



ACI ファブリックの Nexus Dashboard
Orchestrator ファブリック管理テン
プレート、リリース 4.4.x

目次

ファブリック管理テンプレート	1
ファブリックポリシーを作成	3
ファブリック技術情報ポリシーを作成	20
モニタリングポリシーを作成	28

ファブリック管理テンプレート

リリース 4.0(1) 以降、Cisco Nexus Dashboard Orchestrator では、複数のファブリックポリシー、ファブリックリソースポリシー、およびモニタリングポリシーを構成できます。[スキーマおよびアプリケーションテンプレート](#)を使用してオブジェクトを作成し、VRF、BD、または EPG の構成を定義する方法と同様に、これらの新しいポリシーはそれぞれのテンプレートタイプで定義されます。次のセクションでは、NDO から直接構成できるようになったポリシーと、そのために必要な手順について説明します。

アプリケーションテンプレートで定義するオブジェクトは、ファブリックの APIC 内の同じ管理対象オブジェクト (MO) に 1 対 1 でマッピングされますが、新しいテンプレートタイプでは、一部のオブジェクトとポリシーを論理コンテナにグループ化します。このような場合、NDO の新しいテンプレートタイプの 1 つで同じ論理コンテナ内の必要なすべてのポリシーを定義した後、オーケストレータからその構成を展開すると、APIC でやはり個々のポリシーが作成されます。たとえば、APIC では、ノード、インターフェイス、さらには IP アドレスタイプに対して個別のポリシーが作成されます（そのため、単一の L3Out インターフェイスに IPv4 および IPv6 IP アドレスを提供すると、2 つの個別のインターフェイスプロファイルが作成されます）。

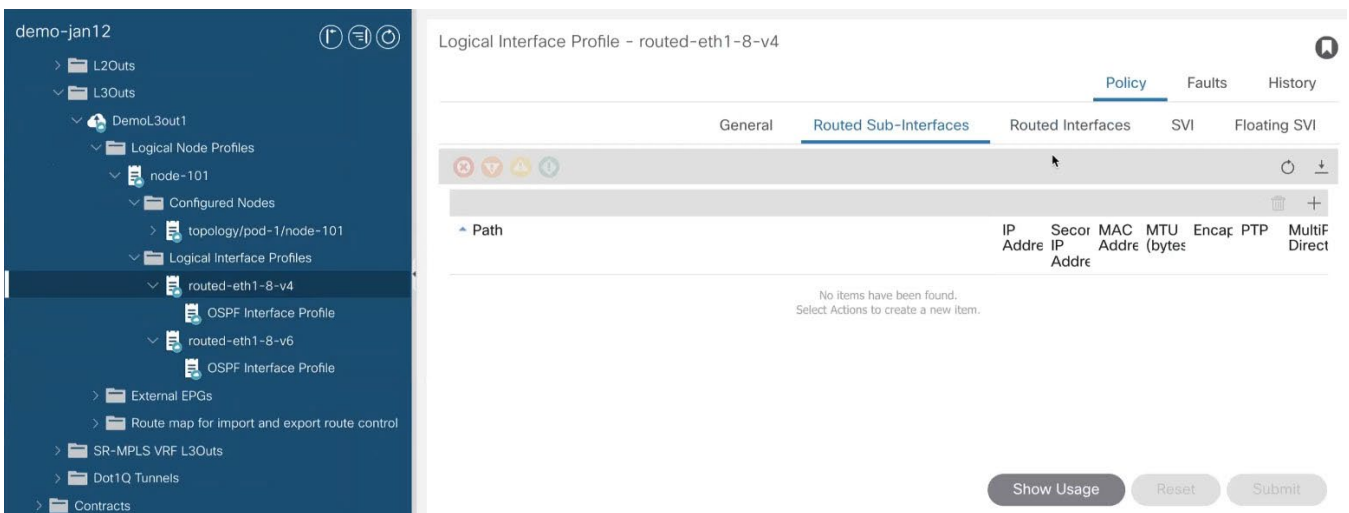


図 1. APIC GUI のルーテッドサブインターフェース



NDO が複数の個別ポリシーを使用してこれらの論理コンテナを維持する方法により、テンプレートの展開中、APIC のポリシーモデルに固有のベストプラクティスも適用されます。そのため、以前の既存の設定を APIC から新しいテンプレートの 1 つにインポートし、構成を編集してから再展開すると、古い MO が削除され、新しい MO が NDO 固有の階層で作成されるシナリオが発生する可能性があります。その場合、短時間（最大 1 秒）のトラフィックの中断を引き起こします。

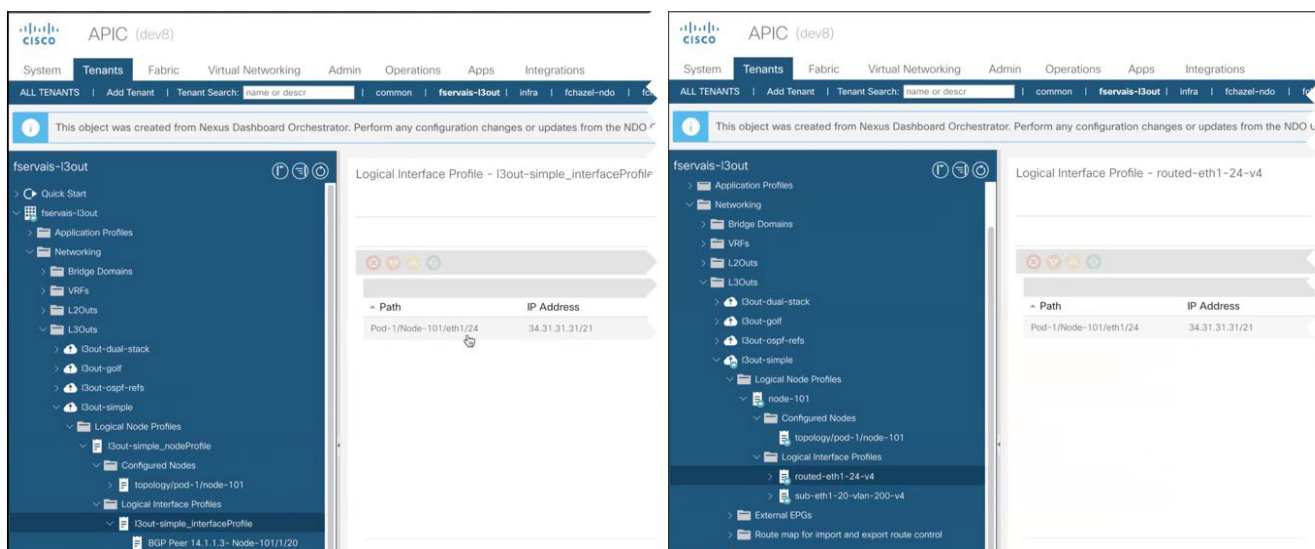


図 2 APIC GUI の管理対象オブジェクト

これは、インポートされたオブジェクトが変更され、再展開された場合にのみ発生します。構成をインポートし、変更せずにすぐに再展開すると、NDO は APIC の MO の所有権を取得するだけで、MO の削除や再作成は行われません。

Cisco Nexus Dashboard Orchestrator リリース 4.4(x) 以降では、ファブリックテンプレートを使用して、リモートリーフファブリックポートで **SyncE** および **MACSec** ポリシーを構成することもできます。

リモートリーフスイッチとその構成の詳細については、「[リモートリーフスイッチを含むファブリックの構成](#)」を参照してください。

ファブリックポリシーを作成

このセクションでは、1 つ以上のファブリック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。ファブリックポリシーテンプレートを使用すると、次のファブリックポリシーを作成および構成できます。

- VLAN Pool
- 物理ドメイン
- L3 ドメイン
- SyncE インターフェイスポリシー
- インターフェイス設定
- ノード設定
- ポッド設定
- MACsec
- NTP ポリシー
- PTP ポリシー
- QoS DSCP ポリシー
- QoS SR-MPLS ポリシー
- QoS クラスポリシー
- MCP グローバルポリシー

ファブリックポリシーテンプレートポリシーを作成するときは、次の点を考慮してください。

- ファブリックポリシーテンプレートをテナントに関連付ける必要はありませんが、展開するには、少なくとも 1 つのファブリックにマップする必要があります。
 - これらのポリシーの構成は、特定のファブリックレベルではなく、テンプレートレベルでのみ可能です。
 - ファブリックポリシーテンプレートを展開解除すると、APIC で関連付けられたポリシーが保持されます。つまり、APIC でのこれらのポリシーの構成は、デフォルト値、またはオーケストレータがそれらの管理を開始する前に APIC で構成された値に戻されません。
1. Cisco Nexus Dashboard にログインし、Cisco Nexus Dashboard Orchestrator サービスを開きます。
 2. 新しいファブリックポリシーテンプレートを作成。
 - a. 左のナビゲーションペインから、**[構成 (Configure)] > [ファブリックポリシー (Fabric Policies)]** を選択します。
 - b. **[ファブリックポリシーテンプレート (Fabric Policy Template)]** ページ内で **[ファブリックポリシーテンプレートを作成 (Create Fabric Policy Template)]** をクリックします。
 - c. **[ファブリックポリシー (Fabric Policies)]** ページの右のプロパティサイドバーにテンプレートの **[名前 (Name)]** を入力します。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 つ以上のファブリック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 つ以上のファブリックに割り当てます。

ファブリック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、ファブリック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)]** ビューで、**[アクション (Actions)]** をクリックし、**[ファブリックの追加/削除 (Add/Remove Fabrics)]** を選択します。

