ePBR L3 の構成

この章では、Cisco NX-OS デバイスで 拡張済みポリシーベース リダイレクト（ePBR）を構成する方法について説明します。

ePBR L3 に関する情報

Elastic Services Re-direction（ESR）の Enhanced Policy-based Redirect（ePBR）は、ポリシーベースのリダイレクト ソリューションを活用することで、NX-OX およびファブリック トポロジ全体でトラフィック リダイレクトとサービスチェーンを可能にします。余分なヘッダーを追加せずにサービスチェーンを可能にし、余分なヘッダーを使用する際の遅延を回避します。

ePBR は、アプリケーション ベースのルーティングを可能にし、アプリケーションのパフォーマンスに影響を与えることなく、柔軟でデバイスに依存しないポリシーベースのリダイレクト ソリューションを提供します。ePBR サービス フローには、次のタスクが含まれます。

ライセンス要件

Cisco NX-OS を動作させるには、機能とプラットフォームの要件に従って適切なライセンスを取得し、インストールする必要があります。

- 基本（Essential）ライセンスとアドオンライセンスが、さまざまな機能セットに使用できます。
- ライセンスは、製品および購入オプションに応じて、永続的、一時的、または評価用のものがあります。
- 高度な機能を使用するには、基本ライセンス以外の追加の機能ライセンスが必要です。
- 高度な機能を使用するには、基本ライセンス以外の追加ライセンスが必要です。

- ライセンスの適用と管理は、デバイスのコマンドライン インターフェイス（CLI）を介して行われます。

ライセンス タイプとインストールの手順の詳細については、『*Cisco NX-OS* ライセンシング ガイド』および『*Cisco NX-OS* ライセンシング オプション ガイド』を参照してください。

ePBR サービスとポリシーの構成

まず、サービスエンドポイントの属性を定義するePBRサービスを作成する必要があります。サービスエンドポイントは、スイッチに関連付けることができるファイアウォール、IPSなどのサービス アプライアンスです。また、サービス エンド ポイントの状態を監視するプローブを定義したり、トラフィック ポリシーが適用されるフォワード インターフェイスと reverse インターフェイスを定義することもできます。また ePBR は、サービスチェーンとともにロードバランシングもサポートします。 ePBR を使用すると、サービス構成の一部として複数のサービス エンド ポイントを構成できます。

サービス端末の障害が発生した場合、障害が発生したサービスエンドポイントにリダイレクトされていたトラフィックは、ePBR サービスで構成された他の到達可能なサービス エンドポイントにリダイレクトされます。復元力のあるハッシュは、複数のサービスエンドポイントで展開されたePBRサービスのエンドポイント障害時にサポートされます。常に特定のサービス エンドポイントにリダイレクトされていたトラフィックは、同じサービスの他のサービスエンドポイントで障害が発生した場合でも、同じデバイスに引き続きリダイレクトされます。

Cisco NX-OS リリース 10.2(1)F 以降、チェーン内のすべてのサービスの VRF は、一意であるか、完全に同一である可能性があります。サービスに定義されたサービスエンドポイントとインターフェイスは、サービスに定義された VRF に関連する必要があります。

既存のIPv4 PBRポリシーを持つサービス エンドポイント インターフェイスは、IPv4 ePBR サービス内では使用できません。同様に、既存の ipv6 PBR ポリシーを持つサービス エンドポイント インターフェイスは、IPv6 ePBR サービス内では使用できません。

ePBR サービスを作成したら、ePBR ポリシーを作成する必要があります。ePBR ポリシーを使用すると、トラフィックの選択、サービスエンドポイントへのトラフィックのリダイレクト、およびエンド ポイントの正常性障害に関するさまざまな fail-action メカニズムを定義できます。許可アクセス コントロール エントリ（ACE）を備えた IP access-list エンド ポイントを使用して、一致する対象のトラフィックを定義し、適切なアクションを実行できます。

ePBRポリシーは、複数のACL一致定義をサポートします。一致には、シーケンス番号によって順序付けできるチェーンに複数のサービスを含めることができます。これにより、単一のサービス ポリシーでチェーン内の要素を柔軟に追加、挿入、および変更できます。すべてのサービス シーケンスで、ドロップ、転送、バイパスなどの失敗時のアクション メソッドを定義できます。ePBR ポリシーを使用すると、トラフィックの詳細なロード バランシングを行うために、送信元または接続先ベースのロード バランシングとバケット数を指定できます。

ePBR のインターフェイスへの適用

ePBR ポリシーを作成したら、インターフェイスにポリシーを適用する必要があります。これにより、トラフィックが NX-OS または Nexus ファブリックに入るインターフェイスを定義できます。順方向と逆方向の両方にポリシーを適用することもできます。インターフェイスに適用される IPv4/IPv6 ポリシーは、順方向と逆方向の 2 つだけです。

Cisco NX-OS リリース 10.2(1)F 以降、ePBR はレイヤ 3 ポートチャネル サブインターフェイスでのポリシー アプリケーションをサポートしています

Cisco NX-OS リリース 10.2(1)F 以降、ePBR ポリシーが適用されるインターフェイスは、チェーン内のサービスの VRF とは異なる VRF にある場合があります。

ePBR IPv4 ポリシーは、IPv4 PBR ポリシーがすでに適用されているインターフェイスには適用できません。 ePBR IPv6 ポリシーは、IPv6 PBR ポリシーがすでに適用されているインターフェイスには適用できません。

バケットの作成およびロード バランシング

ePBR は、チェーン内でサービスエンドポイントの最大数を持つサービスに基づいてトラフィック バケットの数を計算します。ロード バランス バケットを構成する場合は事前に行ってください。ePBR は送信元 IP および接続先 IP のロード バランシングをサポートしますが、L4 ベースの送信元または接続先のロード バランシング メソッドはサポートしていません。

ePBR サービス エンドポイント アウトオブサービス

ePBR サービス エンド ポイントのアウト オブ サービス機能には、エンドポ イントをサービスから一時的に削除するオプションがあります。次の 2 つの方法を使用して、エンドポイントをアウト オブサービスに移行できます。

1. **[管理アウトオブサービス（Administrative Out-of-Service）]**：この方法は、メンテナンス中またはアップグレード中に、サービスエンドポイントを一時的に運用ダウン状態に移行し、ノードへのトラフィックの送信を回避しながら、サービス中の有効なエンドポイントデバイスとしてサービス エンド ポイントを維持するために使用されます。

   また、メンテナンス手順の完了後に、Cisco NX-OS スイッチでサービス エンド ポイントをインサービスに戻す機能も必要です。これは、今日の業界のロードバランサで使用される標準規格です。

2. **[自動アウトオブサービス（Auto Out-of-Service）]**：この方法は、障害発生後のエンドポイントの回復中に使用され、ePBR は再確立されたエンドポイントの到達可能性を検出し、フローのサブセットをノードにリダイレクトしようとします。

   また、特定のネットワークがまれなエンドポイントの障害と回復に耐性がある場合でも、接続を失い、接続を再確立しているエンドポイントを検出する必要がある場合、各イベントはエンドツーエンド接続を 2 回中断します。このようなノードをアウトオブサービスにすることが望ましい場合があります。

ePBR オブジェクト トラッキング、ヘルスモニタリング、および Fail-Action

ePBR は、サービスで構成されたプローブ タイプに基づいて SLA およびトラック オブジェクトを作成し、ICMP、TCP、UDP、DNS、HTTP などのさまざまなプローブとタイマーをサポートします。 ePBR はユーザ定義のトラックもサポートしており、ePBR に関連するミリ秒プローブを含むさまざまなパラメータでトラックを作成できます。

ePBR プローブ構成を適用する場合、ePBR は IP SLA プローブをプロビジョニングすることによりエンドポイントの正常性をモニタし、オブジェクトをトラックして IP SLA の到達可能性をトラックします。

サービス向け、または転送または reverse の各エンドポイント向けに、ePBR プローブ オプションを構成することが可能です。また、IP SLA セッションの送信元 IP に使用できるように、頻度、タイムアウト、再試行のアップ カウントとダウン カウント、および送信元ループバック インターフェイスを構成できます。リトライアップとダウンのカウントは、 **遅延アップ** と **遅延ダウンの**間隔を決定する頻度の乗数として使用されます。サービスエンドポイントが最初に障害または回復として検出されると、システムはこれらの間隔の満了後にこれらのイベントに対処します。任意のタイプのトラックを定義し、順方向または逆方向エンドポイントに関連付けることができます。同じトラック オブジェクトが、同じ ePBR サービスを使用するすべてのポリシーに再利用されます。

