



エンドポイント ロケータ

- [エンドポイント ロケータ \(1 ページ\)](#)
- [エンドポイント ロケータの監視 \(23 ページ\)](#)

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) ((IPv4 and/or IPv6))]とMACアドレスをもつ任意のもので、Cisco DCNM リリース 11.3(1) から、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、ベアメタルサーバー、サービス アプライアンスなどです。



重要

- EPLは、VXLAN BGP EVPN ファブリック展開でDCNM 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、EasyeBGP 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。Cisco DCNM リリース 11.3(1) 以降、EPL はMAC のみのエンドポイントを表示することもできます。EPL の構成時に **[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、通常は DCNM 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、DCNM から RR への IP 到達可能性が必要です。これは、DCNM eth2 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ー (or Route Servers)]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。リリース 11.2(1) から、ファブリックは、イーजी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、DCNM 11.2) において適切な BGP 構成でスパインまたは RR を自動的に構成するオプションで有効にできます。
- Cisco DCNM リリース 11.3(1) 以降、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。これは、クラスタモードでのみサポートされます。
- Cisco DCNM リリース 11.3(1) 以降、EPL はマルチサイトドメイン (MSD) でサポートされます。
- Cisco DCNM リリース 11.3(1) 以降、IPv6 アンダーレイがサポートされます。
- ハイアベイラビリティのサポート
- 最大 180 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。
- サポートされるスケール：ファブリックあたり 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 100K を超えてはなりません。

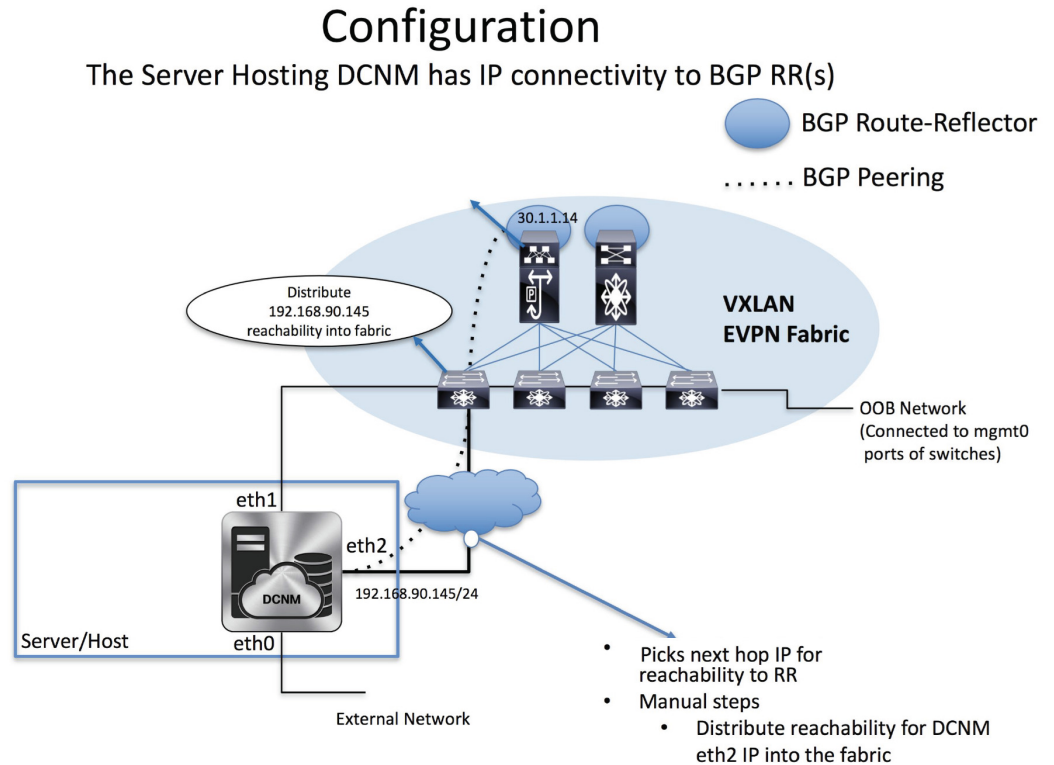
Cisco DCNM リリース 11.4(1) から、すべてのファブリックのエンドポイントの合計数が 100K を超えると、アラームが生成され、ウィンドウの右上にある **[アラーム (Alarms)]** アイコンの下にリストされます。このアイコンは、新しいアラームが生成されるたびに点滅し始めます。

EPL の詳細については、次の項を参照してください。

エンドポイント ロケータの構成

DCNM OVA または ISO インストールには、次の 3 つのインターフェイスが付属しています。

- 外部アクセス用のeth0インターフェイス
- ファブリック管理用のeth1インターフェイス（アウトオブバンドまたはOOB）
- インバンドネットワーク接続用のeth2インターフェイス



eth1インターフェイスは、レイヤ2またはレイヤ3隣接のmgmt0インターフェイスを介してデバイスに到達可能性を提供します。これにより、DCNMは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。EPLでは、DCNMとルートリフレクタの間でBGPピアリングが必要です。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、DCNMからファブリックへのインバンドIP接続が必要です。この目的で、コマンドを使用してeth2インターフェイスを設定できます。**appmgr setup inbandappmgr update network-properties** オプションで、Cisco DCNMのインストール時にeth2インターフェイスを構成できます。

すでに構成されているインバンドネットワーク（eth2インターフェイス）を変更する必要がある場合は、コマンドを実行して、**appmgr setup inbandappmgr update network-properties** コマンドを再度実行します。**appmgr setup inbandappmgr update network-properties** コマンドを実行するには、「[DCNMインストール後のネットワークプロパティの編集](#)」を参照してください。

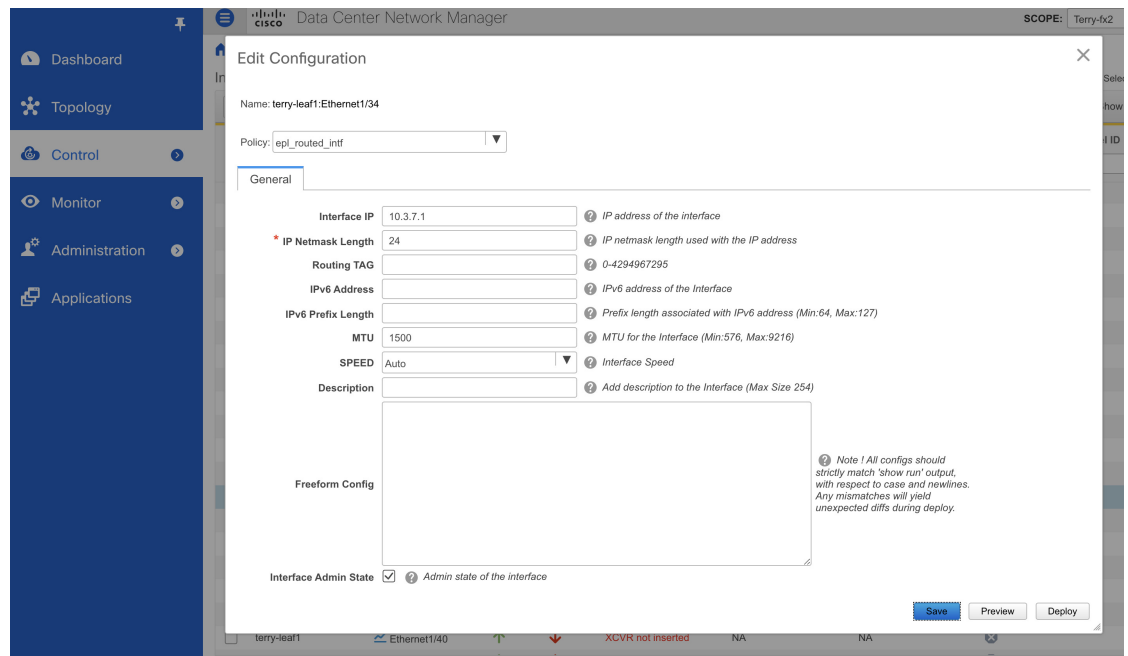


Note DCNM 上の eth2 インターフェイスの設定は、ファブリック内のデバイスへのインバンド接続を必要とするアプリケーションの前提条件です。これには EPL とネットワーク インサイトのリソース (NIR) が含まれます。

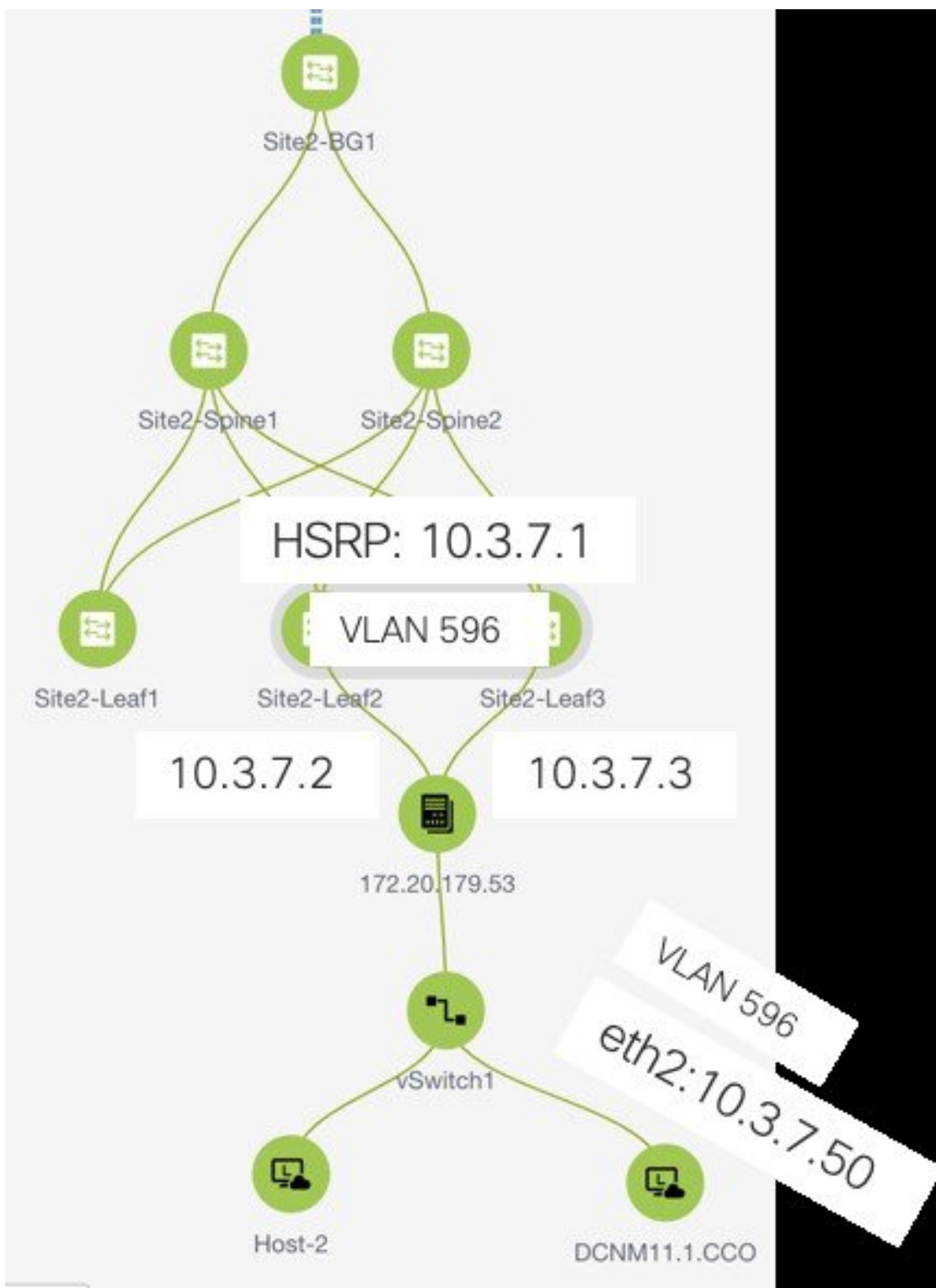


Note スタンドアロンモードで EPL を構成するには、単一のネイバーを EPL に追加する必要があります。DCNM eth2 IP アドレスは EPL IP です。

