ユーザーガイド

AWS Direct Connect

AWS Direct Connect: ユーザーガイド

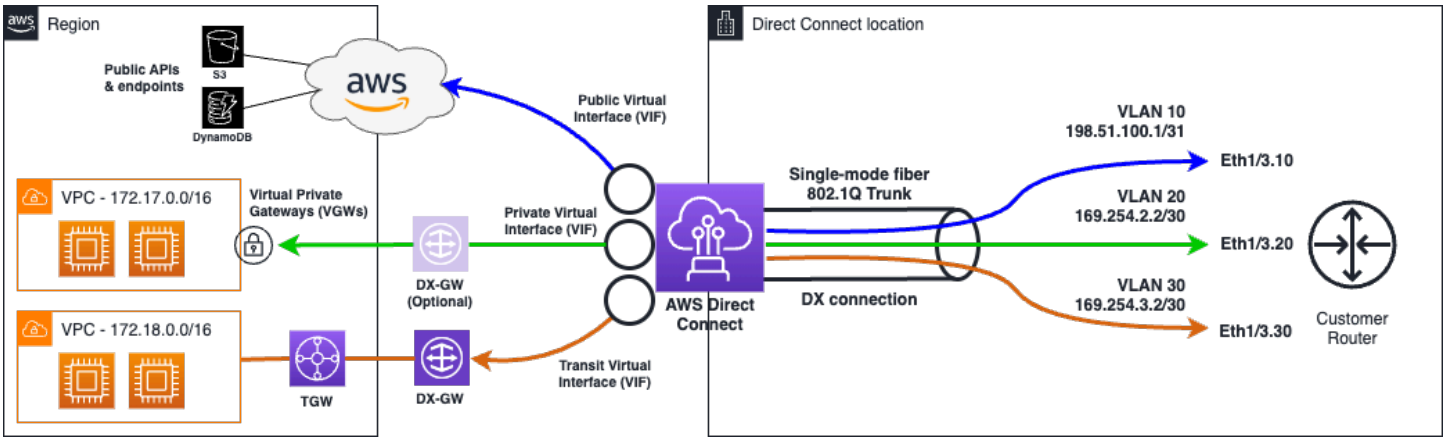
Table of Contents

Direct Connect とは

Direct Connect は、お客様の内部ネットワークを Direct Connect ロケーションに、標準のイーサネット光ファイバケーブルを介して接続するサービスです。ケーブルの一端がお客様のルーターに、他方が Direct Connect のルーターに接続されます。この接続を使用すると、Amazon S3 などの AWS のパブリックサービス、または Amazon VPC に対する仮想インターフェイスを直接作成できるため、ネットワークパスのインターネットサービスプロバイダーを回避できます。Direct Connect ロケーションは、関連付けられているリージョン内の AWS へのアクセスを提供します。パブリックリージョン、または AWS GovCloud (US) 内の単一の接続を使用して、その他すべてのパブリックリージョン内にある AWS のパブリックサービスにアクセスすることができます。

- 接続できる Direct Connect ロケーション一覧については、「AWS Direct Connect Locations」を参照してください。
- Direct Connect に関する質問の回答は、「Direct Connect のよくある質問」を参照してください。

次の図は、Direct Connect とお客様のネットワークがどのように連結されるかを大まかに示したものです。



内容

Direct Connect コンポーネント

以下は、Direct Connect に使用する主要コンポーネントです。

接続

Direct Connect ロケーションで接続を作成し、ユーザーの施設から 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、「Direct Connect 専用接続とホスト接続」を参照してください。

仮想インターフェイス

AWS のサービスへのアクセスを有効にするには、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。サポートされているインターフェイスのタイプについては、the section called “サポートされている Direct Connect 仮想インターフェイスタイプ” で説明します。サポートされているインターフェイスの詳細については、「Direct Connect 仮想インターフェイスとホスト型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

Direct Connect のロケーションで Direct Connect を使用するには、お客様のネットワークが以下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している Direct Connect ロケーションと同じ場所にある。利用可能な 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 パートナーネットワーク (APN) のメンバーである Direct Connect 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 Gbps イーサネットの場合は 1000BASE-LX (1310 nm) トランシーバー、10 Gbps イーサネットの場合は 10GBASE-LR (1310 nm) トランシーバー、100 Gbps イーサネットの場合は 100GBASE-LR4、または 400 Gbps イーサネットの場合は 400GBASE-LR4 を備えたシングルモードファイバーを使用する必要があります。

- 接続を処理する AWS Direct Connect エンドポイントによっては、任意の専用接続についてオンプレミスデバイスのオートネゴシエーションを有効または無効にする必要が生じる場合があります。Direct Connect 接続の起動時に仮想インターフェイスがダウンしたままになる場合は、「レイヤー 2 (データリンク層) の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、Direct Connect 各仮想インターフェイスで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。

Direct Connect では、IPv4 と IPv6 の両方の通信プロトコルがサポートされます。AWS のパブリックサービスが提供する IPv6 アドレスは、Direct Connect パブリック仮想インターフェイス経由でアクセスできます。

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 MTU」を参照してください。

サポートされている Direct Connect 仮想インターフェイスタイプ

AWS Direct Connect は、次の 3 つの仮想インターフェイス (VIF) タイプをサポートしています。

- プライベート仮想インターフェイス

  このタイプのインターフェイスは、プライベート IP アドレスを使用して Amazon Virtual Private Cloud (VPC) にアクセスするために使用されます。プライベート仮想インターフェイスを使用すると、

  - プライベート仮想インターフェイスごとに 1 つの VPC に直接接続して、同じリージョン内のプライベート IP を使用してこれらのリソースにアクセスできます。

  - プライベート仮想インターフェイスを Direct Connect ゲートウェイに接続して、任意のアカウントと AWS リージョン (AWS 中国リージョンを除く) にわたって複数の仮想プライベート ゲートウェイにアクセスします。
- パブリック仮想インターフェイス

  このタイプの仮想インターフェイスは、パブリック IP アドレスを使用してすべての AWS パブリック サービスにアクセスするために使用されます。パブリック仮想インターフェイスを使用すると、すべての AWS パブリック IP アドレスとサービスにグローバルに接続できます。
- トランジット仮想インターフェイス

  このタイプのインターフェイスは、Direct Connect ゲートウェイに関連付けられた 1 つ以上の Amazon VPC Transit Gateway にアクセスするために使用されます。トランジット仮想インターフェイスを使用すると、複数のアカウントおよび AWS リージョン (AWS 中国リージョンを除く) にわたって複数の Amazon VPC トランジット ゲートウェイに接続できます。

> **Note**
>
> Direct Connect ゲートウェイと仮想インターフェイスの組み合わせには、制限があります。各制限の詳細については、Direct Connect クォータ を参照してください。

仮想インターフェイスの詳細については、「仮想インターフェイスとホスト型仮想インターフェイス」を参照してください。

Direct Connect の料金

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送信料金は、データ転送を行う 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。

パブリックにアドレス指定できる AWS リソース (例えば、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経由する EC2 トラフィック) では、アウトバウンドトラフィックが同じ AWS 支払者アカウントによって所有されるパブリックプレフィックス宛てであり、Direct Connect パブリック仮想インターフェイスを通じて AWS にアクティブにアドバタイズさ

れている場合、データ送信 (DTO) の使用量が Direct Connect データ転送レートでリソース所有者に請求されます。

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

リモート Direct Connect リージョンにアクセスする

パブリックリージョン、または AWS GovCloud (US) 内の 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 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 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。

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、「仮想インターフェイスとホスト型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、Direct Connect 接続を、異なるリージョ

ンまたは Transit Gateway 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」を参照してください。

また、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 の接続オプション

Direct Connect ルーティングポリシーと BGP コミュニティ

Direct Connect は、パブリック AWS 接続の (オンプレミスのデータセンターからの) インバウンドルーティングポリシーおよび (Direct Connect リージョンからの) アウトバウンドルーティングポリシーを適用します。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

Direct Connect を使用してパブリック AWS サービスにアクセスする場合、BGP 経由でアドバタイズするには、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。
- Direct Connect は、インバウンドパケットの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てい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 と最長のプレフィックス一致を使用してルーティングパスが決定されます。 AWS は同じプレフィックスが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アドバタイズされる場合は、Direct Connect 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。
- Direct Connect は、すべてのローカルおよびリモート AWS リージョンプレフィックス (それらが利用可能な場合) をアドバタイズし、CloudFront や Route 53 などの、リージョンではない AWS PoP (Points of Presence) からのオンネットプレフィックス (それらが利用可能な場合) を含めます。

  > **Note**
  >
  > - AWS 中国リージョンの AWS 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、AWS 中国リージョンでのみアドバタイズされます。
  > - AWS 商業地域の AWS 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、AWS 商業地域でのみアドバタイズされます。
  >
  > 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。

- Direct Connect はパスの最小長が 3 のプレフィックスをアドバタイズします。
- Direct Connect は well-known NO_EXPORT BGP コミュニティを持つすべてのパブリックプレフィックスをアドバタイズします。
- 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、両方の BGP 属性と最長のプレフィックス長が同じである場合、AWS はアウトバウンドトラフィックのホームリージョンを優先します。
- 複数の Direct Connect 接続がある場合は、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。
- Direct Connect でアドバタイズされるプレフィックスは、接続のネットワーク境界を越えてアドバタイズしてはいけません。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。
- Direct Connect は、Amazon ネットワーク内でカスタマーによってアドバタイズされたプレフィクスを保持します。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。
  - その他の Direct Connect のお客様
  - 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
- パブリックインターフェイスを使用する場合は、パブリック ASN またはプライベート ASN のいずれかを使用できます。ただし、以下に示す重要な考慮事項があります。
  - パブリック ASN: ASN を所有し、そのことを発表する権限を持っている必要があります。AWS によって ASN の所有権が検証されます。ASN (1 ~ 2147483647) と ロング ASN (1 ~ 4294967295) の両方がサポートされています。
  - プライベート ASN: 次の範囲のプライベート ASN を使用できます。
    - プライベート ASN: 64512 ~ 65534
    - プライベートロング ASN: 4200000000 ~ 4294967294

    ただし、Direct Connect は、プレフィックスを他の AWS のお客様またはインターネットにアドバタイズするときに、プライベート ASN を AWS ASN (7224) に置き換えます。
  - ASN プリペンディング:
    - パブリック ASN (ASN と ロング ASN の両方) では、プリペンディングは予期したとおりに動作し、プリペンドされた ASN は他のネットワークに表示されます。
    - プライベート ASN (ASN と ロング ASN の両方) では、AWS がプライベート ASN を 7224 に置き換えると、プリペンディングは削除されます。つまり、ASN プリペンディングは、パブリック仮想インターフェイスでプライベート ASN を使用する場合には、AWS の外部でルーティング決定に影響を与えるのに効果的ではありません。
- パブリック仮想インターフェイスを介して AWS との BGP ピアリングセッションを確立する場合、AWS 側で BGP セッションを確立するための AS 番号 (ASN) に 7224 を使用します。ルーターまたはカスタマーゲートウェイデバイスの ASN は、その ASN とは異なっている必要があります。顧客の ASN は ASN (1 ~ 2147483647、予約済み範囲を除く) または ロング ASN (1 ~ 4294967295、予約済み範囲を除く) のいずれかです。

パブリック仮想インターフェイス BGP コミュニティ

Direct Connect はパブリック仮想インターフェースで、トラフィックの範囲 (リージョン内またはグローバル) やルートの優先度を柔軟に設定できるスコープ BGP コミュニティタグをサポートしています。AWS は、パブリック VIF から受信したすべてのルートを、NO_EXPORT BGP コミュニティタグが付けられているかのように扱います。つまり、AWS ネットワークのみがそのルーティング情報を使用します。

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` — 1 つの大陸にあるすべての AWS リージョン:
  - 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 AWS リージョン)

> **Note**
>
> コミュニティタグを適用しない場合、プレフィックスは、デフォルトですべてのパブリック AWS 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 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の場合、Direct Connect は次の BGP コミュニティをアドバタイズされるルートに適用します。

- `7224:8100`—AWS のプレゼンスポイントが関連付けられている Direct Connect リージョンと同じリージョンから送信されるルート。
- `7224:8200`—Direct Connect のプレゼンスポイントが関連付けられている大陸と同じ大陸から送信されるルート。
- タグなし-他の大陸を起点とするルート。

> **Note**
>
> すべての AWS パブリックプレフィックスを受信するには、フィルターを適用しません。

Direct Connect パブリック接続で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。

Direct Connectまた、 は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。Direct Connect を使用してパブリック AWS 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イスの場合、Direct Connect が顧客にアドバタイズするすべてのルートに NO_EXPORT コミュニティタグが付きます。

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 を使用してプライベート AWS リソースにアクセスしている場合は、BGP 経由でアドバタイズするために 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、パブリックまたはプライベートに設定できます。

アドバタイズされたプレフィックスに基づいて、次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 は、最初に最長のプレフィックス長を評価します。AWS では、必要なルーティングパスがアクティブ/パッシブ接続を対象としている場合、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、「Influencing Traffic over Hybrid Networks using Longest Prefix Match」を参照してください。
- ローカルプレファレンスは、アクティブ/パッシブ接続用に意図されたルーティングパスで、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推奨される BGP 属性です。この値は、7224:7200—Medium ローカルプレファレンスコミュニティ値が設定された、同じ AWS リージョンに関連付けられた AWS Direct Connect ロケーションを優先的に選択するようリージョンごとに設定されます。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、より低い値に設定されます。これは、ローカルプリファレンスコミュニティタグが使用されていない場合にのみ適用されます。

- AS_PATH 長は、プレフィックス長とローカルプリファレンスが同じ場合のルーティングパスを決定するために使用できます。
- 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、マルチエグジット識別子 (MED) を使用してルーティングパスを決定できます。AWS では、評価における優先順位が低いため、MED 値を使用することはお勧めしません。
- AWS は、プレフィックスの AS_PATH 長と BGP 属性が同じである場合、複数のトランジット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等コストマルチパス (ECMP) ルーティングを使用します。プレフィックスの AS_PATH の ASN は一致する必要はありません。

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

AWS リージョンが Direct Connect 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経由でオンプレミスのロケーションにトラフィックをルーティングする場合、Direct Connect ロケーションに関連付けられた AWS リージョンが ECMP を使用する機能に影響します。AWS リージョンは、デフォルトで同じ関連付けられた AWS リージョン内の Direct Connect ロケーションを優先します。Direct Connect ロケーションに関連付けられた AWS リージョンを特定するには、「AWS Direct Connect Locations」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、以下のシナリオにおいて、同じプレフィックス長、AS_PATH 長、および MED 値を持つ 2 つ以上のパスに対して、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上で 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、同じまたは異なるコロケーション施設にあるかどうかに関係なく、同じ関連付けられた AWS リージョン内のロケーションからの 2 つ以上の仮想インターフェイスパスがあります。
- 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ロケーションからの 2 つ以上の仮想インターフェイスパスがあります。

詳細については、「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 AWS へのアクティブ/アクティブまたはアクティブ/パッシブ Direct Connect 接続をセットアップするにはどうすればよいですか?」を参照してください。

> **Note**
>
> これは、オンプレミスから AWS リージョンへの ECMP には影響を与えません。

ルート設定を制御するために、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設定 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。同一または異なる AWS リージョンをホームとする複数の Direct Connect 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間で同じコミュニティタグ、例えば `7224:7200` (中程度の優先設定) を適用します。接続の 1 つに障害が発生すると、トラフィックは、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間で等価コストマルチパス (ECMP) を使用して負荷分散されます。複数の 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)。

Direct Connect でのロング ASN のサポート

ロング ASN (4 バイト) のサポートにより、AWS のネットワークデバイスとお客様のネットワークデバイスの間で確立された BGP セッションのパラメータの一部としてロング AS 番号 (ASN) を設定できます。この機能は、アカウントごとに有効または無効にします。

ASN またはロング ASN の範囲は、コンソールまたは API のいずれかを使用して設定できます。

- コンソールを使用する場合、[ASN] フィールドでは ASN とロング ASN の両方がサポートされます。1 ~ 4294967294 の任意の範囲を追加できます。
- API を使用して仮想インターフェイスを作成する場合は、ASN (`asn`) またはロング ASN (`asnLong`) のいずれかを指定できます。ただし、両方を指定することはできません。ASN またはロング ASN の使用方法の詳細については、「Direct Connect API リファレンス」の次の API を参照してください。
  - `BGPPeer`
  - `DeleteBGPPeerRequest`
  - `NewBGPPeer`
  - `NewPrivateVirtualInterface`
  - `NewPrivateVirtualInterfaceAllocation`
  - `NewPublicVirtualInterface`
  - `NewPublicVirtualInterfaceAllocation`
  - `NewTransitVirtualInterface`
  - `NewTransitVirtualInterfaceAllocation`
  - `VirtualInterface`

考慮事項

ASN またはロング ASN のいずれかを使用する場合は、次の点に注意してください。

- 下位互換性: Direct Connect は、ASN とロング ASN の両方に対応するルーターで BGP セッションを自動的に処理します。お使いのルーターがロング ASN に対応していない場合、BGP セッションは ASN モードで動作します。
- ASN 形式: 4 バイトの ASN は、asplain 形式 (`4200000000` など) または asdot 形式 (`64086.59904` など) のいずれかで指定できます。Direct Connect は両方の形式を受け入れますが、ASN を asplain 形式で表示します。

- プライベート ASN 範囲: プライベートロング ASN (4200000000-4294967294) を使用する場合は、プライベート ASN と同じ置換動作が適用されます。Direct Connect は、他のネットワークにアドバタイズするときに、プライベート ASN を 7224 に置き換えます。
- BGP コミュニティタグ: 既存のすべての BGP コミュニティタグ (7224:xxxx) はロング ASN で動作します。コミュニティタグの形式は変更されないままです。
- モニタリングとトラブルシューティング: CloudWatch メトリクス、BGP セッションログ、およびトラブルシューティングツールでは、一貫性を保つために ASN は asplain 形式で表示されます。

可用性と料金

Direct Connect でのロング ASN のサポートについては、次の点に注意してください。

- 可用性: ロング ASN は、Direct Connect がサポートされているすべての AWS リージョンで使用できます。
- 料金: ロング ASN のサポートには、標準の Direct Connect 料金以外に追加料金はかかりません。

> **Note**
>
> ロング ASN の有効化は AWS アカウント全体に適用されます。個々の仮想インターフェイスまたは BGP ピアに対してロング ASN のサポートを有効にすることはできません。

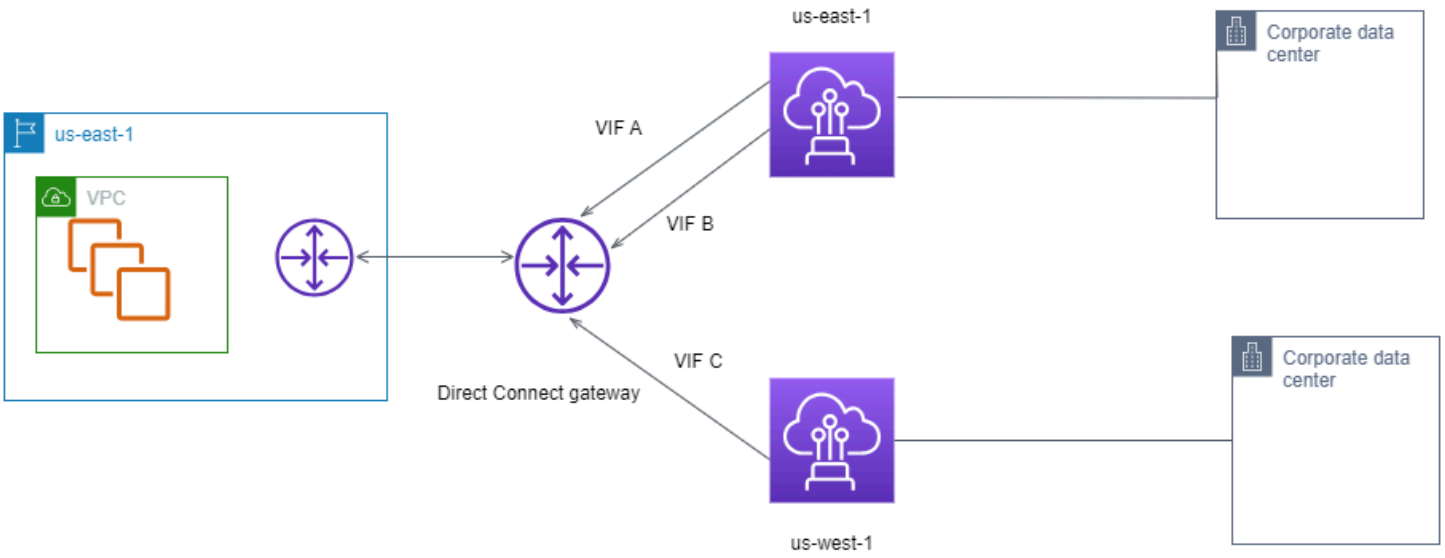
Direct Connect プライベート仮想インターフェイスルーティングの例

Direct Connect のロケーション 1 のホームリージョンが VPC のホームリージョンと同じである設定を考えてみます。Direct Connect 別のリージョンに冗長ロケーションがあります。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。Direct Connect ロケーション (us-west-1) から Direct 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。AWS が VIF A より先に VIF B にトラフィックをルーティングするようにするには、VIF B の AS_PATH 属性を VIF A の AS_PATH 属性より短く設定します。

VIF の設定は次のとおりです。

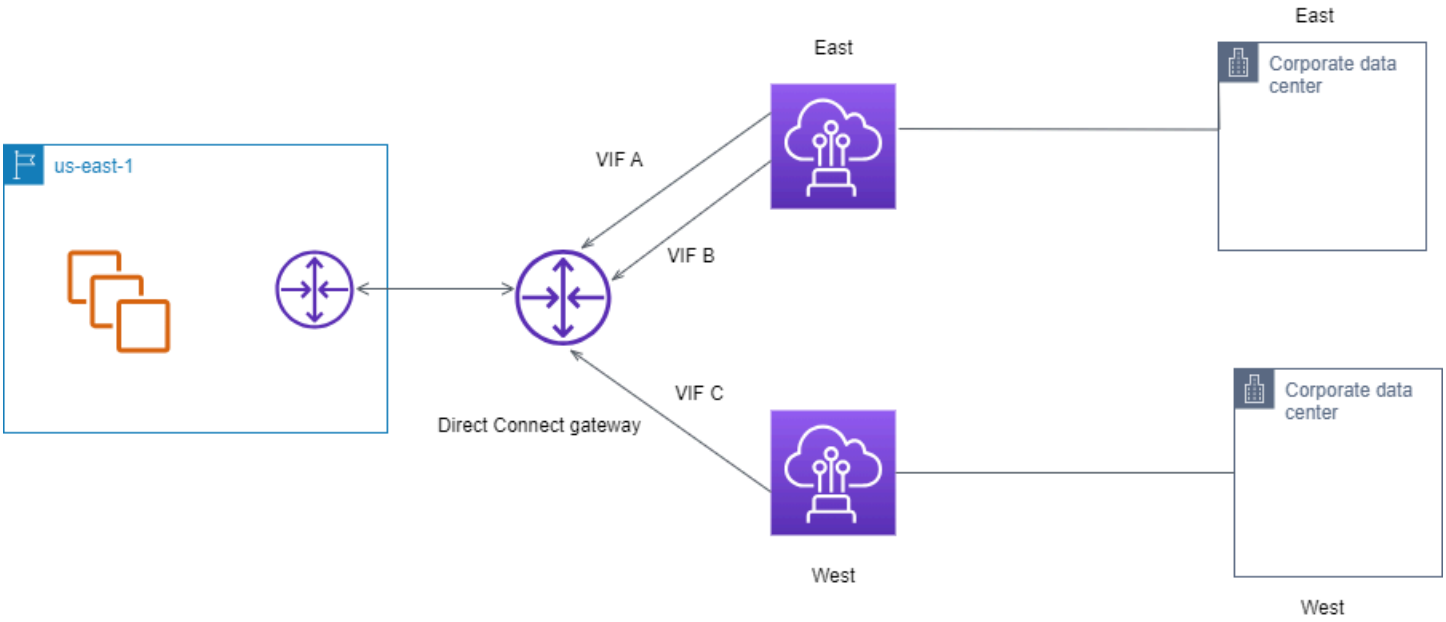
- VIF A (us-east-1) は 172.16.0.0/16 をアドバタイズし、AS_PATH 属性は 65001、65001、65001
- VIF B (us-east-1) は 172.16.0.0/16 をアドバタイズし、AS_PATH 属性は 65001、65001

- 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 の範囲設定を変更した場合、VIF C CIDR 範囲に該当するルートは VIF C を使用します。これは、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



Direct Connect 接続オプション

AWS で、Amazon Virtual Private Cloud (Amazon VPC) およびオンプレミスのインフラストラクチャ間で回復性の高いネットワーク接続を実現できます。AWS Direct Connect Resiliency Toolkit は、複数の復元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。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。

Direct Connect では次の接続オプションを使用できます。

- 最大回復性: このモデルは、AWS Direct Connect Resiliency Toolkit で使用でき、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、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。詳細については、「AWS Direct Connect Resiliency Toolkit」を参照してください。
- 高い回復性: このモデルは、AWS Direct Connect Resiliency Toolkit で使用でき、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、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。詳細については、「AWS Direct Connect Resiliency Toolkit」を参照してください。
- 開発とテスト: このモデルでは、AWS Direct Connect Resiliency Toolkit で使用でき、1 つの場所の個別のデバイスで終端する個別の接続を使用して、重要ではないワークロードの開発およびテストのレジリエンシーを実現できます。詳細については、「AWS Direct Connect Resiliency Toolkit」を参照してください。
- Classic: Classic 接続は、AWS Direct Connect Resiliency Toolkit を必要とせずに接続を作成します。これは、既存の接続があり、ツールキットを使用せずに追加の接続を追加したいユーザーを対象としています。このモデルは 95% の SLA を備えていますが、レジリエンシーや冗長性は提供されません。詳細については、「Classic 接続」を参照してください。

トピック

接続の前提条件

Direct Connect は、シングルモード ファイバー経由で次のポート速度をサポートします。1 Gbps イーサネットの場合は 1000BASE-LX (1310 nm) トランシーバー、10 Gbps イーサネットの場合は 10GBASE-LR (1310 nm) トランシーバー、100 Gbps イーサネットの場合は 100GBASE-LR4 、400 Gbps イーサネットの場合は 400GBASE-LR4 です。

AWS Direct Connect Resiliency Toolkit または Classic 接続を使用して、次のいずれかの方法で Direct Connect 接続をセットアップできます。

モデル	帯域幅	方法
専用接続	1 Gbps、10 Gbps、100 Gbps、400 Gbps	Direct Connect の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、お客様のデータセンター、オフィス、またはコロケーション環境からのルーターを Direct Connect ロケーションに接続します。専用接続に接続するには、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。Direct Connect 専用接続は、シングルモードファイバーで 1 Gbps：1000BASE-LX (1310 nm)、10 Gbps：10GBASE-LR (1310 nm)、100 Gbps：100GBASE-LR4、または 400 Gbps イーサネット用の 400GBASE-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	AWS Direct Connect パートナープログラムのパートナーと連携して、データセンタ

