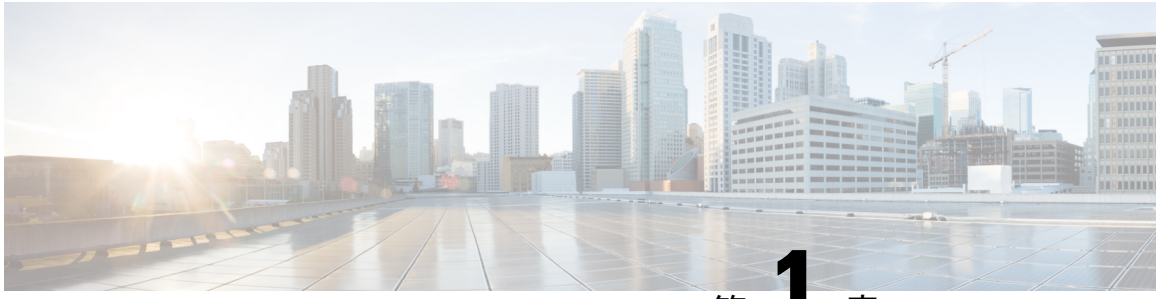
Cisco SD-WAN マルチリージョン ファブリック（階層型 SD-WAN）コンフィギュレーション ガイド

初版：2022 年 4 月 22 日

最終更新：2022 年 9 月 29 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



第 1 章

最初にお読みください

参考資料

- 『Release Notes』[英語]
- 『Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations』[英語]

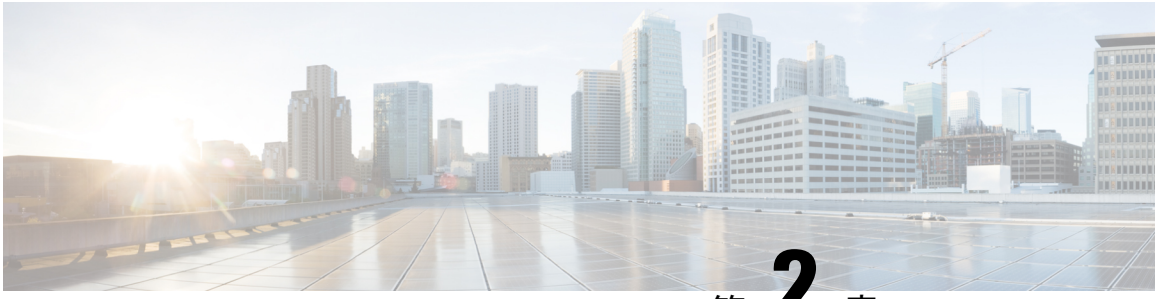
ユーザマニュアル

通信、サービス、およびその他の情報

- Cisco Profile Manager で、シスコの E メールニュースレターおよびその他の情報にサインアップしてください。
- ネットワーク運用の信頼性を高めるための最新のテクニカルサービス、アドバンストサービス、リモートサービスについては、シスコサービスにアクセスしてください。
- 安全かつ検証されたエンタープライズクラスのアプリ、製品、ソリューション、サービスをお求めの場合は、CiscoDevnet にアクセスしてください。
- Cisco Press 出版社による一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。
- リリースで未解決および解決済みのバグをご覧になる場合は、Cisco Bug Search Toolにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 2 章

Cisco IOS XE（SD-WAN）および Cisco SD-WAN リリースにおける新機能

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

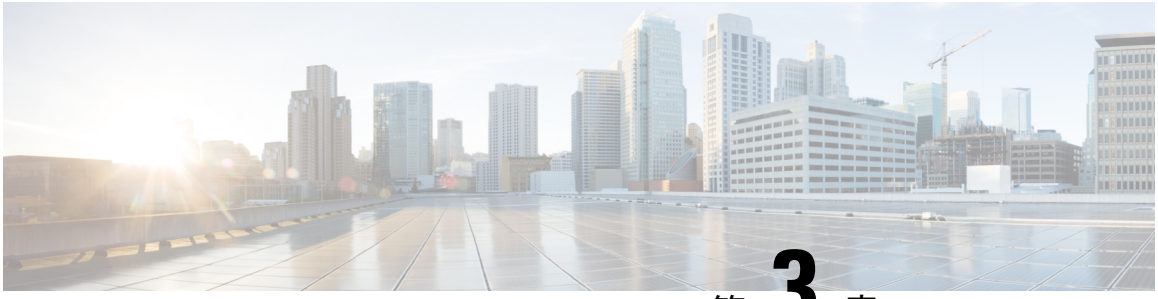
シスコでは、リリースごとに SD-WAN ソリューションを継続的に強化しています。また、コンテンツも最新の強化に合致したものとなるように努めています。次のリンクには、コンフィギュレーションガイド、コマンドリファレンスガイド、およびハードウェア設置ガイドに記載されているリリースごとの新機能と変更された機能が含まれています。Cisco SD-WAN ソリューションに関係する追加機能と修正については、リリースノートの「解決されたバグおよび未解決のバグ」セクションを参照してください。

『What's New in Cisco IOS XE (SD-WAN) Release 17.x』[英語]

『What's New in Cisco IOS XE SD-WAN Release 16.x』[英語]

『What's New in Cisco SD-WAN (vEdge) Release 20.x』[英語]

『What's New in Cisco SD-WAN (vEdge) Release 19.x』[英語]



第 3 章

Cisco SD-WAN マルチリージョン ファブリック

表 *1 :* 機能の履歴

機能名	リリース情報	説明
マルチリージョン ファブリック（階層型 SD-WAN も同様）	Cisco vManage リリース 20.7.1	Cisco SD-WAN マルチリージョン ファブリック は Cisco SD-WAN オーバーレイネットワークのアーキテクチャを、互いに区別して動作する複数のリージョンネットワークと、リージョン間のトラフィックを管理するための中央のコアリージョンネットワークに分割する機能を提供します。 階層型アーキテクチャにより、リージョンごと、および中央のコアリージョンネットワークに異なるトラフィック トランスポート サービス プロバイダーを使用して、コストパフォーマンスとトラフィック パフォーマンスを最適化できます。また、一部のシナリオのトラフィック構成を簡素化し、特定のネットワークシナリオでのルーティング障害を防ぐのに役立つ堅牢で適応性のあるトポロジを提供します。

機能名	リリース情報	説明
再発信ダンプニング	Cisco IOS XE リリース 17.9.1a	ネットワークが不安定になると、TLOC と双方向フォワーディング検出（BFD）トンネルが使用可能と使用不可の間で繰り返し切り替わります。これにより、オーバーレイ マネジメント プロトコル（OMP）がルートの取り消しと再発信を繰り返します。このような動きは、Cisco vSmart コントローラ のパフォーマンスに悪影響を与える可能性があります。 繰り返しダウンしたルートを再発信する前に遅延を追加することで、過度の揺れ動きを防ぎ、この種のネットワークの不安定性による Cisco vSmart コントローラ のパフォーマンスの低下を防ぎます。

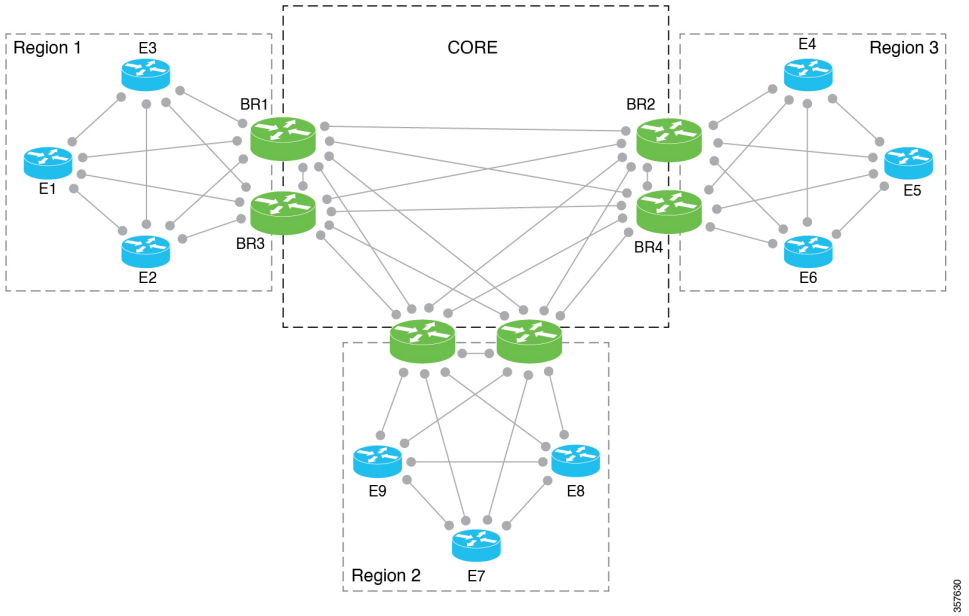
マルチリージョン ファブリックの詳細

マルチリージョン ファブリック（以前の階層 SD-WAN）は、Cisco SD-WAN オーバーレイネットワークのアーキテクチャを次のように分割するオプションを提供します。

- コア オーバーレイ ネットワーク：リージョン 0 と呼ばれるこのネットワークは、リージョンオーバーレイに接続して相互に接続する境界ルータ（下の図の BR）で構成されます。
- 1 つ以上のリージョン オーバーレイ ネットワーク：各リージョンネットワークは、同じリージョン内の他のエッジルータに接続するエッジルータで構成され、そのリージョンに割り当てられているコアリージョン境界ルータに接続できます。

次の図は、6 つの境界ルータ（BR1 ～ BR6）を持つコア オーバーレイ ネットワークを示していて、3 つのリージョンのそれぞれに 2 つが割り当てられています。3 つのリージョン オーバーレイ ネットワークでは、エッジルータは、同じリージョン内の他のエッジルータ、またはリージョンに割り当てられたコア境界ルータにのみ接続します。

図 *1*: マルチリージョン ファブリック のアーキテクチャ



リージョン内およびリージョン間のトラフィック

リージョンに分割することにより、リージョン内トラフィックとリージョン間トラフィックが区別されます。

- リージョン内トラフィック：エッジルータは、リージョン内の他のエッジルータに直接接続します。

  トラフィックは、送信元デバイスと宛先デバイス間のダイレクトトンネルを通過します。

- リージョン間トラフィック：あるリージョンのエッジルータは、別のリージョンのエッジルータに直接接続しません。リージョン間トラフィックの場合、エッジルータはコア境界ルータに接続して、ターゲットリージョンに割り当てられたコア境界ルータにトラフィックを転送し、これらの境界ルータはトラフィックをターゲットリージョン内のエッジルータに転送します。

  トラフィックは、送信元デバイスと宛先デバイスの間の 3 つのトンネルを通過します。

細分化された転送

マルチリージョン ファブリック の重要な原則は、リージョンとコアリージョンネットワークを定義した後、各リージョンおよびコアリージョンネットワークが、異なるトラフィック トランスポート サービスを使用するように調整できることです。

一般的なユースケースでは、コアリージョンは、地理的に離れたリージョン間のトラフィックに使用されます。このシナリオでは、コアリージョンはプレミアム トランスポート サービスを使用して、長距離接続に必要なレベルのパフォーマンスと費用対効果を提供します。

ネットワーク トポロジ

マルチリージョン ファブリック は、さまざまなリージョンでさまざまなネットワークトポロジを使用できる柔軟性を提供します。たとえば、リージョン 1 は Cisco SD-WAN トンネルのフルメッシュを使用でき、リージョン 2 はハブアンドスポークトポロジを使用でき、リージョン 3 はダイナミックトンネルでフルメッシュトポロジを使用できます。

コアリージョン（リージョン 0）のオーバーレイトポロジには、トンネルのフルメッシュを使用することをお勧めします。これは、コアリージョン内の各境界ルータが、コア内の他の境界ルータへのトンネルを必要とすることを意味します。これらのダイレクトトンネルは、あるリージョンから別のリージョンにトラフィックを転送するための最適な接続を提供します。

フルメッシュトポロジの実装により、コア オーバーレイ ネットワーク内のルーティングの複雑さが最小限に抑えられます。対照的に、部分メッシュトポロジでは、リージョン間パスを計算するためにトポロジを認識したルーティングが必要になります。スケーリングの制限については、マルチリージョン ファブリック の制約事項 （12 ページ）を参照してください。

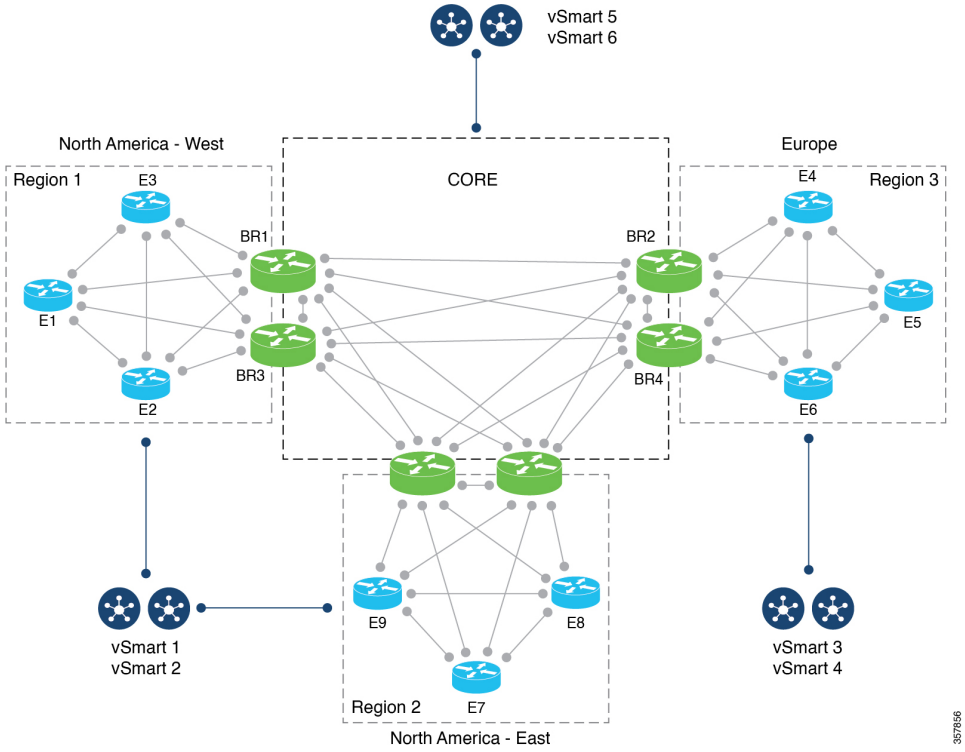
分散型 Cisco vSmart コントローラ

マルチリージョン ファブリック は Cisco vSmart コントローラ を割り当てて、特定のリージョンにサービスを提供できます。組織のネットワークに含まれるデバイスの数が少ない場合は、1 台の Cisco vSmart コントローラ、または通常は 2 台の Cisco vSmart コントローラ でネットワーク内のすべてのリージョンにサービスを提供できます。デバイスの数が多い場合は、特定のリージョンにサービスを提供するために Cisco vSmart コントローラ を割り当てることをお勧めします。

以下の例については、次の点に注意してください。

- Cisco vSmart コントローラ の 1 と 2 はリージョン 1 と 2 にサービスを提供します。
- Cisco vSmart コントローラ の 3 と 4 はリージョン 3 にサービスを提供します。
- Cisco vSmart コントローラ の 5 と 6 はコアリージョン（リージョン 0）にサービスを提供します。

図 *2 : Cisco vSmart* コントローラ がさまざまなリージョンにサービスを提供



（注） Cisco vSmart コントローラ の制約事項については、マルチリージョン ファブリック の制約事項 （12 ページ）を参照してください。

再発信ダンプニング

最小リリース：Cisco IOS XE リリース 17.9.1a

ネットワークが不安定になると、TLOC と双方向フォワーディング検出（BFD）トンネルが使用可能と使用不可の間で繰り返し切り替わります。このタイプのネットワークの安定性には、次のようなさまざまな原因が考えられます。

- 物理接続の機能不全
- 接続を妨げるネットワークの問題
- 携帯電話ネットワークの弱い信号

使用可能と使用不可が切り替わると、境界ルータとトランスポートゲートウェイで動作するオーバーレイ マネジメント プロトコル（OMP）が、使用不可になったルートを繰り返し取り消し、再び使用可能になったときにルートを再発信する可能性があります。この繰り返し切り替わる動きは、ネットワークを管理している Cisco vSmart コントローラ に伝播し、Cisco vSmart コントローラ リソースに対する不必要な要求を作成し、パフォーマンスを低下させます。

ネットワークの不安定性による Cisco vSmart コントローラ のパフォーマンスの低下を防ぐために、Cisco IOS XE リリース 17.9.1a から、境界ルータとトランスポートゲートウェイがネットワークの安定性に関する繰り返しの問題を検出すると、ルートが利用可能になってからルートを再発信するまでに、遅延が導入されています。これにより、Cisco vSmart コントローラ の不要な負荷が軽減され、コントロールプレーンが安定します。

再発信ダンプニングはデフォルトで有効になっていて、設定は必要ありません。

マルチリージョン ファブリックの利点

- 簡素化されたポリシー設計
- ポリシーによって引き起こされる特定のトラフィックルーティング障害、具体的には、トラフィックフローの送信元と宛先の間のホップの 1 つを担当するデバイスが使用できない場合に発生する可能性のあるルーティング障害の防止
- リージョン間トラフィックのエンドツーエンドの暗号化
- リージョンごとに最適なトランスポートを選択できる柔軟性

  この柔軟性により、地理的リージョン全体のトラフィックのパフォーマンスが向上します。一般的なユースケースでは、組織はコアリージョンにプレミアム トラフィック トランスポートを使用するように調整し、地理的に離れたリージョン全体でより優れたトラフィックパフォーマンスを提供します。
- ドメイン間のトラフィックパスのより適切な制御

  一部のシナリオでは、地理的リージョン間など、ドメイン間でトラフィックをルーティングする方法を制御することが有利です。マルチリージョン ファブリック アーキテクチャはこれを簡素化します。

  これがどのように役立つかの例については、マルチリージョン ファブリック の使用例（15 ページ）の「ドメイン間のトラフィックパスの制御」を参照してください。
- ばらばらなプロバイダー間のサイト間トラフィックパスの有効化

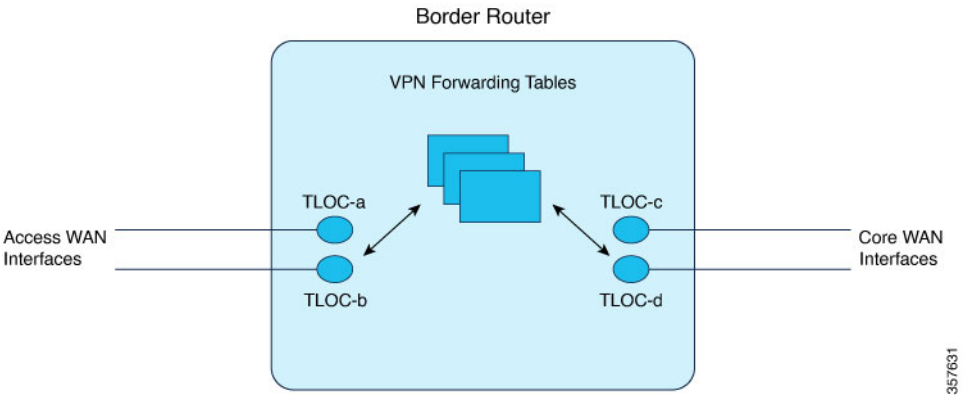
  マルチリージョン ファブリック アーキテクチャはエッジルータと境界ルータ間を分離します。これにより、ばらばらなプロバイダー（プロバイダー間でダイレクト IP ルーティングの到達可能性を提供できない 2 つのプロバイダー）間でサイト間トラフィックパスを確立できます。各サイトがコアリージョン境界ルータに接続している場合、コアリージョンネットワークは 2 つのサイト間の接続を提供できます。

  コアリージョンネットワークは、各境界ルータに次の機能があるため、この接続を提供できます。

  - リージョンのエッジルータに接続するための（1 つ以上の）WAN インターフェイスのセット
  - コアリージョン内の接続用の個別の WAN インターフェイスセット

境界ルータは、VPN 転送テーブルを使用して、2 組の WAN インターフェイス間でトラフィックフローをルーティングします。

図 3: ばらばらなプロバイダー



- 最適化されたトンネルのカプセル化

  コアリージョンとリージョンネットワークには、さまざまなタイプのトンネルのカプセル化を使用できます。

  たとえば、リージョンエッジルータとコア境界ルータの間で、暗号化された IPsec トンネルのカプセル化を使用できます。コアリージョンインフラストラクチャで暗号化が必要ない場合は、コアリージョン内のトンネルに Generic Routing Encapsulation（GRE）を使用して、スループットを向上させることができます。リージョンごとに最適なトンネルのカプセル化方式を選択する利点は、リージョン間トラフィックのパフォーマンスが向上することです。

マルチリージョン ファブリック でサポートされるデバイス

- エッジルータのロール：すべての Cisco IOS XE SD-WAN デバイス、すべての Cisco vEdge デバイス
- 境界ルータのロール：すべての Cisco IOS XE SD-WAN デバイス

マルチリージョン ファブリック の前提条件

- Cisco IOS XE SD-WAN デバイス の最小ソフトウェアバージョン：Cisco IOS XE リリース 17.7.1a
- Cisco vEdge デバイス の最小ソフトウェアバージョン：Cisco SD-WAN リリース 20.7.1

マルチリージョン ファブリック の制約事項

一般的な制約事項

- マルチリージョン ファブリック を使用するようにネットワーク内のデバイスを構成する（各デバイスにリージョンを割り当てる）場合、マルチリージョン ファブリック を使用するようにネットワーク内のすべてのデバイスを構成する必要があります。マルチリージョン ファブリック 用に構成されていないデバイスは、マルチリージョン ファブリック 用に構成されているデバイスに接続できません。

（注） この制限により、既存のネットワークに対して マルチリージョン ファブリック を有効にするプロセスは、ネットワーク内のデバイス間の接続を一時的に中断する可能性があります。

- マルチリージョン ファブリック コアリージョンネットワークにはフルメッシュトポロジを使用し、コアリージョンの各境界ルータからコアの他の境界ルータへのトンネルを使用することをお勧めします。これには、構成が単純になるという利点がありますが、コアリージョン内の境界ルータの数をスケーリングする機能が制限されます。
- Cisco IOS XE SD-WAN デバイス のみが境界ルータロールを持つことができます。

（注） エッジルータと境界ルータの用語の説明については、マルチリージョン ファブリックの詳細 （6 ページ）を参照してください。

- 境界ルータは、1 つのアクセスリージョンにだけサービスを提供できます（コアリージョン以外のリージョンをアクセスリージョンと呼びます）。

ルーティングの制約事項

マルチリージョン ファブリック は、次のルーティング機能をサポートしていません。

- エンドツーエンドの SLA 対応ルーティング
- エッジルータと境界ルータのマルチテナントサポート
- 境界ルータでのオーバーレイ マネジメント プロトコル（OMP）ルート集約
- オーバーレイでの IP マルチキャストのサポート

- リージョンごとの SLA ポリシー。境界ルータは、他のリージョンの SLA 構成に関係なく、常にそのリージョンの SLA ポリシーを他のリージョンとの間のトラフィックに適用します。
- 境界ルータのバックアップパス選択による高速コンバージェンス

Cisco vSmart コントローラ の制約事項

- リージョン 0 の制限：Cisco vSmart コントローラ をコアリージョン（リージョン 0）ネットワークに割り当てると、他のリージョンに割り当てることはできません。
- リージョンパリティ：Cisco vSmart コントローラ は複数のリージョンにサービスを提供できます。2 つの Cisco vSmart コントローラ を構成していずれか 1 つのリージョンに共通にサービスを提供する場合、それらのコントローラはすべての同じリージョンにサービスを提供する必要があります。それらは、リージョンのカバレッジにおいて部分的にのみ重複することはできません。

  次の例は、Cisco vSmart コントローラ の有効なシナリオと無効なシナリオを示しています。

  - 有効（重複しない）：

    コントローラ A はリージョン 1 にサービスを提供します。
    コントローラ B はリージョン 2 にサービスを提供します。

  - 有効（1 つのリージョンに重複）：

    コントローラ A はリージョン 1 にサービスを提供します。
    コントローラ B はリージョン 1 にサービスを提供します。

  - 有効（複数のリージョンに重複）：

    コントローラ A は、リージョン 1、2、および 3 にサービスを提供します。
    コントローラ B は、リージョン 1、2、および 3 にサービスを提供します。

  - 無効（部分的にリージョンに重複）：

    コントローラ A は、リージョン 1、2、および 3 にサービスを提供します。
    コントローラ B は、リージョン 1 と 2 のみにサービスを提供します。

