Cisco Catalyst SD-WAN Cloud Interconnect with Equinix

簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 *1* : 機能の履歴

機能名	リリース情報	説明
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	Cisco Cloud Services Router 1000v（Cisco CSR 1000v）インスタンスを Equinix ファブリックのインターコネクト ゲートウェイとして展開し、Cisco Catalyst SD-WAN ブランチの場所をインターコネクト ゲートウェイに接続することができます。インターコネクト ゲートウェイから、AWS Cloud OnRamp または Equinix ファブリック内の別のインターコネクト ゲートウェイへのソフトウェア定義型インターコネクトを作成することができます。

機能名	リリース情報	説明
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix：Google Cloud および Microsoft Azure	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	Google Cloud VPC、Microsoft Azure VNet または Virtual WAN へのソフトウェア定義型インターコネクトを作成し、Equinix ファブリックを介してブランチの場所をクラウドリソースにリンクすることができます。Equinix ファブリックのインターコネクト ゲートウェイからデバイスリンクを作成、更新、および削除することもできます。
Equinix との暗号化されたマルチクラウド インターコネクト	Cisco vManage リリース 20.9.1	Cisco Catalyst SD-WAN ファブリックを、Equinix のインターコネクト ゲートウェイから AWS、Google Cloud、および Microsoft Azure クラウド サービス プロバイダーに拡張できます。Cisco SD-WAN Manager の Cloud OnRamp ワークフローを使用して、インターコネクト ゲートウェイとクラウド サービス プロバイダー間のセキュアなプライベート Cisco Catalyst SD-WAN 接続をプロビジョニングすることができます。
Cisco Catalyst 8000V Edge ソフトウェアのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	Cisco Catalyst 8000v Edge ソフトウェアを Equinix ファブリックのインターコネクト ゲートウェイとして展開し、Cisco Catalyst SD-WAN ブランチの場所をインターコネクト ゲートウェイに接続することができます。
SDCI 接続への VPC および VNet タグの追加	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	SDCI 接続に関連付けられている VPC および VNet タグと、その他のプロパティを変更できます

機能名	リリース情報	説明
Equinix での監査の管理	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	監査管理は、インターコネクトクラウドとプロバイダーの状態が、Cisco Catalyst SD-WAN Manager の状態と同期しているかどうかを把握するために役立ちます。監査プロセスには、プロバイダーリソース、インターコネクトゲートウェイ、およびクラウドへの接続のスキャンが含まれています。詳細については、「Audit Management」を参照してください。

- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の前提条件 （3 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の制約事項 （4 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix に関する情報 （10 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の設定ワークフロー （14 ページ）
- Cisco SD-WAN Cloud Interconnect with Equinix の前提条件の設定 （16 ページ）
- AWS へのインターコネクトの作成 （24 ページ）
- Google Cloud へのインターコネクトの作成 （35 ページ）
- Microsoft Azure へのインターコネクトの作成 （45 ページ）
- デバイスリンク （64 ページ）
- インターコネクト ゲートウェイ間のインターコネクトの作成 （66 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の設定の確認と変更 （68 ページ）
- 監査管理 （74 ページ）
- Cisco Catalyst SD-WAN Cloud Interconnect with Equinix のトラブルシューティング （76 ページ）

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の前提条件

1. Equinix ポータルでアカウントを作成します。Equinix の「New User Equinix Fabric Portal Access」のドキュメントを参照してください。

   アカウントを作成したら、アカウントのクライアント ID（コンシューマキー）とクライアント シークレット キー（コンシューマシークレット）を生成します。Equinix Developer Platform Knowledge Center の「Generating Client ID and Client Secret Key」のドキュメントを参照してください。

このアカウントを使用してインターコネクト ゲートウェイを展開する各リージョンの請求アカウントを作成します。Equinix の「Billing Account Management」のドキュメントを参照してください。

2. インターコネクト ゲートウェイとクラウドプロバイダー間のパブリック ピアリングを必要とする接続の場合は、パブリック BGP ピアリング IP アドレスを指定します。接続を作成する前に、パブリック IP アドレスの使用が組織で許可されていることを確認してください。または、Equinix ポータルから BGP ピアリングのパブリック IP アドレスを割り当てることもできます。

3. インターコネクト ゲートウェイとして展開する Cisco CSR 1000v インスタンスの UUID が必要な数あることを確認します。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを展開できます。

4. Cisco SD-WAN Manager がインターネットに接続できることを確認します。

   設定ワークフローの一環として、Cisco SD-WAN Manager はインターネットを介して Equinix ポータルに接続します。

5. Cisco SD-WAN Manager が Equinix と対話できるようにするために、Cisco SD-WAN Manager 証明書がルート CA として Cisco（自動）PKI または Symantec によって署名されている必要があります。Cisco（自動）PKI 証明書の使用を推奨します。エンタープライズ CA 証明書は、Cisco vManage リリース 20.9.1 以降でサポートされています。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の制約事項

一般

- Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、接続を作成および編集できます。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 より前では、接続は編集できません。接続を削除し、必要な設定を使用して新しい接続を作成することができます。

- 同じ場所のインターコネクト ゲートウェイを同時に作成または削除することはできません。

- すべてのインターコネクトとクラウドの操作には時間制限があります。操作がタイムアウトした場合は、Cisco SD-WAN Manager が失敗を報告します。現在、このタイムアウト値は設定できません。

- グローバル設定を変更すると、変更後に作成された新しいゲートウェイまたは接続に変更が適用されます。変更前に作成されたゲートウェイまたは接続には、変更は影響しません。

- Cisco Catalyst SD-WAN Manager リリース 20.12.1 より前の Cisco SD-WAN Manager を介して、Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 で Equinix インターコネクト ゲートウェイを展開していた場合は、Cisco SD-WAN Manager を Cisco Catalyst SD-WAN Manager リリース 20.12.1 にアップグレードする前に、Equinix インターコネクト ゲートウェイを Cisco IOS XE Catalyst SD-WAN リリース 17.9.x にアップグレードする必要があります。
- Cisco vManage リリース 20.6.1 を使用して Equinix の場所にインターコネクト ゲートウェイを作成した後に、Cisco SD-WAN Manager ソフトウェアを新しいリリースにアップグレードすると、インターコネクト ゲートウェイのポート 443 が無効になります。この制限事項に対応するには、次のいずれかを実行します。
  - ポート 443 を手動で有効にします。
  - Cisco SD-WAN Manager ソフトウェアのアップグレード後に、既存のインターコネクト ゲートウェイを削除し、新しいインターコネクト ゲートウェイを作成します。
- Cisco Catalyst SD-WAN Manager リリース 20.12.2 以降では、マルチクラウドワークフローの一環として作成されたトランジットゲートウェイは、SDCI ワークフローのトランジット接続の下にリストされません。
- Cisco vManage リリース 20.9.5 以降では、Equinix ファブリックで Cisco Catalyst 8000v Edge ソフトウェアをインターコネクト ゲートウェイとして展開できます。

AWS へのインターコネクト

- AWS クラウドリソースへの接続を作成する際は、AWS のクォータと制限に注意してください。Cisco SD-WAN Manager は、すべての AWS のクォータと制限を適用するわけではありません。
- 異なる AWS アカウントに属するクラウドリソースを、単一の接続の一部として使用することはできません。
- Equinix は、ホスト型接続を介したパブリック、プライベート、およびトランジット VIF のみをサポートしています。ホスト型 VIF はサポートされていません。
- プライベート VIF またはトランジット VIF を Direct Connect ゲートウェイにアタッチします。プライベート VIF とトランジット VIF の組み合わせを、同じ Direct Connect ゲートウェイにアタッチすることはできません。
- Cisco vManage リリース 20.9.2 および Cisco vManage リリース 20.10.1 以降では、AWS リージョンのトランジットホスト型接続で、1 つのトランジットゲートウェイのみを Direct Connect ゲートウェイに関連付けることができます。

  Cisco vManage リリース 20.9.1 以前のリリースでは、AWS リージョンの Direct Connect ゲートウェイに、1 つのトランジットゲートウェイのみを関連付けることを推奨します。
- インターコネクト トランジット接続の編集時に、同じリージョン内の VPC タグのない新しいトランジットゲートウェイが選択された場合、接続の更新は破棄されます。
- 特定の VPC へのすべての接続は、以下を満たしている必要があります

- 同じ Direct Connect ゲートウェイとピアリングしている
- 同じトランジットゲートウェイまたは仮想プライベートゲートウェイのアタッチメントがある

- トランジット VIF の場合、トランジットゲートウェイと Direct Connect ゲートウェイは、異なる BGP ASN を使用する必要があります。
- ホスト VPC タグの作成時に、AWS マルチクラウドワークフローまたはインターコネクト接続ワークフローのいずれかを使用して、タグを使用することを選択します。この選択は、タグの作成後は変更できず、タグが削除されるまで維持されます。
- インターコネクト接続用に選択されたホスト VPC タグは、作成後は編集できません。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、ホスト VPC タグを作成および編集できます。

Microsoft Azure へのインターコネクト

- ホスト VNet タグの作成時に、Microsoft Azure マルチクラウドワークフローまたはインターコネクト接続ワークフローのいずれかを使用して、タグを使用することを選択します。この選択は、タグの作成後は変更できず、タグが削除されるまで維持されます。
- インターコネクト接続用に選択されたホスト VNet タグは、作成後は編集できません。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、ホスト VNet タグを作成および編集できます。
- インターコネクト ゲートウェイから Microsoft Azure ExpressRoute へのプライベートピアリング接続を作成するときは、ExpressRoute 回線と同じリソースグループに属する VNet、仮想 WAN、および仮想ハブのみを接続にアタッチできます。別のリソースグループからの VNet、仮想 WAN、および仮想ハブのアタッチは、サポートされていない設定です。

Google Cloud へのインターコネクト

- 各クラウドルータは、すべての BGP セッションに同じ ASN を使用する必要があります。

デバイスリンク

- デバイスグループ内のすべてのリンクの固定帯域幅には、50 Mbps ～ 10 Gbps の範囲を使用できます。
- 特定のメトロのすべてのリンクの累積帯域幅は、10 Gbps を超えることはできません。

暗号化されたマルチクラウド インターコネクトの制約事項

サポート対象の最小リリース：Cisco vManage リリース 20.9.1

AWS へのインターコネクト

- AWS の要件に従って、
  - クラウドゲートウェイの最小インスタンスタイプは x-large である必要があります。
  - 1 つのインターコネクト接続に最大 10 個のクラウドゲートウェイをアタッチできます。
  - 1 つのクラウドゲートウェイは、30 個のインターコネクト接続に接続できます。

Microsoft Azure へのインターコネクト

- 1 つのクラウドゲートウェイを 8 つの異なるクラウドインターコネクト接続にアタッチでき、1 つのインターコネクト接続を 5 つの異なるクラウドゲートウェイに接続できます。
- 異なるリージョンのクラウドゲートウェイに接続するには、ExpressRoute 回線が Premium タイプである必要があります。
- Microsoft Azure 展開では、クラウドゲートウェイの WAN インターフェイスで Cisco Catalyst SD-WAN トンネルの色は自動的に設定されないため、WAN インターフェイスの色を手動で更新する必要があります。テンプレートの色がブランチルータ、インターコネクトゲートウェイ、およびクラウドゲートウェイの色と一致していることを確認します。

Google Cloud へのインターコネクト

- Google Cloud ゲートウェイへのクラウドインターコネクト接続は、冗長性が有効になっている場合にのみサポートされます。
- 1 つの接続にアタッチできる Google Cloud ゲートウェイは 1 つだけです。
- 既存の Google Cloud ゲートウェイは、クラウドインターコネクトではサポートされません。
- リージョンとネットワークの組み合わせに対して、最大 5 つの Google Cloud Router を作成できます。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の使用上の注意

表 *2*: 接続設定の制限

説明	カウント
インターコネクト ゲートウェイ	
インターコネクトゲートウェイあたりの最大接続数（VXC）	20 **注**：集約 VXC 帯域幅がインターコネクト ゲートウェイの帯域幅容量を超えることはできません。

説明	カウント
AWS へのインターコネクト	
プライベート VIF の AWS への接続あたりの VPC の最大数	10
トランジット VIF の AWS への接続あたりの VPC の数	デフォルト：15 最大：15,000
トランジット VIF の AWS への接続あたりのトランジットゲートウェイの最大数	3
接続あたりの Direct Connect ゲートウェイの最大数	1
AWS Direct Connect ゲートウェイあたりの VIF（プライベートまたはトランジット）の最大数	デフォルト：30 制限はリクエストに応じて増やすことができます。
AWS Direct Connect ホスト型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 VIF の最大数	1
トランジット VIF のブランチの場所から AWS へのプレフィックスの最大数	100
トランジット VIF の AWS からブランチの場所への AWS Transit Gateway あたりのプレフィックスの最大数	20
Microsoft Azure へのインターコネクト	
ExpressRoute に接続できるインターコネクト ゲートウェイの最大数	2
ExpressRoute が接続できる VNet の最大数	10
VNet に接続できる ExpressRoute の最大数	4
仮想ハブに接続できる ExpressRoute の最大数	ピアリングの場所あたり 8
仮想 WAN ExpressRoute ゲートウェイあたりの最大総スループット	20 Gbps
仮想ハブに接続できる VNet の最大数	500 ～（仮想 WAN 内の仮想ハブの合計数）

