



テナントとテナントポリシーテンプレート

- [テナントの概要 \(1 ページ\)](#)
- [新しいテナントの作成 \(2 ページ\)](#)
- [既存テナントのインポート \(3 ページ\)](#)
- [テナントポリシーテンプレートを作成 \(4 ページ\)](#)

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。



(注) テナントを管理するには、パワー ユーザまたはサイトとテナント マネージャの読み取り/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。

- `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 ファブリックの設定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

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。

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 テンプレートを作成 \(4 ページ\)](#) を参照してください。

新しいテナントの作成

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、[既存テナントのインポート \(3 ページ\)](#) に記されているステップに従います。

始める前に

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

ステップ 1 Cisco Nexus Dashboard にログインし、Cisco Nexus Dashboard Orchestrator サービスを開きます。

ステップ 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。

ステップ 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**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**は、**[表示名 (Display Name)]** テキストボックスの下に表示されます。

(注) テナントの**表示名**はいつでも変更できますが、テナントの作成後に**内部名**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。

(注) 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には、そのドメイン内で幅広いレベルの特権を与えることができます。ユーザーが別のテナントの物理環境に不注意で影響を与える心配はありません。

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。

ステップ 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

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 [新しいテナントの作成 \(2 ページ\)](#) で説明されている手順に従ってください。

始める前に

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

ステップ 1 Cisco Nexus Dashboard にログインし、Cisco Nexus Dashboard Orchestrator サービスを開きます。

ステップ 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。

ステップ 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 (...) メニューを取得して、**[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。

ステップ 4 **[インポート テナント (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。

ステップ 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

ステップ 1 Cisco Nexus Dashboard にログインし、Cisco Nexus Dashboard Orchestrator サービスを開きます。

ステップ 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を作成 (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つ以上定義できます。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。

ステップ 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。

ステップ 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 [レイヤ3 マルチキャスト](#) 章の機能とユースケースセクション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、**[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** – 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、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、**[ソース 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、すべての値と一致します。

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、このフィールドは空白のままにします。

- ランデブー ポイントの設定では、**[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 **[ソース IP (Source IP)]** フィールドを空白のままにします。

- **アクション** – 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の許可または拒否を定義します。

- 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。

ステップ 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。しかしこの資料の「機能とユースケース」セクションの[外部接続 \(L3Out\)](#) および[マルチサイトと SR-MPLS L3Out ハンドオフ](#) 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** – 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** – 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の許可または拒否を定義します。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 Attribute)]** 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 タグの設定
- ダンプニングを設定します
- ウェイトの設定
- 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
- 追加のコミュニティを設定

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(例:2003:1:1a5:1a5::/64または205.205.0.0/16)。

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-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。

- (注) 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。

- 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。
- [**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。
- 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。

ステップ 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。

- [**+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。
- 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。
- (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。
- [**+ 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。

- (注) 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」または「ターゲット 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ている場合、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 から – DSCP 範囲の開始。**
- **DSCP へ – DSCP 範囲の終わり。**
- **DSCP ターゲット** – 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** – 「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** – 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。

(注) 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。

さらに、「DSCP ターゲット」または「ターゲット 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ている場合、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 から – CoS 範囲の開始。**
- **Dot1P へ – CoS 範囲の終わり。**
- **DSCP ターゲット** – 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** – 「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** – 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。

ステップ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 [DHCP リレー](#) 章の 機能とユース ケース セクション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、**[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 : 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 : 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。

(注) 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 または外部 EPG を選択できます。展開されていない EPG を選択した場合でも、DHCP リレー構成を完了することができますが、リレーが使用可能になる前に 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]** 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、プロバイダー情報を保存します。
- 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。

ステップ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 [DHCP リレー](#) 章の 機能とユース ケース セクション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、[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：

- **Name** – 技術的には要求されていませんが、[RFC 2132](#) にリストされたオプションに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。
- **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。

ステップ 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ドイングを回避します。

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** – 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** – デバイスからグループ固有のクエリー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。デフォルトではディセーブルになっています。