トラックを個別に定義し、ePBR の各サービス エンド ポイントにトラック ID を割り当てることができます。ユーザ定義のトラックをエンドポイントに割り当てない場合、ePBR はエンドポイントのプローブ メソッドを使用してトラックを作成します。エンドポイント レベルで定義されているプローブ メソッドがない場合、サービスレベルで構成されるプローブ メソッドを使用できます。

ePBR は、自身のサービスチェーンのシーケンスで次の fail-action メカニズムをサポートします。

- バイパス
- ドロップオンフェイル
- 転送

サービス シーケンスのバイパスは、現在のシーケンスで障害が発生した場合に、トラフィックは次のサービス シーケンスにリダイレクトされる必要があることを示しています。

サービス シーケンスのドロップオンフェイルは、サービスのすべてのサービスエンドポイントが到達不能となる場合に、トラフィックはドロップされる必要があることを示しています。

転送はデフォルトのオプションであり、現在のサービスに障害が発生した場合、トラフィックは通常のルーティング テーブルを使用する必要があることを示します。これはデフォルトの fail-action メカニズムです。

（注） 対称性が維持されるのは、fail-action バイパスがサービスチェーン内のすべてのサービス向けに構成された場合です。その他の fail-action シナリオでは、1 つまたはそれ以上の機能不全サービスが存在する場合、転送または reverse フローでの対称性は維持されません。

ePBR セッションベースの構成

ePBR セッションにより、次のサービス内のアスペクトのサービスまたはポリシーの追加、削除、変更が可能になります。サービス内とは、アクティブインターフェイスまたはポリシーに適用されているポリシーに関連付けられたサービスを示し、アクティブインターフェイス上で変更される、現在構成済みのサービスを示します。

- インターフェイスおよびプローブを備えたサービスエンドポイント
- reverse エンドポイントおよびプローブ
- ポリシーで一致
- 一致させるための負荷分散メソッド
- 一致シーケンスおよび fail-action

（注） ePBR セッションで、同じセッション内で 1 つのサービスから別のサービスにインターフェイスを移動することはできません。1 つのサービスから別のサービスにインターフェイスを移動させるには、次の手順を行います。

1. まず初めに、既存のサービスからインターフェイスを削除するための 1 つ目のセッションを実行します。
2. 既存のサービスにインターフェイスを追加するための 2 つ目のセッションを実行します。

ePBR マルチサイト

Cisco NX-OS リリース 10.2(1)F 以降、VXLAN マルチサイト ファブリックでのサービスチェーンは、次の構成およびトポロジ ガイドラインを使用して実現できます。

- サービス内のエンドポイントまたはチェーン内のサービスは、同じサイトまたは異なるサイト内の異なるリーフスイッチに分散される場合があります。
- すべてのサービスは、ePBR ポリシーが適用されるテナント VRF コンテキストとは異なる一意の VRF にある必要があります。
- 異なるテナント VRF のトラフィックを分離するには、サービスに使用される VLAN を分離し、新しいサービスとポリシーを定義する必要があります。

- テナント VRF ルートは、サービスをホストするすべてのリーフスイッチの各サービス VRF にリークする必要があります。これにより、トラフィックがサービスチェーンの最後でテナント VRF 内の接続先にルーティングされるようになります。
- VNI は、さまざまなリーフスイッチおよびサイトに対称的に割り当てる必要があります。
- ePBR ポリシーは、使用されているサービス VRF のすべてのレイヤー 3 VNI、サービスをホストしているすべてのリーフスイッチ、およびマルチサイトのトランジットとして機能している場合はボーダー リーフまたはボーダーゲートウェイ スイッチで有効にする必要があります。
- サービスチェーンが 1 つのサイトに完全に分離され、トラフィックがさまざまなサイトから着信する場合があります。このシナリオにはサービスデバイスのマルチサイト配布は含まれませんが、ボーダーゲートウェイまたはボーダーリーフ上のサービス VRF のレイヤー 3 VNI は、マルチサイト トランジットとしてのみ扱う必要があり、ePBR ポリシーをそれらに適用する必要があります。ePBR ポリシーは、トラフィックが着信するリモートサイトのホストまたはテナントに面したインターフェイスにも適用する必要があります。

ACL リフレッシュ

ePBR セッション ACL リフレッシュにより、ユーザが入力した ACL がACE を使用して変更、追加、または削除される場合に、ACL を生成するポリシーを更新することができるようになります。リフレッシュ トリガーで、ePBR はこの変更によって影響を受けるポリシーを特定し、それらのポリシー向けに ACL を生成するバケットを作成、削除、または変更します。

ePBR のスケール数については、『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

ePBR L3 の注意事項および制約事項

ePBR には、次の注意事項と制限事項 があります。

- L3 ePBR 機能が正しく機能するには、十分な ing-racl TCAMが必要です。現在の TCAM カービングを確認するには、**show hardware access-list tcam region** コマンドを使用します。適切な TCAM サイズが割り当てられていない場合は、 **hardware access-list tcam region ing-racl** *256* の倍数のサイズ コマンドを使用して、適切な TCAM サイズを割り当てます。
- Cisco Nexus NX-OS リリース 10.1(2) 以降、IPv4 および IPv6 を使用した ePBR は N9K-C93108TC-FX3P スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(1) 以降、ePBR ポリシーの各一致ステートメントは、リダイレクト、ドロップ、および除外の 3 つのアクション タイプをサポートできます。ポリシーごとにドロップまたは除外の一致ステートメントを 1 つだけ指定できます。順方向および逆方向で除外またはドロップする必要があるトラフィックの ACE ルールは、除外またはドロップのアクションで使用される match アクセスリストに手動で追加する必要がありま

す。exclude および drop match アクセス リストの統計情報には、両方向のトラフィック ヒット カウンタが表示される場合があります。

- ePBR ポリシーには、リダイレクト アクションとの一致が少なくとも 1 つ必要です。
- Cisco NX-OS リリース 10.1（1）以降、IPv4、IPv6、および VXLAN 上の ePBR を使用した ePBR は、次のプラットフォーム スイッチでサポートされます：N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX、N9K-C93180YC FX3S、N9K-C93360YC-FX3 と N9K-C93108TC-FX3P。
- fail-action がいずれかの一致ステートメントで指定されている場合、プローブは構成内に存在していることが必須です。
- OTM トラックの変更がある場合は常に、RPM の再プログラミングにより ePBR 統計がリセットされます。
- ePBR 構成内の複数の一致ステートメント全体で同じユーザ定義 ACL を共有しないでください。
- トラフィックの対称性が維持されるのは、fail-action バイパスが ePBR サービス向けに構成されたときのみです。サービスチェーン内の転送/ドロップなどのその他の fail-action の場合、トラフィックの順方向と逆方向のフローの対称性は維持されません。
- match access-list の定義に従ってトラフィックが任意の送信元 IP および s送信先 IP と一致する必要があり、VXLAN 環境に分散されたデバイスにリダイレクトする必要がある場合は、一意のレイヤ 4 送信元および宛先ポートパラメータを一致フィルタに指定する必要があります。順方向と逆方向の両方で、またはワンアームデバイスを介してサービスチェーンされます。
- 機能 ePBR および機能 ITD は同じ入力インターフェイスと共存できません。
- 拡張済み ePBR 構成では、**no feature epbr** コマンド を使用する前にポリシーを削除することが推奨されています。
- プローブ トラフィックを別の CoPP クラスに分類することが推奨されています。そうしないと、プローブ トラフィックはデフォルトの CoPP クラスになり、ドロップされる可能性があり、プローブ トラフィックの IP SLA バウンスが発生します。CoPP 構成について詳しくは、「IP SLA パケットの CoPP の構成」を参照してください。
- ePBR は、EX、FX、および FX2 ラインカードを備えた Cisco Nexus 9500 および Cisco Nexus 9300 プラットフォーム スイッチでサポートされています。
- Cisco NX-OS リリース 9.3(5) 以降、Catena 機能は廃止されました。
- システムから削除されたポートチャネルに構成された ePBR サービスエンドポイントを削除する場合、次の手順を実行してください。

  1. 既存の ePBR ポリシーを削除します。
  2. 既存の ePBR サービスを削除します。
  3. ePBR サービス エンドポイントを必要なポートチャネルに再構成します。

- 「epbr_」という名前で始まる、動的に作成された ePBR の access-list エントリは変更しないでください。これらの access-lists は ePBR 内部使用向けに予約済みです。