AWS へのインターコネクト

- AWS へのプライベート VIF 接続を削除すると、Cisco SD-WAN Manager は、接続の確立中に作成された VIF、仮想プライベートゲートウェイ、およびルートテーブルを削除します。
- トランジット VIF 接続を削除すると、Cisco SD-WAN Manager は、接続の確立中に作成された Direct Connect ゲートウェイ、トランジットゲートウェイ、または仮想プライベートゲートウェイへのアタッチメントと関連付けを削除します。
- AWS への接続の作成中に、Cisco SD-WAN Manager から Direct Connect ゲートウェイまたはトランジットゲートウェイを作成した場合、接続を削除してもゲートウェイは削除されません。必要に応じて、これらの AWS リソースを管理する必要があります。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、接続の削除中に Direct Connect ゲートウェイまたはトランジットゲートウェイを削除するオプションがあります。
- 接続を作成すると、新しいルートテーブルが作成され、接続にアタッチされたホスト VPC のメインルートテーブルとして設定されます。トランジットゲートウェイへのデフォルトルートがメインルートテーブルに作成され、ルート伝達が有効になります。必要に応じてルートと伝達を編集します。

  Cisco vManage リリース 20.5.1 以降では、インターコネクトによってアクセスする必要があるスタティックルートとサブネットの関連付けを、Cisco SD-WAN Manager によって新しく作成されたメインルートテーブルに移動する必要があります。

Google Cloud へのインターコネクト

- 非冗長接続の場合は、各ネットワークリージョンに Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成する必要があります。
- 冗長接続の場合は、各ネットワークリージョンに 2 つの Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成する必要があります。
- インターコネクト アタッチメントで使用するには、Google Cloud Router の Google ASN を 16550 に設定する必要があります。

Microsoft Azure へのインターコネクト

- ExpressRoute にアタッチされた VNet への HA 接続を提供するために特定の ExpressRoute に接続できるインターコネクト ゲートウェイのペアは、1 つだけです。

  インターコネクト ゲートウェイの 2 番目のペアを同じ vNet に接続するには、別の ExpressRoute を作成し、vNet を ExpressRoute にアタッチして、インターコネクト ゲートウェイを ExpressRoute に接続します

  VNet に接続するこのような ExpressRoute を最大 4 つ用意して、各 ExpressRoute をインターコネクト ゲートウェイのペアに接続することができます。

- ExpressRoute は最大 10 個の VNet に接続できます。インターコネクト ゲートウェイから ExpressRoute への接続を作成するときに、VNet を ExpressRoute にアタッチすることができます。VNet は、接続用に選択した VNet タグに基づいてアタッチされます。

  10 個を超える VNet に適用される VNet タグを選択した場合、または選択される VNet の総数が 10 個を超えるような VNet タグの組み合わせを選択した場合、インターコネクトの作成は失敗します。

（注） インターコネクト ゲートウェイからの接続を作成するときに ExpressRoute にアタッチできる VNet の数の決定では、Azure ポータルから ExpressRoute にアタッチした可能性のある VNet も考慮されます。

- VNet は、VNet ゲートウェイまたは ExpressRoute ゲートウェイに接続できます。そのため、VNet ゲートウェイを介した VNet へのプライベートピアリングを作成した場合、ExpressRoute ゲートウェイを介した同じ VNet へのプライベートピアリングを作成することはできません。その逆も同様です。
- VNet が仮想 WAN の仮想ハブに接続されている場合、同じ VNet を別の仮想 WAN に接続することはできません。
- リージョン内のすべての VNet は、同じリージョン内の単一の仮想ハブに接続する必要があります。
- デフォルトは冗長接続であり、この設定のみがサポートされています。Equinix ファブリック内のインターコネクト ゲートウェイのペアから Microsoft Azure への接続を作成する必要があります。

  Microsoft Azure ExpressRoute へのプライマリ接続とセカンダリ接続を作成するインターコネクト ゲートウェイのペアを選択するときは、インターコネクト ゲートウェイが BGP ピアリングに同じ BGP ASN を使用するように設定されていることを確認します。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix に関する情報

Cisco SD-WAN Manager から、Cisco Cloud Services Router 1000v（Cisco CSR 1000v）インスタンスを SDCI プロバイダーである Equinix のファブリックに展開し、そのインスタンスを WAN エッジデバイスとして Cisco SD-WAN ファブリックに追加することができます。WAN エッジデバイスとして、Cisco CSR 1000v インスタンスはブランチの場所を Equinix ファブリックにリンクします。Equinix ファブリックでは、Cisco CSR 1000v インスタンスはインターコネクト ゲートウェイとして機能します。インターコネクト ゲートウェイから、Equinix ファブリック内の Cloud OnRamp または別のインターコネクト ゲートウェイへの直接レイヤ 2 接続（インターコネクト）を作成することができます。インターコネクトは、Equinix ファブリックのイ

ンターコネクト ゲートウェイを介してブランチの場所間をリンクするか、ブランチの場所とクラウド サービス プロバイダー間をリンクします。

このセットアップでは、Cisco SD-WAN ファブリックがオーバーレイネットワークとして機能し、Equinix ファブリックがアンダーレイネットワークとして機能します。Equinix ファブリックは、世界全体の複数の場所にあるクラウドリソースへの、効率的で、高速、低遅延、高帯域幅な接続を提供します。ブランチの場所に最も近い Equinix の場所に Cisco CSR 1000v インスタンスを展開することをお勧めします。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを展開できます。

インターコネクト ゲートウェイからの次のタイプの接続を作成できます。

表 *3*: 接続のタイプ

接続先	接続のタイプ	サポート対象ソフトウェアリリース
Amazon Web Services	• インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect プライベートホスト型接続 • インターコネクト ゲートウェイから AWS への Direct Connect パブリックホスト型接続 • インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect トランジットホスト型接続	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a と Cisco Catalyst SD-WAN Manager リリース 20.12.1 を備えた Cisco Catalyst 8000v Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 を備えた Cisco CSR 1000v
Microsoft Azure	• パートナー ExpressRoute 回線：Microsoft ピアリング • パートナー ExpressRoute 回線：プライベートピアリング	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a と Cisco Catalyst SD-WAN Manager リリース 20.12.1 を備えた Cisco Catalyst 8000v Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 を備えた Cisco CSR 1000v

接続先	接続のタイプ	サポート対象ソフトウェアリリース
Google クラウド	Google Cloud Router へのパートナーインターコネクト アタッチメント	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a と Cisco Catalyst SD-WAN Manager リリース 20.12.1 を備えた Cisco Catalyst 8000v Cisco IOS XE リリース 17.3.3 を備えた Cisco CSR 1000v
インターコネクト ゲートウェイ	インターコネクト ゲートウェイに接続された Cisco Catalyst SD-WAN のブランチの場所間のリンク	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a と Cisco Catalyst SD-WAN Manager リリース 20.12.1 を備えた Cisco Catalyst 8000v Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 を備えた Cisco CSR 1000v。

Cisco Catalyst SD-WAN Manager は統合管理ポータルとして機能し、次のタスクを実行できます。

- Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスの設定。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 より前では、Equinix の場所での Cisco CSR 1000v インスタンスの設定および展開。

- パブリッククラウドリソースへのクラウドインターコネクトの作成。
- Equinix ファブリックを介して Cisco Catalyst SD-WAN のブランチの場所をリンクするためのインターコネクトの作成。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを Equinix ファブリックのインターコネクト ゲートウェイとして展開し、Cisco Catalyst SD-WAN ブランチの場所をインターコネクト ゲートウェイに接続することができます。既存の Cisco CSR1000V 展開を使用して接続を作成することができます。

考慮すべき点

以前の Cisco Catalyst SD-WAN Manager のバージョンから Cisco Catalyst SD-WAN Manager リリース 20.12.1 にアップグレードする場合は、Cisco Catalyst 8000v を有効にするために、次の手順を実行します。

- [Edit Account Credentials] を使用して既存の Equinix アカウントを再認証し、カスタマーキーとカスタマーシークレットを入力します。以前のバージョンで使用していたものと同じキーとシークレットを使用できます。Cisco Catalyst 8000v で使用可能な請求アカウントと場所が内部で更新されます。アカウントの詳細の編集については、「View, Edit, or Delete an Interconnect Account」を参照してください。
- アカウントが再認証されたら、インターコネクト ゲートウェイの**グローバル設定**を更新して、新しいゲートウェイの Cisco Catalyst 8000v ソフトウェアバージョンとその他のパラメータを選択する必要があります。グローバル設定の更新については、「Configure Global Settings for Equinix Interconnect Gateways」を参照してください。
- Cisco Catalyst SD-WAN Manager リリース 20.12.1 より前の Cisco SD-WAN Manager を介して Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 を使用して Equinix インターコネクト ゲートウェイを展開していた場合は、Cisco Catalyst SD-WAN Manager リリース 20.12.1 にアップグレードする前に、Equinix インターコネクト ゲートウェイを Cisco IOS XE Catalyst SD-WAN リリース 17.3.3 から Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a または Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a にアップグレードする必要があります。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の利点

1. ブランチの場所が、Cisco Catalyst SD-WAN ファブリックを介して Equinix ファブリックにシームレスに接続します。
2. SLA が保証されたパブリッククラウドへのインターコネクト。
3. Cisco Catalyst SD-WAN ファブリックを介したエンドツーエンドのトラフィックのセキュリティ、セグメンテーション、およびポリシー。
4. Cisco SD-WAN Manager が、クラウドへの接続を管理するための単一のペインを提供します。
5. Cisco Catalyst SD-WAN と Equinix ファブリック全体のエンドツーエンドの可視性。
6. Cisco Catalyst SD-WAN のブランチの場所間、および Cisco Catalyst SD-WAN のブランチの場所とパブリッククラウド間のリンク。

暗号化されたマルチクラウド インターコネクト

サポート対象の最小リリース：Cisco vManage リリース 20.9.1

Cisco SD-WAN Manager の Cloud OnRamp ワークフローを使用して、インターコネクト ゲートウェイとクラウド サービス プロバイダー間のセキュアなプライベート Cisco Catalyst SD-WAN 接続をプロビジョニングすることができます。クラウド インターコネクト プロバイダーのインターコネクト ゲートウェイから、マルチクラウドワークフローの一環として作成された既存のクラウドゲートウェイへの仮想クロスコネクトを終了できます。詳細については、「Cloud OnRamp for Multicloud」を参照してください。この機能により、VPC および VNET ワークロードにアクセスするためのインターネットパスとプライベートパスの両方がサポートされます。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、暗号化されたマルチクラウド インターコネクトは、クラウド WAN ソリューションを使用した AWS クラウドゲートウェイをサポートしています。

利点

- クラウド インターコネクト プロバイダー バックボーンを介して、ブランチサイトからクラウドゲートウェイまでのエンドツーエンドの暗号化を提供します。
- 単一の仮想クロスコネクトで複数の VPN セグメントをサポートしています。
- 接続の作成前後の VPC および VNET タグの変更をサポートしています。VPN から VPC または VNET タグへのマッピングは、[Multicloud Intent Management] 画面を使用して実行できます。
- クラウド サービス プロバイダーによって課されるプレフィックス アドバタイズメントの制限を解消するために、ルートアドバタイズメントがインターコネクト ゲートウェイとクラウドゲートウェイによって制御されます。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の設定ワークフロー

前提条件の設定

1. Equinix ポータルでアカウントを作成します。Equinix の「New User Equinix Fabric Portal Access」のドキュメントを参照してください。

   アカウントを作成したら、アカウントのクライアント ID（コンシューマキー）とクライアント シークレット キー（コンシューマシークレット）を生成します。Equinix Developer Platform Knowledge Center の「Generating Client ID and Client Secret Key」のドキュメントを参照してください。

   また、このアカウントを使用してインターコネクト ゲートウェイを展開する各リージョンの請求アカウントを作成します。Equinix の「Billing Account Management」のドキュメントを参照してください。

2. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
3. インターコネクト ゲートウェイのグローバル設定を構成します。
4. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
5. インターコネクト ゲートウェイとして展開する Cisco CSR 1000v インスタンスの UUID が必要な数あることを確認します。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを展開します。

6. Equinix テンプレートを Cisco CSR 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチできます。

7. Cisco Catalyst SD-WAN のブランチの場所に最も近い Equinix の場所でインターコネクト ゲートウェイを作成します。

   クラウドプロバイダーへの接続のために、Equinix の場所でインターコネクト ゲートウェイを作成します。

   Cisco Catalyst SD-WAN のブランチの場所間の接続のために、ブランチの場所ごとに、最も近い Equinix の場所でインターコネクト ゲートウェイを作成します。