モデル	帯域幅	方法
	Gbps、5 Gbps、10 Gbps、25 Gbps	ー、オフィス、またはコロケーション環境から Direct Connect ロケーションにルーターを接続します。 ー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。

1 Gbps 以上の帯域幅で Direct Connect に接続するには、ネットワークが以下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 Gbps イーサネットの場合は 1000BASE-LX (1310 nm) トランシーバー、10 Gbps イーサネットの場合は 10GBASE-LR (1310 nm) トランシーバー、100 Gbps イーサネットの場合は 100GBASE-LR4、または 400 Gbps イーサネットの場合は 400GBASE-LR4 を備えたシングルモードファイバーを使用する必要があります。
- 接続を処理する AWS Direct Connect エンドポイントによっては、任意の専用接続についてオンプレミスデバイスのオートネゴシエーションを有効または無効にする必要が生じる場合があります。Direct Connect 接続の起動時に仮想インターフェイスがダウンしたままになる場合は、「レイヤー 2 (データリンク層) の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、Direct Connect 各仮想インターフェイスで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。

- Classic 接続を作成しない場合に使用するレジリエンシーモデル。AWS Direct Connect Resiliency Toolkit の接続オプションについては、「AWS Direct Connect Resiliency Toolkit」を参照してください。
- 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。

AWS Direct Connect Resiliency Toolkit

AWS で、Amazon Virtual Private Cloud (Amazon VPC) およびオンプレミスのインフラストラクチャ間で回復性の高いネットワーク接続を実現できます。AWS Direct Connect Resiliency Toolkit は、複数の復元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。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。

AWS Direct Connect Resiliency Toolkit には、以下の利点があります。

- 適切な冗長 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 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。
- AWS の新規のお客様には専用接続承認のためのサポートチケットを自動的に作成するか、未知の (その他の) パートナーを選択します。
- 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、100 Gbps、または 400 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 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 “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、「Direct Connect のリソースをモニタリングする」を参照してください。

回復性モデルを選択した後は、AWS Direct Connect Resiliency Toolkit が次の手順に進みます。

- 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

利用可能な回復性モデル

AWS Direct Connect Resiliency Toolkit では、次の回復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、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、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。

この場合のベストプラクティスは、AWS Direct Connect Resiliency Toolkit の接続ウィザードを使用して、SLA の目標を達成するように指示することです。

> **Note**
>
> AWS Direct Connect Resiliency Toolkit を使用して回復性モデルを作成しない場合は、Classic 接続を作成できます。Classic 接続の詳細については、「Classic 接続」を参照してください。

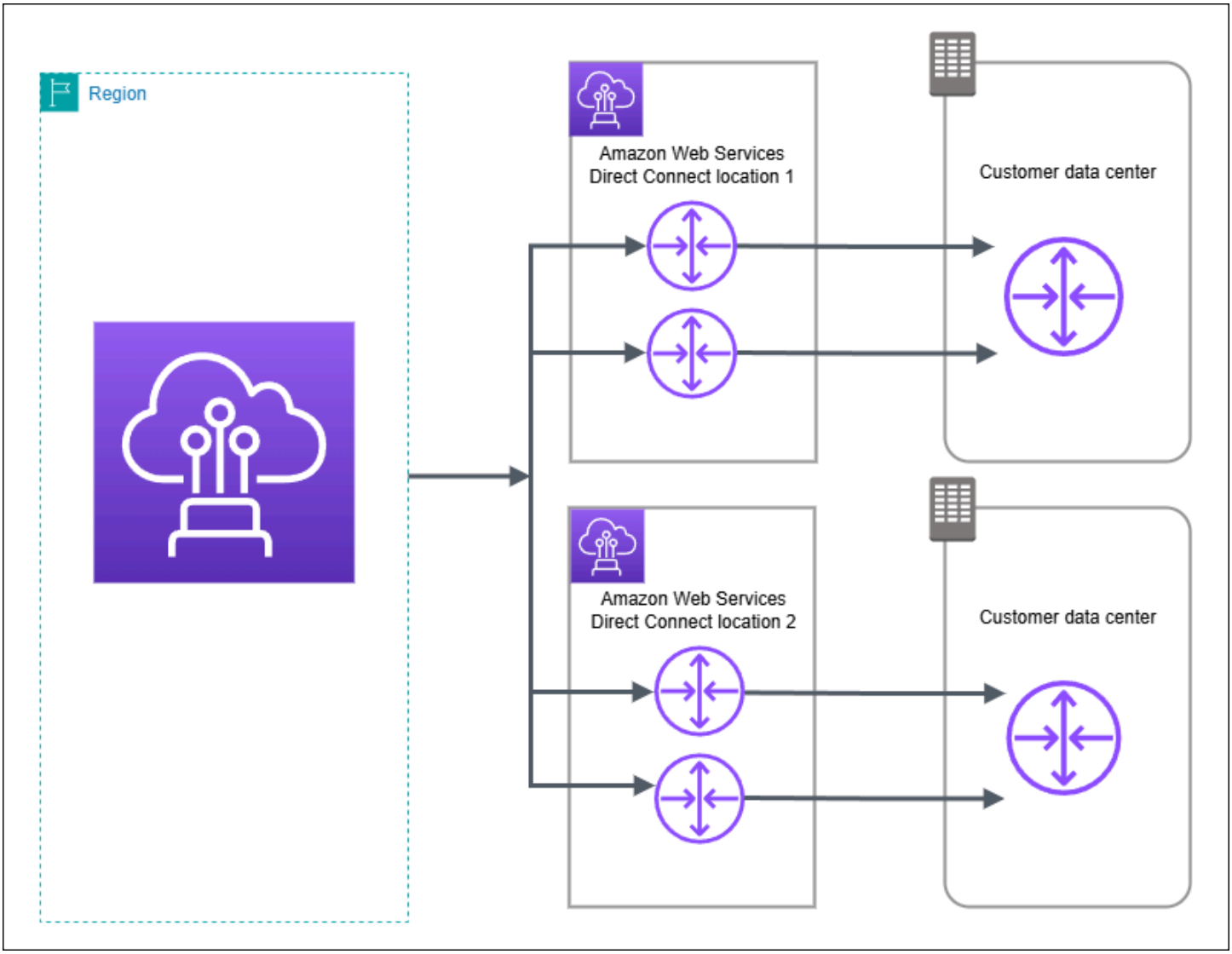
AWS Direct Connect Resiliency Toolkit の前提条件

設定を開始する前に、次の情報に注意してください。

- 接続の前提条件 を十分に理解すること。
- 使用する、使用可能な回復性モデル。

最大回復性

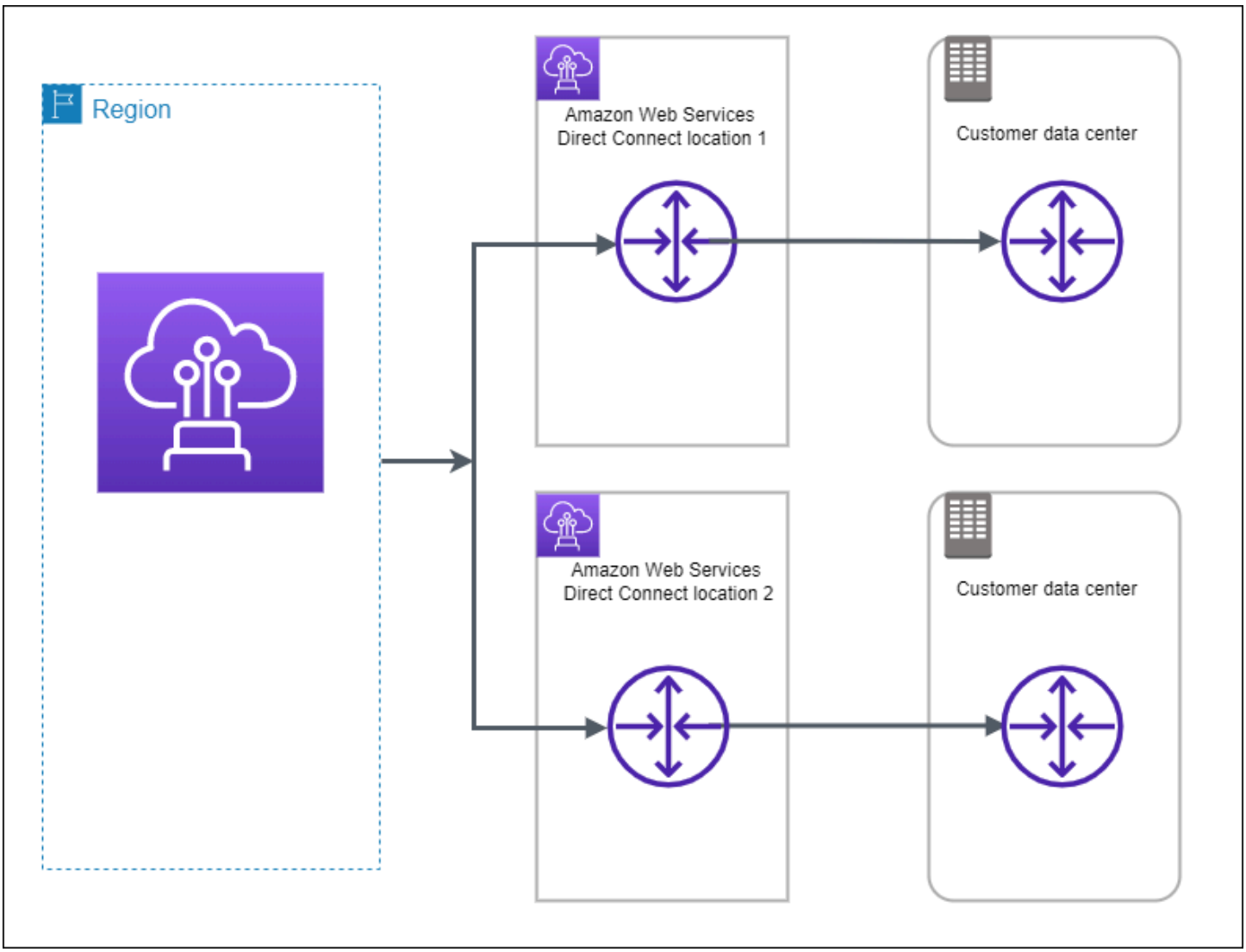
クリティカルなワークロードに対し、複数の場所にある別々のデバイスを終端とする別々の接続を使用することで最大限の回復性を実現できます (以下の図を参照)。このモデルは、デバイス、接続、ロケーション全体の障害に対する回復性を提供します。次の図は、各カスタマーデータセンターから同一の Direct Connect ロケーションに向かう両方の接続の両方を示しています。必要に応じてお客様は、自身のデータセンターから異なるロケーションに向かう、別個の接続を持つこともできます。



AWS Direct Connect Resiliency Toolkit を使用して最大限の回復性モデルを設定する手順については、「最大限の回復性を設定する」を参照してください。

高い回復性

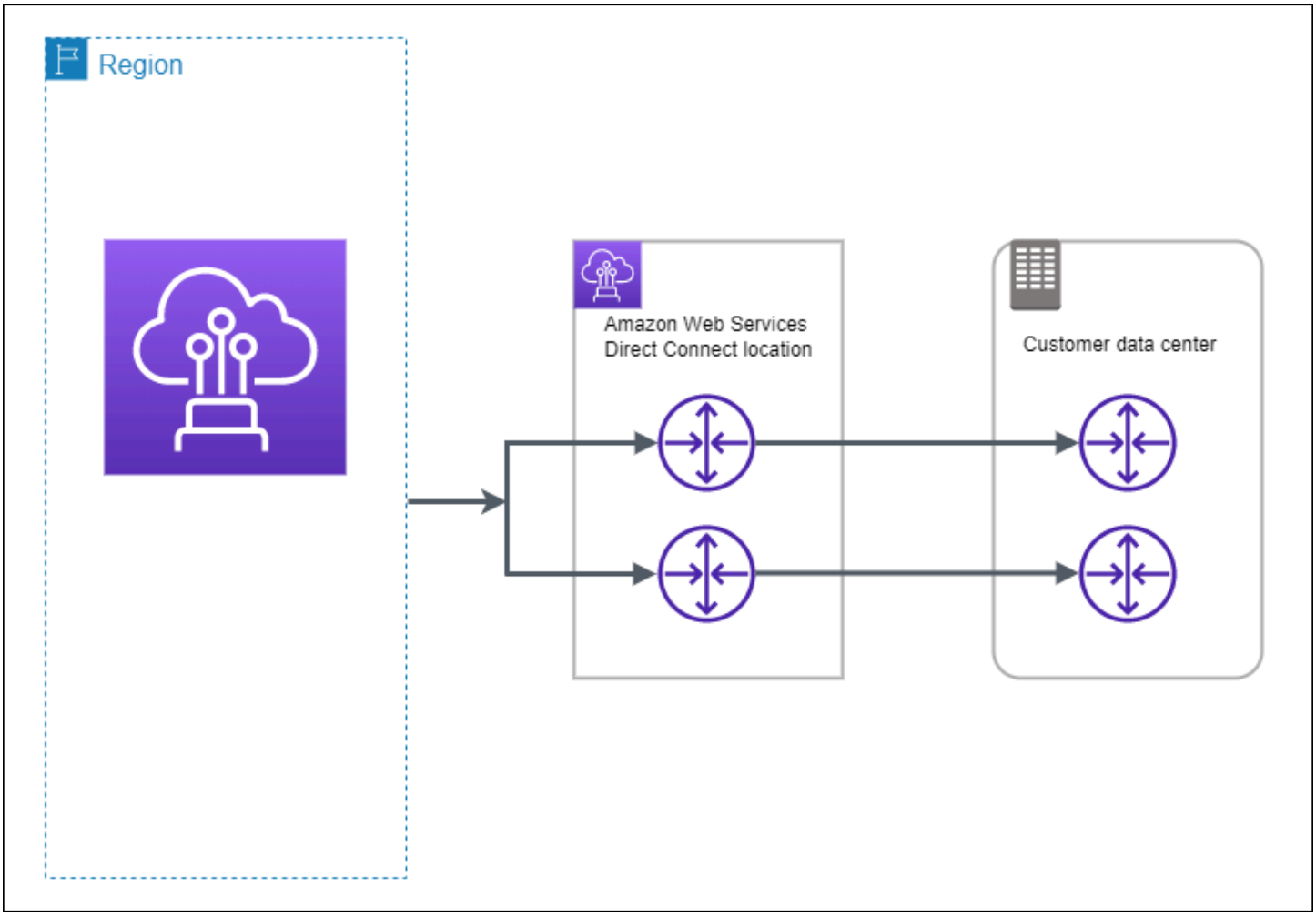
クリティカルなワークロードに対し、複数の場所につながる 2 つの単一接続を使用することで、高い回復性を実現できます (以下の図を参照)。このモデルは、ファイバーの切断やデバイスの障害に起因する接続障害に対し、回復性を提供します。また、ロケーション全体の障害を防ぐのに役立ちます。



AWS Direct Connect Resiliency Toolkit を使用して高回復性モデルを設定する手順については、「高い回復性を設定する」を参照してください。

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。



AWS Direct Connect Resiliency Toolkit を使用して最大限の回復性モデルを設定する手順については、「開発とテスト環境の回復性を設定する」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 を使用してトラフィックルートを確認し、それらのルートが回復性の要件を満たしていることを確認します。

AWS Direct Connect Resiliency Toolkit を使用してフェイルオーバーテストを実行する手順については、「Direct Connect フェイルオーバーテスト」を参照してください。

AWS Direct Connect Resiliency Toolkit を使用して Direct Connect が最大限の回復性を備えるように設定する

この例では、Direct Connect Resiliency Toolkit を使用して最大限の回復性モデルを設定します。

タスク

- ステップ 1: AWS にサインアップする
- 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: AWS にサインアップする

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

AWS アカウント へのサインアップ

AWS アカウント がない場合は、以下のステップを実行して作成します。

AWS アカウントにサインアップするには

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、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   AWS アカウント にサインアップすると、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。

サインアップ処理が完了すると、AWS からユーザーに確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] 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

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

AWS アカウントのルートユーザー をセキュリティで保護する

1. [ルートユーザー] を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS マネジメントコンソール 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」で AWS アカウントのルートユーザーの仮想 MFA デバイスを有効にする方法 (コンソール) を確認してください。

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。

   IAM アイデンティティセンターディレクトリ をアイデンティティソースとして使用するチュートリアルについては、「AWS IAM Identity Center ユーザーガイド」の「 Configure user access with the default IAM アイデンティティセンターディレクトリ」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 アイデンティティセンター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 User Guide」の「Signing in to the AWS access portal」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「Add groups」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. 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. [First location service provider] で、専用接続の Direct Connect の適切な場所を選択します。

   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. [Second location service provider] で、Direct Connect の適切な場所を選択します。

   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。

AWS がお客様の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するまでに、最大 72 営業時間かかることがあります。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。この E メールは、 へのサインアップ時に使用した 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、VPC 外の AWS のパブリック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。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
接続	仮想インターフェイスを作成している Direct Connect 接続または Link Aggregation Group (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している場合は、そのアカウントの AWS アカウント ID が必要です。

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) 接続	同じ AWS リージョン内の VPC への接続には、VPC 用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、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 パートナーが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 任意のパブリックIP (顧客所有または AWS 提供) を使用できますが、お客様のピア 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、/31 の範囲 (203.0.113.0/31 など) を割り当てると、お客様のピア IP に 203.0.113.0 を使用し、AWS ピア IP に 203.0.113.1 を使用できます。また、/24 の範囲 (198.51.100.0/24 など) を割り当てると、お客様のピア IP に 198.51.100.10 を使用し、AWS ピア IP に 198.51.100.20 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 認可 • AWS 提供/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 当社は、AWS 提供パブリック IPv4 アドレスのすべてのリクエストを満たすことができるとは保証できません。 • (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。ご自身で指定する場合は、必ずルー

リソース	必要な情報
	ターインターフェイスと AWS Direct Connect インターフェイスのプライベート CIDR のみを指定してください。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ースと同様に、お客様のピア 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、`/30` の範囲 (`192.168.0.0/30` など) を割り当てると、お客様のピア IP に `192.168.0.1` を使用し、AWS ピア IP に `192.168.0.2` 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 4294967294 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: 次のいずれかに当てはまる場合は、IPv4 CIDR が Direct Connect を使用してアナウンス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。
	  • CIDR が異なる AWS リージョンからのものである。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。
	• Direct Connect パブリック仮想インターフェイスでは、IPv4 の場合は /1 ~ /32、IPv6 の場合は /1 ~ /64 の任意のプレフィックス長を指定できます。
	• 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。

(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み) ジャンボフレーム	経由のパケットの最大送信単位 (MTUDirect 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 Direct Connect から伝達されるルートにのみ適用されます。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、それを Direct Connect コンソールで選択し、仮想インターフェイスの [General configuration] (一般的な設定) ページで [Jumbo frame capable] (ジャンボフレーム対応) を見つけます。

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 営業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. 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 1～4294967294 です。これには、ASN (1～2147483647) とロング ASN (1～4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。
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. 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. [Virtual interface owner] (仮想インターフェイスの所有者) で、[Another AWS account] を選択してから、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 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。

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 Direct Connect 仮想インターフェイスを設定する際には、RFC 1918 を使用して独自の IP アドレスを指定するか、他のアドレス指定スキームを使用するか、ポイントツーポイント接続用に RFC 3927 169.254.0.0/16 IPv4 リンクローカル範囲から割り当てられた、AWS 割り当ての IPv4 /29 CIDR アドレスを選択することができます。これらのポイントツーポイント接続は、カスタマーゲートウェイルーターと Direct Connect エンドポイント間の eBGP ピアリングにのみ使用する必要があります。AWS サイト間プライベート IP VPN や Transit Gateway Connect などの VPC トラフィックまたはトンネリング目的の場合、AWS は、ポイントツーポイント接続の代わりに、カスタマーゲートウェイルーターのループバックまたは LAN インターフェイスを送信元アドレスまたは送信先アドレスとして使用することをお勧めします。
>
> - 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) [Enable SiteLink] (SiteLink の有効化) で [Enabled] (有効) を選択して、Direct Connect の POP (Point Of Presence) 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、設定が回復性の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 “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作成したら、次の手順を実行して 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検証するには

- `traceroute` を実行し、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。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。

AWS Direct Connect Resiliency Toolkit を使用して Direct Connect が高い回復性を備えるように設定する

この例では、Direct Connect Resiliency Toolkit を使用して、高回復性モデルを設定します。

タスク

- ステップ 1: AWS にサインアップする
- 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: AWS にサインアップする

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

AWS アカウント へのサインアップ

AWS アカウント がない場合は、以下のステップを実行して作成します。

AWS アカウントにサインアップするには

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、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

AWS アカウント にサインアップすると、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。

サインアップ処理が完了すると、AWS からユーザーに確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] 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

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

AWS アカウントのルートユーザー をセキュリティで保護する

1. [ルートユーザー] を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS マネジメントコンソール 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」で AWS アカウントのルートユーザーの仮想 MFA デバイスを有効にする方法 (コンソール) を確認してください。

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。

IAM アイデンティティセンターディレクトリ をアイデンティティソースとして使用するチュートリアルについては、「AWS IAM Identity Center ユーザーガイド」の「Configure user access with the default IAM アイデンティティセンターディレクトリ」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 アイデンティティセンター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 User Guide」の「Signing in to the AWS access portal」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「Add groups」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. 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. [First location service provider] で、Direct Connect の適切な場所を選択します。

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. [Second location service provider] で、Direct Connect の適切な場所を選択します。

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。

   AWS がお客様の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するまでに、最大 72 営業時間かかることがあります。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。この E メールは、 へのサインアップ時に使用した 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、VPC 外の AWS のパブリック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。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
接続	仮想インターフェイスを作成している Direct Connect 接続または Link Aggregation Group (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している場合は、そのアカウントの AWS 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 リージョン内の VPC への接続には、VPC 用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、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 パートナーが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 任意のパブリックIP (顧客所有または AWS 提供) を使用できますが、お客様のピア 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、/31 の範囲 (203.0.113.0/31 など) を割り当てると、お客様のピア IP に 203.0.113.0 を使用し、AWS ピア IP に 203.0.113.1 を使用できます。また、/24 の範囲 (198.51.100.0/24 など) を割り当てると、お客様のピア IP に 198.51.100.10 を使用し、AWS ピア IP に 198.51.100.20 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 認可 • AWS 提供/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 当社は、AWS 提供パブリック IPv4 アドレスのすべてのリクエストを満たすことができるとは保証できません。 • (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。ご自身で指定する場合は、必ずルー

リソース	必要な情報
	ターインターフェイスと AWS Direct Connect インターフェイスのプライベート CIDR のみを指定してください。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ースと同様に、お客様のピア 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、`/30` の範囲 (`192.168.0.0/30` など) を割り当てると、お客様のピア IP に `192.168.0.1` を使用し、AWS ピア IP に `192.168.0.2` 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 4294967294 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: 次のいずれかに当てはまる場合は、IPv4 CIDR が Direct Connect を使用してアナウンス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。
	  • CIDR が異なる AWS リージョンからのものである。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。
	• Direct Connect パブリック仮想インターフェイスでは、IPv4 の場合は /1 ~ /32、IPv6 の場合は /1 ~ /64 の任意のプレフィックス長を指定できます。
	• 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。

(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み) ジャンボフレーム	経由のパケットの最大送信単位 (MTUDirect 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 Direct Connect から伝達されるルートにのみ適用されます。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、それを Direct Connect コンソールで選択し、仮想インターフェイスの [General configuration] (一般的な設定) ページで [Jumbo frame capable] (ジャンボフレーム対応) を見つけます。

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、AWS 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。

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 営業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. 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 1～4294967294 です。これには、ASN (1～2147483647) とロング ASN (1～4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。
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. 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. [Virtual interface owner] (仮想インターフェイスの所有者) で、[Another AWS account] を選択してから、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 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。

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 Direct Connect 仮想インターフェイスを設定する際には、RFC 1918 を使用して独自の IP アドレスを指定するか、他のアドレス指定スキームを使用するか、ポイントツーポイント接続用に RFC 3927 169.254.0.0/16 IPv4 リンクローカル範囲から割り当てられた、AWS 割り当ての IPv4 /29 CIDR アドレスを選択することができます。これらのポイントツーポイント接続は、カスタマーゲートウェイルーターと Direct Connect エンドポイント間の eBGP ピアリングにのみ使用する必要があります。AWS サイト間プライベート IP VPN や Transit Gateway Connect などの VPC トラフィックまたはトンネリング目的の場合、AWS は、ポイントツーポイント接続の代わりに、カスタマーゲートウェイルーターのループバックまたは LAN インターフェイスを送信元アドレスまたは送信先アドレスとして使用することをお勧めします。
>
> - 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) [Enable SiteLink] (SiteLink の有効化) で [Enabled] (有効) を選択して、Direct Connect の POP (Point Of Presence) 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、設定が回復性の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 “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作成したら、次の手順を実行して 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検証するには

- `traceroute` を実行し、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。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。

AWS Direct Connect Resiliency Toolkit を使用して AWS Direct Connect が開発およびテスト環境の回復性を備えるように設定する

この例では、Direct Connect Resiliency Toolkit を使用して開発およびテストの回復性モデルを設定します。

タスク

- ステップ 1: AWS にサインアップする
- 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: AWS にサインアップする

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

AWS アカウント へのサインアップ

AWS アカウント がない場合は、以下のステップを実行して作成します。

AWS アカウントにサインアップするには

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、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

AWS アカウント にサインアップすると、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。

サインアップ処理が完了すると、AWS からユーザーに確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] 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

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

AWS アカウントのルートユーザー をセキュリティで保護する

1. [ルートユーザー] を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS マネジメントコンソール 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」で AWS アカウントのルートユーザーの仮想 MFA デバイスを有効にする方法 (コンソール) を確認してください。

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。

IAM アイデンティティセンターディレクトリ をアイデンティティソースとして使用するチュートリアルについては、「AWS IAM Identity Center ユーザーガイド」の「Configure user access with the default IAM アイデンティティセンターディレクトリ」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 アイデンティティセンター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 User Guide」の「Signing in to the AWS access portal」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「Add groups」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. 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. [First location service provider] で、Direct Connect の適切な場所を選択します。

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。

AWS がお客様の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するまでに、最大 72 営業時間かかることがあります。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。この E メールは、 へのサインアップ時に使用した 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

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、VPC 外の AWS のパブリック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。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
接続	仮想インターフェイスを作成している Direct Connect 接続または Link Aggregation Group (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している場合は、そのアカウントの AWS 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 リージョン内の VPC への接続には、VPC 用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、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 パートナーが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
	
