



マルチリージョン ファブリックへの移行

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 \(1 ページ\)](#)
- [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 \(2 ページ\)](#)
- [マルチリージョンファブリックへの移行の前提条件 \(3 ページ\)](#)
- [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 \(3 ページ\)](#)
- [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 \(14 ページ\)](#)
- [CLI を使用した移行モードの有効化または無効化 \(16 ページ\)](#)
- [マルチリージョンファブリックへの移行の検証手順 \(17 ページ\)](#)

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っても適しています。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 \(3 ページ\)](#) 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

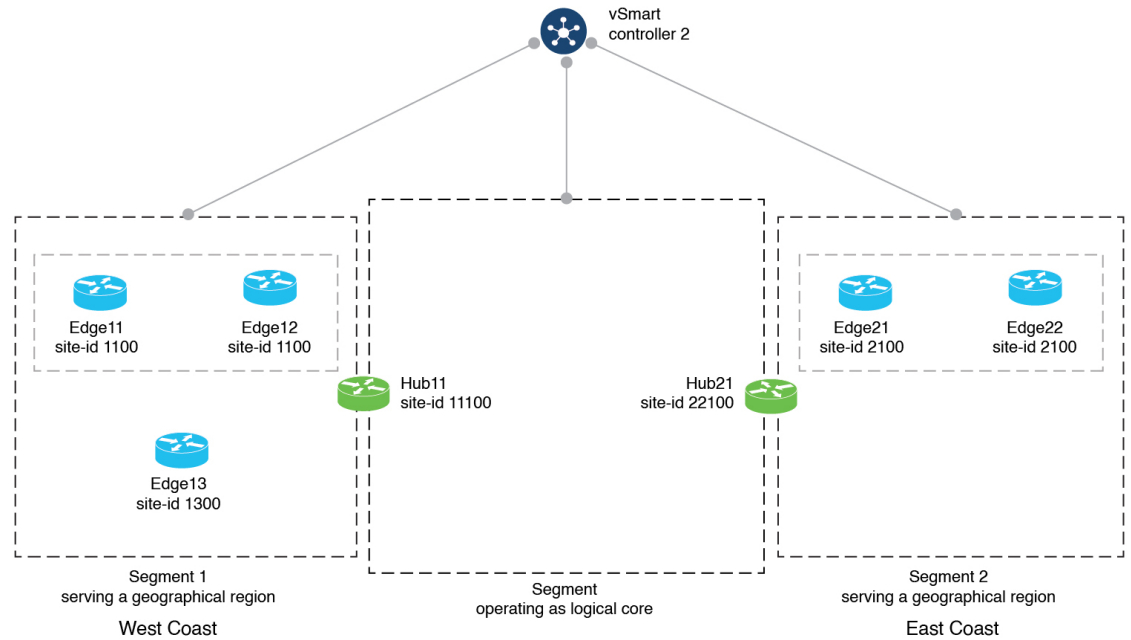
次の例は、マルチリージョン ファブリック アーキテクチャへの移行を計画および実行するための手順についての洞察を提供します。単純化するために、この例には、組織のネットワーク内に少数のルータのみが含まれていて、移行前には単一の Cisco vSmart コントローラ が使用されています。

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 1: 移行前のネットワークアーキテクチャ



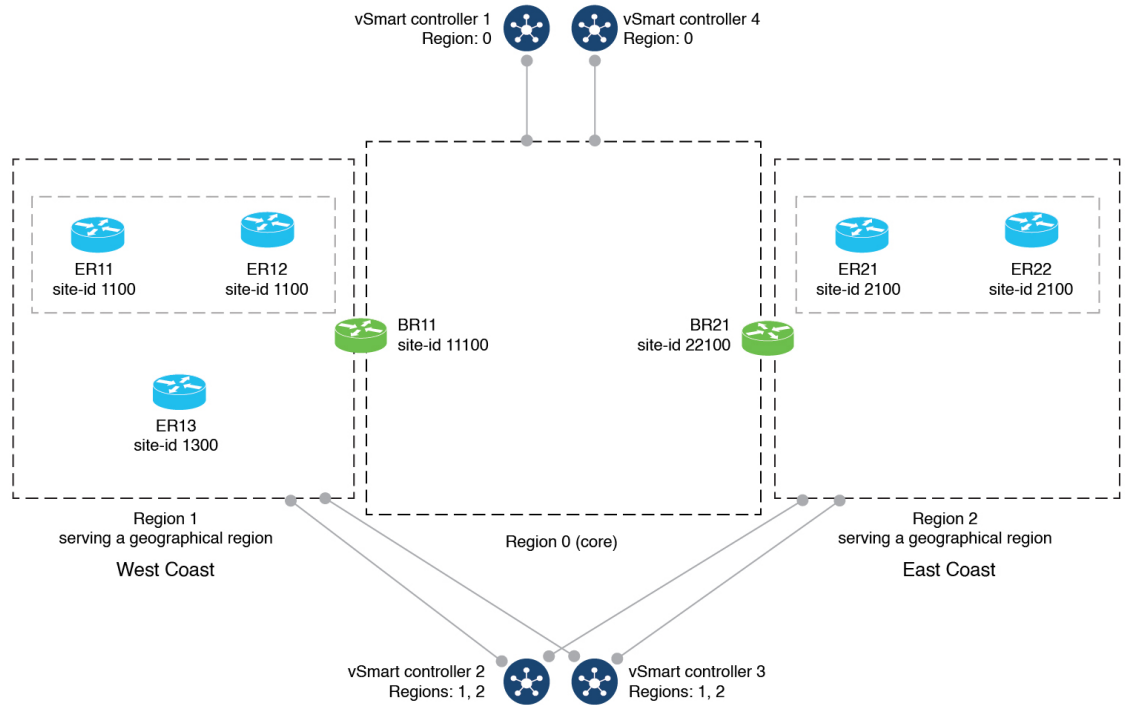
このネットワークでは、マルチリージョンファブリックへの移行前に、このセクションで後ほど詳しく説明する一元化された制御ポリシーにより、ルータがネットワークセグメント1と2にクラスタ化され、セグメント1のハブルルータとセグメント2のハブルルータが提供されます。ポリシーは次のことを行います。