AWS へのインターコネクトを作成するためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

1. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
2. AWS 仮想プライベートクラウド（VPC）に接続するためのホストプライベートネットワークを検出します。
3. 次のいずれかのタイプの接続を作成します。

接続タイプ	ヒント
Direct Connect：パブリックホスト型接続	この接続は、パブリック AWS リソースへのリンクに使用します。リンクの固定帯域幅は最大 10 Gbps です。
Direct Connect：プライベートホスト型接続	この接続は、AWS VPC への専用リンクに使用します。リンクの帯域幅は最大 10 Gbps です。
Direct Connect：トランジットホスト型接続	この接続は、トランジットゲートウェイを介した最大 5,000 の AWS VPC への専用リンクに使用します。リンクの帯域幅は最大 10 Gbps です。最大 3 つのトランジットゲートウェイを Direct Connect ゲートウェイにアタッチし、最大 15,000 の VPC に接続することができます。

Cisco Catalyst SD-WAN のブランチの場所をリンクするためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

- インターコネクト ゲートウェイ間のインターコネクトを作成します。

Google Cloud へのインターコネクトを作成するためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

1. Google Cloud ポータルを使用して、必要な VPC ネットワークを作成します。
2. 接続するネットワークリージョンに Google Cloud Router を展開します。

   非冗長接続の場合は、Google Cloud ポータルを使用して、接続する各ネットワークリージョンに Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

   冗長接続の場合は、Google Cloud ポータルを使用して、接続する各ネットワークリージョンに 2 つの Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

   Cisco vManage リリース 20.9.1 以降では、Cisco SD-WAN Manager のインターコネクト ワークフローを介して Google Cloud Router と VLAN アタッチメントを展開できます。
3. Google Cloud アカウントを Cisco SD-WAN Manager に関連付けます。
4. インターコネクト ゲートウェイから Google Cloud Router へのインターコネクトを作成します。

Microsoft Azure へのインターコネクトを作成するためのワークフロー

次の設定手順を実行する前に、前提条件が満たされ、前提条件の設定が適用されていることを確認してください。

1. Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。
2. Azure Virtual Network（VNet）に接続するためのホスト プライベート ネットワークを検出します。
3. 次のいずれかのタイプの接続を作成します。
   - Azure ExpressRoute へのパブリック ピアリング接続
   - Azure ExpressRoute へのプライベート ピアリング接続

Cisco SD-WAN Cloud Interconnect with Equinix の前提条件の設定

Cisco SD-WAN Manager と Equinix アカウントの関連付け

前提条件

1. Equinix ポータルでアカウントを作成します。Equinix の「New User Equinix Fabric Portal Access」のドキュメントを参照してください。

2. アカウントを作成したら、アカウントのクライアントID（コンシューマキー）とクライアント シークレット キー（コンシューマシークレット）を生成します。Equinix Developer Platform Knowledge Center の「Generating Client ID and Client Secret Key」の情報を参照してください。
3. このアカウントを使用してインターコネクト ゲートウェイを展開する各リージョンの請求アカウントを作成します。Equinix の「Billing Account Management」のドキュメントを参照してください。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Associate Interconnect Account] をクリックします。
4. 次を設定します。

Interconnect Provider	[EQUINIX] を選択します。
アカウント名	任意の名前を入力します。この名前は、クラウドまたはサイト間インターコネクトを定義するワークフローでEquinix アカウントを識別するために使用されます。
[説明（Description）]（任意）	説明を入力します。
Customer Key	クライアント ID（コンシューマキー）を入力します。
Customer Secret	クライアント シークレット キー（コンシューマシークレット）を入力します。

5. [Add] をクリックします。

Cisco SD-WAN Manager はアカウントを認証し、アカウントの詳細をデータベースに保存します。

Equinix インターコネクト ゲートウェイのグローバル設定の構成

前提条件

1. Equinix ポータルでアカウントを作成します。Equinix の「New User Equinix Fabric Portal Access」のドキュメントを参照してください。
2. アカウントを作成したら、アカウントのクライアントID（コンシューマキー）とクライアント シークレット キー（コンシューマシークレット）を生成します。Equinix Developer Platform Knowledge Center の「Generating Client ID and Client Secret Key」の情報を参照してください。

3. このアカウントを使用してインターコネクトゲートウェイを展開する各リージョンの請求アカウントを作成します。Equinix の「Billing Account Management」のドキュメントを参照してください。
4. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Global Settings] をクリックします。
   - グローバル設定を追加するには、[Add] をクリックします。
   - グローバル設定を変更するには、[Edit] をクリックします。
4. 次を設定します。

設定グループの有効化	Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、このオプションを有効にして、設定グループを使用してマルチクラウドワークフローでデバイスを設定します。 このオプションは、デフォルトで無効です。 （注） ここで設定グループを有効にすると、すべてのクラウドプロバイダーに対して設定グループが有効になります。たとえば、ここでこのオプションを有効にすると、他のすべてのマルチクラウドおよびインターコネクト プロバイダーの設定グループも有効になります。
Interconnect Provider	[EQUINIX] を選択します。
ソフトウェア イメージ	Cisco CSR 1000v イメージを選択します。 Cisco Catalyst SD-WAN Manager リリース 20.12.1 の場合は、Cisco Catalyst 8000v イメージを選択します。

Instance Size	インスタンスのサイズは、各 Cisco CSR 1000v インスタンスのコンピューティング フットプリントとスループットを決定します。次のいずれかを選択します。 • [Small]：2vCPU、4 GB DRAM、最大 1 Gbps • [Medium]：4vCPU、4 GB DRAM、最大 2.5 Gbps • [Large]：6vCPU、4 GB DRAM、最大 2.5 Gbps Cisco Catalyst SD-WAN Manager リリース 20.12.1 の場合、インスタンスサイズは次のとおりです。 • [Small]：2vCPU、8 GB DRAM、最大 1 Gbps • [Medium]：4vCPU、8 GB DRAM、最大 2.5 Gbps • [Large]：6vCPU、16 GB DRAM、最大 2.5 Gbps • [xLarge]：8vCPU、16 GB DRAM、最大 2.5 Gbps
Interconnect Transit Color	インターコネクト ゲートウェイ間の接続に割り当てる色を選択します。 この色は、ブランチの場所間を直接ピアリングしないように制限されています。同じ色を Cisco Catalyst SD-WAN ファブリック内の別の接続に割り当てないでください。 （注） プライベートの色を使用することをお勧めします。デフォルトの色は使用しないでください。
BGP ASN	インターコネクト ゲートウェイとクラウドプロバイダー間のピアリングに使用される BGP ASN を入力します。 任意の ASN を入力するか、組織で使用されている既存の ASN を再利用できます。

Interconnect CGW SDWAN Color	サポート対象の最小リリース：Cisco vManage リリース 20.9.1 インターコネクト ゲートウェイがクラウドゲートウェイに接続する際のインターフェイスに使用する色を選択します。 （注） インターフェイスに割り当てられる色は、インターコネクト ゲートウェイ デバイスに対して一意であり、クラウドインターコネクト プロバイダー間では共通である必要があります。 Microsoft Azure 展開では、クラウドゲートウェイの WAN インターフェイスで Cisco Catalyst SD-WAN トンネルの色は自動的に設定されないため、WAN インターフェイスの色を手動で更新する必要があります。テンプレートの色がブランチルータ、インターコネクト ゲートウェイ、およびクラウドゲートウェイの色と一致していることを確認します。

5. 新しく追加したグローバル設定を保存するには、[Save] をクリックします。

   変更したグローバル設定を保存するには、[Update] をクリックします。

Cisco CSR 1000v または Cisco Catalyst 8000v インスタンスへの Equinix テンプレートのアタッチ

（注） 設定グループを有効にした場合、この手順は必要ありません。この場合は、「Create Interconnect Gateway at an Equinix Location」に進みます。

Equinix の場所で Cisco CSR 1000v インスタンスをインターコネクト ゲートウェイとして展開する前に、Equinix のデフォルトテンプレートをデバイスにアタッチする必要があります。Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02 という名前のテンプレートをアタッチすることを推奨します。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 の場合、Cisco Catalyst 8000v のデフォルトテンプレートは Default_EQUINIX_ICGW_C8000V_Template_V01 です。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** の順に選択します。
2. [Device Template] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Template Type] として [Default] を選択し、Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02 という名前のテンプレートを見つけます。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 の場合、デフォルトの Default_EQUINIX_ICGW_C8000V_Template_V01 を選択します。

4. [...] をクリックして、[Attach Devices] をクリックします。
5. [Available Devices] のリストから目的の Cisco CSR 1000v インスタンスの UUID を選択し、そのインスタンスを [Selected Devices] のリストに移動します。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを選択します。

6. [Attach] をクリックします。
7. テンプレートには変数が含まれています。テンプレートの変数の値を入力するには、[…] をクリックし、[Edit Device Template] をクリックします。
8. 次の変数の値を入力し、[Update] をクリックします。
   - DNS アドレス（vpn_dns_primary）
   - DNS アドレス（vpn_dns_secondary）
   - 色（vpn_if_tunnel_color_value）
   - システム IP（system-ip）
   - サイト ID（site-id）
   - ホスト名（host-name）
9. [Next] をクリックします。
10. [Configure Devices] をクリックします。

Equinix の場所でのインターコネクト ゲートウェイの作成

目的の Equinix の場所に、インターコネクト ゲートウェイとして Cisco CSR 1000v インスタンスを展開します。ブランチの場所に最も近い Equinix の場所に Cisco CSR 1000v インスタンスを展開することをお勧めします。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを展開できます。

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。

3. 設定グループを有効にしなかった場合は、Equinix テンプレートを Cisco CSR 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、テンプレートを Cisco Catalyst 8000v インスタンスにアタッチします。

4. 設定グループを有効にした場合は、設定グループに関連付けられているデバイスのデバイスパラメータが設定されていることを確認します。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Create Interconnect Gateway] をクリックします。
4. 次を設定します。

Interconnect Provider	[EQUINIX] を選択します。
ゲートウェイ名	ゲートウェイを一意に識別する名前を入力します。
[説明（Description）]（任意）	説明を入力します。
アカウント名	Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Equinix アカウントを選択します。
参照先	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. Cisco CSR 1000v インスタンスを展開する必要がある Equinix の場所を選択します。 Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを選択します。
Billing Account ID	場所に適した請求アカウントを選択します。
サイト名	サイトを選択します。 Cisco vManage リリース 20.10.1 以降では、[Site Name] フィールドを使用できます。

設定グループ	Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、クラウドゲートウェイを作成したとき、またはインターコネクト ゲートウェイのグローバル設定を構成したときに [Enable Configuration Group] オプションを有効にした場合は、次のいずれかのアクションを実行します。 • 構成グループを選択します。 • 新しい設定グループを作成して使用するには、[Create New] を選択します。[Create Configuration Group] ダイアログボックスで、新しい設定グループの名前を入力し、[Done] をクリックします。ドロップダウンリストから新しい設定グループを選択します。 選択した設定グループは、マルチクラウドワークフローでデバイスを設定するために使用されます。 設定グループの詳細については、『Cisco Catalyst SD-WAN Configuration Groups』を参照してください。 （注） • [Configuration Group] ドロップダウンリストには、このドロップダウンリストから作成した設定グループのみが含まれています。Cisco Catalyst SD-WAN で作成された他の設定グループは含まれません。このドロップダウンリストの設定グループには、このプロバイダーに必要なオプションが含まれています。 • 設定グループを使用して Equinix インターコネクト ゲートウェイを作成する場合、Cisco SD-WAN Manager からの SSH の使用は、インターコネクト ゲートウェイが Cisco Catalyst 8000v 17.13 以降の場合にのみ機能します。
UUID	Equinix のデフォルトテンプレートがアタッチされている Cisco CSR 1000v インスタンスの UUID を選択します。 （注） サイト名を選択すると、サイト名に関連付けられた UUID が [UUID] フィールドに自動的に入力されます。 Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを選択します。
設定	次のいずれかを選択します。 • [Default]：インターコネクトのグローバル設定で定義されたインスタンスサイズとソフトウェアイメージを使用します。 • [Custom]：このゲートウェイの特定のインスタンスサイズとソフトウェアイメージを選択します。

5. [Add] をクリックします。

設定タスクが成功すると、インターコネクト ゲートウェイが [Gateway Management] ページにリストされます。

（注） 先に進む前に、インターコネクト ゲートウェイの [Device Status] 列に [In Sync] と表示され、証明書が正常にインストールされていることを確認します。

AWS へのインターコネクトの作成

AWS アカウントと Cisco SD-WAN Manager の関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Cloud] をクリックします。
3. [Associate Cloud Account] をクリックします。
4. 次を設定します。

Cloud Provider	[Amazon Web Services] を選択します。
Cloud Account Name	任意の名前を入力します。
[説明（Description）]（任意）	説明を入力します。
Use for Cloud Gateway	[No] を選択します。
Log in to AWS with	[Key] または [IAM Role] を選択します。
Role ARN	API/秘密キーまたはロール ARN を入力します。