（注） これらのプレフィックス文字列を変更すると ePBR が正しく機能せず、ISSU に影響を与える可能性があります。

- ルータ ACL は、サポートされているレイヤ 3 インターフェイスでレイヤ 3 ePBR ポリシーとともに有効にできます。この制限の詳細については、『**Cisco 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**』の「ポリシーベース ルーティング」の章にある「ポリシーベース ルーティングの注意事項と制限事項」を参照してください。
- Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、および N9K-C9364C-GX スイッチでは、Cisco NX-OS、リリース 10.2 以降のリリースからリリース 10.1 への ISSD を実行する前に、ePBR ポリシーを無効にして、ダウングレードを続行します。
- ePBR ポリシー定義は、順方向および逆方向でサポートされているインターフェイス タイプの最大 32 個のインターフェイスに適用できます。
- Cisco NX-OS リリース 10.4（1）F 以降、ePBR は、Cisco Nexus 9300-FX2/FX3/GX/GX2 プラットフォーム スイッチでのロードバランシングとリダイレクションのために、GRE および IP-IP トンネル インターフェイスで IPv4 および IPv6 ポリシーをサポートします：
- Cisco NX-OS リリース 10.4（1）F 以降、ePBR は、Cisco Nexus 9300-FX2/FX3/GX/GX2 プラットフォーム スイッチの IP-IP および GRE トンネル インターフェイスを介して到達可能なレイヤ3エンドポイントへのリダイレクションまたはロードバランシングをサポートします。

（注）
- ePBR IPv6 ポリシーは、IP-IP トンネル インターフェイスではサポートされません。
- 現在、ePBR は、IP-IP および GRE トンネルを介して到達可能なデバイスへのサービスチェーンをサポートしていません。

- 構成のロールバックと設定の置換は、ePBR ポリシーがインターフェイスに関連付けられておらず、ePBR サービス定義が送信元設定とターゲット設定の両方のアクティブな ePBR ポリシーで使用されていない場合にのみサポートされます。ただし、構成のロールバックと構成の置換では、ポリシーとインターフェイスの関連付けおよび関連付け解除はサポートされません。
- アトミック アップデートを無効にすると、より多くの TCAM リソースを ePBR ポリシーで使用できるようになりますが、ポリシーの構成変更中、またはサービス エンドポイントのフェイルオーバーとリカバリ中に、トラフィック中断の原因となる可能性があります。詳細については、*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ設定ガイドの**アトミック ACL 更新**を参照してください。

- ePBR ポリシーが設定されているすべてのインターフェイスに対して、一意のポリシーが生成されます。さらに、ePBR ポリシー内で一致するように構成されたサービスチェーン内の次のサービス機能にトラフィックを誘導する必要があるすべてのサービス インターフェイスに対して、一意のポリシーも生成されます。サポートされる EPBR ポリシーの規模は、PBR ポリシーのシステムで使用可能な ACL ラベルによって異なる場合があります。ACL ラベル サイズの詳細については、 *Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ構成ガイドの **ACL タイプでサポートされる最大ラベルサイズ**の項を参照してください。
- 使用される ePBR サービスまたはエンドポイント保留タイマーは、使用中のプローブ（トラックおよび IP SLA）の頻度およびタイムアウトと互換性がある必要があります。これにより、障害を時間内に検出できます。
- デュアルアーム デバイスのフォワード アームとリバース アームのエンドポイントの状態は、自動的に同期されません。これが必要な場合は、フォワード アームとリバース アームで同じプローブ トラック構成を使用する必要があります。エンドポイント用に設定されたプローブ トラックは、同じエンドポイントのフォワード アームとリバース アームの間で共有できますが、同じサービスまたは異なるサービスのエンドポイント間では共有できません。
- Cisco NX-OS リリース 10.5(1)F 以降では、ワンアーム サービス デバイスのリバース IP アドレスを明示的に構成する必要はなくなりました。サービス エンドポイントにリバース IP アドレスが割り当てられていない場合、ワンアームデバイスとして扱われ、トラフィックは順方向と逆方向の両方で同じ IP アドレスにリダイレクトされます。
- サービス プローブに関連付けられているループバック インターフェイスの IP アドレスが変更された場合は、サービスを参照するポリシーとコントラクトを削除して再適用する必要があります。
- Cisco NX-OS リリース 10.5(2)F 以降、ePBR は、Cisco Nexus 9300-FX2、FX3、GX、GX2、H2R、および H1 シリーズ スイッチの指定された VRF インスタンスを介してパケットをリダイレクトする **set-vrf** コマンドをサポートしますが、次の制限があります：
  - **source-vrf** および **destination-vrf** は、ePBR セッションを介して変更または削除することはできません。
  - **set-vrf** はVXLAN 上の ePBR ではサポートされていません。
  - **set-vrf** は、ドロップおよび除外トラフィックの VRF を切り替えません。

次の注意事項および制約事項を VXLAN 上での ePBR 機能に適用します。

- VXLAN ファブリックでは、同じ VLAN 内のデバイスに対してサービスチェーンを実行できません。すべてのデバイスは、個別の VLAN に存在する必要があります。
- チェーン内のすべてのサービスが同じ VRF にある場合、ePBR は VXLAN マルチサイト ファブリックの単一サイトでのみサポートされます。
- チェーン内のすべてのサービスが同じ VRF にある場合：

- アクティブ/スタンバイ チェーンは、制限のない 2 つのサービス ノードでサポートされます。
- チェーン内に3つ以上のサービス ノードがあるアクティブ/スタンバイ チェーンでは、同じサービス リーフの背後にあるタイプの異なる 2 つのノードは必要ありません。
- VXLAN ファブリックでは、リーフ内の 1 つのサービスからのトラフィックをステッチして、後で同じリーフに戻ってくることはできません。

（注） チェーン内のすべてのサービスが異なる VRF コンテキストにある場合、これらの制限は適用されません。

- サービス エンドポイントが VXLAN 環境または VPC ピアに分散されている場合、サービス エンドポイントはすべてのスイッチで同じ順序で構成する必要があります。
- VXLAN環境に分散されたサービスエンドポイントの場合、一意の送信元IPをIP SLAセッションに使用できるように、プローブの送信元ループバック インターフェイスを設定する必要があります。
- ePBR ポリシーは、最初は常にホストまたはテナントに面したインターフェイスに適用する必要があります。ePBR ポリシーは、トランジット インターフェイスとしてのみ、テナントまたはサービス VRF に関連するレイヤ 3 VNI インターフェイスに適用する必要があります。

  特定の VRF のエンドポイントに着信するトラフィックのみが、その VRF に関連するレイヤ 3 VNI インターフェイスに適用されるポリシーによってリダイレクトされます。レイヤ 3 VNI インターフェイスのポリシーに一致するトラフィックの統計情報は、ePBR statistics コマンドでは表示されません。
- Cisco NX-OS リリース 10.3（3）F 以降では、Cisco Nexus 9300-FX、9300-FX2、9300-FX3、9300-GX、および9300-GX2 プラットフォーム スイッチ、の新しい L3VNI インターフェイスに ePBR レイヤ 3 ポリシーを適用できます。

次の注意事項および制約事項を一致 ACL 機能に適用します。

- permit メソッドを持つ ACE のみが ACL でサポートされます。他の方法（deny または remark など）の ACE は無視されます。
- 1 つの ACL で最大 256 の許可 ACE がサポートされます。
- 送信元パラメータまたは宛先パラメータのいずれかでアドレス グループまたはポート グループとして指定されたオブジェクト グループを持つ ACE はサポートされません。
- Cisco NX-OS リリース 10.4（1）F 以降では、match access-list ルールのレイヤ 4 ポート範囲およびその他のポート操作（「等しくない」、「より大きい」、「より小さい」など）は、バケットアクセスリスト内のトラフィックのフィルタリングに使用されます。

- アクセスリストでレイヤ 4 ポートオペレータを使用しながら、TCAM ACE の使用率を最適化するには、この構成 **hardware access-list lou resource threshold**を使用する必要があります。このコマンドの詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ構成ガイド』の「**IP ACL の構成**」のセクションを参照してください。

次のガイドラインと制限事項が VRF 間のサービスチェーンに適用されます。

- Cisco NX-OS 10.2(1)F リリース以降、チェーン内のすべてのサービスは、同じ VRF または完全に一意の VRF に存在する必要があります。
- バージョン 10.2(1)F では、チェーン内のすべてのサービスが一意の VRF に存在する場合、fail-action アクション バイパス メカニズムはサポートされません。
- Cisco NX-OS 10.2(2)F リリースから、チェーン内のサービスが一意の VRF にある場合に fail-action アクション バイパスがサポートされます。
- サービスが、ePBR ポリシーが適用されるインターフェイスの VRF コンテキストとは異なる VRF にある場合、ユーザは、テナント ルートがすべてのサービス VRF にリークされていることを確認して、トラフィックがサービスチェーンの最後にあるテナント VRF にルート バックできるようにする必要があります。
- Cisco NX-OS リリース 10.2(2)F 以降、PBR では、異なる VRF に関連する複数のバックアップ ネクストホップをルート マップ シーケンスに構成できます。これにより、ePBR は、ある VRF に関連するサービスから別の VRF への fail-action バイパスを効果的に有効にすることができます。
- Cisco NX-OS リリース 10.2(3)F 以降、エンドポイントの追加、サービス シーケンスの追加、削除および変更のセッション操作中のトラフィックの中断を最小限にするために、事前にロードバランス バケットの構成を行い、ロードバランス構成への変更を回避することが推奨されています。ロードバランス向けに構成されたバケットの数が、チェーン内の各シーケンス向けのサービスで構成されたエンドポイントの数より多くなるようにしてください。

