ネットワーク

表 *1*：機能の履歴

機能名	リリース情報	説明
ルーティング、ライセンス、ポリシー、およびその他の設定オプションに関する追加のリアルタイムモニタリングのサポート	Cisco IOS XE リリース 17.6.1a Cisco SD-WAN リリース 20.6.1 Cisco vManage リリース 20.6.1	この機能により、ルーティング、ポリシー、Cloud Express、Cisco vBond Orchestrator、TCP 最適化、SFP、トンネル接続、ライセンス、ロギング、Cisco Umbrella 情報など、多数のデバイス設定の詳細をリアルタイムでモニタリングできるようになりました。Cisco vManage でのリアルタイムモニタリングは、デバイスの CLI で **show** コマンドを使用する場合と似ています。 Cisco vManage には多くのデバイス設定の詳細情報がありますが、デバイス設定の詳細の一部分のみが Cisco IOS XE リリース 17.6.1a および Cisco vManage リリース 20.6.1 に追加されます。
AppQoE およびその他の設定オプションに関する追加のリアルタイムモニタリングのサポート	Cisco IOS XE リリース 17.9.1a Cisco SD-WAN リリース 20.9.1 Cisco vManage リリース 20.9.1	この機能により、AppQoE およびその他のデバイス設定の詳細をリアルタイムでモニタリングできるようになります。Cisco vManage でのリアルタイムモニタリングは、デバイスの CLI で **show** コマンドを使用する場合と似ています。

AppQoE 情報の表示

最小リリース：Cisco vManage リリース 20.9.1

AppQoE 情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]**の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、次のコマンドのいずれかを選択します。

デバイスオプション	コマンド	説明
AppQoE アクティブフローの詳細	show sdwan appqoe flow flow-id [flow_id]	1 つの特定フローの詳細を表示します。
AppQoE 期限切れフローの概要	show sdwan appqoe flow closed all	AppQoE の期限切れフローの概要を表示します。
AppQoE アクティブフローの概要	show sdwan appqoe flow vpn-id [vpn_id] server-port [server_port]	特定の VPN のフローを表示します。
AppQoE 期限切れフローの詳細	show sdwan appqoe flow closed flow-id [flow_id]	1 つの特定フローについて、AppQoE 期限切れフローの詳細を表示します。

Configuration Commit List の表示

最小リリース：Cisco vManage リリース 20.9.1

デバイスの configuration commit list を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]**の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、次のコマンドを選択します。

デバイスオプション	コマンド	説明
Configuration Commit List の表示	show configuration commit list	configuration commit list を表示します。

ネットワークサイトのステータスの確認

サイトは、分散拠点、データセンター、キャンパスなど、Cisco SD-WAN オーバーレイネットワーク内にある特定の物理的な場所です。各サイトは、サイトIDと呼ばれる一意の整数によって識別されます。サイトの各デバイスは、同じサイト ID で識別されます。

ネットワークサイトのステータスを確認するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Overview]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Dashboard]** > **[Main Dashboard]**の順に選択します。

2. サイトのデータ接続の状態を表示する [Site BFD Connectivity] ダッシュレットを見つけます。サイトに複数のエッジデバイスがある場合、このダッシュレットには、個々のデバイスではなくサイト全体の状態が表示されます。[Site BFD Connectivity] ダッシュレットには、次の 3 つの状態が表示されます。

   - [Full WAN Connectivity]：すべてのデバイス上のすべての BFD セッションが稼働状態にあるサイトの総数。
   - [Partial WAN Connectivity]：TLOC またはトンネルが停止状態にあるサイトの総数。これらのサイトでは、データプレーン接続が制限されています。
   - [No WAN Connectivity]：すべてのデバイス上のすべての BFD セッションが停止状態にあるサイトの総数。これらのサイトにはデータプレーン接続がありません。

   さらに詳細を表示するには、いずれかをクリックします。詳細がポップアップウィンドウに表示されます。
3. 目的の行で [...] をクリックし、[Device Dashboard]、[SSH Terminal]、[Real Time] のいずれかを選択します。選択に基づいて、適切なウィンドウにリダイレクトされます。

ネットワークサイトトポロジの表示

表 2: 機能の履歴

機能名	リリース情報	説明
Cisco vManage でのサイトトポロジの可視化	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1	Cisco vManage でサイトのトポロジ図を表示できるようになりました。
Cisco vManage でのサイトトポロジの可視化（フェーズII）	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能はサイトトポロジの高度な双方向性の可視化をサポートし、トポロジ内のデバイスとトンネルの状態に関する情報を提供します。これにより、モニタリングとトラブルシューティングのエクスペリエンスが向上します。

サイトトポロジについて

Cisco vManage は設定グループに展開されている Cisco IOS XE SD-WAN デバイス に着目して、各サイトのトポロジ図を生成します。設定グループの詳細については、「Configuration Groups and Feature Profiles」[英語] を参照してください。

このトポロジ図には、次の情報が表示されます。

- デバイス情報：トポロジ図には、選択したサイトに展開されているすべてのデバイスが表示されます。各デバイスのモデルと正常性ステータスが表示されます。デバイス名の上にカーソルを置くと、そのデバイスのホスト名とシステム IP アドレスを表示できます。同様に、デバイス名をクリックすると、そのデバイスに関する詳細情報が右側のナビゲーションウィンドウに表示されます。このペインから、デバイスダッシュボードに移動して詳細を確認できます。

  Cisco vManage リリース 20.8.1 では、トポロジ図にはデバイスのモデルとシステム IP アドレスのみが表示されます。

- トランスポート情報：トポロジ図には、VPN 0 と、デバイスに接続されているすべてのトランスポートインターフェイスが表示されます。インターフェイスとプロトコルの詳細も含まれます。トランスポートインターフェイス名にカーソルを合わせると、過去 3 時間のアップストリームとダウンストリームの平均速度を表示できます。

- VPN サービス情報：トポロジ図には、VPN サービス名と ID が表示されます。VPN サービス名の横にあるドロップダウン矢印をクリックすると、プロトコル、インターフェイス、および過去 3 時間のアップストリームとダウンストリームの平均速度を表示できます。

トポロジ図には、最大 12 個の VPN サービスが表示されます。12 個を超える VPN サービスがある場合は、[More] ボタンをクリックすると、右側のナビゲーションウィンドウに VPN サービスの完全なリストを表示できます。

- 回線の正常性情報：回線とトランスポートインターフェイス間のリンクの色は、回線の正常性を示します。

（注）

- Cisco IOS XE SD-WAN デバイス が設定グループに関連付けられていても、デバイスが展開されていない場合は、トポロジ図にはホスト名とシステム IP のみが表示されます。

  ただし、デバイスが設定グループに関連付けられていて、デバイスも展開されている場合、トポロジ図には LAN および WAN の詳細を含むデバイスの全詳細が表示されます。

- 設定グループに関連付けられていないデバイスがサイトにある場合、トポロジ図にはホスト名とシステム IP のみを持つスタンドアロンデバイスが表示されます。
- 各サイトのトポロジ図に表示されるデバイスの数に制限はありません。ただし、サイトに多数のデバイスがある場合、デバイス間の接続は表示されません。
- 拡大および縮小アイコンをクリックして、トポロジ図の倍率を調整できます。同様に、全画面アイコンをクリックすると、トポロジ図を全画面で表示できます。
- 更新アイコンをクリックすると、トポロジ図が再生成されて最新のデータが表示されます。
- 正常性メトリックの詳細を表示するには、凡例（ⓘ）アイコンをクリックします。

サイトトポロジの可視化に対応したデバイス

この機能は Cisco IOS XE SD-WAN デバイス でのみサポートされています。

サイトトポロジ可視化の前提条件

- デバイスは、設定グループに展開する必要があります。
- デバイスモニタリング機能には、ロール ベース アクセス コントロール（RBAC）が必要です。

ネットワークサイトトポロジの表示

サイトトポロジの表示方法には、次のオプションがあります。

[Devices] ウィンドウを使用する

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。
2. テーブルで対応する Cisco IOS XE SD-WAN デバイス を見つけ、デバイス名の隣にある [Site ID] 列の値をクリックします。

   または、[Hostname] 列でデバイス名をクリックし、デバイスダッシュボードで [Site ID] の値をクリックします。

Cisco vManage にサイトのトポロジが表示されます。

[Geography] ウィンドウを使用する

1. Cisco vManage のメニューから**[Monitor]** > **[Geography]**の順に選択します。
2. マップ内で対応する Cisco IOS XE SD-WAN デバイス をクリックします。
3. [Site ID] の値をクリックします。

Cisco vManage にサイトのトポロジが表示されます。

Cisco SD-WAN テレメトリのデータ収集の管理

表 *3 :* 機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN テレメトリのデータ収集の管理	Cisco IOS XE リリース 17.6.1a Cisco SD-WAN リリース 20.6.1 Cisco vManage リリース 20.6.1	この機能により、Cisco vManage を使用した Cisco SD-WAN テレメトリのデータ収集を無効にできます。 テレメトリのデータ収集はデフォルトで有効になっています。

Cisco vManage リリース 20.6.1 以降では、**[Administration]** > **[Settings]** > **[Data Collection]**から Cisco SD-WAN テレメトリのデータ収集を有効または無効にする新しいオプションが Cisco vManage に追加されました。このリリースより前は、[Data Collection] セクションにはデータ収集を有効または無効にするオプションしかなく、Cisco SD-WAN テレメトリのデータ収集オプションはありませんでした。2 つのオプションについて以下で説明します。

[Data Collection]：クラウドでホストされている Cisco SD-WAN のデータ収集サービス（DCS）への接続を確立する際にこのオプションを使用します。Cisco vManage から DCS への接続を利用して、Cisco vAnalytics や Cisco SD-WAN テレメトリなどのさまざまな機能で必要なデータが、コントローラとネットワークから収集されます。

[SD-WAN Telemetry Data Collection]：コントローラやネットワークからのテレメトリデータ収集を有効または無効にする際にこのオプションを使用します。Cisco SD-WAN で [Data Collection] が有効になっている場合、このオプションはデフォルトで有効になります。シスコ提供のクラウドホステッドコントローラの場合、このオプションはコントローラのプロビジョニング時に有効になります。オンプレミスコントローラの場合、[Data Collection] の設定を使用して Cisco SD-WAN データ収集サービス（DCS）への接続を確立することが、Cisco SD-WAN テレメトリを有効にするために必須な前提条件です。

SD-WAN テレメトリのデータ収集の前提条件

シスコ提供のクラウドホステッドサービス：このクラウドサービスはデフォルトで有効になっています。それ以上の操作は不要です。

オンプレミスサービス：このクラウドサービスはデフォルトで無効になっています。Cisco SD-WANテレメトリのデータ収集を有効にする前に、このクラウドサービスを有効にする必要があります。

1. Cisco vManage のメニューから**[Administration]** > **[Settings]** の順に選択します。
2. [Cloud Services] オプションの横にある [Edit] をクリックします。
3. [Enabled] をクリックします。
4. [OTP] に値を入力します。Cisco TAC サポートケースをオープンすることで、Cisco CloudOps チームにトークンをリクエストできます。
5. [Cloud Gateway URL] は空白のままにします。
6. データ収集を開始し、データをクラウドにアップロードする権限を承認します。
7. [Save] をクリックします。

SD-WAN テレメトリデータ収集の有効化または無効化

1. Cisco vManage のメニューから**[Administration]** > **[Settings]** の順に選択します。
2. [Data Collection] オプションで、[Edit] をクリックします。
3. [SD-WAN Telemetry Data Collection] オプションでは、[Enabled] がデフォルトで選択されています。Cisco SD-WAN のテレメトリデータ収集を無効にするには、[Disabled] をクリックします。
4. [Save] をクリックします。

オンプレミスの Cisco vManage インスタンスでデータ収集を有効にするための追加手順

ポート 443 の Cisco vManage（インターフェイス VPN 0）から次の表の宛先へのアウトバウンド通信を許可するように、ローカルファイアウォールを設定します。Cisco vAnalytics インスタンスの地理的位置に基づいて、適切な一連の宛先を選択します。

Location	Destinations
南・北・中央アメリカ	https://us-west.dcs.viptela.net（Cisco vManage リリース 20.1 以前） https://us01.datagateway.analytics.sdwan.cisco.com（Cisco vManage リリース 20.3 以降） https://datamanagement-us-01.sdwan.cisco.com（Cisco vManage リリース 20.3 以降）
アメリカ（東部）	https://us-east.dcs.viptela.net（Cisco vManage リリース 20.1 以前） https://us02.datagateway.analytics.sdwan.cisco.com（Cisco vManage リリース 20.3 以降） https://datamanagement-us-01.sdwan.cisco.com（Cisco vManage リリース 20.3 以降）
欧州	https://europe.dcs.viptela.net（Cisco vManage リリース 20.1 以前） https://eu01.datagateway.analytics.sdwan.cisco.com (Cisco vManage リリース 20.3 以降) https://datamanagement-us-01.sdwan.cisco.com（Cisco vManage リリース 20.3 以降）https://datamanagement-us-01.sdwan.cisco.com/
オーストラリア	https://au01.datagateway.analytics.sdwan.cisco.com (Cisco vManage リリース 20.3 以降) https://datamanagement-us-01.sdwan.cisco.com (Cisco vManage リリース 20.3 以降)

Cisco vManage の CLI から cURL -k コマンドを使用して、これらの宛先への到達可能性を確認できます。

ネットワークの再検出

[Rediscover Network] ウィンドウを使用して、オーバーレイネットワーク内の新しいデバイスを検出して、Cisco vManage と同期できます。

1. Cisco vManage のメニューから、**[Tools]** > **[Rediscover Network]**を選択します。

2. デバイスモデルの横にあるチェックボックスをオンにして、デバイスを選択します。探しているデバイスを見つけるには、デバイステーブルをスクロールします。または、[Device Groups] ドロップダウンリストからデバイスグループを選択して、特定のデバイスグループに属するデバイスを表示します。
3. デバイスデータの再同期を確認するには、[Rediscover] をクリックします。
4. [Rediscover Network] ダイアログボックスで、[Rediscover] をクリックします。

ルーティング情報の表示

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。
2. 表示されるデバイスリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストで、次のコマンドから該当するものを選択します。

デバイス オプション	コマンド	説明
IP ルート	show ip routes show ipv6 routes	IP ルートテーブルのエントリに関する情報を表示します。 ローカルルートテーブルの IPv6 エントリを表示します。
IP FIB	show ip fib show ipv6 fib	転送テーブルのエントリに関する情報を表示します。 ローカル転送テーブルの IPv6 エントリを表示します。
IP MFIB のサマリー	show ip mfib summary	マルチキャスト FIB のアクティブエントリのサマリーに関する情報を表示します。
IP MFIB の OIL 情報	show ip mfib oil	マルチキャスト FIB からの発信インターフェイスに関する情報を表示します。
IP MFIB の統計情報	show ip mfib stats	マルチキャスト FIB のアクティブエントリの統計情報を表示します。

