Cisco APIC と NetFlow

改訂：2024 年 4 月 22 日

新機能および変更された機能に関する情報

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

表 *1*：新機能と変更された動作

Cisco APIC リリース	特長	説明
5.2(8)	NetFlow スケール	NetFlow の規模が増加した。詳細については、NetFlow スケール （5 ページ）を参照してください。
5.1(1)	NetFlow エクスポータ ポリシー	インバンド管理テナントからのレイヤ 3 EPG を NetFlow エクスポータに関連付けることができるようになりました。
4.0(1)	リモート リーフ スイッチ	NetFlow がリモート リーフ スイッチでサポートされるようになりました。
2.3(1)	FX プラットフォーム スイッチ	NetFlow が FXplatform スイッチでサポートされるようになりました。
2.2(1)	Cisco APIC および NetFlow をサポートします。	このガイドは最初にリリースされました。

NetFlow について

NetFlow テクノロジは、ネットワーク トラフィック アカウンティング、従量制のネットワーク課金、ネットワーク プランニング、そしてサービス拒絶に対する監視機能、ネットワーク監視、社外マーケティング、およびサービス プロバイダと企業顧客向け両方のデータ マイニングなど、主要な一連のアプリケーションの計測基盤を効果的にします。Cisco は NetFlow エクスポート データの収集、データ量削減、ポスト プロセッシングを行う一連の NetFlow アプリケーションを提供し、エンド ユーザー アプリケーションが NetFlow データへ簡単にアクセスできるようにします。この機能により、同じレベルを介したトラフィックのモニタリングを実行する、NetFlow がデータ センターを通過するトラフィックのモニタリングを有効にすると、 Cisco Application Centric Infrastructure (Cisco ACI) ファブリック。

ハードウェアがレコードからコレクタに直接エクスポートする代わりに、レコードはスーパーバイザ エンジンで処理され、必要な形式で標準の NetFlow コレクタにエクスポートされます。

仮想マシン ネットワークでの NetFlow の構成については、『*Cisco ACI Virtualization Guide*』 を参照してください。

NetFlow モニタ ポリシー

NetFlow ポリシーは、インターフェイスごとに展開できます。モニタするトラフィック タイプまたはアドレス ファミリ（IPv4、IPv6、またはレイヤ 2）に応じて、異なる NetFlow モニタ ポリシーを有効にできます。モニタ ポリシー（netflowMonitorPol）は、レコード ポリシーとエクスポータ ポリシーの間の関係を保管するコンテナとしての役割を果たします。モニタ ポリシーは受信 IP パケットのパケット フローを識別して、これらのパケット フローに基づく統計情報を提供します。NetFlow のためにパケットやネットワーキング デバイスを変更する必要はありません。

このポリシーは、物理インターフェイスに展開するため、またはテナントをブリッジドメインと L3Outs に適用するために、ファブリックで構成できます。

NetFlowは、ファブリック全体またはファブリックの一部に展開して、さまざまなインターフェイス タイプのパケット統計情報をモニターできます。

NetFlow 統計情報は、ポリシーが適用される前に入力パケットで収集されます。NetFlow 統計情報は、パケットがポリシー（コントラクト）で許可されていない場合でも記録されます。

NetFlow レコード ポリシー

レコード ポリシー（netflowRecordPol）を使用すると、フローと、各フローについて収集する統計情報を定義できます。これは、フロー内のパケットを識別するために NetFlow で使用するキーとともに、NetFlow がフローについて収集する関連フィールドを定義することで達成できます。キーと関連フィールドを任意の組み合わせで指定して、フローレコードを定義できます。フロー レコードは、フローごとに収集されるカウンタのタイプも定義します。また、32 ビットまたは 64 ビットのパケット カウンタまたはバイト カウンタを構成できます。

レコード ポリシーには、次のプロパティがあります：

- RecordPol.match：次の値の組み合わせである match プロパティを使用してフローを定義できます。
  - src-ipv4、dst-ipv4、src-port、dst-port、proto、vlan、tos
  - src-ipv6、dst-ipv6、src-port、dst-port、proto, vlan、tos
  - ethertype、src-mac、dst-mac、vlan
  - src-ip、dst-ip、src-port、dst-port、proto、vlan、tos

  （注） src-ip および dst-ip パラメータは、IPv4 と IPv6 の両方を修飾します。

- RecordPol.collect：収集プロパティを使用して、特定のフローについて収集する情報を指定できます。

NetFlow エクスポータ ポリシー

エクスポータポリシー（ netflowExporterPol ）は、フロー用に収集されたデータの送信先を指定します。NetFlow コレクタは、外部、標準のNetFlowプロトコルをサポートし、パケットを受け入れているエンティティが付いているNetFlowヘッダーが無効です。

エクスポータ ポリシーには、次のプロパティがあります。

- **[宛先 IP アドレス（Destination IP Address）]**：この必須プロパティは、NetFlow フローパケットを受信する NetFlow エクスポータの IPv4 または IPv6 アドレスを指定します。このホストのフォーマットである必要があります (つまり、「/32」または「/128」)。
- **[宛て先ポート（Destination Port）]**：Tこの必須プロパティは着信接続を受け入れるエクスポータを有効に エクスポータ アプリケーションでリッスンするポートを指定します。
- **[送信元IPアドレスタイプ（Source IP Address Type）]**：このプロパティは、スイッチから送信される NetFlow レコードパケットの送信元 IP アドレスを入力します。送信元 IP アドレスは、次のいずれかの構成オプションに基づいて NetFlow パケットに入力されます。このアドレスで構成されるスイッチ インターフェイスはありません。
  - **[カスタム送信元IP（Custom Src IP）]**：送信元 IP アドレスタイプが **[カスタム送信元 IP（Custom Src IP）]** の場合、このプロパティはタグと同様に使用され、ファブリック内のさまざまなセクションまたはノードからフローを区別します。アドレスは、少なくとも 12 のホスト ビットを持つプレフィックスになります。つまり、マスクは、IPv4 の場合は 20 以下、IPv6 の場合は 116 以下である必要があります。スイッチは、構成されたプレフィックスとホスト ビットを使用して、NetFlow パケットに送信元 IP アドレスを入力します。ホスト部分は、パケットを送信するリーフのノード識別子と等しくなります。
  - **[インバンド管理IP（Inband Management IP）]**：NetFlow パケットの送信元 IP アドレスは、設定されたスイッチのインバンド管理 IP アドレスになります。
  - **[アウトオブバンド管理 IP（OutOfband Management IP）]**：NetFlow パケットの送信元 IP アドレスは、構成されたスイッチのアウトオブバンド管理 IP アドレスになります。
  - **[PTEP アドレス（PTEP address）]**：NetFlow パケットの送信元 IP アドレスは、リーフ スイッチの物理 TEP（トンネル エンドポイント）アドレスになります。

（注） 「show flow exporter」リーフ スイッチ CLI コマンドを使用して、そのスイッチによって送信された NetFlow レコードの送信元 IP アドレスを表示できます。

- **[バージョン（Version）]**：このプロパティは、エクスポータがパケットを理解するための NetFlow バージョンを指定するために使用されます。サポートされている値は v9 のみです。
- **[EPG タイプ（EPG Type）]**：App EPG またはレイヤ 3 EPG

NetFlow エクスポータは、EPG を介してファブリックに直接接続されている NetFlow コレクタ、または L3Oout を介して到達可能なリモート コレクタにデータを送信できます。必要に応じて EPG タイプを選択し、関連するテナント/EPG を入力します。

スイッチは、選択した EPG またはレイヤ 3 EPG に関連付けられている VRF インスタンスから NetFlow パケットを送信します。EPG またはレイヤ EPG に関連付けられている VRF インスタンスは、NetFlow モニターが構成されているすべてのリーフ スイッチに存在する必要があります。

5.1（1）リリース以降、管理テナントのインバンド VRF インスタンスからの EPG または L3Out を NetFlow エクスポータに関連付けることができます。

NetFlow ノード ポリシーについて

ノードポリシー（netflowNodePol）は、フロー レコードが外部エクスポータに送信されるレートを指定する NetFlow タイマーを展開します。タイマーは次のとおりです：

- 収集間隔（Collection interval）：リーフ スイッチがコレクタに NetFlow パケットを送信するまでの時間間隔。デフォルト値は 1 分です。
- テンプレート間隔（Template interval）：リーフ スイッチがレコード テンプレートをコレクタに送信するまでの時間間隔。このテンプレートは、コレクタに送信されるレコードのフォーマットを指定します。デフォルト値は5分です。

