Cflowd を使用したトラフィック フロー モニタリング

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます：**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、および **Cisco vSmart** から **Cisco Catalyst SD-WAN Controller** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 *1:* 機能の履歴

機能名	リリース情報	説明
Flexible NetFlow での IPv6 サポートとキャッシュ サイズ変更	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	これは、Cisco IOS XE Catalyst SD-WAN デバイスの IPv6 トランスポートを介した外部コレクタへのパケットのエクスポートを可能にし、IPv6 ネットワークトラフィックを可視化できるようにする機能です。IPv4 トラフィックと IPv6 トラフィックを同時にモニターする場合は、この機能を使用することで、データプレーンのキャッシュサイズを変更できます。Cisco Flexible NetFlow（FNF）は、ネットワークトラフィックをカスタマイズして可視化できるようにするテクノロジーです。Cisco Catalyst SD-WAN では、FNF を使用して Cisco SD-WAN Manager にデータをエクスポートできるため、お客様はネットワークを簡単に監視および改善できます。
暗黙的な ACL によってドロップされたパケットのログ	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	リンク障害が発生した場合にドロップされたパケットのロギングを有効または無効にできるようになりました。パケットフローをログに記録する頻度も設定できます。
Flexible NetFlow の機能拡張	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	これは、Flexible NetFlow を拡張して、NetFlow レコード内のタイプオブサービス（ToS）、サンプラー ID、および再マーキングされた DSCP 値を収集する機能です。この機能拡張により、フローレコードフィールドを定義してフローレコードをカスタマイズする柔軟性がもたらされます。ToS および再マーキングされた DSCP フィールドは、IPv4 レコードでのみサポートされます。ただし、サンプラー ID フィールドは IPv4 レコードと IPv6 レコードの両方でサポートされます。
VPN0 インターフェイス向け Flexible NetFlow	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	これは、VPN0 インターフェイスで NetFlow をサポートする機能です。 Flexible NetFlow はセキュリティツールとして機能し、Cisco SD-WAN Manager へのデータのエクスポートを可能にし、デバイスへの攻撃を検出し、トラフィックをモニターします。

機能名	リリース情報	説明
Flexible NetFlow 分散エクスポート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.9.x Cisco vManage リリース 20.9.1	これは、分散エクスポートを有効にして、パケットのバーストが外部コレクタに送信されたときに発生するエクスポートストームを防止する機能です。直前の間隔でのエクスポートが現在の間隔中に展開されることにより、エクスポート ストームが回避されます。NetFlowパケットが低帯域幅の回線を介して送信される場合、パケットのドロップを回避するのに分散エクスポート機能が有効です。
Flexible NetFlow による BFD メトリックのエクスポート	Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1	この機能を使用すると、Bidirectional Forwarding Detection (BFD) メトリックを外部コレクタにエクスポートして、損失、遅延、およびジッターの BFD メトリックを生成できます。この機能により、ネットワーク状態データのモニタリングが強化され、収集が高速化されます。 BFD メトリックのエクスポートを有効にした後、BFD メトリックをエクスポートするためのエクスポート間隔を設定します。
Cflowd フローおよび SAIE フローをモニタリングするためのリアルタイム デバイス オプション	Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a Cisco vManage リリース 20.10.1	この機能を使用すると、選択した Cisco IOS XE Catalyst SD-WAN デバイス の VPN 内で実行されている特定の Cflowd および Cisco Catalyst SD-WAN Application Intelligence Engine（SAIE）のアプリケーションまたはアプリケーションファミリをモニタリングするためのフィルタが適用できます。 Cflowd フローおよび SAIE フローをモニタリングするためのリアルタイム デバイス オプションは、Cisco vEdge デバイス で使用できます。このリリースでは、Cisco IOS XE Catalyst SD-WAN デバイス で Cflowd および SAIE のアプリケーションをモニタリングするためのリアルタイムデバイス オプションがサポートされています。
Cisco SD-WAN Analytics のための Flexible NetFlow の拡張機能	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	これは、Cisco SD-WAN Analytics の IPv4 および IPv6 フローレコードのために、Cisco Flexible NetFlow にロギング拡張機能を取り入れる機能です。 これらのレコードに対する **show flow record** コマンドの出力が拡張されました。

機能名	リリース情報	説明
ループバックを TLOC として使用する場合のフローテレメトリの機能拡張。	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	ループバック インターフェイスを入力または出力トランスポート インターフェイスとして設定すると、この機能により、FNF レコードの物理インターフェイスの代わりにループバックを収集できます。この機能は、IPv4 および IPv6 でサポートされています。 ループバック インターフェイスと物理インターフェイス間のバインディング関係を表示するために、show コマンド **show sdwan control local-properties wan-interface-list** を更新しました。 Cisco SD-WAN Manager の既存オプションに、[インターフェイスのバインド（Bind Interface）] という新しい列が追加されました。ループバック インターフェイスと物理インターフェイス間のバインディング関係を表示するには、[モニター（Monitor）] > [デバイス（Devices）] > [リアルタイム（Real Time）]（デバイスオプションである [WANインターフェイス情報の管理（Control WAN Interface Information）] を選択）の順にクリックしてください。

トラフィック フロー モニタリングについて

Cflowd を使用したトラフィック フロー モニタリングの概要

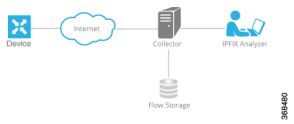
Cflowd は、Flexible NetFlow（FNF）トラフィックデータの分析に使用されるフロー分析ツールです。オーバーレイネットワーク内の Cisco IOS XE Catalyst SD-WAN デバイス を通過するトラフィックをモニタリングし、フロー情報をコレクタにエクスポートします。コレクタでは、フロー情報を IP Flow Information Export（IPFIX）アナライザで処理できます。トラフィックフローの場合、Cflowd は定期的にテンプレートレポートをフローコレクタに送信します。このレポートには、フローに関する情報が含まれており、データはこれらのレポートのペイロードから抽出されます。

Cflowd コレクタの場所、サンプリングされた一連のフローがコレクタに送信される頻度、およびテンプレートがコレクタに送信される頻度を定義する Cflowd テンプレートを作成できます（Cisco SD-WAN コントローラ および Cisco SD-WAN Manager）。Cisco IOS XE Catalyst SD-WAN デバイス ごとに最大 4 つの Cflowd コレクタを設定できます。Cflowd テンプレートを有効にするには、適切なデータポリシーを使用して適用します。

少なくとも 1 つの Cflowd テンプレートを設定する必要がありますが、パラメータを含める必要はありません。パラメータを指定しない場合、ノードのデータフローキャッシュはデフォルト設定で管理され、フローのエクスポートは行われません。

Cflowd トラフィック フロー モニタリングは FNF と同等です。

Cflowd ソフトウェアは、*RFC 7011* および *RFC 7012* で指定されている Cflowd バージョン 10 を実装しています。Cflowd バージョン 10 は、IP Flow Information Export（IPFIX）プロトコルとも呼ばれます。



Cflowd は、1:1 のサンプリングを実行します。すべてのフローに関する情報が Cflowd レコードに集約されます。フローはサンプリングされません。Cisco IOS XE Catalyst SD-WAN デバイス はコレクタにエクスポートされるレコードをキャッシュしません。

（注） セキュア インターネット ゲートウェイ（SIG）トンネル上の NetFlow は、Cisco IOS XE Catalyst SD-WAN デバイス ではサポートされていません。

Cflowd と SNMP の比較

Cflowd は、サービス側のトラフィックをモニタリングします。Cflowd は主に、LAN から WAN、WAN から LAN、LAN から LAN、および DIA へのトラフィックをモニタリングします。Cflowd と SNMP を使用して LAN インターフェイス（入力または出力）のトラフィックをモニタリン

グする場合、パケット数とバイト数は類似するはずです。バイトの違いは、SNMP は L2 ヘッダーから始まりますが、Cflowd は L3 ヘッダーから始まります。ただし、Cflowd や SNMP を使用して WAN インターフェイス（入力または出力）のトラフィックをモニタリングする場合、パケットやバイトが同じになることはほぼありません。WAN インターフェイスのすべてのトラフィックは、サービス側のトラフィックではありません。たとえば、Cflowd は BFD トラフィックをモニタリングしませんが、SNMP はモニタリングします。Cflowd と SNMP のトラフィックのパケットまたはバイトは同じではありません。

ループバックを TLOC として使用する場合のフローテレメトリでの収集ループバックの有効化に関する制約事項

- Cisco Catalyst SD-WAN Controller CLI または Cisco SD-WAN Manager CLI テンプレートを介した設定のみをサポートします。機能テンプレートは、このリリースではサポートされていません。
- FNF VPN0 インターフェイスでの収集ループバックはサポートされていません。
- 専用インターネットアクセス（DIA）シナリオでの収集ループバックはサポートされていません。
- マルチテナントシナリオはサポートされていません。

Cisco IOS XE Catalyst SD-WAN デバイス のための IPFIX 情報要素

Cisco Catalyst SD-WAN Cflowd ソフトウェアは、次の IP Flow Information Export（IPFIX）情報要素を Cflowd コレクタにエクスポートします。フィールドは、使用しているリリースによって異なります。共通フィールドは、Cisco SD-WAN Manager および外部エクスポータにエクスポートされます。機能フィールドは Cisco SD-WAN Manager にのみエクスポートされます。

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以前の場合は、Flexible NetFlow がすべてのフィールドを外部コレクタと Cisco SD-WAN Manager にエクスポートします。Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降の場合は、FNF が次の表の要素（「対応」とマークされている要素）を外部コレクタと Cisco SD-WAN Manager の両方にエクスポートします。**drop cause id** などの他のフィールドは特定の機能用であり、これらのフィールドは Cisco SD-WAN Manager にのみエクスポートされ、外部コレクタにはエクスポートされません。

Information Element（情報要素）	Element ID	外部コレクタへのエクスポート	説明	データ タイプ	データ型セマンティクス	単位または範囲
sourceIPv4Address	8	対応	IP パケットヘッダー内の IPv4 送信元アドレス。	ipv4Address（4 バイト）	デフォルト	—

Information Element（情報要素）	Element ID	外部コレクタへのエクスポート	説明	データ タイプ	データ型セマンティクス	単位または範囲
sourceIPv6Address	27	対応	IP パケットヘッダー内の IPv6 送信元アドレス。	ipv6Address（16 バイト）	デフォルト	—
destinationIPv4Address	12	対応	IP パケットヘッダー内の IPv4 宛先アドレス。	IPv4Address（4 バイト）	デフォルト	—
destinationIPv6Address	28	対応	IP パケットヘッダー内の IPv6 宛先アドレス。	ipv6Address（16 バイト）	デフォルト	—
ingressInterface	10	対応	このフローのパケットが受信されている IP インターフェイスのインデックス。	unsigned32（4 バイト）	identifier	—
ipDiffServCodePoint	195	対応	[差別化サービス（Differentiated Services）] フィールドでエンコードされる Differentiated Services Code Point（DSCP; DiffServ コードポイント）の値。このフィールドは、IPv4 TOS フィールドの最上位 6 ビットにまたがります。	unsigned8（1 バイト）	identifier	0 ～ 63
protocolIdentifier	4	対応	IP パケットヘッダーのプロトコルフィールドにあるプロトコル番号の値。プロトコル番号は、IP パケットペイロードタイプを識別します。プロトコル番号は、IANA プロトコル番号レジストリで定義されています。	unsigned8（1 バイト）	identifier	—
sourceTransportPort	7	対応	トランスポートヘッダー内の送信元ポート ID。トランスポートプロトコル（UDP、TCP、および SCTP）の場合、これは、それぞれのヘッダーで指定されている宛先ポート番号です。GRE および IPsec フローの場合、このフィールドの値は 0 です。	unsigned16（2 バイト）	identifier	—