デバイス オプション	コマンド	説明
OMP ピア	show omp peers	OMP ピアとそのピアリング セッションを表示します。
OMP のサマリー	show omp summary	Cisco vSmart とルータ間で実行されている OMP セッションに関する情報を表示します。
OMP 受信ルートまたは OMP アドバタイズメントルート	show omp routes show sdwan omp routes	OMP ルートを表示します。 ローカルルートテーブルの IPv6 エントリを表示します。
OMP 受信 TLOC または OMP のアドバタイズメント TLOC	show omp tlocs	OMP TLOC を表示します。
OSPF インターフェイス	show ospf interface	OSPF を実行するインターフェイスに関する情報を表示します。
OSPF ネイバー	show ospf neighbor	OSPF ネイバーに関する情報を表示します。
OSPF ルート	show ospf routes	OSPF から学習したルートを表示します。
OSPF データベースのサマリー	show ospf database-summary	OSPF リンクステート データベース エントリのサマリーを表示します
OSPF データベース	show ospf database	OSPF リンクステートデータベースのエントリに関する情報を表示します。
OSPF 外部データベース	N/A	OSPF 外部ルートの表示外部ルートは、OSPF AS（ドメイン）内にない OSPF ルートです。
OSPF プロセス	show ospf process	OSPF プロセスを表示します。
PIM インターフェイス	show pim interface	PIM を実行するインターフェイスに関する情報を表示します。
PIM ネイバー	show pim neighbor	PIM ネイバーに関する情報を表示します。

デバイス オプション	コマンド	説明
PIM 統計情報	show pim statistics	PIM 関連の統計情報を表示します
インターフェイスの詳細	show ipv6 interface	Cisco Cisco IOS XE SD-WAN デバイス の IPv6 に関する情報を表示します Cisco vManage リリース 20.6.1 以降では、すべての Cisco IOS XE SD-WAN デバイス および Cisco vEdge デバイス で、このデバイスオプションを使用できます。

マルチキャスト情報の表示

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストで、次のコマンドから該当するものを選択します。

デバイスオプション	コマンド	説明
マルチキャストトポロジ	show multicast topology	マルチキャストドメインに関するトポロジ情報を表示します
OMP マルチキャストのアドバタイズメントの自動検出または OMP マルチキャスト受信の自動検出	show omp multicast multicast-auto-discover	マルチキャストをサポートするピアを表示します
マルチキャストトンネル	show multicast tunnel	マルチキャストピア間の IPSec トンネルに関する情報を表示します
マルチキャスト RPF	show multicast rpf	マルチキャストリバースパスの転送情報を表示します

デバイスオプション	コマンド	説明
マルチキャストレプリケータ	show multicast replicator	マルチキャストレプリケータを表示します
OMPマルチキャストのアドバタイズメントルートまたはOMPマルチキャスト受信ルート	show omp multicast-routes	OMP が PIM Join メッセージから学習したマルチキャストルートを表示します

データポリシーの表示

集中管理型のデータポリシーが設定され、Cisco vSmart コントローラに適用されると、ポリシーが適用されるサイトリスト内のエッジデバイスに OMP アップデートで送信されます。集中管理型のデータポリシーは、送信元と宛先のアドレスとポート、プロトコル、DSCP 値を参照してデータパケットのヘッダー内のフィールドを調査します。一致するパケットについては、さまざまな方法でネクストホップを変更するか、パケットにポリサーを適用します。データトラフィックを送受信するときに、ポリシーの一致処理と結果のアクションがルータ上で実行されます。

アクセスリスト（ACL）とも呼ばれるローカライズされたデータポリシーは、ローカルルータ上で直接設定され、Cisco SD-WAN オーバーレイネットワーク上のルーター間で送信されるデータトラフィックに影響を与えます。

ルータの ACL 情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、次のコマンドのいずれかを選択します。

コマンド	説明
show policy access-list-names	設定されている ACL 名を表示します
show policy access-list-associations	ACL が適用されるインターフェイスを表示します
show policy access-list-associations	ACL の影響を受けるパケット数を表示します

Cisco vSmart コントローラ ポリシーの表示

デバイスのCisco vSmartコントローラからポリシー情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、次のコマンドのいずれかを選択します。

デバイスオプション	コマンド	説明
vSmart のポリシー	show policy from-vsmart show sdwan policy from-vsmart	Cisco vSmart コントローラ がエッジデバイスにプッシュした集中管理型データポリシー、アプリケーション認識ポリシー、または cflowd ポリシーを表示します。

ゾーンベース ポリシー ファイアウォールの表示

デバイス上のゾーンベースのファイアウォールに関するポリシー情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストで、次のコマンドから該当するものを選択します。

デバイスオプション	CLI コマンド	説明
ポリシーのゾーンベース ファイアウォール統計情報	`show policy zbfw filter-statistics`	ゾーンベースのファイアウォールの一致基準を満たすパケットの数と、基準に一致するバイト数を表示します。

デバイスオプション	CLI コマンド	説明
ポリシー ゾーン ペア セッション	`show policy zbfw sessions`	ゾーンベースのファイアウォールポリシーで設定されているすべてのゾーンペアのセッションフロー情報を表示します。

BFD プロトコル

Cisco SD-WAN ソリューションにおける BFD の役割

BFDプロトコルは、ルータ間のリンク障害を検出します。データトンネルで発生したデータの損失や遅延を測定して、接続の両端にあるデバイスのステータスを判断します。

データプレーンの復元力を高めるため、Cisco SD-WAN ソフトウェアはBFD プロトコルを実装しています。BFD プロトコルは、ルータ間のセキュアな IPsec および GRE 接続で自動的に動作します。これらの接続は、データプレーンとデータトラフィックに使用され、コントロールプレーンで使用される DTLS トンネルから独立しています。

BFD は、Cisco vEdge デバイス 間のすべての接続でデフォルトで有効になっています。 BFD を無効にすることはできません。ただし、Hello パケットとデッドタイムインターバルは調整できます。BFD リンクの両端でタイマーが異なる場合、BFD は低い方の値を使用するようにネゴシエートします。アプリケーション認識型ルーティング向けの BFD 設定、およびトランスポートトンネルでの BFD 設定については、「Configure BFD using vManage」[英語] を参照してください。

BFD の仕組み

Cisco vEdge デバイス が起動して制御接続が確立されると、Cisco vSmart コントローラ はピアの TLOC 情報を Cisco vEdge デバイス にアドバタイズします。Cisco vEdge デバイス はこの TLOC 情報およびその他の設定に基づいて、すべてまたは一部のピアの TLOC と BFD セッションを確立します。

BFD は Hello パケットを定期的に（デフォルトでは 1 秒ごとに）送信して、セッションがまだ動作しているかどうかを判断します。特定の数の Hello パケットが受信されない場合、BFD はリンクに障害が発生したと見なし、BFD セッションを停止します（デフォルトの乗数時間は 7 秒です）。BFD セッションがダウンすると、その IPSec トンネル上のネクストホップを指すルートは転送テーブル（FIB）から削除されますが、ルートテーブル（RIB）には引き続き存在します。

BFD の状態を確認して TLOC 間の接続損失をトラブルシュートする

BFD セッションがダウンしている場合は、それらの TLOC 間でトラフィックが流れないことを意味します。TLOC のペア間でトラフィックが中断していることを確認した場合、またはセッションフラップ数が増加していることに気付いた場合は、show bfd sessions または show bfd

history コマンドを使用して、BFD セッションのステータスを確認します。これらのコマンドは、確立されるべきすべての BFD セッションが実際に確立されているかどうかを把握するのに役立ちます。

BFD セッションには、停止状態、初期状態、稼働状態の 3 つの状態があります。

- **停止状態**：ネットワーク内の他の Cisco vEdge デバイス と接続が確立されていません。
- **初期状態**：接続は到達可能な状態ですが、まだ稼働していません。
- **稼働状態**：ネットワーク内の他の Cisco vEdge デバイス と接続が確立されています。

各デバイスはエコー要求をピアに送信し、また受信した要求に対するエコー応答を送信します。エコー応答で、デバイスは現在の BFD の状態を送信します。ピアはこれに基づいて、BFD の状態を必要に応じて変更します。

Cisco vManage によって生成される BFD アラームの詳細については、「永続的なアラームとアラームフィールド」を参照してください。

ピアからのエコー応答に基づくセッション状態の変化

次の表は、ピアの応答時に送信されたセッション状態に基づいて、デバイスの BFD セッション状態がどのように変化するかを示しています。

デバイスの BFD セッション状態	ピアがエコー応答で送信した BFD の状態	デバイスにおける BFD の状態の変化
稼働状態	稼働状態または初期状態	稼働状態（変化なし）
稼働状態	停止状態	停止状態
初期状態	稼働状態または初期状態	稼働状態
初期状態	停止状態	初期状態（変化なし）
停止状態	停止状態	初期状態
停止状態	初期状態	稼働状態
停止状態	稼働状態	停止状態（変化なし）

BFD セッション情報の表示

デバイスがネットワークに接続されると、ルータ間の Bidirectional Forwarding Detection（BFD）セッションが自動的に開始されます。ルータ間の安全な IPsec 接続で稼働する BFD を使用して、ルータ間の接続障害を検出できます。

ルータの BFD 情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストで、次のコマンドから該当するものを選択します。
   - [BFD Sessions]：リアルタイムの BFD セッションを表示する場合
   - [BFD History]：BFD セッション履歴を表示する場合

BGP 情報の表示

ルータでボーダー ゲートウェイ プロトコル（BGP）を設定して、デバイスのサービス側（サイトローカル側）でルーティングを有効にすると、デバイスのローカルサイトでネットワークに到達可能にすることができます。

ルータの BGP 情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストで、次のコマンドから該当するものを選択します。

オプション	説明
BGP Summary（**show bgp summary**）	BGP 接続ステータスを表示します。
BGP Neigbors（**show bgp neighbor**）	BGP ネイバーを表示します。
BGP Routes（**show bgp routes**）	BGP によって学習されたルートを表示します。

Cflowd 情報の表示

Cflowd はオーバーレイ ネットワーク内のルータ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 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とフロー内のパケットの IP ヘッダーから抽出されたデータが含まれます。

ルータで cflowd を設定するには、集中管理型データポリシーを使用して cflowd テンプレートを定義します。このテンプレートでは、フローの収集を制御する cflowd コレクタとタイマーの場所を指定します。

ルータの cflowd フロー情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]**の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストで、次のコマンドまたはオプションから該当するものを選択します。

オプション	説明
Cflowd Template（**show app cflowd template**）	Cflowd テンプレートを表示します。
Cflowd Collector（**show app cflowd collector**）	Cflowd コレクタの情報を表示します。
Cflowd Flows（**show app cflowd flows**, **show app cflowd flow-count**）	Cflowd フローを表示します。
Cflowd Statistics（**show app cflowd statistics**）	Cflowd 統計情報を表示します。

Cloud Express 情報の表示

Cloud Express 情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]**の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストで、次のコマンドのいずれかを選択します。

デバイスオプション	コマンド	説明
Cloud Express アプリケーション	show sdwan cloudexpress applications	Cisco IOS XE SD-WAN デバイスに設定されている各 SaaS アプリケーションに対して Cloud onRamp for SaaS が選択した最適なパスを表示します。
Cloud Express Gateway Exits	`show sdwan cloudexpress gateway-exits`	Cisco IOS XE SD-WAN デバイス 上の Cloud onRamp for SaaS について、ゲートウェイサイトから受信した Quality of Experience（QoE）の測定値を表示します。
Cloud Express Local Exits	`show sdwan cloudexpress local-exits`	Cisco IOS XE SD-WAN デバイス で Cloud onRamp for SaaS プローブが有効になっているアプリケーションのリストと、プローブが発生するインターフェイスを表示します。

ARP テーブルエントリの表示

Address Resolution Protocol（ARP）は、ネットワーク層アドレス（IPv4 アドレスなど）をリンク層アドレス（イーサネット、MAC アドレスなど）に解決するために使用されます。ネットワークアドレスと物理アドレス間のマッピングは、ARP テーブルに保存されます。

ARP テーブル内のエントリを表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. 右ペインの [Device Options] ドロップダウンリストから、[ARP] を選択します。

CLI での同等コマンド：**show arp**

速度テストの実行

はじめる前に

Cisco vManage の**[Administration]** > **[Settings]**で [Data Stream] が有効になっていることを確認します。

速度テストの実行

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. デバイスを選択するには、[Hostname] 列でデバイス名をクリックします。
3. 左ペインで [Troubleshooting] をクリックします。
4. [Connectivity] 領域で、[Speed Test] をクリックします。
5. 次の詳細を選択します。
   - [Source Circuit]：ドロップダウンリストから、ローカルデバイスのトンネルインターフェイスのカラーを選択します。
   - [Destination Device]: ドロップダウンリストから、デバイス名とシステム IP アドレスでリモートデバイスを選択します。
   - [Destination Circuit]：ドロップダウンリストから、リモートデバイスのトンネルインターフェイスのカラーを選択します。
6. [Start Test] をクリックします。

   速度テストでは、送信元から宛先に単一パケットを送信し、宛先から確認応答を受信します。

右ペインの中央に、速度テストの結果が表示されます。クロックは、ラウンドトリップ時間に基づいて回線速度を報告します。ダウンロード速度は送信元から宛先までの速度を、アップロード速度は宛先から送信元までの速度を共に Mbps 単位で示します。回線に設定されたダウンストリームおよびアップストリーム帯域幅も表示されます。

速度テストが完了すると、テスト結果が右ペインの下部にある表に追加されます。

Network-Wide Path Insight の表示

表 *4 :* 機能の履歴

機能名	リリース情報	説明
Cisco vManage の Network-Wide Path Insight	Cisco IOS XE リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能では、Cisco vManage を使用してネットワーク全体のパスのトレース情報を表示できます。
Cisco vManage の Network-Wide Path Insight 拡張版	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、Network-Wide Path Insight のトレースが強化されます。これには、トレースや DNS ドメイン検出用の追加のフィルタとオプション、およびアプリケーションフロー、トレースビュー、アプリケーショントレンドの新たな表示が含まれます。
Cisco vManage の Network-Wide Path Insight 拡張版	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能により、Network-Wide Path Insight 機能が拡張されます。これには、インサイト情報、トレースレベルのインサイト情報、パスインサイト情報、および詳細なアプリケーショントレース情報の収集と表示が含まれます。

