ACI ファブリックの Nexus Dashboard Orchestrator テナントとテナント ポリシー テンプレート、リリース 4.3.x

目次

テナントの概要

テナントは、アプリケーションポリシーの論理コンテナで、管理者はドメインベースのアクセスコントロールを実行できます。テナントはポリシーの観点から分離の単位を表しますが、プライベート ネットワークは表しません。テナントは、サービス プロバイダーの環境ではお客様を、企業の環境では組織またはドメインを、または単にポリシーの便利なグループ化を表すことができます。

- [common] : ACI ファブリックの他のテナントに「共通」のサービスを提供するための特別なテナント。共通テナントの基本原則はグローバルな再利用です。一般的なサービスには、共有 L3Out、DNS、DHCP、Active Directory、共有プライベート ネットワークまたはブリッジドメインなどがあります。
- [dcnm-default-tn] : Cisco NDFC ファブリックの構成を提供する特別なテナント。
- [infra] : トンネルやポリシー展開など、ファブリック内部の通信に使用されるインフラストラクチャ テナント。これには、スイッチ間の切り替えと APIC 通信への切り替えが含まれます。[infra] テナントは、ユーザー空間（テナント）には公開されず、独自のプライベート ネットワーク空間とブリッジドメインを備えています。ファブリックの検出、イメージ管理、ファブリック機能用の DHCP は、すべてこのテナント内で処理されます。

  Nexus Dashboard Orchestrator を使用して Cisco NDFC ファブリックを管理する場合は、常にデフォルトの [dcnm-default-tn] テナントを使用します。

Nexus Dashboard Orchestrator は APIC の管理テナントをテナントしたり、 NDO で mgmt と 呼ばれる新しいテナントを作成したりすることは
できません。
テナントを管理するには、[パワー ユーザー（Power User）] または [サイトとテナント マネージャ（Site and Tenant Manager）] の読み取り/書き込みロールの
いずれかが必要です。3 つのデフォルト テナントが事前に設定されています。

テナント ポリシー テンプレート

リリース 4.0(1) では、テナント ポリシー テンプレートが追加されています。これにより、次のテナント全体のポリシーを構成できます。

- マルチキャストのルート ポリシー
- ルート制御のルート マップ ポリシー
- カスタム QoS ポリシー
- DHCP リレー ポリシー
- DHCP オプション ポリシー
- IGMP インターフェイス ポリシー
- IGMP スヌーピング ポリシー
- MLD スヌーピング ポリシー

詳細については、「テナント ポリシー テンプレートの作成」を参照してください。

新しいテナントの作成

始める前に：

テナントの作成および管理には、[パワー ユーザー（Power User）] または [サイト マネージャ（Site Manager）] の読み取り/書き込みロールを持つユーザーが必要です。

このセクションでは、Cisco Nexus Dashboard Orchestrator GUI を使用して新しいテナントを追加する方法について説明します。ファブリックから既存のテナントを一つ以上インポートしたい場合、「既存のテナントのインポート」に記されているステップに従います。

1. Cisco Nexus Dashboard にログインし、Cisco Nexus Dashboard Orchestrator サービスを開きます。
2. 新しいテナントを作成。
   a. 左のナビゲーション ペインから、**[操作（Operate）] > [テナント（Tenant）]** を選択します。
   b. メイン ペインの右上にある **[テナントの作成（Create Tenant）]** をクリックします。**[テナントの作成（Create Tenant）]** 画面が開きます。
3. テナントの詳細を入力します。
   a. **[表示名（Display Name）]** とオプションの **[説明（Description）]** を入力します。

      Orchestrator の GUI 全体で、テナントが表示されるたびに、テナントの **[表示名（Display Name）]** が使用されます。ただし、APIC でのオブジェクトの命名要件により、無効な文字は削除され、その結果として得られた内部名が、サイトにテナントをプッシュするときに使用されます。テナントの作成時に使用される **[内部名（Internal Name）]** は、**[表示名（Display Name）]** テキストボックスの下に表示されます。

      テナントの **[表示名（Display Name）]** はいつでも変更できますが、テナントの作成後に **[内部名（Internal Name）]** を変更することはできません。

   b. **[関連付けられたサイト（Associated Sites）]** セクションで、このテナントに関連付けるすべてのサイトをオンにします。選択したサイトのみが、このテナントを使用している任意のテンプレートで使用可能になります。
   c. （オプション）選択したサイトごとに、その名前の横にある **[編集（Edit）]** ボタンをクリックし、1 つ以上のセキュリティ ドメインを選択します。

      制限付きセキュリティ ドメインを使用すると、テナント A などのファブリック管理者は、両方のグループのユーザーに同じ権限が割り当てられている場合、あるユーザー グループがテナント B などの別のセキュリティ ドメインのユーザー グループによって作成されたオブジェクトを表示または変更できないようにすることができます。たとえば、テナント A の制限付きセキュリティ ドメインのテナント管理者は、テナント B のセキュリティ ドメインで構成されたポリシー、プロファイル、またはユーザーを表示できません。テナント B のセキュリティドメインも制限されていない限り、テナント B は、テナント A で構成されたポリシー、プロファイル、またはユーザーを表示できます。

      ユーザーは、ユーザーが適切な権限を持っているシステムで作成された設定に対して、常に読み取り専用の可視性を持ちます。制限付き セキュリティ ドメインのユーザーは、そのユーザーが不注意でその他のテナントの物理環

境に影響を与えることなく
幅広いレベルの権限を与えることが。
できます。

セキュリティ ドメインは APIC GUI を使用して作成し、アクセスをコントロールするために、さまざまな APIC ポリシーに割り当てることができます。詳細については、*Cisco APIC 基本設定ガイド*を参照してください。

d. **[**関連付けられたユーザー（**Associated Users**）**]** セクションで、テナントへのアクセスが許可されている Cisco Nexus Dashboard Orchestratorユーザーを選択します。

テンプレートを作成するときに選択したユーザーのみが、このテナントを使用できます。

4. **[**保存（**Save**）**]** をクリックして、テナントの追加を終了します。

既存テナントのインポート

始める前に：

テナントの作成および管理には、[パワー ユーザー（Power User）] または [サイト マネージャ（Site Manager）] の読み取り/書き込みロールを持つユーザーが必要です。

このセクションでは、1 つ以上の既存のテナントをインポートする方法について説明します。Cisco Nexus Dashboard Orchestrator を使用して新しいテナントを作成する場合は、代わりに「テナントの 新規作成」で説明されている手順に従ってください。