5. [Add] をクリックします。

Cisco SD-WAN Manager は、AWS への接続を作成するための API ワークフローの一環として、API/秘密キーまたはロール ARN を使用して AWS でユーザーアカウントを認証します。

ホスト プライベート ネットワークの検出と AWS VPC のタグ付け

複数のホスト VPC を、タグを使用してグループ化できます。同じタグの下の VPC は、単一のユニットと見なされます。インターコネクト ゲートウェイからのソフトウェア定義型のクラウドインターコネクトを作成する AWS VPC にタグを付けます。

前提条件

AWS アカウントを Cisco SD-WAN Manager に関連付けます。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Amazon Web Services] を選択します。

   使用可能なホスト VPC が検出され、表に一覧表示されます。

   [host VPC] テーブルには次の列があります。

   - クラウド リージョン
   - アカウント名
   - ホスト VPC 名
   - ホスト VPC タグ
   - Interconnect Enabled
   - アカウント ID（Account ID）
   - ホスト VPC ID

5. 左端の列のチェックボックスを使用して、タグ付けする VPC を選択します。
6. [Tag Actions] をクリックします。

   次の操作を実行できます。

   - [Add Tag]：選択した VPC をグループ化し、これらの VPC に同時にタグ付けします。
   - [Edit Tag]：選択した VPC をあるタグから別のタグに移行します。
   - [Delete Tag]：選択した VPC のタグを削除します。

7. [Add Tag] をクリックして、以下を設定します。

[Tag Name]	選択した VPC をリンクするタグの名前を入力します。
リージョン	選択した VPC に対応するリージョンのリスト。タグからリージョンおよび関連する VPC を除外するには、[X] をクリックします。
Selected VPCs	選択したホスト VPC の VPC ID のリスト。タグから VPC を除外するには、[X] をクリックします。

（Cisco vManage リリース 20.8.1 以前） Enable for Interconnect Connectivity （Cisco vManage リリース 20.9.1 以降） Enable for SDCI partner Interconnect Connections	AWS へのクラウドインターコネクト接続を作成するときに VPC タグを使用するには、このチェックボックスをオンにします。 有効にすると、タグはクラウドインターコネクト接続にのみ使用でき、マルチクラウドゲートウェイ インテントマッピングには使用できません。 このチェックボックスをオンにしない場合、VPC タグを使用してクラウドインターコネクト接続を作成することはできません。 （注） クラウドゲートウェイを使用して VPC ワークロードを接続する場合、この設定を有効にしないでください。タグが接続で使用されている場合は、この設定を編集できません。

8. [Add] をクリックします。

[Discover Host Private Networks] ページで、先ほど選択した VPC にタグが付けられ、タグ名が [Host VPC Tag] 列に表示されます。ソフトウェア定義型のクラウドインターコネクトに VPC タグを使用することを選択した場合、[Interconnect Enabled] 列に [Yes] と表示されます。

インターコネクト ゲートウェイから AWS への Direct Connect パブリックホスト型接続の作成

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
5. Equinix テンプレートを Cisco CSR 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。
6. Equinix の場所でインターコネクト ゲートウェイを作成します。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[EQUINIX] を選択します。
5. [Choose Interconnect Account]：アカウント名で Equinix アカウントを選択します。このアカウント名は、Cisco SD-WAN Manager でアカウントを関連付ける際に入力した名前です。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービス プロバイダー	[AWS] を選択します。
Connection Name	接続の一意の名前を入力します。
AWS Account	Cisco SD-WAN Manager で AWS アカウントの詳細を関連付ける際に入力したアカウント名で AWS アカウントを選択します。

9. 以下を設定し、[Next] をクリックします。

Equinix Hosted Connection VIF Type	[Public] を選択します。
参照先	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. AWS Direct Connect の場所を選択します。
帯域幅	接続帯域幅を選択します。 単位：Mbps。
Interconnect IP Address	インターコネクト ゲートウェイの BGP ピア ID として使用するパブリック IP アドレス（CIDR）を入力します。
Amazon IP Address	AWS BGP ピア ID として使用するパブリック IP アドレス（CIDR）を入力します。
Prefixes	ブランチの場所にアドバタイズするサマリー AWS アドレスとプレフィックスを入力します。
Segment	この接続のセグメント ID を選択します。

10. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect プライベートホスト型接続の作成

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
5. ホスト プライベート ネットワークを検出して AWS VPC にタグ付けします。
6. Equinix テンプレートを Cisco CSR1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。
7. Equinix の場所でインターコネクト ゲートウェイを作成します。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[EQUINIX] を選択します。
5. [Choose Interconnect Account]：アカウント名で Equinix アカウントを選択します。このアカウント名は、Cisco SD-WAN Manager でアカウントを関連付ける際に入力した名前です。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービスプロバイダー	[AWS] を選択します。
Connection Name	接続の一意の名前を入力します。
AWS Account	Cisco SD-WAN Manager で AWS アカウントの詳細を関連付ける際に入力したアカウント名で AWS アカウントを選択します。

9. 以下を設定し、[Next] をクリックします。

Equinix Hosted Connection VIF Type	[Private] を選択します。
参照先	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** AWS Direct Connect の場所を選択します。
帯域幅	接続帯域幅を選択します。 単位：Mbps。
Direct Connect Gateway	**1.** [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられている Direct Connect ゲートウェイを取得します。 **2.** Direct Connect 接続を作成する必要がある先の Direct Connect ゲートウェイを選択します。 または、[Add New Direct Connect Gateway] をクリックして、新しい Direct Connect ゲートウェイを作成します。 **1.** [Gateway Name] を入力します。 **2.** ゲートウェイの [BGP ASN] を入力します。 **3.** [Save] をクリックします。

設定	次のいずれかを選択します。 • [Global]： • BGP ピアリング IP アドレスは、内部で予約済みの /16 サブネットから選択されます（198.18.0.0/16）。 • BGP ASN は、グローバル設定から選択されます。 • [Custom]： • BGP ピアリングのカスタム /30 CIDR IP アドレスを入力します。 • ピアリング用のカスタム BGP ASN を入力します。 （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。

添付ファイル	Cisco vManage リリース 20.8.1 以前の場合： [VPC] を選択します。 [Segment]：この接続のセグメント ID を選択します。 [VPC Tags]：VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。
	Cisco vManage リリース 20.9.1 以降の場合： 次のいずれかを選択します。 • **VPC** [Segment]：この接続のセグメント ID を選択します。 [VPC Tags]：VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。 • Cloud Gateway [Cloud Gateways]：この接続にアタッチするクラウドゲートウェイを選択します。ドロップダウンが空の場合は、最初にマルチクラウドワークフローを使用してクラウドゲートウェイを作成する必要があります。単一接続の場合、AWS は最大 10 個のクラウドゲートウェイをサポートします。各クラウドゲートウェイは、30 個のインターコネクト接続に接続できます。

10. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

インターコネクト ゲートウェイから AWS Direct Connect ゲートウェイへの Direct Connect トランジットホスト型接続の作成

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。

2. インターコネクト ゲートウェイのグローバル設定を構成します。

3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. AWS アカウントを Cisco SD-WAN Manager に関連付けます。
5. ホスト プライベート ネットワークを検出して AWS VPC にタグ付けします。
6. Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 より前のバージョンの場合は、Equinix テンプレートを Cisco CSR 1000v インスタンスにアタッチします。
7. Equinix の場所でインターコネクト ゲートウェイを作成します。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[EQUINIX] を選択します。
5. [Choose Interconnect Account]：アカウント名で Equinix アカウントを選択します。このアカウント名は、Cisco SD-WAN Manager でアカウントを関連付ける際に入力した名前です。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービス プロバイダー	[AWS] を選択します。
Connection Name	接続の一意の名前を入力します。
AWS Account	Cisco SD-WAN Manager で AWS アカウントの詳細を関連付ける際に入力したアカウント名で AWS アカウントを選択します。

9. 以下を設定し、[Next] をクリックします。

Equinix Hosted Connection VIF Type	[Transit] を選択します。

参照先	**1.** [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 **2.** AWS Direct Connect の場所を選択します。
帯域幅	接続帯域幅を選択します。 単位：Mbps。
Direct Connect Gateway	**1.** [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられている Direct Connect ゲートウェイを取得します。 **2.** Direct Connect 接続を作成する必要がある先の Direct Connect ゲートウェイを選択します。 または、[Add New Direct Connect Gateway] をクリックして、新しい Direct Connect ゲートウェイを作成します。 **1.** [Gateway Name] を入力します。 **2.** ゲートウェイの [BGP ASN] を入力します。 **3.** [Save] をクリックします。
設定	次のいずれかを選択します。 • [Global]： • BGP ピアリング IP アドレスは、内部で予約済みの /16 サブネットから選択されます（198.18.0.0/16）。 • BGP ASN は、グローバル設定から選択されます。 • [Custom]： **1.** BGP ピアリングのカスタム /30 CIDR IP アドレスを入力します。 **2.** ピアリング用のカスタム BGP ASN を入力します。 （注） インターコネクトゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクトゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。

Segment	この接続のセグメント ID を選択します。
添付ファイル	[Transit Gateway] を選択します。 [Transit Gateway]： **1.** [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられているトランジットゲートウェイを取得します。 **2.** Direct Connect 接続を作成する必要があるトランジットゲートウェイを選択します。 または、[Add New Transit Gateway] をクリックして、新しいトランジットゲートウェイを作成します。 **1.** [Gateway Name] を入力します。 **2.** ゲートウェイの [BGP ASN] を入力します。 **3.** [AWS Region] を選択します。 **4.** [Save] をクリックします。 [VPC Tags]：VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。 [Allowed Prefixes]： **1.** [Add Prefixes] をクリックします。 **2.** 選択した VPC の IPv4 CIDR プレフィックスを入力します。 AWS VPC ダッシュボードから IPv4 CIDR アドレスを見つけることができます。

10. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

Google Cloud へのインターコネクトの作成

Cisco SD-WAN Manager と Google Cloud アカウントの関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Cloud] をクリックします。
3. [Associate Cloud Account] をクリックします。
4. 次を設定します。

Cloud Provider	[Google Cloud] を選択します。
Cloud Account Name	任意の名前を入力します。
[説明（Description）]（任意）	説明を入力します。
Use for Cloud Gateway	[No] を選択します。
Private Key ID	[Upload Credential File] をクリックします。 このファイルは、Google Cloud コンソールにログインして生成する必要があります。秘密キー ID は、JSON または REST API 形式の場合があります。形式は、キーの生成方法によって異なります。詳細については、Google Cloud のドキュメントを参照してください。

5. [Add] をクリックします。

Cisco SD-WAN Manager は、Google Cloud への接続を作成するためのワークフローの一環として、この秘密キー ID を使用して Google Cloud でユーザーアカウントを認証します。

インターコネクト ゲートウェイから Google Cloud Router へのインターコネクトの作成

前提条件

1. Google Cloud コンソールを使用して、必要な VPC ネットワークを作成します。
2. 接続するネットワークリージョンに Google Cloud Router を展開します。

   非冗長接続の場合は、Google Cloud コンソールで、接続する各ネットワークリージョンに Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

冗長接続の場合は、Google Cloud コンソールで、接続する各ネットワークリージョンに 2 つの Google Cloud Router を展開し、各 Google Cloud Router の VLAN アタッチメントを作成します。

Cisco vManage リリース 20.9.1 以降では、接続の作成時に Cisco SD-WAN Manager から Google Cloud Router と VLAN アタッチメントを作成できます。

（注） インターコネクトアタッチメントで使用するには、Google Cloud Router の Google ASN を 16550 に設定する必要があります。

3. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
4. インターコネクト ゲートウェイのグローバル設定を構成します。
5. Equinix テンプレートを Cisco Catalyst 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。
6. Cisco Catalyst SD-WAN のブランチの場所に最も近い Equinix の場所でインターコネクト ゲートウェイを作成します。

   Google Cloud への冗長接続のために、Equinix ファブリックでインターコネクト ゲートウェイのペアを作成します。非冗長接続の場合は、Equinix の場所にインターコネクト ゲートウェイを展開します。
7. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
8. Google Cloud アカウントを Cisco SD-WAN Manager に関連付けます。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[Equinix] を選択します。
5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Equinix アカウントを選択します。
6. [Choose Interconnect Gateway]：接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービスプロバイダー	[Google Cloud] を選択します。
Google Account	Google アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Google アカウントを選択します。
添付ファイル	サポート対象の最小リリース：Cisco vManage リリース 20.9.1 [Shared VPC] を選択して、Google Cloud Router と Google Cloud インターコネクトを接続にアタッチします。
リージョン	サポート対象の最小リリース：Cisco vManage リリース 20.9.1 Google Cloud リージョンを選択します。
VPC Network	サポート対象の最小リリース：Cisco vManage リリース 20.9.1 この接続を展開する VPC ネットワークを選択します。