Network-Wide Path Insight について

Network-Wide Path Insight は、Cisco SD-WAN ネットワーク内にあるオンデマンドのエンドツーエンドアプリケーションのトレースサービスを提供します。パケットレベル、アプリケーションレベル、ドメインレベル、フローレベル、およびネットワークレベルで詳細情報を取得して表示できます。この情報により、ネットワークの運用に関する包括的なインサイトが得られ、パフォーマンス分析、計画、およびトラブルシューティングに役立ちます。

サポートされるデバイス数

この機能は、 Cisco IOS XE SD-WAN デバイスでサポートされています。

概要

Network-Wide Path Insight 機能を使用すると、Cisco vManage でアプリケーションのトレースを開始し、複数のデバイスから収集されたトレース結果を統合ビューで表示できます。

Network-Wide Path Insight のメリット

- Cisco SD-WAN ファブリックを介してアプリケーションのエンドツーエンドの双方向ネットワークパスを可視化
- アプリケーションのネットワークパフォーマンスをリアルタイムで測定して可視化
- Cisco SD-WAN デバイスでの機能実行に関するインサイト。例：QoS、SD-WAN ポリシー、SAIE フロー、および SD-WAN オーバーレイトンネリング

（注） Cisco vManage リリース 20.7.x 以前では、SD-WAN アプリケーション インテリジェンス エンジン（SAIE）フローは、ディープ パケット インスペクション（DPI）フローと呼ばれていました。

- アプリケーションポリシーの検証

Network-Wide Path Insight の使用例

- 新しいサイト、VPN、アプリケーションを展開する際のネットワークとポリシー設計の検証
- ネットワーク、アプリケーション、およびポリシー処理の日々のモニタリング
- 運用上の問題を診断するための情報収集

Network-Wide Path Insight の制約事項

- Cisco vEdge デバイス では、Cisco IOS XE SD-WAN デバイスと相互運用する場合にのみこの機能を使用できます。
- Network-Wide Path Insight 機能を使用してトレースできるのは、UDP と TCP のみです。
- この機能は、VPN 0 やトランスポート VPN ではサポートされていません。
- Cisco SD-WAN の環境でエクストラネット VPN またはサービス チェーンポリシーが設定されている場合、この機能はサポートされません。
- すべてのパケットトレースがフローごとにキャプチャされるわけではありません。最も典型的なパケットのサンプルが自動的に取得されます。
- フローレコードには、Cisco vManage リリース 20.6.1 より前のリリースのフローパスとホップ情報の完全な履歴は表示されません。

- Cisco vManage リリース 20.6.1 より前の場合、混合アプリケーションポリシーとデフォルトポリシーはサポートされていません。
- デバイスごとに最大 2 つのトレース、および Cisco vManage テナントごとに 10 の同時アクティブトレースをモニタリングできます。
- モニタリング可能なアクティブフロー数と、サポートされている完了フロー数を次の表に示します。モニタリングの限界に達すると、トレースは停止します。

リリース	サポートされるアクティブフロー数	サポートされる完了フロー数
Cisco vManage リリース 20.6.1 より前のリリース	Cisco IOS XE SD-WAN デバイス に応じて 50 ～ 100	1,000
Cisco vManage リリース 20.6.1 以降のリリース	Cisco IOS XE SD-WAN デバイス に応じて 50 ～ 100	10,000

- Cisco vManage リリース 20.6.1 より前の場合、次の最適化が有効になっていると、フロートレースで完全なネットワークパスは表示されません。
  - UTD
  - TCP
  - SSL
  - DRE

Network-Wide Path Insight の前提条件

Cisco vManage で [Data Stream] オプションが有効になっていることを確認します。このオプションを有効にするには、次の手順に従います。

1. Cisco vManage のメニューから **[Administration]** > **[Settings]** の順に選択します。
2. [Data Stream] オプションで、[View] をクリックします。
3. [Edit] をクリックし、[Enable] を選択します。
4. [Save] をクリックします。

（注） [Data Stream] が有効になっていないときにトレースパスを設定しようとすると、有効にするように求められます。

Network-Wide Path Insight の表示（Cisco vManage リリース 20.6.1 より前の場合）

ここでは、Cisco vManage リリース 20.6.1 より前のリリースで Network-Wide Path Insight のトレースを実行する方法について説明します。トレースを開始するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Network Wide Path Insight]**の順に選択します。
2. [Policy] 領域で、ドロップダウンリストから [Site ID(*)] を選択します。アクセス権のあるサイトのみを選択してください。
3. [VPN(*)] フィールドで、ドロップダウンリストから VPN ID を選択します。選択したサイトに関連付けられている VPN のみが一覧表示されます。
4. （任意）送信元と宛先の IP アドレスを [Source/ Destination IP Addresses] に入力します。
5. （任意）ドロップダウンリストから [Application] を選択します。
6. （任意）必要なトレース期間を分単位で [Trace Duration] に指定します。デフォルトのトレース期間は 60 分です。指定できる最長期間は 1440 分です。
7. （任意）ドロップダウンリストで [Device] と [Source Interface] を選択します。
8. （任意）ドロップダウンリストで [Protocol] を選択します。[TCP] および [UDP] プロトコルがサポートされています。[All] オプションは、UDP プロトコルと TCP プロトコルの両方を示します。
9. （任意）ドロップダウンリストで [DSCP] を選択します。
10. [Start] をクリックしてパストレースを開始します。ダイアログボックスに、トレース ID、トレースの開始時刻、およびトレースが開始されたデバイスの IP アドレスやトレースステータスなどの詳細がすべて表示されます。

（注） タイマーが期限切れになる前に進行中のトレースを停止するには、[Stop] をクリックします。[Trace History] セクションからトレースを停止することもできます。

Network-Wide Path Insight の表示 （Cisco vManage リリース 20.6.1 以降の場合）

ここでは、Cisco vManage リリース 20.6.1 以降のリリースで Network-Wide Path Insight のトレースを実行する方法について説明します。

トレースにより、アプリケーションの問題に関する詳細情報が得られます。また、ドメインやドメインで実行中のアプリケーションを検出できます。さまざまなオプションを設定して、必要なトレースを指定し、トレースフローに関する詳細情報を表示できます。

トレースを開始するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Tools]** > **[Network Wide Path Insight]**の順に選択します。

（注） Cisco vManage リリース 20.6.x 以前では、[Network Wide Path Insight] は [Monitor] メニュー内にあります。

2. （任意）[Trace] 領域で、[Enable DNS Domain Discovery] チェックボックスをオンにすると、Network-Wide Path Insight で DNS ドメイン検出が有効になります。

   このオプションを有効にすると、DNS スヌーピングを使用して、DNS ドメインと、検出されたドメインで実行中のアプリケーションが検出されます。次に、[Application] オプションでドメインをモニタリングすると、正常性、トレンド、およびメトリックに関する情報を取得できます。このオプションを無効にすると、指定した条件とフィルタに基づいてアプリケーションフローがモニタリングされます。

3. [New Trace] をクリックします。

4. （任意）[Trace Name] フィールドに、トレースの名前を入力します。

   名前を入力しない場合、システムは trace_*ID* という名前を割り当てます。この *ID* は、システムが生成したトレースの ID です。

5. [Trace Duration] フィールドに、トレースを継続する期間を分単位で入力します。

   最小値は 1 です。最大値は 1440（24 時間）です。デフォルト値は 60 です。

6. [Filters] 領域では、次のアクションを実行します。

   1. [Site ID] フィールドに、トレースを実行する Cisco SD-WAN ネットワークサイトの ID を入力します。

   2. [VPN] ドロップダウンリストで、モニタリングするサービス VPN を選択します。

   3. （任意。このオプションは、DNS ドメイン検出が無効になっている場合にのみ適用されます。）[Source Address/Prefix] フィールドに、モニタリングする送信元 IPv4 または IPv6 IP アドレスとフローのプレフィックスを入力します。このフィールドを空白のままにすると、トレース機能は任意の送信元アドレスまたはプレフィックスを持つフローを監視します。

   4. （任意。このオプションは、DNS ドメイン検出が無効になっている場合にのみ適用されます。）[Destination Address/Prefix] フィールドに、モニタリングする宛先 IPv4 または IPv6 IP アドレスとフローのプレフィックスを入力します。このフィールドを空白のままにすると、トレース機能は任意の宛先アドレスまたはプレフィックスを持つフローを監視します。

   5. （任意。このオプションは、DNS ドメイン検出が有効になっている場合にのみ適用されます。）[Client Address/Prefix] フィールドに、モニタリングする送信元 IPv4 または IPv6 IP アドレス、フローのプレフィックスを入力します。このフィールドを空白のままにすると、トレース機能は任意の送信元アドレスまたはプレフィックスを持つフローを監視します。

6. （任意。[Application] オプションは、DNS ドメイン検出が無効になっている場合にのみ適用されます。）次のオプションのいずれかをクリックしてから、オプションの下のフィールドをクリックし、表示されるチェックボックスを使用して、モニタリングするアプリケーションまたはアプリケーショングループを選択します。

   - [Application]：このオプションを選択すると、トレース機能で監視する特定のアプリケーションを指定できます。
   - [Application Group]：このオプションを選択すると、トレース機能で監視する特定のアプリケーショングループを指定できます。

   オプションを選択しない場合、トレース機能はすべてのアプリケーションを監視します。

   このフィールドからアプリケーションまたはアプリケーショングループを削除するには、対応するアプリケーションまたはアプリケーショングループ名の横にある [X] をクリックします。

7. （任意）DNS ドメイン検出が無効になっている場合は、[Expand] アイコンをクリックして [Advanced Filters] 領域を展開します。必要に応じて次のアクションを実行して、トレース機能でモニタリングする特定の項目を設定します。

   1. [Device] ドロップダウンリストから、各デバイスのチェックボックスをオンにして、モニタリングする 1 つ以上のデバイスを選択します。

      デバイスを選択しない場合、ステップ 6 （25 ページ） で指定したサイトのすべてのデバイスがトレース機能によって監視されます。

   2. [Source Interface] ドロップダウンリストで、モニタリングする送信元インターフェイスを選択します。

      送信元インターフェイスを選択しない場合、ステップ 6 （25 ページ） で指定した VPN のすべての送信元インターフェイスからのトラフィックが、トレース機能によって監視されます。

   3. [Source Port] フィールドには、モニタリングするトラフィックの送信元ポート番号を入力します。トレース機能は、このポート番号からフローするトラフィックを監視します。

      送信元ポートを選択しない場合、トレース機能はすべての送信元ポートのトラフィックを監視します。

   4. [Destination Port] フィールドには、モニタリングするトラフィックの宛先ポート番号を入力します。トレース機能は、このポート番号にフローするトラフィックを監視します。

      宛先ポートを選択しない場合、トレース機能はすべての宛先ポートのトラフィックを監視します。

   5. [Protocol] ドロップダウンリストで、モニタリングするトラフィックのプロトコルタイプを選択します。

プロトコルを選択しない場合、トレース機能はサポートされているすべてのプロトコルのトラフィックを監視します。

6. [DSCP] ドロップダウンリストで、モニタリングする DSCP タイプを選択します。[DEFAULT] を選択すると、DSCP タイプは「DSCP0」になります。

   DSCP タイプを選択しない場合、トレース機能はすべての DSCP タイプのトラフィックを監視します。

8. （任意）[Expand] アイコンをクリックして [Monitor Settings] 領域を展開し、次のアクションを実行します。

   1. （Cisco vManage リリース 20.9.1 以降）[QoS Insight] をクリックすると、すべてのトラフィックのアプリケーション、VPN、インターフェイス、およびキュー レベルのスループットとドロップ率のメトリックがトレースの対象になります。

      このオプションは、デフォルトで有効です。

   2. TCP トラフィックのアプリケーション応答時間（ART）メトリックをトレースの対象にするには、[ART Visibility] をクリックします。このメトリックには、クライアントネットワーク遅延（CND）およびサーバーネットワーク遅延（SND）の情報が含まれます。

      DNS ドメイン検出が有効になっている場合、このオプションはデフォルトで有効になっています。

   3. [App Visibility] をクリックすると、トレース機能は SD-WAN Application Intelligence Engine（SAIE）フローを使用してアプリケーションとアプリケーショングループを検出します。

      （注） Cisco vManage リリース 20.7.x 以前では、SAIE フローはディープ パケット インスペクション（DPI）フローと呼ばれていました。

      ステップ 6 （25 ページ） でアプリケーションまたはアプリケーショングループを選択した場合、このオプションは自動的に有効になります。

   4. [DIA Visibility] をクリックすると、ダイレクト インターネット アクセス フローからのダウンストリーム情報を最初のフローから表示できます。

      DNS ドメイン検出が有効になっている場合、このオプションはデフォルトで有効になっています。

      このオプションは、Cisco SD-WAN トンネル経由で転送されるアプリケーションには影響しません。

      このオプションを有効にしない場合、デバイスはダイレクトインターネットアクセス トラフィックを自動的に検出しますが、この検出が開始されるまでに時間がかかることがあります。

5. フローの方向に関係なく、すべてのフローをトレース対象にするには、ハブスポークトポロジのハブサイトでトレースを開始するときに [Hub WAN Visibility] をクリックします。

   デフォルトでは、トレース機能は LAN から WAN への方向のトラフィックを監視します。[Hub WAN Visibility] オプションが無効になっている場合、WAN から WAN へのトランジットフローはトレースの対象に含まれず、WAN から LAN 方向にフローする最初のいくつかのパケットは監視されません。

   ハブスポークトポロジのスポークサイトでトレースを開始する場合、[Hub WAN Visibility] オプションは適用されません。

   DNS ドメイン検出が有効になっている場合、[Hub WAN Visibility] オプションはデフォルトで有効になっており、無効にすることはできません。

6. トレース時のサンプリングを有効にするには、[Sampling] をクリックしてします。これにより、トレース機能は指定された間隔でフローをキャプチャします。

   表示される [Sampling Interval] フィールドに、サンプルの間隔を秒単位で入力します。たとえば、100 と入力すると、他のフローが複数ある場合でも、100 秒ごとに 1 つのフローがトレースされます。

   サンプリング間隔の最小値は 1 秒です。最大値は 86400 秒（24 時間）です。デフォルト値は 60 です。

   サンプリングオプションは、トレース内のフローの最大数に達するまで時間を増やすことで、トレースのモニタリング期間を延長するのに役立ちます。

9. [Start] をクリックしてトレースを開始します。

   [Start Trace] ウィンドウにはトレースに関する情報が表示されます。トレース ID、トレースの開始時刻、およびトレースが開始されたデバイスの IP アドレスやトレースステータスといった関連情報が含まれます。