送信元 IP ベースのロード バランシングを使用して ePBR を構成した場合は、次の注意事項と制限事項が適用されます。

- ACE の送信元 IPv4 のプレフィックス長を /32 にすることはできません
- ACE の送信元 IPv6 アドレスのプレフィックス長を /128 にすることはできません
- 送信元アドレスのサブネットは、構成されたバケットと互換性がある必要があります。

送信先 IP ベースのロード バランシングを使用して ePBR を構成した場合は、次の注意事項と制限事項が適用されます：

- ACE の送信先 IPv4 のプレフィックス長を /32 にすることはできません
- ACE の送信先 IPv6 アドレスのプレフィックス長を /128 にすることはできません
- 送信先アドレスのサブネットは、構成されたバケットと互換性がある必要があります。

ePBR サービス エンドポイントのアウトオブサービス機能を構成している場合は、次の注意事項と制限事項が適用されます。

- ePBR サービスエンドポイントのアウトオブサービス機能は、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2および X97160YC-EX、9700-FX/GX ライン カードを搭載した isco Nexus 9500 スイッチのレイヤ 3 サービスでサポートされます。
- ePBR アウトオブサービス（シャットダウンまたはホールドダウン）では、エンドポイントレベルまたはサービスレベルのいずれかで、エンドポイントにプローブを構成する必要があります。
- サービスがアクティブなポリシーによって使用されている場合、ePBR アウトオブサービス（シャットダウンまたはホールドダウン）は、 **epbr sessions**のみを使用して設定する必要があります。

送信元 IP ベースのロード バランシングおよび複数のエンドポイントへのロード バランシング トラフィックを使用する場合は、次のガイドラインと制限事項が適用されます。

- match access-list 内の ACE の送信元 IPv4 サブネット マスクを /32、または match access-list 内の送信元 IPv6 アドレスのサブネット マスクを /128 にすることはできません。
- match access-list 内の ACE の接続先 IPv4 サブネット マスクを /32、または match access-list 内の送信元 IPv6 アドレスのサブネット マスクを /128 にすることはできません。
- ロードバランシング メソッドに基づく、一致アクセスリスト内の送信元アドレスまたは接続先アドレスのサブネットマスクは、一致に使用されるサービスのエンドポイント数に基づき、一致するように構成されたバケットと互換性を持つか、必要なバケット数と互換性を持つか必要があります。

ePBR L3 の構成

はじめる前に

ePBR 機能を構成する前に、IP SLA および PBR 機能が構成されていることを確認してください。

ePBR サービス、ポリシーの構成およびインターフェイスへの関連付け

次のセクションでは、ePBR サービス、ePBR ポリシーの構成、およびインターフェイスへのポリシーの関連付けについて説明します。

手順の概要

1. **configure terminal**
2. **epbr service** *service-name*

3. [**no**] **probe** {**icmp** | *l4-proto port-number* [**control** *status*] | **http get** [*url-name* [**version** *ver*] | **dns host***host-name* **ctp**} [**frequency** *freq-num* | **timeout** *seconds* | **retry-down-count** *down-count* | **retry-up-count** *up-count* | **source-interface** *src-intf* | **reverse** *rev-src-intf*]
4. **vrf** *vrf-name*
5. **service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*]
6. **probe track** *track ID*
7. **reverse ip** *ip address* **interface** *interface-name interface-number*
8. **exit**
9. **epbr policy** *policy-name*
10. **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] } [**redirect** | **drop** | **exclude**]
11. [**no**] **load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *sequence-number*] [**mask-position** *position-value*]
12. *sequence-number* **set service** *service-name* [**fail-action** { **bypass** | **drop** | **forward**}]
13. **interface** *interface-name interface-number*
14. **epbr** { **ip** | **ipv6**} **policy** *policy-name* [**reverse**]
15. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**epbr service** *service-name* 例： `switch(config)# epbr service firewall`	新しい ePBR サービスを作成します。
ステップ 3	[**no**] **probe** {**icmp**	*l4-proto port-number* [**control** *status*]	**http get** [*url-name* [**version** *ver*]	**dns host***host-name* **ctp**} [**frequency** *freq-num*	**timeout** *seconds*	**retry-down-count** *down-count*	**retry-up-count** *up-count*	**source-interface** *src-intf*	**reverse** *rev-src-intf*] 例： `switch(config)# probe icmp`	ePBR サービスのプローブを構成します。サポートされるプローブ タイプは、ICMP、TCP、UDP、DNS、および HTTP、CTP です。 オプションは次のとおりです。 • 頻度：プローブの頻度を秒単位で指定します。値の範囲は 1 ～ 604800 です。 • 再試行ダウン カウント：ノードがダウンしたときにプローブによって実行される再カウントの数を指定します。指定できる範囲は1～5です。

	コマンドまたはアクション	目的
		• 再試行アップ カウント：ノードが復帰したときにプローブが実行する再カウントの数を指定します。指定できる範囲は 1 ～ 5 です。 • タイムアウト：タイムアウト期間を秒単位で指定します。値の範囲は 1 ～ 604800 です。
ステップ 4	**vrf** *vrf-name* 例： `switch(config)# vrf tenant_A`	ePBR サービスの VRF を指定します。
ステップ 5	**service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*] 例： `switch(config-vrf)# service-endpoint ip 172.16.1.200 interface VLAN100`	ePBR サービスのサービスエンドポイントを構成します。 手順 2 ～ 5 を繰り返して、別の ePBR サービスを構成できます。
ステップ 6	**probe track** *track ID* 例： `switch(config-vrf)# probe track 30`	トラックを個別に定義し、ePBR の各サービス エンドポイントに既存のトラック ID を割り当てます。 各エンドポイントにトラック ID を割り当てることができます。
ステップ 7	**reverse ip** *ip address* **interface** *interface-name interface-number* 例： `switch(config-vrf)# reverse ip 172.16.30.200 interface VLAN201`	トラフィック ポリシーが適用される reverse IP とインターフェイスを定義します。 （注） Cisco NX-OS リリース 10.5(1)F 以降では、ワンアーム サービス デバイスのリバース IP アドレスを明示的に構成する必要はなくなりました。サービス エンドポイントにリバース IP アドレスが割り当てられていない場合、ワンアーム デバイスとして扱われ、トラフィックは順方向と逆方向の両方で同じ IP アドレスにリダイレクトされます。
ステップ 8	**exit** 例： `switch(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 9	**epbr policy** *policy-name* 例： `switch(config)# epbr policy Tenant_A-Redirect`	ePBR ポリシーを構成します。

	コマンドまたはアクション	目的
ステップ 10	**match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] } [**redirect** | **drop** | **exclude**] 例： `switch(config)# match ip address WEB`	IPv4 または IPv6 アドレスを IP、または IPv6 ACL と照合します。リダイレクトは、一致トラフィックのデフォルト アクションです。ドロップは、着信インターフェイスでトラフィックをドロップする必要がある場合に使用されます。除外オプションは、着信インターフェイスのサービスチェーンから特定のトラフィックを除外するために使用されます。 この手順を繰り返して、要件に基づいて複数の ACL を一致させることができます。
ステップ 11	[**no**] **load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *sequence-number*] [**mask-position** *position-value*] 例： `switch(config)# load-balance method src-ip mask-position 3`	ePBR サービスで使用されるロードバランス メソッドとバケット数を計算します。 Cisco NX-OS リリース 10.3（3）F 以降では、ユーザー定義 ACL でロードバランシングに使用されるビットを選択する**mask-position** オプションが提供されています。デフォルト値は 0 です。 mask-position が構成されている場合、ロードバランス ビットは構成された mask-position から始まります。必要なバケットの数に基づいて、最上位ビットに向かって、より多くのビットがロード バランシング バケットを生成するために使用されます。 （注） ユーザー定義の ACL 内の ACE では、ロード バランシング バケットの生成に使用されるビットがユーザー定義のサブネットと重複している場合、ACE のマスク位置は内部的に 0 にリセットされます。
ステップ 12	*sequence-number* **set service** *service-name* [**fail-action** { **bypass** | **drop** | **forward**}] 例： `switch(config)# set service firewall fail-action drop`	fail-action メカニズムを計算します。

ステップ 13	**interface** *interface-name interface-number*
	例：
	`switch(config)# interface vlan 2010`
	`switch(config)# interface vni500001`
		インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
		（注）
		Cisco NX-OS リリース 10.3（3）F 以降では、新しい L3VNI インターフェイスに ePBR L3 ポリシーを適用できます。