冗長性	Cisco vManage リリース 20.8.1 以前の場合： 冗長性のある接続を作成する場合は、[Enable] を選択します。 [Primary Google Cloud Interconnect Attachment]： • [Primary Google Cloud Interconnect Attachment] ドロップダウンリストの横にある更新マークをクリックします。 • 目的のインターコネクト アタッチメントを選択します。インターコネクト アタッチメント名の形式は、<region-name>::<cloud-router-name>::<interconnect-attachment-name> です。 [Secondary Google Cloud Interconnect Attachment]： • 目的のインターコネクト アタッチメントを選択します。インターコネクト アタッチメント名の形式は、<region-name>::<cloud-router-name>::<interconnect-attachment-name> です。 セカンダリ インターコネクト アタッチメント オプションは、プライマリ インターコネクト アタッチメントが属するリージョンとネットワークに基づいて決定されます。プライマリ インターコネクト アタッチメントと同じリージョンおよびネットワークに未使用のインターコネクト アタッチメントがない場合、このドロップダウンリストは空になり、Google Cloud ポータルで冗長インターコネクト アタッチメントを作成する必要があることが示されます。 冗長性のない接続を作成する場合は、[Disable] を選択します。 [Google Cloud Interconnect Attachment]： • [Google Cloud Interconnect Attachment] ドロップダウンリストの横にある更新マークをクリックします。 • 目的のインターコネクト アタッチメントを選択します。インターコネクト アタッチメント名の形式は、<region-name>::<cloud-router-name>::<interconnect-attachment-name> です。

Cisco vManage リリース 20.9.1 以降の場合：

[Google Cloud Router]：

- [Google Cloud Router] ドロップダウンリストの横にある更新マークをクリックします。
- Google Cloud Router を選択するか、[Add New Google Cloud Router] をクリックします。

[Add New Google Cloud Router] をクリックした場合は、[Add Google Cloud Router] スライドインペインでルータ設定を構成します。

以下を設定し、[Save] をクリックします。

- [Region]：Google Cloud Router のリージョンを選択します。
- [VPC Network]：Google Cloud Router ネットワークを選択します。
- [Cloud Router Name]：固有の Google Cloud Router 名を入力します。

（注） Google Cloud Router は常に、BGP ASN が 16,550、MTU が 1,500、デフォルトルーティング有効で作成されます。

[Google Cloud Interconnect Attachment]：

- [Google Cloud Interconnect Attachment] ドロップダウンリストの横にある更新マークをクリックします。
- 必要なインターコネクトアタッチメントを選択するか、[Add New Google Cloud Interconnect Attachment] をクリックします。

[Add New Google Cloud Interconnect Attachment] をクリックした場合は、[Add Google Cloud Interconnect Attachment] スライドインペインでルータ設定を構成します。

以下を設定し、[Save] をクリックします。

- [Region]：Google Cloud インターコネクト アタッチメントのリージョンを選択します。
- [VPC Network]：インターコネクトアタッチメント用の Google Cloud ネットワークを選択します。
- [Cloud Router Name]：インターコネクト アタッチメント用に、選択したリージョンと VPC ネットワークに展開された Google Cloud Router を選択します。
- [IC Attachment Name]：インターコネクト アタッチメントの一意の名前を入力します。

	• [Secondary Zone]：このアタッチメントをセカンダリゾーンに展開する場合は、このチェックボックスをオンにします。

9. プライマリ VLAN アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. Google Cloud Router とプライマリ VLAN アタッチメントを作成した GCP リージョンに最も近い Equinix の場所を選択します。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択したピアリングの場所に基づいて作成されます。

10. ステップ 8 で冗長性を有効にした場合は、セカンダリ VLAN アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. Google Cloud Router とセカンダリ VLAN アタッチメントを作成した GCP リージョンに最も近い Equinix の場所を選択します。 ヒント　冗長性を確保するために、プライマリ VLAN アタッチメントに関連付けられているピアリングの場所以外の場所を選択します。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ VLAN アタッチメントへの接続を確立する必要があるインターコネクト ゲートウェイを選択します。

11. 以下を設定し、[Next] をクリックします。

設定	[Auto-generated] または [Custom] を選択します。 • [Auto-generated]：インターコネクト BGP ASN はシステムによって選択されます • [Custom]：インターコネクト VLAN アタッチメントとのピアリング用に、任意のインターコネクト BGP ASN を指定します。 （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。 Google Cloud Router へのインターコネクトの BGP ピアリング IP アドレスは、サブネット（169.254.0.0/16）から Google によって自動割り当てされます。Cisco SD-WAN Manager から IP アドレスを設定することはできません。
Segment	この接続のセグメント ID を選択します。

12. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

接続設定を保存すると、設定タスクが起動し、インターコネクト ゲートウェイと Google Cloud Router のインターコネクト アタッチメントの間にインターコネクトが作成されます。

タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。Google Cloud コンソールで接続の詳細を表示することもできます。

次の作業：Google Cloud コンソールで、BGP を介して Google Cloud Router からインターコネクト ゲートウェイにアドバタイズされるルートを管理します。

Google Cloud 内のクラウドゲートウェイへのインターコネクト接続の作成

前提条件

1. Google Cloud コンソールを使用して、必要な VPC ネットワークを作成します。

2. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。

3. インターコネクト ゲートウェイのグローバル設定を構成します。

4. Equinix テンプレートを Cisco Catalyst 1000v インスタンスにアタッチします。

Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスを選択します。

5. Cisco Catalyst SD-WAN のブランチの場所に最も近い Equinix の場所でインターコネクト ゲートウェイを作成します。

   Google Cloud への冗長接続のために、Equinix ファブリックでインターコネクト ゲートウェイのペアを作成します。非冗長接続の場合は、Equinix の場所にインターコネクト ゲートウェイを展開します。

6. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。

7. Google Cloud アカウントを Cisco SD-WAN Manager に関連付けます。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. [Interconnect] をクリックします。

3. [Interconnect Connectivity] をクリックします。

4. [Choose Interconnect Provider]：[Equinix] を選択します。

5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Equinix アカウントを選択します。

6. [Choose Interconnect Gateway]：接続を作成する元となるインターコネクト ゲートウェイを選択します。

7. [Add Connection] をクリックします。

8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービス プロバイダー	[Google Cloud] を選択します。
Google Account	Google アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Google アカウントを選択します。
添付ファイル	クラウドゲートウェイに接続するには、[Cloud Gateway] を選択します。 [Cloud Gateways]：ドロップダウンリストからクラウドゲートウェイを 1 つだけ選択できます。

9. 以下を設定し、[Next] をクリックします。

プライマリ

Google Cloud Router	Google Cloud Router を選択します。
Google Cloud Interconnect Attachment	必要なインターコネクトアタッチメントを選択するか、[Add New Google Cloud Interconnect Attachment] をクリックします。 [Add New Google Cloud Interconnect Attachment] をクリックした場合は、[Add Google Cloud Interconnect Attachment] スライドインペインでルータ設定を構成します。 以下を設定し、[Save] をクリックします。 • [Region]：Google Cloud インターコネクト アタッチメントのリージョンを選択します。 • [VPC Network]：アタッチメントに対して関連付けられたネットワークを選択します。 • [Cloud Router Name]：選択したリージョンと VPC ネットワークに展開された Google Cloud Router を選択します。 • [ID Attachment Name]：一意のアタッチメント名を入力します。 • [Secondary Zone]：このアタッチメントをセカンダリゾーンに展開する場合は、このチェックボックスをオンにします。
セカンダリ	
Google Cloud Router	Google Cloud Router を選択します。
Google Cloud Interconnect Attachment	必要なインターコネクトアタッチメントを選択するか、[Add New Google Cloud Interconnect Attachment] をクリックします。 [Add New Google Cloud Interconnect Attachment] をクリックした場合は、[Add Google Cloud Interconnect Attachment] スライドインペインでルータ設定を構成します。 以下を設定し、[Save] をクリックします。 • [Region]：Google Cloud インターコネクト アタッチメントのリージョンを選択します。 • [VPC Network]：アタッチメントに対して関連付けられたネットワークを選択します。 • [Cloud Router Name]：選択したリージョンと VPC ネットワークに展開された Google Cloud Router を選択します。 • [ID Attachment Name]：一意のアタッチメント名を入力します。 • [Secondary Zone]：このアタッチメントをセカンダリゾーンに展開する場合は、このチェックボックスをオンにします。

10. プライマリ VLAN アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. Google Cloud Router とプライマリ VLAN アタッチメントを作成した GCP リージョンに最も近い Equinix の場所を選択します。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択したピアリングの場所に基づいて作成されます。

11. ステップ 8 で冗長性を有効にした場合は、セカンダリ VLAN アタッチメントに次の設定を構成し、[Next] をクリックします。

Peering Location	1. [Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。 2. Google Cloud Router とセカンダリ VLAN アタッチメントを作成した GCP リージョンに最も近い Equinix の場所を選択します。 ヒント　冗長性を確保するために、プライマリ VLAN アタッチメントに関連付けられているピアリングの場所以外の場所を選択します。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ VLAN アタッチメントへの接続を確立する必要があるインターコネクト ゲートウェイを選択します。

12. 以下を設定し、[Next] をクリックします。

設定	[Auto-generated] または [Custom] を選択します。 • [Auto-generated]：インターコネクト BGP ASN はシステムによって選択されます • [Custom]：インターコネクト VLAN アタッチメントとのピアリング用に、任意のインターコネクト BGP ASN を指定します。 （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN を指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。 Google Cloud Router へのインターコネクトの BGP ピアリング IP アドレスは、サブネット（169.254.0.0/16）から Google によって自動割り当てされます。Cisco SD-WAN Manager から IP アドレスを設定することはできません。
Segment	この接続のセグメント ID を選択します。

13. 接続の概要を確認します。

- 接続を作成するには、[Save] をクリックします。
- 接続設定を変更するには、[Back] をクリックします。

接続設定を保存すると、設定タスクが起動し、インターコネクト ゲートウェイと Google Cloud Router のインターコネクト アタッチメントの間にインターコネクトが作成されます。

タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。Google Cloud コンソールで接続の詳細を表示することもできます。

次の作業：Google Cloud コンソールで、BGP を介して Google Cloud Router からインターコネクト ゲートウェイにアドバタイズされるルートを管理します。

Microsoft Azure へのインターコネクトの作成

Cisco SD-WAN Manager と Microsoft Azure アカウントの関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. [Cloud] をクリックします。

3. [Associate Cloud Account] をクリックします。

4. 次を設定します。

Cloud Provider	[Microsoft Azure] を選択します。
Cloud Account Name	任意の名前を入力します。
[説明（Description）]（任意）	説明を入力します。
Use for Cloud Gateway	[No] を選択します。
テナント ID	Azure Active Directory（AD）の ID を入力します。 **ヒント** テナント ID を見つけるには、Azure Active Directory に移動し、[Properties] をクリックします。
サブスクリプション ID	使用する Azure サブスクリプションの ID を入力します。
Client ID	既存の Azure アプリケーション ID を入力します。Azure AD にアプリケーションを登録する方法、クライアント ID と秘密キーを取得する方法などの詳細については、Azure のドキュメントを参照してください。
Secret Key	クライアント ID に関連付けられたパスワードを入力します。

5. [Add] をクリックします。

ホスト プライベート ネットワークの検出と Microsoft Azure VNet のタグ付け

インターコネクト ゲートウェイからのソフトウェア定義型のクラウドインターコネクトを作成する Microsoft Azure VNet にタグを付けます。同じ VNet タグを使用してグループ化された Azure VNet は、単一のユニットと見なされます。

前提条件

Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。

タグの追加

VNet をグループ化し、まとめてタグ付けします。

（注） 異なるリソースグループに属する VNet を一緒に使用することはできません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Microsoft Azure] を選択します。

   使用可能なホスト VNet が検出され、表に一覧表示されます。
5. 対応するチェックボックスをオンにして、タグ付けする Azure VNet を選択します。
6. [Tag Actions] をクリックします。
7. [Add Tag] をクリックして、以下を設定します。

フィールド	説明
[Tag Name]	タグの名前を入力します。
[地域（Region）]	[Add Tag] をクリックする前に VNet を選択した場合、このフィールドには、選択した VNet に対応するリージョンのリストが表示されます。 • [Add Tag] をクリックする前に VNet を選択しなかった場合、またはリージョンをさらに選択する場合は、ドロップダウンリストからリージョンを選択します。 • リージョンおよび関連する VNet をタグから除外するには、[X] をクリックします。
Selected VNets	[Add Tag] をクリックする前に VNet を選択した場合、このフィールドには、選択したホスト VNet の VNet ID のリストが表示されます。 • [Add Tag] をクリックする前に VNet を選択しなかった場合、または VNet をさらに選択する場合は、ドロップダウンリストから VNet を選択します。 • タグから VNet を除外するには、[X] をクリックします。