ファブリック側では、スタンドアロン DCNM 展開の場合、DCNM eth2 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る場合、そのインターフェイスは **[epl_routed_intf]** テンプレートを 사용하여構成できます。ファブリック内の IGP として IS-IS または OSPF を使用する場合は、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、DCNM がインストールされているサーバー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。OVA DCNM 展開では、ポートチャネルを介してサーバーをスイッチに接続できます。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 DCNM 上の eth2 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。次の図に、シナリオの設定例を示します。



この例では、DCNM VM を搭載したサーバーは、それぞれ Site2-Leaf2 および Site2-Leaf3 という名前のスイッチの vPC ペアにデュアル接続されています。IPサブネット10.3.7.0/24に関連付

けられたVLAN 596は、インバンド接続に使用されます。次の図に示すように、インターフェイスvpc trunkホストポリシーを使用して、vPCホストポートをサーバに向けて設定できます。

Add Interface

* Type: virtual Port Channel (vPC)
 * Select a vPC pair: Site2-Leaf2--Site2-Leaf3
 * vPC ID: 1
 * Policy: int_vpc_trunk_host_11_1

Note : PeerOne = Site2-Leaf2 & PeerTwo = Site2-Leaf3

General

Peer-1 Member Interfaces: e1/47 A list of member interfaces for Peer-1 [e.g. e1/5,eth1/7-9]

Peer-2 Member Interfaces: e1/47 A list of member interfaces for Peer-2 [e.g. e1/5,eth1/7-9]

* Port Channel Mode: on Channel mode options: on, active and passive

* Enable BPDU Guard: true Enable spanning-tree bpduguard

Enable Port Type Fast: Enable spanning-tree edge port behavior

* MTU: jumbo MTU for the Port Channel

* Peer-1 Trunk Allowed Vlan: 596 Peer-1 Trunk Allowed Vlans

* Peer-2 Trunk Allowed Vlan: 596 Peer-2 Trunk Allowed Vlans

Buttons: Save, Preview, Deploy

Site2-Leaf2のHSRP設定では、次の図に示すようにswitch_freeformポリシーを使用できます。

Edit Policy

Policy ID: POLICY-237060
 Entity Type: SWITCH
 Template Name: switch_freeform_config
 Entity Name: SWITCH

* Priority (1-1000): 500

General

Variables:

* Freeform Config CLI

```
feature hsrp
vlan 596
interface vlan 596
ip address 10.3.7.3/24
ip router ospf UNDERLAY area 0.0.0.0
no shutdown
no ip redirects
no ipv6 redirects
hsrp 10
ip 10.3.7.1
```

Additional CLI not in the

Buttons: Save, Deploy, Cancel

SVI 596にIPアドレス10.3.7.2/24を使用しながら、Site2-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10.3.7.1に設定されたeth2 インターフェイスを介してDCNM からファブリックへのインバンド接続が確立されます。

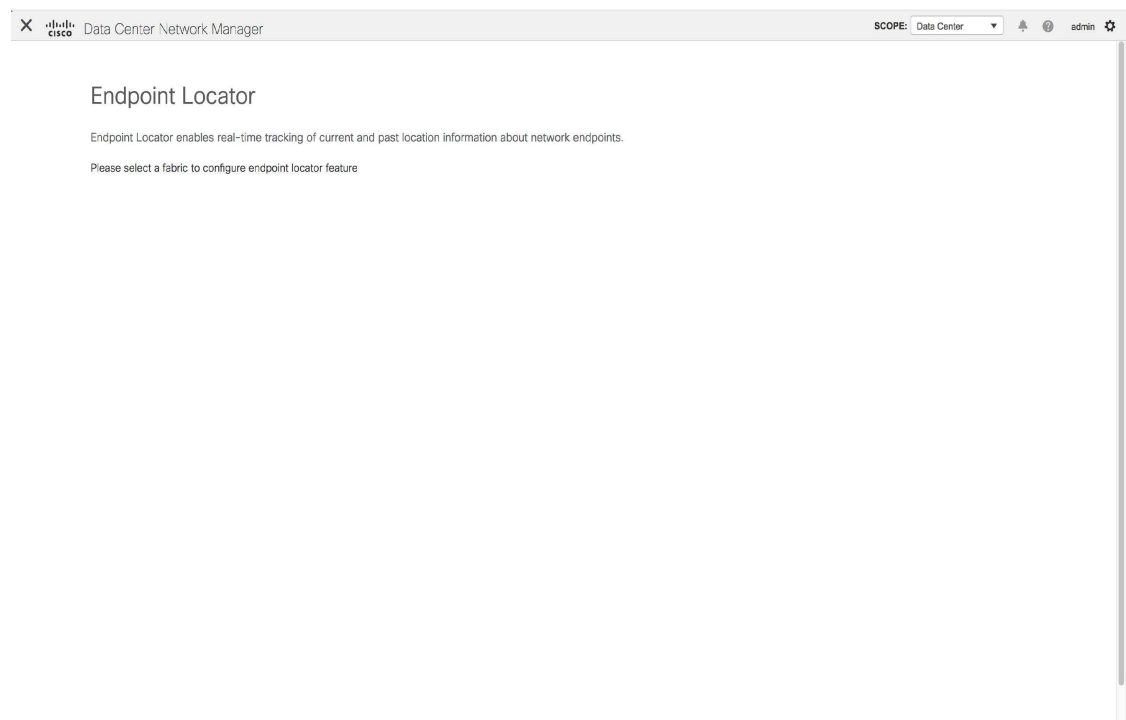
物理または仮想DCNM とファブリック間のインバンド接続を確立した後、BGP ピアリングを確立できます。

EPL の構成時に、ルートリフレクタ (RR) はBGP ピアとしてDCNM を受け入れるように構成されます。同じ構成中に、DCNM は、eth2 ゲートウェイを介してスパイン/RR 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。

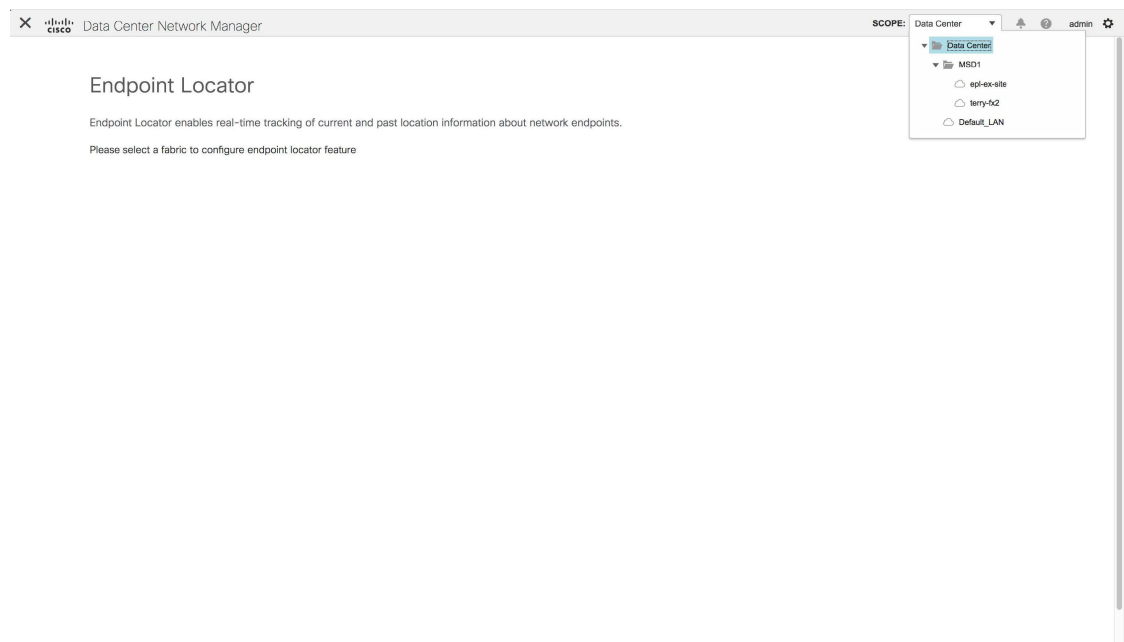


Note Cisco DCNM は、ASN、RR、IP などのピアリングの確立に関する情報を収集するためにBGP RR をクエリします。

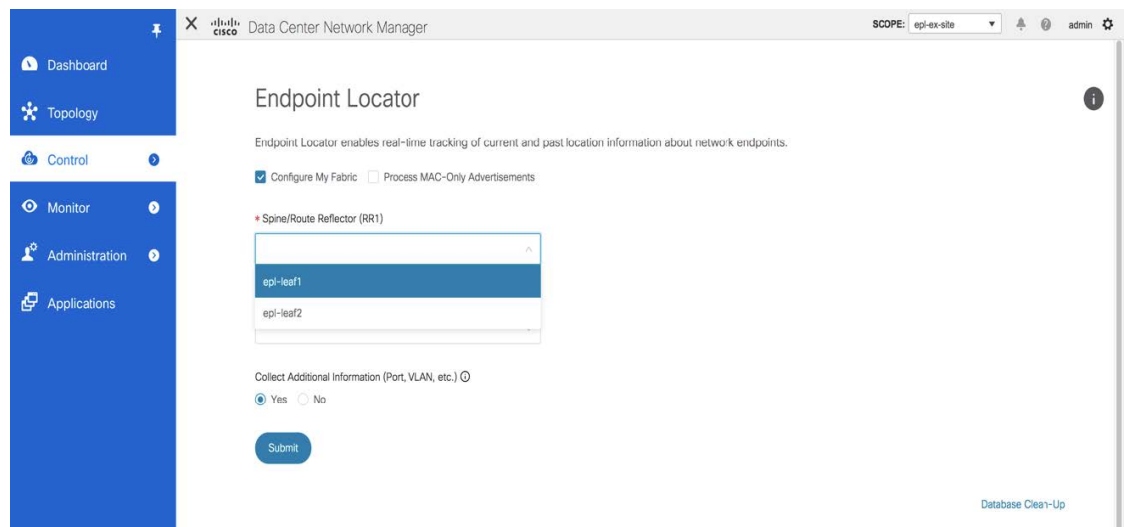
Cisco Web UI からエンドポイントロケータを構成するには、[制御 (Control)] > [エンドポイントロケータ (Endpoint Locator)] > [構成 (Configure)] の順に選択します。[エンドポイントロケータ (Endpoint Locator)] ウィンドウが表示されます。



エンドポイントのアクティビティを追跡するためにエンドポイントロケータ機能を有効にする必要があるファブリックを[範囲 (Scope)] ドロップダウンリストから選択します。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。Cisco DCNM はRR とピアリングします。



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。DCNMによってモニタ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、それらはDCNMによって構成されていないファブリックであるため、このオプションはグレー表示されます。

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、[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。