Information Element（情報要素）	Element ID	外部コレクタへのエクスポート	説明	データ タイプ	データ型セマンティクス	単位または範囲
destinationTransportPort	11	対応	トランスポートヘッダー内の宛先ポートID。トランスポートプロトコル（UDP、TCP、およびSCTP）の場合、これは、それぞれのヘッダーで指定されている宛先ポート番号です。	unsigned16（2 バイト）	identifier	—
tcpControlBits	6	対応	このフローのパケットに対して観測されるTCP制御ビット。この情報はビットフィールドとしてエンコードされます。TCP 制御ビットごとに、このセット内にビットがあります。このフローの観測されたいずれかのパケットで、対応する TCP 制御ビットが 1 に設定されている場合、このビットは 1 に設定されます。それ以外の場合、ビットは 0 に設定されます。このフィールドの値については、「*IANA IPFIX*」 Web ページを参照してください。	unsigned8（1 バイト）	identifier	—
flowEndReason	136	対応	フロー終了の理由。このフィールドの値については、「*IANA IPFIX*」 Web ページを参照してください。	unsigned8（1 バイト）	identifier	—
ingressoverlaysessionid	12432	対応	入力オーバーレイセッションIDの 32 ビット識別子。	unsigned32（4 バイト）	identifier	—
VPN 識別子	企業固有	対応	Cisco IOS XE Catalyst SD-WANデバイスVPN識別子デバイスはVIP_IANA_ENUM または 41916 のエンタープライズ ID を使用し、VPN 要素 ID は 4321 です。	unsigned32（4 バイト）	identifier	0 ～ 65535
connection id long	12441	対応	クライアントとサーバー間を接続するための64ビット識別子。	Unsigned64（8 バイト）	identifier	—

Information Element（情報要素）	Element ID	外部コレクタへのエクスポート	説明	データ タイプ	データ型セマンティクス	単位または範囲
application id	95	対応	アプリケーション名の32ビット識別子	unsigned32（4バイト）	identifier	—
egressInterface	14	対応	このフローのパケットが送信されているIPインターフェイスのインデックス。	unsigned32（4バイト）	デフォルト	—
egressoverlaysessionid	12433	対応	出力オーバーレイセッションIDの32ビット識別子。	unsigned32（4バイト）	identifier	—
sdwan qos-queue-id	12446	未対応	QoSのキューインデックス。	unsigned8（1バイト）	identifier	—
drop cause id	12442	未対応	ドロップ原因名の16ビット識別子。	unsigned16（2バイト）	identifier	—
counter bytes sdwan dropped long	12443	未対応	観測ポイントの計測プロセスが初期化または再初期化されて以降、観測ポイントにおけるこのフローの流入パケットのうちドロップしたオクテットの総数。 この数には、IPヘッドとIPペイロードが含まれます。	unsigned64（8バイト）	totalCounter	Octets
sdwan sla-not-met	12444	未対応	必要なSLAが満たされているかどうかを示すboolean値。	unsigned8（1バイト）	identifier	—
sdwan preferred-color-not-met	12445	未対応	優先色が満たされているかどうかを示すboolean値。	unsigned8（1バイト）	identifier	—
counter packets sdwan dropped long	42329	未対応	観測ポイントの計測プロセスが初期化または再初期化されて以降、観測ポイントにおけるこのフローの流入パケットのうちドロップしたパケットの総数。	unsigned64（8バイト）	totalCounter	パケット
octetDeltaCount	1	対応	観測ポイントにおけるこのフローの流入パケットにおける前回レポート以降のオクテットの数。この数には、IPヘッダーとIPペイロードが含まれます。	unsigned64（8バイト）	deltaCounter	Octets

Information Element（情報要素）	Element ID	外部コレクタへのエクスポート	説明	データ タイプ	データ型セマンティクス	単位または範囲
packetDeltaCount	2	対応	この観測ポイントにおけるこのフローに関する前回レポート以降の流入パケット数。	unsigned64（8 バイト）	deltaCounter	パケット
flowStartMilliseconds	152	対応	このフローの先頭パケットの絶対タイムスタンプ。	dateTime-MilliSeconds（8 バイト）	—	—
flowEndMilliseconds	153	対応	このフローの最終パケットの絶対タイムスタンプ。	dateTime-MilliSeconds（8 バイト）	—	—
ip tos	5	対応	IP ヘッダーの [タイプオブサービス（Type of Service）] フィールド。	unsigned8（1 バイト）	identifier	8 ビット
dscp output	98	対応	[差別化サービス（Differentiated Services）] フィールドでエンコードされる DSCP の値。このフィールドは、IPv4 TOS フィールドの最上位 6 ビットにまたがります。	unsigned8（1 バイト）	identifier	0 ～ 63
フロー サンプラ	48	対応	少なくとも 1 つの物理インターフェイスに適用される NetFlow サンプラマップで定義される特性のセット。	unsigned8（1 バイト）	identifier	—
bfd avg latency	45296	対応	各トンネルの Bidirectional Forwarding Detection（BFD）平均遅延の計算	unsigned64（8 バイト）	identifier	—
bfd avg loss	45295	対応	各トンネルの BFD 平均損失の計算	unsigned64（8 バイト）	identifier	—
bfd avg jitter	45297	対応	各トンネルの BFD 平均ジッターの計算	unsigned64（8 バイト）	identifier	—
bfd rx cnt	45299	対応	受信した BFD パケットの数	unsigned64（8 バイト）	deltaCounter	—
bfd tx cnt	45300	対応	送信された BFD パケットの数	unsigned64（8 バイト）	deltaCounter	—

Information Element（情報要素）	Element ID	外部コレクタへのエクスポート	説明	データ タイプ	データ型セマンティクス	単位または範囲
bfd rx octets	45304	対応	受信した BFD オクテットの数	unsigned64（8 バイト）	deltaCounter	—
bfd tx octets	45305	対応	送信された BFD オクテットの数	unsigned64（8 バイト）	deltaCounter	—
application_CATEGORY	12232	対応	アプリケーションカテゴリ名、各アプリケーションタグの第 1 レベルの分類	変数長	identifier	—
application_SUB_CATEGORY	12233	対応	アプリケーションサブカテゴリ名、各アプリケーションタグの第 2 レベルの分類	変数長	identifier	—
applicaiton_GROUP	12234	対応	アプリケーショングループ名。同じアプリケーションに属する複数のアプリケーションタグをグループ化したもの。	変数長	identifier	—
application traffic-class	12243	対応	SRND モデルに基づくアプリケーション トラフィック クラス	変数長	identifier	—
application business-relevance	12244	対応	ビジネス関連のアプリケーション	変数長	identifier	—

VPN0 インターフェイスに対する Flexible NetFlow

Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a から、Cisco IOS XE Catalyst SD-WAN デバイスの VPN0 インターフェイスで双方向トラフィックの可視性を確保するために FNF を有効にできます。

NetFlow は、デバイスを通過するパケットの統計情報を提供し、トンネルまたはサービス VPN の識別に役立ちます。VPN0 上の Flexible NetFlow は、Cisco IOS XE SD-WAN デバイス上の VPN0 に到達するすべてのトラフィック（入力と出力の両方）を可視化します。

プロファイルは、コンテキストに対して有効または無効にできる、事前定義された一連のトラフィックです。Easy Performance Monitor（ezPM）プロファイルを作成すると、モニターをすばやくプロビジョニングすることができます。この新しいメカニズムを利用すると、モニタのプロビジョニングに従来使用していた方法に影響を与えることなく新機能を導入することができます。この機能の一部として、**sdwan-fnf** プロファイルを作成して、NetFlow VPN0 設定を通過するトラフィックをモニタリングできます。

コンテキストは、インターフェイスの入力方向と出力方向の両方に付加される Performance Monitor ポリシー マップに相当します。コンテキストには、イネーブルにする必要があるトラフィック モニタに関する情報が含まれています。インターフェイスにコンテキストが付加されると 2 つのポリシーマップが作成され、入力方向と出力方向にそれぞれ 1 つずつ適用されます。トラフィック モニタで指定されている方向に基づいてポリシーマップが付加されるとトラフィックの監視が開始されます。コンテキストを編集して定義済みの方向を変更することもできます。

また、1 つのプロファイルをベースに、トラフィック モニタ、エクスポータ、パラメータなどを変更して、選択したトラフィック モニタごとに複数のコンテキストを作成することもできます。1 つの ezPM コンテキストを複数のインターフェイスに付加することもできます。1 つのインターフェイスにアタッチできるコンテキストは 1 つだけです。

表 *2 : Flexible NetFlow* のコンポーネント

	Cisco Catalyst SD-WAN Flexible Netflow	**Cisco vManage リリース 20.7.1 以降の Cisco SD-WAN NetFlow VPN0**
設定	ローカライズ型ポリシー：**app-visibility** または **flow-visibility** 一元管理型ポリシー：**cflowd** policy Cisco SD-WAN Manager 機能テンプレートと CLI テンプレートの両方でサポートされます。	コマンド **performance monitor context xxx profile s** を使用して Flexible NetFlow VPN0 モニターを定義 VPN0 インターフェイスにアタッチします。 Cisco SD-WAN Manager の CLI テンプレートおよ ン CLI 機能テンプレートでサポートされていま
インターフェイス	Cisco Catalyst SD-WAN トンネルインターフェイスおよびサービス VPN インターフェイス	Cisco Catalyst SD-WAN トンネルおよび VPN イン イスを除く VPN0 インターフェイス
フロー レコード	デフォルトでは固定レコード。 FEC、パケット複製、SSL プロキシなどのレコードの動的モニタリングをサポートします。また、一元管理型ポリシーのタイプオブサービス（ToS）、サンプラー ID、および再マークされた DSCP 値の収集もサポートします。	固定レコード。新しいフィールドを変更または ことはできません。
フローの方向	入力フローのみをサポート。	デフォルトで入力と出力の両方をサポートしま
アプリケーション用 NBAR	Network-Based Application Recognition（NBAR）は、**app-visibility** が定義されている場合にのみ有効になります。	NBAR はデフォルトで有効になっています。
エクスポータ	JSON ファイルを Cisco SD-WAN Manager に、IPFIX を外部コレクタにエクスポートします。	Cisco SD-WAN Manager にエクスポートできませ 外部コレクタへの IPFIX