10. [Start Trace] ウィンドウを閉じます。

    [Tools] > **[Network Wide Path Insight]** ウィンドウにトレースのリストが表示されます。

（注） Cisco vManage リリース 20.6.x 以前では、トレースのリストは**[Monitor]** > **[Network Wide Path Insight]**ページに表示されます。

トレース履歴

パストレースインスタンスは、一意のトレース ID とともに [Trace History] 領域（Cisco vManage リリース 20.6.1 より前）または [Trace] 領域（Cisco vManage リリース 20.6.1 以降）に表示されます。状態や実行できるアクションなど、各インスタンスに関する情報も表示されます。

[Trace History] 領域では、次のアクションを実行できます。

- Cisco vManage リリース 20.6.1 より前：

- 実行中のトレースを停止するには、[Stop] をクリックします。トレース期間を指定した場合、タイマーが切れるとトレースは自動的に停止します。
- [Flow Path and Metrics] セクションに移動するには、[Detail] をクリックします。

- Cisco vManage リリース 20.6.1 以降では、次のアクションを実行できます。
  - 進行中のトレースを停止するには、トレースの [Action] 列で [Stop] をクリックします。次に、[Stop Trace] ダイアログボックスで [Confirm] をクリックします。
  - 完了したトレースを削除するには、トレースの [Action] 列で [Delete] をクリックします。次に、[Delete Trace] ダイアログボックスで [Confirm] をクリックします。
  - （Cisco vManage リリース 20.9.1 以降）トレース レベルのインサイト情報を表示するには、[Trace Name] 列の [Insight Summary] をクリックします。
  - [Insight] 領域にトレース対象のフローに関する詳細情報を表示するには、トレースの [Action] 列で [View Insight] をクリックします。
  - トレースのフィルタと設定を表示するには、[Trace Name] 列で対応する名前をクリックします。
  - トレースの送信元に関する情報を表示するには、[Src Site] 列で対応する値をクリックします。
  - トレース機能で監視するアプリケーションまたはアプリケーショングループに関する情報を表示するには、[Application/App Group] 列で対応する値をクリックします。
  - 生成されたトレースメッセージとエラーメッセージのステータスを表示するには、[Trace State] 列で対応する値をクリックします。

フローパスとメトリック

このセクションは、Cisco vManage リリース 20.6.1 より前のリリースに適用されます。

[Flow Path and Metrics] セクションで、ホップごとのメトリックを含む双方向フローパステーブルを表示します。ログ内のトレースインスタンスを展開して、次の詳細を表示できます。

カラム	説明
Last Update Time	実行状態のフローパスインスタンスが 10 秒ごとに更新され、更新時刻が表示されます。
Flow ID	フロー ID は、異なる時間に発生する 2 つの同一のフローパスインスタンスを区別します。
State	この状態は、フローの潜在的な問題を可視化するのに役立ちます。フローの SLA 状態のみがサポートされます。

カラム	説明
Direction	方向はアップストリームまたはダウンストリームです。最初のパケットフローが識別される方向が、アップストリームと見なされます。
Local Color、Remote Color	ローカルエッジ（送信元）とリモートエッジ（宛先）の色は、異なる WAN インターフェイスを示します。
Local Drop(%)、Remote Drop(%)、WAN Drop(%)	パケットドロップは、ローカルおよびリモートのエッジルータで測定されます。パケットドロップは、WAN ネットワーク全体でも測定されます。
Jitter(ms)、Latency(ms)	フローのジッターと遅延のメトリック。これらのメトリックは、アプリケーションのパフォーマンスをリアルタイムで評価するのに役立ちます。
Total Packets、Total Bytes	フローの各方向について、総パケット数と総バイト数が表示されます。

インサイト

このセクションは Cisco vManage リリース 20.6.1 以降に適用されます。

トレースのリストで [View Insight] をクリックすると、対応するトレースのフローに関する詳細情報が表示されます。この詳細情報は [Insight] 領域に表示されます。この領域には、次の情報が表示されます。

- [DNS Domains] タブは、DNS ドメイン検出が有効になっている場合にのみ使用できます。トレースで検出された各ドメインに関する情報が表示されます。リストの任意の行を展開して、アプリケーションに関する詳細情報を表示できます。

  Cisco vManage リリース 20.9.1 で [Discovered Domains] をクリックすると、トレースで検出されたが、トレースがまだ実行されていないすべてのドメインの情報が表示されます。[Monitored Domains] をクリックすると、トレースで監視されたドメインの情報のみが表示されます。

（注） Cisco vManage リリース 20.6.1 から Cisco vManage リリース 20.8.x では、[DNS Domains] タブは [Applications] タブという名称になっています。

- （Cisco vManage リリース 20.9.1 以降）[Applications] タブには、トレースされたアプリケーションに関する情報が表示されます。このリストの任意の行を展開して、各アプリケーションのホップごとのメトリックを含む双方向パス情報を表示できます。

- [Active Flows] タブには、実行状態のフローに関する情報が表示されます。フローインスタンスを展開して、ホップごとのメトリックに加えて、双方向フローパス情報を表示できます。
- [Completed Flows] タブには、停止状態のフローに関する情報が表示されます。フローインスタンスを展開して、ホップごとのメトリックに加えて、双方向フローパス情報を表示できます。
- [DNS Domains] タブでは、アクティブなトレースについて、選択したドメイン内にあるアプリケーションのフローモニタリングを開始または停止します。フローのモニタリングを開始すると、WAN 上のドメインの HTTP プローブ（Cisco vManage リリース 20.8.x まで）または HTTPS プローブ （Cisco vManage リリース 20.9.1 以降） も展開されます。モニタリングが開始されたことを示すダイアログボックスが表示されます。モニタリング情報は、[Active Flows] タブと [Completed Flows] タブに表示されます。
  - Cisco vManage リリース 20.6.1 から Cisco vManage リリース 20.8.x では、必要に応じて [Start Flow Monitor] および [Stop Flow Monitor] をクリックして、選択したドメインのモニタリングを開始または停止します。
  - Cisco vManage リリース 20.9.1 以降では、フローのモニタリングを開始するには、[Discovered Domains] をクリックし、モニタリングを開始する 1 つ以上のドメインの対応するチェックボックスをオンにして、[Start Flow Monitor] をクリックします。表示される確認ダイアログボックスで [Confirm] をクリックします。[Confirm] をクリックする前に、このダイアログボックスでドメインの選択を変更できます。

    Cisco vManage リリース 20.9.1 以降では、フローのモニタリングを停止するには、[Monitored Domains] をクリックし、モニタリングを停止するそれぞれのドメインでチェックボックスをオフにして、[Stop Flow Monitor] をクリックします。表示される確認ダイアログボックスで [Confirm] をクリックします。
- [Search] オプションを使用すると、特定のフローインスタンスを検索できます。
- 完了したフローの場合は、[Filter] オプションを使用すると、指定した条件を満たすトレースインスタンスのみが表示されます。
- 完了したフローについては、発生した期間を指定して、フローの表示を制限できます。1 分、10 分、30 分、または 1 時間、2 時間、5 時間から選択できます。[Custom] をクリックして、日付と時刻の範囲を入力することもできます。

次の表では、各アプリケーションとフロー内の各インスタンスについて表示される情報、および DNS ドメイン検出が有効になっている場合は各ドメインについて説明しています。

表 *5 : DNS* ドメイン検出が有効な場合にのみ使用可能な*[DNS Domains]* タブ（*Cisco vManage* リリース *20.6.1* ～ *Cisco Manage 20.8.x* では *[Applications]* タブ）

カラム	説明
Check box	モニタリングを有効または無効にするドメインのチェックボックスをオンまたはオフにして、[Start Flow Monitor] または [Stop Flow Monitor] をクリックします。
Domain	トレースで検出されたドメイン名。
Update Time	情報が最後に更新された日時。 インスタンスは、デフォルトでは30秒ごとに更新されます。
Application	トレースで検出されたドメイン内のアプリケーション名。
Application Group	トレースで検出されたアプリケーショングループ名。
DNS Server	クライアントから送信されたDNSパケットの宛先。
DNS Redirect	リゾルバが集中型ポリシーまたは Cisco Umbrella で設定されている場合に、デバイスがDNSトラフィックをリダイレクトするDNSリゾルバ。
Resolved IP	アプリケーションの DNS で解決された IP アドレス。
DNS Transport	ドメインで使用されるトランスポートタイプ。
DNS Egress	ドメインで使用される出力インターフェイスとタイプ。
TTL（sec）	DNS の存続時間（秒）。
Request	送信された DNS パケット数。
Monitor State	ドメインのフローモニタリングのステータス。

表 *6 : [Applications]* タブ（*Cisco vManage* リリース *20.9.1* 以降）

カラム	説明
Last Update Time	情報が最後に更新された日時。 インスタンスは、デフォルトで10秒ごとに更新されます。
App Name	アプリケーションの名前。
App Group	アプリケーションが属するアプリケーショングループの名前。
Upstream Flow Count	アプリケーションでカウントされたアップストリームフローの数。
Downstream Flow Count	アプリケーションでカウントされたダウンストリームフローの数。
Upstream Bytes（K）	このアプリケーションのアップストリームトラフィック量（KB）
Downstream Bytes（K）	このアプリケーションのダウンストリームトラフィック量（KB）

表 *7 : [Active Flows]* タブと *[Completed Flows]* タブ

カラム	説明
Last Update Time	情報が最後に更新された日時。 インスタンスは、デフォルトで10秒ごとに更新されます。
Flow ID	システムによって割り当てられたフローの識別子。

カラム	説明
Readout	フローに含まれる情報（エラー、警告、情報）。アイコンをクリックすると、フローに関する詳細情報がダイアログボックス（Cisco vManage リリース 20.9.1 より前のリリース）またはスライドインペイン（Cisco vManage リリース 20.9.1 以降のリリース）に表示されます。フローでアプリケーションの問題が特定された場合、この情報は根本原因の分析に役立ちます。 ダイアログボックスまたはスライドインペインには、次の情報が表示されます。 • [Overview]：フローの非対称性、双方向 WAN カラーの不整合、QoS 輻輳、LAN または WAN パケットドロップ、SLA 違反、パス変更、フローリセット、SAIE パケット分類ステータス、TCP サーバー応答などに関する詳細が含まれます。 • [Path Insight]（Cisco vManage リリース 20.9.1 以降）：フローの転送パスがどのように決定されたかについての情報を提供します。この情報には、エッジルータ名、宛先 IP アドレス、IP アドレスの検索と一致したルート情報。ルート受信ソースプロトコル、プリファレンス、メトリック、フローのパスルーティング候補。フローパスの決定方法、NAT 変換の詳細。使用されたフローパスが含まれます （水平スクロールバーにアクセスするには、[Path Insight] タブの一番下までスクロールする必要がある場合があります）。 （注） Cisco vManage リリース 20.7.x 以前では、SD-WAN アプリケーションインテリジェンスエンジン（SAIE）フローは、ディープ パケット インスペクション（DPI）フローと呼ばれていました。
Source IP	トレースで監視されるトラフィックの送信元 IP アドレス。

カラム	説明
Source Port	トレースで監視されるトラフィックの送信元ポート。
Destination IP	トレースで監視されるトラフィックの宛先 IP アドレス。
Destination Port	トレースで監視されるトラフィックの宛先ポート。
Protocol	トレースで監視されるトラフィックのプロトコル。
DSCP Upstream/Downstream	トレースで監視されるアップストリーム トラフィックとダウンストリーム トラフィックの DSCP タイプ。
Application	フローで監視されるアプリケーション。
Application Group	フローで監視されるアプリケーショングループ。
Domain	フローが属するドメイン。 ドメイン名をクリックすると、ドメインが認識されたプロトコルが表示されます。
ART CND（ms）/SND（ms）	クライアントネットワーク遅延（CND）およびサーバーネットワーク遅延（SND）のアプリケーション応答時間（ミリ秒）。

表 *8*：拡張 *DNS* ドメイン情報（*Cisco vManage* リリース *20.6.1* から *Cisco Manage 20.8.x* では拡張アプリケーション情報と呼ばれました）

カラム	説明
Egress Interface	ドメインで使用される出力インターフェイス。
Local Edge, Remote Edge	フローのローカルエッジ（送信元）とリモートエッジ（宛先）の名前。
Local Color	出力 WAN インターフェイスを示す、フローのローカルエッジ（送信元）のカラー。
Remote Color	入力 WAN インターフェイスを示す、フローのリモートエッジ（宛先）のカラー。

カラム	説明
App CND（ms）/App SND（ms）	クライアントネットワーク遅延（CND）およびサーバーネットワーク遅延（SND）のアプリケーション応答時間（ミリ秒）。
HTTP Probe Response Time（ms）	デバイスからアプリケーションサーバーに対するHTTPプローブping実行時の応答時間（ミリ秒）。
HTTP Probe Loss（%）	デバイスからアプリケーションサーバーに対する HTTP プローブ ping 実行時のパケット損失率。
Path Score	デバイスからアプリケーションサーバーに対するHTTPプローブping実行時のパススコア。

表 *9 :* 拡張アプリケーション情報（***Cisco vManage*** リリース ***20.9.1*** 以降）

カラム	説明
Direction	アプリケーションフローの方向（**upstream** または **downstream**）。 フローで識別される最初のパケットが、アップストリーム方向のフローとして表示されます。
HopIndex	アプリケーションの各方向のホップインデックス番号。
Local Edge	アプリケーションのローカルエッジデバイス（送信元）の名前。
Remote Edge	アプリケーションのリモートエッジデバイス（宛先）の名前。
Local Color	出力 WAN インターフェイスを示す、アプリケーションのローカルエッジデバイス（送信元）のカラー。
Remote Color	入力 WAN インターフェイスを示す、アプリケーションのリモートエッジデバイス（宛先）のカラー。
Local Drop（%）、WAN Drop（%）、Remote Drop（%）	ローカルおよびリモートエッジルータで測定されたパケットドロップ。パケットドロップも WAN ネットワーク全体で測定されます。

カラム	説明
Jitter（ms）、Latency（ms）	アプリケーションのジッターと遅延のメトリック。これらの値は、アプリケーションのパフォーマンスをリアルタイムで評価するのに役立ちます。
ART CND（ms）/SND（ms）	クライアントネットワーク遅延（CND）およびサーバーネットワーク遅延（SND）のアプリケーション応答時間（ミリ秒）。
Total Packets、Total Bytes	アプリケーションフローの各方向について、総パケット数とパケットの総バイト数。