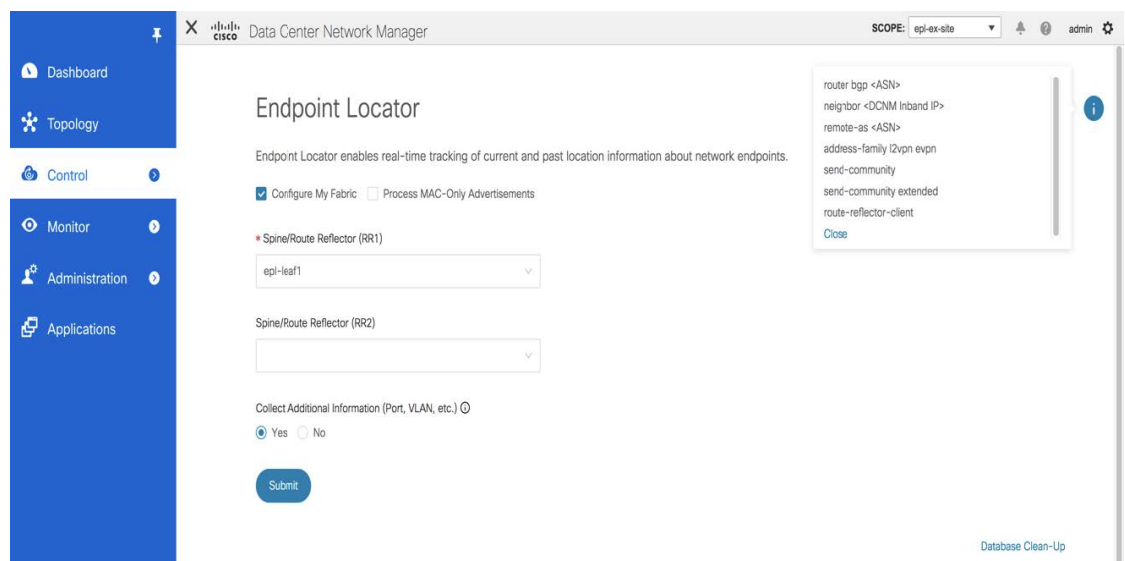
[追加情報の収集 (Collect Additional Information)]で[はい (Yes)]を選択し、EPL機能を有効にしながらPORT、VLAN、VRFなどの追加情報の収集を有効にします。追加情報を収集するには、スイッチ、ToR、およびリーフでNX-APIがサポートされ、有効になっている必要があります。[いいえ (No)]オプションを選択すると、この情報はEPLによって収集および報告されません。



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。

Cisco DCNM を使用して EPL を構成する方法を示すビデオも視聴できます。「[エンドポイントロケータの構成](#)」を参照してください。

Cisco DCNM リリース 11.4(1)以降、**[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構成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。



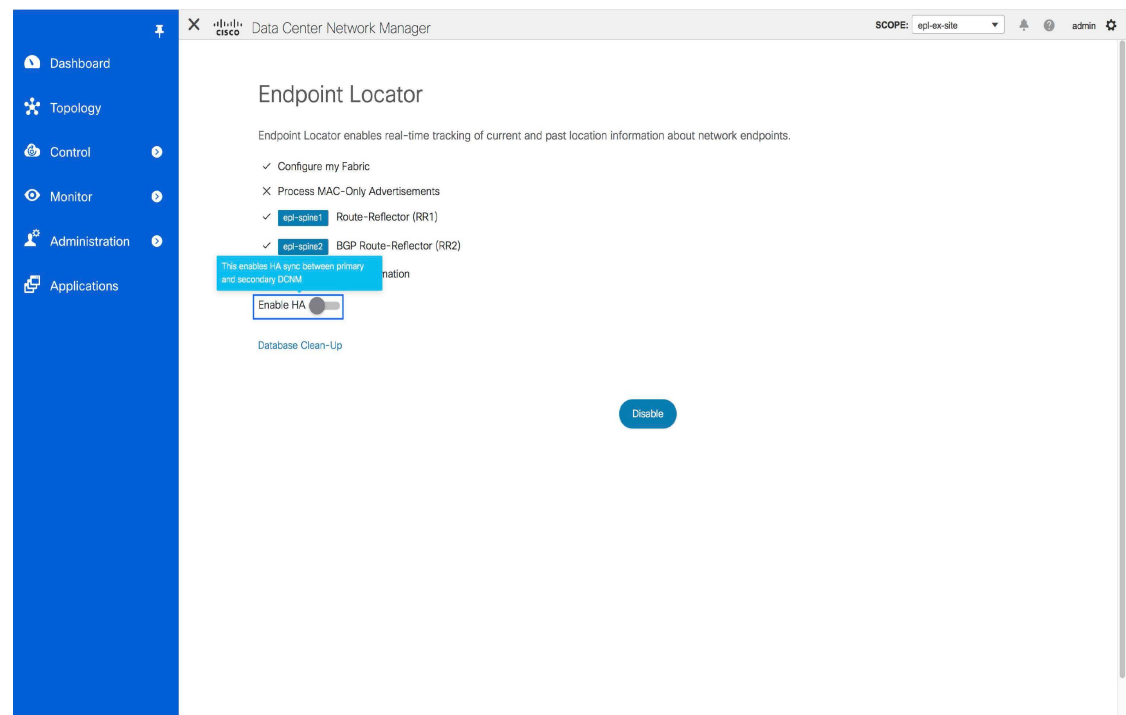
適切な選択を行い、さまざまな入力を確認したら、[送信 (Submit)] をクリックして EPL を有効にします。EPL の有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPL は正常に有効化されます。

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。DCNM は、選択された RR に接続し、ASN を決定します。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、DCNM 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。ネイティブ HA DCNM 展開では、プライマリおよびセカンダリの両方の DCNM eth2 インターフェイス IP が BGP ネイバーとして追加されますが、いずれか一方のみがアクティブになります。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モニタリング](#)」を参照してください。

高可用性の有効化

非 HA モードの展開で EPL が DCNM で有効になり、その後 DCNM が HA モードに移行するシナリオを考えます。このようなシナリオでは、[Enable HA] トグルが [Endpoint Locator] ウィンドウに表示されます。**[HA の有効化 (Enable HA)]** ノブを切り替えて、プライマリとセカンダリ DCNM 間の高可用性同期を有効にします。



Cisco DCNM Web UI から高可用性同期を有効にするには、次の手順を実行します。

Procedure

- ステップ1 [Control]>[エンドポイントロケータ (Endpoint Locator)]>[構成 (Configure)]を選択します。
- ステップ2 [Enable HA]ボタンを切り替えます。

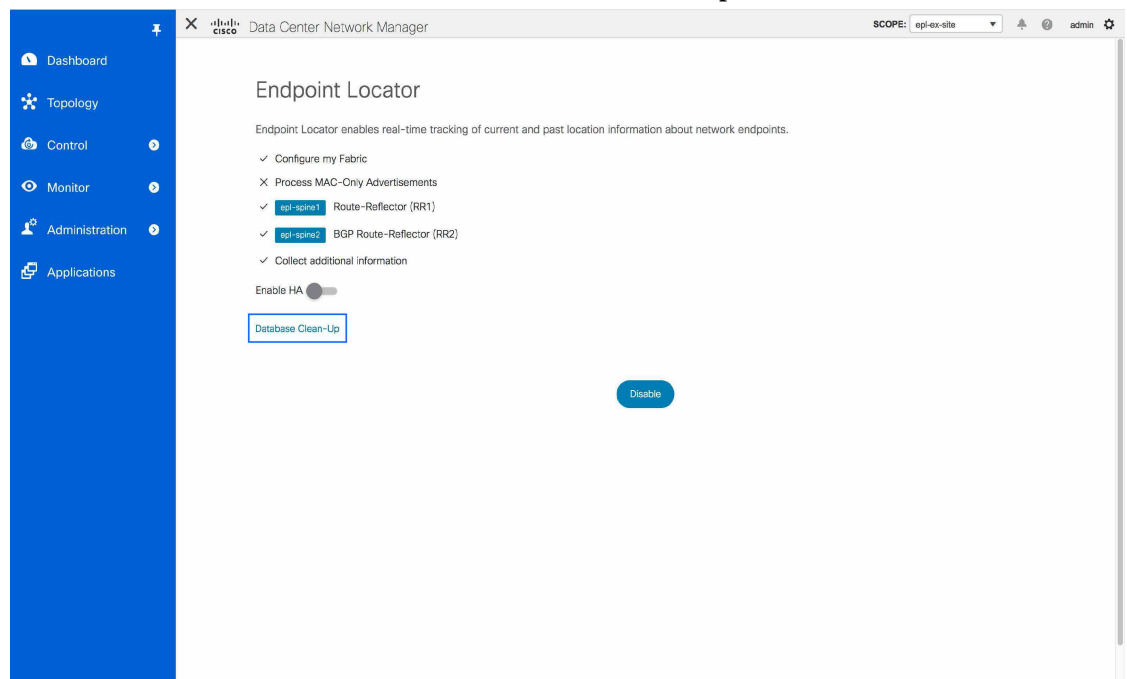
エンドポイントデータベースのフラッシュ

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。Cisco DCNM リリース 11.4(1) 以降、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くても、エンドポイントデータベースをフラッシュできます。

Cisco DCNM 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。

Procedure

- ステップ1 [制御 (Control)]>[エンドポイントロケータ (Endpoint Locator)]>[構成 (Configure)]を選択し、[データベースクリーンアップ (Database Clean-Up)]をクリックします。



データベースに保存されているすべてのエンドポイント情報がフラッシュされることを示すメッセージとともに警告が表示されます。

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。

DCNM 高可用性モードでのエンドポイント ロケータの構成



Note ネイティブ HA モードで EPL を設定するには、2つのネイバーを EPL に追加する必要があります。DCNM プライマリ eth2 および DCNM セカンダリ eth2 アドレスである EPL IP。

実稼働展開の場合は、DCNM ノードのネイティブ HA ペアが推奨されています。DCNM アクティブ ノードとスタンバイ ノードはレイヤ 2 隣接である必要があるため、それぞれの eth2 インターフェイスは同じ IP サブネットまたは VLAN の一部である必要があります。さらに、両方の DCNM ノードに同じ eth2 ゲートウェイを構成する必要があります。推奨オプションは、DCNM アクティブ ノードとスタンバイ ノードを Nexus スイッチの vPC ペア（リーフの場合もあります）に接続し、単一リンク障害、単一デバイス障害、または単一 DCNM ノード障害が発生した場合に十分なフォールトトレランスを確保することです。

次の例は、Cisco DCNM ネイティブ HA アプライアンスに対する **appmgr update network-properties** コマンドの出力例を示しています。この例では、1.1.1.2 はプライマリ eth2 インターフェイス IP アドレス、1.1.1.3 はスタンバイ eth2 インターフェイス IP アドレス、1.1.1.1 はデフォルト ゲートウェイ、1.1.1.4 はインバンドの仮想 IP (VIP) です。

Cisco DCNM プライマリ アプライアンスで、次のようにします。

```
appmgr update network-properties session start
appmgr update network-properties set ipv4 eth2 1.1.1.2 255.255.255.0 1.1.1.1
appmgr update network-properties set ipv4 peer2 1.1.1.3
appmgr update network-properties set ipv4 vip2 1.1.1.4 255.255.255.0
appmgr update network-properties session apply
appmgr update ssh-peer-trust
```

Cisco DCNM セカンダリ アプライアンスで、次のようにします。

```
appmgr update network-properties session start
appmgr update network-properties set ipv4 eth2 1.1.1.3 255.255.255.0 1.1.1.1
appmgr update network-properties set ipv4 peer2 1.1.1.2
appmgr update network-properties set ipv4 vip2 1.1.1.4 255.255.255.0
appmgr update network-properties session apply
appmgr update ssh-peer-trust
```

プライマリ ノードとセカンダリ ノードの両方からファブリックへのインバンド接続が確立された後、Cisco DCNM Web UI からエンドポイント ロケータを DCNM HA モードで構成するには、次の手順を実行します。

Procedure

- ステップ 1 [Control]>[エンドポイント ロケータ (Endpoint Locator)]>[構成 (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、ファブリック設定の詳細が表示されます。
- ステップ 2 DCNMHAモードでエンドポイント ロケータを構成するには、[範囲 (SCOPE)] ドロップダウンリストからファブリックを選択します。
- ステップ 3 ドロップダウン リストからルート リフレクタ (RR) を選択します。
- ステップ 4 [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か PORT、VLAN、VRF などの追加情報の収集を有効にします。[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。
- ステップ 5 [送信 (Submit)] をクリックします。

