エンドポイント ロケータ

エンドポイント ロケータ

エンドポイントロケータ（EPL）機能により、データセンター内のエンドポイントをリアルタイムで追跡できます。追跡には、エンドポイントのネットワーク ライフ履歴のトレースと、エンドポイントの追加、削除、移動などに関連する傾向へのインサイトの取得が含まれます。エンドポイントは少なくとも 1 つの IP アドレス (IPv4 および/または IPv6) と MAC アドレスをもつ任意のものです。EPL機能は、MAC専用エンドポイントを表示することもできます。デフォルトでは、MAC 専用エンドポイントは表示されません。その意味で、エンドポイントは仮想マシン（VM）、コンテナー、ベアメタル サーバー、サービス アプライアンスなどです。

Note

- EPLは、VXLAN BGP EVPN ファブリック展開で Nexusダッシュボード ファブリック コントローラ LAN ファブリック インストール モードでのみサポートされます。VXLAN BGP EVPN ファブリックは、Easy ファブリック、Easy eBGP ファブリック、または外部ファブリック（管理モードまたはモニタ モード）として導入できます。EPL は、3 層のアクセス集約コア ベースのネットワーク展開ではサポートされません。
- EPL は、少なくとも 1 つの IP アドレス（IPv4 または IPv6）を持つエンドポイントを表示します。EPL は、MAC 専用エンドポイントを表示することもできます。EPL の設定時に **[MAC のみのアドバタイズメントを処理（Process MAC-Only Advertisements）]** チェックボックスをオンにして、MAC アドレスのみを持つ EVPN ルートタイプ 2 アドバタイズメントの処理を有効にします。L2VNI：MAC は、このようなすべてのエンドポイントの一意のエンドポイント ID です。EPL は、レイヤ 3 ゲートウェイがファイアウォール、ロードバランサ、またはその他のノード上にあるレイヤ2のみのネットワーク展開でエンドポイントを追跡できるようになりました。

EPL は、エンドポイント情報を追跡するために BGP の更新に依存します。したがって、通常 Nexusダッシュボードファブリック コントローラは、これらの更新を取得するためにBGPルートリフレクタ（RR）とピアリングする必要があります。このためには、Nexusダッシュボードファブリック コントローラ から RR への IP 到達可能性が必要です。これは、Nexusダッシュボードファブリック コントローラ データネットワーク インターフェイスへのインバンドネットワーク接続で実現できます。

エンドポイント ロケータの主な特徴は次のとおりです。

- デュアルホーム接続およびデュアルスタック（IPv4 + IPv6）エンドポイントのサポート
- 最大 2 つの BGP ルート リフレクタまたはルート サーバのサポート
- VRF、ネットワーク、レイヤ2 VNI、レイヤ3 VNI、スイッチ、IP、MAC、ポート、VLAN などのさまざまな検索フィルタで、すべてのエンドポイントのリアルタイムおよび履歴検索をサポートします。
- エンドポイントのライフタイム、ネットワーク、エンドポイント、VRF 日次ビュー、運用ヒートマップなどのインサイトに関するリアルタイムおよび履歴ダッシュボードのサポート。
- iBGP および eBGP ベースの VXLAN EVPN ファブリックのサポート。ファブリックは、イージー ファブリックまたは外部ファブリックとして作成できます。EPLは、適切なBGP設定でスパインまたは RR を自動的に設定するオプションで有効にできます。
- 最大 4 つのファブリックに対して EPL 機能を有効にできます。
- EPL はマルチサイト ドメイン（MSD）でサポートされます。
- IPv6 アンダーレイはサポートされていません。
- ハイ アベイラビリティのサポート
- 最大 60 日間保存されるエンドポイントデータのサポート。最大 100 GB のストレージ容量。
- 新たに開始するためのエンドポイント データのオプションのフラッシュのサポート。
- サポートされる拡張性：ファブリックあたり最大 5 万個の固有エンドポイント。最大 4 つのファブリックがサポートされます。ただし、すべてのファブリックのエンドポイントの最大合計数は 50K を超えてはなりません。

  すべてのファブリックのエンドポイントの合計数が 50K を超えると、アラームが生成され、ウィンドウの右上にある **[アラーム（Alarms）]** アイコンの下にリストされます。このアイコンは、新しいアラームが生成されるたびに点滅し始めます。
- NDFC リリース 12.0.1a 以降、EPL を有効にするには、永続的または外部 IP アドレスが必要です。VXLANファブリックごとに、ファブリックのスパインとピアリングするBGPインスタンスを実行する特定のコンテナが生成されます。このコンテナには、スパイン上の iBGP ネイバーとして設定される永続的な IP が関連付けられている必要があります。ファブリックごとに異なるコンテナが使用されるため、EPLが有効になっているNDFCによって管理されるファブリックの数によって、EPL のために配布する必要がある永続的な IP

アドレスの数が決まります。また、EPL は Nexus Dashboard データインターフェイス上でのみ iBGP セッションを確立します。

- 仮想 Nexus Dashboard の展開では、Nexus Dashboard 管理および/または IP スティッキ性が必要なデータ vNIC に関連付けられたポートグループで無差別モードを有効化し/受け入れます。永続的な IP アドレスがポッドに与えられます（たとえば、SNMP トラップ/Syslog レシーバー、ファブリックごとのエンドポイント ロケーター インスタンス、SAN Insights レシーバーなど）。Kubernetes のすべての POD は、複数の仮想インターフェースを持つことができます。特に IP スティッキ性については、外部サービス IP プールから適切な空き IP が割り当てられた POD に追加の仮想インターフェイスが関連付けられます。vNIC には、vND 仮想 vNIC に関連付けられた MAC アドレスとは異なる独自の一意の MAC アドレスがあります。さらに、POD から外部スイッチとの間のすべての通信は、北から南へのトラフィックフローのために同じボンドインターフェイスから出力されます。EPL コンテナは Nexus Dashboard データインターフェイスを使用します。データ vNIC は、bond0（bond0br とも呼ばれる）インターフェイスにマップします。デフォルトでは、VMware システムは、特定の vNIC からのトラフィックフローがその vNIC に関連付けられた送信元 MAC と一致するかどうかを確認します。NDFC の場合、トラフィックフローは、指定された POD の永続的 IP アドレスを使用して発信されます。そのため、VMware 側で必要な設定を有効にする必要があります。

開始する前に仮想 Nexus ダッシュボードクラスタを使用している場合は、永続的な IP アドレス、EPL 機能、および必要な設定が有効になっていることを確認してください。以下のリンクを参照。

Cisco Nexus Dashboard ファブリックコントローラ導入ガイド

Cisco Nexus Dashboard ファブリックコントローラのインストールとアップグレードガイド

EPL 接続オプション

様々な EPL 接続オプションのサンプル トポロジは次のとおりです。

DCNM クラスタ モード：物理サーバから VM へのマッピング

詳細については、 Cisco Nexus Dashboard Fabric Controller Verified Scalability Guideを参照してください。

