コンソール、AWS CLI、または AWS API を使用して、`AWSServiceRoleForDirectConnect` サービスリンクロールを削除します。詳細については、IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

AWS Direct Connect のサービスにリンクされたロールをサポートするリージョン

AWS Direct Connect は、MAC セキュリティ機能が利用可能になっているすべての AWS リージョンでサービスリンクロールの使用をサポートしています。詳細については、「AWS Direct Connect ロケーション」を参照してください。

AWS の AWS Direct Connect マネージドポリシー

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権の権限を付与しない場合があることにご注意ください。AWS のすべてのお客様が使用できるようになるのを避けるためです。ユースケース別にカスタマー管理ポリシーを定義することで、権限を絞り込むことをお勧めします。

AWS マネージドポリシーで定義したアクセス権限は変更できません。AWS が AWS マネージドポリシーに定義されている権限を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービスを起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS 管理ポリシー: AWSDirectConnectFullAccess

`AWSDirectConnectFullAccess` ポリシーは IAM アイデンティティにアタッチできます。このポリシーは、AWS Direct Connect への完全なアクセスを可能にする許可を付与します。

このポリシーの許可を確認するには、AWS Management Console の「AWSDirectConnectFullAccess」を参照してください。

AWS 管理ポリシー: AWSDirectConnectReadOnlyAccess

`AWSDirectConnectReadOnlyAccess` ポリシーは IAM アイデンティティにアタッチできます。このポリシーは、AWS Direct Connect への読み取り専用アクセスを可能にする許可を付与します。

このポリシーの許可を確認するには、AWS Management Console の「AWSDirectConnectReadOnlyAccess」を参照してください。

AWS 管理ポリシー: AWSDirectConnectServiceRolePolicy

このポリシーは、AWS Direct Connect がユーザーに代わって MAC Security シークレットを取得できるように、AWSserviceRoleForDirectConnect という名前のサービスリンクロースにアタッチされます。詳細については、「the section called “サービスにリンクされたロール”」を参照してください。

このポリシーの許可を確認するには、AWS Management Console の「AWSDirectConnectServiceRolePolicy」を参照してください。

AWS Direct Connect 管理ポリシーの AWS 更新

このサービスがこれらの変更の追跡を開始してからの、AWS Direct Connect 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。このページの変更に関する自動通知については、[AWS Direct ConnectDocument history (ドキュメントの履歴)] ページの RSS フィードをサブスクライブしてください。

変更	説明	日付
AWSDirectConnectServiceRolePolicy - 新しいポリシー	MAC Security をサポートするため、AWSServiceRoleForDirectConnect が追加されました。	2021 年 3 月 31 日
AWS Direct Connect は変更の追跡を開始しました	AWS Direct Connect が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 3 月 31 日

Direct Connect のアイデンティティとアクセスのトラブルシューティング

次の情報は、Direct Connect と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- Direct Connect でアクションを実行する権限がない
- I am not authorized to perform iam:PassRole
- AWS アカウント アカウント外のユーザーに Direct Connect リソースへのアクセスを許可したい

Direct Connect でアクションを実行する権限がない

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次の例は、mateojackson という IAM ユーザーがコンソールを使用して架空の *my-example-widget* リソースに関する詳細を表示しようとしたとき、架空の directconnect:*GetWidget* アクセス許可がない場合に発生するエラーを示しています。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 directconnect:GetWidget on resource: my-example-widget
```

この場合、directconnect:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。管理者とは、サインイン認証情報を提供した担当者です。

I am not authorized to perform iam:PassRole

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Direct Connect にロールを渡せるようにする必要があります。

一部の AWS のサービスでは、新しいサービスロールやサービスリンクロールを作成せずに、既存のロールをサービスに渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、`marymajor` という IAM ユーザーがコンソールを使用して Direct Connect でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。Mary には、ロールをサービスに渡す権限がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新して、Mary に `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。管理者とは、サインイン認証情報を提供した担当者です。

AWS アカウント アカウント外のユーザーに Direct Connect リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセス制御リスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください。

- Direct Connect がこれらの機能をサポートしているかどうかについては、「Direct Connect が IAM と連携する仕組み」を参照してください。
- 所有している AWS アカウント 全体のリソースへのアクセス権を提供する方法については、『IAM ユーザーガイド』の「所有している別の AWS アカウント アカウントへのアクセス権を IAM ユーザーに提供」を参照してください。

- サードパーティーの AWS アカウント にリソースへのアクセス権を提供する方法については、『IAM ユーザーガイド』の「第三者が所有する AWS アカウント へのアクセス権を付与する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、『IAM ユーザーガイド』の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

AWS Direct Connectでのログ記録とモニタリング

以下の自動化されたモニタリングツールを使用して、AWS Direct Connect を監視し、問題が発生したときにレポートできます。

- Amazon CloudWatch アラーム – 指定した期間にわたって 1 つのメトリクスを確認できます。このアラームは、複数の期間にわたる一定のしきい値とメトリクスの値の関係性に基づき、1 つ以上のアクションを実行します。アクションは、Amazon SNS トピックに送信される通知です。CloudWatch のアラームは、メトリクスが特定の状態になっただけではアクションを呼び出しません。アクションを呼び出すには、状態が変化して、指定した期間継続している必要があります。詳細については、「Amazon によるモニタリング CloudWatch」を参照してください。
- AWS CloudTrail ログモニタリング – CloudWatch Logs に送信することで、アカウント間でログファイルを共有し、CloudTrail ログファイルをリアルタイムで監視します。ログ処理アプリケーションを Java で記述し、CloudTrail で配信後にログファイルが変更されていないことを検証することもできます。詳細については、「AWS Direct Connect を使用した AWS CloudTrail API コールのログ記録」と、AWS CloudTrail ユーザーガイドの「CloudTrail ログファイルの操作」を参照してください。

詳細については、「モニタリング」を参照してください。

のコンプライアンス検証 AWS Direct Connect

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。
- Amazon GuardDuty — これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワーク

で義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。

- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

AWS Direct Connect での耐障害性

AWS のグローバルインフラストラクチャは AWS リージョンとアベイラビリティーゾーンを中心に構築されます。AWSリージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立し隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、および拡張性が優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

AWS では、AWS Direct Connect グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズに対応できるように複数の機能を提供しています。

AWS Direct Connect で VPN を使用する方法については、AWS Direct Connect Plus VPN を参照してください。

フェイルオーバー

AWS Direct Connect Resiliency Toolkit は、SLA 目標を達成するための専用接続の注文に役立つ、複数の回復性モデルを備えた接続ウィザードを提供します。回復性モデルを選択すると、AWS Direct Connect Resiliency Toolkit が専用接続を注文するプロセスを案内します。回復性モデルは、複数の場所で適切な数の専用接続を確保するように設計されています。

- 最大回復性: クリティカルなワークロードに対し、複数の場所にある別々のデバイスを終端とする別々の接続を使用することで最大限の回復性を実現できます。このモデルは、デバイス、接続、ロケーション全体の障害に対する回復性を提供します。
- 高い回復性: クリティカルなワークロードに対し、複数の場所につながる 2 つの単一接続を使用することで、高い回復性を実現できます。このモデルは、ファイバーの切断やデバイスの障害に起因する接続障害に対し、回復性を提供します。また、ロケーション全体の障害を防ぐのに役立ちます。

- 開発とテスト: クリティカルでないワークロードの開発とテストの回復性を実現するには、1 つの場所にある別々のデバイスを終端とする別々の接続を使用します。このモデルは、デバイスの障害に対する回復性を提供しますが、ロケーションの障害に対する回復性は提供しません。

詳細については、「Resiliency Toolkit AWS Direct Connect を使用して開始する」を参照してください。

AWS Direct Connect でのインフラストラクチャセキュリティ

マネージドサービスである AWS Direct Connect は AWS グローバルネットワークセキュリティ手順で保護されています。AWS が公開している API コールを使用して、ネットワーク経由で AWS Direct Connect にアクセスします。クライアントで Transport Layer Security (TLS) 1.2 以降がサポートされている必要があります。TLS 1.3 をお勧めします。また、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストは、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時セキュリティ認証情報を生成し、リクエストに署名することもできます。

これらの API オペレーションは任意のネットワークの場所から呼び出すことができますが、AWS Direct Connect ではリソースベースのアクセスポリシーがサポートされています。これには送信元 IP アドレスに基づく制限を含めることができます。また、AWS Direct Connect ポリシーを使用して、特定の Amazon Virtual Private Cloud (Amazon VPC) エンドポイントまたは特定の VPC からのアクセスを制御することもできます。これにより、実質的に AWS ネットワーク内の特定の VPC からの特定の AWS Direct Connect リソースへのネットワークアクセスが分離されます。例については、「the section called “アイデンティティベースポリシーの例”」を参照してください。

ボーダーゲートウェイプロトコル (BGP) セキュリティ

インターネットは、ネットワークシステム間で情報をルーティングするために BGP に大きく依存しています。BGP ルーティングは、悪意のある攻撃や BGP ハイジャックの影響を受けることがあります。AWS がネットワークを BGP ハイジャックからより安全に保護する方法を理解するには、「AWS がインターネットルーティングの保護に役立っている方法」を参照してください。

AWS CLI の使用

AWS CLI を使用して AWS Direct Connect リソースを作成し、操作できます。

以下の例では、AWS CLI コマンドを使用して、AWS Direct Connect 接続を作成します。また、Letter of Authorization and Connecting Facility Assignment (LOA-CFA) をダウンロードしたり、プライベートまたはパブリック仮想インターフェイスをプロビジョニングしたりすることもできます。

開始する前に、AWS CLI がインストールされ、設定されていることを確認します。詳細については、AWS Command Line Interface ユーザーガイドを参照してください。

目次

ステップ 1: 接続を作成する

最初のステップでは、接続リクエストを送信します。必要なポート速度と AWS Direct Connect ロケーションがわかっていることを確認します。詳細については、「AWS Direct Connect 接続」を参照してください。

接続リクエストを作成するには

1. 現在のリージョンの AWS Direct Connect ロケーションについて説明します。返される出力で、接続を確立するロケーションのロケーションコードを書き留めます。

