レイヤ 4 ~ レイヤ 7 サービス 設定、リリース 12.2.1

目次

新規情報および変更情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

リリース バージョン	特長	説明
NDFC リリース 12.2.1	ePBR サポート	NDFC リリース 12.2.1 以降では、レイヤ 4 からレイヤ 7 へのサービス ロード バランシング、および単一サイトのトラフィック ステアリングとリダイレクションに使用される拡張ポリシーベース リダイレクト（ePBR）のサポートを使用できます。

レイヤ 4～レイヤ 7 サービスの設定

Cisco Nexus Dashboard Fabric Controller では、レイヤ 4 ～レイヤ 7 （L4～L7）サービス デバイスをデータ センター ファブリックに挿入する機能が導入されました。これらの L4～L7 サービス デバイスにトラフィックを選択的にリダイレクトすることもできます。L4～L7 サービス アプライアンスを追加し、L4～L7 サービス アプライアンスと L4～L7 サービス リーフ スイッチの間にルート ピアリングを作成してから、これらの L4～L7 サービス アプライアンスにトラフィックを選択的にリダイレクトできます。

レイヤ 4 ～ レイヤ 7 サービス

[レイヤ 4 ～ レイヤ 7 サービス（Layer 4 to Layer 7 Services）] ウィンドウに移動するには、次の手順を実行します。

1. **[管理（Manage）] > [ファブリック（Fabrics）]** の順に選択します。
2. 適切な Data CenterVXLAN EVPN ファブリックをダブルクリックして、そのファブリックの **[ファブリックの概要（Fabric Overview）]** ウィンドウ
   を表示します。
3. そのファブリック の [サービス（**Services**）] タブをクリックします。

次の場所に移動して、スイッチに固有の サービス情報を表示することもできます。

[管理（Manage）] > [スイッチ（Switches）] > [スイッチの概要（Switches Overview）] > [サービス（Services）]

さらに、サービス リダイレクションのビデオも視聴できます。これは、Cisco Nexus Dashboard Fabric Controller が管理するデータセンターで VXLAN ファブリックを使用して L4 ~ L7 サービス アプライアンスを編成する方法を示しています。このデモでは、プロビジョニング、サービス ポリシーの定義、およびリダイレクトされたフローのモニタリングについて説明します。

サービスアプライアンス

外部ファブリックを作成し、サービス アプライアンスを作成時に外部ファブリックに存在するサービス アプライアンスを指定する必要があります。Nexus Dashboard Fabric Controller は、サービス アプライアンスを自動検出または検出しません。サービス アプライアンス名、タイプ、およびフォーム ファクタも指定する必要があります。サービス アプライアンスの名前は、ファブリック内で一意である必要があります。サービス アプライアンスはリーフ、ボーダー リーフ、ボーダー スパイン、ボーダー スーパー スパインまたはボーダー ゲートウェイにアタッチされます。Nexus Dashboard Fabric Controller は、サービス スイッチの新しいスイッチ ロールを定義しません。

Nexus Dashboard Fabric Controller は、サービス アプライアンスに接続されているスイッチを管理します。Nexus Dashboard Fabric Controller は、接続されているこれらのスイッチのインターフェイスも管理します。サービス アプライアンスが接続されているインターフェイスがトランク モードであり、どのインターフェイス グループにも属していないことを確認します。L4 ~ L7 サービスは、そのモードを変更しません。接続されたスイッチが vPC ペアを形成している場合、接続されたスイッチの名前は両方のスイッチの組み合わせになります。

必要なサービス名をダブルクリックして、サービス アプライアンスの詳細ウィンドウの以下のタブを表示します。

- 概要
- ルートピアリング
- サービス ポリシー

MSD サポート

この機能は、マルチサイト ドメイン（MSD）をサポートします。サービス アプライアンスの作成時に MSD メンバー ファブリックをアタッチされたファブリックとして選択し、サービス アプライアンス（ファイアウォール、ロード バランサなど）を作成し、選択した MSD メンバー ファブリック内のスイッチにサービス アプライアンスをアタッチし、ルート ピアリングとサービス ポリシーを定義し、選択した MSD

メンバーファブリックの関連設定を展開します。サービスを構成する手順の詳細については、「レイヤ 4 ~ レイヤ 7 サービスの構成」を参照してください。

RBAC サポート

L4 ~ L7 サービスは、ロールベース アクセス コントロール（RBAC）とファブリック アクセス モードをサポートします。

admin、stager、および operator は、 Nexus Dashboard Fabric Controller の事前定義済みロールです。次の表に、各ロールが実行できるさまざまな操作を示します。

サービス オペレーション	サービスアプライアンス	ルートピアリング	サービス ポリシー
作成/更新/削除/インポート	admin	admin、stager	admin、stager
リスト/エクスポート	admin 、stager、operator	admin、stager、operator	admin、stager、operator
Attach/Detach	該当なし	admin、stager	admin、stager
展開（**Deploy**）	該当なし	admin（ファブリックがファブリック モニタまたは読み取り専用モードの場合はブロックされます）	admin（ファブリックがファブリック モニタまたは読み取り専用モードの場合はブロックされます）
プレビュー/展開履歴	該当なし	admin、stager、operator	admin、stager、operator

境界スイッチの WAN インターフェイスでの PBR サポート

ポリシーベース リダイレクト（PBR）を使用して、トップダウン構成で定義されていない任意のネットワークを、サービス ポリシーの送信元または宛先ネットワークとして指定できます。これは、南北トラフィックのポリシー適用の合理化に役立ちます。Nexus Dashboard Fabric Controller UI には、VRF アソシエーションを持つすべてのボーダー スイッチ（スタンドアロンまたは vPC）のルーテッド レイヤ 3 インターフェイスがリストされます。その後、定義されたポリシーに関連付ける必要がある必要なインターフェイスを選択できます。境界スイッチには、境界リーフ、境界スパイン、境界スーパー スパイン、境界ゲートウェイが含まれます。複数のインターフェイス アソシエーションを設定できます。たとえば、1 つのボーダー スイッチに対して複数の L3 インターフェイス、サブインターフェイス、およびポート チャネルを選択できます。インターフェイス アソシエーション用に複数の境界スイッチを選択することもできます。詳細については、『Cisco Nexus 9000 シリーズ NX-OS 』を参照してください 。

ポリシーの方向によっては、「任意」または任意のネットワークのボーダー スイッチとインターフェイスの関連付けが不要な場合があります。たとえば、転送ポリシーの場合、「任意」または任意の宛先ネットワークには、ボーダー スイッチとインターフェイス入力またはルートマップの関連付けは必要ありません。リバース ポリシーの場合、ボーダー スイッチとインターフェイスまたはルート マップの関連付けは、「任意」または任意の送信元ネットワークには必要ありません。

「任意」または任意のネットワークを含むポリシーが接続されると、ポリシー関連の CLI が生成され、ボーダー スイッチの選択された L3 ルーテッド インターフェイスに関連付けられます。そのポリシーを展開すると、選択した境界スイッチに CLI がプッシュされます。展開履歴には対応するエントリが含まれ、VRF フィルタリングを使用してすばやくアクセスできます。サービス ポリシー統計情報の図には、境界スイッチの選択した L3 ルーテッド インターフェイスに関連付けられたルート マップの PBR 統計情報が含まれます。

ePBR サポート

NDFC リリース 12.2.1 以降では、拡張ポリシーベース リダイレクト（ePBR）のサポートが利用可能です。

これは、レイヤ 4 からレイヤ 7 のサービス ロード バランシング、および単一サイトのトラフィックのステアリングとリダイレクションに使用されます。

「ボーダー スイッチの WAN インターフェイスでの PBR サポート」で説明されている PBR 機能と同様に、ePBR はポリシーベースのリダイレクト ソリューションを利用してトラフィックを誘導し、アプリケーションベースのルーティングを有効にします。 ePBR を使用すると、同じファブリック内またはファブリック間でサービス チェーニングを有効にすることもできます。 ePBR サービス フローは、前のセクションで説明したように、サービス アプライアンス、ルート ピアリング、およびサービス ポリシー機能で構成される PBR サービス フローに似ています。

ePBR サービス フローのサービス ポリシーは、同じファブリックでのサービス チェーンをサポートします。サービス チェーンのサービス アプライアンスは、さまざまなサービスノードタイプの任意の組み合わせにすることができ、さまざまな障害アクションを定義することもできます。複数の送信元ネットワークと接続先ネットワークをサービス ポリシーに関連付けることができます。また、サービス ポリシー向けにアプリケーションを簡単にするため、1 つの ACL で複数の ACL と複数の ACE を定義できます。詳細については、「サービス ポリシーの作成」を参照してください。

静的ルート

L4 ~ L7 サービスは、スタティック ルートで参照されている VRF がアタッチされているすべての VTEP（サービス リーフ スイッチを含む）にスタティック ルートをプッシュします。これにより、スタティック ルートによるサービス アプライアンスのフェールオーバーが促進されます。

NDFC リリース 12.1.3 以降では、オプションの **[**ゲートウェイ **IP** のエクスポート（ **Export Gateway IP**） **]** フラグを有効にして、ゲートウェイ IP（サービス アプライアンス IP）アドレスをネクストホップとしてエクスポートすることもできます。これにより、サービス スイッチ（サービス アプライアンスが接続されているスイッチ）でのみ、静的ルートを展開するようにトリガします。