[<template-name> にファブリックを関連付ける (Associate Sites to <template-name>)] ウィンドウが開きます。

- b. **[ファブリックの関連付け (Associate Fabrics)]** ウィンドウで、テンプレートを展開するファブリック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 ファブリックにのみサポートされ、割り当て可能です。

- c. **Ok** をクリックして保存します。

4. VLAN プールを作成。

VLAN プールは、VLAN ID または、物理または VMM ドメインが消費する VLAN カプセル化に使用されている範囲を指定します。

- a. **[+オブジェクトの作成 (+Create Object)]** ドロップダウンから、**[VLAN プール (VLAN Pool)]** 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. **[+VLAN 範囲の追加 (+Add VLAN Range)]** をクリックして範囲を指定し、チェックマークアイコンをクリックして保存します。

- e. 前のサブステップを繰り返して、同じポリシー内に追加の VLAN 範囲を作成します。

- f. この手順を繰り返して、追加の VLAN プールを作成します。

1. 物理ドメインを作成。

物理ドメインプロファイルは、ベアメタルサーバ接続と管理アクセスに使用します。ドメインは VLAN プールに関連付けられるように設定されます。その後、EPG は、ドメインに関連付けられている VLAN を使用するように設定されます。

- a. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから、**[物理ドメイン (Physical Domain)]** を選択します。

- b. 右のプロパティのサイドバーでは、ドメインの **[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. **[VLAN プールポリシーを選択 (Select a VLAN Pool Policy)]** をクリックし、このドメインの VLAN プールの 1 つを選択します。

ステップ 3 の説明に従って、VLAN プールがすでに作成されている必要があります。

- e. この手順を繰り返して、追加の物理ドメインを作成します。

2. L3 ドメインの作成。

L3 ドメインプロファイルは、ポートや VLAN などの物理インフラストラクチャを管理するためのポリシーであり、ACI ファブリックをレイヤ 3 でルーティングされた外部ネットワークに接続するために使用できます。

- a. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから、**[L3 ドメイン (L3 Domain)]** を選択します。

- b. 右のプロパティのサイドバーでは、ドメインの**[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. (オプション) **[VLAN プールポリシーを選択 (Select a VLAN Pool Policy)]** をクリックし、このドメインの VLAN プールの 1 つを選択します。
point-to-point ルーテッドインターフェイスの使用を計画している場合は、VLAN プールは必要ないため、この手順をスキップできます。
ただし、サブインターフェイスまたは SVI を構成する場合は、VLAN プールを追加して、必要な VLAN を提供する必要があります。この場合、ステップ 3 の説明に従って、VLAN プールがすでに作成されている必要があります。

- e. この手順を繰り返して、追加の L3 ドメインを作成します。

3. SyncE インターフェイスポリシーを作成します。

サービスプロバイダーネットワークで、Synchronous Optical Networking (SONET) と同期デジタル階層 (SDH) 機器を段階的に置き換えるイーサネット機器を使用する場合、イーサネットポート経由で高品質なクロック同期を提供するためには周波数を同期化することが必要です。周波数またはタイミング同期は、ネットワーク全体に精密周波数を配布する機能です。同期イーサネット (SyncE) により、物理レベルで必要な同期化が実現します。SyncE を使用するイーサネットリンクは、SONET/SDH と同じ方法で、つまり高品質なストラタム 1 追跡可能クロック信号とビットクロックのタイミングを取ることで同期されます。

ACI ファブリックの SyncE の詳細については、ご使用のリリースの『Cisco APIC システム管理構成ガイド』の「[同期イーサネット \(SyncE\)](#)」の章を参照してください。

- a. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから、**[SyncE インターフェイスポリシー (SyncE 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。

- **[管理状態 (Admin State)]** : ポリシーを有効化または無効化します。

デフォルトは**無効**です。

- **[同期状態メッセージ (Sync State Msg)]** : オフにすると、ESMC パケットの送信が無効化され、受信した ESMC パケットもすべて無視されます。
- **[選択入力 (Selection Input)]** : インターフェイスの周波数送信元の優先順位構成を有効にします。
- **[送信元優先順位 (Src Priority)]** : インターフェイスの周波数送信元の優先順位。この値は、クロック選択アルゴリズムで同じ QL がある 2 つの送信元間から選択するために使用されます。

値は、1 (最高プライオリティ) から 254 (最低プライオリティ) の範囲で設定できます。デフォルト値は 100 です。

選択入力がある場合にのみ構成できます。

- **[復旧待機時間 (Wait To Restore)]** : 分単位の復旧待機時間で、インターフェイスがアップ状態になってから、インターフェイスの周波数同期に使用されるまでの時間です。有効値の範囲は、0 ~ 12 です。デフォルト値は 5 です。

選択入力がある場合にのみ構成できます。

e. この手順を繰り返して、追加の SyncE インターフェイスポリシーを作成します。

4. インターフェイス設定ポリシーを作成します。

このインターフェイスに SyncE または MACsec を構成する場合は、対応する手順の説明に従って、これらのポリシーをすでに作成しておく必要があります。

インターフェイス設定ポリシーを使用すると、1 つ以上のスイッチの 1 つ以上のポートに後で展開できる共通インターフェイス設定のセットを定義して、それら全体で一貫した構成を行うことができます。

- [+オブジェクトを作成 (+Create Object)]** ドロップダウンから、**[インターフェイスの設定 (Interface Settings)]** を選択します。
- 構成しているインターフェイスの **[タイプ (Type)]** 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。
 - **[速度 (Speed)]** : ポートのデータ転送レート。これは、ポートがリンクされている接続先と一致する必要があります。速度は特定のポートのみで変更できます。すべての速度がすべてのシステムで利用できるわけではありません。詳細については、使用しているスイッチのハードウェア設置ガイドを参照してください。
 - **[自動ネゴシエーション (Auto-Negotiation)]** : ポートに対する自動ネゴシエーションを有効にします。

- **[VLAN 範囲 (VLAN Scope)]** : レイヤ 2 インターフェイスの VLAN 範囲。

[グローバル範囲 (Global scope)] : リーフスイッチごとに 1 つの EPG のみにマッピングするように VLAN カプセル化値を設定します。

[ポートローカル範囲 (Port Local scope)] : 入力方向と出力方向の両方で個別の (ポート、VLAN) 変換エントリを割り当てることができます。EPG が単一のブリッジドメインに属している場合、この設定は無効です。

- **[CDP 管理状態 (CDP Admin State)]** : インターフェイスで Cisco Discovery Protocol (CDP) を有効にします。
- **[LLDP]** : インターフェイスのリンク層検出プロトコル (LLDP) を有効にします。
- **[MCP 管理状態 (MCP Admin State)]** : インターフェイスで MisCabling Protocol (MCP) を有効にします。
- **[ドメイン (Domains)]** : このインターフェイスポリシーに関連付ける 1 つ以上のドメインを選択します。

ドメインの指定は必須ではありません。インターフェイスポリシーを作成して、関連付けられたドメインがなくてもファブリックに展開できます。

- **[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。
 - **[SyncE]** : SyncE ポリシーを定義し、それをこのインターフェイス設定ポリシーに割り当てる場合、ドロップダウンから選択します。
 - **[デバウンス間隔 (Debounce Interval)]** : ポートデバウンス時間は、リンクがダウンしたことをスーパーバイザに通知するまでの、インターフェイスの待機時間です。この時間、インターフェイスはリンクがアップ状態に戻ったかどうかを確認するために待機します。
 - **[アップ時遅延 (Bring Up Delay)]** : ポートがアップ状態になったときに、判定フィードバックイコライザ (DFE) の調整を遅延させる時間を、ミリ秒単位で指定します。遅延は、一部のサードパーティ製アダプタを使用する場合に、リンクの起動中に CRC エラーを回避するために使用されます。

遅延は必要な場合にのみ設定してください。通常遅延を設定する必要はありません。

- **[FEC]** : 転送エラー訂正 (FEC) は、送信元 (送信側) がエラー修正コードを使用して冗長な方法でデータをエンコードし、信頼できないチャネルまたはノイズの多いチャネルを介したデータ送信において、宛先 (受信側) がそれを認識して、エラー制御を実現する方法です。再送信を必要とせずにエラーを修正します。
- **[QinQ]** : 通常のインターフェイス、コンピュータ、または vPC 上で入力される二重タグ付き VLAN トラフィックを EPG にマッピングできるようにします。この機能が有効で、二重タグ付きトラフィックが EPG のネットワークに入ると、両方のタグがファブリック内で個別に処理され、ACI スイッチの出力時に二重タグに復元されます。

単一タグおよびタグなしのトラフィックの入力はドロップします。

- **[リフレクティブリレー (Reflective Relay)]** : すべてのトラフィックを外部スイッチに転送します。外部スイッチはポリシーを適用し、必要に応じてサーバ上の宛先またはターゲット VM にトラフィックを送信します。ローカルスイッチングはありません。ブロードキャストまたはマルチキャストトラフィックは、リフレクティブリレーは、各 VM サーバでローカルにパケットのレプリケーションを提供します。

リフレクティブリレーの利点の 1 つは、スイッチング機能および管理機能、Vm をサポートするサーバリソースを解放するための外部スイッチを活用しています。リフレクティブリレーでは、ポリシー、同じサーバ上の Vm の間のトラフィックに適用する Cisco APIC で設定することもできます。

Cisco ACI、入ってきたのと同じポートからオンに戻すにトラフィックを許可する、リフレクティブリレーを有効にできます。レイヤ 2 インターフェイスポリシーとして individual ports (個々のポート、個別ポート)、ポートチャネルまたは仮想ポートチャネルでリフレクティブリレーを有効にすることができます。