```
aws directconnect describe-locations
```

```
{
    "locations": [
        {
            "locationName": "City 1, United States",
            "locationCode": "Example Location 1"
        },
        {
```

```
            "locationName": "City 2, United States",
            "locationCode": "Example location"
        }
    ]
}
```

2. 接続を作成し、名前、ポート速度、およびロケーションコードを指定します。返される出力で、接続 ID を書き留めます。次のステップで LOA-CFA を取得するには、この ID が必要になります。

```
aws directconnect create-connection --location Example location --bandwidth 1Gbps
 --connection-name "Connection to AWS"
```

```
{
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-EXAMPLE",
    "connectionState": "requested",
    "bandwidth": "1Gbps",
    "location": "Example location",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

ステップ 2: LOA-CFA をダウンロードする

接続をリクエストした後、describe-loa コマンドを使用して LOA-CFA を取得できます。出力は base64 でエンコードされます。関連する LOA コンテンツを抽出し、デコードして、PDF ファイルを作成する必要があります。

Linux または macOS を使用して LOA-CFA を取得するには

この例では、コマンドの最後の部分で base64 ユーティリティを使用してコンテンツをデコードし、出力を PDF ファイルに送信します。

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

Windows を使用して LOA-CFA を取得するには

この例では、出力は myLoaCfa.base64 というファイルに解凍されます。2 番目のコマンドでは、certutil ユーティリティを使用してファイルをデコードし、PDF ファイルに出力を送信します。

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

LOA-CFA をダウンロードした後、ネットワークプロバイダーまたはコロケーションプロバイダーに送信します。

ステップ 3: 仮想インターフェイスを作成し、ルーター設定を取得する

AWS Direct Connect 接続を申し込んだ後、その接続の使用を開始するために仮想インターフェイスを作成する必要があります。プライベート仮想インターフェイスを作成して、VPC に接続することができます。または、VPC 外の AWS のサービスに接続するパブリック仮想インターフェイスを作成することもできます。IPv4 または IPv6 トラフィックをサポートする仮想インターフェイスを作成できます。

開始する前に、必ず「仮想インターフェイスの前提条件」の前提条件を参照してください。

AWS CLI を使用して仮想インターフェイスを作成すると、出力には汎用的なルーター設定情報が含まれます。デバイスに固有のルーター設定を作成するには、AWS Direct Connect コンソールを使用します。詳細については、「ルーター設定ファイルをダウンロードする」を参照してください。

プライベート仮想インターフェイスを作成するには

1. VPC にアタッチされた仮想プライベートゲートウェイの ID (vgw-xxxxxxxx) を取得します。次のステップで仮想インターフェイスを作成するために、この ID が必要になります。

   ```
   aws ec2 describe-vpn-gateways
   ```

   ```
   {
       "VpnGateways": [
           {
               "State": "available",
   ```

```
            "Tags": [
                {
                    "Value": "DX_VGW",
                    "Key": "Name"
                }
            ],
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-ebaa27db",
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-24f33d4d"
                }
            ]
        }
    ]
}
```

2. プライベート仮想インターフェイスを作成します。名前、VLAN ID、および BGP 自律システム番号 (ASN) を指定する必要があります。

   IPv4 トラフィックの場合、BGP ピアリングセッションの両側にプライベート IPv4 アドレスが必要です。独自の IPv4 アドレスを指定するか、このアドレスを自動的に生成できます。次の例では、IPv4 アドレスが自動的に生成されます。

```
aws directconnect create-private-virtual-interface --
connection-id dxcon-fg31dyv6 --new-private-virtual-interface
 virtualInterfaceName=PrivateVirtualInterface,vlan=101,asn=65000,virtualGatewayId=vgw-
ebaa27db,addressFamily=ipv4
```

```
{
    "virtualInterfaceState": "pending",
    "asn": 65000,
    "vlan": 101,
    "customerAddress": "192.168.1.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "vgw-ebaa27db",
    "virtualInterfaceId": "dxvif-ffhhk74f",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [],
```

```
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "192.168.1.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "pending",
            "amazonAddress": "192.168.1.1/30",
            "asn": 65000
        }
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-ffhhk74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>private</connection_type>\n</
logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "PrivateVirtualInterface"
}
```

IPv6 トラフィックをサポートするプライベート仮想インターフェイスを作成するには、上記と同じコマンドを使用して、ipv6 パラメーターに addressFamily を指定します。BGP ピアセッションに独自の IPv6 アドレスを指定することはできません。IPv6 アドレスは自動的に割り当てられます。

3. ルーター設定情報を XML 形式で表示するには、作成した仮想インターフェイスについて説明します。--query パラメーターを使用して customerRouterConfig 情報を抽出し、--output パラメーターを使用してテキストをタブ区切り行に整理します。

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-ffhhk74f
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhhk74f">
  <vlan>101</vlan>
  <customer_address>192.168.1.2/30</customer_address>
  <amazon_address>192.168.1.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
```

```
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>private</connection_type>
</logical_connection>
```

パブリック仮想インターフェイスを作成するには

1. パブリック仮想インターフェイスを作成するには、名前、VLAN ID、および BGP 自律システム番号 (ASN) を指定する必要があります。

   IPv4 トラフィックの場合は、BGP ピア接続の両端にパブリック IPv4 アドレスと、BGP 経由でアドバタイズするパブリック IPv4 ルートを指定する必要もあります。次の例では、IPv4 トラフィック用のパブリック仮想インターフェイスを作成します。

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/
{cidr=203.0.113.4/30}]
```

```
{
    "virtualInterfaceState": "verifying",
    "asn": 65000,
    "vlan": 2000,
    "customerAddress": "203.0.113.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "",
    "virtualInterfaceId": "dxvif-fgh0hcrk",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [
        {
            "cidr": "203.0.113.0/30"
        },
        {
            "cidr": "203.0.113.4/30"
        }
    ],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
```

```
            "customerAddress": "203.0.113.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "verifying",
            "amazonAddress": "203.0.113.1/30",
            "asn": 65000
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>public</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

IPv6 トラフィックをサポートするパブリック仮想インターフェイスを作成するには、BGP 経由でアドバタイズする IPv6 ルートを指定できます。ピアセッションに独自の IPv6 アドレスを指定することはできません。IPv6 アドレスは自動的に割り当てられます。次の例では、IPv6 トラフィック用のパブリック仮想インターフェイスを作成します。

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,addressFamily=ipv6,routeFi
{cidr=2001:db8:64ce:ba01::/64}]
```

2. ルーター設定情報を XML 形式で表示するには、作成した仮想インターフェイスについて説明します。--query パラメーターを使用して customerRouterConfig 情報を抽出し、--output パラメーターを使用してテキストをタブ区切り行に整理します。

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-fgh0hcrk
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-fgh0hcrk">
  <vlan>2000</vlan>
```