1. Cisco Nexus Dashboard にログインし、Cisco Nexus Dashboard Orchestrator サービスを開きます。
2. 左のナビゲーションメニューで、**[操作（Operate）] > [サイト（Sites）]** をクリックします。
3. テナントのインポート元のサイトを見つけ、3 点リーダーをクリックしてアクション（**[...]**）メニューを選択し、**[テナントのインポート（Import Tenants）]** を選択します。

   一度に 1 つのサイトからテナントをインポートできます。

4. **[テナントのインポート（Import Tenants）]** ダイアログ内で、インポートする一つ以上のテナントを選択して **[OK]** をクリックします。

   選択したテナントが Cisco Nexus Dashboard Orchestrator にインポートされ、**[操作（Operate）] > [テナント（Tenants）]** ページに表示されます。

5. これらの手順を繰り返して、他のサイトからテナントをインポートします。

テナント ポリシー テンプレートを作成

このセクションでは、1 つ以上のテナント ポリシー テンプレートを作成する方法について説明します。テナント ポリシー テンプレートを使用すると、次のポリシーを作成および構成できます。

- マルチキャストのルート マップ ポリシー
- ルート制御のルート マップ ポリシー
- カスタム QoS ポリシー
- DHCP リレー ポリシー
- DHCP オプション ポリシー
- IGMP インターフェイス ポリシー
- MLD スヌーピング ポリシー
- L3Out ノード ルーティング ポリシー
- L3Out インターフェイス ルーティング ポリシー
- BGP ピア プレフィックス ポリシー
- IP SLA モニターリング ポリシー
- IP SLA トラック リスト

1. Cisco Nexus Dashboard にログインし、Cisco Nexus Dashboard Orchestrator サービスを開きます。
2. 新しいテナント ポリシー テンプレートを作成します。
    a. 左のナビゲーション ペインから、**[**構成（**Configure**）**] > [**テナント テンプレート（**Tenant Templates**）**] > [**テナント ポリシー（**Tenant Policies**）**]** の順に選択します。
    b. **[**テナント ポリシー テンプレート（**Tenant Policy Template**）**]** ページ内で **[**テナント ポリシー テンプレートの作成（**Create Tenant Policy Template**）**]** をクリックします。
    c. **[**テナント ポリシー（**Tenant Policies**）**]** ページの右のプロパティ サイトバーにテンプレートの **[**名前（**Name**）**]** を入力します。
    d. **[**テナントの選択（**Select a Tenant**）**]** ドロップダウンから、このテンプレートに関連付けるテナントを選択します。

        次の手順で説明するようにテンプレートで作成したすべてのポリシーは、テンプレートを特定のサイトにプッシュすると、展開された選択したテナントに関連付けられます。

        デフォルトでは、新しいテンプレートは空であるため、次のステップに従って 1 つ以上のテナント ポリシーを追加する必要があります。テンプレートで使用可能なすべてのポリシーを作成する必要はありません。このテンプレートとともに展開する各タイプのポリシーを 1 つ以上定義してください。特定のポリシーを作成したくない場合は、説明されている手順をスキップしてください。

3. テンプレートを 1 つ以上のサイトに割り当てます。

    サイトにテナント ポリシー テンプレートを割り当てるプロセスは、サイトにアプリケーション テンプレートを割り当てる方法と同じです。

    a. **[**テンプレート プロパティ（**Template Properties**）**]** 表示内で **[**アクション（**Actions**）**]** をクリックして **[**サイトの関連付け（**Sites Association**）**]** を選択

します。**[<template-name>** にサイトの関連付け（**Associate Sites to <template-name>**）**]** ウィンドウが開きます。

b. **[**サイトの関連付け（**Associate Sites**）**]** ウィンドウで、テンプレートを展開するサイトの横のチェックボックスをオンにします。

テナント ポリシー テンプレートは、オンプレミス ACI サイトにのみサポートされることにご注意ください。そして、割り当て可能です。

c. **[OK]** をクリックして保存します。

4. マルチキャストのルート マップ ポリシーを作成します。

このポリシーは、包括的なレイヤ 3 マルチキャスト ユース ケースの一部です。このセクションにある情報を参照資料として使用することができます。しかし資料の「*機能と使用例*」の項の「レイヤ 3 マルチキャスト」すべての手順のセットに従うことをおすすめします。

a. **[+**オブジェクトの作成（**+Create Object**）**]** ドロップダウンから、**[**マルチキャストのルート マップ ポリシー（**Route Map Policy for Multicast**）**]** を選択します。

b. 右のプロパティのサイドバーでは、ポリシーの **[**名前（**Name**）**]** を指定します。

c. （オプション）**[**説明を追加（**Add Description**）**]** をクリックして、このポリシーの説明を入力します。

d. **[+**マルチキャスト エントリのルート マップを追加（**+Add Route Map for Multicast Entries**）**]** をクリックし、ルート マップ情報を指定します。

ルート マップごとに、1 つ以上のルート マップ エントリを作成する必要があります。次の情報によると各コンテキストは、1 つ以上の一致基準に基づいてアクションを定義するルールです：

- **[**順序（**Order**）**]**：順序は、ルールを評価する順序を決定するために用いられます。
- **[**グループ **IP**（**Group IP**）**]**、**[**発信元 **IP**（**Src IP**）**]** と **[RP IP]**：同じマルチキャスト ルート マップのポリシー UI は 2 つの方法で使用できます。マルチキャスト トラフィックのフィルタのセットを構成すること、またはランデブー ポイントの構成をマルチキャスト グループの特定のセットに制限することです。構成するユース ケースによっては、この画面のフィールドの一部だけを指定すればよい場合もあります。
  - マルチキャスト フィルタリングの場合には、フィルタを定義するために、**[**発信元 **IP**（**Source IP**）**]** と **[**グループ（**Group IP**）**]** フィールドを使用します。これらのフィールドの少なくとも 1 つを提供できますが、両方を含むことを選択できます。フィールドの 1 つが空白のままの場合は、すべての値にマッチします。

    グループ IP の範囲は 224.0.0.0 ~ 239.255.255.255 で、ネットマスクは /4 ~ /32 である必要があります。サブネット マスクを指定する必要があります。

    [RP IP]（ランデブー ポイントの IP）は、マルチキャスト フィルタリング ルート マップでは使用しないので、このフィールドはブランクのままにします。

  - ランデブー ポイントの構成では、**[**グループ **IP**（**Group IP**）**]** フィールドを使用して RP のマルチキャスト グループを定義できます。