スケール制限

（注） ここで説明するスケール制限は、マルチリージョン ファブリック の機能に関するものです。ネットワーク構成には、他の制限が適用される場合があります。

マルチリージョン ファブリック には、次のスケール制限があります。

アイテム	サポートされるスケール
リージョンとルータ	
リージョンの最大数	8 Cisco IOS XE リリース 17.8.1a および Cisco SD-WAN リリース 20.8.1 から：12
リージョンあたりのエッジルータの最大数	1,000
オーバーレイ内のすべてのリージョンにわたるエッジルータの最大数	5,500 Cisco IOS XE リリース 17.8.1a および Cisco SD-WAN リリース 20.8.1 から：6,800
リージョンあたりの境界ルータの最大数	4
オーバーレイ内の一意のユニキャストプレフィックス	50,000 Cisco IOS XE リリース 17.8.1a および Cisco SD-WAN リリース 20.8.1 から：100,000
インターフェイスの制限	
境界ルータの場合、コアリージョン内の TLOC の最大数	2
境界ルータの場合、アクセストラフィック（境界ルータとエッジルータ間のトラフィック）の TLOC の数	2 つ以上
コントローラの制限	
リージョンに割り当てることができる Cisco vSmart コントローラ の最大数	2
Cisco vManage インスタンスの最大数	3 Cisco IOS XE リリース 17.8.1a および Cisco SD-WAN リリース 20.8.1 から：6
Cisco vBond オーケストレーションインスタンスの最大数	2 Cisco IOS XE リリース 17.8.1a および Cisco SD-WAN リリース 20.8.1 から：4
コアリージョン（リージョン0）に割り当てられる Cisco vSmart コントローラ の最大数	2
Cisco vSmart コントローラ がサービスを提供できるリージョンの最大数	7

アイテム	サポートされるスケール
リージョンに割り当てることができる Cisco vSmart コントローラ の最大数	2

マルチリージョン ファブリック の使用例

ドメイン間のトラフィックパスの制御

マルチリージョン ファブリック の利点の 1 つは、個々のリージョンネットワークとコアリージョンが分離されていることです。これらのコンポーネントネットワークはそれぞれ、異なるタイプのルーティングインフラストラクチャ、異なるサービスプロバイダー、および異なるトラフィックポリシーセットを採用できます。

一部のシナリオでは、リージョン内トラフィックとリージョン間トラフィックに異なるタイプのトラフィックトランスポートを使用することが有利です。たとえば、適切なコストで必要なパフォーマンスを提供するために、リージョン間トラフィックにのみ特定のトランスポートサービスを使用する場合があります。マルチリージョン ファブリック アーキテクチャ内のコンポーネントネットワークの分離により、これを達成するために必要な構成が簡素化されます。

たとえば、北米で事業を行っている組織が西海岸にも東海岸にもオフィスとネットワークインフラストラクチャを持っている場合、これら2つのリージョンで異なるサービスプロバイダーを使用して、リージョン内のトラフィックをサポートする場合があります。これらのサービスプロバイダーは、西海岸と東海岸の間のリージョン間トラフィックに最適なコストやパフォーマンスを提供しない場合があります。

マルチリージョン ファブリック を利用しない場合の 1 つのアプローチは次のとおりです。

- 西海岸リージョンにクラウド サービス ゲートウェイを作成します。
- 東海岸リージョンに別のクラウド サービス ゲートウェイを作成します。
- 2 つのリージョン間のトラフィックについては、西海岸ゲートウェイまたは東海岸ゲートウェイのいずれか最も近い方にトラフィックをルーティングするようにエッジデバイスを構成します。
- 2つのゲートウェイ間の転送については、クラウドサービスプロバイダーに依存します。

マルチリージョン ファブリック を使用すると、コアリージョンを使用して西海岸と東海岸の間のすべてのトラフィックを管理でき、特にコアリージョンに最適なタイプのバックボーンインフラストラクチャを選択して、コストとパフォーマンスの要件を満たすことができます。たとえば、組織は次のものを使用する場合があります。

- 西海岸リージョン内トラフィックのための西海岸リージョン サービス プロバイダー
- 東海岸リージョン内トラフィックのための東海岸リージョン サービス プロバイダー

- バックボーン インフラストラクチャ用のクラウド サービス プロバイダーまたは Cisco SD-WAN Cloud Interconnect

このシナリオで マルチリージョン ファブリック を使用すると、次の利点があります。

- ルーティング構成がはるかに単純です。
- マルチリージョン ファブリック 方法により、特定のルーティング障害が防止されます。特に、トラフィックフローの送信元と宛先の間のホップの1つを担当するデバイスが使用できない場合に発生する可能性のあるルーティング障害です。これらの障害は、より複雑な構成方法のいずれかを使用して、同様の結果を得ようとした場合に発生する可能性があります。これらの中間ホップを管理する マルチリージョン ファブリック コアリージョンは、デバイス障害に対して他の方法（前述のようにリージョンゲートウェイを使用するようにトラフィックを構成するなど）よりも応答性が高く、そのようなトラフィックを再ルーティングしてルーティング障害を回避します。

一般に、このトランスポートプロバイダーの細分化により、組織のネットワークの各リージョンセグメントを運用するためのコストとパフォーマンスを最適化できます。

Cisco vManage を使用した マルチリージョン ファブリック の設定

はじめる前に

リージョンとロールの割り当てを開始して マルチリージョン ファブリック を構成する前に、以下を確認してください。

（注） 既存のネットワークに対して マルチリージョン ファブリック を有効にするプロセスは、ネットワーク内のデバイス間の接続を一時的に中断する可能性があります。『マルチリージョン ファブリック の制約事項 （12 ページ）』を参照してください。

1. ネットワークに階層型アーキテクチャが必要かどうかを判断する：エンタープライズ ネットワークが 1 つの地理的リージョンに限定されていて、ネットワーク内のすべてのポイント間のトラフィックに対して 1 つのタイプのトラフィック トランスポートで十分な場合は、マルチリージョン ファブリック を採用する必要はありません。フラットネットワークは、このようなネットワーク要件に対応できます。
2. リージョンを計画する：階層型アーキテクチャを計画するときは、各リージョンにどのデバイスを含めるかを決定します。さらに、境界ルータとして使用するデバイスを含め、コアリージョンを計画します。どの Cisco vSmart コントローラ が各リージョンにサービスを提供するかを計画します。マルチリージョン ファブリック アーキテクチャの例については、マルチリージョン ファブリックの詳細 （6 ページ）を参照してください。

3. 粒度：リージョンを計画するときは、組織のネットワーク要件に対応する粒度のレベルを適用します。たとえば、北米のリージョンを計画している場合で、組織のオフィスが西海岸と東海岸のリージョンにのみ配置されている場合は、西海岸と東海岸のみを使用すれば十分かもしれません。ただし、組織がカナダにオフィスを持ち、その地域のサービスプロバイダーを使用している場合は、カナダ用の別のリージョンを含める必要があるかもしれません。

4. コアリージョンネットワーク要件：通常、コアリージョンは、離れたリージョン間のプレミアムレベルのトランスポートを提供します。このことを考慮して、トラフィックがコアリージョンに入るのに最も効果的な場所を決定します。これは、多くの場合、組織のネットワークに含まれる地理的リージョンと、離れたリージョン間で使用する予定のトランスポートのタイプに依存します。

   次の例でさまざまなコアリージョン要件を検討してください。

   - 例 1：北米

     北米にまたがるエンタープライズ ネットワークの場合、プレミアム トランスポート サービスを使用して、東海岸と西海岸のリージョン間のトラフィックトランスポートを管理するのに、コアリージョンを使用する場合があります。この場合、西海岸で発信されたトラフィックは、コアリージョンの外で東海岸を通過するのではなく、西海岸のコアリージョン境界ルータにルーティングされる必要があります。同様に、東海岸で発信されたトラフィックは、東海岸のコアリージョン境界ルータにルーティングされる必要があります。

   - 例 2：北米およびヨーロッパ

     北米とヨーロッパにまたがるエンタープライズ ネットワークの場合、大陸間のトラフィックに最適なトランスポートサービスを使用して、北米とヨーロッパ間のトラフィックトランスポートのみを管理するのに、コアリージョンを使用する場合があります。この場合、西海岸で発信されたトラフィックは、北米の任意の境界ルータを介してコアリージョンに入ることが許容される場合があります。同様に、ヨーロッパのどこからでも発信されたトラフィックは、ヨーロッパのコアリージョン境界ルータにルーティングされます。

マルチリージョン ファブリック を有効にする

1. Cisco vManage メニューから、**[Administration]** > **[Settings]** を選択します。
2. [Multi-Region Fabric] 領域で、マルチリージョン ファブリック を有効にします。

（注） Cisco vManage リリース 20.7.x および 20.8.x では、この領域は [Hierarchical SDWAN] とラベル付けされていました。

Cisco vManage を使用したデバイスへのロールとリージョンの割り当て

はじめる前に

- マルチリージョン ファブリック アーキテクチャを計画し、ネットワーク内の各デバイスのロール（エッジルータまたは境界ルータ）とリージョンを決定します。
- この手順では、機能テンプレートを使用してロールを割り当てます。テンプレートを使用したデバイスの構成の詳細については、「Configure Devices」を参照してください。
- 各デバイスでサポートされるインターフェイスの数については、マルチリージョン ファブリック の制約事項 （12 ページ）の「スケール制限」を参照してください。
- Cisco vManage リリース 20.9.1 から、ネットワーク階層およびリソース管理を使用して、次の手順で使用するリージョンを作成します。リージョンの作成には、リージョン ID のリージョンへの割り当てが含まれます。リージョンの作成については、『Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x』の「Network Hierarchy and Resource Management」の章を参照してください。

デバイスへのロールとリージョンの割り当て

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] は [Feature] と呼ばれます。

3. [Add template] をクリックします。
4. デバイスタイプを選択して、デバイスで使用可能なテンプレートを表示します。
5. [System] テンプレートをクリックします。
6. [Template Name] フィールドに、テンプレートの名前を入力します。
7. [Basic Configuration] セクションで、次のフィールドを設定します。

フィールド	説明
Region ID	リージョンに 1 から 63 までの値を選択します。 （注） Cisco vManage リリース 20.9.1 から、「はじめる前に」で説明されているように、ネットワーク階層とリソース管理を使用してデバイス用に作成したリージョンの番号を入力します。 （注） デフォルトでは、デバイス上のすべてのインターフェイスは、ここで構成されたリージョンを使用します。 境界ルータの場合、コアリージョンに接続する 1 つ以上の TLOC インターフェイスを設定します。境界ルータのその他の TLOC インターフェイスは、ここで設定されたリージョンを使用します。「Cisco vManage を使用したコアリージョンへの境界ルータ TLOC の割り当て」を参照してください。
Role	[Edge Router] または [Border Router] を選択します。 （注） Cisco IOS XE SD-WAN デバイス のみが [Border Router] ロールを持つことができます。

8. 境界ルータの場合、デバイスがコアリージョンで機能できるようにします。
   1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
   2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] は [Feature] と呼ばれます。

   3. [Add template] をクリックします。
   4. デバイスタイプを選択して、デバイスで使用可能なテンプレートを表示します。
   5. [Cisco VPN Interface Ethernet] テンプレートをクリックします。
   6. [Tunnel] セクションの [Tunnel Interface] フィールドで、[On] をクリックしてトンネルを有効にします。
   7. [Enable Core Region] フィールドで [On] をクリックして、コアリージョンへの接続を有効にします。

Cisco vManage を使用したコアリージョンへの境界ルータ TLOC の割り当て

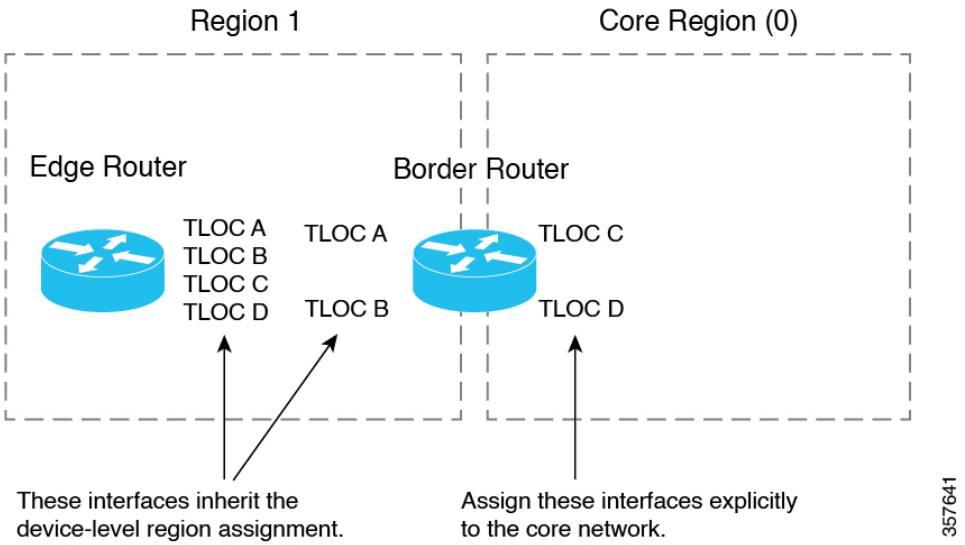
はじめる前に

- デバイスに境界ルータのロールを割り当て、デバイスをリージョンに割り当てます。デフォルトでは、デバイス上のすべてのインターフェイスは、デバイス用に構成されたリージョンを使用します。「Cisco vManage を使用したデバイスへのロールとリージョンの割り当て」を参照してください。

  境界ルータの場合、コアリージョンに接続する 1 つ以上の TLOC インターフェイスを設定します。境界ルータの他の TLOC インターフェイスは、デバイス用に構成されたリージョンを使用します。

- この手順では、指定されたカラーのインターフェイスをコアリージョンに割り当てるテンプレートを作成します。テンプレートを作成する前に、コアリージョンに割り当てるインターフェイスのカラーを設定するか、カラーがすでに設定されていることを確認します。

図 *4: TLOC* インターフェイスリージョンの割り当て



コアリージョンへの境界ルータ TLOC の割り当て

1. コアリージョンに接続する TLOC インターフェイスの Cisco VPN インターフェイス イーサネット テンプレートを作成します。
   1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
   2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] は [Feature] と呼ばれます。

3. [Add template] をクリックします。
4. [Template Name] フィールドに、テンプレートの名前を入力します。
5. [Tunnel] セクションの [Tunnel Interface] フィールドで、[On] をクリックします。
6. [Color] フィールドで、コアリージョンに割り当てるインターフェイスを識別するカラーを指定します。
7. [詳細オプション（Advanced Options）] をクリックします。
8. [Settings] セクションの [Enable Core Region] フィールドで、[On] をクリックします。
9. [Basic Configuration] セクションの [Interface Name] フィールドに、インターフェイス名を入力します。
10. **[保存（Save）]** をクリックします。

2. 前の手順で作成した Cisco VPN インターフェイス イーサネット テンプレートをデバイステンプレートに追加します。
   1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
   2. [Device Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。

   3. [Create Template] をクリックし、[From Feature Template] を選択します。
   4. [Transport & Management VPN] セクションで、[Additional Cisco VPN 0 Templates] リストを見つけて、[Cisco VPN Interface Ethernet] をクリックします。

      これにより、[Transport & Management VPN] セクションに、[Cisco VPN Interface Ethernet] というラベルの付いた新しい行が追加され、インターフェイスを選択するためのメニューが表示されます。
   5. 新しい [Cisco VPN Interface Ethernet] 行で、メニューをクリックし、前の手順で作成した Cisco VPN インターフェイス イーサネット テンプレートを選択します。
   6. [更新（Update）] をクリックします。

3. デバイステンプレートを境界ルータデバイスに適用します。

Cisco vManage を使用したリージョンの Cisco vSmart コントローラ への割り当て

はじめる前に

- マルチリージョン ファブリック アーキテクチャを計画し、ネットワーク内の各デバイスのロール（エッジルータまたは境界ルータ）とリージョンを決定します。どのCisco vSmart コントローラ が各リージョンにサービスを提供するかを計画します。
- この手順では、機能テンプレートを使用してロールを割り当てます。テンプレートを使用したデバイスの構成の詳細については、「Configure Devices」を参照してください。
- Cisco vSmart コントローラ に適用される制限については、「マルチリージョン ファブリック の制約事項 （12 ページ）」を参照してください。

リージョンの Cisco vSmart コントローラ への割り当て

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] は [Feature] と呼ばれます。

3. [Add template] をクリックします。
4. デバイスタイプに [vSmart] を選択します。
5. [System] テンプレートをクリックします。
6. [テンプレート名（Template Name）] フィールドに、テンプレートの名前を入力します。
7. [Basic Configuration] セクションの [Region ID List] フィールドに、リージョンまたはリージョンリストを入力します。
8. テンプレートを Cisco vSmart コントローラ に適用します。

一元化されたポリシーでのリージョンの使用

Cisco vManage を使用したリージョンリストの作成

リージョンリストは、一元化されたポリシーのリージョン一致条件を作成するときに役立ちます。

リージョンリストの作成

1. Cisco vManage メニューで、**[Configuration]** > **[Policies]** を選択します。
2. [Centralized Policy] をクリックします。
3. [Add Policy] をクリックします。
4. リスト領域で、[Region] をクリックします。
5. [New Region List] をクリックします。
6. 次を入力します。
   - [Region List Name]：新しいリストの名前。
   - [Add Region]：1 から 63 の範囲の 1 つ以上のリージョン番号、フィールドの指示を使用します。
7. [Add] をクリックします。

一元化されたポリシーへのリージョン一致条件の追加

マルチリージョン ファブリック のリージョンを構成した後、一元化されたルートポリシーを構成するときに、リージョンまたはリージョンリストを一致条件として指定できます。

一元化されたポリシーの操作の詳細については、を参照してください。

一元化されたポリシーへのリージョン一致条件の追加

1. Cisco vManage メニューから、**[Configuration]** > **[Policies]** を選択します。
2. [Custom Options] をクリックし、[Centralized Policy] セクションで [Topology] を選択します。
3. [Add Topology] をクリックし、[Custom Control] を選択します。
4. [Sequence Type] をクリックし、[Route] を選択します。
5. [Sequence Rule] をクリックします。
6. [Match] をクリックします。
7. [Region] をクリックします。
8. [Match Conditions] 領域で、リージョンまたはリージョンリストを入力します。

   「Cisco vManage を使用したリージョンリストの作成」を参照してください。

一元化されたポリシーのリージョンへの添付

マルチリージョン ファブリック のリージョンを構成した後、一元化されたポリシーを添付するときにリージョンまたはリージョンリストを指定します。

一元化されたポリシーの操作の詳細については、を参照してください。

一元化されたポリシーのリージョンへの添付

1. Cisco vManage メニューから、**[Configuration]** > **[Policies]** を選択します。
2. [Centralized Policy] をクリックします。
3. 表で、添付するポリシーを見つけます。ポリシーの行で [...] をクリックし、[Edit] を選択します。

   [Topology]、[Application-Aware Routing]、および [Traffic Data] オプションについては、新しいサイトまたは新しいリージョンを追加することを選択できます。
4. [New Site/Region List] をクリックします。
5. [Region] をクリックします。
6. リージョン ID またはリージョンリストを入力します。
7. ポリシーの添付に進みます。

CLI を使用した マルチリージョン ファブリック の設定

CLI を使用したデバイスへのロールの割り当て

デバイスで **role** コマンドを使用して、マルチリージョン ファブリック 機能用に、境界ルータのロールを割り当てます。デフォルトのロールはエッジルータです。ロールを境界ルータからエッジルータに変更するには、コマンドの **no** 形式を使用します。

例（境界ルータ）

```
Device#config-transaction
Device(config)#system
Device(config-system)#role border-router
```

例（エッジルータ）

```
Device#config-transaction
Device(config)#system
Device(config-system)#no role border-router
```

CLI を使用したエッジルータ TLOC へのリージョン ID の割り当て

デバイス上のすべての TLOC インターフェイスは、デバイスに割り当てたリージョン ID を継承します。

デバイスで、システム コンフィギュレーション モードを開始し、**region** コマンドを使用してリージョンを割り当てます。

```
Device#config-transaction
Device(config)#system
Device(config-system)#region region
```

例

```
Device#config-transaction
Device(config)#system
Device(config-system)#region 1
```

CLI を使用した境界ルータ TLOC へのリージョン ID の割り当て

デフォルトでは、デバイス上のすべての TLOC は、デバイスに割り当てたリージョン ID を継承します。境界ルータの場合、1 つ以上の TLOC インターフェイスをコアリージョンに明示的に割り当てる必要があります。コア領域に割り当てることができる TLOC の数については、マルチリージョン ファブリック の制約事項 （12 ページ）を参照してください。

1. デバイスで、システム コンフィギュレーション モードを開始し、**region** コマンドを使用してリージョンを割り当てます。

   ```
   Device#config-transaction
   Device(config)#system
   Device(config-system)#region region
   ```

   デフォルトでは、デバイス上のすべてのインターフェイスは、割り当てられたリージョンで動作します。

2. TLOC インターフェイスをコアリージョンに割り当てるには、インターフェイスのインターフェイス コンフィギュレーション モードを開始し、**region core** コマンドを使用します。

   ```
   Device#config-transaction
   Device(config)#sdwan
   Device(config-sdwan)#interface interface
   Device(config-interface-GigabitEthernet1)#tunnel-interface
   Device(config-tunnel-interface)#region core
   ```

例

```
Device#config-transaction
Device(config)#system
Device(config-system)#region 1
Device(config-system)#exit
Device(config)#sdwan
Device(config-sdwan)#interface GigabitEthernet1
Device(config-interface-GigabitEthernet1)#tunnel-interface
Device(config-tunnel-interface)#region core
```

CLI を使用したリージョンの Cisco vSmart コントローラ への割り当て

マルチリージョン ファブリック のセットアップ時に、既存の Cisco vSmart コントローラ をリージョンに割り当てたり、マルチリージョン ファブリック に使用する新しい Cisco vSmart コントローラ を作成したりできます。

コアリージョンのみにサービスを提供するようにプロビジョニングする必要があるコアリージョンCisco vSmartコントローラを除いて、組織のネットワークのすべてのリージョンで同じCisco vSmartコントローラのセットを使用してデバイスにサービスを提供できます。デバイスの数が少ないネットワークでは、これが実現可能な場合があります。ただし、多数のデバイスがあるネットワークの場合は、コントローラを特定のリージョンに割り当てることをお勧めします。

リージョンの Cisco vSmart コントローラ への割り当て

Cisco vSmart コントローラ で、 **region** コマンドを使用して Cisco vSmart コントローラ を 1 つまたは複数のリージョンに割り当てます。

region {*region*} [*region ...*]

例：

この例では、Cisco vSmart コントローラ をリージョン 1 と 2 に割り当てています。

```
vSmart(config-system)#region 1 2
```

マルチリージョン ファブリック の確認

デバイスのロールとリージョン、またはCisco vSmartコントローラの割り当てられたリージョンを確認するには、**show omp summary** および **show control local-properties** コマンドを使用します。

show omp summary

デバイスでこのコマンドを使用して、デバイスロールを表示します。[device-role] フィールドは、[Edge-Router] または [Border-Router] のいずれかを示します。

```
vEdge# show omp summary
oper-state UP
admin-state UP
personality vedge
device-role Edge-Router
...
```

Cisco vSmart コントローラ でこのコマンドを使用して、コントローラが管理するように設定されているリージョンを表示します。[region-id] フィールドは、リージョンのリストを示します。

```
vSmart1# show omp summary
oper-state             UP
admin-state            UP
personality            vsmart
...
vsmart-peers           1
vedge-peers            0
region-id              0 1 2 3 4 5
```

show control local-properties

デバイスでこのコマンドを使用して、各TLOCインターフェイスに設定されているリージョンを表示します。

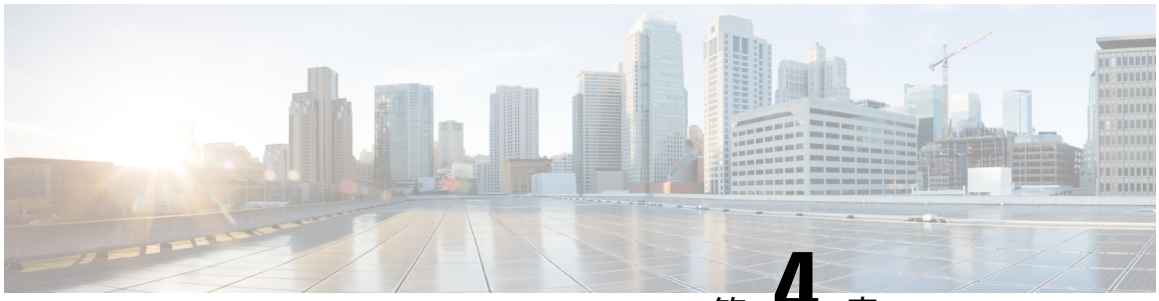
```
Device# show sdwan control local-properties
...
                        PUBLIC      PUBLIC PRIVATE      PRIVATE  PRIVATE
    MAX   RESTRICT/           LAST         SPI TIME    NAT  VM
INTERFACE                IPv4         PORT   IPv4         IPv6     PORT    VS/VM COLOR
STATE CNTRL CONTROL/     LR/LB  CONNECTION   REMAINING   TYPE CON REG

          STUN                                              PRF ID
------------------------------------------------------------------------------------------------------------------------
GigabitEthernet0/0/0     10.0.0.1    12366  10.0.0.1     ::       12366    1/1  public-internet  up
     2     yes/yes/no   No/No  0:00:00:04   0:11:59:27  N    8  0
GigabitEthernet0/0/1     10.0.0.2    12366  10.0.0.2     ::       12366    1/0  green            up
     2      no/yes/no   No/No  0:00:00:07   0:11:57:39  N    5  2
GigabitEthernet0/1/1.10  10.0.0.3    5062   10.0.0.5     ::       12346    1/0  gold             up
     2      no/yes/no  Yes/No  0:00:00:07   0:11:57:41  N    5  2
Loopback300              10.10.0.10  12366  10.10.0.10   ::       12366    0/0  blue             up
     0      no/ no/no   No/No  0:00:10:37   0:11:54:42  N    5  2
```