デフォルト値は [無効 (Disabled)] です。

- **[LLDP 送信状態 (LLDP Transmit State)]** : インターフェイスから Link Layer Discovery Protocol (LLDP) パケットを送信できるようにします。

LLDP 受信/送信状態フラグは、LLDP がインターフェイスポリシーでグローバルに有効になっている場合にのみ構成できます。

- **[LLDP 受信状態 (LLDP Receive State)]** : インターフェイスで LLDP パケットを受信できるようにします。
- **[BPDU フィルタ (BPDU Filter)]** : ブリッジプロトコルデータユニット (BPDU) フィルタは、ポート上のすべての BPDU をフィルタリングします。

BPDU フィルタは、インバウンド BPDU とアウトバウンド BPDU の両方を阻止します。受信した BPDU はドロップされ、BPDU は送信されません。

- **[BPDU ガード (BPDU Guard)]** : BPDU ガードは、ポートが BPDU を受信するのを防ぎます。ポートで BPDU を受信すると、ポートは **errdisable** モードになります。
- **[LLFC 送信状態 (LLFC Transmit State)]** : リンクレベルフロー制御 (LLFC) パケットをインターフェイスから送信できるようにします。
- **[LLFC 受信状態 (LLFC Receive State)]** : インターフェイスが LLFC パケットを受信できるようにします。
- **[アクセス MACsec ポリシー (Access MACsec Policy)]** : アクセス MACsec ポリシーを定義し、それをこのインターフェイス設定ポリシーに割り当てる場合は、ドロップダウンから選択します。

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

5. ノード設定ポリシーを作成します。

ノード設定ポリシーを使用すると、共通のノード設定のセットを定義できます。これを後で 1 つまたは複数のスイッチに展開して、それら全体で一貫した構成を実現できます。

このリリースでは、ノード設定ポリシーは、SyncE および PTP 機能の有効化をサポートしています。

- a. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから、**[ノードの設定 (Node Settings)]** 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. **SyncE** 構成をノードに展開する場合は、SyncE を有効にして設定を指定します。

SyncE の詳細については、ご使用のリリースの『Cisco APIC システム管理構成ガイド』の「[同期イーサネット \(SyncE\)](#)」の章を参照してください。

- **[管理状態 (Admin State)]** : ポリシーを有効化または無効化します。
 - **[品質レベルオプション (Quality Level Option)]** - クロックの正確度を指定します。この情報は、ESMC に運ばれている SSM を使用してネットワークに渡って送信されシステム内のデバイスが同期できる最適な利用可能な送信元を決定するために使用されます。
- e. **PTP** 構成をノードに展開する場合は、PTP を有効にして設定を指定します。

PTP の詳細については、ご使用にリリースの「[Cisco APIC システム管理構成ガイド](#)」の「正確な時間プロトコル」章を参照します。

- f. このステップを繰り返して、追加のノード設定ポリシーを作成します。

6. ポッド設定ポリシーを作成します。

ポッド設定ポリシーを作成する前に、対応する手順で説明されているように、そのポリシー用に NTP ポリシーを作成しておく必要があります。

ポッド全体の MACsec ポリシーを構成する場合は、対応する手順の説明に従って、MACsec ポリシーを作成しておく必要があります。

Pod 設定ポリシーを使用すると、共通のポッド設定のセットを定義できます。これを後でファブリック内の 1 つ以上のポッドに展開して、それら全体で一貫した構成を実現できます。

- a. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから、**[ポッドの設定 (Pod Settings)]** 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. **[NTP ポリシーの選択 (Select a NTP Policy)]** をクリックして、NTP ポリシーを選択します。

e. **[ファブリック MACsec ポリシー (Fabric MACsec Policy)]** ドロップダウンから、MACsec ポリシーを選択します。

f. このステップを繰り返して、追加のポッド設定ポリシーを作成します。

7. MACsec ポリシーを作成します。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement (MKA) プロトコルでは、必要なセッションキーを提供し、必要な暗号化キーを管理します。

ACI ファブリックの MACsec の詳細については、ご使用のリリースの [「Cisco APIC システム管理構成ガイド」](#) の「MACsec」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、**[MACsec]** 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。

- **[タイプ (Type)]** : このポリシーが適用されるインターフェイスのタイプを定義します。

スパインスイッチ上のすべてのリンクは、ファブリックリンクと見なされます。ただし、スパインスイッチリンクを IPN 接続のために使用している場合、そのリンクはアクセスリンクとして扱われます。これらのリンクで MACsec を展開するには、MACsec アクセスポリシーを使用する必要があります。

- **[管理状態 (Admin State)]** : ポリシーを有効化または無効化します。

- **[暗号スイート (Cipher Suite)]** : 暗号スイート AES 128 または拡張パケットナンバリング (XPN) のない AES 256 を選択する場合は、セキュリティ関連キー (SAK) の有効期限を明示的に指定する必要があります SAK の有効期限値をデフォルト (「無効」) のままにすると、インターフェイスがランダムにアウトオブサービスになる可能性があります。

- **[ウィンドウサイズ (Window Size)]** : フレームの順序が変更されるプロバイダネットワーク上で MACsec の使用をサポートするには、リプレイウィンドウが必要です。ウィンドウ内のフレームは順不同で受信できますが、リプレイ保護されません。デフォルトのウィンドウサイズは 64 です。Cisco APIC GUI または CLI を使用する場合、リプレイウィンドウのサイズは、0 ~ 232-1 の範囲で設定できます。XPN 暗号スイートの場合、最大リプレイウィンドウサイズは 230-1 です。これより大きなウィンドウサイズを構成しても、ウィンドウサイズは 230-1 に制限されます。暗号スイートを非 XPN 暗号スイートに変更した場合、制限はなく、設定されたウィンドウサイズが使用されます。

- **セキュリティポリシー** : APIC MACsec では、2 つのセキュリティモードをサポートしています。MACsec **セキュリティで保護する必要がある** 中に、リンクの暗号化されたトラフィックのみを許可する **セキュリティで保護する必要がある** により、両方のクリアし、リンク上のトラフィックを暗号化します。たとえば、ポートをオンにできますで MACsec **セキュリティで保護する必要がある** モードがピアがしているリンクでのキーチェーンを受信する前にします。MACsec を導入することが推奨されて、この問題に対処する **[セキュリティ**

ィで保護する必要がある (Should-Secure)] モードで展開し、リンクがアップしたら [セキュリティ保護が必須 (Must-Secure)] にセキュリティモードに変更することをお勧めします。



セキュリティで保護する必要があるモードで MACsec を展開する前にキーチェーンは、影響を受けるインターフェイスに導入する必要があります、またはインターフェイスがダウンします。

- **[SAK 失効時間 (SAK Expiry Time)]** : 暗号スイート AES 128 または拡張パケットナンバリング (XPN) のない AES 256 を選択する場合は、セキュリティ関連キー (SAK) の有効期限を明示的に指定する必要があります。SAK の有効期限値をデフォルトのままにすると、インターフェイスがランダムにアウトオブサービスになる可能性があります。
- **[キー名 (Key Name)]** : MACsec キーを作成できます。APIC はまたは責任を負う MACsec キーチェーンディストリビューションのポッド内のすべてのノードに特定のポートのノードになります。
 - **[+MACsec キーの追加 (+Add MACsec Key)]** をクリックします。
 - **[キー名 (Key Name)]** を入力します。
 - **[PSK] フィールド**に事前共有キーを指定します。
 - **[開始時間 (Start Time)]** フィールドで、キーが有効になる日付を入力します。
 - **[終了時間 (End Time)]** フィールドで、キーの有効期限が切れる日付を入力します。
 - **[OK]** をクリックして保存します。
 - 提供する追加のキーについて、この手順を繰り返します。

e. 追加の MACsec 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。

8. NTP 設定ポリシーを作成します。

ACI ファブリックにおいて、時刻の同期は、モニタリング、運用、トラブルシューティングなどの多数のタスクが依存している重要な機能です。クロック同期は、トラフィックフローの適切な分析にとって重要であり、複数のファブリックノード間でデバッグとフォールトのタイムスタンプを関連付けるためにも重要です。

ACI ファブリックの NTP の詳細については、ご使用のリリースの「Cisco APIC 基本構成ガイド」の [「コア ACI Cisco ファブリックサービスのプロビジョニング」](#) の章を参照してください。

- a. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから、**[NTP の設定 (NTP Settings)]** 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。
 - **[+ キーの追加 (+Add Key)]** をクリックして、NTP クライアント認証キーを提供します。

- **[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。

- **[管理状態 (Admin State)]** : NTP ポリシーを有効化または無効化します。
- **[サーバー状態 (Server State)]** : ACI リーフスイッチを NTP サーバーとして動作し、下流のクライアントに NTP 情報を提供できるようにします。

有効にすると、ダウンストリームクライアントは、接続先のリーフスイッチのインバンド/アウトオブバンド管理 IP アドレスを NTP サーバーとして使用できます。

- **[マスターモード (Master Mode)]** : これにより、指定された NTP サーバが、下流のクライアントに対し、他からの調整を受けていないローカルクロック時刻を、構成されたストラタム番号とともに提供することが可能になります。たとえば、NTP サーバとして動作しているリーフスイッチは、クライアントとして動作しているリーフスイッチに対し、調整されていないローカルクロック時刻を提供できます。これが適用できるのは、サーバーのクロックが調整されていない場合のみです。
- **[ストラタム (Stratum)]** : NTP クライアントが同期した時刻を取得するときのストラタム番号を指定します。