- 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（14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 2: 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 2: 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。	<pre>policy lists site-list SEGMENT1 site-id 1100 site-id 1300 !</pre>
	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。	<pre>policy lists site-list SEGMENT1_HUB1 site-id 1100 site-id 1300 site-id 11100 !</pre>
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。	<pre>policy lists site-list SEGMENT2 site-id 2100 !</pre>
	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。	<pre>policy lists site-list SEGMENT2_HUB2 site-id 2100 site-id 22100 !</pre>
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。	<p>次のリストを定義します。</p> <ul style="list-style-type: none"> 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 	<pre>policy lists site-list HUB1_HUB2_SEGMENT2 site-id 11100 site-id 2100 site-id 22100 !</pre>

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。 <ul style="list-style-type: none"> 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 	<pre> policy lists site-list HUB1_HUB2_SEGMENT1 site-id 1100 site-id 11100 site-id 1300 site-id 22100 ! </pre>
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。 <ul style="list-style-type: none"> 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 	<pre> policy lists site-list SEGMENT1_HUB2 site-id 1100 site-id 1300 site-id 22100 ! </pre>
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。 <ul style="list-style-type: none"> 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 	<pre> policy lists site-list HUB1_SEGMENT2 site-id 11100 site-id 2100 ! </pre>

表 3: 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。)	<ul style="list-style-type: none"> 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。 	<pre> policy lists tloc-list HUB1_CORE_TLOC tloc 172.16.11.10 color green encaps ipsec ! tloc-list HUB2_CORE_TLOC tloc 172.17.13.10 color green encaps ipsec ! </pre>

ポリシー構成の目的の簡単な説明	詳細な説明	例
<p>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。</p> <p>(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。)</p>	<ul style="list-style-type: none"> • 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。 	<pre> 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 ! </pre>

表 4: 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
<p>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。</p>	<p>CP1 という制御ポリシーを作成して、次のことを行います。</p> <ul style="list-style-type: none"> 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。 	<pre>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 !</pre>
<p>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。</p>		<pre>apply-policy site-list SEGMENT1 control-policy CP1 out</pre>

ポリシー構成の目的の簡単な説明	詳細な説明	例
<p>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。</p>	<p>CP4 という制御ポリシーを作成して、次のことを行います。</p> <ul style="list-style-type: none"> 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。 	<pre>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 ! !</pre>
<p>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。</p>		<pre>apply-policy site-list SEGMENT2 control-policy CP4 out</pre>

ポリシー構成の目的の簡単な説明	詳細な説明	例
<p>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。</p>	<p>CP2 という制御ポリシーを作成して、次のことを行います。</p> <ul style="list-style-type: none"> 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。 	<pre>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 !</pre>
<p>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。</p>		<pre>apply-policy site-list HUB1 control-policy CP2 out !</pre>

ポリシー構成の目的の簡単な説明	詳細な説明	例
<p>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。</p>	<p>CP3 という制御ポリシーを作成して、次のことを行います。</p> <ul style="list-style-type: none"> • 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。 	<pre>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 !</pre>
<p>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。</p>		<pre>apply-policy site-list HUB2 control-policy CP3 out !</pre>

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勧めます。

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](#)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](#) 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](#) 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 ピア表示については、[Cisco vManage を使用した OMP ピアの表示 \(17 ページ\)](#) 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](#) 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 \(17 ページ\)](#) 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				
TENANT	VPN	GROUP	FROM PEER	ID	LABEL	STATUS	TYPE	TLOC IP	COLOR	ENCAP
PREFERENCE		PREFIX 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						

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

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

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。