マルチリージョン ファブリック のモニター

マルチリージョンファブリック構成のステータスを監視するには、次のコマンドを使用して、デバイスリージョン、デバイスロールなどに関する情報を表示します。

コマンド	説明
show control local-properties	デバイスでこのコマンドを使用して、各 TLOC インターフェイスに設定されているリージョンを表示します。
show omp summary	デバイスまたは Cisco vSmart コントローラ でこのコマンドを使用して、リージョン設定、デバイスロールなどを表示します。
show omp routes	デバイスまたは Cisco vSmart コントローラ でこのコマンドを使用して、デバイスまたは Cisco vSmart コントローラ によって管理される各ルートのリージョン情報を表示します。
show bfd sessions	デバイスでこのコマンドを使用して、デバイスの各 BFD セッションのリージョン情報を表示します。



第 4 章

マルチリージョン ファブリックへの移行

表 *2:* 機能の履歴

機能名	リリース情報	説明
マルチリージョン ファブリックへの移行	Cisco IOS XE リリース 17.9.1a Cisco SD-WAN リリース 20.9.1 Cisco vManage リリース 20.9.1	Cisco SD-WAN マルチリージョン ファブリックは、エンタープライズ ネットワークの Cisco SD-WAN への移行を容易にする移行モードを提供します。移行モードにより、マルチリージョン ファブリック ネットワークの一部ではない Cisco vSmart コントローラ からマルチリージョン ファブリック アーキテクチャで動作する Cisco vSmart コントローラ へのデバイスの段階的な移行が可能になります。 移行モードは、マルチリージョンファブリック アーキテクチャと同様に機能する複雑なネットワークを移行する場合に特に役立ちます。つまり、複数のネットワークセグメントがあり、ネットワークハブを介してセグメント間のトラフィックを誘導する制御ポリシーがあります。

マルチリージョン ファブリックへの移行に関する情報

一部のエンタープライズネットワークは論理セグメントに分割され、ハブデバイスを介してセグメント間のトラフィックをルーティングするように構成されています。これらのネットワー

クアーキテクチャは、マルチリージョンファブリック アーキテクチャに似ていて、マルチリージョン ファブリックへの移行にとても適しています。Cisco SD-WAN は、このタイプのネットワークをマルチリージョン ファブリック アーキテクチャに変換するのに役立つ移行モードを提供します。

1 つのユースケースは、複数の地理的リージョンにまたがり、各地理的リージョンを組織の全体的なネットワークアーキテクチャ内のセグメントとして扱う組織です。組織は、Cisco vSmart コントローラで一元化された制御ポリシーを使用して、セグメント間のハブごとのルーティングを構成します。デバイスで移行モードを構成し、ここで説明する手順を使用して、次のことを行います。

- 各セグメントをマルチリージョン ファブリック リージョンに変換する
- 境界ルータをセットアップする
- マルチリージョンファブリック アーキテクチャで動作するように Cisco vSmart コントローラ を割り当てる

マルチリージョン ファブリックに移行するメリット

複数の地理的リージョンにまたがり、各地理的リージョンをネットワークセグメントとして扱う組織の場合、セグメントポリシーの構成は複雑であり、ネットワークが拡大するにつれて複雑さは急速に増します。マルチリージョンファブリックに移行すると、一元化された制御ポリシーのオーバーヘッドが大幅に簡素化されます。マルチリージョンファブリックを使用して簡素化できる複雑な一元化された制御ポリシーの例については、マルチリージョンファブリックへの移行のユースケース （31 ページ）を参照してください。

このセクションで説明する移行手順を使用すると、ネットワーク内の各ルータの機能、およびネットワークトポロジにおける各ルータのロールを維持しながら、ネットワークをマルチリージョン ファブリックに移行できます。

たとえば、非マルチリージョン ファブリック ネットワークの 1 つのセグメントにサービスを提供することに特化したデバイスは、エッジルータのロールを備えたマルチリージョン ファブリック アーキテクチャで引き続きサービスを提供します。非マルチリージョン ファブリック ネットワークでハブとして機能するデバイスは、境界ルータのロールで、マルチリージョン ファブリック アーキテクチャでも引き続き機能します。

マルチリージョンファブリックへの移行でサポートされるデバイス

- エッジルータのロール：すべての Cisco IOS XE SD-WAN デバイス、すべての Cisco vEdge デバイス
- 境界ルータのロール：すべての Cisco IOS XE SD-WAN デバイス

マルチリージョン ファブリックへの移行の前提条件

- アーキテクチャ内の各デバイスのロールを計画します。
- 元のネットワークアーキテクチャのセグメント内で動作する各エッジルータには、マルチリージョン ファブリック アーキテクチャの単一リージョン内でエッジルータとして動作するためのシステム要件があります。
- ハブとして機能する各ルータには、マルチリージョンファブリック境界ルータとして動作するためのシステム要件があります。
- コアリージョンを含む、マルチリージョン ファブリック アーキテクチャの各リージョンにサービスを提供できる Cisco vSmart コントローラ を決定します。

マルチリージョンファブリックへの移行のユースケース

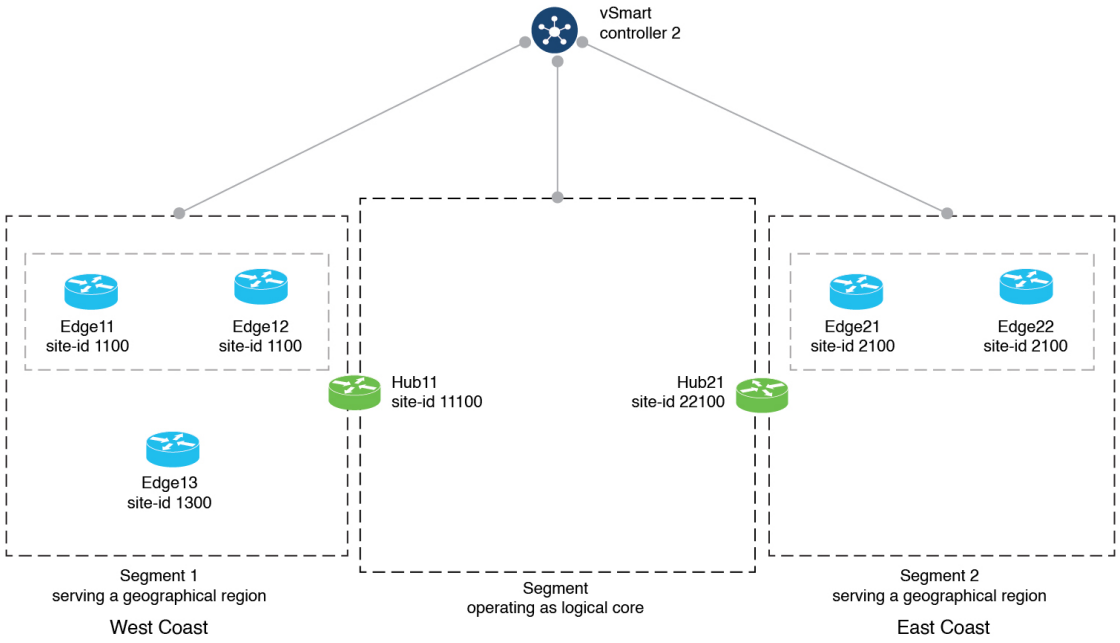
次の例は、マルチリージョン ファブリック アーキテクチャへの移行を計画および実行するための手順についての洞察を提供します。単純化するために、この例には、組織のネットワーク内に少数のルータのみが含まれていて、移行前には単一の Cisco vSmart コントローラ が使用されています。

ユースケースは、複数の地理的リージョンにまたがり、各地理的リージョンをネットワークセグメントとして扱う組織です。セグメント 1 は西海岸にサービスを提供し、セグメント 2 は東海岸にサービスを提供します。2 つのセグメント間のすべてのトラフィックは、各セグメントのハブデバイスを経由します。

移行前と移行後

次の図はネットワークのアーキテクチャを示しています。この例では、1 つの Cisco vSmart コントローラ がネットワーク全体にサービスを提供します。

図 *5:* 移行前のネットワークアーキテクチャ



このネットワークでは、マルチリージョンファブリックへの移行前に、このセクションで後ほど詳しく説明する一元化された制御ポリシーにより、ルータがネットワークセグメント 1 と 2 にクラスタ化され、セグメント 1 のハブルータとセグメント 2 のハブルータが提供されます。ポリシーは次のことを行います。

- 西海岸の地理的リージョンにサービスを提供する、セグメント 1 内のデバイス間のダイレクトルートを有効にします。

  これらには、Edge11、Edge12、Edge13、および Hub11 が含まれます。

- 東海岸の地理的リージョンにサービスを提供する、セグメント 2 内のデバイス間のダイレクトルートを有効にします。

  これらには、Edge21、Edge22、および Hub21 が含まれます。

- 論理コアリージョン内のデバイス間のダイレクトルートを有効にします。

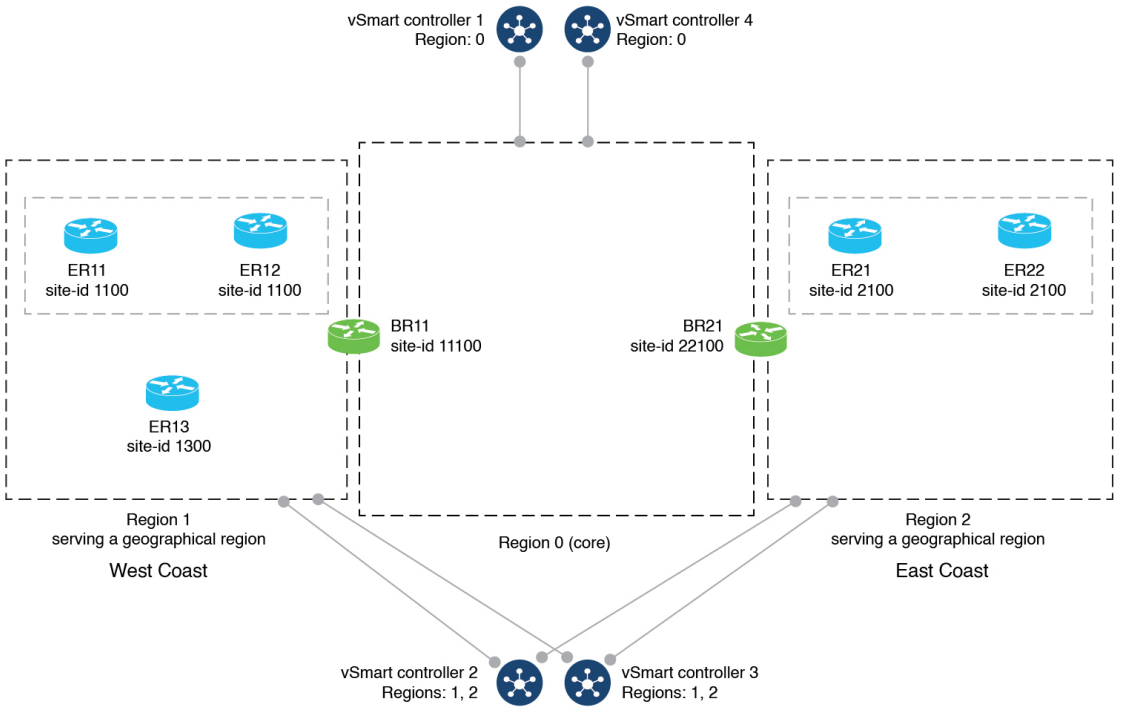
  これらには、Hub11 と Hub21 が含まれます。

- ハブ、および Hub11 と Hub21 を介してリージョン間トラフィックをルーティングします。

マルチリージョンファブリックに移行するために、ネットワーク管理者は、ネットワークアーキテクチャ内の各ルータに期待されるロールとリージョンを計画し、4 つの Cisco vSmart コントローラの使用を計画し、Cisco vManage の手順（Cisco vManage を使用したマルチリージョンファブリックへの移行 （42 ページ））を使用して各ルータを移行します。

次の図は、移行後のネットワークを示しています。

図 *6 :* マルチリージョン ファブリックへの移行後のネットワークアーキテクチャ



前の図に示した移行では、各ルータは引き続きネットワーク内で同様の機能を実行しますが、ルータとセグメントを説明する用語が変更されています。次の表は、移行前と移行後の各ルータに適用される用語を比較したものです。ハブ機能を持つルータは境界ルータになり、ネットワークセグメントはマルチリージョン ファブリック アーキテクチャ内のリージョンとして形式化されます。

地理的リージョン	サイト	移行前のデバイス名と説明	マルチリージョン ファブリックへの移行後のデバイス名と説明
西海岸	1100	Edge11： エッジ ルータ	ER11： エッジルータ、リージョン 1
西海岸	1100	Edge12： エッジ ルータ	ER12： エッジルータ、リージョン 1
西海岸	1300	Edge13： エッジ ルータ	ER13： エッジルータ、リージョン 1

地理的リージョン	サイト	移行前のデバイス名と説明	マルチリージョン ファブリックへの移行後のデバイス名と説明
西海岸	11100	Hub11： ハブルータ	BR11： 境界ルータ、リージョン 1
東海岸	22100	Hub21： ハブ	BR21： 境界ルータ、リージョン 2
東海岸	2100	Edge21： エッジ ルータ	ER21： エッジルータ、リージョン 2
東海岸	2100	Edge22： エッジ ルータ	ER22： エッジルータ、リージョン 2

移行前の制御ポリシー要件

次の表は、（a）ネットワーク セグメンテーション、および（b）ハブを介したセグメント間ルーティングを、マルチリージョンファブリックなしで実現するために必要な複雑な制御ポリシーの例を示しています。このポリシーの例は、同様に構成されたエンタープライズ ネットワークのマルチリージョンファブリックへの移行を計画するときに役立つ可能性があり、マルチリージョンファブリックを使用してこのタイプのネットワーク機能を実現し、ポリシーを大幅に簡素化する利点を示しています。

表で、次の手順について説明します。

- パート A。制御ポリシーで使用するサイト ID のポリシーリストを定義する
- パート B。制御ポリシーで使用する TLOC のポリシーリストを定義する
- パート C。前の表で定義したリストを使用した制御ポリシーを作成して適用する

表 *3 :* パート *A*。制御ポリシーで使用するサイト *ID* のポリシーリストを定義する

ポリシー構成の目的の簡単な説明	詳細な説明	例

1. セグメント 1 のエッジルータを含むリストを定義します。	セグメント 1 のすべてのサイトのサイトリストを定義します。これらのサイトには、セグメント 1 のすべてのエッジルータが含まれます。	`policy`
		` lists`
		`  site-list SEGMENT1`
		`   site-id 1100`
		`   site-id 1300`
		`   !`

	セグメント 1 のすべてのエッジルータのサイトリストと、セグメント 1 のハブサイトを定義します。これらのサイトには、セグメント 1 のすべてのエッジルータとハブルータが含まれます。	`policy`
		` lists`
		`  site-list SEGMENT1_HUB1`
		`   site-id 1100`
		`   site-id 1300`
		`   site-id 11100`
		`   !`

2. セグメント 2 のエッジルータを含むリストを定義します。	セグメント 2 のすべてのサイトのサイトリストを定義します。これらのサイトには、セグメント 2 のすべてのエッジルータが含まれます。	`policy`
		` lists`
		`  site-list SEGMENT2`
		`   site-id 2100`
		`   !`

	セグメント 2 のすべてのエッジルータのサイトリストと、セグメント 2 のハブサイトを定義します。これらのサイトには、セグメント 2 のすべてのエッジルータとハブルータが含まれます。	`policy`
		` lists`
		`  site-list SEGMENT2_HUB2`
		`   site-id 2100`
		`   site-id 22100`
		`   !`

3. セグメント 1 の発信トラフィックの制御ポリシーを作成するときに役立つセグメント 2 の宛先のリストを定義します。	次のリストを定義します。
	• セグメント 2 のすべてのエッジルータ
	• セグメント 2 のハブサイト
	• セグメント 1 のハブサイト
		`policy`
		` lists`
		`   site-list HUB1_HUB2_SEGMENT2`
		`   site-id 11100`
		`   site-id 2100`
		`   site-id 22100`
		`   !`

ポリシー構成の目的の簡単な説明	詳細な説明	例
4. セグメント 2 の発信トラフィックの制御ポリシーを作成するときに役立つセグメント 1 の宛先のリストを定義します。	次のリストを定義します。 • セグメント 1 のすべてのエッジルータ • セグメント 1 のハブサイト • セグメント 2 のハブサイト	policy lists site-list HUB1_HUB2_SEGMENT1 site-id 1100 site-id 11100 site-id 1300 site-id 22100 !
5. セグメント 1 のルータのリストと、セグメント 2 のハブルータを定義します。これは、セグメント 1 のハブルータの制御ポリシーを作成するときに役立ちます。	次のリストを定義します。 • セグメント 1 のすべてのエッジルータ • セグメント 2 のハブサイト	policy lists site-list SEGMENT1_HUB2 site-id 1100 site-id 1300 site-id 22100 !
6. セグメント 2 のルータのリストと、セグメント 1 のハブルータを定義します。これは、セグメント 2 のハブルータの制御ポリシーを作成するときに役立ちます。	次のリストを定義します。 • セグメント 2 のすべてのエッジルータ • セグメント 1 のハブサイト	policy lists site-list HUB1_SEGMENT2 site-id 11100 site-id 2100 !

表 *4:* パート *B*。制御ポリシーで使用する *TLOC* のポリシーリストを定義する

ポリシー構成の目的の簡単な説明	詳細な説明	例
1. ハブ間のトラフィックの TLOC のリストを定義します。 （ネットワークがマルチリージョン ファブリックに移行されると、このハブ間トラフィックがコアリージョントラフィックを構成します。）	• Hub21 から Hub11 へのトラフィックの TLOC のリスト（HUB1_CORE_TLOC）を定義します。 • Hub11 から Hub21 へのトラフィックの TLOC のリスト（HUB2_CORE_TLOC）を定義します。	policy lists tloc-list HUB1_CORE_TLOC tloc 172.16.11.10 color green encap ipsec ! tloc-list HUB2_CORE_TLOC tloc 172.17.13.10 color green encap ipsec !

ポリシー構成の目的の簡単な説明	詳細な説明	例
2. ハブと、それらがサービスを提供しているセグメント内のルータとの間のトラフィックの TLOC のリストを定義します。 （ネットワークがマルチリージョン ファブリックに移行されると、これがアクセス リージョン トラフィックを構成します。）	• Hub11 と、ハブとして機能するセグメント 1 のルータとの間のトラフィックの TLOC のリスト（HUB1_TLOCS）を定義します。 • Hub21 と、ハブとして機能するセグメント 2 のルータとの間のトラフィックの TLOC のリスト（HUB2_TLOCS）を定義します。	policy lists tloc-list HUB1_TLOCS tloc 172.16.11.10 color lte encap ipsec tloc 172.16.11.10 color 3g encap ipsec tloc 172.16.11.10 color red encap ipsec tloc 172.16.11.10 color green encap ipsec ! tloc-list HUB2_TLOCS tloc 172.17.13.10 color lte encap ipsec tloc 172.17.13.10 color 3g encap ipsec tloc 172.17.13.10 color green encap ipsec !

表 *5:* パート *C*。前の表で定義したリストを使用した制御ポリシーを作成して適用する

ポリシー構成の目的の簡単な説明	詳細な説明	例
1.（a）セグメント 1 内のルータが互いにトラフィックを直接送信できるようにする、および（b）セグメント 2 宛てのすべてのトラフィックが最初のホップとして Hub11 を使用するように指示する、セグメント 1 の制御ポリシーを作成します。このようにして、Hub11 はセグメント 2 へのトラフィックのハブとして機能します。	CP1 という制御ポリシーを作成して、次のことを行います。 • シーケンス 1：セグメント 1 のすべてのデバイスに、セグメント 1 の他のデバイスの TLOC へのアクセスを提供します。これには、エッジルータとハブルータが含まれます。これにより、セグメント 1 にフルメッシュ接続が作成されます。 • シーケンス 2：宛先が Hub11 またはセグメント 2 のデバイスのいずれかであるセグメント 1 のすべてのトラフィックについて、最初のホップが Hub11 である必要があることを確認します。 • シーケンス 3：セグメント 1 内のすべてのトラフィックについて、デバイスがトラフィックをリージョン内の宛先デバイスに直接転送するようにします。	control-policy CP1 sequence 1 match tloc site-list SEGMENT1_HUB1 ! action accept ! ! sequence 2 match route site-list HUB1_HUB2_SEGMENT2 ! action accept set tloc-list HUB1_TLOCS ! ! ! sequence 3 match route site-list SEGMENT1 ! action accept ! ! default-action reject !
2. 前の行で説明した制御ポリシー CP1 を、発信トラフィックのセグメント 1 に適用します。		apply-policy site-list SEGMENT1 control-policy CP1 out

ポリシー構成の目的の簡単な説明	詳細な説明	例

3.（a）セグメント 2 内のルータが互いにトラフィックを直接送信できるようにする、および（b）セグメント 1 宛てのすべてのトラフィックが最初のホップとして Hub21 を使用するように指示する、セグメント 2 の制御ポリシーを作成します。このようにして、Hub21 はセグメント 1 へのトラフィックのハブとして機能します。	CP4 という制御ポリシーを作成して、次のことを行います。
	• シーケンス 1：セグメント 2 のすべてのデバイスに、セグメント 2 の他のデバイスの TLOC へのアクセスを提供します。これには、エッジルータとハブルータが含まれます。これにより、セグメント 2 にフルメッシュ接続が作成されます。
	• シーケンス 2：宛先が Hub21 またはセグメント 1 のデバイスのいずれかであるセグメント 2 のすべてのトラフィックについて、最初のホップが Hub21 である必要があることを確認します。
	• シーケンス 3：セグメント 2 内のすべてのトラフィックについて、デバイスがトラフィックをリージョン内の宛先デバイスに直接転送するようにします。
		`control-policy CP4`
		`  sequence 1`
		`   match tloc`
		`    site-list HUB2_SEGMENT2`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  sequence 2`
		`   match route`
		`    site-list HUB1_HUB2_SEGMENT1`
		`   !`
		`   action accept`
		`    set`
		`     tloc-list HUB2_TLOCS`
		`    !`
		`   !`
		`  !`
		`  sequence 3`
		`   match route`
		`    site-list SEGMENT2`
		`   !`
		`   action accept`
		`   !`
		`  !`
		`  default-action reject`
		`!`
		`!`

4. 前の行で説明した制御ポリシー CP4 を、発信トラフィックのセグメント 2 に適用します。		`apply-policy`
		` site-list SEGMENT2`
		`  control-policy CP4 out`

ポリシー構成の目的の簡単な説明	詳細な説明	例
5.（a）セグメント 1 のデバイスとのフルメッシュ接続を提供する、および（b）他のハブルータ（Hub21）とのフルメッシュ接続を提供する、セグメント 1 のハブルータ Hub11 の制御ポリシーを作成します。	CP2 という制御ポリシーを作成して、次のことを行います。 • シーケンス 1：セグメント 1 のデバイスの TLOC およびセグメント 2 のハブルータの TLOC へのアクセスを提供します。これにより、（a）セグメント 1 のハブルータとセグメント 1 の他のルータとのフルメッシュ接続、および（b）セグメント 1 と 2 のハブルータ間のフルメッシュ接続が作成されます。 • シーケンス 2：宛先がセグメント 1 のデバイスであるすべてのトラフィックについて、トラフィックをデバイスに直接転送するようにします。 • シーケンス 3：宛先がセグメント 2 のデバイスであるすべてのトラフィック（ハブおよびエッジルータを含む）について、トラフィックを Hub21 に転送するようにします。	control-policy CP2 sequence 1 match tloc site-list SEGMENT1_HUB2 ! action accept ! ! sequence 2 match route site-list SEGMENT1 ! action accept ! ! sequence 3 match route site-list HUB2_SEGMENT2 ! action accept set tloc-list HUB2_CORE_TLOC ! ! ! default-action reject !
6. 前の行で説明した制御ポリシー CP2 を、セグメント 1 のハブルータに適用します。		apply-policy site-list HUB1 control-policy CP2 out !

ポリシー構成の目的の簡単な説明	詳細な説明	例

7.（a）セグメント 2 のデバイスとのフルメッシュ接続を提供する、および（b）他のハブルータ（Hub11）とのフルメッシュ接続を提供する、セグメント 2 のハブルータ Hub21 の制御ポリシーを作成します。	CP3 という制御ポリシーを作成して、次のことを行います。
	• シーケンス 1：セグメント 2 のデバイスの TLOC およびセグメント 1 のハブルータの TLOC へのアクセスを提供します。これにより、（a）セグメント 2 のハブルータとセグメント 2 の他のルータとのフルメッシュ接続、および（b）セグメント 1 と 2 のハブルータ間のフルメッシュ接続が作成されます。
	• シーケンス 2：宛先がセグメント 2 のデバイスであるすべてのトラフィックについて、トラフィックをデバイスに直接転送するようにします。
	• シーケンス 3：宛先がセグメント 1 のデバイスであるすべてのトラフィック（ハブおよびエッジルータを含む）について、トラフィックを Hub11 に転送するようにします。
		control-policy CP3
		  sequence 1
		  match tloc
		  site-list HUB1_SEGMENT2
		  !
		  action accept
		  !
		  !
		  sequence 2
		  match route
		  site-list SEGMENT2
		  !
		  action accept
		  !
		  !
		  sequence 3
		  match route
		  site-list SEGMENT1_HUB1
		  !
		  action accept
		  set
		  tloc-list HUB1_CORE_TLOC
		  !
		  !
		  !
		  default-action reject
		!