[サーバー状態 (Server State)] オプションが有効になっていて、ACI リーフスイッチに接続されているクライアントが、スイッチの管理 IP アドレスを NTP サーバーとして使用するように構成されている場合、クライアントはストラタムに 1 を加えた値で NTP 情報を受信します。

指定できる範囲は 1 ~ 14 です。

- **[認証状態 (Authentication State)]** : 証明書ベースの認証を有効にします。

このオプションを有効にする場合は、上記の **[+ キーを追加 (+Add Key)]** オプションを使用してキーを指定する必要があります。

- NTP サーバー情報を指定するために **[+ プロバイダーを追加 (+Add Provider)]** をクリックします。

表示される **[プロバイダの追加 (Add Provider)]** ウィンドウで、サーバーの **[ホスト名/IP アドレス (Host name / IP Address)]**、**[管理 EPG (Management EPG)]** の名前、および **[管理 EPG タイプ (Management EPG Type)]** を指定する必要があります。



選択した特定のタイプの管理 EPG は、このテンプレートが関連付けられているファブリックの APIC ですでに構成されている必要があります。

複数のプロバイダーを作成する場合は、最も信頼できる NTP 時刻源の **[優先]** オプションをオンにします。

- e. このステップを繰り返して、追加の NTP 設定ポリシーを作成します。

9. PTP 設定ポリシーを作成します。

高精度時間プロトコル (PTP) はネットワークに分散したノードの時刻同期プロトコルです。PTP を使用すると、イーサネットネットワークを介して 1 マイクロ秒未満の精度で、分散したクロックを同期できます。PTP の正確さは、ACI ファブリックスパインおよびリーフスイッチでの PTP のハードウェアサポートによるものです。

ACI ファブリックの PTP の詳細については、ご使用にリリースの『*Cisco APIC システム管理構成ガイド*』の「高精度時間プロトコル」の章を参照します。

- a. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから、**[PTP の設定 (PTP Settings)]** 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)]** : ポリシーを有効化または無効化します。
- **[グローバル優先度 1 (Global Priority 1)]** : このクロックをアドバタイズするときに使用される値を指定します。優先順位 1 はベストプライマリクロック選択のためにデフォルトの条件 (例えば、クロック品質とクロッククラス) をオーバーライドします。

有効な値は 0 ~ 255 です。デフォルト値は 128 です。低い値が優先されます。

- **[グローバル優先度 2 (Global Priority 2)]** : このクロックをアドバタイズするときに使用される値を指定します。優先度 2 は、デフォルト条件で同等になる 2 台のデバイスのうち、どちらを優先するかを決めるために使用されます。

有効な値の範囲は 0 ~ 255 です。デフォルト値は 128 です。低い値が優先されます。

- **[グローバルドメイン (Global Domain)]** : PTP ドメイン番号を指定します。Cisco ACI では複数の PTP ドメインはサポートされていませんが、使用中のドメイン番号を変更することはできます。すべてのリーフスイッチとスパインスイッチで同じ値が使用されます。

有効な値は 0 ~ 128 です。デフォルトは 0 です。

- **[ファブリックプロファイルテンプレート (Fabric Profile Template)]** : 以下の間隔設定のデフォルト値を定義する PTP プロファイルを指定します。プロファイルは、PTP のさまざまなユースケースに最適化されたさまざまなパラメータを定義するために使用されます。これらのパラメータの一部には、PTP メッセージ間隔の適切な範囲と PTP トランスポートプロトコルが含まれますが、これらに限定されません。PTP プロファイルは、さまざまな業界の多くの組織/標準規格によって定義されています。
- **AES67-2015** : AES67-2015。これは、オーディオオーバーイーサネットおよびオーディオオーバー IP の相互運用性の標準です。

- **[デフォルト (Default)]** : IEEE 1588-2008。これは、クロック同期のデフォルトの PTP プロファイルです。
- **SMPTE-2059-2** : SMPTE ST2059-2015、これはビデオオーバー IP の標準です。
- **Telecom-8275-1** : ITU-T G.8275.1。これは、完全なタイミングサポートを備えた電気通信の標準的な推奨事項です。

フルタイミングサポートは、すべてのホップで PTP G.8275.1 プロファイルをデバイスに提供できる電気通信ネットワークを表すために ITU によって定義された用語です。ACI でサポートされていない G.8275.2 は、パスに PTP をサポートしないデバイスが含まれる可能性がある部分的なタイミングサポート用です。

- **[ファブリックアナウンス間隔 (Fabric Announce Interval)]** : プライマリポートがアナウンスメッセージを送信するための秒単位の平均間隔を対数で指定します (対数の底は 2)。範囲は、選択したプロファイルによって異なります。
- **[ファブリック同期間隔 (Fabric Sync Interval)]** : プライマリポートが同期メッセージを送信するための秒単位の平均間隔を対数で指定します (対数の底は 2)。範囲とデフォルトは、選択した PTP プロファイルによって異なります。
- **[ファブリック遅延間隔 (Fabric Delay Interval)]** : スレーブポートが遅延要求メッセージを送信するための秒単位の平均間隔を対数で指定します (対数の底は 2)。範囲は、選択した PTP プロファイルによって異なります。
- **[ファブリックアナウンスタイムアウト (Fabric Announce Timeout)]** : PTP アナウンスメッセージが期限切れと見なされる前にシステムが待機するアナウンスメッセージの数を指定します。範囲とデフォルトは、選択した PTP プロファイルによって異なります。
- **[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。ここで追加されたプロファイルは、上で選択したプロファイルとどのように異なるのでしょうか？
 1. **[+プロファイルの追加 (+Add Profile)]** をクリックして PTP プロファイルを追加します。プロファイルは、PTP のさまざまなユースケースに最適化されたさまざまなパラメータを定義するために使用されます。これらのパラメータの一部には、PTP メッセージ間隔の適切な範囲と PTP トランスポートプロトコルが含まれますが、これらに限定されません。PTP プロファイルは、さまざまな業界の多くの組織/標準規格によって定義されています。
 2. **[プロファイルの追加 (Add Profile)]** ダイアログ内に **[名前 (Name)]** を入力します。
 3. **[プロファイルテンプレート (Profile Template)]** ドロップダウンから、使用可能なプロファイルの 1 つを選択します。

プロファイルの詳細については、[「Cisco APIC システム管理構成ガイド」](#)を参照してください。

- 4. 特定のユースケースの必要に応じて、デフォルトのプロファイル値を更新します。

e. このステップを繰り返して、追加の PTP 設定ポリシーを作成します。

10. QoS DSCP ポリシーを作成します。

このポリシーは、IPN ユースケース全体での包括的な QoS 保持の一部です。このセクションの情報は参照情報として使用できますが、「[IPM 全体での QoS の保持](#)」の章に記載されている手順をすべて実行することをお勧めします。

- a. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから **QoS DSCP** 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)]** : ポリシーを有効化または無効化します。
- **[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。

各 ACI QoS レベルの DSCP 値を選択します。各ドロップダウンには、使用可能な DSCP 値のデフォルトリストが含まれています。レベルごとに一意の DSCP 値を選択する必要があります。

- e. 追加の QoS DSCP 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。

通常、マルチファブリックドメインの一部であるすべてのファブリックにこのポリシーを一貫して適用することをお勧めします。

11. QoS SR-MPLS ポリシーの作成

このポリシーは、包括的な SR-MPLS 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「[マルチファブリックおよび SR-MPLS L3Out ハンドアウト](#)」の項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. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから **QoS SR-MPLS** を作成します。
- 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. 入力 QoS 変換ルールを追加するには、**[+入力ルールの追加 (+Add Ingress Rule)]** をクリックします。

これらのルールは MPLS ネットワークから ACI ボーダーリーフスイッチへ入力しているトラフィックに適用されます。そして、着信パケットの EXP ビット (EXP) の ACI QoS レベルへのマップに使用されます。それとともに Differentiated Services Code Point (DSCP) またはオリジナルトラフィックの CoS 値の設定に使用されます。指定された CoS 値が ACI リーフ

ノードを出るトラフィックに使用されるようにするには、「QoS クラスポリシー」の一部として CoS 保持機能も構成する必要があります。

カスタムポリシーが定義されていないか、一致していない場合、デフォルトの QoS レベル (Level 3) が割り当てられます。

- i. **[EXP 照合開始 (Match Exp From)]** と **[EXP 照合終了 (Match EXP To)]** フィールドで、照合する入力 MPLS パケットの EXP 範囲を指定します。
- ii. **[キューの優先順位 (Queuing Priority)]** ドロップダウンから、マッピングする ACI QoS レベルを選択します。

これは、ACI ファブリック内のトラフィックに割り当てる QoS レベルで、ACI はファブリック内のトラフィックのプライオリティを決めるために使用します。オプションの範囲は **レベル 1 ~ レベル 6** です。デフォルト値は、**レベル 3** です。このフィールドで選択しない場合、トラフィックには自動的に **レベル 3** の優先順位が割り当てられます。

- iii. **[DSCP の設定 (Set DSCP)]** ドロップダウンから、接続先 ACI リーフスイッチから送信されるときにトラフィックに割り当てる DSCP 値を選択します。

指定された DSCP 値は、外部ネットワークから受信した元のトラフィックに設定されるため、トラフィックが宛先 ACI リーフノードで VXLAN カプセル化解除された場合にのみ再公開されます。

値を **[未指定 (Unspecified)]** に設定すると、パケットの元の DSCP 値が保持されます。

- iv. **[CoS の設定 (Set CoS)]** ドロップダウンから、接続先 ACI リーフスイッチから送信されるときにトラフィックに割り当てる CoS 値を選択します。