    グループ IP の範囲は 224.0.0.0 ~ 239.255.255.255 で、ネットマスクは /4 ~ /32 である必要があります。サブネット マスクを指定する必要があります。

ランデブー ポイント構成の場合、**[RP IP]** は RP 構成の一部として構成されます。ルート マップをグループ フィルタリングに使用する場合は、ルート マップに RP IP アドレスを設定する必要はありません。この場合には、**[RP IP]** と **[発信元 IP（Source IP）]** フィールドを空白のままにします。

- **[アクション（Action）]**：アクションは、一致が検出された場合に実行するアクション定義します。トラフィックの [許可（Permit）] または [拒否（Deny）] のいずれかです。

e. チェックマーク アイコンをクリックして、エントリを保存します。

f. 前のサブステップを繰り返して、同じポリシーの追加のルート マップ エントリを作成します。

g. **[保存（Save）]** をクリックしてポリシーを保存し、テンプレート ページに戻ります。

h. この手順を繰り返して、マルチキャスト ポリシーの追加のルート マップを作成します。

5. ルート制御のルート マップ ポリシーを作成。

このポリシーは、包括的な L3Out および SR-MPLS L3Out の使用例の一部です。このセクションにある情報を参照資料として使用することができます。しかし資料の「*機能と使用例*」の項の「外部接続（L3Out）」と「マルチサイトおよび SR-MPLS L3Out ハンドアウト」の章のすべての手順のセットに従うことをおすすめします。

a. **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[ルート コントロールのルート マップ ポリシー（Route Control Policy for Multicast）]** を選択します。

b. 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。

c. （オプション）**[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。

d. **[+エントリを追加（+Add Entry）]** をクリックして、ルート マップ情報を入力します。

ルート マップごとに、1 つ以上のコンテキスト エントリを作成する必要があります。次の情報によると各コンテキストは、1 つ以上の一致基準に基づいてアクションを定義するルールです：

- **[コンテキストの順序（Context Order）]**：コンテキストの順序は、コンテキストが評価される順序を決定するために使用されます。値は 0 ~ 9 の範囲内である必要があります。
- **[コンテキスト アクション（Context Action）]**：コンテキスト アクションは、一致が検出された場合に実行するアクション（[許可（permit）] または [拒否（deny）]）を定義します。複数のコンテキストに同じ値が使用されている場合、それらは定義された順序で 1 つ評価されます。

コンテキストの順序とアクションを定義したら、コンテキストを一致させる方法を選択します。

- **[+ 属性の作成（+Create Attibute）]** をクリックして、コンテキストが一致する必要があるアクションを指定します。

  次のアクションのうちの 1 つを選択できます。

  - コミュニティの設定
  - ルートタグを設定します
  - ダンプニングを設定します
  - 重量の設定
  - ネクストホップの設定

- プリファレンスの設定
- メトリックの設定
- メトリックタイプの設定
- ASパスの設定
- 付加的なコミュニティの設定

属性を構成したら、**[保存（Save）]** をクリックします。

- *定義したアクションを IP アドレスまたはプレフィックスに関連付ける場合は、[IP アドレスの追加（Add IP Address）] をクリックします。

  [プレフィックス（prefix）] フィールドに、IP アドレス プレフィックスを入力します。IPv4 と IPv6 の両方のプレフィックスがサポートされています 。たとえば 2003:1:1a5:1a5::/64 または 205.205.0.0/16 です。

  特定の範囲の IP を集約する場合は、**[集約（aggregate）]** チェックボックスをオンにして、範囲を指定します。たとえば、0.0.0.0/0 プレフィックスを指定して任意の IP に一致させるか、10.0.0.0/8 プレフィックスを指定して任意の 10.xxx アドレスに一致させることができます。

- 定義したアクションをコミュニティ リストに関連付ける場合は、**[コミュニティの追加（Add Community）]** をクリックします。

  [コミュニティ（Community）] フィールドに、コミュニティ文字列を入力します。たとえば、 regular:as2- nn2:200:300 などです。

  次に、**[範囲（Scope）]**を選択します：推移性は、コミュニティが eBGP ピアリング全体（自律システム（AS）全体） に伝播することを意味し、非推移性は、コミュニティが伝播しないことを意味します。

L3Out からアナウンスする必要があるプレフィックスを定義するため、特定のプレフィックスと一致する **IP** アドレスまたはコミュニティ文字列を指定する必要があります（**Set** 属性を指定しない場合でも）。これは、BD のサブネットまたは他の L3Out から学習した中継ルートのいずれかです。

e. 前のサブステップを繰り返して、同じポリシーの追加のルート マップ エントリを作成します。

f. **[保存（Save）]** をクリックしてポリシーを保存し、テンプレート ページに戻ります。

g. この手順を繰り返して、ルート コントロール ポリシーの追加のルート マップを作成します。

6. カスタム QoS ポリシーを作成。

Cisco APIC でカスタム QoS ポリシーを作成して、DSCP または CoS 値に基づいて入力トラフィックを分類し、それを QoS 優先度レベル （QoS ユーザー クラス） に関連付けて、ACI ファブリック内で適切に処理することができます。DSCP の値が IP ヘッダーにある場合または CoS の値が入力トラフィックのイーサネット ヘッダーにあるのみ、分類はサポートされます。さらに、カスタム QoS ポリシーを使用して、入力トラフィックのヘッダー内の DSCP または CoS 値を変更できます。

たとえば、カスタム QoS ポリシーを使用すると、IP ヘッダーのないレイヤ 2 パケットなど、CoS 値のみに基づいてトラフィックをマークするデバイスから ACI ファブリック トラフィックに着信するトラフィックを分類できます。

ACI ファブリック内の QoS 機能の詳細については、「*Cisco APIC と QoS*」を参照します。

a. **[+**オブジェクトの作成（**+Create Object**）**]** ドロップダウンから、**[**カスタム **QoS** ポリシー（**Custom QoS Policy**）**]** を選択します。

b. 右のプロパティのサイドバーでは、ポリシーの **[**名前（**Name**）**]** を指定します。

c. （オプション）**[**説明を追加（**Add Description**）**]** をクリックして、このポリシーの説明を入力します。

d. **[+ DSCP** マッピングを追加（**+Add DSCP Mappings**）**]** をクリックして、必要な情報を入力します。

DSCP マッピング構成を使用すると、マッピングで指定された範囲内に DSCP 値がある入力トラフィックを指定された QoS 優先度レベル（クラス）に関連付けることができます。また、入力トラフィックの DSCP または CoS 値を設定して、トラフィックがファブリックを出るときにそれらの値を保持できるようにすることもできます。