エンドポイント ロケータの構成

Nexusダッシュボード ファブリック コントローラ の OVA または ISO インストールでは、次の 2 つのインターフェイスを使用します。

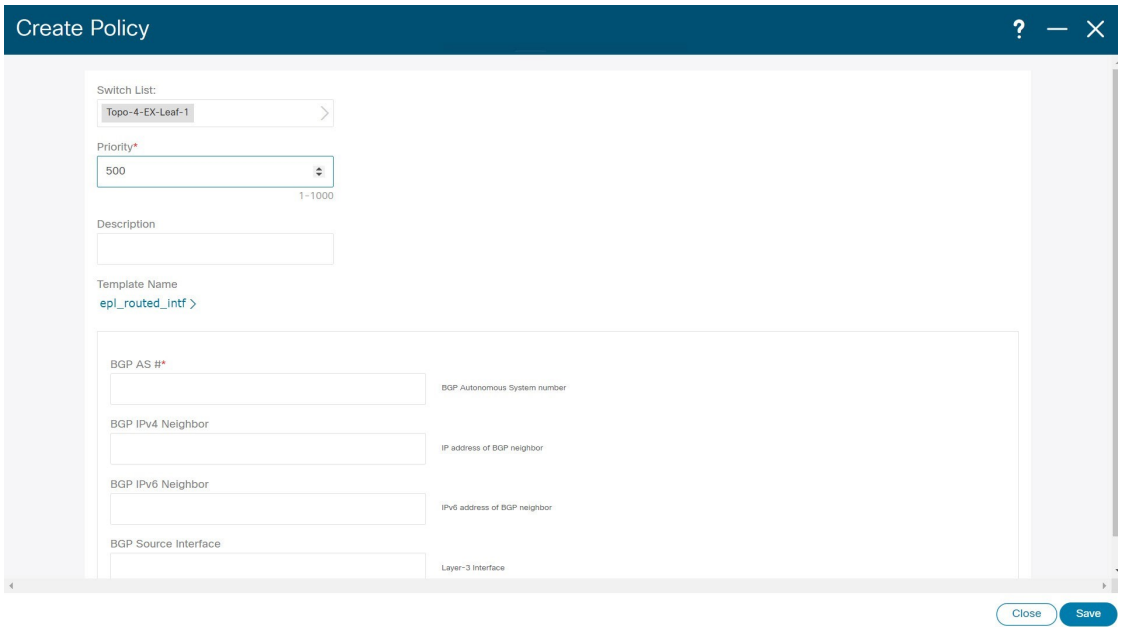
- 管理
- データ

（アウトオブバンドまたは OOO）スイッチ mgmt0 インターフェイスを介したスイッチの接続は、データ インターフェイスまたは管理インターフェイスによって行うことができます。詳細については、NDFC Installation and Upgrade Guide を参照してください。

管理インターフェイスは、レイヤ 2 またはレイヤ 3 隣接の mgmt0 インターフェイスにより、デバイスに到達できるようにします。これにより、POAPを含むこれらのデバイスを管理およびモニタできます。Nexusダッシュボード ファブリック コントローラEPLでは、とルートリフレクタの間でBGPピアリングが必要です。Nexusダッシュボード ファブリック コントローラNexusデバイスのBGPプロセスは通常、デフォルトVRFで実行されるため、からファブリックへのインバンドIP接続が必要です。Nexusダッシュボード ファブリック コントローラデータ ネットワーク インターフェイスは、Nexusダッシュボードのインストール中に構成できます。構成されたインバンド ネットワーク構成を変更することはできません。

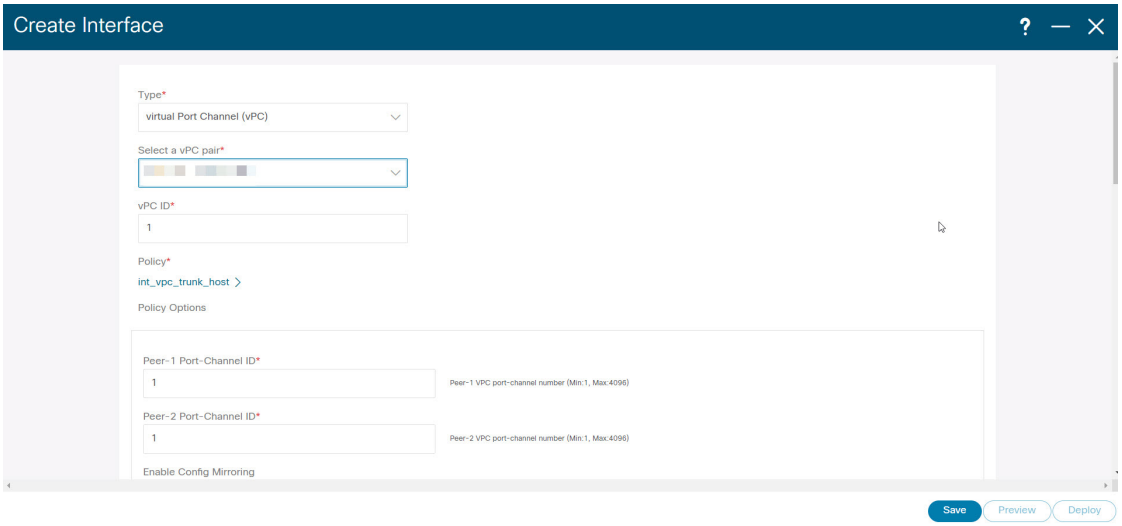
Note Nexusダッシュボード ファブリック コントローラ 上のデータ ネットワーク インターフェイスのセットアップは、ファブリック内のデバイスへのインバンド接続を必要とするアプリケーションの前提条件です。これには EPL とネットワーク インサイトのリソース（NIR）が含まれます。

ファブリック側では、スタンドアロン Nexusダッシュボード ファブリック コントローラ 展開の場合、Nexus Dashboard データ ネットワーク ポートがリーフ上のフロントエンド インターフェイスの 1 つに直接接続されていれば、そのインターフェイスを **epl_routed_intf** テンプレートを使用して設定できます。ファブリック内のIGPとしてIS-ISまたはOSPFを使用する場合の、このシナリオの例を以下に示します。