NetFlow スケール

Cisco Application Policy Infrastructure Controller（APIC）5.2（7）以前のリリースでは、設定可能な NetFlow オプションのスケール番号の一部は次のとおりです。

表 *2 : Cisco APIC5.2（7）以前のリリースでの NetFlow スケール*

設定可能なオプション	拡張性
収集間隔ごとのレコード数	20,000[1]
リーフ スイッチごとのブリッジ ドメインの NetFlow モニター ポリシー	100

[1] NetFlow は 1 分あたりにはるかに多くのフロー レコードを収集できますが、20,000 フローのみが適格です。

Cisco APIC5.2（8）リリース以降、これらの構成可能な NetFlow オプションのスケール番号は次のとおりです：

表 *3 : Cisco APIC5.2（8）リリース以降の NetFlow スケール*

設定可能なオプション	拡張性
収集間隔ごとのレコード数	1,000,000
リーフ スイッチごとのブリッジ ドメインの NetFlow モニター ポリシー	350

より多くのフローがある電話会社や企業のデータ センターでの遵守とモニタリングのユース ケースに対応して、NetFlow の規模を拡大しました。また、アプリケーションのコンテナ化もあり、単一のアプライアンスまたは少数の仮想マシンとは対照的に、1 つのアプリケーションが数百のコンテナによって提供されます。多数のコンテナにより、多数のフローがデータ センターに送られます。

NetFlow スケール詳細については、お使いのCisco APICリリースの「検証されたスケーラビリティ ガイド」を参照してください。

https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html#Verified_Scalability_Guides

NetFlow 展開に関する考慮事項

次の NetFlow 展開考慮事項に注意します：

- 次のように、NetFlow ノードポリシーの MTU を 9000 に変更します。

  1. メニュー バーで、**[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）]** に移動します。
  2. [ナビゲーション（Navigation）] ペインで、**[ポリシー（Policies）] > [スイッチ（Switch）] > [NetFlow ノード（NetFlow Node）] > [デフォルト（default）]**に移動します。
  3. [Work] ペインで、MTU プロパティを 9000 に設定します。

  この値により、より多くのフロー レコードが単一のパケットにエクスポートされるため、レコードが NetFlow コレクタにエクスポートされるときの CPU 使用率が低下します。これは、NetFlow を大規模に展開する場合に特に重要です。たとえば、100 万のフローレコードで、NetFlow MTU が 1500 に設定されている場合、（外部コレクタへのエクスポート中）各収集間隔で数秒間、CPU 使用率が 100% に急増する可能性があります。対照的に、NetFlow MTU を 9000 に設定した後、これらの CPU 使用率のスパイクは 80% 未満にとどまり、期間は短縮されます。

- NetFlow は、ハッシュに基づいてハードウェア テーブル内のフローをキャプチャし、これらのフローをハードウェア テーブルからスイッチの CPU に組み込まれたソフトウェア キャッシュに定期的にエクスポートします。NetFlow はハッシュに基づいてフロー レコードをキャプチャするため、フローの衝突が発生し、フロー テーブルにスペースがある場合でも NetFlow がフローをキャプチャできない可能性があります。このため、NetFlow はすべてのフローをキャプチャしない場合があります。

- ハードウェア テーブルのキャパシティは、ソフトウェア キャッシュの一部です。その理由は次のとおりです。

  - 一部のフローは、ハードウェア テーブルでのハッシュの衝突が原因で見落とされるだけでなく、ハードウェア テーブルからソフトウェア キャッシュへの各更新に重複するフローが含まれている可能性があります（フローはソフトウェア キャッシュにすでに存在します）。
  - フロー レコードで伝送されるフロー期間の粒度は、フローの総数が増加するにつれて低下します。

- スイッチの CPU のソフトウェア キャッシュには、最大 100 万の IPv6 または IPv4 フロー レコードを保持できます。ただし、ハードウェア テーブルでは、IPv6 フロー レコードには IPv4 フロー レコードの 2 倍のスペースが必要です。

NetFlow に関するサポートおよび制限事項

次のリストは、NetFlow で利用可能なサポートとそのサポートの制限に関する情報を提供します。

- EX、FX、FX2 以降のスイッチは NetFlow をサポートしています。特定のリリースでサポートされるスイッチ モデルの完全なリストについては、そのリリースの「*Cisco Nexus 9000 ACI* モード スイッチ リリース ノート」を参照してください。

- Cisco Application Policy Infrastructure Controller（APIC）リリース 4.0(1) 以降では、リモート リーフスイッチの NetFlow はサポート対象です。

- Cisco Application Centric Infrastructure（ACI）は NetFlow の入力のみをサポートし、NetFlow の出力はサポート対象外です。ブリッジドメインでは、NetFlow はスパイン スイッチから入ってくるパケットを確実にキャプチャできません。
- スパイン スイッチは NetFlow をサポートしていないため、スパイン スイッチのパケットからテナント レベルの情報をローカルに取得することはできません。
- ハードウェアは、アクティブ/非アクティブ タイマーをサポートしていません。フローテーブル レコードはテーブルがフラッシュされると集約され、レコードは毎分エクスポートされます。
- すべてのエクスポート間隔で、ソフトウェア キャッシュがフラッシュされ、フローが長期間有効であっても、次の間隔でエクスポートされるレコードには、リセットされたパケット/バイト カウントおよびその他の統計が含まれます。
- フィルタ TCAM には、ブリッジドメインまたはインターフェイスのラベルがありません。NetFlow モニターを 2 つのブリッジドメインに追加すると、NetFlow モニターは IPv4 の場合は 2 つのルール、IPv6 の場合は 8 つのルールを使用します。そのため、スケールは 1K フィルタ TCAM で制限されます。
- ARP/ND は IP パケットとして処理され、それらのターゲット プロトコル アドレスは、プロトコル範囲として 249 から 255 までのいくつかの特別なプロトコル番号とともに IP フィールドに配置されます。NetFlow コレクタは、この処理を理解していない可能性があります。
- ICMP チェックサムはフロー レコードのレイヤ 4 src ポートの一部であるため、ICMP レコードの場合、他の非 TCP/UDP パケットと同様に、これがマスクされていないと多くのフロー エントリが作成されます。
- Cisco ACI-mode スイッチは、2 つのアクティブなエクスポータのみをサポートします。
- スイッチが CPU 生成パケットの VRF インスタンス間ルーティングを実行できないため、リーフスイッチからの NetFlow トラフィックがコレクタに到達できないことがあります。回避策として、NetFlow コレクタに使用される L3Out と同じ VRF インスタンスですでに構成されている EPG の偽の静的パスを作成します。偽のパスにより、トラフィックはコレクタに到達できます。
- 混合モードで、NetFlow とフロー テレメトリの両方を同時に有効にすると、NetFlow CE はサポートされません。NetFlow とフロー テレメトリの両方で、IPv4 および IPv6 トラフィックのみがサポートされます。
- 混合モードで NetFlow エクスポータ ポリシーを構成する場合、特定の VRF インスタンスのサブネットを構成できます。フロー テレメトリは、EPG に関連付けられているすべてのテナントを追跡します。サブネットごとに個別のポリシーを構成する必要はありません。

  たとえば、**`t1:ctx2`** VRF インスタンスのサブネットとして **`0.0.0.0/0`** を指定すると、フロー テレメトリは、関連付けられている VRF インスタンスに関係なく、すべての IPv4 フローを追跡します。
- NetFlow エクスポータ エンドポイントがブリッジ ドメインの背後にある場合は、ブリッジ ドメインのユニキャスト ルーティング ノブを有効にして、ブリッジ ドメイン サブネットの URIB ルートをインストールする必要があります。ノブが無効になっている場合、パケットはコレクタに転送されず、コレクタ ポリシーに対して operSt が無効になります。