出力トラフィックのターゲット CoS 値を保持するには、NDO ファブリックポリシーの一部である「CoS を保持する」ポリシーを構成する必要があります。

[DSCP ターゲット（DSCP Target）] または [ターゲット CoS（Target CoS）] の値が DSCP マッピングと CoS マッピングの両方の一部として設定される場合、DSCP マッピングで指定された値が優先されます。

マッピングごとに、次のフィールドを指定できます：

- **[DSCP** 開始（**DSCP From**）**]**：DSCP 範囲の開始。
- **[DSCP** 終了（**DSCP To**）**]**：DSCP 範囲の終了。
- **[DSCP** ターゲット（**DSCP Target**）]：出力トラフィックのために保持される入力トラフィックに設定する DSCP 値。
- **[**ターゲット **CoS**（**Target CoS**）**]**：「CoS を保持」が有効になっている場合に、出力トラフィックのために保持される入力トラフィックに設定する CoS 値。
- **[**優先度（**Priority**）**]**：トラフィックが割り当てられる QoS 優先度クラス。

マッピングを指定したら、チェックマーク アイコンをクリックして保存します。 次に、**[+DSCP** マッピングの追加（**+Add DSCP Mappings**）**]** をクリックして、同じポリシー内に追加のマッピングを提供できます。

e. **[**追加（**Add**）**]** をクリックしてポリシーを保存し、テンプレート ページに戻ります。

f. **[+ CoS** マッピングを追加（**+Add CoS Mappings**）**]** をクリックして、必要な情報を入力します。

DSCP マッピング構成を使用すると、マッピングで指定された範囲内に DSCP 値がある入力トラフィックを指定された QoS 優先度レベル（クラス）に関連付けることができます。また、入力トラフィックの DSCP または CoS 値を設定して、トラフィックがファブリックを出るときにそれらの値を保持できるようにすることもできます。

出力トラフィックのターゲット CoS 値を保持するには、NDO ファブリックポリシーの「CoS を保持する」ポリシーを構成する必要があります。

[DSCP ターゲット（DSCP Target）] または [ターゲット CoS（Target CoS）] の値が DSCP マッピングと CoS マッピングの両方の一部として設定される場合、

DSCP マッピングで指定された値が
優先されます。

マッピングごとに、次のフィールドを指定できます：

- **[Dot1P 開始（Dot1P From）]**：CoS 範囲の開始。
- **[Dot1P 終了（Dot1P To）]**：Dot1P 範囲の終了。
- **[DSCP ターゲット（DSCP Target）]**：出力トラフィックのために保持される入力トラフィックに設定する DSCP 値。
- **[ターゲット CoS（Target CoS）]**：「CoS を保持」が有効になっている場合に、出力トラフィックのために保持される入力トラフィックに設定する CoS 値。
- **[優先度（Priority）]**：トラフィックが割り当てられる QoS 優先度クラス。

マッピングを指定したら、チェックマーク アイコンをクリックして保存します。 次に、**[+Cos マッピングの追加（+Add Cos Mappings）]** をクリックして、同じポリシー内に追加のマッピングを提供できます。

g. **[追加（Add）]** をクリックしてポリシーを保存し、テンプレート ページに戻ります。

h. この手順を繰り返して、ルート コントロール ポリシーの追加のルート マップを作成します。

7. DHCP リレー ポリシーの作成。

このポリシーは、包括的な DHCP リレー ユース ケースの一部です。このセクションにある情報を参照資料として使用することができます。しかし資料の「*機能と使用例*」項の「DHCP リレー」の章で説明されているすべての手順のセットに従うことをおすすめします。

a. **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[DHCP リレー ポリシー（DHCP Relay Policy）]** を選択します。

b. 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。

c. （オプション）**[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。

d. **[プロバイダの追加（Add Provider）]** をクリックして、エンドポイントによって発信された DHCP 要求をリレーする DHCP サーバを構成します。

e. プロバイダ タイプを選択します。

リレー ポリシーを追加するときには、次の 2 つのタイプのうちの 1 つを選択できます。

- [アプリケーション EPG（Application EPG）]：DHCP 要求をリレーする DHCP サーバを含むアプリケーション EPG を指定します。
- [L3 外部ネットワーク（L3 External Network）]：ファブリックの外部のネットワークの場所 でもある DHCP サーバが接続されている場所へのアクセスに使用される L3Out に関連付けられた外部 EPG を指定します。

Orchestrator をサイトにまだ展開していない場合でも、Orchestratorで作成され、指定したテナントに割り当てられている EPG またを
選択できます。展開されていない EPG を選択した
場合、DHCP リレー構成を完了することはできますが、
は、リレーを使用できるようにする前に EPG を展開する必要があります。

f. **[アプリケーション EPG を選択（Select an Application EPG）]** または **[外部 EPG を選択（Select an External EPG）]**（選択したプロバイダー タイプに基づく）をクリックし、プロ

バイダー EPG を選択します。

g. **[DHCP** サーバ アドレス（**DHCP Server Address**）**]** フィールドに、DHCP サーバの IP アドレスを入力します。

h. 必要に応じて、**[DHCP** サーバ **VRF** 設定（**DHCP Server VRF Preference**）**]** オプションを有効にします。

この機能は、Cisco APIC リリース 5.2（4）に紹介されています。必要なユース ケースの詳細については、『Cisco APIC 基本構成ガイド』を参照してください。

i. **[OK]** をクリックして、プロバイダ情報を保存します。

j. 同じ DHCP リレー ポリシー内の追加のプロバイダーについて、前のサブステップを繰り返します。

k. このステップを繰り返して、追加の DHCP リレー ポリシーを作成します。

8. DHCP オプション ポリシーの作成。

このポリシーは、包括的な DHCP リレーの使用例の一部です。このセクションにある情報を参照資料として使用することができます。しかし資料の「*機能と使用例*」項の「DHCP リレー」の章で説明されているすべての手順のセットに従うことをおすすめします。

a. **[+**オブジェクトの作成（**+Create Object**）**]** ドロップダウンから、**[DHCP** オプション ポリシー（**DHCP Option Policy**）**]** を選択します。

b. 右のプロパティのサイドバーでは、ポリシーの **[**名前（**Name**）**]** を指定します。

c. （オプション）**[**説明を追加（**Add Description**）**]** をクリックして、このポリシーの説明を入力します。

d. [Add Option] をクリックします。

e. オプションの詳細を入力します。

DHCP オプションごとに、以下を指定します：

- **[**名前（**Name**）**]**：必ずしも要求されてはいませんが、RFC 2132 にリストされているオプションには、同じ名前を使用することをお勧めします。