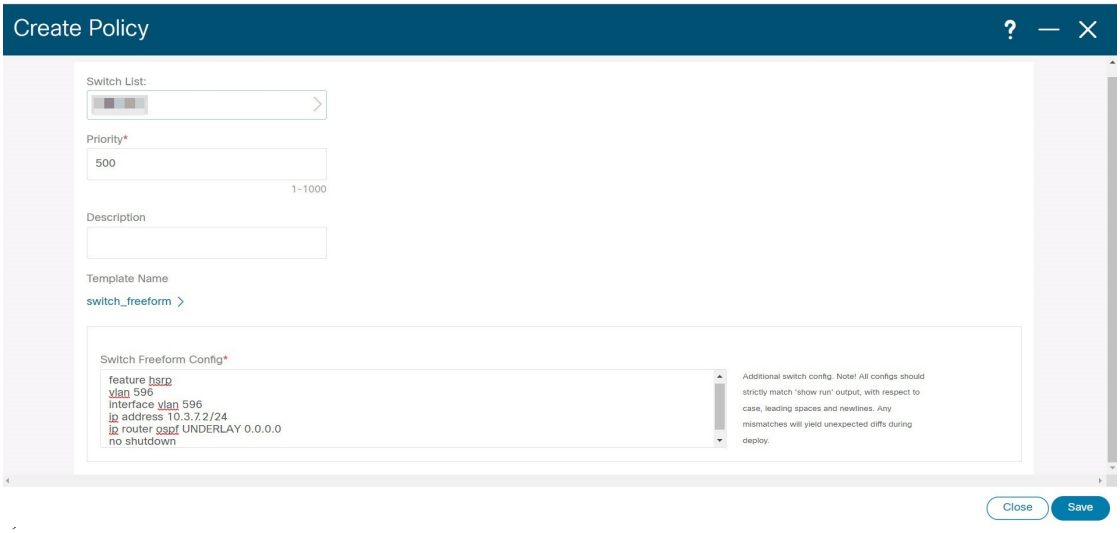


ただし、冗長性を確保するために、がインストールされているサーバをデュアルホームまたはデュアル接続にすることをお勧めします。Nexusダッシュボード ファブリック コントローラ OVA導入では、ポートチャネルを介してサーバをスイッチに接続できます。Nexusダッシュボー

ドファブリック コントローラこれにより、リンクレベルの冗長性が提供されます。ネットワーク側のノードレベルの冗長性を確保するために、サーバをリーフスイッチのvPCペアに接続することもできます。このシナリオでは、HSRP VIP が Nexusダッシュボード ファブリック コントローラ 上のデータ ネットワーク インターフェイスのデフォルトゲートウェイとして機能するようにスイッチを構成する必要があります。



terry-leaf3 上の HSRP 構成では、次の図に示すように、**switch_freeform** ポリシーを使用できま



SVI 596 に IP アドレス 10.3.7.2/24 を使用しながら、terry-leaf3 に同様の設定を展開できます。これにより、デフォルトゲートウェイが 10.3.7.3 に設定されたデータ ネットワーク インターフェイスを介して、Nexusダッシュボード ファブリック コントローラ からファブリックへのインバンド接続が確立されます。

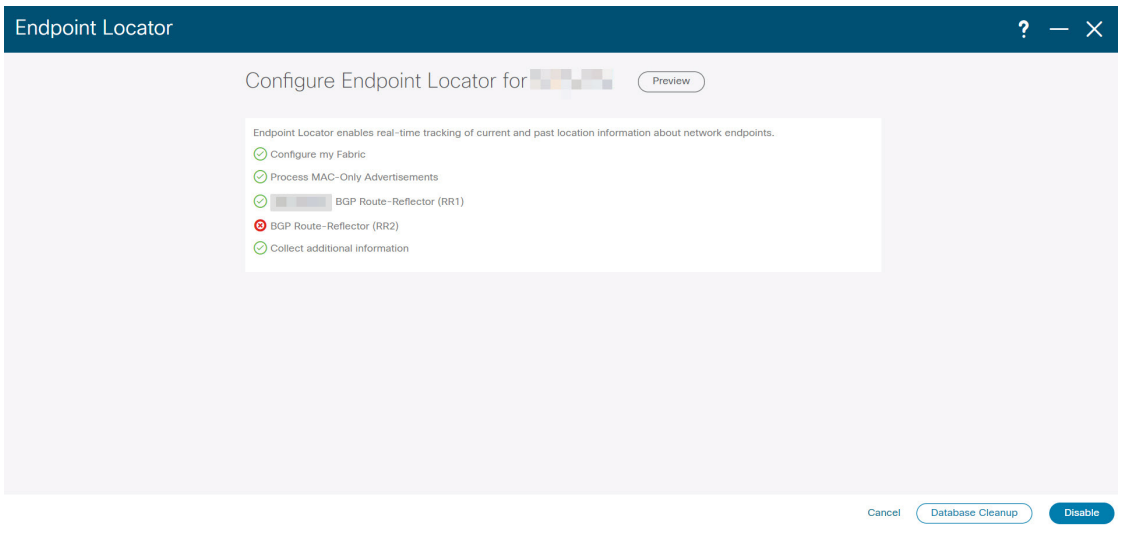
物理または仮想とファブリック間のインバンド接続を確立した後、BGPピアリングを確立できます。Nexusダッシュボード ファブリック コントローラ

EPLの設定時に、ルートリフレクタ（RR）はBGPピアとして受け入れるように設定されます。Nexusダッシュボード ファブリック コントローラ同じ構成中、Nexusダッシュボード ファブリック コントローラは、データ ネットワーク インターフェイス ゲートウェイを介してスパイン/RR 上の BGP ループバック IP にルートを追加することによっても構成されます。

Note Cisco Nexusダッシュボード ファブリック コントローラ の EPL 機能をイネーブルにしていることを確認します。**[設定（Settings）] > [機能管理（Feature Management）] > [ファブリック コントローラ（Fabric Controller）]**を選択し、**[エンドポイント ロケータ（Endpoint Locator）]** チェックボックスをオンにします。追加された EPL の詳細をダッシュボードで表示できます。

Note シスコは、ASN、RR、IPなどのピアリングの確立に関する情報を収集するためにBGP RRを照会します。Nexusダッシュボード ファブリック コントローラ

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からエンドポイント ロケータを構成するには、[ファブリックの概要（Fabric Overview）]ページで、**[アクション（Actions）]> [その他（More）] > [エンドポイント ロケータの構成（Configure Endpoint Locator）]**を選択します。同様に、[トポロジ（Topology）] ページで EPL を構成し、必要なファブリックを右クリックして、**[その他（More）] > [エンドポイント ロケータの構成（Configure Endpoint Locator）]**をクリックします。**[エンドポイント ロケータ（Endpoint Locator）]** ウィンドウが表示されます。



一度に1つのファブリックに対してEPLを有効にできます。

ドロップダウンリストから、RRをホストするファブリック上のスイッチを選択します。シスコはRRとピアリングします。Nexusダッシュボード ファブリック コントローラ

デフォルトでは、**[マイ ファブリックを構成（Configure My Fabric）]** オプションが選択されています。このノブは、EPL機能の有効化の一環として、選択したスパイン/ RRにBGP設定をプッシュするかどうかを制御します。EPL BGPネイバーシップのカスタムポリシーを使用してスパイン/RRを手動で設定する必要がある場合は、このオプションをオフにします。モニタされているだけで設定されていない外部ファブリックの場合、このオプションはグレー表示されます。Nexusダッシュボード ファブリック コントローラNexusダッシュボード ファブリック コントローラ

EPL機能の設定時にMAC専用アドバタイズメントの処理を有効にするには、[Process MAC-Only Advertisements]オプションを選択します。