フィールド	説明
（Cisco vManage リリース 20.9.1 以降）[Enable for SDCI partner Interconnect Connections] （Cisco vManage リリース 20.8.1 以前）[Enable for Interconnect Connectivity]	Microsoft Azure へのインターコネクト接続を作成するときに VNet タグを使用するには、このチェックボックスをオンにします。 インターコネクト接続に対して有効になっている場合、タグは Microsoft Azure マルチクラウドワークフローで使用することはできません。 インターコネクト接続に対して有効になっていない場合、タグは Microsoft Azure マルチクラウドワークフローでのみ使用できます。 （注） クラウドゲートウェイを使用して VNet ワークロードに接続する場合、この設定を有効にしないでください。

8. [Add] をクリックします。

[Host Private Networks] ページで、先ほど選択した Azure vNet にタグが付けられ、タグ名が [VNET Tag] 列に表示されます。クラウドインターコネクトに vNet タグを使用することを選択した場合、[Interconnect Enabled] 列に [Yes] と表示されます。

タグの編集

既存のタグに VNet を追加するか、既存のタグから VNet を削除します。

Cisco vManage リリース 20.10.1 以降では、次の条件に従ってインターコネクト接続に関連付けられた VNet タグを編集します。

- 1 つの VNet のみが VNet タグに関連付けられている場合、タグから VNet を削除することはできません。タグから VNet を削除するには、インターコネクト接続を削除してからタグを編集します。
- 仮想 WAN アタッチメントを使用したプライベートピアリング接続の場合、タグに関連付ける VNet は、タグにすでに関連付けられている VNet と同じリージョンのものである必要があります。

  新しいリージョンの VNet をプライベートピアリング接続にアタッチするには、次の手順を実行します。

  1. リージョンの新しいタグを作成し、必要な VNet を関連付けます。
  2. プライベートピアリング接続を編集し、VNet タグを接続にアタッチします。

- VNet アタッチメントを使用したプライベートピアリング接続の場合、タグの編集中に、新しいリージョンの VNet をタグに関連付けることができます。

（注） Cisco vManage リリース 20.9.1 以前のリリースでは、インターコネクト接続に関連付けられている VNet タグを編集することはできません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Microsoft Azure] を選択します。

   使用可能なホスト VNet が検出され、表に一覧表示されます。
5. [Tag Actions] をクリックします。
6. [Edit Tag] をクリックし、必要に応じて以下を変更します。

フィールド	説明
[Tag Name]	ドロップダウンリストからタグ名を選択します。
[地域（Region）]	このフィールドには、タグに関連付けられた VNet に対応するリージョンのリストが表示されます。 • ドロップダウンリストから追加のリージョンを選択します。 • リージョンおよび関連する VNet をタグから除外するには、[X] をクリックします。
Selected VNets	このフィールドには、タグに関連付けられている VNet のリストが表示されます。 • ドロップダウンリストから追加の VNet を選択します。 • タグから VNet を除外するには、[X] をクリックします。
（Cisco vManage リリース 20.9.1 以降）[Enable for SDCI partner Interconnect Connections] （Cisco vManage リリース 20.8.1 以前）[Enable for Interconnect Connectivity]	（読み取り専用）VNet をインターコネクト接続の設定中に使用するように設定されているか、またはマルチクラウドゲートウェイのインテントマッピングに使用するように設定されているかを示します。

7. [Update] をクリックします。

タグの削除

VNet をグループ化しているタグを削除します。

（注） VNet タグがインターコネクト接続に関連付けられている間は、タグを削除できません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Host Private Networks] をクリックします。
4. [Cloud Provider]：[Microsoft Azure] を選択します。

   使用可能なホスト VNet が検出され、表に一覧表示されます。
5. [Tag Actions] をクリックします。
6. [タグを削除（Delete Tag）]をクリックします。
7. [Tag Name]：ドロップダウンリストからタグ名を選択します。
8. [Delete] をクリックします。

インターコネクト ゲートウェイから Microsoft Azure ExpressRoute への Microsoft ピアリング接続の作成

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。
5. Equinix テンプレートを Cisco Catalyst 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。
6. Equinix の場所でインターコネクト ゲートウェイを作成します。

   Microsoft Azure に接続するために、Equinix ファブリックにインターコネクト ゲートウェイのペアを作成します。デフォルトは冗長接続であり、この設定のみがサポートされています。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[Equinix] を選択します。
5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Equinix アカウントを選択します。
6. [Choose Interconnect Gateway]：接続を作成する元となるインターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウド サービス プロバイダー	[Microsoft Azure] を選択します。
Azure Account	Microsoft Azure アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Microsoft Azure アカウントを選択します。

ExpressRoute	

1. [Refresh] ボタンをクリックして、使用可能な ExpressRoute のリストを更新します
2. ExpressRoute を選択するか、[Add New ExpressRoute] をクリックします。

   （注）
   - Cisco vManage リリース 20.8.1 以降では、Equinix ExpressRoute を使用できます。
   - Cisco vManage リリース 20.8.1 以降では、使用可能な ExpressRoute のリストのドロップダウンに表示される、それぞれのインターコネクト プロバイダー用に作成されたすべての ExpressRoute は、プロビジョニングのステータスに応じて色分けされます。色とその意味のリストを示します。
     - 黒：プロビジョニングされていません。
     - グレー：プロビジョニング済み。
     - 赤：失敗。
   - 選択した Azure アカウントのプロビジョニングされていない ExpressRoute のみを選択できます。ExpressRoute の状態は、Microsoft Azure ポータルで確認できます。

   [Add New ExpressRoute] をクリックした場合は、[Create New ExpressRoute] スライドインペインで ExpressRoute 設定を構成します。

   次の項目を設定して、[保存（Save）] をクリックします。

   - [Resource Group]：Microsoft Azure アカウントに関連付けられているリソースグループを選択します。
   - [Region]：Azure リージョンを選択します。
   - [Instance Name]：ExpressRoute インスタンスの名前を入力します。
   - [Provider]：[Equinix] を選択します。
   - [Peering Location]：[Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。ExpressRoute の場所を選択します。
   - [Bandwidth]：ExpressRoute 回線の帯域幅を選択します。
   - [SKU]：[Premium] または [Standard] SKU を選択します。
   - [Billing Model]：[Metered] 課金または [Unlimited] を選択

	します。

9. ExpressRoute へのプライマリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択した ExpressRoute の場所に基づいて作成されます。

10. ExpressRoute へのセカンダリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ接続を確立する必要があるインターコネクト ゲートウェイを選択します。

11. 以下を設定し、[Next] をクリックします。

展開タイプ	[Public] を選択します。
Primary IPv4 Subnet	プライマリ インターコネクト ゲートウェイからの BGP ピアリングの /30 CIDR パブリック IP アドレスを入力します。 接続を作成する前に、パブリック IPv4 アドレスの使用が組織で許可されていることを確認してください。
Secondary IPv4 Subnet	セカンダリ インターコネクト ゲートウェイからの BGP ピアリングの /30 CIDR パブリック IP アドレスを入力します。 接続を作成する前に、パブリック IPv4 アドレスの使用が組織で許可されていることを確認してください。
BGP Advertise Prefix	インターコネクト ゲートウェイにアドバタイズするサマリーアドレスとプレフィックスを入力します。
Segment	この接続のセグメント ID を選択します。

12. 接続の概要を確認します。
    - 接続を作成するには、[Save] をクリックします。
    - 接続設定を変更するには、[Back] をクリックします。

接続設定を保存すると、設定タスクが起動します。このタスクでは、次のリソースが作成されます。

- インターコネクト ゲートウェイと ExpressRoute 間の Equinix ファブリック内の仮想クロスコネクト
- ExpressRoute 回線の Microsoft Azure パブリック/プライベートピアリング
- vNet ゲートウェイ（vNet 用の vNet ゲートウェイが存在しない場合）
- ExpressRoute と vNet ゲートウェイ間の接続

タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

Microsoft Azure ポータルで接続の詳細を表示することもできます。

インターコネクト ゲートウェイから Microsoft Azure ExpressRoute へのプライベートピアリング接続の作成

前提条件

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. Microsoft Azure アカウントを Cisco SD-WAN Manager に関連付けます。
5. ホスト プライベート ネットワークを検出して Microsoft Azure VNet をタグ付けします。
6. Equinix テンプレートを Cisco Catalyst 1000v インスタンスにアタッチします。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、Cisco Catalyst 8000v インスタンスをアタッチします。
7. Equinix の場所でインターコネクト ゲートウェイを作成します。

   Microsoft Azure に接続するために、Equinix ファブリックにインターコネクト ゲートウェイのペアを作成します。デフォルトは冗長接続であり、この設定のみがサポートされています。

手順

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。

4. [Choose Interconnect Provider]：[Equinix] を選択します。
5. [Choose Interconnect Account]：Cisco SD-WAN Manager でアカウントの詳細を関連付ける際に入力したアカウント名で Equinix アカウントを選択します。
6. [Choose Interconnect Gateway]：Direct Connect 接続を作成する元となるインターコネクトゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Cloud] を選択します。
クラウドサービスプロバイダー	[Microsoft Azure] を選択します。
Azure Account	Microsoft Azure アカウントの詳細を Cisco SD-WAN Manager に関連付ける際に入力したアカウント名で Microsoft Azure アカウントを選択します。

ExpressRoute	

1. [Refresh] ボタンをクリックして、使用可能な ExpressRoute のリストを更新します
2. ExpressRoute を選択するか、[Add New ExpressRoute] をクリックします。

   （注）
   - Cisco vManage リリース 20.8.1 以降では、Equinix ExpressRoute を使用できます。
   - Cisco vManage リリース 20.8.1 以降では、使用可能な ExpressRoute のリストのドロップダウンに表示される、それぞれのインターコネクト プロバイダー用に作成されたすべての ExpressRoute は、プロビジョニングのステータスに応じて色分けされます。色とその意味のリストを示します。
     - 黒：プロビジョニングされていません。
     - グレー：プロビジョニング済み。
     - 赤：失敗。
   - 選択した Azure アカウントのプロビジョニングされていない ExpressRoute のみを選択できます。ExpressRoute の状態は、Microsoft Azure ポータルで確認できます。

   [Add New ExpressRoute] をクリックした場合は、[Create New ExpressRoute] スライドインペインで ExpressRoute 設定を構成します。

   次の項目を設定して、[保存（Save）] をクリックします。

   - [Resource Group]：Microsoft Azure アカウントに関連付けられているリソースグループを選択します。
   - [Region]：Azure リージョンを選択します。
   - [Instance Name]：ExpressRoute インスタンスの名前を入力します。
   - [Provider]：[Equinix] を選択します。
   - [Peering Location]：[Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。ExpressRoute の場所を選択します。
   - [Bandwidth]：ExpressRoute 回線の帯域幅を選択します。
   - [SKU]：[Premium] または [Standard] SKU を選択します。
   - [Billing Model]：[Metered] 課金または [Unlimited] を選択

	します。

9. ExpressRoute へのプライマリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	接続帯域幅（Mbps）を選択します。許可された帯域幅の値のリストは、選択した ExpressRoute の場所に基づいて作成されます。

10. ExpressRoute へのセカンダリ接続について次の設定を構成し、[Next] をクリックします。

Peer Location	場所は、前に選択した ExpressRoute に基づいて自動的に選択されます。
Connection Name	接続の一意の名前を入力します。
Bandwidth (Mbps)	セカンダリ接続の帯域幅は、プライマリ接続の帯域幅と同じ値に設定されます。
Source Gateway	セカンダリ接続を確立する必要があるインターコネクト ゲートウェイを選択します。

11. 以下を設定し、[Next] をクリックします。

展開タイプ	[Private] を選択します。

BGP-Peering Settings	[Auto-generated] または [Custom] を選択します。 [Auto-generated]：インターコネクト BGP ASN、およびプライマリおよびセカンダリ IPv4 サブネットがシステムによって選択されます。IPv4 サブネットは、内部で予約された /16 サブネット（198.18.0.0/16）から選択されます。 [Custom]： （注） インターコネクト ゲートウェイからの最初のインターコネクトに対してのみ、カスタム BGP ASN とカスタム IPv4 サブネットを指定できます。インターコネクト ゲートウェイからインターコネクトが作成された後は、その後作成されたインターコネクトに対して BGP ASN を変更することはできません。 • [BGP ASN]：ExpressRoute とのプライマリおよびセカンダリピアリングに選択した ASN を指定します。 • [Primary IPv4 Subnet]：プライマリ インターコネクト ゲートウェイとの BGP ピアリングの /30 CIDR IP アドレスを入力します。 • [Secondary IPv4 Subnet]：セカンダリ インターコネクト ゲートウェイとの BGP ピアリングの /30 CIDR IP アドレスを入力します。
添付ファイル	次のいずれかを選択します。 • [vNet]：VNet タグを使用して VNet を接続にアタッチします。 • [vWAN]：仮想 WAN を接続にアタッチし、VNet タグを使用して仮想 WAN のリージョンから VNet を選択します。 • サポート対象の最小リリース：Cisco vManage リリース 20.9.1 [Cloud Gateway]：クラウドゲートウェイを接続にアタッチします。接続ごとに最大 5 つのクラウドゲートウェイを選択できます。
VNet Settings	[VNet Tags]：VNet タグを選択して、この接続を介してトラフィックをルーティングする必要がある VNet を識別します。

virtual WAN Settings	

[vWAN]：新しい仮想 WAN を選択または追加します。

（注） ExpressRoute 回線の選択されたリソースグループに対して、インターコネクト ゲートウェイから Microsoft Azure への最初の接続にのみアタッチする仮想 WAN を選択できます。同じ仮想 WAN が、仮想 WAN をアタッチするように選択した同じリソースグループ内の後続の接続にアタッチされます。

