# マルチリージョン ファブリック ポリシー

**表 *1*: 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<br>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<br>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<br>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<br>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<br>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 *2 : 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<br>および<br>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<br>および<br>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 *3 : 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**<br>（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<br>および<br>コアリージョンからアクセスリージョンへ |
| | **from-service**<br>（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**<br>（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<br>および<br>コアリージョンからアクセスリージョンへ<br>および<br>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**<br>（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<br>および<br>アクセスリージョンからコアリージョンへ |
| | **from-service**<br>（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**<br>（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<br>および<br>アクセスリージョンからコアリージョンへ<br>および<br>サービス VPN からコアリージョンへ |
| **match traffic-to service** | **from-tunnel**<br>（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<br>および<br>アクセスリージョンからサービス VPN へ |
| | **from-service**<br>（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**<br>（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<br>および<br>アクセスリージョンからサービス VPN へ<br>および<br>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。

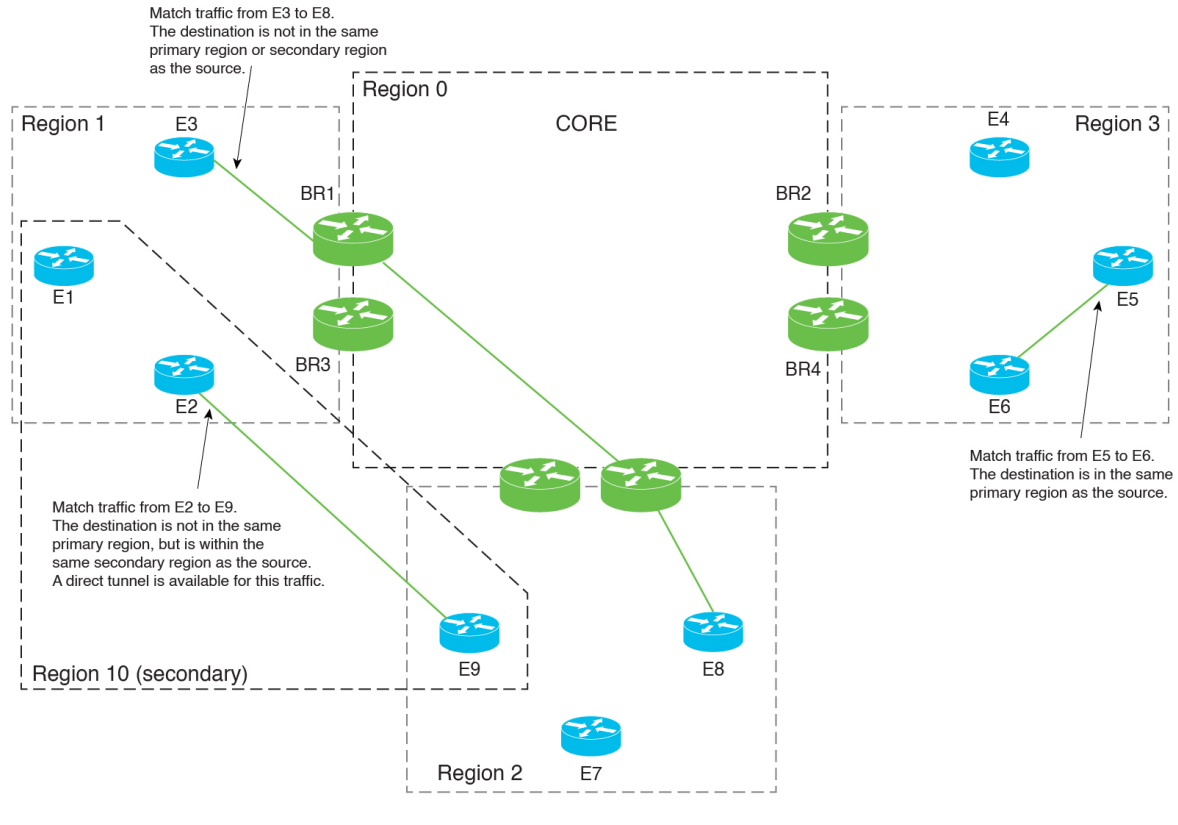
# 宛先リージョンに応じたトラフィックの一致に関する情報

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 *1*: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。

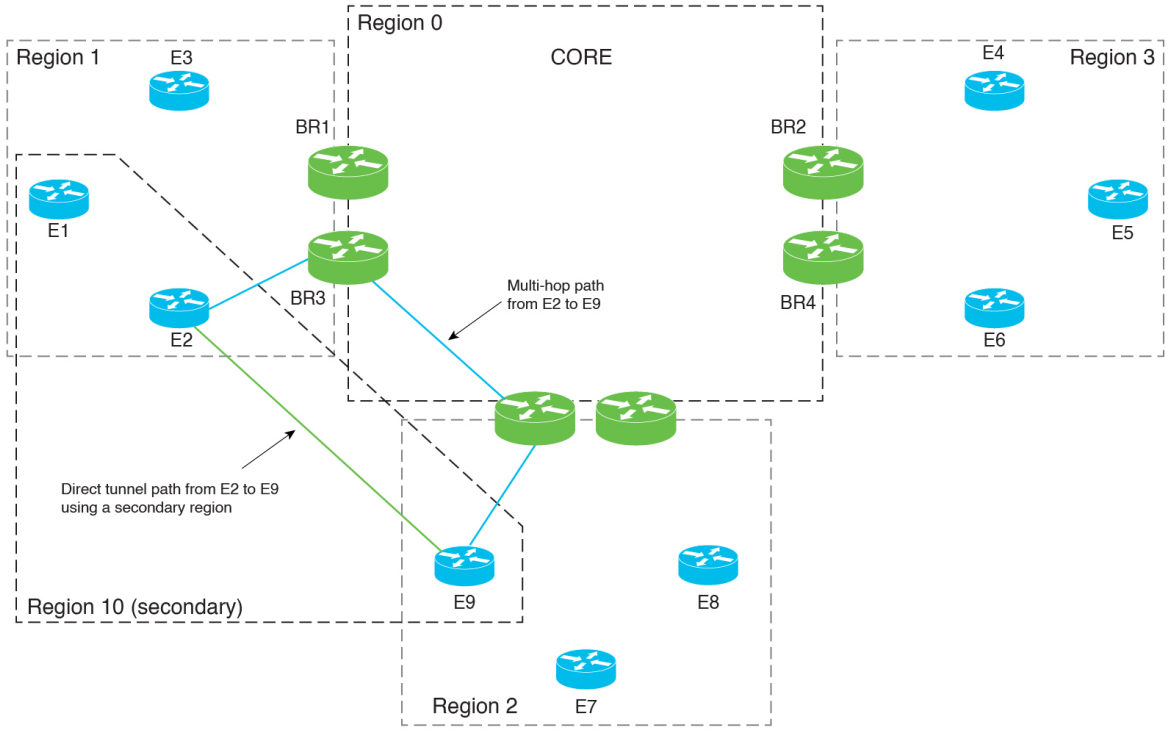
## パス設定の構成のユースケース

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 *2:* 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：<br>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：<br>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。<br>• [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。<br>（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。<br>• [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。<br>• [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。<br>（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：<br>Color Preference<br>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：<br>Color Preference<br>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。