L4～L7 サービスの注意事項と制限事項

- Nexus Dashboard Fabric Controller の L4 ~ L7 サービスは、ファイアウォール、ロード バランサ、仮想ネットワーク機能などのサービス アプライアンスを管理またはプロビジョニングしません。
- L4 ~ L7 サービス機能は、**Data Center VXLAN EVPN** テンプレートを使用する VXLAN BGP EVPN ファブリックでのみサポートされます。
- この機能で定義されたサービス ポリシーは、ポリシーベース ルーティング（PBR）を利用し、NDFC リリース 12.2.1 以降では、拡張ポリシーベースルーティング（ePBR）を利用します。PBR および ePBR 関連校生および制約については、『Nexus 9000 シリーズ NX-OS ユニキャスト ルーティング構成ガイド』を参照してください。
- PBR および ePBR 機能は排他的です。同じファブリックで PBR と ePBR の両方のサービス フローを同時に有効にすることはできません。
- ePBR 機能では、アクティブ/スタンバイ、スケールアップ、およびスケールアウトのクラスタ展開がサポートされています。
- この機能は、Cisco Nexus 9300-EX および 9300-FX プラットフォーム スイッチを、リーフ、ボーダー リーフ、ボーダー スパイン、ボーダー スーパース パイン、およびボーダー ゲートウェイ スイッチとして動作するようにサポートします。
- L3 ネットワーク用のテナント内およびテナント間ファイアウォール、およびワンアーム仮想ネットワーク機能およびツーアーム ロード バランサを含む構成がサポートされています。
- 既存の Nexus Dashboard Fabric Controller トポロジ ビューは、サービス アプライアンスが接続されているスイッチに関連付けられたリダイレクトされたフローを表示します。特定のリダイレクトされたフローを見つけるためにも利用されます。
- L4 ~ L7 サービス REST API は、Nexus ダッシュボード ファブリック コントローラによりパッケージ化された REST API ドキュメントからアクセスできます。詳細については、『*Cisco Nexus Dashboard Fabric Controller REST API リファレンス ガイド*』を参照してください。
- L4 ~ L7 サービスは、リアルタイムの対話のために Kafka 通知を生成します。
- ロード シェアリングはサポートされていません。
- ワンアーム ファイアウォールの展開は、eBGP ピアリングおよび静的ピアリング オプションでサポートされています。
- IPv6 は L4 ~ L7 サービスでサポートされます。アンダーレイ制約の IPv6 を使用した VXLAN 上の PBR については、『 Cisco Nexus 9000 シリーズ NX-OS VXLAN 構成ガイド』を参照してください。
- この機能は、必要に応じてサービスネットワークを作成、更新、削除します。サービスネットワークは、**[管理（Manage）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** ウィンドウから作成または削除することはできません。

サービス デバイスのタイプ

Cisco Nexus Dashboard Fabric Controller の L4 ~ L7 サービスは、すべてのベンダーのサービス アプライアンス接続をサポートします。データセンターに導入される一般的なサービス アプライアンス タイプは、ファイアウォール、ロード バランサ、およびその他のレイヤ 4 ～レイヤ 7 製品です。

サポートされているファイアウォール ベンダーの例は、Cisco Systems、Palo Alto Networks、Fortinet、Check Point Software Technologies などです。

サポートされているロード バランサ ベンダーの例は、F5 ネットワーク、Citrix システム、A10 ネットワークなどです。

これらの例のリストは例として使用するものであり、すべてを網羅するものでは
ありません。L4 ~ L7 サービス接続は汎用であり、すべてのベンダー サービス アプライアンスに適用されます 。

概要

[概要（**Overview**）**]** タブでは、選択したサービス アプライアンスの **[**概要（**Summary**）**]**、**[**ルート ピアリング（**Route Peering**）**]**、**[**サービス ポリシー（ **Service Policy**）**]** トポロジを表示できます。

[更新（**Refresh**）**]** アイコンをクリックして、最新の詳細を表示します。

レイヤ 4 ～ レイヤ 7 サービスのファブリック設定の構成

レイヤ 4 ～ レイヤ 7 のサービス機能を有効にするには、特定のファブリック設定を行う必要があ

ります。これらの設定を構成するには：

1. **[**管理（**Manage**）**] > [**ファブリック（**Fabrics**）**]** を選択し、**[**アク

   ション（**Actions**）**] > [**ファブリックの作成（**Create Fabric**）**]**

   をクリックします。**[**ファブリックの作成（**Create Fabric**）**]** ウ

   ィンドウが表示されます。

2. ファブリック名を入力し、 **Data CenterVXLAN EVPN** テンプレートを選択します。
3. **[**詳細設定（**Advanced**）**]** タブをクリックします。
4. **[Elastic Services Re-direction (ESR)** オプション（**Elastic Services Re-direction (ESR) Options**）**]** フィールドを見つけて、 適切な構成を選択します。

   [ESR] フィールドは、NDFC リリース 12.1.3 以降で使用できます。次のいずれかのオプションを選択します。

   - **[PBR]** : ポリシーベース ルーティング（'デフォルト設定）
   - **[ePBR]** : 拡張ポリシーベース ルーティング
5. **[**ポリシーベース ルーティング（**PBR**）**/**拡張 **PBR** の有効化（**Enable Policy-Based Routing (PBR)/Enhanced PBR (ePBR)**）**]** チェックボックスをオンにして、指定したポリシーに基づいてパケットのルーティングを有効にします。
   - 上記の **[ESR]** フィールドで **[PBR]** を選択した場合、このチェックボックスをオンにすると、ポリシーベース ルーティング（PBR）が有効になります。
   - 上記の **[ESR]** フィールドで **[ePBR]** を選択した場合、このチェックボックスをオンにすると、拡張ポリシーベース ルーティング回送（ePBR）が有効になり、スイッチで PBR、SLA 送信者、および ePBR 機能が有効になります 。
6. **[**リソース（**Resources**）**]** タブをクリックし、**[**サービス ネットワーク **VLAN** 範囲（**Service Network VLAN Range**）**]** フィールドで VLAN 範囲を指定します。

   これは、スイッチ オーバーレイ サービス ネットワーク単位での VLAN 範囲です。最小許容値は 2、最大許容値は 4094 です。

7. **[**ルート マップ シーケンス番号の範囲（**Route Map Sequence Number Range**）**]** フィールドの値を指定します。

   最小許容値は 1、最大許容値は 65534 です。

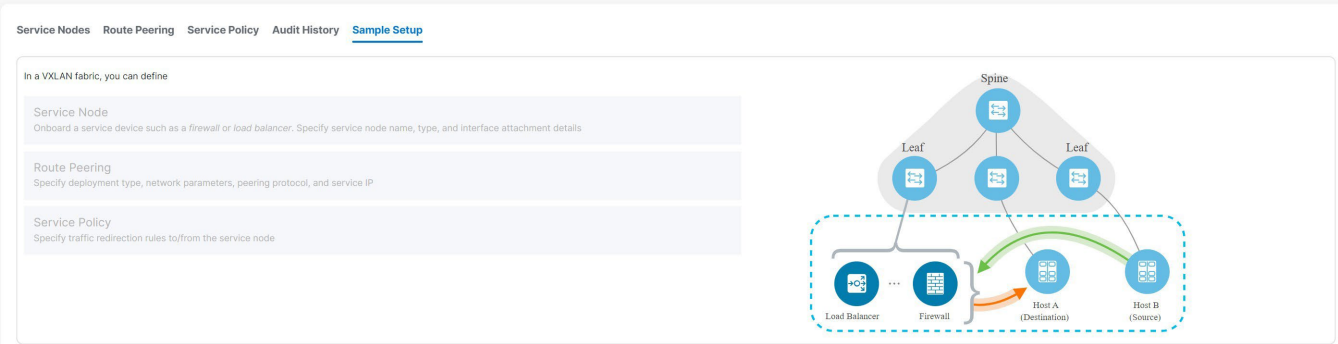
8. **[** 保 存 （ **Save** ） **]** を クリック して 、 更新 された 構成 を 保存 します 。

レイヤ 4 ～ レイヤ 7 サービスの構成

Cisco **Nexus Dashboard Fabric Controller** の **Web UI** で レイヤ **4** ～ レイヤ **7** サービスまたは **Elastic Service** を起動するには、**[**管理（**Manage**）**] > [**ファブリック（**Fabrics**）**] > [**ファブリックの概要（**Fabric Overview**）**] > [**サービス（**Services**）**]** を選択します。

次の場所に移動して、スイッチに固有の [サービス（Services）]ウィンドウを表示することもできます。

[管理（**Manage**）**] > [**スイッチ（**Switches**）**] > [**スイッチの概要（**Switches Overview**）**] > [**サービス（**Services**）**]**



[サービス（**Services**）**]** ウィンドウには、次のタブが表示されます。

- **[**サービスアプライアンス（**Service Appliances**）**]**：NDFC で構成した L4 ～ L7 サービスアプライアンスを表示します。
- **[**ルート ピアリング（**Route Peering**）**]**：NDFC のルート ピアリング構成を表示します。詳細については、「 ルート ピアリング 」を参照してください。
- **[**サービス ポリシー（**Service Policy**）**]**：NDFC で構成したサービス ポリシーに関する情報を表示します。詳細については、「サービス ポリシー」を参照してください。
- **[**監査履歴（**Audit History**）**]**：選択したサービス ポリシーまたはルート ピアリングに関連するスイッチおよびネットワークの監査履歴を表示できます。

サービス アプライアンスの追加

サービス アプライアンスを作成する方法：

1. **[サービス インスタンス（Service Instance）]** タブに移動します。
   a. 次の順に選択：

      [管理（Manage）] > [ファブリック（Fabrics）]

   b. 適切な Data CenterVXLAN EVPN ファブリックをダブルクリッ

      クします。ファブリックの **[概要（Overview）]** が表示されます。

   c. **[サービス（Services）]** タブをクリックします。

      [サービス アプライアンス（Service Appliances）] サブタブがデフォルトで選択されている必要があります。

2. **[アクション（Actions）] > [追加（Add）]** をクリックします。

   [新しいサービス アプライアンスの作成（Create New Service Appliance）] ウィンドウが表示されます。

[新しいサービス アプライアンスの作成（Create New Service Appliance）] ウィンドウには、次の 3 つのガイド付き手順があります。

- サービスアプライアンスの作成
- ルート ピアリングの作成
- サービス ポリシーの作成

サービスアプライアンスの作成

[サービス アプライアンスの作成（Create Service Appliance）] ウィンドウには、次の 2 つのセクションがあります。

- サービスアプライアンスの作成
- サービスノードのスイッチアタッチメント

その後に **[リンク テンプレート（Link Template）]**ドロップダウン リストが続きます。

1. **[サービス アプライアンスの作成（Create Service Appliance）]** セクションに必要な情報を入力します。

   [サービス アプライアンスの作成（Create Service Appliance）] ウィンドウのフィールドは次のとおりです。アスタリスクが付いたフィールドに入力する必要があります。

フィールド	説明
サービス [アプライアンス	サービス アプライアンスの名前を入力します。 事前 name できる に構成

（Appliance）] 名前	にはアルファベット、数字、アンダースコア、または文字を含めることができます。
サービスノードのタイプ	[ファイアウォール (Firewall)]、[ロード バランサ (Load Balancer)]、または [仮想ネットワークの機能 (Virtual Networking Function)] を選択します。
アプライアンスの種類	このフィールドは、NDFC リリース 12.2.1 で導入されました。次のオプションがあります。 ・ Cluster ・ [HA] : 2 つのサービス アプライアンスに適用されます。 ・ [スタンドアロン（Standalone）] : 1 つのサービスアプライアンスに適用されます。
フォーム ファクタ	[物理（Physical）] または [仮想（Virtual）] を選択します。