EX プラットフォーム スイッチの NetFlow

EX プラットフォーム スイッチには、一般的なサポート情報に加えて、次の制限事項が適用されます。

- NetFlow はブリッジ ドメインでサポートできます。ただし、NetFlow はブリッジド パケットとルーテッド パケットを区別できません。ルーテッドパケットのみをキャプチャするようにインターフェイスVLAN（SVI）でNetFlowを構成した場合、NetFlow は EX スイッチで収集をこのタイプに制限できません。
- EX スイッチは、フロー レコードでカプセル化 VLAN を提供できません。
- EX スイッチには MAC アドレス パケット分類機能がないため、構成エンジンのフロー レコードには非 IP アドレス フローのみが含まれます（ARP はすでに IP として扱われます）。
- EX スイッチは、パケットベースのサンプリング（N 中の M）など、定期的に展開され理解されている NetFlow サンプリングをサポートしていません。
- フロー ハッシュの一部としてタイプ オブ サービスまたは送信元インターフェイスを使用することはサポートされていません。送信元インターフェイス情報はレコードで収集されますが、EX スイッチではタイプオブサービス情報は収集されません。
- EX スイッチには、固定のフロー収集パラメータがあります。
- EX スイッチは、各タイプの 2 つのフロー レコードのみをサポートします。例外として、4 つの構成エンジン フロー レコードがサポートされています。
- EX スイッチは、ARP および ND パケットを識別するために次のプロトコル番号を割り当てます。
  - ARP Req 249
  - ARP Res 250
  - RARP Req 247
  - RARP Res 248
  - Nd Sol 249
  - Nd Adv 250

  他のすべての ARP および ND パケットは 255 に設定されます。

NetFlow にサポートされているインターフェイス

NetFlowでは、次のインターフェイスがサポートされています：

- 物理イーサネット（レイヤ 2 およびレイヤ 3）
- ポート チャネル（PC）
- 仮想ポート チャネル（vPC）
- ファブリック エクステンダ（FEX）、FEX PC、および FEX VPC
- レイヤ 3 サブインターフェイス
- SVI
- ブリッジドメイン

他のインターフェイス ポリシーとは異なり、NetFlowポリシーはデフォルトではインターフェイスに適用されません。NetFlow は、特定のインターフェイスで明示的に有効にする必要があります。

インターフェイスごとに、NetFlowモニタリングを有効にするときに、アドレス ファミリ（またはフィルタ）を指定する必要があります。アドレス ファミリは、次のいずれかのタイプになります：

- IPv4
- IPv6
- CE（クラシカル イーサネット/Layer 2）

アドレス ファミリを使用すると、ハードウェアは、指定されたアドレス ファミリに基づいてのみパケットをモニターします。同じインターフェイス上のアドレス ファミリごとに異なるモニタリング ポリシーを有効にできます。

NetFlow および Cisco Tetration Analytics の優先順位

Cisco Application Centric Infrastructure (Cisco ACI) ハードウェアに関する限り、NetFlow と Cisco Tetration Analytics は同じ ASIC 構成要素を使用してデータを収集します。両方の機能を同時にイネーブルにできません。関連するポリシーを構成して展開する前に、NetFlow または Tetration Analytics を明示的に有効にする必要があります。デフォルトは、Tetration Analyticsです。

Cisco APIC が Cisco Tetration Analytics と NetFlow の両方の構成を特定のノードにプッシュする場合、選択されたプライオリティ フラグによって、どちらの機能を優先する必要があるかがスイッチに警告されます。他の機能の構成は無視されます。

GUI を使用したファブリック レベルでの NetFlow の構成

GUI を使用したファブリック NetFlow モニター ポリシーの構成

次の手順では、Cisco APICGUI を使用してファブリック NetFlow モニター ポリシーを構成します。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **[展開（ナビゲーション）]** ペインで **[ポリシー（Policies）] > [インターフェイス（Interface）] > NetFlow > [NetFlow モニター（NetFlow Monitors）]** を選択します。

（注） 以前のリリースでは、NetFlowモニターポリシー設定は、代わりに**[インターフェイス ポリシー（Interface Policies）] > [ポリシー（Policies）] > [分析（Analytics）] > [NetFlow モニター（NetFlow Monitors）]** の下にある場合があります。

ステップ 3 **[NetFlow モニター（NetFlow Monitors）]** を右クリックし、**[NetFlow モニターの作成（Create NetFlow Monitor）]** を選択します。

ステップ 4 **[NetFlow モニターを作成（Create NetFlow Monitor）]** ダイアログボックスで、必要に応じてフィールドに入力します。

フロー レコードとエクスポータを新規作成するか、既存のフロー レコードとエクスポータを追加できます。

[関連付けられたフローレコード（Associated Flow Record）]の作成については、GUI を使用したファブリック NetFlow レコード ポリシーの構成 （10 ページ）を参照してください。

[関連付けられたフロー エクスポータ（Associated Flow Exporters）]の作成については、GUI を使用したファブリック NetFlow エクスポータ ポリシーの構成 （11 ページ）を参照してください。

最大 2 つのフロー エクスポータをモニター ポリシーに関連付けることができます。

GUI を使用したファブリック NetFlow レコード ポリシーの構成

次の手順では、Cisco APIC GUI を使用して ファブリック NetFlow レコード ポリシーを構成します。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **[展開（ナビゲーション）]** ペインで **[ポリシー（Policies）]** > **[インターフェイス（Interface）]** > **NetFlow** > **[NetFlow レコード（NetFlow Records）]** を選択します。

（注） 以前のリリースでは、NetFlow レコード ポリシー設定は、代わりに **[インターフェイス ポリシー（Interface Policies）]** > **[ポリシー（Policies）]** > **[分析（Analytics）]** > **[NetFlow レコード（NetFlow Records）]** の下にある場合があります。

ステップ 3 **[NetFlow レコード（NetFlow Records）]** を右クリックし、**[NetFlow レコードの作成（Create NetFlow Record）]** を選択します。

ステップ 4 [Netflow レコードを作成（Create NetFlow Record）] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) **[パラメータを作成（Collect Parameters）]** ドロップダウン リストでは、複数のパラメータを選択できます。

b) **[パラメータを一致（Match Parameters）]** ドロップダウン リストでは、複数のパラメータを選択できます。

複数のパラメータを選択する場合は、次のいずれかの組み合わせまたはいずれかの組み合わせのサブセットを選択する必要があります。

- 送信元 IPv4、接続先 IPv4、送信元 ポート、宛て先ポート、IP プロトコル、VLAN、IP TOS
- 送信元 IPv4、接続先 IPv4、送信元 ポート、宛て先ポート、IP プロトコル、VLAN、IP TOS
- Ethertype、送信元 MAC、接続先 MAC、VLAN
- 送信元 IP、接続先 IP、送信元ポート、宛て先ポート、IP プロトコル、VLAN、IP TOS。送信元 IP/接続先 IP は、IPv4 と IPv6 の両方を修飾します。

GUI を使用したファブリック NetFlow エクスポータ ポリシーの構成

次の手順では、Cisco APIC GUI を使用して ファブリック NetFlow エクスポータ ポリシーを構成します。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **[展開（ナビゲーション）]** ペインで **[ポリシー（Policies）] > [インターフェイス（Interface）] > NetFlow > [NetFlow エクスポータ（NetFlow Exporters）]** を選択します。

（注） 以前のリリースでは、NetFlowモニターポリシー設定は、代わりに**[インターフェイス ポリシー（Interface Policies）] > [ポリシー（Policies）] > [分析（Analytics）] > [NetFlow エクスポータ（NetFlow Exporters）]** の下にある場合があります。

ステップ 3 **[NetFlow エクスポータ（NetFlow Exporters）]** を右クリックし、**[外部コレクタ到達可能性を作成（Create External Collector Reachability]** を選択します。

ステップ 4 **[外部コレクタ到達可能性を作成（Create External Collector Reachability]** ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します：

a) **[NetFlow エクスポータ バージョン フォーマット（NetFlow Exporters Version Format）]** ボタンでは、**バージョン 9** が唯一の有効な選択肢です。他のボタンのいずれかをクリックしても、バージョンはデフォルトで 9 に設定されます。

b) **[EPG タイプ（EPG Type）]** チェックボックスについては、チェックボックスをオフのままにするか、1つのボックスをオンにすることができます。複数のボックスにチェックをオンにすることはできません。

Cisco APIC GUI を使用したセレクタによる NetFlow モニター ポリシーの展開

次の手順では、Cisco APIC GUI を使用してセレクタを介して NetFlow モニター ポリシーを展開します。

手順

ステップ 1 メニュー バーで、**[Fabric] > [Access Policies]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[インターフェイス（Interfaces）] > [リーフ インターフェイス（Leaf Interfaces）] > [ポリシー グループ（Policy Groups）]** を選択します。

以前のリリースでは、構成は **[インターフェイス ポリシー > ポリシー グループ（Interface Policies Policy Groups）] > [リーフ ポリシー グループ（Leaf Policy Groups）]** の下にある場合があります。

ステップ 3 新しいリーフ ポリシー グループを作成するときに NetFlow モニター ポリシーを展開できます。または、既存のリーフ ポリシー グループに NetFlow モニター ポリシーを展開できます。