	任意のパブリックIP (顧客所有または AWS 提供) を使用できますが、お客様のピア 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、/31 の範囲 (203.0.113.0/31 など) を割り当てると、お客様のピア IP に 203.0.113.0 を使用し、AWS ピア IP に 203.0.113.1 を使用できます。また、/24 の範囲 (198.51.100.0/24 など) を割り当てると、お客様のピア IP に 198.51.100.10 を使用し、AWS ピア IP に 198.51.100.20 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 認可
	  • AWS 提供/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
	当社は、AWS 提供パブリック IPv4 アドレスのすべてのリクエストを満たすことができるとは保証できません。
	  • (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。ご自身で指定する場合は、必ずルーターインターフェイスと AWS Direct Connect インターフェイスのプライベート CIDR のみを指定してください。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ースと同様に、お客様のピア 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、/30 の範囲 (192.168.0.0/30 など) を割り当てると、お客様のピア IP に

リソース	必要な情報
	`192.168.0.1` を使用し、AWS ピア IP に `192.168.0.2` 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 4294967294 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: 次のいずれかに当てはまる場合は、IPv4 CIDR が Direct Connect を使用してアナウンス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。
	  • CIDR が異なる AWS リージョンからのものである。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。
	• Direct Connect パブリック仮想インターフェイスでは、IPv4 の場合は /1 ~ /32、IPv6 の場合は /1 ~ /64 の任意のプレフィックス長を指定できます。
	• 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。

(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み) ジャンボフレーム	経由のパケットの最大送信単位 (MTUDirect 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 Direct Connect から伝達されるルートにのみ適用されます。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、それを Direct Connect コンソールで選択し、仮想インターフェイスの [General configuration] (一般的な設定) ページで [Jumbo frame capable] (ジャンボフレーム対応) を見つけます。

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 営業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. 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 1～4294967294 です。これには、ASN (1～2147483647) とロング ASN (1～4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。
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. 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. [Virtual interface owner] (仮想インターフェイスの所有者) で、[Another AWS account] を選択してから、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 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。

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 Direct Connect 仮想インターフェイスを設定する際には、RFC 1918 を使用して独自の IP アドレスを指定するか、他のアドレス指定スキームを使用するか、ポイントツーポイント接続用に RFC 3927 169.254.0.0/16 IPv4 リンクローカル範囲から割り当てられた、AWS 割り当ての IPv4 /29 CIDR アドレスを選択することができます。これらのポイントツーポイント接続は、カスタマーゲートウェイルーターと Direct Connect エンドポイント間の eBGP ピアリングにのみ使用する必要があります。AWS サイト間プライベート IP VPN や Transit Gateway Connect などの VPC トラフィックまたはトンネリング目的の場合、AWS は、ポイントツーポイント接続の代わりに、カスタマーゲートウェイルーターのループバックまたは LAN インターフェイスを送信元アドレスまたは送信先アドレスとして使用することをお勧めします。
>
> - 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) [Enable SiteLink] (SiteLink の有効化) で [Enabled] (有効) を選択して、Direct Connect の POP (Point Of Presence) 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、設定が回復性の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 “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作成したら、次の手順を実行して 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検証するには

- `traceroute` を実行し、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。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。

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**
>
> メンテナンス中またはメンテナンス後に BGP セッションが早期に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この機能を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します。”」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。

トピック

- AWS Direct Connect Resiliency Toolkit 仮想インターフェイスフェイルオーバーテストを開始する
- AWS Direct Connect Resiliency Toolkit 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します。
- AWS Direct Connect Resiliency Toolkit 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します。

AWS Direct Connect Resiliency Toolkit 仮想インターフェイスフェイルオーバーテストを開始する

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

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. 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 営業時間) 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

StartBgpFailoverTest を使用します。

AWS Direct Connect Resiliency Toolkit 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します。

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、Direct Connect コンソールまたは AWS CLI を使用して表示できます。

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. 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

ListVirtualInterfaceTestHistory を使用します。

AWS Direct Connect Resiliency Toolkit 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します。

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

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. 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

StopBgpFailoverTest を使用します。

Direct Connect Classic 接続

Classic 接続は、オンプレミスインフラストラクチャと AWS 間の専用ネットワーク接続を確立するための簡単なアプローチを提供します。この接続タイプは、独自のネットワーク設定を管理し、既存の Direct Connect インフラストラクチャを導入することを希望する組織に最適です。Classic 接続は AWS Direct Connect Resiliency Toolkit に依存しません。

既存の接続があり、さらに接続を追加する場合は、Classic を選択します。Classic 接続の SLA は 95% です。ただし、レジリエンシーや冗長性は提供されません。これらは、接続を作成するときに AWS Direct Connect Resiliency Toolkit でのみ提供されます。

> **Note**
>
> Classic 接続を設定する前に、「接続の前提条件」についてよく理解しておいてください。

タスク

- Direct Connect Classic 接続を設定する

Direct Connect Classic 接続を設定する

既存の Direct Connect 接続がある場合は、Classic 接続を設定します。

ステップ 1: AWS にサインアップする

Direct Connect を使用するにはアカウントが必要です (まだお持ちでない場合)。

AWS アカウント へのサインアップ

AWS アカウント がない場合は、以下のステップを実行して作成します。

AWS アカウントにサインアップするには

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、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

AWS アカウント にサインアップすると、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。

サインアップ処理が完了すると、AWS からユーザーに確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] 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

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

AWS アカウントのルートユーザー をセキュリティで保護する

1. [ルートユーザー] を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS マネジメントコンソール 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」で AWS アカウントのルートユーザーの仮想 MFA デバイスを有効にする方法 (コンソール) を確認してください。

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。

IAM アイデンティティセンターディレクトリ をアイデンティティソースとして使用するチュートリアルについては、「AWS IAM Identity Center ユーザーガイド」の「 Configure user access with the default IAM アイデンティティセンターディレクトリ」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 アイデンティティセンター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 User Guide」の「Signing in to the AWS access portal」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「Add groups」を参照してください。

ステップ 2: Direct Connect 専用接続をリクエストする

専用接続では、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。ホスト接続では、AWS Direct Connect パートナーと連携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。
- 接続が終了する Direct Connect ロケーション。

> **Note**
>
> 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。その代わりに、ホスト接続を作成できる AWS Direct Connect パートナーにお問い合わせください。その後、接続に同意します。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 Direct Connect 接続を作成するには

1. 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 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. 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 Direct Connect partner] (パートナー経由で接続する) を選択します。

   f. [Service provider] (サービスプロバイダー) には 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。

AWS がお客様の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するまでに、最大 72 営業時間かかることがあります。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。この E メールは、 へのサインアップ時に使用した 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、「Direct Connect 専用接続とホスト接続」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の作成前に、そのホスト接続を Direct Connect コンソールで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。

ホスト型仮想インターフェイスを承諾するには

1. 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 AWS に接続するための認可であり、クロスネットワーク接続 (クロスコネクト) を確立するために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で必要になります。

LOA-CFA のダウンロード方法

1. 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 営業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、そのパートナーかプロバイダーに LOA-CFA を送信し、Direct Connect ロケーションでのクロスコネクトを注文できるようにします。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。
   - 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ます。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、ネットワークへの接続に必要な情報をコロケーションプロバイダーに提示する必要もあります。

Direct Connect複数のサイト (たとえば、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 Direct Connect ロケーションとして処理されます。高可用性を実現するために、別の 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) の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

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 外の AWS のパブリック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
接続	仮想インターフェイスを作成している Direct Connect 接続または Link Aggregation Group (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している場合は、そのアカウントの AWS 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 リージョン内の VPC への接続には、VPC 用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、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 パートナーが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 任意のパブリックIP (顧客所有または AWS 提供) を使用できますが、お客様のピア 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、/31 の範囲 (203.0.113.0/31 など) を割り当てると、お客様のピア IP に 203.0.113.0 を使用し、AWS ピア IP に 203.0.113.1 を使用できます。また、/24 の範囲 (198.51.100.0/24 など) を割り当てると、お客様のピア IP に 198.51.100.10 を使用し、AWS ピア IP に 198.51.100.20 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 認可 • AWS 提供/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 当社は、AWS 提供パブリック IPv4 アドレスのすべてのリクエストを満たすことができるとは保証できません。 • (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。ご自身で指定する場合は、必ずルー

リソース	必要な情報
	ターインターフェイスと AWS Direct Connect インターフェイスのプライベート CIDR のみを指定してください。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ースと同様に、お客様のピア 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、`/30` の範囲 (`192.168.0.0/30` など) を割り当てると、お客様のピア IP に `192.168.0.1` を使用し、AWS ピア IP に `192.168.0.2` 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 4294967294 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: 次のいずれかに当てはまる場合は、IPv4 CIDR が Direct Connect を使用してアナウンス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。
	  • CIDR が異なる AWS リージョンからのものである。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。
	• Direct Connect パブリック仮想インターフェイスでは、IPv4 の場合は /1 ~ /32、IPv6 の場合は /1 ~ /64 の任意のプレフィックス長を指定できます。
	• 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。

(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み) ジャンボフレーム	経由のパケットの最大送信単位 (MTUDirect 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 Direct Connect から伝達されるルートにのみ適用されます。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、それを Direct Connect コンソールで選択し、仮想インターフェイスの [General configuration] (一般的な設定) ページで [Jumbo frame capable] (ジャンボフレーム対応) を見つけます。

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。プライベート仮想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、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。

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 営業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. 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 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれま

す。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。

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. 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. [Virtual interface owner] (仮想インターフェイスの所有者) で、[Another AWS account] を選択してから、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 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) と ロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN と ロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。

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 Direct Connect 仮想インターフェイスを設定する際には、RFC 1918 を使用して独自の IP アドレスを指定するか、他のアドレス指定スキームを使用するか、ポイントツーポイント接続用に RFC 3927 169.254.0.0/16 IPv4 リンクローカル範囲から割り当てられた、AWS 割り当ての IPv4 /29 CIDR アドレスを選択することができます。これらのポイントツーポイント接続は、カスタマーゲートウェイルー

ターと Direct Connect エンドポイント間の eBGP ピアリングにのみ使用する必要があります。AWS サイト間プライベート IP VPN や Transit Gateway Connect などの VPC トラフィックまたはトンネリング目的の場合、AWS は、ポイントツーポイント接続の代わりに、カスタマーゲートウェイルーターのループバックまたは LAN インターフェイスを送信元アドレスまたは送信先アドレスとして使用することをお勧めします。

- 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) [Enable SiteLink] (SiteLink の有効化) で [Enabled] (有効) を選択して、Direct Connect の POP (Point Of Presence) 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

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します。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. 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 Direct Connect に接続できることを確認します。

ルーターを手動で設定する方法の詳細については、「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。

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、Direct Connect デバイスのピア IP アドレスに対して ping を送信できない場合は、「レイヤー 2 (データリンク層) の問題のトラブルシューティング」を参照してください。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) の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作成したら、次の手順を実行して 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検証するには

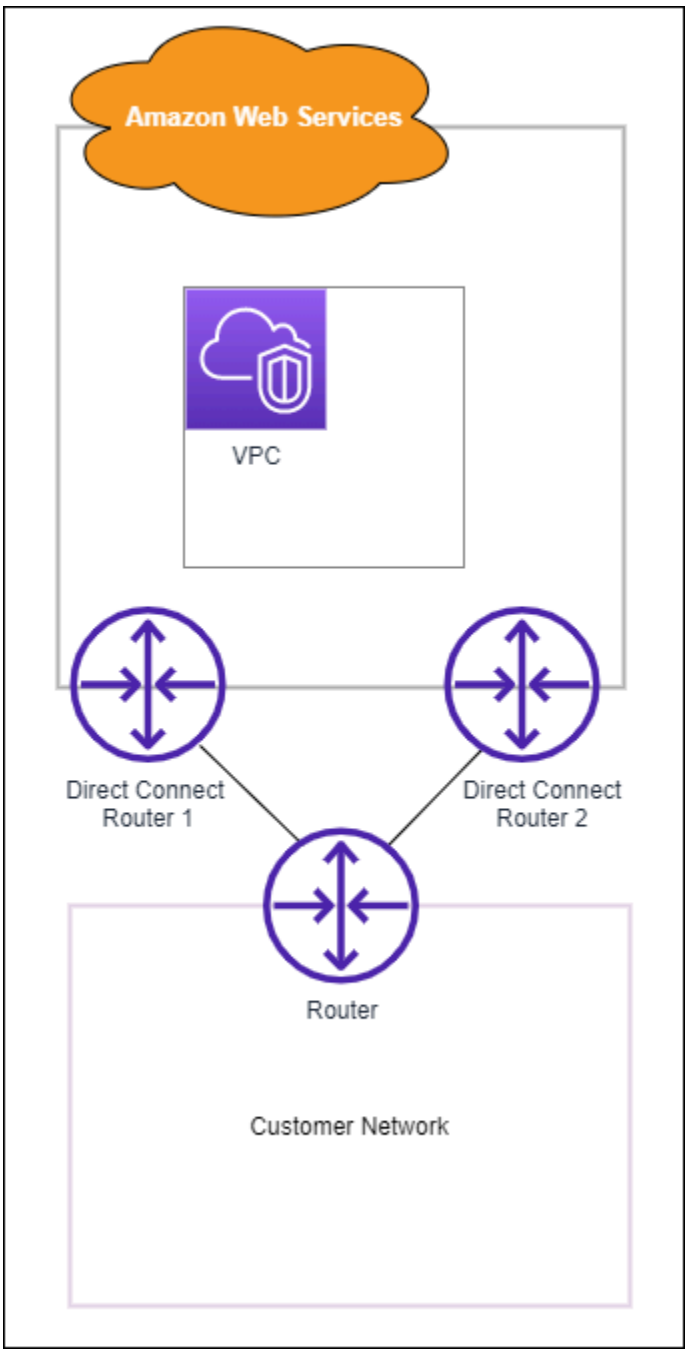
- `traceroute` を実行し、Direct Connect 識別子がネットワークトレースにあることを確認します。

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。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提供するため、下の図にあるように、AWS への専用接続を 2 つ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なデフォルト設定です。Direct Connect 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負荷共有されます。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ために、別の Direct Connect ロケーションへの接続を設定することを強くお勧めします。

Direct Connect の回復性についての詳細は、「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 のメンテナンス

Direct Connect は、サービスのセキュリティ、可用性、およびスケーラビリティの確保に取り組んでいます。これらの標準を維持するには、ハードウェアネットワークデバイスの定期的なメンテナンスが必要です。Direct Connect のメンテナンスには、計画的と緊急の 2 種類があります。

これらのメンテナンスイベントには、セキュリティの脆弱性とハードウェアの問題への対応、ハードウェアの問題、標準に準拠するためのデバイス移行の実行、欠陥の修正、新機能の提供が含まれます。「メンテナンスイベントの準備」で説明されているプラクティスに従うことで、メンテナンスイベント中の中断を避けられるよう Direct Connect 環境をより適切に準備できます。回復力のないネットワーク設定や単一の接続がある場合は、オンプレミスネットワークと AWS リソース間の接続が中断されます。

Direct Connect は、Direct Connect 接続または仮想インターフェイスリソースを所有する AWS アカウントに関連付けられているメールアドレスに、計画的メンテナンスイベントと緊急メンテナンスイベントに関するメール通知を送信します。お客様がいずれかの Direct Connect デリバリーパートナーと共同で Direct Connect ホスト接続を使用している場合、メンテナンスイベントに関するメール通知はお客様とパートナーアカウントの両方に送信されます。通知を受け取るメールアドレスまたはディストリビューションリストを追加することもできます。詳細については、「AWS アカウントの代替連絡先の更新」を参照してください。

メンテナンスイベント

- Direct Connect の計画的メンテナンス
- Direct Connect の緊急メンテナンス
- サードパーティーのメンテナンス
- メンテナンスイベントの準備
- メンテナンスイベントの延期またはキャンセルのリクエスト

Direct Connect の計画的メンテナンス

計画的メンテナンスイベントには、可用性の向上と新機能の提供に必要なネットワークアップグレード (オペレーティングシステムのパッチ適用やハードウェアデバイスエンドポイントの設定更新など) が含まれます。

これらのメンテナンスイベントは 14 日前にスケジュールされ、通常はデバイスエンドポイントが存在する Direct Connect ロケーションでトラフィックが少ない時間帯に 4 時間の時間枠で実行されま

す。メンテナンスアクティビティは通常、4 時間の時間枠が完全に終了する前に完了し、作業が完了するとお客様に通知が届きます。まれに、予期しない状況が発生してメンテナンス期間の延長が必要になる場合、当社は改訂された完了見積もりが記載された通知を別途送信します。

最初の通知とリマインダー通知は、以下のスケジュールに従ってリソースを所有する AWS アカウントに送信されます。

- 計画的メンテナンスイベントの 14 暦日前
- 計画的メンテナンスイベントの 7 暦日前
- 計画的メンテナンスイベントの 1 日前

> **Note**
>
> 暦日には、非営業日と現地の祝日が含まれます。

加えて、

- AWS Health と統合すると、お使いのモニタリングシステムまたはチケットシステムに通知が届きます。AWS Health を統合するには、「AWS Health ユーザーガイド」の「「Amazon EventBridge を使用して AWS Health のイベントをモニタリングする」を参照してください。
- AWS Health Dashboard に計画的メンテナンスのスケジュールが表示されます。

まれに、計画的メンテナンスイベントをスケジュールどおりに実行できない状況が発生することがあります。これが発生した場合、当社はキャンセル通知を送信し、上記と同じプロセスに従って今後のイベントを再スケジュールします。

Direct Connect の緊急メンテナンス

緊急メンテナンスイベントは、サービスに影響を及ぼす差し迫ったイベントを防止したり、既に接続の中断を引き起こしている障害を解決したりするために、緊急ベースで開始されます。このような場合は、影響を受けているエンドポイントを正常な状態に復元するためにすぐにアクションを実行する必要があります。

当社は、可能な限り事前に通知するよう努めますが、状況によってはメンテナンスをすぐに開始しなければならない場合があります。緊急メンテナンスがスケジュールされるか、既に開始されたとき、および完了したときにお客様に通知が届きます。

これらのイベントは通常、デバイスエンドポイントが存在する Direct Connect ロケーションで 2 時間の時間枠で実行されます。メンテナンスアクティビティは通常、この時間枠内に完了します。予期しない状況 (ハードウェアの交換など) が発生してメンテナンス期間の延長が必要になる場合、当社は改訂された完了見積もりが記載された通知を別途送信します。

サードパーティーのメンテナンス

AWS によって開始されたメンテナンスイベントに加えて、お客様のオンプレミスから Direct Connect ロケーションへのネットワーク接続を提供している Direct Connect デリバリーパートナーまたはネットワークサービスプロバイダーがメンテナンスアクティビティを実行する場合があります。Direct Connect デリバリーパートナーは、AWS からメンテナンスイベント通知を受け取ります。これにより、パートナーは、重複を避けて独自のメンテナンススケジュールを計画できます。AWS はパートナーのメンテナンスアクティビティを把握できないため、お客様はパートナーのスケジューリングプロセス、通知方法、およびベストプラクティスについてパートナーに確認する必要があります。

メンテナンスイベントの準備

Direct Connect では、メンテナンスイベント中に本稼働ワークロードが機能し続けられるように、AWS Direct Connect Resiliency Toolkit を使用して、お使いのネットワーク接続が最大限の回復性を備えるように設定することをお勧めします。最大回復性モデルの例については、「最大回復性」を参照してください。

最大限の回復性では、接続は 2 つ以上の Direct Connect ロケーションに分散され、各 Direct Connect ロケーション内にある 2 つの一意のデバイスエンドポイントで終了します。これにより、複数の冗長性レイヤーが提供され、単一エンドポイントの障害のリスクが軽減されるとともに、メンテナンスイベント中に接続を維持することが可能になります。Direct Connect は、複数の冗長接続を同時に停止させる計画的メンテナンスイベントをスケジュールすることは決してありません。AWS Direct Connect Resiliency Toolkit を使用して最大限の回復性を設定する手順については、「最大限の回復性を設定する」を参照してください。

計画的メンテナンスイベント中、Direct Connect はメンテナンス中の接続エンドポイントとの間で送受信されるトラフィックをドレインし、トラフィックに冗長接続を使用するよう強制します。これにより、最大限の回復性が設定されていない場合の手動介入を必要とせずに、よりシームレスなネットワークトラフィックの再ルーティングが可能になります。または、ローカル優先設定のボーダーゲートウェイプロトコル (BGP) コミュニティを使用して、メンテナンス期間中の冗長接続間のトラフィック再ルーティングを制御することもできます。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。

最大回復性モデルを使用して Direct Connect 環境を設定することで、メンテナンスイベントやインフラストラクチャの障害の際にビジネスが影響が受けないようにすることができます。適切に実装およびテストされている場合、通常はこれらのメンテナンスイベントについて何らかのアクションを実行する必要はありません。

回復性の検証

Direct Connect 環境が回復性を備えるように設定している場合は、接続が中断されたときにトラフィックが他の冗長接続を介してルーティングされることを定期的に検証します。定期的なプロアクティブテストは、実際のメンテナンスイベントまたは障害シナリオの際に潜在的な問題が本番稼働ワークロードに影響を与える前に、それらの問題を特定して解決するのに役立ちます。これにより、メンテナンスイベント中のネットワークの信頼性に対する自信が高まります。Direct Connect フェイルオーバーテストを使用して、冗長接続の回復性を検証します。Direct Connect フェイルオーバーテストを使用する手順については、「Direct Connect フェイルオーバーテスト」を参照してください。

Amazon CloudWatch Network Monitor を活用して、Direct Connect 接続をアクティブにモニタリングすることもできます。詳細については、「Amazon CloudWatch Network Synthetic Monitor によるハイブリッド接続のモニタリング」を参照してください。

メンテナンスイベントの延期またはキャンセルのリクエスト

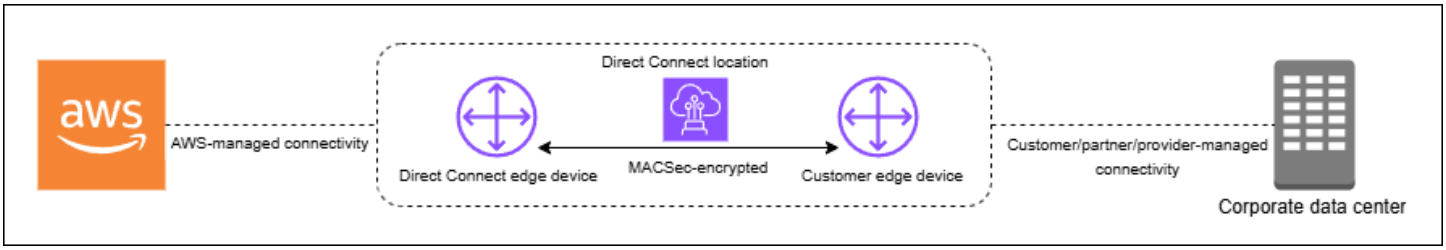
Direct Connect デバイスは複数のお客様の間で共有されます。そのため、当社はメンテナンスの再スケジュールやキャンセルに関する特定のリクエストには対応していません。あるお客様のリクエストを再スケジュールまたはキャンセルすると、そのエンドポイントを使用している他のお客様に悪影響が及ぶ可能性があります。また、可用性やセキュリティの問題をタイムリーに軽減する上でリスクが生じる可能性もあります。

Direct Connect における 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、AWS へのクロス接続でレイヤー 2 のポイントツーポイント暗号化を提供し、2 つのレイヤー 3 ルーター間で動作します。MACsec は、ルーターと Direct Connect ロケーション間の接続をレイヤー 2 で保護します。一方、AWS は、データが Direct Connect ロケーションと AWS リージョン間のネットワークを流れるときに物理レイヤーですべてのデータを暗号化することで、セキュリティを強化します。これにより、トラフィックが最初に AWS に入るときと AWS ネットワークを通過するときの両方で保護される階層的セキュリティアプローチが実現します。

次の図では、Direct Connect クロス接続コネクトはお客様のエッジデバイスの MACsec 対応インターフェイスに接続されている必要があります。Direct Connect 経由の MACsec は、Direct Connect エッジデバイスとお客様のエッジデバイス間のポイントツーポイントトラフィックにレイヤー 2 暗号化を提供します。この暗号化は、クロス接続の両端のインターフェイス間でセキュリティキーが交換および検証された後に行われます。

> **Note**
>
> MACsec は、イーサネットリンク上でポイントツーポイントのセキュリティを提供します。そのため、複数のシーケンシャルイーサネットまたは他のネットワークセグメントにまたがってエンドツーエンドの暗号化を提供することはありません。



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。

- セキュア関連付けキー (SAK) – お客様側のオンプレミスルーターと Direct Connect ロケーションにある接続ポートの間で、MACsec 接続を確立するセッションキー。SAK は事前共有ではなく、暗号化キー生成プロセスを通じて CKN/CAK ペアから自動的に派生します。この派生は、お客様が CKN/CAK ペアを指定してプロビジョニングした後に接続の両端で行われます。SAK は、MACsec セッションが確立されるたびに、セキュリティ目的で定期的に再生成されます。
- 接続関連付けキー名 (CKN) と接続関連付けキー (CAK) – このペアの値は、MACsec キーを生成するために使用されます。お客様はこのペア値を生成し、Direct Connect 接続に関連付けた上で、Direct Connect 接続の終端にあるエッジデバイスにそれらをプロビジョニングします。Direct Connect では、静的 CAK モードのみがサポートされ、動的 CAK モードはサポートされません。静的 CAK モードのみがサポートされるため、キーの生成、配布、ローテーションについては独自のキー管理ポリシーに従うことをお勧めします。
- キー形式 – キー形式は、16 進数文字を使用し、正確に 64 文字で指定する必要があります。Direct Connect では、64 文字の 16 進文字列に対応する、専用接続用の Advanced Encryption Standard (AES) 256 ビットキーのみがサポートされます。
- 暗号化モード – Direct Connect では、次の 2 つの MACsec 暗号化モードがサポートされます。
  - must_encrypt – このモードでは、接続はすべてのトラフィックに MACsec 暗号化が必要です。MACsec ネゴシエーションが失敗するか、暗号化を確立できない場合、接続はトラフィックを一切送信しません。このモードは最高のセキュリティ保証を提供しますが、MACsec 関連の問題がある場合には、可用性に影響を与える可能性があります。
  - should_encrypt – このモードでは、接続は MACsec 暗号化を確立しようとしますが、MACsec ネゴシエーションが失敗した場合には、暗号化されていない通信にフォールバックします。このモードでは、柔軟性と可用性が向上しますが、特定の障害シナリオで暗号化されていないトラフィックが許可される可能性があります。

  暗号化モードは、接続を設定するときに設定でき、後で変更できます。デフォルトでは、新しい MACsec 対応接続は、初期設定時の潜在的な接続の問題を防止するために、「should_encrypt」モードに設定されます。

MACsec キーローテーション

- CNN/CAK ローテーション (手動)