```
  <customer_address>203.0.113.2/30</customer_address>
  <amazon_address>203.0.113.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>public</connection_type>
</logical_connection>
```

AWS Direct Connect を使用した AWS CloudTrail API コールのログ記録

AWS Direct Connect は AWS CloudTrail と統合されています。このサービスは、ユーザーやロール、または AWS の AWS Direct Connect 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。CloudTrail は、AWS Direct Connect のすべての API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、AWS Direct Connect コンソールの呼び出しと、AWS Direct Connect 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、AWS Direct Connect のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます 証跡を設定しない場合でも、CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、AWS Direct Connect に対するリクエスト、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。

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

AWS Direct ConnectCloudTrail での 情報

CloudTrail は、アカウントを作成すると AWS アカウントで有効になります。AWS Direct Connect でアクティビティが発生すると、そのアクティビティは [Event history (イベント履歴)] で AWS のその他のサービスのイベントと共に CloudTrail イベントに記録されます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

AWS のイベントなど、AWS Direct Connect アカウントのイベントの継続的なレコードについては、追跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべての AWS リージョンに適用されます。追跡は、AWSパーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS のサービスを設定できます。詳細については、次を参照してください。

- 追跡を作成するための概要
- CloudTrail のサポート対象サービスと統合
- Amazon SNS の CloudTrail の通知の設定

- 複数のリージョンから CloudTrail ログファイルを受け取る、および複数のアカウントから CloudTrail ログファイルを受け取る

すべての AWS Direct Connect アクションは CloudTrail によってログに記録され、AWS Direct Connect API リファレンスに記録されます。例えば、`CreateConnection` および `CreatePrivateVirtualInterface` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。同一性情報は次の判断に役立ちます。

- リクエストが、ルートまたは AWS Identity and Access Management (IAM ユーザー) の認証情報で作成されたかどうか。
- 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一時的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 サービスによって送信されたかどうか。

詳細については、CloudTrail `userIdentity` 要素を参照してください。

AWS Direct Connect ログファイルエントリの概要

追跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、単一か複数のログエントリがあります。イベントはあらゆる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、リクエストのパラメータなどの情報が含まれます。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。

以下は、AWS Direct Connect の CloudTrail ログレコードの例です

Example 例: CreateConnection

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
```

```
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:28:16Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "location": "EqSE2",
            "connectionName": "MyExampleConnection",
            "bandwidth": "1Gbps"
        },
        "responseElements": {
            "location": "EqSE2",
            "region": "us-west-2",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-fhajolyy",
            "connectionName": "MyExampleConnection"
        }
    },
    ...
  ]
}
```

Example 例: CreatePrivateVirtualInterface

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
```

```
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
                "customerAddress": "[PROTECTED]",
                "authKey": "[PROTECTED]",
                "asn": -1,
                "virtualGatewayId": "vgw-bb09d4a5",
                "amazonAddress": "[PROTECTED]",
                "vlan": 123
            }
        },
        "responseElements": {
            "virtualInterfaceId": "dxvif-fgq61m6w",
            "authKey": "[PROTECTED]",
            "virtualGatewayId": "vgw-bb09d4a5",
            "customerRouterConfig": "[PROTECTED]",
            "virtualInterfaceType": "private",
            "asn": -1,
            "routeFilterPrefixes": [],
            "virtualInterfaceName": "MyVirtualInterface",
            "virtualInterfaceState": "pending",
            "customerAddress": "[PROTECTED]",
            "vlan": 123,
            "ownerAccount": "123456789012",
```

```
            "amazonAddress": "[PROTECTED]",
            "connectionId": "dxcon-fhajolyy",
            "location": "EqSE2"
        }
    },
    ...
  ]
}
```

Example 例: DescribeConnections

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:27:28Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeConnections",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": null,
        "responseElements": null
    },
    ...
  ]
}
```

Example 例: DescribeVirtualInterfaces


```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:37:53Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeVirtualInterfaces",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy"
        },
        "responseElements": null
    },
    ...
  ]
}
```

AWS Direct Connect リソースのモニタリング

モニタリングは、Direct Connect リソースの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、 AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。ただし、Direct Connect のモニタリングを開始する前に、以下の質問に対する回答を反映したモニタリング計画を作成する必要があります。

- どのような目的でモニタリングしますか?
- どのようなリソースをモニタリングする必要がありますか?
- これらのリソースをモニタリングする頻度は?
- 使用できるモニタリングツールは?
- 誰がモニタリングタスクを実行しますか?
- 問題が発生したときに誰が通知を受け取りますか?

次のステップでは、さまざまなタイミングと負荷条件でパフォーマンスを測定することにより、お客様の環境で通常の Direct Connect パフォーマンスのベースラインを確立します。Direct Connect をモニタリングするときは、過去のモニタリングデータを保存します。保存すれば、パフォーマンスデータをこの過去のデータと比較して、通常のパフォーマンスパターンとパフォーマンス異常を識別することで、問題の対処方法を考案しやすくなります。

ベースラインを確立するには、物理的な Direct Connect 接続の使用状況、状態、ヘルス状態をモニタリングする必要があります。

コンテンツ

モニタリングツール

AWS には、 AWS Direct Connect 接続のモニタリングに使用できるさまざまなツールが用意されています。これらのツールの一部はモニタリングを行うように設定できますが、一部のツールは手動による介入が必要です。モニタリングタスクをできるだけ自動化することをお勧めします。

自動モニタリングツール

次の自動モニタリングツールを使用して、Direct Connect を監視し、問題が発生したときにレポートできます。

- Amazon CloudWatch アラーム – 指定した期間にわたって 1 つのメトリクスを監視します。このアラームは、複数の期間にわたる一定のしきい値とメトリクスの値の関係性に基づき、1 つ以上のアクションを実行します。アクションは、Amazon SNS topic. CloudWatch alarms に送信される通知です。アクションは、単に特定の状態にあるというだけでは呼び出されません。状態が変わり、それが指定された期間にわたって持続している必要があります。利用可能なメトリクスとディメンションの詳細については、Amazon によるモニタリング CloudWatch を参照してください。
- AWS CloudTrail ログのモニタリング – アカウント間でログファイルを共有し、 CloudWatch ログに送信してリアルタイムで CloudTrail ログファイルを監視します。ログ処理アプリケーションを Java で記述し、 CloudTrail で配信後にログファイルが変更されていないことを検証することもできます。詳細については、AWS Direct Connect を使用した AWS CloudTrail API コールのログ記録「」および「 ユーザーガイド」の CloudTrail 「ログファイルの操作AWS CloudTrail 」を参照してください。

手動モニタリングツール

AWS Direct Connect 接続のモニタリングでもう 1 つ重要な点は、 CloudWatch アラームの対象外の項目を手動でモニタリングすることです。Direct Connect と CloudWatchコンソールのダッシュボードには、環境の状態 at-a-glance AWS が表示されます。

- AWS Direct Connect コンソールには以下が表示されます。
  - 接続のステータス ([State] 列を参照)
  - 仮想インターフェイスのステータス ([State] 列を参照)
- CloudWatch ホームページには以下が表示されます。
  - 現在のアラームとステータス
  - アラームとリソースのグラフ
  - サービスのヘルスステータス

  さらに、 CloudWatch を使用して次の操作を実行できます。
  - 重要なサービスをモニタリングするためにカスタマイズされたダッシュボードを作成する。
  - メトリクスデータをグラフ化して、問題のトラブルシューティングを行い、傾向を確認する。

- すべての AWS リソースメトリクスを検索して参照します。
- 問題があることを通知するアラームを作成および編集する。

Amazon によるモニタリング CloudWatch

を使用して、物理 AWS Direct Connect 接続と仮想インターフェイスをモニタリングできます CloudWatch。 CloudWatch は Direct Connect から raw データを収集し、読み取り可能なメトリクスに処理します。デフォルトでは、 は Direct Connect メトリクスデータを 5 分間隔で CloudWatch 提供します。

の詳細については CloudWatch、「Amazon CloudWatch ユーザーガイド」を参照してください。サービスをモニタリング CloudWatch して、リソースを使用しているサービスを確認することもできます。詳細については、AWS CloudWatch 「メトリクスを発行する のサービス」を参照してください。

コンテンツ

AWS Direct Connect メトリクスとディメンション

メトリクスは、 AWS Direct Connect 物理接続と仮想インターフェイスで使用できます。

AWS Direct Connect 接続メトリクス

以下のメトリクスは、Direct Connect 専用接続から入手できます。

メトリクス	説明
`ConnectionState`	接続の状態。1 はアップ、0 はダウンを示します。 このメトリクスは、専用接続とホスト接続で使用できます。

メトリクス	説明
	Note このメトリクスは、接続所有者アカウントに加えて、ホストされている仮想インターフェイス所有者アカウントでも使用できます。 単位: ブール
ConnectionBpsEgress	接続の AWS 側から送信されるデータのビットレート。 報告される数値は、指定した時間長 (デフォルトは 5 分、最低 1 分) にわたる集計 (平均) です。デフォルトの集計は変更できます。 このメトリクスは、新しい接続やデバイスの再起動時には使用できない場合があります。メトリクスは、接続を使用してトラフィックの送受信を行うときに開始されます。 単位: ビット/秒
ConnectionBpsIngress	接続の AWS 側に受信されるデータのビットレート。 このメトリクスは、新しい接続やデバイスの再起動時には使用できない場合があります。メトリクスは、接続を使用してトラフィックの送受信を行うときに開始されます。 単位: ビット/秒