2. **[+** スイッチ アタッチメントの追加（**+ Add Switch Attachment**）**]** をクリックします。

   [スイッチ アタッチメントの追加（**Add Switch Attachment**）**]** ポップアップが表示されます。

3. **[**スイッチ アタッチメントの追加（**Add Switch Attachment**）**]** ポップアップに必要な情報を入力します。

フィールド	説明
サービスノード名	構成済みのサービス ノードのリストから選択するか、**[+** サービス ノードの作成（**+ Create Service Node**）**]** をクリックして新しいノードを作成します。
外部ファブリック	外部ファブリックを指定します。
サービス ノード インターフェイス	サービス ノード インターフェイスを指定します。
アタッチされたファブリック	リストからファブリックを選択します。
アタッチされたスイッチ	リストからスイッチまたはスイッチ ペアを選択します。
アタッチされた スイッチ インターフェイス	リストからインターフェイスを選択します。**[**アタッチされたリーフ スイッチ（**Attached Leaf Switch**）**]** リストから vPC ペアを選択すると、vPC チャネルが **[**アタッチされたスイッチ インターフェイス（**Attached Switch Interface**）**]** リストに表示されます。それ以外の場合、トランクモードのポートチャネルおよびインターフェイスは、**[**アタッチされたリーフ スイッチ インターフェイス（**Attached Leaf Switch Interface**）**]** リストに表示されます。
リンク テンプレート	指定されたアタッチ済みスイッチ インターフェイス タイプに基づき、ドロップダウン リストから service_link_trunk 、service_link_port_channel_trunk、または the service_link_vpc を選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。

4. 適切なリンクテンプレートを選択したら、[パスワード を 変

   更）] をクリックします。[サービス アプライアンスの作成

   （**Create Service Appliance**）] ウィンドウに戻ります。

5. [サービス アプライアンスの作成（**Create Service Appliance**）] ウィンドウで [保存（**Save**）] をクリックします。

   プロセスの [ルート ピアリングの作成（**Create Route Peering**）] の部分に進みます。詳細については、「ルート ピアリングの作成」を参照してください。

ルート ピアリングの作成

[ルート ピアリングの作成（**Create Route Peering**）] ウィンドウは、「サービス アプライアンスの追加」プロセスの 2 番目のステップとして表示されます。サービス アプライアンスを追加した後、次の場所に移動して [ルート ピアリングの作成（**Create Route Peering**）] ウィンドウに移動することもできます。

[管理（Manage）] > [ファブリック（Fabrics）] > [ファブリックの概要（Fabric Overview）] > [サービス（Services）]

[ルート ピアリング（**Route Peering**）] タブをクリックし、[アクション（**Actions**）] > [追加（**Add**）] の順にクリックします。[ルート ピアリングの作成（**Create Route Peering**）]ウィンドウが表示されます。このウィンドウでアスタリスクが付いたフィールドに入力する必要があります。

1. [ピアリング名（**Peering Name**）] フィールドで、ピアリングの名前を指定します。

   名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。

2. [サービス アプライアンス名（**Service Appliance Name**）] フィールドで、[サービス アプライアンスの作成（ Create Service Appliance ）] で作成したサービス アプライアンスが表示されていることを確認します。
3. [展開（**Deployment**）] フィールドで、展開のタイプを選択します。

   [ルート ピアリングの作成（**Create Route Peering**）] ウィンドウに表示されるフィールドは、[サービス アプライアンスの作成（**Create New Service Node**）] ウィンドウで選択した L4 ~ L7 サービス アプライアンスのタイプによって異なります。選択したタイプ（ファイアウォール、ロードバランサ、または VNF）に応じて、展開のタイプは次のいずれかになります。

   - ファイアウォール：
     - テナント内ファイアウォール
     - テナント間ファイアウォール
     - ワンアームファイアウォール
   - ロード バランサー：
     - ワンアームモード
     - ツーアームモード
   - VNF：
     - ワンアーム VNF
4. [ピアリング オプション（**Peering Option**）] フィールドで適切な選択を

   行います（使用可能な場合）。次のオプションがあります。

   - スタティックピアリング
   - EBGP ダイナミックピアリング
5. [ノード ピアリング（**Node Peerings**）] テーブルの下で、[+

   ノードピアリングの追加（**+Add Node Peering**）] をクリッ

   クします。[ノード ピアリングの追加（**Add Node**）] ウィン

   ドウが表示されます。

6. 次の表を使用して、ルート ピアリングの残りの構成を完了します。

   構成するルート ピアリングのタイプに応じてフィールドがどのように入力されるかを確認するには、「ルート ピアリングの構成例」を参照してください。

> ヒ
>
> [管理（**Manage**）] > [ファブリック（**Fabrics**）] > [ネットワーク（**Networks**）] ウィンドウでは、サービス ネットワークの削除は

ウィンドウに入力できます。

フィールド	説明
サービスノード	サービス ノードを選択します。
Attach/Detach	トグルを使用して、ノード ピアリングをアタッチまたはデタッチします。
ファースト アーム/内部ネットワーク	
VRF	VRF を指定します。
サービスネットワーク	サービス ネットワークの名前を指定します。
VLAN ID	VLAN ID を指定します。有効な ID の範囲は 2 ～ 3967 です。定義済みの L4 ~ L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。
ネットワーク ID（Network ID）	ネットワーク ID を指定します。有効な ID 値の範囲は 0 ～ 16777214 です。このフィールドの値が 0 の場合、ネットワーク識別子は自動的に生成されます。
サービス ネットワーク テンプレート	ドロップダウン リストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。
サービス ノードの IP アドレス	IPv4 サービス ノードの IP アドレスを指定します。
サービス ノードのIPv6アドレス	IPv6 サービス ノードの IP アドレスを指定します。
[ルート名（Route Name）]	リストからルートを選択するか、**[+ルートの作成（+Create Route）]** オプション をクリックして新しいルートを作成します。詳細については、「ルート ピアリング テンプレート」 を参照してください。
ルートテンプレート	ルート テンプレートを表示します（該当する場合）。
プローブ名	リストからプローブを選択するか、**[+プローブの作成（+Create Probe）]** オプション をクリックして新しいプローブを作成します。詳細については、[プローブ テンプレート（Probe Tempate）] を参照してください。
プローブテンプレート	プローブ テンプレートを表示します（該当する場合）。
セカンド アーム/外部ネットワーク	
VRF	VRF を指定します。
サービスネットワーク	サービス ネットワークの名前を指定します。
VLAN ID	VLAN ID を指定します。有効な ID の範囲は 2 ～ 3967 です。定義済みの L4 ~ L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。
ネットワーク ID（Network ID）	ネットワーク ID を指定します。有効な ID 値の範囲は 0 ～ 16777214 です。このフィールドの値が 0 の場合、ネットワーク識別子は自動的に生成されます。
サービス ネットワーク テンプレート	ドロップダウン リストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。

リバーストラフィックのサービスノード IP アドレス	リバース トラフィックの IPv4 サービス ノード IP アドレスを指定します。
リバーストラフィックのサービスノード IPv6 アドレス	リバース トラフィックの IPv6 サービス ノード IP アドレスを指定します。

プローブ名	このフィールドは、NDFC リリース 12.2.1 で導入されました。 ・ePBR サービス フローを構成する場合は、プローブに必要な情報を構成する必要があります。PBR サービス フローを構成する場合は、プローブ情報を構成しないでください。 ・アクティブ/スタンバイ構成の場合、現用系ノードとスタンバイ ノードのノード ピアリングは、同じサービス ネットワークとルートを共有できます。 リストからプローブを選択するか、**[+プローブの作成（+Create Probe）]** オプション をクリックして新しいプローブを作成します。
リモートスイッチ	
+ リモート スイッチの追加	該当する場合はクリックしてリモート スイッチを追加します。
スイッチ名	リモート スイッチが追加されている場合は、リモート スイッチ名を表示します。
ピアリングテンプレート	リモート スイッチが追加された場合に、使用されるピアリング テンプレートを表示します。

7. **[保存（Save）]** をクリックします。

   プロセスの **[サービス ポリシーの 作成（Create Service Policy）]** 部分に進みます。詳細については、「サービス ポリシーの作成」を参照してください。

ルート ピアリングの構成例

次に、構成するルート ピアリングのタイプに応じて、フィールドがどのように入力されるかを示すルート ピアリング構成の例をいくつか示します。

- 例：テナント間ファイアウォールの展開
- 例：ワンアーム モードのロード バランサ
- 例：ツーアーム モードのロード バランサ
- 例：ワンアーム仮想ネットワーク機能

例：テナント間ファイアウォールの展開

ピアリング オプション：静的ピアリング、内部ネットワーク ピアリング テンプレート：**service_static_route**、外部ネットワーク ピアリング テンプレート：**service_static_route**

テナント間ファイアウォールを展開するための **[ルート ピアリングの作成（Create Route Peering）]** ウィンドウのフィールドは次のとおりです。

フィールド	説明
Peering Name	ピアリングの名前を指定します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。
デプロイ	テナント間ファイアウォールを選択します。
ピアリング オプション	[静的ピアリング（Static Peering）] または [eBGP 動的ピアリング（eBGP Dynamic Peering）] を選択します。
内部ネットワーク	
VRF	ドロップダウン リストから [VRF] を選択します。
サービスネットワーク	L4 ~ L7 サービス ネットワーク名を指定します。
VLAN ID	VLAN ID を指定します。有効な ID の範囲は 2 ～ 3967 です。定義済みの L4 ~ L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。
ネットワーク ID（Network ID）	ネットワーク ID を指定します。有効な ID 値の範囲は 0 ~ 16777214 です。このフィールドの値が 0 の場合、ネットワーク識別子は自動的に生成されます。
サービス ネットワーク テンプレート	ドロップダウン リストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。
ピアリングテンプレート	ドロップダウン リストから [service_static_route] または [service_ebgp_route] を選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。
外部ネットワーク	
VRF	ドロップダウン リストから [VRF] を選択します。
サービスネットワーク	L4 ~ L7 サービス ネットワーク名を指定します。
VLAN ID	VLAN ID を指定します。有効な ID の範囲は 2 ～ 3967 です。定義済みの L4 ~ L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。
ネットワーク ID（Network ID）	ネットワーク ID を指定します。有効な ID 値の範囲は 0 ~ 16777214 です。このフィールドの値が 0 の場合、ネットワーク識別子は自動的に生成されます。
サービス ネットワーク テンプレート	ドロップダウン リストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。
ピアリングテンプレート	ドロップダウン リストから [service_static_route] または [service_ebgp_route] を選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。