Note [Process Mac-Only Advertisements]チェックボックスをオンまたはオフにしてEPLをファブリックで有効にし、後でこの選択を切り替える場合は、まずEPLを無効にしてから、[データベースのクリーンアップ（Database Clean-up）]をクリックしてエンドポイントデータを削除してから、EPLを再度有効にします。必要な[Macのみのアドバタイズメントの処理（Process Mac-Only Advertisements）]設定を使用します。

[追加情報の収集（Collect Additional Information）] で **[はい（Yes）]**を選択し、EPL 機能を有効にしながら PORT、VLAN、VRF などの追加情報の収集を有効にします。追加情報を収集するには、スイッチ、ToR、およびリーフでNX-APIがサポートされ、有効になっている必要があります。**[いいえ（No）]** オプションを選択すると、この情報は EPL によって収集および報告されません。

Note 外部ファブリックを除くすべてのファブリックでは、NX-APIがデフォルトで有効になっています。外部ファブリックの場合、External_Fabric_11_1ファブリックテンプレートの[Advanced]タブで[Enable NX-API]チェックボックスをオンにして、外部ファブリック設定でNX-APIを有効にする必要があります。

[i]アイコンをクリックすると、EPLを有効にしている間にスイッチにプッシュされる設定のテンプレートが表示されます。この設定は、外部モニタ対象ファブリックでEPLを有効にするために、スパインまたは境界ゲートウェイデバイスにコピーアンドペーストできます。

適切な選択を行い、さまざまな入力を確認したら、[送信（Submit）]をクリックしてEPLを有効にします。EPLの有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPLは正常に有効化されます。

Nexus ダッシュボード データ サービスの IP は、BGP ネイバーとして使用されます。

エンドポイントロケータ機能を有効にすると、バックグラウンドでいくつかの手順が実行されます。選択したRRに接続し、ASNを決定します。Nexusダッシュボード ファブリック コントローラまた、BGPプロセスにバインドされているインターフェイスIPも決定します。また、eBGPアンダーレイの場合は、から開始されるBGP接続を受け入れる準備をするために、適切なBGPネイバーステートメントがRRまたはスパインに追加されます。Nexusダッシュボード ファブリック コントローラEPL ポッドに割り当てられている外部 Nexus ダッシュボード デー

タ サービスの IP アドレスは、BGP ネイバーとして追加されます。EPLが正常に有効化されると、ユーザは自動的にEPLダッシュボードにリダイレクトされ、ファブリック内に存在するエンドポイントの運用上および探索的洞察が示されます。

EPL ダッシュボードの詳細については、エンドポイント ロケータの監視を参照してください。

エンドポイントデータベースのフラッシュ

エンドポイントロケータ機能を有効にすると、すべてのエンドポイント情報をクリーンアップまたはフラッシュできます。これにより、エンドポイントに関する古い情報がデータベースに存在しないことを確認するために、クリーンな状態から開始できます。データベースがクリーンになると、BGPクライアントはBGP RRから学習したすべてのエンドポイント情報を再入力します。以前にEPL機能が無効にされていたファブリックでEPL機能を再度有効にしていない場合でも、エンドポイントデータベースをフラッシュできます。

Cisco Web UIからすべてのエンドポイントロケータ情報を消去するには、次の手順を実行します。Nexusダッシュボード ファブリック コントローラ

Procedure

ステップ 1 [Endpoint Locator]の[Configure]を選択し、[Database Clean-Up]をクリックします。

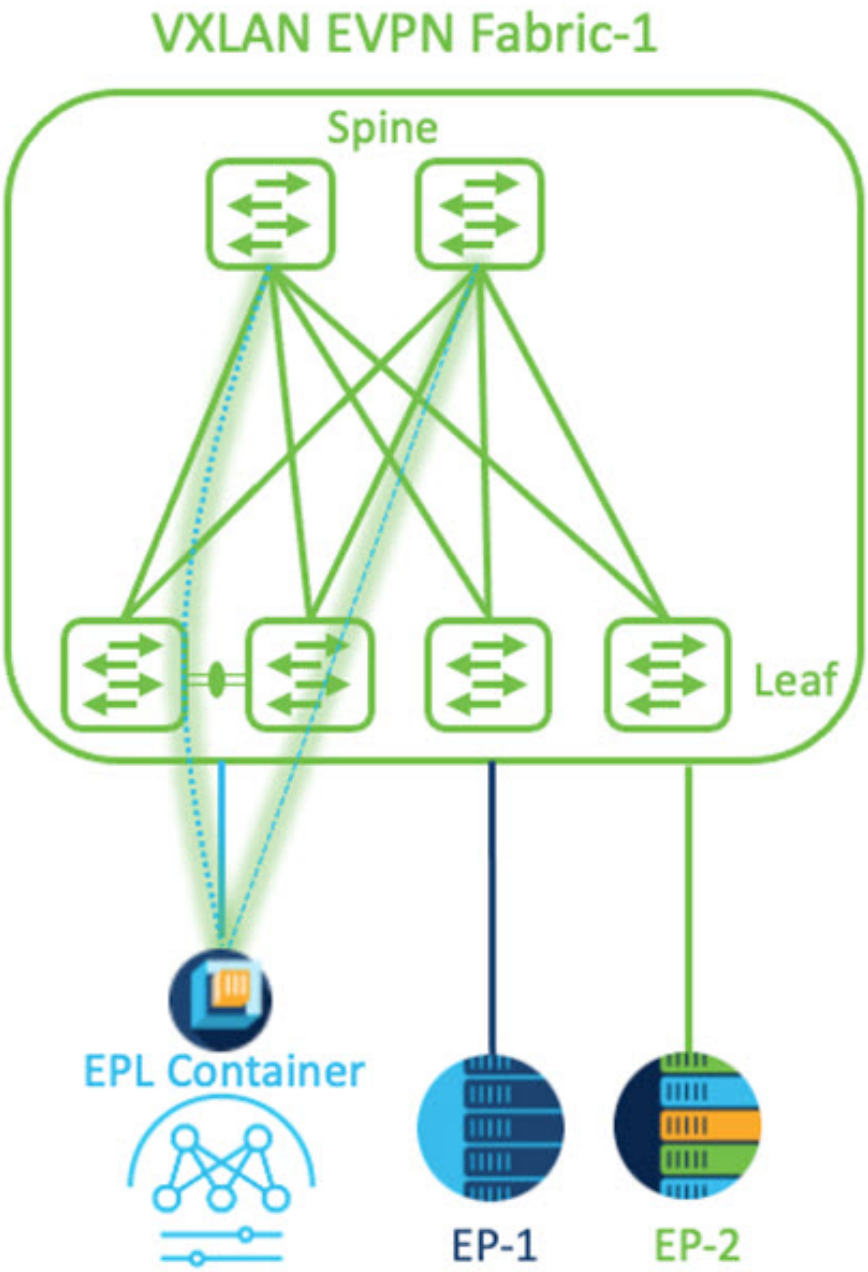
ステップ 2 [Delete]をクリックして続行するか、[Cancel]をクリックして中止します。