メトリクス	説明
ConnectionPpsEgress	接続の AWS 側から送信されるデータのパケットレート。 報告される数値は、指定した時間長 (デフォルトは 5 分、最低 1 分) にわたる集計 (平均) です。デフォルトの集計は変更できます。 このメトリクスは、新しい接続やデバイスの再起動時には使用できない場合があります。メトリクスは、接続を使用してトラフィックの送受信を行うときに開始されます。 単位: パケット/秒
ConnectionPpsIngress	接続の AWS 側に受信されるデータのパケットレート。 報告される数値は、指定した時間長 (デフォルトは 5 分、最低 1 分) にわたる集計 (平均) です。デフォルトの集計は変更できます。 このメトリクスは、新しい接続やデバイスの再起動時には使用できない場合があります。メトリクスは、接続を使用してトラフィックの送受信を行うときに開始されます。 単位: パケット/秒
ConnectionCRCErrorCount	このカウントはもう使用されていません。代わりに ConnectionErrorCount を使用します。

メトリクス	説明
ConnectionErrorCount	AWS デバイス上のすべてのタイプの MAC レベルエラーの合計エラー数。この合計には、巡回冗長検査 (CRC) エラーが含まれます。 このメトリクスは、最後にレポートされたデータポイント以降に発生したエラー数です。インターフェイスにエラーがある場合、メトリクスはゼロ以外の値を報告します。5 分など CloudWatch、 で選択した間隔のすべてのエラーの合計数を取得するには、「合計」統計を適用します。合計統計の取得の詳細については、「Amazon CloudWatch ユーザーガイド」の「メトリクスの統計の取得」を参照してください。 インターフェイスのエラーが停止すると、メトリクス値は 0 に設定されます。 **Note** このメトリクスは、現在使用されていない ConnectionCRCErrorCount に置き換わります。 単位: カウント
ConnectionLightLevelTx	接続の AWS 側からのアウトバウンド (出力) トラフィックのファイバー接続の正常性を示します。 このメトリクスには 2 つのディメンションがあります。詳細については、「the section called “AWS Direct Connect 使用可能なディメンション”」を参照してください。 単位: dBm

メトリクス	説明
ConnectionLightLevelRx	接続の AWS 側へのインバウンド (入力) トラフィックのファイバー接続の正常性を示します。 このメトリクスには 2 つのディメンションがあります。詳細については、「the section called “AWS Direct Connect 使用可能なディメンション”」を参照してください。 単位: dBm
ConnectionEncryptionState	1 は接続の暗号化が up であることを示し、0 は接続の暗号化が down であることを示します。このメトリクスが LAG に適用される場合、1 は LAG 内のすべての接続の暗号化が up であることを示し、0 は少なくとも 1 つの LAG 接続の暗号化が down であることを示します。

AWS Direct Connect 仮想インターフェイスのメトリクス

以下のメトリクスは、 AWS Direct Connect 仮想インターフェイスから使用できます。

メトリクス	説明
VirtualInterfaceBpsEgress	仮想インターフェイスの AWS 側から送信されるデータのビットレート。 報告される数値は、指定した時間長 (デフォルトは 5 分) にわたる集計 (平均) です。 単位: ビット/秒
VirtualInterfaceBpsIngress	仮想インターフェイスの AWS 側に受信されるデータのビットレート。 報告される数値は、指定した時間長 (デフォルトは 5 分) にわたる集計 (平均) です。

メトリクス	説明
	単位: ビット/秒
VirtualInterfacePpsEgress	仮想インターフェイスの AWS 側から送信されるデータのパケットレート。 報告される数値は、指定した時間長 (デフォルトは 5 分) にわたる集計 (平均) です。 単位: パケット/秒
VirtualInterfacePpsIngress	仮想インターフェイスの AWS 側に受信されるデータのパケットレート。 報告される数値は、指定した時間長 (デフォルトは 5 分) にわたる集計 (平均) です。 単位: パケット/秒

AWS Direct Connect 使用可能なディメンション

次のディメンションを使用して AWS Direct Connect データをフィルタリングできます。

ディメンション	説明
ConnectionId	このディメンションは、Direct Connect 接続と仮想インターフェイスのメトリクスで使用できます。このディメンションでは、接続でデータをフィルターします。
OpticalLaneNumber	このディメンションは、ConnectionLightLevelTx データとConnectionLightLevelRx データをフィルタリングし、Direct Connect 接続の光車線番号でデータをフィルタリングします。
VirtualInterfaceId	このディメンションは Direct Connect 仮想インターフェイスのメトリクスで使用でき、仮想インターフェイスでデータをフィルタリングします。

AWS Direct Connect CloudWatch メトリクスの表示

AWS Direct Connect は、Direct Connect 接続に関する次のメトリクスを送信します。次に、Amazon CloudWatch はこれらのデータポイントを 1 分または 5 分間隔で集計します。デフォルトでは、Direct Connect メトリクスデータは 5 分間隔で CloudWatch に書き込まれます。

> **Note**
>
> 1 分間隔を設定すると、Direct Connect は、この間隔 CloudWatch を使用してメトリクスをに書き込むよう最善を尽くしますが、必ずしも保証できるとは限りません。

次の手順を使用して、Direct Connect 接続のメトリクスを表示できます。

CloudWatch コンソールを使用してメトリクスを表示するには

メトリクスはまずサービスの名前空間ごとにグループ化され、次に各名前空間内のさまざまなディメンションの組み合わせごとにグループ化されます。数学関数や事前構築されたクエリの追加など、 Amazon CloudWatch を使用して Direct Connect メトリクスを表示する方法の詳細については、「Amazon CloudWatch ユーザーガイド」の Amazon CloudWatch「メトリクスの使用」を参照してください。

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[Metrics] (メトリクス)、[All metrics] (すべてのメトリクス) の順に選択します。
3. [Metrics] (メトリクス) セクションで、DX を選択します。
4. ConnectionId またはメトリクス名 を選択し、次のいずれかを選択してメトリクスをさらに定義します。

   - [Add to search] (検索に追加) - このメトリクスを検索結果に追加します。
   - [Search for this only] (これのみ検索) - このメトリクスのみを検索します。
   - [Remove from graph] (グラフから削除) - このメトリクスをグラフから削除します。
   - [Graph this metric only] (このメトリクスのみをグラフ化) - このメトリクスのみをグラフ化します。
   - [Graph all search results] (すべての検索結果をグラフ化) - すべてのメトリクスをグラフ化します。

- [Graph with SQL query] (SQL クエリ付きグラフ) - [Metric Insights -query builder] (Metric Insights クエリビルダー) を開きます。SQL クエリを作成して、グラフにする対象を選択できます。Metric Insights の使用の詳細については、「Amazon CloudWatch ユーザーガイド」の CloudWatch 「Metrics Insights を使用してメトリクスをクエリする」を参照してください。

AWS Direct Connect コンソールを使用してメトリクスを表示するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Connections (接続)] を選択します。
3. 接続を選択します。
4. [モニタリング] タブを接続して、接続のメトリクスを表示します。

を使用してメトリクスを表示するには AWS CLI

コマンドプロンプトで、次のコマンドを使用します。

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```

CloudWatch アラームを作成して AWS Direct Connect 接続をモニタリングする

CloudWatch アラームの状態が変わったときに Amazon SNS メッセージを送信するアラームを作成できます。1 つのアラームで、指定した期間中、1 つのメトリクスを監視します。このアラームは、複数の期間にわたる一定のしきい値とメトリクスの値の関係性に基づき、Amazon SNS トピックに通知を送信します。

たとえば、 AWS Direct Connect 接続の状態を監視するアラームを作成できます。接続状態が 5 回連続して 1 分間ダウンとなったときに、通知を送信します。アラームの作成について知っておくべきこと、およびアラームの作成の詳細については、「Amazon ユーザーガイド」の「Amazon CloudWatch アラームの使用」を参照してください。 CloudWatch

CloudWatch アラームを作成するには。

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[Alarms] (アラーム) を選択し、[All alarms] (アラームの作成) を選択します。