Cisco vManage リリース 20.8.1 以降では、Cisco SD-WAN Manager は、Microsoft Azure アカウントごとに、各 Microsoft Azure リソースグループに対して 1 つの仮想 WAN をサポートします。その vWAN が選択され、仮想 WAN 接続の一部として使用されると、同じ Microsoft Azure リソースグループへの後続の仮想 WAN 接続には同じ仮想 WAN が使用されます。

接続に ExpressRoute 回線が選択されると、接続用に Microsoft Azure リソースグループが決定されます。接続に属する他のすべての Microsoft Azure リソースは、選択した ExpressRoute 回線と同じ Microsoft Azure リソースグループに含まれている必要があります。

[vNet]：VNet タグを選択して、この接続を介してトラフィックをルーティングする必要がある VNet を識別します。

Cisco SD-WAN Manager は、選択された VNet タグに基づいて VNet を検索し、VNet が属するリージョンを識別します。選択された仮想 WAN と特定されたリージョンについて、Cisco SD-WAN Manager は、検証に使用できる仮想ハブを見つけて一覧表示します。仮想ハブが存在しないリージョンの場合、名前とアドレスプレフィックスを指定して仮想ハブを追加する必要があります。

[vHub Settings]：

（注） Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、リージョンに複数の Azure Virtual WAN ハブがある場合は、そのリージョンの特定の Azure Virtual WAN ハブを選択できます。Azure Virtual WAN ハブを選択すると、Azure Virtual WAN 用に作成される後続のすべての接続で同じ Azure Virtual WAN ハブが使用されます。

1. [Add Settings] をクリックします。設定を変更する場合は、[Edit Settings] をクリックします。
2. 該当するリージョンの仮想ハブ名とアドレスプレフィックスを確認します。リージョンに仮想ハブが存在しない場合は、リージョンに使用する仮想ハブの名前とアドレスプレフィッ

	クスを入力します。 （注） 入力する仮想ハブのアドレスプレフィックスが、どの VNet のアドレスプレフィックスとも重複していないことを確認してください。 3. 変更を適用するには、[Save] をクリックします。変更を破棄するには、[Cancel] をクリックします。
Segment	この接続のセグメント ID を選択します。

12. 接続の概要を確認します。
    - 接続を作成するには、[Save] をクリックします。
    - 接続設定を変更するには、[Back] をクリックします。

接続設定を保存すると、設定タスクが起動します。

VNet アタッチメントの場合は、設定タスクにより次のリソースが作成されます。

- インターコネクト ゲートウェイと ExpressRoute 間の Equinix ファブリック内の仮想クロスコネクト
- ExpressRoute 回線の Microsoft Azure パブリック/プライベートピアリング
- vNet ゲートウェイ（vNet 用の vNet ゲートウェイが存在しない場合）
- ExpressRoute と vNet ゲートウェイ間の接続

仮想 WAN アタッチメントの場合は、設定タスクにより次のリソースが作成されます。

- インターコネクト ゲートウェイと ExpressRoute 間の Equinix ファブリック内の仮想クロスコネクト
- ExpressRoute 回線の Microsoft Azure パブリック/プライベートピアリング
- 必要な仮想ハブ
- vNet と仮想ハブ間の接続
- 各仮想ハブの ExpressRoute ゲートウェイ（必要な場合）
- ExpressRoute ゲートウェイと ExpressRoute 回線間の接続

タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

Microsoft Azure ポータルで接続の詳細を表示することもできます。

デバイスリンク

デバイスリンクグループは、2 つ以上のエッジデバイス間にフルメッシュネットワークを作成します。デバイスリンクは、グループの一部であるすべてのエッジデバイスを接続して WAN を作成します。メッシュ内のすべてのデバイスリンクは、エッジデバイス間で同じ帯域幅を共有します。

（注）
- Equinix アカウントごとにサポートされるデバイスリンクは 1 つだけです。
- デバイスリンクグループに属するインターコネクト ゲートウェイ間でポイントツーポイント接続を形成することはできません。
- Cisco vManage リリース 20.9.2 および Cisco vManage リリース 20.10.1 にアップグレードする場合は、いくつかのデバイスを追加または削除して新しい設定をデバイスにプッシュすることで、デバイスリンクを変更する必要があります。これを行わないと、サイト間およびデバイスリンクが同じインターコネクト ゲートウェイ上に存在する場合、サイト間接続の BFD セッションがダウンします。

デバイスリンクの追加

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Device Links] をクリックします。
5. [Add Device Links] をクリックします。
6. ドロップダウンメニューから [Account name] を選択します。これは、アカウントの関連付けを通じて Cisco SD-WAN Manager に関連付けられている Equinix アカウントです。
7. [Device link name] を入力します。
8. ドロップダウンメニューから [Bandwidth] を選択します。

（注） Equinix でサポートされる最大帯域幅は、メトロあたり 10,000 Mbps です。

9. （オプション）

   [Subnet] を入力します。

（注）
- インターコネクト ゲートウェイのデバイス リンク インターフェイスに IP サブネットを指定します。
- サブネットは、10.0.0.0/8、172.16.0.0/12、および 192.168.0.0/16 の範囲にある必要があります。
- サブネットは、172.31.251.0/21 と競合しないようにする必要があります。
- サブネットは、他の接続と競合しないようにする必要があります。
- サブネットを入力しない場合、デフォルトで 198.19.0.0/16 が使用されます。

10. ドロップダウンメニューから [Gateway Name] を選択します。少なくとも 2 つのゲートウェイ名を選択してください。
11. [Save] をクリックします。

デバイスリンクの削除

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Device Links] をクリックします。

   既存のデバイスリンクの概要がテーブルに示されます。
5. このテーブルで、目的のリンクを見つけて [...] をクリックします。
6. デバイスリンクを削除するには、[Delete] をクリックし、デバイスリンクを削除することを確定します。

デバイスリンクの更新

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** に移動します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Device Links] をクリックします。

   既存のデバイスリンクの概要がテーブルに示されます。

5. このテーブルで、目的のリンクを見つけて [...] をクリックします。
6. デバイスリンクを編集するには、[Edit] をクリックします。
7. [Edit Device Link] ページで、[Bandwidth] および [Gateway Name] のみを更新して、ゲートウェイを追加または削除することができます。

（注） 編集できるパラメータは、[Bandwidth] と [Gateway Name] の 2 つだけです。

デバイスを追加または削除するときは、デバイスリンクに少なくとも2つのデバイスが存在している必要があります。

Equinix でサポートされる最大帯域幅は、メトロあたり 10,000 Mbps です。

8. [Save] をクリックします。

インターコネクトゲートウェイ間のインターコネクトの作成

Cisco SD-WAN Manager から、2 つ以上の Equinix の場所にあるインターコネクト ゲートウェイ間のインターコネクトを作成できます。これにより、Equinix ファブリックを介してこれらのインターコネクト ゲートウェイに接続されている SD-WAN ブランチの場所をリンクできます。

前提条件

Equinix ファブリックを介して接続する SD-WAN ブランチの場所ごとに、次の設定の前提条件を満たします。

1. Equinix アカウントを Cisco SD-WAN Manager に関連付けます。
2. インターコネクト ゲートウェイのグローバル設定を構成します。
3. 必要なネットワークセグメントを作成します（『Segmentation Configuration Guide』を参照）。
4. 最も近い Equinix の場所を特定します。
5. ブランチの場所に最も近い Equinix の場所にインターコネクト ゲートウェイを作成します。

（注） 2 つのブランチの場所で定義された VRF があり、インターコネクト ゲートウェイ間の接続を介して VRF にアタッチされたトラフィックを交換する場合は、インターコネクト ゲートウェイで VRF と適切な集中管理型ポリシーを設定して、インターコネクト ゲートウェイ間の接続を介してブランチのトラフィックをルーティングする必要があります。

手順

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。
4. [Choose Interconnect Provider]：[EQUINIX] を選択します。
5. [Choose Interconnect Account]：アカウント名で Equinix アカウントを選択します。このアカウント名は、Cisco SD-WAN Manager でアカウントを関連付ける際に入力した名前です。
6. [Choose Interconnect Gateway]：送信元インターコネクト ゲートウェイを選択します。
7. [Add Connection] をクリックします。
8. 以下を設定し、[Next] をクリックします。

接続先タイプ	[Edge] を選択します。
Connection Name	接続の一意の名前を入力します。
Interconnect Gateway	宛先インターコネクト ゲートウェイを選択します。
帯域幅	接続帯域幅を選択します。 単位：Mbps。

（注） デバイスリンクグループに属するインターコネクト ゲートウェイを使用してポイントツーポイント接続を形成することはできません。

9. 接続の概要を確認します。
   - 接続を作成するには、[Save] をクリックします。
   - 接続設定を変更するには、[Back] をクリックします。

設定タスクが成功すると、[Interconnect Connectivity] ページにこの接続が表示されます。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の設定の確認と変更

インターコネクト ゲートウェイと接続の概要の表示

Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** > **[Interconnect]** を選択します。このページでは、作成したインターコネクト ゲートウェイと接続の概要を表示できます。インターコネクト ゲートウェイを作成していない場合、このページにはインターコネクト ゲートウェイと接続を作成および管理するためのワークフローの概要が表示されます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。

   次の情報が表示されます。

Interconnect Gateways	• インターコネクト ゲートウェイの総数 • 到達可能な（アップ状態の）インターコネクト ゲートウェイの数 • 到達不能な（ダウン状態の）インターコネクト ゲートウェイの数
接続	• 接続の合計数 • アップ状態の接続の数 • ダウン状態の接続の数
Summary Table	すべてのインターコネクト ゲートウェイとゲートウェイからの接続の要約リスト。
Device Link	• デバイスリンクの総数 • アップ状態のデバイスリンクの数 • ダウン状態のデバイスリンクの数

接続の表示、編集、または削除

（注）
- AWS への接続を削除すると、Cisco SD-WAN Manager は、接続の確立中に作成された VIF、仮想プライベートゲートウェイ、およびルートテーブルのみを削除します。
- AWS への接続の作成中に、Cisco SD-WAN Manager から Direct Connect ゲートウェイまたはトランジットゲートウェイを作成した場合、接続を削除してもゲートウェイは削除されません。必要に応じて、これらの AWS リソースを管理する必要があります。

  Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降では、接続の削除中に Direct Connect ゲートウェイまたはトランジットゲートウェイを削除するオプションがあります。
- AWS への接続を削除する場合、AWS および Equinix によってリソースが破棄される順序には一般的ではないタイミングの問題があるため、Cisco SD-WAN Manager は、サービスプロバイダーによって返される 400 エラーとともに、接続の削除に失敗したことを示すエラーを返す可能性があります。Cisco SD-WAN Manager は、そのデータベースから接続を完全にクリアし、関連するすべてのデバイスの設定をクリアします。Equinix ポータルにログインし、インターフェイスの設定と関連付けが Equinix データベースからも削除されていることを確認することをお勧めします。これにより、同じインターフェイスを後で別の接続に再利用できます。

  Equinix ポータルでインターフェイスのステータスを確認しないと、同じデバイスに新しい接続を作成する際にエラーが発生する可能性があります。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Interconnect Connectivity] をクリックします。

   既存の接続の概要がテーブルに示されます。
4. このテーブルで、目的の接続を見つけて [...] をクリックします。
   - 接続の詳細を表示するには、[View] をクリックします。
   - 接続を削除するには、[Delete] をクリックして、接続を削除することを確認します。

接続設定の編集

サポート対象の最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.12.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。

3. [Interconnect Connectivity] をクリックします。

   既存の接続の概要がテーブルに示されます。

4. 接続設定を変更するには、目的の接続の [...] をクリックし、[Edit] をクリックします。

   次の表は、接続先と接続タイプ（ある場合）に基づいて、編集可能なパラメータを説明しています。必要に応じてパラメータを設定します。

   Cisco Catalyst SD-WAN Manager では、これらの編集可能なパラメータに加えて、接続に関する読み取り専用のプロパティも表示されます。

（注） アクティブな接続のプロパティのみを変更できます。

表 *4 : AWS* へのインターコネクト接続の編集可能なプロパティ

フィールド	説明	適用される接続タイプ
Segment	この接続の別のセグメント ID を選択します。	AWS へのすべての接続
Transit Gateway	1. [Refresh] ボタンをクリックして、選択した AWS アカウントに関連付けられているトランジットゲートウェイを取得します。 2. Direct Connect 接続を作成する必要があるトランジットゲートウェイを選択します。 （注） • 削除するトランジットゲートウェイは、この接続に関連付けられている唯一のトランジットゲートウェイではない。 • 同じ編集操作で、トランジットゲートウェイが提供するリージョンに対応する VPC タグを削除できる。 （注） あるリージョンの既存のトランジットゲートウェイを、同じリージョンの別のトランジットゲートウェイに置き換えることはできません。	トランジットホスト型接続