指定された CoS 値は、接続先 ACI リーフスイッチを出るトラフィックに設定されます。これには、CoS 保存を有効にする必要があります。

値を **[未指定 (Unspecified)]** に設定すると、パケットの元の CoS 値が保持されますが、これはファブリックで CoS 保存オプションが有効になっている場合のみです。CoS 保存の詳細については、[「Cisco APIC and QoS」](#) を参照してください。

- v. チェックマークアイコンをクリックして、ルールを保存します。
- vi. 追加の入力 QoS ポリシールールについて、これらの手順を繰り返します。

- e. 出力 QoS 変換ルールを追加するには、**[出力ルールの追加 (Add Egress Add Rule)]** をクリックします。

これらのルールは、MPLS L3Out を介して ACI ファブリックを離れるトラフィックのボーダリーフスイッチに適用され、パケットの DSCP 値を照合するために使用され、一致が見つかった場合は、次の構成されたポリシーに基づいて MPLS EXP および CoS 値を設定します。

カスタムポリシーが定義されていないか、一致していない場合、デフォルトの EXP 値 **0** がすべてのラベルでマークされます。EXP 値は、デフォルトポリシーシナリオとカスタムポリシーシナリオの両方でマークされ、パケット内のすべての MPLS ラベルで行われます。

カスタム MPLS 出力ポリシーは、既存の EPG、L3Out、および契約 QoS ポリシーをオーバーライドできます。

- i. **[DSCP 照合開始 (Match DSCP From)]** と **[DSCP 照合終了 (Match DSCP To)]** ドロップダウンを使用して、出力 MPLS パケットの優先順位を割り当てるために照合する DSCP 範囲を指定します。
 - ii. **[MPLS EXP の設定 (SET MPLS EXP)]** ドロップダウンから、出力 MPLS パケットに割り当てる EXP 値を選択します。
 - iii. **[CoS の設定 (Set CoS)]** ドロップダウンから、出力 MPLS パケットに割り当てる CoS 値を選択します。
 - iv. チェックマークアイコンをクリックして、ルールを保存します。
 - v. 追加の出力 QoS ポリシールールについて、この手順を繰り返します。
 - f. 追加の QoS SR-MPLS 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。
12. QoS クラスポリシーポリシーを作成します。

Cisco ACI には、ユーザーが構成可能な QoS レベルがいくつか用意されています。Cisco APIC リリース 4.0(1) 以降では、6 つのユーザ構成可能な QoS レベルがサポートされていますが、以前のリリースでは 3 がサポートされています。この手順では、Cisco Nexus Dashboard Orchestrator を使用して、これらの各レベルの特定の設定を構成する方法について説明します。

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。

これらのポリシーの最も一般的な使用例は、ACI ファブリックに着信するトラフィックの CoS 保存を有効にすることです。

- a. **[+オブジェクトの作成 (+Create Object)]** ドロップダウンから、**[QoS クラスポリシー (QoS Class Policies)]** 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. 必要に応じて、**[CoS の保持 (Preserve CoS)]** を有効にします。

トラフィックが ACI ファブリックに入ると、構成された QoS ポリシーに基づいて、各パケットを ACI QoS レベルにマッピングできます。これらの QoS レベルは、パケットの外部ヘッダーの CoS フィールドと DE ビットに格納され、元のヘッダーは破棄されます。入力パケットの元の CoS 値を保持し、パケットリーフがファブリックに切り替えるときにそれを復元する場合は、802.1p サービスクラス (CoS) の保持をこの設定を利用することで有効にすることができます。

- e. **[+レベルの追加 (+Add Level)]** をクリックして、特定の QoS クラスの構成の詳細を定義します。

[QoS レベル構成を追加 (Add QoS Level Configuration)] ウィンドウが開きます。

f. **[QoS レベル設定の追加 (Add QoS Level Configuration)]** ウィンドウで、構成する QoS レベルを選択し、構成の詳細を指定します。

- **[MTU]** : この QoS クラスのパケットに使用される最大伝送単位。
- **[最小バッファ]** : 予約済みバッファの最小数。指定できる数値は 0 ~ 3 です。

デフォルト値は 0 です。

- **[輻輳アルゴリズム (Congestion Algorithm)]** : この QoS レベルで使用される輻輳アルゴリズム。
- **[スケジューリングアルゴリズム (Scheduling Algorithm)]** : この QoS レベルで使用されるスケジューリングアルゴリズム。
- **[割り当てられた帯域幅 (Bandwidth Allocated)]** : この QoS レベルに割り当てられた合計帯域幅の割合。値は 0 ~ 100 です。

デフォルト値は 20 です。

- **[PFC 管理状態 (PFC Admin State)]** : FCoE トラフィックに適用されるプライオリティフロー制御ポリシーの管理状態。
- **[管理状態 (Admin State)]** : ポリシーを有効化または無効化します。
- **[ドロップ Cos 無し (No Drop Cos)]** : FCoE トラフィックの輻輳の場合でも FCoE パケット処理をドロップしない CoS レベル。
- **[PFC 範囲 (PFC Scope)]** : 優先フロー制御 (PFC) の範囲。ファブリック全体の**ファブリック全体の PFC**、またはスパインスイッチのみの **IntraTor PFC**。

g. 追加の QoS クラス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。

13. MCP グローバルポリシーを作成します。

誤配線プロトコル (MCP) は、Link Layer Discovery Protocol (LLDP) 、スパニングツリープロトコル (STP) が検出できない設定不備を処理するために設計されています。MCP は、レイヤ 2 パケットを使用して、外部インフラストラクチャでループを形成するポートを検出して無効にします。MCP パケットを使用して、リーフスイッチに関連するループを検出し、それが発生したときにファブリックで障害とイベントを発生させることができます。MCP は、グローバルに、またはインターフェイスごとに有効にできます。デフォルトでは、MCP はグローバルに無効になっており、各ポートで有効になっていますが、MCP が機能するにはグローバルに有効にする必要があります。



MCP グローバルポリシーを構成して 1 つ以上のファブリックに展開し、テンプレートを展開解除すると、ポリシーはファブリックに残ります。

a. **[+オブジェクトの作成 (+Create Object)]** ドロップダウンから、**[MCP グローバルポリシー (MCP Global Policy)]** を選択します。

作成できる MCP グローバルポリシーは 1 つだけです。

- 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. ポリシーを有効にするには、**[管理状態 (Admin State)]** を有効にします。
- e. **VLAN ごとに MCP PDU** を有効にする

これは、MCP が EPG 単位でパケットを送信できるようにします。このオプションが無効になっている場合、パケットはタグなしの EPG でのみ送信され、ネイティブ VLAN でのみループを検出できます。

- f. **[管理状態 (Admin State)]** を有効にしている場合は、ファブリック内の MCP パケットを一意に識別するための **[キー (Key)]** を提供します。
- g. 必要に応じて、**ループ検出倍率**の値を更新します。

これは、ループ保護アクションが起きる前に ACI ファブリックに届く MCP パケットの数を指定します。

- h. (オプション) 追加の MCP 設定を変更します。

- **[初期遅延時間 (Initial Delay Time)]** : MCP がアクションを開始するまでの時間。システムの開始から初期遅延タイマーのタイムアウトまで、MCP はループが検出された場合にのみ syslog エントリを作成します。
- **[送信周波数 (Transmission Frequency)]** : MCP パケットの送信周波数。

- 14. 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。

- 15. **[展開 (Deploy)]** をクリックして、ファブリックを関連付けるためテンプレートを再展開します。

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。

そうでなかった場合、**[ファブリックに展開 (Deploy to fabrics)]** ウィンドウには、ファブリック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、構成の違いのみがファブリック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。

ファブリック技術情報ポリシーを作成

始める前に：

- ほとんどのファブリック技術情報ポリシーには 1 つ以上のファブリックポリシーが必要なため、「[ファブリックポリシーの作成](#)」で説明されているように、それらのファブリックポリシーがすでに定義されている必要があります。

たとえば、インターフェイスポリシー（物理、ポートチャネル、または仮想ポートチャネル）を作成する場合は、インターフェイス設定ポリシーがすでに作成されている必要があります。

- ファブリック技術情報ポリシーに必要なファブリックポリシーを含むテンプレートは、ファブリック技術情報ポリシーテンプレートの前に展開する必要があります。
- ファブリック技術情報ポリシーテンプレートは、テナントに関連付ける必要はありませんが、展開するには、少なくとも 1 つのファブリックにマッピングする必要があります。

この場合、関連するポリシーの構成を、ファブリックレベルではなく常にグローバルテンプレートレベルでプロビジョニングすることもお勧めします。

このセクションでは、1 つ以上のファブリック技術情報テンプレートを作成する方法について説明します。ファブリック技術情報テンプレートを使用すると、次のものを作成および構成できます。

- 物理インターフェイス
- ポートチャネルインターフェイス
- 仮想ポートインターフェイス
- ノードプロファイル
- ポッドプロファイル
- FEX デバイス



[インターフェイス構成 (Interface Configuration)] で作成された物理インターフェイス、ポートチャネル (PC)、および仮想ポートチャネル (VPC) ポリシーでのファブリックリソーステンプレートのポリシーのインポートはサポートされていません。この制限は、FEX およびノード構成にも適用されます。手動で設定されたポリシーのみをインポートできます。

ファブリックリソースポリシーを作成するには：

1. **[オーケストレーション (Orchestration)]** ページに移動します。

[管理 (Manage)] > [オーケストレーション (Orchestration)]