新しいリーフ ポリシー グループの作成時に NetFlow モニター ポリシーを展開するには、次の手順を実行します。

a) 作成するインターフェイス グループのタイプを右クリックし、**[リーフ アクセス ポート ポリシー グループの作成（Create Leaf Access Port Policy Group）]** を選択します。
b) ダイアログボックスで、必要に応じてフィールドに入力します。

[NetFlow モニター ポリシー（NetFlow Monitor Policies）] テーブルで、**[+]** をクリックしてポリシーを追加し、IP フィルタ タイプとモニター ポリシーを選択します。

既存のリーフ ポリシー グループに NetFlow モニター ポリシーを展開するには、次の手順を使用します。

a) **[ナビゲーション（Navigation）]** ペインで、既存のリーフ アクセス ポート ポリシー グループ、PC インターフェイス ポリシー グループ、または VPC インターフェイス ポリシー グループのいずれかを選択します。
b) **[ワーク（Work）]**ペイン内の**[NetFlow モニター ポリシー（NetFlow Monitor Policies）]** テーブルで、**[+]** をクリックしてポリシーを追加し、IP フィルタ タイプとモニター ポリシーを選択します。
c) [Submit] をクリックします。

GUI を使用したテレメトリ方式の設定Cisco APIC

この手順では、Cisco APICGUI を使用してファブリック ノード プロファイルを作成し、テレメトリ方式を指定してから、ファブリック ノード プロファイルをファブリック ポリシー グループに関連付けます。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]**を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[モニタリング（Monitoring）]** > **[ファブリック ノード コントロール（Fabric Node Controls）]**を右クリックし、**[ファブリック ノード コントロールを作成（Create Fabric Node Control）]** を選択します。

以前のリリースでは、**[ナビゲーション（Navigation）]** ペインで、代わりに **[ファブリック ノード コントロール（Fabric Node Controls）]** を直接右クリックし（ナビゲーションブランチを展開する必要はありません）、**[ファブリック ノード コントロールの作成（Create Fabric Node Control）]** を選択します。

ステップ 3 **[ファブリック ノード コントロールを作成（Create Fabric Node Control）]** ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します：

a) **[機能選択（Feature Selection）]** の場合テレメトリ メソッドを選択します：

- **[分析の優先順位（Analytics Priority）]**：Cisco Tetration Analytics を指定します。これは、x より前のリリースのデフォルト値です。
- **[NetFlow の優先順位（NetFlow Priority）]**：NetFlow を指定します。
- **[テレメトリ優先度（Telemetry Priority）]**：Cisco Nexus ダッシュボード インサイト フローのテレメトリを指定します。これは、xリリース以降で使用可能になり、そのリリースのデフォルト値になりました。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 ファブリック ノード制御ポリシーを適切なファブリック ポリシー グループおよびプロファイルに関連付けます。たとえば、ファブリック ノード制御ポリシーをリーフ スイッチ ポリシー グループに関連付けるには、次のサブステップを実行します。

a) **[ナビゲーション（Navigation）]** ウィンドウで、**[スイッチ（Switches）]** > **[リーフ スイッチ（Leaf Switches）]** > **[ポリシー グループ（Policy Groups）]** > ***[policy_group_name]*** をクリックします。

b) **[仕事（Work）]** ペインの **[ノード コントロール ポリシー（Node Control Policy）]** で、作成したファブリック ノード制御ポリシーを選択します。

GUI を使用したテナント レベルでの NetFlow の構成

GUI を使用したテナント NetFlow モニター ポリシーの構成

次の手順では、Cisco APIC GUI を使用して テナント NetFlow モニター ポリシーを構成します。

手順

ステップ 1 メニュー バーから**[テナント（Tenants）]** > **[すべてのテナント（All Tenants）]** の順に選択します。

ステップ 2 **[作業]** ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 **[ナビゲーション ウィンドウ（Navigation）]** で **[テナント（Tenant）]<tenant-name>** > **[ポリシー（Policies）]** > **NetFlow** > **[NetFlow モニター（NetFlow Monitors）]** を選択します。

（注） 以前のリリースでは、NetFlow モニター ポリシー構成は、代わりに**Tenant <*tenant-name*>** > **Application Profiles** > **<*application-profile-name*>** の下にある場合があります。

ステップ 4 **[NetFlow モニター（NetFlow Monitors）]** を右クリックし、**[NetFlow モニターの作成（Create NetFlow Monitor）]** を選択します。

ステップ 5 **[NetFlow モニターを作成（Create NetFlow Monitor）]** ダイアログボックスで、必要に応じてフィールドに入力します。

フロー レコードとエクスポータを新規作成するか、既存のフロー レコードとエクスポータを追加できます。

[関連付けられたフローレコード（Associated Flow Record）]の作成については、GUI を使用したテナント NetFlow レコード ポリシーの構成 （14 ページ）を参照してください。

[関連付けられたフロー エクスポータ（Associated Flow Exporters）]の作成については、GUI を使用したテナント ファブリック NetFlow エクスポータ ポリシーの構成 （14 ページ）を参照してください。

最大 2 つのフロー エクスポータをモニター ポリシーに関連付けることができます。

GUI を使用したテナント NetFlow レコード ポリシーの構成

次の手順では、Cisco APIC GUI を使用して テナント NetFlow レコード ポリシーを構成します。

手順

ステップ 1 メニュー バーから**[テナント（Tenants）] > [すべてのテナント（All Tenants）]** の順に選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ペインで、**[テナント（Tenant）] <*tenant-name*> > ポリシー > NetFlow > [NetFlow レコード（NetFlow Records）]**を選択します。

（注） 以前のリリースでは、NetFlow エクスポータ ポリシー設定は代わりに **[テナント（Tenant）]<*tenant-name*> > [分析（Analytics）] > [Netflow レコード（NetFlow Records）]** の下にある場合があります。

ステップ 4 **[NetFlow レコード（NetFlow Records）]** を右クリックし、**[Flow レコードの作成（Create Flow Record）]** を選択します。

ステップ 5 [Netflow レコードを作成（Create NetFlow Record）] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) **[パラメータを作成（Collect Parameters）]** ドロップダウン リストでは、複数のパラメータを選択できます。

b) **[パラメータを一致（Match Parameters）]** ドロップダウン リストでは、複数のパラメータを選択できます。

複数のパラメータを選択する場合は、次のいずれかの組み合わせまたはいずれかの組み合わせのサブセットを選択する必要があります。

- 送信元 IPv4、接続先 IPv4、送信元 ポート、宛て先ポート、IP プロトコル、VLAN、IP TOS
- 送信元 IPv4、接続先 IPv4、送信元 ポート、宛て先ポート、IP プロトコル、VLAN、IP TOS
- Ethertype、送信元 MAC、接続先 MAC、VLAN
- 送信元 IP、接続先 IP、送信元ポート、宛て先ポート、IP プロトコル、VLAN、IP TOS。送信元 IP/接続先 IP は、IPv4 と IPv6 の両方を修飾します。

GUI を使用したテナント ファブリック NetFlow エクスポータ ポリシーの構成

次の手順では、Cisco APIC GUI を使用して テナント NetFlow エクスポータ ポリシーを構成します。

手順

ステップ 1 メニュー バーから**[テナント（Tenants）] > [すべてのテナント（All Tenants）]** の順に選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ウィンドウで **[テナント（Tenant）]<*tenant-name*>** > **[ポリシー（Policies）]** > **NetFlow** > **[NetFlow エクスポータ（NetFlow Exporters）]** を選択します。

（注） 代わりに以前のリリースでは、NetFlow エクスポータ ポリシー構成は、**[テナント（Tenant）]<*tenant-name*>** > **[分析（Analytics）]** > **[NetFlow エクスポータ（NetFlow Exporters）]** にあります。

ステップ 4 **[NetFlow エクスポータ（NetFlow Exporters）]** を右クリックし、**[外部コレクタ到達可能性を作成（Create External Collector Reachability）]** を選択します。

ステップ 5 **[外部コレクタ到達可能性を作成（Create External Collector Reachability]** ダイアログ ボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します：

a) **[NetFlow エクスポータ バージョン フォーマット（NetFlow Exporters Version Format）]** ボタンの場合、サポートされている選択肢は **[バージョン 9（Version 9）]** のみです。

b) **[EPG タイプ（EPG Type）]** チェックボックスについては、チェックボックスをオフのままにするか、1 つのボックスをオンにすることができます。複数のボックスにチェックを入れることはできません。