8. 前の行で説明した制御ポリシー CP3 を、セグメント 2 のハブルータに適用します。		apply-policy site-list HUB2 control-policy CP3 out !

Cisco vManage を使用したマルチリージョン ファブリックへの移行

はじめる前に

- 既存のネットワークアーキテクチャから始めて、ネットワーク内のどのデバイスをマルチリージョンファブリックに移行するかを計画します。これらのデバイスはマルチリージョン ファブリック アーキテクチャ内で機能するため、これらの各デバイスのロールとリージョンを計画します。
- 移行後にネットワークで必要になる Cisco vSmart コントローラ を計画します。移行前に使用されていたデフォルトの Cisco vSmart コントローラ は、移行後に使用できなくなります。この Cisco vSmart コントローラ をコアリージョンで使用するために転用することをお勧めします。

マルチリージョン ファブリックへの移行

1. ネットワーク内のデバイスごとに、デバイスの Cisco System テンプレート（Cisco IOS XE SD-WAN デバイス）または Cisco vEdge System テンプレート（Cisco vEdge デバイス）を作成するか、デバイスにすでに割り当てられている既存のテンプレートを開きます。
2. [Basic Configuration] セクションで、[Enable Migration Mode to Multi-Region Fabric] フィールドを [Enable] に設定します。
3. テンプレートをデバイスに適用します。これにより、デバイスが移行モードになります。
4. Cisco vSmart コントローラ を展開して、マルチリージョン ファブリック コア リージョンにサービスを提供します。

   Cisco vSmart コントローラ の展開については、『Cisco SD-WAN Getting Started Guide』の「Cisco SD-WAN Overlay Network Bring-Up Process」の章を参照してください。

   - デフォルトリージョンの Cisco vSmart コントローラ で現在アクティブになっているものと同じ機能テンプレート、デバイステンプレート、およびポリシーテンプレートを適用します。
   - Cisco vSmart コントローラ のマルチリージョン ファブリック リージョンを 0 に設定します。

     Cisco vSmart コントローラ へのリージョンの割り当てについては、Cisco vManage を使用したリージョンの Cisco vSmart コントローラ への割り当て （22 ページ）を参照してください。
5. Cisco vSmart コントローラ を展開して、マルチリージョン ファブリック アクセス リージョンにサービスを提供します。

- デフォルトリージョンの Cisco vSmart コントローラ で現在アクティブになっているものと同じ機能テンプレート、デバイステンプレート、およびポリシーテンプレートを適用します。
- 各 Cisco vSmart コントローラ のマルチリージョン ファブリック リージョンを、サービスを提供する予定のリージョン番号に設定します。

6. 境界ルータとして機能するデバイスごとに、構成を適用して、デバイスがコアリージョン、関連するアクセスリージョン、およびデフォルトリージョンの Cisco vSmart コントローラ に接続できるようにします。

   詳細については、Cisco vManage を使用したデバイスへのロールとリージョンの割り当て（18 ページ）およびCisco vManage を使用したコアリージョンへの境界ルータ TLOC の割り当て （20 ページ）を参照してください。

7. 境界ルータとして機能する各デバイスについて、OMP ピアを表示して、デフォルトリージョン Cisco vSmart コントローラ、コアリージョン Cisco vSmart コントローラ、およびアクセスリージョン Cisco vSmart コントローラ への接続を確認します。OMP ピアの表示については、Cisco vManage を使用した OMP ピアの表示 （45 ページ）を参照してください。

8. エッジルータとして機能するデバイスごとに、次の手順を実行します。

   1. 構成を適用して、デバイスがデフォルトリージョンの Cisco vSmart コントローラ、およびエッジルータが属するアクセスリージョンの Cisco vSmart コントローラ に接続できるようにします。
   2. リージョンを構成します。

      リージョンの構成の詳細については、Cisco vManage を使用したデバイスへのロールとリージョンの割り当て （18 ページ）を参照してください。

9. 境界ルータごとに、次の手順を実行して移行モードを無効にします。

   1. デバイスの Cisco System テンプレート（Cisco IOS XE SD-WAN デバイス）または Cisco vEdge System テンプレート（Cisco vEdge デバイス）を開きます。
   2. [Basic Configuration] セクションで、[Enable Migration Mode to Multi-Region Fabric] フィールドを [Default] に設定します（[Default] を選択すると、フィールドは空白になります）。
   3. テンプレートをデバイスに適用します。

   デバイスでこの手順を完了すると、境界ルータはデフォルトリージョンの Cisco vSmart コントローラ に接続しなくなります。

10. OMP ピアを表示して、デバイスに次のピアがあることを確認します。

    - このデバイスが境界ルータとして機能するアクセスリージョンにサービスを提供する Cisco vSmart コントローラ
    - コアリージョンにサービスを提供する Cisco vSmart コントローラ

OMP ピアの表示については、Cisco vManage を使用した OMP ピアの表示 （45 ページ）を参照してください。

11. エッジルータごとに、次の手順を実行して移行モードを無効にします。
    1. デバイスの Cisco System テンプレート（Cisco IOS XE SD-WAN デバイス）または Cisco vEdge System テンプレート（Cisco vEdge デバイス）を開きます。
    2. [Basic Configuration] セクションで、[Enable Migration Mode to Multi-Region Fabric] フィールドを [Default] に設定します（[Default] を選択すると、フィールドは空白になります）。
    3. テンプレートをデバイスに適用します。
12. 各デバイスの移行モードを無効にすると、ネットワーク内のデバイスはデフォルトリージョンの Cisco vSmart コントローラ を使用しなくなります。必要に応じて、ネットワークプランニングでコアリージョンにこのコントローラを使用する必要がある場合は、[Before You Begin] セクションで推奨されているように、この Cisco vSmart コントローラを再割り当てしてコアリージョンにサービスを提供できます。
13. 移行が完了すると、ネットワークをセグメントに分割し、ハブを介してトラフィックをルーティングするために以前使用されていた制御ポリシーは必要なくなります。デフォルトリージョンの Cisco vSmart コントローラ として機能する Cisco vSmart コントローラで、これらのポリシーのポリシーテンプレートを各 Cisco vSmart コントローラ から切り離して、制御ポリシーを削除します。

    ポリシーテンプレートを Cisco vSmart コントローラから削除する方法については、『Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x』の「Centralized Policy」の章を参照してください。

CLI を使用した移行モードの有効化または無効化

移行モードの有効化

1. システムモードを開始します。

   ```
   system
   ```

2. 移行モードを有効にします。

   ```
   multi-region-fabric migration-mode enabled
   ```

移行モードの無効化

1. システムモードを開始します。

   ```
   system
   ```

2. 移行モードを無効にします。

```
no multi-region-fabric migration-mode
```

マルチリージョン ファブリックへの移行の検証手順

次の手順は、ネットワークをマルチリージョンファブリックに移行した後に、接続とその他の情報を確認するのに役立ちます。

Cisco vManage を使用した OMP ピアの表示

1. Cisco vManage メニューから、**[Monitor]** > **[Devices]** の順に選択します。
2. デバイスのテーブルで、目的の境界ルータの右側にある [...] をクリックし、[Real Time] を選択します。
3. 左側のペインで、[Real Time] をクリックします。
4. [Device Options] フィールドに、[OMP Peers] と入力します。

   show sdwan omp peers CLI コマンドと同様に、テーブルにピア情報が表示されます。出力で、各ピアについて次のいずれかを示す [REGION ID] 列を確認します。

   - [None]：マルチリージョン ファブリックで動作するように構成されていない Cisco vSmart コントローラ。これには、マルチリージョン ファブリックへの移行前に構成されたデフォルトリージョンの Cisco vSmart コントローラ が含まれます。
   - [0]：コアリージョンの Cisco vSmart コントローラ。
   - *access-region-id*：アクセスリージョンの Cisco vSmart コントローラ。

Cisco vManage を使用したデバイス間の接続の確認

この手順を使用して、デバイス間の接続を確認するために、異なるリージョンにある 2 つのエッジデバイスなど、2 つのデバイス間のルートをトレースします。

1. Cisco vManage メニューから、**[Monitor]** > **[Devices]** の順に選択します。
2. デバイスのテーブルで、目的の境界ルータの隣にある [...] をクリックし、[Real Time] を選択します。
3. 左側のペインで、[Troubleshooting] をクリックします。
4. [Trace Route] をクリックします。
5. [Destination IP] フィールドで、ルートトレースのエンドポイントの IP アドレスを入力します。
6. [VPN] ドロップダウンリストをクリックし、ルートトレースの VPN を選択します。

境界ルータが Cisco vManage を使用してルートを再発信していることの確認

1. Cisco vManage メニューから、**[Monitor]** > **[Devices]** の順に選択します。
2. デバイスのテーブルで、目的の境界ルータの隣にある [...] をクリックし、[Real Time] を選択します。
3. 左側のペインで、[Real Time] をクリックします。
4. [Device Options] フィールドに、[OMP Received Routes] と入力します。

[Peer] 列で 0.0.0.0 を示すテーブルの行を見つけます。これらの行は、境界ルータ自体からのルートに対応します。境界ルータがルートを再発信している場合、これらの行では、[Region Path] 列にコアリージョンの 0 を含むルートの 2 つの番号が表示され、[Status] 列に [BR-R]（境界ルータ再発信）が表示されます。

境界ルータが CLI を使用してルートを再発信していることの確認

境界ルータで、次のコマンドを使用します。

show sdwan omp routes *ip-number/subnet-mask*

[Peer] 列で 0.0.0.0 を示すテーブルの行を見つけます。これらの行は、境界ルータ自体からのルートに対応します。境界ルータがルートを再発信している場合、これらの行では、[Region Path] 列にコアリージョンの 0 を含むルートの 2 つの番号が表示され、[Status] 列に [BR-R]（境界ルータ再発信）が表示されます。

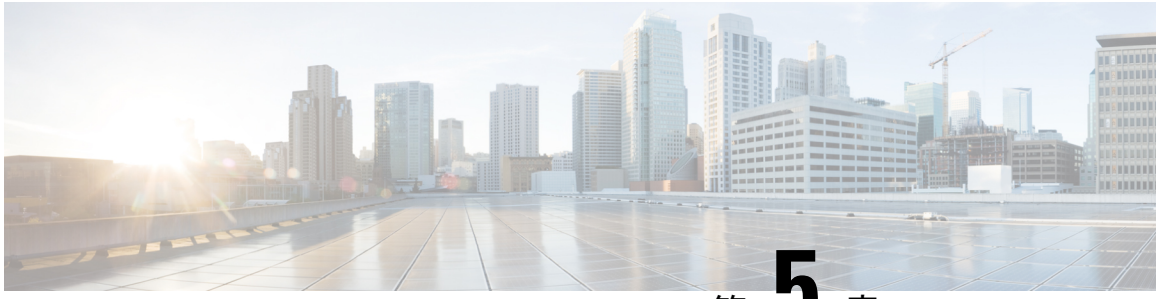
例：

```
show sdwan omp routes 10.1.1.0/24
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved
BR-R -> Border-Router reoriginated
TGW-R -> Transport-Gateway reoriginated

             AFFINITY
                                      PATH                    ATTRIBUTE
             GROUP
TENANT   VPN PREFIX       FROM PEER      ID     LABEL  STATUS   TYPE       TLOC IP      COLOR  ENCAP
 PREFERENCE  NUMBER     REGION ID  REGION PATH
-------------------------------------------------------------------------------------------------------
0        1   10.1.1.0/24 0.0.0.0        21474  1003   C,Red,R, installed  172.18.11.10  green ipsec
 -           None       0           0 1
                                      83721          BR-R

                         172.16.122.10   104    1003   C,I,R   installed  172.18.51.10  lte   ipsec
 -           None       1           1
```

```
                      172.16.122.10   105    1003   C,I,R   installed  172.18.51.10  red   ipsec
-           None      1           1
                      172.16.123.10   118    1003   C,R     installed  172.18.51.10  lte   ipsec
-           None      1           1
                      172.16.123.10   119    1003   C,R     installed  172.18.51.10  red   ipsec
-           None      1           1
```



第 5 章

セカンダリリージョン

表 *6*：機能の履歴

機能名	リリース情報	説明
マルチリージョン ファブリック：セカンダリリージョン	Cisco IOS XE リリース 17.8.1a Cisco SD-WAN リリース 20.8.1 Cisco vManage リリース 20.8.1	セカンダリリージョンは、マルチリージョン ファブリック アーキテクチャに別のファセットを提供し、異なるプライマリアクセスリージョン内のエッジルータ間のダイレクトトンネル接続を可能にします。エッジルータをセカンダリリージョンに割り当てると、ルータは2つのリージョンで同時に効果的に動作し、プライマリリージョンとセカンダリリージョンを介して異なるパスを使用できます。

セカンダリリージョンに関する情報

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

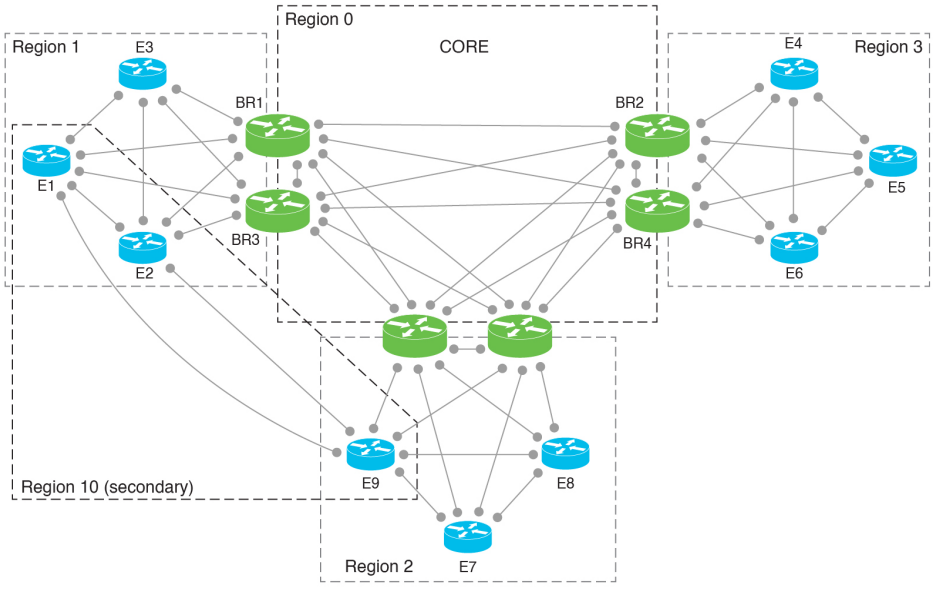
最も基本的な マルチリージョン ファブリック アーキテクチャでは、各デバイスは 1 つのリージョンに属します。あるリージョンのエッジルータから別のリージョンのエッジルータへの接

続は、境界ルータとリージョン 0 を介してルーティングされるため、複数のホップが必要です。

セカンダリリージョンは、アーキテクチャに別のファセットを提供し、追加の機能を有効にします。セカンダリリージョンは、プライマリリージョンよりも単純に動作します。エッジルータのみが含まれ、異なるプライマリリージョン内のエッジルータ間のダイレクトトンネル接続が可能になります。エッジルータをセカンダリリージョンに追加すると、ルータは2つのリージョンで同時に効果的に動作し、プライマリリージョンとセカンダリリージョンを介して異なるパスを使用できます。

ネットワーク内に複数のセカンダリリージョンを作成して、さまざまなエッジルータセットの特定のルーティングニーズに対応できますが、エッジルータは複数のセカンダリリージョンに属することはできません。

図 7: セカンダリリージョンを含む マルチリージョン ファブリック



セカンダリリージョンの使用

次のいずれかに対してセカンダリリージョンパスを構成できます。

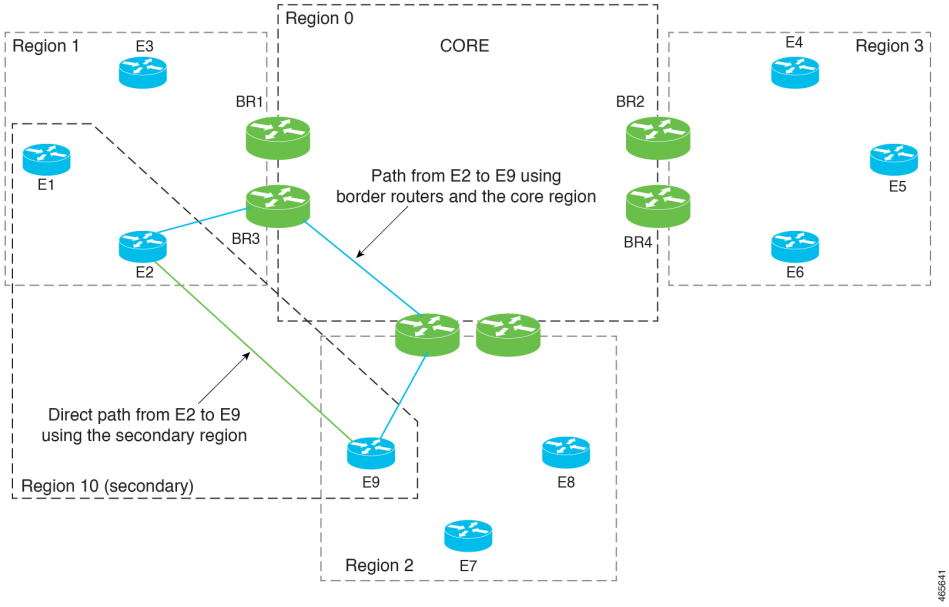
- プライマリリージョンとセカンダリリージョンのパスを使用したロードバランシング
- パフォーマンスの高いプレミアムパスとすることができる、セカンダリリージョンパスを使用するように特定のアプリケーションに指示

プライマリリージョンパスとセカンダリリージョンパス

ダイレクトパスはより少ないホップを使用するため、ダイレクトパスが宛先に到達可能な場合は、デフォルトでは、オーバーレイ マネジメント プロトコル（OMP）は、ルーティング フォワーディング レイヤへのダイレクトパスのみを有効にします。その結果、アプリケーション認

識型ポリシーを含む転送レイヤは、ダイレクトパスのみを使用できます。このホップ数の比較を無効にして、トラフィックが直接のセカンダリリージョンパス（より少ないホップ）またはプライマリリージョンパス（より多くのホップ）のいずれかを使用できるようにすることができます。ホップ数の比較を無効にすると、OMPは等コストマルチパスルーティング（ECMP）をすべてのルートに適用し、パケットは使用可能なすべてのパスを使用できます。Cisco vManage を使用してプライマリリージョンパスとセカンダリリージョンパスの両方を使用するようにデバイスを設定 （57 ページ）を参照してください。

図 *8*:セカンダリリージョンを使用するダイレクトパスと、プライマリリージョンとコアリージョンを使用するマルチホップパス



制御ポリシー

Cisco vSmart コントローラ のセカンダリリージョンの制御ポリシーを作成する場合、プライマリリージョンパスまたはセカンダリリージョンパスのどちらを使用しているかに応じてトラフィックを一致させることができます。

ワークフロー

1. デバイスで、デバイスレベルのセカンダリリージョンを構成します。

   Cisco vManage を使用したエッジルータのセカンダリリージョン ID の設定 （56 ページ）を参照してください。

2. デバイスで、セカンダリリージョンを使用できる TLOC を指定します。

   CLI を使用した TLOC のセカンダリリージョンモードの設定 （58 ページ）を参照してください。

3. セカンダリリージョンのみ、またはプライマリリージョンとセカンダリリージョンの両方で動作するように TLOC を構成します。

Cisco vManage を使用した TLOC のセカンダリリージョンモードの設定 （56 ページ）を参照してください。

4. デバイスがプライマリリージョンパスとセカンダリリージョンパスの両方を使用できるようにします。

   Cisco vManage を使用してプライマリリージョンパスとセカンダリリージョンパスの両方を使用するようにデバイスを設定 （57 ページ）を参照してください。

5. Cisco vSmart コントローラ をセカンダリリージョンに割り当てます。セカンダリリージョンを使用するデバイスのいずれのアクセスリージョンでも動作しない Cisco vSmart コントローラを使用します。これを確実にするために、セカンダリリージョンでのみ動作し、どのアクセスリージョンでも動作しない Cisco vSmart コントローラ を割り当てることをお勧めします。たとえば、リージョン 0 でのみ動作する Cisco vSmart コントローラ を、セカンダリリージョンでも動作するように割り当てることができます。

   「Cisco vManage を使用した Cisco vSmart コントローラへのリージョンの割り当て」を参照してください。

用語

マルチリージョン ファブリック アーキテクチャへのセカンダリリージョンの導入により、ここで使用される用語を明確にすることが重要です。

用語	説明または同等の用語
コアリージョン	リージョン 0
アクセスリージョン	リージョン 0 以外のリージョン
プライマリ アクセス リージョン	プライマリリージョン
セカンダリ アクセス リージョン	セカンダリリージョン
プライマリリージョンパス	エッジルータから境界ルータへ、コアリージョンを経由、別の境界ルータへ、別のリージョンのエッジルータへのパス
セカンダリリージョンパス	あるプライマリリージョンのエッジルータ 1 から別のプライマリリージョンのエッジルータ 2 へのダイレクトパス。エッジルータ 1 と 2 は同じセカンダリリージョンにあります

セカンダリリージョンの利点

- 異なるプライマリリージョン間で、あるエッジルータから別のエッジルータにダイレクトトンネルを使用して特定のトラフィックをルーティングする機能。

- 異なるプライマリリージョン間のダイレクトトンネルで、データセンターへのトラフィックなど、大量のスループットを提供する機能。大量のスループットを直接ルーティングすると、過剰なトラフィックボリュームによる境界ルータの過負荷を防ぐことができます。

パスのタイプ、リージョン、またはロールによるルートの一致

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

パスタイプ

マルチリージョン ファブリック アーキテクチャの制御ポリシーを設定する場合、ルートが次のいずれかを使用しているかどうかに応じてルートを一致させることができます。

- 階層パス：アクセスリージョンから境界ルータへ、リージョン 0 を経由して、別の境界ルータへ、さらに別のアクセスリージョンのエッジルータへのホップを含むルートに一致します。

  階層パスルートを表示するには、**show sdwan omp routes** コマンドを使用し、[REGION PATH] 列に 3 つのリージョンをリストするルートを書き留めます。

- ダイレクトパス：あるエッジルータから別のエッジルータへのダイレクトパス（ダイレクトルート）に一致します。セカンダリリージョンを構成し、2 つのエッジルータをセカンダリリージョンに追加することにより、異なるアクセスリージョンのエッジルータ間のダイレクトパスを有効にすることができます。セカンダリリージョンに関する情報（49 ページ）を参照してください。

  ダイレクトパスルートを表示するには、**show sdwan omp routes** コマンドを使用し、[REGION PATH] 列に 1 つのリージョンをリストするルートを書き留めます。

- トランスポート ゲートウェイ パス：トランスポートゲートウェイ機能が有効になっているルータによって再発信されたルートに一致します。

  トランスポートゲートウェイについては、トランスポートゲートウェイに関する情報（63 ページ）を参照してください。

リージョンとロール

パスタイプによる一致と同様に、ルートを発信するデバイスのリージョンまたはロール（エッジルータまたは境界ルータ）によってルートを一致させることができます。

セカンダリリージョンの制約事項

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

- セカンダリリージョンは、境界ルータではなく、エッジルータにのみ適用されます。
- ルータは、1 つのセカンダリリージョンにのみ属することができます。
- セカンダリリージョンに割り当てる Cisco vSmart コントローラは、セカンダリリージョンを使用するデバイスのプライマリ（アクセス）リージョンで動作してはなりません。これを確実にするために、セカンダリリージョンでのみ動作し、どのアクセスリージョンでも動作しない Cisco vSmart コントローラ を割り当てることをお勧めします。
- トランスポートゲートウェイとして構成されているルータでセカンダリリージョンを構成することはできません。

（注） このようなルータでセカンダリリージョンを構成しようとすると、エラーが発生します。

セカンダリリージョンのユースケース

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

ユースケース 1：特定のアプリケーション トラフィック

マルチリージョン ファブリック アーキテクチャを使用している組織は、境界ルータの帯域幅の需要を削減するためにダイレクトパスルートを使用して、2つの異なるリージョン（リージョン 1 とリージョン 2）のサイト間で特定のアプリケーション トラフィックをルーティングすることを選択します。組織は、この目的のために 2 つのサイト間にキャリアを配置します。

ネットワーク管理者は、次のように、リージョン 1 のエッジルータとリージョン 2 のエッジルータのセカンダリリージョンを構成し、2 つのルータが両方ともセカンダリリージョン 5 にあるようにします。

- エッジルータ ER10

  プライマリリージョン：1
  セカンダリリージョン：5

- エッジルータ ER20

  プライマリリージョン：2
  セカンダリリージョン：5

ネットワーク管理者は、エッジルータ ER10 とエッジルータ ER20 の間にダイレクトトンネルを設定し、ダイレクトトンネルを介して特定のアプリケーション トラフィックをルーティングするポリシーを設定します。