3. [アラームの作成] を選択します。
4. [Select metric] (メトリクスの選択)、DX の順に選択します。
5. [Connection Metrics] (接続メトリクス) メトリクスを選択します。
6. AWS Direct Connect 接続を選択し、メトリクスの選択 メトリクスを選択します。
7. [Specify metric and conditions] (メトリクスと条件の指定) ページで、アラームのパラメータを設定します。メトリクスと条件の指定の詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon アラームの使用」を参照してください。 CloudWatch
8. [次へ] を選択します。
9. [Configure actions] (アクションの設定) ページでアラームアクションを設定します。アラームアクションの設定の詳細については、「Amazon ユーザーガイド」の「アラームアクション」を参照してください。 CloudWatch
10. [次へ] を選択します。
11. [Add name and description] (名前と説明を追加) ページで、[Name] (名前) とオプションの [Alarm description] (アラームの説明) を入力してこのアラームについて説明し、[Next] (次へ) をクリックします。
12. 提案されているアラームについて [Preview and create] (プレビューと作成) ページで確認します。
13. 必要に応じて、[Edit] (編集) をクリックして情報を変更し、[Create alarm] (アラームの作成) を選択します。

    [Alarms] (アラーム) ページに、新しいアラームに関する情報が記載された新しい行が表示されます。[Actions] (アクション) ステータスには、[Actions enabled] (有効済みのアクション) と表示されアラームがアクティブであることを示します。

AWS Direct Connect クォータ

次の表に、 に関連するクォータを示します AWS Direct Connect。

コンポーネント	クォータ	コメント
AWS Direct Connect 専用接続あたりのプライベートまたはパブリック仮想インターフェイス	50	この制限を増やすことはできません。
AWS Direct Connect 専用接続あたりのトランジット仮想インターフェイス	4	この制限を増やすことはできません。
AWS Direct Connect 専用接続あたりのプライベート仮想インターフェイスまたはパブリック仮想インターフェイス、 AWS Direct Connect 専用接続あたりのトランジット仮想インターフェイス	51	Amazon VPC Transit Gateway AWS Direct Connect のサポートが開始されると、専用接続あたり 50 個のプライベートまたはパブリック仮想インターフェイスのクォータに、1 つの (1) トランジット仮想インターフェイスのクォータが追加されました。現在許可されているトランジット仮想インターフェイスの数は 4 つで、専用接続あたりの仮想インターフェイスの最大数は 51 個です。この制限を増やすことはできません。
AWS Direct Connect ホスト接続あたりのプライベート、パブリック、またはトランジット仮想インターフェイス	1	この制限を増やすことはできません。
1 リージョン、1 アカウントあたりの Direct Connect ロケーションあたりのアクティブな AWS Direct Connect 接続	10	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。
Link Aggregation Group (LAG) あたりの仮想インターフェイスの数	51	Amazon VPC Transit Gateway AWS Direct Connect のサポートが開始されると、LAG あたり 50 個のプライベートま

コンポーネント	クォータ	コメント
		たはパブリック仮想インターフェイスのクォータに、1 つの (1) トランジット仮想インターフェイスのクォータが追加されました。現在許可されているトランジット仮想インターフェイスの数は 4 つで、LAG あたりの仮想インターフェイスの最大数は 51 個です。この制限を増やすことはできません。
オンプレミスから へのプライベート仮想インターフェイスまたはトランジット仮想インターフェイス上のボーダーゲートウェイプロトコル (BGP) セッションあたりのルート数 AWS。 BGP セッションで IPv4 と IPv6 にそれぞれ 100 を超えるルートをアドバタイズする場合、BGP セッションはアイドル状態になり BGP セッションが DOWN になります。	IPv4 と IPv6 にそれぞれ 100	この制限を増やすことはできません。
パブリック仮想インターフェイスのボーダーゲートウェイプロトコル (BGP) セッションあたりのルート数	1,000	この制限を増やすことはできません。

コンポーネント	クォータ	コメント
Link Aggregation Group (LAG) ごとの専用接続数	ポート速度が 100 G 未満の場合は 4 ポート速度が 100 G の場合は 2	
リージョンごとの Link Aggregation Group (LAG) の数	10	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。
AWS Direct Connect アカウントあたりのゲートウェイ	200	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。
ゲートウェイあたりの仮想プライベート AWS Direct Connect ゲートウェイ	20	この制限を増やすことはできません。
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	この制限を増やすことはできません。
AWS Direct Connect ゲートウェイあたりの仮想インターフェイス (プライベートまたはトランジット)	30	この制限を増やすことはできません。

コンポーネント	クォータ	コメント
トランジット仮想インターフェイス上の AWS Transit Gateway からオンプレミス AWS への あたりのプレフィックス数	IPv4 と IPv6 に合計で 200	この制限を増やすことはできません。
仮想プライベートゲートウェイあたりの仮想インターフェイス数	制限はありません。	
トランジットゲートウェイに関連付けられている Direct Connect ゲートウェイの数	20	この制限を増やすことはできません。
SiteLink プレフィックスの制限	100	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。

AWS Direct Connect は、シングルモードファイバーで次のポート速度をサポートします: 1 Gbps: 1000BASE-LX (1310TAK)、10 Gbps: 10GBASE-LR (1310TAK)、100Gbps 100GBASE-LR4。

BGP クォータ

以下は、BGP クォータです。BGP タイマーは、ルーター間で最小値までネゴシエートします。BFD インターバルは、最も遅いデバイスによって定義されます。

- デフォルトのホールドタイマー: 90 秒
- 最小ホールドタイマー: 3 秒

  ホールド値 0 はサポートされていません。
- デフォルトのキープアライブタイマー: 30 秒
- 最小キープアライブタイマー: 1 秒
- グレースフルリスタートタイマー: 120 秒