  たとえば、ネーム サーバ が挙げられます。

- **[id]**：オプションが値を要求した場合はそれを指定します。

  たとえば、[ネーム サーバ] オプションのクライアントに使用可能なネーム サーバのリスト。

- **[**データ（**Data**）**]**：オプションが値を要求した場合はそれを指定します。

  たとえば、[ネーム サーバ] オプションのクライアントに使用可能なネーム サーバのリスト。

f. **[OK]** をクリックして保存します。

g. 同じ DHCP オプション ポリシー内の追加オプションについて、前のサブステップを繰り返します。

h. このステップを繰り返して、追加の DHCP オプション ポリシーを作成します。

9. IGMP インターフェイス ポリシーを作成します。

IGMP スヌーピングは、ブリッジ ドメイン内の IP マルチキャスト トラフィックを調べて、該当する受信側が常駐するポートを検出します。IGMP スヌーピングではポート情報を利用することによ

り、マルチアクセスブリッジ ドメイン環境における帯域幅消費量を削減し、ブリッジ ドメイン全体へのフラッディングを回避します。

ACI ファブリックでの IGMP スヌーピングの詳細については、使用しているリリースの *Cisco APIC Layer 3 Networking Configuration Guide* の「IGMP Snooping」の章を参照してください。

a. **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[IGMP インターフェイス ポリシー（IGMP Interface Policy）]** を選択します。
b. 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c. （オプション）**[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d. ポリシーの詳細を入力します。

   - **[バージョン 3 ASM を許可（Allow Version 3 ASM）]**：SSM 範囲外のマルチキャスト グループの IGMP バージョン 3 送信元固有レポートの受け入れを許可します。この機能がイネーブルの場合、グループが設定された SSM 範囲外であっても、グループと送信元の両方を含む IGMP バージョン 3 レポートを受信すると、スイッチは（S, G）mroute エントリを作成します。ホストが SSM 範囲外の（*, G）レポートを送信する場合、または SSM 範囲の（S、G）レポートを送信する場合、この機能は不要です。
   - **[高速脱退（Fast Leave）]**：デバイスからグループ固有のクエリが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間を最小限にできるオプション。高速脱退を有効にすると、デバイスではグループに関する脱退メッセージの受信後、ただちにマルチキャスト ルーティング テーブルからグループ エントリが削除されます。デフォルトは次のとおりです。
     アラートメールを送信する頻度。

     これは、所定のグループに対する BD/インターフェイスの背後にただ 1 つの受信者しか存在しない場合に使用します。

   - **[レポート リンクローカル グループ（Report Link Local Groups）]**：224.0.0.0/24 に含まれるグループに対して、レポート送信を有効にします。非リンク ローカル グループには、常にレポートが送信されます。デフォルトでは、リンク ローカル グループにレポートは送信されません。
   - **[IGMP バージョン（IGMP Version）]**：ブリッジ ドメインまたはインターフェイスで有効にする IGMP のバージョン。有効な IGMP バージョンは 2 または 3 です。デフォルトは 2 です。
   - **[詳細設定（Advanced Settings）]**：このセクションの横にある矢印をクリックして展開します。
     - **[グループ タイムアウト（Group Timeout）]**：ルータによって、ネットワーク上にグループのメンバーまたは送信元が存在しないと見なされるまでのグループ メンバーシップ インターバル。有効範囲は 3 ~ 65,535 秒です。デフォルト値は 260 秒です。
     - **[クエリ インターバル（Query Interval）]**： IGMP ホスト クエリ メッセージの送信頻度を設定します。値の範囲は 1 ~ 18,000 秒です。デフォルト値は 125 秒です。
     - **[クエリ応答インターバル（Query Response Interval）]**：IGMP クエリでアドバタイズされる応答時間を設定します。値の範囲は 1 ~ 25 秒です。デフォルトは 10 秒です。
     - **[最終メンバー カウント（Last Member Count）]**：ホストの Leave メッセージを受信してから、IGMP クエリが送信される回数を設定します。値の範囲は 1 ~ 5 です。デフォルトは 2 です。

- **[最終メンバー応答時間（Last Member Response Time）]**：メンバーシップ レポートを送信してから、ソフトウェアがグループ ステートを解除するまでのクエリ インターバルを設定します。値の範囲は 1 ~ 25 秒です。デフォルト値は 1 秒です。
- **[スタートアップ クエリ カウント（Startup Query Count）]**：マルチキャスト トラフィックをルーティングする必要がないため、プロトコル独立マルチキャストを有効にしていない場合に、起動時に送信される多くのクエリに対してスヌーピングを構成します。値の範囲は 1 ~ 10 です。デフォルト値は 2 メッセージです。
- **[スタートアップ クエリ インターバル（Startup Query Interval）]**：起動時の IGMP スヌーピング クエリ間隔を設定します。指定できる範囲は 1 ~ 18,000 秒です。デフォルト値は 125 秒です。
- **[クエリア タイムアウト（Querier Timeout）]**：クエリアとして処理を引き継ぐかどうかをソフトウェアが判断するための、クエリア タイムアウト値を設定します。値の範囲は 1 ~ 65,535 秒です。デフォルト値は 255 秒です。
- **[ロバストネス変数（Robustness Variable）]**：ロバストネス変数を設定します。ネットワークのパケット損失が多い場合は、この値を大きくします。値の範囲は 1 ~ 7 です。デフォルトは 2 です。
- **[ステート リミットルート マップ（State Limit Route Map）]**：予約済み

  マルチキャスト エントリ機能で使用。ルート マップ ポリシーは、ステッ

  プ 2 の説明に従ってすでに作成されている必要があります。

- **[レポート ポリシー ルート マップ（Report Policy Route Map）]**：ルート マップ ポリシーに基づく IGMP レポートのポリシーにアクセスします。IGMP グループ レポートは、ルートマップで許可されたグループに対してのみ選択されます。

  ルート マップ ポリシーは、ステップ 2 の説明に従ってすでに作成されている必要があります。

- **[スタティック レポート ルート マップ（Static Report Route Map）]**：マルチキャスト グループを発信インターフェイスに静的にバインドし、スイッチ ハードウェアで処理されます。グループ アドレスのみを指定する
  場合、（*、G）ステートが作成されます。送信元アドレスを指定した場合は、（S, G）ステートが作成されます。グループ プレフィックス、グループ範囲、および送信元プレフィックスを示すルートマップ ポリシー名を指定できます。IGMPv3 をイネーブルにした場合にのみ、（S, G）ステートに対して送信元ツリーが作成されます。