VPN0 インターフェイスでの Flexible Netflow の制限

- VPN0 での Flexible NetFlow は Cisco Catalyst SD-WAN トンネルおよび Cisco Catalyst SD-WAN VPN インターフェイスでサポートされていません。
- VPN0 トラフィックの FNF レコードは固定レコードであり、変更できません。
- Cisco Catalyst SD-WANVPN0 フローエントリは、CLI 設定で定義された外部コレクタに報告されますが、Cisco SD-WAN Manager には報告されません。
- OMP、Netconf、SSH などの Cisco Catalyst SD-WAN BFD および Cisco Catalyst SD-WAN 制御接続は、Datagram Transport Layer Security（DTLS）または Transport Layer Security（TLS）トンネルによってカプセル化されます。FNF は DTLS トラフィックについてのみを報告し、カプセル化されたプロトコルパケットについては報告しません。
- VPN0 WAN インターフェイスに FNF が設定されている場合、
  - 入力フロー（WAN > Cisco Catalyst SD-WAN - トンネル > LAN）では、出力インターフェイスは NULL として報告されます。
  - 出力フロー（LAN > Cisco Catalyst SD-WAN - トンネル > WAN）では、入力インターフェイスは WAN インターフェイス（Cisco Catalyst SD-WAN アンダーレイトンネル）として報告されます。
- VPN0 モニターは、IPv4 および IPv6 プロトコルのみをサポートします。
- OSPF、BGP などのルーティングプロトコルについては、出力トラフィックのみがサポートされます。入力 OSPF および BGP トラフィックは、高プライオリティパケットとして扱われます。
- Cflowd フローエクスポートの送信元インターフェイスとしてサポートされるのは、ループバック インターフェイスのみです。
- FNF は、パケットが外部コレクタに送信されるときに、元の DSCP 値のみを記録します。FNF は入力フローのみをサポートします。

Flexible NetFlow 分散エクスポート

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1

Cisco IOS XE Catalyst SD-WAN デバイス で Flexible NetFlow 分散エクスポートを有効にする機能です。分散エクスポート機能は、モニターキャッシュ内のレコードのエクスポートを一定の時間間隔で分散して、コレクタのパフォーマンスを向上させます。同期キャッシュの場合、すべてのネットワークデバイスがモニターキャッシュ内のレコードを同時にエクスポートします。複数のネットワークデバイスに同じモニター間隔と同期キャッシュが設定されている場合、コレクタはすべてのデバイスからすべてのレコードを同時に受信することもあるため、そのパフォーマンスに影響が出る可能性があります。分散エクスポートの時間間隔を設定して、一定の時間間隔でエクスポートを分散させてください。

コレクタのパフォーマンスに影響が出ないようにするため、所定の時間間隔でレコードをエクスポートし、レコードのエクスポートをキャッシュタイムアウトの間、均等に分散させます。

FNF エクスポートはオプションテンプレートとデータテンプレートを使用して設定してください。システムレベルの属性を設定するには、オプションテンプレートを使します。フローレコードと対応するデータを設定するには、データテンプレートを使用します。

export-spread を有効化する場合は、次の 3 つの分散間隔を以下のように設定してください。

- **app-table**：application-table、application-attributes のオプションテンプレート
- **tloc-tables**：tunnel-tloc-table オプションテンプレート

  Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a と Cisco vManage リリース 20.10.1 で導入された bfd-metric-table は、tloc-table カテゴリに属します。
- **other-tables**：その他のオプションテンプレート

次に、分散間隔の仕組みについて例を示します。

- app-table が 10 の application-attributes または application-table で設定されている場合、オプション テンプレート パケットはすべての属性に対して 10 秒で均等に送信されます。
- デフォルトインターバルは1秒です。したがって、分散エクスポートでは、10秒の大きなトラフィックバースト 1 件が、それぞれ 1 秒の 小さなバースト10 件に分散されます。

Flexible NetFlow オプション テンプレート パケットは、timeout オプションで設定されたバーストとして定期的に送信されます。分散エクスポート間隔では、オプションテンプレートパケットをバーストとして送信する代わりに、パケットをタイムアウトおよび分散エクスポート間隔で分散させます。

Cisco vManage リリース 20.8.1 とそれ以前のリリースでは、60 秒ごとにオプション テンプレート パケットがバーストとして送信されます。たとえば、1000 個のパケットがある場合、60 秒経ったときに 1000 個すべてのパケットがキューに入れられるため、パケットがドロップされます。

分散エクスポートを設定すると、60秒経ったときに送信されるパケットが1000個ある場合に、100パケットを10秒で100パケットのレートで送信し、エクスポートバーストを回避します。エクスポートの展開が指定されない場合、デフォルトの動作は、即時エクスポートです。

分散エクスポートをサポートしていない以前のバージョンからアップグレードする場合、Cflowd テンプレートのデフォルトの分散値は無効になります。

Flexible NetFlow による BFD メトリックのエクスポート

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

Flexible NetFlow（FNF）による BFD メトリックのエクスポート機能を使用すると、BFD テレメトリデータを外部 FNF コレクタにエクスポートして、トンネルごとの平均ジッター、平均遅延、および損失を分析できます。ジッターと遅延はマイクロ秒単位で測定されます。損失

は、1% の 100 分の 1 単位（0.01%）で測定されます。この機能により、ネットワーク状態データのモニタリングが強化され、収集が高速化されます。

BFD メトリックのエクスポート用である新しいオプションテンプレート bfd-metric-table が追加されました。

Cisco SD-WAN Manager 機能テンプレートまたは Cisco SD-WAN コントローラ のCLI を使用して、Cisco IOS XE Catalyst SD-WAN デバイス で BFD メトリックのエクスポートを設定します。Cisco SD-WAN Manager 機能テンプレートを使用した BFD メトリックのエクスポートの設定の詳細については、「Configure Cflowd Monitoring Policy」を参照してください。CLI を使用した BFD メトリックのエクスポートの設定の詳細については、「Configure Flexible Netflow with Export of BFD Metrics Using the CLI」を参照してください。

BFD メトリックのエクスポートの仕組み

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

Cisco IOS XE Catalyst SD-WAN デバイス は、IP Flow Information Export（IPFIX）パケットを外部コレクタに送信するようになっています。Cisco SD-WAN コントローラ または Cisco SD-WAN Manager で BFD エクスポート間隔を設定すると、転送テーブルマネージャ（FTM）によって送信元メトリックが生成されます。

- 例 1：

  Cisco IOS XE Catalyst SD-WAN デバイス をリブートすると、デバイスは、設定した BFD エクスポート間隔に従って BFD メトリックをエクスポートします。この時点では、FTM にはエクスポートするデータがありません。その結果、[TLOC テーブルオーバーレイセッション ID（TLOC TABLE OVERLAY SESSION ID）] フィールドを除くすべてのフィールドに、次の無効な値が含まれることになります。

  0xFFFFFFFF

  例 2：

- データを送信するための FTM 間隔が BFD エクスポート間隔より大きくなっています。この状況では、FTM がデータを 1 回だけ送信しても、データが 2 回エクスポートされる可能性があります。結果的に、FTM から新しいデータを受信しないことになります。BFD メトリックとタイムスタンプは、最後のパケットと同じになります。

  外部コレクタに送信される BFD テレメトリデータの例については、「Flexible NetFlow による BFD メトリックのエクスポート設定例」を参照してください。

SAIE フローを使用した Cflowd トラフィック フロー モニタリング

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco vManage リリース 20.10.1

この機能を使用すると、Cflowd フローと SAIE フローの両方をモニタリングするための 2 つの Cisco SD-WAN Manager リアルタイム デバイス オプションを選択できます。

SAIE フローの詳細については、「SD-WAN Application Intelligence Engine Flow」の章を参照してください。

この機能を使用すると、選択した Cisco IOS XE Catalyst SD-WAN デバイス の VPN 内で実行されている特定のアプリケーションまたはアプリケーションファミリを表示するためのフィルタを適用できます。

Cflowd および SAIE フローのデバイス フィルタリング オプションの詳細については、『*Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*』の「Devices and Controllers」の章を参照してください。

SAIE フローを使用した Cflowd トラフィック フロー モニタリングの利点

- ネットワークトラフィックの可視性が向上し、ネットワークオペレータがネットワークの使用状況を分析し、ネットワークパフォーマンスを向上させることができます。
- Cisco IOS XE Catalyst SD-WAN デバイス のリアルタイムモニタリングを提供します。
- Cisco IOS XE Catalyst SD-WAN デバイス の Cisco SD-WAN Manager のリアルタイム デバイス オプションのパリティを提供します。

SAIE フローを使用した Cflowd トラフィック フロー モニタリングの前提条件

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco vManage リリース 20.10.1

Cflowd with SAIE フローデバイスオプションを表示する前に、アプリケーションとフローの可視性を設定します。

アプリケーションフローの可視性の設定の詳細については、アプリケーション可視性のグローバルな設定 （19 ページ） を参照してください。

グローバルフローの可視性の設定の詳細については、グローバルフローの可視性の設定 （17 ページ）を参照してください。

SAIE フローを使用した Cflowd トラフィック フロー モニタリングに関する制約事項

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco vManage リリース 20.10.1

- Cisco SD-WAN Manager で一度に表示できる Cflowd レコードは 4001 件のみです。
- 2 人の異なるユーザーが同じデバイスから同じクエリに同時にアクセスしようとした場合、Cisco IOS XE Catalyst SD-WAN デバイス が処理するのは、最初のリクエストのみです。2 番目のユーザーは、最初のリクエストがタイムアウトになるため、リクエストを再送信する必要があります。
- SAIE を使用した Cflowd の検索フィルタは、取得された 4001 Cflowd フローレコードと照合されます。

- 有効な結果を返せるよう、検索フィルタには、アプリケーションまたはアプリケーションファミリをフルネームで入力します。

  たとえば、**netbios-dgm** アプリケーションを検索する場合に、**アプリケーション**または**アプリケーションファミリ**に **netbios** と入力しても、正しい結果は表示されません。

Cisco IOS XE Catalyst SD-WAN デバイスでのトラフィック フロー モニタリングの設定

Cflowd トラフィック フローモニタリングでは、Flexible NetFlow（FNF）を使用してトラフィックデータをエクスポートします。Cflowd モニタリングを設定するには、次の手順を実行します。

グローバルフローの可視性の設定

LAN 内のすべての VPN からルータに着信するトラフィックのトラフィック フロー モニタリングを実行できるように、すべての Cisco IOS XE Catalyst SD-WAN デバイス で Cflowd の可視性をグローバルに有効にします。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [Localized Policy] をクリックします。
3. [Add Policy] をクリックします。
4. [次へ（Next）] をクリックして、[ポリシー概要（Policy Overview）]、[ポリシー設定（Policy Settings）] ページが表示されるまで、ウィザードページを進めます。
5. [ポリシー名（Policy Name）] と [ポリシーの説明（Policy Description）] を入力します。
6. **[Netflow]** チェックボックスをオンにして、IPv4 トラフィックのフローの可視性を有効にします。
7. **[Netflow IPv6]** チェックボックスをオンにして、IPv6 トラフィックのフローの可視性を有効にします。

（注） SAIE 可視性で Cflowd トラフィックフローを設定する前に、IPv4 および IPv6 トラフィックのフロー可視性を有効にします。

Cflowd および SAIE フローのモニタリングの詳細については、『*Cisco Catalyst SD-WANMonitor and Maintain Configuration Guide*』の「Devices and Controllers」の章を参照してください。

8. トラフィックでドロップされたパケットをログに記録するように Cisco IOS XE Catalyst SD-WAN デバイス を設定するには、[暗黙的なACLロギング（Implicit ACL Logging）] をオンにします。

この設定では、システムでリンク障害が発生した場合に、暗黙的なアクセス制御リスト（ACL）によってドロップされたパケットを可視化できます。

9. [ログ頻度（Log Frequency）] を入力します。

ログ頻度は、パケットフローがログに記録される頻度を決定します。最大値は2147483647です。最も近い2の累乗に切り捨てられます。たとえば、1000の場合、ロギング頻度は512です。したがって、フロー内の512番目のパケットごとにログが記録されます。