表 *10*：拡張フローインスタンス情報

カラム	説明
Direction	フローの方向（**upstream** または **downstream**）。 フローで識別される最初のパケットが、アップストリーム方向のフローと見なされます。
HopIndex	フローの各方向のホップインデックス番号。
Local Edge	フローのローカルエッジ（送信元）の名前。
Remote Edge	フローのリモートエッジ（宛先）の名前。
Local Color	出力 WAN インターフェイスを示す、フローのローカルエッジ（送信元）のカラー。
Remote Color	入力 WAN インターフェイスを示す、フローのリモートエッジ（宛先）のカラー。
Local Drop（%）、WAN Drop（%）、Remote Drop（%）	ローカルおよびリモートエッジルータで測定されたパケットドロップ。パケットドロップは、WAN ネットワーク全体でも測定されます。
Jitter（ms）、Latency（ms）	フローのジッターと遅延のメトリック。これらの値は、アプリケーションのパフォーマンスをリアルタイムで評価するのに役立ちます。
ART CND（ms）/SND（ms）	クライアントネットワーク遅延（CND）およびサーバーネットワーク遅延（SND）のアプリケーション応答時間（ミリ秒）。

カラム	説明
Total Packets、Total Bytes	フローの各方向について、総パケット数とパケットの総バイト数。
Queue Id	フローの QoS キューの識別子。
QDepthLimit/Max/Min/Avg	フローの QoS キュー深度の制限値、最大値、最小値、および平均値。

インサイトサマリー

最小リリース：Cisco vManage リリース 20.9.1

トレースのリストで [Insight Summary] をクリックすると、アプリケーショントラフィックとフローに関するトレース レベルのインサイト情報がスライドイン ペインに表示されます。このスライドインペインは、次のタブで構成されています。

- [Overview] タブ：次の情報が表示されます。
  - [Applications] グラフ：監視対象トラフィックの各アプリケーションでトレース機能が検出したフロー数が表示されます。グラフ内のデータポイントにカーソルを合わせると、対応するアプリケーションフローが示す合計フローの割合が表示されます。
  - [Events] グラフ：監視対象のトラフィックでトレース機能が検出したイベントと、各イベントで影響を受けたアプリケーションフロー数が表示されます。グラフ内のデータポイントにカーソルを合わせると、対応するイベントで影響を受けた合計アプリケーションフローの割合が表示されます。
  - [Hotspot Issues]：イベントごとに、影響を受けた各アプリケーションフローに関する情報（イベントが発生したトラフィックパスやイベントの期間など）が表示されます。

    この情報は、イベントごとに [Events] フィールドに表示されます。デフォルトでは、トレースで検出されたすべてのイベントがこのフィールドに表示されます。名前の横にある [X] をクリックしてイベントを削除できます。また、[Events] ドロップダウンリストからイベントを選択して追加することもできます。

（注） [Event Insight] タブでは、イベントに関するより詳細な情報を表示できます。

- [App Performance Insight] タブ：選択したアプリケーションとホップに関する次のパフォーマンス情報が表示されます。
  - [Score] グラフ：アプリケーションのパフォーマンスの評価が提供されます。
  - [Loss] グラフ：パケット損失に関する情報が提供されます。

- [Delay] グラフ：トラフィックの遅延に関する情報が提供されます。
- [Jitter] グラフ：遅延間のドリフトに関する情報が提供されます。
- [CND/SND] グラフ：クライアントネットワーク遅延（CND）およびサーバーネットワーク遅延（SND）に関する情報が提供されます。
- [Applications Path & Performance] サンキーチャート：特定の時点における帯域幅と損失情報のスナップショットが提供されます。

グラフでは、[Application] フィールドに各アプリケーションの情報が表示され、[Hop] フィールドにホップの情報が表示されます。サンキーチャートでは、アプリケーションごとに情報が [Application] フィールドに表示されます。また、すべてのホップについても [Application] フィールドに表示されます。

デフォルトでは、ホットスポットの問題が最も多い 5 つのアプリケーションが [Application] フィールドに表示されます。名前の横にある [X] をクリックしてアプリケーションを削除できます。また、[Application] ドロップダウンリストからアプリケーションを選択して追加することもできます。ホップは [Hop] ドロップダウンリストから選択できます。

[Upstream] をクリックすると、アップストリームトラフィックの情報がグラフとチャートに表示されます。[Downstream] をクリックすると、ダウンストリームトラフィックの情報がグラフとチャートに表示されます。

グラフ内のデータポイントにカーソルを合わせると、より詳細な情報が表示されます。グラフ内のデータポイントをクリックすると、そのデータポイントのサンキーチャートが更新されます。サンキーチャート内のデータポイントにカーソルを合わせると、より詳細な情報が表示されます。

- [Event Insight] タブ：イベント発生時に影響を受けたアプリケーションフローに関する次の情報が、分単位で表示されます。この情報は根本原因の分析に役立ちます。
  - [Flows] グラフ：特定の時点におけるフロー数に関する情報が提供されます。
  - [Applications Path & Event] サンキーチャート：指定したイベントが特定の時点に受けた影響に関する詳細情報が提供されます。データポイントにカーソルを合わせると、詳細が表示されます。

グラフでは、[Application] フィールドに各アプリケーションの情報が表示され、[Hop] フィールドにホップの情報が表示されます。サンキーチャートでは、アプリケーションごとに情報が [Application] フィールドに表示されます。また、ホップは [Hop] フィールドに、イベントは [Events] フィールドに表示されます。

デフォルトでは、ホットスポットの問題が最も多い 5 つのアプリケーションが [Application] フィールドに表示されます。名前の横にある [X] をクリックしてアプリケーションを削除できます。また、[Application] ドロップダウンリストからアプリケーションを選択して追加することもできます。ホップは [Hop] ドロップダウンリストから選択できます。

トレースで検出されたホットスポットイベントは、デフォルトで [Events] フィールドに表示されます。名前の横にある [X] をクリックしてイベントを削除できます。また、[Application] ドロップダウンリストからイベントを選択して追加することもできます。

[Upstream] をクリックすると、アップストリームトラフィックの情報がグラフとチャートに表示されます。[Downstream] をクリックすると、ダウンストリームトラフィックの情報がグラフとチャートに表示されます。

データポイントにカーソルを合わせると、その時点でフローに影響を与えたイベントに関する詳細情報が表示されます。データポイントをクリックすると、そのデータポイントのサンキーチャートが更新されます。サンキーチャート内のデータポイントにカーソルを合わせると、より詳細な情報が表示されます。

- [QoS Insight] タブ：どのアプリケーショントラフィックが、デバイス上のどの QoS キューに入ったかに関するネットワーク全体の情報が表示されます。これはトレースによって検出されたものです。この情報には、トラフィックのすべてのホップが含まれます。

  このタブに情報を表示するには、トレースを開始するときに [QoS Insight] オプションを有効にします。

  - [QoS Drop Rate] グラフ：選択したデバイスについて、トレース期間中のパケットまたはバイトドロップ率に関する情報が提供されます。
  - [QoS - Applications Distribution] サンキーチャート：特定の時点におけるトラフィックスペクトルと QoS 処理に関する詳細情報が提供されます。このチャートは、アプリケーションから VPN、物理インターフェイス、キューへのフローで発生する転送されたトラフィックやドロップされたトラフィックを示します。

  パケットドロップの原因となる帯域幅の消費に関する詳細情報を提供するために、このタブには、トレースの開始時に [Application] フィルタで選択したアプリケーションだけでなく、デバイス上のすべてのアプリケーションに関する情報が表示されます。また、トレースの開始時に [VPN] フィルタで選択したサービス VPN だけでなく、**VPN0** を含むすべてのサービス VPN の情報も表示されます。

  グラフとチャートの [Devices] フィールドには、各デバイスの情報が表示されます。

  チャートに表示される情報は、項目ごとに [Applications]、[VPNs]、[Interfaces]、[Queues]、および [Forward/Drop] フィールドに表示されます。パケット/秒（PPS）レートが 0.05 未満の項目を除き、トレースで検出されたすべての項目が、デフォルトでこれらのフィールドに表示されます。名前の横にある [X] をクリックして項目を削除できます。また、対応するドロップダウンリストから項目を選択して追加することもできます。

  [Packet] をクリックすると、パケットドロップ率の情報がグラフに表示され、1 秒あたりのパケット数（PPS）情報がサンキーチャートに表示されます。[Byte] をクリックすると、バイトドロップ率の情報がグラフに表示され、1 秒あたりのキロビット（Kbps）情報がサンキーチャートに表示されます。

  グラフ内のデータポイントにカーソルを合わせると、より詳細な情報が表示されます。グラフ内のデータポイントをクリックすると、そのデータポイントのサンキーチャートが更新されます。サンキーチャート内のデータポイントにカーソルを合わせると、より詳細な情報が表示されます。

トレースビュー

Cisco vManage リリース 20.6.1 より前では、[Geography View]、[Feature View（Upstream）]、および [Feature View（Downstream）] の 3 つのセクションからトレースフローを表示できます。

Cisco vManage リリース 20.6.1 以降では、[Insight] 領域でフローを展開した後、[Insight - Advanced Views] 領域のタブ（[Domain Trend]、[Flow Trend]、[Upstream Feature]、[Downstream Feature]、[Geography]）からトレースフロー情報を表示できます。

（注） Cisco vManage リリース 20.6.1 から Cisco vManage 20.8.x では、[Domain Trend] は [App Trend] というタブ名になっています。

Domain Trend

[Domain Trend] タブがあるのは Cisco vManage リリース 20.6.1 以降です。Cisco vManage リリース 20.6.1 から Cisco vManage 20.8.x では、[Domain Trend] は [App Trend] というタブ名になっています。このタブは DNS 検出が有効になっている場合にのみ表示され、アプリケーションフローのメトリックとイベントのトレンドを示します。タブ内のデータポイントにカーソルを合わせると、詳細情報が表示されます。

[Chart Metrics] ドロップダウンリストでは、情報を表示するメトリックタイプを選択できます。[Devices] ドロップダウンリストでは、データを表示する特定のデバイスを選択できます。デフォルトでは、すべてのメトリックタイプとすべてのデバイスのトレンド情報が表示されます。

発生した期間を指定して、表示するトレンド情報を制限できます。1 分、10 分、30 分、または 1 時間、2 時間、5 時間から選択できます。また、[Custom] をクリックして日付と時刻の範囲を入力することも、[Real Time] をクリックして、情報が収集されるたびに表示することもできます。

Flow Trend

[Flow Trend] タブがあるのは Cisco vManage リリース 20.6.1 以降です。このタブには、トレースフローのメトリックとイベントのトレンドが表示されます。データポイントにカーソルを合わせると、詳細情報が表示されます。

[Chart Metrics] ドロップダウンリストでは、情報を表示する特定のメトリックタイプを選択できます。[Flow Direction] ドロップダウンリストでは、データを表示するトラフィックフローの方向を選択できます。デフォルトでは、すべてのフロー方向について、遅延、ジッター、WAN 損失、平均キュー深度のトレンド情報が表示されます。

[Navigate to Event] ドロップダウンリストでは、特定のイベントに関する情報を選択できます。

発生した期間を指定して、表示するトレンド情報を制限できます。1 分、10 分、30 分、または 1 時間、2 時間、5 時間から選択できます。また、[Custom] をクリックして日付と時刻の範囲を入力することも、[Real Time] をクリックして、情報が収集されるたびに表示することもできます。

Geography View

Cisco vManage リリース 20.6.1 より前の [Geography View] セクションまたは Cisco vManage リリース 20.6.1 以降の [Geography] タブでは、選択したトレースについて、マップ上にプロットされたエンドツー エンドのトレースフローとメトリックを表示できます。トポロジグラフには、フローに含まれるデバイスに関する地理情報が表示されます。

- 地理ビューは「自動ネットワークパス検出」をサポートしています。サイトと VPN を入力するだけで、完全な**双方向のエンドツーエンド**のリアルトラフィック ネットワーク フロー パスが追跡されます。
- トポロジーの各ノードは 2 本の線で接続されています。1 本の線はアップストリーム方向を表し、もう 1 本はダウンストリーム方向を表します。
- フローメトリックで検出された問題（例：SLA 違反）は、異なる色の線で示されます。

Feature View（Upstream および Downstream）

Cisco vManage リリース 20.6.1 より前の [Feature View] セクション、または Cisco vManage リリース 20.6.1 以降の [Upstream Feature] タブと [Downstream Feature] タブでは、アップストリームとダウンストリーム機能のトレースが、関連するポリシーの詳細とともに表示されます。

フローのアップストリームとダウンストリームの詳細を表示するには、フローパスとメトリックのテーブルでフローレコードを展開します。

- 機能ビューには、フローに適用された入力および出力機能のリストと、各機能の実行結果が表示されます。
  - 一般的な入力機能には、SD-WAN ACL、NBAR、SD-WAN データポリシー、SD-WAN アプリルートポリシー、SD-WAN 転送などがあります。
  - 一般的な出力機能には、NBAR、IPSec、SDWAN QoS 出力、QoS、送信レポートなどがあります。
- Cisco vManage リリース 20.6.1 より前では、入力ビューまたは出力ビューでポリシーをクリックして、ポップアップウィンドウに詳細設定を表示し、ポリシーの挙動を検証します。Cisco vManage リリース 20.6.1 以降では、[View Policy] をクリックしてこの情報を表示し、対応するポリシーの挙動を検証します（[View Policy] は、CLI テンプレートを使用して設定されたポリシーには適用されません）。

（注） ダウンストリーム機能ビューには、同様の情報が表示されますが、ダウンストリーム方向から編成されています。

Network-Wide Path Insight のトラブルシューティング

問題

トレースの結果を表示しても、情報が表示されない。

解決方法

次の点をチェックします。

- データストリームの収集が正しく実行されていない可能性があります。この問題を解決するには、**[Administration]** > **[Settings]** > **[Data stream]**を選択し、[Disabled] をクリックしてから [Save] をクリックします。もう一度 [Data stream] をクリックし、[Enabled] をクリックします。IP アドレスタイプに [System] を選択して、[Save] をクリックします。
- トレースで DNS ドメイン検出を有効にしていて、モニタリング対象トラフィックが DNS ドメインからのものではない可能性があります。この問題を解決するには、**[Tools]** > **[Network Wide Path Insight]**を選択し、[Trace] 領域の [Enable DNS Domain Discovery] チェックボックスをオフにして、トレースを再度実行します。

問題

Cisco vManage リリース 20.6.1 より前の [Geography View] セクション、または Cisco vManage リリース 20.6.1 の [Geography] タブにデバイスの場所が表示されない。