単一の VXLAN EVPN サイトのエンドポイント ロケータの構成

単一の VXLAN EVPN サイトのエンドポイント ロケータを構成するには、次の手順を実行します。

始める前に

次の図では、NDFC サービス アプリケーションは、リンクおよびノード レベルの冗長性を提供するため、リーフ スイッチの VPC ペアに接続されています。EPL コンテナで実行されている BGP インスタンスは、ファブリック スパインとの iBGP ピアリングを確立します。iBGP ピアリングは、スパイン ループバック アドレス（loopback0）と、EPL コンテナの永続的 IP アドレスの間で形成されます。スパインの loopback0 アドレスは VXLAN アンダーレイを介して到達可能であるため、EPL コンテナ IP にはスパインへの IP 到達可能性が必要です。IP 接続を提供できるリーフ スイッチに SVI を設定できます。SVI は非 VXLAN 対応 VLAN になり、アンダーレイにのみ参加します。



手順

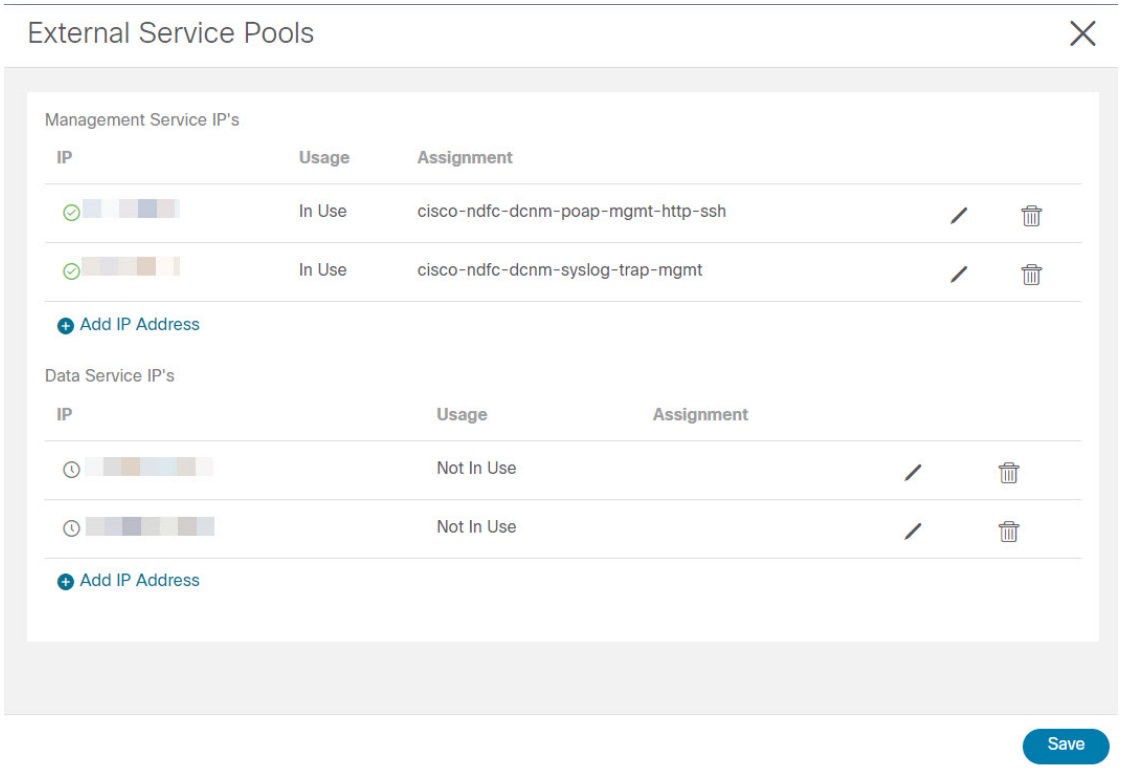
ステップ 1 Cisco Nexus Dashboard で永続 IP アドレスを構成する必要があります。Nexus Dashboard で、**[管理コンソール（Admin Console）]**>**[インフラストラクチャ（Infrastructure）]**>**[クラスタ構成（Cluster Configuration）]**を選択します。

ステップ 2 **[全般（General）]** タブの、**[外部サービス プール（External Service Pools）]** カードで、**[編集（Edit）]** アイコンをクリックします。

[外部サービスプール（External Service Pools）] ウィンドウが表示されます。

ステップ 3 **[データ サービス IP（Data Service IP's）]** に永続的 IP アドレスを入力し、**[チェック（check）]** アイコンをクリックします。

（注） IP アドレスは、Nexus ダッシュボード データ プールに関連付ける必要があります。単一のサイトの EP を視覚化および追跡するには、単一の永続的な IP アドレスが必要です。



ステップ 4 ND データ インターフェイスおよびアンダーレイ IP 接続に FHRP を使用するように SVI を構成します。

ファブリック リーフ 1 で **switch_freeform** ポリシーを使用できます。

自由形式ポリシーを作成するには、次の手順を実行します。

a) **[LAN]** > **[ファブリック（Fabrics）]** を選択し、必要な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（Fabric Overview）] ページが表示されます。

b) **[ポリシー（Policy）]** タブで、**[アクション（Actions）]** > **[ポリシーの追加（Add Policy）]** の順に選択します。

[ポリシーの追加（Add Policy）] ウィンドウが表示されます。

c) **[スイッチ リスト（Switch List）]** ドロップダウン リストから適切な Leaf1 スイッチを選択し、**[テンプレートの選択（Choose Template）]** をクリックします。

d) **[ポリシー テンプレートの選択（Select Policy Template）]** ウィンドウで、**switch_freeform** テンプレートを選択し、**[選択（Select）]** をクリックします。

FHRP 構成を適用し、テンプレートを保存します。

テンプレート構成を展開します。

この例では、ファブリック リーフ 1 で作成された HSRP ゲートウェイを備えた SVI 100 です。同様に、ファブリック リーフ 2 の手順を繰り返します。

以下の設定例をご覧ください：

```
feature hsrp
vlan 100
name EPL-Inband
interface Vlan100
  no shutdown
  no ip redirects
  ip address 192.168.100.252/24
  no ipv6 redirects
  ip router ospf 100 area 0.0.0.0
  hsrp 100
    ip 192.168.100.254
```