例：ワンアーム モードのロード バランサ

ワンアーム ファイアウォールを展開するための **[ルート ピアリングの作成（Create Route Peering）]** ウィンドウのフィールドは次のとおりです。

フィールド	説明

Peering Name	ピアリングの名前を指定します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。
デプロイ	[ワンアーム モード（One-Arm Mode）] を選択します。
ピアリング オプション	[静的ピアリング（Static Peering）] または [eBGP 動的ピアリング（eBGP Dynamic Peering）] を選択します。
ファースト アーム	
VRF	ドロップダウン リストから [VRF] を選択します。
サービスネットワーク	L4 ~ L7 サービス ネットワーク名を指定します。
VLAN ID	VLAN ID を指定します。有効な ID の範囲は 2 ～ 3967 です。定義済みの L4 ~ L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。
ネットワーク ID（Network ID）	ネットワーク ID を指定します。有効な ID 値の範囲は 0 ~ 16777214 です。このフィールドの値が 0 の場合、ネットワーク識別子は自動的に生成されます。
サービス ネットワーク テンプレート	ドロップダウン リストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。

ピアリングテンプレート	ドロップダウン リストから [service_static_route] または [service_ebgp_route] を選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。
サービス アプライアンス **IP** セクション	
リバース トラフィックのサービス アプライアンス IP アドレス	リバース トラフィックの IPv4 サービス アプライアンスの IP アドレスを指定します。
リバース トラフィックのサービス アプライアンス IPv6 アドレス	リバース トラフィックの IPv6 サービス アプライアンスの IP アドレスを指定します。

例：ツーアーム モードのロード バランサ

ツーアーム モード ロード バランサを展開するための [ルート ピアリングの作成（Create Route Peering）] ウィンドウのフィールドは、次のとおりです。

フィールド	説明
Peering Name	ピアリングの名前を指定します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。
デプロイ	[ツーアーム モード（Two-Arm Mode）] を選択します。
ピアリング オプション	[静的ピアリング（Static Peering）] または [eBGP 動的ピアリング（eBGP Dynamic Peering）] を選択します。
ファースト アーム	
VRF	ドロップダウン リストから [VRF] を選択します。
サービスネットワーク	L4 ~ L7 サービス ネットワーク名を指定します。

VLAN ID	VLAN ID を指定します。有効な ID の範囲は 2 ～ 3967 です。定義済みの L4 ~ L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。
ネットワーク ID（Network ID）	ネットワーク ID を指定します。有効な ID 値の範囲は 0 ~ 16777214 です。このフィールドの値が 0 の場合、ネットワーク識別子は自動的に生成されます。
サービス ネットワーク テンプレート	ドロップダウン リストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。
ピアリングテンプレート	ドロップダウン リストから [service_static_route] または [service_ebgp_route] を選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。
セカンド アーム	
VRF	ドロップダウン リストから [VRF] を選択します。
サービスネットワーク	L4 ~ L7 サービス ネットワーク名を指定します。
VLAN ID	VLAN ID を指定します。有効な ID の範囲は 2 ～ 3967 です。定義済みの L4 ~ L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。
ネットワーク ID（Network ID）	ネットワーク ID を指定します。有効な ID 値の範囲は 0 ~ 16777214 です。このフィールドの値が 0 の場合、ネットワーク識別子は自動的に生成されます。
サービス ネットワーク テンプレート	ドロップダウン リストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。

サービス アプライアンス **IP** セクション	
リバース トラフィックのサービス アプライアンス IP アドレス	リバース トラフィックの IPv4 サービスアプライアンスの IP アドレスを指定します。
リバース トラフィックのサービス アプライアンス IPv6 アドレス	リバース トラフィックの IPv6 サービスアプライアンスの IP アドレスを指定します。

例：ワンアーム仮想ネットワーク機能

ワンアーム モード仮想ネットワーク機能を導入するための [ルート ピアリングの作成（Create Route Peering）] ウィンドウのフィールドは、次のとおりです。

フィールド	説明
Peering Name	ピアリングの名前を指定します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。
デプロイ	[ワンアーム モード（One-Arm Mode）] を選択します。
ピアリング オプション	[静的ピアリング（Static Peering）] または [eBGP 動的ピアリング（eBGP Dynamic Peering）] を選択します。
ファースト アーム	

VRF	ドロップダウン リストから [VRF] を選択します。
サービスネットワーク	L4 ~ L7 サービス ネットワーク名を指定します。
VLAN ID	VLAN ID を指定します。有効な ID の範囲は 2 ～ 3967 です。定義済みの L4 ~ L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、[提案（Propose）] をクリックします。
ネットワーク ID（Network ID）	ネットワーク ID を指定します。有効な ID 値の範囲は 0 ~ 16777214 です。このフィールドの値が 0 の場合、ネットワーク識別子は自動的に生成されます。
サービス ネットワーク テンプレート	ドロップダウン リストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。
IPv4 ゲートウェイ/ネットマスク	IPv4 ゲートウェイとネットマスクを指定します。
ピアリングテンプレート	ドロップダウン リストから [service_static_route] または [service_ebgp_route] を選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。
リバース トラフィックのサービス アプライアンス IP アドレス	リバース トラフィックの IPv4 サービス アプライアンスの IP アドレスを指定します。
リバース トラフィックのサービス アプライアンス IPv6 アドレス	リバース トラフィックの IPv6 サービス アプライアンスの IP アドレスを指定します。

サービス ポリシーの作成

[サービス ポリシーの作成（**Create Service Policy**）**]** ウィンドウは、[サービス アプライアンスの追加（Adding a Service Appliance）] プロセスの 3 番目のステップとして表示されます。サービス アプライアンスを追加した後、次の場所に移動して **[**サービス ポリシーの 作成（**Create Service Policy**） **]** ウィンドウに移動することもできます。

[管理（Manage）] > [ファブリック（Fabrics）] > [ファブリックの概要（Fabric Overview）] > [サービス（Services）]

[サービス ポリシー（Service Policy）] タブをクリックし、**[アクション（Actions）] > [追加（Add）]** をクリックします。**[サービス ポリシーの作成（Create Service Policy）]** ウィンドウが表示されます。このウィンドウでアスタリスクが付いたフィールドに入力する必要があります。

1. **[ポリシー名（Name）]** フィールドにポリシーの名前を入力します。

   名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。

2. **[送信元ファブリック名（Source Fabric Name）]** フィールドで、[サービス アプライアンスの作成（Create Service Appliance ）] で選択したファブリックが表示されていることを確認します。
3. **[宛先ファブリック名（Destination Fabric Name）]** フィールドで、[サービス アプライアンスの作成（Create Service Appliance ）] で選択したファブリックが表示されていることを確認します。
4. トグルを使用して、サービス ポリシーをアタッチまたはデタッチします。サービス ポリシーがアタッチまたは有効化されると、対応するポリシーが VRF（テナント）、送信元、および宛先ネットワークに適用されます。
5. **[送信元 VRF 名（Source VRF Name）]** フィールドで、ドロップダウン リストから送信元 VRF を選択します。
6. **[接続先 VRF 名（Destination VRF Name）]** フィールドで、ドロップダウン リストから接続先 VRF を選択します。
7. **[+ ネットワークの追加（+ Add Network）]** をクリックします。

   [ネットワークの追加（Add Network）] ウィンドウが表示されます。

   a. **[送信元ネットワーク（Source Network）]** フィールドで、ドロップダウン リストから IP アドレスを選択します。

   b. **[宛先ネットワーク（Destination Network）]** フィールドで、ドロップダウン リストからネットワークを選択します。接続先ネットワークは、上記の送信元ネットワークとは異なる必要があります。

   c. **[保存（Save）]** をクリックします。
8. この機能を有効にするには、**[ePBR 統計情報の有効化（Enable ePBR Statistics）]** の横にあるボックスをオンにします。このフィールドは、

   NDFC リリース 12.2.1 で導入されました。
9. この機能を有効にするには、**[リバース ポリシーを有効にする（Enable Reverse Policy）]** の横にあるチェックボックスをオンにします。このフィールドは、NDFC リリース 12.2.1 で導入されました。
10. **[フローリダイレクトエントリ（Flow redirect entries）]** テーブルの下にある **[+ フロー リダイレクトの追加（+ Add Flow Redirect）]** をクリックします。**[フロー リダイレクトの追加（Add**

Flow Redirect）] ウィンドウが表示します。

11. 次の表を使用して、フロー リダイレクトの残りの構成を完了します。

フィールド	説明
アクセス コントロール リスト（ACL）	ドロップダウン リストからアクセス コントロール リストを選択します。オプションは、icmp、ip、tcp、および udp です。
ACL テンプレート	適切な ACL テンプレートを選択します。詳細については、「 ACL テンプレート」を参照して ください。
ACL 一致アクション	適切な ACL 一致アクションを選択します。次のオプションがあります。 ・ リダイレクト ・ ドロップ ・ 除外
サービスチェーニング名	サービス チェーン名を入力します。
+ サービス チェーニングの追加	クリックしてサービス チェーニングを追加します。
サービスチェーニングの追加	
アプライアンスの種類	サービス チェーンに適切なアプライアンス タイプをセレクトします。オプションは、[ファイアウォール (Firewall)]、[ロード バランサ (Load Balancer)]、または [仮想ネットワークの機能 (Virtual Networking Function)] です。
サービス アプライアンスの選択	サービス チェーンに適切なサービス アプライアンスを選択します。使用可能なオプションは、「サービス アプライアンスの 作成」の手順を使用して構成したサービス アプライアンスに基づいています。
Peering Name	サービス チェーンに適切なルート ピアリングを選択します。使用可能なオプションは、「ルート ピアリングの 作成」の手順を使用して構成したルートピアリングに基づいています。
失敗アクション	適切な失敗アクションを選択します。次のオプションがあります。 ・ 転送 ・ ドロップ ・ Bypass ・ なし
連続番号	シーケンス番号を入力します。
詳細設定	
ハッシュ方法	適切なハッシュ方法を選択します。次のオプションがあります。 ・ src-ip ・ dst-ip
ハッシュ バケット	ハッシュ バケットを入力します。2 の累乗。