	コマンドまたはアクション	目的
ステップ 14	**epbr** { **ip** | **ipv6**} **policy** *policy-name* [**reverse**] 例： `switch(config-if)# epbr ip policy Tenant_A-Redirect`	インターフェイスは、いつでも次の1つ以上に関連付けることができます。 • 順方向の IPV4 ポリシー • 逆方向の IPv4 ポリシー • 順方向の IPv6 ポリシー • 逆方向の IPv6 ポリシー
ステップ 15	**exit** 例： `switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

ePBR セッションを使用したサービスの変更

次の手順では、ePBR セッションを使用してサービスを変更する方法を説明しています。

手順の概要

1. **epbr session**
2. **epbr service** *service-name*
3. [**no**] **service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*]
4. **service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*]
5. **reverse ip** *ip address* **interface** *interface-name interface-number*
6. **commit**
7. **abort**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**epbr session** 例： `switch(config)# epbr session`	ePBR セッション モードに入ります。
ステップ 2	**epbr service** *service-name* 例： `switch(config-epbr-sess)# epbr service TCP_OPTIMIZER`	ePBR セッション モードで構成する ePBR サービスを指定します。

	コマンドまたはアクション	目的
ステップ 3	[**no**] **service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*] 例： `switch(config-epbr-sess-svc)# no service-end-point ip 172.16.20.200 interface VLAN200`	ePBR サービス向けに構成されたサービスエンドポイントを無効にします。
ステップ 4	**service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*] 例： `switch(config-epbr-sess-svc)#service-end-point ip 172.16.25.200 interface VLAN200`	サービスエンドポイントを変更し、ePBR サービスの IP を置き換えます。
ステップ 5	**reverse ip** *ip address* **interface** *interface-name interface-number* 例： `switch(config-epbr-sess-svc-ep)# reverse ip 172.16.30.200 interface VLAN201`	トラフィック ポリシーが適用される reverse IP とインターフェイスを定義します。
ステップ 6	**commit** 例： `switch(config-epbr-sess)# commit`	ePBR セッションを使用した ePBR サービスの変更を完了します。 （注） このステップの完了後に ePBR セッションを再起動します。
ステップ 7	**abort** 例： `switch(config-epbr-sess)# abort`	セッションを中止し、セッションの現在の構成をクリアまたはリセットします。コミット中にエラーまたはサポートされていない構成が識別された場合に、現在のセッション構成を破棄するには、このコマンドを使用します。 （注） その後、修正した構成を使用して新しい ePBR セッションを再開します。

ePBR セッションを使用したポリシーの変更

次の手順では、ePBR セッションを使用してポリシーを変更する方法について説明します。

手順の概要

1. **epbr session**
2. **epbr policy** *policy-name*
3. [**no**] **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] [**l2 address** *ipv6 acl-name*]} **vlan** {**vlan** | **vlan range** | **all**} [**redirect** | **drop** | **exclude**] }

4. **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] [**l2 address** *ipv6 acl-name*]} **vlan** {**vlan** | **vlan range** | **all**} [**redirect** | **drop** | **exclude**] }
5. *sequence-number* **set service** *service-name* [**fail-action** { **bypass** | **drop** | **forward**}]
6. [**no**] **load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *sequence-number*] [**mask-position** *position-value*]
7. **commit**
8. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**epbr session** 例： `switch(config)# epbr session`	ePBR セッション モードに入ります。
ステップ 2	**epbr policy** *policy-name* 例： `switch(config-epbr-sess)# epbr policy Tenant_A-Redirect`	ePBR セッション モードで構成する ePBR ポリシーを指定します。
ステップ 3	[**no**] **match** { [**ip address** *ipv4 acl-name*]	[**ipv6 address** *ipv6 acl-name*] [**l2 address** *ipv6 acl-name*]} **vlan** {**vlan**	**vlan range**	**all**} [**redirect**	**drop**	**exclude**] } 例： `switch(config-epbr-sess-pol)# no match ip address WEB`	IP または IPv6 ACL に対する IP アドレスの照合を無効にします。
ステップ 4	**match** { [**ip address** *ipv4 acl-name*]	[**ipv6 address** *ipv6 acl-name*] [**l2 address** *ipv6 acl-name*]} **vlan** {**vlan**	**vlan range**	**all**} [**redirect**	**drop**	**exclude**] } 例： `switch(config-epbr-sess-pol)# match ip address HR`	IP または IPv6 ACL に対する IP アドレスの照合を変更します。
ステップ 5	*sequence-number* **set service** *service-name* [**fail-action** { **bypass**	**drop**	**forward**}] 例： `switch(config-epbr-sess-pol-match)# set service firewall fail-action drop`	一致するシーケンスを追加、変更、または削除するか、既存のシーケンスの fail-action アクションを変更します。
ステップ 6	[**no**] **load-balance** [**method** { **src-ip**	**dst-ip**}] [**buckets** *sequence-number*] [**mask-position** *position-value*] 例： `switch(config-epbr-sess-pol-match)# load-balance method src-ip mask-position 3`	ePBR サービスで使用されるロードバランス メソッドとバケット数を計算します。 （注） 既存の一致のサービスチェーンを変更するときに、セッションコンテキストでこの構成を省略すると、

	コマンドまたはアクション	目的
		一致のロードバランス構成がデフォルトにリセットされます。 Cisco NX-OS リリース 10.3（3）F 以降では、ユーザー定義 ACL でロードバランシングに使用されるビットを選択する**mask-position** オプションが提供されています。デフォルト値は 0 です。 mask-position が構成されている場合、ロードバランス ビットは構成された mask-position から始まります。必要なバケットの数に基づいて、最上位ビットに向かって、より多くのビットがロードバランシング バケットを生成するために使用されます。 （注） ユーザー定義の ACL 内の ACE では、ロード バランシング バケットの生成に使用されるビットがユーザー定義のサブネットと重複している場合、ACE のマスク位置は内部的に 0 にリセットされます。
ステップ 7	**commit** 例： `switch(config-epbr-sess)#commit`	ePBR セッションを使用した ePBR サービスの変更を完了します。
ステップ 8	**end** 例： `switch(config-epbr-sess)#end`	ePBR セッション モードを終了します。

ePBR ポリシーによる使用される Access-list の更新

次の手順では、ePBR ポリシーで使用される access-list を更新する方法について説明します。

手順の概要

1. **epbr session access-list** *acl-name* **refresh**
2. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**epbr session access-list** *acl-name* **refresh** 例： `switch(config)# epbr session access-list WEB refresh`	ポリシーによって生成された ACL を更新またはリフレッシュします。
ステップ 2	**end** 例： `switch(config)# end`	グローバル コンフィギュレーション モードを終了します。

ePBR サービス エンドポイント アウトオブサービスを構成

ここでは、ePBR サービス エンドポイント アウトオブサービスの設定について説明します。

手順の概要

1. **configure terminal**
2. **epbr service** *service-name*
3. [**no**] **shut**
4. **service-endpoint** [**interface** *interface-name interface-number*]
5. [**no**] **hold-down threshold count** *threshold count* **time** *threshold time*

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**epbr service** *service-name* 例： `switch(config)# epbr service s1`	構成されたサービスを開始します。
ステップ 3	[**no**] **shut** 例：	エンドポイントをシャットダウンしてアウトオブサービスにする

	コマンドまたはアクション	目的
	`switch(config)# shut`	このコマンドの **no** 形式は、ノードをシャットダウンしてエンドポイントをサービスに戻します。
ステップ 4	**service-endpoint** [**interface** *interface-name interface-number*] 例： `switch(config-epbr-svc)# service-end-point ip 1.1.1.1`	ePBR サービスのサービスエンドポイントを構成します。 手順 2 ～ 5 を繰り返して、別の ePBR サービスを構成できます。
ステップ 5	[**no**] **hold-down threshold count** *threshold count* **time** *threshold time* 例： `switch(config)# hold-down threshold count 2 time 5`	は、エンドポイント レベルまたはサービス レベルのしきい値タイマーと障害カウントを構成します。それと共にエンドポイント レベルのパラメータは、サービス レベルのパラメータを上書きします。 しきい値カウントが 1 より大きい場合、タイマーは必須です。しきい値カウントが 1 の場合、タイマーは無視または拒否されます。

ePBR ポリシーの ePBR Set-VRF の構成

Cisco NX-OS リリース 10.5(2)F 以降、ePBR は ePBR L3 ポリシーの **set-vrf** コマンドをサポートします。この機能拡張により、ePBR VRF 間の展開でホスト VRF からサービス VRF へのルートリークが不要になります。

set-vrf 機能は、ルートリークなしで、ホスト VRF コンテキストでルーティングされる最後のホップからのトラフィックを許可します。

set-vrf コマンドは、ePBR ポリシー レベルまたは一致レベルで設定できます。両方が構成されている場合、一致レベルが優先されます。

set-vrf を構成するには、次のステップを実行します:

始める前に

- インターフェイスに ePBR ポリシーを適用する前に、ホスト VRF コンテキストごとに 1 つの専用ポートチャネル インターフェイスと 1 つのポート チャネル サブインターフェイスを構成する必要があります。

  次に、source-vrf（vrf551）と destination-vrf（vrf555）の両方のポートチャネルおよびポートチャネル サブインターフェイスを作成する例を示します。

```
int port-channel 1
   no shut
 int e1/1
   channel-group 1
   link loopback
   no shut
int port-channel 1.1
   encapsulation dot1q 10
   vrf member vrf551
```

```
    ip forward
    ipv6 address use-link-local-only
    ipv6 nd dad attempts 0
    ipv6 nd prefix default no-advertise
    ipv6 nd suppress-ra
    mtu 9216
    no shut
 int port-channel 1.2
    encapsulation dot1q 11
    vrf member vrf555
    ip forward
    ipv6 address use-link-local-only
    ipv6 nd dad attempts 0
    ipv6 nd prefix default no-advertise
    ipv6 nd suppress-ra
    mtu 9216
    no shut
```

- また、ePBR ポリシーを適用する前に、VRF コンテキストで同等の RPM 構成を関連付ける必要があります。

  次に、VRF コンテキスト構成を作成する例を示します。

```
vrf context vrf551
    pbr set-vrf recirc interface port-channel1.1
vrf context vrf555
    pbr set-vrf recirc interface port-channel1.2
```

手順の概要

1. **configure terminal**
2. **epbr policy** ポリシー名*-IPv4* |ポリシー名*-IPv6*
3. （任意） **source-vrf** *source-vrf-name* **destination-vrf** *destination-vrf-name*
4. （任意） **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] } **source-vrf** *source-vrf-name* **destination-vrf** *destination-vrf-name*

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**epbr policy** ポリシー名*-IPv4* |ポリシー名*-IPv6*
	例：
	IPV4 の場合：
	`switch(config)# epbr policy p_v4`
	`switch(config-epbr-policy)#`
		ePBR ポリシーを構成し、ePBR ポリシー構成モードを開始します。

	コマンドまたはアクション	目的
	IPV6 の場合： `switch(config-epbr-policy)# epbr policy p_v6`	
ステップ 3	（任意） **source-vrf** *source-vrf-name* **destination-vrf** *destination-vrf-name* 例： `switch(config-epbr-policy)# source-vrf vrf551 destination-vrf vrf555`	順方向の場合は `destination-vrf`、逆方向の場合は `source-vrf` を設定します。

ステップ 4	（任意） **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] } **source-vrf** *source-vrf-name* **destination-vrf** *destination-vrf-name*
	例：
	IPv4 の場合：
	`switch(config-epbr-policy)# match ip address acl1 source-vrf vrf551 destination-vrf vrf555`
	IPV6 の場合：
	`switch(config-epbr-policy)# match ipv6 address acl1 source-vrf vrf551 destination-vrf vrf555`
		指定した送信元および接続先 VRF の IPv4 または IPv6 ACL を照合します。

ePBR Show コマンド

次のリストに、ePBR に関連する show コマンドを示します。

手順の概要

1. **show epbr policy** *policy-name* [**reverse**]
2. **show epbr statistics** *policy-name* [**reverse**]
3. **show tech-support epbr**
4. **show running-config epbr**
5. **show startup-config epbr**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**show epbr policy** *policy-name* [**reverse**] 例： `switch# show epbr policy Tenant_A-Redirect`	順方向または逆方向に適用される ePBR ポリシーに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 2	**show epbr statistics** *policy-name* [**reverse**] 例： `switch# show ePBR statistics policy pol2`	ePBR ポリシー統計を表示します。
ステップ 3	**show tech-support epbr** 例： `switch# show tech-support epbr`	ePBR のテクニカル サポート情報を表示します。
ステップ 4	**show running-config epbr** 例： `switch# show running-config epbr`	ePBR の実行構成を表示します。
ステップ 5	**show startup-config epbr** 例： `switch# show startup-config epbr`	ePBR のスタートアップ構成を表示します。

ePBR 構成の確認

ePBR 構成を確認するためには、次のコマンドを使用します。

コマンド	目的
show ip/ipv6 policy vrf <context>	サービスチェーンが適用されるインターフェイスおよびサービスチェーンの関連するエンドポイント インターフェイスで、レイヤ 3 ePBR ポリシー用に作成された IPv4/IPv6 ルート マップ ポリシーを表示します。
show route-map dynamic <route-map name>	サービスチェーンのすべてのポイントでトラフィックを転送するために使用される、特定のバケットアクセスリストのトラフィック リダイレクション用に構成されたネクスト ホップを表示します。
show ip/ipv6 access-list <access-list name> dynamic	バケットアクセス リストのトラフィック一致基準を表示します。
show ip sla configuration dynamic	プローブが有効になっている場合に、チェーン内のサービスエンドポイントに対して ePBR によって生成された IP SLA 構成を表示します。

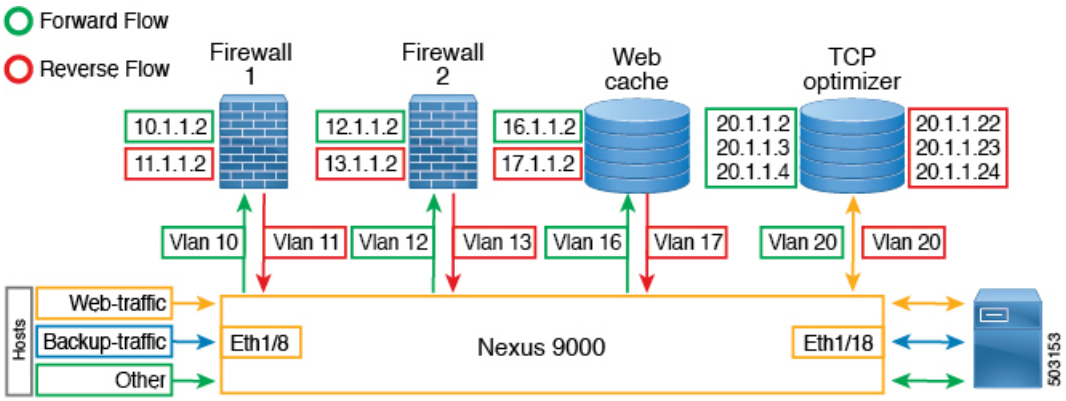
コマンド	目的
show track dynamic	プローブが有効になっている場合に、チェーン内のサービスエンドポイントに対してePBRによって生成されたトラックを表示します。

ePBR L3 の構成例

例：ePBR NX-OS 構成

次のトポロジは、ePBR NX-OS 構成を示しています。

図 *1 : ePBR NX-OS* の構成



例：ユースケース：順方向のみの Web トラフィックのサービスチェーンを作成する

次の構成例は、順方向のみの Web トラフィックのサービスチェーンを作成する方法を示しています。

```
IP access list web_traffic
        10 permit tcp any any eq www

ePBR service FW1
  service-end-point ip 10.1.1.2 interface Vlan10
    reverse interface Vlan11

ePBR service FW2
  service-end-point ip 12.1.1.2 interface Vlan12
    reverse interface Vlan13

ePBR service Web_cache
  service-end-point ip 16.1.1.2 interface Vlan16
    reverse interface Vlan17

ePBR policy tenant_1
  match ip address web-traffic
    10 set service FW1
    20 set service FW2
    30 set service Web_cache
```

```
interface Eth1/8
  ePBR ip policy tenant_1
```

次の例は、順方向の Web トラフィックのサービスチェーン作成の構成を確認する方法を示しています。

```
switch# show ePBR policy tenant_1

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): web-traffic
  Service chain:
    service FW1, sequence 10, fail-action No fail-action
      IP 10.1.1.2
    service FW2, sequence 20, fail-action No fail-action
      IP 12.1.1.2
    service Web_cache, sequence 30, fail-action No fail-action
      IP 16.1.1.2
  Policy Interfaces:
    Eth1/8
```

例：ユースケース：順方向のみで ePBR を使用して TCP トラフィックを負荷分散する

次の構成例は、順方向のみでePBRを使用してTCPトラフィックを負荷分散する方法を示しています。

```
IP access list tcp_traffic
        10 permit tcp any any

ePBR service TCP_Optimizer
  service-interface Vlan20
  service-end-point ip 20.1.1.2
  service-end-point ip 20.1.1.3
  service-end-point ip 20.1.1.4

ePBR policy tenant_1
  match ip address tcp_traffic
    10 set service TCP_Optimizer

interface Eth1/8
  ePBR ip policy tenant_1
```