ステップ 5 Nexus ダッシュボード データ インターフェイスとファブリック スイッチ間の IP 到達可能性を確認します。

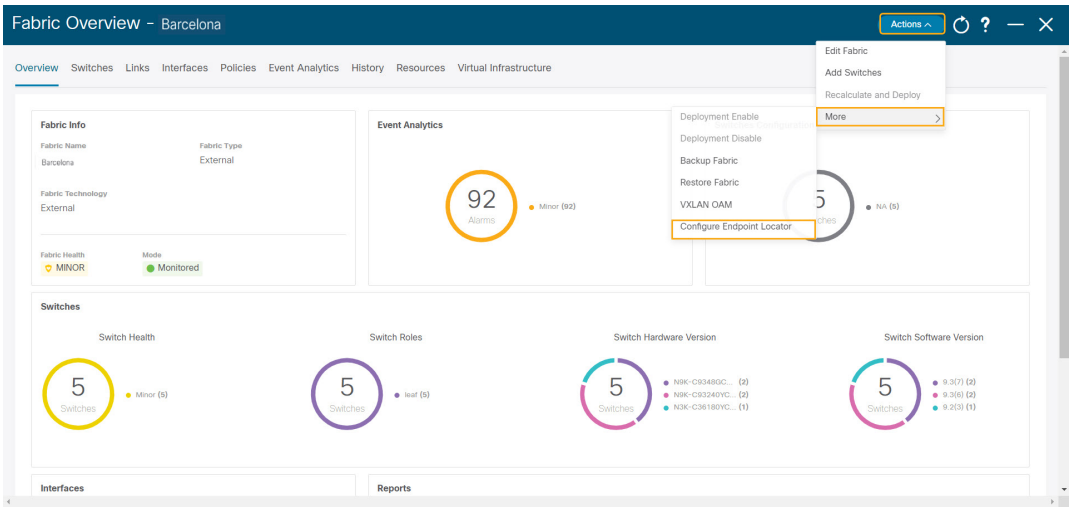
```
[rescue-user@ndfc-12-parth ~]$ ping 192.168.100.254 -c 2
PING 192.168.100.254 (192.168.100.254) 56(84) bytes of data.
64 bytes from 192.168.100.254: icmp_seq=1 ttl=255 time=1.95 ms
64 bytes from 192.168.100.254: icmp_seq=2 ttl=255 time=2.09 ms

--- 192.168.100.254 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 1.950/2.021/2.093/0.084 ms
[rescue-user@ndfc-12-parth ~]$
```

ステップ 6 ファブリック レベルで EPL を有効にします。

a) EPL を設定するには、**[LAN]** > **[ファブリック（Fabrics）]** > **[ファブリックの概要（Fabric Overview）]** を選択します。

b) **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[アクション（Actions）]** > **[その他（More）]** > **[エンドポイント ロケータの構成（Configure EndPoint Locator）]** を選択します



c) ドロップダウンリストから、スパイン/ルートリフレクタ RR をホストするファブリック上の適切なスイッチを選択します。

ノブ コントロールの **[マイ ファブリックの構成（Configure my Fabric）]** オプションを選択します。

これは、EPL 機能の有効化の一環として、選択したスパイン/ RR に BGP 設定をプッシュするかどうかを制御します。EPL BGP ネイバーシップのカスタム ポリシーを使用してスパイン/RR を手動で設定する必要がある場合は、このオプションをオフにします。モニタリングされているだけで構成されていない外部ファブリックの場合、このオプションはグレー表示されます。これらのファブリックは NDFC で構成されていないためです。

EPL 機能の設定時に MAC 専用アドバタイズメントの処理を有効にするには、**[MAC 専用アドバタイズメントを処理（Process MAC-Only Advertisements）]** オプションを選択します。

（注） **[MAC 専用アドバタイズメントを処理（Process Mac-Only Advertisements）]** チェックボックスをオンまたはオフにして EPL をファブリックで有効にしてから、後ほどこの選択を切り替える場合は、まず EPL を無効にしてから **[データベースのクリーンアップ（Database Clean-up）]** をクリックしてエンドポイント データを削除し、必要な **[Mac 専用アドバタイズメントを処理（Process Mac-Only Advertisements）]** 設定で EPL を再度有効にします。

[追加情報の収集（Collect Additional Information）] で **[はい（Yes）]** を選択し、EPL 機能を有効にしながら PORT、VLAN、VRF などの追加情報の収集を有効にします。追加情報を収集するには、スイッチ、ToR、およびリーフで NX-API がサポートされ、有効になっている必要があります。**[いいえ（No）]** オプションを選択すると、この情報は EPL によって収集および報告されません。

（注） 外部ファブリックを除くすべてのファブリックでは、NX-APIがデフォルトで有効になっています。外部ファブリックの場合、External_Fabric_11_1 ファブリック テンプレートで **[NX-API の有効化（Enable NX-API）]** チェックボックスをオンにして（**[詳細設定（Advanced）]**タブ）、外部ファブリック設定で NX-API を有効にする必要があります。

[プレビュー（Preview）]アイコンをクリックすると、EPL を有効にしている間にスイッチにプッシュされる設定のテンプレートが表示されます。この設定は、外部モニタ対象ファブリックでEPLを有効にするために、スパインまたは境界ゲートウェイデバイスにコピーアンドペーストできます。

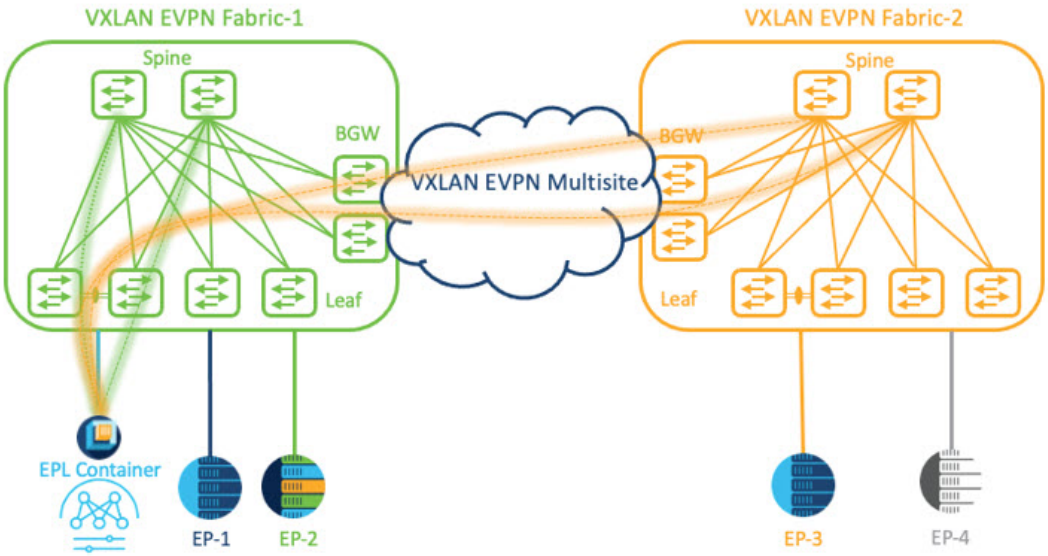
適切な選択を行い、さまざまな入力を確認したら、**[構成の保存（Save Config）]**をクリックして、EPL を有効にします。EPL の有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPLは正常に有効化されます。EPL が有効になると、永続 IP が使用されます。

VXLAN EVPN マルチサイトを使用したマルチファブリックのエンドポイント ロケータの構成

マルチファブリック VXLAN EVPN マルチサイトのエンドポイント ロケータを構成するには、次の手順を実行します。

始める前に

次の図では、VXLAN EVPN マルチサイトを使用してマルチファブリックの EPL を有効にしています。BGP ピアリングは、各 VXLAN EVPN サイトのスパイン/RR と NDFC EPL コンテナの間で確立されます。永続的な IP は、VXLAN EVPN サイトの数に基づいて必要です。Cisco ND クラスタでホストされる NDFC アプリケーションは、サイト 1 にあります。リモート サイトに展開されたスパイン/RR に到達するためのルーティング情報は、マルチサイト全体で交換する必要があります。BGP セッションが形成されると、ファブリック 2 のローカル EP を可視化して追跡できます。