2. 新しいファブリック技術情報ポリシーテンプレートを作成します。

- a. **[ファブリックテンプレート (Fabric Templates)] > [ファブリックリソースポリシー (Fabric Resources Policies)]** を選択します。

b. **[ファブリックリソーステンプレートの作成 (Create Fabric Resource Template)]** をクリックします。

c. **[リソースポリシー (Resource 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。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 つ以上のファブリック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 つ以上のファブリックに割り当てます。

ファブリック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、ファブリック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)]** ビューで、**[アクション (Actions)]** をクリックし、**[ファブリックの追加/削除 (Add/Remove Fabrics)]** を選択します。

[<template-name> にファブリックを関連付ける (Associate Sites to <template-name>)] ページが開きます。

b. **[ファブリックの関連付け (Associate Fabrics)]** ページで、テンプレートを展開するファブリック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 ファブリックにのみサポートされ、割り当て可能です。

c. **Ok** をクリックして保存します。

4. 物理インターフェイスポリシーを作成します。

物理インターフェイスポリシーを作成する前に、「[ファブリックポリシーの作成](#)」で説明されているように、インターフェイス設定 (**物理**) ポリシーを作成しておく必要があります。

a. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから、**[物理インターフェイス (Physical Interface)]** を選択します。

b. (オプション) **[説明の追加 (Add Description)]** フィールド：ポリシーの簡単な説明を入力します。

c. 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。

d. **[ノード (Nodes)]** フィールドで、この物理インターフェイスポリシーが展開される 1 つ以上のノード識別子を指定します。

ノードポリシーの構成は、テンプレートのファブリックローカルビューでも実行できます。その場合、ファブリックレベルの構成は、グローバルテンプレートレベルの構成を上書きします。前述のように、異なるテンプレートが作成され、マルチファブリックドメインの一部である各ファブリックに関連付けられる特定のシナリオでは、グローバルテンプレートレベルでのみノードポリシーを構成することをお勧めします。

たとえば、101、102 と 103 です。

- e. **【インターフェース (Interfaces)】** フィールドに、ポリシーが展開されるインターフェース名を指定します。

たとえば、1/1、1/2-4 と 1/5 です。

- f. インターフェイスが**【物理 (Physical)】** インターフェイスか**【ブレイクアウト (Breakout)】** インターフェイスかを選択します。

- g. **【物理 (Physical)】** インターフェイスを構成する場合は、**【物理ポリシーの選択 (Select Physical Policy)】** をクリックして、このために作成したインターフェイス設定ポリシーを選択します。

インターフェイス設定ポリシーで定義されたインターフェイス設定は、前のサブステップで指定したノード (101、102 と 103) 上のインターフェイス (1/1、1/2-4、1/5) に適用されます。

- h. **ブレイクアウト** インターフェイスを構成している場合は、**ブレイクアウトモード**を選択します。

このリリースでは、4x10G、4x25G、および 4x100G モードがサポートされています。

- i. この手順を繰り返して、追加の物理インターフェイスポリシーを作成します。

たとえば、各ノードで一意的な物理インターフェイスのセットを構成する必要がある場合など、別のポリシーが必要になる可能性があります。その場合、特定のノードごとに一意的な物理インターフェイスポリシーを定義します。

The screenshot shows the configuration page for a physical interface policy in the Cisco Nexus Dashboard Orchestrator. The page is titled "phy_intf_1" and is part of the "fabric_resr" configuration. The "General Settings" section includes a "Display Name" field set to "phy_intf_1". The "Interface Policy Properties" section includes a "Nodes" field set to "101", an "Interfaces" field set to "1/1-5", and a "Type" dropdown menu set to "Physical". The "Policy" dropdown menu is set to "phy_policy". The "Advanced Settings" section includes a table for "Interface Description" with columns for "Node", "Interface", and "Description". The table has one row with "101", "1/10", and "ESX 110". There is a "+ Add Interface Description" link below the table. The page has a sidebar with "Overview", "Operate", "Configure", and "Admin" tabs. The "Configure" tab is selected. The page also has a search bar and a user profile icon in the top right corner.

Node	Interface	Description
101	1/10	ESX 110



リモートリーフファブリックポートの物理インターフェイスを作成する場合、この物理インターフェイスポリシーを、 **SyncE** および **MACSec** ポリシーを含むインターフェイス設定に関連付けることができます。

5. ポートチャンネルインターフェイスポリシーを作成します。

ポートチャンネルインターフェイスポリシーを作成する前に、「[ファブリックポリシーの作成](#)」で説明されているように、インターフェイス設定 (**PC/VPC**) ポリシーを作成しておく必要があります。

- a. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから、**[ポートチャンネル (Port Channel Interface)]** 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. **[ノード (Node)]** フィールドで、この物理インターフェイスポリシーが展開されるスイッチのノード識別子を指定します。

ノードポリシーの構成は、テンプレートのファブリックローカルビューでも実行できます。その場合、ファブリックレベルの構成は、グローバルテンプレートレベルの構成を上書きします。前述のように、異なるテンプレートが作成され、マルチファブリックドメインの一部である各ファブリックに関連付けられる特定のシナリオでは、グローバルテンプレートレベルでのみノードポリシーを構成することをお勧めします。

たとえば、**104**。

- e. ポートチャンネルの一部である使用可能なファブリックポートまたはアクセスポートのリストから**インターフェイス**を選択します。

たとえば、**1/6** と **1/7** です。

注：

- f. **[選択した PC/VPC ポリシーはない (No selected PC/VPC Policy)]** をクリックし、作成したインターフェイス設定ポリシーを選択します。

インターフェイス設定ポリシーで定義されたポートチャンネル設定は、前のサブステップで指定したノード (**104**) 上のインターフェイス (**1/6**、**1/7**) に適用されます。

- g. この手順を繰り返して、追加のポートチャンネルインターフェイスポリシーを作成します。

たとえば、各ノードでポートチャンネルインターフェイスの一意のセットを設定する必要がある場合など、別のポリシーが必要になることがあります。その場合、特定のノードごとに一意のポートチャンネルインターフェイスポリシーを定義します。

6. 仮想ポートチャンネルインターフェイスポリシーを作成します。

仮想ポートチャネルインターフェイスポリシーを作成する前に、「[ファブリックポリシーの作成](#)」で説明されているように、インターフェイス設定 (PC/VPC) ポリシーを作成しておく必要があります。

- a. **[+オブジェクトを作成 (+Create Object)]** ドロップダウンから、**[仮想ポートチャネル (Virtual Port Channel Interface)]** 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. **[ノード 1 (Node 1)]** フィールドに、仮想ポートチャネルの一部であるインターフェイスを含む最初のスイッチのノード識別子を指定します。

たとえば、**105**。

- e. **[ノード 1 のインターフェイス (Interfaces on Node 1)]** フィールドで、最初のスイッチのインターフェイスを指定します。

たとえば、**1/8 と 1/9** です。

- f. **[ノード 2 (Node 2)]** フィールドに、仮想ポートチャネルの一部であるインターフェイスを含む 2 番目のスイッチのノード識別子を指定します。

ノードポリシーの構成は、テンプレートのファブリックローカルビューでも実行できます。その場合、ファブリックレベルの構成は、グローバルテンプレートレベルの構成を上書きします。前述のように、異なるテンプレートが作成され、マルチファブリックドメインの一部である各ファブリックに関連付けられる特定のシナリオでは、グローバルテンプレートレベルでのみノードポリシーを構成することをお勧めします。

たとえば、**106**。

- g. **[ノード 2 のインターフェイス (Interfaces on Node 2)]** フィールドで、2 番目のスイッチのインターフェイスを指定します。

たとえば、**1/8 と 1/9** です。

- h. **[選択した PC/VPC ポリシーはない (No selected PC/VPC Policy)]** をクリックし、作成したインターフェイス設定ポリシーを選択します。

インターフェイス設定ポリシーで定義されたポートチャネル設定は、前のサブステップで指定したノード上のインターフェイスに適用されます。

- i. この手順を繰り返して、追加の仮想ポートチャネルインターフェイスポリシーを作成します。

7. ノードプロファイルポリシーを作成します。

ノードプロファイルポリシーを作成する前に、「[ファブリックポリシーの作成](#)」で説明されているように、ノード設定ポリシーを作成しておく必要があります。

このリリースでは、ノード設定ポリシーを使用して、SyncE または PTP 機能を有効にすることができます。

- a. **[+オブジェクトの作成 (+Create Object)]** ドロップダウンから、**[ノードプロファイル (Node Profile)]** 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. **[ノード (Nodes)]** フィールドに、このノードプロファイルポリシーを展開するスイッチのノード識別子を指定します。

ノードポリシーの構成は、テンプレートのファブリックローカルビューでも実行できます。その場合、ファブリックレベルの構成は、グローバルテンプレートレベルの構成を上書きします。前述のように、異なるテンプレートが作成され、マルチファブリックドメインの一部である各ファブリックに関連付けられる特定のシナリオでは、グローバルテンプレートレベルでのみノードポリシーを構成することをお勧めします。

- e. **[ノードポリシーは選択されていない (No selected Node Policy)]** をクリックし、作成したノード設定ポリシーを選択します。

ノード設定ポリシーで定義されたノード設定は、前のサブステップで指定したすべてのノードに適用されます。

特定のノードプロファイルでは、単一のノード設定ポリシーのみを参照できます。つまり、特定のノード（またはノードのセット）に対して SyncE ポリシーと PTP ポリシーの両方を有効にする場合は、両方の機能を同時に有効にした対応するノード設定ポリシーを（ファブリックポリシーテンプレートの一部として）作成し、ノードプロファイルで参照される必要があります。