12. **[保存（Save）]** をクリックします。

テンプレート （Templates）

ACL テンプレート

次のプローブ テンプレートは、NDFC リリース 12.2.1 以降で使用できます。

service_acl

L4 ~ L7 サービスの IP ACL テンプレート。

フィールド	説明
シーケンス番号（Sequence Number）	ACL のシーケンス番号を入力します。有効な範囲は 1 ~ 4294967295 です。
プロトコル	ACL に使用するプロトコルを指定します。次のオプションがあります。 ・ icmp ・ ip ・ tcp ・ udp
送信元 IP	ACL の送信元 IP アドレスを入力します。このエントリには、IPv4 アドレス、IPv6 アドレス、または any を指定できます。
宛先 IP	ACL の宛先 IP アドレスを入力します。このエントリには、IPv4 アドレス、IPv6 アドレス、または any を指定できます。
接続元ポート（Source Port）	送信元ポート番号を入力します（たとえば、*any* または *443*）。**[**プロトコル（**Protocol**）**]** フィールドで **ip** または **icmp** を選択した場合、このフィールドの値は無視されます。
接続先ポート（Destination Port）	宛先ポート番号を入力します（たとえば、*any* または *443*）。**[**プロトコル（**Protocol**）**]** フィールドで **ip** または **icmp** を選択した場合、このフィールドの値は無視されます。

プローブテンプレート

次のプローブ テンプレートは、NDFC リリース 12.2.1 以降で使用できます。

service_endpoint

L4-L7 サービスの ePBR サービス エンドポイント テンプレート。

フィールド	説明
一般的なパラメータ	
プローブの有効化	（反転された）ネクスト ホップアドレスのプローブを有効にするには、このボックスをオンにします。
プロトコル	プローブに使用するプロトコルを指定します。次のオプションがあります。 ・ icmp ・ tcp ・ udp ・ http
VRF ごとに自動作成されたループバックの使用	VRF ごとに自動作成されたループバックを使用するには、このボックスをオンにします。このオプションは、ファブリック設定で **[Per VRF Per VTEP Loopback Auto-Provisioning]** オプションが有効になっている場合にのみ適用されます。
送信元 ループバック インターフェイス IP	プローブ用に新しく作成したループバック インターフェイスの IP アドレスまたはアドレスをネットマスクとともに入力します。
送信元 ループバック インターフェイス IPv6	プローブ用に新しく作成されたループバック インターフェイスの IPv6 アドレスまたはネットマスク付きアドレスを入力します。
ポート番号	プローブのポート番号を入力します。有効な範囲：1 ~ 65535（推奨範囲：1025 ~ 65534）。
HTTP プローブのユーザー 入力	HTTP プ ローブのユーザー入力テキスト/ファイル名を入力します（例：http://192.168.50.254/index.html）。最大サイズ：99
詳細設定	
しきい値（Threshold）	しきい値（秒）を入力します。有効な範囲：1 ~ 60
頻度	頻度値を秒単位で入力します。有効な範囲：1 ~ 604800。
遅延 ダウン 変更履歴	遅延ダウン変更通知の値を秒単位で入力します。有効な範囲：1 ~ 180。
遅延 アップ 変更履歴	遅延アップ変更通知の値を秒単位で入力します。有効な範囲は 1 ~ 180 です。
タイムアウト（Timeout）	タイムアウト値を秒単位で入力します。有効な範囲：1 ~ 604800。

ルートピアリングサービスネットワークテンプレート

Service_Network_Universal

フィールド	説明
一般的なパラメータ	
IPv4 エニーキャスト ゲートウェイ/	サービス ネットワークのゲートウェイ IP アドレスとマスクを指定します。

ネットマスク	
IPv6 エニーキャスト ゲートウェイ/プレフィックス	サービス ネットワークのゲートウェイ IPv6 アドレスとプレフィックスを指定します。
VLAN 名	VLAN の名前を入力します。
インターフェイスの説明	インターフェイスの説明を入力します。
詳細設定	

ルーティングタグ	ルーティング タグを指定します。有効値の範囲は、0 ~ 4294967295 です。

ルートピアリングテンプレート

- [service_static_route]
- [service_ebgp_route]

service_static_route

フィールド	説明
スタティック ルート	**[静的ルート（Static Routes）]** フィールドにスタティックルートを入力します。回線ごとに 1 つのスタティックルートを入力できます。
エクスポート ゲートウェイ IP	ゲートウェイ IP（サービス ノード IP）アドレスをネクスト ホップアドレスとしてエクスポートするには、 をクリックします。

service_ebgp_route

フィールド	説明
一般的なパラメータ	
サービス ノードの IP アドレスまたはサブネット	IPv4 アドレスまたはネットマスク付きアドレスを指定します（たとえば、1.2.3.4 または 1.2.3.1/24）。 IPv4 または IPv6 アドレスは必須です。
ループバック IP	スイッチのループバックの IPv4 アドレスを指定します。ループバック IPv4 または IPv6 アドレスは必須です。
vPC ピアのループバック IP	ピア スイッチのループバックの IPv4 アドレスを指定します。シリアル番号が小さいスイッチがこの値を使用します。
エクスポート ゲートウェイ IP	ゲートウェイ IP（サービス ノード IP）アドレスをネクスト ホップアドレスとしてエクスポートするには、 をクリックします。
詳細設定	
サービス ノード の IPv6 アドレスまたはプレフィックス	ネイバーの IPv6 アドレスを指定します。
ループバック IPv6	スイッチのループバックの IPv6 アドレスを指定します。

vPC ピアのループバック IPv6	ピア スイッチのループバックの IPv6 アドレスを指定します。
ルートマップ タグ	インターフェイス ID に関連付けられているルート マップ タグを指定します。
インターフェイスの説明	インターフェイスの説明を入力します。
ローカル ASN	システム ASN を上書きするローカル ASN を指定します。
アドバタイズ ホスト ルート	エッジルータへの/ 32 および/ 128 ルートのアドバタイズメントを有効にします。
eBGP パスワードの有効化	eBGP パスワードを有効にするには、このオプションを選択します。 このオプションを有効にすると、次の **[**ファブリック設定から **eBGP** パスワードを継承（**Inherit eBGP Password from Fabric Settings**）**]** フィールドが自動的に有効になります。

ファブリック設定からの eBGP パスワードの継承	**[**ファブリック設定（**Fabric Settings**）**]** から eBGP パスワードを継承するには、このオプションを選挙します。 このオプションを有効にすると、次の **eBGP** パスワードと **[eBGP** 認証キー暗号化タイプ（**eBGP Authentication Key Encryption Type**）**]** フィールドが自動的に無効になります。
eBGP Password	上記の [ファブリック設定から eBGP パスワードを継承（ **Inherit eBGP** パスワード **from Fabric** 設定 ）] フィールドを有効にしなかった場合は有効になります。 有効になっている場合、暗号化された eBGP パスワードの 16 進文字列を指定します。
eBGP 認証キー暗号化タイプ	上記の [ファブリック設定から eBGP パスワードを継承（ **Inherit eBGP** パスワード **from Fabric** 設定 ）] フィールドを有効にしなかった場合は有効になります。 有効になっている場合は、BGP キー暗号化タイプを入力します。 ・**3**：3DES ・**7**：Cisco
[Enable Interface]	インターフェイスを無効にするには、このオプションをクリアします。デフォルトでは、インターフェイスは有効になっています。
vPC	
vPC ピア経由のピアリング- リンク	vPC ピアリンクを介して Per-VRF ピアリングを構成するには、このボックスをオンにします。 通常は、ファブリック レベルで **vPC advertise-pip** オプションを有効にします。ファブリック内のすべての vPC ペアに対して vPC アドバタイズピップ設定を行わない場合は、この **[vPC** ピア経由のピアリング（**Peering via vPC Peer-Link**） **]** オプションを活用します。このオプションは、レイヤ 4 ~ レイヤ 7 のデバイスを使用した共有ボーダー展開がある場合にも必要です。 このタブの残りのフィールドは、[vPC ピア経由のピアリング- リンク（Peering via vPC Peer-Link）] オプションが

	有効になる場合にのみ利用可能になります。
送信元 IP アドレス/ネットマスク	送信元 IP アドレスとネットマスクを指定します。たとえば、192.168.10.1/30 です。
宛先 IP アドレス	宛先 IP アドレスを指定します。たとえば、192.168.10.2 などです。シリアル番号が小さいスイッチがこの値を使用します。
送信元 IPv6 アドレス/プレフィックス	送信元 IPv6 アドレスとネットマスクを指定します。たとえば、2001:db9::1/120 です。
宛先 IPv6 アドレス	宛先 IPv6 アドレスを指定します。たとえば、2001:db9::10 です。シリアル番号が小さいスイッチがこの値を使用します。
vPC ピア間のピアリング用の VLAN	**vPC** 間の **VLAN** ピアリングの値を入力します（最小：**2**、最大：**4094**）。このフィールドに値が指定されていない場合、**VLAN ID** は 、ファブリック設定画面の [vPC] タブの [vPC ピア リンク VLAN 範囲（vPC Peer Link VLAN Range）] フィールドに表示される **VLAN** プールから自動的に割り当てられます。

サービスノードリンクテンプレート

- [service_link_trunk]
- [service_link_port_channel_trunk]
- [service_link_vpc]

service_link_trunk

フィールド	説明
一般的なパラメータ	
MTU	インターフェイスの MTU 値を指定します。デフォルトでは、ジャンボに設定されています。
SPEED	インターフェイスの速度を示します。デフォルトでは、これは[自動（Auto）]に設定されています。必要に応じて、サポートされている別の速度に変更できます。
トランク許可 VLAN	'none'、'all'、または VLAN 範囲を指定します。デフォルトでは、何も指定されていません。
BPDU ガードの有効化	ドロップダウン リストからオプションを指定します。使用可能なオプションは、true、false、または no です。デフォルトでは、no が指定されています。
ポート タイプ高速の有効化	このオプションをオンにすると、スパニング ツリー エッジ ポートの動作が有効になります。デフォルトでは有効になっています。
[Enable Interface]	このチェックボックスをオフにすると、インターフェイスが無効になります。デフォルトでは、インターフェイスは有効になっています。
詳細設定	
[送信元 インターフェイスの説明	送信元インターフェイスの説明を入力します。
宛先 インターフェイスの説明	宛先インターフェイスの説明を入力します。
[送信元 インターフェイスの自由形式構成（Source Interface Freeform Config）]	送信元インターフェイスの追加 CLI を入力します。
[宛先 インターフェイスの自由形式構成（Destination Interface Freeform Config）]	宛先インターフェイスの追加 CLI を入力します。

service_link_port_channel_trunk

フィールド	説明
ポート チャネル モード	ドロップダウンリストからポート チャネルを選択します。デフォルトでは、アクティブが指定されています。
BPDU ガードの有効化	ドロップダウン リストからオプションを選択します。使用可能なオプションは、true、false、または no です。
MTU	インターフェイスの MTU 値を指定します。デフォルトでは、ジャンボに設定されています。
トランク許可 VLAN	'none'、'all'、または VLAN 範囲を指定します。デフォルトでは、何も指定されていません。
ポート チャネルの説明	ポート チャネルの説明を入力します。
自由形式の構成	必要な自由形式の構成 CLI を指定します。