次の例は、順方向で EPBR を使用して負荷分散 TCP トラフィックの構成を確認する方法を示しています。

```
switch# show ePBR policy tenant_1

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): tcp_traffic
  Service chain:
    service TCP_Optimizer, sequence 10, fail-action No fail-action
      IP 20.1.1.2
      IP 20.1.1.3
      IP 20.1.1.4
  Policy Interfaces:
    Eth1/8
```

例：ユースケース：双方向の Web トラフィックのサービスチェーンを作成する

次の構成例は、順方向と逆方向の両方で Web トラフィックのサービスチェーンを作成する方法を示しています。

```
IP access list web_traffic
        10 permit tcp any any eq www


ePBR service FW1
  service-end-point ip 10.1.1.2 interface Vlan10
    reverse ip 11.1.1.2 interface Vlan11

ePBR service FW2
  service-end-point ip 12.1.1.2 interface Vlan12
    reverse ip 13.1.1.2 interface Vlan13

ePBR service Web_cache
  service-end-point ip 16.1.1.2 interface Vlan16
    reverse ip 17.1.1.2 interface Vlan17

ePBR policy tenant_1
  match ip address web-traffic
    10 set service FW1
    20 set service FW2
    30 set service Web_cache

interface Eth1/8
  ePBR ip policy tenant_1

interface Eth1/18
  ePBR ip policy tenant_1 reverse
```

次の例は、順方向と逆方向の両方の Web トラフィックのサービスチェーン作成の構成を確認する方法を示しています。

```
switch# show ePBR policy tenant_1

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): web-traffic
  Service chain:
    service FW1, sequence 10, fail-action No fail-action
      IP 10.1.1.2
    service FW2, sequence 20, fail-action No fail-action
      IP 12.1.1.2
    service Web_cache, sequence 30, fail-action No fail-action
      IP 16.1.1.2
  Policy Interfaces:
    Eth1/8

switch# show ePBR policy tenant_1 reverse

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): web-traffic
  Service chain:
    service Web_cache, sequence 30, fail-action No fail-action
      IP 17.1.1.2
    service FW2, sequence 20, fail-action No fail-action
      IP 13.1.1.2
    service FW1, sequence 10, fail-action No fail-action
      IP 11.1.1.2
  Policy Interfaces:
    Eth1/18
```

例：ユースケース：ePBR を使用して両方向で TCP トラフィックを負荷分散する

次の構成例は、ePBR を使用して順方向と逆方向の両方で TCP トラフィックを負荷分散する方法を示しています。

```
ePBR service TCP_Optimizer
  service-interface Vlan20
  service-end-point ip 20.1.1.2
    reverse ip 20.1.1.22
  service-end-point ip 20.1.1.3
    reverse ip 20.1.1.23
  service-end-point ip 20.1.1.4
    reverse ip 20.1.1.24

ePBR policy tenant_1
  match ip address tcp_traffic
    10 set service TCP_Optimizer

interface Eth1/8
  ePBR ip policy tenant_1

interface Eth1/18
  ePBR ip policy tenant_1 reverse
```

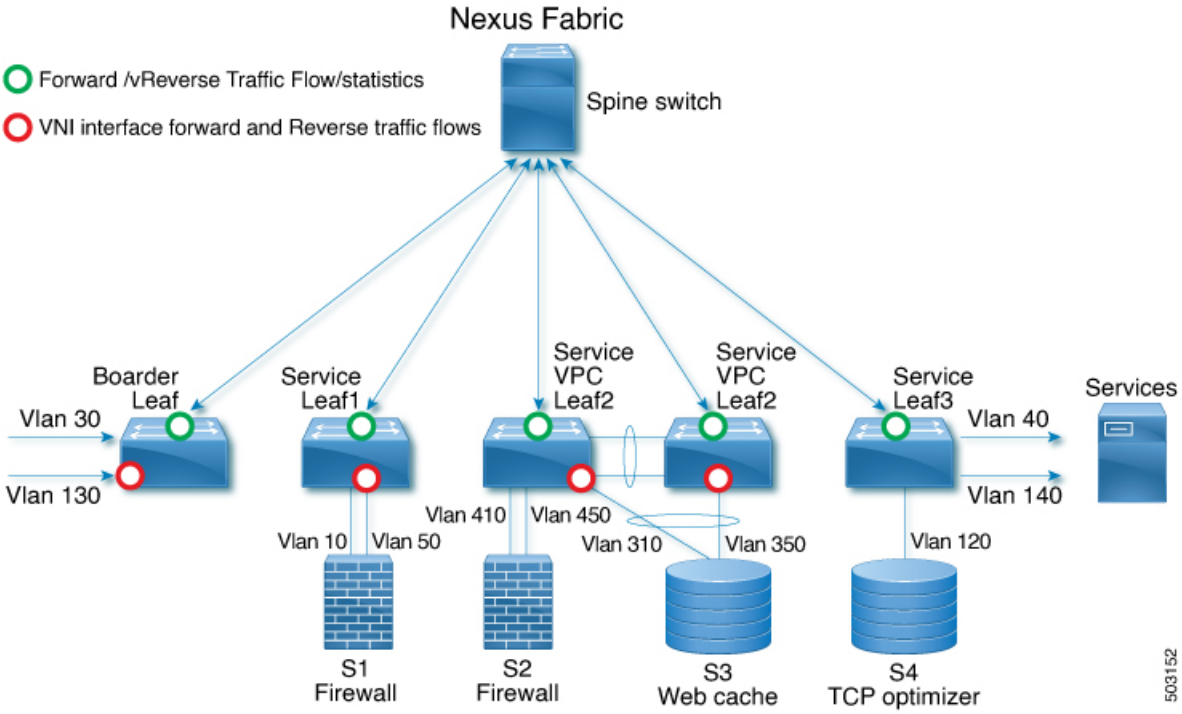
次の例は、ePBR を使用して双方向の負荷分散 TCP トラフィックの構成を確認する方法を示しています。

```
switch# show ePBR policy tenant_1

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): tcp_traffic
  Service chain:
    service TCP_Optimizer, sequence 10, fail-action No fail-action
      IP 20.1.1.2
      IP 20.1.1.3
      IP 20.1.1.4
  Policy Interfaces:
    Eth1/8

switch# show ePBR policy tenant_1 reverse

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): tcp_traffic
  Service chain:
    service TCP_Optimizer, sequence 10, fail-action No fail-action
      IP 20.1.1.22
      IP 20.1.1.23
      IP 20.1.1.24
  Policy Interfaces:
    Eth1/18
```

例：VXLAN ファブリックを使用した ePBR ポリシーの作成

次の例/トポロジは、VXLAN ファブリック上で ePBR を構成する方法を示しています。

図 *2 : VXLAN* ファブリック上の *ePBR* の構成




```
ip access-list acl1
        10 permit ip 30.1.1.0/25 40.1.1.0/25
        20 permit ip 30.1.1.128/25 40.1.1.128/25
ip access-list acl2
        10 permit ip 130.1.1.0/25 140.1.1.0/25
        20 permit ip 130.1.1.128/25 140.1.1.128/25

epbr service s1
  vrf vrf_s1
  service-end-point ip 10.1.1.2 interface Vlan10
     probe icmp frequency 4 retry-down-count 1 retry-up-count 1 timeout 2 source-interface
 loopback9
    reverse ip 50.1.1.2 interface Vlan50

       probe icmp frequency 4 retry-down-count 1 retry-up-count 1 timeout 2
source-interface loopback10

epbr service s2
  vrf vrf_s2
  service-end-point ip 41.1.1.2 interface Vlan410
     probe icmp source-interface loopback11
    reverse ip 45.1.1.2 interface Vlan450

       probe icmp source-interface loopback12

 epbr service s3
  vrf vrf_s3
  service-end-point ip 31.1.1.2 interface Vlan310
     probe http get index.html source-interface loopback13
    reverse ip 35.1.1.2 interface Vlan350

     probe http get index.html source-interface loopback14
```

```
epbr service s4
  service-interface Vlan120
  vrf vrf_s4
   probe udp 6900 control enable source-interface loopback15
  service-end-point ip 120.1.1.2

    reverse ip 120.1.1.2

epbr policy p1
 statistics
  match ip address acl1
    load-balance buckets 16 method src-ip
    10 set service s1 fail-action drop
    20 set service s2 fail-action drop
    30 set service s4 fail-action bypass
  match ip address acl2
    load-balance buckets 8 method dst-ip
    10 set service s1 fail-action drop
    20 set service s3 fail-action forward
    30 set service s4 fail-action bypass

! VXLAN L3 VNI interface for vrf_s1, vrf_s2, vrf_s3, vrf_s4 to which the policy is applied
 on all service leafs
interface vlan 100
epbr ip policy p1
epbr ip policy p1 reverse

interface vlan 101
epbr ip policy p1
epbr ip policy p1 reverse

interface vlan 102
epbr ip policy p1
epbr ip policy p1 reverse

interface vlan 103
epbr ip policy p1
epbr ip policy p1 reverse

Apply forward policy on ingress interface in border leaf where traffic coming in needs
to be service-chained:

interface Vlan 30 - Traffic matching acl1
  epbr ip policy p1
  int vlan 130  -  Traffic matching acl2
  epbr ip policy p1

Apply the reverse policy On leaf connected to server if reverse traffic flow needs to
be enabled:

int vlan 40 - Traffic matching reverse flow for acl1
epbr ip policy p1 rev
int vlan 140 - Traffic matching reverse flow for acl1
epbr ip policy p1 rev
```

