ユーザーガイド

AWS Direct Connect

AWS Direct Connect: ユーザーガイド

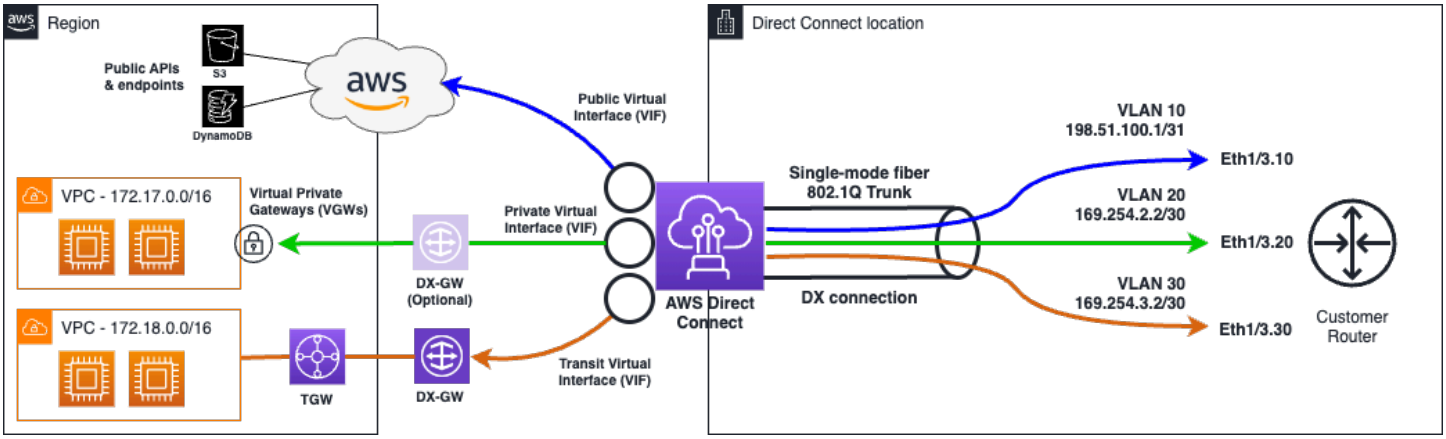
Table of Contents

とは AWS Direct Connect

AWS Direct Connect は、標準イーサネット光ファイバケーブルを介して内部ネットワークを AWS Direct Connect ロケーションにリンクします。ケーブルの一方の端はルーターに接続され、もう一方の端は AWS Direct Connect ルーターに接続されています。この接続を使用すると、パブリック AWS サービス (Amazon S3 など) または Amazon VPC への仮想インターフェイスを直接作成し、ネットワークパス内のインターネットサービスプロバイダーをバイパスできます。 AWS Direct Connect ロケーションは、関連付けられているリージョン AWS の へのアクセスを提供します。パブリックリージョンで 1 つの接続を使用するか AWS GovCloud (US) 、他のすべてのパブリックリージョンでパブリック AWS サービスにアクセスできます。

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



内容

AWS 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

AWS Direct Connect ロケーションに接続を作成して、オンプレミスから AWS リージョンへのネットワーク接続を確立します。詳細については、「AWS Direct Connect 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 サービスへのアクセスを有効にする仮想インターフェイスを作成します。パブリックな仮想インターフェイスでは、Amazon S3 などのパブリックなサービスへのアクセスが可能です。プライベート仮想インターフェイスは、VPC へのアクセスを有効にします。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、「AWS Direct Connect 仮想インターフェイスとホスト仮想インターフェイス」および「仮想インターフェイスの前提条件」を参照してください。

ネットワークの要件

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

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

さらに、お客様のネットワークは以下の条件を満たしている必要があります。

- ネットワークでは、1 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。

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

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

AWS Direct Connect は 1522 バイトまたは 9023 バイトのイーサーネットフレームサイズ (14 バイトイーサーネットヘッダー + 4 バイト VLAN タグ + IP データグラム用バイト + 4 バイト FCS) をリンクレイヤーでサポートします。使用するプライベート仮想インターフェイスの MTU を設定できます。詳細については、「プライベート仮想インターフェイスまたはトランジット仮想インターフェイスの 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) の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、 AWS パブリック IP アドレスを使用してすべてのパブリックサービスにアクセス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では、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) にまたがる複数の Amazon VPC Transit Gateway を接続します。

> **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転送出力料金は、データ転送を担当する AWS アカウントに割り当てられます。マルチアカウントの AWS Direct Connect ゲートウェイを使用する際に追加料金はかかりません。

パブリックアドレス可能な AWS リソース (Amazon S3 バケット、Classic EC2 インスタンス、インターネットゲートウェイを通過する EC2 トラフィックなど) の場合、アウトバウンドトラフィッ

クが同じ AWS 支払者アカウントが所有するパブリックプレフィックスを宛先とし、 AWS Direct Connect パブリック仮想インターフェイス AWS を介して にアクティブにアドバタイズされている場合、データ転送出力 (DTO) 使用量は AWS Direct Connect データ転送レートでリソース所有者に対して計測されます。

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

リモート AWS Direct Connect リージョンへのアクセス

AWS Direct Connect パブリックリージョンまたは の ロケーション AWS GovCloud (US) は、他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。さらに、パブリックリージョンまたは AWS Direct Connect の接続 AWS GovCloud (US) は、他のパブリックリージョン (中国 (北京および寧夏) を除く) のアカウントの VPC にアクセスするように設定できます。したがって、単一の AWS Direct Connect 接続を使用して、マルチリージョンサービスを構築できます。すべてのネットワークトラフィックは、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かかわらず、 AWS グローバルネットワークバックボーンに残ります。

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

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

リモートリージョンでのパブリックサービスへのアクセス

リモートリージョンのパブリックリソースにアクセスするには、パブリック仮想インターフェイスをセットアップし、ボーダーゲートウェイプロトコル (BGP) のセッションを設定する必要があります。詳細については、「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、そのインターフェイスへの BGP セッションを確立すると、ルーターは他のパブリック 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 AWS、のAWS 「IP アドレスの範囲」を参照してくださいAmazon Web Services 全般のリファレンス。

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。これを使用して、プライベート仮想インターフェイス経由で AWS Direct Connect 、異なるリージョンにあるアカウントの VPCs またはトランジットゲートウェイに接続できます。詳細については、「AWS Direct Connect ゲートウェイ」を参照してください。

または、 AWS Direct Connect 接続用のパブリック仮想インターフェイスを作成し、リモートリージョンの 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 リソースを既存のオンサイトサービスと統合する場合に役立ちます。

- Amazon Virtual Private Cloud の接続オプション

AWS Direct Connect ルーティングポリシーと BGP コミュニティ

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

パブリック仮想インターフェイスのルーティングポリシー

AWS 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、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して、BGP 経由でアドバタイズする必要があります。

次のインバウンドルーティングポリシーが適用されます。

- パブリックプレフィックスを所有しており、それが適切な地域のインターネットレジストリに登録されている必要があります。
- トラフィックは Amazon パブリックプレフィックス宛である必要があります。接続間の推移的ルーティングはサポートされていません。

- AWS Direct Connect はインバウンドパケットフィルタリングを実行して、トラフィックのソースがアドバタイズされたプレフィックスから発信されたことを確認します。

次のアウトバウンドルーティングポリシーが適用されます。

- AS_PATH と最長プレフィックス一致は、ルーティングパスを決定するために使用されます。AWS では、同じプレフィックス AWS Direct Connect 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ている場合、 を使用してより具体的なルートをアドバタイズすることをお勧めします。
- AWS Direct Connect は、利用可能な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をアドバタイズし、CloudFront や Route 53 など、利用可能な他の AWS 非リージョンのプレゼンスポイント (PoP) からのオンネットプレフィックスを含めます。

  > **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 にリスト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 商用リージョンの AWS IP アドレス範囲 JSON ファイル ip-ranges.json にリストされているプレフィックスは、 AWS 商用リージョン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。

- AWS Direct Connect は、最小パス長が 3 のプレフィックスをアドバタイズします。
- AWS Direct Connect は、よく知られている NO_EXPORT BGP コミュニティで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、どちらも同じ BGP 属性と最長のプレフィックス長を持つ場合、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 AWS 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ロード共有を調整できます。
- によってアドバタイズされるプレフィックスは、接続のネットワーク境界を超えてアドバタイズ AWS Direct Connect 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。
- AWS Direct Connect は、Amazon ネットワーク内でお客様がアドバタイズしたプレフィックスを保持します。パブリック VIF から学習したカスタマープレフィクスを、次のいずれかに再アドバタイズすることはありません。

  - その他の AWS Direct Connect 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 を使用できます。ただし、重要な考慮事項があります。
  - パブリック ASNs: ASN を所有し、それを発表する権限を持っている必要があります。 AWS は ASN の所有権を検証します。
  - プライベート ASNs: プライベート ASNs (64512-65534、4200000000-4294967294) を使用できます。ただし、 AWS Direct Connect は、プレフィックスを他の AWS 顧客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 の先頭 :
    - パブリック ASN では、先頭の は期待どおりに動作し、先頭の ASN は他のネットワークに表示されます。
    - プライベート ASN では、 がプライベート ASN AWS を 7224 に置き換えると、追加したすべてのプレフィックスが削除されます。つまり、パブリック仮想インターフェイスでプライベート ASN AWS を使用する場合、ASN の先頭付加は 以外の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 AWS を介して と BGP ピアリングセッションを確立する場合は、自律システム番号 (ASN) に 7224 を使用して、 AWS 側で BGP セッションを確立します。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 とは異なる必要があります。

パブリック仮想インターフェイス BGP コミュニティ

AWS Direct Connect は、スコープ BGP コミュニティタグをサポートして、パブリック仮想インターフェイスでのトラフィックの範囲 (リージョンまたはグローバル) とルート設定の制御を支援します。 は、パブリック VIF から受信したすべてのルートを、NO_EXPORT BGP コミュニティタグでタグ付けされているかのように AWS 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— 大陸 AWS リージョン のすべての :
  - 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 AWS Direct Connectによって予約されています。

アウトバウンドルーティングポリシーの場合、 はアドバタイズされたルートに次の BGP コミュニティ AWS Direct Connect を適用します。

- 7224:8100— プレゼンス AWS Direct Connect ポイントが関連付けられているのと同じ AWS リージョンから発信されるルート。
- 7224:8200— プレゼンス AWS Direct Connect ポイントが関連付けられているのと同じ大陸を起点とするルート。
- タグなし-他の大陸を起点とするルート。

> **Note**
>
> すべての AWS パブリックプレフィックスを受信するには、フィルターは適用されません。

AWS 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。

AWS Direct Connect は、アドバタイズされた Amazon ルートで BGP コミュニティタグも提供します。 AWS 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ーを作成できます。

パブリック仮想インターフェイスの場合、顧客に AWS Direct Connect アドバタイズするすべてのルートには NO_EXPORT コミュニティタグが付けられます。

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

AWS Direct Connect を使用してプライベート AWS リソースにアクセスする場合は、BGP 経由でアドバタイズする IPv4 または IPv6 プレフィックスを指定する必要があります。これらのプレフィックスは、パブリック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、プレフィックスの最長長を最初に評価します。目的のルーティングパスがアクティブ/パッシブ接続用である場合、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 AWS 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 ローカル設定コミュニティ値 AWS リージョン を使用して同じ が関連付けられているAWS Direct Connect ロケーションを優先するようにリージョンごとに設定されます。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。
- プレフィックスの長さ、ローカル設定、AS_PATH が同じ場合、Multi-Exit Discriminator (MED) を使用してルーティングパスを決定できます。評価の優先度が低いため、MED 値を使用することはお勧め AWS しません。
- AWS プレフィックスの AS_PATH 長と BGP 属性が同じである場合、 は複数のトランジット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 ASNs 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

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を介してトラフィックをオンプレミスロケーションに AWS リージョン ルーティングする場合、Direct Connect ロケーション AWS リージョン の関連付けは、デフォルトで関連付けられているのと同じ で ECMP. AWS リージョン prefer Direct Connect ロケーションを使用する機能に影響 AWS リージョン 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、同じコロケーション施設か異なるコロケーション施設かにかかわらず AWS リージョン、同じ関連付けられた場所からの 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、同じリージョン外の場所からの 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、オンプレミスの場所 AWS リージョン から への ECMP には影響しません。

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。同じリージョンまたは異なる AWS リージョンにホームを置く複数の AWS 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、同じコミュニティタグを適用します。たとえば、接続のプレフィックスに `7224:7200` (中程度の設定) 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 AWS Direct Connect 接続 (アクティブ/パッシブ) でフェイルオーバーをサポートするには、プライマリまたはアクティブな仮想インターフェイスのプレフィックスに、優先設定が高いコミュニティタグを適用し、バックアップまたはパッシブな仮想インターフェイスのプレフィックスに低い優先設定を適用します。例えば、プライマリまたはアクティブな仮想インターフェイスの BGP コミュニティタグを `7224:7300` (高優先設定) に設定し、パッシブ仮想インターフェイスの BGP コミュニティタグを `7224:7100` (低優先設定) に設定します。

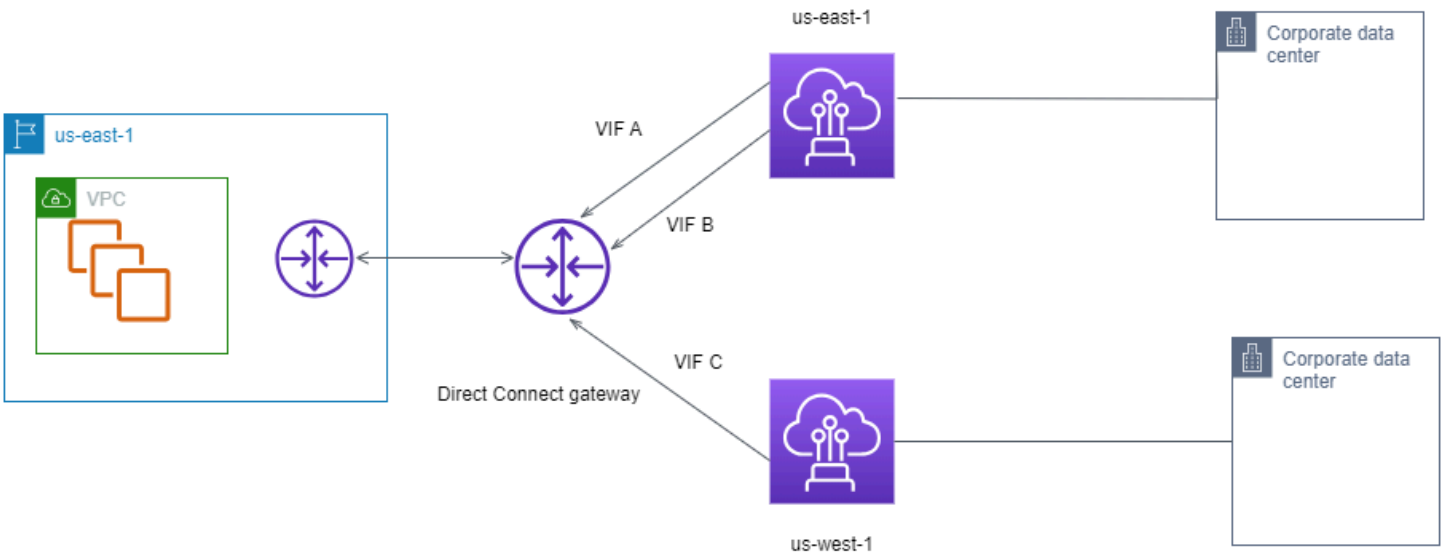
ローカル設定 BGP コミュニティタグは AS_PATH 属性の前に評価され、最も低い設定から最も高い設定の順に評価されます (最も高い設定が優先されます)。

AWS 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

AWS Direct Connect 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検討してください。別のリージョンに冗長な AWS Direct Connect 場所がある AWS Direct Connect 場所 1 VIFs (us-east-1) から Direct Connect ゲートウェイに 2 つのプライベート VIF (VIF A と VIF B) があります。 AWS Direct Connect ロケーション (us-west-1) から Direct Connect ゲートウェイまで 1 つのプライベート VIF (VIF C) があります。VIF A より前に VIF B 経由でトラフィックを AWS ルーティングするには、VIF B の AS_PATH 属性を VIF A AS_PATH 属性よりも短く設定します。

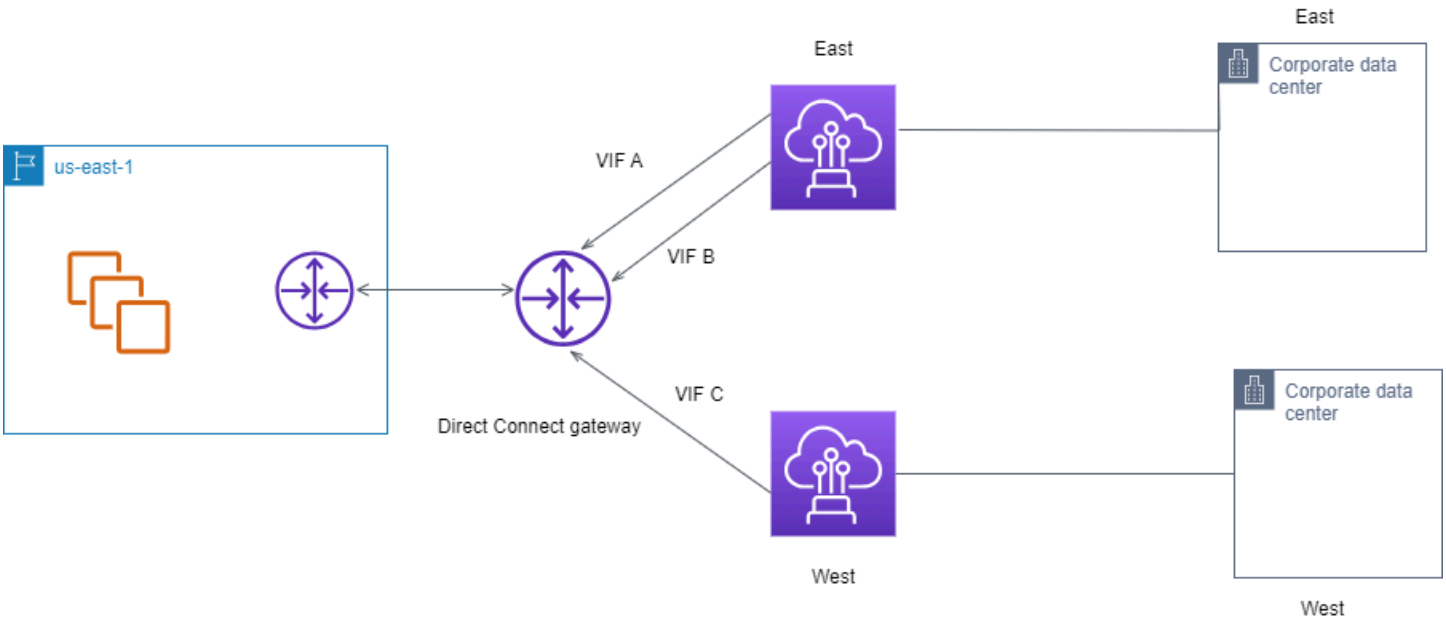
VIF の設定は次のとおりです。

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



VIF C の CIDR 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


East
East
Corporate data center
us-east-1
VIF A
VIF B
VIF C
Direct Connect gateway
Corporate data center
West
West

AWS Direct Connect レジリエンシーツールキット

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

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

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

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

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

ベストプラクティスは、 AWS Direct Connect Resiliency Toolkit の接続ウィザードを使用して、SLA 目標を達成するために専用接続を注文することです。

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

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

前提条件

AWS Direct Connect は、シングルモードファイバーで次のポート速度をサポートします。1 ギガビットイーサネット用の 1000BASE-LX (1310 nm) トランシーバー、10 ギガビットイーサネット用の 10GBASE-LR (1310 nm) トランシーバー、100 ギガビットイーサネット用の 100GBASE-LR4、または 400 Gbps イーサネット用の 400GBASE-LR4。

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

モデル	帯域幅	方法
専用接続	1 Gbps、10 Gbps、100 Gbps、400 Gbps	AWS Direct Connect パートナーまたはネットワークプロ

モデル	帯域幅	方法
		バイダーと協力して、データセンター、オフィス、またはコロケーション環境から AWS Direct Connect ロケーションにルーターを接続します。専用接続に接続するには、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。 AWS 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 Gbps、5 Gbps、10 Gbps、25 Gbps	AWS Direct Connect パートナープログラムのパートナーと協力して、データセンター、オフィス、またはコロケーション環境から AWS Direct Connect ロケーションにルーターを接続します。 一部のパートナーのみがより大きな容量の接続を提供しています。

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

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

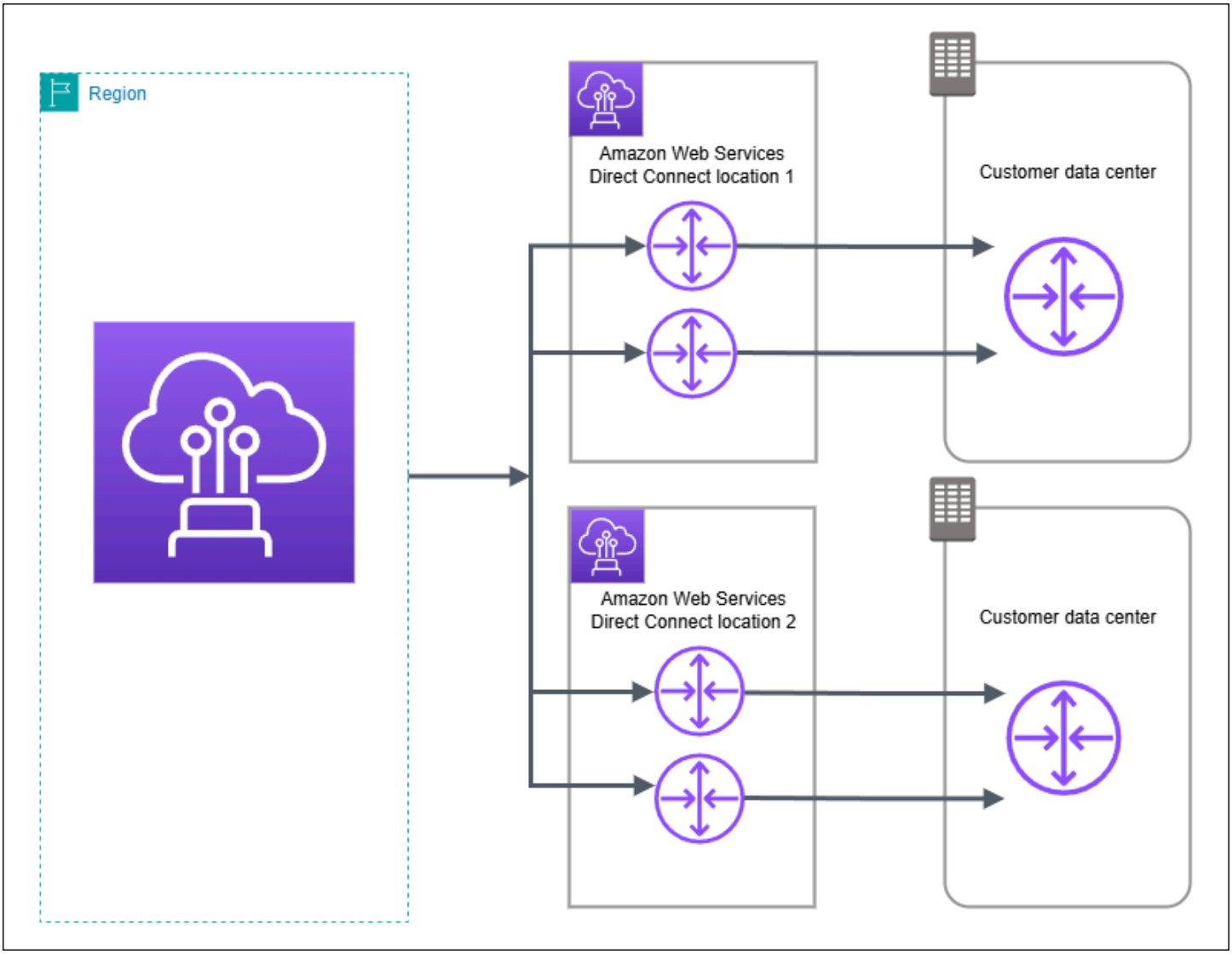
設定を開始する前に、次の情報が揃っていることを確認してください。

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

  速度は、1 つの接続分のみ必要です。

最大回復性

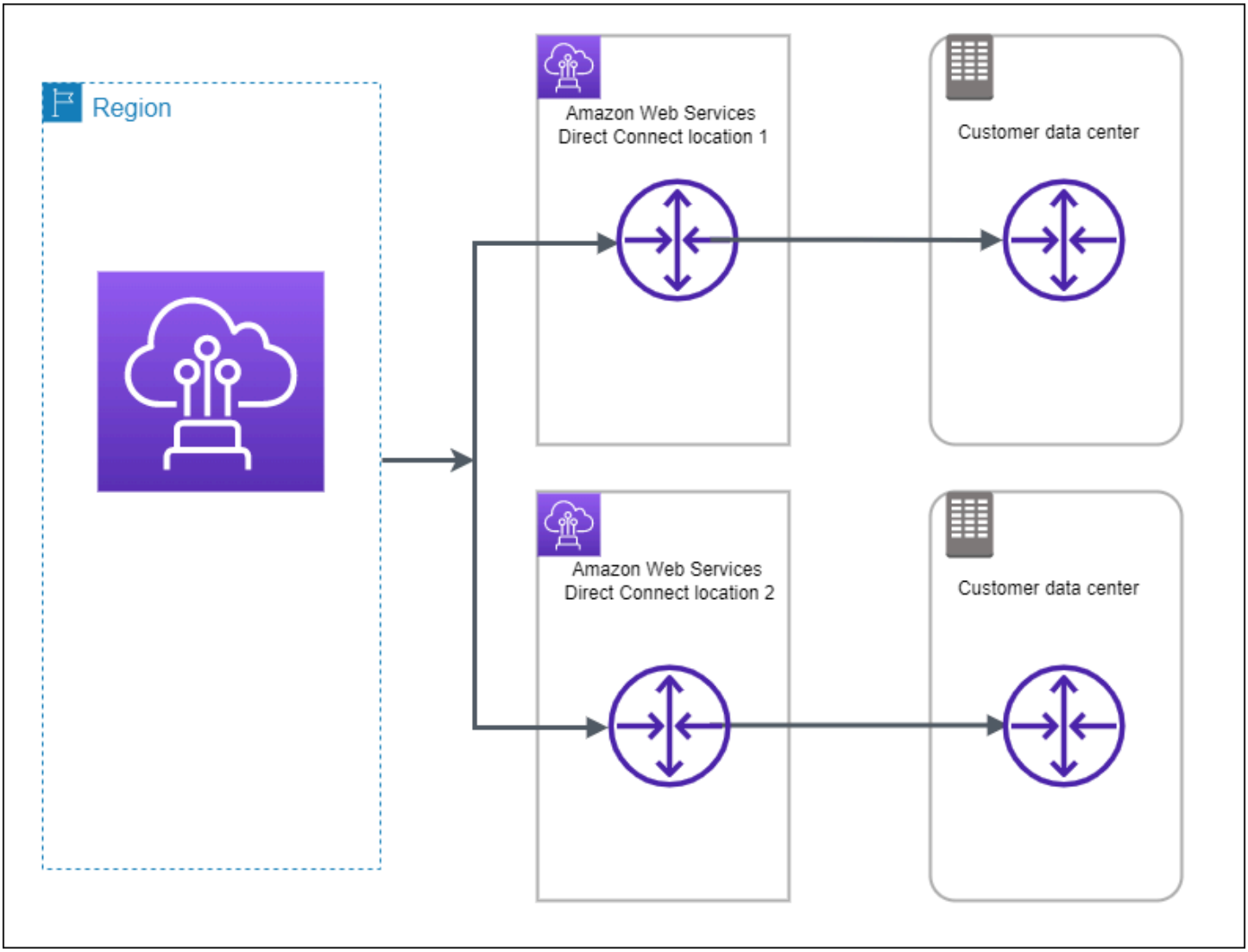
クリティカルなワークロードに対し、複数の場所にある別々のデバイスを終端とする別々の接続を使用することで最大限の回復性を実現できます (以下の図を参照)。このモデルは、デバイス、接続、ロケーション全体の障害に対する回復性を提供します。次の図は、各カスタマーデータセンターから同じ AWS Direct Connect 場所への両方の接続を示しています。必要に応じてお客様は、自身のデータセンターから異なるロケーションに向かう、別個の接続を持つこともできます。