  Direct Connect MACsec は、最大 3 つの CKN/CAK ペアを保存できる容量を持つ MACsec キーチェーンをサポートします。これにより、お客様は接続を中断することなく、これらの長期キーを手動でローテーションできます。`associate-mac-sec-key` コマンドを使用して新しい CKN/CAK ペアを関連付ける場合は、デバイスで同じペアを設定する必要があります。Direct Connect

デバイスは、最後に追加されたキーを使用しようとします。そのキーがデバイスのキーに一致しない場合は、以前の使用可能キーにフォールバックし、ローテーション時の接続の安定性を確保します。

`associate-mac-sec-key` の使用については、「associate-mac-sec-key」を参照してください。

- セキュア関連付けキー (SAK) のローテーション (自動)

  アクティブな CKN/CAK ペアから派生した SAK は、以下の条件に基づいて自動的にローテーションされます。

  - 時間間隔
  - 暗号化されるトラフィックの量
  - MACsec セッションの確立

  このローテーションは、プロトコルによって自動的に処理され、接続の中断なしに透過的に行われます。手動による介入は必要ありません。SAK は永続的に保存されることはなく、IEEE 802.1X 標準に従った安全なキー派生プロセスを通じて再生成されます。

サポートされている接続

MACsec は、専用 Direct Connect 接続と Link Aggregation Group で使用できます。

サポートされている MACsec 接続

- 専用接続
- LAG
- パートナー相互接続

> **Note**
>
> サポート対象デバイスを使用しているパートナーは、MACsec を使用して、エッジネットワークデバイスと Direct Connect デバイス間のレイヤー 2 接続を暗号化できます。この機能を有効にしているパートナーは、保護されたリンクを通過するすべてのトラフィックを暗号化できます。MACsec 暗号化は、レイヤー 2 の 2 つの特定のデバイス間で動作し、ホスト接続ではサポートされません。

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

以下は、Direct Connect 専用接続の MACsec をより良く理解するために役立ちます。MACsec の使用には追加料金はかかりません。専用接続で MACsec を設定する手順は、「専用接続で MacSec の使用を開始する」を参照してください。

パートナー相互接続オペレーションは、専用接続と同じ手順に従います。パートナー相互接続に対して CLI または SDK コマンドを実行すると、レスポンスに MACsec 関連情報が含まれます (該当する場合)。

専用接続の MACsec 前提条件

専用接続では、次の MACsec の要件に注意してください。

- MACsec は、選択された POP (Point Of Presence) において、10Gbps、100Gbps、および 400Gbpsの専用 Direct Connect 接続でサポートされています。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 接続の場合、GCM-AES-256 および GCM-AES-XPN-256。
  - 100 Gbps、400 Gbps 接続の場合、GCM-AES-XPN-256。
- 256 ビット MACsec キーのみがサポートされています。
- 100 Gbps および 400 Gbps 接続には、拡張パケット番号付け (XPN) が必要です。10Gbps 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 専用接続や 400 Gbps 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枯渇してしまうため、新しい接続アソシエーションを確立するために数分ごとに暗号鍵を口ーテーションする必要があります。この状況を回避するため、IEEE Std 802.1AEbw -2013 修正では、拡張パケット番号付けが導入され、番号付けスペースが 64 ビットに拡大され、キー口ーテーションの適時性要件が緩和されました。
- 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/dot1q-in-clear は、暗号化されたペイロードの外部への VLAN タグの移動ではサポートされていません。

さらに、専用接続で MACsec の設定を行う前に、以下のタスクを完了する必要があります。

- MACsec 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 "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。

LAG

次の要件は、Direct Connect Link Aggregation Group (LAG) の MACsec を理解するのに役立ちます。

- LAG は、MACsec 暗号化をサポートする MACsec 対応専用接続で構成されている必要があります。
- LAG 内の接続はすべて同じ帯域幅で、MACsec をサポートしている必要があります。
- MACsec 設定は、LAG 内のすべての接続に均一に適用されます。
- LAG 作成と MACsec を同時に有効にできます。
- すべての LAG リンクでいつでも使用できる MACsec キーは 1 つだけです。複数の MACsec キーをサポートする機能は、キーのローテーションのみを目的としています。

パートナー相互接続

相互接続を所有しているパートナーアカウントは、その物理接続または LAG で MACsec を使用できます。オペレーションは専用接続の場合と同じですが、パートナー固有の API/SDK 呼び出しを使用して実行します。

サービスにリンクされたロール

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、 に直接リンクされた一意のタイプの IAM ロールですDirect Connect サービスにリンクされたロールは、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 AWS の他のサービスを呼び出すために必要なすべてのアクセス許可を備えています。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、Direct Connect の設定が簡単になります。Direct Connect は、このサービスにリンクされた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、Direct

Connect のみがその口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。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 LAG に関連付ける事前共有されたキーに AWS マネージド CMK を使用します。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。

保存された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、7～30 日間隔で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。

Direct Connect 専用接続で MacSec の使用を開始する

次のタスクでは、Direct Connect 専用接続で使用する MACsec の設定を開始します。

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。

(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、「MacSec に関する考慮事項」および「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。

- MACSec CKN/CAK を接続に関連付ける
- 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。オンプレミスのルーターと Direct Connect ロケーションの MACsec シークレットキーが一致する必要があります。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。

(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

必要に応じて、CKN/CAK と接続または LAG 間での関連付けを削除できます。関連付けを削除する必要がある場合は、次のいずれかを参照してください。

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

Direct Connect 専用接続とホスト接続

Direct Connect を使用すると、お客様のネットワークと Direct Connect の 1 つの場所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ネット接続。お客様は、Direct Connect コンソール、CLI、または API を介して専用接続をリクエストできます。詳細については、「専用接続」を参照してください。
- ホスト接続: お客様に代わって AWS Direct Connect パートナーが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、「ホスト接続」を参照してください。

トピック

Direct Connect 専用接続

Direct Connect 専用接続を作成するには、次の情報が必要です。

Direct Connect の場所

AWS Direct Connect パートナープログラムのパートナーと連携して、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設置します。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、「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、100 Gbps、および 400 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 を使用して一度に 1 つずつ接続を作成できます。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。

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 (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 AWS に接続するための認可で、ネットワークプロバイダーがクロスコネクトを代行注文するために必要です。お客様の機器が Direct Connect ロケーションにない場合、そのロケーションでお客様は直接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。

- 接続ウィザードを使用して接続を作成する
- Classic 接続を作成する
- the section called “接続の詳細の表示”
- the section called “接続を更新する”
- 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 “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、「仮想インターフェイスとホスト型仮想インターフェイス」を参照してください。

Direct Connect ロケーションに設備がない場合は、まず AWS Direct Connect パートナープログラムで 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、「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 “専用接続の MACsec 前提条件”」を参照してください。

Letter of Authorization and Connecting Facility Assignment (LOA-CFA)

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。

ダウンロードした LOA には、AWS が発行した LOA の真正性を検証するためのデジタル署名と透かしが付与されています。LOA のデジタル署名と透かし。PDF ドキュメントは、変更された、もしくは不正の可能性がある LOA が Direct Connect サイトの施設プロバイダーによって処理されることを防ぎます。デジタル署名は、PDF を開いて署名パネルを確認することで認証できます。有効なドキュメントには、「Signature is valid」(署名は有効です) または「Document has not been modified since the signature was applied」(署名が適用されてからドキュメントは変更されていません) と表示されます。LOA の本文全体にパッチパネルとストランド模様の透かしが繰り返し挿入されています。この透かしは、視覚的であってもセキュリティを保証するものではなく真正性の指標として機能します。

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。

LOA-CFA をダウンロードする手順については、「LOA-CFA をダウンロードする」を参照してください。

> **Note**
>
> 料金の詳細については、「Direct Connect 料金表」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、「Direct Connect 接続を削除する」を参照してください。

トピック

- 接続ウィザードを使用して Direct Connect 専用接続を作成する
- Direct Connect Classic 接続を作成する
- Direct Connect LOA-CFA をダウンロードする
- MACSec CKN/CAK を Direct Connect 接続に関連付ける
- MACsec シークレットキーと Direct Connect 接続の間の関連付けを解除する

接続ウィザードを使用して Direct Connect 専用接続を作成する

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: 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. 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、the section called “AWS Direct Connect Resiliency Toolkit” を参照してください。
5. [次へ] を選択します。
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 400 Gbps までの範囲で設定できます。

   b. [ロケーション] で、適切な Direct Connect の場所を選択し、[First location service provider] を選択し、こ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。

c. [2 つめのロケーション] で、2 つめのロケーションの適切な Direct Connect を選択し、[Second location service provider] を選択し、この 2 つめ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。

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] を選択します。
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 “Letter of Authorization and Connecting Facility Assignment (LOA-CFA)” 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 (Direct Connect API)

Direct Connect Classic 接続を作成する

専用接続では、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。ホスト接続では、AWS Direct Connect パートナーと連携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。

- 接続が終了する Direct Connect ロケーション。

> **Note**
>
> 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。その代わりに、ホスト接続を作成できる AWS Direct Connect パートナーにお問い合わせください。その後、接続に同意します。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 Direct Connect 接続を作成するには

1. Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. [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 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 Direct Connect partner] (パートナー経由で接続する) を選択します。
9. [Service provider] (サービスプロバイダー) には 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。

AWS がお客様の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するまでに、最大 72 営業時間かかることがあります。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。この E メールは、 へのサインアップ時に使用した 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、「専用接続とホスト接続」を参照してください。

Direct Connect LOA-CFA をダウンロードする

LOA-CFA は、Direct Connect コンソールまたはコマンドラインを使用してダウンロードできます。LOA-CFA をダウンロードして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提供すると、そのプロバイダーはお客様に代わってクロスコネクトを注文できるようになります。

LOA-CFA のダウンロード方法

1. 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、「Direct Connect ロケーションのクロスコネクトのリクエスト」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 LOA-CFA をダウンロードするには

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

MACSec CKN/CAK を Direct Connect 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。関連付けを作成するには、Direct Connect コンソール、コマンドライン、または API を使用します。

> **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、「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。

MACsec キーを接続に関連付けるには

1. 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。

コマンドラインまたは API を使用して MACsec キーを接続に関連付けるには

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

MACsec シークレットキーと Direct Connect 接続の間の関連付けを解除する

接続と MACsec キー間の関連付けを削除するには、Direct Connect コンソール、コマンドライン、または API を使用します。

接続と MACsec キー間の関連付けを解除するには

1. 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。

コマンドラインまたは API を使用して接続と MACsec キー間の関連付けを解除するには

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

Direct Connect ホスト接続

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

Direct Connect の場所

AWS Direct Connect パートナープログラムの AWS Direct Connect パートナーと連携して、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設置します。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、「Direct Connect Delivery Partners」(デリバリーパートナー) を参照してください。

> **Note**
>
> 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 パートナーはお客様に代わってホスト接続を作成して設定することができます。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、「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、および 25 Gbps です。特定の要件を満たした 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 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 パートナーのみが変更できます。AWS Direct Connect パートナーが既存の接続のアップグレードまたはダウングレードをサポートしているかどうかを確認してください。パートナーが接続のアップグレード/ダウングレードをサポートしている場合、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。
- AWS は、ホスト接続でトラフィックポリシングを使用します。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、超過したトラフィックはドロップされます。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、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。

- 接続を削除
- 接続を更新する
- 接続の詳細の表示

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、「仮想インターフェイスとホスト型仮想インターフェイス」を参照してください。

Direct Connect ホスト接続を承認する

ホスト接続の購入をご希望の場合は、AWS Direct Connect パートナープログラムの AWS Direct Connect パートナーにお問い合わせ頂く必要があります。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、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。ホスト接続を承認するには、Direct Connect コンソール、コマンドライン、または API を使用します。

1. 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。

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 (Direct Connect API)

Direct Connect 接続を削除する

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、その接続のすべてのポートの時間料金が停止しますが、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可能性があります (下記参照)。Direct Connect データ転送料金は、仮想インターフェイスと関連しています。仮想インターフェイスの削除方法の詳細については、「仮想インターフェイスを削除する」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、「Letter of Authorization and Connecting Facility Assignment (LOA-CFA)」を参照してください。

接続を削除すると、AWS は該当する AWS パッチパネルからクロスコネクト用光ファイバケーブルを取り外して、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。

接続は、Direct Connect コンソール、コマンドライン、または API を使用して削除できます。

接続を削除するには

1. 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。

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 (Direct Connect API)

Direct Connect 接続を更新する

Direct Connect コンソール、コマンドライン、または API を使用して、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**
>
> ホスト接続の MACSec プロパティを直接変更することはできませんが、パートナーは独自の相互接続で MACSec を有効にして、顧客に安全なホスト接続を提供できます。

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`

接続を更新するには

1. 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。

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 (Direct Connect API)

Direct Connect 接続の詳細の表示

接続の現在のステータスは、Direct Connect コンソール、コマンドライン、または API を使用して表示できます。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、「Direct Connect のリソースをモニタリングする」を参照してください。

接続の詳細情報を表示するには

1. 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。

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 (Direct Connect API)

Direct Connect ロケーション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。Direct Connect ロケーションに機器を設置済みの場合は、適切なプロバイダに連絡して、クロスコネクトを完了します。プロバイダごとの具体的な手順については、以下の表を参照してください。パートナーと連絡先情報は、リージョン別に整理されています。特定のクロスコネクトの料金については、Direct Connect パートナーに直接お問い合わせください。クロスコネクトを確立したら、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、「Direct Connect Locations」を参照してください。

Direct Connect ロケーションに設置された機器をまだお持ちでない場合は、AWS パートナーネットワーク (APN) のいずれかのパートナー企業に設置の支援を依頼してください。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、「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。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。

Direct Connect 接続では、他のリージョンのリソースにアクセスできます。詳細については、「リモート Direct Connect リージョンにアクセスする」を参照してください。

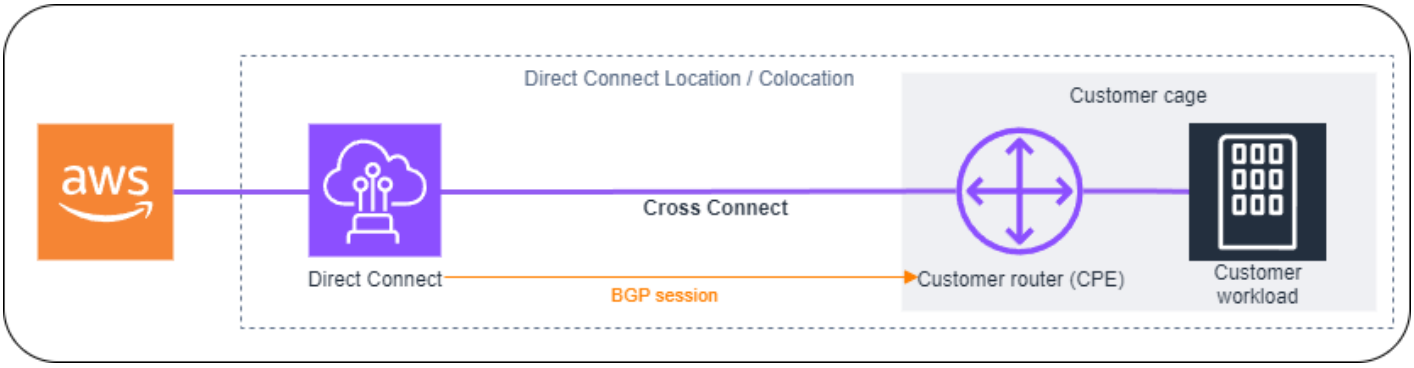
> **Note**
>
> クロスコネクトが 90 日以内に完了しない場合は、LOA-CFA が付与した権利は無効になります。有効期限が切れた LOA-CFA を更新するには、Direct Connect コンソールから再度ダウンロードできます。詳細については、「Letter of Authorization and Connecting Facility Assignment (LOA-CFA)」を参照してください。

接続オプション

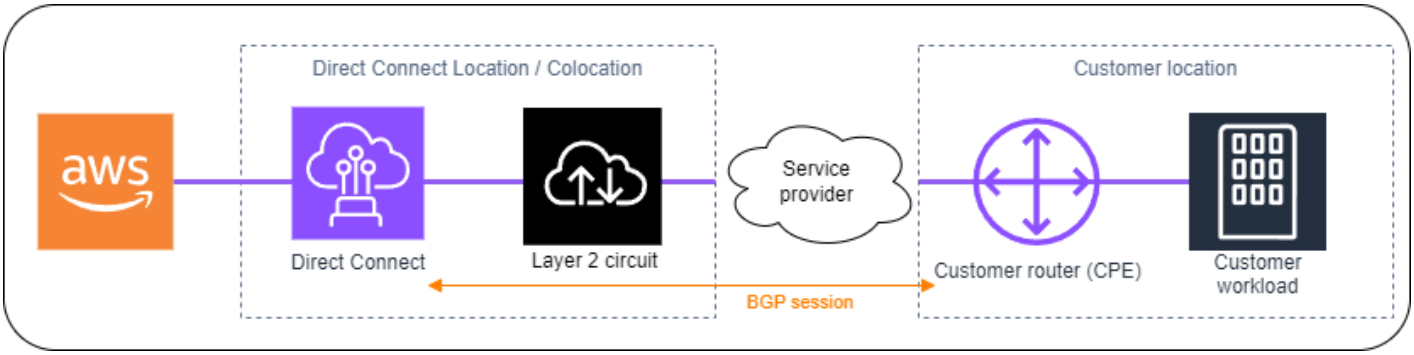
Direct Connect ロケーションへの接続に使用できるオプションは、パートナーと AWS リージョンによって異なる場合があります。次の接続オプションを 1 つ以上提供できる、AWS パートナーネットワーク (APN) のいずれかのパートナー企業に支援を依頼してください。

- Direct Connect ロケーションと同じデータセンター/コロケーション施設にリソースがデプロイされている場合、その施設では Direct Connect 機器とリソース間のクロスコネクトの提供が可能で

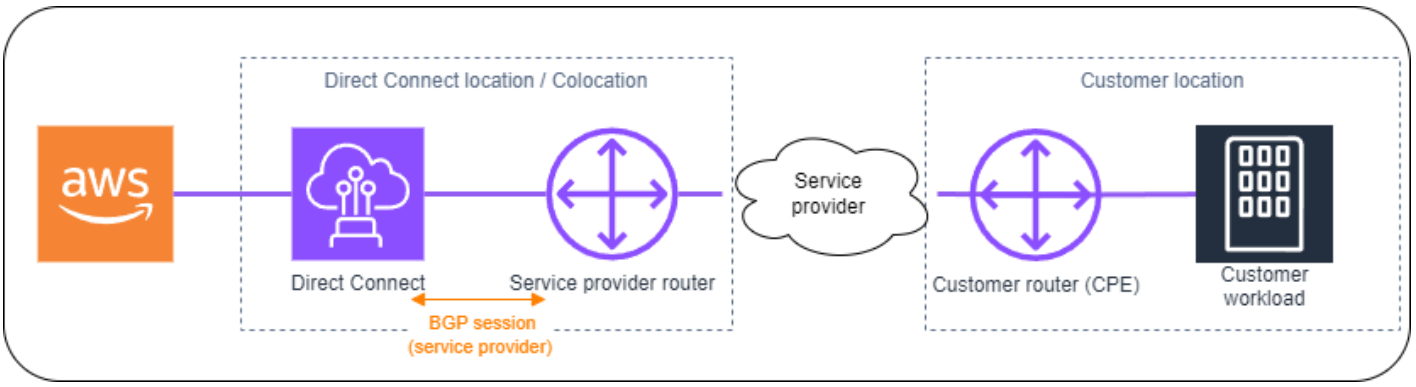
す。そのためには、まず LOA-CFA を施設に提供する必要があります。詳細については「Letter of Authorization and Connecting Facility Assignment (LOA-CFA)」を参照してください。この Direct Connect 接続オプションの例を次に示します。



- Direct Connect パートナーと連携することで、レイヤー 2 (データリンクレイヤー) の Direct Connect 接続を「回線」経由で Direct Connect ロケーションから顧客ロケーションに拡張します。顧客ロケーションにインストールされたルーターは、AWS 機器との BGP セッションを直接形成します。例えば、使用できるテクノロジーとしては、メトロイーサネット、ダークファイバー、波長などがあります。この Direct Connect 接続オプションの例を次に示します。



- Direct Connect パートナーと連携することで、レイヤー 3 (ネットワークレイヤー) の Direct Connect 接続を Direct Connect ロケーションから自分のロケーションに拡張します。この接続オプションでは、Direct Connect パートナーは Direct Connect ロケーション内に、AWS 機器とのボーダーゲートウェイプロトコル (BGP) セッションを形成するルーターを提供します。その後、Direct Connect パートナーがお客様との間に別の BGP を確立したとしたら、これはマルチプロトコルラベルスイッチング (MPLS) 経由で行われた可能性があります。この Direct Connect 接続オプションの例を次に示します。



米国東部 (オハイオ)

場所	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。
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、ヒューストン	顧客連絡先フォーム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)

場所	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、発注してください。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、レストン	CoreSite カスタマーポータル で発注してください。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 および ATL2、アトランタ	Digital Realty へのお問い合わせは、amazon.orders@digitalrealty.com までご連絡ください。
Digital 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。
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 および 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、セカーカス	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、メキシコ、ケレタロ	KIO Networks までお問い合わせください。
Markley、One Summer Street、ボストン	現在ご利用中のお客様は、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。

場所	接続をリクエストする方法
Netrality Data Centers、2nd floor MMR、フィラデルフィア	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、アトランタ	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)

場所	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、発注してください。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、ミルピタス	CoreSite 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 SV4、サンタクララ	CoreSite カスタマーポータル を使用して、発注してください。フォームに記入したら、注文の内容が正しいことを確認してから、MyCoreSite ウェブサイトを使用して注文を承認してください。
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。フォームの送信後、EdgeConneX から承認のためのサービス注文フォームが届きます。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 および 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。

場所	接続をリクエストする方法
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)

場所	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、発注してください。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、Westin Building、シアトル	Digital Realty へのお問い合わせは、amazon.orders@digitalrealty.com までご連絡ください。
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。フォームの送信後、EdgeConneX から承認のためのサービス注文フォームが届きます。質問は cloudaccess@edgeconnex.com に送ることができます。
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	TierPoint へのお問い合わせは、sales@tierpoint.com までご連絡ください。

アフリカ (ケープタウン)

場所	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)

場所	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 (awsdx@dci-indonesia.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)

場所	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、バンガロール	NetMagic の販売およびマーケティングへのお問い合わせは、フリーダイアル (18001033130) あるいは 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。

場所	接続をリクエストする方法
STT デリー DC 2、デリー	STT へのお問い合わせは、enquiry.AWSDX@sttelemediagdc.in までご連絡ください。
STT GDC Pvt. Ltd。VSB、チェンナイ	STT へのお問い合わせは、enquiry.AWSDX@sttelemediagdc.in までご連絡ください。
STT ハイデラバード DC 1、ハイデラバード	STT へのお問い合わせは、enquiry.AWSDX@sttelemediagdc.in までご連絡ください。

アジアパシフィック (ソウル)

場所	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)

場所	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。

場所	接続をリクエストする方法
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)

場所	接続をリクエストする方法
CDC Hume 2、キャンベラ	CDC カスタマーポータルのカスタマーポータルにログインしてください。
Datacom DH6、オークランド	Datacom へのお問い合わせは、Datacom Orbit (オークランド) までご連絡ください。
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。

場所	接続をリクエストする方法
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)

場所	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。
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)

場所	接続をリクエストする方法
Telehouse、250 Front St W、トロント	product@ca.telehouse.com までご連絡ください。
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)

場所	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。
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)

場所	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。

場所	接続をリクエストする方法
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)

場所	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	DigiPlex へのお問い合わせは、helpme@digiplex.com までご連絡ください。
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。
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。

場所	接続をリクエストする方法
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)

場所	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。
Eircom Clonshaugh	Eircom へのお問い合わせは、datacentre@eirevo.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)

場所	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)

場所	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。
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)

場所	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。

場所	接続をリクエストする方法
テレハウスボルテール、パリ	Telehouse パリボルテアへのお問い合わせは、お問い合わせページよりご連絡ください。

欧州 (ストックホルム)

場所	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)

場所	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)

場所	接続をリクエストする方法
MedOne、ハイファ	MedOne (support@Medone.co.il) に連絡する
EdgeConnex、ヘルツリーヤ	EdgeConnect へのお問い合わせは、info@edgeconnecx.com までご連絡ください

中東 (バーレーン)

場所	接続をリクエストする方法
AWS Bahrain DC53、マナーマ	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の Letter of Authorization (承認分書 = LOA) を AWS Support センター経由で AWS に提出します。その後、AWS がこのロケーションのクロスコネクトを完了します。
AWS Bahrain DC52、マナーマ	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の Letter of Authorization (承認分書 = LOA) を AWS Support センター経由で AWS に提出します。その後、AWS がこのロケーションのクロスコネクトを完了します。

中東 (アラブ首長国連邦)

場所	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、フジャイラ、アラブ首長国連邦	Etisalat SmartHub データセンターへのお問合せは、IntlSales-C&WS@etisalat.ae までご連絡ください。

南米 (サンパウロ)

場所	接続をリクエストする方法
Cirion BNARAGMS、ブエノスアイレス	Cirion へのお問い合わせは、cloud.connect@cirionotechnologies.com までご連絡ください。

場所	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)

場所	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。

Direct Connect 仮想インターフェイスとホスト型仮想インターフェイス

Direct Connect 接続の使用を開始するには、次のいずれかの仮想インターフェイス (VIF) 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、パブリック IP アドレスを使用してすべての AWS 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。任意の速度の Direct Connect 専用接続またはホスト接続で、トランジット仮想インターフェイスを使用できます。Direct Connect ゲートウェイの設定については、「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 AWS のその他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

お客様が VPC や他の AWS のサービス内のワークロードのパブリック IP アドレスにアクセスできるように、適切な Amazon プレフィックスがアドバタイズされます。この接続を介してすべての AWS プレフィックスにアクセスできます。例えば、Amazon EC2 インスタンス、Amazon S3、AWS のサービスの API エンドポイント、Amazon.com で使用されるパブリック IP アドレスなどです。Amazon 以外のプレフィックスにアクセスできません。AWS で使用されるプレフィックスの最新のリストについては、「Amazon VPC ユーザーガイド」の「AWS IP アドレス範囲」を参照してください。このページでは、現在公開されている AWS IP 範囲の `.json` ファイルをダウンロードできます。公開された IP アドレス範囲については、次の点に注意してください。

- パブリック仮想インターフェイスを介して BGP 経由でアナウンスされたプレフィックスは、AWS IP アドレス範囲リストに記載されているものと比較して集約または集約解除される可能性があります。

- 独自の IP アドレス (BYOIP) を使用して AWS に持ち込んだ IP アドレス範囲は `.json` ファイルに含まれませんが、AWS はこれらの BYOIP アドレスをパブリック仮想インターフェイスを介してアドバタイズします。
- AWS は、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 AWS の外部のネットワークに再アドバタイズしません。パブリック仮想インターフェイスでアドバタイズされたプレフィックスは、AWS 上のすべてのお客様に表示されます。