解決方法

デバイスに GPS が設定されていることを確認します。

NMS サーバーステータスの表示

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]**の順に選択します。
2. 表示されるデバイスのリストから Cisco vManage デバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストから [NMS Server Running] を選択します。

デバイスオプション	コマンド	説明
NMS Server Running	show nms-server running	Cisco vManage NMS サーバーが稼働しているかどうかを表示します。 このデバイスオプションは、Cisco vManage リリース 20.6.1 以降で使用できます。

Cisco vBond オーケストレーション情報の表示

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストで、次のコマンドのいずれかを選択します。

デバイスオプション	CLI コマンド	説明
Orchestrator リバースプロキシマッピング	show orchestrator reverse-proxy-mapping	リバースプロキシで用に設定されているプロキシの IP アドレスとポート番号を表示します。
Orchestrator の統計情報	show orchestrator statistics	オーバーレイネットワークで Cisco IOS XE SD-WAN デバイス へのセキュアな DTLS 接続を確立して維持しているプロセスで Cisco vBond オーケストレーション が送受信したパケットに関する統計情報を表示します。
Orchestrator の有効な vManage ID	show orchestrator valid-vmanage-id	オーバーレイネットワーク内の有効な Cisco vManage インスタンスのシャーシ番号の一覧を表示します。

トレースルートの実行

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. デバイスを選択するには、[Hostname] 列でデバイス名をクリックします。
3. 左ペインで [Troubleshooting] をクリックします。
4. [Connectivity] で [Trace Route] をクリックします。
5. 次の詳細を入力します。
   - [Destination IP]：ネットワーク上のデバイスの IP アドレスを入力します。
   - [VPN]：ドロップダウンリストから、デバイスに到達するために使用する VPN を選択します。

- [Source/Interface for VPN]：ドロップダウンリストから、トレースルート プローブ パケットの送信に使用するインターフェイスを選択します。

6. [Advanced Options] をクリックします。
7. [Size] フィールドには、トレースレート プローブ パケットのサイズをバイト単位で入力します。
8. [Start] をクリックして、要求された宛先へのトレースルートをトリガーします。

右ペインの下部には、以下の情報が表示されます。

- 出力：トレースルート プローブ パケットが宛先に到達するまでにたどるパスのRAWデータ出力。
- トレースルート プローブ パケットが宛先に到達するまでにたどるパスのグラフィック表示。

トレースルートがサービス側のトラフィックを対象にしている場合、Cisco vEdge デバイス はサービス VPN のいずれかのインターフェイスからトレースルート応答を生成します。

トンネルの損失統計の表示

データプレーンのトンネル損失統計の表示

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]**の順に選択します。
2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストから、[Tunnel Statistics] を選択します。

アプリケーション認識型ルーティングのトラフィック損失の表示

1. Cisco vManage のメニューから**[Monitor]** > **[Overview]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Dashboard]** > **[Main Dashboard]**の順に選択します。
2. [Application-Aware Routing] ペインまで下にスクロールします。

show app-route statistics コマンドを使用して、アプリケーション認識型ルーティングのトラフィック損失を表示することもできます。

SAIE フローの表示

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

   Cisco vManage リリース 20.6.1 以降では、送信元 IP アドレス、宛先 IP アドレス、ポートの詳細などの詳細な SD-WAN アプリケーション インテリジェンス エンジン（SAIE）のフロー情報を表示するには、デバイスをオンデマンド トラブルシューティング リストに追加する必要があります。オンデマンド トラブルシューティング リストにデバイスを追加するには、**[Tools]** > **[On Demand Troubleshooting]**の順に選択します。

（注）
- Cisco vManage リリース 20.6.x 以前では、[On Demand Troubleshooting] は [Monitor] メニュ内にあります。
- Cisco vManage リリース 20.7.x 以前では、SAIE フローはディープ パケット インスペクション（DPI）フローと呼ばれていました。
- オンデマンドトラブルシューティングの停止を指示するシスコまたはサードパーティの API が呼び出されないようにしてください。こうした API は、オンデマンド トラブルシューティングでの情報編集の妨げになります。

   アプリケーションの可視性を高めるために、デバイスのデータ収集プロセスは集約されたアプリケーション使用状況の統計データを生成します。これにより、管理プレーンでデフォルトで処理される統計データファイルのサイズが削減されます。この機能強化により、Cisco vManage は SAIE データを効率的に収集し、管理プレーンの処理時間を短縮できます。

2. 左ペインの [Applications] で、[SAIE Applications] をクリックします。右ペインには、デバイスの SAIE フロー情報が表示されます。

（注）
- SAIE フローの使用状況を表示する場合、ピーク時の使用状況は、同じ期間の別の時間間隔よりも上の位置に表示されます。このような状況が発生するのは、Cisco vManage で表示するデータが統計データベースで利用可能になっていないためです。Cisco vManage では利用可能なデータのみが表示され、データは適切な軸にプロットされます。
- Cisco vManage リリース 20.7.x 以前では、**SAIE アプリケーション**は **DPI アプリケーション**と呼ばれていました。

右ペイン上部は、次の要素から構成されています。

- フィルタオプション：[Filter] オプションをクリックすると、目的の VPN やローカル TLOC を選択するためのドロップダウンメニューが表示されます。[Search] をクリックします。データを表示する事前定義した期間またはカスタム期間をクリックします。

（注） [Local TLOC : Dia] のフィルタリングは Cisco vEdge デバイスでのみサポートされています。

- グラフィック形式の SAIE フロー情報。
- SAIE フローグラフの凡例：アプリケーションファミリを選択すると、そのフローに関する情報のみが表示されます。合計ネットワークトラフィックの割合でフロー情報を表示するには、[Total Network Traffic] チェックボックスをオンにします。

右ペインの下部は、次の要素から構成されています。

- フィルタ基準。
- 用途別にソートされたすべてのアプリケーションファミリが一覧表示される SAIE フロー情報テーブル。デフォルトでは、上位 6 つのアプリケーションファミリが選択されています。右ペインの上部には、選択されたアプリケーションファミリのフローと使用状況がグラフで表示されます。
  - アプリケーションファミリの左側のチェックボックスをオンまたはオフにすると、選択または選択解除できます。一度に最大 6 つのアプリケーションファミリを選択して情報を表示できます。
  - アプリケーションファミリをクリックすると、ファミリ内のアプリケーションが表示されます。
  - アプリケーションにアクセスしているデバイスの送信元 IP アドレスを表示するには、アプリケーションをクリックします。グラフの横にある TLOC ごとのトラフィックを示す円グラフには、TLOC あたりのトラフィック分散（カラー）が表示されます。
  - 列を再配置するには、列のタイトルを目的の位置にドラッグします。

VNF ステータスの表示

VNF ステータスを確認すると、ネットワークサービスの設計時に使用する VNF を決定するのに役立ちます。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表から CSP デバイスを選択します。

3. 左ペインで [VNF Status] をクリックします。
4. 表から VNF 名をクリックします。右ペインには、特定の VNF に関する情報が表示されます。ネットワーク使用率、CPU 使用率、メモリ使用率、ディスク使用率をクリックして、VNF のリソース使用状況を監視できます。

   右ペインの主要部分は、次の要素から構成されています。

   - 次のオプションを含むチャートオプションバー：
     - [Chart Options] ドロップダウン：[Chart Options] ドロップダウンリストをクリックして、表示するデータのタイプを選択します。
     - 期間：データを表示する事前定義された期間またはカスタム期間をクリックします。
   - グラフィック形式の VNF 情報。
   - VNF グラフの凡例：VNF を選択すると、その VNF に関する情報のみが表示されます。

左ペインの詳細部分は、次の要素から構成されています。

- Filter criteria
- すべての VNF に関する情報が一覧表示された VNF テーブル。デフォルトでは、最初の 6 つの VNF が選択されています。右ペインの上部には、選択された VNF の情報がグラフで表示されます。
  - 左側のチェックボックスをオンまたはオフにして、VNF を選択または選択解除します。一度に最大 6 つの VNF を選択して情報を表示できます。
  - 列のソート順を変更するには、列のタイトルをクリックします。

TCP 最適化情報の表示

WAN スループットの表示

ルータで TCP 最適化が有効になっている場合、最適化がルータでの TCP データトラフィックの処理とスループットにどのように影響するかについての情報を表示できます。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。
2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで、[WAN Throughput] をクリックします。右ペインには、WAN スループットがメガビット/秒の単位で表示されます。

右ペインの上部は、次の要素から構成されています。

- チャートオプションバー：デバイス名のすぐ下にあるこのバーは、フィルタオプションのドロップダウンと期間で構成されます。[Filter] をクリックして、VPN、ローカル TLOC カラー、宛先 IP アドレス、リモート TLOC カラー、およびリモートシステムの IP アドレスに基づいて、表示するデータを制限できます。データを表示する事前定義した期間またはカスタム期間をクリックします。
- グラフィック形式の最適化平均スループット情報。
- WAN グラフの凡例：最適化されていないパケットと TCP 最適化パケットのスループットを識別します。

右ペインの下部には、1 時間あたりの平均スループットと最適化された合計スループットが、どちらもメガビット/秒単位で表示されます。

左ペインで [TCP Optimization–Connections] をクリックすると、最も TCP 最適化されたトラフィックが通過するすべてのトンネルに関するステータス情報が表示されます。右ペインの上部は、次の要素から構成されています。

- グラフィック形式の TCP 最適化接続。
- [Connection State] ボックス：接続状態を選択すると、TCP 最適化情報が表示されます。

右ペインの下部は、次の要素から構成されています。

- フィルタ基準。
- トンネルの接続状態など、各トンネルに関する情報を一覧表示するフローテーブル。

Cisco vEdge デバイス の TCP 最適化フローの表示

Cisco vEdge デバイス の TCP 最適化フローに関する情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。
2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、次のコマンドのいずれかを選択します。

（注） Cisco vEdge デバイス を選択すると、次のオプションを使用できます。

デバイスオプション	コマンド	説明
TCP 最適化アクティブフロー	show app tcp-opt	アクティブな TCP 最適化フローに関する情報を表示します。
TCP 最適化期限切れフロー	show app tcp-opt	期限切れの TCP 最適化フローに関する情報を表示します。
TCP 最適化サマリー	show app tcp-opt	TCP 最適化フローのサマリーを表示します。

SFP 情報の表示

ルータの SFP 情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、次のコマンドのいずれかを選択します。

デバイスオプション	コマンド	説明
SFP の詳細	show interface sfp detail	デジタル診断情報の詳細なSFPステータスを表示します。
SFP 診断	show interface sfp detail	SFP 診断情報を表示します。
SFP 測定値	show interface sfp detail	SFP測定データを表示します。
SFP 測定アラーム	show interface sfp detail	測定の SFP アラーム情報を表示します。

NAT DIA トラッカー設定のモニタリング

インターフェイス DIA トラッカーの表示

トランスポート インターフェイスで DIA トラッカーに関する情報を表示するには、次を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. デバイスのリストからデバイスを選択します。
3. [Real Time] をクリックします。
4. シングルエンドポイント トラッカーの場合、[Device Options] ドロップダウンリストから、[Endpoint Tracker Info] を選択します。
5. デュアルエンドポイント トラッカーの場合、[Device Options] ドロップダウンリストから、[Endpoint Tracker Info] を選択します。

TLOC の損失、遅延、ジッター情報の表示

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。
2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで、[WAN] 領域の下にある [TLOC] をクリックします。右ペインには、すべての TLOC カラーについて集約された平均損失または遅延/ジッター情報が表示されます。

右ペインの上部は、次の要素から構成されています。

- チャートオプション：[Chart Options] ドロップダウンと期間が組み込まれています。表示するデータの種類を選択するには、[Chart Options] をクリックします。データを表示する事前定義した期間またはカスタム期間をクリックします。
- グラフィック形式の TLOC 情報：グラフの時間間隔は、BFD アプリケーション認識型ルーティングのポーリング間隔の値によって決まります。
- TLOC グラフの凡例：TLOC カラーを選択すると、その TLOC に関する情報だけが表示されます。

右ペインの下部は、次の要素から構成されています。

- 検索ボックス：検索オプションフィルタが組み込まれています。
- すべての TLOC に関する平均ジッター、損失、および遅延データが一覧表示された TLOC カラーテーブル。デフォルトでは、最初の 6 色が選択されています。右ペインの上部には、選択されたインターフェイスの情報がグラフで表示されます。
  - TLOC カラーを選択または選択解除するには、左のチェックボックスをオンまたはオフにします。一度に最大 30 個の TLOC を選択して情報を表示できます。
  - 選択した TLOC の SD-WAN アプリケーション インテリジェンス エンジン（SAIE）のフロー情報を表示するには、右側の [Application Usage] をクリックします。

（注）

- Cisco vManage リリース 20.8.1 以降では、[Application Usage] 列と [Application Usage] リンクが**[Monitor]** > **[Devices]** > **[WAN – Tunnel]**ウィンドウから削除されています。デバイスのオンデマンド トラブルシューティングを設定すると、選択したフィルタに基づいて、または用途別にソートされたアプリケーションファミリに基づいて SAIE の使用状況データを表示できます。
- Cisco vManage リリース 20.7.x 以前では、SD-WAN アプリケーション インテリジェンス エンジン （SAIE） フローは、ディープ パケット インスペクション（DPI）フローと呼ばれていました。

オンデマンド トラブルシューティングの設定の詳細については、「オンデマンド トラブルシューティング」を参照してください。SAIE フロー表示の詳細については、「SAIE フローの表示」を参照してください。

トンネル接続の表示

平均遅延が最小の Cisco SD-WAN デバイス間で上位 100 のデータプレーントンネルに関する詳細を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Tunnels]**の順に選択します。

   [Tunnels]テーブルには、すべてのトンネルエンドポイントに関する次の情報が一覧表示されます。

   - 正常性
   - 状態
   - Quality of Experience（QoE）スコア。QoE スコアは、ネットワークが一定期間提供できるアプリケーション エクスペリエンスの品質を評価します。
   - ローカル IP とリモート IP
   - 平均遅延、損失、およびジッターデータ

   トンネルの正常性は、次の基準に基づいて定義されます。

   - 良好：QOE スコアが 8 ～ 10 で、トンネルステータスが 1/1 の場合。
   - 可：QOE スコアが 5 ～ 7 で、トンネルステータスが 1/1 の場合。
   - 不良：QOE スコアが 1 ～ 4 の場合、またはトンネルステータスが 0/1 の場合。