- f. 追加のノードプロファイル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。

特定のノード（またはノードのセット）に関連付けることができるノードプロファイルポリシーは 1 つだけです。

8. ポッドプロファイルポリシーを作成します。

ノードプロファイルポリシーを作成する前に、「[ファブリックポリシーの作成](#)」で説明されているように、ノード設定ポリシーを作成しておく必要があります。このリリースでは、Pod 設定ポリシーを使用して NTP 機能を有効にできます。

- a. **[+オブジェクトの作成 (+Create Object)]** ドロップダウンから、**[ポッドプロファイル (Pod Profile)]** 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. **[タイプ (Type)]** ドロップダウンから、ポリシーを **[すべて (All)]** のポッドに適用するか、ポッドの**[範囲 (Range)]** に適用するかを選択します。

- e. **[タイプ (Type)]** で **[範囲 (Range)]** を選択した場合は、このポリシーを適用するポッドの範囲を指定します。
- f. **[ポッドポリシーは選択されていない (No selected Pod Policy)]** をクリックし、作成したポッド設定ポリシーを選択します。

ポッド設定ポリシーで定義されたポッド設定は、前のサブステップで指定したすべてのノードに適用されます。

- g. 追加のポッドプロファイル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。

特定のポッド（またはポッドのセット）関連付けることができるポッドプロファイルポリシーは 1 つだけです。

9 です。FEX デバイスポリシーを作成します。

- a. **[+オブジェクトの作成 (+Create Object)]** ドロップダウンから、**[FEX デバイス (FEX Device)]** 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. FEX デバイスに接続する 1 つ以上の **ノード (スイッチ)** を提供します。

現在、FEX と親リーフスイッチ間のストレート接続のみがサポートされているため、各 FEX は単一の親スイッチにのみ関連付ける必要があります。

ただし、FEX デバイスポリシーでは、次のように複数のノードを指定できます。

FEX Devices

×

UntitledFexDevice1

Common Properties

^

Name *

UntitledFexDevice1

Add Description

Nodes

101,102

Interfaces *

1/34

FEX Device ID *

101

上記の設定は、2 つの FEX デバイスがあり、1 つはリーフスイッチ **101** に接続され、もう 1 つはリーフスイッチ **102** に接続され、両方のデバイスが FEX ID **101** を持つことを意味します。FEX ID はリーフスイッチ範囲に制限されているため、異なるリーフスイッチに接続されている FEX デバイスは同じ ID を持つことができます。

e. FEX デバイスに接続する 1 つ以上の**インターフェイス**を提供します。

f. **FEX デバイス識別子**を提供します。

g. 追加の FEX デバイス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。

10. 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 つ以上のファブリックに保存（または展開）すると、オーケストレータは、指定されたノードやインターフェイスがファブリックに対して有効であることを確認し、有効でなければエラーを返します。

11. **【展開 (Deploy)】**をクリックして、ファブリックを関連付けるためテンプレートを再展開します。

ファブリック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。

そうでなかった場合、**【ファブリックに展開 (Deploy to fabrics)】**ページには、ファブリック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、構成の違いのみがファブリックに展開されます。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。

モニタリングポリシーを作成

このセクションでは、モニタリングポリシーテンプレートを使用して 1 つ以上の SPAN セッションポリシーを作成する方法について説明します。

1. Cisco Nexus Dashboard にログインし、Cisco Nexus Dashboard Orchestrator サービスを開きます。
2. 新しいテナントポリシーを作成。
 - a. 左のナビゲーションペインから、**[構成 (Configure)] > [ポリシーテンプレート (Policy Templates)]** を選択します。
 - b. **[モニタリングポリシーテンプレート (Monitoring Policy Template)]** タブで、**[モニタリングポリシーテンプレートの作成 (Create Monitoring Policy Template)]** をクリックします。
 - c. このテンプレートの SPAN セッションタイプを選択します。

次のいずれかを選択できます。

- **[テナント (Tenant)]** : このタイプの SPAN セッションは ERSPAN セッションと呼ばれ、ファブリック内の任意の場所にある指定されたテナントに属する EPG を SPAN セッションの**送信元**として構成し、同じまたは異なるテナントに属する別の EPG を**接続先**として構成できます。
- **[アクセス (Access)]** : 次の 2 つのシナリオのいずれかを構成できます。
 - アクセスポート、ポートチャネル、および vPC を送信元として、接続先を物理/ポートチャネルインターフェイスとして使用します。この場合、**送信元**インターフェイスと**接続先**インターフェイスは同じスイッチ上にある必要があります。
 - アクセスポート、ポートチャネル、および vPC を送信元として、接続先を EPG として使用します。この場合、これは ERSPAN セッションであり、SPAN 接続先をファブリック内の任意の場所に接続できます。
- d. セッションタイプとして**テナント**を選択した場合は、モニタリングポリシーを関連付ける**テナント**を選択します。
- e. モニタリングポリシーを関連付ける**[ファブリック (Fabric)]**を選択します。



モニタリングテンプレートに関連付けることが可能なファブリックは 1 つだけです。テナントポリシーテンプレートは、オンプレミス ACI ファブリックにのみサポートされ、割り当て可能です。

- f. **[モニタリングポリシー (Monitoring 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。

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 つ以上のファブリックポリシーを追加する必要があります。

- a. **Ok** をクリックして保存します。
3. **テナント**タイプテンプレートの SPAN セッションポリシーを作成します。

テンプレートタイプに**アクセス**を選択した場合は、代わりに次の手順を使用します。

- a. **[+オブジェクトの作成 (+Create Object)]** ドロップダウンから、**[SPAN セッション (SPAN Session)]** 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. **[管理状態 (Admin State)]** チェックボックスをオンにします。

管理状態が**無効**に設定されている場合、構成されたモニターにデータは送信されません。

- e. **[+ 送信元の追加 (+Add Source)]** をクリックして、SPAN 送信元情報を指定します。

送信元情報については、次の情報を提供します。

- **名前**
- **[方向 (Direction)]** : SPAN 送信元パケットの方向。次のいずれかになります。
 - **[両方 (Both)]** : 送信元に着信し、送信元から発信するパケットを複製して転送します。
 - **[着信 (Incoming)]** : 送信元に着信するパケットを複製して転送します。
 - **[発信 (Outgoing)]** : 送信元から発信されるパケットを複製して転送します。
- **[送信元 EPG (Source EPG)]** : SPAN トラフィックの送信元。

[テナント (Tenant)] タイプテンプレートの場合、送信元は常に EPG です。

[OK] をクリックして、送信元を保存します。次に、必要に応じて **[+ 送信元の追加 (+Add Source)]** をクリックして、追加の送信元を提供できます。

- f. **[接続先グループ (Destination Group)]** セクションから、複製されたパケットの転送先となる **[テナント (Tenant)]**、**[接続先 EPG (Destination EPG)]**、および **[接続先 IP アドレス (Destination EPG)]** を指定します。

このフィールドでは、IPv4 および IPv6 の IP アドレスがサポートされています。ただし、**接続先 IP** に IPv4 を使用し、**送信元 IP プレフィックス**に IPv6 を使用すること、またはその逆を混在させてはなりません。

- g. **[送信元 IP プレフィックス]** に入力します。

特定の IP アドレスが構成されている場合、すべての ERSPAN トラフィックはその IP から発信されます (たとえば、ERSPAN トラフィックを発信するすべての ACI リーフスイッチの場合)。代わりにプレフィックスが構成されている場合、各 ACI リーフスイッチには、送信元 ERSPAN トラフィックへのそのプレフィックスの一部である一意の IP が割り当てられます。これは、接続先スイッチで ERSPAN トラフィックの発信元を区別するのに役立ちます。

h. **SPAN バージョン**を選択します。

i. (オプション) 必要な場合、**詳細設定**を構成します。

- **[SPAN バージョンを施行 (Enforce SPAN Version)]** : 有効にすると、選択した SPAN バージョンを強制します。

有効の場合、ハードウェアがサポートしている場合、SPAN セッションは指定された SPAN バージョンを使用します。そうしないと、セッションは機能不全になります。

無効でバージョン 2 が指定されているが、ハードウェアでサポートされていない場合は、バージョン 1 が使用されます。

- **[フロー ID (Flow ID)]** : ERSPAN パケットの ID。

パケットがコピーされ、ERSPAN 経由で送信されると、パケットは ERSPAN ヘッダーを付けてカプセル化されます。フロー ID は、これらのパケットがコピーされた ERSPAN セッションを識別するための ERSPAN ヘッダー内の番号です。

指定できる範囲は 1 ~ 1023 です。デフォルトは 1 です。

- **[TTL]** : 存続可能時間 (TTL) または **1 ~ 255** ホップの範囲のホップ制限。ゼロに設定すると、TTL は指定されません。デフォルトのホップカウントは 64 です。
- **[DSCP]** : ERSPAN パケットの IP ヘッダーに設定される DSCP 値。
- **[MTU]** : ERSPAN で生成されるパケットの最大伝送単位。

範囲は 64 ~ 9216 です。デフォルトは、**1518** です。

ERSPAN の場合、ERSPAN カプセル化が追加されるため、接続先デバイスが受信する実際の MTU は、構成された MTU より大きくなります。ERSPAN バージョン 2 では、さらに 46 バイトが追加されます。ERSPAN バージョン 1 では、さらに 34 バイトが追加されます。その結果、デフォルトの MTU が 1518 の場合、エンドデバイスが実際にサポートする必要があるのはバージョン 2 では 1564 (1518 + 36)、バージョン 1 では 1552 (1518 + 34) です。