  ルート マップ ポリシーは、ステップ 2 の説明に従ってすでに作成されている必要があります。

- **[最大マルチキャスト エントリ（Maximum Multicast Entries）]**：IGMP レポートによって作成される BD またはインターフェイスの mroute 状態を制限します。デフォルトは無効にされ、制限は設定されません。有効な範囲は 1 ~ 4294967295 です。

e. このステップを繰り返して、追加の IGMP インターフェイス ポリシーを作成します。

10. MLD スヌーピング ポリシーを作成します。

    マルチキャスト リスナー検出（MLD）スヌーピングにより、ホストとルータ間で IPv6 マルチキャスト トラフィックを効率的に配信できます。これは、MLD クエリまたはレポートを送受信したポートのサブセットにブリッジ ドメイン内の IPv6 マルチキャスト トラフィックを制限する レイヤ 2 機能です。このように、MLD スヌーピングは、マルチキャスト トラフィックの受信に関心を示

しているノードがないネットワークのセグメントでは帯域幅を節約できるという利点があります。これにより、ブリッジ ドメインでフラッディングが生じることがなく、帯域幅の使用量が削減され、ホストとルータで不要なパケット処理を節約できます。

ACI ファブリックでの MLD スヌーピングの詳細については、使用しているリリースの *Cisco APIC Layer 3 Networking Configuration Guide* の「MLD Snooping」の章を参照してください。

a. **[+**オブジェクトの作成（**+Create Object**）**]** ドロップダウンから、**[MLD** スヌーピング ポリシー（**MLD Snooping Policy**）**]** を選択します。
b. 右のプロパティのサイドバーでは、ポリシーの **[**名前（**Name**）**]** を指定します。
c. （オプション）**[**説明を追加（**Add Description**）**]** をクリックして、このポリシーの説明を入力します。
d. ポリシーの詳細を入力します。

   - **[**管理状態（**Admin State**）**]** : MLD スヌーピング機能を有効または無効にします。
   - **[**高速脱退コントロール（**Fast Leave Control**）**]** : ブリッジ ドメインごとに高速脱退機能をオンまたはオフにできます。これは MLDv2 ホストに適用され、1 つのホストだけがそのポートの背後で MLD を実行することがわかっているポートで使用されます。

     デフォルトは無効です。

   - **[**クエリア コントロール（**Querier Control**）**]** : MLD スヌーピング クエリア処理を有効または無効にします。MLD スヌーピング クエリアは、マルチキャスト トラフィックをルーティングする必要がないため、PIM および MLD を設定していないブリッジ ドメイン内で MLD スヌーピングをサポートします。

     デフォルトは無効です。

   - **[**クエリア バージョン（**Querier Version**）**]** : クエリア バージョンを選択できます。デフォルトは、Version2 です。

   - **[**詳細設定（**Advanced Settings**）**]** : このセクションの横にある矢印をクリックして展開します。
     - **[**クエリ インターバル（**Query Interval**）**]** : MLD ホスト クエリ メッセージをソフトウェアが送信する頻度を設定します。値の範囲は 1 ~ 18,000 秒です。

デフォルト値は 125 秒です。

- **[クエリ応答間隔（Query Response Interval）]**：MLD クエリでアドバタイズされる応答時間を設定します。値の範囲は 1 ~ 25 秒です。

  デフォルトは 10 秒です。

- **[最終メンバー クエリ インターバル（Last Member Query Interval）]**：メンバーシップ レポートを送信してから、ソフトウェアがグループ ステートを削除するまでのクエリ応答時間を設定します。値の範囲は 1 ~ 25 秒です。

  デフォルト値は 1 秒です。

- **[スタート クエリ カウント（Start Query Count）]**：マルチキャスト トラフィックをルーティングする必要がないため、PIM を有効にしていない場合に、起動時に送信される多くのクエリに対してスヌーピングを構成します。値の範囲は 1 ~ 10 です。

  デフォルトは 2 です。

- **[スタート クエリ インターバル（Start Query Interval）]**：マルチキャスト トラフィックをルーティングする必要がないため、PIM を有効にしていない場合に、起動時のスヌーピング クエリ インターバルを構成します。値の範囲は 1 ~ 18,000 秒です。

  デフォルト値は 31 秒です。

e. 追加のMLD スヌーピング ポリシーを作成するために、このステップを繰り返します。

11. L3Out ノード ルーティング ポリシーを作成します。

このポリシーは、包括的な L3Out および SR-MPLS L3Out 構成の使用例の一部です。このセクションにある情報を参照資料として使用することができます。しかし資料「機能と使用例」の項の「*外部接続（L3Out）*」章のすべての手順のセットに従うことをおすすめします。

a. メインペインで、**[オブジェクトの作成（Create Object）] > [L3Out ノード ルーティング ポリシー（L3Out Node Routing Policy）]** を選択します。

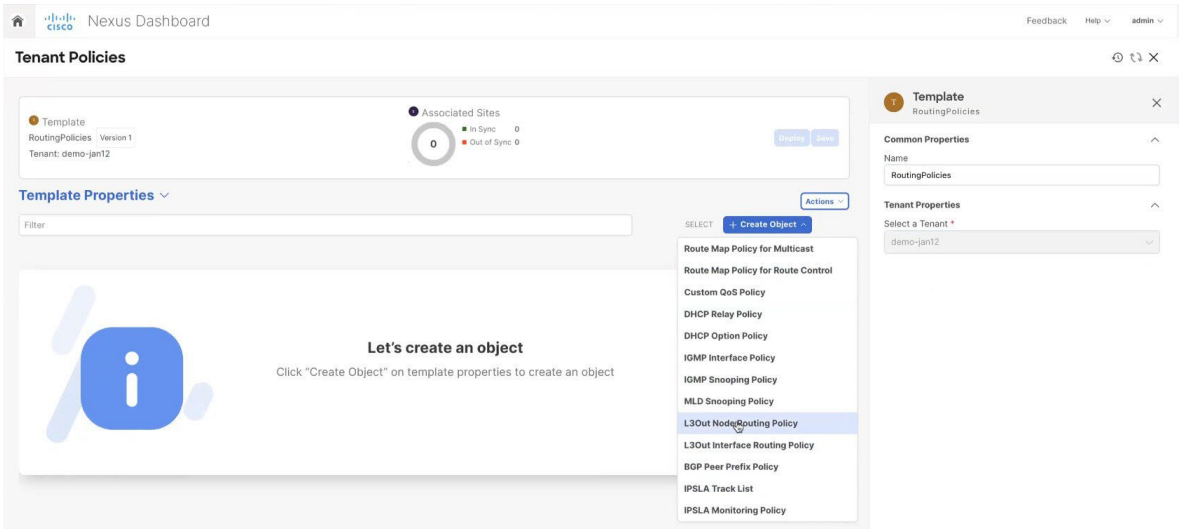

図 1. オブジェクトの作成

b. ポリシーの **[名前（Name）]** を入力し、**[BFD マルチホップ設定（BFD MultiHop Settings）]**、**[BGP ノード設定（BGP Node Settings）]**、または **[BGP ベスト パス制御（BGP Best Path Control）]** オプションの少なくとも 1 つを追加します。