10. IPv4 トラフィックの FNF キャッシュサイズを設定するには、[FNF IPv4最大キャッシュエントリ（FNF IPv4 Max Cache Entries）] を入力します。

たとえば、次の例に示すように、IPv4/IPv6 トラフィックの FNF キャッシュを設定するには、100 と入力します。

11. IPv6 トラフィックの FNF キャッシュ サイズを設定するには、[FNF IPv6最大キャッシュエントリ（FNF IPv6 Max Cache Entries）] を入力します。

たとえば、次の例に示すように、IPv4/IPv6 トラフィックの FNF キャッシュを設定するには、100 と入力します。

（注） 最小キャッシュサイズ値は 16 です。合計キャッシュサイズ（IPv4 キャッシュ + IPv6 キャッシュ）の最大値は、各プラットフォームの制限を超えることはできません。キャッシュサイズが定義されておらず、プラットフォームがリストにない場合、デフォルトの最大キャッシュエントリは 200k です。

最大キャッシュエントリは、Cflowd がモニタリングできる最大同時フローです。最大キャッシュエントリは、プラットフォームによって異なります。詳細については、シスコサポートにお問い合わせください。

次に、IPv4 と IPv6 の両方の flow-visibility を設定する例を示します。

```
policy
    flow-visibility
    implicit-acl-logging
    log-frequency 1000
    flow-visibility-ipv6
    ip visibility cache entries 100
    ipv6 visibility cache entries 100
```

`policy flow-visibility` または `app-visibility` を実行して FNF モニターを有効にすると、グローバルメモリ割り当ての失敗を示す次の警告メッセージが表示される場合があります。このログは、大きなキャッシュサイズで FNF モニタリング（`policy flow-visibility` または `app-visibility`）を有効にするとトリガーされます。

```
Jul  4 01:45:00.255: %CPPEXMEM-3-NOMEM: F0/0: cpp_cp_svr: QFP: 0, GLOBAL memory allocation
 of 90120448 bytes by FNF failed
Jul  4 01:45:00.258: %CPPEXMEM-3-TOPUSER: F0/0: cpp_cp_svr: QFP: 0, Top User: CPR STILE
 EXMEM GRAPH, Allocations: 877, Type: GLOBAL
Jul  4 01:45:00.258: %CPPEXMEM-3-TOPUSER: F0/0: cpp_cp_svr: QFP: 0, Top User: SBC, Bytes
 Allocated: 53850112, Type: GLOBAL
```

警告メッセージは、必ずしもフロー モニター アプリケーションの障害を示しているわけではありません。警告メッセージは、外部メモリマネージャ（EXMEM）インフラストラクチャからメモリを適用するために FNF が使用する内部手順を示している可能性があります。

show platform hardware qfp active classification feature-manager exmem-usage コマンドを使用して、さまざまなクライアントの EXMEM メモリ使用率を表示します。

```
Device# show platform hardware qfp active active classification feature-manager exmem-usage

EXMEM Usage Information

Total exmem used by CACE: 39668

Client       Id   Total VMR     Total Usage   Total%   Alloc     Free
-------------------------------------------------------------------------
acl           0      11           2456          6         88       84
qos           2     205          31512         79          7        5
fw            4       8            892          2          2        1
obj-group    39      82           4808         12          5        2
```

FNF モニターが正常に有効になっていることを確認するには、**show flow monitor** *monitor-name* コマンドを使用して、フローモニターのステータス（`allocated` または `not allocated`）を確認します。

```
Device# show flow monitor sdwan_flow_monitor
Flow Monitor sdwan_flow_monitor:
  Description:       monitor flows for vManage and external collectors
  Flow Record:       sdwan_flow_record-003
  Flow Exporter:     sdwan_flow_exporter_1
                     sdwan_flow_exporter_0
  Cache:
    Type:                 normal (Platform cache)
    Status:               allocated
    Size:                 250000 entries
    Inactive Timeout:     10 secs
    Active Timeout:       60 secs

    Trans end aging:   off

SUCCESS
   Status:            allocated
FAILURE
   Status:            not allocated
```

アプリケーション可視性のグローバルな設定

LAN 内のすべての VPN からルータに着信するトラフィックのトラフィック フロー モニタリングを実行できるように、すべての Cisco IOS XE Catalyst SD-WAN デバイス で Cflowd の可視性をグローバルに有効にします。

`app-visibility`により、`nbar` は、LAN 内のすべての VPN からルータに着信するフローの各アプリケーションを確認できます。`app-visibility` または `app-visibility-ipv6` が定義されている場合、`nbar` は IPv4 と IPv6 の両方のフローに対してグローバルに有効になります。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [Localized Policy] をクリックします。

3. [Add Policy] をクリックします。
4. [次へ（Next）] をクリックして、[ポリシー概要（Policy Overview）]、[ポリシー設定（Policy Settings）] ページが表示されるまで、ウィザードページを進めます。
5. [ポリシー名（Policy Name）] と [ポリシーの説明（Policy Description）] を入力します。
6. [アプリケーション（Application）] チェックボックスをオンにして、IPv4 トラフィックのアプリケーションの可視性を有効にします。
7. [アプリケーション IPv6（Application IPv6）] チェックボックスをオンにして、IPv6 トラフィックのアプリケーションの可視性を有効にします。

（注） SAIE 可視性で Cflowd トラフィックフローを設定する前に、IPv4 および IPv6 トラフィックのアプリケーション可視性を有効にします。

Cflowd および SAIE フローのモニタリングの詳細については、『*Cisco Catalyst SD-WANMonitor and Maintain Configuration Guide*』の「Devices and Controllers」の章を参照してください。

8. IPv4 トラフィックの FNF キャッシュサイズを設定するには、[FNF IPv4最大キャッシュエントリ（FNF IPv4 Max Cache Entries）] を入力します。

   たとえば、IPv4 トラフィックの FNF キャッシュサイズを設定するには、次の例に示すように 100 と入力します。
9. IPv6 トラフィックの FNF キャッシュ サイズを設定するには、[FNF IPv6最大キャッシュエントリ（FNF IPv6 Max Cache Entries）] を入力します。

   たとえば、IPv6 トラフィックの FNF キャッシュサイズを設定するには、次の例に示すように 100 と入力します。

次の例は、IPv4 と IPv6 の両方に対する application visibility の設定を示しています。

```
policy
 app-visibility


 app-visibility-ipv6
 ip visibility cache entries 100
 ipv6 visibility cache entries 100
!
```

（注） **policy app-visibility** コマンドは、**nbar** を有効にしてアプリケーション名を取得することで、グローバルフローの可視性も有効にします。

（注） Cflowd global `flow-visibility` を設定しても、Cflowd `app-visibility` を設定していない場合、Cisco SD-WAN Managerにエクスポートされたアプリケーションは不明という結果を返します。IPFIXアナライザを使用して外部コレクタにエクスポートされた同じアプリケーションに、誤ったアプリケーション名が含まれている可能性があります。

アプリケーション名を保持する場合は、Cflowd `app-visibility` を定義してこの問題を回避します。

Cflowd モニタリングポリシーの設定

Cflowd トラフィック フロー モニタリングのポリシーを設定するには、Cisco SD-WAN Manager ポリシー構成ウィザードを使用します。このウィザードは、4連続のページ構成となっており、これに従って操作を進めていくと、次のようなポリシーコンポーネントの作成および編集ができます。

1. [アプリケーションまたは対象グループの作成（Create Applications or Groups of Interest）]：関連する項目をグループ化し、ポリシーのマッチやアクションコンポーネントで呼び出すリストを作成します。
2. [トポロジの設定（Configure Topology）]：ポリシーが適用されるネットワーク構造を作成します。
3. [トラフィックルールの設定（Configure Traffic Rules）]：ポリシーのマッチ条件とアクション条件を作成します。
4. [サイトとVPNにポリシーを適用（Apply Policies to Sites and VPNs）]：ポリシーをオーバーレイネットワークのサイトと VPN に関連付けます。

ポリシー構成ウィザードの最初の3ページで、ポリシーコンポーネント、つまりブロックを作成します。最後のページで、オーバーレイネットワークのサイトと VPN にポリシーブロックを適用します。Cflowd ポリシーを有効にするには、ポリシーをアクティブ化します。

1. Cisco SD-WAN Manager メニューから、**[設定（Configuration）]** > **[ポリシー（Policies）]** の順に選択します。
2. [カスタムオプション（Custom Options）] をクリックします。
3. [一元管理型ポリシー（Centralized Policy）] で、[トラフィックポリシー（Traffic Policy）] をクリックします。
4. **[Cflowd]** をクリックします。
5. [ポリシーの追加（Add Policy）] をクリックしてから、[新規作成（Create New）] をクリックします。
6. 新しいポリシーの名前と説明を [名前（Name）] と [説明（Description）] に入力します。

7. [Cflowd テンプレート（Cflowd Template）] セクションで、アクティブフローのタイムアウト範囲を [アクティブフロータイムアウト（Active Flow Timeout）] に入力します。
8. [非アクティブフロータイムアウト（Inactive Flow Timeout）] フィールドに、非アクティブフローのタイムアウト範囲を入力します。
9. [フローの更新（Flow Refresh）] フィールドに、フローの更新間隔を入力します。
10. [サンプリング間隔（Sampling Interval）] フィールドに、サンプル期間を入力します。
11. [プロトコル（Protocol）] ドロップダウンリストで、オプションを選択します。

    Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a および Cisco vManage リリース 20.6.1 以降では、オプションから [IPv4] または [両方（Both）] を選択すると、[詳細設定（Advanced Settings）] フィールドが表示されます。
12. [詳細設定（Advanced Settings）] で次の手順を実行して、追加の IPv4 フローレコードを収集します。
    - **[TOS]** チェックボックスをオンにします。
    - [DSCPのリマーク（Re-marked DSCP）] チェックボックスをオンにします。
13. [コレクタリスト（Collector List）] で [新しいコレクタ（New Collector）] をクリックします。コレクタは最大 4 つまで設定できます。
    1. **[VPN ID]** フィールドには、コレクタが配置されている VPN の番号を入力します。
    2. [IPアドレス（IP Address）] フィールドには、コレクタの IP アドレスを入力します。
    3. [ポート（Port）] フィールドには、コレクタのポート番号を入力します。
    4. [トランスポートプロトコル（Transport Protocol）] ドロップダウンリストでは、コレクタに到達するために使用するトランスポートタイプを選択します。
    5. [送信元インターフェイス（Source Interface）] フィールドに、フローをコレクタに送信するために使用するインターフェイスの名前を入力します。
    6. [分散エクスポート（Export Spreading）] フィールドにある、[有効（Enable）] または [無効（Disable）] オプションボタンをクリックします。

       Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降では、[分散エクスポート（Export Spreading）] フィールドを使用して、キャッシュの同期化によって発生するエクスポートストームを防ぐことができます。直前の間隔でのエクスポートが現在の間隔中に展開されることにより、エクスポート ストームが回避されます。
    7. [BFDメトリックのエクスポート（BFD Metrics Exporting）] フィールドにある、[有効（Enable）] または [無効（Disable）] オプションボタンをクリックします。

       Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco vManage リリース 20.10.1 以降では、[BFDメトリックのエクスポート（BFD Metrics Exporting）] フィールドを使用して、損失、ジッター、および遅延の BFD メトリックを収集できます。

8. [エクスポート間隔（Exporting Interval）] フィールドで、BFD メトリックを送信する間隔を秒単位で指定します。

   Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco vManage リリース 20.10.1 以降では、[エクスポート間隔（Exporting Interval）] フィールドを使用して、BFD メトリックのエクスポート間隔を指定できます。