What to do next

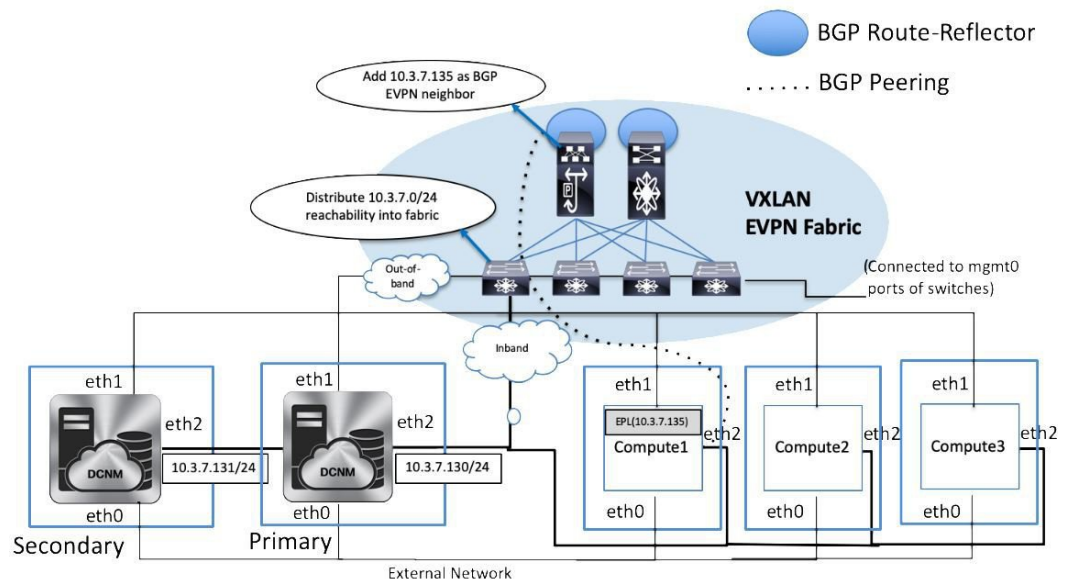
エンドポイント ロケータを HA モードで設定すると、エンドポイント ロケータ ダッシュボードでエンドポイント アクティビティやエンドポイント履歴などの詳細を表示できます。これらの詳細を表示するには、[監視 (Monitor)]>[エンドポイント ロケータ (Endpoint Locator)]>[検出 (Explore)] の順に移動します。

DCNM クラスタ モードでのエンドポイント ロケータの構成



- (注) クラスタモードでEPLを設定するには、単一のネイバーをEPLに追加する必要があります。DCNM EPL コンテナのインバンド IP アドレスはEPLのIPです。

DCNM クラスタ モードの展開では、DCNM ノードに加えて、追加の3つのコンピューティングノードが展開内に存在するようになります。クラスタモードでのアプリケーションの展開については、「クラスタモードの Cisco DCNM」を参照してください。



DCNM クラスタモードでは、EPL を含むすべてのアプリケーションがコンピューティングノードで実行されます。DCNM アプリケーションフレームワークは、コンピューティングノードで実行されるすべてのアプリケーションの完全な耐用周期の管理を行います。EPL インスタンスは、コンピューティングノードに割り当てられたインバンドプールから割り当てられた独自の IP アドレスを持つコンテナとして実行されます。この IP アドレスは、eth2 またはインバンドインターフェイスに割り当てられたものと同じ IP サブネットにあります。EPL 機能を有効にすると、EPL インスタンスはこの IP アドレスを使用してスパイン/RR と BGP ピアリングを形成します。EPL インスタンスをホストしているコンピューティングノードがダウンすると、残りの 2 つのコンピューティングノードのいずれかで EPL インスタンスが自動的に再生成されます。EPL インスタンスに関連付けられているすべての IP アドレスおよびその他のプロパティは保持されます。

コンピューティングノードのレイヤ 2 隣接関係（アジャセンシー）要件により、コンピューティングノードの eth2 インターフェイスは DCNM ノードと同じ IP サブネットの一部である必要があります。この場合もやはり、同じ vPC ペアのスイッチにコンピューティングノードを接続することが、推奨される導入オプションです。以下に示すように、クラスタモード DCNM の OVA 設定では、eth2 インターフェイスに対応するポートグループで無差別モードが有効になっていることを確認してください。

EPL-Inband - Edit Settings

Properties			
Security	Promiscuous mode	<input checked="" type="checkbox"/> Override	Accept
Traffic shaping	MAC address changes	<input checked="" type="checkbox"/> Override	Accept
Teaming and failover	Forged transmits	<input checked="" type="checkbox"/> Override	Accept

CANCEL

OK

DCNM クラスタ モードの EPL 機能の有効化は、非クラスタ モードの有効化と同じです。主な違いは、スパイン/RR では、EPL インスタンスに割り当てられた IP アドレスを指す単一の BGP ネイバーシップだけが必要なことです。非クラスタモードでの DCNM ネイティブ HA 導入では、すべてのスパイン/RR に常に 2 つの構成済み BGP ネイバーがあります。1 つは DCNM プライマリ eth2 インターフェイスを指し、もう 1 つは DCNM セカンダリ eth2 インターフェイスを指します。ただし、アクティブになるネイバーは常に 1 つだけです。

外部ファブリックのエンドポイント ロケータの構成

DCNM リリース 11.2(1) 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。DCNM からモニタ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

Cisco DCNM リリース 11.2(1) 以降、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。eBGPEVPN 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ダプタイズする必要があります。Cisco DCNM Web UI から eBGP EVPN ファブリックの EPL を構成するには、次の手順を実行します。

Procedure

ステップ 1 [制御 (Control)] > [ファブリック ビルダ (Fabric Builder)] 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。

Add Fabric
✕

* Fabric Name :

* Fabric Template :

General	EVPN	vPC	Advanced	Manageability	Bootstrap	Configuration Backup
<p>* BGP ASN for Spines <input type="text" value="65535"/> ⓘ 1-4294967295 1-65535[,0-65535]</p> <p>* BGP AS Mode <input type="text" value="Multi-AS"/> ⓘ Multi-AS: Unique ASN per Leaf/Border Dual-AS: One ASN for all Leafs/Borders</p> <p>* Routing Loopback Id <input type="text" value="0"/> ⓘ 0-512</p> <p>* Underlay Subnet IP Mask <input type="text" value="30"/> ⓘ Mask for Underlay Subnet IP Range</p> <p>Manual Underlay IP Address Allocation <input type="checkbox"/> ⓘ Checking this will disable Dynamic Underlay IP Address Allocations</p> <p>* Underlay Routing Loopback IP Range <input type="text" value="10.2.0.0/22"/> ⓘ Typically Loopback0 IP Address Range</p> <p>* Underlay Subnet IP Range <input type="text" value="10.4.0.0/16"/> ⓘ Address range to assign Numbered and Peer Link SVI IPs</p> <p>* Subinterface Dot1q Range <input type="text" value="2-511"/> ⓘ Per Border Dot1q Range For VRF Lite Connectivity (Min:2, Max:511)</p> <p>NX-OS Software Image Version <input type="text"/> ⓘ If Set, Image Version Check Enforced On All Switches. Images Can Be Uploaded From Control:Image Upload</p>						

ステップ 2 すべてのリーフで一意的 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 ロケータの削除

Cisco DCNM WebUI 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。

手順

ステップ 1 [Control] > [エンドポイント ロケータ (Endpoint Locator)] > [構成 (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。

エンドポイント ロケータのトラブルシューティング

エンドポイントロケータ機能の有効化に失敗する理由は複数あります。通常、適切なデバイスが選択され、使用する IP アドレスが正しく指定されている場合は、DCNM から BGP RR への接続が存在しないため、機能を有効にできません。これは、基本的な IP 接続が使用可能であることを確認するための健全性チェックです。次の図は、EPL 機能を有効にしようとしたときに発生したエラーシナリオの例を示しています。

EPL 機能が有効または無効になったときに発生した内容の詳細を示すログは、`/usr/local/cisco/dcm/fm/logs/epl.log`にある、`epl.log` ファイルに記載されています。次の例は、ファブリックの EPL 設定の進行状況を示す `epl.log` のスナップショットです。

```
2019.12.05 12:18:23 INFO [epl] Found DCNM Active Inband IP: 192.168.94.55/24
2019.12.05 12:18:23 INFO [epl] Running script: [sudo, /sbin/appmgr, setup, inband-route,
--host, 11.2.0.4]
2019.12.05 12:18:23 INFO [epl] Getting EPL configure progress for fabric 4
2019.12.05 12:18:23 INFO [epl] EPL Progress 2
2019.12.05 12:18:23 INFO [epl] [sudo, /sbin/appmgr, setup, inband-route, --host,
11.2.0.4] command executed, any errors? No
2019.12.05 12:18:23 INFO [epl] Received response:
2019.12.05 12:18:23 INFO [epl] Validating host route input
2019.12.05 12:18:23 INFO [epl] Done configuring host route
2019.12.05 12:18:23 INFO [epl] Done.
2019.12.05 12:18:23 INFO [epl] Running script: [sudo, /sbin/appmgr, setup, inband-route,
--host, 11.2.0.5]
2019.12.05 12:18:23 INFO [epl] [sudo, /sbin/appmgr, setup, inband-route, --host,
11.2.0.5] command executed, any errors? No
2019.12.05 12:18:23 INFO [epl] Received response:
2019.12.05 12:18:23 INFO [epl] Validating host route input
2019.12.05 12:18:23 INFO [epl] Done configuring host route
2019.12.05 12:18:23 INFO [epl] Done.
2019.12.05 12:18:23 INFO [epl] Running command: sudo /sbin/appmgr show inband
2019.12.05 12:18:24 INFO [epl] Received response: Physical IP=192.168.94.55/24
Inband GW=192.168.94.1
No IPv6 Inband GW found

2019.12.05 12:18:26 INFO [epl] Call:
http://localhost:35000/afw/apps?imtag=cisco:epl:2.0&fabricid=epl-ex-site, Received
response:
2019.12.05 12:18:26 INFO [epl] Epl started on AFW
```

EPL が正常に有効化されると、エンドポイント情報に関連付けられているすべてのデバッグ、エラー、および情報ログが、関連するファブリックのディレクトリの下の `/var/afw/applogs/` に保存されます。たとえば、`[test]` ファブリックで EPL が有効になっている場合、ログは `/var/afw/applogs/epl_cisco_test_afw_log/epl/` に置かれ、ファイル名 `afw_bgp.log.1` で始まります。ネットワークの規模とエンドポイントイベントの数に応じて、ファイルサイズが増加します。したがって、`afw_bgp.log` の最大数とサイズには制限があります。ファイルサイズは最大 100 MB、10 ファイルまで保存されます。



Note EPL は Docker コンテナ内のこのディレクトリにシンボリックリンクを作成するので、ネイティブにアクセスすると破損しているように見えます。

EPL は、BGP アップデートを使用してエンドポイント情報を取得します。これが機能するためには、エンドポイントを持つすべてのスイッチのスイッチループバックまたは VTEP インターフェイスの IP アドレスを DCNM で検出する必要があります。検証するには、Cisco DCNM の **[Web UI] > [ダッシュボード (Dashboard)] > [スイッチ (Switch)] > [インターフェイス (Interfaces)]** タブに移動し、対応するレイヤ 3 インターフェイス（通常はループバック）に関連付けられている IP アドレスとプレフィックスが正しく表示されるかどうかを確認します。

Cisco DCNM クラスタの導入で、EPL が BGP ピアリングを確立できず、アクティブな DCNM はスパインのループバック IP アドレスに ping を送信できるものの、EPL コンテナはできない場合、Cisco DCNM およびそのコンピューティング ノードの eth2 ポートグループで無差別 (Promiscuous) モードが **[受容 (Accept)]** に設定されていないことを意味します。この設定を変更すると、コンテナはスパインに ping を送信でき、EPL は BGP を確立します。

大規模なセットアップでは、スイッチからこの情報を取得するために 30 秒（Cisco DCNM で設定されたデフォルトタイマー）以上かかる場合があります。この場合、ssh.read-wait-timeout プロパティ (**[管理 (Administration)] > [DCNM サーバー (DCNM Server)] > [サーバー プロパティ (Server Properties)]**) をデフォルトの 30000 から、60000 以上の値に変更する必要があります。