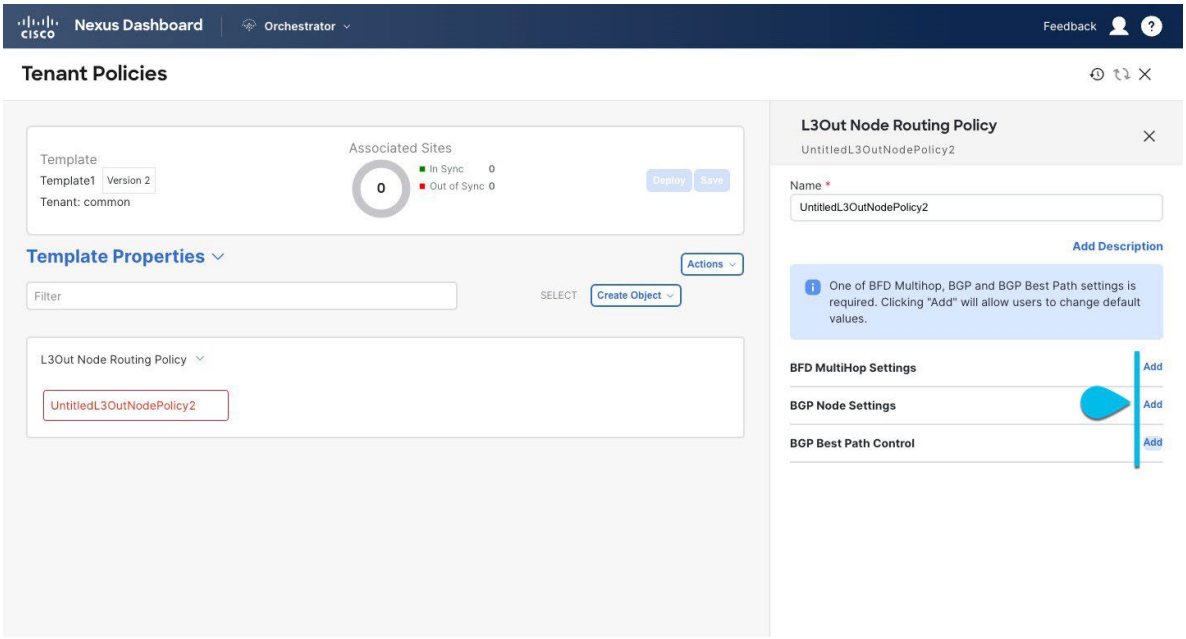

図 2 BFDマルチホップ設定

- **[BFD マルチホップ設定（BFD MultiHop Settings）]**：1 つ以上のホップのある接続先の転送の失敗を検出します。

  この場合、単一ホップで作られるインターフェイスの代わりにマルチホップ セッションが送信元と接続先の間に作られます。

  BFD マルチホップ構成には、Cisco APIC リリース 5.0(1) 以降が必要です。

- **[BGP ノード設定（BGP Node Settings）]**：BGP ピアの間の BGP 隣接関係に BGP プロトコル タイマーとセッション設定を構成することができます。
- **[BGP ベストパス コントロール（BGP Best Path Control）]**：様々な BGP ASN から受けとった複数のパスの間のロードバランシングを有効化する as-path multipath-relax を有効にします。

12. L3Out インターフェイス ルーティング ポリシーを作成します。

    このポリシーは、包括的な L3Out および SR-MPLS L3Out 構成の使用例の一部です。このセクションにある情報を参照資料として使用することができます。しかし資料「機能と使用例」の項の「*外部接続（L3Out）*」章のすべての手順のセットに従うことをおすすめします。

    a. メインペインで、**[オブジェクトの作成（Create Object）] > [L3Out インターフェイス ルーティング ポリシー（L3Out Interface Routing Policy）]** を選択します。

    b. ポリシーの **[名前（Name）]** を指定し、**[BFD 設定（BFD Settings）]**、**[BFD マルチホップ設定（BFD Multi-Hop Settings）]**、および **[OSPF インターフェイス設定（OSPF Interface Settings）]** を定義します。

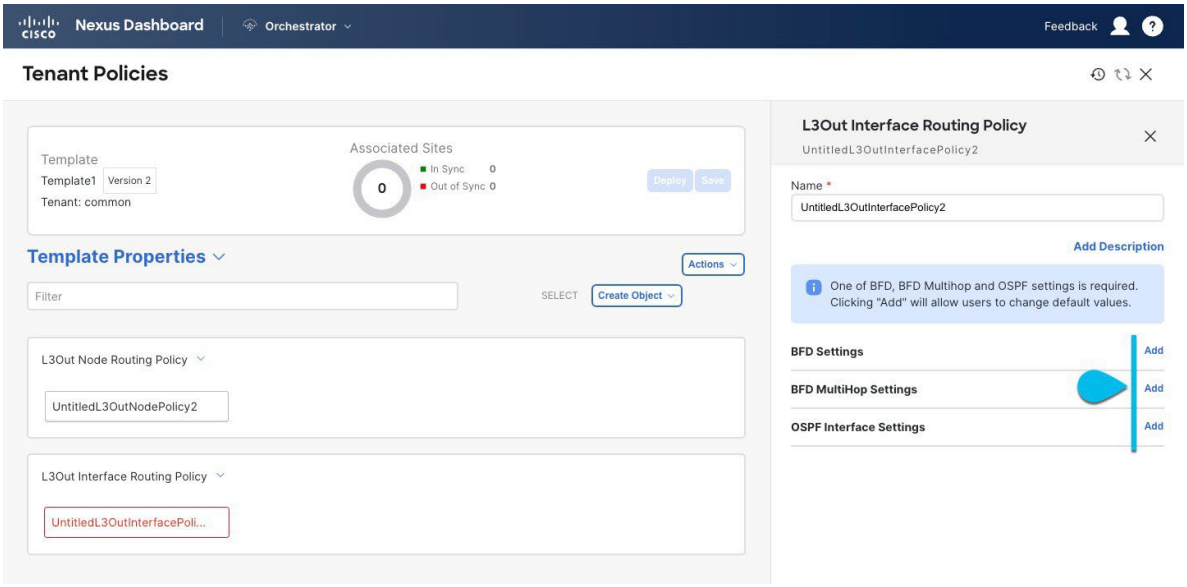

図 3. ObjectL3Out の作成

- **[BFD 設定（BFD Settings）]**：直接接続されているインターフェイス上のデバイス間で確立される BFD セッションの BFD パラメータを指定します。