ユースケース 2：大容量データセンター

マルチリージョン ファブリック アーキテクチャを使用する組織には、エッジルータ ER10 がサービスを提供するデータセンターがリージョン 1 にあります。リージョン 2、3、および 4 のサイト（エッジルータ ER20、ER30、および ER40 によってサービスを提供）はデータセンターに接続し、大量のトラフィックを生成します。組織は、コアリージョンにプレミアム サービス プロバイダー リンクを使用します。

コアリージョンで使用されるプレミアムリンクを介して大量のデータセントラフィックをルーティングしないようにするために、ネットワーク管理者は、データセンター（ER10）を含み、ダイレクトトンネルを使用してデータセンターに接続できるようにするための各リモートサイト（ER20、ER30、および ER40）を含むセカンダリリージョンを構成します。大量のトラフィックにダイレクトトンネルを使用すると、コアリージョンの帯域幅の需要が減少します。

プライマリリージョンとセカンダリリージョンの構成は次のとおりです。

- データセンター：エッジルータ ER10

  プライマリリージョン：1
  セカンダリリージョン：5

- リモートサイト：エッジルータ ER20

  プライマリリージョン：2
  セカンダリリージョン：5

- リモートサイト：エッジルータ ER30

  プライマリリージョン：3
  セカンダリリージョン：5

- リモートサイト：エッジルータ ER40

  プライマリリージョン：4
  セカンダリリージョン：5

Cisco vManage を使用したセカンダリリージョンの設定

Cisco vManage を使用したエッジルータのセカンダリリージョン ID の設定

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. 次のいずれかを実行します。
   - デバイスのシステムテンプレートを作成します。
   - テーブルで、デバイスの既存のシステムテンプレートを見つけます。テンプレートの行で [...] をクリックし、[Edit] を選択します。
4. [Basic Configuration] セクションの [Secondary Region ID] フィールドで、グローバルモードを有効にして、1 ～ 63 の範囲でセカンダリリージョンの番号を入力します。
5. 既存のテンプレートを編集している場合は、[Update]、[Configure Device] の順にクリックして、テンプレートを使用して更新をデバイスにプッシュします。

Cisco vManage を使用した TLOC のセカンダリリージョンモードの設定

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

はじめる前に

この手順では、Cisco VPN インターフェイス イーサネット テンプレートを使用して TLOC のセカンダリリージョンモードを設定する方法について説明します。テンプレートを適用するインターフェイスの指定方法など、テンプレートの一般的な使用方法については、『Cisco SD-WAN Systems and Interfaces Configuration Guide』の「Configure VPN Ethernet Interface」を参照してください。

TLOC のセカンダリリージョンモードの設定

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. 次のいずれかを実行します。
   - デバイスの Cisco VPN インターフェイス イーサネット テンプレートを作成します。

- テーブルで、デバイスの既存の Cisco VPN インターフェイスイーサネットテンプレートを見つけます。テンプレートの行で [...] をクリックし、[Edit] を選択します。

4. [Tunnel] セクションに移動し、そのセクション内の [Advanced Options] セクションに移動します。
5. [Enable Secondary Region] フィールドで、グローバルモードを有効にして、次のいずれかのオプションを選択します。

オプション	説明
Only in Secondary Region	セカンダリリージョンのトラフィックのみを処理するようにインターフェイスを構成します。
Shared Between Primary and Secondary Regions	プライマリリージョンとセカンダリリージョンでトラフィックを処理するようにインターフェイスを構成します。

（注） インターフェイスは、システムレベルでデバイスに構成されたセカンダリリージョンの割り当てを継承します。

6. 既存のテンプレートを編集している場合は、[Update]、[Configure Device] の順にクリックして、テンプレートを使用して更新をデバイスにプッシュします。

CiscovManageを使用してプライマリリージョンパスとセカンダリリージョンパスの両方を使用するようにデバイスを設定

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. 次のいずれかを実行します。
   - デバイスの Cisco OMP テンプレートを作成します。
   - テーブルで、デバイスの既存の OMP テンプレートを見つけます。テンプレートの行で [...] をクリックし、[Edit] を選択します。
4. [Best Path] セクションに移動し、[Ignore Region-Path Length During Best-Path Algorithm] フィールドで [On] を選択します。

   [On] を選択すると、テンプレートは [Direct-Tunnel Path] と [Hierarchical Path] を自動的に選択します。

（注） デフォルト値は [Off] です。デフォルトでは、ダイレクトパスのホップ数が少ないため、OMP は階層パスよりもダイレクトトンネルパスを優先します。

5. 既存のテンプレートを編集している場合は、[Update]、[Configure Device] の順にクリックして、テンプレートを使用して更新をデバイスにプッシュします。

CLI を使用したセカンダリリージョンの設定

CLI を使用したエッジルータのセカンダリリージョン ID の設定

1. コンフィギュレーション モードを入力します。

```
Device#config-transaction
```

2. システム コンフィギュレーション モードを開始します。

```
Device(config)#system
```

3. リージョンとセカンダリリージョンを割り当てます。

デバイスには、1 つのセカンダリリージョンのみを割り当てることができます。以前にデバイスにセカンダリリージョンを割り当てていた場合は、新しいセカンダリリージョンの割り当てが以前の割り当てに置き換わります。

1 つ以上の TLOC インターフェイスのセカンダリ リージョン トラフィックを有効にすると、インターフェイスは、システムレベルで割り当てたセカンダリリージョン ID を継承します。

```
Device(config-system)#region region-id secondary-region region-id
```

例

```
Device#config-transaction
Device(config)#system
Device(config-system)#region 1 secondary-region 20
```

CLI を使用した TLOC のセカンダリリージョンモードの設定

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

1. コンフィギュレーション モードを入力します。

```
Device#config-transaction
```

2. VPN 0 コンフィギュレーション モードを開始します。

```
Device(config)#sdwan
```

3. インターフェイスを指定します。

```
Device(config-sdwan)#interface interface
```

4. トンネル インターフェイス コンフィギュレーション モードを開始します。

```
Device(config-sdwan-interface)#tunnel-interface
```

5. TLOC に対して次のいずれかのモードを選択して、TLOC がプライマリリージョンおよびセカンダリリージョンのトラフィックに使用されるように、またはセカンダリリージョンのトラフィック専用に使用されるように TLOC を設定します。

モード	説明
secondary-only	TLOC は、デバイスのセカンダリリージョンのトラフィックのみを処理できます。
secondary-shared	TLOC は、デバイスのプライマリリージョンとセカンダリリージョンのトラフィックを処理できます。

```
Device(config-tunnel-interface)#region {secondary-only | secondary-shared}
```

例 1

この例では、プライマリリージョンとセカンダリリージョンのトラフィックを処理するように TLOC を設定します。

```
Device#config-transaction
Device(config)#sdwan
Device(config-sdwan)#interface GigabitEthernet0/0/0
Device(config-interface-GigabitEthernet0/0/0)#tunnel-interface
Device(config-tunnel-interface)#region secondary-shared
```

例 2

この例では、TLOC がセカンダリリージョンのトラフィックを処理しない、デフォルトの動作を復元します。

```
Device#config-transaction
Device(config)#sdwan
Device(config-sdwan)#interface GigabitEthernet0/0/0
Device(config-interface-GigabitEthernet0/0/0)#tunnel-interface
Device(config-tunnel-interface)#no region
```

CLI を使用してプライマリリージョンパスとセカンダリリージョンパスの両方を使用するようにデバイスを設定

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

1. コンフィギュレーション モードを入力します。

```
Device#config-transaction
```

2. OMP コンフィギュレーション モードを開始します。

```
Device(config)#sdwan omp
```

3. デバイスがプライマリリージョンパス（複数ホップ）とセカンダリリージョンパス（ダイレクトパス）の両方を使用できるようにします。

```
Device(config-omp)#best-path region-path-length ignore
```

（注） この機能を無効にするには、このコマンドの **no** 形式を使用します。

Cisco vManage を使用したデバイスのセカンダリリージョンの割り当ての確認

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

1. Cisco vManage メニューから、**[Monitor]** > **[Devices]** の順に選択します。
2. テーブルで、デバイスをクリックします。
3. [Real Time] をクリックします。
4. [Device Options] フィールドで、[Control Local Properties] を選択します。

   [Region ID Set] フィールドには、プライマリリージョンとセカンダリリージョンが表示されます。

CLI を使用したデバイスのセカンダリリージョンの割り当ての確認

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

デバイスで **show sdwan running-config system** コマンドを使用して、セカンダリリージョンが設定されていることを確認します。[region] フィールドと [secondary-region] フィールドには、プライマリリージョンとセカンダリリージョンが表示されます。

```
Device#show sdwan running-config system
system
 system-ip             175.2.55.10
 domain-id             1
 site-id               2200
 region 2
```

```
  secondary-region 20
 !
```

デバイスで **show sdwan omp summary** コマンドを使用して、プライマリリージョン ID（[region-id] フィールド内）とセカンダリリージョン ID（[secondary-region-id] フィールド内）を確認することもできます。

```
Device#show sdwan omp summary
...
region-id                    1
secondary-region-id          20
```

CLI を使用したインターフェイスのセカンダリリージョンモードの確認

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

インターフェイスのセカンダリリージョンモードを表示するには、**show sdwan running-config sdwan** コマンド（Cisco IOS XE SD-WAN デバイス）または **show running-config vpn 0 interface** *interface-name* コマンド（Cisco vEdge デバイス）を使用します。[region] フィールドにモードが表示されます。モードオプションは、[secondary-only] と [secondary-shared] です。

次の例は、Cisco IOS XE SD-WAN デバイス の場合です。

```
Device#show sdwan running-config sdwan
sdwan
 interface GigabitEthernet1
  ip address 173.3.1.11/24
  tunnel-interface
   encapsulation ipsec
   color 3g
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   region secondary-only
  !
  no shutdown
 !
!
```

次の例は、Cisco vEdge デバイス の場合です。

```
Device#show running-config vpn 0 interface ge0/1
vpn 0
 interface ge0/1
  ip address 173.3.1.11/24
  tunnel-interface
   encapsulation ipsec
   color 3g
```

```
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   region secondary-only
  !
  no shutdown
 !
!
```

CLIを使用したインターフェイスのセカンダリリージョンの割り当ての確認

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

デバイスで、**show sdwan control local-properties** コマンド（Cisco IOS XE SD-WAN デバイス）または **show control local-properties** コマンド（Cisco vEdge デバイス）を使用して、各インターフェイスのリージョン割り当てを表示します。

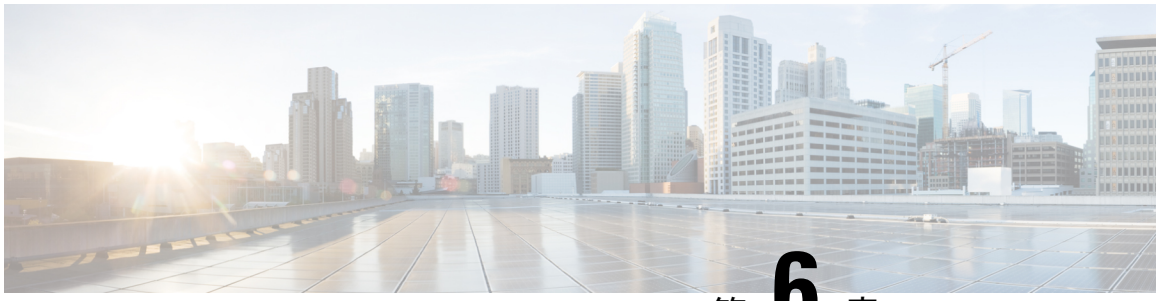
show sdwan control local-properties コマンドの出力では、インターフェイスごとに、[REG IDs] 列にリージョンの割り当てが表示されます。

```
Device#show sdwan control local-properties
...
                  PUBLIC          PUBLIC PRIVATE         PRIVATE   PRIVATE
         MAX   RESTRICT/           LAST         SPI TIME    NAT  VM
INTERFACE         IPv4            PORT   IPv4            IPv6      PORT    VS/VM COLOR
   STATE CNTRL CONTROL/     LR/LB  CONNECTION   REMAINING   TYPE CON REG

               STUN                                                  PRF IDs
-------------------------------------------------------------------------------------------------------
GigabitEthernet1       172.2.2.11      12366  172.2.2.11      ::        12366    4/1
lte      up     2      no/yes/no   No/No  0:00:00:16   0:11:58:49  N    5  2
GigabitEthernet2       173.2.2.11      12366  173.2.2.11      ::        12366    4/0
3g       up     2      no/yes/no   No/No  0:00:00:16   0:11:58:49  N    5  2,10
```

show control local-properties コマンドの出力では、インターフェイスごとに、[REGION IDs] 列にリージョンの割り当てが表示されます。

```
Device#show control local-properties
           PUBLIC          PUBLIC PRIVATE         PRIVATE  PRIVATE
MAX     CONTROL/           LAST         SPI TIME    NAT  CON REGION
INTERFACE  IPv4            PORT   IPv4            IPv6     PORT     VS/VM COLOR  STATE
CNTRL   STUN        LR/LB  CONNECTION   REMAINING   TYPE PRF IDs
-------------------------------------------------------------------------------------------------------
ge0/0      172.3.1.11      12366  172.3.1.11      ::       12366    4/1  lte     up
 2      no/yes/no   No/No  0:00:00:04   0:11:59:38  N    5  3
ge0/1      173.3.1.11      12366  173.3.1.11      ::       12366    4/0  3g      up
 2      no/yes/no   No/No  0:00:00:04   0:11:59:56  N    5  10
```



第 6 章

トランスポートゲートウェイ

表 7: 機能の履歴

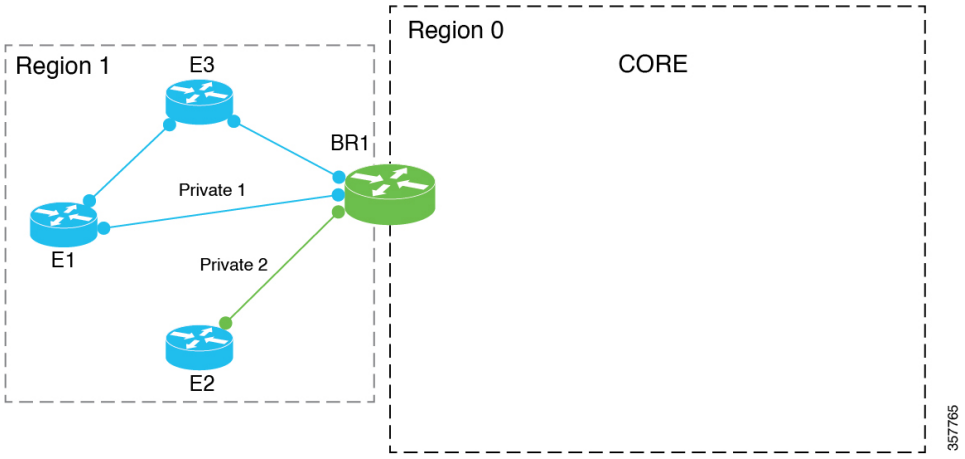
機能名	リリース情報	説明
マルチリージョンファブリック：トランスポートゲートウェイ	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1	直接接続されていない2つのネットワークに接続しているエッジルータまたは境界ルータは、トランスポートゲートウェイとして機能できます。これは、同じアクセスリージョン内にあるように構成されているが、直接接続されていないルータ間の接続を有効にする場合に役立ちます。

トランスポートゲートウェイに関する情報

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

同じアクセスリージョンに割り当てられたさまざまなデバイスは、直接接続がないネットワーク、いわゆるディスジョイント ネットワークで動作する場合があります。同じアクセスリージョンで動作するエッジルータまたは境界ルータがあり、2つのディスジョイントネットワークに接続している場合、そのルータをトランスポートゲートウェイとして機能するように構成できます。ルータは、トランスポートゲートウェイとして、ディスジョイントネットワーク内のエッジルータへの接続を提供します。

図 *9*: 直接接続のないエッジルータのトランスポートゲートウェイとして機能する境界ルータ



トランスポートゲートウェイが対処する問題

トランスポートゲートウェイ機能がない場合、直接接続のないデバイス間のトラフィックを有効にする 1 つの方法は、両方のネットワークへの接続を持つ中間デバイスを使用し、特定のルートを構成して、ディスジョイントネットワーク内のデバイス間のトラフィックをルーティングする制御ポリシーを作成することです。

このアプローチには次のような問題があります。

- 複雑さ：プレフィックスをアドバタイズするための制御ポリシーの構成は複雑です。
- 潜在的なトラフィックブラックホール：制御ポリシーは、デバイスまたは構成されたルートが使用できないかどうかを検出できません。これにより、ルートが使用できなくなった場合にパケット損失が発生する可能性があります。

ルーティングメカニズム

ルータがトランスポートゲートウェイとして機能するように構成されている場合、ルータは、プライマリリージョン内のデバイス間の各ルートに対して次のことを行います。

1. アクセスリージョンの Cisco vSmart コントローラ から学習した各ルートをインストールします。
2. Cisco vSmart コントローラ から学習した各ルートを再発信し、ルートのネクストホップとして独自の TLOC を置き換えます。これは、TLOC を各ルートのネクストホップとして置き換え、そのリージョンの Cisco vSmart コントローラ にルートをアドバタイズすることを意味します。

このプロセスでは、プライマリリージョンルートをコアリージョンに再発信したり、コアリージョンルートをアクセスリージョンに再発信したりしないことに注意してください。

ルータをトランスポートゲートウェイとして構成する効果は、すべてのリージョン内トラフィックにルートを提供できることです。ネットワーク内のデバイスは、宛先へのダイレクトルートがない場合にのみ、トランスポート ゲートウェイ ルートを使用します。

プライマリリージョンのみ

エッジルータがトランスポートゲートウェイとして機能するように構成した場合、エッジルータはプライマリ アクセス リージョン内のルートのみを再発信します。プライマリリージョンとセカンダリリージョンについては、セカンダリリージョンに関する情報 （49 ページ）を参照してください。

トランスポートゲートウェイとして機能するように境界ルータを構成すると、コアリージョンではなく、アクセスリージョン内のルートのみが再発信されます。

トランスポート ゲートウェイ ルートの優先度

トランスポートゲートウェイを構成した後、アクセスリージョン内の2つのルータ間で複数のパスが使用可能になる場合があります。2 つのルータ間で複数のパスを使用できる場合、オーバーレイ マネジメント プロトコル（OMP）は、最適パス選択ロジックを適用して最適パスを選択します。最適パス選択ロジックは、ホップ数が最も少ないパスに偏っていて、トランスポート ゲートウェイ パスが除外される可能性があります。OMP 最適パス選択ロジックには、次のものが含まれます。

- デフォルトでは、OMP はダイレクトパスを選択します（使用可能な場合）。
- ダイレクトパスが利用できない場合、OMP は、トランスポートゲートウェイを経由するなど、より多くのホップを持つパスを選択します。

次のように OMP ロジックを構成できます。

- ダイレクトパスよりもトランスポート ゲートウェイ パスを優先します。
- ダイレクトパスとトランスポート ゲートウェイ パスは同等であるとみなします。

Cisco vManage を使用したトランスポート ゲートウェイ パスの設定の構成 （67 ページ）を参照してください。

複数のトランスポートゲートウェイ

リージョンにアクティブなトランスポートゲートウェイが複数ある場合、デバイスは、使用可能なすべてのトランスポートゲートウェイに等コストマルチパス ルーティング（ECMP）を適用します。

トランスポートゲートウェイの利点

トランスポートゲートウェイを使用する利点

- 制御ポリシー方式よりも簡単に設定できます。
- ルートが利用できなくなった場合、トランスポートゲートウェイはエッジルータへのルートを取り消し、そのルートへのパスの再生成を停止して、ネットワークのブラックホールを防ぎます。

トラフィックプロトコル

トランスポート ゲートウェイ ルータは、IPv4 および IPv6 トラフィックを処理できます。

トランスポートゲートウェイでサポートされるデバイス

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

- トランスポートゲートウェイ機能：Cisco IOS XE SD-WAN デバイス のみ
- トランスポート ゲートウェイ パスを使用する機能：Cisco IOS XE SD-WAN デバイス および Cisco vEdge デバイス

トランスポートゲートウェイの制約事項

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

- SaaS ルートの Cloud onRamp には影響しません。
- トランスポートゲートウェイ機能は、セカンダリリージョンが構成されているルータではサポートされていません。

（注） このようなルータでトランスポートゲートウェイ機能を構成しようとすると、エラーが発生します。

- 同じリージョン内の複数のデバイスでトランスポートゲートウェイ機能を有効にして、ディスジョイント ネットワーク内のエッジルータ間に複数のトランスポート ゲートウェイ パスを提供する場合、エッジルータは最適パス選択ロジックを適用して最適パスを決定します。

  複数のトランスポートゲートウェイがあり、OMP が選択したトランスポート ゲートウェイ パスがある場合は、使用可能なすべてのトランスポート ゲートウェイ パスに ECMP が適用されます。

  デフォルトでは、OMP はダイレクトパスが利用可能な場合はそれを選択し、利用できない場合は、トランスポートゲートウェイを経由する（利用可能な場合）など、より多くのホップを持つパスを選択します。ただし、OMP ロジックを別の方法で構成することもできます。トランスポートゲートウェイに関する情報 （63 ページ）を参照してください。

- 同じリージョン内の複数のデバイスでトランスポートゲートウェイ機能を有効にすると、リージョンの Cisco vSmart コントローラにより、あるトランスポートゲートウェイによって再発信されたルートが別のトランスポートゲートウェイにアドバタイズされなくなります。別のトランスポートゲートウェイへのトランスポート ゲートウェイ ルートのアドバ

タイズを防止することにより、Cisco vSmart コントローラ で潜在的なルーティングループを防止できます。

- トランスポートゲートウェイ機能のリソース要求のため、追加の負荷を処理する CPU とメモリリソースを備えた高性能デバイスでのみこれを有効にすることをお勧めします。特定のリソース要件は、ネットワーク環境によって異なります。
- トランスポートゲートウェイとして構成されたデバイスに動的オンデマンドトンネルを構成することはできません。この制限は、MRF および非 MRF アーキテクチャに適用されます。動的オンデマンドトンネルの詳細については、『Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x』の「Dynamic On-Demand Tunnels」を参照してください。

Cisco vManage を使用したトランスポートゲートウェイの設定

Cisco vManage を使用したルータでのトランスポートゲートウェイ機能の有効化

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. 次のいずれかを実行します。
   - デバイスのシステムテンプレートを作成します。
   - テーブルで、デバイスの既存のシステムテンプレートを見つけます。テンプレートの行で [...] をクリックし、[Edit] を選択します。
4. [Basic Configuration] セクションの [Transport Gateway] フィールドで、[On] を選択します。
5. 既存のテンプレートを編集している場合は、[Update]、[Configure Device] の順にクリックして、テンプレートを使用して更新をデバイスにプッシュします。

Cisco vManage を使用したトランスポート ゲートウェイ パスの設定の構成

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. 次のいずれかを実行します。
   - デバイスの OMP テンプレートを作成します。
   - テーブルで、デバイスの既存の OMP テンプレートを見つけます。テンプレートの行で […] をクリックし、[Edit] を選択します。
4. [Best Path] セクションの [Transport Gateway Path Behavior] フィールドで、[Global] モードを選択し、次のオプションのいずれかを選択します。

オプション	説明
Do ECMP Between Direct and Transport Gateway Paths	トランスポートゲートウェイとダイレクトパスを介して接続できるデバイスの場合、使用可能なすべてのパスに等コストマルチパス（ECMP）を適用します。
Prefer Transport Gateway Path	トランスポートゲートウェイを介して接続できるデバイスの場合、他のパスが使用可能な場合でも、トランスポートゲートウェイ パスのみを使用します。

5. 既存のテンプレートを編集している場合は、[Update]、[Configure Device] の順にクリックして、テンプレートを使用して更新をデバイスにプッシュします。

CLI を使用したトランスポートゲートウェイの設定

CLI を使用したルータでのトランスポートゲートウェイ機能の有効化

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

1. コンフィギュレーション モードを入力します。

```
Device#config-transaction
```

2. システム コンフィギュレーション モードを開始します。

```
Device(config)#system
```

3. トランスポートゲートウェイ機能を有効にします。

```
Device(config-system)#transport-gateway enable
```

（注） トランスポートゲートウェイ機能を無効にするには、このコマンドの **no** 形式を使用します。

CLI を使用したトランスポート ゲートウェイ パスの設定の構成

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

1. コンフィギュレーション モードを入力します。

   ```
   Device#config-transaction
   ```

2. システム コンフィギュレーション モードを開始します。

   ```
   Device(config)#sdwan
   ```

3. システム OMP コンフィギュレーション モードを開始します。

   ```
   Device(config)#omp
   ```

4. 次のいずれかのオプションを使用して、トランスポート ゲートウェイ パスの設定を構成します。

   ```
   Device(config-omp)#best-path transport-gateway {prefer | ecmp-with-direct-path}
   ```

オプション	説明
ecmp-with-direct path	トランスポートゲートウェイとダイレクトパスを介して接続できるデバイスの場合、使用可能なすべてのパスに等コストマルチパス（ECMP）を適用します。
prefer	トランスポートゲートウェイを介して接続できるデバイスの場合、他のパスが使用可能な場合でも、トランスポート ゲートウェイ パスのみを使用します。