（注） Cisco vManage リリース 20.7.1 以降では、トンネル情報は別のメニューとして Cisco vManage で利用できます。

特定のデバイスのトンネル接続を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで、[WAN] 領域の下にある [TLOC] をクリックします。右ペインには、すべてのトンネル接続に関する情報が表示されます。
4. （任意）[Chart Options] ドロップダウンリストをクリックして、表示するデータのタイプを選択します。

   定義済みの期間またはカスタムの期間を選択して、データを並べ替えることもできます。
5. （任意）右ペインの下部で、検索バーのフィルタオプションを使用して、表示するテーブルフィールドをカスタマイズします。

   トンネルテーブルには、すべてのトンネルエンドポイントに関する平均遅延、損失、およびジッターデータが一覧表示されます。デフォルトでは、最初の 6 つのトンネルが選択されています。右ペインの上部には、選択されたトンネルの情報がグラフで表示されます。
6. （任意）トンネルを選択または選択解除するには、左のチェックボックスをオンまたはオフにします。一度に最大 30 個のトンネルを選択して情報を表示できます。
7. （任意）選択した TLOC の SD-WAN Application Intelligence Engine（SAIE）のフロー情報を表示するには、右側の [Application Usage] をクリックします。

（注）
- Cisco vManage リリース 20.8.1 以降では、[Application Usage] 列と [Application Usage] リンクが**[Monitor]** > **[Devices]** > **[WAN – Tunnel]**ウィンドウから削除されています。デバイスのオンデマンド トラブルシューティングを設定すると、選択したフィルタに基づいて、または用途別にソートされたアプリケーションファミリに基づいてSAIEの使用状況データを表示できます。
- Cisco vManage リリース 20.7.x 以前では、SAIE フローはディープ パケット インスペクション（DPI）フローと呼ばれていました。

オンデマンド トラブルシューティングの設定の詳細については、「オンデマンド トラブルシューティング」を参照してください。SAIE フロー表示の詳細については、「SAIE フローの表示」を参照してください。

IPSec トンネル情報の表示

デバイスの IPSec トンネル情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、次のコマンドのいずれかを選択します。

デバイスオプション	CLI コマンド	説明
IPsec インバウンド接続	show tunnel inbound-connections	ローカルルータを起点とする IPSec トンネル接続に関する情報を表示し、トンネルの両端の TLOC アドレスを示します。
IPsec ローカル SA	show tunnel local-sa	ローカル TLOC の IPSec トンネルのセキュリティ アソシエーションを表示します。

ライセンス情報の表示

デバイスのライセンス情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、次のコマンドのいずれかを選択します。

デバイスオプション	コマンド	説明
スマートライセンス <情報>	show licenses	Cisco SD-WAN で使用されているソフトウェアパッケージのライセンスを表示します。

ロギング情報の表示

デバイスのロギング情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]**の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、次のコマンドを選択します。

デバイスオプション	コマンド	説明
Logging	show logging	syslog メッセージのロギング設定を表示します。

トンネルの損失率、遅延、ジッター、オクテット情報の表示

Cisco vManage の 1 つのチャートオプションで、トンネルの損失率、遅延、ジッター、およびオクテットを表示できます。

表 *11* : 機能の履歴

機能名	リリース情報	説明
トンネルの損失率、遅延、ジッター、オクテット情報の表示	Cisco IOS XE リリース 17.5.1a Cisco SD-WAN リリース 20.5.1 Cisco vManage リリース 20.5.1	この機能は、パケット損失、遅延、ジッター、オクテットなどのトンネル情報を表示するための単一チャートオプションを Cisco vManage で提供します。

トンネルの損失率、遅延、ジッター、オクテットの表示

[Real Time] オプションまたは他の時間枠を選択して、グラフにトンネル情報を表示できます。

Cisco vManage で損失率、遅延、ジッター、およびオクテットを表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. デバイスを選択します。
3. 左ペインで、[WAN] 領域の下にある [Tunnel] をクリックします。右ペインには、すべてのトンネル接続に関する情報が表示されます。
4. 右ペインで [Chart Options] をクリックして、情報を表示する際の形式を選択します。トンネル情報をトラブルシューティングするには、[Loss Percentage/Latency/Jitter/Octets] をクリックします。

右ペインの上部は、次の要素から構成されています。

- 各トンネルのデータが時間に基づいてグラフ化されています。
- グラフの凡例：トンネルを選択すると、そのトンネルだけの情報が表示されます。各トンネルの線とデータポイントは、一意に色分けされています。

右ペインの下部は、次の要素から構成されています。

- 検索バー：部分一致や完全一致条件に基づいてテーブルをフィルタリングするための検索オプションフィルタが組み込まれています。
- トンネルテーブル：すべてのトンネルエンドポイントに関するジッター、遅延、損失率などのデータが一覧表示されます。デフォルトでは、最初の 6 つのトンネルが選択されています。右ペインの上部には、選択されたトンネルの情報がグラフで表示されます。
  - 列のドロップダウンリストをクリックして、すべての説明を有効または無効にできます。
  - トンネルを選択または選択解除するには、左のチェックボックスをオンまたはオフにします。一度に最大 6 つのトンネルを選択して情報を表示できます。

Wi-Fi 設定の表示

Cisco vEdge デバイス などのワイヤレス LAN（WLAN）をサポートする Cisco SD-WAN ルータの Wi-Fi 設定を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。
2. デバイスを選択します。
3. 左ペインで [WiFi] をクリックします。右ペインには、ルータの Wi-Fi 設定に関する情報が表示されます。

右ペインの上部は、次の要素から構成されています。

- AP 情報バー：デバイス名のすぐ下にあります。アクセスポイント情報と [Clients Details] ボタンが表示されます。[Clients Details] ボタンをクリックすると、選択した期間中に Wi-Fi アクセスポイントに接続されたクライアントに関する情報が表示されます。
- アクセスポイントの無線周波数パラメータ。
- 仮想アクセスポイント（VAP）の SSID パラメータ。

右ペインの下部は、次の要素から構成されています。

- VAP の送受信の統計情報バー：期間が表示されます。データを表示する事前定義した期間またはカスタム期間をクリックします。
- VAP は統計情報をグラフィック形式で送受信します。
- VAP 統計グラフの凡例：VAP インターフェイスを選択すると、そのインターフェイスに関する情報だけが表示されます。VAP インターフェイスをもう一度クリックすると、前の表示に戻ります。

制御接続のリアルタイム表示

Cisco vEdge デバイス のコントロールプレーン接続をリアルタイムビューで表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。
2. デバイスを選択します。
3. 左ペインで [Troubleshooting] をクリックします。
4. [Connectivity] 領域で、[Control Connections (Live View)] をクリックします。

コントロールプレーンの接続画面は、15 秒ごとに自動的に更新されます。

右ペインの上部には、エッジデバイス、Cisco vManage、および Cisco vSmart コントローラ間で稼働中のコントロール プレーン トンネルを示す図が表示されます。

下部ペインの下方には、リモートデバイスの IP アドレスやトンネルエンドポイントのステータス（エンドポイントの障害の理由など）など、各コントロール プレーン トンネルの詳細を示すテーブルが表示されます。

Cisco Umbrella 情報の表示

デバイスの Cisco Umbrella 情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、次を選択します。

デバイスオプション	コマンド	説明
Umbrella デバイスの登録	show umbrella deviceid	Cisco IOS XE SD-WAN デバイス の Cisco Umbrella 登録ステータスを表示します。

VRRP 情報の表示

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。
2. デバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、[VRRP Information] を選択します。

QoS 情報の表示

QoS統計を表示して、ネットワーク内のどのデバイスのどのトラフィッククラスで、最も多くのドロップが発生したかを把握できます。

表 *12* : 機能の履歴

機能名	リリース情報	説明
Cisco vManage での QoS モニタリング	Cisco IOS XE リリース 17.2.1r	このリリースでは、Cisco vManage を使用してインターフェイス単位の QoS 情報を表示する機能が拡張され、Cisco IOS XE SD-WAN デバイス をサポートするようになりました。このリリースより前は、Cisco IOS XE SD-WAN デバイスの QoS 情報は、デバイスの CLI を介してのみモニタリングできました。

Cisco vEdge デバイス では、この機能はすでに利用可能になっています。

QoS モニタリングの制限事項

- この機能はサブインターフェイスではサポートされていません。
- トンネルごとに QoS が有効になっている場合、この機能はサポートされません。

QoS 情報チャートの表示

QoS チャートには、選択したインターフェイスのパケット速度と各キューでドロップされたパケット数が表示されます。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]**の順に選択します。

2. 表示されるデバイスリストからデバイスを選択します。
3. 左ペインの [Applications] 領域にある [QoS] をクリックします。
4. 右ペインの上部から次のオプションを選択できます。
   - [Interface Name]：ドロップダウンメニューから、QoS データを表示するインターフェイスを選択します。
   - [Time Range]：リアルタイムまたは事前定義した時間範囲（1 時間、3 時間、6 時間など）で、特定の時間範囲の情報を表示すか、[Custom] をクリックして時間範囲を定義します。

     リアルタイムの QoS 情報は表形式で表示することもできます。「リアルタイム QoS 情報テーブルの表示」のセクションを参照してください。

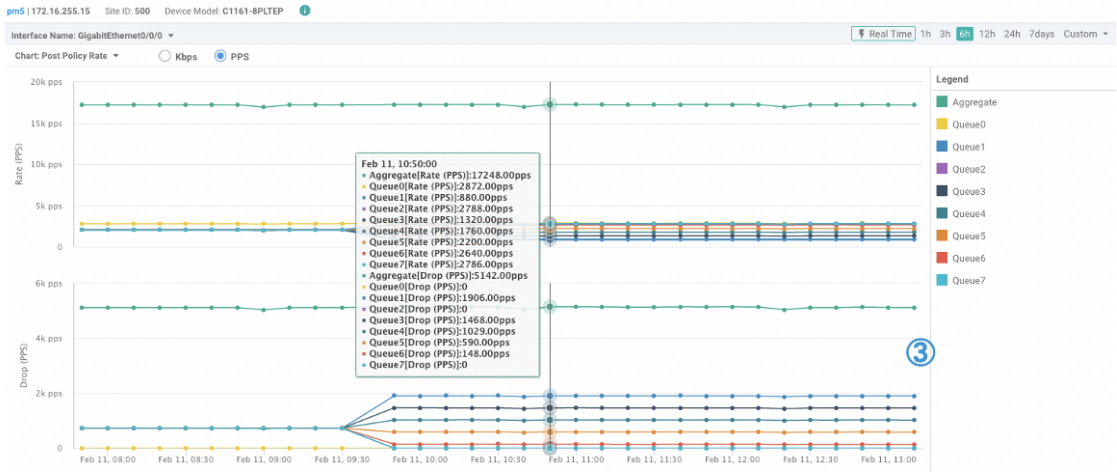
5. [Chart] ドロップダウンリストから、次のいずれかを選択します。
   - [Post Policy Rate]：1 秒あたりのデータ転送速度を kbps（デフォルト）または 1 秒あたりのパケット数（PPS）で表示します。この値の計算では、ポストポリシーカウンタ/10 の式を使用して 1 秒あたりの速度が求められます。

   または

   - [Post Policy Counter]：過去 10 秒間にキューを通過したパケット数（またはバイト単位のパケット数）を表示します。

   QoS チャートが表示されます。次の例は、選択したインターフェイスに対して時間範囲履歴を指定した場合の QoS データを示しています。このチャートでは、各データポイントは 10 分を表します。長い時間範囲の場合、Cisco vManage はデータポイントを集約します。

図 *1 : QoS* チャート



Cisco vManage では、チャートの下にテーブルも表示されます。ただし、チャートを生成する際に [Real Time] オプションを選択した場合でも、テーブルには常に履歴データが表示されます。リアルタイムチャートの下にそのような履歴テーブルが生成ますが、チャートのリアルタイム値とは関係ありません。

次の例は、リアルタイム QoS チャートの下に生成された履歴データを示すテーブルです。

図 *2 : QoS* 履歴テーブル

Queue Name	Pre Policy Tx (in kbps)	Post Policy Tx (in kbps)	Drop (in kbps)
Aggregate	259230.875	199686.969	59543.344
Queue0	32538.344	32538.344	0
Queue1	32362.406	14931.094	17430.75
Queue2	32380.75	29467.031	2913.563
Queue3	32390.906	18288.25	14102.031
Queue4	32401.281	21645.594	10755.188
Queue5	32404.125	25002.75	7400.875
Queue6	32391.5	28359.969	4030.969
Queue7	32358.031	29450.25	2907.656

リアルタイム QoS 情報テーブルの表示

リアルタイムの QoS 情報を表形式で表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスリストからデバイスを選択します。
3. 左ペインで、[Security Monitoring] 領域の下にある [Real Time] をクリックします。
4. [Device Options] ドロップダウンリストから、[Interface QoS Statistics] を選択します。

QoS 統計の表が表示されます。[Filter] ドロップダウンリストからインターフェイスを選択すると、インターフェイス名で表をフィルタリングできます。

トラフィックの正常性の確認

トンネルの正常性の表示

双方向からのトンネルの正常性を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。
2. デバイスを選択するには、[Hostname] 列でデバイス名をクリックします。
3. 左ペインで [Troubleshooting] をクリックします。
4. [Traffic] 領域で [Tunnel Health] をクリックします。
5. [Local Circuit] ドロップダウンリストから、送信元の TLOC を選択します。
6. [Remote Device] ドロップダウンリストから、リモートデバイスを選択します。
7. [Remote Circuit] ドロップダウンリストから、宛先の TLOC を選択します。
8. [Go] をクリックします。画面の下部には、以下の情報が表示されます。
9. [Chart Options] ドロップダウンリストから [Loss Percentage]、[Latency/Jitter]、[Octets] のいずれかを選択します。
10. （任意）左ペインで事前定義した期間またはカスタム期間を選択すると、指定した期間のデータが表示されます。

ウィンドウに次の情報が表示されます。

- 各方向の 2 つのデバイス間にあるすべてのトンネルに関するグラフィック形式のアプリケーションルート データ （損失、遅延、ジッター）。
- アプリケーションルート グラフの凡例：選択されたトンネルを両方向から識別します。

アプリケーション認識型ルーティングトラフィックの確認

送信元デバイスから宛先デバイスへのアプリケーション認識型ルーティングトラフィックを確認するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスリストからデバイスを選択します。
3. 左ペインで [Troubleshooting] をクリックします。
4. 右ペインで、[Traffic] の下にある [App Route Visualization] をクリックします。
5. [Remote Device] ドロップダウンリストから宛先デバイスを選択します。
6. （任意）[Traffic Filter] をクリックします。[No Filter] または [SAIE] を選択します。デフォルトでは、[No Filter] が選択されています。