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** – 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** – ブリッジドメインまたはインターフェイスでイネーブルにする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。
- **高度な設定** – このセクションの隣の→をクリックして、展開してください。
 - **グループタイムアウト** – 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** – IGMPホストクエリメッセージの送信頻度を設定します。有効範囲は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** – 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** – ホストのLeaveメッセージを受信してから、IGMPクエリー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** – 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タスを解除するまでのクエリー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** – 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** – 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** – 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** – 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** – 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** – 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** – 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した場合は、(*, 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** – 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。

ステップ 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グ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。

- [+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。
- 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。
- (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。
- ポリシーの詳細を入力します。

- **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** – 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** – 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** – 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。

- **高度な設定** – このセクションの隣の→をクリックして、展開してください。

- **クエリ インターバル** – 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。有効範囲は 1 ~ 18,000 秒です。

デフォルト値は 125 秒です。

- **クエリ応答間隔** : 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** – 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** : 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** – 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 をイネーブル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。

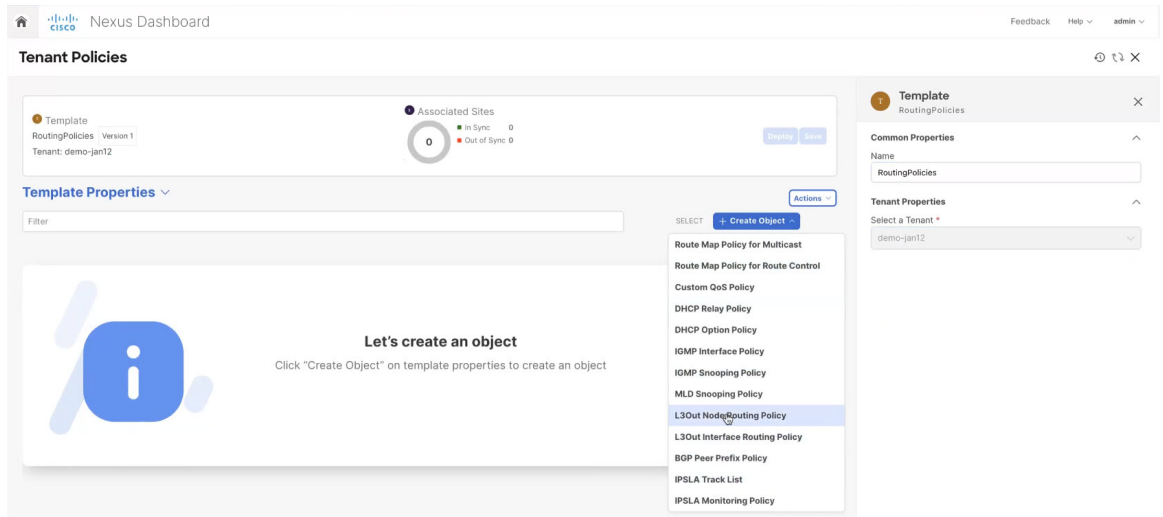
デフォルト値は 31 秒です。

- 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。

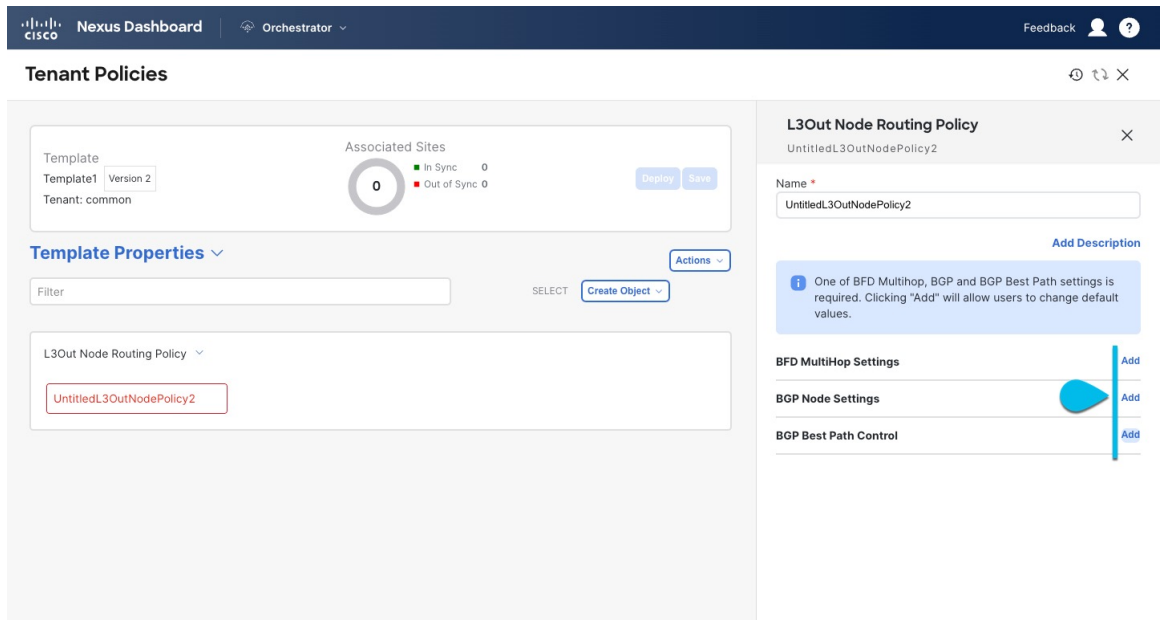
ステップ 11 L3Out ノードルーティング ポリシーを作成します。

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。しかし資料の [外部接続 \(L3Out\)](#) 章の機能とユースケース セクション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。



- 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。



- **BFD マルチホップ設定** : 1 つ以上のホップのある接続先の転送の失敗の検出を提供します。

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。

(注) 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 ピアの間 BGP 隣接関係に BGP プロトコル タイマーとセッション構成を構成することができます。

- **BGP ベストパスコントロール**：様々な BGP ASN から受けとった複数のパスの間の load-balancing の有効化である `as-path multipath-relax` を有効にできます。