グレースフルリスタートと BFD を同時に設定しないことを推奨いたします。

- BFD 活性検出の最小間隔: 300 ミリ秒
- BFD 最小乗数: 3

負荷分散に関する考慮事項

複数のパブリック VIF で負荷分散を使用する場合は、すべての VIF が同じリージョンにある必要があります。

トラブルシューティング AWS Direct Connect

以下のトラブルシューティング情報は、 AWS Direct Connect 接続に関する問題を診断して修正するために役立ちます。

目次

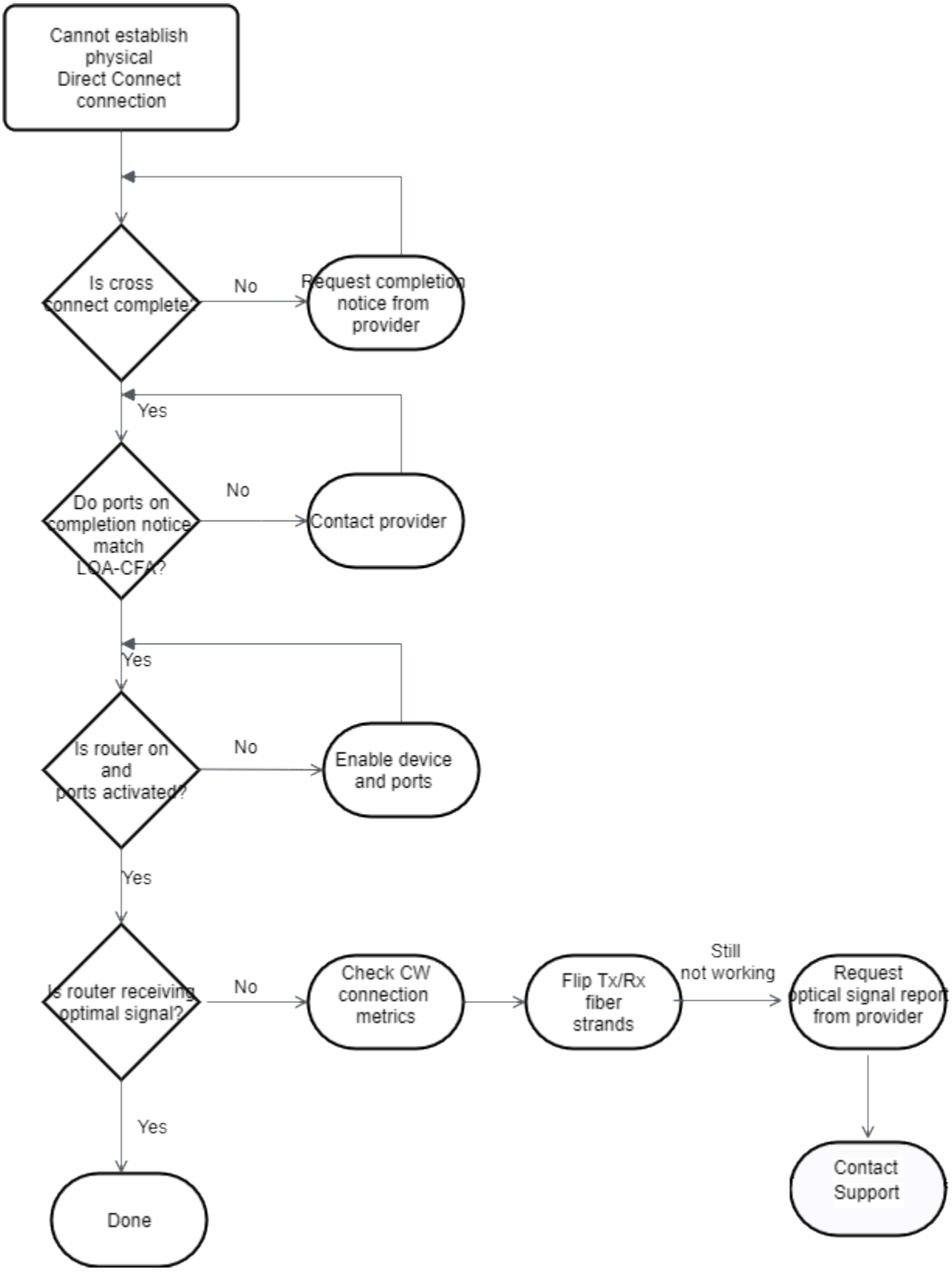
レイヤー 1 (物理層) 問題のトラブルシューティング

ユーザーまたはネットワークプロバイダーが AWS Direct Connect デバイスへの物理的な接続を確立できない場合は、次の手順を使用して問題のトラブルシューティングを行います。

1. クロスコネクトが完了したことをコロケーションプロバイダに確認します。コロケーションプロバイダまたはネットワークプロバイダにクロスコネクトの完了通知の提供を依頼し、LOA-CFA に記載されているものとポートを比較します。
2. ルーターまたはプロバイダのルーターの電源が入っていて、ポートがアクティブ化されていることを確認します。
3. ルーターが正しい光トランシーバを使用していることを確認します。ポート速度が 1 Gbps を超える接続では、ポートのオートネゴシエーションを無効にする必要があります。ただし、接続を提供する AWS Direct Connect エンドポイントによっては、1 Gbps の接続で自動ネゴシエーションを有効または無効にする必要がある場合があります。接続で自動ネゴシエーションを無効にする必要がある場合は、ポート速度と全二重モードを手動で設定する必要があります。仮想インターフェイスがダウンしたままの場合は、レイヤー 2 (データリンク層) 問題のトラブルシューティング を参照してください。
4. ルーターが、許容される光信号をクロスコネクト経由で受信していることを確認します。
5. 送信/受信ファイバーストランドのフリッピング (ローリングとも呼ばれます) を試みます。
6. の Amazon CloudWatch メトリクスを確認します AWS Direct Connect。 AWS Direct Connect デバイスの Tx/Rx 光の読み取り値 (1 Gbps と 10 Gbps の両方) 、物理エラー数、および動作ステータスを確認できます。詳細については、「Amazon によるモニタリング CloudWatch」を参照してください。

7. コロケーションプロバイダに連絡し、クロスコネクト全体での送信/受信光信号に関する書面によるレポートをリクエストします。
8. 上記のステップで物理的な接続性の問題が解決しない場合は、AWS Support に問い合わせて、コロケーションプロバイダーからのクロスコネクト完了通知と光信号レポートを提出します。

次のフローチャートには、物理的な接続の問題を診断するためのステップが含まれています。

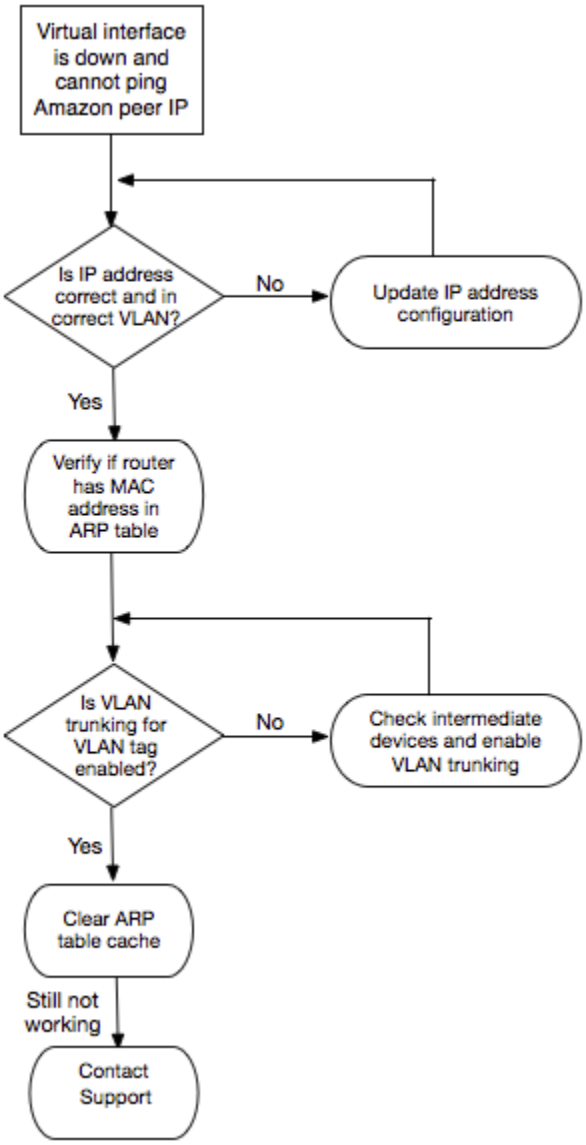

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

レイヤー 2 (データリンク層) 問題のトラブルシューティング

AWS Direct Connect 物理接続は稼働しているが仮想インターフェイスは停止している場合は、次の手順を使用して問題のトラブルシューティングを行います。

1. Amazon のピア IP アドレスに対して ping を送信できない場合は、ピア IP アドレスが正しく設定されていて、正しい VLAN にあることを確認します。IP アドレスが物理インターフェイスではなく VLAN サブインターフェイスで設定されていることを確認します (例: GigabitEthernet0/0 ではなく GigabitEthernet0/0.123)。
2. ルーターに、アドレス解決プロトコル (ARP) テーブルの AWS エンドポイントからの MAC アドレスエントリがあるかどうかを確認します。
3. エンドポイント間の中間デバイスで、802.1 Q VLAN タグに対して VLAN トランキングが有効になっていることを確認します。がタグ付けされたトラフィック AWS を受信するまで、ARP を AWS 側で確立することはできません。
4. お客様またはプロバイダの ARP テーブルキャッシュをクリアします。
5. 上記のステップで ARP が確立されない場合、または Amazon ピア IP に ping を送信できない場合は、 AWS サポートにお問い合わせください。

次のフローチャートには、データリンクに関する接続の問題を診断するためのステップが含まれています。



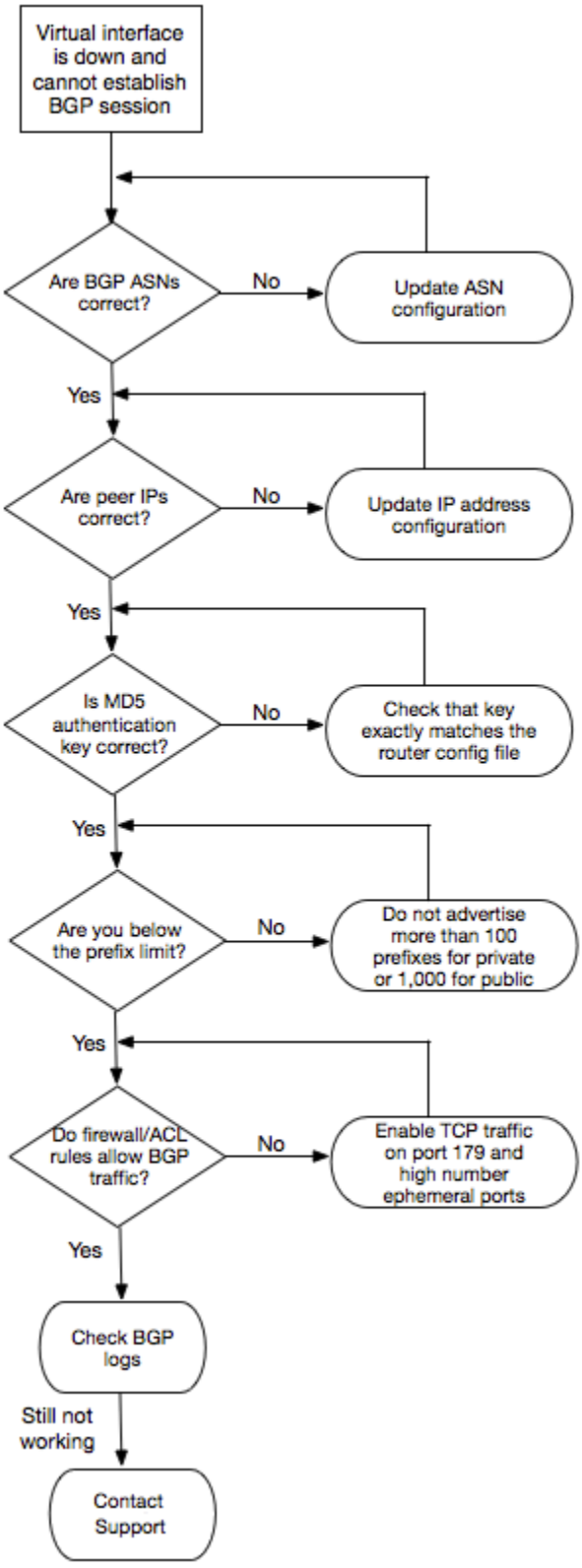
これらのステップの確認後に BGP セッションがまだ確立されない場合は、「レイヤー 3/4 (ネットワーク層/トランスポート層) 問題のトラブルシューティング」を参照してください。BGP セッションが確立されたが、まだルーティングの問題が発生している場合は、「ルーティング問題のトラブルシューティング」を参照してください。