大規模なセットアップでは、ダッシュボードに表示されるエンドポイントデータがいくらか不正確になることがあります。エンドポイント数が多い場合、パフォーマンスの精度は最大で約 1% 低下します。ダッシュボードが予想と大きく異なる場合は、DCNM にパッケージ化されている検証スクリプトを使用して有効性を確認できます。root として、/root/packaged-files/scripts/にある epl-rt-2.py スクリプトを実行します。このスクリプトを実行するには、RR/スパインの IP と、関連するユーザー名とパスワードが必要です。/root/packaged-files/scripts/ディレクトリは読み取り専用であるため、スクリプトはそのディレクトリの外部で実行する必要があります。たとえば、IP 10.2.0.5、ユーザ名 admin、パスワード cisco123 を使用してスパインのスクリプトを実行するには、作業ディレクトリを /root/ にして、/root/packaged-files/scripts/epl-rt-2.py -s 10.2.0.5 -u admin -p cisco123 を実行します。EPL ダッシュボードに予想された数値が表示されず、epl-rt-2.py スクリプトの出力がダッシュボードと大きく異なる場合は、テクニカルサポートにお問い合わせください。

クラスタモードでは、BGP はスパイン/RR と DCNM の間で確立されません。eth2 DCNM インターフェイスに対応するポートグループの **[無差別モード (Promiscuous mode)]** 設定が **[受容 (Accept)]** に設定されていることを確認します。接続がまだ確立されていない場合は、次の手順を実行して、DCNM の BGP クライアントとスパイン/RR 間の接続を確認します。

1. アクティブな DCNM でシェルを開いて、次のコマンドを実行します。
 - a. `docker service ls`
 - * EPL サービスの ID をメモします
 - b. `docker service ps $ID`

*[ノード (NODE)] フィールドをメモします、

c. *afw compute list -b*

*以前の ホスト名 (HostName) (ノード) に一致する HostIp をメモします。これは、EPL サービスが現在実行されているコンピューティング ノードです。

2. 手順 1-c でメモしたコンピューティング ノードでシェルを開き、次のコマンドを実行します。

a. *docker container ls*

EPL のコンテナ ID をメモします複数の EPL コンテナがある場合は、コンテナ名を確認して、どのコンテナがどのファブリックに対応しているかを確認します。命名スキームは `epl_cisco_ $ FabricName_afw` です。

b. *docker container inspect \$CONTAINER_ID*

*SandboxKeyの値をメモします

c. *nsenter --net=\$SandboxKey*

このコマンドにより、EPL コンテナのネットワーク名前空間に入ります。これで、`ifconfig`、`ip`、`ping` などのネットワーク コマンドは、シェルで `exit` コマンドを発行するまで、コンテナ内から実行されているかのように動作します。

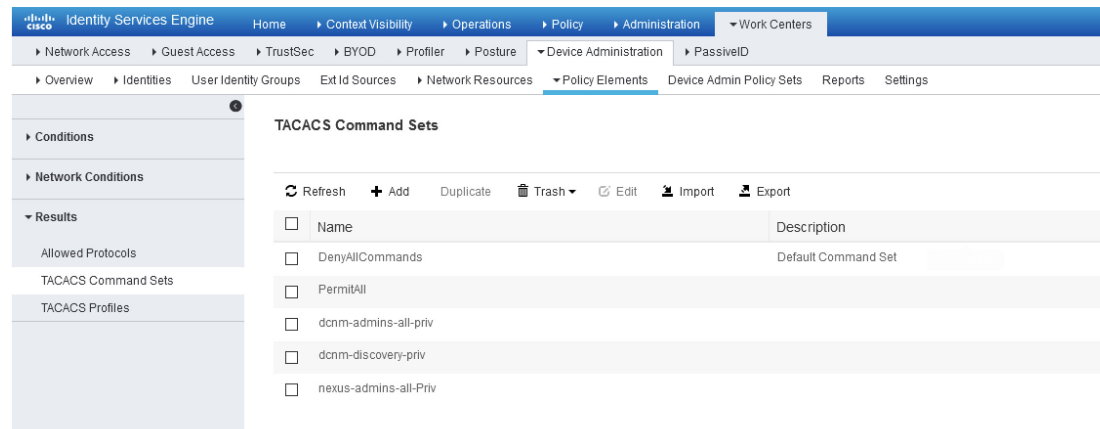
3. スパイン/RR に ping を送信してみます。DCNM クラスタに構成されているインバンド IP プールが、スイッチループバック IP と競合しないことを確認します。

ISE ポリシーが設定された EPL

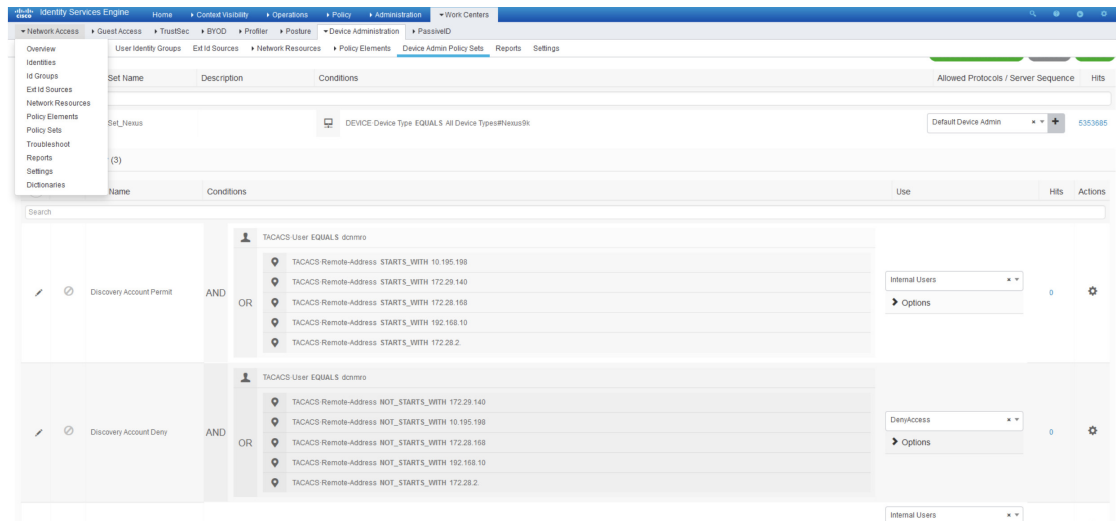
Cisco NX-OS リリース 9.3(4) 以前のリリースを実行しているスイッチで、AAA 構成が設定されているシナリオを考えます。AAA スwitchの構成例を次に示します。

```
feature tacacs+
tacacs-server host ISE_ACS_IP_ADDDDRESS 5 key 7 "Fewhg12345"
aaa group server tacacs+ AAA_TACACS
    server ISE_ACS_IP_ADDDDRESS
    use-vrf management
    source-interface mgmt0
aaa authentication login default group AAA_TACACS local
aaa authentication login console local
aaa authorization config-commands default group AAA_TACACS local
aaa authorization commands default group AAA_TACACS local
aaa accounting default group AAA_TACACS
aaa authentication login error-enable
```


`guestshell`、`run guestshell`、`show` といったコマンドにより設定された ISE サーバーは、ISE 内で作成された検出アカウントまたはポリシーにアクセスすることが許可されます。許可されるコマンドは、**[TACACS コマンド セット (TACACS Command Sets)]** ウィンドウで設定します。このウィンドウは、ISE の **[ポリシー エレメント (Policy Elements)]** タブの下にあります。



DCNM の eth0 IP およびファブリック デバイスのサブネットも許可されます。これは、[デバイス管理ポリシー セット (Device Admin Policy Sets)] ウィンドウで設定します。このウィンドウは、[デバイス管理 (Device Administration)] タブの下にあります。



これで、DCNMは、エンドポイントロケータ機能に必要なすべての **show** コマンドを実行するために検出アカウントを使用するように構成されます。ただし、スイッチ NXAPI の問題により、リクエスト IP がリモート AAA 認証要求に入力されていないため、AAA 検証が失敗します。 **show** コマンドは IP アドレスから発行されたものとは見なされないため、コマンドはブロックされ、EPL ダッシュボードに必要なエンドポイント情報が表示されなくなります。

回避策として、AAA ルールを緩和し、「ブランク」の送信者からの要求を許可することを推奨します。「空白」の送信者からの要求を許可するには、[ステータス (Status)] 列の下にある  アイコンをクリックします ([アカウント検出許可 (Discovery Account Permit)] と [アカウント検出拒否 (Discovery Account Deny)] の両方で、[デバイス管理ポリシーセット (Device Admin Policy Sets)] ウィンドウにあります)。[無効 (Disabled)] を選択して [保存 (Save)] をクリックします。

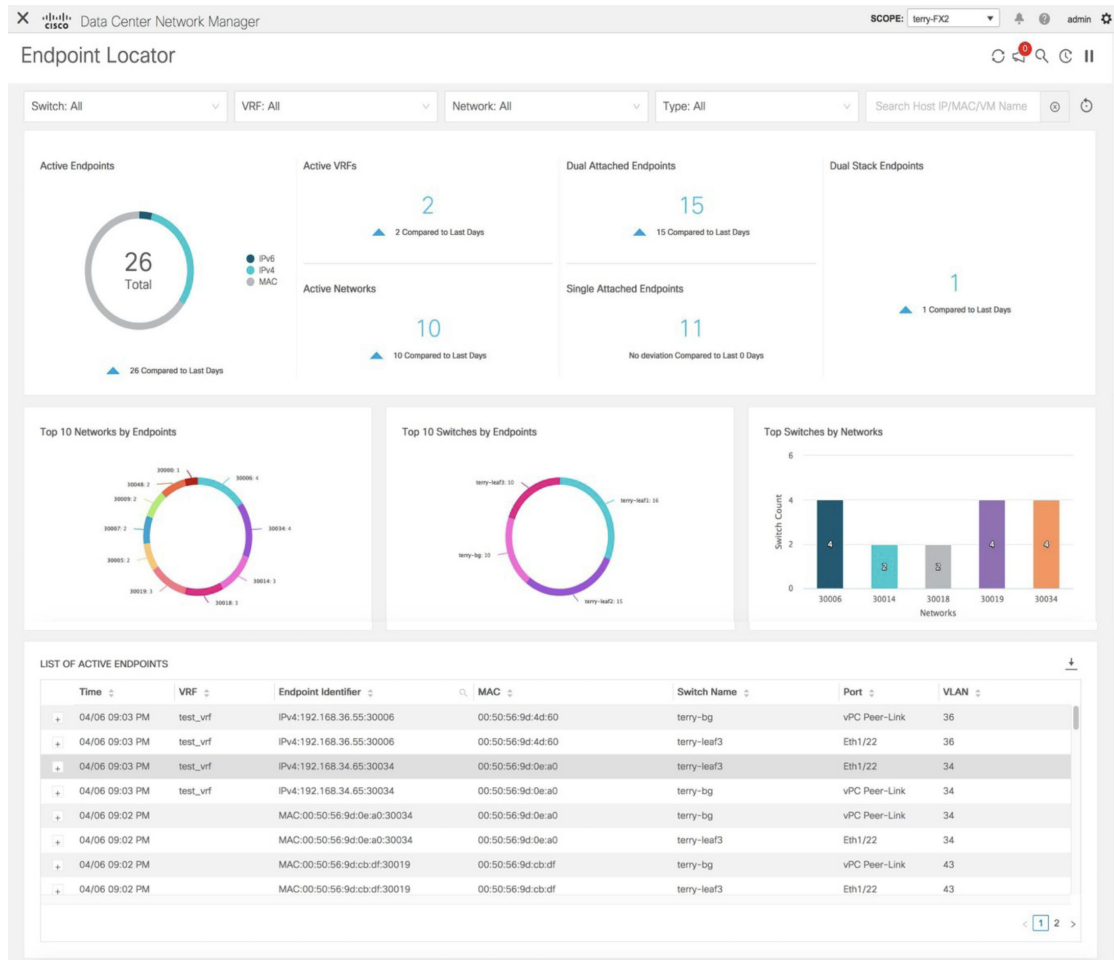
また、この問題は、Cisco NXOS リリース 9.3(5) 以降のリリースを実行しているスイッチでは発生しません。