   BFD メトリックのエクスポートを有効にすると、[エクスポート間隔（Exporting Interval）] フィールドが表示されます。

   [エクスポート間隔（Exporting Interval）] フィールドにより、BFD メトリックが送信される間隔が制御されます。

   デフォルトの BFD エクスポート間隔は 600 秒です。

フィールド	説明
[Cflowd ポリシー名（Cflowd Policy Name）]	Cflowd ポリシーの名前を入力します。
説明	Cflowd ポリシーの説明を入力します。
[アクティブ フロータイムアウト（Active Flow Timeout）]	アクティブフローのタイムアウト値を入力します。指定できる範囲は 30 ～ 3600 秒です。
[非アクティブフロータイムアウト（Inactive Flow Timeout）]	非アクティブフローのタイムアウト値を入力します。指定できる範囲は 1 ～ 3600 秒です。
[フローの更新（Flow Refresh）]	Cflowd レコードを外部コレクタに送信する間隔を入力します。指定できる範囲は 60 ～ 86400 秒です。
Sampling Interval	サンプル期間を入力します。指定できる範囲は 1 ～ 65536 秒です。
Protocol	ドロップダウンリストからトラフィックプロトコルのタイプを選択します。オプションは、[IPv4]、[IPv6]、または [両方（Both）] です。 デフォルトのプロトコルは **[IPv4]** です。
TOS	**[TOS]** チェックボックスをオンにします。 こうすることで、IPv4 ヘッダーのフィールドタイプが示されます。
[DSCPのリマーク（Re-marked DSCP）]	[DSCPのリマーク（Re-marked DSCP）] チェックボックスをオンにします。 こうすることで、リマークされたデータポリシーによって指定されたトラフィック出力が示されます。

フィールド	説明
VPN ID	VPN ID を入力します。指定できる範囲は 0 ～ 65536 です。
IP Address	コレクタの IP アドレスを入力します。
Port	コレクタのポート番号を入力します。指定できる範囲は 1024 ～ 65535 です。
トランスポート プロトコル	ドロップダウンリストから、コレクタに到達するためのトランスポートタイプを選択します。 オプションは、**[TCP]** または **[UDP]** です。
Source Interface	ドロップダウンリストから送信元インターフェイスを選択します。
分散エクスポート	[有効（Enable）] または [無効（Disable）] オプションボタンをクリックして、分散エクスポートを設定します。 デフォルトは [無効（Disable）] です。
[BFD メトリックのエクスポート（BFD Metrics Exporting）]	[有効（Enable）] または [無効（Disable）] オプションボタンをクリックして、Bidirectional Forwarding Detection（BFD）メトリックのエクスポートを設定します。 デフォルトは [無効（Disable）] です。
[エクスポート間隔（Exporting Interval）]	BFD メトリックを外部コレクタに送信するエクスポート間隔を秒単位で入力します。整数値を入力してください。 このフィールドは、BFD メトリックのエクスポートを有効にした場合にのみ表示されます。 デフォルトの BFD エクスポート間隔は 600 秒です。

14. [Cflowdポリシーの保存（Save Cflowd Policy）] をクリックします。

Cflowd 情報の表示

Cflowd の情報を表示するには、Cisco IOS XE Catalyst SD-WAN デバイス で次のコマンドを使用します。

- show sdwan app-fwd cflowd collector
- show sdwan app-fwd cflowd flow-count
- show sdwan app-fwd cflowd flows [vpn *vpn-id*] format table
- show sdwan app-fwd cflowd statistics
- show sdwan app-fwd cflowd template [name *template-name*]

- show sdwan app-fwd cflowd flows format table

次の出力例は、Cflowd の情報を表示したものです。

```
Device# show sdwan app-fwd cflowd flows
Generating output, this might take time, please wait ...
app-fwd cflowd flows vpn 1 src-ip 10.2.2.11 dest-ip 10.20.24.17 src-port 0 dest-port
2048 dscp 63 ip-proto 1
 tcp-cntrl-bits           0
 icmp-opcode              2048
 total-pkts               6
 total-bytes              600
 start-time               "Fri May 14 02:57:23 2021"
 egress-intf-name         GigabitEthernet5
 ingress-intf-name        GigabitEthernet1
 application              unknown
 family                   network-service
 drop-cause               "No Drop"
 drop-octets              0
 drop-packets             0
 sla-not-met              0
 color-not-met            0
 queue-id                 2
 tos                      255
 dscp-output              63
 sampler-id               3
 fec-d-pkts               0
 fec-r-pkts               0
 pkt-dup-d-pkts-orig      0
 pkt-dup-d-pkts-dup       0
 pkt-dup-r-pkts           0
 pkt-cxp-d-pkts           0
 traffic-category         0
```

Cflowd フローの詳細については、**show sdwan app-fwd cflowd flows** コマンドページを参照してください。

CLI を使用した、Cflowd トラフィック フロー モニタリングの設定

Cisco IOS XE Catalyst SD-WAN デバイス を制御している Cisco SD-WAN コントローラ の CLI から、次の手順を実行します。

1. Cflowdテンプレートを設定して、フローの可視性とフローのサンプリングパラメータを指定します。

```
vSmart(config)# policy cflowd-template template-name
 vSmart(config-cflowd-template)#  flow-active-timeout seconds
 vSmart(config-cflowd-template)#  flow-inactive-timeout seconds
 vSmart(config-cflowd-template)#  flow-sampling-interval number
 vSmart(config-cflowd-template)#  template-refresh seconds
 vSmart(config-cflowd-template)#  protocol ipv4|ipv6|Both
```

2. フローモニターで TOS、DSCP 出力、および TLOC ループバックを収集するには、次の手順を実行します。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降、ループバック インターフェイスを入力または出力トランスポート インターフェイスとして設定すると、この機能により、FNF レコードの物理インターフェイスの代わりにループバックを収集できるようになりました。この機能は、IPv4 および IPv6 でサポートされています。

```
vSmart(config-cflowd-template)# customized-ipv4-record-fields
vsmart(config-customized-ipv4-record-fields)# collect-tos
vsmart(config-customized-ipv4-record-fields)# collect-dscp-output
vSmart(config-cflowd-template)#  collect-tloc-loopback
```

3. フローコレクタを設定します。

```
vSmart(config-cflowd-template)# collector vpn vpn-id address
ip-address port port-number transport transport-type
source-interface interface-name
export-spread
enable
app-tables app-tables
tloc-tables tloc-tables
other-tablesother-tables
```

（注） app-tables、tloc-tables、other-tables オプションは、Cisco SD-WAN コントローラ を使用してのみ設定できます。

（注） Cisco IOS XE Catalyst SD-WAN デバイス は UDP コレクタのみをサポートします。設定されているトランスポートプロトコルに関係なく、UDP は Cisco IOS XE Catalyst SD-WAN デバイスのデフォルトコレクタです。

4. トラフィックマ ッチ パラメータを定義し、アクション **cflowd** を含むデータポリシーを設定します。

```
vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy)# sequence number
vSmart(config-sequence)# match match-parameters
vSmart(config-sequence)# action cflowd
```

5. トラフィック フロー モニタリング ポリシーを適用する Cisco IOS XE Catalyst SD-WAN デバイスを含むオーバーレイネットワーク内のサイトのリストを作成します。リストに複数のサイトを含めるには、複数の **vpn** *vpn-id* コマンドを設定します。

```
vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-vpn-list)# vpn vpn-id
```

6. Cisco IOS XE Catalyst SD-WAN デバイス を含むオーバーレイネットワーク内のサイトにデータポリシーを適用します。

```
vSmart(config)# apply-policy site-list list-name
vSmart(config-site-list)# data-policy policy-name
vSmart(config-site-list)# cflowd-template template-name
```

収集ループバックの確認

次のコマンドを使用して、入力および出力インターフェイスの出力を確認できます。

show sdwan app-fwd cflowd flows

次に、**show sdwan app-fwd cflowd flows** で**flows** キーワードを指定した場合の出力例を示します。

```
Device#show sdwan app-fwd cflowd flows
app-fwd cflowd flows vpn 1 src-ip 10.10.15.12 dest-ip 10.20.15.12 src-port 0 dest-port
0 dscp 0 ip-proto 1
 tcp-cntrl-bits           24
 icmp-opcode              0
 total-pkts               5
 total-bytes              500
 start-time               "Tue Jun 27 09:21:09 2023"
 egress-intf-name         Loopback1
 ingress-intf-name        GigabitEthernet5
 application              ping
 family                   network-service
 drop-cause               "No Drop"
 drop-octets              0
 drop-packets             0
 sla-not-met              0
 color-not-met            0
 queue-id                 2
 initiator                2
 tos                      0
 dscp-output              0
 sampler-id               0
 fec-d-pkts               0
 fec-r-pkts               0
 pkt-dup-d-pkts-orig      0
 pkt-dup-d-pkts-dup       0
 pkt-dup-r-pkts           0
 pkt-cxp-d-pkts           0
 category                 0
 service-area             0
 cxp-path-type            0
 region-id                0
 ssl-read-bytes           0
 ssl-written-bytes        0
 ssl-en-read-bytes        0
 ssl-en-written-bytes     0
 ssl-de-read-bytes        0
 ssl-de-written-bytes     0
 ssl-service-type         0
 ssl-traffic-type         0
 ssl-policy-action        0
 appqoe-action            0
 appqoe-sn-ip             0.0.0.0
 appqoe-pass-reason       0
 appqoe-dre-input-bytes   0
 appqoe-dre-input-packets 0
 appqoe-flags             0
```