レイヤー 3/4 (ネットワーク層/トランスポート層) 問題のトラブルシューティング

AWS Direct Connect 物理接続が稼働していて、Amazon ピア IP アドレスに ping を送信できる状況を考えてみましょう。仮想インターフェイスがダウンしていて、BGP ピアリングセッションを確立できない場合は、次の手順を実行して問題のトラブルシューティングを行います。

1. BGP ローカル AS 番号 (ASN) と Amazon の ASN が正しく設定されていることを確認します。
2. BGP ピア接続セッションの両側のピア IP が正しく設定されていることを確認します。
3. MD5 認証キーが正しく設定されていて、ダウンロードしたルーター設定ファイルのキーに正確に一致することを確認します。余分なスペースや文字が含まれていないか確認してください。
4. お客様、またはお客様のプロバイダが、プライベート仮想インターフェイスに対して 100 個を超えるプレフィックス、またはパブリック仮想インターフェイスに対して 1,000 個を超えるプレフィックスをアドバタイズしていないことを確認します。これらはハード制限であり、超過することはできません。
5. TCP ポート 179 または高い番号の一時 TCP ポートをブロックしているファイアウォールまたは ACL ルールがないことを確認します。これらのポートは、BGP がピア間の TCP 接続を確立するために必要です。
6. BGP ログで、エラーまたは警告メッセージを確認します。
7. 上記のステップで BGP ピア接続セッションが確立されない場合は、 AWS サポートにお問い合わせください。

次のフローチャートには、BGP のピア接続セッションの問題を診断するためのステップが含まれています。



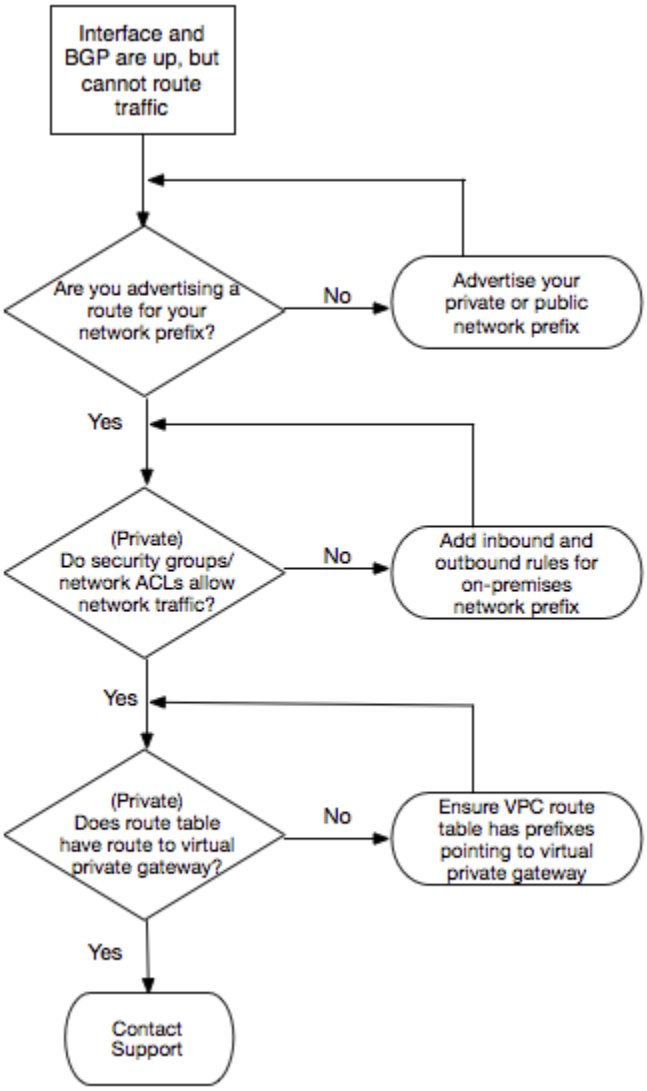
BGP ピア接続セッションが確立されたが、まだルーティングの問題が発生している場合は、「ルーティング問題のトラブルシューティング」を参照してください。

ルーティング問題のトラブルシューティング

仮想インターフェイスが稼動していて、BGP ピアリングセッションを確立している状況を考えてみましょう。仮想インターフェイス上でトラフィックをルーティングできない場合は、次の手順を実行して問題のトラブルシューティングを行います。

1. BGP セッションを介して、オンプレミスネットワークのプレフィックスのルートをアドバタイズしていることを確認します。プライベート仮想インターフェイスの場合、これはプライベートネットワークプレフィックスまたはパブリックネットワークプレフィックスとすることができます。パブリック仮想インターフェイスの場合、これはパブリックにルーティング可能なプレフィックスとする必要があります。
2. プライベート仮想インターフェイスの場合は、VPC セキュリティグループとネットワーク ACL で、オンプレミスネットワークプレフィックスに対してインバウンドトラフィックおよびアウトバウンドトラフィックを許可していることを確認します。詳細については、Amazon VPC ユーザーガイドの「セキュリティグループ」および「ネットワーク ACL」を参照してください。
3. プライベート仮想インターフェイスの場合、VPC ルートテーブルに、プライベート仮想ゲートウェイの接続先となる仮想プライベートゲートウェイを指すプレフィックスがあることを確認します。たとえば、デフォルトでオンプレミスネットワークにすべてのトラフィックをルーティングする場合は、デフォルトルート (0.0.0.0/0 または ::/0) と仮想プライベートゲートウェイを VPC ルートテーブルでターゲットとして追加できます。
   - または、ルート伝達で動的な BGP ルートアドバタイズに基づいて、ルートテーブルで自動的にルートを更新するようにできます。ルートテーブルあたり最大 100 の伝播されたルートを持つことができます。この制限を増やすことはできません。詳細については、Amazon VPC ユーザーガイドの「ルート伝達の有効化と無効化」を参照してください。
4. 上記の手順でルーティングの問題を解決できない場合は、 AWS サポートにお問い合わせください。

次のフローチャートには、ルーティングの問題を診断するためのステップが含まれています。


Interface and BGP are up, but cannot route traffic
Are you advertising a route for your network prefix?
No
Advertise your private or public network prefix
Yes
(Private) Do security groups/ network ACLs allow network traffic?
No
Add inbound and outbound rules for on-premises network prefix
Yes
(Private) Does route table have route to virtual private gateway?
No
Ensure VPC route table has prefixes pointing to virtual private gateway
Yes
Contact Support

ドキュメント履歴

次の表では、AWS Direct Connect のリリースを説明しています。

機能	説明	日付
SiteLink のサポート	同じ AWS リージョン内の 2 つの Direct Connect Point of Presence (POP) 間における接続を有効にする仮想プライベートインターフェイスを作成することができます。詳細については、「ホスト型仮想インターフェイス」を参照してください。	2012-12-01
MAC セキュリティのサポート	MACsec をサポートする AWS Direct Connect 接続を使用して、企業のデータセンターから AWS Direct Connect ロケーションへのデータを暗号化できます。詳細については、「MAC セキュリティ」を参照してください。	2021 年 3 月 31 日
100G のサポート	100G の専用接続のサポートについて説明するためにトピックを更新しました。	2021 年 2 月 12 日
イタリアの新しいロケーション	イタリアの新しいロケーションの追加について、トピックを更新しました。詳細については、「the section called “欧州 (ミラノ)”」を参照してください。	2021 年 1 月 22 日
イスラエルの新しいロケーション	イスラエルの新しいロケーションの追加について、トピックを更新しました。詳細については、「the section called “イスラエル (テルアビブ)”」を参照してください。	2020 年 7 月 7 日
Resiliency Toolkit のフェイルオーバーテストのサポート	Resiliency Toolkit のフェイルオーバーテスト機能を使用して、接続の回復性をテストします。詳細については、「the section called “AWS Direct Connect フェイルオーバーテスト”」を参照してください。	2020 年 6 月 3 日
CloudWatch VIF メトリックのサポート	CloudWatch を使用して、物理的な AWS Direct Connect 接続と仮想インターフェイスをモニタリングできます。詳細については、「the section called “Amazon によるモニタリング CloudWatch”」を参照してください。	2020 年 5 月 11 日