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。DCNM 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。

エンドポイント ロケータ ダッシュボード

Cisco DCNM Web UI からエンドポイント ロケータの詳細を確認するには、**[モニタ (Monitor)]** > **[エンドポイント ロケータ (Endpoint Locator)]** > **[調査 (Explore)]** を選択します。エンドポイント ロケータ ダッシュボードが表示されます。

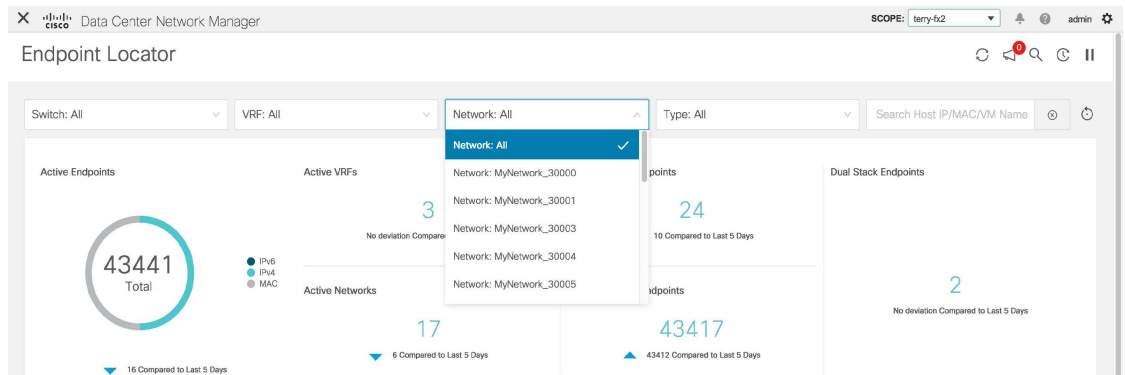


(注) Cisco DCNMリリース 11.3(1)からの規模の拡大により、システムがエンドポイントデータを収集してダッシュボードに表示するまでに時間がかかる場合があります。また、エンドポイントの一括追加または削除では、EPLダッシュボードに表示されるエンドポイント情報が最新のエンドポイントデータを更新して表示するまでに数分かかります。

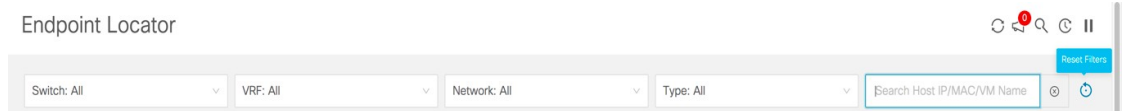
また、それぞれのドロップダウンリストを使用して、特定のスイッチ、VRF、ネットワーク、およびタイプのエンドポイントロケータの詳細をフィルタリングおよび表示することもできます。Cisco DCNM リリース 11.3(1)以降では、フィルタ属性としてエンドポイントのMACタイプを選択できます。Cisco DCNM リリース 11.4(1)以降、ネットワークの名前は、[ネットワーク (Network)]ドロップダウンリストにも表示されます。デフォルトでは、選択したオプションはこれらのフィールドで[すべて (All)]です。[ホストIP/MAC/VM名の検索 (Search Host IP/MAC/VM Name)]フィールドにホストIPアドレス、MACアドレス、または仮想マシンの名前を入力して、特定のデバイスのエンドポイントデータを表示することもできます。



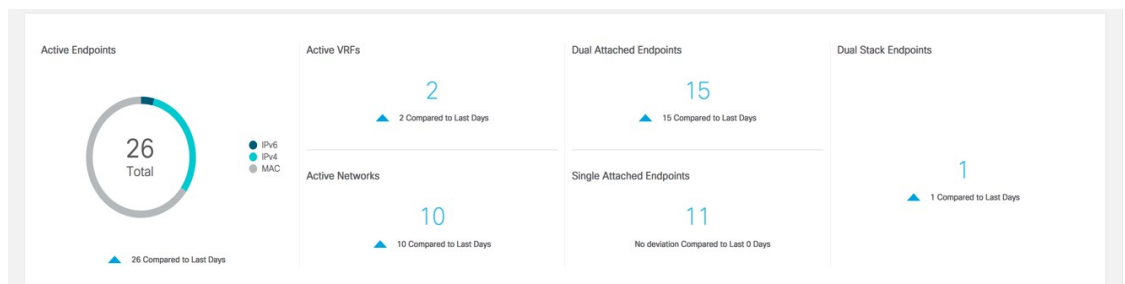
- (注) ドロップダウンリストから使用可能なオプションを使用するか、[**Host IP/MAC/VM Name Search (Search Host IP/MAC/VM Name)**] フィールドを使用して、検索を開始できます。ドロップダウンリストと検索フィールドの組み合わせを使用して検索を開始することはできません。



[**フィルタのリセット (Reset Filters)**] アイコンをクリックすると、フィルタをデフォルトのオプションにリセットできます。



ウィンドウの[上部 (Top)] ペインには、選択したスコープのアクティブエンドポイント、アクティブ VRF、アクティブ ネットワーク、デュアル接続エンドポイント、デュアル接続エンドポイントの数が表示されます。Cisco DCNM リリース 11.3(1) 以降、デュアル接続エンドポイント、シングル接続エンドポイント、デュアルスタック エンドポイントの数の表示のサポートが追加されました。デュアル接続エンドポイントは、少なくとも2つのスイッチの背後にあるエンドポイントです。デュアルスタックエンドポイントは、少なくとも1つの IPv4 アドレスと1つの IPv6 アドレスを持つエンドポイントです。

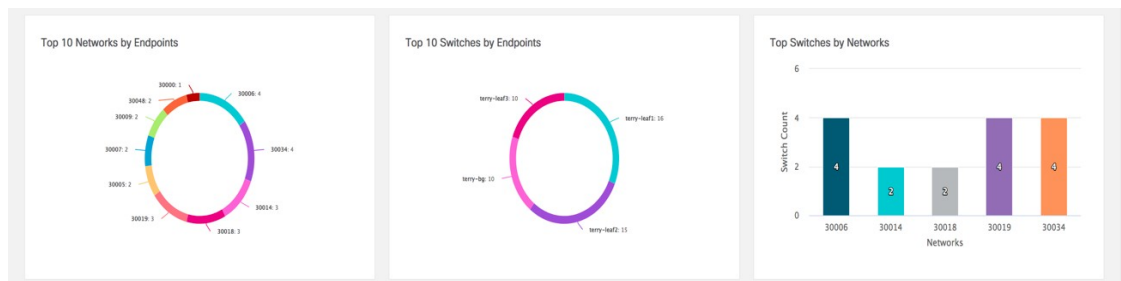


データの履歴分析が実行され、前の日に偏差が発生したかどうかを示す文が各タイトルの下部に表示されます。

[**エンドポイント履歴 (Endpoint History)**] ウィンドウに移動するには、EPL ダッシュボードの上部ペインで任意のタイトルをクリックします。

ウィンドウの「中央のペイン」には、次の情報が表示されます。

- **エンドポイント別の上位 10 個のネットワーク**：エンドポイントの数が最も多い上位 10 個のネットワークを示す円グラフが表示されます。円グラフにカーソルを合わせると、詳細情報が表示されます。必要なセクションをクリックして、IPv4、IPv6、および MAC アドレスの数を表示します。
- **エンドポイント別の上位 10 個のスイッチ**：最も多くのエンドポイントに接続されている上位 10 個のスイッチを示す円グラフが表示されます。円グラフにカーソルを合わせると、詳細情報が表示されます。必要なセクションをクリックして、IPv4、IPv6、および MAC アドレスの数を表示します。
- **ネットワーク別の上位スイッチ**：特定のネットワークに関連付けられているスイッチの数を示す棒グラフが表示されます。たとえば、スイッチの vPC ペアがネットワークに関連付けられている場合、ネットワークに関連付けられているスイッチの数は 2 です。



ウィンドウの「下部ペイン」には、アクティブなエンドポイントのリストが表示されます。

Time	VRF	Endpoint Identifier	MAC	Switch Name	Port	VLAN
04/06 09:03 PM	test_vrf	IPv4:192.168.36.55:30006	00:50:56:9d:4d:60	terry-bg	vPC Peer-Link	36
04/06 09:03 PM	test_vrf	IPv4:192.168.36.55:30006	00:50:56:9d:4d:60	terry-leaf3	Eth1/22	36
04/06 09:03 PM	test_vrf	IPv4:192.168.34.65:30034	00:50:56:9d:0e:a0	terry-leaf3	Eth1/22	34
04/06 09:03 PM	test_vrf	IPv4:192.168.34.65:30034	00:50:56:9d:0e:a0	terry-bg	vPC Peer-Link	34
04/06 09:02 PM		MAC:00:50:56:9d:0e:a0:30034	00:50:56:9d:0e:a0	terry-bg	vPC Peer-Link	34
04/06 09:02 PM		MAC:00:50:56:9d:0e:a0:30034	00:50:56:9d:0e:a0	terry-leaf3	Eth1/22	34
04/06 09:02 PM		MAC:00:50:56:9d:cb:df:30019	00:50:56:9d:cb:df	terry-bg	vPC Peer-Link	43
04/06 09:02 PM		MAC:00:50:56:9d:cb:df:30019	00:50:56:9d:cb:df	terry-leaf3	Eth1/22	43

特定のエンドポイントの詳細情報を表示するには、[+] をクリックします。仮想マシンが設定されている場合は、VM の名前が [ノード名 (Node Name)] フィールドに表示されます。VM の名前が EPL ダッシュボードに反映されるまでに最大 15 分かかることに注意してください。それまでは、EPL ダッシュボードの [ノード名 (Node Name)] フィールドに [データなし (No DATA)] と表示されます。

LIST OF ACTIVE ENDPOINTS

Time	VRF	Endpoint Identifier	MAC	Switch Name	Port	VLAN
06/11 09:39 AM	myvrf_50001	IPv6:2188:1:99:30001	00:50:56:be:71:e9	leg-fab2-bgw2	Po606	2344

L3_VNI: 50001
 Switch_Type: N9K
 Origin_IP: 40.4.0.1,0.0.0.0,0.0.0.0,0.0.0.0
 Switch_NextHop_IP: 40.3.0.2
 Operation: ACTIVE
 Seq_Num: 0
 Cluster: 40.3.0.2:0
 RouteDistinguisher: 40.2.0.1:35111
 Node Name: ppp-leg-fab2-188

[ホスト寿命 (Host Life)] アイコンをクリックして、そのエンドポイントの [エンドポイント寿命 (Endpoint Life)] ウィンドウを表示します。

LIST OF ACTIVE ENDPOINTS

Time	VRF	Endpoint Identifier	MAC	Switch Name	Port	VLAN
04/06 09:03 PM	test_vrf	IPv4:192.168.36.55:30006	00:50:56:9d:4d:60	terry-bg	vPC Peer-Link	36

L3_VNI: 52000
 Switch_Type: N9K
 Origin_IP: 10.2.0.5,0.0.0.0,0.0.0.0,0.0.0.0
 Switch_NextHop_IP: 10.3.0.4
 Operation: ACTIVE
 Seq_Num: 0
 Cluster: 10.3.0.4:0
 RouteDistinguisher: 12.2.0.1:32803
 Node Name: No DATA