デフォルトでは、Nexus Dashboard データ インターフェイスおよびサイト 2 のスパイン/RR ループバックのプレフィックスは、BGW 全体にはアドバタイズされません。したがって、プレフィックスは、サイト全体でカスタム ルート マップとプレフィックス リストを使用して交換する必要があります。同時に、スパイン/RR ループバック プレフィックスは OSPF プロトコルの一部であり、BGW は BGP を使用して相互にピアリングするため、OSPF と BGP 間のルート再配布が必要です。

手順

ステップ 1 Cisco Nexus Dashboard で永続 IP アドレスを構成する必要があります。Nexus Dashboard で、**[管理コンソール（Admin Console）]**>**[インフラストラクチャ（Infrastructure）]**>**[クラスタ構成（Cluster Configuration）]**を選択します。

ステップ 2 **[全般（General）]** タブの、**[外部サービス プール（External Service Pools）]** カードで、**[編集（Edit）]** アイコンをクリックします。

[外部サービスプール（External Service Pools）] ウィンドウが表示されます。

ステップ 3 **[データ サービス IP（Data Service IP's）]** に永続的 IP アドレスを入力し、**[チェック（check）]** アイコンをクリックします。

（注） IP アドレスが Nexus ダッシュボード データ プールに関連付けられていることを確認します。2 つのメンバー ファブリックを持つマルチサイトの EP を可視化して追跡するには、2 つの永続的な IP アドレスが必要です。1 つの永続データ IP アドレスは EPL コンテナ IP として使用され、サイト 1 ファブリックとの BGP セッションが確立されます。サイト 2 ファブリックとのピアリングに使用できる新しい永続 IP アドレスが構成されます。

ステップ 4 VXLAN EVPN ファブリックのルート再配布を構成します。

ファブリック 1 のルート再配布

次の switch_freeform ポリシーは、ファブリック 1 BGW で使用できます。新しい **switch_freeform** ポリシーを作成するには、上記の例を参照してください。

下のサンプル構成例

```
ip prefix-list site-2-rr seq 5 permit 20.2.0.1/32 >> Site 2 RR
ip prefix-list site-2-rr seq 6 permit 20.2.0.2/32 >> Site 2 RR
ip prefix-list epl-subnet seq 5 permit 192.168.100.0/24 >> EPL Subnet

route-map bgp-to-ospf permit 10
   match ip address prefix-list site-2-rr
route-map ospf-to-bgp permit 10
   match ip address prefix-list epl-subnet

router ospf 100
   redistribute bgp 100 route-map bgp-to-ospf

router bgp 100
   address-family ipv4 unicast
       redistribute ospf 100 route-map ospf-to-bgp
```

ファブリック 2 のルート再配布

次の switch_freeform ポリシーは、ファブリック 2 BGW で使用できます。新しい **switch_freeform** ポリシーを作成するには、上記の例を参照してください。

下のサンプル構成例

```
ip prefix-list site-2-rr seq 5 permit 20.2.0.1/32 >> Site 2 RR
ip prefix-list site-2-rr seq 6 permit 20.2.0.2/32 >> Site 2 RR
ip prefix-list epl-subnet seq 5 permit 192.168.100.0/24 >> EPL Subnet

route-map bgp-to-ospf permit 10
  match ip address prefix-list epl-subnet
route-map ospf-to-bgp permit 10
  match ip address prefix-list site-2-rr

router ospf 200
  redistribute bgp 200 route-map bgp-to-ospf

router bgp 200
    address-family ipv4 unicast
        redistribute ospf 200 route-map ospf-to-bgp
```

ステップ 5 EPL を設定するには、**[LAN]** > **[ファブリック（Fabrics）]** > **[ファブリックの概要（Fabric Overview）]** を選択します。

ステップ 6 **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[アクション（Actions）]** > **[その他（More）]** > **[エンドポイント ロケータの構成（Configure EndPoint Locator）]** を選択します

ステップ 7 ドロップダウンリストから、スパイン/ルート リフレクタ RR をホストするファブリック上の適切なスイッチを選択します。

適切な選択を行い、さまざまな入力を確認したら、**[構成の保存（Save Config）]**をクリックして、EPL を有効にします。EPLの有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPLは正常に有効化されます。EPL が有効になると、永続 IP が使用されます。

ファブリック 1 およびファブリック 2 で有効になっている EPL は正常に表示できます。EP を表示および追跡するには、エンドポイント ロケータのモニタリングセクションを参照してください。

vPC ファブリック ピアリング スイッチのエンドポイント ロケータの構成

ネットワーク管理者は、物理ピア リンクまたは仮想ピア リンクを使用して、スイッチのペア間に vPC を作成できます。 vPC ファブリック ピアリングは、vPC ピア リンクの物理ポートを無駄にするオーバーヘッドのない、拡張されたデュアルホーミング アクセス ソリューションを提供します。仮想ピア リンクの場合でも、リンクおよびノード レベルの冗長性のために、EPL は引き続きリーフ スイッチの vPC ペアに接続できます。ただし、EPL の最初のホップとして VXLAN VLAN（エニーキャスト ゲートウェイ）が使用されます。VXLAN VLAN はテナント VRF の一部になりますが、スパイン/RR の loopback0 アドレスは、VXLAN アンダーレイを介してのみ到達可能です。そのため、IP 通信を確立するために、テナント VRF とデフォルト VRF の間でルートリーキングが構成されます。詳細については、vPC ファブリック ピアリングのセクションを参照してください。

vPC ファブリック ピアリング スイッチのエンドポイント ロケータを構成するには、次の手順を実行します。

手順

ステップ 1 Cisco Nexus Dashboard で永続 IP アドレスを構成する必要があります。Nexus Dashboard で、**[管理コンソール（Admin Console）]**>**[インフラストラクチャ（Infrastructure）]**>**[クラスタ構成（Cluster Configuration）]**を選択します。

ステップ 2 **[全般（General）]** タブの、**[外部サービス プール（External Service Pools）]** カードで、**[編集（Edit）]** アイコンをクリックします。

[外部サービスプール（External Service Pools）] ウィンドウが表示されます。

ステップ 3 **[データ サービス IP（Data Service IP's）]** に永続的 IP アドレスを入力し、**[チェック（check）]** アイコンをクリックします。