機能	説明	日付
AWS Direct Connect Resiliency Toolkit	AWS Direct Connect Resiliency Toolkit は、SLA 目標を達成するための専用接続の注文に役立つ、複数の回復性モデルを備えた接続ウィザードを提供します。詳細については、「Resiliency Toolkit AWS Direct Connect を使用して開始する」を参照してください。	2019-10-07
アカウント全体の AWS Transit Gateway のサポートに対する追加のリージョンのサポート	詳細については、the section called “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。	2019-09-30
AWS Direct Connect による AWS Transit Gateway のサポート	AWS Direct Connect ゲートウェイを使用して AWS Direct Connect 接続をトランジット仮想インターフェイス経由で VPC に接続するか、トランジットゲートウェイにアタッチされた VPN に接続できます。Direct Connect ゲートウェイをトランジットゲートウェイに関連付けます。次に、Direct Connect ゲートウェイへの AWS Direct Connect 接続のトランジット仮想インターフェイスを作成します。詳細については、the section called “トランジットゲートウェイの関連付け” を参照してください。	2019-03-27
ジャンボフレームのサポート	AWS Direct Connect でジャンボフレーム (9001 MTU) を送信することができます 詳細については、「プライベート仮想インターフェイスまたはトランジット仮想インターフェイスのネットワーク MTU の設定」を参照してください。	2018 年 10 ~ 11 月
BGP コミュニティのローカル優先設定	ローカル優先設定の BGP コミュニティタグを使用すると、ネットワークの着信トラフィックでロードバランシングやルート設定を実現できます。詳細については、「BGP コミュニティのローカル優先設定」を参照してください。	2018-02-06

機能	説明	日付
AWS Direct Connect ゲートウェイ	Direct Connect ゲートウェイを使用して、AWS Direct Connect 接続をリモートリージョンの VPC に接続できます。詳細については、「Direct Connect ゲートウェイの操作」を参照してください。	2017-11-01
Amazon CloudWatch メトリクス	AWS Direct Connect 接続の CloudWatch メトリクスを表示できます。詳細については、「Amazon によるモニタリング CloudWatch」を参照してください。	2017-06-29
Link Aggregation Group (LAG)	Link Aggregation Group (LAG) を作成して、複数の AWS Direct Connect 接続を集約することができます。詳細については、「Link Aggregation Group (LAG)」を参照してください。	2017-02-13
IPv6 サポート	仮想インターフェイスで IPv6 BGP ピアリングセッションをサポートできるようになりました。詳細については、「BGP ピアを追加もしくは削除する」を参照してください。	2016-12-01
タグ指定のサポート	AWS Direct Connect リソースにタグ付けできるようになりました。詳細については、「AWS Direct Connect リソースのタグ付け」を参照してください。	2016-11-04
セルフサービス LOA-CFA	AWS Direct Connect コンソールまたは API を使用して、Letter of Authorization and Connecting Facility Assignment (LOA-CFA) をダウンロードできるようになりました。	2016-06-22
シリコンバレーの新しいロケーション	米国西部 (北カリフォルニア) リージョンの新しいシリコンバレーロケーションの追加について、トピックを更新しました。	2016-06-03
アムステルダムの新しいロケーション	欧州 (フランクフルト) リージョンの新しいアムステルダムロケーションの追加について、トピックを更新しました。	2016-05-19

機能	説明	日付
オレゴン州ポートランドとシンガポールの新しいロケーション	米国西部 (オレゴン) およびアジアパシフィック (シンガポール) リージョンでの新しいロケーション (オレゴン州ポートランドとシンガポール) の追加について、トピックを更新しました。	2016-04-27
サンパウロ (ブラジル) の新しいロケーション	南米 (サンパウロ) リージョンの新しいサンパウロロケーションの追加について、トピックを更新しました。	2015-12-09
ダラス、ロンドン、シリコンバレー、ムンバイの新しいロケーション	ダラス (米国東部 (バージニア北部) リージョン)、ロンドン (欧州 (アイルランド) リージョン)、シリコンバレー (AWS GovCloud (米国西部) リージョン)、およびムンバイ (アジアパシフィック (シンガポール) リージョン) での新しいロケーションの追加を含めるようにトピックを更新しました。	2015-11-27
中国 (北京) リージョンの新しいロケーション	中国 (北京) リージョンの新しい北京ロケーションの追加について、トピックを更新しました。	2015-04-14
米国西部 (オレゴン) リージョンの新しいラスベガスのロケーション	米国西部 (オレゴン) リージョンにサービスを提供するラスベガスの新しい AWS Direct Connect ロケーションの追加について、トピックを更新しました。	2014-11-10
新しい欧州 (フランクフルト) リージョン	EU (フランクフルト) リージョンにサービスを提供する新しい AWS Direct Connect ロケーションの追加について、トピックを更新しました。	2014-10-23

機能	説明	日付
アジアパシフィック (シドニー) リージョンの新しいロケーション	アジアパシフィック (シドニー) リージョンにサービスを提供する新しい AWS Direct Connect ロケーションの追加について、トピックを更新しました。	2014-07-14
サポート対象AWS CloudTrail	のアクティビティをログに記録するために CloudTrail を使用する方法について説明する新しいトピックを追加しましたAWS Direct Connect 詳細については、「AWS Direct Connect を使用した AWS CloudTrail API コールのログ記録」を参照してください。	2014-04-04
リモート AWS リージョンへのアクセスのサポート	リモートリージョンのパブリックリソースにアクセスする方法を説明する新しいトピックを追加しました。詳細については、「リモート AWS リージョンへのアクセス」を参照してください。	2013-12-19
ホスト接続のサポート	ホスト接続のサポートについて説明するためにトピックを更新しました。	2013-10-22
欧州 (アイルランド) リージョンの新しいロケーション	EU (アイルランド) リージョンにサービスを提供する新しい AWS Direct Connect ロケーションの追加について、トピックを更新しました。	2013-06-24
米国西部 (オレゴン) リージョンの新しいシアトルのロケーション	米国西部 (オレゴン) リージョンにサービスを提供するシアトルの新しい AWS Direct Connect ロケーションの追加について、トピックを更新しました。	2013-05-08

機能	説明	日付
での IAM の使用のサポートAWS Direct Connect	AWS Identity and Access Management で AWS Direct Connect を使用することに関するトピックが追加されました。詳細については、「the section called “Identity and Access Management”」を参照してください。	2012-12-21
新しいアジアパシフィック (シドニー) リージョン	アジアパシフィック (シドニー) リージョンにサービスを提供する AWS Direct Connect の新しいロケーションの追加について、トピックを更新しました。	2012-12-14
新しい AWS Direct Connect コンソールと、米国東部 (バージニア北部) リージョンおよび南米 (サンパウロ) リージョン	『AWS Direct Connect 入門ガイド』を『AWS Direct Connect ユーザーガイド』で置き換えました。新しい AWS Direct Connect コンソールに関するトピックの追加、請求に関するトピックの追加、ルーター設定情報の追加を行いました。2 つの新しい AWS Direct Connect ロケーションの記述を追加しました。これらは、米国東部 (バージニア北部) リージョンと南米 (サンパウロ) リージョンに対応するものです。	2012-08-13
EU（アイルランド）、アジアパシフィック（シンガポール）、およびアジアパシフィック（東京）リージョン向けサポート	新しいトラブルシューティングのセクションを追加しました。4 つの新しい AWS Direct Connect ロケーションの記述を追加しました。これらは、米国西部（北カリフォルニア）、欧州（アイルランド）、アジアパシフィック（シンガポール）、およびアジアパシフィック（東京）の各リージョンに対応するものです。	2012-01-10

機能	説明	日付
米国西部（北カリフォルニア）リージョンのサポート	米国西部（北カリフォルニア）リージョンの追加を含めるため、トピックが更新されました。	2011-09-08
パブリックリリース	AWS Direct Connect の最初のリリースです	2011-08-03

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。