フィールド	説明	適用される接続タイプ
VPC Tags	VPC タグを選択して、この接続を介してトラフィックをルーティングする必要がある VPC を識別します。	• VPC アタッチメントを使用したプライベートホスト型接続 • トランジットホスト型接続
許可プレフィックス（**Allowed Prefixes**）	[Edit Prefixes] をクリックします。 選択した VPC の IPv4 Classless Inter-Domain Routing（CIDR）プレフィックスを入力します。AWS VPC ダッシュボードから IPv4 CIDR アドレスを見つけることができます。 （注） さらにプレフィックスを追加できます。既存のプレフィックスを削除することはできません。	トランジットホスト型接続

表 *5 : Google Cloud* へのインターコネクト接続の編集可能なプロパティ

フィールド	説明
接続速度	[Connectivity Speed] ドロップダウンリストから必要な帯域幅を選択します。 冗長接続の場合は、プライマリ接続またはセカンダリ接続のいずれかの接続速度を変更します。ピア接続は、同じ接続速度を使用するように更新されます。 接続の帯域幅オプションは、関連付けられたピアリングの場所によって異なる場合があります。

（注） プライマリ接続またはセカンダリ接続のいずれかのプロパティを変更します。ピア接続は、同じ設定を使用するように更新されます。

表 *6 : Microsoft Azure* へのインターコネクト接続の編集可能なプロパティ

フィールド	説明	適用される接続タイプ
帯域幅	接続帯域幅を変更します。 単位：Mbps。 （注） Microsoft Azure への接続の帯域幅のみを増やすことができます。Microsoft Azure への接続の場合、Cisco SD-WAN Manager で接続帯域幅を増やす前に、Azure ポータルで ExpressRoute の帯域幅を増やす必要があります。	プライベートおよびパブリック（Microsoft）ピアリング接続
Segment	この接続の別のセグメント ID を選択します。	プライベートおよびパブリック（Microsoft）ピアリング接続
BGP Advertise Prefix	インターコネクト ゲートウェイにアドバタイズするサマリーアドレスとプレフィックスを入力します。 （注） Microsoft Azure のデフォルトでは、BGP アドバタイズプレフィックスが正しく表示されないリソースまたはネットワークオブジェクトを表示するために、ポータルで古いバージョンの API が使用されます。Microsoft Azure ポータルから BGP アドバタイズプレフィックスを確認するには、2020-05-01 以降の API バージョンを選択します。	パブリック（Microsoft）ピアリング接続
VNet Settings		
VNet	VNet タグを選択して、この接続を介してトラフィックをルーティングする必要がある VNet を識別します。	プライベートピアリング接続

フィールド	説明	適用される接続タイプ
vHub Settings	**1.** [Edit Settings] をクリックします。 **2.** 該当するリージョンの仮想ハブ名とアドレスプレフィックスを確認します。リージョンに仮想ハブが存在しない場合は、リージョンに使用する仮想ハブの名前とアドレスプレフィックスを入力します。 （注） 入力する仮想ハブのアドレスプレフィックスが、どの VNet のアドレスプレフィックスとも重複していないことを確認してください。 **3.** 変更を適用するには、[Save] をクリックします。変更を破棄するには、[Cancel] をクリックします。	プライベートピアリング接続

表 *7:* エッジデバイス間のインターコネクト接続の編集可能なプロパティ

フィールド	説明
帯域幅	接続帯域幅を変更します。 単位：Mbps。

5. 変更を適用するには、[Update] または [Save] をクリックします。

インターコネクト ゲートウェイの表示、編集、または削除

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. [Interconnect] をクリックします。

3. [Gateway Management] をクリックします。

既存のインターコネクト ゲートウェイの詳細がテーブルにまとめられています。

4. このテーブルで、目的のインターコネクト ゲートウェイを見つけて [...] をクリックします。

- インターコネクト ゲートウェイの詳細を表示するには、[View] をクリックします。
- インターコネクト ゲートウェイの説明を編集するには、[Edit Interconnect Gateway] をクリックします。

- インターコネクトゲートウェイを削除するには、[Delete]をクリックして、ゲートウェイを削除することを確定します。

  インターコネクト ゲートウェイを削除すると、Equinix ファブリックからブランチの場所の接続が切断されます。

インターコネクトアカウントの表示、編集、または削除

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Interconnect] をクリックします。
3. [Account Management] をクリックします。

   使用可能なインターコネクトアカウントがテーブルに表示されます。
4. 目的のインターコネクトアカウントに対して、[...]をクリックし、次の手順を実行します。
   - インターコネクトアカウントの詳細を表示するには、[View] をクリックします。
   - インターコネクトアカウントの詳細を変更するには、[Edit Account Information] をクリックします。

     [Account Name] と [Description] を変更できます。
   - インターコネクトアカウントのログイン情報を変更するには、[Edit Account Credentials] をクリックします。

     アカウントの [Customer Key] と [Customer Secret] を変更できます。

（注） Cisco SD-WAN Manager でログイン情報を変更しても、インターコネクトプロバイダーのログイン情報は変更されません。この設定オプションは、インターコネクトプロバイダーの関連ポータルで実行した、アカウントログイン情報の変更内容を複製する場合にのみ使用してください。

   - インターコネクトアカウントを削除するには、[Remove]をクリックして、アカウントの削除を確定します。

監査管理

サポート対象の最小リリース：Cisco Catalyst SD-WAN Manager リリース 20.12.1

SDCIプロバイダーEquinixのファブリックに追加された監査管理のサポートは、クラウドの状態が Cisco SD-WAN Manager の状態と同期しているかどうかを確認するために役立ちます。監

査プロセスには、プロバイダーリソース、インターコネクトゲートウェイ、およびクラウドへの接続のスキャンが含まれています。エラーがある場合はエラーが表示され、エラーがない場合はステータスに [In Sync] と表示されます。

監査レポートへのアクセス

1. [Cloud onRamp for Multicloud] ページで、[Interconnect] タブに移動します。
2. [Intent Management] ペインで、[Audit] をクリックします。
3. [Intent Management- Audit] 画面の [Interconnect Gateways] で、ドロップダウンリストから [Interconnect Provider] を選択します。
4. [Interconnect Connections] を選択します。
5. 目的の監査レポートを表示するには、[Destination Type] を選択し、宛先タイプが [cloud] の場合はドロップダウンリストから [Cloud Provider] を選択します。
6. [Device Links] オプションを選択します。

パラメータ名	説明
Interconnect Provider	ドロップダウンからインターコネクト プロバイダー タイプを選択します。次のオプションがあります。 • Megaport • Equinix
Interconnect Connections	インターコネクト接続を有効または無効にします。
Destination Type	ドロップダウンリストから宛先タイプを選択します。次のオプションがあります。 • **クラウド** • **Edge**
クラウドプロバイダー	ドロップダウンリストからクラウドプロバイダーを選択します。次のオプションがあります。 • Amazon Web Services • **Microsoft Azure** • **Google Cloud**
Device Links	インターコネクト プロバイダーのデバイスリンクを選択します。

（注） 監査が完了すると、次のレポートが生成されます。

- [Edge Gateway]：設定されたエッジゲートウェイに関する情報を提供します。
- [Edge Connections]：設定されたエッジ接続に関する情報を提供します。
- [Unknown Edge Gateways]：不明なエッジゲートウェイに関する情報を提供します。
- [Unknown Edge Connections]：不明なエッジ接続に関する情報を提供します。

監査レポートに詳細とともに表示されるステータスは次のとおりです。

- In Sync
- Out of Sync
- AUDIT_INFO

監査の利点

監査は、Cisco SD-WAN Manager インテントとクラウドで実現された内容の間の乖離または不一致を特定するのに役立ちます。この乖離は、クラウドリソース、接続、および状態に関して発生します。このような乖離が検出されると、Cisco SD-WAN Manager によりその乖離にフラグが付けられ、修正アクションの実行に役立てることができます。

Cisco Catalyst SD-WAN Cloud Interconnect with Equinix のトラブルシューティング

シナリオ	対処法
インターコネクトアカウントを追加できない	• Cisco SD-WAN Manager に関連付けられているアカウントのログイン情報が正しいことを確認します。 • インターコネクトプロバイダーでログイン情報を更新した場合は、Cisco SD-WAN Manager でアカウントのログイン情報を更新します。
インターコネクト ゲートウェイの作成を試みている際に、デバイスリストが空になる	Equinix テンプレートがデバイスにアタッチされていることを確認します。（推奨テンプレート：Default_EQUINIX_DHCP_DNS_ICGW_CSR1000V_Template_V02）
インターコネクト ゲートウェイの作成を試みている際に、目的の場所が見つからない	[Refresh] ボタンをクリックして、使用可能な場所のリストを更新します。

シナリオ	対処法
インターコネクト ゲートウェイの作成に失敗した	**1.** Cisco SD-WAN Manager で設定タスクの進行状況を確認し、エラーメッセージがないか確認します。 **2.** インターコネクトグローバル設定を使用している場合は、選択したソフトウェアイメージがインターコネクト プロバイダーの場所で使用可能かどうかを確認します。 **3.** VM インスタンスが展開されていない場合、または IP プールが使い果たされている場合は、インターコネクト プロバイダーに確認してください。
インターコネクト ゲートウェイの証明書が正常にインストールされない	Cisco SD-WAN Manager のメニューから、**[Maintenance]** > **[Device Reboot]** をクリックします。[Device Reboot] ページで、インターコネクト ゲートウェイを再起動します。
Direct Connect 接続の作成中に、Direct Connect ゲートウェイまたはトランジット ゲートウェイ リストが空になる	**1.** AWS ポータルで、目的の Direct Connect ゲートウェイまたはトランジットゲートウェイが使用可能であることを確認します。 **2.** [Refresh] ボタンをクリックして、AWS からゲートウェイのリストを取得します。 **3.** ゲートウェイが AWS で使用できない場合は、Cisco SD-WAN Manager からゲートウェイを作成します。
Direct Connect 接続の作成中に、ホスト VPC タグがリストに表示されない	ホスト VPC タグが使用可能であり、インターコネクト接続に対して有効になっていることを確認します。

シナリオ	対処法
Direct Connect 接続の作成に失敗した	1. Cisco SD-WAN Manager で設定タスクの進行状況を確認し、エラーメッセージがないか確認します。 2. インターコネクトグローバル設定を使用している場合は、内部 IP アドレスプールが使い果たされているかどうかを確認します。該当する場合は、一部の接続を削除して再試行します。 3. カスタム設定を使用している場合は、ピアリングに重複する CIDR サブネットを入力していないことを確認します。 4. 接続制限に達しているかどうかを確認します。「Cisco Catalyst SD-WAN Cloud Interconnect with Equinix の使用上の注意」を参照してください。 5. インターコネクト プロバイダー アカウントと AWS アカウントの権限を確認します。
トラフィックフローの問題	1. インバウンドおよびアウトバウンドトラフィックに必要なセキュリティルールがホスト VPC に設定されていることを確認します。 2. 仮想インターフェイスが作成され、Direct Connect ゲートウェイにアタッチされているかどうかを確認します。 3. AWS で、仮想インターフェイスの BGP ピアリングステータスが UP 状態かどうかを確認します。 4. 正しいルートテーブルがホスト VPC のメインルーティングテーブルとして使用されているかどうかと、必要なルートが仮想プライベートゲートウェイまたはトランジットゲートウェイに伝達されているかどうかを確認します。 5. 仮想プライベートゲートウェイまたはトランジットゲートウェイが、Direct Connect ゲートウェイにアタッチされているかどうかを確認します。
遅延の問題	1. インターコネクト ゲートウェイの場所が、接続の作成時に選択した Direct Connect の場所と近いかどうかを確認します。 2. 接続に適切な帯域幅が設定されていることを確認します。

シナリオ	対処法
クラウドゲートウェイがドロップダウンリストに表示されない	必要なクラウドゲートウェイがマルチクラウドワークフローを使用して作成され、このドキュメントに記載されている最小要件が満たされていることを確認します。
クラウドゲートウェイへのインターコネクト接続を作成した後も、VPC または VNET ワークロードへのトラフィックがインターネット経由で送信される	Cisco Catalyst SD-WAN のブランチがインターネットを介してクラウドゲートウェイに接続されていて、同じ VPC または VNET ワークロードにアクセスするためにインターコネクト ゲートウェイからのインターコネクト接続を介して接続されている場合、デフォルトでは、ブランチからのトラフィックはインターネットを介して送信されます。 インターコネクト ゲートウェイを介したプライベートパスを優先パスにするには、ブランチの WAN エッジデバイス、インターコネクト ゲートウェイ、およびクラウドゲートウェイに適切な制御ポリシーとデータポリシーを適用します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。