例：ePBR サービスの構成

次の例は、ePBR サービスを構成する方法を示します。

```
epbr service FIREWALL
  probe icmp
  vrf TENANT_A
  service-endpoint ip 172.16.1.200 interface VLAN100
        reverse ip 172.16.2.200 interface VLAN101
```

```
service-endpoint ip 172.16.1.201 interface VLAN100
        reverse ip 172.16.2.201 interface VLAN101

epbr service TCP_Optimizer
   probe icmp
   vrf TENANT_A
service-endpoint ip 172.16.20.200 interface VLAN200
       reverse ip 172.16.30.200 interface VLAN201
```

例：ePBR ポリシーの構成

次の例は、ePBR ポリシーを構成する方法を示します。

```
epbr service FIREWALL
  probe icmp
  service-end-point ip 1.1.1.1 interface Ethernet1/1
     reverse ip 1.1.1.2 interface Ethernet1/2
epbr service TCP_Optimizer
 probe icmp
 service-end-point ip 1.1.1.1 interface Ethernet1/3
     reverse ip 1.1.1.4 interface Ethernet1/4
epbr policy Tenant_A-Redirect
 match ip address WEB
  load-balance method src-ip
  10 set service FIREWALL fail-action drop
  20 set service TCP_Optimizer fail-action bypass
match ip address APP
  10 set service FIREWALL fail-action drop
match ip address exclude_acl exclude
match ip address drop_acl drop
```

次の例は、fail-action drop 情報を含む show ePBR Policy コマンドの出力を示しています。

```
switch(config-if)# show epbr policy Tenant_A-Redirect

Policy-map : Tenant_A-Redirect
  Match clause:
    ip address (access-lists): WEB
action:Redirect
   service FIREWALL, sequence 10, fail-action Drop
     IP 1.1.1.1 track 1 [INACTIVE]
   service TCP_Optimizer, sequence 20, fail-action Bypass
     IP 1.1.1.1 track 2 [INACTIVE]
Match clause:
     ip address (access-lists): APP
action:Redirect
   service FIREWALL, sequence 10, fail-action Drop
     IP 1.1.1.1 track 1 [INACTIVE]
Match clause:
    ip address (access-lists): exclude_acl
action:Deny
Match clause:
   ip address (access-lists): drop_acl
action:Drop
 Policy Interfaces:
  Eth1/4
```

例：インターフェイスと ePBR ポリシーの関連付け

次の例は、ePBR ポリシーを構成する方法を示します。

```
interface vlan 2010
  epbr ip policy Tenant_A-Redirect
```

```
interface vlan 2011
  epbr ip policy Tenant_A-Redirect reverse
```

例：順方向に適用される ePBR ポリシー

次の例は、順方向に適用されるポリシーのサンプル出力を示しています。

```
show epbr policy Tenant_A-Redirect
policy-map Tenant_A-Redirect
 Match clause:
  ip address (access-lists): WEB
 Service chain:
  service FIREWALL  , sequence 10 , fail-action drop
   ip 172.16.1.200 track 10  [ UP ]
   ip 172.16.1.201 track 11 [ DOWN ]
                    service TCP_Optimizer, sequence 20 , fail-action bypass
   ip 172.16.20.200 track 12  [ UP] ]

 Match clause:
  ip address (access-lists): APP
 Service chain:
  service FIREWALL  , sequence 10 , fail-action drop
   ip 172.16.1.200 track 10  [ UP ]
   ip 172.16.1.201 track 11 [ DOWN ]

 Policy Interfaces:
     Vlan 2010
```

例：reverse 方向に適用される ePBR ポリシー

次の例は、reverse 方向に適用されるポリシーのサンプル出力を示しています。

```
show epbr policy Tenant_A-Redirect reverse
policy-map Tenant_A-Redirect
 Match clause:
  ip address (access-lists): WEB

 Service chain:
  service TCP_Optimizer, sequence 20 , fail-action bypass
   ip 172.16.30.200 track 15  [ UP] ]

  service FIREWALL  , sequence 10 , fail-action drop
   ip 172.16.2.200 track 13  [ UP ]
   ip 172.16.2.201 track 14 [ DOWN ]

 Match clause:
  ip address (access-lists): APP

 Service chain:

  service FIREWALL  , sequence 10 , fail-action drop
   ip 172.16.2.200 track 13  [ UP ]
   ip 172.16.2.201 track 14 [ DOWN ]

 Policy Interfaces:
     Vlan 2011
```

例：ユーザ定義トラック

次の例は、各エンド ポイントにトラック ID を割り当てる方法を示しています。

```
epbr service FIREWALL
  probe icmp
  service-end-point ip 1.1.1.2 interface Ethernet1/21
```

```
probe track 30
reverse ip 1.1.1.3 interface Ethernet1/22
  probe track 40
 service-end-point ip 1.1.1.4 interface Ethernet1/23
    reverse ip 1.1.1.5 interface Ethernet1/24
```

例：ePBR セッションを使用した ePBR サービスの変更

次の例は、ePBR サービスの IP を置き換え、別のサービス エンド ポイントを追加する方法を示しています。

```
switch(config)#epbr session
switch(config-epbr-sess)#epbr service TCP_OPTIMIZER
switch(config-epbr-sess-svc)# no service-end-point ip 172.16.20.200 interface VLAN200

switch(config-epbr-sess-svc)#service-end-point ip 172.16.25.200 interface VLAN200
switch(config-epbr-sess-svc-ep)# reverse ip 172.16.30.200 interface VLAN201
switch(config-epbr-sess)#commit
```

例：EPBR セッションを使用した ePBR ポリシーの変更

次の例は、ePBR ポリシーの IP を置き換え、変更されたポリシー トラフィックのサービスチェーンを追加する方法を示しています。

```
switch(config)#epbr session
switch(config-epbr-sess)#epbr policy Tenant_A-Redirect
switch(config-epbr-sess-pol)# no match ip address WEB
switch(config-epbr-sess-pol)#match ip address WEB
switch(config-epbr-sess-pol-match)# 10  set service Web-FW fail-action drop load-balance
 method src-ip
switch(config-epbr-sess-pol-match)# 20 set service TCP_Optimizer fail-action bypass
switch(config-epbr-sess-pol)#match ip address HR
switch(config-epbr-sess-pol-match)# 10  set service Web-FW
switch(config-epbr-sess-pol-match)# 20 set service TCP_Optimizer
switch(config-epbr-sess)#commit
```

例：ePBR 統計ポリシーの表示

次の例は、ePBR 統計ポリシーを表示する方法を示しています。

```
switch# show epbr statistics policy pol2

Policy-map pol2, match testv6acl

    Bucket count: 2

      traffic match : epbr_pol2_1_fwd_bucket_1
        two : 0
      traffic match : epbr_pol2_1_fwd_bucket_2
        two : 0
```

例：mask-position の使用方法の表示

次に、mask-position の使用例を示します。

```
IP access list acl1
        10 permit tcp 10.0.0.0/24 any
epbr policy l3_Pol
  statistics match ip address acl1
  load-balance buckets 4 mask-position 5
10 set service s1_l3
switch# show ip access-list dynamic
IP access list epbr_l3_Pol_1_fwd_bucket_1
 10 permit tcp 10.0.0.0 0.0.0.159 any
IP access list epbr_l3_Pol_1_fwd_bucket_2
```

```
 10 permit tcp 10.0.0.32 0.0.0.159 any
IP access list epbr_l3_Pol_1_fwd_bucket_3
 10 permit tcp 10.0.0.64 0.0.0.159 any
IP access list epbr_l3_Pol_1_fwd_bucket_4
 10 permit tcp 10.0.0.96 0.0.0.159 any
```

その他の参考資料

ePBR の構成の詳細については、次の各セクションを参照してください。

関連資料

関連項目	マニュアル タイトル
IP SLA パケットの CoPP の構成	*Cisco Nexus 9000* シリーズ *NX-OS IP SLA* 構成ガイド *9.3(x)*
ePBR ライセンス	『*Cisco NX-OS Licensing Guide*』
ePBR スケール値	『*Cisco Nexus 9000 Series NX-OS Verified Scalability Gu*

標準

標準
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポート れていません。

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