ポート タイプ高速の有効化	このオプションをオンにすると、スパニング ツリー エッジ ポートの動作が有効になります。デフォルトでは有効になっています。
ポートチャネルを有効にします	ポート チャネルを有効にするには、このオプションをオンにします。デフォルトでは有効になっています。

service_link_vpc

このテンプレートには指定可能なパラメータがありません。

サービスポリシーテンプレート

service_pbr

フィールド	説明
一般的なパラメータ	
プロトコル	ドロップダウンリストからプロトコル を選択します。オプションは、icmp、ip、tcp、および udp です。
接続元ポート（Source Port）	送信元ポート番号を指定します。ip または icmp が上の **[**プロトコル（**Protocol**）**]** フィールドで選択された場合、 この **[**送信元ポート（**Source Port**）**]** フィールドの値は無視されます。
接続先ポート（Destination Port）	宛先ポート番号を指定します。上記の **[**プロトコル（**Protocol**）**]** フィールドで ip または icmp を選択した場合、この **[**宛先ポート（**Destination Port**）**]** フィールドの値は 無視されます。
詳細設定	
ルートマップアクション	ドロップダウン リストからアクションを選択します。オプションは permit または deny です。**[**許可（**permit**）**]** を選択すると、一致したトラフィックはネクストホップ オプションと定義されたポリシーに基づいてリダイレクトされます。**[**拒否（**deny**）**]** を選択すると、トラフィックはルーティング テーブル ルールに基づいてルーティングされます。
ネクストホップオプション	ネクストホップのオプションを指定します。オプションは、none、drop-on-fail、および drop です。none を選択すると、一致したトラフィックは定義された PBR ルールに基づいてリダイレクトされます。drop-on-fail を選択すると、指定したネクストホップが到達不能な場合、一致したトラフィックはドロップされます。ドロップを選択すると、一致したトラフィックがドロップされます。
ACL 名	生成されたアクセス制御リスト（ACL）の名前を指定します。指定しない場合、これは自動生成されます。
リバーストラフィックの ACL 名	反転トラフィック用に生成される ACL の名前を指定します。指定しない場合、これは自動生成されます。
ルート マップ 一致番号	ルート マップの一致番号を指定します。有効な値の範囲は 1 ~ 65535 です。指定しない場合、ルートマップの一致シーケンス番号が事前定義されたリソースプールから取得されます。この番号は、ACL の名前に関連付けられます。
リバース トラフィックのルート マップ一致番号	リバース トラフィックのルートマップ一致番号を指定します。有効な値の範囲は 1 ~ 65535 です。指定しない場合、ルートマップの一致シーケンス番号が事前定義されたリソースプールから取得されます。この番号は、リバーストラフィック用に生成された ACL の名前に関連付けられます。

また、特定の要件に基づいてテンプレートをカスタマイズすることもできます。

ルートピアリング

[ルート ピアリング（**Route Peering**）] ウィンドウに移動するには、次の手順を実行します。

1. **[管理（Manage）] > [ファブリック（Fabrics）]** の順に選択します。
2. 適切な Data CenterVXLAN EVPN ファブリックをダブルクリックして、そのファブリックの **[ファブリックの概要（Fabric Overview）]** ウィンドウ
   が開きます。
3. そのファブリック の [サービス（**Services**）] タブをクリックします。
4. **[ルーティング ピアリング（Route Peering）]** タブをクリックします。

ルート ピアリングはサービス ネットワークを作成します。Nexus Dashboard ファブリック コントローラは、スタティック ルートと eBGP ベースのダイナミック ルート ピアリング オプションの両方をサポートします。サービス ネットワークを指定し、テナントのピアリング ポリシーを選択すると、Nexus ダッシュボード ファブリック コントローラは指定されたテナントの下にサービス ネットワークを自動的に作成します。このガイドでは、テナントと VRF という用語は同じ意味で使用されます。

サービス ネットワークは削除できません。サービス ネットワークの削除は、サービス ルート ピアリング削除プロセス中に自動的に処理されます。テナント/VRF ごとに複数のルート ピアリングを定義できます。

ルート ピアリングを作成するには、「ルート ピアリングの作成」を参照してください。

次の表で、**[ルート ピアリング（Route Peering）]** ウィンドウに表示されるフィールドについて説明します。

フィールド	説明
サービスネットワーク **1**	
サービスアプライアンス名	サービス アプライアンスの名前を指定します。
サービスアプライアンスのタイプ	サービス アプライアンスの tupe を指定します。 ・ファイアウォール ・ロード バランサ ・仮想ネットワーク機能
Peering Name	サービスのピアリング名を指定します **[ピアリング名（Peering Name）]** をダブルクリックして、詳細ウィンドウを表示します。詳細については、「ルート ピアリングの詳細」を参照してください。
デプロイ	展開のタイプを指定します。展開は次のいずれかになります。 ・テナント内ファイアウォール ・テナント間ファイアウォール ・ワンアームファイアウォール ・ワンアーム ロード バランサおよびツーアーム ロードバランサ ・ワンアーム VNF
ピアリング オプション	選択したピアリング オプションを指定します。

フィールド	説明
リモートピアリングが有効	リモート ピアリング オプションを有効にするかどうかを指定します。
ステータス	サービスのステータスを指定します。
添付ファイルの状態	サービスがアタッチされているか、デタッチされているかの状態を指定します。
アタッチされたファブリックの名前	サービス アプライアンスが接続されているファブリックの名前を指定します。
VRF	サービス アプライアンスにアタッチされている VRF の名前を指定します。
[ネットワーク名（Network Name）]	サービス アプライアンスに関連付けられたネットワークの名前を指定します。
Gateway IP	サービス アプライアンスのゲートウェイの IP アドレスを指定します。
サービスネットワーク **2**	
VRF	サービスにアタッチされている VRF の名前を指定します。
[ネットワーク名（Network Name）]	サービス アプライアンスに関連付けられたネットワークの名前を指定します。
Gateway IP	ゲートウェイ IP アドレスを指定します。
サービス アプライアンス IP	サービス アプライアンスに関連付けられたホップ IP アドレスを指定します。
リバース トラフィックのサービス アプライアンス IP アドレス	リバース トラフィックのサービス アプライアンス IP アドレスを指定します。
サービス アプライアンス IP IPv6	サービス アプライアンスに関連付けられた IPv6 アドレスを指定します
リバース トラフィックのサービス アプライアンス IPv6 アドレス	リバース　トラフィックのサービス アプライアンス IPv6 アドレスを指定します。
最終更新	サービス アプライアンスの最終変更日時を指定します。

次の表では、**[**アクション（**Actions**）**]** ドロップダウン リストにあるアクション項目について説明します。このリストは、
[ルートピアリング（**Route Peering**）**]** ウィンドウをに表示されます。

アクション項目	説明
追加（Add）	[追加（Add）] を選択します。**[**ルート ピアリングの作成（**Create Route Peering**）**]**ウィンドウが表示されます。 必要なパラメータを指定し、**[**保存（**Save**）**]** をクリックします。

編集	必要なピアリングを選択し、**[編集（Edit）]** をクリックします。ルート ピアリングの編集 ウィンドウが表示されます。 トグルを使用して、ルート ピアリングをアタッチまたはデタッチします。サービス ポリシーがアタッチまたは有効化されると、対応するポリシーが VRF（テナント）、送信元、および宛先ネットワークに適用されます。 必要なパラメータを指定し、**[保存（Save）]** をクリックします。
添付	特定のルート ピアリングをスイッチにアタッチするには、必要なピアリングを選択して、**[アタッチ（Attach）]** をクリックします。  ルート ピアリングの一括アタッチメント、デタッチメント、およびプレビュー 展開がサポートされ、最大 10 ルート ピアリングのみに制限されます。

アクション項目	説明
切断	特定のルート ピアリングをスイッチからデタッチするには、必要なピアリングを選択して、**[デタッチ（Detach）]** をクリックします。
プレビュー	プレビューを表示するには、必要なピアリングを選択して［プレビュー（Preview）］を クリックします。 **[ルート ピアリングのプレビュー（Preview Route Peering）]** ウィンドウが表示されます。 特定のスイッチ、ネットワーク、または VRF のルート ピアリングを表示するには、それぞれのドロップダウン リストから特定のスイッチ、ネットワーク、または VRF を選択します。**[閉じる（Close）]** をクリックして、ウィンドウを閉じます。
展開	ルート ピアリングを展開するには、必要なピアリングを選択し、**[展開（Deploy）]** をクリックします。 展開の確認のためのポップアップ ウィンドウが表示されます。クリックします。 **[展開（Deploy）]** をクリックします。
インポート	ルート ピアリング情報を Excel ファイルとしてインポートするには、**[インポート（Import）]** をクリックします。**[ルート ピアリングのインポート（Route Peering Import）]**ウィンドウが表示されます。 **[参照（Browse）]** をクリックして適切なファイルを選択し、**[インポート（Import）]** をクリックしてルート ピアリングに関する情報をインポートします。

エクスポート	ルート ピアリング情報を Excel ファイルとしてエクスポートするには、**[エクスポート（Export）]** をクリックします。**[ルート ピアリングのエクスポート（Route Peering Export）]**ウィンドウが表示されます。 **[エクスポート（Export）]** をクリックして、選択したルート ピアリングに関する情報をエクスポートします。
削除（Delete）	ルート ピアリングを削除するには、適切なルート ピアリングを選択し、**[削除（Delete）]** をクリックします。

ルート ピアリングの詳細

ルート ピアリングの詳細ウィンドウを表示するには、**[管理（ Manage）]**、**[ファブリック（Fabrics）]**、**[ファブリックの概要（Fabric Overview）]**、**[サービス（Services）]**、**[ルート ピアリング（Route Peering ）]** の順に選択し、ルート ピアリング名をダブルクリックします。ルート ピアリングの詳細ウィンドウが表示され、次のタブが表示されます。

ルートピアリング名...をダブルクリックします。[概要（Overview）]、[ステータスの詳細（Status Details）]、[サービス ポリシー（Service Policy）]、および [展開履歴（Deployment History）] タブは、ルート ピアリングの詳細画面に表示されます。