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

高い回復性

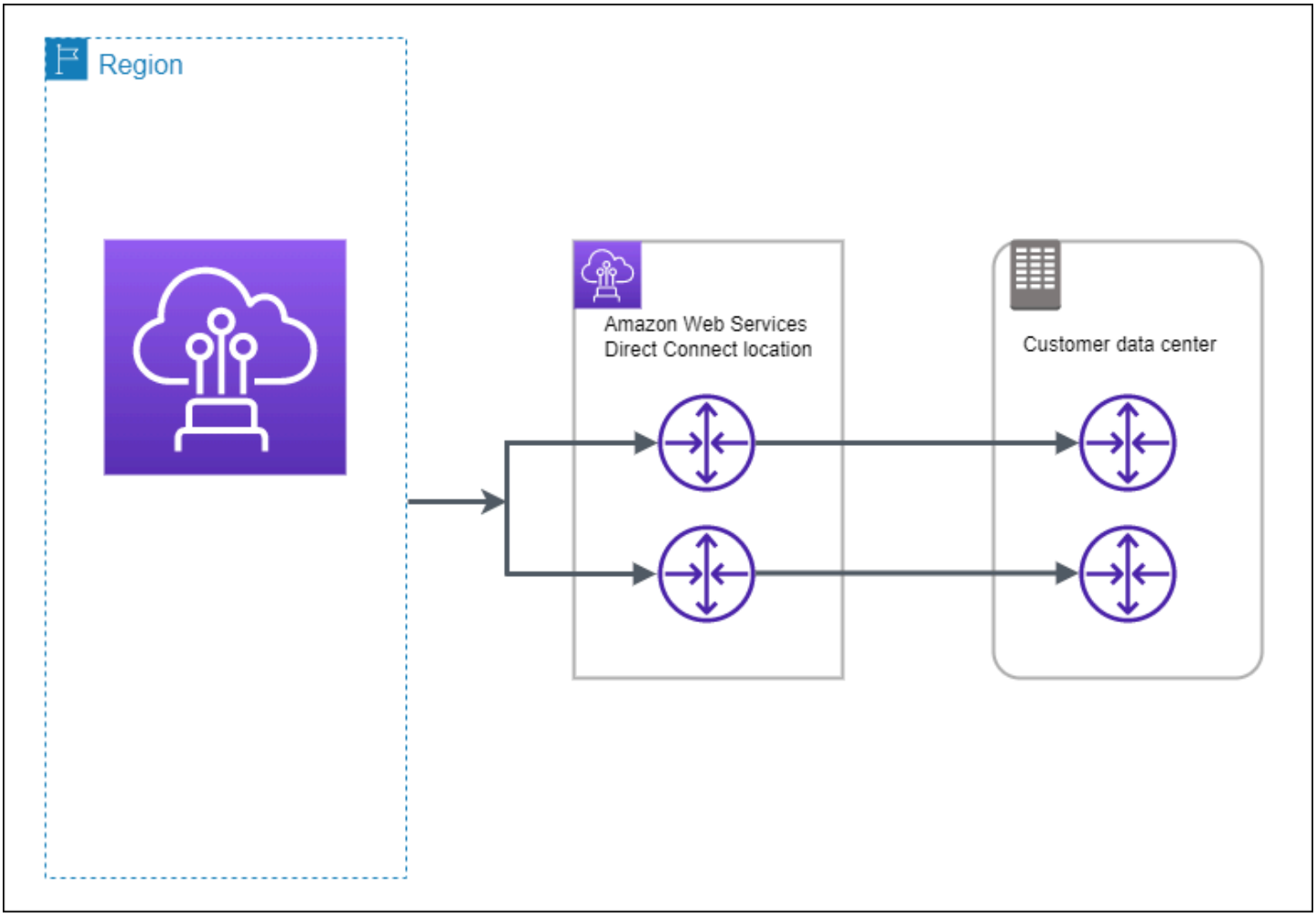
クリティカルなワークロードに対し、複数の場所につながる 2 つの単一接続を使用することで、高い回復性を実現できます (以下の図を参照)。このモデルは、ファイバーの切断やデバイスの障害に起因する接続障害に対し、回復性を提供します。また、ロケーション全体の障害を防ぐのに役立ちます。



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、「」を参照してください高い回復性を設定する。

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 を使用して最大耐障害性モデルを設定する手順については、「」を参照してください開発とテスト環境の回復性を設定する。

クラシック

既存の接続がある場合は、[Classic] を選択します。

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

前提条件

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

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

AWS Direct Connect Resiliency Toolkit を使用して Classic 接続を設定する手順については、「」を参照してくださいClassic 接続を設定する。

AWS Direct Connect FailoverTest

AWS Direct Connect Resiliency Toolkit を使用して、トラフィックルートと、それらのルートが障害耐性要件を満たしていることを確認します。

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、 AWS Direct Connect 「」を参照してくださいDirect Connect フェイルオーバーテスト。

AWS Direct Connect Resiliency Toolkit を使用して、耐障害性を最大化 AWS Direct Connect するように を設定します。

この例では、 AWS Direct Connect Resiliency Toolkit を使用して最大耐障害性モデルを設定します。

タスク

ステップ 1: にサインアップする AWS

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

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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

   サインアップ手順の一環として、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。

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

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [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

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

を保護する AWS アカウントのルートユーザー

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

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

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

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

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

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

管理アクセス権を持つユーザーとしてサインインする

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

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

追加のユーザーにアクセス権を割り当てる

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

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

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

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

ステップ 2: 回復性モデルを設定する

最大回復性モデルを設定するには

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

   a. [帯域幅] で、専用接続の帯域幅を選択します。

      この帯域幅は、作成されたすべての接続に適用されます。

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

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

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

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

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

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

h. (オプション) タグを追加または削除します。

[タグの追加] [タグの追加] を選択して、以下を実行します。

- [キー] にはキー名を入力します。
- [値] にキー値を入力します。

[タグの削除] タグの横にある [タグの削除] を選択します。

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

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

がリクエストを確認し、接続用のポートをプロビジョニング AWS するまでに最大 72 営業時間かかる場合があります。この時間中、ユースケースまたは指定された場所に関する詳細情報のリクエストを含む E メールが送信される場合があります。E メールは、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、パブリック仮想インターフェイスを作成して、VPC にないパブリック AWS サービスに接続することもできます。VPC へのプライベート仮想インターフェイスを作成するときは、接続する VPC ごとにプライベート仮想インターフェイスが必要です。たとえば、3 つの VPC に接続するには 3 つのプライベート仮想インターフェイスが必要です。

作業を開始する前に、次の情報が揃っていることを確認してください。

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

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

リソース	必要な情報

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

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

リソース	必要な情報

(パブリック仮想インターフェイスのみ) アドバタイズするプレフィックス	BGP 経由でアドバタイズするパブリックの IPv4 ルートまたは IPv6 ルート。BGP を使用して少なくとも 1 つ (最大 1,000 個) のプレフィックスをアドバタイズする必要があります。
	• IPv4: IPv4 CIDR は、次のいずれか AWS Direct Connect に該当する場合、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs は異なる AWS リージョンからのものです。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• 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。

(プライベートおよび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	パケットオーバーの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェースの MTU を 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。ジャンボフレームは、 からの伝播されたルートにのみ適用されます AWS Direct Connect。仮想プライベートゲートウェイを指すルートテーブルに静的ルートを追加する場合、静的ルートを介してルーティングされるトラフィックは 1500 MTU を使用して送信されます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでそれを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが対応しているかどうかを確認します。

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

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

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

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

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

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

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

   d. [BGP ASN] に、ゲートウェイのボーダーゲートウェイプロトコル (BGP) 自律システム番号 (ASN) を入力します。

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

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

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

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

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

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

値が入力されない場合は、当社の側で自動的に BGP キーを生成します。

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

d. (オプション) タグを追加または削除します。

[タグの追加] [タグの追加] を選択して、以下を実行します。

- [キー] にはキー名を入力します。
- [値] にキー値を入力します。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

VPC へのプライベート仮想インターフェイスをプロビジョニングするには

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

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

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

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

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

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

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

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

有効な値は 1 ~ 2,147,483,647 です。

6. [追加設定] で、以下を実行します。

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

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

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

> **Important**
>
> AWS Direct Connect 仮想インターフェイスを設定するときは、RFC 1918 を使用して独自の IP アドレスを指定したり、他のアドレス指定スキームを使用したり、point-to-point接続のために RFC 3927 169.25IPv4.0.0/16 IPv4 リンクローカル範囲から割り当てられた AWS 割り当てられた IPv4 /29 CIDR アドレスを選択したりできます。 IPv4 これらのpoint-to-point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 ピア接続にのみ使用する必要があります。VPC トラフィックまたはトンネリングの目的で、 AWS Site-to-Site Private IP VPN や Transit Gateway Connect などでは、point-to-point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または送信先アドレスとして使用 AWS 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、設定が障害耐性要件を満たしていることを確認します。詳細については、「the section called “Direct Connect フェイルオーバーテスト”」を参照してください。

ステップ 5: 仮想インターフェイス接続を検証する

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

AWS クラウドへの仮想インターフェイス接続を確認するには

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

Amazon VPC への仮想インターフェイス接続を検証するには

1. Amazon Linux AMI など Ping に応答する AMI を使用して、仮想プライベートゲートウェイにアタッチされている VPC に EC2 インスタンスを起動します。Amazon EC2 コンソールのインスタンス起動ウィザードを使用すれば、Amazon Linux AMI を [Quick Start (クイックスタート)] タブで使用することができます。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの起動」を参照してください。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、高い耐障害性 AWS Direct Connect を実現するように を設定する

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

ステップ 1: にサインアップする AWS

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

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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

   サインアップ手順の一環として、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。

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

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [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

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

を保護する AWS アカウントのルートユーザー

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

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

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

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

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

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

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

管理アクセス権を持つユーザーとしてサインインする

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

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

追加のユーザーにアクセス権を割り当てる

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

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

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

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

ステップ 2: 回復性モデルを設定する

高回復性モデルを設定するには

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

   a. [帯域幅] で、接続の帯域幅を選択します。

      この帯域幅は、作成されたすべての接続に適用されます。

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

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

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

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

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

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

   h. (オプション) タグを追加または削除します。

      [タグの追加] [タグの追加] を選択して、以下を実行します。

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

      [タグの削除] タグの横にある [タグの削除] を選択します。

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

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

   がリクエストを確認し、接続用のポートをプロビジョニング AWS するまでに最大 72 営業時間かかる場合があります。この時間中、ユースケースまたは指定された場所に関する詳細情報のリクエストを含む E メールが送信される場合があります。E メールは、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、パブリック仮想インターフェイスを作成して、VPC にないパブリック AWS サービスに接続することもできます。VPC へのプライベート仮想インターフェイスを作成するときは、接続する VPC ごとにプライベート仮想インターフェイスが必要です。たとえば、3 つの VPC に接続するには 3 つのプライベート仮想インターフェイスが必要です。

作業を開始する前に、次の情報が揃っていることを確認してください。

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

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

リソース	必要な情報

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

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

リソース	必要な情報

(パブリック仮想インターフェイスのみ) アドバタイズするプレフィックス	BGP 経由でアドバタイズするパブリックの IPv4 ルートまたは IPv6 ルート。BGP を使用して少なくとも 1 つ (最大 1,000 個) のプレフィックスをアドバタイズする必要があります。
	• IPv4: IPv4 CIDR は、次のいずれか AWS Direct Connect に該当する場合、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs は異なる AWS リージョンからのものです。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• 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。

(プライベートおよび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	パケットオーバーの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェースの MTU を 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。ジャンボフレームは、 からの伝播されたルートにのみ適用されます AWS Direct Connect。仮想プライベートゲートウェイを指すルートテーブルに静的ルートを追加する場合、静的ルートを介してルーティングされるトラフィックは 1500 MTU を使用して送信されます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでそれを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが対応しているかどうかを確認します。

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

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

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

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

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

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

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

   d. [BGP ASN] に、ゲートウェイのボーダーゲートウェイプロトコル (BGP) 自律システム番号 (ASN) を入力します。

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

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

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

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

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

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

値が入力されない場合は、当社の側で自動的に BGP キーを生成します。

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

d. (オプション) タグを追加または削除します。

[タグの追加] [タグの追加] を選択して、以下を実行します。

- [キー] にはキー名を入力します。
- [値] にキー値を入力します。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

VPC へのプライベート仮想インターフェイスをプロビジョニングするには

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

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

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

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

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

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

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

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

有効な値は 1 ~ 2,147,483,647 です。

6. [追加設定] で、以下を実行します。

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

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

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

> **Important**
>
> AWS Direct Connect 仮想インターフェイスを設定するときは、RFC 1918 を使用して独自の IP アドレスを指定したり、他のアドレス指定スキームを使用したり、point-to-point接続のために RFC 3927 169.25IPv4.0.0/16 IPv4 リンクローカル範囲から割り当てられた AWS 割り当てられた IPv4 /29 CIDR アドレスを選択したりできます。 IPv4 これらのpoint-to-point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 ピア接続にのみ使用する必要があります。Site AWS Site-to-Site Private 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の目的で、 AWS ではpoint-to-point接続ではなく、送信元アドレスまたは送信先アドレスとして、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、設定が障害耐性要件を満たしていることを確認します。詳細については、「the section called “Direct Connect フェイルオーバーテスト”」を参照してください。

ステップ 5: 仮想インターフェイス接続を検証する

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

AWS クラウドへの仮想インターフェイス接続を確認するには

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

Amazon VPC への仮想インターフェイス接続を検証するには

1. Amazon Linux AMI など Ping に応答する AMI を使用して、仮想プライベートゲートウェイにアタッチされている VPC に EC2 インスタンスを起動します。Amazon EC2 コンソールのインスタンス起動ウィザードを使用すれば、Amazon Linux AMI を [Quick Start (クイックスタート)] タブで使用することができます。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの起動」を参照してください。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、開発とテストの回復性 AWS Direct Connect のために を設定する

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

タスク

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

ステップ 1: にサインアップする AWS

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

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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

   サインアップ手順の一環として、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。

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

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [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

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

を保護する AWS アカウントのルートユーザー

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

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

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

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

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

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

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

管理アクセス権を持つユーザーとしてサインインする

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

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

追加のユーザーにアクセス権を割り当てる

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

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

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

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

ステップ 2: 回復性モデルを設定する

回復性モデルを設定するには

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

   a. [帯域幅] で、接続の帯域幅を選択します。

      この帯域幅は、作成されたすべての接続に適用されます。

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

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

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

   e. (オプション) タグを追加または削除します。

      [タグの追加] [タグの追加] を選択して、以下を実行します。

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

      [タグの削除] タグの横にある [タグの削除] を選択します。

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

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

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

クエストを含む E メールが送信される場合があります。E メールは、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

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

作業を開始する前に、次の情報が揃っていることを確認してください。

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

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

リソース	必要な情報

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

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

リソース	必要な情報

(パブリック仮想インターフェイスのみ) アドバタイズするプレフィックス	BGP 経由でアドバタイズするパブリックの IPv4 ルートまたは IPv6 ルート。BGP を使用して少なくとも 1 つ (最大 1,000 個) のプレフィックスをアドバタイズする必要があります。
	• IPv4: IPv4 CIDR は、次のいずれかに該当する場合 AWS Direct Connect 、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs は異なる AWS リージョンからのものです。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• 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。

(プライベートおよび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	パケットオーバーの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェースの MTU を 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。ジャンボフレームは、伝播されたルートにのみ適用されます AWS Direct Connect。仮想プライベートゲートウェイを指すルートテーブルに静的ルートを追加する場合、静的ルートを介してルーティングされるトラフィックは 1500 MTU を使用して送信されます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでそれを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが対応しているかどうかを確認します。

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

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

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

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

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

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

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

   d. [BGP ASN] に、ゲートウェイのボーダーゲートウェイプロトコル (BGP) 自律システム番号 (ASN) を入力します。

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

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

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

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

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

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

値が入力されない場合は、当社の側で自動的に BGP キーを生成します。

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

d. (オプション) タグを追加または削除します。

[タグの追加] [タグの追加] を選択して、以下を実行します。

- [キー] にはキー名を入力します。
- [値] にキー値を入力します。

[タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

VPC へのプライベート仮想インターフェイスをプロビジョニングするには

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

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

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

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

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

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

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

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

有効な値は 1 ~ 2,147,483,647 です。

6. [追加設定] で、以下を実行します。

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

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

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

> **Important**
>
> AWS Direct Connect 仮想インターフェイスを設定するときは、RFC 1918 を使用して独自の IP アドレスを指定したり、他のアドレス指定スキームを使用したり、point-to-point接続用に RFC 3927 169.25 AWS IPv4.0.0/16 IPv4 リンクローカル範囲から割り当てられた IPv4 /29 CIDR アドレスを選択したりできます。これらのpoint-to-point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 ピア接続にのみ使用する必要があります。Site AWS Site-to-Site Private 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の目的で、 ではpoint-to-point接続ではなく、送信元アドレスまたは送信先アドレスとして、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使用する AWS 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、設定が障害耐性要件を満たしていることを確認します。詳細については、「the section called “Direct Connect フェイルオーバーテスト”」を参照してください。

ステップ 5: 作成した仮想インターフェイスを検証する

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

AWS クラウドへの仮想インターフェイス接続を確認するには

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

Amazon VPC への仮想インターフェイス接続を検証するには

1. Amazon Linux AMI など Ping に応答する AMI を使用して、仮想プライベートゲートウェイにアタッチされている VPC に EC2 インスタンスを起動します。Amazon EC2 コンソールのインスタンス起動ウィザードを使用すれば、Amazon Linux AMI を [Quick Start (クイックスタート)] タブで使用することができます。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの起動」を参照してください。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 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: にサインアップする AWS

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

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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

   サインアップ手順の一環として、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。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルー

トユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [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

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

を保護する AWS アカウントのルートユーザー

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

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

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

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

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

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

管理アクセス権を持つユーザーとしてサインインする

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

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

追加のユーザーにアクセス権を割り当てる

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

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。
2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

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

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

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

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

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

新しい AWS Direct Connect 接続を作成するには

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

   a. [名前] に、接続の名前を入力します。

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

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

   d. [ポートスピード] で接続帯域幅を選択します。

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

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

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

   h. (オプション) タグを追加または削除します。

   [タグの追加] [タグの追加] を選択して、以下を実行します。

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

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

がリクエストを確認し、接続用のポートをプロビジョニング AWS するまでに最大 72 営業時間かかる場合があります。この時間中、ユースケースまたは指定された場所に関する詳細情報のリクエストを含む E メールが送信される場合があります。E メールは、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、「AWS 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を作成する前に、 AWS Direct Connect コンソールでホスト接続を受け入れる必要があります。このステップは、ホスト接続にのみ適用されます。

ホスト型仮想インターフェイスを承諾するには

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

   [Accept (承諾)] を選択します。

(専用接続) ステップ 3: LOA-CFA をダウンロードする

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

LOA-CFA のダウンロード方法

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

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

> **Note**
>
> リンクが有効になっていない場合、LOA-CFA がまだダウンロード可能になっていません。追加情報のリクエストメールを確認します。それでも使用できない場合、または 72 営業時間経過しても E メールが届かない場合は、 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を使用している場合は、AWS Direct Connect ロケーションでクロスコネクトを注文できるように、LOA-CFA を送信します。メンバーまたはプロバイダがクロスコネクトをお客様に代わって注文できない場合は、直接コロケーションプロバイダにお問い合わせください。
   - AWS Direct Connect ロケーションに機器がある場合は、コロケーションプロバイダーに連絡してクロスネットワーク接続をリクエストしてください。お客様はコロケーションプロバイダーの顧客である必要があります。また、 AWS ルーターへの接続を許可する LOA-CFA と、ネットワークに接続するために必要な情報も提示する必要があります。

AWS Direct Connect 複数のサイトとしてリストされているロケーション (Equinix DC1-DC6 や DC10-DC11 など) 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 1 つの AWS Direct Connect 場所として扱われます。高可用性を実現するために、別の AWS Direct Connect ロケーションへの接続を設定します。

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

ステップ 4: 仮想インターフェイスを作成する

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

作業を開始する前に、次の情報が揃っていることを確認してください。

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

リソース	必要な情報

	• IPv4:
	  • (パブリック仮想インターフェイスのみ) お客様が所有している一意のパブリック IPv4 アドレスを指定する必要があります。以下のいずれかを指定できます。
	  • カスタマー所有 IPv4 CIDR
	
	これらは任意のパブリック IPs (顧客所有または 提供 AWS) にすることができますが、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。たとえば、 などの/31範囲を割り当てる場合203.0.113.0/31 、 をピア IP 203.0.113.0 に、 を AWS ピア IP 203.0.113.1 に使用することができます。または、 などの/24範囲を割り当てる場合は、 をピア IP 198.51.100.10 に198.51.100.0/24 、 を AWS ピア IP 198.51.100.20 に使用することができます。
	  • 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が提供する /31 CIDR。AWS Support に連絡して、パブリック IPv4 CIDR をリクエストします (リクエストにはユースケースを提供します)
	
	Note
	AWS提供されたパブリック IPv4 アドレスに対するすべてのリクエストを当社が処理できることを保証することはできません。
	  • (プライベート仮想インターフェイスのみ) Amazon がプライベート IPv4 アドレスを自動的に生成できます。独自の CIDR を指定する場合は、ルーターインターフェイスと AWS Direct Connect インターフェイスにのみプライベート CIDRs 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イスと同様に、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。たとえば、 などの/30範囲を割り当てる場合192.168.0.0/30 、 をピア IP

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

リソース	必要な情報

(パブリック仮想インターフェイスのみ) アドバタイズするプレフィックス	BGP 経由でアドバタイズするパブリックの IPv4 ルートまたは IPv6 ルート。BGP を使用して少なくとも 1 つ (最大 1,000 個) のプレフィックスをアドバタイズする必要があります。
	• IPv4: IPv4 CIDR は、次のいずれかに該当する場合 AWS Direct Connect 、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs は異なる AWS リージョンからのものです。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• 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。

(プライベートおよび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	パケットオーバーの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェースの MTU を 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。ジャンボフレームは、伝播されたルートにのみ適用されます AWS Direct Connect。仮想プライベートゲートウェイを指すルートテーブルに静的ルートを追加する場合、静的ルートを介してルーティングされるトラフィックは 1500 MTU を使用して送信されます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでそれを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが対応しているかどうかを確認します。

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

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

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

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

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

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

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

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

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

      有効な値は 1 ~ 2147483647 です。

6. [追加設定] で、以下を実行します。

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

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

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

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

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

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

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

   d. (オプション) タグを追加または削除します。

      [タグの追加] [タグの追加] を選択して、以下を実行します。

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

      [タグの削除] タグの横にある [タグの削除] を選択します。

7. [仮想インターフェイスの作成] を選択します。

VPC へのプライベート仮想インターフェイスをプロビジョニングするには

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

5. [プライベート仮想インターフェイス設定] で以下を実行します。

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

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

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

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

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

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

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

      有効な値は 1～2,147,483,647 です。

6. [追加設定] で、以下を実行します。

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

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

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

      > **Important**
      >
      > AWS Direct Connect 仮想インターフェイスを設定するときは、RFC 1918 を使用して独自の IP アドレスを指定したり、他のアドレス指定スキームを使用したり、point-to-point接続用に RFC 3927 169.25 AWS IPv4.0.0/16 IPv4 リンクローカル範囲から割り当てられた IPv4 /29 CIDR アドレスを選択したりできます。これらのpoint-to-point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 ピア接続にのみ使用する必要があります。Site AWS Site-to-Site Private 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の目的で、 ではpoint-to-point接続ではなく、送信元アドレスまたは送

信先アドレスとして、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使用する AWS 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

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

ルーター設定をダウンロードするには

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

2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. 接続を選択したら、[View Details (詳細の表示)] を選択します。
4. [ルーター設定をダウンロードする] を選択します。
5. [ルーター設定をダウンロードする] で、次を実行します。

   a. [Vendor] で、ルーターの製造元を選択します。
   b. [Platform] で、ルーターのモデルを選択します。
   c. [Software] で、ルーターのソフトウェアのバージョンを選択します。
6. [ダウンロード] を選択してから、ルーターに対応する適切な設定を使用して AWS Direct Connectに接続できることを確認します。