キャプチャされたフレームが構成された MTU より大きい場合、フレームは複製時に MTU 長に切り捨てられます。パケット/フレームのペイロードは不完全ですが、ヘッダーは分析のためにそのままの状態である必要があります。

j. 追加のテナント SPAN セッションポリシーを作成するためにこのステップを繰り返してください。

4. **アクセス**タイプテンプレートの SPAN セッションポリシーを作成します。

テンプレートタイプに **[テナント]**を選択した場合は、代わりに前の手順を使用します。

- a. **[+オブジェクトの作成 (+Create Object)]** ドロップダウンから、**[SPAN セッション (SPAN Session)]** 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. **管理状態 (Admin State)**] チェックボックスを有効にします。

管理状態が**無効**に設定されている場合、構成されたモニターにデータは送信されません。

- e. **[+ 送信元の作成 (+Create Source)]** をクリックして、SPAN 送信元情報を指定します。

送信元情報については、次の情報を提供します。

- **名前**
- **[+ アクセスパスの追加 (+Add Access Path)]** をクリックして、リーフスイッチに 1 つ以上のパスを追加します。次のパスがサポートされます：
 - **ポート**
 - **ポートチャネル**
 - **仮想ポートチャネル**
 - **VPC コンポーネント PC**

vPC を送信元として構成し、物理/ポートチャネルインターフェイスを接続先として構成する場合は、**[VPC コンポーネント PC (VPC Component PC)]** オプションを使用できます。このユースケースでは、すべてのインターフェイスが同じスイッチ上にある必要があるため、vPC を送信元として選択してはならず、接続先が接続されている同じスイッチ上のその vPC のインターフェイスを表す **VPC コンポーネント PC オプション** を選択する必要があります。つまり、vPC ドメインの一部である 2 番目のスイッチに 2 番目の SPAN セッションを作成して、ローカルの接続先に向かうそのスイッチの vPC の一部である送信元インターフェイスにトラフィックをスパンできるようにする必要があります。
- **[方向 (Direction)]** : SPAN 送信元パケットの方向。次のいずれかになります。
 - **[両方 (Both)]** : 送信元に着信し、送信元から発信するパケットを複製して転送します。
 - **[着信 (Incoming)]** : 送信元に着信するパケットを複製して転送します。
 - **[発信 (Outgoing)]** : 送信元から発信されるパケットを複製して転送します。
- **[+フィルタを作成 (+Create Filter)]** をクリックして、SPAN トラフィックフィルタ処理情報を提供します。

トラフィックフィルタ処理はオプションであり、フィルタが指定されていない場合、すべてのトラフィックがスパンされます。

次の属性に基づいてフィルタ処理を有効化できます：

- **送信元 IP プレフィックス**
- **送信元ポートから**
- **送信元ポートへ**
- **宛て先 IP プレフィックス**

- 宛て先ポートから
- 宛て先ポートへ
- IP プロトコル
- **[SPAN ドロップパケット (SPAN Drop Packets)]** : SPAN で、通常の SPAN ではキャプチャされないドロップされたパケットの一部をキャプチャできるようにします。ただし、「フォワードドロップ」としてドロップされたパケットに限定されます。

[有効 (Enabled)] にすると、ドロップされたパケットのみのスパニングが許可され、ドロップされなかったトラフィックは許可されません。

[無効 (Disabled)] にすると、SPAN はドロップされなかったトラフィックのみをキャプチャします。

デフォルト値は **Disabled** です。

- **[フィルタ (Filter)]** : **[SPAN ドロップパケット (SPAN Drop Packets)]** が無効になっている場合、送信元の EPG または L3Out に基づいて送信元パケットをフィルタ処理できます。フィルタ処理を有効にするには、**[EPG]** タブまたは **[L3Out]** タブを選択し、**[テナント (Tenant)]** を選択します。選択に基づいて、**[送信元 EPF (Source EPG)]** ドロップダウンからの特定の EPG、またはドロップダウンリストからの特定の **[L3Out]** および **[VLAN ID]** で有効になります。



これらの **[VLAN ID]** のみが、**[L3Out]** のインターフェイスに関連付けられているドロップダウンにリストされ、**[SPAN]** の送信元パスとしてインターフェイスとの照合が行われます。

以前に設定された送信元インターフェイスで送受信されるトラフィックは、指定された EPG または L3Out ノードに属している場合にのみスパンされます。

[OK] をクリックして、送信元を保存します。次に、必要に応じて **[+ 送信元の追加 (+Add Source)]** をクリックして、追加の送信元を提供できます。

f. 接続先タイプを選択します。

複製されたパケットは、EPG または特定のアクセスインターフェイスに転送できます。最初のケースでは、ファブリック内の任意の場所に接続された接続先にスパントラフィックを送信するために ERSPAN セッションが作成されます。後者の場合、接続先は、送信元インターフェイスと同じスイッチ上の物理/ポートチャネルインターフェイスに接続されている必要があります。

g. 接続先タイプに **EPG** を選択した場合は、次の情報を提供します。

- 複製されたパケットの転送先となる **[テナント (Tenant)]**、**[接続先 EPG (Destination IP Address)]**、および **[接続先 IP アドレス (Destination IP Address)]**。

このフィールドでは、IPv4 または IPv6 IP アドレスがサポートされています。ただし、**接続先 IP** に IPv4 を使用し、**送信元 IP プレフィックス**に IPv6 を使用すること、またはその逆を混在させてはなりません。

- **[送信元 IP プレフィックス (Source IP Prefix)]** : 送信元パケットの IP サブネットのベース IP アドレスです。
- **SPAN バージョン**
- (オプション) **[詳細設定 (Advanced Settings)]**
 - **[SPAN バージョンを施行 (Enforce SPAN Version)]** : 有効にすると、選択した SPAN バージョンを強制します。

有効の場合、ハードウェアがサポートしている場合、SPAN セッションは指定された SPAN バージョンを使用します。そうしないと、セッションは機能不全になります。

無効でバージョン 2 が指定されているが、ハードウェアでサポートされていない場合は、バージョン 1 が使用されます。

- **[フロー ID (Flow ID)]** : ERSPAN パケットの ID。

パケットがコピーされ、ERSPAN 経由で送信されると、パケットは ERSPAN ヘッダーを付けてカプセル化されます。フロー ID は、これらのパケットがコピーされた ERSPAN セッションを識別するための ERSPAN ヘッダー内の番号です。

範囲は 1 ~ 1023 です。デフォルトは 1 です。

- **[TTL]** : 存続可能時間 (TTL) または **1 ~ 255** ホップの範囲のホップ制限。ゼロに設定すると、TTL は指定されません。デフォルトのホップカウントは 64 です。
- **[DSCP]** : ERSPAN パケットの IP ヘッダーに設定される DSCP 値。
- **[MTU]** : ERSPAN で生成されたパケットの MTU。

範囲は 64 ~ 9216 です。デフォルトは、**1518** です。

ERSPAN の場合、ERSPAN カプセル化が追加されるため、接続先デバイスが受信する実際の MTU は、構成された MTU より大きくなります。ERSPAN バージョン 2 では、さらに 46 バイトが追加されます。ERSPAN バージョン 1 では、さらに 34 バイトが追加されます。その結果、デフォルトの MTU が 1518 の場合、エンドデバイスは実際にバージョン 2 の場合は 1564 (1518 + 36)、バージョン 1 の場合は 1552 (1518 + 34) をサポートする必要があります。

キャプチャされたフレームが構成された MTU より大きい場合、フレームは複製時に MTU 長に切り捨てられます。パケット/フレームのペイロードは不完全ですが、ヘッダーは分析のためにそのままの状態である必要があります。

- h. それ以外の場合、**接続先タイプ**に**アクセスインターフェイス**を選択した場合は、代わりに次の情報を提供します :

- **[パスタイプ (Path Type)]** : インターフェイスのタイプ。**[ポート (Port)]** または **[ポートチャネル (Port Channel)]** です。
- **ポート** インターフェイスの場合は、**ノードとパス**を選択します。
- **ポートチャネル** インターフェイスの場合、ポートチャネルの名前を選択します。
- **[MTU]** : ERSPAN で生成されたパケットの MTU。

範囲は 64 ~ 9216 です。デフォルトは、**1518** です。

ERSPAN の場合、ERSPAN カプセル化が追加されるため、接続先デバイスが受信する実際の MTU は、構成された MTU より大きくなります。ERSPAN バージョン 2 では、さらに 46 バイトが追加されます。ERSPAN バージョン 1 では、さらに 34 バイトが追加されます。その結果、デフォルトの MTU が 1518 の場合、エンドデバイスが実際にサポートする必要があるのはバージョン 2 では 1564 (1518 + 36) 、バージョン 1 では 1552 (1518 + 34) です。

キャプチャされたフレームが構成された MTU より大きい場合、フレームは複製時に MTU 長に切り捨てられます。パケット/フレームのペイロードは不完全ですが、ヘッダーは分析のためにそのままの状態である必要があります。

i. 追加のアクセス SPAN セッションポリシーを作成するためにこのステップを繰り返してください。

5. 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。

6. **[展開 (Deploy)]** をクリックして、ファブリックを関連付けるためテンプレートを再展開します。

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。

そうでなかった場合、**[ファブリックに展開 (Deploy to fabrics)]** ウィンドウには、ファブリック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、構成の違いのみがファブリック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 7 月 26 日

米国本社

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<http://www.cisco.com>

電話: 408 526-4000

800 553-NETS (6387)

Fax : 408 527-0883