次のコマンドを使用して、入力および出力インターフェイスの出力を確認できます。

show sdwan app-fwd cflowd table

次に、**show sdwan app-fwd cflowd table** で**table** キーワードを指定した場合の出力例を示します。

```
show sdwan app-fwd cflowd flows table
PKT    PKT    PKT   PKT                                                                  SSL
    SSL                                                                               APPQOE  APPQOE

                                                                                                TCP

                                                                                 SLA  COLOR
                              FEC   FEC   DUP D  DUP D  DUP   CXP                          CXP
          SSL    SSL       EN     SSL EN   DE     SSL DE   SSL      SSL      SSL
              APPQOE  DRE     DRE
                                                                 SRC    DEST         IP     CNTRL
  ICMP    TOTAL  TOTAL                                    EGRESS INTF       INGRESS INTF
                                                      DROP    DROP     NOT  NOT    QUEUE
           DSCP    SAMPLER  D     R      PKTS   PKTS   R     D               SERVICE
PATH  REGION  READ   WRITTEN  READ   WRITTEN  READ   WRITTEN  SERVICE  TRAFFIC  POLICY
 APPQOE  APPQOE   PASS    INPUT   INPUT    APPQOE
VPN  SRC IP                  DEST IP                 PORT   PORT   DSCP  PROTO  BITS
  OPCODE  PKTS   BYTES   START TIME                NAME              NAME
APPLICATION  FAMILY            DROP CAUSE   OCTETS  PACKETS  MET  MET    ID     INITIATOR
  TOS  OUTPUT  ID       PKTS  PKTS  ORIG   DUP    PKTS  PKTS  CATEGORY  AREA     TYPE
ID      BYTES  BYTES    BYTES  BYTES    BYTES  BYTES    TYPE     TYPE     ACTION  ACTION
  SN IP    REASON  BYTES   PACKETS  FLAGS
----------------
1    10.10.15.11             10.20.20.10             0      0      0     1      24
  0       5      500     Tue Jun 27 09:21:06 2023  Loopback1         GigabitEthernet5
ping         network-service     No Drop      0       0        0    0      2      2
      0    0       0        0     0     0      0      0     0     0         0        0
    0       0      0        0      0        0      0        0        0        0       0
       0.0.0.0  0       0       0        0
0    10.0.5.5                10.0.15.10               58048  22     4     6      24
   0       41     1752    Tue Jun 27 09:21:06 2023  internal0/0/rp:0  GigabitEthernet9
 unknown      network-service     No Drop      0       0        0    0      2      0
       0    0       0        0     0     0      0      0     0     0         0        0
     0       0      0        0      0        0      0        0        0        0
0       0.0.0.0  0       0       0        0
1    10.10.15.11             10.20.20.10             0      2048   0     1      24
  2048    5      500     Tue Jun 27 09:21:06 2023  GigabitEthernet5  Loopback1
ping         network-service     No Drop      0       0        0    0      2      2
      0    0       0        0     0     0      0      0     0     0         0        0
    0       0      0        0      0        0      0        0        0        0       0
       0.0.0.0  0       0       0        0
1    10.10.15.11             10.5.10.15              0      2048   0     1      31
  2048    20     960     Tue Jun 27 09:21:06 2023  Null              GigabitEthernet5
ping         network-service     Ipv4NoRoute  960     20       0    0      2      2
      0    0       0        0     0     0      0      0     0     0         0        0
    0       0      0        0      0        0      0        0        0        0       0
       0.0.0.0  0       0       0        0
1    10.10.15.11             10.20.20.10             50920  4739   0     17     31
  0       473    524768  Tue Jun 27 09:21:06 2023  GigabitEthernet5  internal0/0/rp:0
ipfix        network-management  No Drop      0       0        0    0      2      1
      0    0       0        0     0     0      0      0     0     0         0        0
    0       0      0        0      0        0      0        0        0        0       0
       0.0.0.0  0       0       0        0
0    10.0.5.10               10.0.5.10                22     58048  48    6      24
   0       39     3020    Tue Jun 27 09:21:05 2023  GigabitEthernet9  internal0/0/rp:0
 ssh          terminal            No Drop      0       0        0    0      2      2
       0    0       0        0     0     0      0      0     0     0         0        0
```

```
     0       0      0        0      0        0      0        0        0        0
0       0.0.0.0  0       0       0        0
1    10.10.15.11              10.20.20.10              0      771    48    1      31
  771     8      4192    Tue Jun 27 09:21:05 2023  internal0/0/rp:0  GigabitEthernet5
icmp         network-service     No Drop      0       0        0    0      2      2
      0    0       0        0     0     0      0      0     0     0         0        0
    0       0      0        0      0        0      0      0        0        0       0
       0.0.0.0  0       0       0        0
1    fe40::6044:ff:feb7:c2db  ff01::1:ff00:10          0      34560  0     58     0
  34560   6      432     Tue Jun 27 09:20:41 2023  internal0/0/rp:0  GigabitEthernet5
ipv6-icmp    network-service     No Drop      0       0        0    0      0      2
      0    0       0        0     0     0      0      0     0     0         0        0
    0       0      0        0      0        0      0      0        0        0       0
       0.0.0.0  0       0       0        0
1    10:20:20::10             fe40::6024:ff:feb6:c1db  0      34816  56    58     0
  34816   4      288     Tue Jun 27 09:20:41 2023  GigabitEthernet5  internal0/0/rp:0
ipv6-icmp    network-service     No Drop      0       0        0    0      2      2
      0    0       0        0     0     0      0      0     0     0         0        0
    0       0      0        0      0        0      0      0        0        0       0
       0.0.0.0  0       0       0        0
```

デバイスのインターフェイスバインドの確認

次のコマンドを使用してデバイスのインターフェイスバインドを確認することができます。

show sdwan control local-properties wan-interface-list

次に、**wan-interface-list** キーワードを使用した **show sdwan control local-properties wan-interface-list** の出力例を示します。

コマンドは次を表示します。

- バインドモードでループバック WAN インターフェイスにバインドされた物理インターフェイス。
- バインド解除モードでのループバック WAN インターフェイスのバインド解除。
- その他の場合は該当なし。

```
Device#show sdwan control local-properties wan-interface-list
 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                          PUBLIC          PUBLIC PRIVATE         PRIVATE
                  PRIVATE
MAX   RESTRICT/           LAST         SPI TIME    NAT  VM          BIND
INTERFACE                 IPv4           PORT   IPv4            IPv6
                  PORT    VS/VM COLOR            STATE
CNTRL CONTROL/     LR/LB  CONNECTION   REMAINING   TYPE CON REG     INTERFACE

                                                          STUN
                       PRF IDs
-------------------------------------------------------------------------------
GigabitEthernet1             10.0.10.10      12346  10.0.10.10      ::
                     12346    2/1  lte              up     2      no/yes/no   No/No
0:20:20:27   0:01:14:20  N    5  Default N/A
GigabitEthernet4             10.0.10.10      12346  10.0.10.10      ::
```

```
                     12346    2/0  blue              up      2       no/yes/no   No/No
0:20:20:27   0:01:14:20  N    5  Default N/A
Loopback1                     1.1.1.1         12366  1.1.1.1          ::
                     12366    2/0  custom1           up      2       no/yes/no   No/No
0:20:20:27   0:01:14:20  N    5  Default GigabitEthernet1
Loopback2                     2.2.2.2         12406  2.2.2.2          ::
                     12406    2/0  custom2           up      2       no/yes/no   No/No
0:20:20:27   0:01:14:20  N    5  Default Unbind
```

VPN0 インターフェイスでの Flexible NetFlow の設定

CLI テンプレートまたは CLI アドオンテンプレートを使用して、VPN0 インターフェイスで FNF を有効にできます。ezPM プロファイルは、すべての NetFlow VPN0 モニター設定を伝送する新しいプロファイルを作成するのに役立ちます。プロファイルを選択していくつかのパラメータを指定するだけで、残りのプロビジョニング情報は ezPM により自動的に設定されます。プロファイルは、コンテキストに対して有効または無効にできる、事前定義された一連のトラフィックモニターです。Easy Performance Monitor（ezPM）を設定し、次のように FNF を有効にすることができます。

```
Device# config-transaction
Device(config)# performance monitor context <monitor_name> profile <sdwan-fnf>
traffic-monitor <all> [ipv4/ipv6]
Device(config-perf-mon)# exporter destination <destination address> source <source
interface> transport udp vrf <vrf-name> port <port-number> dscp <dscp>
```

次の例は、sdwan-fnf プロファイルを使用してパフォーマンスモニターのコンテキストを設定する方法を示しています。この設定により、トラフィックメトリックのモニタリングが有効になります。ここで、10.1.1.1 はサードパーティ製コレクタの IP アドレス、GigabitEthernet5 は送信元インターフェイス、4739 はサードパーティ製コレクタのリスニングポートです。

```
Device# config-transaction
Device(config)# performance monitor context <monitor_name> profile sdwan-fnf
traffic-monitor all [ipv4/ipv6]
Device(config-perf-mon)# exporter destination <10.1.1.1> source <GigabitEthernet5>
transport udp vrf <vrf1> port <4739> dscp <1>
```

VPN0 インターフェイスでの Flexible NetFlow 設定の確認

Flexible NetFlow レコード設定の概要の表示

次のコマンドを使用して、FNF レコードの設定を確認できます。

```
Device# show flow record <monitor-context-name>
```

（注） 次の例では、temp0 というモニター名が使われます。

次の出力例は、ezPM プロファイルを使用した IPv4 トラフィックフローレコードに関する情報を示しています。

```
Device# show flow record temp0-sdwan-fnf-vpn0-monitor_ipv4
flow record temp0-sdwan-fnf-vpn0-monitor_ipv4:
  Description:        ezPM record
  No. of users:       1
  Total field space:  66 bytes
  Fields:
    match ipv4 dscp
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match flow direction
    collect routing next-hop address ipv4
    collect transport tcp flags
    collect interface input
    collect interface output
    collect flow sampler
    collect counter bytes long
    collect counter packets long
    collect timestamp absolute first
    collect timestamp absolute last
    collect application name
    collect flow end-reason
```

次の出力例は、ezPM プロファイルを使用した IPv6 トラフィックフローレコードに関する情報を示しています。

```
Device# show flow record temp0-sdwan-fnf-vpn0-monitor_ipv6

  flow record temp0-sdwan-fnf-vpn0-monitor_ipv6:
  Description:        ezPM record
  No. of users:       1
  Total field space:  102 bytes
  Fields:
    match ipv6 dscp
    match ipv6 protocol
    match ipv6 source address
    match ipv6 destination address
    match transport source-port
    match transport destination-port
    match flow direction
    collect routing next-hop address ipv6
    collect transport tcp flags
    collect interface input
    collect interface output
    collect flow sampler
    collect counter bytes long
    collect counter packets long
    collect timestamp absolute first
    collect timestamp absolute last
    collect application name
    collect flow end-reason
```

次の出力例は、ezPM プロファイルを使用した IPv4 トラフィックの NetFlow 設定に関するモニター情報を示しています。

```
Device# show flow monitor temp0-sdwan-fnf-vpn0-monitor_ipv4
Flow Monitor temp0-sdwan-fnf-vpn0-monitor_ipv4:
  Description:       ezPM monitor
  Flow Record:       temp0-sdwan-fnf-vpn0-monitor_ipv4
  Cache:
    Type:                normal (Platform cache)
    Status:              allocated
    Size:                5000 entries
    Inactive Timeout:    10 secs
    Active Timeout:      60 secs

    Trans end aging:   off
```

次の出力例は、ezPM プロファイルを使用した IPv6 トラフィックの NetFlow 設定に関するモニター情報を示しています。

```
Device# show flow monitor temp0-sdwan-fnf-vpn0-monitor_ipv6
Flow Monitor temp0-sdwan-fnf-vpn0-monitor_ipv6:
  Description:       ezPM monitor
  Flow Record:       temp0-sdwan-fnf-vpn0-monitor_ipv6
  Cache:
    Type:                normal (Platform cache)
    Status:              allocated
    Size:                5000 entries
    Inactive Timeout:    10 secs
    Active Timeout:      60 secs

    Trans end aging:   off
```

フローレコードキャッシュの表示

次の出力例は、指定したモニター（この場合は temp0-sdwan-fnf-vpn0-monitor_ipv4）のフローレコードキャッシュを示しています。

```
Device# show flow monitor temp0-sdwan-fnf-vpn0-monitor_ipv4 cache
Cache type:                               Normal (Platform cache)
  Cache size:                                 5000
  Current entries:                              14
  High Watermark:                               14

  Flows added:                                 170
  Flows aged:                                  156
    - Active timeout      (    60 secs)       156

IPV4 SOURCE ADDRESS:       10.0.0.0
IPV4 DESTINATION ADDRESS:  10.255.255.254
TRNS SOURCE PORT:          0
TRNS DESTINATION PORT:     0
FLOW DIRECTION:            Input
IP DSCP:                   0x00
IP PROTOCOL:               1
ipv4 next hop address:     10.0.0.1
tcp flags:                 0x00
interface input:           Gi1
interface output:          Gi2
flow sampler id:           0
counter bytes long:        840
counter packets long:      10
timestamp abs first:       02:55:24.359
```

```
timestamp abs last:        02:55:33.446
flow end reason:           Not determined
application name:          layer7 ping
……
```