ルーターの手動設定の詳細については、「」を参照してください ルーター設定ファイルをダウンロードする。

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

ステップ 6: 作成した仮想インターフェイスを検証する

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

AWS クラウドへの仮想インターフェイス接続を確認するには

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

Amazon VPC への仮想 int+erface 接続を確認するには

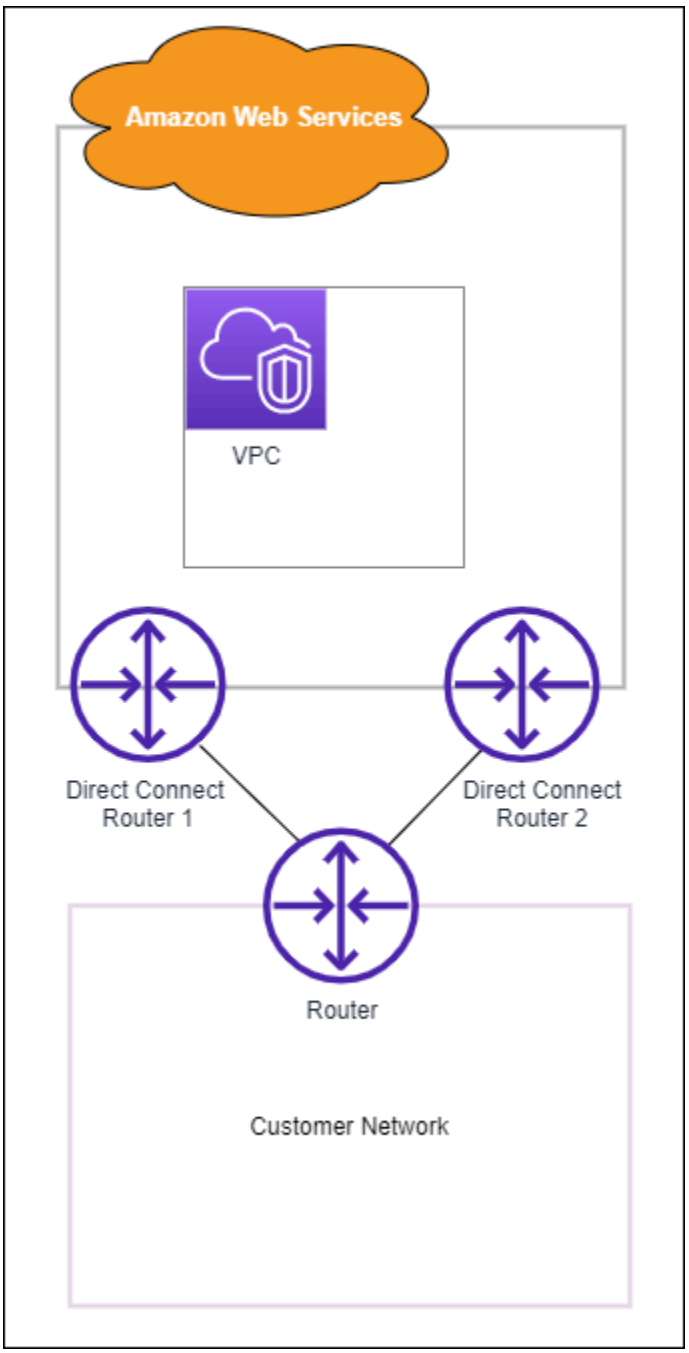
1. Amazon Linux AMI など Ping に応答する AMI を使用して、仮想プライベートゲートウェイにアタッチされている VPC に EC2 インスタンスを起動します。Amazon EC2 コンソールのインスタンス起動ウィザードを使用すれば、Amazon Linux AMI を [Quick Start (クイックスタート)] タ

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



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

- アクティブ/アクティブ (BGP マルチパス)。これは、両方の接続がアクティブであるデフォルト設定です。 は、同じ場所内の複数の仮想インターフェイスへのマルチパス AWS Direct Connect をサポートし、トラフィックはフローに基づいてインターフェイス間でロード共有されます。一方の接続が使用できなくなった場合、すべてのトラフィックが他方の接続のネットワーク経由でルーティングされます。

- アクティブ/パッシブ (フェイルオーバー)。一方の接続がトラフィックを処理し、他方はスタンバイ状態となります。アクティブな接続が使用できなくなった場合、すべてのトラフィックがパッシブ接続を介してルーティングされます。AS パスに、パッシブリンクとなるいずれかのリンクのルートを付加する必要があります。

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

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

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

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

障害耐性の詳細については、 AWS Direct Connect AWS Direct Connect 「障害耐性に関する推奨事項」を参照してください。

AWS Direct Connect フェイルオーバーテスト

AWS Direct Connect Resiliency Toolkit の耐障害性モデルは、複数の場所に適切な数の仮想インターフェイス接続があるように設計されています。ウィザードを完了したら、 AWS Direct Connect Resiliency Toolkit フェイルオーバーテストを使用して BGP ピアリングセッションを停止し、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、回復性要件を満たしていることを確認します。

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 ピアリングセッション、およびテストの実行時間を選択します。 AWS は、選択した仮想インターフェイス BGP ピアリングセッションをダウン状態にします。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。テストが完了すると、またはテストを手動で停止すると、 は BGP セッション

を AWS 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。アカウント所有者は、テストが仮想インターフェイスで実行された AWS CloudTrail ことを示す 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の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を停止する

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、 AWS Direct Connect コンソールまたは を使用して開始できます AWS CLI。

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

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

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

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

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

      最大値は 4,320 分 (72 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。

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 AWS CLI

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する

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

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

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

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

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 AWS CLI

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、 AWS Direct Connect コンソールまたは を使用して停止できます AWS CLI。

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

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

4. [Confirm (確認)] を選択します。

AWS は BGP ピアリング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。

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 AWS CLI

StopBgpFailoverTest を使用します。

AWS Direct Connect メンテナンス

AWS Direct Connect は、サービスのセキュリティ、可用性、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で定期的なメンテナンスが必要です。Direct Connect のメンテナンスは、計画型と緊急型の 2 つのタイプに分かれています。

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。「」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の準備、メンテナンスイベント中の中断を避けるために 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または 1 つの接続がある場合、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た E メールアドレスに、計画された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 E メール通知を送信します。Direct Connect のいずれかの配信パートナーと 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 E メール通知がユーザーとパートナーアカウントの両方に送信されます。追加の E 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して、通知を受信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 の計画されたメンテナンス
- Direct Connect 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 の計画されたメンテナンス

計画された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、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のネットワークアップグレードが含まれます。

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、デバイスエンドポイントが存在する Direct Connect の場所で、トラフィックが少ない時間帯の 4 時間の間に発生します。通常、

メンテナンスアクティビティは 4 時間の時間枠が終了する前に完了し、作業が完了すると通知を受け取ります。まれに、予期しない状況でメンテナンス期間を延長する必要がある場合は、修正された完了見積もりを記載した通知を別途送信します。

次のスケジュールを使用して、最初の通知とリマインダー通知がリソースを所有する AWS アカウントに送信されます。

- 計画されたメンテナンスイベントの 14 暦日前
- 計画されたメンテナンスイベントの 7 暦日前、および
- 計画された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、

- と統合することで、モニタリングまたはチケット発行システムで通知を受信します AWS Health。統合するには AWS Health、「 AWS Health ユーザーガイド」の「Amazon EventBridge AWS Health を使用した でのイベントのモニタリング」を参照してください。
- で計画されたメンテナンススケジュールを表示しますAWS Health Dashboard。

まれに、計画されたメンテナンスイベントをスケジュールどおりに実行することはできません。これが発生した場合は、キャンセル通知を送信し、今後は上記と同じプロセスに従ってイベントを再スケジュールします。

Direct Connect 緊急メンテナンス

緊急メンテナンスイベントは、サービスが差し迫ったイベントに影響を与えないようにしたり、すで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、重要な基準で開始されます。このような場合、影響を受けるエンドポイントを正常な状態に復元するには、すぐにアクションを実行する必要があります。

可能な限り事前に通知するよう努めていますが、状況によってはメンテナンスをすぐに開始する必要がある場合があります。緊急メンテナンスがスケジュールまたは進行中、および完了すると、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 ロケーションの 2 時間の間に発生します。メンテナンスアクティビティは通常、このウィンドウ内に完了します。ハードウェア交換など、予期しない状況でメンテナンス期間を延長する必要がある場合は、修正された完了見積もりを記載した別の通知を送信します。

サードパーティーのメンテナンス

AWS 開始されたメンテナンスイベントに加えて、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 配信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 配信パートナーは からメンテナンスイベント通知を受け取り AWS 、重複を避けるために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可視化できないため、スケジューリングプロセス、通知方法、ベストプラクティスについて確認する必要があります。

メンテナンスイベントの準備

メンテナンスイベント中に本稼働ワークロードが引き続き機能するように、Direct Connect では AWS Direct Connect Resiliency Toolkit を使用してネットワーク接続を最大耐障害性に設定することをお勧めします。最大耐障害性モデルの例については、「」を参照してください最大回復性。

最大回復性を使用すると、接続は少なくとも 2 つの Direct Connect ロケーションに分散され、各 Direct Connect ロケーション内の 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るため、単一のエンドポイント障害のリスクが軽減され、メンテナンスイベント中の接続を維持するのに役立ちます。Direct Connect は、冗長接続を同時に停止する計画されたメンテナンスイベントをスケジュールすることはありません。 AWS Direct Connect Resiliency Toolkit を使用して最大回復性を設定する手順については、「」を参照してください最大限の回復性を設定する。

計画的な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トラフィックをドレインし、トラフィックに冗長接続の使用を強制します。これにより、最大の回復性が設定されていない場合、手動による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、メンテナンスウィンドウ中の冗長接続間のトラフィックの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、「」を参照してくださいルーティングポリシーと BGP コミュニティ。

最大限の回復性モデルで Direct Connect 環境を設定すると、メンテナンスイベントやインフラストラクチャの障害発生時にビジネスに影響が及ばないようにできます。適切に実装およびテストされている場合、通常、これらのメンテナンスイベントに対してアクションを実行する必要はありません。

耐障害性の検証

Direct Connect 環境が回復力を持つように設定されている場合は、接続がout-of-serviceになったときに、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中に本番環境のワークロードに影響を与える前に、潜在的な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の信頼性が向上します。Direct Connect フェイルオーバーテストを使用して、冗長接続の耐障害性を検証します。 AWS 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、「」を参照してくださいDirect Connect フェイルオーバーテスト。

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 との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

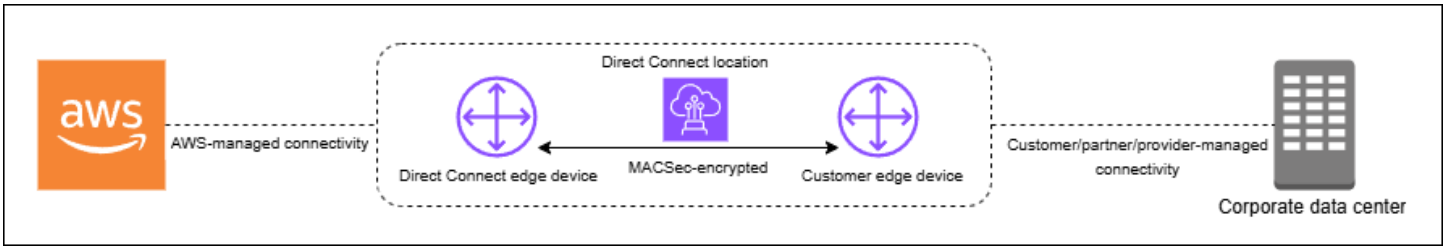
Direct Connect デバイスは複数のお客様間で共有されます。したがって、メンテナンスの再スケジュールやキャンセルに関する特定のリクエストは受け付けません。ある顧客のリクエストを再スケジュールまたはキャンセルすると、そのエンドポイントを使用している他の顧客に悪影響が及ぶ可能性があります。また、可用性やセキュリティの問題がタイムリーに軽減されるリスクもあります。

での MAC セキュリティ AWS Direct Connect

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、2 つの Layer 3 ルーター間で動作し AWS、クロスコネクトを介して Layer 2 point-to-point暗号化を提供します。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 で保護しますが、 は AWS Direct Connect 、ロケーションと AWS リージョン間のネットワークを通過するときに物理レイヤーのすべてのデータを暗号化することで、追加のセキュリティ AWS を提供します。これにより、ネットワークへの初回侵入時 AWS と AWS ネットワーク経由の転送時の両方でトラフィックを保護するレイヤードセキュリティアプローチが作成されます。

次の図では、 AWS Direct Connect クロス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する必要があります。Direct Connect 経由の MACsec は、Direct Connect エッジデバイスと顧客のエッジデバイス間のpoint-to-pointトラフィックに対してレイヤー 2 暗号化を提供します。この暗号化は、クロスコネクトの両端にある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でpoint-to-pointセキュリティを提供するため、複数のシーケンシャルイーサネットやその他のネットワークセグメントにわたってend-to-endの暗号化を提供しません。



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。

- Secure Association Key (SAK) — お客様のオンプレミスルーターと Direct Connect ロケーションの接続ポート間の MACsec 接続を確立するセッションキー。SAK は事前共有されず、暗号化キー生成プロセスを通じて CKN/CAK ペアから自動的に取得されます。この取得は、CKN/CAK ペアを指定してプロビジョニングした後、接続の両端で行われます。SAK は、セキュリティ上の目的および MACsec セッションが確立されるたびに定期的に再生成されます。
- Connectivity Association Key Name (CKN) と Connectivity Association Key (CAK) — このペアの値は、MACsec キーの生成に使用されます。ペア値を生成して AWS Direct Connect 接続に関連付け、 AWS Direct Connect 接続の最後にエッジデバイスにプロビジョニングします。Direct Connect は静的 CAK モードのみをサポートしますが、動的 CAK モードはサポートしません。静的 CAK モードのみがサポートされているため、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、正確に 64 文字を使用する必要があります。Direct Connect は、64 文字の 16 進文字列に対応する専用接続の Advanced Encryption Standard (AES) 256 ビットキーのみをサポートします。
- 暗号化モード — Direct Connect は 2 つの MACsec 暗号化モードをサポートしています。
  - must_encrypt — このモードでは、接続にはすべてのトラフィックに対して 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、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すると、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は暗号化されていないトラフィックを許可する場合があります。

  暗号化モードは接続設定中に設定でき、後で変更できます。デフォルトでは、新しい MACsec 対応接続は「should_encrypt」モードに設定され、初期設定中の潜在的な接続の問題を防ぎます。

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、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の使用を試みます。そのキーがデバイスのキーと一致しない場合、以前の作業キーにフォールバックし、ローテーション中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。

- Secure Association Key (SAK) 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、以下に基づいて自動ローテーションを実行します。

  - 時間間隔
  - 暗号化されたトラフィックの量
  - 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、接続を中断することなく透過的に行われ、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取得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、専用の Direct Connect 接続とリンク集約グループで使用できます。

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**
>
> AWS Direct Connect パートナーが相互接続に実装した場合、ホスト接続は MACsec をサポートします。

MACsec をサポートする接続の注文方法については、AWS Direct Connect を参照してください。

専用接続

以下は、 AWS Direct Connect 専用接続で MACsec に慣れるのに役立ちます。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、必要に応じてレスポンスに MACsec 関連情報が含まれます。

専用接続の MACsec 前提条件

専用接続での MACsec の次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ロ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、キーロ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 を設定する前に、次のタスクを完了する必要があります。

- MACsec キーの 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

以下の要件は、Direct Connect リンク集約グループ (LAGs) の MACsec を理解するのに役立ちます。

- LAGs 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 内のすべての接続は同じ帯域幅で、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

パートナー相互接続

相互接続を所有す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されます。

サービスにリンクされたロール

AWS Direct Connect は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、直接リンクされた一意のタイプの IAM ロールです AWS Direct Connect。サービスにリンクされたロールは によって事前定義 AWS Direct Connect されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、 の設定 AWS Direct Connect が簡単になります。は、サービスにリンクされたロールのアクセス許可 AWS Direct Connect を定義し、特に定義されている場合を除き、 のみがそのロールを引き受け AWS Direct Connect ることができます。定義される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 “サービスにリンクされた役割”」を参照してください。

MACSec の事前共有 CKN/CAK キーに関する考慮事項

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

保存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。

AWS 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。オンプレミスルーターと AWS Direct Connect ロケーションの MACsec シークレットキーが一致している必要があります。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

AWS Direct Connect 専用接続とホスト接続

AWS Direct Connect を使用すると、ネットワークといずれかの AWS Direct Connect ロケーションの間に専用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、 AWS Direct Connect コンソール、 CLI、または API を使用して専用接続をリクエストできます。詳細については、「専用接続」を参照してください。
- ホスト接続: AWS Direct Connect パートナーが顧客に代わってプロビジョニングする物理イーサネット接続。お客様は、この接続をプロビジョニングする AWS Direct Connect パートナープログラムのパートナーに連絡することで、ホスト接続をリクエストします。詳細については、「ホスト接続」を参照してください。

トピック

専用 AWS Direct Connect 接続

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

AWS Direct Connect location

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

Port speed

指定できる値は 1 Gbps、10 Gbps、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 に接続するための認可であり AWS、ネットワークプロバイダーがクロスコネクトを注文するために必要です。 AWS Direct Connect ロケーションに機器がない場合は、そこで自分でクロスコネクトを注文することはできません。

次のオペレーションが専用接続で利用できます。

- 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。

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

MAC セキュリティ (MACsec) を使用する接続を作成する場合は、その作業を開始する前に、接続の前提条件をご確認ください。詳細については、「the section called “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 のデジタル署名とウォーターマーク。PDF ドキュメントは、変更された、また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のを防ぎます。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、「AWS Direct Connect 料金」を参照してください。LOA-CFA を再発行した後に接続が必要なくなった場合は、お客様ご自身で接続を削除する必要があります。詳細については、「AWS 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 AWS 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: AWS Direct Connect 専用接続をリクエストする” の手順をご覧ください。

接続ウィザードの接続を作成するには

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

   - 最大回復性
   - 高い回復性
   - 開発とテスト

   これらの回復性レベルの説明と詳細については、AWS Direct Connect レジリエンシーツールキット 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. Location で適切な AWS Direct Connect 場所を選択し、First location サービスプロバイダーを選択し、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 番目の口ケーションでは、2 番目の口ケーション AWS Direct Connect で適切な を選択し、2 番目の口ケーションサービスプロバイダーを選択し、この 2 番目の口ケーションで接続を提供するサービスプロバイダーを選択します。

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 (AWS Direct Connect API)

AWS Direct Connect Classic 接続を作成する

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

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

- 接続を終了する AWS Direct Connect 場所。

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

新しい AWS Direct Connect 接続を作成するには

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

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

12. [接続の作成] を選択します。

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

LOA-CFA AWS Direct Connect のダウンロード

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

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

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

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

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

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

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

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

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

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 (AWS Direct Connect API)

MACsec シークレットキーと AWS Direct Connect 接続間の関連付けを削除する

コンソール、 AWS Direct Connect コマンドライン、または API を使用して、接続と MACsec キーの関連付けを削除できます。

接続と MACsec キー間の関連付けを解除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2.
3. 左のペインで、[接続] を選択します。
4. 接続を選択したら、[詳細の表示] をクリックします。
5. 解除する MacSec シークレットを選択し、[キーの関連付けを解除する] をクリックします。
6. 確認ダイアログボックスで、disassociate と入力し、[関連付けを解除] をクリックします。

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 (AWS Direct Connect API)

ホスト接続 AWS Direct Connect

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

AWS Direct Connect location

AWS Direct Connect パートナープログラムの AWS Direct Connect パートナーと協力して、AWS Direct Connect ロケーションとデータセンター、オフィス、またはコロケーション環境との間にネットワーク回線を確立します。また、ロケーションと同じ施設内にコロケーションスペー

スを提供するのにも役立ちます。詳細については、「AWS Direct Connect Delivery Partners」(デリバリーパートナー) を参照してください。

> **Note**
>
> AWS Direct Connect コンソールからホスト接続をリクエストすることはできません。ただし、 AWS Direct Connect パートナーはホスト接続を作成して設定できます。接続が設定されたら、 コンソールの [Connections] (接続) ペインに接続が表示されます。
> ホスト接続を使用する前に同意する必要があります。詳細については、「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。特定の要件を満たす AWS Direct Connect パートナーのみが、1 Gbps、2 Gbps、5 Gbps、10 Gbps、または 25 Gbps のホスト接続を作成できることに注意してください。25 Gbps 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 Direct Connect AWS パートナーによってのみ変更できます。 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す。
- AWS はホスト接続でトラフィックポリシーを使用します。つまり、トラフィックレートが設定された最大レートに達すると、余分なトラフィックがドロップされます。これにより、高バーストトラフィックのスループットは、非バーストトラフィックよりも低くなる可能性があります。
- ジャンボフレームは、 AWS Direct Connect ホスト親接続で最初に有効になっている場合にのみ接続で有効にできます。ジャンボフレームがその親接続で有効になっていない場合、どの接続でも有効にすることはできません。

ホスト接続をリクエストして承認すると、次のコンソール操作が可能になります。

- 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。

AWS Direct Connect ホスト接続を受け入れる

ホスト接続の購入に関心がある場合は、 AWS Direct Connect パートナープログラムの AWS Direct Connect パートナーに連絡する必要があります。パートナーがお客様の接続をプロビジョニングします。接続を設定されたら、 AWS Direct Connect コンソールの [Connections] ペインに接続が表示されます。

ホスト接続を使用する前に接続を受け入れる必要があります。ホスト接続を受け入れるには、 AWS 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。

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

コマンドラインまたは API を使用して接続を説明するには

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

AWS 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、この接続のすべてのポート時間料金が停止しますが、クロスコネクトまたはネットワーク回路料金が発生する場合があります (以下を参照) 。 AWS Direct Connectデータ転送料金は仮想インターフェイスに関連付けられます。仮想インターフェイスの削除方法の詳細については、「仮想インターフェイスを削除する」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 はコロケーションプロバイダーに、該当する AWS パッチパネルから光ファイバークロスコネクトケーブルを削除して、Direct Connect ルーターからネットワークデバイスを切断するよう指示します。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。

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

接続を削除する方法

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

AWS Direct Connect 接続を更新する

AWS 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**
>
> MACSec は専用接続でのみ使用が可能です。

有効な値は以下のとおりです。

- `should_encrypt`
- `must_encrypt`

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

接続を更新するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Connections (接続)] を選択します。
3. 接続を選択した後、[編集] をクリックします。
4. 接続を変更するには

   [名前の変更] [名前] に新しい接続名を入力します。

   [タグの追加] [タグの追加] を選択して、以下を実行します。

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

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

コマンドラインまたは API を使用して接続を更新するには

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

AWS Direct Connect 接続の詳細を表示する

AWS Direct Connect コンソール、コマンドライン、または API を使用して、接続の現在のステータスを表示できます。接続 ID (たとえば、dxcon-12nikabc) を表示し、受信またはダウンロードした LOA-CFA の接続 ID との一致を確認することもできます。

接続のモニタリングの詳細については、「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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. 左のペインで、[接続] を選択します。
3. 接続を選択したら、[詳細の表示] をクリックします。

コマンドラインまたは API を使用して接続を記述するには

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

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

Letter of Authorization and Connecting Facility Assignment (LOA-CFA) をダウンロードしたら、クロスネットワーク接続 (別名クロスコネクト) を完了する必要があります。 AWS Direct Connect ロケーションにすでに機器がある場合は、適切なプロバイダーに連絡してクロスコネクトを完了してください。プロバイダごとの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。クロスコネクトが確立されたら、 AWS Direct Connect コンソールを使用して仮想インターフェイスを作成できます。

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

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

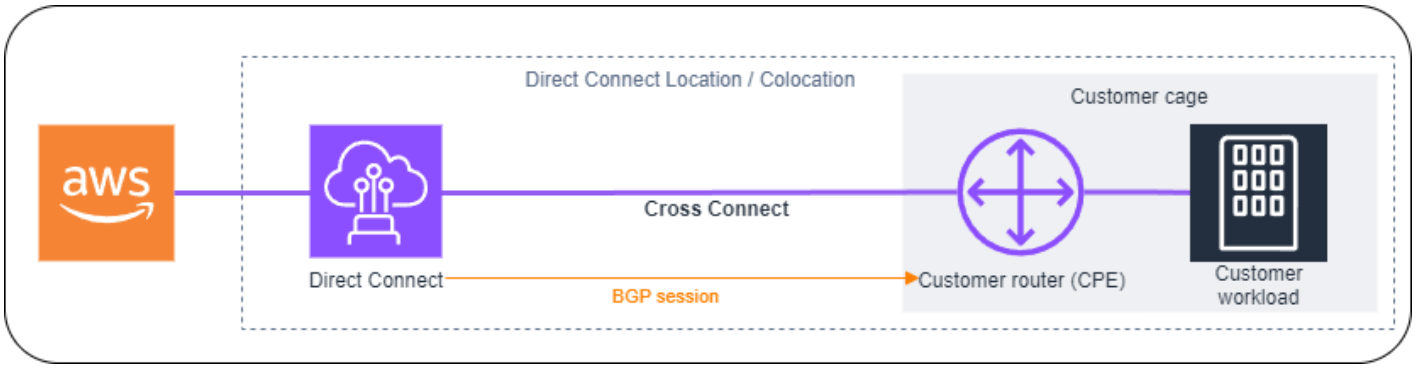
AWS Direct Connect 接続は、他のリージョンのリソースへのアクセスを提供できます。詳細については、「リモート AWS Direct Connect リージョンへのアクセス」を参照してください。

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

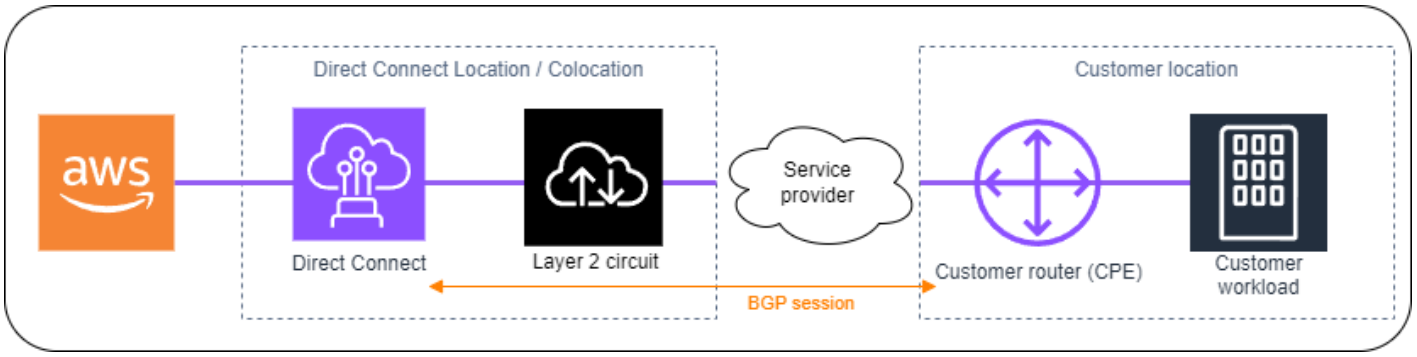
接続オプション

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 Partner Network (APN) のパートナーのいずれかと連携できます。