例

```
Device#omp best-path transport-gateway prefer
```

CLI を使用したトランスポートゲートウェイ設定の確認

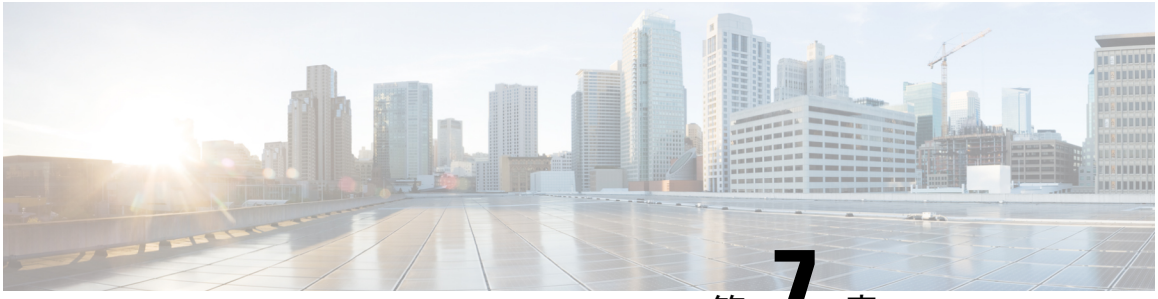
サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

デバイスで **show sdwan running-config system** コマンドを使用して、デバイスがトランスポートゲートウェイとして設定されているかどうかを確認します。出力では、[transport-gateway enable] は、設定されていることを示しています。

```
Device#show sdwan running-config system
system
system-ip             192.168.1.1
domain-id             1
site-id               11100
region 1
!
role                  border-router
```

```
transport-gateway enable
...
```

デバイスで **show sdwan omp summary** コマンドを使用して、デバイスがトランスポートゲートウェイとして設定されているかどうかを確認することもできます。出力では、[transport-gateway enabled] は、トランスポートゲートウェイ機能が有効になっていることを示しています。



第 7 章

ルータアフィニティ

表 *8*：機能の履歴

機能名	リリース情報	説明
マルチリージョンファブリック：ルータアフィニティ	Cisco IOS XE リリース 17.8.1a Cisco SD-WAN リリース 20.8.1 Cisco vManage リリース 20.8.1	多くの場合、ルータには、フローを宛先にルーティングするときにネクストホップとして選択するための複数のオプションがあります。複数のデバイスがフローのネクストホップとして機能できる場合、ルータアフィニティグループを構成することで、デバイス間の優先順位を指定できます。その結果、ルータは最初に優先度が最も高いネクストホップデバイスへのルートを使用しようとし、そのデバイスが使用できない場合は、次の優先度のネクストホップデバイスへのルートを使用しようとします。アフィニティグループは、複雑な制御ポリシーを必要とせずにこの機能を有効にします。
アフィニティグループの優先リストでのピアデバイスへのルートの優先順位付けの改善	Cisco SD-WAN コントローラリリース 20.9.x	この機能により、Cisco vSmart コントローラがデバイスにルートをアドバタイズする順序が変更されます。このリリースから、Cisco vSmart コントローラがデバイスにルートをアドバタイズする場合、（a）アフィニティグループの優先リスト内のピアデバイスへのルートに高い優先順位を与え、（b）より高い最適パススコアを持つ可能性があるが優先アフィニティグループに関連付けられたデバイスへのルートではないルートに低い優先順位を与えます。その効果は、優先アフィニティグループ内のピアデバイスへのルートに優先順位を付けることです。

ルータアフィニティグループに関する情報

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco SD-WAN リリース 20.8.1、Cisco vManage リリース 20.8.1

ルータアフィニティグループを使用すると、ネットワークフローの次の中継ホップとして機能できる複数のルータの中から選択する優先順位を指定できます。これは、（a）ルータがフローのネクストホップを決定している場合、および（b）マルチリージョンファブリックアーキテクチャ内の複数のルータがネクストホップとして機能できる場合に適用されます。機能の構成には 2 つの部分があります。

- ルータ上で、ルータアフィニティグループ ID（1 ～ 63 の数字）を割り当てます。
- ルータ上で、ネクストホップのルータを選択するための優先順位を割り当てます。これはアフィニティグループ ID の一覧です。

ルータ上で動作するオーバーレイ マネジメント プロトコル（OMP）がフローに最適なパスを選択すると、次のことが行われます。

1. フローの宛先のプレフィックスをアドバタイズしているルータに基づいて、考えられるネクストホップルータを決定します（これは標準の OMP 機能です）。
2. OMP は、最適なパスを選択するときに、考えられるネクストホップルータからアフィニティグループの設定を考慮し、それに応じて考えられるネクストホップルータに優先順位を付けます（これは、アフィニティグループ機能に固有です）。

その結果、ルータは最初に優先度が最も高いネクストホップデバイスへのルートを使用しようとし、そのデバイスが使用できない場合は、次の優先度のネクストホップデバイスへのルートを使用しようとします。アフィニティ優先リストに使用可能なデバイスがない場合、ルータはネクストホップとして機能できる他のデバイスへのルートを使用しようとします。これによる影響の 1 つとして、最初のネクストホップルータが使用できない場合に、1 つの考えられるネクストホップルータから別のネクストホップルータへの自動フェールオーバーがあります。アフィニティグループは、複雑な制御ポリシーを必要とせずにこの機能を有効にします。

ルーティングメカニズム

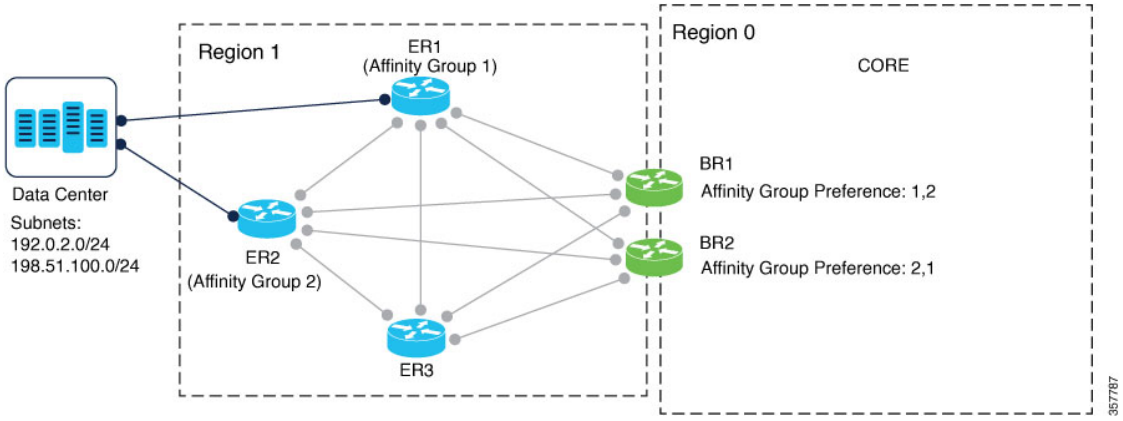
ルータアフィニティは、次のようにルート選択に影響します。

- 特定のネットワーク内、または マルチリージョン ファブリック の場合にはリージョン内では、オーバーレイ マネジメント プロトコル（OMP）がネットワーク内のデバイスによるプレフィックスのアドバタイズを管理します。

- デバイスがネットワークフローを宛先にルーティングする場合、OMP により、デバイスは宛先のプレフィックスをアドバタイズしているネクストホップデバイスを選択できます。
- プレフィックスへのネクストホップとして機能できるデバイスのみがプレフィックスをアドバタイズします。
- 考えられるネクストホップデバイスの中で、構成されたアフィニティグループの設定によって、ネクストホップの優先順位が決まります。

次の例では、エッジルータ ER1 および ER2 が、データセンターで使用されるサブネットをアドバタイズします。境界ルータ BR1 がデータセンターサブネットの 1 つにあるプレフィックスにフローをルーティングしている場合、ネクストホップとして ER1 または ER2 を使用できます。図に示すように、ER1 と ER2 で構成されたアフィニティグループ、および BR1 で構成されたアフィニティグループの優先順位に基づいて、BR1 は ER1 をネクストホップとして選択します。ER1 が使用できない場合、BR1 はフローをネクストホップとして ER2 にルーティングします。

図 *10* : ルータアフィニティの例



アフィニティ値で構成されたパスのみの使用

必要に応じて、ルータがアフィニティリストにあるルータにのみ接続できるように Cisco SD-WAN を構成できます。これを行うには、リージョンを管理する Cisco vSmart コントローラで [filter route outbound affinity-group preference] オプションを使用します。Cisco vSmart コントローラは、リージョン内の各デバイスに、アフィニティリストにあるルータへのルートのみを提供します。Cisco vManage を使用してアフィニティ優先リストのパスのみを提供するように Cisco vSmart コントローラを設定 （82 ページ）を参照してください。

このオプションは、アフィニティリストにないデバイスにルータを接続させたくない場合にのみ使用してください。利点は、管理するルートを少なくすることで、Cisco vSmart コントローラ およびエッジルータのメモリリソースを節約できることです。

アフィニティグループの優先リストでのピアデバイスへのルートの優先順位付け

Cisco SD-WAN コントローラリリース 20.9.x から、Cisco vSmart コントローラ がデバイスにルートをアドバタイズする場合、アフィニティグループの優先リスト内のピアデバイスへのルートのアドバタイズに高い優先順位を与え、より高い最適パススコアを持つ可能性があるが優先アフィニティグループに関連付けられたデバイスへのルートではないルートに低い優先順位を与えます。これは、送信パス制限が Cisco vSmart コントローラ に設定されていて、特定のデバイスにアドバタイズされるルートの数を制限している場合に特に重要です。これにより、ルータが限られた数のルートを管理している場合、ルートにアフィニティグループの優先リストにあるピアデバイスが含まれるようにします。

以下で、これがどのように機能するかをより詳細に説明します。

アフィニティグループごとに、Cisco vSmart コントローラ ではネットワーク内のデバイスによってアドバタイズされた各ルートのリンクリストが維持されます。Cisco vSmart コントローラ は、定義されたアフィニティグループごとに、2 つのリンクリストを作成します。

- （a）アフィニティグループ内のデバイス用で、（b）最適パス選択アルゴリズムによって選択されたルートのリスト（これらのルートは、最適パススコアが高く、アルゴリズムによって優先されることを意味します）
- （a）アフィニティグループ内のデバイス用であるが、（b）最適パス選択アルゴリズムによって選択されていないルートのリスト

最適パス選択アルゴリズムは、ルートの特性、ポリシー、およびその他の要因に基づいて選択されたルートを指定することに注意してください。

Cisco vSmart コントローラ が特定のデバイスへのルートをアドバタイズする場合、リンクリストを使用して、デバイスのアフィニティグループの優先リストにあるピアデバイスへのルートを優先します。

たとえば、前の図とほぼ一致しても、より多くの利用可能なルートがあるネットワークの場合は、次のシナリオを検討してください。

デバイス	デバイスによる Cisco vSmart コントローラへのルートのアドバタイズ	最適パス選択アルゴリズムの結果	結果のリンクリスト
アフィニティグループ 1 に割り当てられる ER1	ER1 には 4 つのルートがあり、それらをアフィニティグループ 1 に関連付けられたルートとして Cisco vSmart コントローラにアドバタイズします。	この例では、最適パス選択アルゴリズムにより、2 つのルートが選択済みとして指定され、2 つのルートが未選択として指定されます。	Cisco vSmart コントローラは、各ルートをリンクリストに追加します。 • アフィニティグループ 1 のリンクリスト、選択されたルート：2 ルート • アフィニティグループ 1 のリンクリスト、選択されていないルート：2 ルート （注） 「選択された」とは、この表の前で説明されているように、最適パス選択アルゴリズムによって選択されたことを意味します。

デバイス	デバイスによる Cisco vSmart コントローラへのルートのアドバタイズ	最適パス選択アルゴリズムの結果	結果のリンクリスト
アフィニティグループ 2 に割り当てられる ER2	ER2 には 3 つのルートがあり、それらをアフィニティグループ 2 に関連付けられたルートとして Cisco vSmart コントローラにアドバタイズします。	この例では、最適パス選択アルゴリズムにより、2 つのルートが選択済みとして指定され、1 つのルートが未選択として指定されます。	Cisco vSmart コントローラは、各ルートをリンクリストに追加します。 • アフィニティグループ 2 のリンクリスト、選択されたルート：2 ルート • アフィニティグループ 2 のリンクリスト、選択されていないルート：1 ルート
アフィニティグループに割り当てられていない ER3	ER3 には 3 つのルートがあり、それらをアフィニティグループ 0 に関連付けられたルートとして Cisco vSmart コントローラにアドバタイズします。 （アフィニティグループ 0 は、アフィニティグループに割り当てられていないデバイスに対応します。）	この例では、最適パス選択アルゴリズムにより、2 つのルートが選択済みとして指定され、1 つのルートが未選択として指定されます。	Cisco vSmart コントローラは、各ルートをリンクリストに追加します。 • アフィニティグループ 0 のリンクリスト、選択されたルート：2 ルート • アフィニティグループ 0 のリンクリスト、選択されていないルート：1 ルート

図に示すように、デバイス BR1 には 1、2 のアフィニティグループの優先リストがあります。このため、BR1 へのルートのアドバタイズには次の可能性があります。

- 送信パスの制限が定義されていない：

  Cisco vSmart コントローラ に送信パス制限が定義されていない場合、表に示すように、選択されたルートのリンクリストにある 6 つのルートすべてを BR1 にアドバタイズできます。ER1 に 2 つ、ER2 に 2 つ、ER3 に 2 つです。

- 送信パス制限が定義されている：

  Cisco vSmart コントローラ の送信パス制限が 4 の場合、ER1 のアフィニティグループ 1 で選択されたルートのリンクリストにある 2 つのルートを最初に BR1 にアドバタイズします。さらに、ER2 のアフィニティグループ 2 で選択されたルートのリンクリストにある 2 つのルートをアドバタイズします。この時点で、制限である 4 つのルートがアドバタイズされていて、アフィニティグループ 0（どのアフィニティグループにも割り当てられていないデバイス）で選択されたルートのリンクリスト内のルートはアドバタイズされません。したがって、ER3 のルートは含まれていません。その結果、BR1 のアフィニティグループの優先リストが 1、2 の場合、Cisco vSmart コントローラ では ER3 ルートの最適パススコアの方が高くても、ピアデバイス ER1 および ER2（アフィニティグループ 1 および 2 のデバイス）へのルートを優先します。

ワークフロー

- ルータ上で、アフィニティグループ ID 番号を設定します。

  『Cisco vManage を使用してデバイスでアフィニティグループまたはアフィニティグループ設定を構成 （81 ページ）』を参照してください。

- ルータ上で、アフィニティグループ ID 番号のリストを、優先順位の高いものから低いものの順に構成して、ルータに接続するための優先順位を指定します。

  Cisco vManage を使用してデバイスでアフィニティグループまたはアフィニティグループ設定を構成 （81 ページ）。

- 必要に応じて、アクセスリージョンを提供する Cisco vSmart コントローラ で、ルータがアフィニティグループの優先リストにあるデバイスのみに接続するように制限します。

  Cisco vManage を使用してアフィニティ優先リストのパスのみを提供するように Cisco vSmart コントローラを設定 （82 ページ）を参照してください。

ルータアフィニティグループの利点

ルータアフィニティグループは、ネクストホップに複数のルータを使用できる場合に、デバイスから特定のルータに優先的にトラフィックを転送できるようにすることで、キャパシティプランとロードバランシングに役立ちます。

ルータアフィニティグループでサポートされるデバイス

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco SD-WAN リリース 20.8.1、Cisco vManage リリース 20.8.1

- Cisco IOS XE SD-WAN デバイスについて
- Cisco vEdge デバイスについて

ルータアフィニティグループの制約事項

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco SD-WAN リリース 20.8.1、Cisco vManage リリース 20.8.1

アフィニティグループの範囲は 1 ～ 63 に制限されています。

ルータアフィニティグループのユースケース

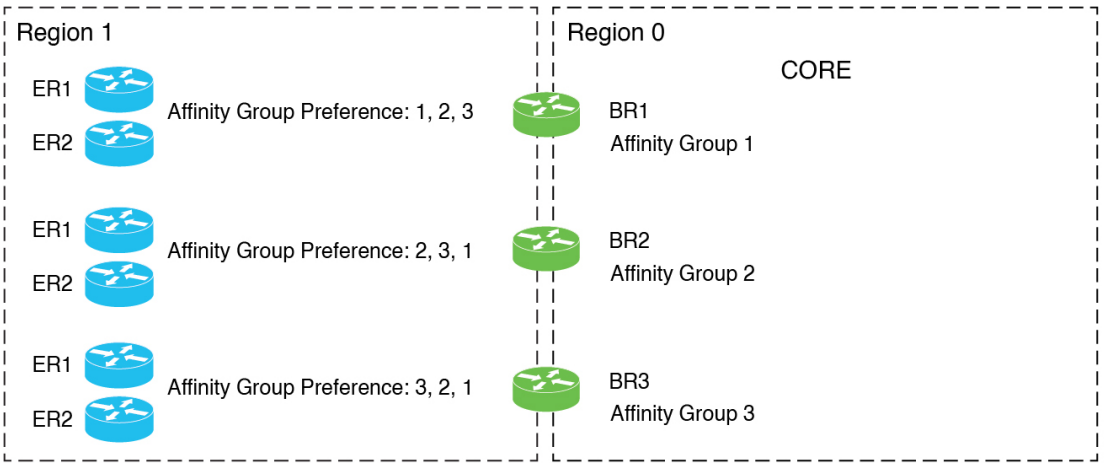
ユースケース 1：境界ルータへのアクセス リージョン トラフィックのロードバランシング

アクセスリージョンに 6 つのエッジルータ（ER1 ～ ER6）と 3 つの境界ルータ（BR1、BR2、およびBR3）があるシナリオでは、次のようにアフィニティグループを使用して負荷を分散できます。

デバイス	設定	結果
BR1	アフィニティグループ 1 を割り当てます。	
BR2	アフィニティグループ 2 を割り当てます。	
BR3	アフィニティグループ 3 を割り当てます。	
ER1 と ER2	アフィニティグループの優先順位1、2、3 を割り当てます。	これら 2 つのエッジルータは、ネクストホップのためにトラフィックを優先的に BR1 に転送しますが、BR1 が使用できない場合、BR2 の使用を試みます。BR2 が使用できない場合は、BR3 の使用を試みます。
ER3 と ER4	アフィニティグループの優先順位2、3、1 を割り当てます。	これら 2 つのエッジルータは、ネクストホップのためにトラフィックを優先的に BR2 に転送しますが、BR2 が使用できない場合、BR3 の使用を試みます。BR3 が使用できない場合は、BR1 の使用を試みます。

デバイス	設定	結果
ER5 と ER6	アフィニティグループの優先順位3、1、2 を割り当てます。	これら 2 つのエッジルータは、ネクストホップのためにトラフィックを優先的に BR3 に転送しますが、BR3 が使用できない場合、BR1 の使用を試みます。BR1 が使用できない場合は、BR2 の使用を試みます。

図 *11* : ユースケース *1* : 境界ルータへのアクセス リージョン トラフィックのロードバランシング

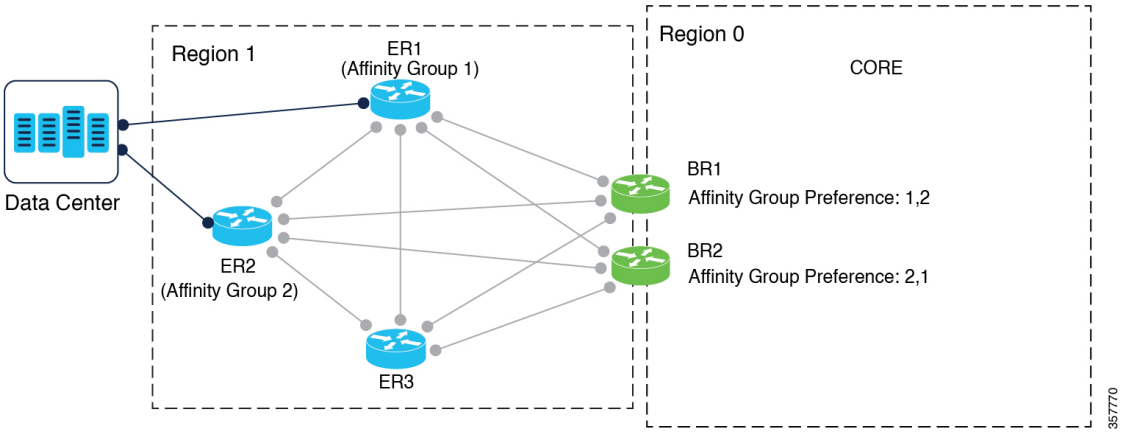


ユースケース 2 : エッジルータへのアクセス リージョン トラフィックのロードバランシング

アクセスリージョンに大容量データセンターにサービスを提供する 2 つのエッジルータ（ER1 と ER2）と 2 つの境界ルータ（BR1 と BR2）があるシナリオでは、次のようにアフィニティグループを使用して負荷を分散できます。

デバイス	設定	結果
ER1	アフィニティグループ 1 を割り当てます。	
ER2	アフィニティグループ 2 を割り当てます。	
BR1	アフィニティグループの優先順位1、2 を割り当てます。	この境界ルータは、データセンターのトラフィックを優先的に ER1 に転送しますが、ER1 が使用できない場合は ER2 を使用できます。
BR2	アフィニティグループの優先順位2、1 を割り当てます。	この境界ルータは、データセンターのトラフィックを優先的に ER2 に転送しますが、ER2 が使用できない場合は ER1 を使用できます。

図 *12 :* ユースケース *2* : エッジルータへのアクセス リージョン トラフィックのロードバランシング

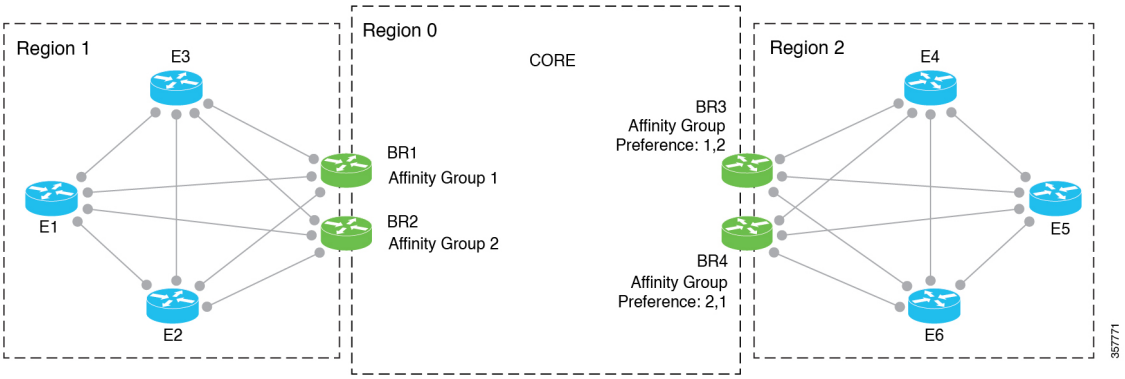


ユースケース 3 : コアリージョントラフィックのロードバランシング

大容量アクセスリージョン（リージョン 1）に 2 つの境界ルータ（BR1 と BR2）があり、2 つの境界ルータ（BR3 と BR4）を持つ別のアクセスリージョン（リージョン 2）から大量のトラフィックを受信するシナリオでは、次のようにアフィニティグループを使用して負荷を分散できます。

デバイス	設定	結果
BR1 （リージョン 1）	アフィニティグループ 1 を割り当てます。	
BR2 （リージョン 1）	アフィニティグループ 2 を割り当てます。	
BR3 （リージョン 2）	アフィニティグループの優先順位1、2 を割り当てます。	トラフィックをリージョン 1 に転送する場合、この境界ルータはトラフィックを優先的に BR1 に転送しますが、BR1 が使用できない場合は BR2 を使用できます。
BR4 （リージョン 2）	アフィニティグループの優先順位2、1 を割り当てます。	トラフィックをリージョン 1 に転送する場合、この境界ルータはトラフィックを優先的に BR2 に転送しますが、BR2 が使用できない場合は BR1 を使用できます。

図 *13* : ユースケース *3* : コアリージョントラフィックのロードバランシング



Cisco vManage を使用したルータアフィニティグループの設定

Cisco vManage を使用してデバイスでアフィニティグループまたはアフィニティグループ設定を構成

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco SD-WAN リリース 20.8.1、Cisco vManage リリース 20.8.1

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. 次のいずれかを実行します。
   - デバイスのシステムテンプレートを作成します。
   - テーブルで、デバイスの既存のシステムテンプレートを見つけます。テンプレートの行で [...] をクリックし、[Edit] を選択します。
4. アフィニティグループを境界ルータに割り当てるには、[Advanced] セクションの [Affinity Group] フィールドで、モードを [Global] に変更し、アフィニティグループ番号を 1 ～ 63 の範囲で入力します。

   アフィニティグループがデバイスで以前に構成されている場合、新しい値が以前の値に置き換わります。
5. 境界ルータまたはエッジルータのアフィニティグループの優先順位を構成するには、[Advanced] セクションの [Affinity Group Preference] フィールドで、モードを [Global] に変更し、アフィニティグループ番号のコンマ区切りリストを入力します。これにより、境界ルータへの接続の優先順位が決まります。アフィニティグループの範囲は 1 ～ 63 です。