- 概要
- ステータスの詳細
- サービス ポリシー
- 導入履歴

[概要（Overview）]タブで

[概要（Overview）] タブには、**[ルート ピアリングの概要（Route Peering Summary）]** と、内部及び外部ネットワークの詳細、
[サービス ポリシー（Service Policies）]、および **[サービス アプライアンス（Service Appliance）]** がカードとして表示されます。

[ステータスの詳細（Status Details）] タブ

[ステータスの詳細（Status Details）] タブには、サービス ネットワークのリアルタイム ステータスとポリシー ステータスが、更新されたタイムスタンプとエンティティとともに表示されます。

[サービス ポリシー（Service Policy）] タブ

「サービス ポリシー」を参照してください。

[展開履歴（Deployment History）] タブ

このタブには、ルート ピアリングに関係するスイッチとネットワークの展開履歴が表示されます。このタブには、ネットワークの名前、VRF、スイッチ、ステータス、ステータス メッセージ、ステータスの詳細、実行時間などの情報が表示されます。

VNF サービス デバイスのリモート ピアリング

仮想ネットワーク機能（VNF）レイヤ 4 ~ レイヤ 7 サービス デバイスのリモート ピアリングをサポートします。これにより、VNF サービス アプライアンスのコントロール プレーン ピアリングを物理ポート アタッチメントから分離できます。

VNF サービス アプライアンスのルート ピアリングを構成するプロセスの一環として、デフォルトのサービス スイッチではなく、リモート リーフ、ボーダー、またはボーダー ゲートウェイ スイッチで eBGP ダイナミック ピアリングを指定するオプションがあります。また、レイヤ 4 ~ レイヤ 7 サービスの eBGP テンプレートへのアップデートを通じて、リモート ピアリング関連の構成をプッシュすることもできます。

リモート ピアリング機能により、VNF は eBGP ダイナミック ピアリングを介して複数のリモート リーフ、ボーダー、またはボーダー ゲートウェイスイッチとピアリングできます。リモート ピアリングの構成プロセスの一環として、ローカル ピアリングまたはリモート ピアリングのいずれかを選択し、リモート ピアリング用の eBGP テンプレートを使用してゲートウェイをエクスポートするかどうかを選択できます。リモート ピアリングの構成ステータスは、展開履歴とポリシー適用ステータスによって追跡されます。

注意事項と制約事項

- リモート ピアリング機能は、VNF サービス デバイスでのみサポートされます。
- リモート ピアリング機能は、eBGP ダイナミック ピアリングでのみサポートされます。
- VNF L4-L7 サービス デバイスを使用してローカル ピアリングまたはリモート ピアリングのいずれかを有効にできますが、VNF L4-L7 サービス デバイスとともにローカル ピアリングとリモート ピアリングの両方を有効にすることはできません。

リモート ピアリングの構成

VNF サービス デバイスのリモート ピアリングを構成するには、次の手順を実行します。

1. 「サービス アプライアンス の作成」に記載されている手順を使用して、通常どおりにサービス アプライアンスを構成します。

   特にリモート ピアリング機能の場合は、[サービス アプライアンスの作成（Create Service Appliance）] ステップで、[サービス アプライアンス タイプ（Service Appliance Type）] フィールドで [仮想ネットワーク機能（Virtual Networking Function）] を選択します。

2. [ルート ピアリングの作成（ Create Route Peering ）] ステップで、この機能専用の次の設定を使用して、通常どおりにルート ピアリングを構成します。

標準規格設定手順の詳細については、「ルート ピアリングの作成」と「ルート ピアリング」を参照してください。

特にリモート ピアリング機能については、次の構成を行ってリモート ピアリングを有効にし、複数のリモート スイッチとのダイナミックピアリングを定義します。

a. **[ピアリング オプション（Peering Option）]** フィールドで、**[EBGP ダイナミック ピアリング（EBGP Dynamic Peering）]** を選択します。

b. この機能を有効にするには、**[リモート ピアリングを有効にする（Enable Remote Peering）]** の横にあるボックスをクリックします。

> **[リモート ピアリングの有効化（Enable Remote Peering）]** フィールドは、**[ピアリング オプション（Peering Option）]** フィールドで **[EBGP ダイナミック ピアリング（EBGP Dynamic Peering）]** を選択した場合にのみ表示されます。

[リモート ピアリングの有効化（Enable Remote Peering）] 機能を有効にすると、**[リモートスイッチ（Remote Switches）]** フィールドが表示されます。

c. **[リモート スイッチ（Remote Switches）]** フィールドで、

[+ リモートスイッチの追加（+ Add Remote Switch）] をクリックします。**[リモート ピアリングの追加（Add Remote Peering）]** ウィンドウが表示されます。

d. リモート ピアリングを追加ために必要な情報を入力します。

フィールド	説明
リモートスイッチ	リモート ピアリングで使用するリモート スイッチを選択します。 サービス アプライアンスに対してローカルではないリーフ、ボーダー、またはボーダー ゲートウェイ スイッチのみが、このフィールドのオプションとして提供されます。 ・**[リモート スイッチ（Remote Switch）]** フィールドに single-switch オプション（ **leaf1-v** など）が表示されている場合は、これが単一のスタンドアロン リモート スイッチであることを意味します。 ・このフィールドにデュアル スイッチ オプション（たとえば、bgw1-v ~ bgw2-v）が表示されます。これは vPC ペアであることを意味します。
ピアリングテンプレート	リモート ピアリングで使用するピアリングテンプレートとして **service_ebgp_route** を選択します。 [service_ebgp_route] で提供される情報を使用して構成を完了します。

e. 必要に応じて、**[リモート ピアリングの追加（Add Remote Peering）]** ウィンドウで残りの設定を完了し、**[パスワードを 変更）]** をクリックします。

f. ルート ピアリング ポリシー ステータスの一部として追跡されるリモート ピアリング適用ステー

タスをビューします。

サービス ポリシー

任意または任意のネットワークでサービス ポリシーを定義し、境界スイッチの L3 ルーテッド インターフェイスに関連付けることができます。詳細については、「ボーダー スイッチの WAN インターフェイスでの PBR サポート 」を参照してください。L4 ~ L7 サービスは、ルート ピアリング中に定義されたサービス ネットワーク以外の VRF またはネットワークを作成しません。作成されたネットワーク間でサービス ポリシーを定義する場合、送信元と宛先のネットワークは、サブネット、個々の IP アドレス、またはファブリックの詳細画面の [サービス（**Services**）] タブで定義されたネットワークにすることができます。

[管理（Manage ）] > [ファブリック（Fabric）] を選択し、[ファブリック（Fabric）] の詳細ビューをクリックして、[サービス（Services）] タブを表示します。テナント内ファイアウォール、ワンアームおよびツーアームのロード バランサの場合、Nexus ダッシュボード ファブリック コントローラ の L4 ~ L7 サービスはサービスの挿入にポリシーベース ルーティング（PBR）を使用します。テナント間ファイアウォールにはサービス ポリシーがありません。必要なのは、サービス アプライアンスを作成し、テナント間ファイアウォールのピアリングをルーティングすることだけです。

送信元および宛先ネットワークはサービス ポリシーの展開とは関係なくアタッチまたは展開できるため、テナント/VRF 関連のサービス ポリシー構成は、サービス アプライアンスにアタッチされたスイッチにのみ接続またはプッシュされ、送信元および宛先ネットワークは更新されます。サービス ポリシー関連の構成を使用します。生成された設定をプレビューして確認できます。デフォルトでは、サービス ポリシーは定義されていますが、有効またはアタッチされていません。アクティブ化するには、サービス ポリシーを有効にするか、アタッチする必要があります。

送信元および宛先ネットワークが接続されている場合は、送信元および宛先ネットワークに関連するサービス構成が自動処理され、ネットワークがすでに接続または展開されている場合は自動更新されます。デフォルトでは、Nexus Dashboard ファブリック コントローラ は 5 分ごとに統計情報を収集し、集計および分析のためにデータベースに保存します。デフォルトでは、統計情報は最大 7 日間保存されます。

サービスの挿入は、作成されるフローでのみ有効です。既存のフローには影響ありません。有効なサービス ポリシーがそのネットワークに関連付けられている場合、ネットワークの削除は許可されません。

L4 ~ L7 サービス統合は、Easy ファブリック ポリシーを適用した上で構築されます。**[管理（Manage）] > [ファブリック（Fabrics）]** を選択し、VXLAN EVPN ファブリックを作成し、事前定義されたファブリック ポリシーを使用して Cisco Nexus 9000 シリーズ スイッチをファブリックにインポートします。

サービス ポリシーの作成については、「サービス ポリシーの作成」を参照してください。

次の表で、この **[サービス ポリシー（Service Policy）]** ウィンドウに表示されるフィールドについて説明します。

フィールド	説明
ポリシー名	サービスのポリシー名を指定します。 **[ポリシー名（Policy Name）]** をダブルクリックすると、詳細ウィンドウが表示されます。詳細については、「サービス ポリシーの詳細」を参照してください。
ルートピアリング	ルート ピアリング名を指定します。
ステータス	サービスのステータスを指定します。
添付ファイルの状態	サービスがアタッチされているか、デタッチされているかの状態を指定します。

Source VRF	サービス アプライアンスにアタッチされている VRF の名前を指定します
送信元ネットワーク	送信元ネットワークの名前を指定します。
フィールド	説明
宛先 VRF	サービス アプライアンスにアタッチされている宛先 VRF の名前を指定します。
宛先ネットワーク（Destination Network）	宛先ネットワークの名前を指定します。
サービス アプライアンス IP	サービス アプライアンスに関連付けられたホップ IP アドレスを指定します
リバース トラフィックのサービス アプライアンス IP アドレス	リバース トラフィックのサービス アプライアンス IP アドレスを指定します。
サービス アプライアンス IPv6	サービス アプライアンスに関連付けられた IPv6 アドレスを指定します
リバース Trafficv6 のサービス アプライアンス IPv6 アドレス	リバース トラフィックのサービス アプライアンス IPv6 アドレスを指定します。
Reverse Enabled	リバース トラフィックのサービス アプライアンスを有効にするかどうかを指定します。
ルートマップアクション	オプションは permit または deny です。 **[許可（permit）]** を選択すると、一致したトラフィックはネクストホップ オプションと定義されたポリシーに基づいてリダイレクトされます。 **[拒否（deny）]** を選択すると、トラフィックはルーティング テーブル ルールに基づいてルーティングされます。
ネクストホップオプション	ネクスト ホップのオプションを指定します。オプションは、**[none]**、**[drop -on-fail]**、および **[drop]**です。 **[none]** を選択すると、一致したトラフィックは定義された PBR ルールに基づいてリダイレクトされます。 **drop-on-fail** を選択すると、指定したネクストホップが到達不能な場合、一致したトラフィックはドロップされます。 ドロップを選択すると、一致したトラフィックがドロップされます。
最終更新日	サービス ポリシーが最後に更新された時刻を表示します。