  複数のプロトコルがルータ間ので有効にされている場合、各プロトコルにリンク失敗の検出機能が備わっています。それぞれ、違うタイムアウトがある可能性があります。BFD は、一貫性のある予測できる統合時間を出すために全てのプロトコルに対して均一なタイムアウトを出します。

- **[BFD マルチホップ設定（BFD MultiHop Settings）]**：直接接続されていないインターフェイス上のデバイス間で確立される BFD セッションの BFD パラメータを指定します。

  上記の「テナント ポリシー テンプレート：ノード ルーティング グループ ポリシー」セクションで説明したように、これらの設定をノード レベルで構成できます。インターフェイスがその設定を継承した場合、インターフェイス ルーティング グループ ポリシーの単独インターフェイスの node-level 設定を上書きできます。

  BFD マルチホップ構成には、Cisco APIC リリース 5.0(1) 以降が必要です。

- **[OSPF インターフェイス設定（OSPF Interface Settings）]**：OSPF ネットワーク タイプ、優先度、コスト、間隔、制御などのインターフェイス レベルの設定を構成できます。

  このポリシーは、OSPF を使用して L3Out を展開するときに作成する必要があります。

13. BGP ピア プレフィックス ポリシーを作成します。

    このポリシーは、包括的な L3Out および SR-MPLS L3Out 構成の使用例の一部です。このセクションにある情報を参照資料として使用することができます。しかし資料「機能と使用例」の項の「*外部接続（L3Out）*」章のすべての手順のセットに従うことをおすすめします。

    a. メインペインで、**[オブジェクトの作成（Create Object）] > [BGP ピア プレフィックス ポリシー（BGP Peer Prefix Policy）]** を選択します。

    b. ポリシーの **[名前（Name）]** を指定し、**[プレフィックスの最大数（Max Number of Prefixes）]** と、その数を超えた場合に実行する **[アクション（Action）]** を

定義します。
次の動作が設定可能です。

- ログ
- 却下
- 再起動
- シャットダウン

14. IP SLA モニタリングポリシーを作成します。

このポリシーは、包括的な L3Out および SR-MPLS L3Out 構成の使用例の一部です。このセクションにある情報を参照資料として使用することができます。しかし資料「機能と使用例」の項の「*外部接続（L3Out）*」章のすべての手順のセットに従うことをおすすめします。

a. メインペインで、**[**オブジェクトの作成（**Create Object**）**] > [IP SLA** モニタリング ポリシー（**IPSLA Monitoring Policy**）**]** を選択します。

b. ポリシーの **[**名前（**Name**）**]** を指定し、その設定を定義します。

[SLA タイプ（SLA **Type**）**]** に HTTP を選択した場合、ファブリックは Cisco APIC リリース 5.1(3) 以降を実行している必要があります。

15. IP SLA トラック リストを作成します。

このポリシーは、包括的な L3Out および SR-MPLS L3Out 構成の使用例の一部です。このセクションにある情報を参照資料として使用することができます。しかし資料「機能と使用例」の項の「*外部接続（L3Out）*」章のすべての手順のセットに従うことをおすすめします。

a. メインペインで、**[**オブジェクトを作成（**Create Object**）**] > [IP SLA** トラック リスト（**IP SLA Track List**）**]** を選択します。

b. ポリシーの **[**名前（**Name**）**]** を入力します。

c. **[**タイプ（**Type**）**]** を選択します。

利用可能または利用不可能なルートの定義は、[しきい値パーセンテージ（Threshold Percentage）] または [しきい値重み（Threshold Weight）] に基づいて行うことができます。

d. **[+** トラック リストをトラック メンバー関係に追加（**+Add Track List to Track Member Relation**）**]** をクリックして、1 つ以上のトラック メンバーをこのトラック リストに追加します。

トラック メンバーに関連付けるブリッジ ドメインまたは L3Out を選択する必要があります。作成されたブリッジ ドメイン（BD）または L3Out がまだない場合は、
トラック メンバーの追加をスキップして、
割り当てをせずにポリシーを保存し、BD または L3Out が作成された後に戻ることができます。

e. [トラック メンバー関係にトラック リストを追加（**Add Track List to Track Member Relation**）] ダイアログで、**[**宛先 **IP**（**Destination IP**）**]**、**[**範囲タイプ（**Scope Type**）**]** を指定し、**[IP SLA** モニタリング ポリシー（**IP SLA Monitoring Policy**）**]** を選択します。

追跡リストの範囲は、ブリッジ ドメインまたは L3Out のいずれかです。IP SLA モニタリング

ポリシーは、前の手順で作成したものです。

16. テンプレートの変更内容を保存するために**[保存（Save）]** をクリックします。

    テンプレートを 1 つ以上のサイトに保存（または展開）すると、Orchestrator は、指定されたノードまたはインターフェースがサイトに対して有効であることを確認し、エラーを返します。

17. 関連サイトに新しいテンプレートを展開するために**[展開（Deploy）]** をクリックします。

    テナント ポリシー テンプレートの展開方法とアプリケーション テンプレートの展開方法は同じです。

    以前にこのテンプレートを展開したものの、それ以降に変更を加えていない場合は、**[展開（Deploy）]** の概要に変更がないことが示され、テンプレート全体を再展開することを選択できます。この場合は、この手順をスキップできます。

    そうでなかった場合、**[サイトに展開（Deploy to Sites）]** ウィンドウには、サイトに展開される構成の違いの概要が表示されます。この場合、構成の違いのみがサイトに展開されることにご注意ください。テンプレート全体を再展開したい場合、違いを同期するために1 回展開をする必要があります。そして、前のパラグラフに記されている通り、構成全体をプッシュするためにまた再展開します。

初版：2024 年 3 月 1 日
最終更新日：2024 年 3 月 1 日

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax：408 527-0883