ステップ 4 vPC ファブリック ピアリング スイッチでテナント VRF およびエニーキャスト ゲートウェイを作成します。

2 つのイメージを追加

ステップ 5 テナント VRF とデフォルト VRF 間のルート リークを構成します。

テナント VRF からデフォルト VRF にアドバタイズします。

次の switch_freeform ポリシーは、ND が接続されているファブリック リーフで使用できます。

```
ip prefix-list vrf-to-default seq 5 permit 192.168.100.0/24 >> EPL subnet
route-map vrf-to-default permit 10
  match ip address prefix-list vrf-to-default
vrf context epl_inband
  address-family ipv4 unicast
```

```
    export vrf default map vrf-to-default allow-vpn
router ospf UNDERLAY
   redistribute bgp 200 route-map vrf-to-default
```

デフォルト VRF からテナント VRF にアドバタイズします。

次の switch_freeform ポリシーは、ND が接続されているファブリック リーフで使用できます。

```
ip prefix-list default-to-vrf seq 5 permit 20.2.0.3/32 >> Spine loopback IP
ip prefix-list default-to-vrf seq 6 permit 20.2.0.4/32 >> Spine loopback IP
route-map default-to-vrf permit 10
   match ip address prefix-list default-to-vrf
vrf context epl_inband
   address-family ipv4 unicast
       import vrf default map default-to-vrf
        router bgp 200
   address-family ipv4 unicast
       redistribute ospf UNDERLAY route-map default-to-vrf
```

ステップ 6 ファブリック レベルで EPL を有効にします。

a) EPL を設定するには、**[LAN]** > **[ファブリック（Fabrics）]** > **[ファブリックの概要（Fabric Overview）]** を選択します。

b) **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[アクション（Actions）]** > **[その他（More）]** > **[エンドポイント ロケータの構成（Configure EndPoint Locator）]** を選択します

c) ドロップダウンリストから、スパイン/ルートリフレクタ RR をホストするファブリック上の適切なスイッチを選択します。

適切な選択を行い、さまざまな入力を確認したら、**[構成の保存（Save Config）]**をクリックして、EPL を有効にします。EPLの有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPLは正常に有効化されます。EPL が有効になると、永続 IP が使用されます。

外部ファブリックのエンドポイント ロケータの構成

Nexusダッシュボードファブリック コントローラでは、Easy ファブリックに加えて、外部ファブリックにインポートされるスイッチで構成される VXLAN EVPN ファブリックの EPL を有効にできます。外部ファブリックは、の **[ファブリック モニタ モード (Fabric Monitor Mode)]** フラグ (**[外部ファブリック設定 (External Fabric Settings)]**) の選択に基づいて、管理対象モードまたはモニタ対象モードにすることができます。Nexusダッシュボードファブリック コントローラからモニタのみされ、設定されていない外部ファブリックの場合、このフラグは無効になります。そのため、OOB 経由で、または CLI を使用して、スパインの BGP セッションを設定する必要があります。サンプル テンプレートを確認するには、 アイコンをクリックして、EPL を有効にしながら必要な設定を表示します。

[外部ファブリック設定 (External Fabric settings)] の **[ファブリック モニタ モード (Fabric Monitor Mode)]** チェックボックスがオフの場合でも、EPL はデフォルトの **[ファブリックの設定 (Configure my fabric)]** オプションを使用してスパイン/RRを設定できます。ただし、EPL を無

効にすると、スパイン/RR のルータ bgp 設定ブロックが消去されます。これを防ぐには、BGP ポリシーを手動で作成し、選択したスパイン/RR にプッシュする必要があります。

eBGP EVPN ファブリックのエンドポイント ロケータの構成

VXLAN EVPN ファブリックの EPL は有効にできます。この場合、eBGP がアンダーレイ ルーティングプロトコルとして使用されます。eBGP EVPN ファブリック展開では、iBGP に似た従来の RR は存在しないことに注意してください。インバンドサブネットの到達可能性は、ルートサーバーとして動作するスパインにアドバタイズする必要があります。Cisco Nexusダッシュボード ファブリック コントローラ Web UIから eBGP EVPN ファブリックの EPL を設定するには、次の手順を実行します。

Procedure

ステップ 1 **[LAN] > [ファブリック（Fabrics）]** を選択します。

eBGP を設定するファブリックを選択するか、**Easy_Fabric_eBGP** テンプレートを使用して eBGP ファブリックを作成します。

ステップ 2 すべてのリーフで一意の ASN を設定するには、**leaf_bgp_asn** ポリシーを使用します。

ステップ 3 各リーフに **ebgp_overlay_leaf_all_neighbor** ポリシーを追加します。

[スパイン IP リスト (Spine IP List)] にスパインの BGP インターフェイスの IP アドレス（通常は loopback0 の IP アドレス）を入力します。

[BGP アップデートソース インターフェイス (BGP Update-Source Interface)] にリーフの BGP インターフェイス（通常は loopback0）を入力します。

ステップ 4 **ebgp_overlay_spine_all_neighbor** ポリシーを各スパインに追加します。

[リーフ IP リスト (Leaf IP List)] にリーフの BGP インターフェイスの IP（通常は loopback0 の IP）を入力します。

[リーフの BGP ASN (Leaf BGP ASN)] に、**[リーフ IP リスト (Leaf IP List)]** と同じ順序でリーフのASNを入力します。

[BGP アップデートソース インターフェイス (BGP Update-Source Interface)] に、スパインの BGP インターフェイス（通常は loopback0）を入力します。

インバンド接続が確立された後も、EPL 機能の有効化の状態はそれまでにリストされていたものと同じままです。EPL は、スパインで実行されているルート サーバーの iBGP ネイバーになります。

エンドポイント ロケータの監視

エンドポイント ロケータに関する情報は、単一のランディング ページまたはダッシュボードに表示されます。ダッシュボードには、すべてのアクティブなエンドポイントに関するデータがほぼリアルタイムで（30秒ごとに更新されて）1つのペインに表示されます。このダッシュボードに表示されるデータは、**[範囲（Scope）]** ドロップダウン リストで選択した範囲によって異なります。Nexusダッシュボード ファブリック コントローラ 範囲階層はファブリックから始まります。ファブリックは、マルチサイト ドメイン（MSD）にグループ化できます。MSDのグループはデータセンターを構成します。エンドポイント ロケータ ダッシュボードに表示されるデータは、選択した範囲に基づいて集約されます。このダッシュボードから、[エンドポイント履歴（Endpoint History）]、[エンドポイント検索（Endpoint Search）]、および[エンドポイント寿命（Endpoint Life）] にアクセスできます。

（注） これは、Nexus Dashboard Fabric Controller、Release 12.0.1a のフィーチャのプレビューです。ラボセットアップでのみ、ベータ版としてマークされたこの機能を使用することをお勧めします。実稼働環境でこれらのフィーチャを使用しないでください。

エンドポイント ロケータの削除

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からエンドポイント ロケータを無効にするには、次の手順を実行します。

Procedure

ステップ 1 **[エンドポイント ロケータ（Endpoint Locator）] > [設定（Configure）]** を選択します。

[エンドポイント ロケータ（Endpoint Locator）] ウィンドウが表示されます。**[範囲（SCOPE）]** ドロップダウン リストから必要なディスクを選択します。選択したファブリックのファブリック設定詳細が表示されます。

ステップ 2 [無効（Disable）] をクリックします。

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