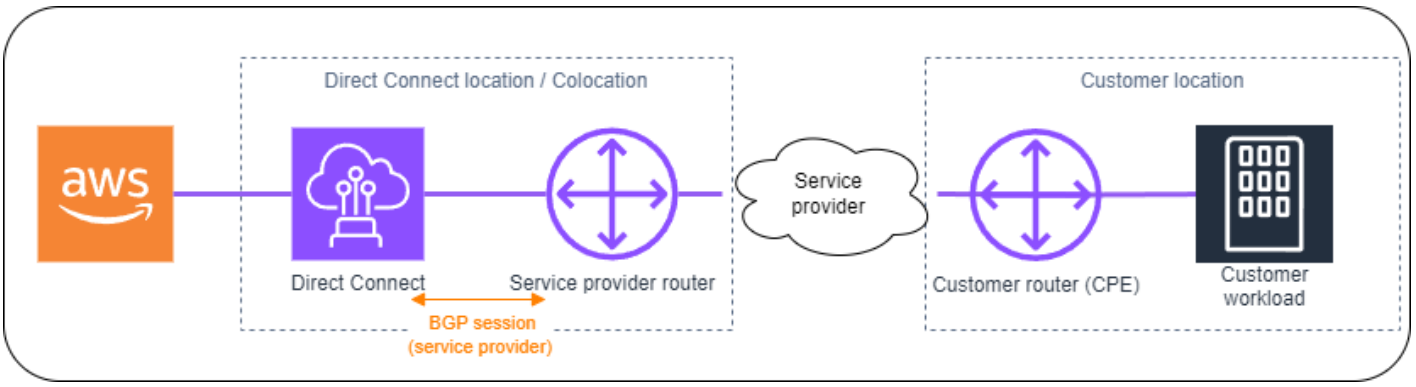
- Direct Connect ロケーションと同じデータセンター/コロケーション施設にリソースがデプロイされている場合、その施設では AWS Direct Connect 機器とリソース間のクロスコネクトの提供が可能です。そのためには、まず LOA-CFA を施設に提供する必要があります。詳細については「Letter of Authorization and Connecting Facility Assignment (LOA-CFA)」を参照してください。この Direct Connect 接続オプションの例を次に示します。



- 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。お客様の場所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の場合、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。Direct Connect パートナーは、ユーザーと別の BGP を確立しました。例えば、これはマルチプロトコルラベル切り替え (") 経由である可能性があります。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	awsdx@dci-indonesia.com から DCI Indonesia にお問い合わせください。
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 までお問い合わせください。
Cologix MTL3、モントリオール	Cologix へのお問い合わせは、sales@cologix.com までご連絡ください。
Cologix VAN2、バンクーバー	Cologix へのお問い合わせは、sales@cologix.com までご連絡ください。
eStruxture、モントリオール	eStruxture へのお問い合わせは、 directconnect@estruxture.com までご連絡ください。

中国 (北京)

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 バーレーン DC53、マナマ	接続を完了するには、現地のネットワークプロバイダーパートナーと連携して接続を確立します。次に、ネットワークプロバイダーから AWS サポートセンター AWS を通じて に認可書 (LOA) を提供します。 はこの場所でクロスコネクト AWS を完了します。
AWS バーレーン DC52、マナマ	接続を完了するには、現地のネットワークプロバイダーパートナーと連携して接続を確立します。次に、ネットワークプロバイダーから AWS サポートセンター AWS を通じて に認可書 (LOA) を提供します。 はこの場所でクロスコネクト AWS を完了します。

中東 (アラブ首長国連邦)

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。

AWS Direct Connect 仮想インターフェイスとホスト仮想インターフェイス

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

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

パブリック仮想インターフェイスプレフィックス広告ルール

VPCsおよびその他の AWS サービスのワークロードのパブリック IP アドレスに到達できるように、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 サービスの API エンドポイント、 で使用されるパブリック IP アドレスAmazon.comです。Amazon 以外のプレフィックスにアクセスできません。で使用されるプレフィックスの現在のリストについてはAWS、「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 を介して通知されるプレフィックスは、 AWS IP アドレス範囲リストにリストされているものと比較して集約または集約解除される場合があります。

- 独自の IP アドレス (BYOIP) AWS を介して に持ち込む IP アドレス範囲は .json ファイルに含まれませんが、パブリック仮想インターフェイスを介してこれらの BYOIP アドレスをアドバタイズ AWS 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 外のネットワークに再アドバタイズしません AWS。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、 のすべてのお客様に表示されます AWS。

> **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 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 ポイントオブプレゼンス (PoPs) 間の接続を可能にします。これにより、トラフィックをリージョン経由でルーティングすることなく、 AWS グローバルネットワークを介してオンプレミスネットワークに接続できます。SiteLink の詳細については、「Introducing AWS Direct Connect SiteLink」を参照してください。

> **Note**
>
> - SiteLink は、 AWS GovCloud (US) および中国リージョンでは使用できません。
> - SiteLink は、オンプレミスルーターが複数の仮想インターフェイス AWS で同じルートをにアドバタイズする場合、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 対応仮想インターフェイスを介した AWS リージョン （ 仮想ゲートウェイまたはトランジットゲートウェイ) からオンプレミスの場所へのトラフィックのトラフィックルーティング動作は、 AWS パスが付加されたデフォルトの Direct Connect 仮想インターフェイス動作とは若干異なります。SiteLink が有効になっている場合、 の仮想インターフェイスは、関連付けられたリージョンに関係なく、Direct Connect の場所からの AS パスの長さが低い BGP パスを AWS リージョン 優先します。例えば、Direct Connect の場所ごとに、関連するリージョンがアドバタイズされます。SiteLink が無効になっている場合、仮想ゲートウェイまたは 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
Connection	仮想インターフェイスを作成する AWS Direct Connect 接続またはリンク集約グループ (LAG)。
仮想インターフェイス名	仮想インターフェイスの名前。
仮想インターフェイス所有者	別のアカウントの仮想インターフェイスを作成する場合は、別の AWS アカウントのアカウント ID が必要です。
(プライベート仮想インターフェイスのみ) 接続	同じ AWS リージョンの VPC に接続するには、VPC の仮想プライベートゲートウェイが必要です。Amazon 側の BGP セッションのための ASN は、仮想プライベートゲートウェイから継承されます。仮想プライベートゲートウェイを作成するときに、独自のプライベート ASN を指定できます。そうでない場合は、Amazon によってデフォルトの ASN が指定されます。詳細については、Amazon VPC ユーザーガイドの Create a Virtual Private Gateway を参照してください。Direct Connect Gateway 経由で VPC に接

リソース	必要な情報
	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。 **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 と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、 AWS Direct Connect 接続を通過するすべてのトラフィックに必要です。 ホスト接続がある場合、 AWS Direct Connect パートナーはこの値を提供します。仮想インターフェイス作成後に値を変更することはできません。

リソース	必要な情報

ピア IP アドレス	仮想インターフェイスは、IPv4 または IPv6 に対して 1 つの BGP ピアリングセッションをサポートできます。または両方に対して 1 つずつ BGP ピアリングセッションをサポートできます (デュアルスタック)。パブリック仮想インターフェイスの作成に Amazon プールからの Elastic IP (EIP) および Bring your own IP アドレス (BYOIP) を使用して作成しないでください。同じ仮想インターフェイスで同じ IP アドレスファミリに対して複数の BGP セッションを作成することはできません。BGP ピアセッションでは、仮想インターフェイスの両端に IP アドレス範囲が割り当てられます。
	
	• IPv4:
	  • (パブリック仮想インターフェイスのみ) お客様が所有している一意のパブリック IPv4 アドレスを指定する必要があります。
	
	  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 IPs は、任意の有効な IP 範囲から取得できます。これには、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経由でアドバタイズされたり、NAT に使用されたりしない限り、顧客所有のパブリック IP アドレスを含めることもできます。
	  • 提供されたパブリック IPv4 アドレスに対する AWS すべてのリクエストを当社が処理できることを保証することはできません。
	
	  値は次のいずれかになります:
	  • カスタマー所有 IPv4 CIDR
	
	  これらは任意のパブリック IPs (顧客所有または 提供 AWS) にすることができますが、ピア IP と AWS ルーターピア IP の両方に

リソース	必要な情報
	同じサブネットマスクを使用する必要があります。たとえば、 などの/31範囲を割り当てる場合203.0.113.0/31 、 をピア IP 203.0.113.0 に、 を AWS ピア IP 203.0.113.1 に使用することができます。または、 などの/24範囲を割り当てる場合は、 をピア IP 198.51.100.10 に198.51.100.0/24 、 を AWS ピア IP 198.51.100.20 に使用することができます。 • 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 指定された /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イスと同様に、ピア IP と AWS ルーターピア IP の両方に同じサブネットマスクを使用する必要があります。たとえば、 などの/30範囲を割り当てる場合192.168.0.0/30 、 をピア IP 192.168.0.1 に、 を AWS ピア IP 192.168.0.2 に使用することができます。 • 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: IPv4 CIDR は、次のいずれか AWS Direct Connect に該当する場合、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs は異なる AWS リージョンからのものです。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• 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
(プライベートおよび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	パケットオーバーの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェイスの MTU を 8500 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。Direct Connect では、最大 8500 MTU のジャンボフレームがサポートされます。Transit Gateway ルートテーブルで設定された静的なルートと伝播されたルートはジャンボフレームをサポートします。これには、VPC の静的なルートテーブルのエントリを持つ EC2 インスタンスから Transit Gateway アタッチメントへのものが含まれます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでそれを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが対応しているかどうかを確認します。

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

- プライベート VIF およびトランジット VIF の場合、アカウントは仮想インターフェイスおよび仮想プライベートゲートウェイ/Direct Connect ゲートウェイの宛先に適用されます。
- パブリック VIF の場合、アカウントは仮想インターフェイスの課金に使用されます。Data Transfer Out (DTO) の使用量は、 AWS Direct Connect データ転送レートでリソース所有者に対して計測されます。

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

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

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

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

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

> **Important**
>
> ジャンボフレームは、 経由の伝播ルート AWS Direct Connect とトランジットゲートウェイ経由の静的ルートにのみ適用されます。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。

AWS 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。

内のアカウント AWS Organizations、または とは異なるアカウントの仮想インターフェイスを作成するには、ホスト AWS Organizations された仮想インターフェイスを作成します。

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

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

ネットワーク接続の最大送信単位 (MTU) とは接続を介して渡すことができる最大許容パケットサイズ (バイト単位) です。プライベート仮想インターフェイスの MTU は、1500 または 9001 (ジャンボフレーム) のいずれかです。トランジット仮想プライベートインターフェイスの MTU では、1500 あるいは 8500 (ジャンボフレーム) のどちらでも使用できます。インターフェイスの作成時あるいは作

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

> **Important**
>
> Transit Gateway を 1 つ以上の Direct Connect ゲートウェイに関連付ける場合、Transit Gateway およびその Direct Connect ゲートウェイで使用される自律システム番号 (ASN) は異なる値である必要があります。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。

AWS 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と、リクエストの確認と承認に最大 72 営業日かかる場合があります。

パブリック仮想インターフェイスをプロビジョニングするには

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

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

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

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

   d. BGP ASN の場合は、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 (ASN) を入力します。

      有効な値は 1 ~ 2147483647 です。

> **Note**
>
> パブリック仮想インターフェイス AWS を介して で BGP ピアリングセッションを確立する場合は、7224 を ASN として使用して、 AWS 側で BGP セッションを確立します。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 (AWS Direct Connect API)

AWS Direct Connect プライベート仮想インターフェイスを作成する

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

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 は 1500 または 9001 (ジャンボフレーム) のいずれかです。トランジット仮想プライベートインターフェイスの MTU では、1500 あるいは 8500 (ジャンボフレーム) のどちらでも使用できます。インターフェイスの作成時あるいは作成後の更新時に、MTU を指定できます。仮想インターフェイスの MTU を8500 (ジャンボフレーム) または 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。接

続あるいは仮想インターフェイスがジャンボフレームをサポートしているかを確認するには、 AWS Direct Connect コンソールを選択して [概要] タブで [ジャンボフレーム対応] を見つけます。

VPC へのプライベート仮想インターフェイスをプロビジョニングするには

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

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

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

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

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

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

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

      有効な値は 1 ~ 2,147,483,647 です。

6. [追加設定] で、以下を実行します。

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

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

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

      > **Important**
      >
      > AWS Direct Connect 仮想インターフェイスを設定するときは、RFC 1918 を使用して独自の IP アドレスを指定したり、他のアドレス指定スキームを使用した

り、point-to-point接続のために RFC 3927 169.25IPv4.0.0/16 IPv4 リンクローカル範囲から割り当てられた AWS 割り当てられた IPv4 /29 CIDR アドレスを選択したりできます。 IPv4 これらのpoint-to-point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 ピア接続にのみ使用する必要があります。VPC トラフィックまたはトンネリングの目的で、 AWS Site-to-Site Private IP VPN や Transit Gateway Connect などでは、point-to-point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または送信先アドレスとして使用 AWS 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 (AWS Direct Connect API)

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

   a. [仮想インターフェイス名] に、仮想インターフェイスの名前を入力します。
   b. [接続] で、このインターフェイスに使用する Direct Connect 接続を選択します。
   c. 仮想インターフェイスの所有者は、仮想インターフェイスがアカウント用 AWS である場合は、マイ AWS アカウントを選択します。
   d. [Direct Connect ゲートウェイ] の場合、[Direct Connect ゲートウェイ] を選択します。
   e. [VLAN] に、仮想ローカルエリアネットワーク (VLAN) の ID 番号を入力します。
   f. [BGP ASN] に、新しい仮想インターフェイスが使用するオンプレミスピアルーターの、ボーダーゲートウェイプロトコル自律システム番号を入力します。

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

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

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

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

> **Important**
>
> AWS Direct Connect 仮想インターフェイスを設定するときは、RFC 1918 を使用して独自の IP アドレスを指定したり、他のアドレス指定スキームを使用したり、RFC 3927 169.25IPv4.0.0/16 IPv4 リンクローカル範囲から AWS 割り当てられた IPv4 /29 CIDR アドレスを選択してpoint-to-point接続を行ったりすることができます。 IPv4 これらのpoint-to-point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 ピア接続にのみ使用する必要があります。VPC トラフィックまたはトンネリングの目的で、 AWS Site-to-Site Private IP VPN や Transit Gateway Connect などでは、point-to-point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または送信先アドレスとして使用 AWS 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 (AWS Direct Connect API)

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

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGatewayAttachments (AWS Direct Connect API)

AWS 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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. 仮想インターフェイスを選択したら、[View details (詳細の表示)] を選択します。
4. [ルーター設定をダウンロードする] を選択します。
5. [ルーター設定をダウンロードする] で、次を実行します。
   a. [Vendor] で、ルーターの製造元を選択します。
   b. [Platform] で、ルーターのモデルを選択します。

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

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

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
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 >

ホストされた AWS Direct Connect 仮想インターフェイス

別のアカウントと AWS Direct Connect の接続を使用するには、そのアカウントのホスト仮想インターフェイスを作成します。他のアカウントの所有者は、利用を開始するためにはホスト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
Connection	仮想インターフェイスを作成する AWS Direct Connect 接続またはリンク集約グループ (LAG)。
仮想インターフェイス名	仮想インターフェイスの名前。
仮想インターフェイス所有者	別のアカウントの仮想インターフェイスを作成する場合は、別の AWS アカウントのアカウント ID が必要です。
(プライベート仮想インターフェイスのみ) 接続	同じ AWS リージョンの VPC に接続するには、VPC の仮想プライベートゲートウェイが必要です。Amazon 側の BGP セッションのための ASN は、仮想プライベートゲートウェイから継承されます。仮想プライベートゲートウェイを作成するときに、独自のプライベート ASN を指定できます。そうでない場合は、Amazon によってデフォルトの ASN が指定されます。詳細については、Amazon VPC ユーザーガイドの Create a Virtual Private Gateway を参照してください。Direct Connect Gateway 経由で VPC に接続する場合は、Direct Connect Gateway が必要です。詳細については、「Direct Connect Gateway」を参照してください。
VLAN	仮想ローカルエリアネットワーク (VLAN) の、まだ接続で使用されていない一意のタグ。値は 1 ~ 4094 を指定する必要があります。またイーサネット 802.1Q 規格を満たしている必要があります。このタグは、 AWS Direct Connect 接続を通過するすべてのトラフィックに必要です。

リソース	必要な情報
	ホスト接続がある場合、 AWS Direct Connect パートナーはこの値を提供します。仮想インターフェイス作成後に値を変更することはできません。

リソース	必要な情報

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

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

リソース	必要な情報

(パブリック仮想インターフェイスのみ) アドバタイズするプレフィックス	BGP 経由でアドバタイズするパブリックの IPv4 ルートまたは IPv6 ルート。BGP を使用して少なくとも 1 つ (最大 1,000 個) のプレフィックスをアドバタイズする必要があります。
	• IPv4: IPv4 CIDR は、次のいずれかに該当する場合 AWS Direct Connect 、を使用して発表された別のパブリック IPv4 CIDR と重複する可能性があります。
	  • CIDRs は異なる AWS リージョンからのものです。パブリックプレフィクスに BGP コミュニティタグを適用していることを確認してください。
	  • アクティブ/パッシブ構成にパブリック ASN がある場合は、AS_PATH を使用します。
	  詳細については、Routing policies and BGP communities を参照してください。
	• 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	パケットオーバーの最大送信単位 (MTU) AWS Direct Connect。デフォルトは 1500 です。仮想インターフェースの MTU を 9001 (ジャンボフレーム) に設定すると、基盤となる物理接続を更新する要因となることがあります (ジャンボフレームをサポートするために更新されていない場合)。接続の更新は、この接続に関連付けられるすべての仮想インターフェイスのネットワーク接続を最大で 30 秒間中断します。ジャンボフレームは、 からの伝播されたルートにのみ適用されます AWS Direct Connect。仮想プライベートゲートウェイを指すルートテーブルに静的ルートを追加する場合、静的ルートを介してルーティングされるトラフィックは 1500 MTU を使用して送信されます。接続または仮想インターフェイスがジャンボフレームをサポートしているかどうかを確認するには、 AWS Direct Connect コンソールでそれを選択し、仮想インターフェイスの一般的な設定ページでジャンボフレームが使用可能かどうかを確認します。

で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 AWS Direct Connect

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

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

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

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

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

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

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

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

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

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

> **Important**
>
> AWS Direct Connect 仮想インターフェイスを設定するときは、RFC 1918 を使用して独自の IP アドレスを指定したり、他のアドレス指定スキームを使用したり、point-to-point接続のために RFC 3927 169.25IPv4.0.0/16 IPv4 リンクローカル範囲から割り当てられた AWS 割り当てられた IPv4 /29 CIDR アドレスを選択したりできます。 IPv4 これらのpoint-to-point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 ピア接続にのみ使用する必要があります。VPC トラフィックまたはトンネリングの目的で、 AWS Site-to-Site Private IP VPN や Transit Gateway Connect などでは、point-to-point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または送信先アドレスとして使用 AWS 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 (AWS Direct Connect API)

で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 AWS Direct Connect

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

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

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

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

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

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

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

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

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

[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 (AWS Direct Connect API)

AWS Direct Connect ホストされたトランジット仮想インターフェイスを作成する

ホストされたトランジット仮想インターフェイスを作成するには

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

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

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

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

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

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

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

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

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

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

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

> **Important**
>
> AWS Direct Connect 仮想インターフェイスを設定するときは、RFC 1918 を使用して独自の IP アドレスを指定したり、他のアドレス指定スキームを使用したり、RFC 3927 169.25IPv4.0.0/16 IPv4 リンクローカル範囲から AWS 割り当てられた IPv4 /29 CIDR アドレスを選択してpoint-to-point接続を行ったりすることができます。 IPv4 これらのpoint-to-point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 ピア接続にのみ使用する必要があります。VPC トラフィックまたはトンネリングの目的で、 AWS Site-to-Site Private IP VPN や Transit Gateway Connect などでは、point-to-point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または送信先アドレスとして使用 AWS 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 (AWS Direct Connect API)

AWS Direct Connect 仮想インターフェイスの詳細を表示する

仮想インターフェイスの現在のステータスは、 AWS 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。詳細は次のとおりです。

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

仮想インターフェイスに関する詳細を表示するには

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

コマンドラインまたは API を使用して仮想インターフェイスを説明するには

- describe-virtual-interfaces (AWS CLI)
- DescribeVirtualInterfaces (AWS Direct Connect API)

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

AWS 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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. 仮想インターフェイスを選択したら、[View details (詳細の表示)] を選択します。
4. [ピア接続の追加] を選択します。
5. (プライベート仮想インターフェイス) IPv4 BGP ピアを追加するには、以下を実行します。
   - [IPv4] を選択します。
   - これらの IP アドレスを手動で指定するには、[ルーターのピア IP] に、Amazon がトラフィックを送信する送信先 IPv4 CIDR アドレスを入力します。[Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。
6. (パブリック仮想インターフェイス) IPv4 BGP ピアを追加するには、以下を実行します。
   - [ルーターのピア IP] に、トラフィックの送信先となる IPv4 CIDR アドレスを入力します。
   - [Amazon ルーターのピア IP] に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

> **Important**
>
> AWS Direct Connect 仮想インターフェイスを設定するときは、RFC 1918 を使用して独自の IP アドレスを指定したり、他のアドレス指定スキームを使用したり、RFC 3927 169.25IPv4.0.0/16 IPv4 リンクローカル範囲から AWS 割り当てられた IPv4 /29 CIDR アドレスを選択してpoint-to-point接続を行ったりすることができます。 IPv4 これらのpoint-to-point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 ピア接続にのみ使用する必要があります。VPC トラフィックまたはトンネリングの目的で、 AWS Site-to-Site Private IP VPN や Transit Gateway Connect などでは、point-to-point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または送信先アドレスとして使用 AWS 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 ~ 2147483647 です。

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

コマンドラインまたは API を使用して BGP ピアを作成するには

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

AWS 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)。仮想インターフェイス BGP ピアは、 AWS 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。

BGP ピアを削除するには

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

コマンドラインまたは API を使用して BGP ピアを削除するには

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

AWS 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、 AWS 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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. 仮想インターフェイスを選択し、[編集] を選択します。
4. ジャンボ MTU (MTU サイズ 8500) で、有効を選択します。
5. [確認] で [I understand the selected connection(s) will go down for a brief period (選択された接続は短時間停止することを理解しています)] を選択します。更新が完了するまでの仮想インターフェイスのステータスは、`pending` です。

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

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

AWS Direct Connect 仮想インターフェイスタグの追加または削除

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

   [タグの追加] [タグの追加] を選択して、以下を実行します。

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

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

コマンドラインを使用してタグを追加または削除するには

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

AWS Direct Connect 仮想インターフェイスを削除する

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

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

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

- delete-virtual-interface (AWS CLI)
- DeleteVirtualInterface (AWS Direct Connect API)

ホスト AWS Direct Connect 仮想インターフェイスを受け入れる

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。

コンソール、 AWS Direct Connect コマンドライン、または API を使用して、ホスト仮想インターフェイスを受け入れることができます。

ホスト型仮想インターフェイスを承諾するには

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

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

   (プライベート仮想インターフェイス) [仮想インターフェイスの承諾] ダイアログボックスで、仮想プライベートゲートウェイまたは Direct Connect ゲートウェイを選択して、[仮想インターフェイスの承諾] を選択します。
6. ホスト型仮想インターフェイスを承諾すると、 AWS Direct Connect 接続の所有者はルーター設定ファイルをダウンロードすることができます。[ルーター設定をダウンロードする] オプションは、ホストされた仮想インターフェイスを承諾するアカウントでは利用できません。

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

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

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

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

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

- confirm-transit-virtual-interface (AWS CLI)

- ConfirmTransitVirtualInterface (AWS Direct Connect API)

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

3. 仮想インターフェイスを選択し、[編集] を選択します。
4. [接続] で、LAG または接続を選択します。
5. [Edit virtual interface (仮想インターフェイスの編集)] を選択します。

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

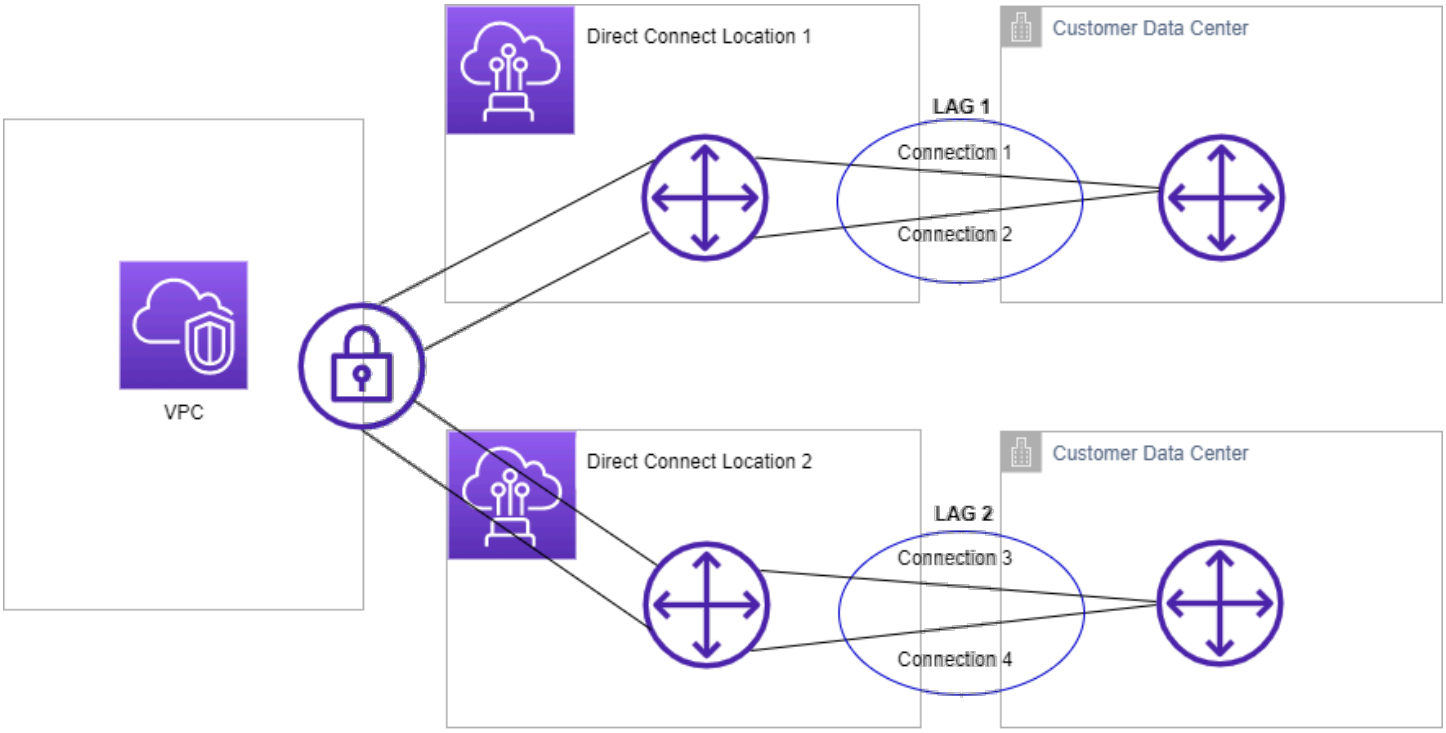
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface (AWS Direct Connect API)