Host Life

特定の IP アドレスを検索するには、[エンドポイント ID (Endpoint Identifier)] 列の検索アイコンをクリックします。

LIST OF ACTIVE ENDPOINTS


Time	VRF	Endpoint Identifier	MAC	Switch Name	Port	VLAN
04/06 09:03 PM	test_vrf	IPv4:192.168	00:50:56:9d:4d:60	terry-bg	vPC Peer-Link	36
04/06 09:03 PM	test_vrf	IPv4:192.168	00:50:56:9d:4d:60	terry-leaf3	Eth1/22	36
04/06 09:03 PM	test_vrf	IPv4:192.168	00:50:56:9d:0e:a0	terry-leaf3	Eth1/22	34
04/06 09:03 PM	test_vrf	IPv4:192.168.34.65:30034	00:50:56:9d:0e:a0	terry-bg	vPC Peer-Link	34
04/06 09:02 PM		MAC:00:50:56:9d:0e:a0:30034	00:50:56:9d:0e:a0	terry-bg	vPC Peer-Link	34
04/06 09:02 PM		MAC:00:50:56:9d:0e:a0:30034	00:50:56:9d:0e:a0	terry-leaf3	Eth1/22	34
04/06 09:02 PM		MAC:00:50:56:9d:cb:df:30019	00:50:56:9d:cb:df	terry-bg	vPC Peer-Link	43
04/06 09:02 PM		MAC:00:50:56:9d:cb:df:30019	00:50:56:9d:cb:df	terry-leaf3	Eth1/22	43

Search ip
Search Reset


特定のシナリオでは、データポイントデータベースが同期せず、エンドポイントの数などの情報が、次のようなネットワークの問題により正しく表示されないことがあります。

- エンドポイントが同じスイッチの下でポート間を移動し、ポート情報を更新するのに時間がかかる。
- 孤立したエンドポイントが 2 番目の VPC スイッチに接続され、孤立したエンドポイントではなくなりました。
- NX-API は最初は有効になっておらず、後で有効になります。

- NX-API は、最初は構成ミスが原因で失敗します。
- ルート リフレクタ (RR) の変更。
- スイッチの管理 IP が更新されます。

このような場合、[再同期 (Resync)]  アイコンをクリックすると、現在 RR にあるデータにダッシュボードが同期されます。ただし、履歴データは保持されます。これはコンピューティング集約型のアクティビティであるため、[再同期 (Resync)] を複数回クリックしないことを推奨します。




[通知 (Notifications)]  アイコンをクリックして、最新の通知のリストを表示します。



通知が生成された時刻、通知の説明、シビラティ (重大度)、ノードの名前などの情報が表示されます。

通知は、IP アドレスの重複、MAC 専用アドレスの重複、ファブリックからの VRF の消失、スイッチからのすべてのエンドポイントの消失、エンドポイントの移動、ファブリックのエンドポイントがゼロになる、エンドポイントがスイッチに接続されたとき、新しい VRF が検出されたとき、RR BGP 接続ステータスが変更されたときなどのイベントに対して生成されます。RR connected ステータスは、DCNM が BGP を介して RR に接続できることを示します (DCNM および RR は BGP ネイバーです)。RR 切断ステータスは、RR が切断され、基盤となる BGP が機能していないことを示します。ダウンロードアイコンをクリックすると、通知のリストを CSV ファイルの形式でダウンロードできます。

Cisco DCNM リリース 11.4(1) 以降、エンドポイント関連の異常がある場合は、アラームが生成されます。エンドポイントアラームの詳細については、「[エンドポイント ロケータ アラーム](#)」を参照してください。

[一時停止 (Pause)]  アイコンをクリックすると、ほぼリアルタイムでのデータの収集と表示が一時的に停止します。



EPL が最初に有効になり、[MAC-Only アドバタイズメントの処理 (Process MAC-Only Advertisements)] チェックボックスがオンになっているシナリオを考えます。次に、[MAC-Only アドバタイズメントの処理 (Process MAC-Only Advertisements)] チェックボックスを選択せずに、EPL を無効にしてから再度有効にします。ElasticSearch のキャッシュデータは EPL を無効にしても削除されないため、MAC エンドポイント情報は EPL ダッシュボードに表示されたままになります。ルートリフレクタが切断された場合も、同じ動作が見られます。規模に応じて、エンドポイントはしばらくしてから EPL ダッシュボードから削除されます。場合によっては、古い MAC 専用エンドポイントの削除に最大 30 分かかることがあります。ただし、最新のエンドポイント データを表示するには、EPL ダッシュボードの右上にある[再同期 (Resync)] アイコンをクリックします。

エンドポイント履歴

[エンドポイント履歴 (Endpoint History)] ウィンドウに移動するには、EPL ダッシュボードの上部ペインで任意のタイトルをクリックします。さまざまな時点でのアクティブエンドポイント、VRF およびネットワーク、デュアル接続エンドポイント、デュアルスタック MAC エンドポイントの数を示すグラフが表示されます。ここに表示されるグラフは、選択したファブリックに存在するエンドポイントだけでなく、すべてのエンドポイントを示します。エンドポイント履歴情報は、過去 180 日間の最大 100 GB のストレージ容量に使用できます。



特定のポイントでグラフにカーソルを合わせると、詳細情報が表示されます。グラフのポイントは 30 分間隔でプロットされます。各グラフの下部にある色分けされたポイントをクリックして、特定の要件のグラフを表示することもできます。たとえば、[アクティブ (IPv4) (active (IPv4))] のみが強調表示され、他のポイントが強調表示されないように、上記の[アクティブ エンドポイント (Active Endpoints)] ウィンドウで[アクティブ (IPv4) (active (IPv4))]]

以外のすべての色分けされたポイントをクリックします。このようなシナリオでは、アクティブな IPv4 エンドポイントのみがグラフに表示されます。また、グラフの下部にある色分けされたポイントにカーソルを合わせると、特定の要件のグラフが表示されます。たとえば、**[アクティブ (IPv4) (active (IPv4))]** にカーソルを合わせると、アクティブな IPv4 エンドポイントのみがグラフに表示されます。

グラフ内の任意のポイントをクリックすると、その時点に関する詳細情報を示すウィンドウが表示されます。たとえば、**[アクティブ エンドポイント (Active Endpoints)]** グラフで特定のポイントをクリックすると、**[エンドポイント (Endpoints)]** ウィンドウが表示されます。このウィンドウには、エンドポイントに関する情報とともに、エンドポイントに関連付けられているスイッチおよび VRF の名前が表示されます。**[エンドポイント (Endpoints)]** ウィンドウの右上にあるダウンロードアイコンをクリックして、データを CSV ファイルとしてダウンロードします。

Endpoints ↓ ×

Endpoint	Switch Name	VRF
IPv4:192.168.36.20:30006	terry-leaf3	test_vrf
IPv4:192.168.200.2:32000	terry-leaf3	test_vrf
IPv4:192.168.36.29:30006	terry-leaf2	test_vrf
IPv4:192.60.0.100:30004	terry-leaf1	myvrf_50000
IPv4:192.168.80.90:30080	terry-leaf1	test_vrf
IPv4:192.168.180.100:30008	terry-leaf3	myvrf_50009
IPv4:192.168.48.2:30048	terry-leaf2	test_vrf
IPv4:192.168.39.2:30043	terry-leaf2	test_vrf
IPv4:192.60.7.208:30004	terry-leaf3	myvrf_50000
IPv4:192.60.10.168:30004	terry-leaf3	myvrf_50000

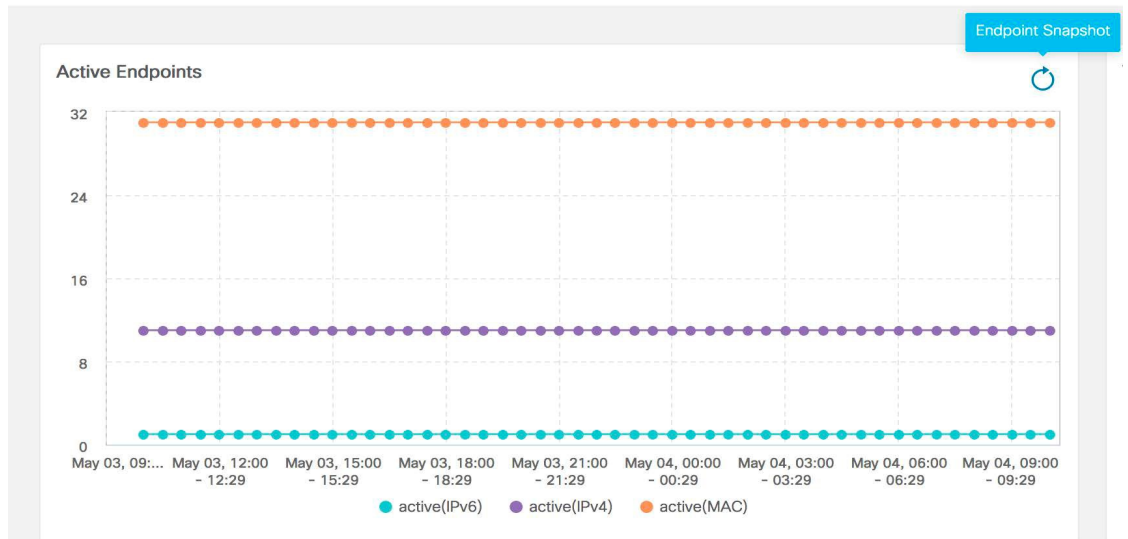
< 1 2 3 4 5 ... 303 >

エンドポイント スナップショット

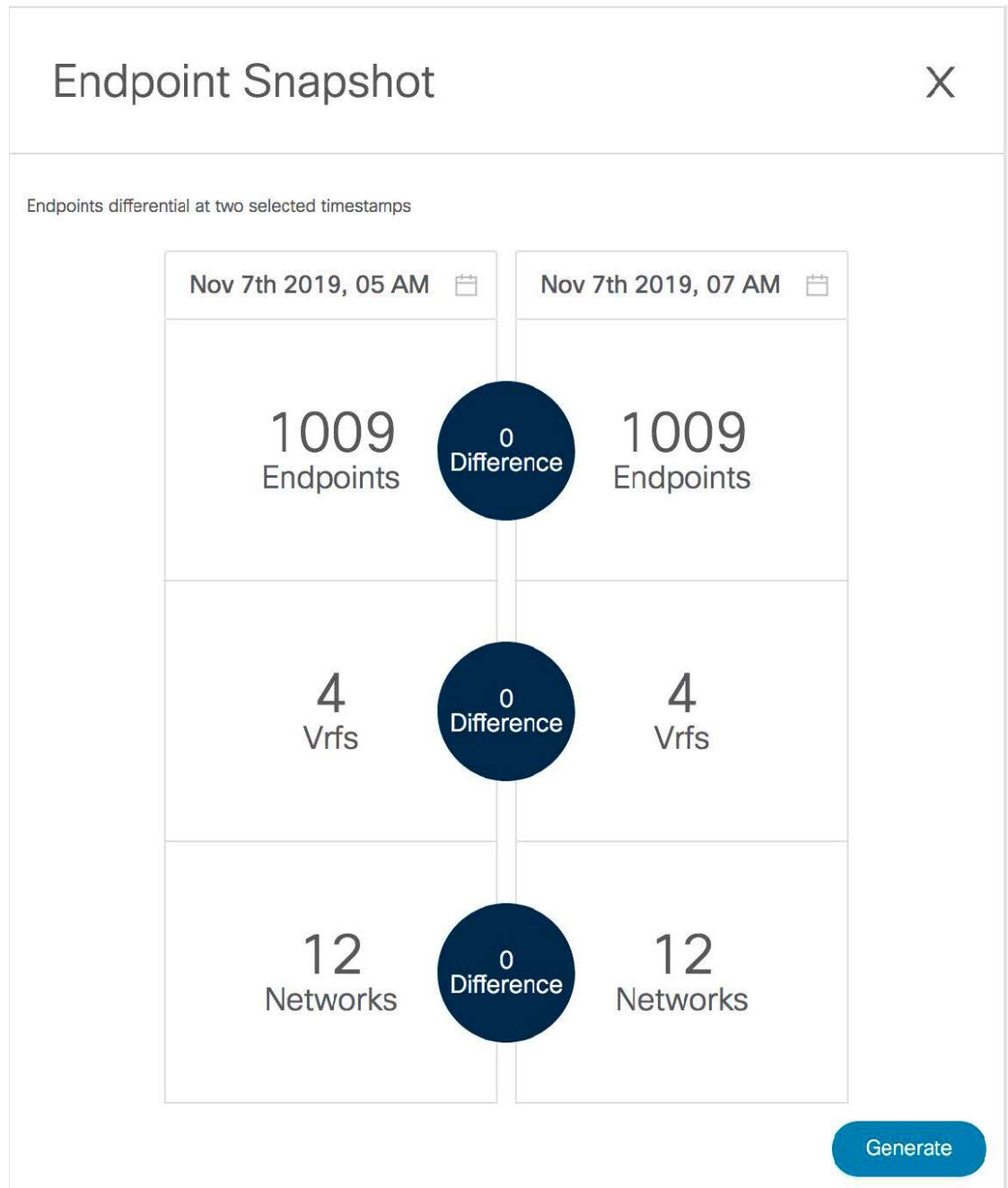
Cisco DCNM リリース 11.3(1) から、特定の 2 つの時点でエンドポイント データを比較できます。**[エンドポイント スナップショット (Endpoint Snapshot)]** ウィンドウを表示するには、**[エンドポイント履歴 (Endpoint History)]** ウィンドウの**[アクティブなエンドポイント (Active Endpoints)]** グラフの右上にある**[エンドポイント スナップショット (Endpoint Snapshot)]** アイコンをクリックします。