次の出力例は、指定した IPv6 モニター（temp0-sdwan-fnf-vpn0-monitor_ipv6）のフローレコードキャッシュを示しています。

```
Device# show flow monitor temp0-sdwan-fnf-vpn0-monitor_ipv6 cache
Cache type:                                 Normal (Platform cache)
  Cache size:                                   5000
  Current entries:                                 6
  High Watermark:                                  6

  Flows added:                                    10
  Flows aged:                                      4
    - Inactive timeout    (    10 secs)          4

IPV6 SOURCE ADDRESS:       2001:DB8::/32
IPV6 DESTINATION ADDRESS:  2001:DB8::1
TRNS SOURCE PORT:          0
TRNS DESTINATION PORT:     32768
FLOW DIRECTION:            Output
IP DSCP:                   0x00
IP PROTOCOL:               58
ipv6 next hop address:     2001:DB8:1::1
tcp flags:                 0x00
interface input:           Gi2
interface output:          Gi1
flow sampler id:           0
counter bytes long:        2912
counter packets long:      28
timestamp abs first:       02:57:06.025
timestamp abs last:        02:57:33.378
flow end reason:           Not determined
application name:          prot ipv6-icmp
```

次の出力例は、フローエクスポータの詳細を示しています。

```
Device# show flow exporter temp0
Flow Exporter temp0:
  Description:              performance monitor context temp0 exporter
  Export protocol:          IPFIX (Version 10)
  Transport Configuration:
    Destination type:       IP
    Destination IP address: 10.0.0.1
    VRF label:              1
    Source IP address:      10.0.0.0
    Source Interface:       GigabitEthernet5
    Transport Protocol:     UDP
    Destination Port:       4739
    Source Port:            51242
    DSCP:                   0x1
    TTL:                    255
    Output Features:        Used
  Export template data timeout:        300
  Options Configuration:
    interface-table (timeout 300 seconds) (active)
    vrf-table (timeout 300 seconds) (active)
    sampler-table (timeout 300 seconds) (active)
    application-table (timeout 300 seconds) (active)
    application-attributes (timeout 300 seconds) (active)
```

CLI を使用した BFD メトリックのエクスポートに対する Flexible NetFlow の設定

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

Cisco IOS XE Catalyst SD-WAN デバイス を制御している Cisco SD-WAN コントローラ の CLI から、データポリシーを使用して BFD メトリックのエクスポートを有効にするか無効にするかに応じて、次のコマンドを入力します。

1. BFD メトリックのエクスポートを有効にします。

```
policy
 cflowd-template template-name
   collector vpn vpn-id address ip-address port port transport transport
     source-interface interface
     bfd-metrics-export
     export-interval export-interval
```

   デフォルトの BFD エクスポート間隔は 600 秒です。BFD エクスポート間隔は、Cflowd テンプレートの更新には影響を受けません。BFD エクスポート間隔では、bfd-metrics-export テーブルからデータを送信する間隔のみを制御します。tunnel-tloc テーブルでは、BFD エクスポート間隔は、BFDエクスポート間隔とCflowdテンプレート更新間の最小値を、データ送信間隔に使用しています。

2. BFD メトリックのエクスポートを無効にします。

```
policy
 cflowd-template template-name
   collector vpn vpn-id address ip-address port port transport transport
   source-interface interface
   no bfd-metrics-export
```

BFD メトリックのエクスポートを有効にする一連の設定例を次に示します。

```
policy
 cflowd-template fnf
  template-refresh 600
  collector vpn 0 address 10.0.100.1 port 4739 transport transport_udp
   bfd-metrics-export
    export-interval 30
   !
  !
 !
 lists
  site-list 500
   site-id 500
  !
 !
!
apply-policy
 site-list 500
  cflowd-template fnf
 !
!
```

BFD メトリックのエクスポートに対する Flexible NetFlow 設定の確認

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

以下は、**show flow exporter** コマンドの出力例で、各フローエクスポータの設定を示したものです。

```
Device# show flow exporter
…
Flow Exporter sdwan_flow_exporter_1:
  Description:              export flow records to collector
  Export protocol:          IPFIX (Version 10)
  Transport Configuration:
    Destination type:       IP
    Destination IP address: 10.0.100.1
    Source IP address:      10.0.100.15
    Transport Protocol:     UDP
    Destination Port:       4739
    Source Port:            54177
    DSCP:                   0x0
    TTL:                    255
    MTU:                    1280
    Output Features:        Used
  Options Configuration:
    interface-table (timeout 600 seconds)  (active)
    tunnel-tloc-table (timeout 600 seconds) (active)
    bfd-metrics-table (timeout 600 seconds) (active)
```

以下は、**show flow exporter statistics** コマンドの出力例で、各フローエクスポータのクライアント送信統計情報を示したものです。

```
Device# show flow exporter statistics
…
Flow Exporter sdwan_flow_exporter_1:
  Packet send statistics (last cleared 3d05h ago):
    Successfully sent:         1433                  (907666 bytes)

  Client send statistics:
    Client: Option options interface-table
      Records added:           6552
        - sent:                6552
      Bytes added:             694512
        - sent:                694512

    Client: Option options tunnel-tloc-table
      Records added:           1916
        - sent:                1916
      Bytes added:             99632
        - sent:                99632

    Client: Flow Monitor sdwan_flow_monitor
      Records added:           0
      Bytes added:             0

    Client: Option options bfd-metrics-table
      Records added:           4
```

```
    - sent:               4
  Bytes added:            196
    - sent:               196
```

以下は、**show flow exporter templates** コマンドの出力例で、各テンプレートの詳細を示したものです。

```
Device# show flow exporter templates
…
 Client: Option options tunnel-tloc-table
  Exporter Format: IPFIX (Version 10)
  Template ID    : 257
  Source ID      : 6
  Record Size    : 52
  Template layout
  _____________________________________________________________________________
  |                 Field                    |    ID | Ent.ID | Offset |  Size |
  -----------------------------------------------------------------------------
  | TLOC TABLE OVERLAY SESSION ID            | 12435 |      9 |      0 |     4 |
  | tloc local color                         | 12437 |      9 |      4 |    16 |
  | tloc remote color                        | 12439 |      9 |     20 |    16 |
  | tloc tunnel protocol                     | 12440 |      9 |     36 |     8 |
  | tloc local system ip address             | 12436 |      9 |     44 |     4 |
  | tloc remote system ip address            | 12438 |      9 |     48 |     4 |
  -----------------------------------------------------------------------------

  Client: Option options bfd-metrics-table
  Exporter Format: IPFIX (Version 10)
  Template ID    : 262
  Source ID      : 6
  Record Size    : 49
  Template layout
  _____________________________________________________________________________
  |                 Field                    |    ID | Ent.ID | Offset |  Size |
  -----------------------------------------------------------------------------
  | TLOC TABLE OVERLAY SESSION ID            | 12435 |      9 |      0 |     4 |
  | IP DSCP                                  |   195 |        |      4 |     1 |
  | bfd loss                                 | 12527 |      9 |      5 |     4 |
  | bfd pfr update ts                        | 12530 |      9 |      9 |     8 |
  | bfd avg latency                          | 12528 |      9 |     17 |     8 |
  | bfd avg jitter                           | 12529 |      9 |     25 |     8 |
  | bfd rx cnt                               | 12531 |      9 |     33 |     8 |
  | bfd tx cnt                               | 12532 |      9 |     41 |     8 |
  -----------------------------------------------------------------------------
```

Flexible NetFlow による BFD メトリックのエクスポート設定例

最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

以下は、BFD メトリックのエクスポートを有効にする場合の一元管理型ポリシーの設定例です。

```
Device# show sdwan policy from-vsmart
from-vsmart cflowd-template fnf
 flow-active-timeout    600
 flow-inactive-timeout  60
```

```
 template-refresh       600
 flow-sampling-interval 1
 protocol               ipv4
 customized-ipv4-record-fields
  no collect-tos
  no collect-dscp-output
 collector vpn 0 address 10.0.100.1 port 4739 transport transport_udp
  bfd-metrics-export
   export-interval 600
```

以下は、平均ジッター、平均遅延、および損失メトリックに関する FNF BFD テレメトリデータの例です。

```
{ 'Data_Template': 'Data_Flow',
  'ObservationDomainId': 6,
  'Version': 10,
  'arrive_time': 1658807309.2496994,
  'dfs_tfs_length': 200,
  'export_dfs_tfs_templates_list_dict': { 'FlowSequence': 3354,
                                          'Flowset_id': '258',
                                          'Flowset_length': 200,
                                          'Length': 286,
                                          'ObservationDomainId': 6,
                                          'TimeStamp': 1658807269,
                                          'Version': 10,
                                          'flow': [ { 'bfd_avg_jitter': 1000,
                                                      'bfd_avg_latency': 1000,
                                                      'bfd_loss': 15,
                                                    'bfd_pfr_update_ts': 1658806692155,

                                                      'bfd_rx_cnt': 0,
                                                      'bfd_tx_cnt': 0,
                                                      'ipDiffServCodePoint': 48,
                                                      'tloc_table_overlay_session_id':
10},
                                                      …
                                                ]},
   'flow_length': 4,
   'flow_time': 1658807269,
   'flowset_id': '258',
   'header': { 'FlowSequence': 3354,
               'Length': 286,
               'ObservationDomainId': 6,
               'TimeStamp': 1658807269,
               'Version': 10},
   'host': '10.0.100.15',
   'ipfix_length': 286,
   'packet_number': 2,
   'template_id': '258'}
```

Cflowd ポリシーの適用と有効化

一元管理型データポリシーを有効にするには、次のようにオーバーレイネットワーク内のサイトのリストに適用します。

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name
```

Cflowd テンプレートをアクティブにするには、データポリシーに関連付けます。

```
vSmart(config)# apply-policy cflowd-template template-name
```

apply-policy コマンドで適用するすべての **data-policy** ポリシーについて、すべてのサイトリストのサイト ID は一意である必要があります。つまり、サイトリストに重複するサイト ID が含まれていてはなりません。重複するサイト ID の例には、2 つのサイトリスト **site-list 1**、**site-id 1-100**、および **site-list 2 site-id 70-130** のサイト ID があります。ここでは、サイト 70 ～ 100 が両方のリストに含まれています。これらの 2 つのサイトリストを 2 つの異なる **data-policy** ポリシーに適用すると、Cisco Catalyst SD-WAN コントローラ で設定をコミットする試行が失敗します。

同じタイプの制限は、次のポリシーのタイプにも適用されます。

- アプリケーション認識型ルーティングポリシー（**app-route-policy**）
- 一元管理型制御ポリシー（**control-policy**）
- 一元管理型データポリシー（**data-policy**）

ただし、異なるタイプのポリシーに適用するサイトリストのサイト ID は重複させることができます。たとえば、**control-policy** ポリシーと **data-policy** ポリシーのサイトリストでは、サイト ID が重複している可能性があります。したがって、上記 2 つのサイトリストの例（**site-list 1 site-id 1-100** および **site-list 2 site-id 70-130**）では、1 つを制御ポリシーに、もう 1 つをデータポリシーに適用できます。

commit コマンドを発行して設定を正常にアクティブにすると、Cisco Catalyst SD-WAN コントローラ は、指定されたサイトにある Cisco IOS XE Catalyst SD-WAN デバイス にデータポリシーをプッシュします。Cisco Catalyst SD-WAN コントローラ で設定されたポリシーを表示するには、Cisco Catalyst SD-WAN コントローラ で **show running-config** コマンドを使用します。デバイスにプッシュされたポリシーを表示するには、デバイスで **show policy from-vsmart** コマンドを使用します。

Cisco Catalyst SD-WAN コントローラ で設定されている一元管理型データポリシーを表示するには、**show running-config** コマンドを使用します。