AWS Direct Connect リンク集約グループ (LAGs)

複数の接続を使用して、利用できる帯域幅を増やすことができます。Link Aggregation Group (LAG) は、Link Aggregation Control Protocol (LACP) を使用して 1 つの AWS Direct Connect エンドポイントで複数の接続を集約する論理インターフェイスであり、単一のマネージド接続として扱うことができます。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**
>
> マルチシャーシ LAG (MLAG) は ではサポートされていません AWS。

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に終了する接続の LAG を作成し、設定と管理に 4 つの接続の代わりに 2 つの LAGs を使用できます。



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

以下のルールが適用されます。

- すべての接続は専用接続でなければならず、ポートスピードが 1 Gbps、10 Gbps、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 内のすべての接続は、同じ AWS Direct Connect エンドポイントで終了する必要があります。
- LAGは、パブリック、プライベート、トランジットのすべての仮想インターフェースタイプでサポートされています。

LAG を作成すると、新しい物理接続の Letter of Authorization and Connecting Facility Assignment (LOA-CFA) を AWS Direct Connect コンソールから個別に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 を作成したり、LAG にさらに接続を関連付けたりすると、特定の AWS Direct Connect エンドポイントで十分な数の利用可能なポートを保証できない場合があります。

トピック

- の MACsec に関する考慮事項 AWS Direct Connect
- AWS Direct Connect エンドポイントで LAG を作成する
- AWS Direct Connect エンドポイントで LAG の詳細を表示する
- AWS Direct Connect エンドポイントで LAG を更新する
- AWS Direct Connect エンドポイントで接続を LAG に関連付ける
- AWS 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 を AWS Direct Connect エンドポイント LAG に関連付ける

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

の MACsec に関する考慮事項 AWS Direct Connect

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。

AWS 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、接続が同じ AWS デバイス上にある必要があります (同じ AWS Direct Connect エンドポイントで終了する必要があります) 。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**
> 既存の接続の場合、LAG の作成中に への接続 AWS が中断されます。

新しい接続で LAG を作成するには

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

4. [Lag creation type (LAG 作成タイプ)] で [新しい接続のリクエスト] を選択し、次の情報を入力します。

   - [LAG name (LAG 名)]: LAG の名前。
   - [Location (場所)]: LAG の場所。
   - [ポートスピード]: 接続のポートスピード。
   - [Number of new connections (新しい接続の数)]: 作成する新しい接続の数。ポート速度が 1G または 10G の場合は最大 4 つの接続が可能で、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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. [Create LAG] を選択します。
4. [Lag creation type (LAG 作成タイプ)] で [既存の接続を使用] を選択し、次の情報を入力します。

   - [LAG name (LAG 名)]: LAG の名前。
   - [既存の接続]: LAG に使用する Direct Connect 接続。
   - (オプション) [新しい接続の数]: 作成する新しい接続の数。ポート速度が 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。

- [最小リンク数]: LAG 自体が機能するために使用できる必要がある接続の最小数。値を指定しない場合は、デフォルト値 0 が割り当てられます。

5. (オプション) タグを追加または削除します。

   [タグの追加] [タグの追加] を選択して、以下を実行します。

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

   [タグの削除] タグの横にある [タグの削除] を選択します。

6. [Create LAG] を選択します。

コマンドラインまたは API を使用して LAG を作成するには

- create-lag (AWS CLI)
- CreateLag (AWS Direct Connect API)

コマンドラインまたは API を使用して LAG を記述するには

- describe-lags (AWS CLI)
- DescribeLags (AWS Direct Connect API)

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

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

LAG を作成したら、この LAG に接続を関連付けたり、その関連付けを解除したりできます。詳細については、「接続を LAG に関連付ける」および「LAG から接続の関連付けを解除する」を参照してください。

AWS Direct Connect エンドポイントで LAG の詳細を表示する

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

LAG に関する情報を表示するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択したら、[View details (詳細の表示)] を選択します。
4. ID や接続が終了する AWS Direct Connect エンドポイントなど、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 (AWS Direct Connect API)

AWS Direct Connect エンドポイントで LAG を更新する

AWS 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 Link Aggregation Group (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 の一部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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択し、その後で [編集] をクリックします。
4. LAG の変更

   [名前の変更] [LAG 名] に新しい LAG 名を入力します。

   [接続最小数の調整]: [最小リンク数] に、使用可能な状態にする接続の最小数を入力します。

   [タグの追加] [タグの追加] を選択して、以下を実行します。
   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

   [タグの削除] タグの横にある [タグの削除] を選択します。
5. [Edit LAG (LAG の編集)] を選択します。

コマンドラインまたは API を使用して LAG を更新するには

- update-lag (AWS CLI)
- UpdateLag (AWS Direct Connect API)

AWS Direct Connect エンドポイントで接続を LAG に関連付ける

AWS Direct Connect コンソール、コマンドライン、または API を使用して、既存の接続を LAG に関連付けることができます。接続は、スタンドアロンであっても、別の LAG の一部であってもかまいません。接続は同じ AWS デバイス上にあり、LAG と同じ帯域幅を使用する必要があります。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**
>
> 関連付け中は、接続 AWS を介した への接続が中断されます。

接続を LAG と関連付けるには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択した上で、[詳細の表示] をクリックします。
4. [接続] で [接続の関連付け] を選択します。
5. [接続] では、LAG を使用する Direct Connect 接続を選択します。
6. [接続の関連付け] を選択します。

コマンドラインまたは API を使用して接続を関連付けるには

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag (AWS Direct Connect API)

AWS 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

AWS Direct Connect コンソール、コマンドライン、または API を使用して LAG から関連付けを解除することで、接続をスタンドアロン に変換します。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**
>
> との関連付けを解除すると、 への接続 AWS 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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. 左側のペインで、[LAG] を選択します。
3. LAG を選択した上で、[詳細の表示] をクリックします。
4. [接続] で利用できる接続のリストかた接続を選択したら、[関連付け解除] を選択します。
5. 確認ダイアログボックスで、[関連付け解除] を選択します。

コマンドラインまたは API を使用して接続の関連付けを解除するには

- disassociate-connection-from-lag (AWS CLI)
- DisassociateConnectionFromLag (AWS Direct Connect API)

MACsec CKN/CAK を AWS Direct Connect エンドポイント LAG に関連付ける

MACsec をサポートする LAG を作成したら、 AWS 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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択したら、[View details (詳細の表示)] を選択します。
4. [キーの関連付け] をクリックします。

5. MACsec キーを入力します。

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

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

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

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 (AWS Direct Connect API)

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

AWS Direct Connect コンソール、コマンドライン、または API を使用して、LAG と MACsec キーの関連付けを削除できます。

LAG と MACsec キー間の関連付けを解除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択したら、[View details (詳細の表示)] を選択します。
4. 解除する MacSec シークレットを選択し、[キーの関連付けを解除する] をクリックします。
5. 確認ダイアログボックスで、disassociate と入力し、[関連付けを解除] をクリックします。

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 (AWS Direct Connect API)

AWS 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、 AWS 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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [LAGs] を選択します。
3. LAG を選択し、[削除] をクリックします。
4. 確認ダイアログボックスで、[Delete (削除)] を選択します。

コマンドラインまたは API を使用して LAG を削除するには

- delete-lag (AWS CLI)
- DeleteLag (AWS Direct Connect API)

AWS Direct Connect ゲートウェイ

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

- 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 VPCs、仮想プライベートゲートウェイ、または AWS Cloud WAN を使用している場合は Cloud WAN コアネットワークと Transit Gateway 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して、トランジット仮想インターフェイスを介して、トランジットゲートウェイにアタッチされている VPCs VPNs に Direct Connect 接続を接続します。

- クラウド 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

- AWS Direct Connect ゲートウェイ
- AWS Direct Connect 仮想プライベートゲートウェイの関連付け
- AWS Direct Connect ゲートウェイと Transit Gateway の関連付け
- AWS 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
- AWS Direct Connect ゲートウェイで許可されるプレフィックスインタラクション

AWS Direct Connect ゲートウェイ

AWS Direct Connect ゲートウェイを使用して VPCsを接続します。 AWS Direct Connect ゲートウェイを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 クラウド 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 が含まれますが AWS GovCloud (US)、 AWS 中国リージョンは含まれません。Direct Connect ゲートウェイは、BGP ルートリフレクターの分散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 への依存関係の導入を回避できます AWS リージョン。高可用性は本質的にその設計に組み込まれているため、複数の Direct Connect ゲートウェイは必要ありません。

現在、親アベイラビリティーゾーンをバイパスしている VPC で Direct Connect を使用しているお客様は、Direct Connect 接続または仮想インターフェイスを移行できません。

以下は、Direct Connect ゲートウェイを使用できるシナリオを説明しています。

Direct Connect ゲートウェイでは、同じ Direct Connect ゲートウェイ上にあるゲートウェイの関連付けが相互にトラフィックを送信することはできません (たとえば、仮想プライベートゲートウェイから別の仮想プライベートゲートウェイへ)。2021 年 11 月に実装されたこのルールの例外は、スーパーネットが、同じ Direct Connect ゲートウェイおよび同じ仮想インターフェイス上に関連付けられている接続された仮想プライベートゲートウェイ (VGW) を持つ 2 つ以上の VPC にわたってアドバタイズされる場合です。この場合、VPC は Direct Connect エンドポイントを介して互いに通信できます。例えば、Direct Connect ゲートウェイ (10.0.0.0/24 および 10.0.1.0/24 など) に接続された VPC と重複するスーパーネット (10.0.0.0/8 または 0.0.0.0/0 など) をアドバタイズし、同じ仮想インターフェイス上で、オンプレミスネットワークから VPC は相互に通信できます。

Direct Connect ゲートウェイ内の VPC 間通信をブロックする場合は、次の手順を実行します。

1. VPC 内のインスタンスおよびその他のリソースにセキュリティグループを設定し、VPC 間のトラフィックをブロックします。また、これを VPC のデフォルトのセキュリティグループの一部として使用します。
2. VPC と重複するオンプレミスネットワークからスーパーネットをアドバタイズすることは避けてください。代わりに、VPC と重複しないオンプレミスネットワークからのより具体的なルートをアドバタイズできます。
3. 複数の VPC に同じ Direct Connect Gateway を使用する代わりに、オンプレミスネットワークに接続する VPC ごとに 1 つの Direct Connect ゲートウェイをプロビジョニングします。例えば、開発用および本番用 VPC に単一の Direct Connect ゲートウェイを使用する代わりに、これらの VPC ごとに個別のダイレクトConnect ゲートウェイを使用します。

Direct Connect ゲートウェイは、1 つのゲートウェイの関連付けからゲートウェイの関連付け自体へのトラフィックの送信を禁止しません (ゲートウェイ関連付けからのプレフィックスを含むオンプレミスのスーパーネットルートがある場合など)。同じ Direct Connect ゲートウェイに関連付けられた 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

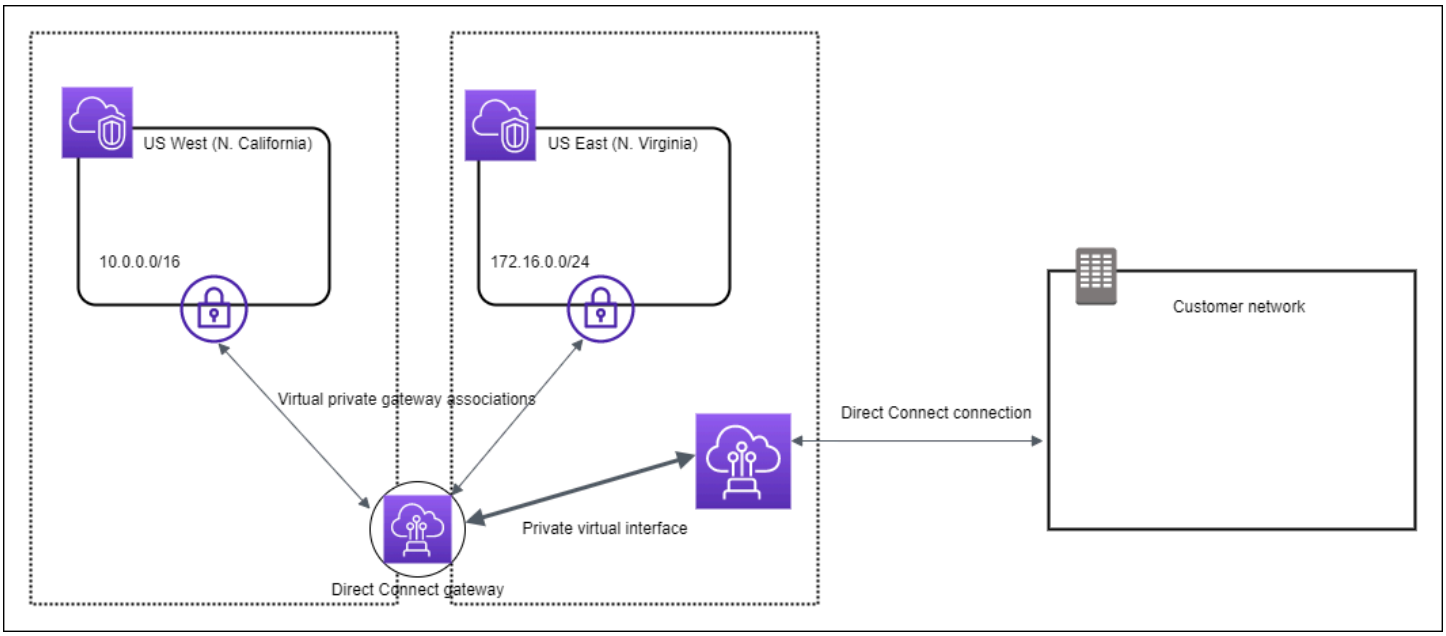
シナリオ

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

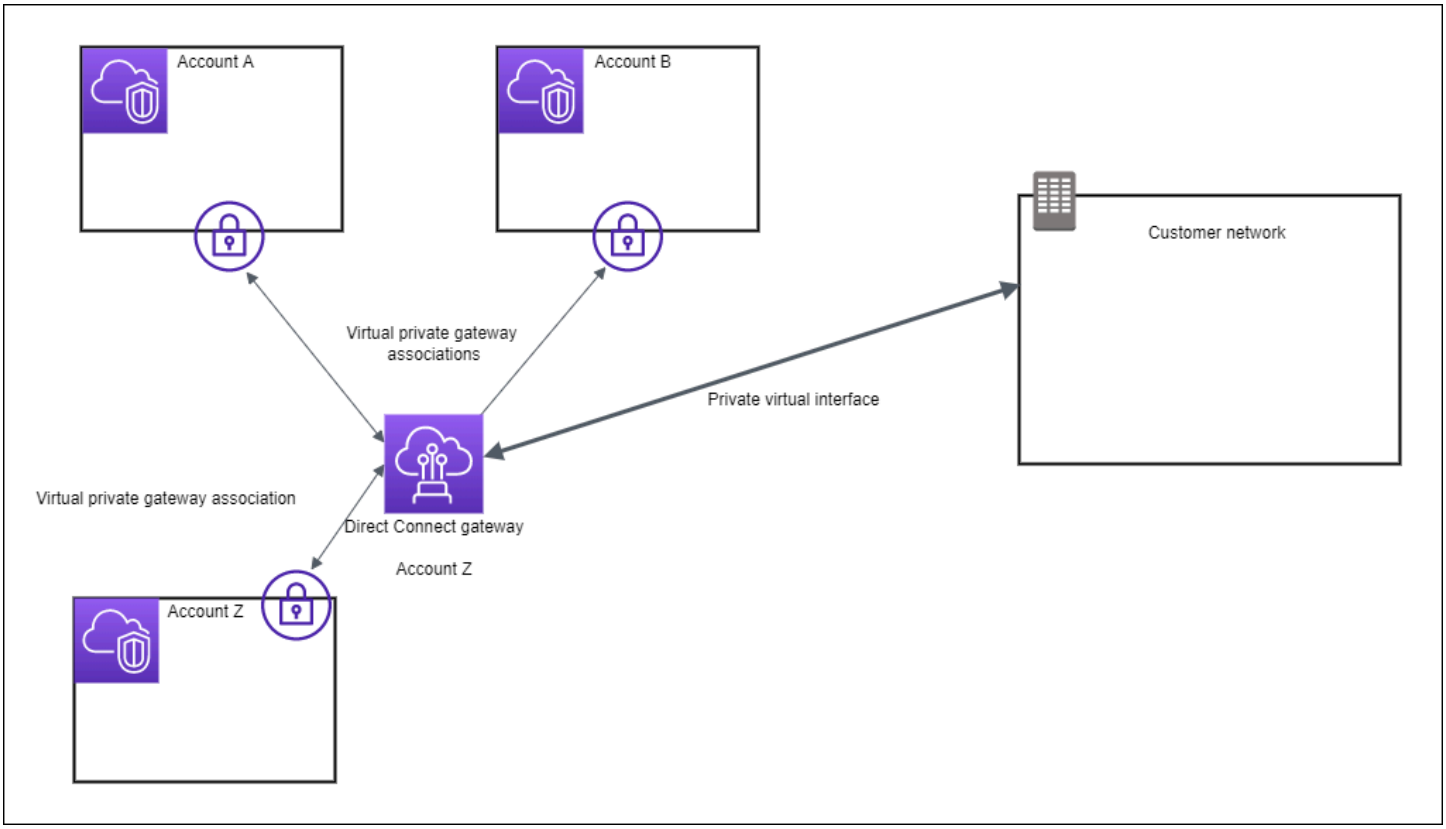
次の図では、Direct Connect ゲートウェイが米国東部 (バージニア北部) リージョンの AWS Direct Connect 接続を使用して、米国東部 (バージニア北部) と米国西部 (北カリフォルニア) の両リージョンにあるアカウント内の VPC へのアクセスを可能にします。

各 VPC には、仮想プライベートゲートウェイの関連付けを使用して Direct Connect ゲートウェイに接続する仮想プライベートゲートウェイがあります。Direct Connect ゲートウェイは、 AWS Direct Connect ロケーションへの接続にプライベート仮想インターフェイスを使用します。ロケーションからお客様のデータセンターへの AWS Direct Connect 接続があります。



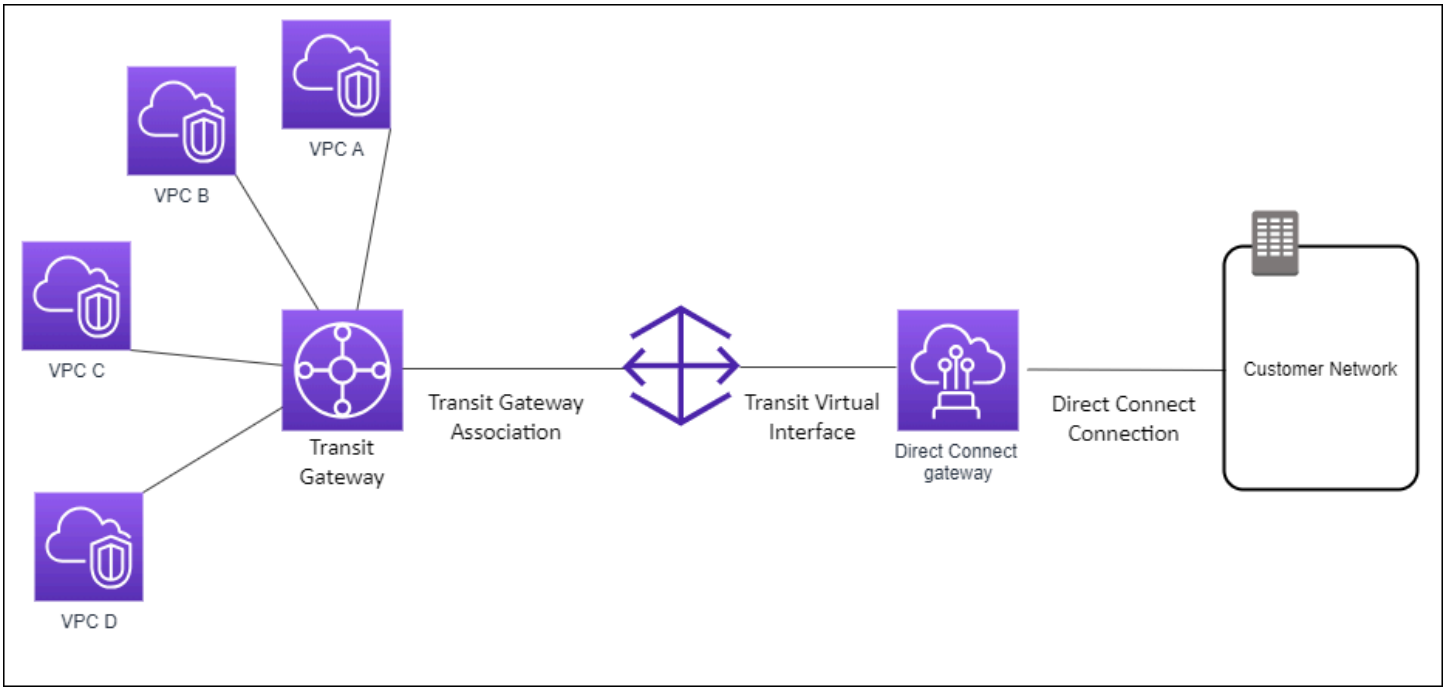
シナリオ: アカウント間の仮想プライベートゲートウェイの関連付け

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。

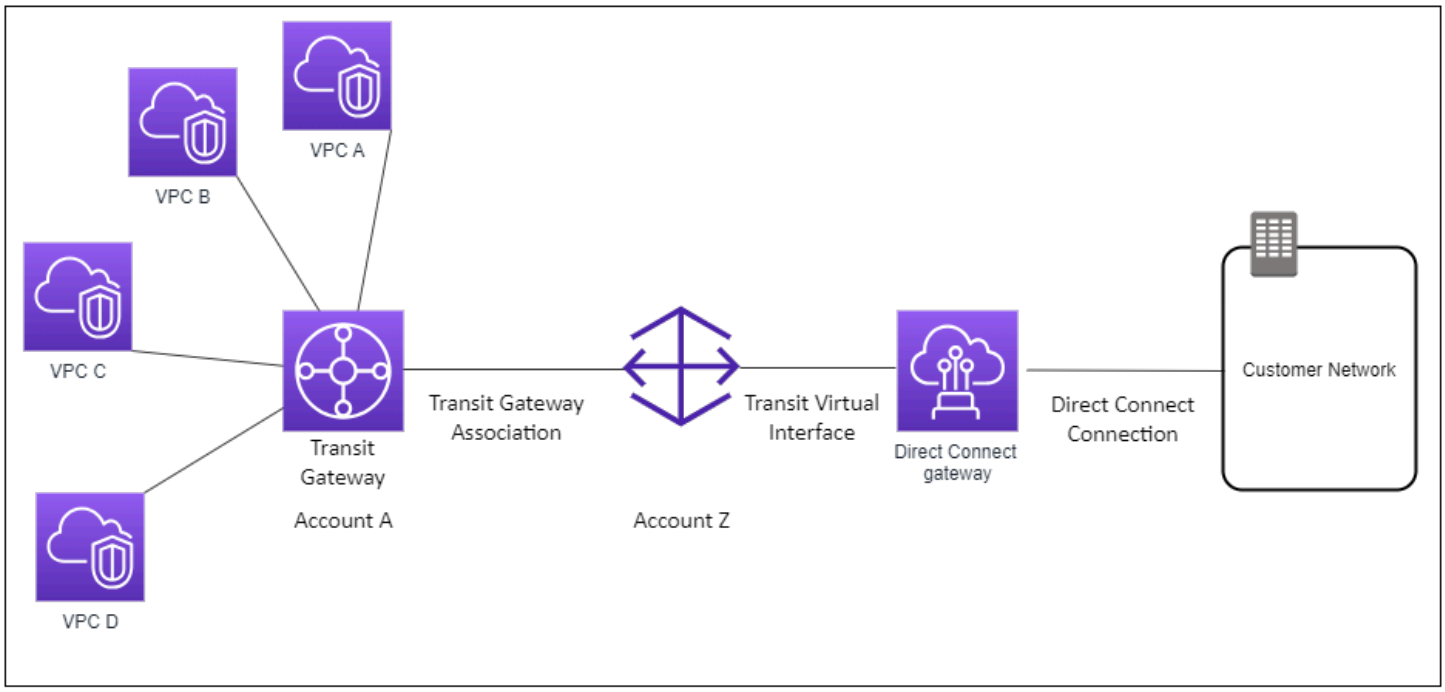
この設定には次のような利点があります。以下を実行できます。

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

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。



AWS Direct Connect ゲートウェイを作成する

Direct Connect ゲートウェイは、 AWS 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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Direct Connect Gateway] を選択します。
3. [Direct Connect Gateway の作成] を作成します。
4. 次の情報を指定し、[Create Direct Connect gateway (Direct Connect ゲートウェイの作成)] を選択します。

   - 名前: Direct Connect ゲートウェイを識別するのに役立つ名前を入力します。
   - Amazon 側の ASN: Amazon 側の BGP セッションのための ASN を指定します。ASN は、64,512 ~ 65,534 または 4,200,000,000 ~ 4,294,967,294 の範囲内で指定する必要があります。

> **Note**
>
> AWS クラウド 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 (AWS Direct Connect API)

仮想プライベートゲートウェイから AWS 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。

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

コマンドラインまたは API を使用して Direct Connect ゲートウェイを削除するには

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway (AWS Direct Connect API)

AWS Direct Connect 仮想プライベートゲートウェイの関連付け

AWS Direct Connect ゲートウェイを使用して、 AWS Direct Connect プライベート仮想インターフェイス経由で、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 VPCs に接続できます。Direct Connect Gateway を VPC の仮想プライベートゲートウェイに関連付けます。次に、Direct Connect ゲートウェイ AWS Direct Connect への接続用のプライベート仮想インターフェイスを作成します。複数のプライベート仮想インターフェイスを、Direct Connect ゲートウェイにアタッチできます。