Cisco APIC GUI を使用した L3Out による NetFlow モニター ポリシーの展開

次の手順では、Cisco APIC GUI を使用して L3Out を介して NetFlow モニター ポリシーを展開します。

手順

ステップ 1 メニュー バーから**[テナント（Tenants）]** > **[すべてのテナント（All Tenants）]** の順に選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ペインで、**[テナント（Tenant）]<*tenant-name*>** > **[ネットワーク（ネットワーク）]** > **[外部ルーテッド ネットワーク（External Routed Networks）]** > **<*network-name*>** > **[論理的な ノード プロファイル（Logical Node Profiles）]** > **<*node-profile-name*>** > **[論理的なインターフェイス プロファイル（Logical Interface Profile）]** > **<*interface-profile-name*>**を選択します。

ステップ 4 **[全般（General）]** タブを選択します。

ステップ 5 **[NetFlow モニター ポリシー（NetFlow Monitor Policies）]** で、**[+]** をクリックして NetFlow ポリシーを追加します。

ステップ 6 **[更新（Update）]** をクリックして、NetFlow ポリシーを追加します。

Cisco APIC GUI を使用したブリッジ ドメインを介した NetFlow モニター ポリシーの展開

次の手順では、Cisco APIC GUI を使用してブリッジ ドメインを介して NetFlow モニター ポリシーを展開します。

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ウィンドウで、**[テナント（Tenant）]*[tenant_name]*** > **[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]**を選択します。

ステップ 4 新しいブリッジ ドメインを作成するときに NetFlow モニター ポリシーを展開できます。または、既存のブリッジ ドメインに NetFlow モニター ポリシーを展開できます。

新しいブリッジ ドメインの作成時に NetFlow モニター ポリシーを展開するには、次の手順を実行します。

a) **[仕事（Work）]** ウィンドウで、**[アクション（Actions）]** > **[レイヤー 3 ドメイン（Create Layer 3 Domain）]** を選択します。

b) **[ブリッジ ドメインを作成（Create Bridge Domain）]** ダイアログ ボックスで、次に指定されている点を除き、必要に応じてフィールドに入力します：

1. **[高度なトラブルシューティング（Advanced Troubleshooting）]** ステップの **[NetFlow モニター ポリシー（NetFlow Monitor Policies）]** テーブルで、**[+]** をクリックし、NetFlow IP フィルタ タイプを選択し、NetFlow モニター ポリシーを選択して、**[更新（Update）]** をクリックします。
2. [Finish] をクリックします。

既存のブリッジ ドメインに NetFlow モニター ポリシーを展開するには、次の手順を使用します：

a) **[ナビゲーション（Navigation）]** ペインで、既存のブリッジ ドメインの 1 つを選択します。

b) **[作業（Work）]** ペインで、**[ポリシー（Policy）]** > **[アドバンスト トラブルシューティング（Advanced Troubleshooting）]**を選択します。

c) **[NetFlow モニター ポリシー（NetFlow Monitor Policies）]** テーブルで、**[+]** をクリックし、NetFlow IP フィルタ タイプを選択し、NetFlow モニター ポリシーを選択して、**[更新（Update）]** をクリックします。

d) [Submit] をクリックします。

GUI を使用したテレメトリ方式の設定Cisco APIC

この手順では、Cisco APICGUI を使用してファブリック ノード プロファイルを作成し、テレメトリ方式を指定してから、ファブリック ノード プロファイルをファブリック ポリシー グループに関連付けます。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]**を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[モニタリング（Monitoring）]** > **[ファブリック ノード コントロール（Fabric Node Controls）]**を右クリックし、**[ファブリック ノード コントロールを作成（Create Fabric Node Control）]** を選択します。

以前のリリースでは、**[ナビゲーション（Navigation）]** ペインで、代わりに **[ファブリック ノード コントロール（Fabric Node Controls）]** を直接右クリックし（ナビゲーションブランチを展開する必要はありません）、**[ファブリック ノード コントロールの作成（Create Fabric Node Control）]** を選択します。

ステップ 3 **[ファブリック ノード コントロールを作成（Create Fabric Node Control）]** ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します：

a) **[機能選択（Feature Selection）]** の場合テレメトリ メソッドを選択します：

- **[分析の優先順位（Analytics Priority）]**：Cisco Tetration Analytics を指定します。これは、x より前のリリースのデフォルト値です。
- **[NetFlow の優先順位（NetFlow Priority）]**：NetFlow を指定します。
- **[テレメトリ優先度（Telemetry Priority）]**：Cisco Nexus ダッシュボード インサイト フローのテレメトリを指定します。これは、x リリース以降で使用可能になり、そのリリースのデフォルト値になりました。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 ファブリック ノード制御ポリシーを適切なファブリック ポリシー グループおよびプロファイルに関連付けます。たとえば、ファブリック ノード制御ポリシーをリーフ スイッチ ポリシー グループに関連付けるには、次のサブステップを実行します。

a) **[ナビゲーション（Navigation）]** ウィンドウで、**[スイッチ（Switches）]** > **[リーフ スイッチ（Leaf Switches）]** > **[ポリシー グループ（Policy Groups）]** > ***[policy_group_name]*** をクリックします。

b) **[仕事（Work）]** ペインの **[ノード コントロール ポリシー（Node Control Policy）]** で、作成したファブリック ノード制御ポリシーを選択します。

NX-OS スタイルの CLI を使用したNetFlow の構成

NX-OS スタイルの CLI を使用したNetFlow ノード ポリシーの構成

次の手順例では、NX-OS スタイルの CLI を使用して NetFlow ノード ポリシーを構成します：

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 ノード ポリシーの構成。

例：

```
apic1(config)# flow node-policy nodePol
apic1(config-flow-node-pol)# flow timeout collection 100
```

```
apic1(config-flow-node-pol)# flow timeout template 123
apic1(config-flow-node-pol)# exit
```

NX-OS スタイルの CLI を使用したNetFlow インフラ セレクタの構成

NX-OS スタイルの CLI を使用して、NetFlow インフラ セレクタを構成できます。インフラ セレクタは、NetFlow モニターを PHY、ポート チャネル、仮想ポート チャネル、ファブリック エクステンダ（FEX）、またはポート チャネル ファブリック エクステンダ（FEXPC）インターフェイスに接続するために使用されます。

次の CLI コマンドの例は、NX-OS スタイルの CLI を使用して NetFlow インフラ セレクタを構成する方法を示しています。

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 NetFlow エクスポータ ポリシーを作成します。

例：

次のコマンドでは、接続先エンドポイント グループは、エクスポータが背後にあるエンドポイント グループです。このエンドポイント グループは、外部レイヤ 3 エンドポイント グループにすることもできます。

```
apic1(config)# flow exporter infraExporter1 destination address 1.2.3.4 transpo udp 1234
apic1(config-flow-exporter)# destination epg tenant tn2 application ap2 epg epg2
apic1(config-flow-exporter)# vrf member tenant tn2 vrf vrf2
apic1(config-flow-exporter)# version v9
apic1(config-flow-exporter)# source address 1.1.1.1
apic1(config-flow-exporter)# exit
```

ステップ 3 2 つ目の NetFlow エクスポータ ポリシーを作成します。

例：

次のコマンドでは、接続先エンドポイント グループはエクスポータが背後にあるエンドポイント グループです。この場合は外部レイヤ 3 エンドポイント グループです。

```
apic1(config)# flow exporter infraExporter2
apic1(config-flow-exporter)# transport udp 9990
apic1(config-flow-exporter)# destination address 2001:db5:a0c:1f0::2
apic1(config-flow-exporter)# destination external-l3 epg tenant tn2 vrf v2 epg accounting-inst
apic1(config-flow-exporter)# vrf member tenant tn2 vrf vrf2
apic1(config-flow-exporter)# version v5
apic1(config-flow-exporter)# source address 2001:db8:a0b:12f0::1
apic1(config-flow-exporter)# exit
```