例：10、11、1、5

（注） アフィニティグループの優先リストにないルートを除外するように Cisco vSmart コントローラを設定すると、デバイスはアフィニティグループ内のルータにのみ接続できます。Cisco vManage を使用してアフィニティ優先リストのパスのみを提供するように Cisco vSmart コントローラを設定 （82 ページ）を参照してください。

6. 既存のテンプレートを編集している場合は、[Update]、[Configure Device] の順にクリックして、テンプレートを使用して更新をデバイスにプッシュします。

Cisco vManage を使用してアフィニティ優先リストのパスのみを提供するように Cisco vSmart コントローラを設定

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco SD-WAN リリース 20.8.1、Cisco vManage リリース 20.8.1

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. 次のいずれかを実行します。
   - Cisco vSmart コントローラ の OMP テンプレートを作成します。
   - テーブルで、Cisco vSmart コントローラ の既存の OMP テンプレートを見つけます。テンプレートの行で [...] をクリックし、[Edit] を選択します。
4. [Best Path] セクションの [Enable Filtering Route Updates Based on Affinity] フィールドで、[Global] モードを選択し、[On] を選択します。
5. 既存のテンプレートを編集している場合は、[Update]、[Configure Device] の順にクリックして、テンプレートを使用して更新を Cisco vSmart コントローラ にプッシュします。

CLI を使用したルータアフィニティグループの設定

CLI を使用したルータでのアフィニティグループの設定

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco SD-WAN リリース 20.8.1、Cisco vManage リリース 20.8.1

1. コンフィギュレーション モードを入力します。

```
Device#config-transaction
```

2. システム コンフィギュレーション モードを開始します。

```
Device(config)#system
```

3. アフィニティグループ ID を 1 ～ 63 の範囲で設定します。

   アフィニティグループがデバイスで以前に構成されている場合、新しい値が以前の値に置き換わります。

```
Device(config-system)#affinity-group group-id
```

例

```
Device#config-transaction
Device(config)#system
Device(config-system)#affinity-group 10
```

CLI を使用したルータでのアフィニティグループ設定の構成

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco SD-WAN リリース 20.8.1、Cisco vManage リリース 20.8.1

1. コンフィギュレーション モードを入力します。

```
Device#config-transaction
```

2. システム コンフィギュレーション モードを開始します。

```
Device(config)#system
```

3. 1 ～ 63 の範囲のグループ ID のリストを入力して、アフィニティグループの優先順位を最高の優先順位から最低の優先順位まで示します。グループ ID はスペースで区切ります。

```
Device(config-system)#affinity-group preference group-id [group-id ...]
```

例

```
Device(config-system)#affinity-group preference 10 11 1 5
```

CLI を使用してアフィニティグループ優先リストのパスのみを提供するように Cisco vSmart コントローラを設定

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco SD-WAN リリース 20.8.1、Cisco vManage リリース 20.8.1

1. コンフィギュレーション モードを入力します。

```
vSmart#config terminal
```

2. システム OMP コンフィギュレーション モードを開始します。

```
vSmart(config)#omp
```

3. アフィニティグループの優先リスト内のルータへのパスのみを各ルータに提供するように Cisco vSmart コントローラ を設定します。

これにより、ルータは、アフィニティグループの優先リストにあるルータのみに接続するように制限されます。

```
vSmart(config-omp)#filter-route outbound affinity-group-preference
```

（注） この設定を無効にするには、このコマンドの **no** 形式を使用します。デフォルトでは、無効になっています。

例

```
vSmart#config terminal
vSmart(config)#omp
vSmart(config-omp)#filter-route outbound affinity-group-preference
```

Cisco vManage を使用したアフィニティグループとアフィニティグループ設定の確認

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco SD-WAN リリース 20.8.1、Cisco vManage リリース 20.8.1

1. Cisco vManage メニューから、**[Monitor]** > **[Devices]** の順に選択します。
2. テーブルで、デバイスをクリックします。
3. [Real Time] をクリックします。
4. [Device Options] フィールドで、[OMP Summary] を選択します。

   [Affinity Group Number] および [Affinity Group Preference] フィールドを参照してください。

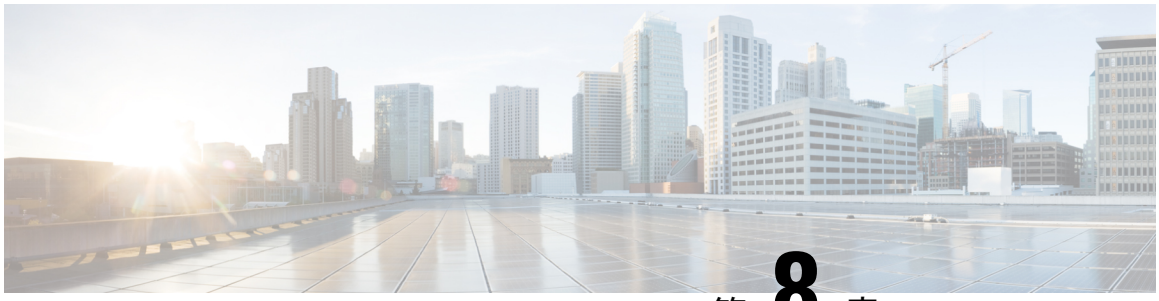
CLI を使用したアフィニティグループとアフィニティグループ設定の確認

デバイスのアフィニティグループとアフィニティグループ設定を表示するには、**show sdwan running-config system** コマンドを使用します。[affinity-group preference] フィールドには、優先リストが表示されます。

例

```
Device#show sdwan running-config system
system
 system-ip          192.168.0.1
 domain-id          1
 site-id            1100
 affinity-group 10
```

```
 affinity-group preference 15 16
...
```



第 8 章

マルチリージョン ファブリック ポリシー

表 *9*：機能の履歴

機能名	リリース情報	説明
宛先によるトラフィックの一致：アクセスリージョン、コアリージョン、またはサービス VPN	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1	宛先がアクセスリージョン、コアリージョン、サービス VPN のいずれかであるトラフィックにポリシーを適用できます。この一致条件は、境界ルータのデータポリシーまたはアプリケーション ルート ポリシーに使用します。
パスタイプに応じたルートの一致	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1	マルチリージョン ファブリック アーキテクチャの制御ポリシーを構成する場合、ルートが階層パス、ダイレクトパス、またはトランスポート ゲートウェイ パスのいずれを使用しているかに応じてルートを一致させることができます。
制御ポリシーのリージョンおよびロールによるルートの一致	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1	制御ポリシーでは、ルートを発信するデバイスのリージョン、またはルートを発信するデバイスのロール（エッジルータまたは境界ルータ）に従って、ルートを一致させることができます。
宛先リージョンによるトラフィックの一致	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	アプリケーション ルート ポリシーまたはデータポリシーを作成するときに、宛先リージョンに応じてトラフィックを一致させることができます。宛先は、同じプライマリリージョン、同じセカンダリリージョン、またはこれらのいずれでもないデバイスである場合があります。

機能名	リリース情報	説明
パスタイプの設定を指定	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	一元化されたポリシーを構成する場合、プライマリ、セカンダリ、およびターシャリと呼ばれる3つのレベルのルート設定を指定する優先カラーグループリストを作成できます。ルート設定は、TLOCカラーと、オプションでパスタイプ（ダイレクトトンネル、マルチホップパス、またはすべてのパス）に基づいています。パスタイプは、マルチリージョンファブリック を使用しているネットワークに関連しています。

マルチリージョンファブリックのポリシーの設定に関する情報

パスのタイプ、リージョン、またはロールによるルートの一致

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

パスタイプ

マルチリージョン ファブリック アーキテクチャの制御ポリシーを設定する場合、ルートが次のいずれかを使用しているかどうかに応じてルートを一致させることができます。

- 階層パス：アクセスリージョンから境界ルータへ、リージョン 0 を経由して、別の境界ルータへ、さらに別のアクセスリージョンのエッジルータへのホップを含むルートに一致します。

  階層パスルートを表示するには、**show sdwan omp routes** コマンドを使用し、[REGION PATH] 列に 3 つのリージョンをリストするルートを書き留めます。

- ダイレクトパス：あるエッジルータから別のエッジルータへのダイレクトパス（ダイレクトルート）に一致します。セカンダリリージョンを構成し、2 つのエッジルータをセカンダリリージョンに追加することにより、異なるアクセスリージョンのエッジルータ間のダ

イレクトパスを有効にすることができます。セカンダリリージョンに関する情報（49ページ）を参照してください。

ダイレクトパスルートを表示するには、**show sdwan omp routes** コマンドを使用し、[REGION PATH] 列に 1 つのリージョンをリストするルートを書き留めます。

- トランスポート ゲートウェイ パス：トランスポートゲートウェイ機能が有効になっているルータによって再発信されたルートに一致します。

  トランスポートゲートウェイについては、トランスポートゲートウェイに関する情報（63ページ）を参照してください。

リージョンとロール

パスタイプによる一致と同様に、ルートを発信するデバイスのリージョンまたはロール（エッジルータまたは境界ルータ）によってルートを一致させることができます。

Traffic-To に一致

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

バックグラウンド

フラットな非 マルチリージョン ファブリック アーキテクチャでは、各エッジルータは次のいずれかの方法でトラフィックフローを処理します。

- サービス VPN からオーバーレイネットワークへ
- サービス VPN からサービス VPN へ
- オーバーレイネットワークからサービス VPN へ
- オーバーレイネットワークから同じオーバーレイネットワークへ

これらのタイプのトラフィックのいずれかをトラフィックポリシーの対象にするには、次のように、トラフィックポリシーを適用するときに **apply-policy** キーワードを使用できます。

表 *10 : apply-policy* の使用

トラフィックタイプ	使用するコマンド
サービス VPN からオーバーレイネットワークへ および サービス VPN からサービス VPN へ	**apply-policy from-service**

トラフィックタイプ	使用するコマンド
オーバーレイネットワークからサービス VPN へ および オーバーレイネットワークから同じオーバーレイネットワークへ	**apply-policy from-tunnel**

マルチリージョン ファブリック：複数のオーバーレイネットワーク

マルチリージョンファブリックアーキテクチャと境界ルータのロールの導入により、境界ルータは、あるオーバーレイネットワークから別のオーバーレイネットワークへ（アクセスリージョンからコアリージョンへ、またはコアリージョンからアクセスリージョンへ）のトラフィックフローを処理できます。境界ルータは、次のいずれかの方法でトラフィックフローを処理できます。

- アクセスリージョンから次のいずれかへ：
  - アクセスリージョン
  - コアリージョン
  - サービス VPN
- コアリージョンから次のいずれかへ：
  - アクセスリージョン
  - コアリージョン
  - サービス VPN
- サービス VPN から次のいずれかへ：
  - アクセスリージョン
  - コアリージョン
  - サービス VPN

境界ルータでのトラフィックフローの方向が多い場合、**apply-policy** オプションは十分な粒度を提供しません。**traffic-to** 一致基準はこれに対処し、これらのタイプのトラフィックフローをそれぞれ指定できるようにします。

一致基準：Traffic-To

境界ルータのデータポリシーまたは app-route ポリシーを作成する場合、次の一致基準を使用して、アクセスリージョン、コアリージョン、またはサービス VPN へのトラフィックフローを一致させることができます。

- **traffic-to access**：次のいずれかの方法のすべてのトラフィックフローに一致します。
  - サービス VPN からアクセスリージョンへ
  - コアリージョンからアクセスリージョンへ
  - アクセスリージョンからアクセスリージョンへ
- **traffic-to core**：次のいずれかの方法のすべてのトラフィックフローに一致します。
  - サービス VPN からコアリージョンへ
  - アクセスリージョンからコアリージョンへ
  - コアリージョンからコアリージョンへ
- **traffic-to service**：次のいずれかの方法のすべてのトラフィックフローに一致します。
  - アクセスリージョンからサービス VPN へ
  - コアリージョンからサービス VPN へ
  - あるサービス VPN から別のサービス VPN へ

これらの一致条件は、**prefix-list**、**site-list** などのマルチリージョン ファブリック に固有ではない他の一致条件と一緒に使用できます。

一致条件と Apply-Policy キーワードの組み合わせ

ポリシーを適用するときに、これらの一致条件を使用でき、次の表で説明するように、ポリシーをトラフィックに適用するときに **apply-policy** キーワードを使用できます。

表 *11 : Traffic-To* と *Apply-Policy*

一致条件	apply-policy キーワード	効果：ポリシーは次のトラフィックに作用します
match traffic-to access	**from-tunnel** （アクセスおよびコアリージョンからのトラフィックを含む）	アクセスリージョンからアクセスリージョンへ および コアリージョンからアクセスリージョンへ
	from-service （サービス VPN トンネルからのトラフィックを含む）	サービス VPN からアクセスリージョンへ
	all （アクセスリージョンとコアリージョン、およびサービス VPN トンネルからのトラフィックを含む）	アクセスリージョンからアクセスリージョンへ および コアリージョンからアクセスリージョンへ および サービス VPN からアクセスリージョンへ

一致条件	apply-policy キーワード	効果：ポリシーは次のトラフィックに作用します
match traffic-to core	**from-tunnel** （アクセスおよびコアリージョンからのトラフィックを含む）	コアリージョンからコアリージョンへ および アクセスリージョンからコアリージョンへ
	from-service （サービス VPN トンネルからのトラフィックを含む）	サービス VPN からコアリージョンへ
	all （アクセスリージョンとコアリージョン、およびサービス VPN トンネルからのトラフィックを含む）	コアリージョンからコアリージョンへ および アクセスリージョンからコアリージョンへ および サービス VPN からコアリージョンへ
match traffic-to service	**from-tunnel** （アクセスおよびコアリージョンからのトラフィックを含む）	コアリージョンからサービス VPN へ および アクセスリージョンからサービス VPN へ
	from-service （サービス VPN トンネルからのトラフィックを含む）	サービス VPN からサービス VPN へ
	all （アクセスリージョンとコアリージョン、およびサービス VPN トンネルからのトラフィックを含む）	コアリージョンからサービス VPN へ および アクセスリージョンからサービス VPN へ および あるサービス VPN から別のサービス VPN へ

リージョンとロールによる一致

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco SD-WAN リリース 20.8.1、Cisco vManage リリース 20.8.1

制御ポリシーを設定するときは、ルートを発信するデバイスのリージョン、またはルートを発信するデバイスのロール（エッジルータまたは境界ルータ）に従って、ルートと TLOC を一致させることができます。発信元デバイスは、エッジルータまたは境界ルータのいずれかです。

（注） Cisco IOS XE SD-WAN デバイス のみが境界ルータのロールをサポートします。

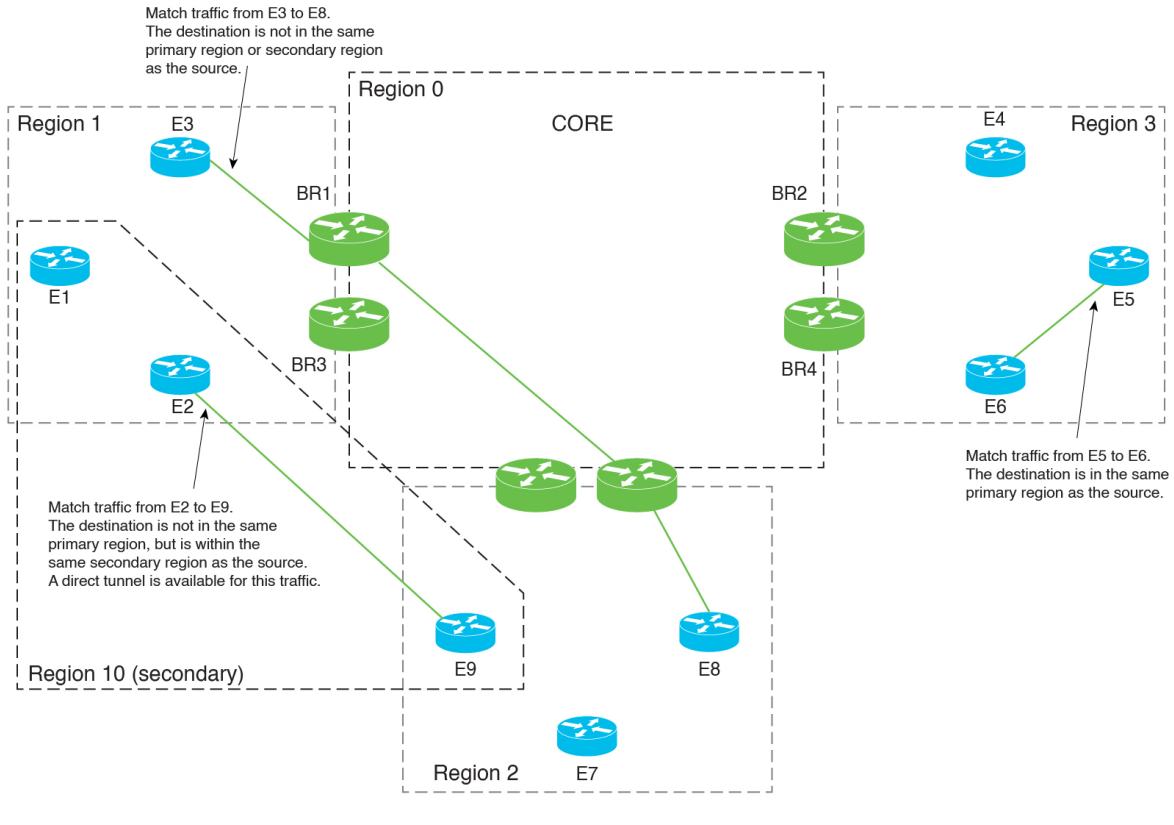
宛先リージョンに応じたトラフィックの一致に関する情報

最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco vManage リリース 20.9.1

アプリケーション ルート ポリシーまたはデータポリシーを作成する場合、次のオプションを使用して、トラフィックの宛先のリージョンに応じてトラフィックを一致させることができます。

- [Primary]：宛先デバイスが送信元と同じプライマリリージョン（アクセスリージョンとも呼ばれる）にある場合、トラフィックに一致します。このトラフィックは、アクセスリージョンの双方向フォワーディング検出（BFD）を使用して宛先に到達します。
- [Secondary]：宛先デバイスが送信元と同じプライマリリージョンにないが、送信元と同じセカンダリリージョンにある場合、トラフィックに一致します。このトラフィックは、セカンダリリージョンで説明されているように、ダイレクトトンネルを使用して宛先に到達できます。
- [Other]：宛先デバイスが送信元と同じプライマリリージョンまたはセカンダリリージョンにない場合、トラフィックに一致します。このトラフィックには、送信元から宛先へのマルチホップパスが必要です。

図 *14 :* 宛先によるトラフィックの一致



パスの設定の構成に関する情報

最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco vManage リリース 20.9.1

一元化されたポリシーを設定する場合、プライマリ、セカンダリ、およびターシャリと呼ばれる3つのレベルのルート設定を指定する優先カラーグループリストを作成できます。ルート設定は、次のいずれかまたは両方に基づいています。

- TLOC カラー
- マルチリージョン ファブリック を使用するネットワークに関連するパスタイプ（ダイレクトトンネル、マルチホップパス、またはすべてのパス）

アプリケーション認識型ルーティング（AAR）ポリシーまたはトラフィックデータポリシーを設定する場合、シーケンスのアクション部分で優先カラーグループリストを使用して、一致したトラフィックのルーティング方法を指定できます。

ポリシーリスト設定の構成の詳細については、『Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x』の「Configure Centralized Policies Using Cisco vManage」を参照してください。

手順の順序

1. 優先カラーグループリストを作成します。
2. 優先カラーグループリストで、パス設定（ダイレクトトンネルまたはマルチホップパス）を指定します。
3. AARポリシーまたはトラフィックデータポリシーで優先カラーグループリストを使用します。

その結果、ポリシーは、優先カラーグループリストで設定したパス設定を適用します。

マルチリージョンファブリックポリシーオプションでサポートされるデバイス

- ポリシーの一致条件
  - traffic-to に一致：Cisco IOS XE SD-WAN デバイス のみ
  - リージョンに一致：Cisco IOS XE SD-WAN デバイス および Cisco vEdge デバイス
  - ロールに一致：Cisco IOS XE SD-WAN デバイス および Cisco vEdge デバイス
  - 宛先リージョンによる一致：Cisco IOS XE SD-WAN デバイス および Cisco vEdge デバイス

    （最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco SD-WAN リリース 20.9.1）
- ポリシーアクション：
  - パスの設定：Cisco IOS XE SD-WAN デバイス および Cisco vEdge デバイス

    （最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco SD-WAN リリース 20.9.1）

マルチリージョンファブリックポリシーオプションの制約事項

- traffic-to に一致：この一致条件は、境界ルータに適用されるポリシーでのみ使用します。このようなポリシーをエッジルータに適用しても効果はありません。
- パス設定：マルチリージョン ファブリック を使用しないネットワークのポリシーを作成する場合は、パス設定を定義しないか、すべてのパスを使用するオプションを選択します（パス設定を定義しないことと同じになります）。

マルチリージョン ファブリックのユースケース

以下は、マルチリージョン ファブリック ポリシー機能のユースケースです。

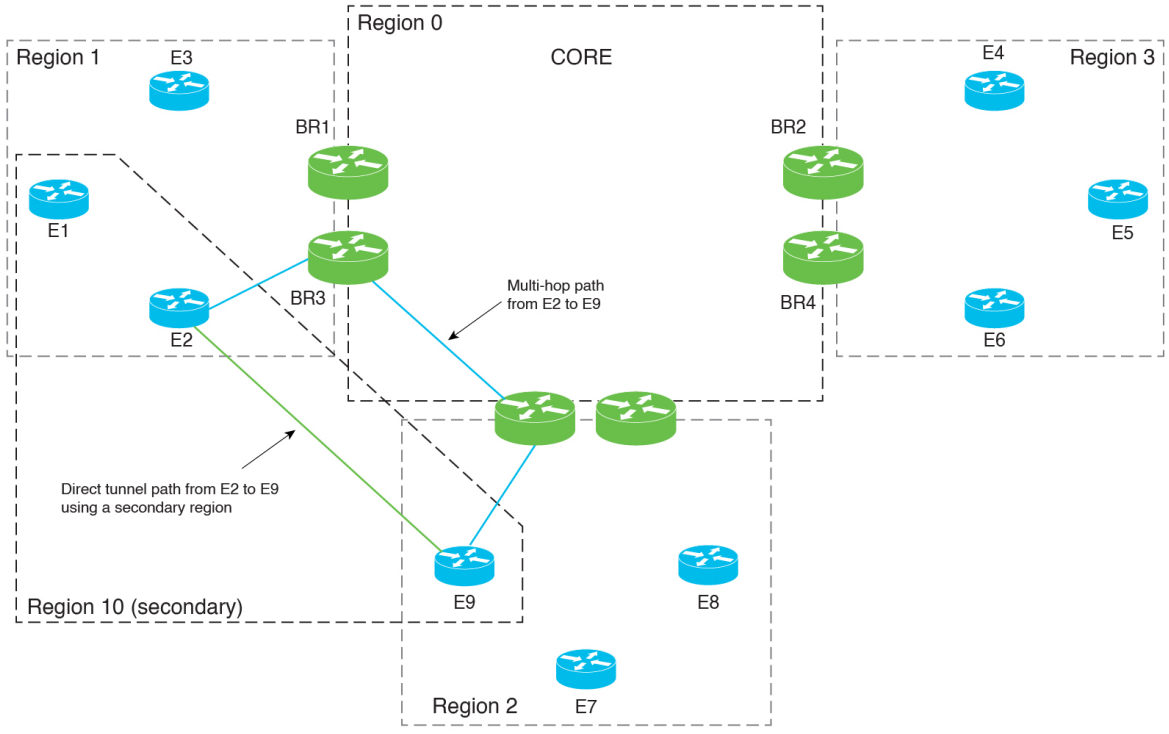
パス設定の構成のユースケース

最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco vManage リリース 20.9.1

マルチリージョン ファブリック ネットワークを使用している組織は、セカンダリリージョンを構成して、異なるプライマリリージョンにある2つのエッジルータ間のダイレクトトンネルパスを有効にします。

2 つのエッジルータ間のトラフィックは、コアリージョンを介したマルチホップパスを使用できるか、セカンダリリージョンによって可能になるダイレクトトンネルパスを使用できます。ダイレクトパスは、重要なトラフィックを対象としています。プレミアムキャリアを使用し、このパスのトラフィック量に基づいて課金されます。

図 *15*：マルチホップパスとダイレクトトンネルパス



重要なトラフィックのみをダイレクトパス経由で優先的にルーティングするポリシーを作成するために、ネットワーク管理者は 2 つの優先カラーグループリスト A と B を作成します。

- 優先カラーグループリスト A は、重要でないトラフィックを対象としています。マルチホップパスのプライマリ設定を指定します。セカンダリ設定は、ダイレクトトンネルパス

を指定します。セカンダリ設定を含めることで、マルチホップパスが使用できない場合のバックアップパスが提供されます。

- 優先カラーグループリストBは、重要なトラフィックを対象としています。これは、料金が発生するプレミアムリンクであるダイレクトトンネルパスのプライマリ設定を指定します。そのセカンダリ設定は、マルチホップパスを指定します。これにより、ダイレクトトンネルパスが使用できない場合のバックアップパスが提供されます。

ネットワーク管理者は、次の 2 つのシーケンスでアプリケーション ルーティング ポリシーを作成します。

- シーケンス 1 は重要でないトラフィックに一致し、そのアクションのために、優先カラーグループリスト A が適用されます。
- シーケンス 2 は重要なトラフィックに一致し、そのアクションのために、優先カラーグループリスト B が適用されます。