仮想プライベートゲートウェイの関連付けには、次の規則が適用されます。

- 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 にのみ AWS Direct Connect 接続を接続するには、Direct Connect ゲートウェイを作成できます。または、プライベート仮想インターフェイスを作成し、VPCの仮想プライベートゲートウェイにアタッチすることもできます。詳細については、プライベート仮想インターフェイスを作成する および VPN CloudHub を参照してください。

別のアカウントの VPC と AWS Direct Connect の接続を使用するには、そのアカウントのホストされたプライベート仮想インターフェイスを作成します。他のアカウントの所有者は、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

- AWS Direct Connect 仮想プライベートゲートウェイを作成する
- AWS 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解除
- AWS Direct Connect ゲートウェイへのプライベート仮想インターフェイスを作成する
- アカウント間で AWS Direct Connect 仮想プライベートゲートウェイを関連付ける

AWS Direct Connect 仮想プライベートゲートウェイを作成する

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、 AWS 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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [仮想プライベートゲートウェイ] を選択してから、[仮想プライベートゲートウェイの作成] を選択します。
3. (オプション) 仮想プライベートゲートウェイの名前を入力します。これにより、Name というキーと指定した値を含むタグが作成されます。
4. [ASN] では、デフォルトの Amazon ASN を使用するためにデフォルトの選択のままにします。それ以外の場合は、[カスタム ASN] を選択して値を入力します。16 ビット ASN では、値は 64512 から 65534 の範囲内である必要があります。32 ビット ASN では、値は 4200000000 から 4294967294 の範囲内である必要があります。
5. [Create Virtual Private Gateway] を選択します。
6. 作成した仮想プライベートゲートウェイを選択した後、[Actions]、[Attach to VPC] を選択します。
7. リストから VPC を選択し、[Yes, Attach] を選択します。

コマンドラインまたは API を使用して仮想プライベートゲートウェイを作成するには

- CreateVpnGateway (Amazon EC2 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)

AWS 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解除

仮想プライベートゲートウェイと Direct Connect ゲートウェイの関連付けまたは関連付け解除は、AWS Direct Connect コンソール、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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Direct Connect ゲートウェイ] を選択し、Direct Connect ゲートウェイを選択します。
3. [詳細を表示] を選択します。
4. [ゲートウェイの関連付け]、[ゲートウェイを関連付ける] の順に選択します。
5. [ゲートウェイ] で、関連する仮想プライベートゲートウェイを選択したら、[Associate gateway (ゲートウェイを関連付ける)] を選択します。

[Gateway associations (ゲートウェイの関連付け)] を選択すると、Direct Connect ゲートウェイに関連付けられたすべての仮想プライベートゲートウェイを表示できます。

仮想プライベートゲートウェイの関連付けを解除するには

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

2. ナビゲーションペインで [Direct Connect Gateway] を選択し、Direct Connect ゲートウェイを選択します。
3. [View details] を選択します。
4. [Gateway associations (ゲートウェイの関連付け)] を選択し、仮想プライベートゲートウェイを選択します。
5. [関連付け解除] を選択します。

コマンドラインまたは API を使用して仮想プライベートゲートウェイを関連付けるには

- create-direct-connect-gateway-association (AWS CLI)
- CreateDirectConnectGatewayAssociation (AWS Direct Connect API)

コマンドラインまたは API を使用して、Direct Connect ゲートウェイに関連付けられた仮想プライベートゲートウェイを表示するには

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

コマンドラインまたは API を使用して仮想プライベートゲートウェイの関連付けを解除するには

- delete-direct-connect-gateway-association (AWS CLI)
- DeleteDirectConnectGatewayAssociation (AWS Direct Connect API)

AWS Direct Connect ゲートウェイへのプライベート仮想インターフェイスを作成する

AWS Direct Connect 接続をリモート VPC に接続するには、接続用のプライベート仮想インターフェイスを作成する必要があります。接続先の Direct Connect ゲートウェイを指定します。プライベート仮想インターフェイスは、 AWS Direct Connect コンソール、コマンドライン、または API を使用して作成できます。

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

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

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

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

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

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

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

      有効な値は 1～2,147,483,647 です。

6. [追加設定] で、以下を実行します。

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

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

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

> **Important**
>
> AWS Direct Connect 仮想インターフェイスを設定するときは、RFC 1918 を使用して独自の IP アドレスを指定したり、他のアドレス指定スキームを使用したり、RFC 3927 169.25IPv4.0.0/16 IPv4 リンクローカル範囲から AWS 割り当てられた IPv4 /29 CIDR アドレスを選択してpoint-to-point接続を行ったりすることができます。 IPv4 これらのpoint-to-point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 ピア接続にのみ使用する必要があります。VPC トラフィックまたはトンネリングの目的で、 AWS Site-to-Site Private IP VPN や Transit Gateway Connect などでは、point-to-point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または送信先アドレスとして使用 AWS 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 (AWS Direct Connect API)

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

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGatewayAttachments (AWS Direct Connect API)

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

Direct Connect ゲートウェイは、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。

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

AWS Direct Connect ゲートウェイを使用して、トランジット仮想インターフェイス経由で、トランジットゲートウェイにアタッチされている VPCs または VPNs に Direct Connect 接続を接続できます。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 AWS Direct Connect への接続用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。
- `/30` 範囲を使用するpoint-to-point接続アドレスは、例えば、トランジットゲートウェイには伝達`192.168.0.0/30`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トランジットゲートウェイに関連付けることができます。Transit Gateway の所有者が関連付け提案を作成し、Direct Connect ゲートウェイの所有者がこの関連付け提案を承諾する必要があります。

関連付け提案には、Transit Gateway から許可されるプレフィックスを含めることができます。Direct Connect ゲートウェイの所有者は、関連付け提案でリクエストされたプレフィックスを必要に応じて上書きできます。

許可されたプレフィックス

Transit Gateway の関連付けの場合、許可されたプレフィックスリストを Direct Connect ゲートウェイでプロビジョニングします。このリストは、Transit Gateway にアタッチされた VPCs に CIDRs が割り当てられていない場合でも、オンプレミスから Transit Gateway AWS にトラフィックを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

- AWS Direct Connect と Transit Gateway の関連付けまたは関連付け解除
- AWS 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 と AWS Direct Connect 関連付け提案を作成する
- Transit Gateway と AWS Direct Connect 関連付け提案を承諾または拒否する
- トランジットゲートウェイと AWS Direct Connect 関連付けの許可されたプレフィックスを更新する
- Transit Gateway と AWS Direct Connect 関連付け提案を削除する

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

AWS Direct Connect コンソール、コマンドライン、または API を使用して、トランジットゲートウェイの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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Direct Connect Gateway] を選択し、Direct Connect ゲートウェイを選択します。
3. [View details] を選択します。
4. [Gateways associations (ゲートウェイの関連付け)]、[Associate gateway (ゲートウェイを関連付ける)] の順に選択します。
5. [Gateways (ゲートウェイ)] で、Transit Gateway を選択して関連付けます。

6. [許可されたプレフィックス] に、Direct Connect ゲートウェイがオンプレミスのデータセンターにアドバタイズするプレフィックス (カンマ区切りまたは改行) を入力します。許可されたプレフィックスの詳細については、「許可されたプレフィックスのインタラクション」を参照してください。
7. [Associate gateway (ゲートウェイを関連付ける)] を選択します

[Gateway associations (ゲートウェイの関連付け)] を選択すると、Direct Connect ゲートウェイに関連付けられたすべてのゲートウェイを表示できます。

Transit Gateway の関連付けを解除するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Direct Connect ゲートウェイ] を選択し、Direct Connect ゲートウェイを選択します。
3. [View details] を選択します。
4. [Gateway associations (ゲートウェイの関連付け)] を選択し、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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Direct Connect gateways] (Direct Connect ゲートウェイ) をクリックしてから、許可されたプレフィックスの追加または削除を行う Direct Connect ゲートウェイを選択します。
3. [Gateway associations] (ゲートウェイの関連付け) タブを選択します。
4. 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、編集を選択します。
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 (AWS Direct Connect API)

コマンドラインまたは API を使用して、Direct Connect ゲートウェイに関連付けられた Transit Gateway を表示するには

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

コマンドラインまたは API を使用して Transit Gateway の関連付けを解除するには

- delete-direct-connect-gateway-association (AWS CLI)
- DeleteDirectConnectGatewayAssociation (AWS 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 (AWS Direct Connect API)

AWS 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

AWS Direct Connect 接続をトランジットゲートウェイに接続するには、接続用のトランジットインターフェイスを作成する必要があります。接続先の Direct Connect ゲートウェイを指定します。AWS 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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Virtual Interfaces] を選択します。
3. [仮想インターフェイスの作成] を選択します。
4. [Virtual interface type (仮想インターフェイスタイプ)] の [タイプ] で [Transit (トランジット)] を選択します。
5. [Transit virtual interface settings (トランジット仮想インターフェイス設定)] で以下を実行します。

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

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

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

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

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

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

      有効な値は 1 ~ 2,147,483,647 です。

6. [追加設定] で、以下を実行します。

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

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

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

- [Amazon router peer ip] (Amazon ルーターのピア IP) に、 AWSへのトラフィック送信に使用する IPv4 CIDR アドレスを入力します。

> **Important**
>
> AWS Direct Connect 仮想インターフェイスを設定するときは、RFC 1918 を使用して独自の IP アドレスを指定したり、他のアドレス指定スキームを使用したり、RFC 3927 169.25IPv4.0.0/16 IPv4 リンクローカル範囲から AWS 割り当てられた IPv4 /29 CIDR アドレスを選択してpoint-to-point接続したりできます。 IPv4 これらのpoint-to-point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 ピア接続にのみ使用する必要があります。 AWS Site-to-Site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の目的で、 ではpoint-to-point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または送信先アドレスとして使用 AWS 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 (AWS Direct Connect API)

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

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGatewayAttachments (AWS Direct Connect API)

Transit Gateway と AWS Direct Connect 関連付け提案を作成する

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 にアタッチする必要があります。Direct Connect ゲートウェイの所有者は、Direct Connect ゲートウェイの ID とその AWS アカウントの ID を共有する必要があります。提案を作成したら、Direct Connect ゲートウェイの所有者は、 を介したオンプレミスネットワークへのアクセスを取得するためにこの提案を承諾する必要があります AWS Direct Connect AWS 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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Transit Gateways] 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 (AWS Direct Connect API)

Transit Gateway と AWS Direct Connect 関連付け提案を承諾または拒否する

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

関連付け提案を承諾するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Direct Connect Gateway] を選択します。
3. 保留中の提案がある Direct Connect ゲートウェイを選択し、[詳細を表示] を選びます。
4. [Pending proposals (保留中の提案)] タブで提案を選択し、[提案を許可] を選びます。
5. (オプション) Transit Gateway から許可されるプレフィックスのリストを指定するには、[Allowed prefixes (許可されたプレフィックス)] にプレフィックスを追加します。プレフィックスは、カンマを使用して区切るか、1 行ずつ入力します。
6. [提案を許可] を選択します。

関連付け提案を拒否するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Direct Connect Gateway] を選択します。
3. 保留中の提案がある Direct Connect ゲートウェイを選択し、[詳細を表示] を選びます。
4. [Pending proposals (保留中の提案)] タブで 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 (AWS 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 (AWS 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 (AWS Direct Connect API)

トランジットゲートウェイと AWS Direct Connect 関連付けの許可されたプレフィックスを更新する

コンソール、コマンドライン AWS Direct Connect 、または API を使用して、Direct Connect ゲートウェイ経由で Transit Gateway から許可されるプレフィックスを更新できます。 AWS 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ている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 (AWS Direct Connect API)

Transit Gateway と AWS Direct Connect 関連付け提案を削除する

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、 AWS 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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで、[Transit Gateways] 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 (AWS Direct Connect API)

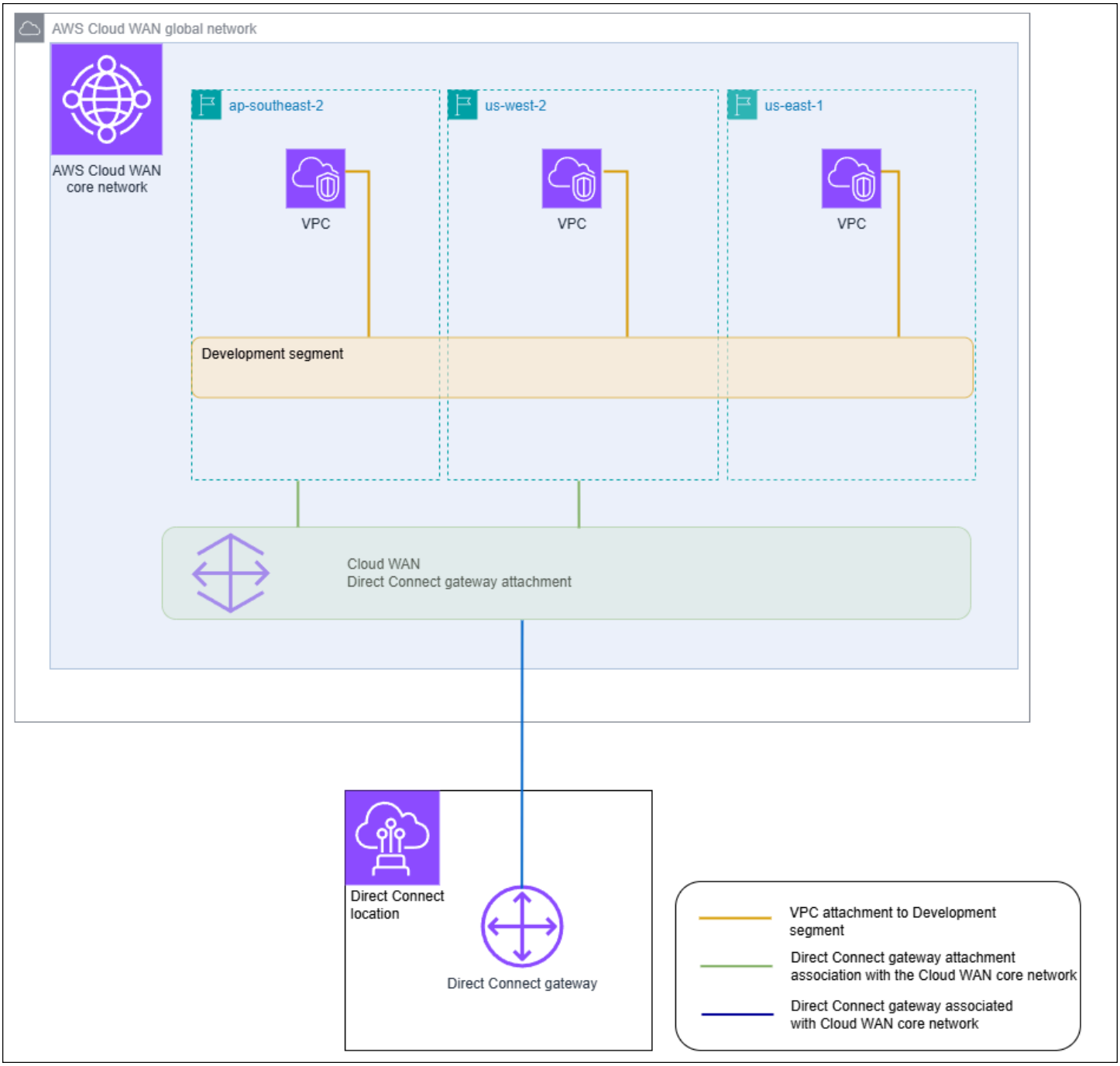
AWS Direct Connect ゲートウェイと AWS Cloud WAN コアネットワークの関連付け

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

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) をサポートします。Direct Connect アタッチメントは、中央ポリシーベースの管理、タグベースのアタッチメントの自動化、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。クラウド WAN で Direct Connect ゲートウェイを使用する場合、Direct Connect コンソールと APIsおよび 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 つのリージョンがある 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、これら 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た独自の VPC があります。Cloud WAN を使用すると、Direct Connect ゲートウェイを使用して作成された Direct Connect ゲートウェイを使用して、Direct Connect ゲートウェイアタッチメントが Cloud WAN 内に作成されます。アタッチメントは、ap-southeast-2 と us-west-2 の 3 つのリージョンのうちの 2 つに関連付けられ、開発セグメントへのアクセスが許可されます。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ないため、使用できません。



トピック

- 前提条件
- 考慮事項
- クラウド 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 AWS Direct Connect ゲートウェイの関連付けを検証する

前提条件

クラウド 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 クラウド 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

クラウド 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はできません。ゲートウェイとコアネットワーク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ます。
- Cloud WAN Direct Connect ゲートウェイアタッチメントは、接続にトランジット仮想インターフェイスタイプを使用します。
- 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。
- オンプレミスからトランジット仮想インターフェイス AWS を介して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他の Direct Connect リソースのクォータも適用されます。「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。
- クラウド WAN は、転送に 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ていない場合があります。クラウド 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 「 クラウド WAN ユーザーガイド」の「クラウド WAN の Direct Connect ゲートウェイアタッチメント」を参照してください。 AWS

- 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と、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 「ネットワークモニターの使用」を参照してください。

クラウド 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 APIs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。

クラウド 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 「 クラウド WAN ユーザーガイド」の「クラウド WAN の Direct Connect ゲートウェイアタッチメント」を参照してください。 AWS

AWS Cloud WAN コアネットワークへの AWS 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確認できます。

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. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで Direct Connect ゲートウェイを選択します。
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。
   - State 列には、関連付けられている が表示されます。
   - 関連付けタイプの列には、Cloud WAN Core Network 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 (AWS Direct Connect API)
- describe-direct-connect-gateway-association (AWS CLI)

AWS Direct Connect ゲートウェイで許可されるプレフィックスインタラクション

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のみが遅延またはドロップされ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。

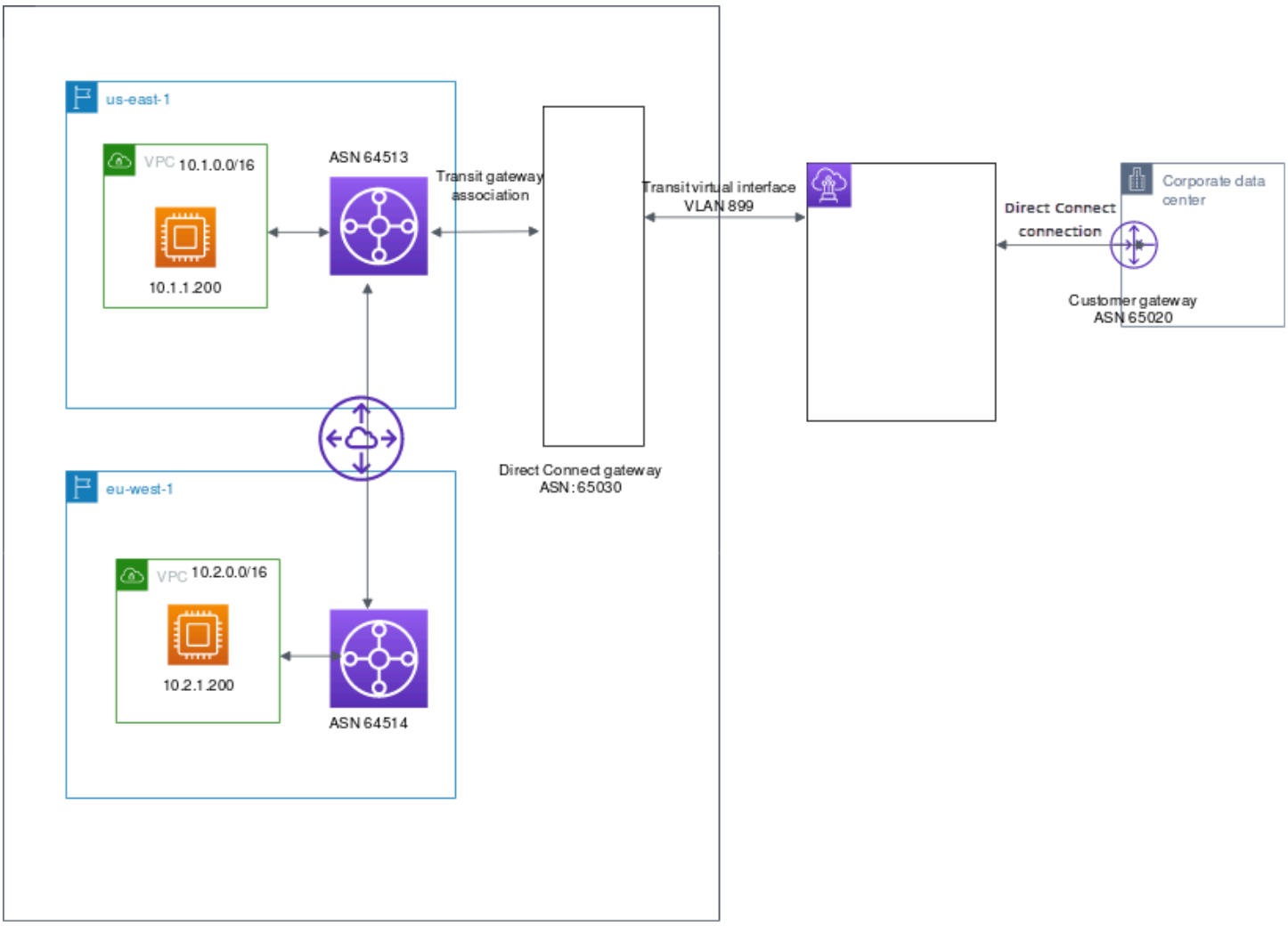
複数の Transit Gateway が Direct Connect ゲートウェイに関連付けられている場合、許可されるプレフィックスの重複は許可されません。例えば、許可されたプレフィックスリストに 10.1.0.0/16 を含む Transit Gateway があり、許可されたプレフィックスリストが 10.2.0.0/16 と 0.0.0.0/0 を含む 2 番目の Transit Gateway がある場合、2 番目の Transit Gateway からの関連付けを 0.0.0.0/0 に設定することはできません。0.0.0.0/0 にはすべての IPv4 ネットワークが含まれるため、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のみが遅延またはドロップされ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 2 つの異なる AWS リージョンにインスタンスがある設定を検討してください。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。
- オンプレミスのロケーションと AWS Direct Connect ロ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 に設定し、カスタマールーターピア 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 ゲートウェイとトランジットゲートウェイの関連付け: 許可されたプレフィックスを 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 からトラフィックをルーティングするには、送信先が 0.0.0.0/0 でトランジットゲートウェイ ID をターゲットとするルートを VPC ルートテーブルに作成します。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。トランジットゲートウェイへのルーティングの詳細については、「Amazon VPC ユーザーガイド」の「トランジットゲートウェイのルーティング」を参照してください。

AWS Direct Connect リソースにタグを付ける

タグは、リソース所有者が AWS Direct Connect リソースに割り当てるラベルです。タグはそれぞれ、1 つのキーとオプションの 1 つの値で設定されており、どちらもお客様側が定義します。タグを使用すると、リソース所有者はリソース AWS Direct Connect を目的や環境など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、リージョンに 2 つの AWS Direct Connect 接続があり、それぞれが異なる場所にあります。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。一貫性のある一連のタグキーを使用することで、リソースの管理が容易になります。タグには意味的な意味はなく AWS Direct Connect 、厳密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。

AWS Direct Connect コンソール、 AWS Direct Connect API、、 AWS CLI、または AWS SDK を使用して AWS Tools for Windows PowerShell、次の AWS Direct Connect リソースにタグを付ける

ことができます。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	はい	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	はい	あり	はい	いいえ

タグの制限

タグには以下のルールや制限があります。

- リソースあたりのタグの最大数: 50
- キーの最大長: 128 文字 (Unicode)
- 値の最大長: 265 文字 (Unicode)
- タグのキーと値は大文字と小文字が区別されます。
- aws: プレフィックスは AWS 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。コスト管理でタグを使用する方法については、 AWS Billing and Cost Management 「 ユーザーガイド」の「コスト配分タグの使用」を参照してください。

CLI または API でのタグの操作

リソースのタグの追加、更新、リスト表示、および削除には、次を使用します。

タスク	API	CLI
1 つ以上のタグを追加、または上書きします。	TagResource	タグリソース
1 つ以上のタグを削除します。	UntagResource	タグなしリソース
1 つ以上のタグを記述します。	DescribeTags	describe-tags