ステップ 4 NetFlow レコード ポリシーを作成します。

例：

```
apic1(config)# flow record infraRecord1
apic1(config-flow-record)# match dst-ip
```

```
apic1(config-flow-record)# match dst-ipv4
apic1(config-flow-record)# match dst-ipv6
apic1(config-flow-record)# match dst-mac
apic1(config-flow-record)# match dst-port
apic1(config-flow-record)# match ethertype
apic1(config-flow-record)# match proto
apic1(config-flow-record)# match src-ip
apic1(config-flow-record)# match src-ipv4
apic1(config-flow-record)# match src-ipv6
apic1(config-flow-record)# match src-mac
apic1(config-flow-record)# match src-port
apic1(config-flow-record)# match tos
apic1(config-flow-record)# match vlan
apic1(config-flow-record)# collect count-bytes
apic1(config-flow-record)# collect count-pkts
apic1(config-flow-record)# collect pkt-disp
apic1(config-flow-record)# collect sampler-id
apic1(config-flow-record)# collect src-intf
apic1(config-flow-record)# collect tcp-flags
apic1(config-flow-record)# collect ts-first
apic1(config-flow-record)# collect ts-recent
apic1(config-flow-record)# exit
```

ステップ 5 NetFlow モニター ポリシーを作成します。

例：

```
apic1(config)# flow monitor infraMonitor1
apic1(config-flow-monitor)# record infraRecord1
apic1(config-flow-monitor)# exporter infraExporter1
apic1(config-flow-monitor)# exporter infraExporter2
apic1(config-flow-monitor)# exit
```

最大 2 つのエクスポータを接続できます。

ステップ 6 インターフェイス ポリシー グループ（AccPortGrp）を作成します。

例：

```
apic1(config)# template policy-group pg1
apic1(config-pol-grp-if)# ip flow monitor infraMonitor1
apic1(config-pol-grp-if)# ipv6 flow monitor infraMonitor2
apic1(config-pol-grp-if)# exit
```

アドレス ファミリ（IPv4 および IPv6）ごとに 1 つのモニター ポリシーを設定できます。

ステップ 7 ノード プロファイルとインフラ セレクタを作成します。

例：

```
apic1(config)# leaf-profile lp1
apic1(config-leaf-profile)# leaf-group lg1
apic1(config-leaf-group)# leaf 101
apic1(config-leaf-profile)# exit
apic1(config)# leaf-interface-profile lip1
apic1(config-leaf-if-profile)# exit
apic1(config)# leaf-interface-profile lip1
apic1(config-leaf-if-profile)# leaf-interface-group lig1
apic1(config-leaf-if-group)# interface ethernet 1/5
apic1(config-leaf-if-profile)# policy-group pg1
apic1(config-leaf-if-profile)# exit
apic1(config-leaf-profile)# exit
```

ステップ 8 ポート チャネル ポリシー グループ（AccBndlGrp）を作成します。

例：

```
apic1(config)# template port-channel po6
apic1(config-if)# ip flow monitor infraMonitor1
apic1(config-if)# ipv6 flow monitor infraMonitor1
apic1(config-if)# exit
apic1(config-leaf-profile)# leaf-profile lp2
apic1(config-leaf-group)# leaf-group lg2
apic1(config-leaf-profile)# leaf 101
apic1(config-leaf-profile)# exit
apic1(config)# leaf-interface-profile lip2
apic1(config-leaf-if-profile)# exit
apic1(config)# leaf-interface-profile lip2
apic1(config-leaf-if-profile)# leaf-interface-group lig2
apic1(config-leaf-if-group)# interface ethernet 1/6
apic1(config-leaf-if-profile)# channel-group po6
apic1(config-leaf-if-profile)# exit
```

アドレス ファミリ（IPv4 および IPv6）ごとに 1 つのモニター ポリシーを設定できます。インターフェイスは vPC にすることもできます。

NX-OS スタイルの CLI を使用したNetFlow 上書きの構成

次の手順では、NX-OS スタイルの CLI を使用して NetFlow オーバーライドを構成します：

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 オーバーライドを作成。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant tn2 vrf vrf2
apic1(config-leaf)# exit
apic1(config)# interface ethernet 1/15
apic1(config-if)# ip flow monitor infraMonitor1
apic1(config-if)# ipv6 flow monitor infraMonitor2
apic1(config-if)# exit
apic1(config)# exit
apic1# exit
```

アドレス ファミリ（IPv4 および IPv6）ごとに 1 つのモニター ポリシーを設定できます。インターフェイスは vPC にすることもできます。

NX-OS スタイル CLI を使用して NetFlow テナント階層の構成

次の手順例では、NX-OS スタイルの CLI を使用して NetFlow テナント階層を構成します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 テナントとブリッジ ドメインを作成し、VRF に追加します。

例：

```
apic1(config)# tenant tn2
apic1(config-tenant)# vrf context vrf2
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# bridge-domain bd2
apic1(config-tenant-bridge-domain)# vrf member vrf2
apic1(config-tenant-bridge-domain)# exit
apic1(config-tenant)# bridge-domain bd3
apic1(config-tenant-bridge-domain)# vrf member vrf2
apic1(config-tenant-bridge-domain)# exit
```

ステップ 3 エクスポータが存在するアプリケーション エンドポイント グループを作成します。

例：

```
apic1(config-tenant)# application ap2
apic1(config-tenant-app)# epg epg2
apic1(config-tenant-app)# bridge-domain member bd2
apic1(config-tenant-app-bridge-domain)# exit
apic1(config-tenant-app)# exit
```

ステップ 4 エクスポータが存在する 2 番目のアプリケーション エンドポイント グループを作成します。

例：

```
apic1(config-tenant)# application ap3
apic1(config-tenant-app)# epg epg3
apic1(config-tenant-app)# bridge-domain member bd3
apic1(config-tenant-app-bridge-domain)# exit
apic1(config-tenant-app)# exit
```

ステップ 5 ブリッジ ドメインに NetFlow モニター ポリシーを添付します。

例：

```
apic1(config)# interface bridge-domain bd2
apic1(config-if)# ipv6 flow monitor tnMonitor1
apic1(config-if)# ip flow monitor tnMonitor1
apic1(config-if)# layer2-switched flow monitor tnMonitor1
apic1(config-if)# exit
apic1(config)# interface bridge-domain bd3
apic1(config-if)# ipv6 flow monitor tnMonitor1
apic1(config-if)# ip flow monitor tnMonitor1
apic1(config-if)# exit
```

アドレス ファミリ（IPv4 および IPv6）ごとに 1 つのモニター ポリシーを設定できます。インターフェイスは vPC にすることもできます。

ステップ 6 NetFlow エクスポータ ポリシーを作成します。

例：

次のコマンドでは、接続先エンドポイント グループは、エクスポータが背後にあるエンドポイント グループです。このエンドポイント グループは、外部レイヤ 3 エンドポイント グループにすることもできます。

```
apic1(config)# flow exporter tnExporter1
apic1(config-flow-exporter)# transport udp 1234
apic1(config-flow-exporter)# destination address 2.2.2.2
apic1(config-flow-exporter)# destination epg tenant tn2 application ap2 epg epg2
apic1(config-flow-exporter)# vrf member tenant tn2 vrf vrf2
apic1(config-flow-exporter)# version v9
apic1(config-flow-exporter)# source address 1.1.1.1
apic1(config-flow-exporter)# exit
```

ステップ 7 2 つ目の NetFlow エクスポータ ポリシーを作成します。

例：

次のコマンドでは、接続先エンドポイント グループはエクスポータが背後にあるエンドポイント グループです。この場合は外部レイヤ 3 エンドポイント グループです。

```
apic1(config)# flow exporter tnExporter2
apic1(config-flow-exporter)# transport udp 9990
apic1(config-flow-exporter)# destination address 2001:db5:a0c:1f0::2
apic1(config-flow-exporter)# destination external-l3 epg tenant tn2 vrf v2 epg accounting-inst
apic1(config-flow-exporter)# vrf member tenant tn2 vrf vrf2
apic1(config-flow-exporter)# version v5
apic1(config-flow-exporter)# source address 2001:db8:a0b:12f0::1
apic1(config-flow-exporter)# exit
```

ステップ 8 NetFlow レコード ポリシーを作成します。

例：

```
apic1(config)# flow record tnRecord1
apic1(config-flow-record)# match dst-ip
apic1(config-flow-record)# match dst-ipv4
apic1(config-flow-record)# match dst-ipv6
apic1(config-flow-record)# match dst-mac
apic1(config-flow-record)# match dst-port
apic1(config-flow-record)# match ethertype
apic1(config-flow-record)# match proto
apic1(config-flow-record)# match src-ip
apic1(config-flow-record)# match src-ipv4
apic1(config-flow-record)# match src-ipv6
apic1(config-flow-record)# match src-mac
apic1(config-flow-record)# match src-port
apic1(config-flow-record)# match tos
apic1(config-flow-record)# match vlan
apic1(config-flow-record)# collect count-bytes
apic1(config-flow-record)# collect count-pkts
apic1(config-flow-record)# collect pkt-disp
apic1(config-flow-record)# collect sampler-id
apic1(config-flow-record)# collect src-intf
apic1(config-flow-record)# collect tcp-flags
```