ステップ 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。しかし資料の [外部接続 \(L3Out\)](#) 章の機能とユースケースセクションのすべての手順のセットに従うことをおすすめします。

- 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。
- ポリシーの名前を指定し、**BFD 設定**、**BFD マルチホップ設定**、および **OSPF インターフェイス設定** を定義します。

The screenshot displays the Cisco Nexus Dashboard interface for configuring a Tenant Policy. The main area shows the 'Template Properties' section with a filter and a 'Create Object' button. The right-hand panel is titled 'L3Out Interface Routing Policy' and contains a form for configuring the policy. The form includes a 'Name' field, a 'Description' field, and three sections for settings: 'BFD Settings', 'BFD MultiHop Settings', and 'OSPF Interface Settings'. Each of these sections has an 'Add' button next to it. A notification message states: 'One of BFD, BFD MultiHop and OSPF settings is required. Clicking "Add" will allow users to change default values.'

- **BFD 設定**：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**：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。

(注) BFD マルチホップ設定には、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 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。

(注) 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。

ステップ 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。しかし資料の [外部接続 \(L3Out\)](#) 章の機能とユースケース セクションのすべての手順のセットに従うことをおすすめします。

- 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。
- ポリシーの**名前**を指定し、**プレフィックスの最大数**と、その数を超えた場合に実行する**アクション**を定義します。

次の動作が設定可能です。

- Log
- 拒否
- [Restart]
- シャットダウン

ステップ 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。しかし資料の [外部接続 \(L3Out\)](#) 章の機能とユースケース セクションのすべての手順のセットに従うことをおすすめします。

- 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。
- ポリシーの**名前**を指定し、その設定を定義します。

(注) **SLA タイプ**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。

ステップ 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。しかし資料の [外部接続 \(L3Out\)](#) 章の機能とユースケース セクションのすべての手順のセットに従うことをおすすめします。

- 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。
- ポリシーの**名前**を入力します。
- 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またはしきい値重み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**] 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。

(注) 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。ブリッジ ドメイン (BD) または L3Out をまだ作成していない場合は、トラック メンバーの追加をスキップし、1つを割り当てずにポリシーを保存し、BD または L3Out を作成し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、範囲タイプを指定し、**IP SLA モニタリング ポリシー**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。

ステップ 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。

(注) 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。

ステップ 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が、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。

或いは、**[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する必要があります。

翻訳について

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