例

tag-resource コマンドを使用して、接続 dxcon-11aa22bb にタグ付けします。

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

describe-tags コマンドを使用して、接続 dxcon-11aa22bb のタグを示します。

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb
```

untag-resource コマンドを使用して、接続 dxcon-11aa22bb からタグを削除します。

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

のセキュリティ AWS Direct Connect

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、最もセキュリティの影響を受けやすい組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。「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。が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 AWS Direct Connect、AWS 「コンプライアンスプログラムによる対象範囲内のサービス」を参照してください。
- クラウドのセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、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、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS Direct Connect。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 AWS Direct Connect ように を設定する方法を示します。また、 AWS Direct Connect リソースのモニタリングや保護に役立つ他の 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
- Direct Connect のための Identity and Access Management
- での口グ記録とモニタリング AWS Direct Connect
- のコンプライアンス検証 AWS Direct Connect
- の耐障害性 AWS Direct Connect
- のインフラストラクチャセキュリティ AWS Direct Connect

でのデータ保護 AWS Direct Connect

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS Direct Connect。このモデルで説明されているように、 AWS はすべての 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責任があります AWS クラウド。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。

データ保護の目的で、認証情報を保護し AWS アカウント 、 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設定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。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。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 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- 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 AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」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を、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含めないことを強くお勧めします。これは、コンソール AWS Direct Connect 、API、または SDK を使用して AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、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 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 は、デフォルトで転送中のトラフィックを暗号化しません。が通過する転送中のデータを暗号化するには AWS Direct Connect、そのサービスの転送暗号化オプションを使用する必要があります。EC2 インスタンス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 では AWS Site-to-Site VPN、1 つ以上の AWS Direct Connect 専用ネットワーク接続を Amazon VPC VPN と組み合わせることができます。この組み合わせにより、IPsec

で暗号化されたプライベート接続が提供されます。これにより、ネットワークコストが削減され、帯域幅のスループットが向上し、インターネットベースの VPN 接続よりも一貫性のあるネットワーク体験が提供されます。詳細については、Amazon VPC から Amazon VPC への接続オプションを参照してください。

MAC Security (MACsec) は IEEE 標準の 1 つです。データの機密性、データの整合性、およびデータオリジンの信頼性を定義しています。MACsec をサポートする AWS Direct Connect 接続を使用して、企業のデータセンターから AWS Direct Connect の場所にデータを暗号化できます。詳細については、「MAC セキュリティ (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 AWS のサービス するのに役立つ 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、追加料金なしで使用できる AWS のサービス です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- 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
- のサービスにリンクされたロール AWS Direct Connect
- AWS 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、Direct Connect で行う作業によって異なります。

サービスユーザー – Direct Connect サービスを使用してジョブを実行する場合は、必要なアクセス許可と認証情報を管理者が用意します。さらに多くの Direct Connect 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者から適切なアクセス許可をリクエストするのに役に立ちます。Direct Connect の機能にアクセスできな

い場合は、 Direct Connect のアイデンティティとアクセスのトラブルシューティング を参照してください。

サービス管理者 – 社内の Direct Connect リソースを担当している場合は、通常、Direct Connect へのフルアクセスがあります。サービスのユーザーがどの Direct Connect 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を確認して、IAM の基本概念を理解してください。会社で Direct Connect を使用して IAM を利用する方法の詳細については、 Direct Connect が IAM と連携する仕組み を参照してください。

IAM 管理者 – 管理者は、Direct Connect へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる Direct Connect アイデンティティベースのポリシーの例を表示するには、Direct Connect アイデンティティベースのポリシーの例 を参照してください。

アイデンティティを使用した認証

認証は、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーの種類に応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 AWS サインイン ユーザーガイド」の「 へのサインイン AWS アカウント方法」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、 では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS ことを

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「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを介して提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がにアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成するか、独自の ID ソースのユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー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、特定のアクセス許可 AWS アカウント を持つ 内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、

「IAM ユーザーガイド」の「IAM 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。

- クロスサービスアクセス – 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「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。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールの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。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は JSON AWS 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。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「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は、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための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。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所

有する複数の をグループ化して一元管理するためのサービス AWS アカウント です。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」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ポリシー	はい

IAM の機能	Direct Connect のサポート
リソースベースのポリシー	いいえ
ポリシーアクション	はい
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	いいえ
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	はい
プリンシパル権限	はい
サービスロール	はい
サービスリンクロール	いいえ

Direct Connect およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

Direct Connect のアイデンティティベースのポリシー

アイデンティティベース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 ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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。ID ベースの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。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「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は、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM 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 JSON AWS 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。ポリシーアクションの名前は通常、関連付けられた AWS API オペレー

ションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Direct Connect 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 JSON AWS 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。ステートメントにはResource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Direct Connect リソースタイプとその ARN のリストを表示するには、「AWS Direct Connect API リファレンス」の「Direct Connect で定義されるリソースタイプ」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、「 Direct Connect で定義されるアクション」を参照してください。

Direct Connect アイデンティティベースのポリシーの例については、Direct Connect アイデンティティベースのポリシーの例 を参照してください。

Direct Connect リソースベースのポリシーの例については、タグベースの条件を使用した Direct Connect アイデンティティベースのポリシーの例 を参照してください。

Direct Connect のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS 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 (または `Condition` ブロック) を使用すると、ステートメントが有効な条件を指定できます。`Condition` 要素はオプションです。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。

1 つのステートメントに複数の `Condition` 要素を指定する場合、または 1 つの `Condition` 要素に複数のキーを指定する場合、 AWS では `AND` 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理`OR`オペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

Direct Connect 条件キーのリストを確認するには、「AWS Direct Connect API リファレンス」の「Direct Connect の条件キー」を参照してください。条件キーを使用できるアクションおよびリソー

スについては、「サービス認可リファレンス」の「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、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。IAM エンティティ (ユーザーまたはロール) と多くの AWS リソースにタグをアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの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「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

Direct Connect での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する場合などの詳細については、IAM ユーザーガイドAWS のサービス の「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。たとえば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用してアクセスすることができます AWS。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 AWS することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

Direct Connect のクロスサービスプリンシパル許可

転送アクセスセッション (FAS) のサポート: あり

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FASリクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Direct Connect のサービスロール

サービスロールのサポート: 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、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、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。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

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

- Direct Connect のアクション、リソース、および条件
- Direct Connect コンソールの使用
- ユーザーが自分の許可を表示できるようにする
- AWS Direct Connectへの読み取り専用アクセス
- AWS Direct Connectへのフルアクセス
- タグベースの条件を使用した Direct Connect アイデンティティベースのポリシーの例

ポリシー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を実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス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にアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。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することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「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。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、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 AWS CloudFormation。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 – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。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 JSON AWS 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。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Direct Connect のポリシーアクションでは、アクションの前にプレフィックス `directconnect:` を使用します。たとえば、 Amazon EC2 `DescribeVpnGateways` API オペレーションで Amazon EC2 インスタンスを実行するためのアクセス許可をユーザーに付与するには、ポリシーに `ec2:DescribeVpnGateways` アクションを含めます。ポリシーステートメントには、`Action` または `NotAction` エレメントを含める必要があります。Direct Connect は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

次のポリシー例では、 への読み取りアクセスを許可します AWS Direct Connect。

JSON

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

次のポリシー例では、 へのフルアクセスを許可します AWS Direct Connect。

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 JSON AWS 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。ステートメントには`Resource` または `NotResource` 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルのアクセス許可をサポートしないアクションの場合は、ワイルドカード (*) を使用して、ステートメントがすべてのリソースに適用されることを示します。

```
"Resource": "*"
```

Direct Connect では、次の ARN を使用します。

Direct Connect リソース ARN

リソースタイプ	ARN
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`
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 (ARNs AWS 「サービス名前空間」を参照してください。

たとえば、ステートメントで dxcon-11aa22bb インターフェイスを指定するには、次の ARN を使用します。

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

特定のアカウントに属するすべての仮想インスタンスを指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

リソースの作成など、一部の Direct Connect アクションは、特定のリソースで実行できません。このような場合は、ワイルドカード (*) を使用する必要があります。

```
"Resource": "*"
```

Direct Connect のリソースタイプとその ARN のリストを確認するには、IAM ユーザーガイドの「AWS Direct Connectで定義されるリソースタイプ」を参照してください。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。

DescribeConnectionsDescribeVirtualInterfacesDescribeDirectConnectGateways DescribeInterconnects 、または DescribeLags の IAM ポリシーステートメントの Resource フィールドで 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 が API コールでも渡されない限り、指定された は発生Effect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、指定されたEffectが機能します。

次の例では、リクエストで をconnectionId渡さずにDescribeConnectionsアクションが呼び出された場合、どちらの指定も成功Effect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、 "Effect": "Allow" がリクエストでconnectionId指定されたかどうかにかかわらず、 *は 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 アクションで成功します。

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

条件キー

管理者は JSON AWS 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 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。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。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条

件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

Direct Connect は独自の条件キーを定義し、一部のグローバル条件キーの使用をサポートしています。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドのAWS 「グローバル条件コンテキストキー」を参照してください。

タグリソースには条件キーが使用できます。詳細については、「例: 特定のリージョンへのアクセスの制限」を参照してください。

Direct Connect 条件キーのリストを確認するには、「IAM ユーザーガイド」の「Direct Connect の条件キー」を参照してください。条件キーを使用できるアクション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 リソースの詳細を一覧表示および表示できます。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 Direct Connect コンソールを引き続き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アクセス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 または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Direct Connectへの読み取り専用アクセス

次のポリシー例では、 への読み取りアクセスを許可します AWS Direct Connect。

JSON

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

AWS Direct Connectへのフルアクセス

次のポリシー例では、 へのフルアクセスを許可します AWS Direct Connect。

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 ポリシーの条件を使用して、 AWS リソースにタグを付けるリクエストで渡すことができるタグキーと値のペアを制御できます。次の例は、 AWS Direct Connect TagResource アクションを使用して、タグに環境キーと preprod 値または本番値が含まれている場合にのみ、仮想インターフェイスにタグをアタッチす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。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"
       ]
     }
   }
 }
}
```

のサービスにリンクされたロール AWS Direct Connect

AWS Direct Connect は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、直接リンクされた一意のタイプの IAM ロールです AWS Direct Connect。サービスにリンクされたロールは によって事前定義 AWS Direct Connect されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、 の設定 AWS Direct Connect が簡単になります。 は、サービスにリンクされたロールのアクセス許可 AWS Direct Connect を定義し、特に定義されている場合を除き、 のみがその ロールを引き受け AWS Direct Connect ることができます。定義される許可は信頼ポリシーと許可ポリシーに含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールを削除するには、最初に関連リソースを削除する必要があります。これにより、 AWS Direct Connect リソースへのアクセス許可が誤って削除されないため、リソースが保護されます。

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がはいになっているサービスを見つけてく

ださい。サービスにリンクされた役割に関するドキュメントをサービスで表示するには[はい] リンクを選択してください。

のサービスにリンクされたロールのアクセス許可 AWS Direct Connect

AWS Direct Connect は、 という名前のサービスにリンクされたロールを使用しますAWSServiceRoleForDirectConnect。これにより、 AWS Direct Connect は AWS Secrets Manager ユーザーに代わって に保存されている MACSec シークレットを取得できます。

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、 AWS Direct Connect で使用する IAM アイデンティティに必要な許可が付与されている必要があります。必要な許可を付与するには、次のポリシーを IAM アイデンティティにアタッチします。

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。

のサービスにリンクされたロールの作成 AWS Direct Connect

サービスにリンクされたロールを手動で作成する必要はありません。 はサービスにリンクされたロールを自動的に AWS Direct Connect 作成します。`associate-mac-sec-key` コマンドを実行すると、 は、 AWS Secrets Manager ユーザーに代わって AWS Direct Connect 、 AWS Management Console、 AWS CLIまたは AWS API に保存されている MACsec シークレットを が取得できるようにするサービスにリンクされたロール AWS 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、再度作成する必要がある場合は、同じプロセスを使用してアカウントでロールを再作成できます。 は、サービスにリンクされたロールを再度 AWS Direct Connect 作成します。

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、サービス名を使用して`directconnect.amazonaws.com`サービスにリンクされたロールを作成します。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。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

のサービスにリンクされたロールの編集 AWS Direct Connect

AWS Direct Connect では、`AWSServiceRoleForDirectConnect`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「サービスリンクロールの編集」を参照してください。

のサービスにリンクされたロールの削除 AWS Direct Connect

`AWSServiceRoleForDirectConnect` ロールを手動で削除する必要はありません。サービスにリンクされたロールを削除するときは、 AWS Secrets Manager ウェブサービスに保存されているすべての関連リソースを削除する必要があります。 AWS Management Console、 AWS CLI、または AWS API は、リソースを AWS Direct Connect クリーンアップし、サービスにリンクされた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**
>
> リソースを削除しようとしたときに AWS Direct Connect サービスがロールを使用している場合、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。

が使用する AWS Direct Connect リソースを削除するには **`AWSServiceRoleForDirectConnect`**

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

サービスリンクロールを IAM で手動削除するには

IAM コンソール、 AWS CLI、または AWS API を使用して、`AWSServiceRoleForDirectConnect`サービスにリンクされたロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

AWS Direct Connect サービスにリンクされたロールでサポートされているリージョン

AWS Direct Connect は、MAC セキュリティ機能が利用可能なすべての AWS リージョン でサービスにリンクされたロールの使用をサポートします。詳細については、「AWS Direct Connect ロケーション」を参照してください。

AWS の 管理ポリシー AWS Direct Connect

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケース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 管理ポリシーで定義されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が高くなります。

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 マネージドポリシー: AWSDirectConnectFullAccess

`AWSDirectConnectFullAccess` ポリシーを 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、 へのフルアクセスを許可するアクセス許可を付与します AWS Direct Connect。

このポリシーの許可を確認するには、 AWS Management Consoleの「AWSDirectConnectFullAccess」を参照してください。

AWS マネージドポリシー: 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、 への読み取り専用アクセスを許可するアクセス許可を付与します AWS Direct Connect。

このポリシーの許可を確認するには、 AWS Management Consoleの「AWSDirectConnectReadOnlyAccess」を参照してください。

AWS マネージドポリシー: AWSDirectConnectServiceRolePolicy

このポリシーは、AWSServiceRoleForDirectConnect という名前のサービスにリンクされたロールにアタッチされ、 AWS Direct Connect がユーザーに代わって MAC セキュリティシークレットを取得できるようにします。詳細については、「the section called “サービスにリンクされた役割”」を参照してください。

このポリシーの許可を確認するには、 AWS Management Consoleの「AWSDirectConnectServiceRolePolicy」を参照してください。

AWS Direct ConnectAWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始 AWS Direct Connect してからの の AWS 管理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アラートについては、 AWS Direct Connect ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSDirectConnectServiceRolePolicy - 新しいポリシー	MAC Security をサポートするため、AWSServiceRoleForDirectConnect が追加されました。	2021 年 3 月 31 日
AWS Direct Connect が変更の追跡を開始しました	AWS Direct Connect は、AWS 管理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
- 自分の 以外のユーザーに Direct Connect リソース AWS アカウント 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 管理者にお問い合わせください。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にリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して Direct Connect でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。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 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

自分の 以外のユーザーに Direct Connect リソース AWS アカウント 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 AWS アカウント している のリソースへの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「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」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。

でのログ記録とモニタリング AWS Direct Connect

以下の自動化されたモニタリングツールを使用して、 AWS Direct Connect を監視し、問題が発生したときにレポートできます。

- Amazon CloudWatch アラーム – 指定した期間にわたって 1 つのメトリクスを確認できます。このアラームは、複数の期間にわたる一定のしきい値とメトリクスの値の関係性に基づき、1 つ以上のアクションを実行します。アクションは、Amazon SNS トピックに送信される通知です。CloudWatch のアラームは、メトリクスが特定の状態になっただけではアクションを呼び出しません。アクションを呼び出すには、状態が変化して、指定した期間継続している必要があります。詳細については、「Amazon 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 – アカウント間でログファイルを共有し、CloudWatch Logs に送信して CloudWatch CloudTrail ログファイルをリアルタイムでモニタリングします。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 AWS 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。

のコンプライアンス検証 AWS Direct Connect

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスAWS のサービス プログラムによる範囲内コンプライアンスを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「 Compliance ProgramsAssurance」を参照してください。

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

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべてが HIPAA 対応 AWS のサービス であるわけではありません。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) など) にわたるセキュリティコントロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめたものです。

- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、セキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – 環境をモニタリングして AWS アカウント不審なアクティビティや悪意のあるアクティビティがないか調べることで、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

の耐障害性 AWS Direct Connect

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された複数の物理的に分離されたアベイラビリティーゾーンを提供します。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。

グローバル AWS インフラストラクチャに加えて、 AWS Direct Connect には、データの耐障害性とバックアップのニーズをサポートするのに役立ついくつかの機能が用意されています。

で VPN を使用する方法については AWS Direct Connect、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 には、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が用意されています。障害耐性モデルを選択すると、AWS Direct Connect Resiliency Toolkit が専用の接続順序付けプロセスをガイドします。回復性モデルは、複数の場所で適切な数の専用接続を確保するように設計されています。

- 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、「AWS Direct Connect レジリエンシーツールキット」を参照してください。

のインフラストラクチャセキュリティ AWS Direct Connect

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の手順で保護されています。が AWS 公開した API コールを使用して、ネットワーク AWS Direct Connect 経由で にアクセスします。クライアントは、Transport Layer Security (TLS) 1.2 以降をサポートする必要があります。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、 ではリソースベースのアクセスポリシー AWS Direct Connect がサポートされており、ソース IP アドレスに基づく制限を含めることができます。 AWS Direct Connect ポリシーを使用して、特定の Amazon

Virtual Private Cloud (Amazon VPC) エンドポイントまたは特定の VPCs からのアクセスを制御することもできます。これにより、実質的にネットワーク内の特定の VPC からのみ、特定の AWS Direct Connect リソースへの AWS 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 BGP ハイジャックからネットワークを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どのように役立つか」を参照してください。

CLI AWS Direct Connect を使用する

を使用して AWS CLI 、 AWS Direct Connect リソースを作成および操作できます。

次の例では、 AWS CLI コマンドを使用して AWS Direct Connect 接続を作成します。また、Letter of Authorization and Connecting Facility Assignment (LOA-CFA) をダウンロードしたり、プライベートまたはパブリック仮想インターフェイスをプロビジョニングしたりすることもできます。

開始する前に、 AWS CLIがインストールされ、設定されていることを確認します。詳細については、「AWS Command Line Interface ユーザーガイド」を参照してください。

目次

ステップ 1: 接続を作成する

最初のステップでは、接続リクエストを送信します。必要なポート速度と AWS Direct Connect 場所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 AWS Direct Connect の場所を記述します。返される出力で、接続を確立するロケーションの ロケーションコードを書き留めます。

```
aws directconnect describe-locations
```

```
{
    "locations": [
        {
            "locationName": "City 1, United States",
            "locationCode": "Example Location 1"
        },
        {
            "locationName": "City 2, United States",
            "locationCode": "Example location"
```

```
        }
    ]
}
```

2. 接続を作成し、名前、ポート速度、およびロケーションコードを指定します。返される出力で、接続 ID を書き留めます。次のステップで LOA-CFA を取得するには、この ID が必要になります。

```
aws directconnect create-connection --location Example location --bandwidth 1Gbps
 --connection-name "Connection to AWS"
```

```
{
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-EXAMPLE",
    "connectionState": "requested",
    "bandwidth": "1Gbps",
    "location": "Example location",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

ステップ 2: LOA-CFA をダウンロードする

接続をリクエストした後、describe-loa コマンドを使用して LOA-CFA を取得できます。出力は base64 でエンコードされます。関連する LOA コンテンツを抽出し、デコードして、PDF ファイルを作成する必要があります。

Linux または macOS を使用して LOA-CFA を取得するには

この例では、コマンドの最後の部分で base64 ユーティリティを使用してコンテンツをデコードし、出力を PDF ファイルに送信します。

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

Windows を使用して LOA-CFA を取得するには

この例では、出力は myLoaCfa.base64 というファイルに解凍されます。2 番目のコマンドでは、certutil ユーティリティを使用してファイルをデコードし、PDF ファイルに出力を送信します。

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

LOA-CFA をダウンロードした後、ネットワークプロバイダーまたはコロケーションプロバイダーに送信します。

ステップ 3: 仮想インターフェイスを作成し、ルーター設定を取得する

AWS Direct Connect 接続を注文したら、仮想インターフェイスを作成して使用を開始する必要があります。プライベート仮想インターフェイスを作成して、VPC に接続することができます。または、パブリック仮想インターフェイスを作成して、VPC にない AWS サービスに接続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。

を使用して仮想インターフェイスを作成すると AWS CLI、出力には一般的なルーター設定情報が含まれます。デバイス固有のルーター設定を作成するには、 AWS Direct Connect コンソールを使用します。詳細については、「 ルーター設定ファイルをダウンロードする」を参照してください。

プライベート仮想インターフェイスを作成するには

1. VPC にアタッチされた仮想プライベートゲートウェイの ID (vgw-xxxxxxxx) を取得します。次のステップで仮想インターフェイスを作成するために、この ID が必要になります。

   ```
   aws ec2 describe-vpn-gateways
   ```

   ```
   {
       "VpnGateways": [
           {
               "State": "available",
               "Tags": [
                   {
                       "Value": "DX_VGW",
                       "Key": "Name"
   ```

```
                }
            ],
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-ebaa27db",
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-24f33d4d"
                }
            ]
        }
    ]
}
```

2. プライベート仮想インターフェイスを作成します。名前、VLAN ID、および BGP 自律システム番号 (ASN) を指定する必要があります。

   IPv4 トラフィックの場合、BGP ピアリングセッションの両側にプライベート IPv4 アドレスが必要です。独自の IPv4 アドレスを指定するか、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 AWS Direct Connect API コールのログ記録 AWS CloudTrail

AWS Direct Connect は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています AWS Direct Connect。CloudTrail は、 AWS Direct Connect のすべての API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、 AWS Direct Connect コンソールからの呼び出しと AWS Direct Connect API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、 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 AWS Direct Connect。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 によって収集された情報を使用して、リクエストの実行元の IP アドレス AWS Direct Connect、リクエストの実行者、リクエストの実行日時などの詳細を確認できます。

詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

AWS Direct Connect CloudTrail の情報

CloudTrail は、 AWS アカウントの作成時にアカウントで有効になります。でアクティビティが発生すると AWS Direct Connect、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。最近のイベントは、 AWS アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrailイベント履歴でのイベントの表示」を参照してください。

のイベントなど、 AWS アカウントのイベントの継続的な記録については AWS Direct Connect、証跡を作成します。追跡により、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、証跡はすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントを口グに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように、他の AWS サービスを設定できます。詳細については、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 AWS Direct Connect アクションは CloudTrail によってログに記録され、 AWS Direct Connect API リファレンスに記載されています。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認証情報または AWS Identity and Access Management (IAM ユーザー) 認証情報のどちらを使用して行われたか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、CloudTrail `userIdentity` 要素を参照してください。

AWS Direct Connect ログファイルエントリを理解する

「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 呼び出し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、 の CloudTrail ログレコードの例です AWS Direct Connect。

Example 例: CreateConnection

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
```

```
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:28:16Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "location": "EqSE2",
            "connectionName": "MyExampleConnection",
            "bandwidth": "1Gbps"
        },
        "responseElements": {
            "location": "EqSE2",
            "region": "us-west-2",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-fhajolyy",
            "connectionName": "MyExampleConnection"
        }
    },
    ...
  ]
}
```

Example 例: CreatePrivateVirtualInterface

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
```

```
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
                "customerAddress": "[PROTECTED]",
                "authKey": "[PROTECTED]",
                "asn": -1,
                "virtualGatewayId": "vgw-bb09d4a5",
                "amazonAddress": "[PROTECTED]",
                "vlan": 123
            }
        },
        "responseElements": {
            "virtualInterfaceId": "dxvif-fgq61m6w",
            "authKey": "[PROTECTED]",
            "virtualGatewayId": "vgw-bb09d4a5",
            "customerRouterConfig": "[PROTECTED]",
            "virtualInterfaceType": "private",
            "asn": -1,
            "routeFilterPrefixes": [],
            "virtualInterfaceName": "MyVirtualInterface",
            "virtualInterfaceState": "pending",
            "customerAddress": "[PROTECTED]",
            "vlan": 123,
            "ownerAccount": "123456789012",
```

```
            "amazonAddress": "[PROTECTED]",
            "connectionId": "dxcon-fhajolyy",
            "location": "EqSE2"
        }
    },
    ...
  ]
}
```

Example 例: DescribeConnections

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:27:28Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeConnections",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": null,
        "responseElements": null
    },
    ...
  ]
}
```