> **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。

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。

SiteLink

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作成している場合は、SiteLink を使用できます。

SiteLink は、プライベート仮想インターフェイス用のオプションの Direct Connect の機能であり、AWS ネットワーク上で利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 POP (Point Of Presence) 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。SiteLink の詳細については、「Introducing Direct Connect SiteLink」(SiteLink の紹介) 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。
> - オンプレミスルーターが複数の仮想インターフェイスで AWS に同じルートをアドバタイズしている場合、SiteLink は機能しません。

SiteLink の使用には別途料金がかかります。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の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 Transit Gateway 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 対応の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 Transit Gateway) からオンプレミスの場所へのトラフィックルーティングの動作は、AWS パスが先頭に追加されたデフォルトの Direct Connect 仮想インターフェイスの動作とは少し異なります。SiteLink を有効にすると、関連するリージョンに関係なく、Direct Connect ロケーションからの AS パスの長さが短い BGP パスが AWS リージョン 優先されます。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 Transit Gateway 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した場合でも、その AWS リージョン と共にデフォルトではそれに関連付けられた Direct Connect ロケーションを優先します。仮

想ゲートウェイまたは Transit Gateway 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種類に応じて、最大 8500 または 9001 のジャンボフレーム MTU サイズをサポートします。詳細については、「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 MTU」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、「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
接続	仮想インターフェイスを作成している Direct Connect 接続または Link Aggregation Group (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している場合は、そのアカウントの AWS 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 リージョン内の VPC への接続には、VPC 用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。

リソース	必要な情報
	Note • 仮想インターフェイスのカスタマーゲートウェイと仮想ゲートウェイ/Direct Connect ゲートウェイに同じ ASN を使用することはできません。 • 複数の仮想インターフェイスに同じカスタマーゲートウェイ ASN を使用できます。 • 複数の仮想インターフェイスは、異なる Direct Connect 接続の一部である限り、同じ仮想ゲートウェイ/Direct Connect ゲートウェイ ASN およびカスタマーゲートウェイ ASN を持つことができます。例: 仮想ゲートウェイ (ASN 64,496) <---仮想インターフェイス 1 (Direct Connect 接続 1)---> カスタマーゲートウェイ (ASN 64,511) 仮想ゲートウェイ (ASN 64,496) <---仮想インターフェイス 2 (Direct Connect 接続 2)---> カスタマーゲートウェイ (ASN 64,511)
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、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 パートナーが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。
	
	  Note
	  • 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ピアリング IP は、任意の有効な IP 範囲から指定できます。これには、お客様所有のパブリック IP アドレスを含めることもできます。ただし、それらの IP アドレスが BGP ピアリングセッションの作成にのみ使用され、仮想インターフェイスを介してアドバタイズされたり、NAT に使用されたりしないことが条件です。
	  • 当社は、AWS 提供のパブリック IPv4 アドレスのすべてのリクエストを満たすことができるとは保証できません。
	
	  値は次のいずれかになります:
	  • カスタマー所有 IPv4 CIDR
	
	  任意のパブリックIP (顧客所有または AWS 提供) を使用できますが、お客様のピア IP と AWS ルーターピア IP の両方に同じサブネットマ

リソース	必要な情報
	スクを使用する必要があります。例えば、/31 の範囲 (203.0.113.0/31 など) を割り当てると、お客様のピア IP に 203.0.113.0 を使用し、AWS ピア IP に 203.0.113.1 を使用できます。また、/24 の範囲 (198.51.100.0/24 など) を割り当てると、お客様のピア IP に 198.51.100.10 を使用し、AWS ピア IP に 198.51.100.20 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 認可。 • AWS 提供の /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) • (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。ご自身で指定する場合は、必ずルーターインターフェイスと AWS Direct Connect インターフェイスのプライベート CIDR のみを指定してください。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ースと同様に、お客様のピア 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、/30 の範囲 (192.168.0.0/30 など) を割り当てると、お客様のピア IP に 192.168.0.1 を使用し、AWS ピア IP に 192.168.0.2 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。

リソース	必要な情報
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: 次のいずれかに当てはまる場合は、IPv4 CIDR が Direct Connect を使用してアナウンス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。
	  • CIDR が異なる AWS リージョンからのものである。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。
	• Direct Connect パブリック仮想インターフェイスでは、IPv4 の場合は /1 ~ /32、IPv6 の場合は /1 ~ /64 の任意のプレフィックス長を指定できます。
	• 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。

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とトランジット仮想インターフェイスのみ) ジャンボフレーム	経由のパケットの最大送信単位 (MTUDirect 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、それを Direct Connect コンソールで選択し、仮想インターフェイスの [General configuration] (一般的な設定) ページで [Jumbo frame capable] (ジャンボフレーム対応) を見つけます。

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。自分のアカウントではない AWS 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。データ送信 (DTO) の使用量に関しては、リソースの所有者に対して、Direct Connect のデータ転送料金に基づいた計算が行われます。

> **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。

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 MTU

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。

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。プライベート仮想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、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。

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、Direct Connect 経由で伝播されたルートと、Transit Gateway 経由の静的ルートのみに適用されます。Transit Gateway 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。
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 を設定する手順については、「プライベート仮想インターフェイスの MTU を設定する」を参照してください。

Direct Connect 仮想インターフェイス

Transit Gateway 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。

仮想インターフェイスをお客様の AWS Organizations、またはそれとは異なる AWS Organizations に作成するには、ホスト型仮想インターフェイスを作成します。

仮想インターフェイスを作成するには、以下を実行します。

- パブリック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する
- 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

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。

Direct Connect ゲートウェイへの仮想インターフェイスのトランジットの前提条件

Transit Gateway に Direct Connect 接続をつなげるには、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。プライベート仮想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、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。例えば、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 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 営業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. 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 AS 番号 (ASN) を入力します。

有効な値は 1 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。

> **Note**
>
> パブリック仮想インターフェイスを介して AWS との BGP ピアリングセッションを確立する場合、AWS 側で BGP セッションを確立するための ASN として 7224 を使用します。ルーターまたはカスタマーゲートウェイデバイスの ASN は、その ASN とは異なっている必要があります。

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 (Direct Connect API)

Direct Connect プライベート仮想インターフェイスを作成する

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仮想プライベートインターフェイスをプロビジョニングできます。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、「Direct Connect ゲートウェイ」を参照してください。

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。プライベート仮想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、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. 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がユーザー自身の AWS アカウント用である場合は、[Virtual interface owner] (仮想インターフェイスの所有者) で [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 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。

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 Direct Connect 仮想インターフェイスを設定する際には、RFC 1918 を使用して独自の IP アドレスを指定するか、他のアドレス指定スキームを使用するか、ポイントツーポイント接続用に RFC 3927 169.254.0.0/16 IPv4 リンクローカル範囲から割り当てられた、AWS 割り当ての IPv4 /29 CIDR アドレスを選択することができます。これらのポイントツーポイント接続は、カスタマーゲートウェイルーターと Direct Connect エンドポイント間の eBGP ピアリングにのみ使用する必要があります。AWS サイト間プライベート IP VPN や Transit Gateway Connect などの VPC トラフィックまたはトンネリング目的の場合、AWS は、ポイントツーポイント接続の代わりに、カスタマーゲートウェイルーターのループバックまたは LAN インターフェイスを送信元アドレスまたは送信先アドレスとして使用することをお勧めします。
>
> - 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) [Enable SiteLink] (SiteLink の有効化) で [Enabled] (有効) を選択して、Direct Connect の POP (Point Of Presence) 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 (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を作成する

Direct Connect ゲートウェイに対して作成したトランジット仮想インターフェイスを接続する前に、テキスト をよくお読みください。

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. 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がユーザー自身の AWS アカウント用である場合は、[Virtual interface owner] (仮想インターフェイスの所有者) で [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 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。

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 Direct Connect 仮想インターフェイスを設定する際には、RFC 1918 を使用して独自の IP アドレスを指定するか、他のアドレス指定スキームを使用するか、ポイントツーポイント接続用に RFC 3927 169.254.0.0/16 IPv4 リンクローカル範囲から割り当てられた、AWS 割り当ての IPv4 /29 CIDR アドレスを選択することができます。これらのポイントツーポイント接続は、カスタマーゲートウェイルーターと Direct Connect エンドポイント間の eBGP ピアリングにのみ使用する必要があります。AWS サイト間プライベート IP VPN や Transit Gateway Connect などの VPC トラフィックまたはトンネリング目的の場合、AWS は、ポイントツーポイント接続の代わりに、カスタマーゲートウェイルーターのループバックまたは LAN インターフェイスを送信元アドレスまたは送信先アドレスとして使用することをお勧めします。
>
> - 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) [Enable SiteLink] (SiteLink の有効化) で [Enabled] (有効) を選択して、Direct Connect の POP (Point Of Presence) 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 (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)
- DescribeDirectConnectGatewayAttachments (Direct Connect API)

Direct Connect 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

ルーター設定ファイルをダウンロードするには

1. 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 Direct Connect に接続できることを確認します。
7. 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。
暗号アルゴリズム	AES_256_CMAC

Parameter	説明
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 >

ホスト型 Direct Connect 仮想インターフェイス

別のアカウントで Direct Connect 接続を使用するには、そのアカウントにホスト型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型仮想インターフェイスを受け入れる必要があります。ホスト型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
接続	仮想インターフェイスを作成している Direct Connect 接続または Link Aggregation Group (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している場合は、そのアカウントの AWS 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 リージョン内の VPC への接続には、VPC 用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、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 パートナーが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 任意のパブリックIP (顧客所有または AWS 提供) を使用できますが、お客様のピア 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、/31 の範囲 (203.0.113.0/31 など) を割り当てると、お客様のピア IP に 203.0.113.0 を使用し、AWS ピア IP に 203.0.113.1 を使用できます。また、/24 の範囲 (198.51.100.0/24 など) を割り当てると、お客様のピア IP に 198.51.100.10 を使用し、AWS ピア IP に 198.51.100.20 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 認可 • AWS 提供/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 当社は、AWS 提供パブリック IPv4 アドレスのすべてのリクエストを満たすことができるとは保証できません。 • (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。ご自身で指定する場合は、必ずルー

リソース	必要な情報
	ターインターフェイスと AWS Direct Connect インターフェイスのプライベート CIDR のみを指定してください。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ースと同様に、お客様のピア 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、`/30` の範囲 (`192.168.0.0/30` など) を割り当てると、お客様のピア IP に `192.168.0.1` を使用し、AWS ピア IP に `192.168.0.2` 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 4294967294 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: 次のいずれかに当てはまる場合は、IPv4 CIDR が Direct Connect を使用してアナウンス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。
	  • CIDR が異なる AWS リージョンからのものである。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。
	• Direct Connect パブリック仮想インターフェイスでは、IPv4 の場合は /1 ~ /32、IPv6 の場合は /1 ~ /64 の任意のプレフィックス長を指定できます。
	• 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。

(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み) ジャンボフレーム	経由のパケットの最大送信単位 (MTUDirect 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 Direct Connect から伝達されるルートにのみ適用されます。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、それを Direct Connect コンソールで選択し、仮想インターフェイスの [General configuration] (一般的な設定) ページで [Jumbo frame capable] (ジャンボフレーム対応) を見つけます。

Direct Connect でホスト型プライベート仮想インターフェイスを作成する

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には

1. 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. [仮想インターフェイスの所有者] で [別の AWS アカウント] を選択し、[仮想インターフェイスの所有者] に、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 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。
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 Direct Connect 仮想インターフェイスを設定する際には、RFC 1918 を使用して独自の IP アドレスを指定するか、他のアドレス指定スキームを使用するか、ポイントツーポイント接続用に RFC 3927 169.254.0.0/16 IPv4 リンクローカル範囲から割り当てられた、AWS 割り当ての IPv4 /29 CIDR アドレスを選択することができます。これらのポイントツーポイント接続は、カスタマーゲートウェイルーターと Direct Connect エンドポイント間の eBGP ピアリングにのみ使用する必要があります。AWS サイト間プライベート IP VPN や Transit Gateway Connect などの VPC トラフィックまたはトンネリング目的の場合、AWS は、ポイントツーポイント接続の代わりに、カスタマーゲートウェイルーターのループバックまたは LAN インターフェイスを送信元アドレスまたは送信先アドレスとして使用することをお勧めします。
>
> - 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) 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. ホスト型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、設定ファイル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 (Direct Connect API)

Direct Connect でホスト型パブリック仮想インターフェイスを作成する

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。

ホストされたパブリック仮想インターフェイスを作成するには

1. 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の所有者] で [別の AWS アカウント] を選択し、[仮想インターフェイスの所有者] に、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 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。
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。

[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. ホスト型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、設定ファイル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 (Direct Connect API)

Direct Connect ホスト型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. 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 [別の AWS アカウント] を選択し、[仮想インターフェイスの所有者] に、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 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。
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 Direct Connect 仮想インターフェイスを設定する際には、RFC 1918 を使用して独自の IP アドレスを指定するか、他のアドレス指定スキームを使用するか、ポイントツーポイント接続用に RFC 3927 169.254.0.0/16 IPv4 リンクローカル範囲から割り当てられた、AWS 割り当ての IPv4 /29 CIDR アドレスを選択することができます。これらのポイントツーポイント接続は、カスタマーゲートウェイルーターと Direct Connect エンドポイント間の eBGP ピアリングにのみ使用する必要があります。AWS サイト間プライベート IP VPN や Transit Gateway Connect などの VPC トラフィックまたはトンネリング目的の場合、AWS は、ポイントツーポイント接続の代わりに、カスタマーゲートウェイルーターのループバックまたは LAN インターフェイスを送信元アドレスまたは送信先アドレスとして使用することをお勧めします。
>
> - 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) 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. ホスト型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、デバイスのルーター設定ファイル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 (Direct Connect API)

Direct Connect 仮想インターフェイスの詳細を表示する

モニタのステータスは、Direct Connect コンソール、コマンドライン、または API を使用して変更できます。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. 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)
- DescribeVirtualInterfaces (Direct Connect API)

BGP ピアを Direct Connect 仮想インターフェイスに追加する

Direct Connect コンソール、コマンドライン、または API を使用して、IPv4 または IPv6 BGP ピアリング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。

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. 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**
>
> AWS Direct Connect 仮想インターフェイスを設定する際には、RFC 1918 を使用して独自の IP アドレスを指定するか、他のアドレス指定スキームを使用するか、ポイントツーポイント接続用に RFC 3927 169.254.0.0/16 IPv4 リンクローカル範囲から割り当てられた、AWS 割り当ての IPv4 /29 CIDR アドレスを選択することができます。これらのポイントツーポイント接続は、カスタマーゲートウェイルーターと Direct Connect エンドポイント間の eBGP ピアリングにのみ使用する必要があります。AWS サイト間プライベート IP VPN や Transit Gateway Connect などの VPC トラフィックまたはトンネリング目的の場合、AWS は、ポイントツーポイント接続の代わりに、カスタマーゲートウェイルーターのループバックまたは LAN インターフェイスを送信元アドレスまたは送信先アドレスとして使用することをお勧めします。
>
> - 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。

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 ~ 4294967294 です。これには、ASN (1 ~ 2147483646) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。

   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 (Direct Connect API)

Direct Connect 仮想インターフェイス 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)。Direct Connect コンソール、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 BGP ピアを削除できます。

BGP ピアを削除するには

1. 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 (Direct Connect API)

Direct Connect プライベート仮想インターフェイスの MTU を設定する

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)。MTU とプライベート仮想インターフェイスの詳細については、「MTUs 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用」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の MTU は、Direct Connect コンソール、コマンドライン、または API を使用して設定できます。

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. 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. [Jumbo MTU (MTU size 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 (Direct Connect API)

Direct Connect 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、Direct Connect コンソール、コマンドライン、または API を使用して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. 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)

Direct Connect 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、その仮想インターフェイスに関連する Direct Connect データ転送への課金が停止します。

仮想インターフェイスは、Direct Connect コンソール、コマンドライン、または API を使用して削除できます。

仮想インターフェイスを削除するには

1. 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)
- DeleteVirtualInterface (Direct Connect API)

ホスト型 Direct Connect 仮想インターフェイスを承諾する

ホスト型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。

ホスト型仮想インターフェイスを受け入れるには、Direct Connect コンソール、コマンドライン、または API を使用します。

ホスト型仮想インターフェイスを承諾するには

1. 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. ホスト型仮想インターフェイスを承諾すると、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 (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 (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 (Direct Connect API)

Direct Connect 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. 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

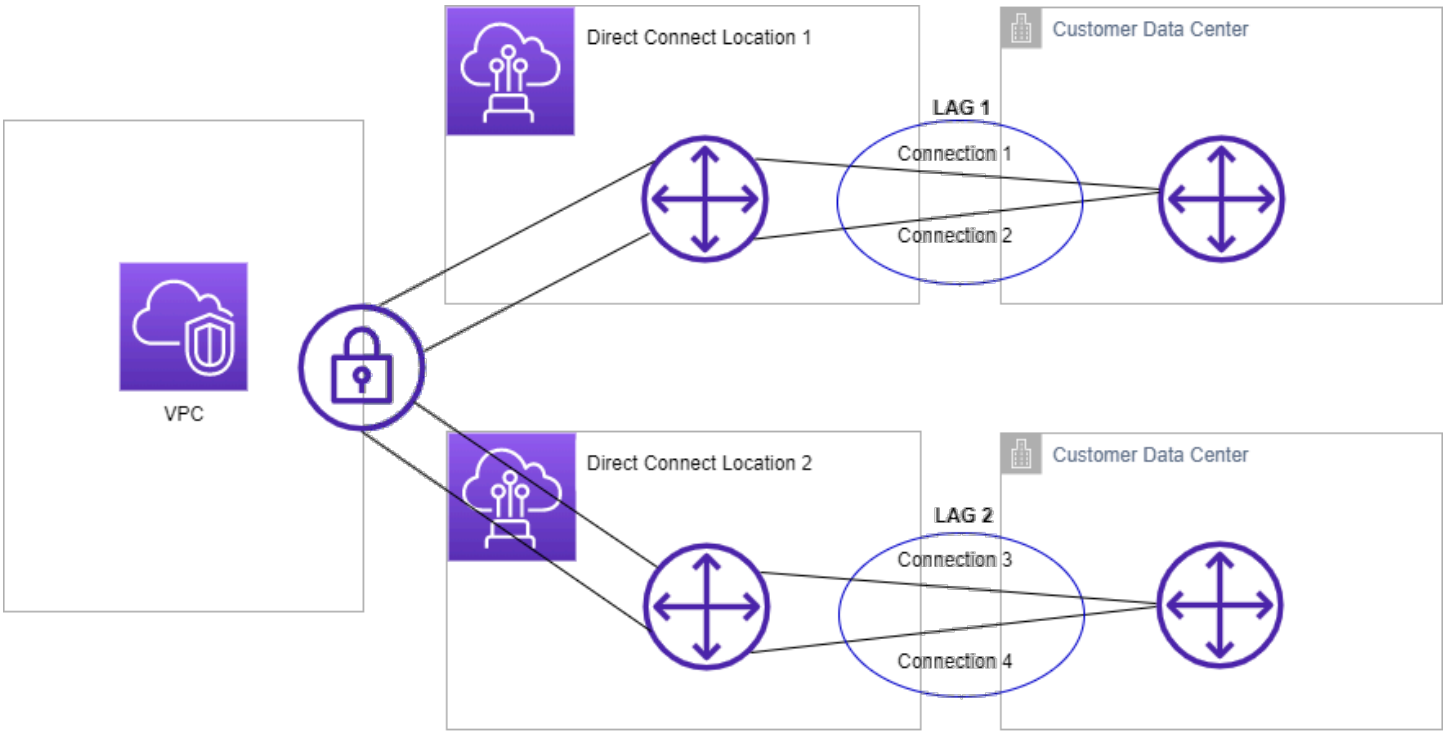
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface (Direct Connect API)

Direct Connect Link aggregation groups (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 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端とする接続の LAG を作成すれば、4 つの接続の代わりに 2 つの LAG を使って設定と管理を行うことができます。



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、100 Gbps、または 400 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、100 Gbps または 400 Gbps の接続を 最大 2 つ、もしくは 100 Gbps 未満のポート速度を持つ接続を 4 つまで集約して利用できます。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 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、新しい物理接続用の Letter of Authorization and Connecting Facility Assignment (LOA-CFA) を 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、「Letter of Authorization and Connecting Facility Assignment (LOA-CFA)」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 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。

トピック

- Direct Connect の MacSec に関する考慮事項
- Direct Connect エンドポイントで LAG を作成する
- Direct Connect エンドポイントで LAG の詳細の表示
- Direct Connect エンドポイントで LAG を更新する
- Direct Connect エンドポイントで接続を LAG に関連付ける
- Direct Connect エンドポイントで LAG から接続の関連付けを解除する
- MACSec CKN/CAK と Direct Connect エンドポイント LAG を関連付ける

- MACsec シークレットキーと Direct Connect エンドポイント LAG の間の関連付けを解除する
- Direct Connect エンドポイント LAG を削除する

Direct Connect の 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。
- すべての LAG リンクでいつでも使用できる MACsec キーは 1 つだけです。複数の MACsec キーをサポートする機能は、キーのローテーションのみを目的としています。

Direct Connect エンドポイントで 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 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。

新しい接続で LAG を作成するには

1. 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、ポート速度が 100 Gbps または 400 Gbps 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。

既存の接続から LAG を作成するには

1. 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 1 Gbps または 10 Gbps の場合は最大 4 つの接続が可能で、ポート速度が 100 Gbps または 400 Gbps の場合は最大 2 つの接続が可能です。

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。

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 (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 (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 (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。

Direct Connect エンドポイントで LAG の詳細の表示

LAG を作成したら、Direct Connect コンソール、コマンドライン、または API を使用してその詳細を表示できます。

LAG に関する情報を表示するには

1. 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 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。

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 (Direct Connect API)

Direct Connect エンドポイントで LAG を更新する

Direct Connect コンソール、コマンドライン、または API を使用して、次のリンク集約グループ (LAG) 属性を更新できます。

- 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。

LAG を更新するには

1. 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。

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 (Direct Connect API)

Direct Connect エンドポイントで接続を LAG に関連付ける

既存の接続を LAG に関連付けるには、Direct Connect コンソール、コマンドライン、または API を使用します。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。

接続を LAG と関連付けるには

1. 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。

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 (Direct Connect API)

Direct Connect エンドポイントで 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、Direct Connect コンソール、コマンドライン、または API を使用して LAG から接続の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。

LAG から接続の関連付けを解除するには

1. 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。

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 (Direct Connect API)

MACSec CKN/CAK と Direct Connect エンドポイント 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、Direct Connect コンソール、コマンドライン、または API を使用して、CKN/CAK を接続に関連付けることができます。

> **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。

MACsec キーと LAG を関連付けるには

1. 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。

コマンドラインまたは API を使用して MACsec キーを LAG に関連付けるには

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

MACsec シークレットキーと Direct Connect エンドポイント LAG の間の関連付けを解除する

LAG と MACsec キー間の関連付けを解除するには、Direct Connect コンソール、コマンドライン、または API を使用します。

LAG と MACsec キー間の関連付けを解除するには

1. 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。

コマンドラインまたは API を使用して LAG と MACsec キー間の関連付けを解除するには

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

Direct Connect エンドポイント 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、「接続を削除」を参照してください。

LAG は、Direct Connect コンソール、コマンドライン、または API を使用して削除できます。

LAG を削除するには

1. 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。

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 (Direct Connect API)

Direct Connect ゲートウェイ

Amazon VPC コンソールまたは Direct Connect を使用して、AWS CLI ゲートウェイを操作できます。

- Direct Connect ゲートウェイ

  Direct Connect ゲートウェイを使用すると、Direct Connect ゲートウェイを複数の VPC を持つ Transit Gateway、仮想プライベートゲートウェイ、または AWS Cloud WAN を使用する場合は Cloud WAN コアネットワークに関連付けることができます。
- 仮想プライベートゲートウェイの関連付け

  仮想プライベート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経由で、Direct Connect ゲートウェイを、同じリージョンまたは異なるリージョンにある任意のアカウントの 1 つ以上の VPC に関連付けることができます。
- Transit Gateway の関連付け

  Direct Connect ゲートウェイを使用すると、トランジット仮想インターフェイス経由で、Transit Gateway にアタッチされた VPC または VPN に Direct Connect 接続を接続できます。
- Cloud WAN コアネットワークの関連付け

  Direct Connect ゲートウェイを使用して、Direct Connect ゲートウェイを AWS Network Manager コアネットワークに関連付けます。
- 許可されたプレフィックスのインタラクション

  Transit Gateway や仮想プライベートゲートウェイで動作する、許可されたプレフィックスを使用します。

トピック

- Direct Connect ゲートウェイ
- Direct Connect 仮想プライベートゲートウェイの関連付け
- Direct Connect ゲートウェイと Transit Gateway の関連付け
- Direct Connect ゲートウェイと AWS Cloud WAN コアネットワークの関連付け
- Direct Connect ゲートウェイでの許可されたプレフィックスのインタラクション

Direct Connect ゲートウェイ

Direct Connect ゲートウェイを使用して VPC を接続します。Direct Connect ゲートウェイは、次のいずれかに関連付けます。

- 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
- AWS Cloud WAN コアネットワーク

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。これには AWS GovCloud (US) は含まれますが、AWS 中国リージョンは含まれません。Direct Connect ゲートウェイは、分散された BGP ルートリフレクターのセットとして機能するように設計された Direct Connect の仮想コンポーネントです。データトラフィックパスの外部で動作するため、単一障害点の作成や特定の AWS リージョンへの依存関係の導入を回避できます。高可用性は設計に本質的に組み込まれているため、複数の Direct Connect ゲートウェイが不要になります。

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 Transit Gateway 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、blackhole オプションが設定された VPC アタッチメントにルートテーブルを関連付けます。