```
apic1(config-flow-record)# collect ts-first
apic1(config-flow-record)# collect ts-recent
apic1(config-flow-record)# exit
```

ステップ 9 NetFlow モニター ポリシーを作成します。

例：

```
apic1(config)# flow monitor tnMonitor1
apic1(config-flow-monitor)# record tnRecord1
apic1(config-flow-monitor)# exporter tnExporter1
apic1(config-flow-monitor)# exporter tnExporter2
apic1(config-flow-monitor)# exit
```

最大 2 つのエクスポータを接続できます。

ステップ 10 VLAN ドメインに VLAN を追加し、リーフ ノードの VRF を構成します。

例：

```
apic1(config)# vlan-domain dom1
apic1(config-vlan)# vlan 5-100
apic1(config-vlan)# exit
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant tn2 vrf vrf2
apic1(config-leaf-vrf)# exit
```

ステップ 11 インターフェイスにエンドポイント グループを展開して、ブリッジ ドメインを展開します。

例：

```
apic1(config-leaf)# interface ethernet 1/10
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# switchport trunk allowed vlan 10 tenant tn2 application ap2 epg epg2
apic1(config-leaf-if)# exit
```

ステップ 12 インターフェイスに別のエンドポイント グループを展開します。

例：

```
apic1(config-leaf)# interface ethernet 1/11
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# switchport trunk allowed vlan 11 tenant tn2 application ap3 epg epg3
apic1(config-leaf-if)# exit
```

ステップ 13 サブインターフェースにモニター ポリシーを添付します。

例：

```
apic1(config-leaf)# interface ethernet 1/20
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/20.20
apic1(config-leaf-if)# vrf member tenant tn2 vrf vrf2
apic1(config-leaf-if)# ipv6 address 20::1/64 preferred
apic1(config-leaf-if)# ipv6 flow monitor tnMonitor1
apic1(config-leaf-if)# ip flow monitor tnMonitor2
apic1(config-leaf-if)# exit
```

ステップ 14 スイッチ仮想インターフェイス（SVI）にモニター ポリシーを添付します。

例：

```
apic1(config-leaf)# interface vlan 30
apic1(config-leaf-if)# vrf member tenant tn2 vrf vrf2
apic1(config-leaf-if)# ipv6 address 64::1/64 preferred
apic1(config-leaf-if)# ip flow monitor tnMonitor1
apic1(config-leaf-if)# ip6 flow monitor tnMonitor1
apic1(config-leaf-if)# exit
```

ステップ 15 SVI をレイヤ 2 インターフェイスに関連付けます。

例：

```
apic1(config-leaf)# interface ethernet 1/30
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# switchport trunk allowed vlan 30 tenant tn2 external-svi
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# exit
```

NX-OS スタイルの CLI を使用したノード制御ポリシーによる NetFlow および Tetration 分析機能の優先順位の設定

次の手順例では、NX-OS スタイルの CLI を使用して、ノード制御ポリシーを介して NetFlow および Tetration 分析機能の優先順位を構成します：

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 ノード制御ポリシーを作成します。

例：

```
apic1(config)# node-control policy pol1
```

ステップ 3 プライオリティ機能として NetFlow を設定します。

例：

```
apic1(config-node)# feature netflow
```

ステップ 4 ノード制御ポリシー構成を終了します。

例：

```
apic1(config-node)# end
```

ステップ 5 ポリシーをノード 101 とノード 102 に展開します。

例：

```
ifav-isim15-ifc1(config)# fabric-internal
ifav-isim15-ifc1(config-fabric-internal)# template leaf-policy-group lpg1
ifav-isim15-ifc1(config-leaf-policy-group)# inherit node-control-policy pol1
```

```
ifav-isim15-ifc1(config-leaf-policy-group)# exit
ifav-isim15-ifc1(config-fabric-internal)# leaf-profile leafProfile1
ifav-isim15-ifc1(config-leaf-profile)# leaf-group leafgrp1
ifav-isim15-ifc1(config-leaf-group)# leaf 101
ifav-isim15-ifc1(config-leaf-group)# leaf 102
ifav-isim15-ifc1(config-leaf-group)# leaf-policy-group lpg1
ifav-isim15-ifc1(config-leaf-group)# end
```

NX-OS スタイルの CLI を使用した NetFlow 構成の確認

次の手順では、Cisco Application Policy Infrastructure Controller（Cisco APIC）NX-OS スタイル CLI とリーフ スイッチの NX-OS CLI を使用して NetFlow 構成を確認します。

手順

ステップ 1 Cisco APIC NX-OS スタイルの CLI で、必要に応じて、インフラ テナントまたは指定されたテナントの NetFlow モニター情報を表示します。

show flow monitor {infra *policy_name* detail | tenant *tenant_name*}

例：

```
apic1# show flow monitor infra default detail
```

ステップ 2 CLI のいずれかのリーフ スイッチを使用して、次のコマンドを実行します。

例：

```
leaf# show flow exporter
leaf# show flow record
leaf# show flow monitor
leaf# show flow timers
leaf# show flow interface
leaf# show flow vlan
```

REST API を使用した NetFlow の構成

REST API を使用した NetFlow インフラ セレクタの構成

REST API を使用して、NetFlow インフラ セレクタを構成できます。インフラ セレクタは、NetFlow モニターを PHY、ポート チャネル、仮想ポート チャネル、ファブリック エクステンダ（FEX）、またはポート チャネル ファブリック エクステンダ（FEXPC）インターフェイスに接続するために使用されます。

次の XML の例は、REST API を使用して NetFlow インフラ セレクタを構成する方法を示しています。

```
<infraInfra>
    <!--Create Monitor Policy /-->
    <netflowMonitorPol name='monitor_policy1' descr='This is a monitor policy.'>
        <netflowRsMonitorToRecord tnNetflowRecordPolName='record_policy1' />
        <!-- A Max of 2 exporters allowed per Monitor Policy /-->
```

```
        <netflowRsMonitorToExporter tnNetflowExporterPolName='exporter_policy1' />
        <netflowRsMonitorToExporter tnNetflowExporterPolName='exporter_policy2' />
    </netflowMonitorPol>

    <!--Create Record Policy /-->
    <netflowRecordPol name='record_policy1' descr='This is a record policy.' match='src-ipv4,src-port'/>

    <!--Create Exporter Policy /-->
    <netflowExporterPol name='exporter_policy1' dstAddr='10.10.1.1' srcAddr='10.10.1.10' ver='v9' descr='This
 is an exporter policy.'>
        <!--Exporter can be behind app EPG or external L3 EPG (InstP) /-->
        <netflowRsExporterToEPg tDn='uni/tn-t1/ap-app1/epg-epg1'/>
        <!--This Ctx needs to be the same Ctx that EPG1's BD is part of /-->
        <netflowRsExporterToCtx tDn='uni/tn-t1/ctx-ctx1'/>
    </netflowExporterPol>

    <!--Node-level Policy for collection Interval /-->
    <netflowNodePol name='node_policy1' collectIntvl='500' />

    <!-- Node Selectors - usual config /-->
    <infraNodeP name="infraNodeP-17" >
        <infraLeafS name="infraLeafS-17" type="range">
            <!-- NOTE: The nodes can also be fex nodes /-->
            <infraNodeBlk name="infraNodeBlk-17" from_="101" to_="101"/>
            <infraRsAccNodePGrp tDn='uni/infra/funcprof/accnodepgrp-nodePGrp1' />
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-infraAccPortP"/>
    </infraNodeP>

    <!-- Port Selectors - usual config /-->
    <infraAccPortP name="infraAccPortP" >
        <infraHPortS name="infraHPortS" type="range">
            <!-- NOTE: The interfaces can also be Port-channels, fex interfaces or fex PCs /-->
            <infraPortBlk name="infraPortBlk" fromCard="1" toCard="1" fromPort="8" toPort="8"/>
            <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-infraAccPortGrp"/>
        </infraHPortS>
    </infraAccPortP>

    <!-- Policy Groups - usual config /-->
    <infraFuncP>
        <!-- Node Policy Group - to setup Netflow Node Policy /-->
        <infraAccNodePGrp name='nodePGrp1' >
            <infraRsNetflowNodePol tnNetflowNodePolName='node_policy1' />
        </infraAccNodePGrp>