```
vSmart# show running-config policy
vSmart# show running-config apply-policy
```

Cisco IOS XE Catalyst SD-WAN デバイス にプッシュされた一元管理型データポリシーを表示するには、デバイスで **show omp data-policy** コマンドを発行します。

```
デバイス# show sdwan policy from-vsmart
```

Cisco IOS XE Catalyst SD-WAN デバイス での Cflowd の可視性の有効化

データポリシーを設定せずに Cisco IOS XE Catalyst SD-WAN デバイス で Cflowd の可視性を直接有効にすることもできます。これにより、LAN 内のすべての VPN からルータに着信するトラフィックのトラフィックフローモニタリングを実行できます。これを行うには、デバイスで Cflowd の可視性を設定します。

```
デバイス(config)# policy flow-visibility
```

アプリケーションをモニタリングするには、デバイスで **show app cflowd flows** および **show app cflowd statistics** コマンドを使用します。

Cflowd トラフィック フロー モニタリングの設定例

このトピックでは、トラフィック フロー モニタリングの設定例を示します。

設定手順

一元管理型データポリシーを使用して Cflowd トラフィックモニタリングを有効にします。これにより、すべての設定が Cisco Catalyst SD-WAN コントローラ で実行されます。すべての TCP トラフィックをモニタリングし、単一のコレクタに送信する手順の例を次に示します。

1. Cflowdテンプレートを作成してコレクタの場所を定義し、Cflowdタイマーを変更します。

```
vsmart(config)# policy cflowd-template test-cflowd-template
vsmart(config-cflowd-template-test-cflowd-template)# collector vpn 1 address
172.16.155.15 port 13322 transport transport_udp
vsmart(config-cflowd-template-test-cflowd-template)# flow-inactive-timeout 60
vsmart(config-cflowd-template-test-cflowd-template)# template-refresh 90
```

2. トラフィックをモニタリグする VPN のリストを作成します。

```
vsmart(config)# policy lists vpn-list vpn_1 vpn 1
```

3. データポリシーを適用するサイトのリストを作成します。

```
vsmart(config)# policy lists site-list cflowd-sites site-id 400,500,600
```

4. データポリシーを設定します。

```
vsmart(config)# policy data-policy test-cflowd-policy
vsmart(config-data-policy-test-cflowd-policy)# vpn-list vpn_1
vsmart(config-vpn-list-vpn_1)# sequence 1
vsmart(config-sequence-1)# match protocol 6
vsmart(config-match)# exit
vsmart(config-sequence-1)# action accept cflowd
vsmart(config-action)# exit
vsmart(config-sequence-1)# exit
vsmart(config-vpn-list-vpn_1)# default-action accept
```

5. オーバーレイネットワーク内のサイトにポリシーと Cflowd テンプレートを適用します。

```
vsmart(config)# apply-policy site-list cflowd-sites data-policy test-cflowd-policy
デバイス(config-site-list-cflowd-sites)# cflowd-template test-cflowd-template
```

6. データポリシーを有効にします。

```
vsmart(config-site-list-cflowd-sites)# validate
Validation complete
vsmart(config-site-list-cflowd-sites)# commit
Commit complete.
vsmart(config-site-list-cflowd-sites)# exit configuration-mode
```

設定例

Cflowd 設定の完全な例を次に示します。

```
vsmart(config)# show configuration
apply-policy
```

```
 site-list cflowd-sites
  data-policy     test-cflowd-policy
  cflowd-template test-cflowd-template
 !
!
policy
 data-policy test-cflowd-policy
  vpn-list vpn_1
   sequence 1
    match
     protocol 6
    !
    action accept
     cflowd
    !
   !
   default-action accept
  !
 !
 cflowd-template test-cflowd-template
  flow-inactive-timeout 60
  template-refresh      90
  collector vpn 1 address 192.168.0.1 protocol ipv4 port 13322 transport transport_udp
 !
 lists
  vpn-list vpn_1
   vpn 1
  !
  site-list cflowd-sites
   site-id 400,500,600
  !
 !
!
```

show sdwan run policy コマンドの次の出力例は、SAIE フローを使用した Cflowd の IPv4 および IPv6 アプリケーションの可視性とフローの可視性の設定を示しています。

```
Device# show sdwan run policy
policy
 app-visibility
 app-visibility-ipv6
 flow-visibility
 flow-visibility-ipv6
```

Cflowd 設定の検証

Cisco Catalyst SD-WAN コントローラ で Cflowd の設定をアクティブ化した後に検証するには、**show running-config policy** コマンドと **show running-config apply-policy** コマンドを使用します。

次に、**show sdwan policy from-vsmart cflowd-template** コマンドの出力例を示します。

```
デバイス# show sdwan policy from-vsmart cflowd-template
from-vsmart cflowd-template test-cflowd-template
 flow-active-timeout   30
 flow-inactive-timeout 60
 template-refresh      90
 flow-sampling-interval 1
 protocol ipv4/ipv6/both
 customized-ipv4-record-fields
  collect-tos
  collect-dscp-output

collector vpn 1 address 192.0.2.1 protocol ipv4 port 13322 transport transport_udp
```

次に、**show sdwan policy from-vsmart** コマンドの出力例を示します。

```
デバイス# show sdwan policy from-vsmart
from-vsmart data-policy test-cflowd-policy
 vpn-list vpn_1
  sequence 1
   match
    protocol 6
   action accept
    cflowd
  default-action accept
from-vsmart cflowd-template test-cflowd-template
 flow-active-timeout   30
 flow-inactive-timeout 60
 protocol ipv4/ipv6/both
 template-refresh      90
 customized-ipv4-record-fields
   collect-tos
   collect-dscp-output
 collector vpn 1 address 192.0.2.1 port 13322 transport transport_udp
from-vsmart lists vpn-list vpn_1
 vpn 1
```

Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a 以降、cflowd コマンドは、IPv4 と IPv6 の両方のフローレコードに対して拡張されています。

次に、**show flow record** コマンドの出力例を示します。フローの方向を指定する新しいフィールド `[collect connection initiator]` の追加によって拡張されています。

```
Device# show flow record sdwan_flow_record-xxx
```

IPv4 フローレコード：

```
flow record sdwan_flow_record-1666223692122679:
  Description:        flow and application visibility records
  No. of users:       1
  Total field space:  102 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match routing vrf service
    collect ipv4 dscp
    collect transport tcp flags
    collect interface input
    collect interface output
    collect counter bytes long
    collect counter packets long
    collect timestamp absolute first
    collect timestamp absolute last
    collect application name
    collect flow end-reason
    collect connection initiator
    collect overlay session id input
    collect overlay session id output
    collect connection id long
    collect drop cause id
    collect counter bytes sdwan dropped long
    collect sdwan sla-not-met
    collect sdwan preferred-color-not-met
    collect sdwan qos-queue-id
collect counter packets sdwan dropped long
```

IPv6 フロー形式：

```
flow record sdwan_flow_record_ipv6-1667963213662363:
  Description:        flow and application visibility records
  No. of users:       1
  Total field space:  125 bytes
  Fields:
    match ipv6 protocol
    match ipv6 source address
    match ipv6 destination address
    match transport source-port
    match transport destination-port
    match routing vrf service
    collect ipv6 dscp
    collect transport tcp flags
    collect interface input
    collect interface output
    collect counter bytes long
    collect counter packets long
    collect timestamp absolute first
    collect timestamp absolute last
    collect application name
    collect flow end-reason
    collect connection initiator
    collect overlay session id input
    collect overlay session id output
    collect connection id long
    collect drop cause id
    collect counter bytes sdwan dropped long
    collect sdwan sla-not-met
    collect sdwan preferred-color-not-met
    collect sdwan qos-queue-id
    collect counter packets sdwan dropped long
```

次に、**show flow monitor** *monitor-name* **cache** コマンドの拡張出力例を示します。フロー方向を示す新しい `[connection initiator]` フィールドが出力に追加されました。`[connection initiator]` フィールドには、`initiator`（クライアントからサーバーへのトラフィックフローの場合）、`reverse`（サーバーからクライアントの場合）、`unknown`（トラフィックフローの方向が不明の場合）のいずれかの値を指定できます。

```
Device# show flow monitor sdwan_flow_monitor cache
Cache type: Normal (Platform cache)
Cache size: 128000
Current entries: 4
High Watermark: 5
Flows added: 6
Flows aged: 2
- Inactive timeout ( 10 secs) 2
IPV4 SOURCE ADDRESS: 10.20.24.110
IPV4 DESTINATION ADDRESS: 10.20.25.110
TRNS SOURCE PORT: 40254
TRNS DESTINATION PORT: 443
IP VPN ID: 1
IP PROTOCOL: 6
tcp flags: 0x02
interface input: Gi5
interface output: Gi1
counter bytes long: 3966871
counter packets long: 52886
timestamp abs first: 02:07:45.739
timestamp abs last: 02:08:01.840
flow end reason: Not determined
connection initiator: Initiator
```

```
interface overlay session id input: 0
interface overlay session id output: 4
connection connection id long: 0xD8F051F000203A22
```

フローを確認します。

Cflowd データポリシーの影響を受ける Cisco IOS XE Catalyst SD-WAN デバイス では、さまざまなコマンドで Cflowd フローのステータスを確認できます。

```
デバイス# show sdwan app-fwd cflowd statistics

      data_packets             :      0
      template_packets         :      0
      total-packets            :      0
      flow-refresh             :      123
      flow-ageout              :      117
      flow-end-detected        :      0
      flow-end-forced          :      0
```

IPv6 トラフィックの FNF IPv6 設定例

IPv6 トラフィック用の Cflowd を使用した一元管理型ポリシーの設定例を次に示します。

```
policy
 data-policy _vpn_1_accept_cflowd_vpn_1
  vpn-list vpn_1
   sequence 102
    match
     source-ipv6      2001:DB8:0:/32
     destination-ipv6 2001:DB8:1:/32
    !
    action accept
     count  cflowd_ipv6_1187157291
     cflowd
    !
   !
   default-action accept
  !
 !
 cflowd-template cflowd_server
  flow-active-timeout   60
  flow-inactive-timeout 30
  protocol              ipv6
 !
 lists
  vpn-list vpn_1
   vpn 1
  site-list vedge1
   site-id 500
  !

apply-policy
 site-list vedge1
  data-policy _vpn_1_accept_cflowd_vpn_1 all
  cflowd-template cflowd_server
```

FNF 展開エクスポートの設定例

展開エクスポートの設定例を次に示します。

```
Device# show sdwan policy from-vsmart
from-vsmart cflowd-template cflowd
 flow-active-timeout    600
 flow-inactive-timeout  60
 template-refresh       60
 flow-sampling-interval 1
 protocol               ipv4
 customized-ipv4-record-fields
  no collect-tos
  no collect-dscp-output
 collector vpn 0 address 10.0.100.1 port 4739 transport transport_udp
  export-spread
   app-tables   20
   tloc-tables  10
   other-tables 5
```

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。