トピック

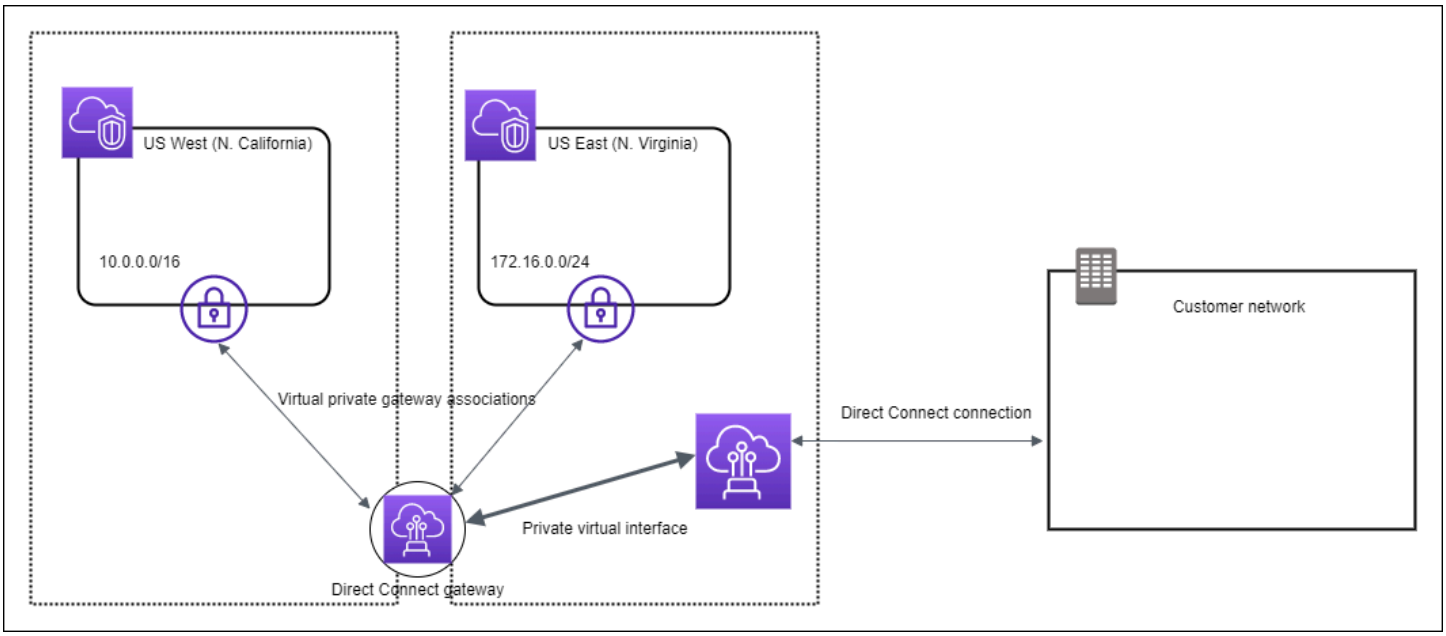
シナリオ

以下では、Direct Connect ゲートウェイを使用するシナリオをいくつか説明します。

シナリオ: 仮想プライベートゲートウェイの関連付け

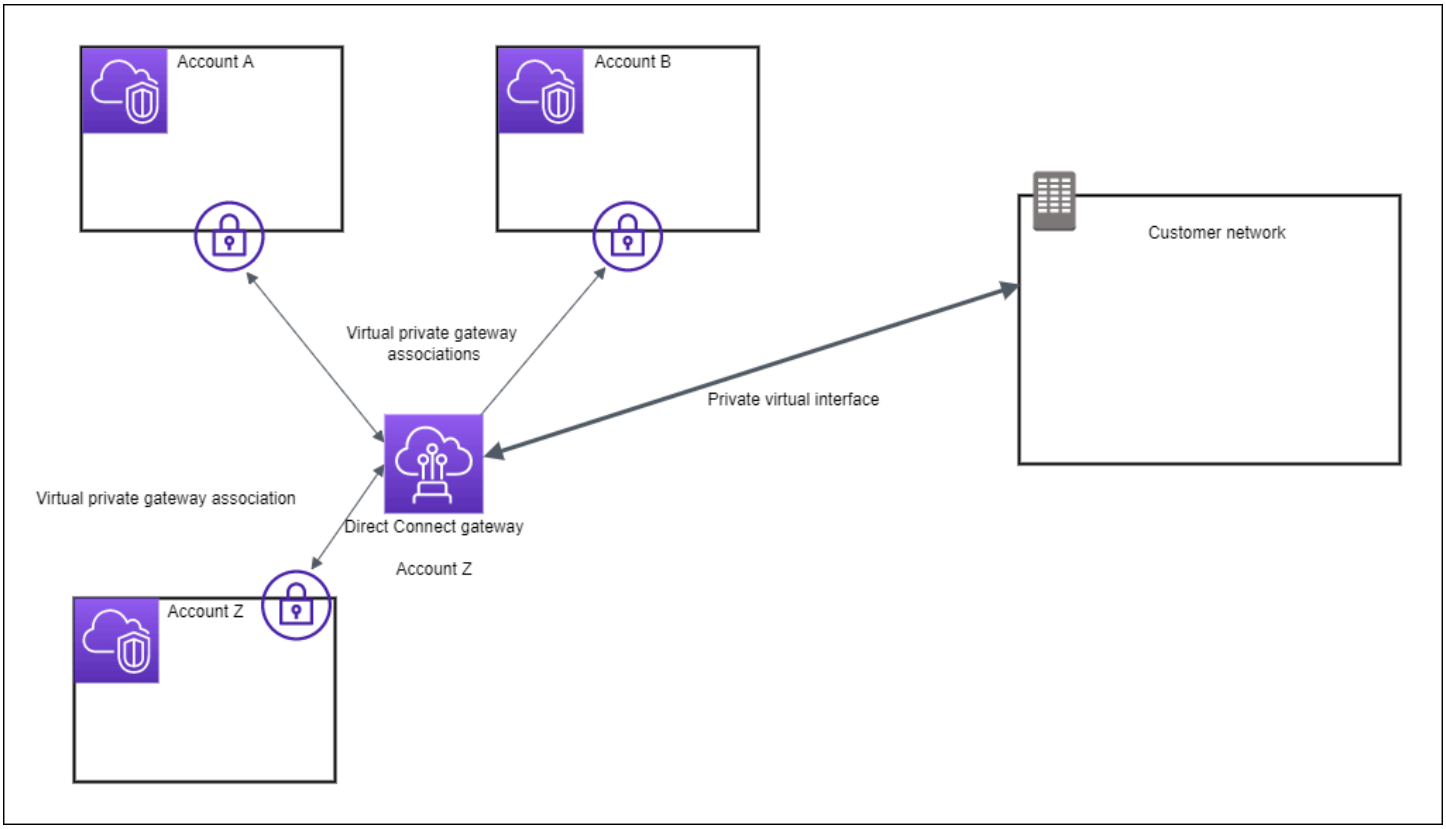
次の図では、Direct Connect ゲートウェイが米国東部 (バージニア北部) リージョンの Direct Connect 接続を使用して、米国東部 (バージニア北部) と米国西部 (北カリフォルニア) の両リージョンにあるアカウント内の VPC へのアクセスを可能にします。

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、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 Direct Connect 接続があります。



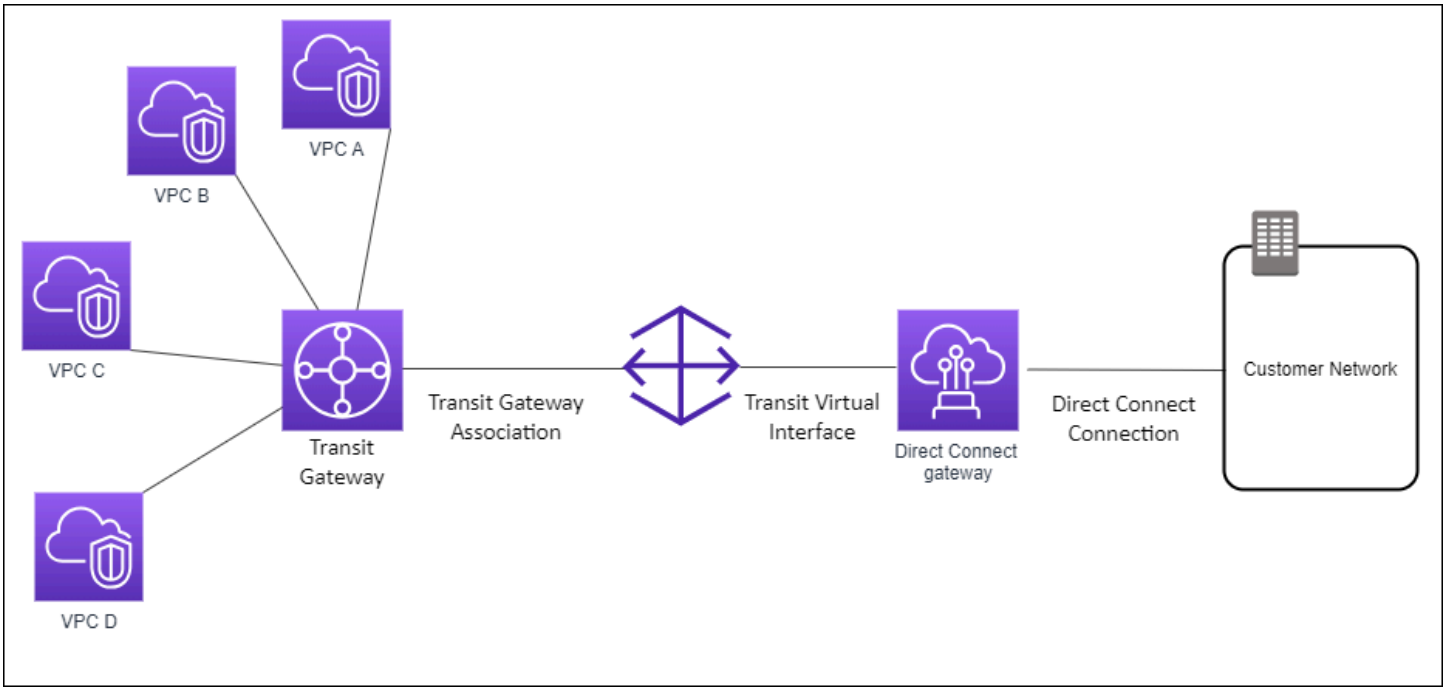
シナリオ: アカウント間の仮想プライベートゲートウェイの関連付け

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。



シナリオ: Transit Gateway 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。

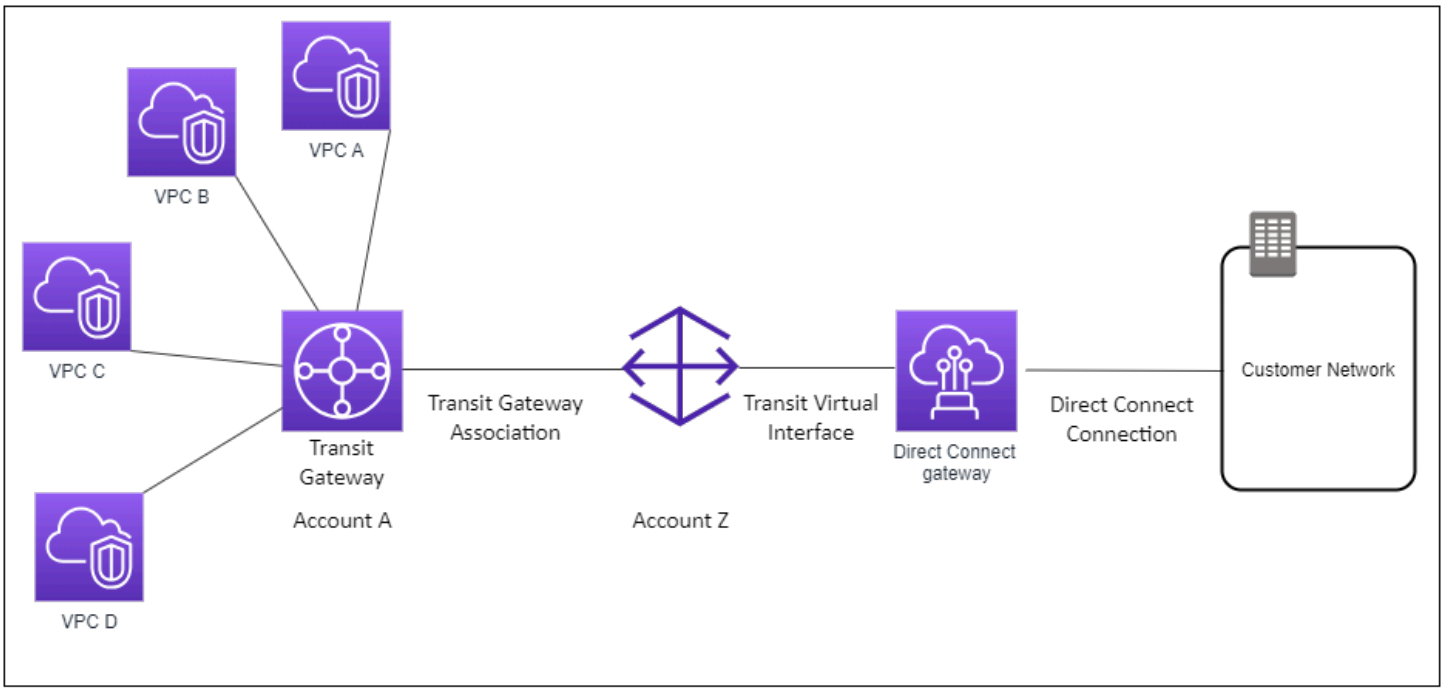
この設定には次のような利点があります。以下を実行できます。

- 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。
- オンプレミスから AWS に、または AWS からオンプレミスにプレフィックスをアドバタイズする。

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。

シナリオ: アカウント間の Transit Gateway 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。



Direct Connect ゲートウェイを作成する

Direct Connect ゲートウェイは、Direct Connect コンソール、コマンドライン、または API を使用して、サポートされている任意のリージョンに作成できます。

Direct Connect ゲートウェイを作成するには

1. 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。

> **Note**
>
> AWS Cloud WAN コアネットワークで使用する Direct Connect ゲートウェイを作成する場合。ASN は、コアネットワークの ASN と同じ範囲にすることはできません。

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 (Direct Connect API)

仮想プライベートゲートウェイから Direct Connect ゲートウェイに移行する

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を Direct Connect ゲートウェイに移行できます。

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 を使用している場合は、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。

次の手順では、仮想プライベートゲートウェイを Direct Connect ゲートウェイに移行するために必要な手順について説明します。

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。

   Direct Connect ゲートウェイがまだ存在しない場合は、作成する必要があります。Direct Connect ゲートウェイを作成する手順については、「Direct Connect ゲートウェイを作成する」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。

   移行には仮想インターフェイスが必要です。インターフェイスが存在しない場合は、作成する必要があります。仮想インターフェイスを作成する手順については、「仮想インターフェイス」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。

Direct Connect ゲートウェイと仮想プライベートゲートウェイの両方を関連付ける必要があります。関連付けを作成する手順については、「仮想プライベートゲートウェイを関連付けまたは関連付け解除する」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、「仮想インターフェイスを削除する」を参照してください。

Direct Connect ゲートウェイを削除する

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。関連付けられた仮想プライベートゲートウェイの関連付けを解除し、アタッチされたプライベート仮想インターフェイスを削除したら、Direct Connect コンソール、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手順については、「仮想プライベートゲートウェイを関連付けまたは関連付け解除する」を参照してください。
- 仮想インターフェイスを削除する手順については、「仮想インターフェイスを削除する」を参照してください。

Direct Connect ゲートウェイを削除するには

1. 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 (Direct Connect API)

Direct Connect 仮想プライベートゲートウェイの関連付け

Direct Connect ゲートウェイと仮想プライベートゲートウェイを関連付けることで、さまざまなアカウントやリージョンにまたがって Direct Connect 接続と VPC 間の接続を有効にすることができます。各 VPC には、Direct Connect ゲートウェイと関連付ける仮想プライベートゲートウェイが必要です。これらの関連付けを設定したら、Direct Connect ゲートウェイへの Direct Connect 接続にプライベート仮想インターフェイスを作成し、複数の VPC がそれぞれの仮想プライベートゲートウェイの関連付けを通じて同じ Direct Connect 接続を共有できるようにします。

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。

- Direct Connect ゲートウェイに仮想ゲートウェイを関連付けるまで、ルート伝播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伝播を有効にすると、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、「Direct Connect クォータ」を参照してください。
- Direct Connect ゲートウェイが既に Transit Gateway 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。
- 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。

同じリージョン内の VPC のみに Direct Connect 接続を接続するには、Direct Connect ゲートウェイを作成します。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 および VPN CloudHub を参照してください。

Direct Connect 接続を別のアカウントの VPC で使用するには、そのアカウントのホスト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、ホスト型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、「仮想インターフェイスとホスト型仮想インターフェイス」を参照してください。

トピック

- Direct Connect 仮想プライベートゲートウェイの作成
- Direct Connect 仮想プライベートゲートウェイの関連付けまたは関連付けを解除する
- 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作成する
- アカウント間での Direct Connect 仮想プライベートゲートウェイを関連付ける

Direct Connect 仮想プライベートゲートウェイの作成

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。仮想プライベートゲートウェイを作成し、Direct Connect コンソールまたはコマンドラインまたは API を使用して VPC にアタッチできます。

> **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. 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 Query 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 Query API)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Direct Connect 仮想プライベートゲートウェイの関連付けまたは関連付けを解除する

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または関連付け解除は、Direct Connect コンソールまたはコマンドラインまたは API を使用して行うことができます。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. 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. 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-association (AWS CLI)
- CreateDirectConnectGatewayAssociation (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-associations (AWS CLI)
- DescribeDirectConnectGatewayAssociations (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-association (AWS CLI)
- DeleteDirectConnectGatewayAssociation (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を作成する

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。プライベート仮想インターフェイスを作成するには、Direct Connect コンソールを使用するか、コマンドラインまたは API を使用します。

> **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、「ホスト型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. 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がユーザー自身の AWS アカウント用である場合は、[Virtual interface owner] (仮想インターフェイスの所有者) で [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 1～4294967294 です。これには、ASN (1～2147483647) とロング ASN (1～4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。

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 Direct Connect 仮想インターフェイスを設定する際には、RFC 1918 を使用して独自の IP アドレスを指定するか、他のアドレス指定スキームを使用するか、ポイントツーポイント接続用に RFC 3927 169.254.0.0/16 IPv4 リンクローカル範囲から割り当てられた、AWS 割り当ての IPv4 /29 CIDR アドレスを選択することができます。これらのポイントツーポイント接続は、カスタマーゲートウェイルーターと Direct Connect エンドポイント間の eBGP ピアリングにのみ使用する必要があります。AWS サイト間プライベート IP VPN や Transit Gateway Connect などの VPC トラフィックまたはトンネリング目的の場合、AWS は、ポイントツーポイント接続の代わりに、カスタマーゲートウェイルーターのループバックまたは LAN インターフェイスを送信元アドレスまたは送信先アドレスとして使用することをお勧めします。
>
> - 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) [Enable SiteLink] (SiteLink の有効化) で [Enabled] (有効) を選択して、Direct Connect の POP (Point Of Presence) 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 (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)
- DescribeDirectConnectGatewayAttachments (Direct Connect API)

アカウント間での Direct Connect 仮想プライベートゲートウェイを関連付ける

Direct Connect ゲートウェイを、任意の AWS 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 経由で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 Transit Gateway でのみ利用でき、同一リージョン内では利用できません。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、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。

Direct Connect ゲートウェイと Transit Gateway の関連付け

Direct Connect ゲートウェイを使用すると、トランジット仮想インターフェイス経由で Direct Connect 接続を、Transit Gateway に接続されている VPC または VPN に接続できます。Direct Connect ゲートウェイを Transit Gateway に関連付けます。次に、Direct Connect ゲートウェイへの 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。

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、「Direct Connect 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。
- 例えば、/30 範囲を使用するポイントツーポイント接続アドレス (192.168.0.0/30 など) は、トランジットゲートウェイには伝播されません。

アカウント間の Transit Gateway 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、任意の AWS アカウントが所有する Transit Gateway 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、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、オンプレミスから AWS へのトラフィックを Transit Gateway にルーティングするために使用されます。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、「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。

トピック

- Direct Connect と Transit Gateway の関連付けまたは関連付け解除
- 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作成する
- Transit Gateway の Direct Connect 関連付け提案の作成
- Transit Gateway と Direct Connect の関連付け提案の受諾または拒否
- Transit Gateway と Direct Connect の関連付けの許可されたプレフィックスを更新する
- Transit Gateway の Direct Connect 関連付け提案の削除

Direct Connect と Transit Gateway の関連付けまたは関連付け解除

Direct Connect コンソール、コマンドライン、または API を使用して、Transit Gateway の関連付けまたは関連付け解除を行います。

Transit Gateway を関連付けるには

1. 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、「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. 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、Transit Gateway を選択します。
5. [関連付け解除] を選択します。

Transit Gateway の許可されたプレフィックスを更新する

Transit Gateway 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. 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. 許可されたプレフィックスを変更するゲートウェイを選択してから、[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、「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。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-association (AWS CLI)
- CreateDirectConnectGatewayAssociation (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-associations (AWS CLI)
- DescribeDirectConnectGatewayAssociations (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-association (AWS CLI)
- DeleteDirectConnectGatewayAssociation (Direct Connect API)

コマンドラインまたは API を使用して Transit Gateway の許可されたプレフィックスを更新する

- update-direct-connect-gateway-association (AWS CLI)
- UpdateDirectConnectGatewayAssociation (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を作成する

Transit Gateway に Direct Connect 接続をつなげるには、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。Direct Connect コンソール、コマンドライン、または APIを使用できます。

> **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. 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がユーザー自身の AWS アカウント用である場合は、[Virtual interface owner] (仮想インターフェイスの所有者) で [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 ~ 4294967294 です。これには、ASN (1 ~ 2147483647) とロング ASN (1 ~ 4294967294) の両方のサポートが含まれます。ASN とロング ASN の詳細については、「Direct Connect でのロング ASN のサポート」を参照してください。

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 Direct Connect 仮想インターフェイスを設定する際には、RFC 1918 を使用して独自の IP アドレスを指定するか、他のアドレス指定スキームを使用するか、ポイントツーポイント接続用に RFC 3927 169.254.0.0/16 IPv4 リンクローカル範囲から割り当てられた、AWS 割り当ての IPv4 /29 CIDR アドレスを選択することができます。これらのポイントツーポイント接続は、カスタマーゲートウェイルーターと Direct Connect エンドポイント間の eBGP ピアリングにのみ使用する必要があります。AWS サイト間プライベート IP VPN や Transit Gateway Connect などの VPC トラフィックまたはトンネリング目的の場合、AWS は、ポイントツーポイント接続の代わりに、カスタマーゲートウェイルーターのループバックまたは LAN インターフェイスを送信元アドレスまたは送信先アドレスとして使用することをお勧めします。
   >
   > - 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) [Enable SiteLink] (SiteLink の有効化) で [Enabled] (有効) を選択して、Direct Connect の POP (Point Of Presence) 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 (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)
- DescribeDirectConnectGatewayAttachments (Direct Connect API)

Transit Gateway の Direct Connect 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。Transit Gateway は、AWS アカウントの VPC または VPN にアタッチされている必要があります。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Direct Connect Direct Connect コンソール、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できます。

関連付け提案を作成するには

1. 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] を選択し、Transit Gateway 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-association-proposal (AWS CLI)
- CreateDirectConnectGatewayAssociationProposal (Direct Connect API)

Transit Gateway と Direct Connect 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。Direct Connect コンソール、コマンドライン、または API を使用して、関連付け提案を受諾または拒否できます。

関連付け提案を承諾するには

1. 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. 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 Transit Gateway 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-association-proposals (AWS CLI)
- DescribeDirectConnectGatewayAssociationProposals (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-association-proposal (AWS CLI)
- AcceptDirectConnectGatewayAssociationProposal (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-association-proposal (AWS CLI)

- DeleteDirectConnectGatewayAssociationProposal (Direct Connect API)

Transit Gateway と Direct Connect の関連付けの許可されたプレフィックスを更新する

Direct Connect コンソール、コマンドライン、または API を使用して、Transit Gateway から Direct Connect ゲートウェイを経由して許可されたプレフィックスを更新できます。Direct Connect コンソールを使用して、Transit Gateway と Direct Connect の関連付けで許可されたプレフィックスを更新するには、

- Transit Gateway のオーナーである場合、許可するプレフィックスを指定して、その Direct Connect ゲートウェイの新しい関連付け提案を作成する必要があります。新しい関連付け提案を作成する手順については、「Transit Gateway の関連付け提案の作成」を参照してください。
- 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、または既存の関連付けの許可されたプレフィックス更新するときに、許可されたプレフィックスを更新できます。関連付けを受け入れるときに、許可されたプレフィックスを更新する手順については、「Transit Gateway の関連付け提案の受諾または拒否」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、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-association (AWS CLI)
- UpdateDirectConnectGatewayAssociation (Direct Connect API)

Transit Gateway の Direct Connect 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 Transit Gateway の関連付けを解除することができます。詳細については、「Transit Gateway の関連付け提案の作成」を参照してください。

Transit Gateway と Direct Connect の関連付け提案は、Direct Connect コンソール、コマンドライン、または APIを使用して削除できます。

関連付け提案を削除するには

1. 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] を選択し、Transit Gateway 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-association-proposal (AWS CLI)
- DeleteDirectConnectGatewayAssociationProposal (Direct Connect API)

Direct Connect ゲートウェイと AWS Cloud WAN コアネットワークの関連付け

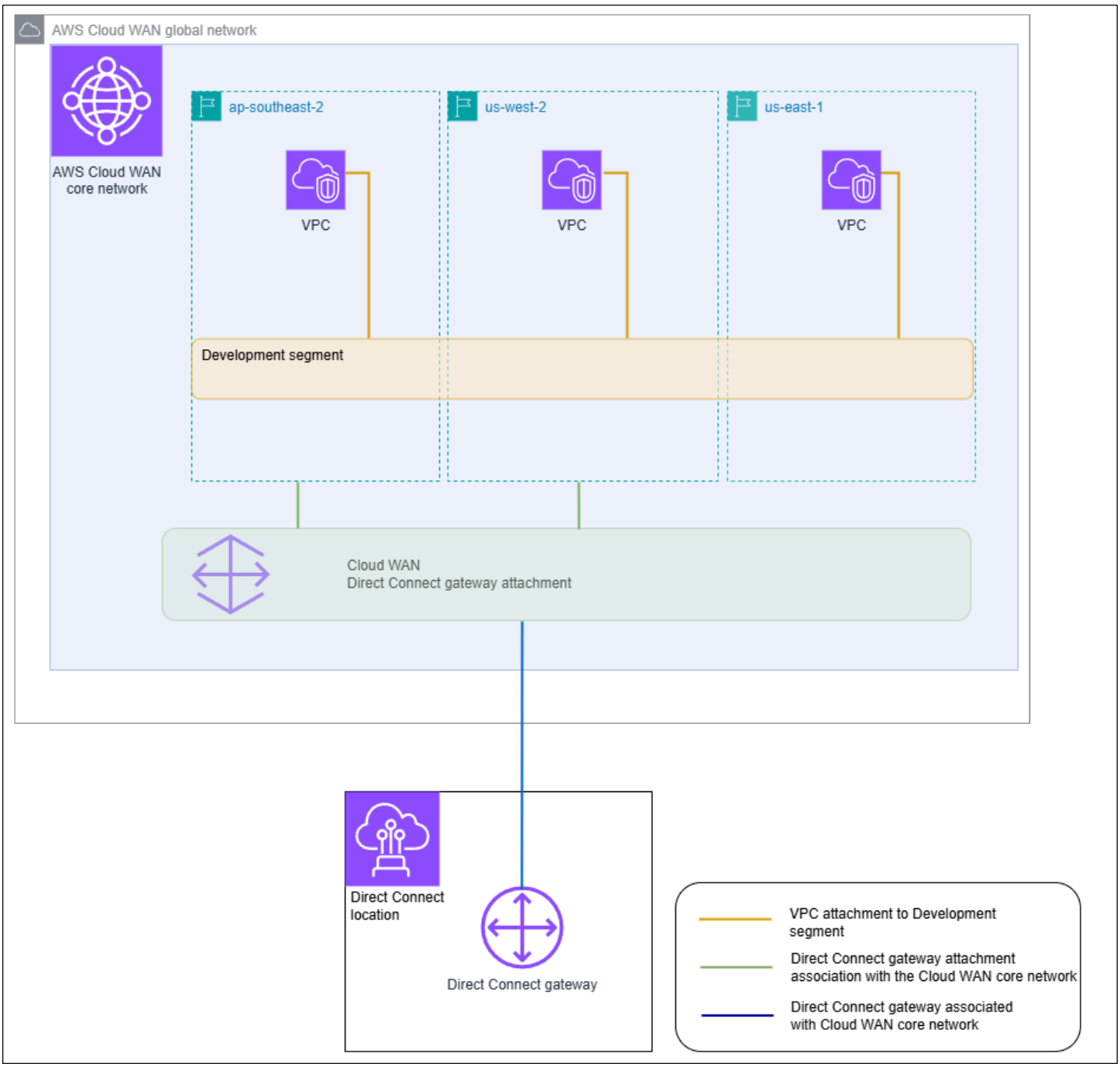
Cloud WAN の Direct Connect アタッチメントタイプを使用して、Direct Connect ゲートウェイを AWS Cloud WAN コアネットワークに関連付けます。この直接関連付けにより、コアネットワークの選択されたエッジロケーションと Direct Connect 接続間のトラフィックが、利用可能な最短パスを使用してルーティングされます。