        <!-- Access Port Policy Group - to setup Netflow Monitor Policy /-->
        <infraAccPortGrp name="infraAccPortGrp" >
            <!--One Monitor Policy per address family (ipv4, ipv6, ce) /-->
            <infraRsNetflowMonitorPol tnNetflowMonitorPolName='monitor_policy1' fltType='ipv4'/>
            <infraRsNetflowMonitorPol tnNetflowMonitorPolName='monitor_policy2' fltType='ipv6'/>
            <infraRsNetflowMonitorPol tnNetflowMonitorPolName=`monitor_policy2' fltType=`ce'/>
        </infraAccPortGrp>
    </infraFuncP>
</infraInfra>
```

REST API を使用した NetFlow テナント階層の構成

REST API を使用して、NetFlow テナント階層を構成できます。テナント階層は、NetFlow モニターをブリッジ ドメイン、レイヤ 3 サブインターフェイス、またはレイヤ 3 スイッチ仮想インターフェイス（SVI）に接続するために使用されます。

次の XML の例は、REST API を使用して NetFlow テナント階層を構成する方法を示しています。

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- api/policymgr/mo/.xml -->
<polUni>
    <fvTenant name="t1">

        <!--Create Monitor Policy /-->
        <netflowMonitorPol name='monitor_policy1' descr='This is a monitor policy.'>
            <netflowRsMonitorToRecord tnNetflowRecordPolName='record_policy1' />
            <!-- A Max of 2 exporters allowed per Monitor Policy /-->
            <netflowRsMonitorToExporter tnNetflowExporterPolName='exporter_policy1' />
            <netflowRsMonitorToExporter tnNetflowExporterPolName='exporter_policy2' />
        </netflowMonitorPol>
        <!--Create Record Policy /-->
        <netflowRecordPol name='record_policy1' descr='This is a record policy.'/>

        <!--Create Exporter Policy /→
        <netflowExporterPol name='exporter_policy1' dstAddr='10.0.0.1' srcAddr='10.0.0.4'>

            <!--Exporter can be behind app EPG or external L3 EPG (InstP) /-->
            <netflowRsExporterToEPg tDn='uni/tn-t1/ap-app1/epg-epg2'/>
            <!--netflowRsExporterToEPg tDn='uni/tn-t1/out-out1/instP-accountingInst' /-->
            <!--This Ctx needs to be the same Ctx that EPG2's BD is part of /-->
            <netflowRsExporterToCtx tDn='uni/tn-t1/ctx-ctx1' />
        </netflowExporterPol>

        <!--Create 2nd Exporter Policy /-->
        <netflowExporterPol name='exporter_policy2' dstAddr='11.0.0.1' srcAddr='11.0.0.4'>
            <netflowRsExporterToEPg tDn='uni/tn-t1/ap-app1/epg-epg2'/>
            <netflowRsExporterToCtx tDn='uni/tn-t1/ctx-ctx1' />
        </netflowExporterPol>

        <fvCtx name="ctx1" />

        <fvBD name="bd1" unkMacUcastAct="proxy" >
            <fvSubnet descr="" ip="11.0.0.0/24"\>
            <fvRsCtx tnFvCtxName="ctx1" />

            <!--One Monitor Policy per address family (ipv4, ipv6, ce) /-->
            <fvRsBDToNetflowMonitorPol tnNetflowMonitorPolName='monitor_policy1' fltType='ipv4'/>
            <fvRsBDToNetflowMonitorPol tnNetflowMonitorPolName='monitor_policy2' fltType='ipv6'/>
            <fvRsBDToNetflowMonitorPol tnNetflowMonitorPolName=`monitor_policy2' fltType='ce'/>
        </fvBD>

        <!--Create App EPG /-->
        <fvAp name="app1">
            <fvAEPg name="epg2" >
                <fvRsBd tnFvBDName="bd1" />
                <fvRsPathAtt encap="vlan-20" instrImedcy="lazy" mode="regular"
tDn="topology/pod-1/paths-101/pathep-[eth1/20]"/>
            </fvAEPg>
        </fvAp>

        <!--L3 Netflow Config for sub-intf and SVI /-->
        <l3extOut name="out1">
            <l3extLNodeP name="lnodep1" >
                <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="1.2.3.4" />
                <l3extLIfP name='lifp1'>
                    <!--One Monitor Policy per address family (ipv4, ipv6, ce) /-->
                    <l3extRsLIfPToNetflowMonitorPol tnNetflowMonitorPolName='monitor_policy1' fltType='ipv4'
/>
                    <l3extRsLIfPToNetflowMonitorPol tnNetflowMonitorPolName='monitor_policy2' fltType='ipv6'
/>
                    <l3extRsLIfPToNetflowMonitorPol tnNetflowMonitorPolName=`monitor_policy2' fltType=`ce' />
```

```
                    <!--Sub-interface 1/40.40 on node 101 /-->
                   <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/40]" ifInstT='sub-interface'
 encap='vlan-40' />

                    <!--SVI 50 attached to eth1/25 on node 101 /-->
                   <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]" ifInstT='external-svi'
 encap='vlan-50' />
                </l3extLIfP>
            </l3extLNodeP>

            <!--External L3 EPG for Exporter behind external L3 Network /-->
            <l3extInstP name="accountingInst">
                <l3extSubnet ip="11.0.0.0/24" />
            </l3extInstP>
            <l3extRsEctx tnFvCtxName="ctx1"/>
        </l3extOut>
    </fvTenant>
</polUni>
```

REST API を使用した NetFlow または Tetration Analytics の優先順位の構成

`<fabricNodeControl>` エレメントの`FeatureSel` 属性を設定することで NetFlow または、 Cisco Tetration 分析機能を使用するかを指定できます。`FeatureSel` 属性には、次のいずれかの値を指定できます。

- `[分析（analytics）]` — Cisco Tetration Analytics を指定します。これはデフォルト値です。
- `netflow` — NetFlow を指定します。

次の REST API ポストの例では、NetFlow 機能を使用するようにスイッチ「test1」を指定しています。

```
http://192.168.10.1/api/node/mo/uni/fabric.xml
<fabricNodeControl name="test1" FeatureSel="netflow" />
```

付録

NetFlow 一致基準について

FT ブロックのフィルタ Ternary Content-Addressable Memory（TCAM）は、フロー テーブルにインストールする必要があるフローと一致します。この TCAM は、IPv4 と IPv6、およびレイヤ 2 キーをサポートします。IPv4 の場合、TCAM は 1k の一致基準を保持できます。IPv6 には 4 つのエントリが必要で、256 の一致基準のみを保持できます。

TCAM では、次のキーがサポートされています：

IP：

- 送信元 TEP/VIF
- 宛先 TEP
- IP フラグ
- TCP フラグ
- 送信元 IP

- 宛先 IP
- テナント = インフラトランジットまたは BD の VNI。
- プロトコル
- Src L4 ポート
- Dst L4 ポート

CE：

- 送信元 TEP
- 宛先 TEP
- テナント
- Mac SA
- Mac DA
- イーサタイプ

パケットが TCAM でプログラムされた基準に一致し、TCAM アクションが特定のマスクでフローを収集するように指示すると、パケットはフロー テーブルにインストールされます。

NetFlow フロー マスクについて

EX スイッチは、フローのタイプ（IPv4、IPv6、および CE）ごとに 4 つのマスクを提供します。このマスクは、一連のパケットから同じフローを構成するものを定義し、1 つのフローがフローテーブルの 1 つのエントリを占有します。たとえば、5 タプル（SIP、DIP、Protocol、Sport、および Dport）とブリッジ ドメインをフローとして構成し、これらのフィールドが他のパケットと異なるパケットを別のフローの一部にすることができます。スポートがマスクされている場合、残りのすべてのフィールドに一致するが、このフィールドが異なるすべてのパケットは同じフローを構成し、統計情報はテーブル内の 1 つのエントリに収集されます。

次のパケットの例は、フロー マスクの動作を示しています。

```
Pkt 1: BD1, 10.1.1.12 > 10.1.1.13, TCP, Sport 10000, Dport 80 Bytes = 100
Pkt 2: BD1, 10.1.1.12 > 10.1.1.13, TCP, Sport 20000, Dport 80 Bytes = 200
```

これらのパケットのマスクがレイヤ 4 スポーツをマスクするように設定されている場合、次のようにマスクによってフロー テーブルに 1 つのエントリが作成されます。

```
Flow 1: BD1, 10.1.1.12 > 10.1.1.13, TCP, Sport = 0, Dport 80, Bytes = 300
```

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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。