Cisco vManage を使用した マルチリージョン ファブリック ポリシーの設定

Cisco vManage を使用して Traffic-To に一致するデータポリシーまたはアプリケーション ルート ポリシーを設定

はじめる前に

ポリシーを適用するときに使用する VPN リストを構成します。

Traffic-To に一致するデータポリシーまたはアプリケーション ルート ポリシーを設定

1. Cisco vManage メニューから、**[Configuration]** > **[Policies]** を選択します。
2. [Centralized Policies] をクリックします。
3. 次のいずれかを実行します。
   - 新しいポリシーを作成するには、[Add Policy] をクリックします。
   - 既存のポリシーを編集するには、ポリシーの行で [...] をクリックし、[Edit Policy] をクリックします。
4. [Next] をクリックします。
5. [Next] をクリックします。
6. 次のいずれかをクリックして、トラフィックポリシーを作成します。

- Application Aware Routing
- **Traffic Data**

7. [Add Policy] をクリックし、[Create New] を選択します。

（注） 既存のポリシーを再利用するには、[Import Existing] を選択できます。

8. 新しいポリシーの名前と説明を入力します。
9. [Sequence Type] をクリックし、[Custom] を選択します。
10. [Sequence Rule] をクリックします。
11. [Match]（デフォルトで選択）をクリックし、[Traffic To] をクリックします。
12. [Match Conditions] 領域の [Traffic To] フィールドで、次のいずれかを選択します。
    - Access
    - Core
    - Service
13. シーケンスのアクションを選択し、ポリシーの構成を完了します。

    一般的なトラフィックポリシーの作成については、『Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x』の「Centralized Policy」を参照してください。
14. ポリシーを保存するには、作成するポリシーのタイプに応じて、[Save Application Aware Routing Policy] または [Save Data Policy] をクリックします。新しいポリシーを表に示します。
15. [Next] をクリックします。
16. [Apply Policies to Sites and VPNs] ステップで、適用するポリシーの名前を入力します。
17. 作成および適用するポリシーのタイプに応じて、次のいずれかをクリックします。
    - Application-Aware Routing
    - Traffic Data
18. [New Site/Region List and VPN List] をクリックします。
19. トラフィックデータポリシーを設定している場合は、次のいずれかのオプションを選択します。
    - From Service
    - From Tunnel
    - All

20. 次のいずれかのオプションを選択して、ポリシーを適用するサイトまたは マルチリージョン ファブリック リージョンを構成します。
    - [Site List]：サイトリストを選択します。
    - [Region]：マルチリージョン ファブリック リージョン ID を入力するか、リージョンリストを選択します。
21. データポリシーを設定している場合は、次の手順を実行します。
    1. [Select VPN List] フィールドで、VPN リストを選択します。
    2. [Add] をクリックします。
22. [Role Mapping for Regions] をクリックします。
23. リージョン ID またはリージョンリストごとに、[Role] 列で、[Edge] または [Border] のロールを選択します。ロールを選択しない場合は、Cisco vManage はリージョン内のすべてのルータにポリシーを適用します。

（注） Traffic-To で一致するポリシーについては、[Border] を選択します。この一致条件は、エッジルータには影響しません。

24. [Save Policy] をクリックします。新しいポリシーを表に示します。必要に応じて、ポリシーの詳細を表示するには、ポリシーの行で […] をクリックし、[Preview] を選択します。

CiscovManageを使用してリージョンとロールに一致する制御ポリシーを設定

1. Cisco vManage メニューから、**[Configuration]** > **[Policies]** を選択します。
2. [Centralized Policies] をクリックします。
3. 次のいずれかを実行します。
    - 新しいポリシーを作成するには、[Add Policy] をクリックします。
    - 既存のポリシーを編集するには、ポリシーの行で […] をクリックし、[Edit Policy] をクリックします。
4. [Next] をクリックします。
5. [Configure Topology and VPN Membership] ステップで、[Add Topology] をクリックし、[Custom Control (Route & TLOC)] を選択します。
6. 新しいポリシーの名前と説明を入力します。

7. [Sequence Rule] をクリックします。
8. [Match]（デフォルトで選択）をクリックし、[Region] をクリックします。
9. [Match Conditions] 領域で、次のいずれかを実行します。
   - [Region List] フィールドに、事前設定済みのリージョンリスト名を入力します。

（注） フィールドをクリックし、[New Region List] を選択してリストを定義できます。

   - [Region ID] フィールドに、単一のリージョン ID を入力します。
10. （オプション）構成されたリージョン内のルータタイプを指定するには、[Role]をクリックし、[Border] または [Edge] を選択します。
11. シーケンスのアクションを選択し、ポリシーの構成を完了します。

    一般的なトラフィックポリシーの作成については、『Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x』の「Centralized Policy」を参照してください。
12. ポリシーを保存するには、[Save Control Policy] をクリックします。新しいポリシーを表に示します。
13. [Next] をクリックします。
14. [Apply Policies to Sites and VPNs] ステップで、適用するポリシーの名前を入力します。
15. [トポロジ（Topology）] をクリックします。
16. [New Site/Region List] をクリックします。
17. 次のいずれかのオプションを選択して、ポリシーを適用するサイトまたは マルチリージョン ファブリック リージョンを構成します。
    - [Site List]：サイトリストを選択します。
    - [Region]：マルチリージョン ファブリック リージョン ID を入力するか、リージョンリストを選択します。
18. [Role Mapping for Regions] をクリックします。
19. リージョン ID またはリージョンリストごとに、[Role] 列で、[Edge] または [Border] のロールを選択します。ロールを選択しない場合は、Cisco vManage はリージョン内のすべてのルータにポリシーを適用します。

（注） Traffic-To で一致するポリシーについては、[Border] を選択します。この一致条件は、エッジルータには影響しません。

20. [Save Policy] をクリックします。新しいポリシーを表に示します。必要に応じて、ポリシーの詳細を表示するには、ポリシーの行で [...] をクリックし、[Preview] を選択します。

Cisco vManage を使用した宛先リージョンに応じたトラフィックの一致

最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco vManage リリース 20.9.1

アプリケーション認識型ルーティング（AAR）ポリシーまたはトラフィックデータポリシーの設定の詳細については、『Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x』の「Configure Centralized Policies Using Cisco vManage」を参照してください。ここでの情報は、[Destination Region] 一致条件の使用方法のみを扱っています。

アプリケーション認識型ポリシーまたはトラフィックデータポリシーには、次の手順を使用します。

1. Cisco vManage メニューから、**[Configuration]** > **[Policies]** を選択します。
2. デフォルトで選択されている [Centralized Policy] を選択します。
3. [Add Policy] をクリックします。
4. 必要に応じて、リストタイプをクリックしてリストを定義できます。
5. [Next] をクリックします。
6. 必要に応じて、トポロジを追加します。
7. **[Next]** をクリックします。
8. 次のいずれかを実行します:
   - AAR ポリシーの場合、デフォルトで選択されている [Application Aware Routing] をクリックします。
   - トラフィックデータポリシーの場合、[Traffic Data] をクリックします。
9. [Add Policy] をクリックし、[Create New] を選択します。
10. 次のいずれかを実行します。
    - AAR ポリシーの場合、[Sequence Type] をクリックして、宛先ごとにトラフィックを一致させるシーケンスを作成します。
    - トラフィックデータポリシーの場合、[Sequence Type] をクリックし、[Custom] を選択して、宛先ごとにトラフィックを一致させるシーケンスを作成します。
11. [Sequence Rule] をクリックして、シーケンスの新しいルールを作成します。

12. [Match] オプションを選択した状態で、[Destination Region] をクリックして、このオプションをシーケンスルールの一致条件領域に追加します。
13. [Match Conditions] 領域で、[Destination Region] フィールドをクリックし、次のいずれかを選択します。
    - [Primary]：宛先デバイスが送信元と同じプライマリリージョン（アクセスリージョンとも呼ばれる）にある場合、トラフィックに一致します。このトラフィックは、アクセスリージョンの双方向フォワーディング検出（BFD）を使用して宛先に到達します。
    - [Secondary]：宛先デバイスが送信元と同じプライマリリージョンにないが、送信元と同じセカンダリリージョンにある場合、トラフィックに一致します。このトラフィックは、セカンダリリージョンで説明されているように、ダイレクトトンネルを使用して宛先に到達できます。
    - [Other]：宛先デバイスが送信元と同じプライマリリージョンまたはセカンダリリージョンにない場合、トラフィックに一致します。このトラフィックには、送信元から宛先へのマルチホップパスが必要です。
14. このセクションで前述した「Configure Centralized Policies Using Cisco vManage」の説明に従って、ポリシーの設定を続行します。

Cisco vManage を使用した優先カラーグループリストのパス設定の構成

最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco vManage リリース 20.9.1

アプリケーション認識型ルーティング（AAR）ポリシーの設定の詳細については、『Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x』の「Configure Centralized Policies Using Cisco vManage」を参照してください。ここでの情報は、優先カラーグループの一部としてパス設定を構成する方法のみを扱っています。

1. Cisco vManage メニューから、**[Configuration]** > **[Policies]** を選択し、[Centralized Policy] を選択します。
2. [Add Policy] をクリックします。
3. デフォルトで選択されている [Application List] をクリックします。
4. [Preferred Color Group] をクリックします。
5. [New Preferred Color Group] をクリックします。
6. 次のフィールドを設定します。

フィールド	説明
Preferred Color Group Name	カラーグループの名前を入力します。

フィールド	説明
Primary Colors： Color Preference	フィールドをクリックして、プライマリ設定として 1 つ以上のカラーを選択します。
Primary Colors： Path Preference	ドロップダウンリストをクリックし、プライマリ設定として次のいずれかを選択します。 • [Direct Path]：送信先デバイスと宛先デバイス間のダイレクトパスのみを使用します。 （注） 非マルチリージョン ファブリック ネットワークでは、このオプションを使用しないでください。 • [Multi Hop Path]：マルチリージョン ファブリック ネットワークでは、ダイレクトパスが使用可能な場合でも、コアリージョンを含むマルチホップパスを送信先デバイスと宛先デバイス間で使用します。 • [All Paths]：送信先デバイスと宛先デバイス間の任意のパスを使用します。 （注） このオプションは、パス設定をまったく構成しないことと同じです。ポリシーをマルチリージョンファブリック ネットワーク以外に適用する場合は、このオプションを使用します。
Secondary Colors： Color Preference Path Preference	[Primary Colors] オプションと同じ方法を使用して、セカンダリ設定を構成します。
Tertiary Colors： Color Preference Path Preference	[Primary Colors] オプションと同じ方法を使用して、ターシャリ設定を構成します。

ポリシーの優先カラーグループの使用

最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco vManage リリース 20.9.1

ポリシーの設定の詳細については、『Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x』の「Configure Centralized Policies Using Cisco vManage」を参照してください。ここでの情報は、パス設定を組み込んだ[Preferred Color Group]アクションの使用方法のみを扱っています。

アプリケーション認識型ポリシーまたはトラフィックデータポリシーには、次の手順を使用します。

1. Cisco vManage メニューから、**[Configuration]** > **[Policies]** を選択します。
2. [Add Policy] をクリックします。
3. デフォルトで選択されている [Centralized Policy] を選択します。
4. [Add Policy] をクリックします。
5. 必要に応じて、リストタイプをクリックしてリストを定義できます。
6. [Next] をクリックします。
7. 必要に応じて、トポロジを追加します。
8. **[Next]** をクリックします。
9. 次のいずれかを実行します:
   - AAR ポリシーの場合、デフォルトで選択されている [Application Aware Routing] をクリックします。
   - トラフィックデータポリシーの場合、[Traffic Data] をクリックします。
10. [Add Policy] をクリックし、[Create New] を選択します。
11. 次のいずれかを実行します。
    - AAR ポリシーの場合、[Sequence Type] をクリックして、宛先ごとにトラフィックを一致させるシーケンスを作成します。
    - トラフィックデータポリシーの場合、[Sequence Type] をクリックし、[Custom] を選択して、宛先ごとにトラフィックを一致させるシーケンスを作成します。
12. [Sequence Rule] をクリックして、シーケンスの新しいルールを作成します。
13. [Actions] をクリックします。
14. AAR ポリシーの場合は、次の手順を実行します。
    1. [SLA Class List] をクリックします。
    2. [Preferred Color Group] フィールドをクリックして、優先カラーグループを選択します。

15. トラフィック制御ポリシーの場合は、次の手順を実行します。
    1. [承認（Accept）] をクリックします。
    2. [Preferred Color Group] をクリックします。
    3. [Preferred Color Group] フィールドをクリックして、優先カラーグループを選択します。

CLI を使用した マルチリージョン ファブリック ポリシーの設定

CLI を使用したパスタイプに応じたルートの一致

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

はじめる前に

この手順は、マルチリージョン ファブリック アーキテクチャに適用されます。

パスタイプによる一致の背景情報については、パスのタイプ、リージョン、またはロールによるルートの一致 （53 ページ）を参照してください。

制御ポリシーでの一致パラメータの使用に関する一般的な情報については、「Match Parameters - Control Policy」を参照してください。

パスタイプに応じたルートの一致

制御ポリシーで、**path-type** を使用してパスタイプに応じてルートに一致します。

```
match route path-type {hierarchical-path | direct-path | transport-gateway-path}
```

例

この例には、次のことを行う 2 つの制御ポリシーシーケンスが含まれています。

- シーケンス 1 は、あるエッジルータから別のエッジルータへの階層パスを使用するルートに一致します。これは、**accept** のポリシーアクション、ルートの優先値、および 100 の omp タグを構成します。
- シーケンス 2 は、あるエッジルータから別のエッジルータへのダイレクトパスを使用するルートに一致します。これは、**accept** のポリシーアクションと 200 の omp タグを構成します。

```
policy
 control-policy control_policy_A
   sequence 1
```

```
    match route
     path-type hierarchical-path
    !
    action accept
     set
      preference 200
      omp-tag 100
     !
    !
   !
sequence 2
    match route
     path-type direct-path
    !
    action accept
     set
      omp-tag 200
    !
   !
  !
  default-action reject
 !
!
```

CLI を使用したリージョンとロールに応じたルートの一致

サポートされている最小リリース：Cisco IOS XE リリース 17.8.1a、Cisco vManage リリース 20.8.1

はじめる前に

この手順は、マルチリージョン ファブリック アーキテクチャに適用されます。

パスタイプによる一致の背景情報については、パスのタイプ、リージョン、またはロールによるルートの一致 （53 ページ）を参照してください。

制御ポリシーでの一致パラメータの使用に関する一般的な情報については、「Match Parameters - Control Policy」を参照してください。

リージョンとロールに応じたルートの一致

制御ポリシーで、**region** を使用して特定のリージョンにあるデバイスによって発信されたルートを一致させます。必要に応じて、発信元デバイスのロールに応じて一致する **role** キーワードを含めることができます。

match route region {*region-id* | *region-list*} [**role** {**border-router** | **edge-router**}]

例

次の **match** ステートメントは、リージョン 1 のエッジルータから発信されるルートに一致します。

```
match route region 1 role edge-router
```

CLI を使用して Traffic-To に一致するデータポリシーまたはアプリケーション ルート ポリシーを設定

はじめる前に

この構成には、特定の マルチリージョン ファブリック 機能である **match traffic-to** 条件と、マルチリージョン ファブリック に特定ではないが マルチリージョン ファブリック のリージョン オプションがある **apply-to** ステップが含まれます。

Traffic-To に一致するデータポリシーまたはアプリケーション ルート ポリシーを設定

1. Cisco vSmart コントローラ で、コンフィギュレーション モードを開始します。

   ```
   vSmart# config terminal
   ```

2. データポリシーまたはアプリケーション ルート ポリシーを設定するときに、一致条件を設定します。

   ```
   vSmart(config)# vSmart(config)#policy {app-route-policy | data-policy } policy-name
    vpn-list vpn-list-name sequence sequence-number match traffic-to {access | core |
   service}
   ```

3. 一致モードを終了します。

   ```
   vSmart(config-match)# top
   ```

4. ポリシーを適用し、オプションで マルチリージョン ファブリック リージョンまたはリージョンリストを指定し、border-router のロールを指定します。

（注） **role** キーワードはエッジルータを指定することもできますが、**match traffic-to** は境界ルータに適用されるポリシーにのみ使用します。

```
vSmart(config)# apply-policy {region region-id | region-list | site-list} role
border-router data-policy policy-name [from-tunnel | from-service | all]
```

例

この例では、アクセスリージョンへのトラフィックフローに一致するデータポリシーを作成し、そのポリシーをリージョン 1 の境界ルータに適用します。**apply-policy** コマンドの **from-tunnel** キーワードは、ポリシーのターゲットを絞り込み、次のいずれかの方法でトラフィックフローに対処します。

- アクセスリージョンからアクセスリージョンへ
- コアリージョンからアクセスリージョンへ

```
vSmart# config terminal
vSmart(config)# policy data-policy data_policy_a vpn-list vpn1 sequence 1 match traffic-to
 access
vSmart(config-match)# top
```

```
vSmart(config)# apply-policy region 1 role border-router data-policy data_policy_a
from-tunnel
```

CLI を使用してリージョンとロールに一致する制御ポリシーを設定

はじめる前に

この手順では、リージョンに応じて、およびオプションでロール（境界ルータまたはエッジルータ）に応じて、ルートまたはTLOCを一致させる制御ポリシーを構成します。ロールを指定しない場合、ポリシーは両方のロールのルータに適用されます。

たとえば、リージョン 1 のエッジルータのすべての TLOC に一致するポリシーを作成できます。

region および **role** 一致条件は マルチリージョン ファブリック アーキテクチャに固有ですが、ポリシーにはマルチリージョンファブリックに関係のない一致条件を含めることができます。

リージョンとロールに一致する制御ポリシーを設定

1. Cisco vSmart コントローラ で、コンフィギュレーション モードを開始します。

   ```
   vSmart# config terminal
   ```

2. 制御ポリシーで使用するリージョンリストを定義します。

   1. `vSmart(config)# policy lists region-list region-list-name`
   2. リージョンリストに追加するリージョンごとに、次のコマンドを繰り返します。

      ```
      vSmart(config-region-list-region-list-name)# region-id region-id
      ```

   3. リージョン リスト コンフィギュレーション モードを終了します。

      ```
      vSmart(config-region-list-region-list-name)# top
      ```

   4. リージョンリストが正しく構成されていることを確認するには、構成を表示します。

      ```
      vSmart(config)# show configuration
      ```

3. 制御ポリシーを設定するときは、特定のリージョン、およびオプションでデバイスロールに一致させます。

   ```
   vSmart(config)# policy control-policy policy-name sequence sequence-number match
   {route | tloc} {region region-id | region-list region-list-name} [role {border-router
    | edge-router}]
   ```

例

この例では、リージョン 1、2、および 3 を含む region_a というリージョンリストを作成します。

```
vSmart# config terminal
vSmart(config)# policy lists region-list region_list_a
vSmart(config-region-list-region_list_a)# region-id 1
vSmart(config-region-list-region_list_a)# region-id 2
vSmart(config-region-list-region_list_a)# region-id 3
```

```
vSmart(config-region-list-region_list_a)# top
vSmart(config)# show configuration
policy
 lists
  region-list region_list_a
   region-id 1
   region-id 2
   region-id 3
  !
 !
!
vSmart(config)# policy control-policy policy_a sequence 1 match route region-list
region_list _a role border-router
```

CLI を使用した宛先リージョンに応じたトラフィックの一致

最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco vManage リリース 20.9.1

アプリケーション ルート ポリシーまたはデータポリシー内で、**destination-region** キーワードを使用して、宛先リージョンに応じてトラフィックを一致させます。

1. アプリケーション ルート ポリシーまたはデータポリシーを作成します。

   app-route-policy *policy-name*

   または

   data-policy *policy-name*

2. VPN または VPN リストを指定します。

   vpn *vpn-id*

   または

   vpn-list *vpn-list-name*

3. シーケンスを作成します。

   sequence *sequence-number*

4. シーケンス内で一致条件を作成します。

   match

5. 一致条件の詳細を入力します。

   dscp *dscp-id*
   destination-region {**primary** | **secondary** | **other**}

次に、3 つの異なる **destination-region** タイプのそれぞれのシーケンスを含むサンプル アプリケーション ルート ポリシーを示します：**primary**、**secondary**、**other**。

```
app-route-policy SAMPLE_HSDWAN_AAR
 vpn-list ONE
  sequence 10
   match
    dscp 46
    destination-region primary
   !
```

```
   action
    sla VOICE_SLA strict preferred-color-group GROUP2_COLORS
   !
  !
  sequence 20
   match
    dscp 46
    destination-region secondary
   !
   action
    sla VOICE_SLA preferred-color-group GROUP1_COLORS
   !
  !
  sequence 30
   match
    dscp 46
    destination-region other
   !
   action
    sla VOICE_SLA preferred-color-group GROUP1_COLORS
   !
  !
 !
!
```

次に、3 つの異なる **destination-region** タイプのそれぞれのシーケンスを含むサンプルデータポリシーを示します：**primary**、**secondary**、**other**。

```
data-policy SAMPLE_HSDWAN_DATA
 vpn-list ONE
  sequence 10
   match
    dscp 46
    destination-region primary
   !
   action
    set
     preferred-color-group GROUP2_COLORS
   !
  !
  sequence 20
   match
    dscp 46
    destination-region secondary
   !
   action
    set
     preferred-color-group GROUP1_COLORS
   !
  !
  sequence 30
   match
    dscp 46
    destination-region other
   !
   action
    set
     preferred-color-group GROUP1_COLORS
   !
  !
 !
!
```

CLI を使用した優先カラーグループリストのパス設定の構成

最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco vManage リリース 20.9.1

1. 新しいポリシーリストを設定します。

   policy
   lists

2. 優先カラーグループリストを作成します。

   preferred-color-group *group-name*

3. プライマリ設定を構成します。

（注） プライマリ、セカンダリ、ターシャリの設定があります。

   primary-preference

4. プライマリ設定のカラー設定を構成します。

（注） カラーオプションの完全なリストについては、Cisco SD-WAN のドキュメントを参照してください。オプションは、デフォルト、3g、biz-internet、blue、bronze、custom1、custom2、custom3、gold、green、lte、metro-ethernet、mpls、private1、private2、private3、private4、private5、private6、public-internet、red、および silver を含みます。

   color-preference *color-option*

5. プライマリ設定のパス設定を構成します。

   path-preference {**direct-path** | **multi-hop-path** | **all-paths**}

6. プライマリ設定の構成を終了します。

   exit

7. セカンダリ設定とターシャリ設定について、手順 3 から 6 を繰り返します。

例：優先カラーグループのパス設定を構成

次の優先カラーグループ構成では、GROUP1_COLORS カラーグループに [direct-tunnel] を指定するプライマリ設定があります。セカンダリ設定は、[multi-hop-path] を指定します。ポリシーで GROUP1_COLORS を使用すると、ポリシーはマルチホップパスよりもダイレクトトンネルパスを優先します。

```
policy
 lists
  preferred-color-group GROUP1_COLORS
   primary-preference
    color-preference internet
    path-preference direct-tunnel
```

```
   !
   secondary-preference
    color-preference mpls
    path-preference multi-hop-path
   !
   tertiary-preference
    color-preference lte
   !
  !
  preferred-color-group GROUP2_COLORS
   priority-one
    color-preference mpls
   !
   priority-two
    color-preference internet
   !
  !
  preferred-color-group GROUP3_COLORS
   priority-one
    color-preference mpls internet lte
   !
    !
```

例：AAR ポリシーでのパス設定の使用

次の AAR ポリシーは、前述の優先カラーグループ構成を使用します。3 つのシーケンスのそれぞれについて、アクションは GROUP1_COLORS、GROUP2_COLORS、または GROUP3_COLORS などの優先カラーグループを指定します。たとえば、シーケンス 20 は GROUP1_COLORS カラーグループを適用します。これには、ダイレクトトンネルのプライマリ設定とマルチホップパスのセカンダリ設定が含まれます。

```
app-route-policy SAMPLE_HSDWAN_AAR
 vpn-list ONE
  sequence 10
   match
    dscp 46
   !
   action
    sla VOICE_SLA strict preferred-color-group GROUP2_COLORS
   !
  !
  sequence 20
   match
    dscp 34
   !
   action
    sla VOICE_SLA preferred-color-group GROUP1_COLORS
   !
  !
  sequence 30
   match
    dscp 28
   !
   action
    sla VOICE_SLA preferred-color-group GROUP3_COLORS
   !
  !
 !
!
```

例：トラフィックデータポリシーでのパス設定の使用

次のデータポリシーは、このセクションで前述したのと同じ優先カラーグループ構成を使用します。上記のアプリケーション ルート ポリシーと同様に、このデータポリシーのシーケンス 20は、ダイレクトトンネルのプライマリ設定とマルチホップパスのセカンダリ設定が含まれる GROUP1_COLORS カラーグループを適用します。

```
data-policy SAMPLE_HSDWAN_DATA
 vpn-list ONE
  sequence 10
   match
    dscp 46
   !
   action
    set
     preferred-color-group GROUP2_COLORS
   !
  !
  sequence 20
   match
    dscp 34
   !
   action
    set
     preferred-color-group GROUP1_COLORS
   !
  !
  sequence 30
   match
    dscp 28
   !
   action
    set
     preferred-color-group GROUP3_COLORS
   !
  !
 !
!
```

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。