Direct Connect ゲートウェイアタッチメントタイプは、コアネットワークとオンプレミスロケーション間のルーティング情報の自動伝達のために BGP (ボーダーゲートウェイプロトコル) をサポートしています。Direct Connect アタッチメントは、一元的なポリシーベースの管理、タグベースのアタッチメントオートメーション、高度なセキュリティ設定のセグメンテーションなどの標準の Cloud WAN 機能もサポートしています。

> **Note**
>
> コアネットワークと Direct Connect ゲートウェイ間の関連付けは、Network Manager の Cloud WAN コンソールから作成、削除、管理されます。Cloud WAN で Direct Connect ゲートウェイを使用する場合、Direct Connect コンソールおよび API と CLI には関連付けが反映

されますが、変更には使用できません。ただし、Direct Connect API またはコマンドラインを使用して、関連付けが作成されたかどうかを確認することはできます。

次の例は、Cloud WAN コアネットワーク内に 3 つのリージョンを持つ Cloud WAN グローバルネットワークを示しています。各リージョンには独自の VPC があり、それらは 3 つのリージョン間で共有されるコアネットワーク開発セグメントに接続されています。Cloud WAN を使用すると、Direct Connect を使用して作成された Direct Connect ゲートウェイを使用して、Cloud WAN 内に Direct Connect ゲートウェイアタッチメントが作成されます。アタッチメントは、3 つのリージョンのうち 2 つ (ap-southeast-2 と us-west-2) に関連付けられており、開発セグメントへのアクセスが許可されています。us-east-1 は同じ開発セグメントを共有していますが、Direct Connect ゲートウェイアタッチメントはそのリージョンと共有されていないため、利用できません。



トピック

- 前提条件
- 考慮事項
- Cloud WAN コアネットワークへの Direct Connect ゲートウェイの関連付け
- AWS Cloud WAN コアネットワークへの Direct Connect ゲートウェイの関連付けを検証する

前提条件

Cloud WAN コアネットワークとの Direct Connect ゲートウェイの関連付けには、以下が必要です。

- 既存の Direct Connect ゲートウェイ。Direct Connect ゲートウェイを作成する手順については、「Direct Connect ゲートウェイを作成する」を参照してください。
- AWS Cloud WAN コアネットワーク。Cloud WAN の詳細については、AWS Cloud WAN ユーザーガイドを参照してください。

考慮事項

Cloud WAN コアネットワークとの Direct Connect ゲートウェイの関連付けには、次の制限が適用されます。

- Direct Connect ゲートウェイは、単一の Cloud WAN コアネットワークとそのコアネットワークの単一のセグメントに関連付けることができます。関連付けが作成されると、そのゲートウェイは AWS リージョン内の他のリソースに関連付けることができなくなります。コアネットワークからゲートウェイの関連付けを解除すると、そのゲートウェイを他の関連付けタイプに使用できるようになります。
- Cloud WAN Direct Connect ゲートウェイアタッチメントでは、接続にトランジット仮想インターフェイスタイプが使用されます。
- Cloud WAN アタッチメントは、許可されたプレフィックスリストをサポートしていません。コアネットワークセグメント内のすべてのプレフィックスは、そのセグメントに関連付けられた Direct Connect ゲートウェイにアドバタイズされます。
- オンプレミスから AWS にトランジット仮想インターフェイス経由でアドバタイズできる最大プレフィックスのクォータは、Cloud WAN コアネットワークからオンプレミスにアドバタイズされるプレフィックスのクォータとは異なります。Cloud WAN の関連付けで使用されるその他の Direct Connect リソースのクォータも適用できます。「Direct Connect クォータ」を参照してください。
- AS-PATH BGP 属性は、コアネットワーク、Direct Connect ゲートウェイ、仮想インターフェイス全体で保持されます。
- Direct Connect ゲートウェイの ASN は、Cloud WAN コアネットワーク用に設定された ASN 範囲外である必要があります。例えば、コアネットワークの ASN 範囲が 64512 ~ 65534 の場合、Direct Connect ゲートウェイの ASN はその範囲外の ASN を使用する必要があります。
- Cloud WAN は、トランスポート用の Direct Connect アタッチメントタイプを使用する特定のアタッチメントタイプをサポートしない可能性があります。Cloud WAN コアネットワークへの

Direct Connect ゲートウェイアタッチメントの詳細については、AWS Cloud WAN ユーザーガイドの「Direct Connect gateway attachments in AWS Cloud WAN」を参照してください。

- CloudWatch Network Monitor は、Cloud WAN Direct Connect ゲートウェイアタッチメントタイプで使用する場合、レイテンシーとパケット損失のメトリクスをサポートします。ネットワークヘルスインジケータ機能はサポートされていません。詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch Network Monitor の使用」を参照してください。

Cloud WAN コアネットワークへの Direct Connect ゲートウェイの関連付け

Direct Connect ゲートウェイを AWS Cloud WAN コアネットワークに関連付けるには、AWS Cloud WAN コンソール、Cloud WAN API、またはコマンドラインを使用します。

既存の Direct Connect ゲートウェイを Cloud WAN コアネットワークに関連付けるには、Cloud WAN コンソールで新しい Direct Connect アタッチメントを作成します。Direct Connect アタッチメントが作成されると、関連付けが確立されます。デフォルトでは、関連付けを作成するときに、選択したコアネットワークセグメント内のすべてのコアネットワークエッジロケーションを含めるようにデフォルトを選択できます。または、個々のエッジロケーションを指定することもできます。

Cloud WAN コアネットワークへの Direct Connect ゲートウェイアタッチメントの詳細については、AWS Cloud WAN ユーザーガイドの「Direct Connect gateway attachments in AWS Cloud WAN」を参照してください。

AWS Cloud WAN コアネットワークへの Direct Connect ゲートウェイの関連付けを検証する

Direct Connect コンソール、Direct Connect API、またはコマンドラインを使用して、Direct Connect ゲートウェイと Cloud WAN コアネットワークの関連付けを検証できます。

コンソールを使用して Direct Connect ゲートウェイと Cloud WAN コアネットワークとの関連付けを検証するには

1. 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] を選択します。
3. 関連付けを表示する Direct Connect ゲートウェイアタッチメントを選択します。
4. [Gateway associations] (ゲートウェイの関連付け) タブを選択します。

- [ID] 列には、Direct Connect ゲートウェイが関連付けられているコアネットワーク ID が表示されます。
- [状態] 列には、[関連付け] が表示されます。
- [関連付けタイプ] 列には、[Cloud WAN コアネットワーク] が表示されます。

コマンドラインまたは API を使用して Direct Connect ゲートウェイと Cloud WAN コアネットワークとの関連付けを検証するには

- DescribeDirectConnectGatewayAssociations (Direct Connect API)
- describe-direct-connect-gateway-association (AWS CLI)

Direct Connect ゲートウェイでの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、「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したり削除されたりする可能性があります。

Transit Gateway 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。

- Transit Gateway 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。

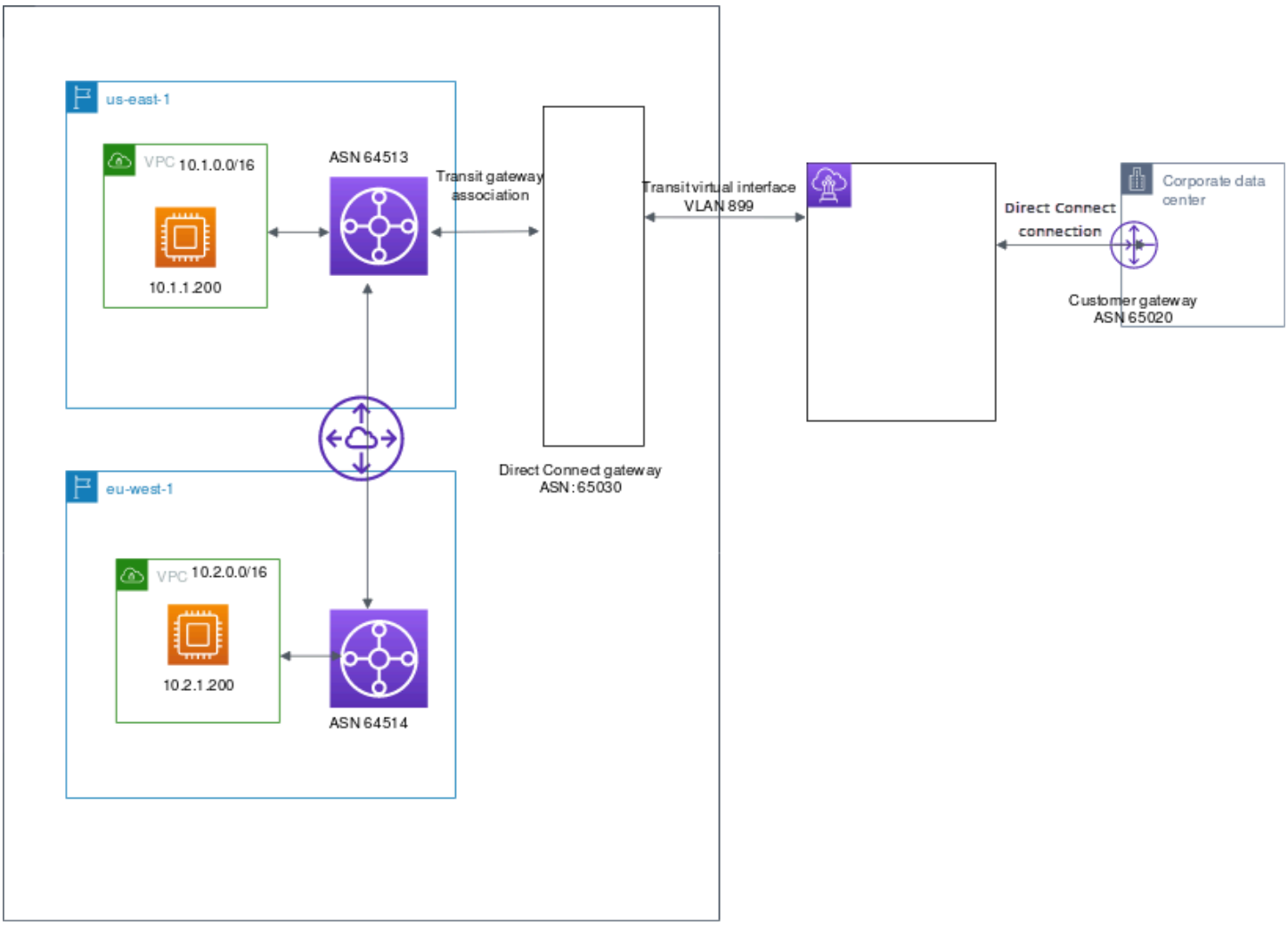
複数の Transit Gateway が Direct Connect ゲートウェイに関連付けられている場合、許可されるプレフィックスの重複は許可されません。例えば、許可されたプレフィックスリストに 10.1.0.0/16 を含む Transit Gateway があり、許可されたプレフィックスリストが 10.2.0.0/16 と 0.0.0.0/0 を含む 2 番目の Transit Gateway がある場合、2 番目の Transit Gateway からの関連付けを 0.0.0.0/0 に設定することはできません。0.0.0.0/0 にはすべての IPv4 ネットワークが含まれるため、複数の Transit Gateway 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したり削除されたりする可能性があります。

例: Transit Gateway 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 Transit Gateway 。
- 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。
- Transit Gateway (us-east-1 のゲートウェイ) と Direct Connect ゲートウェイの間の Transit Gateway の関連付け。
- オンプレミスの口ケーションと 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、「Direct Connect ゲートウェイを作成する」を参照してください。
- トランジット仮想インターフェイス: VLAN を 899、お客様のルーターピア ASN を 65020 に設定します。詳細については、「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 Transit Gateway 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 (10.0.0.0/16 および 10.2.0.0/16) を含みます。詳細については、「Transit Gateway と Direct Connect の関連付けまたは関連付け解除。」を参照してください。

- VPC ルート: 10.2.0.0/16 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、Transit Gateway ID がターゲットになります。これにより、VPC からのトラフィックが Direct Connect ゲートウェイに到達できるようになります。Transit Gateway 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 リソースにタグを付ける

タグは、リソースの所有者が自分の 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、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 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、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 Direct Connect リソースは、Direct Connect コンソール、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	あり	あり	はい
仮想インターフェイス	はい	あり	あり	いいえ
Link aggregation groups (LAG)	はい	あり	あり	はい
相互接続	はい	あり	あり	はい
Direct Connect ゲートウェイ	可能	あり	あり	不可

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	tag-resource
1 つ以上のタグを削除します。	UntagResource	untag-resource
1 つ以上のタグを記述します。	タグの説明	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」 ではクラウドセキュリティが最優先事項です。セキュリティを最も重視する組織の要件を満たすために構築された 「AWS」 のデータセンターとネットワークアーキテクチャは、お客様に大きく貢献します。

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、この責任が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されています。

- 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、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。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Direct Connect を設定する方法を示します。また、Direct Connect リソースのモニタリングや保護に役立つ、その他 AWS サービスの使用方法についても説明します。

トピック

でのデータ保護AWS Direct Connect

AWS責任共有モデル は、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。ユーザーは、このインフラストラクチャでホストされ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に関する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」 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が各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 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、TLS 1.3 をお勧めします。
- AWS CloudTrail で API とユーザーアクティビティロギングを設定します。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「AWS CloudTrail ユーザーガイド」の「CloudTrail 証跡の使用」を参照してください。
- AWS のサービス 内のすべてのデフォルトセキュリティコントロールに加え、AWS 暗号化ソリューションを使用します。
- Amazon Macie などの高度な管理された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 を使用して 「AWS」 にアクセスする際に FIPS 140-3 検証済みの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) 140-3」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 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。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

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、「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、「仮想プライベートゲートウェイの関連付け」および「Transit Gateway 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、「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、「仮想プライベートゲートウェイの関連付け」および「Transit Gateway 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 では、転送中のトラフィックはデフォルトでは暗号化されません。AWS Direct Connect を通過する転送中のデータを暗号化するには、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 インスタンスのトラフィック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 AWS Site-to-Site VPN では、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 Direct Connect 接続を使用して、企業のデータセンターから Direct Connect 口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 (MACsec)」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
- アイデンティティによる認証
- ポリシーを使用したアクセス権の管理
- Direct Connect が IAM と連携する仕組み
- Direct Connect アイデンティティベースのポリシーの例
- Direct Connect のサービスにリンクされたロール
- AWS 用の 管理ポリシーAWS Direct Connect
- 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

対象者

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者に許可をリクエストします (「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)
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「Direct Connect が IAM と連携する仕組み」を参照)

- IAM 管理者 - アクセスを管理するポリシーを記述します (「Direct Connect アイデンティティベースのポリシーの例」を参照)

アイデンティティによる認証

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

AWS IAM Identity Center (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーテッドアイデンティティとしてサインインできます。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「How to sign in to your AWS アカウント」を参照してください。

プログラムによるアクセスの場合、AWS はリクエストに暗号で署名するための SDK と CLI を提供します。詳細については、「IAM ユーザーガイド」の「API リクエストに対する AWS Signature Version 4」を参照してください。

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と、すべての AWS のサービスとリソースに対する完全なアクセス権を持つ AWS アカウントルートユーザーと呼ばれる 1 つのサインイン ID を使用して開始します。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。ルートユーザー認証情報を必要とするタスクについては、「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。

フェデレーテッドアイデンティティ

ベストプラクティスでは、人間のユーザーが一時的な認証情報を使用して AWS のサービス にアクセスする際、アイデンティティプロバイダーとのフェデレーションを使用することが求められます。

フェデレーテッドアイデンティティは、エンタープライズディレクトリ、ウェブ ID プロバイダー、Directory Service のユーザーであり、ID ソースからの認証情報を使用して AWS のサービスにアクセスするユーザーです。フェデレーティッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、AWS IAM Identity Center をお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたは 1 つのアプリケーションに対して特定の許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの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。詳細については、「IAM ユーザーガイド」の「人間のユーザーが一時的な認証情報を使用して AWS にアクセスするにはID プロバイダーとのフェデレーションの使用が必要です」を参照してください。

IAM グループは IAM ユーザーのコレクションを指定し、大量のユーザーのアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、一時的な認証情報を提供する特定のアクセス許可を持つ ID です。ユーザーから IAM ロールに切り替える (コンソール)、または AWS CLI や AWS API オペレーションを呼び出すことで、ロールを引き受けることができます。詳細については、「IAM ユーザーガイド」の「ロールを引き受けることができない」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行されているアプリケーションに役立ちます。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

ポリシーを使用したアクセス権の管理

AWS でアクセスを制御するには、ポリシーを作成して AWS ID またはリソースにアタッチします。ポリシーはアイデンティティやリソースに関連付けて、これらのアクセス許可を定義します。AWS は、プリンシパルがリクエストを行う際に、それらのポリシーを評価します。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。

ポリシーを使用して、管理者は、どのプリンシパルがどのリソースに対してどの条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

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 IAM ポリシーを作成し、ユーザーが引き受けることができるロールに追加します。IAM ポリシーは、オペレーションの実行方法を問わずアクセス許可を定義します。

アイデンティティベースのポリシー

アイデンティティベースのポリシーは、アイデンティティ (ユーザー、グループ、ロール) にアタッチする JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティ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ポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

ID ベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーおよびインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチする JSON ポリシードキュメントです。例としては、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーなどがあります。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コントロールできます。リソースベースのポリシーで、プリンシパルを指定する必要があります。

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 IAM の AWS マネージドポリシーを使用することはできません。

その他のポリシータイプ

AWS 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る、追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできる許可の上限を設定します。詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可境界」を参照してください。
- サービスコントロールポリシー (SCP) – AWS Organizations において組織または組織単位のアクセス許可の上限を指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCP) – アカウント内のリソースで利用できるアクセス許可の上限を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。

- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを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。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

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

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	なし
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
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	あり
プリンシパルアクセス権限	あり
サービスロール	あり
サービスリンクロール	なし

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 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のポリシーのサポート: あり

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

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

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には例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、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。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」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のサポート:あり

管理者は AWS JSON 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。

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。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 アクションの一覧は、「サービス認可リファレンス」の「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": [
      "directconnect:action1",
      "directconnectaction2"
         ]
```

Direct Connect のポリシーリソース

ポリシーリソースのサポート: あり

管理者は AWS JSON ポリシーを使用して、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。

`Resource` JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。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。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」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: あり

管理者は AWS JSON 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。

`Condition` 要素は、定義された基準に基づいてステートメントが実行されるタイミングを指定します。イコールや未満などの 条件演算子 を使用して条件式を作成して、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。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「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許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Direct Connect で使用できる ABAC

ABAC (ポリシー内のタグ) のサポート: 一部

属性ベースのアクセス制御 (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグを付けることで、プリンシパルのタグがリソースタグと一致するときに操作を許可する ABAC ポリシーを設計できます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素 でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順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「属属性ベースのアクセス制御 (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

一時的な認証情報は、AWS リソースへの短期的なアクセスを提供し、フェデレーションまたはスイッチロールの使用時に自動的に作成されます。AWS では、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 ユーザーガイド」の「IAM の一時的な認証情報」および「IAM と連携する AWS のサービス」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

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、AWS のサービスを呼び出すプリンシパルの権限を、AWS のサービスのリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエストを行います。FASリクエスト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

サービスロールのサポート: 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 に許可を委任するロールを作成する」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: なし

サービスにリンクされたロールは、AWS のサービス にリンクされているサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント に表示され、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

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「サービスリンクロール」列に Yes と記載されたサービスを見つけます。サービス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。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。

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 (コンソール)」を参照してください。

Direct Connect で定義されるアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「サービス認可リファレンス」の「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

ポリシーに関する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では、AWS アカウント に費用が発生する場合があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS マネージドポリシーを使用して開始し、最小特権の許可に移行する – ユーザーとワークロードへの許可の付与を開始するには、多くの一般的なユースケースのために許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能の AWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。また、CloudFormation などの特定の AWS のサービス を介して使用する場合、条件を使用してサービスアクションへのアクセスを許可することもできます。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語

(JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。

- 多要素認証 (MFA) を要求する – AWS アカウントで IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

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、また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 ポリシーの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。

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。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、Direct Connect に読み取りアクセス権限が付与されます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

次のポリシーの例では、Direct Connect にフルアクセス権限が付与されます。

JSON

```
{
    "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。

`Resource` JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。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。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 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}`
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「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。

DescribeConnections、DescribeVirtualInterfaces、DescribeDirectConnectGateways、DescribeInterconnects または DescribeLags の IAM ポリシーステートメントの Resource フィールドに * 以外のリソース ARN またはリソース ARN パターンが指定されている場合、一致するリソース ID も API コールで渡されない限り、指定された Effect は発生しません。ただし、IAM ポリシーステートメントで特定のリソース ID ではなくリソースとして * を指定すると、指定した Effect が機能します。

次の例では、リクエストで connectionId が渡されずに DescribeConnections アクションが呼び出された場合、指定された Effect はどちらも成功しません。

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/*"
        ]
    },
```

```
{
        "Effect": "Deny",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/example1"
        ]
    }
]
```

ただし、次の例では、リクエストで connectionId が指定されたかどうかに関係なく、IAM ポリシーステートメントの Resource フィールドに * が指定されているため、DescribeConnections アクションに対して "Effect": "Allow" が成功します。

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections
        ],
        "Resource": [
            "*"
        ]
    }
]
```

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。

Condition 要素は、定義された基準に基づいてステートメントが実行されるタイミングを指定します。イコールや未満などの 条件演算子 を使用して条件式を作成して、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。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とリソースについては、「Direct Connect で定義されるアクション」を参照してください。

Direct Connect 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": "*"
        }
    ]
}
```

Direct Connect への読み取り専用アクセス

次のポリシーの例では、Direct Connect に読み取りアクセス権限が付与されます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Direct Connect へのフルアクセス

次のポリシーの例では、Direct Connect にフルアクセス権限が付与されます。

JSON

```
{
    "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。

JSON

```
        {
```

```
    "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、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。

JSON

```
  {
      "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。

JSON

```
    {
     "Version":"2012-10-17",
     "Statement": {
       "Effect": "Allow",
       "Action": "directconnect:TagResource",
       "Resource": "*",
       "Condition": {
         "ForAllValues:StringEquals": {
           "aws:TagKeys": [
             "environment"
           ]
         }
       }
     }
    }
```

Direct Connect のサービスにリンクされたロール

AWS Direct Connect では AWS Identity and Access Management (IAM) のサービスリンクロールを使用します。サービスリンクロールは、Direct Connect に直接リンクされた一意のタイプの IAM ロールです。サービスリンクロールは、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権限を備えています。

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、Direct Connect の設定が簡単になります。このサービスリンクロールのアクセス許可は Direct Connect で定義します。特に定義されている場合を除き、Direct Connect のみがその口ールを引き受けることができます。定義された権限には、信頼ポリシーと権限ポリシーに含まれており、その権限ポリシーを他の 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、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 サービス」を参照して、[サービスにリンクされたロール] 列で [はい] になっているサービスを見つけます。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。

Direct Connect のサービスリンクロールのアクセス許可

Direct Connect は、 という名前のサービスリンクロールを使用します。`AWSServiceRoleForDirectConnect`これは、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。

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) に許可するにはアクセス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、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。

JSON

```
{
    "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。

Direct Connect のサービスリンクロールの作成

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、Direct Connect が AWS マネジメントコンソール、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 アカウントに新しいロールが表示される」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、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。

Direct Connect のサービスにリンクされたロールの編集

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。サービスリンク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 を使用したロール記述の編集はできます。詳細については、『IAM ユーザーガイド』の「サービスにリンクされたロールの編集」を参照してください。

Direct Connect のサービスリンクロールの削除

`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 マネジメントコンソール、AWS CLI、 AWS API、または 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 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 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。

Direct Connect のサービスリンクロールをサポートするリージョン

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 用の 管理ポリシーAWS Direct Connect

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に対してアクセス許可を提供するように設計されているため、ユーザー、グループ、ロールへのアクセス権の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることにご注意ください。これは、すべての AWS ユーザーが使用できるようになるのを避けるためです。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可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されたアクセス許可は変更できません。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、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 マネジメントコンソール 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、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 マネジメントコンソール 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、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 “サービスリンクロール”」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 マネジメントコンソール の「AWSDirectConnectServiceRolePolicy」を参照してください。

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、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、「Direct Connect ドキュメン履歴ページ」ページで 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、AWSServiceRoleForD	2021 年 3 月 31 日

変更	説明	日付
	irectConnect が追加されました。	
Direct Connect は変更の追跡を開始しました	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
- iam:PassRole を実行する権限がありません
- 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

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、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なdirectconnect:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 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。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して 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または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許可されています。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。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

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コントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください。

- 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「サードパーティーが所有する AWS アカウント へのアクセス権を付与する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

AWS 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、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 CloudWatch で を監視する」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、「を使用した Direct Connect API コールのログ記録AWS CloudTrail」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、「Direct Connect のリソースをモニタリングする」を参照してください。

AWS Direct Connect のコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの対象であるかどうかを確認するには、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」をご覧いただき、関心のあるコンプライアンスプログラムを選択してください。一般的な情報については、「AWSコンプライアンスプログラム」を参照してください。

AWS Artifact を使用して、サードパーティーの監査レポートをダウンロードできます。詳細については、「AWS Artifact でレポートをダウンロードする」を参照してください。

AWS のサービス を使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性や貴社のコンプライアンス目的、適用可能な法律および規制によって決定されます。AWS のサービスを使用する際のコンプライアンス責任の詳細については、「AWS セキュリティドキュメント」を参照してください。

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として構築されています。AWSリージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立し隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

AWS では、Direct Connect グローバルインフラストラクチャに加えて、データの回復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、「the section called “AWS Direct Connect Resiliency Toolkit”」を参照してください。

Direct Connect 内のインフラストラクチャセキュリティ

マネージドサービスである AWS 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 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、一時的ディフィー・ヘルマン 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、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。またはAWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

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、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、Direct Connect ポリシーを使用して、特定の Amazon Virtual Private Cloud (Amazon VPC) エンドポイントあるいは特定の 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 Direct Connect ネットワーク内の特定の VPC からの特定の AWS 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 “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。

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。

Direct Connect CLI を使用する

AWS CLI を使用して 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、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 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、「専用接続とホスト接続」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 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

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「the section called “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、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、Amazon にアドレスを生成させることが可能です。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、Amazonが自動的に割り当てます。

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、Amazon が自動的に割り当てます。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>
```