Endpoint History

May 03 . 2020 - May 04 . 2020 ▾



デフォルトでは、過去1時間のエンドポイントスナップショット比較データが表示されます。



特定の時点のエンドポイント スナップショットを比較するには、2つの時点（T1 と T2）を選択し、[生成（Generate）] をクリックします。

Endpoint Snapshot



Endpoints differential at two selected timestamps

Nov 7th 2019, 04 AM |
2019, 19 PM 📅

<< <
Nov 2019
> >>

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

Now
select time

Ok

12
Networks

Difference

12
Networks

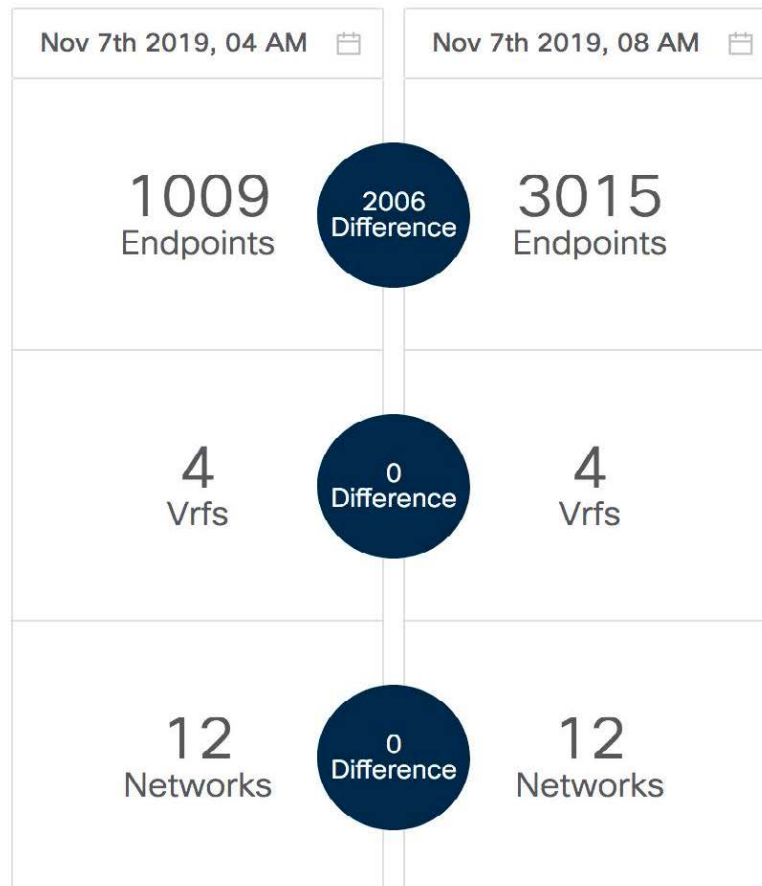
Generate

選択した時点のエンドポイント、VRF、およびネットワークの比較が表示されます。エンドポイント、VRF、またはネットワークに関する詳細情報をダウンロードするには、各タイトルをクリックします。**[相違 (Difference)]** アイコンをクリックして、指定した時間間隔のデータの相違に関する詳細をダウンロードします。スナップショットは最大3か月間保存され、その後破棄されます。

Endpoint Snapshot



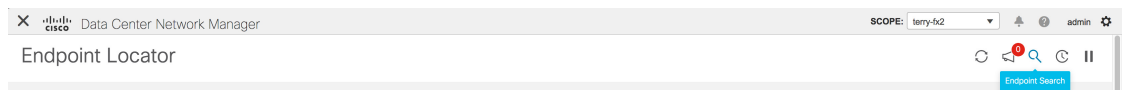
Endpoints differential at two selected timestamps



Generate

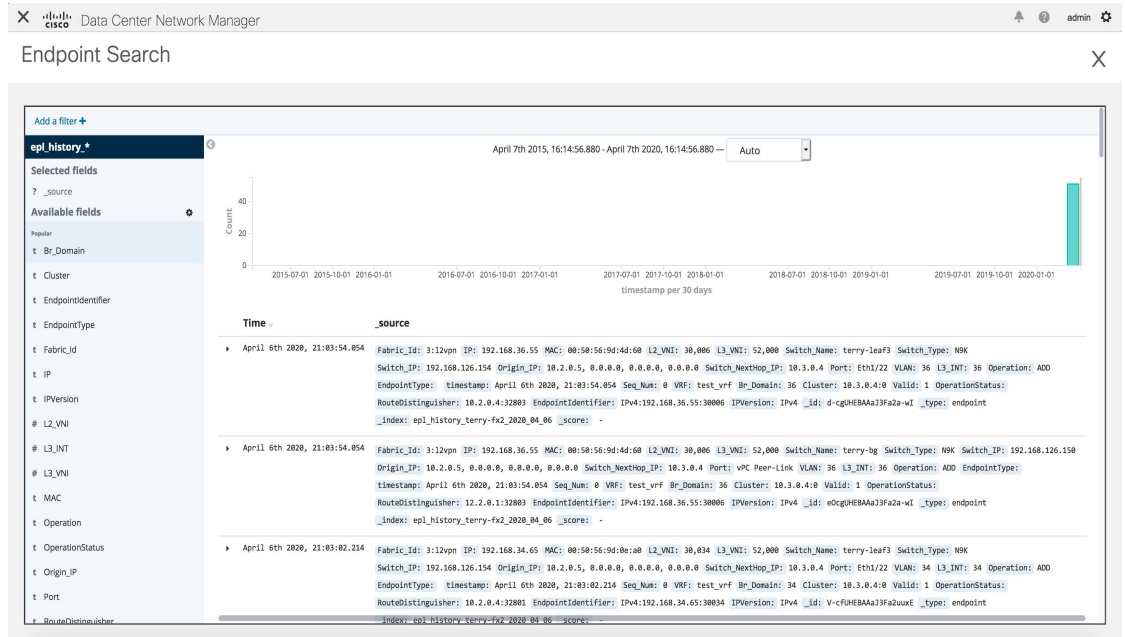
エンドポイント検索

エンドポイントロケータランディングページの右上にある[エンドポイント検索 (Endpoint Search)]アイコンをクリックして、日付範囲で指定された期間のエンドポイントイベントを表示するリアルタイムプロットを表示します。



ここに表示される結果は、左側のメニューにある[選択済みフィールド (Selected fields)]の下に表示されるフィールドによって異なります。[使用可能なフィールド (Available fields)]の

下にあるフィールドを[選択済みフィールド (Selected fields)]に追加して、必須フィールドを使用して検索を開始できます。



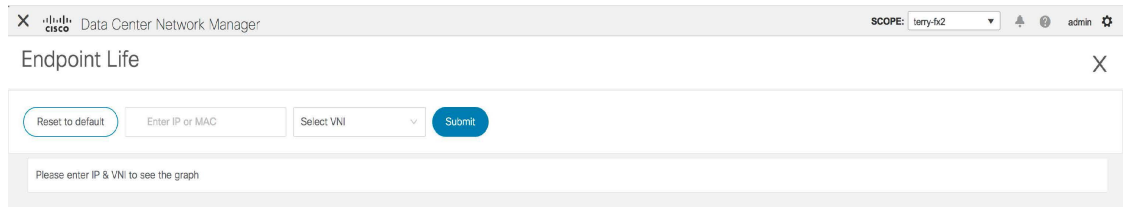
エンドポイントの寿命

[エンドポイントロケータ (Endpoint Locator)]ランディングページの右上にある[エンドポイント寿命 (Endpoint Life)]アイコンをクリックして、ファブリック内に存在する特定のエンドポイントのタイムラインを表示します。

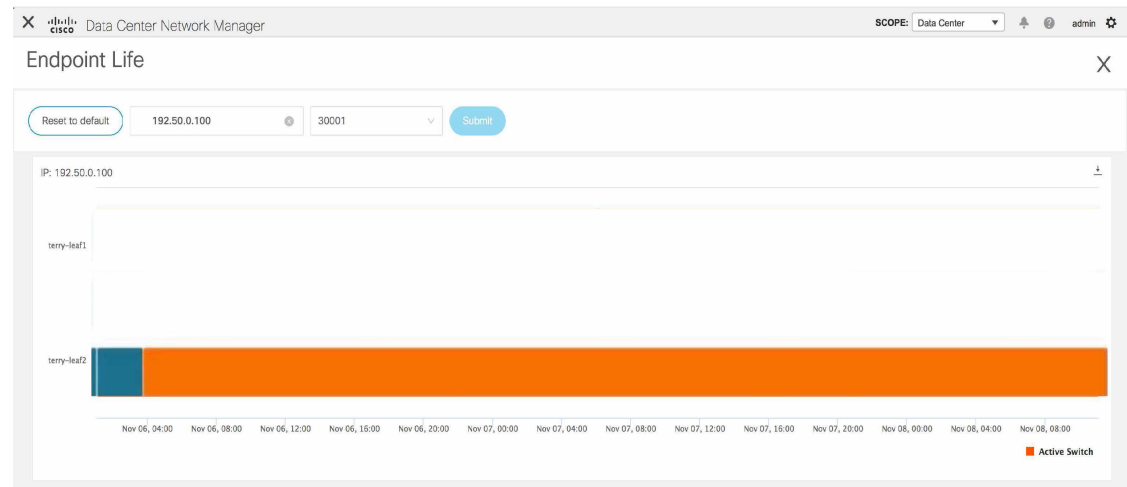


エンドポイントのIPまたはMACアドレスとVXLANネットワーク識別子(VNI)を指定して、エンドポイントが存在していたスイッチのリストを、関連する開始日と終了日を含めて表示します。[送信 (Submit)]をクリックします。

IPv4またはIPv6アドレスを使用して検索を開始し、IPv4/IPv6エンドポイントのエンドポイント寿命グラフを表示します。MACアドレスを使用して検索を開始し、MAC専用エンドポイントのエンドポイント寿命グラフを表示します。



表示されるウィンドウは、基本的には特定のエンドポイントのエンドポイントの寿命です。オレンジ色のバーは、そのスイッチのアクティブエンドポイントを表します。エンドポイントがネットワークによってアクティブと見なされる場合、エンドポイントには帯域があります。エンドポイントがデュアルホーム接続されている場合は、エンドポイントの存在を報告する2つの水平バンドがあり、各スイッチ（通常はスイッチのvPCペア）に1つのバンドがあります。エンドポイントが削除または移動された場合は、このウィンドウでエンドポイントの削除と移動の履歴を確認することもできます。



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。