Example 例: DescribeVirtualInterfaces

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:37:53Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeVirtualInterfaces",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy"
        },
        "responseElements": null
    },
    ...
  ]
}
```

AWS Direct Connect リソースのモニタリング

モニタリングは、Direct Connect リソースの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、 AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。ただし、Direct Connect のモニタリングを開始する前に、以下の質問に対する回答を反映したモニタリング計画を作成する必要があります。

- どのような目的でモニタリングしますか?
- どのようなリソースをモニタリングする必要がありますか?
- これらのリソースをモニタリングする頻度は?
- 使用できるモニタリングツールは?
- 誰がモニタリングタスクを実行しますか?
- 問題が発生したときに誰が通知を受け取りますか?

次のステップでは、さまざまなタイミングと負荷条件でパフォーマンスを測定することにより、お客様の環境で通常の Direct Connect パフォーマンスのベースラインを確定します。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 には、 AWS Direct Connect 接続のモニタリングに使用できるさまざまなツールが用意されています。これらのツールの一部はモニタリングを行うように設定できますが、一部のツールは手動による介入が必要です。モニタリングタスクをできるだけ自動化することをお勧めします。

自動モニタリングツール

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 – アカウント間でログファイルを共有し、CloudWatch Logs に送信して CloudWatch CloudTrail ログファイルをリアルタイムでモニタリングします。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

AWS Direct Connect 接続をモニタリングするもう 1 つの重要な点は、CloudWatch アラームでカバーされていない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。

- AWS Direct Connect コンソールには以下が表示されます。
  - 接続のステータス ([State] 列を参照)
  - 仮想インターフェイスのステータス ([State] 列を参照)
- CloudWatch 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。

- すべての AWS リソースメトリクスを検索して参照します。
- 問題があることを通知するアラームを作成および編集する。

Amazon CloudWatch で を監視する

CloudWatch を使用して、物理 AWS Direct Connect 接続と仮想インターフェイスをモニタリングできます。CloudWatch 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。

内容

- AWS Direct Connect メトリクスとディメンション
- View AWS Direct Connect CloudWatch メトリクス
- AWS Direct Connect 接続をモニタリングする Amazon CloudWatch アラームを作成する

AWS Direct Connect メトリクスとディメンション

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

AWS Direct Connect 接続メトリクス

以下のメトリクスは、Direct Connect 専用接続から入手できます。

メトリクス	説明
`ConnectionState`	接続の状態。1 はアップ、0 はダウンを示します。 このメトリクスは、専用接続とホスト接続で使用できます。

メトリクス	説明
	Note このメトリクスは、接続所有者アカウントに加えて、ホストされている仮想インターフェイス所有者アカウントでも使用できます。 単位: このメトリクスに対して返される単位はありません。
ConnectionBpsEgress	接続の AWS 側からのアウトバウンド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 側へのインバウンド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 側からのアウトバウンド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 側へのインバウンド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 側からのアウトバウンド (送信) トラフィックのファイバー接続の状態を示します。 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 側へのインバウンド (進入) トラフィックのファイバー接続の状態を示します。 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。

AWS Direct Connect 仮想インターフェイスメトリクス

AWS Direct Connect 仮想インターフェイスでは、次のメトリクスを使用できます。

メトリクス	説明
VirtualInterfaceBpsEgress	仮想インターフェイスの AWS 側からのアウトバウンド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 側へのインバウンド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 側からのアウトバウンド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 側へのインバウンドデータのパケットレート。 報告される数値は、指定した時間長 (デフォルトは 5 分) にわたる集計 (平均) です。 単位: パケット/秒

AWS Direct Connect 使用可能なディメンション

次のディメンションを使用して AWS Direct Connect データをフィルタリングできます。

ディメンション	説明
ConnectionId	このディメンションは、Direct Connect 接続と仮想インターフェイスのメトリクスで使用できます。このディメンションでは、接続でデータをフィルターします。
OpticalLaneNumber	このディメンションでは、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

View AWS Direct Connect CloudWatch メトリクス

AWS Direct Connect は、Direct Connect 接続に関する次のメトリクスを送信します。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、1 分間隔でメトリクスを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。CloudWatch は間隔を制御するため、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。計算関数や事前構築クエリの追加を含めた、Amazon CloudWatch を使用して Direct Connect メトリクスを表示するための詳細については、「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。

AWS Direct Connect コンソールを使用してメトリクスを表示するには

1. AWS Direct Connect コンソール (https://console.aws.amazon.com/directconnect/v2/home) を開きます。
2. ナビゲーションペインで [Connections (接続)] を選択します。
3. 接続を選択します。
4. [モニタリング] タブを接続して、接続のメトリクスを表示します。

を使用してメトリクスを表示するには AWS CLI

コマンドプロンプトで、次のコマンドを使用します。

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```

AWS Direct Connect 接続をモニタリングする Amazon CloudWatch アラームを作成する

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、 AWS Direct Connect 接続の状態を監視するアラームを作成できます。接続状態が 5 回連続して 1 分間ダウンとなったときに、通知を送信します。アラームを作成するために知っておくべきことと、アラームを作成するための詳細については、「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 (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで、[Alarms] (アラーム) を選択し、[All alarms] (アラームの作成) を選択します。
3. アラームの作成(アラームの作成) を選択します。
4. [Select metric] (メトリクスの選択)、DX の順に選択します。
5. [Connection Metrics] (接続メトリクス) メトリクスを選択します。
6. AWS Direct Connect 接続を選択し、メトリクスの選択メトリクスを選択します。
7. [Specify metric and conditions] (メトリクスと条件の指定) ページで、アラームのパラメータを設定します。メトリクスや条件を指定するための詳細については、「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. [Next (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を設定するための詳細については、「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. [Next (次へ)] を選択します。
11. [Add name and description] (名前と説明を追加) ページで、[Name] (名前) とオプションの [Alarm description] (アラームの説明) を入力してこのアラームについて説明し、[Next] (次へ) をクリックします。
12. 提案されているアラームについて [Preview and create] (プレビューと作成) ページで確認します。
13. 必要に応じて、[Edit] (編集) をクリックして情報を変更し、[Create alarm] (アラームの作成) を選択します。

    [Alarms] (アラーム) ページに、新しいアラームに関する情報が記載された新しい行が表示されます。[Actions] (アクション) ステータスには、[Actions enabled] (有効済みのアクション) と表示されアラームがアクティブであることを示します。

AWS Direct Connect クォータ

次の表に、関連するクォータを示します AWS Direct Connect。

コンポーネント	クォータ	コメント
AWS Direct Connect 専用接続あたりのプライベートまたはパブリック仮想インターフェイス	50	この制限を増やすことはできません。
AWS Direct Connect 専用接続あたりのトランジット仮想インターフェイス。 トランジット仮想インターフェイスは、トランジットゲートウェイまたは AWS クラウド WAN コアネットワークに接続するために使用できます。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。
AWS Direct Connect 専用接続あたりのプライベート仮想インターフェイスまたはパブリック仮想インターフェイス、 AWS Direct Connect 専用接続あたりのトランジット仮想インターフェイス	51	Amazon VPC Transit Gateway AWS Direct Connect のサポートが開始されると、専用接続ごとに 50 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 (1) のトランジット仮想インターフェイスのクォータが追加されました。現在許可されているトランジット仮想インターフェイスの数は 4 つで、専用接続あたりの仮想インターフェイスの最大数は 51 個です。この制限を増やすことはできません。
AWS Direct Connect ホスト接続あたりのプライベート、パブリック、またはトランジット仮想インターフェイス	1	この制限を増やすことはできません。

コンポーネント	クォータ	コメント
Direct Connect ロケーション、リージョン、アカウントあたりのアクティブな AWS Direct Connect 接続数	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。
Link Aggregation Group (LAG) あたりの仮想インターフェイスの数	51	Amazon VPC Transit Gateway AWS Direct Connect のサポートが開始されると、1 つの (1) トランジット仮想インターフェイスのクォータが、LAG あたり 50 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追加されました。現在許可されているトランジット仮想インターフェイスの数は 4 つで、LAG あたりの仮想インターフェイスの最大数は 51 個です。この制限を増やすことはできません。
オンプレミスから へのプライベート仮想インターフェイスまたはトランジット仮想インターフェイス上のボーダーゲートウェイプロトコル (BGP) セッションあたりのルート AWS。 BGP セッションで IPv4 と IPv6 にそれぞれ 100 を超えるルートをアドバタイズする場合、BGP セッションはアイドル状態になり BGP セッションが DOWN になります。	IPv4 と IPv6 にそれぞれ 100	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。
AWS Direct Connect アカウントあたりのゲートウェイ	200	詳細については、ソリューションアーキテクト (SA) またはテクニカルアカウントマネージャー (TAM) にお問い合わせください。
ゲートウェイあたりの仮想プライベート AWS Direct Connect ゲートウェイ	20	この制限を増やすことはできません。
ゲートウェイあたりのトランジット AWS Direct Connect ゲートウェイ	6	この制限を増やすことはできません。

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 Direct Connect ゲートウェイアタッチメントからオンプレミスへのアドバタイズされた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すべてのトランジット仮想インターフェイスは、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。
AWS Direct Connect ゲートウェイあたりの仮想インターフェイス (プライベートまたはトランジット)	30	この制限を増やすことはできません。
トランジット仮想インターフェイスでの AWS Transit Gateway からオンプレミス AWS への あたりのプレフィックスの数	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。

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

BGP クォータ

以下は、BGP クォータです。BGP タイマーは、ルーター間で最小値までネゴシエートします。BFD インターバルは、最も遅いデバイスによって定義されます。

- デフォルトのホールドタイマー: 90 秒
- 最小ホールドタイマー: 3 秒

  ホールド値 0 はサポートされていません。
- デフォルトのキープアライブタイマー: 30 秒
- 最小キープアライブタイマー: 1 秒
- グレースフルリスタートタイマー: 120 秒

  グレースフルリスタートと BFD を同時に設定しないことを推奨いたします。
- BFD 活性検出の最小間隔: 300 ミリ秒
- BFD 最小乗数: 3

負荷分散に関する考慮事項

複数のパブリック VIF で負荷分散を使用する場合は、すべての VIF が同じリージョンにある必要があります。

トラブルシューティング AWS Direct Connect

以下のトラブルシューティング情報は、 AWS Direct Connect 接続に関する問題を診断して修正するために役立ちます。

目次

レイヤー 1 (物理層) 問題のトラブルシューティング

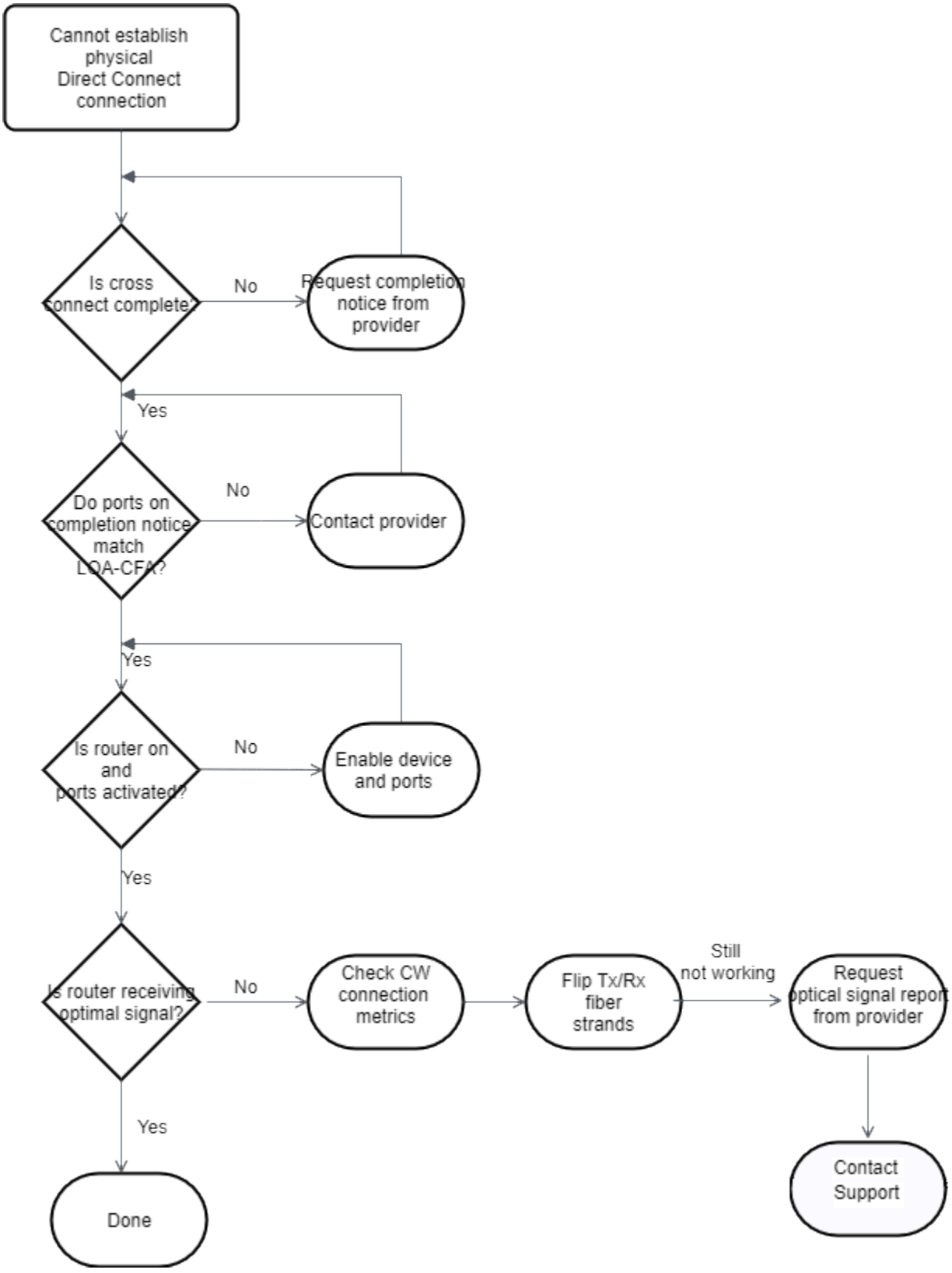
お客様またはお客様のネットワークプロバイダーが AWS Direct Connect デバイスへの物理的な接続を確立できない場合は、次の手順を使用して問題のトラブルシューティングを行います。

1. クロスコネクトが完了したことをコロケーションプロバイダに確認します。コロケーションプロバイダまたはネットワークプロバイダにクロスコネクトの完了通知の提供を依頼し、LOA-CFA に記載されているものとポートを比較します。
2. ルーターまたはプロバイダのルーターの電源が入っていて、ポートがアクティブ化されていることを確認します。
3. ルーターが正しい光トランシーバを使用していることを確認します。ポート速度が 1 Gbps を超える接続では、ポートのオートネゴシエーションを無効にする必要があります。ただし、接続を提供する AWS Direct Connect エンドポイントによっては、1 Gbps 接続に対して自動ネゴシエーションを有効または無効にする必要がある場合があります。接続で自動ネゴシエーションを無効にする必要がある場合は、ポート速度と全二重モードを手動で設定する必要があります。仮想インターフェイスがダウンしたままの場合は、レイヤー 2 (データリンク層) 問題のトラブルシューティング を参照してください。接続が終了する Direct Connect エンドポイントによっては、それに応じて自動ネゴシエーションを有効または無効にする必要がある場合があります。
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. Amazon CloudWatch メトリクスを確認します AWS Direct Connect。 AWS Direct Connect デバイスの Tx/Rx 光学読み取り値 (1 Gbps と 10 Gbps の両方) 、物理エラー数、運用ステータスを確

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。

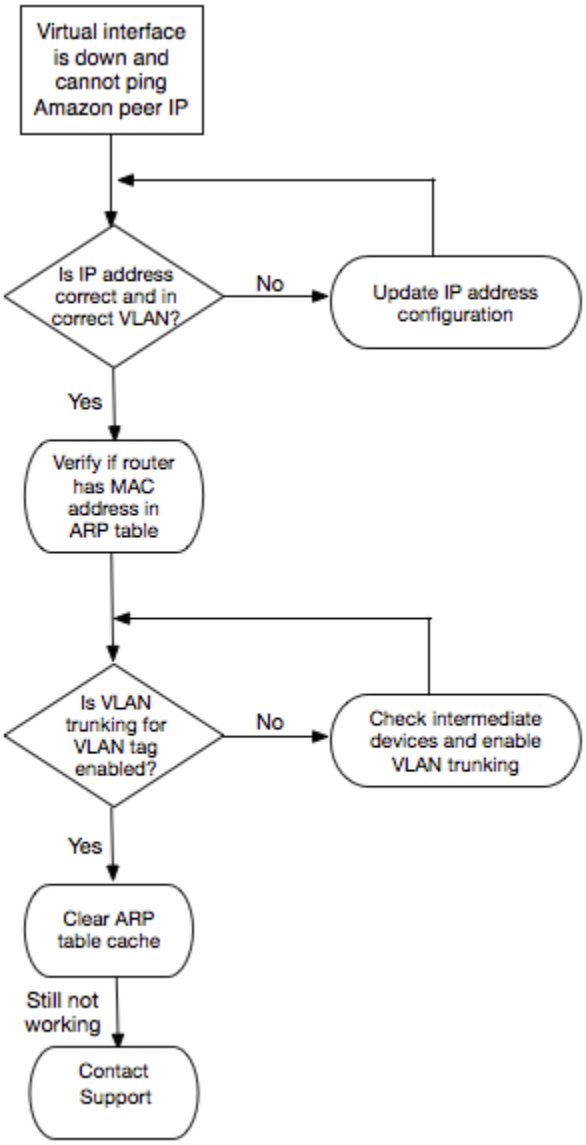

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check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

AWS Direct Connect 物理接続が稼働しているが仮想インターフェイスがダウンしている場合は、次の手順を使用して問題をトラブルシューティングします。

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. ルーターにアドレス解決プロトコル (ARP) テーブルの AWS エンドポイントからの MAC アドレスエントリがあるかどうかを確認します。
3. エンドポイント間の中間デバイスで、802.1 Q VLAN タグに対して VLAN トランキングが有効になっていることを確認します。がタグ付けされたトラフィック AWS を受信するまで、ARP を AWS 側で確立することはできません。
4. お客様またはプロバイダの ARP テーブルキャッシュをクリアします。
5. 上記の手順で ARP が確立されていない場合、または Amazon ピア IP に ping を実行できない場合は、 AWS サポートにお問い合わせください。

次のフローチャートには、データリンクに関する接続の問題を診断するためのステップが含まれています。



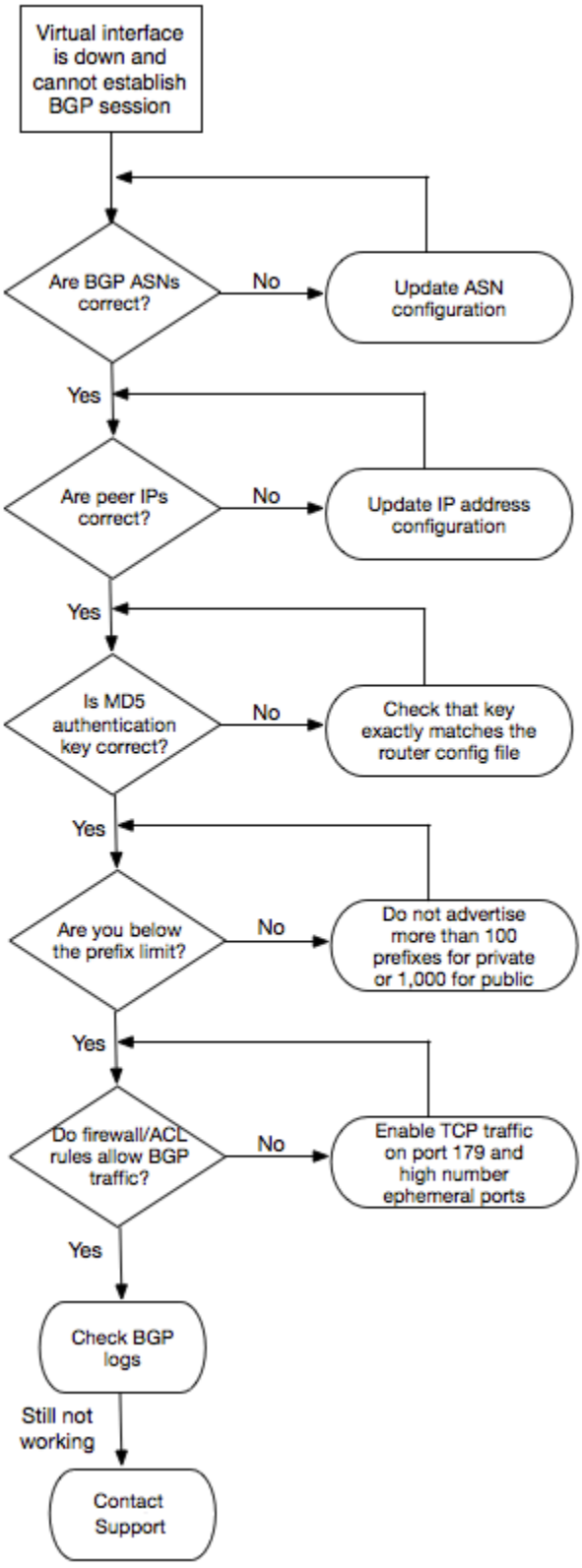
これらのステップの確認後に BGP セッションがまだ確立されない場合は、「レイヤー 3/4 (ネットワーク層/トランスポート層) 問題のトラブルシューティング」を参照してください。BGP セッションが確立されたが、まだルーティングの問題が発生している場合は、「ルーティング問題のトラブルシューティング」を参照してください。

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

AWS Direct Connect 物理接続が稼働していて、Amazon ピア IP アドレスに ping を送信できる状況を考えてみましょう。仮想インターフェイスが稼働していて、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. 上記のステップで BGP ピアリングセッションが確立されない場合は、AWS サポートにお問い合わせください。

次のフローチャートには、BGP のピア接続セッションの問題を診断するためのステップが含まれています。



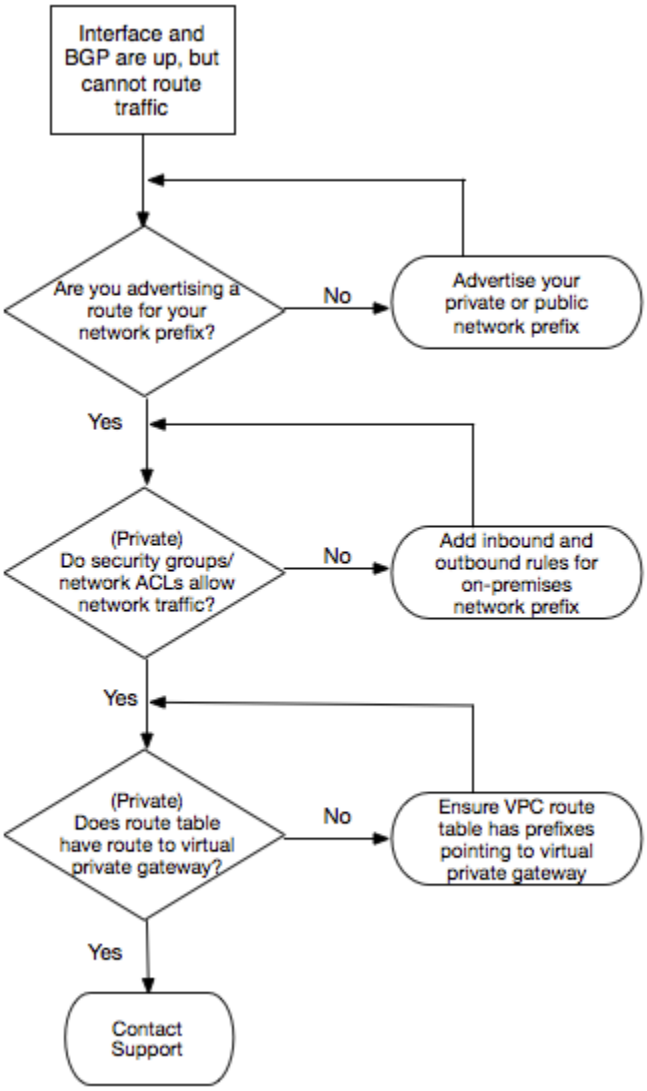
BGP ピア接続セッションが確立されたが、まだルーティングの問題が発生している場合は、「ルーティング問題のトラブルシューティング」を参照してください。

ルーティング問題のトラブルシューティング

仮想インターフェイスが稼動していて、BGP ピアリングセッションを確立している状況を考えてみましょう。仮想インターフェイス上でトラフィックをルーティングできない場合は、次の手順を実行して問題のトラブルシューティングを行います。

1. BGP セッションを介して、オンプレミスネットワークのプレフィックスのルートをアドバタイズしていることを確認します。プライベート仮想インターフェイスの場合、これはプライベートネットワークプレフィックスまたはパブリックネットワークプレフィックスとすることができます。パブリック仮想インターフェイスの場合、これはパブリックにルーティング可能なプレフィックスとする必要があります。
2. プライベート仮想インターフェイスの場合は、VPC セキュリティグループとネットワーク ACL で、オンプレミスネットワークプレフィックスに対してインバウンドトラフィックおよびアウトバウンドトラフィックを許可していることを確認します。詳細については、Amazon VPC ユーザーガイドの「セキュリティグループ」および「ネットワーク ACL」を参照してください。
3. プライベート仮想インターフェイスの場合、VPC ルートテーブルに、プライベート仮想ゲートウェイの接続先となる仮想プライベートゲートウェイを指すプレフィックスがあることを確認します。たとえば、デフォルトでオンプレミスネットワークにすべてのトラフィックをルーティングする場合は、デフォルトルート (0.0.0.0/0 または ::/0) と仮想プライベートゲートウェイを VPC ルートテーブルでターゲットとして追加できます。
   - または、ルート伝達で動的な BGP ルートアドバタイズに基づいて、ルートテーブルで自動的にルートを更新するようにできます。ルートテーブルあたり最大 100 の伝播されたルートを持つことができます。この制限を増やすことはできません。詳細については、Amazon VPC ユーザーガイドの「ルート伝達の有効化と無効化」を参照してください。
4. 上記の手順でルーティングの問題を解決できない場合は、 AWS サポートにお問い合わせください。

次のフローチャートには、ルーティングの問題を診断するためのステップが含まれています。


Interface and BGP are up, but cannot route traffic
Are you advertising a route for your network prefix?
No
Advertise your private or public network prefix
Yes
(Private) Do security groups/ network ACLs allow network traffic?
No
Add inbound and outbound rules for on-premises network prefix
Yes
(Private) Does route table have route to virtual private gateway?
No
Ensure VPC route table has prefixes pointing to virtual private gateway
Yes
Contact Support

ドキュメント履歴

次の表に、 のリリースを示します AWS Direct Connect。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
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 ゲートウェイの関連付けを Direct Connect と AWS Cloud WAN コアネットワークとの間で直接作成できるようになりました。	2024 年 11 月 25 日
400G のサポート	400G 接続のサポートを含むようにトピックを更新しました。	2024 年 7 月 18 日
SiteLink プレフィックスの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 プレゼンスポイント (PoPs) 間の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 AWS Direct Connect 接続を使用して、企業のデータセンターから AWS Direct Connect ロケーションにデータを暗号化できます。	2021 年 3 月 31 日

100G のサポート	100G の専用接続のサポートについて説明するためにトピックを更新しました。	2021 年 2 月 12 日
イタリアの新しいロケーション	イタリアの新しいロケーションの追加について、トピックを更新しました。	2021 年 1 月 22 日
イスラエルの新しい場所	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 フェイルオーバーテストのサポート	障害耐性ツールキットのフェイルオーバーテスト機能を使用して、接続の障害耐性をテストします。	2020 年 6 月 3 日
CloudWatch VIF メトリクスのサポート	CloudWatch を使用して、物理 AWS Direct Connect 接続と仮想インターフェイスをモニタリングできます。	2020 年 5 月 11 日
AWS Direct Connect レジリエンシーツールキット	AWS Direct Connect Resiliency Toolkit は、SLA 目標を達成するために専用接続を注文するの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 AWS Transit Gateway 間の のサポートの追加リージョンサポート	アカウント AWS Transit Gateway 間の の追加リージョンサポート。	2019 年 9 月 30 日

AWS Direct Connect のサポート AWS Transit Gateway	AWS Direct Connect ゲートウェイを使用して、トランジット仮想インターフェイス経由で AWS Direct Connect トランジットゲートウェイにアタッチされた VPCs VPNs 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 AWS Direct Connect への接続用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	ジャンボフレーム (9001 MTU) は送信できます AWS Direct Connect。	2018 年 10 月 11 日
ローカル設定 BGP コミュニティ	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
AWS Direct Connect ゲートウェイ	Direct Connect ゲートウェイを使用して、リモートリージョンVPCs AWS Direct Connect に接続できます。	2017 年 11 月 1 日
Amazon CloudWatch メトリクス	AWS Direct Connect 接続の CloudWatch メトリクスを表示できます。	2017 年 6 月 29 日

リンク集約グループ	リンク集約グループ (LAG) を作成して、複数の AWS Direct Connect 接続を集約できます。	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	AWS Direct Connect リソースにタグを付けることが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	AWS Direct Connect コンソールまたは API を使用して、認可書と接続施設割り当て (LOA-CFA) をダウンロードできます。	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

ポートランド、オレゴン、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
ブラジル、サンパウロ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) 、ムンバイ (アジアパシフィック (シンガポール) リージョン) の新しいロケーションの追加を含む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ロケーション	米国西部 (オレゴン) リージョンの新しい AWS Direct Connect ラスベガスロケーションの追加を含むように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	欧州 (フランクフルト) リージョンにサービスを提供する新しい AWS Direct Connect ロケーションの追加を含むように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 AWS Direct Connect ロケーションの追加を含むようにトピックを更新しました。	2014 年 7 月 14 日
のサポート AWS CloudTrail	のアクティビティをログに記録するために CloudTrail を使用する方法について説明する新しいトピックを追加しました AWS Direct Connect	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	欧州 (アイルランド) リージョンにサービスを提供する新しい AWS Direct Connect ロケーションの追加を含むように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ロケーション	米国西部 (オレゴン) リージョンにサービスを提供するシアトルの新しい AWS Direct Connect ロケーションの追加を含むように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 AWS Direct Connect	AWS Identity and Access Management での の使用に関するトピックを追加しました AWS Direct Connect。	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新しい AWS Direct Connect ロケーションの追加を含むように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、米国東部 (バージニア北部) および南米 (サンパウロ) リージョン	入 AWS Direct Connect 門ガイドを AWS Direct Connect ユーザーガイドに置き換えました。新しい AWS Direct Connect コンソールをカバーする新しいトピックを追加し、請求トピックを追加し、ルーター設定情報を追加し、米国東部 (バージニア北部) および南米 (サンパウロ) リージョンにサービスを提供する 2 つの新しい AWS Direct Connect ロケーションの追加を含むトピックを更新しました。	2012 年 8 月 13 日

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) リージョンのサポート	新しいトラブルシューティングセクションを追加し、トピックを更新して、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) 、アジアパシフィック (東京) の各リージョンに 4 つの新しい AWS Direct Connect ロケーションを追加しました。	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	の最初のリリース AWS Direct Connect。	2011 年 8 月 3 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。