を使用した Direct Connect API コールのログ記録AWS CloudTrail

Direct Connect は AWS CloudTrail という、Direct Connect の ユーザー、ロール、または AWS のサービスが実行したアクションを記録するサービスと統合しています。CloudTrail は、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。キャプチャされたコールには、Direct Connect コンソールのコールと、Direct Connect API オペレーションへのコードのコールが含まれます。証跡を作成する場合は、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 「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、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。

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。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、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、コンソールで証跡を作成すると、すべての AWS リージョンに証跡が適用されます。証跡は、AWSパーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- 複数のリージョンから CloudTrail ログファイルを受け取る、および複数のアカウントから CloudTrail ログファイルを受け取る

すべての Direct Connect アクションは CloudTrail によってログに記録され、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。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルートまたは 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テンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS サービスによって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。

Direct Connect ログファイルエントリについて理解する

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。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、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
    },
    ...
  ]
}
```

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定します。Direct Connect をモニタリングする際、過去のモニタリングデータを保存することができます。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。

ベースラインを確定するには、物理的な Direct Connect 接続の使用状況、状態、正常性をモニタリングする必要があります。

内容

モニタリングツール

AWS は、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を提供します。これらのツールの中には、自動モニタリングを設定できるものもあれば、手操作を必要とするものもあります。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

以下の自動化された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。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 CloudWatch で を監視する 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、「API コールをログする」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。

手動モニタリングツール

Direct Connect 接続のモニタリングでもう 1 つ重要な点は、CloudWatch の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 および CloudWatch のコンソールダッシュボードには、AWS 環境の状態が一目でわかるビューが表示されます。

- 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 のホームページには、以下の情報が表示されます。
  - 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

  また、CloudWatch を使用して以下のことを行えます。
  - 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。

- AWS リソースのすべてのメトリクスを検索およびブラウズする。
- 問題があることを通知するアラームを作成/編集する。

Amazon CloudWatch で を監視する

CloudWatch を使用して、物理的な 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 は Direct Connect から生データを収集し、それを処理して読み取り可能なメトリクスを生成します。デフォルトでは、CloudWatch は Direct Connect メトリックデータを 5 分間隔で提供します。各間隔のメトリクスデータは、その間隔中に収集された少なくとも 2 つのサンプルの集計値です。

Amazon CloudWatch の詳細については、Amazon CloudWatch ユーザーガイドを参照してください。また、サービスの CloudWatch をモニタリングして、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、「CloudWatch メトリクスを発行する AWS のサービス」を参照してください。

目次

Direct Connect のメトリクスとディメンション

メトリクスは、Direct Connect 物理接続と仮想インターフェイスで使用できます。

Direct Connect の接続メトリクス

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: このメトリクスで返される単位はありません。
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。CloudWatch で選択した間隔 (5 分間など) 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。 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 側から送信 (出力) されるトラフィックのファイバー接続状態を示します。 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、「Direct Connect で利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 側に受信 (入力) されるトラフィックのファイバー接続状態を示します。 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、「Direct Connect で利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。

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、Direct Connect 仮想インターフェイスから入手できます。

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

Direct Connect の使用可能なディメンション

以下のディメンションを使用して 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では、ConnectionLightLevelTx データと ConnectionLightLevelRx データをフィルターし、Direct Connect 接続の光レーン番号でデータをフィルターします。
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ーします。

トピック

Direct Connect CloudWatch メトリクスを表示する

Direct Connect は、Direct Connect 接続に関する次のメトリクスを送信します。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**
>
> CloudWatch を介して Direct Connect をモニタリングする場合は、メトリクスを 1 分間隔でリクエストできます。ただし、実際の更新頻度は CloudWatch によって制御されます。間隔は CloudWatch によって制御されるため、Direct Connect は必ずしも 5 分未満の間隔を保証することはできません。

以下の手順を使用して、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。Amazon CloudWatch を使用して Direct Connect メトリクスを表示する方法 (数学関数や事前構築済みクエリの追加を含む) の詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch メトリクスを使用する」を参照してください。

1. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
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 [Metric name] (メトリクス名) をクリックし、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 Metric 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。

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. 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。

AWS CLI を使ってメトリクスを表示するには

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"
```

Direct Connect 接続をモニタリングする Amazon CloudWatch アラームの作成

アラームの状態が変わったら、Amazon SNS メッセージを送信する Amazon CloudWatch のアラームを作成することができます。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、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。アラームを作成するために知っておくべきことと、アラームの作成に関する詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch アラームを使用する」を参照してください。

CloudWatch アラームを作成するには。

1. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
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. [Create Alarm] (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. 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に関する詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch アラームを使用する」を参照してください。
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に関する詳細については、「Amazon CloudWatch 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。
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。

Direct Connect のクォータ

次の表に、Direct Connect に関連するクォータの一覧を示します。

コンポーネント	クォータ	コメント
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数	50	この制限を増やすことはできません。
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数。 トランジット仮想インターフェイスを使用すると、Transit Gateway または AWS Cloud WAN コアネットワークに接続できます。詳細については、「ゲートウェイ」を参照してください。	4	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。
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数、および 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数	51	AWS Direct Connect による Amazon VPC Transit Gateway のサポートが開始されたとき、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 つのトランジット仮想インターフェイスの割り当てが追加されました。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。
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。

コンポーネント	クォータ	コメント
1 つのアカウントで、リージョンごとの Direct Connect ロケーションあたりのアクティブな 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	AWS Direct Connect による Amazon VPC Transit Gateway のサポートが開始されたとき、LAG 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 つのトランジット仮想インターフェイスの割り当てが追加されました。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。
プライベート仮想インターフェイス、またはオンプレミスから AWS へのトランジット仮想インターフェイスで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 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	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。
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。
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。
Direct Connect ゲートウェイ当たりの仮想プライベートゲートウェイの数	20	この制限を増やすことはできません。
Direct Connect ゲートウェイあたりの Transit Gateway 数	6	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
AWS Cloud WAN コアネットワークの Direct Connect ゲートウェイアタッチメントからオンプレミスにアドバタイズされるルートプレフィックスの最大数。 **Note** 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はすべて、コアネットワークによってアドバタイズされたすべてのルートプレフィックスを受け取ります。	5,000	詳細については、ソリューションアーキテクト (SA) またはテクニカルアカウントマネージャー (TAM) にお問い合わせください。
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。
トランジット仮想インターフェイスでの AWS からオンプレミスへの AWS Transit Gateway あたりのプレフィックス数	IPv4 と IPv6 に合計で 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。
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。	
Transit Gateway 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 プレフィックス限度	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。

Direct Connect はシングルモードファイバーで、1000BASE-LX (1310 nm) では 1 Gbps、10GBASE-LR (1310 nm) では 10 Gbps、100GBASE-LR4 では 100 Gbps、400GBASE-LR4 では 400 Gbps のポート速度をサポートします。

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

ASN の制限

Direct Connect で使用される自律システム番号 (ASN) には、次の制限が適用されます。

- お客様側の ASN 範囲: 1 ~ 4,294,967,294
  - ASN: 1 ~ 2147483647
  - ロング ASN: 1 ~ 4294967294
- Amazon 側の ASN: AWS によって割り当てられる固定値 (パブリック仮想インターフェイスの場合、通常は 7224)
- プライベート ASN 範囲:
  - プライベート ASN: 64,512 ~ 65,534
  - プライベートロング ASN: 4,200,000,000 ~ 4,294,967,294

> **Note**
>
> パブリック仮想インターフェイスの場合、ASN はプライベート ASN であるか、既に登録されていて、仮想インターフェイスでの使用が許可されている必要があります。

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。

Direct Connect のトラブルシューティング

以下のトラブルシューティング情報は、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

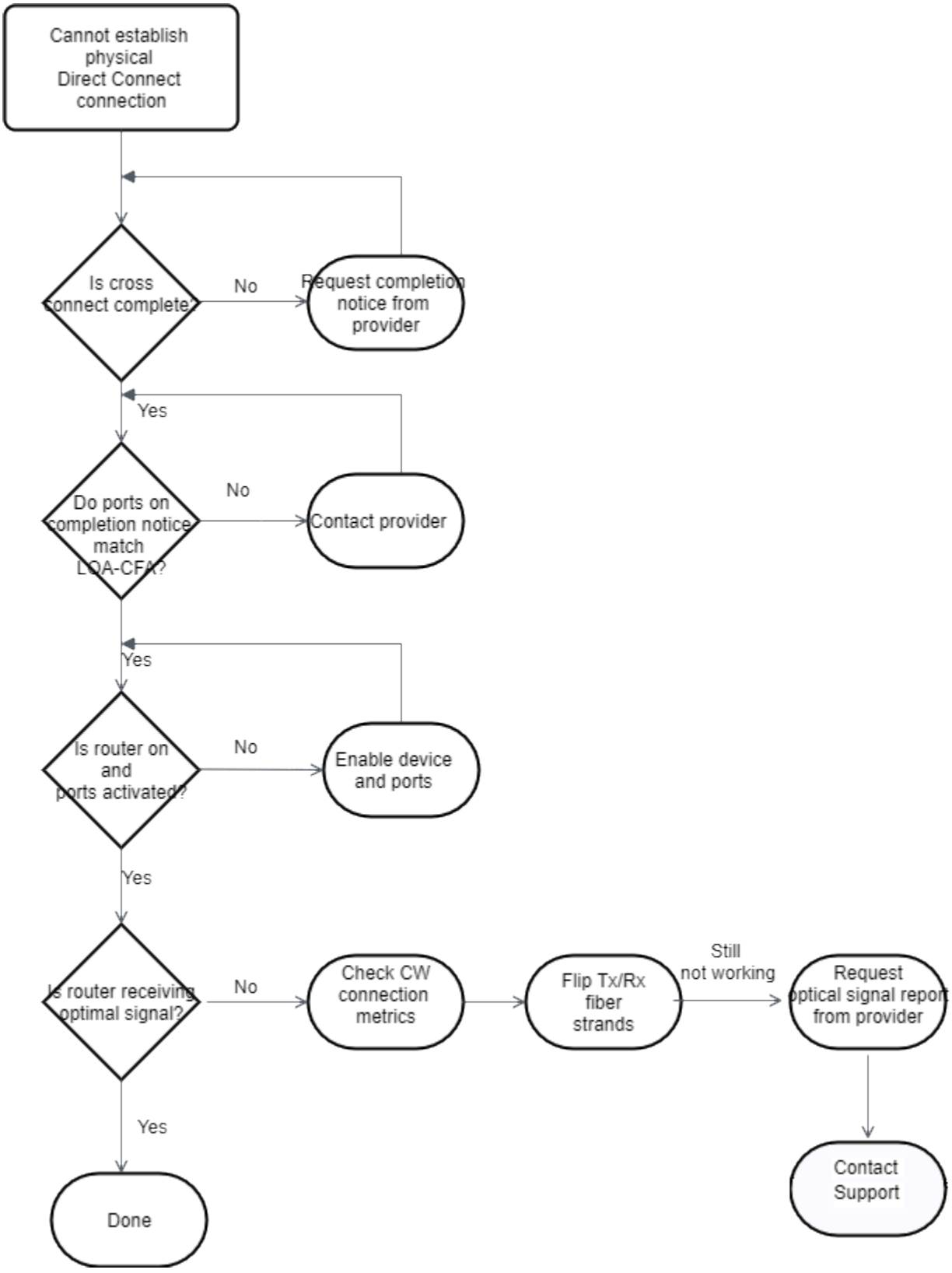
レイヤー 1 (物理層) の問題のトラブルシューティング

お客様、またはお客様のネットワークプロバイダによる Direct Connect デバイスへの物理的な接続の確立で問題が発生した場合は、次のステップを使用して、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、AWS Direct Connect エンドポイントが接続を処理する場合、1 Gbps 接続でオート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) の問題のトラブルシューティング を参照してください。接続の終了を処理する Direct Connect エンドポイントによっては、必要に応じてオート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。
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. Direct Connect の Amazon CloudWatch メトリクスをチェックします。Direct Connect デバイスの送信/受信の光学読み取り (1 Gbps と 10 Gbps の両方)、物理的なエラー数、およびオペレーションステータスを確認できます。詳細については、「Amazon CloudWatch によるモニタリング」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 サポート 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。

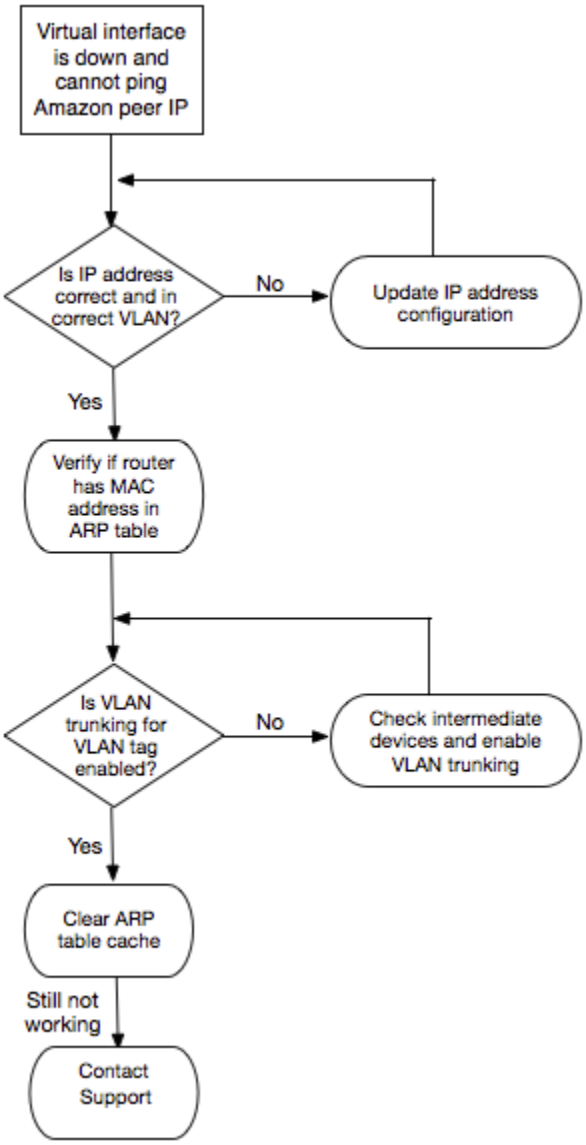

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check 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) の問題のトラブルシューティング

Direct Connect の物理的な接続は機能しているが、仮想インターフェイスがダウンしている場合は、以下のステップ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 (たとえば、GigabitEthernet0/0 ではなく GigabitEthernet0/0.123) で設定されていることを確認します。
2. アドレス解決プロトコル (ARP) テーブルにある AWS エンドポイントからの MAC アドレスのエントリがルーターにあることを確認します。
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。AWS がタグ付けされたトラフィックを受信するまでは、ARP を AWS 側に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. 上記のステップを実行しても ARP が確立されない、または Amazon ピア IP に ping を送信できない場合は、AWS Support 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。



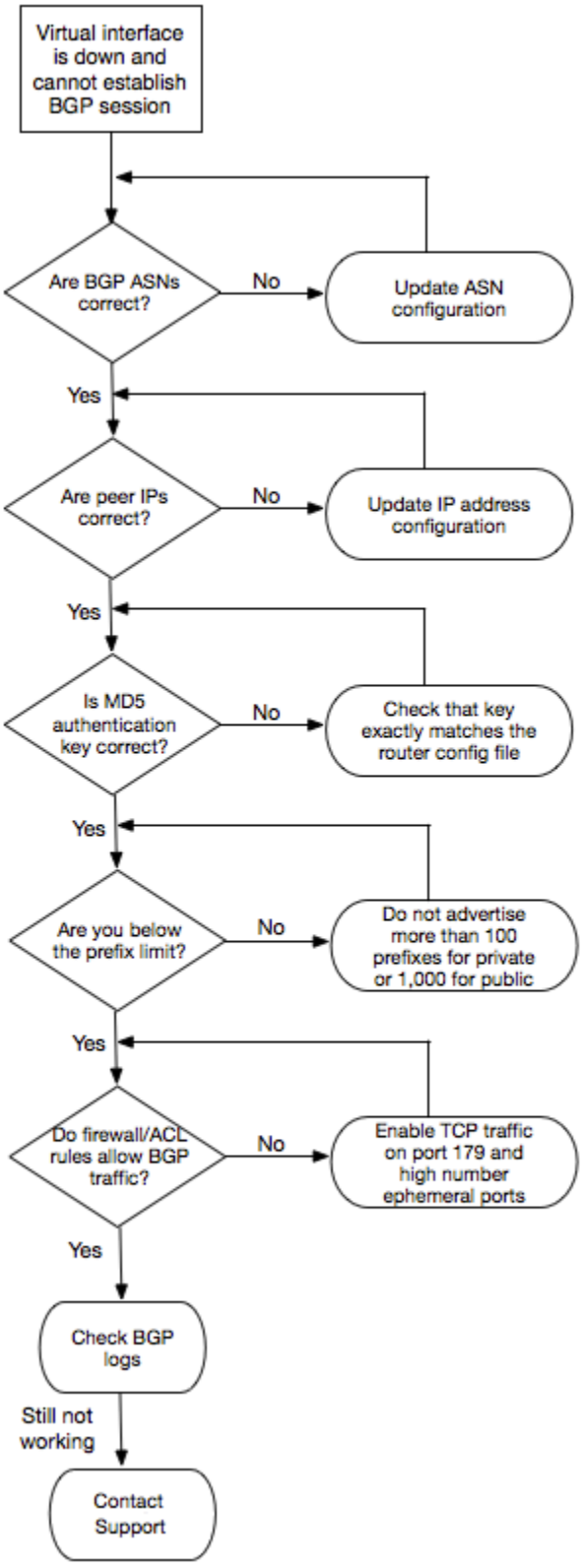
これらのステップの確認後に BGP セッションがまだ確立されない場合は、「レイヤー 3/4 (ネットワーク層/トランスポート層) の問題のトラブルシューティング」を参照してください。BGP セッションが確立されたが、まだルーティングの問題が発生している場合は、「ルーティング問題のトラブルシューティング」を参照してください。

レイヤー 3/4 (ネットワーク層/トランスポート層) の問題のトラブルシューティング

Direct Connect の物理的な接続がアップしていて、Amazon のピア IP アドレスに対して 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稼働していて、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をトラブルシューティングしてください。

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. 上記のステップを実行しても BGP ピアリング接続セッションを確立できない場合は、AWS Support 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。

ロング ASN の問題のトラブルシューティング

ロング ASN 設定で問題が発生した場合は、次の手順を使用してトラブルシューティングを行います。

BGP セッションがロング ASN で失敗する

症状: ロング ASN を設定した後に BGP セッションが確立できない

原因: オンプレミスルーターがロング ASN 機能をサポートしていない可能性がある

解決策:*

- ルーターが RFC 6793 をサポートしていることを確認する
- BGP 設定を調べて ASN 形式が一貫していることを確認する
- BGP ログを調べて機能ネゴシエーションエラーが発生していないか確認する

API レスポンスに ASN が 0 と表示される

症状: API レスポンスに asn フィールドが 0 と表示される

原因: これは実際の ASN が 2,147,483,647 を超えると予想される動作

解決策: API レスポンスの asnLong フィールドを正しい ASN 値に使用する

ASN からロング ASN への移行の問題

症状: ASN 移行中に接続が失われる

原因: ASN を変更する場合は必要な BGP セッションの再確立が必要

解決策:*

- 移行をメンテナンス期間中に行うことを計画する
- 一度に 1 つの仮想インターフェイスを更新する
- 変更中に BGP セッションのステータスをモニタリングする
- 移行後にルーティングテーブルが収束したことを確認する

これらのトラブルシューティング手順を実行した後もロング ASN 設定の問題が解決しない場合は、以下の情報を用意して[AWS サポートにお問い合わせください]。

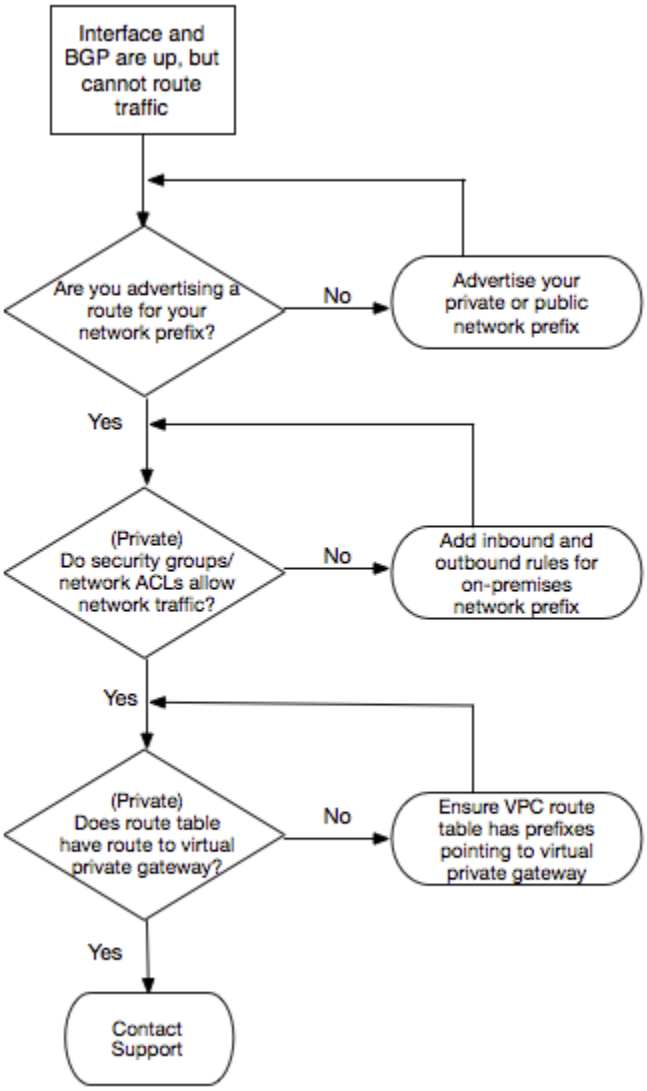
- 仮想インターフェイス ID または BGP ピア ID
- 設定されている ASN 値 (ASN とロング ASN の両方)
- ルーターモデルとソフトウェアバージョン
- BGP 設定とログ
- エラーメッセージまたは観察された症状

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. 上記のステップでルーティング問題が解決しない場合は、AWS Support 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。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブできます。

変更	説明	日付
ロング ASN のサポート	Direct Connect 仮想インターフェイスで BGP セッションにロング ASN 値を使用できるようになりました。	2025 年 7 月 24 日
Direct Connect ゲートウェイと AWS Network Manager コアネットワーク間の関連付けを作成する	Direct Connect と AWS Cloud WAN コアネットワークの間に Direct Connect ゲートウェイの関連付けを直接作成できるようになりました。	2024 年 11 月 25 日
G のサポート	400G 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。	2024 年 7 月 18 日
SiteLink プレフィックス制限を追加しました	SiteLink のプレフィックス制限がクォータと制限のトピックに追加されました。	2023 年 6 月 15 日
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プライベート仮想インターフェイスを作成することができます。	2021 年 12 月 1 日
MAC セキュリティのサポート	MACsec をサポートする Direct Connect 接続を使用して、企業のデータセンターから Direct Connect ロケーショ	2021 年 3 月 31 日

	ンへのデータを暗号化できます。	
G 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。	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。	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、接続のレジリエンシーをテストします。	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 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。	2020 年 5 月 11 日
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。	2019 年 10 月 7 日
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	AWS Transit Gateway アカウント全体に対する追加のリージョンのサポート	2019 年 9 月 30 日

AWS Direct Connect による AWS Transit Gateway のサポート	トランジット仮想インターフェイス経由で Transit Gateway にアタッチした VPC または VPN に Direct Connect 接続をつなげるには、Direct Connect ゲートウェイを使用します。Direct Connect ゲートウェイを Transit Gateway に関連付けます。次に、Direct Connect ゲートウェイへの 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。	2019 年 3 月 27 日
ジャンボフレームのサポート	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	2018 年 10 月 11 日
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。	2018 年 2 月 6 日
Direct Connect ゲートウェイ	Direct Connect ゲートウェイを使用して、Direct Connect 接続をリモートリージョンの VPC に接続できます。	2017 年 11 月 1 日
Amazon CloudWatch メトリクス。	Direct Connect 接続の CloudWatch メトリクスを表示できます。	2017 年 6 月 29 日

Link Aggregation Group (LAG	Link Aggregation Group (LAG) を作成して、複数の Direct Connect 接続を集約することができます。	2017 年 2 月 13 日
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。	2016 年 12 月 1 日
タグ付けのサポート	Direct Connect リソースにタグ付けできるようになりました。	2016 年 11 月 4 日
セルフサービス LOA-CFA	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 年 6 月 22 日
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 年 6 月 3 日
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 年 5 月 19 日

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 年 4 月 27 日
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 年 12 月 9 日
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 年 27 月 11 日
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 年 4 月 14 日
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 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 年 11 月 10 日

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 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 年 10 月 23 日
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 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 年 7 月 14 日
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Direct Connect	2014 年 4 月 4 日
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。	2013 年 12 月 19 日2013 年 12 月 5 日
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 年 10 月 22 日
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 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 年 6 月 24 日

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 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 年 5 月 8 日
での IAM の使用のサポートDirect Connect	AWS Identity and Access Management で 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。	2012 年 12 月 21 日
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 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 年 12 月 14 日
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	『Direct Connect 入門ガイド』を『Direct Connect ユーザーガイド』で置き換えました。新しい 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 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 年 8 月 13 日

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 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 年 1 月 10 日
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 年 9 月 8 日
パブリックリリース	Direct Connect の最初のリリースです	2011 年 8 月 3 日