次の表では、**[アクション（Actions）]** ドロップダウン リストにあるアクション項目について説明します。このリストは、
[サービス ポリシー（Service Policy）] ウィンドウに表示されます。

アクション項目	説明
追加（Add）	[追加（Add）] を選択します。**[サービス ポリシーの作成（Create Service Policy）]** ウィンドウが表示されます。

	必要なパラメータを指定し、**[保存（Save）]** をクリックします。
編集	必要なサービス ポリシーを選択し、**[編集（Edit）]** をクリックします。**[サービス ポリシーの編集（Edit Service Policy）]** ウィンドウが表示されます。 トグルを使用して、サービス ポリシーをアタッチまたはデタッチします。サービス ポリシーがアタッチまたは有効化されると、対応するポリシーが VRF（テナント）、送信元、および宛先ネットワークに適用されます。 必要なパラメータを指定し、**[保存（Save）]** をクリックします。

アクション項目	説明
添付	特定のサービス ポリシーをスイッチにアタッチするには、必要なポリシーを選択して **[アタッチ（Attach）]** をクリックします。 ルート ピアリングの一括 アタッチメント、 デタッチメント、 プレビューおよび 展開がサポートされ、最大 10 サービス ポリシーのみに制限されます。
切断	特定のサービス ポリシーをスイッチから切り離すには、必要なサービス ポリシーを選択し、**[デタッチ（Detach）]** をクリックします。
プレビュー	プレビューを表示するには、必要なピアリングを選択して［プレビュー（Preview）］を クリックします。 **[サービス ポリシーのプレビュー（Preview Service Policy）]** ウィンドウが表示されます。 特定のスイッチ、ネットワーク、または VRF のサービス ポリシーを表示するには、それぞれのドロップダウン リストから特定のスイッチ、ネットワーク、または VRF を選択します。**[閉じる（Close）]** をクリックして、ウィンドウを閉じます。
展開	サービス ポリシーを展開するには、必要なサービス ポリシーを選択し、[展開（Deploy）] をクリックします。 展開の確認のためのポップアップ ウィンドウが表示されます。クリックします。 [展開（Deploy）] をクリックします。
インポート	サービス ポリシー情報を Excel ファイルとしてインポートするには、**[インポート（Import）]** をクリックします。**[サービス ポリシーのインポート（Service Policy Import）]** ウィンドウが表示されます。 **[参照（Browse）]** をクリックして適切なファイルを選択し、**[インポート（Import）]** をクリックしてサービス ポリシーに関する情報をイ

	ンポートします。
エクスポート	ルート サービス ポリシー情報を Excel ファイルとしてエクスポートするには、[エクスポート（Export）] をクリックします。**[**サービス ポリシーのエクスポート（**Service Policy Export**）**]** ウィンドウが表示されます。 **[**エクスポート（**Export**）**]** をクリックして、選択したサービス ポリシーに関する情報をエクスポートします。
削除（Delete）	サービス ポリシーを削除するには、適切なサービス ポリシーを選択し、**[**削除（**Delete**）**]** をクリックします。

サービス ポリシーの詳細

サービス ポリシー ウィンドウを表示するには、**[**サービス（**Services**）**]** に移動し、必要なサービスの**[**名前（**Name**）**]** をダブルクリックします。サービス ポリシーの詳細ウィンドウが表示されます。このウィンドウでは、以下のタブを表示できます。

- 概要
- ステータスの詳細
- ルートピアリング
- サービス ポリシー

概要

[概要（Overivew）] タブには、内部および外部ネットワークの **[ポリシーの概要（Policy Summary）]**、**[サービス アプライアンス（Service Appliance）]**、および**[ルート ピアリング（Route Peering）]** が、カードとして表示されます。

ステータスの詳細

このタブには、選択したサービス ポリシーに関連付けられた **[リソース タイプ（Resource Type）]**、**[ファブリック名（Fabric Name）]**、**[リソース名（Resource Name）]** の詳細が表示されます。

統計情報

このタブには、構成されたサービス ポリシーに関する統計情報が表示されます。**[時間範囲（Time Range）]** ドロップダウン ボックスから、統計を表示する時間範囲を選択します。ウィンドウに表示されているカレンダーから日付と時刻を選択するには、ウィンドウの右下隅にある時間の選択をクリックします。過去 15 分、1 時間、6 時間、1 日、1 週間、1 か月の統計を表示することもできます。必要な時間範囲を選択し、**[適用（Apply）]** をクリックします。**[スイッチ（Switch）]** ドロップダウン リストから、統計を表示するスイッチを選択します。選択したスイッチの指定した時間範囲での統計が表示されます。

関連するすべてのスイッチの特定のポリシーの統計をリセットするには、**[統計のクリア（Clear Stats）]** をクリックします。複数のポリシーが同じルート マップを共有している場合、他のポリシーの統計も影響を受けます。

展開履歴の表示

このタブには、サービス ポリシーに関係するスイッチおよびネットワークの展開履歴が表示されます。このタブには、ネットワーク名、VRF、スイッチ名、ステータス、ステータス メッセージ、ステータスの詳細、実行時間などの情報が表示されます。

サービス アプライアンスの更新 36

[サービス アプライアンス（**Service Appliances**）**]** ウィンドウに表示されるサービス アプライアンスのリストを更新するには、
[更新（**Refresh**）**]** アイコンをクリックします。

監査履歴の表示

選択したサービス ポリシーまたはルート ピアリングに関連するスイッチおよびネットワークの監査履歴を表示するには、**[**サービス（**Services**）**]** ウィンドウの **[**監査履歴（**Audit History**）**]** タブをクリックします。

[監査履歴（Audit History）] ウィンドウの [監査ログ（Audit Logs）] テーブルには、実行されたすべてのアクションに関する情報が表示されます。

フィールド	説明
User Name	サービス アプライアンスのユーザー名を指定します。
ユーザー ロール	最新のアクションを実行したユーザー ロール名を指定します。
行われるアクション	最近実行したアクションを指定します。
エンティティ	サービス アプライアンスの名前を指定します。
詳細	サービス アプライアンスの詳細を指定します。
ステータス	サービス アプライアンスのステータスを示します。
時間	そのノードのアクション時間を指定します。
詳細	選択したサービス アプライアンスの詳細情報を表示するには、**[**詳細情報（ **More Info**）**]** をクリックします。

- サービス アプライアンス、ルート ピアリング、およびサービス ポリシーの作成
- サービス アプライアンス、ルート ピアリング、およびサービス ポリシーの削除
- サービス アプライアンス、ルート ピアリング、およびサービス ポリシーの更新
- ルート ピアリングの接続と切断、およびサービス ポリシー
- ルート ピアリングおよびサービス ポリシーの展開

上記のアクションが実行されるときに監査ログが生成され、この監査ログは、アクションを実行したユーザの名前、ユーザのロール、実行されたアクション、アクションが実行されたエンティティ、アクションの詳細、ステータス、およびアクションが実行されました。

古い監査レポートを削除するには、**[**アクション（**Action**）**] > [**変更履歴の消去（**Purge Audit History**）**]** をクリックし、最大保持日を指定して、削除を確認します。監査ログ エントリを削除できるのは管理者ロールを持つユーザーのみであることに注意してください。

サービス アプライアンスのインポート

Excel ファイルからサービス アプライアンスをインポートするには、次の手順を実行します。

1. **[**サービス アプライアンス（**Service Appliances**）**]** タブに移動します。

   [管理（**Manage**）**] > [**ファブリック（**Fabrics**）**] > [**ファブリックの概要（**Fabric Overview**）**] > [**サービス（**Services**）**] > [**サービス アプライアンス（**Service Appliances**）**]**

2. [アクション（**Actions**）**] > [**インポート（**Import**）**]** をクリックします。

   [サービス アプライアンスのインポート（**Service Appliance Import**）**]** ウィンドウが表示されます。

3. **[**参照（**Browse**）**]** をクリックして Excel ファイルをドロップし、**[**インポート（**Import**）**]** をクリックしてサービス アプライアンスに関する情報をインポートします。

   また、**[**アクション（**Actions**）**] > [**インポート（**Import**）**]** をクリックして、サービス アプライアンスに関するデータを Excel ファイルからインポートして、サービス アプライアンス レベルのデータを復元することもできます。

サービス アプライアンスのエクスポート

サービス アプライアンス レベルでデータをバックアップするには、**[**アクション（**Actions**）**] > [**エクスポート（**Export**）**]** オプションをクリックして、サービス アプライアンスに関するデータを Excel ファイルにエクスポートします。すべてのサービス アプライアンス、それぞれのルート ピアリング、およびサービス ポリシーに関するデータがエクスポートされます。

アプライアンスを選択し、[アクション（Actions）] > [エクスポート（Export）] をクリックして、特定のサービス アプライアンスのデータを
エクスポートすることもできます。確認ウィンドウが表示されます。**[**エクスポート（**Export**）**]** をクリックし ま す 。

サービス アプライアンスの編集

Cisco Nexus Dashboard Fabric Controller Web UI からサービス アプライアンスを編集するには、次の手順を実行します。

1. テーブルからサービス アプライアンスを選択し、**[**アクション（**Actions**）**] > [**編集（**Edit**）**]** をクリックします。
2. **[**サービス アプライアンスの編集（**Edit Service Appliance**）**]** ウィンドウが表示されます。必要な

   変更を行って、**[**保存（**Save**）**]** をクリックします。

サービス アプライアンスの削除

Cisco Nexus Dashboard Fabric Controller Web UI からサービス アプライアンスを削除するには、次の手順を実行します。

1. 削除する必要があるサービス アプライアンスにルート ピアリングまたはサービス ポリシーが関連付けられていないことを確認します。

   サービス アプライアンスに関連付けられているサービス ポリシーまたはルート ピアリングがある場合、サービス アプライアンスを削除する前にサービス アプライアンスに関連付けられているルート ピアリングまたはサービス ポリシーを削除する必要があることを示す警告が出され、削除がブロックされます。

2. テーブルからサービス アプライアンスを選択し、**[**アクション（**Actions**）**] > [**削除（**Delete**）**]** をクリックします。

著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

Cisco および Cisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。
商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/ go/trademarks でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。