（注） Cisco vManage リリース 20.7.x 以前では、SD-WAN アプリケーション インテリジェンス エンジン（SAIE）フローは、ディープ パケット インスペクション（DPI）フローと呼ばれていました。

7. [Go] をクリックします。画面の下部には、以下の情報が表示されます。
8. [Chart Options] ドロップダウンリストから [Loss Percentage]、[Latency/Jitter]、[Octets] のいずれかを選択します。
9. （任意）左ペインで事前定義した期間またはカスタム期間を選択すると、指定した期間のデータが表示されます。

パケットのキャプチャ

表 *13 :* 機能の履歴

機能名	リリース情報	説明
組み込みパケットキャプチャ	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能は、ネットワーク管理者がデバイスに出入りするパケットをキャプチャできるオンボード パケット キャプチャ機能です。管理者は Cisco vManage を使用してキャプチャしたパケットをローカルで分析することも、保存やエクスポートしてからオフラインで分析することもできます。この機能により、パケットの形式に関する情報が収集され、アプリケーションの分析、セキュリティ、トラブルシューティングに役立てることができます。

機能名	リリース情報	説明
CLI コマンドを使用した Cisco vEdge デバイスの組み込みパケットキャプチャ	Cisco SD-WAN リリース 20.6.1	この機能はトラフィック データをキャプチャするための代替方法を提供します。サポートされている CLI コマンドを使用して、Cisco vEdge デバイスと Cisco vManage 間の接続問題をトラブルシュートすることができます。この機能の一部として、トラフィックの詳細をキャプチャする次のコマンドが導入されています。 request stream capture show packet-capture
Cisco IOS XE SD-WAN デバイスの双方向パケットキャプチャ	Cisco IOS XE リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能により、組み込みパケットキャプチャ機能が強化され、Cisco vManage を通して双方向のパケットキャプチャがサポートされます。
IPv6 対応の双方向パケットキャプチャ	Cisco IOS XE リリース 17.9.1a	この機能により、IPv6 トラフィックデータの双方向キャプチャのサポートが追加され、CLI テンプレートを使用して接続問題をトラブルシュートできます。

双方向パケットキャプチャについて

インターフェイスを通過するトラフィックをキャプチャできます。コントロールプレーンの場合は、一方向または両方向（双方向）でトラフィックをキャプチャできます。パケットをローカルで分析することも、キャプチャしたトラフィックをエクスポートしてオフラインで分析することもできます。Cisco IOS XE リリース 17.9.1a では、パケットキャプチャは IPv6 トラフィックをサポートしています。

Cisco vManage を使用したパケットキャプチャの設定

コントロールプレーンとデータプレーンのパケットをリアルタイムでキャプチャし、これらのパケットをエッジデバイスで使用可能なファイルに保存するには、次の手順を実行します。

（注） ループバック インターフェイスでは、パケットキャプチャはサポートされていません。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]**の順に選択します。

2. デバイスを選択するには、[Hostname] 列でデバイス名をクリックします。

3. 左ペインで [Troubleshooting] をクリックします。
4. [Traffic] で [Packet Capture] をクリックします。
5. VPN ドロップダウンリストで VPN を選択します。
6. [Interface] ドロップダウンリストでインターフェイスを選択します。

（注） Cisco vManage リリース 20.8.1 以降では、トラフィックのトレースとトラブルシューティングのために IPv6 パケットをキャプチャできます。これを実行するには、[Interface] ドロップダウンリストで IPv6 インターフェイスを選択します。Cisco vManage リリース 20.8.1 より前は、IPv4 インターフェイスのキャプチャのみがサポートされていました。

7. （任意）[Traffic Filter] をクリックして、IP ヘッダーの値に基づいてキャプチャするパケットをフィルタ処理します。次のフィールドの値を入力します。
   1. [Source IP] フィールドには、パケットの送信元 IP アドレスを入力します。
   2. [Source Port] フィールドには、パケットの送信元ポート番号を入力します。
   3. [Protocol] フィールドには、パケットのプロトコル ID を入力します。
   4. [Destination IP] フィールドには、パケットの宛先 IP アドレスを入力します。
   5. [Destination Port] フィールドには、パケットの宛先ポート番号を入力します。
8. Cisco IOS XE SD-WAN デバイスの場合、双方向パケットキャプチャを有効にするには、[Bidirectional] ボタンをオンに設定します。

（注） Cisco vManage リリース 20.7.1では、双方向パケットキャプチャ機能が導入されています。

9. [Start] をクリックします。パケットキャプチャが開始され、進行状況が表示されます。
   1. 「Packet Capture in Progress」：収集されたパケットが 5 MB に達した場合、または [Stop] をクリックすると、パケットキャプチャが停止します。
   2. 「Preparing file to download」：Cisco vManage は `libpcap` 形式のファイル（.pcap ファイル）を作成します。
   3. 「File ready, click to download the file」：ダウンロードアイコンをクリックして、生成されたファイルをダウンロードします。

（注） Cisco vManage クラスタ環境では、デバイスが接続されている Cisco vManage ノードに関係なく、クラスタ内のすべてのデバイスで速度テストを実行し、パケットをキャプチャできます。以下を使用してデータストリームを設定できます。

管理 IP アドレスと VPN 512（Cisco CSR 1000v シリーズ プラットフォームは管理 IP アドレスをサポートしていません）

または

トランスポート IP アドレスと VPN 0

Cisco vManage ノードのシステム IP アドレスと VPN 0 を使用したデータストリームの設定は、クラスタ環境では推奨されません。速度テストとパケットキャプチャが、データストリームで設定されている Cisco vManage ノードに接続されたデバイスのみに制限されるためです。

CLI テンプレートを使用したパケットキャプチャの設定

はじめる前に

CLI テンプレートの使用方法の詳細については、「CLI テンプレート」を参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

パケットキャプチャのモニタリングのCLI設定を有効にするには、手順に従って、[Administration] 設定の [Data Stream] が [Enabled] になっていることを確認します。

1. Cisco vManage のメニューで、**[Administration]** > **[Settings]** を選択します。
2. [Data Stream] 領域で、[Edit] をクリックします。
3. [Enabled] をクリックして、[IP Address Type] を選択します。デフォルトでは、[System] が選択されています（[Transport] および [Management] のタイプには、[Hostname] と [VPN] を追加で設定する必要があります）。
4. [Save] をクリックします。

IPv4 トラフィックのパケットキャプチャの設定

IPv4 パケットキャプチャをモニタリングするためのコアフィルタを定義します。

monitor capture *capture-name* **match ipv4** *source-prefix/length destination-prefix/length* **[bidirectional]**

IPv4 トラフィックをフィルタリングしてキャプチャする場合の設定例を以下に示します。

```
monitor capture mycap match ipv4 198.51.100.0/24 host 198.51.100.1
```

IPv6 トラフィックのパケットキャプチャの設定

インターフェイスまたはコントロールプレーンを通過するインバウンドトラフィックまたはアウトバウンドトラフィック、またはインバウンドとアウトバウンドの両方のトラフィック（双方向）の IPv6 パケットキャプチャをモニタリングするためのフィルタを設定します。次のいずれかを実行します。

- インターフェイスのパケットキャプチャを設定します。

  monitor capture *capture_name* [**interface** *interface-name interface-num* {**both** | **in** | **out**}] **match ipv6** {{*ipv6-source-prefix/length*| **host** *ipv6-src-addr*| any} {*ipv6-destination-prefix/length*| **host** *ipv6-dest-addr*| any}} |**protocol** {*<0-255>*|**tcp**|**udp**} {*ipv6-source-prefix/length*| **host** *ipv6-src-addr*| any} [{**eq** | **lt**| **gt**| **neq** |**range** *port_number*} *port_number*] {*ipv6-destination-prefix/length*| **host** *ipv6-dest-addr*| any} [{**eq** | **lt**| **gt**| **neq** |**range** *port_number*} *port_number*]} [**bidirectional**]

- コントロールプレーンのパケットキャプチャを設定します。

  monitor capture *capture_name* [**control-plane** {**both** | **in** | **out**}] **match ipv6** {{*ipv6-source-prefix/length*| **host** *ipv6-src-addr*| any} {*ipv6-destination-prefix/length*| **host** *ipv6-dest-addr*| any}} |**protocol** {*<0-255>*|**tcp**|**udp**} {*ipv6-source-prefix/length*| **host** *ipv6-src-addr*| any} [{**eq** | **lt**| **gt**| **neq** |**range** *port_number*} *port_number*] {*ipv6-destination-prefix/length*| **host** *ipv6-dest-addr*| any} [{**eq** | **lt**| **gt**| **neq** |**range** *port_number*} *port_number*]} [**bidirectional**]

IPv6 トラフィックをフィルタリングしてキャプチャする場合の設定例を以下に示します。

```
monitor capture test interface GigabitEthernet 5 both match ipv6 protocol tcp host
2001:3c0:1::71 host 2001:380:1::71 bidirectional
monitor capture cap interface gig 2 in match ipv6 50::1/128 50::2/128 bidirectional
monitor capture cap interface gig 2 out match ipv6 50::1/128 50::2/128 bidirectional
monitor capture cap interface gig 2 both match ipv6 50::1/128 50::2/128 bidirectional
monitor capture cap control-plane in match ipv6 50::1/128 50::2/128 bidirectional
monitor capture cap control-plane out match ipv6 50::1/128 50::2/128 bidirectional
monitor capture cap control-plane both match ipv6 50::1/128 50::2/128 bidirectional
```

フローのシミュレート

表 *14 :* 機能の履歴

機能名	リリース情報	説明
転送サービサビリティ	Cisco IOS XE リリース 17.2.1r	この機能により、Cisco vManage テンプレートのフローのシミュレート機能でサービスパスとトンネルパスが有効になり、IP パケットのネクストホップ情報が表示されます。また、Cisco IOS XE SD-WAN デバイスの速度テストとフローのシミュレート機能が有効になります。

ルータで利用可能な IP パケットのネクストホップ情報を表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスリストからデバイスを選択します。
3. 左ペインで [Troubleshooting] をクリックします。
4. [Traffic] で、[Simulate Flows] をクリックします。
5. データトラフィックのパスを指定するには、必須フィールドで値を選択するかデータを入力します。
   - [VPN]：データトンネルが配置されている VPN。
   - [Source/Interface]：cflowd フローを開始するインターフェイス。
   - [Source IP]：cflowd フローの開始 IP アドレス。
   - [Destination IP]：cflowd フローの宛先 IP アドレス。
   - [Application]：ルータで実行されているアプリケーション。
   - カスタムアプリケーション（CLIで作成）
6. [Advanced Options] をクリックします。
   1. [Path] フィールドで、[Tunnel] または [Service] を選択して、データトラフィックパス情報がルータのサービス側から来るのか、トンネル側から来るのかを示します。
   2. [Protocol] フィールドにプロトコル番号を入力します。
   3. [Source Port] フィールドに cflowd フローを開始するポートを入力します。
   4. [Destination Port] フィールドに cflowd フローの宛先ポートを入力します。

5. [DSCP] フィールドに cflowd パケットの DSCP 値を入力します。
6. （任意）パケットの利用可能パスをすべて表示するには、[All Paths] チェックボックスをオンにします。

7. [Simulate] をクリックして、指定したヘッダーを持つパケットのネクストホップを判断します。

サービスパスおよびトンネルパスのコマンドについては、show sdwan policy service-path および show sdwan policy tunnel-path のコマンドページを参照してください。

セキュリティモニタリング

表 *15*：機能の履歴

機能名	リリース情報	説明
Cisco SD-WAN デバイスで強化されたセキュリティモニタリング	Cisco IOS XE リリース 17.5.1a Cisco SD-WAN リリース 20.5.1 Cisco vManage リリース 20.5.1	この機能を使用すると、デバイスの CPU、メモリ、およびトラフィックの使用状況を表示できます。個々の UTD 機能の状態を表示することもできます。

トラフィック、CPU、メモリの使用状況の表示

1. Cisco vManage の**[Monitor]** > **[Devices]**ページでデバイスを選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage の**[Monitor]** > **[Network]**ページでデバイスを選択します。

2. 左ペインの [Security Monitoring] で、[Intrusion Prevention]、[URL Filtering] などの UTD 機能を 1 つ選択します。
3. デフォルトでは、トラフィックカウンタグラフが表示されます。

   時間範囲をカスタマイズして、**リアルタイム**、**1 時間**、**3 時間**などの特定の時間範囲のトラフィック量を表示することも、**カスタム**の時間範囲を指定することもできます。デフォルトの時間範囲は、**24 時間**です。365 日を超える時間範囲を指定することはできません。

4. CPU やメモリの使用率を表示するには、次の手順を実行します。
   - CPU の使用率を表示するには、[UTD Stats: CPU Usage] をクリックします。
   - メモリの使用率を表示するには、[UTD Stats: Memory Usage] をクリックします。

UTD の正常性と到達可能性の表示

1. Cisco vManage の**[Monitor]** > **[Devices]**ページでデバイスを選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco vManage の**[Monitor]** > **[Network]**ページでデバイスを選択します。

2. 左ペインの [Security Monitoring] で、[Intrusion Prevention]、[URL Filtering] などの UTD 機能を 1 つ選択します。

3. すべての機能について、UTD の状態が次のいずれかで表示されます。

   - ダウン：UTD が設定されていないなどを示します。
   - 緑色：UTD は正常です。
   - 黄色：メモリ使用率が高いなどを示します。
   - 赤色：1 つ以上の Snort インスタンスが停止しているなどを示します。

   デバイスで UTD を設定したにもかかわらずステータスが緑色でない場合は、Cisco TAC にサポートを依頼してください。

4. 選択した UTD 機能に応じて、次の追加情報が表示されます。

UTD 機能	ステータス
Intrusion Prevention	パッケージのバージョン 最後に更新されたIPS 最後の更新ステータスの理由
URL Filtering	クラウドの到達可能性
Advanced Malware Protection	AMP クラウド到達可能性ステータス TG クラウド到達可能性ステータス
Umbrella DNS Redirect	Umbrella に登録されたVPN DNSCrypt

システムクロックの表示

最小リリース：Cisco vManage リリース 20.9.1

システムクロックを表示するには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Devices]**の順に選択します。

Cisco vManage リリース 20.6.x 以前：Cisco vManage のメニューから**[Monitor]** > **[Network]** の順に選択します。

2. 表示されるデバイスのリストからデバイスを選択します。
3. 左ペインで [Real Time] をクリックします。
4. [Device Options] をクリックし、次のコマンドを選択します。

デバイスオプション	コマンド	説明
システム クロック	show clock	システムクロックの日時を表示します。

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